



FortiAnalyzer VM - Install Guide for Hyper-V

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 Hyper-V

05-600-480495-20190318

TABLE OF CONTENTS

Change Log	4
About FortiAnalyzer VM on Microsoft Hyper-V	5
Licensing	5
Evaluation license	5
Preparing for deployment	7
Minimum system requirements	7
Registering your FortiAnalyzer VM	8
Editing FortiAnalyzer VM IP addresses	9
Deployment package for Microsoft Hyper-V	10
Downloading deployment packages	10
Deployment	12
Deploying FortiAnalyzer VM on Hyper-V	12
Creating the virtual machine	13
Configuring hardware settings	14
Starting the virtual machine	17
Configuring initial settings	18
Enabling GUI access	18
Connecting to the GUI	19
Uploading the license file	19
Configuring your FortiAnalyzer VM	20
Index	21

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 Microsoft Hyper-V

This document provides information about deploying a FortiAnalyzer virtual appliance in Microsoft Hyper-V 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.

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

License Registration Registering FortiAnalyzer VM

1 Registration Code > 2 Registration Info > 3 Agreement > 4 Verification > 5 Completion

Registration Completed

Thank you for choosing Fortinet product. Your registration process has successfully completed. Please be aware that the registration information may not reflect on your product immediately, a delay (up to 4 hours) can occur.

Product Info

General

Product Model: FortiAnalyzer VM
 Serial Number: FAZ-VM00000
 License Number: FLVM500
 GB Logs/Day: 1
 Registration Date: 2014-02-07
 Description: FortiAnalyzer VM
 Partner: WebTech Wireless Inc.
 IP Address: 172.12.44.36
 License File: [License File Download\(v4.3.7 or newer\)](#)
[License File Download\(v5.x\)](#)

Support Coverage
 No service coverage!

[Register More](#) [Finish](#)

- 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 19](#).

Editing FortiAnalyzer VM IP addresses

To edit the FortiAnalyzer VM IP address:

- In the toolbar, select *Asset > Manage/View Products* to open the *View Products* page.
- Select the FortiAnalyzer VM serial number to open the *Product Details* page.
- Click *Edit* to change the description, partner information, and IP address of your FortiAnalyzer VM from the *Edit Product Info* page.

Product Details FortiAnalyzer VM
 FAZ-VM00000

[Back To List](#)

Information

General

Location

Entitlement

License

Registration

Renew Contract

Add Licenses

FNDN Trial

Assistance

Ticket List

Technical Request

Customer Service

DOA Request

RMA Request

WebChat

Edit Product Info

Description:
 FortiAnalyzer VM

Partner Info:
 WebTech Wireless Inc.

IP Address:
 172.12.44.36
 You can update IP address for 5 time(s).

[Save](#) [Cancel](#)

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 19](#).

Deployment package for Microsoft Hyper-V

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
Microsoft Hyper-V Server 2012 and 2016	FAZ_VM64_HV-vX-buildxxxx-FORTINET.out.hyperv.zip

The .out.hyperv.zip file contains:

- faz.vhd: The FortiAnalyzer VM system hard disk in VHD 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 18](#)).

If the FortiAnalyzer VM does 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 Hyper-V

Once you have downloaded the `FAZ_VM64_HV-vX-buildxxxx-FORTINET.out.hyperv.zip` file and extracted the package contents to a folder on your Microsoft server, you can deploy the VHD package to your Microsoft Hyper-V environment.

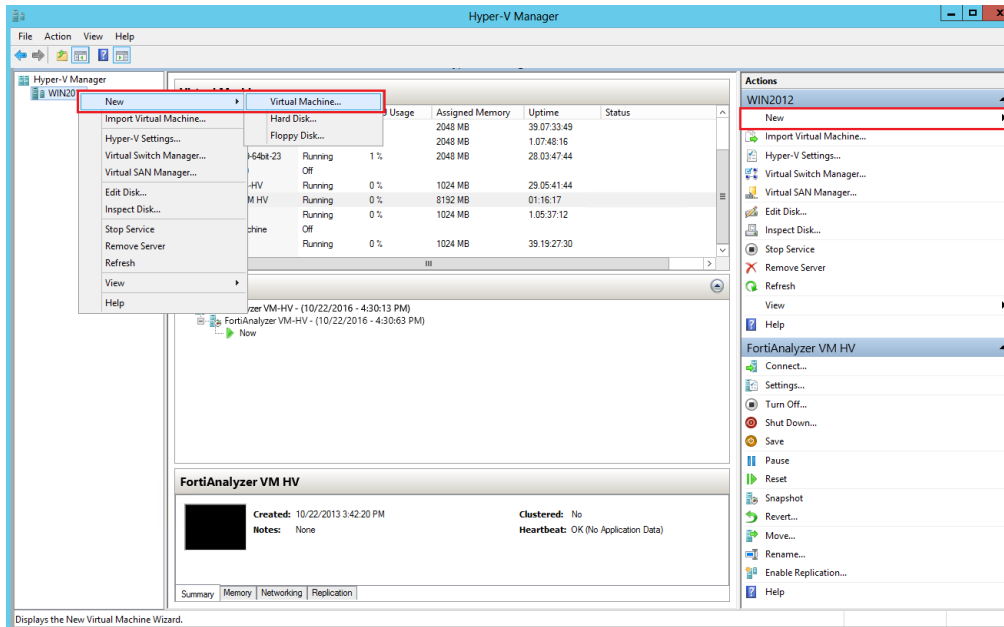
The following topics are included in this section:

