



FortiAnalyzer-VM™

Version 4.0 MR2
Install Guide

FORTINET®

FortiAnalyzer-VM™ Installation Guide

Version 4.0 MR2

June 28, 2011

Revision 2

© Copyright 2011 Fortinet, Inc. All rights reserved. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet, Inc.

Trademarks

ABACAS, APSecure, Dynamic Threat Prevention System (DTPS), FortiAnalyzer®, FortiASIC, FortiBIOS, FortiBridge, FortiClient®, FortiDB, FortiGate®, FortiGate Unified Threat Management System, FortiGuard®, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiManager®, FortiMail®, Fortinet®, FortiOS®, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiScan, FortiShield, FortiSwitch, FortiVoIP, FortiWeb, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

Overview of FortiAnalyzer-VM	5
Resources.....	5
Architecture of the FortiAnalyzer-VM.....	6
Licensing	6
Registering your Fortinet product.....	6
Customer service & technical support	7
Training	7
Documentation	7
Comments on Fortinet technical documentation	7
Installing FortiAnalyzer-VM.....	9
Installation Overview	9
Installing FortiAnalyzer-VM.....	10
Getting the FortiAnalyzer-VM software	10
Deploying the FortiAnalyzer-VM software	10
Logging in.....	12
Resize disk (VMDK).....	12
Configuring the number of virtual CPUs	13
Setting the virtual RAM.....	13
Configuring virtual networks	13
Configuring virtual network adaptor(s).....	14
Powering on FortiAnalyzer-VM	15
Uploading the License.....	15
What next?.....	17

Overview of FortiAnalyzer-VM

FortiAnalyzer-VM is a virtual appliance that provides integrated log collection and reporting tools. Reports analyze logs for email, FTP, web browsing, security events, and other network activity to help identify security issues and reduce network misuse and abuse.

In addition to logging and reporting, FortiAnalyzer-VM also has several major features that augment or enable certain FortiGate unit functionalities, such as DLP archiving and quarantining, and improve your ability to stay informed about the state of your network.

FortiAnalyzer-VM includes a 15-day trial. The trial period begins the first time you start FortiAnalyzer-VM. You can install your full license from FortiCare at any time during or after the trial period.

This chapter provides an overview of the FortiAnalyzer-VM and the prerequisites to install the FortiAnalyzer-VM.

Fortinet provides:

- FortiAnalyzer-VM in VMware VM version 4
- six models of FortiAnalyzer-VM: VM-100, VM-400, VM-1000, VM-2000, VM-4000, and VM-UNL.

Resources

Table 1 shows the resources available with each FortiAnalyzer-VM model.

Table 1: FortiAnalyzer-VM resources

	FortiAnalyzer-VM-100	FortiAnalyzer-VM-400	FortiAnalyzer-VM-1000	FortiAnalyzer-VM-2000	FortiAnalyzer-VM-4000	FortiAnalyzer-VM-UNL
Hypervisor supported versions	VMware ESX/ESXi 3.5/4.0/4.1					
Maximum vCPUs	4 (VM version 4) / 8 (VM version 7)					
Maximum vNICs	4 (VM version 4) / 10 (VM version 7)					
Maximum vRAM	4 GB					
Maximum Internal Storage	1 TB	2 TB	2 TB (VMware limitation)	2 TB (VMware limitation)	2 TB (VMware limitation)	2 TB (VMware limitation)
Maximum External SQL Database	1 TB	2 TB	4TB	8TB	24TB	Unlimited
Maximum Devices Support	100	300	2000	2000	2000	Unlimited ¹

1. Currently software limited to 5000.

Most resources in Table 1 are available after successful deployment of the OVF file and validation of the license file. See “[Deploying the FortiAnalyzer-VM software](#)” on page 10 and “[Uploading the License](#)” on page 15.

