FortiWeb-VM Deployment Guide for VMware

Version 6.2.x

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/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

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

FEEDBACK
Email: techdoc@fortinet.com

TABLE OF CONTENTS

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. On hardware models with ASIC chips, cryptography is also hardware-accelerated.

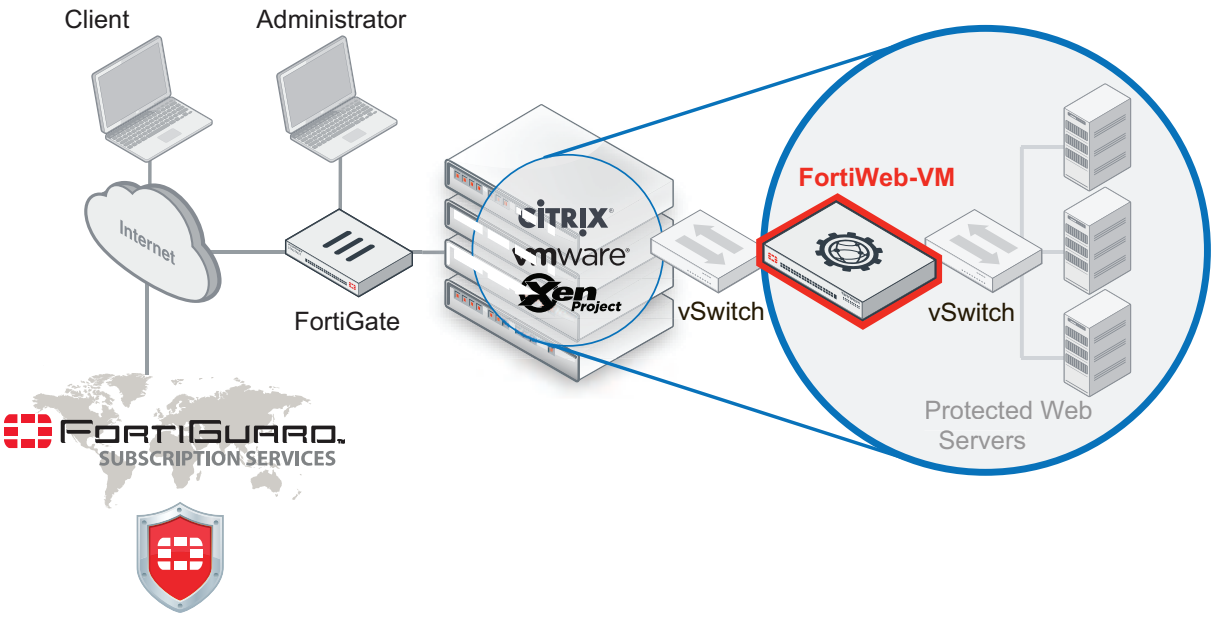
FortiWeb significantly reduces deployment costs by consolidating WAF, hardware acceleration, load balancing, and vulnerability scanning into a single device with no per-user pricing. Those features drastically reduce the time required to protect your regulated, Internet-facing data and eases the challenges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

Hypervisor deployments uses FortiWeb-VM licenses that 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.

FortiWeb-VM licenses are available at the sizing levels described in the table.

FortiWeb-VM resource limitations

	License/model			
	VM01	**VM02**	**VM04**	**VM08**
Virtual CPUs (vCPUs)	1	2	4	8

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 15.

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 58.

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 a VMware ESXi environment. To learn how to deploy FortiWeb-VM on public cloud platforms, see https://docs2.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:

- VMware vSphere Hypervisor ESX/ESXi 4.0/4.1/5.0/5.1/5.5/6.0/6.5/6.7

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 4 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 (currently only supported on Microsoft Hyper-V since FortiWeb 6.1.0), 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.

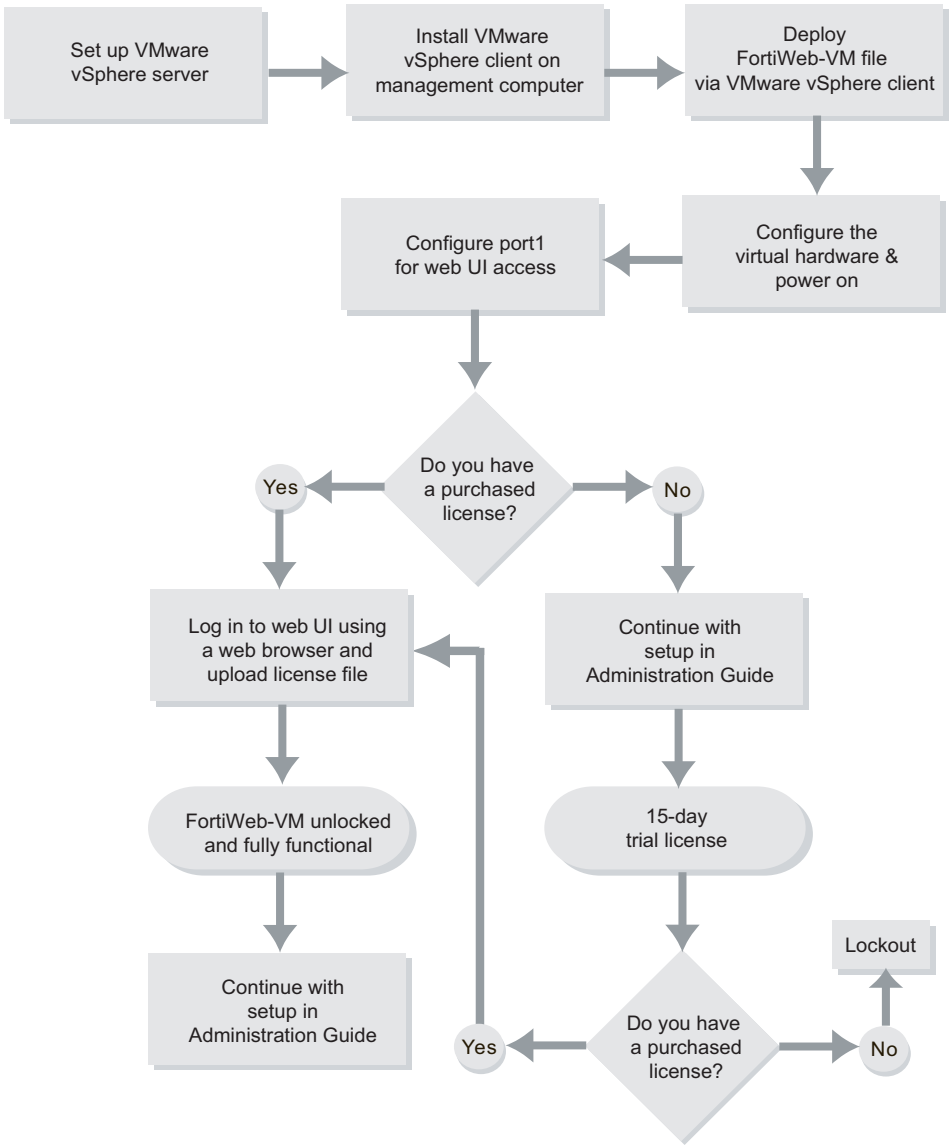
If you have a library of virtual machine images stored on a CIFS or NFS share, download and unzip the folder there instead of on your management computer. When deploying the VM, you can also use a CIFS or NFS network share as the storage repository instead of a vDisk stored locally, on the hypervisor's 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 FortiWeb-VM on VMware vSphere on page 17.

Deploying FortiWeb-VM on VMware vSphere

The diagram below overviews the process for installing FortiWeb-VM on VMware vSphere, which is described in the subsequent text.

Basic steps for installing FortiWeb-VM (VMware)



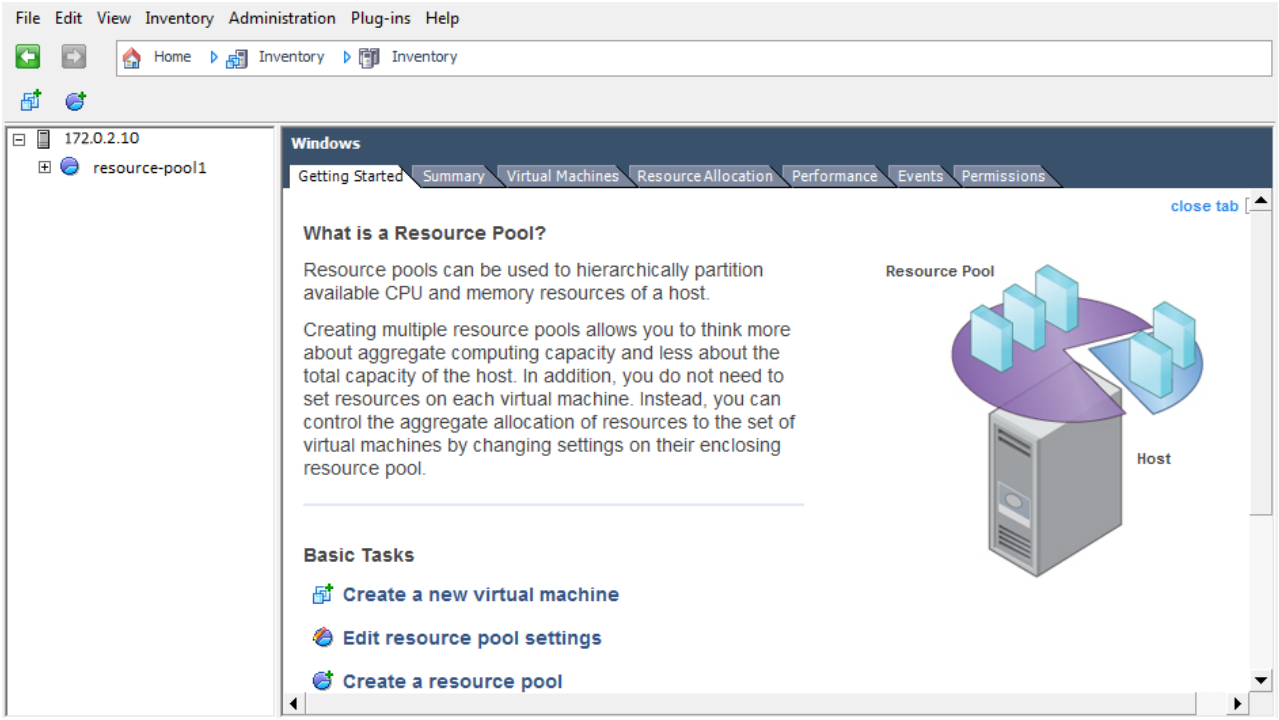
Deploying the OVF file

Before you can configure FortiWeb-VM, you must first use VMware vSphere Client to deploy the FortiWeb-VM OVF package.

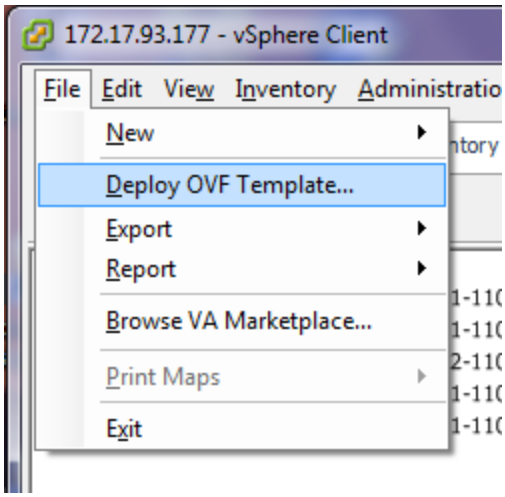
To deploy the virtual appliance

1. On your management computer, start VMware vSphere Client.

In **IP address / Name**, type the IP address or FQDN of the VMware vSphere server.
In **User name**, type the name of your account on that server.
In **Password**, type the password for your account on that server.
Click *Login*.
When you successfully log in, the vSphere Client window appears.

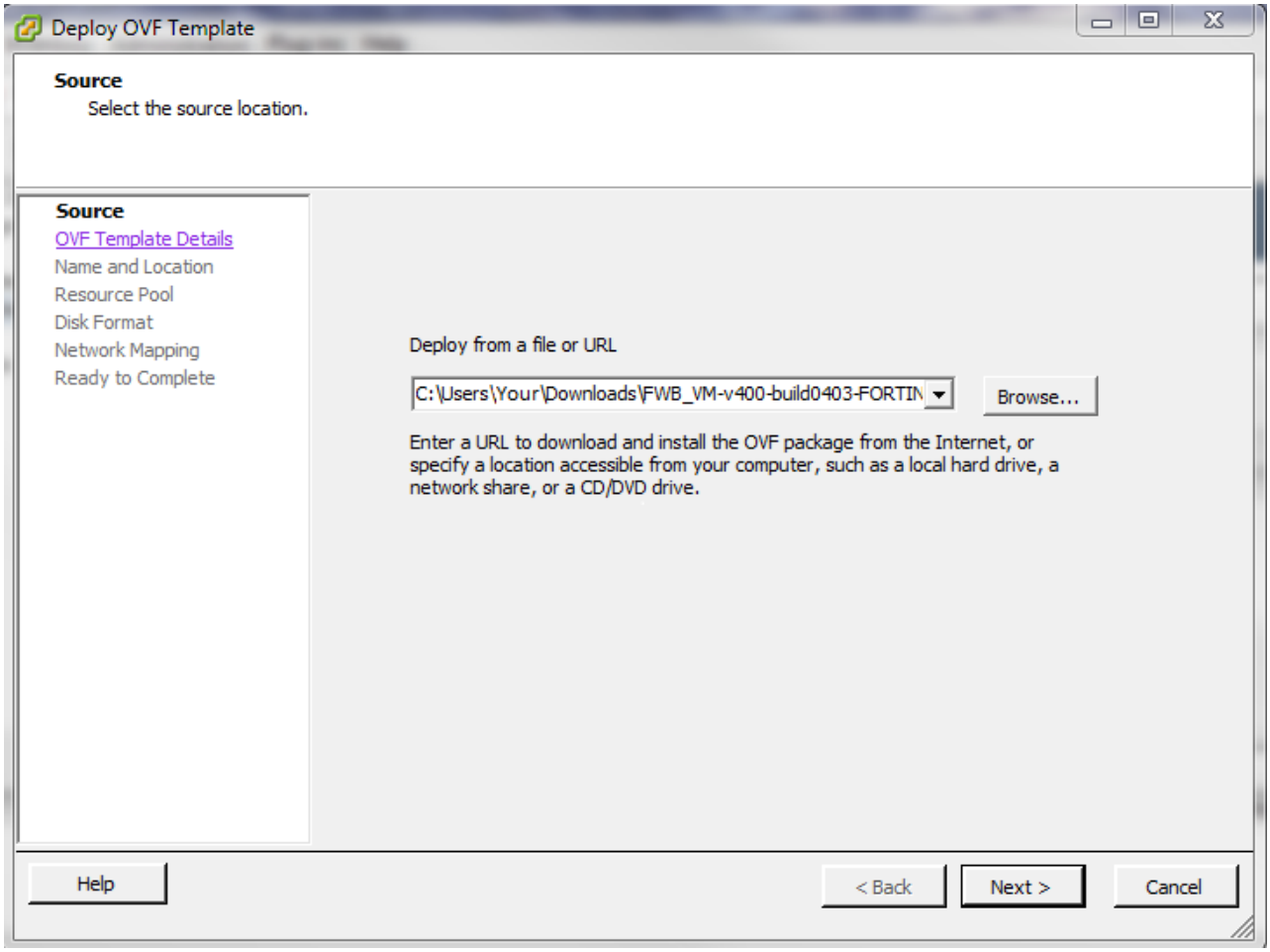


2. Go to **File > Deploy OVF Template**.

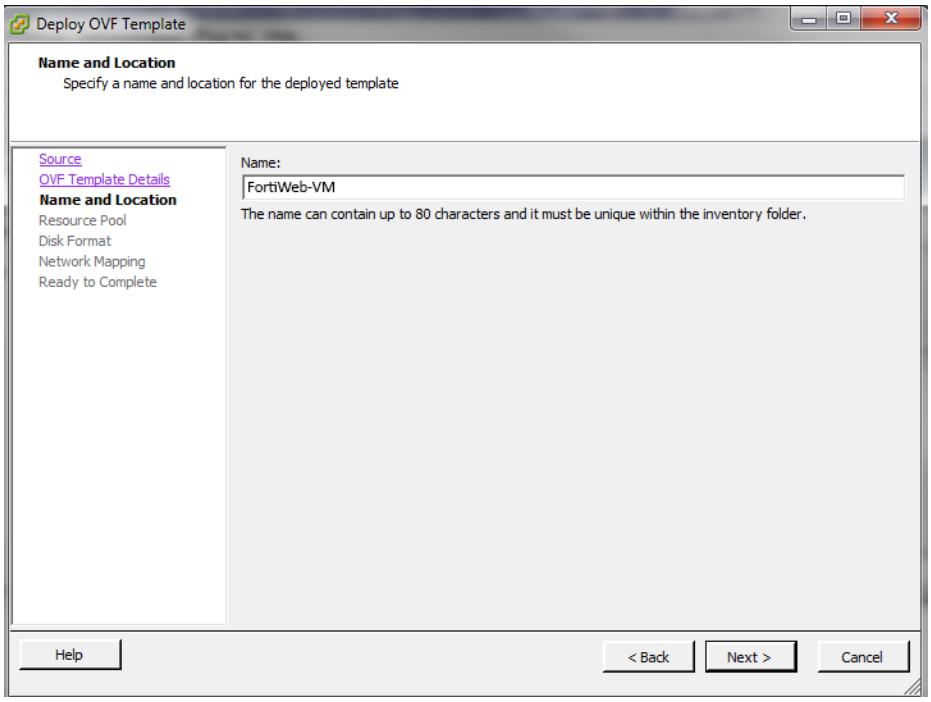


A deployment wizard window appears.

