FortiAnalyzer VM - Install Guide for KVM

Version 6.0

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 COOKBOOK
https://cookbook.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: techdocs@fortinet.com

March 18, 2019
FortiAnalyzer VM 6.0 Install Guide for KVM
05-600-480495-20190318

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-04-18	Initial release.
2018-09-07	VM deployment package versions updated.
2019-03-18	Added Minimum system requirements on page 7.

About FortiAnalyzer VM on KVM

This document provides information about deploying a FortiAnalyzer virtual appliance in Linux KVM server environments.

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

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

Licensing

Fortinet offers the FortiAnalyzer VM in a stackable license model. This model allows you to expand your VM solution as your environment expands. Virtual appliance licenses are also perpetual - they never expire.

For information on purchasing a FortiAnalyzer VM license, contact your Fortinet Authorized Reseller, or visit https://www.fortinet.com/how_to_buy/.

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

	GB / Day of logs	Storage Capacity
VM-BASE	1	500GB
VM-GB1	+1	+500GB
VM-GB5	+5	+3TB
VM-GB25	+25	+10TB
VM-GB100	+100	+24TB
VM-GB500	+500	+48TB
VM-GB2000	+2000	+100TB

See also Minimum system requirements on page 7 and the FortiAnalyzer product data sheet:

https://www.fortinet.com/products/management.html#models-specs

Evaluation license

FortiAnalyzer VM includes a free, full featured 15 day trial license. No activation is required for the built-in evaluation license.

The trial period begins the first time you start the FortiAnalyzer VM. When the trial expires, all functionality is disabled until you upload a license file.

Technical support is not included with the 15-day evaluation.

Contact your Fortinet Reseller to request a full evaluation (60-days) license.

Preparing for deployment

You can prepare for deployment by reviewing the following information:

- Minimum system requirements
- Registering your FortiAnalyzer VM
- Downloading deployment packages

Minimum system requirements

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

Analytic Sustained Rate (logs/sec)	VM Hardware Requirements		
	RAM (GB)	CPU cores	IOPS
3000	8	4	300
4000	8	4	400
5000	8	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

The collector sustained rate can be calculated 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.

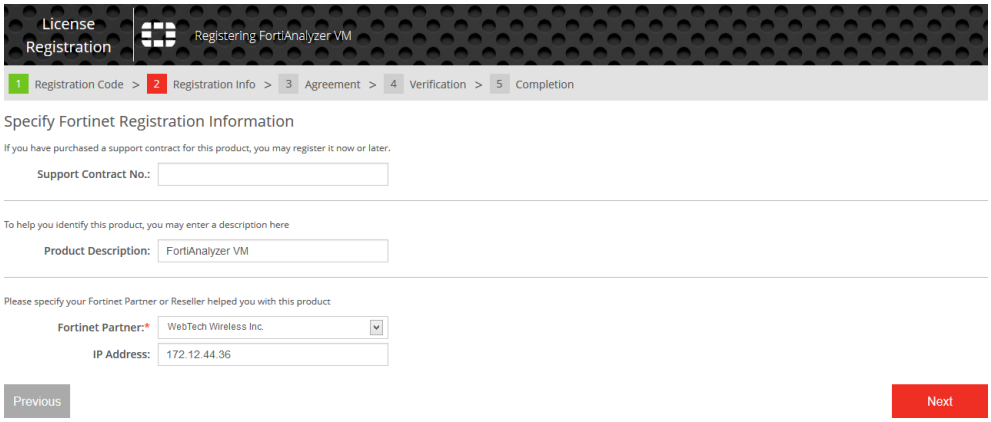
Registering your FortiAnalyzer VM

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

Upon registration, you can download the license file. You will need this file to activate your 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 will be fully functional.

To register your FortiAnalyzer VM:

1. Ensure that you have the following items needed to complete the procedure:
   - License registration code that was emailed to you after you placed an order for FortiAnalyzer VM
   - Support contract number
   - IPv4 address for the FortiAnalyzer VM
2. Log into the Fortinet Customer Service & Support portal at https://support.fortinet.com/ using an existing support account, or click *Create an Account* to create a new account.
3. In the toolbar, select *Asset* > *Register/Renew*. The *Registration Wizard* opens.
4. Enter the registration code from the FortiAnalyzer VM License Certificate that was emailed to you, select the end user type, and then click *Next*. The *Registration Info* page is displayed.

