FortiManager - Xen 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

November 18, 2022
FortiManager 6.4 Xen Cookbook
02-640-620521-20221118

TABLE OF CONTENTS

Change log

Date	Change description
2020-04-09	Initial release.
2020-12-03	Updated Minimum system requirements on page 7.
2021-03-09	Updated Minimum system requirements on page 7.
2021-03-12	Updated About FortiManager on Xen on page 5.
2021-05-13	Updated About FortiManager on Xen on page 5.
2021-05-28	Updated information about trial licenses and add-on licenses.
2022-11-18	Updated "Minimum system requirements" on page 7.

About FortiManager on Xen

This document provides information about deploying a FortiManager virtual appliance in Open Source XenServer and Citrix XenServer 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 *FortiManager Administration Guide*.

Licensing

Fortinet offers the FortiManager-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 FortiManager-VM license, contact your Fortinet-authorized reseller, or visit How To Buy.

When configuring your FortiManager-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	Devices/VDOMs	GB/day of logs with FortiAnalyzer enabled (not stackable)
Trial License	3	0 FortiAnalyzer features not supported
VM-10-UG	+10	2
VM-100-UG	+100	5
VM-1000-UG	+1000	10
VM-5000-UG	+5000	25
VM-10K-UG	+10000	50

See Minimum system requirements on page 7.

See also the FortiManager product datasheet.

Trial license

With a FortiCare account and FortiManager 6.4.1 or later, FortiManager-VM includes a free limited non-expiring trial license.

The free trial license includes support for to add 3 devices/VDOMS and use 3 ADOMs.

The free trial license does not include services or support.

You can activate the trial license when you connect to the GUI for the FortiManager-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 17.

Add-on license

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

See also FortiManager 6.4 Trial License Guide.

Preparing for deployment

You can prepare for deployment by reviewing the following information:

- Minimum system requirements
- Deployment package for Open Source XenServer
- Downloading a deployment package

Minimum system requirements

FortiManager-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 the number of devices, VDOMs, or ADOMs that your VM manages.

Maximum devices/ VDOMs	VM hardware requirements	
	RAM (GB)	CPU cores
100	8	4
300	16	6
1200	32	6
4000	64	16
10000	128	24

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

Enabling FortiAnalyzer features requires more resources.

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

Deployment package for Citrix XenServer

FortiManager 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
Citrix XenServer 7.2	`FMG_VM64_XEN-vX-buildxxxx-FORTINET.out.CitrixXen.zip`

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

- `FMG.xva`: The Citrix XenServer Virtual Appliance (XVA) binary file containing virtual hardware configuration settings.
- `ovf` folder:
  - `FortiManager.ovf`: Open Virtualization Format (OVF) template file, containing virtual hardware settings for Xen.
  - `FMG.vhd`: The FortiManager system hard disk in VHD format.
  - `datadrive.vhd`: The FortiManager log disk in VHD format.

For more information FortiManager, see the FortiManager datasheet.

Deployment package for Open Source XenServer

FortiManager 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
Open Source XenServer 4.2.5	`FMG_VM64_XEN-vX-buildxxxx-FORTINET.out.OpenXen.zip`

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

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

For more information FortiManager, see the FortiManager 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 `FMG_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 *FortiManager Release Notes* and MIB file from this directory. The Fortinet Core MIB file is located in the *FortiManager* > *Download* tab.

Download the `.out` file to upgrade your existing FortiManager 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 *FortiManager* 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

FortiManager-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 FortiManager-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 FortiManager-VM.

Deployment

Prior to deploying the FortiManager, the VM platform must be installed and configured so that it is ready to create virtual machines. The installation instructions for FortiManager 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 FortiManager appliance for the first time, you might need to adjust virtual disk sizes and networking settings. The first time you start FortiManager, 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 FortiManager GUI (see Enabling GUI access on page 16).

