

# ESET Virtualization Security for VMware NSX

## User Guide

VMware vSphere 5.5/6.0/6.5+

[Click here to display Online help version of this document](#)

## ESET VIRTUALIZATION SECURITY FOR VMWARE NSX

**Copyright ©2017 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](http://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](http://www.eset.com/support)

REV. 12/18/2017

# Contents

<b>1. What is ESET Virtualization Security and how does it work?.....</b>	<b>5</b>
1.1 Architecture for VMware NSX.....	5
1.2 Requirements.....	6
1.3 How the components interact.....	7
1.4 Features & Benefits.....	7
<b>2. How to upgrade your VMware environment to NSX.....</b>	<b>9</b>
2.1 Unregistration of current ESET solution.....	9
2.2 Upgrade vShield to NSX.....	10
<b>3. Installation/Deployment ESET Virtualization Security for VMware NSX.....</b>	<b>13</b>
3.1 Guest Introspection installation.....	13
3.2 VMware Tools installation.....	14
3.3 vAgent Host deployment.....	14
3.4 Register ESET to VMware NSX Manager.....	19
3.5 ESET Virtualization Security Appliance (SVM) deployment.....	22
3.6 Activate Virtual Agent Host from ESET Remote Administrator.....	25
3.7 Automatic activation of all ESET Virtualization Security appliances.....	26
3.8 Creating Security Group with policy.....	28
<b>4. Configuration of ESET Virtualization Security.....</b>	<b>31</b>
4.1 Managing ESET Virtualization Security from the console.....	31
4.1.1 Tasks.....	33
4.2 Policies for Security Appliance & Protected VMs.....	33
4.2.1 ESET Virtualization Security - Security Appliance policy.....	34
4.2.1.1 Antivirus.....	35
4.2.1.2 Update.....	35
4.2.1.2.1 Primary/Secondary Server.....	35
4.2.1.3 Virtual Agent Host.....	36
4.2.1.4 Tools.....	36
4.2.1.4.1 Log files.....	36
4.2.1.4.2 Proxy server.....	36
4.2.1.4.3 System console.....	37
4.2.2 ESET Virtualization Security - Protected VM policy.....	37
4.2.2.1 Antivirus.....	38
4.2.2.2 Real-time file system protection.....	38
4.2.2.2.1 Basic.....	38
4.2.2.2.2 ThreatSense parameters.....	38
4.2.2.2.3 Additional ThreatSense parameters.....	40
4.2.2.2.4 Clean file cache.....	40
4.2.2.3 On-demand computer scan.....	40
4.2.2.3.1 Basic.....	40
4.2.2.3.2 ThreatSense parameters.....	40
<b>5. Working with ESET Virtualization Security for NSX.....</b>	<b>43</b>
5.1 Creating On-Demand Scan task.....	43
5.2 Automate On-Demand Scan after infection.....	44
5.3 Tagging workflow for Guest Introspection.....	45
5.4 Understanding of Security Tags and how ESET triggers them.....	45
5.5 Automatically quarantine VM upon malware detection using NSX.....	46
<b>6. Updating ESET Virtualization Security.....</b>	<b>49</b>
6.1 How to check for available updates.....	49
6.2 How to update vAgent Host.....	50
6.3 How to update ESET NSX Service Manager.....	51
6.4 How to update ESET Virtualization Security Appliance - Secure Virtual Machine.....	51
6.5 How to update Operating System on ESET Virtualization Security Appliance.....	52
6.6 Ports.....	52
<b>7. Working with ESET Remote Administrator..</b>	<b>53</b>
7.1 Detection engine update.....	53
7.2 On-Demand scan.....	54
7.3 Quarantine management.....	54
7.4 How to find vAgent Host in ESET Remote Administrator.....	56
7.5 How to find ESET Virtualization Security in ESET Remote Administrator.....	56
7.6 How to identify problematic VMs in ESET Remote Administrator.....	56
7.7 How to add virtual machines to ESET Remote Administrator.....	56
7.8 How to sync with vCenter.....	57
<b>8. Common Questions.....</b>	<b>58</b>
8.1 How vAgent Host works.....	58
8.2 How to activate and initial setup.....	59
8.2.1 How to get a license.....	59
8.2.2 How unilicense works.....	59
8.2.3 How to import license to ESET Remote Administrator.....	59
8.3 How ESET Virtualization Security interacts with VMware products.....	61
8.4 What ports are needed for each component.....	61
8.5 How to collect logs.....	62
8.6 How to read the logs.....	62
8.7 How to uninstall ESET Virtualization Security.....	63

8.8	How to access system logs.....	63
8.9	How to deploy vAgent Host with existing certificates.....	65
<b>9.</b>	<b>Troubleshooting.....</b>	<b>66</b>
9.1	Where to find the logs for ESET Remote Administrator .....	66
9.2	Where to find the logs for ESET Virtualization Security.....	66
9.3	Where to find the logs for vAgent.....	66
9.4	What to send to Customer Care .....	66
9.5	What ports to enable for licensing.....	67
9.6	What ports to enable for HTTP Proxy (update caching).....	67
9.7	How to use the offline mirror tool to receive updates.....	67
9.8	Cannot register to VMware vShield.....	69
9.9	ESET Virtualization Security shows no connected/protected virtual machines.....	69
9.10	No accessibility on license servers.....	69
9.11	Path excluded from scanning.....	70
<b>10.</b>	<b>Glossary.....</b>	<b>71</b>
10.1	ESXi host.....	71
10.2	Hypervisor .....	71
10.3	Virtual machine .....	71
10.4	Virtual appliance.....	71
10.5	VMware Tools.....	71
10.6	vMotion Migration.....	71

# 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:

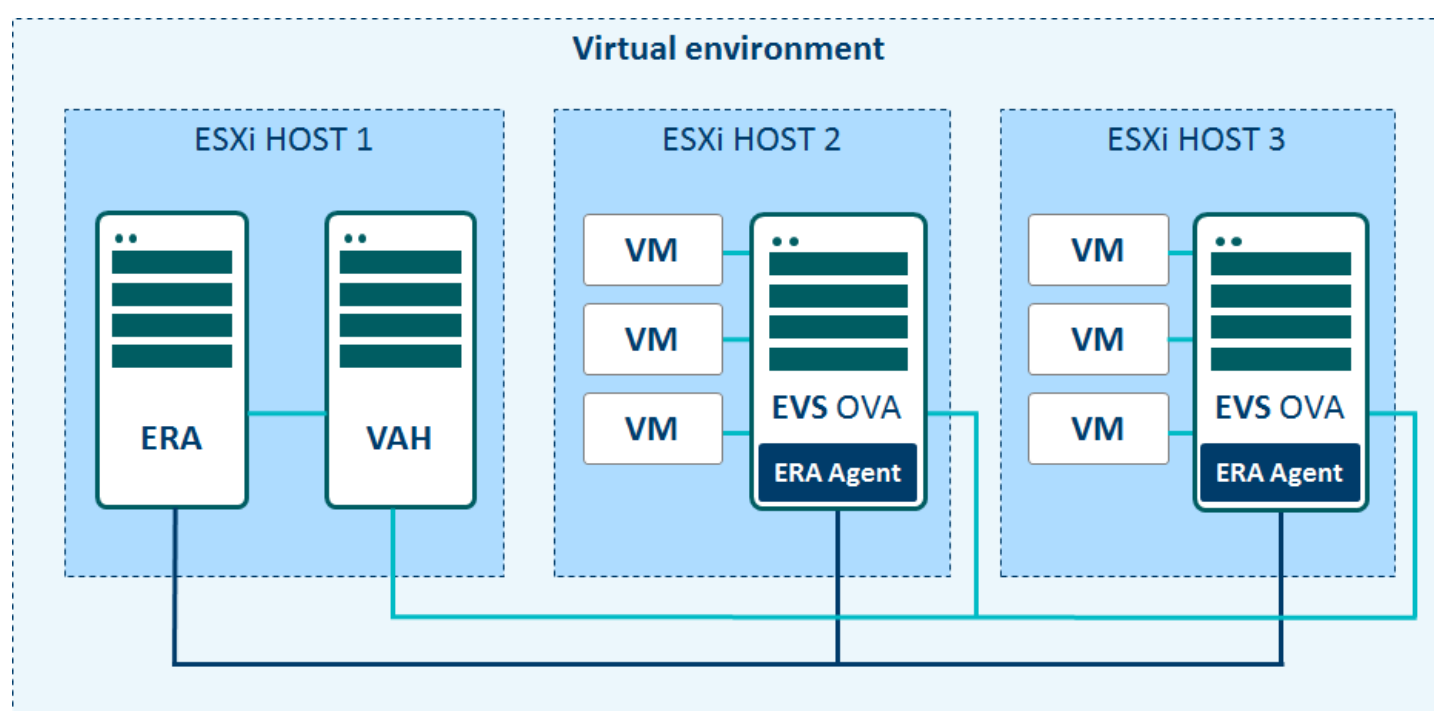


Figure 1

## 1.1 Architecture for VMware NSX

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

- VMware NSX Manager installed in VMware environment
- Guest Introspection service installed
- VMware Tools with Guest Introspection driver installed on each virtual machine
- ESET Remote Administrator 6.4 and higher management server installed
- ESET Remote Administrator Virtual Agent Host
- ESET Virtualization Security integrates components from VMware and the ESET Scanning Engine, registers that with NSX, which creates a dedicated on-hypervisor network to allow rapid file exchange

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

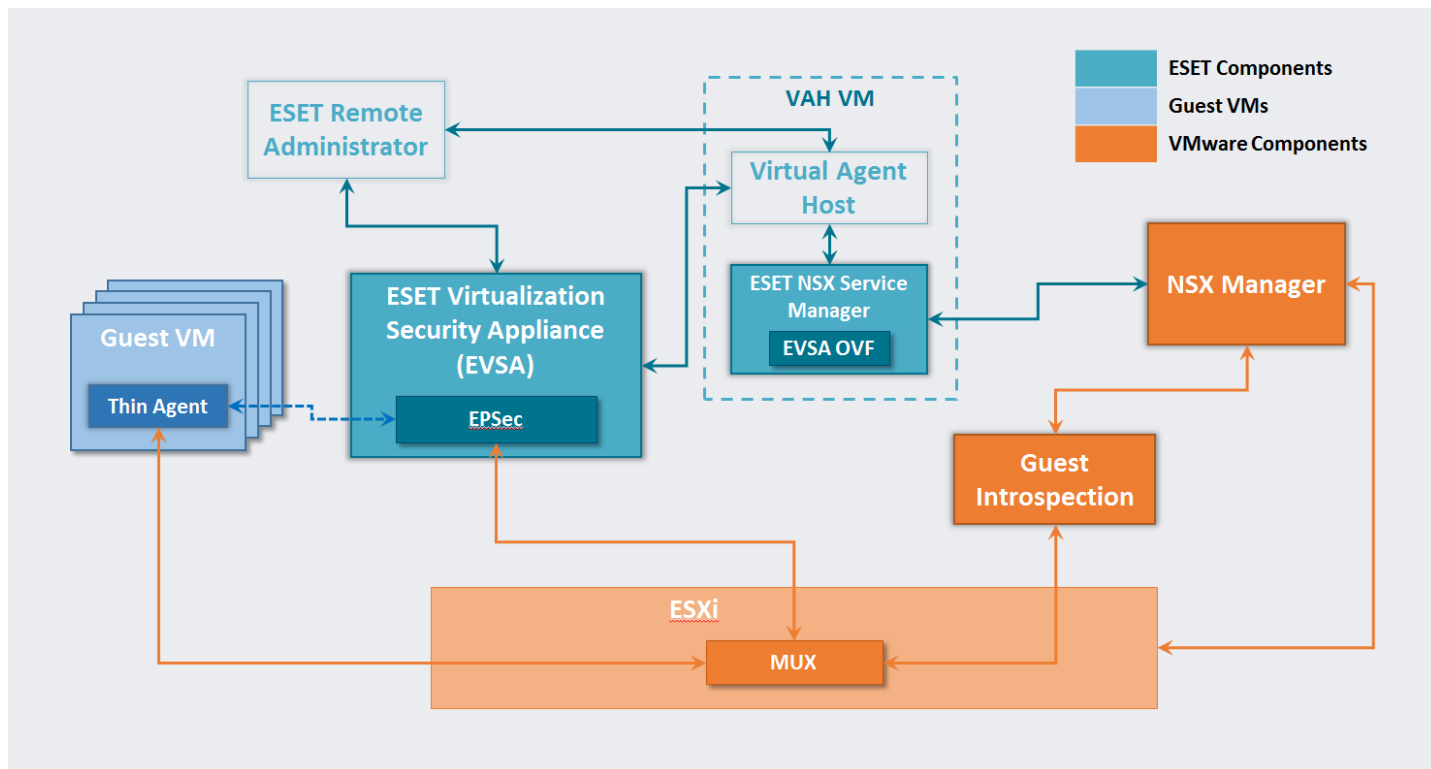


Figure 2

- <%ESET\_REMOTE\_ADMINISTRATOR%> (ERA) is an application that allows you to manage ESET products in a networked environment from one central location. For more information see the [ESET Remote Administrator Online help](#).
- Virtual Agent Host (VAH) is a component of ESET Remote Administrator that virtualizes agent entities to allow management of agentless virtual machines. For more information click [here](#).
- Guest Introspection is a service from NSX Manager to offload security functions to ESET security solution.
- The NSX Manager is the centralized management component of NSX and runs as a virtual appliance on an ESXi host.

## 1.2 Requirements

### System requirements

- VMware vSphere 5.5 U2+/6.0/6.5+ (vCenter Single Sign-On, vSphere Client/Web Client, vCenter Server, vCenter Inventory Service)
- VMware NSX Manager 6.2.4+/6.3+
- VMware Guest Introspection 6.2.4+/6.3+
- ESET Remote Administrator 6.5+ management server installed
- Virtual Agent Host deployed as VM
- Reservation for ESET Virtualization Security appliance (SVM): 2 CPU, 2 GB RAM, 8 GB Disk
- NSX Manager rights:  
For Registration to NSX Manager and deployment of SVMs (using vSphere client): Security Administrator  
For group/names synchronization with VMware vSphere: Read-only for vCenter and NSX Manager

### EVS and VMware compatibility matrix

	EVS 1.5	EVS 1.6
VMware vSphere 5.5 U2+	✓	✓
VMware vSphere 6.0.x	✓	✓
VMware vSphere 6.5.x		✓
VMware NSX 6.2.x	✓	✓

VMware NSX 6.3.x		✓
Windows VMs protection*	✓	✓
Linux VMs protection**		✓

\* List of compatible Windows versions can be found [here](#)

\*\* List of compatible Linux distributions can be found [here](#)

## 1.3 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/vAgent Host <-> VMware NSX Manager

This communication serves for NSX registration and ESET Virtualization Security monitoring purposes.

