FortiAuthenticator - VM Install Guide

Version 6.2.0

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

November 2, 2022
FortiAuthenticator 6.2.0 VM Install Guide
23-620-657434-20221102

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-09-16	Initial release.
2020-12-01	Added VM requirements and sizing guidelines to System requirements on page 9.
2021-01-27	Updated Download the FortiAuthenticator-VM software on page 15.
2021-02-17	Updated Licensing on page 7.
2021-04-12	Added Deploying FortiAuthenticator-VM on Nutanix on page 33.
2021-06-02	Updated Unlicensed FortiAuthenticator-VM on page 18.
2022-11-02	Updated Licensing on page 7 and System requirements on page 9.

Introduction

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

FortiAuthenticator-VM is a virtual appliance designed specifically to provide authentication services for multiple devices, including firewalls, SSL and IPsec VPNs, wireless access points, switches, routers, and servers. FortiAuthenticator includes a RADIUS and LDAP server. Authentication servers are an important part of an enterprise network, controlling access to protected network assets, and tracking users' activities to comply with security policies.

FortiAuthenticator is not a firewall; it requires a FortiGate appliance to provide firewall-related services. Multiple FortiGate units can use a single FortiAuthenticator appliance for Fortinet Single Sign On (FSSO) and other types of remote authentication, two-factor authentication, and FortiToken device management. This centralizes authentication and FortiToken maintenance.

FortiAuthenticator provides an easy-to-configure remote authentication option for FortiGate users. Additionally, it can replace the FSSO Agent on a Windows AD network.

Whilst FortiAuthenticator is a hardened server it should be installed with adequate protection from the Internet. Management protocols should be configured on private networks and only the resources required exposed to the outside.

The FortiAuthenticator-VM delivers centralized, secure two-factor authentication for a virtual environment with a stackable user license for the greatest flexibility. Supporting from 100 to 1 million+ users, the FortiAuthenticator-VM supports the widest range of deployments, from small enterprise right through to the largest service provider.

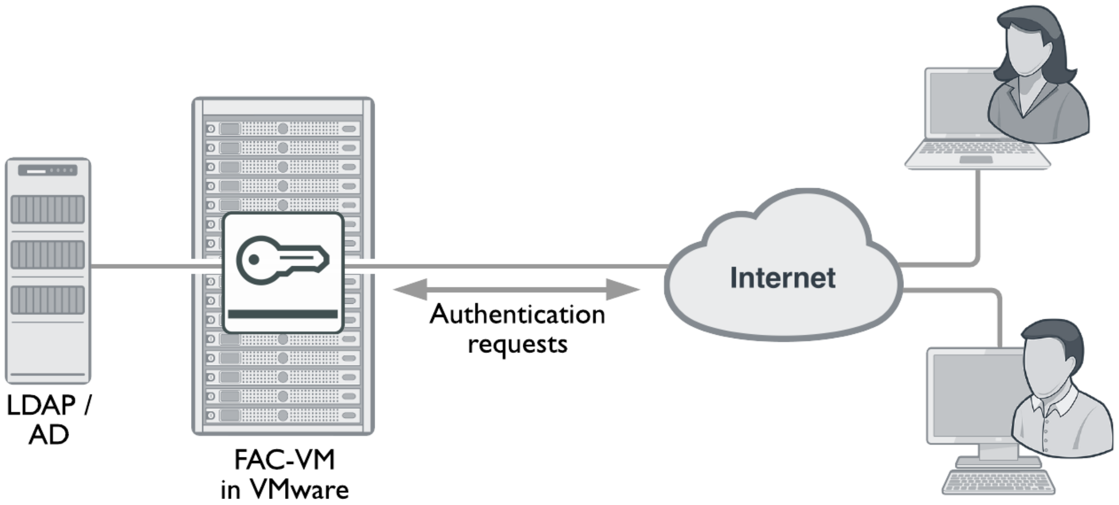
⚠ Failure to protect the FortiAuthenticator may result in compromised authentication databases.

This document includes an overview of the FortiAuthenticator-VM, its deployment with VMware vSphere, MS Hyper-V, KVM, and Nutanix, and information on how to perform an initial configuration.

Architecture

FortiAuthenticator-VM is a virtual appliance version of FortiAuthenticator. It is deployed in a virtual machine environment such as VMware ESX (or ESXi), MS Hyper-V, or the Linux based Virtual Machine Manager.

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



FortiAuthenticator-VM requires the following connectivity for management. Inbound management using Telnet and HTTP is not recommended. SSH is intended for initial configuration and diagnostics only. For more information, see the FortiAuthenticator Administration Guide.

Inbound management:

Service	Port
Telnet	TCP 23
HTTP	TCP 80
HTTPS	TCP 443
SSH	TCP 22

Outbound management:

Service	Port
DNSlookup	UDP 53
NTP	UDP 123
FortiGuard Licensing	TCP 443 (required for initial token registration)
Log Export (FTP)	TCP 21

FortiAuthenticator-VM Overview

This section provides an overview of FortiAuthenticator-VM.

The following topics are included in this section:

- Licensing on page 7
- System requirements on page 9
- Register FortiAuthenticator-VM on FortiCloud on page 10
- Download the FortiAuthenticator-VM software on page 15
- Unlicensed FortiAuthenticator-VM on page 18

Licensing

Fortinet offers the FortiAuthenticator-VM in a stackable license model. This model allows you to expand your VM solution as your environment expands. When configuring your FortiAuthenticator-VM, make sure to configure hardware settings as outlined in table three and consider future expansion. Contact your Fortinet Authorized Reseller for more information.

FortiAuthenticator-VM license options:

SKU	Description
FAC-VM-Base	Base FortiAuthenticator-VM with 100 user licenses. Unlimited vCPU.
FAC-VM-100-UG	FortiAuthenticator-VM with 100 user license upgrade.
FAC-VM-1000-UG	FortiAuthenticator-VM with 1,000 user license upgrade.
FAC-VM-10000-UG	FortiAuthenticator-VM with 10,000 user license upgrade.
FAC-VM-100000-UG	FortiAuthenticator-VM with 100,000 user license upgrade.

Note that the FAC-VM-Base license is always required and that other licenses are upgrades to the base license.

Virtualization environments supported:

- VMware ESXi 4/5/6
- Microsoft Hyper-V Server 2010 and 2016
- KVM
- Nutanix
- Xen Virtual Machine
- Amazon Web Service
- Microsoft Azure
- Oracle Cloud Infrastructure

FortiAuthenticator-VM support options:

SKU	Description
FC1-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1 - 500 USERS)
FC2-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1 - 1100 USERS)
FC3-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1 - 5100 USERS)
FC4-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1 - 10100 USERS)
FC8-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1 - 25100 USERS)
FC5-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1 - 50100 USERS)
FC6-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1 - 100100 USERS)
FC9-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1 - 500100USERS)
FC7-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1 - 1M USERS)

FortiAuthenticator-VM license information:

Technical Specification	VM-BASE	VM-100-UG	VM-1000-UG	VM-10000-UG	VM-100000-UG
Virtual CPUs (Maximum)	64				
Virtual Interfaces (Min / Max)	1 / 4				
Virtual Memory (Min / Max)	2GB / 1TB				
Virtual Storage (Min / Max)	60GB / 16TB				
High Availability	Yes (Active-Passive HA and Config Sync HA)				
FortiTokens	200	+200	+2,000	+20,000	+200,000
NAS Devices	33	+33	+333	+3,333	+33,333
User Group	10	+10	+100	+1,000	+10,000
Local Users / Remote Users	100	+100	+1,000	+10,000	+100,000
User Certificates	100	+500	+5,000	+50,000	+500,000
CA Certificates	5	+5	+50	+500	+500

After placing an order for FortiAuthenticator-VM, a license registration code is sent to the email address used in the order form. Use the license registration code provided to register the FortiAuthenticator-VM with FortiCloud.

Upon registration, you can download the license file. You will need this file to activate your FortiAuthenticator-VM. For more information on configuring basic network settings and applying your license, see the FortiAuthenticator Administration Guide.

System requirements

Prior to deploying the FortiAuthenticator-VM virtual appliance, either VMware vSphere Hypervisor (ESX versions 4.0 or 4.1, ESXi versions 4/5/6), Microsoft Hyper-V Server (2010 and 2016), or Virtual Machine Manager for KVM must be installed and configured. Note that, Virtual Machine Manager version 1.3.2 was used for the purposes of this document.

The installation instructions for FortiAuthenticator-VM assume you are familiar with both VM platforms and their related terminology.

For more details on all platforms, refer to:

- http://www.vmware.com/products/vsphere-hypervisor/overview.html
- https://www.microsoft.com/en-ca/server-cloud/solutions/virtualization.aspx
- https://virt-manager.org/

⚠ Upgrade to the latest stable server update and patch release.

The following table provides a detailed summary on FortiAuthenticator virtual machine (VM) system requirements. Installing FortiAuthenticator-VM requires that you have already installed a supported VM environment.

VM requirements

Virtual machine	Requirement
VM form factor	Open Virtualization Format (OVF)
Virtual CPUs supported (minimum / maximum)	1 / 64
Virtual NICs supported (minimum / maximum)	1 / 4
Storage support (minimum / maximum)	60 GB / 16 TB
Memory support (minimum / maximum)	2 GB / 1 TB
High Availability (HA) support	Yes

FortiAuthenticator-VM sizing guidelines

The following table provides FortiAuthenticator-VM sizing guidelines based on typical usage. Actual requirements may vary based on usage patterns.

Users	Virtual CPUs	Memory	Storage*
1 - 500	1	2 GB	1 TB
500 to 2,500	2	4 GB	1 TB
2,500 to 7,500	2	8 GB	2 TB
7,500 to 25,000	4	16 GB	2 TB
25,000 to 75,000	8	32 GB	4 TB
75,000 to 250,000	16	64 GB	4 TB
250,000 to 750,000	32	128 GB	8 TB
750,000 to 2,500,000	64	256 GB	16 TB
2,500,000 to 7,500,000	64	512 GB	16 TB

*1TB is sufficient for any number of users if there is no need for long-term storage of logs onboard FortiAuthenticator.

FortiAuthenticator-VM firmware

Fortinet provides FortiAuthenticator-VM firmware images in two formats:

- **.out**
  Use this image for new and upgrades to physical appliance installations. Upgrades to existing virtual machine installations are also distributed in this format.
- **ovf.zip / kvm.zip / hyperv.zip / xen.zip**
  Used for new VM installations.

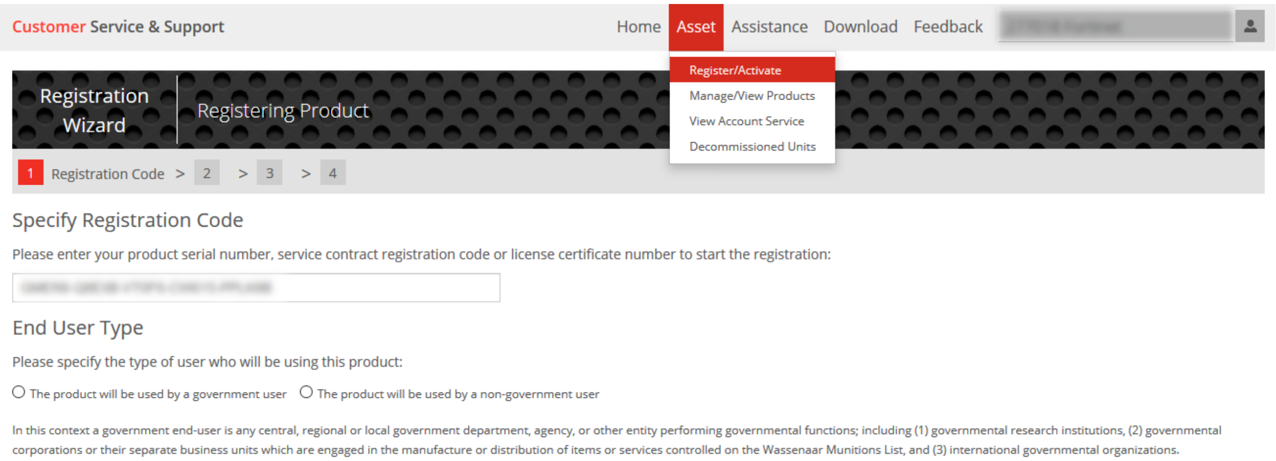
For more information see the FortiAuthenticator product datasheet available on the Fortinet web site.

Register FortiAuthenticator-VM on FortiCloud

To obtain the FortiAuthenticator-VM license file you must first register your FortiAuthenticator-VM on FortiCloud.

