



# FortiWeb-VM on Microsoft Hyper-V

**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](mailto:techdoc@fortinet.com)



---

# TABLE OF CONTENTS

<b>Overview of FortiWeb-VM</b> .....	<b>4</b>
Benefits .....	4
Architecture .....	5
Licensing .....	7
Flex-VM .....	8
Evaluation limitations .....	8
FortiWeb Manager virtual machine .....	8
<b>About this document</b> .....	<b>10</b>
Scope .....	10
Conventions .....	10
IP addresses .....	10
Cautions, notes, & tips .....	11
Typographical conventions .....	11
Command syntax conventions .....	12
<b>System requirements</b> .....	<b>15</b>
<b>Downloading the FortiWeb-VM license &amp; registering with Technical Support</b>	<b>16</b>
<b>Downloading the FortiWeb-VM software</b> .....	<b>17</b>
<b>Importing the FortiWeb-VM virtual machine</b> .....	<b>18</b>
<b>Resizing the virtual disk</b> .....	<b>22</b>
<b>Configuring the number of virtual CPUs (vCPUs)</b> .....	<b>24</b>
Updating the license for more vCPUs .....	25
<b>MAC address spoofing</b> .....	<b>27</b>
<b>Mapping the virtual NICs (vNICs) to physical NICs</b> .....	<b>28</b>
Configuring the vNetwork for the transparent modes .....	28
<b>Starting the FortiWeb-VM</b> .....	<b>30</b>
<b>Configuring access to FortiWeb's web UI &amp; CLI</b> .....	<b>31</b>
<b>Uploading the license</b> .....	<b>34</b>
License Validation .....	34
Uploading the license .....	35
Updating the license for more vCPUs .....	40
<b>What's next?</b> .....	<b>42</b>

# Overview of FortiWeb-VM

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

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

## Benefits

FortiWeb is designed specifically to protect web servers.

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

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

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

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

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

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

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

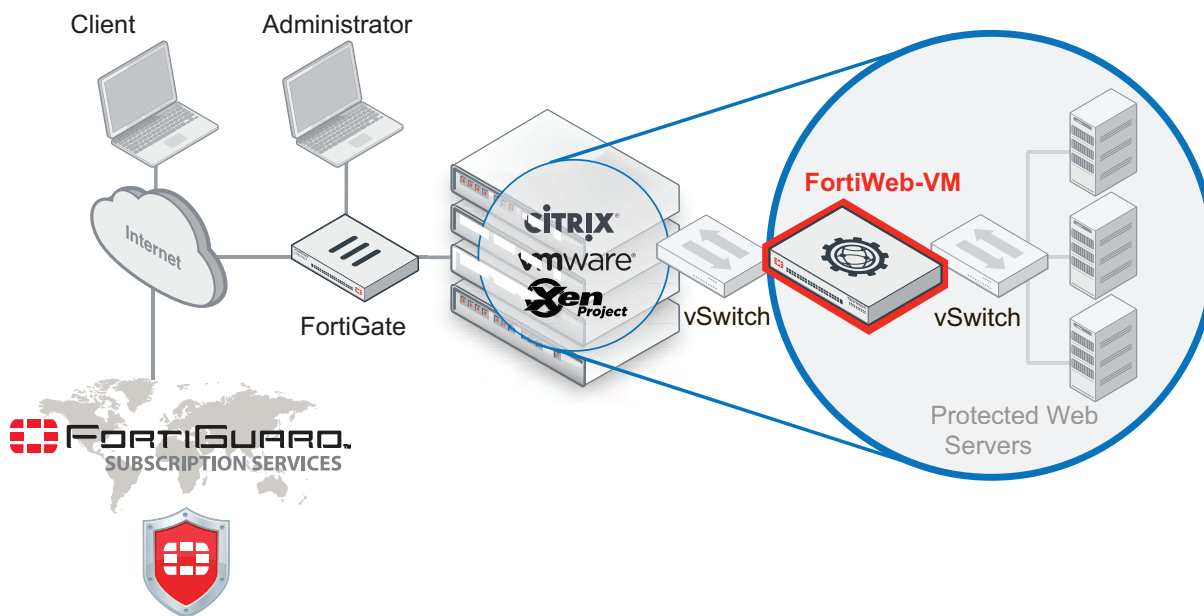
FortiWeb significantly reduces deployment costs by consolidating WAF, hardware acceleration, load balancing, and vulnerability scanning into a single device with no per-user pricing. Those features drastically reduce the time required to protect your regulated, Internet-facing data and eases the challenges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

## Architecture

FortiWeb-VM is deployed in the following environments:

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

### FortiWeb-VM network topology



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

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

FortiWeb-VM requires Internet connectivity.

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

---

## Licensing

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

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

The FortiWeb-VM licenses specify the size of the virtual appliance you can deploy. It's not allowed to import license to a virtual machine with greater vCPU number than the license specifies. 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
<b>Virtual CPUs (vCPUs)</b>	1	2	4	8	16

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 34](#).

---

---

## Flex-VM

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

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

### To get the Flex-VM license file:

1. Get the token on Support site. Refer to [this article](#).

2. Run the following command in FortiWeb CLI:

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

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

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

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

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

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

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

## Evaluation limitations

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

- High availability (HA)
- FortiGuard updates
- Technical support

You do not need to manually upload the trial license. It is built-in. The trial period begins the first time you start FortiWeb-VM.

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

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

## FortiWeb Manager virtual machine

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



---

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

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

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

# About this document

## Scope

This document provides the following information:

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

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

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

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

Convention	Description
	<ul style="list-style-type: none"><li data-bbox="477 254 1300 317">• <code>&lt;xxx_int&gt;</code> — An integer number that is <b>not</b> another data type, such as 15 for the number of minutes.</li></ul>

## System requirements

FortiWeb-VM supports the following hypervisor versions:

- Microsoft Hyper-V (version 6.2 or higher, running on Windows 8 or higher, or Windows Server 2012/2016/2019/2022)



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](#).

