FortiWeb-VM on Xen Project

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

NSE 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

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

Deploying FortiWeb-VM on Open Xen 18

Bridging to one of the Xen server’s physical network interfaces 18

Configuring the vNetwork for the transparent modes 19

Creating the VM instance’s logical volume 20

Deploying via Virtual Machine Manager 21

Deploying via dom0 command line 26

Configuring access to FortiWeb’s web UI & CLI 33

Uploading the license 36

License Validation 36

Uploading the license 37

Updating the license for more vCPUs 42

What’s next? 44

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 reduces 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.

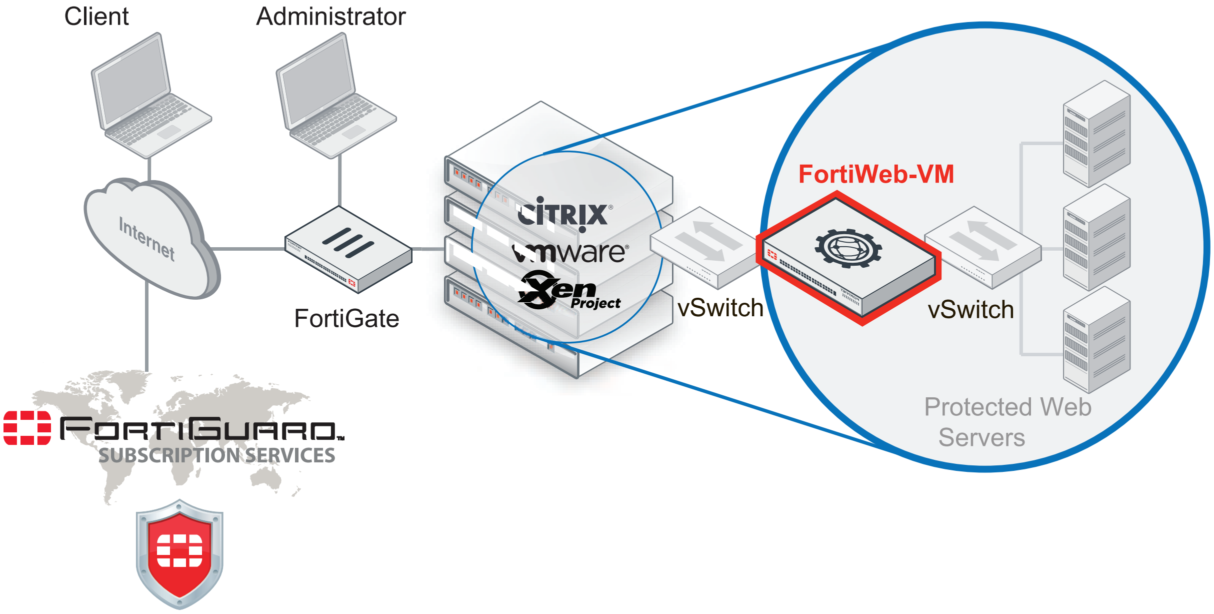
FortiWeb significantly reduces deployment costs by consolidating WAF, hardware acceleration, load balancing, and vulnerability scanning into a single device with no per-user pricing. Those features drastically reduce the time required to protect your regulated, Internet-facing data and eases the challenges 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 36.

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 evaulate 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 Open Xen 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	`config system dns`
	`set primary <address_ipv4>`
	`end`

CLI output	`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`

Emphasis	HTTP connections are **not** secure and can be intercepted by a third party.
File content	<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD><BODY><H4>You must authenticate to use this service.</H4></BODY></HTML>

Convention	Example
Hyperlink	https://support.fortinet.com
Keyboard entry	Type the IP address or domain name of an NTP server or pool, such as `pool.ntp.org`.
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 [ ]	A non-required (optional) word or words. For example:
	`[verbose {1 | 2 | 3}]`
	indicates that you may either omit or type both the `verbose` word and its accompanying option, such as:
	`verbose 3`

Curly braces { }	A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces. You must enter at least one of the options, unless the set of options is surrounded by square brackets [ ].
Options delimited by vertical bars |	Mutually exclusive options. For example: `{enable | disable}` indicates that you must enter either `enable` or `disable`, but must not enter both.

Options delimited by spaces	Non-mutually exclusive options. For example:
	`{http https ping snmp ssh telnet}`
	indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as:
	`ping https ssh`

	Note: To change the options, you must re-type the entire list. For example, to add `snmp` to the previous example, you would type:

Convention	Description
	`ping https snmp ssh` 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.
Angle brackets < >	A word constrained by data type. To define acceptable input, the angled brackets contain a descriptive name followed by an underscore (_) and suffix that indicates the valid data type. For example: `<retries_int>` indicates that you should enter a number of retries, such as `5`. Data types include: • `<xxx_name>` — A name referring to another part of the configuration, such as `policy_A`. • `<xxx_index>` — An index number referring to another part of the configuration, such as `0` for the first static route.
	• `<xxx_pattern>` — A regular expression or word with wild cards that matches possible variations, such as `*@example.com` to match all e-mail addresses ending in `@example.com`. • `<xxx_fqdn>` — A fully qualified domain name (FQDN), such as `mail.example.com`. • `<xxx_email>` — An email address, such as `admin@mail.example.com`. • `<xxx_url>` — A uniform resource locator (URL) and its associated protocol and host name prefix, which together form a uniform resource identifier (URI), such as `http://www.fortinet.com/`. • `<xxx_ipv4>` — An IPv4 address, such as `192.168.1.99`.
	• `<xxx_v4mask>` — A dotted decimal IPv4 netmask, such as `255.255.255.0`. • `<xxx_ipv4mask>` — A dotted decimal IPv4 address and netmask separated by a space, such as `192.168.1.99 255.255.255.0`. • `<xxx_ipv4/mask>` — A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as such as `192.168.1.99/24`. • `<xxx_ipv6>` — A colon(:)-delimited hexadecimal IPv6 address, such as `3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234`. • `<xxx_v6mask>` — An IPv6 netmask, such as `/96`. • `<xxx_ipv6mask>` — An IPv6 address and netmask separated by a space.
	• `<xxx_str>` — A string of characters that is **not** another data type, such as `P@ssw0rd`. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences. See the *FortiWeb CLI Reference*.

Convention	Description
	- `<xxx_int>` — 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:

- Open source Xen (Hypervisor) 4.0.1, 4.1, 4.2, 4.4

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.

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 this guide. For example, see Deploying -VM on VMware vSphere on page 1.

Deploying FortiWeb-VM on Open Xen

FortiWeb-VM is deployed as a fully virtualized `domU` virtual machine.

To deploy FortiWeb-VM on an open source Xen hypervisor/XAPI cloud, you can use either the `dom0` virtual machine's:

- command line or
- desktop environment, such as GNOME or KDE

Once FortiWeb-VM is deployed, however, either your Xen server itself or your management computer **must** have a desktop environment. (`sudo xm console <domain_int>` using an alias to `/dev/pty` does not succeed. Instead, VNC is required to connect to FortiWeb-VM's virtual local console in Configuring access to FortiWeb's web UI & CLI on page 33.)

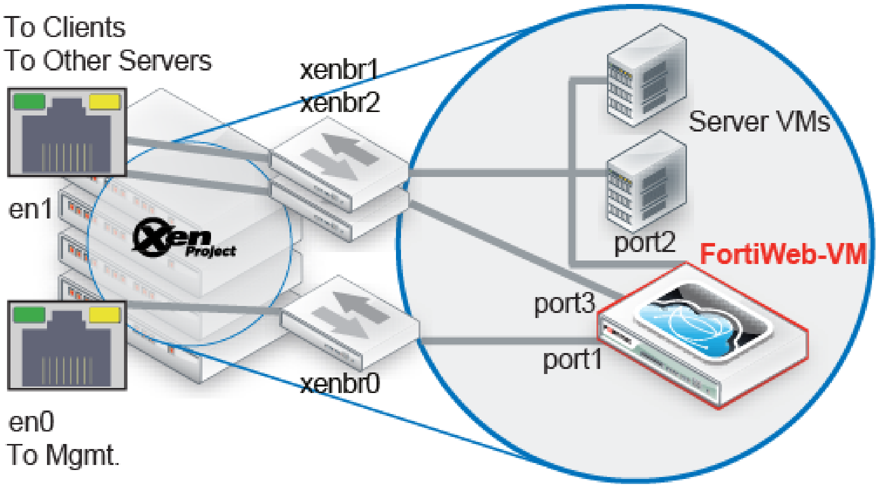
Bridging to one of the Xen server's physical network interfaces

If you have not yet installed the network bridge utilities required by Xen in order to bridge virtual machines' vNICs to the hypervisor's network connection, you must do that by installing the bridge network utilities and then editing the network interface configuration.

```
sudo apt-get install bridge-utils
sudo nano /etc/network/interfaces
```

When editing the network interface configuration, usually you should bind the bridge (in the `vif` example in Deploying via Virtual Machine Manager on page 21 or Deploying via dom0 command line on page 26, the bridge is `xenbr0`) to one of your network interfaces (e.g. `eth0`) in `/etc/network/interfaces`. Depending on the number of physical interfaces on the server and how you will map them to vNetworks, you may need to create multiple bridges.

The following table provides an example of how vNICs could be mapped to the physical network ports on a server with two physical NICs for a FortiWeb operating in reverse proxy mode.



