ESET Virtualization Security for VMware NSX

Click here to display Online help version of this document
Contents

1. What is ESET Virtualization Security and how does it work? .............................. 5
   1.1 Architecture for VMware NSX ........................................ 5
   1.2 Requirements .............................................................. 6
   1.3 How the components interact ...................................... 7
   1.4 Features & Benefits ...................................................... 8

2. How to upgrade your VMware environment to NSX ....................................... 9
   2.1 Unregistration of current ESET solution ....................... 9
   2.2 Upgrade vShield to NSX ............................................... 10

   3.1 Guest Introspection installation .................................. 12
   3.2 VMware Tools installation .......................................... 12
   3.3 vAgent Host deployment ............................................ 13
   3.4 Register ESET to VMware NSX Manager ...................... 17
   3.5 ESET Virtualization Security Appliance (SVM) deployment .................................. 20
   3.6 Activate Virtual Agent Host from ESET Remote Administrator .............................. 24
   3.7 Automatic activation of all ESET Virtualization Security appliances ..................... 25
   3.8 Creating Security Group with policy ................................ 27

4. Configuration of ESET Virtualization Security ............................................... 30
   4.1 Managing ESET Virtualization Security from the console ............................... 30
      4.1.1 Tasks ..................................................................... 32
   4.2 Policies for Security Appliance & Protected VMs .......................................... 32
      4.2.1 ESET Virtualization Security - Security Appliance policy .......................... 33
      4.2.1.1 Antivirus ............................................................ 34
      4.2.1.2 Update ............................................................. 34
      4.2.1.2.1 Primary/Secondary Server ................................ 34
      4.2.1.3 Virtual Agent Host ............................................. 35
      4.2.1.4 Tools ............................................................... 35
      4.2.1.4.1 Log files ....................................................... 35
      4.2.1.4.2 Proxy server ................................................ 35
      4.2.1.4.3 System console ........................................... 36
      4.2.2 ESET Virtualization Security - Protected VM policy .................................. 36
      4.2.2.1 Antivirus ............................................................ 37
      4.2.2.2 Real-time file system protection ................................ 37
      4.2.2.2.1 Basic ............................................................ 37
      4.2.2.2.2 ThreatSense parameters .................................. 37
      4.2.2.2.3 Additional ThreatSense parameters ...................... 39
      4.2.2.4 Clean file cache ................................................. 39
      4.2.2.3 On-demand computer scan .................................. 39
      4.2.2.3.1 Basic ............................................................ 39
      4.2.2.3.2 ThreatSense parameters .................................. 40

5. Working with ESET Virtualization Security for NSX ...................................... 43
   5.1 Creating On-Demand Scan task .................................... 43
   5.2 Automate On-Demand Scan after infection .......................... 44
   5.3 Understanding of Security Tags and how ESET triggers them ......................... 45
   5.4 Automatically quarantine VM upon malware detection using NSX .................... 46

6. Updating ESET Virtualization Security ......................................................... 49
   6.1 Check for available updates ........................................... 49
   6.2 Update vAgent Host .................................................... 50
   6.3 Update ESET NSX Service Manager ................................ 51
   6.4 Update ESET Virtualization Security Appliance - Secure Virtual Machine .......... 51
   6.5 Update Operating System on ESET Virtualization Security Appliance ............... 51
   6.6 Ports ............................................................................ 52

7. Working with ESET Remote Administrator ...................................................... 53
   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

8. Common Questions ......................................................................................... 58
   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
      8.5.1 Enable trace logging .............................................. 63
   8.6 How to read the logs .................................................... 64
   8.7 How to uninstall ESET Virtualization Security ............................................. 64
   8.8 How to access system logs ............................................ 64
   8.9 How to deploy vAgent Host with existing certificates ................................. 66
8.10 What client tasks can be executed regarding EVS and VAH

9. Troubleshooting

9.1 Where to find the logs for ESET Remote Administrator

9.2 Where to find the logs for ESET Virtualization Security

9.3 Where to find the logs for vAgent

9.4 What to send to Customer Care

9.5 What ports to enable for licensing

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

9.7 How to use the offline mirror tool to receive updates

9.8 Cannot register to VMware vShield

9.9 ESET Virtualization Security shows no connected/protected virtual machines

9.10 No accessibility on license servers

9.11 Path excluded from scanning

10. Glossary
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 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 Security Management Center (formerly ESET Remote Administrator) Web Console. This allows you to 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:

```
ESXi HOST 1

ERA

VAH

ESXi HOST 2

VM

VM

VM

EVS OVA

ERA Agent

ESXi HOST 3

VM

VM

VM

EVS OVA

ERA Agent
```

