



Deploying FortiTester-VM on OpenStack

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



TABLE OF CONTENTS

About FortiTester-VM on OpenStack	4
Overview	4
About this document	4
System requirements	5
Downloading the FortiTester-VM license & registering with Technical Support	6
Downloading the FortiTester-VM software	7
Deploying FortiTester-VM on OpenStack	8
Configuring access to FortiTester's web UI & CLI	19
Uploading the license	20

About FortiTester-VM on OpenStack

Overview

Welcome, and thank you for selecting Fortinet products for your testing environment.

FortiTester™ appliances offer enterprises and service providers a cost-effective solution for performance testing and validating their network security infrastructure and services, providing a comprehensive range of application test cases to evaluate equipment and right-size infrastructure. All test functionality is included in one simple device-based license.

FortiTester provides powerful yet easy-to-use test cases that simulate many applications and a case history browser for simple analysis. It enables you to establish performance standards and run audits to validate they continue to be met. The virtual appliance version provides an ideal tester for NFV and SDN environments.

About this document

This document provides the following information:

- How to deploy a FortiTester-VM in an OpenStack environment. To learn how to deploy FortiTester-VM on public cloud platforms, see <https://docs2.fortinet.com/vm/product/fortitester>.
- How to configure any required virtual hardware settings. For hypervisor deployments, it assumes you have already successfully installed a virtualization server on the physical machine or the required EC2 environment.

This document does **not** cover initial configuration of the virtual appliance, nor ongoing use and maintenance. After deploying the virtual appliance, for information on initial appliance configuration, see [FortiTester Handbook](#).

This document is intended for administrators, not end users. If you have a user account on a computer that accesses websites through a FortiTester appliance, please contact your system administrator.

System requirements

FortiTester-VM supports the following hypervisor versions:

- OpenStack Rocky or above



For best performance in hypervisor deployments, install FortiTester-VM on a “bare metal” (type 1) hypervisor. Hypervisors that are installed as applications on top of a general purpose operating system (Windows, Mac OS X or Linux) host have fewer computing resources available due to the host OS’s own overhead.

To ensure high performance, it's recommended to deploy FortiTester on the machine types with minimum 4 vCPUs, and memory size larger than 8 GB.

For hypervisor deployments, hardware-assisted virtualization (Intel VT or AMD-V) must be enabled in the BIOS.

Downloading the FortiTester-VM license & registering with Technical Support

For Hypervisor deployments, when you purchase FortiTester-VM from your reseller, you receive an email that contains a registration number. You use this number to download the software and your purchased license, and also to register your purchase for technical support.

Many Fortinet customer services such as firmware updates, technical support, and FortiGuard services require product registration.

For details, see the Fortinet Knowledge Base article [Registration Frequently Asked Questions](#).

To register & download your FortiTester-VM license

1. On your management computer, start a web browser.
2. Log in to the Fortinet Technical Support website:
<https://support.fortinet.com/>
3. In the **Asset Management** quadrant of the page, click **Register/Renew**.
4. Provide the registration number that was emailed to you when you purchased the software. Registration numbers are a hyphenated mixture of 25 numbers and characters in groups of 5. For example:
12C45-AB3DE-678G0-F9HIJ-123B5
A registration form is displayed.
5. Complete the form to register your ownership of FortiTester-VM with Technical Support.
After you complete the form, a registration acknowledgment page is displayed.
6. Click the **License File Download** link.
Your browser downloads the `.lic` file that was purchased for that registration number.
7. Download the FortiTester-VM software following steps in [Downloading the FortiTester-VM software on page 7](#).

Downloading the FortiTester-VM software

To download your FortiTester-VM software

1. On the main page of the Fortinet Technical Support website, under **Download**, click **Firmware Images**.
2. Click the FortiTester link and navigate to the version that you want to download.
3. Download the appropriate `.zip` file.

You use this file for **new virtual appliance (VM)** installations. It contains a deployable virtual machine package. (`.out` image files are for upgrades of existing installations only, and cannot be used for a new installation.)



Files for FortiTester-VM have a `FTS_VM` file name prefix. Other prefixes indicate that the file is for hardware versions of FortiTester such as FortiTester 3000E. These hardware versions are not used with FTS-VM.



If you have a library of virtual machine images stored on a CIFS or NFS share, download and unzip the folder there instead of on your management computer. When deploying the VM, you can also use a CIFS or NFS network share as the storage repository instead of a vDisk stored locally, on the hypervisor's disk.



