FortiAnalyzer - VMware ESXi Cookbook

Version 6.4

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
http://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

April 5, 2024
FortiAnalyzer 6.4 VMware ESXi Cookbook
05-640-620531-20240405

TABLE OF CONTENTS

Change log

Date	Change description
2020-04-09	Initial release.
2021-03-09	Updated Minimum system requirements on page 7.
2021-05-13	Updated About FortiAnalyzer on VMware ESXi on page 5.
2021-05-28	Updated information about trial licenses and add-on licenses.
2021-06-02	Updated "Deployment package for VMware ESXi" on page 8
2021-07-15	Updated "Deployment package for VMware ESXi" on page 8.
2021-11-24	Updated "Deploying FortiAnalyzer on VMware vSphere" on page 11
2022-09-09	Added "Compatibility for VM hardware versions" on page 9. Updated "Deploying the OVF file" on page 12.
2022-11-18	Updated "Minimum system requirements" on page 7.
2023-02-01	Updated "About FortiAnalyzer on VMware ESXi" on page 5.
2024-04-05	Updated "About FortiAnalyzer on VMware ESXi" on page 5.

About FortiAnalyzer on VMware ESXi

This document provides information about deploying a FortiAnalyzer virtual appliance in VMware vSphere Hypervisor (ESX/ESCi) and VMware vSphere Client environments.

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*.

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 as the following table outlines 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
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 and FortiAnalyzer 6.4.1 or later, 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 19.

Add-on license

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

See also FortiAnalyzer 6.4 Trial License Guide.

Preparing for deployment

You can prepare for deployment by reviewing the following information:

- Minimum system requirements
- Deployment package for VMware ESXi
- 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.

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	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

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.

Deployment package for VMware ESXi

Firmware images on the Customer Service & Support site include FortiAnalyzer-VM deployment packages. The following table lists the available VM deployment package:

VM platform	Deployment file

VMware ESXi	ESX/ESXi server:
	`FAZ_VM64-vX-buildxxxx-FORTINET.out.ovf.zip`
	VMware Player:
	`FAZ_VM64-vX-buildxxxx-FORTINET.out.vmware.zip`

For the latest information on virtualization software support, see the corresponding FortiAnalyzer Release Notes on the Fortinet Docs Library.

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

File	Description
`DATADRIVE.vmdk`	The FortiAnalyzer-VM log disk in VMDK format.
`FAZ.vmdk`	The FortiAnalyzer system hard disk in Virtual Machine Disk (VMDK) format.
`FortiAnalyzer-VM64.hw14.ovf`	OVF template file for VMware ESXi 6.7 and later versions. Only available in 6.4.2 and later.
`FortiAnalyzer-VM64.hw14.vapp.ovf`	OVF template file for VMware vSphere, vCenter, and vCloud (ESXi 6.7 and later). Only available in 6.4.2 and later.
`FortiAnalyzer-VM64.ovf`	OVF template based on Intel e1000 NIC driver.
`FortiAnalyzer-VM64.vapp.ovf`	OVF template file for VMware vSphere, vCenter, and vCloud (earlier than ESXi 6.7).

The `.out.vmware.zip` file, for use with VMware Player, contains:

- `FAZ.vmdk`: The FortiAnalyzer system hard disk in VMDK format.
- `FortiAnalyzer-VM64.ovf`: The VMware virtual hardware configuration file.
- `DATADRIVE.vmdk`: The FortiAnalyzer log disk in VMDK format.
- `DATADRIVE-S0XX.vmdk`: 41 VMDK files used during deployment.

For more information about FortiAnalyzer, see the FortiAnalyzer datasheet.

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. For example, the `FAZ_VM64_HV-vX-buildxxxx-FORTINET.out.hyperv.zip` image, found in the 5.6.0 directory, is specific to the 64-bit 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* > *Download* tab.

Download the `.out` file to upgrade your existing FortiAnalyzer 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* dropdown 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.

Compatibility for VM hardware versions

FortiAnalyzer-VM supports ESXi 6.5 and later versions. Using corresponding hardware versions 13 and later is highly recommended, as mentioned in Virtual machine hardware versions.

It is recommended to upgrade hardware versions incrementally with only one delta at a time. For example, upgrading from 10 to 11, 11 to 12, 12 to 13, then 13 to 14 is recommended, although directly upgrading from 10 to 14 generally has no issues.