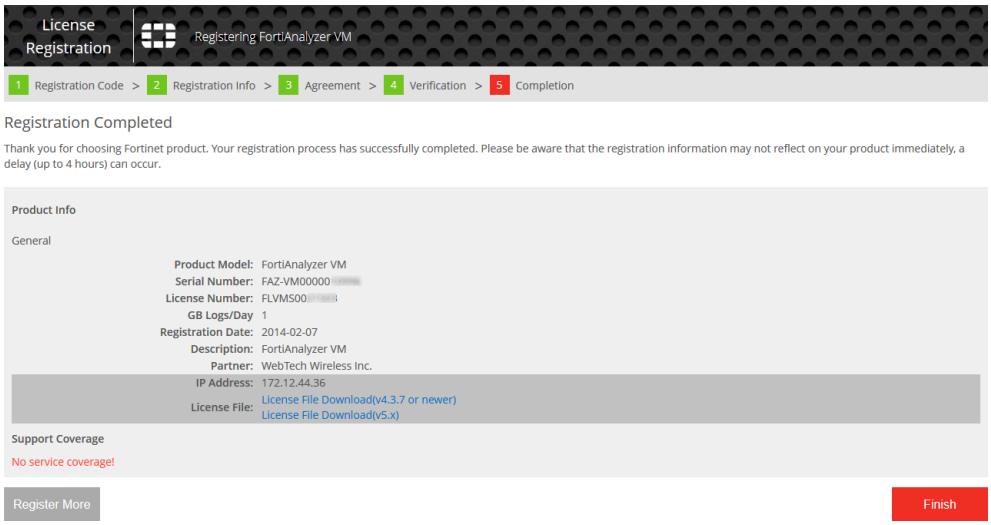


5. Enter your support contract number, product description, Fortinet Partner, and IP address in the requisite fields, then select *Next*.

As a part of the license validation process, FortiAnalyzer VM compares its configured IP addresses with the IP information in the license file. The license must be associated with an IP address assigned to one of the interfaces on the FortiAnalyzer VM. If a new license has been imported or the FortiAnalyzer VM's associated IP address has been changed, the FortiAnalyzer 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 FortiAnalyzer VM license validation. You must specify an IPv4 address in both the support portal and the port management interface.

6. 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.
7. The verification page displays the product entitlement. Select the checkbox to indicate that you accept the terms then select *Confirm* to submit the request.

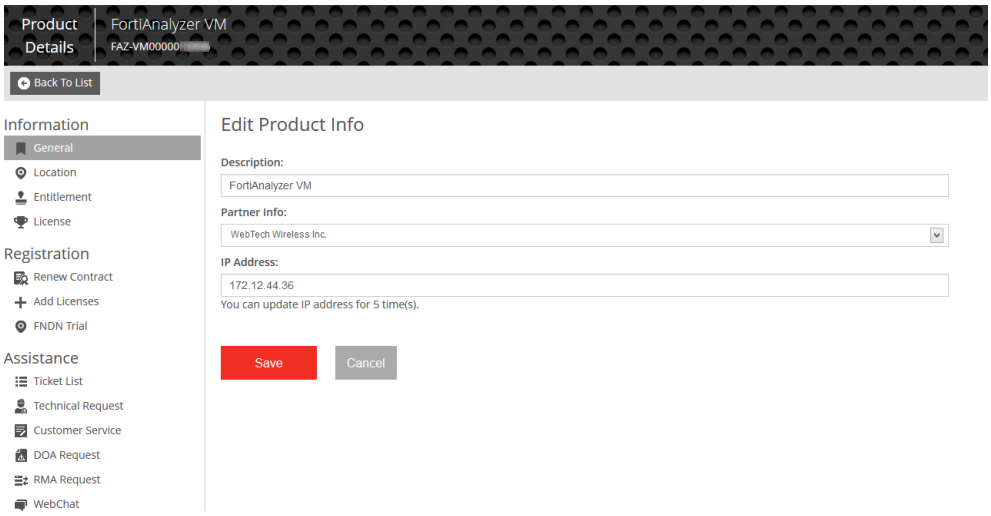


8. From the *Registration Completed* page, you can download the FortiAnalyzer VM license file, select *Register More* to register another FortiAnalyzer VM, or select *Finish* to complete the registration process.
   Select *License File Download* to save the license file (`.lic`) to your management computer. For instructions on uploading the license file to your FortiAnalyzer VM via the GUI, see Uploading the license file on page 17 .

