ESET PROTECT On-Prem

Virtual Appliance Deployment Guide

Click here to display the online version of this document

ESET PROTECT On-Prem was developed by ESET, spol. s r.o.

For more information visit https://www.eset.com.

Technical Support: https://support.eset.com

REV. 4/12/2024

ESET PROTECT Virtual Appliance

The ESET PROTECT Virtual Appliance (ESET PROTECT VA) is available for users who want to run ESET PROTECT On-Prem in a virtualized environment. Additionally, the ESET PROTECT Virtual Appliance simplifies deployment of ESET PROTECT On-Prem and is faster than using the All-in-one installer or component installation packages.

The ESET PROTECT VA can be deployed in most virtual environments. It supports native/bare-metal hypervisors (VMware vSphere/ESXi and Microsoft Hyper-V) as well as hosted hypervisors that usually run on desktop operating systems (VMware Workstation, VMware Player and Oracle VirtualBox), see Supported hypervisors for a complete list.

The ESET PROTECT Virtual Appliance runs out of the box:

- It contains the ESET PROTECT Server running on a dedicated VM and contains a functional operating system.

- It also includes other ESET PROTECT components—ESET Management Agent, ESET Rogue Detection Sensor and ESET Bridge (HTTP Proxy).

The new ESET PROTECT Virtual Appliance based on Rocky Linux

Due to the CentOS 7 End of Life, a new ESET PROTECT Virtual Appliance (VA) based on Rocky Linux 9.3 was released on March 26, 2024:

- You can verify the operating system of your ESET PROTECT Virtual Appliance 11.0 based on the **Server version**:
  - 11.0.199.0 and earlier—CentOS 7 (VA 11.0.14.0 and earlier)
  - 11.0.215.0 and later—Rocky Linux 9.3 (VA 11.0.19.0 and later)
- ESET PROTECT components in the new VA have been adjusted to be compatible with Rocky Linux. Despite their higher version numbers, they are the same as the officially released ESET PROTECT 11.0 components.
- See the migration instructions to migrate to the new Virtual Appliance.

This guide describes in detail how to deploy and manage ESET PROTECT VA, including its features.

Deployment and configuration

1. ESET PROTECT VA deployment process—Actual deployment of ESET PROTECT Virtual Appliance *.ova* file on your hypervisor.

2. ESET PROTECT VA configuration—Post-deployment configuration done via web interface of the ESET PROTECT VA. It is a configuration page that allows you to choose appliance type and then type specific details and properties required for that specific ESET PROTECT VA type to run correctly.

Further configuration and management

- ESET PROTECT VA Management Console is a simple text-based user interface based around a main menu. The interface will assist you with text commands by asking you to specify values when necessary. Even users who do not have advanced experience with Linux operating systems can use and manage ESET PROTECT VA with ease. Some important features include:

  - Set static IP address—Manually specify the static IP address if your ESET PROTECT VA is not assigned an IP address by a DHCP server.

- Pull database from other server—If you need to upgrade or migrate your ESET PROTECT VA.
- Backup and restore of ESET PROTECT database—These features are important for your disaster recovery strategy and are available in case of problems with ESET PROTECT VA.
- Factory reset—Restores the appliance to a freshly deployed state. This can be useful if you experience issues with ESET PROTECT VA. Have a backup of the database ready to avoid losing your data.

- Webmin Management Interface—A third-party web-based interface that simplifies the management of a Linux system. It gives you the convenience of managing your ESET PROTECT VA remotely from your web browser using an intuitive interface. The most important Webmin modules are described in this document.

Upgrade, migration and disaster recovery procedures

- ESET PROTECT VA upgrade/migration—If you want to upgrade your ESET PROTECT VA to the latest version, see this section for details and step-by-step procedure. Also, the same procedure applies if you need to migrate your ESET PROTECT VA.

- ESET PROTECT VA disaster recovery—Follow this procedure if ESET PROTECT VA stopped working and you cannot fix the problem or if you are unable to recover a damaged ESET PROTECT VA instance.

About help

This guide, the VA Deployment Guide, provides instructions to deploy and configure the ESET PROTECT Virtual Appliance (ESET PROTECT VA). This guide is intended for anyone who wants to deploy, manage and update ESET PROTECT VA.

For consistency and to help prevent confusion, the terminology used throughout this guide is based on the ESET PROTECT On-Prem parameter names. We also use a set of symbols to highlight topics of specific interest or significance.

Notes can provide valuable information, such as specific features or a link to a related topic.

This requires your attention and it should not be skipped. Usually, it provides non-critical but significant information.

Critical information you should treat with increased caution. Warnings are placed specifically to deter you from committing potentially harmful mistakes. Please read and understand text placed in warning brackets, as it references highly sensitive system settings or something risky.

Example scenario that describes a user case relevant for the topic where it is included. Examples are used to explain more complicated topics.

Convention	Meaning
Bold type	Names of interface items such as boxes and option buttons.
Italic type	Placeholders for information you provide. For example, filename or path means you type the actual path or a name of file.
`Courier New`	Code samples or commands.
Hyperlink	Provides quick and easy access to cross-referenced topics or external web location. Hyperlinks are highlighted in blue and may be underlined.

Convention	Meaning
%ProgramFiles%	The Windows system directory which stores installed programs of Windows and others.

- Online Help is the primary source of help content. The latest version of Online Help will automatically be displayed when you have a working internet connection. The ESET PROTECT On-Prem online help pages include four active tabs at the top navigation header: Installation/Upgrade, Administration and VA Deployment.
- Topics in this guide are divided into several chapters and sub-chapters. You can find relevant information by using the search field at the top.

When you open a User Guide from the navigation bar at the top of the page, search will be limited to the contents of that guide. For example, if you open the Administrator guide, topics from the Installation/Upgrade and VA Deployment guides will not be included in search results.

- The ESET Knowledgebase contains answers to the most frequently asked questions, as well as recommended solutions for various issues. Regularly updated by ESET technical specialists, the Knowledgebase is the most powerful tool for resolving various types of problems.
- The ESET Forum provides ESET users with an easy way to get help and to help others. You can post any problem or question related to your ESET products.
- You can post your rating and/or provide a feedback on a specific topic in help: Click the **Was this information helpful?** link underneath the help page.

Prerequisites

The following prerequisites must be met before ESET PROTECT Virtual Appliance deployment:

- You must use a supported hypervisor.
- Verify that the guest operating system (if a hosted hypervisor, such as VMware Workstation/Player or Oracle VirtualBox is used) is supported.
- Verify that system clock settings between the host and guest operating systems are synchronized.
- **VT must be enabled** in the host system BIOS. This feature may be named VT, Vanderpool Technology, Virtualization Technology, VMX, or Virtual Machine Extensions. This setting is commonly located in the security screen of the BIOS. The location of this setting varies depending on the system vendor.
- Ensure the connection for the network adapter on your Virtual Machine is set to **Bridged** (or, alternatively **NAT**).
- If you are using **NAT** mode, port forwarding must be configured on your virtual machine for ESET PROTECT On-Prem to be accessible from the network. Ports that need forwarding are displayed in the console window of your ESET PROTECT VA after you have deployed and configured it.
- ESET PROTECT Virtual Appliance only supports IPv4 environments. While You can manually set up an IPv6 environment, IPv6 is not supported.

We recommend that you create a snapshot of your newly deployed and configured ESET PROTECT VA and synchronize it with Active Directory. We also recommend that you back up the database before deploying the ESET Management Agent on client computers.

Recommended system configurations

Depending on the size of your infrastructure, namely number of client machines that will be managed by ESET PROTECT Virtual Appliance, take into account recommended and minimal virtual machine configuration.

The default ESET PROTECT Virtual Appliance configuration settings:

	CentOS	Rocky Linux
CPU cores	4	6
RAM	4 GB	8 GB
Disk	64 GB	128 GB

The following sizing applies to ESET PROTECT Server running on a Virtual Appliance:

Number of clients	Up to 1,000	1,000–5,000
Number of CPU cores	4	8
RAM size	4 GB	8 GB
Disk IOPS*	500	1,000
Agent connection interval (during deployment phase)	60 seconds	5 minutes
Agent connection interval (after deployment, during standard usage)	10 minutes	10 minutes
Other recommendations	Thick provisioned disk, manually change configuration to increase memory size for MySQL.	Proportionally increase available resources for your ESET PROTECT VA to prevent performance issues.

* IOPS (total I/O operations per second)—We recommend having approximately 0.2 IOPS per connected client, but no less than 500.

If you are planning to have more than 5,000 managed clients, we highly recommend that you install ESET PROTECT Server/MDM on a physical machine running Microsoft Windows Server with Microsoft SQL Server.

Supported hypervisors

The ESET PROTECT Virtual Appliance (*protect_appliance.ova*) is a `vmx-08` virtual hardware family type appliance.

The Virtual Appliance is supported only on the listed hypervisors. Running it on other hypervisors is on user risk.

Hypervisor	Version	ESET PROTECT Server Appliance	ESET PROTECT MDM Appliance
VMware vSphere/ESXi	6.5 and later	✔	✔
VMware Workstation	9 and later	✔	✔
VMware Player	7 and later	✔	✔
Microsoft Hyper-V	Server 2012, 2012 R2, 2016, 2019	✔	✔
Oracle VirtualBox	6.0 and later	✔	✔
Citrix	7.0 and later	✔	✔

We recommend that you use a DHCP server in your network to assign your ESET PROTECT VA an IP address. This IP address is necessary for access to the ESET PROTECT VA configuration web interface. If you do not have a DHCP server in your network, you must Set static IP address.

Download ESET PROTECT Virtual Appliance

The ESET PROTECT Virtual Appliance is available from the ESET PROTECT On-Prem download page:

- The appliance is available as protect_appliance.ova (Open Virtualization Appliance).
- If you are deploying your VA on Microsoft Hyper-V, use the protect_appliance.vhdx.zip file instead of the *.ova* file.

ESET PROTECT On-Prem Mobile Device Management (MDM) reached the End of Life. This feature is no longer available in the latest VA based on Rocky Linux. We recommend that you migrate to the cloud ESET PROTECT with the Cloud MDM.

The *.ova* file is a template that contains a functional operating system (CentOS or Rocky Linux—read more). To deploy the ESET PROTECT VA *.ova* file, follow the instructions for your hypervisor. When using *protect_appliance.ova*, you can choose which ESET PROTECT Virtual Appliance type you want your VM to run following deployment. When you have selected the type, you can start configuring your ESET PROTECT Virtual Appliance. After you deploy the *.ova* file, select the appliance type and configure settings for your VA. The VA is a complete environment with ESET PROTECT On-Prem (or one of its components).

Before you begin deployment, ensure that all prerequisites are met.

When you finish the deployment and configuration process, you can connect to the ESET PROTECT Server using the ESET PROTECT Web Console and start using ESET PROTECT On-Prem.

ESET provides the ESET PROTECT Virtual Appliances, however, ESET is not responsible for support and maintenance of your OS or OS components. ESET PROTECT Virtual Appliances are designed to simplify usage and deployment and come with a publicly available operating system that includes non-ESET components. Managing and updating these components is the sole responsibility of the user of the ESET PROTECT Virtual Appliance. We recommend that you regularly update the operating system to prevent security issues.

ESET PROTECT VA passwords

ESET PROTECT Virtual Appliance uses a few different user accounts. The following table explains the different account types:

Account type	Username	Default password	Description and use
Operating system root	`root`	`eraadmin`	This is an account which you can use to log into your ESET PROTECT Virtual Appliance. It allows you to access ESET PROTECT VA Management Console and Webmin Management Interface, allows you to perform Factory reset or if you need to Pull database from other server. Usually, you will be asked to type your **VM password**.
Administrator	`admin`	`eraadmin`	This user account in the `sudo` group is only in Rocky Linux and serves for remote access via SSH (use `root` in CentOS).
Database (MySQL) root	`root`	`eraadmin`	This is a root account for the MySQL database server. It allows you to perform database operations such as database Backup or database Restore. Usually, you will be asked to type your **database root password**.
ESET PROTECT Web Console Administrator	`Administrator`	specified during ESET PROTECT VA configuration	This password is important because it allows you to access ESET PROTECT Web Console.

The default password is changed during ESET PROTECT Virtual Appliance configuration. All the accounts above will have the same password you have specified during ESET PROTECT VA configuration. However, each account can be set with a different password. It is more secure to use different passwords, although it may be intricate when using multiple passwords. You might want to find an effective way of handling multiple passwords for ESET PROTECT VA to prevent confusion.

When you deploy ESET PROTECT VA which is not configured yet, it uses the same password `eraadmin` for all the above accounts until the password is changed during ESET PROTECT Virtual Appliance configuration.

In case of a forgotten password for any of the above accounts, see How to recover a forgotten password for ESET PROTECT VA.

ESET PROTECT VA deployment

Ensure that you have a supported hypervisor.

Select the hypervisor you will use to view deployment instructions:

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

- Oracle VirtualBox
- Citrix

VMware vSphere/ESXi

1. Connect to your vCenter Server using vSphere Client, or directly to ESXi server.

2. If you use the vSphere Client for desktop, click **File** > **Deploy OVF Template**. If you use the vSphere Web Client, click **Actions** > **Deploy OVF Template**.

3. Click **Browse**, navigate to the *protect_appliance.ova* file that you downloaded from the ESET website and then click **Open**.

Unsupported versions of VMware ESXi do not accept SHA-256 certificates. If you see a certificate error when importing the ESET PROTECT VA *.ova* package, you need to delete the *.cert* file from *.ova* and then proceed with the deployment.

4. Click **Next** in the **OVF Template Details** window.

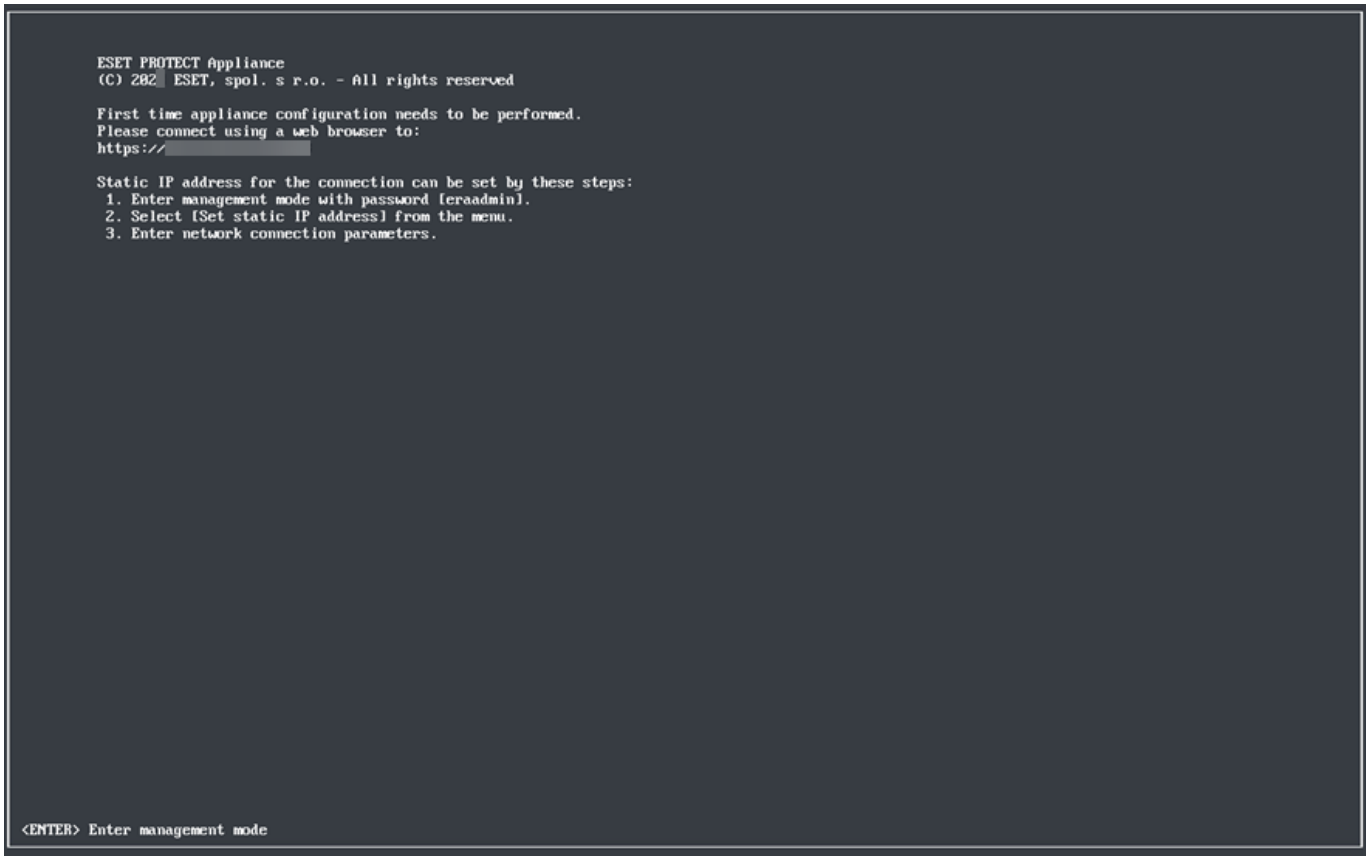
5. Read and accept the End User License Agreement (EULA).

6. Follow the instructions on screen to complete installation and specify the following information about your virtual client:

- **Name and Location**—Specify a name for the deployed template and a location where virtual machine files are stored.
- **Host / Cluster**—Select the host or cluster on which you want to run the template.
- **Resource Pool**—Select the resource pool within which you want to deploy the template.
- **Storage**—Select a location to store virtual machine files.
- **Disk Format**—Select the format that virtual disks will use.
- **Network Mapping**—Select the network for the virtual machine to use. Ensure that you select the virtual machine network associated with the IP pool you created.

7. Click **Next**, review the deployment summary and click **Finish**. The process will automatically create a virtual machine with the settings you specify.

8. When the ESET PROTECT VA is successfully deployed, power it on. The following information will be displayed:

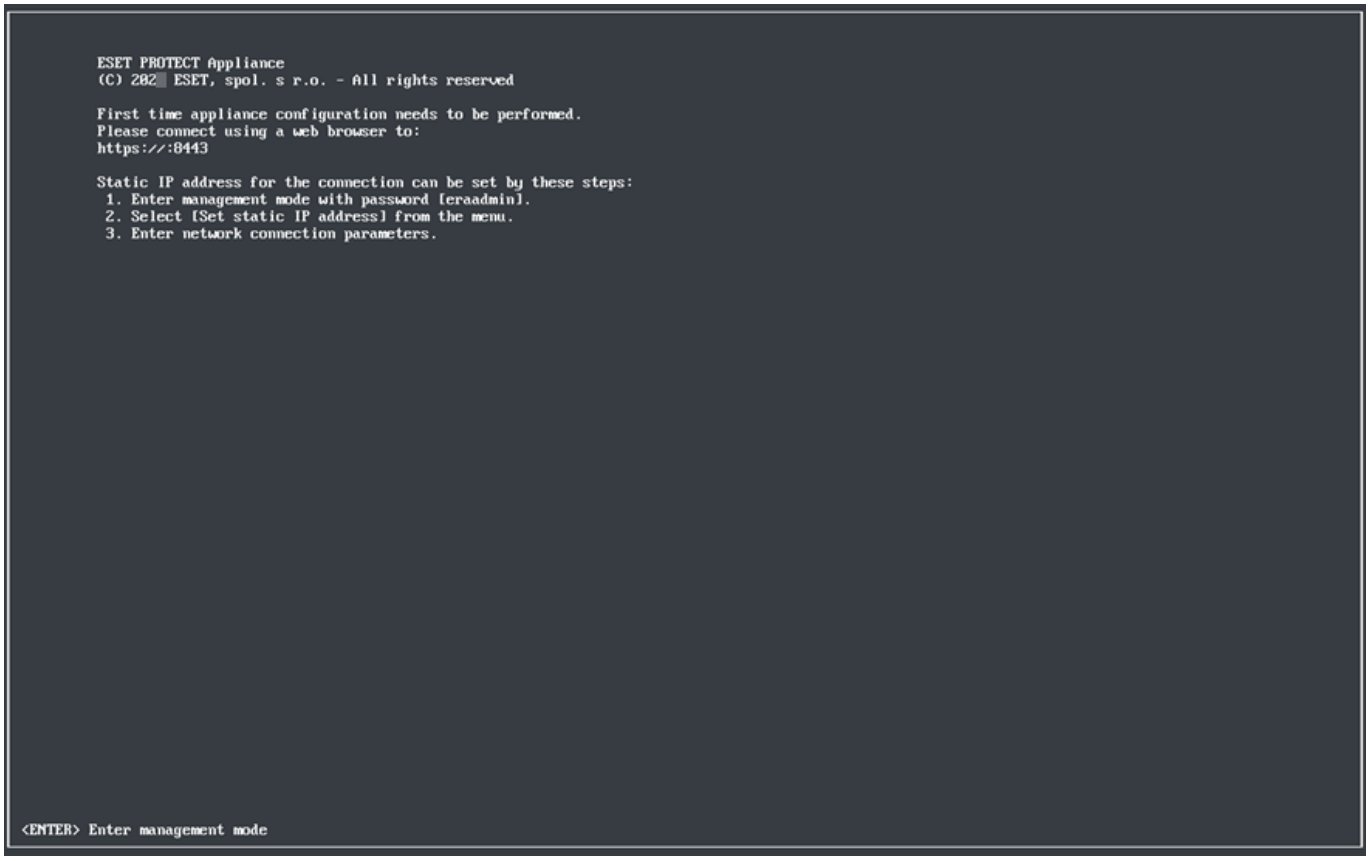


Open your web browser and type the IP address of your newly deployed ESET PROTECT Virtual Appliance in the address bar. You can see the IP address listed in the console window (as shown above). It will say **First time appliance configuration needs to be performed. Please connect using a web browser to:**

- *https://[IP address]* (CentOS)
- *https://[IP address:8443]* (Rocky Linux)

The next step is to configure your appliance via the web interface.

If you do not have a DHCP server in your network, you will need to Set static IP address for the ESET PROTECT VA via Management Console. If there is no IP address assigned, the following information will be displayed; the URL will not contain an IP address.
If no IP address is assigned, the DHCP server may not be able to assign one. Ensure there are free IP addresses in the subnet where the VA is located.



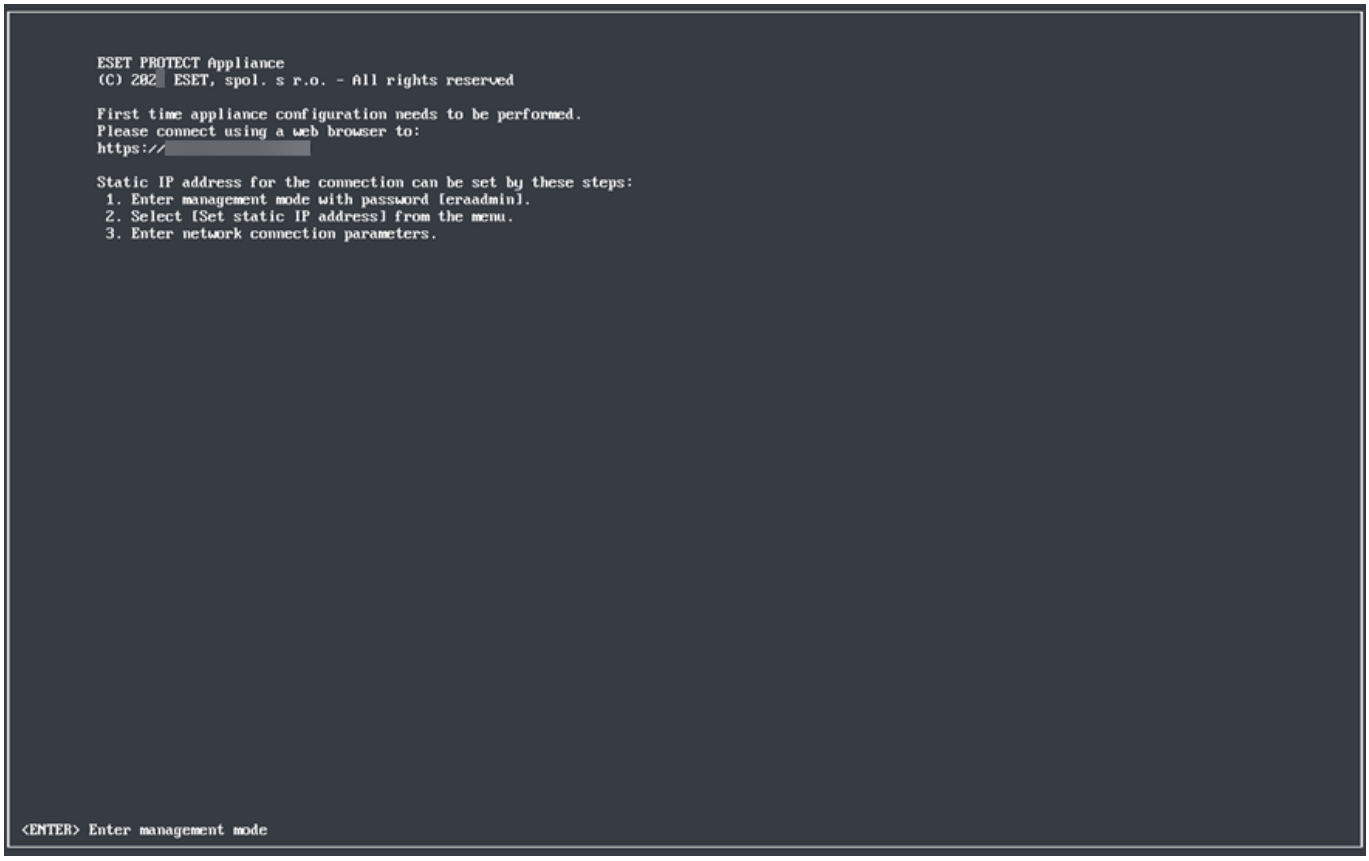
> We highly recommend that you configure vCenter roles and permissions in such a way that VMware users will not be able to access the ESET PROTECT virtual machine. This will prevent users from tampering with the ESET PROTECT VM. There is no need for ESET PROTECT users to access the VM. To manage access to ESET PROTECT On-Prem, use Access Rights in the ESET PROTECT Web Console.

VMware Workstation/Player

We recommend that you use the latest version of VMware Player. Set the connection for the network adapter on your VM to **Bridged** or **NAT**.

> Port forwarding must be configured on your virtual machine for ESET PROTECT On-Prem to be accessible from the network.