# Importing the FortiWeb-VM virtual machine

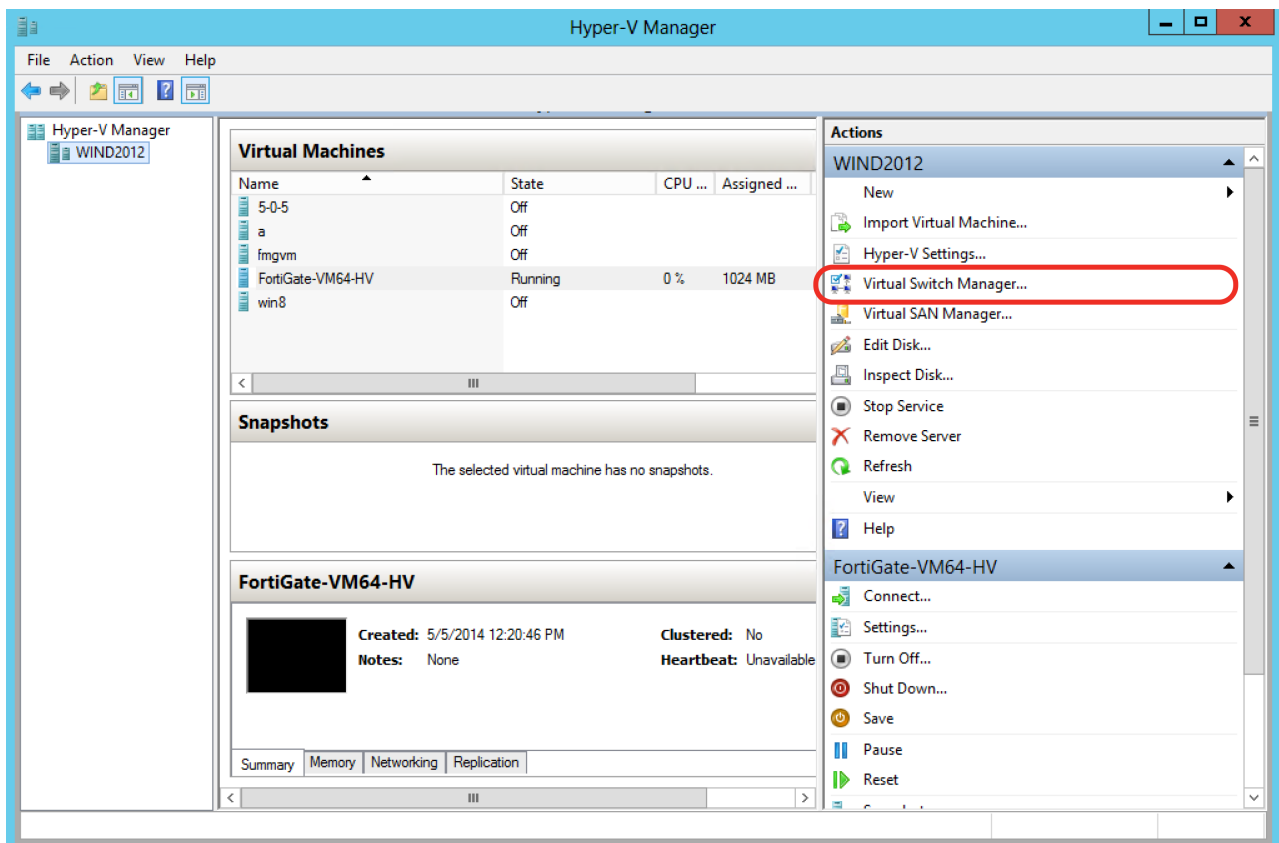
You deploy FortiWeb-VM on Hyper-V by importing a virtual machine.

These instructions create a virtual switch named `vmnet`. The FortiWeb-VM virtual machine you import uses a virtual switch with this name by default.

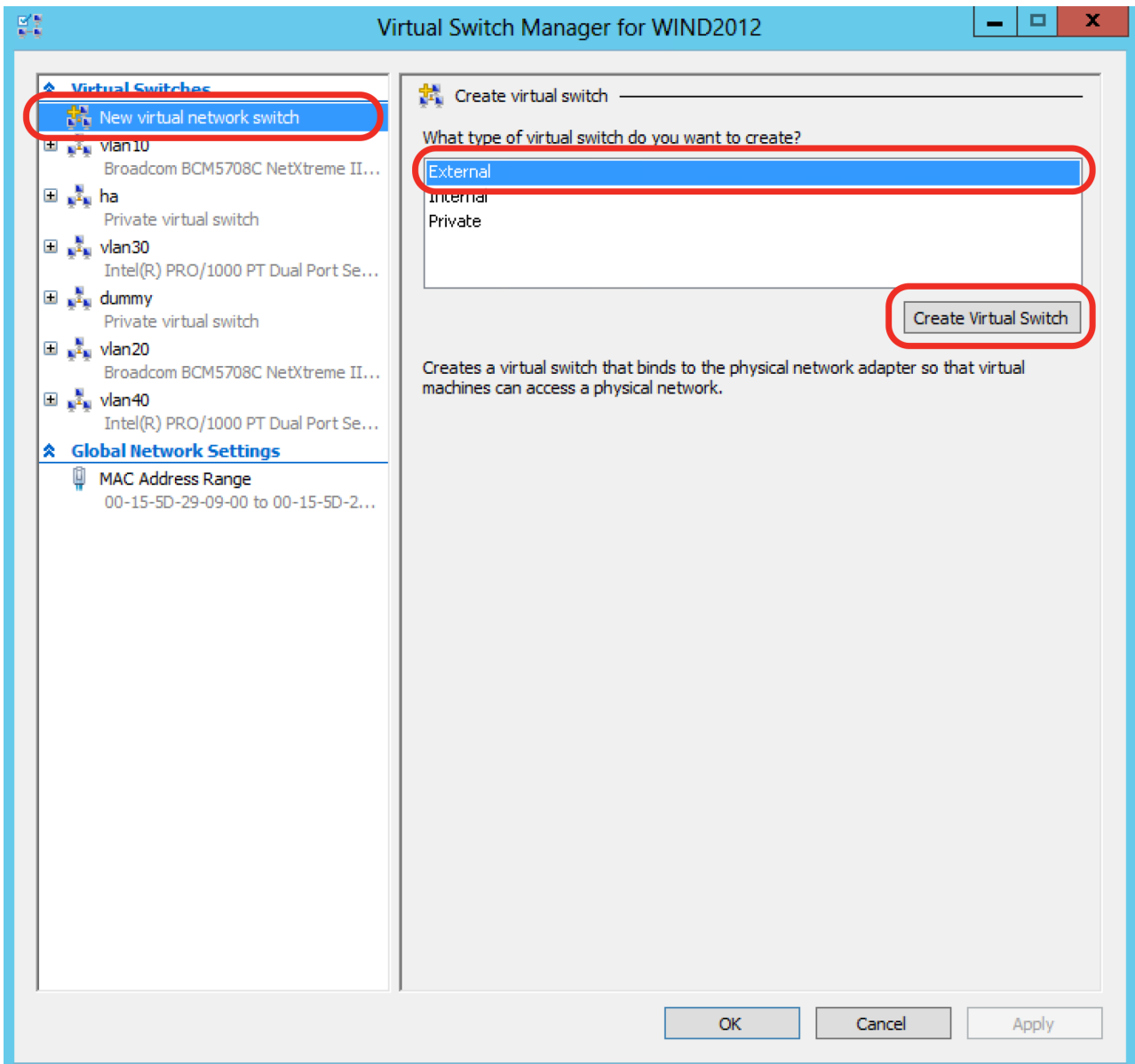
Alternatively, you can use an existing virtual switch or one with different name. You are prompted to select the switch you want to use when you import the virtual machine.