To register your FortiAuthenticator-VM:

1. Log in to FortiCloud using an existing support account or select *Create an Account*.
2. In the toolbar select *Asset* > *Register/Activate*.
   The *Registration Wizard* opens.
3. Enter the license registration code from the FortiAuthenticator-VM License Certificate that was emailed to you, and select *Next*.
   The *Registration Info* page is displayed.



Specify Registration Code

Please enter your product serial number, service contract registration code or license certificate number to start the registration:

[redacted]

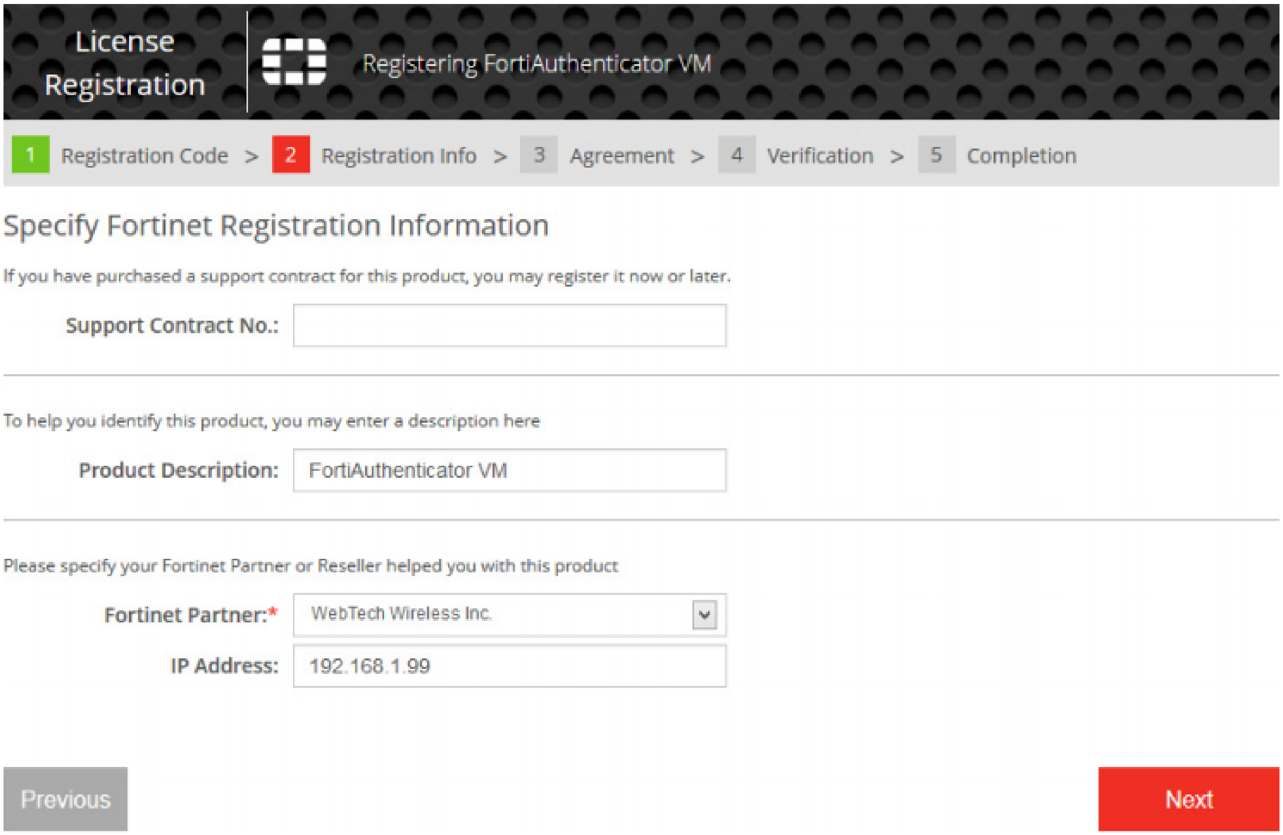
End User Type

Please specify the type of user who will be using this product:

○ The product will be used by a government user ○ The product will be used by a non-government user

In this context a government end-user is any central, regional or local government department, agency, or other entity performing governmental functions; including (1) governmental research institutions, (2) governmental corporations or their separate business units which are engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List, and (3) international governmental organizations.

4. Enter the support contract number, product description, Fortinet Partner, and IP address.


License Registration
Registering FortiAuthenticator VM
1 Registration Code > 2 Registration Info > 3 Agreement > 4 Verification > 5 Completion
Previous
Next

Specify Fortinet Registration Information

If you have purchased a support contract for this product, you may register it now or later.

Support Contract No.:

To help you identify this product, you may enter a description here

Product Description: FortiAuthenticator VM

Please specify your Fortinet Partner or Reseller helped you with this product

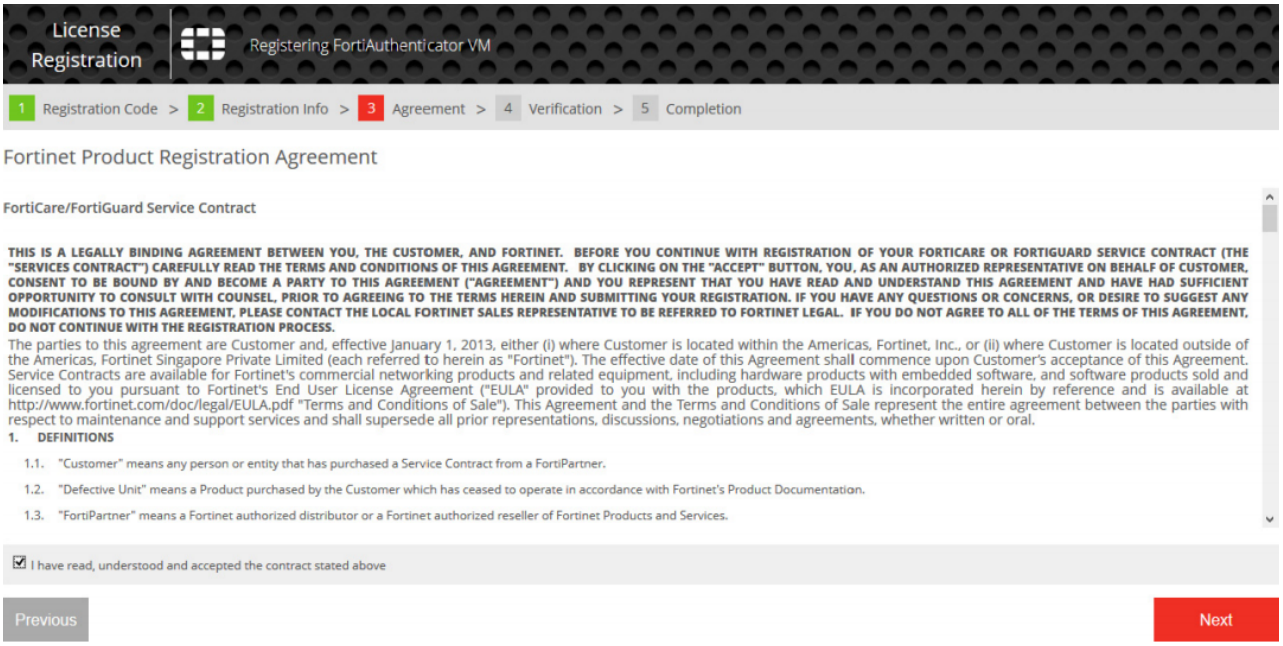
Fortinet Partner:* WebTech Wireless Inc.

IP Address: 192.168.1.99

As a part of the license validation process, FortiAuthenticator-VM compares its IP address with the IP information in the license file. If a new license has been imported or the FortiAuthenticator-VM's IP address has been changed, the FortiAuthenticator-VM must be rebooted in order for the system to validate the change and operate with a valid license.

FortiCloud does not currently support IPv6 for FortiAuthenticator-VM license validation. You must specify an IPv4 address in both the support portal and the port management interface.

5. Select *Next* to continue.
   The *Fortinet Product Registration Agreement* page is displayed.



License Registration
Registering FortiAuthenticator VM
1 Registration Code > 2 Registration Info > 3 Agreement > 4 Verification > 5 Completion

Fortinet Product Registration Agreement

FortiCare/FortiGuard Service Contract

THIS IS A LEGALLY BINDING AGREEMENT BETWEEN YOU, THE CUSTOMER, AND FORTINET. BEFORE YOU CONTINUE WITH REGISTRATION OF YOUR FORTICARE OR FORTIGUARD SERVICE CONTRACT (THE "SERVICES CONTRACT") CAREFULLY READ THE TERMS AND CONDITIONS OF THIS AGREEMENT. BY CLICKING ON THE "ACCEPT" BUTTON, YOU, AS AN AUTHORIZED REPRESENTATIVE ON BEHALF OF CUSTOMER, CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT ("AGREEMENT") AND YOU REPRESENT THAT YOU HAVE READ AND UNDERSTAND THIS AGREEMENT AND HAVE HAD SUFFICIENT OPPORTUNITY TO CONSULT WITH COUNSEL, PRIOR TO AGREEING TO THE TERMS HEREIN AND SUBMITTING YOUR REGISTRATION. IF YOU HAVE ANY QUESTIONS OR CONCERNS, OR DESIRE TO SUGGEST ANY MODIFICATIONS TO THIS AGREEMENT, PLEASE CONTACT THE LOCAL FORTINET SALES REPRESENTATIVE TO BE REFERRED TO FORTINET LEGAL. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT CONTINUE WITH THE REGISTRATION PROCESS.

The parties to this agreement are Customer and, effective January 1, 2013, either (i) where Customer is located within the Americas, Fortinet, Inc., or (ii) where Customer is located outside of the Americas, Fortinet Singapore Private Limited (each referred to herein as "Fortinet"). The effective date of this Agreement shall commence upon Customer's acceptance of this Agreement. Service Contracts are available for Fortinet's commercial networking products and related equipment, including hardware products with embedded software, and software products sold and licensed to you pursuant to Fortinet's End User License Agreement ("EULA" provided to you with the products, which EULA is incorporated herein by reference and is available at http://www.fortinet.com/doc/legal/EULA.pdf "Terms and Conditions of Sale"). This Agreement and the Terms and Conditions of Sale represent the entire agreement between the parties with respect to maintenance and support services and shall supersede all prior representations, discussions, negotiations and agreements, whether written or oral.

1. DEFINITIONS

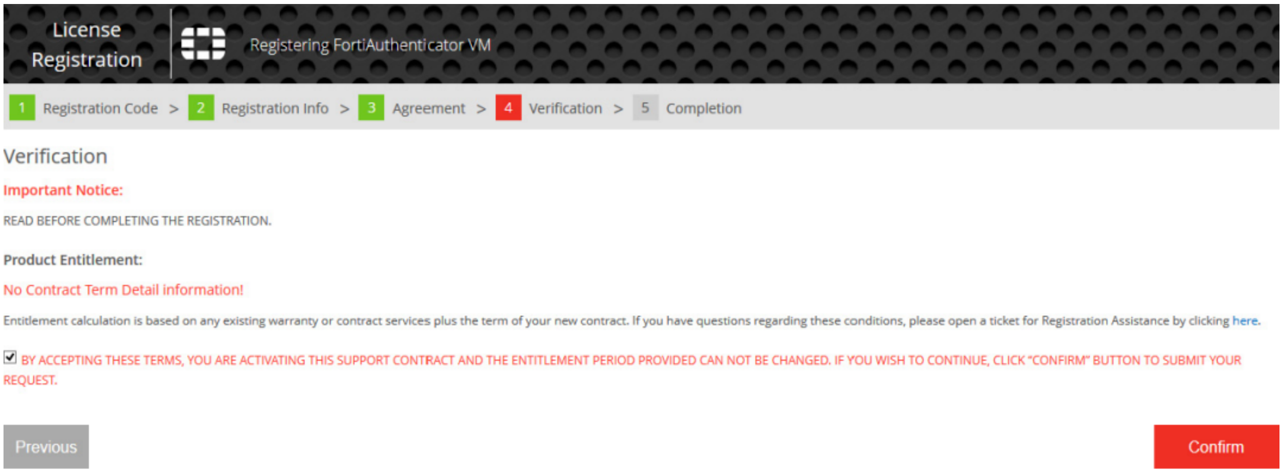
1.1. "Customer" means any person or entity that has purchased a Service Contract from a FortiPartner.

1.2. "Defective Unit" means a Product purchased by the Customer which has ceased to operate in accordance with Fortinet's Product Documentation.

1.3. "FortiPartner" means a Fortinet authorized distributor or a Fortinet authorized reseller of Fortinet Products and Services.

☑ I have read, understood and accepted the contract stated above

6. Select the check box to indicate that you have read, understood, and accepted the service contract, and select *Next* to continue.
   The *Verification* page is displayed.