To upgrade hardware versions:

1. Log in to vSphere Client web console.
2. In the left pane tree-menu, right-click the FortiAnalyzer-VM.
3. From the shortcut menu, select *Compatibility* > *Schedule VM Compatibility Upgrade*.
4. Click *YES*.
5. From the *Compatible with* dropdown, select the desired compatibility.
6. Click *OK*.
7. Reboot the FortiAnalyzer-VM.

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 18).

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 VMware vSphere

After you download the `FAZ_VM64-v5-buildxxxx-FORTINET.out.ovf.zip` file and extract the package contents to a folder on your management computer, you can deploy the OVF package to your VMware environment.

Prior to deploying the FortiAnalyzer-VM, ensure that you configure the following and they are functioning properly:

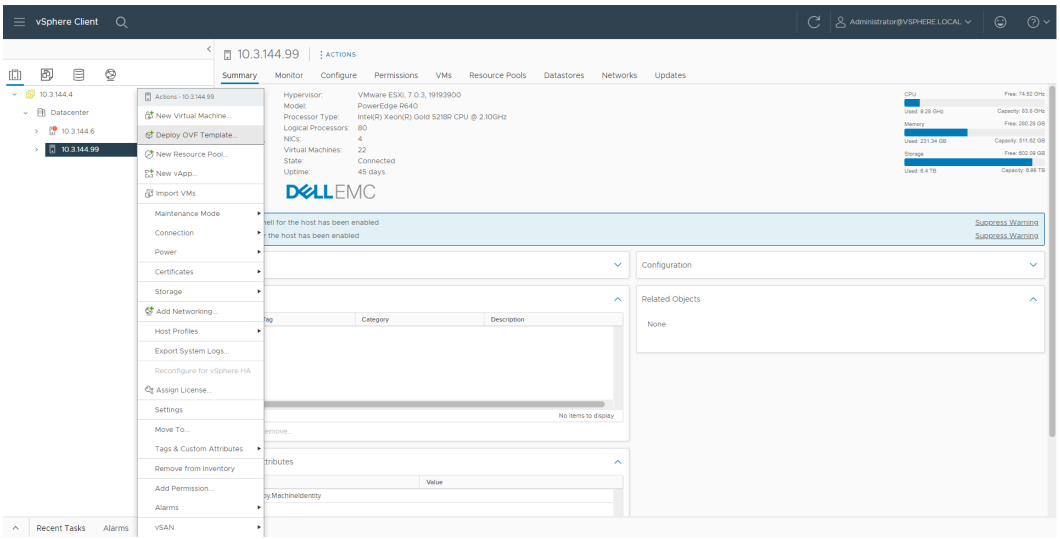
- You must install VMware vSphere Hypervisor™ (ESX/ESXi) software on a server and update it to the latest patch release prior to installing FortiAnalyzer. Go to What is a vSphere Hypervisor? for installation details.
- You must install VMware vSphere Client™ on the computer that you will use for managing the FortiAnalyzer-VM.

This section includes the following topics:

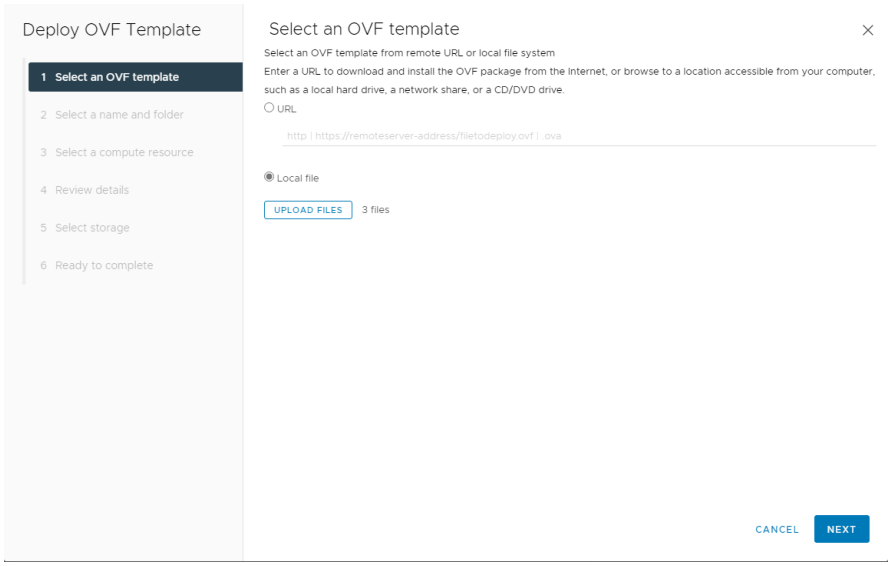
Deploying the OVF file

To deploy the OVF file template:

1. Log in to vSphere Client web console.
2. In the sidebar tree, right-click the intended physical host.



3. From the shortcut menu, select *Deploy OVF Template...*.
   The *Deploy OVF Template* wizard displays.
4. Using the *Deploy OVF Template* wizard, configure the FortiAnalyzer-VM:
   a. Select an OVF Template.



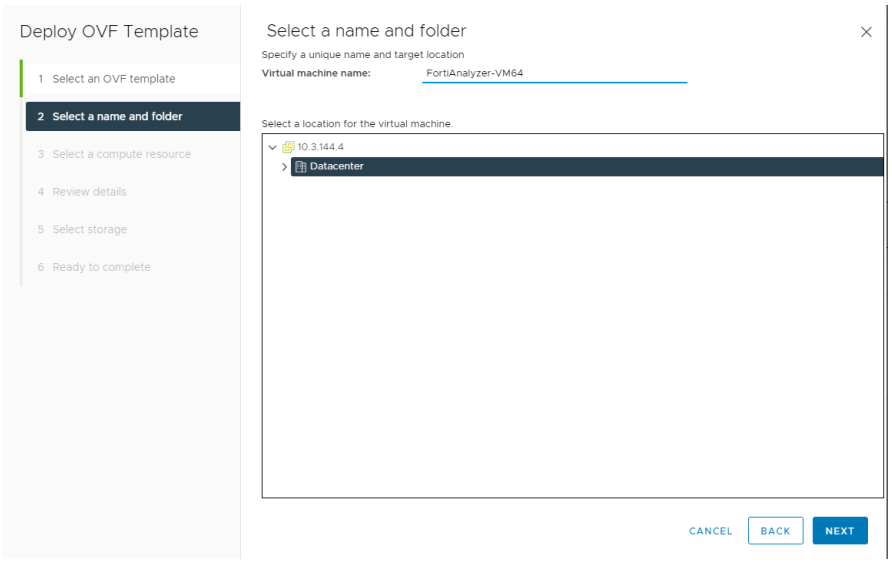
   i. Select the *Local file* radio button.
   ii. Click *Browse* and select all OVF related files.

iii. Click *NEXT*.

Alternatively, you can upload the OVF from a remote server. In this case, select the *URL* radio button and enter the URL of the OVF file.

Make sure all necessary files from the deployment package are in the same path. See "Deployment package for VMware ESXi" on page 8.

b. Select a name and folder.

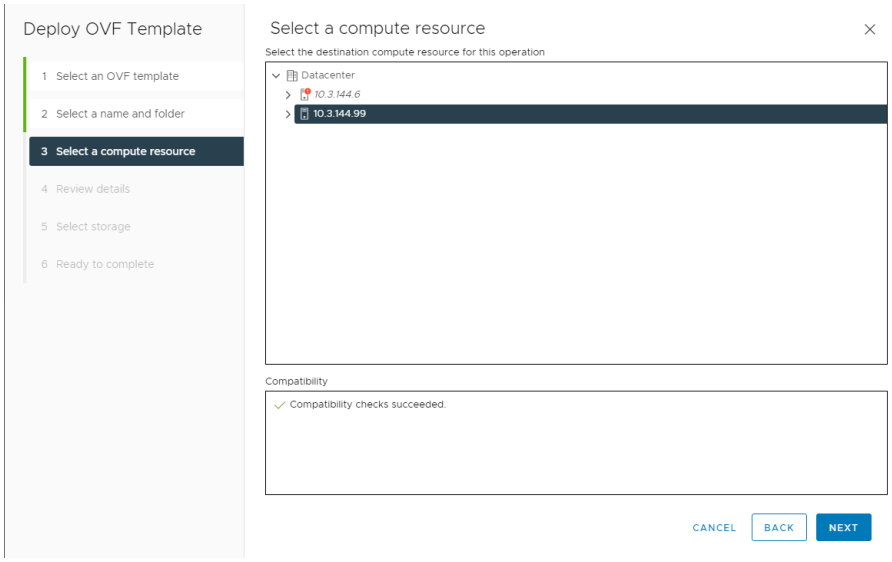


i. In the *Virtual machine name* field, enter a name for the VM.
The name can contain up to 80 characters and must be unique within the inventory folder.

ii. From the tree menu, select the location for the VM.

iii. Click *NEXT*.