FortiTester-VM on OpenStack platform uses `FTS_VM_KVM` series image.

4. Extract the `.zip` compressed archive's contents to a folder.
5. Continue by deploying the virtual appliance package using the appropriate deployment instructions in this guide. For example, see [Deploying FortiTester-VM on OpenStack on page 8](#).

Deploying FortiTester-VM on OpenStack

This section shows examples on how to create a FortiTester-VM instance with the following properties.

- A direct connection to the public network
- A 60GB log disk (an OpenStack volume)
- 4 vCPUs with 8GB RAM and a 2GB root disk (specified by the OpenStack flavor)
- Fully licensed

Follow steps below:

1. To set up your OpenStack environment, create an `openrc.sh` (OpenStack `rc`) file that specifies the admin credentials and admin endpoint.

For example, the OpenStack `rc` file `admin-openrc` includes the following:

```
export OS_PROJECT_DOMAIN_NAME=Default
export OS_USER_DOMAIN_NAME=Default
export OS_PROJECT_NAME=admin
export OS_USERNAME=admin
export OS_PASSWORD=fortinet
export OS_AUTH_URL=http://openstack-ctl:5000/v3
export OS_IDENTITY_API_VERSION=3
export OS_IMAGE_API_VERSION=2
```

2. Use Linux shell to run OpenStack commands, import the OpenStack `rc` file.

For example, `$ source admin-openrc`

3. Log in to the OpenStack dashboard, and navigate to **Admin > Compute > Flavors**. Click Create Flavor to create a flavor for FortiTester if it does not exist.

Create Flavor ✕

Flavor Information *

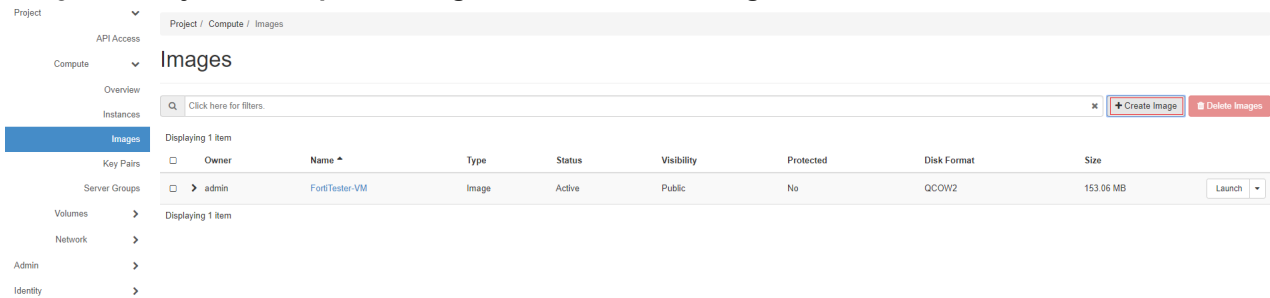
Flavor Access

Name ***ID ⓘ****VCPUs *****RAM (MB) *****Root Disk (GB) *****Ephemeral Disk (GB)****Swap Disk (MB)****RX/TX Factor**

Flavors define the sizes for RAM, disk, number of cores, and other resources and can be selected when users deploy instances.

Enter 2 for the Root Disk (GB); it is recommended to use 4 VCPUs and 8G (or above) memory for this flavor. Click **Create Flavor** after you configure the settings.

4. Navigate to **Project > Compute > Images**, and click **Create Image**.



5. Complete the settings below:
Create Image

Image Details *

✕

Image Details

Specify an image to upload to the Image Service.

Image Name*

Image Source

File*

Browse...

Format*

QCOW2 - QEMU Emulator
▼

Image Requirements

Kernel

Choose an image
▼

Architecture

Image Sharing

Visibility

Public

Private

Protected

Yes

No

Image Description

Ramdisk

Choose an image
▼

Minimum Disk (GB)

0

Minimum RAM (MB)

0

✕ Cancel

< Back

Next >

✔ Create Image

Click **Create Image** after you configure the settings.

6. Navigate to **Compute > Images** to check whether the image has been successfully created.

7. Navigate to **Compute > Instances**, check **FortiTester-VM**, and click **Launch Instance**.

Project / Compute / Instances

Instances

Instance ID = Filter [Launch Instance](#) [Delete Instances](#) [More Actions](#)

Displaying 1 item

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
<input checked="" type="checkbox"/> FortiTester-VM	-	traffic-network 17.1.0.1 17.1.2.2 17.1.2.3 17.1.2.4 17.1.2.5 17.1.2.6 17.1.0.2 17.1.1.100 extern-network 192.168.13.18	m1.large	-	Shutoff	nova	None	Shut Down	1 week	Start Instance

8. In the **Launch Instance** window, enter the instance name, and click **Next**.

Launch Instance

Please provide the initial hostname for the instance, the availability zone where it will be deployed, and the instance count. Increase the Count to create multiple instances with the same settings.