## To import the FortiWeb-VM virtual machine

1. In the Hyper-V Manager, under **Actions**, click **Virtual Switch Manager**.

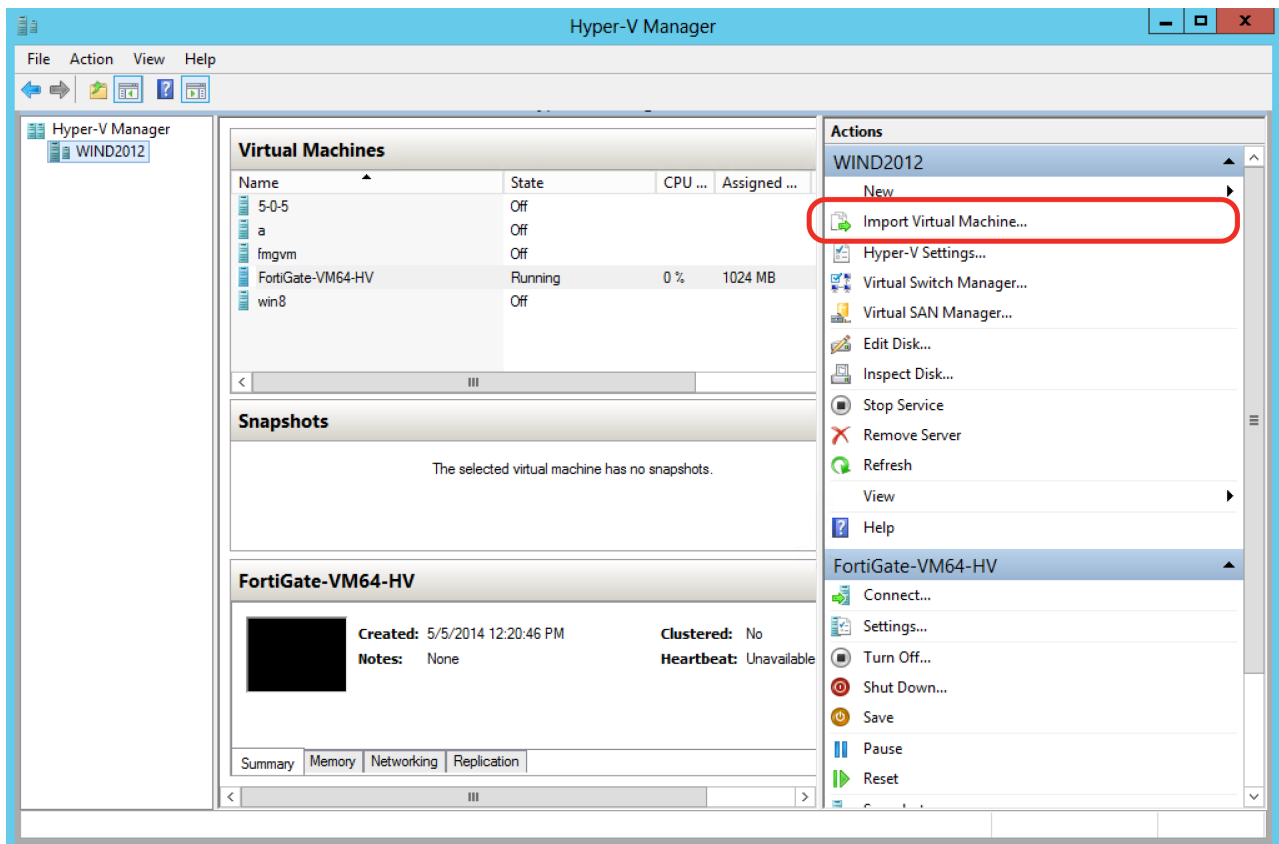


2. Under **Virtual Switches**, click **New virtual network switch**, click **External**, and then click **Create Virtual Switch**.