Example: Network mapping for Reverse Proxy mode

Xen Project			FortiWeb-VM
Physical Network Adapter	**Network Mapping (vSwitch Port Group)**	**Virtual Network Adapter for FortiWeb-VM**	**Network Interface Name in Web UI/CLI**
eth0	xenbr0	Management	port1
eth1		External	port2
		Internal	port3
		External	port4

Below is a configuration example assuming the server has only one physical NIC, `eth0`:

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet manual

auto xenbr0
iface xenbr0 inet static
address 192.0.2.10
netmask 255.255.255.0
gateway 192.0.2.1
#Enable line below for vSwitch with FortiWeb transparent mode
#allow-hotplug xenbr0
```

Configuring the vNetwork for the transparent modes

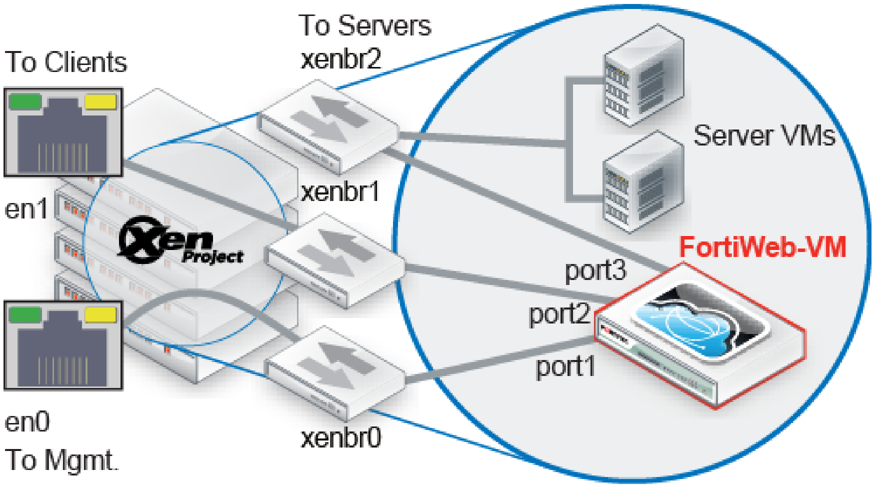
A simple Xen bridge configuration does **not** function with FortiWeb bridges (V-zones), which will be used if you deploy your FortiWeb-VM in either true transparent proxy or Transparent Inspection operation mode.

For information on how to choose the operation mode, see the setup instructions in the *FortiWeb Administration Guide*.

Use the following general configuration steps to support the transparent modes:

- To create the bridge, use one of the following to create two FortiWeb ports: one for the web server side and one for the client side:
  - 2 vSwitches or distributed vSwitches (dvSwitch)
  - 1 vSwitch that has 2 port groups with different VLAN IDs
- Set each vSwitch that you add to promiscuous mode and map each port group to a network adapter (vNIC) in the vNIC configuration (see Deploying via Virtual Machine Manager on page 21 or Deploying via dom0 command line on page 26)

Similar to a deployment that does not use virtual machines, connections between clients and servers are piped through two port groups (on two vSwitches or a single vSwitch) that comprise the bridge, with FortiWeb-VM in between them.



For instructions on how to create distributed vSwitches, see:

http://wiki.xen.org/wiki/Xen_Networking#Open_vSwitch

Creating the VM instance’s logical volume

You must create the logical volume that FortiWeb-VM will use to store its vDisks. In this case, the logical volume is on the Xen server’s local disk, but usually it is preferable to store it on an NFS or CIFS share.

To create a local logical volume

1. Connect to the command line in `dom0` on the Xen server where you will deploy FortiWeb-VM (for example, via an SSH client such as PuTTY).
2. Find the name of your `dom0` logical volume group. (Volume group is highlighted below in bold).
```
xenuser@LabXen:~$ sudo pvs
[sudo] password for xenuser:
PV VG Fmt Attr PSize PFree
/dev/sda5 LabXen-vg lvm2 a- 698.39g 673.45g
```
3. Create a logical volume. In this case, the logical volume is on the Xen server’s local disk, but you could store it on an NFS or CIFS share.
```
sudo lvcreate -L 100G -n fortiweb-vm /dev/LabXen-vg
```

   where you would replace:

   - `100G` — The amount of disk space to allocate to FortiWeb-VM’s vDisk in gigabytes.
   - `fortiweb-vm` — The name of your virtual machine, as it appears in Virtual Machine Manager or when you use the `xm` command to create the virtual machine.
   - `LabXen-vg` — The name of your `dom0` volume group according to the output of the `sudo pvs` command.

Deploying via Virtual Machine Manager

If you have not yet installed a graphical centralized management tool for Xen on your management computer, begin by installing it. Multiple clients exist for managing Xen Project servers. In these instructions, we use Virtual Machine Manager.

On Debian-related Linux distributions, to install Virtual Machine Manager, open a terminal and enter:

```
sudo apt-get install virt-manager
```

On Red Hat-related Linux distributions, the command is :