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 6.4 and higher
- 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 an on-access scanner and the administrator can initiate on-demand scans from ESET Remote Administrator.
1.2 Requirements

System requirements

- ESET Virtualization Security (EVS) version 1.7:
  - VMware vSphere 6.0/6.5+/6.7 (vCenter Single Sign-On, vSphere Client/Web Client, vCenter Server, vCenter Inventory Service)
  - VMware NSX Manager 6.3+/6.4+
  - VMware NSX-T is not supported
  - VMware Guest Introspection 6.2.4+/6.3+/6.4+

- EVS version 1.6:
  - 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+

- EVS common requirements:
  - ESET Remote Administrator (ERA) 6.5+ server or ESET Security Management Center (formerly ESET Remote Administrator) 7.0, 7.1, 7.2 server installed
  - Virtual Agent Host (VAH) deployed as VM; refer to the EVS and ERA and VAH compatibility table below.
  - 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

MySQL database and ODBC driver

VAH supports MySQL database version 5.5 - 5.7, and ODBC driver version 5.1. - 5.3.
Latest supported vSphere version

Since ESET Virtualization Security is not developed anymore, we do not support versions of vSphere higher than 6.7.

### EVS and VMware compatibility matrix

<table>
<thead>
<tr>
<th></th>
<th>EVS 1.5</th>
<th>EVS 1.6</th>
<th>EVS 1.7</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vSphere 5.5 U2+</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>VMware vSphere 6.0.x</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>VMware vSphere 6.5.x</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>VMware vSphere 6.7.x</td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>VMware NSX 6.2.x</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>VMware NSX 6.3.x</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>VMware NSX 6.4.x</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Windows VMs protection*</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Linux VMs protection**</td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
</tbody>
</table>

* [List of compatible Windows versions](#)
** [List of compatible Linux distributions](#)

### EVS and ERA and VAH compatibility

<table>
<thead>
<tr>
<th></th>
<th>ERA version</th>
<th>VAH version</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS 1.0</td>
<td>up to 6.5</td>
<td>up to 6.5</td>
</tr>
<tr>
<td>EVS 1.5</td>
<td>up to 6.5</td>
<td>up to 6.5</td>
</tr>
<tr>
<td>EVS 1.6</td>
<td>up to 7.2</td>
<td>up to 6.5</td>
</tr>
<tr>
<td>EVS 1.7</td>
<td>up to 7.2</td>
<td>up to 6.5</td>
</tr>
</tbody>
</table>

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

If you have already upgraded to VMware NSX, continue to Installation/Deployment.

Prerequisites
Before upgrading, verify the following applications are installed:

- VMware vSphere 5.5 U2+
- VMware vSphere 6.0+

To determine which vShield or vCNS is installed read the following article.

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+

Upgrade
To upgrade your existing VMware environment:

1. Unregister your current ESET solution
2. Upgrade vShield to NSX

2.1 Unregistration of current ESET solution

1. Unregister ESET Virtualization Security from vShield Manager.
   a. Open the ESET Virtualization Security console through vCenter.
   b. Enter the Management Mode.
   c. Choose vShield Registration.
   d. Enter username and password and select UNREGISTER.

   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 the 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

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
   b. Syslog server (if available)
   c. Locale
4. In the 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
   e. Confirm by clicking OK and proceed with the certificate. 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

Do not select the Modify plugin script download location checkbox unless necessary (for more information refer to https://pubs.vmware.com/NSX-62/topic/com.vmware.ICbase/PDF/nsx_62_install.pdf#38).
d. Click OK.
e. You should be able to see the **Connected - Last successful inventory update was on <date>** status.

VShield has been upgraded to NSX and is working properly.

