OpenStack Administration Guide

FortiAnalyzer 7.2.0

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

FORTINET VIDEO LIBRARY
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

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

May 23, 2025
FortiAnalyzer 7.2.0 OpenStack Administration Guide
02-720-1077550-20251024

TABLE OF CONTENTS

Change log

Date	Change description
2022-04-11	Initial release of FortiAnalyzer 7.2.0.
2025-10-24	Initial release of FortiAnalyzer OpenStack documentation.

About FortiAnalyzer on OpenStack

This document provides information about deploying FortiAnalyzer-VM in an OpenStack environment. You can install FAZ-VM64-KVM firmware into an OpenStack environment.

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

This document does not cover configuring and operating the virtual appliance after successfully installing and starting it. For that information, see the *FortiAnalyzer Administration Guide*.

OpenStack prerequisites

This guide assumes that before deploying the FortiAnalyzer-VM virtual appliance on the OpenStack virtual platform, you have addressed the following requirements:

- The OpenStack software is installed on a physical server with sufficient resources to support the FortiAnalyzer-VM and all other VMs that you deploy on the platform. See Minimum system requirements on page 7.
- Ensure you have access to the OpenStack Horizon web interface from the computer you are uploading the image from. Alternatively, ensure you have a working environment for the OpenStack CLI.

See the following for OpenStack release series support: https://releases.openstack.org/

Licensing

Fortinet offers the FortiAnalyzer-VM with a limited, free trial license. Stackable licenses can be purchased, letting you expand your VM solution as your environment expands. You can purchase perpetual or subscription-based licenses. Perpetual licenses never expire.

For information on purchasing a FortiAnalyzer-VM license, contact your Fortinet-authorized reseller, or visit How To Buy.

When configuring your FortiAnalyzer-VM, ensure that you configure hardware settings acording to the minimum system requirements and consider future expansion. Contact your Fortinet-authorized reseller for more information.

License	GB/day of logs
Trial License	1
VM-GB1	+1
VM-GB5	+5

License	GB/day of logs
VM-GB25	+25
VM-GB100	+100
VM-GB500	+500
VM-GB2000	+2000

See Minimum system requirements on page 7.

See also the FortiAnalyzer product datasheet.

Trial license

With a FortiCare account, FortiAnalyzer-VM includes a free limited non-expiring trial license.

The free trial license includes support for 3 ADOMs and 1 GB/day of logs.

The free trial license does not include services or support.

You can activate the trial license when you connect to the GUI for the FortiAnalyzer-VM. Full-feature products and services are available for purchase with an add-on license. See Connecting to the GUI and enabling a trial license on page 14.

Add-on license

You must activate a trial license before you can upgrade FortiAnalyzer-VM to a purchased add-on license.

See also the FortiAnalyzer VM Trial License Guide on the Document Library.

Licensing in an air-gap environment

Enabling the trial license requires internet access. This is used to connect to FortiCloud and your FortiCare account on the Technical Supoprt Site. It is also used to receive the license agreement. If you are licensing in an air-gap environment, see Licensing in an air-gap environment in the FortiAnalyzer Administration Guide.

Preparing for deployment

You can prepare for deployment by reviewing the following information:

- Minimum system requirements
- Registering your FortiAnalyzer-VM
- Downloading a deployment package

Minimum system requirements

FortiAnalyzer-VM has a minimum requirement of 4 CPU, 8 GB of RAM, and 500 GB of disk storage. For v7.2.2 and later, the minimum requirement for RAM is increased to 16 GB.

The following table lists the minimum system requirements for your VM hardware, based on your VM's analytic sustained rate.

Analytic sustained rate (logs/sec)	VM hardware requirements		
	RAM (GB)	CPU cores	IOPS
3000	16	4	300
4000	16	4	400
5000	16	4	500
6000	16	8	600
7000	16	8	700
8000	16	8	800
9000	16	8	900
10000	16	8	1000
20000	32	16	2000
30000	32	16	3000
40000	64	32	4000
50000	64	32	5000

You can calculate the collector sustained rate by multiplying the analytic sustained rate by 1.5.

