

# Install Guide for KVM

**FortiSandbox 4.2**



**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/training-certification>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



June 10, 2022

FortiSandbox 4.2 Install Guide for KVM

34-42-808999-20220610

# TABLE OF CONTENTS

<b>About FortiSandbox VM on KVM</b> .....	<b>4</b>
Licensing .....	4
FSA-VM and FSA-VM00 .....	4
<b>Preparing for deployment</b> .....	<b>6</b>
Minimum system requirements .....	6
Registering your FortiSandbox VM .....	7
Editing FortiSandbox VM IP addresses .....	7
Deployment package for KVM .....	8
Downloading deployment packages .....	8
<b>Deployment</b> .....	<b>10</b>
Deploying FortiSandbox VM on KVM .....	10
Creating the virtual machine .....	10
Configuring initial settings .....	15
Enabling GUI access .....	15
Connecting to the GUI .....	16
Uploading the license file .....	16
Installing the Windows VM package .....	16
Install Windows license key file for newly installed Windows VM .....	17
Configuring your FortiSandbox VM .....	18
<b>Change Log</b> .....	<b>19</b>

# About FortiSandbox VM on KVM

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

This guide assumes that you have a thorough understanding of virtualization servers and terminology, and you know your VM server configuration.

This document provides information about deploying a FortiSandbox VM in Linux KVM server environments.

This guide covers instructions on how to configure the virtual hardware settings of the virtual appliance.

This guide 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 in a stackable license model so that you can expand your VM solution as your needs grow. For information on purchasing a FortiSandbox license, contact your Fortinet Authorized Reseller, or visit [https://www.fortinet.com/how\\_to\\_buy/](https://www.fortinet.com/how_to_buy/).

For more information, see the FortiSandbox product data sheet at <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf>.

After placing an order for FortiSandbox VM, Fortinet sends a license registration code to the email address in the order. Use that license registration code to register the FortiSandbox VM with Customer Service & Support at <https://support.fortinet.com>.

After registration, you can download the license file. You need this file to activate your FortiSandbox VM. You can configure basic network settings using CLI commands to complete the deployment. When 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

Prepare for deployment by reviewing the following information:

- [Minimum system requirements on page 6](#)
- [Registering your FortiSandbox VM](#)
- [Deployment package for KVM on page 8](#)
- [Downloading deployment packages](#)

## Minimum system requirements

Prior to deploying the FortiSandbox VM virtual appliance, KVM must be installed and configured.



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 you meet the following prerequisites before installing FortiSandbox VM:

- A compatible Linux distribution, such as Ubuntu 16.04 with Kernel 4.6.7 and later and the qemu-kvm 2.5 and later packages, or CentOS 7.2 with Kernel 4.1.12 and later and the qemu-kvm 2.3 and later packages.
- virt-manager is installed on the management computer.

When configuring your FortiSandbox hardware settings, use the following table as a guide with consideration for future expansion.

Technical Specification	Details
Hypervisor Support	VMware ESXi Microsoft Hyper-V Windows server 2016 and 2019 Kernel Virtual Machine (KVM)
HA Support	FortiSandbox 2.4 or later
Virtual CPUs (min / max)	4 / Unlimited Fortinet recommends four virtual CPUs plus the number of VM clones.
Virtual Network Interfaces	6
Virtual Memory (min / max)	16GB / Unlimited Fortinet recommends a minimum of 16GB for up to 5 clones. For more clones, use 3GB per Windows VM clone + 1GB. For example, 8 clones require at least 25GB (3GB x 8 clones + 1GB).
Virtual Storage (min / max)	200GB / 16TB Fortinet recommends at least 1TB for a production environment.

## 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 16](#) 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 16](#) for instructions on uploading the license file to your FortiSandbox VM via the GUI.

## Deployment package for KVM

FortiSandbox deployment packages are included with firmware images on the [Customer Service & Support site](#).

- FSA\_KVM-vxxx-build0xxx-FORTINET.out: Download this firmware image to upgrade your existing FortiSandbox installation.
- FSA\_KVM-vxxx-build0xxx-FORTINET.out.kvm.zip: Download this package for a new FortiSandbox VM installation on KVM.

The out.kvm.zip file contains:

- image.out.qcow2: The FortiSandbox VM firmware.
- datadrive.qcow2: The data drive.
- fsa-kvm.sh: The installation script for easy installation.