Deploying FortiManager on Citrix XenServer

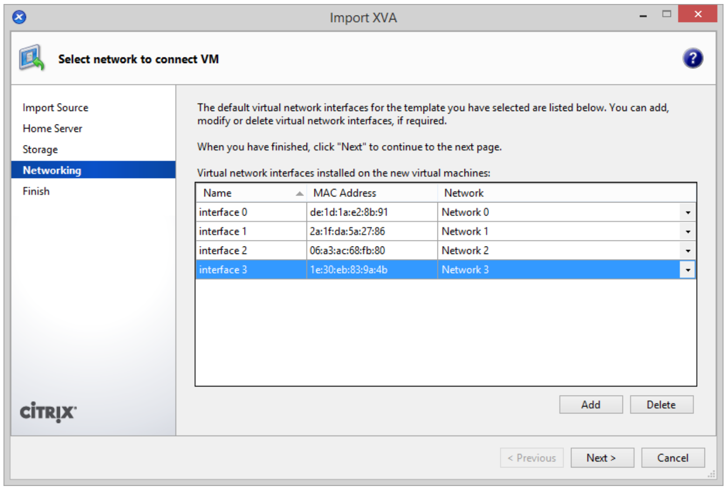
After you download the `FMG_VM64_XEN-vX-buildxxxx-FORTINET.out.CitrixXen.zip` file and extract the files, you can create the VM in your Citrix Xen environment.

Creating the virtual machine

To create the virtual machine:

1. Launch XenCenter on your management computer. The management computer can be any computer that can run Citrix XenServer, a Microsoft Windows application.
2. Click *ADD a server*, then enter the Citrix XenServer IP address and the root logon credentials required to manage that server. XenCenter adds your Citrix XenServer to the list in the left pane, and the *Virtual Machine Manager* homepage opens.
3. Select *File* > *Import*.
4. Click *Browse*, locate the `fmg.xva` file, select *Open*, then select *Next*.
5. Choose the pool or standalone server to host the VM, then click *Next*.
6. Select the storage location for the FortiManager disk drives, then click *Next*.

7. Configure the virtual network interfaces, then click *Next*. By default, there are four virtual network interfaces.



The default virtual network interfaces for the template you have selected are listed below. You can add, modify or delete virtual network interfaces, if required.

When you have finished, click "Next" to continue to the next page.

Virtual network interfaces installed on the new virtual machines:

Name	MAC Address	Network
interface 0	de:1d:1a:e2:8b:91	Network 0
interface 1	2a:1f:da:5a:27:86	Network 1
interface 2	06:a3:ac:68:fb:80	Network 2
interface 3	1e:30:eb:83:9a:4b	Network 3

8. Review the import settings, deselect *Start VM(s) after import*, and then click *Finish* to import the VM.

   The Citrix XenServer imports the FortiManager files and configures the VM as specified in the template. Depending on your computer's hardware speed and resource load, the file size, and the network connection speed, this may take several minutes to complete

   When the VM import is complete, the XenServer left pane includes the FortiManager-VM in the list of deployed VMs for your Citrix XenServer.

Configuring hardware settings

Before starting your FortiManager for the first time, you must adjust the VM's virtual hardware settings to meet your network requirements.

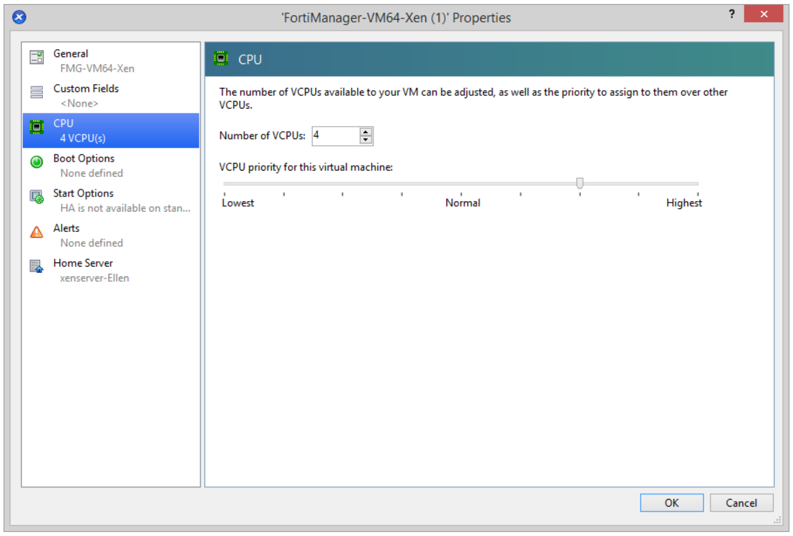
To access VM settings, open XenCenter and select the FortiManager in the left pane. The tabs in the right pane provide access to the virtual hardware configuration, and the console tab provides access to the FortiManager console.

