



Install Guide

for FortiScan-VM™ 4.0 MR2 Patch 3

Courtney Schwartz

Contributors:
Hamid Karimi
Shant Mosvessian
Idan Soen



Contents

Overview of FortiScan-VM	4
Architecture	4
Licensing	5
Forums	5
Technical support	5
Documentation	6
Fortinet Knowledge Base	6
Comments	6
Scope	6
Conventions	7
IP addresses.....	7
Cautions, notes, & tips.....	7
Typographical conventions.....	7
Command syntax conventions.....	8
System requirements	10
Downloading the FortiScan-VM software & registering with Technical Support	12
Deploying FortiScan-VM on VMware vSphere	14
Deploying the OVF package.....	15
Configuring the virtual appliance's virtual hardware settings	17
Resizing the virtual disk (vDisk).....	17
Configuring the number of virtual CPUs (vCPUs).....	22
Configuring the virtual RAM (vRAM) limit	24
Mapping the virtual NICs (vNICs) to physical NICs	25
Powering on the virtual appliance.....	28
Deploying FortiScan-VM on Citrix XenServer	30
Converting and deploying the OVF package.....	31

Configuring the virtual appliance's virtual hardware settings	31
Resizing the virtual disk (vDisk).....	32
Configuring the number of virtual CPUs (vCPUs).....	33
Configuring the virtual RAM (vRAM) limit	35
Mapping the virtual NICs (vNICs) to physical NICs	37
Deploying FortiScan-VM on open source Xen	41
Configuring access to the web UI & CLI	43
Uploading the license	48
What's next?	54
Updating the virtual hardware	54
Index	55

Overview of FortiScan-VM

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

The FortiScan-VM Vulnerability and Compliance Management (VCM) platform is a managed security service provider (MSSP)- and enterprise-level IT security solution that empowers you to protect your many network hosts from known vulnerabilities and exploits.

FortiScan-VM virtual appliances, together with FortiScan agents, help you to efficiently address the ever-increasing number of computer security threats. FortiScan-VM appliances provide ready-to-deploy remediation actions and enforcement actions, which can change host configurations to mitigate weak settings and patch applications. This frees your time to focus on zero-day vulnerabilities and exploits, before vendor-provided patches or fixes are available.

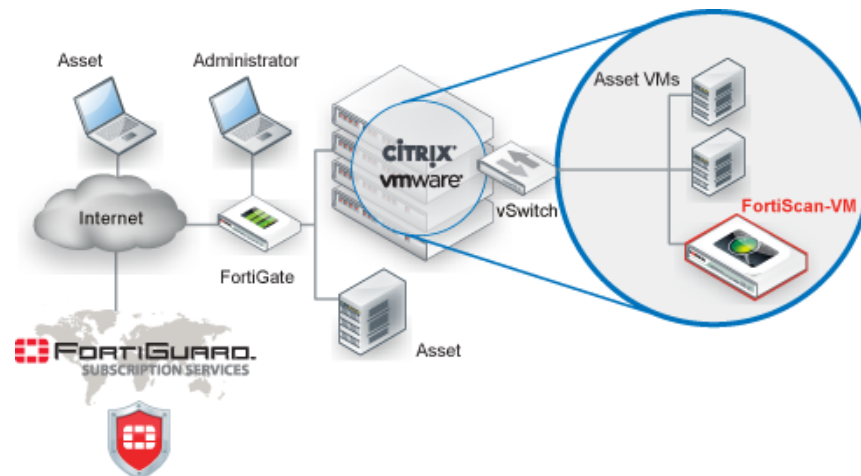
FortiScan-VM installations can also scan your network for vulnerabilities and compliance exposures, prioritizing hosts by risk.

Architecture

FortiScan-VM is a virtual appliance version of FortiScan. It is deployed in a virtual machine environment such as VMware vSphere or Citrix XenServer.

Once the virtual appliance is deployed and set up, you can manage FortiScan-VM via its web UI from a web browser on your management computer.

Figure 1: FortiScan-VM architecture



Licensing

Licenses are available at multiple levels, empowering you to scale at the pace of business. Increasing your license level increases the number of assets that you can manage. 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 FortiScan-VM license to support your needs.

Managed security service providers (MSSPs) or Internet service providers (ISPs) with software-as-a-service (SaaS) models can especially benefit from the flexibility of stackable licenses with FortiScan-VM.

For information on the number of assets supported at each license level, and the limits of configurable values in FortiScan-VM, see the *FortiScan Administration Guide*.



Note: FortiScan-VM images include a free 15-day limited trial license for evaluation. The trial period begins the first time you power on your FortiScan-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 details, see “[Uploading the license](#)” on page 48.

The trial license version of FortiScan-VM uses weak encryption (LENC), making it faster even if you use less powerful hardware during your trial phase, and also downloadable even in countries where strong encryption is subject to export controls.



Note: Cryptography laws vary by country. If you are uncertain about which laws apply to you, consult a legal advisor.

Once upgraded to a purchased license, FortiScan-VM can use strong encryption, where legally available.

Forums

Fortinet Technical Discussion forums provide a place for you to connect with your fellow IT professionals to discuss best practices and solutions. Visit the forums at:

<http://support.fortinet.com/forum/>

Technical support

Fortinet Technical Support provides services designed to make sure that you can install your Fortinet products quickly, configure them easily, and operate them reliably in your network.



Note: Technical support is *not* included with the 15-day free trial license included with FortiScan-VM.

To learn about the customer services that Fortinet provides, visit the Fortinet Technical Support web site at:

<https://support.fortinet.com>

You can dramatically improve the time that it takes to resolve your technical support ticket by providing your configuration file, a network diagram, and other specific information. For a list of required information, see the Fortinet Knowledge Base article [Technical Support Requirements](#).

Documentation

The Fortinet Technical Documentation web site:

<http://docs.fortinet.com>

provides the most up-to-date versions of Fortinet publications, as well as additional technical documentation.

Fortinet Knowledge Base

The Fortinet Knowledge Base provides additional Fortinet technical documentation, such as troubleshooting and how-to-articles, examples, and FAQs. Visit the Fortinet Knowledge Base at:

<http://kb.fortinet.com>

Comments

Please send information about any errors or omissions in this document to:

techdoc@fortinet.com

Scope

This document describes how to deploy a FortiScan-VM virtual appliance disk image onto a virtualization server, and how to configure the virtual hardware settings of the virtual appliance. It assumes you have already successfully installed a virtualization server on the physical machine.

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

This document is intended for administrators, not end users. If you have a user account on a host where the FortiScan agent is installed, please contact your system administrator.

Conventions

Fortinet technical documentation uses the conventions described below.

IP addresses

To avoid publication of public IP addresses that belong to Fortinet or any other organization, the IP addresses used in Fortinet technical documentation are fictional and follow the documentation guidelines specific to Fortinet. The addresses used are from the private IP address ranges defined in RFC 1918: Address Allocation for Private Internets, available at:

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

Cautions, notes, & tips

Fortinet technical documentation uses the following guidance and styles for notes, tips and cautions.



Caution: Warns you about commands or procedures that could have unexpected or undesirable results including loss of data or damage to equipment.



Note: Presents useful information, but usually focused on an alternative, optional method, such as a shortcut, to perform a step.



Tip: Highlights useful additional information, often tailored to your workplace activity.

Typographical conventions

Fortinet documentation uses the following typographical conventions:

Table 1: Typographical conventions in Fortinet technical documentation

Convention	Example
Button, menu, text box, field, or check box label	From <i>Minimum log level</i> , select <i>Notification</i> .
CLI input	<pre>config system dns set primary <address_ipv4> end</pre>
CLI output	<pre>FGT-602803030703 # get system settings comments : (null) opmode : nat</pre>
Emphasis	HTTP connections are <i>not</i> secure and can be intercepted by a third party.
File content	<pre><HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD> <BODY><H4>You must authenticate to use this service.</H4></pre>
Hyperlink	https://support.fortinet.com

Table 1: Typographical conventions in Fortinet technical documentation

Keyboard entry	Type a name for the remote VPN peer or client, such as <code>Central_Office_1</code> .
Navigation	Go to <i>VPN > IPSEC > automatic Key (IKE)</i> .
Publication	For details, see the <i>FortiGate Administration Guide</i> .

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.

Table 2: Command syntax notation

Convention	Example
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 <code>enable</code> or <code>disable</code> , 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 <code>snmp</code> to the previous example, you would type: 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.

Table 2: Command syntax notation

Convention	Example
Square brackets []	<p>A non-required word or series of words. For example: <code>[verbose {1 2 3}]</code> indicates that you may either omit or type both the <code>verbose</code> word and its accompanying option, such as: <code>verbose 3</code></p>
Angle brackets < >	<p>A word constrained by data type. 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: <code><retries_int></code> indicates that you should enter a number of retries, such as 5. Data types include:</p> <ul style="list-style-type: none"> • <code><xxx_name></code> — A name referring to another part of the configuration, such as <code>policy_A</code>. • <code><xxx_index></code> — An index number referring to another part of the configuration, such as 0 for the first static route. • <code><xxx_pattern></code> — A regular expression or word with wild cards that matches possible variations, such as <code>*@example.com</code> to match all e-mail addresses ending in <code>@example.com</code>. • <code><xxx_fqdn></code> — A fully qualified domain name (FQDN), such as <code>mail.example.com</code>. • <code><xxx_email></code> — An email address, such as <code>admin@mail.example.com</code>. • <code><xxx_url></code> — A uniform resource locator (URL) and its associated protocol and host name prefix, which together form a uniform resource identifier (URI), such as <code>http://www.fortinet.com/</code>. • <code><xxx_ipv4></code> — An IPv4 address, such as <code>192.168.1.99</code>. • <code><xxx_v4mask></code> — A dotted decimal IPv4 netmask, such as <code>255.255.255.0</code>. • <code><xxx_ipv4mask></code> — A dotted decimal IPv4 address and netmask separated by a space, such as <code>192.168.1.99 255.255.255.0</code>. • <code><xxx_ipv4/mask></code> — A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as <code>192.168.1.99/24</code>. • <code><xxx_ipv6></code> — A colon (<code>:</code>)-delimited hexadecimal IPv6 address, such as <code>3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234</code>. • <code><xxx_v6mask></code> — An IPv6 netmask, such as <code>/96</code>. • <code><xxx_ipv6mask></code> — An IPv6 address and netmask separated by a space. • <code><xxx_str></code> — A string of characters that is not another data type, such as <code>P@ssw0rd</code>. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences. See the FortiScan CLI Reference. • <code><xxx_int></code> — An integer number that is not another data type, such as 15 for the number of minutes.

System requirements

Before you can install FortiScan-VM, you must first have virtual machine (VM) environment software (a hardware abstraction layer (HAL) that is sometimes called a hypervisor) on your server. FortiScan-VM is a virtual appliance that runs inside that environment. Supported hypervisor versions include:

- VMware vSphere ESX 4.0/4.1
- VMware vSphere ESXi 4.0/4.1/5.0
- VMware vSphere Workstation 4.0/4.1/5.0
- VMware vSphere Hypervisor 4.0/4.1/5.0
- Citrix XenServer 5.6
- Open source Xen Hypervisor 3.0.3



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

For installation instructions, see the documentation for your VM environment, such as:

- <http://www.vmware.com/products/esxi>
- <http://support.citrix.com/productdocs/>
- <http://xen.org/>

In the BIOS, for VMware vSphere ESX or Citrix XenServer, you may also need to enable support for **hardware-assisted virtualization**. Steps vary by manufacturer. Consult the documentation for your hardware.

For example, on a Dell PowerEdge, during boot, you would interrupt the process by pressing F2, then enter the *CPU Information* section and enable *Virtualization Technology*.

Figure 2: Enabling 64-bit support and virtualization in a Dell PowerEdge BIOS

```
System Time ..... 15:17:48
System Date ..... Mon Feb 02,

Memory Information .. <ENTER>
CPU Information ..... <ENTER>

64-bit ..... Yes
Core Speed ..... 3.00 GHz
Bus Speed ..... 1333 MHz
Execute Disable ..... Enabled
Number of Cores per Processor ..... 4 Cores
Virtualization Technology ..... Enabled
Adjacent Cache Line Prefetch ..... Enabled
Hardware Prefetcher ..... Enabled
Demand-Based Power Management ..... Disabled
Processor 1 Family-Model-Stepping ..... 06-17-A
[Intel(R) Xeon(R) CPU E5450 @ 3.00 GHz]
```

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 will use to deploy and manage your virtual machines.)

Downloading the FortiScan-VM software & registering with Technical Support

FortiScan-VM software is freely available via download from:

http://www.fortinet.com/product_trials/fortiscan_vm.html

This download comes with a free 15-day trial than can be converted to a paid, permanent license.

When purchasing FortiWeb-VM from your reseller, you will receive an email that contains a registration number. This is used to download the software, your purchased license, and also to register your purchase for technical support.

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

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

To register & download FortiScan-VM and your license

- 1 On your management computer, start a web browser.
- 2 Log in to the Fortinet Technical Support web site:

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

The screenshot shows the Fortinet Customer Service & Support website. The navigation bar includes the Fortinet logo, 'CUSTOMER SERVICE & SUPPORT', and a user profile section with 'Welcome Courtney Schwartz!' and 'Log Out | My Profile'. The main content area is divided into several service categories, each with an icon and a list of links. The 'Asset Management' category is highlighted with a red circle around the 'Register/Renew' link. The 'Download' category is also highlighted with a red circle around the 'Firmware Images' link. On the right side, there is a sidebar with 'IMPORTANT INFO' and 'RESOURCE CENTER' sections.

- 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, such as:

12C45-AB3DE-678G0-F9HIJ-123B5

A registration form will appear.

- 5 Use the form to register your ownership of FortiScan-VM with Technical Support, and to indicate the IP address of your FortiScan-VM, to which the license will be bound (*Management Address*).

After completing the form, a registration acknowledgement page will appear.

- 6 Click the *License File Download* link.

Your browser will download the `.lic` file that was purchased for that registration number.

- 7 In the upper left corner of the page, click the *Home* link to return to the initial page.

- 8 In the *Download* quadrant of the page, click *Firmware Images*.

- 9 Click the FortiScan link and navigate to the version that you want to download.

- 10 Download both:

- `.pkg` image file — Use this for **upgrades**. Contains the `.out` file, plus:
 - FortiScan agent software
 - Windows application version of the push installer
 - Microsoft Installer and other software required for agent-based vulnerability and compliance management of a network
 - [FortiScan-VM Release Notes](#)
- `.zip` or `.tgz` image file — Use this for **new virtual appliance (VM)** installations. Contains a deployable virtual machine package. Download whichever is appropriate for your hypervisor. (If you have purchased licenses or want to try FortiScan-VM for multiple hypervisor platforms, download the package for each platform.)

File name suffix	Supported hypervisor platform
<code>.out.esx.zip</code>	VMware vSphere ESX/ESXi/Hypervisor
<code>.out.citrix.zip</code>	Citrix XenServer
<code>.out.vmware.zip</code>	VMware vSphere Workstation
<code>.out.xen.tgz</code>	Open source Xen Hypervisor



Note: Files for FortiScan-VM have a `FSC_VM` file name prefix. Other prefixes indicate that the file is for hardware versions of FortiScan such as FortiScan-3000C. Such other files cannot be used with FortiScan-VM.

- 11 Extract the `.zip` or `.tgz` compressed archive's contents to a folder.