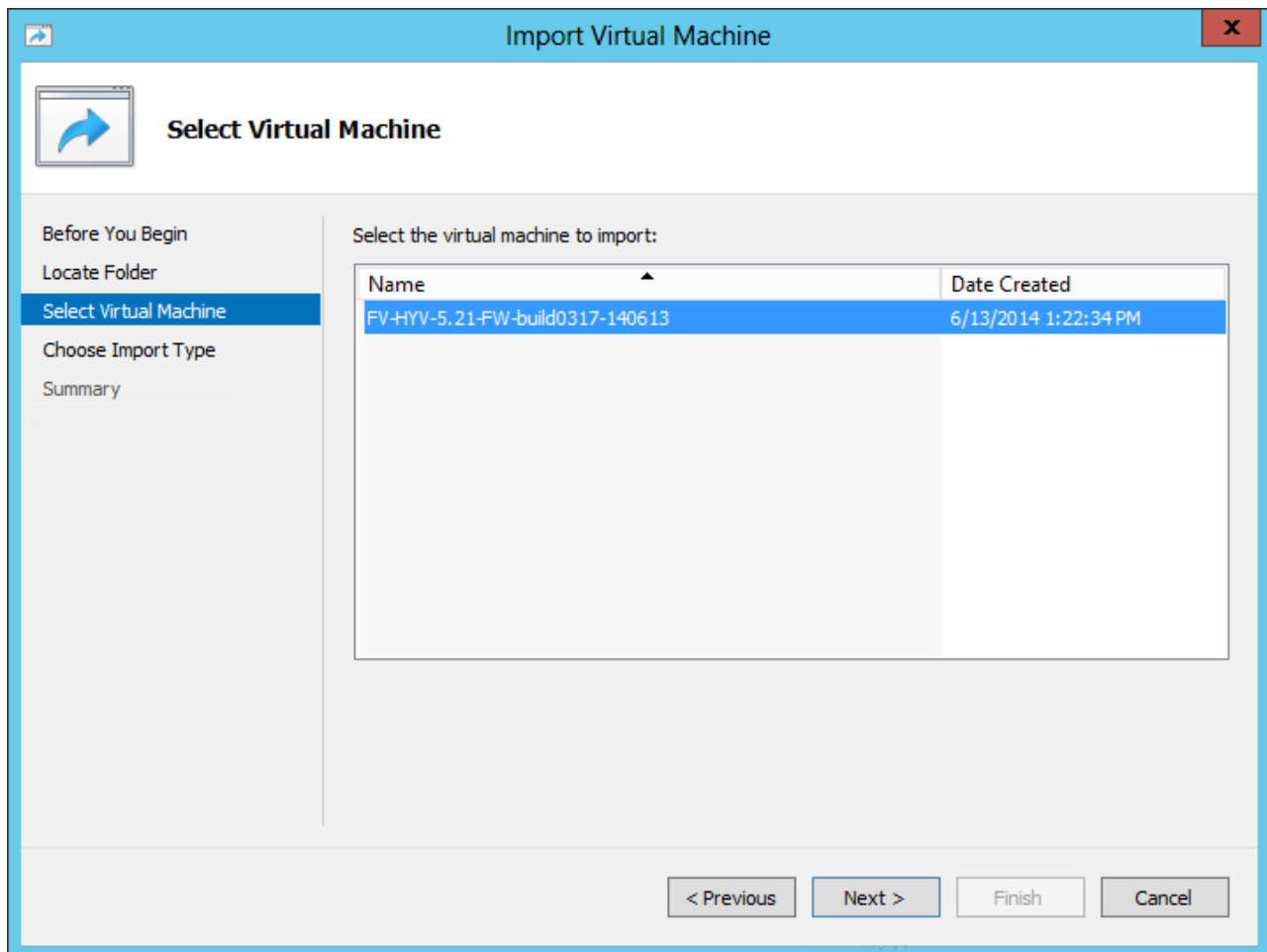
3. Under **Virtual Switch Properties**, for **Name**, enter `vmnet`.  
For all other settings, use the default values.
4. Click **OK**.
5. Extract the `.zip` archive's contents to a folder that you can access from the Hyper-V Manager.

6. In Hyper-V Manager, under **Actions**, click **Import Virtual Machine**.



7. In the **Import Virtual Machine** wizard, navigate to the **Locate Folder** page.
8. For **Folder**, specify the folder that contains the contents of the `.zip` file, and then click **Next**.

- On the **Select Virtual Machine** page, select the name of the FortiWeb-VM virtual machine, and then click **Next**.



- On the **Choose Import Type** page, select **Copy the virtual machine (create a new unique ID)**, and then click **Next**.
- On the **Choose Folders for Virtual Machine Files** page, preserve the default values or specify the folders where you want to store the virtual machine. Then, click **Next**.
- On the **Locate Virtual Hard Disks** page, for **Location**, specify the folder where you extracted the contents of the `.zip` file, and then click **Next**.
- On the **Choose Storage Folders to Store Virtual Hard Disks** page, preserve the default value or specify a different folder. Then, click **Next**.
- On the **Completing Import Wizard** page, review the settings, and then click **Finish**.



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.

## Resizing the virtual disk

The virtual disk size of the imported FortiWeb-VM virtual machine is 30G (the default size for a Hyper-V virtual machine).



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 deletes all data on that disk.** For backup instructions, see the [FortiWeb Administration Guide](#).