Editing FortiAnalyzer VM IP addresses

To edit the FortiAnalyzer VM IP address:

1. In the toolbar, select *Asset* > *Manage/View Products* to open the *View Products* page.
2. Select the FortiAnalyzer VM serial number to open the *Product Details* page.
3. Click *Edit* to change the description, partner information, and IP address of your FortiAnalyzer 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 FortiAnalyzer 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. For instructions on uploading the license file to your FortiAnalyzer VM via the GUI, see Uploading the license file on page 17.

Deployment package for Linux KVM

FortiAnalyzer VM deployment packages are included with firmware images on the Customer Service & Support site. The following table list the available VM deployment package.

VM Platform	Deployment File
Linux KVM RedHat 7.1	`FAZ_VM64_KVM-vX-buildxxxx-FORTINET.out.kvm.zip`

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

- `faz.qcow2`: TheFortiAnalyzer VM system hard disk in QCOW2 format.
  The log disk and virtual hardware settings have to be configured manually.

For more information FortiAnalyzer VM, see the FortiAnalyzer VM datasheet available on the Fortinet web site:

https://www.fortinet.com/products/management/fortianalyzer.html.

Downloading deployment packages

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. For example, the `FAZ_VM64_HV-vX-buildxxxx-FORTINET.out.hyperv.zip` image, found in the 5.6.0 directory, is specific to the 64bit Microsoft Hyper-V Server virtualization environment.

You can download the *FortiAnalyzer Release Notes* and MIB file from this directory. The Fortinet Core MIB file is located in the FortiAnalyzer 6.0.0 directory.

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

To download deployment packages:

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

Deployment

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

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

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

If the FortiAnalyzer VMdoes 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 VM on KVM

Once you have downloaded the `FAZ_VM64_KVM-vX-buildxxxx-FORTINET.out.kvm.zip` file and extracted the virtual hard drive image file, you can create the virtual machine in your KVM environment.

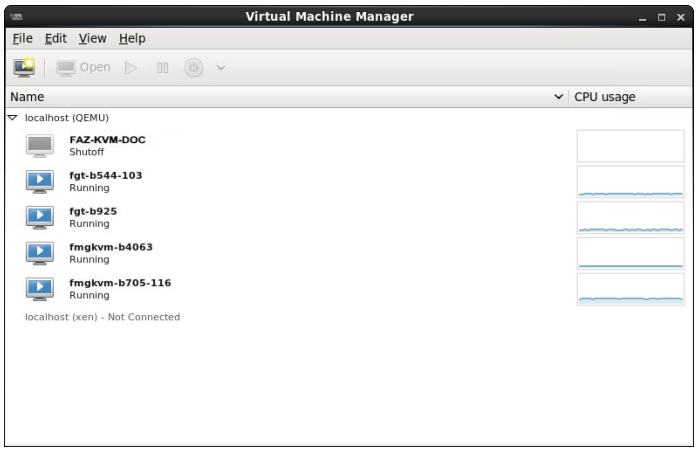
The following topics are included in this section:

- Creating the virtual machine
- Configuring hardware settings
- Starting the virtual machine

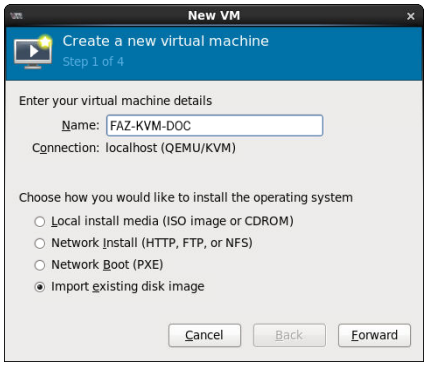
Creating the virtual machine

To create the virtual machine:

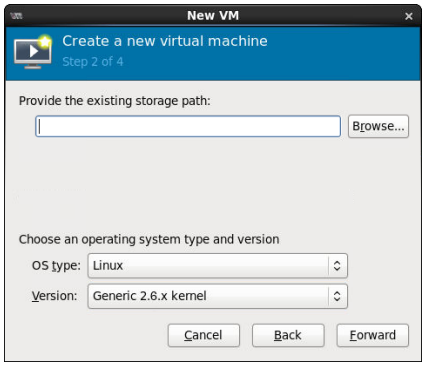
1. Launch Virtual Machine Manager (virt-manager) on you KVM host server. The *Virtual Machine Manager* home page opens.