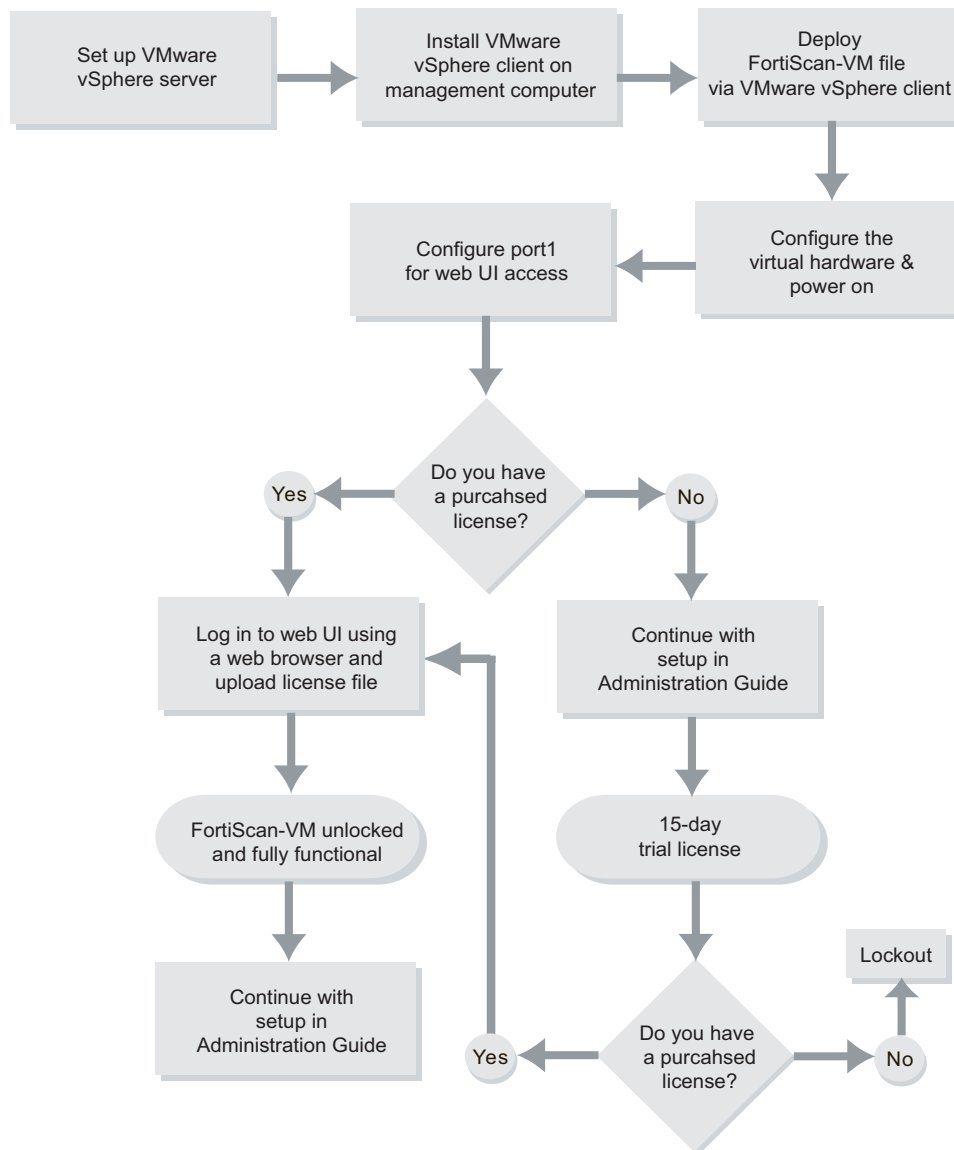
- 12 Continue by deploying the virtual appliance package. Steps vary by which hypervisor you are using. See one of the following:

- “[Deploying FortiScan-VM on VMware vSphere](#)” on page 14
- “[Deploying FortiScan-VM on Citrix XenServer](#)” on page 30
- “[Deploying FortiScan-VM on open source Xen](#)” on page 41

Deploying FortiScan-VM on VMware vSphere

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

Figure 3: Basic steps for installing FortiScan-VM (VMware)

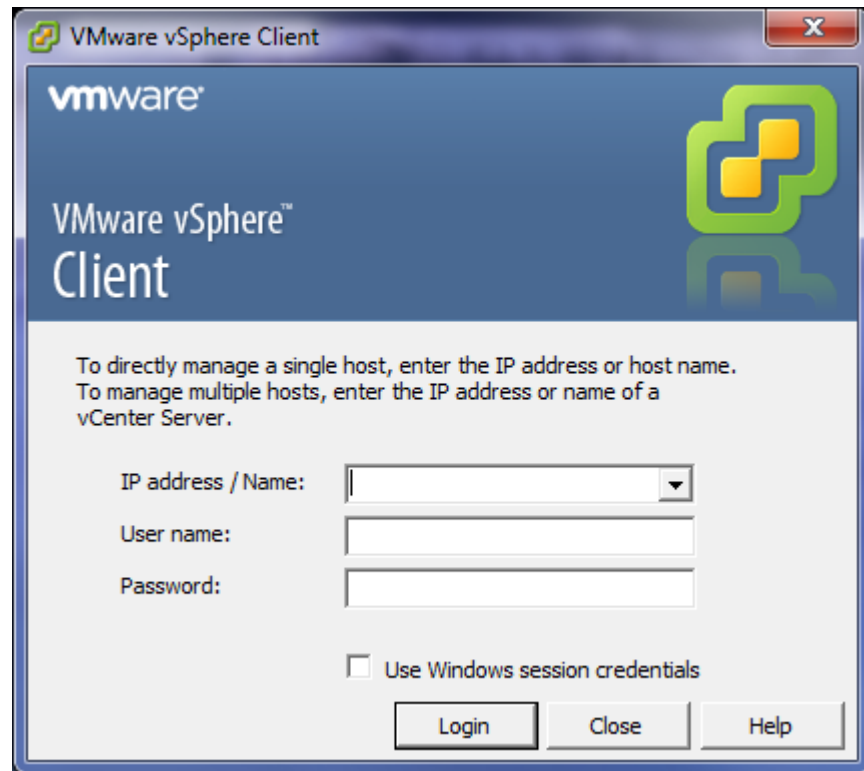


Deploying the OVF package

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

To deploy the virtual appliance

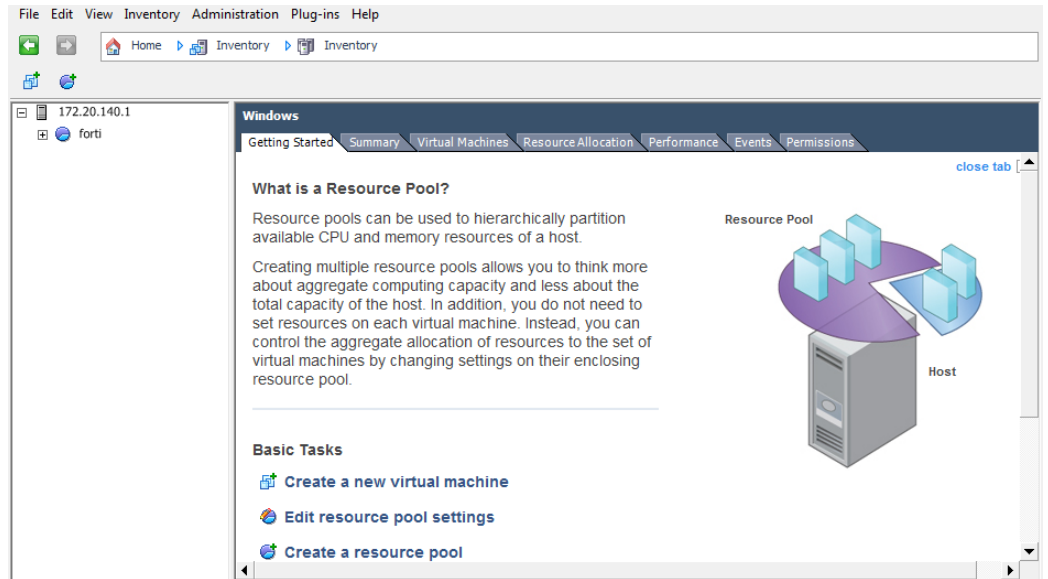
- 1 On your management computer, start VMware vSphere Client.



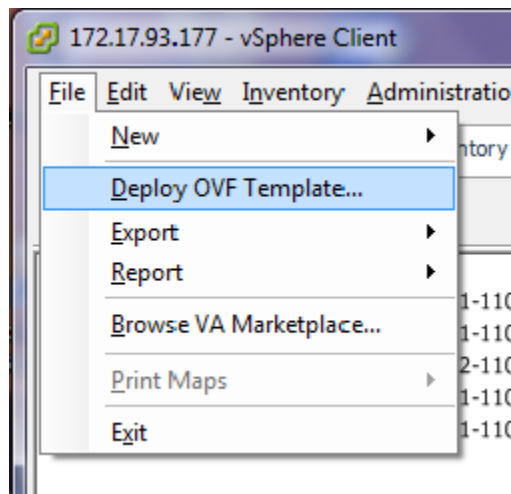
- 2 In *IP address / Name*, type the IP address or FQDN of the VMware vSphere server.
- 3 In *User name*, type the name of your account on that server.
- 4 In *Password*, type the password for your account on that server.

5 Click *Login*.

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



6 Go to *File > Deploy OVF Template*.



A deployment wizard window appears.

- 7 In the *Deploy OVF Template* window, select the *Deploy from file* option, then locate the FortiScan-VM OVF file.
- 8 Click *Next* twice.
- 9 Read the end user license agreement (EULA). If you agree, click *Accept* to continue the deployment. Otherwise click *Cancel* to abort the deployment.
- 10 Click *Next*.
- 11 In *Name*, type a unique descriptive name for this instance of FortiScan-VM as it will appear in vSphere Client's inventory, such as FortiScan-VM-4.2.3. 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 FortiScan-VM web UI.)

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 FortiScan-VM.

Continue with "Configuring the virtual appliance's virtual hardware settings" on page 17.



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

- Resize the virtual disk (VMDK) (see "Resizing the virtual disk (vDisk)" on page 17)
- Set the number of vCPUs (see "Configuring the number of virtual CPUs (vCPUs)" on page 22)
- Set the vRAM on the virtual appliance ("Configuring the virtual RAM (vRAM) limit" on page 24)
- Map the virtual network adapter(s) ("Mapping the virtual NICs (vNICs) to physical NICs" on page 25).

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

Configuring the virtual appliance's virtual hardware settings

After installing FortiScan-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 information on the limits of configurable values for FortiScan-VM, see the *FortiScan 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.



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

The FortiScan-VM package that you downloaded includes pre-sized VMDK (Virtual Machine Disk Format) files. However, they are only 30 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.

During the creation of a VM datastore, you have the following formatting options:

- 1 MB block size — 256 GB maximum file size
- 2 MB block size — 512 GB maximum file size
- 4 MB block size — 1,024 GB maximum file size
- 8 MB block size — 2,048 GB maximum file size

These options affect the possible size of each vDisk.

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

Consider also that, depending on the size of your organization's network, you might require more or less storage for your asset inventory, scan results, and reports. Guidelines for storage size vary by the number of assets (*n*):

- *n* < 10,000 assets: 1 TB
- 10,000 assets < *n* < 20,000 assets: 2 TB

Fortinet recommends that you choose a vDisk size greater than 1024 GB (1 TB).

For more information on vDisk sizing, see:

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

To resize the vDisk

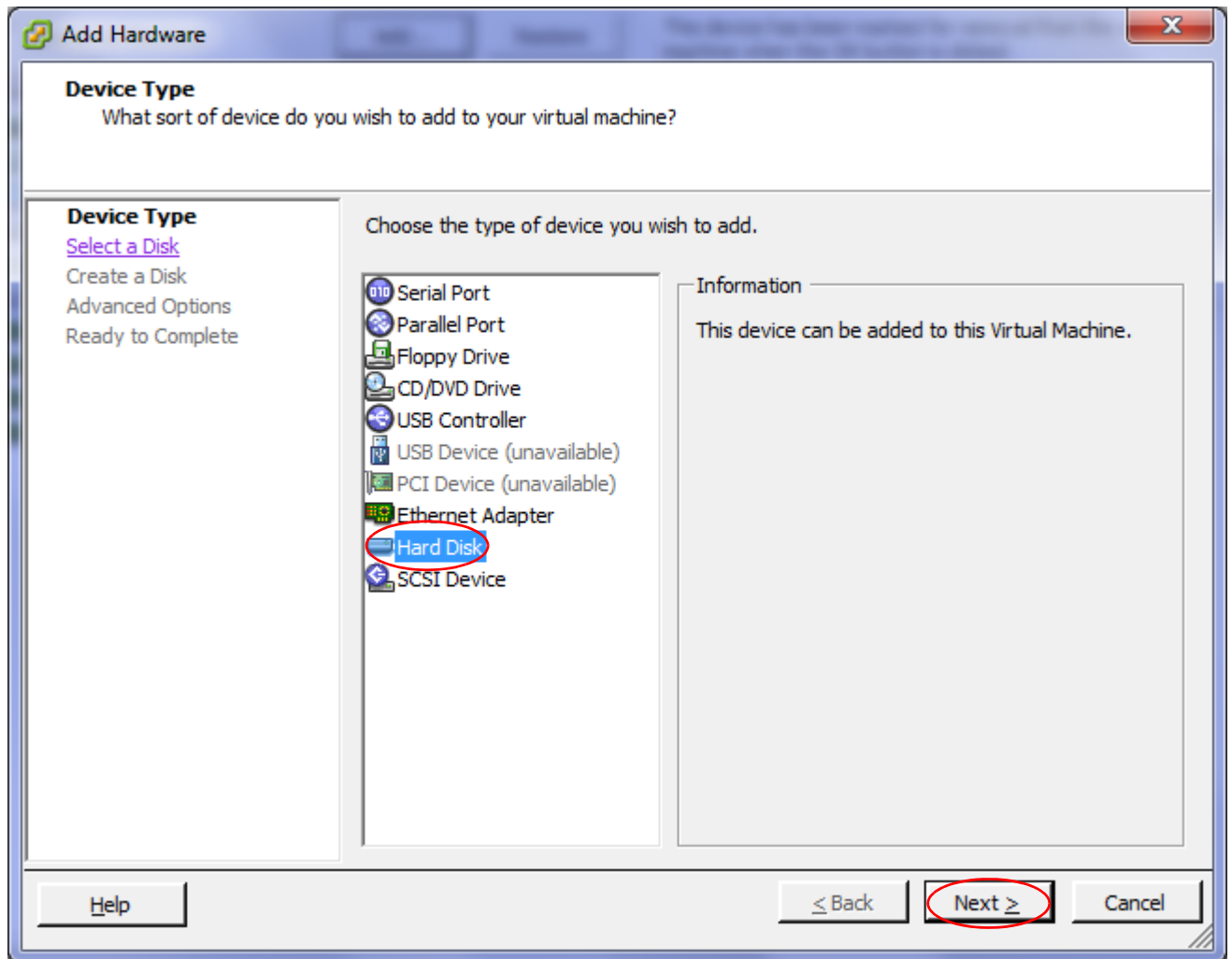
- 1 On your management computer, start VMware vSphere Client.
- 2 In *IP address / Name*, type the IP address or FQDN of the VMware vSphere server.
- 3 In *User name*, type the name of your account on that server.
- 4 In *Password*, type the password for your account on that server.
- 5 Click *Login*.
- 6 In the left pane, right-click the name of the virtual appliance, such as *FortiScan-VM-4.2.3*, 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 2*.
- 8 Click *Remove*.
- 9 Click *Add*.

