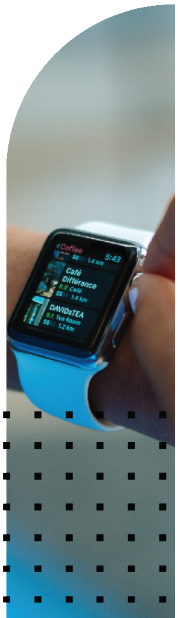
VMware vSphere Deployment Guide

FortiProxy 7.0



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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

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

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

June 06, 2023
FortiProxy 7.0 VMware vSphere Deployment Guide
45-700-818700-20230606

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-06-16	Initial release.
2023-04-25	Updated Getting started on page 5.
2023-06-06	Updated Configure virtual hardware settings on page 16.

Getting started

FortiProxy is a secure web proxy that protects employees against internet-borne attacks by incorporating multiple detection techniques such as web filtering, DNS filtering, data loss prevention, antivirus, intrusion prevention, and advanced threat protection. It helps enterprises enforce internet compliance using granular application control. High-performance physical and virtual appliances deploy on-site to serve small, medium, and large enterprises

FortiProxy provides multiple detection methods such as reputation lookup, signature-based detection, and sandboxing to protect against known malware, emerging threats, and zero-day malware. It also intercepts outgoing client connections to the internet and has some firewall capabilities. However, the primary focus of FortiProxy is to be a secure web gateway solution that provides visibility, compliance, web security, and threat protection for any organization.

This document describes how to deploy a FortiProxy-VM in a VMware vSphere environment. More information about configuring and using FortiProxy is available in the Fortinet Document Library.

In the initial setup, the following ports are used:

- DNS lookup — UDP 53
- FortiGuard licensing — TCP 443

Evaluation license

FortiProxy-VM can be evaluated with a free 15-day trial license that includes most features, except:

- HA
- FortiGuard updates
- Technical support

You do not need to manually upload the trial license; it is built-in. The trial period begins the first time you start FortiProxy-VM. When the trial expires, most functionality is disabled. You must purchase a license to continue using FortiProxy-VM.

License sizes

VM licenses are available in the following sizes:

	Evaluation	VM02	VM04	VM08	VM16	VMUL
Maximum number of CPUs	2	4	8	16	32	Unlimited
Memory (GB)	2	Unlimited				
Number of disks (boot + storage)	1+1	1+2	1+2	1+4	1+8	16 total

The maximum number of IP sessions varies by license and by available vRAM, just as it does for hardware models. For more information, see the FortiProxy Datasheet.

License validation

FortiProxy-VM must periodically revalidate its license with the Fortinet Distribution Network (FDN). If it cannot contact the FDN for 24 hours, access to the FortiProxy-VM web UI and CLI are locked.

By default, FortiProxy-VM attempts to contact FDN over the internet. If the management port cannot access the internet (for example, in closed network environments), it is possible for FortiProxy-VM to validate its license with a FortiManager that has been deployed on the local network to act as a local FDS (FortiGuard Distribution Server).

On the FortiProxy-VM, specify the FortiManager IP address for the “override server” in the FortiGuard configuration:

```
config system central-management
    set type fortimanager
    config server-list
        edit 1
            set server-type update
            set server-address <FortiManager IP address for updates>
        next
        edit 2
            set server-type rating
            set server-address <FortiManager IP address for web filter ratings>
        next
    end
    set include-default-servers disable
end
```

TCP port 8890 is the port where the built-in FDS feature listens for requests. For more information on the FortiManager local FDS feature, see the FortiManager Administration Guide. Although FortiManager can provide FortiGuard security service updates to some Fortinet devices, for FortiProxy, its FDN features can provide license validation only.

Preparing for deployment

This documentation assumes that before deploying the FortiProxy-VM on the VMware vSphere virtual platform, you have addressed the following requirements:

Virtual environment

For best performance, install FortiProxy-VM on a “bare metal” hypervisor. Hypervisors that are installed as applications on top of a general-purpose operating system (Windows, Mac OS X, or Linux) host and have fewer computing resources available due to the host OS’s own overhead.

Hardware-assisted virtualization (VT) must be enabled in the BIOS.

You have installed the VMware vSphere software on a physical server with sufficient resources to support the FortiProxy-VM and all other VMs deployed on the platform.

If you configure the FortiProxy-VM to operate in transparent mode, or include it in an high availability (HA) cluster, configure any virtual switches to support the FortiProxy-VM's operation before you create the FortiProxy-VM.

VM Environment	Tested Versions
VMware	ESXi versions 6.0, 6.5, 6.7, and 7.0

Management software

You can access the VMware vSphere in one of the following ways:

- Directly with the ESXi web GUI
- With the vSphere Web Client if a vCenter is managing the ESXi server

Connectivity

The FortiProxy-VM requires an internet connection to contact FortiGuard to validate its license.

Registering the FortiProxy-VM

When you purchase a FortiProxy-VM, you receive an email that contains a registration number. This registration number is used to download the software, your purchased license, and also to register your purchase with Fortinet Customer Service & Support so that your FortiProxy-VM will be able to validate its license with Fortinet.

Many Fortinet customer services such as firmware updates, technical support, and FortiGuard services require product registration.

For registration instructions, see Registering products in the FortiCloud Account ServicesAsset Management guide.

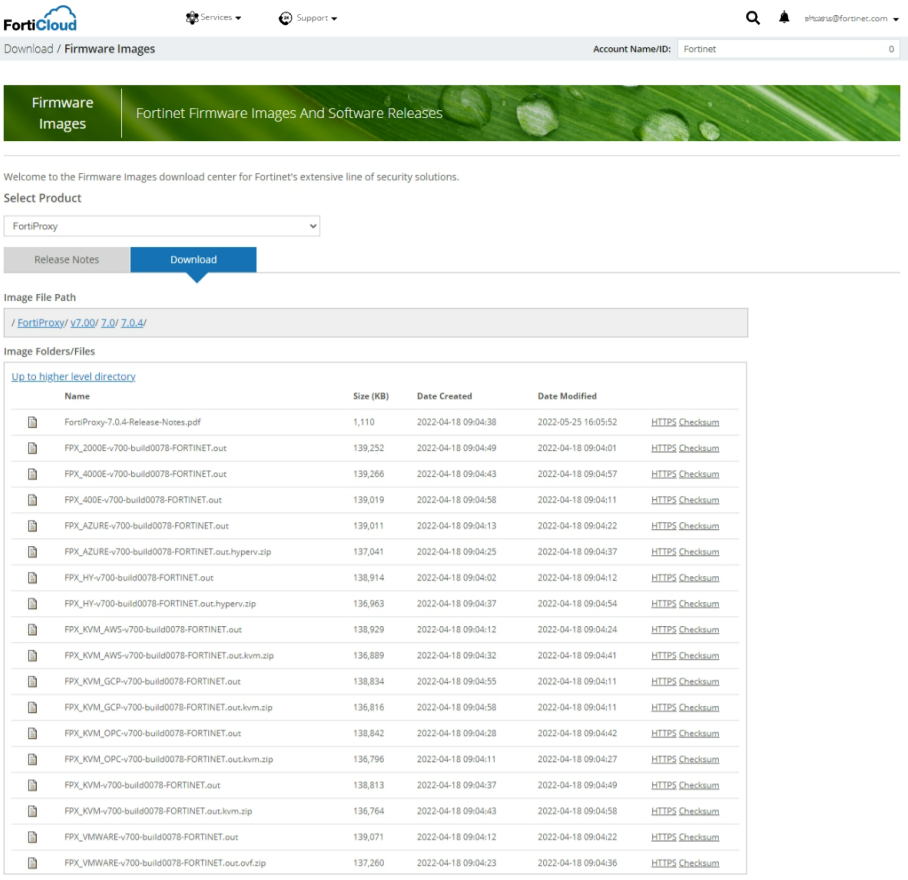
For information about downloaded the license file, see Viewing licenses and keys in the Product details topic of the FortiCloud Account ServicesAsset Management guide.