License Registration
Registering FortiAuthenticator VM
1 Registration Code > 2 Registration Info > 3 Agreement > 4 Verification > 5 Completion

Verification

Important Notice:

READ BEFORE COMPLETING THE REGISTRATION.

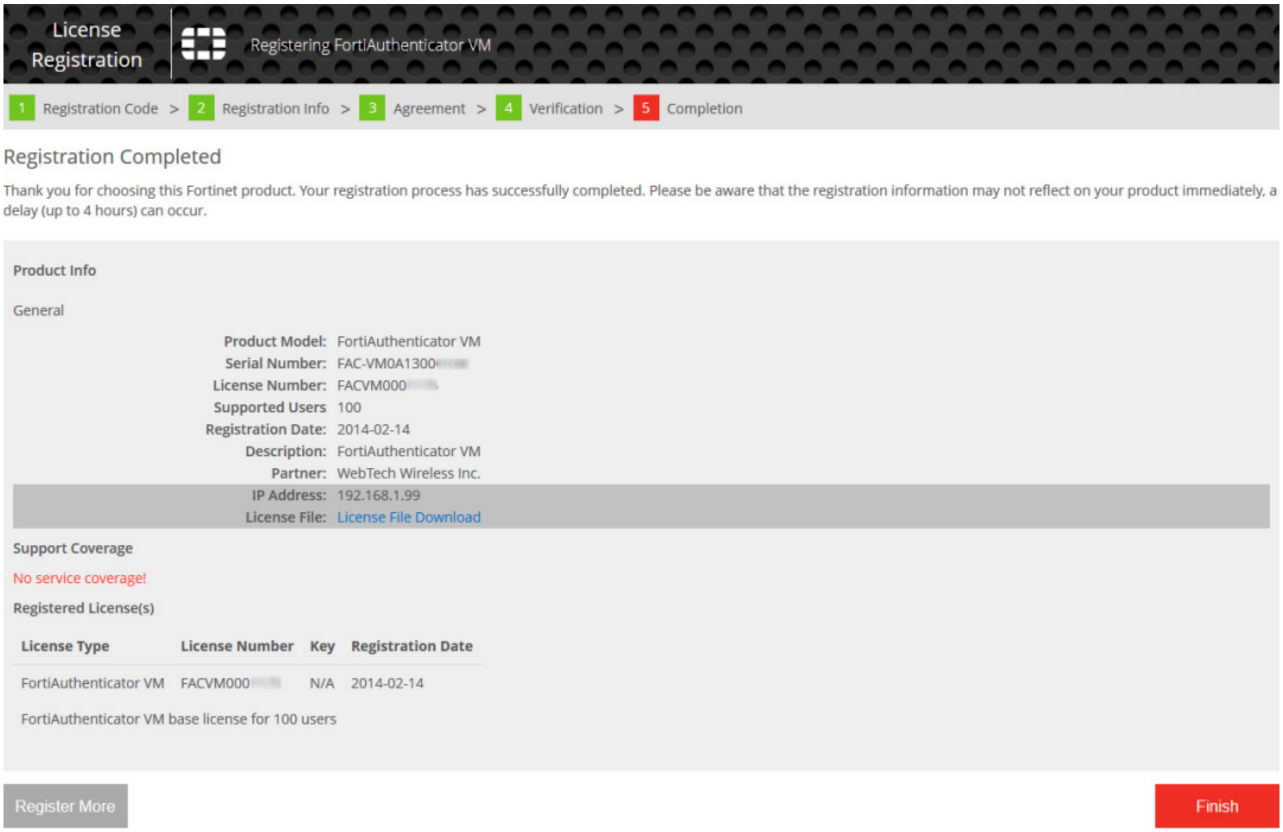
Product Entitlement:

No Contract Term Detail information!

Entitlement calculation is based on any existing warranty or contract services plus the term of your new contract. If you have questions regarding these conditions, please open a ticket for Registration Assistance by clicking here.

☑ BY ACCEPTING THESE TERMS, YOU ARE ACTIVATING THIS SUPPORT CONTRACT AND THE ENTITLEMENT PERIOD PROVIDED CAN NOT BE CHANGED. IF YOU WISH TO CONTINUE, CLICK "CONFIRM" BUTTON TO SUBMIT YOUR REQUEST.

7. The verification page displays the product entitlement. Select the checkbox to indicate that you accept the terms and select *Confirm* to submit the request.
   The *Registration Completed* page is displayed.


License Registration
Registering FortiAuthenticator VM
1 Registration Code > 2 Registration Info > 3 Agreement > 4 Verification > 5 Completion

Registration Completed

Thank you for choosing this Fortinet product. Your registration process has successfully completed. Please be aware that the registration information may not reflect on your product immediately, a delay (up to 4 hours) can occur.

Product Info

General

Product Model:	FortiAuthenticator VM
Serial Number:	FAC-VM0A1300[redacted]
License Number:	FACVM000[redacted]
Supported Users	100
Registration Date:	2014-02-14
Description:	FortiAuthenticator VM
Partner:	WebTech Wireless Inc.
IP Address:	192.168.1.99
License File:	License File Download

Support Coverage

No service coverage!

Registered License(s)

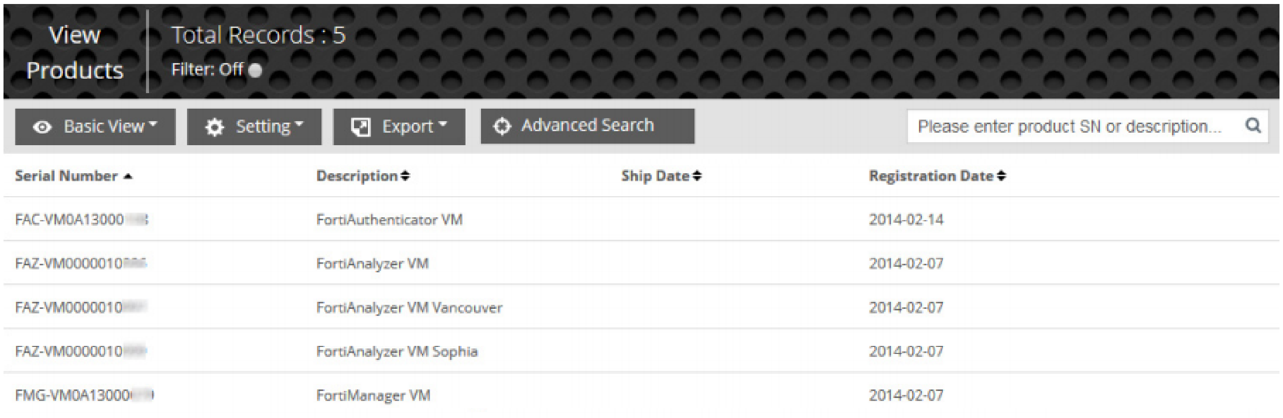
License Type	License Number	Key	Registration Date
FortiAuthenticator VM	FACVM000[redacted]	N/A	2014-02-14

FortiAuthenticator VM base license for 100 users

8. In the *Registration Completed* page you can download the FortiAuthenticator-VM license file. Select the *License File Download* link. You will be prompted to save the license file (`.lic`) to your management computer.

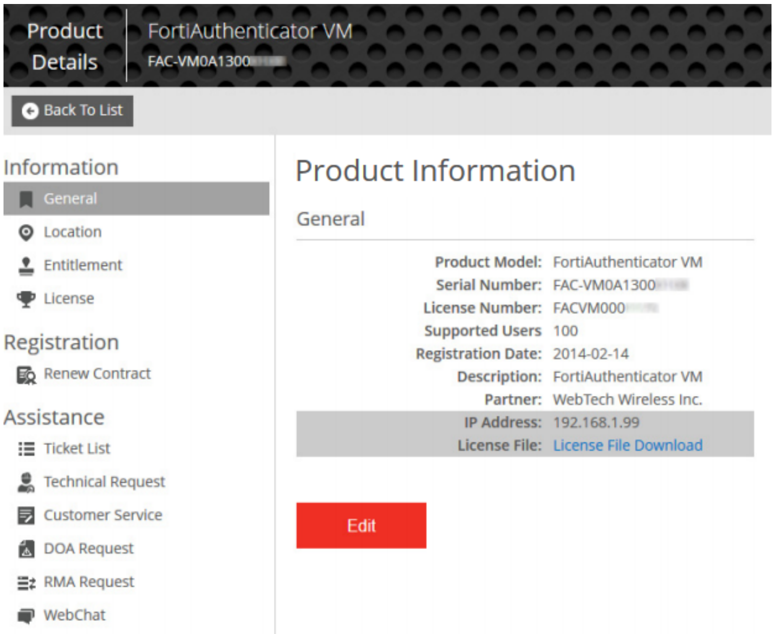
To edit the FortiAuthenticator-VM IP address:

1. In the toolbar select *Asset* > *Manage/View Products*.
The *View Products* page opens.



Serial Number ▲	Description ⇕	Ship Date ⇕	Registration Date ⇕
FAC-VM0A13000[redacted]	FortiAuthenticator VM		2014-02-14
FAZ-VM0000010[redacted]	FortiAnalyzer VM		2014-02-07
FAZ-VM0000010[redacted]	FortiAnalyzer VM Vancouver		2014-02-07
FAZ-VM0000010[redacted]	FortiAnalyzer VM Sophia		2014-02-07
FMG-VM0A13000[redacted]	FortiManager VM		2014-02-07

2. Select the FortiAuthenticator-VM serial number.
The *Product Information* page opens.



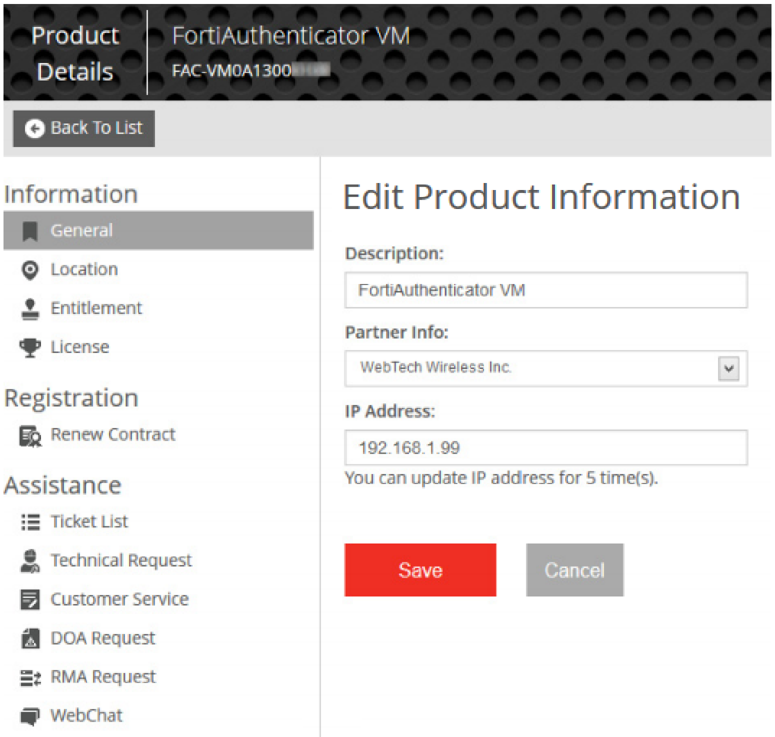
FortiAuthenticator VM
FAC-VM0A1300[redacted]

Product Information

General

Product Model:	FortiAuthenticator VM
Serial Number:	FAC-VM0A1300[redacted]
License Number:	FACVM000[redacted]
Supported Users	100
Registration Date:	2014-02-14
Description:	FortiAuthenticator VM
Partner:	WebTech Wireless Inc.
IP Address:	192.168.1.99
License File:	License File Download

3. Select *Edit* to change the description, partner information, and IP address of your FortiAuthenticator-VM. The *Edit Product Information* page opens.



FortiAuthenticator VM
FAC-VM0A1300[redacted]

Edit Product Information

Description:
FortiAuthenticator VM

Partner Info:
WebTech Wireless Inc.

IP Address:
192.168.1.99

You can update IP address for 5 time(s).

4. Enter the new IP address and select *Save*.

You can change the IP address five (5) times on a regular FortiAuthenticator-VM license. There is no restriction on a full evaluation license.

5. Select the *License File Download* link. You will be prompted to save the license file (`.lic`) to your management computer.

Download the FortiAuthenticator-VM software

Fortinet provides the FortiAuthenticator-VM software for 64-bit environments in two formats:

Upgrades: Download this firmware image to upgrade your existing FortiAuthenticator-VM installation.

- FAC_VM-vxxx-build0xxx-FORTINET.out:

New Installations: Download for a new FortiAuthenticator-VM installation. Choose the package relevant to your environment.