You must resize the disk before starting the VM for the first time.

If you know your environment will expand in the future, or if you will be using ADOMs, adding hard disks larger than 500 GB. This allows your environment to expand as required while not taking up more space than is needed.

To set the number of CPUs:

1. In the XenCenter left pane, right-click the FortiManager and select *Properties*.
2. In the left pane of the *Properties* window, select *CPU*.



'FortiManager-VM64-Xen (1)' Properties

General
FMG-VM64-Xen
Custom Fields
<None>
CPU
4 VCPU(s)
Boot Options
None defined
Start Options
HA is not available on stan...
Alerts
None defined
Home Server
xenserver-Ellen

CPU

The number of VCPUs available to your VM can be adjusted, as well as the priority to assign to them over other VCPUs.

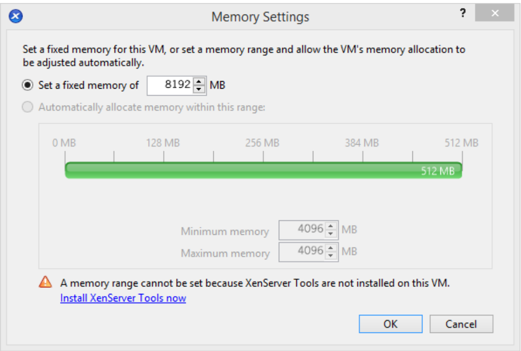
Number of VCPUs: 4

VCPU priority for this virtual machine:

3. Adjust the value in the *Number of VCPUs* field, then click *OK*. XenCenter displays a warning if you select more CPUs than the Xen host computer contains. Such a configuration may reduce performance.

To set the memory size:

1. In the XenCenter left pane, select the FortiManager.
2. In the right pane, select the *Memory* tab.
3. Click *Edit* and modify the value in the *Set a fixed memory of* field. See Minimum system requirements on page 7 to determine your required memory.
4. Click *OK*.



Memory Settings

Set a fixed memory for this VM, or set a memory range and allow the VM's memory allocation to be adjusted automatically.

● Set a fixed memory of 8192 MB

○ Automatically allocate memory within this range:

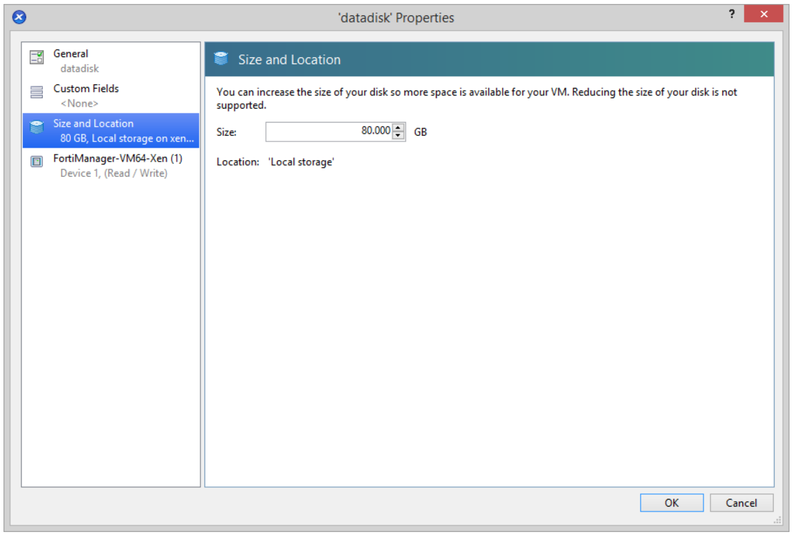
Minimum memory 4096 MB
Maximum memory 4096 MB

A memory range cannot be set because XenServer Tools are not installed on this VM.
Install XenServer Tools now

To resize the data disk:

1. In the XenCenter left pane, select the FortiManager.
2. In the right pane, select the *Storage* tab.
3. Select the data disk, then click *Properties* to open the *Properties* window.