Downloading the FortiProxy-VM deployment package

FortiProxy-VM deployment packages can be downloaded from the Customer Service & Support.

To download the VM deployment package:

1. Log in to your FortiCloud account.
2. Go to *Support* > *Firmware Download*.
3. In the *Select Product* list, select *FortiProxy*.
4. Select the *Download* tab.
5. Browse to the appropriate directory for the version that you need to download.



6. Download the firmware `.zip` file by clicking the *HTTPS* link to its right.
   The `.out` image files are for upgrades of existing installations only and cannot be used for a new installation.
7. Extract the .zip file contents to a folder.

Deployment package contents

The *FPX_VMWARE-vxxx-buildxxxx-FORTINET.out.ovf.zip* file contains:

Component	Description
fortiproxy.vmdk	FortiProxy-VM system hard disk in VMDK format.
datadrive.vmdk	FortiProxy-VM log disk in VMDK format.
datadriv2.vmdk	FortiProxy-VM log disk 2 in VMDK format.
readme.txt	Explains compatibility information for each template.
Open Virtualization Format (OVF) template files	
FortiProxy-VM64.ovf	OVF template file for VMware ESXi 7.0 and later versions, vmxnet3-based.
FortiProxy-VM64.hw13.ovf	OVF template file for VMware ESXi 6.5 and later versions, vmxnet3-based.
FortiProxy-VM64.hw15.ovf	OVF template file for VMware ESXi 6.7 and later versions, vmxnet3-based.

Component	Description
FortiProxy-VM64.vapp.ovf	OVF template file for VMware ESXi 7.0 and later versions. SR-IOV is available on the adapters list after deployment with this template.
FortiProxy-VM64.nsxt.ovf	OVF template file for VMware ESXi 5.0 and later versions, vmxnet3-based.

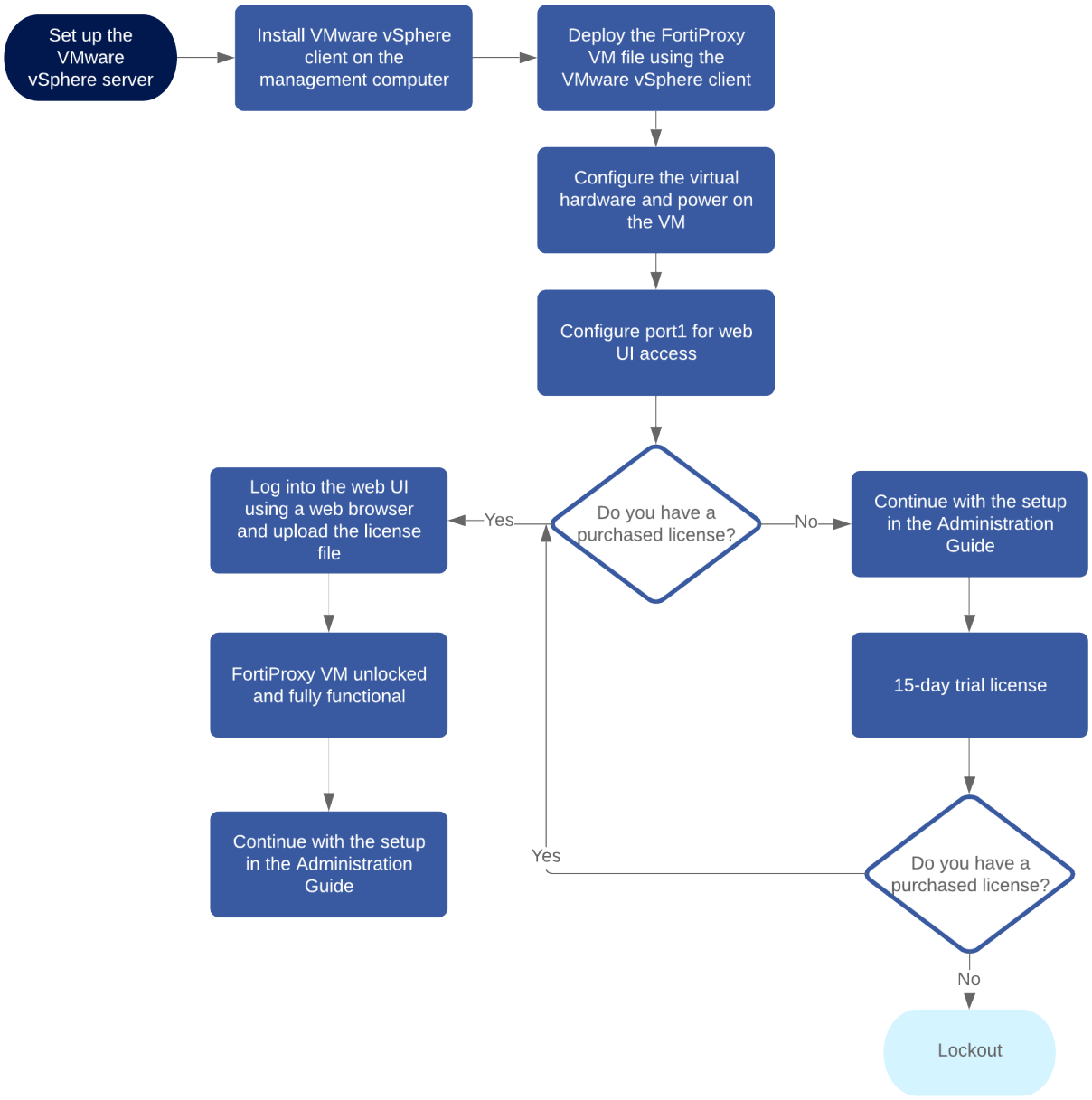
Deploying FortiProxy-VM

After you have downloaded the FPX_VMWARE-vxxx-buildxxxx-FORTINET.out.ovf.zip file and extracted the package contents to a folder on your server, you can deploy the FortiProxy-VM on on VMware vSphere.