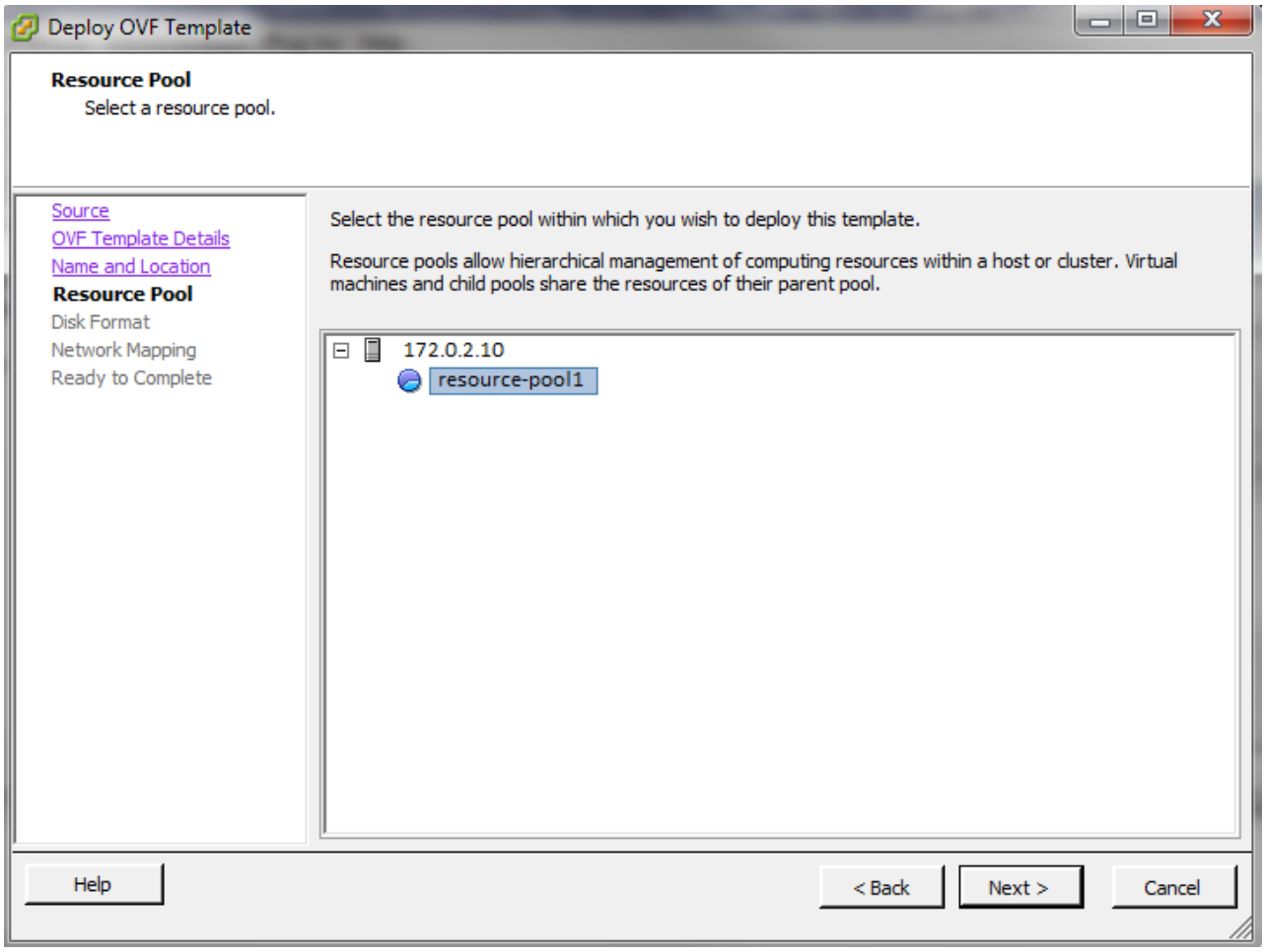
3. In the **Deploy OVF Template** window, click **Browse**, then locate the FortiWeb-VM OVF file.



4. Click **Next** twice.
5. In **Name**, type a unique descriptive name for this instance of FortiWeb-VM as it will appear in vSphere Client's inventory, such as `FortiWeb-VM`. If you will deploy multiple instances of this file, consider a naming scheme that will make each VM's purpose or IP address easy to remember. (This name will not be used as the host name, nor will it appear within the FortiWeb-VM web UI.)

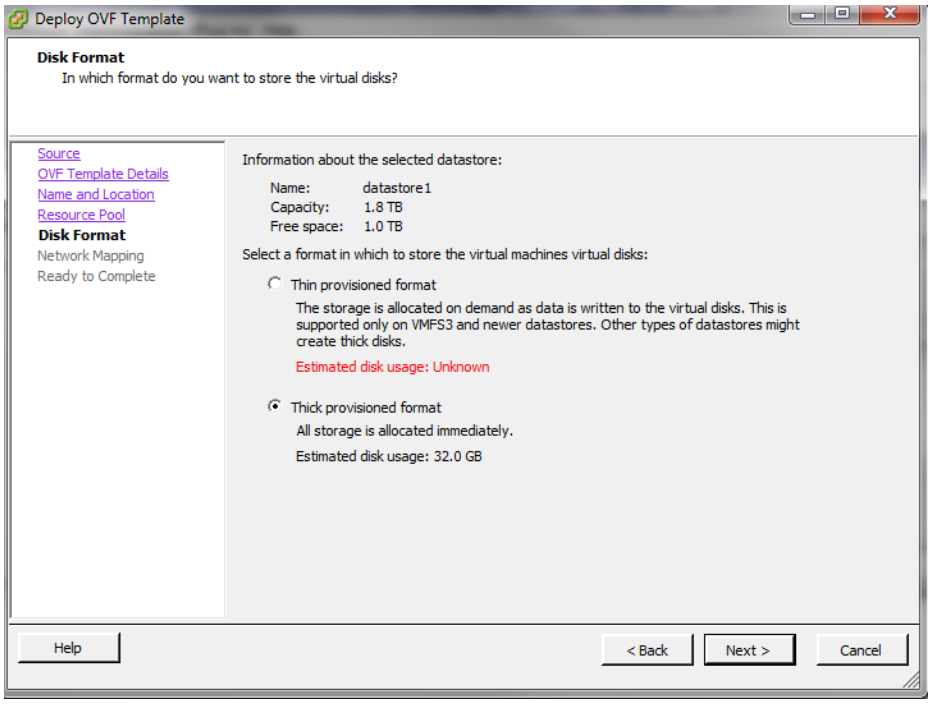


6. Click **Next**.
7. In the resource pool tree, select a virtual machine.



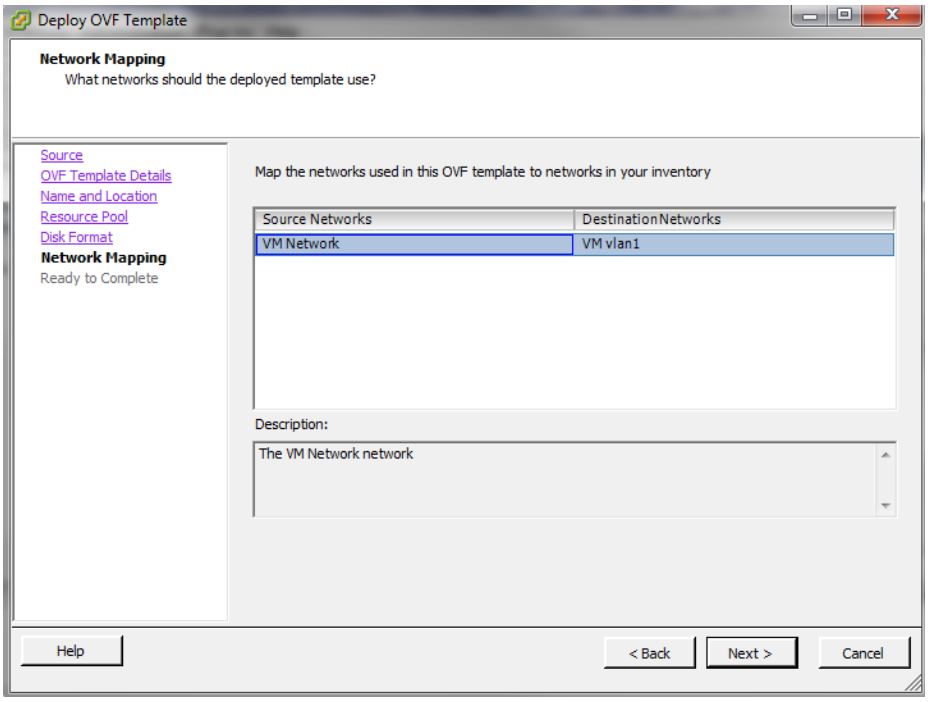
8. Click **Next**.
9. For the storage repository, select either:
   - **Thin provisioned format** — Allocate more disk space on demand, if the storage repository uses a VMFS3 or newer file system.

- **Thick provisioned format** — Immediately allocate disk space (specifically 32 GB) for the storage repository



Regardless of your choice here, you must later either allocate or make available at least 40 GB of disk space. 32 GB is only the default minimum value, and is not recommended.

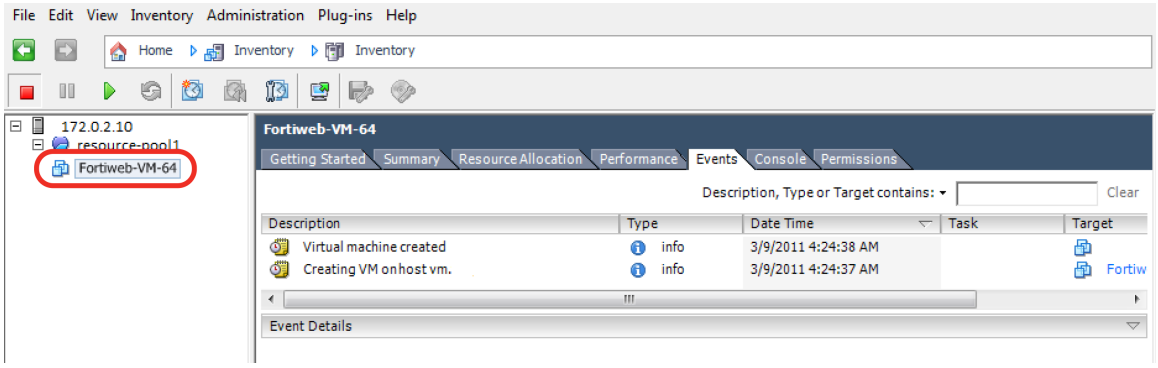
10. Click **Next**.
11. If the hypervisor has more than one possible network mapping for its vSwitch, click to select the row for the network mapping that FortiWeb-VM should use.



12. Click **Next**.
13. Click **Finish**.

    The wizard closes. The client connects to the VM environment and deploys the OVF 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 several minutes to complete.

    The vSphere Client window reappears. The navigation pane's list of virtual machines on the left now should include your new instance of FortiWeb-VM.



Continue with Configuring the virtual appliance's virtual hardware settings on page 25.

Do **not** power on the virtual appliance **until** you:

- Resize the virtual disk (VMDK) (see Resizing the virtual disk (vDisk) on page 25)
- Set the number of vCPUs (see Configuring the number of virtual CPUs (vCPUs) on page 28)
- Set the vRAM on the virtual appliance (Configuring the virtual RAM (vRAM) limit on page 30)
- Map the virtual network adapter(s) (Mapping the virtual NICs (vNICs) to physical NICs on page 32).

These settings cannot be configured inside FortiWeb-VM, and must be configured in the VM environment. **Some settings cannot be easily reconfigured after you power on the virtual appliance.**

Configuring the virtual appliance's virtual hardware settings

After installing FortiWeb-VM, log in to VMware vSphere on the server and configure the virtual appliance's hardware settings to suit the size of your deployment. For sizing guidelines, contact your reseller or Fortinet Technical Support.

For information on the limits of configurable values for FortiWeb-VM, see the *FortiWeb Administration Guide*.

Resizing the virtual disk (vDisk)

If you configure the virtual appliance's storage repository to be internal (i.e. local, on its own vDisk), resize the vDisk **before** powering on.

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

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.**

Before doing so, make sure that you understand the effects of your vDisk settings.

For example, if you have an 800 GB data store which has been formatted with 1 MB block size, you cannot size a single vDisk greater than 256 GB on your FortiWeb-VM.

Consider also that, depending on the size of your organization's network, you might require more or less storage for your auto-learning data, anti-defacement backups, scan results, and reports.

For more information on vDisk sizing, see:

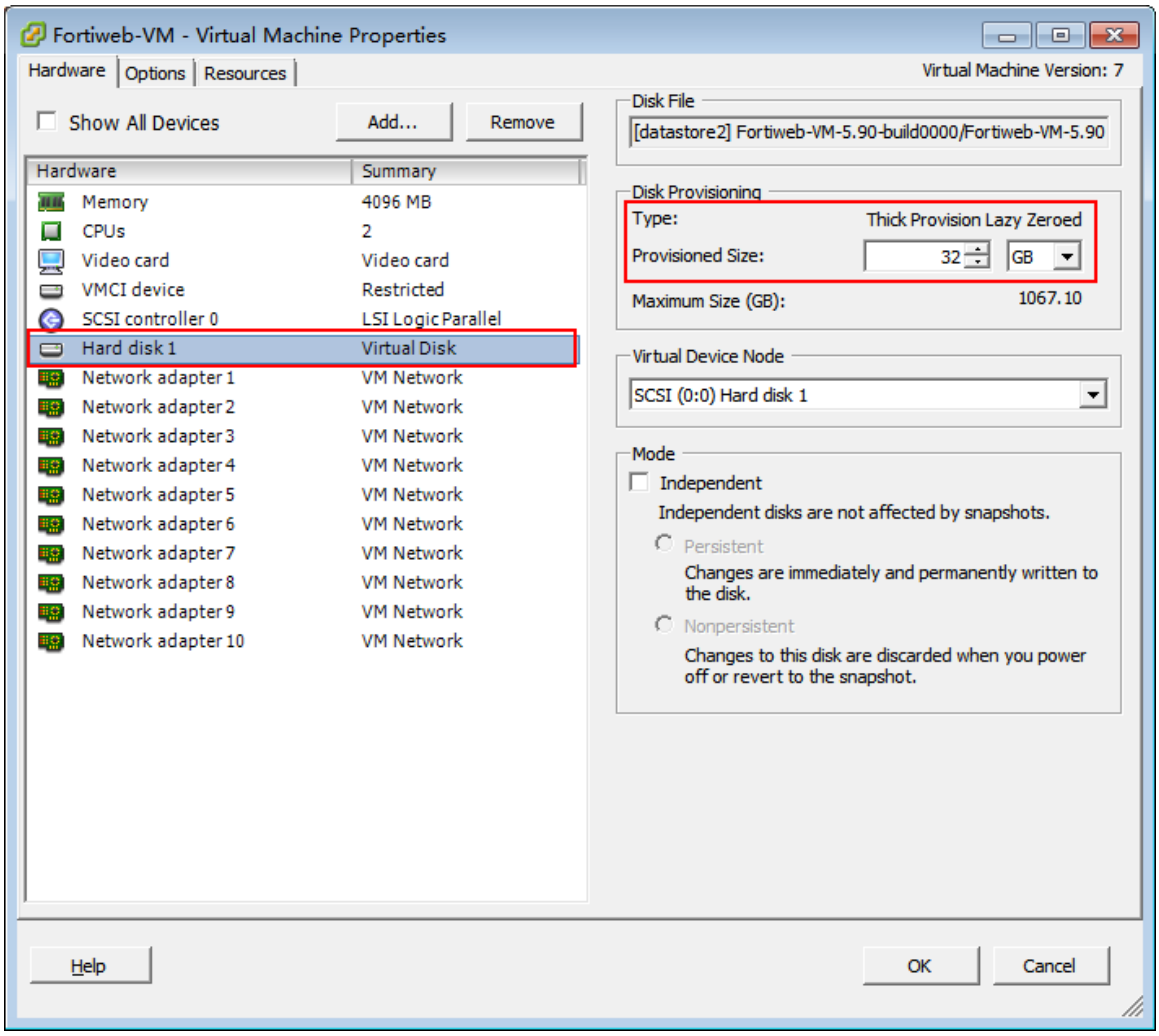
http://communities.vmware.com/docs/DOC-11920

To resize the vDisk

If you are resizing the disk for an existing deployment of FortiWeb-VM, back up the logs and other non-configuration data **before** beginning this procedure. **Formatting the disk will delete all data on that disk.** For backup instructions, see the *FortiWeb Administration Guide*.