- [Creating the virtual machine](#)
- [Configuring hardware settings](#)
- [Starting the virtual machine](#)

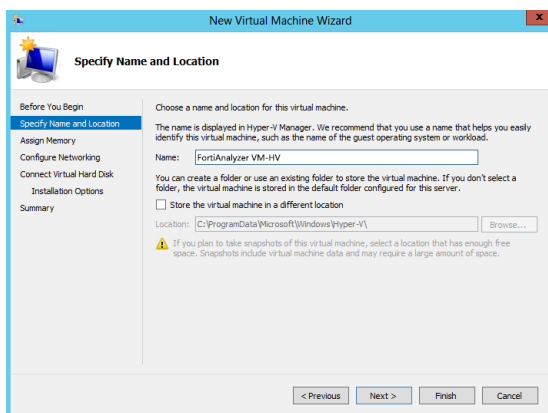
Creating the virtual machine

To create the virtual machine:

1. Launch the Hyper-V Manager in your Microsoft server. The *Hyper-V Manager* home page opens.
2. Select the server in the right-tree menu. The server details page opens.

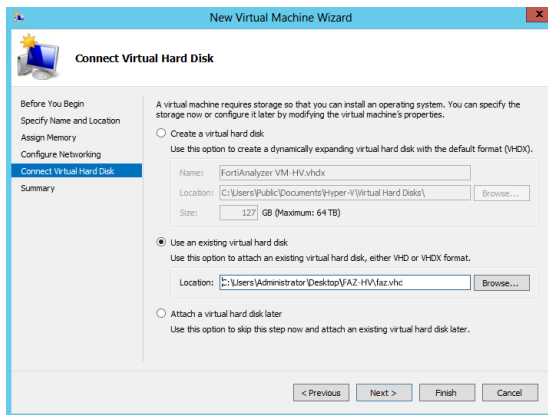


3. Right-click the server and select *New > Virtual Machine*, or in the *Actions* menu, select *New > Virtual Machine*. The *New Virtual Machine Wizard* opens.
4. Click *Next* to create a virtual machine with a custom configuration. The *Specify Name and Location* page opens.



5. Enter a name for this VM. The name is displayed in the Hyper-V Manager.
6. Click *Next* to continue to the *Assign Memory* page.
7. Specify the amount of memory to allocate to this virtual machine. See [Minimum system requirements on page 7](#) to determine your required memory.
8. Click *Next* to continue to the *Configure Networking* page.
9. You must configure network adapters in the *Settings* page.
Each new VM includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected. FortiAnalyzer VM requires four network adapters.

10. Select **Next** to continue to the *Connect Virtual Hard Disk* page.

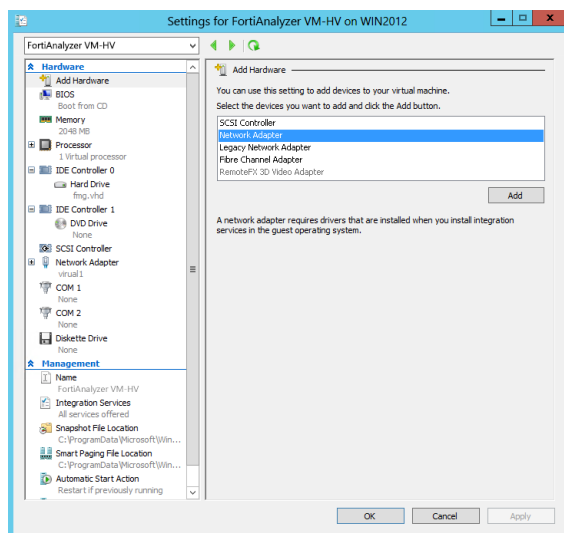


11. Select to use an existing virtual hard disk and browse for the `faz.vhdx` file that you downloaded from the [Fortinet Customer Service & Support](#) portal.
12. Select **Next** to continue to the *Summary* page.
13. To create the virtual machine and close the wizard, select **Finish**.