This chapter covers the following topics:

Installation overview

The following diagram gives an overview of the process for installing FortiProxy-VM on VMware vSphere.

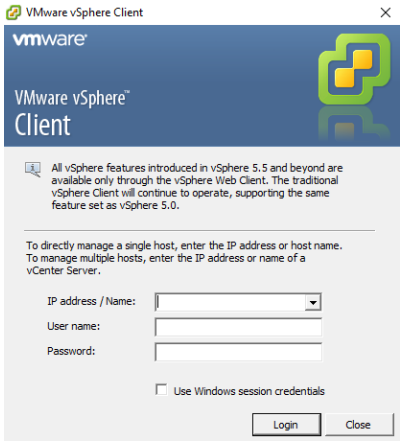


Deploy the OVF file

You must first use VMware vSphere Client to deploy the FortiProxy-VM OVF package.

To deploy the virtual appliance:

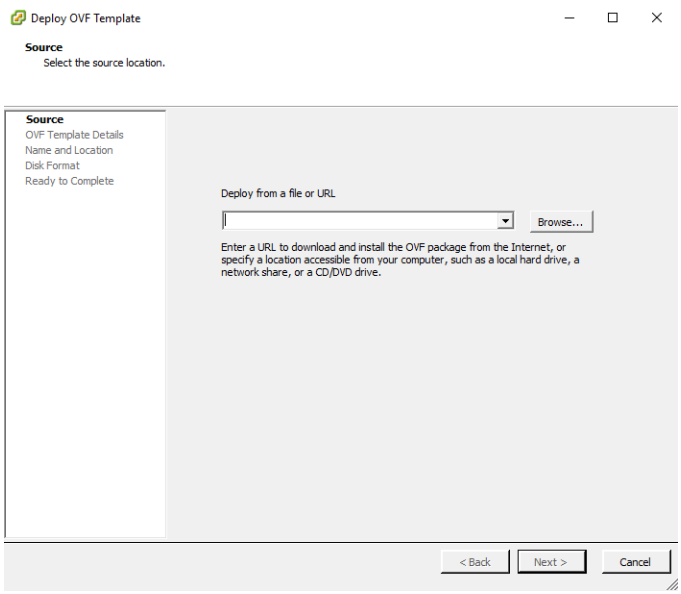
1. Use the VMware vSphere client to connect to VMware vSphere server:
   a. On your management computer, start the VMware vSphere Client.



   b. In *IP address / Name* field type the IP address or FQDN of the VMware vSphere server.
   c. Enter the user name and password then click *Login*.

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

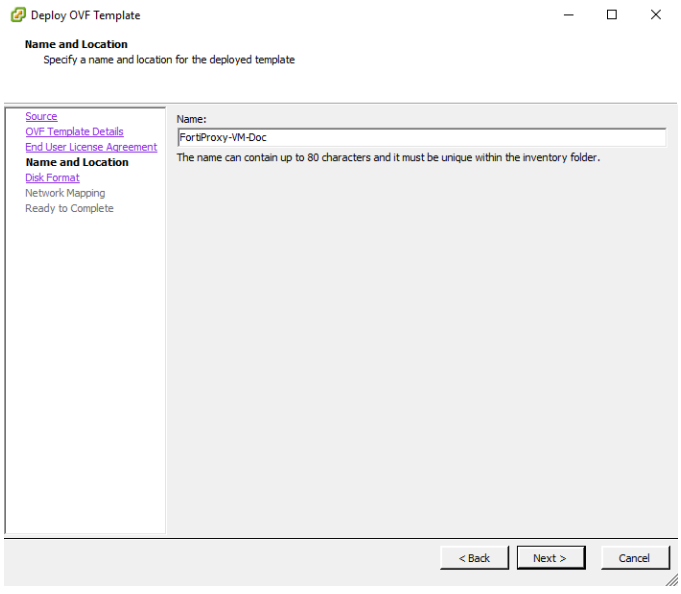
2. Go to *File* > *Deploy OVF Template*.



A deployment wizard window appears.

3. In the *Deploy OVF Template* window, click *Browse* and navigate to the FortiProxy-VM OVF file.
4. Click *Next* twice.
   Click *Accept* to agree to the End User License Agreement, then click *Next*.
5. On the *Name and Location* page, type a unique descriptive name for this instance of FortiProxy-VM, then click *Next*.

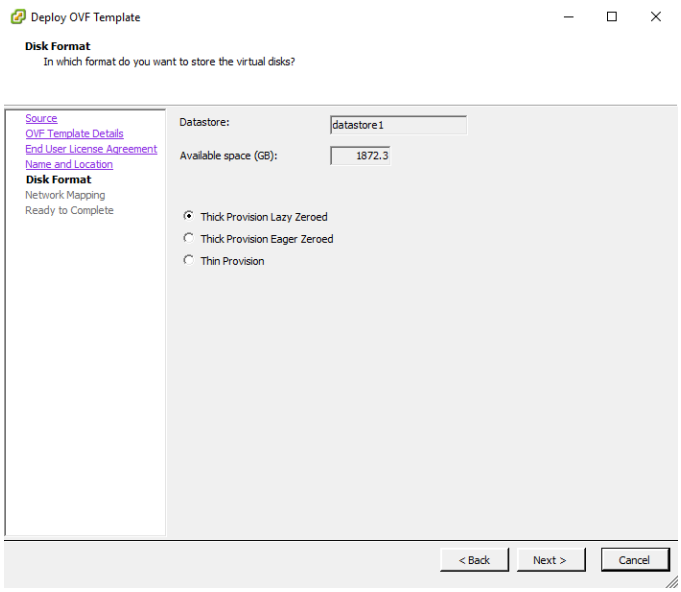
   The name appears in the vSphere Client inventory, such as `FortiProxy-VM-Doc`. If you plan to deploy multiple instances of this file, consider a naming scheme that makes each VM's purpose or IP address easy to remember.
   This name is *not* used as the host name, and it does not appear in the FortiProxy-VM GUI.



