

ESET Virtualization Security for VMware vShield

User Guide

Linux distribution: CentOS 6.6 64-bit

[Click here to download the most recent version of this document](#)

ESET VIRTUALIZATION SECURITY FOR VMWARE VSHIELD

Copyright ©2016 by ESET, spol. s r. o.

ESET Virtualization Security Appliance was developed by ESET, spol. s r. o.

For more information visit www.eset.com.

All rights reserved. No part of this documentation may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise without permission in writing from the author.

ESET, spol. s r. o. reserves the right to change any of the described application software without prior notice.

Worldwide Customer Support: www.eset.com/support

REV. 9/12/2016

Contents

1. What is ESET Virtualization Security and how does it work?.....	5
1.1 Architecture.....	5
1.2 Features & Benefits.....	6
2. How to setup your VMware environment....	7
2.1 VMware prerequisites.....	7
2.1.1 ESXi host.....	7
2.1.2 vCenter Installer.....	7
2.1.2.1 vSphere Web Client.....	8
2.1.2.2 vCenter Inventory Service.....	8
2.1.2.3 vCenter Server.....	8
2.1.3 Guest virtual machines.....	8
2.2 vShield Manager & vShield Endpoint.....	10
3. Installation/Deployment.....	12
3.1 System Requirements.....	12
3.2 Installation of standalone components, with manual configuration.....	13
3.2.1 ESET Remote Administrator VA deployment.....	13
3.2.2 vAgent Host deployment.....	15
3.2.3 ESET Virtualization Security deployment.....	20
3.2.4 VMware Tools installation.....	23
3.3 Installation of ESET Virtualization Security using deployment tool.....	24
4. Basics of ESET Remote Administrator.....	25
4.1 ESET Remote Administrator Server.....	25
4.2 Web Console.....	26
4.3 Getting to know ERA Web Console.....	27
4.4 Proxy.....	30
4.5 ERA Agent.....	31
4.6 Virtual Agent Host.....	31
4.7 RD Sensor.....	31
5. Working with ESET Virtualization Security...32	32
5.1 Managing ESET Virtualization Security from the console.....	32
5.2 Administering Clients.....	34
5.2.1 Tasks.....	34
5.2.1.1 Virus Signature Database update.....	34
5.2.1.2 On-Demand scan.....	35
5.2.1.3 Operating system update (EVS appliance).....	36
5.2.1.4 Quarantine management.....	38
5.2.2 Policies.....	39
5.2.2.1 ESET Virtualization Security - Security Appliance policy.....	40
5.2.2.1.1 Antivirus.....	41
5.2.2.1.2 Update.....	41
5.2.2.1.2.1 Primary/Secondary Server.....	41
5.2.2.1.3 Virtual Agent Host.....	42
5.2.2.1.4 Tools.....	42
5.2.2.1.4.1 Log files.....	42
5.2.2.1.4.2 Proxy server.....	42
5.2.2.1.4.3 System console.....	43
5.2.2.2 ESET Virtualization Security - Protected VM policy.....	43
5.2.2.2.1 Antivirus.....	44
5.2.2.2.2 Real-time file system protection.....	44
5.2.2.2.2.1 Basic.....	44
5.2.2.2.2.2 ThreatSense parameters.....	44
5.2.2.2.2.3 Additional ThreatSense parameters.....	46
5.2.2.2.2.4 Clean file cache.....	46
5.2.2.2.3 On-demand computer scan.....	46
5.2.2.2.3.1 Basic.....	46
5.2.2.2.3.2 ThreatSense parameters.....	46
5.2.3 Dynamic groups.....	49
6. Common Questions.....	50
6.1 How to find vAgent Host in ESET Remote Administrator.....	50
6.2 How to find ESET Virtualization Security in ESET Remote Administrator.....	50
6.3 How to identify problematic VMs in ESET Remote Administrator.....	50
6.4 How to add virtual machines to ESET Remote Administrator.....	51
6.5 How to sync with vCenter.....	51
6.6 How vAgent Host works.....	52
6.7 How to activate and initial setup.....	52
6.7.1 How to get a license.....	52
6.7.2 How unilicense works.....	52
6.7.3 Online activation.....	53
6.7.4 Offline activation.....	55
6.8 How to update ESET Virtualization Security.....	59
6.9 How to update vAgent Host.....	61
6.10 How to update ESET Remote Administrator Web Console.....	63
6.11 How the components interact.....	68
6.12 How ESET Virtualization Security interacts with VMware products.....	69
6.13 What ports are needed for each component.....	69
6.14 How to collect logs.....	70
6.15 How to read the logs.....	70
6.16 How to uninstall ESET Virtualization Security.....	71
6.16.1 Deactivate virtual machines from ERA.....	71
6.16.2 Remove ESET Virtualization Security.....	71
6.16.3 Turn off vAgent Host.....	71
6.16.4 Delete virtual machines.....	71
6.17 How to access system logs.....	72
7. Troubleshooting.....	73

7.1	Where to find the logs for ESET Remote Administrator	73
7.2	Where to find the logs for vAgent.....	73
7.3	What to send to Customer Care.....	73
7.4	What ports to enable for licensing.....	73
7.5	What ports to enable for HTTP Proxy (update caching).....	74
7.6	How to use the offline mirror tool to receive updates.....	74
7.7	Cannot register to VMware vShield.....	76
7.8	ESET Virtualization Security shows no connected/protected virtual machines.....	76
7.9	No accessibility on license servers.....	76
8.	Glossary.....	77
8.1	ESXi host.....	77
8.2	Hypervisor	77
8.3	Virtual machine	77
8.4	Virtual appliance.....	77
8.5	VMware Tools.....	77
8.6	vMotion Migration.....	77

1. What is ESET Virtualization Security and how does it work?

ESET Virtualization Security (EVS) performs agentless anti-malware scanning of machines using VMware infrastructure. This agentless solution does not require the installation of ESET solutions on [virtual machines](#), as all the scanning tasks are offloaded to a centralized scanning engine via [VMware Tools](#). EVS takes advantage of the resident protection driver and dedicated TCP/IP communication network included with VMware Tools to facilitate communication with the scanner. What's more, ESET Virtualization Security is fully integrated with VMware vSphere and automatically optimizes scanning performance based on [hypervisor](#) load. ESET Virtualization Security can be combined with other ESET Endpoint security solutions.

The ESET Virtualization Security User Guide provides useful pointers on how to deploy, configure and maintain ESET Virtualization Security in a virtual environment. This Guide is intended for experienced system administrators familiar with virtualization technology.

ESET Virtualization Security can be managed from ESET Remote Administrator 6 Web Console. This allows you monitor the security status of individual virtual machines and quickly execute tasks.

Figure 1 below shows an example of a virtual environment with ESET Virtualization Security installed:

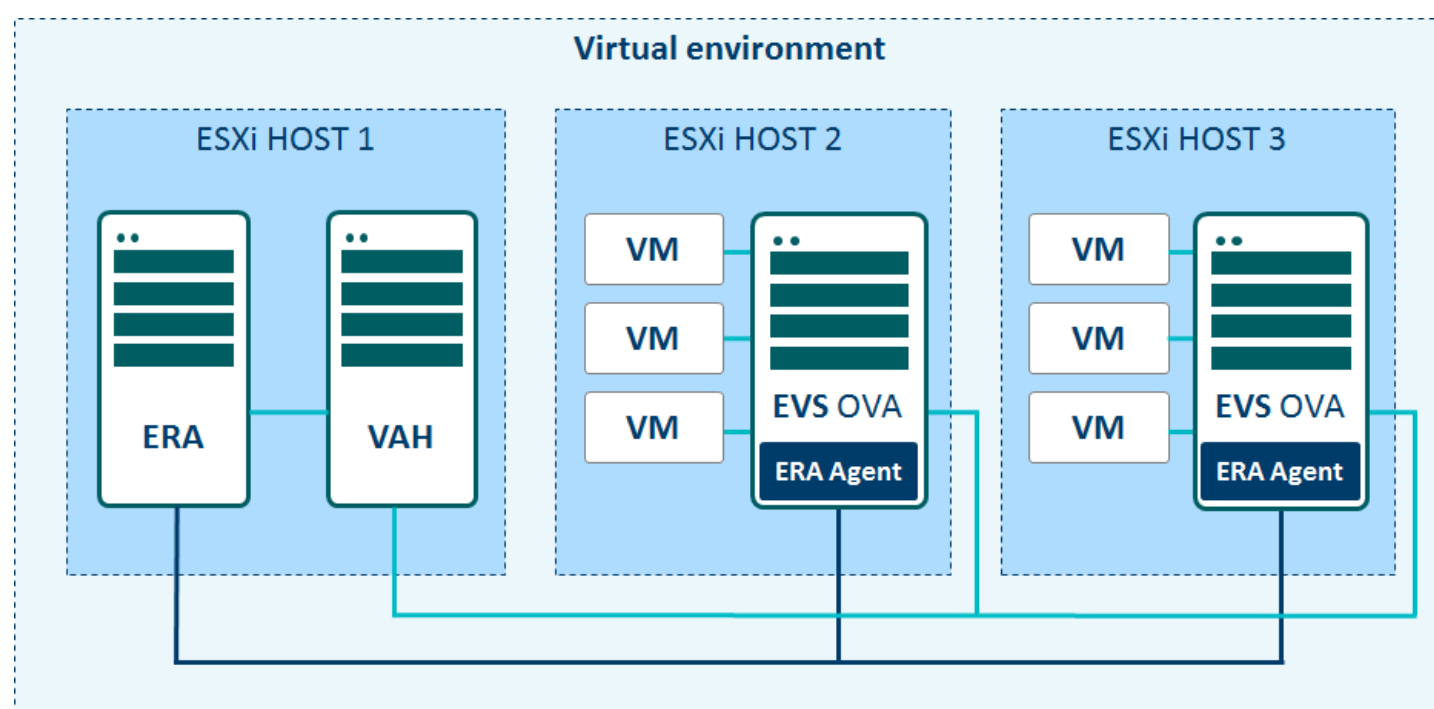


Figure 1

1.1 Architecture

Figure 2 below gives an example of ESET Virtualization Security in a sample environment with the following characteristics:

- VMware vShield Endpoints in VMware environment (hypervisor + managed using VMware vSphere)
- VMware Tools installed on each virtual machine
- ESET Remote Administrator 6.3 and higher management server installed
- ESET Remote Administrator Virtual Agent Host
- ESET Virtualization Security integrates components from VMware (vShield library) and the ESET Scanning Engine, registers that with vShield, which creates a dedicated on-hypervisor network to allow rapid file exchange

With this configuration in place, all virtual machines with VMware Tools installed are protected by on-access scanner and the administrator can initiate on-demand scans from ESET Remote Administrator.

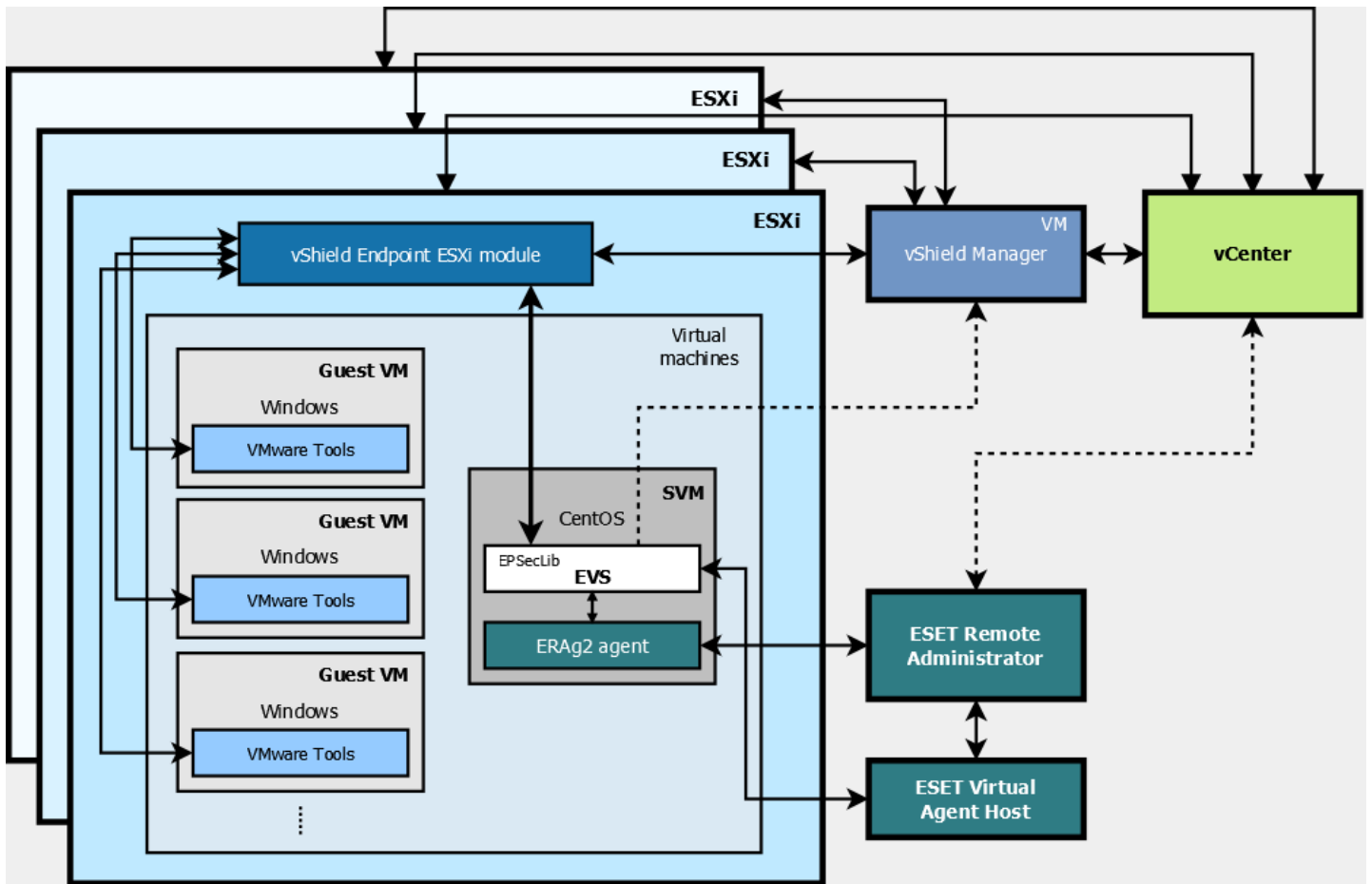


Figure 2

1.2 Features & Benefits

Light on resources

ESET Virtualization Security reduces the complexity of virtualization security by enabling a merged security infrastructure.

ESET Virtualization Security also:

- prevents bottlenecks associated with endpoint security agents by eliminating the need to install antivirus software on individual machines
- reduces the amount of RAM which would be needed by multiple scanners (for example, ESET Endpoint Security) on multiple virtual machines on the same hypervisor
- reduces CPU and disk usage when scanning machines simultaneously using the centralized scanner
- reduces the vulnerability of the scanning engine present on dedicated and secured virtual machines

Easy migration

Migration of each virtual machine using [vMotion Migration](#) is as simple as registering a new security virtual appliance (SVA) within the vShield manager.

Licensing

Each virtual machine using the same licensing as an endpoint. You can use ESET Endpoint Security solution to protect your physical machines and you can protect your virtual machines using ESET Virtualization Security with vShield agentless protection.

2. How to setup your VMware environment

This chapter will help you configure your VMware environment, virtual machines and vShield security software (vShield Manager + vShield Endpoint).

After you have completed VMware set up procedure, you can deploy ESET Virtualization Security on it.

NOTE

If you have already configured VMware and vShield, continue to [Installation/Deployment](#).

2.1 VMware prerequisites

To manage your virtual machines, install:

- [ESXi host](#)
- [vCenter](#)
- [vSphere Web Client](#)
- [Guest virtual machines](#)

2.1.1 ESXi host

Requirements

Your system should meet the following minimum hardware requirements:

- 64-bit processor, 2 cores
- minimum 4 GB of memory
- minimum 1 Gbps Network connection

NOTE: For more details see the [VMware Compatibility Guide](#).

Install ESXi host

1. Go to [Vmware web page](#) and log in.
2. Download the ISO image for ESXi from the [VMware download page](#).
3. Burn the ISO image to a CD or DVD and insert it into your CD/DVD-ROM drive, or format a USB flash drive to boot the installation and attach it. Restart your server.
4. In the boot menu, select **ESXi Standard Installer**.
5. On the **Select a Disk** page, select the drive on which to install ESXi and press **Enter**.
6. Select the keyboard type for the host. You can change it after installation in the direct console.
7. Enter the root password for the host.

When the installation is complete, reboot the host. You can set up basic configuration in **System Customization**. A restart is required for the changes to take effect.

2.1.2 vCenter Installer

Requirements

Your system should meet the following minimum hardware requirements:

- 64-bit processor, 2 or more cores
- minimum 12 GB of memory
- 100 GB of disk storage
- minimum 1 Gbps Network connection

Your server should meet the following minimum requirements:

- Windows Server 2008 SP2
- MSI 4.5

vCenter installer

1. Download the ISO image for ESXi from the [VMware download page](#).
2. Double-click *autorun.exe* in the folder where you placed the installer files.
3. Select **Simple Install**.
4. The installation wizard will guide you through the installation of the components.

vCenter Single Sign On

- A password for an administrator account must be set
- A name for the vCenter Single Sign On site must be entered
- You must accept or change the HTTPS port used for vCenter Single Sign On
- You must select the destination folder for vCenter components.

The installation process will continue with installation wizard for **vSphere Web Client**.

2.1.2.1 vSphere Web Client

The installation wizard will install vSphere Web Client in non-interactive mode. Installation process will continue with installation wizard for **vCenter Inventory Service**.

2.1.2.2 vCenter Inventory Service

Installation wizard will install vCenter Inventory Service in non-interactive mode. The installation process will continue with installation wizard for **vCenter Server**.

2.1.2.3 vCenter Server

Installation wizard for vCenter Server will prompt you to:

- enter your license key
- specify a new or existing database for vCenter Server
- select the account vCenter will run on
- accept or configure ports used for communications
- select the amount of memory available for the vCenter inventory (depending on the number virtual machines)

2.1.3 Guest virtual machines

To create guest virtual machines access vSphere Web Client and follow the steps below:

1. Open your browser and enter the web address for your vCenter Server in the following format *https://your_ip_address_or_hostname_of_a_vCenter_Server*.
2. Click **Log in to vSphere Web Client** and log in.
3. Select **VMs and Templates** under **Navigator**.
4. Click **Install this certificate and do not display any security warnings** and then click **Ignore**.
5. Right-click a host and select **New Virtual Machine** > **New Virtual Machine** from the context menu.
6. A wizard will prompt you to:
 - enter the name of the virtual machine
 - specify the datacenter where you want to create the virtual machine
 - specify the host where you want to run the virtual machine
 - select compatibility with the host for the virtual machine
 - select a guest operating system version that corresponds to your installation media and finish the wizard

7. Select created virtual machine.
8. Prepare your Windows installation disk or ISO image and click the icon.
9. Select the drive letter or Connect to ISO image on local disk.
10. Right-click a virtual machine and select **Power > Power On** from the context menu.
11. Launch your virtual machine and finish the installation of Windows operating system.

2.2 vShield Manager & vShield Endpoint

The vShield Manager is a network management component of vShield installed on ESXi host in your virtual environment. vShield Endpoint is the integrated AV client used by vShield.

Installation of vShield Manager

1. Go to [Vmware web page](#) and log in then continue to [VMware download page](#).
2. Go to and download the ISO image for ESXi host.
3. Use the vSphere Web Client to log in to your vCenter Server, select **Host and Clusters** > right-click the host and select **Deploy OVF Template** from the context menu or use vSphere Client to log in to your vCenter Server and select **File > Deploy OVF Template**.
4. The wizard will guide you through the deployment.
5. Browse to a location where the source OVF file is stored. After validation select **Accept extra configuration options** and accept license agreements.
6. Specify a name for the deployed template.
7. Select the location to run the deployed template.
8. Select the **Thin Provision** disk format.
9. Check the network setup.
10. Enter and confirm the password for CLI admin for this virtual machine.
11. Enter and confirm the password for CLI privilege mode for this virtual machine.
12. Select **Power on** after deployment and click **Finish**.

Configuring the vShield Manager

1. If you do not have DHCP Server, you will need to configure network setting for vShield Manager. You can do that by following these steps:
 - a) Navigate to **Summary > Launch Remote Console**.
 - b) Log in (default username is **admin** and password **default**).
 - c) When you see "**manager >**" type **enable** and enter password. Then type setup and follow instructions for entering IP address, mask, default gateway, primary and secondary DNS server. Then save the configuration.
2. Open the **vShield Manager** web interface in your browser (type the IP address) and log in (default username is **admin** and password is **default**). We recommend to change the password immediately after login.
3. In a **Configuration** tab under **Settings & Reports** (Host & Clusters view) specify the IP address or the hostname of the NTP server of your company.
4. Go back to your vSphere Web Client and go to **Actions** (above the **Summary** tab) > **Power**, select and confirm the **Restart Guest OS** option from the context menu.
5. It is best practise not to use main administrator account, but create another account with administrator right and use that to register with vShield. You can do that by following these steps.
 - a) Go to vSphere Web Client > **Navigator** object > **Administration** and click **Users and Groups** under **Single Sign-On**, then add a new user by clicking plus button and enter username and password.
 - b) In Home section choose vCenter Inventory Lists and click **vCenter Servers** under **Resources**.
 - c) Right-click selected vCenter Server and choose **Add Permission** for this account.
 - d) Enable Administrator rights for that account.
6. Go back to **vShield Manager** web interface and log in.
7. In a **Configuration** tab under **Settings & Reports** (Host & Clusters view) click **Edit** next to the **Lookup Service**.
 - a) Enable **Configure lookup service** checkbox.
 - b) Enter Hostname or IP address of vCenter Server.
 - c) For vSphere 5.5 enter port 7444, for vSphere 6+ enter port 443.
 - d) Use your exact vCenter login credentials under **SSO Administrator Username** and **Password**.
8. Go back to your **vShield Manager** web interface and log in.
9. In a **Configuration** tab under **Settings & Reports** (Host & Clusters view) click **Edit** next to the **vCenter Server**, specify the hostname and enter the newly created or administrator credentials.

Installation of vShield Endpoint

1. Under **Datacenters** (Host & Clusters view), click plus button until you see hosts in cluster and select the host where you want to install **vShield Endpoint** and then navigate to the **Summary** tab and click **Install**.
2. Confirm by clicking **Install** in the upper-right corner of the window.
3. Repeat the steps 1 and 2 for every ESXi host.

3. Installation/Deployment

This section will guide you through the installation (deployment) process.

3.1 System Requirements

ESET Virtualization Security is a preconfigured virtual machine running on a Linux distribution (CentOS). ESET Virtualization Security must be installed on each ESXi host that is running virtual machines to be protected.

Prerequisites

Before installing ESET Virtualization Security, make sure your system meets the following prerequisites:

1. [VMware vCenter](#) and [VMware vShield](#) deployed according to instructions provided by VMware
2. [vShield auditor present with username, password and vShield IP address \(recommended\)](#)
3. [ESET Remote Administrator Virtual Appliance 6.3 or higher deployed \(one per environment\)](#) or installed on a dedicated machine
4. [ESET Remote Administrator Virtual Agent host installed \(one per environment\)](#)
5. [ESET Virtualization Security installed on each ESXi host](#) or [installed via deployment tool](#)
6. [VMware Tools installed \(on each protected virtual machine/guest\)](#)

The following infrastructure configuration is required to install ESET Virtualization Security:

- VMware vSphere 5.5 and 6.0 (vCenter Single Sign-On, vSphere Client/Web Client, vCenter Server, vCenter Inventory Service)
- VMware vShield Manager 5.5.4
- VMware vShield Endpoint 5.1.0

VMware is available as a pre-configured appliance, so all you have to do is deploy it and run the initial configuration.

Software requirements for guest virtual machine(s)

- Windows Vista (32 bit)
- Windows 7 (32 bit)
- Windows 7 (64 bit)
- Windows XP (32 bit) - SP3 and above
- Windows 2003 (32/64 bit) - SP2 and above
- Windows 2003 R2 (32/64 bit)
- Windows 2008 (32/64 bit)
- Windows 2008 R2 (32/64 bit)
- Windows 8 (32/64 bit) (vSphere 5.5 only)
- Windows 8.1 (32/64 bit) (vSphere 5.5 - ESXi build 1892794 and above)
- Windows 2012 (64 bit) (vSphere 5.5 only)
- Windows 2012 R2 (64 bit) (vSphere 5.5 - ESXi build 1892794 and above)

Recommended hardware configuration for ESXi host

CPU type	64-bit
CPU model	Xeon E5-2690 v3 2.50 GHz
Memory	64 GB
Storage size	local 551 GB, shared 650 GB

Virtual machine hardware configuration

CPU type	64-bit
CPU model	Xeon E5-2690 v3 2.50 GHz

Memory	1 GB
Storage size	shared 20 GB

ESET Virtualization Security minimal hardware requirements

Number of protected VMs	CPU	RAM
1 - 1024	1 core	1 GB

ESET Virtualization Security recommended hardware requirements

Number of protected VMs	CPU	RAM
1 - 63	1 core	1 GB
64 - 127	2 cores	2 GB
128 - 255	4 cores	2 GB
256 - 511	8 cores	2 GB
512 - 1024	16 cores	2 GB

3.2 Installation of standalone components, with manual configuration

To install separate components and configure them manually, follow the instructions for the component you want to deploy:

[ESET Remote Administrator VA deployment](#)

[vAgent Host deployment](#)

[ESET Virtualization Security deployment](#)

[VMware Tools installation](#)

3.2.1 ESET Remote Administrator VA deployment

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

Deploying ERA VA on a vSphere Client

1. Connect to your vCenter Server using vSphere Client, or directly to your ESXi server.
2. Click **File > Deploy OVF Template**.
3. Click **Browse**, navigate to the [ERA_Appliance.ova](#) file that you [downloaded from ESET.com](#) and then click **Open**.
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

Host/Cluster

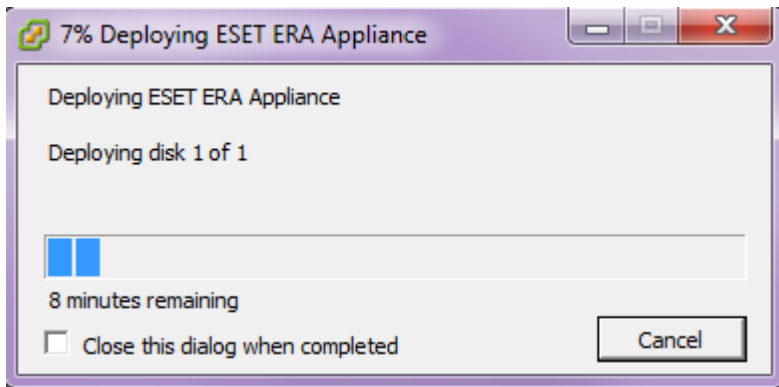
Resource Pool

Storage

Disk Format

Network Mapping

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



8. Once the ERA VA is successfully deployed, power it on. The following information will be displayed:

```
ESET Remote Administrator Appliance
(C) 2015 ESET, spol. s r.o. - All rights reserved

First time appliance configuration needs to be performed
through a web browser by connecting to:
https://10.1.119.178:8443

Or it can be done manually by these steps:
1. Enter management mode with password [eraadmin].
2. Exit console to root terminal.
3. Edit and save OVF configuration XML for server by typing:
   nano ovf.xml
4. Restart appliance by typing:
   reboot

<ENTER> Enter management mode
```

Open your web browser and enter the IP address of your newly deployed ERA 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 through a web browser by connecting to: https://[IP address]:8443"**.