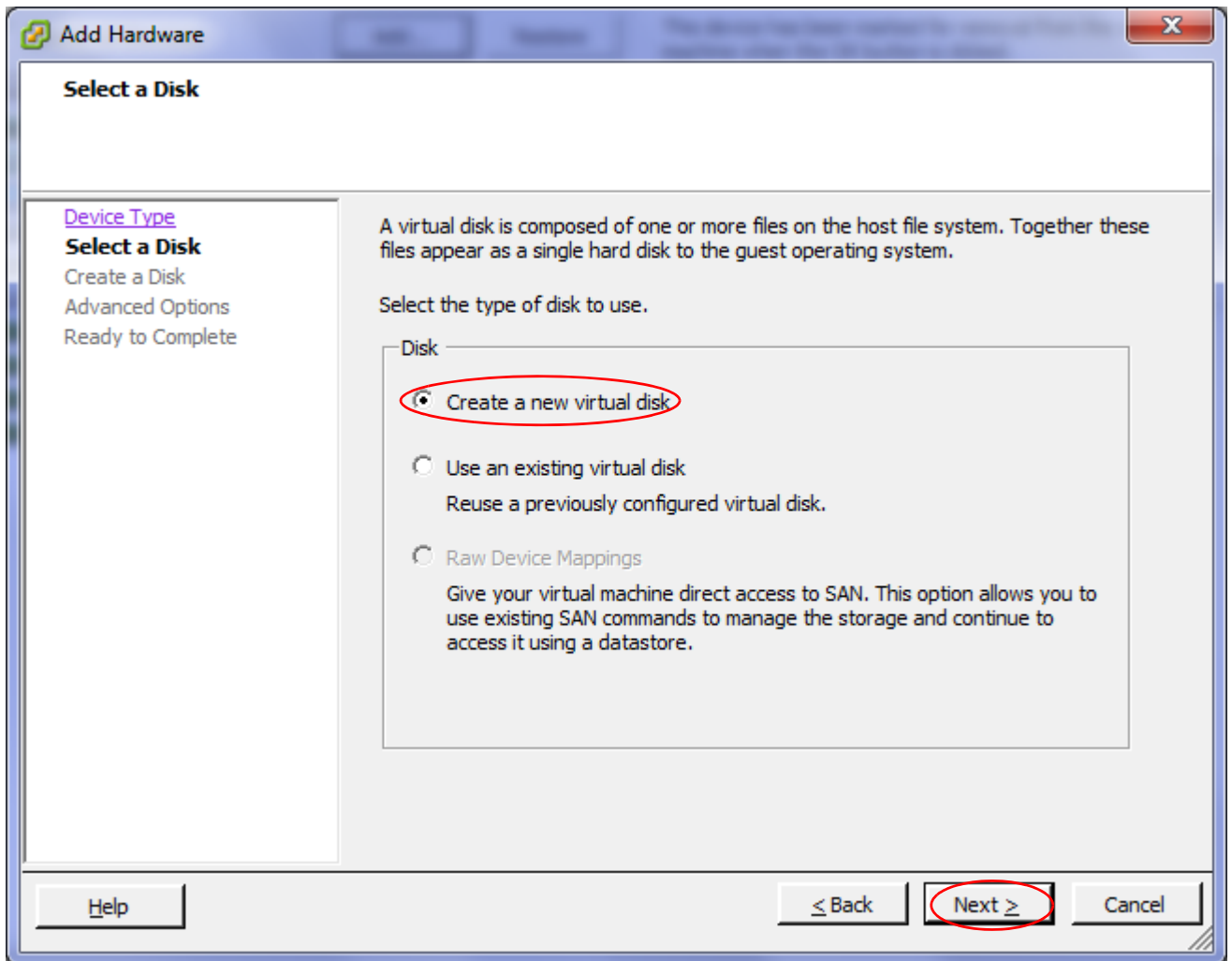
The *Add Hardware* dialog appears.

10 In the list of device types, click *Hard Disk*.



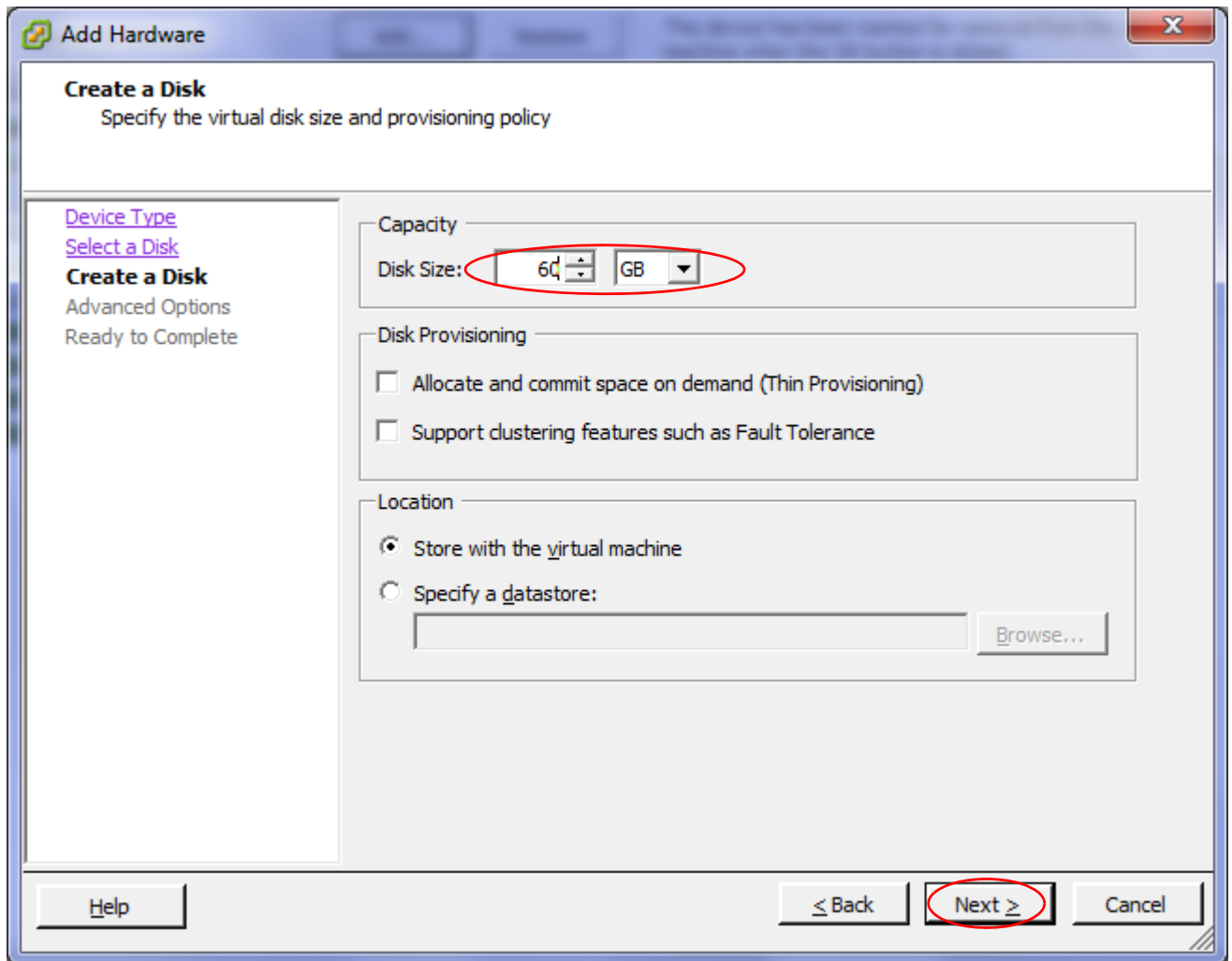
11 Click Next.

12 Select *Create a new virtual disk*.



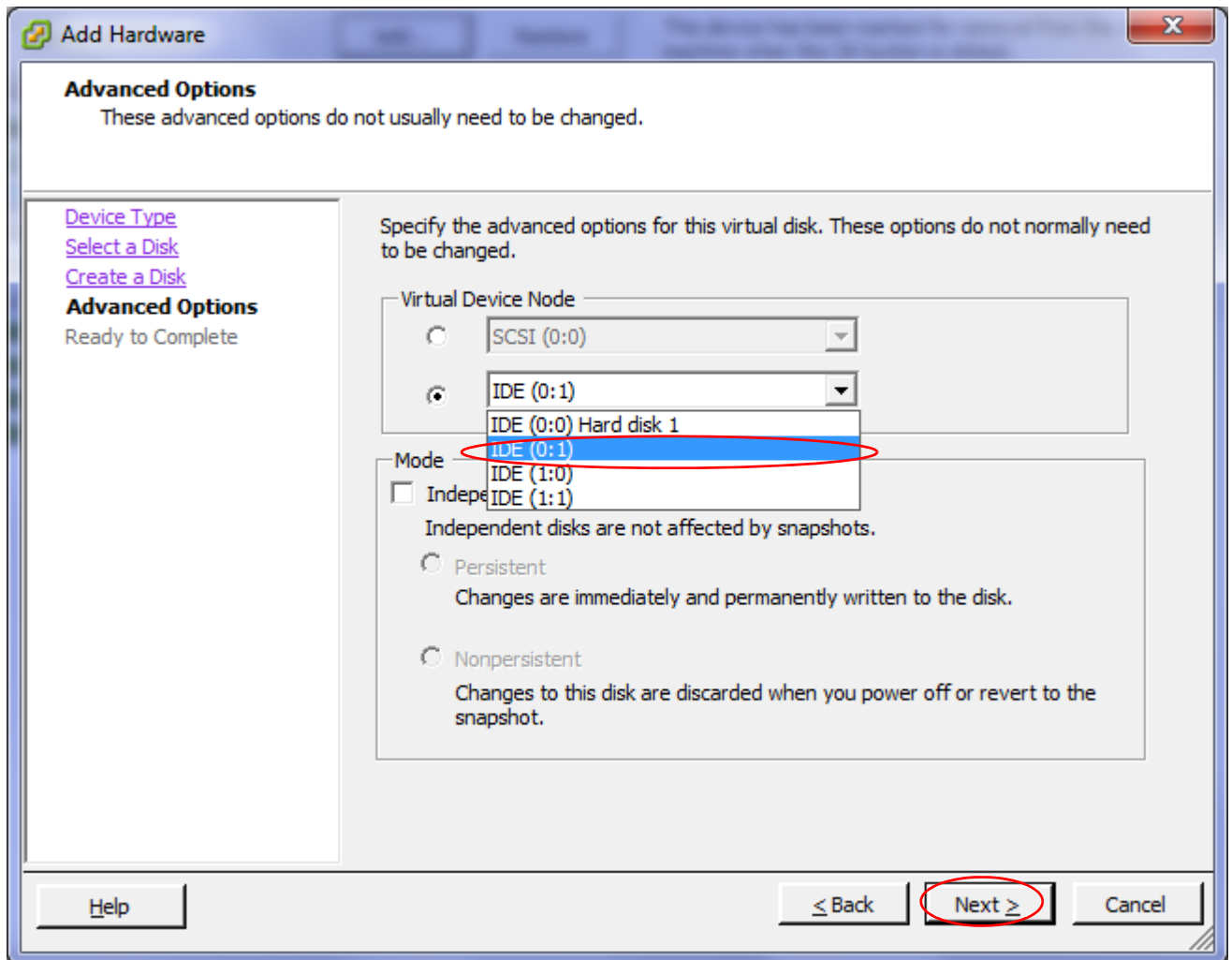
13 Click *Next*.

14 In *Disk Size*, type the new size, in gigabytes (GB), of the vDisk.



15 Click *Next*.

- 16 Select the bottom option in *Virtual Device Node*, then from its drop-down menu, select *IDE (0:1)*.



- 17 Click *Next*.
- 18 Click *Finish*.
- 19 Click *OK*.
- 20 If you do not need to change the other resources, continue with “Powering on the virtual appliance” on page 28. Otherwise continue with “Configuring the number of virtual CPUs (vCPUs)” on page 22.

Configuring the number of virtual CPUs (vCPUs)

By default, the virtual appliance is configured to use 2 vCPUs. Guidelines for vCPU allocation vary by the number of assets (*n*):

- $n < 10,000$ assets: 2 vCPUs
- $10,000 \text{ assets} < n < 20,000 \text{ assets}$: 4 vCPUs

Change the value if necessary to allocate enough vCPUs for the size of your deployment.

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

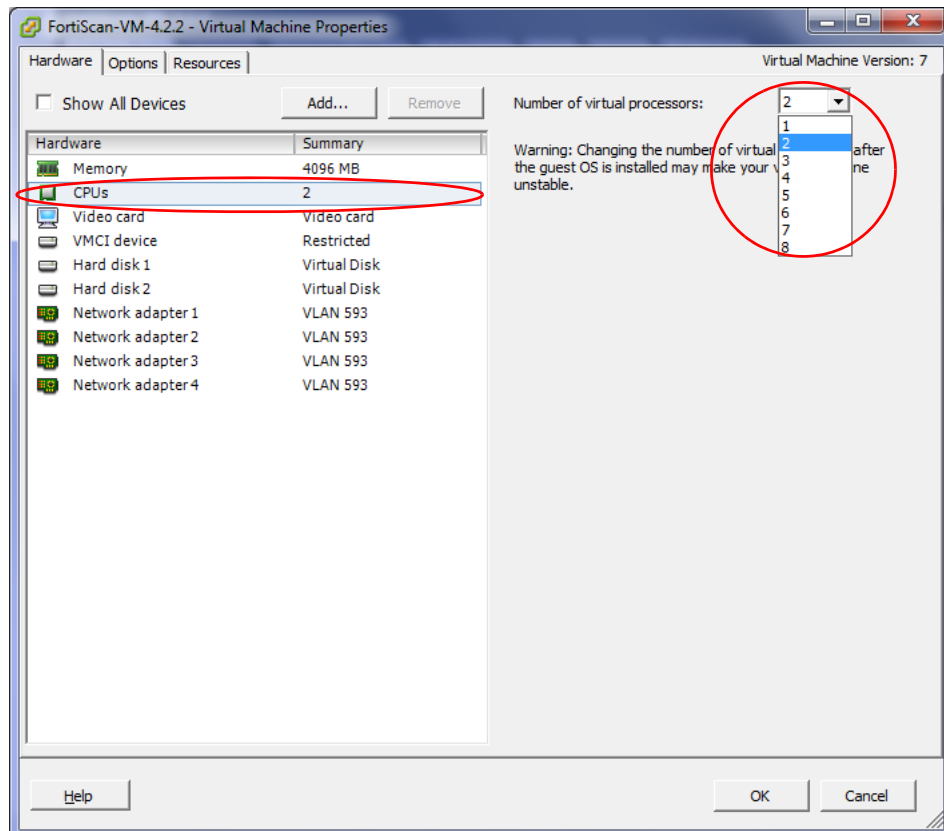
<http://www.vmware.com/products/vsphere-hypervisor/index.html>

To change the number of vCPUs

- 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 left pane, right-click the name of the virtual appliance, such as *FortiScan-VM-4.2.3*, 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.



- 9 Click *OK*.
- 10 If you do not need to change the other resources, continue with “Powering on the virtual appliance” on page 28. Otherwise continue with “Configuring the virtual RAM (vRAM) limit” on page 24.

Configuring the virtual RAM (vRAM) limit

FortiScan-VM comes pre-configured to use 4 GB of vRAM. You can change this value. The valid range is from 4 GB to 16 GB. Appropriate values are suggested as follows, according to the number of assets (n) that will be monitored by your FortiScan-VM.