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, verify 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 instructions provided by VMware
4. vAgent Host deployed
5. Registrate VAH to NSX
6. ESET Virtualization Security installed

**NSX Manager rights**

The administrator needs the following NSX Manager rights 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

Guest Introspection installs a new kernel module (VIB) and a service virtual machine on each host in the cluster. Guest Introspection is required to use ESET Virtualization Security.

**Install Guest Introspection according to instructions provided by VMware.**

**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 on how to install Guest Introspection for Linux click [here](#).

### 3.2 VMware Tools installation

**Install VMware Tools according to instructions provided by VMware.**

We recommend to install VMware Tools 10.0.9 or later. For more information on 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.

**Hostname and IP address**

Before deployment of the Virtual Agent Host you must contact your networking team to register the 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.
4. Review details and click Next.
5. Read and accept the End User License Agreement.
6. To complete installation, follow the instructions on screen and specify the following information about your virtual appliance:
   - **Select name and folder** – Specify a name for the deployed template and location where your 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 the following (fields not mentioned are optional):
   - Hostname – Hostname in FQDN format of your vAgent Host appliance (registered on DNS Server with networking team, as mentioned above).
   - Password – Will be used for your vAgent Host virtual machine, as well as, its CentOS root password.
   - ERA Server Hostname – Enter 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.

**vAgent Host and ERA Server/Proxy**

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:

- ERA Server Hostname – Enter the hostname or IP address of your ERA Server or ERA Proxy and the vAgentHost will connect to ERA Server.
- Webconsole Hostname – Enter the hostname or IP address of your Web Console and the vAgentHost will connect to the ERA Server.
- Webconsole username and password – Enter your credentials and the vAgent Host will connect to the ERA Server.
Static IP address

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.

8. Review the deployment summary and click **Finish**. The deployment process will automatically create a virtual machine with the settings you specified. This process can take several minutes depending on network performance.

Once the vAgent Host is successfully deployed, power it on. The basic information screen, shown below, gives an overview of protected machines. To configure settings, press **Enter**.
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.

<table>
<thead>
<tr>
<th>ESET Remote Administrator Virtual Agent Host Appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable/Disable Webmin interface</strong></td>
</tr>
<tr>
<td>Change VM password</td>
</tr>
<tr>
<td>Change database password</td>
</tr>
<tr>
<td>Register to VMware NSX Manager</td>
</tr>
<tr>
<td>Factory reset</td>
</tr>
<tr>
<td>Restart system</td>
</tr>
<tr>
<td>Shut down system</td>
</tr>
<tr>
<td>Lock screen</td>
</tr>
<tr>
<td>Exit to terminal</td>
</tr>
</tbody>
</table>

Enables or disables Webmin management interface running on port 10000.

**<UP>/<DOWN> Select item**  **<ENTER> Perform action**  **<ESC> Lock screen**
3.4 Register ESET to VMware NSX Manager

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

2. Select Register to VMware NSX Manager.
3. Enter your NSX Manager fully qualified domain name (FQDN) **hostname** and accept the certificate.

4. Enter your NSX Manager admin **username** and **password**. The Registration status will display: **not registered**.

5. Enter the **ESET_Security.ThreatFound** tag which will be used as default after finding malware on a VM.

To view tags for specific virtual machine, see **vCenter > Summary > Security Tags**.
6. Type `r` (register) and then press Enter.

7. Type `s` (status) and then recheck the registration status. If it is successful you will see the registered status.
8. Type `q` (quit) and then exit the ESET NSX Service Manager Console. 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, click **Networking & Security > Installation > Service Deployments** and then click to add new service deployment.
2. Select the check box next to ESET Virtualization Security and then click **Next**.
3. Select the applicable cluster(s) and then click **Next**. ESET Virtualization Security will be installed on all hosts in the cluster.
4. Select storage and assign a network for ESET Virtualization Security to use and click **Next**. DHCP IP assignment is selected by default. To assign a static IP addresses to EVS service appliances, in NSX Manager, click **Change an IP assignment > Use IP Pool**.

**Important**

This feature strictly requires that the whole infrastructure of virtualization security (ERA server, Virtual Agent host) hostnames during deployment were set to FQDN and are resolvable by configured DNS servers.

When creating IP pools make sure that selected IP addresses are available to be used. Check this on your DHCP server.
5. Select the radio button next to Use IP pool and then select the applicable IP pool below or create a new one.
We recommend you leave the DNS Suffix option empty.

