FortiSandbox VM - Install Guide for VMware

Version 3.1.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

June 18, 2019
FortiSandbox VM 3.1.0 Install Guide for VMware
34-300-495252-20190618

TABLE OF CONTENTS

Change Log

Date	Change Description
2019-06-18	Initial release.
2019-08-30	Updated Windows VM package install section with new download link and instructions.

About FortiSandbox VM on VMware

FortiSandbox VM is a 64-bit virtual appliance version of FortiSandbox. It is deployed in a virtual machine environment. Once the virtual appliance is deployed and set up, you can manage FortiSandbox VM via its GUI in a web browser on your management computer.

This document provides information about deploying a FortiSandbox VM in VMware VSphere Hypervisor (ESX/ESCi) and VMware vShpere Client environments.

This includes how to configure the virtual hardware settings of the virtual appliance. This guide presumes that the reader has a thorough understanding of virtualization servers.

This document does not cover configuration and operation of the virtual appliance after it has been successfully installed and started. For that information, see the *FortiSandbox Administration Guide* in the Fortinet Document Library.

Licensing

Fortinet offers the FortiSandbox VM in a stackable license model. This model allows you to expand your VM solution as your environment expands. For information on purchasing a FortiSandbox VM license, contact your Fortinet Authorized Reseller, or visit https://www.fortinet.com/how_to_buy/.

When configuring your FortiSandbox VM, ensure to configure hardware settings as outlined in the following table and consider future expansion. Contact your Fortinet Authorized Reseller for more information.

Technical Specification	Details
Hypervisor Support	VMware ESXi version 5.1, 5.5, or 6.0 and later Citrix XenServer 6.5 and later Kernel Virtual Machine (KVM)
HA Support	FortiSandbox 2.1.0 and later
Virtual CPUs (min / max)	4 / Unlimited*
Virtual Network Interfaces	6
Virtual Memory (min / max)	8GB / Unlimited**
Virtual Storage (min / max)	200GB / 16TB***

* Fortinet recommends that the number of virtual CPUs is four plus the number of Windows VMs.

** Fortinet recommends that the size of virtual memory is 8GB plus 3 GB for every Windows VM clone.

*** Fortinet recommends that the size of virtual storage is 1TB for production environment.

For more information, see the FortiSandbox product data sheet available on the Fortinet web site, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf.

After placing an order for FortiSandbox VM, a license registration code is sent to the email address used in the order form. Use the license registration code provided to register the FortiSandbox VM with Customer Service & Support at https://support.fortinet.com.

Upon registration, you can download the license file. You will need this file to activate your FortiSandbox VM. You can configure basic network settings from the CLI to complete the deployment. Once the license file is uploaded and validated, the CLI and GUI will be fully functional.

FSA-VM and FSA-VM00

The VM model available to order is FSA-VM00, which replaces previous FSA-VM model.

For previous FSA-VM models, its base license contains four Windows license keys to activate four different Windows VM in the base VM package. Users can purchase 50 more Windows license keys to allow the unit to run at most 54 Windows clones.

The serial number of FSA-VM model starts with *FSA-VM*. Starting from Q3, 2017, the licenses for this model are no longer available for purchase. However, user can still upgrade the existing installations with new firmware releases.

For the new FSA-VM00 models, the base license does not contain a Windows license key. Users can purchase the needed Windows license keys to activate enabled Windows VMs. For example, if the user only wants to use Window 8 VMs, the user can purchase Windows 8 license keys. The maximum allowed Windows clones for FSA-VM00 model is eight. The serial number for FSA-VM00 models starts with *FSAVM0*.

Preparing for deployment

You can prepare for deployment by reviewing the following information:

Minimum system requirements

Prior to deploying the FortiSandbox VM virtual appliance, VMware vSphere Hypervisor (ESXi version 5.1, 5.5, 5.0, and later) must be installed and configured.

The installation instructions for FortiSandbox VM assume you are familiar with your VM server and terminology.