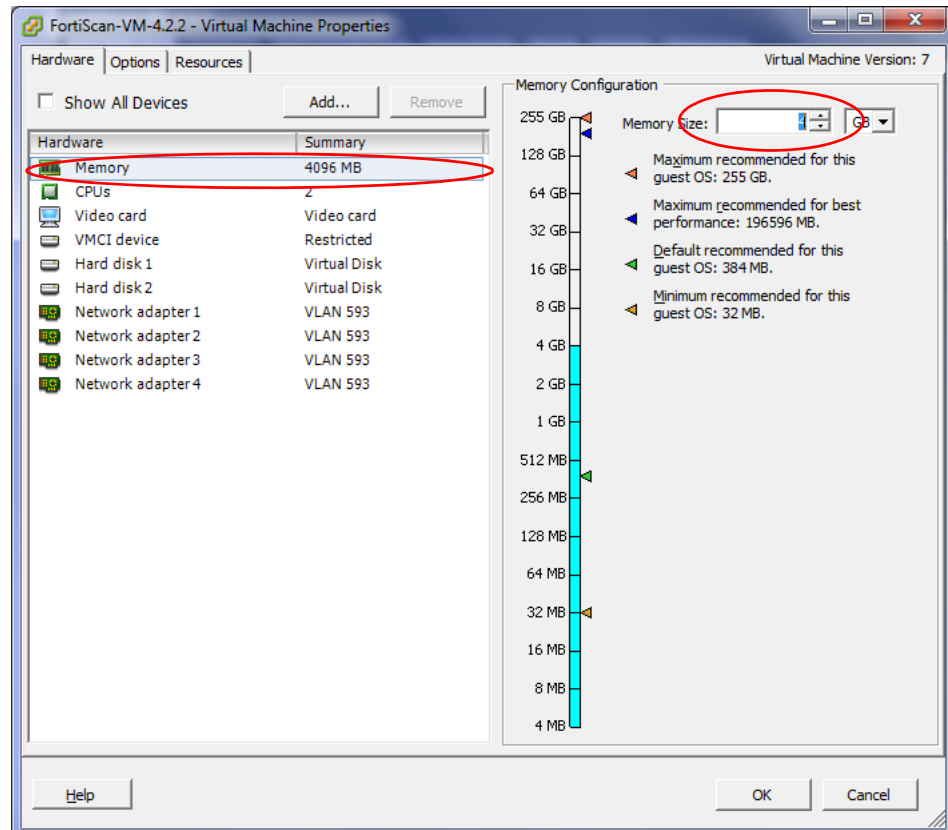
- $n < 2,000$ assets: 4 GB vRAM
- 2,000 assets $< n < 10,000$ assets: 8 GB vRAM
- 10,000 assets $< n < 20,000$ assets: 16 GB vRAM



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

To change the amount of vRAM

- 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 left pane, right-click the name of the virtual appliance, such as *FortiScan-VM-4.2.3*, 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 *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 the virtual appliance” on page 28. Otherwise continue with “Mapping the virtual NICs (vNICs) to physical NICs” on page 25.

Mapping the virtual NICs (vNICs) to physical NICs

Appropriate mappings of the FortiScan-VM ports to physical ports depends on your existing virtual environment.



Tip: 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.

When you deploy the FortiScan-VM package, 4 bridging vNICs are created and automatically mapped to a port group on 1 virtual switch (vSwitch) within the hypervisor. Each of those vNICs can be used by one of the 4 network interfaces in FortiScan-VM. (Alternatively, if you prefer, some or all of the network interfaces may be configured to use the same vNIC.) vSwitches are themselves mapped to physical ports on the server.

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

Table 3 provides an example of how vNICs could be mapped to the physical network ports on a server.

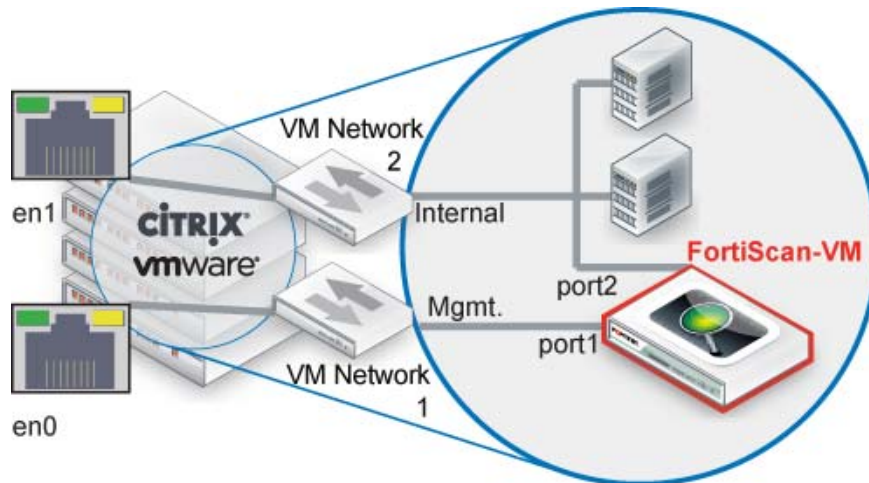


Table 3: Example: Network mapping

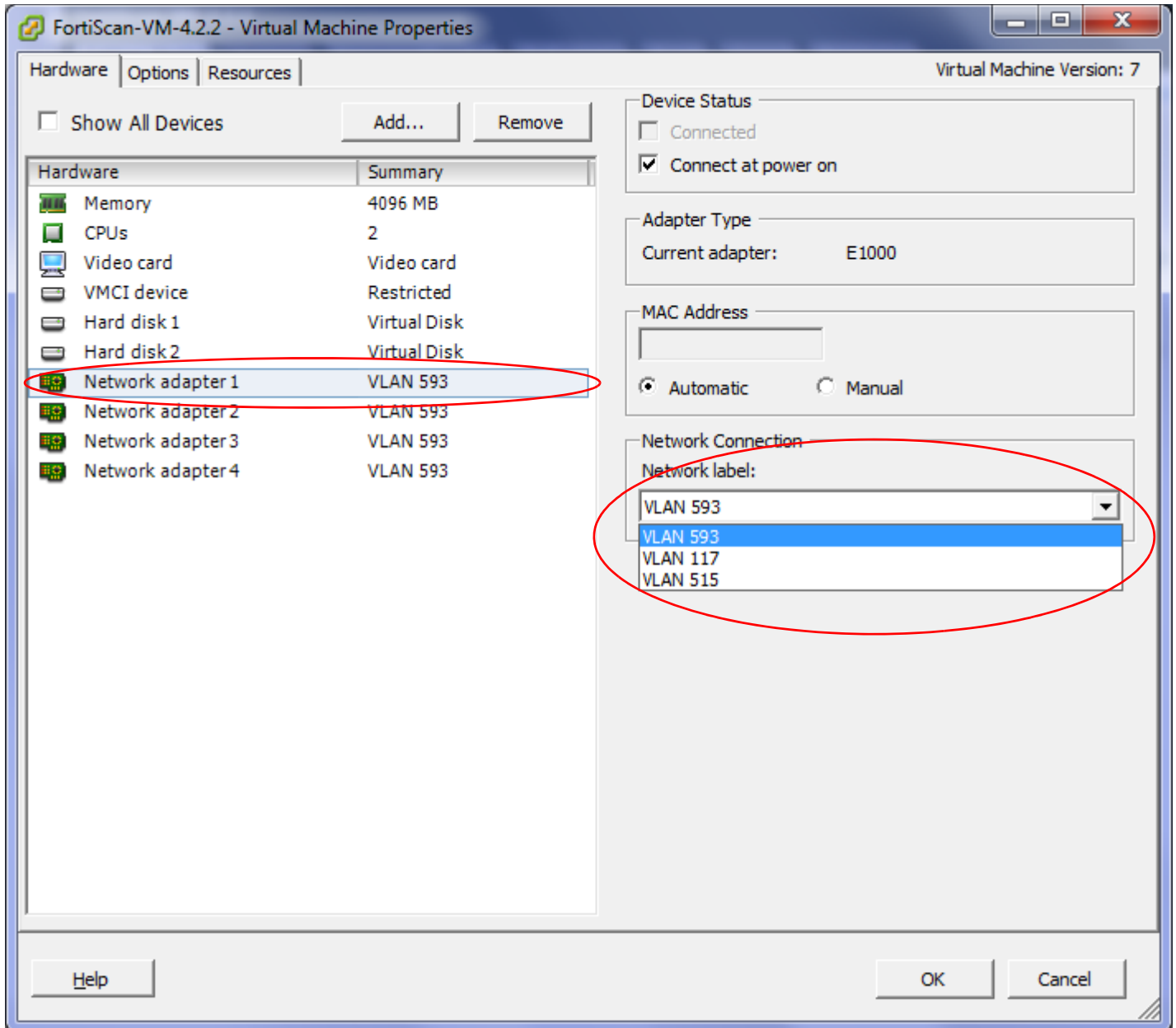
VMware vSphere			FortiScan-VM
Physical Network Adapter	Network Mapping (vSwitch Port Group)	Virtual Network Adapter for FortiScan-VM	Network Interface Name in Web UI/CLI
eth0	VM Network 1	Management	port1
eth1	VM Network 2	Internal	port2
eth1	VM Network 2	Internal	port3
eth1	VM Network 3	Internet	port4

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 left pane, right-click the name of the virtual appliance, such as *FortiScan-VM-4.2.3*, 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 the virtual appliance" on page 28.

Powering on the virtual appliance

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



Note: 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 25](#)). You may also want to:

- Resize disk (VMDK) (see "[Resizing the virtual disk \(vDisk\)](#)" on [page 17](#))
- Configure the number of CPUs (see "[Configuring the number of virtual CPUs \(vCPUs\)](#)" on [page 22](#))
- Set the RAM on virtual appliance ("[Configuring the virtual RAM \(vRAM\) limit](#)" on [page 24](#))

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

The first power up initializes the database and it takes a minute or two to finish powering up.

To power on FortiScan-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 left pane, click the name of the virtual appliance, such as *FortiScan-VM-4.2.3*.

- 7 Click the *Getting Started* tab.

FortiScan-VM-4.2.2

Getting Started Summary Resource Allocation Performance Events Console Permissions

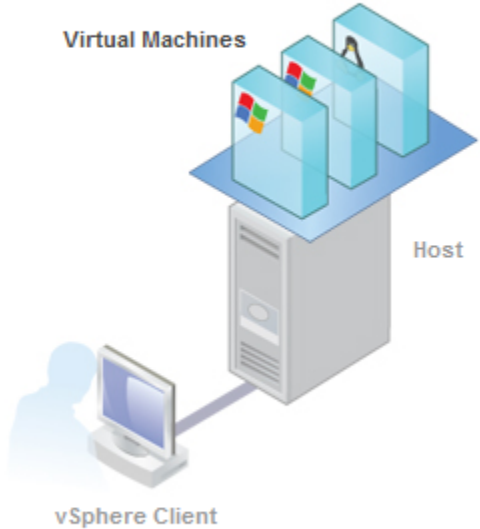
close tab X

What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

Virtual machines run on hosts. The same host can run many virtual machines.



Basic Tasks

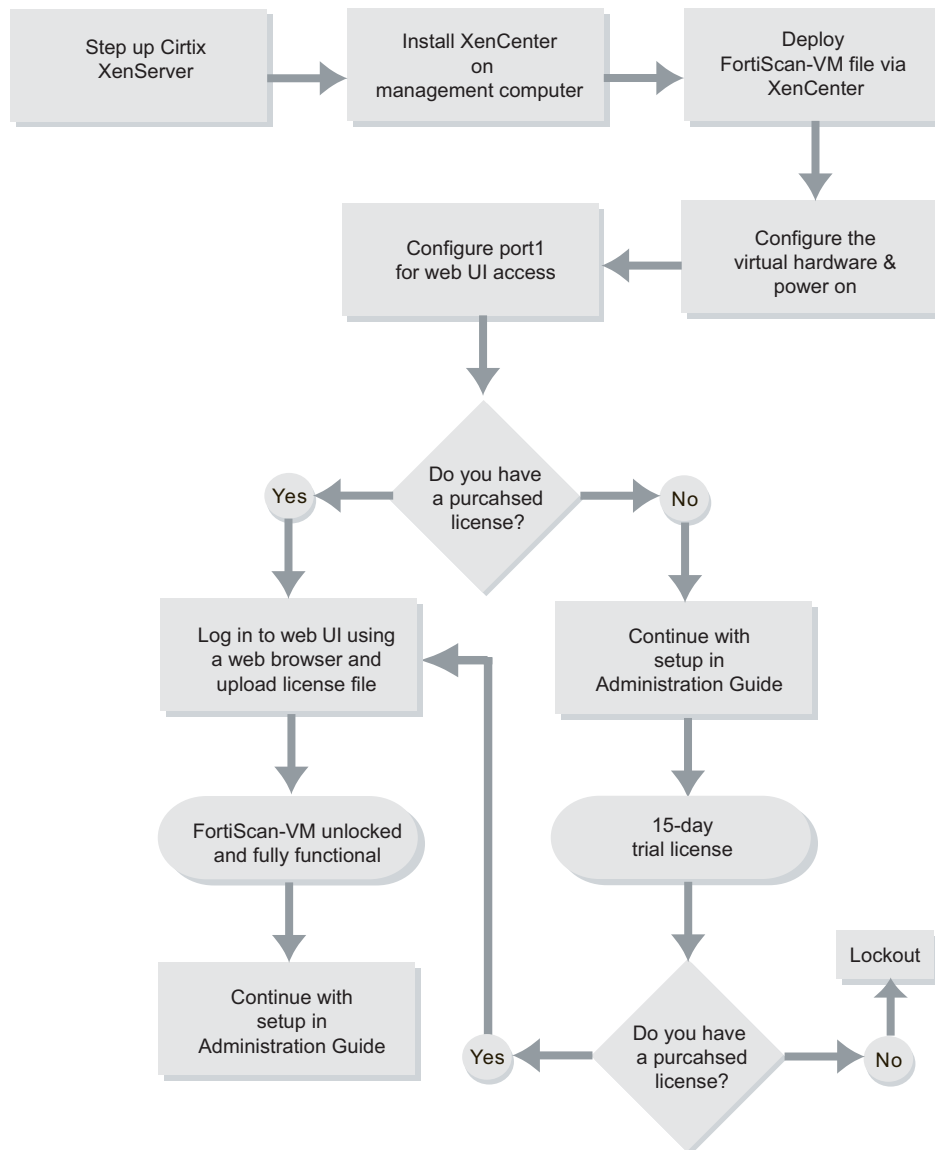
- ▶ **Power on the virtual machine**
- ✎ **Edit virtual machine settings**

- 8 Click *Power on the virtual machine*.
- 9 Continue with “Configuring access to the web UI & CLI” on page 43.

Deploying FortiScan-VM on Citrix XenServer

The diagram below overviews the process for installing FortiScan-VM on Citrix XenServer, which is described in the subsequent text.

Figure 4: Basic steps for installing FortiScan-VM (Citrix)



Converting and deploying the OVF package

Before you can configure FortiScan-VM, you must first use Citrix XenCenter to convert the open virtualization format (OVF) package to a format that can be used with Citrix XenServer, and to deploy the FortiScan-VM.ovf template package.



Tip: Alternatively, you can deploy the package using XenConvert.