## 1.4 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

### 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 NSX agentless protection.

### Protection

**ESET LiveGrid®** is an advanced early warning system comprised of several cloud-based technologies. It helps detect emerging threats based on reputation and improves scanning performance by means of whitelisting.

**DNA Detections** can identify specific known malware samples, new variants of a known malware family or even previously unseen or unknown malware which contains genes that indicate malicious behavior.

**Other benefits**

Native support of VMware NSX automation, supporting Micro Segmentation & automatic task execution. It automatically moves infected machines to different micro segment, to prevent malware spread, and executes scanning. When machine is proven clean, it is returned to original place.

Automatic deployment of new EVS appliances to hosts newly connected to NSX Manager. This allows automatic protection of newly added virtual hosts, and virtualized workloads. This drastically reduces time needed for security deployment.

ESET Virtualization Security supports native integration with 3rd party security solutions, using VMware Service Composer.



## 2. How to upgrade your VMware environment to NSX

This chapter will help you upgrade your existing VMware environment.

1. [Unregistration of current ESET solution](#)
2. [Upgrade vShield to NSX](#)

### **i** NOTE

Before upgrading make sure you have installed:

- VMware vSphere 5.5 U2+
- VMware vSphere 6.0+

To determine which vShield or vCNS is installed read the following [article](#).

### **i** NOTE

If you have already upgraded to VMware NSX, continue to [Installation/Deployment](#).

### **i** NOTE

The following versions of VMware vSphere and VMware NSX are compatible together:

- VMware vSphere 5.5, 6.0, 6.5
- VMware NSX 6.2.4+, 6.3+

### 2.1 Unregistration of current ESET solution

1. First, unregister ESET Virtualization Security from vShield Manager. To accomplish this, follow the steps below:
  - a. Open ESET Virtualization Security console through vCenter.
  - b. Enter the **Management Mode**.
  - c. Choose **vShield Registration**.
  - d. Enter username and password and select **UNREGISTER**.

### **i** NOTE

Apply the steps above also for each ESET Virtualization Security appliance in your virtual environment.

2. After successful unregistration of ESET Virtualization Security from vShield:
  - a. Enter vShield Manager web console.
  - b. In Tree view in **Host & Clusters** under **Datacenters** for each host:
    - i. Click **Uninstall** next to vShield Endpoint.
    - ii. Make sure that after successful uninstallation you see **Install** button again.
    - iii. Repeat these steps for each host in the cluster.

## 2.2 Upgrade vShield to NSX

### NOTE

Please read the official [NSX Upgrade Guide](#) to upgrade from vShield to NSX.

After successful unregistration of vShield Manager delete vShield Manager virtual machine, [download](#) and deploy the latest NSX Manager [compatible with ESET](#).

To deploy NSX Manager, perform the following steps:

1. Deploy NSX Manager .ova file.
2. Connect to NSX Manager using web browser and log in.
3. In **Manage Appliances Settings** select the **General** tab and specify:
  - a. NTP Server (if you haven't done it during deployment)
  - b. Syslog server (if available)
  - c. Locale
4. Under **Components** section choose **NSX Management Service**
5. Under **Lookup Service URL** click **Edit** and specify:
  - a. Lookup service host (URL of your vCenter Server)
  - b. Port (depending on your vSphere version)
  - c. Administrator Username
  - d. Password

Lookup Service URL

For vCenter versions 5.5 and above, you may configure Lookup Service and provide the SSO administrator credentials to register NSX Management Service as a solution user. It is also recommended to set the NTP server for SSO configuration to work correctly.

Lookup Service Host:

Lookup Service Port:

*Enter port 443 for vSphere 6.0, for vSphere 5.5 use 7444.*

Lookup Service URL:

SSO Administrator User Name:

Password:

OK Cancel

- e. Confirm by clicking **OK** and proceed with the certificate.
  - f. You should be able to see **Connected** status.
6. Under vCenter Server click Edit specify:
  - a. vCenter Server address
  - b. vCenter Username
  - c. vCenter Password
  - d. **Do not** select the **Modify plugin script download location** checkbox unless necessary (please read [https://pubs.vmware.com/NSX-62/topic/com.vmware.ICbase/PDF/nsx\\_62\\_install.pdf#38](https://pubs.vmware.com/NSX-62/topic/com.vmware.ICbase/PDF/nsx_62_install.pdf#38)).
  - e. Proceed with the certificate.

**vCenter Server**

Connecting to a vCenter server enables NSX Management Service to display the VMware Infrastructure inventory. HTTPS port (443) needs to be opened for communication between NSX Management Service, ESX and VC. For a full list of ports required, see section 'Client and User Access' of Chapter 'Preparing for Installation' in the 'NSX Installation and Upgrade Guide'.

If your vCenter server is hosted by a vCenter Server Appliance, please ensure that appropriate CPU and memory reservation is given to this appliance VM. After successful configuration of vCenter on NSX Manager, you need to log out of any active client sessions on vSphere Web Client and log back in to enable NSX user interface components.

vCenter Server:

vCenter User Name:

Password:

☐ Modify plugin script download location

OK Cancel

7. You should be able to see the **Connected - Last successful inventory update was on <date>** status.
8. Now you will see that everything is connected and working properly.

**vmware NSX**

Summary Manage

SETTINGS

- General
- Network
- SSL Certificates
- Backups & Restore
- Upgrade

COMPONENTS

- NSX Management Service**

**Lookup Service URL**

For vCenter versions 5.5 and above, you may configure Lookup Service and provide the SSO administrator credentials to register NSX Manager with vCenter.

Lookup Service URL:	https://192.168.1.100:443/lookup/
SSO Administrator User Name:	Administrator@vsphere.local
Status:	<span style="color: green;">●</span> Connected

**vCenter Server**

Connecting to a vCenter server enables NSX Management Service to display the VMware Infrastructure inventory. HTTPS port (443) needs to be opened for communication between NSX Management Service, ESX and VC. For a full list of ports required, see section 'Client and User Access' of Chapter 'Preparing for Installation' in the 'NSX Installation and Upgrade Guide'.

If your vCenter server is hosted by a vCenter Server Appliance, please ensure that appropriate CPU and memory reservation is given to this appliance VM. After successful configuration of vCenter on NSX Manager, you need to log out of any active client sessions on vSphere Web Client and log back in to enable NSX user interface components.

vCenter Server:	192.168.1.100
vCenter User Name:	Administrator@vsphere.local
Status:	<span style="color: green;">●</span> Connected - Last successful inventory update was on Mon, 10 Oct 2016 10:59:17 GMT

### **i NOTE**

If vCenter is already open, log out of vCenter and log in again with the same Administrator role used to register NSX Manager with vCenter.

## 3. Installation/Deployment ESET Virtualization Security for VMware NSX

To deploy ESET Virtualization Security, make sure your system meets the system requirements and do the following:

1. VMware NSX Manager installed
2. [Guest Introspection installed according to instructions provided by VMware](#)
3. [VMware Tools installed on guest virtual machines according to instruction provided by VMware](#)
4. [vAgent Host deployed](#)
5. [Register VAH to NSX](#)
6. [ESET Virtualization Security installed](#)

### NOTE

Administrator needs following rights in NSX Manager for deployment of ESET Virtualization Security:

- for registration to NSX Manager and deployment of SVMs (using vSphere client): Security Administrator
- For group/names synchronization with VMware vSphere: Read-only for vCenter and NSX Manager

### 3.1 Guest Introspection installation

Installing Guest Introspection installs a new vib and a service virtual machine on each host in the cluster. Guest Introspection is required for ESET Virtualization Security security solution.

To install the Guest Introspection perform the following steps according to instructions provided by VMware:

1. On the **Installation** tab click **Service Deployments**.
2. Click the **New Service Deployment** (+) icon.
3. In the **Deploy Network and Security Services** dialog box, select **Guest Introspection**.
4. In **Specify schedule**, select **Deploy now** to deploy Guest Introspection as soon as it is installed or select a deployment date and time and click **Next**.
5. Select the datacenter and cluster(s) where you want to install Guest Introspection and click **Next**.
6. On the Select storage and Management Network Page, select the datastore on which to add the service virtual machines storage or select **Specified on host**. It is recommended that you use shared datastores and networks instead of **Specified on host** so that deployment workflows are automated. The selected datastore must be available on all hosts in the selected cluster. If you selected **Specified on host**, follow the steps below for each host in the cluster.
  - a) On the vSphere Web Client home page, click **vCenter** and then click **Hosts**.
  - b) Click a host in the **Name** column and then click the **Manage** tab.
  - c) Click **Agent VM Settings** and click **Edit**.
  - d) Select the datastore and click **OK**.
7. Select the distributed virtual port group to host the management interface. If the datastore is set to **Specified on host**, the network must also be Specified on host. The selected port group must be able to reach the NSX Manager's port group and must be available on all hosts in the selected cluster. If you selected **Specified on host**, follow the substeps in Step 6 to select a network on the host. When you add a host (or multiple hosts) to the cluster, the datastore and network must be set before each host is added to the cluster.
8. In IP assignment, select **DHCP** or **An IP pool**.
9. Click **Next** and then click **Finish**.
10. Monitor the deployment until the **Installation Status** column displays **Succeeded**.
11. If the **Installation Status** column displays **Failed**, click the icon next to **Failed**. All deployment errors are displayed. Click **Resolve** to fix the errors. In some cases, resolving the errors displays additional errors. Take the required action and click **Resolve** again.

## Install Guest Introspection for Linux

The following Linux operating systems are supported for NSX Guest Introspection:

- Red Hat Enterprise Linux 7 GA 64-bit
- SUSE Linux Enterprise Server 12 GA 64-bit
- Ubuntu 14.04 LTS 64-bit

### NOTE

For more information how to install Guest Introspection for Linux click [here](#).

## 3.2 VMware Tools installation

To install the VMware Tools perform the following steps according to instructions provided by VMware:

1. Mount the VMware Tools virtual disc on the guest operating system.
2. In your vSphere Web Client, right-click the virtual machine and select **Guest OS > Install/Upgrade VMware Tools**.

### NOTE

We recommend to install VMware Tools 10.0.9 or later.

### NOTE

For more information how to install VMware Tools on Linux Guests click [here](#).

## 3.3 vAgent Host deployment

The Virtual Agent Host (VAH) 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 [download](#) and deploy the OVA file using vSphere Client.

### IMPORTANT

Before deployment of Virtual Agent Host you have to contact your networking team to register desired hostname (e.g. company-vah.domain.com) in FQDN (fully qualified domain name) format on your DNS Server and assign a static IP.

### Deployment procedure:

1. Log in to your vSphere Web Client, in **Navigator** choose **Hosts and Clusters**, right-click the host 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. Review details and continue by clicking **Next**.
5. Read and accept the end user license agreement.
6. Follow the instructions on screen to complete installation and specify the following information about your virtual appliance:

- **Select name and folder** – Specify a name for the deployed template and location where virtual machine files are stored.
- **Select a resource** – Select a host, cluster, resource pool on which you want to run the template.
- **Select storage** – Select a location to store virtual machine files and format that virtual disks will use.
- **Setup networks** – 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 **Customize template** page, specify following (fields not mentioned are optional):

**Hostname** – this will be the hostname in FQDN format of your vAgent Host appliance, which you registered on DNS Server with networking team as mentioned above.

**Password** – this will be used for your vAgent Host virtual machine 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.

#### **i NOTE**

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 vAgent Host can connect to ERA Server/Proxy:

#### **i NOTE**

If you or your network team decided to deploy appliance with **Static IP Address**, please expand **Networking Properties** section and fill the following:

**Network IP Address** – type the IP address to which DNS server resolves pre-configured FQDN hostname.

**Network Netmask** – The netmask for this interface

**Default Gateway** – The default gateway address for this VM

**DNS1** – The domain name server , which is able to resolve configured FQDN hostname

**DNS2** – Alternative domain name server , which is able to resolve configured FQDN hostname

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

**Webconsole Hostname** – type in the hostname or IP address of your Web Console, so that vAgentHost can connect to ERA Server.

**Webconsole username and password** – type in credentials so that vAgent Host can connect to ERA Server.

Deploy OVF Template

1 Source

1a Select source

1b Review details

1c Accept License Agreements

2 Destination

2a Select name and folder

2b Select a resource

2c Select storage

2d Setup networks

2e Customize template

3 Ready to complete

Customize template

Customize the deployment properties of this software solution

2 properties have invalid values

Show next...

Collapse all...

Application

15 settings

Hostname

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

Password

VM and database password. Use ASCII characters except reserved '{' and '}'.

Enter password

Confirm password

ERA Server Hostname

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

ERA Server Port

ERA Server port.

2222

Webconsole Hostname

Hostname used by webconsole to connect to the server (if left empty, value will be copied from Server Hostname)

Webconsole Port

Port used by webconsole to connect to the server. (Default is '2223')

Back

Next

Finish

Cancel

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 Virtual Agent Host Appliance  
(C) 2016 ESET, spol. s r.o. - All rights reserved

Server certificate fingerprint (check carefully):  
5d:40:41:a6:26:4e:4a:10:a1:57:4f:8d:39:53:b2:7d:a8:0f:66:c9

Virtual Agent Host version: 6.5.331.0  
Agent version: 6.4.320.0

Virtual Agent Host hostname: era-vah-nsx.192.168.1.100.com  
Virtual Agent Host IP address: 192.168.1.100  
Virtual Agent Host comm port: see config (default is 9880)  
NSX Service Manager port: 8443

Webmin access is enabled on port 10000.

<ENTER> Enter management mode

The following options can be edited in management mode:

- **Enable/Disable Webmin interface** – enables/disables Webmin management interface running on port 10000.
- **Change VM password** – Changes root password used to log into this virtual machine.
- **Change database password** – Changes root database password. This will not change randomly generated password in the connection string for vAgent Host
- **Register to VMware NSX Manager** – Registers ESET security solution to VMware NSX Manager.
- **Factory reset** – will reset the appliance to factory settings. All data will be lost. Please create a backup before resetting.
- **Restart system** – Virtual Agent Host will restart.
- **Shut down system** – will shut down appliance.
- **Lock screen** – will lock the console and return to the basic information screen (also by pressing **Esc**).
- **Exit to terminal** – will exit the console and return to the command line. To go back to Management mode, type **exit** and press **Enter**.