Upgrade to the latest, stable update and patch release for your virtual environment.

FortiSandbox VM has specific CPU requirements: Intel Virtualization Technology (VT-x/EPT) or AMD Virtualization (AMD-V/RVI).
Enter the BIOS to enable Virtualization Technology and 64-bit support.
Detailed information can be found at https://communities.vmware.com/docs/DOC-8970.

Ensure the following prerequisites are met before installing FortiSandbox VM:

- The VMware vSphere ESXi Hypervisor software must be installed and configured.
  - ESXi version 5.1: Hardware version 9
  - ESXi version 5.5: Hardware version 9 or 10
  - ESXi version 6.0: Hardware version 9, 10, or 11
- The VMware vSphere client is installed on the management computer.

Registering your FortiSandbox VM

To obtain the FortiSandbox VM license file you must first register your FortiSandbox VM with Fortinet Customer Service & Support.

To register your FortiSandbox VM:

1. Log in to the Fortinet Customer Service & Support portal using an existing support account or select *Create an Account* to create a new account.
2. In the toolbar select *Asset* > *Register/Renew*. The *Registration Wizard* opens.
3. Enter the registration code from the FortiSandbox VM License Certificate that was emailed to you, then select *Next*. The *Registration Info* page is displayed.
4. Enter your support contract number, product description, Fortinet Partner, and IP address in the requisite fields, then select *Next*.

As a part of the license validation process FortiSandbox VM compares its IP address with the IP information in the license file. If a new license has been imported or the FortiSandbox VM's IP address has been changed, the FortiSandbox VM must be rebooted in order for the system to validate the change and operate with a valid license.

The Customer Service & Support portal currently does not support IPv6 for FortiSandbox VM license validation. You must specify an IPv4 address in both the support portal and the port management interface.

5. On the *Fortinet Product Registration Agreement* page, select the checkbox to indicate that you have read, understood, and accepted the service contract, then select *Next* to continue to the *Verification* page.
6. The verification page displays the product entitlement. Select the checkbox to indicate that you accept the terms then select *Confirm* to submit the request.
7. From the *Registration Completed* page you can download the FortiSandbox VM license file, select *Register More* to register another FortiSandbox VM, or select *Finish* to complete the registration process.
   Select *License File Download* to save the license file (`.lic`) to your management computer. See Uploading the license file on page 17 for instructions on uploading the license file to your FortiSandbox VM via the GUI.

Editing FortiSandbox VM IP addresses

To edit the FortiSandbox VM IP address:

1. In the toolbar select *Asset* > *Manage/View Products* to open the *View Products* page.
2. Select the FortiSandbox VM serial number to open the *Product Details* page.
3. Select *Edit* to change the description, partner information, and IP address of your FortiSandbox VM from the *Edit Product Info* page.

4. Enter the new IP address then select *Save*.

You can change the IP address five (5) times on a regular FortiSandbox VM license. There is no restriction on a full evaluation license.

5. Select *License File Download* to save the license file (`.lic`) to your management computer. See Uploading the license file on page 17 for instructions on uploading the license file to your FortiSandbox VM via the GUI.

Deployment package for VMware

FortiSandbox VM deployment packages are included with firmware images on the Customer Service & Support site.

- FSA_VM-v2xx-build0xxx-FORTINET.out: Download this firmware image to upgrade your existing FortiSandbox VM installation.
- FSA_VM-v2xx-build0xxx-FORTINET.out.ovf.zip: Download this package for a new FortiSandbox VM installation on ESXi server.

The `.out.ovf.zip` file contains:

- `fsa.vmdk`: The FortiSandbox VM system hard disk in Virtual Machine Disk (VMDK) format.
- `FortiSandbox-VM.ovf`: The VMware virtual hardware configuration file.
- `DATADRIVE.vmdk`: The FortiSandbox VM log disk in VMDK format

Downloading deployment packages

Firmware images FTP directories are organized by firmware version, major release, and patch release. The firmware images in the directories follow a specific naming convention and each firmware image is specific to the device model.