Instance Name *

Description

Availability Zone

Count *

Total Instances (10 Max)



20%

- 1 Current Usage
- 1 Added
- 8 Remaining

[Cancel](#)
[Back](#)
[Next](#)
[Launch Instance](#)

9. Set the Volume Size to 2, and select the FortiTester-VM image created in Step 6.

Launch Instance ✕

Details

Source *

Flavor *

Networks *

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Instance source is the template used to create an instance. You can use an image, a snapshot of an instance (image snapshot), a volume or a volume snapshot (if enabled). You can also choose to use persistent storage by creating a new volume. ?

Select Boot Source

Image ▼

Create New Volume

Yes No

Volume Size (GB) *

2

Delete Volume on Instance Delete

Yes No

Allocated

Name	Updated	Size	Type	Visibility
Select an item from Available items below				

Available 1 Select one

Click here for filters. ✕

Name	Updated	Size	Type	Visibility
FortiTester-VM	11/14/19 5:50 PM	153.06 MB	qcow2	Public

✕ Cancel
< Back
Next >
Launch Instance

10. Select an available flavor created in Step 4, and click Next.

Launch Instance ✕

Details

Source *

Flavor

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Flavors manage the sizing for the compute, memory and storage capacity of the instance. ?

Allocated

Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public
m1.large	4	8 GB	2 GB	2 GB	0 GB	Yes

Available 3 Select one

Click here for filters. ✕

Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public
m1.tiny	1	512 MB	1 GB	1 GB	0 GB	Yes
m1.small	1	2 GB	2 GB	2 GB	0 GB	Yes
m1.medium	2	4 GB	2 GB	2 GB	0 GB	Yes

✕ Cancel
< Back
Next >
Launch Instance

11. Select an available network for the management port, then click **Launch Instance**.

Launch Instance ✕

Details

Source ^{*}

Flavor

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Networks provide the communication channels for instances in the cloud. ?

▼ Allocated ¹ Select networks from those listed below.

Network	Subnets Associated	Shared	Admin State	Status
1 > extern-network	mgmt-network	Yes	Up	Active ↓

▼ Available ² Select at least one network

🔍 Click here for filters. ✕

Network	Subnets Associated	Shared	Admin State	Status
> selfservice1	selfservice1	No	Up	Active ↑
> traffic-network	traffic-network	No	Up	Active ↑

✕ Cancel
< Back
Next >
Launch Instance



FortiTester requires at least three ports; one is for management network, and the other two are for traffic network. In the Launch Instance step, you need to create a management network, and the traffic networks will be added after creating the instance.

12. The instance is running now, but FortiTester can't be booted until the log volume is attached. Navigate to **Project > Compute > Instances**, click **Shut Off Instance**.

Project / Compute / Instances

Instances

Instance ID = Filter Launch Instance Delete Instances More Actions

Displaying 1 item

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions	
FortiTester-VM	-	traffic-network 17.1.0.1 17.1.2.2 17.1.2.3 17.1.2.4 17.1.2.5 17.1.2.6 17.1.0.2 17.1.1.100 extern-network 192.168.13.18	m1.large	-	Active	us-east-1a	nova	None	Running	1 week	Create Snapshot Associate Floating IP Attach Interface Detach Interface Edit Instance Attach Volume Detach Volume Update Metadata Edit Security Groups Edit Port Security Groups Console View Log Pause Instance Suspend Instance Shelve Instance Resize Instance Lock Instance Soft Reboot Instance Hard Reboot Instance Shut Off Instance Rebuild Instance Delete Instance

Displaying 1 item

When the instance is shut off, the power status will change from Running to Shut Down.

Project / Compute / Instances

Instances

Instance ID = Filter Launch Instance Delete Instances More Actions

Displaying 1 item

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions	
FortiTester-VM	-	traffic-network 17.1.0.1 17.1.2.2 17.1.2.3 17.1.2.4 17.1.2.5 17.1.2.6 17.1.0.2 17.1.1.100 extern-network 192.168.13.18	m1.large	-	Shutoff	us-east-1a	nova	None	Shut Down	1 week	Start Instance

Displaying 1 item

13. Navigate to **Project > Volumes > Volumes**, click **Create Volume**.

14. Configure the volume settings as below.

Create Volume ✕

Volume Name

FortiTester-Logdisk

Description

Volume Source

No source, empty volume

Type

No volume type

Size (GiB) *

60

Availability Zone

nova

Group ?

