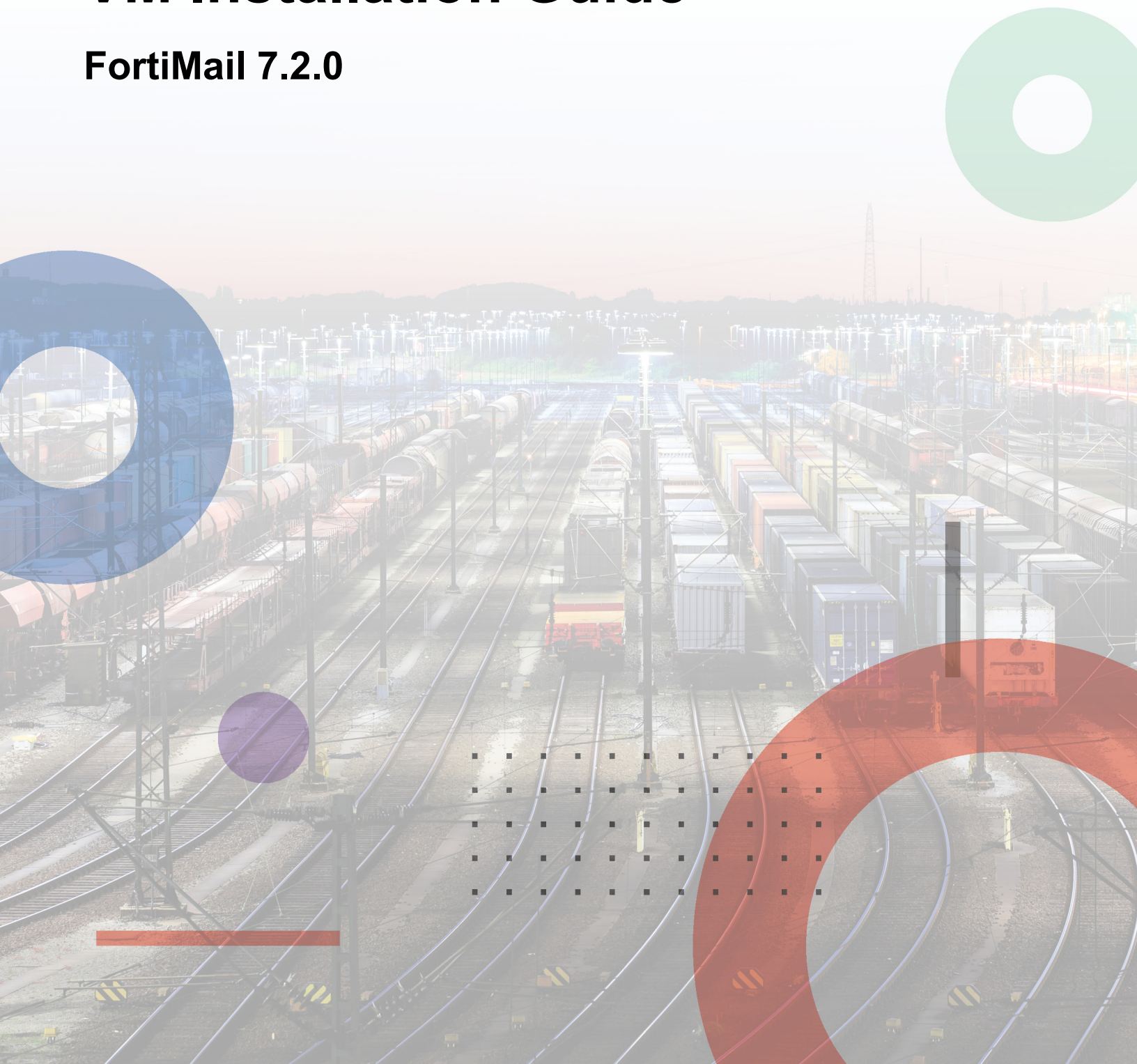
VM Installation Guide

FortiMail 7.2.0



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

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

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

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

October 23, 2024
FortiMail 7.2.0 VM Installation Guide
00-720-000000-20241023

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-05-17	Initial release of FortiMail 7.2.0 VM Installation Guide.

FortiMail VM Overview

Welcome and thank you for selecting Fortinet products to protect your network.

The FortiMail VM Secure Messaging Platform (FortiMail VM) is part of an integrated hardware and software solution that provides powerful and flexible antispam, antivirus, email archiving, logging, and reporting capabilities to incoming and outgoing email traffic. FortiMail has reliable and high performance features for detecting and blocking spam messages and malicious attachments. Built on Fortinet's FortiOS™, FortiMail antivirus technology extends full content inspection capabilities to detect the most advanced email threats.

This guide assumes that the reader has a thorough understanding of virtualization servers.

This section contains the following topics:

Licensing

When you place an order for FortiMail VM, Fortinet sends a registration number to the email address supplied on the order form. Use that number to register with FortiCare (support.fortinet.com) and to obtain a license file (.lic). You need the license file to activate FortiMail VM and unlock the full range of features, such as the maximum virtual memory and number of CPUs.

FortiMail VM includes a 15-day trial (VM00). The trial version provides all FortiMail VM functions except antispam and antivirus signature updates and the FortiGuard Antispam query. Because the trial version only provides low encryption, you may not be able to access the FortiMail VM web UI through HTTPS, unless you have enabled weak cipher in your browser. The trial period begins the first time you start FortiMail VM. If you do not install a valid license after the trial period expires or after your licence expires, you will not be able to make configuration changes to FortiMail VM.

Fortinet provides several licenses for FortiMail VM: a 1-CPU license (VM01), a 2-CPU license (VM02), a 4-CPU license (VM04), an 8-CPU license (VM08), a 16-CPU license (VM16), and a 32-CPU license (VM32). You can install your full license from FortiCare at any time during or after the trial period. For details about how to install or update a license, see Uploading the FortiMail VM license file on page 46.

Resources

The following table shows the resources available with each license.

FortiMail VM resources:

	VM00	VM01	VM02	VM04	VM08	VM16	VM32
Maximum Virtual CPUs Supported	1	1	2	4	8	16	32
Virtual NICs (Minimum/Maximum)	1/4	1/4	1/4	1/6	1/6	1/6	1/6
Virtual Machine Storage (Minimum/Maximum)	50 GB/1 TB	50 GB/1 TB	50 GB/2 TB	50GB/4 TB	50GB/8 TB	50GB/12 TB	50GB/24 TB
Virtual Machine Memory (Minimum/Maximum)	1 GB/2 GB	1 GB/6 GB	1 GB/8 GB	1 GB/16 GB	1 GB/64 GB	1 GB/128 GB	1 GB/128 GB

Most resources are available after successful deployment of the OVF file and validation of the license file. See Deploying the FortiMail VM software on page 11 and Starting FortiMail VM on page 18.

To use more than one CPU, you must configure its use once you deploy FortiMail VM. See Configuring the number of CPUs on page 17.

For v4.0 MR3 GA and earlier releases, you can reduce the virtual storage to as small as 50 GB (but not smaller than 50 GB) once you deploy FortiMail VM. Starting from v4.0 MR3 Patch 1 release, you can reduce the size to as small as 5 GB. See Configuring a smaller disk on page 18.

In addition, FortiMail VM requires a valid FortiGuard connection using:

- for DNS lookup; RBL lookup — UDP 53
- for FortiGuard Licensing — TCP 443

Registering your Fortinet product

To obtain the FortiMail VM license file you must first register your FortiMail VM with Fortinet Customer Service & Support.

To register your FortiMail VM:

1. Log in to the Fortinet Customer Service & Support portal using an existing support account or select *Create an Account* to create a new account.
2. In the toolbar select *Asset* > *Register/Renew*.
3. The *Registration Wizard* opens.
4. Enter the license registration code from the FortiMail VM License Certificate that was emailed to you and select *Next*. The *Registration Info* page is displayed.
5. Follow the instructions to finish the registration.

As part of the license validation process, FortiMail VM compares its IP address with the IP information in the license file. If a new license has been imported or the FortiMail VM's IP address has been changed, the FortiMail 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 FortiMail VM license validation. You must specify an IPv4 address in both the support portal and the port management interface.

6. In the *Registration Completed* page you can download the FortiMail VM license file. Select the *License File Download* link. You will be prompted to save the license file (`.lic`) to your management computer. See Uploading the FortiMail VM license file on page 46 for instructions on uploading the license file to your FortiMail VM via the GUI.

Downloading the FortiMail deployment package

FortiMail deployment packages are included with FortiMail firmware images on the Customer Service & Support site. First, see the following table to determine the appropriate VM deployment package for your VM platform. For up-to-date platform support information, see the latest FortiMail release notes.

FortiMail VM deployment packages and supported VM platforms:

VM Platform	FortiMail VM Deployment File
Citrix XenServer v5.6sp2, 6.0 and later	FE_VMXE-64-vXXX-buildnnnn-FORTINET.out.xenserver.zip
Microsoft Hyper-V Server 2008R2 and 2012	FE_VMHV-64-vXXX-buildnnnn-FORTINET.out.hyperv.zip
KVM (qemu 0.12.1)	FE_VMKV-64-vXXX-buildnnnn-FORTINET.out.kvm.zip
VMware ESX 5.0 and later	FE_VM-64-vXXX-buildnnnn-FORTINET.out.ovf.zip
OpenStack	FML_VMKV-64-vXXX-buildnnnn-FORTINET.out.kvm.zip

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

To download the FortiMail deployment package:

1. In the main page of the Customer Service & Support site, select *Download* > *Firmware Images*.
   The *Firmware Images* page opens.
2. In the *Firmware Images* page, select *FortiMail*.
3. Browse to the appropriate directory on the FTP site for the version that you would like to download.
4. Download the appropriate `.zip` file for your VM server platform.
   You can also download the corresponding release notes.
5. Extract the contents of the deployment package to a new file folder.

Deployment package contents

Citrix XenServer

The FORTINET.out.CitrixXen.zip file contains:

- fortimail-vm-xen.vhd and xxx.vhd files: the FortiMail system hard disk in VHD format
- fortimail-vm-xen-xxxgb.ovf: Open Virtualization Format (OVF) template file, containing virtual hardware settings for Xen

Microsoft Hyper-V

The FORTINET.out.hyperv.zip file folder contains the following file:

- fortimail-hv.vhd: Virtual hard disk (VHD) format file
- nnngb.vhd: the VHD files for the virtual storage disk

KVM and OpenStack

The FORTINET.out.kvm.zip contains:

- fortimail-kvm.qcow2: the FortiMail system hard disk in qcow2 format
- nnngb.qcow2 files: the qcow2 files for the virtual storage disk

VMware ESX/ESXi

The FORTINET-.out.ovf.zip contains multiple .ovf files for different virtual machine hardware versions and the virtual disk sizes. For example:

- `fortimail-vm-64bit-hw14.ovf: hw14` represents ESXi 6.7.
- `FortiMail VM-disk1.vmdk`
- `FortiMail VM-disk2-250gb.vmdk: 250gb` represents the virtual hard disk size of 250GB.

For the list of VMware products and their corresponding virtual machine hardware versions, see https://kb.vmware.com/s/article/1003746.

Deploying the FortiMail appliance

Prior to deploying the FortiMail appliance, the VM platform must be installed and configured so that it is ready to create virtual machines. The installation instructions for FortiMail assume that

- You are familiar with the management software and terminology of your VM platform.
- An Internet connection is available for FortiMail to contact FortiGuard to validate its license

For assistance in deploying FortiMail, refer to the deployment chapter in this guide that corresponds to your VMware environment. You might also need to refer to the documentation provided with your VM server. The deployment chapters are presented as examples because for any particular VM server there are multiple ways to create a virtual machine. There are command line tools, APIs, and even alternative graphical user interface tools.

Before you start your FortiMail appliance for the first time, you might need to adjust virtual disk sizes and networking settings. The first time you start FortiMail, you will have access only through the console window of your VM server

environment. After you configure one FortiMail network interface with an IP address and administrative access, you can access the FortiMail web-based manager.

Deployment example: VMWare

Once you have downloaded the install file and extracted the package contents to a folder on your local computer, you can use the vSphere client to create the virtual machine from the deployment package OVF template.

This section contains the following topics:

Deploying the FortiMail VM software

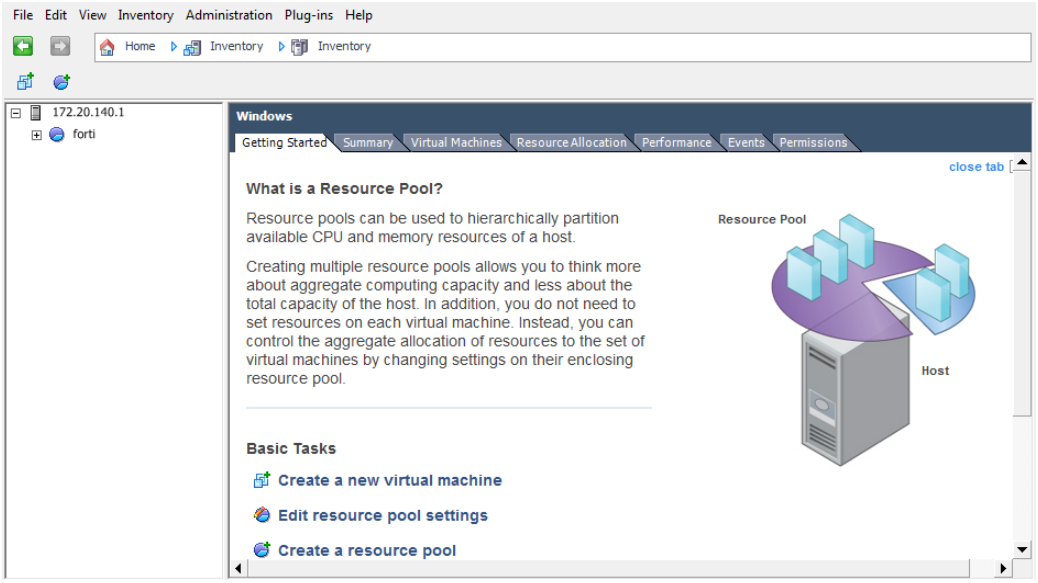
To install FortiMail VM, you must successfully deploy the OVF file using the VMware vSphere Client™.

To deploy the software

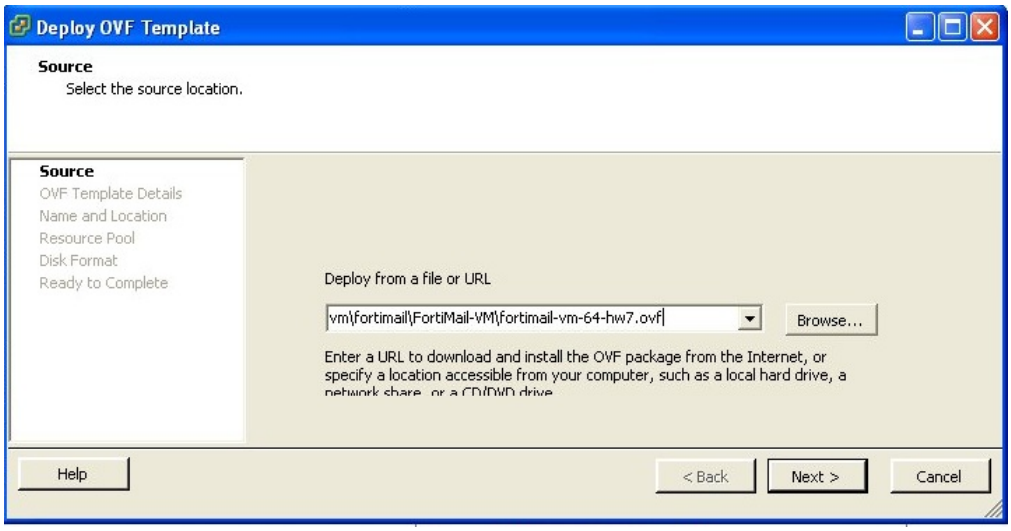
1. Start the VMware vSphere Client.
   The client's login dialog appears.