For your convenience, the FortiAnalyzer-VM includes pre-sized VMDKs (Virtual Machine Disk Format). After deploying the FortiAnalyzer-VM (see “[Deploying the FortiAnalyzer-VM software](#)” on page 10), you can change the size of the files before the initial startup and configuration. Before doing so, you need to understand the size limitations of your VMFS VM datastore (not relevant to NFS datastores). 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 - 1024 GB maximum file size
- 8 MB block size - 2048 GB maximum file size

For example, if you select an 800 GB datastore which has been formatted with 1 MB block size, you cannot size a single virtual disk (VMDK) greater than 256 GB on your FortiAnalyzer-VM.

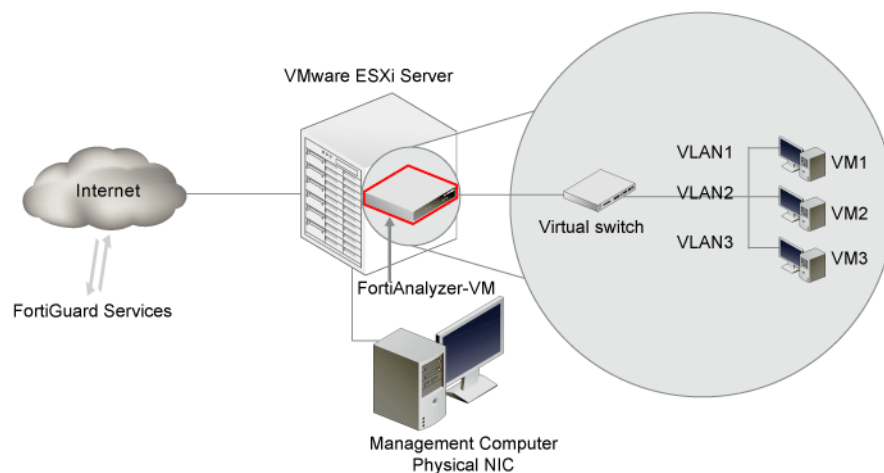
For more information of VMFS block sizing and recommendations, see <http://communities.vmware.com/docs/DOC-11920>.

Architecture of the FortiAnalyzer-VM

FortiAnalyzer-VM works in conjunction with VMware vSphere to leverage the power of virtualization to provide integrated log collection and reporting tools.

The FortiAnalyzer-VM runs on the VMware ESX/ESXi server and is managed using the Web Config GUI running on the management computer. See [Figure 1](#).

Figure 1: FortiAnalyzer-VM architecture



Licensing

When you place an order for FortiAnalyzer-VM, a registration number is sent to the email address used on the order form. Use the registration number to register with FortiCare (<https://support.fortinet.com>) and to obtain a license file, which is used to activate the FortiAnalyzer-VM.

For new installations, the CLI and Web Config are locked until you enter a license. Once a license is entered, the CLI and Web Config are unlocked and fully functional.

Registering your Fortinet product

Before you begin to configure and customize features, take a moment to register your Fortinet product at the Fortinet Technical Support web site, <https://support.fortinet.com>. Many Fortinet customer services, such as firmware updates, technical support, and FortiGuard Antivirus and other FortiGuard services, require product registration.

Customer service & 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.

To learn about the technical support 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 [Fortinet Technical Support Requirements](#).

Training

Fortinet Training Services provides classes that orient you quickly to your new equipment, and certifications to verify your knowledge level. Fortinet provides a variety of training programs to serve the needs of our customers and partners world-wide.

To learn about the training services that Fortinet provides, visit the Fortinet Training Services web site at <http://campus.training.fortinet.com>, or email them at training@fortinet.com.

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 such as technical notes.

Fortinet Knowledge Base

The Fortinet Knowledge Base provides additional Fortinet technical documentation, such as troubleshooting and how-to-articles, examples, FAQs, technical notes, and more. Visit the Fortinet Knowledge Base at <http://kb.fortinet.com>.

Comments on Fortinet technical documentation

Please send information about any errors or omissions in this technical document to techdoc@fortinet.com.