4. Select *Size and Location*.



You can increase the size of your disk so more space is available for your VM. Reducing the size of your disk is not supported.

Size: 80.000 GB

Location: 'Local storage'

5. Adjust the *Size* to the required value, then click *OK*.

The FortiManager-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 ..>
```

Starting the VM

You can now proceed to start on your FortiManager-VM.

- In the XenCenter left pane, right-click the FortiManager-VM name and select *Start*.
- Select the FortiManager-VM name from the left pane, then select *Start* in the toolbar.

After the VM starts, proceed with the initial configuration. See Configuring initial settings on page 16.

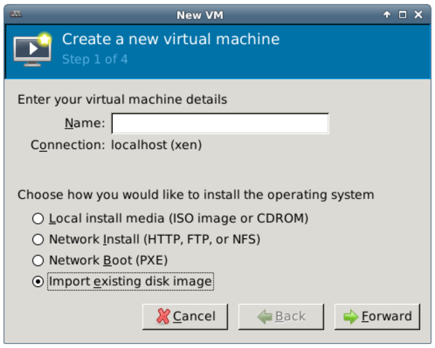
Deploying FortiManager on Open Xen

After you download the `FMG_VM64_XEN-vX-buildxxxx-FORTINET.out.OpenXen.zip` file and extract the *fmg.qcow2*, you can create the VM in your Open Xen environment.

To deploy and configure the virtual machine:

1. Launch Virtual Machine Manager (virt-manager) on your Open Xen host server. The *Virtual Machine Manager* homepage opens.

2. Select *Create a new virtual machine* from the toolbar.



New VM

Create a new virtual machine

Step 1 of 4

Enter your virtual machine details

Name:

Connection: localhost (xen)

Choose how you would like to install the operating system

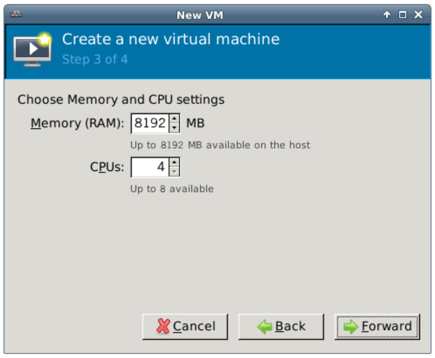
○ Local install media (ISO image or CDROM)

○ Network Install (HTTP, FTP, or NFS)

○ Network Boot (PXE)

● Import existing disk image

3. Configure the VM:
   a. Enter the VM name, such as *FMG-VM*.
   b. Ensure that *Connection* is *localhost*, select *Import existing disk image*, then click *Forward* to continue.
   c. In the *OS Type* field select *Linux*. In the *Version* field select *Generic 2.6.x kernel*.
   d. Click *Browse* to open the *Locate or create storage volume* window.
   e. Click *Browse Local*, find the fmg.qcow2 disk image file, then click *Choose Volume* and then *Forward*.



New VM

Create a new virtual machine

Step 3 of 4

Choose Memory and CPU settings

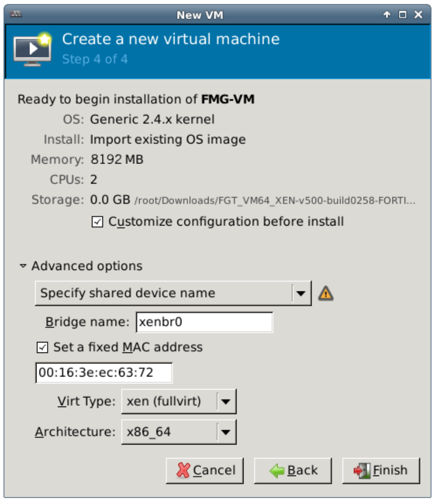
Memory (RAM): 8192 MB

Up to 8192 MB available on the host

CPUs: 4

Up to 8 available

   f. Specify the amount of memory and the number of CPUs to allocated to this VM. See Minimum system requirements on page 7 to determine your required memory. Click *Forward*.