2. Enter:
   - the IP address of the ESX/ESXi server hosting VMware vSphere Hypervisor
   - an account user name on the ESX/ESXi server
   - the account password

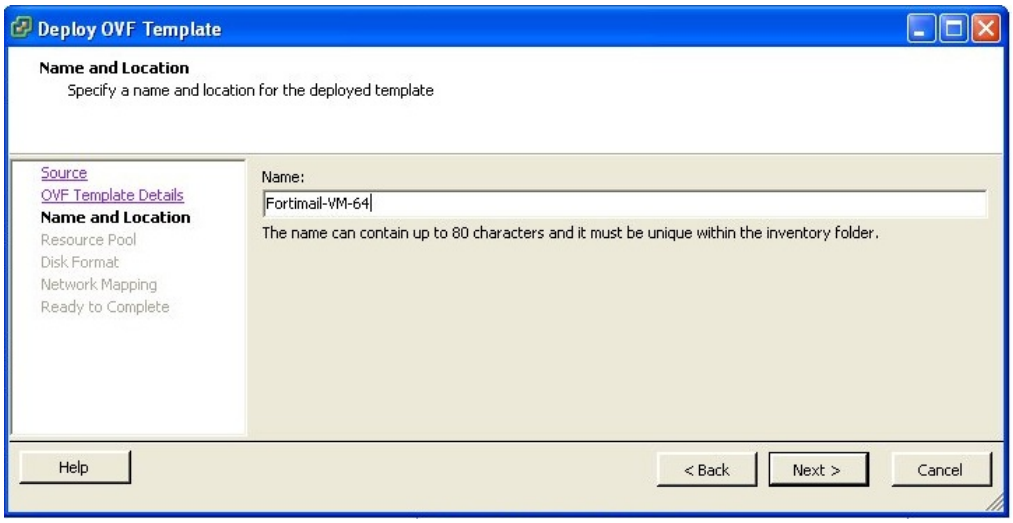
   When you successfully log in, the vSphere Client window appears.



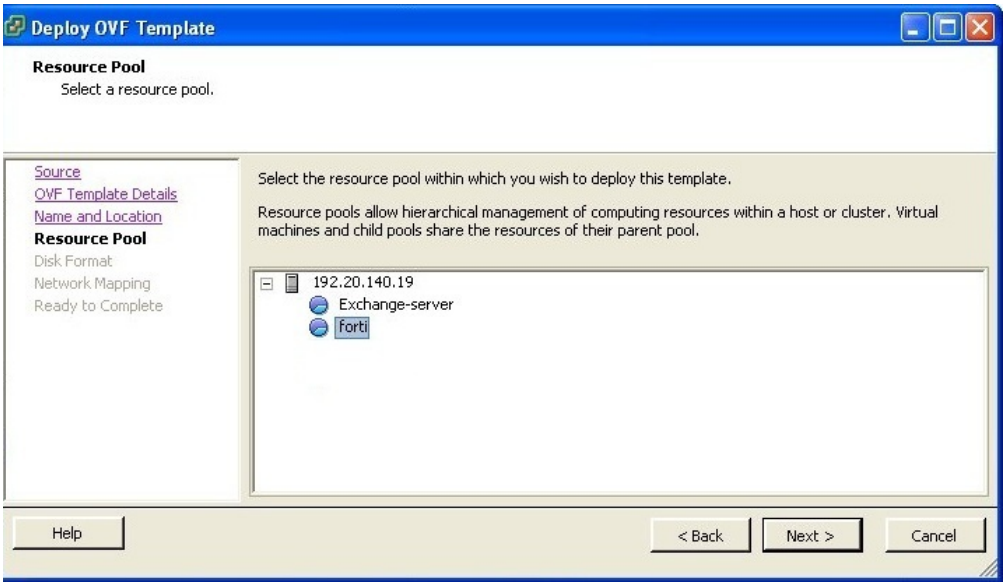
3. On the vSphere Client window, select *File* > *Deploy OVF Template*.
   The first dialog of the OVF deployment wizard appears.



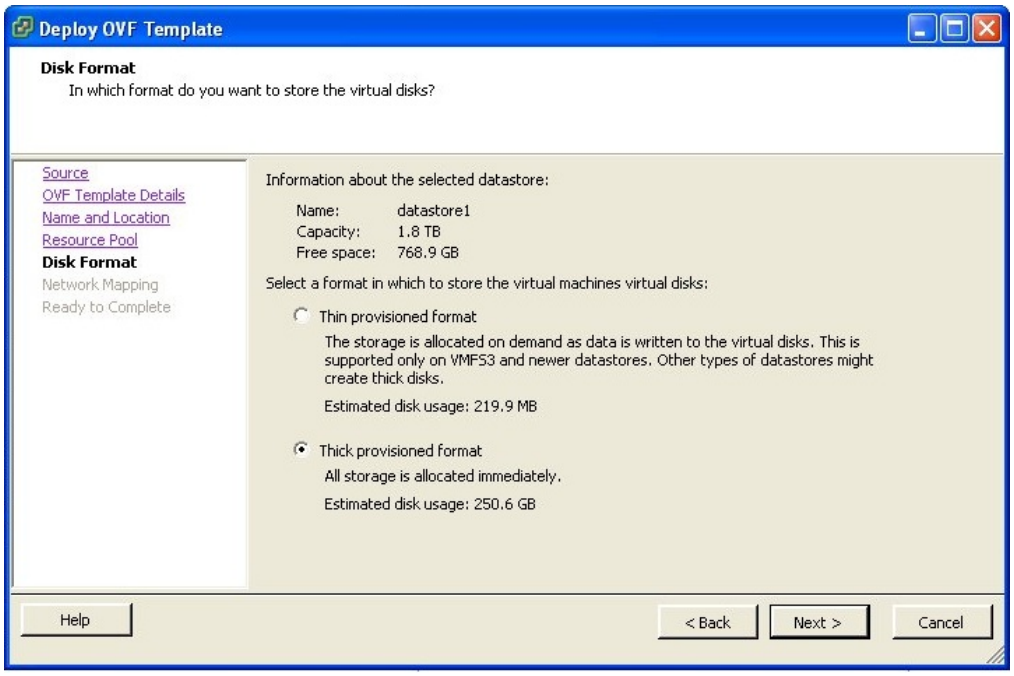
4. Select *Browse* and locate the applicable OVF template file you extracted earlier (for example, FortiMail VM-64-hw7.ovf), and click *Next*.
5. The second dialog displays the details of the deployed file. Click *Next*.
   A window appears and prompts for the name of your OVF template.



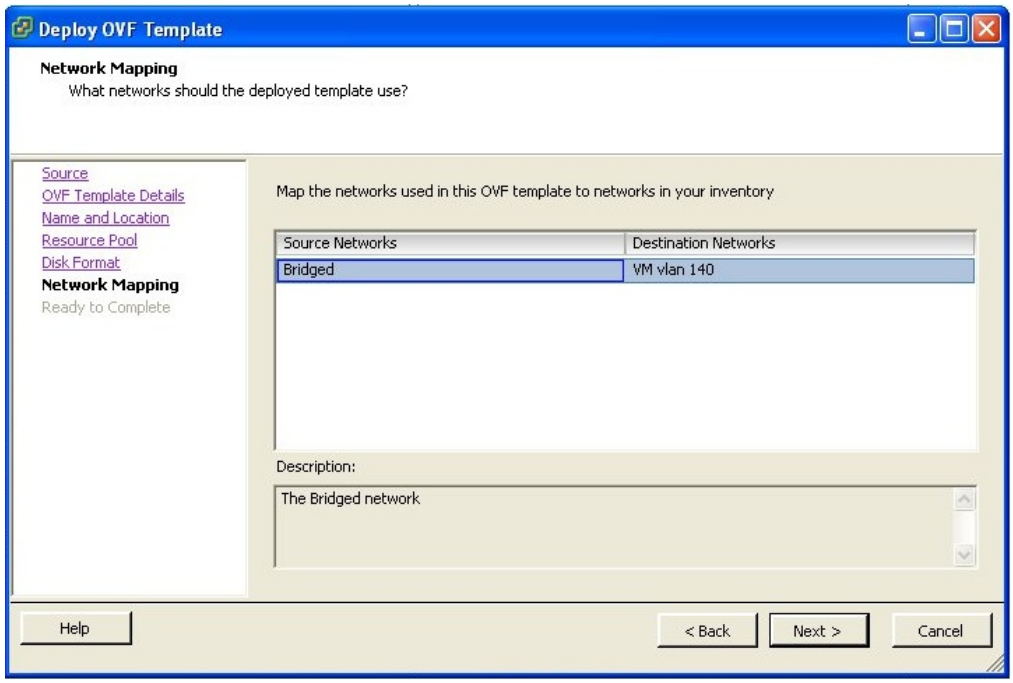
6. Enter a unique name and click *Next*. This becomes the name of your virtual machine.
   A window appears asking where to deploy the OVF template.



7. Select a resource pool and click *Next*.
   A windows appears asking for the disk storage format.

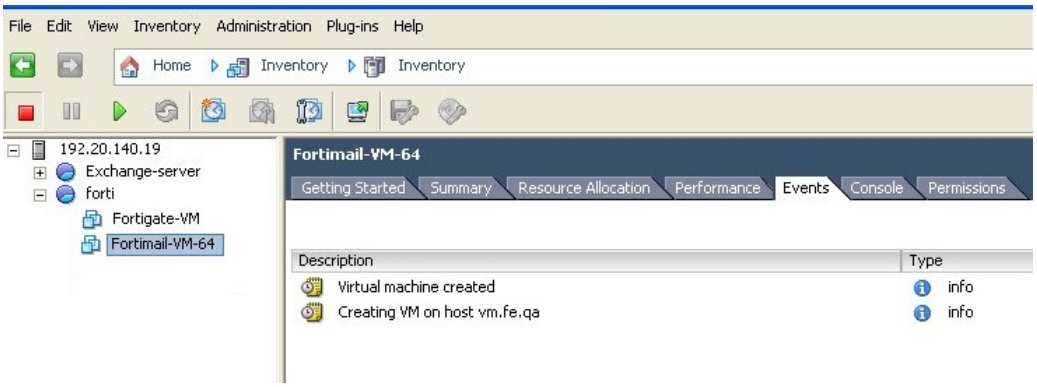


8. Select a format option and click *Next*.
   A window appears asking which network to deploy on.



9. Select a virtual network if there is more than one and click *Next*.
10. A window appears listing all your settings. Click *Finish*.
    The wizard closes.

The vSphere Client window reappears and displays your new virtual machine.



Do **not** power on FortiMail VM yet if you need to configure the virtual network first.

Configuring virtual network settings

Before you power on FortiMail VM, you may need to set the number of virtual CPUs or configure the virtual network to support your implementation of transparent mode for FortiMail VM.

This section includes:

- Preparing for transparent mode on page 15
- Configuring the number of CPUs on page 17
- Configuring a smaller disk on page 18

When you deploy the FortiMail VM OVF file, one virtual network interface card (vNIC) is automatically mapped to a port on the ESX/ESXi server. You can change the mapping, or map other vNICs if required. Each vNIC has its own MAC address and one or more IP addresses.

For more information, see the VMware vSphere documentation.

Preparing for transparent mode

If you plan to use transparent mode with your FortiMail VM installation, you need to:

- Set promiscuous mode. See To set promiscuous mode on page 16.
- Modify the network adapter configuration. See To modify a network adapter on page 17.

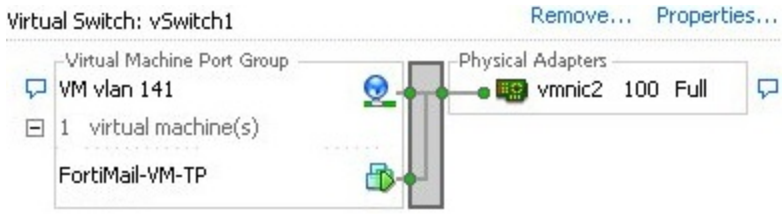
An ESX/ESXi server always has at least one vSwitch. For transparent mode, you need at two vSwitches, one to connect FortiMail VM to the network and one to connect it to the mail server.

Add an additional vSwitch if necessary.

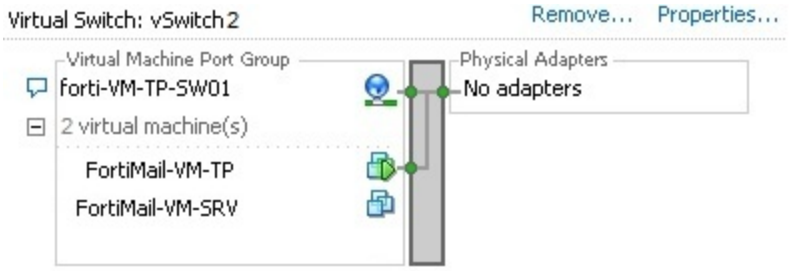
The following example of vSwitch creation shows connection to a virtual mail server hosted on the same ESXi server. For a physical mail server, you need to connect to a physical NIC.

To add a virtual switch

1. Log in to the vSphere Client.
2. **Do not** power on FortiMail VM.
3. Select the host IP at the top of the left navigation pane.
4. On the *Configuration* tab, select *Networking*.
   A window with information similar to the image below appears.



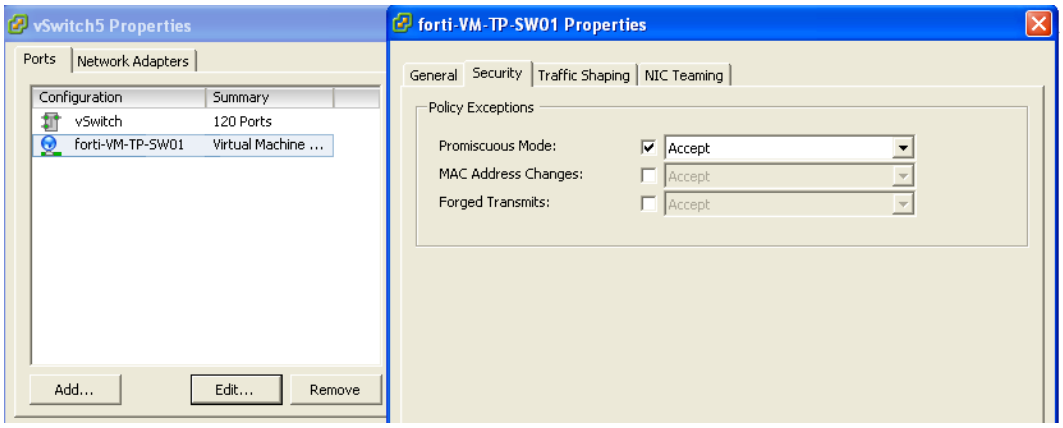
5. Select the *Virtual Switch* view and click *Add Networking*.
6. Accept the default connection type, *Virtual Machines*, and click *Next*.
7. Select *Create a virtual switch* and click *Next*.
8. Under *Port Group Properties*, enter a network label that identifies the port group to create.
9. Click *Finish*.



Next, set the network to run in promiscuous mode.