The next step is to [configure your appliance](#) via the web interface.

i NOTE: If you do not have a DHCP server in your network, you will need to [configure your ERA VA manually](#). The following information will be displayed; the URL will not contain an IP address.

```
ESET Remote Administrator Appliance
(C) 2015 ESET, spol. s r.o. - All rights reserved

First time appliance configuration needs to be performed
through a web browser by connecting to:
https://:8443

Or it can be done manually by these steps:
1. Enter management mode with password [eraadmin].
2. Exit console to root terminal.
3. Edit and save OVF configuration XML for server by typing:
   nano ovf.xml
4. Restart appliance by typing:
   reboot
```

```
<ENTER> Enter management mode
```

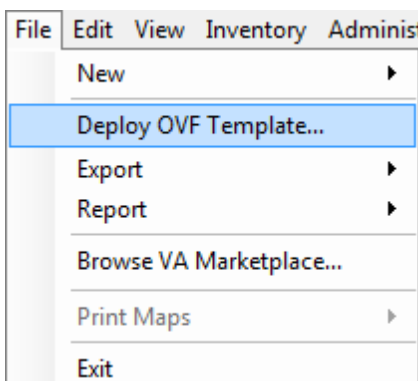
i NOTE: We highly recommend that you configure vCenter roles and permissions in such a way that VMware users won't be able to access the ERA virtual machine. This will prevent users from tampering with the ERA VM. There is no need for ERA users to access the VM. To manage access to ESET Remote Administrator, use [Access Rights](#) in the ERA Web Console.

3.2.2 vAgent Host deployment

The Virtual Agent Host appliance is formatted as a VMware compatible image intended primarily for use in local networks. The OVA file contains a functional operating system, and is ready to use as soon as it is deployed. You can deploy the OVA file using vSphere Client.

Deployment procedure:

1. Log into vSphere Client, click **File** in the top menu bar and select **Deploy OVF Template**.



2. Click **Browse** and navigate to the image stored on your computer (local hard drive, network share...) or enter a URL where the image is located.
3. Click **Next** to verify that you have selected the correct image to use.
4. Read and accept the end user license agreement.
5. Follow the instructions on screen to complete installation and specify the following information about your virtual appliance:

- **Name and Location** – Specify a name for the deployed template and 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. In the **Properties** page, specify following (fields not mentioned are optional):

Hostname – this will be the hostname of your ERA VAgentHost appliance.

Password – this will be used for your ERA VM as well as its CentOS root password.

ERA Server Hostname – type in the hostname or IP address of your ERA Server or ERA Proxy, so that ERA VAgentHost can connect to ERA Server/Proxy.

ERA Server Port – port of your ERA Server or ERA Proxy, the default is 2222. If you are using a different port, replace the default port with your custom port number.

Certification Authority - Base64 – paste your Certification Authority here in Base64 format.

Proxy Certificate - Base64 – paste your Proxy Certificate here in Base64 format.

Agent Certificate - Base64 – paste your Agent Certificate here in Base64 format.

vAgent Host is able to connect to ERA Server/Proxy and gather certificates automatically from it after specifying all required fields and also specifying the following fields with valid values so that ERA vAgent Host can connect to ERA Server/Proxy:

ERA Server Hostname

Webconsole Hostname

Webconsole username and password

Deploy OVF Template

Properties
Customize the software solution for this deployment.

[Source](#)
[OVF Template Details](#)
[End User License Agreement](#)
[Name and Location](#)
[Host / Cluster](#)
[Resource Pool](#)
[Storage](#)
[Disk Format](#)
[Network Mapping](#)
Properties
 Ready to Complete

Application

Hostname
The fully qualified hostname for this VM (e.g.: era-vagenthost.domain.com). Leave blank to try to reverse lookup the IP address.

Password
VM and database password. Use ASCII characters except reserved '{' and '}'.
 Enter password
 Confirm password
 Enter a string value with 8 to 65535 characters.

ERA Server Hostname
ERA Server hostname or IP address for VAgentHost to connect to.

 A value must be provided.

Properties with invalid values will be left unassigned. The vApp will not be able to power on until all properties have valid values.

[Help](#) [< Back](#) [Next >](#) [Cancel](#)

8. Skip the certificate export and continue with deployment.
9. If vAgent Host is not able to download a certificate authority and agent/server certificate for some reason, you will need to export certificates (as Base64) in ERA Web Console:

To create a **certificate authority**, follow the steps below in ERA Web Console:

- a) Navigate to **Admin > Certificates > Certificate Authorities** and click **New**.
- b) Complete the required fields, add whatever optional information you want to and then click **Save**.

To create an **agent/server certificate** follow the steps below in ERA Web Console:

- a) Navigate to **Admin > Certificates > Peer Certificates** and click **New** at the bottom of the window to add a new certificate.
- b) Complete all mandatory fields, add any optional information that you want to and then click **Finish**.
- c) Select your Agent certificate and select **Export as Base64** from the **Action** drop-down menu. You will be prompted to save the text file.
- d) To enter this certificate into the respective field, open the file, copy all text and paste the text into the appropriate field. Repeat these steps when exporting and entering the Server certificate.

The screenshot shows the 'Create Certificate - Basic' form in the ESET Remote Administrator web console. The form is divided into two main sections: 'BASIC' and 'ATTRIBUTES (SUBJECT)'. The 'BASIC' section includes fields for 'DESCRIPTION' (Agent), 'PRODUCT' (Agent), 'HOST' (*), 'PASSPHRASE' (masked with dots), and 'CONFIRM PASSPHRASE' (masked with dots). There is a 'SHOW PASSPHRASE' link below the passphrase fields. The 'ATTRIBUTES (SUBJECT)' section includes fields for 'COMMON NAME' (Agent certificate for host *), 'COUNTRY CODE', 'STATE OR PROVINCE', 'LOCALITY NAME', 'ORGANIZATION NAME', 'ORGANIZATIONAL UNIT', 'VALID FROM' (2014 Dec 2), and 'VALID TO' (2019 Dec 2). At the bottom of the form, there are buttons for '+ SIGN', '+ SUMMARY', 'FINISH', and 'CANCEL'. The top of the console shows the 'eset REMOTE ADMINISTRATOR' header with a search bar, a help icon, and a user profile 'ADMINISTRATOR' with a session duration of '>9 MIN'.

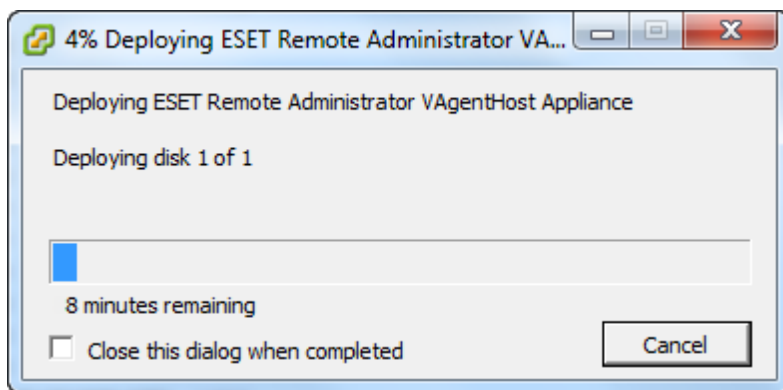
10. Repeat these steps to create a new Server certificate.

i NOTE: For more details on creating Agent/Server certificates and certificate authority, navigate to the **Peer Certificates** and **Certificate Authorities** sections of [ESET Remote Administrator online help](#).

11. Review the deployment summary and confirm by clicking **Finish** (the **Power on after deployment** check box is optional).

12. The deployment process will automatically create a virtual machine with the settings you specified. This

process can take several minutes depending on network performance.



Once the vAgent Host is successfully deployed, power it on. The basic information screen, shown below, gives an overview of protected machines and allows you to configure settings by pressing **Enter**.

```
ESET Remote Administrator Appliance
(C) 2015 ESET, spol. s r.o. - All rights reserved

First time appliance configuration needs to be performed
through a web browser by connecting to:
https://10.1.173.95:8443

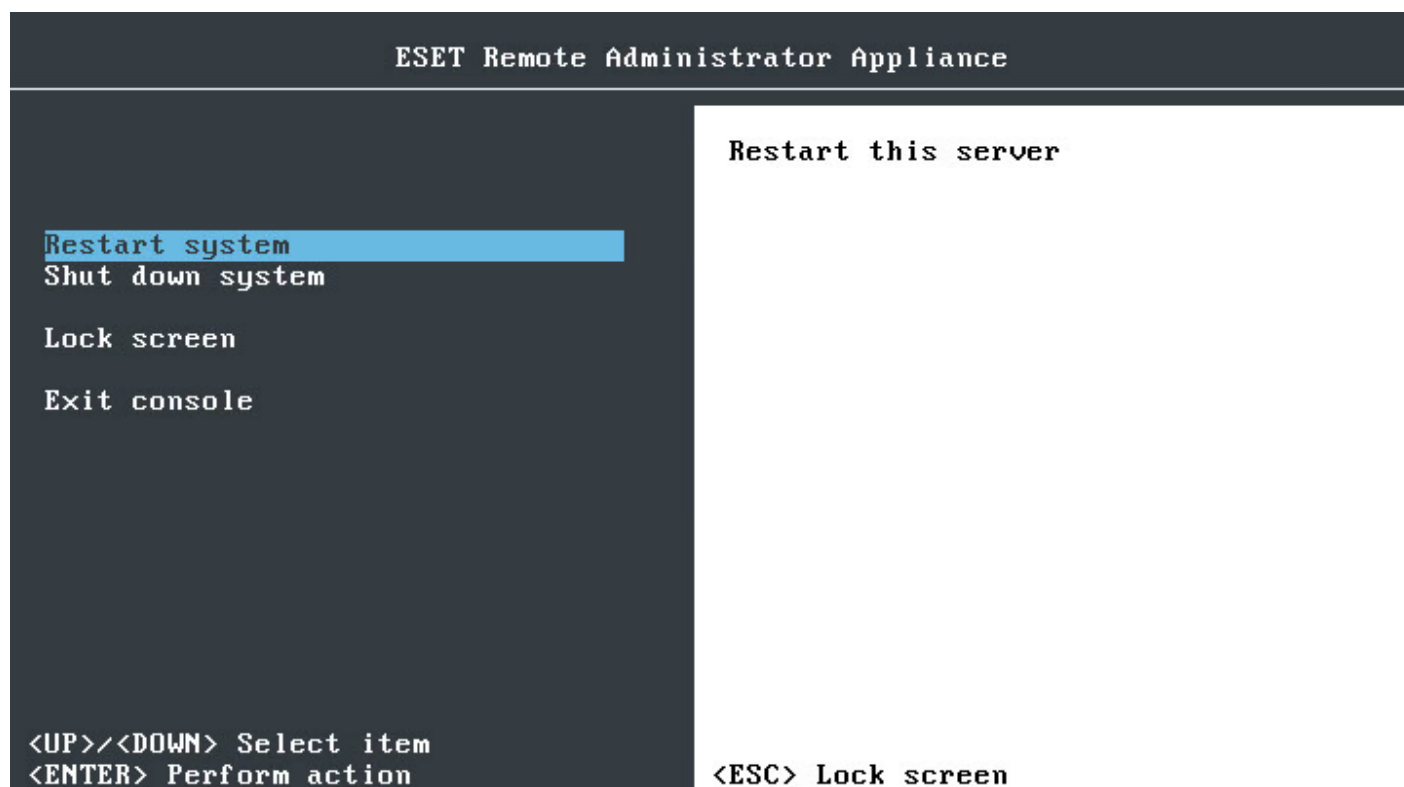
Or it can be done manually by these steps:
1. Enter management mode with password [eraadmin].
2. Exit console to root terminal.
3. Edit and save OVF configuration XML for server by typing:
   nano ovf.xml
4. Restart appliance by typing:
   reboot

<ENTER> Enter management mode
```

The following options can be edited in management mode:

- **Restart system** – ESET Virtualization Security will restart.
- **Shut down system** – will shut down your system.
- **Lock screen** – will lock the console and return to the basic information screen (also by pressing **Esc**).
- **Exit console** – will exit the console and return to the command line.

Use the arrow keys to select a setting and press **Enter** to configure it.



3.2.3 ESET Virtualization Security deployment

Before you deploy ESET Virtualization Security, we recommend that you create a local vShield user with role **auditor**. Enter your username and password into the configuration parameters under the **vShield Environment** section. ESET Virtualization Security will periodically check to see that vShield is properly registered.

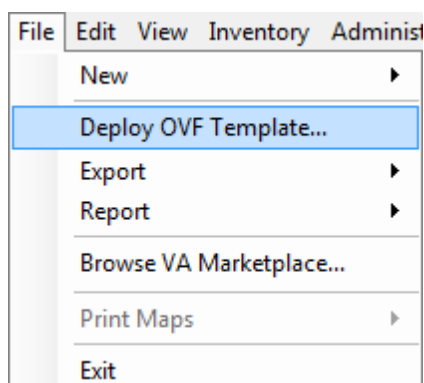
The appliance is formatted as a VMware compatible image intended primarily for use in local networks. The OVA file contains a functional operating system, and is ready to use as soon as it is deployed. You can deploy the OVA file using vSphere Client.

Connection with ESET Remote Administrator can be established in the following 3 ways:

- If configuration options are left blank, ESET Virtualization Security will prompt you to enter them when the system boots up.
- If the address and password of ESET Remote Administrator are entered – server-assisted installation will be carried out. You will not be prompted for an address after deployment.
- You can enter all parameters (hostname, IP address, Agent Certificate, Certification Authority public key) during initial configuration to avoid their entry after deployment.

Deployment procedure:

1. Log into vSphere Client, click **File** in the top menu bar and select **Deploy OVF Template**.



2. Click **Browse** and navigate to the image stored on your computer (local hard drive, network share...) or enter a URL where the image is located.
3. Click **Next** to verify that you have selected the correct image to use.
4. Read and accept the end user license agreement.
5. Follow the instructions on-screen to complete installation and specify the following information about your virtual appliance:
 - **Name and Location** – Specify a name for the deployed template and 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.
6. Specify all required values on the **Properties** window. Failure to enter these values can keep your virtual machine from starting or deny it the necessary certificates for communication with ESET Remote Administrator.

Deploy OVF Template

Properties
Customize the software solution for this deployment.

Source
[OVF Template Details](#)
[End User License Agreement](#)
[Name and Location](#)
[Host / Cluster](#)
[Resource Pool](#)
[Storage](#)
[Disk Format](#)
[Network Mapping](#)
Properties
 Ready to Complete

ESET Remote Administrator settings

ERA Server Hostname
ESET Remote Administrator Server hostname or IP address to connect to.

ERA Server Port
ESET Remote Administrator Server port

ERA Agent Certificate - Base64
PKCS12 base64 encoded managing agent certificate.

ERA Agent Certificate Password
Managing agent peer certificate password. Leave blank if the certificate is not password protected.
 Enter password
 Confirm password

ERA Certification Authority - Base64
DER base64 encoded certification authority certificate used for signing ERA server certificate.

Help < Back Next > Cancel

7. If you do not already have a certificate authority and agent/server certificate, you will need to create them in

ERA Web Console:

To create a **certificate authority**, follow the steps below in ERA Web Console:

- a) Navigate to **Admin > Certificates > Certificate Authorities** and click **New**.
- b) Complete the required fields, add whatever optional information you want to and then click **Save**.

To create an **agent/server certificate** follow the steps below in ERA Web Console:

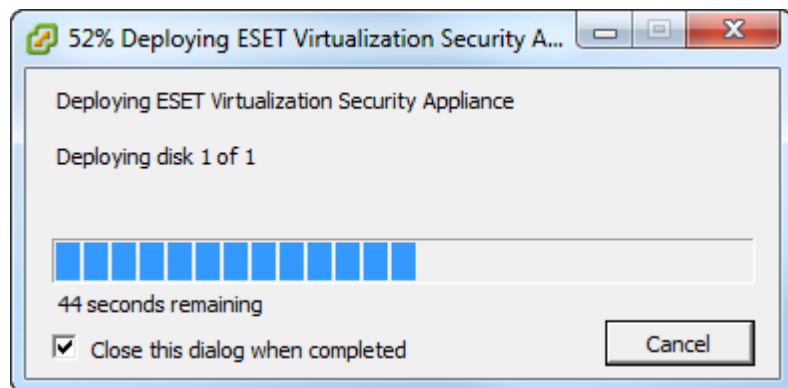
- a) Navigate to **Admin > Certificates > Peer Certificates** and click **New** at the bottom of the window to add a new certificate.
- b) Complete all mandatory fields, add any optional information that you want to and then click **Finish**.
- c) Select your Agent certificate and select **Export as Base64** from the **Action** drop-down menu. You will be prompted to save the text file.
- d) To enter this certificate into the respective field, open the file, copy all text and paste the text into the appropriate field. Repeat these steps when exporting and entering the Server certificate.

The screenshot shows the 'Create Certificate - Basic' form in the ESET Remote Administrator console. The form is divided into several sections: 'BASIC', 'ATTRIBUTES (SUBJECT)', and 'SIGN'. The 'BASIC' section includes fields for 'DESCRIPTION' (Agent), 'PRODUCT' (Agent), 'HOST' (*), 'PASSPHRASE' (masked with dots), and 'CONFIRM PASSPHRASE' (masked with dots). There is a 'SHOW PASSPHRASE' link below the passphrase fields. The 'ATTRIBUTES (SUBJECT)' section includes fields for 'COMMON NAME' (Agent certificate for host *), 'COUNTRY CODE', 'STATE OR PROVINCE', 'LOCALITY NAME', 'ORGANIZATION NAME', 'ORGANIZATIONAL UNIT', 'VALID FROM' (2014 Dec 2), and 'VALID TO' (2019 Dec 2). The 'SIGN' section has a '+ SIGN' button, and the 'SUMMARY' section has a '+ SUMMARY' button. At the bottom, there are 'FINISH' and 'CANCEL' buttons. The left sidebar shows navigation icons for Home, Alerts, Reports, and Settings. The top bar includes the ESET logo, 'REMOTE ADMINISTRATOR', a 'Computer Name' dropdown, a search icon, a help icon, 'ADMINISTRATOR', and a '>9 MIN' indicator.

8. Repeat these steps to create a new Server certificate.

i NOTE: For more details on creating Agent/Server certificates and certificate authorities, navigate to the **Peer Certificates** and **Certificate Authorities** sections of the [ESET Remote Administrator User Guide](#).

- Review the deployment summary and confirm by clicking **Finish** (the **Power on after deployment** feature is optional).
- The deployment process will automatically create a virtual machine with the settings you specified. This process can take several minutes depending on network performance.



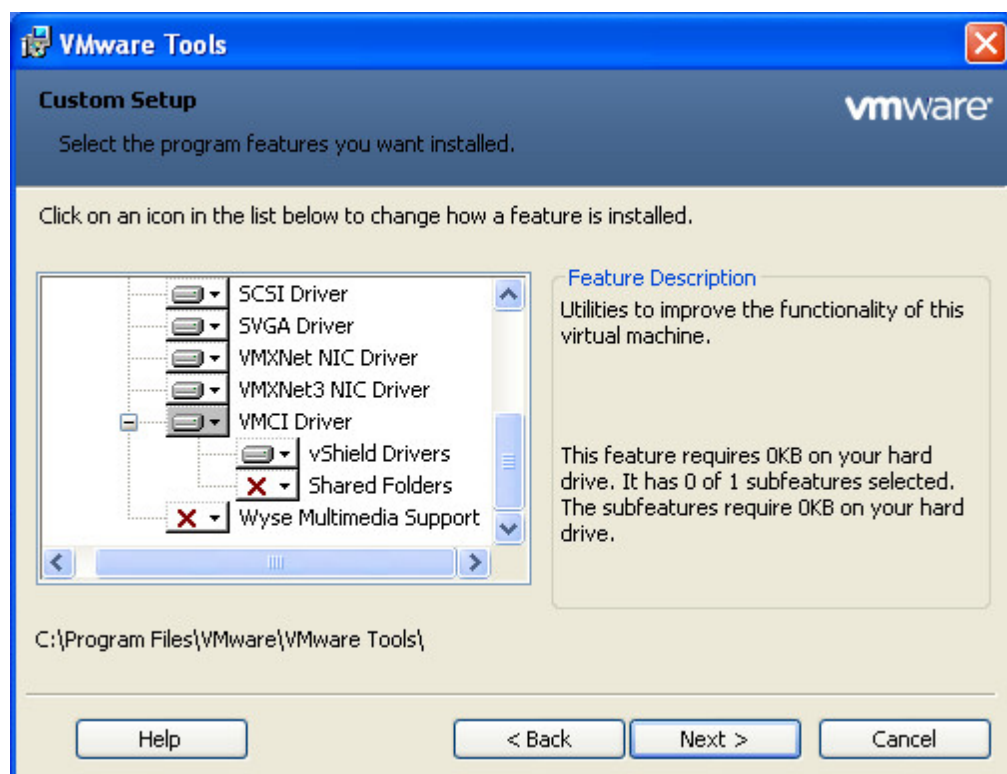
3.2.4 VMware Tools installation

ESET Virtualization Security uses the EPSEC library provided by VMware to interact with virtual machines.

! IMPORTANT: VMware Tools must be installed on each virtual machine protected by ESET Virtualization Security for protection to be effective.

To install VMware Tools, perform the following steps on each virtual machine in your vCenter environment:

- In vCenter, navigate to **Inventory > Virtual Machine > Guest > Install/Upgrade VMware Tools** and select the **Custom** setup.
- Open the console for the virtual machine where VMware tools will be installed.
- Follow the steps from the wizard to complete the installation process. Make sure to install the VMCI Driver component.



3.3 Installation of ESET Virtualization Security using deployment tool

The **Deployment tool** allows administrator to deploy ESET Virtualization Security on multiple ESXi hosts.

To download the **Deployment tool** click [here](#). The *evs_deployment_tool.zip* file contains:

- **EvsaDeploymentTool.jar** – a jar file used for deployment of ESET Virtualization Security.
- **deploy.bat** – a script file that consists of command to be executed by the command line.
- **deploy-template.csv** – a comma-separated values file that stores important values defined below.
- **deploy-two-hosts-minimal-example.csv** – an example of CSV file.

Complete the following prerequisites before you perform a batch deployment:

1. Configure your VMware vShield environment.
2. Create a vShield auditor user to allow the ESET Virtualization Security virtual machine to access information from vShield.
3. Deploy ERA Server (virtual appliance or normal installation).
4. Deploy vAgent Host (virtual appliance or normal installation).
5. Prepare a CSV file by using the provided templates (deploy-template.csv). Below is a list of the criteria defined in the .csv file:

Host – a specific host for which ESET Virtualization Security will be deployed

Folder – location where ESET Virtualization Security virtual machine should be placed (optional)

Resource pool – resource pool for ESET Virtualization Security virtual machine (optional)

Datastore – datastore where ESET Virtualization Security virtual machine disk will be stored, datastore must be available for selected host

Management Network – network for connection to ERA and vAgent Host

vShield network – network used for connection to vShield

EVSA Hostname – hostname used for ESET Virtualization Security virtual machine

IPv4 address – ESET Virtualization Security virtual machine network configuration (if empty, DHCP is used)

IPv4 netmask – ESET Virtualization Security virtual machine network configuration (if empty, DHCP is used)

IPv4 gateway – ESET Virtualization Security virtual machine network configuration (if empty, DHCP is used)

IPv6 address – ESET Virtualization Security virtual machine network configuration (if empty, DHCP is used)

IPv6 gateway – ESET Virtualization Security virtual machine network configuration (if empty, DHCP is used)

DNS1 – ESET Virtualization Security virtual machine network configuration (if empty, DHCP is used)

DNS2 – ESET Virtualization Security virtual machine network configuration (if empty, DHCP is used)

ERA Server Hostname – hostname of ERA Server that will manage ESET Virtualization Security virtual machine

ERA Server Port – Port of ERA Server port that enables management of ESET Virtualization Security

ERA Agent Certificate Base64 – ERA Agent certificate as Base64 that will be used for authentication of ESET Virtualization Security virtual machine

ERA Agent Certificate Password – password to decrypt ERA Agent certificate

ERA Certification Authority Base64 – ERA certification authority that will be used for authentication of ERA Server

vAgent Host Hostname – hostname of vAgent Host

vAgent Host Port – port of vAgent Host

vAgent Host Agent Certificate Base64 – vAgent Host certificate as Base64 that will be used for authentication of ESET Virtualization Security virtual machine

vAgent Host Agent Certificate Password – password to decrypt vAgent Host certificate

6. Open a command line and run `deploy.bat` Or `java -jar EvsaDeploymentTool.jar`.
7. Enter your vCenter hostname and administrator credentials.
8. Enter your vShield hostname and administrator credentials.
9. Enter the full path to the ESET Virtualization Security OVA file
10. Enter the full path to the CSV file you created in step 5.