---

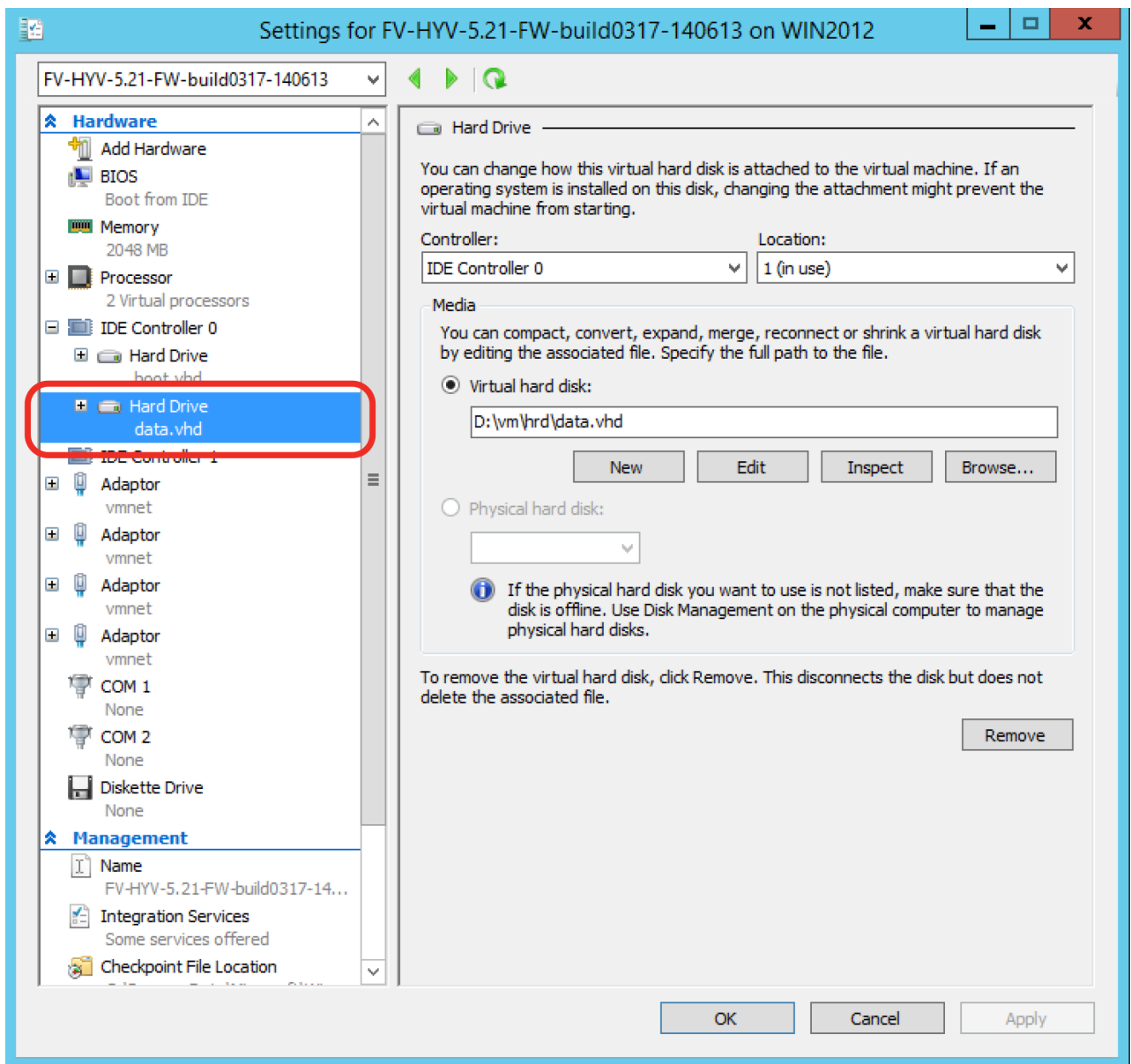


You shut down the FortiWeb-VM to resize the vDisk.

---

### To increase the size of the virtual hard disk

1. Shut down the FortiWeb-VM virtual machine (**Actions > Shut Down**).
2. Select the FortiWeb-VM virtual machine in the list of machines, and then, under **Actions**, click **Settings**.
3. Under **Hardware**, expand the IDE Controller item that contains the machine's hard drives, and then select the hard drive `data.vhd`.



4. In the hard drive settings, under Media, ensure that **Virtual hard disk** is selected, click **Edit**, and then use the Edit Virtual Hard Disk wizard to expand the size of the virtual disk.
5. Start the virtual machine (**Actions > Start**).
6. Using the CLI, log in to FortiWeb and use the following command to reformat the log disk:
 

```
execute formatlogdisk
```

After a reboot, the disk operates at the new size.

## 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 from 1 to 10 vCPUs for an appliance.



If you need to increase or decrease the vCPUs after the initial boot, shut down FortiWeb-VM, adjust the number of vCPUs, then see [Updating the license for more vCPUs on page 40](#).

---

### To change the number of vCPUs

---

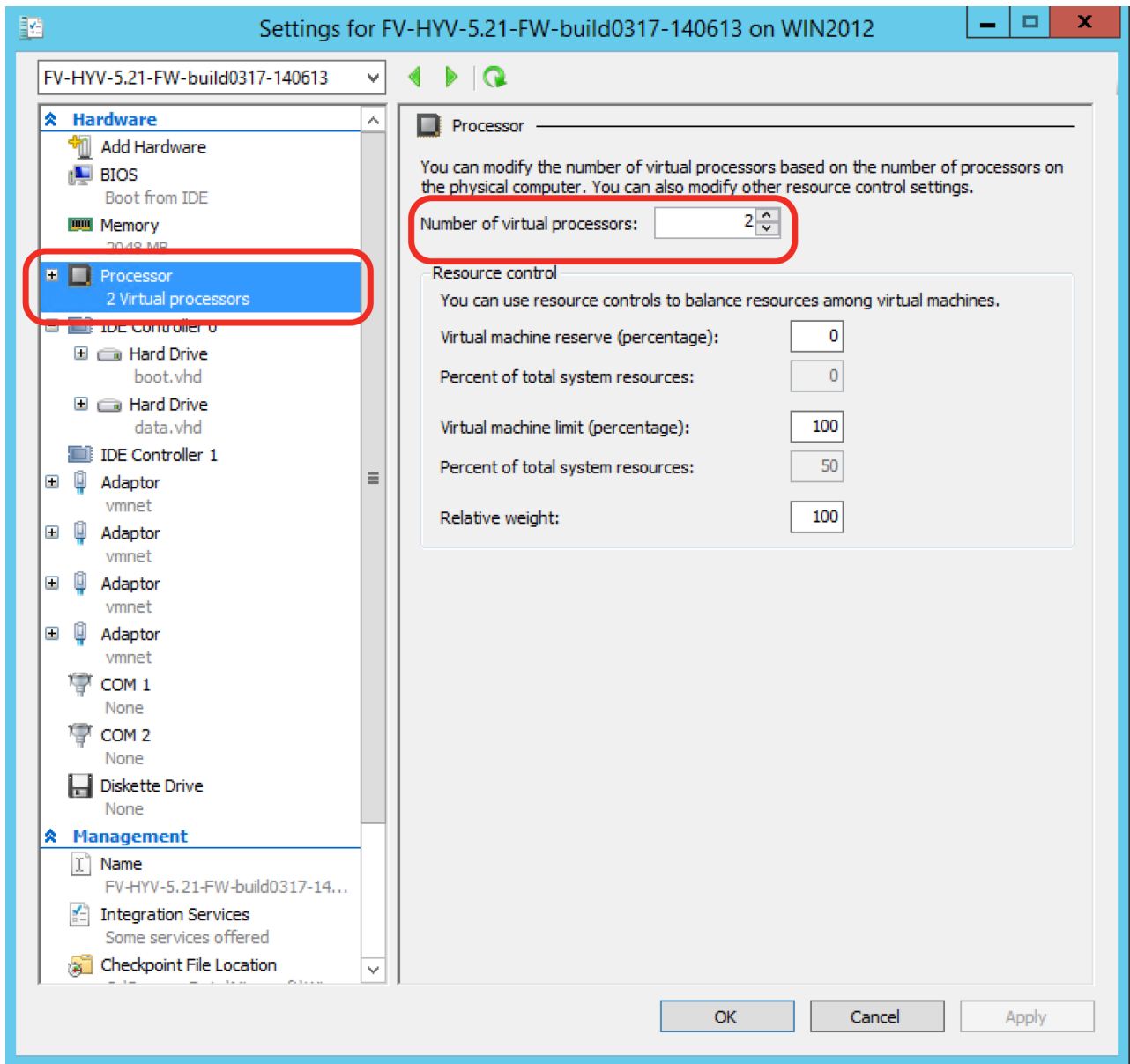


You shut down FortiWeb-VM to resize the vCPU.