To set promiscuous mode

1. On the *Configuration* tab, select *Networking*.
2. For each virtual switch, select *Properties*.



3. On the *Ports* tab, click *Edit*.
   A dialog appears.

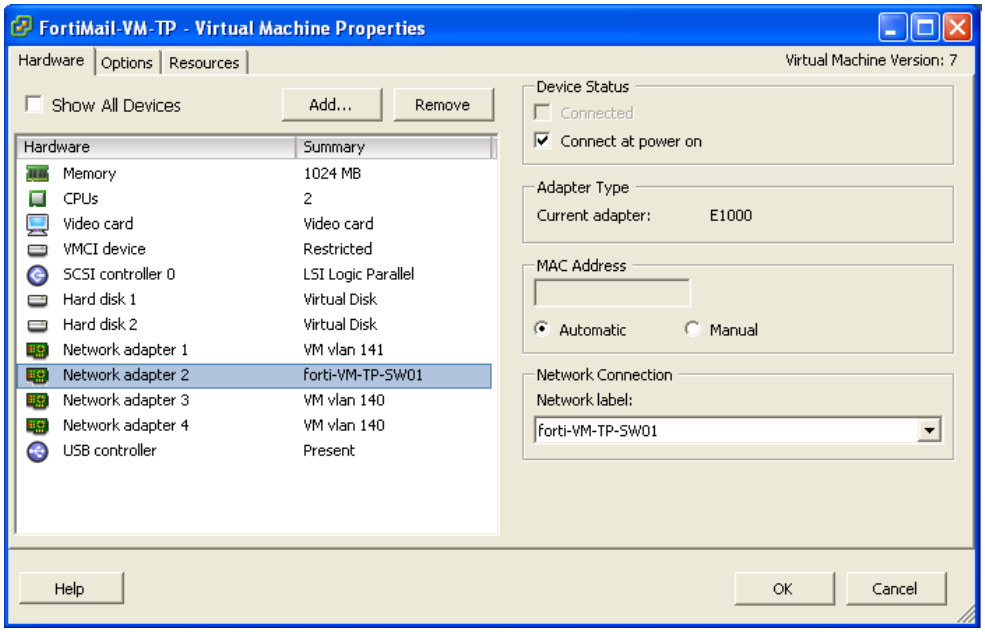
4. Select the *Security* tab.
5. Select *Accept* from the drop-down list for *Promiscuous Mode*.

The setting on the port group overrides the virtual switch setting.

Next, you need to link a FortiMail VM network adapter to each new vSwitch.

To modify a network adapter

1. Select your FortiMail VM machine in the left navigation pane.
2. On the *Getting Started* tab, select *Edit Virtual Machine Settings.*
3. On the *Hardware* tab, select a network adapter from the hardware list.



4. Select the new vSwitch from the *Network label* drop-down list.
5. Click *OK*.

Later, configure the applicable FortiMail VM port or ports using the web-based manager. See Configuring the network interfaces section in the *FortiMail Administration Guide*.

Configuring the number of CPUs

You may have more than one CPU depending on the type of license you purchased. By default, FortiMail VM is set to one CPU. You can change the number of CPUs that the virtual machine uses by changing the number of virtual processors (you cannot change the CPU setting while FortiMail VM is running).

To change the number of CPUs

1. Make sure FortiMail VM is not running.
2. Go to the *Hardware* tab.

3. Select *CPUs* in the hardware list.
4. In the CPUs drop-down list, select the number of virtual processors for the virtual machine.
5. Click *OK*.

Maintaining license limits

If you set the number of CPUs or memory beyond your license limit, your FortiMail VM license becomes invalid. To determine if you have exceeded license limits, use the following CLI command:

```
get system status
```

If so, use the vSphere Client to restore valid settings.

Configuring a smaller disk

FortiMail VM comes prepackaged with a 1-TB disk. An alternate configuration with a 250-GB disk is provided for installing in a VMware datastore that does not support a 1-TB disk.

If neither of these sizes suits your resources, you can configure FortiMail VM to support a disk size as small as 50 GB. Starting from v4.0 MR3 Patch 1, you can even configure the virtual disk to as small as 5 GB. The FortiMail VM system will still be able to start up with warnings. However, the system will not start up if the virtual disk is smaller than the 5 GB minimum size.

To reduce the disk size

1. Stop FortiMail VM if it is running.
2. Log in to the vSphere Client.
3. On the *Hardware* tab, select either the 250-GB or 1-TB disk (Hard Disk 2) in the hardware list.
4. Click *Remove*.
5. Click *OK*.
6. Click *Add* and select *Hard Disk*.
7. Configure the new disk.
   The *Virtual Device Node* setting must be SCSI (0:1).
8. Complete the disk configuration and click *OK*.
9. Start the FortiMail VM.
   If FortiMail VM was previously run, you need to manually initialize this new disk.
10. Log in as the administrator and run the CLI command:
    ```
    execute partitionlogdisk 10
    ```

Starting FortiMail VM

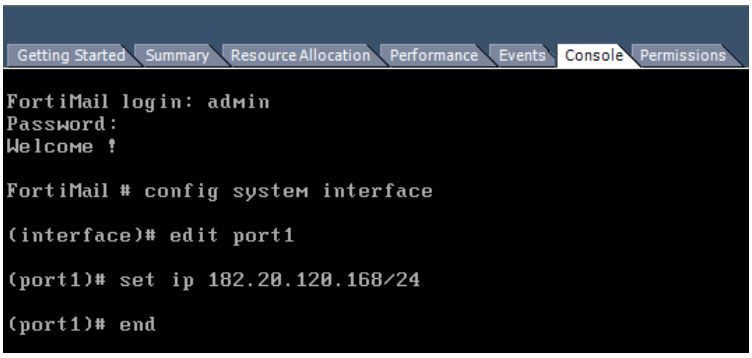
Once you successful deploy the OVF file and set up the network (if required), you need to power on your FortiMail VM virtual appliance and enter initial setup commands.

To power on FortiMail VM

1. Log in to the vSphere Client.
2. Select your newly deployed FortiMail VM virtual machine in the left navigation pane of vSphere Client and power it on.
   There are several ways to power on a virtual machine. The easiest is to click the green triangle icon on the icon bar.
3. Select the *Console* tab in the vSphere Client window.
   When you power on the virtual appliance, the console displays a sequence of messages ending in a login prompt.

At this point, you have accessed the FortiMail VM command line interface (CLI) but you do not have access to all CLI commands until you confirm the license in a later step.

4. Press the Enter key once to get a new prompt, and log in using the default FortiMail VM administrator name, `admin`. There is no password yet for this administrator. Press *Enter* when prompted.
   You will see a welcome message.
5. Use CLI commands to configure the IP address of a virtual interface (usually port1) on the virtual appliance to use for administrative access.
   You will later access the FortiMail VM web-based manager through a browser at this IP.



   Enter the following CLI commands in the vSphere Client console:

```
config system interface
   edit <port_name>
      set ip <ipv4-mask>
end
```

   Where:

   - `port_name` is the name of the FortiMail VM virtual port (usually port1)
   - `ipv4-mask` is the IP (with a netmask) of your virtual machine on the the ESX/ESXi server

Take note of the IP you enter. Later, you will use that IP, minus the netmask, to configure and manage FortiMail VM through the CLI or web-based manager.

6. Use CLI commands to configure a static route to act as a default gateway. This is needed for license updates.
   Enter the following CLI commands in the vSphere Client console:

```
config system route
   edit <index_int>
      set gateway <gateway_ipv4>
end
```

Where:

- `<index_int>` is the index number, such as 1, of the route in the list of static routes
- `<gateway_ipv4>` is the IP address of the gateway router

To log on to the FortiMail VM web UI

When you successfully configure administrative access, the web-based manager login dialog may appear automatically if you have a browser open.

If not, open a browser and enter the IP address of the virtual interface your set in Step 5 and include `/admin` with the URL; for example:

`https://192.168.1.99/admin`

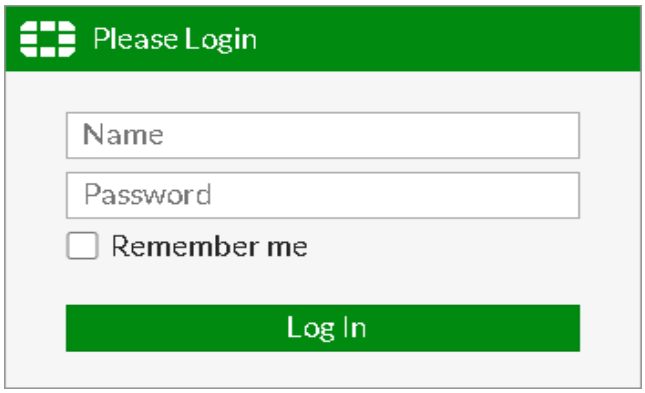
FortiMail VM start-up settings:

Web-based administrator URL	https://<virtual-ipaddress>/admin
Administrator account	admin
Administrator password	none
Management access	HTTPS, SSH, ping
Operation mode	gateway mode
Webmail URL	https://<virtual-ipaddress>

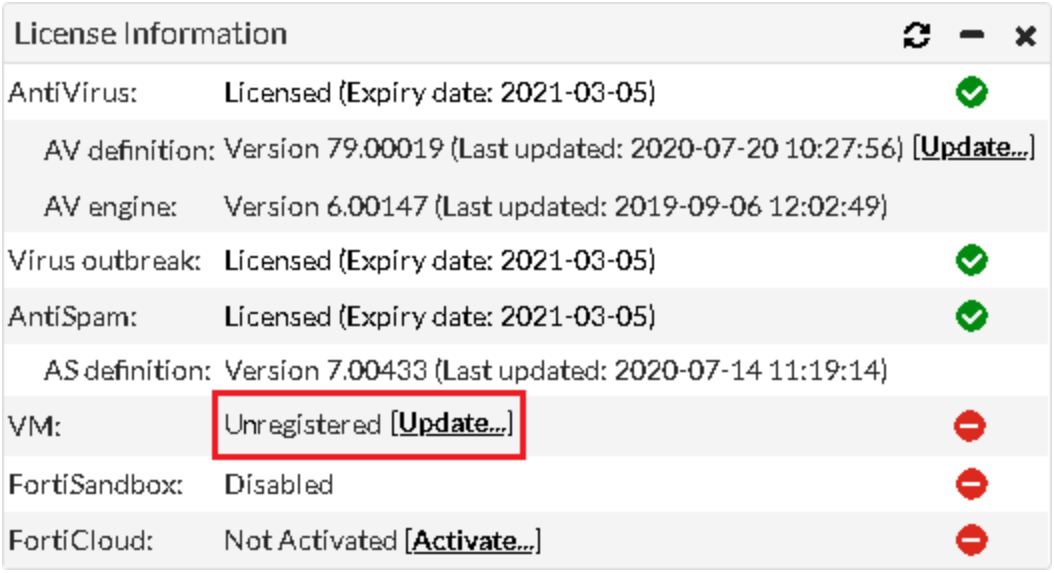
If you are connecting to FortiMail VM with a trial license or a LENC version of FortiMail, you may not be able to see the logon page due to an SSL cipher error during the connection. In this case, you must configure the FortiMail interface to allow HTTP connections and access it with HTTP only.

```
config system interface
   edit port1
      set allowaccess http
end
```

1. On the logon page, in *Name*, enter `admin`.
2. Skip the *Password* field (until you assign the `admin` a password later).
3. Click *Logon*.



The FortiMail web-based manager opens at the dashboard. Notice the VM status in the *License Information* widget.



Installing the license

If you have a FortiMail VM license (for details, see Licensing on page 6), you can install it now after you start up FortiMail VM.

To install the license

1. In the *License Information* widget on the FortiMail VM web-based manager, click the *Update* link to the right of *VM*.
2. Locate and select the license file (.lic) you downloaded earlier from Fortinet.
3. Click *Open*.
   A message box appears stating your license is being authenticated. This may take a few minutes.
   If you uploaded a valid license, a second message box will appear informing you that your license authenticated successfully.
4. Click *OK* on the message box.
   The system will reload and log out.
5. Log in again if prompted using `admin`, as the user name.

Congratulations! You have successfully installed FortiMail VM and can now configure your virtual appliance.

Deployment example: Hyper-V

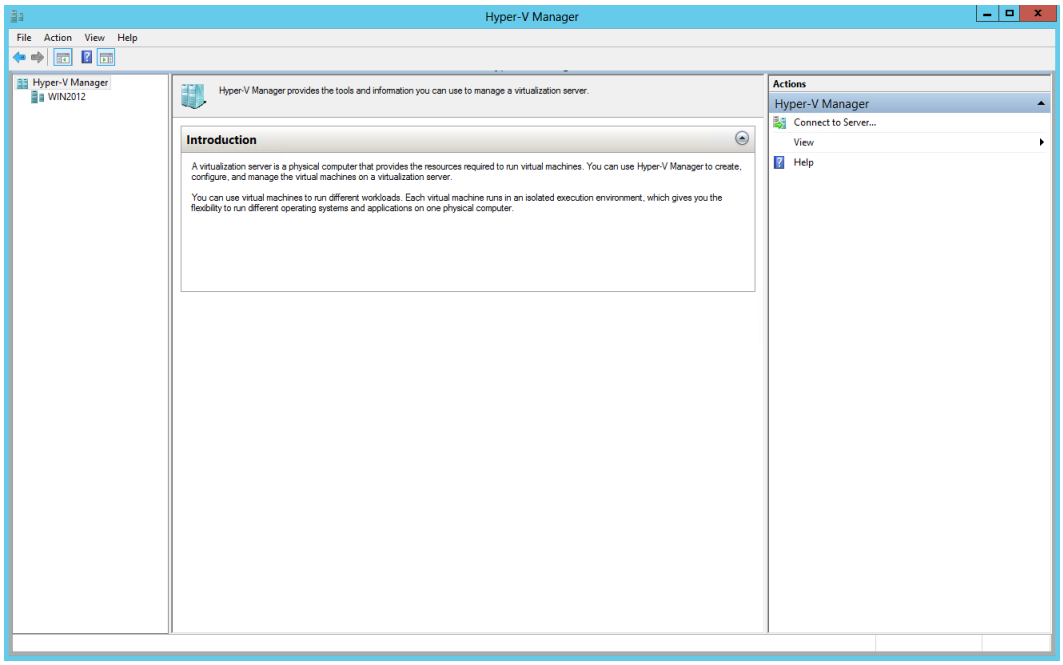
Once you have downloaded the `.hyperv.zip` file and extracted the package contents to a folder on your Microsoft server, you can deploy the VHD package to your Microsoft Hyper-V environment.

The following topics are included in this section:

Creating the FortiMail VM virtual machine

To create the FortiMail VM 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 is displayed.
3. Right-click the server and select *New* and select *Virtual Machine* from the menu. Optionally, in the *Actions* menu, select *New* and select *Virtual Machine* from the menu.
   The *New Virtual Machine Wizard* opens.
4. Select *Next* to create a virtual machine with a custom configuration.
   The *Specify Name and Location* page is displayed.

5. Enter a name for this virtual machine. For example, FortiMail-VM. The name is displayed in the Hyper-V Manager.
6. Select *Next* to continue. The *Assign Memory* page is displayed.
7. Specify the amount of memory to allocate to this virtual machine. The default memory for FortiMail VM is 2GB (2048MB).
8. Select *Next* to continue. The *Configure Networking* page is displayed.
   Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected. FortiMail VM requires four network adapters. You must configure network adapters in the *Settings* page.
9. Select *Next* to continue. The *Connect Virtual Hard Disk* page is displayed.
10. Select to use an existing virtual hard disk and browse for the `fortimail-hv.vhd` file that you downloaded from the Fortinet Customer Service & Support portal.
11. Select *Next* to continue. The *Summary* page is displayed.
12. To create the virtual machine and close the wizard, select *Finish*.

