Install Guide for VMware

FortiSandbox 4.2.0

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/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

FORTINET®

November 04, 2022
FortiSandbox 4.2.0 Install Guide for VMware
34-420-809007-20221104

TABLE OF CONTENTS

About FortiSandbox VM 4

Preparing for deployment 5

Licensing 5

FSA-VM and FSA-VM00 5

Minimum system requirements 6

Registering your FortiSandbox VM 8

Editing FortiSandbox VM IP addresses 9

Deployment package for VMware 9

Downloading deployment packages 10

Deployment 11

Deploying FortiSandbox VM on VMware 11

Deploying the OVF file 12

Configuring hardware settings 14

Powering on the virtual machine 16

Configuring initial settings 16

Enabling GUI access 16

Connecting to the GUI 17

Uploading the license file 17

Installing the Windows VM package 18

Install Windows license key file for newly installed Windows VM 19

Configuring your FortiSandbox VM 20

Change Log 21

About FortiSandbox VM

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

Preparing for deployment

Prepare for deployment by reviewing the following information:

- Minimum system requirements
- Registering your FortiSandbox VM
- Deployment package for VMware
- Downloading deployment packages

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/.

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

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*.

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*.

Minimum system requirements

Before deploying the FortiSandbox VM virtual appliance, install and configure the latest stable release of VMware vSphere ESXi Hypervisor software. Supported versions are ESXi version 5.1 to 7.0.1.

Access VMware vSphere using a web browser or install the VMware vSphere client.

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.

In VMware, you can expose full CPU virtualization to the guest operating system so that applications that require hardware virtualization can run on virtual machines without binary translation or paravirtualization. For more information, see https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.vm_admin.doc/GUID-2A98801C-68E8-47AF-99ED-00C63E4857F6.html.

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

Technical Specification	Details		
	On-Premise (Private) Cloud	Public Cloud - BYOL	Public Cloud - PAYG
Hypervisor Support	VMware ESXi Microsoft Hyper-V Windows server 2016 and 2019	AWS Azure	
HA Support	FortiSandbox 3.2 or later		
Virtual CPUs (min / max)	4/Unlimited Fortinet recommends four virtual CPUs plus the number of VM clones.	4/16 Fortinet recommends following virtual CPUs based on the number of VM Clones: 0-4 clones - 4 cores, 5-32 clones - 8 cores, 33-100 clones - 16 cores, 101+ clones - 16 cores or higher. Pick up the appropriate Instance Type.	
Virtual Memory (min / max)	16 GB / 32 GB Fortinet recommends following virtual memory based on the number of VM Clones:	8 GB / 64 GB Recommended: Following virtual memory based on the number of VM Clones: 0-4 clones - 8 GB, 5-32 clones - 16 GB, 33-100 clones - 32 GB, 101+ clones - 64 GB.	

Technical Specification	Details		
	On-Premise (Private) Cloud	Public Cloud - BYOL	Public Cloud - PAYG
	0-4 clones - 24 GB 5-8 clones - 32 GB	Pick the appropriate Instance Type.	
Virtual Storage (min / max)	200 GB / 16 TB Fortinet recommends at least 500 GB for a production environment.		
Virtual Network Interfaces	Recommended: 4 and above	Recommended: 2 and above	
VM Clones Support (Min/Max)	0[1]/ 8 (Local VMs) and 200 (Cloud VMs)	0[1] / 216[2]	0[1] / 128[3]