While resizing the vDisk, the FortiWeb-VM must be powered off.

1. On your management computer, start VMware vSphere Client.
2. In **IP address / Name**, type the IP address or FQDN of the VMware vSphere server.
3. In **User name**, type the name of your account on that server.
4. In **Password**, type the password for your account on that server.
5. Click *Login*.
6. In the pane on the left side, right-click the name of the virtual appliance, such as **FortiWeb-VM**, then select **Edit Settings**.
   The virtual appliance's properties dialog appears.



7. In the list of virtual hardware on the left side of the dialog, click *Hard disk 1*.
8. In **Provisioned Size**, type the new size of the vDisk as desired. It's recommended to allocate at least 32 GB for the hard disk. The maximum value is 2 TB.
9. Click **OK**.
10. If you do not need to change the other resources, continue with Powering on and shutting down the virtual appliance on page 42. Otherwise continue with Configuring the number of virtual CPUs (vCPUs) on page 28.
11. After powering on the appliance, in the CLI, enter the command:
```
exec formatlogdisk
```

On VMware ESXi, the expanded space will not be recognized **until** the vDisk is reformatted.

Configuring the number of virtual CPUs (vCPUs)

By default, the virtual appliance is configured to use 1 vCPU. Depending on the FortiWeb-VM license that you purchased, you can allocate up to 1, 2, 4, or 8 vCPUs.

If you need to increase or decrease the vCPUs after the initial boot, power off FortiWeb-VM, adjust the number of vCPUs, then see Updating the license for more vCPUs on page 64.

For FortiWeb-VM deployed on an ESXi hypervisor, when you set the number of vCPUs to 8, you also change the default CPU affinity settings (which restrict the virtual machines to a subset of the available processors). This additional configuration can help prevent performance problems.

For more information on vCPUs, see the VMware vSphere documentation:

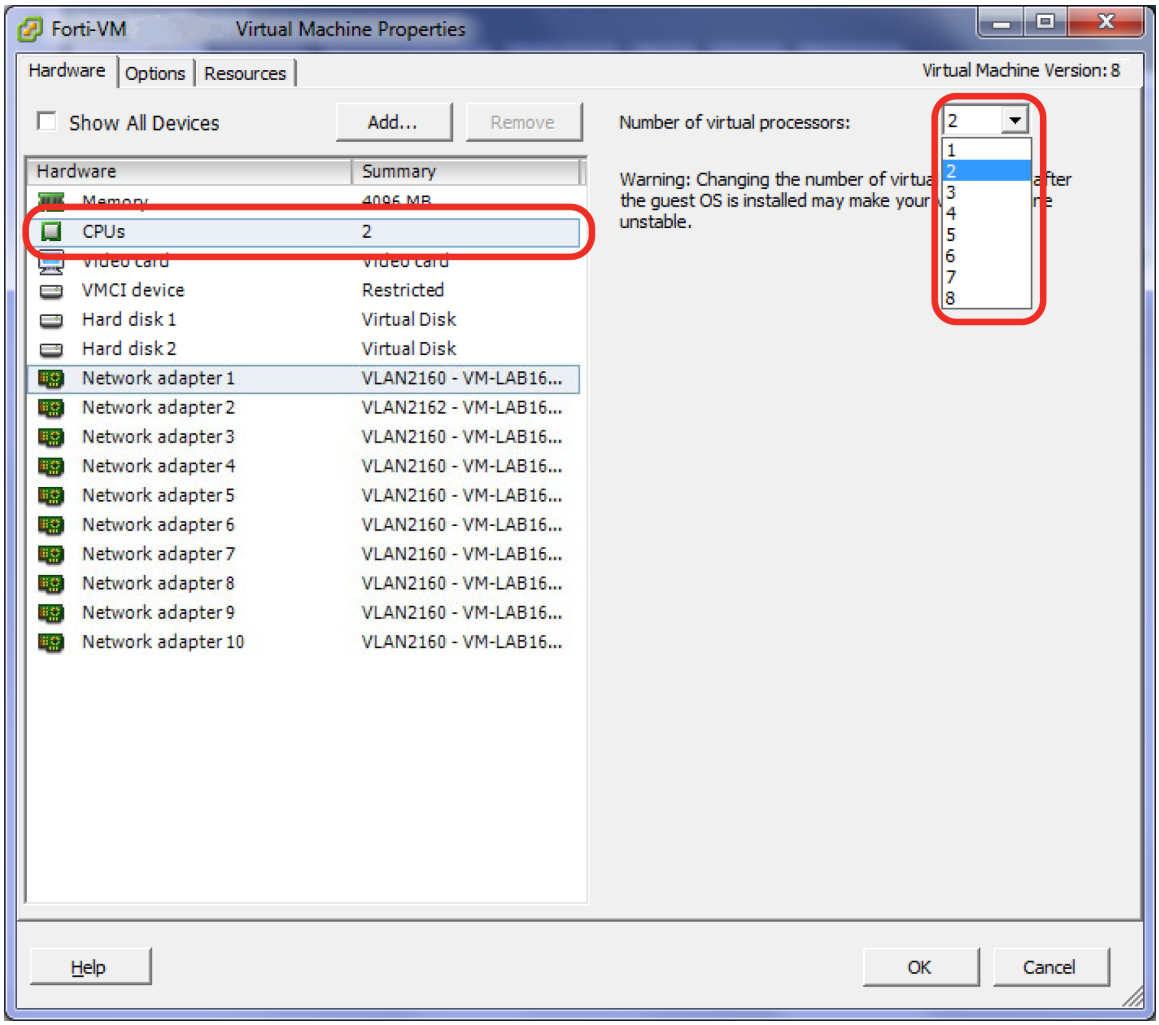
http://www.vmware.com/products/vsphere-hypervisor/index.html

To change the number of vCPUs

While resizing the vCPU, the FortiWeb-VM must be powered off.

1. On your management computer, start VMware vSphere Client.
2. In **IP address / Name**, type the IP address or FQDN of the VMware vSphere server.
3. In **User name**, type the name of your account on that server.
4. In **Password**, type the password for your account on that server.
5. Click *Login*.
6. In the pane on the left side, right-click the name of the virtual appliance, such as **FortiWeb-VM**, then select **Edit Settings**.
   The virtual appliance's properties dialog appears.
7. In the list of virtual hardware on the left side of the dialog, click *CPUs*.

8. In *Number of virtual processors*, type the maximum number of vCPUs to allocate. Valid values range from 1 to 8.



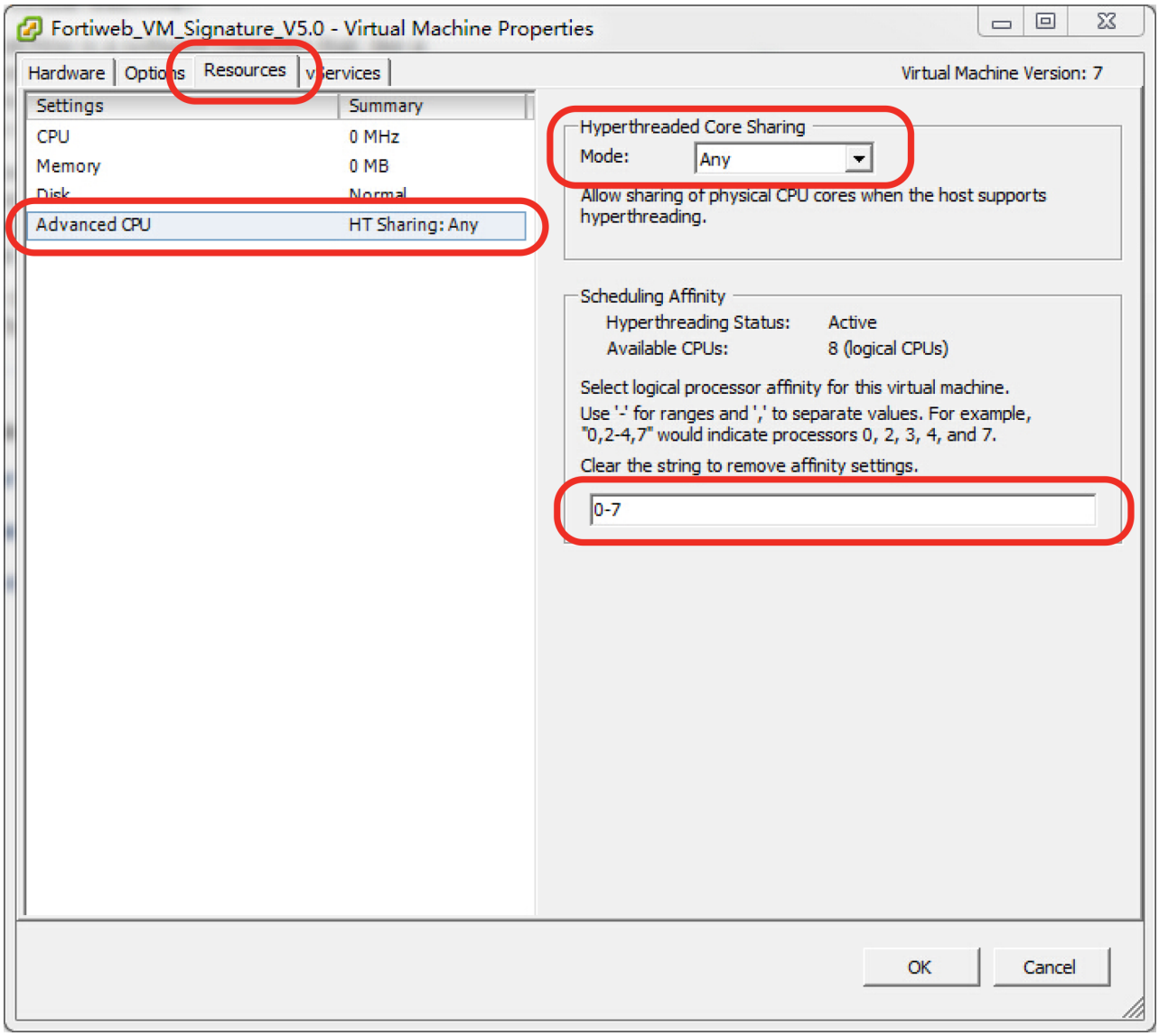
9. Click *OK*.
10. Do one of the following:

- **For vSphere Hypervisor deployments and ESXi deployments with 2 or 4 vCPUs** – If you do not need to change the other resources, continue with Powering on and shutting down the virtual appliance on page 42. Otherwise continue with Configuring the virtual RAM (vRAM) limit on page 30.
- **For ESXi deployments with 8 vCPUs** – Continue with the instructions in To configure vCPUs for FortiWeb-VM08 on ESXi on page 29

To configure vCPUs for FortiWeb-VM08 on ESXi

1. On VMware vSphere Client, ensure you are logged in to the VMware vSphere server.
2. Right-click the name of the virtual appliance, such as **FortiWeb-VM**, then select **Edit Settings**.
   The virtual appliance's properties dialog appears.
3. On the Resources tab, click *Advanced CPU*.
4. Under Hyperthreaded Core Sharing, for **Mode**, select **Any**.

5. Under Scheduling Affinity, to set the logical processor affinity to the required range, enter `0-7`.



6. If you do not need to change the other resources, continue with Powering on and shutting down the virtual appliance on page 42. Otherwise continue with Configuring the virtual RAM (vRAM) limit on page 30

Configuring the virtual RAM (vRAM) limit

FortiWeb-VM comes pre-configured to use 4 GB of vRAM. You can change this value.

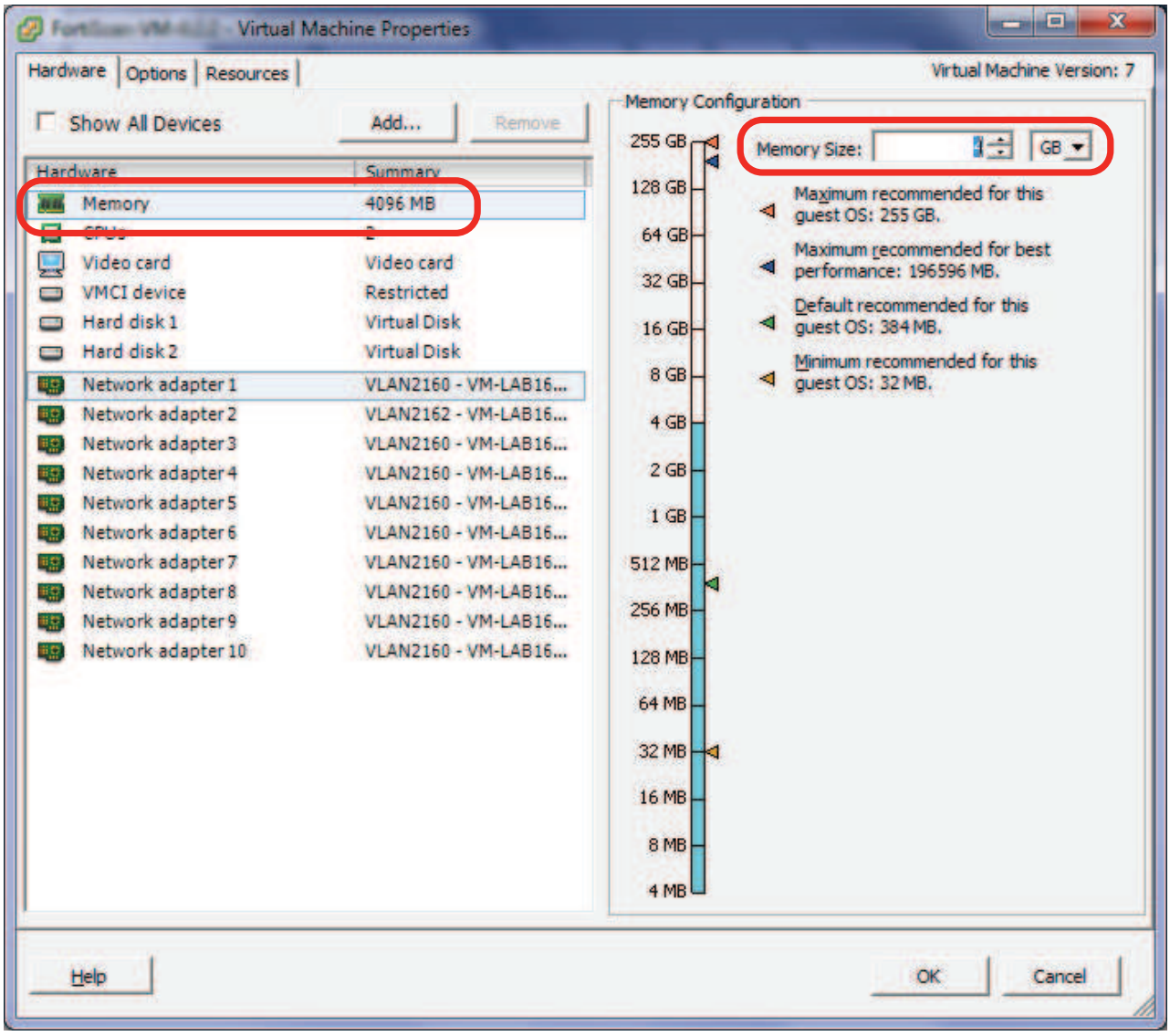
It is possible to configure FortiWeb-VM to use less vRAM, such as 2 GB. However, for performance reasons, it is not recommended.

To change the amount of vRAM

While resizing the vRAM, the FortiWeb-VM must be powered off.

1. On your management computer, start VMware vSphere Client.
2. In **IP address / Name**, type the IP address or FQDN of the VMware vSphere server.
3. In **User name**, type the name of your account on that server.
4. In **Password**, type the password for your account on that server.
5. Click *Login*.
6. In the pane on the left side, right-click the name of the virtual appliance, such as **FortiWeb-VM**, then select **Edit Settings**.
7. The virtual appliance's properties dialog appears.
   In the list of virtual hardware on the left side of the dialog, click *Memory*.