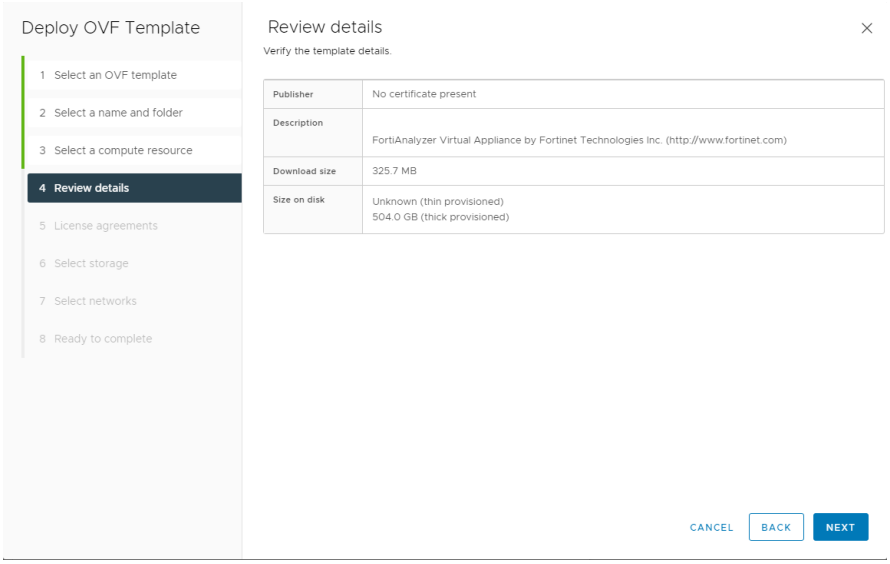
c. Select a compute resource.



i. From the tree menu, select the physical machine.

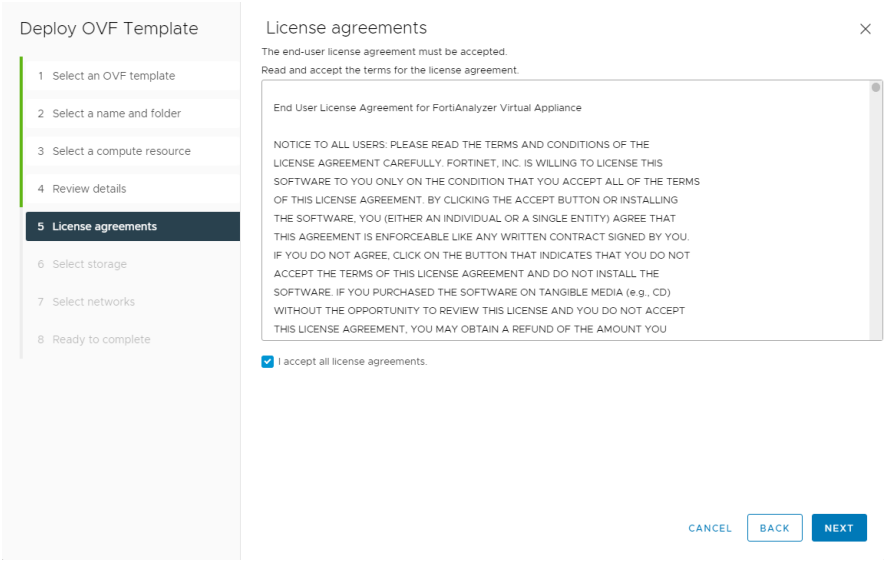
ii. Click *NEXT*.

d. Review details.



i. After reviewing the OVF details, click *NEXT*.