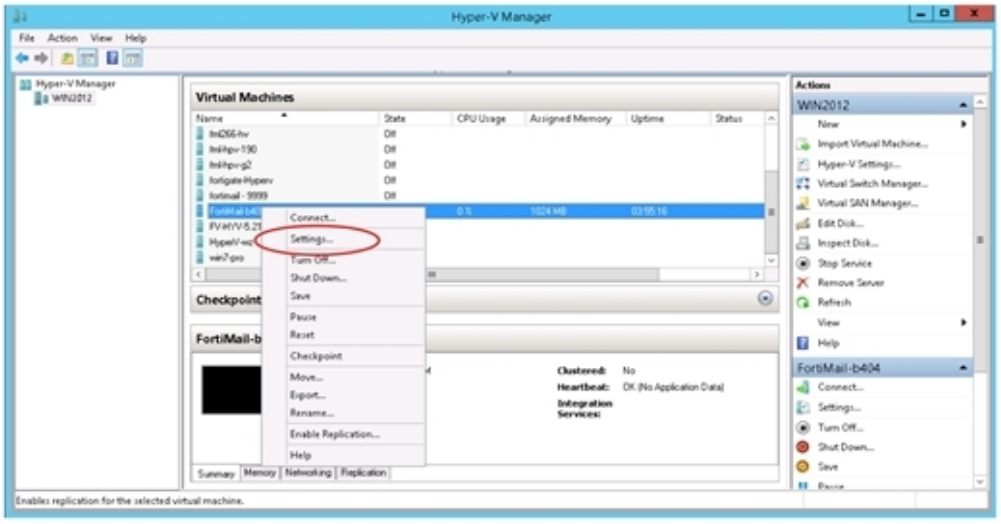
Configuring FortiMail VM hardware settings

Before powering on your FortiMail VM you must configure the virtual CPU, and create network adapters and virtual disk configuration to match your FortiMail VM license. See Licensing on page 6 for FortiMail VM license information.

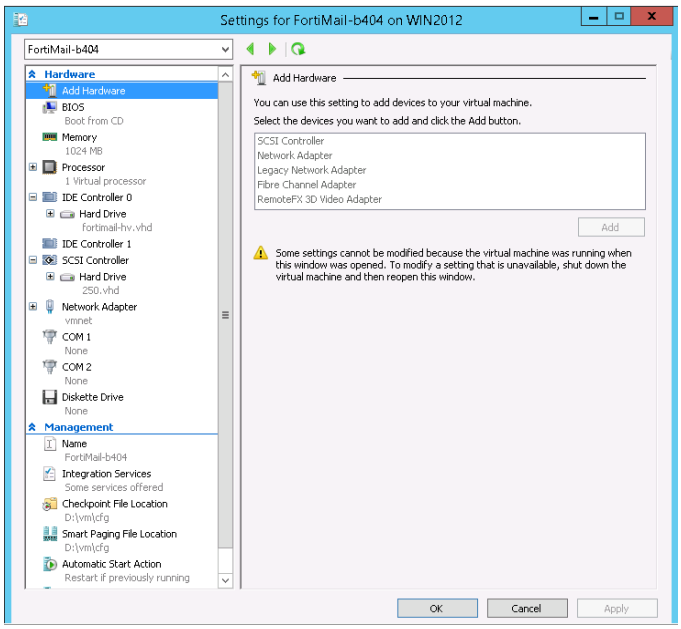
It is recommended to configure the FortiMail VM hardware settings prior to powering on the FortiMail VM.

To configure settings for FortiMail VM on the server:

1. In the Hyper-V Manager, locate the name of the virtual machine, right-click the entry, and select *Settings* from the menu. Optionally, you can select the virtual machine and select *Settings* in the *Actions* menu.



The *Settings* page is displayed.



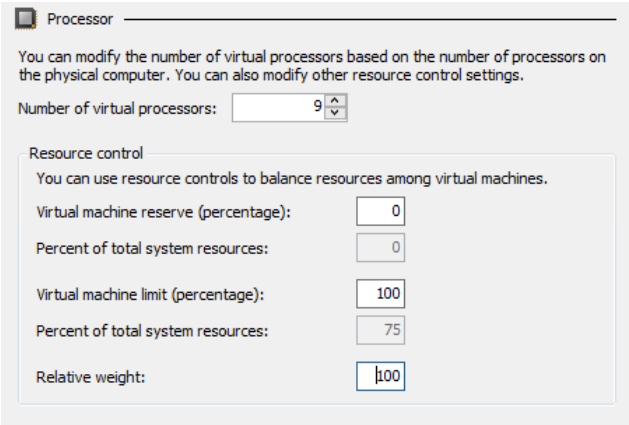
2. Configure virtual processors, network adapters, and virtual hard drive settings.
3. Select *Apply* to save the settings and then select *OK* to close the settings page.

FortiMail VM virtual processors

You must configure FortiMail VM virtual processors in the server settings page. The number of processors is dependent on your server environment.

Configure FortiMail VM virtual processors:

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



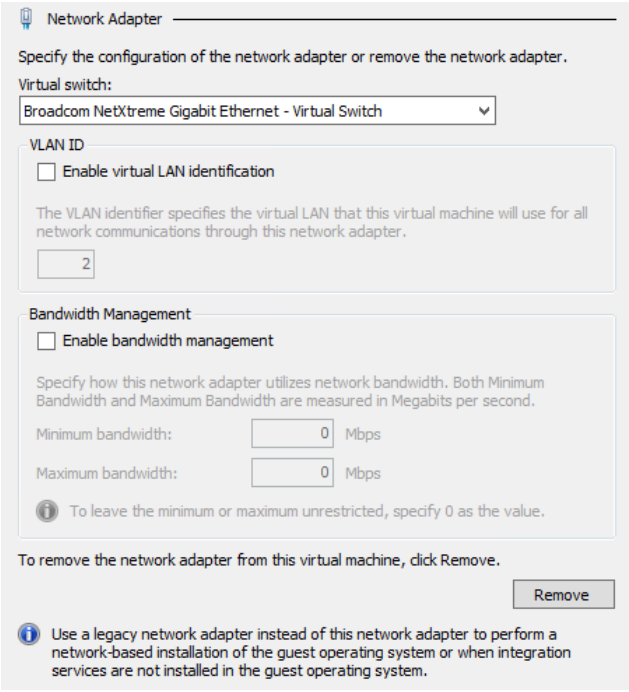
2. Configure the number of virtual processors for the FortiMail VM virtual machine. Optionally, you can use resource controls to balance resources among virtual machines.
3. Select *Apply* to save the settings.

FortiMail VM network adapters

You must configure FortiMail VM network adapters in the server settings page. FortiMail VM supports four network adapters.

Configure FortiMail VM network adapters:

1. In the *Settings* page, select *Add Hardware* from the *Hardware* menu, select *Network Adapter* in the device list, and select the *Add* button.
   The *Network Adapter* page is displayed.



2. You must manually configure four network adapters for FortiMail VM in the settings page. For each network adapter, select the virtual switch from the drop-down list.
3. Select *Apply* to save the settings.

FortiMail VM virtual hard disk

You must configure the FortiMail VM virtual hard disk in the server settings page.

FortiMail VM requires at least two virtual hard disks. Before powering on the FortiMail VM, you need to add at least one more virtual hard disk. The default hard drive, `fortimail-hv.vhd`, contains the operating system. The second hard drive will be used for logs and mail data.

If you know your environment will expand in the future, it is recommended to add hard disks larger than the 250GB FortiMail VM base license requirement. This will allow your environment to be expanded as required while not taking up more space in the SAN than is needed.

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

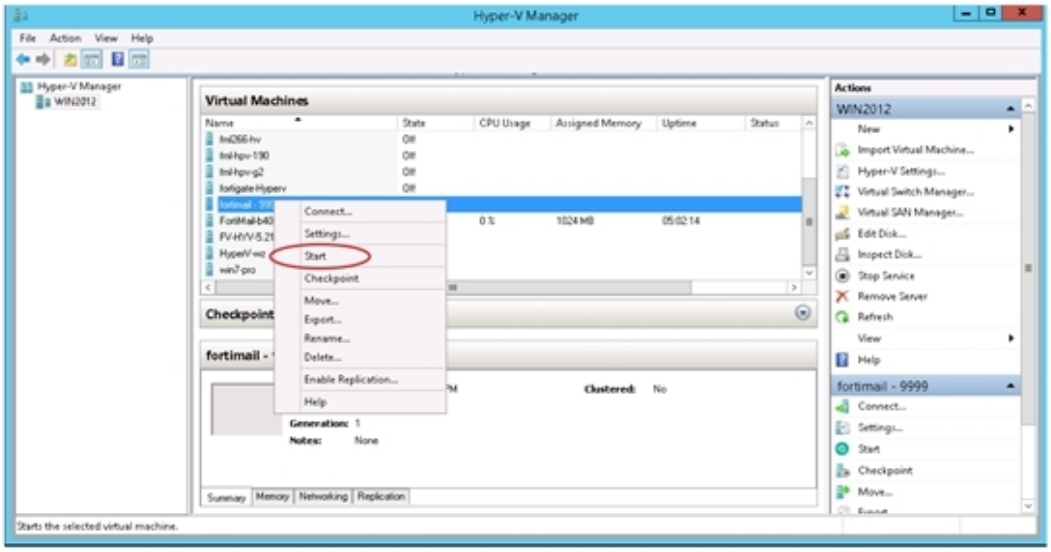
```
execute lvm enable
execute lvm extend <arg ..>
```

Create a FortiMail VM virtual hard drive:

1. In the *Settings* page, select *IDE Controller 1* from the *Hardware* menu.
2. Select *Virtual Hard Disk*.
3. Select *Browse* and select the .vhd file that matches your license.
4. Select *OK*.

Starting FortiMail VM

You can now proceed to power on your FortiMail VM. Select the name of the FortiMail VM in the list of virtual machines, right-click, and select *Start* in the menu. Optionally, you can select the name of the FortiMail VM in the list of virtual machines and select *Start* in the *Actions* menu.



FortiMail VM backup

Once the FortiMail VM license has been validated you can begin to configure your device. For more information on configuring your FortiMail VM, see the *FortiMail Administration Guide* available at the Fortinet Documentation Library.

In VM environments, it is recommended that you use the Microsoft Hyper-V Manager *Snapshot* utility to backup the VM instance (depending on the Hyper-V version you use, the utility might be called checkpoint). In the event of an issue with a firmware upgrade or configuration issue, you can use *Snapshots* to revert the VM instance to a previous *Snapshot*.

To create a virtual machine snapshot:

1. In the Hyper-V Manager, locate the name of the virtual machine, right-click the entry, and select *Snapshot* from the menu. Optionally, you can select the virtual machine and select *Snapshot* in the *Actions* menu.
2. The virtual machine snapshot will be listed in the *Snapshot* pane in the Hyper-V Manager.

To apply a virtual machine snapshot:

1. In the Hyper-V Manager, locate the name of the virtual machine. All snapshots for this virtual machine are displayed in the Snapshots pane.
2. Right-click the snapshot entry, and select *Apply* from the menu.
3. Select *Apply* in the confirmation dialog box. The virtual machine's current state will be lost.

Deployment example: KVM

Once you have downloaded the install file and extracted the package contents to a folder on your local computer, you can create the virtual machine in your KVM environment.

This section contains the following topics:

Creating the FortiMail virtual machine

To create the FortiMail virtual machine:

1. Launch Virtual Machine Manager (virt-manager) on your KVM host server.
   The *Virtual Machine Manager* home page opens.
2. In the toolbar, select *Create a new virtual machine*.
3. Enter a *Name* for the VM, FortiMail-VM for example.
4. Ensure that *Connection* is localhost (this is the default.)
5. Select *Import existing disk image*.
6. Select *Forward*.
7. In *OS Type* select *Linux*.
8. In *Version*, select *Generic 2.6 and later kernel*.
9. Select *Browse*.
10. If you copied the fortimail-kvm.qcow2 file to `/var/lib/libvirt/images`, it will be visible on the right. If you saved it somewhere else on your server, select *Browse Local* and find it.
11. Select *Choose Volume*.
12. Select *Forward*.
13. Specify the amount of memory and number of CPUs to allocate to this virtual machine. The amounts must not exceed your license limits. See "Resources" on page 4.
14. Select *Forward*.
15. Expand *Advanced options*. A new virtual machine includes one network adapter by default. Select a network adapter on the host computer. Optionally, set a specific MAC address for the virtual network interface. Set *Virt Type* to *virtio* and *Architecture* to *qcow2*.
16. Select *Finish*.

Configuring FortiMail hardware settings

Before powering on your FortiMail you must add the storage disk and configure the virtual hardware of your FortiMail.

To configure settings for FortiMail on the server:

1. In the Virtual Machine Manager, locate the name of the virtual machine and then select *Open* from the toolbar.
2. Select *Add Hardware*. In the *Add Hardware* window select *Storage*.
3. Browse to the storage disk file that matches your licence, for example, 250.qcow2 (250 GB storage space) and click OK.
4. Select *Network* to add more network interfaces. The *Device type* must be *Virtio*.
   A new virtual machine includes one network adapter by default. You can add more through the Add Hardware window. FortiMail requires four or six network adapters (see Resources on page 6). You can configure network adapters to connect to a virtual switch or to network adapters on the host computer.
5. Select *Finish*.

Starting FortiMail VM

You can now proceed to power on your FortiMail. Select the name of the FortiMail in the list of virtual machines. In the toolbar, select *Console* and then select *Start*.

Deployment example: Citrix XenServer

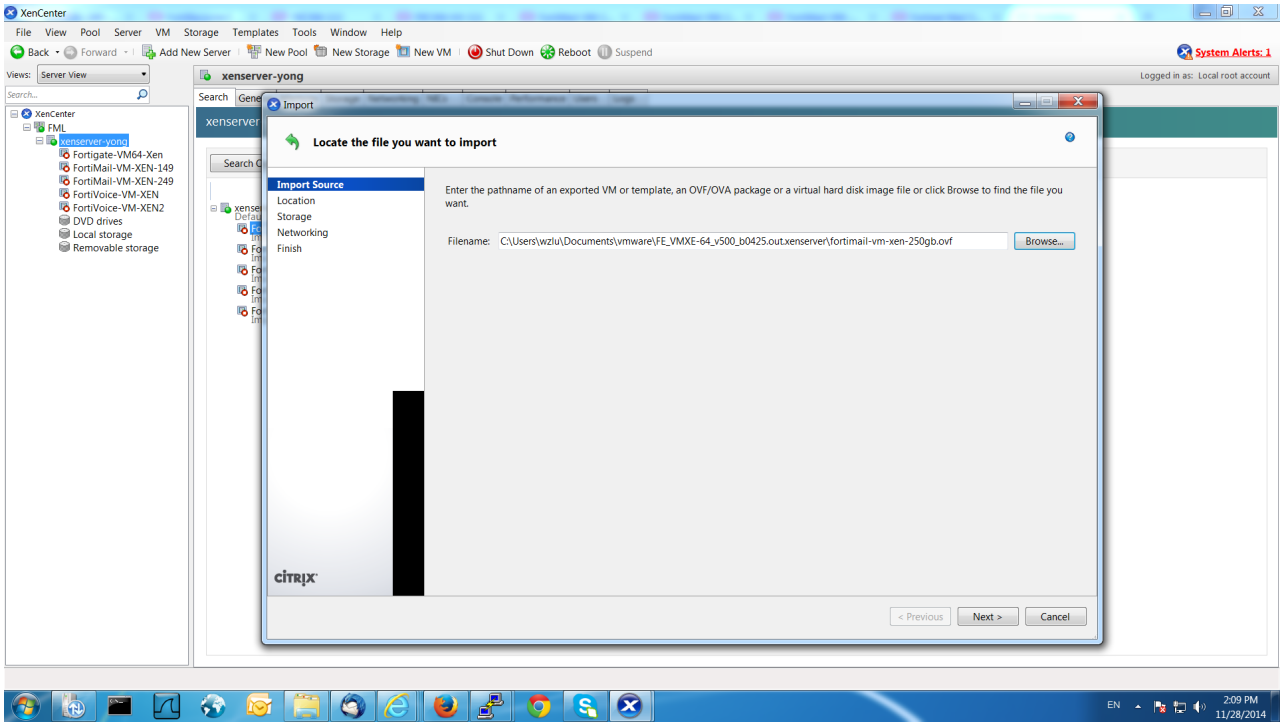
Once you have downloaded the install file and extracted the package contents to a folder on your local computer, you can create the virtual machine in your Citrix XenServer environment.