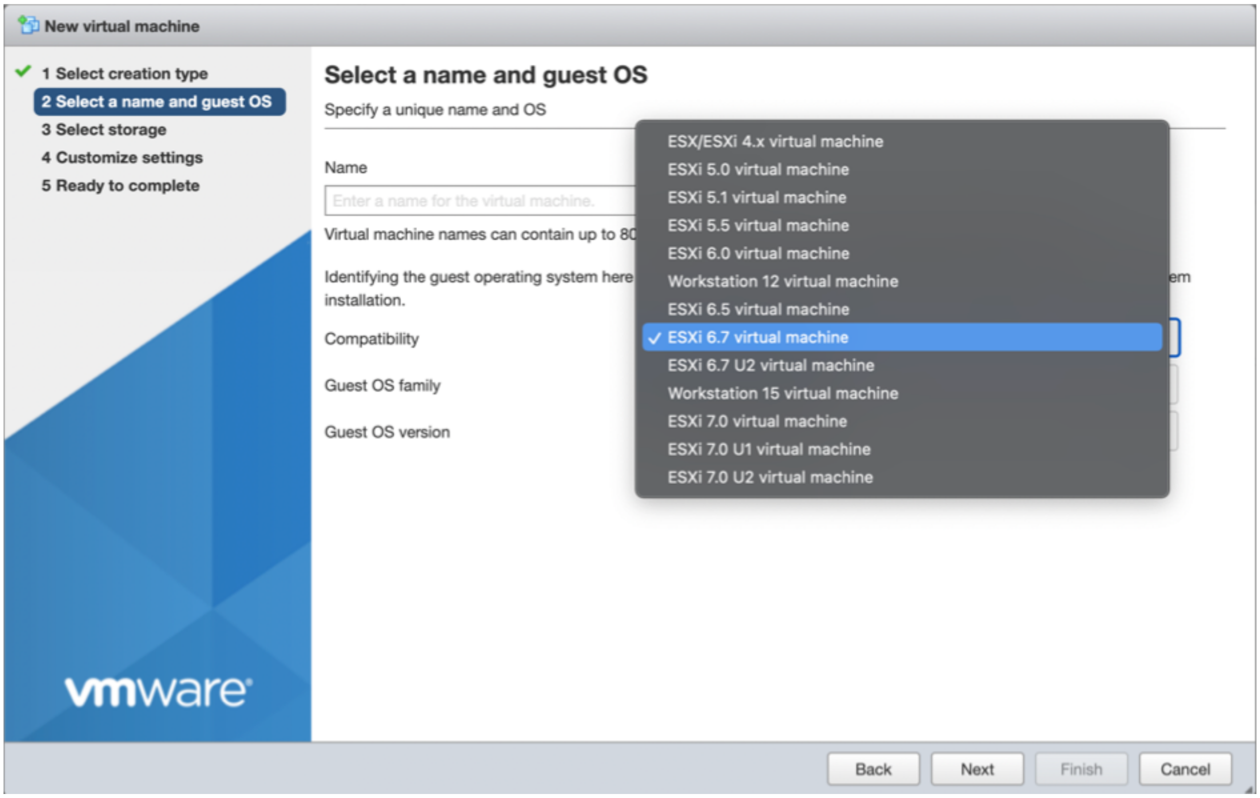
[1] For HA-Cluster deployment setup configured as Primary node acting as a dispatcher.

[2] Can enable any of the Custom VM or Cloud VM types up to the total seat count which is based on a combination of Windows licenses (max of 8), BYOL (8) and Cloud VMs (max of 200).

[3] Total seat count is based on the number of cores multiplied by 4. Maximum VMs is 128 since the highest available vCPU on PAYG is 32. CloudVMs can also be added on top and registered, however, this is not advised due to product serial number changes after shutdown.

Virtual Machine compatibility

The Virtual Machine compatibility setting should be 6.7 or later to support AMD SMT (Simultaneous multithreading).


New virtual machine
1 Select creation type
2 Select a name and guest OS
3 Select storage
4 Customize settings
5 Ready to complete
Select a name and guest OS
Specify a unique name and OS
Name
Enter a name for the virtual machine.
Virtual machine names can contain up to 80
Identifying the guest operating system here
em
installation.
Compatibility
Guest OS family
Guest OS version
ESX/ESXi 4.x virtual machine
ESXi 5.0 virtual machine
ESXi 5.1 virtual machine
ESXi 5.5 virtual machine
ESXi 6.0 virtual machine
Workstation 12 virtual machine
ESXi 6.5 virtual machine
✓ ESXi 6.7 virtual machine
ESXi 6.7 U2 virtual machine
Workstation 15 virtual machine
ESXi 7.0 virtual machine
ESXi 7.0 U1 virtual machine
ESXi 7.0 U2 virtual machine
vmware
Back
Next
Finish
Cancel

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

- FSA_VM-vxxx-build0xxx-FORTINET.out: Download this firmware image to upgrade your existing FortiSandbox VM installation.
- FSA_VM-vxxx-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 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 16.