---

1. Shut down the virtual machine (**Actions > Shut Down**).
2. Select the FortiWeb-VM virtual machine in the list of machines, and then, under **Actions**, click **Settings**.
3. Under **Hardware**, select the **Processor** item, and then use the Processor settings to increase or decrease the number of vCPUs.





4. Click **OK** and then start the machine.

## Updating the license for more vCPUs

If either:

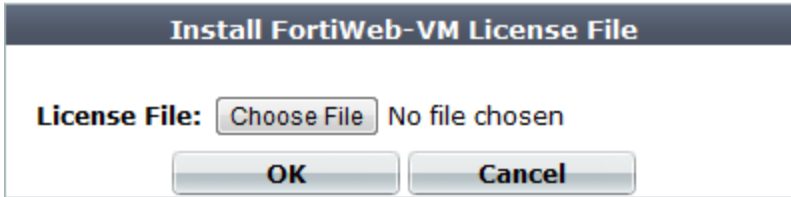
- you want to upgrade FortiWeb-VM to a license with a higher vCPU limit
- your original FortiWeb-VM license was an extended (but temporary) evaluation license, and you have now purchased a permanent, paid license

you must upload a new license file.

To replace an evaluation license with a paid license, use [Uploading the license on page 34](#).

**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 34](#).



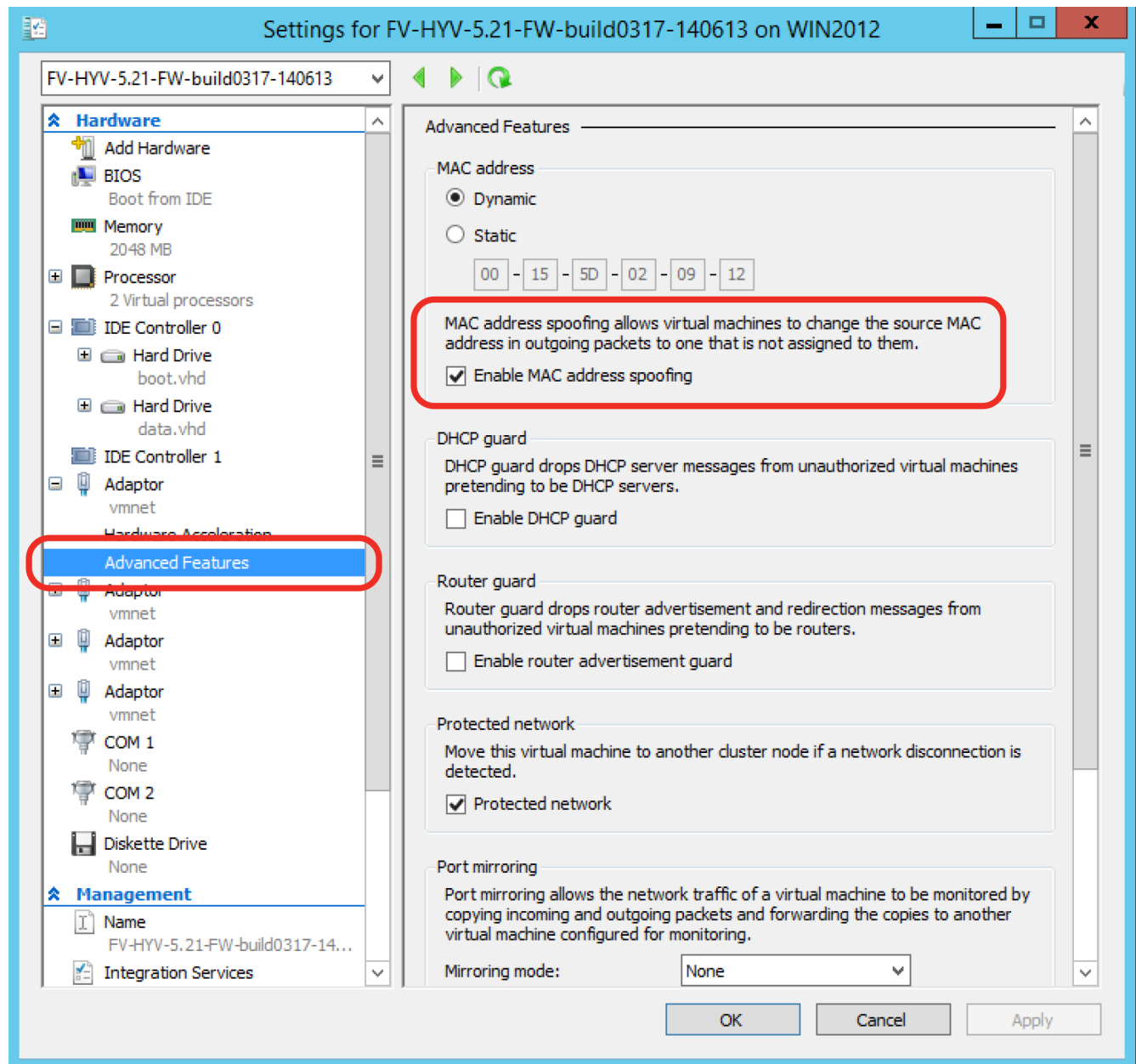
4. In the **System Information** widget, click **Shut Down**.  
The virtual appliance will flush its data to its virtual disk, and prepare to be powered off. If you skip this step and immediately power off FortiWeb-VM, you may lose buffered data.
5. On your management computer, start your central management 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 <a href="#">[Change]</a>
Serial Number	FVVM040000010871
Operation Mode	Reverse Proxy <a href="#">[Change]</a>
HA Status	Standalone <a href="#">[Configure]</a>
System Time	Mon Jan 13 13:23:38 2014 <a href="#">[Change]</a>
Firmware Version	FortiWeb-VM 5.10,build0182,140107 <a href="#">[Update]</a>
System Uptime	0 day(s) 5 hour(s) 45 min(s)
Administrative Domain	Disabled <a href="#">[Enable]</a>

## MAC address spoofing

To operate correctly, FortiWeb-VM virtual switches require MAC address spoofing. When you create a virtual switch, this option is enabled by default.