This section contains the following topics:

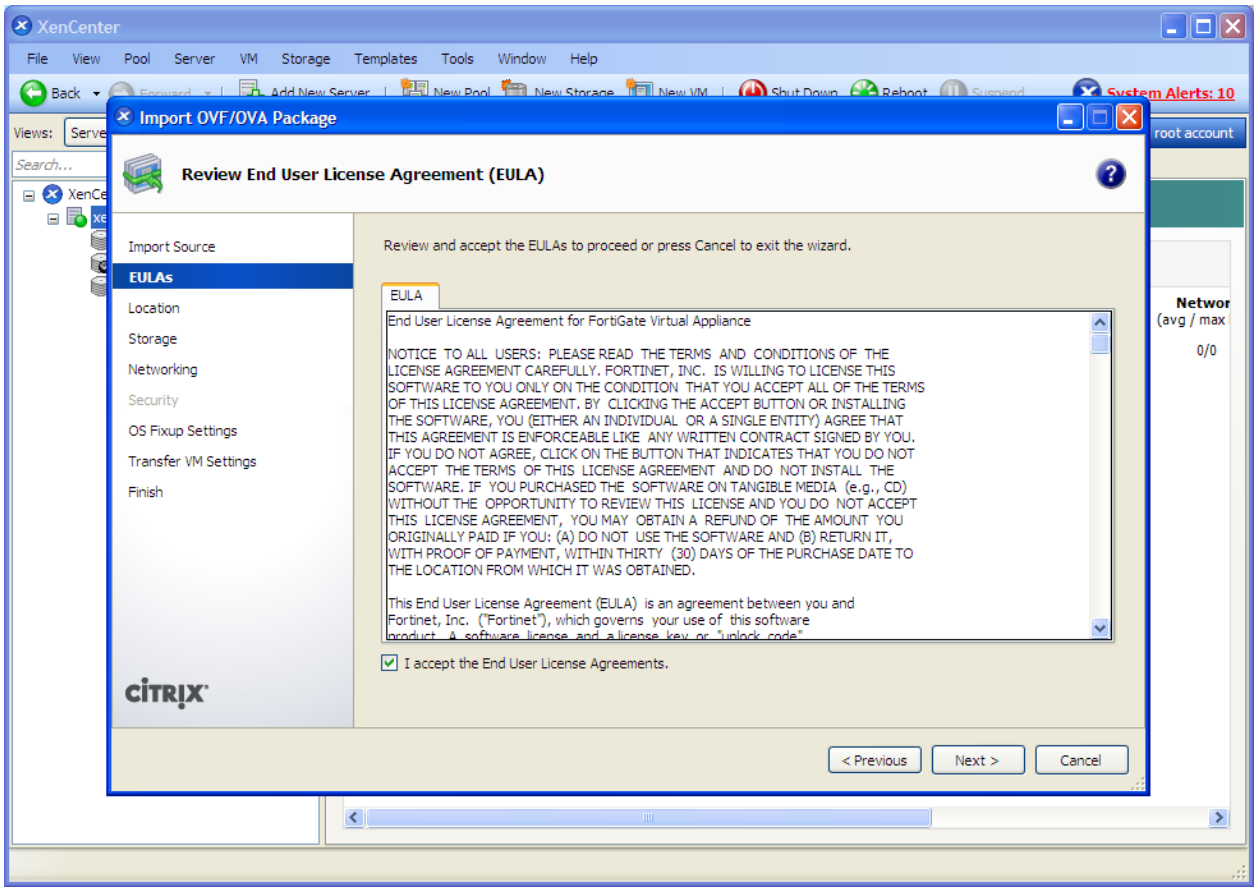
Creating the FortiMail VM virtual machine (XenCenter)

To create the FortiMail virtual machine from the OVF file

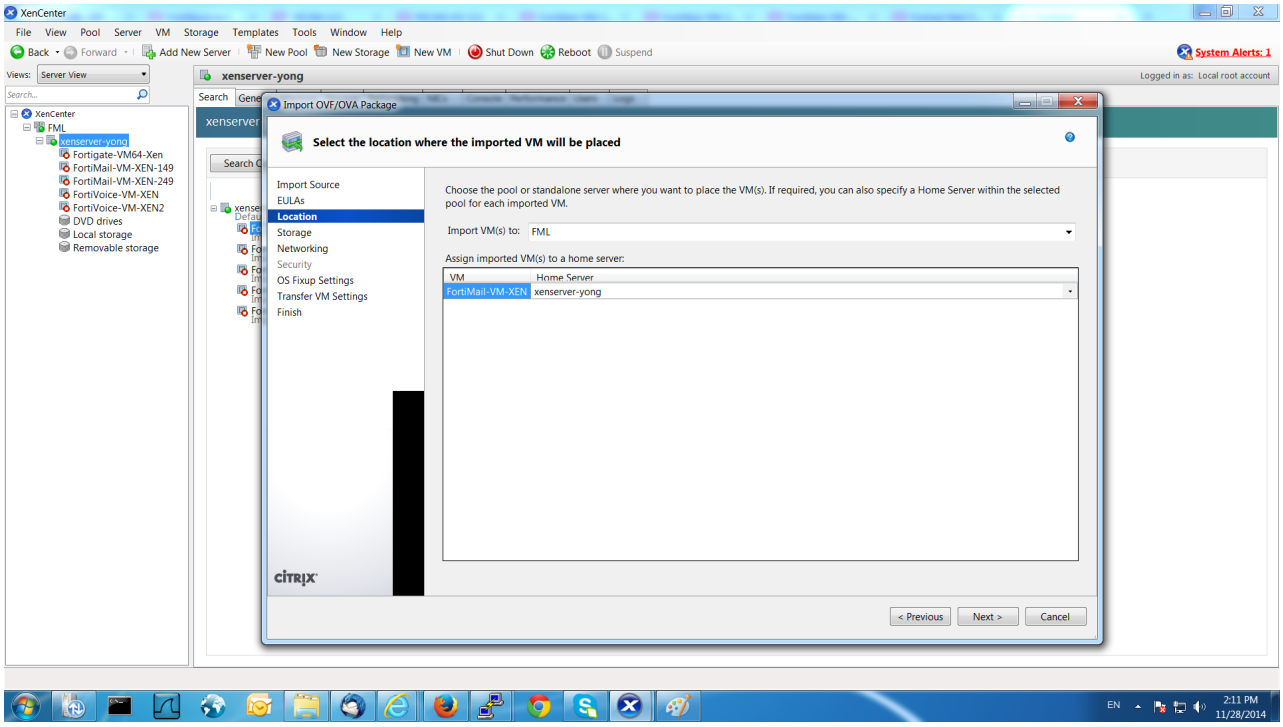
1. Launch XenCenter on your management computer.
   The management computer can be any computer that can run Citrix XenCenter, a Windows application.
2. If you have not already done so, select *ADD a server*. Enter your Citrix XenServer IP address and the root logon credentials required to manage that server.
   Your Citrix XenServer is added to the list in the left pane.
   The *Virtual Machine Manager* home page opens.
3. Go to *File* > *Import*. An import dialog will appear.
4. Click the *Browse* button, find the FortiMail .ovf template file, then click *Open*.



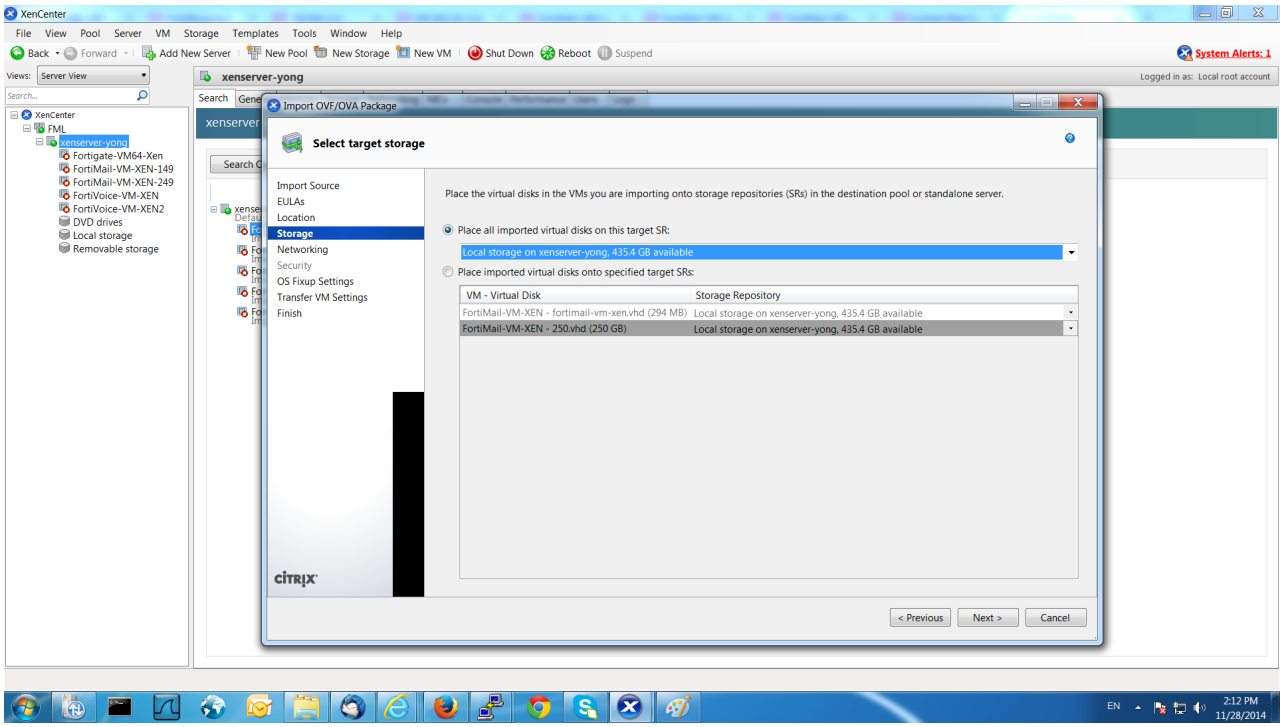
5. Select *Next*.
6. Accept the FortiMail Virtual Appliance EULA, then select *Next*.



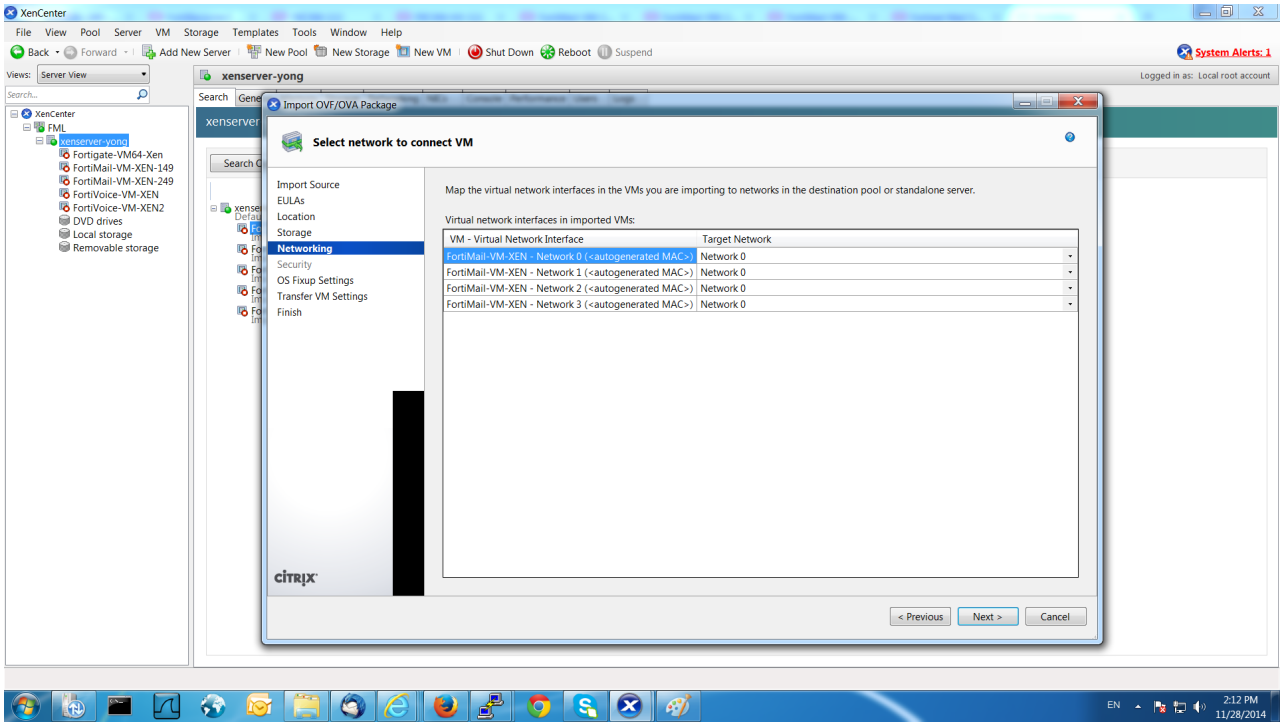
7. Choose the pool or standalone server that will host the VM, then select *Next*.



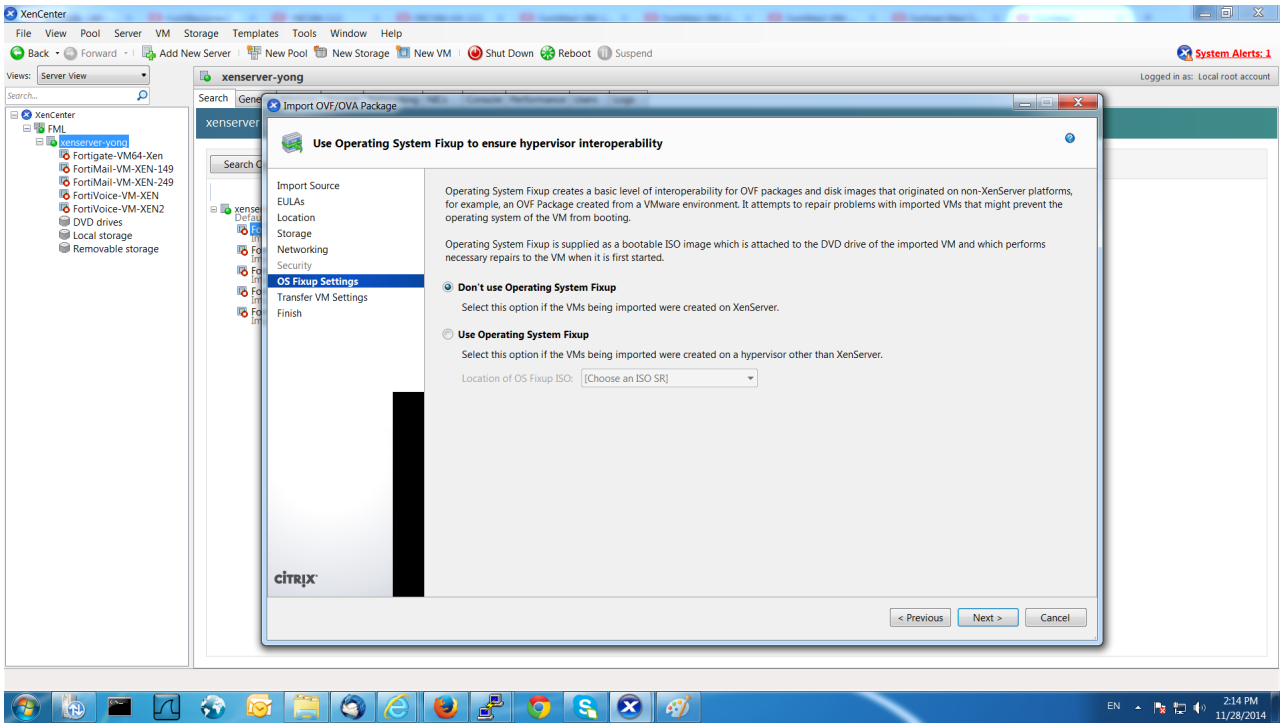
8. Select the storage location for FortiMail disk drives or accept the default. Select *Next*.