8. In *Memory Size*, type the maximum number in gigabytes (GB) of the vRAM to allocate.



9. Click **OK**.
10. If you do not need to change the other resources, continue with Powering on and shutting down the virtual appliance on page 42. Otherwise continue with Mapping the virtual NICs (vNICs) to physical NICs on page 32.

Mapping the virtual NICs (vNICs) to physical NICs

Appropriate mappings of the FortiWeb-VM network adapter ports to the host computer's physical ports depends on your existing virtual environment.

Often, the default bridging vNICs work, and don't need to be changed.

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

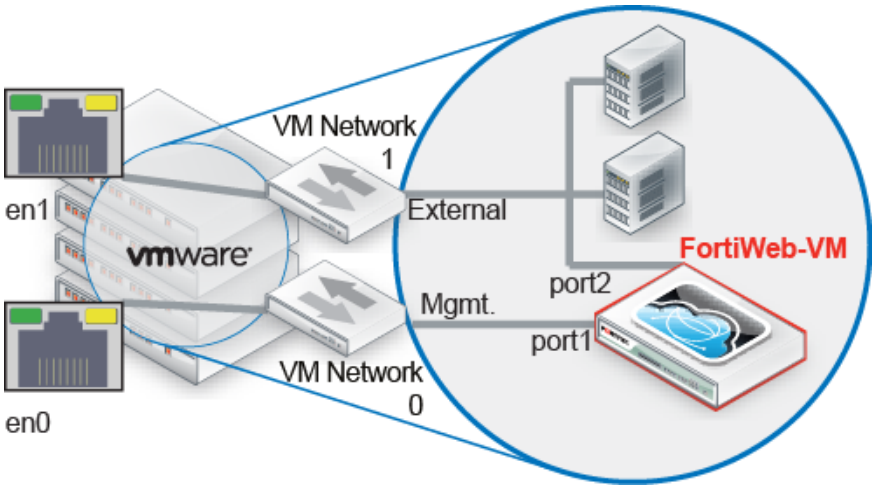
The most common exceptions to this rule are for VLANs and the transparent modes. See Configuring the vNetwork for the transparent modes on page 36

When you deploy the FortiWeb-VM package, 10 bridging vNICs are created and automatically mapped to a port group on 1 virtual switch (vSwitch) within the hypervisor. Each vNIC is mapped to one of 10 FortiWeb-VM network interfaces. (Alternatively, you can configure some or all of the network interfaces to use the same vNIC.) vSwitches are themselves mapped to physical ports on the server.

In some cases, FortiWeb-VM deployed on ESXi cannot update the mapping between vNICs and FortiWeb-VM network interfaces after you remove and add adaptors. See Changing the default network adaptors for EXSi deployments on page 35.

You can change the mapping, or map other vNICs, if either your VM environment requires it or FortiWeb-VM will be operating in either true transparent proxy or Transparent Inspection mode. (For information on how to choose the operation mode, see the setup instructions in the *FortiWeb Administration Guide*.)

The following table provides an example of how vNICs could be mapped to the physical network ports on a server.



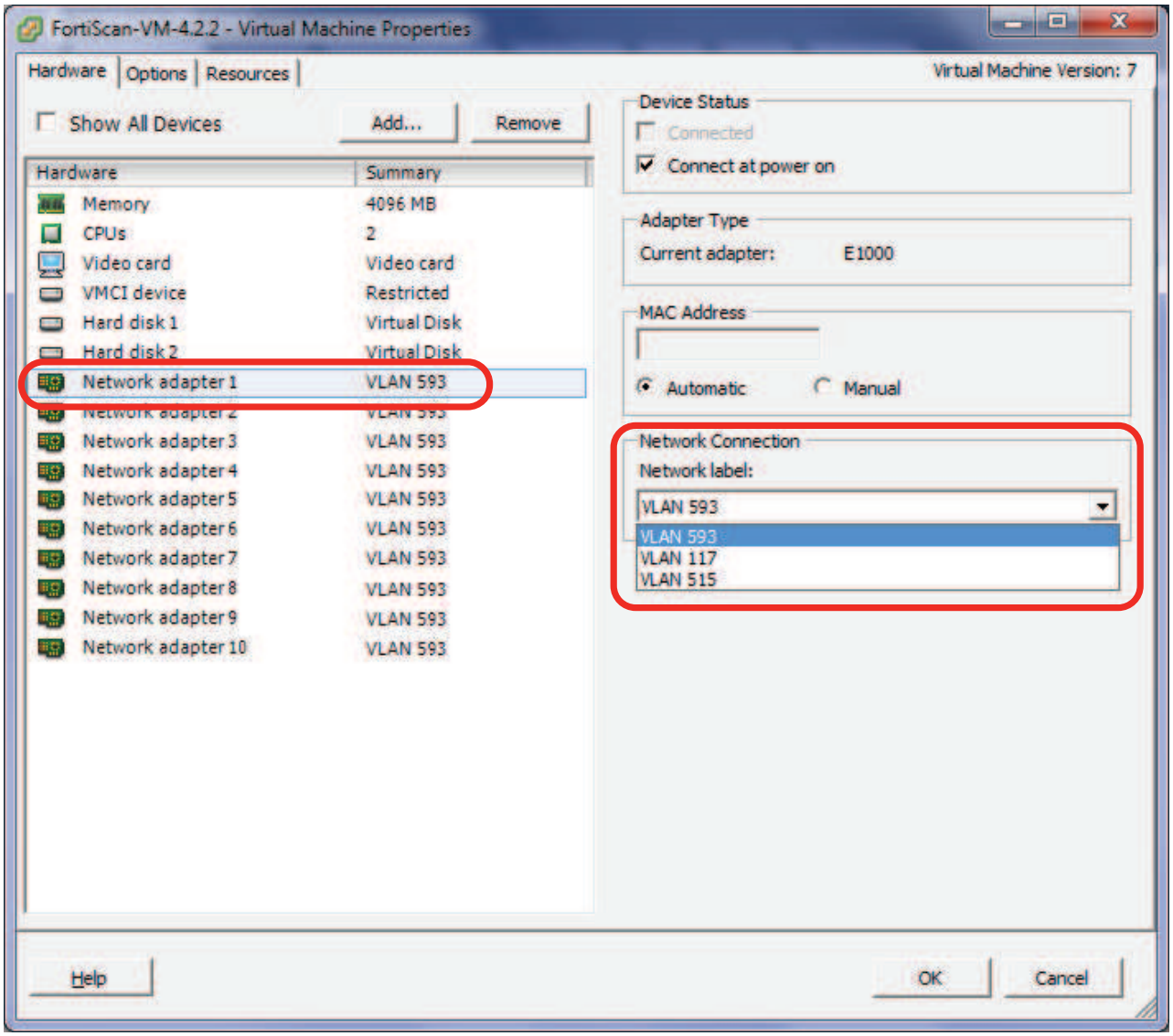
Example: Network mapping for Reverse Proxy mode

VMware vSphere			FortiWeb-VM
Physical Network Adapter	**Network Mapping (vSwitch Port Group)**	**Virtual Network Adapter for FortiWeb-VM**	**Network Interface Name in Web UI/CLI**
eth0	VM Network 0	Management	port1

eth1	VM Network 1	External	port2
	VM Network 2	Internal	port3
	VM Network 1	External	port4

To map network adapters

1. On your management computer, start VMware vSphere Client.
2. Enter the IP address, user name, and password of the VMware vSphere server.
3. Click *Login*.
4. In the pane on the left side, right-click the name of the virtual appliance, such as **FortiWeb-VM**, then select **Edit Settings**.
   The virtual appliance's properties dialog appears.
5. In the list of virtual hardware on the left side of the dialog, click the name of a virtual network adapter to see its current settings.
6. From the **Network Connection** drop-down menu, select the virtual network mapping for the virtual network adapter.
   The correct mapping varies by your virtual environment's network configuration. In the example illustration below, the vNIC **Network adapter 1** is mapped to the virtual network (vNetwork) named **VLAN 593.**



7. Click **OK**.
8. Continue with Powering on and shutting down the virtual appliance on page 42.

Changing the default network adaptors for EXSi deployments

By default, FortiWeb-VM deploys on ESXi using VMXNET network adaptors.

However, you can delete the VMXNET adaptors and add E1000 network adaptors that replace them, if required. E1000 adaptors do not have the same limitations as VMXNET adaptors. However, for best performance, use VMXNET adaptors because they are optimized for performance in a virtual machine.

To avoid problems with the mapping of vNICs to FortiWeb-VM network interfaces, do the following:

- Ensure the network adaptors are all of the same type: VMXNET or E1000.
- If you are using VMXNET adaptors, do not remove and add adaptors. FortiWeb-VM cannot update the initial mappings to work with the new adaptors.

However, you can add VMXNET adaptors if you are upgrading from a previous version of FortiWeb-VM that provides only 4 adaptors. (Because the additional adaptors are new, there is no existing mapping to create a conflict.) Ensure that the total number of adaptors after the upgrade is 8 or 10.

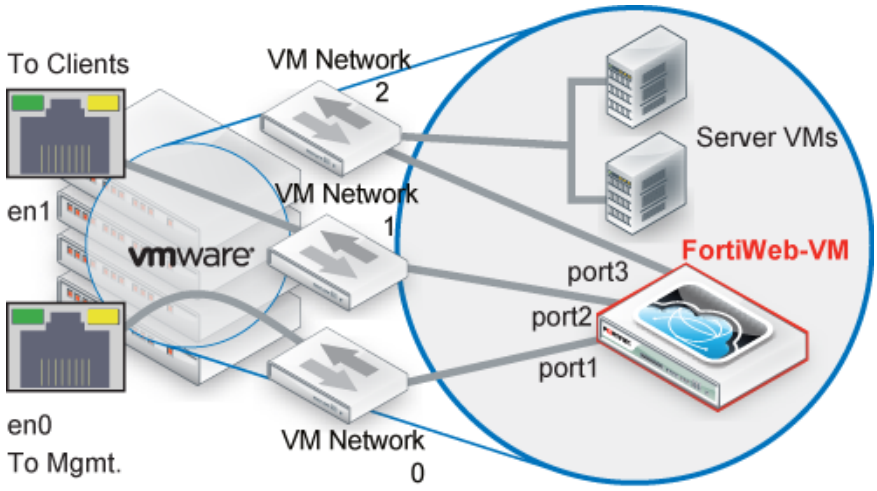
Configuring the vNetwork for the transparent modes

The default vNetwork configuration does **not** function with FortiWeb bridges (V-zones). You use bridges when you deploy your FortiWeb-VM in either true transparent proxy or Transparent Inspection operation mode.

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

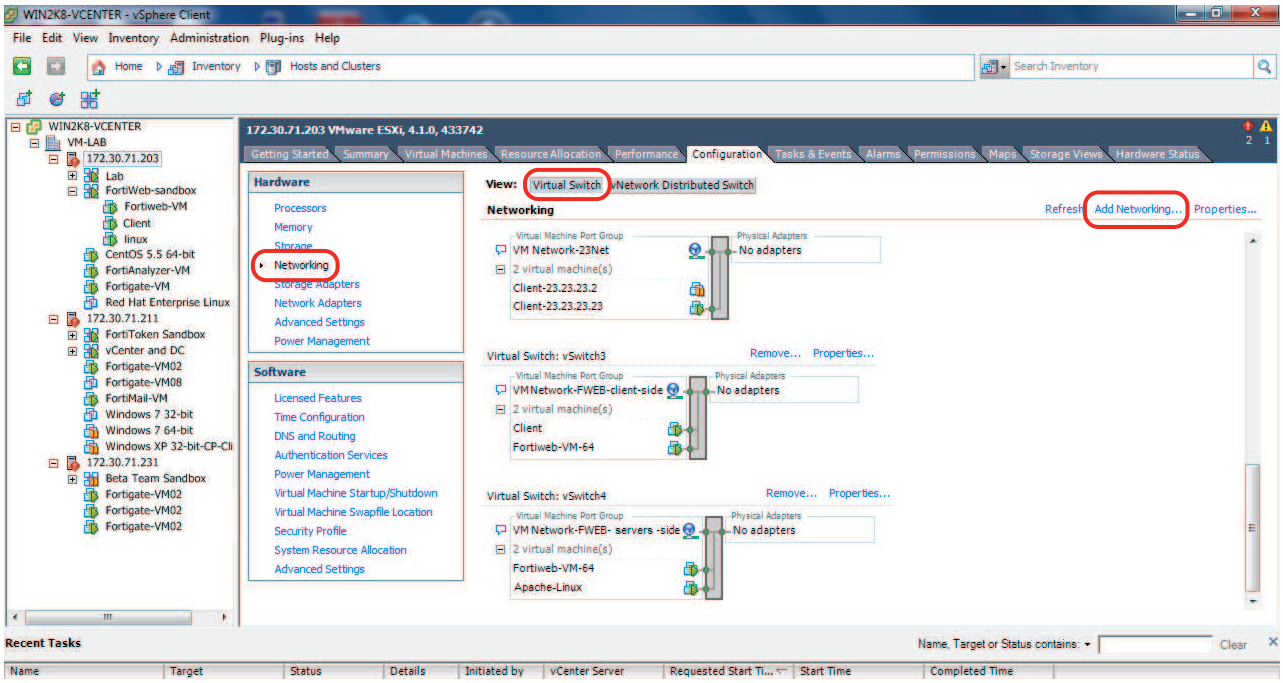
- To create the bridge, use one of the following to create two FortiWeb ports: one for the web server side and one for the client side:
  - 2 vSwitches or distributed vSwitches (dvSwitch)
  - 1 vSwitch that has 2 port groups with different VLAN IDs
- Set each vSwitch that you add to promiscuous mode and map each port group to a network adapter (vNIC)

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.



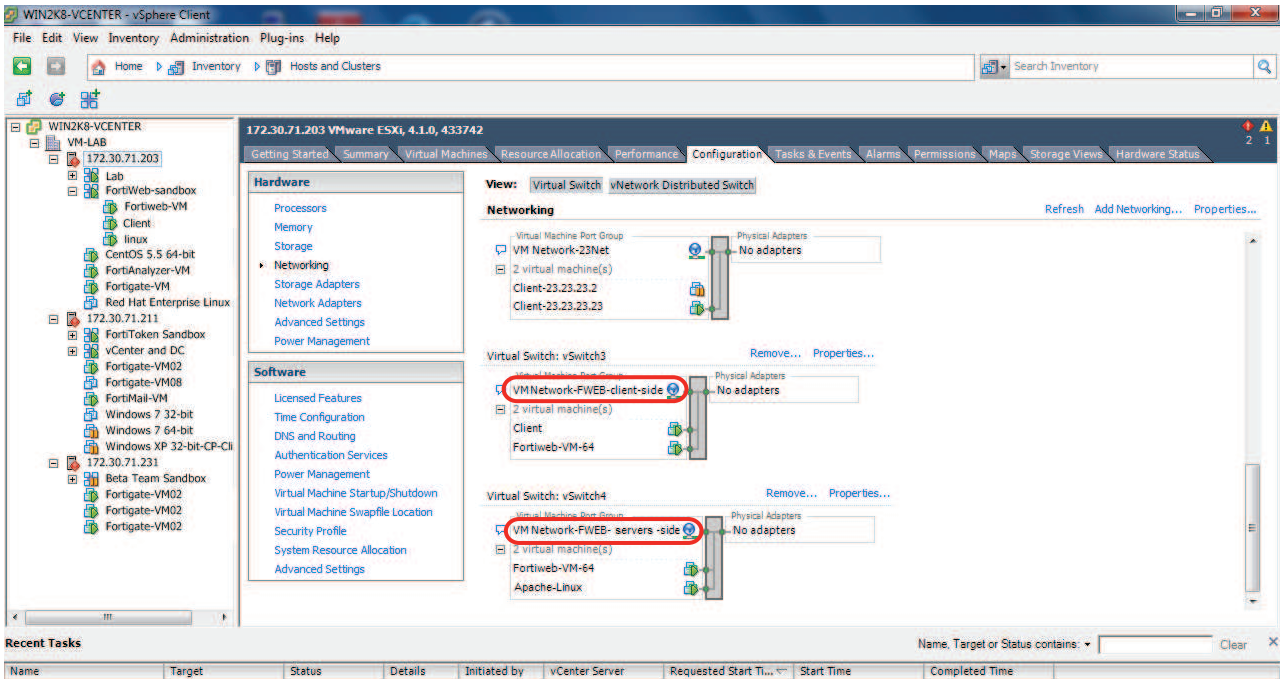
To create a vSwitch

1. On your management computer, start VMware vSphere Client.
2. In **IP address / Name**, type the IP address or FQDN of the VMware vSphere server.
3. In **User name**, type the name of your account on that server.
4. In **Password**, type the password for your account on that server.
5. Click *Login*.
6. In the pane on the left side, click the name of the virtual appliance, such as **FortiWeb-VM**.
7. On the **Configuration** tab, click **Networking**.
   A window appears where you can configure vSwitches or distributed vSwitches.