This table does not take into account other hardware specifications, such as bus speed, CPU model, or storage type.

Using Management Extension Applications (MEA) requires more resources. For details, see the FortiAnalyzer Release Notes.

Registering your FortiAnalyzer-VM

After placing an order for a FortiAnalyzer-VM, you receive a license registration code to the email address that you used in the order form. Use the license registration code provided to register the FortiAnalyzer-VM with Customer Service & Support.

Upon registration, you can download the license file. You need this file to activate your FortiAnalyzer-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 are fully functional.

For more information on registering assets in FortiCloud, see the FortiCloud Asset Management Guide.

To register your FortiAnalyzer:

1. Ensure that you have the following items needed to complete the procedure:
   - License registration code emailed to you after you placed an order for a FortiAnalyzer-VM
   - Support contract number
   - A static FortiAnalyzer IPv4 address
2. Log in to FortiCloud using a support account, or create an account.
3. In the main page, select *Register Now*.
4. Enter the registration code from the FortiAnalyzer license certificate emailed to you, select the *End User Type*, then click *Next*.
5. Enter an optional product description and the static IP address that will be used during license validation, then click *Next*.

As a part of the license validation process, the FortiAnalyzer-VM compares its configured IP addresses with the IP address information in the license file. The license must be associated with an IP address assigned to one of the interfaces on the FortiAnalyzer. If a new license has been imported or the FortiAnalyzer's associated IP address has changed, you must reboot the FortiAnalyzer for the system to validate the change and operate with a valid license.

The FortiCloud portal does not support IPv6 for FortiAnalyzer license validation. You must specify an IPv4 address in the support portal and the port management interface.

6. Review your asset details and accept the terms of the contract, then click *Confirm*.
7. From the *Registration Completed* page, you can download the FortiAnalyzer license file, select *Register More* to register another FortiAnalyzer, or select *Done* to complete the registration process.
8. Select *License File Download* to save the license file (`.lic`) to your management computer.
   - In FortiCloud, you can also download your license file by selecting your FortiAnalyzer in *Products > Product List* and selecting the license file under *Product Information*.

Downloading a deployment package

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

To deploy a FortiAnalyzer into OpenStack, you must download the KVM image files: `FAZ_VM64_KVM-vX.-buildxxxx-FORTINET.out.kvm.zip`.

You can download the *FortiAnalyzer Release Notes* and MIB file from this directory. The Fortinet Core MIB file is located in the *FortiAnalyzer > Download* tab.

Download the `.out` file to upgrade your existing FortiAnalyzer installation.

To download deployment packages:

1. Log in to the FortiCloud portal and select your account if applicable.
2. From the top menu bar, select *Support > Firmware Downloads*.
3. From the *Select Product* dropdown, select *FortiAnalyzer*. Then select the *Download* tab underneath the dropdown.
4. Browse to the appropriate directory for the version that you would like to download.
5. Download the appropriate firmware image and release notes to your management computer.
   To deploy a FortiAnalyzer into OpenStack, you must download the KVM image files (*.out.kvm.zip*).

   

   You can use your browser's built-in find feature to quickly find the files you need. Use `Ctrl+F` or `CMD+F` and search for `VM64_KVM`.

6. Extract the contents of the package to a new folder on your management computer.

Deployment

Prior to deploying the FortiAnalyzer, the VM platform must be installed and configured so that it is ready to create virtual machines. The installation instructions for FortiAnalyzer 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 FortiAnalyzer appliance for the first time, you might need to adjust virtual disk sizes and networking settings. The first time you start FortiAnalyzer, 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 FortiAnalyzer GUI (see Enabling GUI access on page 14).

If the FortiAnalyzerdoes not have a valid Logical Volume Management (LVM) configuration, the LVM service will not start automatically upon boot-up when the disk already contains data. To manually enable the service, use the `execute lvm start` CLI command.