Deploying FortiSandbox VM on VMware

Once you have downloaded the `FSA_VM-vxxx-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, 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.

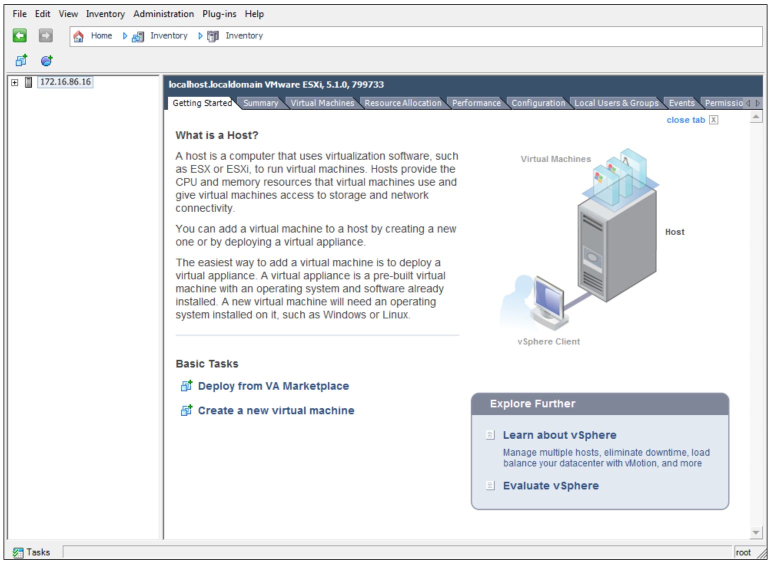
The following topics are included in this section:

- Deploying the OVF file
- Configuring hardware settings
- Powering on the virtual machine

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.



localhost.localdomain VMware ESXi, 5.1.0, 799733

What is a Host?

A host is a computer that uses virtualization software, such as ESX or ESXi, to run virtual machines. Hosts provide the CPU and memory resources that virtual machines use and give virtual machines access to storage and network connectivity.

You can add a virtual machine to a host by creating a new one or by deploying a virtual appliance.

The easiest way to add a virtual machine is to deploy a virtual appliance. A virtual appliance is a pre-built virtual machine with an operating system and software already installed. A new virtual machine will need an operating system installed on it, such as Windows or Linux.

Basic Tasks

Deploy from VA Marketplace

Create a new virtual machine

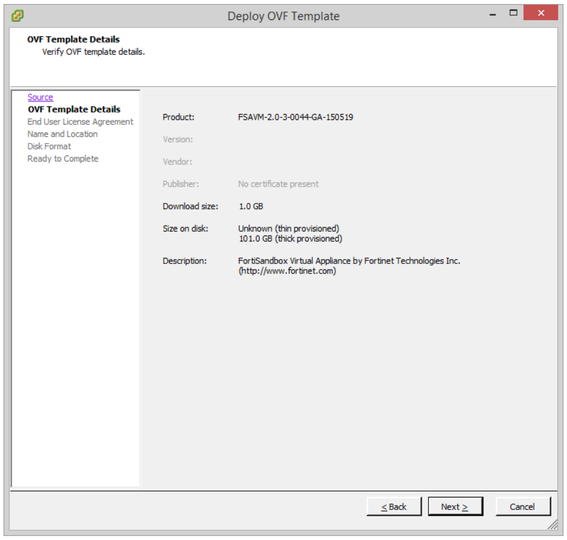
Explore Further

Learn about vSphere

Manage multiple hosts, eliminate downtime, load balance your datacenter with vMotion, and more

Evaluate vSphere

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.