8. In the **View** set of buttons, click **Virtual Switch**. (If you are configuring a distributed vSwitch, click **vNetwork Distributed Switch** instead. Your steps will vary slightly, but will be similar.)
9. Click **Add Networking**.
10. Accept the default connection type, **Virtual Machines**, and click **Next**.
11. Select **Create a virtual switch**.
12. Click **Next**.
13. Under **Port Group Properties**, enter a network label such as `Client-Side-vSwitch1` that identifies the port group.
14. In **VLAN ID**, if your network uses VLANs, enter a number between 1 and 4,094 to specify the VLAN tag that the vSwitch uses.
    If your configuration uses only one vSwitch, add a second port group with a different VLAN tag.
15. Click **Next**.
16. Click **Finish**.

17. If your configuration uses 2 vSwitches, repeat this procedure to create the other vSwitch.

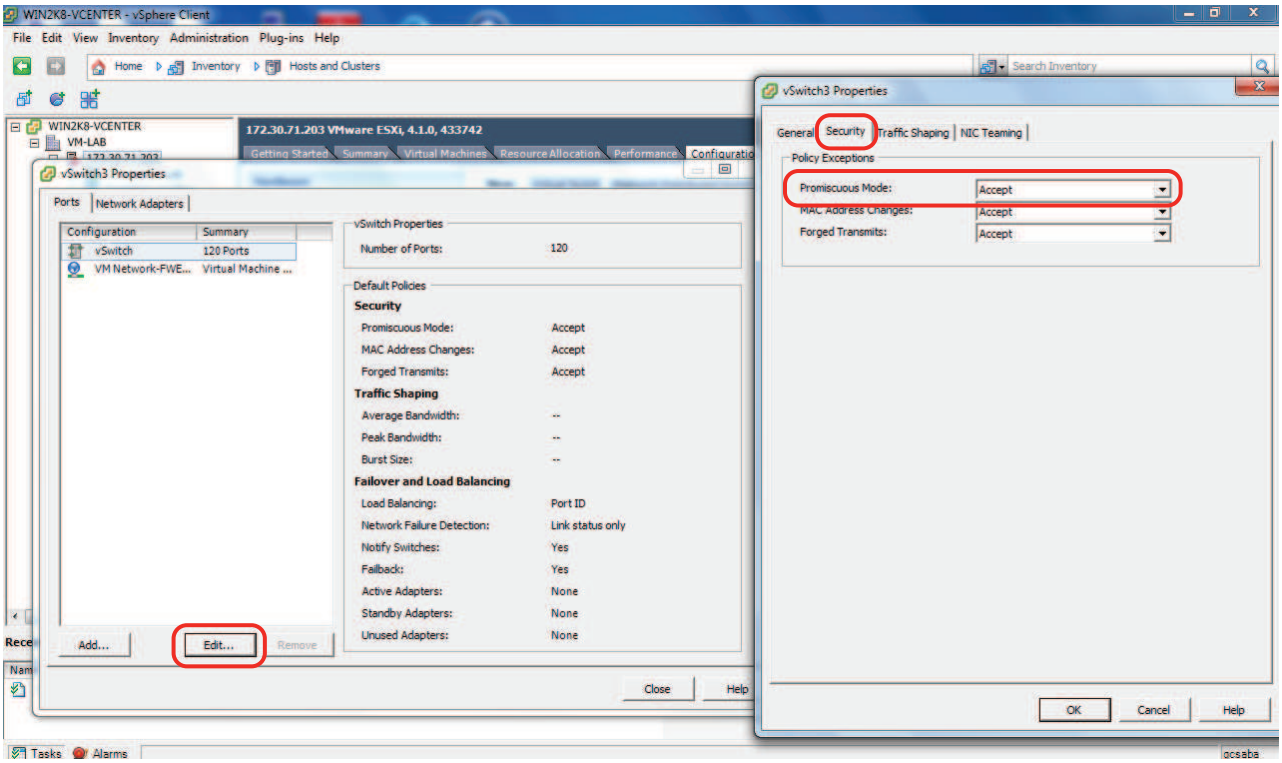


18. If you are creating vSwitches to support True Transparent Proxy, ensure that the vSwitch is configured to use only one VMNIC.
19. Continue with To configure promiscuous mode for the new vSwitch.

To configure promiscuous mode for the new vSwitch

1. On the **Configuration** tab, click **Networking**.

2. Select **Properties**.

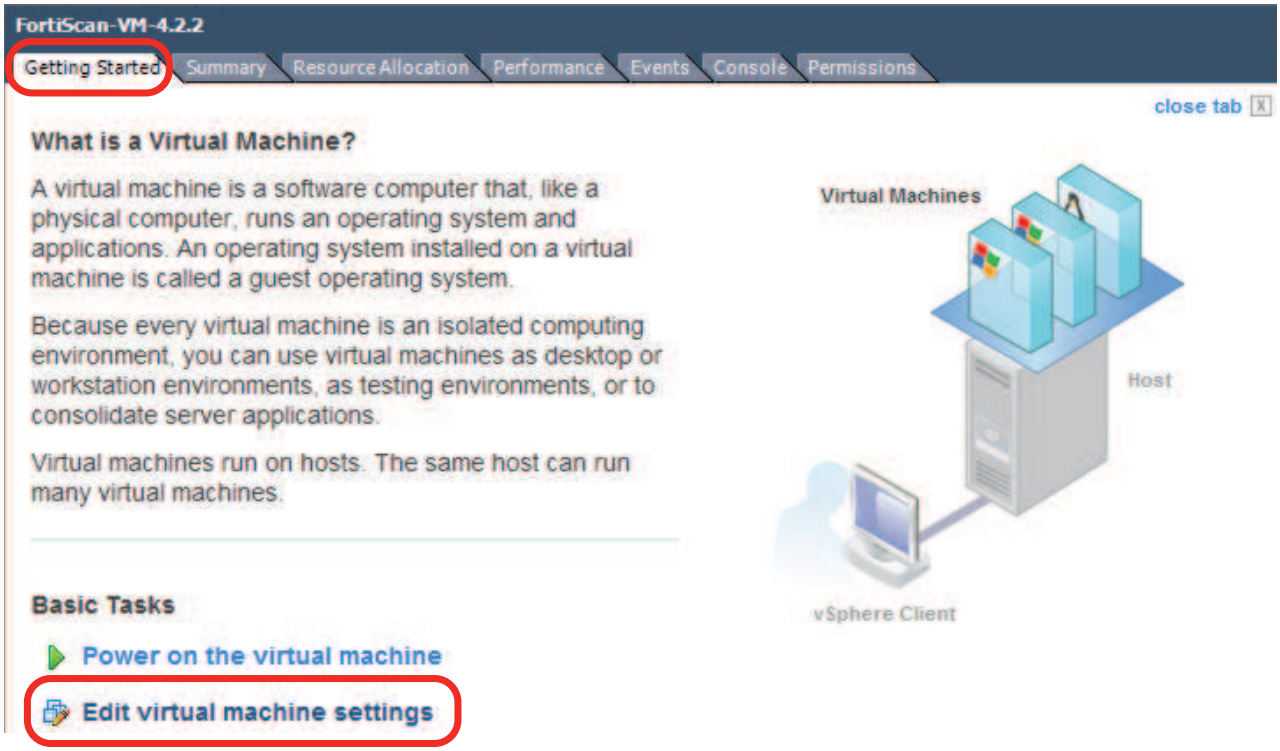


3. Click **Edit**.
4. Select the **Security** tab.
5. From the drop-down list for **Promiscuous Mode**, select **Accept.**
6. If your configuration uses 2 vSwitches, repeat this procedure with the other vSwitch for the bridge.
7. Continue with To map a network adapter to the new vSwitch port groups.

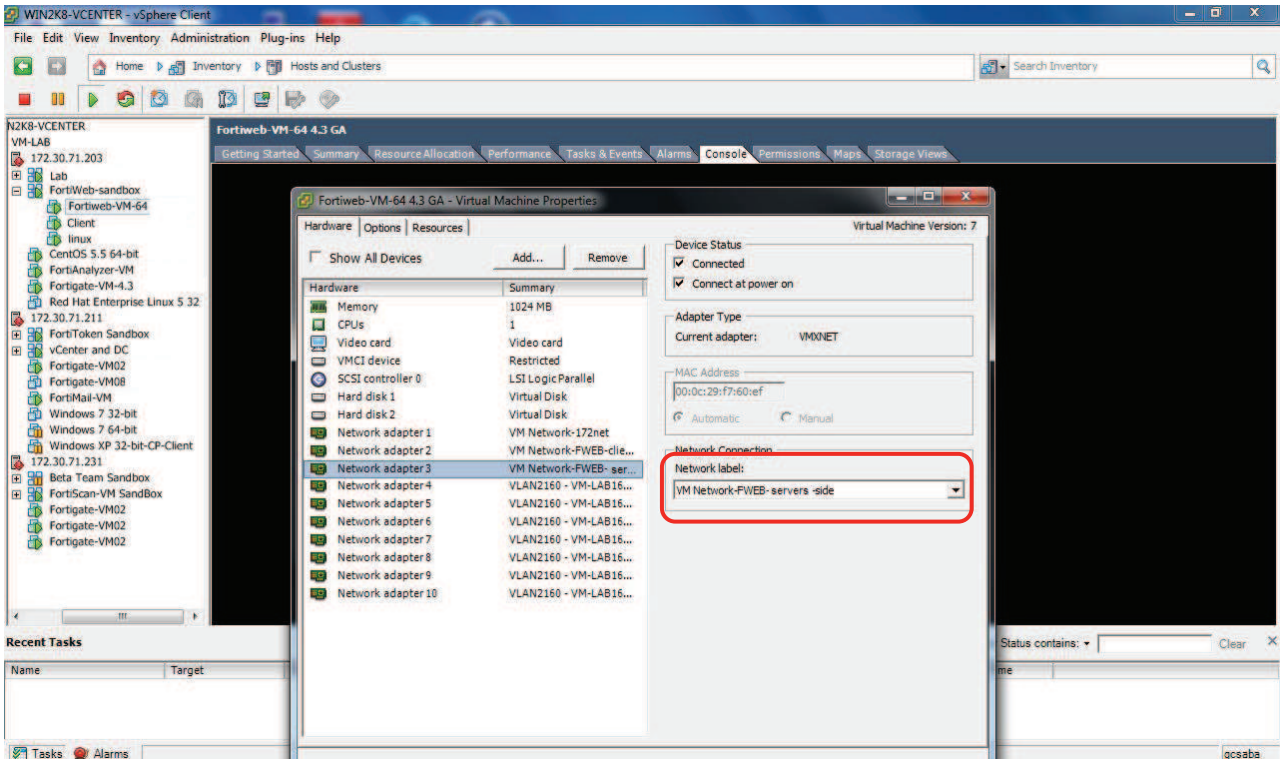
To map a network adapter to the new vSwitch port groups

1. In the pane on the left side, click the name of the virtual appliance, such as **FortiWeb-VM**.

2. On the **Getting Started** tab, select **Edit Virtual Machine Settings**.



A properties window appears.



3. On the **Hardware** tab, select a network adapter from the hardware list.

4. Select the port group of the new vSwitch from the **Network label** drop-down list.
5. Click **OK**.
6. Do one of the following:
   - If your configuration uses 2 vSwitches, repeat this procedure with the port group on the second vSwitch.
   - If your configuration users 1 vSwitch, repeat this procedure with the second port group on the vSwitch.
7. Later, when you configure FortiWeb-VM, add the FortiWeb ports that correspond to the mapped vSwitch port groups to the bridge (V-zone).

Configuring vSwitches and vLANs to support an HA group on ESXi

To include FortiWeb-VM deployed on an ESXi hypervisor in a high availability (HA) group, ensure that the vSwitch and vLAN **Promiscuous Mode**, **MAC Address Changes** and **Forged Transmits** security policies are configured as shown in the following tables. The configurations allow the VM to become part of a group and process traffic correctly if there is a failover.

Table 1: vSwitch and vLAN security policies when FortiWeb is deployed in **Reverse Proxy** operation mode

	active-passive HA / active-active standard HA		active-active high volume HA	
	vSwitch	vLAN	vSwitch	vLAN
Promiscuous mode	Reject	Reject	Reject	Accept
MAC Address Changes	Reject	Accept	Reject	Reject
Forged Transmits	Reject	Accept	Reject	Accept

Table 2: vSwitch and vLAN security policies when FortiWeb is deployed in **True Transparent Proxy** operation mode

	active-passive HA / active-active standard HA	
	vSwitch	vLAN
Promiscuous mode	Reject	Accept
MAC Address Changes	Reject	Accept
Forged Transmits	Reject	Accept

It's suggested to exactly follow the configurations listed in the tables above, especially for the **Accept** settings, because changing the settings from **Accept** to **Reject** will lead to traffic disruption.

However, it's allowed to change the settings from **Reject** to **Accept** because the traffic will not be affected in this way. Just keep in mind that it may compromise the security of the network.

1. Log in to the vSphere Client and select the host from the inventory panel.
2. Click the **Configuration** tab and click **Networking**.
3. On the right side of the page, click **Properties** for the vSwitch to edit.
4. Click the **Ports** tab.
5. Select the vSwitch item in the Configuration list, and click **Edit**.
6. Click the **Security** tab.

7. For **Promiscuous Mode**, **MAC Address Changes** and **Forged Transmits**, configure them as shown in the tables above.
8. Select the vLAN item and configure **Promiscuous Mode**, **MAC Address Changes** and **Forged Transmits** as specified.
9. Click **OK**.

Powering on and shutting down the virtual appliance

Once the virtual appliance's package has been deployed and its virtual hardware configured, you can power on the virtual appliance.

Do **not** power on the virtual appliance **unless** you have already mapped the virtual network adapter(s) (Mapping the virtual NICs (vNICs) to physical NICs on page 32). You may also want to:

- Resize disk (VMDK) (see Resizing the virtual disk (vDisk) on page 25)
- Configure the number of CPUs (see Configuring the number of virtual CPUs (vCPUs) on page 28)
- Set the RAM on virtual appliance (Configuring the virtual RAM (vRAM) limit on page 30)

These settings cannot be configured inside FortiWeb-VM, and must be configured in the virtual machine environment.

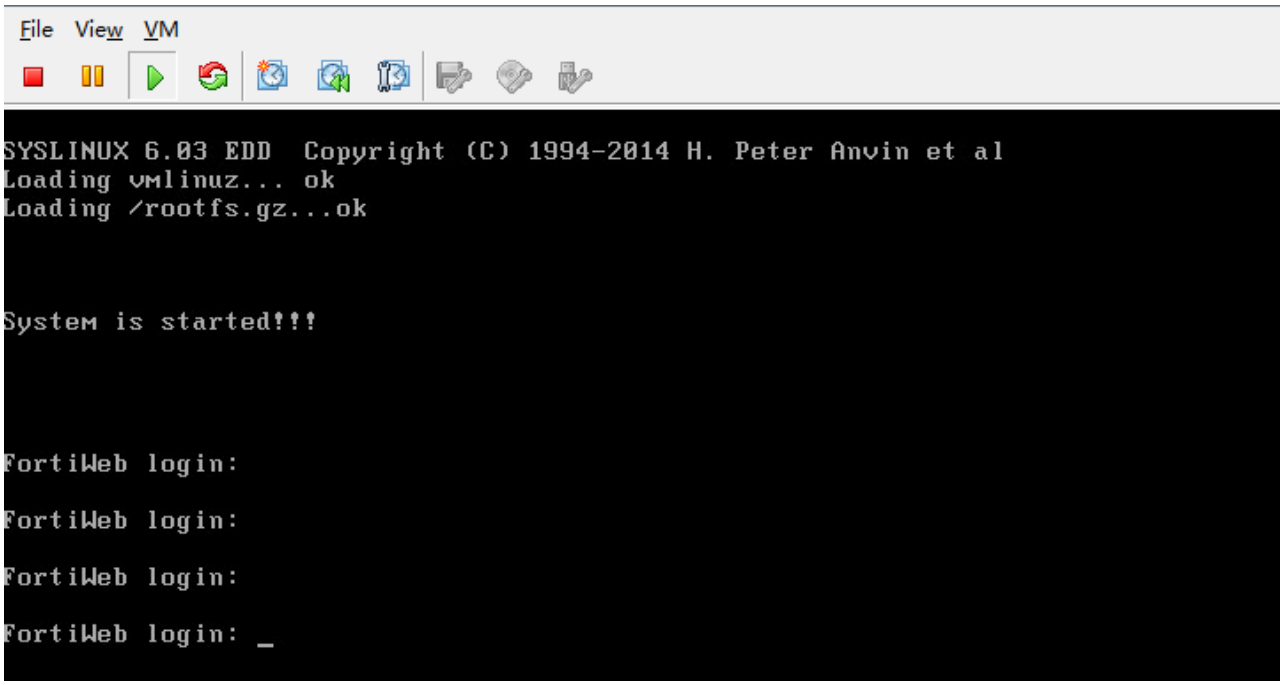
To power on FortiWeb-VM

1. On your management computer, start VMware vSphere Client.
2. In **IP address / Name**, type the IP address or FQDN of the VMware vSphere server.
3. In **User name**, type the name of your account on that server.
4. In **Password**, type the password for your account on that server.
5. Click *Login*.
6. In the pane on the left side, click the name of the virtual appliance, such as **FortiWeb-VM**.
7. Click the **Getting Started** tab.