For more information see the FortiSandbox VM datasheet available on the Fortinet web site, <https://www.fortinet.com/products/fortisandbox/advanced-threat-protection-appliances.html>.

792466 System Settings Dashboard's widgets did not display properly and must be adjusted manually

791657 FortiView: The data can't be shown in list for "Top Cloud Applications" and "Top Cloud Users" if select All Devices.

## 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 into the [Customer Service & Support site](#).
2. From the *Download* dropdown list, select *VM Images* to access the available VM deployment packages.
3. From the *Select Product* dropdown list, select *Other*.
4. Click to *download other firmware images, please click here*.

5. In the *Select Product* dropdown list, select FortiSandbox.
6. Click the Download tab and find the deployment package zip file for your product.
7. To download the file, click the HTTPS link beside the zip file for your product.
8. Extract the package file to a new folder on your management computer.

# Deployment

Before deploying the FortiSandbox VM, install and configure the VM platform so that it is ready to create virtual machines. This guide assumes 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 since there are different ways of creating a virtual machine, such as 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 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 15](#).

## Deploying FortiSandbox VM on KVM

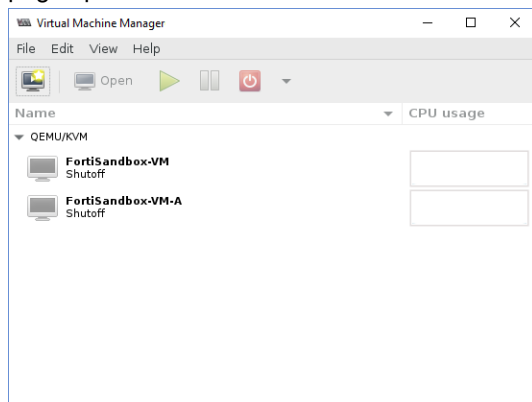
Once you have downloaded the `FSA_KVM-vxxx-build0xxx-FORTINET.out.kvm.zip` file and extracted files, you can create the virtual machine in your KVM environment.

### Creating the virtual machine

The easiest way to create the virtual machine is to execute the `fsa-kvm.sh` script in the shell. You can also install it manually.

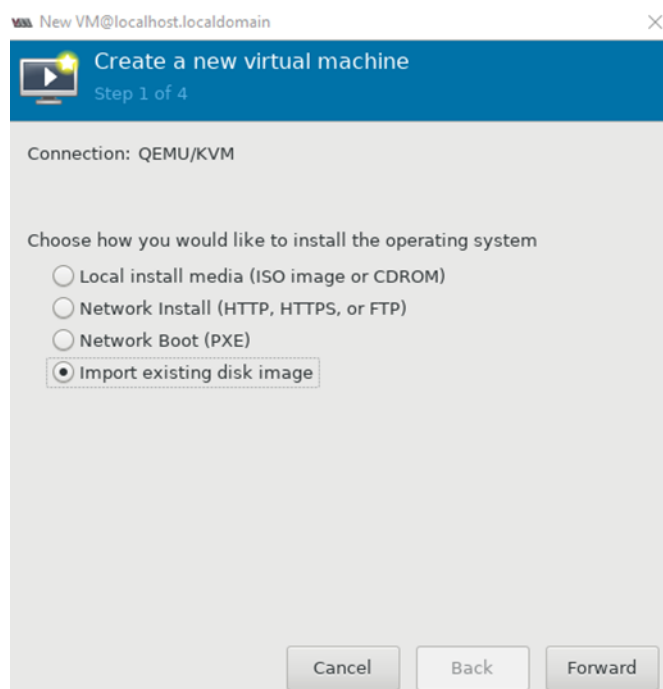
**To create the virtual machine:**

1. Launch the Virtual Machine Manager (virt-manager) on you KVM host server. The *Virtual Machine Manager* home page opens.