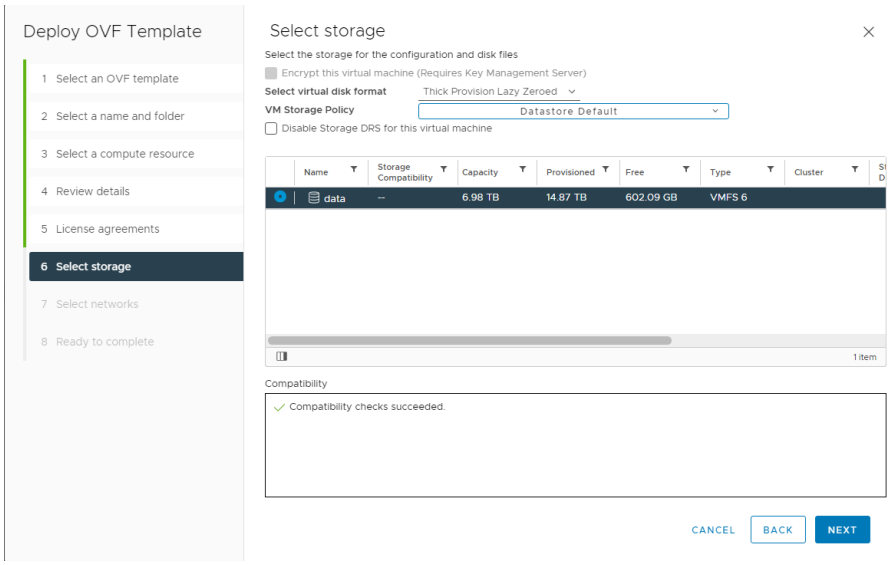
e. License agreements.



i. After reviewing the license agreements, select the checkbox for *I accept all license agreements*.

ii. Click *NEXT*.

f. Select storage.



i. From the *Select virtual disk format* dropdown, select one of the following:

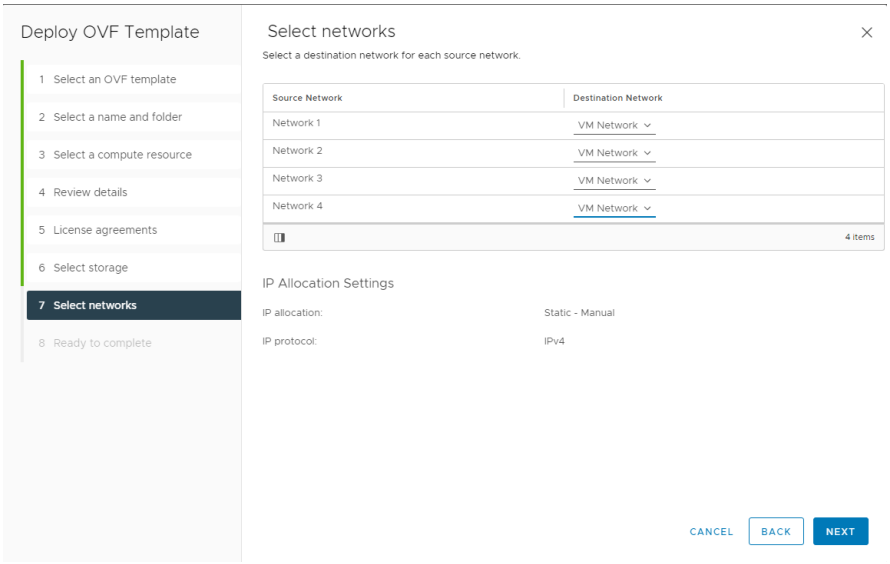
- *Thick Provision Lazy Zeroed*: Allocates the disk space statically (no other volumes can take the space), but does not write zeros to the blocks until the first write takes place to that block during runtime (which includes a full disk format).
- *Thick Provision Eager Zeroed*: Allocates the disk space statically (no other volumes can take the space), and writes zeros to all the blocks.
- *Thin Provision*: Allocates the disk space only when a write occurs to a block, but the Virtual Machine File System (VMFS) reports the total volume size to the OS. Other volumes can take the remaining space. This allows you to float space between your servers, and expand your storage when your size monitoring indicates there is a problem. Once a Thin Provisioned block is allocated, it remains in the volume regardless of whether you have deleted data.