To deploy the virtual appliance

- 1 On your management computer, start Citrix XenCenter.
- 2 Go to *Tools > Virtual Appliance Tools > Import Appliance*.
- 3 Select the FortiScan-VM.ovf template package.
- 4 In *Host name*, type the IP address or FQDN of the Citrix XenServer server.
- 5 In *User name*, type the name of your account on that server.
- 6 In *Password*, type the password for your account on that server.
- 7 Click *Next*.

The client converts the OVF package, 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 15 minutes to complete. When complete, the deployment should appear in XenCenter.

- 8 Continue with “[Configuring the virtual appliance's virtual hardware settings](#)” on [page 31](#).



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

- Resize the virtual disk (VMDK) (see “[Resizing the virtual disk \(vDisk\)](#)” on [page 32](#))
- Set the number of vCPUs (see “[Configuring the number of virtual CPUs \(vCPUs\)](#)” on [page 33](#))
- Set the vRAM on the virtual appliance (“[Configuring the virtual RAM \(vRAM\) limit](#)” on [page 35](#))
- Map the virtual network adapter(s) (“[Mapping the virtual NICs \(vNICs\) to physical NICs](#)” on [page 37](#)).

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

Configuring the virtual appliance's virtual hardware settings

After installing FortiScan-VM, log in to Citrix XenServer on the server and configure the virtual appliance's hardware settings to suit the size of your deployment.

For information on the limits of configurable values for FortiScan-VM, see the [FortiScan 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.



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

The FortiScan-VM package that you downloaded includes pre-sized VMDK (Virtual Machine Disk Format) files. However, they are only 30 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 datastore which has been formatted with 1 MB block size, you cannot size a single vDisk greater than 256 GB on your FortiScan-VM.

Consider also that, depending on the size of your organization's network, you might require more or less storage for your asset inventory, scan results, and reports. Guidelines for storage size vary by the number of assets (n):

- $n < 10,000$ assets: 1 TB
- $10,000$ assets $< n < 20,000$ assets: 2 TB

Fortinet recommends that you choose a vDisk size greater than 1024 GB (1 TB).

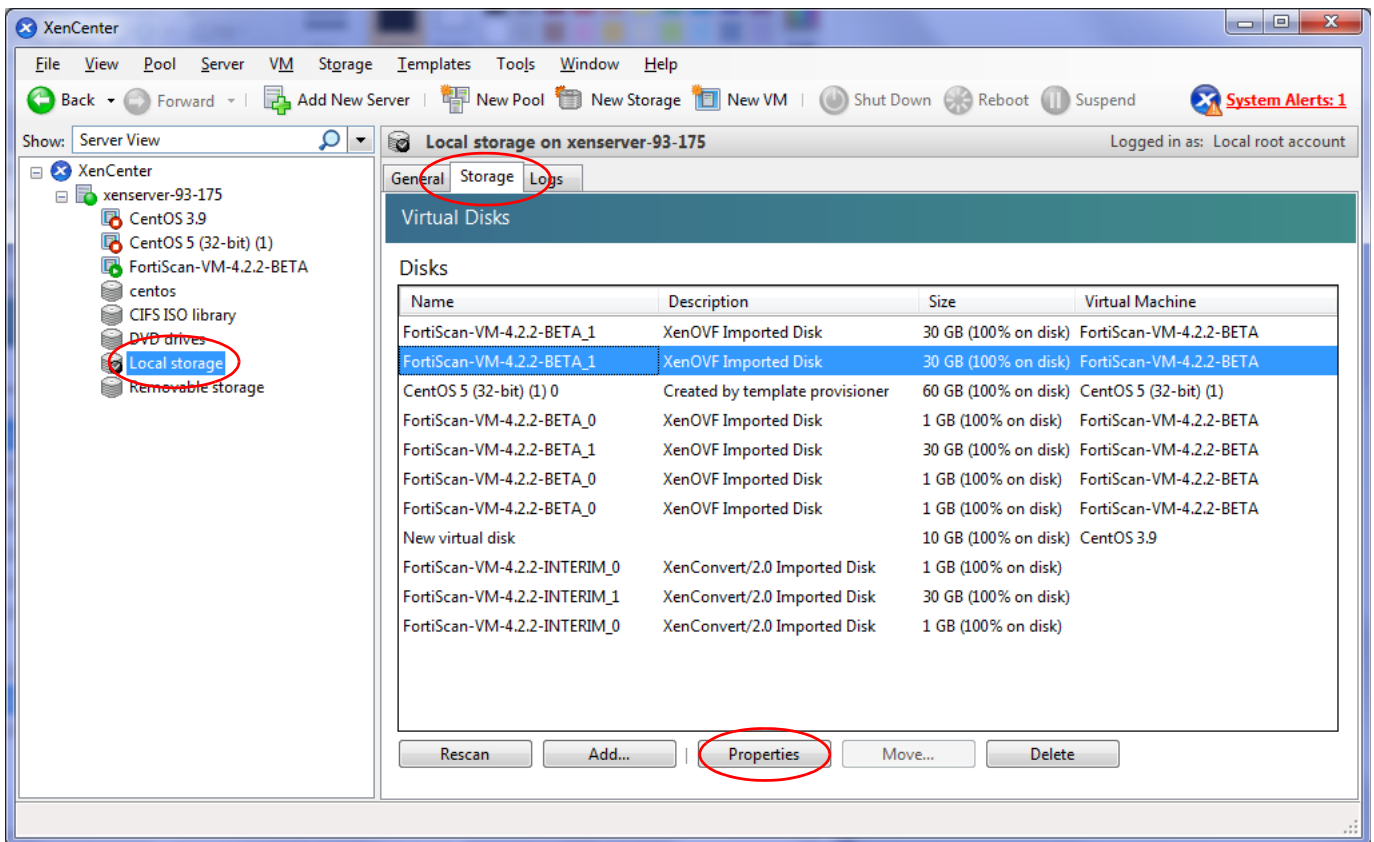
For more information on vDisk sizing, see:

<http://support.citrix.com/article/CTX125405>

To resize the vDisk

- 1 On your management computer, start Citrix XenCenter.
- 2 In *Hostname*, type the IP address or FQDN of the Citrix XenServer 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 left pane, click *Local Storage*.



7 Click the *Storage* tab.

8 From the list of vDisks, select the vDisk that you want to alter.

9 Click *Properties*.

The vDisk's properties dialog appears.

10 In the dialog's left pane, select *Size and Location*.

11 In the dialog's right pane, in *Size*, type the new size, in gigabytes (GB), of the vDisk.

12 Click *OK*.

13 If you do not need to change the other resources, power on the virtual appliance before continuing with "Configuring access to the web UI & CLI" on page 43.

Configuring the number of virtual CPUs (vCPUs)

By default, the virtual appliance is configured to use 2 vCPUs. Guidelines for vCPU allocation vary by the number of assets (n):

- $n < 10,000$ assets: 2 vCPUs
- $10,000$ assets $< n < 20,000$ assets: 4 vCPUs

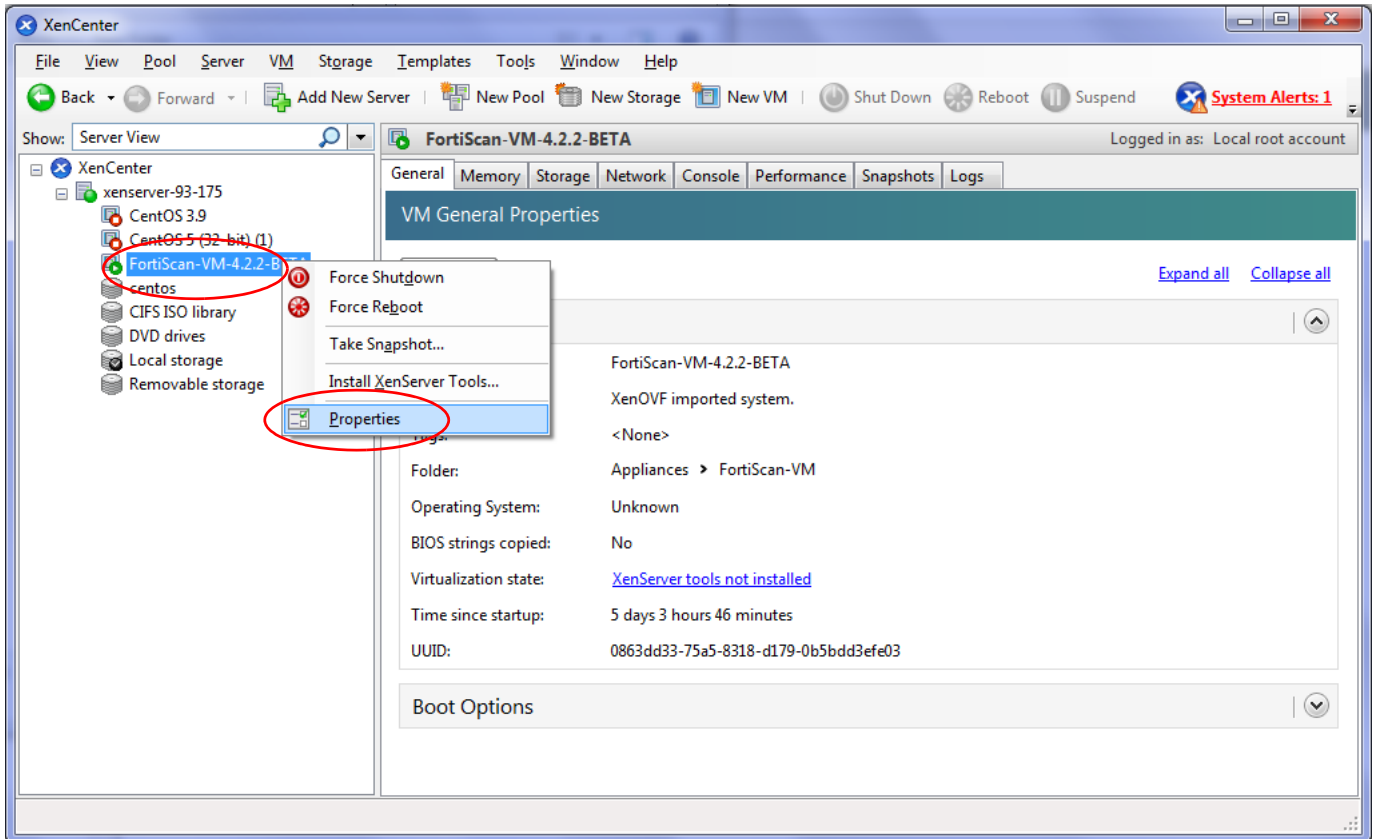
Change the value if necessary to allocate enough vCPUs for the size of your deployment.

For more information on vCPUs, see:

<http://support.citrix.com/article/CTX117960>

To change the number of vCPUs

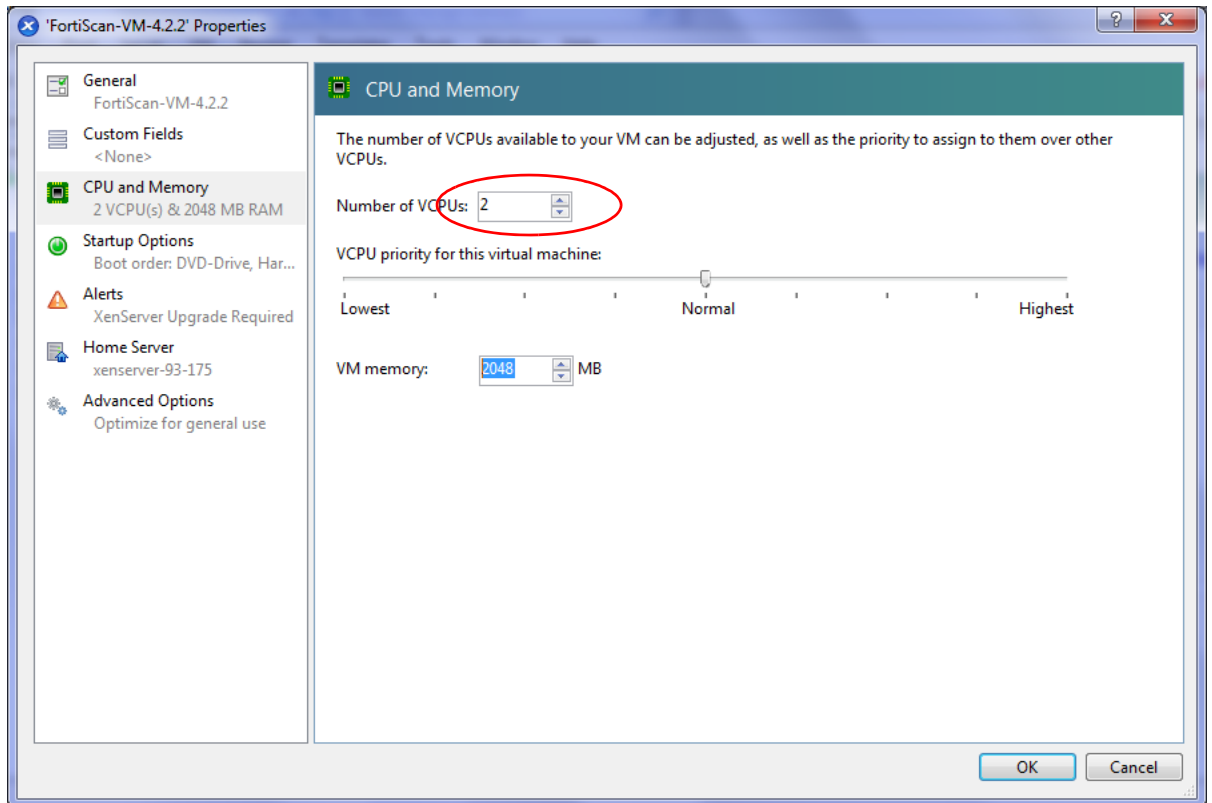
- 1 On your management computer, start Citrix XenCenter.
- 2 In *Hostname*, type the IP address or FQDN of the Citrix XenServer server.
- 3 In *User name*, type the name of your account on that server.
- 4 In *Password*, type the password for your account on that server.
- 5 Click *Login*.
- 6 In the left pane, right-click the name of the virtual appliance, such as *FortiScan-VM-4.2.3*, then select *Properties*.



The virtual appliance's properties dialog appears.

- 7 In the left pane, click *CPU and Memory*.

8 In *Number of vCPUs*, type the maximum number of vCPUs to allocate.



9 Click *OK*.

Configuring the virtual RAM (vRAM) limit

FortiScan-VM comes pre-configured to use 4 GB of vRAM. You can change this value. The valid range is from 4 GB to 16 GB. Appropriate values are suggested as follows, according to the number of assets (*n*) that will be monitored by your FortiScan-VM.