No group

Description:

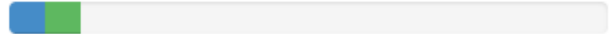
Volumes are block devices that can be attached to instances.

Volume Type Description:

If "No volume type" is selected, the volume will be created without a volume type.

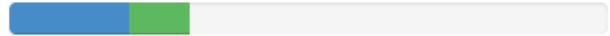
Volume Limits

Total Gibibytes 62 of 1000 GiB Used



Number of Volumes

2 of 10 Used



Cancel

Create Volume

15. In the Volumes list, check the volume you have created. Select **Manage Attachments** from the drop-down list to attach this volume to the instance.

Volumes

+ Create Volume
⇄ Accept Transfer
🗑 Delete Volumes

Displaying 2 items											
<input type="checkbox"/>	Name	Description	Size	Status	Group	Type	Attached To	Availability Zone	Bootable	Encrypted	Actions
<input checked="" type="checkbox"/>	FortiTester-Logdisk	-	60GiB	In-use	-	-	/dev/vdb on FortiTester-VM	nova	No	No	Edit Volume <div style="border: 1px solid #ccc; padding: 2px; margin-top: 5px;"> Manage Attachments Create Snapshot Change Volume Type Upload to Image Update Metadata </div>
<input type="checkbox"/>	1f7dccb1-1f4e-44c7-807a-efbdc130e8d	-	2GiB	In-use	-	-	/dev/vda on FortiTester-VM	nova	Yes	No	

Displaying 2 items

16. In the Manage Attachments window, select the instance you just shut off, and click **Attach Volume**.

Manage Volume Attachments ✕

Instance	Device	Actions
No items to display.		

Attach To Instance

Attach to Instance * ⓘ

FortiTester-VM (857ef2cb-7082-40ec-a277-775b994fc37e) ▼

Cancel

Attach Volume

17. Navigate to **Project > Network > Networks**, click **Create Network**.
18. Configure the network settings below.

Network

Enter a name for the network, check **Enable Admin State** and **Create Subnet**.

Subnet

Enter a subnet name, and a network address in CIDR format; select IPv4 for IP Version; check **Disable Gateway**.

Subnet Details

Keep the default values.

Create Network



- Network
- Subnet
- Subnet Details

Network Name

Create a new network. In addition, a subnet associated with the network can be created in the following steps of this wizard.

Enable Admin State ?

Shared

Create Subnet

Availability Zone Hints ?

nova

- Cancel
- « Back
- Next »

Click **Create** to finish the configurations.

19. Add two traffic ports in traffic network. Click the traffic network created, go to the detail page. Click **Create Port** from the **Ports** tab.

Enter a name for the port, and for other fields, just create the default ones;
Continue creating one more port.

20. Attach the traffic ports to the instance by navigating to **Project > Compute > Instances**, select the instance and click **Attach Interface** from the drop-down list.
Instances

Instance ID =
Filter
Launch Instance
Delete Instances
More Actions ▾

☑	Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
☑	FortiTester-VM	-		m1.large	-	Shutoff	nova	None	Shut Down	1 week, 1 day	Start Instance ▾

Displaying 1 item

- Create Snapshot
- Associate Floating IP
- Attach Interface
- Detach Interface
- Edit Instance
- Update Metadata
- Edit Port Security Groups
- Shelve Instance
- Resize Instance
- Lock Instance
- Hard Reboot Instance
- Rebuild Instance
- Delete Instance

21. In the **Attach Interface** window, configure the fields as below. Click **Attach Interface**.

Attach Interface ✕

The way to specify an interface *

by Port ▾

Port *

fts-port1 (17.1.0.1) - traffic-network ▾

Description:

Select the network for interface attaching.

Cancel
Attach Interface

Continue adding the second traffic port.

22. Start the instance by navigating to **Project > Compute > Instance**, click **Start Instance**.
Instances

Instance ID ▾
Filter
🔍 Launch Instance
🗑 Delete Instances
More Actions ▾

Displaying 1 item

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions	
<input type="checkbox"/> FortiTester-VM	-	traffic-network 17.1.0.1 17.1.2.2 extern-network 192.168.13.18	m1.large	-	Shutoff	us-east-1a	nova	None	Shut Down	27 minutes	Start Instance ▾

Displaying 1 item

Configuring access to FortiTester's web UI & CLI

For hypervisor deployments, after the virtual appliance is powered on, you log in to the FortiTester-VM command line interface (CLI) via the console and configure basic network settings so that you can connect to the appliance's web UI, CLI, or both through your management computer's network connection.