If you know your environment will expand in the future, adding hard disks larger than the FortiAnalyzer base license requirement and utilizing Thin Provision when setting the OVF Template disk format is recommended. This allows your environment to expand as required while not taking up more space in the SAN than needed.

ii. From the menu, select the data storage location.

iii. Click *NEXT*.

g. Select networks.

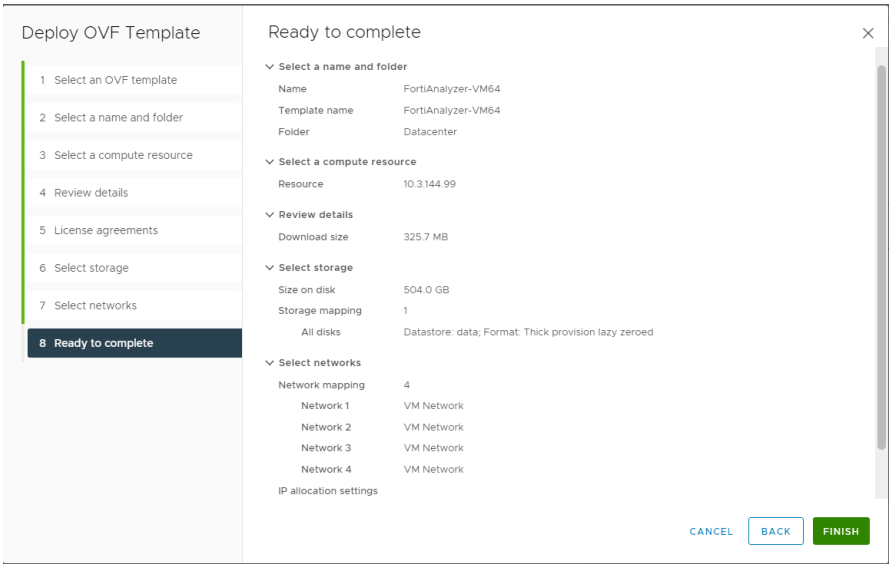


i. Map the networks used in this OVF template to networks in your inventory.

Network 1 maps to port1 of the FortiAnalyzer. You must set the destination network for this entry to access the device console.

ii. Click *NEXT*.

h. Ready to complete.



i. After verifying the information, click *FINISH* to start the deployment.

You may need to configure the FortiAnalyzer hardware settings before powering on the VM. See "Configuring hardware settings" below.

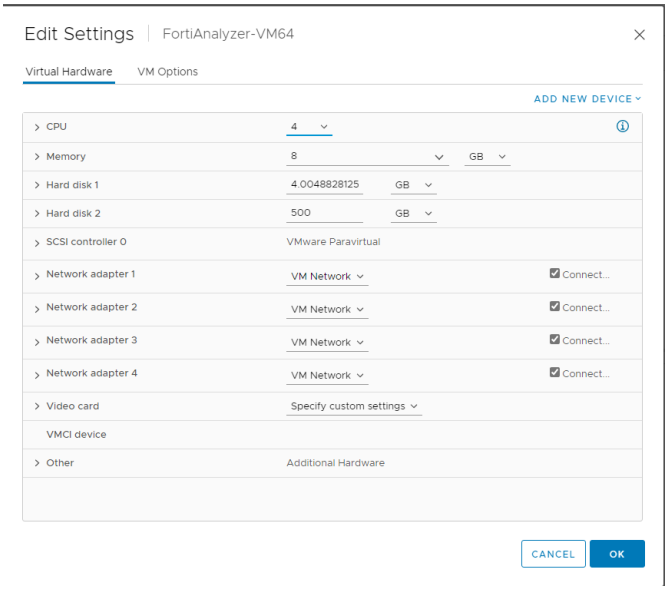
Configuring hardware settings

Before powering on your FortiAnalyzer-VM, you must configure the virtual memory, virtual CPU, and virtual disk.

In FortiAnalyzer 5.6 and later, the network interface mapping has changed. See the *FortiAnalyzer Upgrade Guide* for more information.

To configure hardware settings:

1. In the vSphere Client, select the VM from the tree menu in the left pane.
2. In the VM Hardware pane, click *Edit Settings...*.
   The *Edit Settings* dialog displays.