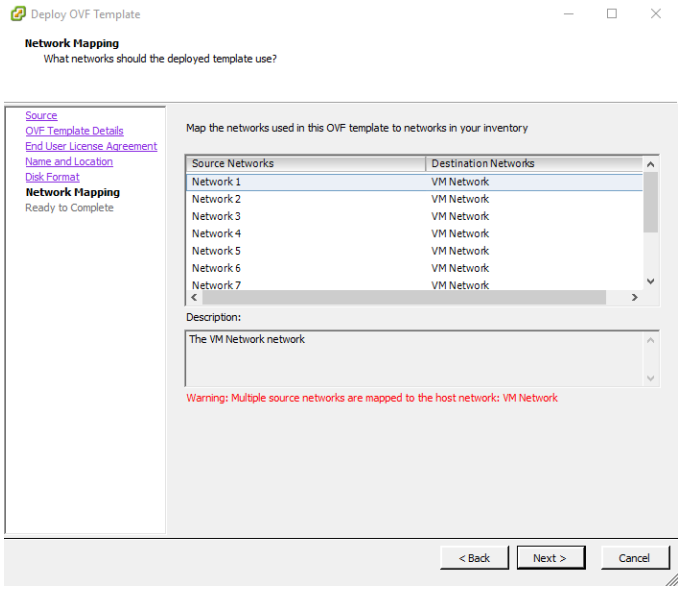
6. On the *Disk Format* page, select one of the following options and then click *Next*:
   - *Thick Provision Lazy Zeroed*: Allocates the disk space statically (no other volumes can take the space), but does not write zeros to the blocks until the first write takes place to that block during runtime (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.

Regardless of your choice here, you should later either allocate or make available at least 40 GB of disk space. 30 GB is only the default minimum value, and is not recommended.



7. On the *Network Mapping* page, if the hypervisor has more than one possible network mapping, select the row for the network mapping that FortiProxy-VM should use, then click *Next*.



8. On the *OVF Template Ready to Complete* page, review the template configuration. Ensure that *Power on after deployment* is not enabled. You need to configure the FortiProxy hardware settings before powering on the VM.
9. Click *Finish* to deploy the OVF template. A *Deployment Completed Successfully* dialog displays once the FortiProxy OVF template wizard has finished.

Do not power on the virtual appliance until you have completed the following in the VM environment:

- Resize the virtual disk (VMDK).
- Set the number of vCPUs.
- Set the vRAM on the virtual appliance.
- Map the virtual network adapter(s).

Configure virtual hardware settings

After deploying the FortiProxy-VM image and before powering on the virtual appliance, log into VMware vSphere and configure the virtual appliance hardware settings to suit the size of your deployment.

The following table summarizes the defaults that are set in the default image and provides rough guidelines to help you understand whether you need to upgrade the hardware before you power on the virtual appliance. For more precise guidance on sizing, contact your sales representative or Fortinet Technical Support.

Component	Default	Guidelines
Hard disk	32 GB	32 GB is insufficient for most deployments. The hard disk size should be increased before you power on the appliance. After you power on the appliance, reformat the FortiProxy log disk with the following command: `execute formatlogdisk`
CPU	1 CPU	You need a minimum of 2 CPU for a VM02 license. Upgrade to 4, 8, or 16 CPU for VM04, VM08, and VM16 licenses, respectively.
RAM	2 GB	For optimal performance, Fortinet recommends a minimum of 4 GB of memory for all FortiProxy VM deployments. See the section on vRAM for guidelines based on expected concurrent connections.
Network interfaces	10 bridging vNICs are mapped to a port group on one virtual switch (vSwitch).	Change the mapping as required for your VM environment and network.

For more information on virtual hardware, see http://kb.vmware.com/selfservice/documentLinkInt.do?micrositeID=&popup=true&languageId=&externalID=1010675.

Resizing the virtual disk (vDisk)

If you configure the virtual appliance storage repository to be internal (that is, local on its own vDisk), resize the vDisk before powering on the VM appliance. If you configured the virtual appliance to use external network file system datastores (such as NFS) then you can skip this step.

The FortiProxy-VM package includes pre-sized VMDK (Virtual Machine Disk Format) files. However, they are only 32 GB, which is not large enough for most deployments. You must resize the vDisk before powering on the virtual machine. Before doing so, make sure that you understand the effects of the vDisk settings. These options affect the possible size of each vDisk:

- 1MB block size = 256GB maximum file size
- 2MB block size = 512GB maximum file size
- 4MB block size = 1024GB maximum file size
- 8MB block size = 2048GB maximum file size

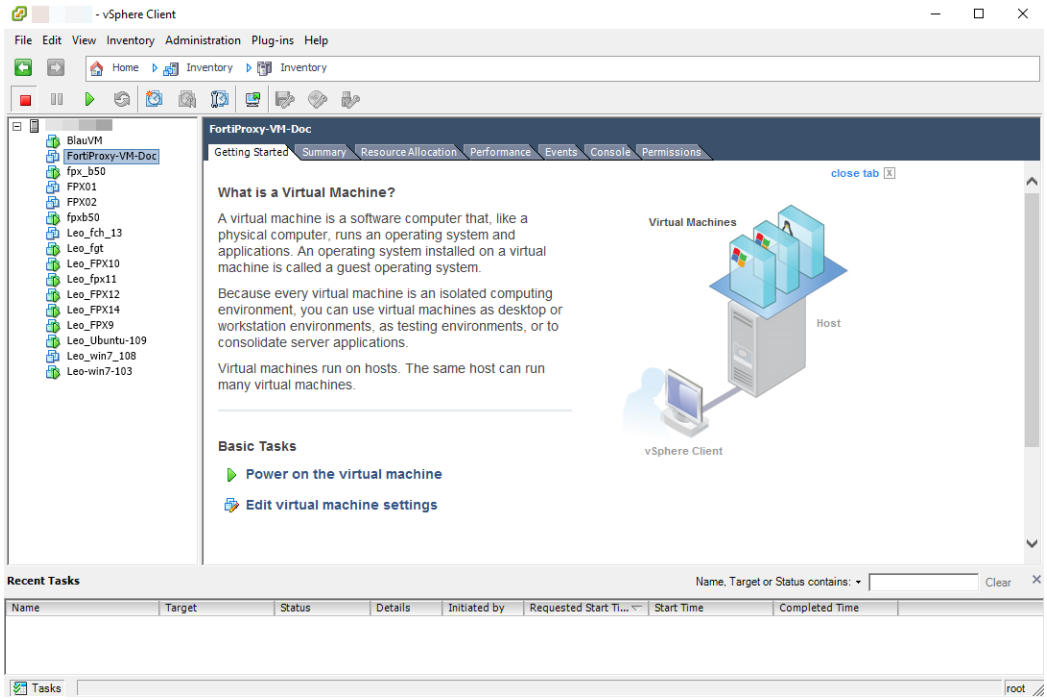
For example, if you have an 800GB datastore which has been formatted with 1MB block size, you cannot size a single vDisk greater than 256 GB.

