

		IOC Rules Upgrade	<a href="https://intelligence.sangfor.com.cn">https://intelligence.sangfor.com.cn</a>
		Patches, signature, and antivirus database	<a href="http://download.sangfor.comhttps://download.sangfor.com">http://download.sangfor.comhttps://download.sangfor.com</a>

Table 2: Network connectivity requirements

## 2.1.4 Trusted File Whitelisting

To prevent false error reports during virus scans and removal, you need to collect and whitelist trusted files in advance. Whitelisted files include customer-developed virus-free service software or files that have been whitelisted for other antivirus products. After the Manager is installed and activated, log in to the Manager, choose **Endpoints > Security Protection > Trusted Files**, and add files to the whitelist. Whitelisted files are skipped during virus scans and removal.

## 2.2 Manager Installation

The Manager functions in both the software and hardware modes. The following describes how to install the Manager software and hardware.

### 2.2.1 Manager Software Installation

The Manager software can be installed in either of the following modes:

1. OVA image mode is used in virtualization scenarios, such as when VMware or HCI is used.
2. ISO image mode: is used in virtualization scenarios or scenarios where physical servers are used.

#### 2.2.1.1 Installation Package Downloading

To download related component packages, visit <https://community.sangfor.com> and choose **Self-Service > Software Download > Endpoint**.



Download the OVA template of the ES3.7.12EN official version for installation in OVA image mode.

Download the ISO template of the ES3.7.12EN official version for installation in ISO image mode.

Download the installation and update package of the ES3.7.12EN official version for update.

Offline agent installer can download at: <https://community.sangfor.com> (Path: **Self Services > Download > Endpoint**)

## 2.2.1.2 Installation in OVA Image Mode



The following describes installing the Manager software in OVA image mode on the HCI. Refer to the following procedure for installation on other virtualization platforms.

**Step 1.** Import the OVA template.

Import the OVA template from the local environment, as shown in the following figure.

**Import Virtual Machine File**

❗ QXL graphics adapter will be used by default after VM is imported. If display issue occurs after startup, change the graphics adapter manually.

File Type: OVA or VMA

To use a vhd, vhdx or qcow2 image file, choose Existing disk and then select that image file when configuring disk for virtual machine.

VM Image Files: ova or vma file

Group: Default Group

HA: ☒ Migrate to another node if the node fails HA Settings ⓘ

Datastore: VirtualDatastore1

Storage Policy: 2\_replica

Run Location: <Auto>

OS: Default ⓘ

**Import**

**Step 2.** Configure the network.

You can configure the network on the web portal in the 3.2.22EN or a later version (full installation).

---

## 1. Log in to the Manager.

Configure the PC IP address in the same network segment as the management port of the Manager. Open the browser, enter the default Manager address **https://10.251.251.251** in the address box, and press **Enter**. Log in to the Manager. The default user name and password are **admin** and **admin**, respectively.



The default IP address of the Manager management port is 10.251.251.251/24. Internet Explorer 11 or later, Firefox, and Google Chrome are supported.

---

## 2. Configure the Manager's IP address.

Choose **System > System > Network**, click the **Interfaces** tab, and set **IP Address**, as shown in the following figure.

Interfaces				
<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Disable <input type="button" value="Refresh"/>				
No.	Interface	Description	IP Address	Status
<input type="checkbox"/> 1	eth0		10.251.251.251	Up ✓

## 3. Configure DNS addresses.

Choose **System > System > Network**, click the **Advanced** tab, and set **Preferred DNS** and **Alternate DNS**, as shown in the following figure.



The DNS addresses must be configured because domain names need to be parsed when the Manager updates the antivirus database.

---

The screenshot shows the 'Advanced' configuration tab in the Sangfor Endpoint Secure interface. It contains three main sections:

- SSH Service:** A checkbox labeled 'Enable' is checked. Below it is a 'Port' input field.
- DNS Server:** Two input fields are present: 'Preferred DNS' and 'Alternate DNS'.
- Ports:** Two input fields are present: 'Manager Access Port' and 'Agent Update Port'.

#### 4. Configure routes.

Choose **System** > **System** > **Network**, click the **Routing** tab, and configure routes, as shown in the following figure.



Routes must be configured for the Manager to connect to and communicate with endpoints.

The screenshot shows the 'Routing' configuration tab. At the top, there are buttons for '+ New', 'X Delete', and 'Refresh'. Below is a table with the following columns: 'No.', 'Dst IP', 'Netmask', 'Next-Hop IP', and 'Operation'.

#### Step 3. Verify that the Manager installation is successful.

Log in to the Manager (default address: <https://10.251.251.251>, default user name and password: **admin** and **admin**) and check whether the version number on the home page is correct, as shown in the following figure. If the version number is correct, the installation is successful.



## 2.2.1.3 Installation in ISO Image Mode

#### Step 1. Prepare for the installation.