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

ESET Remote Administrator Virtual Agent Host Appliance

Enable/Disable Webmin interface

Change UM password

Change database password

Register to VMware NSX Manager

Factory reset

Restart system

Shut down system

Lock screen

Exit to terminal

<UP>/<DOWN> Select item

<ENTER> Perform action

Enables or disables Webmin management interface running on port 10000.

<ESC> Lock screen

### 3.4 Register ESET to VMware NSX Manager

1. Open vAgent Host console from your vSphere Web client or vSphere Client and enter the **Management mode**.

```
ESET Remote Administrator Virtual Agent Host Appliance
(C) 2016 ESET, spol. s r.o. - All rights reserved

Server certificate fingerprint (check carefully):
5d:40:41:a6:26:4e:4a:10:a1:57:4f:8d:39:53:b2:7d:a8:0f:66:c9

Virtual Agent Host version: 6.5.331.0
Agent version: 6.4.320.0

Virtual Agent Host hostname: era-vah-nsx.10.10.10.10.com
Virtual Agent Host IP address: 10.10.10.10
Virtual Agent Host comm port: see config (default is 9880)
NSX Service Manager port: 8443

Webmin access is enabled on port 10000.
```

<ENTER> Enter management mode

2. Select **Register to VMware NSX Manager**.

Registers this appliance to VMware NSX Manager.

Enable/Disable Webmin interface  
Change UM password  
Change database password  
Register to VMware NSX Manager  
Factory reset

Restart system  
Shut down system

Lock screen

Exit to terminal

<UP>/<DOWN> Select item  
<ENTER> Perform action

<ESC> Lock screen

3. Enter NSX Manager **FQDN** (fully qualified domain name) **hostname** and **accept** the certificate.
4. Enter NSX Manager admin **username** and **password**. You will see the **not registered** status.
5. Enter **ESET\_Security.ThreatFound** tag which will be used as default after finding malware on VM. You can check created tag in **vCenter > Summary > Security Tags** for specific virtual machine.

```

=====
Welcome to ESET NSX Service Manager Console version 1.6.7
-----

Hostname: 192.168.1.100
Enter NSX Manager hostname []: NSX-manager
NSX Manager SHA-1 fingerprint is 75:48:57:4C:3B:4C:3A:2B:45:23:3B:47:43:79:3A:5F:4F:26:47:5B.
Do you accept this certificate [yes]? yes
Enter NSX Manager admin username []: admin
Enter NSX Manager admin password []:
Enter ThreatFound tag name [ESET_Security.ThreatFound]: ANTI_VIRUS.VirusFound.threat=high

Registration status:
    Service Manager:      [not registered]
    Service:              [not registered]
    Deployment Spec:      [not registered]
    Vendor Template:      [not registered]
    Service Instance:     [not registered]
    Security Tag:         [ registered ]

Menu:
s) status
r) register
c) change NSX manager credentials
q) quit
Command: _

```

6. Type r (register) and confirm by pressing **Enter**.

```

Enter NSX Manager hostname []: NSX-manager
NSX Manager SHA-1 fingerprint is 75:48:57:4C:3B:4C:3A:2B:45:23:3B:47:43:79:3A:5F:4F:26:47:5B.
Do you accept this certificate [yes]? yes
Enter NSX Manager admin username []: admin
Enter NSX Manager admin password []:

Registration status:
    Service Manager:      [not registered]
    Service:              [not registered]
    Deployment Spec:      [not registered]
    Vendor Template:      [not registered]
    Service Instance:     [not registered]
    Security Tag:         [not registered]

Menu:
s) status
r) register
c) change NSX manager credetials
q) quit
Command: r

```

7. Type s (status) and recheck the registration status. If it is successful then you will see the **registered** status.

```
=====
Welcome to ESET NSX Service Manager Console version 1.6.7
-----

Hostname: 192-168-1-100.lan

Registration status:
  Service Manager: [ registered ]
  Service:         [ registered ]
  Deployment Spec: [ registered ]
  Vendor Template: [ registered ]
  Service Instance: [ registered ]
  Security Tag:    [ registered ]

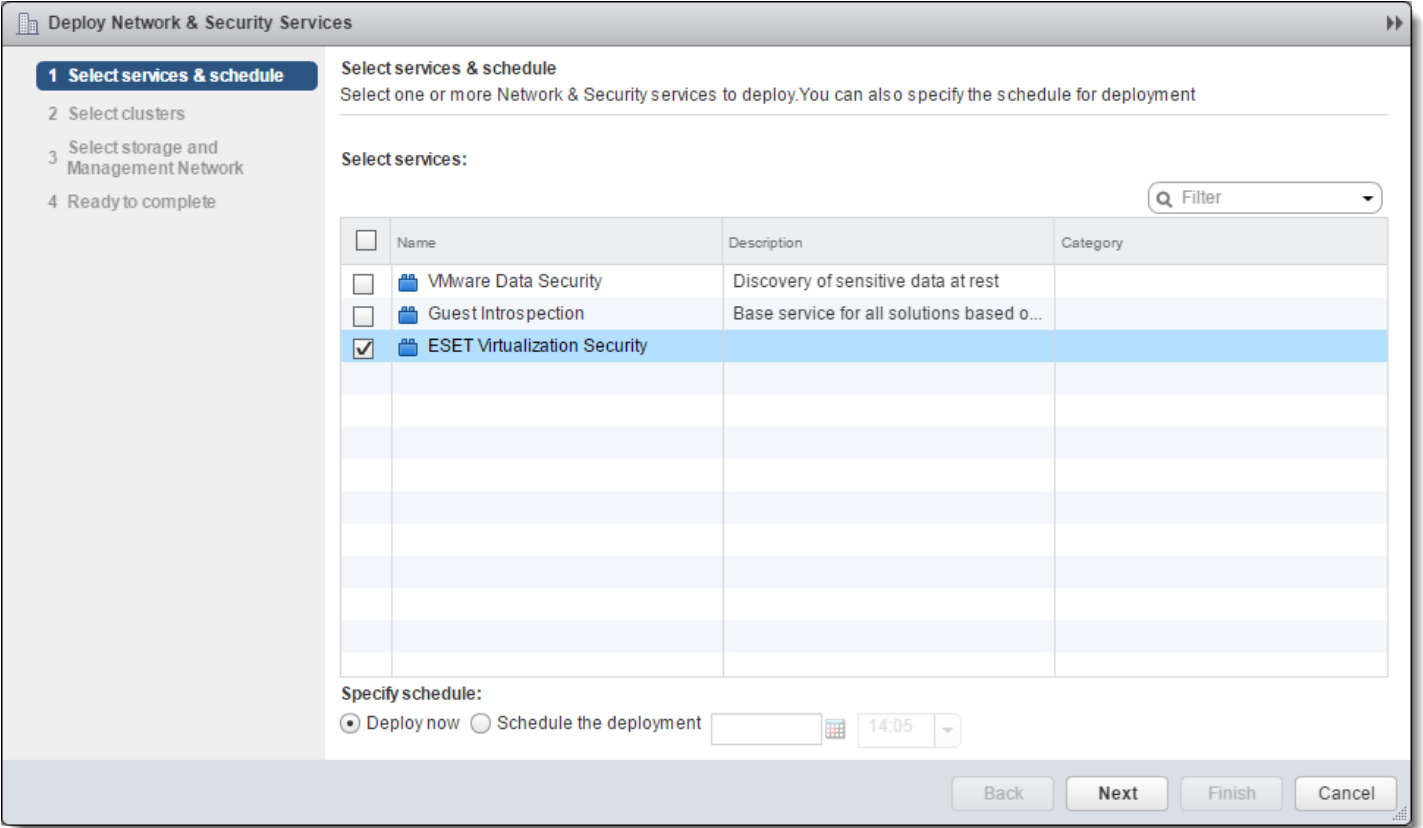
Settings:
  Security Tag Name: ESET_Security.ThreatFound

Menu:
  s) status
  u) unregister
  c) change NSX manager credentials
  q) quit
Command:
```

- 8. Type **q** (quit) and exit the ESET NSX Service Manager Console.
- 9. You can now use the vCenter Web Client to deploy ESET Virtualization Security.

3.5 ESET Virtualization Security Appliance (SVM) deployment

- 1. In your vSphere Web Client, go to **Networking & Security > Installation > Service Deployments** and click **+** to add new service deployment.
- 2. Select checkbox next to ESET Virtualization Security and click **Next**.



- 3. Select cluster(s) on which you want to deploy ESET Virtualization Security and click **Next**. ESET Virtualization Security will be installed on all hosts in the cluster.



**! IMPORTANT** When creating IP pools make sure that selected IP addresses are available to be used. Check this on your DHCP server!

Select **Use IP pool** and if there are already created IP pools choose one of them or create a new one by clicking the  sign.

[illegible]

**Add Static IP Pool**

Name: \* EVS appliances

Gateway: \* 10.1.173.1  
*A gateway can be any IPv4 or IPv6 address.*

Prefix Length: \* 24

Primary DNS: 10.1.15.10

Secondary DNS: 10.1.15.11

DNS Suffix:

Static IP Pool: \* 10.1.173.15-10.1.173.16

*for example 192.168.1.2-192.168.1.100 or  
abcd:87:87::10-abcd:87:87::20*

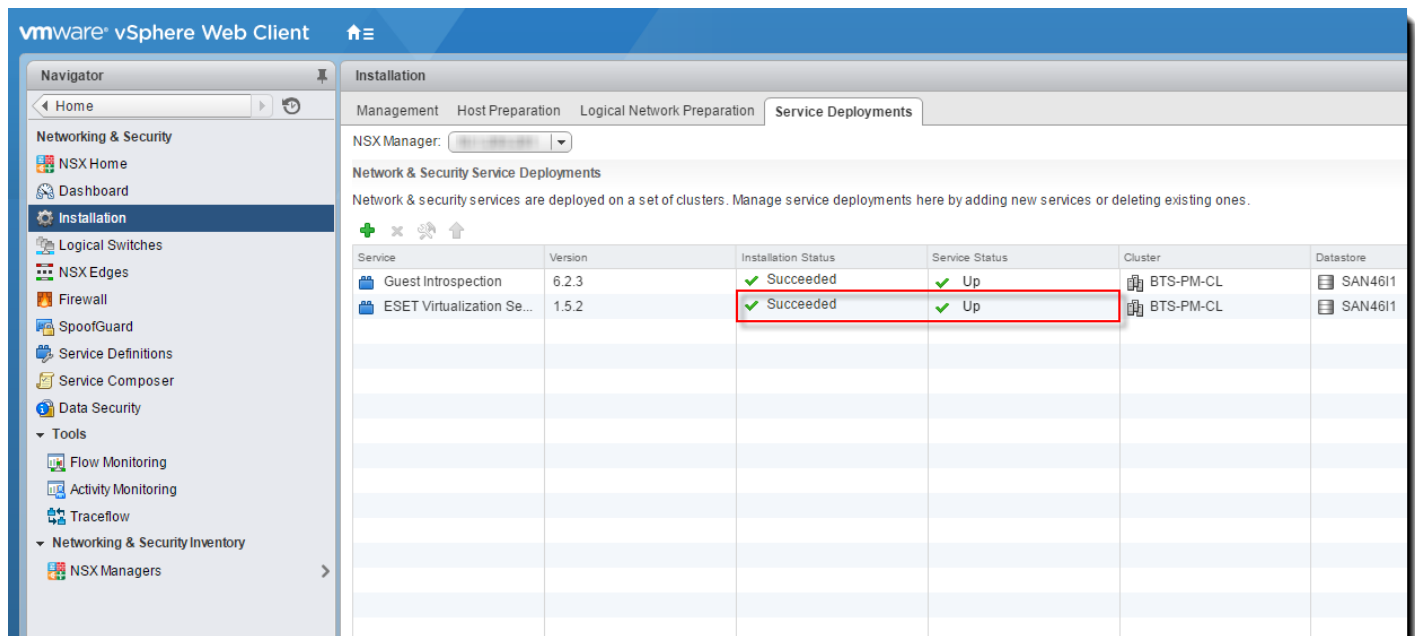
OK Cancel

**NOTE**  
We recommend to leave the DNS Suffix option empty.

We recommend to leave the DNS Suffix option empty.

5. Review settings and click **Finish**. After processing and successful deployment, **wait a few minutes** and you should see that **Unknown** status is changed to **Succeeded** and **Up** in status columns.





**! IMPORTANT**

When installation fails, click [here](#).

**! IMPORTANT**

When you see **Warning** in Service status it means, that ESET Virtualization Security Appliance (SVM) is not able to access vAgent Host virtual machine. Firstly ensure that ESET Virtualization Security has correct policy where to find vAgent Host in ERA settings. For more information read the following [ESET Knowledgebase article](#).

**i NOTE**

After you have successfully installed ESET Virtualization Security, continue to [Activate Virtual Agent Host from ESET Remote Administrator](#) and then [Automatic activation of all EVS VMs](#) for how to activate all of ESET Virtualization Security virtual machine and also dynamic group for ESET Virtualization Security machines that are not activated.

### 3.6 Activate Virtual Agent Host from ESET Remote Administrator

Follow the steps below to activate vAgent Host:

1. To create new client task navigate to **Admin > Client Task > New** in your ERA Web Console.
2. Enter basic information about the task such as the **Name**, **Description** and the **Task Category** (ESET Security Product) and **type of task** (Product activation).
3. You will be able to add Targets after the task has been created.
4. In **Settings** select a license for the vAgent Host (same license as for ESET Virtualization Security). This license will be applied to vAgent Host already deployed in your virtual environment. If you do not see any license, go to [Licenses - add new license](#).
5. Review the summary of configured settings and click **Finish**.
6. The Client Task is now created. The Client Task is now created and a pop-up window will open. We recommend you to click **Create Trigger** to specify when this Client Task should be executed (select As Soon As Possible) and on what Targets (select vAgent Host VM). If you click **Close**, you can create a Trigger later on.

**i NOTE**

Internet connection required for activation.

### 3.7 Automatic activation of all ESET Virtualization Security appliances

To make sure that all ESET Virtualization Security in the cluster are activated, follow this procedure to create dynamic groups in ESET Remote Administrator Web Console:

#### Create Dynamic Group 1

Dynamic Group will group all ESET Virtualization Security appliances for which you can apply same policies.