```
sudo yum virt-manager
```

This centralized manager includes a Xen client for connecting to a remote Xen Project hypervisor to deploy FortiWeb-VM. It also includes a built-in VNC client that you will need later in order to connect to FortiWeb-VM’s local console and configure its network connection. When the download and installation is complete, if you are not already logged into your desktop environment (GNOME, KDE, xfce, etc.), start X Windows and log in.

To enable Virtual Machine Manager to connect to your Xen server, you must also modify the **server’s** configuration file (usually `/etc/xen/xend-config.sxp`). Un-comment these lines (remove the hash (`#`) from the beginning) and change ‘`no`’ to ‘`yes`’:

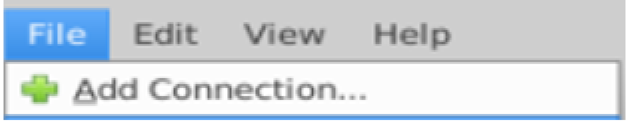
```
(xend-unix-server yes)
(xend-unix-path /var/lib/xend/xend-socket)
```

To deploy the VM image using Virtual Machine Manager

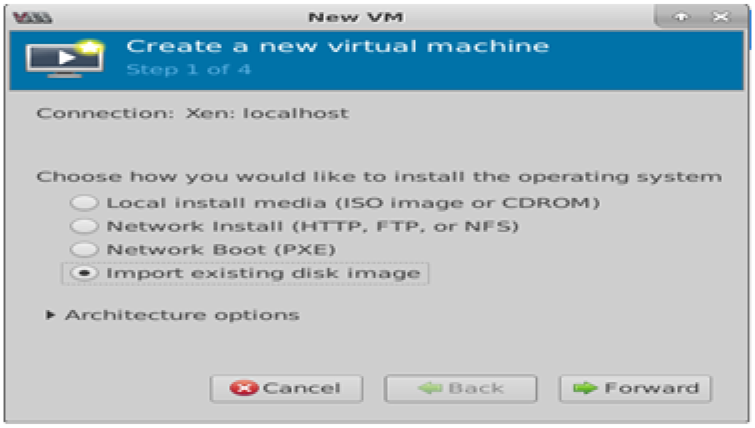
1. On your management computer, open a terminal application and enter the command to extract the package to a folder, then start Virtual Machine Manager:

   ```
   unzip FWB_XENOPEN-v500-build-0057-FORTINET.out.xenopensource.zip
   sudo virtu-manager
   ```

   The application will open in your desktop environment, so its appearance may vary slightly.
2. Go to **File > Add Connection** and connect to the Xen server where you will deploy the VM.



3. To open the wizard for a new virtual machine, Select **Import existing disk image**, then click **Forward**.



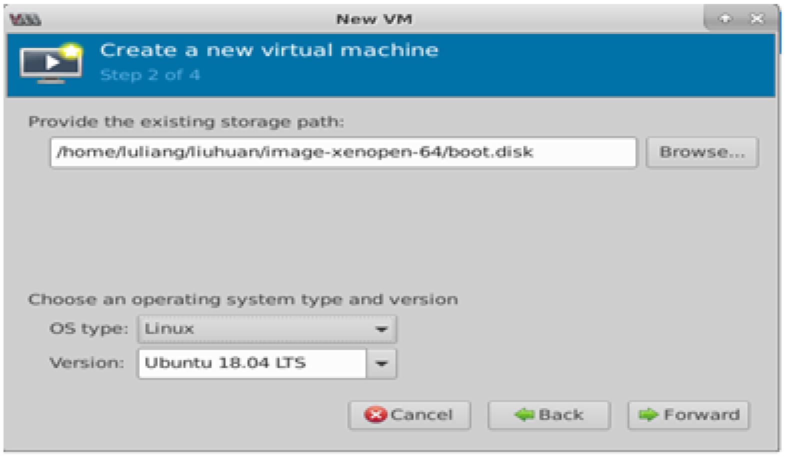
Create a new virtual machine
Step 1 of 4

Connection: Xen: localhost

Choose how you would like to install the operating system
○ Local install media (ISO image or CDROM)
○ Network Install (HTTP, FTP, or NFS)
○ Network Boot (PXE)
● Import existing disk image

▸ Architecture options

4. Click **Browse** and locate the boot.disk file from your local folder. Select the OS type and version of your environment. Click **Forward**.



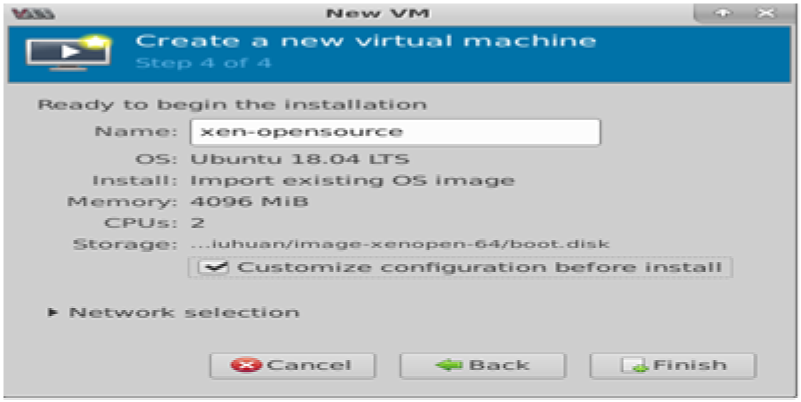
Create a new virtual machine
Step 2 of 4

Provide the existing storage path:
/home/luliang/liuhuan/image-xenopen-64/boot.disk

Choose an operating system type and version
OS type: Linux
Version: Ubuntu 18.04 LTS

5. Adjust the vRAM and vCPU settings as desired. To ensure high performance, it's recommended to configure at least 2 vCPUs, and 8 GB RAM. Click **Forward**.

6. Enter a name for the FortiWeb-VM instance. It will appear in Virtual Machine Manager's inventory. Check **Customize configure before install**. Click **Finish**.

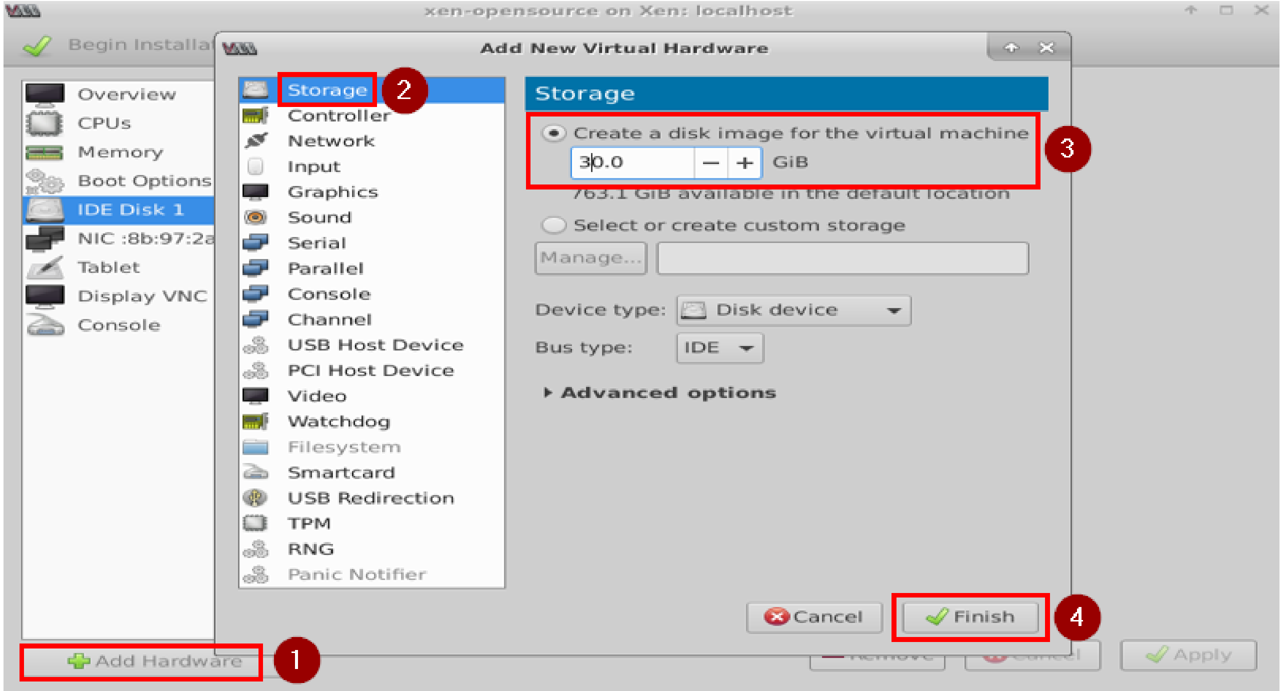


Create a new virtual machine
Step 4 of 4

Ready to begin the installation
Name: xen-opensource
OS: Ubuntu 18.04 LTS
Install: Import existing OS image