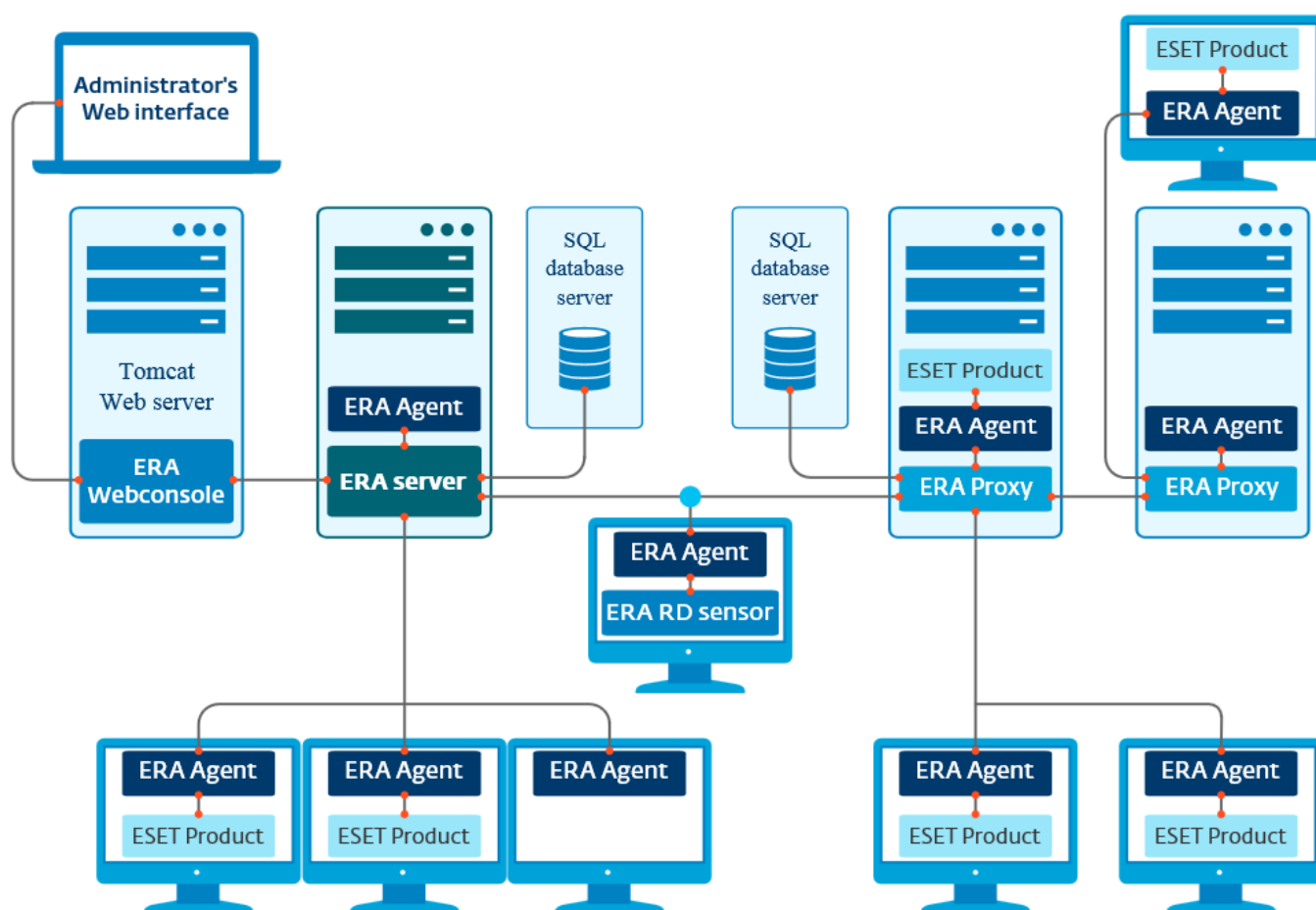
Allow the necessary time for deployment to complete, duration may vary depending on system configuration and network performance. Follow the instructions on-screen to complete deployment.

4. Basics of ESET Remote Administrator

ESET Remote Administrator (ERA) is an application that allows you to manage ESET Virtualization Security in a networked environment from one central location. The ESET Remote Administrator task management system allows you to install ESET security solutions on remote computers and quickly respond to new problems and threats. ESET Remote Administrator does not provide protection against malicious code on its own, it relies on the presence of an ESET security solution on each client.

ESET security solutions support networks that include multiple platform types. Your network can include a combination of current Microsoft, Linux-based, Mac OS and operating systems that run on mobile devices (mobile phones and tables).

The picture below depicts a sample architecture for a network protected by ESET security solutions managed by ERA:



NOTE: For more information see the [ESET Remote Administrator online help](#).

4.1 ESET Remote Administrator Server

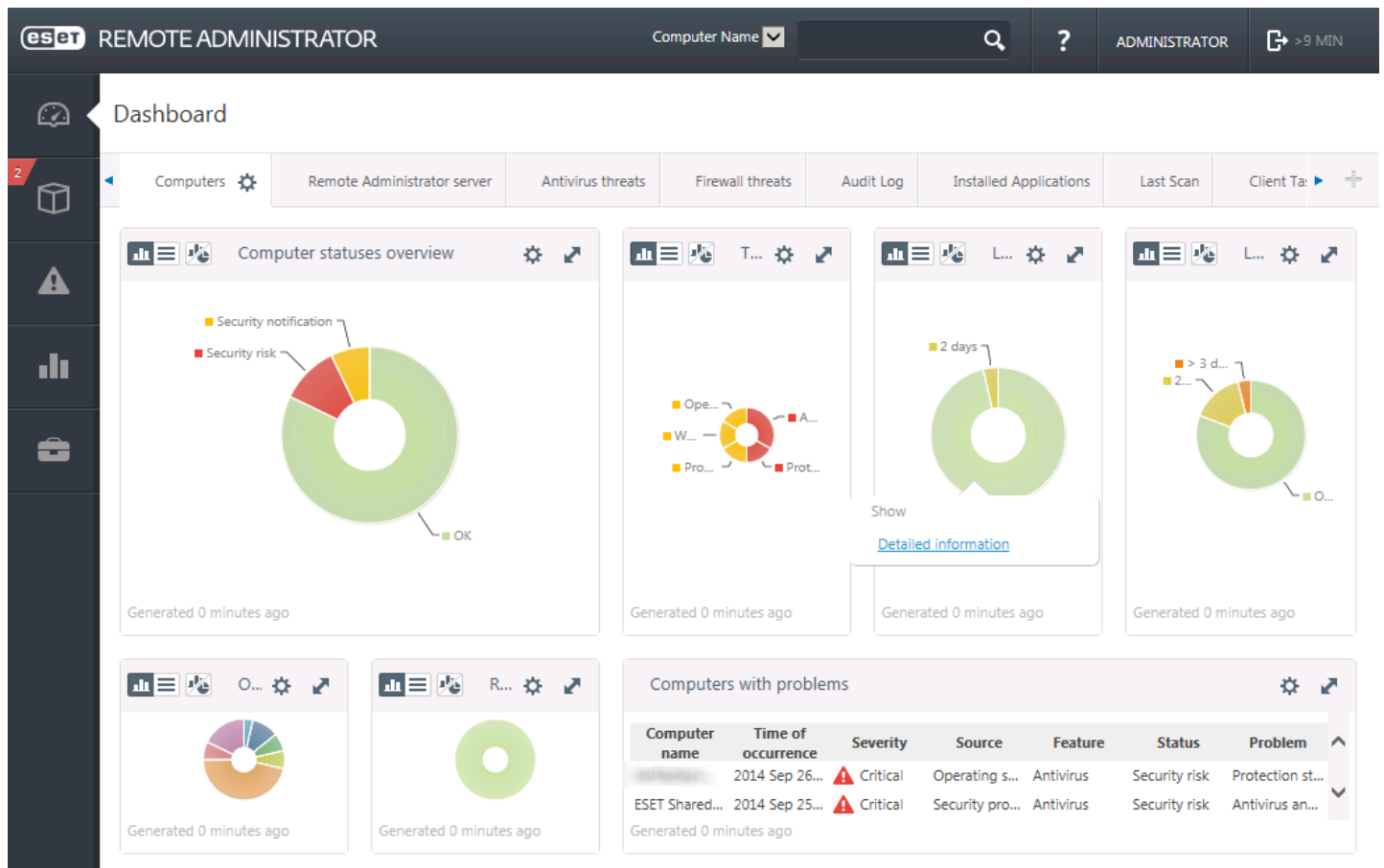
ESET Remote Administrator Server is a primary component of ESET Remote Administrator. It is the executive application that processes all data received from clients that connect to the Server (through the [ERA Agent](#)). The ERA Agent facilitates communication between the client and the server. Data (Client logs, configuration, agent replication, etc.) are stored in a database. To correctly process the data, the ERA Server requires a stable connection to a Database server. We recommend that you install ERA Server and your database on separate servers to optimize performance. The machine on which ERA Server is installed must be configured to accept all Agent/Proxy/RD Sensor connections which are verified using certificates. Once installed, you can open [ERA Web Console](#) which connects to the ERA Server (as can be seen in the diagram). From the Web Console, all ERA Server operations are performed when managing ESET security solutions within your network.

NOTE: For more information see the [ESET Remote Administrator online help](#).

4.2 Web Console

ERA Web Console is a web-based user interface that presents data from [ERA Server](#) and allows you to manage ESET security solutions in your network. Web Console can be accessed using a browser. It displays an overview of the status of clients on your network and can be used to deploy ESET solutions to unmanaged computers remotely. You can choose to make the web server accessible from the internet to allow for the use of ESET Remote Administrator from virtually any place or device.

This is the Web Console's Dashboard:



The **Quick Search** tool is located at the top of the Web Console. Select **Computer Name**, **IPv4/IPv6 Address** or **Threat Name** from the drop-down menu, type your search string into the text field and then click the magnifier symbol or press **Enter** to search. You will be redirected to the **Groups** section, where your search result will be displayed.

NOTE: For more information see [Getting to know ERA Web Console](#).

See also the **How to** part:



[How to find vAgent Host in ESET Remote Administrator](#)

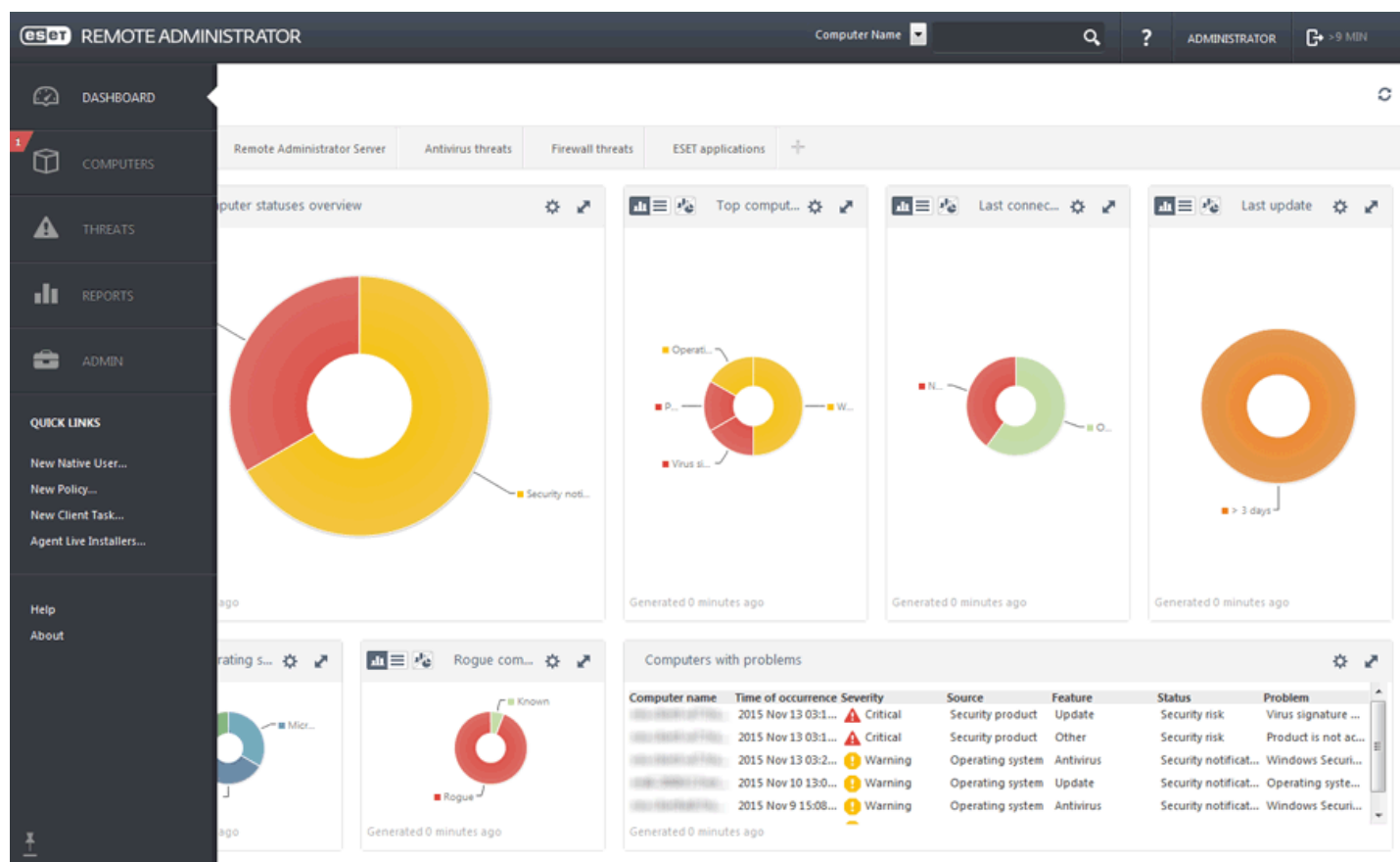
[How to find ESET Virtualization Security in ESET Remote Administrator](#)

4.3 Getting to know ERA Web Console

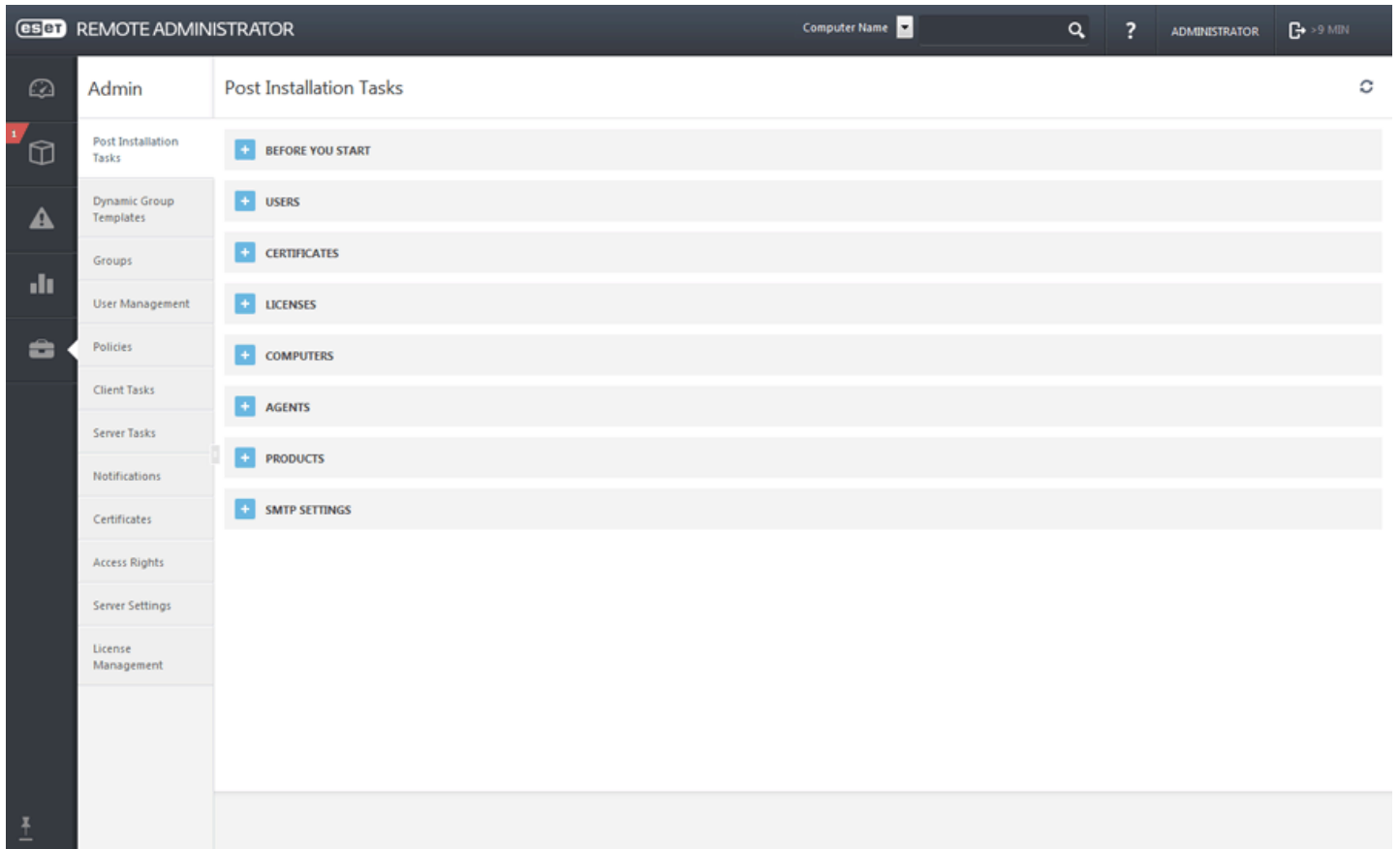
ESET Remote Administrator Web Console is the main interface used to communicate with ERA Server. You can think of it as a control panel, a central place from which you can manage all of your ESET security solutions. It is a web-based interface that can be accessed using a browser (see [Supported Web browsers](#)) from any place and any device with internet access.

In the ERA Web Console standard layout:

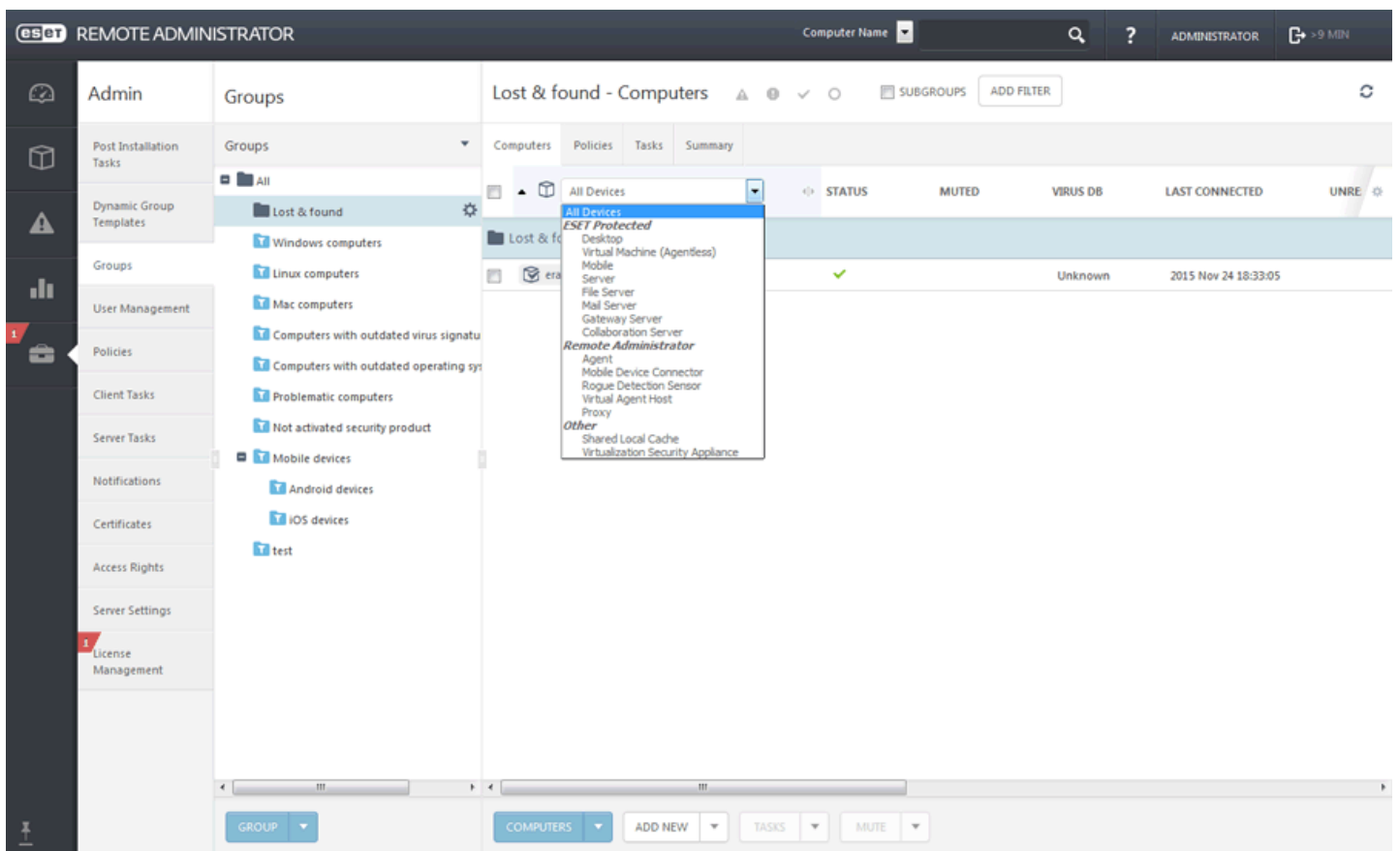
- The current user is always shown in upper right, where the timeout for his/her session counts down. You can click **Logout** to log out at any time. When a session times out (because of user inactivity), a user must log in again.
- You can click **?** at the top of any screen to view help for that specific screen.
- The **Menu** is accessible on the left at all times except when using a Wizard. Place your mouse on the left of the screen to display the menu. The menu also contains **Quick Links** and displays your **Web Console version**.
- The  icon always denotes a context menu.
- Click  **Refresh** to reload/refresh displayed information.



Post-Installation Tasks show you how to get most from ESET Remote Administrator. These will guide you through the recommended steps.



Screens with tree have specific controls. The tree itself is on the left with actions bellow. Click an item from the tree to display options for that item.



Tables allow you to manage units from rows individually or in a group (when more rows are selected). Click a row to display options for units in that row. Data in tables can be filtered and sorted.

eset

REMOTE ADMINISTRATOR

Computer Name

ADMINISTRATOR

> 9 MIN

Admin

Post Installation Tasks

Dynamic Group Templates

Groups

User Management

1 Policies

Client Tasks

Server Tasks

Notifications

Certificates

Access Rights

Server Settings

1 License Management

Groups

Groups

All

Lost & found

Windows computers

Linux computers

Mac computers

Computers with outdated virus signature

Computers with outdated operating system

Problematic computers

Not activated security product

Mobile devices

Android devices

iOS devices

test

Lost & found - Computers

Computers Policies Tasks Summary

All Devices

STATUS MUTED VIRUS DB LAST CONNECTED UNRE

Lost & found (1)

Computer

Details...

Delete

Move...

Scan

Update Virus DB

Mobile

Reboot

Run Task...

New task...

Manage Policies

Send Wake

Deploy Agent

Run task

Enroll...

Find

Lock

Unlock

Siren

Wipe

Computer

Mute

Un-mute

GROUP

COMPUTERS

ADD NEW

TASKS

MUTE

Objects in ERA can be edited using Wizards. All Wizards share the following behaviors:

- Steps are vertically oriented from top to bottom.
- User can return to any step at any time.
- Invalid input data are marked when you move your cursor to a new field. The Wizard step containing invalid input data is marked as well.
- User can check for invalid data any time by clicking **Mandatory Settings**.
- **Finish** is not available until all input data is correct.

The screenshot displays the ESET Remote Administrator (ERA) interface for configuring a new notification distribution. The top bar shows the ESET logo, 'REMOTE ADMINISTRATOR', and a search bar. The left sidebar contains navigation icons. The main area is titled 'New Notification - Distribution' and features a list of steps: BASIC, NOTIFICATION TEMPLATE, CONFIGURATION, ADVANCED SETTINGS - THROTTLING, and DISTRIBUTION. The DISTRIBUTION step is selected and expanded, showing three checkboxes: 'Send SNMP trap' (unchecked), 'Send email' (checked), and 'Send syslog' (unchecked). Below these are two input fields: 'EMAIL ADDRESSES' and 'SUBJECT'. The 'EMAIL ADDRESSES' field has a red border and a warning icon, indicating it is required or has an issue. The 'SUBJECT' field has a yellow border and an information icon. At the bottom, there are three buttons: 'FINISH', 'MANDATORY SETTINGS >', and 'CANCEL'.

4.4 Proxy

ERA Proxy is another component of ESET Remote Administrator and serves two purposes. In a medium-sized or enterprise network with many clients (for example, 10,000 clients or more), you can use ERA Proxy to distribute load between multiple ERA Proxies facilitating the main [ERA Server](#). The other advantage of the ERA Proxy is that you can use it when connecting to a remote branch office with a weak link. This means that the ERA Agent on each client is not connecting to the main ERA Server directly via ERA Proxy, which is on the same local network as the branch office. This configuration frees up the link to the branch office. The ERA Proxy accepts connections from all local ERA Agents, compiles data from them and uploads it to the main ERA Server (or another ERA Proxy). This allows your network to accommodate more clients without compromising the performance of your network and database queries.

Depending on your network configuration, it is possible for ERA Proxy to connect to another ERA Proxy and then connect to the main ERA Server.

For proper function of the ERA Proxy, the host computer where you install ERA Proxy must have an ESET Agent installed and must be connected to the upper level (either ERA Server or an upper ERA Proxy, if there is one) of your network.

NOTE: For more information see the [ESET Remote Administrator online help](#).

4.5 ERA Agent

The ESET Remote Administrator Agent is an essential part of ESET Remote Administrator 6. Clients do not communicate with the Server directly, rather the Agent facilitates this communication. The Agent collects information from the client and sends it to the ERA Server. If the ERA Server sends a task for the client - it is sent to the Agent which then sends this task to the client. By default, the ERA Agent synchronizes with ERA Server every 20 minutes. You can change this setting by creating a new policy for the [ERA Agent Connection Interval](#).

i NOTE: For more information see the [ESET Remote Administrator online help](#).

4.6 Virtual Agent Host

Virtual Agent Host is a component of the ESET Remote Administrator product that virtualizes agent entities to allow for the management of agent-less virtual machines. This solution enables vMotion of virtual machines and thereby automation, dynamic group utilization and the same level of task management as ERA Agent for physical computers. The Virtual Agent collects information from virtual machines and sends it to the Server. When the Server sends a task to a virtual machine, the task is sent to the Virtual Agent which then communicates with the virtual machine. All network communications occur between the Virtual Agent and the upper part of the ERA network – Server and Proxy.

The Virtual Agent Host communicates with ESET Virtualization Security, collects information from programs on protected virtual machines and passes configuration information received from the Server to the virtual machine.

With Virtual Agent Host you are able to configure any virtual machine on any host. The virtual machine can then be migrated from one host to another with its own settings in your environment.