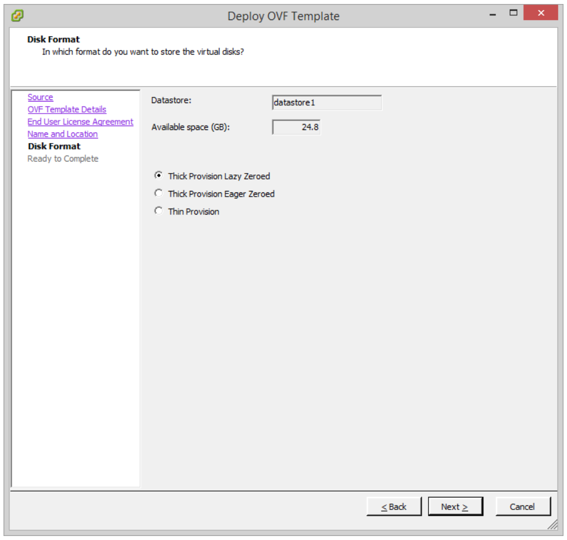


OVF Template Details

Verify OVF template details.

Product:	FSAVM-2.0-3-0044-GA-150519
Version:	
Vendor:	
Publisher:	No certificate present
Download size:	1.0 GB
Size on disk:	Unknown (thin provisioned) 101.0 GB (thick provisioned)
Description:	FortiSandbox Virtual Appliance by Fortinet Technologies Inc. (http://www.fortinet.com)

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.



Disk Format
In which format do you want to store the virtual disks?

Datastore: datastore1

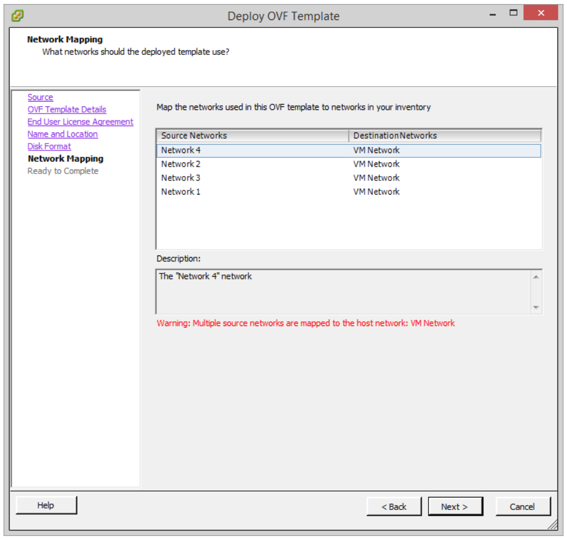
Available space (GB): 24.8

● Thick Provision Lazy Zeroed
○ Thick Provision Eager Zeroed
○ Thin Provision

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.



Network Mapping
What networks should the deployed template use?

Map the networks used in this OVF template to networks in your inventory

Source Networks	Destination Networks
Network 4	VM Network
Network 2	VM Network
Network 3	VM Network
Network 1	VM Network

Description:
The "Network 4" network

Warning: Multiple source networks are mapped to the host network: VM Network

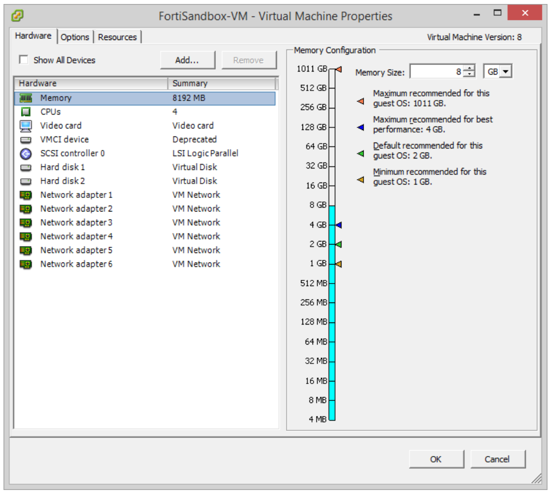
9. Map the networks used in this OVF template to networks in your inventory. Network 1 maps to port1 of the FortiSandbox VM. You must set the destination network for this entry to access the device console. Select *Next* to continue. The OVF Template *Ready to Complete* page opens.
10. Review the template 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*.
   For information on virtual memory size, see Minimum system requirements on page 6.