6. 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.

Troubleshooting

When installation fails, click here.

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.

7. 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

To activate vAgent Host, follow the steps below:

2. Enter basic information about the task (such as, the Name, Description, Task Category (ESET Security Product) and type of task [Product activation]).
3. In Settings, select a license for the vAgent Host (same license as for ESET Virtualization Security). This license will be applied to the vAgent Host already deployed in your virtual environment. If you do not see any license, go to Licenses - add new license.
4. Review the configured settings summary and click Finish.
5. The Client Task is now created. At this time, we recommend you specify triggers and targets.

Internet connection required for activation.
3.7 Automatic activation of all ESET Virtualization Security appliances

Create dynamic groups in the ESET Remote Administrator (ERA) Web Console to verify all ESET Virtualization Security appliances in the cluster are activated.

**Create Dynamic Group 1**

Dynamic Group 1 will group all ESET Virtualization Security appliances together, making it easier to apply policies.

1. Log in to the ESET Remote Administrator (ERA) Web Console.
2. Click **Computers > Groups > All**.
3. Click the gear icon and select **New Dynamic Group**.
   a. **Basic**
      Enter a **Name** (e.g. Machine is EVS) and **Description** for the new Dynamic Group. Verify the parent group is set to All.
   b. **Template**
      Click **New**. Enter a **Name** and **Description** for the new template.
   c. **Expression**
      Click **Add rule**, expand **Computer**, select **Managed products mask** and then click **OK**. Click + and select **Other: Virtual Security Appliance** and then click **Finish** twice.

Create a policy for Dynamic Group 1 (Machine is EVS)

This policy will determine settings for every ESET Virtualization Security appliance in this group.
1. Click Admin > Policies > New policy.
2. Enter the name and select ESET Virtualization Security - Security Appliance from the Select product... drop-down menu in Settings section.
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 contain only ESET Virtualization Security appliances that are not activated.

1. Click Computers > Groups > Machine is EVS > click 🌅 > New Dynamic Group.
   a. 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 Machine is EVS.
   b. Template
      Create a new Dynamic Group Template by clicking New. Enter a name and description for the new template.
   c. 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).

Create an activation task for Dynamic Group 2 (EVS is not activated)
This task automatically activates any ESET Virtualization Security appliances with an IP address of Virtual Agent Host machine.
1. Click 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.

After successful activation of all ESET Virtualization Security machines, the EVS is not activated group will not contain any virtual machines.

3.8 Creating Security Group with policy

Create a Security Group that includes all VMs, and apply a Security Policy to it that uses ESET Virtualization Security service as a security solution.

1. In your vSphere Web Client, click Networking & Security > Service Composer and then click 🗂.
2. Enter a name (e.g. AV-group) and define the dynamic membership rules or include objects manually for this group.
3. Click Security Policies and click 🗂.
4. Enter a name (e.g. EVSA-protection) and then click Next.
5. To add Guest Introspection Services, click 🕵️. Enter a name (e.g. ESET), select the radio button next to Apply and then click OK.
6. Select **ESET Virtualization Security** from the **Service Name** drop-down menu. Next to **State**, select **Enabled**, and next to **Enforce**, select **Yes**. Click **Finish**.

![Image of Security Groups](image1)

8. To apply this policy to your group, click 📞.

![Image of Apply Policy](image2)