The ESET Remote Administrator Agent is not installed on agentless protected machines. These virtual machines use a virtualized vAgent Host and cannot be assigned all of the same tasks as machines with ERA Agent installed.

The following tasks are available on agentless machines:

- identification of product components
- activation
- on-access/on-demand scan and scanner properties
- updates
- policies
- generating reports
- troubleshooting

i NOTE: For more information see [How vAgent Host works](#).

4.7 RD Sensor

RD (Rogue Detection) Sensor is a part of ESET Remote Administrator designed to find computers on your network. It provides a convenient way of adding new computers to ESET Remote Administrator without the need to find and add them manually. Every computer found on your network is displayed in the Web Console and added to the default **All** group. From here, you can take further actions with individual client computers.

RD Sensor is a passive listener that detects computers that are present on the network and sends information about them to the ERA Server. The ERA Server evaluates whether the PCs found on the network are unknown or already managed.

i NOTE: For more information see the [ESET Remote Administrator online help](#).

5. Working with ESET Virtualization Security

5.1 Managing ESET Virtualization Security from the console

The basic information screen, shown below, gives an overview of protected machines and allows you to configure settings by pressing **Enter**.

```
ESET Virtualization Security Appliance, version 1.0.10.0
(C) 2015 ESET, spol. s r.o.

IP address: 10.1.173.88
IPv6 address: fe80::250:56ff:fea4:af29

Antivirus and antispware scanner module: 1474.1 (20160104)
Virus signature database:                12872 (20160115)

ESET Remote Administrator agent version: 6.3.115.0
ESET Remote Administrator agent status:  connected

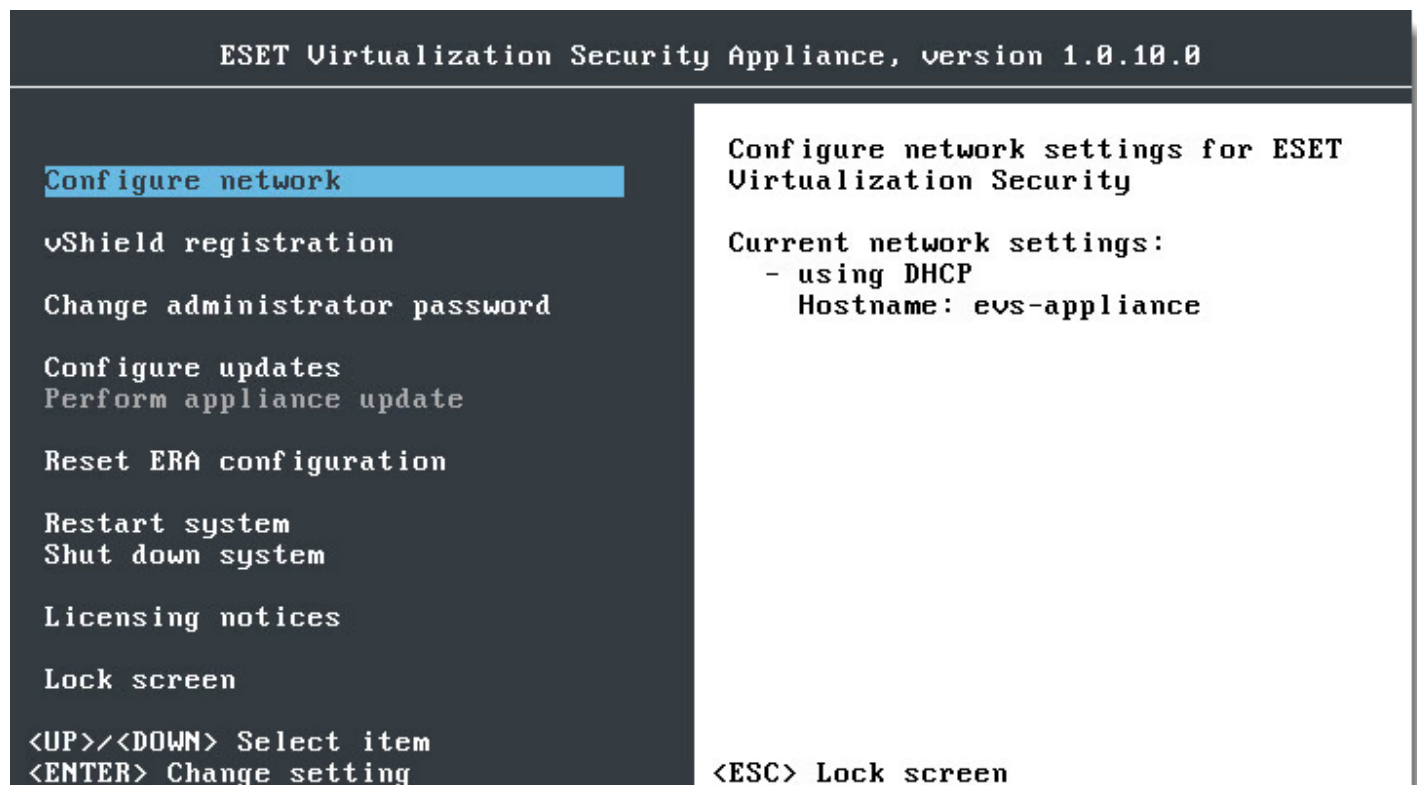
Number of connected machines:            10
Number of protected machines:            9

<ENTER> Enter management mode
```


The following options can be edited in management mode:

- **Configure network** – network settings for ESET Virtualization Security such as IP address, mask, gateway and DNS server
- **vShield registration** – shows the current vShield registration status
- **Change administrator password** – the system console can be configured so that only administrators can change settings (set an administrator password to use this configuration)
- **Configure updates** – contains update settings. For more information see [How to update ESET Virtualization Security](#)
- **Perform appliance update** – shows available system updates
- **Reset ERA configuration** – will revert settings to the defaults specified in virtual machine parameters
- **Restart system** – ESET Virtualization Security will restart
- **Shut down system** – will shut down your system
- **Licensing notices** – contains licensing information about third-party products included in software
- **Lock screen** – will lock the console and return to the basic information screen (also by pressing **Esc**)

Use the arrow keys to select a setting and press **Enter** to configure it.



Configure network

ESET Virtualization Security requires the following information for proper configuration:

To use DHCP:

- IP address or hostname of the ERA server
- Netmask
- Gateway
- DNS server 1
- DNS server 2

To use IPv6:

- IPv6 address
- IPv6 gateway

To create a policy for ESET Virtualization Security, see the following topics:

- [Security Appliance policy](#)
- [Protected VM policy](#)

5.2 Administering Clients

5.2.1 Tasks

The following tasks can be assigned to ESET Virtualization Security clients using ESET Remote Administrator:

- [virus signature database update](#)
- [on-demand scan \(with several levels of cleaning\)](#)
- [operating system update \(appliance\)](#)
- [quarantine management task](#)


These tasks are configured like any task in ESET Remote Administrator, see the [Client Tasks](#) topic in ERA online help for more information. All Client tasks are created and managed from the **Admin** tab of ERA Webconsole. To create a new task, navigate to **Client tasks**, select a task from the **Task Types** list and then click **New**.

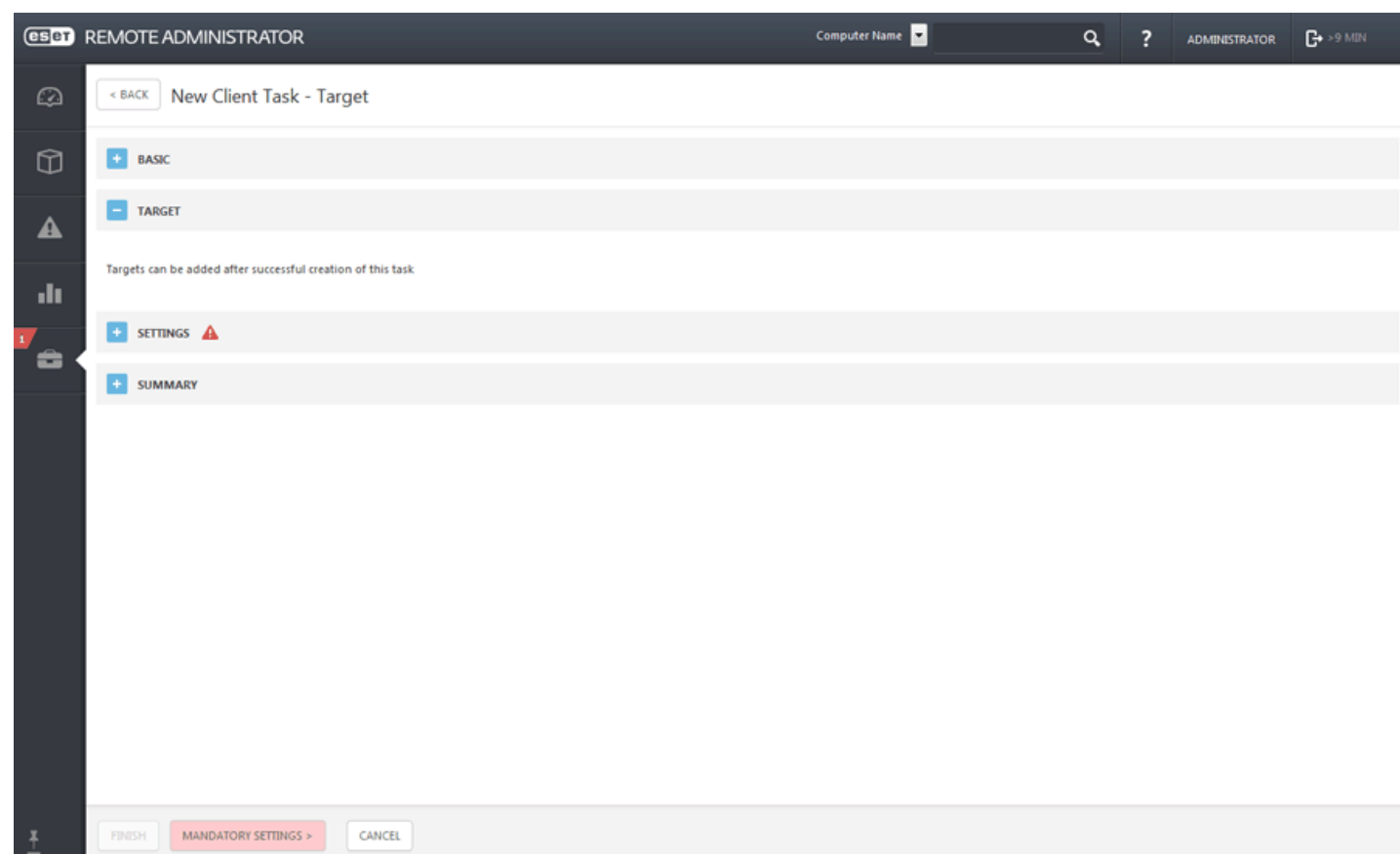
5.2.1.1 Virus Signature Database update

The **Product Update** task will update virus signature information for security product installed on clients. This is a general task for all products on all systems.

From your ERA Web Console, navigate to **Admin > Client Tasks**, select **Virus Signature Database Update** from the **Task Types** list and then click **New**.

Target

 **IMPORTANT:** It is not possible to add Targets while creating a Client Task. You will be able to add Targets after the task has been created. Configure **Settings** for the task and click **Finish** to create the task and then create a [Trigger](#) to specify Targets for the task.

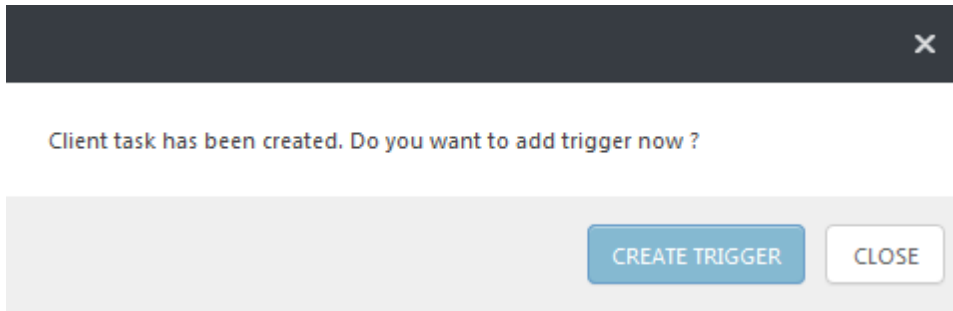


Settings

- **Clear Update Cache** - This option deletes temporary update files in the cache on the client, and can be used to repair failed virus signature database update errors.

Summary

Review the summary of configured settings and click **Finish**. The Client Task is now created and a pop-up window will open. We recommend that you click [Create Trigger](#) to specify when this Client Task should be executed and on which Targets. If you click **Close**, you can create a [Trigger](#) later on.



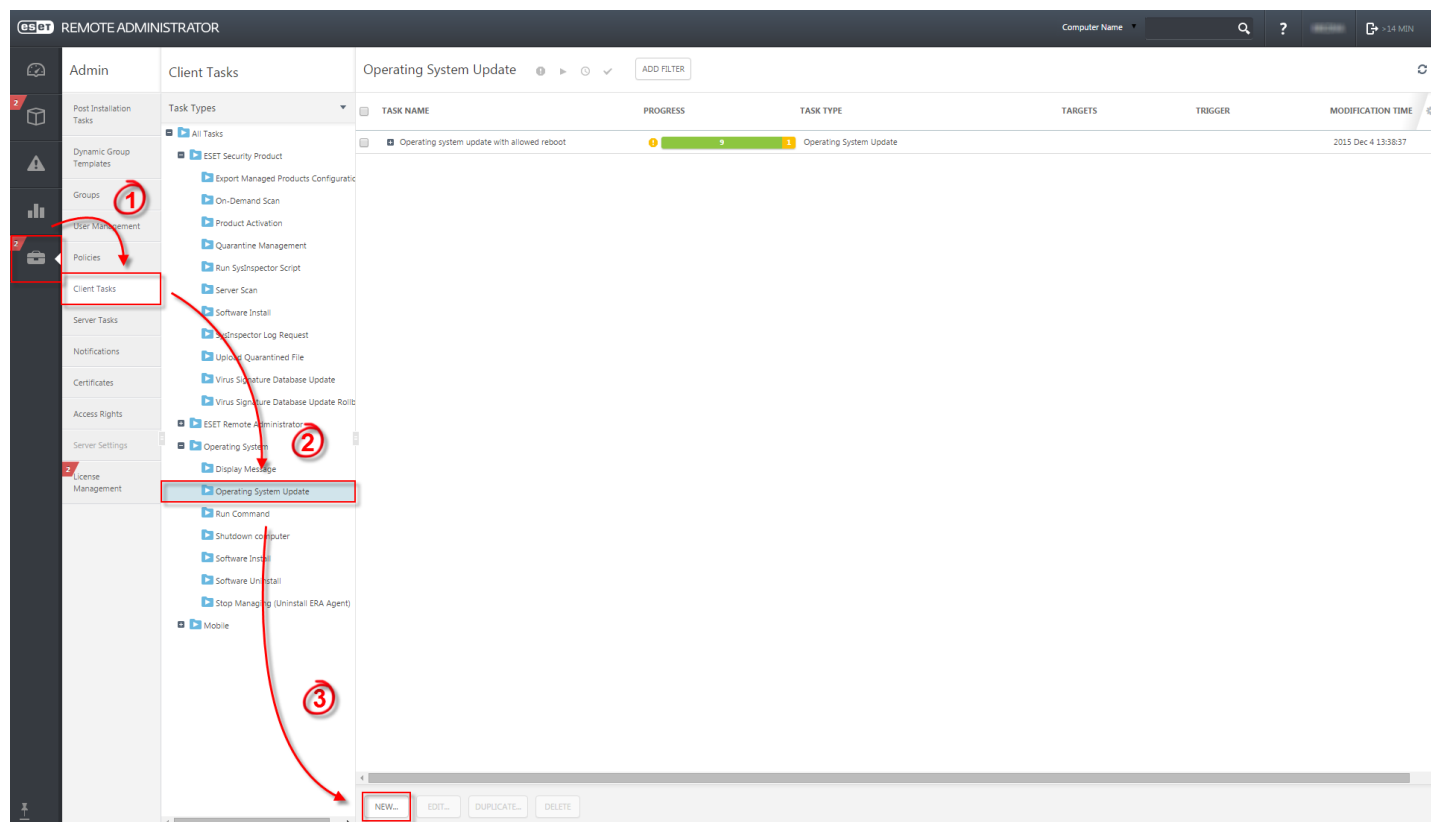
5.2.1.2 On-Demand scan

To run an **On-Demand scan** on a protected virtual machine, follow the steps below:

1. From your ERA Web Console, navigate to **Admin > Client tasks > All Tasks > ESET Security Product**.
2. Select **On-Demand Scan** from the list and click **New**.
3. Enter Basic information about the task such as the Name and optional Description.
4. In the **Target** section, specify the clients (individual computers or whole groups) that will receive this task.
Click **Add targets** to select Virtual machines from the Static and Dynamic Groups listed.
5. In the **Trigger** section, select **Execute ASAP** to send the task to clients immediately or choose the appropriate setting for your application.
6. In the **Settings** section, select the scan profile and other scan parameters.
7. Click **Finish** to execute the task (after it is delivered to the VM by vAgent Host).

5.2.1.3 Operating system update (EVS appliance)

The **Operating System Update** task is used to update the operating system of the ESET Virtualization Security appliance. This task can trigger the operating system update on Linux operating systems. In the ERA Web Console, navigate to **Admin > Client tasks**, select **Operating System Update** from the **Task Types** list and click **New**.



Basic

Enter basic information about the task, such as a **Name** and **Description** and then select the **Operating System Update** task. The **Task Type** defines the settings and behavior for the task. Enter basic information about the task, such as the **Name** and optional **Description**.

Target

IMPORTANT: It is not possible to add Targets while creating a Client Task. You will be able to add Targets after the task has been created. Configure **Settings** for the task and click **Finish** to create the task and then create a [Trigger](#) to specify Targets for the task.

REMOTE ADMINISTRATOR
Computer Name
?
ADMINISTRATOR
>9 MIN

< BACK
New Client Task - Target

+ BASIC
- TARGET

Targets can be added after successful creation of this task

+ SETTINGS
+ SUMMARY

FINISH
MANDATORY SETTINGS >
CANCEL

Settings

- **Automatically Accept EULA** - select this check box if you want to accept the EULA automatically. No text will be displayed to the user.
- **Install Optional Updates** - this option applies to Windows operating systems only, updates that are marked as optional will also be installed.
- **Allow Reboot** - this option applies to Windows operating systems only and causes the client computer to reboot once the updates are installed.

Summary

Review the summary of configured settings and click **Finish**. The Client Task is now created and a pop-up window will open. We recommend that you click [Create Trigger](#) to specify when this Client Task should be executed and on which Targets. If you click **Close**, you can create a [Trigger](#) later on.



Client task has been created. Do you want to add trigger now ?

CREATE TRIGGER
CLOSE

5.2.1.4 Quarantine management


The **Quarantine Management** task is used to manage objects in the ERA Server quarantine - infected or suspicious objects found during the scan.

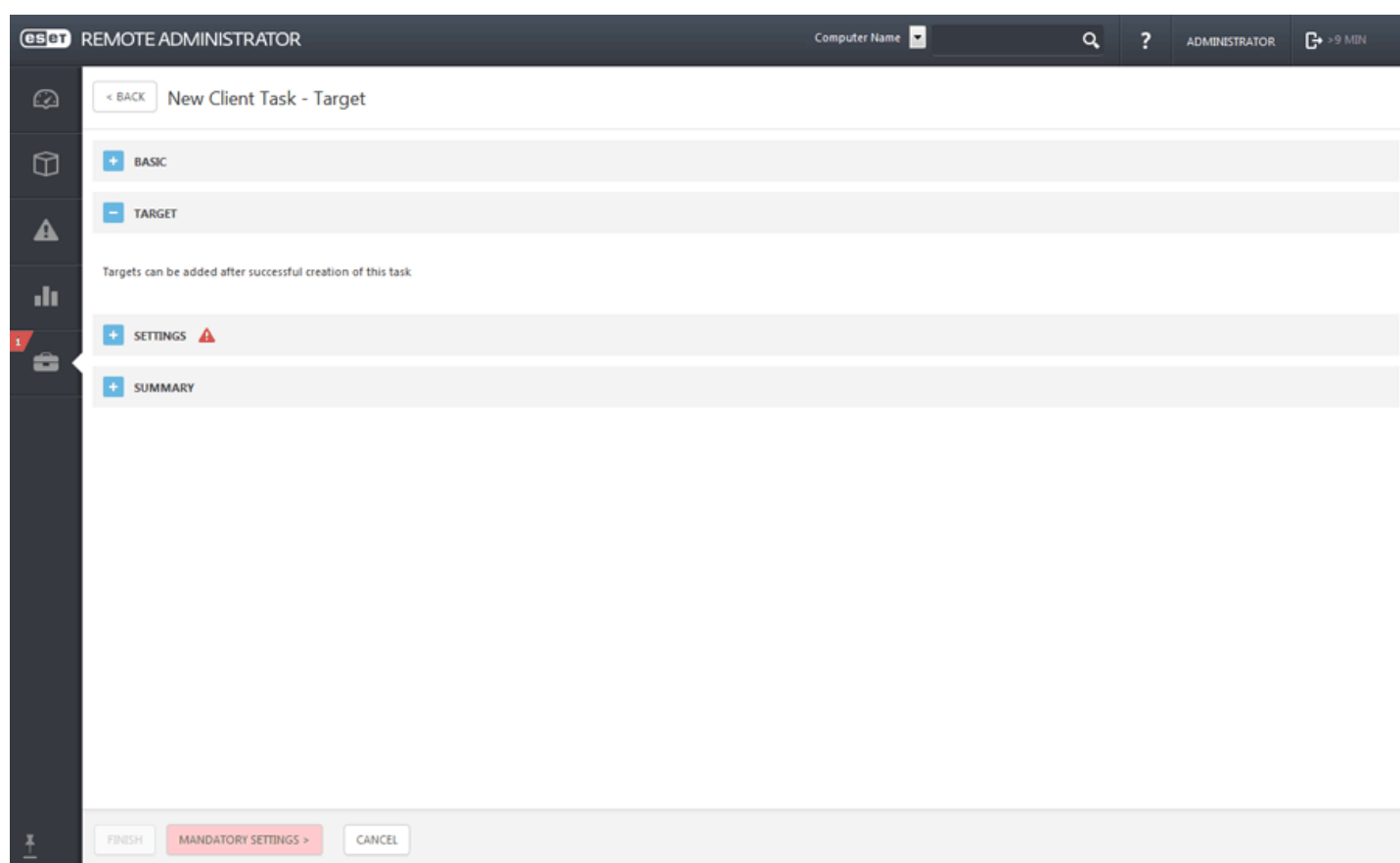
In the ERA Web Console, navigate to **Admin > Client Tasks**, select **Quarantine Management** from the **Task Types** list and then click **New**.

Basic

Enter basic information about the task, such as the **Name**, optional **Description** and the **Task Type**. The **Task Type** (see the list above) defines the settings and the behavior for the task. In this case you can use the **Quarantine Management** task.

Target

 **IMPORTANT:** It is not possible to add Targets while creating a Client Task. You will be able to add Targets after the task has been created. Configure **Settings** for the task and click **Finish** to create the task and then create a [Trigger](#) to specify Targets for the task.



Settings

Quarantine management settings

Action - Select the action to be taken with the object in Quarantine.

- **Restore Object(s)** (restores the object to its original location, but it will be scanned and if the reasons for the Quarantine persist, the object will be quarantined again)
- **Restore Object(s) and Exclude in Future** (restores the object to its original location and it will not be quarantined again).
- **Delete Object(s)** (deletes the object completely).

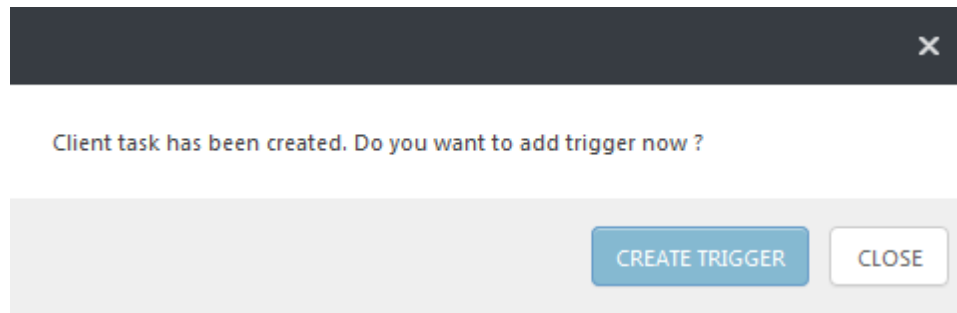
Filter type - Filter the objects in the Quarantine based on the criteria defined below. Either based on the hash string of the object or conditions.

Conditional filter settings:

- **Hash filter settings** - Add hash items into the field. Only known objects can be entered, for example, an object that has already been quarantined.
- **Occurred from/to** - Define the time range, when the object was quarantined.
- **Minimal/maximal size (bytes)** - Define the size range of the quarantined object (in bytes).
- **Threat name** - Select a threat from the quarantined items list.
- **Object name** - Select an object from the quarantined items list.

Summary

Review the summary of configured settings and click **Finish**. The Client Task is now created and a pop-up window will open. We recommend that you click [Create Trigger](#) to specify when this Client Task should be executed and on which Targets. If you click **Close**, you can create a [Trigger](#) later on.



5.2.2 Policies

You can use policies to configure your ESET product. Policies for ESET Virtualization Security are created and managed from the ESET Remote Administrator Webconsole in the **Admin > Policies** tab. Click **Policies** at the bottom and select [New](#) from the context menu.

Policies are used to push specific configurations to ESET products running on client computers. This allows you to avoid configuring each client's ESET product manually. A policy can be applied directly to individual [Computers](#) (virtual machines) as well as groups ([Static](#) and [Dynamic](#)). You can also assign multiple policies to a virtual machine or a group.

Policy application

Policies are applied in the order that Static Groups are arranged. This is not true for Dynamic Groups, where policies are enforced on child Dynamic Groups first. This allows you to apply policies with greater impact at the top of the Group tree and apply more specific policies for subgroups. Using [flags](#), an ERA user with access to groups located higher in the tree can override the policies of lower Groups. The algorithm is explained in detail in [How Policies are applied to clients](#).