Installing FortiAnalyzer-VM

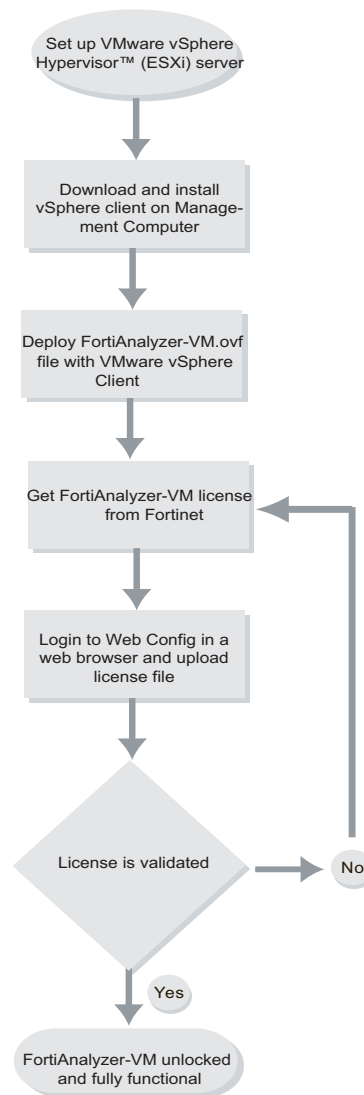
FortiAnalyzer-VM software is installed on the VMware vSphere Hypervisor™ (ESX/ESXi) server. VMware vSphere Hypervisor™ (ESX/ESXi) software **MUST** be installed prior to installing FortiAnalyzer-VM. For installation instructions, refer to the following web site: <http://www.vmware.com/products/esxi>.

This chapter provides the details of installing the FortiAnalyzer-VM.

Installation Overview

Figure 2 outlines the basic steps of installing the FortiAnalyzer-VM.

Figure 2: Overview of installing FortiAnalyzer-VM



Installing FortiAnalyzer-VM

Ensure the following prerequisites are met before installing FortiAnalyzer-VM:

- The VMware vSphere Hypervisor software (ESX/ESXi) must be installed on a server prior to installing the FortiAnalyzer-VM. This documentation does not cover how to install the VMware server. Go to <http://www.vmware.com/products/vsphere-hypervisor/index.html> for installation details.
- The VMware vSphere Client™ is installed on the Management Computer. This could be a desktop or a laptop that will be used to manage the devices.

Getting the FortiAnalyzer-VM software

The FortiAnalyzer-VM software is provided by Fortinet.

- 1 From the link provided by Fortinet, save the virtual appliance to the management computer.
- 2 Extract the zipped files to a folder. The following table describes the files in the folder:

Table 2: Files in the folder

Filename	Description
datadrive.vmdk	Virtual disk.
FortiAnalyzer-VM.ovf	This is a *.ovf file formatted in VM version 4 and is deployed for ESX/ESXi 3.5/4.0/4.1.
faz.vmdk	Virtual disk.

Deploying the FortiAnalyzer-VM software

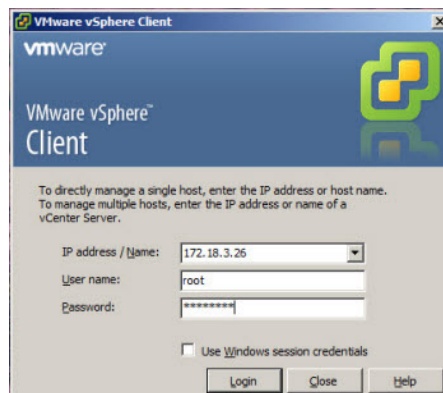
Before configuring the FortiAnalyzer-VM, the FortiAnalyzer-VM.ovf file needs to be deployed using the VMware vSphere Client™.

To deploy the software

Using the VMware vSphere Client on your management computer, deploy the *.ovf template:

- 1 Login using the VMware vSphere Client.
- 2 Enter the IP address, user name, and password of the ESX/ESXi server.