Hardware	Summary
Memory	8192 MB
CPUs	4
Video card	Video card
VMCI device	Deprecated
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
Network adapter 1	VM Network
Network adapter 2	VM Network
Network adapter 3	VM Network
Network adapter 4	VM Network
Network adapter 5	VM Network
Network adapter 6	VM Network

Memory Size: 8 GB

Maximum recommended for this guest OS: 1011 GB.

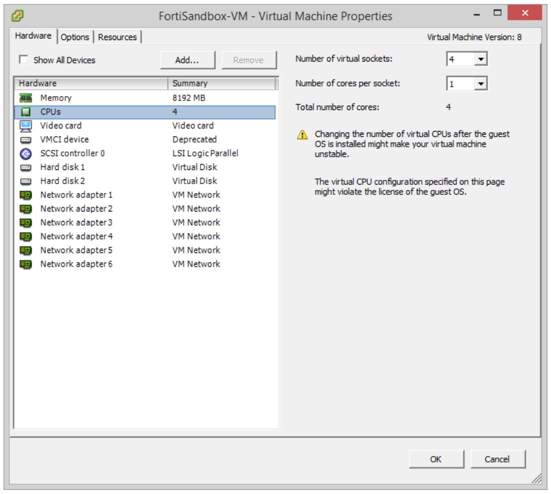
Maximum recommended for best performance: 4 GB.

Default recommended for this guest OS: 2 GB.

Minimum recommended for this guest OS: 1 GB.

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.



FortiSandbox-VM - Virtual Machine Properties

Hardware | Options | Resources — Virtual Machine Version: 8

□ Show All Devices — Add... — Remove

Hardware	Summary
Memory	8192 MB
CPUs	4
Video card	Video card
VMCI device	Deprecated
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
Network adapter 1	VM Network
Network adapter 2	VM Network
Network adapter 3	VM Network
Network adapter 4	VM Network
Network adapter 5	VM Network
Network adapter 6	VM Network

Number of virtual sockets: 4

Number of cores per socket: 1

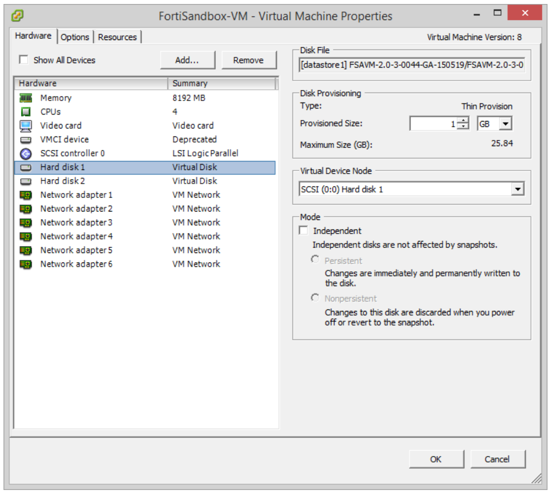
Total number of cores: 4

⚠ Changing the number of virtual CPUs after the guest OS is installed might make your virtual machine unstable.

The virtual CPU configuration specified on this page might violate the license of the guest OS.

OK — Cancel

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.