Consider also that, depending on the size of your network, you might require more or less storage for logs, reports, and other data.

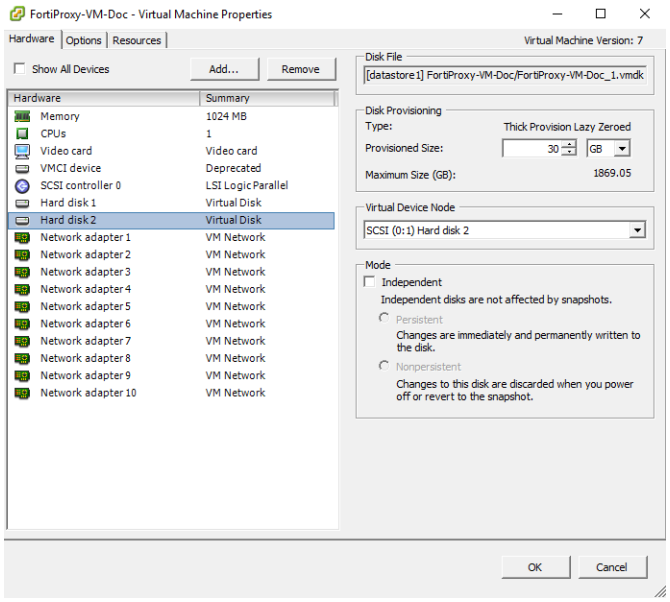
For more information on vDisk sizing, see https://communities.vmware.com/docs/DOC-11920.

To resize the vDisk:

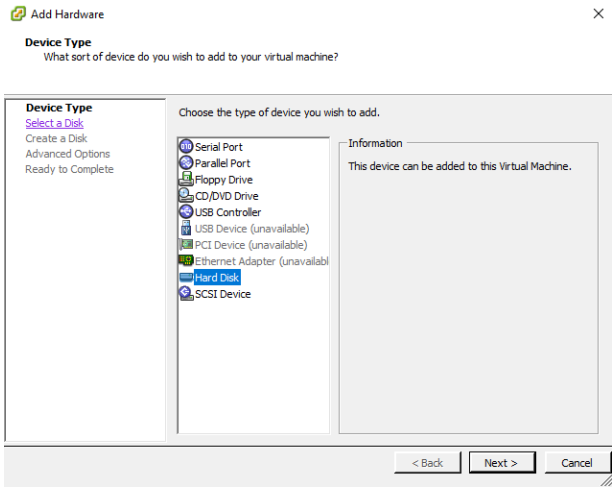
1. Use the VMware vSphere Client to connect to VMware vSphere server.



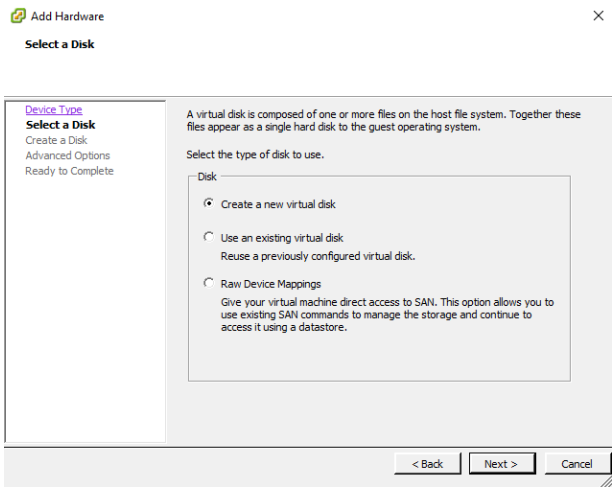
2. In the left pane, right-click the name of the virtual appliance, such as *FortiProxy-VM-Doc*, and select *Edit Settings*.



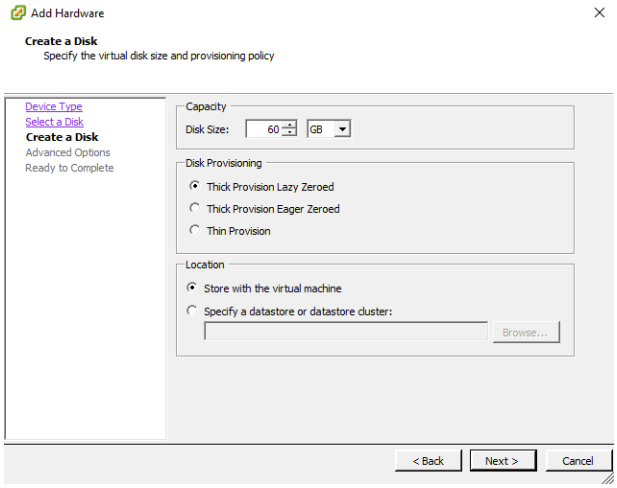
3. In the list of virtual hardware on the left side of the dialog box, select *Hard disk 2*, click *Remove*, and then click *OK*.
4. In the left pane, right-click the name of the virtual appliance and select *Edit Settings*.
5. Click *Add*.



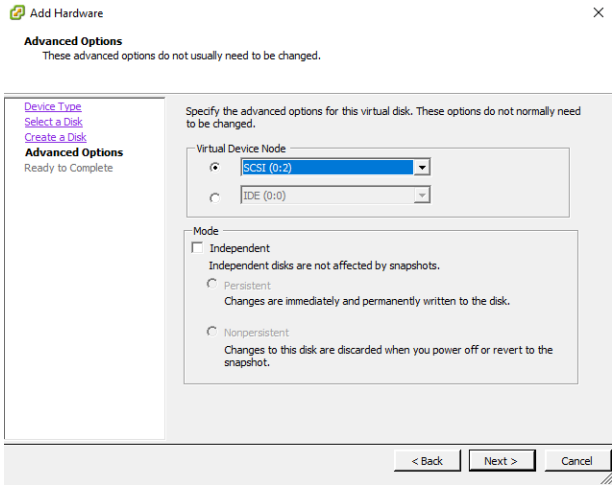
6. From the device types list, select *Hard Disk*, then click *Next*.
7. Select *Create a new virtual disk* then click *Next*.