To create a new Dynamic Group navigate to **Computers > Groups > click All > click  > New Dynamic Group.**


##### Basic

Enter a **name** (e.g. Machine is EVS) and **description** for the New Dynamic Group. Make sure that parent group is set to **All**.


##### Template


Create a new Dynamic Group Template by clicking **New**. Enter a **name** and **description** for the new template.

##### Expression

Click **Add rule**, expand **Computer**, select **Managed products mask** and confirm by clicking **OK**. Click  and select **Other: Virtual Security Appliance** and confirm by clicking **Finish** (2x).

[< BACK](#) New Template - Expression

 BASIC



 EXPRESSION


OPERATION

AND (All conditions have to be true)

Computer . Managed products mask

in



[+ ADD RULE](#)

FINISH

CANCEL

#### Creating policy for Dynamic Group 1 (Machine is EVS)

This policy will determinate settings for every ESET Virtualization Security appliance which appears in this group.

1. Navigate to **Admin > Policies > New policy**.
2. Enter the **name** and select **ESET Virtualization Security - Security Appliance** from drop-down menu in **Settings**.
3. If not predefined, enter the **hostname** or **IP address** and **port** (9880 by default) for Virtual Agent Host.

## Create Dynamic Group 2

Dynamic Group 2 will group all ESET Virtualization Security appliances which are not activated. An auto-activation task will be assigned on this group.

Navigate to **Computers > Groups > Machine is EVS** > click  > **New Dynamic Group**.

### Basic

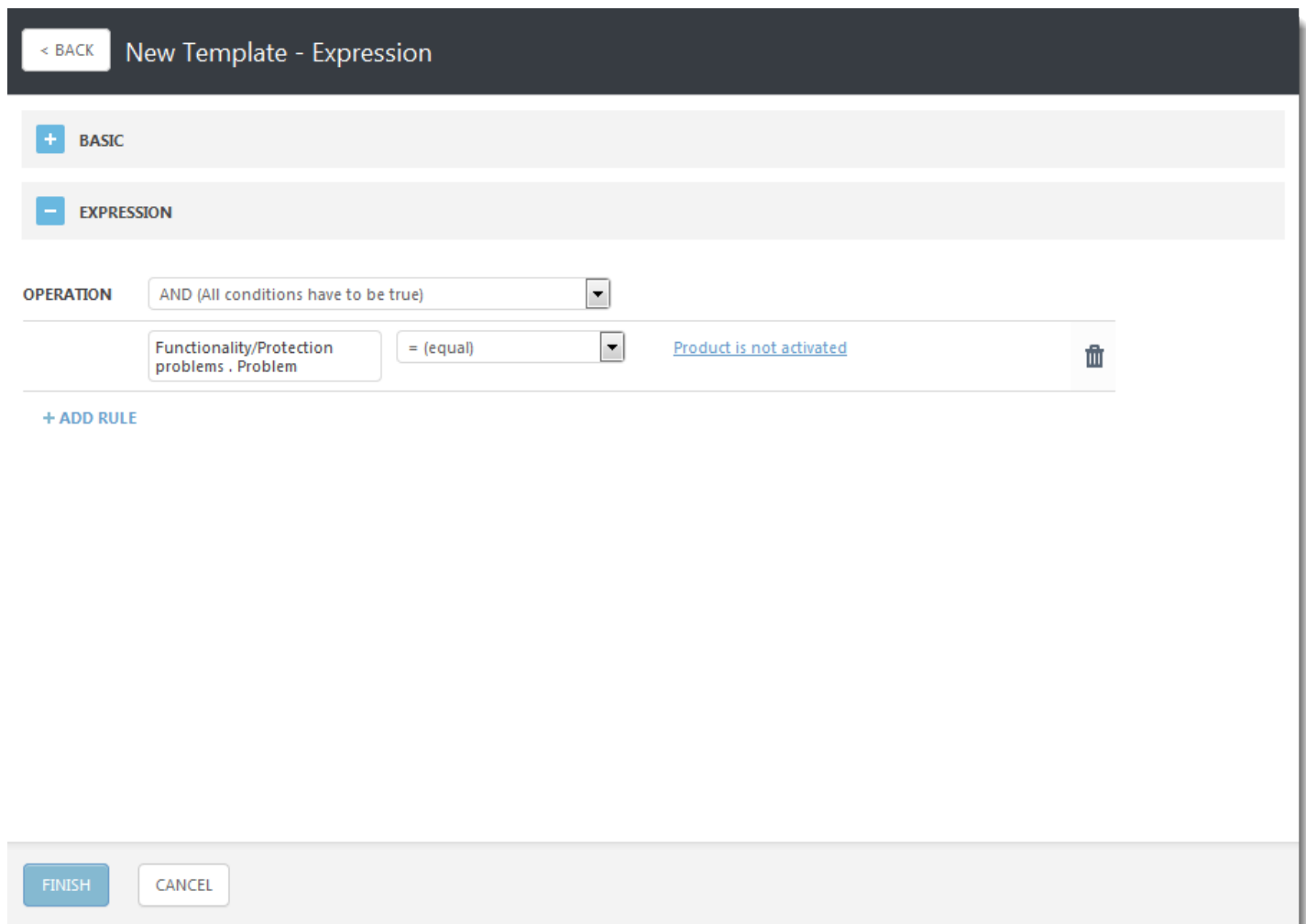
Enter a **name** (e.g. "EVS is not activated") and **description** for the New Dynamic Group. Make sure that parent group is set to **All**.

## Template

Create a new Dynamic Group Template by clicking **New**. Enter a **name** and **description** for the new template.

### Expression

Click **Add rule**, expand **Functionality/Protection problems**, select **Problem** and confirm by clicking **OK**. Select **Product is not activated** and confirm by clicking **Finish** (2x).



## Creating activation task for Dynamic Group 2 (EVS is not activated)

By creating this task, all ESET Virtualization Security appliances that fall into this dynamic group will be automatically activated.

1. Navigate to **Admin > Client Tasks > New**.
2. Enter the **name** and select **Product activation** from the **Task** drop-down menu.
3. In **Settings**, choose the **license** and confirm by clicking **OK**.
4. After you have successfully created activation task, you will be prompted to **create trigger**.
5. Enter the **name**.
6. In **Target**, click **Add Groups**. Expand the **Machine is EVS** group and select checkbox next to **EVS is not activated**.
7. Click **OK** to confirm.
8. In **Trigger**, choose **Joined Dynamic Group Trigger** from the **Trigger type** drop-down menu.
9. Click **Finish** to confirm.
10. Create a new Trigger to run task on Machines, which are already present in this Dynamic Group.
11. Select newly created task and choose **Run On**.
12. In **Target**, click **Add Groups**. Expand the **Machine is EVS** group and select checkbox next to **EVS is not activated**.
13. Click **OK** to confirm.
14. In **Trigger**, choose **As Soon As Possible** from the **Trigger type** drop-down menu.
15. Click **Finish** to confirm.

This task will manage activation of all ESET Virtualization Security machines with an IP address of Virtual Agent Host machine. After successful activation of all ESET Virtualization Security machines, the **EVS is not activated** group contains no virtual machines.

#### **i NOTE**




This allows for each new ESET Virtualization Security deployed in the cluster to be activated automatically.

#### **i NOTE**

The first dynamic group will contain all ESET Virtualization Security machines. The second dynamic group will contain unactivated ESET Virtualization Security machines only.

## **3.8 Creating Security Group with policy**

In this step we will define Security Group where we include all VMs, which we want to protect with ESET Virtualization Security. For this group, we need to apply Security Policy with configured ESET Virtualization Security as security solution in order to protect defined Group.

1. In your vSphere Web Client navigate to **Networking & Security > Service Composer** and click  to create a new security group.
2. Enter the name (e.g. Protected) and define dynamic membership rules or include objects manually for this group.
3. Then navigate to the **Security Policies** tab and create new security policy by clicking .
4. Enter the name (e.g. ESET) and click next.
5. Click  to add Guest Introspection Services. Enter the name (e.g. ESET) and choose the **Apply** action.

**Add Guest Introspection Service**

Name:

Description:

Action: ☒ Apply ☐ Block

Service Type:  ▼

Service Name:  ▼

Service Profile:  ▼

State: ☒ Enabled ☐ Disabled

Enforce: ☒ Yes ☐ No

OK Cancel

6. Select **ESET Virtualization Security** from the **Service Name** drop-down menu, select **Enabled** next to **State** and select **Yes** next to **Enforce**. Click **Finish** to confirm.

ESET - Edit Security Policy

- 1 Name and description
- 2 Guest Introspection Services**
- 3 Firewall Rules
- 4 Network Introspection Services
- 5 Ready to complete

### Guest Introspection Services

Filter

No.	Name	Action	Enforce
1	ESET	Apply ESET Virtualization Security ...	Yes


1 items

Back Next Finish Cancel

7. Go back to the **Security Groups** tab, select your Security Group (e.g. Protected).

The screenshot shows the VMware vSphere Web Client interface. The left sidebar contains the 'Navigator' with 'Service Composer' selected. The main pane shows the 'Security Groups' tab. At the top, there are status boxes for 'Synchronization Status' (Success) and 'Firewall Publish Status' (Success). Below these is a table with columns: Name, Description, Security Policies, Guest Inspection Services, Firewall Rules, Network Inspection Services, Virtual Machines, and Included Security Groups. The table contains two rows: 'Activity Monitoring D...' and 'AV-group'. The 'AV-group' row is highlighted. At the bottom, there are 'Recent Objects' and 'Recent Tasks' sections.

Name	Description	Security Policies	Guest Inspection Services	Firewall Rules	Network Inspection Services	Virtual Machines	Included Security Groups
Activity Monitoring D...		4	0	0	0	0	0
AV-group		1	1	0	0	11	0

8. Click  to apply this policy to your group.

The screenshot shows the VMware vSphere Web Client interface. The left sidebar contains the 'Navigator' with 'Service Composer' selected. The main pane shows the 'Security Groups' tab. At the top, there are status boxes for 'Synchronization Status' (Success) and 'Firewall Publish Status' (Success). Below these is a table with columns: Name, Description, Security Policies, Guest Inspection Services, Firewall Rules, Network Inspection Services, Virtual Machines, and Included Security Groups. The table contains two rows: 'Activity Monitoring D...' and 'AV-group'. The 'AV-group' row is highlighted. A dialog box titled 'AV-group - Security Policy' is open, showing a table with columns: Name, Description, and Applied To. The table contains one row: 'EVS4-protection' applied to 'AV-group'. At the bottom, there are 'Recent Objects' and 'Recent Tasks' sections.

Name	Description	Applied To
EVS4-protection		AV-group

## NOTE

From now on, your virtual machines are protected by ESET Virtualization Security. To check the status navigate to **Host and Clusters**, click your ESET Virtualization Security, open EVS console and you will see the number of protected machines.

## 4. Configuration of ESET Virtualization Security

### 4.1 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 1.5.2.0 T0  
(C) 2016 ESET, spol. s r.o.
```

```
IP address: 10.1.203.159  
IPv6 address: fe80::250:56ff:fe9e:9c30
```

```
Antivirus and antispysware scanner module: 1503 (20161007)  
Virus signature database: 14335 (20161025)
```

```
ESET Remote Administrator agent version: 6.4.293.0  
ESET Remote Administrator agent status: connected
```

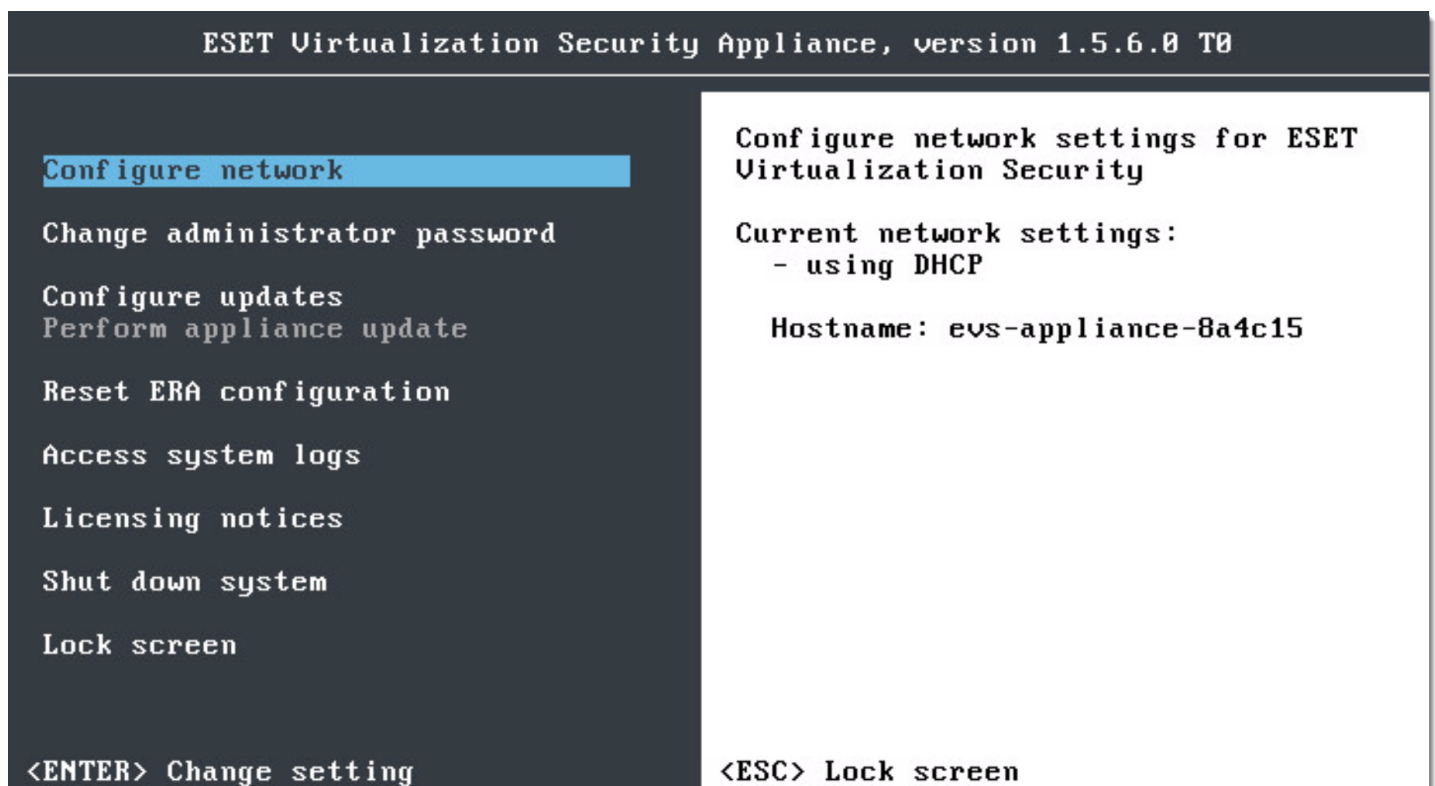
```
Number of connected machines: 8  
Number of protected machines: 8
```

```
<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.
- **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.
- **Access system logs** – Enable SFTP access to system logs.
- **Licensing notices** – contains licensing information about third-party products included in software.
- **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**).