1. Select **File** > **Deploy OVF Template**.
2. Navigate to the *protect_appliance.ova* file that you downloaded from the ESET website and click **Open**.
3. Provide a name and local store path for the new virtual machine and click **Import**.
4. Read and accept the End User License Agreement (EULA) if you agree with it.
5. When the ESET PROTECT VA is successfully deployed, power it on. The following information will be displayed:

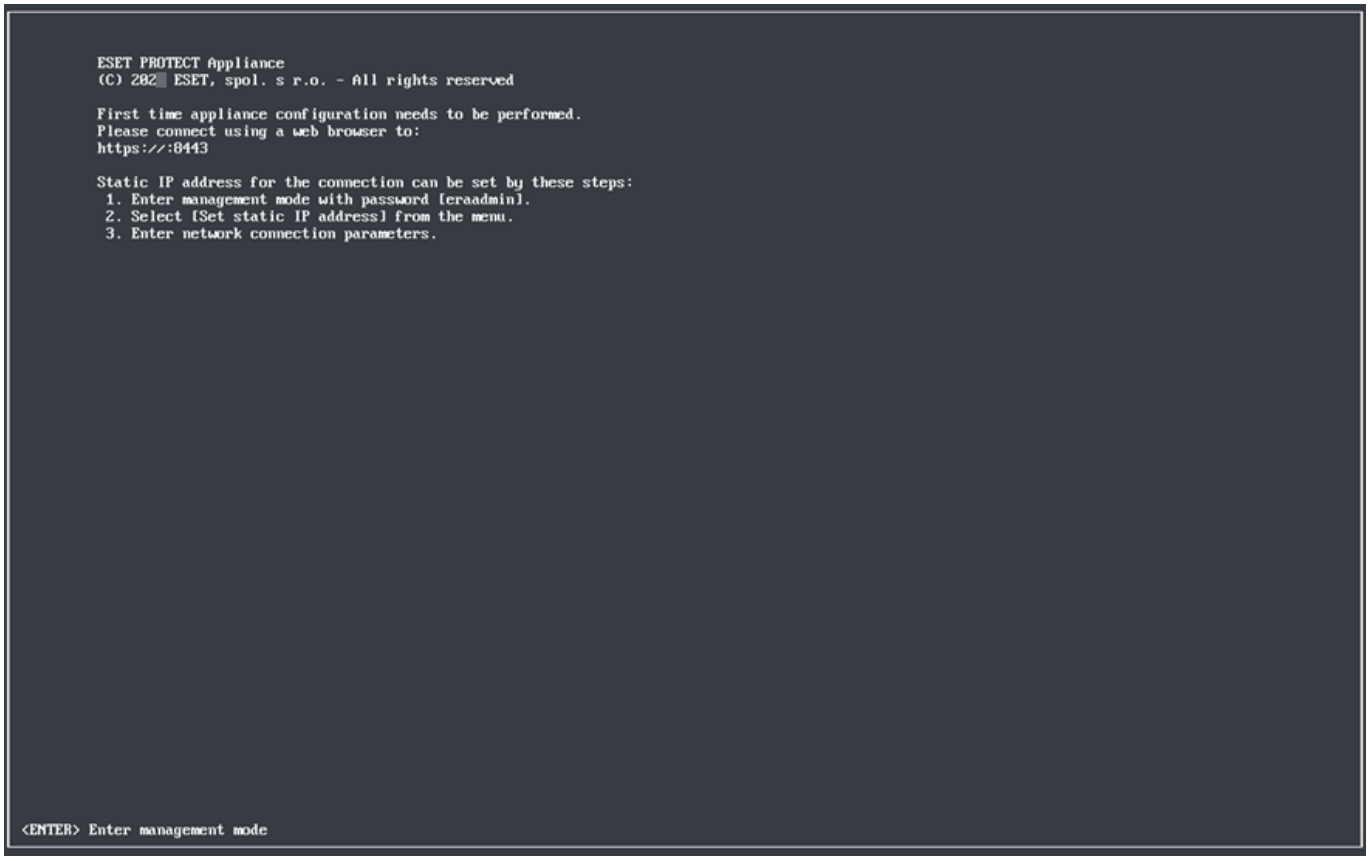


Open your web browser and type the IP address of your newly deployed ESET PROTECT Virtual Appliance in the address bar. You can see the IP address listed in the console window (as shown above). It will say **First time appliance configuration needs to be performed. Please connect using a web browser to:**

- *https://[IP address]* (CentOS)
- *https://[IP address:8443]* (Rocky Linux)

The next step is to configure your appliance via the web interface.

If you do not have a DHCP server in your network, you will need to Set static IP address for the ESET PROTECT VA via Management Console. If there is no IP address assigned, the following information will be displayed; the URL will not contain an IP address.
If no IP address is assigned, the DHCP server may not be able to assign one. Ensure there are free IP addresses in the subnet where the VA is located.



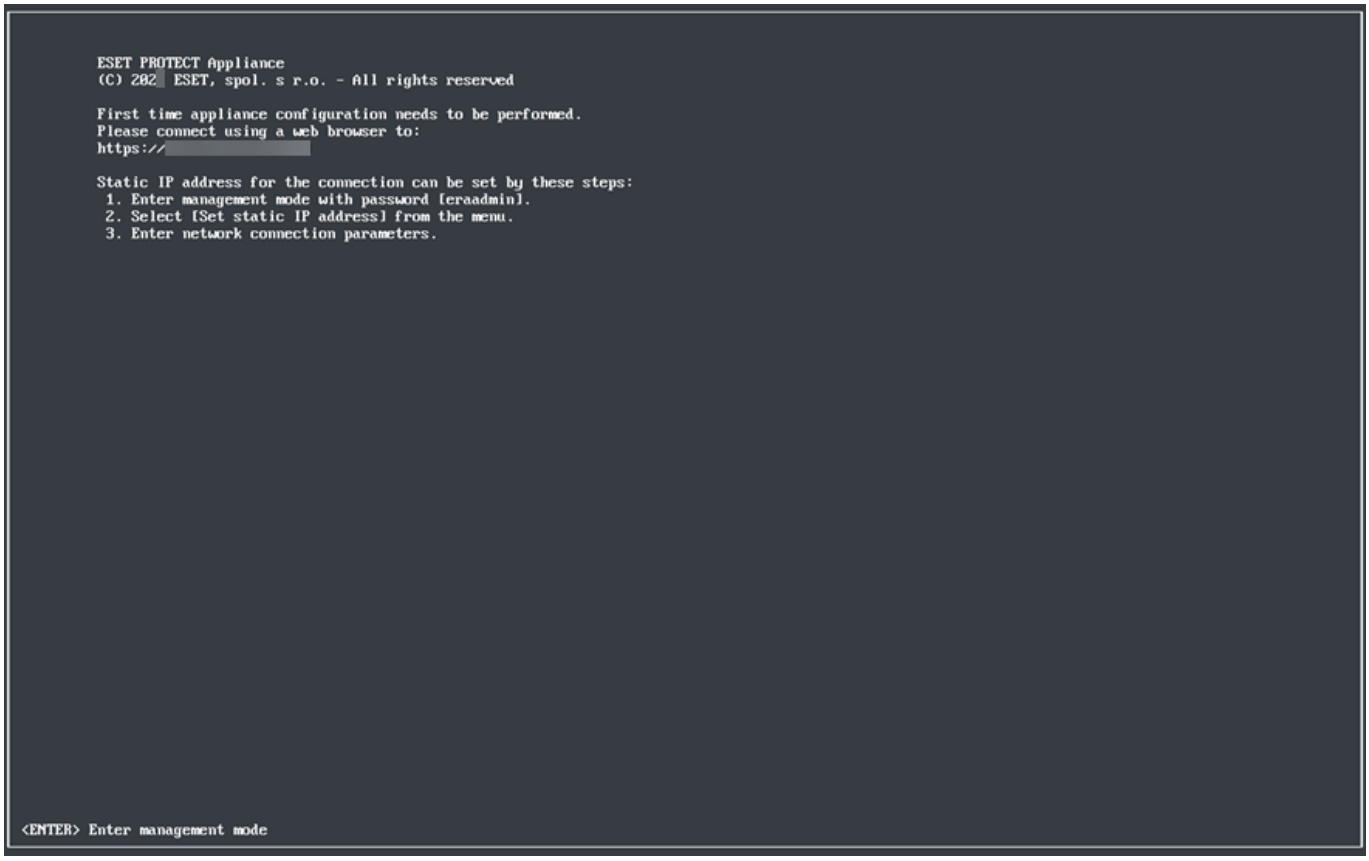
Microsoft Hyper-V

1. Extract the *protect_appliance.vhdx.zip* file (that you downloaded from the ESET website) using a utility such as Tar or 7-Zip.

2. Launch the Hyper-V manager and connect to the appropriate Hyper-V.

3. Create a new virtual machine, (Generation 1) with at least 4 Cores and 4 GB of RAM.

4. When the ESET PROTECT VA is successfully deployed, power it on. The following information will be displayed:

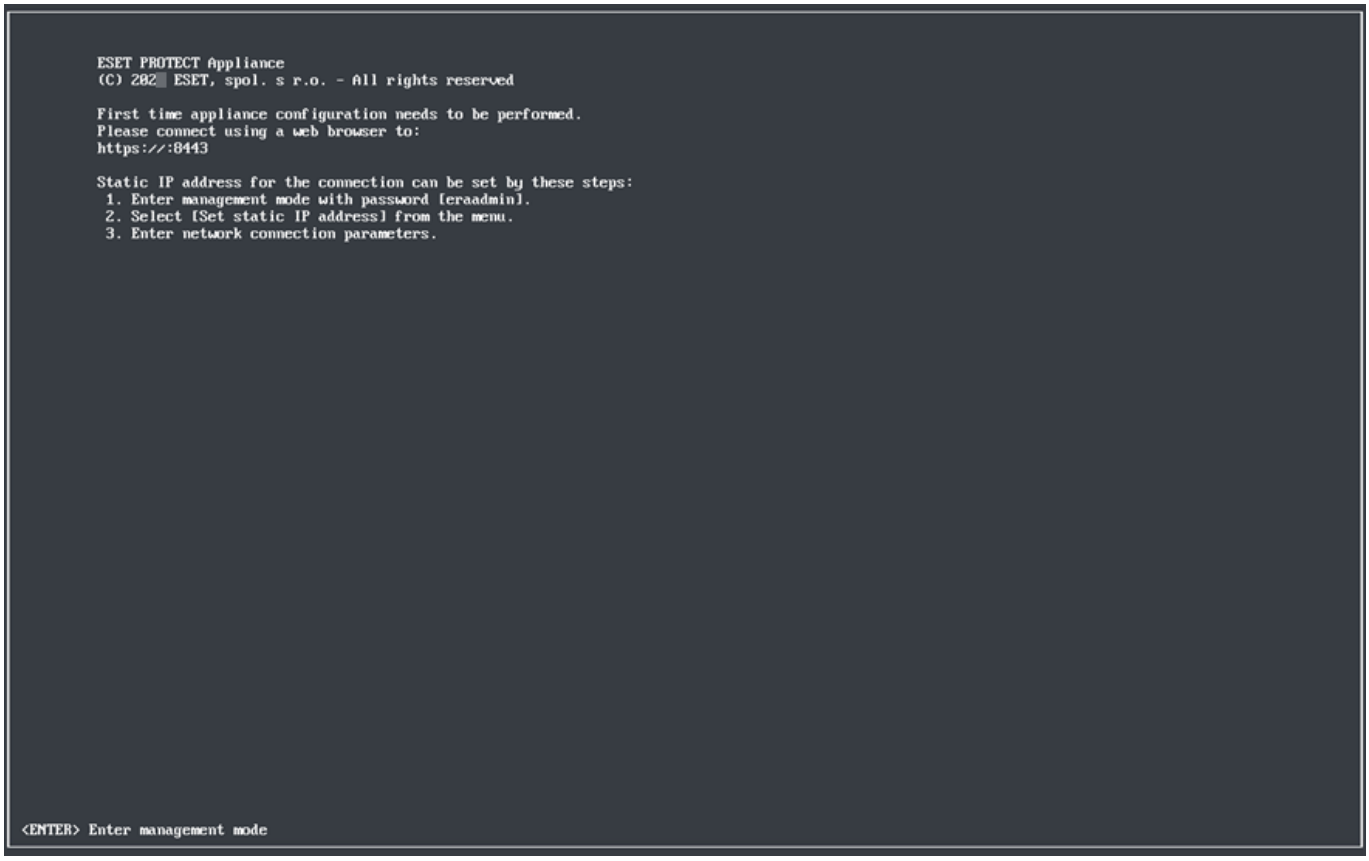


Open your web browser and type the IP address of your newly deployed ESET PROTECT Virtual Appliance in the address bar. You can see the IP address listed in the console window (as shown above). It will say **First time appliance configuration needs to be performed. Please connect using a web browser to:**

- *https://[IP address]* (CentOS)
- *https://[IP address:8443]* (Rocky Linux)

The next step is to configure your appliance via the web interface.

If you do not have a DHCP server in your network, you will need to Set static IP address for the ESET PROTECT VA via Management Console. If there is no IP address assigned, the following information will be displayed; the URL will not contain an IP address.
If no IP address is assigned, the DHCP server may not be able to assign one. Ensure there are free IP addresses in the subnet where the VA is located.



Oracle VirtualBox

We recommend that you use the latest version of VirtualBox. Set the connection for the network adapter on your VM to **Bridged**, or alternatively **NAT**.

> Port forwarding must be configured on your virtual machine for ESET PROTECT On-Prem to be accessible from the internet (if required).

1. Click **File** and select **Import Appliance**.

2. Click **Browse**, navigate to the *protect_appliance.ova* file that you downloaded from the ESET website and click **Open**.

3. Click **Next**.

4. Review your appliance settings and click **Import**.

5. Read and accept the End User License Agreement (EULA) if you agree with it.

6. Adjust the SCSI controller settings:

   a.Right-click the appliance virtual machine and select **Settings**.

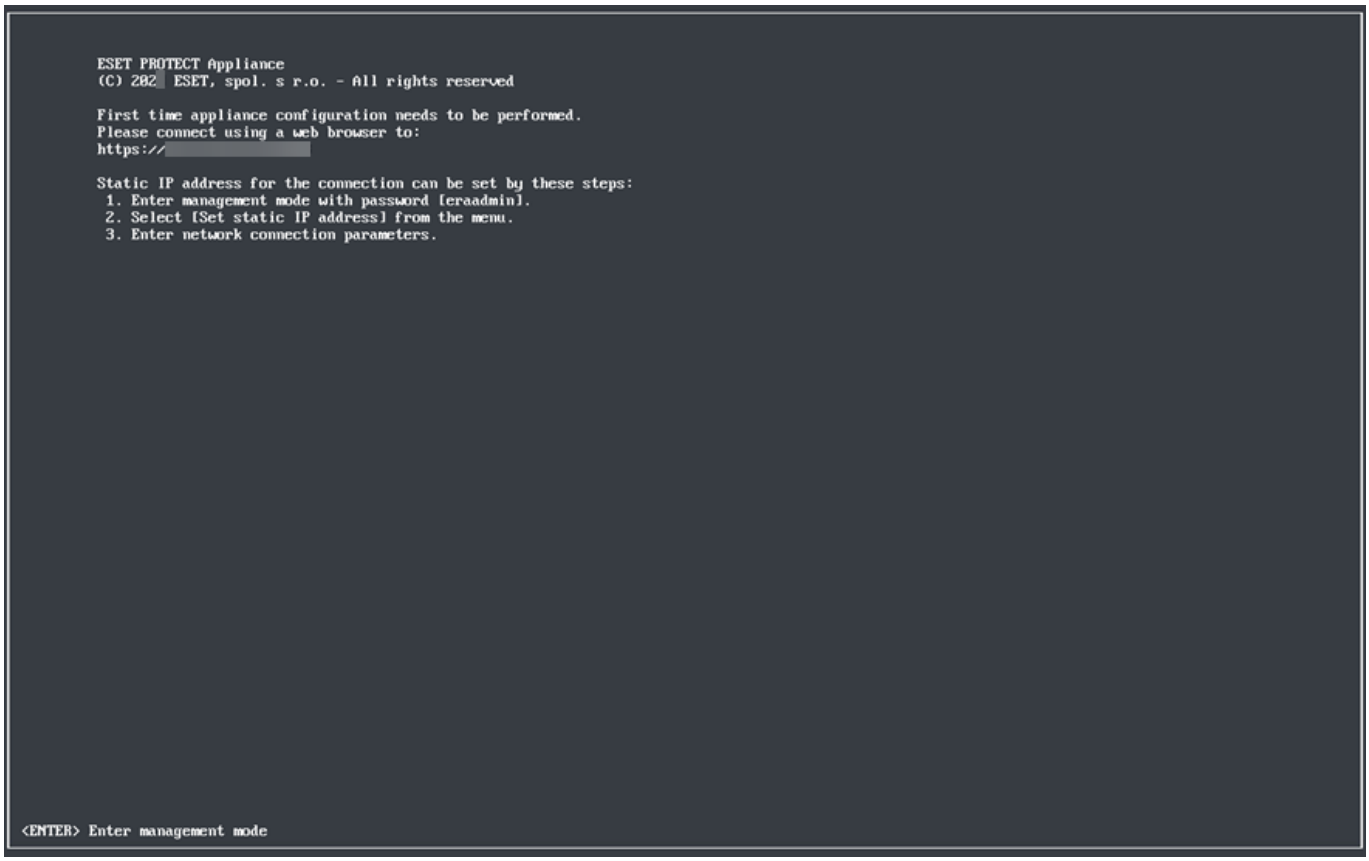
   b.Select **Storage** in the left panel.

   c.Select the **SCSI** controller.

   d.Change the type from **LsiLogic** to **virtio-scsi**.

e.Save the changes.

7. When the ESET PROTECT VA is successfully deployed, power it on. The following information will be displayed:

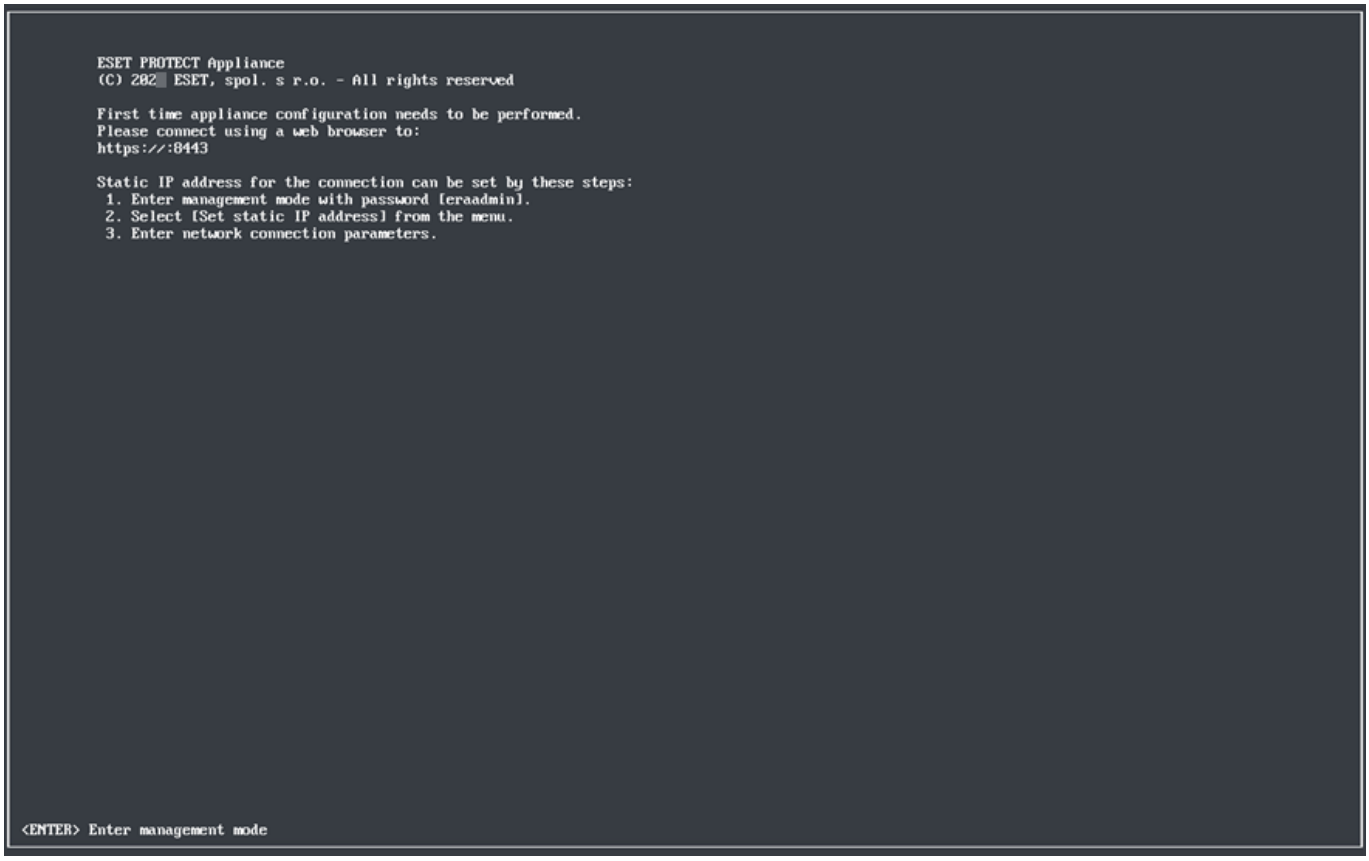


Open your web browser and type the IP address of your newly deployed ESET PROTECT Virtual Appliance in the address bar. You can see the IP address listed in the console window (as shown above). It will say **First time appliance configuration needs to be performed. Please connect using a web browser to:**

- *https://[IP address]* (CentOS)
- *https://[IP address:8443]* (Rocky Linux)

The next step is to configure your appliance via the web interface.

If you do not have a DHCP server in your network, you will need to Set static IP address for the ESET PROTECT VA via Management Console. If there is no IP address assigned, the following information will be displayed; the URL will not contain an IP address.
If no IP address is assigned, the DHCP server may not be able to assign one. Ensure there are free IP addresses in the subnet where the VA is located.



Citrix

Prerequisites

- Your IPv4 network is available in the Citrix environment. IPv6 is not supported in the ESET PROTECT VA.
- The appliance *.ovf* file is available on the machine where you will deploy ESET PROTECT VA.
- Pool Admin Permissions are required to import the *OVF/OVA* package.
- Enough storage space must be available to the deploying user, at least 100 GB.

Deployment process

> You can ignore warnings during the OVF/OVA import—the Virtual Appliance is based on VMware and Citrix XenCenter expects explicit OVF version and different hardware compatibility type.

1. Select **File** > **Import**.

2. Click **Browse**, navigate to the *protect_appliance.ova* file that you downloaded from the ESET website and click **Next**.

3. Select the check box **I accept the End User License Agreements** and click **Next**.

4. Choose the pool or standalone server where you want to place the ESET PROTECT VA and click **Next**.

5. Place the imported virtual disk in a storage repository and click **Next**.

6. Map the virtual network interfaces by selecting the **Target Network** and click **Next**.

7. Choose to verify the digital signature (optional) and click **Next**.

8. Select **Don't use Operating System Fixup** and click **Next**.

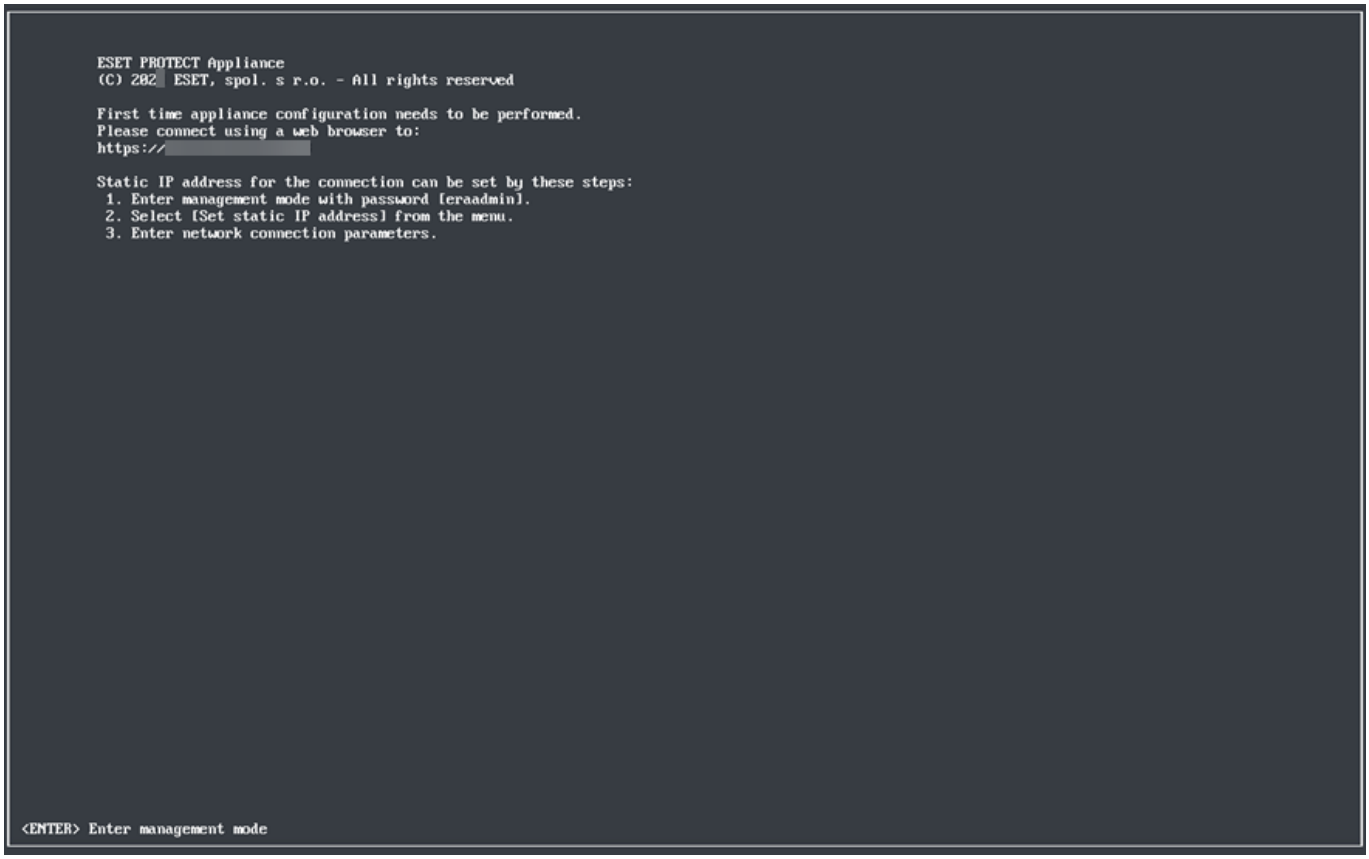
9. Select the network (the same one you selected in step 6 above) where you will install the temporary ESET PROTECT VA used to perform the import operation and click **Next**.