- FAC_VM-vxxx-build0xxx-FORTINET.out.ovf.zip
- FAC_VM-vxxx-build0xxx-FORTINET.out.kvm.zip
- FAC_VM-vxxx-build0xxx-FORTINET.out.hyperv.zip
- FAC_VM-vxxx-build0xxx-FORTINET.out.xen.zip

The zip file is available in hyperv and OVF formats, for MS Hyper-V and VMware ESXi respectively. The .out file can upgrade both.

For more information see the FortiAuthenticator product datasheet available on the Fortinet web site.

MS Hyper-V deployment package contents

The **FAC_VM_HV-vxxx-buildxxxx-FORTINET.out.hyperv.zip** file contains:

- **Snapshots folder**:
  - Optionally, Hyper-V stores snapshots of the FortiAuthenticator-VM state here.
- **Virtual Hard Disks folder**:
  - DATADRIVE.vhd: The FortiAuthenticator-VM log disk in VHD format.
  - fac.vhd: The FortiAuthenticator-VM system hard disk in VHD format.
- **Virtual Machines folder**:
  - fortiauthenticator.xml: XML file containing virtual hardware configuration settings for Hyper-V.

VMware ESXi deployment package contents

The **FAC_VM-vxxx-buildxxxx-FORTINET.out.ovp.zip** file contains:

- datadrive.vmdk: The FortiAuthenticator-VM log disk in VMDK format.
- fac.vmdk: The FortiAuthenticator-VM system hard disk in VMDK format.
- FortiAuthenticator-VM.ovf: OVF template file for the highest supported VMware hardware type (intel E1000 NIC Driver). To find out the hardware type of your OVF template, open the file with a text editor, and search `vssd:VirtualSystemType`.
- FortiAuthenticator-VM.hwXX.ovf: OVF template file for VMware Hardware Type XX (intel E1000 NIC Driver).

For compatibility of your VMware ESXi/ESX server and the various hardware types, see ESXi/ESX hosts and compatible virtual machine hardware versions list (2007240).

The FAC_VM-vxxx-build0xxx-FORTINET.out.ovf.zip file contains the following files:

- datadrive.vmdk: Virtual machine disk format file used by the OVF file.
- fac.vmdk: Virtual machine disk format file used by the OVF file.
- FortiAuthenticator-VM.hw04.ovf: Open Virtualization Format file for VMware ESX 4.0 environments that support hardware version 4.
- FortiAuthenticator-VM.hw07.ovf: Open Virtualization Format file for VMware ESX 4.0 environments that support hardware version 7.
- FortiAuthenticator-VM.hw10.ovf: Open Virtualization Format file for VMware ESX 4.0 environments that support hardware version 10.
- FortiAuthenticator-VM.hw13.ovf: Open Virtualization Format file for VMware ESX 4.0 environments that support hardware version 13.
- FortiAuthenticator-VM.ovf: Open Virtualization Format file for VMware.

KVM deployment package contents

The **FAC_VM_KVM-vxxx-build0216-FORTINET.out.kvm.zip** file contains the following QCOW2 and XML files:

- datadrive.qcow2
- fackvm.file
- fackvm.xml
- fackvm.qcow2
- README.file

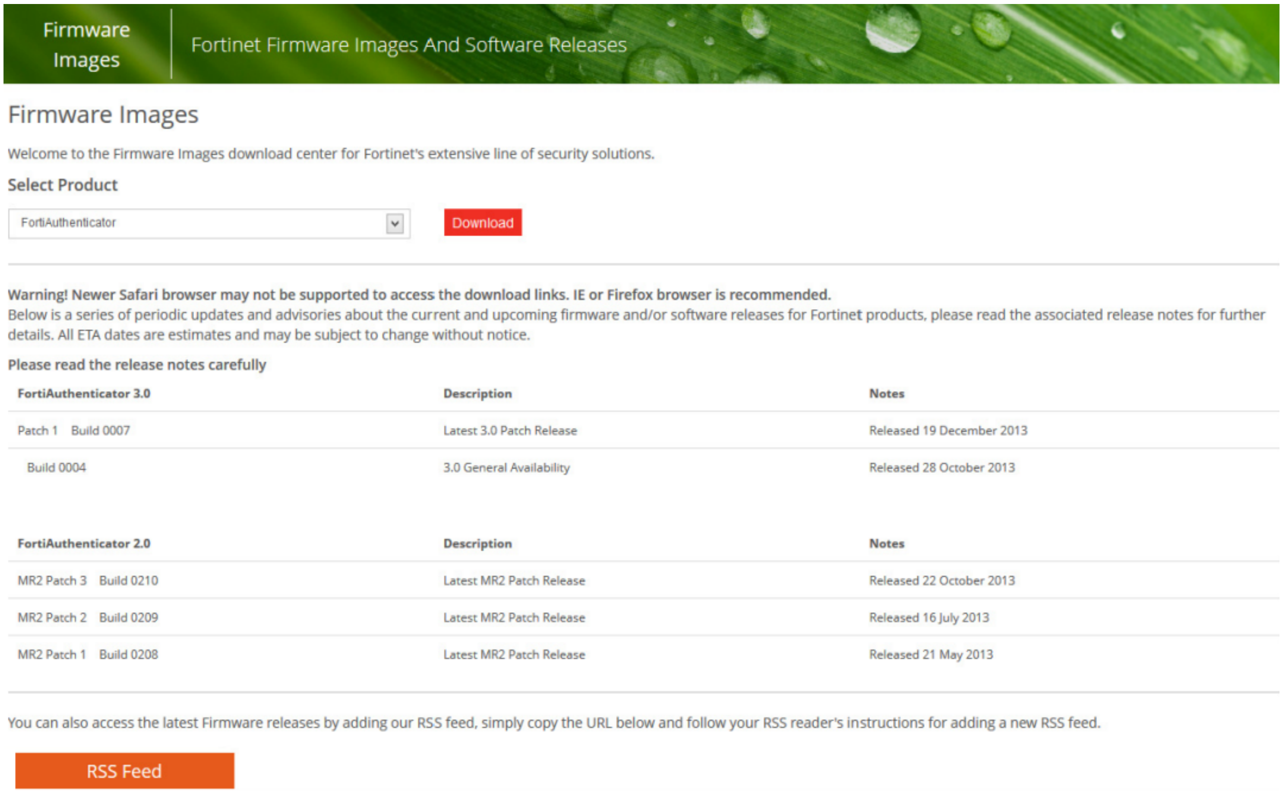
FortiAuthenticator-VM firmware images in the FortiCloud FTP directory are organized by firmware version, major release, and patch release. The firmware images in the directories follow a specific naming convention and each firmware image is specific to the device model. For example, the FAC_VM-v300-build0004-FORTINET.out.ovf.zip image found in the v3.0 directory is specific to the FortiAuthenticator-VM VMware environment.

You can download the FortiAuthenticator Release Notes available on the Fortinet web site.

Note that the download steps below are for VMWare specifically. For other platforms, download the corresponding .ZIP deployment package.

To download the FortiAuthenticator-VM .ovf.zip package:

1. Log into FortiCloud, select *Download* in the toolbar, and select *Firmware Images* from the dropdown list.
   The *Firmware Images* page opens.



Firmware Images

Welcome to the Firmware Images download center for Fortinet's extensive line of security solutions.

Select Product

FortiAuthenticator

Warning! Newer Safari browser may not be supported to access the download links. IE or Firefox browser is recommended.
Below is a series of periodic updates and advisories about the current and upcoming firmware and/or software releases for Fortinet products, please read the associated release notes for further details. All ETA dates are estimates and may be subject to change without notice.

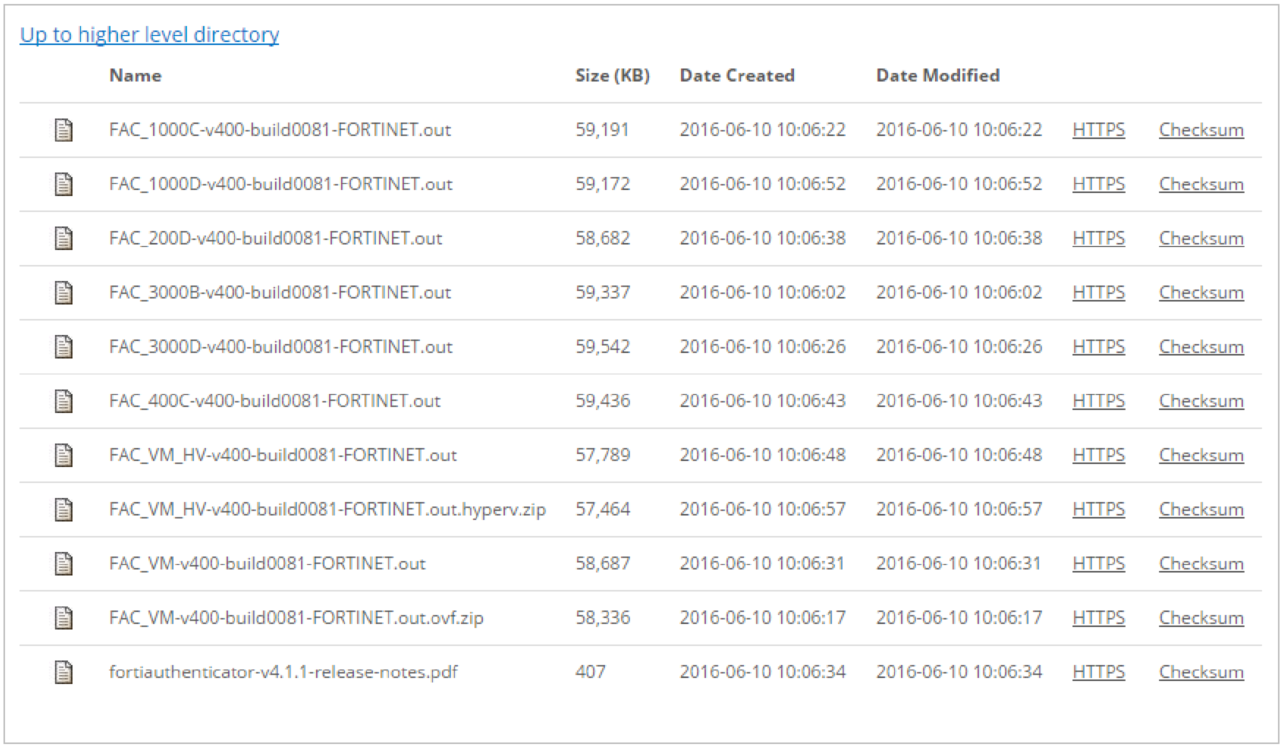
Please read the release notes carefully

FortiAuthenticator 3.0	Description	Notes
Patch 1 Build 0007	Latest 3.0 Patch Release	Released 19 December 2013
Build 0004	3.0 General Availability	Released 28 October 2013

FortiAuthenticator 2.0	Description	Notes
MR2 Patch 3 Build 0210	Latest MR2 Patch Release	Released 22 October 2013
MR2 Patch 2 Build 0209	Latest MR2 Patch Release	Released 16 July 2013
MR2 Patch 1 Build 0208	Latest MR2 Patch Release	Released 21 May 2013

You can also access the latest Firmware releases by adding our RSS feed, simply copy the URL below and follow your RSS reader's instructions for adding a new RSS feed.

2. In the *Firmware Images* page, select **FortiAuthenticator**.
3. Browse to the appropriate directory in the FTP site for the version that you would like to download.



Up to higher level directory

Name	Size (KB)	Date Created	Date Modified		
FAC_1000C-v400-build0081-FORTINET.out	59,191	2016-06-10 10:06:22	2016-06-10 10:06:22	HTTPS	Checksum
FAC_1000D-v400-build0081-FORTINET.out	59,172	2016-06-10 10:06:52	2016-06-10 10:06:52	HTTPS	Checksum
FAC_200D-v400-build0081-FORTINET.out	58,682	2016-06-10 10:06:38	2016-06-10 10:06:38	HTTPS	Checksum
FAC_3000B-v400-build0081-FORTINET.out	59,337	2016-06-10 10:06:02	2016-06-10 10:06:02	HTTPS	Checksum
FAC_3000D-v400-build0081-FORTINET.out	59,542	2016-06-10 10:06:26	2016-06-10 10:06:26	HTTPS	Checksum
FAC_400C-v400-build0081-FORTINET.out	59,436	2016-06-10 10:06:43	2016-06-10 10:06:43	HTTPS	Checksum
FAC_VM_HV-v400-build0081-FORTINET.out	57,789	2016-06-10 10:06:48	2016-06-10 10:06:48	HTTPS	Checksum
FAC_VM_HV-v400-build0081-FORTINET.out.hyperv.zip	57,464	2016-06-10 10:06:57	2016-06-10 10:06:57	HTTPS	Checksum
FAC_VM-v400-build0081-FORTINET.out	58,687	2016-06-10 10:06:31	2016-06-10 10:06:31	HTTPS	Checksum
FAC_VM-v400-build0081-FORTINET.out.ovf.zip	58,336	2016-06-10 10:06:17	2016-06-10 10:06:17	HTTPS	Checksum
fortiauthenticator-v4.1.1-release-notes.pdf	407	2016-06-10 10:06:34	2016-06-10 10:06:34	HTTPS	Checksum

4. Download the `.ovf.zip` file and FortiAuthenticator Release Notes, and save these files to your management computer.

5. Select the `.ovf.zip` file on your management computer and extract the files to a new file folder.

Unlicensed FortiAuthenticator-VM

A FortiAuthenticator-VM is unlicensed until the administrator uploads a Fortinet-issued license file. An unlicensed FortiAuthenticator-VM can be identified by its serial number FAC-VM0000000000 and has a non-expiring five-user limit for small scale evaluation purposes. No activation is required for the unlicensed FortiAuthenticator-VM.