- $n < 2,000$ assets: 4 GB vRAM
- $2,000$ assets $< n < 10,000$ assets: 8 GB vRAM
- $10,000$ assets $< n < 20,000$ assets: 16 GB vRAM

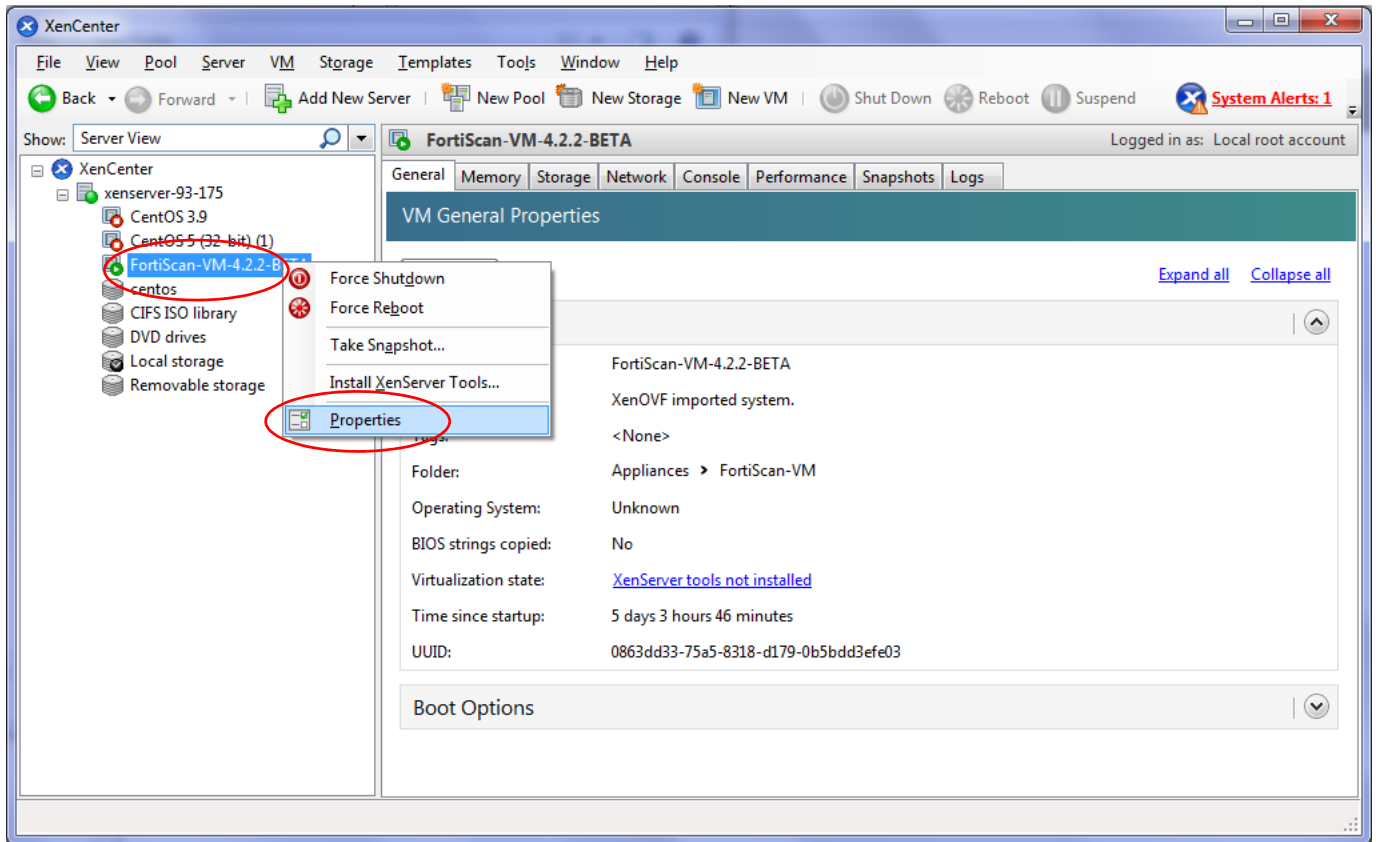


Note: It is possible to configure FortiScan-VM to use less vRAM, such as 2 GB. However, for performance reasons, it is not recommended.

To change the amount of vRAM

- 1 On your management computer, start Citrix XenCenter.
- 2 In *Hostname*, type the IP address or FQDN of the Citrix XenServer 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*.

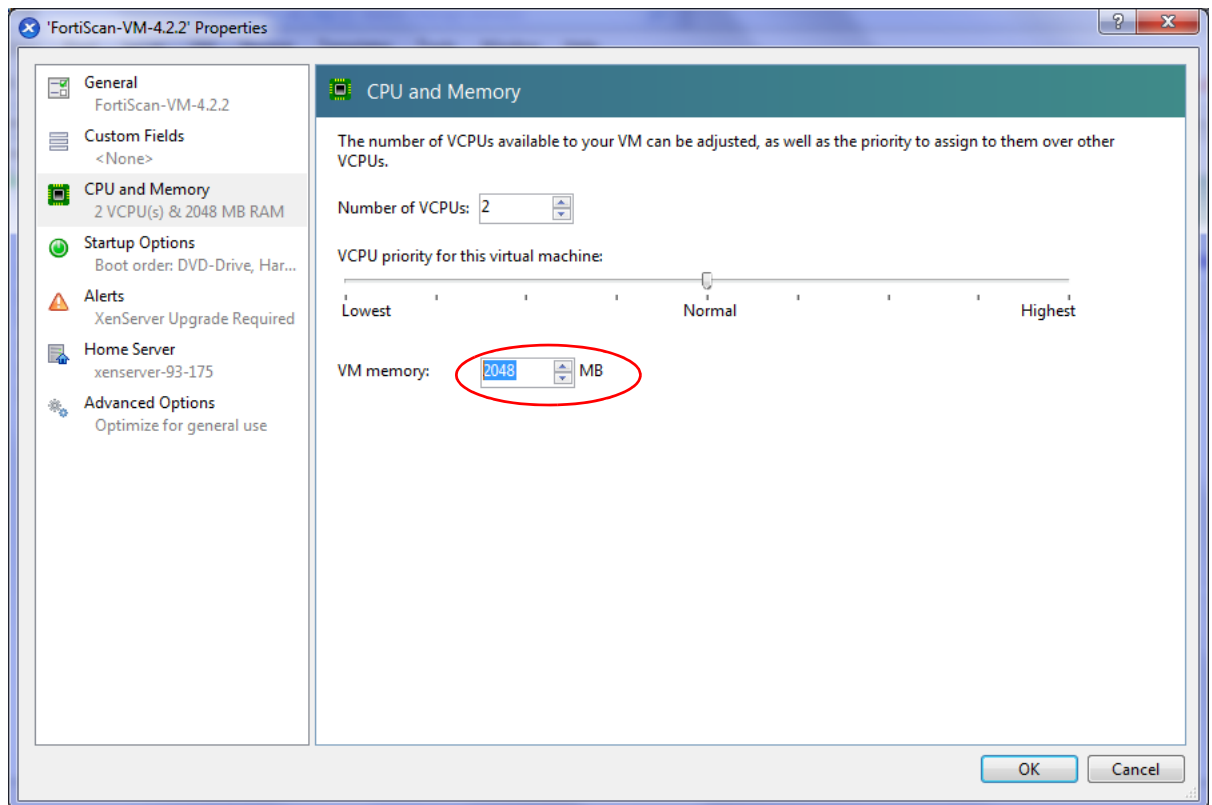
- 6 In the left pane, right-click the name of the virtual appliance, such as *FortiScan-VM-4.2.3*, then select *Properties*.



The virtual appliance's properties dialog appears.

- 7 In the left pane, click *CPU and Memory*.

8 In *VM memory*, type the maximum number in megabytes (MB) of the vRAM to allocate.



9 Click **OK**.

Mapping the virtual NICs (vNICs) to physical NICs

Appropriate mappings of the FortiScan-VM ports to physical ports depends on your existing virtual environment.

When you deploy the FortiScan-VM package, 4 vNICs are created and automatically mapped to a port group on 1 virtual switch (vSwitch) within the hypervisor. Each of those vNICs can be used by one of the 4 network interfaces in FortiScan-VM. (Alternatively, if you prefer, some or all of the network interfaces may be configured to use the same vNIC.) vSwitches are themselves mapped to physical ports on the server.

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

Table 4 provides an example of how vNICs could be mapped to the physical network ports on a server.

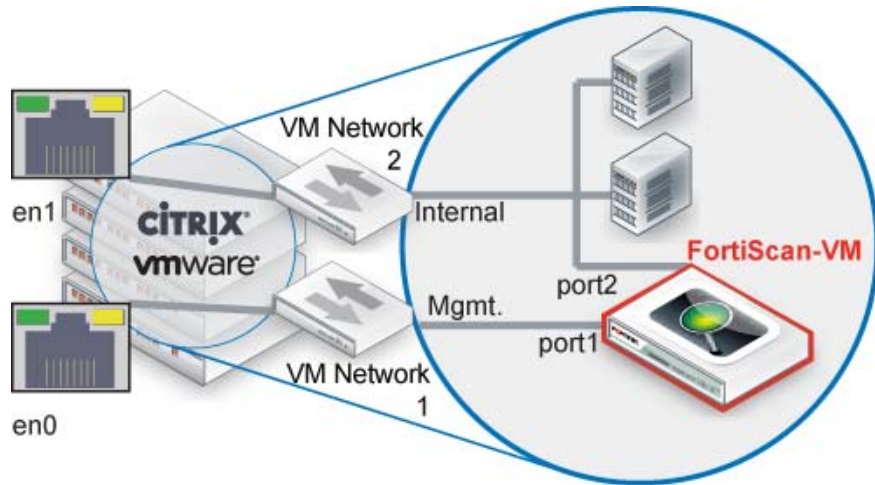


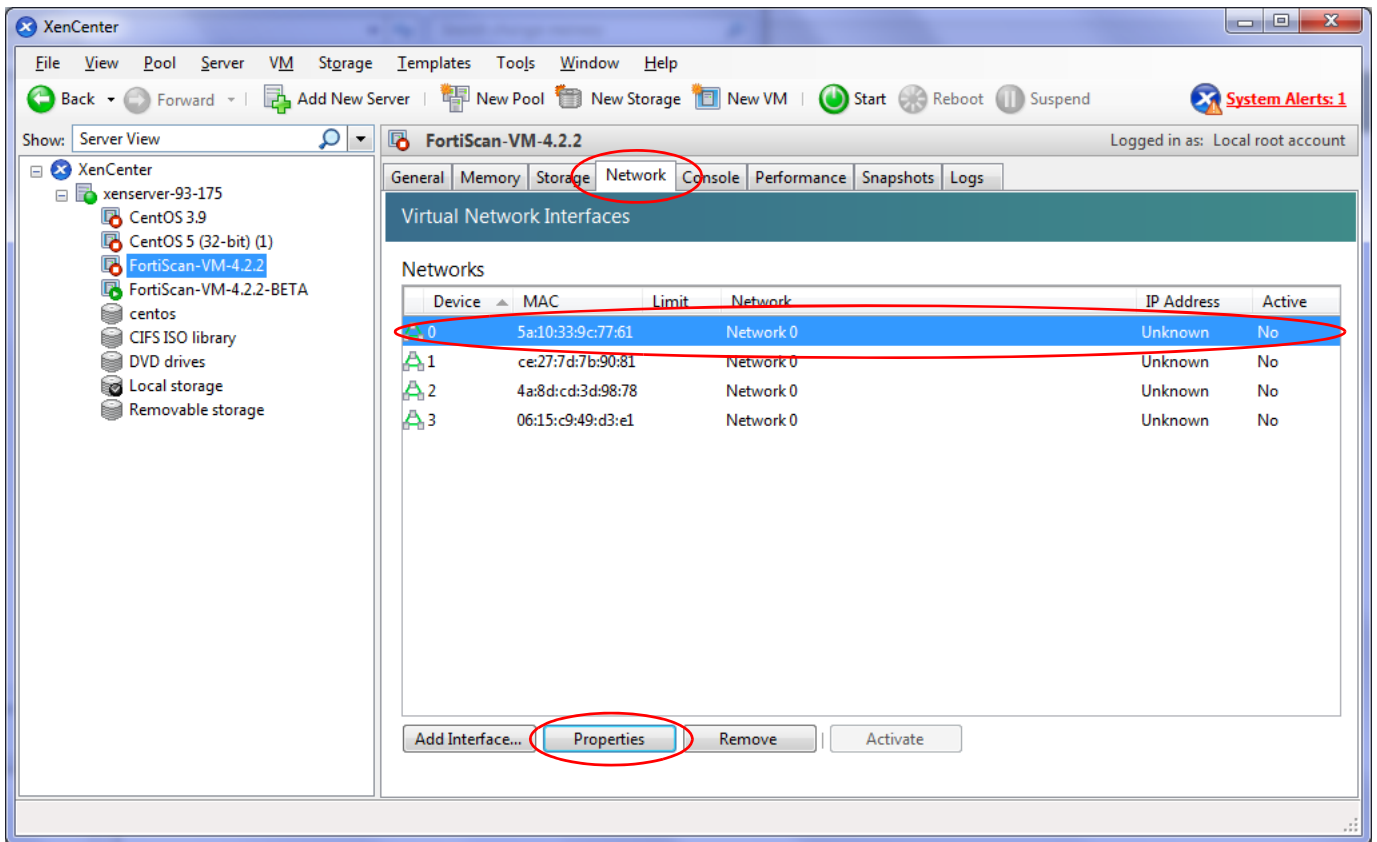
Table 4: Example: Network mapping

Citrix XenServer			FortiScan-VM
Physical Network Adapter	Network Mapping (vSwitch Port Group)	Virtual Network Adapter for FortiScan-VM	Network Interface Name in Web UI/CLI
eth0	VM Network 1	Management	port1
eth1	VM Network 2	Internal	port2
eth1	VM Network 2	Internal	port3
eth1	VM Network 3	Internet	port4

To map vNICs

- 1 On your management computer, start Citrix XenCenter.
- 2 In *Hostname*, type the IP address or FQDN of the Citrix XenServer 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 left pane, select the name of the virtual appliance, such as *FortiScan-VM-4.2.3*.

7 Click the *Network* tab.



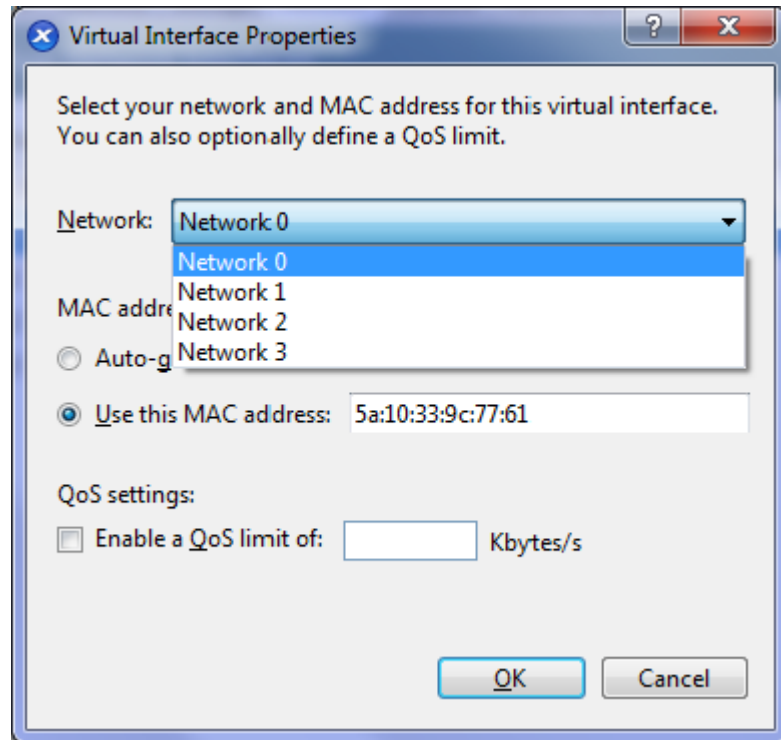
8 In the list of virtual network adapters, click the name of the virtual network adapter whose network mapping you want to change.

9 Click *Properties*.

The virtual appliance's properties dialog appears.

- From the *Network* 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 *Device 0* is mapped to the virtual network (vNetwork) named *Network 0*.



