



FortiWeb-VM on OpenStack

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



TABLE OF CONTENTS

Overview of FortiWeb-VM	4
Benefits	4
Architecture	5
Licensing	7
Flex-VM	8
Evaluation limitations	8
FortiWeb Manager virtual machine	8
About this document	10
Scope	10
Conventions	10
IP addresses	10
Cautions, notes, & tips	11
Typographical conventions	11
Command syntax conventions	12
System requirements	15
Downloading the FortiWeb-VM license & registering with Technical Support	16
Downloading the FortiWeb-VM software	17
Preparing to deploy on OpenStack	17
Downloading the FortiWeb-VM license and software	19
Creating an initial FortiWeb configuration file	19
Deploying FortiWeb-VM on OpenStack	19
Configuring access to FortiWeb's web UI & CLI	33
Uploading the license	35
License Validation	35
Uploading the license	36
Updating the license for more vCPUs	41
What's next?	43

Overview of FortiWeb-VM

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

FortiWeb-VM is a virtual appliance version of FortiWeb. FortiWeb-VM models are suitable for medium and large enterprises, as well as service providers.

Benefits

FortiWeb is designed specifically to protect web servers.

FortiWeb web application firewalls (WAF) provide specialized application layer threat detection and protection for many HTTP or HTTPS services, including:

- Apache Tomcat
- nginx
- Microsoft IIS
- JBoss
- IBM Lotus Domino
- Microsoft SharePoint
- Microsoft Outlook Web App (OWA)
- RPC and ActiveSync for Microsoft Exchange Server
- Joomla
- WordPress

FortiWeb's integrated web vulnerability scanner can drastically reduce challenges associated with protecting regulated and confidential data by detecting your exposure to the latest threats, especially the [OWASP Top 10](#).

In addition, FortiWeb's XML firewall and denial-of-service (DoS) attack-prevention protect your Internet-facing web-based applications from attack and data theft. Using advanced techniques to provide bidirectional protection against sophisticated threats like SQL injection and cross-site scripting (XSS), FortiWeb helps you prevent identity theft, financial fraud, and corporate espionage. FortiWeb delivers the technology you need to monitor and enforce government regulations, industry best practices, and internal security policies, including firewalling and patching requirements from [PCI DSS](#).

FortiWeb's application-aware firewalling and load balancing engine can:

- Secure HTTP applications that are often gateways into valuable databases
- Prevent and reverse defacement
- Improve application stability
- Monitor servers for downtime & connection load
- Reduces response times
- Accelerate SSL/TLS *
- Accelerate compression/decompression
- Rewrite content on the fly

* On VM models, acceleration is due to offloading the cryptography burden from the back-end server. The VM models support the modern acceleration technology such as Advanced Encryption Standard New Instructions (AES-NI). On hardware models with ASIC chips, cryptography is also hardware-accelerated.

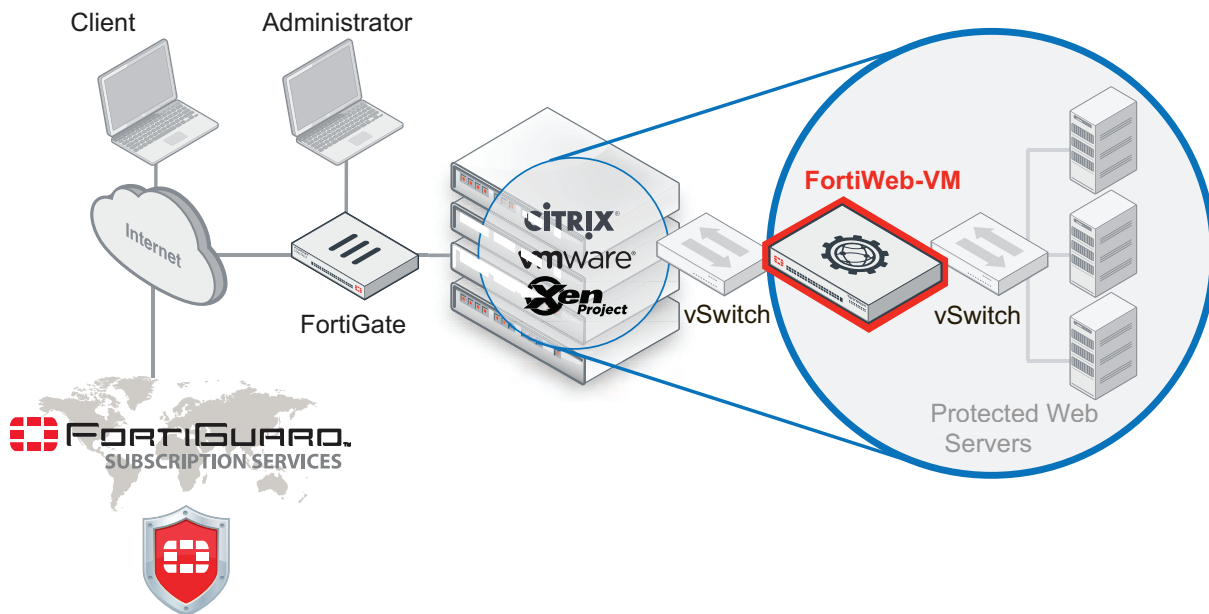
FortiWeb significantly reduces deployment costs by consolidating WAF, hardware acceleration, load balancing, and vulnerability scanning into a single device with no per-user pricing. Those features drastically reduce the time required to protect your regulated, Internet-facing data and eases the challenges associated with policy enforcement and regulatory compliance.

Architecture

FortiWeb-VM is deployed in the following environments:

- VMware ESXi (see illustration)
- Microsoft Hyper-V
- OpenStack cloud computing platform
- KVM
- Citrix XenServer
- Docker
- Open Xen

FortiWeb-VM network topology



FortiWeb can be deployed in a one-arm topology, but is more commonly positioned inline to intercept all incoming clients' connections and redistribute them to your servers. FortiWeb has TCP- and HTTP-specific firewalling capability. Because it is not designed to provide security to non-HTTP applications, it should be deployed behind a firewall such as FortiGate that focuses on security for other protocols that can be forwarded to your back-end servers, such as FTP and SSH.

Once the virtual appliance is deployed, you can configure FortiWeb-VM via its web UI and CLI, from a web browser and terminal emulator on your management computer.

FortiWeb-VM requires Internet connectivity.

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

Licensing

FortiWeb-VM has two license types. The VM license series is for permanent use of FortiWeb-VM, and the VM S license series is used for annual subscription. VM S license is supported only on 6.3.0 and later releases.

The licenses determine the size of the virtual appliance. The registration number you use to obtain the license is also required to download software (for hypervisor deployments) and register for FortiGuard services and technical support.

The following table lists the FortiWeb-VM licenses and the supported vCPU number. To ensure high performance, it's recommended to use a license with at least 2 vCPUs.

FortiWeb-VM resource limitations

	License/model				
	VM/VM S 01	VM/VM S 02	VM/VM S 04	VM/VM S 08	VM/VM S 16
Virtual CPUs (vCPUs)	1	2	4	8	16

It's allowed to import license to a virtual machine with greater vCPU number than the license specifies, for example, you can use FWB-VM04 on a virtual machine with 6 vCPUs, but the extra 2 vCPUs will not be used by FortiWeb-VM.

Maximum IP sessions and policies varies by license, but also by available vRAM, just as it does for hardware models. For details, see maximum configuration values in the [FortiWeb Administration Guide](#).

When you place an order for FortiWeb-VM, Fortinet emails a registration number to the recipient address you supplied on the order form. To register your appliance with Technical Support and to obtain a license file, enter that registration number on the Fortinet Technical Support website at the following location:

<https://support.fortinet.com/>

The license file is required to permanently activate FortiWeb-VM. For details, see [Downloading the FortiWeb-VM license & registering with Technical Support on page 16](#).



FortiWeb-VM needs to periodically re-validate its license by contacting either Fortinet's FortiGuard Distribution Network (FDN) via an Internet connection or a FortiManager.

If FortiWeb-VM cannot contact FDN or FortiManager for 24 hours, it locks access to the web UI and CLI. In some cases, the web UI displays a message such as:

License has been uploaded. Please wait for authentication with registration servers.

For information on restoring access or configuring license validation using FortiManager, see [Uploading the license on page 35](#).

Flex-VM

FortiWeb-VM 7.0.1 and later releases support Flex-VM license on private cloud platforms as well as public cloud platforms including AWS, Azure, and Google Cloud. With Flex-VM license, resource consumption is calculated on a daily basis.

For more information on Flex-VM license, refer to <https://docs.fortinet.com/product/flex-vm/>.

To get the Flex-VM license file:

1. Get the token on Support site. Refer to [this article](#).
2. Run the following command in FortiWeb CLI:

```
exec vm-license <token>
```

A license file will be fetched if the token validation can be passed.

You will see the license status turning into **Valid** on **Dashboard** in GUI, or run `diagnose debug vm license` to check if the license is valid.

Since 7.0.2, it's supported to get the Flex-VM license file through a proxy server:

```
exec vm-license <token> [user:password@]proxyhost[:port]
```

Please note if a proxy server is deployed before FortiWeb, make sure you have run the following command so that FortiWeb can connect with FortiGuard Distribution Network (FDN) through the proxy server for license validation.

```
config system autoupdate tunneling
  set status enable
  set address <proxy_host>
  set port <proxy_port>
  set username <username>
  set password <password>
end
```

Evaluation limitations

Hypervisor FortiWeb-VM deployments include a free 15-day trial license that includes all features **except**:

- High availability (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 FortiWeb-VM.

Once the trial expires, most functionality is disabled. You need to purchase a license to continue using FortiWeb-VM.

AWS BYOL FortiWeb-VM deployments do not include the free trial license. Instead, you can evaluate FortiWeb using the on-demand/hourly version from AWS.