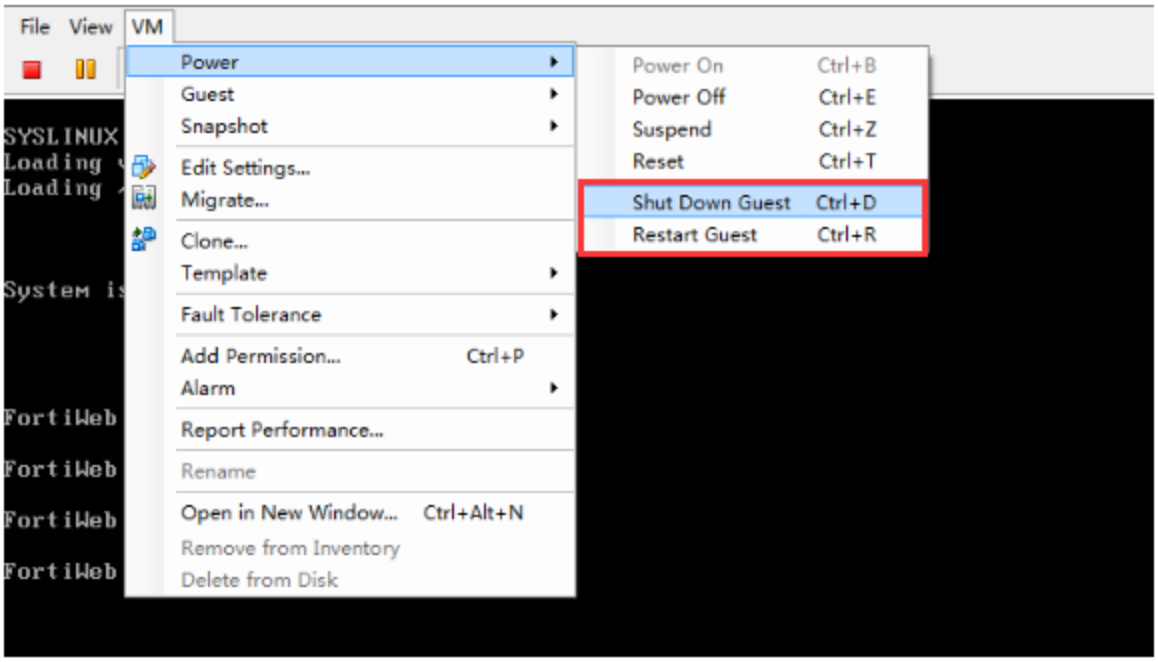
8. Click **Power on the virtual machine**.
9. Continue with Configuring access to FortiWeb's web UI & CLI on page 55.

To shut down or restart FortiWeb-VM

1. In the vSphere Client, access the FortiWeb-VM console.



2. Click **VM > Power**, and then select an option to shut down or restart the VM.



Deploying FortiWeb-VM from templates in vSphere

A template is a virtual machine that has been converted to make copies of itself. You can save the settings and configuration for a FortiWeb-VM instance in a template. You can then deploy additional FortiWeb-VM instances using the template and use the Customization Wizard to configure the virtual network settings of each FortiWeb-VM instance according to your environment's needs.

This section provides basic instructions to:

- Clone a FortiWeb-VM instance to a template.
- Deploy a FortiWeb-VM instance using a saved template and configure the virtual network settings.

For more details, see the VMware vSphere documentation:

https://docs.vmware.com/en/VMware-vSphere/6.0/vsphere-esxi-vcenter-server-601-virtual-machine-admin-guide.pdf

Deploy the OVF package and modify the FortiWeb configuration before cloning a FortiWeb-VM instance to a template. For details, see Deploying the OVF file on page 18 and refer to the *FortiWeb Administration Guide*:
http://docs.fortinet.com/fortiweb/admin-guides

To clone a virtual machine to a template

1. Log in to the VMware vSphere client. For details, see On your management computer, start VMware vSphere Client. on page 18.
2. Right-click the FortiWeb-VM instance for which you want to create a template.
3. Select **Template** and click **Clone to Template**.
4. Enter a **Name** for the template. The maximum length is 80 characters.
   Note: If you change the name of the template, the names of the files in the database for that template do **not** change.
5. For **Location**, select the folder or datacenter location in which you want to store the template.
6. Click **Next**.
7. Select a **Resource** for the template. This will handle all requests for the template.
8. Click **Next**.
9. Select a **Datastore Format** for the template's virtual disk and files:
   Same format as source—Use the same format as the FortiWeb-VM instance that you're cloning to a template.
   Thick Provision Lazy Zeroed—Create a virtual disk that allocates space at the moment of creation. Any remaining data on the disk is zeroed out on first write from the FortiWeb-VM instance.
   Thick Provision Eager Zeroed—Create a virtual disk that allocates space at the moment of creation. Any remaining data is zeroed out at the moment of creation.
   Thin Provision—Create a virtual disk that allocates only as much space as initially needed. If the virtual disk requires more space at a later time, it will increase to the maximum capacity allocated to it.
10. Select a **Datastore Location** for the virtual disk:
    Store with the virtual machine—Store the virtual disk in the same location that you specified for the template.
    Browse—Select a datastore for the virtual disk.
    Disable Storage DRS for this virtual machine—Disable the Distributed Resource Scheduler (DRS) and select a datastore for the virtual disk.
11. Click **Next**.
12. Review the template settings. If you need to change any settings, click **Back** until you find the relevant page.
13. Click **Finish**.

To deploy a FortiWeb-VM from a saved template and configure the virtual network settings

1. Log in to the VMware vSphere client. For details, see On your management computer, start VMware vSphere Client. on page 18.
2. Right-click the template that you want to use to deploy a FortiWeb-VM instance.
3. Select **Deploy VM from this Template**.
4. Enter a **Name** for the virtual machine. The maximum length is 80 characters.
5. For **Location**, select the folder or datacenter location in which you want to store the virtual machine.
6. Click **Next**.
7. Select a **Resource** for the virtual machine. This will handle all requests for the virtual machine.
8. Click **Next**.
9. Select a **Datastore Format** for the virtual machine's virtual disk and files:
   Same format as source—Use the same format as the FortiWeb-VM instance that you cloned to a template.
   Thick Provision Lazy Zeroed—Create a virtual disk that allocates space at the moment of creation. Any remaining data on the disk is zeroed out on first write from the FortiWeb-VM instance.

Thick Provision Eager Zeroed—Create a virtual disk that allocates space at the moment of creation. Any remaining data is zeroed out at the moment of creation.

Thin Provision—Create a virtual disk that allocates only as much space as initially needed. If the virtual disk requires more space at a later time, it will increase to the maximum capacity allocated to it.

10. Select a **Datastore Location** for the virtual disk:
    Store with the virtual machine—Store the virtual disk in the same location that you specified for the virtual machine.
    Browse—Select a datastore for the virtual disk.
    Disable Storage DRS for this virtual machine—Disable the Distributed Resource Scheduler (DRS) and select a datastore for the virtual disk.
11. Click **Next**.
12. For **Guest Customization**, select **Customize using the Customization Wizard**. You can configure:
    Computer Name
    Management Port IP
    DNS Servers
13. Review the virtual machine settings. If you need to change any settings, click **Back** until you find the relevant page.
14. Click **Finish**.

Configuring vSphere HA and Fault Tolerance

vSphere High Availability (HA) allows you to pool virtual machines and the hosts they reside on into a cluster. In the event of a failure, the HA feature restarts the virtual machines on a failed host on alternate hosts. This alternative to FortiWeb HA requires no HA configuration on the FortiWeb.

When you create a vSphere HA cluster, a single host automatically becomes the master host. The master host communicates with vCenter Server and monitors the state of all protected virtual machines and of the slave hosts.

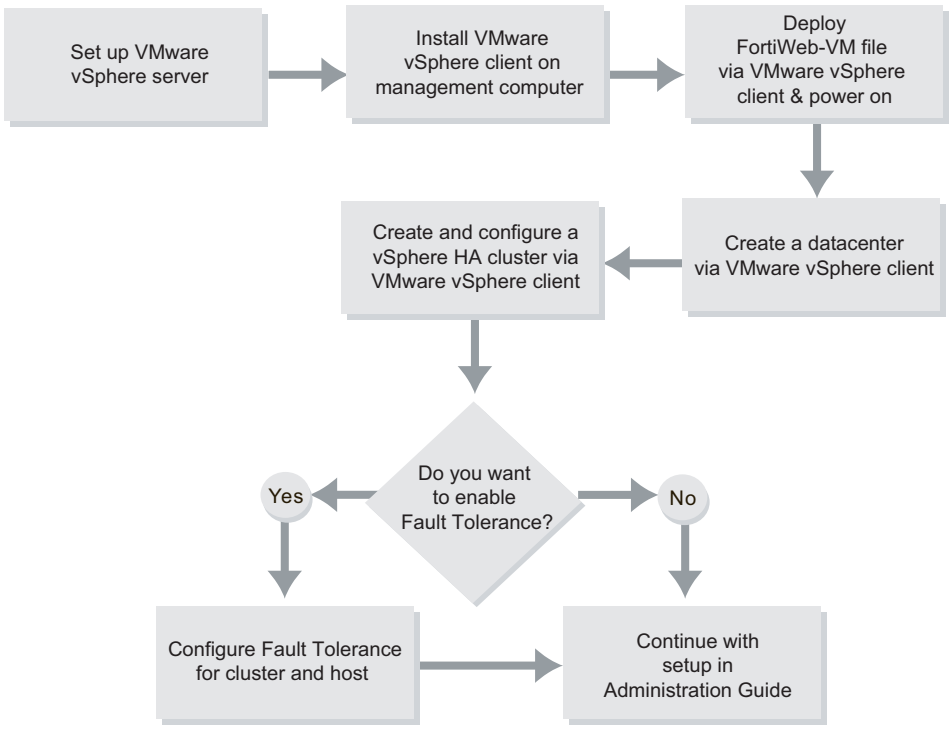
After you create a vSphere HA cluster, you can optionally enable Fault Tolerance (FT).

vSphere Fault Tolerance (FT) provides continuous availability by having identical virtual machines run in virtual lockstep on separate hosts. The lockstep mechanism captures activity and events on a primary virtual machine and sends them to a secondary VM.

To obtain optimal results from Fault Tolerance, ensure that you are familiar with how it works, how to enable it for your cluster and virtual machines, and FT best practices.

The key difference between VMware's Fault Tolerance and High Availability is how the failure of an ESXi host affects VM operation. Fault-tolerant systems instantly transition to a new host. For high-availability systems, the VMs fail with the host before restarting on another host.

Steps for configuring vSphere HA and Fault Tolerance



vSphere HA requirements

- VMware Infrastructure Suite Standard or Enterprise
- At least 2 VMware vSphere ESXi host systems
- A shared SAN or NAS between the ESXi servers where FortiWeb-VM is deployed. When a host system fails, ownership of its virtual machines is transferred from the failed host to the new host.
- CPU compatibility between the hosts

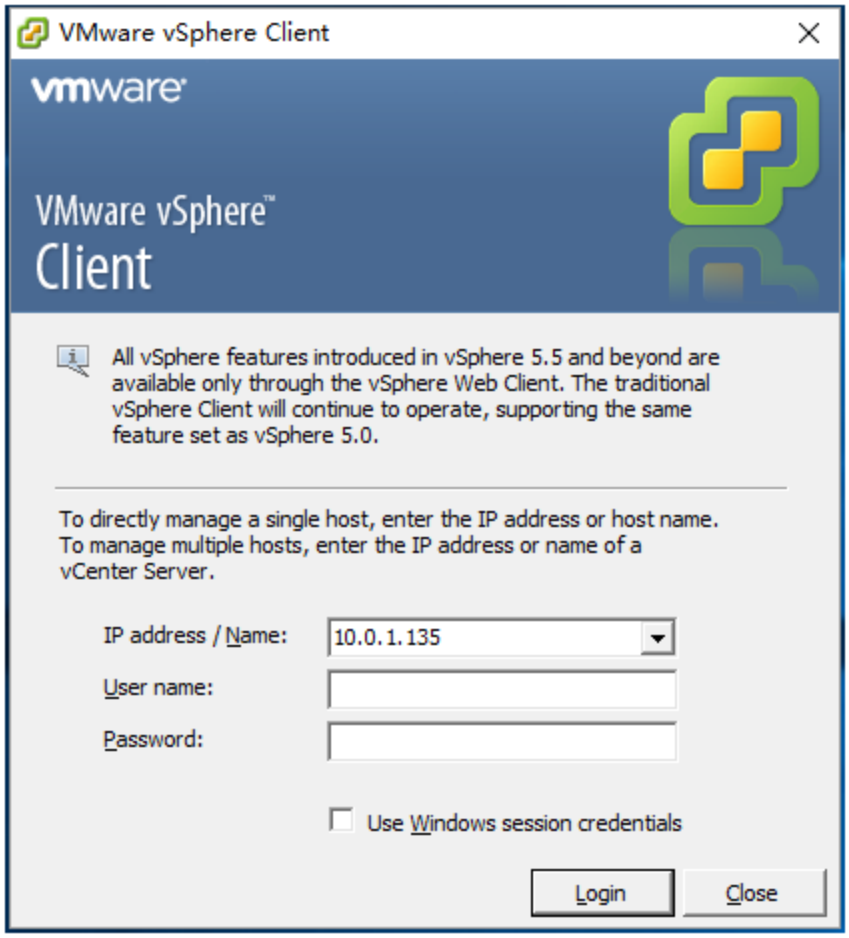
vSphere Fault Tolerance requirements

- Ensure the hosts use supported processors
- Ensure the hosts are licensed for Fault Tolerance
- Ensure the hosts are certified for Fault Tolerance. To determine if your hosts are certified, search the VMware Compatibility Guide by Fault Tolerant Compatible Sets.
- Ensure Hardware Virtualization (HV) is enabled in the BIOS for each host

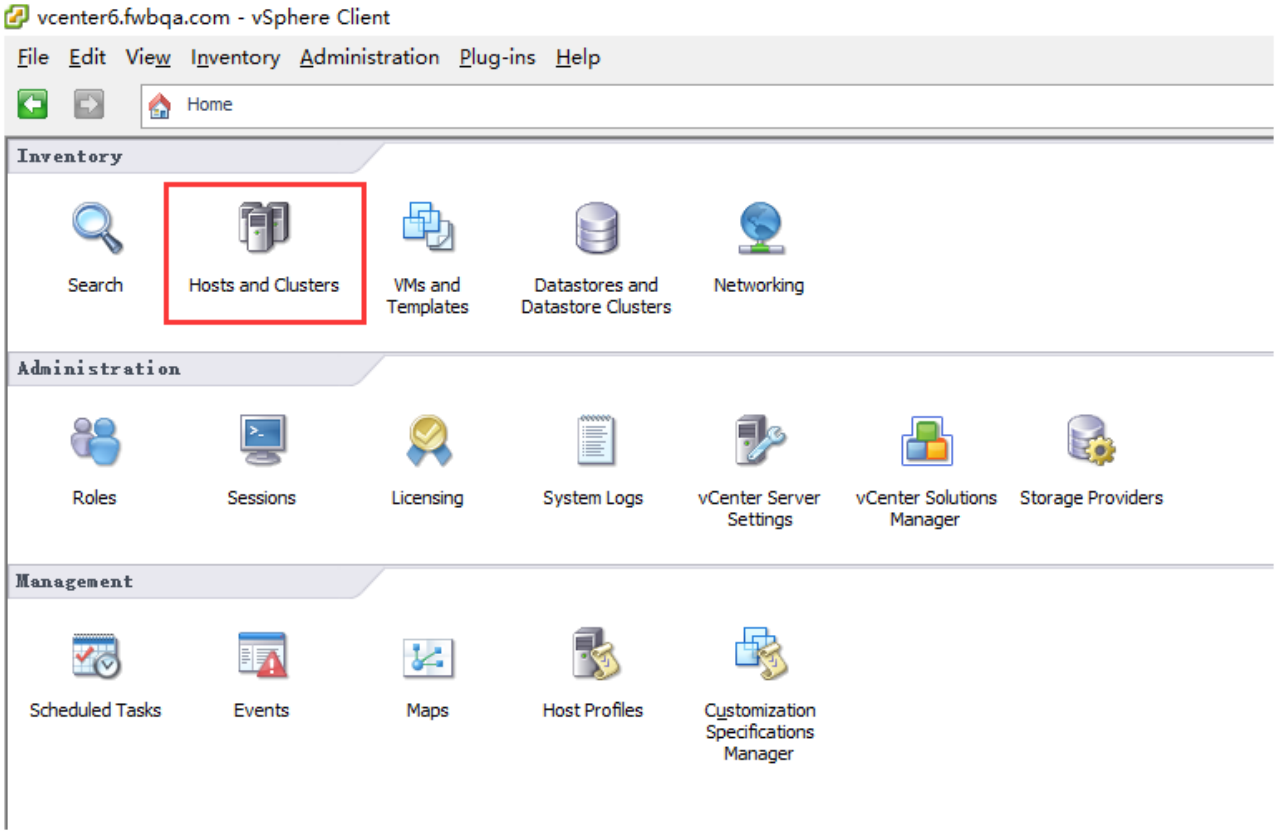
For more information on Fault Tolerance, see the topic "Providing Fault Tolerance for Virtual Machines" in ESXi and vCenter Server 5 Documentation.