Configuring hardware settings

Before powering on your FortiAnalyzer VM you must configure the virtual processors, memory, network adapters, and hard disk to match your FortiAnalyzer VM license. See [Licensing on page 5](#) for FortiAnalyzer VM license information.

To open the *Settings* page, in the Hyper-V Manager, right-click on the name of the virtual machine and select *Settings*, or select the virtual machine then click *Settings* from the *Actions* menu.



To configure virtual memory:

1. In the *Settings* page, select *Memory* from the *Hardware* menu. The *Memory* page is displayed.
2. Configure the memory for the VM. See [Minimum system requirements on page 7](#) to determine your required memory.
3. Click **Apply** to save your settings.

To configure virtual processors:

1. In the *Settings* page, select *Processor* from the *Hardware* menu. The *Processor* page is displayed.

2. Configure the number of virtual processors for the VM. Optionally, you can use resource controls to balance resources among VMs.
3. Click *Apply* to save your settings.

To configure network adapters:

1. In the *Settings* page, select *Add Hardware* from the *Hardware* menu.
2. From the device list, select *Network Adapter*, then click *Add*. The *Network Adapter* page opens.

3. Manually configure four network adapters in the settings page. For each network adapter, select a virtual switch from the drop-down list.
4. Click *Apply* to save your settings.

To configure the virtual hard disk:



The FortiAnalyzer VM requires at least two virtual hard disks. Before powering on the FortiAnalyzer VM, you must add at least one more virtual hard disk. The default hard drive, `faz.vhd`, contains the operating system. The second hard drive is used for logs.