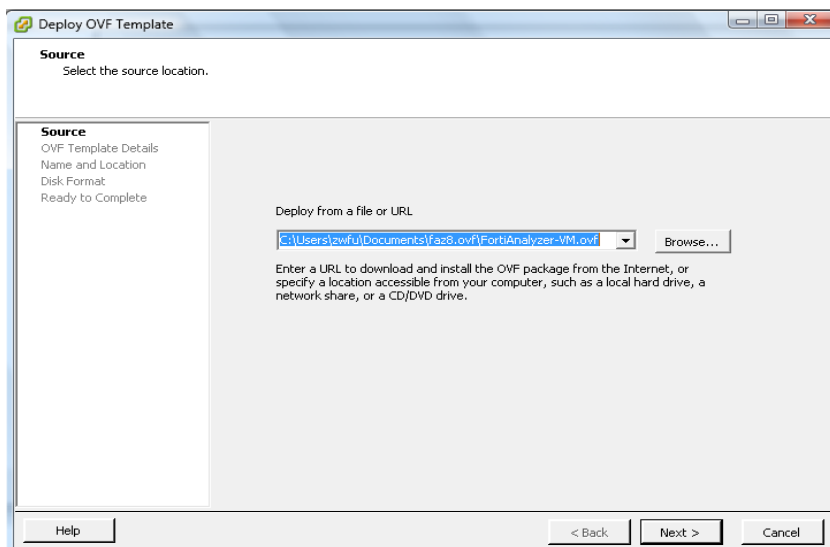
Figure 3: Logging into VMware vSphere Client



- 3 Go to *File > Deploy OVF Template*.

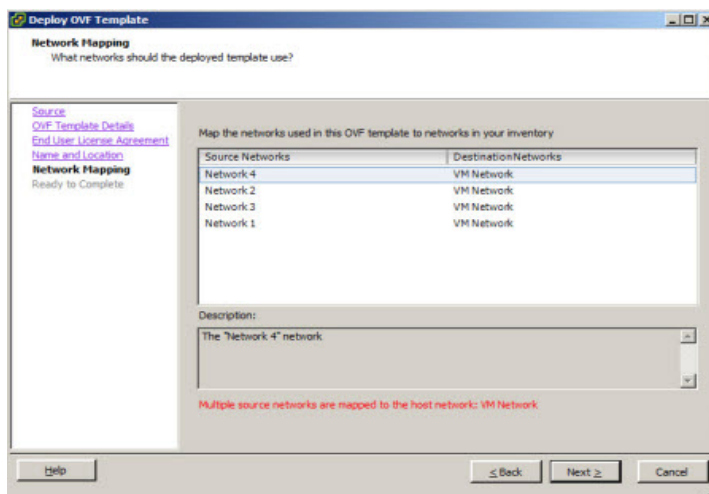
- 4 In the Browse to OVF Template window, locate the *FortiAnalyzer-VM.ovf* file, and click *Next*.

Figure 4: Deploying *.OVF file



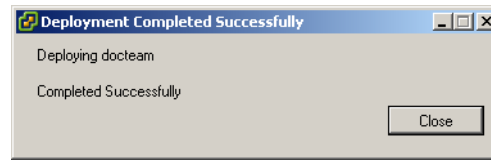
- 5 Import the FortiAnalyzer-VM software using the installation wizard.
- 6 Review the OVF template details and click *Next*.
- 7 Read the *End User License Agreement* and click *Accept* at the bottom. Then click *Next*.
- 8 Enter the name of the FortiAnalyzer-VM virtual device and click *Next*.
- 9 Map the networks used in the FortiAnalyzer-VM to the networks in your inventory. For each Source Network, select a Destination Network from the drop-down list.

Figure 5: Mapping networks



- 10 Click *Finish* after verifying the settings.
- 11 After the deployment is complete, click *Close*.