You can download the *FortiSandbox Release Notes* and FortiSandbox and Fortinet core MIB files from this directory.

Download the `.out` file to upgrade your existing FortiSandbox VM installation.

To download the firmware package:

1. Log in to the Fortinet Customer Service & Support portal then, from the toolbar, select *Download* > *Firmware Images*. The *Firmware Images* page opens.
2. Select *FortiSandbox* from the *Select Product* drop-down list, then select *Download*.
3. Browse to the appropriate directory for the version that you would like to download.
4. Download the appropriate firmware image and release notes to your management computer.
5. Extract the contents of the package to a new folder on you management computer.

Deployment

Prior to deploying the FortiSandbox VM, the VM platform must be installed and configured so that it is ready to create virtual machines. The installation instructions for FortiSandbox VM presume that you are familiar with the management software and terminology of your VM platform.

You might also need to refer to the documentation provided with your VM server. The deployment information in this guide is provided as an example because, for any particular VM server, there are multiple ways of creating a virtual machine - command line tools, APIs, alternative graphical user interface tools.

Before you start your FortiSandbox VM appliance for the first time, you might need to adjust virtual disk sizes, networking settings, and CPU configuration. The first time you start FortiSandbox VM, you will have access only through the console window of your VM server environment. After you configure one network interface with an IP address and administrative access, you can access the FortiSandbox VM GUI (see Enabling GUI access on page 16).

Deploying FortiSandbox VM on VMware

Once you have downloaded the `FSA_VM-v210-build0xxx-FORTINET.out.ovf.zip` file and extracted the package contents to a folder on your management computer, you can deploy the OVF package to your VMware environment.

Prior to deploying the FortiSandbox VM, ensure that the following are configured and functioning properly:

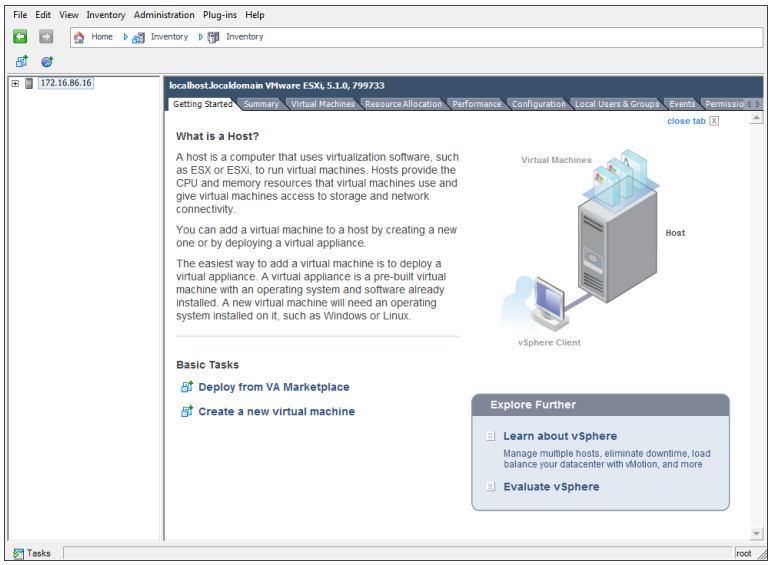
- VMware vSphere Hypervisor™ (ESX/ESXi) software must be installed on a server prior to installing FortiSandbox VM. Go to https://www.vmware.com/products/vsphere-hypervisor/index.html for installation details.
- VMware vSphere Client™ must be installed on the computer that you will be using for managing the FortiSandbox VM.