---

---

- Your virtual machines are now protected by ESET Virtualization Security. To check their status, click **Host and Clusters**, click ESET Virtualization Security, open the 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. To configure settings, press 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 antisyware 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
```
Use the arrow keys to select the applicable setting and press **Enter**:

- **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.
- **Perform appliance update** – Displays available system updates.
- **Reset ERA configuration** – Reverts settings to default configurations 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 ESET Virtualization Security software.
- **Shut down system** – Shuts down your system.
- **Lock screen** – Locks the console and returns to the basic information screen.

---

**Configure network**

ESET Virtualization Security requires initial network configuration. See available options below.

a) Select to use DHCP

b) Configure connection details manually

i. Enable IPv4:

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

ii. Enable IPv6 in addition to IPv4:

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

Basic

General

Processing threads – The number of processing threads used for parallel scans. By default it is set to “64” and it is recommended to keep this value to ensure optimal functionality. Lowering this value can have negative impact on scanning performance. (Value changes could be required during troubleshooting.)

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.

![ESET Virtualization Security - Protected VM policy settings](image)

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

**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** 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.

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.

### 4.2.2.3 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.

### 4.2.2.4 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.

**Basic**

**ThreatSense 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 in 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 an On-Demand Scan task, perform the following steps:

1. Click Admin > Client Tasks > New.
2. Enter a Name (e.g. "On-Demand Scan") for the task, and from the Task drop-down menu, select On-Demand Scan.
3. In Settings, from the Scan Profile drop-down menu, select In-Depth Scan. Select Scan with cleaning and Scan all targets.
4. Click Finish.
5. In the dialog box click Create trigger.
6. Enter the trigger description.
7. In Target section, click Add Group, select the checkbox next to the Infected VM group (the group you created above).
8. In Trigger section, select Joined Dynamic Group Trigger from the Trigger type drop-down menu.
9. Click Finish.
5.2 Automate On-Demand Scan after infection

To automatically run an On-Demand Scan when threat(s) are found on virtual machine(s):

1. Click **Computers > Groups > All > New Dynamic Group** and create a new dynamic group.
2. Enter a **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 click **OK**.
7. Select **has mask** from the drop-down menu and enter an asterisk (*) in the following field.

8. To confirm, click **Finish** twice.

This dynamic group will contain agent-less virtual machines where threats were found.

Create a client task according to the following steps:
1. Click Admin > Client Tasks > New.
2. Enter a Name (e.g. "On-Demand Scan") for the task, and from the Task drop-down menu, select On-Demand Scan.
3. In Settings, from the Scan Profile drop-down menu, select In-Depth Scan. Select Scan with cleaning and Scan all targets.
4. Click Finish.
5. In the dialog box click Create trigger.
6. Enter the trigger description.
7. In Target section, click Add Group, select the checkbox next to the Infected VM group (the group you created above).
8. In Trigger section, select Joined Dynamic Group Trigger from the Trigger type drop-down menu.
9. Click Finish.

5.3 Understanding of Security Tags and how ESET triggers them

Security tagging is a labeling mechanism in VMware Service Composer that can be used as to describe the state of a machine. 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 third-party services. For more information visit VMware NSX 6 Documentation Center.

By default, once ESET finds malware on any VM, a security tag is applied. You can use pre-defined security tags or define new tags during Registration to NSX.

An admin can enable or disable security tagging (under NSX Security Tagging) and choose from the following tagging options using an 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:
5.4 Automatically quarantine VM upon malware detection using NSX

In this use-case, once ESET Virtualization Security detects malware, it will automatically tag the infected VM (see Understanding of Security Tags and how ESET triggers them) and the VM will fall into Quarantine Security Group. This will block all network access to the infected VM until the machine is scanned and cleaned. Once the machine has been cleaned, the VM is moved to its previous Group and network access is reinstated.

Prerequisites

1. A valid Standard edition VMware NSX license or higher (not one included in vSphere license).
2. Deployed NSX Distributed Switch on your hosts.