Figure 6: Completing the deployment



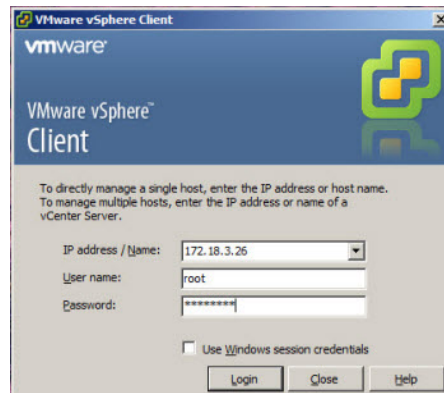
Logging in

After installing the FortiAnalyzer-VM, log in to the VMware Hypervisor (ESX/ESXi) and configure the FortiAnalyzer-VM settings.

To log in to the ESX/ESXi host

- 1 Open the VMware vSphere Client and enter the IP address, user name, and password.
- 2 Click *Login*.

Figure 7: Entering login information



- 3 Highlight the FortiAnalyzer-VM in the left pane.
- 4 Click *Edit Settings* to edit information on CPUs, RAM, Interfaces, video cards, and other virtual hardware.



Note: Do NOT power on the FortiAnalyzer-VM if you want to change its configuration. Before powering on the FortiAnalyzer-VM virtual appliance:

- Resize disk (VMDK) if necessary (see [“Resize disk \(VMDK\)”](#) on page 12)
- Configure the number of CPUs (see [“Configuring the number of virtual CPUs”](#) on page 13)
- Set RAM on virtual appliance ([“Setting the virtual RAM”](#) on page 13)
- Configure the virtual network adaptor(s) ([“Configuring virtual network adaptor\(s\)”](#) on page 14)

Resize disk (VMDK)

FortiAnalyzer-VM deploys with pre-sized VMDKs. If you configure the FortiAnalyzer-VM to log in to an internal database, you need to resize the disk (VMDK) before powering on.

To resize the disk (VMDK)

- 1 Log in to the ESX/ESXi host.

- 2 Open the VMware vSphere Client and enter the IP address, username and password.
- 3 Click *Login*.
- 4 Highlight the FortiAnalyzer-VM in the left pane and click *Edit Settings*
- 5 Click on *Hard disk 2* and edit the *Provisioned Size* as necessary up to your licensed limit
- 6 Click *Ok*.

Configuring the number of virtual CPUs

After import, the FortiAnalyzer-VM, by default, will be configured with 2 vCPUs. You may change the number of vCPUs from 1 to 8 depending on your VMware license level.

For more information, see the VMware vSphere documentation at <http://www.vmware.com/products/vsphere-hypervisor/index.html>

To change the number of CPUs

- 1 Log in to the ESX/ESXi host.
- 2 Open the VMware vSphere Client and enter the IP address, user name and password.
- 3 Click *Login*.
- 4 Highlight the FortiAnalyzer-VM in the left pane and click *Edit Settings*.
- 5 Click *CPUs* and edit the number of virtual processors.
- 6 Click *Ok*.

Setting the virtual RAM

The FortiAnalyzer-VM comes pre-configured with 512 MB of RAM. You may change this value to be anywhere from 512 MB to the current limit of 4 GB.

To change the amount of vRAM

- 1 Log in to the ESX/ESXi host.
- 2 Open the VMware vSphere Client and enter the IP address, user name and password.
- 3 Click *Login*.
- 4 Highlight the FortiAnalyzer-VM in the left pane and click *Edit Settings*.
- 5 Click *Memory* and edit the *Memory Size*.
- 6 Click *Ok*.

Configuring virtual networks

Mapping FortiAnalyzer-VM ports to physical ports depends on your existing virtual environment. When you deploy the FortiAnalyzer-VM OVF file, one Virtual Network Interface Card (vNIC) is automatically mapped to a port group on a virtual switch within the ESX/ESXi server. You can change the mapping, or map other vNICs if required. [Table 3](#) provides an example of how vNICs may be mapped to the ports on the VMware ESX/ESXi server.