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



### 4.1.1 Tasks

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

- [detection engine update \(previously known as virus signature database\)](#)
- [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**.

## 4.2 Policies for Security Appliance & Protected VMs

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.

#### 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 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](#)).

#### 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.

### 4.2.1 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.

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**.

#### 4.2.1.1 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.

#### 4.2.1.2 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 detection engine will be reported as out of date. The default value is 7.

##### Rollback

**Create snapshots of update files** – Creates a detection engine snapshot.

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

#### 4.2.1.2.1 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.

### 4.2.1.3 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.

### 4.2.1.4 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 detection engine and program modules.

#### 4.2.1.4.1 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.

#### 4.2.1.4.2 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.

### 4.2.1.4.3 System console

**Password** – Specify a password for ESET Virtualization Security.

## 4.2.2 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' and a 'Computer Name' dropdown. The main content area is titled 'New Policy - Settings'. On the left sidebar, there are icons for dashboard, policies, alerts, reports, and a '1' next to the 'Policies' icon. The main panel has a 'Basic' tab selected, showing a dropdown menu for 'ESET Virtualization Security - Protected VM'. Below this, there's a search bar and a list of categories: 'ANTIVIRUS' (with sub-items 'Real-time file system protection' and 'On-demand computer scan'), 'BASIC' (with sub-items 'SCANNER OPTIONS' and 'EXCLUSIONS'), 'ASSIGN', and 'SUMMARY'. The 'BASIC' section is expanded, showing 'SCANNER OPTIONS' with three checkboxes: 'Enable detection of potentially unwanted applications' (unchecked), 'Enable detection of potentially unsafe applications' (unchecked), and 'Enable detection of suspicious applications' (checked). Below this is the 'EXCLUSIONS' section with a text field for 'Paths to be excluded from scanning' and an 'Edit' button. 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**.

#### 4.2.2.1 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.

#### 4.2.2.2 Real-time file system protection

##### 4.2.2.2.1 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.

##### 4.2.2.2.2 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*.

#### NOTE

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

### 4.2.2.2.3 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 detection engine 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**.

### 4.2.2.2.4 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.

### 4.2.2.3 On-demand computer scan

This section provides options to select scanning parameters.

#### 4.2.2.3.1 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.

#### 4.2.2.3.2 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. Working with ESET Virtualization Security for NSX



### 5.1 Creating On-Demand Scan task

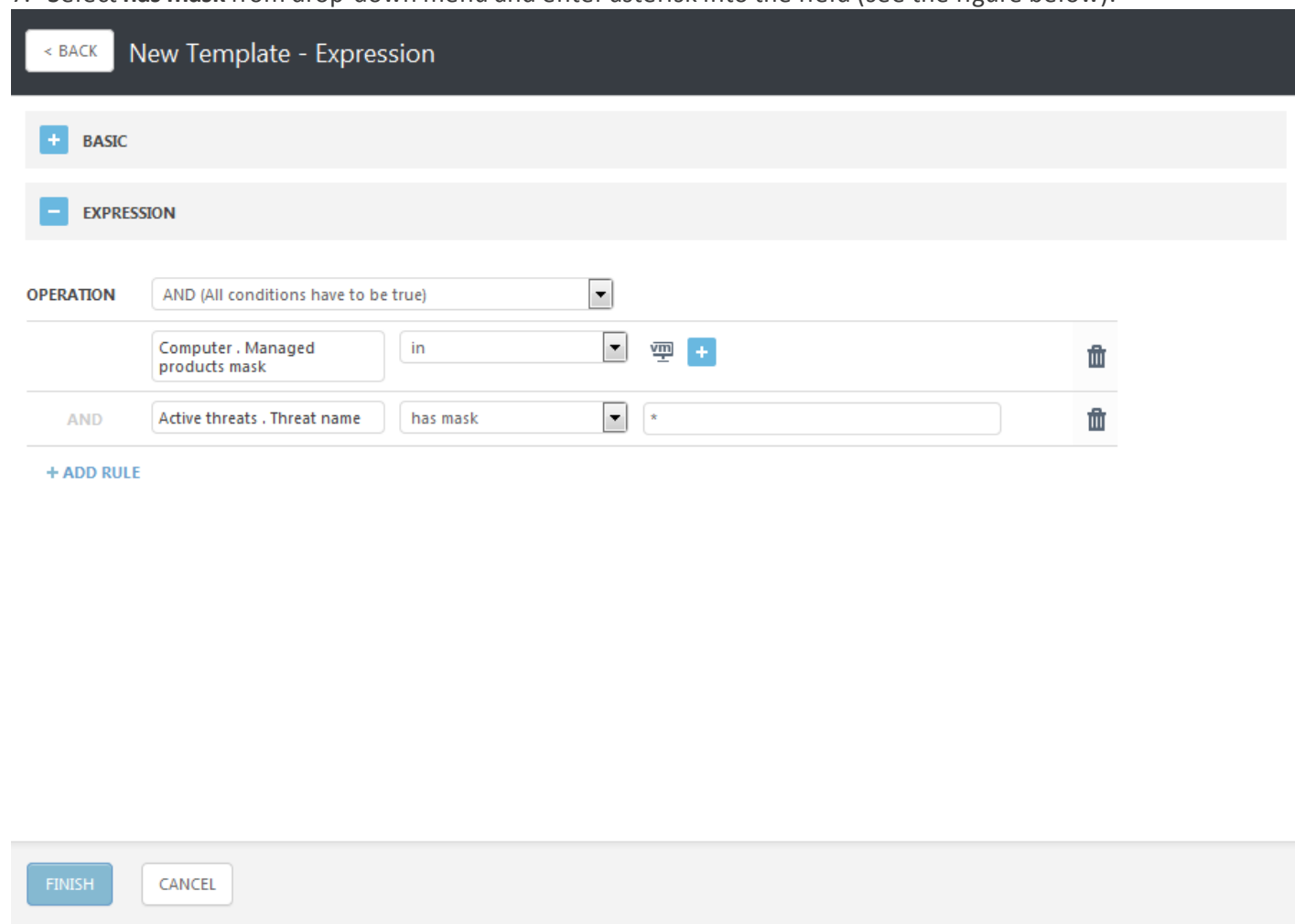
To create On-Demand Scan task perform the following steps:

1. Navigate to **Admin > Client Tasks** and click **New**.
2. Enter the **name** (e.g. "On-Demand Scan") and select **On-Demand Scan** from the **Task** drop-down menu.
3. In **Settings**, select **In-Depth Scan** from the **Scan Profile** drop-down menu with selected **Scan with cleaning** and **Scan all targets**.
4. Confirm by clicking **Finish**. You will be prompted to **create trigger**.
5. Enter the **trigger description**.
6. In **Target**, click **Add Group**, select the checkbox next to the **Infected VM** group (the group you created above).
7. In **Trigger**, select **Joined Dynamic Group Trigger** from the **Trigger type** drop-down menu.
8. Confirm by clicking **Finish**.

## 5.2 Automate On-Demand Scan after infection

You have to create two client task in ERA Web Console to run On-Demand Scan automatically when threat(s) found on virtual machine(s). To do this, perform the following steps:

1. Navigate to **Computers > Groups > All** > click  > **New Dynamic Group** and create new dynamic group.
2. Enter the **name** (e.g. "Infected VM").
3. In **Template**, click **New** and enter the **name**.
4. In **Expression**, click **Add rule**, expand **Computer**, select **Managed product masks** and confirm by clicking **OK**.
5. Click  and select **ESET protected: Virtual Machine (agentless)** and remove **ESET protected: Desktop** (monitor icon).
6. Add another rule. Expand **Active threats**, select **Threat name** and confirm by clicking **OK**.
7. Select **has mask** from drop-down menu and enter asterisk into the field (see the figure below).



8. Click **Finish** (2x) to confirm.

### NOTE

This dynamic group will contain agentless virtual machines where threats were found.

The next step is to create the second client task according to the following steps:

1. Navigate to **Admin > Client Tasks** and click **New**.
2. Enter the **name** (e.g. "On-Demand Scan") and select **On-Demand Scan** from the **Task** drop-down menu.
3. In **Settings**, select **In-Depth Scan** from the **Scan Profile** drop-down menu with selected **Scan with cleaning** and **Scan all targets**.
4. Confirm by clicking **Finish**. You will be prompted to **create trigger**.
5. Enter the **trigger description**.
6. In **Target**, click **Add Group**, select the checkbox next to the **Infected VM** group (the group you created above).
7. In **Trigger**, select **Joined Dynamic Group Trigger** from the **Trigger** type drop-down menu.
8. Confirm by clicking **Finish**.

### 5.3 Tagging workflow for Guest Introspection

1. Use NSX Manager console to create security groups and policies.
2. Create a security group called **Desktop Security Group** and any virtual machine can be part of this group.
3. Create a dynamic security group called **Quarantine Security Group**. Any virtual machine tagged with a tag **ABC.VirusFound.Severe** becomes a part of this group.
4. Create a security policy for **Desktop Security Group**. This policy states if on a virus scan a member virtual machine is found to be infected then set a tag on this virtual machine with value **ABC.VirusFound.Severe**.
5. Create a security policy for **Quarantine Security Group**. This policy states if on a virus scan a member virtual machine is found clean then remove the tag with value **ABC.VirusFound.Severe**.

On Access virus scan runs on ESET Virtualization Security and for virtual machines that are clean no action is taken. If a virtual machine is found infected the ESET Virtualization Security can clean the malware. Virtual machine that is not clean will be tagged with **ABC.VirusFound.Severe** and this virtual machine will be removed from Desktop Security Group and moved to Quarantine group (infected files are not deleted). In Quarantine group all incoming accesses are blocked, except for remediation. After you run an On-Demand Scan for the quarantined virtual machines and the malware was cleaned, the virtual machines will be untagged and moved back to the Desktop Security Group.

### 5.4 Understanding of Security Tags and how ESET triggers them

Security Tag is a labelling mechanism in VMware Service Composer that can be used as an abstraction to describe a state. This can be impressed upon a workload or be the matching criteria to a Security Group. With Security tags you can automate any behavior using NSX Service Composer using ESET or 3rd party services. For more information [click here](#).

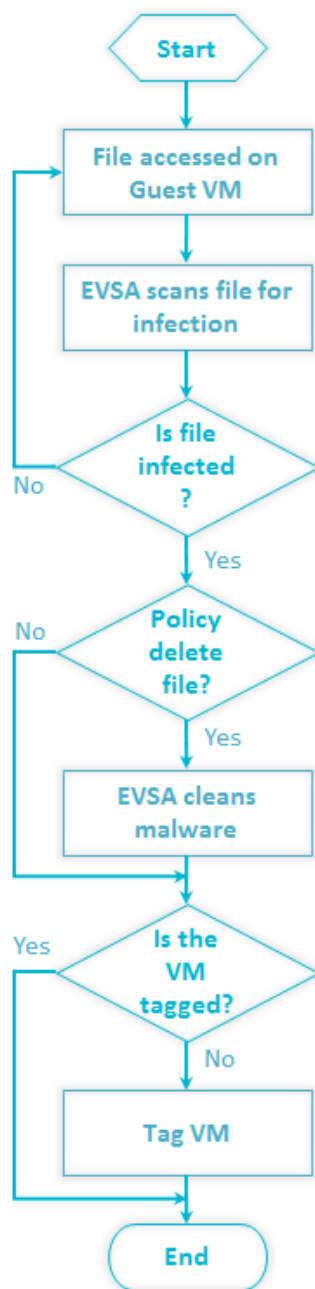
By defaults, once ESET finds Malware on any VM a Security tag is applied. You can use pre-defined Security tag or define it during [Registration to NSX](#).

Admin can enable or disable security tagging (under **NSX Security Tagging**) and choose from the following tagging options using ERA policy:

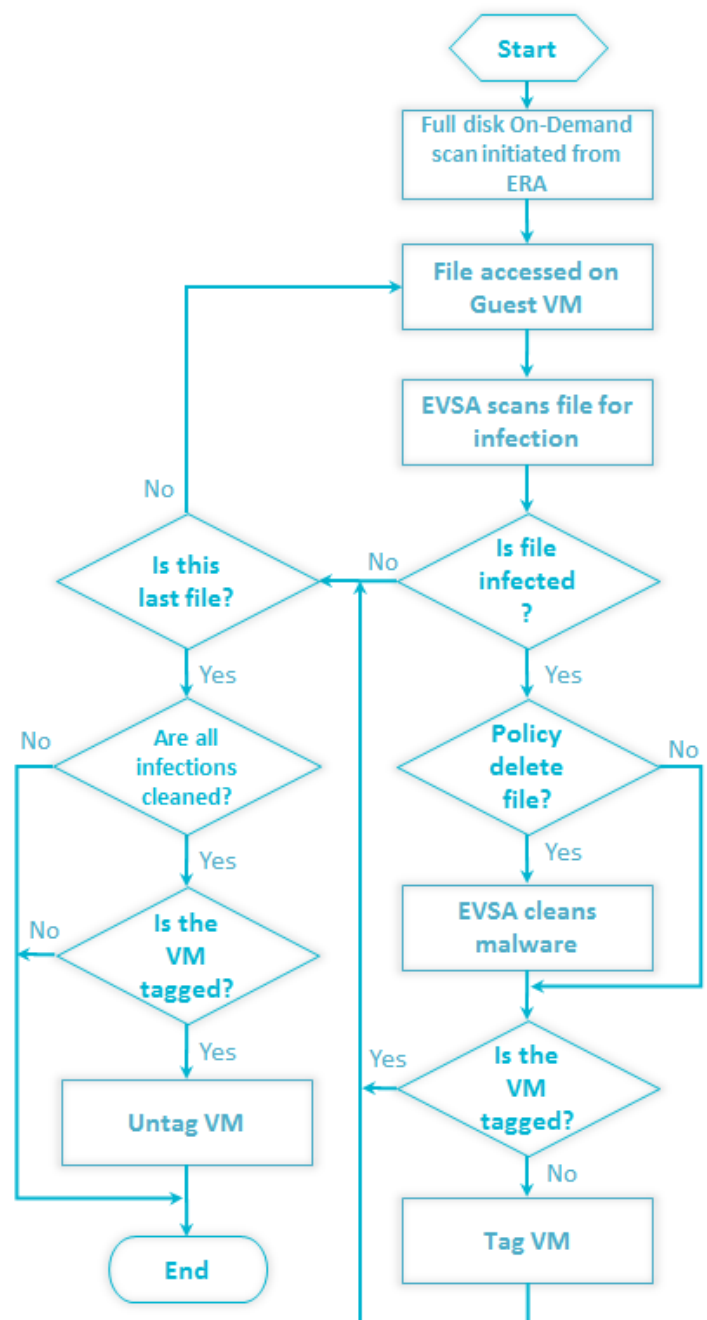
- Apply the tag only when the threat cannot be cleaned
- On-demand scan profile required to remove the tag

ESET Virtualization Security is able to automatically tag and un-tag VMs according to following workflow:

## On-Access Workflow



## On-Demand Workflow



### 5.5 Automatically quarantine VM upon malware detection using NSX


In this use-case, once ESET Virtualization Security detects malware, infected VM will be put into Quarantine Security Group, which will block all network access to this VM until machine is scanned and cleaned. Once cleaned, VM is moved to previous Group with enabled network access.