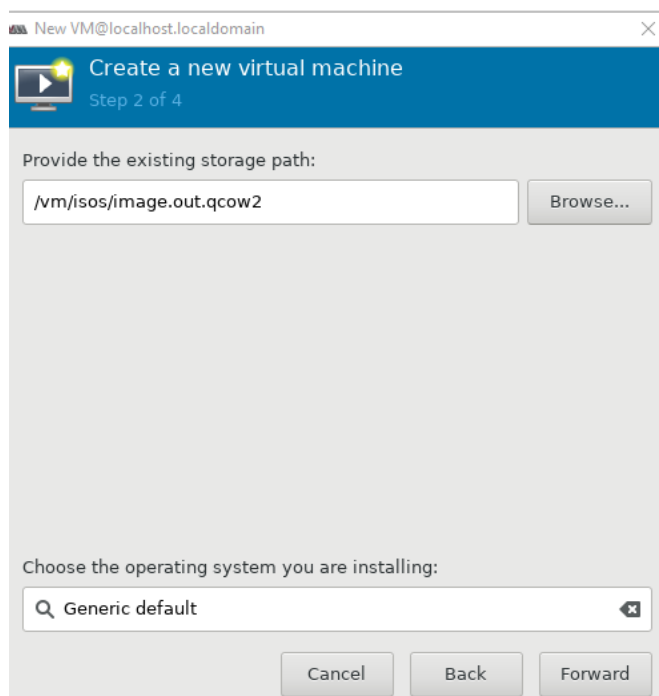
2. Select *Create a new virtual machine* from the toolbar. The Create a new virtual machine dialog opens.

3. Select *Import existing disk image*, then click *Forward*.

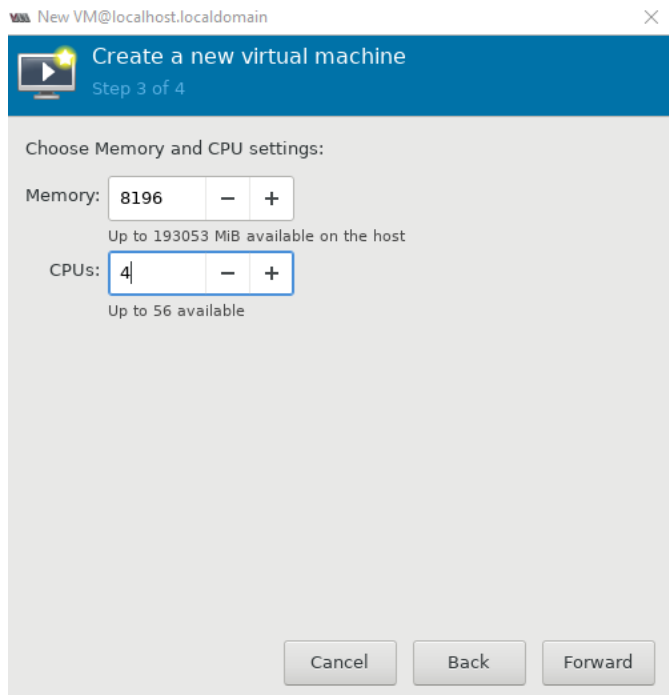


4. Provide the storage path and select the OS.

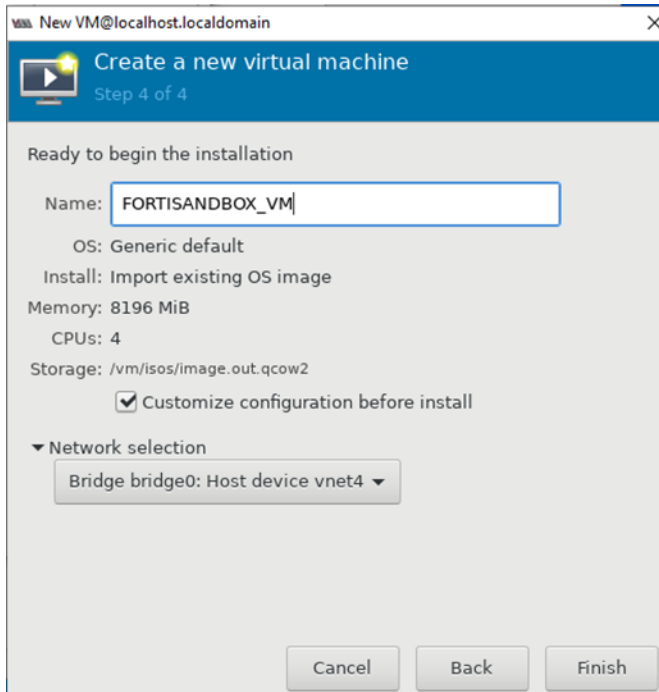
- a. Enter the full path to extract the `image.out.qcow2` file or click *Browse*.
- If you copied the file to `/var/lib/libvirt/images`, it will be shown on the right.
  - If you saved it elsewhere on the server, select *Browse Local* to find it.
- b. Choose *Generic default* for the OS and click *Forward*.