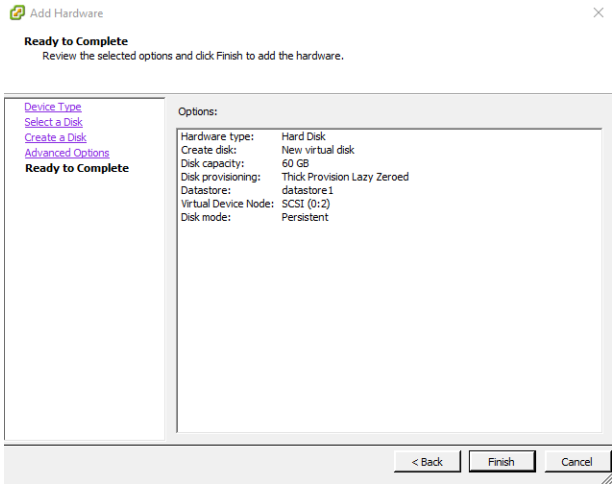
8. Set *Disk Size* to the new size of the vDisk, in GB, then click *Next*.



9. In *Virtual Device Node* box, select *SCSI (0:2)*, then click *Next*.



10. Review the configuration then click *Finish*.



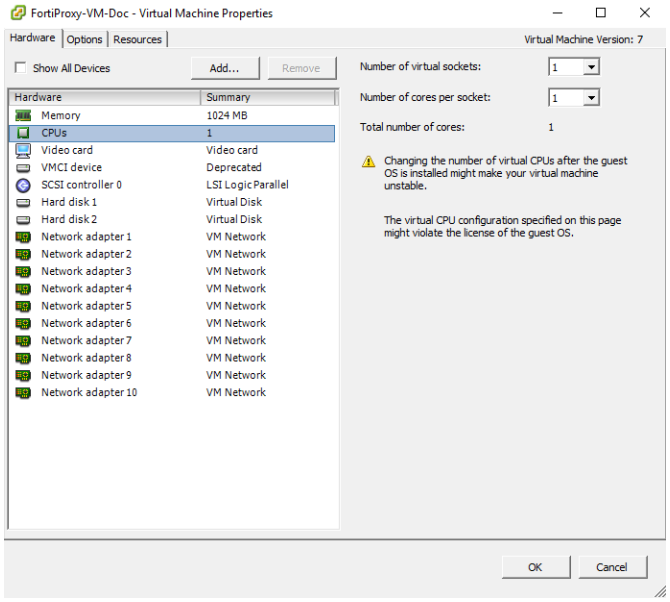
11. Click *OK* to close the *Virtual Machine Properties* dialog box.

Configuring the number of virtual CPUs (vCPUs)

By default, the VM is configured to use one vCPU. Depending on the FortiProxy-VM license that you purchased, you can allocate 2, 4, 8, or 16 vCPUs. For more information on vCPUs, see the VMware vSphere documentation: https://www.vmware.com/support/vsphere-hypervisor.html.

To change the number of vCPUs:

1. Use the VMware vSphere Client to connect to VMware vSphere server.
2. In the left pane, right-click the name of the virtual appliance, such as *FortiProxy-VM-Doc*, and select *Edit Settings*.
3. In the list of virtual hardware on the left side of the dialog box, select *CPUs*.



4. Set *Number of Virtual Sockets* to the maximum number of vCPUs to allocate, which can be 2, 4, 8, or 16, depending on the FortiProxy-VM license that you purchased.
5. Click *OK*.

Configuring the virtual RAM (vRAM) limit

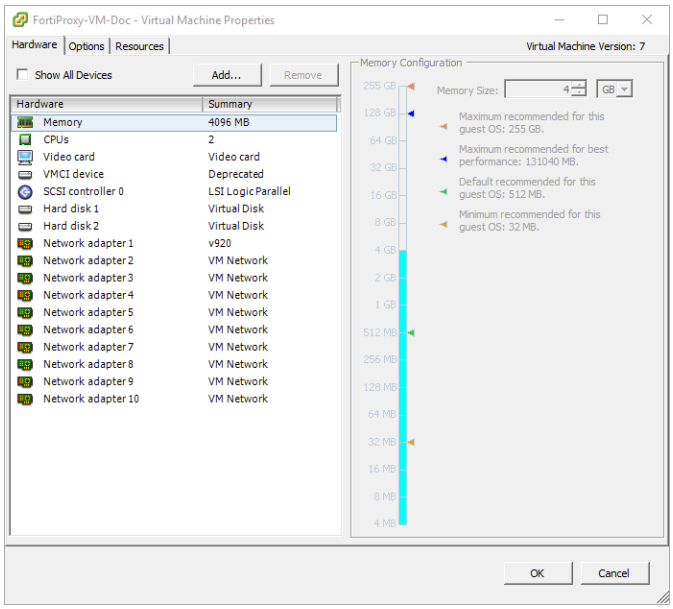
The FortiProxy-VM image is pre-configured to use 2 GB of vRAM. For optimal performance, Fortinet recommends a minimum of 4 GB of memory for all FortiProxy VM deployments.

Appropriate values depend on the number (*n*) of layer-7 transactions that will be handled simultaneously by FortiProxy-VM. Sizing should also be adjusted if the FortiProxy-VM will be handling layer-4 connections, or a mixture of layer-4 and layer-7 connections.

Number of simultaneous layer-7 transactions	vRAM
1 < *n* < 140,000	4 GB
140,001 < *n* < 300,000	8 GB
300,001 < *n* < 600,000	16 GB

To change the amount of vRAM:

1. Use the VMware vSphere Client to connect to VMware vSphere server.
2. In the left pane, right-click the name of the virtual appliance and select *Edit Settings*.
3. In the list of virtual hardware on the left side of the dialog, select *Memory*.



4. Set *Memory Size* to the maximum vRAM to allocate, in GB. For optimal performance, Fortinet recommends a minimum of 4 GB of memory for all FortiProxy VM deployments.
5. Click *OK*.

Mapping the virtual NICs (vNICs) to physical NICs

When you deploy the FortiProxy-VM package, 10 bridging vNICs are created and automatically mapped to a port group on one virtual switch (vSwitch) in the hypervisor. Eac vNIC can be used by one of the 10 network interfaces in FortiProxy-VM. Conversely, some or all of the network interfaces can be configured to use the same vNIC. vSwitches are themselves mapped to physical ports on the server.

You can change the mapping, or map other vNICs, if your VM environment requires it.