   g. Select *Customize configuration before install*. This enables you to make hardware configuration changes before the VM creation is started.
   h. Expand the *Advanced options* section.
      - By default, a new VM includes one network adapter.
      - Select *Specify shared device name*, and enter the name of the bridge interface on the Open Xen host.
      - Optionally, set a fixed MAC address for the virtual network interface.
      - *Virt Type* and *Architecture* are set by default and you should not need to change it.



Ready to begin installation of **FMG-VM**
OS: Generic 2.4.x kernel
Install: Import existing OS image
Memory: 8192 MB
CPUs: 2
Storage: 0.0 GB /root/Downloads/FGT_VM64_XEN-v500-build0258-FORTI...
☑ Customize configuration before install

Advanced options
Specify shared device name
Bridge name: xenbr0
☑ Set a fixed MAC address
00:16:3e:ec:63:72
Virt Type: xen (fullvirt)
Architecture: x86_64

i. Click *Finish*. The VM hardware configuration window opens. You can use it to add hardware such as network interfaces and disk drives. Configure the VM hardware:

i. Click *Add Hardware* to open the *Add Hardware* window, then click *Storage*.

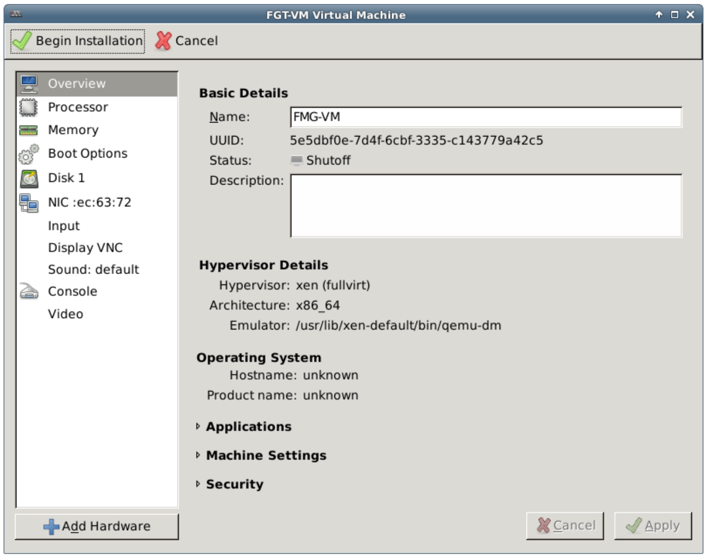
i. Select *Create a disk image on the computer's harddrive*, and set the size to an appropriate size.

If you know your environment will expand in the future, or if you will be using ADOMs, adding hard disks larger than 500 GB. This allows your environment to expand as required while not taking up more space than is needed.

The FortiManager-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 ..>
```

ii. Select *Network* to add more network interfaces. A new VM includes one network adapter by default. You can add more through the *Add Hardware* window. A FortiManager-VM requires four network adapters. You can configure network adapters to connect to a virtual switch or to network adapters on the host computer.



Basic Details

Name: FMG-VM
UUID: 5e5dbf0e-7d4f-6cbf-3335-c143779a42c5
Status: Shutoff
Description:

Hypervisor Details

Hypervisor: xen (fullvirt)
Architecture: x86_64
Emulator: /usr/lib/xen-default/bin/qemu-dm

Operating System

Hostname: unknown
Product name: unknown

4. Click *Finish*.
5. Click *Begin Installation*.

   After the installation completes successfully, the VM starts and the console window opens. You can then proceed with the initial configuration (Configuring initial settings on page 16).