The following topics are included in this section:

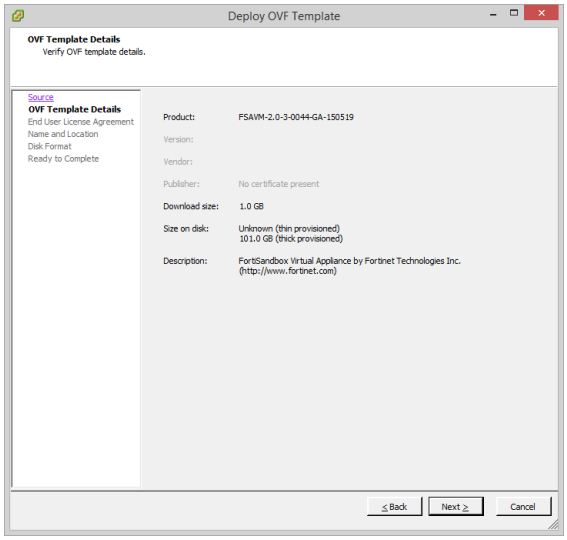
Deploying the OVF file

To deploy the OVF file template:

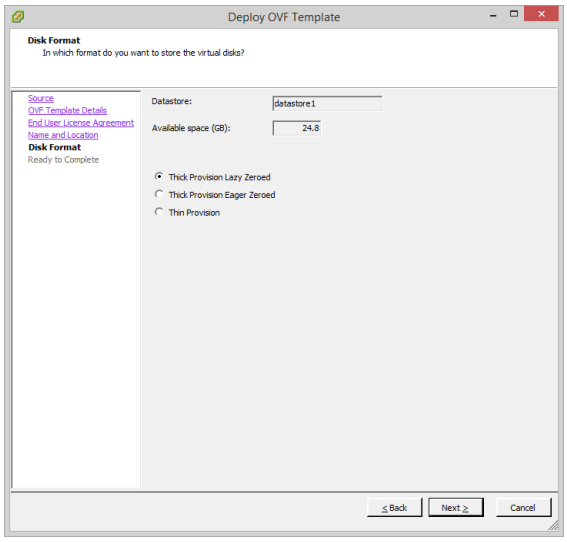
1. Launch the VMware vSphere client, enter the IP address or host name of your server, enter your user name and password, then select *Login*. The vSphere client home page opens.



2. Select *File* > *Deploy OVF Template* to launch the OVF Template wizard. The OVF Template *Source* page opens.
3. Select *Browse*, locate the OVF file on your computer, then select *Next* to continue. The OVF Template *Details* page opens.



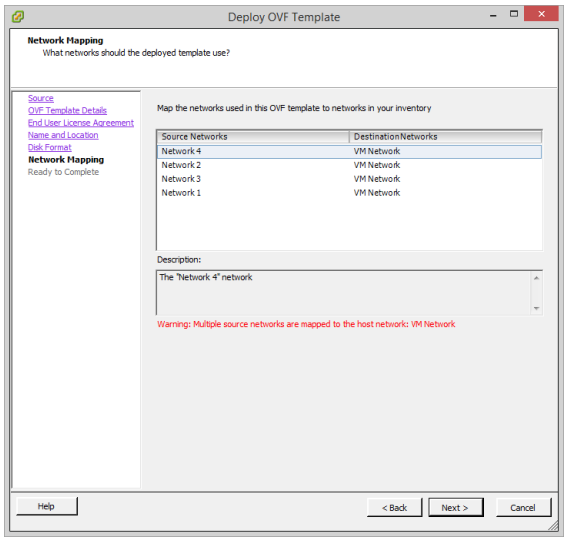
4. Verify the OVF template details. This page details the product name, download size, size on disk, and description. Select *Next* to continue. The OVF Template *End User License Agreement* page opens.
5. Read the end user license agreement, then select *Accept* then *Next* to continue. The OVF Template *Name and Location* page opens.
6. Enter a name for this OVF template. The name can contain up to 80 characters and it must be unique within the inventory folder. Select *Next* to continue. The OVF Template *Disk Format* page opens.