Technical support is not included with the unlicensed FortiAuthenticator-VM.

Please contact your Fortinet Reseller should you require an extended evaluation, i.e. with more users.

FortiAuthenticator-VM Deployment

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

The following sections detail deployments for MS Hyper-V, VMware ESX/ESXi, and Linux Virtual Machine Manager:

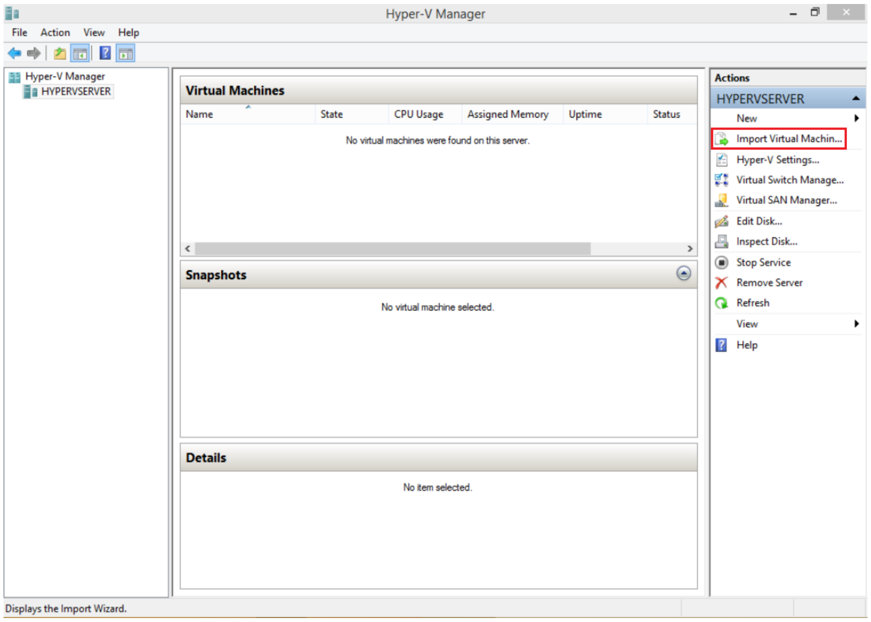
- Deploying FortiAuthenticator-VM on MS Hyper-V
- Deploying FortiAuthenticator-VM on VMware
- Deploying FortiAuthenticator-VM on KVM
- Deploying FortiAuthenticator-VM on Nutanix on page 33
- Configure FortiAuthenticator-VM hardware settings
- Power on your FortiAuthenticator-VM

Deploying FortiAuthenticator-VM on MS Hyper-V

Once you have downloaded the `out.hyperv.zip` file and extracted the package contents to a folder on your management computer, you can deploy the VHD package to your MS Hyper-V environment.

To deploy the FortiAuthenticator VHD template:

1. As an administrator, launch the Hyper-V Manager and connect to your Hyper-V Server.
2. Select the server in the right-hand menu and select *Import Virtual Machine*.



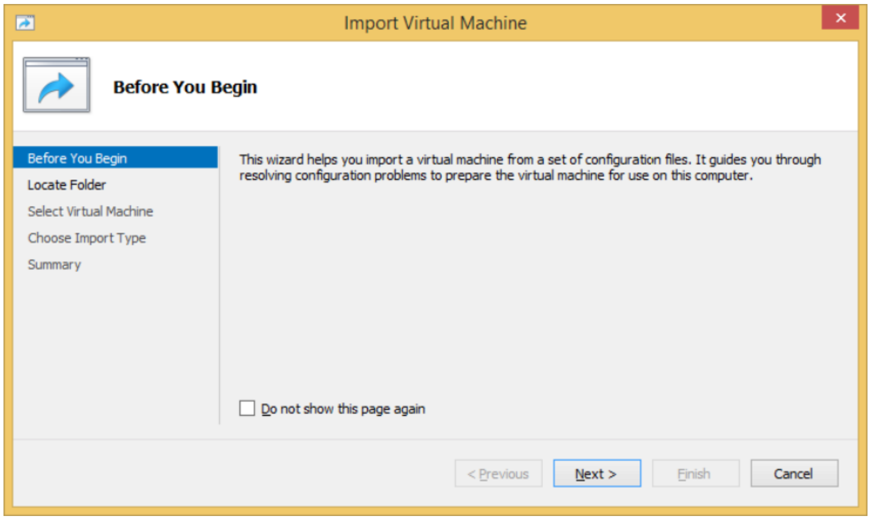
No virtual machines were found on this server.

No virtual machine selected.

No item selected.

Displays the Import Wizard.

The *Import Virtual Machine* page opens. Select *Next* to begin the VM Import process.



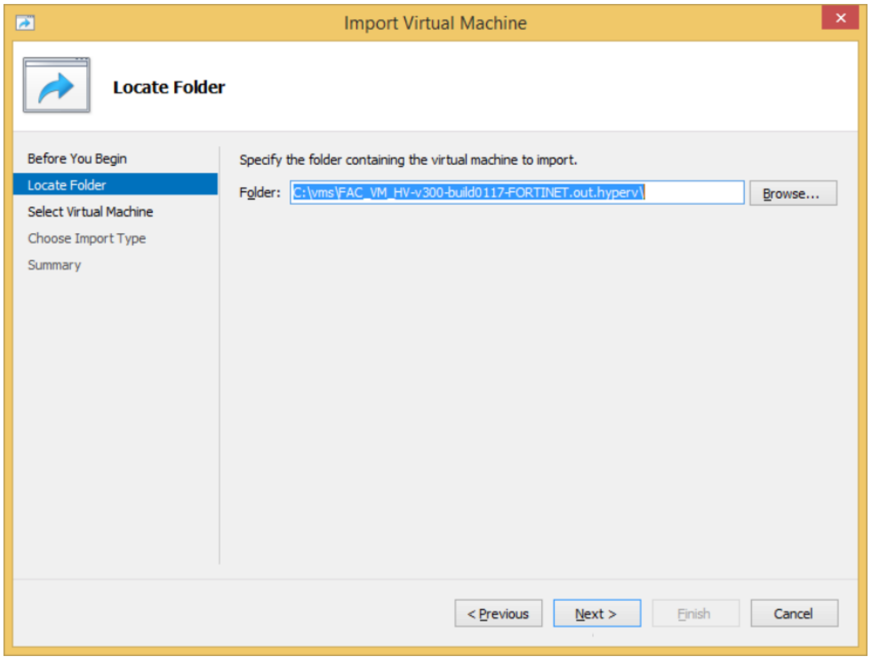
Import Virtual Machine

Before You Begin

This wizard helps you import a virtual machine from a set of configuration files. It guides you through resolving configuration problems to prepare the virtual machine for use on this computer.

☐ Do not show this page again

3. Enter the location of the VM to be imported. This is the location of the folder that you extracted the FortiAuthenticator `hyperv.zip` file to.



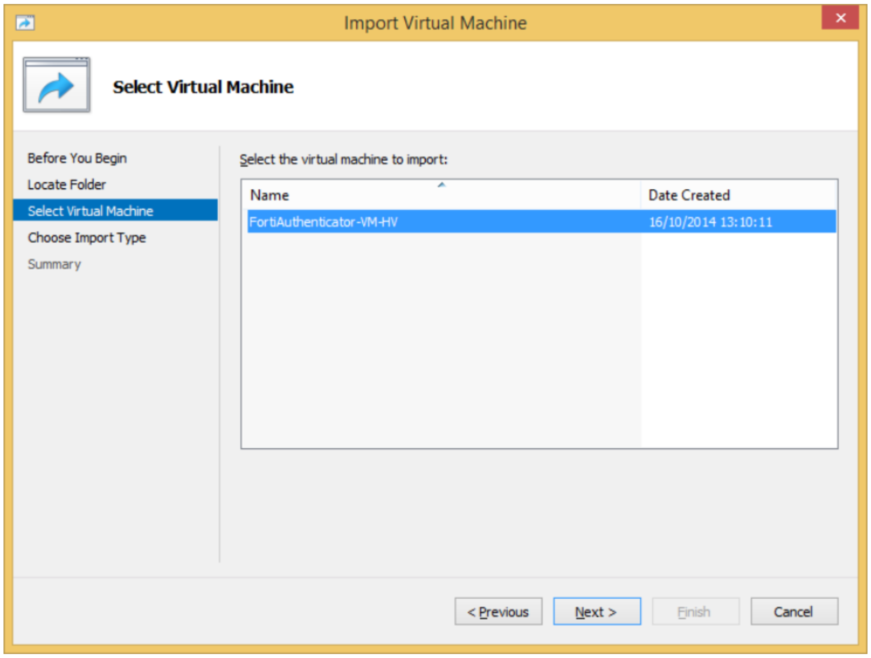
Import Virtual Machine

Locate Folder

Specify the folder containing the virtual machine to import.

Folder: C:\vms\FAC_VM_HV-v300-build0117-FORTINET.out.hyperv\

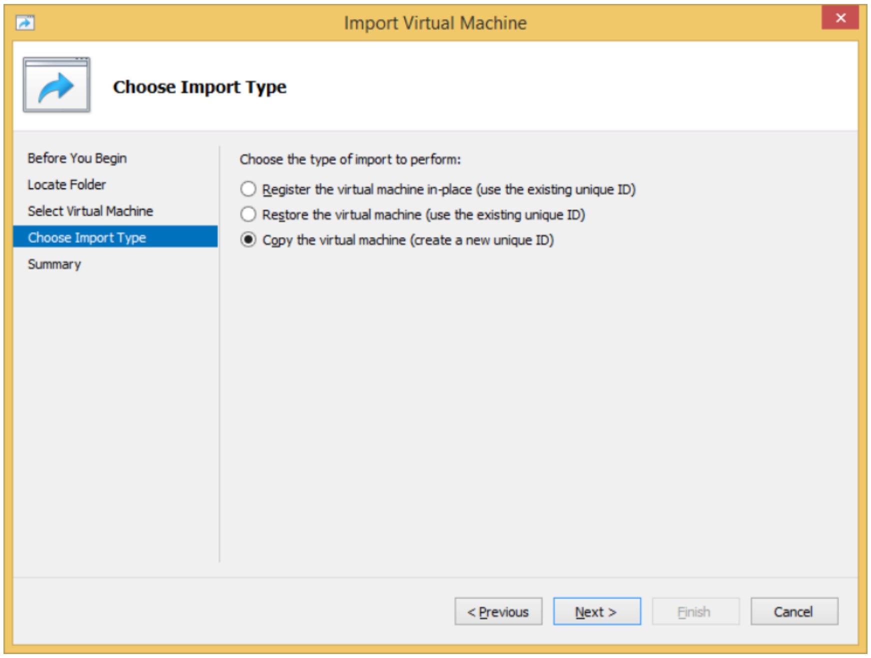
4. Select the FortiAuthenticator-VM and select *Next*.