3. Distributed Port Group as Network adapter on VMs.
4. NSX Components and Firewall must be installed and enabled on Cluster and Hosts in vCenter > Networking & Security > Installation > Host Preparation.

**Creation of Quarantine Security Group**

1. In vCenter, click Networking & Security > Service Composer > Security Groups.

2. Click New Security Group 🔄, name it Quarantine and click Next.

3. Under Define dynamic membership click Add, from Entity drop-down menu choose Security Tag and type a tag name you registered during Registration*.

4. Click Finish.

* To view all available tags, click Networking & Security > Networking & Security Inventory > NSX Managers > IP Address > Manage > Security Tags.

**Create a Quarantine Security Policy**

1. Click Security Policies > Create Security Policy 🏷️ and name it Block network access.

2. Click 3 Firewall Rules and click 🔄.

3. Next to Action, select Block.

4. For Source, choose Policy’s Security Groups.

5. For Destination, select Any.


7. Click OK.

8. Click 🔄.

9. Next to Action, select Block.

10. For Source, choose Any.

11. For Destination, select Policy’s Security Groups.

12. State Enabled.

13. Click OK.

14. Click OK.

15. Click Finish.
16. Verify the newly created policy is number one in the priority list. To adjust the order, click Manage Priority.

Assign a Quarantine Security Policy to the Quarantine Security Group

1. Select the appropriate Security Policy and click the Apply Security Policy icon.
2. Check Quarantine group and click OK.

To automatically start on-demand scan when malware is detected by real-time protection, refer to Automate On-Demand Scan after infection.
6. Updating ESET Virtualization Security

ESET Virtualization Security for VMware NSX consists of multiple components.

Virtual Agent Host Virtual Machine contains:

1. Virtual Agent Host, a component of ESET Security Management Center that virtualizes agent entities to allow management of agentless virtual machines. For more information refer to How vAgent Host works.

2. ESET NSX Service Manager, a component responsible for registration to VMware NSX Manager, and serves as a communication channel between the ESET Virtualization Security Appliances (EVSA) and VMware NSX Manager. VMware NSX Manager also contains EVSA OVF image.

To update EVSA (OVF) through the vCenter NSX plug-in, update the ESET NSX Service Manager first, which contains new image of EVSA. In some cases, to provide new functionality or compatibility, updating the Virtual Agent Host is necessary too.

6.1 Check for available updates

To check for available Virtual Agent Host VM and ESET NSX Service Manager updates:

1. Log in to ESET Remote Administrator (ERA), click ESET applications.

2. All application updates are visible in the Outdated applications section.

Alternatively:

1. Log in to ERA, click Computers and find your Virtual Agent Host machine. Names or versions of outdated entities will be highlighted yellow.

2. Select the applicable machine, click Details > Installed Applications. All outdated applications will be highlighted yellow.

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

1. Log in to ERA, click Computers and find your Virtual Agent Host machine. Names or versions of outdated entities will be highlighted yellow.

2. Select the applicable machine, click Details > Alerts. If updates available, you will see "Operating system is not up to date" alert.
6.2 Update vAgent Host

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

1. Click Virtual Agent Host VM > New Task.

2. Basic
   Enter Basic information about the task, such as the Name, Description and Task Type. The Task Type defines the settings and the behavior for the task.

3. In the Task drop-down menu, select Remote Administrator Components Upgrade.

   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.

4. 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.

5. 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 - Force a reboot of the client operating system, if installation requires it.

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

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

6.3 Update ESET NSX Service Manager

To update ESET NSX Service Manager:
1. Click Virtual Agent Host VM > New Task.
2. In the Task drop-down menu, select Software Install.
3. In the Settings section, accept the End User License Agreement and select the applicable ESET License.
4. Select Install package from repository and then click <CHOOSE PACKAGE>.
5. Select ESET NSX Service Manager and click OK.
6. Confirm everything by clicking on Finish.

6.4 Update ESET Virtualization Security Appliance - Secure Virtual Machine

When the ESET NSX Service Manager has been updated, a new upgrade button appears in the VMware NSX Manager > Installations section. To update the ESET Virtualization Security Appliance for a specific cluster, select the applicable cluster, click the upgrade icon, and then follow the on screen instructions.

6.5 Update Operating System on ESET Virtualization Security Appliance

To update Operating System using ESET Remote Administrator, please:
2. In the Task drop-down menu, select Operating System Update.
3. In the Settings section, accept the End User License Agreement.
4. Click Finish.
### 6.6 Ports

**ESET Remote Administrator**

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