Merging policies

The policy applied to a client is usually the result of multiple policies being [merged](#) into one final policy.

i NOTE: We recommend that you assign more generic policies (for example, general settings such as update server) to groups that are higher within the groups tree. More specific policies (for example device control settings) should be assigned deeper in the groups tree. The lower policy usually overrides the settings of upper policies when merging (unless defined otherwise with [policy flags](#)).

i NOTE: When you have a policy in place and remove it later on, the configuration of the virtual machine will not automatically revert back to their original settings once the policy is removed. The configuration will remain true to the last policy that was applied to the virtual machine. The same thing happens when a virtual machine becomes a member of a [Dynamic Group](#) to which a certain policy is applied that changes the virtual machine's settings. These settings remain even if the virtual machine leaves the Dynamic Group. Therefore, we recommend that you create a policy with default settings and assign it to the root group (**All**) to have the settings revert to defaults in such a situation. This way, when a virtual machine leaves a Dynamic Group that changed its settings, this virtual machine receives the default settings.

5.2.2.1 ESET Virtualization Security - Security Appliance policy

ESET Virtualization Security is fully manageable from the ERA Web Console. The updates, scanner properties and performance settings are configured in the **Admin > Policies** section of the ERA Web Console. To change a setting from the ERA Web Console, navigate to **Admin > Policies > ESET Virtualization Security Appliance - General - Recommended settings > ⚙ > New** and set the product in the **Settings** section to **ESET Virtualization Security - Security Appliance**. The following settings are available:

— BASIC

Enter a **Name** for the new policy. The **Description** field is optional.

— SETTINGS

Select your product (**ESET Virtualization Security - Security Appliance**) from the drop-down menu.

The screenshot displays the ESET Remote Administrator (ERA) Web Console interface. At the top, the header shows 'eset REMOTE ADMINISTRATOR' with a 'Computer Name' dropdown, a search icon, a help icon, and user information 'ADMINISTRATOR' with a session duration of '> 9 MIN'. The main content area is titled 'New Policy - Settings'. On the left, a sidebar contains navigation icons and a tree view with categories: ANTIVIRUS (1), UPDATE, VIRTUAL AGENT HOST, and TOOLS. The main panel is divided into sections: 'BASIC' (collapsed), 'SETTINGS' (expanded), 'ASSIGN' (collapsed), and 'SUMMARY' (collapsed). The 'SETTINGS' section shows a dropdown menu set to 'ESET Virtualization Security - Security Appliance' and a search bar. Below this, the 'BASIC' section is expanded, showing 'GENERAL' settings with 'Processing threads' set to '64' and 'SCANNER OPTIONS' with 'Enable antivirus protection' checked. At the bottom, there are 'FINISH' and 'CANCEL' buttons.

Select a category in the tree on the left. In the right pane, edit settings as required. Each setting is a rule for which you can set a [flag](#). To make navigation easier, all rules are counted. The number of rules you have defined in a particular section will be displayed automatically. Also, you'll see a number next to a category name in the tree on the left that displays the sum of rules in all its sections.

You can also use these suggestions to make policy editing easier:

- use **+** to set **Apply** flags to all item in current a section
- Click the **Trashcan** icon to delete rules

After a Policy is created, you can assign it to a **Static** or **Dynamic Group**. There are a two ways to assign a policy in the ERA Web Console:

- Under **Admin > Policies** select a policy and click **Assign Group(s)**. Select a static or Dynamic Group and click **OK**.
- Click **Admin > Groups > Group** or click the gear ⚙ icon next to the group name and select **Manage Policies**.

5.2.2.1.1 Antivirus

Basic

General

Processing threads – The number of processing threads used for parallel scans.

Scanner options

Enable antivirus protection – Detect, prevent and clean up threats which may infect your system.

5.2.2.1.2 Update

Basic

Update type – By default, the **Update type** is set to **Regular update** to ensure that update files will automatically be downloaded from the ESET server with the least network traffic. Pre-release updates (the **Pre-release update** option) are updates that have gone through thorough internal testing and will be available to the general public soon. You can benefit from enabling pre-release updates by having access to the most recent detection methods and fixes. However, pre-release updates might not be stable enough at all times and **SHOULD NOT** be used on production servers and workstations where maximum availability and stability is required. **Delayed update** allows clients to receive updates with a delay of at least X hours (updates tested in a real environment and therefore considered stable).

Update server list – The Update server is the location where updates are stored.

Set maximum database age automatically – Allows you to set the maximum time (in days) after which the virus signature database will be reported as out of date. The default value is 7.

Rollback

Create snapshots of update files – Creates a virus signature database snapshot.

Number of locally stored snapshots – Defines the number of previous virus database snapshots stored.

5.2.2.1.2.1 Primary/Secondary Server

Basic

Update server – We recommend that you leave the **Choose automatically** option selected.

Username/Password – Are intended for accessing the update server.

HTTP Proxy

Proxy mode – Select one of three options for the action to be performed.

Proxy server – Specify the proxy server address.

Port – Specify the proxy server communication port (default 3128).

Username/Password – Authentication data such as **Username** and **Password** is intended to access the proxy server. Complete these fields only if a username and password are required.

5.2.2.1.3 Virtual Agent Host

This section allows you to configure connection parameters to the vAgent Host such as **hostname**, **port** (default 9880) or **change certificate**. A certificate is required for a secure TLS connection and authentication. An Agent certificate is used to make sure that illegitimate agents will be denied by proxies and servers.

5.2.2.1.4 Tools

This section allows you to configure log maintenance (for example, the ESET LiveGrid reputation system or scheduler tasks). The proxy server and system console password can be edited here.

ESET LiveGrid®

Enable ESET LiveGrid® reputation system (recommended) – The ESET LiveGrid® reputation system improves the efficiency of ESET anti-malware solutions by comparing scanned files to a database of whitelisted and blacklisted items in the cloud.

SCHEDULER

Scheduler manages and launches scheduled tasks with predefined configuration and properties. Select the desired task by clicking **Edit**:

Log maintenance – Log files also contains leftovers from deleted records. This task optimizes records in log files on a regular basis to work effectively.

Regular automatic update – Schedules an Update task by updating the virus signature database and program modules.

5.2.2.1.4.1 Log files

Automatically delete records older than (days) – Log entries older than the specified number of days in this field will automatically be deleted (field becomes active when you turn on the toggle).


Optimize log files automatically – When enabled, log files will automatically be defragmented if the percentage is higher than the value specified in the **If the number of unused records exceeds (%)** field.

5.2.2.1.4.2 Proxy server

Select **Do not use proxy server** to specify that no proxy server will be used to update ESET Virtualization Security.

The **Connection through a proxy server** option should be selected if:

- A proxy server different from the proxy server specified in the global settings (**Tools > Proxy server**) should be used to update ESET Virtualization Security. In such a configuration, settings should be specified here: **Proxy server** address, communication **Port** (3128 by default), plus **Username** and **Password** for the proxy server if required.
- Proxy server settings are not set globally, but ESET Virtualization Security will connect to a proxy server for updates.
- Your computer is connected to the Internet via a proxy server. Settings are taken from Internet Explorer during program installation, but if they are subsequently changed (for example, if you change your ISP), please check that the HTTP proxy settings listed in this window are correct. Otherwise the program will not be able to connect to update servers.

 **NOTE:** Authentication data such as **Username** and **Password** is intended for accessing the proxy server. Complete these fields only if a username and password are required. Note that these fields should only be completed if you know you need a password to access the internet via a proxy server.

5.2.2.1.4.3 System console

Password – Specify a password for ESET Virtualization Security.

5.2.2.2 ESET Virtualization Security - Protected VM policy

ESET Virtualization Security is fully manageable from ERA Web Console. The updates, scanner properties, performance settings are configured in the **Admin > Policies** section of ERA Web Console. Navigate to **Admin > Policies > ESET Virtualization Security Appliance - General - Recommended settings > ⚙ > New** and set the product in the **Settings** section to **ESET Virtualization Security - Protected VM**. The following settings are available.

— BASIC

Enter a **Name** for the new policy. The **Description** field is optional.

— SETTINGS

Select your product **ESET Virtualization Security - Security Appliance** or **ESET Virtualization Security - Protected VM** from the drop-down menu.

The screenshot displays the ESET Remote Administrator web interface. At the top, the header shows 'eset REMOTE ADMINISTRATOR' with a 'Computer Name' search bar, a help icon, and user information 'ADMINISTRATOR' with a session duration of '>9 MIN'. The left sidebar contains navigation icons for Dashboard, Policies, Alerts, Reports, and a '1' next to the Settings icon. The main content area is titled 'New Policy - Settings'. It features a left-hand tree view with 'ANTIVIRUS' selected, showing sub-items 'Real-time file system protection' and 'On-demand computer scan'. The right pane is divided into sections: 'BASIC' (with a '+ -' icon and a trash icon), 'SCANNER OPTIONS' (with three toggle switches for 'Enable detection of potentially unwanted applications', 'Enable detection of potentially unsafe applications', and 'Enable detection of suspicious applications'), and 'EXCLUSIONS' (with a text field for 'Paths to be excluded from scanning' and an 'Edit' link). At the bottom of the main area are 'FINISH' and 'CANCEL' buttons.

Select a category in the tree on the left. In the right pane, edit settings as required. Each setting is a rule for which you can set a [flag](#). To make navigation easier, all rules are counted. The number of rules you have defined in a particular section will be displayed automatically. Also, you'll see a number next to a category name in the tree on the left that displays the sum of rules in all its sections.

You can also use these suggestions to make policy editing easier:

- use **+** to set **Apply** flags to all item in current a section
- Click the **Trashcan** icon to delete rules

After a Policy is created, you can assign it to a **Static** or **Dynamic Group**. There are a two ways to assign a policy in the ERA Web Console:

- Under **Admin > Policies** select a policy and click **Assign Group(s)**. Select a static or Dynamic Group and click **OK**.
- Click **Admin > Groups > Group** or click the gear ⚙ icon next to the group name and select **Manage Policies**.

5.2.2.2.1 Antivirus

BASIC

Scanner options allow you to enable or disable detection of the following:

- **Potentially unwanted applications** (PUAs) are not necessarily intended to be malicious, but may affect the performance of your computer in a negative way.
- **Potentially unsafe applications** refers to legitimate commercial software that has the potential to be misused for malicious purposes. Examples of potentially unsafe applications include remote access tools, password-cracking applications, and keyloggers (programs recording each keystroke typed by a user). This option is disabled by default.
- **Suspicious applications** include programs compressed with packers or protectors. These types of protectors are often exploited by malware authors to evade detection.

Exclusions enable you to exclude files and folders from scanning. To ensure that all objects are scanned for threats, we recommend only creating exclusions when it is absolutely necessary. Situations where you may need to exclude an object might include scanning large database entries that would slow your computer during a scan or software that conflicts with the scan.

5.2.2.2.2 Real-time file system protection

5.2.2.2.2.1 Basic

BASIC

Scan on

By default, all files are scanned upon opening, creation, or execution. We recommend that you keep these default settings, as they provide the maximum level of real-time protection for your computer:

- **File open** – Enables or disables scanning when files are opened.
- **File creation** – Enables or disables scanning when files are created.

Other

Increase network volumes compatibility – Enable on network file access problems.

5.2.2.2.2.2 ThreatSense parameters

THREATSENSE PARAMETERS

ThreatSense is technology comprised of many complex threat detection methods. This technology is proactive, which means it also provides protection during the early spread of a new threat. It uses a combination of code analysis, code emulation, generic signatures and virus signatures which work in concert to significantly enhance system security. The scanning engine is capable of controlling several data streams simultaneously, maximizing the efficiency and detection rate. ThreatSense technology also successfully eliminates rootkits.

ThreatSense parameters are highly optimized for each module, and their modification can significantly influence system operation. For example, changing parameters to always scan runtime packers, or enabling advanced heuristics in the Real-time file system protection module could result in a system slow-down (normally, only newly-created files are scanned using these methods). We recommend that you leave the default ThreatSense parameters unchanged for all modules except Computer scan.

Objects to scan

This section allows you to define which computer components and files will be scanned for infiltrations.

Runtime packers – After being executed, runtime packers (unlike standard archive types) decompress in memory. In addition to standard static packers (UPX, yoda, ASPack, FSG, etc.), the scanner is able to recognize several additional types of packers through the use of code emulation.

Scan options

Select the methods used when scanning the system for infiltrations. The following options are available:

Heuristics – A heuristic is an algorithm that analyzes the (malicious) activity of programs. The main advantage of this technology is the ability to identify malicious software which did not exist, or was not known by the previous virus signatures database. The disadvantage is a (very small) probability of false alarms.

Advanced heuristics/DNA/Smart signatures – Advanced heuristics consist of a unique heuristic algorithm developed by ESET, optimized for detecting computer worms and trojan horses and written in high level programming languages. The use of advanced heuristics greatly increases the threat detection capabilities of ESET products. Signatures can reliably detect and identify viruses. Utilizing the automatic update system, new signatures are available within a few hours of a threat discovery. The disadvantage of signatures is that they only detect viruses they know (or slightly modified versions of these viruses).

Cleaning

The cleaning settings determine the behavior of the scanner while cleaning infected files. There are 3 levels of cleaning:

No cleaning – Infected files will not be cleaned automatically. The program will display a warning window and allow the user to choose an action. This level is designed for more advanced users who know which steps to take in the event of an infiltration.

Normal cleaning – The program will attempt to automatically clean or delete an infected file based on a predefined action (depending on the type of infiltration). Detection and deletion of an infected file is signaled by a notification the bottom-right corner of the screen. If it is not possible to select the correct action automatically, the program provides other follow-up actions. The same happens when a predefined action cannot be completed.

Strict cleaning – The program will clean or delete all infected files. The only exceptions are the system files. If it is not possible to clean them, the user is prompted to select an action by a warning window.

Warning: If an archive contains a file or files which are infected, there are two options for dealing with the archive. In standard mode (Standard cleaning), the whole archive would be deleted if all the files it contains are infected files. In **Strict cleaning** mode, the archive would be deleted if it contains at least one infected file, regardless of the status of the other files in the archive.

Exclusions

An extension is the part of a file name delimited by a period. An extension defines the type and content of a file. This section of the ThreatSense parameter setup lets you define the types of files to scan.

Other

Enable Smart optimization – With Smart Optimization enabled, the most optimal settings are used to ensure the most efficient scanning level, while simultaneously maintaining the highest scanning speeds. The various protection modules scan intelligently, making use of different scanning methods and applying them to specific file types. If the Smart Optimization is disabled, only the user-defined settings in the ThreatSense core of the particular modules are applied when performing a scan.

– Limits

The Limits section allows you to specify the maximum size of objects and levels of nested archives to be scanned:

Object settings

Maximum object size – Defines the maximum size of objects to be scanned. The given antivirus module will then scan only objects smaller than the size specified. This option should only be changed by advanced users who may have specific reasons for excluding larger objects from scanning. Default value: *unlimited*.

Maximum scan time for object (sec.) – Defines the maximum time value for scanning of an object. If a user-defined value has been entered here, the antivirus module will stop scanning an object when that time has

elapsed, regardless of whether the scan has finished. Default value: *unlimited*.

Archive scan setup

Archive nesting level – Specifies the maximum depth of archive scanning. Default value: *10*.

Maximum size of file in archive – This option allows you to specify the maximum file size for files contained in archives (when they are extracted) that are to be scanned. Default value: *unlimited*.

i NOTE: We do not recommend changing the default values; under normal circumstances, there should be no reason to modify them.

5.2.2.2.3 Additional ThreatSense parameters

ADDITIONAL THREATSENSE PARAMETERS

Additional ThreatSense parameters for newly created and modified files – The probability of infection in newly-created or modified files is comparatively higher than in existing files. For this reason, the program checks these files with additional scanning parameters. Along with common signature-based scanning methods, advanced heuristics, which can detect new threats before the virus signature database update is released, are also used. In addition to newly-created files, scanning is performed on self-extracting files (.sfx) and runtime packers (internally compressed executable files). By default, archives are scanned up to the 10th nesting level and are checked regardless of their actual size. To modify archive scan settings, disable **Default archive scan settings**.

5.2.2.2.4 Clean file cache

Clean file cache minimizes system footprint when using Real-time protection. When enabled, clean scanned files are not scanned repeatedly unless they have been modified or the virus database has been updated. When disabled, all files are scanned each time they are accessed.

Enable clean cache file – Enable clean file cache to improve real-time protection performance but also increase memory usage.

Cache size (files) – Set clean file cache size.

5.2.2.2.3 On-demand computer scan

This section provides options to select scanning parameters.

5.2.2.2.3.1 Basic

Selected profile – Allows you to select one of the predefined scan profiles.

List of profiles – Allows you to create a custom scan profile that can be saved.

5.2.2.2.3.2 ThreatSense parameters

ThreatSense is technology comprised of many complex threat detection methods. This technology is proactive, which means it also provides protection during the early spread of a new threat. It uses a combination of code analysis, code emulation, generic signatures and virus signatures which work in concert to significantly enhance system security. The scanning engine is capable of controlling several data streams simultaneously, maximizing the efficiency and detection rate. ThreatSense technology also successfully eliminates rootkits.

ThreatSense engine setup options allow you to specify several scan parameters:

- File types and extensions that are to be scanned,
- The combination of various detection methods,
- Levels of cleaning, etc.

To enter the setup window, click **ThreatSense engine parameter setup** in the Advanced setup window for any module that uses ThreatSense technology (see below). Different security scenarios may require different configurations. With this in mind, ThreatSense is individually configurable for the following protection modules:

- Real-time file system protection,
- Idle-state scanning,
- Startup scan,
- Document protection,
- Email client protection,
- Web access protection,
- Computer scan.

ThreatSense parameters are highly optimized for each module, and their modification can significantly influence system operation. For example, changing parameters to always scan runtime packers, or enabling advanced heuristics in the Real-time file system protection module could result in a system slow-down (normally, only newly-created files are scanned using these methods). We recommend that you leave the default ThreatSense parameters unchanged for all modules except Computer scan.

Objects to scan

This section allows you to define which computer components and files will be scanned for infiltrations.

Email files – The program supports the following extensions: DBX (Outlook Express) and EML.

Mailboxes – Scans various mailboxes.

Archives – The program supports the following extensions: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE, and many others.

Self-extracting archives – Self-extracting archives (SFX) are archives needing no specialized programs – archives – to decompress themselves.

Runtime packers – After being executed, runtime packers (unlike standard archive types) decompress in memory. In addition to standard static packers (UPX, yoda, ASPack, FSG, etc.), the scanner is able to recognize several additional types of packers through the use of code emulation.

Scan options

Select the methods used when scanning the system for infiltrations. The following options are available:

Heuristics – A heuristic is an algorithm that analyzes the (malicious) activity of programs. The main advantage of this technology is the ability to identify malicious software which did not exist, or was not known by the previous virus signatures database. The disadvantage is a (very small) probability of false alarms.

Advanced heuristics/DNA/Smart signatures – Advanced heuristics consist of a unique heuristic algorithm developed by ESET, optimized for detecting computer worms and trojan horses and written in high level programming languages. The use of advanced heuristics greatly increases the threat detection capabilities of ESET products. Signatures can reliably detect and identify viruses. Utilizing the automatic update system, new signatures are available within a few hours of a threat discovery. The disadvantage of signatures is that they only detect viruses they know (or slightly modified versions of these viruses).

Cleaning

The cleaning settings determine the behavior of the scanner while cleaning infected files. There are 3 levels of cleaning:

No cleaning – Infected files will not be cleaned automatically. The program will display a warning window and allow the user to choose an action. This level is designed for more advanced users who know which steps to take in the event of an infiltration.

Normal cleaning – The program will attempt to automatically clean or delete an infected file based on a predefined action (depending on the type of infiltration). Detection and deletion of an infected file is signaled by a notification the bottom-right corner of the screen. If it is not possible to select the correct action

automatically, the program provides other follow-up actions. The same happens when a predefined action cannot be completed.

Strict cleaning – The program will clean or delete all infected files. The only exceptions are the system files. If it is not possible to clean them, the user is prompted to select an action by a warning window.

Warning: If an archive contains a file or files which are infected, there are two options for dealing with the archive. In standard mode (Standard cleaning), the whole archive would be deleted if all the files it contains are infected files. In **Strict cleaning** mode, the archive would be deleted if it contains at least one infected file, regardless of the status of the other files in the archive.

Exclusions

An extension is the part of a file name delimited by a period. An extension defines the type and content of a file. This section of the ThreatSense parameter setup lets you define the types of files to scan.

Other

When configuring ThreatSense engine parameters setup for a On-demand computer scan, the following options in **Other** section are also available:

Scan alternate data streams (ADS) – Alternate data streams used by the NTFS file system are file and folder associations which are invisible to ordinary scanning techniques. Many infiltrations try to avoid detection by disguising themselves as alternate data streams.

Enable Smart optimization – With Smart Optimization enabled, the most optimal settings are used to ensure the most efficient scanning level, while simultaneously maintaining the highest scanning speeds. The various protection modules scan intelligently, making use of different scanning methods and applying them to specific file types. If the Smart Optimization is disabled, only the user-defined settings in the ThreatSense core of the particular modules are applied when performing a scan.

– Limits

The Limits section allows you to specify the maximum size of objects and levels of nested archives to be scanned:

Object settings

Maximum object size – Defines the maximum size of objects to be scanned. The given antivirus module will then scan only objects smaller than the size specified. This option should only be changed by advanced users who may have specific reasons for excluding larger objects from scanning. Default value: *unlimited*.

Maximum scan time for object (sec.) – Defines the maximum time value for scanning of an object. If a user-defined value has been entered here, the antivirus module will stop scanning an object when that time has elapsed, regardless of whether the scan has finished. Default value: *unlimited*.

Archive scan setup

Archive nesting level – Specifies the maximum depth of archive scanning. Default value: *10*.

Maximum size of file in archive – This option allows you to specify the maximum file size for files contained in archives (when they are extracted) that are to be scanned. Default value: *unlimited*.

NOTE: We do not recommend changing the default values; under normal circumstances, there should be no reason to modify them.

5.2.3 Dynamic groups

Dynamic Groups are in essence custom filters defined in [Templates](#). Computers are filtered on the Agent side, so no extra information needs to be transferred to the server. The Agent decides on its own which Dynamic Groups a client belongs to. Dynamic Group templates are defined in ERA Web Console, see our Knowledgebase article for more information about how to [define Dynamic Group templates](#).

There are some pre-defined Dynamic Groups available after you have installed ESET Virtualization Security. If you need to, you can create custom Dynamic Groups. When creating them, [create a template](#) first and then [create a Dynamic Group](#).

Another approach is to [create a new Dynamic Group and new template on the fly](#).

More than one Dynamic Group can be created from one template.

A user can use Dynamic Groups in other parts of ERA. It is possible to assign policies to them or prepare a task for all computers therein.

Dynamic Groups can be nested under Static Groups or Dynamic Groups. However, the topmost group is always static.

All the Dynamic Groups under a certain Static Group only filter clients from that Static Group no matter how deep they are in the tree. Moreover, for nested Dynamic Groups, a child Dynamic Group filters the results of the parent Dynamic Group.

Policies are applied as described [here](#). However, once created, they can be [moved within the tree](#).

6. Common Questions

This chapter covers some of the most frequently asked questions encountered. Click a topic below to jump to it:

- [How to find vAgent Host in ESET Remote Administrator](#)
- [How to find ESET Virtualization Security in ESET Remote Administrator](#)
- [How to identify problematic VMs in ESET Remote Administrator](#)
- [How to add virtual machines to ESET Remote Administrator](#)
- [How to sync with vCenter](#)
- [How vAgent works](#)
- [How to update ESET Virtualization Security](#)
- [How to update vAgent Host](#)
- [How to update ESET Remote Administrator \(Web Console\)](#)
- [How the components interact](#)
- [How the ESET Virtualization Security interacts with VMware products](#)
- [What ports are needed for each component](#)
- [How to collect logs](#)
- [How to read the logs](#)
- [How to uninstall ESET Virtualization Security](#)

If you cannot find the solution to your problem/question in the list above, you can visit our regularly updated online [ESET Knowledgebase](#).

If necessary, you can contact [ESET Customer Care](#) with your questions or problems.

6.1 How to find vAgent Host in ESET Remote Administrator

From the ERA Web Console, navigate to **Computers**, select the **Subgroups** check box and then select **Virtual Agent Host** from drop-down menu.

i NOTE: If you are not able to find a particular computer in the list and know it is in your ERA infrastructure, make sure that all filters are turned off.

6.2 How to find ESET Virtualization Security in ESET Remote Administrator

From the ERA Web Console, navigate to **Computers** and filter for **ESET Virtualization Security** at the top of the page. Select the **Subgroups** check box and then select **Virtualization Security Appliance** from drop-down menu.

i NOTE: If you are not able to find a particular computer in the list and know it is in your ERA infrastructure, make sure that all filters are turned off.

6.3 How to identify problematic VMs in ESET Remote Administrator

A standard feature of ESET Remote Administrator is the ability to easily drill-down to problematic computers directly from the ERA Web console from **Dashboard** by adding a new **Agentless virtual machines with problems** template. Alternatively you can filter for these clients from the **Computers** tab.

i NOTE: See the [Edit report template topic of ESET Remote Administrator online help](#).

6.4 How to add virtual machines to ESET Remote Administrator

Virtual machines will appear automatically as soon as virtual machines are turned on and connected to the ESET Virtualization Security Appliance. Connected virtual machines will appear in the **Lost & Found** group. You can use Active Directory synchronization by running the **Static Group Synchronization** server task. For more information [see the ESET Remote Administrator Online Help](#).

6.5 How to sync with vCenter

By default, all protected machines are displayed under the name of vAgent Host and to resolve their correct names, a synchronization with vCenter is needed to map vCenter used names.

To achieve the same view as in vCenter, synchronize virtual machines running on your VMware vCenter Server.

From your ERA Web Console, navigate to **Admin > Server Task > Static Group Synchronization** and click **New...**

Basic

Enter basic information about the task, such as the **Name** and **Description** (optional). The **Task** type defines the settings and behavior of the task. Select the check box next to **Run task immediately after finish** to have the task run automatically after you click **Finish**.

Settings

Expand **settings** and click **Select** under **Static group name** - By default, the root for synchronized computers will be used. Alternatively you can create a new Static Group.

- **Object to synchronize** - Either **Computers and Groups**, or **Only Computers**.
- **Computer creation collision handling** - If the synchronization adds computers that are already members of the Static Group, you can select a conflict resolution method: **Skip** (synchronized computers will not be added) or **Move** (new computers will be moved to a subgroup).
- **Computer extinction handling** - If a computer no longer exists, you can either **Remove** this computer or **Skip** it.
- **Group extinction handling** - If a group no longer exists, you can either **Remove** this group or **Skip** it.

From the **Synchronization mode** drop-down menu select the **VMware** option.