Select the virtual machine to import:

Name	Date Created
FortiAuthenticator-VM-HV	16/10/2014 13:10:11

5. For the import type, choose *Copy the virtual machine* and select *Next*.



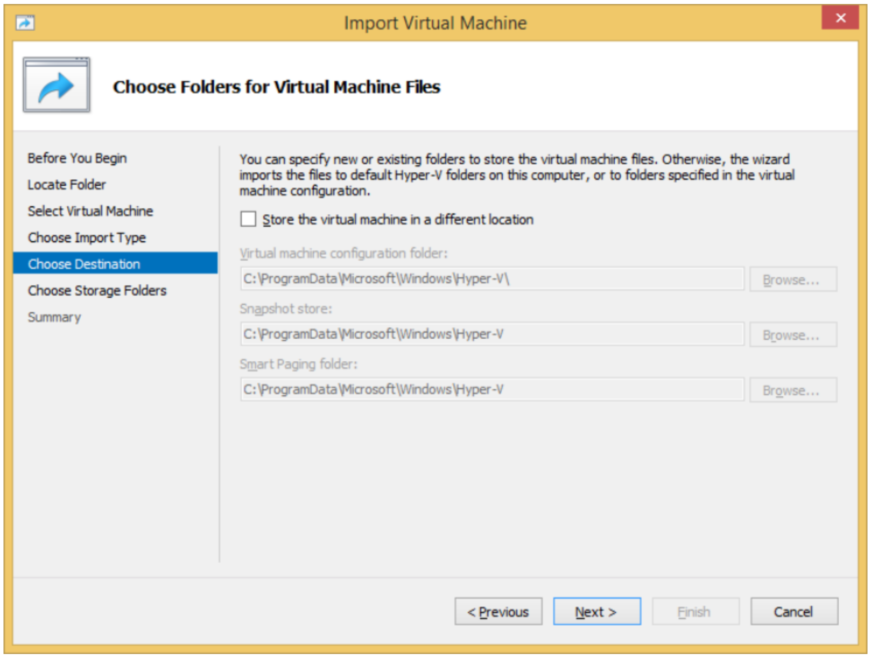
Choose the type of import to perform:

○ Register the virtual machine in-place (use the existing unique ID)

○ Restore the virtual machine (use the existing unique ID)

● Copy the virtual machine (create a new unique ID)

6. Select *Next* if you wish to use the default storage location settings, or specify your own.



Choose Folders for Virtual Machine Files

You can specify new or existing folders to store the virtual machine files. Otherwise, the wizard imports the files to default Hyper-V folders on this computer, or to folders specified in the virtual machine configuration.

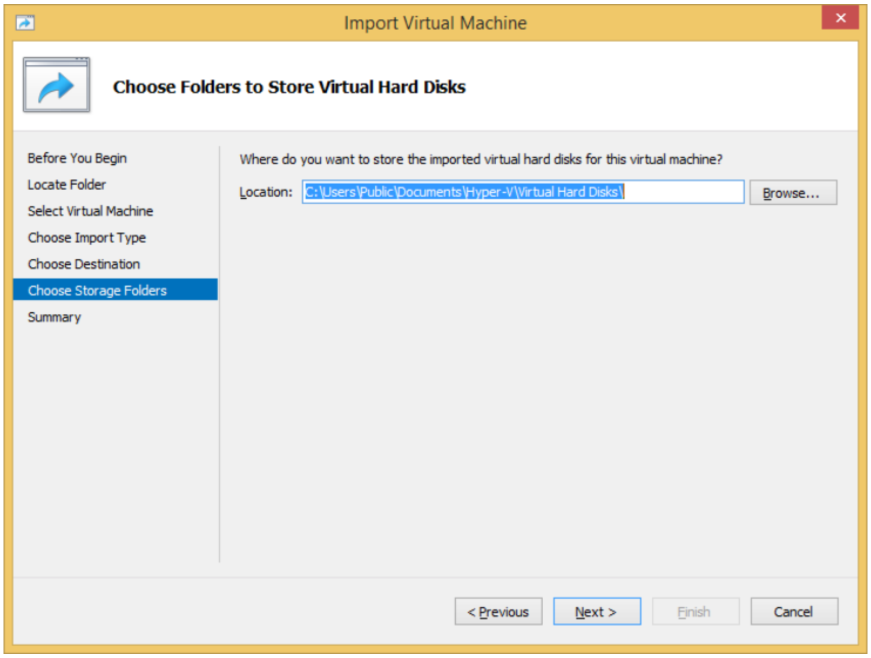
☐ Store the virtual machine in a different location

Virtual machine configuration folder: C:\ProgramData\Microsoft\Windows\Hyper-V\

Snapshot store: C:\ProgramData\Microsoft\Windows\Hyper-V

Smart Paging folder: C:\ProgramData\Microsoft\Windows\Hyper-V

7. Select *Next* if you wish to use the default VM hard disk storage settings, or specify your own.

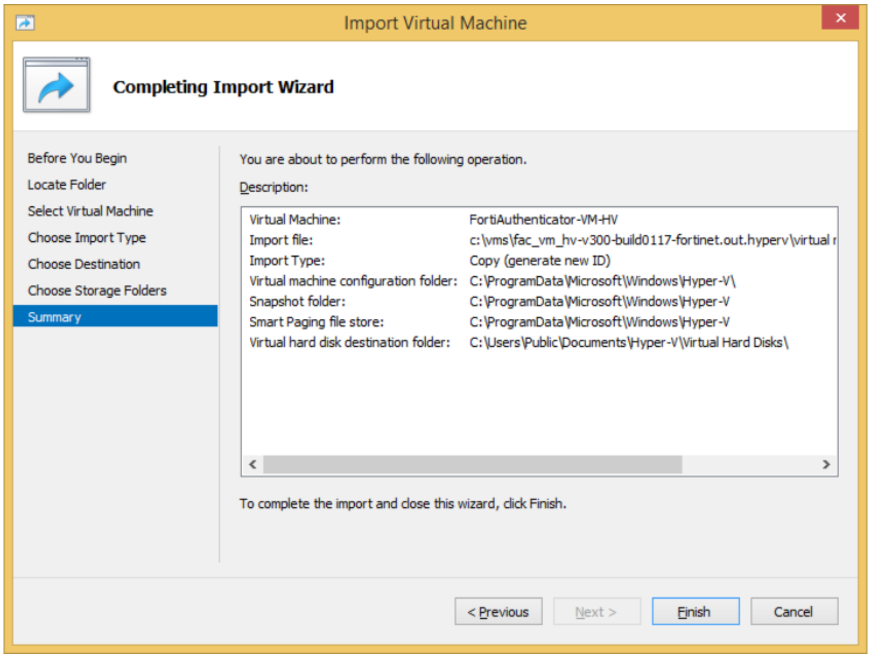


Choose Folders to Store Virtual Hard Disks

Where do you want to store the imported virtual hard disks for this virtual machine?

Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\

8. Select *Finish* to accept the configuration and complete the VM installation.



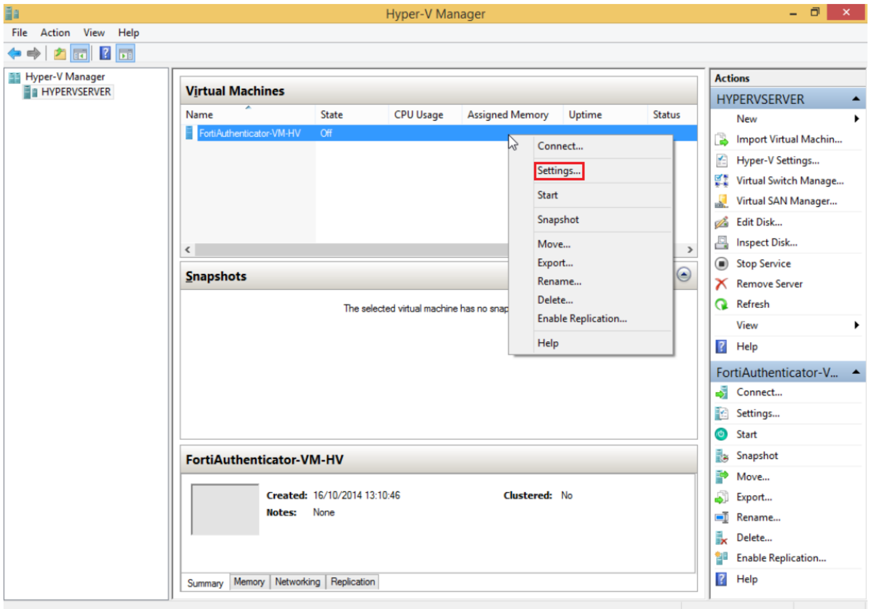
You are about to perform the following operation.

Description:

Virtual Machine:	FortiAuthenticator-VM-HV
Import file:	c:\vms\fac_vm_hv-v300-build0117-fortinet.out.hyperv\virtual r
Import Type:	Copy (generate new ID)
Virtual machine configuration folder:	C:\ProgramData\Microsoft\Windows\Hyper-V\
Snapshot folder:	C:\ProgramData\Microsoft\Windows\Hyper-V
Smart Paging file store:	C:\ProgramData\Microsoft\Windows\Hyper-V
Virtual hard disk destination folder:	C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\

To complete the import and close this wizard, click Finish.

9. The VM will be installed and will be displayed in the Hyper-V Manager. Once complete, and before the VM is started, the hardware settings can be modified. Right-click the new VM and select *Settings...*.



Name	State	CPU Usage	Assigned Memory	Uptime	Status
FortiAuthenticator-VM-HV	Off				

The selected virtual machine has no snap

FortiAuthenticator-VM-HV

Created: 16/10/2014 13:10:46 **Clustered:** No

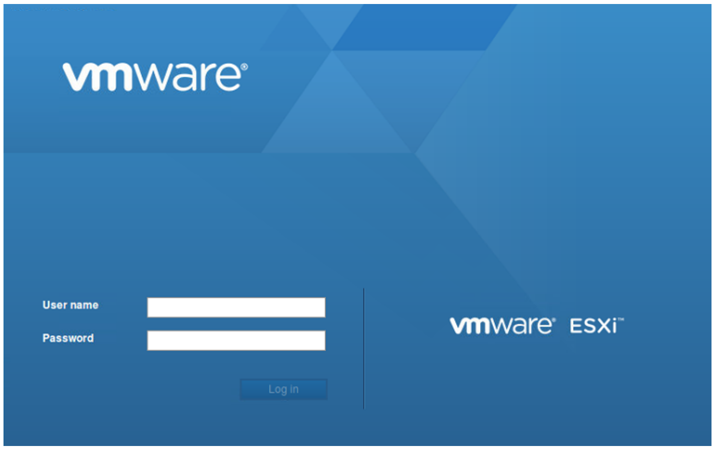
Notes: None

Deploying FortiAuthenticator-VM on VMware

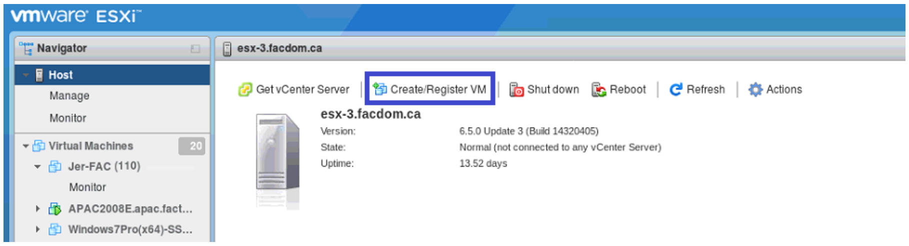
Once you have downloaded the `out.ovf.zip` file and extracted the package contents to a folder on your management computer, you can deploy it into your VMware environment.

To deploy the FortiAuthenticator-VM OVF template:

1. Connect to your VMware ESXi server by visiting its URL in your browser. Enter your username and password, and click *Log in*.



2. Select *Create/Register VM*.



esx-3.facdom.ca

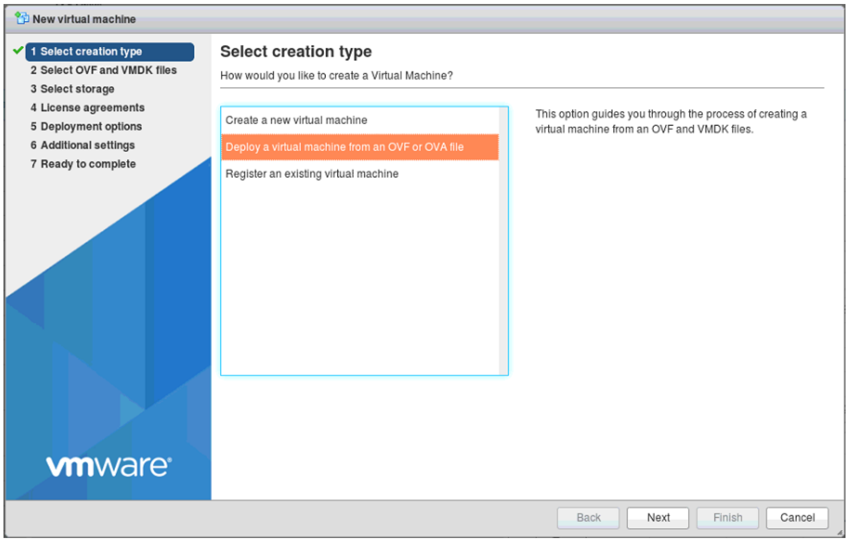
Version: 6.5.0 Update 3 (Build 14320405)

State: Normal (not connected to any vCenter Server)

Uptime: 13.52 days

The VM creation wizard opens.