Configuring initial settings

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

Enabling GUI access

To enable GUI access to the FortiManager, you must configure the IP address and network mask of the appropriate port on the FortiManager. 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 FortiManager and access the console window. You might need to press *Enter* to see the login prompt.
2. At the FortiManager 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 FortiManager 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 FortiManager 6.4 Trial License Guide.

Upgrading to an add-on license

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

See also FortiManager 6.4 Trial License Guide.

Configuring your FortiManager

Once the FortiManager 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 FortiManager, see the *FortiManager Administration Guide*.

Security Fabric connector integration with Xen

You can use FortiManager to create Fabric connectors for Xen, and then install the Fabric connectors to FortiOS.

The Fabric connectors in FortiManager define the type of connector and include information for FortiOS to communicate with and authenticate with the products. In some cases the FortiGate must communicate with products through the Fabric connector, and in other cases the FortiGate communicates directly with the products.

FortiOS works with the Fabric connector to communicate with Xen.

For information about the Fabric connector, see the Fortinet Document Library.

You cannot import a policy package for the Fabric connector from FortiOS to FortiManager.

Following is an overview of creating Fabric connectors for Xen using FortiManager:

1. Create a Fabric connector. See Creating a Fabric connector for Xen on page 18.
2. Import address names from Xen to the Fabric connector. See Importing address names to a Fabric connector on page 19. FortiManager imports the address names and converts them to dynamic firewall address objects. The objects do not include IP addresses and display in *Firewall Objects > Addresses*.
3. In the policy package in which you are creating the new policy, create an IPv4 policy and include the firewall address objects for Xen. See Creating an IP address policy on page 19.
4. Install the policy package to FortiOS. See Installing a policy package on page 20.

   FortiGate communicates with Xen to dynamically populate the firewall address objects with IP addresses.

   If the address names change in Xen after you import them to FortiManager, you must reimport the address names.

Creating a Fabric connector for Xen

With FortiManager, you can create a Fabric connector for Xen and import address names from Xen to automatically create dynamic objects that you can use in policies.

When you install the policies to one or more FortiGates, FortiOS uses the information and the Fabric connector to communicate with Xen and dynamically populate the objects with IP addresses.

When you create a Fabric connector for Xen, you specify how FortiOS can communicate with Xen through the Fabric connector. As a result, you are configuring communication and authentication information for the Fabric connector.

If you have enabled ADOMs, you can create multiple Fabric connectors per ADOM. Each Fabric connector requires a unique IP address.

This configuration requires the following:

- FortiManager version 6.0 ADOM or later
- FortiManager is managing the FortiGate.
- You have configured the managed FortiGate to work with Xen.

To create a Fabric connector object for Xen:

1. Go to *Fabric View* > *Fabric Connectors*.
2. Click *Create New*. The *Create New Fabric Connector* wizard displays.
3. Under *SDN*, select *Xen*, and click *Next*.
4. Under *SDN*, select *Horizon*, and click *Next*.
5. Configure the following options, then click *OK*:

Name	Enter the Fabric connector name.
Domain	Enter the Fabric connector domain.
Server	Enter the Fabric connector IP address.
IP	Enter the Fabric connector IP address.
Port	Identify the port used for the Fabric connector: • Click *Use Default* to use the default port. • Click *Specify* and type the port number.
User Name	Enter the Fabric connector username.
Password	Enter the Fabric connector password.
Status	Toggle *On* to enable the Fabric connector. Toggle *OFF* to disable the Fabric connector.

Importing address names to a Fabric connector

After you configure a Fabric connector, you can import dynamic objects from cloud platforms, such as Xen, to the Fabric connector, and dynamic firewall address objects are automatically created.

To import address names for Xen:

1. Go to *Policy & Objects* > *Object Configurations*.
2. Go to *Security Fabric* > *Fabric Connectors*.
3. In the content pane, right-click the Xen Fabric connector, and select *Import*. The *Import SDN Connector* dialog displays.
4. Select the address names, and click *Import*. FortiManager imports the address names and converts them to dynamic firewall address objects that display on the *Firewall Objects* > *Addresses* pane.