FortiWeb Manager virtual machine

FortiWeb Manager is a specialized VM model that you use to provision, configure, and update FortiWeb appliances (either VM or hardware-based). You use the same steps to install a FortiWeb-VM and the FortiWeb Manager virtual

machine, but FortiWeb Manager performs management tasks only and does not include FortiWeb itself.

FortiWeb Manager's evaluation license has different limitations and the steps for uploading a license are different from FortiWeb-VM.

For details, see the [FortiWeb Manager Administration Guide](#).

About this document

Scope

This document provides the following information:

- How to deploy a FortiWeb virtual appliance in an OpenStack environment. To learn how to deploy FortiWeb-VM on public cloud platforms, see <https://docs.fortinet.com/vm>.
- How to configure any required virtual hardware settings. For hypervisor deployments, it assumes you have already successfully installed a virtualization server on the physical machine or the required EC2 environment.

This document does **not** cover initial configuration of the virtual appliance, nor ongoing use and maintenance. After deploying the virtual appliance, for information on initial appliance configuration, see the [FortiWeb Administration Guide](#) or [FortiWeb Manager Administration Guide](#).

This document is intended for administrators, not end users. If you have a user account on a computer that accesses websites through a FortiWeb appliance, please contact your system administrator.

Conventions

This document uses the conventions described below.

IP addresses

To avoid IP conflicts that would occur if you used examples in this document with public IP addresses that belong to a real organization, the IP addresses used in this document are fictional. They belong to the private IP address ranges defined by these RFCs.

RFC 1918: Address Allocation for Private Internets

<http://ietf.org/rfc/rfc1918.txt?number-1918>

RFC 5737: IPv4 Address Blocks Reserved for Documentation

<http://tools.ietf.org/html/rfc5737>

RFC 3849: IPv6 Address Prefix Reserved for Documentation

<http://tools.ietf.org/html/rfc3849>

For example, even though a real network's Internet-facing IP address would be routable on the public Internet, in this document's examples, the IP address would be shown as a non-Internet-routable IP such as 10.0.0.1, 192.168.0.1, or 172.16.0.1.

Cautions, notes, & tips

This document uses the following guidance and styles for notes, tips and cautions.



Warns you about procedures or feature behaviors that could have unexpected or undesirable results including loss of data or damage to equipment.



Highlights important, possibly unexpected but non-destructive, details about a feature's behavior.



Presents best practices, troubleshooting, performance tips, or alternative methods.

Typographical conventions

This document uses the following typefaces to indicate items such as code or button names.

Typographical conventions in this document

Convention	Example
Button, menu, text box, field, or check box label	From Minimum log level , select Notification .
CLI input	<pre>config system dns set primary <address_ipv4> end</pre>
CLI output	<pre>FortiWeb# diagnose hardware logdisk info disk number: 1 disk[0] size: 31.46GB raid level: no raid exists partition number: 1 mount status: read-write</pre>
Emphasis	HTTP connections are not secure and can be intercepted by a third party.
File content	<pre><HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD> <BODY><H4>You must authenticate to use this service.</H4></BODY></HTML></pre>

Convention	Example
Hyperlink	https://support.fortinet.com
Keyboard entry	Type the IP address or domain name of an NTP server or pool, such as <code>pool.ntp.org</code> .
Navigation	Go to System > Status > Status .
Publication	For details, see the FortiWeb Administration Guide .

Command syntax conventions

The command line interface (CLI) requires that you use valid syntax, and conform to expected input constraints. It will reject invalid commands.

Brackets, braces, and pipes are used to denote valid permutations of the syntax. Constraint notations, such as `<address_ipv4>`, indicate which data types or string patterns are acceptable value input.

Command syntax notation

Convention	Description
Square brackets []	<p>A non-required (optional) word or words. For example:</p> <pre>[verbose {1 2 3}]</pre> <p>indicates that you may either omit or type both the <code>verbose</code> word and its accompanying option, such as:</p> <pre>verbose 3</pre>
Curly braces { }	<p>A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces.</p> <p>You must enter at least one of the options, unless the set of options is surrounded by square brackets [].</p>
Options delimited by vertical bars 	<p>Mutually exclusive options. For example:</p> <pre>{enable disable}</pre> <p>indicates that you must enter either <code>enable</code> or <code>disable</code>, but must not enter both.</p>
Options delimited by spaces	<p>Non-mutually exclusive options. For example:</p> <pre>{http https ping snmp ssh telnet}</pre> <p>indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as:</p> <pre>ping https ssh</pre> <p>Note: To change the options, you must re-type the entire list. For example, to add <code>snmp</code> to the previous example, you would type:</p>

Convention	Description
	<p><code>ping https snmp ssh</code></p> <p>If the option adds to or subtracts from the existing list of options, instead of replacing it, or if the list is comma-delimited, the exception will be noted.</p>
Angle brackets < >	<p>A word constrained by data type.</p> <p>To define acceptable input, the angled brackets contain a descriptive name followed by an underscore (<code>_</code>) and suffix that indicates the valid data type. For example:</p> <p><code><retries_int></code></p> <p>indicates that you should enter a number of retries, such as 5.</p> <p>Data types include:</p> <ul style="list-style-type: none"> • <code><xxx_name></code> — A name referring to another part of the configuration, such as <code>policy_A</code>. • <code><xxx_index></code> — An index number referring to another part of the configuration, such as 0 for the first static route. • <code><xxx_pattern></code> — A regular expression or word with wild cards that matches possible variations, such as <code>*@example.com</code> to match all e-mail addresses ending in <code>@example.com</code>. • <code><xxx_fqdn></code> — A fully qualified domain name (FQDN), such as <code>mail.example.com</code>. • <code><xxx_email></code> — An email address, such as <code>admin@mail.example.com</code>. • <code><xxx_url></code> — A uniform resource locator (URL) and its associated protocol and host name prefix, which together form a uniform resource identifier (URI), such as <code>http://www.fortinet.com/</code>. • <code><xxx_ipv4></code> — An IPv4 address, such as <code>192.168.1.99</code>. • <code><xxx_v4mask></code> — A dotted decimal IPv4 netmask, such as <code>255.255.255.0</code>. • <code><xxx_ipv4mask></code> — A dotted decimal IPv4 address and netmask separated by a space, such as <code>192.168.1.99 255.255.255.0</code>. • <code><xxx_ipv4/mask></code> — A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as <code>192.168.1.99/24</code>. • <code><xxx_ipv6></code> — A colon (<code>:</code>)-delimited hexadecimal IPv6 address, such as <code>3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234</code>. • <code><xxx_v6mask></code> — An IPv6 netmask, such as <code>/96</code>. • <code><xxx_ipv6mask></code> — An IPv6 address and netmask separated by a space. • <code><xxx_str></code> — A string of characters that is not another data type, such as <code>P@ssw0rd</code>. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences. See the FortiWeb CLI Reference.

Convention	Description
	<ul style="list-style-type: none">• <code><xxx_int></code> — An integer number that is not another data type, such as 15 for the number of minutes.

System requirements

FortiWeb-VM supports the following hypervisor versions:

- OpenStack Wallaby; OpenStack deployment does not support True Transparent Proxy or Transparent Inspection operation modes.



For best performance in hypervisor deployments, install FortiWeb-VM on a “bare metal” (type 1) hypervisor. Hypervisors that are installed as applications on top of a general purpose operating system (Windows, Mac OS X or Linux) host have fewer computing resources available due to the host OS’s own overhead.

To ensure high performance, it's recommended to deploy FortiWeb on the machine types with minimum 2 vCPUs, and memory size larger than 8 GB.

Please enable `sse4` if host cpu supports it. Modify OpenStack "nove.conf" file. Set `cpu_mode=host-model` and then reboot the OpenStack server.

For hypervisor deployments, hardware-assisted virtualization (Intel VT or AMD-V) must be enabled in the BIOS. You must also have the VM environment client, such as VMware vSphere Client, installed on a management computer. (A management computer is a desktop or a laptop that you use to deploy and manage your virtual machines.)

Downloading the FortiWeb-VM license & registering with Technical Support

For Hypervisor deployments, when you purchase FortiWeb-VM from your reseller, you receive an email that contains a registration number. You use this number to download the software and your purchased license, and also to register your purchase for technical support.

If you have purchased an offline license, that is, the license for FortiWeb-VM which is deployed in a closed network environment, your license file is sent directly to you from Fortinet Customer Support team. You can skip the following register & download steps.

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

For details, see the Fortinet Knowledge Base article [Registration Frequently Asked Questions](#).

To register & download your FortiWeb-VM license

1. On your management computer, start a web browser.
2. Log in to the Fortinet Technical Support website:
<https://support.fortinet.com/>
3. In the **Asset Management** quadrant of the page, click **Register/Renew**.
4. Provide the registration number that was emailed to you when you purchased the software. Registration numbers are a hyphenated mixture of 25 numbers and characters in groups of 5. For example:
12C45-AB3DE-678G0-F9HIJ-123B5
A registration form is displayed.
5. Complete the form to register your ownership of FortiWeb-VM with Technical Support.
After you complete the form, a registration acknowledgement page is displayed.
6. Click the **License File Download** link.
Your browser downloads the `.lic` file that was purchased for that registration number.
7. Download the FortiWeb software using the steps in [Downloading the FortiWeb-VM software](#).

Downloading the FortiWeb-VM software

To download your FortiWeb-VM software

1. On the main page of the Fortinet Technical Support website, under **Download**, click **Firmware Images**.
2. Click the FortiWeb link and navigate to the version that you want to download.
3. Download the appropriate `.zip` file. .
You use this file for **new virtual appliance (VM)** installations. It contains a deployable virtual machine package. (`.out` image files are for upgrades of existing installations only, and cannot be used for a new installation.)



Files for FortiWeb-VM have a `FWB_VM` file name prefix. Other prefixes indicate that the file is for hardware versions of FortiWeb such as FortiWeb 4000D. These hardware versions are not used with FortiWeb-VM.