Deploying FortiAnalyzer on OpenStack

After you download the `FAZ_VM64_KVM-vX-buildxxxx-FORTINET.out.kvm.zip` file and extract the virtual hard drive image file, you can create the VM in your OpenStack environment.

Upload the FortiAnalyzer image to OpenStack

You can upload the FortiAnalyzer image using the OpenStack dashboard (Horizon) or the OpenStack CLI.

To upload the image using the OpenStack dashboard (Horizon):

1. In the OpenStack dashboard, go to *Project* > *Compute* > *Images*.
2. Click *Create Image*.
3. In the *Create An Image* dialog, configure the following:

Image Name	Enter a name for the image.
Image Source	Select *Image File* and upload the QCOW2 file that was downloaded and extracted as part of Downloading a deployment package on page 9.
Format	Select QCOW2.

4. Configure the remaining options according to your needs.
   Note that the *Minimum Disk* and *Minimum RAM* should meet the minimum requirements for FortiAnalyzer VM outlined in Minimum system requirements on page 7.

5. Click *Create Image*.

To upload the image using the OpenStack CLI:

1. Open the terminal in which you have access to the OpenStack CLI.
2. Go to the folder containing the image.
   For example,
   ```
   cd <folder containing the contents of the deployment package>
   ```
3. Use the following command to upload the image:
   ```
   openstack image create --disk-format qcow2 --container-format bare --public --file ./<QCOW2
   file in the deployment package> --min-disk <integer> --min-ram <integer> <image name> --
   fit-width
   ```
   Note that the `--min-disk` and `--min-ram` should meet the minimum requirements for FortiAnalyzer VM outlined in Minimum system requirements on page 7.
   An output will display once the upload is finished.

Create a network for the FortiAnalyzer VM

You must create a network and subnet for the FortiAnalyzer VM in OpenStack. The following steps are completed in the OpenStack dashboard (Horizon), but the network and subnet can also be created using the OpenStack CLI.

To create the network using the OpenStack dashboard (Horizon):

1. In the OpenStack dashboard, go to *Project* > *Network* > *Networks*.
   The *Create Network* dialog displays.
2. In the *Network* tab, configure the following and then click *Next*.

Network Name	Enter a name for the FortiAnalyzer VM network.
Enable Admin State	Enabled.
Create Subnet	Enabled.

3. In the *Subnet* tab, configure the following and then click *Next*.

Subnet Name	Enter a name for the subnet.
Network Address	Enter the CIDR.
IP Version	Select IPv4.
Gateway IP	Enter a gateway IP or select *Disable Gateway* if you do not want to use a gateway.

4. In the *Subnet Details* tab, configure additional attributes as needed and then click *Create*.

Configure security groups

Security groups in OpenStack are used to control inbound and outbound traffic to and from the FortiAnalyzer VM instance.

To configure security groups in the OpenStack dashboard (Horizon):

1. In the OpenStack dashboard, go to *Project* > *Network* > *Security Groups*.
2. Click *Create Security Group*.
   The *Create Security Group* dialog displays.
3. Enter a name and description for the security group.
4. Click *Create Security Group*.
5. Select the security group and click *Manage Rules*.
6. To add a new rule, click *Add Rule*.
7. Configure rules according to your needs for the FortiAnalyzer.
   For example, you may need to configure rules to allow access for the following:

Direction	Ports/Protocols	Purpose
Ingress	TCP 22	SSH access
Ingress	TCP 80	HTTP
Ingress	TCP 443	HTTPS, which is required for GUI access FortiAnalyzer VM

For more information about FortiAnalyzer ports and protocols, see FortiAnalyzer*Ports and Protocols* on the Fortinet Document Library.

Launch the FortiAnalyzer VM instance

Once you have created the network and security groups, you can launch the FortiAnalyzer VM instance in OpenStack. Before launching the instance, you may also need to configure a flavor in OpenStack that meets your needs.

To create a flavor in the OpenStack dashboard (Horizon):

Flavors define the CPU, memory, and storage resources that can be assigned to instances. If default flavors are available in your OpenStack, you can skip this step and select an appropriate default flavor when launching the FortiAnalyzer VM instance.