10. Review the settings and click **Finish**.

The deployment process can take some time, during which the Citrix server will appear idle. Do not interrupt it.

> See the vendor's documentation on *OVF/OVA* deployment.

When the ESET PROTECT VA is successfully deployed, power it on. The following information will be displayed:

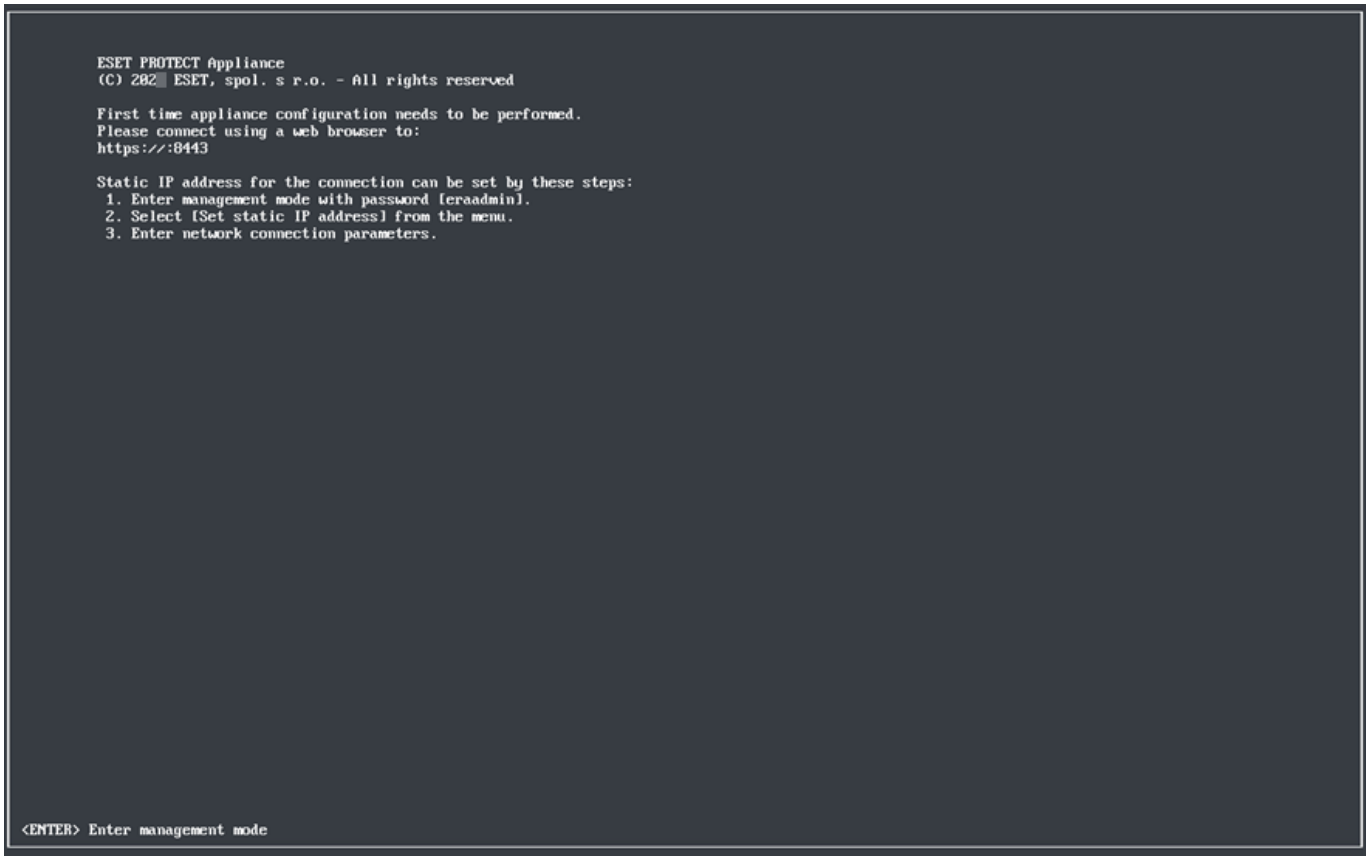


Open your web browser and type the IP address of your newly deployed ESET PROTECT Virtual Appliance in the address bar. You can see the IP address listed in the console window (as shown above). It will say **First time appliance configuration needs to be performed. Please connect using a web browser to:**

- *https://[IP address]* (CentOS)
- *https://[IP address:8443]* (Rocky Linux)

The next step is to configure your appliance via the web interface.

If you do not have a DHCP server in your network, you will need to Set static IP address for the ESET PROTECT VA via Management Console. If there is no IP address assigned, the following information will be displayed; the URL will not contain an IP address.
If no IP address is assigned, the DHCP server may not be able to assign one. Ensure there are free IP addresses in the subnet where the VA is located.



ESET PROTECT VA configuration

The ESET PROTECT Virtual Appliance (ESET PROTECT VA) can easily be configured via its web interface. You will need to have a DHCP server in your network so that your ESET PROTECT VA is automatically assigned an IP address, which in turn allows you to access the ESET PROTECT VA configuration web interface.

If you do not have a DHCP server in your network, you will need to Set static IP address for ESET PROTECT VA.

After you have deployed your ESET PROTECT Virtual Appliance, you can configure it.

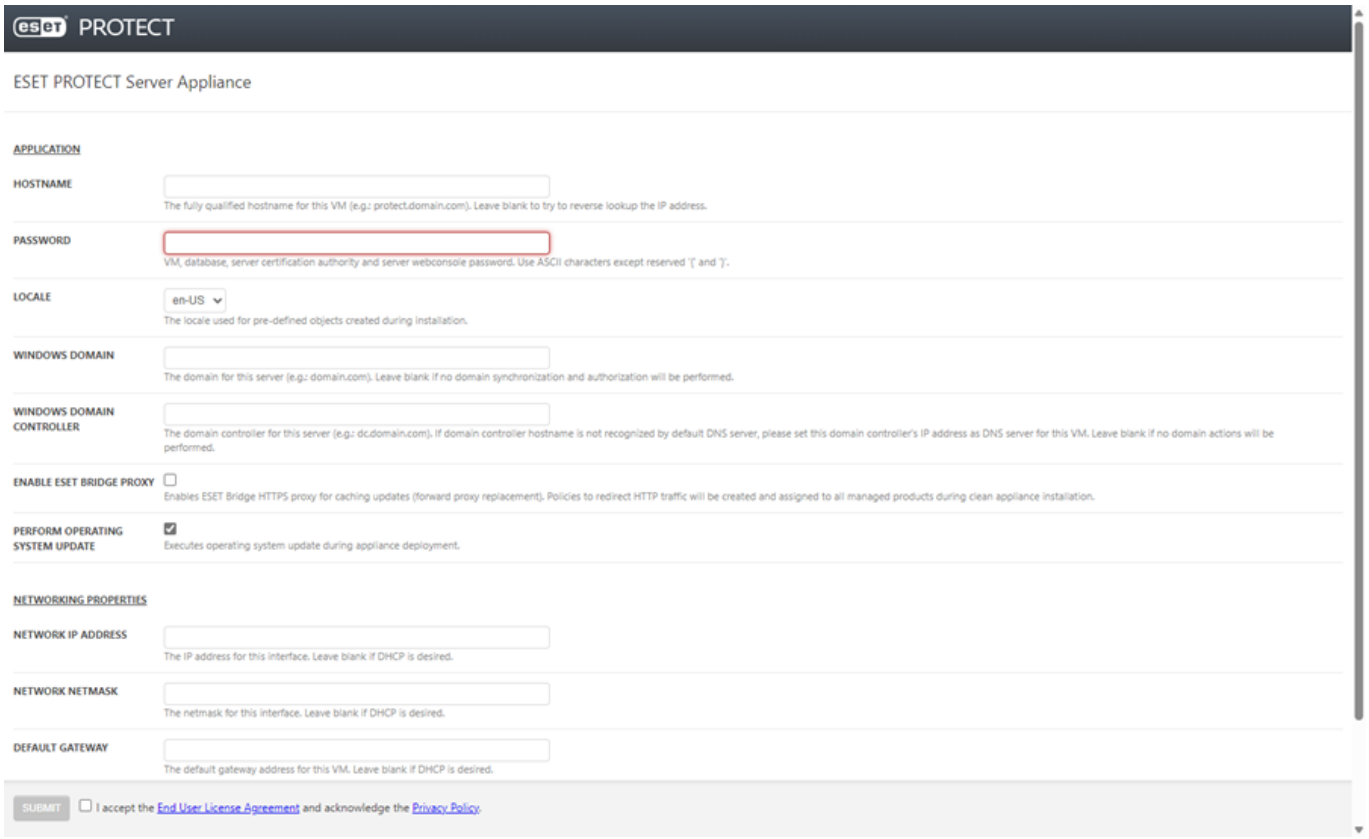
ESET PROTECT On-Prem Mobile Device Management (MDM) reached the End of Life. This feature is no longer available in the latest VA based on Rocky Linux. We recommend that you migrate to the cloud ESET PROTECT with the Cloud MDM.

The configuration page for the ESET PROTECT Server appliance consists of two sections, **Application** and **Networking properties**. Complete all mandatory fields (marked in red). You can specify optional configuration parameters if necessary.

Mandatory configuration fields

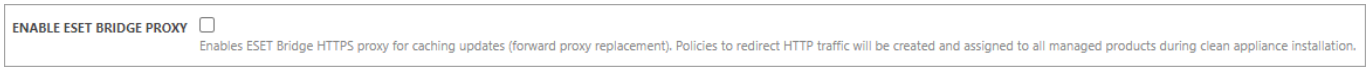
- **Password**—This password is important because it will be used in the VM, ESET PROTECT database, ESET PROTECT Server Certification Authority and ESET PROTECT Web Console.

The default Web Console user is **Administrator**.



Optional configuration fields

Although not mandatory, we recommend that you specify optional parameters. For example, domain details, DC details, domain administrator account credentials, etc. This is useful for domain actions, such as synchronization.



View the image larger

You can also enable ESET Bridge to cache updates. Select the check box next to **Enable ESET Bridge Proxy** to install ESET Bridge, create and apply policies (named **HTTP Proxy usage**, applied on the group **All**) for the following products:

- ESET Endpoint for Windows
- ESET Endpoint for macOS and Linux
- ESET Management Agent
- ESET File Security for Windows Server (6+)

- ESET Server Security for Windows (8+)
- ESET Shared Local Cache

• The policy enables HTTP Proxy for applicable products. Using default settings, the proxy host is set to the ESET PROTECT Server's local IP address on port 3128. Authentication is disabled. You can copy these settings to other policies to set up other products.

• The HTTPS traffic caching is enabled by default:

- The ESET Bridge policy contains the HTTPS certificate, and the **Cache HTTPS Traffic** toggle is enabled.
- The **HTTP Proxy usage** policy for ESET Endpoint for Windows contains the Certificate Authority for the HTTPS traffic caching.

• Using HTTP Proxy can save a lot of bandwidth on data downloaded from internet and improve download speeds for product updates. We recommend that you select the check box next to **Enable ESET Bridge Proxy** if you will manage more than 37 computers from ESET PROTECT On-Prem.

• You can install and configure ESET Bridge later or configure another HTTP Proxy, for example Apache HTTP Proxy.

• **Perform operating system update**—Update the operating system during the Virtual Appliance deployment (enabled by default).

Networking Properties

Scroll down to set the following network properties: **Network IP Address**, **Network Netmask**, **Default Gateway**, **DNS1**, **DNS2**. All fields are optional.

Join ESET PROTECT Virtual Appliance to domain

You can configure the ESET PROTECT VA to run in a domain during initial configuration. The following settings are mandatory to use ESET PROTECT VA on a domain:

> You can configure the domain connection in the ESET PROTECT Web Console > **More** > **Settings** > **Advanced Settings** > Active Directory.

• **Windows workgroup**—A workgroup or NETBIOS domain name for this server, for example DOMAIN. This feature is no longer available in the latest VA based on Rocky Linux.

• **Windows domain**—A domain for this server, for example domain.com.

• **Windows domain controller**—A domain controller for this server. Type the domain controller fully qualified domain name (FQDN).

• **Windows domain administrator**—An account used to join the domain. This feature is no longer available in the latest VA based on Rocky Linux.

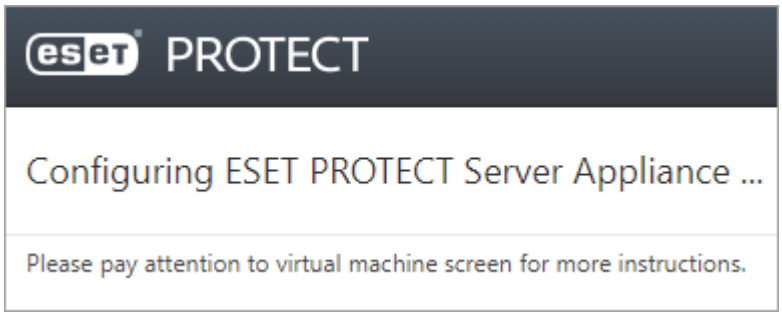
• **Windows domain administrator password**—An administrator password used to join the domain. This feature is no longer available in the latest VA based on Rocky Linux.

- **DNS1**—A domain name server for this virtual machine. Type the IP address of domain controller.

Review the specified configuration parameters. Ensure that the configuration is correct because additional configuration changes cannot be made.

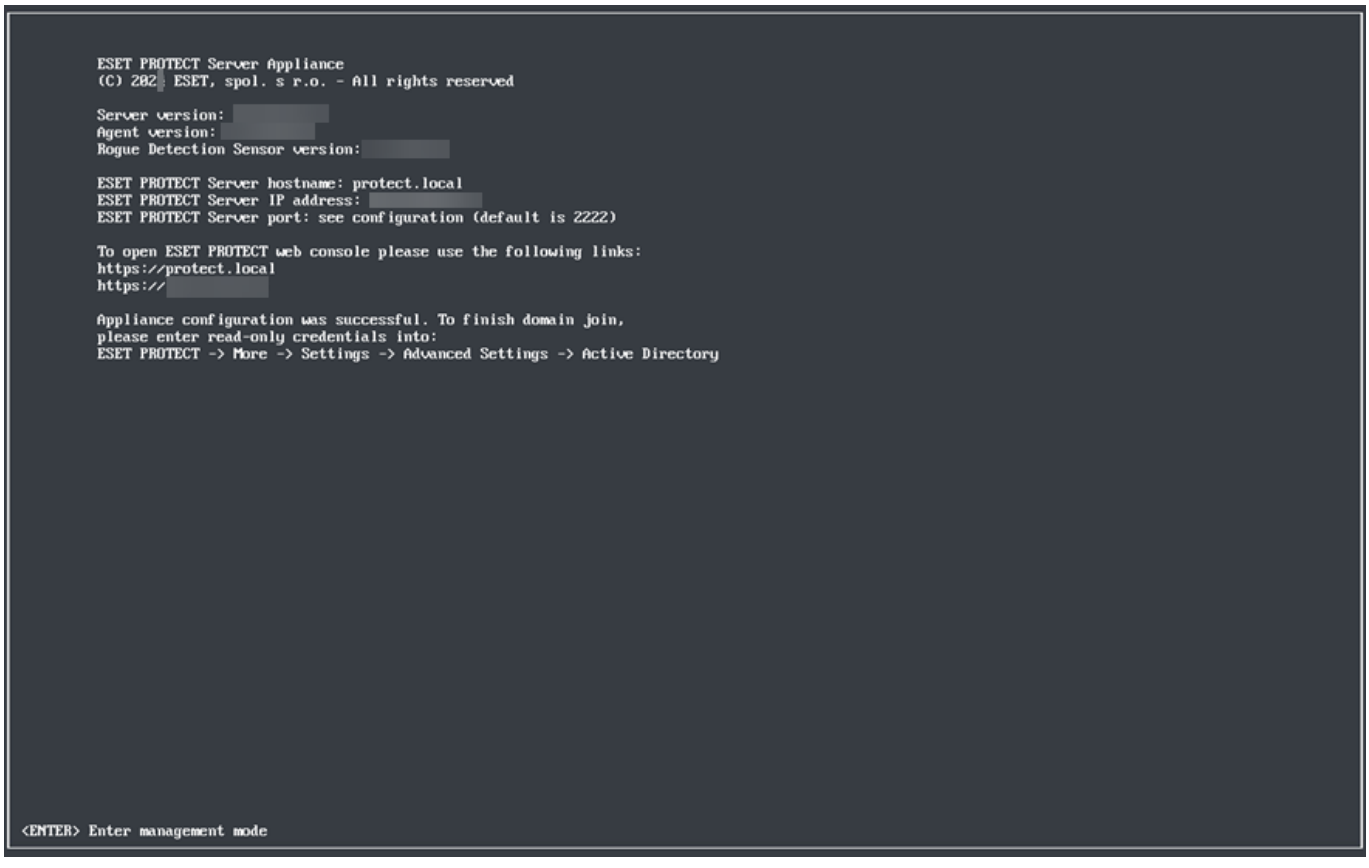
Select the check box **I accept the End User License Agreement and acknowledge the Privacy Policy**. See End User License Agreement (EULA), Terms of Use and Privacy Policy for ESET products.

After you click **Submit**, the following information will be displayed:



Do not refresh this page in your web browser, close the tab and go to your ESET PROTECT VA console window.

Your ESET PROTECT Virtual Appliance console window will display status information. The ESET PROTECT component versions as well as ESET PROTECT Server hostname, IP address and port number will be displayed. The ESET PROTECT Web Console address will also be displayed in the format *https://[hostname] and https://[IP address]*.



We recommend that you create a snapshot or backup Virtual machine before deploying and connecting the first ESET Management Agents.

Type the ESET PROTECT Web Console address (as shown above) in your web browser and log into the ESET PROTECT Web Console. Your hostname and IP address will most likely be different, those shown above are for illustration only. When your are logged in, you can start using ESET PROTECT On-Prem.

After the first login to ESET PROTECT Web Console, we advise that you run the Operating System Update Client Task on the computer where ESET PROTECT On-Prem is installed.

ESET PROTECT MDM Appliance

ESET PROTECT On-Prem Mobile Device Management (MDM) reached the End of Life. This feature is no longer available in the latest VA based on Rocky Linux. We recommend that you migrate to the cloud ESET PROTECT with the Cloud MDM.

This is the configuration page for the ESET PROTECT MDM Appliance. Configuration consists of two sections, **Application** and **Networking properties**. Fill-in all mandatory fields (marked in red). You can specify other optional configuration parameters if necessary.

This ESET PROTECT Virtual Appliance type runs ESET PROTECT MDM on a dedicated VM. Suitable for enterprise-sized networks, but can be also used for small business.

Before you start configuring ESET PROTECT MDM Appliance, create a Mobile Device Connector certificate in the Web Console of ESET PROTECT Server that will be connected to your ESET PROTECT MDM Appliance.

You can configure ESET PROTECT MDM in two ways:

Configuration with Web Console credentials

Mandatory configuration fields for ESET PROTECT MDM Appliance:

- **Password**—This password is important because it will be used in the VM and ESET PROTECT database.
- **ESET PROTECT Server Hostname**—Type in the ESET PROTECT Server hostname or IP address, so that ESET PROTECT MDM can connect to ESET PROTECT Server.
- **ESET PROTECT Server Port**—The default ESET PROTECT Server port is 2222, if you are using a different port, replace the default port with your custom port number.
- **Web Console Port**—The default Web Console port is 2223, if you are using a different port, replace the default port with your custom port number.
- **Web Console password**—This password is important because you need it to access the ESET PROTECT Web Console.
- Optionally, you can type the **Webconsole Hostname**. This hostname is used by Web Console to connect to the server. If you leave the field empty, the value will be automatically copied from **ESET PROTECT Server Hostname**.
- **MDM Hostname**—Type the MDM FQDN or IP address (as specified in the MDC Certificate you created in the ESET PROTECT Web Console).

Configuration with Certificates usage

Mandatory configuration fields for ESET PROTECT MDM Appliance:

- **Password**—This password is important because it will be used in the VM and ESET PROTECT database.
- **ESET PROTECT Server Hostname**—Type in the ESET PROTECT Server hostname or IP address, so that ESET PROTECT MDM can connect to ESET PROTECT Server.
- **ESET PROTECT Server Port**—The default ESET PROTECT Server port is 2222, if you are using a different port, replace the default port with your custom port number.
- **Web Console Port**—The default Web Console port is 2223, if you are using a different port, replace the default port with your custom port number.
- **Certification Authority Base64**—Paste the Certification Authority Certificate in Base64 format (see ESET PROTECT certificates for details on how to obtain the certificate).
- **Proxy Certificate Base64**—Paste Proxy Certificate in Base64 format (see ESET PROTECT certificates for details on how to obtain the certificate). To authenticate communication between ESET PROTECT Server and MDM, a Proxy certificate is used.
- **Agent Certificate Base64**—Paste Agent Certificate in Base64 format (see ESET PROTECT certificates for details on how to obtain the certificate).
- **MDM Hostname**—Type the MDM FQDN or IP address (as specified in the MDC Certificate you created in the ESET PROTECT Web Console).

Networking Properties

Scroll down to set the following network properties: **Network IP Address**, **Network Netmask**, **Default Gateway**, **DNS1**, **DNS2**. All fields are optional.

Review the configuration parameters. Ensure the configuration is correct because additional configuration changes are not possible.

Select the check box **I accept the End User License Agreement and acknowledge the Privacy Policy**. See End User License Agreement (EULA), Terms of Use and Privacy Policy for ESET products.

Click **Submit** when you are finished making changes.

> Do not refresh this page in your web browser, close the tab and go to your ESET PROTECT VA console window.

Your ESET PROTECT Virtual Appliance console window will display its status information. You will find ESET PROTECT component versions as well as ESET PROTECT MDM hostname, IP address and port number. You will also find MDM enrollment address in format *https:///[hostname]:9980 and https:///[IP address]:9980*.

Type displayed MDM enrollment address (as shown above) into your web browser to confirm the Mobile Device Connector is running correctly. Your hostname and IP address will most likely be different, those shown above are

for illustration only. If the deployment was successful, you will see following message: **MDC Server up and running!**

ESET PROTECT VA Management Console

After you have successfully deployed the ESET PROTECT VA, open Virtual Machine's terminal window. You will see a basic information screen of your ESET PROTECT VA and its status. This is the main ESET PROTECT VA screen. From here, you can log into **ESET PROTECT VA Management Console** (also known as **management mode**) by pressing **Enter** key on your keyboard. To enter the management mode, type your password that you specified during ESET PROTECT VA configuration and press **Enter** twice. If you have not configured your ESET PROTECT VA yet, you can use default password `eraadmin` to access management mode.

When you are logged into ESET PROTECT VA Management Console, the following configuration/management items are available:

- Set static IP address
- Enable/Disable remote access
- Backup database
- Restore database
- Reset after snapshot revert
- Pull database from other server
- Change VM password
- Change database password
- Rejoin domain
- Configure domain
- Factory reset

Presence of the items above may vary depending on ESET PROTECT VA implementation phase and configured Appliance type.

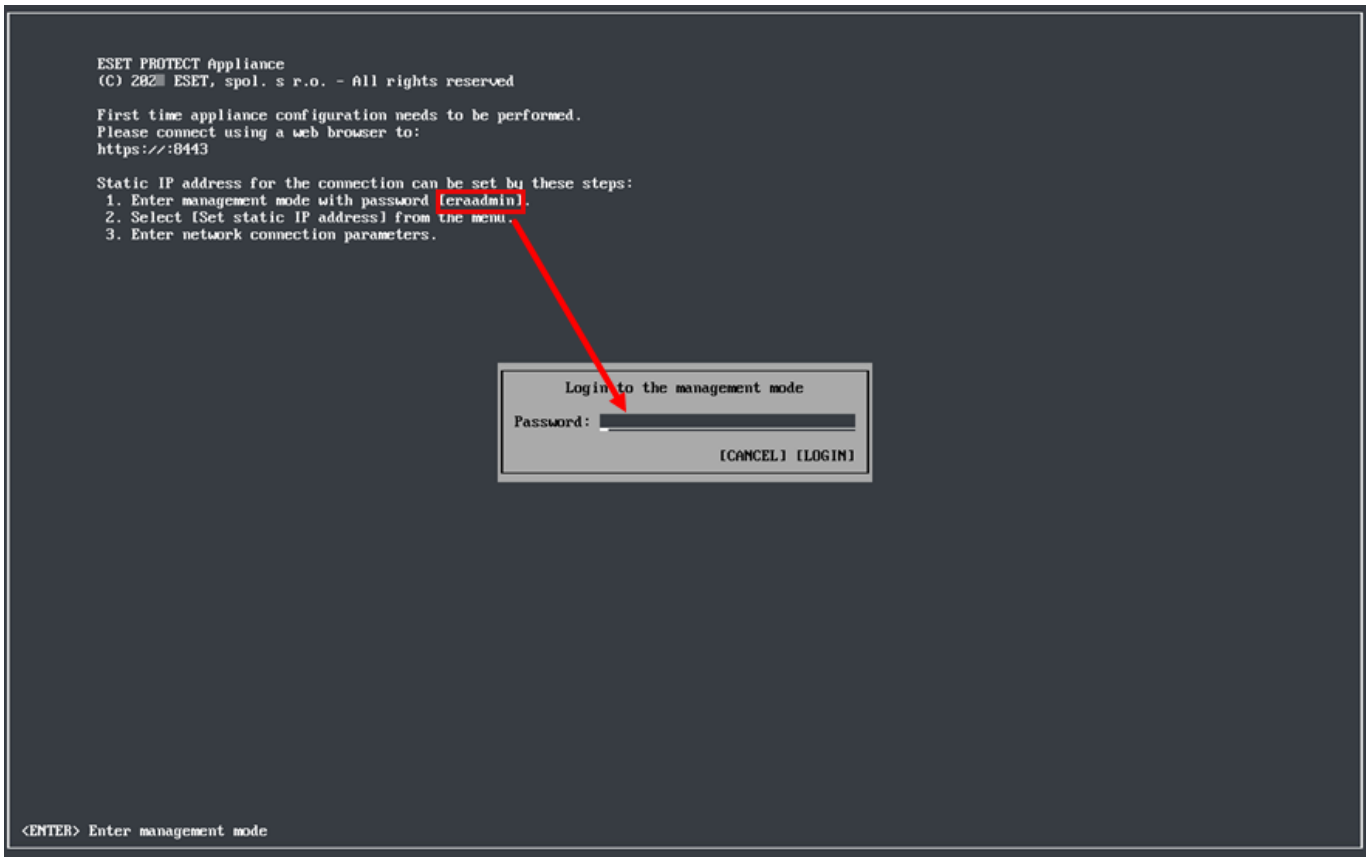
- **Restart system**—Reboot your ESET PROTECT VA.
- **Shut down system**—Shut down your ESET PROTECT VA.
- **Lock screen**—Lock the screen to prevent other people from using your ESET PROTECT VA and accessing its files. You can also use an **Esc** key to lock the screen which is even quicker. The management mode will close and you will see the main ESET PROTECT VA screen.
- **Exit to terminal**—Use it if you want to access operating system's terminal. It closes ESET PROTECT VA Appliance Management Console and enters the terminal. To get from the terminal back to the main ESET

PROTECT VA screen, type `exit` and press **Enter** key (you can also use the `logout` command which has the same effect).