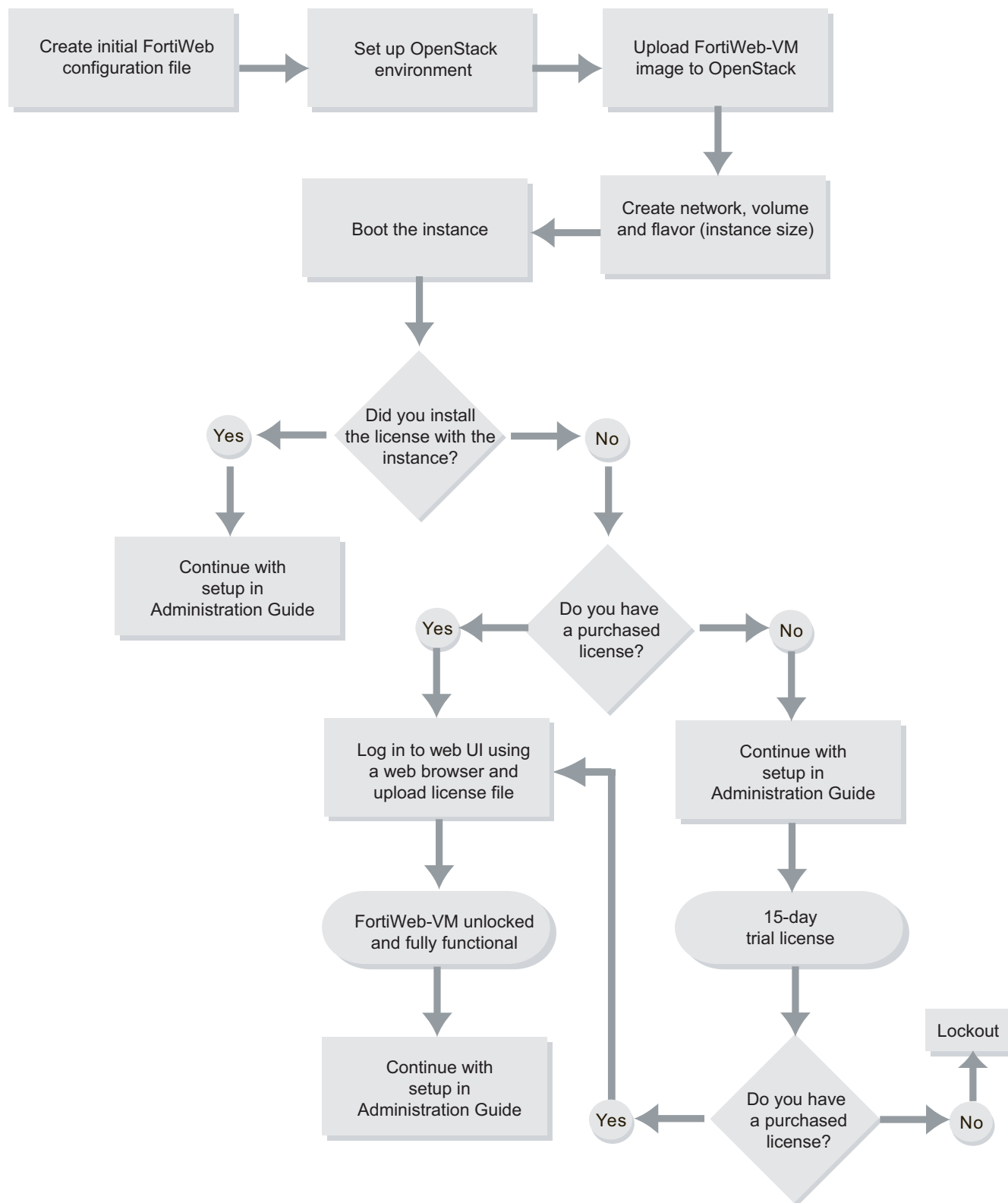


If you have a library of virtual machine images stored on a CIFS or NFS share, download and unzip the folder there instead of on your management computer. When deploying the VM, you can also use a CIFS or NFS network share as the storage repository instead of a vDisk stored locally, on the hypervisor's disk.

4. Extract the `.zip` compressed archive's contents to a folder.
5. Continue by deploying the virtual appliance package using the appropriate deployment instructions in the next section.

Preparing to deploy on OpenStack

You deploy FortiWeb-VM on the OpenStack cloud computing platform using the KVM version of the FortiWeb-VM software.



Downloading the FortiWeb-VM license and software

You can include the license file when you deploy FortiWeb-VM on OpenStack. See [Downloading the FortiWeb-VM license & registering with Technical Support on page 16](#).

If you do not include the license file, the instance runs using the built-in trial license and you can upload the license later. For details, see [Licensing on page 7](#).

Download the appropriate KVM version of the FortiWeb-VM software and extract the .zip compressed archive's contents. The archive's contents include the image file `boot.qcow2` that you upload to OpenStack.

For details, see [Downloading the FortiWeb-VM software on page 17](#).

Creating an initial FortiWeb configuration file

Deploying a FortiWeb-VM instance on OpenStack requires a FortiWeb configuration file.

Ensure the file configures:

- port1 to use DHCP, which allows it to acquire an IP address from OpenStack
- A DNS server address for verifying the FortiWeb-VM license

You can include additional configuration that takes affect when you deploy the FortiWeb-VM instance.

The following commands are an example of the configuration file:

```
config system global
set hostname KVM-CLOUD-INIT
set admintimeout 480
end
config system interface
edit "port1"
set type physical
set allowaccess https ping ssh snmp http telnet
set mode dhcp
config secondaryip
end
next
end
config system dns
set secondary 114.114.114.114
end
```

Deploying FortiWeb-VM on OpenStack

The examples shown in this procedure create a FortiWeb-VM instance with the following properties:

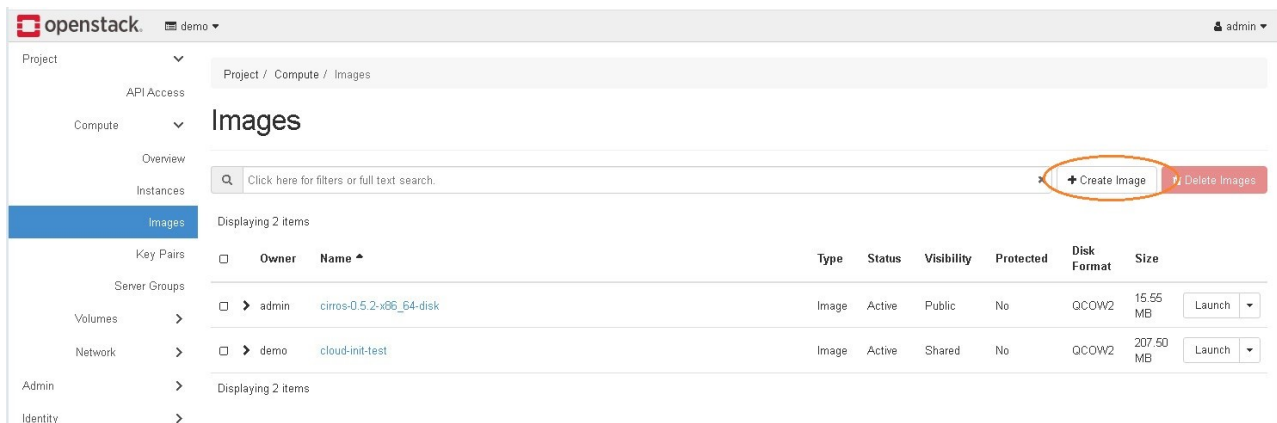
- A direct connection to the public network
 - A 30 GB log disk (an OpenStack volume)
 - 2 vCPUs with 8 GB RAM and a 40 GB root disk (specified by the OpenStack flavor)
 - Fully licensed
1. To set up your OpenStack environment, create an `openrc.sh` (OpenStack rc) file that specifies the admin credentials and admin endpoint.

For example, the OpenStack rc file `admin-openrc.sh` has the following:

```
openstack@controller:~$
openstack@controller:~$ cat admin-openrc.sh
export OS_PROJECT_DOMAIN_ID=default
export OS_USER_DOMAIN_ID=default
export OS_PROJECT_NAME=admin
export OS_TENANT_NAME=admin
export OS_USERNAME=admin
export OS_PASSWORD=fortiweb
export OS_AUTH_URL=http://controller:35357/v3
export OS_IDENTITY_API_VERSION=3

export HEAT_DOMAIN_PASSWORD=fortiweb
export OS_IMAGE_API_VERSION=2
export OS_AUTH_VERSION=3
#export OS_TOKEN=7e6bb6afe0d80196e240
#export OS_URL=http://10.200.2.120:35357/v2.0/
#export SERVICE_TOKEN=7e6bb6afe0d80196e240
openstack@controller:~$
```

- Using the shell you use to run OpenStack commands, source the OpenStack rc file. For example:
\$ `source admin-openrc.sh`
- Log in to the OpenStack dashboard, under **Compute**, navigate to the list of images, and then click **Create Image**.



- Complete the image settings.

For **Image Source**, select **Image File**. Use the Image File options to navigate to and select the `boot.qcow2` file you extracted from the FortiWeb-VM KVM software package. For **Format**, select **QCOW2-QEMU Emulator**.

Create Image

Image Details

Metadata

Image Details

Specify an image to upload to the Image Service.

Image Name

cloud-init-test

Image Description

Image Source

File

Browse...

boot.qcow2

Format

QCOW2 - QEMU Emulator

Image Requirements

Kernel

Choose an image

Ramdisk

Choose an image

Architecture

Minimum Disk (GB)

0

Minimum RAM (MB)

0

Image Sharing

Visibility

Private Shared Community Public

Protected

Yes No

Cancel

Back

Next

Create Image

5. Click **Create Image**, and then use the dashboard to verify that OpenStack added the image.

openstack demo

admin

Project / Compute / Images

Images

Click here for filters or full text search.