#### Prerequisites

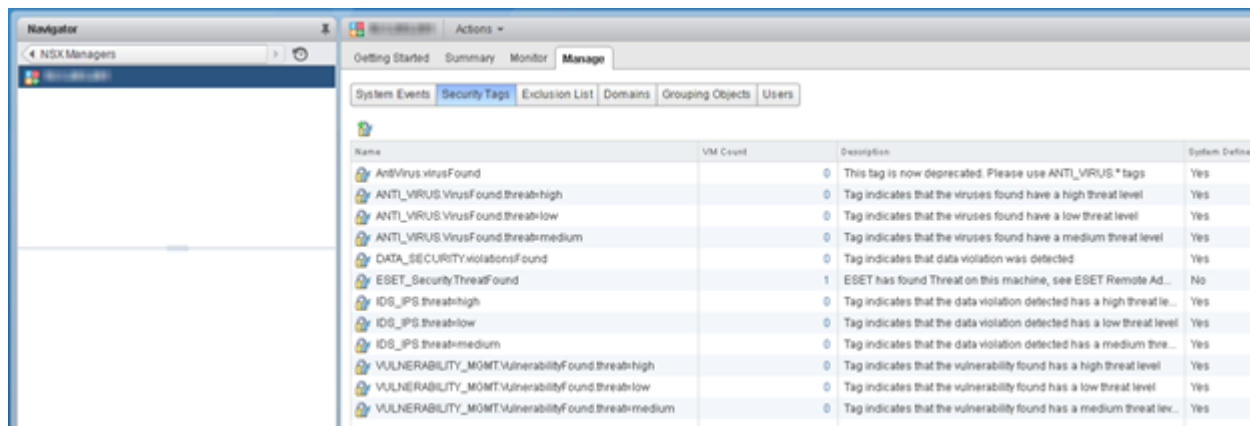
1. You must have valid VMware NSX license at least in Standard edition (not one included in vSphere license)
2. Deployed NSX Distributed Switch on your hosts
3. VMs have to use Distributed Port Group as Network adapter

- NSX Components & Firewall have to be installed and Enabled on Cluster and Hosts in **vCenter > Networking & Security > Installation > Host Preparation**

### Creation of Quarantine Security Group





- In vCenter go to **Networking & Security > Service Composer > Security Groups**
- Click on **New Security Group**  , name it **Quarantine** and click **Next**
- Under **Define dynamic membership** click **Add**, from drop-down menu choose **Security Tag** and to entry field type tag, which you registered during Registration\*.
- Click on **Finish**

\* You can see all available tags in **Networking & Security** Section > under **Networking & Security Inventory** click **NSX Managers > click IP Address > under Manage** tab choose **Security Tags** and all available tags will be listed.

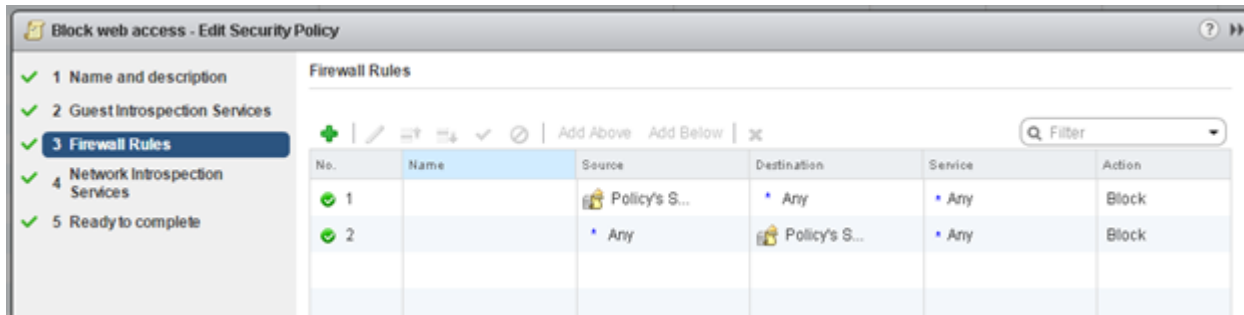


Name	VM Count	Description	System Defined
AntiVirus.virusFound	0	This tag is now deprecated. Please use ANTI_VIRUS.* tags	Yes
ANTI_VIRUS.VirusFound.threat-high	0	Tag indicates that the viruses found have a high threat level	Yes
ANTI_VIRUS.VirusFound.threat-low	0	Tag indicates that the viruses found have a low threat level	Yes
ANTI_VIRUS.VirusFound.threat-medium	0	Tag indicates that the viruses found have a medium threat level	Yes
DATA_SECURITY.violationsFound	0	Tag indicates that data violation was detected	Yes
ESET_SecurityThreatFound	1	ESET has found Threat on this machine, see ESET Remote Ad...	No
IDS_IPS.threat-high	0	Tag indicates that the data violation detected has a high threat le...	Yes
IDS_IPS.threat-low	0	Tag indicates that the data violation detected has a low threat level	Yes
IDS_IPS.threat-medium	0	Tag indicates that the data violation detected has a medium thre...	Yes
VULNERABILITY_MOMT.VulnerabilityFound.threat-high	0	Tag indicates that the vulnerability found has a high threat level	Yes
VULNERABILITY_MOMT.VulnerabilityFound.threat-low	0	Tag indicates that the vulnerability found has a low threat level	Yes
VULNERABILITY_MOMT.VulnerabilityFound.threat-medium	0	Tag indicates that the vulnerability found has a medium threat lev...	Yes


### Creation of Quarantine Security Policy

- Choose **Security Policies** tab and click on **Create Security Policy**  and name it **Block network access**
- Click on **3 Firewall Rules** and select plus button 
- Next to **Action** select **Block**
- As **Source** choose **Policy's Security Groups**
- As **Destination** select **Any**
- State **Enabled**
- Confirm by clicking **OK**
- Once again click the button 
- Repeats steps 3-7, but now as **Source** choose **Any** and as **Destination** choose **Policy's Security Groups**
- Confirm by clicking **OK**
- Click on **Finish**
- Ensure that newly created policy is on top of other policies. You can adjust it with **Manage Priority** button 

You should be able to see the following rules:



### Assigning Quarantine Security Policy to Quarantine Security Group

1. Click on newly created Security Policy and click on **Apply Security Policy** icon 
2. Check Quarantine group and confirm by clicking **OK**

### Automate on-demand scan after on-access detect malware on VM

To automatically start on-demand scan once on-access detect malware, please [click here](#).

### Expected Behavior

From now on, if ESET detects Malware, it'll automatically Tag infected VM (see "Understanding of Security Tags and how ESET triggers them" Section) and this VM will fall into **Quarantine** Security Group, for which configured blocking of network access. Once Security Tag is removed by Full Disk On-demand scan, VM will not be part of **Quarantine** Security Group and all network access will be recovered.



## 6. Updating ESET Virtualization Security

ESET Virtualization Security for VMware NSX consists of multiple components. Virtual Agent Host Virtual Machine contains Virtual Agent Host, which is a component of ESET Remote Administrator that virtualizes agent entities to allow management of agentless virtual machines. For more information [click here](#).

Virtual Agent Hosts Virtual Machine contains ESET NSX Service Manager, which is a component responsible for registration to VMware NSX Manager, serves as a communication channel between ESET Virtualization Security Appliances and VMware NSX Manager and it also contains ESET Virtualization Security Appliance (EVSA) OVF image.



In order to update EVSA (OVF) through vCenter NSX plugin, firstly we need to update ESET NSX Service Manager, which contains new image of EVSA. In some cases, update of Virtual Agent Host will be necessary too to provide new functionality or compatibility.


### 6.1 How to check for available updates


To check if any updates are available for Virtual Agent Host VM, please:

1. Open ESET Remote Administrator Dashboard and choose **ESET applications** tab
2. All application updates are visible in **Outdated applications** section

Or do the following:

1. In ESET Remote Administrator choose **Computers** and find Virtual Agent Host machine


2. Name should be in yellow rectangle:  Virtual Agent Host


3. Click on machine, select **Details** and choose **Installed Applications** 

4. All outdated application will be available with yellow color as Warning

To check for available updates for ESET Virtualization Security Appliance CentOS Operating System, please:

1. In ESET Remote Administrator choose **Computers** and find Virtual Agent Host machine

2. Name should be in yellow rectangle:  EVS-Appliance-1

3. Click on machine, select **Details** and choose **Alerts** 

4. You should be able to see following alert: 

## 6.2 How to update vAgent Host

When update of Virtual Agent Host will be available, please do the following:

1. Click on Virtual Agent Host VM and choose **New Task**
2. From **Task** field choose **Remote Administrator Components Upgrade**
3. 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.

eset REMOTE ADMINISTRATOR

Computer Name [dropdown] [search] [help] 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

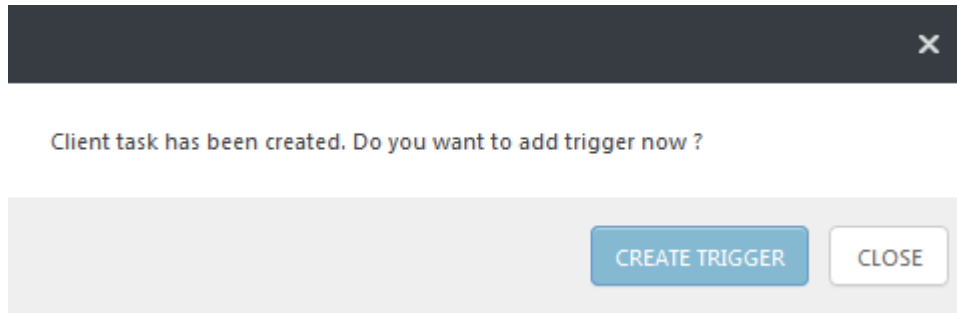
### Settings

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.



## 6.3 How to update ESET NSX Service Manager

When update of ESET NSX Service Manager will be available, please follow these steps

1. Click on Virtual Agent Host VM and choose **New Task**
2. From **TASK** field choose **Software Install**
3. In **Settings** section please accept EULA, choose ESET License
4. For ESET Remote Administrator 6.5+, please:
  - a. Choose **Install package from repository** and click on **<CHOOSE PACKAGE>**
  - b. Find updated **ESET NSX Service Manager** using scrolling or filtering and press **OK**

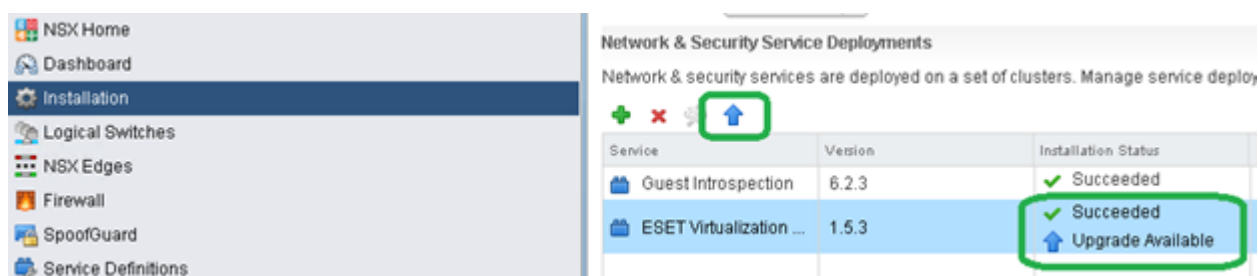
Confirm everything by clicking on **Finish**.

### NOTE

ESET Virtualization Security Appliance 1.6 is compatible with ESET Remote Administrator 6.5+ only.

## 6.4 How to update ESET Virtualization Security Appliance - Secure Virtual Machine

Once you update ESET NSX Service Manager a new upgrade button will be visible in VMware NSX Manager under **Installations** section:



To update ESET Virtualization Security Appliance for selected cluster, please:

1. Select ESET Virtualization Security for corresponding cluster and click on upgrade
2. Follow instructions on screen

## 6.5 How to update Operating System on ESET Virtualization Security Appliance

To update Operating System using ESET Remote Administrator, please:

1. Click on ESET Virtualization Security Appliance and choose **New Task**
2. From **TASK** field choose **Operating System Update**
3. Ensure that in **Settings** section you have checked **Automatically Accept EULA**
4. Confirm everything by clicking on **Finish**

## 6.6 Ports

### ESET Remote Administrator

For list of all ports necessary for ESET Remote Administrator, please [click here](#).