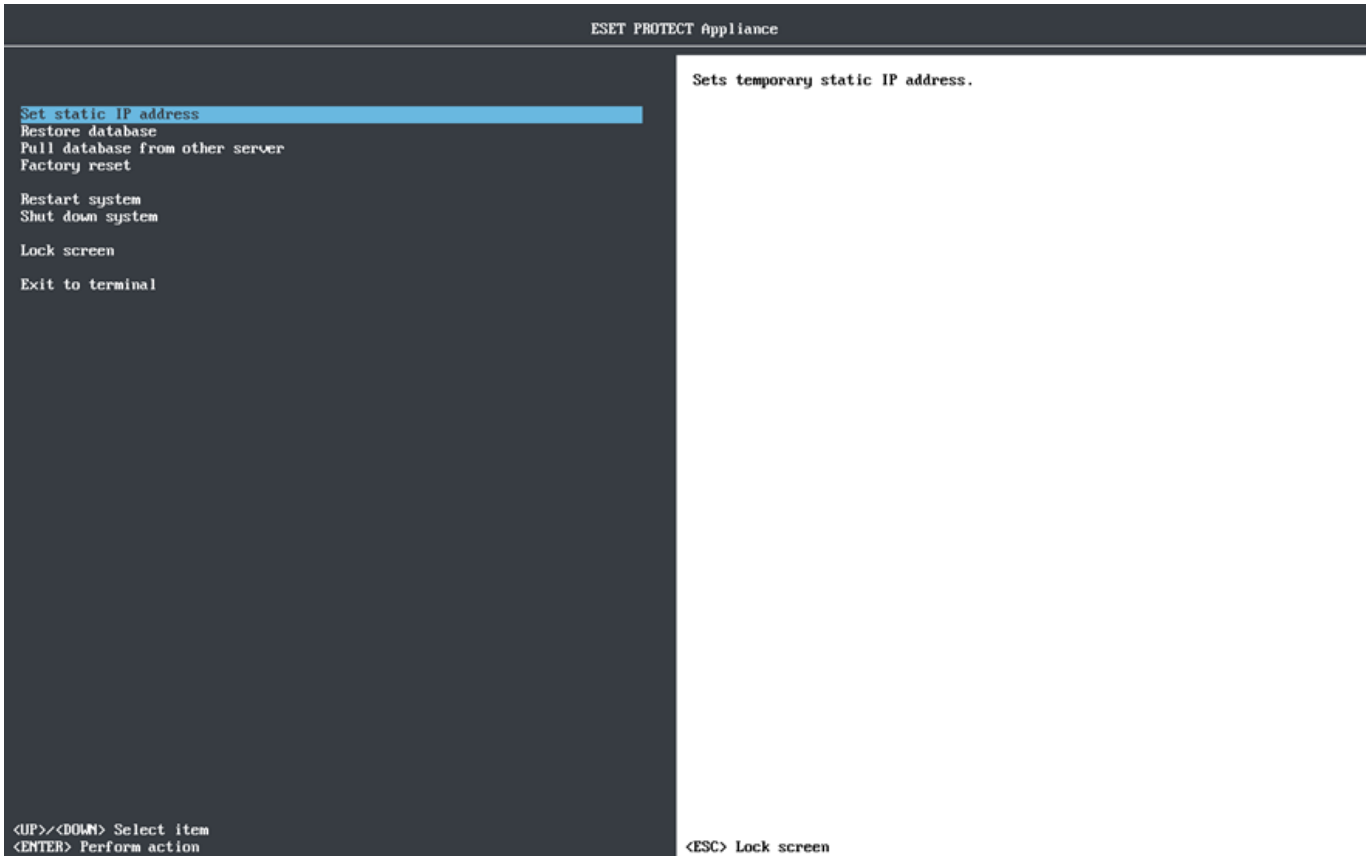
Set static IP address

Manual configuration is required if your ESET PROTECT VA is not assigned an IP address by a DHCP server. Follow the instructions below to set a static IP address manually:

1. While in the VM console main screen, press **Enter** on your keyboard to log in to the management mode. Type `eraadmin` and press **Enter** twice to login.



2. Choose **Set static IP address** using the arrow keys and press **Enter**.



3. A network configuration interactive wizard will start, asking you to set:
   - Static IP address
   - Network mask
   - Gateway address
   - DNS server address

> Network parameters must be typed in IPv4 dot-decimal notation, for example `192.168.1.10` (IP address) or `255.255.255.0` (network mask).
> See also Enable/disable ping on the ESET PROTECT Virtual Appliance.

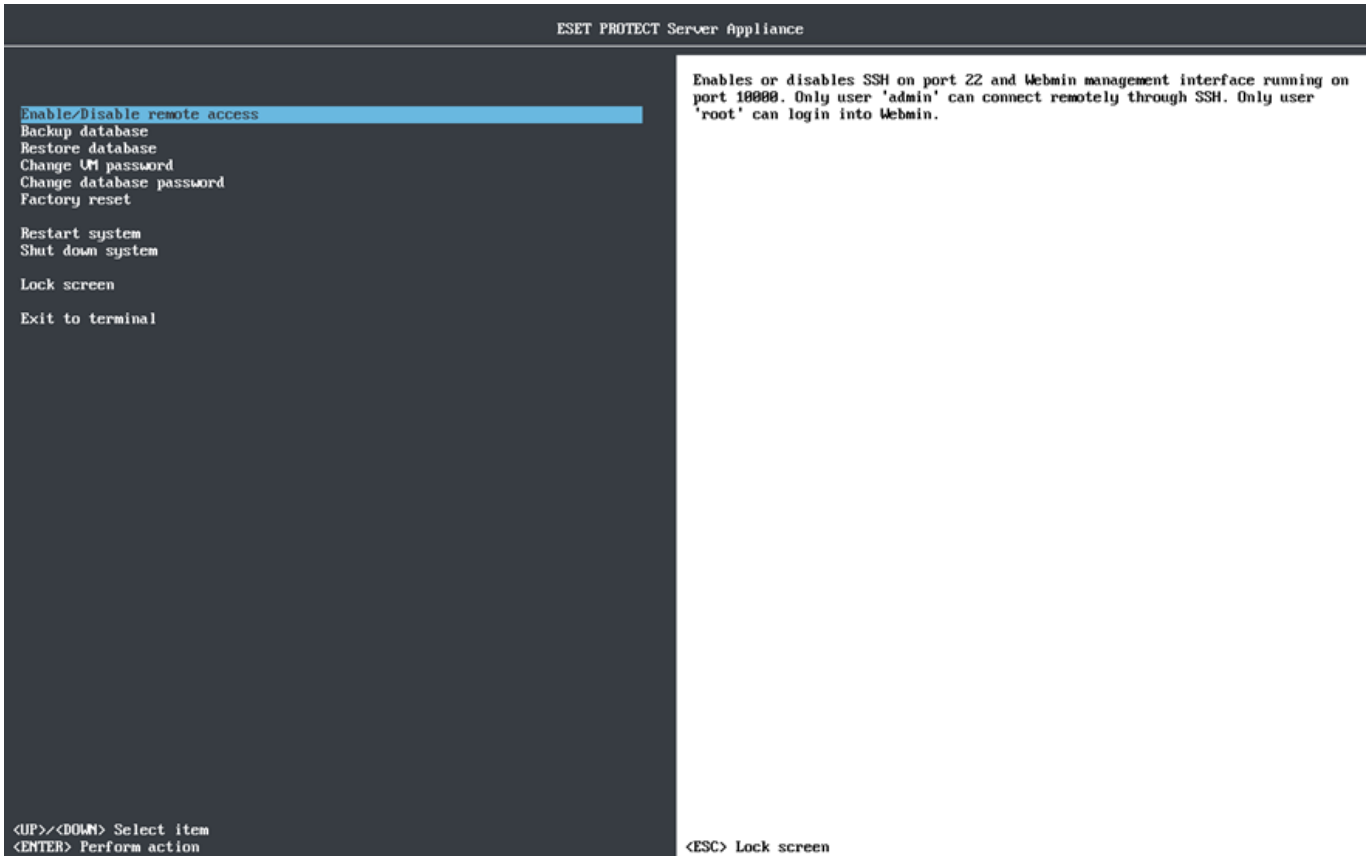
4. Press **Enter** to continue or **Ctrl+C** to stay in terminal.

ESET PROTECT VA has one network adapter by default which is sufficient, but if you add multiple network adapters for other reasons, **Set static IP address** will apply to the `eth0` (CentOS)/`lan0` (Rocky Linux) adapter only.

Enable/Disable remote access

To use remote access (Webmin Management Interface and SSH), you need to enable it first.

Log in to the management mode by typing your password and pressing **Enter** twice. Select **Enable/Disable remote access** using the arrow keys and press **Enter**.



You can now use:

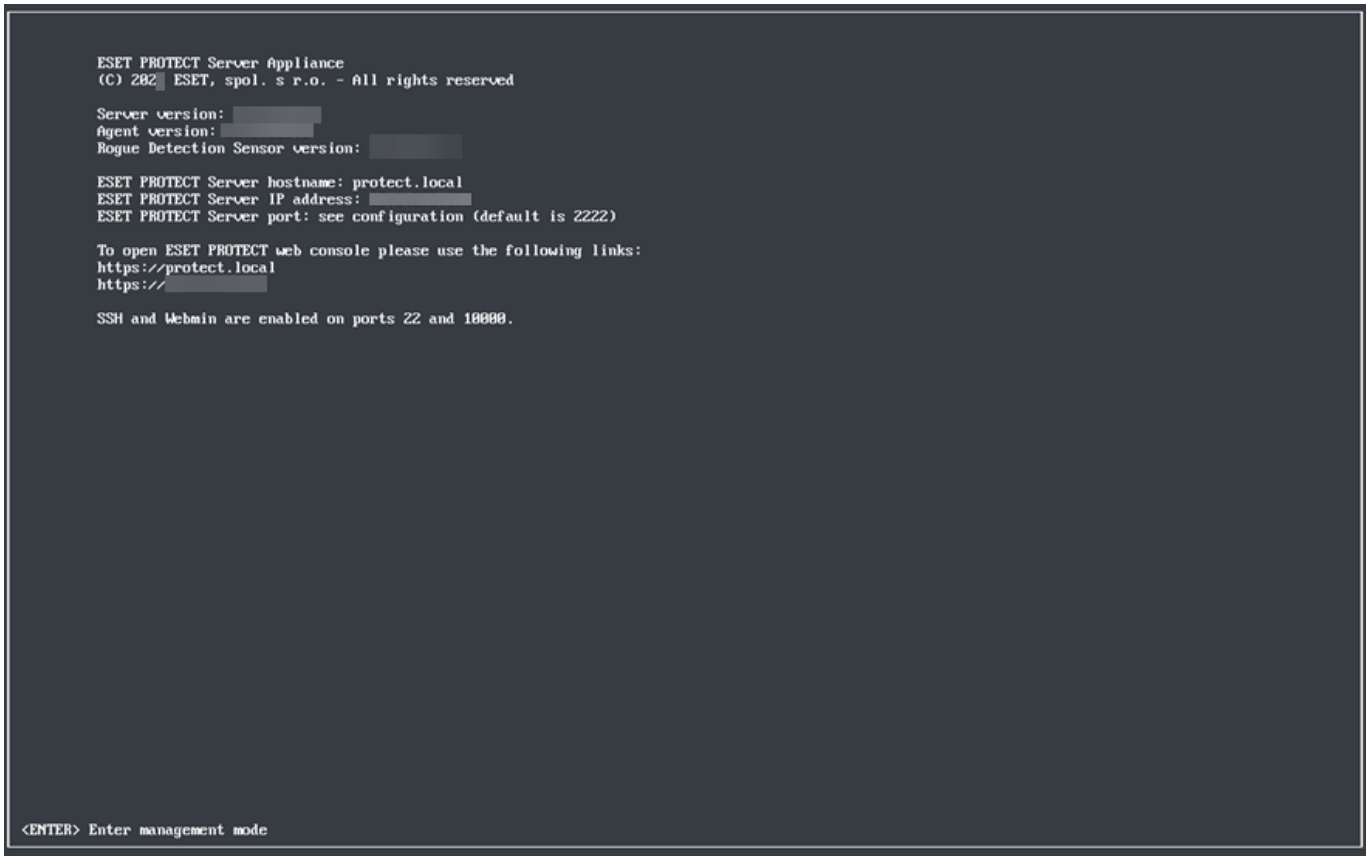
- Webmin—See Webmin Management Interface for details. Webmin uses HTTPS and runs on port 10000. To access the Webmin interface, use the IP address listed along with the port number 10000 (*https://<host name or IP address>:10000* for example *https://10.20.30.40:10000* or *https://protect.local:10000*). When disabled, Webmin is still running and only access to it is blocked in the firewall.

- Remote access over SSH on port 22 (this is required to enable database pull).

User permissions

- The earlier Virtual Appliance based on CentOS: Use the user `root` for remote connection via SSH and for Webmin login.
- The latest Virtual Appliance based on Rocky Linux (read more):
  - Only the user `admin` can connect remotely via SSH.
  - Only the user `root` can log into Webmin.

The following information will be displayed on the main ESET PROTECT VA Management Console screen:



See also SSH troubleshooting.

Backup database

Backup is an absolutely vital part of a sound disaster recovery strategy. Using the **Backup database** feature, you will get your **ESET PROTECT database** backed up and stored in MySQL backup file.

Alternatively, you can back up the database manually.

We recommend that you back up your ESET PROTECT database frequently and save the backup file on an external storage. This is important because you will have a copy of the whole ESET PROTECT database stored elsewhere (not locally on your ESET PROTECT VA), should a disaster happen. For example if your ESET PROTECT VA gets broken, deleted or otherwise destroyed. Having a recent ESET PROTECT database backup, you will be able to restore ESET PROTECT VA to the state it was in shortly before the disaster. For detailed procedure see ESET PROTECT VA disaster recovery.

1. Log in to the management mode by typing your password and pressing **Enter** twice. Select **Backup database** using the arrow keys and then press **Enter**.

2. Type your database root password to start the database backup.

If you do not remember database root password, you can change it and run the database backup again.

```
Backing up database ...
Enter database root password.
Enter password:

Database backup finished. Review any errors and then press Enter to continue.
```

This process can take anywhere from a few seconds to a few hours depending on the size of your database. During the database backup process, ESET PROTECT Server stops to ensure data consistency.

Always check the screen for errors. If there are error messages, the database backup cannot be considered successfully completed. Try running **Backup database** again.

You will find the database backup here:

- CentOS: */root/era-backup.sql*
- Rocky Linux: */opt/appliance/conf/db-backup.sql*

Download the backup file using Webmin File manager to a safe location.

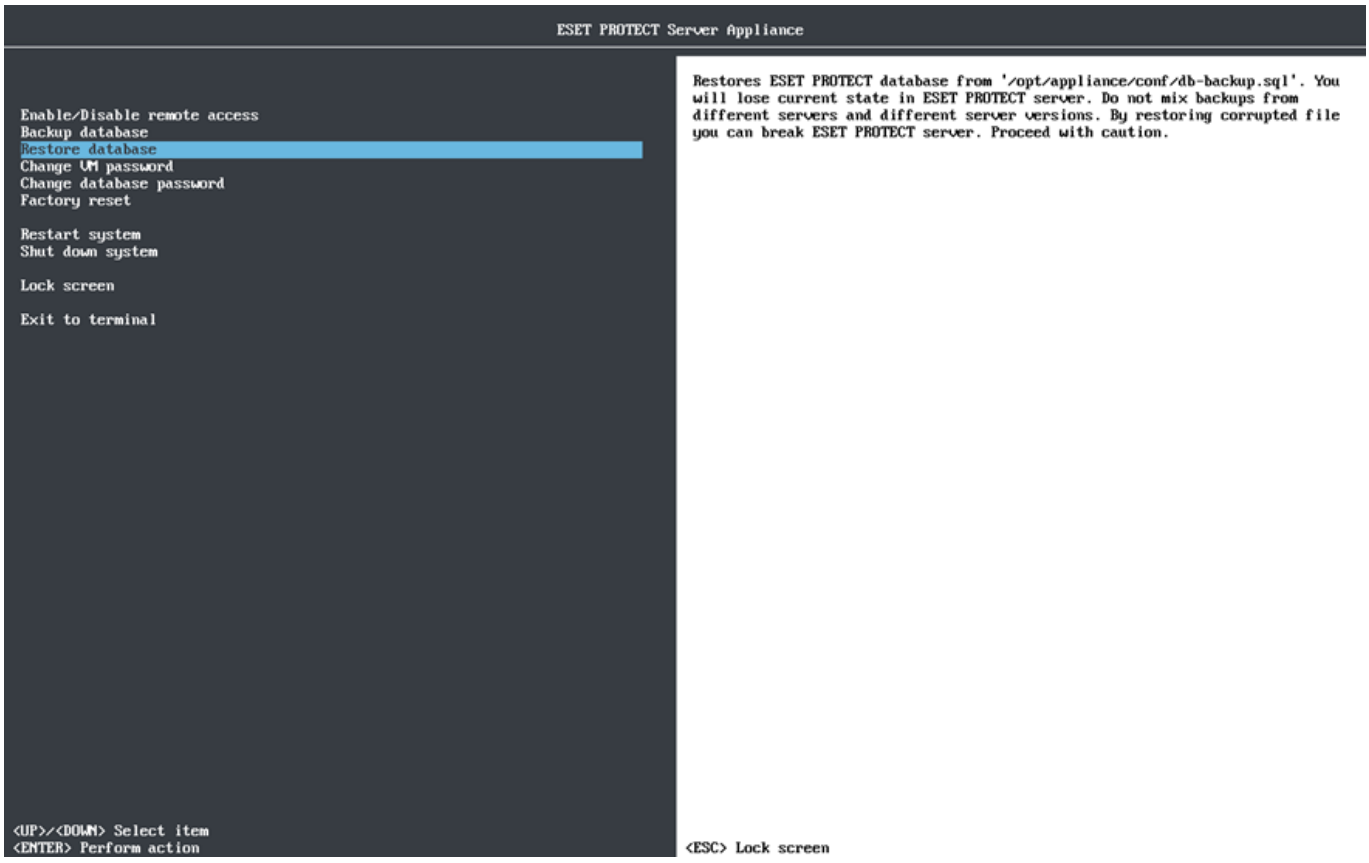
Restore database

This feature will replace your current database with a database from the backup.

We recommend that you have a snapshot of the VM, or a backup of the current database. This is a fallback if you experience issues during restore.

Follow these instructions below to restore the database:

1. Log in to the management mode by typing your password and pressing **Enter** twice. Select **Restore database** using the arrow keys and then press **Enter**.



Upload the backup file you want to restore to the following directory using Webmin File manager:
- CentOS: */root*
- Rocky Linux: */opt/appliance/conf*

The target file will be overwritten. Skip this step if you want to restore the backup file that is already in the same location.

Do not mix backups from different servers and different server versions. Use only the file that was backed up on this same ESET PROTECT VA. You can restore database to a different ESET PROTECT VA, only if it has been freshly deployed and before its configuration.

2. You will be prompted to **Enter database root password** at the beginning of database restore process. If you are restoring database on a freshly deployed ESET PROTECT VA which has not been configured yet, you will not be prompted to type the password.

```
Restoring database ...
Enter database root password:

Restoring of database backup is finished. Review any errors and then press Enter to continue.
```

This process can take from a few seconds to a few hours depending on the size of your database.

Always check the screen for errors. If there are error messages, the database restore cannot be considered successfully completed. Try running **Restore database** again.

Reset after snapshot revert

This feature is no longer available in the latest VA based on Rocky Linux. Use Backup database instead.

An alternative to database backup is to create snapshots of the VM. It will preserve whole ESET PROTECT VA, all its settings as well as ESET PROTECT database.

If you restore a snapshot of your VM to an earlier state, you need to run **Reset after snapshot revert** feature to force all connecting clients to synchronize their statutes with this server.

1. Log in to the management mode by typing your password and pressing **Enter** twice. Select **Reset after snapshot revert** using the arrow keys and press **Enter**.

2. You will be prompted to type in your database root password before the **ESET PROTECT Server realm** is reset.

Pull database from other server

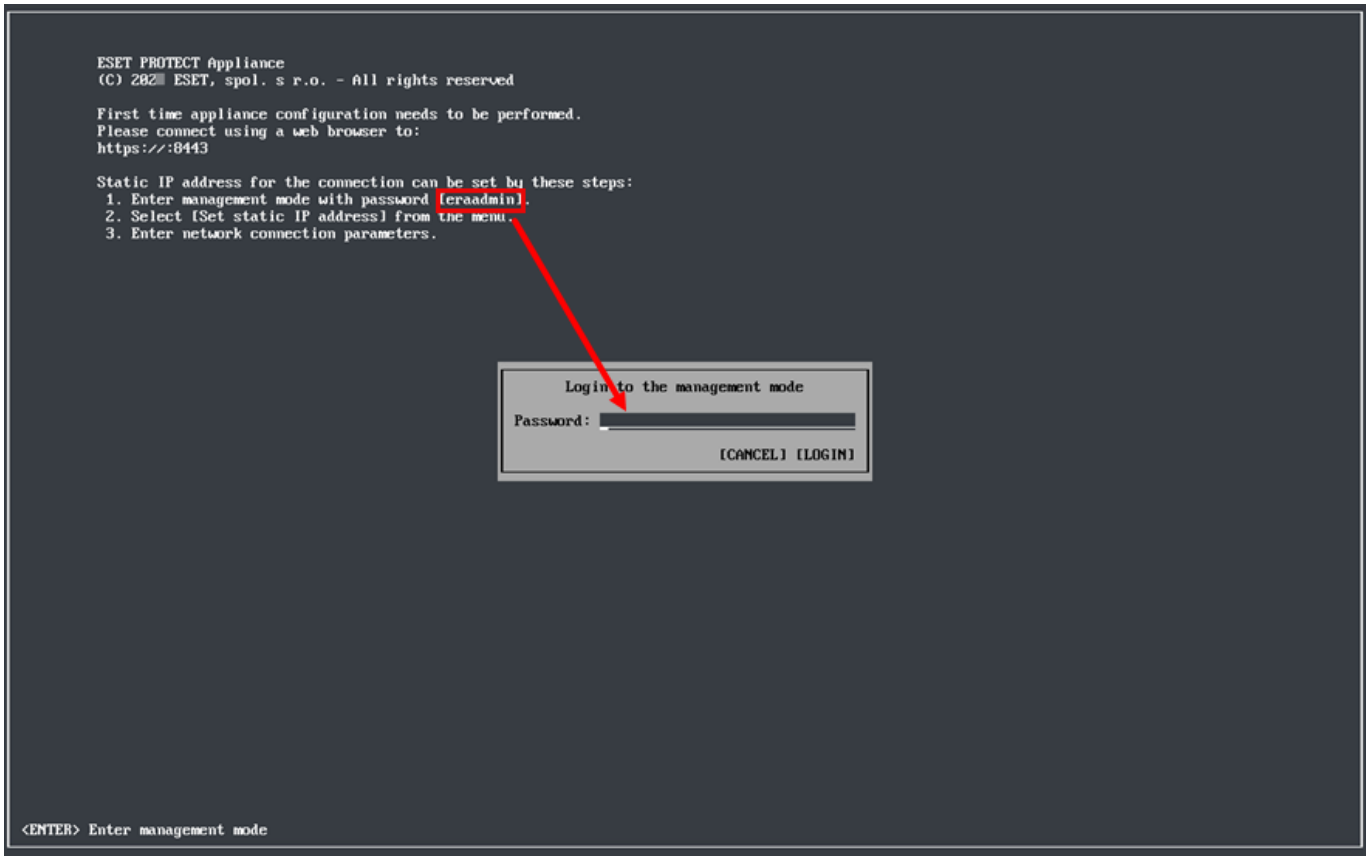
This feature enables you to pull the ESET PROTECT database from an existing ESET PROTECT VA running in your infrastructure. It is only supported on the ESET PROTECT Server, not on the other components (MDM). It is convenient when upgrading your earlier ESET PROTECT VA to the latest ESET PROTECT VA or if you want to migrate your ESET PROTECT VA.

In a migration scenario, you must keep your old ESET PROTECT VA accessible to apply the hostname/IP address change policy to all client computers. Otherwise, clients will not connect to your new ESET PROTECT VA and keep trying to connect to the old one.
Ensure to enable SSH on your old ESET PROTECT VA.
Perform a database pull only when migrating to a later version or the same version of ESET PROTECT Server. The database structure gets updated during the procedure, but this process will fail when pulling to an earlier server. Database pull is one of two ways how to upgrade your VA.