3. Select *Deploy a virtual machine from an OVF or OVA file*, and click *Next*.

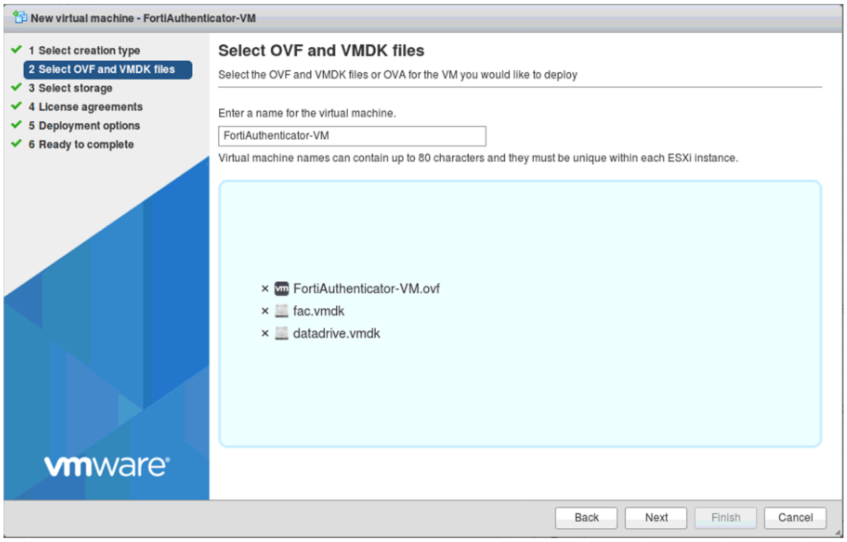


Select creation type

How would you like to create a Virtual Machine?

This option guides you through the process of creating a virtual machine from an OVF and VMDK files.

4. Enter a name for your VM and select the OVF (FortiAuthenticator-VM.ovf), firmware VMDK (fac.vmdk), and data storage VMDK (datadrive.vmdk) files previously extracted to your management computer, and click *Next*.



Select OVF and VMDK files

Select the OVF and VMDK files or OVA for the VM you would like to deploy

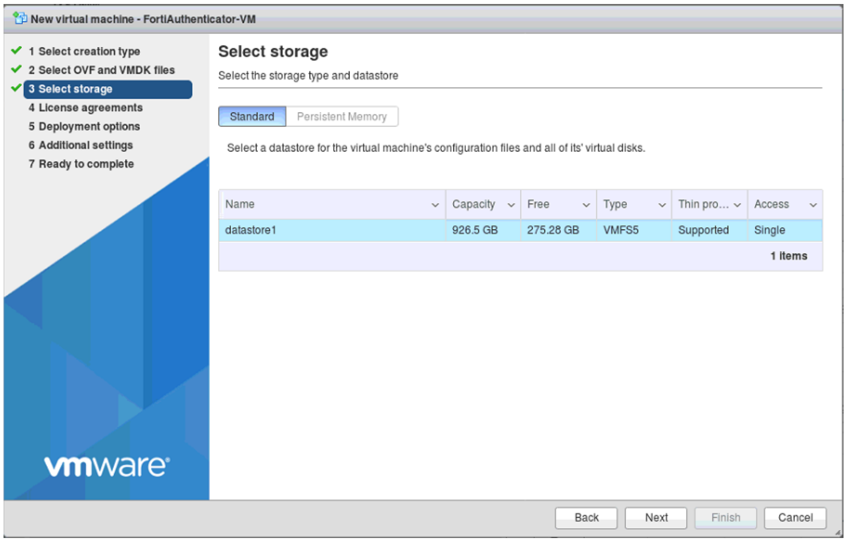
Enter a name for the virtual machine.

FortiAuthenticator-VM

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

× FortiAuthenticator-VM.ovf
× fac.vmdk
× datadrive.vmdk

5. Select which ESXi server's datastore to use for the deployment of FortiAuthenticator-VM, and click *Next*.



Select storage

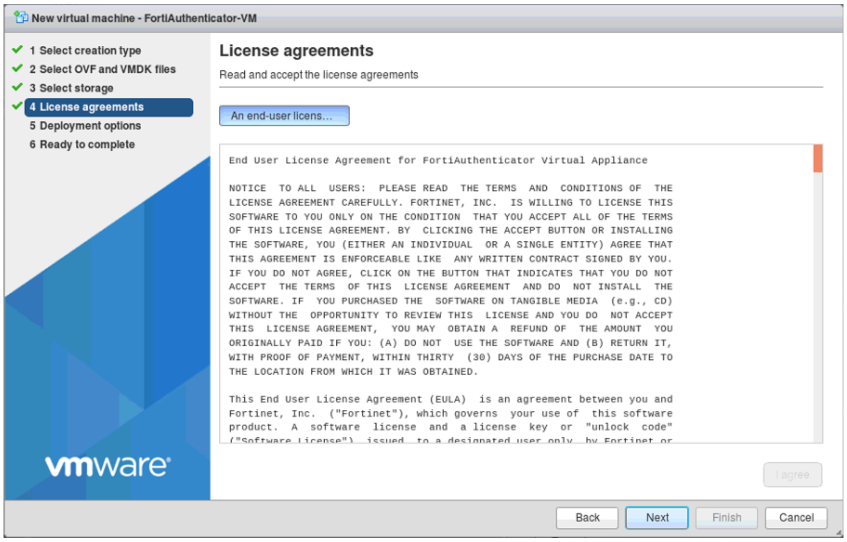
Select the storage type and datastore

Select a datastore for the virtual machine's configuration files and all of its' virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
datastore1	926.5 GB	275.28 GB	VMFS5	Supported	Single

1 items

6. Read the licensing terms and click *I agree* and *Next*.

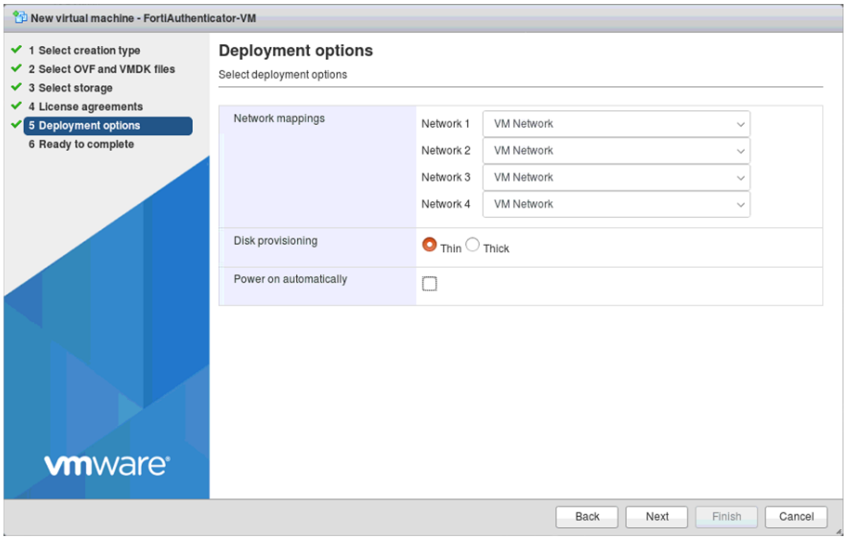


License agreements

Read and accept the license agreements

```
End User License Agreement for FortiAuthenticator Virtual Appliance

NOTICE  TO ALL  USERS:  PLEASE READ  THE TERMS  AND  CONDITIONS OF  THE
LICENSE AGREEMENT CAREFULLY. FORTINET, INC.  IS WILLING TO LICENSE THIS
SOFTWARE TO YOU ONLY ON THE CONDITION  THAT YOU ACCEPT ALL OF THE TERMS
OF THIS LICENSE AGREEMENT. BY  CLICKING THE ACCEPT BUTTON OR INSTALLING
THE SOFTWARE, YOU (EITHER AN INDIVIDUAL  OR A SINGLE ENTITY) AGREE THAT
THIS AGREEMENT IS ENFORCEABLE LIKE  ANY WRITTEN CONTRACT SIGNED BY YOU.
IF YOU DO NOT AGREE, CLICK ON THE BUTTON THAT INDICATES THAT YOU DO NOT
ACCEPT  THE TERMS  OF THIS  LICENSE AGREEMENT  AND DO  NOT INSTALL  THE
SOFTWARE. IF  YOU PURCHASED THE  SOFTWARE ON TANGIBLE MEDIA  (e.g., CD)
WITHOUT THE  OPPORTUNITY TO REVIEW THIS  LICENSE AND YOU DO  NOT ACCEPT
THIS  LICENSE AGREEMENT,  YOU MAY  OBTAIN A  REFUND OF  THE AMOUNT  YOU
ORIGINALLY PAID IF YOU: (A) DO NOT  USE THE SOFTWARE AND (B) RETURN IT,
WITH PROOF OF PAYMENT, WITHIN THIRTY  (30) DAYS OF THE PURCHASE DATE TO
THE LOCATION FROM WHICH IT WAS OBTAINED.

This End User License Agreement (EULA)  is an agreement between you and
Fortinet, Inc.  ("Fortinet"), which governs  your use of  this software
product.  A  software  license  and  a license  key  or  "unlock  code"
("Software License")  issued  to a designated user only  by Fortinet or
```

7. Select the appropriate network mappings, disk provisioning, and power on options for your deployment, and click *Next*.
   - **Thin Provision**: This option optimizes storage use at the cost of sub-optimal disk I/O rates. It allocates disk space only when a write occurs to a block, but the total volume size is reported by VMFS to the OS. Other volumes can take the remaining space. This allows you to float between your servers and expand storage when your size monitoring indicates there is a problem.
     Once a Thin Provisioned block is allocated, it remains in the volume regardless of whether you have deleted data, etc...
   - **Thick Provision**: This option has higher storage requirements, but benefits from optimal disk I/O rates. It allocates the disk space statically. No other volumes can take the allocated space.



New virtual machine - FortiAuthenticator-VM

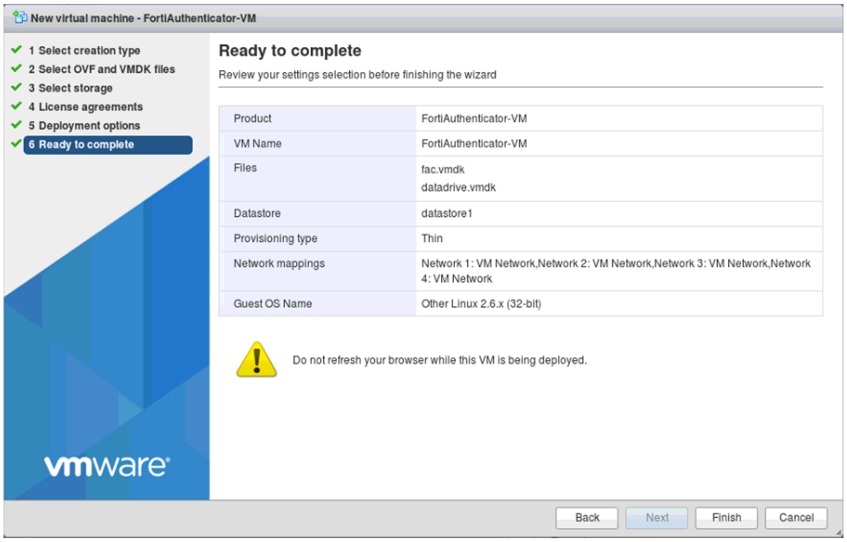
✓ 1 Select creation type
✓ 2 Select OVF and VMDK files
✓ 3 Select storage
✓ 4 License agreements
✓ 5 Deployment options
6 Ready to complete

Deployment options

Select deployment options

Network mappings	Network 1	VM Network
	Network 2	VM Network
	Network 3	VM Network
	Network 4	VM Network
Disk provisioning	● Thin ○ Thick	
Power on automatically	□	

8. Review the summary of your VM settings, and click *Finish*.



New virtual machine - FortiAuthenticator-VM

✓ 1 Select creation type
✓ 2 Select OVF and VMDK files
✓ 3 Select storage
✓ 4 License agreements
✓ 5 Deployment options
✓ 6 Ready to complete

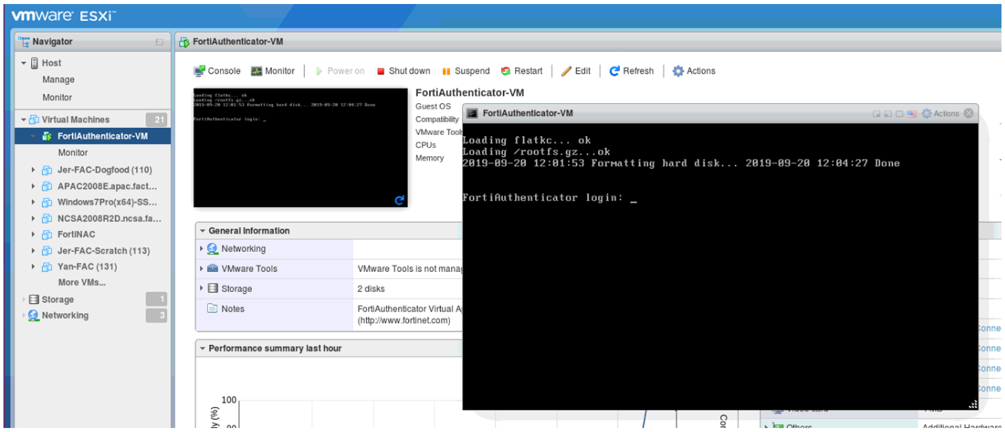
Ready to complete

Review your settings selection before finishing the wizard

Product	FortiAuthenticator-VM
VM Name	FortiAuthenticator-VM
Files	fac.vmdk datadrive.vmdk
Datastore	datastore1
Provisioning type	Thin
Network mappings	Network 1: VM Network,Network 2: VM Network,Network 3: VM Network,Network 4: VM Network
Guest OS Name	Other Linux 2.6.x (32-bit)

Do not refresh your browser while this VM is being deployed.