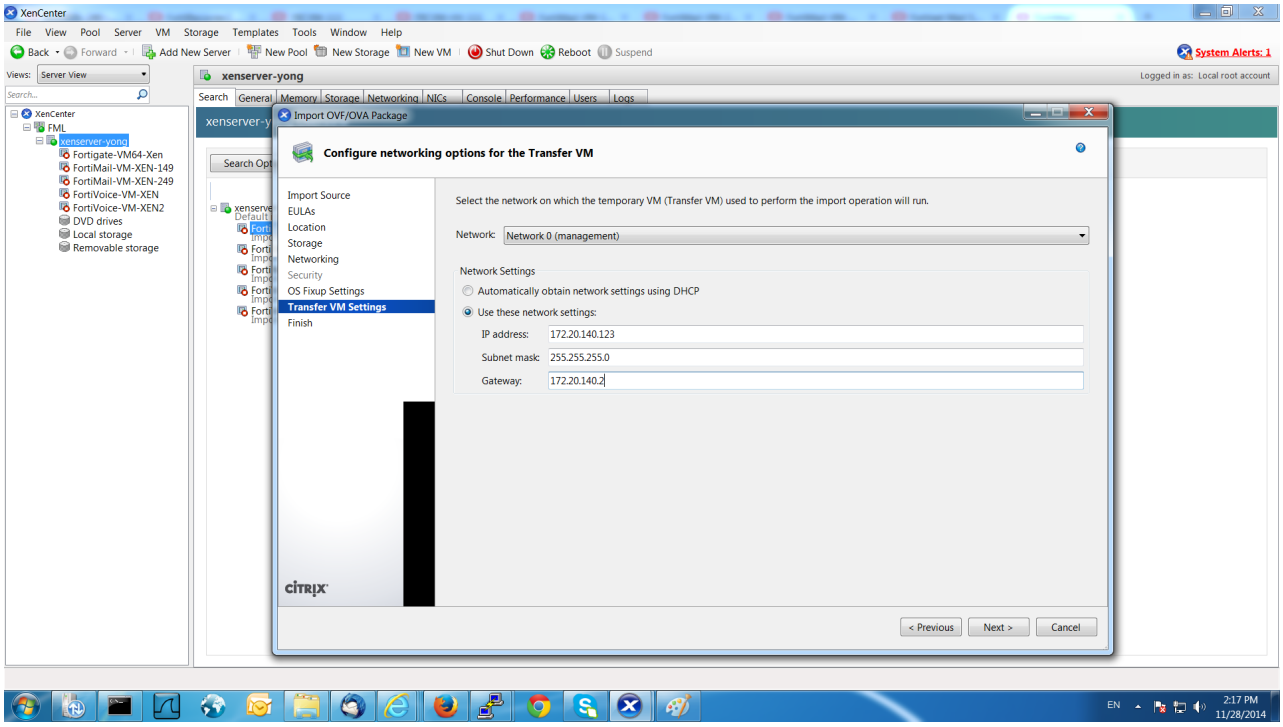
9. Configure how each vNIC (virtual network adapter) in FortiMail will be mapped to each vNetwork on the Citrix XenServer, then click *Next*.



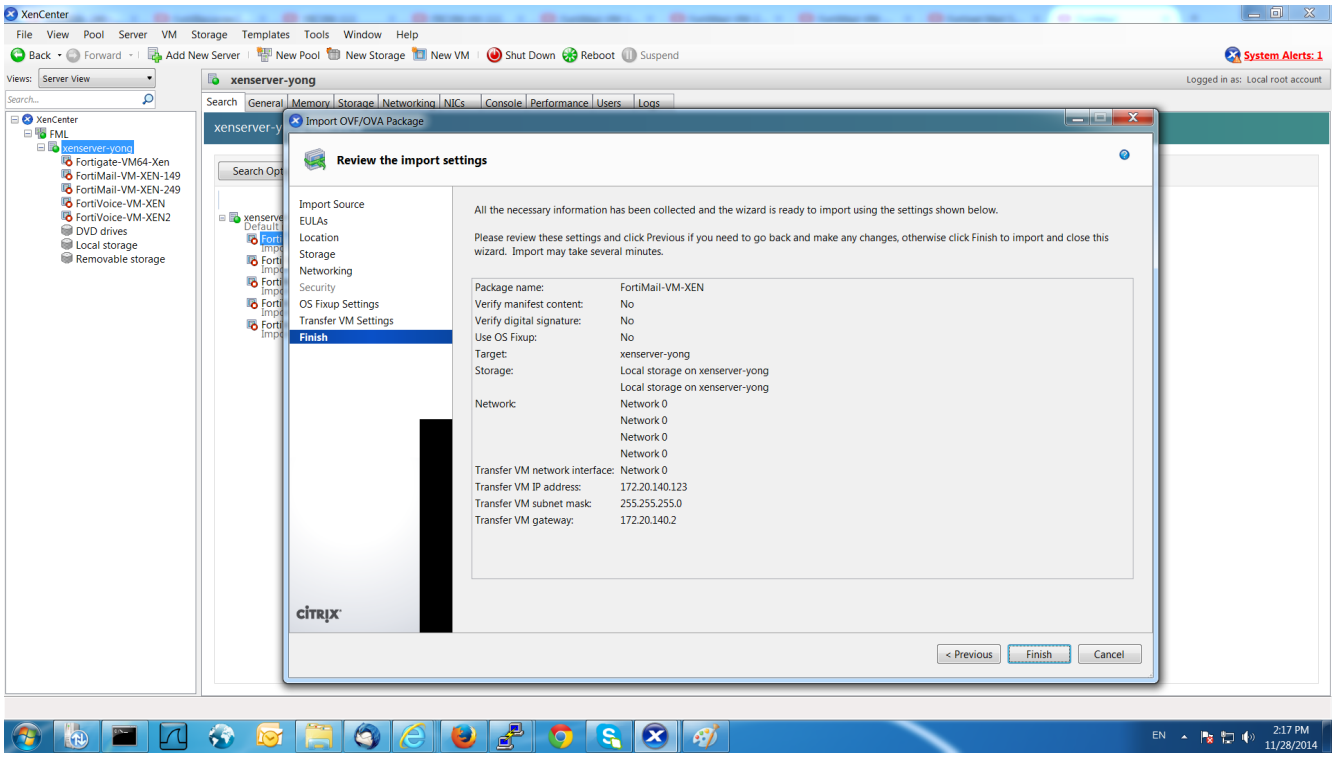
10. Click *Next* to skip OS fixup.



11. Select *Next* to use the default network settings for transferring the VM to the host.



12. Select *Finish*.



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

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

Configuring virtual hardware

Before you start your FortiMail VM for the first time, you can optionally adjust your virtual machine's virtual hardware settings to meet your network requirements.

Configuring number of CPUs and memory size

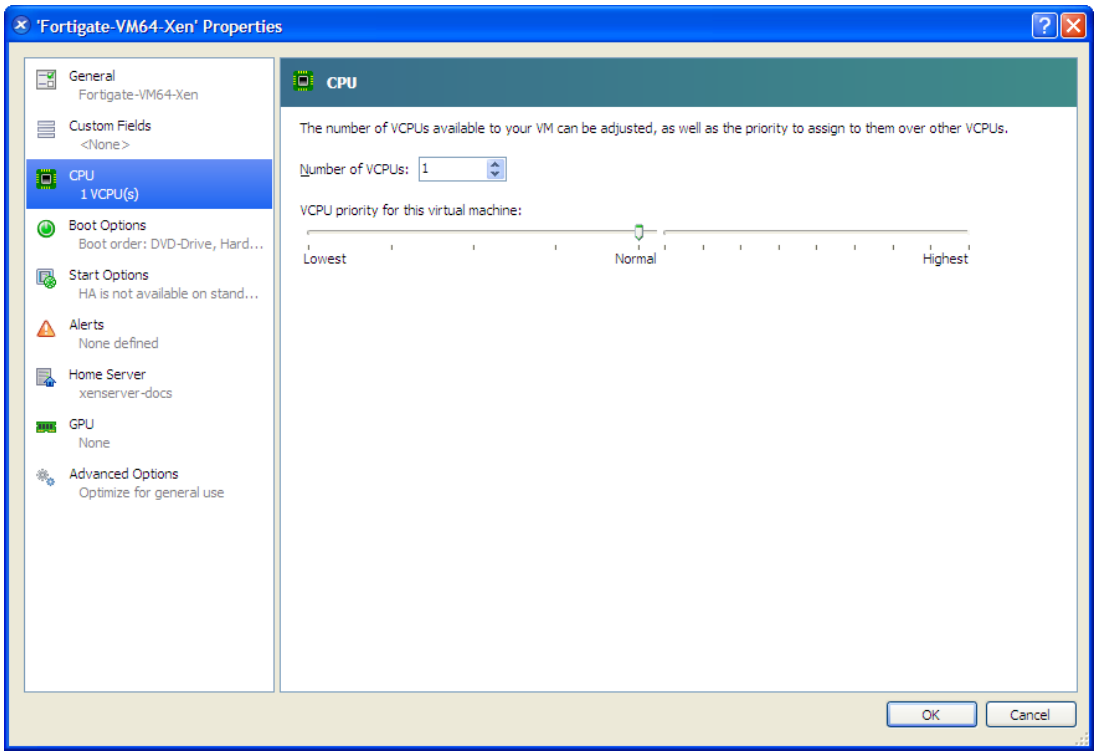
Your FortiMail VM license limits the number CPUs and amount of memory that you can use. The amounts you allocate must not exceed your license limits. See Licensing on page 6.

To access virtual machine settings

1. Open XenCenter.
2. Select your FortiMail VM in the left pane.
   The tabs in the right pane provide access to the virtual hardware configuration. The Console tab provides access to the FortiMail console.

To set the number of CPUs

1. In the XenCenter left pane, right-click the FortiMail VM and select Properties.
   The Properties window opens.
2. In the left pane, select CPU.

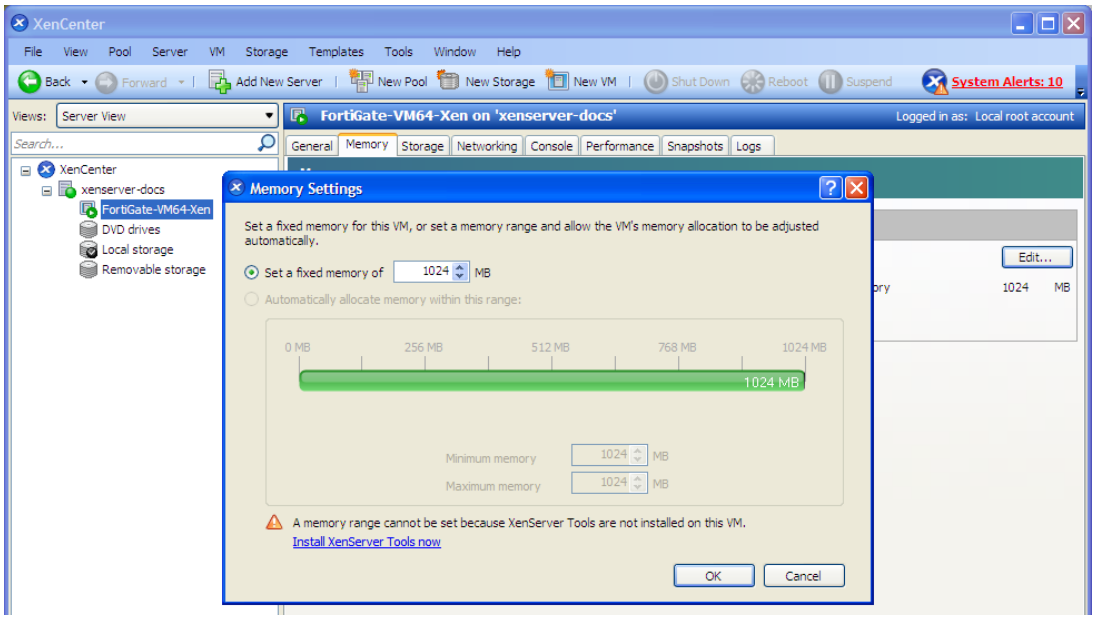


3. Adjust *Number of CPUs* and then select *OK*.
   XenCenter will warn if you select more CPUs than the Xen host computer contains. Such a configuration might reduce performance.

To set memory size

1. In the XenCenter left pane, select the FortiMail VM.
2. In the right pane, select the *Memory* tab.

3. Select *Edit*, modify the value in the *Set a fixed memory of* field and select *OK*.



Deployment example: OpenStack

FortMail VM supports cloud-init integration, allowing cross-platform cloud instance initialization. Cloud-init for FortiMail places all of its config data in OpenStack, or a content directory.

OpenStack-based clouds provide the environment needed for elastic, on-demand multitenant applications. Networks are transitioning to new models more suited to the cloud with SDN, NFV, and Virtual Network Infrastructure, and their relationships between networking, security orchestration, and policy enforcement.

You can install FML-VMKV (KVM) firmware into an OpenStack environment.

This section contains the following topics:

Overview

FortiMail VM looks for three configuration files to apply:

- **mode**: CLI command that has the system mode configured (i.e. Gateway, Server, or Transparent).
  It is recommended to set the mode before any configuration, as setting the mode effectively factory resets the system.
  Note that some configuration options are only available in certain modes.
- **config**: Any other CLI configuration that apply to the system after the mode is set.
- **license**: The VM license file.

Any combination of these configuration files (or none) may be provided.

The license file is a typical VM license (.lic) file. Below are some samples of what might be in the mode and config files:

The mode text file:

```
config system global
   set operation-mode server
end
```

The config text file:

```
config system interface
   edit port1
      set ip 172.20.140.250/24
      set allowaccess https ping ssh telnet
   next
end

config system dns
   set primary 8.8.8.8
   set secondary 4.4.4.4
end
```

```
config system route
   edit 1
      set gateway 172.20.140.2
   next
end

config system admin
   edit fmltest
      set access-profile super_admin_prof
      set password 123456
   next
end
```

Bootup the instance

To bootup a FortiMail VM instance, OpenStack can use something similar to the following command (in this example, using nova boot):

```
nova boot --flavor FML_small --image fml_image --file license=FEVM010000041191.lic --file
     config=fmlinit.txt --file mode=fmlmode.txt fml_instance
```

In this example the system will reboot twice: after loading mode and then after loading a new license.

Without OpenStack

Without OpenStack you would need to place all necessary configuration files in the Windows content directory. For example:

1. Place the configuration files in:
   `openstack/content/0000` (for example the "mode" file)
   `openstack/content/0001` (for example the "config" file)
   `openstack/content/0002` (for example the 'license' file)

   Any combination of these may be present.