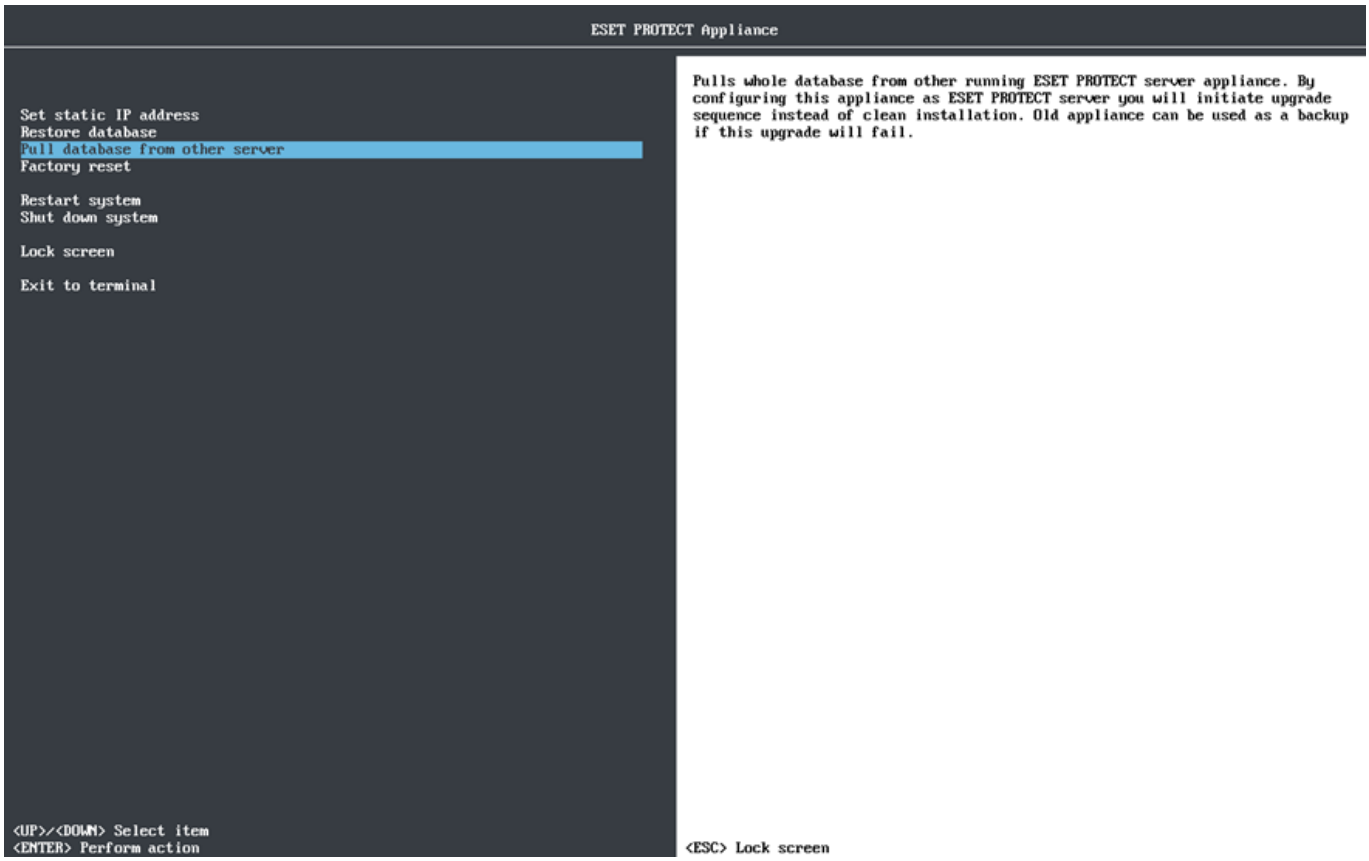
To perform a database pull, follow the steps below:

1. Deploy a new ESET PROTECT VA, but do not configure it.

2. Open the VM's console. The default password is `eraadmin`. Log in to the management mode by typing your password and pressing **Enter** twice.



3. Select **Pull database from other server** using the arrow keys and press **Enter**.



4. Type the database root password on the remote ESET PROTECT VA you want to pull the ESET PROTECT database from (your old ESET PROTECT VA). If you only use one password on your old ESET PROTECT VA, type it here.

5. Connect to the remote ESET PROTECT VA via SSH—Type the username and your old ESET PROTECT VA hostname or IP address in the following format:

- CentOS 7 (when migrating the VA from CentOS to Rocky Linux): `root@IPaddress` or `root@hostname`
- Rocky Linux 9.3 (when migrating VA from Rocky Linux to another Rocky Linux): `admin@IPaddress` or `admin@hostname`

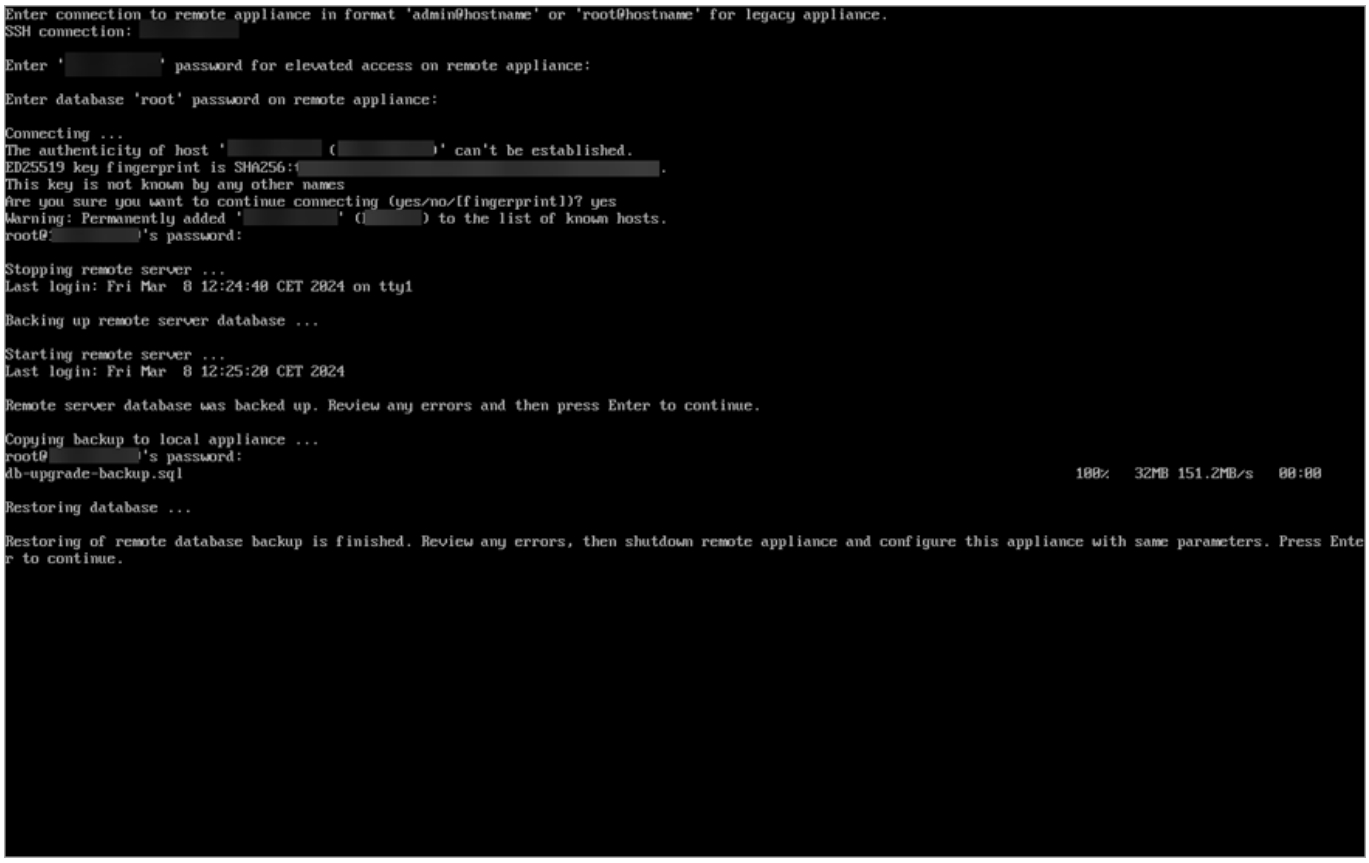
6. If you are asked about **The authenticity of host**, type `yes`. Otherwise, ignore this step.

7. Type the VM password of your old ESET PROTECT VA and press **Enter**. The message **Remote Server database was backed up** will be displayed when backup operations are complete.

The time needed for backup and restore operations to complete will vary depending on database size.

8. Type the VM password of your old ESET PROTECT VA again. You might be asked to type the password multiple times during copying, depending on the time it takes to copy the database.

9. Wait until the database is restored.



10. If you are performing an upgrade: After a successful ESET PROTECT database pull, shut down the old ESET PROTECT VA to decommission it.

- We recommend that you keep your old ESET PROTECT VA long enough before you verify that the new VA is functioning correctly.
- We strongly recommend that you do not uninstall the old ESET PROTECT VA Server using an uninstallation script. This uninstallation procedure will dissociate (remove) all licenses from the new ESET PROTECT VA Server database as well. To prevent this behavior, delete the old ESET PROTECT VA Server database (`DROP DATABASE`) before the uninstallation.

11. Configure your new appliance:

- **Upgrade**—Configure your new VA like your previous ESET PROTECT VA.
- **Migration**—Change the configuration to suit a new domain (configure or rejoin domain) or network properties, for example if you have moved your ESET PROTECT VA to a different network.

Ensure all data is preserved, all clients are connecting to your new server and your ESET PROTECT VA behaves the same way as the previous one.

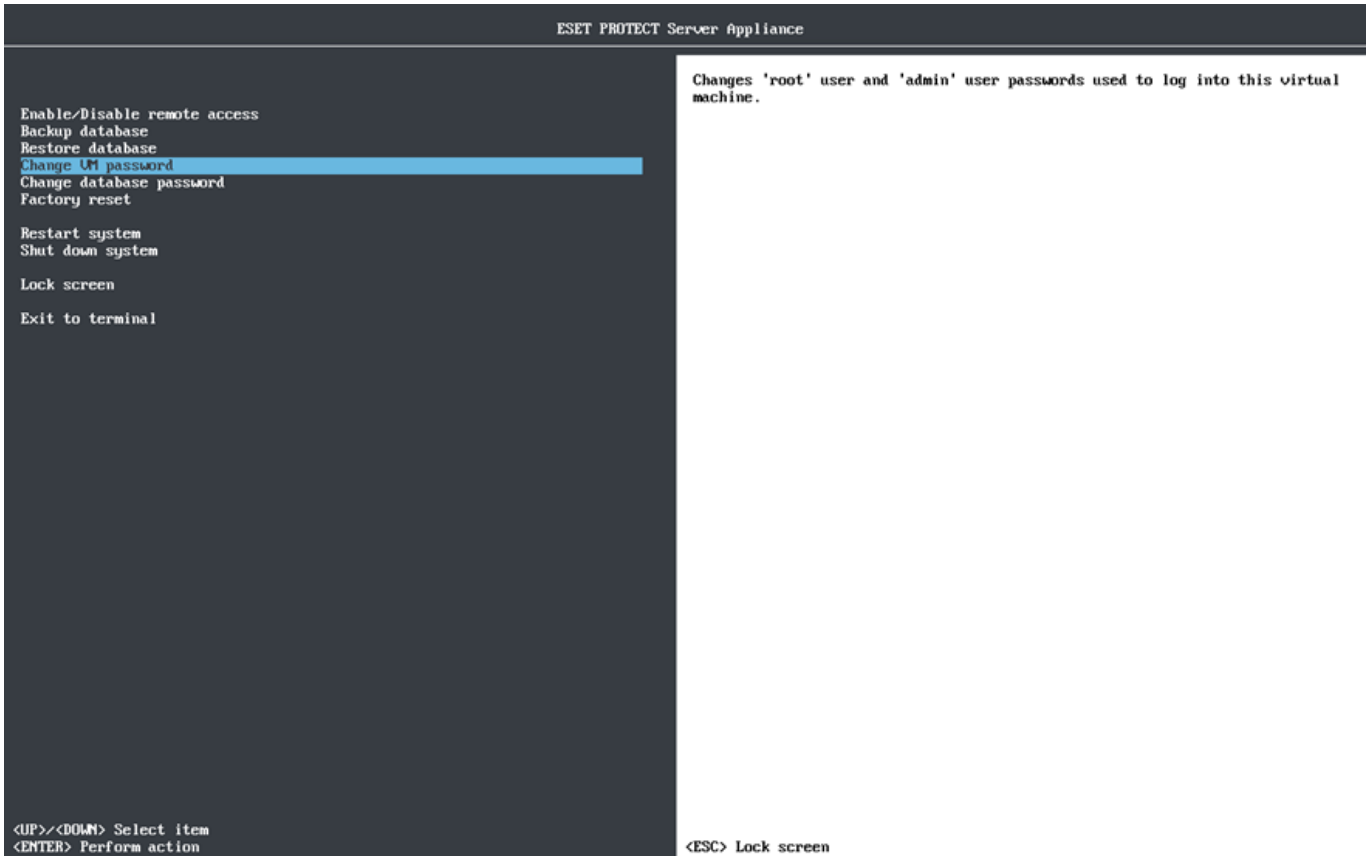
Change VM password

Your VM password is used to log on to your deployed ESET PROTECT Virtual Appliance. If you want to change your VM password or keep your VM more secure, we recommend that you use strong passwords and change them regularly.

This procedure will change your password for the Virtual Machine only. Your ESET PROTECT Web Console and Database root password will not be changed. For more information, see ESET PROTECT VA password types.

If you have forgotten your password, see How to recover a forgotten ESET PROTECT VA password.

1. Log in to the management mode by typing your password and pressing **Enter** twice. Select **Change VM password** using the arrow keys and press **Enter**.



2. Type your **New password** into the empty field, press **Enter** and then **Retype** it to confirm for each of the following users:

- `root`
- `admin`

See ESET PROTECT VA passwords for more information about the users.

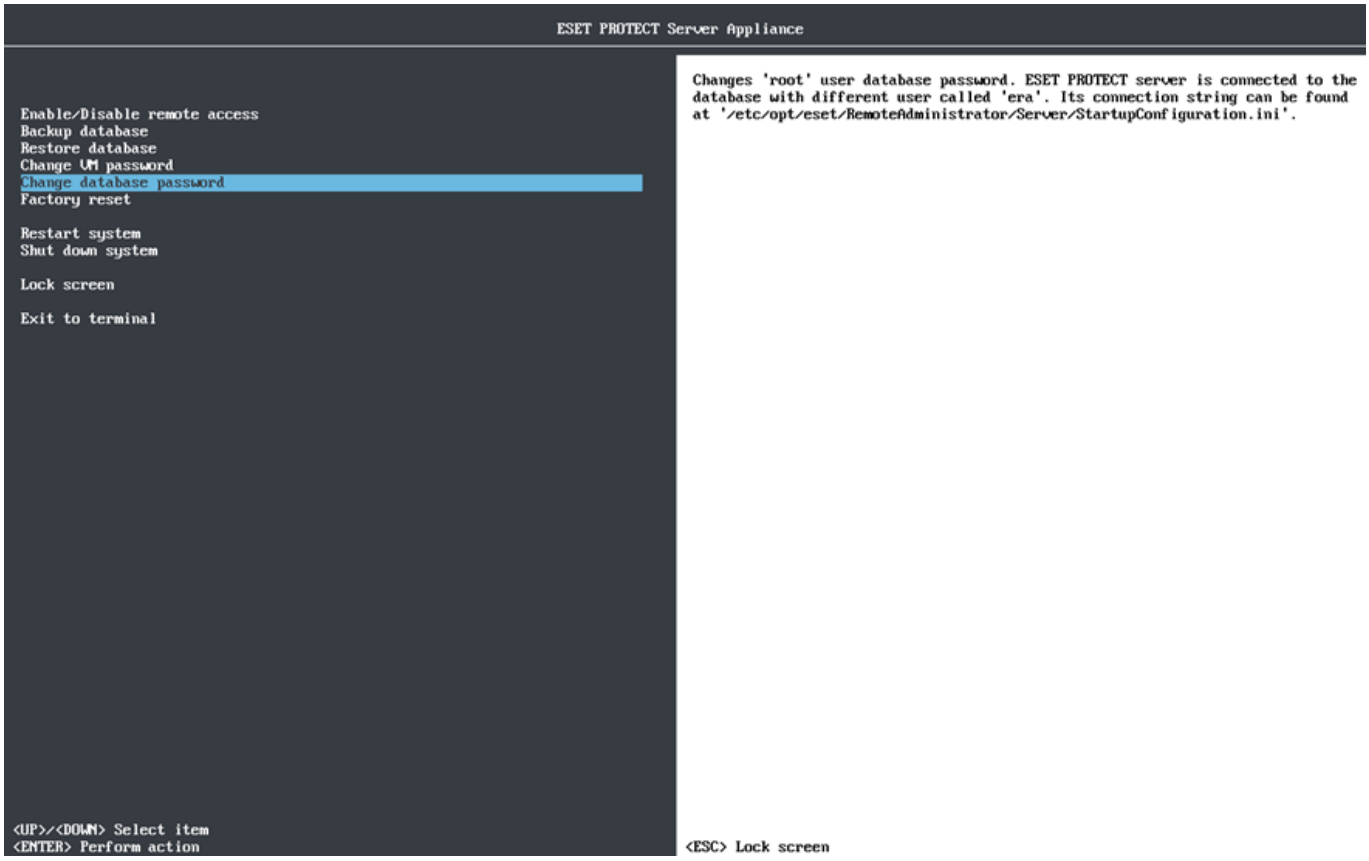
> Use a complex password that:
> • has at least 18 characters
> • contains numbers, uppercase letters, and non-alphanumeric characters
> You will see a warning if the password does not meet the above recommendations.

The message **all authentication tokens updated successfully** will be displayed when you are finished and your new password will now be required to log in.

Change database password

The database `root` password allows full access to the MySQL database server. The MySQL `root` user has complete control over the MySQL server only.

1. Log in to the management mode by typing your password and pressing **Enter** twice. Select **Change database password** using the arrow keys and press **Enter**.



2. When you are prompted to **Type old database root password**, type the password you set during ESET PROTECT Virtual Appliance configuration. This password may be different from your **VM password** if you have changed it separately.

```
Enter new database root password:
Enter old database root password.
Enter password:

Press Enter to continue.
```

Now the database `root` password has been changed.

Rejoin domain

> This feature is no longer available in the latest VA based on Rocky Linux. You can configure the domain connection in the ESET PROTECT Web Console > **More** > **Settings** > **Advanced Settings** > Active Directory. See also the domain connection troubleshooting.

Use this feature if you experience problems with Active Directory or trust relationships with the domain.

> You need to have domain configured correctly, otherwise **Rejoin domain** might not work.

1. Log in to the management mode by typing your password and pressing **Enter** twice. Select **Rejoin domain** using the arrow keys and press **Enter**.

2. Type the domain username that will be used to join the domain.

If you are not familiar with Linux and terminal, you can access the Webmin and use the **Bind to Domain** feature

under **Servers** > Samba Windows File Sharing.

Configure domain

This feature is no longer available in the latest VA based on Rocky Linux. You can configure the domain connection in the ESET PROTECT Web Console > **More** > **Settings** > **Advanced Settings** > Active Directory. See also the domain connection troubleshooting.

Configure Domain allows you to modify configuration files to include specific settings of your environment. The following configuration files are available:

Filename	Description
/etc/hosts	The Hosts file should correctly map to your domain controller name and its IP address.
/etc/krb5.conf	The Kerberos configuration file should be correctly generated. Verify that `kinit <user-from-domain>` works.
/etc/ntp.conf	The NTP configuration file should contain a record for regular time updates against the domain controller.
/etc/samba/smb.conf	The Samba configuration file should be correctly generated.

These files are pre-configured and require minimal changes to them when specifying a domain name, for example, or a domain controller name, a DNS server name, etc.

1. Log in to the management mode by typing your password and pressing **Enter** twice. Select **Configure domain** using the arrow keys and press **Enter**.

This is an advanced procedure that we recommend for expert administrators only.

2. Press **Enter** to edit the first configuration file.

3. Press **Ctrl+X** to close the text editor. You will be prompted to save changes, press **Y** to save or **N** to discard. If you have not made any changes, the text editor will just close. If you want to make further changes, do not use **Ctrl+X**, but press **Ctrl+C** to cancel and return to the text editor. Visit this Knowledgebase article to view examples of how to edit the configuration files.

See */root/help-with-domain.txt* on your ESET PROTECT VA, the easiest way is to search for *help-with-domain.txt* using Webmin File manager. Alternatively, you can use `nano help-with-domain.txt` command to see the help file.
If you are not familiar with Linux and terminal, you can configure domain connection (Kerberos, NTP or network settings through Samba Windows File Sharing) using Webmin.

4. After completing the domain configuration, select **Rejoin Domain** and type the Administrator name and password for domain connection.

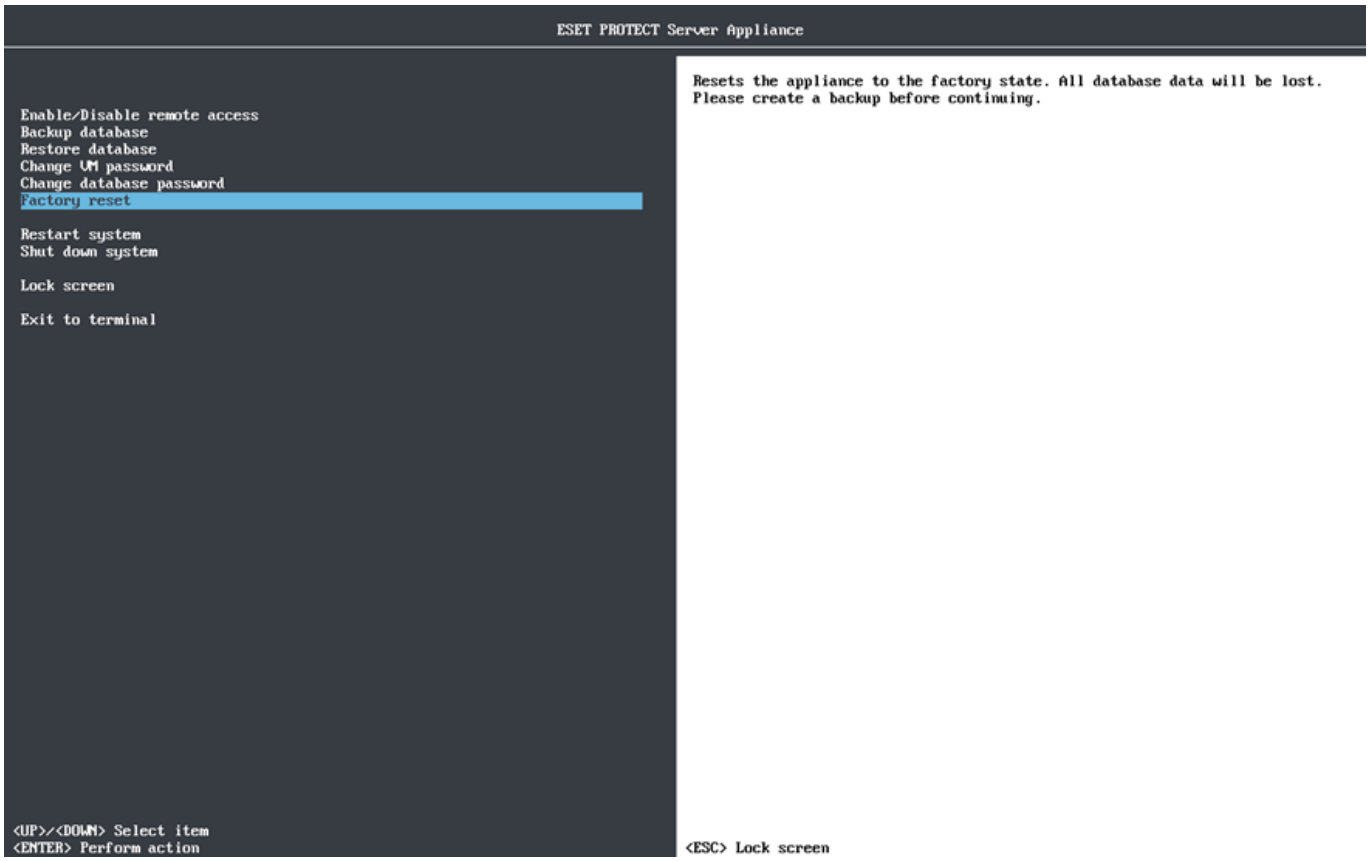
Factory reset

You can use **Factory reset** to restore your ESET PROTECT Virtual Appliance to its original state as when freshly deployed. All of the configuration and settings will be reset and the whole ESET PROTECT database will be dropped.

We highly recommend that you back up your ESET PROTECT database before executing a factory reset. Your database will be empty after performing a reset.

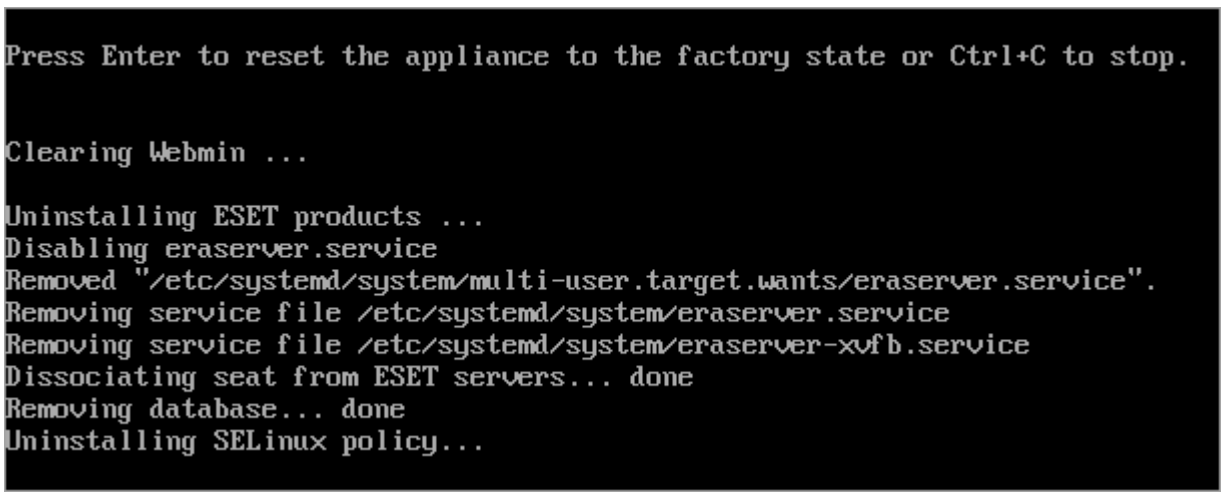
Factory reset will only restore settings that were changed during ESET PROTECT VA configuration, other changes and settings will remain. In rare cases, **Factory reset** will not completely restore your VA's original state. If you are experiencing issues with ESET PROTECT VA, we recommend that you deploy a new machine. Follow the steps to perform upgrade/migration or perform a disaster recovery procedure.

1. Log in to the management mode by typing your password and pressing **Enter** twice. Select **Factory reset** using the arrow keys and press **Enter**.



2. Press **Enter** to execute the factory reset of your ESET PROTECT VA or you can exit to menu by pressing **Ctrl+C** at this point.

When the factory reset is running, do not press **Ctrl+C**, because it may damage your virtual appliance.



If you see any error messages on screen during the **Factory reset**, try running the reset again. If re-running the **Factory reset** does not help or if you are not sure, we recommend that you do a fresh deployment, you can follow the same steps as described in upgrade/migration or perform a disaster recovery procedure.

Factory reset performs the following actions:

- resets network configuration, all passwords and a hostname
- removes all data from ESET PROTECT database
- resets ESET PROTECT database user password

After your ESET PROTECT VA reboots, it will be in its original state as if freshly deployed and ready for you to begin configuring it from scratch.

Custom modifications or settings not related to ESET PROTECT On-Prem will remain unchanged.

Webmin Management Interface

Webmin is a third-party web based interface that simplifies the process of managing a Linux system. Webmin was written for use by people who have some Linux experience, but are not familiar with the intricacies of system administration. It allows you to perform these tasks through an easy to use web interface and automatically updates all of the required configuration files for you. This makes the job of administering your system much easier.