To configure vSphere HA

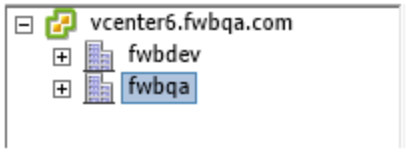
1. On your management computer, log in to VMware vSphere Client.


VMware vSphere Client
vmware
VMware vSphere™
Client
All vSphere features introduced in vSphere 5.5 and beyond are available only through the vSphere Web Client. The traditional vSphere Client will continue to operate, supporting the same feature set as vSphere 5.0.
To directly manage a single host, enter the IP address or host name.
To manage multiple hosts, enter the IP address or name of a vCenter Server.
IP address / Name:
10.0.1.135
User name:
Password:
Use Windows session credentials
Login
Close

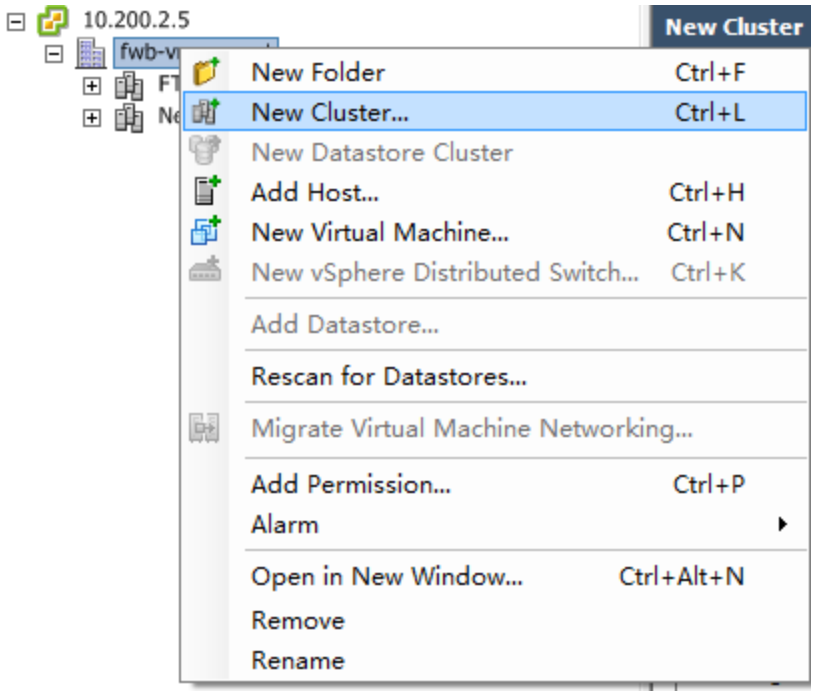
2. In the Home, under Inventory, click **Hosts and Clusters**.



3. Select **File > New > Datacenter**.
4. Rename the new datacenter. (In this example, it is `fwbqa`.)

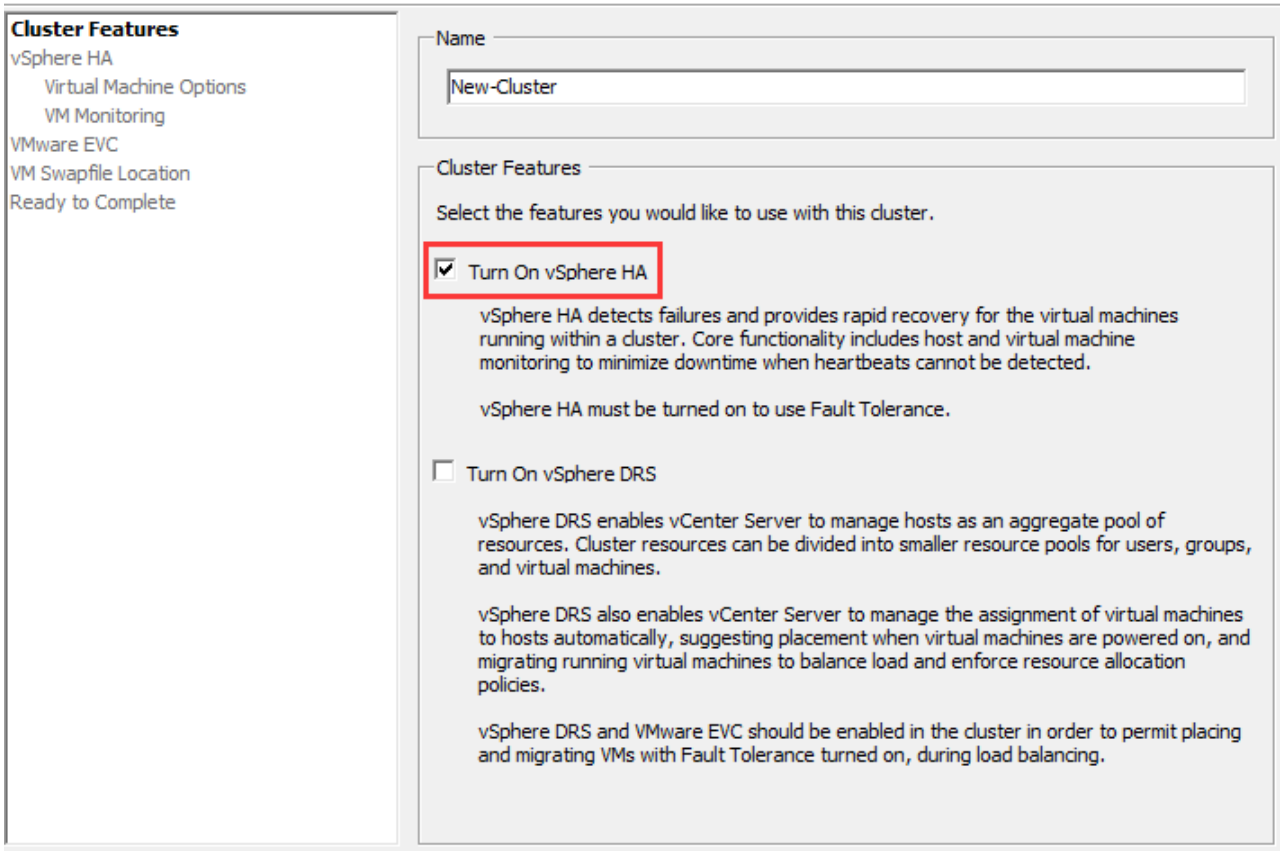


5. Right-click the datacenter, and then click **New Cluster**.



The New Cluster wizard is displayed.

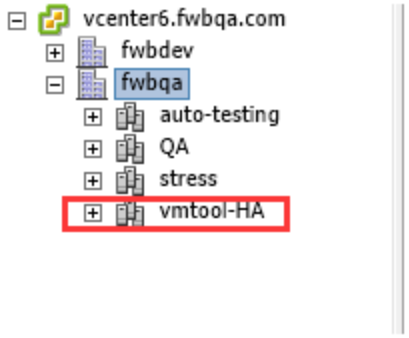
6. For **Name**, enter a name for the cluster, and then select **Turn On vSphere HA**.



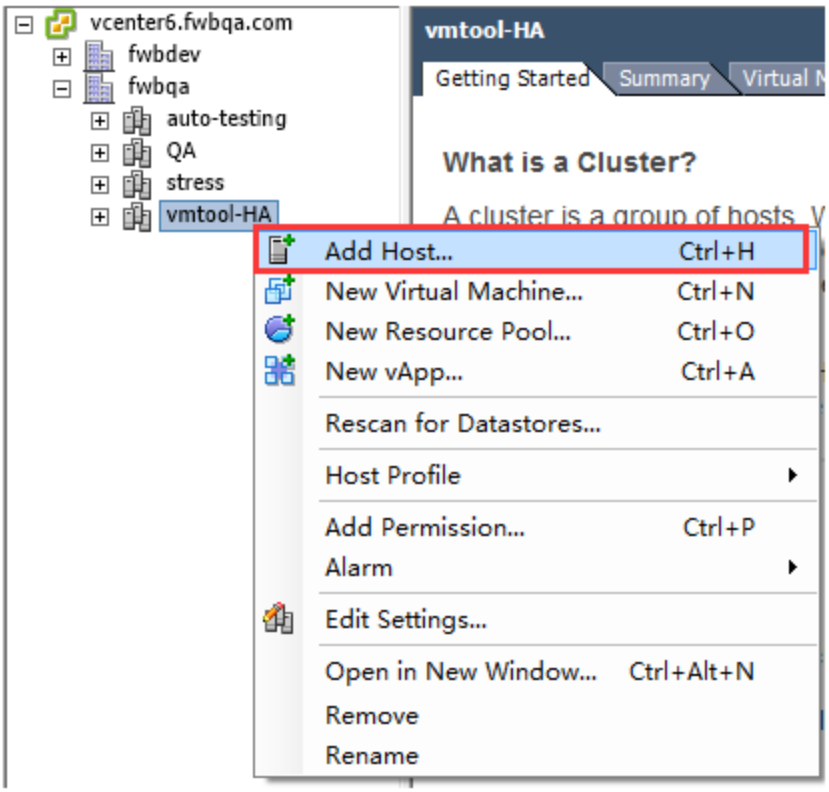
7. Navigate through the wizard to complete the configuration for your cluster.

   For information on the settings, see the topic "Configuring vSphere HA Cluster Settings" in ESXi and vCenter Server 5 Documentation.

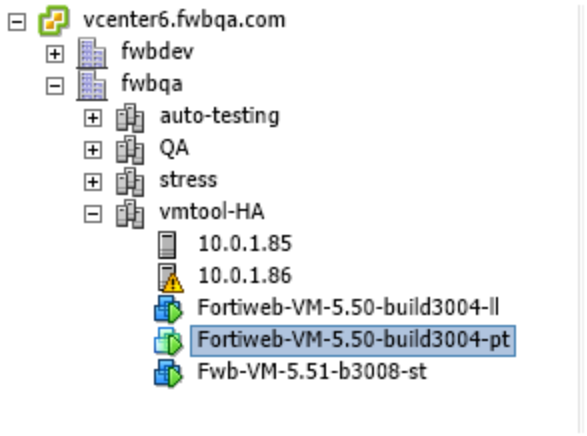
   The new cluster is displayed in the Inventory tree. (In this example, `vmtool-HA`.)



8. To add hosts to the cluster, right-click it, click **Add Host**.



9. Navigate through the wizard to add the hosts. (In this example, `10.0.1.85` and `10. 0.1.86`.)

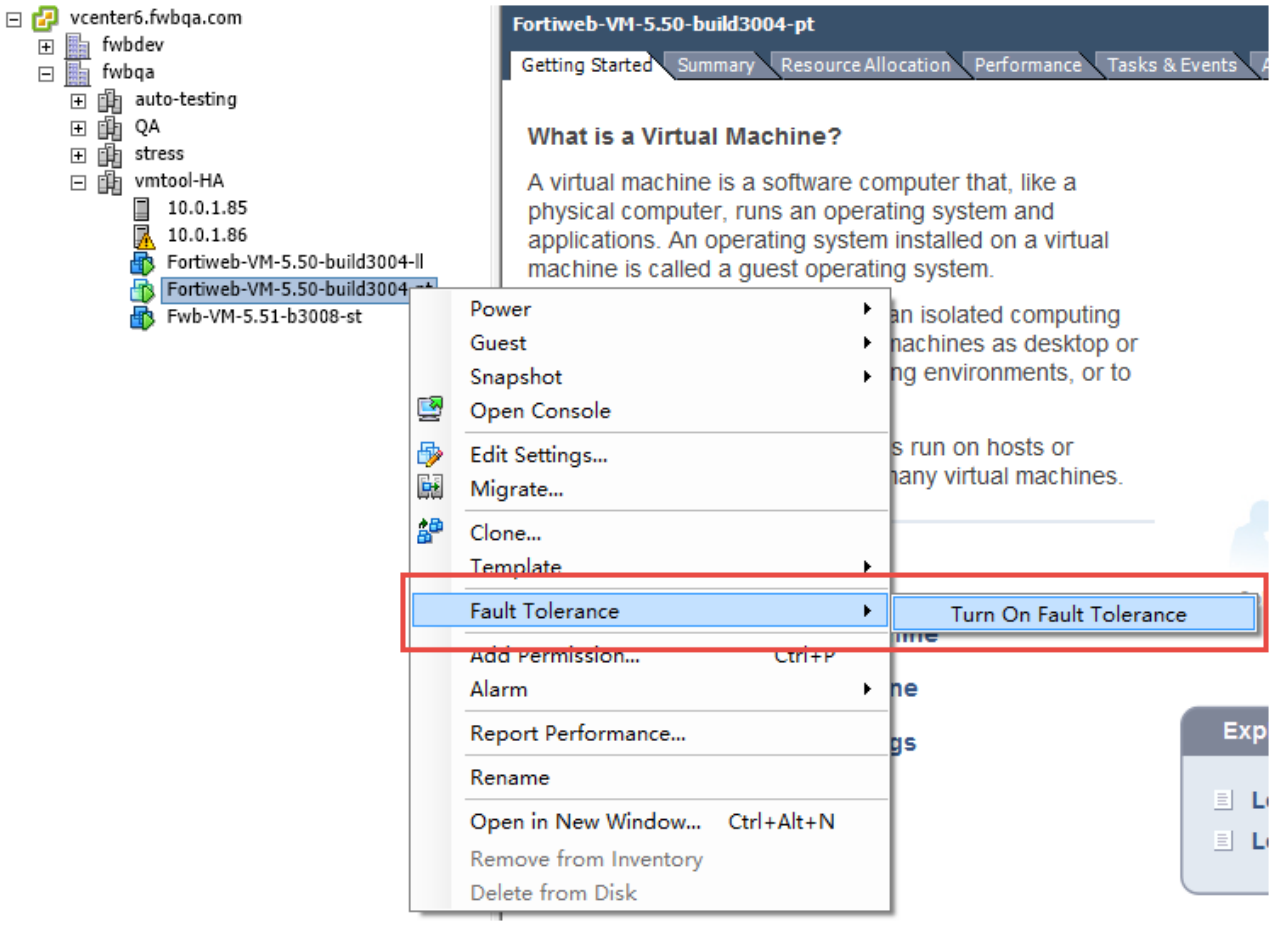


10. Select the cluster to view its settings and ensure that there are no configuration issues.

    For information on troubleshooting virtual machines, ESXi hosts, and clusters, see the topic "vSphere Troubleshooting" in ESXi and vCenter Server 5 Documentation.

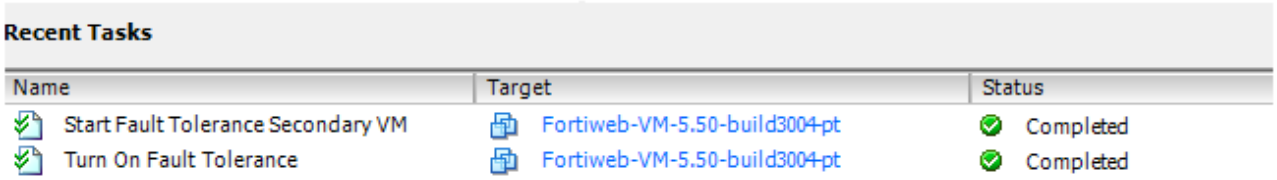
To configure vSphere FT

1. On your management computer, start VMware vSphere Client.
2. Right-click your virtual machine, and then click **Fault Tolerance > Turn On Fault Tolerance**.