Memory: 4096 MiB
CPUs: 2
Storage: ...iuhuan/image-xenopen-64/boot.disk
☑ Customize configuration before install

▸ Network selection

7. Click **Add Hardware**, then select **Storage**. Configure 30 GB or larger for the disk image. This disk will be used to store logs generated by FortiWeb. Disk images less than 30 GB will cause the deployment to fail. Click **Finish**.



Storage

● Create a disk image for the virtual machine

30.0 GiB

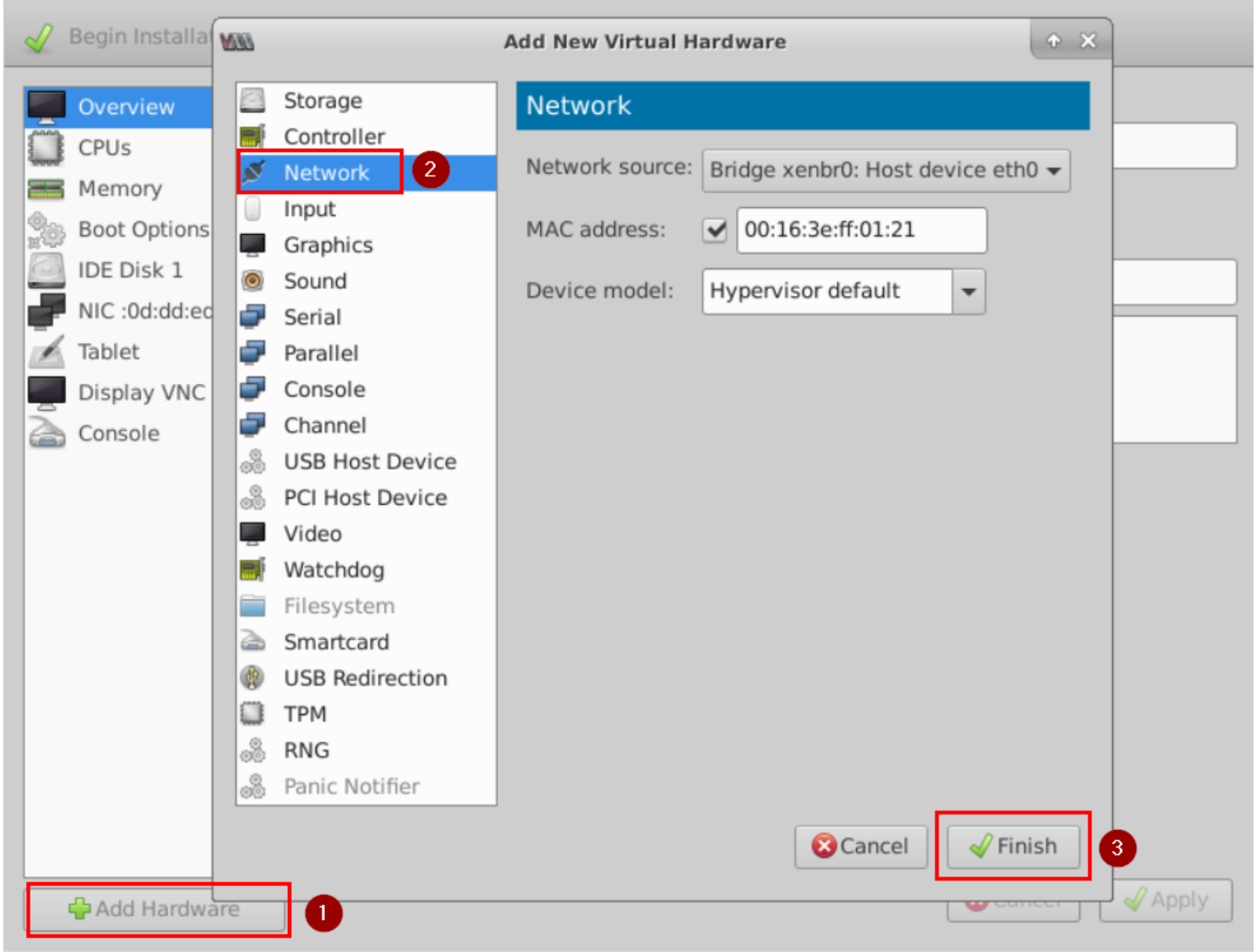
763.1 GiB available in the default location

○ Select or create custom storage

Device type: Disk device

Bus type: IDE

8. Click **Add Hardware**, then select **Network** to add another virtual network adapter that is bound to the bridge. Leave the options with their default values, then click **Finish**.



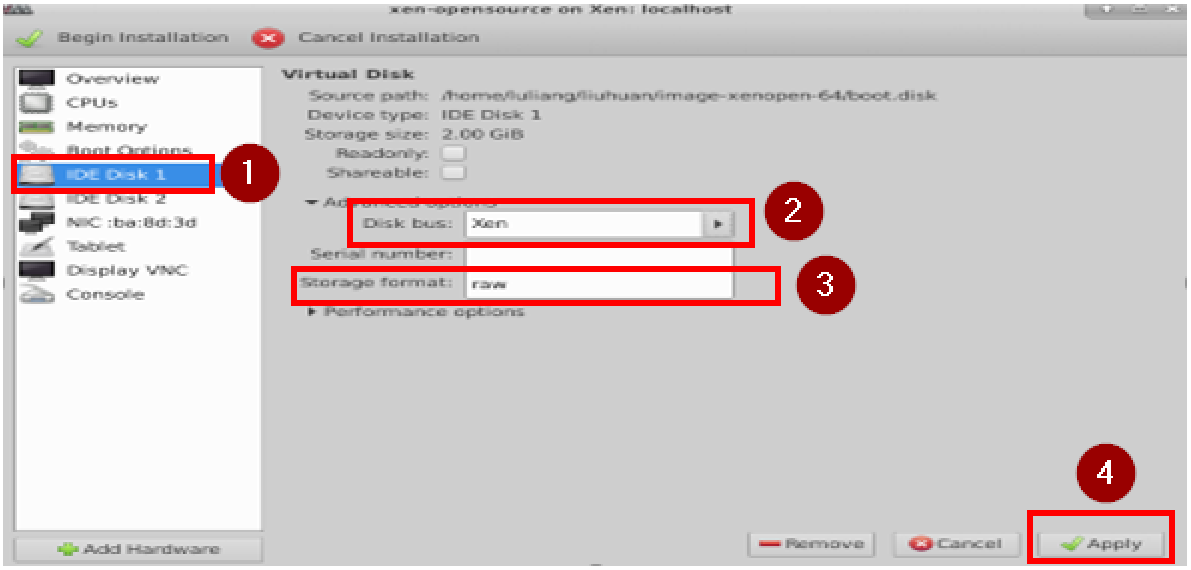
Network

Network source: Bridge xenbr0: Host device eth0

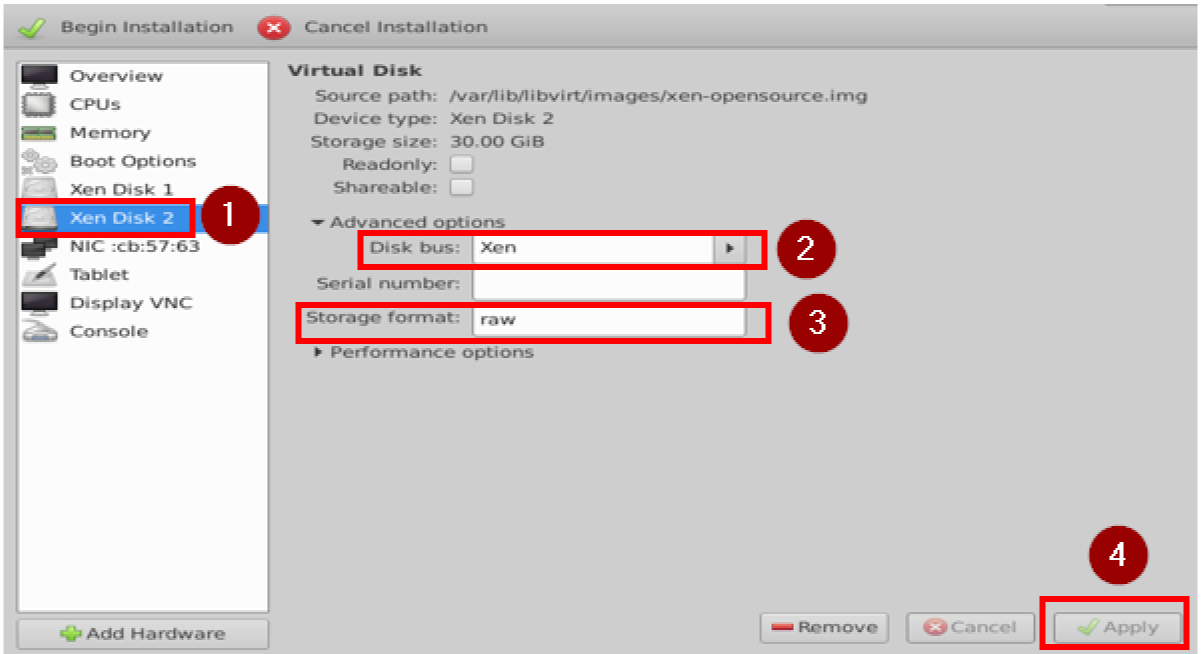
MAC address: ☑ 00:16:3e:ff:01:21

Device model: Hypervisor default

9. Choose **IDE Disk1** and **IDE Disk2**, modify their **Disk bus** type to **Xen**, and **Storage format** to **raw**. Click **Apply**.



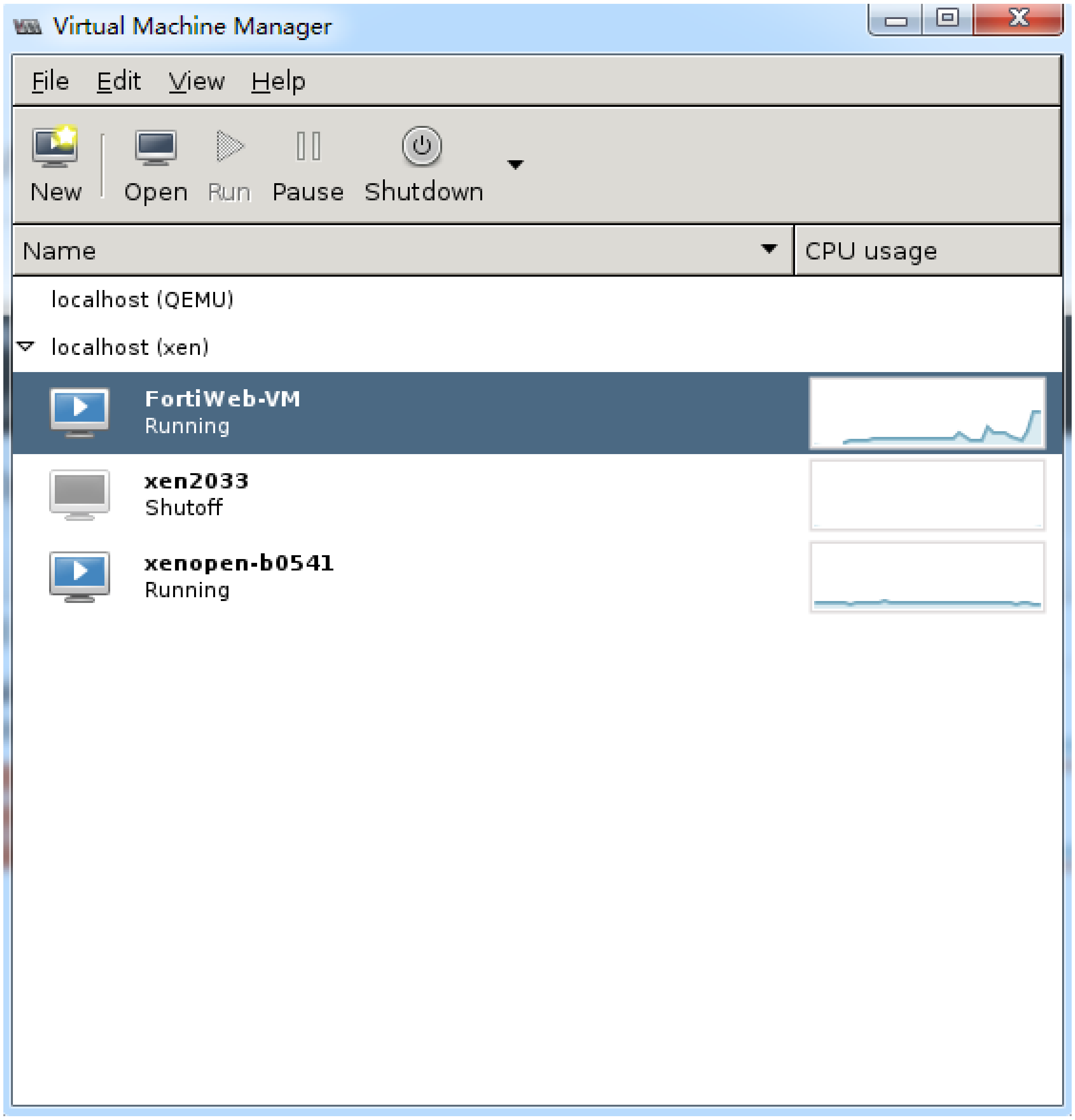
Virtual Disk
Source path: /home/luliang/liuhuan/image-xenopen-64/boot.disk
Device type: IDE Disk 1
Storage size: 2.00 GiB
Readonly: □
Shareable: □
Disk bus: Xen
Serial number:
Storage format: raw



Virtual Disk
Source path: /var/lib/libvirt/images/xen-opensource.img
Device type: Xen Disk 2
Storage size: 30.00 GiB
Readonly: □
Shareable: □
Disk bus: Xen
Serial number:
Storage format: raw

10. For other tabs on the left menu such as Display VNC and boot options, leave them as is.
11. Click **Begin installation** to send the FortiWeb-VM image and its VM settings to the Xen server.
    The client connects to the VM environment, and deploys the image to it. Time required depends on your computer's hardware speed and resource load, and also on the file size and speed of the network connection, but might take 15 minutes to complete.

    When complete, the deployment should appear in the list of deployed VMs for that Xen server, in the pane on the left side of Virtual Machine Manager.
12. To power on the VM, click the **Play** button.



localhost (QEMU)

localhost (xen)

FortiWeb-VM
Running

xen2033
Shutoff

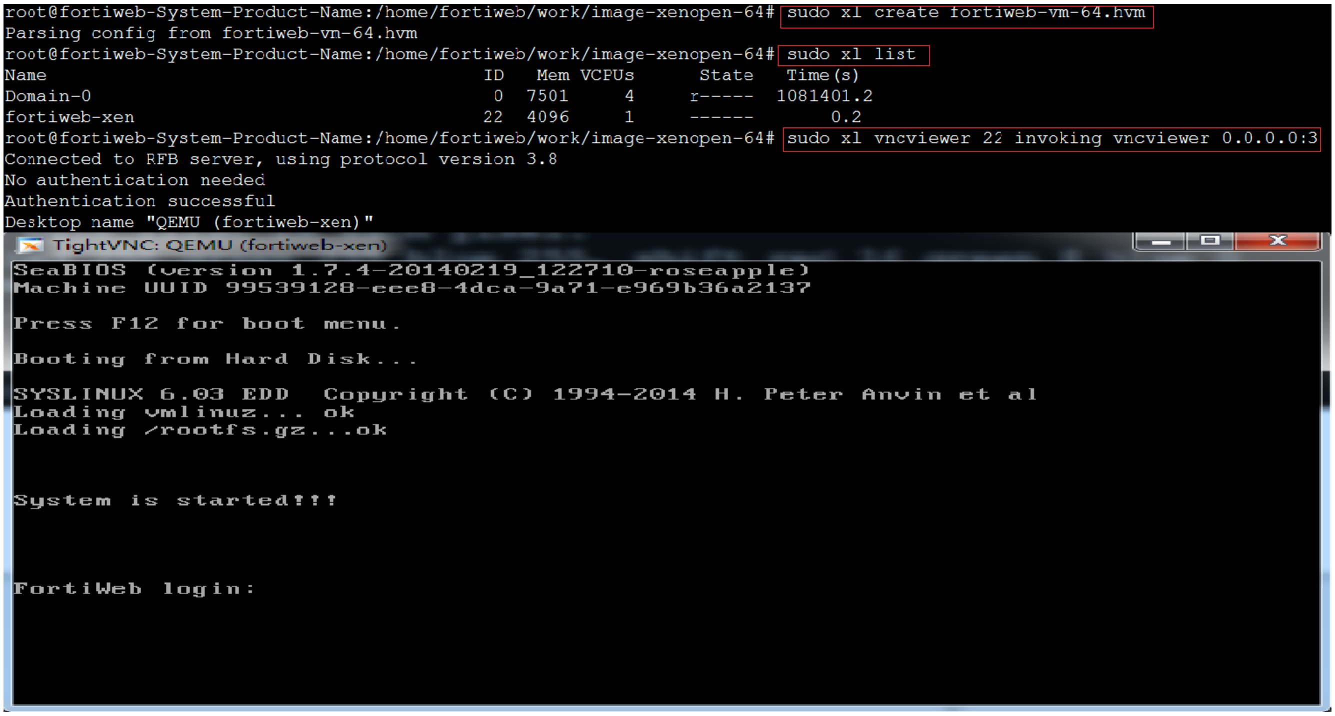
xenopen-b0541
Running

13. Continue with Configuring access to FortiWeb's web UI & CLI on page 33.

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.

Deploying via dom0 command line

Connect to the command line of your `dom0` guest. For example, you may be able to use PuTTY to make an SSH connection to the Xen server's IP address, or you may use a local GNOME Terminal application.