7. Select one of the following:
   - *Thick Provision Lazy Zeroed*: Allocates the disk space statically (no other volumes can take the space), but does not write zeros to the blocks until the first write takes place to that block during runtime (which includes a full disk format).
   - *Thick Provision Eager Zeroed*: Allocates the disk space statically (no other volumes can take the space), and writes zeros to all the blocks.
   - *Thin Provision*: Allocates the disk space only when a write occurs to a block, but the total volume size is reported by the Virtual Machine File System (VMFS) to the OS. Other volumes can take the remaining space. This allows you to float space between your servers, and expand your storage when your size monitoring indicates there is a problem. Note that once a Thin Provisioned block is allocated, it remains in the volume regardless of if you have deleted data, etc.

If you know your environment will expand in the future, it is recommended to add hard disks larger than the 200GB FortiSandbox VM base license requirement and utilize Thin Provision when setting the OVF Template disk format. This will allow your environment to be expanded as required while not taking up more space in the SAN than is needed.

8. Select *Next* to continue. The OVF Template *Network Mapping* page opens.



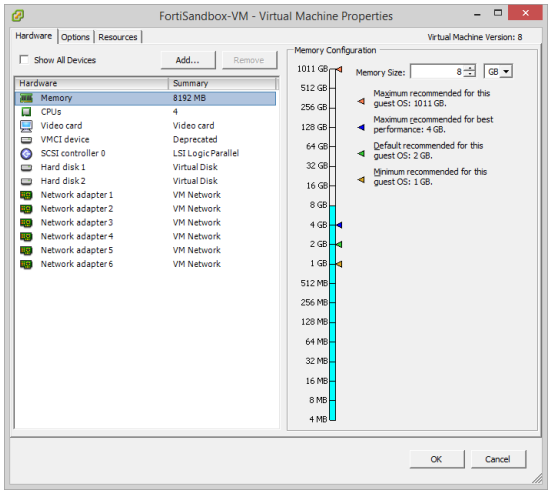
9. Map the networks used in this OVF template to networks in your inventory. Network 1 maps to port1 of the FortiSandbox VM. You must set the destination network for this entry to access the device console. Select *Next* to continue. The OVF Template *Ready to Complete* page opens.
10. Review the template configuration.
    Ensure that *Power on after deployment* is not enabled. You need to configure the FortiSandbox VM hardware settings prior to powering on the VM.
11. Select *Finish* to deploy the OVF template. You will receive a *Deployment Completed Successfully* dialog box once the FortiSandbox VM OVF template wizard has finished.

Configuring hardware settings

Before powering on your FortiSandbox VM you must configure the virtual memory, virtual CPU, and virtual disk.

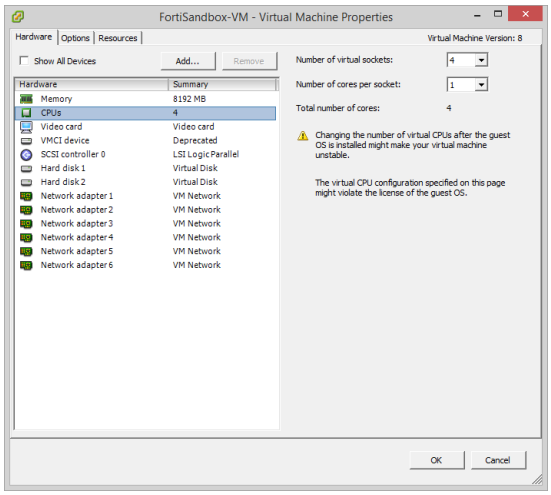
To configure the VM:

1. In the vSphere Client, right-click on the FortiSandbox VM in the left pane and select Edit Settings to open the *Virtual Machine Properties* window.
2. Select *Memory* from the *Hardware* list, then adjust the *Memory Size* as required. 3GB of RAM per Windows VM is recommended.