Creating an IP address policy

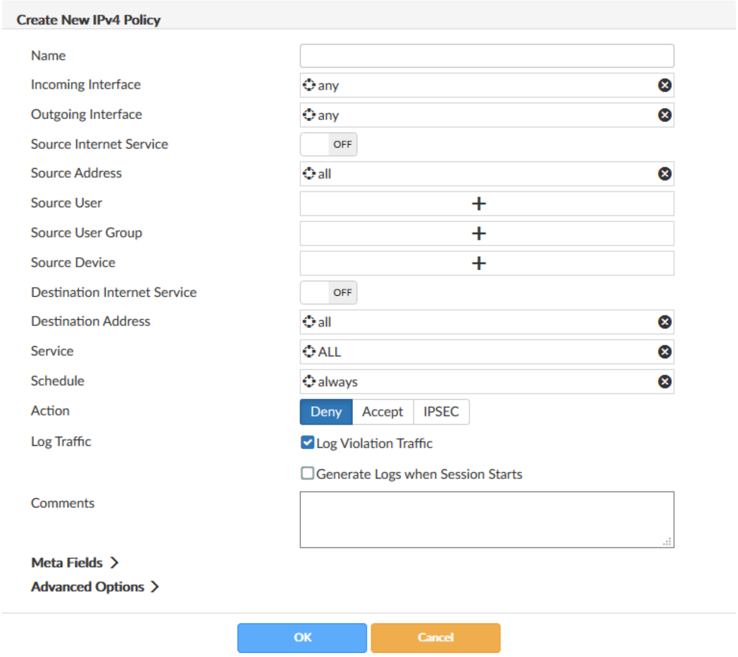
The section describes how to create new IPv4 and IPv6 policies.

You can create an IPv6 security policy for an IPv6 network and a transitional network. A transitional network is a network that is transitioning to IPv6 but must still have access to the Internet or must connect over an IPv4 network. IPv6 policies allow for this specific type of traffic to travel between the IPv6 and IPv4 networks.

On the *Policy & Objects* tab, from the *Tools* menu, select *Display Options*. In the *Policy* section, select the *IPv6 Policy* checkbox to display this option.

To create a new IPv4 or IPv6 policy:

1. Ensure that you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the tree menu for the policy package in which you will be creating the new policy, select *IPv4 Policy* or *IPv6 Policy*. If you are in the Global Database ADOM, select *IPv4 Header Policy*, *IPv4 Footer Policy*, *IPv6 Header Policy*, or *IPv6 Footer Policy*.
4. Click *Create New*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be added to the bottom of the list, but above the implicit policy. The *Create New Policy* pane opens.



Create New IPv4 Policy

Name	
Incoming Interface	any
Outgoing Interface	any
Source Internet Service	OFF
Source Address	all
Source User	+
Source User Group	+
Source Device	+
Destination Internet Service	OFF
Destination Address	all
Service	ALL
Schedule	always
Action	Deny Accept IPSEC
Log Traffic	☑ Log Violation Traffic ☐ Generate Logs when Session Starts
Comments	

Meta Fields >
Advanced Options >

5. Complete the options.
6. Click *OK* to create the policy.

   You can enable or disable the policy in the right-click menu. When disabled, a disabled icon displays in the *Seq.#* column to the left of the number.

Installing a policy package

When installing a policy package, objects that the policy references are installed to the target device. Default or per-device mapping must exist or the installation fails.

Some objects that the policy does not directly reference are also installed to the target device, such as FSSO polling objects, address and profile groups, and CA certificates.

To install a policy package to a target device:

1. Ensure you are in the ADOM that contains the policy package.
2. Go to *Policy & Objects* > *Policy Packages*.
3. Select a policy package and from the *Install* menu or right-click menu select *Install Wizard*. The *Install Wizard* opens.
4. Follow the steps in the install wizard to install the policy package. You can install policy package and device settings or install the interface policy only.