Create Image Delete Images

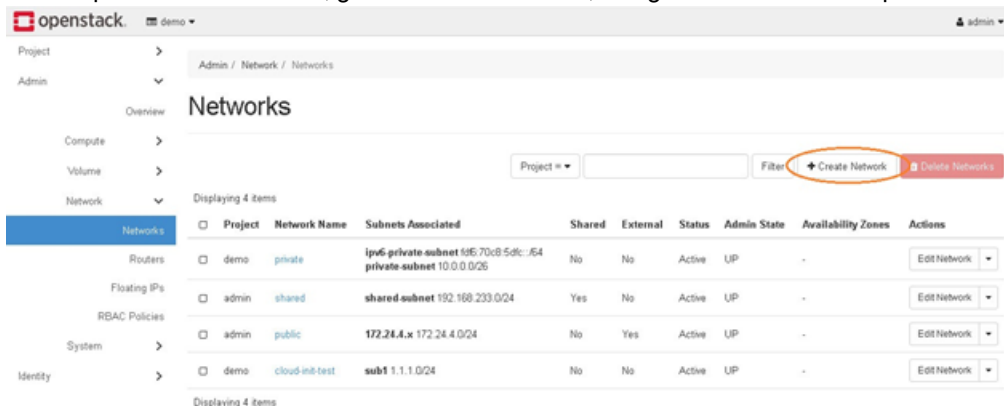
Displaying 2 items

	Owner	Name	Type	Status	Visibility	Protected	Disk Format	Size	
	admin	cirros-0.5.2-x86_64-disk	Image	Active	Public	No	QCOW2	15.55 MB	Launch
	demo	cloud-init-test	Image	Active	Shared	No	QCOW2	207.50 MB	Launch

Alternatively, use the CLI command `openstack image list` to verify the image.

```
fortinet@fortinet-virtual-machine:~$ openstack image list
+-----+-----+-----+
| ID | Name | Status |
+-----+-----+-----+
| e387b7f6-038c-4185-ab84-e008af481888 | cirros-0.5.2-x86_64-disk | active |
| f16d1e33-458a-4dba-97ab-0dce8e89b06a | cloud-init-test | active |
+-----+-----+-----+
fortinet@fortinet-virtual-machine:~$
```

6. In the OpenStack dashboard, go to Admin > Network, navigate to the Network options and click **Create Network**.



7. In the network creation wizard, configure MTU to 1500 and complete the network and subnet settings.

✕

Create Network

Network ^{*}

Subnet

Subnet Details

Name

Project ^{*}

demo
▼

Provider Network Type ^{*} ?

Local
▼

☒ **Enable Admin State** ?

☒ **Shared**

☐ **External Network**

☒ **Create Subnet**

Availability Zone Hints ?

MTU ?

1500

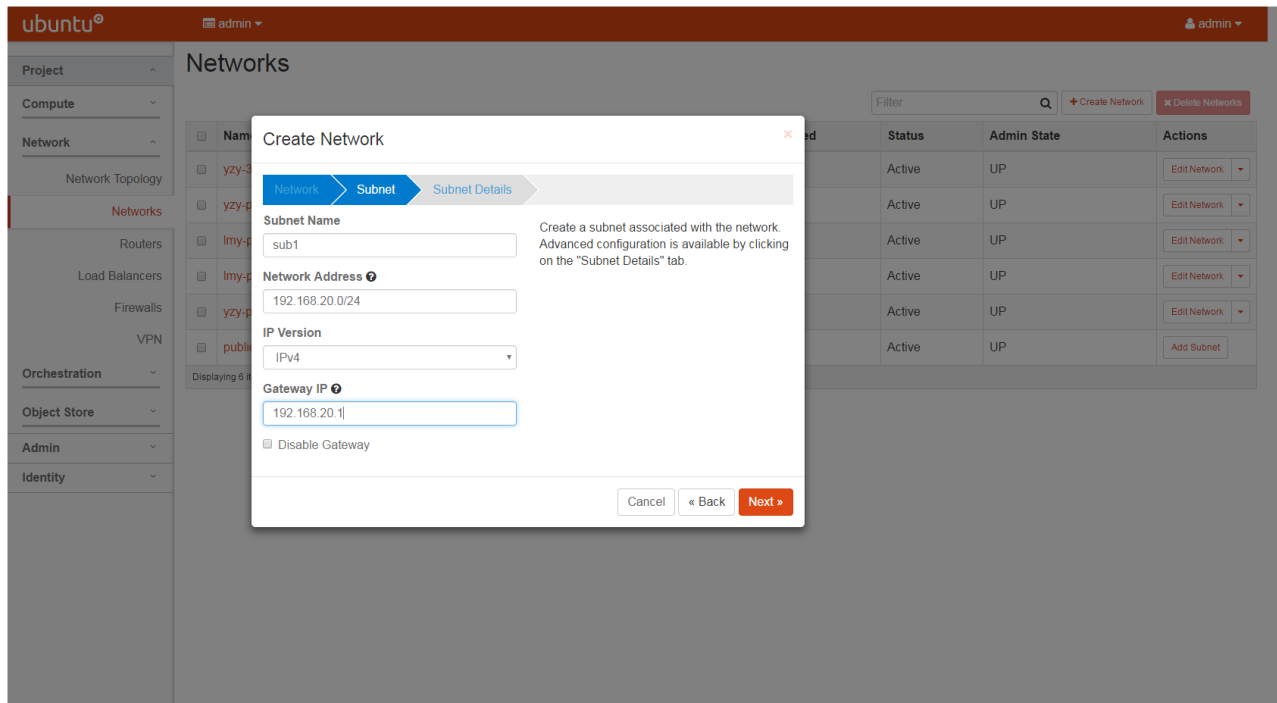
▲
▼

Create a new network. In addition, a subnet associated with the network can be created in the following steps of this wizard.

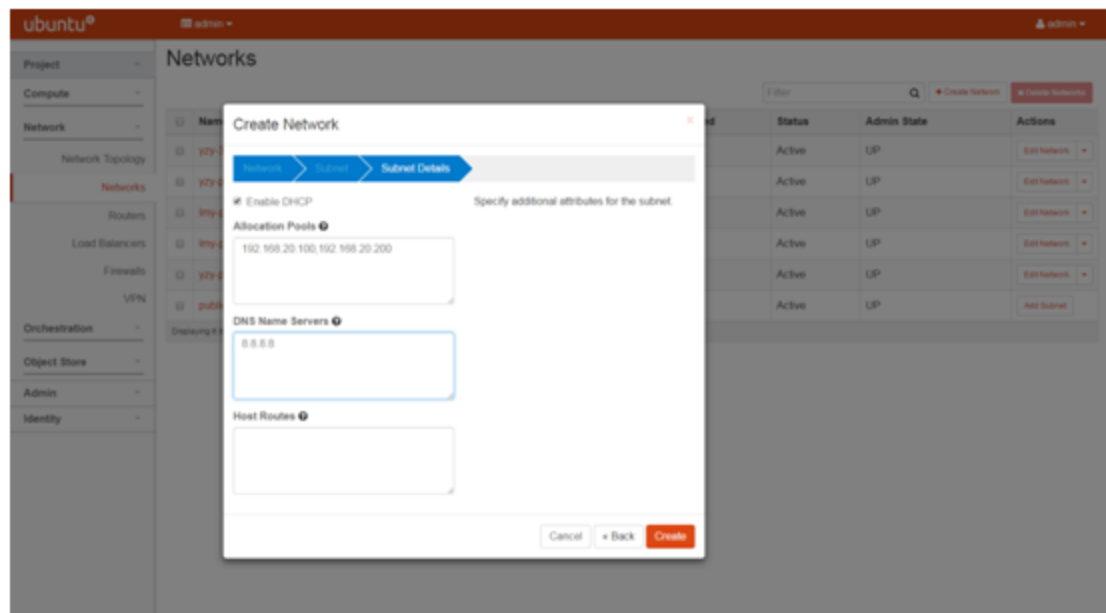
Cancel

« Back

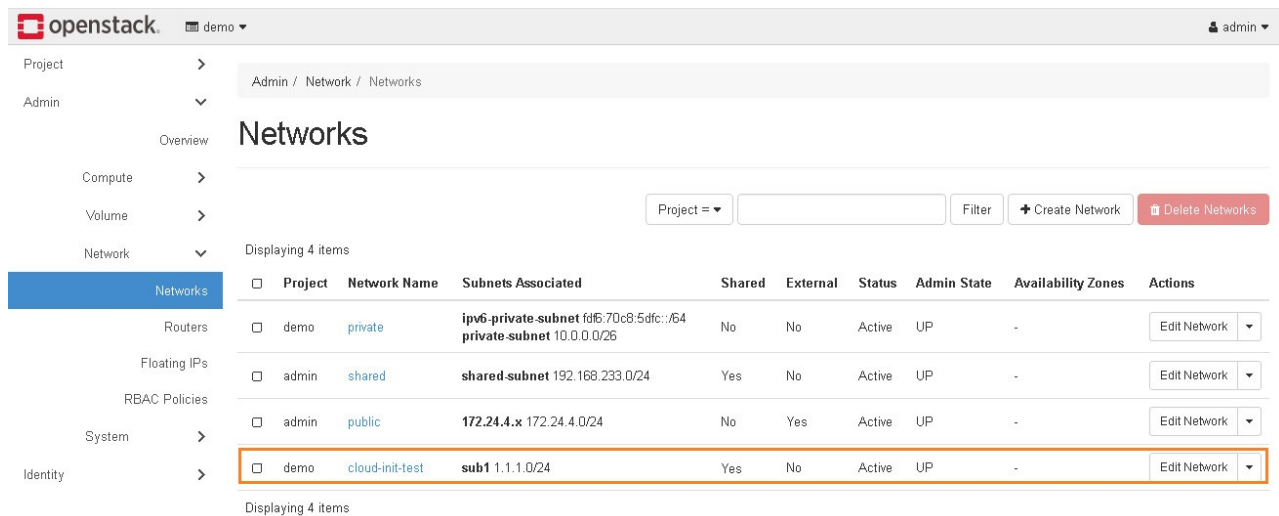
Next »