```
root@fortiweb-System-Product-Name:/home/fortiweb/work/image-xenopen-64# sudo xl create fortiweb-vm-64.hvm
Parsing config from fortiweb-vn-64.hvm
root@fortiweb-System-Product-Name:/home/fortiweb/work/image-xenopen-64# sudo xl list
Name                                        ID   Mem VCPUs      State   Time(s)
Domain-0                                     0  7501     4     r-----  1081401.2
fortiweb-xen                                22  4096     1     ------        0.2
root@fortiweb-System-Product-Name:/home/fortiweb/work/image-xenopen-64# sudo xl vncviewer 22 invoking vncviewer 0.0.0.0:3
Connected to RFB server, using protocol version 3.8
No authentication needed
Authentication successful
Desktop name "QEMU (fortiweb-xen)"
```

```
SeaBIOS (version 1.7.4-20140219_122710-roseapple)
Machine UUID 99539128-eee8-4dca-9a71-e969b36a2137

Press F12 for boot menu.

Booting from Hard Disk...

SYSLINUX 6.03 EDD  Copyright (C) 1994-2014 H. Peter Anvin et al
Loading vmlinuz... ok
Loading /rootfs.gz...ok


System is started!!!



FortiWeb login:
```

Next, unpack the file that you downloaded from Fortinet, and open the configuration file in a plain text editor such as `nano`.

```
unzip FWB_XENOPEN-v500-build-0057-FORTINET.out.xenopensource.zip
cd FWB_XENOPEN-v500-build-0057-FORTINET.out.xenopensource/
nano fortiweb.hvm
```

Then edit these lines in `fortiweb-vm-64.hvm`:

```
memory = 8192
vcpus = 2
vif = [ 'type=netfront, bridge=xenbr0', 'type=netfront, bridge=xenbr0', 'type=netfront,
     bridge=xenbr0', 'type=netfront, bridge=xenbr0', ]
disk = ["format=raw, vdev=xvda, access=rw, target=boot.disk", 'format=qcow2, vdev=xvdb,
     access=rw, target=log.qcow2']
```

If FortiWeb-VM will be running in transparent mode, the vNIC (`vif`) must be configured differently to include vSwitches and vNICs in promiscuous mode. For instructions, see:

http://wiki.xen.org/wiki/Xen_Networking#Open_vSwitch

For more information on network mappings, see Example: Network mapping for Reverse Proxy mode on page 19.

```
Alternatively to locally stored disk images, you can reference an NFS or CIFS share:
#Mount point on the server's local file system
root = "/dev/nfs"
nfs_server = '192.0.2.100'
#Root directory on the NFS server
nfs_root = '/path/to/directory'
```

Configure virtual hardware settings to allocate appropriate resources for the size of your deployment before powering on the virtual appliance. For details, see the documentation for the open source Xen Hypervisor.

Change the value if necessary to allocate enough vCPUs for the size of your deployment. Valid vCPU values range from 1 to 8, depending on your FortiWeb-VM license.

Similarly, FortiWeb-VM for Xen Project comes pre-configured to use 8 GB of vRAM (`memory`). However, this is not enough for most deployments. Change this value to be appropriate for your deployment. The valid range is from 8 GB to 16 GB.

If you configure the virtual appliance’s storage to be internal (that is, local, on its own vDisk), resize the vDisk before powering on. The FortiWeb-VM package that you downloaded includes presized VMDK (Virtual Machine Disk Format) files. However, they are only 32 GB, which is not large enough for most deployments. Resize the vDisk before powering on the virtual machine.

This step is not applicable if the virtual appliance will use external network file system (such as NFS or CIFS) datastores.

Depending on your Xen `dom0` platform, you may also need to reconfigure `fortiweb-vm-64.hvm` with the path to your `hvmloader`. For example, this may be correct for CentOS or Red Hat Linux:

```
kernel = "/usr/lib/xen/boot/hvmloader
```

but this is required by Ubuntu 12.0.4 LTS:

```
kernel = "/usr/lib/xen-4.1/boot/hvmloader
```

Apply the changes by rebooting or restarting networking. (In some cases rebooting is required: `sudo /etc/init.d/networking restart` may not delete your old IP address from `eth0` and therefore not correctly bring up all interfaces.)

Run these commands to deploy the VM, power it on, and show its Xen domain ID number (highlighted below in bold):

```
xenuser@LabXen:/$ sudo xm create fortiweb.hvm
xenuser@LabXen:/$ sudo xm list
Name ID Mem VCPUs State Time(s)
Domain-0 0 5877 4 r----- 1556.9
fortiweb-vm 2 2048 2 -b---- 126.8
```

If your `dom0` is Ubuntu 12.04 and/or when creating the VM, you receive this error:

```
Error: Domain ‘fortiweb-xen’ does not exist.
```

and if `/var/log/xen/qemu-dm-fortiweb-xen.log` contains this line:

```
Could not read keymap file: ‘/usr/share/qemu/keymaps/en-us’
```

then the key mapping is not in its expected location. Enter this line:

```
sudo ln -s /usr/share/qemu-linaro /usr/share/qemu
```

then retry the command to create FortiWeb-VM.

Since VNC listening port numbers are dynamically allocated to guest VMs, use the domain ID number in the output from the previous command to run this command to show the current VNC listening port number and IP address for FortiWeb-VM:

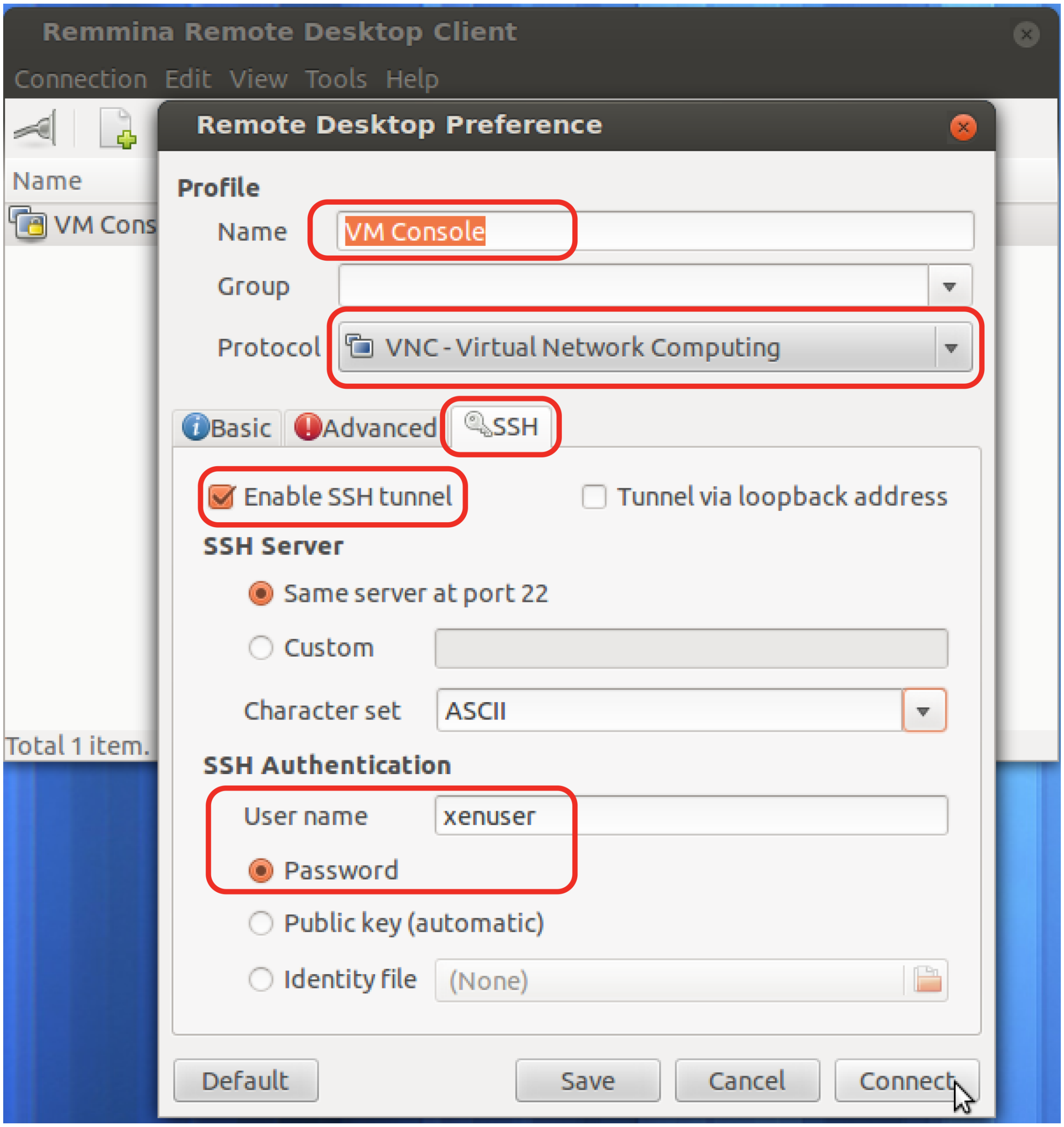
```
xenuser@LabXen:/$ sudo xenstore-ls /local/domain/2/console
```

```
port = "4"
limit = "1048576"
type = "ioemu"
vnc-port = "5900"
vnc-listen = "127.0.0.1"
tty = "/dev/pts/5"
```

Finally, on your management computer, install and start a VNC viewer and connect to the Xen server’s IP address and listening port number for VNC. (In the images below, the VNC viewer is installed in `dom0` on the Xen server that is hosting FortiWeb-VM, so the VNC viewer connects to 127.0.0.1. If connecting from your management computer, replace this with the IP address of your Xen server.) For example, on a Debian or Ubuntu Linux management computer, you could use these commands:

```
sudo apt-get install remmina
remmina
```

You **must** run this command from a terminal with an X Windows environment such as GNOME Terminal in order for it to be able to open the VNC viewer window.


Remmina Remote Desktop Client
Connection Edit View Tools Help
Name
VM Cons
Total 1 item.
Remote Desktop Preference
Basic
Advanced
SSH
Default
Save
Cancel
Connect

Profile

Name: VM Console

Group:

Protocol: VNC - Virtual Network Computing

☑ Enable SSH tunnel □ Tunnel via loopback address

SSH Server

● Same server at port 22

○ Custom

Character set: ASCII

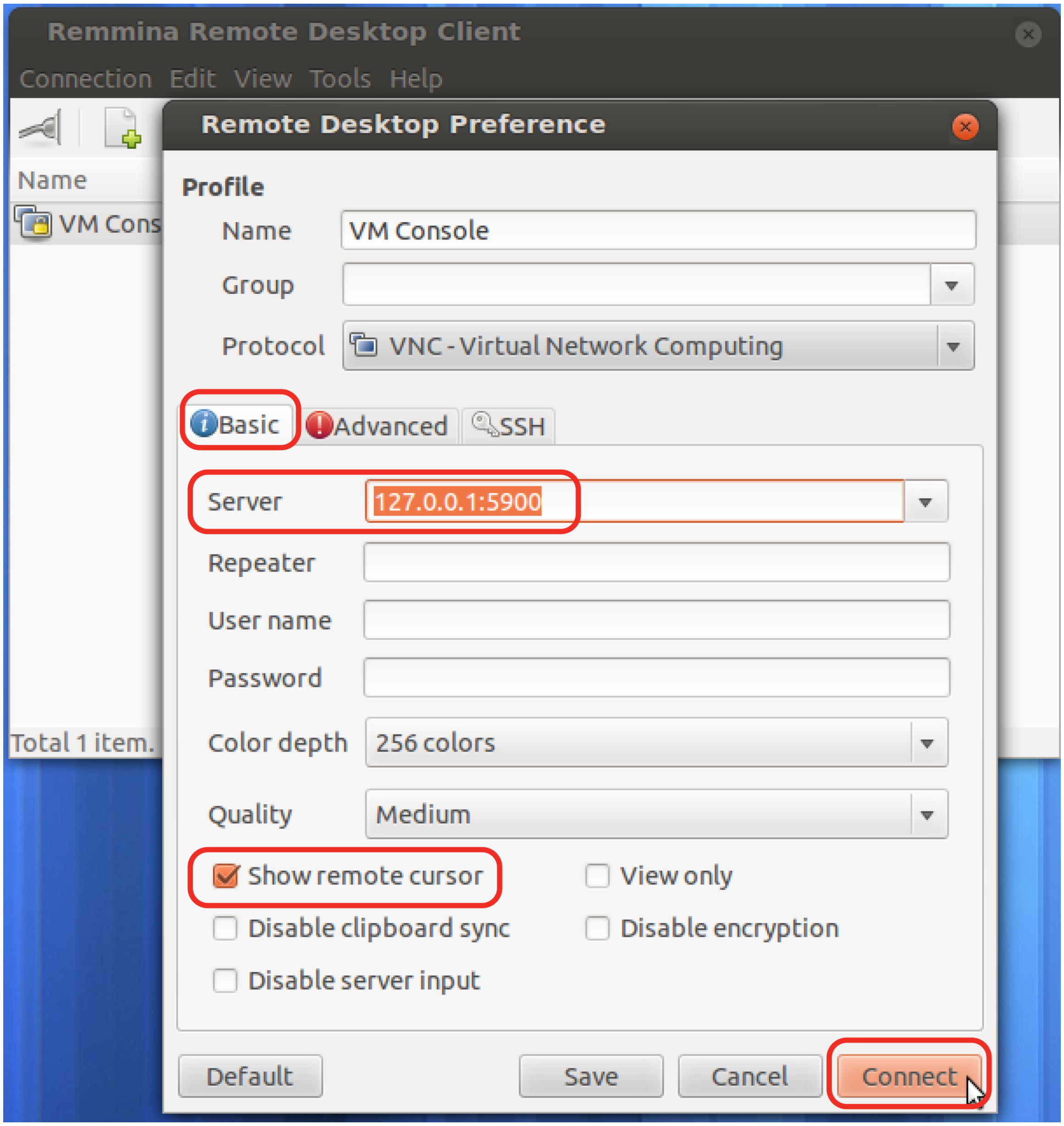
SSH Authentication

User name: xenuser

● Password

○ Public key (automatic)

○ Identity file (None)



Remmina Remote Desktop Client
Connection Edit View Tools Help
Name
VM Cons
Total 1 item.
Remote Desktop Preference

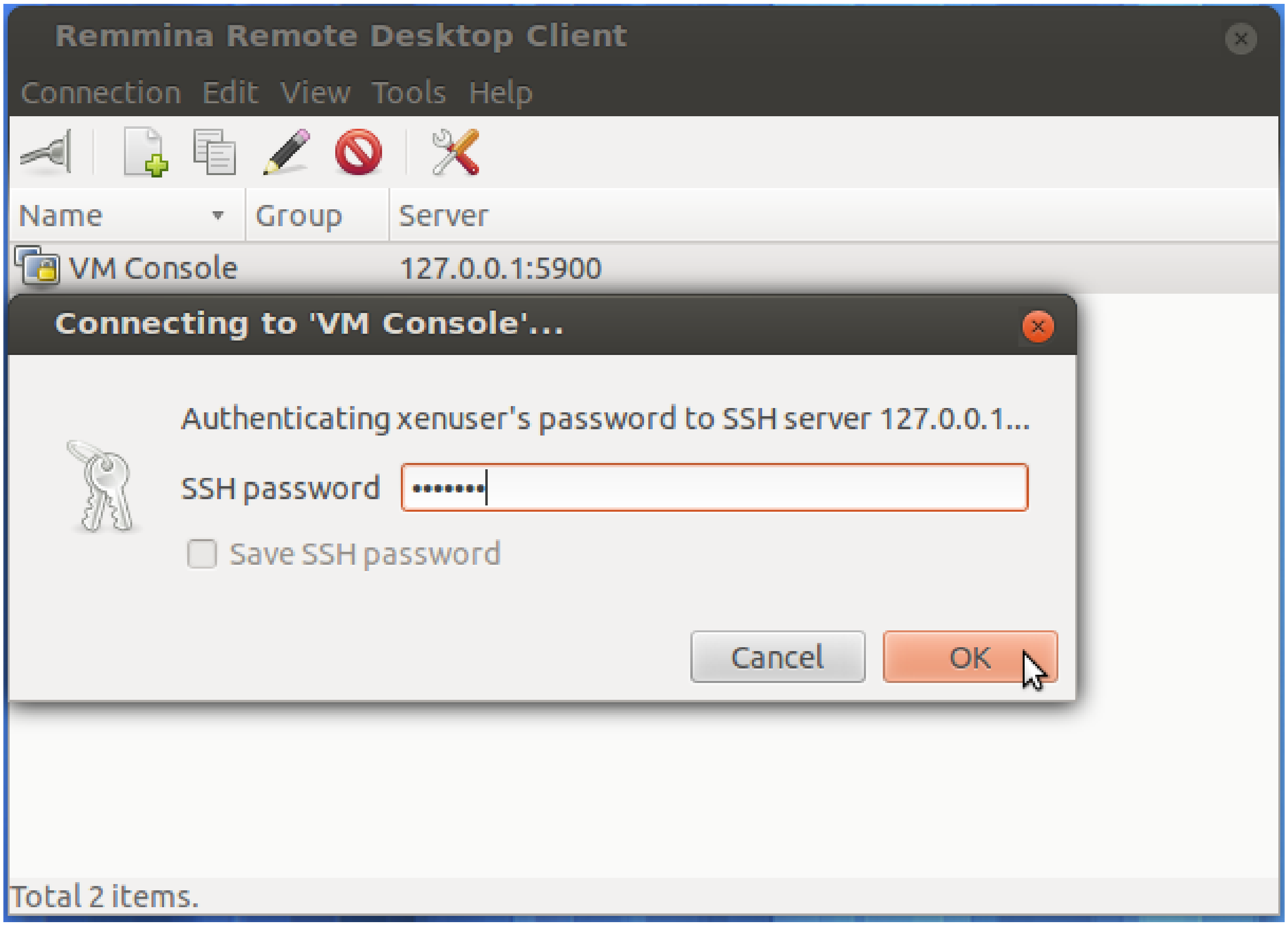
Profile

Name	VM Console
Group	
Protocol	VNC - Virtual Network Computing

Server	127.0.0.1:5900
Repeater	
User name	
Password	
Color depth	256 colors
Quality	Medium

☑ Show remote cursor
□ View only
□ Disable clipboard sync
□ Disable encryption
□ Disable server input

Default
Save
Cancel
Connect


Remmina Remote Desktop Client
Connection Edit View Tools Help
Name
Group
Server
VM Console
127.0.0.1:5900
Connecting to 'VM Console'...
Cancel
OK
Total 2 items.

Authenticating xenuser's password to SSH server 127.0.0.1...

SSH password ••••••••

□ Save SSH password

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.

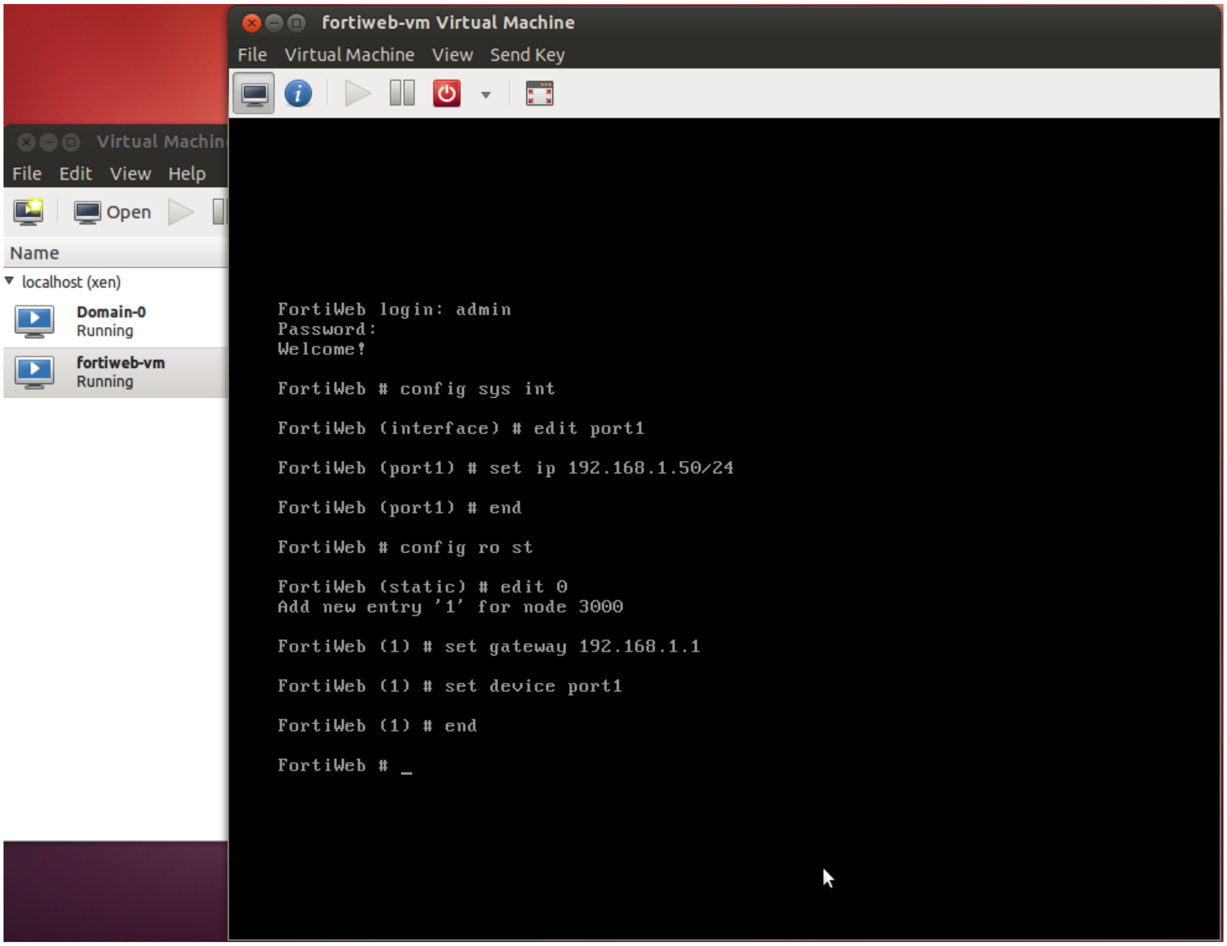
Continue with Configuring access to FortiWeb's web UI & CLI on page 33.

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.

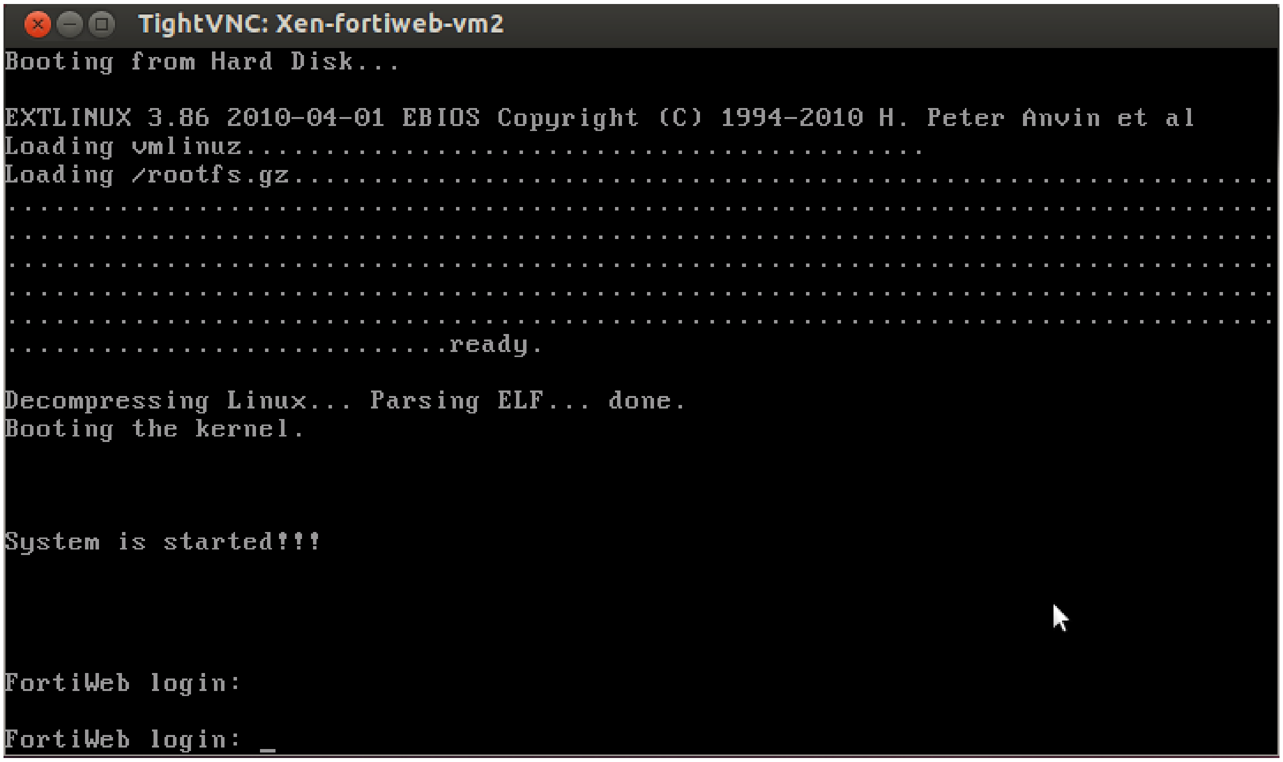
To configure basic network settings for FortiWeb-VM deployed on a hypervisor

1. On your management computer, start the following according to the VM environment in which you have deployed FortiWeb-VM:
   - Open Xen Virtual Machine Manager (`virt-manager`) or a VNC viewer
2. Log in to the VM server.
3. Open the console of the FortiWeb-VM virtual appliance.
   On Open Xen Virtual Machine Manager:
   - In the pane on the left side, select the name of the virtual appliance, such as **FortiWeb-VM**.
   - Click **Open**.
   - In the window that appears, click the monitor icon.