To access the option, in the settings for the virtual machine, under Hardware, expand the virtual switch item, and then select **Advanced Features**.



## Mapping the virtual NICs (vNICs) to physical NICs

When you import the FortiWeb-VM package, the import process creates 4 bridging vNICs and automatically maps them to a port group on 1 virtual switch (vSwitch) within the hypervisor (the default name of this vSwitch is `vmnet`). Each of the 4 network interfaces in FortiWeb-VM uses one of these vNICs. (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 many cases, you do not need to change the default mappings of the FortiWeb-VM network adapter ports to the host computer's physical ports.

You can change the mapping, or map other vNICs, if either your VM environment requires it or you want the FortiWeb-VM to operate in either True Transparent Proxy or Transparent Inspection mode. (See [Configuring the vNetwork for the transparent modes on page 28.](#))

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

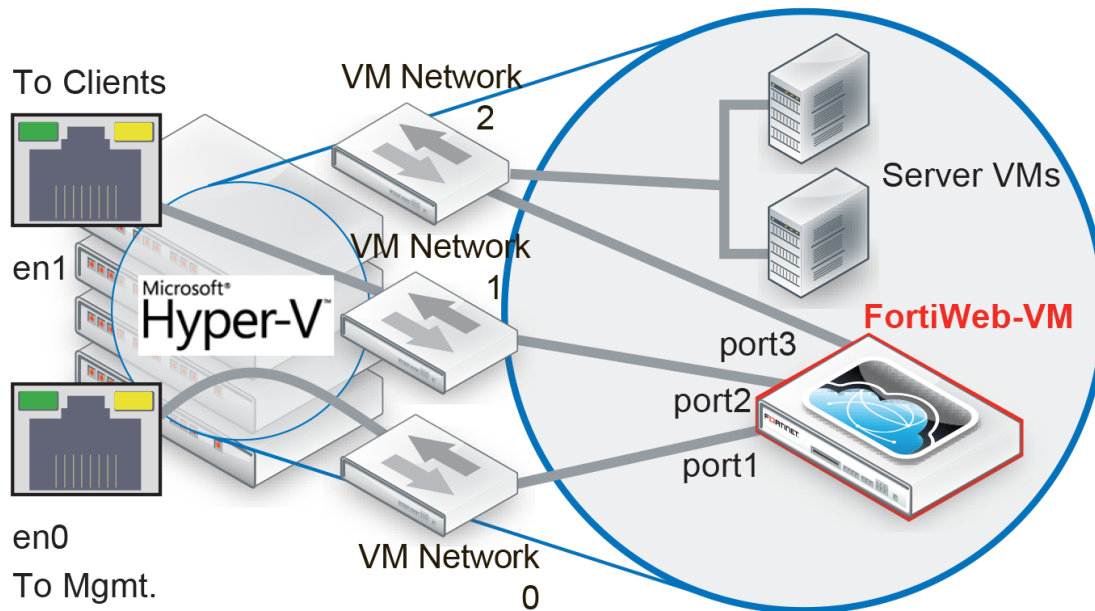
## Configuring the vNetwork for the transparent modes

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

To support the transparent modes, you **must**:

- ensure a total of at least three network cards are available to Hyper-V
- add 2 vSwitches for the bridge: one for the web server side, and one for the client side
- map the new vSwitches to a network adapter (vNIC)

Similar to a deployment that does not use virtual machines, connections between clients and servers are piped through the two vSwitches that comprise the bridge, with FortiWeb-VM in between them.



### To create a vSwitch

1. In the Hyper-V Manager, under **Actions**, click **Virtual Switch Manager**.
2. Under **Virtual Switches**, click **New virtual network switch**, click **External**, and then click **Create Virtual Switch**.
3. Under **Virtual Switch Properties**, for **Name**, enter a network label that identifies the port group.  
For example, `Client-Side-vSwitch1`.  
For all other settings, use the default values.
4. Click **OK**.
5. Repeat this procedure to create the other vSwitch.  
For example, create a vSwitch with the name `Server-Side-vSwitch2`.
6. In the list of virtual machines, select the FortiWeb-VM machine, and then click **Settings**.
7. Under **Hardware**, for the second and third **Adaptor** items, select the virtual switches you created earlier.  
For example, select `Client-Side-vSwitch1` and `Server-Side-vSwitch2`.
8. Click **OK**.
9. Later, when you configure FortiWeb-VM, add port2 and port3 (or whichever FortiWeb ports correspond to the vSwitches you created in this procedure) to the bridge (V-zone).