In the **Server connection settings** section enter the DNS name or IP address of the VMware vCenter Server and enter the credentials used to access VMware vCenter Server.

In the **Synchronization settings** section, type the following information:

- **Structure view** - select the type of VMware structure that will be enumerated during the synchronization.
- **Structure path** - click **Browse...** to navigate through nodes and enter the path in VMware structure that will be enumerated. Leave it empty to synchronize entire tree.
- **Computer view** - select the attribute that will be used as a name of computer.

Triggers

Select an existing [trigger](#) for this task, or [create a new trigger](#). It is also possible to **Remove** or **Modify** a selected trigger.

Summary

Review the configuration information displayed here and if it is ok, click **Finish**. The task is now created and ready to be used.

6.6 How vAgent Host works

ESET Virtual Agent Host (vAgent Host) is a component of ESET Remote Administrator that virtualizes agent entities to allow management of agentless virtual machines. This solution enables vMotion for virtual machines connected to one vAgent Host and thereby automation, dynamic group utilization and the same level of task management as ERA Agent for physical computers.

Virtual Agent Host creates a virtual agent for each virtual machine on the host. You can have multiple vAgent Hosts connected to the ERA Server in your environment but virtual machines are not allowed to be vMotion-migrated between vAgent Hosts. Each virtual agent is awakening and connected to the ERA Server regularly to check for assigned tasks or policies to be performed. By default, 64 virtual agents are active simultaneously for 1 minute periods. If there are more than 64 virtual agents, activity is cycled. If a task or policy for several virtual machines must be performed immediately (or if ESET Virtualization Security discovers an infiltration), vAgent Host facilitates execution of the task or policy prior to other periodically connected virtual machines.

Virtual Agent Host also contains a component called Multi-proxy. This component performs synchronization between ERA Server and multi-agents controlled by vAgent Host. This solution reduces network traffic and system resources used by multi-agent, so it is possible to run several multi-agents at the same time.

The ESET Remote Administrator Agent is not installed on agentless protected machines. These virtual machines use a virtualized vAgent Host and cannot be assigned all of the same tasks as machines with ERA Agent installed.

The following tasks are available on agentless machines:

- identification of product components
- activation
- on-access/on-demand scan and scanner properties
- updates
- policies
- generating reports
- troubleshooting

6.7 How to activate and initial setup

To get more information about how to activate ESET Virtualization Security see the following topics:

1. How to get a license
2. How unilicense works
3. Online activation
4. Offline activation

6.7.1 How to get a license

There are two ways to obtain a new License Key; you can purchase a license online or at a retail location.

i NOTE: For more details about how to get a license see the [ESET License Administrator Online help](#) or [ESET Knowledgebase article](#).

6.7.2 How unilicense works

Unilicense is a simple licensing where one virtual machine represents one physical endpoint (for example, a PC or mobile device). Also, licensing per Host and per processor is supported.

For example, if you have 100 virtual machines that are protected by one ESET Virtualization Security, you need a license for ESET Virtualization Security and 100 endpoint seats for protected virtual machines.

6.7.3 Online activation

Licenses are available on the [ESET License Administrator portal](#). ESET Virtualization Security and ESET Remote Administrator Virtual Agent host can be activated only from ESET Remote Administrator 6.

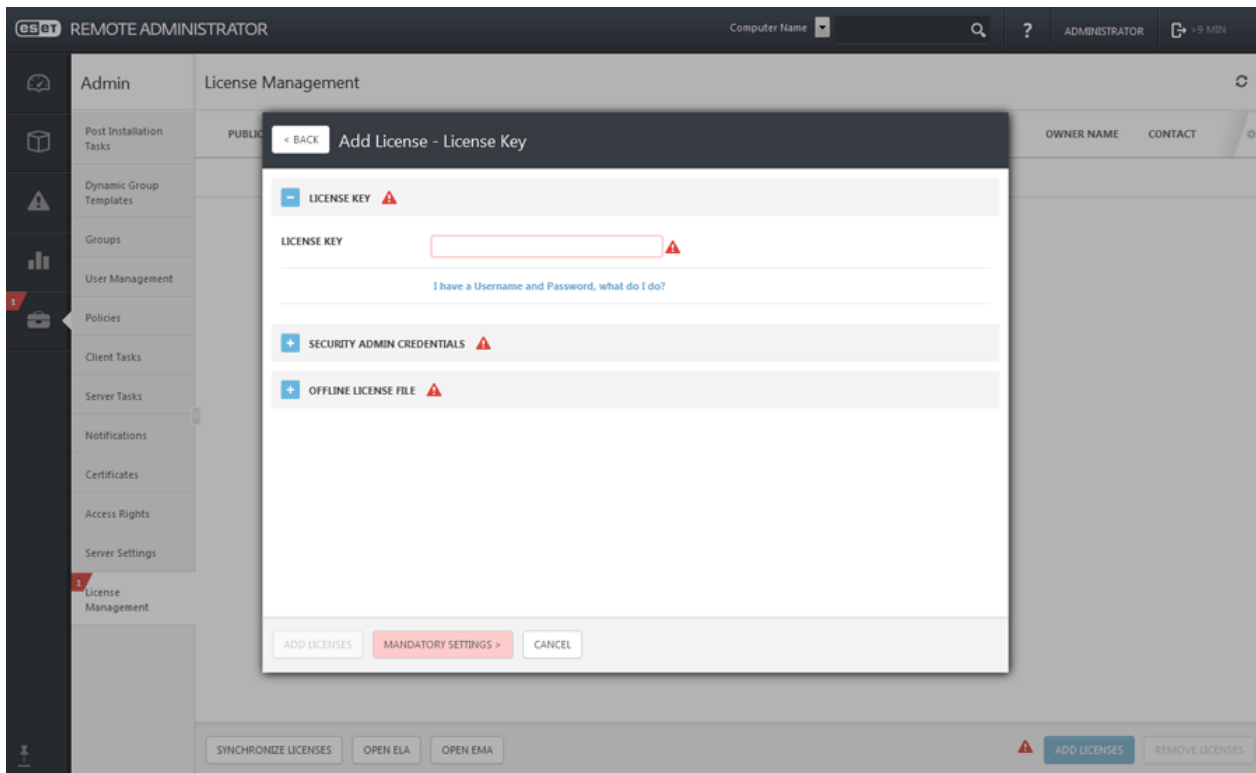
From your ERA Web Console, navigate to **Admin > License Management** and click **Add Licenses**.

The screenshot displays the ESET Remote Administrator (ERA) Web Console interface. The top navigation bar includes the ESET logo, the text 'REMOTE ADMINISTRATOR', a 'Computer Name' dropdown menu, a search icon, a help icon, the user role 'ADMINISTRATOR', and a session duration indicator '>9 MIN'. The left sidebar contains a list of administrative functions: Admin, Post Installation Tasks, Dynamic Group Templates, Groups, User Management, Policies, Client Tasks, Server Tasks, Notifications, Certificates, Access Rights, Server Settings, and License Management. The 'License Management' section is currently active, showing a table with the following data:

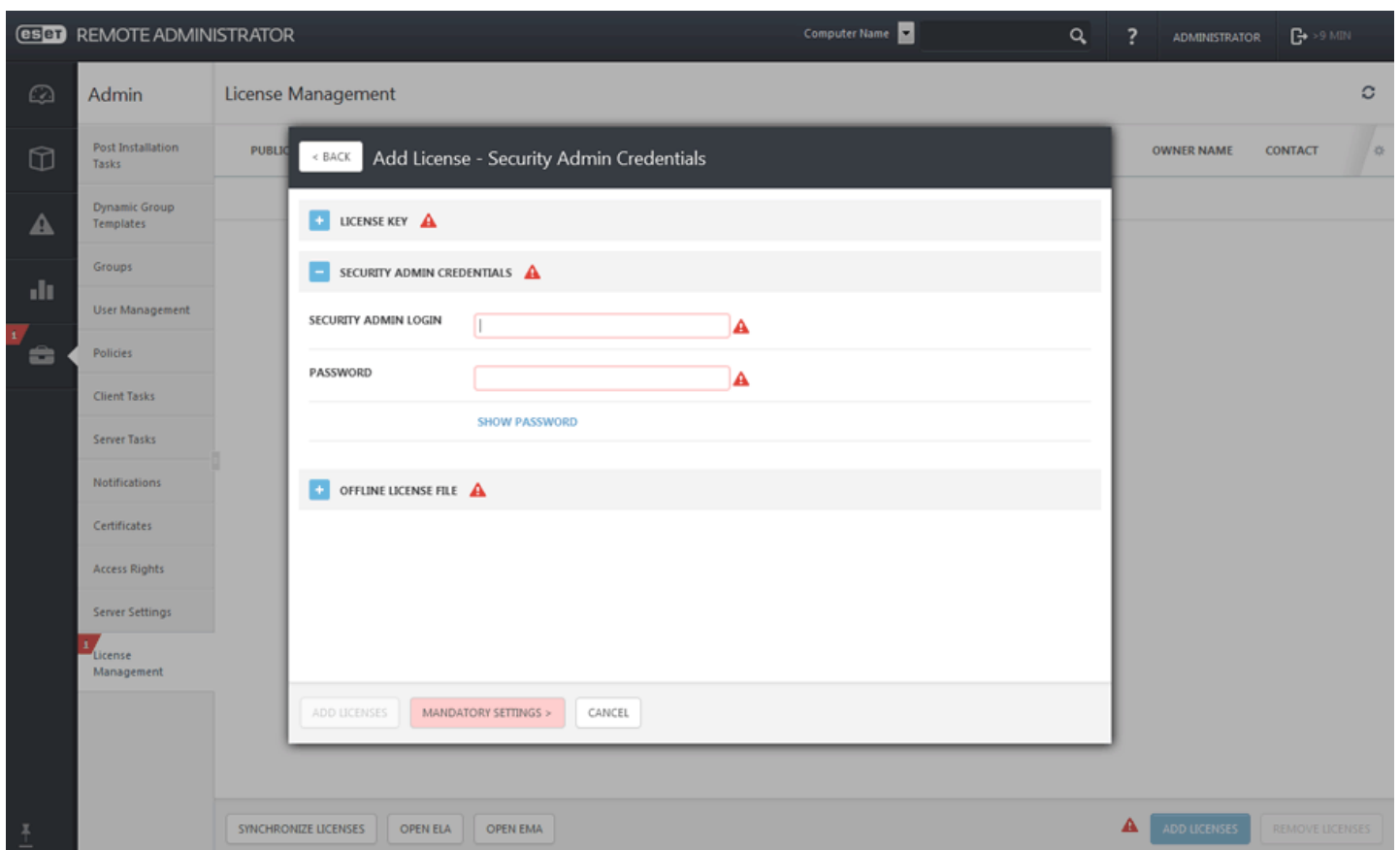
PUBLIC ID	PRODUCT NAME	STATUS	UNITS	SUBUNITS	EXPIRES	OWNER NAME	CONTACT
333-3VW-PSP	Bussiness	ESET Endpoint Antivirus for Wind...	✓	0/0 (2 offline)	2016 Nov 10 13:00:00	ESET TEST ERA	

At the bottom of the console, there are buttons for 'SYNCHRONIZE LICENSES', 'OPEN ELA', 'OPEN EMA', 'ADD LICENSES', and 'REMOVE LICENSES'.

1. Type or copy and paste the **License key** you received when you purchased your ESET security solution into the **License Key** field. If you are using legacy license credentials (a Username and password), [convert](#) the credentials to a license key. If the license is not registered, it will trigger the registration process on the ELA portal (ERA will provide the URL valid for registration based on the origin of the license).



2. Enter your **Security Admin** account credentials (ERA will display all delegate licenses later in ERA License Manager).




i NOTE: Communication with license servers is outgoing only. See our [ESET Knowledgebase article](#).

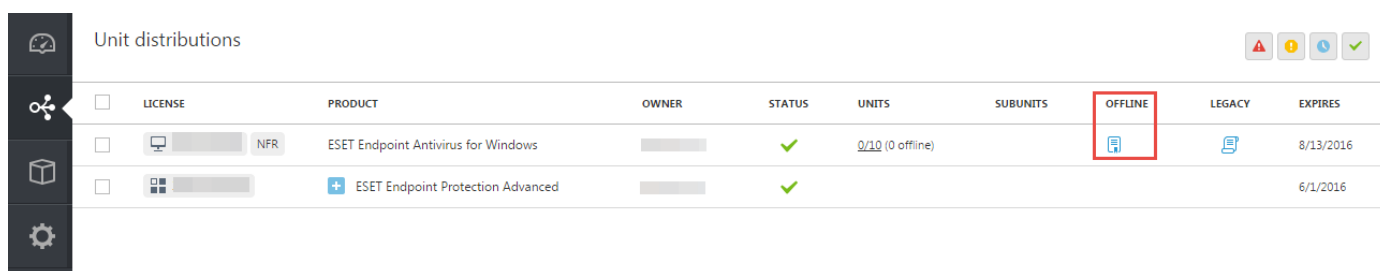
6.7.4 Offline activation





ESET Virtualization Security and ESET Remote Administrator Virtual Agent host can be activated using an offline license file when not connected to the internet.

How to create and download your offline license file

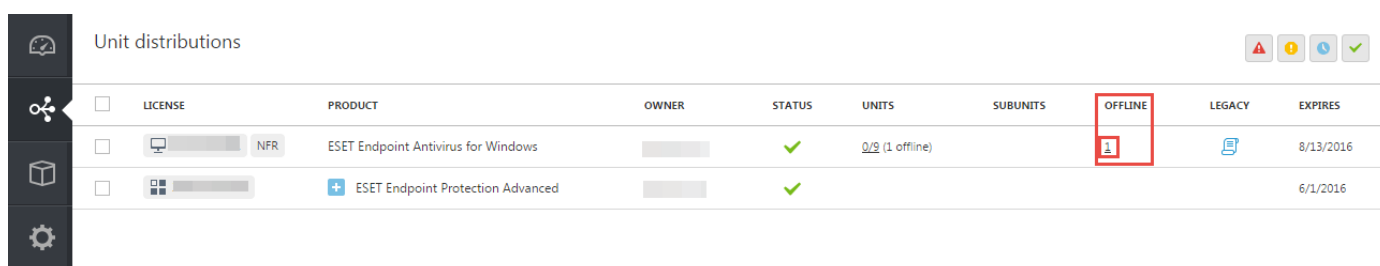
To create and download an offline license file, register a **Security Admin** account on [ESET License Administrator portal](#) and log in. If you want to download offline licenses that can be used to activate offline products, follow the steps below:




1. Navigate to the license for which you want to download the offline license file. Remember that licenses are platform specific - you need to download a specific license type to activate the specific product. Click the document symbol  under **Offline**.



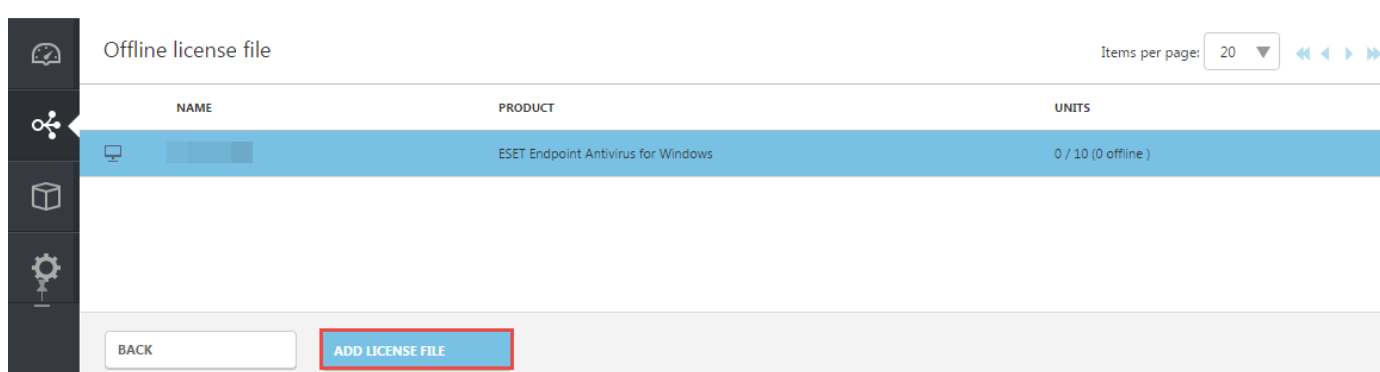
LICENSE	PRODUCT	OWNER	STATUS	UNITS	SUBUNITS	OFFLINE	LEGACY	EXPIRES
 NFR	ESET Endpoint Antivirus for Windows		✓	0/10 (0 offline)				8/13/2016
	+ ESET Endpoint Protection Advanced		✓					6/1/2016


NOTE: If the license has already been used to create offline license files, the document symbol will be replaced with a number. In this case, click the number.



LICENSE	PRODUCT	OWNER	STATUS	UNITS	SUBUNITS	OFFLINE	LEGACY	EXPIRES
 NFR	ESET Endpoint Antivirus for Windows		✓	0/10 (1 offline)		1		8/13/2016
	+ ESET Endpoint Protection Advanced		✓					6/1/2016

2. Check the license information and then click **Add License File**.



NAME	PRODUCT	UNITS
	ESET Endpoint Antivirus for Windows	0 / 10 (0 offline)

BACK ADD LICENSE FILE

3. Select the specific product from the available **Product** list, set the number of **Units** you want to activate offline, enter the desired name (will be shown in the list of generated offline licenses) and click **Generate**.

If you want the particular ESET product activated by this offline license file to be able to receive updates directly from the ESET servers (if the target machine has internet access), select the check box next to **Include Username and Password**. If you do not supply these credentials, the product must be updated from a different location (mirror) configured by you.

If you select the check box next to **Allow management with Remote Administrator**, you will be asked to provide a **Server Token**. To obtain the Server Token, follow the instructions in [ESET Remote Administrator](#)

[Online help](#). Once the Server Token is listed, make a note of it and type it into the **Server Token** field in ESET License Administrator.

Offline license file ✕

PRODUCT	ESET Endpoint Antivirus for Windows ▼
UNITS	1 / 10
LICENSE FILENAME	EEA testing offline lic.
<input type="checkbox"/> Include Username and Password When included it is possible to update from ESET servers.	
<input type="checkbox"/> Allow management with Remote Administrator	

GENERATE CANCEL

4. New offline license files will be generated. As you can see, the number of available units decreases as the offline licenses are subtracted from the total number of units. Select the check box next to the offline license and click **Download**.

Offline license file

Items per page: 20

<input type="checkbox"/>	NAME	PRODUCT	UNITS
<input type="checkbox"/>		ESET Endpoint Antivirus for Windows	0 / 9 (1 offline)
<input checked="" type="checkbox"/>	EEA testing offline lic.	ESET Endpoint Antivirus for Windows	1

BACK ADD LICENSE FILE REMOVE DOWNLOAD

Or click the offline license and from the pop up menu and select **Download**.

Offline license file

Items per page: 20

<input type="checkbox"/>	NAME	PRODUCT	UNITS
<input type="checkbox"/>		ESET Endpoint Antivirus for Windows	0 / 9 (1 offline)
<input type="checkbox"/>	EEA testing offline lic.	ESET Endpoint Antivirus for Windows	1

Offline license file

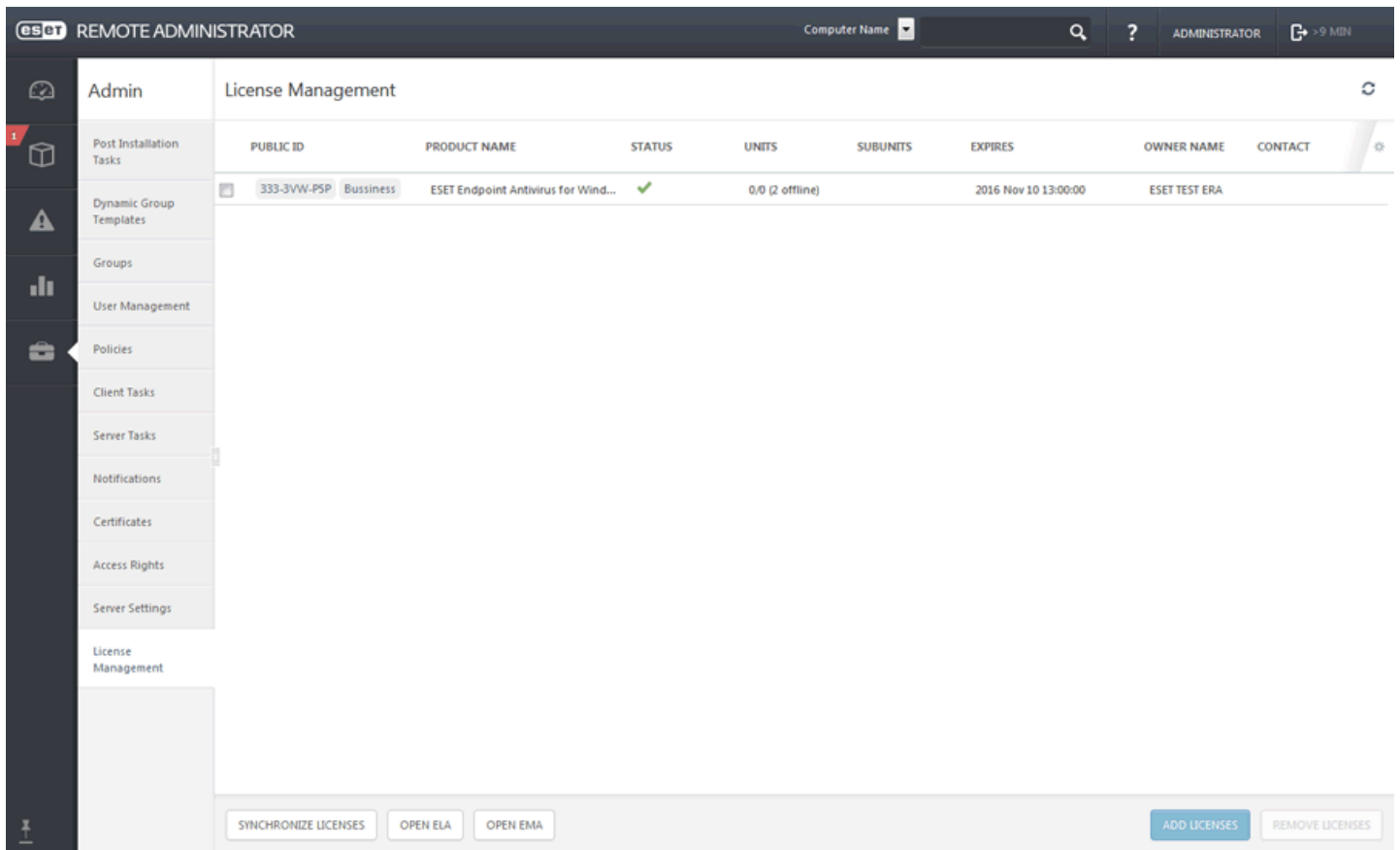
- Download
- Remove

BACK ADD LICENSE FILE REMOVE DOWNLOAD

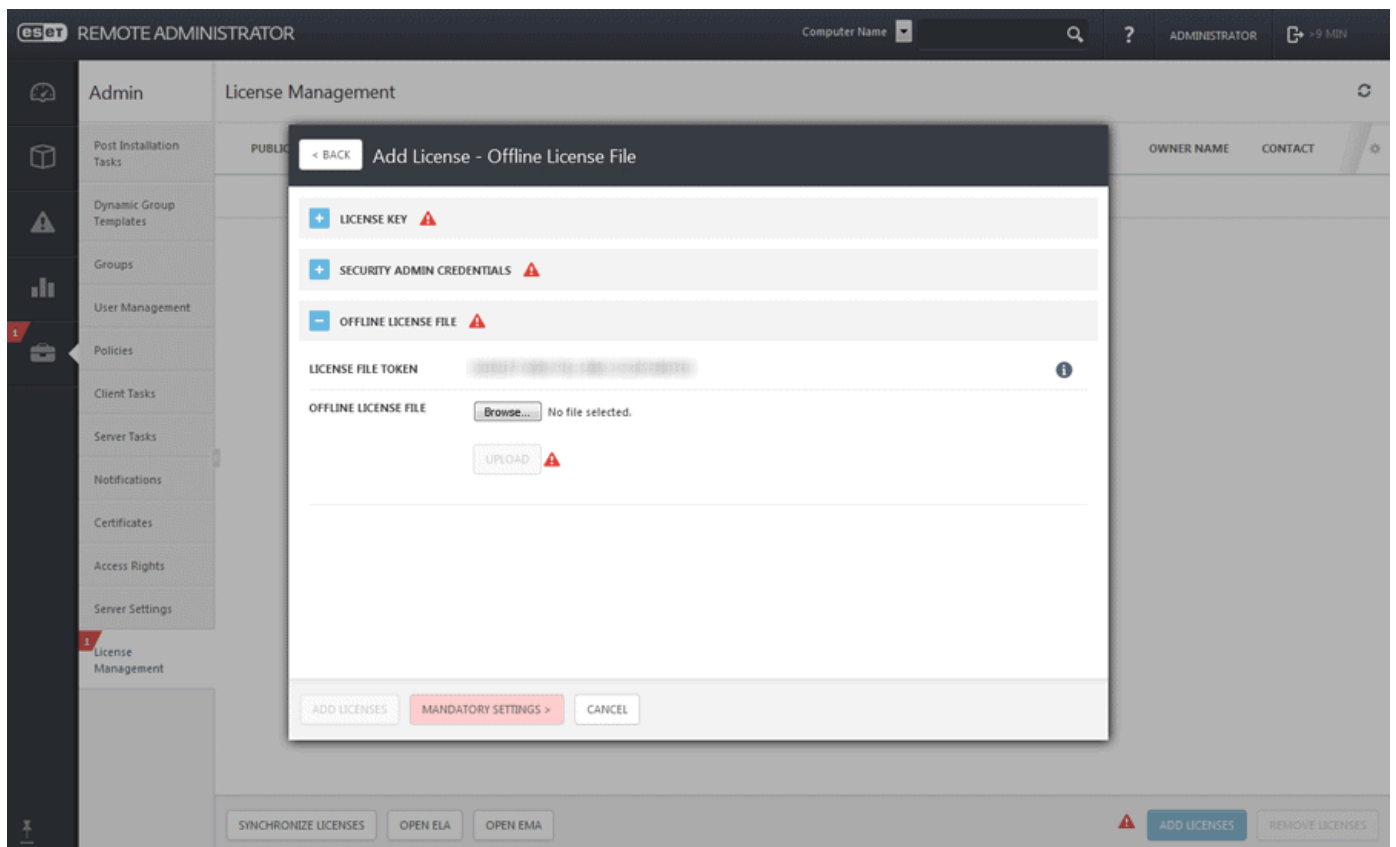
If you want to create another offline license file, click **Add License File**.