8. In the wizard, complete the subnet details. You can use a pool to assign the network's IP address range.



9. Click **Create**, and then use the dashboard to verify that OpenStack added the network.



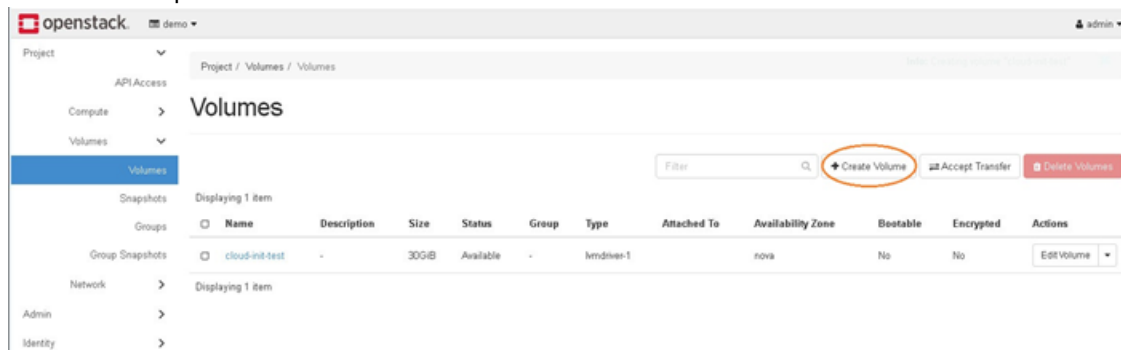
The screenshot shows the OpenStack dashboard interface. On the left is a sidebar with navigation links: Project, Admin, Overview, Compute, Volume, Network, Networks (selected), Routers, Floating IPs, RBAC Policies, System, and Identity. The main content area is titled 'Networks' and shows a table of four networks. The 'cloud-init-test' network is highlighted with an orange border.

Project	Network Name	Subnets Associated	Shared	External	Status	Admin State	Availability Zones	Actions
demo	private	ipv6-private-subnet fd6:70c8:5dfc::/64 private-subnet 10.0.0.0/26	No	No	Active	UP	-	Edit Network
admin	shared	shared-subnet 192.168.233.0/24	Yes	No	Active	UP	-	Edit Network
admin	public	172.24.4.x 172.24.4.0/24	No	Yes	Active	UP	-	Edit Network
demo	cloud-init-test	sub1 1.1.1.0/24	Yes	No	Active	UP	-	Edit Network

Alternatively, use the CLI command `openstack network list` to verify the image.

```
fortinet@fortinet-virtual-machine:~$ openstack network list
+-----+-----+-----+
| ID | Name | Subnets |
+-----+-----+-----+
| 0b793a46-5820-4615-95e4-477976b64758 | private | 9aa23c64-761a-4d99-88dd-8853e6119b7d, db48b582-122c-428b-a2c5-4a9fab5cace |
| 32ccf0bc-d4de-41df-88ef-443342047c4c | cloud-init-test | 2fd9c791-4df8-4ec9-9ec3-72116718f0bc |
| 34ec6e41-229b-4ff7-acc6-ff67823bc475 | shared | 20447f6b-83fa-4fcc-aef5-107cf319928e |
| 9b13e3a6-ac37-4bff-a3d1-81071a3c235c | public | 40b00ec2-369e-48c9-aa69-e38b89ca8b93, b83cdcd5-42f2-43ca-837b-7c32baba49e2 |
+-----+-----+-----+
```

- To create the volume FortiWeb-VM uses for its log disk, in the OpenStack dashboard, under **Volumes**, navigate to the **Volumes** options and click **Create Volume**.



The screenshot shows the OpenStack dashboard interface for the 'Volumes' section. The 'Create Volume' button is highlighted with an orange circle. The table below shows a single volume named 'cloud-init-test'.

Name	Description	Size	Status	Group	Type	Attached To	Availability Zone	Bootable	Encrypted	Actions
cloud-init-test	-	30GB	Available	-	lvmdriver-1	nova	nova	No	No	Edit Volume

11. Complete the volume settings.

Create Volume ✕

Volume Name

Description

Volume Source

No source, empty volume ▼

Type

lvmdriver-1 ▼

Size (GiB) *

▲▼

Availability Zone

nova ▼

Group ⓘ

No group ▼

Description:

Volumes are block devices that can be attached to instances.

Volume Type Description:

lvmdriver-1

No description available.

Volume Limits

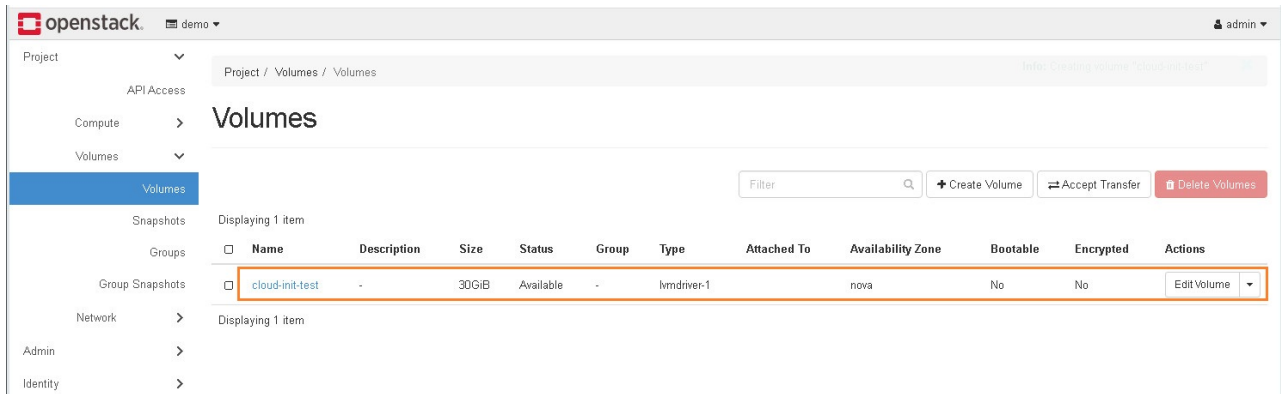
Total Gibibytes 0 of 1,000 GiB Used

Number of Volumes 0 of 10 Used

Cancel

Create Volume

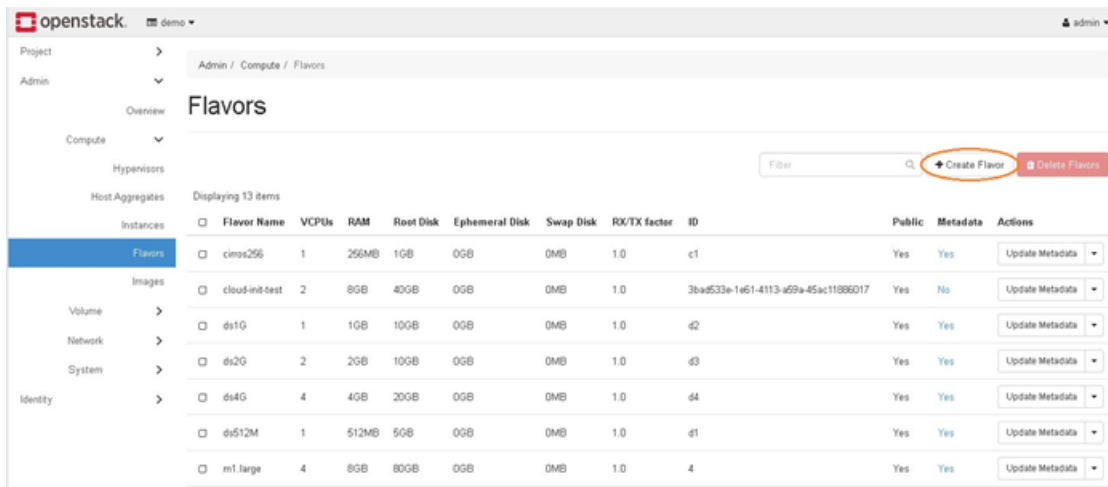
12. Click **Create Volume**, and then use the dashboard to verify that OpenStack added the volume.



Alternatively, use the CLI command `openstack volume list` to verify the volume.

```
fortinet@fortinet-virtual-machine:~$ openstack volume list
+-----+-----+-----+-----+-----+-----+-----+
| ID                               | Name           | Status   | Size | Attached to |
+-----+-----+-----+-----+-----+-----+
| 5a15be2d-2b99-4a93-8da7-47794bd10bd7 | cloud-init-test | available | 30 |             |
+-----+-----+-----+-----+-----+-----+
fortinet@fortinet-virtual-machine:~$
```

- To specify the size of the instance, in the OpenStack dashboard, under **System**, navigate to the Flavors options and click **Create Flavor**.



- Complete the flavor settings.
For *VCPUs*, type the maximum number of vCPUs to allocate. Valid values range from 1 to 8.