## Starting the FortiWeb-VM

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

## Configuring access to FortiWeb's web UI & CLI

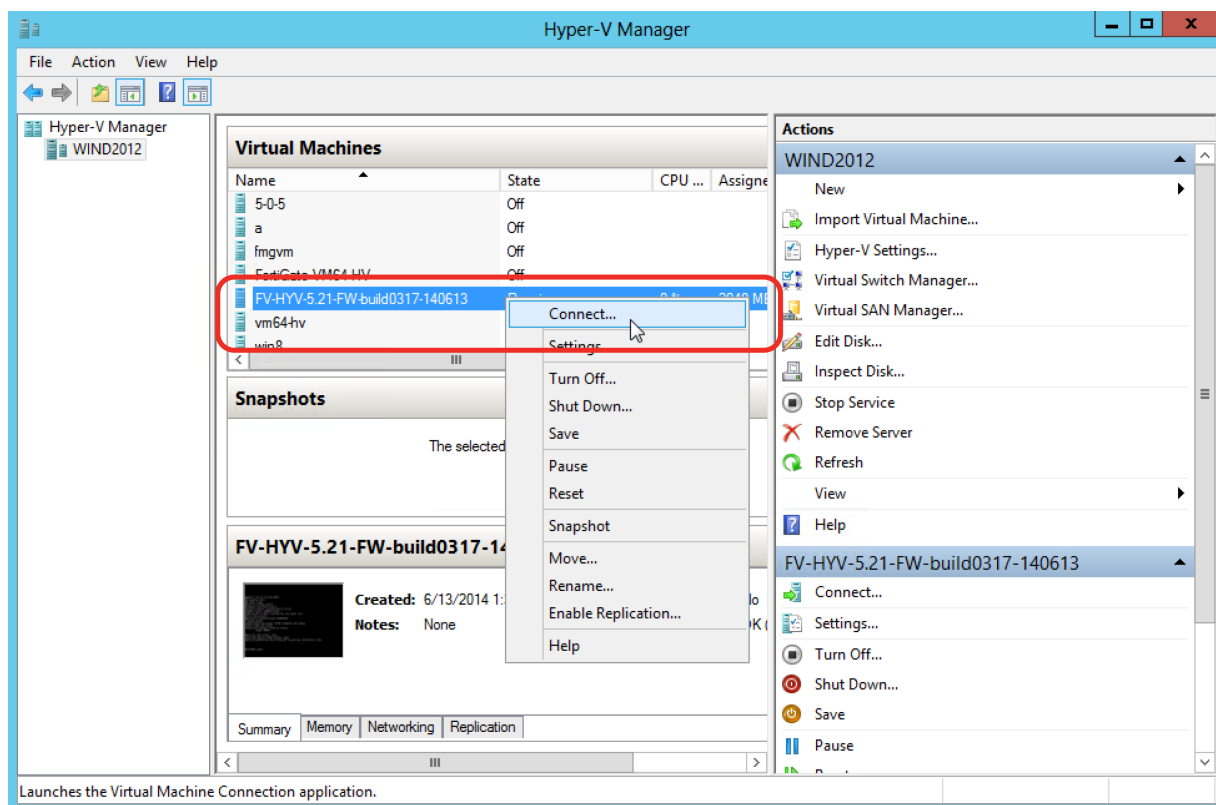
For hypervisor deployments, after the virtual appliance is powered on, you log in to the FortiWeb-VM command line interface (CLI) via the console and configure basic network settings so that you can connect to the appliance's web UI, CLI, or both through your management computer's network connection.

### 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:
  - Hyper-V Manager
2. Log in to the VM server.
3. Open the console of the FortiWeb-VM virtual appliance.

On Hyper-V Manager:

- Under **Virtual Machines**, right-click the name of the virtual appliance, such as **FortiWeb-VM**.
- Click **Connect**.



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 34](#). 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 42](#).





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 34](#).

---

## 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://.)



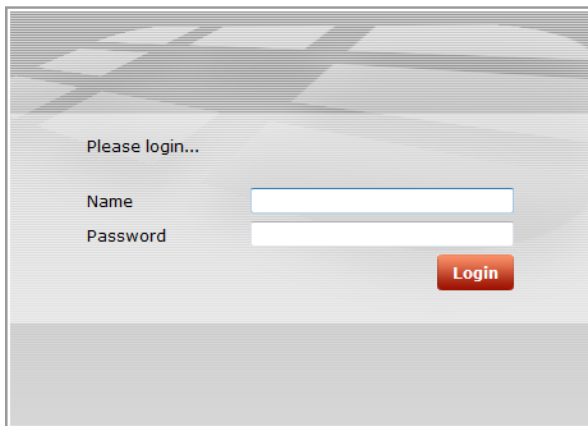
Initially, you must access the web UI via HTTPS. By default, HTTP is not enabled. After uploading the license, you can configure the administrative access protocols. For details, see the [FortiWeb Administration Guide](#).

- 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**.

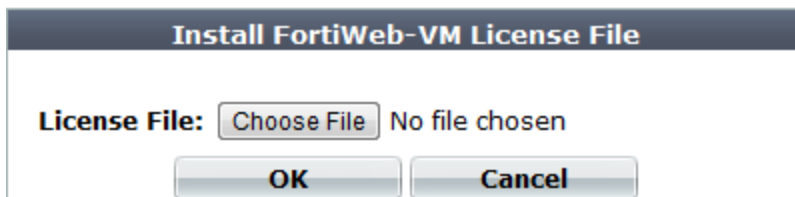
The web UI appears.

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 <a href="#">[Update]</a>
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.



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

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

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

```
License status changed to VALID
```

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

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

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

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

```
exec update-now
```



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

If the connection did **not** succeed:

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

```
C:\Users\cswartz>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 31](#).

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 35](#).

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

## Updating the license for more vCPUs

If either:

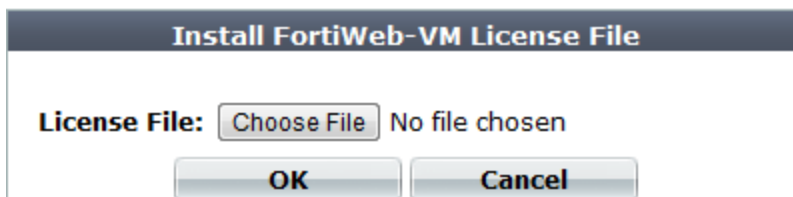
- you want to upgrade FortiWeb-VM to a license with a higher vCPU limit
- your original FortiWeb-VM license was an extended (but temporary) evaluation license, and you have now purchased a permanent, paid license

you must upload a new license file.

To replace an evaluation license with a paid license, use [Uploading the license on page 34](#).

### 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 34](#).



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

## What's next?

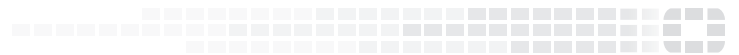
At this point, the FortiWeb-VM virtual appliance is running, and it has received a license file, but its operating system is almost entirely unconfigured. Before you can use FortiWeb-VM, you must configure it.

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.



**FORTINET®**



Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.