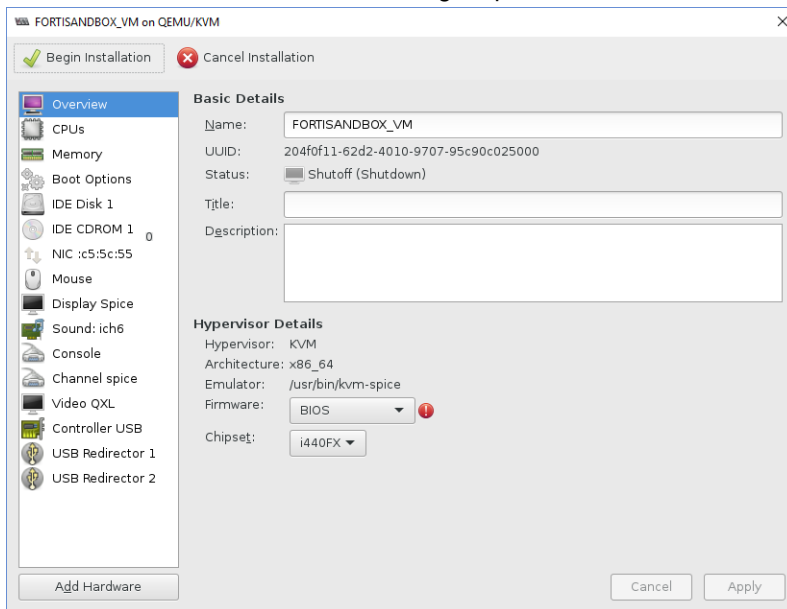
5. Specify the amount of memory and the number of CPUs to allocate to this VM, then click *Forward*.  
A minimum of 8GB of memory and two CPUs are required for the VM. Fortinet recommends that the number of CPU cores be four more than the number of Windows VMs, and 3GB of RAM per Windows VM.



6. In the *Ready to begin the installation* dialog:
  - a. In the *Name* field, enter the name of your VM.
  - b. Select *Customize Configuration before install*.
  - c. Select the correct interface for the *Network Selection* field.

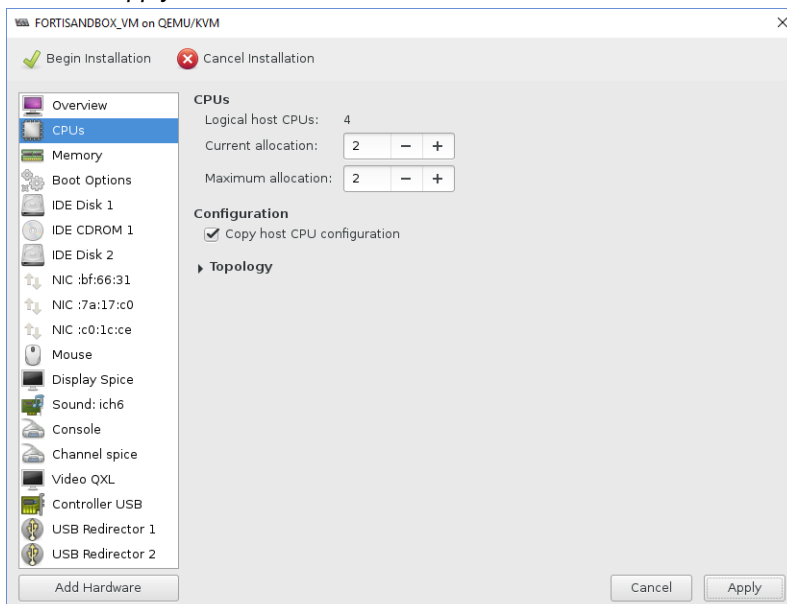


- d. Click *Finish*. The Virtual Machine Manager opens.

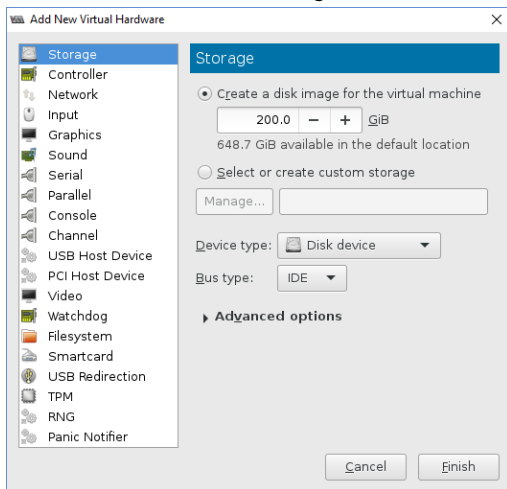


Before powering on your FortiSandbox VM you must configure the CPUs to copy the host configuration, and add a local hard drive of at least 200GB and at least two more network interfaces.