Create Flavor

Flavor Information *

Flavor Access

Name *

cloud-init-test

ID ?

auto

VCPUs *

2

RAM (MB) *

8192

Root Disk (GB) *

40

Ephemeral Disk (GB)

0

Swap Disk (MB)

0

RX/TX Factor

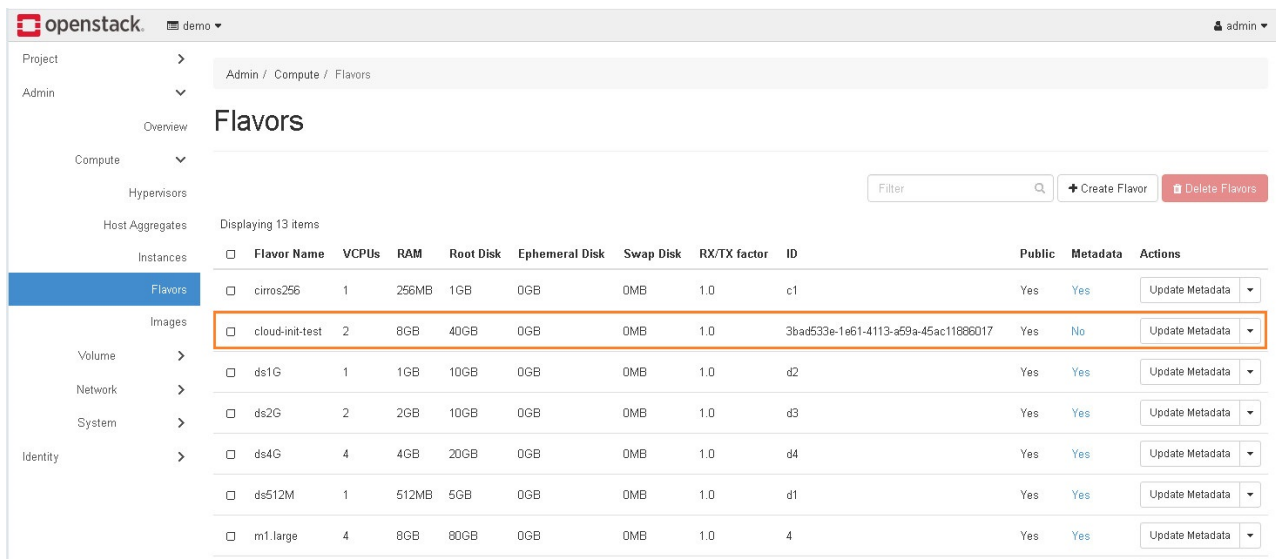
1

Flavors define the sizes for RAM, disk, number of cores, and other resources and can be selected when users deploy instances.

Cancel

Create Flavor

15. Click **Create Flavor**, and then use the dashboard to verify that OpenStack added the flavor.



Flavor Name	VCPUs	RAM	Root Disk	Ephemeral Disk	Swap Disk	RX/TX factor	ID	Public	Metadata	Actions
cirros256	1	256MB	1GB	0GB	0MB	1.0	c1	Yes	Yes	Update Metadata
cloud-init-test	2	8GB	40GB	0GB	0MB	1.0	3bad533e-1e61-4113-a59a-45ac11886017	Yes	No	Update Metadata
ds1G	1	1GB	10GB	0GB	0MB	1.0	d2	Yes	Yes	Update Metadata
ds2G	2	2GB	10GB	0GB	0MB	1.0	d3	Yes	Yes	Update Metadata
ds4G	4	4GB	20GB	0GB	0MB	1.0	d4	Yes	Yes	Update Metadata
ds512M	1	512MB	5GB	0GB	0MB	1.0	d1	Yes	Yes	Update Metadata
m1.large	4	8GB	80GB	0GB	0MB	1.0	4	Yes	Yes	Update Metadata

16. Confirm the location of the initial FortiWeb configuration file you created earlier and the FortiWeb-VM license file. See [Preparing to deploy on OpenStack on page 17](#).

This example uploads the license as part of the boot process. Alternatively, you can omit the license file and upload it later. See [Uploading the license on page 35](#).

```
fortinet@fortinet-virtual-machine:~$ cat lmy/config.txt
config system global
set hostname KVM-CLOUD-INIT
set admintimeout 480
end
config system interface
edit "port1"
set type physical
set allowaccess https ping ssh snmp http
set mode dhcp
config secondaryip
end
next
end
config system dns
set secondary 114.114.114.114
end
fortinet@fortinet-virtual-machine:~$ ls lmy/FVVM08TM21000623.lic
lmy/FVVM08TM21000623.lic
fortinet@fortinet-virtual-machine:~$
```

17. Use the utility 'write-mime-multipart' in Ubuntu system to convert the initial FortiWeb configuration file and FortiWeb-VM license file to a user data file for deployment.

```
write-mime-multipart -o <user_data_file> <config_file>:text/cloud-config
<fweb_license>:text/cloud-config
```

where:

<fweb_license> is the name and path of the FortiWeb license file

<config_file> is the name and path of the initial configuration file you created earlier. It is the booting CLI configuration that FortiWeb uses. You can use this file for some public initialization configuration that scales the deployment.

<user_data_file> is the name and path of the combined file which contains information of the initial

configuration file and the FortiWeb license file.

For example: `write-mime-multipart -o user_data.txt lmy/config.txt:text/cloud-config lmy/FVVM08TM21000623.lic:text/cloud-config`

18. Use the following command to boot the instance:

```
nova boot --config-drive true --image <image_name> --flavor <flavor_name> --user-data
<user_data_file> --nic net-id=<network_id> --block-device-mapping vdb=<volume_
id> <instance_name>
```

where:

`--config-drive true` enables OpenStack to write metadata to a special configuration drive that it attaches to the instance when it boots

`<image_name>` is the name of the FortiWeb-VM KVM image you uploaded earlier

`<flavor_name>` is the OpenStack flavor you configured earlier that specifies the size of the instance

`<user_data_file>` is the name and path of the combined file which contains information of the initial configuration file and the FortiWeb license file

`<network_id>` is the ID of public network you created earlier for the instance to use

`<volume_id>` is the ID of the volume you created earlier to use as the FortiWeb log disk

`<instance_name>` is the name for the instance

For example (the image and the instance are both named cloud-init-test):

```
nova boot --config-drive true --image cloud-init-test --flavor cloud-init-test --user-
data user_data --nic net-id=703fb27e-37e4-4dbe-8bfb-c65f948648a4 --block-device-
mapping vdb=5a15be2d-2b99-4a93-8da7-47794bd10bd7 cloud-init-test
```

19. OpenStack returns a table that allows you to confirm the instance configuration.

```
fortinet@fortinet-virtual-machine:~$ nova boot --config-drive true --image cloud-init-test --flavor cloud-init-test --user-data user-data.txt -
-nic net-id=32ccf0bc-d4de-41df-88ef-443342047c4c --block-device-mapping vdb=eae2d2d-da2e-4bfb-bf00-9ec486d5ec83 cloud-init-test
```

Property	Value
OS-DCF:diskConfig	MANUAL
OS-EXT-AZ:availability_zone	-
OS-EXT-SRV-ATTR:host	-
OS-EXT-SRV-ATTR:hostname	cloud-init-test
OS-EXT-SRV-ATTR:hypervisor_hostname	-
OS-EXT-SRV-ATTR:instance_name	-
OS-EXT-SRV-ATTR:kernel_id	-
OS-EXT-SRV-ATTR:launch_index	0
OS-EXT-SRV-ATTR:ramdisk_id	-
OS-EXT-SRV-ATTR:reservation_id	r-68qlcs9b
OS-EXT-SRV-ATTR:root_device_name	-
OS-EXT-STS:power_state	0
OS-EXT-STS:task_state	scheduling
OS-EXT-STS:vm_state	building
OS-SRV-USG:launched_at	-
OS-SRV-USG:terminated_at	-
accessIPv4	-
accessIPv6	-
adminPass	rF9s4pWMyz3p
config_drive	True
created	2021-09-23T03:16:55Z
description	-
flavor:disk	40
flavor:ephemeral	0
flavor:extra_specs	{}
flavor:original_name	cloud-init-test
flavor:ram	8192
flavor:swap	0
flavor:vcpus	2
hostId	-
host_status	-
id	531396d8-72ad-456b-b37a-a9f66bbb0438
image	cloud-init-test (f874d0a6-c5c5-4839-91cd-06a198c160cc)
key_name	-
locked	False
locked_reason	-
metadata	{}
name	cloud-init-test
os-extended-volumes:volumes_attached	[]
progress	0
security_groups	default
server_groups	[]
status	BUILD
tags	[]
tenant_id	79644821ca854a18a30ba9aca07ad0c6
trusted_image_certificates	-
updated	2021-09-23T03:16:54Z
user_id	528a8a5212e14ab6b8f3c1c208aedbbc

20. Use the CLI command `nova list` to display the status of the instance and the IP address it was assigned.

```
fortinet@fortinet-virtual-machine:~$ nova list
```

ID	Name	Status	Task State	Power State	Networks
531396d8-72ad-456b-b37a-a9f66bbb0438	cloud-init-test	ACTIVE	-	Running	cloud-init-test=1.1.1.162

21. Use OpenStack Instance Console or SSH to connect to the instance to confirm the initial configuration and that the license file has been uploaded to the FortiWeb.

```
KUM-CLOUD-INIT # get system interface
== [ port1 ]
    type: physical
    ip: 1.1.1.162/24
    ip6: ::40
    allowaccess: ping ssh snmp http https
    status: up
    mode: dhcp
    ip6-mode: static
    description:
    ip6-allowaccess:
    wccp: disable
    mtu: 1442
    dynamic_gateway: 1.1.1.254
    dynamic_dns1: 8.8.8.8
    dynamic_dns2:
```

22. Continue with the appliance configuration using the CLI or access the web UI using the assigned IP address. For complete configuration information, see the [FortiWeb Administration Guide](#).



When you deploy the FortiWeb-VM package, network adapters are created automatically. If you want to delete network adapters, do it during the deployment process. It's not recommended to delete network adapters once the FortiWeb is deployed, otherwise unexpected error will occur.

Configuring access to FortiWeb's web UI & CLI

For hypervisor deployments, after the virtual appliance is powered on, you log in to the FortiWeb-VM command line interface (CLI) via the console and configure basic network settings so that you can connect to the appliance's web UI, CLI, or both through your management computer's network connection.