How to activate ESET Virtualization Security from ERA Web Console using an offline license file

From your ERA Web Console, navigate to **Admin > License Management** and click **Add Licenses**.



1. Enter the **Offline license file** - Exported using the ELA portal and include all information about product(s) ERA is able to manage. You will need to enter a specific **License file token** in the ESET License Administrator portal when generating an offline license file, otherwise the license file won't be accepted by ESET Virtualization Security.



2. Click the document symbol  to save the offline license file.

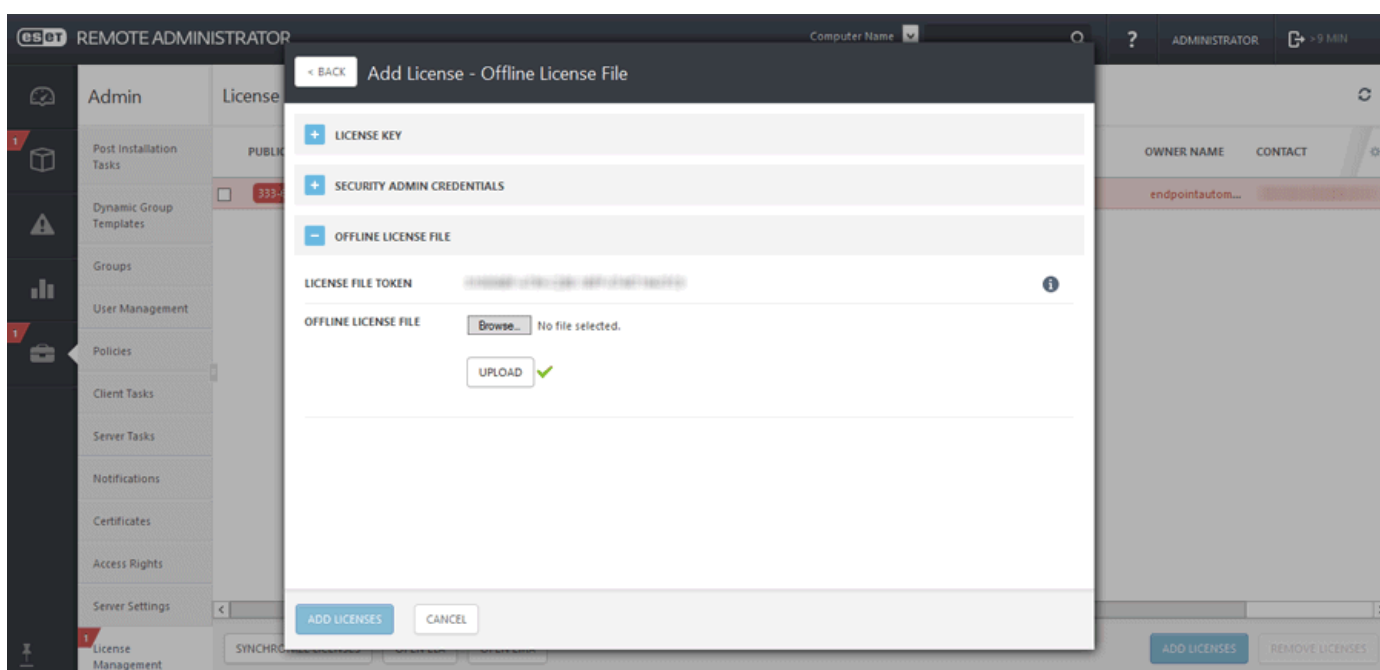
Offline license file ✕

LICENSE	333-3FM-SPF ESET Endpoint Security
UNITS	0 / 4 (1 offline)

PRODUCT	UNITS	LICENSE FILE
ESET Endpoint Security	1	Remove

ADD LICENSE FILE
CLOSE

- Go back to ERA License Management, click **Add licenses**, Browse for the offline license file you've exported in ELA and then click **Upload**.



NOTE: ESET Virtualization Security represents one virtual machine. ESET Virtualization Security reports the number of protected and connected machines. For more information read this [ESET Knowledgebase article](#).

6.8 How to update ESET Virtualization Security

Updating ESET Virtualization Security and updating the operating system is an important part of protecting your environment. Pay attention to their proper configuration and operation.

Updating ESET Virtualization Security from ESET Remote Administrator

The **Software Install** task is used to install software on your client computers. It is primarily intended to install ESET products, but you can use it to install any software you like.

Basic

Enter basic information about the task, such as the **Name**, optional **Description** and the **Task Type**. The **Task Type** (see the list above) defines the settings and the behavior for the task. In this case you can use the **Software Install** task.

Target

IMPORTANT: It is not possible to add Targets while creating a Client Task. You will be able to add Targets after the

task has been created. Configure **Settings** for the task and click **Finish** to create the task and then create a [Trigger](#) to specify Targets for the task.

Settings

Select the check box next to **I agree with application End User License Agreement** if you agree. See [License Management](#) or [EULA](#) for more information.

Click **<Choose ESET License>** and select the appropriate license for the installed product from the list of available licenses.

Click **<Choose package>** to select a installer package from the repository or specify a package URL. A list of available packages where you can select the ESET product you want to install (for example, ESET Endpoint Security) will be displayed. Select your desired installer package and click **OK**. If you want to specify a URL where the installation package is located, type or copy and paste the URL (for example *file:///\\pc22\\install\\ees_nt64_ENU.msi*) into the text field (do not use a URL that requires authentication).

http://server_address/ees_nt64_ENU.msi - If you are installing from a public web server or from your own HTTP server.

file:///\\pc22\\install\\ees_nt64_ENU.msi - if you are installing from network path.

file:///C:\\installs\\ees_nt64_ENU.msi - if you are installing from local path.

NOTE: Please note that both ERA Server and ERA Agent require access to the internet to access the repository and perform installation. If you do not have internet access, you can install the client software locally.

If you need to, you can specify [Installation parameters](#), otherwise leave this field empty. Select the check box next to **Automatically reboot when needed** to force an automatic reboot of the client computer after installation. Alternatively, you can leave this option deselected and the the client computer can be restarted manually.

Summary

Review the summary of configured settings and click **Finish**. The Client Task is now created and a pop-up window will open. We recommend that you click [Create Trigger](#) to specify when this Client Task should be executed and on which Targets. If you click **Close**, you can create a [Trigger](#) later on.

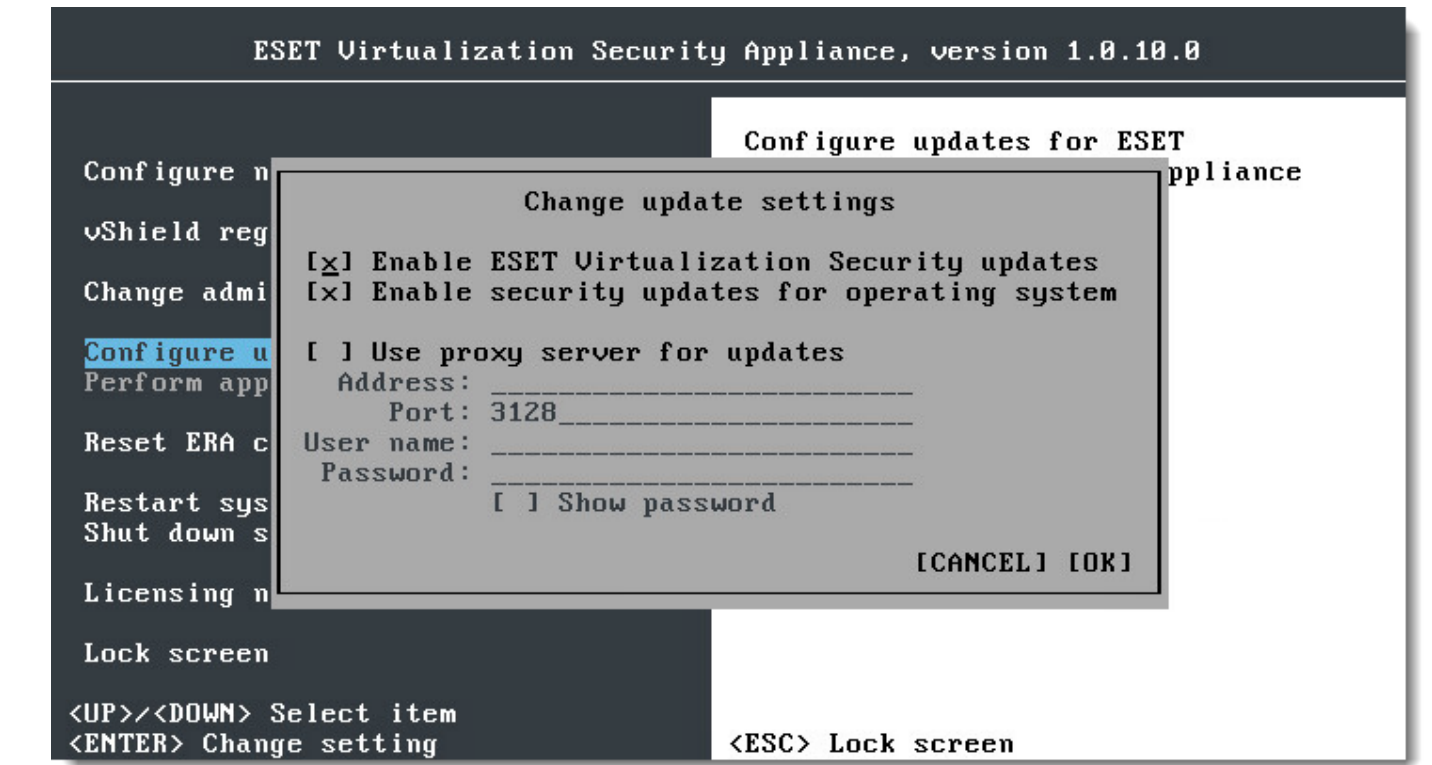
Client task has been created. Do you want to add trigger now ?

CREATE TRIGGER

CLOSE

Updating ESET Virtualization Security and operating system using text-based user interface (console)

Enter the management mode by pressing **Enter** and then select **Configure updates**. You can choose to update ESET Virtualization Security, your operating system, or both. To update ESET Virtualization Security and apply available system updates select the **Perform appliance update** option.



Updating ESET Virtualization Security manually by replacing an appliance

For step-by-step instruction see [ESET Virtualization Security deployment](#) or [installation of ESET Virtualization Security using deployment tool](#).

6.9 How to update vAgent Host

The **Remote Administrator Components Upgrade** task is used to upgrade ERA components (ERA vAgent Host, ERA Proxy, ERA Server and MDM). For example, when you want to upgrade from ERA version 6.1.28.0, 6.1.33.0 to ERA version 6.2.x. See [Components upgrade](#) for detailed instructions.

Basic

Enter Basic information about the task, such as the **Name**, optional **Description** and the **Task Type**. The **Task Type** (see the list above) defines the settings and the behavior for the task. In this case you can use the **Remote Administrator Components Upgrade** task.

Target

IMPORTANT: It is not possible to add Targets while creating a Client Task. You will be able to add Targets after the task has been created. Configure **Settings** for the task and click **Finish** to create the task and then create a [Trigger](#) to

specify Targets for the task.

The screenshot shows the 'New Client Task - Target' window in the Remote Administrator application. The window has a dark header bar with the 'eset' logo, 'REMOTE ADMINISTRATOR' text, a 'Computer Name' dropdown, a search icon, a help icon, 'ADMINISTRATOR' text, and a '+ 9 MIN' indicator. On the left is a dark sidebar with icons for Home, Tasks, Alerts, Reports, and a red notification badge. The main content area has a '< BACK' button and the title 'New Client Task - Target'. Below the title are expandable sections: 'BASIC' (expanded), 'TARGET' (collapsed), 'SETTINGS' (collapsed with a red warning icon), and 'SUMMARY' (collapsed). A message states: 'Targets can be added after successful creation of this task'. At the bottom are 'FINISH', 'MANDATORY SETTINGS >', and 'CANCEL' buttons.

Settings

Select the check box next to **I agree with application End User License Agreement** if you agree. See [License Management](#) or [EULA](#) for more information.

- **Reference Remote Administrator Server** - Select ERA Server version from the list. All ERA components will be upgraded to versions compatible with the selected server.
- **Automatically reboot when needed** - You can force a reboot of the client operating system, if the installation requires it.

Summary

Review the summary of configured settings and click **Finish**. The Client Task is now created and a pop-up window will open. We recommend that you click [Create Trigger](#) to specify when this Client Task should be executed and on which Targets. If you click **Close**, you can create a [Trigger](#) later on.


The screenshot shows a dark pop-up dialog box with a close button (X) in the top right corner. Below the dialog box, the text 'Client task has been created. Do you want to add trigger now ?' is displayed. At the bottom are two buttons: 'CREATE TRIGGER' (blue) and 'CLOSE' (white).

6.10 How to update ESET Remote Administrator Web Console

ESET Remote Administrator Web Console can be updated in two ways:

- [Using ESET Remote Administrator Components upgrade task](#)
- [Manual upgrade on windows](#)
- [Locally, when installed on Linux as standalone installer](#)

Using ESET Remote Administrator Components upgrade task

 **IMPORTANT:** It is necessary to backup your database and all certificates (Certificate Authority, Server Certificate, Proxy Certificate and Agent Certificate). To backup your certificates do the following:

- Export your [Certification Authority Certificates](#) from an old ERA Server to a .der file and save to external storage.
- Export your [Peer Certificates](#) /ERA Agent, ERA Server, ERA Proxy/ and private key .pfx file from an old ERA Server and save to external storage.

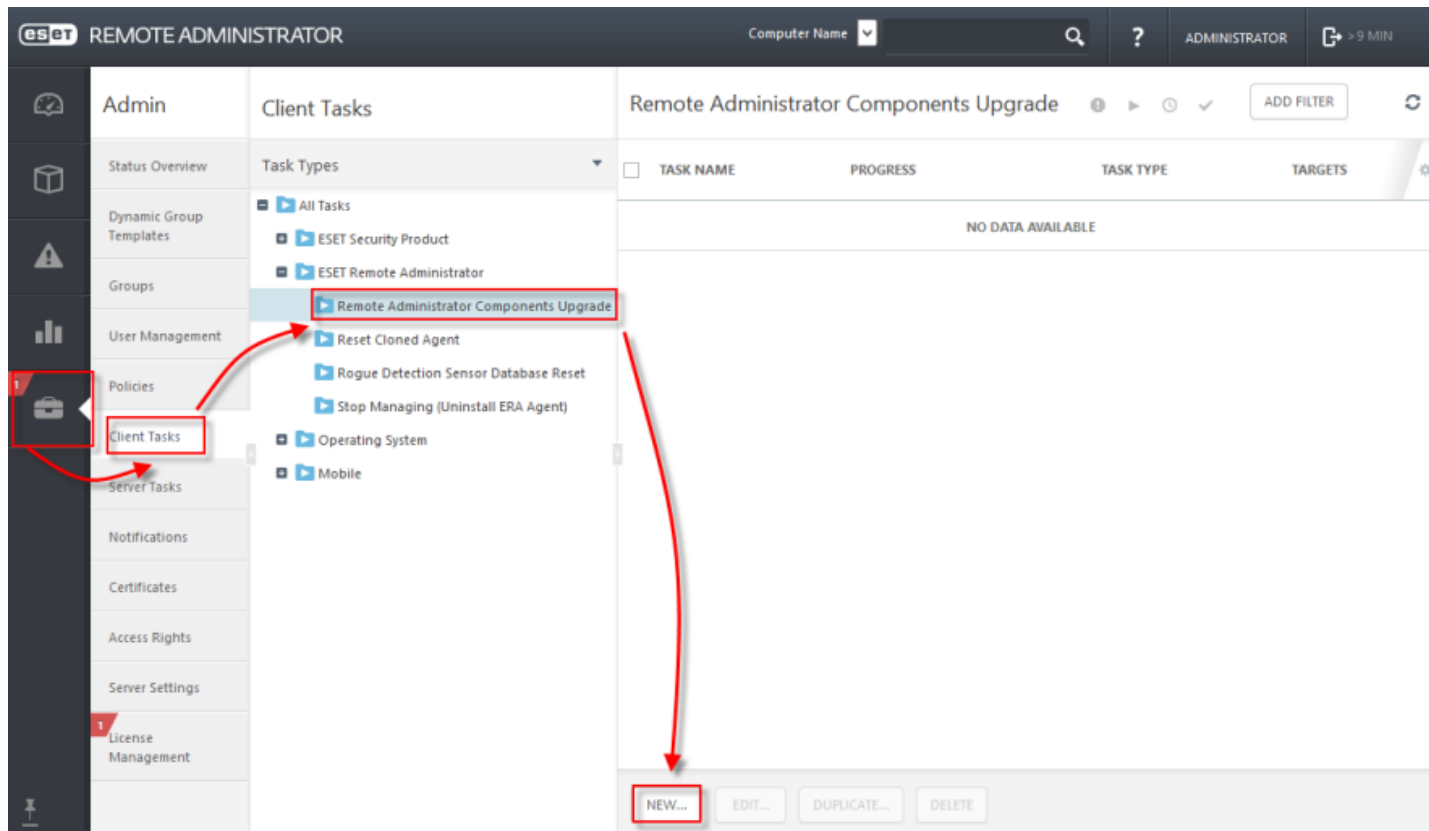
 **NOTE:** Upgrade of the Web Console using Components upgrade task is possible:

- for Windows, if the Web Console was installed via All-in-one installer
- for Linux, if the Web Console is installed in one of the following locations:

- /var/lib/tomcat8/webapps/
- /var/lib/tomcat7/webapps/
- /var/lib/tomcat6/webapps/
- /var/lib/tomcat/webapps/
- /usr/lib/tomcat/webapps/
- /usr/share/tomcat/webapps/
- /usr/share/tomcat6/webapps/

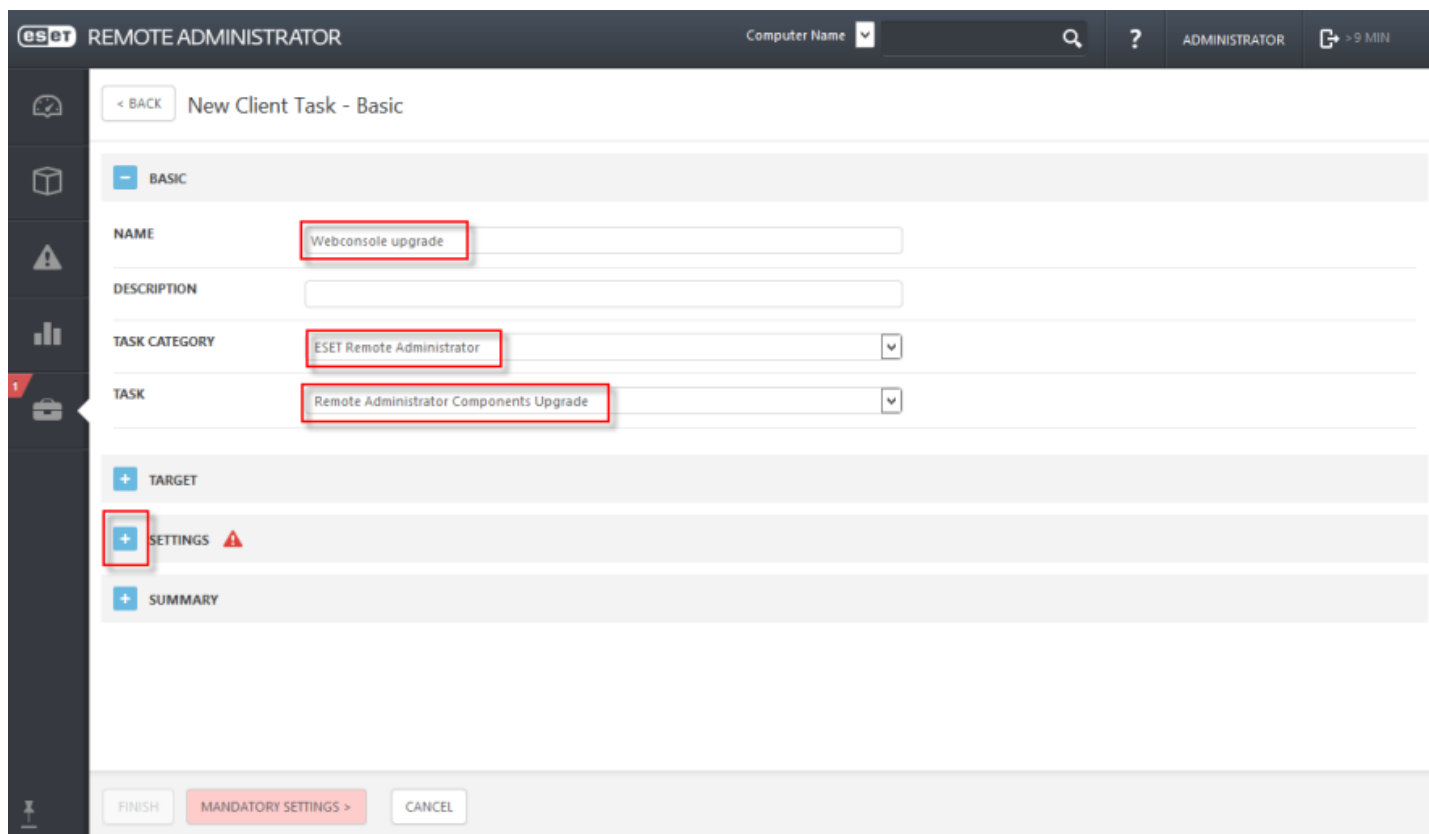
When running this task, we highly recommend that you select **group All** as a target to ensure the whole ERA infrastructure is upgraded.

1. Click **Admin > Client Tasks** and navigate to **All Tasks > ESET Remote Administrator > Remote Administrator Components Upgrade**.
2. Click **New** to set up your new task.



Basic

1. Enter a task **Name** and **Description**.
2. In the **Task category** drop-down menu, select **ESET Remote Administrator** and in the **Task** drop-down menu, select **Remote Administrator Components Upgrade**.



Settings

1. Select the check box next to I agree with application End User License Agreement, if you agree. See [License Management](#) or [EULA](#) for more information. Click the <**CHOOSE SERVER**> and from the list select the version

of ERA Server with which the upgraded components will be compatible. Click **OK** to confirm and proceed to the **Summary**.

Summary

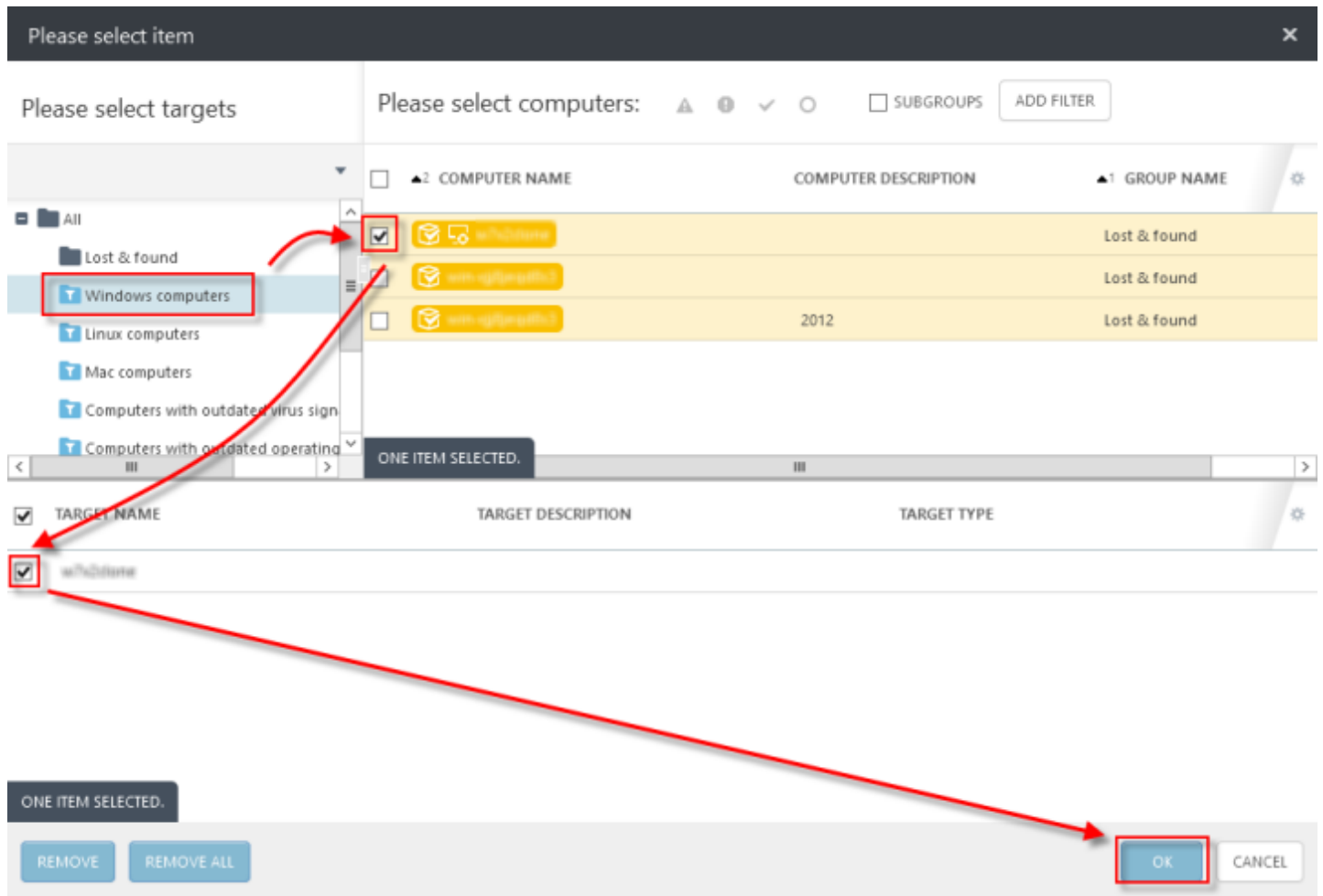
1. Review the summary of configured settings and click **Finish**. Click **Create trigger** to continue. (Or you click **Close** and create trigger later.)