- Webmin is accessible through a web browser, you can log in to it from any system (client computer or a mobile device) that is connected to your network. It is easier to use over the network than locally using other graphical configuration programs.
- All recent versions of Webmin may be freely distributed and modified for commercial and non-commercial use. You can find more information on the Webmin web pages.

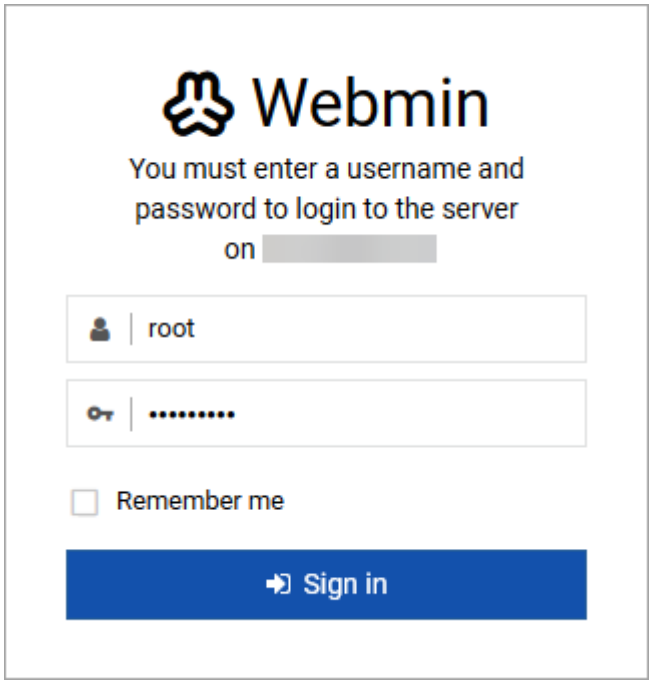
Access Webmin

Webmin is included in your ESET PROTECT Virtual Appliance:
- To begin using it, you must enable it.
- It uses HTTPS and runs on port 10000. The IP address for Webmin will be shown in the ESET PROTECT VA Management Console screen.

1. Open your web browser and type the IP address or hostname of your deployed ESET PROTECT VA in the address bar and use port 10000. The URL should be in the following format: *https://<hostname or IP address>:10000* for example *https://10.20.30.40:10000* or *https://protectva:10000*.

2. Type username and password:

   - the username is **root**
   - the default password is **eraadmin**, but if you have already changed it, use the password you specified during ESET PROTECT VA configuration.



After a successful login, the Webmin Dashboard will be displayed.

Dashboard

When you are logged into Webmin, the **Dashboard** will display System Information for your ESET PROTECT VA. Information such as hostname, OS, system uptime, memory usage, package updates, etc. Also, you will see a notification area at the bottom of the page where items that require your attention will be displayed. For example a notification that a later Webmin version is available allowing you to take action by pressing **Upgrade Webmin Now** button. We recommend that you upgrade it. When the upgrade is finished, a message **Webmin install complete** is displayed.

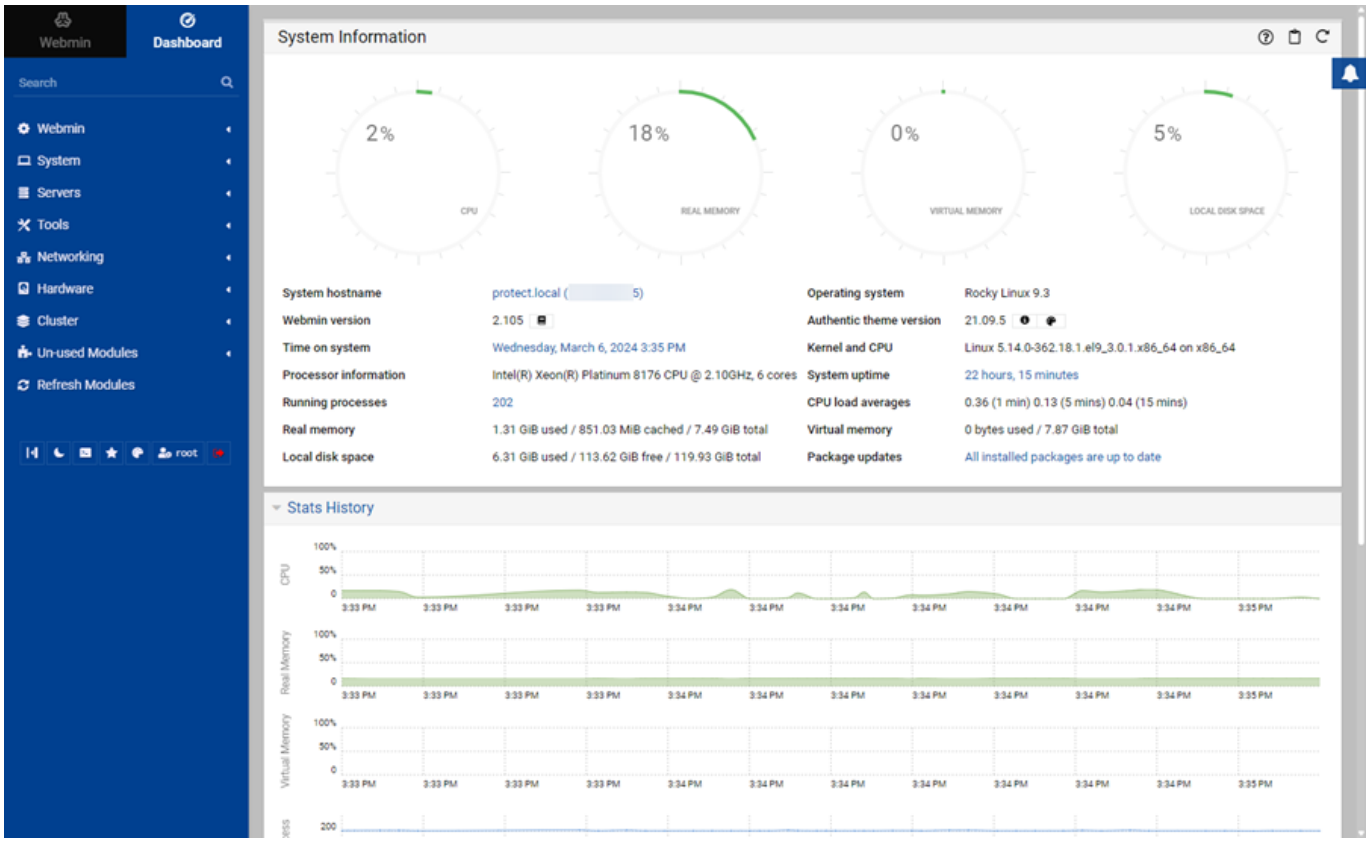
The main menu includes the module categories: **Webmin**, **System**, **Servers**, **Tools**, **Networking**, **Hardware** and **Cluster**. For more information about modules see Webmin Modules pages.

> The Webmin automatically detects what is configured in the VA and shows relevant modules accordingly.

The most important modules for managing your ESET PROTECT VA are:

- System
- Servers
- Tools
- Networking

Webmin runs with full Linux **root privileges**, which means that it can edit any file and run any command on your system. You can delete all of the files on your system or make it unbootable if you make a mistake. For this reason it is important that you use caution while running Webmin. Even though Webmin will usually warn you before performing a potentially dangerous action, do not make configuration changes to items you are not familiar with.



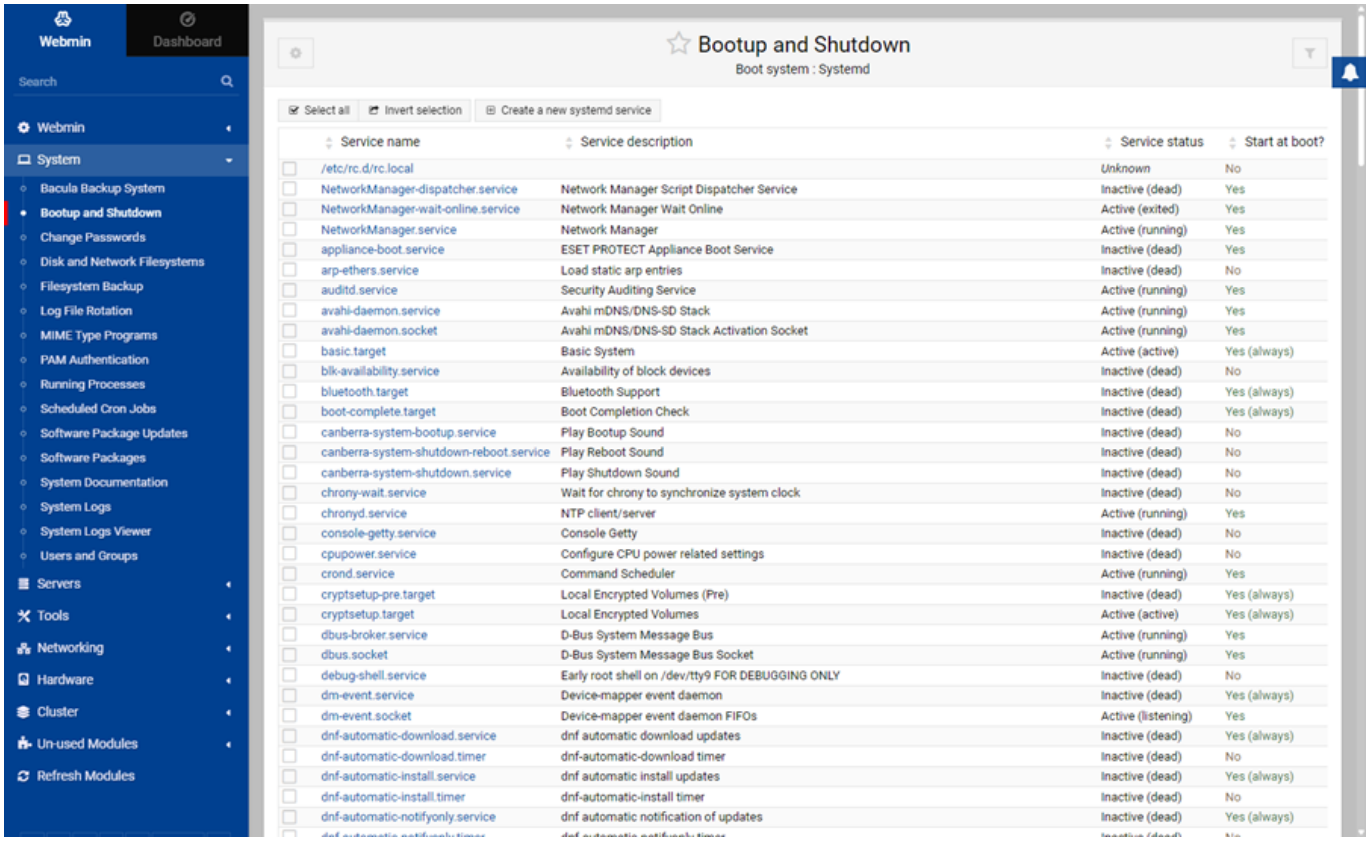
Notification—If Webmin wants to notify you, a notification will be displayed at the bottom of the Dashboard.

Logout—When you are done using Webmin, use the logout icon  from the menu on the left.

System

In this section you can configure some **System** modules.

Bootup and Shutdown—Manage services, modify, Start/Stop/Restart each service or multiple services at the same time. You can also create and edit scripts that run at bootup and shutdown, etc. You can **Reboot** or **Shutdown** the ESET PROTECT VM using the buttons at the bottom of the page.



Change Passwords—Change VM's operating system user's passwords.

> Do not use this when you want to change password to ESET PROTECT VA or to ESET PROTECT database, use Change VM password or Change database password from within ESET PROTECT Virtual Appliance Management Console.

Running Processes—Manage all Running processes on your system using Webmin. This module can be used to view, kill, re-prioritize and run processes on your system.

Software Package Updates—Shows you available updates and allows you to update all or selected packages.

System Logs—View log files on your system and, if necessary, change the location where log messages are recorded.

Servers

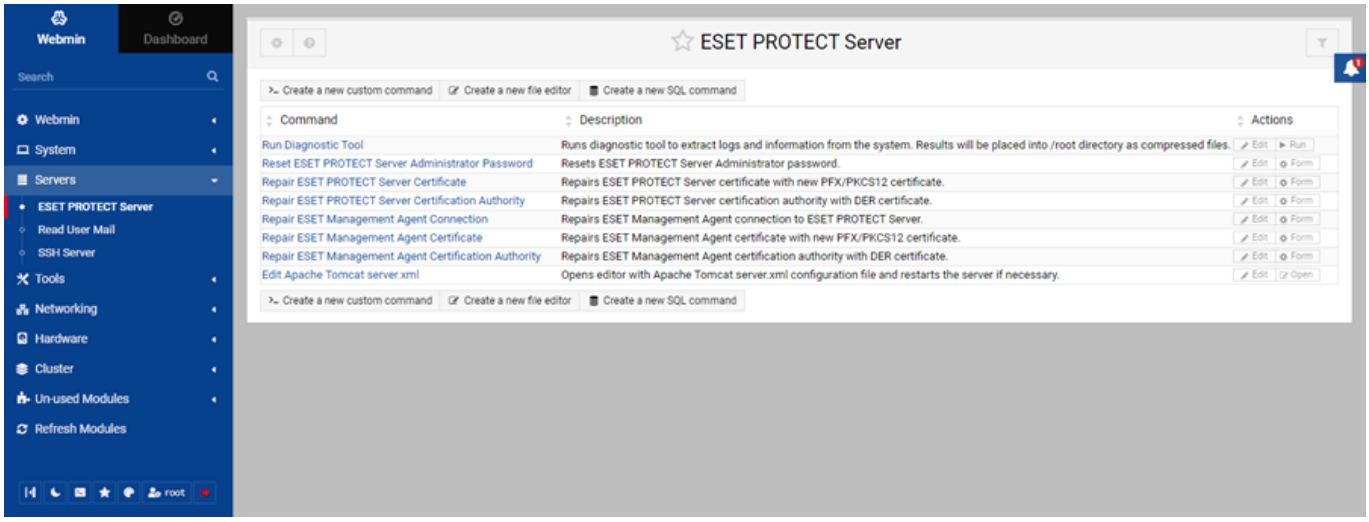
In this section you can configure some **Servers** modules:

SSH Server

SSH Server—This module is used to configure SSH and OpenSSH servers, and assumes that you have a basic knowledge of the client programs as a user. You can configure SSH Server and clients on your system.

ESET PROTECT Server

The **ESET PROTECT Server** module allows you to run certain pre-defined commands, mostly to Repair ESET PROTECT certificates, Run a diagnostic tool or to Reset ESET PROTECT Server password.



- **Run Diagnostic Tool**—Click the button to extract logs and information from the system. Logs will be exported for ESET PROTECT Server and ESET Management Agent. You can use the File Manager module to find and download exported diagnostic log files compressed in a *.zip* format.

- **Reset ESET PROTECT Server Administrator Password**—If you have forgotten your ESET PROTECT Server password or just want to reset the password, type your new password for ESET PROTECT Server Administrator account and press the button to run the command.

- **Repair ESET PROTECT Server Certificate**—Repair ESET PROTECT Server certificate with new PFX/PKCS12 certificate. Click the **paper clip** icon and browse for ESET PROTECT Server PFX or PKCS12 certificate file, then click **Open**. Type ESET PROTECT Server certificate password and press the button to run the command.

- **Repair ESET PROTECT Server Certification Authority**—Repair ESET PROTECT Server Certification Authority with DER certificate. Click the **paper clip** icon and browse for CA *.der* certificate file, then click **Open**.

- **Repair ESET Management Agent Connection**—Repair ESET Management Agent connection to ESET PROTECT Server. Type your ESET PROTECT Server **Hostname** and **port** number, then press the button to run the command.

- **Repair ESET Management Agent Certificate**—Repair ESET Management Agent certificate with new PFX/PKCS12 certificate. Click the **paper clip** icon and browse for ESET Management Agent *PFX* or *PKCS12* certificate file, then click **Open**. Type ESET Management Agent certificate password and press the button to run the command.

The certificate passphrase must not contain following characters: " \ These characters cause critical error during the initialization of the Agent.

- **Repair ESET Management Agent Certification Authority**—Repair ESET Management Agent Certification Authority with DER certificate. Click the **paper clip** icon and browse for CA *.der* certificate file, then click **Open**.

- **Edit Apache Tomcat server.xml**—You can edit Apache Tomcat server.xml configuration file to change Web Console HTTPS certificates and cipher algorithms. When you press the button, a text editor will open and allow you to edit the */etc/tomcat/server.xml* file. Click **Save** button to save changes. If a restart is necessary, it will be done automatically. If you do not want to save changes you have made, click **Return to commands**.

Tools

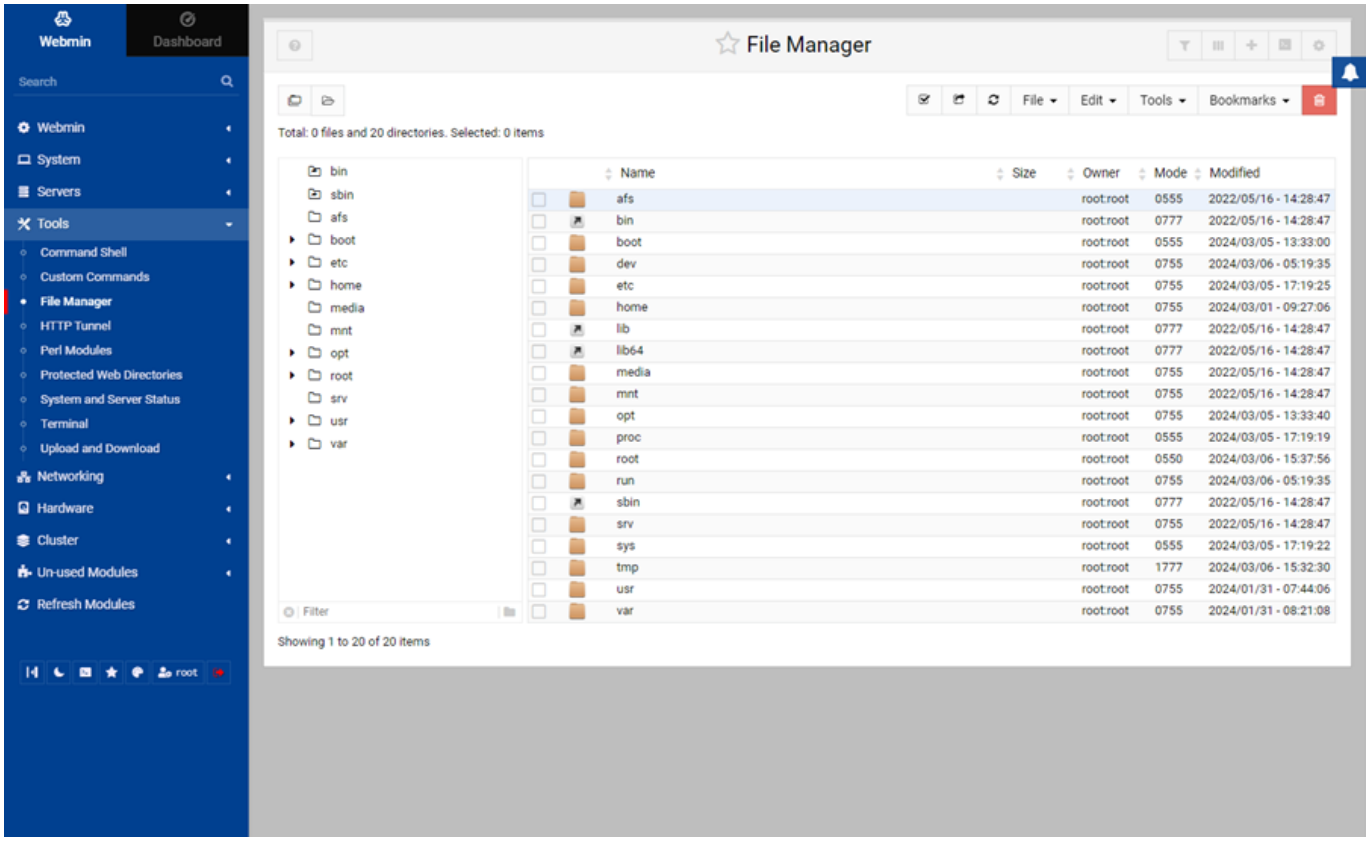
This category of Webmin contain number of different modules. There are two very useful modules:

- **File Manager**
- **Upload and Download**

File Manager

File Manager allows you to view and manipulate files on the server through an HTML interface. When you first load the File manager (also known as **Filemin**), contents of the root directory on your ESET PROTECT VA will be shown, depending on which user you are logged in as.

- Navigation within the directory structure is simple, click the directory name or its icon (folder). You will see current directory at the upper left part of the Filemin window, click any part of the path to show contents of that specific directory.
- The Filemin can also be used to search for files, click **Tools** in the toolbar (at the upper right corner of the Filemin window), select **Search**, and type a search pattern to look for.
- If you want to download a file from your ESET PROTECT VA to the computer your web browser is running on, just click the filename or its icon.
- If you want to upload a file from the computer your web browser is running on, click **File** then **Upload to current directory**. This will open a dialog window, click the paperclip icon to browse for file(s) you want to upload. You can select multiple files and upload them by clicking the **Upload** button. Uploaded file(s) will be stored in your current directory. When the upload is complete, the directory list will be updated and you will see the file(s) you have uploaded.
- You can also retrieve a file from a remote URL. To do that, click **File** and select **Download from remote URL**.
- To create a new empty text file, click **File** then **Create new file**, type name of the new file.
- To rename a file or directory, click **Rename** in the right-click context menu.



Upload and Download

Upload and Download allows different file actions:

- **Download from web**—Type URL(s) of the file(s) you want to download from the internet to your ESET PROTECT VA and specify location where you want to store the file(s).

- **Upload to server**—Click the paperclip icon(s) to browse for file(s) you want to upload, you can upload up to four files at the time. Specify location where you want to store the file(s).

- **Download from server**—Specify path including the filename in the **File to download** text field or click the icon next to it to browse ESET PROTECT VA file system for the file you want to download to the computer your web browser is running on. Click the **Download** button to start downloading the file, you can download one file at a time.

Networking

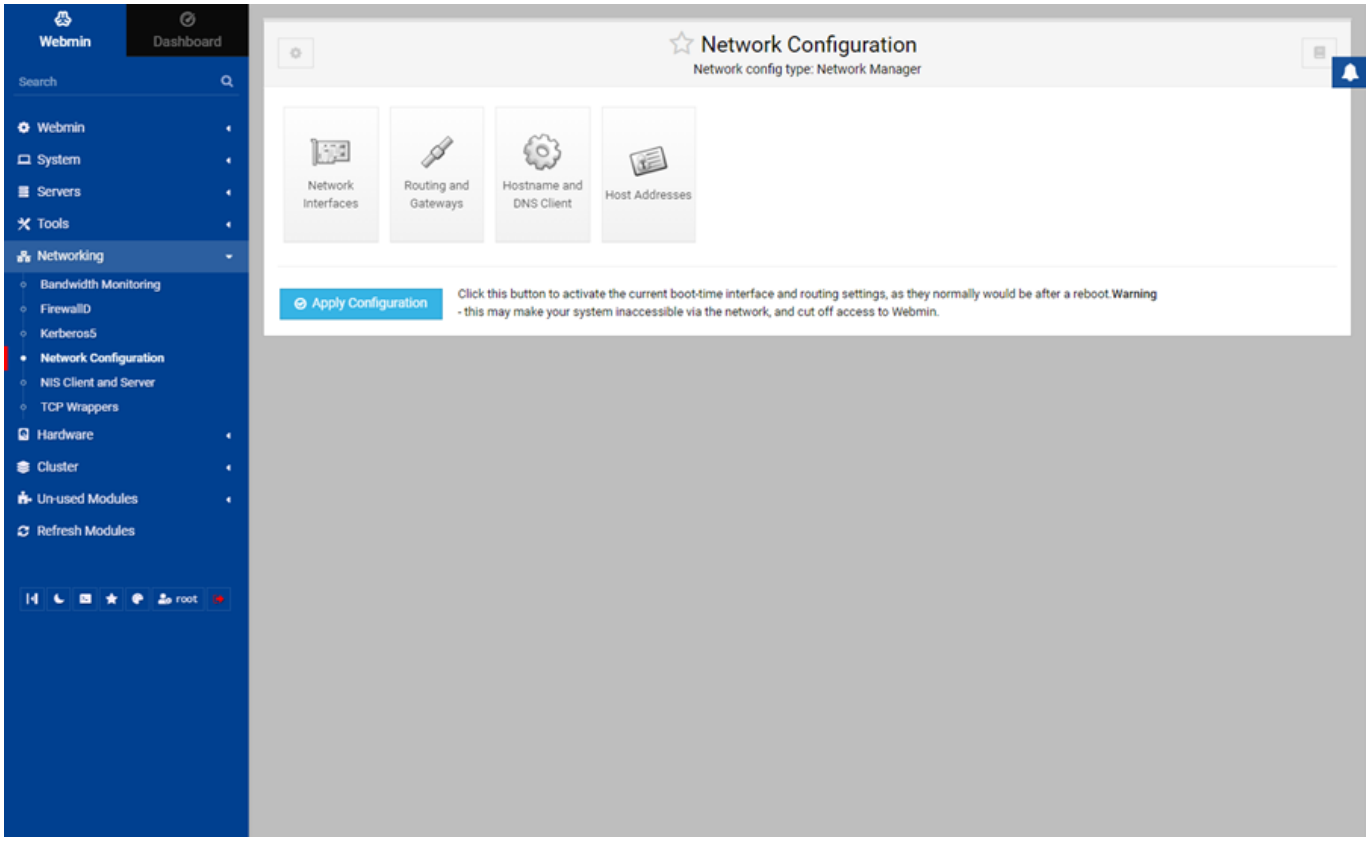
You do not need to change networking settings most of the time, but if it is required, you can do so in **Networking** category. In this section you can configure some of the useful modules:

- **FirewallD**—If you need to allow ports, you can do so here by adding rules or edit existing rules.

- Network configuration—You can configure network adapter, change IP address, hostname, DNS and other network settings.

> When you are finished with configuration, press **Apply Configuration** button in order for the changes to take place.

This is for advanced administrators only. If the network configuration is incorrect, it may make your system inaccessible via the network and cut off access to Webmin. However, you will still be able to access ESET PROTECT VA Management Console via the Virtual Machine's terminal window.



ESET PROTECT certificates

ESET PROTECT certificates are required for secure communication between ESET PROTECT components and ESET PROTECT Server and also for establishing secured connection of ESET PROTECT Web Console.