1. Go to *Admin* > *Compute* > *Flavors*.
2. Click *Create Flavor*.
3. In the *Create Flavor* dialog, configure the following according to your needs.
   The flavor must also meet the specifications defined in Minimum system requirements on page 7.

Name	Enter a name for the flavor.
VCPUs	Enter the number of virtual CPUs.
RAM	Enter the amount of RAM in MB.
Root Disk	Enter the size of the root disk in GB.

4. Click *Create Flavor*.

Once the instance starts, you can proceed with the initial configuration. See Configuring initial settings on page 13.

To launch the FortiAnalyzer instance from the OpenStack dashboard (Horizon):

1. In the OpenStack dashboard, go to *Project* > *Compute* > *Instances*.
2. With no instance selected, click *Launch Instance*.
   The *Launch Instance* dialog displays.
3. Configure the following options:

Instance Name	Enter a name for the instance.
Source	Select *Image* and choose the FortiAnalyzer VM image. For more information about uploading the image, see Upload the FortiAnalyzer image to OpenStack on page 10.
Flavor	Select a flavor that meets the requirements for your FortiAnalyzer VM. You can use a default flavor, if available, or you can create a new flavor according to your needs prior to launching the instance.
Networks	Select the network for the FortiAnalyzer VM. For more information about creating a network, see Create a network for the FortiAnalyzer VM on page 11.
Security Groups	In the *Security Groups* tab, select the security group(s) you want to assign to the instance. For more information about creating security groups and rules, see Configure security groups on page 12.

4. Click *Launch Instance*.

Configuring initial settings

Before you can connect to the FortiAnalyzer-VM, you must configure basic network settings via the CLI console. Once configured, you can connect to the FortiAnalyzer GUI.

Enabling GUI access

To enable GUI access to the FortiAnalyzer, you must configure the IP address and network mask of the appropriate port on the FortiAnalyzer. The following instructions use port 1.

You can determine the appropriate by matching the network adapter's MAC address and the `HWaddr` that the CLI command `diagnose fmnetwork interface list` provides.

To configure the port1 IP address and netmask:

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

```
config system interface
   edit port1
      set ip <IP address> <netmask>
end
```

The port management interface should match the first network adapter and virtual switch that you have configured in the hypervisor VM settings.

4. To configure the default gateway, enter the following commands:

```
config system route
   edit 1
      set device port1
      set gateway <gateway_ipv4_address>
end
```

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

Connecting to the GUI and enabling a trial license

Once you have configured a port's IP address and network mask, you can connect to the GUI by using a web browser.

Enabling the trial license requires internet access. This is used to connect to FortiCloud and your FortiCare account on the Technical Supoprt Site. It is also used to receive the license agreement. If you are licensing in an air-gap environment, see Licensing in an air-gap environment in the FortiAnalyzer Administration Guide.

To connect to the GUI and enable a trial license:

1. Launch a web browser, and enter the IP address you configured for the port management interface.
2. At the login page, select *Free Trial*, and click *Login with FortiCloud* to start the process of activating your free trial license.
   If you do not have a FortiCloud account, click *Register with FortiCloud* to create one.

See also the FortiAnalyzer VM Trial License Guide on the Document Library.

Upgrading to an add-on license

You must activate a trial license before you can upgrade FortiAnalyzer-VM to a purchased add-on license.

See also the FortiAnalyzer VM Trial License Guide on the Document Library.

Configuring your FortiAnalyzer

Once the FortiAnalyzer license has been validated, you can configure your device.

If the amount of memory or number of CPUs is too small for the VM, or if the allocated hard drive space is less than the licensed VM storage volume, warning messages show in the GUI in the *System Resources* widget on the dashboard and in the *Notification* list.

For more information on configuring your FortiAnalyzer, see the FortiAnalyzer Administration Guide.

www.fortinet.com

Copyright© 2025 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 Chief Legal Officer, 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.