Table 3: Network mapping example

ESX Server-OS Physical Adapter	Network Mapping: ESX/ESXi Server - vNetwork VM Port Group	FortiAnalyzer-VM Settings Network Adapter	FortiAnalyzer-VM OS Port
eth0	VM Network 1	Network Adapter 1	Port 1
eth1	VM Network 2	Network Adapter 2	Port 2

Configuring virtual network adaptor(s)

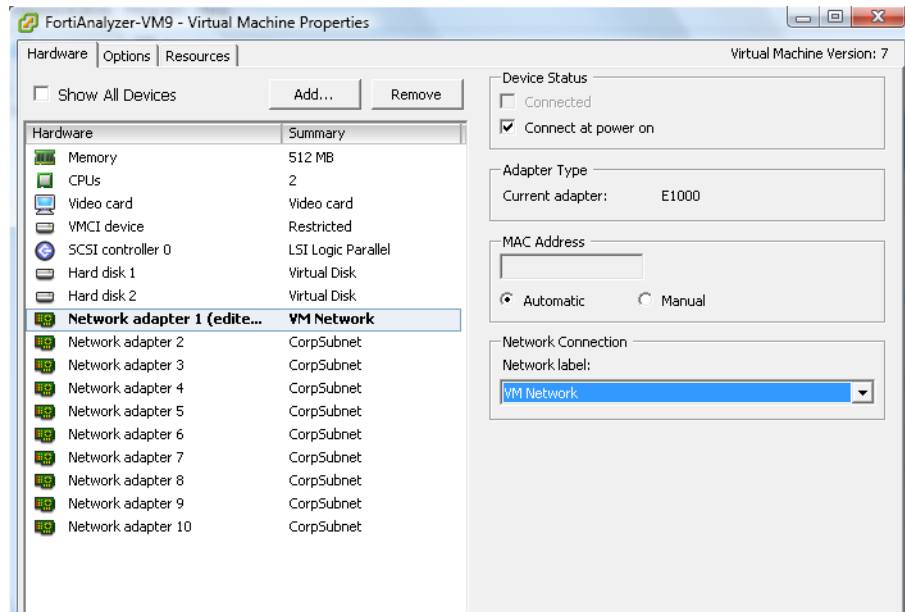
Virtual machine ports can be mapped to port groups on virtual switches and subsequently mapped to ports on the ESX/ESXi server. To map virtual ports or change the existing virtual port configurations, edit the FortiAnalyzer-VM settings.

To map the network adaptors

- 1 Log in to the ESX/ESXi host.
- 2 Open the VMware vSphere Client and enter the IP address, user name and password.
- 3 Click *Login*.
- 4 Highlight the FortiAnalyzer-VM in the left pane and click *Edit Settings*.
Network adapters are mapped to a virtual port on virtual networks (VM Network).
- 5 Highlight a specific Network adapter to see its current settings.
- 6 Select the network adapter and map it to an appropriate VM Network.

This depends on your configuration. For example, in the illustration below, Network adapter 1 is mapped to "VM Network".

Figure 8: Mapping network adapters



- 7 Click *OK* when done.

Powering on FortiAnalyzer-VM

Once FortiAnalyzer-VM has been deployed, you can power on the virtual machine and log in using the Console.

In the Console, you are extremely limited to the type of commands you can enter until a valid license is entered through the Web Config. You can configure the internal interface, system DNS, and the static router.

To power on FortiAnalyzer-VM

- 1 Open the VMware vSphere Client and enter the IP address, user name, and password. Click *Login*.
- 2 Select the FortiAnalyzer-VM from the tree.
- 3 In the *Getting Started* tab, click *Power on the virtual machine*.
- 4 Select the Console tab. It may take a few minutes for the FortiAnalyzer-VM software to format.
- 5 At the FortiAnalyzer-VM login prompt, type `admin`. There is no password.

- 6 Configure the FortiAnalyzer internal interface. Type:

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

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

```
config system dns
  set primary <dns-server_ip>
  set secondary <dns-server_ip>
end
```

- 8 Configure the default gateway. Type:

```
config system route
  edit 1
    set device port1
    set gateway <gateway_ip>
  end
```

- 9 If you want to override the default FDS server with another one, type:

```
config system fortiguard
  set fds-override-enabled enable
  set fds-override-addr <new_fds_server_ip>
end
```



Note: To access Web Config in the web browser, only https is allowed; http is not allowed.