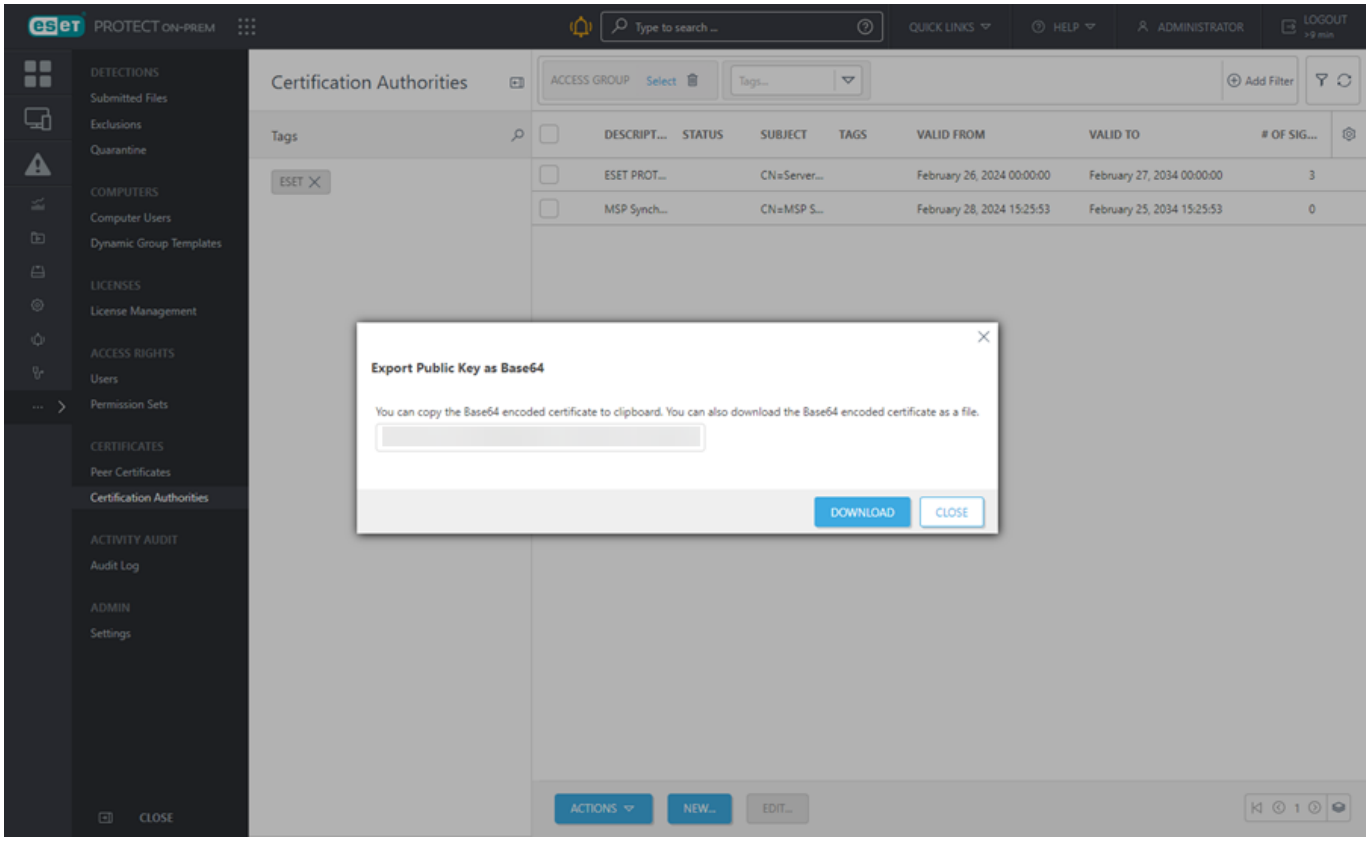
Certificates for ESET PROTECT components are available in the Web Console.

To copy the contents of a certificate in Base64 format:

1. Click **More** > **Peer Certificates**.

2. Select a certificate and then select Export as Base64. You can also download the Base64 encoded certificate as a file.

Repeat these steps for other component certificates as well as for your Certification Authority.



To export a certificate, a user is required to have **Use** rights over **Certificates**. See the full list of access rights for more information.

ESET PROTECT VA upgrade/migration

For upgrading or migrating your VA, you can perform the following:

- **Upgrade**—Install a later version of ESET PROTECT components.
- **Migration**—Move the ESET PROTECT Virtual Appliance to another instance of the same version.
- **Migration and upgrade**—Move the ESET PROTECT Virtual Appliance to another instance of the later version.

There are two ways of upgrading your VA:

- Using the database pull—Upgrades your whole Appliance (the underlying operating system), not just the ESET PROTECT Server. The process is more complicated and requires having two concurrent appliances during the transition period. We recommend using the database pull to upgrade to the major versions or as a troubleshooting method.
- Upgrading via Components Upgrade task in the Web Console—The process is more simple and does not require access to the appliance, only to the Web Console. We recommend this procedure for minor and hotfix upgrades. Components upgrade does not upgrade other VA software (operating system, packages needed for proper functioning of ESET PROTECT Server).

Migration and upgrade process (recommended way to upgrade)

Before the migration

Back up your database and export Certification Authority and Peer Certificates from your old ESET PROTECT VA before migrating or upgrading the ESET PROTECT Server.

If your old ESET PROTECT VA does not use advanced security and has the certificates signed by the SHA-1 Certification Authority, follow these steps before the migration in your old ESET PROTECT VA to prevent the failed login in the new VA:

1. Enable the advanced security.
2. Create a new Certification Authority.
3. Create a new Server certificate and sign it using the new Certification Authority.
4. Wait until the public part of the Certification Authority replicates to all ESET Management Agents in the network.

ESET PROTECT On-Prem Mobile Device Management (MDM) reached the End of Life. This feature is no longer available in the latest VA based on Rocky Linux. We recommend that you migrate to the cloud ESET PROTECT with the Cloud MDM.

Follow these instructions to migrate from the earlier VA based on CentOS to the latest VA based on Rocky Linux.

1. Download the latest *protect_appliance.ova* (or *protect_appliance.vhdx.zip* if you use Microsoft Hyper-V).

2. Deploy a new ESET PROTECT VA. See ESET PROTECT Virtual Appliance deployment process for instructions. **Do not configure** the new ESET PROTECT VA via its web interface.

3. Pull the database from your old VA.

Do not uninstall/decommission your old VA Server.

4. Configure ESET PROTECT Virtual Appliance via its web interface.

5. Verify that your new ESET PROTECT VA behaves the same way as the previous one:

   - If the new ESET PROTECT VA has a **different IP address**:

     a)Create a policy on your old VA to set a new ESET PROTECT Server IP address and assign it to all computers.

     b)Wait for the policy to be distributed to all ESET Management Agents.
     c)Ensure all computers are connecting to the new ESET PROTECT VA.

     d)Turn off and decommission the old VA.

We strongly recommend that you do not uninstall the old ESET PROTECT VA Server using an uninstallation script. This uninstallation procedure will dissociate (remove) all licenses from the new ESET PROTECT VA Server database as well. To prevent this behavior, delete the old ESET PROTECT VA Server database (DROP DATABASE) before the uninstallation.

   - If the new ESET PROTECT VA has the **same IP address**:

Ensure the network configuration on your new ESET PROTECT Server (IP address, FQDN, Computer name, DNS SRV record) matches that of your old VA Server. You can also use the hostname by changing the DNS record to the new server.

a)Turn off the old VA.

b)Turn on the new ESET PROTECT VA.

c)Ensure all computers are connecting to the new ESET PROTECT VA.

d)Decommission the old VA.

We strongly recommend that you do not uninstall the old ESET PROTECT VA Server using an uninstallation script. This uninstallation procedure will dissociate (remove) all licenses from the new ESET PROTECT VA Server database as well. To prevent this behavior, delete the old ESET PROTECT VA Server database (DROP DATABASE) before the uninstallation.

6. Upgrade a ESET Management Agents sample group using an ESET PROTECT Components Upgrade task.

7. If the sample upgrade is successful and Agents are still connecting, continue with the rest of the Agents.

Upgrade process (an alternative way to upgrade)

Upgrading earlier ESET PROTECT On-Prem to the latest ESET PROTECT On-Prem on the same VA does not upgrade other VA software (operating system, packages needed for proper functioning of ESET PROTECT Server). We recommend that you migrate the server after the clean upgrade.

Upgrade the VA using a Components Upgrade task:

1. Upgrade the ESET PROTECT Server first.

2. Upgrade a ESET Management Agents sample group.

3. If the sample upgrade is successful and Agents are still connecting, continue with the rest of the Agents.

ESET PROTECT VA disaster recovery

When your ESET PROTECT VA gets broken, and you cannot start it again, or if it is deleted from storage or otherwise destroyed, you can follow the disaster recovery procedure.

You must have ESET PROTECT VA's database backup for a successful recovery.

1. Download the latest version of *protect_appliance.ova*, or *protect_appliance.vhdx.zip* if you use Microsoft Hyper-V. The advantage of this recovery procedure is that your ESET PROTECT VA will be up to date.

2. Deploy a new ESET PROTECT VA, but do not configure it.

3. Enable Webmin so that you can upload the database backup file.

4. Restore the database using the latest backup file you have.

5. Configure your freshly deployed ESET PROTECT VA with the restored database in the same way as your previous VA.

Troubleshooting

The following log files can be used to troubleshoot the ESET PROTECT Virtual Appliance. Also, you may be asked by ESET technical support to provide diagnostic logs. These are the log files you can send for analysis:

Log name	Location	Description
ESET PROTECT VA configuration	CentOS: */root/appliance-configuration-log.txt* Rocky Linux: */opt/appliance/log/appliance-configuration-log.txt*	If your ESET PROTECT VA deployment fails, do not restart the appliance and check configuration log file.
ESET PROTECT Server	*/var/log/eset/RemoteAdministrator/EraServerInstaller.log* */var/log/eset/RogueDetectionSensor/RDSensorInstaller.log*	ESET PROTECT Server installation log file. Other ESET PROTECT components use a similar path and corresponding filename.
ESET PROTECT Server trace log ESET Management Agent trace log	*/var/log/eset/RemoteAdministrator/Server/* */var/log/eset/RemoteAdministrator/Agent/*	Check your trace logs: *trace.log* *status.html* *last-error.html* Other ESET PROTECT components use similar path and filenames.
ESET Bridge (HTTP Proxy)	See ESET Bridge Online Help.	ESET Bridge log files
ESET PROTECT Server crash dumps	*/var/opt/eset/RemoteAdministrator/Server/Dumps/*	
ESET PROTECT Server or ESET Management Agent run diagnostic tool	*/root/RemoteAdministratorAgentDiagnostic20240313T113830.zip* */root/RemoteAdministratorServerDiagnostic20240313T113829.zip*	If you experience issues with your ESET PROTECT VA, you can **Run diagnostic tool**, see ESET PROTECT Server Webmin module for details.

If the Server or Agent are crashing and you cannot change the logging verbosity via Web Console, you can enable full trace logging by creating the empty file:

- Agent:

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

- Server:

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

We recommend that you use Webmin File manager where you can easily search for files and download logs if necessary.

ESET PROTECT Virtual Appliance FAQ

This chapter covers some of the most frequently asked questions and problems encountered. Click the topic title to find out how to solve your problem:

- Find out which ESET PROTECT components are installed
- Do I need to add other components to my ESET PROTECT VA?
- Enable ESET Bridge (HTTP Proxy) on the ESET PROTECT VA
- Enable/disable ping on ESET PROTECT Virtual Appliance
- Configure ESET PROTECT VA to allow Static Group synchronization via LDAP
- Configure the domain connection
- Configure LDAPS connection to a domain
- Recover a forgotten password for ESET PROTECT VA
- Change ESET PROTECT database connection string
- Set up Hyper-V Server for RD Sensor
- Change port numbers for ESET PROTECT VA Web Console
- Increase memory size for MySQL Server
- Error with ESET PROTECT On-Prem running on a Hyper-V Server 2012 R2
- Improve Oracle VirtualBox performance
- Enable YUM command under HTTP Proxy server
- Update the operating system on a machine running ESET PROTECT VA Server
- Disable SELinux permanently
- Restart Virtual Appliance Management Console
- Enable SSH

If your problem is not included in the help pages list above, try searching by keyword or phrase describing your problem and search within the ESET PROTECT On-Prem Help Pages.

If you cannot find the solution to your problem/question within the Help Pages, you can try our regularly updated online Knowledgebase.

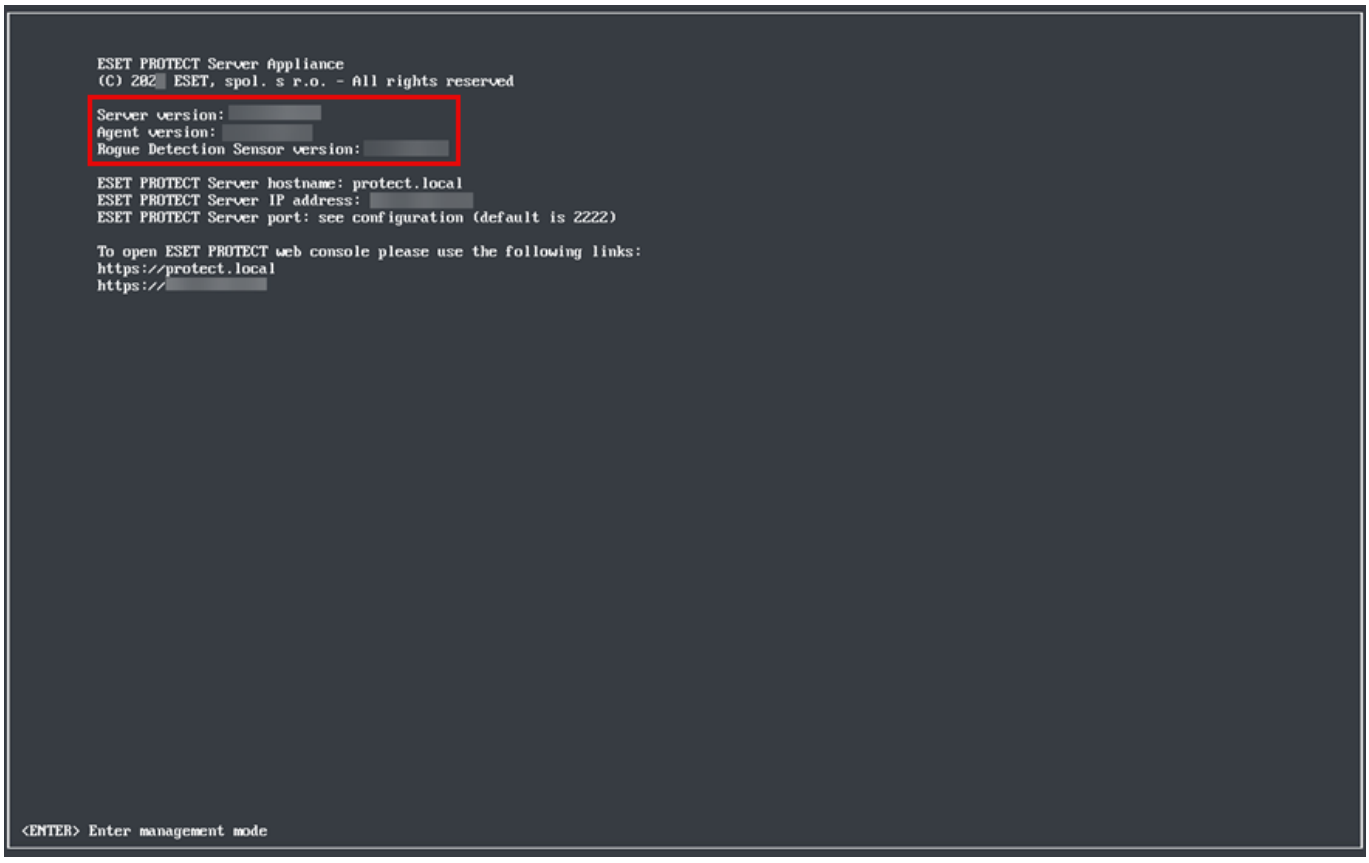
If necessary, you can directly contact our online technical support center with your questions or problems. The contact form can be found in the ESET PROTECT Web Console > **Help** > **Contact Support**.

Find out which ESET PROTECT components are installed

A list of installed ESET PROTECT components and their versions is available in the console window of your ESET PROTECT Virtual Appliance.

To refresh this dialog after components upgrade, you can:

- reboot the VA
- Log in to the management mode by typing your password and pressing **Enter** twice. Select **Exit to terminal**, then exit the terminal to return back to lock screen.



`

Do I need to add other components to my ESET PROTECT VA?

No. Using the Virtual Appliance is the simplest way to deploy ESET PROTECT On-Prem as long as you use a supported hypervisor. Deploy the appliance and configure it.

The ESET PROTECT Virtual Appliance runs out of the box:

- It contains the ESET PROTECT Server running on a dedicated VM and contains a functional operating system.

- It also includes other ESET PROTECT components—ESET Management Agent, ESET Rogue Detection Sensor and ESET Bridge (HTTP Proxy).

Enable ESET Bridge (HTTP Proxy) on the ESET PROTECT VA

We recommend that you enable ESET Bridge during the ESET PROTECT VA initial configuration.

You can install and configure ESET Bridge later or configure another HTTP Proxy, for example Apache HTTP Proxy.

Enable/disable ping on ESET PROTECT Virtual Appliance

Open the terminal and run the following commands (based on your operating system) as root to enable/disable ping on an ESET PROTECT Virtual Appliance machine.

CentOS 7

Ping is disabled by default on CentOS 7. Follow the steps below to enable ping:

1. Call the iptables command:

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

2. Save iptables:

```
service iptables save
```

Now, you can ping the ESET PROTECT Virtual Appliance from other computers in the same subnet.

Rocky Linux 9.3

Ping (ICMP) is enabled by default on Rocky Linux 9.3.

Disable ping (ICMP requests)

1. `firewall-cmd --set-target=DROP --zone=public --permanent`
2. `firewall-cmd --add-icmp-block-inversion --permanent`
3. `firewall-cmd --reload`

Now, you cannot ping the ESET PROTECT Virtual Appliance from other computers in the same subnet.

Enable ping (ICMP requests)

If you have disabled ping, you can enable it by following the steps below:

1. `firewall-cmd --set-target=default --zone=public --permanent`

2. `firewall-cmd --remove-icmp-block-inversion --permanent`
3. `firewall-cmd --reload`

Now, you can ping the ESET PROTECT Virtual Appliance from other computers in the same subnet.

Configure ESET PROTECT VA to allow Static Group synchronization via LDAP

You can configure the domain connection in the ESET PROTECT Web Console > **More** > **Settings** > **Advanced Settings** > Active Directory.

After configuring the domain, you can synchronize static groups via LDAP.

Configure the domain connection

CentOS

You can configure the domain connection during the initial ESET PROTECT VA configuration.

Rocky Linux

You can configure the domain connection in the ESET PROTECT Web Console > **More** > **Settings** > **Advanced Settings** > Active Directory.

Domain connection troubleshooting

If the domain connection does not work, configure Kerberos5, as described in section III in the Configure domain connection for ESET PROTECT Virtual Appliance Knowledgebase article:

- You can skip the steps that do not apply to your network environment.
- Skip steps 6 and 7. Do the following instead: You can configure the domain connection in the ESET PROTECT Web Console > **More** > **Settings** > **Advanced Settings** > Active Directory.

Configure LDAPS connection to a domain

Follow the steps below to configure ESET PROTECT Virtual Appliance to connect to Active Directory via LDAPS.

Prerequisites

- Set up LDAPS on the Domain Controller—Ensure to export the DC Certification Authority public key.
- Ensure Kerberos is correctly configured on your ESET PROTECT VA

Enable LDAPS on ESET PROTECT VA

1. Open virtual machine's terminal window with ESET PROTECT VA.

2. Press **Enter**, type your password that you specified during ESET PROTECT VA configuration and press **Enter** twice.

3. Select **Exit to terminal** and press **Enter**.

4. Stop the ESET PROTECT Server service:

```
systemctl stop eraserver
```

5. Type the following command:

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

6. Add the following line to the `[Service]` section:

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

7. Press **CTRL+X** and type **Y** to save the file changes. Press **Enter** to exit the editor.

8. Run the following command to reload the configuration:

```
systemctl daemon-reload
```

9. Start the ESET PROTECT Server service:

```
systemctl start eraserver
```

10. Copy the certificate file you generated on the Domain Controller to the following location on your ESET PROTECT VA Server:

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

11. Run the following command:

```
update-ca-trust
```

Recover a forgotten password for ESET PROTECT VA

1. In the Boot Grub Menu select the option to edit: `e`.

2. Go to the line starting with `linux...` and change `ro` to `rw init=/sysroot/bin/sh`

3. Press **CTRL+X** to start the ESET PROTECT VA in a Single-User Mode.

4. Access the system with this command:

```
chroot /sysroot
```

5. When you are in the shell in Single-User Mode, change your root password using the `passwd root` command.

If you receive the “passwd: Authentication token manipulation error”, follow these troubleshooting steps.

6. Update SELinux information:

```
touch /.autorelabel
```

7. Exit `chroot`:

```
exit
```

8. Reboot your system:

```
reboot
```

Change ESET PROTECT database connection string

You can change the ESET PROTECT database connection string on your ESET PROTECT VA by editing the `StartupConfiguration.ini` file.

To change the ESET PROTECT database connection string, follow the instructions below:

1. Log in to the management mode by typing your password and pressing **Enter** twice.

2. Select **Exit to terminal** using the arrow keys and then press **Enter**.

3. Type:

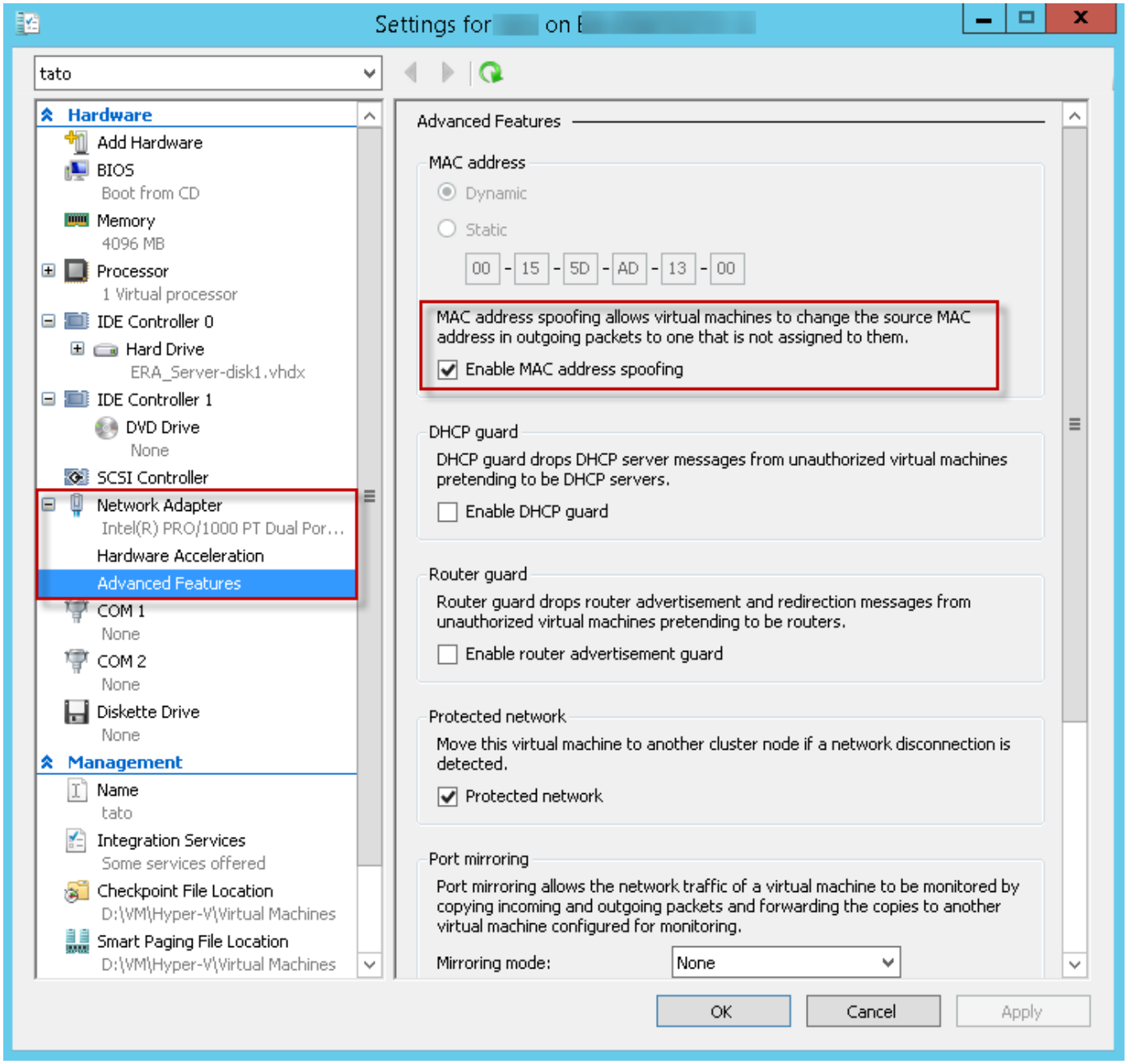
```
nano /etc/opt/eset/RemoteAdministrator/Server/StartupConfiguration.ini
```

3. Edit data in the ESET PROTECT database connection string.

4. Press `Ctrl+X` and `y` to save the changes.

Set up Hyper-V Server for RD Sensor

Ensure that MAC address spoofing is enabled in your Hyper-V Manager settings (see below).



Change port numbers for ESET PROTECT VA Web Console

Change the port on which ESET PROTECT Web Console (Apache Tomcat) runs (default—CentOS: 8443; Rocky Linux: 443)

1. Open Webmin.
2. Navigate to **Servers** > **ESET PROTECT** > click **Edit Apache Tomcat server.xml**
3. Edit the line `<Connector port=` to include the custom port and click **Save and Close**.
4. Restart the Tomcat service: `systemctl restart tomcat`

Change the port on which ESET PROTECT Web Console (Apache Tomcat) connects to ESET PROTECT Server (default: 2223)

1. Log into ESET PROTECT Web Console, navigate to **More** > **Settings** > **Connection** and edit the **Web Console port** to include the custom port.

2. Restart the ESET PROTECT VA.

3. Select **Exit to Terminal** from the Virtual Appliance Management Console.

4. Open the *EraWebServerConfig.properties* file:

```
sudo nano /var/lib/tomcat/webapps/era/WEB-
INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.proper
ties
```

5. Edit the line `server_port=` to include the custom port and save the changes.

6. Restart the Tomcat service: `systemctl restart tomcat`

If you have changed any of the ports above, you may need to modify:
- Firewall settings—Open Webmin, navigate to **Networking** > **Linux Firewall** and change port numbers in existing rules. Alternatively, you can add new rules.
- SELinux

Increase memory size for MySQL Server

To increase the memory size for a MySQL Server, follow these steps:

1. Log in to the management mode by typing your password and pressing **Enter** twice. Select **Exit to terminal** using the arrow keys and then press **Enter**.