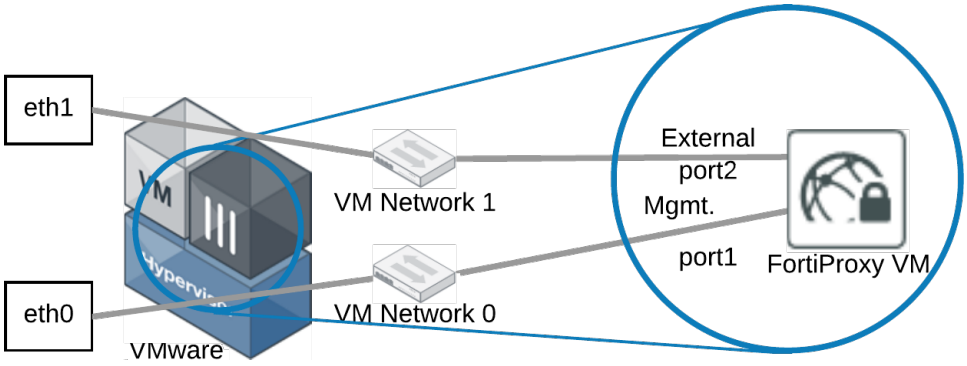
The appropriate mappings of the FortiProxy-VM network adapter ports to the host computer physical ports depends on your existing virtual environment.

Often, the default bridging vNICs work, and do not need to be changed.

If you are unsure of your network mappings, try bridging first before trying non-default vNIC modes, such as NAT or host-only networks. The default bridging vNIC mappings are appropriate where each of the host's guest virtual machines have their own IP addresses on your network.

The most common exceptions to this rule are for VLANs.

The following shows how vNICs could be mapped to the physical network ports on a server:

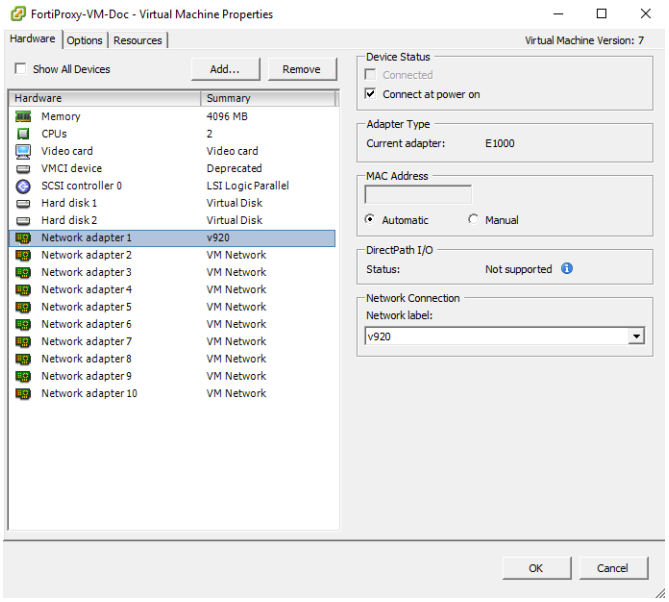


VMware vSphere			FortiProxy-VM
Physical Network Adapter	**Network Mapping (vSwitch Port Group)**	**Virtual Network Adapter for FortiProxy-VM**	**Network Interface Name in Web UI/CLI**
eth0	VM Network 0	Management	port1
eth1	VM Network 1	External	port2
	VM Network 2	Internal	port3
			port4
			port5
			port6
			port7
			port8
			port9
			port10

To map network adapters:

1. Use the VMware vSphere Client to connect to VMware vSphere server.
2. In the left pane, right-click the name of the virtual appliance and select *Edit Settings*.

3. In the list of virtual hardware on the left side of the dialog box, select the name of a virtual network adapter to see its current settings.



4. Set *Network Connection* to the virtual network mapping for the virtual network adapter.

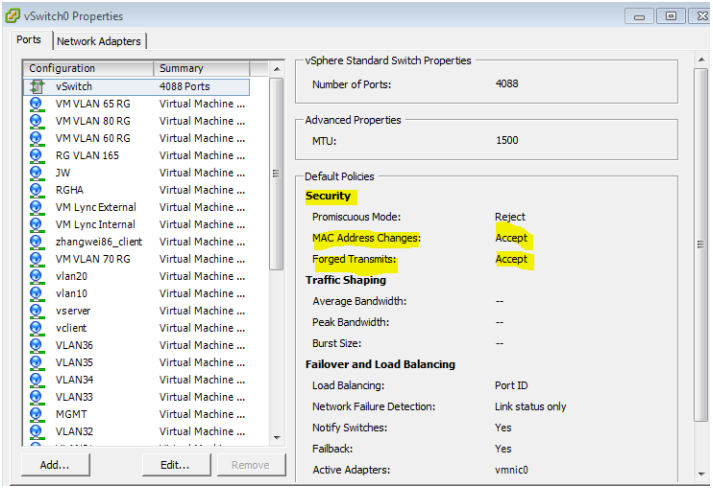
   The correct mapping varies depending on the virtual environment network configuration. In this example, the *Network adapter 1* is mapped to *v920*.

5. Click *OK*.

HA configuration

When configuring HA on FortiProxy appliances using VMware VMs, ensure that the vSwitch can accept MAC address changes and forced transmits on the HA heartbeat VLAN. For more information, see the FortiProxy Administration Guide.

The following image shows what the *vSwitch Properties* page looks like with these settings enabled:



Power on the virtual appliance

After the virtual appliance software has been deployed and its virtual hardware configured, you can power on the virtual appliance.

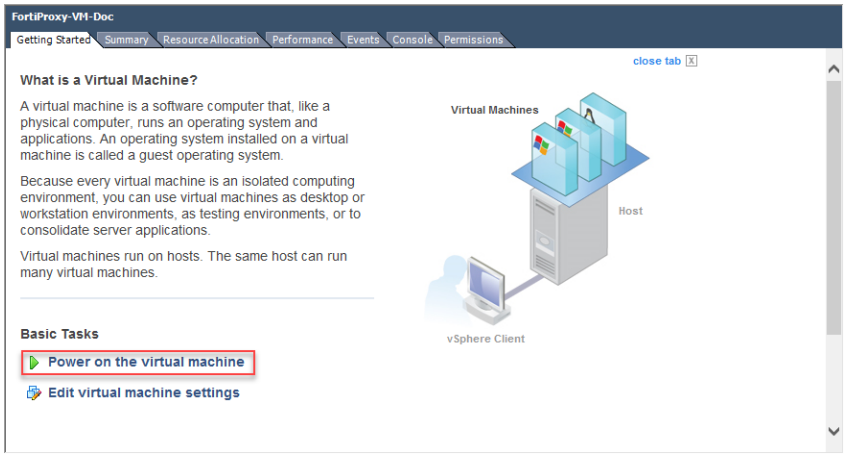
Before you begin:

- You must have resized the disk (VMDK).
- You must have resized the CPUs and RAM, if necessary.
- You must have mapped the virtual network adapters if the defaults are not appropriate.

These settings must be configured in virtual machine environment. You do not configure them in the FortiProxy OS.

To power on the FortiProxy-VM:

1. Use the VMware vSphere Client to connect to VMware vSphere server.
2. In the left pane, select the name of the virtual appliance.
3. Click the *Getting Started* tab.