**Virtual Agent Host VM**

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

**ESET Virtualization Security Appliance**

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Usage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2222</td>
<td>TCP</td>
<td>Call</td>
<td>Communication to ESET Remote Administrator</td>
</tr>
<tr>
<td>9880</td>
<td>TCP</td>
<td>Call</td>
<td>Communication to Virtual Agent Host</td>
</tr>
</tbody>
</table>
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.

**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 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.
- **Delete Object(s)** (deletes the object completely).

**NOTE:** **Restore Object(s)** and **Restore Object(s) and Exclude in Future** option is not available, because there is no API for that in VMware's Guest Introspection.

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.

**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.

**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.

**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 vAgent Host
- 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 then 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

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.

**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 structure 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.

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

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

- 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 Guest Introspection service (MUX) located on particular ESXi over random port from range 48651-48666 in internal "vmservice-vshield-pg" network. The charts below list all possible network communication ports used when ESET Remote Administrator and its components are installed in your infrastructure.

### ERA Server:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Usage</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>2222</td>
<td>ERA Server listening</td>
<td>Communication between ERA Agents and ERA Server</td>
</tr>
<tr>
<td>TCP</td>
<td>2223</td>
<td>ERA Server listening</td>
<td>Communication between ERA Web Console and ERA Server, used for Assisted installation</td>
</tr>
</tbody>
</table>

### ERA Web Console web server:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Usage</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>443</td>
<td>Listening</td>
<td>HTTP SSL Web Console call</td>
</tr>
</tbody>
</table>

### ERA Proxy:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Usage</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>2222</td>
<td>Listening</td>
<td>Communication between ERA Agents and ERA Proxy</td>
</tr>
</tbody>
</table>

### HTTP Proxy:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Usage</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>3128</td>
<td>Listening</td>
<td>HTTP Proxy (update caching)</td>
</tr>
</tbody>
</table>

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

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

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

**NOTE**
For more about ports see [ESET Knowledgebase article](ESET Knowledgebase article).
8.5 How to collect logs

ESET Virtualization Security consists of 3 components: Virtual Agent Host (VAH), ESET Virtualization Security Appliance, ESET Remote Administrator. The logs of each component must be retrieved to troubleshoot any issue.

To ensure logs contain all essential data required to identify the cause of a problem: enable trace logging for Virtual Agent Host and ESET Remote Administrator server and enable access to system logs for ESET Virtualization Security.

Logs can be collected using the diagnostic tool or manually.

Collect logs using the diagnostic tool

The diagnostic tool is part of all ERA components. Run the diagnostic tool to collect logs from ERA and VAH, select a root folder where the logs will be saved, and then select one of following actions below:

- **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.

**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.

Location of the Diagnostic Tool:

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

**LINUX** - Server path /opt/eset/RemoteAdministrator/<product>/, there is a Diagnostic<product> executable (one word, for example, DiagnosticServer, DiagnosticAgent)

The <product> can represent Server or Agent in case of ESET Remote Administrator server machine, or it can be Agent or VAgentHost in case of VAH Appliance.

Manually collect logs from VAH

Necessary log files from VAH can be found at the following locations:

/var/opt/eset/RemoteAdministrator/VAgentHost/MultiAgent - Contains logs for each protected virtual machine (directory is represented by UUID).

/var/opt/eset/RemoteAdministrator/VAgentHost/Dumps - Contains crashdumps that have not been sent to the ESET CrashReporting service yet.

/var/log/eset/RemoteAdministrator/VAgentHost - Contains the tracelog of VAgentHost.

/var/log/eset/RemoteAdministrator/VAgentHost/Proxy - Contains the tracelog of VAgentHost’s MultiProxy component.

/var/log/eset/RemoteAdministrator/vahinstaller.log - Contains installation logs
**VAH Database dump**

Sometimes a copy of VAH database might be needed for troubleshooting purposes. To create a database dump, run the following command in the VAH appliance:

```bash
mysqldump -u root -p era_vah_db > /tmp/vah_db_export.sql
```

Where `/tmp/vah_db_export.sql` is the desired path and filename of database dump.

See how to [access system logs of ESET Virtualization Security](#).

### 8.5.1 Enable trace logging

To ensure logs contain all data essential to identify the cause of occurred issues, enable Trace logging for both Virtual Agent Host and ESET Remote Administrator (ERA) Server.

#### Enable trace logging for Virtual Agent Host (VAH) through ERA Web Console

1. In the ERA Web Console, navigate to Admin → Policies → New Policy.
2. Select ESET Remote Administrator Virtual Agent Host, in General tab select Trace from Trace log verbosity list box.
3. Configure the policy and assign it to the Virtual agent host (VAH).
4. Click Finish, wait till the policy is replicated to VAH (depends on replication time configured in ERA agent).

#### Enable trace logging for Virtual Agent Host (VAH) through VAH appliance console or SSH access

Run the commands listed below in VAH appliance console or via SSH access.

   ```bash
echo all > /etc/opt/eset/RemoteAdministrator/VAgentHost/loggerLevel.cfg
```
2. Restart VAH service.
   ```bash
   systemctl restart eravagenthost
   ```
3. Check VAH service status.
   ```bash
   systemctl status eravagenthost
   ```

#### Enable trace logging for ERA Server

1. In the ERA Web Console, navigate to Admin → Server Settings → Advanced Settings.
2. In the Logging section, select Trace from Trace log verbosity.
3. Click Save.
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

**SFTP access to system logs**

For security reasons, we recommend you disable SFTP access to system logs after you have sent logs to ESET Customer Care. If some log files could not be downloaded, re-enabling this feature could resolve it.

1. Enter Management mode, select **Access system logs** and then select **Enable SFTP access to the system logs**. Enter your SFTP username and password and select **Apply**.
2. Run your SFTP client (we recommend using the free WinSCP SFTP client).
3. Enter the Hostname you find in ESET Virtualization Security in management mode > Configure network.
4. Default SFTP port is 22. In the User name field, enter logs. At this time, you have the ability to Save the configuration or login.
5. When you are prompted for a password, enter the password you used in ESET Virtualization Security.
6. Now, you can access ESET Virtualization Security logs.

In order to provide troubleshooting assistance as quickly and accurate as possible, ESET Customer Care requires the following files to be sent:

- 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

Complete the following steps to deploy vAgent Host and ESET Virtualization Security and to use existing certificates:

- Deploy vAgent Host and ESET Virtualization Security in a standard way
- Import existing certificates via ERA policy

Import existing certificates via ERA policy

1. Navigate to Admin > Policies > New Policy. Type a name for the policy.
2. Expand Settings, select product ESET Virtual Agent Host.
3. Expand General, next to HTTPS certificate, click Change certificate.
4. Select Remote Administrator certificate (or "Security Management Center certificate"), click Open certificate list and choose Proxy certificate.
5. Click OK.
6. Click Finish.
8.10 What client tasks can be executed regarding EVS and VAH

List of supported client tasks that can be executed in ESET Remote Administrator regarding ESET Virtualization Security (EVS) and vAgentHost (VAH).

**EVS**
- Display Message - shows up as a broadcast message, however, might break the design of console
- Export Managed Product Configuration
- Module Update
- Module Update Rollback
- Operating System Update
- Product activation
- Remote Administrator Components Upgrade
- Set Policy (configuration)
- Shutdown Computer
- Upload Quarantined File

> When uploading quarantined files to a shared disk accessed via SAMBA protocol that you specified in ESET Remote Administrator, ESET Virtualization Security mounts the disk using ntlm security mode. Make sure it is enabled for your SAMBA share.

- Update detection engine

**VAH**
- Export configuration
- Operating system update
- Product activation - silent seat
- Product update
- Remote Administrator Components Upgrade - upgrades both VAH and ERA agent
- Reboot
- Shutdown Computer
- Software install
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 at the following paths:

Windows
C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs

Linux
/var/eset/RemoteAdministrator/<product>/
while <product> can represent Server or Agent.

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
Windows environment: C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs
Linux environment: /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.

**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.

**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.

**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.

---

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

The parameter --offlineLicenseFilename is mandatory. You must specify a path to your offline license file (as mentioned above).

To create a mirror, run the MirrorTool with at least the minimal required parameters. Here is an example:

- Linux:
  ```
sudo ./MirrorTool --mirrorType regular --intermediateUpdateDirectory /tmp/mirrorTool/mirrorTemp --offlineLicenseFilename /tmp/mirrorTool/offline.lf --outputDirectory /tmp/mirrorTool/mirror
  ```

Mirror tool and Update settings:

- To automate the distribution of virus database updates, you can create a schedule to run the Mirror tool. To do so, open ERA Web Console and navigate to Client Tasks > Operating System > Run Command. Select Command line to run (including a path to the MirrorTool.exe) and set a reasonable trigger (such as CRON for every hour 0 0 * * * ? *). 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 to test connectivity.

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

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

ESET Security Management Center (ESMC) (formerly ESET Remote Administrator (ERA))
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.

Guest Introspection
Guest Introspection is a service from NSX Manager to offload security functions to ESET security solution.

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).

NSX Manager
The NSX Manager is the centralized management component of NSX and runs as a virtual appliance on an ESXi host.

Virtual Agent host (VAH)
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.

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

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.

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.

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).