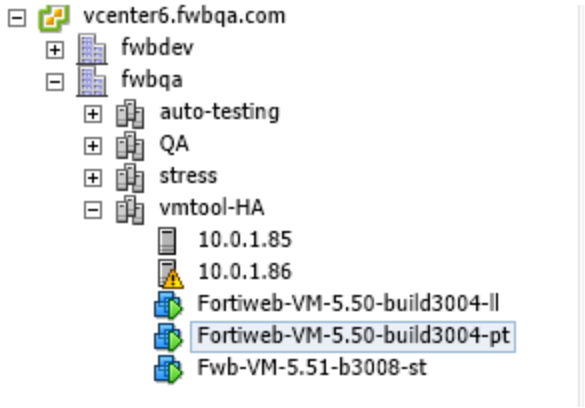


A confirmation dialog box is displayed.

3. Click **Yes** to confirm the feature activation.
4. Use the Recent Tasks panel to ensure there are no configuration issues.



The Inventory tree icons for VMs with FT are a different colour than VMs without FT.



Configuring vRealize Orchestrator

VMware vRealize Orchestrator is a development and process-automation tool that provides a library of extensible workflows. These workflows allow you to create and run automated, configurable processes to manage the VMware vSphere infrastructure as well as other VMware and third-party technologies. Orchestrator exposes vCenter Server API operations, which allows you to integrate them into your automated processes.

See the topics "Installing and Configuring VMware vRealize Orchestrator" and "Managing Workflows" in VMware vRealize Orchestrator 6.0 Documentation.

For example, you can create a workflow that modifies an existing virtual machine, including shutting down the guest operating system, renaming the machine, and modifying the memory. Go to the following location for more information:

www.vmwarebits.com/content/create-your-first-vcenter-orchestrator-workflow

VM Tools

When you deploy FortiWeb-VM on VMware vSphere, VM Tools is installed with the virtual machine. VM Tools allows FortiWeb-VM to work with native vSphere functionality, such as vSphere HA and Fault Tolerance and guest system shutdown and restart.

However, because the version of VM Tools included with FortiWeb-VM is Open VM Tools, you cannot install or upgrade the tools using the **Install/Upgrade VMware Tools** option from the toolbar or vCenter server. Instead, updates are included with FortiWeb-VM updates.

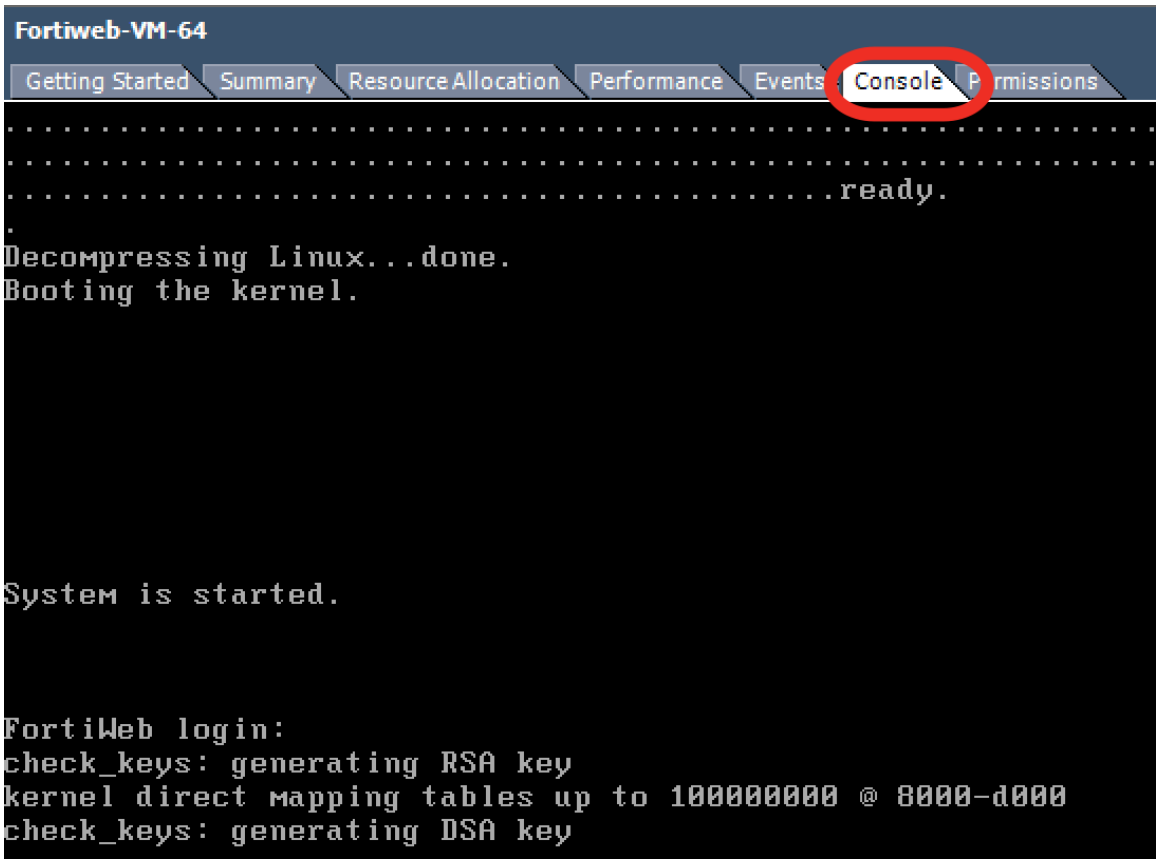
Configuring access to FortiWeb's web UI & CLI

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:
   - VMware vSphere Client
2. Log in to the VM server.
3. Open the console of the FortiWeb-VM virtual appliance.
   On VMware vSphere Client:
   - In the pane on the left side, select the name of the virtual appliance, such as **FortiWeb-VM**.
   - Click the **Console** tab.

   Console tab in VMware vSphere Client



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 32)
   - `<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*.

9. Continue by uploading the license file. (See Uploading the license on page 58. 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 66.

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 58.

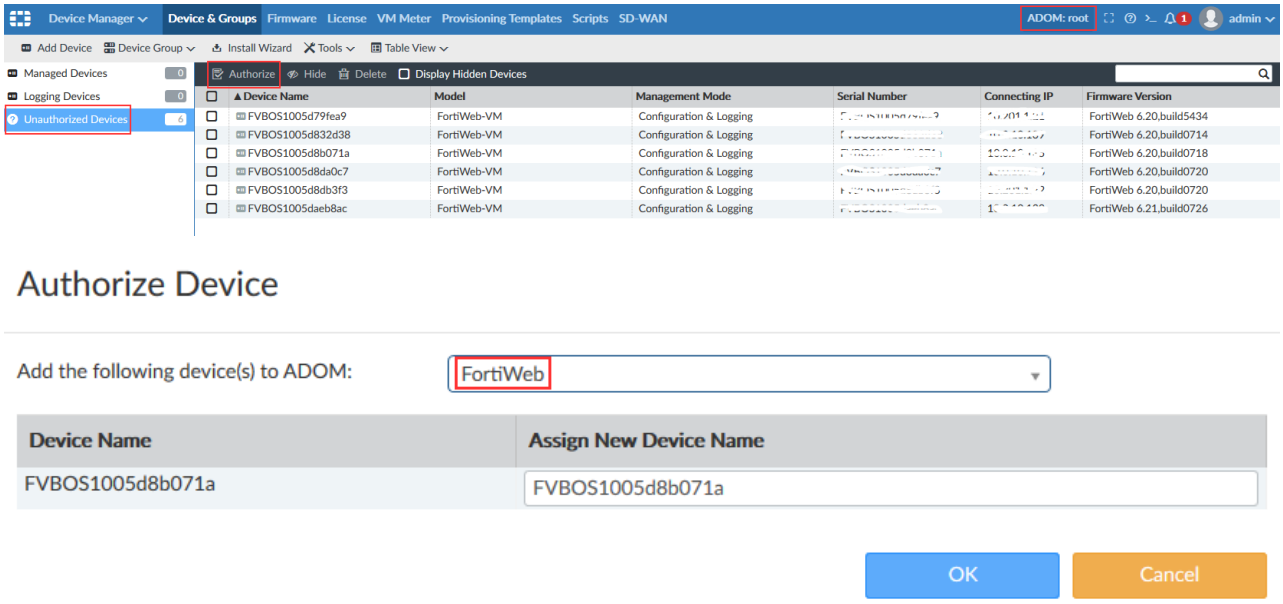
Additional operations if you deploy the PAYG image

For FortiWeb PAYG image, you need to use a FortiManager to manage the FortiWeb-VM and meter the usage. The FortiManager should meet the following requirements:

- Online.
- Registered with VM Meter contract.
- Having an ADOM for FortiWeb devices. For how to add ADOM, refer to the section "Administration Domains" in FortiManager Administration Guide.

Perform the following steps to authorize FortiWeb-VM in FortiManager.

1. In FortiWeb-VM, enable Central Management so that FortiManager can discover and manage FortiWeb.
   For FortiWeb-VM PAYG image, you are required to enter the FortiManager's IP address for central management during the deployment process.
   Or, run the following command in FortiWeb to enable central management.
   ```
   config system centmgmt
      set serveraddr <the-ip-address-of-FortiManager>
   end
   ```
2. Authorize FortiWeb-VM in FortiManager for central management.
   In FortiManager, go to **root** ADOM. Select **Unauthorized Devices**. Check the box before the FortiWeb-VM, then click **Authorize** to add this device to **FortiWeb** ADOM. For more information on how to authorize a device for central management, refer to the section "Authorizing devices" in FortiManager Administration Guide.



3. Authorize FortiWeb-VM in FortiManager for metering.
   In FortiManager, go to **FortiWeb** ADOM, then select **Device Manager > VM Meter**. Check the box before the FortiWeb-VM, then click **Authorize**. For more information on how to authorize FortiWeb-VM for metering, refer to the section "Authorizing FortiWeb VMs" in FortiManager Administration Guide.

Now the FortiWeb-VM is valid and can update services from FortiGuard without Internet.

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 contact 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 way.

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.

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://.)

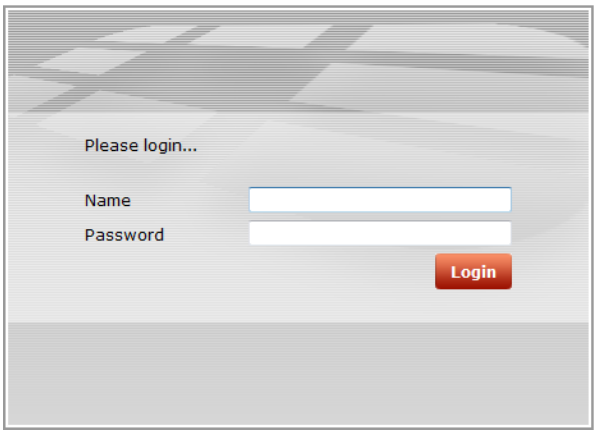
     Initially, you must access the web UI via HTTPS. By default, HTTP is not enabled. After uploading the license, you can configure the administrative access protocols. For details, see the *FortiWeb Administration Guide*.

   - 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**.

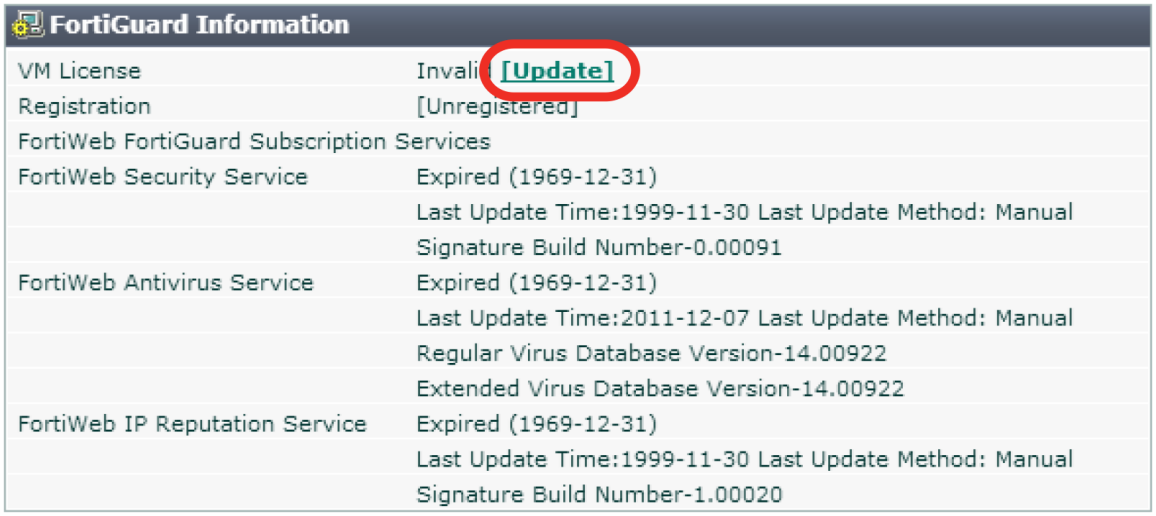
To support HTTPS authentication, the FortiWeb appliance ships with a self-signed X.509 certificate, which it presents to clients whenever they initiate an HTTPS connection to the FortiWeb appliance. When you connect, depending on your web browser and prior access of the FortiWeb appliance, your browser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

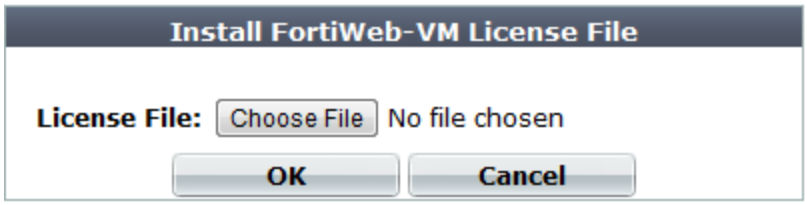
Both warnings are normal for the default certificate.

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



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



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

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:

GUI item	Description
	• **Valid** — The appliance has a valid, non-trial license. **Serial 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 64. • **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 55.

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 59.
4. Continue with What's next?.

Updating the license for more vCPUs

If either:

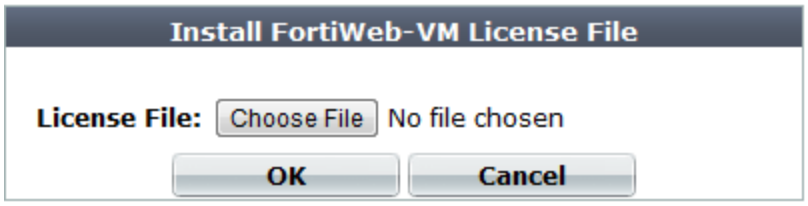
- you want to upgrade FortiWeb-VM to a license with a higher vCPU limit
- your original FortiWeb-VM license was an extended (but temporary) evaluation license, and you have now purchased a permanent, paid license

you must upload a new license file.

To replace an evaluation license with a paid license, use Uploading the license on page 58.

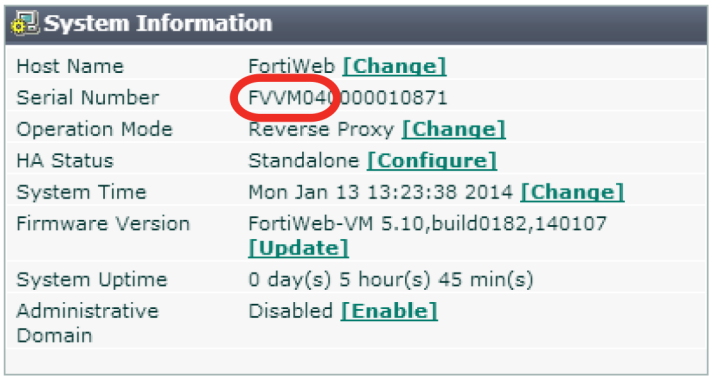
To allocate more vCPUs

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 58.



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 one of the following topics:
   - Configuring the number of virtual CPUs (vCPUs) on page 28 (VMware vSphere)
   - Configuring the number of virtual CPUs (vCPUs) on page 1 (Citrix Xen)
   - Deploying via Virtual Machine Manager on page 1 (Xen Project)
   - Configuring the number of virtual CPUs (vCPUs) on page 1 (Hyper-V)
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.



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.

Updating the virtual hardware

By default, FortiWeb-VM uses VMware virtual hardware version 5. If you need to update your FortiWeb-VM's virtual hardware, shut down FortiWeb-VM before doing so.

For example, if you have a VMware vSphere ESXi 5.1 environment that supports virtual hardware version 9, and you want to provide version 9 feature support such as backups to FortiWeb-VM, you would update the virtual hardware.

For more information on virtual hardware, see:

http://kb.vmware.com/selfservice/documentLinkInt.do?micrositeID=&popup=true&languageId=&externalID=1010675

To update the virtual hardware

1. Shut down FortiWeb-VM. To do this, you can enter the CLI command:
   ```
   execute shutdown
   ```
2. In VMware vCenter, right-click the VM and select the option to upgrade the virtual hardware.
3. When the upgrade is complete, power on FortiWeb-VM.