To configure basic network settings for FortiTester-VM deployed on a hypervisor

1. Log in to the OpenStack Dashboard.
2. Open the console of the FortiTester-VM virtual appliance.
3. At the login prompt for the local console, type:
admin
4. Press **Enter** twice. (Initially, there is no password.)
5. To configure the network and default route, for manual mode, go through **Step 6** and **Step 7**; for DHCP mode, go to **Step 8**.
6. Configure the IP address and netmask of the network interface named `mgmt`, or whichever network interface maps to the network physically connected to your management computer. Type:

```
config system interface
  edit mgmt
    set ip <address_ip> <netmask_ip>
  end
```

7. Configure a static route with the default gateway. Type:

```
config system route
  set gateway <router_ip>
end
```

where `<router_ip>` is the IP address of the gateway router.

8. Configure a dhcp mode in interface. Type:

```
config system interface
  edit mgmt
    set mode dhcp
  end
```

To show the address from dhcp server, Type:

```
show system interface
```

You should now be able to connect via the network from your management computer to `mgmt` of FortiTester-VM using:

- a web browser for the web UI (e.g. If `mgmt` has the IP address 192.168.1.1, go to <https://192.168.1.1/>)
 - an SSH client for the CLI (e.g. If `mgmt` has the IP address 192.168.1.1, connect to 192.168.1.1 on port 22.)
9. Continue by uploading the license file (See [Uploading the license on page 20](#)).

Uploading the license

To upload the license via the web UI

1. On your management computer, start a web browser.
For hypervisor installations, your computer must be connected to the same network as the hypervisor.
2. Do one of the following:
 - For hypervisor deployments, in your browser’s URL or location field, enter the IP address of `mgmt` of the virtual appliance, such as:

`https://192.168.1.99/`

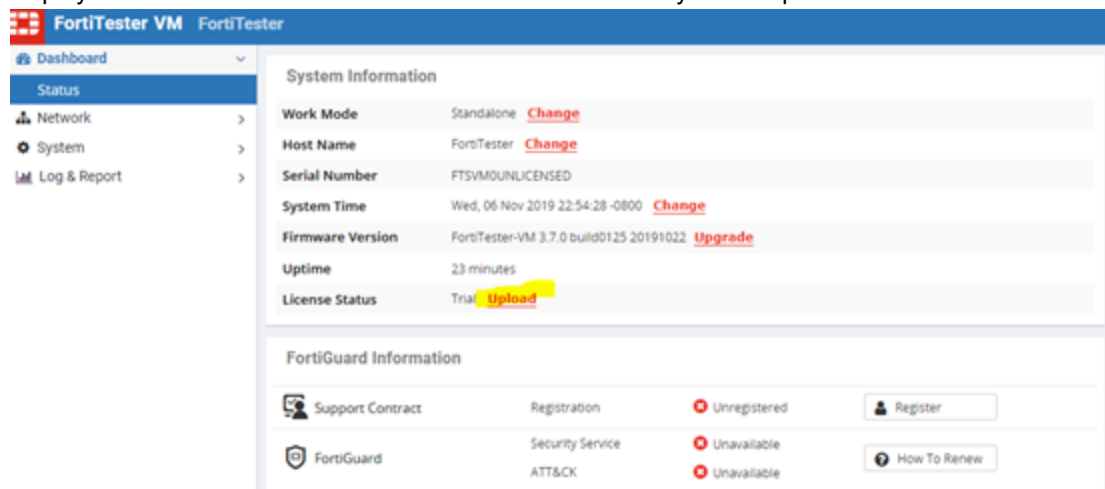
- For FortiTester-VM deployed on AWS, access the web UI using the public DNS address displayed in the instance information for the appliance in your AWS console.

For example, if the public DNS address is `ec2-54-234-142-136.compute-1.amazonaws.com`, you connect to the web UI using the following URL:

`https://ec2-54-234-142-136.compute-1.amazonaws.com/`

Your browser connects the appliance. The web UI’s login page appears.

The web UI initially displays its dashboard, **System > Dashboard > Status**. The System Information widget displays the current license status and contains a link where you can upload a license file.





FORTINET[®]



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.