2. Create or update the openstack/latest/meta_data.json file to point to these files:

```
{"files": [
{"path": "mode", "content_path": "/content/0000"},
{"path": "config", "content_path": "/content/0001"},
{"path": "license", "content_path": "/content/0002"}
]}
```

Deploying FortiMail VM in OpenStack

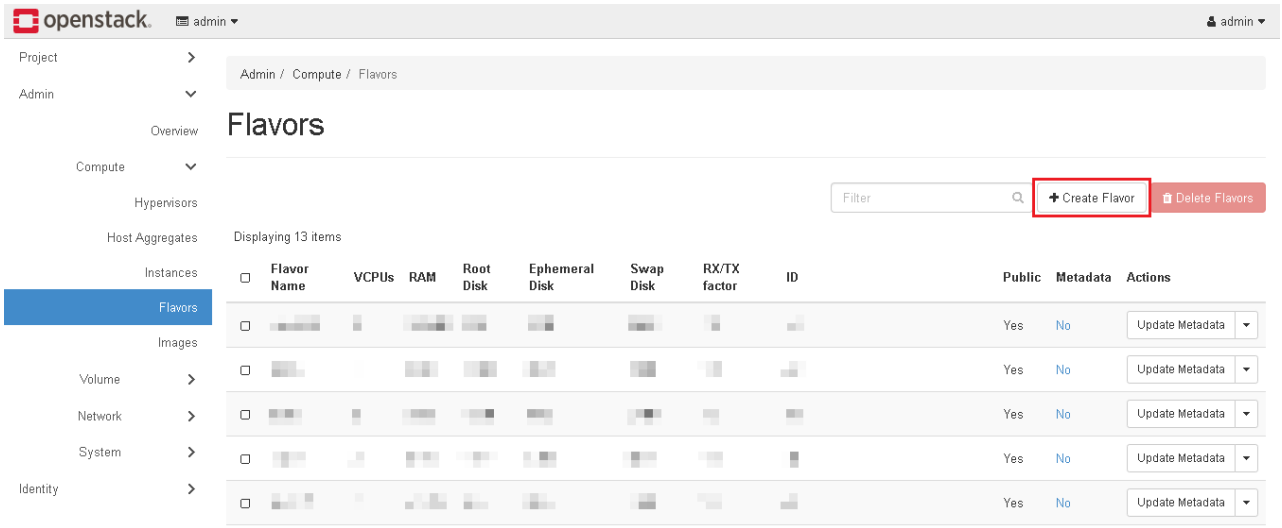
The VMware management software, in this case OpenStack Horizon, is installed on a computer with network access to the OpenStack server.

Once you have access to the OpenStack dashboard, configure the following steps to launch a FortiMail VM instance.

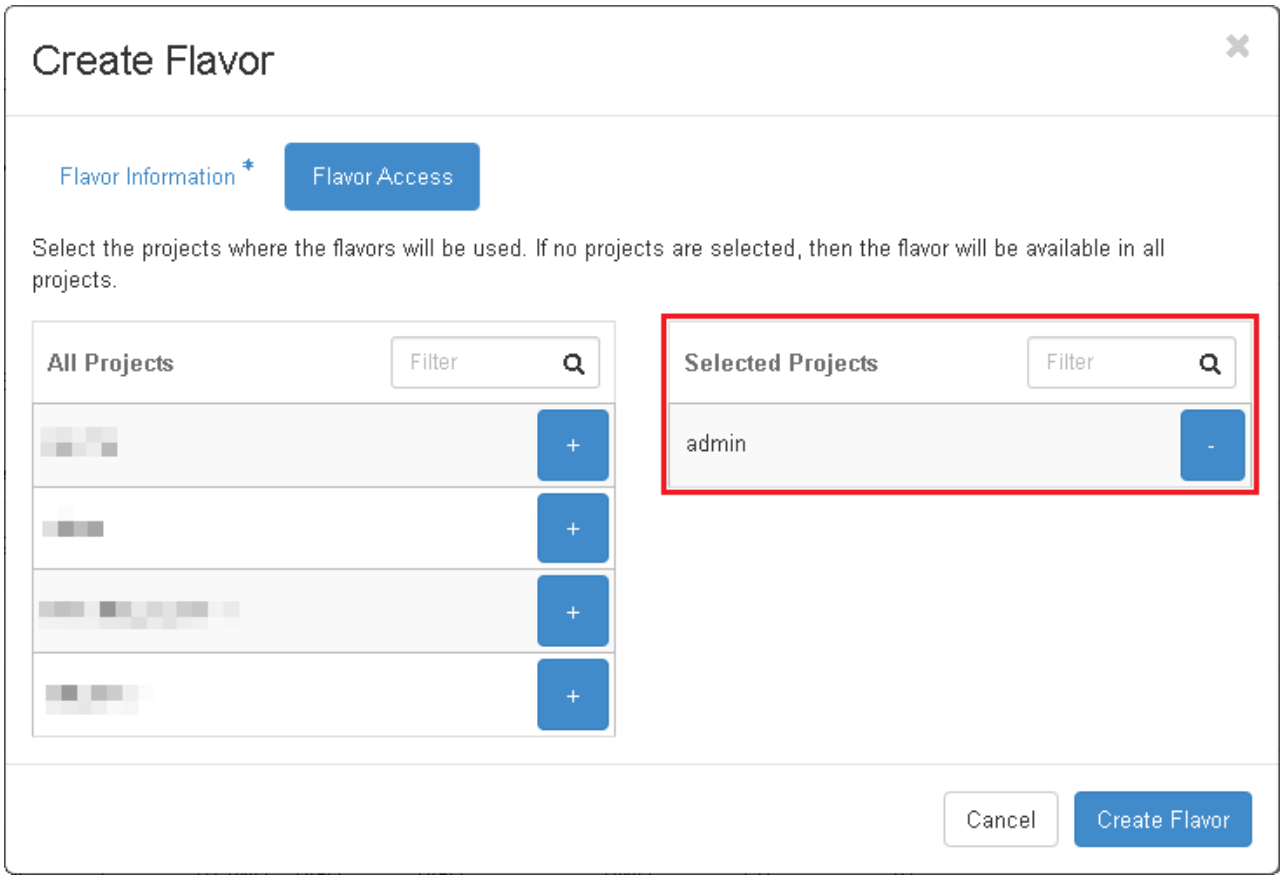
An Internet connection is required for the FortiMail VM to contact FortiGuard to validate its license. If the FortiMail VM is in a closed environment, it must be able to connect to a FortiManager to validate the FortiMail VM license.

Creating the flavor

1. In the OpenStack dashboard, go to *Admin* > *Compute* > *Flavors* and click *Create Flavor*.



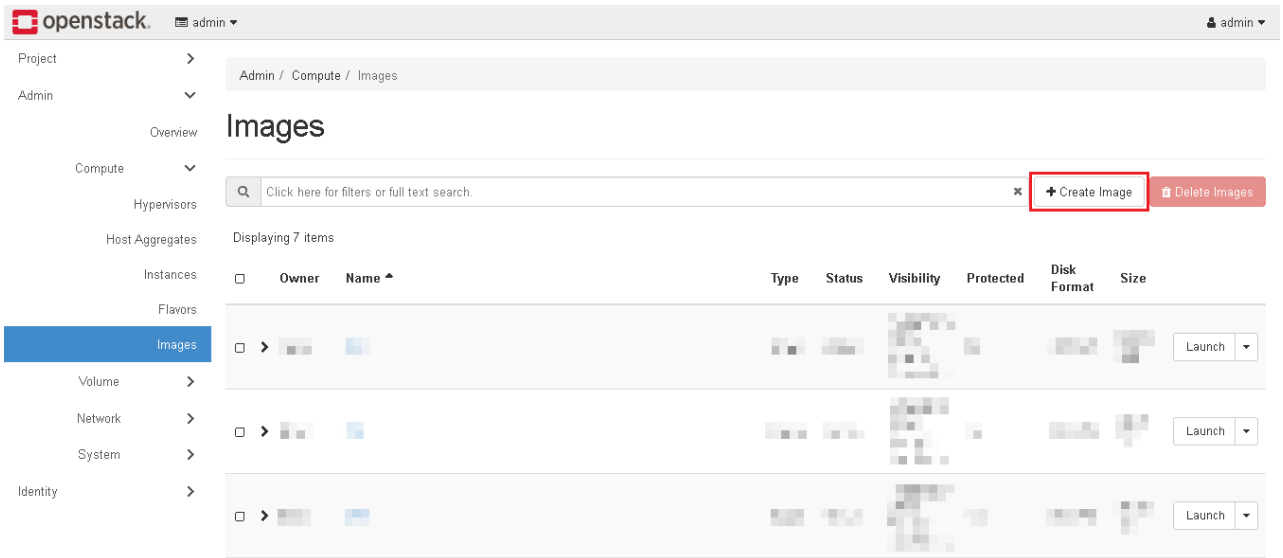
2. Under *Flavor Information*, define the parameters for FortiMail VM instance deployments. Make sure to set the following *minimum* requirements:
   - **VCPUs**: 1
   - **RAM**: 1024MB
   - **Root Disk**: 2GB
   - **Ephemeral Disk**: 55GB
3. Click *Flavor Access*, and add the projects you wish to have access to this flavor. In this case, the current project is selected (admin).



4. Click *Create Flavor*.

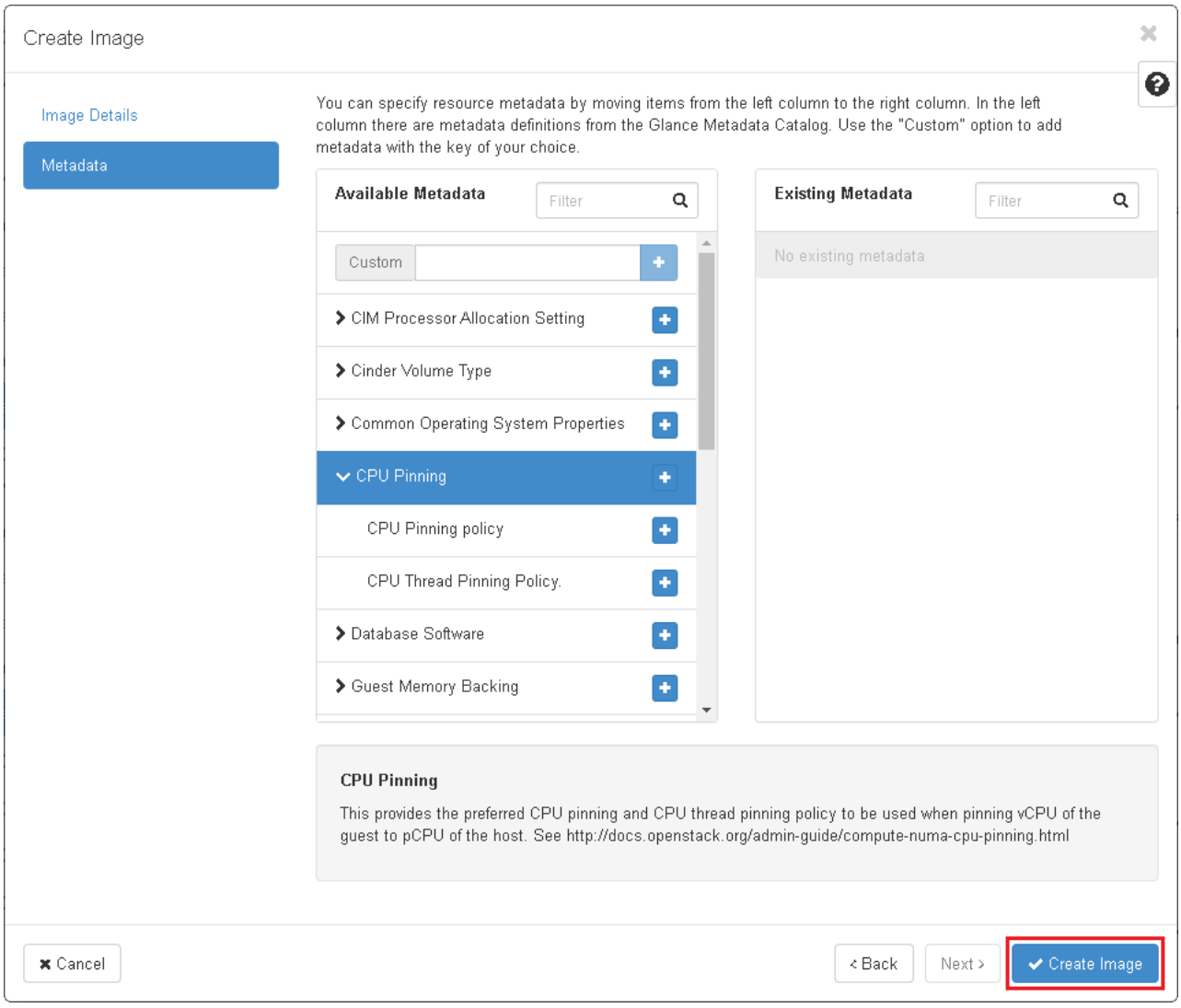
Creating the image

1. Go to *Admin* > *Compute* > *Images* and click *Create Image*.



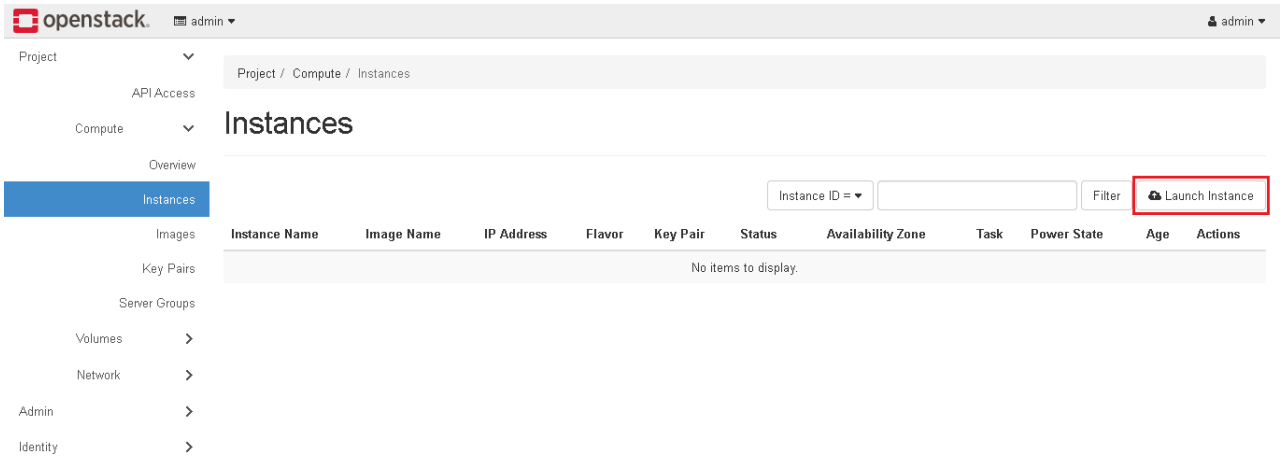
2. From the *Image Details* tab, under *Image Source* > *File*, click *Browse*.

3. Select the image file downloaded from the Fortinet Customer Service & Support portal.
   The image file name is:
   fortimail-kvm.qcow2
4. Set *Format* to *QCOW2 - QEMU Emulator*.
5. Optionally, click the *Metadata* tab and assign any necessary metadata definitions.
   Selecting each option opens a dropdown menu showing what is included for each metadata resource and their descriptions below.
6. When finished, click *Create Image*.