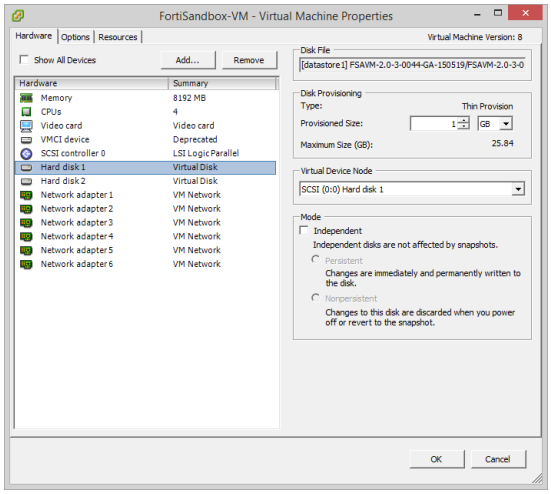


3. Select *CPUs* from the *Hardware* list, then adjust the *Number of virtual sockets* and *Number of cores per socket* as required.

If you need to change the vCPUs after the initial boot, power off FortiSandbox VM. Fortinet recommends that the number of vCPUs be four more than the number of Windows VMs.



4. Select *Hard disk 2*, the data disk, from the *Hardware* list, and configure it as required. Fortinet recommends making the virtual disk 1TB or larger. *Hard disk 1* should not be edited.



5. Select a network adapter from the *Hardware* list, then adjust the virtual network mapping as required by your network configuration. To use sniffer mode promiscuous mode must be enable on a port, see Sniffer mode.

By default, six bridging virtual network adapters are created and automatically mapped to a port group on a virtual switch (vSwitch) in the virtual server. Each of the network adapters can be used by one of the six network interfaces in the FortiSandbox VM. The default mappings are appropriate when each of the host's guest virtual machines have their own IP address on your network.

6. Select *OK* to apply your changes.

Sniffer mode

To use sniffer mode, promiscuous mode must be enable on a port of your VMware server.

To enable promiscuous mode:

1. In the vSphere client, select your VMware server in the left pane, then select the *Configuration* tab in the right pane.
2. In the *Hardware* list, select *Networking*.
3. Select *Properties* for the switch, such as *vSwitch0*. The properties window opens.
4. In the *Ports* tab, select *vSwitch*, then select *Edit*. to open the switch properties window.
5. Select the *Security* tab.
6. In the *Promiscuous Mode* drop-down list select *Accept*, then select *OK*, and then *Close*.
7. Repeat the process for any further switches.

Powering on the virtual machine

You can now proceed to power on your FortiSandbox VM.

- Select the FortiSandbox VM in the left pane and select *Power on the virtual machine* in the *Getting Started* tab.
- Select the VM in the left pane, then select *Power On* in the toolbar.
- Right-click the VM in the left pane, then select *Power* > *Power On* from the right-click menu.

Configuring initial settings

Before you can connect to the FortiSandbox VM you must configure basic configuration via the CLI console. Once configured, you can connect to the FortiSandbox VM GUI and upload the FortiSandbox VM license file that you downloaded from the Customer Service & Support portal.