- Click *OK*.

Deploying FortiScan-VM on open source Xen

FortiScan-VM is deployed on the open source offering of the Xen Hypervisor via command lines, such as:

```
tar xvf FSC-VM-4.2.3.0229-FORTINET.out.xen.tgz
cd FortiScan-VM
./mk-fsc.sh
```



Note: You must run these command lines from a terminal with an X Windows environment. The shell script finishes by starting the virtual appliance in a foreground window.

Similar to the commercial offering of Citrix XenServer, configure virtual hardware settings to allocate appropriate resources for the size of your deployment **before** powering on the virtual appliance. For details, see the [documentation for the open source Xen Hypervisor](#).

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.



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

The FortiScan-VM package that you downloaded includes pre-sized VMDK (Virtual Machine Disk Format) files. However, they are only 30 GB, which is not large enough for most deployments. **Resize the vDisk before powering on the virtual machine.**

Consider that, depending on the size of your organization's network, you might require more or less storage for your asset inventory, scan results, and reports. Guidelines for storage size vary by the number of assets (n):

- $n < 10,000$ assets: 1 TB
- $10,000$ assets $< n < 20,000$ assets: 2 TB

Fortinet recommends that you choose a vDisk size greater than 1024 GB (1 TB).

By default, the virtual appliance is configured to use 2 vCPUs. Guidelines for vCPU allocation vary by the number of assets (n):

- $n < 10,000$ assets: 2 vCPUs
- $10,000$ assets $< n < 20,000$ assets: 4 vCPUs

Change the value if necessary to allocate enough vCPUs for the size of your deployment.

FortiScan-VM comes pre-configured to use 4 GB of vRAM. You can change this value. The valid range is from 4 GB to 16 GB. Appropriate values are suggested as follows, according to the number of assets (n) that will be monitored by your FortiScan-VM.

- $n < 2,000$ assets: 4 GB vRAM
- $2,000$ assets $< n < 10,000$ assets: 8 GB vRAM
- $10,000$ assets $< n < 20,000$ assets: 16 GB vRAM



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

Table 4 provides an example of how vNICs could be mapped to the physical network ports on a server.

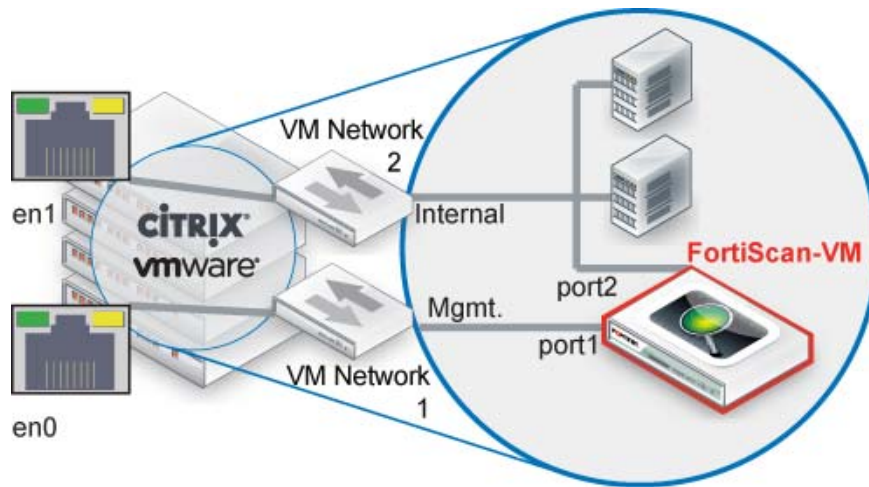


Table 5: Example: Network mapping

Citrix XenServer			FortiScan-VM
Physical Network Adapter	Network Mapping (vSwitch Port Group)	Virtual Network Adapter for FortiScan-VM	Network Interface Name in Web UI/CLI
eth0	VM Network 1	Management	port1
eth1	VM Network 2	Internal	port2
eth1	VM Network 2	Internal	port3
eth1	VM Network 3	Internet	port4

Continue with “Configuring access to the web UI & CLI” on page 43.

Configuring access to the web UI & CLI

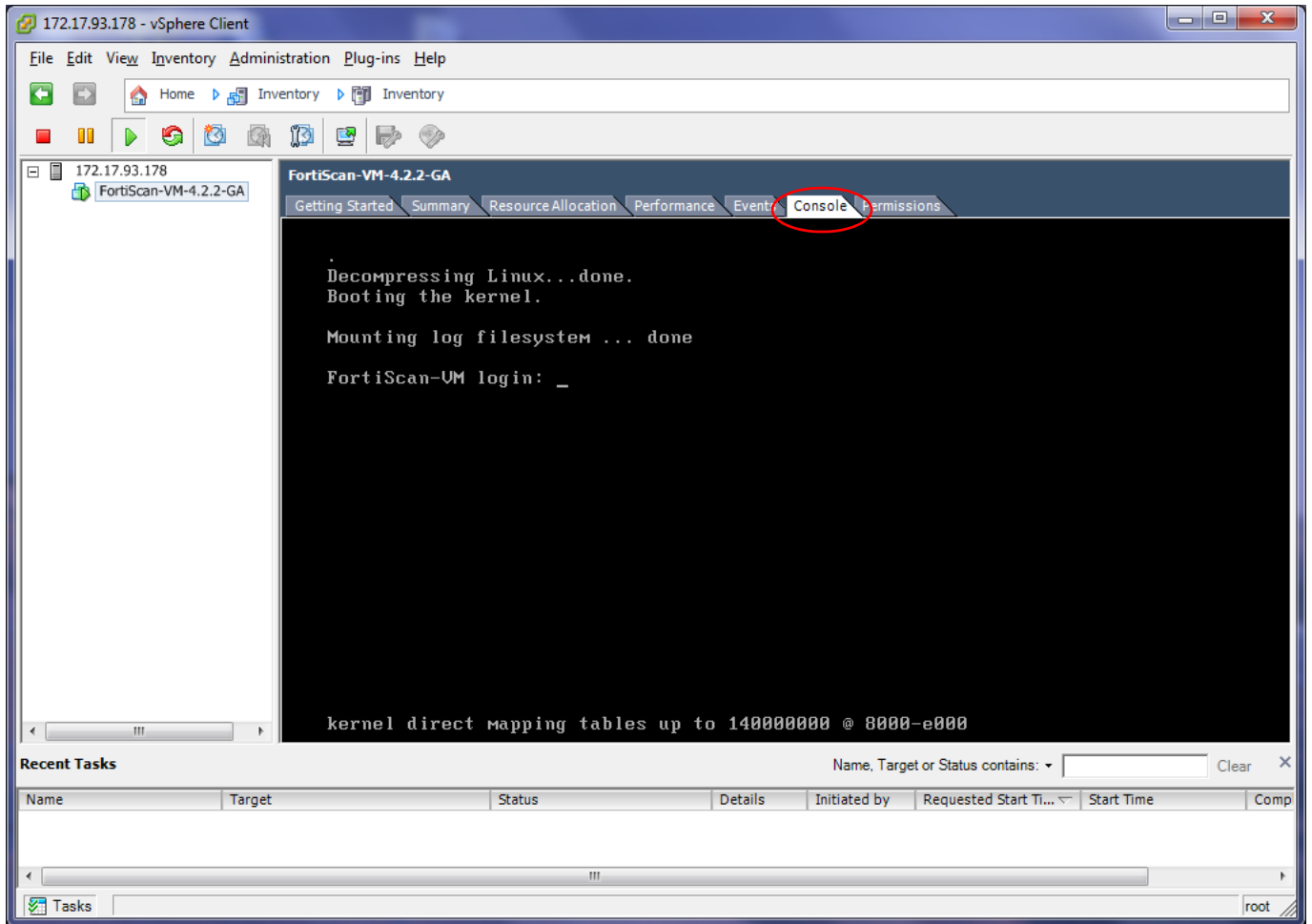
Once it is powered on, you must log in to the FortiScan-VM command line interface (CLI) via the console and configure basic network settings so that you can connect to the web UI and/or CLI of the appliance through your management computer's network connection.

To configure basic network settings in FortiScan-VM

- 1 On your management computer, start either:
 - VMware vSphere Client
 - Citrix XenCenterdepending on the VM environment in which you have deployed FortiScan-VM.
- 2 Log in to the VM environment.

- 3 Open the console of the FortiScan-VM virtual appliance.
On VMware vSphere Client:
 - In the left pane, select the name of the virtual appliance, such as *FortiScan-VM-4.2.3*.
 - Click the *Console* tab.

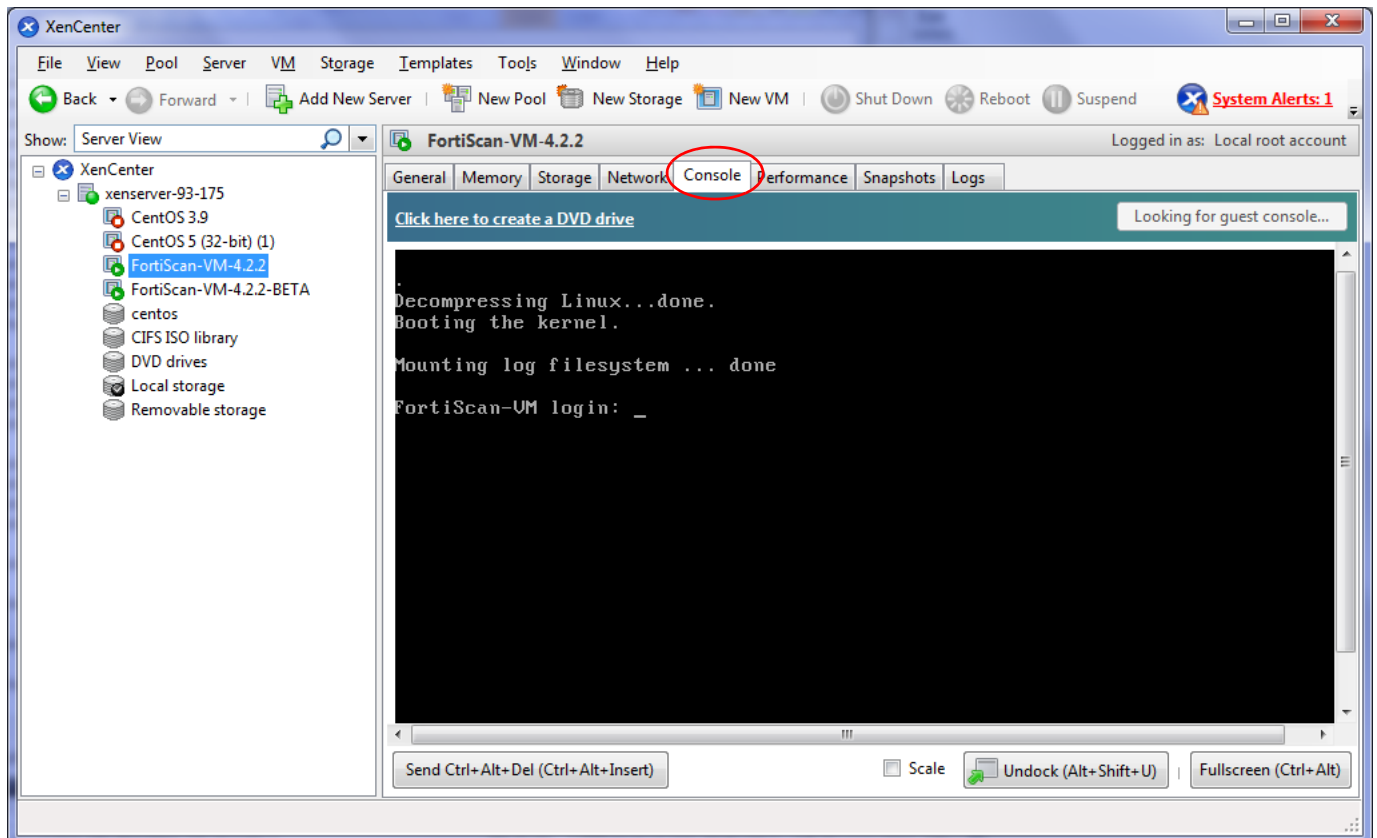
Figure 5: Console tab in VMware vSphere Client



On Citrix XenCenter:

- In the left pane, select the name of the virtual appliance, such as *FortiScan-VM-4.2.3*.
Several tabs for that virtual machine will appear in the right pane.
- Click the *Console* tab.

Figure 6: *Console tab in Citrix XenCenter*



- 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 global
  config system interface
    edit port1
      set ip <address_ipv4> <netmask_ipv4>
    end
```

where:

- `<address_ipv4>` is the IP 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 25](#), [“Mapping the virtual NICs \(vNICs\) to physical NICs” on page 37](#), or [“Deploying FortiScan-VM on open source Xen” on page 41](#))
- `<netmask_ipv4>` is its netmask in dotted decimal format, such as `255.255.255.0`



Note: By default, to prevent potential route confusion, `port2`, `port3`, and `port4` are disabled (“down”). To bring up a network interface, when editing it, enter the command `set status up`.

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

```
config system dns
  set primary <dns_ipv4>
  set secondary <dns_ipv4>
end
```

where `<dns_ipv4>` is the IP address of a DNS server.

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