To configure basic network settings for FortiWeb-VM deployed on a hypervisor

1. On your management computer, start the following according to the VM environment in which you have deployed FortiWeb-VM:
2. Log in to the VM server.
3. Open the console of the FortiWeb-VM virtual appliance.
4. At the login prompt for the local console, type:
admin
5. Press **Enter** twice. (Initially, there is no password.)
6. Configure the IP address and netmask of the network interface named `port1`, or whichever network interface maps to the network physically connected to your management computer. Type:

```
config system interface
edit port1
set ip <address_ip> <netmask_ip>
end
```

where:

- `<address_ip>` is the IPv4 or IPv6 address assigned to the network interface, such as `192.168.1.99`; the correct IP will vary by your configuration of the vNetwork (see [Mapping the virtual NICs \(vNICs\) to physical NICs on page 1](#))
- `<netmask_ip>` is its netmask in dotted decimal format, such as `255.255.255.0` (alternatively, append a CIDR-style subnet such as `/24` to the IP)

7. Configure the primary and secondary DNS server IP addresses. Type:

```
config system dns
set primary <dns_ip>
set secondary <dns_ip>
end
```

where `<dns_ip>` is the IPv4 or IPv6 address of a DNS server.

8. Configure a static route with the default gateway. Type:

```
config router static
edit 0
set gateway <router_ip>
set device port1
end
```

where `<router_ip>` is the IP address of the gateway router.

You should now be able to connect via the network from your management computer to `port1` of FortiWeb-VM using:

- a web browser for the web UI (e.g. If `port1` has the IP address `192.168.1.1`, go to `https://192.168.1.1/`)
- an SSH client for the CLI (e.g. If `port1` has the IP address `192.168.1.1`, connect to `192.168.1.1` on port `22`.)



When connecting to the web UI via HTTPS, if you cannot get a connection, verify that your computer's time zone matches the appliance's configured system time. For more first-time connection troubleshooting, or instructions on how to configure the time and time zone, see the [FortiWeb Administration Guide](#).



In versions earlier than 6.3.6, enabling HA requires all interfaces to enable DHCP mode. From 6.3.6, only port1 is required to enable DHCP mode.

9. Continue by uploading the license file. (See [Uploading the license on page 35](#). For the FortiWeb Manager license, see the [FortiWeb Manager Administration Guide](#).)

If you are using the 15-day free trial license and do not yet have a paid license file, you can continue instead with [What's next? on page 43](#).



When the 15-day free trial license expires, you will not be able to perform any actions in the web UI until a license has been uploaded. After a valid license has been uploaded, the web UI and the CLI will be unlocked and fully functional. The trial period begins the first time you power on your FortiWeb-VM virtual appliance. You can upgrade the trial license to a purchased one at any time during or after the trial period by uploading the license file via the **License Information** widget in the dashboard of the web UI. For instructions, see [Uploading the license on page 35](#).

Uploading the license

When you purchase a license for FortiWeb-VM, Fortinet Customer Service & Support (<https://support.fortinet.com>) provides a license file that you can use to convert the 15-day trial license to a permanent, paid license.

(Licensing for FortiWeb Manager virtual machine is different. See the [FortiWeb Manager Handbook](#).)

You can upload the license via a web browser connection to the web UI or the CLI. No maintenance period scheduling is required. The uploading process does not interrupt traffic or trigger an appliance reboot.



As your organization grows, you can simply either allocate more resources or migrate your virtual appliance to a physical server with more power, then upgrade your FortiWeb-VM license to support your needs.

License Validation

FortiWeb-VM requires an Internet connection to periodically re-validate its license. If FortiWeb-VM cannot communicate with Fortinet's FDN for 24 hours, access to the web UI and CLI are locked.

If FortiWeb-VM is deployed in a closed network environment, license validation can be done in the following two ways.

License validation with FDS proxy

You can validate your FortiWeb-VM license through an FDS proxy. FortiManager's built-in FDS (FortiGuard Distribution Servers) feature can serve this purpose. This requires FortiManager to have Internet connection. To configure FortiWeb-VM to validate its license using FortiManager, before you upload the license, enter the following command:

```
config system autoupdate override
    set status enable
    set address <fortimanager_ip>:8890
    set fail-over disable
end
```

where <fortimanager_ip> is the IP address of the FortiManager. (TCP port 8890 is the port where the built-in FDS feature listens for requests.)

For more information on the FortiManager built-in FDS feature, see the [FortiManager Administration Guide](#).



Although FortiManager can provide FortiGuard security service updates to some Fortinet devices, for FortiWeb, its FDS features can provide license validation only.

License validation with UUID

If you have purchased a FortiWeb-VM license specially designed for a closed network environment, the Fortinet customer support team validates the license with an UUID, and then issues the license file to you. This license type does not require an FDS proxy for license validation.

Uploading the license

To upload the license via the web UI

1. On your management computer, start a web browser.
For hypervisor installations, your computer must be connected to the same network as the hypervisor.
2. Do one of the following:
 - For hypervisor deployments, in your browser's URL or location field, enter the IP address of `port1` of the virtual appliance, such as:

<https://192.168.1.99/>

(Remember to include the "s" in https://.)



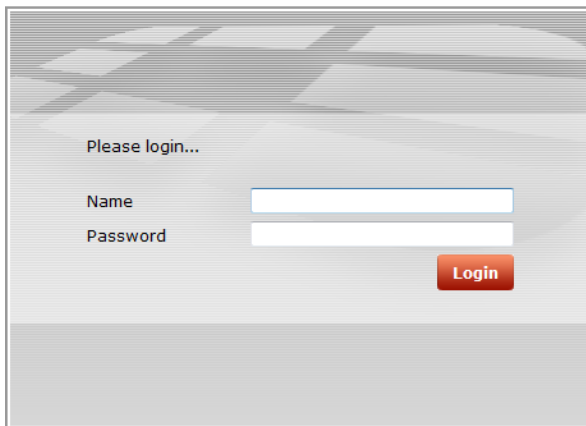
Initially, you must access the web UI via HTTPS. By default, HTTP is not enabled. After uploading the license, you can configure the administrative access protocols. For details, see the [FortiWeb Administration Guide](#).

- For FortiWeb-VM deployed on AWS, access the web UI using the public DNS address displayed in the instance information for the appliance in your AWS console.

For example, if the public DNS address is `ec2-54-234-142-136.compute-1.amazonaws.com`, you connect to the web UI using the following URL:

<https://ec2-54-234-142-136.compute-1.amazonaws.com/>

Your browser connects the appliance. The web UI's login page should appear.



If you do **not** see the login page due to an SSL cipher error during the connection, and you are connecting to the trial license of FortiWeb-VM or a LENC version of FortiWeb, then your browser must be configured to accept encryption of 64-bit strength or less during the handshake. (RC2, RC4, and DES with less than 64-bit strength is supported. AES and 3DES is **not** supported in these versions.) Otherwise SSL v3 and TLS v1.0 are supported.

For example, in Mozilla Firefox, if you receive this error message:

`ssl_error_no_cypher_overlap`

you may need to enter `about:config` in the URL bar, then set **`security.ssl3.rsa.rc4_40_md5`** to **true**.

To support HTTPS authentication, the FortiWeb appliance ships with a self-signed X.509 certificate, which it presents to clients whenever they initiate an HTTPS connection to the FortiWeb appliance. When you connect, depending on your web browser and prior access of the FortiWeb appliance, your browser might display two security warnings related to this certificate:

- The certificate is not automatically trusted because it is self-signed, rather than being signed by a valid certificate authority (CA). Self-signed certificates cannot be verified with a proper CA, and therefore might be fraudulent. You must manually indicate whether or not to trust the certificate.
- The certificate might belong to another website. The common name (CN) field in the certificate, which usually contains the host name of the website, does not exactly match the URL you requested. This could indicate server identity theft, but could also simply indicate that the certificate contains a domain name while you have entered an IP address. You must manually indicate whether this mismatch is normal or not.

Both warnings are normal for the default certificate.

3. Verify and accept the certificate, either permanently (the web browser will not display the self-signing warning again) or temporarily. You cannot log in until you accept the certificate.
4. For details on accepting the certificate, see the documentation for your web browser.
5. In the *Name* field, type `admin`. Do one of the following:
 - For hypervisor deployments, do not enter a password.
 - For AWS deployments, for **Password**, enter the AWS instance ID.
6. Click **Login**.

The web UI appears.

The web UI initially displays its dashboard, **System > Status > Status**. The **FortiGuard Information** widget displays the current license status and contains a link where you can upload a license file.

FortiGuard Information widget on System > Status > Status in the web UI before license upload

FortiGuard Information	
VM License	Invalid [Update]
Registration	[Unregistered]
FortiWeb FortiGuard Subscription Services	
FortiWeb Security Service	Expired (1969-12-31) Last Update Time:1999-11-30 Last Update Method: Manual Signature Build Number-0.00091
FortiWeb Antivirus Service	Expired (1969-12-31) Last Update Time:2011-12-07 Last Update Method: Manual Regular Virus Database Version-14.00922 Extended Virus Database Version-14.00922
FortiWeb IP Reputation Service	Expired (1969-12-31) Last Update Time:1999-11-30 Last Update Method: Manual Signature Build Number-1.00020

7. In the **VM License** row of the **FortiGuard Information** widget, click the **Update** link.

Install FortiWeb-VM License File

License File: No file chosen

8. Depending on your browser, you may see either a **Browse** or **Choose File** button. Locate the license file (.lic) you downloaded earlier from Fortinet, then click **OK**.

Your browser uploads the license file. Time required varies by the size of the file and the speed of the network connection. If you have uploaded a file that is not a license file, an error message will appear:

Uploaded file is not a license. Please upload a valid license.

If you upload the right file type, FortiWeb will then connect to Fortinet to validate its license. Time required varies, but is usually only a few seconds. A message appears:

License has been uploaded. Please wait for authentication with registration servers.

9. Click **Refresh** on the message box.
If you uploaded a valid license, a second message should appear, informing you that your license authenticated successfully:

License has been successfully authenticated with registration servers.

The web UI logs you out. The login dialog reappears.

10. Log in again.
11. To verify that the license was uploaded successfully, log in to the web UI again, then view the **FortiGuard Information** widget. The **VM License** row should say **Valid**.
Also view the **System Information** widget. The **Serial Number** row should have a number that indicates the maximum number of vCPUs that can be allocated according to the FortiWeb-VM software license, such as **FVVM020000003619** (where "VM02" indicates a limit of 2 vCPUs).