7. Click *CPUs* in the navigation pane.
- Select *Copy host CPU Configuration*.
  - Click *Apply*.

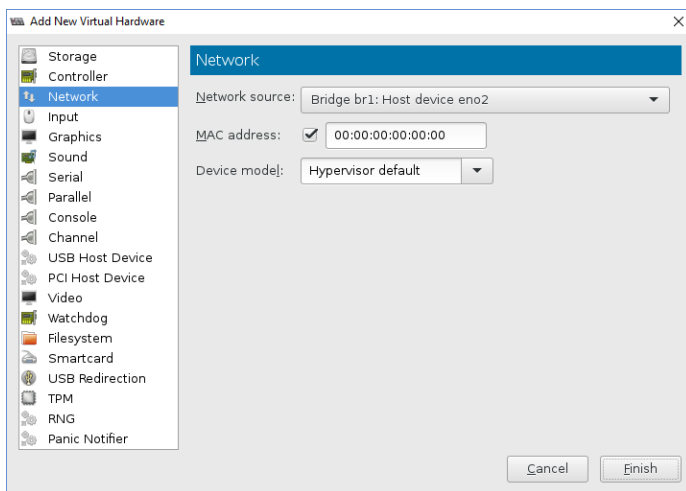


## 8. Add a second hard drive:

a. Click *Add Hardware > Storage*.b. Enter 200 or a larger number in the disk size field, then click *Finish*. Fortinet recommends making the virtual disk 1TB or larger.

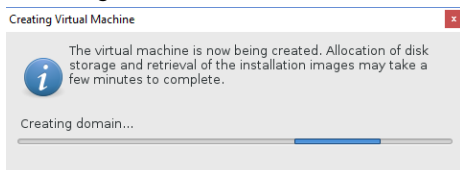
The disk is created and added to the hardware list as *IDE Disk 2*.

## 9. Add more network interfaces:

a. Click *Add Hardware > Network*.b. Edit the settings as required, then click *Finish* to create the interface.

## c. Repeat these steps to create a third interface.

FortiSandbox VM supports up to six network adapters. You can configure network adapters to connect to a virtual switch or to network adapters on the host computer.

10. Click *Begin Installation* to create the VM.

The FortiSandbox VM is created and started. See [Configuring initial settings on page 15](#) for information on configuring your FortiSandbox VM.

## Configuring initial settings

Before you can connect to the FortiSandbox VM, configure basic configuration via the CLI console. Then 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:

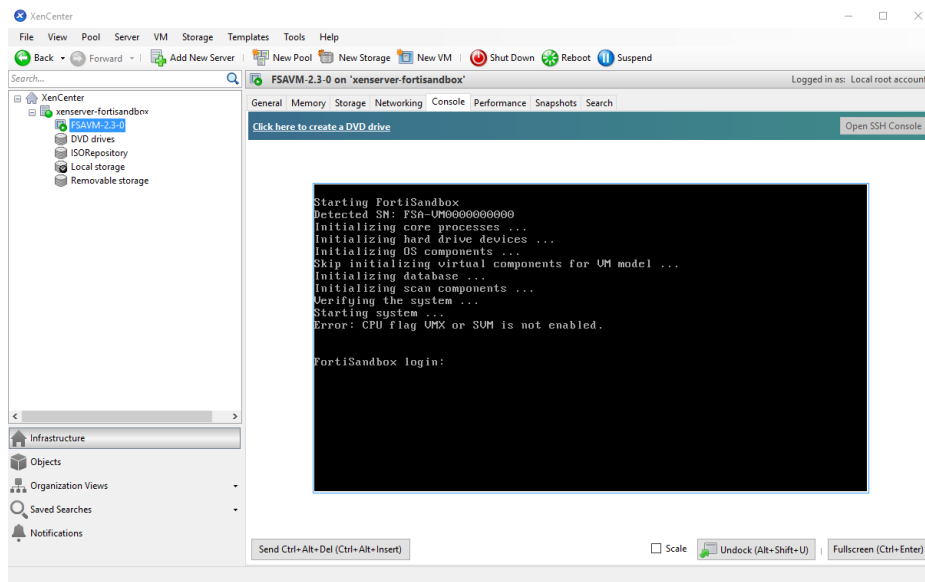
- [Enabling GUI access](#)
- [Connecting to the GUI](#)
- [Uploading the license file](#)
- [Installing the Windows VM package](#)