4. Click *Power on the virtual machine*.

Initial settings

The first time that you start the FortiProxy-VM, you will only have access through the console window of your VMware vSphere environment. After you configure one FortiProxy network interface with an IP address and administrative access, you can access the FortiProxy-VM GUI.

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

More information about configuring and operating FortiProxy-VM after a successful deployment is available in the Fortinet Document Library.

To configure GUI access on the port1 interface:

1. In your hypervisor manager, start the FortiProxy-VM and access the console window. You might need to press *Enter* to see the login prompt.
2. At the login prompt, enter the username `admin` then press `Enter`.
3. Enter an administrator password, and then confirm the password.

If you upgrade the vDisk size, the vDisk size and FortiProxy-VM log partition size likely do not match, and you will see `failed to determine size` errors when you attempt to log into the console.

Press `Enter` repeatedly until you see the log in prompt, log in to the console, then enter:
`execute formatlogdisk`

4. Configure the port1 IP address and netmask:

```
config system interface
    edit port1
        set mode static
        set ip <IP address> <netmask>
        append allowaccess https
    next
end
```

5. Configure the default gateway:

```
config router static
    edit 1
        set device port1
        set gateway <ip_address>
    next
end
```

6. Optionally, configure the DNS servers:

```
config system dns
    set primary <Primary DNS server>
    set secondary <Secondary DNS server>
end
```

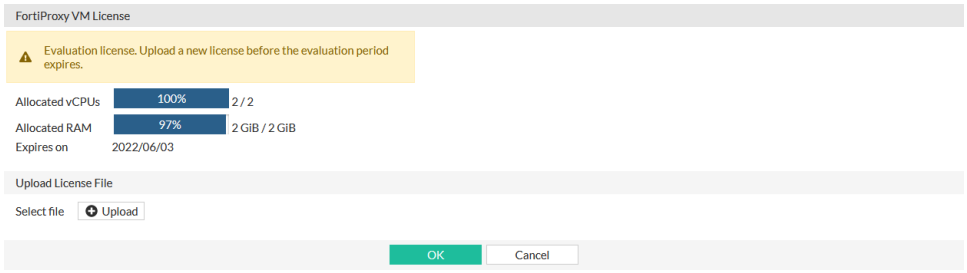
The default DNS servers are 208.91.112.53 and 208.91.112.52.

To connect to the FortiProxy-VM GUI:

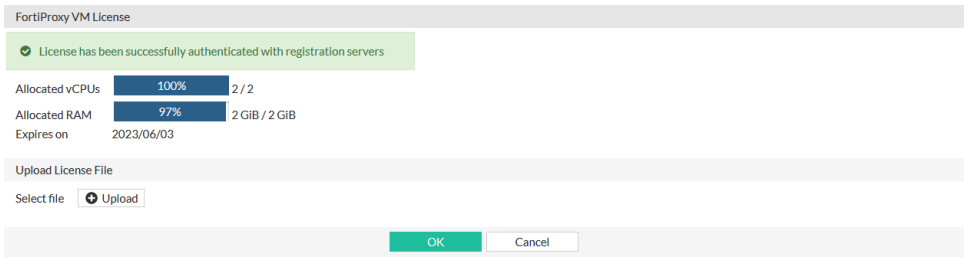
1. Launch a web browser, and enter the IP address you configured for the port1 management interface. For example: `https://192.168.0.1`.
2. At the login page, enter the username `admin` and the password that you configured.

To upload the license file:

1. Go to *System* > *FortiGuard* and click *FortiProxy-VM License*.



2. Click *Upload* and find the license file (.lic) on your computer.
3. Click *OK* to upload the license.
4. Log in to the FortiProxy-VM.
5. Confirm that the license has been successfully uploaded and validated by FortiGuard Distribution Network (FDN):
   a. Go to *Dashboard* > *Status*. The VM registration status appears as valid in the *Virtual Machine* and *Licenses* widgets
   b. Go to *System* > *FortiGuard* and click *FortiProxy-VM License*. A message reports that the license was successfully authenticated.



   c. If logging is enabled, the log message "`License status changed to VALID`" is recorded in the event log.
   d. If the update failed:
      i. Check the following settings on the FortiProxy-VM:
         - Time and time zone
         - DNS settings
         - Network interface statuses and IP addresses
         - Static routes
      ii. On the management computer, verify that FortiGuard domain names are resolving:

```
C:\>nslookup update.fortiguard.net
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Name:    fds1.fortinet.com
```

```
Addresses:  2620:101:9005:1100::205
          192.168.100.205
          192.168.100.220
Aliases:  update.fortiguard.net
```

iii. On the FortiProxy, verify that communication with the internet and FortiGuard is possible:

```
# execute ping update.fortiguard.net
PING fds1.fortinet.com (173.243.138.67): 56 data bytes
64 bytes from 173.243.138.67: icmp_seq=0 ttl=58 time=8.1 ms
64 bytes from 173.243.138.67: icmp_seq=1 ttl=58 time=3.2 ms
64 bytes from 173.243.138.67: icmp_seq=2 ttl=58 time=3.0 ms
64 bytes from 173.243.138.67: icmp_seq=3 ttl=58 time=3.8 ms
64 bytes from 173.243.138.67: icmp_seq=4 ttl=58 time=2.6 ms

--- fds1.fortinet.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.6/4.1/8.1 ms
```

```
# execute traceroute update.fortiguard.net
traceroute to update.fortiguard.net (173.243.138.67), 32 hops max, 3 probe
packets per hop, 84 byte packets
 1  192.168.0.7  10.584 ms  2.927 ms  5.073 ms
 2  10.29.206.1  5.982 ms  8.006 ms  4.199 ms
 3  154.11.11.113  3.584 ms  7.947 ms  8.679 ms
 4  154.11.2.86  2.428 ms  2.337 ms  2.645 ms
 5  * 66.163.69.46 <rd3bb-tge0-11-0-0.vc.shawcable.net>  1.586 ms  1.915 ms
 6  * 64.141.25.113 <h64-141-25-113.bigpipeinc.com>  3.491 ms  2.571 ms
 7  64.141.25.114 <h64-141-25-114.bigpipeinc.com>  1.563 ms  2.385 ms  1.966 ms
 8  96.45.47.39  2.475 ms  2.106 ms  2.105 ms
 9  173.243.138.252  2.452 ms  2.305 ms  1.877 ms
10  173.243.138.67 <update.fortiguard.net>  2.220 ms  1.620 ms  1.990 ms
```

iv. Wait for the next automatic license query (about 30 minutes), or reboot the FortiProxy-VM: `execute reboot`.

If FortiProxy is unable to validate the license after four hours a warning message it displayed in the local console.

www.fortinet.com