```
config system route
  edit 0
    set gateway <router_ipv4>
    set device port1
  end
```

where `<router_ipv4>` 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 FortiScan-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.)



Tip: 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 details, or instructions on how to configure the time and time zone, see the [FortiScan Administration Guide](#).

- 9 Continue by uploading the license file (see [“Uploading the license” on page 48](#)).

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 54](#).



Note: 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.



Note: The trial period begins the first time you power on your FortiScan-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 48](#).

Uploading the license

When you purchase a license for FortiScan-VM, Fortinet Technical Support (<https://support.fortinet.com>) will provide a license file that you can use to convert the 15-day trial license to a permanent, paid license.



Tip: 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 FortiScan-VM license to support your needs.

You can upload the license via a web browser connection to the web UI, or via the CLI.

To upload the license via the web UI

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

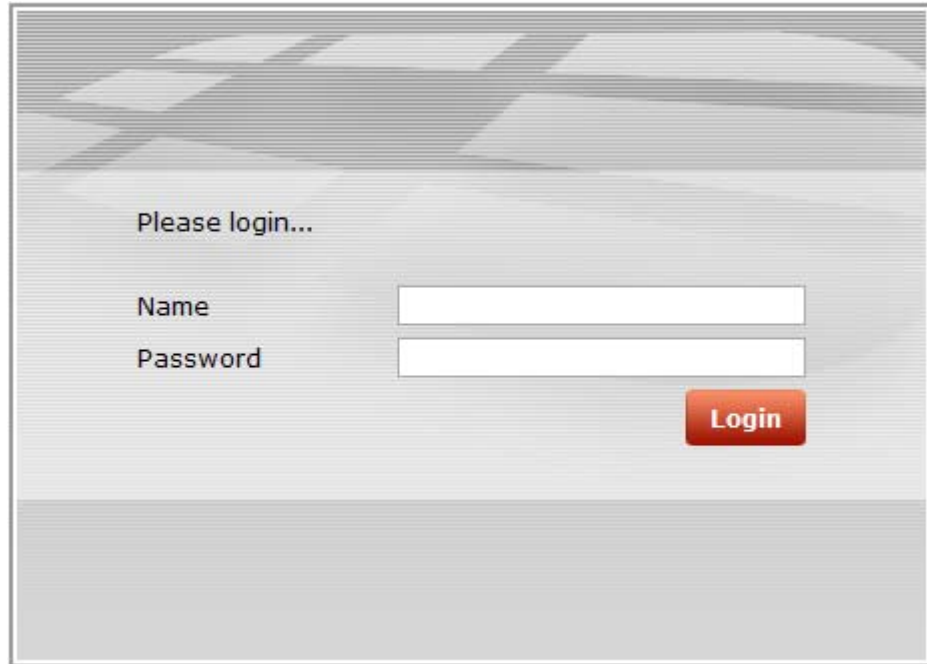
<https://192.168.1.99/>

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



Note: 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 [FortiScan Administration Guide](#).

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 FortiScan-VM or a LENC version of FortiScan, 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.)

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 FortiScan appliance ships with a self-signed X.509 certificate, which it presents to clients whenever they initiate an HTTPS connection to the FortiScan appliance. When you connect, depending on your web browser and prior access of the FortiScan 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 web site. The common name (CN) field in the certificate, which usually contains the host name of the web site, 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.

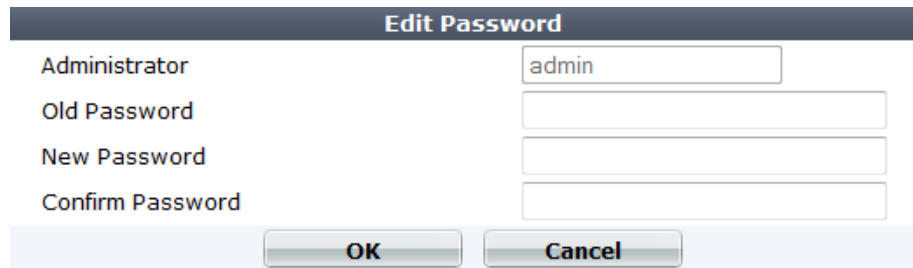
Both warnings are normal for the default certificate. SSL v3 and TLS v1.0 are supported.

- 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.

For details on accepting the certificate, see the documentation for your web browser.

- 4 In the *Name* field, type `admin`.
- 5 Click *Login*. (Initially, there is no password.)

A password setting dialog appears.

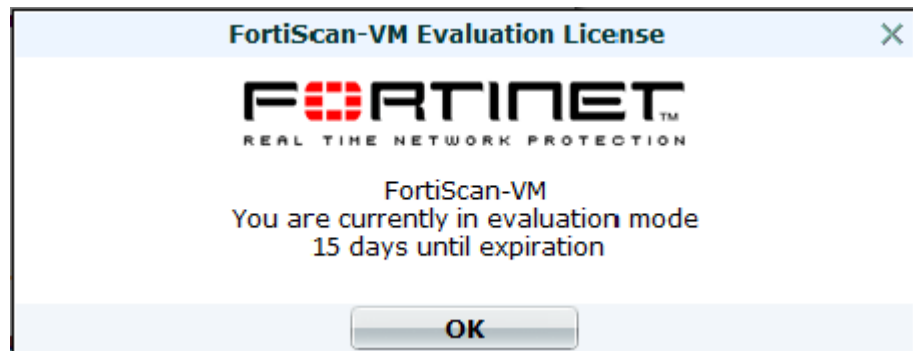


The screenshot shows a dialog box titled "Edit Password". It contains four text input fields. The first field, labeled "Administrator", contains the text "admin". The other three fields, labeled "Old Password", "New Password", and "Confirm Password", are empty. At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

- 6 In *New Password* and *Confirm Password*, enter a password with sufficient complexity and number of characters to deter brute force and other attacks.
- 7 Click *OK*.
- 8 Log in again with the new password.

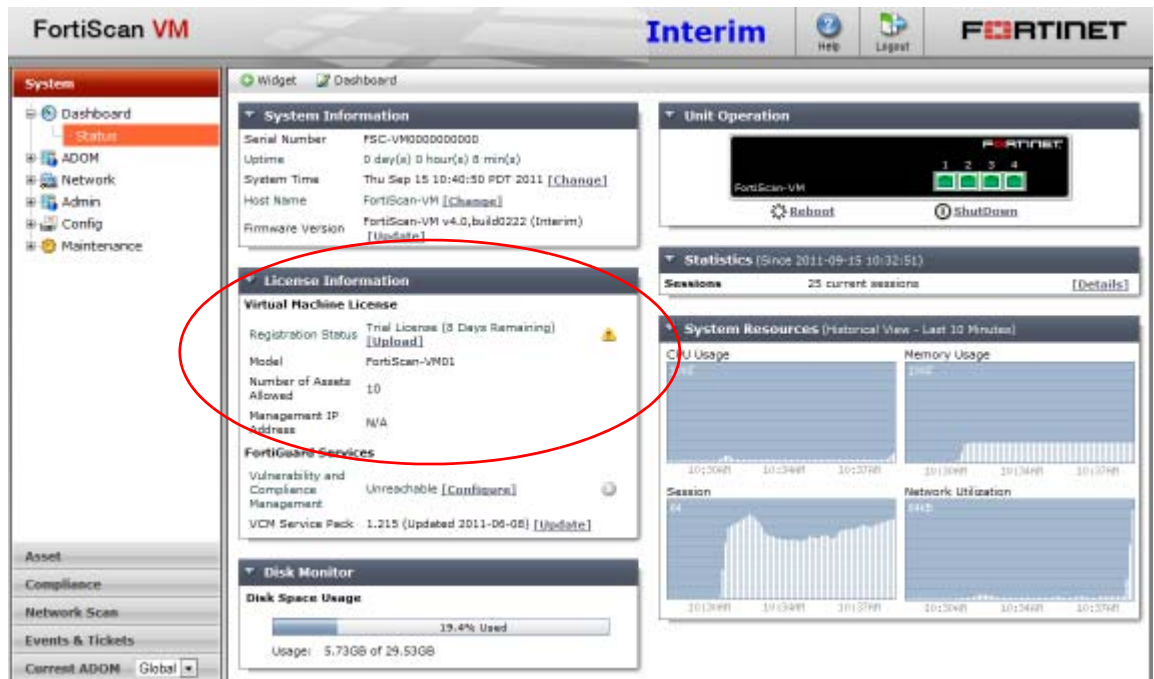
The web UI appears. A banner may appear that indicates the number of days remaining in the trial license period. If so, click *OK* to dismiss the banner.

Figure 7: Trial license period notification banner

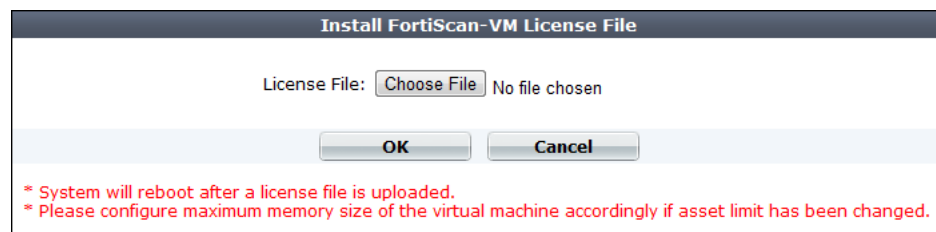


Otherwise the web UI initially displays its dashboard. The *License Information* widget displays the current license status and contains a link where you can upload a license file.

Figure 8: License Information widget in the web UI



- 9 In the *Registration Status* row of the *License Information* widget, click the *Upload* link. The *Install FortiScan-VM License File* dialog opens.



- 10 Locate the license file and click *OK*.

Your browser uploads the license file. Time required varies by the size of the file and the speed of the network connection. A message appears:

FortiScan Virtual Machine license has been uploaded. Please wait while system is being restarted.

The virtual appliance restarts. This may take a few minutes, depending on the hardware capabilities and resource allocation of the VM environment.

- 11 To verify that the license was uploaded successfully, log in to the web UI again, then view the *License Information* widget. (Alternatively, go to *System > Maintenance > FortiGuard*.)

Figure 9: System > Maintenance > FortiGuard

The screenshot shows the 'Install FortiScan-VM License File' page. It is divided into two main sections: 'Virtual Machine License' and 'FortiGuard Subscription Services'. In the 'Virtual Machine License' section, the 'Registration Status' is 'Licensed' with an '[Upload]' link, which is circled in red. Other details include 'Number of Assets Allowed' (20000) and 'Management IP Address' (192.168.4.99). A green checkmark icon is visible to the right. The 'FortiGuard Subscription Services' section includes 'Vulnerability and Compliance Management' (Not Registered with a '[Subscribe]' link) and 'VCM Service Pack' (1.234, updated 2011-10-20, with an '[Update]' link). A yellow warning icon is present. Below this is the 'Service Configuration Options' section, which is expanded to show 'FortiGuard Server' settings (checkboxes for 'Use override server address' and 'Use Web Proxy', and input fields for 'IP', 'Port' (8080), 'Name', and 'Password') and 'Vulnerability and Compliance Management' settings (checkbox for 'Scheduled Update' with a '[Request Update Now]' link, and radio buttons for 'Every', 'Daily' (selected), and 'Weekly' with dropdown menus for frequency and hour/day).

12 Continue with “What’s next?”.

To upload the license via the CLI

- 1 In a plain text editor, open the FortiScan-VM license file.
- 2 Select and copy **all** of the text in the license file.
- 3 Log in to the CLI of the appliance.

To connect through the console, see [Figure 5](#) or [Figure 6](#).

To connect through SSH, use an SSH client such as PuTTY configured to use SSH v1 with DES and 64-bit strength or less. Connect to the IP address that you configured for port1 on TCP port 22.

- 4 Enter the following commands:

```
config global
  execute update-vm-license '<license_str>'
```

where <license_str> is the pasted contents of the license file.

- 5 To confirm that the license was successfully uploaded and view its bound IP, enter the following command:

```
get system status
```

Output similar to the following should appear:

```
global # get system status
Version: FortiScan-VM v4.0,build0229,111115 (MR2)
Branch point: 229
Release Version Information: MR2
Serial-Number: FSC-VM0000000004
BIOS version: 04000002
VCM Service Pack: 2.075_1.234 [Thu Nov 20 19:13:00 2011]
The number of registered Compliance Assets: 11
Max Number of Compliance Host Asset Agents: 20000
Admin Domain Status: enabled
Number of Admin Domain: 2
Max number of administrative domains: 200
Hostname: FortiScan-VM
FIPS mode: disabled
System Time: Fri Nov 28 12:19:38 PDT 2011

Disk Usage: Free 2890.26GB, Total 2900.53GB
License Status: Valid
```

where License Status and Max Number of Compliance Host Asset Agents should match your purchased license.

- 6 Continue with "What's next?".

What's next?

At this point, the FortiScan-VM virtual appliance is running, and it has received a license file, but its operating system is almost entirely unconfigured, and you have not deployed FortiScan agents. Before you can use FortiScan-VM, you must configure it. Usually, you should also deploy FortiScan agents.

Configure the FortiScan-VM software and deploy FortiScan agents using the [FortiScan Administration Guide](#).

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

Updating the virtual hardware

By default, FortiScan-VM uses VMware virtual hardware version 4. Should you need to update your FortiScan-VM's virtual hardware, simply be sure to shut down FortiScan-VM before doing so.

For example, if you have a VMware ESX 4.0 environment that supports virtual hardware version 7, and you want to provide version 7 feature support such as backups to FortiScan-VM, you would:

- 1 Shut down FortiScan-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 FortiScan-VM.

For more information, see:

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

Index

Symbols

- _email, 9
- _fqdn, 9
- _index, 9
- _int, 9
- _ipv4, 9
- _ipv4/mask, 9
- _ipv4mask, 9
- _ipv6, 9
- _ipv6mask, 9
- _name, 9
- _pattern, 9
- _str, 9
- _url, 9
- _v4mask, 9
- _v6mask, 9

Numerics

- 3DES, 49

A

- AES, 49
- authentication, 49

B

- backup, 54
- best practices, 5
- bit strength, 49, 52
- bridging, 25
- browser
 - warnings, 49

C

- certificate
 - default, 49
 - mismatch, 49
 - self-signed, 49
 - warning, 49
- certificate authority (CA), 49
- CIDR, 9
- command line interface (CLI), 8
- comments, 6

- common name (CN) field, 49
- console, 43, 44
- conventions, 7

D

- datastore, 32
- default
 - certificate, 49
 - IP address, 46
 - password, 50
- DES, 49, 52
- documentation, 6
 - commenting on, 6
 - conventions, 7
- domain name
 - certificate, 49
 - FortiScan, 53
- dotted decimal, 9
- down, 46

E

- encryption
 - weak, 5, 49
- Error 113, 49
- ERROR_SSL_VERSION_OR_CIPHER_MISMATCH, 49
- evaluation, 5
- expected input, 8
- exploit, 4

F

- FAQ, 6
- Firefox, 49
- FortiGuard
 - services, 12
 - Vulnerability and Compliance Management service, 53
- Fortinet
 - customer service, 5
 - Forums, 5
 - Knowledge Base, 6
 - Technical Documentation, 6
 - conventions, 7
 - Technical Support, 5, 12
 - Technical Support, registering with, 12
- FortiScan-VM, 49
- fully qualified domain name (FQDN), 9

G

gateway, 46
guidelines, 17, 18, 22, 31, 32, 33, 41

H

handshake, 49
hardware abstraction layer (HAL), 10
host name, 49, 53
how-to, 6
HTTPS, 49
hypervisor, 10

I

index number, 9
input constraints, 8
installation, 6
IP address, 46, 49
 private network, 7

K

Knowledge Base, 6

L

LENC, 5
license, 5, 12, 49
 status, 50, 53
 trial, 5, 50
 upload, 50
low encryption (LENC), 5, 49

M

managed security service provider (MSSP), 5
management computer, 11
Mozilla
 Firefox, 49

N

netmask, 46
network file system (NFS), 32
network interface, 46
NFS, 17

O

open virtualization format (OVF), 31

P

password, 50
pattern, 9
performance, 10, 24
port
 down, 46
port1, 46, 48
port2, 46
port3, 46
port4, 46
product registration, 12

R

RC2, 49
RC4, 49
registering
 with Fortinet Technical Support, 12
regular expression, 9
RFC
 1918, 7
risk, 4
route
 confusion, 46
 static, 46
router, 46

S

security certificate, 49
self-signed, 49
serial number, 53
shell script, 41
sizing guidelines, 17, 18, 22, 31, 32, 33, 41
software-as-a-service (SaaS), 5
SSH, 46
 version, 52
SSL
 version, 49
ssl_error_no_cypher_overlap, 49
stackable license, 5
static route, 46
storage repository, 17
string, 9
syntax, 8

T

technical
 documentation, 6
 support, 5
time zone, 46
TLS
 version, 49
trial license, 5, 49
 period, 50

trust certificate, 49

U

up, 46
upload, 50
URL, 49

V

value parse error, 9
vDisk, 17
version
 FortiScan, 53
 supported hypervisor, 10
virtual machine, 10, 11
virtual machine disk format (VMDK), 17, 32, 41
virtualization, 6

virtualization technology (VT), 10

W

web browser, 46
 warnings, 49
wild cards, 9

X

X Windows, 41
X.509, 49
XenConvert, 31

Z

zero-day vulnerabilities, 4

FortiScan-VM 4.0 MR2 Patch 3 Install Guide

12 April 2012 • 5th Edition

Copyright© 2012 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance 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 the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. 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.

Technical Documentation	http://docs.fortinet.com
Knowledge Base	http://kb.fortinet.com
Forums	http://support.fortinet.com/forum
Training	http://training.fortinet.com
Technical Support	https://support.fortinet.com

Please report errors or omissions to:
techdoc@fortinet.com