```
FortiWeb login: admin
Password:
Welcome!

FortiWeb # config sys int

FortiWeb (interface) # edit port1

FortiWeb (port1) # set ip 192.168.1.50/24

FortiWeb (port1) # end

FortiWeb # config ro st

FortiWeb (static) # edit 0
Add new entry '1' for node 3000

FortiWeb (1) # set gateway 192.168.1.1

FortiWeb (1) # set device port1

FortiWeb (1) # end

FortiWeb # _
```

On a VNC client, connect to the IP address of the Open Xen and the port number allocated to that instance of FortiWeb-VM.



```
Booting from Hard Disk...

EXTLINUX 3.86 2010-04-01 EBIOS Copyright (C) 1994-2010 H. Peter Anvin et al
Loading vmlinuz.................................
Loading /rootfs.gz...............................................................
.................................................................................
.................................................................................
.................................................................................
.................................................................................
.................................................................................
............................ready.

Decompressing Linux... Parsing ELF... done.
Booting the kernel.


System is started!!!



FortiWeb login:

FortiWeb login: _
```

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 36. 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 44.

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 36.

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://.)

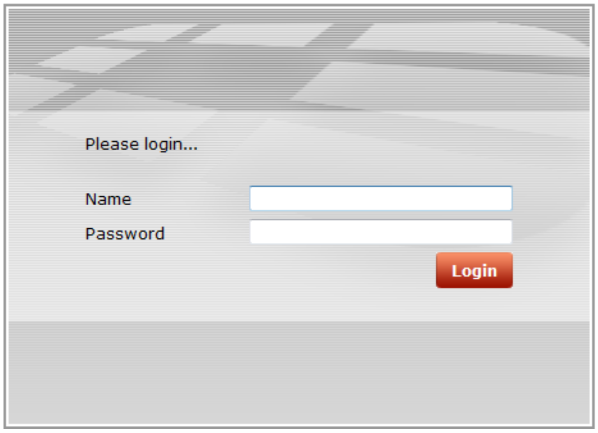
   Initially, you must access the web UI via HTTPS. By default, HTTP is not enabled. After uploading the license, you can configure the administrative access protocols. For details, see the *FortiWeb Administration Guide*.

   - 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.

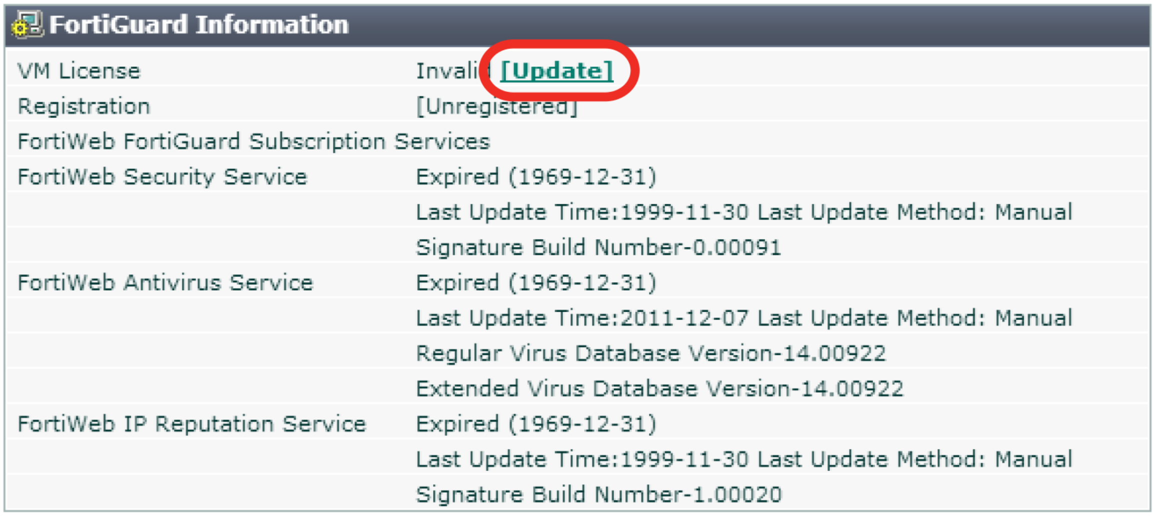
Both warnings are normal for the default certificate.

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.

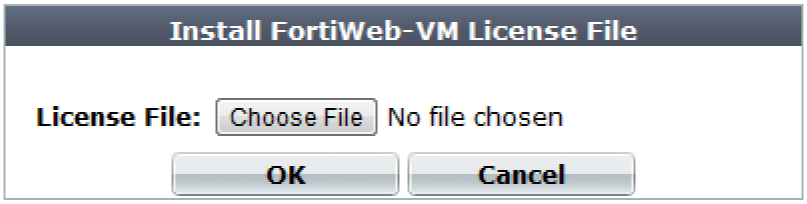
FortiGuard Information widget on System > Status > Status in the web UI before license upload



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

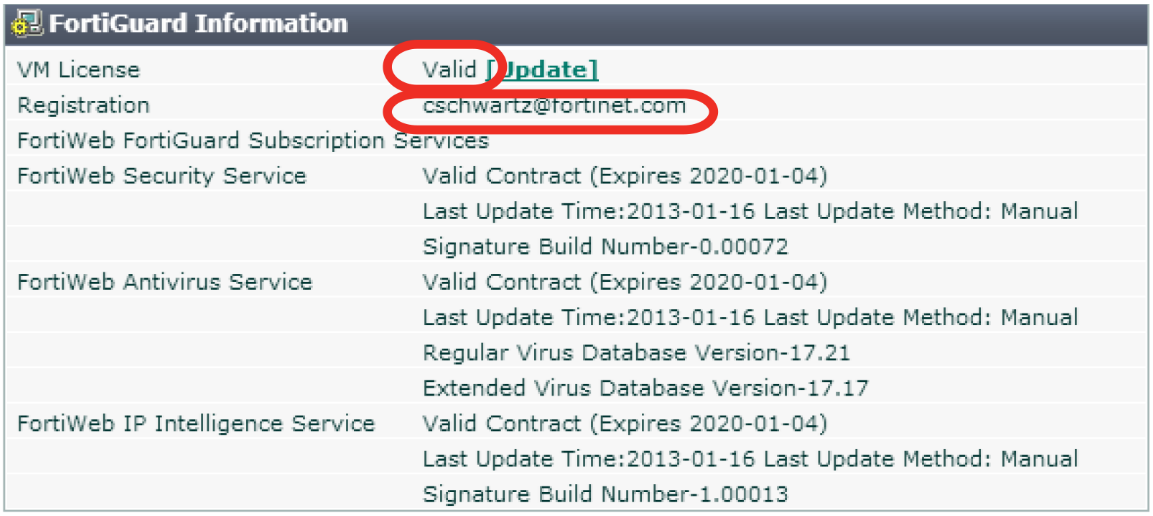
License File: Choose File No file chosen

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: • **Valid** — The appliance has a valid, non-trial license. **Serial**

GUI item	Description
	Number in the **System Information** widget indicates the maximum number of vCPUs that can be allocated according to this license. 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 42. • **Invalid** — The FortiWeb-VM appliance license either was **not** valid, **or** is currently a **trial** license. To upload a purchased license, click **Update**. This appears only in FortiWeb-VM.
Registration	Indicates which account registered this appliance with Fortinet Technical Support. Possible states are: • **Unregistered** — Not registered with Fortinet Technical Support. • **<registration_email>** — Registered with Fortinet Technical Support. To manage technical support or FortiGuard service contracts for this device, go to the Fortinet Technical Support website.

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_ipv4>` 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_ipv4>` 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 37.
4. Continue with What's next?.

Updating the license for more vCPUs

If either:

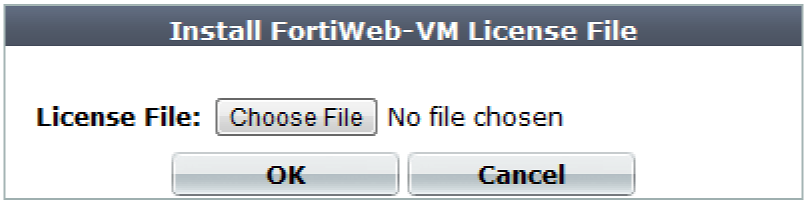
- you want to upgrade FortiWeb-VM to a license with a higher vCPU limit
- your original FortiWeb-VM license was an extended (but temporary) evaluation license, and you have now purchased a permanent, paid license

you must upload a new license file.

To replace an evaluation license with a paid license, use Uploading the license on page 36.

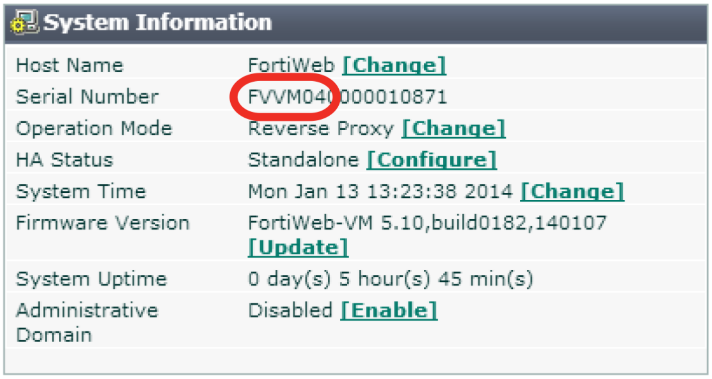
To allocate more vCPUs

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 36.



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.

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.