#### Virtual Agent Host VM

Port	Protocol	Usage	Description
9880	TCP	Listening	Communication from ESET Virtualization Security Appliance
8443	TCP	Listening	Connection from VMware NSX Manager to ESET NSX Service Manager
443	TCP	Call	Connection from ESET NSX Service Manager to VMware NSX Manager
22	TCP	Listening	Connection via SSH
10000	TCP	Listening	Webmin Interface
1237/1238	UDP	Listening	Wake-up call from ESET Remote Administrator

### ESET Virtualization Security Appliance

Port	Protocol	Usage	Description
2222	TCP	Call	Communication to ESET Remote Administrator
9880	TCP	Call	Communication to Virtual Agent Host

## 7. Working with ESET Remote Administrator

### 7.1 Detection engine update

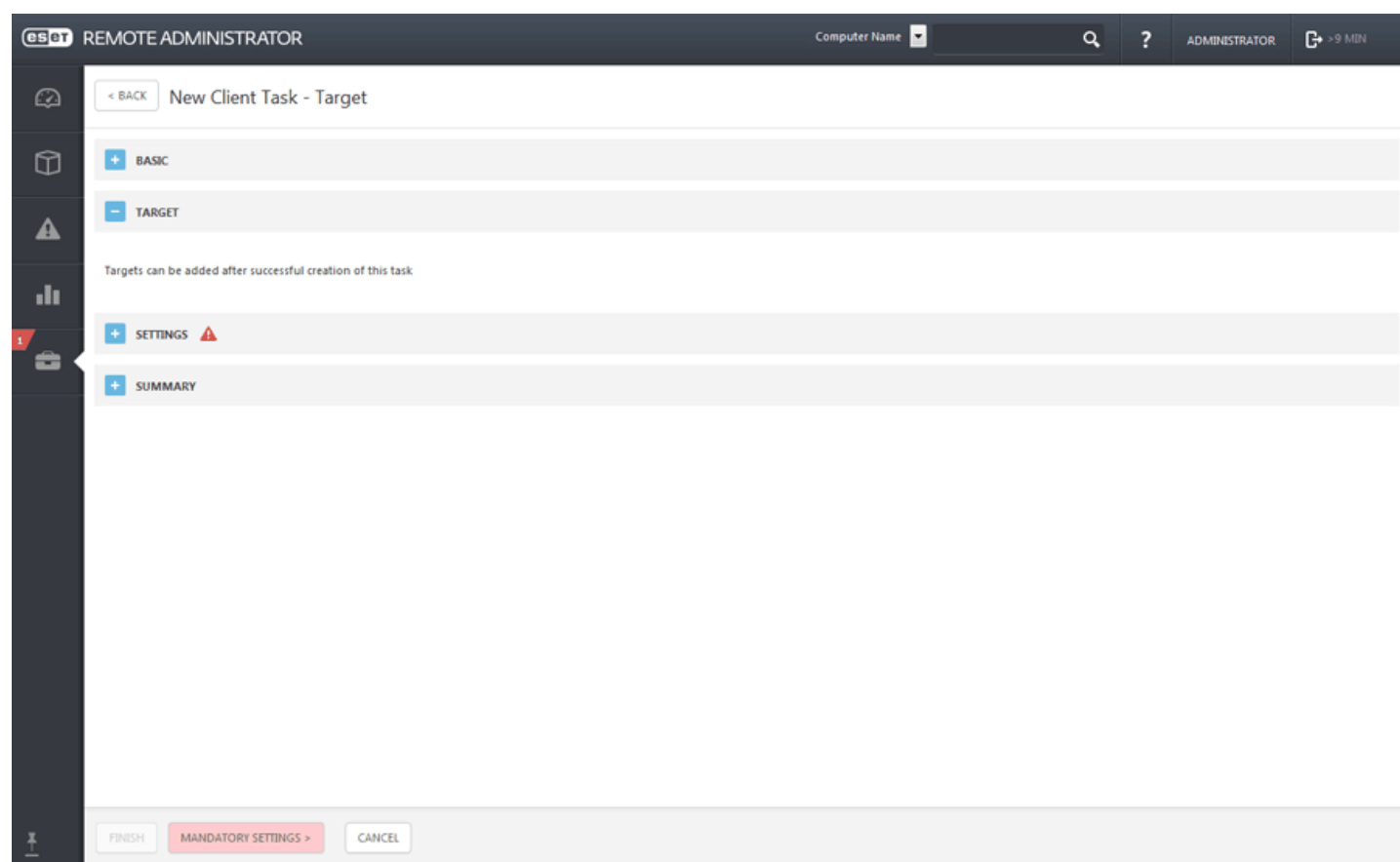
The **Product Update** task will update detection engine information (previously known as virus signature database) for security product installed on clients. This is a general task for all products on all systems.

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.



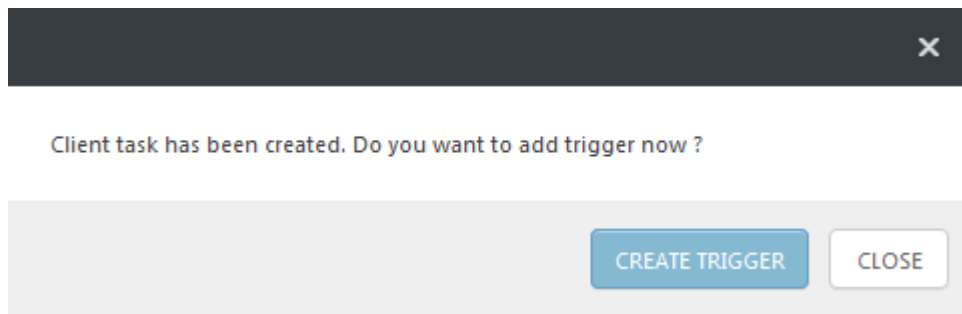
The screenshot shows the ESET Remote Administrator web interface. The top header includes the ESET logo, 'REMOTE ADMINISTRATOR', a 'Computer Name' dropdown, a search icon, a help icon, 'ADMINISTRATOR', and a '>9 MIN' indicator. The left sidebar contains navigation icons for Home, Tasks, Alerts, Reports, and a red notification badge. The main content area is titled 'New Client Task - Target' and features a breadcrumb '< BACK'. Below the title are four expandable sections: 'BASIC', 'TARGET' (which is currently expanded), 'SETTINGS' (with a red warning icon), and 'SUMMARY'. A message states 'Targets can be added after successful creation of this task'. At the bottom, there are three buttons: 'FINISH', 'MANDATORY SETTINGS >' (highlighted in red), and 'CANCEL'.

#### Settings

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



## 7.2 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).

### NOTE

ESET Virtualization Security can run only one on-demand scan at the same time on your Protected VM. Running second or more scans will cause to **Task failed** result in ERA Web Console.

## 7.3 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**.

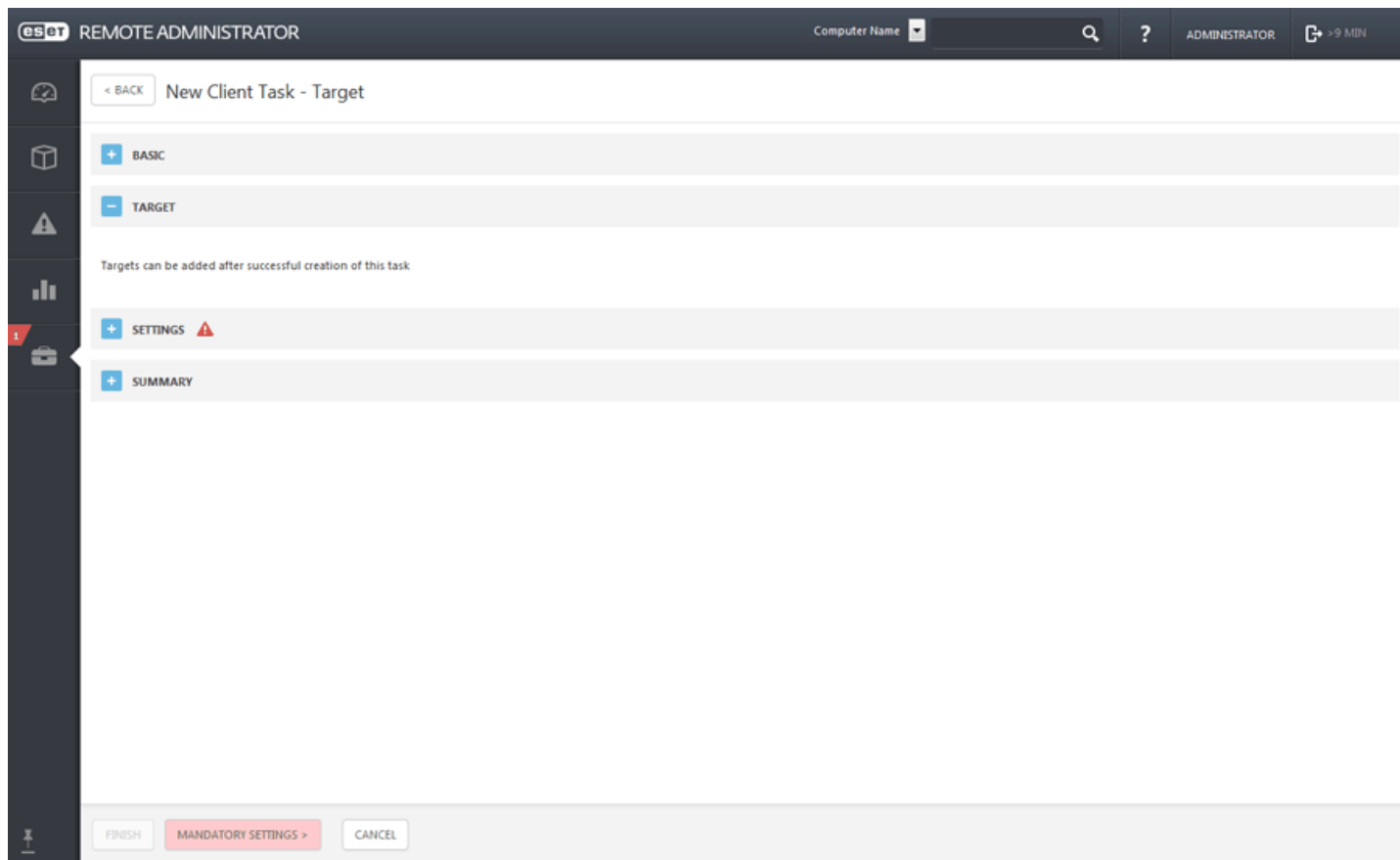
### Basic

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).

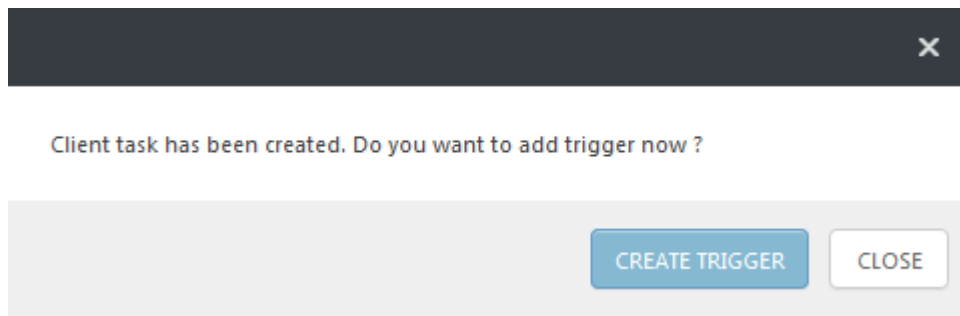
**Filter type** - Filter the objects in the Quarantine based on the criteria defined below. Either based on the hash string of the object or conditions.

**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.



## 7.4 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.

## 7.5 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.

## 7.6 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](#).

## 7.7 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](#).



## 7.8 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.

## 8. 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](#)
- [How to access system logs](#)

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.

### 8.1 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

## 8.2 How to activate and initial setup

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

1. [How to activate ESET Virtualization Security](#)
2. [How to get a license](#)
3. [How unilicense works](#)
4. [How to import license to ESET Remote Administrator](#)
5. How to use offline license

### 8.2.1 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](#).

### 8.2.2 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 want to protect 100 virtual machines with ESET Virtualization Security, you need an ESET License with 100 endpoint seats.

### 8.2.3 How to import license to ESET Remote Administrator

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, a search icon, a help icon, the user role "ADMINISTRATOR", and a session timer showing "+ 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 (which is currently selected). The main content area is titled "License Management" and features a table with the following columns: PUBLIC ID, PRODUCT NAME, STATUS, UNITS, SUBUNITS, EXPIRES, OWNER NAME, and CONTACT. A single license entry is visible in the table with the following details: PUBLIC ID "333-3VW-PSP", Product Name "Business", Product "ESET Endpoint Antivirus for Wind...", Status "Active" (indicated by a green checkmark), Units "0/0 (2 offline)", Expires "2016 Nov 10 13:00:00", and Owner Name "ESET TEST ERA". At the bottom of the interface, there are buttons for "SYNCHRONIZE LICENSES", "OPEN ELA", "OPEN EMA", "ADD LICENSES", and "REMOVE LICENSES".

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

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).

The screenshot shows the ESET Remote Administrator (ERA) interface. On the left is a sidebar with navigation icons and labels: 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 main window is titled 'License Management' and contains a 'PUBLIC' tab and a '< BACK' button. A modal dialog box titled 'Add License - License Key' is open. It has a 'LICENSE KEY' section with a text input field and a red warning icon. Below this is a link: 'I have a Username and Password, what do I do?'. There are also sections for 'SECURITY ADMIN CREDENTIALS' and 'OFFLINE LICENSE FILE', each with a plus icon and a red warning icon. At the bottom of the dialog are buttons: 'ADD LICENSES', 'MANDATORY SETTINGS >', and 'CANCEL'. The background interface shows buttons for 'SYNCHRONIZE LICENSES', 'OPEN ELA', 'OPEN EMA', and 'ADD LICENSES' (with a red warning icon) and 'REMOVE LICENSES'.

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

The screenshot shows the ESET Remote Administrator (ERA) interface. On the left is a sidebar with navigation icons and labels: 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 main window is titled 'License Management' and contains a 'PUBLIC' tab and a '< BACK' button. A modal dialog box titled 'Add License - Security Admin Credentials' is open. It has a 'LICENSE KEY' section with a plus icon and a red warning icon. Below this is a 'SECURITY ADMIN CREDENTIALS' section with a minus icon and a red warning icon. It contains two text input fields: 'SECURITY ADMIN LOGIN' and 'PASSWORD', each with a red warning icon. Below the password field is a 'SHOW PASSWORD' link. There is also an 'OFFLINE LICENSE FILE' section with a plus icon and a red warning icon. At the bottom of the dialog are buttons: 'ADD LICENSES', 'MANDATORY SETTINGS >', and 'CANCEL'. The background interface shows buttons for 'SYNCHRONIZE LICENSES', 'OPEN ELA', 'OPEN EMA', and 'ADD LICENSES' (with a red warning icon) and 'REMOVE LICENSES'.