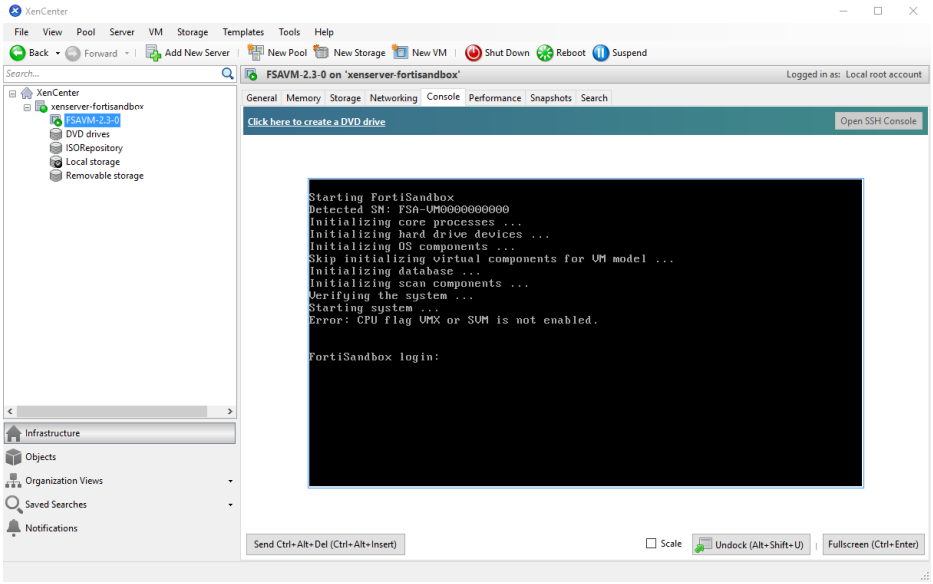
The following topics are included in this section:

Enabling GUI access

To enable GUI access to the FortiSandbox VM you must configure the port1 IP address and network mask of the FortiSandbox VM.

To configure the port1 IP address and netmask:

1. In your hypervisor manager, start the FortiSandbox VM and access the console window. You might need to press *Enter* to see the login prompt.



2. At the FortiSandbox VM login prompt, enter the username *admin*, then press *Enter*. By default, there is no password.
3. Using CLI commands, configure the port1 IP address and netmask with the following command:
   `set port1-ip <ip address>/<netmask>`
4. Configure the static route for the default gateway with the following command:
   `set default-gw <default gateway>`

The Customer Service & Support portal does not currently support IPv6 for FortiSandbox VM license validation. You must specify an IPv4 address in both the support portal and the port management interface.

Connecting to the GUI

Once you have configured the port1 IP address and network mask, launch a web browser and enter the IP address you configured for the port management interface. By default the GUI is accessible via HTTPS. At the login page, enter the user name `admin` and no password, then select *Login*.

Uploading the license file

Before using the FortiSandbox VM you must enter the license file that you downloaded from the Customer Service & Support portal upon registration.

To upload the license file:

1. Log in to the FortiSandbox VM GUI and find the *System Information* widget on the dashboard.
2. In the *VM License* field, select `Upload License`. The *VM License Upload* page opens.
3. Select *Browse*, locate the VM license file (`.lic`) on your computer, then select *OK* to upload the license file.
   A reboot message will be shown, then the FortiSandbox VM system will reboot and load the license file.

4. Refresh your browser and log back in to the FortiSandbox VM(username *admin*, no password).
The VM registration status appears as valid in the *System Information* widget once the license has been validated.

As a part of the license validation process FortiSandbox VM compares its IP address with the IP information in the license file. If a new license has been imported or the FortiSandbox's IP address has been changed, the FortiSandbox VM must be rebooted in order for the system to validate the change and operate with a valid license.

If the IP address in the license file and the IP address configured in the FortiSandbox VM do not match, you will receive an error message when you log back into the VM.
If this occurs, you will need to change the IP address in the Customer Service & Support portal to match the management IP and re-download the license file. To change the management IP address, see Editing FortiSandbox VM IP addresses on page 8

Installing the Windows VM package

To complete the installation, the Microsoft Windows VM package must be downloaded and installed either manually or automatically, and then activated.

To manually download and install the package:

1. **For FSA-VM model:**
The base package can be downloaded from ftp://fsavm.fortinet.net/general/image/2.0.0/2015022118_vm.pkg.7z
The following Windows VM are contained in the package:
   - WINXPVM (Windows XP with Microsoft Office installed, 32 bit)
   - WINXPVM1 (Windows XP, 32 bit)
   - WIN7X86VM (Windows 7 with Microsoft Office installed, 32 bit)
   - WIN7X64VM (Windows 7, 64 bit)