2. On the toolbar, click *Create a new virtual machine*.

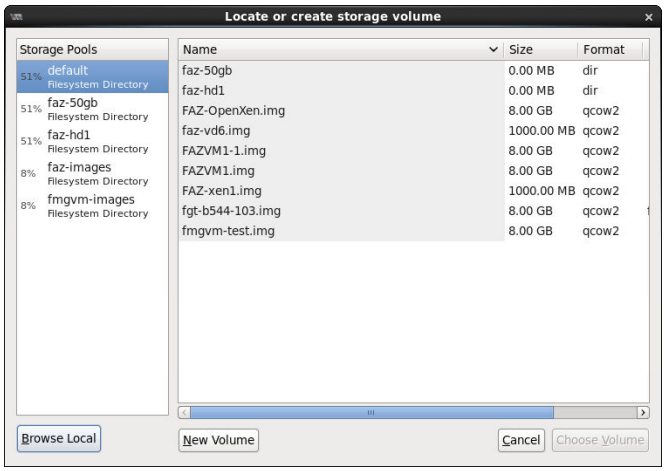


3. Enter a name for the virtual machine, such as *FAZ-KVM-DOC*.
4. Ensure that *Connection* is *localhost*, select *Import existing disk image*, then click *Forward* to continue.

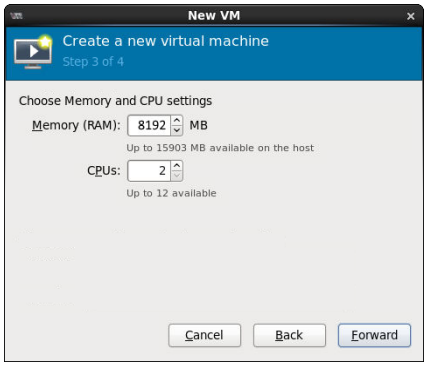


5. In the *OS Type* field select *Linux*.
6. In the *Version* field select *Generic 2.6.x kernel*. You may have to first select *Show all OS options*.

7. Click *Browse* to locate the storage volume.



8. If you copied the *faz.qcow2* file to `/var/lib/libvirt/images` it will be shown on the right. If you saved it elsewhere on the server, click *Browse Local* to find it.
9. Once the file has been located, click *Choose Volume*, then click *Forward*.



10. Specify the amount of memory and the number of CPUs to allocate to this VM, then select *Forward*. To determine your required memory, see Minimum system requirements on page 7.
11. Expand the *Advanced options* section. By default, a new virtual machine includes one network adapter. Select a network adapter on the host computer.
    Optionally, set a specific MAC address for the virtual network interface.
12. Set *Virt Type* to *virtio* and set *Architecture* to *qcow2*.
13. Click *Finish* to create the VM.

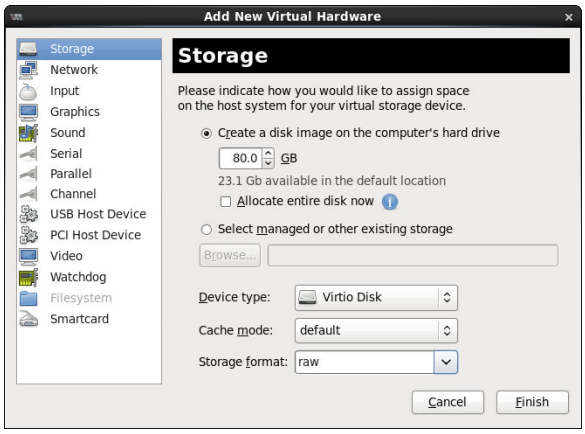
Configuring hardware settings

Before powering on your FortiAnalyzer VM you must configure virtual disks and at least four network interfaces.

To configure settings on the server:

1. In the Virtual Machine Manager, locate the name of the VM, then click *Open* on the toolbar.
2. In the Virtual Machine window, select *Show virtual hardware details*.
3. Click *Add Hardware* to open the *Add Hardware* window

4. Select *Storage*.



5. Select *Create a disk image on the computer's harddrive*, and set the size to 80GB.

If you know your environment will expand in the future, or if you will be using ADOMs, it is recommended to add hard disks larger than 500GB. This will allow your environment to be expanded as required while not taking up more space than is needed. See Licensing on page 5 for more information.