#### **NOTE**

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

## 8.3 How ESET Virtualization Security interacts with VMware products

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

## 8.4 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 ERA Web Console 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](#).

## 8.5 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.

## 8.6 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.

## 8.7 How to uninstall ESET Virtualization Security

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

1. Delete policies with ESET Guest Introspection via Service Composer
2. Ensure that number of protected virtual machines is zero in ESET Virtualization Security
3. Delete ESET Virtualization Security from NSX Service Deployments
4. Open Virtual Agent Host virtual machine and:
  - a. enter the **Management mode**
  - b. choose **Register to VMware NSX Manager**
  - c. type **u** and confirm by pressing **Enter** to unregister Virtual Agent Host from VMware NSX Manager
  - d. ensure that status is **Not registered**
5. Execute **stop managing -uninstall ERA agent** task on all **Agentless machines**
6. Delete ESET Virtualization Security and Virtual Agent Host virtual machines
7. Remove computers from ESET Remote Administrator (select them and delete them)

## 8.8 How to access system logs

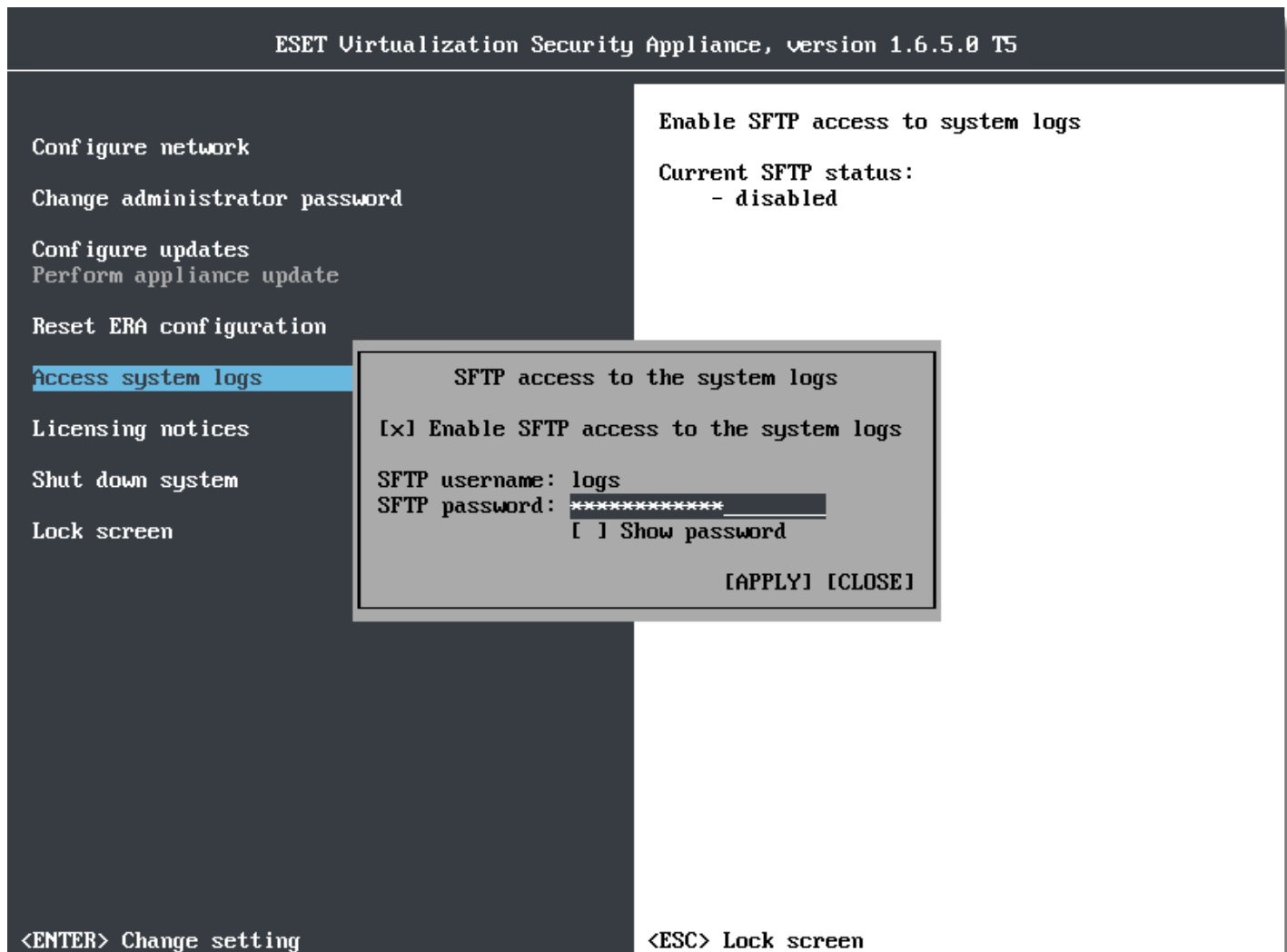
### IMPORTANT

For security reasons, we recommend that you disable SFTP access to the system logs after you have sent logs to ESET Customer Care.

### NOTE

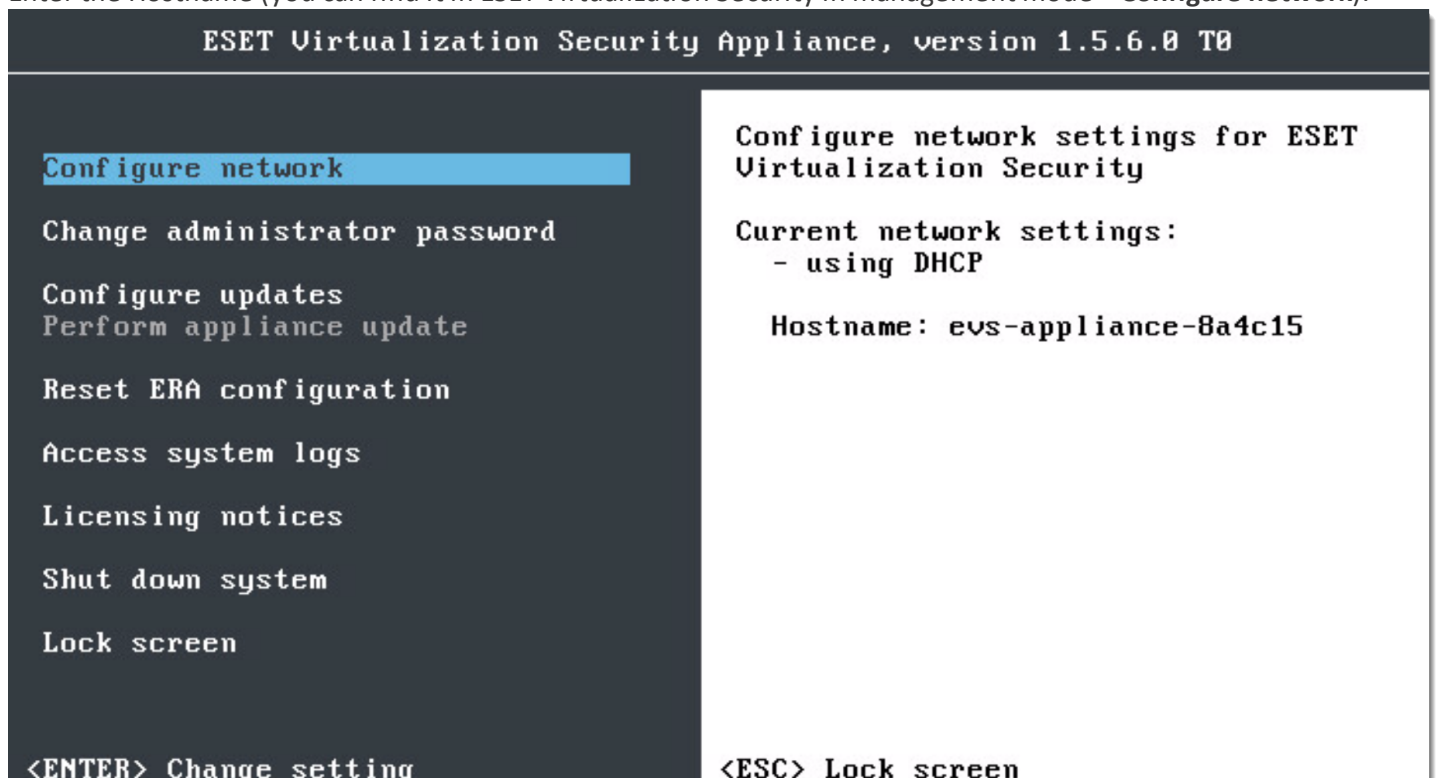
If some log files could not be downloaded, re-enabling this feature could resolve it.

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**.



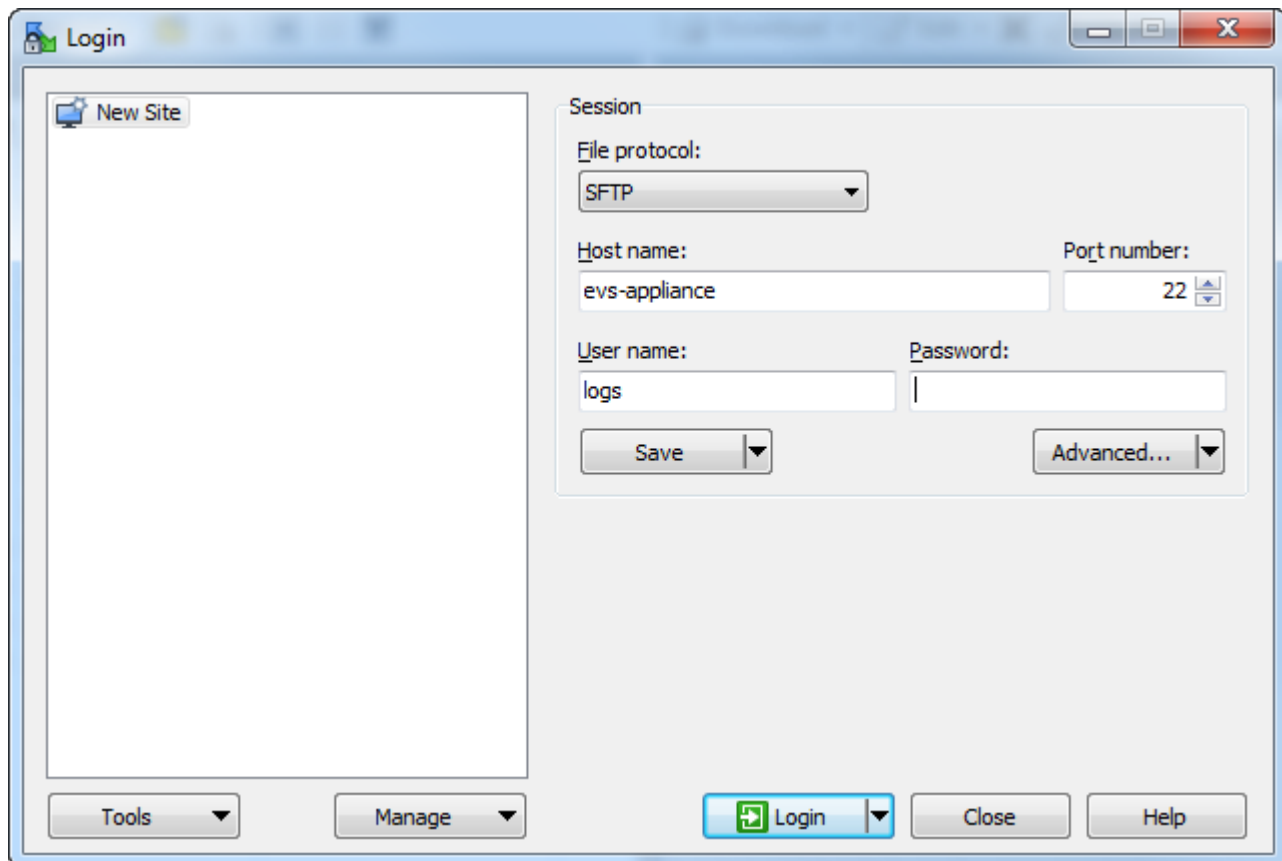
Run your SFTP client (we recommend to use free WinSCP SFTP client).

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/

## 8.9 How to deploy vAgent Host with existing certificates

If you want to deploy vAgent Host and ESET Virtualization Security and use existing certificates do the following steps:

- [Deploy vAgent Host and ESET Virtualization Security in a standard way](#)
- Import existing certificates via ERA policy

### Import existing certificates via ERA policy

You can import existing certificates from ERA Web Console. Navigate to **Admin > Policies > New Policy > select product > ESET Remote Administrator Virtual Agent Host > Agents > Change certificate > Remote Administrator certificate > Open certificate list** and choose **Proxy certificate**.

## 9. Troubleshooting

### 9.1 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>/`

#### NOTE

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

### 9.2 Where to find the logs for ESET Virtualization Security

Logs are used by developers to solve problems with product components. By default, access to the system logs is disabled. To enable an access to the system logs via File-Transfer over SSH (SFTP) enter the management console and go to **Access system logs**. Enter the **logs** username and set password for it and confirm.

For more information see [How to access system logs](#).

### 9.3 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/`

#### NOTE

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

### 9.4 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.*`

#### ESET Virtualization Security

See [How to access system logs](#).

#### 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`.

## 9.5 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](#).

## 9.6 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](#)

## 9.7 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:

```
G:\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 --o
/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.

## 9.8 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)

## 9.9 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

## 9.10 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](https://edf.eset.com) to test connectivity.

### **i** NOTE

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

## 9.11 Path excluded from scanning

There may be a problem with path excluded from scanning. Excluded local directories will be resolved once when the function is called. This means that path exclusion does not work if the path does not exist at the time when policy applied. This is a limitation of EPSec provided by VMware.

## 10. Glossary

### 10.1 ESXi host

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

### 10.2 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).

### 10.3 Virtual machine

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

### 10.4 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.

### 10.5 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.

### 10.6 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).