FortiGuard Information widget on System > Status > Status in the web UI after license validation

FortiGuard Information	
VM License	Valid [Update]
Registration	cschwartz@fortinet.com
FortiWeb FortiGuard Subscription Services	
FortiWeb Security Service	Valid Contract (Expires 2020-01-04) Last Update Time:2013-01-16 Last Update Method: Manual Signature Build Number-0.00072
FortiWeb Antivirus Service	Valid Contract (Expires 2020-01-04) Last Update Time:2013-01-16 Last Update Method: Manual Regular Virus Database Version-17.21 Extended Virus Database Version-17.17
FortiWeb IP Intelligence Service	Valid Contract (Expires 2020-01-04) Last Update Time:2013-01-16 Last Update Method: Manual Signature Build Number-1.00013

GUI item	Description
VM License	Indicates whether or not this FortiWeb-VM appliance has a paid software license. The license affects the maximum number of allocatable vCPUs. Possible states are: <ul style="list-style-type: none"> Valid — The appliance has a valid, non-trial license. Serial

GUI item	Description
	<p>Number in the System Information widget indicates the maximum number of vCPUs that can be allocated according to this license.</p> <p>To increase the number of vCPUs that this appliance can utilize, invalidate the current license by allocating more vCPUs in your virtual machine environment (e.g. VMware), then upload a new license. See Updating the license for more vCPUs on page 1.</p> <ul style="list-style-type: none"> • Invalid — The FortiWeb-VM appliance license either was not valid, or is currently a trial license. <p>To upload a purchased license, click Update. This appears only in FortiWeb-VM.</p>
Registration	<p>Indicates which account registered this appliance with Fortinet Technical Support. Possible states are:</p> <ul style="list-style-type: none"> • Unregistered — Not registered with Fortinet Technical Support. • <registration_email> — Registered with Fortinet Technical Support. <p>To manage technical support or FortiGuard service contracts for this device, go to the Fortinet Technical Support website.</p>

If logging is enabled, this log message will be recorded in the event log:

```
License status changed to VALID
```

If you are still connected to the CLI when license authentication succeeds, it should print this message:

```
*ATTENTION*: license registration status changed to 'VALID',please logout and re-login
```

If FortiWeb was also able to contact FortiGuard, its **FortiWeb Update Service** row should also indicate that the FortiGuard service contract is valid. (This second license validation may occur a minute or two after the first, and so may not appear immediately.)

If there was a connectivity interruption, you can either wait up to 30 minutes for the next license query, reboot, or enter the CLI command:

```
exec update-now
```



This command also contacts FortiGuard for FortiWeb Security Service contract validation and update availability.

If the connection did **not** succeed:

- On FortiWeb, verify the:
 - time zone & time
 - DNS settings
 - network interface up/down status & IP
 - static routes
- On your computer, use `nslookup` to verify that FortiGuard domain names are resolving (VM license queries are sent to `update.fortiguard.net`).

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

```
Non-authoritative answer:
Name: fds1.fortinet.com
Addresses: 209.66.81.150
209.66.81.151
208.91.112.66
Aliases: update.fortiguard.net
```

- On FortiWeb, use `execute ping` and `execute traceroute` to verify that connectivity from FortiWeb to the Internet and FortiGuard is possible. Check the configuration of any NAT or firewall devices that exist between the FortiWeb appliance and the FDN or FDS server override.

```
FortiWeb # exec traceroute update.fortiguard.net
traceroute to update.fortiguard.net (209.66.81.150), 32 hops max, 84 byte packets
 1 192.0.2.2 0 ms 0 ms 0 ms
 2 209.87.254.221 <static-209-87-254-221.storm.ca> 4 ms 2 ms 3 ms
 3 209.87.239.161 <core-2-g0-3.storm.ca> 2 ms 3 ms 3 ms
 4 67.69.228.161 3 ms 4 ms 3 ms
 5 64.230.164.17 <core2-ottawa23_POS13-1-0.net.bell.ca> 3 ms 5 ms 3 ms
 6 64.230.99.250 <tcore4-ottawa23_0-4-2-0.net.bell.ca> 16 ms 17 ms 15 ms
 7 64.230.79.222 <tcore3-montreal01_pos0-14-0-0.net.bell.ca> 14 ms 14 ms 15 ms
 8 64.230.187.238 <newcore2-newyork83_so6-0-0_0> 63 ms 15 ms 14 ms
 9 64.230.187.42 <bxX5-newyork83_POS9-0-0.net.bell.ca> 21 ms 64.230.187.93 <BX5-NEWYORK83_POS12-0-0_core.net.bell.ca> 17 ms 16 ms
10 67.69.246.78 <Abovenet_NY.net.bell.ca> 28 ms 28 ms 28 ms
11 64.125.21.86 <xe-1-3-0.cr2.lga5.us.above.net> 29 ms 29 ms 30 ms
12 64.125.27.33 <xe-0-2-0.cr2.ord2.us.above.net> 31 ms 31 ms 33 ms
13 64.125.25.6 <xe-4-1-0.cr2.sjc2.us.above.net> 82 ms 82 ms 100 ms
14 64.125.26.202 <xe-1-1-0.er2.sjc2.us.above.net> 80 ms 79 ms 82 ms
15 209.66.64.93 <209.66.64.93.t01015-01.above.net> 80 ms 80 ms 79 ms
16 209.66.81.150 <209.66.81.150.available.above.net> 83 ms 82 ms 81 ms
```

If after 4 hours FortiWeb still cannot validate its license, a warning message will be printed to the local console:

```
*WARNING*: Unable to validate license for over 4 hours
```

12. Continue with [What's next?](#).

To upload the license via the CLI

1. Using an SSH client, log in to the CLI using the IP address of the network interface you configured earlier. For example, if you configured `port1` with the IP address `192.168.1.1`, connect to `192.168.1.1` on port 22.

For details, see [Configuring access to FortiWeb's web UI & CLI on page 33](#).

2. Enter the following command:

```
execute restore vmlicense {ftp | tftp} <license-file_str> {<ftp_ipv4> | <user_str>:<password_str>@<ftp_ipv4> | <tftp_ipv4>}
```

where:

{ftp | tftp} specifies whether to connect to the server using file transfer protocol (FTP) or trivial file transfer protocol (TFTP).

<license-file_str> is the name of the license file.

{<ftp_ip4> is the IP address of the FTP server.

<user_str> is the user name that FortiWeb uses to authenticate with the server.

<password_str> is the password for the account specified by <user_str>.

<tftp_ip4> is the IP address of the TFTP server.

3. Confirm that you want to perform the license upload.

After the license is authenticated successfully, the following message is displayed:

```
"*ATTENTION*: license registration status changed to 'VALID', please logout and re-
login"
```

For information on troubleshooting a license upload, see [To upload the license via the web UI on page 36](#).

4. Continue with [What's next?](#).

Updating the license for more vCPUs

If either:

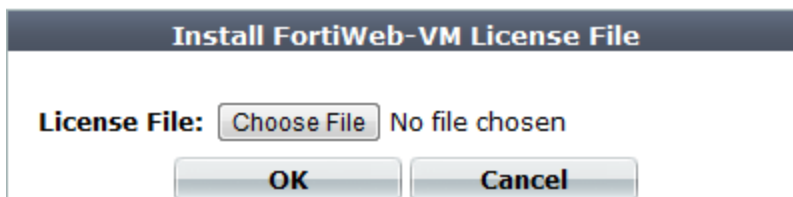
- you want to upgrade FortiWeb-VM to a license with a higher vCPU limit
- your original FortiWeb-VM license was an extended (but temporary) evaluation license, and you have now purchased a permanent, paid license

you must upload a new license file.

To replace an evaluation license with a paid license, use [Uploading the license on page 35](#).

To allocate more vCPUs

1. Log in to FortiWeb-VM as `admin` via the web UI.
2. Go to **System > Status > Dashboard**.
3. Upload the new license. For details, see [Uploading the license on page 35](#).



4. In the **System Information** widget, click **Shut Down**.
The virtual appliance will flush its data to its virtual disk, and prepare to be powered off. If you skip this step and immediately power off FortiWeb-VM, you may lose buffered data.
5. On your management computer, start your central management client, connect and log in to the server that is currently hosting FortiWeb-VM.
6. In the pane on the left side, click the name of the virtual appliance, such as **FortiWeb-VM**.
7. Power off the virtual machine.
8. Increase the vCPU allocation. For details, see [Deploying FortiWeb-VM on OpenStack](#).

9. Power on the virtual appliance again.
FortiWeb-VM evaluates its current license and discovers that you have allocated an unsupported number of vCPUs, causing the current license to become invalid.
10. Log in to the web UI again. In the **License Information** widget, the maximum number of vCPUs allowed by your FortiWeb-VM license should now match the VMware setting.

System Information	
Host Name	FortiWeb [Change]
Serial Number	FVVM040000010871
Operation Mode	Reverse Proxy [Change]
HA Status	Standalone [Configure]
System Time	Mon Jan 13 13:23:38 2014 [Change]
Firmware Version	FortiWeb-VM 5.10,build0182,140107 [Update]
System Uptime	0 day(s) 5 hour(s) 45 min(s)
Administrative Domain	Disabled [Enable]

What's next?

At this point, the FortiWeb-VM virtual appliance is running, and it has received a license file, but its operating system is almost entirely unconfigured. Before you can use FortiWeb-VM, you must configure it.

Configure the FortiWeb-VM software using the [FortiWeb Administration Guide](#).

After you have completed this first-time setup, you can refer to the [FortiWeb Administration Guide](#) and/or [FortiWeb CLI Reference](#). Updates, reconfiguration, and ongoing use of both FortiWeb-VM virtual appliances and physical appliance models such as FortiWeb-3000C are the same.