### Enabling GUI access

To enable GUI access to the FortiSandbox VM, 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*. There is no password by default. The system will require you to set a 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

When 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 password, then click *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 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 7](#)

## Installing the Windows VM package

Downloading and installing the Microsoft Windows VM package is optional for FortiSandbox VM. For example, you do not need to install the Windows VM package when you choose to:

- Deploy the unit as Primary or Secondary node of a cluster without doing any dynamic scans on it, or
- Use Windows Cloud VM to do dynamic scans instead of using local VMs.

If you choose to install local Windows VM, there are two types to choose from: *Default* and *Optional*.

## Install the default Windows VM package

The default Windows VMs includes two versions:

- Windows 7, 32 bit with SP1 and Microsoft Office installed
- Windows 10, 64bit

To view the VMs after they are installed, go to *Scan Policy and Object > VM Settings > Default VMs*.

You can install the VMs directly with the CLI, or download it to local FTP or SCP server first and then install it with the CLI command. For either method, the system must be able to access <https://fsavm.fortinet.net>.

### To download and install the default Windows VM package directly with the CLI:

```
fw-upgrade -v -sfsavm.fortinet.net -thttps -f/images/v4.00/VM00_base.pkg
```

### To download the default Windows VM package to a local server and install it:

1. Go to [https://fsavm.fortinet.net/images/v4.00/VM00\\_base.pkg](https://fsavm.fortinet.net/images/v4.00/VM00_base.pkg) to download the Windows VM package.
2. Save the package on a host that supports file copy with the SCP or FTP protocol. FortiSandbox must be able to access the SCP or FTP server.
3. In a CLI console window, use the following command to download and install the package:

```
fw-upgrade -v -t<ftp|scp> -s<SCP/FTP server IP address> -u<user name> -f<file path>
```

For example, `fw-upgrade -v -tscp -sx.x.x.x -utest -f/home/test/xxxx`

## Install Optional Windows VM package

You can install an optional Windows VM to best mimic your environment. For example, if the majority of installations in your environment are Windows 10 with Office 2016, you can install WIN10O16V4 VM.

Available optional VMs are displayed in *Scan Policy and Object > VM Settings > Optional VMs*. You can download and install one from the list. The system must be able to access <https://fsavm.fortinet.net>. For more information, see the [Scan Policy and Object > VM Settings](#) chapter in the *FortiSandbox Administration Guide*.

Windows Sandbox VMs must be activated on the Microsoft activation server. This is done automatically when a system reboots after Windows activation keys are uploaded to the unit. For the activation to work, ensure port3 can access the Internet and the DNS server can resolve the Microsoft activation servers.

## Install Windows license key file for newly installed Windows VM

An unused license key for the Windows OS version is required to activate a newly installed Windows VM. For example, a newly installed Windows 10 VM requires the unit to have one unused Windows 10 license key for activation. If the unit has no available key for the activation, you can purchase and install the license key file from Fortinet.

Windows license keys are stackable, which means new Windows keys are appended to existing ones and the new license file contains all ordered keys.




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

---

For FortiSandbox VM model, you can just purchase Windows license keys for enabled Windows VM only. For example, if you enable a Windows 7 VM which has Microsoft Office software installed, you only need to purchase one Windows 7 license key and one Microsoft Office key to activate them.

### To install a Windows license key file on a Windows VM:

1. Download the license key file from the Fortinet [Customer Service & Support portal](#).
2. Log into the FortiSandbox VM GUI and go to *Status > Licenses widget*.
3. Click the *Upload License*  button beside *FortiSandbox-VM*.
4. Select the license file on the management computer and click *Submit*.

The unit will reboot. On reboot, the Windows VM or Microsoft Office is automatically activated on the Microsoft activation server.



A Microsoft Windows key or Office key can only activate one Windows VM. The key cannot be re-used.

Make sure to activate the correct Windows VM with the license key, as you will not be able to use the key again.

---

## 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](#).

## Change Log

Date	Change Description
2022-06-08	Initial release.



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.