The FortiAnalyzer VM allows for 12 virtual log disks to be added to a deployed instance. When adding additional hard disks use the following CLI command to extend the LVM logical volume:

```
execute lvm start
execute lvm extend <arg ..>
```

6. Enter the following information:

Device Type	Virtio disk
Cache mode	writethrough
Storage format	raw

7. Select *Network* to add more network interfaces. The *Device Model* must be *Virtio*.

A new VM includes one network adapter by default. More can be added through the *Add Hardware* window. FortiAnalyzer VM supports up to four network adapters. You can configure network adapters to connect to a virtual

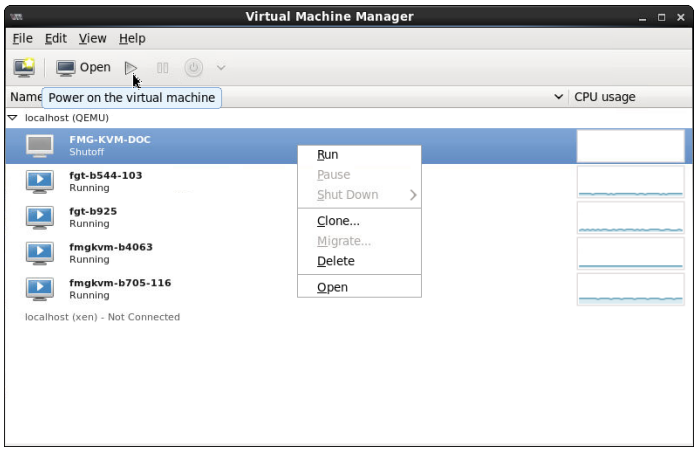
switch or to network adapters on the host computer.

8. Click *Finish*.

Starting the virtual machine

You can now proceed to power on your FortiAnalyzer VM.

1. Right-click on the FortiAnalyzer VM and select *Run*, or
2. Select the FortiAnalyzer VM from the list of VMs, then click *Power on the virtual machine* from the toolbar.



Once the VM has started, proceed with the initial configuration. See Configuring initial settings on page 16.

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 VM GUI and upload the FortiAnalyzer 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

Enabling GUI access

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

The appropriate port can be determined by matching the MAC address of the network adapter and the `HWaddr` provided by the CLI command `diagnose fmnetwork interface list`.

To configure the port1 IP address and netmask:

1. In your hypervisor manager, start the FortiAnalyzer VM and access the console window. You might need to press *Enter* to see the login prompt.
2. At the FortiAnalyzer VM login prompt, enter the username *admin*, then press *Enter*. By default, there is no password.
3. Using CLI commands, configure the port1 IP address and netmask.

```
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 virtual machine 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 VM license validation. You must specify an IPv4 address in both the support portal and the port management interface.

Connecting to the GUI

Once you have configured a port's IP address and network mask, launch a web browser and enter the IP address you configured for the port management interface. At the login page, enter the user name `admin` and no password, then select *Login*.

The GUI will open with an *Evaluation License* dialog box.

Uploading the license file

FortiAnalyzer VM includes a free, full featured 15 day trial.

Before using the FortiAnalyzer VM, you must enter the license file that you downloaded from the Customer Service & Support portal when you registered your FortiAnalyzer VM. See Registering your FortiAnalyzer VM on page 8.

To upload the license via the CLI:

1. Open the license file in a text editor and copy the VM license string.
2. In a FortiAnalyzer VM console window, enter the following:

```
execute add-vm-license <"vm license string">
```

See the *FortiAnalyzer CLI Reference*, available from the Fortinet Document Library, for more details on using this command.

To upload the license file via the GUI:

1. In the *Evaluation License* dialog box, select *Enter License*.
   Optionally, you can also select *Upload License* in the *License Information* dashboard widget.
2. In the license upload page, click *Browse*, locate the VM license file (`.lic`) on your computer, then click *OK* to upload the license file.
   A reboot message will be shown, then the FortiAnalyzer VM system will reboot and load the license file.
3. Refresh your browser and log back into the FortiAnalyzer VM with username *admin* and no password.
   The VM registration status appears as valid in the *License Information* widget once the license has been validated.

As a part of the license validation process, FortiAnalyzer VM compares its IP address with the IP information in the license file. If a new license has been imported or the FortiAnalyzer's IP address has been changed, the FortiAnalyzer 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 FortiAnalyzer VM do not match, you will receive an error message when you log back into the VM.

If this occurs, you will need to change the IP address in the Customer Service & Support portal to match the management IP and re-download the license file. To change the management IP address, see Editing FortiAnalyzer VM IP addresses on page 9

After an invalid license file has been loaded onto the FortiAnalyzer VM, the GUI will be locked until a valid license file is uploaded. A new license file can be uploaded via the CLI.

Configuring your FortiAnalyzer VM

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

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

For more information on configuring your FortiAnalyzer VM, see the *FortiAnalyzer Administration Guide* available in the Fortinet Document Library.

Index