Basic

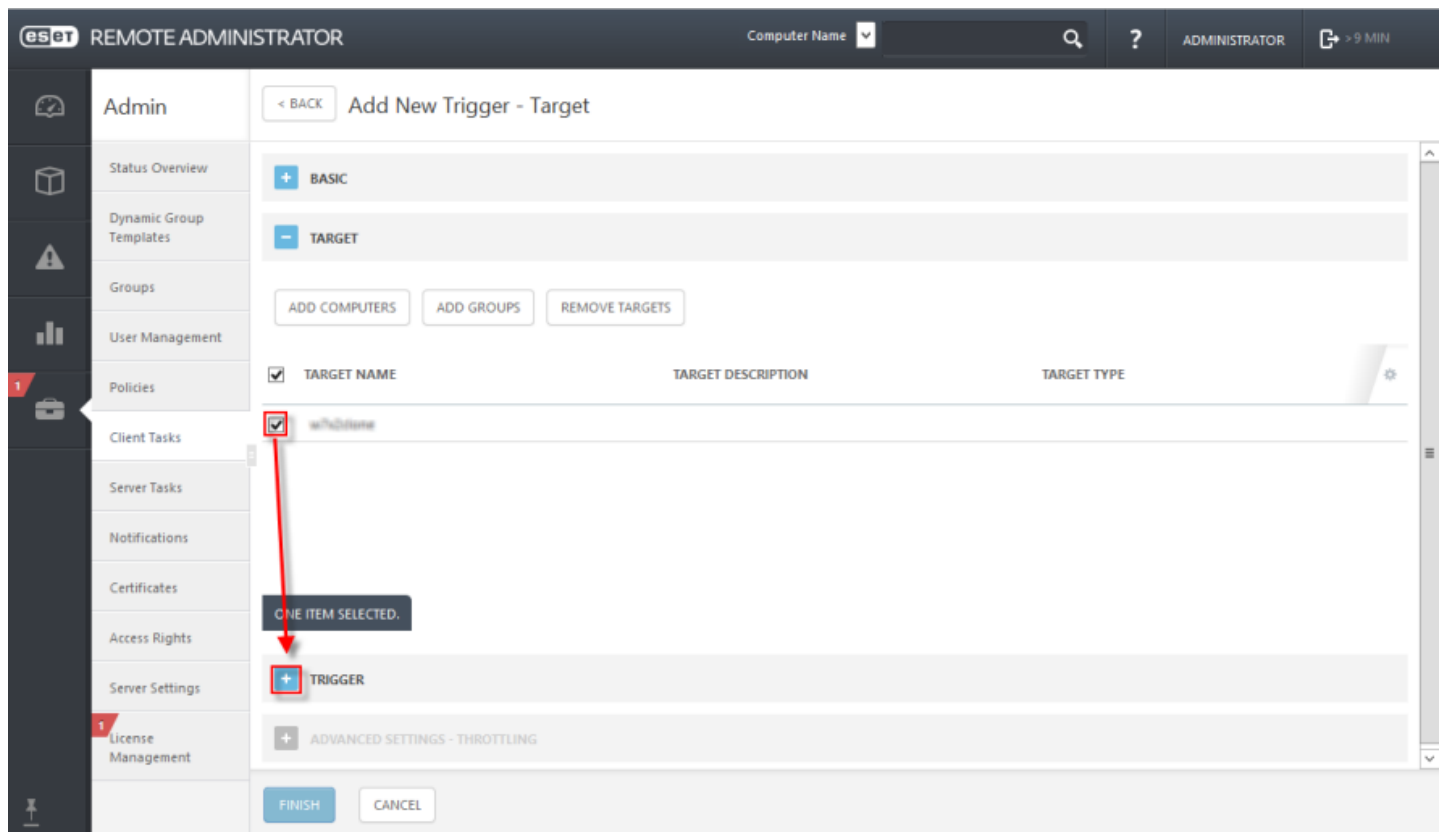
1. Type name for the trigger in the **Trigger Description** field.

Target

1. Click **Add Computers** or **Add Groups** to define the target computers or groups where you want to execute the client task. If you want to upgrade only Web Console, select only the computer where it is installed.
2. In the target selection window, select a group to display client computers or devices in that group. Select the check box next to a group to display subgroups and clients that belong to that group in the selected targets section.
3. After adding groups and clients to the selected targets section, select the check box(es) next to them in the bottom pane.
4. Click **OK** when you are finished adding computers and groups.

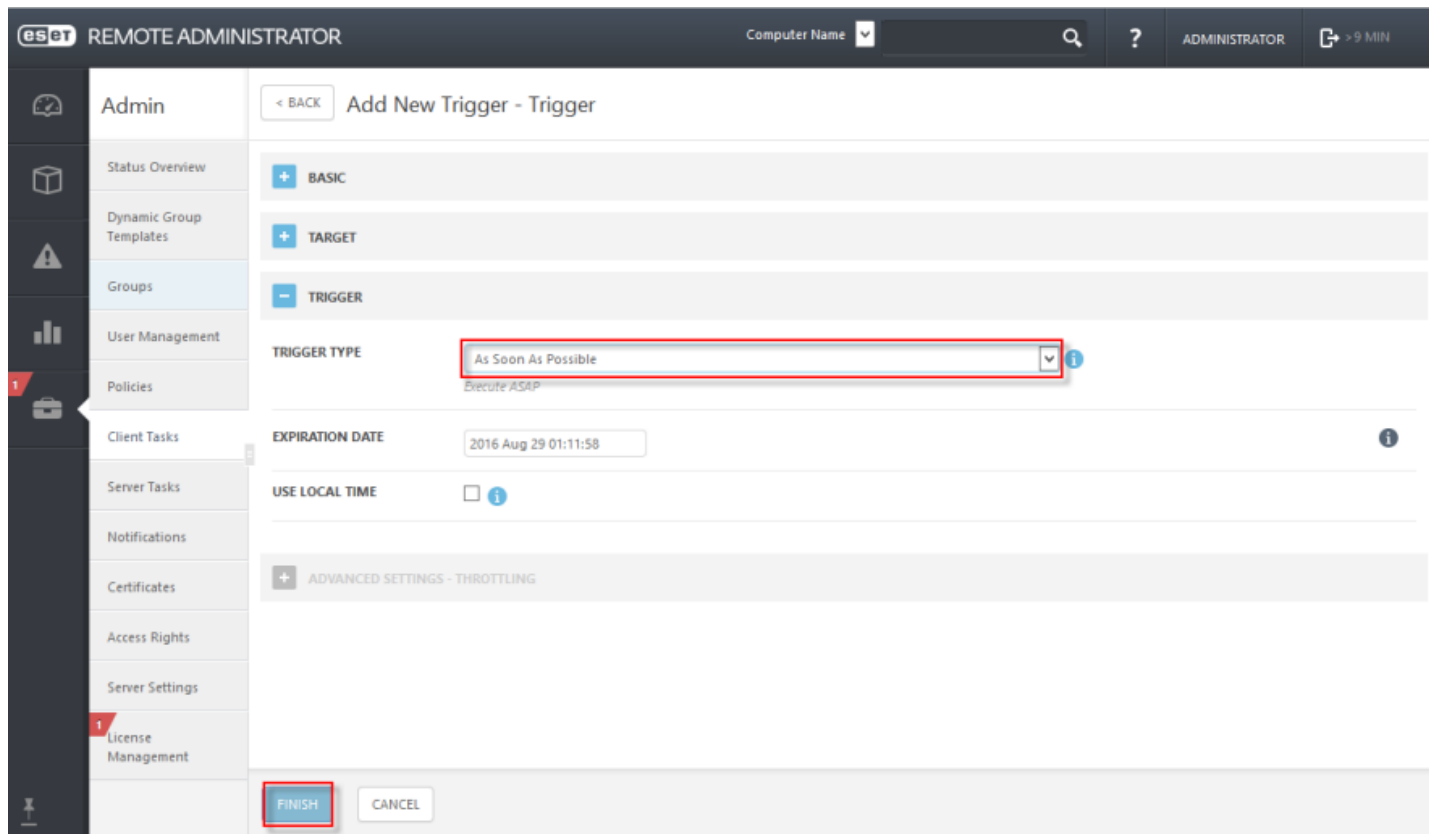


5. In the **Target** section, select the check box(es) next to the targets you added.



Trigger

1. Complete the applicable event trigger settings for the task (**As Soon As Possible** is selected by default). Click **Finish** to create the trigger. Your new task will display in the **Client Tasks** window.



Manual installation on windows

- a. [Download the necessary ERA 6 Web Console installer.](#) (Name of the installer file is era.war)
- b. Stop Apache Tomcat. Navigate to your %TOMCAT_HOME%\bin directory (for example, C:\Program Files\Apache Tomcat\Tomcat7\bin) and double-click tomcat7w.exe.
- c. Back up the C:\Program Files (x86)\Apache Software Foundation\Tomcat 7.0\webapps\era folder and all of its contents.

! IMPORTANT: File location will differ on 32-bit systems: On 32-bit systems, the "Program Files (x86)" folder is named "Program files".

- d. Copy the EraWebServerConfig.properties configuration file located at: C:\Program Files (x86)\Apache Software Foundation\Tomcat 7.0\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties.
- e. Delete the contents of the original C:\Program Files (x86)\Apache Software Foundation\Tomcat 7.0\webapps\era folder (including the era.war file).
- f. In the downloaded installer files from Step a. , locate the era.war file and extract it to: C:\Program Files (x86)\Apache Software Foundation\Tomcat 7.0\webapps\era.
- g. Move the EraWebServerConfig.properties configuration file from Step d to: C:\Program Files (x86)\Apache Software Foundation\Tomcat 7.0\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config.
- h. Start the Apache Tomcat service. Depending on your system configuration, allow up to 40 seconds for the service to start.
- i. Open **ESET Remote Administrator** Web Console (ERA Web Console) in your web browser and log in. [How do I open ERA Web Console?](#)

Locally, when installed on Linux as standalone installer

Before installing the ERA Web Console component, make sure all [prerequisites](#) are met. To install ERA Web Console, follow these steps:

1. Run the following commands to copy the *era.war* file to the Tomcat folder:

Debian and Ubuntu distributions	<code>sudo cp era.war /var/lib/tomcat7/webapps/</code>
CentOS, RedHat and Fedora distributions	<code>sudo cp era.war /var/lib/tomcat/webapps/</code>
OpenSUSE distribution	<code>sudo cp era.war /usr/share/tomcat/webapps/</code>

Alternatively, you can extract the contents of *era.war* to */var/lib/tomcat/webapps/era/*

2. Run the following command to restart the Tomcat service and deploy the *.war* file:

Debian and Ubuntu distributions	<code>sudo service tomcat7 restart</code>
CentOS, RedHat and Fedora distributions	<code>sudo service tomcat restart</code>
OpenSUSE distribution	<code>sudo service tomcat restart</code>

Test the connection to ERA Web Console after installation. Open the following link in your browser on localhost (a login screen should be displayed):

`http://localhost:8080/era` or, if you access the server remotely, http://IP_ADDRESS_OR_HOSTNAME:8080/era

i NOTE: HTTP port, by default 8080, is set during manual Apache Tomcat installation. You can also set up [HTTPS connection for Apache Tomcat](#).

6.11 How the components interact

ERA Server <-> vCenter

ERA Server synchronizes static groups with folders/resource pools on vCenter.

ERA Server <-> ERA Agent/vAgent Host

1. ERA Server requests tasks and configuration data (such as policies etc.)
2. ERA Agent/vAgent Host provides logs

ERA Server <-> ERA Web Server

Requests initiated by Web Console user and ERA Server responses.

ESET Virtualization Security <-> Guest virtual machines

1. File data transfer from/to guest virtual machines
2. ESET Virtualization Security collects events from guest virtual machines and registry information

ESET Virtualization Security <-> VMware vShield Manager

This communication serves for vShield registration purposes.

6.12 How ESET Virtualization Security interacts with VMware products

- ESET Virtualization Security connects to VMware vShield Manager during the registration process.
- ESET Virtualization Security maintains a permanent connection with vShield Endpoint ESXi module and VMware Tools on guest virtual machines via EPSec Library provided by VMware.
- ESET Virtualization Security periodically connects to vShield Manager to check registration status.
- ERA Server synchronizes its computer structure with vCenter.
- The deployment tool connects to vCenter in order to deploy appliances.

6.13 What ports are needed for each component

ESET Virtualization Security communicates with vShield Endpoint using TCP port 48651. The charts below list all possible network communication ports used when ESET Remote Administrator and its components are installed in your infrastructure.

ERA Server:

Protocol	Port	Usage	Descriptions
TCP	2222	ERA Server listening	Communication between ERA Agents and ERA Server
TCP	2223	ERA Server listening	Communication between <%ERAC%> and ERA Server, used for Assisted installation

ERA Web Console web server:

Protocol	Port	Usage	Descriptions
TCP	443	Listening	HTTP SSL Web Console call

ERA Proxy:

Protocol	Port	Usage	Descriptions
TCP	2222	Listening	Communication between ERA Agents and ERA Proxy

HTTP Proxy:

Protocol	Port	Usage	Descriptions
TCP	3128	Listening	HTTP Proxy (update caching)

The pre-defined ports 2222, 2223 can be changed if they are already in use by other applications.

i NOTE: For the proper function of ESET Remote Administrator, none of the ports above can be used by other applications.

i NOTE: Make sure to configure any firewall(s) within your network to allow communication via the ports listed above.

i NOTE: For more about ports see [ESET Knowledgebase article](#).

6.14 How to collect logs

Diagnostic tool is a part of all ERA components. It is used to collect and pack logs that are used by developers to solve problems with product components. Run the Diagnostic tool, select a root folder where the logs will be saved, and then select the actions to be taken (see **Actions** below).

Location of the **Diagnostic Tool**:

Windows

Folder `C:\Program Files\ESET\RemoteAdministrator\<product>\` , a file called **Diagnostic.exe**.

Linux

Path on the server: `/opt/eset/RemoteAdministrator/<product>/` , there is a **Diagnostic<product>** executable (one word, for example, **DiagnosticServer**, **DiagnosticAgent**)

Actions

- **Dump logs** - A logs folder is created where all logs are saved.
- **Dump process** - A new folder is created. A process dump file is generally created in cases where a problem was detected. When a serious problem is detected, a dump file is created by system. To check it manually, go to the folder `%temp%` (in Windows) or folder `/tmp/` (in Linux) and insert a dmp file.
i NOTE: Service (Agent, Proxy, Server, RD Sensor, FileServer) must be running.
- **General application information** - The GeneralApplicationInformation folder is created and inside it the file GeneralApplicationInformation.txt. This file contains text information including the product name and product version of the currently installed product.
- **Action configuration** - A configuration folder is created where file storage.lua is saved.

6.15 How to read the logs

Log files contain information about all important events that have occurred. Logging is an essential part of system analysis, threat detection and troubleshooting. Logging is performed actively in the background with no user interaction. Information is recorded based on the current log verbosity settings. It is possible to view logs directly from ESET Remote Administrator.

Logs can be found as zip files in the following locations:

Windows

Folder `C:\Program Files\ESET\RemoteAdministrator\<product>\`

Linux

Path on the server: `/var/eset/RemoteAdministrator/<product>/`

The following logs in are available in html format:

last-error.html – protocol (table) that displays the last error recorded while the ERA Agent is running.

status.html – a table showing the current state of communication (synchronization) of ERA Agent with ERA Server.

trace.log – a detailed report of all ERA Agent activity including any errors that have been recorded.

6.16 How to uninstall ESET Virtualization Security

To remove ESET Virtualization Security from your VMware ESXi host, perform the following steps in your environment:

1. [Deactivate all virtual machines \(remove licenses from ERA\)](#)
2. [Remove ESET Virtualization Security appliance from each host \(unregister from VMware vShield and delete appliances\)](#)
3. [Turn off vAgent Host](#)
4. [Delete virtual machines](#)

6.16.1 Deactivate virtual machines from ERA

From the **ERA Web Console > Computers**, filter for the virtual machines you want to deactivate and then click **Computers > Deactivate Products**.

Licenses for the deactivated client computers will display as inactive in [ESET License Administrator](#). ESET security products running on client computers will deactivate the next time that they connect to the internet. This configuration makes it possible to deactivate ESET products on computers not managed by ERA.

6.16.2 Remove ESET Virtualization Security

Remove the ESET Virtualization Security appliance from each host. Press **Enter** to access management mode and then select **vShield registration > Unregister**. After you complete these steps, ESET Virtualization Security is no longer registered in VMware vShield.

6.16.3 Turn off vAgent Host

The easiest way to disable vAgent Host is to find vAgent Host in the ERA Web Console and then create and perform a **Stop Managing (Uninstall ERA Agent)** task. To do so, follow the steps below:

1. From the ERA Web Console, navigate to **Computers** and select the group where Virtual Agent Host is located (if you are not sure, select the **All** group).
2. Select **Virtual Agent Host** from the drop-down menu.
3. Make sure the **Subgroups** option above this drop-down menu is selected.
4. Click the desired Virtual Agent Host and select **New task...** from the action menu.
5. Enter a **name** and **description** for the task.
6. Select **Stop Managing (Uninstall ERA Agent)** from the **Task** drop-down menu.
7. There is no need to add **Targets** when creating a task from **Computers**.
8. Click **Finish**.

After you complete the steps above, Virtual Agent Host is no longer managed by ERA (vAgent Host is removed).

6.16.4 Delete virtual machines

To delete a virtual machine from the host, right-click the name of the virtual machine in your environment and select **Delete from Disk** from the context menu or select the virtual machine and navigate to **Inventory > Virtual Machine** and select **Delete from disk**.

6.17 How to access system logs

- Enter Management mode and select menu **Access system logs** and then select **Enable SFTP access to the system logs**. Enter your password for SFTP access and select **Apply**.
- Run your SFTP client (we recommend to use free WinSCP SFTP client).
- Enter the Hostname (you can find it in ESET Virtualization Security in management mode > **Configure network**).
- Default SFTP port is 22. As User name, enter **logs**. Now you can **save** the configuration or just click **Login**.
- When you are prompted for password, enter the password that you used in ESET Virtualization Security.
- Now you have access to ESET Virtualization Security logs.

In communication with ESET Customer Care, you are normally prompted for these files:

- messages, dmesg, boot.log, yum.log (and all rotated copies (for example messages-20160411, maillog-20160411 and so on).
- all files from audit folder
- eset/RemoteAdministrator/EraAgentInstaller.log
- all files from eset/RemoteAdministrator/Agent/

7. Troubleshooting

7.1 Where to find the logs for ESET Remote Administrator

Logs are used by developers to solve problems with product components.

The latest ERA Server log file can be found here:

/var/eset/RemoteAdministrator/<product>/

i NOTE: For more information see [How to collect logs](#).

7.2 Where to find the logs for vAgent

Logs are used by developers to solve problems with product components.

The log files can be found here:

/var/log/eset/RemoteAdministrator/VAgentHost/

i NOTE: For more information see [How to collect logs](#).

7.3 What to send to Customer Care

Sending system data such as logs will help ESET solve your problem. ESET will use this data only to provide technical assistance. Below is the list of logs ESET Customer Care may request for each component.

ESET Remote Administrator

/var/eset/RemoteAdministrator/Server/

Virtual Agent Host

*/var/log/eset/RemoteAdministrator/VAgentHost/trace.**

Virtual Agent Multi-proxy

*/var/log/eset/RemoteAdministrator/VAgentHost/Proxy/trace.**

Multi-agent

*/var/opt/eset/RemoteAdministrator/VAgentHost/MultiAgent/<uuid>/ProgramLogs/trace.**

i NOTE: When the stack is full for the **trace.log** file, another file called **trace.1** is created.

i NOTE: Multi-agent has a separate folder according to universal unique identifier (UUID) of each virtual machine. When you have a large number of virtual machines, you can create archives from that folder up one level */var/opt/eset/RemoteAdministrator/VAgentHost/MultiAgent*.

7.4 What ports to enable for licensing

ESET products communicate with resources on the Internet using standard HTTP protocol on Port 80 or using HTTPS on Port 443.

i NOTE: For more information see [ESET Knowledgebase article](#).

7.5 What ports to enable for HTTP Proxy (update caching)

Apache HTTP Proxy, is a service that can be used in combination with ESET Remote Administrator 6 and later. It performs a similar role to the mirror server feature popular in older products (see our [Knowledgebase article](#) for more information). The pre-defined port for the HTTP Proxy service is [port 3128](#).

More information about Apache HTTP Proxy:

- [What is Apache HTTP Proxy Server?](#)
- [Apache HTTP Proxy installation - Linux](#)

7.6 How to use the offline mirror tool to receive updates

ESET Virtualization Security can download updates directly from ESET update servers or use a mirror server to download updates.

In large environments, we recommend balancing mirror updates among additional ESET Remote Administrator mirror servers. If the mirror needs to be centralized on a single server, we recommend using another type of HTTP server, such as Apache.

The mirror tool is necessary for offline virus database updates. If your client computers do not have an internet connection and need virus database updates, you can use the Mirror tool to download update files from ESET update servers and store them locally.

i NOTE: The mirror tool downloads virus database definitions only, it does not download PCUs (Program Component Updates). To update ESET Virtualization Security offline, we recommend that you upgrade the product using the [Software Install client task](#) in ERA. Alternatively, you can upgrade the product individually.

Prerequisites:

- The target folder must be shared using the Samba or HTTP/FTP service, depending on how you want to make updates accessible.
- You must have a valid [Offline license](#) file that includes a Username and Password. When generating a license file, be sure to select the check box next to **Include Username and Password**. Also, you must enter a **License filename**.

Offline license file

PRODUCT: ESET

UNITS: 1 / 949

LICENSE FILENAME:

☒ Include Username and Password
When included it is possible to update from ESET servers.

☐ Allow management with Remote Administrator

GENERATE CANCEL

- [Visual C++ Redistributables for Visual Studio 2010](#) must be installed on the system.
- There is no installation step, the tool consists of two files:
 - Linux:
MirrorTool and updater.so

Usage:

- If you need assistance running the tool, run `MirrorTool --help` to view all available commands for the tool:

```
C:\Users\administrator.FRANTO\Desktop\1.0.136.0\Win32>MirrorTool.exe --help
Mirror Tool, Copyright (c) ESET, spol. s r.o. 1992-2015. All rights reserved.
Allowed options:
--mirrorType arg                [required]
                                Type of mirror. Possible values (case
                                insensitive): regular, pre-release,
                                delayed.
--intermediateUpdateDirectory arg [required]
                                Files will be downloaded to this directory
                                to create mirror in output directory.
--offlineLicenseFilename arg    [required]
                                Offline license file.
--updateServer arg              [optional]
                                Update server. (e.g.:http://update.eset.com
                                /eset_upd/ep6/) Mirror will be created in
                                output directory, only specified path in
                                server will be mirrored.
--outputDirectory arg           [required]
                                Directory where mirror will be created.
--proxyHost arg                 [optional]
                                Http proxy address (fqdn or IP).
--proxyPort arg                 [optional]
                                Http proxy port.
--proxyUsername arg             [optional]
                                Http proxy username.
--proxyPassword arg             [optional]
                                Http proxy password.
--excludedProducts arg          [optional]
                                Disable creating mirror for specified
                                products. Possible values:ep4 ep5 ep6 era6.
--help                          [optional]
                                Display this help and exit
```

- The parameter `--updateServer` is optional. When you use it, you must specify the full URL of the update

server.

- The parameter `--offlineLicenseFilename` is mandatory. You must specify a path to your offline license file (as mentioned above).
- To create a mirror, run the `MirrorTool` with at least the minimal required parameters. Here is an example:
 - Linux:
 - `sudo ./MirrorTool --mirrorType regular --intermediateUpdateDirectory /tmp/mirrorTool/mirrorTemp --offlineLicenseFilename /tmp/mirrorTool/offline.lf --outputDirectory /tmp/mirrorTool/mirror`

Mirror tool and Update settings:

- To automate the distribution of virus database updates, you can create a schedule to run the Mirror tool. To do so, open ERA Web Console and navigate to **Client Tasks > Operating System > Run Command**. Select **Command line to run** (including a path to the `MirrorTool.exe`) and set a reasonable trigger (such as CRON for every hour `00 * * * ? *`). Alternatively, you can use the Cron in Linux.
- To configure updates on a client computer(s), create a new policy and configure an **Update server** to point to your mirror address or shared folder.

7.7 Cannot register to VMware vShield

If you cannot register with VMware vShield, we suggest the following troubleshooting steps:

- Verify that communication with vShield Manager using port 443 is allowed
- Restart your VMware vShield virtual machine
- Reinstall the vShield Endpoint module on ESXi (via VMware vShield Manager Web user interface)

7.8 ESET Virtualization Security shows no connected/protected virtual machines

If ESET Virtualization Security shows zero connected or protected virtual machines make sure that:

- Virtual machines are running and have VMware tools installed with the VMCI Driver
- Your Network allows for communication via port 48651 to or from ESET Virtualization Security
- vShield is running and vShield credentials are correctly supplied

7.9 No accessibility on license servers

There may be a problem with access to license servers, for example, firewall rules may be blocking ESET Virtualization Security from connecting to them. Verify that you are able to access edf.eset.com to test connectivity.

i NOTE: Communication with license servers is outgoing only. See our [ESET Knowledgebase article](#).

8. Glossary

8.1 ESXi host

A computer on which a hypervisor is running one or more virtual machines. Each virtual machine is called a guest machine.

8.2 Hypervisor

A hypervisor or virtual machine monitor is a piece of computer software or hardware that creates and runs virtual machines (for example, VMware vSphere).

8.3 Virtual machine

A virtual machine (VM) is a software implementation of a machine (computer) that executes programs like a physical machine.

8.4 Virtual appliance

A virtual appliance is a pre-configured virtual machine image, ready to run on a hypervisor. Virtual appliances are provided as files, via downloads or physical distribution. The most commonly used format is the Open Virtualization Format (OVF).

An OVA is a single file distribution of the same file package, stored in the TAR format.

8.5 VMware Tools

VMware Tools is an optional set of drivers and utilities that you install in the operating system of a virtual machine. This suite enhances both the performance of a virtual machine's guest operating system and interaction between the guest and the host.

8.6 vMotion Migration

vMotion migration enables live migration of a virtual machines from one physical server (ESXi server) to another while maintaining continuous service availability. Additionally, vMotion allows you to perform maintenance on a host machine without the need for downtime on your virtual machine.

A virtual machine must meet the following requirements before migration:

- A virtual machine must not have a connection to a virtual device (CD-ROM or floppy drive) with a local image mounted. You can place your ISO images into a shared data store.
- A virtual machine must not have a connection to an internal vSwitch.
- A virtual machine must not have CPU affinity configured.
- Shared storage where the VM can store their files.
- A Gigabit Ethernet or faster connection for vMotion.
- Access to the same physical networks (hosts must be plugged into the same physical network).
- Hosts must have compatible CPUs. If you do not perform live migration between hosts with identical CPUs, you could experience a vMotion crash.
- A VMkernel port on each host (with a different IP address for each host).