If you know your environment will expand in the future, it is recommended to add hard disks larger than the 500GB base license requirement. This will allow your environment to be expanded as required while not taking up more space in the Storage Area Network (SAN) 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 >>
```

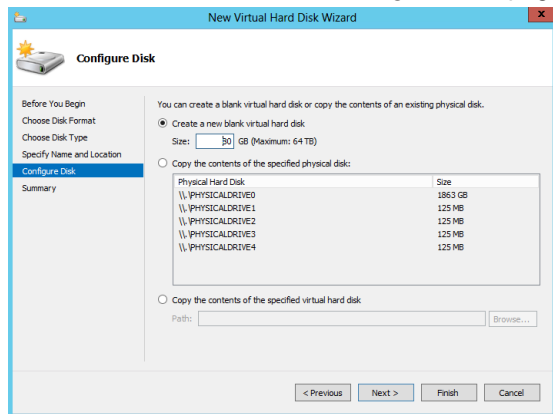
1. In the *Settings* page, select *IDE Controller 0* from the *Hardware* menu.
2. Select the type of drive that you want to attach to the controller, then click *Add*. The *Hard Drive* page opens.

3. Click *New* to create a new virtual hard disk. The *New Virtual Hard Disk Wizard* opens to help you create a new virtual hard disk.
4. Click *Next* to continue to the *Choose Disk Format* page.
5. Select to use VHDX format virtual hard disks. This format supports virtual disks up to 64TB and is resilient to consistency issues that might occur from power failures. This format is not supported in operating systems earlier than Windows Server 2012.
6. Click *Next* to continue to the *Choose Disk Type* page.

7. Select the type of virtual disk you want to use, one of the following:
 - **Fixed Size:** This type of disk provides better performance and is recommended for servers running applications with high levels of disk activity. The virtual hard disk file that is created initially uses the size of the virtual hard disk and does not change when data is deleted or added.
 - **Dynamically Expanding:** This type of disk provides better use of physical storage space and is recommended for servers running applications that are not disk intensive. The virtual disk file that is created is small initially and changes as data is added.
 - **Differencing:** This type of disk is associated in a parent-child relationship with another disk that you want to leave intact. You can make changes to the data or operating system without affecting the parent disk, so that

you can revert the changes easily. All children must have the same virtual hard disk format as the parent (VHD or VHDX).

8. Click *Next* to continue to the *Specify Name and Location* page.
9. Specify the name and location of the virtual hard disk file. Use the *Browse* button to select a specific file folder on your server.
10. Click *Next* to continue to the *Configure Disk* page.

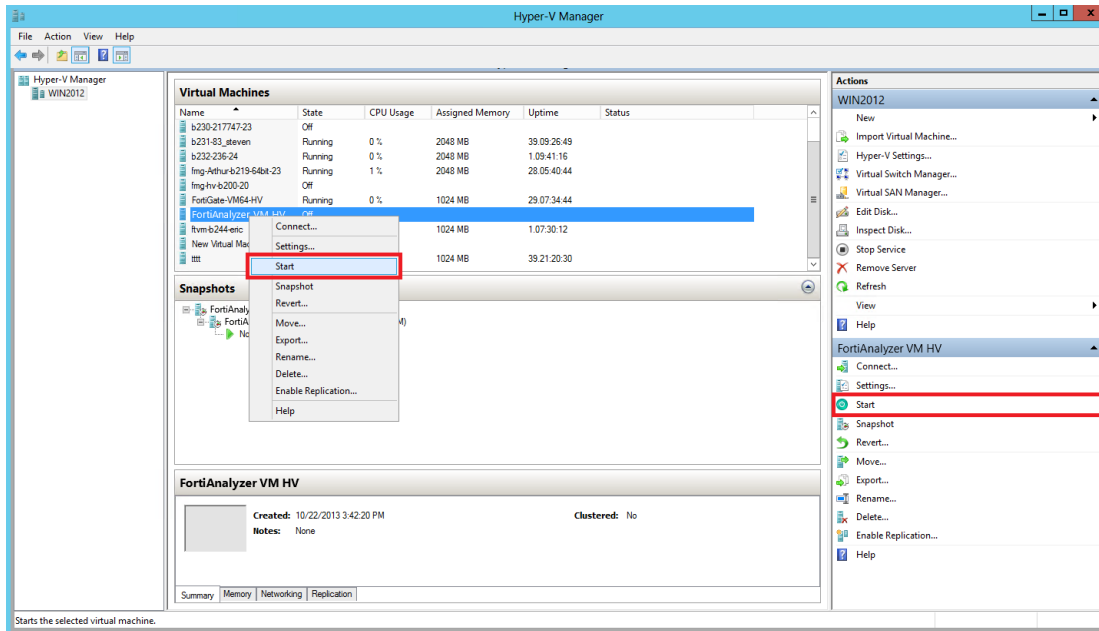


11. Select *Create a new blank virtual hard disk*, then enter the size of the disk in GB. The maximum size is dependent on your server environment.
12. Click *Next* to continue to the *Summary* page.
The summary page provides details about the virtual hard disk.
13. Click *Finish* to create the virtual hard disk, then click *Apply* to save the settings, and then click *OK* to exit the settings page.

Starting the virtual machine

You can now proceed to power on your FortiAnalyzer VM.

1. In the list of virtual machines, right-click on the name of the FortiAnalyzer VM and select **Start**.
2. Select the name of the FortiAnalyzer VM from the list of virtual machines, then click **Start** from the **Actions** menu.



Once the VM has started, proceed with the initial configuration. See [Configuring initial settings on page 18](#).

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

C

- CLI 8, 12, 16, 18-19
- Command Line Interface See CLI
- configure
 - CPU 15
 - disk 15
 - hardware 5
 - VM 20
- CPU 7, 20
 - configure 15
 - cores 7

D

- datasheet 10
- deploy
 - package 10
- device
 - model 10
- disk
 - configure 15

F

- firmware 10

G

- Graphical User Interface See GUI
- GUI
 - access 18

H

- hardware requirements 7
- Hyper-V 5, 10, 12-14

I

- instance 16
- interface 12
- IOPS 7
- IP address 8, 12, 18-20

L

- license 5, 8, 10, 14, 18-20
 - evaluation 5, 10, 19-20
 - file 6, 8, 10, 18-19
 - trial 5
 - upload 19
- logs
 - daily maximum 5

M

- MAC 18
- maximum
 - logs per day 5
- Media Access Control See MAC
- memory
 - minimum 7
 - size 13, 20
 - virtual 14

minimum

cores 7

IOPS 7

memory 7

N

network

adapter 13-14, 18

interface 12

P

package

deployment 10

VHD 12

password 19-20

R

requirements 7

S

SAN 15

storage

physical 16

type 7

volume 20

Storage Area Network See SAN

system requirements 7

V

VHD 10, 12

package 12

virtual

memory 14

Virtual Hard Disk See VHD

Virtual Machine See VM

Virtual Processor See CPU

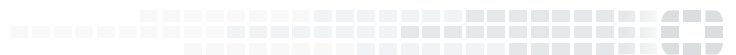
VM

configure 20

create 13



FORTINET®



Copyright© 2019 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.