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

3. Locate the line `innodb_buffer_pool_size=2G` and change the number to 50% of RAM of the VM. `2G` means two gigabytes.

4. Press `Ctrl+X` to exit the text editor, then press `Y` to save.

5. Reboot the appliance using the **Restart system** option in **management mode**.

Error with ESET PROTECT On-Prem running on a Hyper-V Server 2012 R2

After logging into ESET PROTECT Web Console, the error message "Unable to handle Kernel NULL pointer dereference at (null)" is displayed.

Disable Dynamic memory in virtual computer settings to resolve this issue.

Improve Oracle VirtualBox performance

You can change number of processors (CPU cores) in **Settings** of ESET PROTECT Virtual Appliance. Go to **System** > **Processor** tab. Lower the number of processors for the VA. For example, if you have 4 physical CPUs, change the setting to let the VA use only 2 processors.

Enable YUM command under HTTP Proxy server

If you have a local network that uses a proxy server as an intermediary for internet access, the `yum` command may not be configured properly and might not work.

To configure `yum` to work with the proxy:

1. Log in to the management mode by typing your password and pressing **Enter** twice. Select **Exit to terminal** using the arrow keys and then press **Enter**.

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

3. Add a line with information about your proxy. For example:
```
proxy=http://proxysvr.yourdom.com:3128
```

4. If the proxy requires username and password, add these settings. For example:
```
proxy=http://proxysvr.yourdom.com:3128
proxy_username=YourProxyUsername
proxy_password=YourProxyPassword
```

5. Press `Ctrl+X` and `y` to save the changes.

The `/etc/yum.conf` file is readable for all users and allows them to work with the `yum` command. As a result, other users can read your proxy password. Do not use the same password anywhere else.

For more information, read the official vendor's documentation.

Update the operating system on a machine running ESET PROTECT VA Server

If ESET PROTECT Web Console shows a warning that the ESET PROTECT VA Server **Operating system is not up to date**, you need to update the ESET PROTECT VA Server operating system. Run the Operating System Update task from the ESET PROTECT Web Console. After the update is finished, the warning message will disappear.

If the operating system update is performed from the Webmin interface, from terminal, or by a third-party tool, the warning message will not disappear even after the operating system has been updated. In this scenario, we recommend that you run the **Operating System Update** task from the ESET PROTECT Web Console.

Disable SELinux permanently

SELinux is enabled by default in the virtual appliance. To disable it permanently, follow these steps:

1. Select **Exit to Terminal** from the Virtual Appliance Management Console.

2. Run the command:
`nano /etc/selinux/config`

3. Change the line:
`SELINUX=permisive`
to
`SELINUX=disabled`

4. Save the changes and exit the editor.

5. Restart the computer with the following command to apply the new setting.
`reboot`

Restart Virtual Appliance Management Console

You can restart the graphical interface of virtual appliance without restarting the virtual machine. This will force refresh all data in the console. (For example, if a changed setting is not taking effect in the Virtual Appliance Management Console.)

1. Select **Exit to Terminal** from the Virtual Appliance Management Console.

2. Run the command:
`exit`

Enable SSH

To enable SSH on ESET PROTECT VA, see Enable/Disable remote access.

SSH troubleshooting

Open the terminal and run the following commands:

- `sudo systemctl status sshd` Verify that SSH is running. If SSH is not running, you can start it: `sudo systemctl start sshd`

- Run this terminal command to verify that the port 22 is in the list of the open ports: `firewall-cmd --list-ports`

End User License Agreement

Effective as of October 19, 2021.

IMPORTANT: Please read the terms and conditions of product application set out below carefully prior to download, installation, copy or use. **THROUGH DOWNLOADING, INSTALLING, COPYING OR USING THE SOFTWARE YOU ARE EXPRESSING YOUR CONSENT TO THESE TERMS AND CONDITIONS AND YOU ACKNOWLEDGE PRIVACY POLICY.**

End User License Agreement

Under the terms of this End User License Agreement ("Agreement") executed by and between ESET, spol. s r. o., having its registered office at Einsteinova 24, 85101 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31333532 ("ESET" or "Provider") and you, a physical person or legal entity ("You" or "End User"), You are entitled to use the Software defined in Article 1 of this Agreement. The Software defined in Article 1 of this Agreement can be stored on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources, subject to the terms and conditions specified below.

THIS IS AN AGREEMENT ON END USER RIGHTS AND NOT AN AGREEMENT FOR SALE. The Provider continues to own the copy of the Software and the physical media contained in the sales package and any other copies that the End User is authorized to make pursuant to this Agreement.

By clicking on "I Accept" or "I Accept…" while installing, downloading, copying or using the Software, You agree to the terms and conditions of this Agreement and acknowledge the Privacy Policy. If You do not agree to all of the terms and conditions of this Agreement and/or Privacy Policy, immediately click on the canceling option, cancel the installation or download, or destroy or return the Software, installation media, accompanying documentation and sales receipt to the Provider or the outlet from which You acquired the Software.

YOU AGREE THAT YOUR USE OF THE SOFTWARE ACKNOWLEDGES THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS.

1. **Software**. As used in this Agreement the term "Software" means: (i) computer program accompanied by this Agreement and all components thereof; (ii) all the contents of the disks, CD-ROMs, DVDs, e-mails and any attachments, or other media with which this Agreement is provided, including the object code form of the Software supplied on a data carrier, via electronic mail or downloaded via the Internet; (iii) any related explanatory written materials and any other possible documentation related to the Software, above all any description of the Software, its specifications, any description of the Software properties or operation, any description of the operating environment in which the Software is used, instructions for use or installation of the Software or any description of how to use the Software ("Documentation"); (iv) copies of the Software, patches for possible errors in the Software, additions to the Software, extensions to the Software, modified versions of the Software and updates of Software components, if any, licensed to You by the Provider pursuant to Article 3 of this Agreement. The Software shall be provided exclusively in the form of executable object code.

2. **Installation, Computer and a License key**. Software supplied on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources requires installation. You must install the Software on a correctly configured Computer, complying at least with requirements set out in the Documentation. The installation methodology is described in the Documentation. No computer programs or hardware which could have an adverse effect on the Software may be installed on the Computer on which You install the Software. Computer means hardware, including but not limited to personal computers, laptops, workstations, palmtop computers, smartphones, hand-held electronic devices, or other electronic devices for which the Software is designed, on which it will be installed and/or used. License key means the unique sequence of symbols, letters, numbers or special signs provided to the End User in order to allow the legal use of the Software, its specific version or extension of the term of the License in compliance with this Agreement.

3. **License**. Subject to the condition that You have agreed to the terms of this Agreement and You comply with all the terms and conditions stipulated herein, the Provider shall grant You the following rights ("License"):

a) **Installation and use**. You shall have the non-exclusive, non-transferable right to install the Software on the hard disk of a Computer or other permanent medium for data storage, installation and storage of the Software in the memory of a computer system and to implement, store and display the Software.

b) **Stipulation of the number of licenses.** The right to use the Software shall be bound by the number of End Users. One End User shall be taken to refer to the following: (i) installation of the Software on one Computer; or (ii) if the extent of a license is bound to the number of mailboxes, then one End User shall be taken to refer to a Computer user who accepts electronic mail via a Mail User Agent ("MUA"). If MUA accepts electronic mail and subsequently distributes it automatically to several users, then the number of End Users shall be determined according to the actual number of users for whom the electronic mail is distributed. If a mail server performs the function of a mail gate, the number of End Users shall equal the number of mail server users for which the said gate provides services. If an unspecified number of electronic mail addresses are directed to and accepted by one user (e.g., through aliases) and messages are not automatically distributed by the client to a larger number of users, a License for one computer shall be required. You must not use the same License at the same time on more than one Computer. The End User is entitled to enter the License key to the Software only to the extent to which the End User has the right to use the Software in accordance with the limitation arising from the number of Licenses granted by Provider. The License key is deemed confidential, You must not share the License with third parties or allow third parties to use the License key unless permitted by this Agreement or Provider. If your License key is compromised, notify Provider immediately.

c) **Home/Business Edition.** A Home Edition version of the Software shall be used exclusively in private and/or non-commercial environments for home and family use only. A Business Edition version of the Software must be obtained for use in a commercial environment as well as to use the Software on mail servers, mail relays, mail gateways, or Internet gateways.

d) **Term of the License.** Your right to use the Software shall be time-limited.

e) **OEM Software.** Software classified as "OEM" shall be limited to the Computer You obtained it with. It cannot be transferred to a different Computer.

f) **NFR, TRIAL Software.** Software classified as "Not-for-resale", NFR or TRIAL cannot be assigned for payment and must only be used for demonstration or testing the Software's features.

g) **Termination of the License.** The License shall terminate automatically at the end of the period for which granted. If You fail to comply with any of the provisions of this Agreement, the Provider shall be entitled to withdraw from the Agreement, without prejudice to any entitlement or legal remedy open to the Provider in such eventualities. In the event of cancellation of the License, You must immediately delete, destroy or return at your own cost, the Software and all backup copies to ESET or to the outlet from which You obtained the Software. Upon termination of the License, the Provider shall also be entitled to cancel the End User's entitlement to use the functions of the Software, which require connection to the Provider's servers or third-party servers.

4. **Functions with data collection and internet connection requirements.** To operate correctly, the Software requires connection to the Internet and must connect at regular intervals to the Provider's servers or third-party servers and applicable data collection in compliance with Privacy Policy. Connection to the Internet and applicable data collection is necessary for functioning of the Software and for updating and upgrading the Software. The Provider shall be entitled to issue updates or upgrades to the Software ("Updates"), but shall not be obliged to provide Updates. This function is enabled under the Software's standard settings and Updates are therefore installed automatically, unless the End User has disabled the automatic installation of Updates. For provisioning of Updates, License authenticity verification is required, including information about Computer and/or the platform

on which the Software is installed in compliance with Privacy Policy.

Provision of any Updates may be subject to End of Life Policy ("EOL Policy"), which is available on https://go.eset.com/eol_business. No Updates will be provided after the Software or any of its features reaches the End of Life date as defined in the EOL Policy.

For the purpose of this Agreement, it is necessary to collect, process and store data enabling the Provider to identify You in compliance with Privacy Policy. You hereby acknowledge that the Provider checks using its own means whether You are using the Software in accordance with the provisions of this Agreement. You hereby acknowledge that for the purpose of this Agreement it is necessary for your data to be transferred, during communication between the Software and the Provider's computer systems or those of its business partners as part of Provider's distribution and support network to ensure functionality of Software and authorization to use the Software and to protection of the Provider's rights.

Following conclusion of this Agreement, the Provider or any of its business partners as part of Provider's distribution and support network shall be entitled to transfer, process and store essential data identifying You for billing purposes, performance of this Agreement and transmitting notifications on your Computer.

Details about privacy, personal data protection and Your rights as a data subject can be found in Privacy Policy which is available on Provider's website and accessible directly from the installation process. You can also visit it from Software's help section.

5. **Exercising End User rights**. You must exercise End User rights in person or via your employees. You are only entitled to use the Software to safeguard your operations and protect those Computers or computers systems for which You have obtained a License.

6. **Restrictions to rights.** You may not copy, distribute, extract components or make derivative works of the Software. When using the Software, You are required to comply with the following restrictions:

a) You may make one copy of the Software on a permanent storage medium as an archival backup copy, provided your archival back-up copy is not installed or used on any Computer. Any other copies You make of the Software shall constitute a breach of this Agreement.

b) You may not use, modify, translate or reproduce the Software or transfer rights to use the Software or copies of the Software in any manner other than as provided for in this Agreement.

c) You may not sell, sub-license, lease or rent or borrow the Software or use the Software for the provision of commercial services.

d) You may not reverse engineer, reverse compile or disassemble the Software or otherwise attempt to discover the source code of the Software, except to the extent that this restriction is expressly prohibited by law.

e) You agree that You will only use the Software in a manner that complies with all applicable laws in the jurisdiction in which You use the Software, including, but not limited to, applicable restrictions concerning copyright and other intellectual property rights.

f) You agree that You will only use the Software and its functions in a way which does not limit the possibilities of other End Users to access these services. The Provider reserves the right to limit the scope of services provided to individual End Users, to enable use of the services by the highest possible number of End Users. Limiting the scope of services shall also mean complete termination of the possibility to use any of the functions of the Software and deletion of Data and information on the Provider's servers or third-party servers relating to a specific function of the Software.

g) You agree not to exercise any activities involving use the License key, contrary to the terms of this Agreement or leading to provide License key to any person who is not entitled to use the Software, such as the transfer of used or unused License key in any form, as well as the unauthorized reproduction, or distribution of duplicated or generated License keys or using the Software as a result of the use of a License key obtained from the source other than the Provider.

7. **Copyright**. The Software and all rights, without limitation including proprietary rights and intellectual property rights thereto are owned by ESET and/or its licensors. They are protected by international treaty provisions and by all other applicable national laws of the country in which the Software is being used. The structure, organization and code of the Software are the valuable trade secrets and confidential information of ESET and/or its licensors. You must not copy the Software, except as set forth in Article 6(a). Any copies which You are permitted to make pursuant to this Agreement must contain the same copyright and other proprietary notices that appear on the Software. If You reverse engineer, reverse compile, disassemble or otherwise attempt to discover the source code of the Software, in breach of the provisions of this Agreement, You hereby agree that any information thereby obtained shall automatically and irrevocably be deemed to be transferred to and owned by the Provider in full, from the moment such information comes into being, notwithstanding the Provider's rights in relation to breach of this Agreement.

8. **Reservation of rights**. The Provider hereby reserves all rights to the Software, with the exception of rights expressly granted under the terms of this Agreement to You as the End User of the Software.

9. **Multiple language versions, dual media software, multiple copies**. In the event that the Software supports multiple platforms or languages, or if You receive multiple copies of the Software, You may only use the Software for the number of computer systems and for the versions for which You obtained a License. You may not sell, rent, lease, sub-license, lend or transfer versions or copies of the Software which You do not use.

10. **Commencement and termination of the Agreement.** This Agreement shall be effective from the date You agree to the terms of this Agreement. You may terminate this Agreement at any time by permanently uninstalling, destroying and returning, at your own cost, the Software, all backup copies and all related materials provided by the Provider or its business partners. Your right to use Software and any of its features may be subject to EOL Policy. After the Software or any of its features reaches the End of Life date defined in the EOL Policy, your right to use the Software will terminate. Irrespective of the manner of termination of this Agreement, the provisions of Articles 7, 8, 11, 13, 19 and 21 shall continue to apply for an unlimited time.

11. **END USER DECLARATIONS**. AS THE END USER YOU ACKNOWLEDGE THAT THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. NEITHER THE PROVIDER, ITS LICENSORS OR AFFILIATES, NOR THE COPYRIGHT HOLDERS MAKE ANY REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR THAT THE SOFTWARE WILL NOT INFRINGE ANY THIRD-PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. THERE IS NO WARRANTY BY THE PROVIDER OR BY ANY OTHER PARTY THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE. YOU ASSUME ALL RESPONSIBILITY AND RISK FOR THE SELECTION OF THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS AND FOR THE INSTALLATION, USE AND RESULTS OBTAINED FROM IT.

12. **No other obligations**. This Agreement creates no obligations on the part of the Provider and its licensors other than as specifically set forth herein.

13. **LIMITATION OF LIABILITY**. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE PROVIDER, ITS EMPLOYEES OR LICENSORS BE LIABLE FOR ANY LOST PROFITS, REVENUE, SALES, DATA OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, PROPERTY DAMAGE, PERSONAL INJURY, INTERRUPTION OF BUSINESS, LOSS OF BUSINESS INFORMATION OR FOR ANY SPECIAL, DIRECT, INDIRECT,

INCIDENTAL, ECONOMIC, COVER, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND WHETHER ARISING UNDER CONTRACT, TORT, NEGLIGENCE OR OTHER THEORY OF LIABILITY, ARISING OUT OF THE INSTALLATION, THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF THE PROVIDER OR ITS LICENSORS OR AFFILIATES ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME COUNTRIES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF LIABILITY, BUT MAY ALLOW LIABILITY TO BE LIMITED, IN SUCH CASES, THE LIABILITY OF THE PROVIDER, ITS EMPLOYEES OR LICENSORS OR AFFILIATES SHALL BE LIMITED TO THE SUM THAT YOU PAID FOR THE LICENSE.

14. Nothing contained in this Agreement shall prejudice the statutory rights of any party dealing as a consumer if running contrary thereto.

15. **Technical support**. ESET or third parties commissioned by ESET shall provide technical support at their own discretion, without any guarantees or declarations. No technical support will be provided after the Software or any of its features reaches the End of Life date defined in the EOL Policy. The End User shall be required to back up all existing data, software and program facilities prior to the provision of technical support. ESET and/or third parties commissioned by ESET cannot accept liability for damage or loss of data, property, software or hardware or loss of profits due to the provision of technical support. ESET and/or third parties commissioned by ESET reserve the right to decide that resolving the problem is beyond the scope of technical support. ESET reserves the right to refuse, suspend or terminate the provision of technical support at its own discretion. License information, Information and other data in compliance with Privacy Policy may be required for the purpose of technical support provision.

16. **Transfer of the License**. The Software can be transferred from one Computer to another, unless contrary to the terms of the Agreement. If not contrary to the terms of the Agreement, the End User shall only be entitled to permanently transfer the License and all rights ensuing from this Agreement to another End User with the Provider's consent, subject to the condition that (i) the original End User does not retain any copies of the Software; (ii) the transfer of rights must be direct, i.e. from the original End User to the new End User; (iii) the new End User must assume all the rights and obligations incumbent on the original End User under the terms of this Agreement; (iv) the original End User has to provide the new End User with documentation enabling verification of the genuineness of the Software as specified under Article 17.

17. **Verification of the genuineness of the Software.** The End User may demonstrate entitlement to use the Software in one of the following ways: (i) through a license certificate issued by the Provider or a third party appointed by the Provider; (ii) through a written license agreement, if such an agreement was concluded; (iii) through the submission of an e-mail sent by the Provider containing licensing details (user name and password). License information and End User identification data in compliance with Privacy Policy may be required for the purpose of Software genuineness verification.

18. **Licensing for public authorities and the US Government**. The Software shall be provided to public authorities, including the United States Government, with the license rights and restrictions described in this Agreement.

19. **Trade control compliance**.

a) You will not, directly or indirectly, export, re-export, transfer or otherwise make available the Software to any person, or use it in any manner, or be involved in any activity, that could result in ESET or its holding companies, its subsidiaries, and the subsidiaries of any of its holding companies, as well as entities controlled by its holding companies ("Affiliates") being in violation of, or being subject to, negative consequences under trade control laws which include:

i. any laws that control, restrict, or impose licensing requirements on export, re-export or transfer of goods, software, technology, or services, issued or adopted by any government, state or regulatory authority of the United States of America, Singapore, the United Kingdom, the European Union or any of its Member States, or any country in which obligations under the Agreement are to be performed, or in which ESET or any of its

Affiliates are incorporated or operate, and

ii. any economic, financial, trade or other, sanction, restriction, embargo, import or export ban, prohibition on transfer of funds or assets or on performing services, or equivalent measure imposed by any government, state or regulatory authority of the United States of America, Singapore, the United Kingdom, the European Union or any of its Member States, or any country in which obligations under the Agreement are to be performed, or in which ESET or any of its Affiliates are incorporated or operate.

(legal acts referred to in points i, and ii. above together as "Trade Control Laws").

b) ESET shall have the right to suspend its obligations under, or terminate, these Terms with immediate effect in the event that:

i. ESET determines that, in its reasonable opinion, the User has breached or is likely to breach provision of Article 19 a) of the Agreement; or

ii. the End User and/or the Software become subject to Trade Control Laws and, as a result, ESET determines that, in its reasonable opinion, the continued performance of its obligations under the Agreement could result in ESET or its Affiliates being in violation of, or being subject to negative consequences under, Trade Control Laws.

c) Nothing in the Agreement is intended, and nothing should be interpreted or construed, to induce or require either party to act or refrain from acting (or to agree to act or refrain from acting) in any manner which is inconsistent with, penalized, or prohibited under any applicable Trade Control Laws.

20. **Notices**. All notices and returns of the Software and Documentation must be delivered to: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, without prejudice to ESET´s right to communicate to You any changes to this Agreement, Privacy Policies, EOL Policy and Documentation in accordance with art. 22 of the Agreement. ESET may send You emails, in-app notifications via Software or post the communication on our website. You agree to receive legal communications from ESET in electronic form, including any communications on change in Terms, Special Terms or Privacy Policies, any contract proposal/acceptance or invitations to treat, notices or other legal communications. Such electronic communication shall be deemed as received in writing, unless applicable laws specifically require a different form of communication.

21. **Applicable law**. This Agreement shall be governed by and construed in accordance with the laws of the Slovak Republic. The End User and the Provider hereby agree that the principles of the conflict of laws and the United Nations Convention on Contracts for the International Sale of Goods shall not apply. You expressly agree that any disputes or claims ensuing from this Agreement with respect to the Provider or any disputes or claims relating to use of the Software shall be settled by Bratislava I District Court and You expressly agree to the said court exercising jurisdiction.

22. **General provisions**. Should any of the provisions of this Agreement be invalid or unenforceable, this shall not affect the validity of the other provisions of the Agreement, which shall remain valid and enforceable under the conditions stipulated therein. This Agreement has been executed in English. In case any translation of the Agreement is prepared for the convenience or any other purpose or in any case of a discrepancy between language versions of this Agreement, the English version shall prevail.

ESET reserves the right to make changes to the Software as well as to revise terms of this Agreement, its Annexes, Addendums, Privacy Policy, EOL Policy and Documentation or any part thereof at any time by updating the relevant document (i) to reflect changes to the Software or to how ESET does business, (ii) for legal, regulatory or security reasons, or (iii) to prevent abuse or harm. You will be notified about any revision of the Agreement by email, in-app notification or by other electronic means. If You disagree with the proposed changes to the Agreement, You may terminate it in accordance with Art. 10 within 30 days after receiving a notice of the change. Unless You terminate the Agreement within this time limit, the proposed changes will be deemed accepted and

become effective towards You as of the date You received a notice of the change.

This is the entire Agreement between the Provider and You relating to the Software and it supersedes any prior representations, discussions, undertakings, communications or advertising relating to the Software.

ADDENDUM TO THE AGREEMENT

Forwarding of Information to the Provider. Additional provisions apply to the Forwarding of Information to the Provider as follows:

The Software contains functions which collect data about the installation process, the Computer and/or the platform on which the Software is installed, information about the operations and functionality of the Software and information about managed devices (hereinafter referred to as "Information") and then send them to the Provider. The Information may contain data (including randomly or accidentally obtained personal data) concerning managed devices. By activating this function of the Software, Information may be collected and processed by the Provider as specified in Privacy Policy and in compliance with relevant legal regulations.

The Software requires a component installed on managed computer, which enables transfer of information between managed computer and remote management software. Information, which are subject to transfer contains management data such as hardware and software information of managed computer and managing instructions from the remote management software. Other content of data transferred from managed computer shall be determined by the settings of software installed on managed computer. The content of instructions from management software shall be determined by settings of remote management software.

EULAID: EULA-PRODUCT-PROTECT; 3537.0

Privacy Policy

ESET, spol. s r. o., having its registered office at Einsteinova 24, 851 01 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31333532 as a Data Controller ("ESET" or "We") would like to be transparent when it comes to processing of personal data and privacy of our customers. To achieve this goal, We are publishing this Privacy Policy with the sole purpose of informing our customer ("End User" or "You") about following topics:

- Processing of Personal Data,
- Data Confidentiality,
- Data Subject's Rights.

Processing of Personal Data

Services provided by ESET implemented in our product are provided under the terms of End User License Agreement ("EULA"), but some of them might require specific attention. We would like to provide You with more details on data collection connected with the provision of our services. We render various services described in the EULA and product documentation such as update/upgrade service, ESET LiveGrid®, protection against misuse of data, support, etc. To make it all work, We need to collect the following information:

- Management of ESET security products requires and locally stores information such as seat ID and name, product name, license information, activation and expiration information, hardware and software information concerning managed computer with ESET security product installed. Logs concerning activities of managed ESET security products and devices are collected and available in order to facilitate managing and supervising

features and services without automated submission to ESET.

• Information concerning installation process, including platform on which our product is installed and information about the operations and functionality of our products such as hardware fingerprint, installation IDs, crash dumps, license IDs, IP address, MAC address, configuration settings of product which may also include managed devices.

• Licensing information such as license ID and personal data such as name, surname, address, email address is required for billing purposes, license genuineness verification and provision of our services.

• Contact information and data contained in your support requests may be required for service of support. Based on the channel You choose to contact us, We may collect your email address, phone number, license information, product details and description of your support case. You may be asked to provide us with other information to facilitate service of support such as generated log files.

• Data concerning usage of our service are completely anonymous by the end of session. No personally identifiable information is stored after the session ends.

Data Confidentiality

ESET is a company operating worldwide via affiliated entities or partners as part of our distribution, service and support network. Information processed by ESET may be transferred to and from affiliated entities or partners for performance of the EULA such as provision of services or support or billing. Based on your location and service You choose to use, We might be required to transfer your data to a country with absence of adequacy decision by the European Commission. Even in this case, every transfer of information is subject to regulation of data protection legislation and takes place only if required. Standard Contractual Clauses, Binding Corporate Rules or another appropriate safeguard must be established without any exception.

We are doing our best to prevent data from being stored longer than necessary while providing services under the EULA. Our retention period might be longer than the validity of your license just to give You time for easy and comfortable renewal. Minimized and pseudonymized statistics and other data from ESET LiveGrid® may be further processed for statistical purposes.

ESET implements appropriate technical and organizational measures to ensure a level of security which is appropriate to potential risks. We are doing our best to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and Services. However, in case of data breach resulting in a risk to your rights and freedoms, We are ready to notify supervisory authority as well as data subjects. As a data subject, You have a right to lodge a complaint with a supervisory authority.

Data Subject’s Rights

ESET is subject to regulation of Slovak laws and We are bound by data protection legislation as part of European Union. Subject to conditions laid down by applicable data protection laws, You are entitled to following rights as a data subject:

• right to request access to your personal data from ESET,

• right to rectification of your personal data if inaccurate (You also have the right to have the incomplete personal data completed),

• right to request erasure of your personal data,

• right to request restriction of processing your personal data,

• right to object to processing,

- right to lodge a complaint as well as,
- right to data portability.

If You would like to exercise your right as a data subject or You have a question or concern, send us a message at:

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