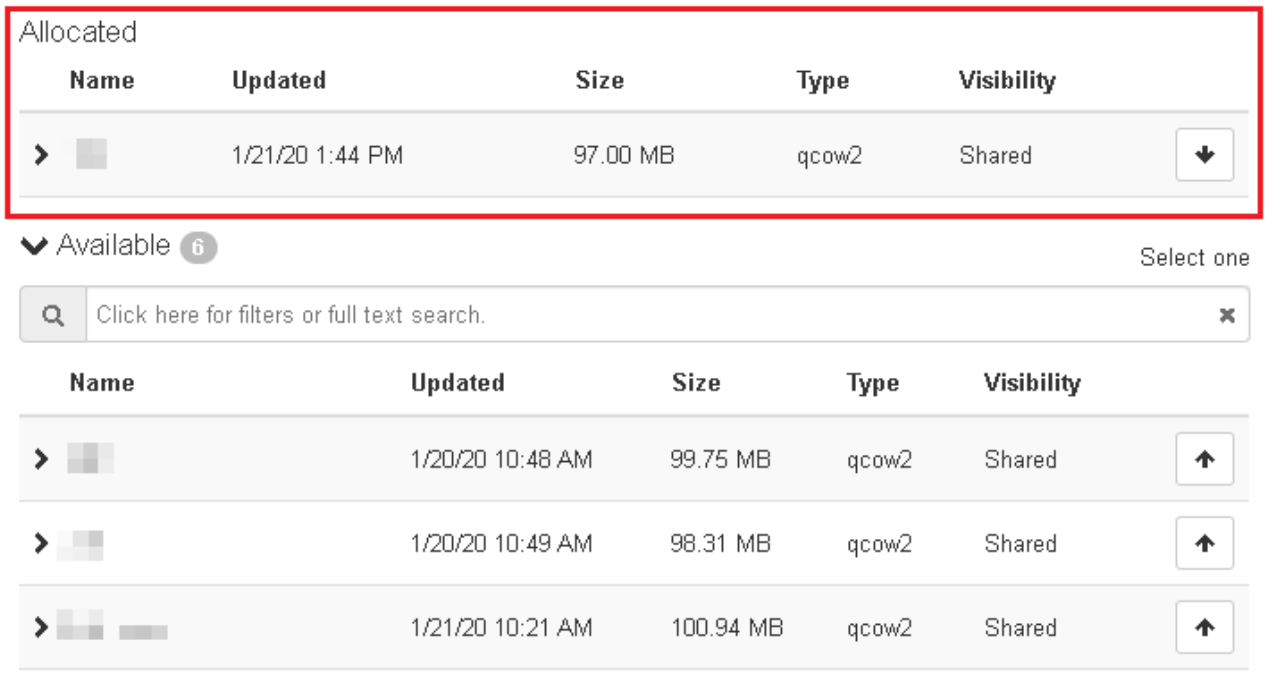


Launching the instance

1. Go to *Project* > *Compute* > *Instances* and click *Launch Instance*.



2. Under the *Details* tab, enter an *Instance Name* and an optional *Description*, define the *Availability Zone* where the instance will be deployed, and the instance *Count*, in cases where you require multiple instances with the same settings.
3. Click *Next*.
4. Under the *Source* tab, set *Select Boot Source* to *Image*. By default, *Create New Volume* is set to *Yes*. Increase the *Volume Size* as required.
5. Upload the image created earlier from under the *Available* list by clicking the  icon.
The image is moved to the *Allocated* list as shown in the following example:



6. Click *Next*.
7. Under the *Flavor* tab, select the *Flavor* created earlier by moving it from the *Available* list to the *Allocated* list.

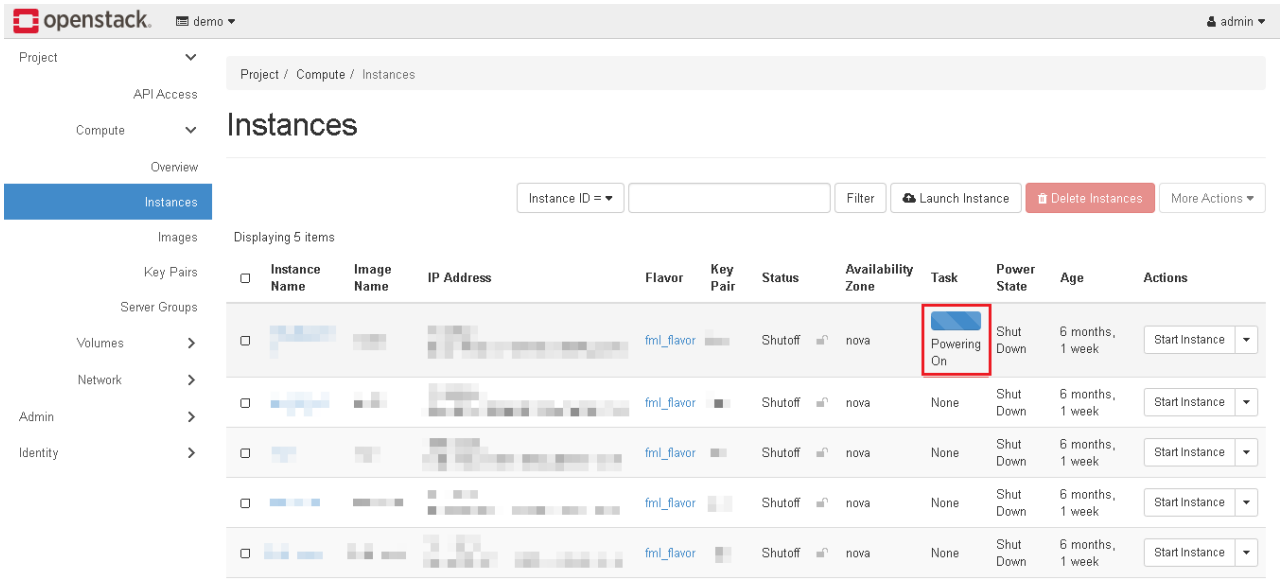
8. Click *Next*.
9. Under the Networks tab, define whether the instance should be located on a public, private, or shared network.
10. Optionally, continue configuring the remaining tabs. When finished, click *Launch Instance*.

The newly created FortiMail VM instance is launched.

Accessing instance console

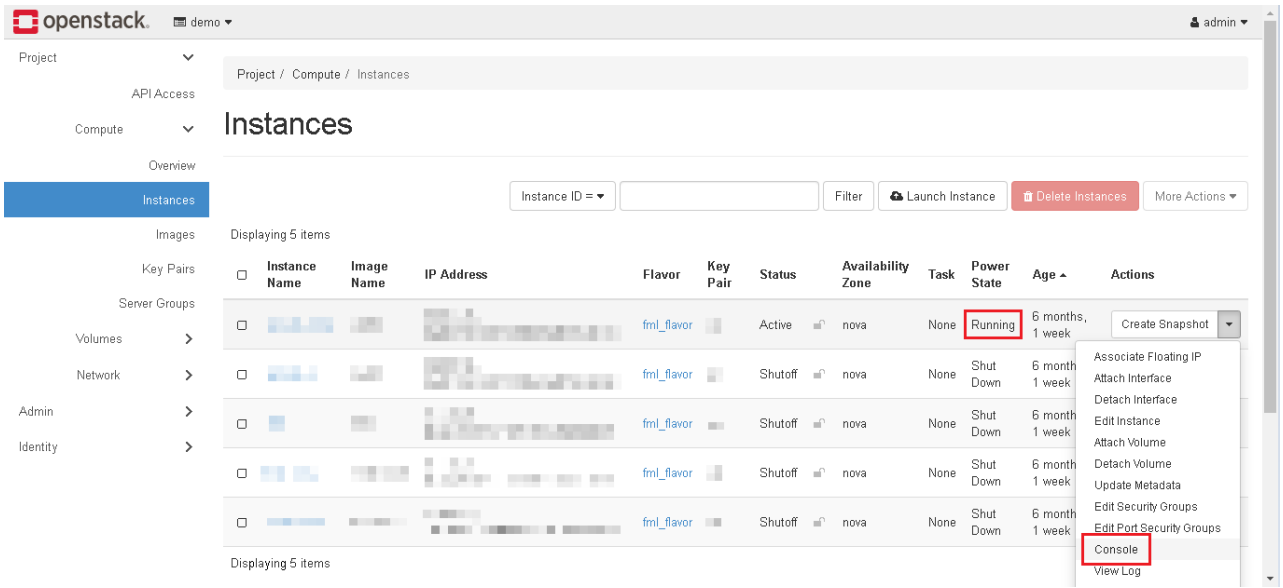
You can access your list of instances from under *Project* > *Compute* > *Instances*.

1. If you haven't already, launch an instance by selecting *Start Instance* from the *Actions* column.
The *Power State* column will show that the instance is powering on.

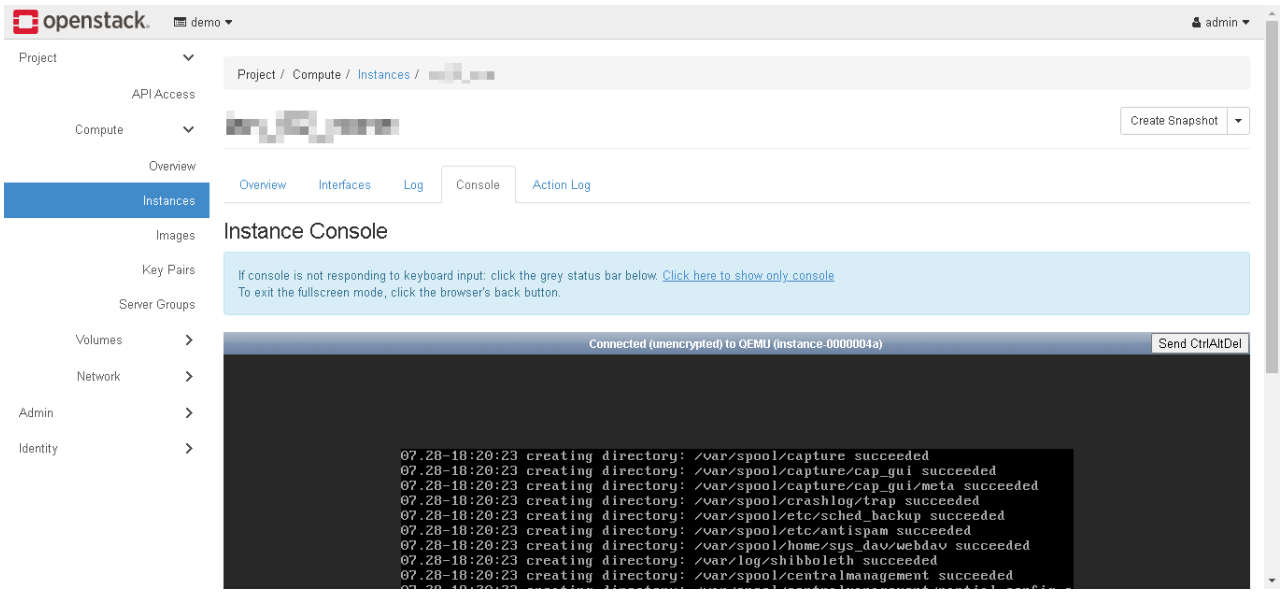


After a few seconds, the instance will show a *Power State* of *Running*.

2. To access the instance's console, click the *Actions* drop-down menu and select *Console*.



You are redirected to the *Instance Console*.



If you just started the instance, you may need to wait a few minutes for the instance initialization to complete.

3. Once it is complete, you can login to the FortiMail VM.

```
07.28-18:20:23 creating directory: /var/spool/etc/sched_backup succeeded
07.28-18:20:23 creating directory: /var/spool/etc/antispam succeeded
07.28-18:20:23 creating directory: /var/spool/home/sys_dav/webdav succeeded
07.28-18:20:23 creating directory: /var/log/shibboleth succeeded
07.28-18:20:23 creating directory: /var/spool/centralmanagement succeeded
07.28-18:20:23 creating directory: /var/spool/centralmanagement/partial_config s
ucceeded
07.28-18:20:23 creating directory: /var/spool/centralmanagement/task_status succ
eeded
07.28-18:20:23 creating directory: /var/spool/centralmanagement/config succeeded
07.28-18:20:23 creating directory: /var/spool/centralmanagement/firmware succeed
ed
07.28-18:20:23 creating directory: /var/spool/delayqueue succeeded
Initialize Database ...
Initialize Configuration ...
07.28-11:20:48 Warning: The system supports 4 ethernet interfaces but only 1 wer
e found.
07.28-11:20:48          If interfaces are changed outside of FortiMail-VM please
 ensure
07.28-11:20:48          the FortiMail configuration is still valid.
Serial number is FEVM000000000000
Loading realtime mail statistics data returns -26


FEVM000000000000 login: _
```

Initial configuration

Before you can connect to the FortiMail VM Web-based Manager you must configure the FortiMail VM basic configuration via the CLI console. Once configured, you can connect to the FortiMail VM Web-based Manager and upload the FortiMail VM license file that you downloaded from the Customer Service & Support portal.

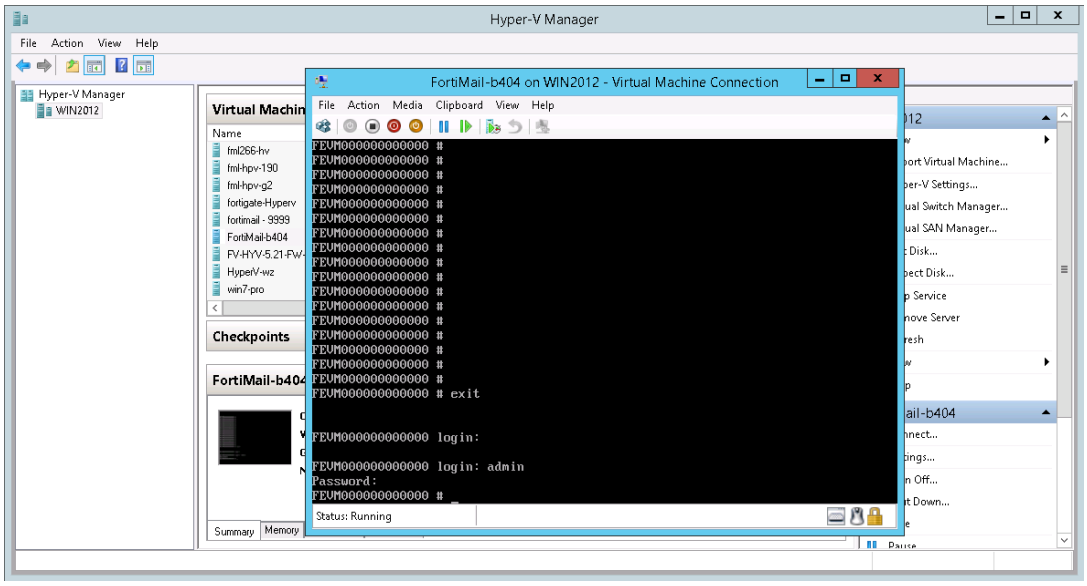
This section contains the following topics:

FortiMail VM console access

To enable Web-based Manager access to the FortiMail VM you must configure the port1 IP address and network mask of the FortiMail VM.

To configure the port1 IP address and netmask:

1. In the list of virtual machines, select the FortiMail VM that you deployed, right-click, and select *Connect* from the menu.
   The *Console* window appears



2. At the FortiMail VM login prompt enter the user name `admin` and password. The default password is no password.
3. To configure the port1 IP address and netmask, enter the following CLI commands:

```
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 Microsoft Hyper-V Server virtual machine settings.

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

Connecting to the FortiMail VM Web-based Manager

Once you have configured the port1 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 password and select *Login*. The default password is no password. The Web-based Manager will appear with an *Evaluation License* dialog box.

By default, the Web-based Manager is accessible via HTTPS.

Uploading the FortiMail VM license file

Every Fortinet VM includes a 15-day trial license. During this time the FortiMail VM operates in evaluation mode. Before using the FortiMail VM you must enter the license file that you downloaded from the Customer Service & Support portal upon registration.

To install the license

1. In the *License Information* widget on the FortiMail VM web-based manager, click the *Update* link to the right of *VM*.
2. Locate and select the license file (.lic) you downloaded earlier from Fortinet.
3. Click *Open*.
   A message box appears stating your license is being authenticated. This may take a few minutes.
   If you uploaded a valid license, a second message box will appear informing you that your license authenticated successfully.
4. Click *OK* on the message box.
   The system will reload and log out.
5. Log in again if prompted using `admin`, as the user name. The VM registration status appears as valid in the *License Information* widget once the license has been validated.

After an invalid license file is loaded to FortiMail VM, the Web-based Manager will be locked until a valid license file is uploaded.

Configuring your FortiMail VM

Once the FortiMail VM license has been validated you can begin to configure your device. For more information on configuring your FortiMail VM, see the *FortiMail Administration Guide*.

VM Installation Guide

FortiMail 7.2.0