FortiSandbox-VM - Virtual Machine Properties

Hardware | Options | Resources — Virtual Machine Version: 8

□ Show All Devices — Add... — Remove

Hardware	Summary
Memory	8192 MB
CPUs	4
Video card	Video card
VMCI device	Deprecated
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
Network adapter 1	VM Network
Network adapter 2	VM Network
Network adapter 3	VM Network
Network adapter 4	VM Network
Network adapter 5	VM Network
Network adapter 6	VM Network

Disk File: [datastore1] FSAVM-2.0-3-0044-GA-150519/FSAVM-2.0-3-0

Disk Provisioning
Type: Thin Provision
Provisioned Size: 1 GB
Maximum Size (GB): 25.84

Virtual Device Node: SCSI (0:0) Hard disk 1

Mode
□ Independent
Independent disks are not affected by snapshots.
○ Persistent
Changes are immediately and permanently written to the disk.
○ Nonpersistent
Changes to this disk are discarded when you power off or revert to the snapshot.

OK — Cancel

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, 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:

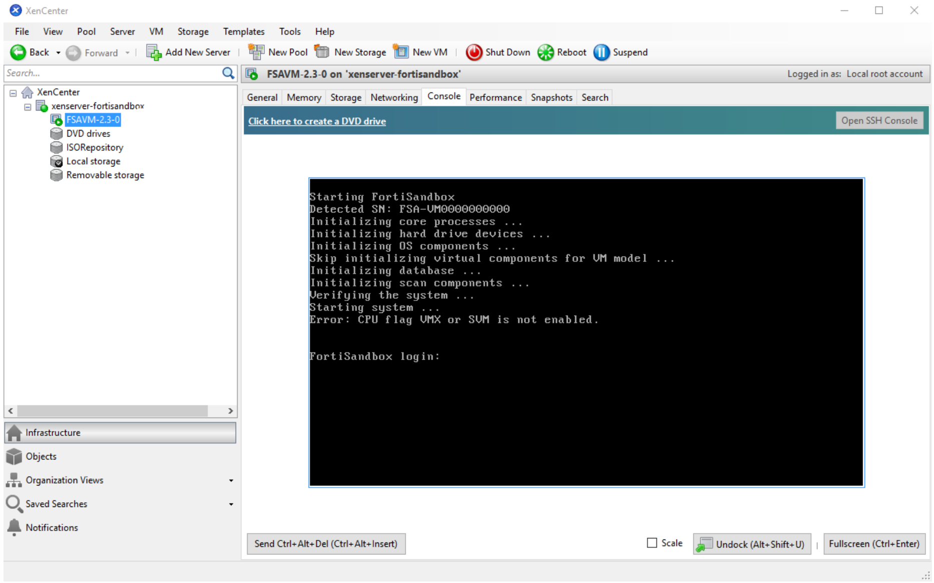
- Enabling GUI access
- Connecting to the GUI
- Uploading the license file
- Installing the Windows VM package

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.


XenCenter
File View Pool Server VM Storage Templates Tools Help
Back Forward Add New Server New Pool New Storage New VM Shut Down Reboot Suspend
Search...
FSAVM-2.3-0 on 'xenserver-fortisandbox'
Logged in as: Local root account
XenCenter
xenserver-fortisandbox
FSAVM-2.3-0
DVD drives
ISORepository
Local storage
Removable storage
General Memory Storage Networking Console Performance Snapshots Search
Click here to create a DVD drive
Open SSH Console
Infrastructure
Objects
Organization Views
Saved Searches
Notifications
Send Ctrl+Alt+Del (Ctrl+Alt+Insert)
Scale
Undock (Alt+Shift+U)
Fullscreen (Ctrl+Enter)

```
Starting FortiSandbox
Detected SN: FSA-VM0000000000
Initializing core processes ...
Initializing hard drive devices ...
Initializing OS components ...
Skip initializing virtual components for VM model ...
Initializing database ...
Initializing scan components ...
Verifying the system ...
Starting system ...
Error: CPU flag VMX or SVM is not enabled.


FortiSandbox login:
```

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 9

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 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 example, the rating engine and tracer engine should be installed before the unit can fully function.

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.
2022-09-28	Updated Minimum system requirements on page 6.
2022-11-04	Updated Minimum system requirements on page 6.

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.