Uploading the License

Once the system interface has been configured in the Console, you can enter the license through a web browser in the Web Config. A license cannot be entered in the CLI.

You cannot perform any actions in the Web Config until a license has been uploaded, although some initial settings, such as interface IP, DNS, gateway and FDS server address overriding can be set through the CLI. After a valid license has been uploaded and verified, the Web Config and the CLI are unlocked and fully functional. For more information about licenses and FortiGuard, see “[Licensing](#)” on page 6.

To upload the license

- 1 Open a web browser and type the IP address you configured in the console. For example, `https://192.168.1.99`.
- 2 Type `admin` in the *Name* field and click *Login*.
The *Install FortiAnalyzer-VM License File* tab opens.

Figure 9: Installing FortiAnalyzer-VM License File



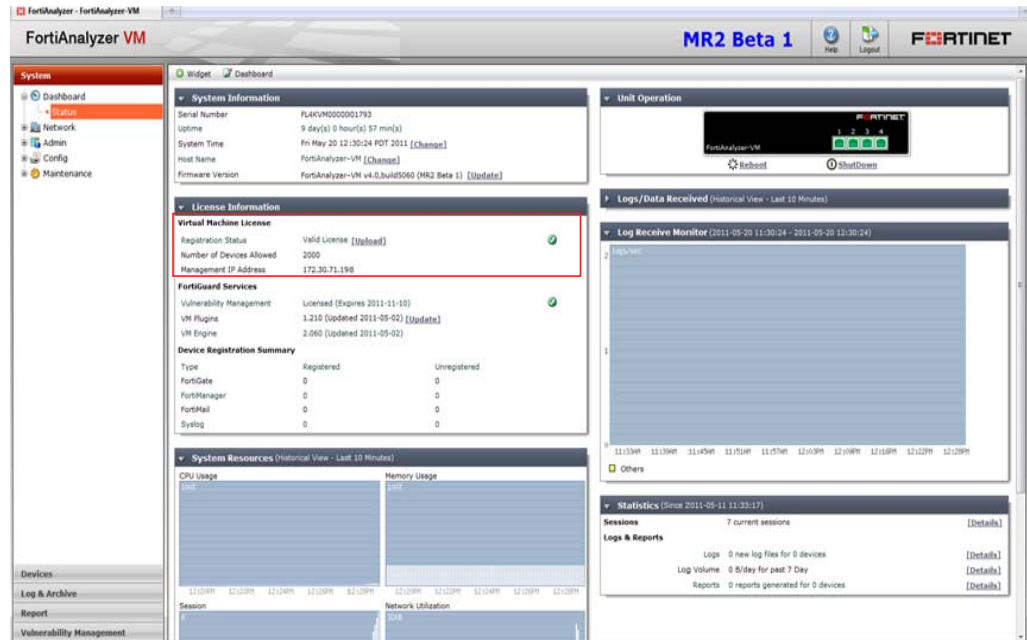
- 3 Browse for the license file and click *OK*.
The system will restart. This will take a few minutes.
- 4 You will get the message, “FortiAnalyzer Virtual Machine license has already been uploaded, please wait while system starts.” Click *OK*.

Figure 10: License uploaded message.



- 5 Refresh the web browser to login.
- 6 Type `admin` in the Name field and click Login. The FortiAnalyzer-VM Web Config opens.
The VM License Registration Status and number of CPUs detected are shown in the FortiAnalyzer-VM dashboard.

Figure 11: FortiAnalyzer-VM in Web Config



What next?

At this point, FortiAnalyzer-VM is running but is almost entirely unconfigured. Before you can use it to collect log messages and generate reports, you must configure its system settings and add other devices to the FortiAnalyzer unit.

For more information on how to set up and use the FortiAnalyzer-VM features, see the [FortiAnalyzer Administration Guide](#) or visit <http://docs.fortinet.com/fa.html> for all FortiAnalyzer documentation.

FORTINET®