3. In the *CPU* field, adjust the number of CPU cores as required.
4. In the *Memory* field, adjust the memory size as required. See "Minimum system requirements" on page 7 to determine your required memory.
5. In the *Hard disk 2* field (the log disk), adjust the size required. You should not edit *Hard disk 1*.

   The FortiAnalyzer-VM allows you to add twelve virtual log disks 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. Click *OK* to apply your changes.

Powering on the VM

You can now proceed to power on your FortiAnalyzer.

- Select the FortiAnalyzer in the left pane, then click *Power on the virtual machine* in the *Getting Started* tab.
- Select the VM in the left pane, then click *Power On* in the toolbar.
- Right-click the VM in the left pane, then select *Power* > *Power On* from the right-click menu.

Once the VM starts, 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 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.

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, click the *Login with FortiCloud* button to start the process of activating your free trial license.

See also FortiAnalyzer 6.4 Trial License Guide.

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 FortiAnalyzer 6.4 Trial License Guide.

Configuring your FortiAnalyzer

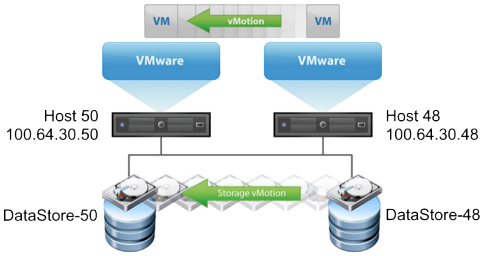
Once the FortiAnalyzer license has been validated, you can configure your device.

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.

vMotion in a VMware environment

This guide provides sample configuration of a vMotion FortiAnalyzer-VM in a VMware environment. VMware vMotion enables the live migration of a running FortiAnalyzer-VM from one physical server to another with zero downtime, continuous service availability, and complete transaction integrity. It also provides transparency to users.

The following depicts the network topology for this sample deployment. In this sample deployment, there are two hosts, Host 48 (100.64.30.48) and Host 50 (100.64.30.50), that are members of Cluster 1 in the DataCenter 1. The vCenter server (vcenter67.faz.lab) manages DataCenter 1.



This configuration requires the following prerequisites:

- You have set up the vCenter server and created the data center and cluster.
- Host 48 and Host 50 are members of the cluster.
- A Gigabit Ethernet network interface card with a VMkernel port enabled for vMotion exists on both ESXi hosts.
- A FortiAnalyzer-VM that is set up and able to handle traffic.

To migrate the FortiAnalyzer-VM on the vCenter web portal:

1. Log in to the vCenter web portal.
2. Verify the current location of the FortiAnalyzer-VM:
   a. Go to the FortiAnalyzer-VM.
   b. On the *Summary* tab, check the *Host*. In this example, the host is currently Host 48 (100.64.30.48).
   c. Go to *Storage* > *Files*. Check that the FortiAnalyzer-VM is located in the correct datastore. In this example, the datastore is currently Datastore 48, in Host 48.
3. Right-click the FortiAnalyzer-VM and select *Migrate*.
4. Configure the migration options:
   a. For *Select a migration type*, select *Change both compute resource and storage*. Click *NEXT*.
   b. For *Select a compute resource*, select the desired new compute resource. In this example, Host 50 (100.64.30.50) is selected. Click *NEXT*.
   c. For *Select storage*, select the storage associated with the selected compute resource. In this example, Datastore 50 (as corresponds to Host 50) is selected. Click *NEXT*.
   d. For *Select networks*, select the desired destination network at the selected compute resource. In this example, the source network is at Host 48, and the destination network is at Host 50. Click *NEXT*.
   e. For *Select vMotion priority*, select *Schedule vMotion with high priority (recommended)*. Click *NEXT*.
5. Before initiating the migration, open the CLI for the FortiAnalyzer-VM to check on traffic during the migration. Enter `diagnose sniffer packet any 'icmp and host 8.8.8.8'` to check if traffic is stable.

6. Click *FINISH*.

   After a few seconds, the FortiAnalyzer-VM is migrated to the new compute resources, in this case Host 50.
7. Log into the vCenter web portal. Go to the FortiAnalyzer-VM. On the *Summary* tab, the *Host* is now the new compute resources, in this case Host 50 (100.64.30.50).
8. Go to *Storage* > *Files*. It shows that the FortiAnalyzer-VM is now located in a new datastore, in this example Datastore 50.