   The base license file contains Windows license keys and Microsoft Office key to activate them. Users can also purchase, download and install extra Android, Windows 8.1 and Windows 10 image packages. These packages can be downloaded from:
   - **Android**: Download the package from ftp://fsavm.fortinet.net/images/v2.00/AndroidVM.pkg.7z
   - **Windows 8.1**: Download the package from ftp://fsavm.fortinet.net/images/v2.00/WIN81VM.pkg.7z
   - **Windows 10**: Download the package from ftp://fsavm.fortinet.net/images/v2.00/WIN10VM.pkg.7z

   For FSA-VM00 model:

   The base package is optional but recommended to install because you can use Windows Cloud VM, or use FSA-VM00 unit to work as Master and Primary Slave, which doesn't participate in job scans. If you plan to use the unit to do scans, you can choose to install the necessary VM. See To automatically download and install the package: on page 19 for more detailed information. The default base package can be downloaded from ftp://fsavm.fortinet.net/images/v3.00/VM00_base.pkg

   The following VMs are contained in the package:
   - WIN7X86VMO16 (Windows 7 with Microsoft Office installed, 32 bit)
   - WIN81X64VM (Windows 8.1, 64 bit)
   - WIN10X64VM (Windows 10, 64 bit)

   MD5 File:

   Download the md5 value of images from ftp://fsavm.fortinet.net/images/v2.00/md5.txt

Downloading the Windows VM package with a web browser is not recommended due to the size of the file. An FTP client that supports resume download is recommended.

2. Put the package on a host that supports file copy with the SCP or FTP command. The FortiSandbox must be able to access the SCP or FTP server.
3. In a console window, enter the following command string to download and install the package:
   ```
   fw-upgrade -v --s<SCP/FTP server IP address> -u<user name> -p<password> -t<ftp|scp> -f<file path>
   ```
   Windows Sandbox VMs must be activated against the Microsoft activation server. This is done automatically after a system reboot. To make sure the activation is successful, port3 of the system must be able to access Internet, and the DNS server should be available to resolve the Microsoft activation servers.

To automatically download and install the package:

FortiSandbox can automatically check for and download new Microsoft Windows VM packages. Login to the unit, go to *Virtual Machine* > *VM Images* page, download and install the *Windows VM* image needed. The system must be able to access https://fsavm.fortinet.net. Detailed information can be found in the *FortiSandbox Administration Guide*, under the *Virtual Machine* > *VM Images* section.

Install Windows license key file for newly installed Windows VM if needed

Windows license keys might be needed to activate newly installed Windows VMs. The user needs to purchase them from Fortinet and install the license file. For example, the base license for FSA-VM00 model does not contain any Windows license key. Windows license keys are stackable, which means newly ordered Windows keys will be appended to existing ones and the new license file will contain all ordered keys.

For FSA-VM00 models, users can just purchase Windows license keys for enabled Windows VM only. For example, if user only enables WIN7X86VMO16 VM, only Windows 7 license keys and Microsoft Office keys are needed.

1. Download the Key license file from the Fortinet Customer Service & Support portal.
2. Log in to the FortiSandbox VM GUI and find the *System Information* widget on the dashboard.
3. In the *VM License* field, select *Upload License*. The *VM License Upload* pane opens.
4. Browse to the license file on the management computer then click *Submit*. The FortiSandbox VM will reboot. The Windows VM or Microsoft Office on it is automatically activated against the Microsoft activation server when the system is rebooted.

For the VM unit, the number of simultaneously scanned Microsoft Office files is limited by the number of installed Microsoft Office license keys. Users can purchase extra Microsoft Office license keys to improve Office file scan capacity.

To ensure that the Windows VM and Microsoft Office activation is successful, port3 must be able to access the Internet, and the DNS servers must be able to resolve the Microsoft activation servers.

Configuring your FortiSandbox VM

Once the FortiSandbox VM license has been validated, you can configure your device. For more information on configuring your FortiSandbox VM, see the *FortiSandbox Administration Guide* available in the Fortinet Document Library.