9. Select your newly created VM and launch it.
   The VM console will be displayed where you can monitor the booting progress of your FortiAuthenticator-VM.



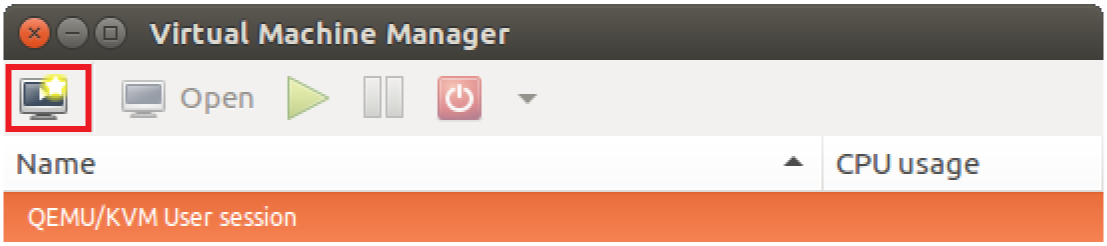
```
Loading flatkc... ok
Loading /rootfs.gz...ok
2019-09-20 12:01:53 Formatting hard disk... 2019-09-20 12:04:27 Done

FortiAuthenticator login: _
```

Deploying FortiAuthenticator-VM on KVM

Once you have downloaded the `out.kvm.zip` file and extracted the virtual hard drive image file fackvm.qcow2, you can create the virtual machine in your KVM environment.

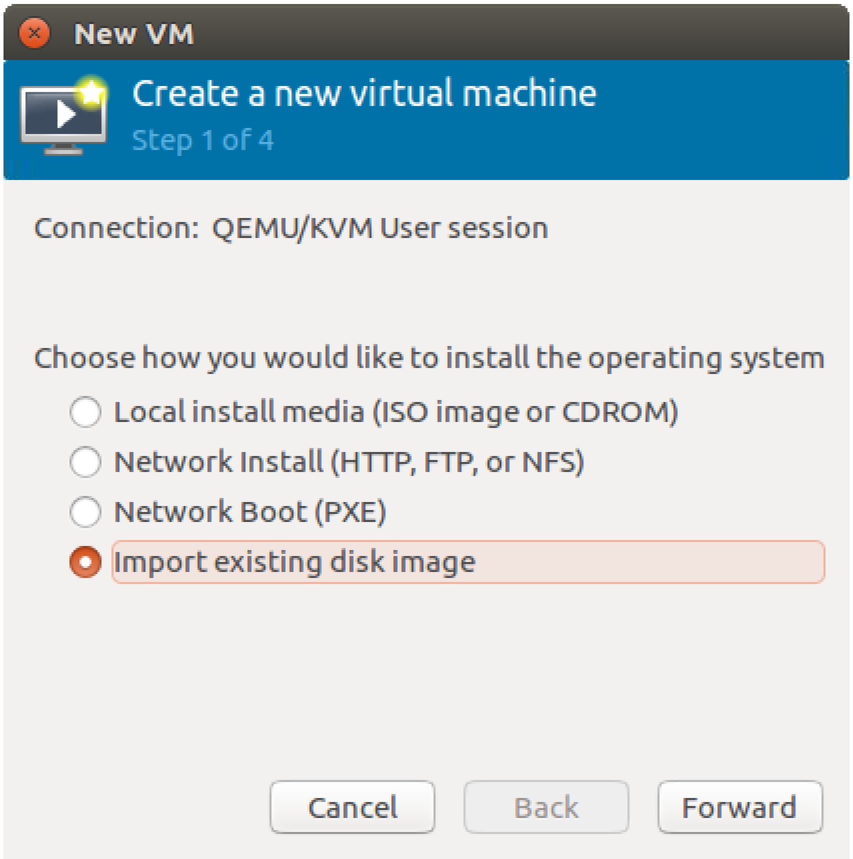
To deploy the FortiAuthenticator-VM virtual machine:

1. Launch *Virtual Machine Manager* on your KVM host server.
2. From the Virtual Machine Manager (VMM) home page, select *Create a new virtual machine*.



The *New VM* window will open.

3. Select *Import existing disk image* and select *Forward*.



New VM

Create a new virtual machine

Step 1 of 4

Connection: QEMU/KVM User session

Choose how you would like to install the operating system

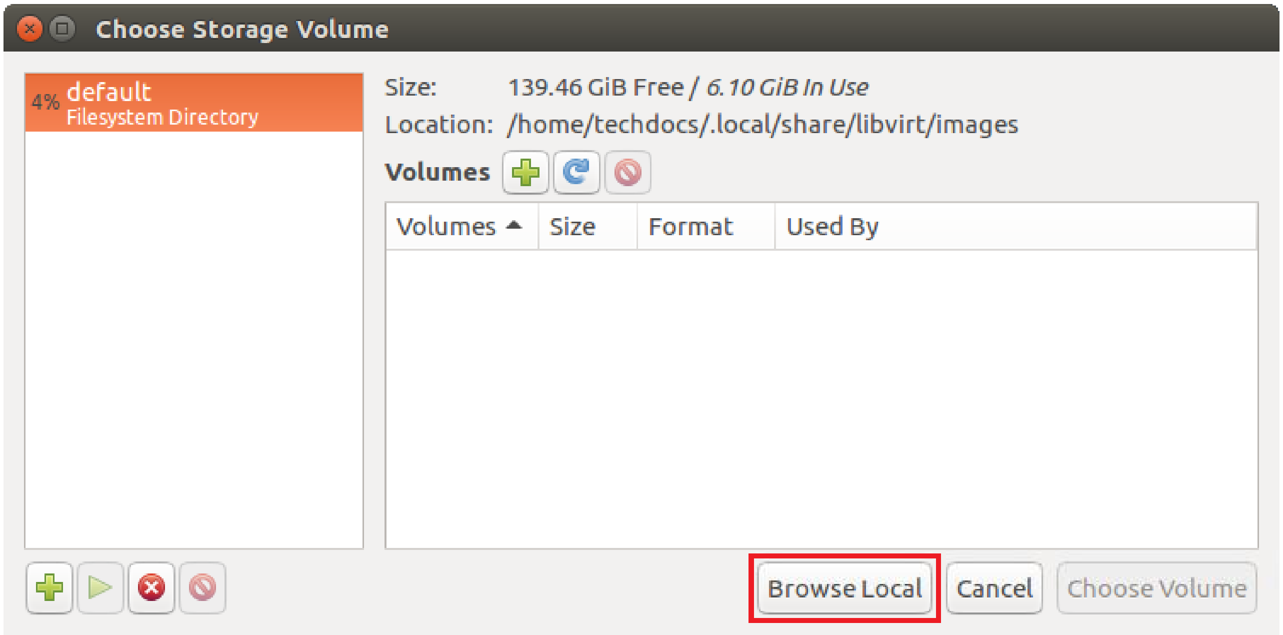
○ Local install media (ISO image or CDROM)

○ Network Install (HTTP, FTP, or NFS)

○ Network Boot (PXE)

● Import existing disk image

4. Select *Browse*. If you saved the *fackvm.qcow2* file to */var/lib/libvirt/images*, it will be visible on the right. If you saved it somewhere else on your server, select *Browse Local*, find it, and select *Choose Volume*.



Choose Storage Volume

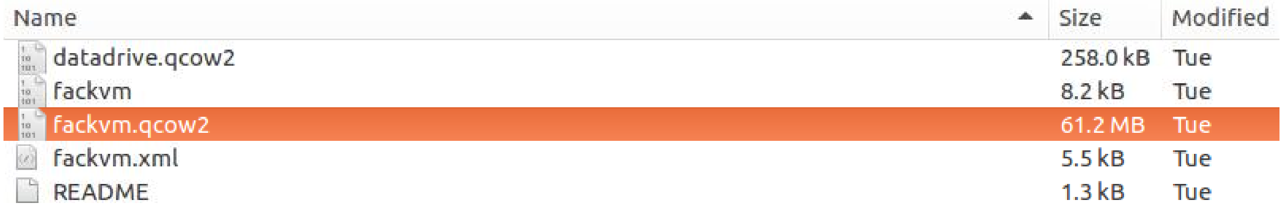
4% default
Filesystem Directory

Size: 139.46 GiB Free / *6.10 GiB In Use*

Location: /home/techdocs/.local/share/libvirt/images

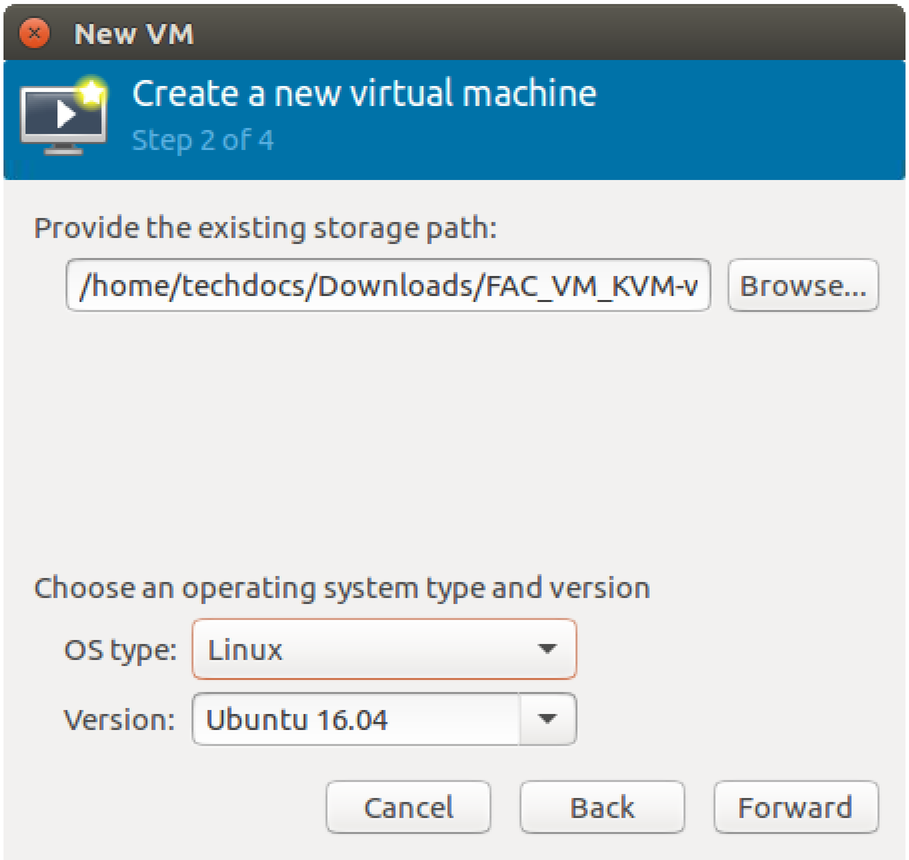
Volumes

Volumes ▲	Size	Format	Used By



Name	Size	Modified
datadrive.qcow2	258.0 kB	Tue
fackvm	8.2 kB	Tue
fackvm.qcow2	61.2 MB	Tue
fackvm.xml	5.5 kB	Tue
README	1.3 kB	Tue

5. Select the *OS type* and *Version* you are running (in this case *Linux Ubuntu 16.04*), and select *Forward*.



Create a new virtual machine

Step 2 of 4

Provide the existing storage path:

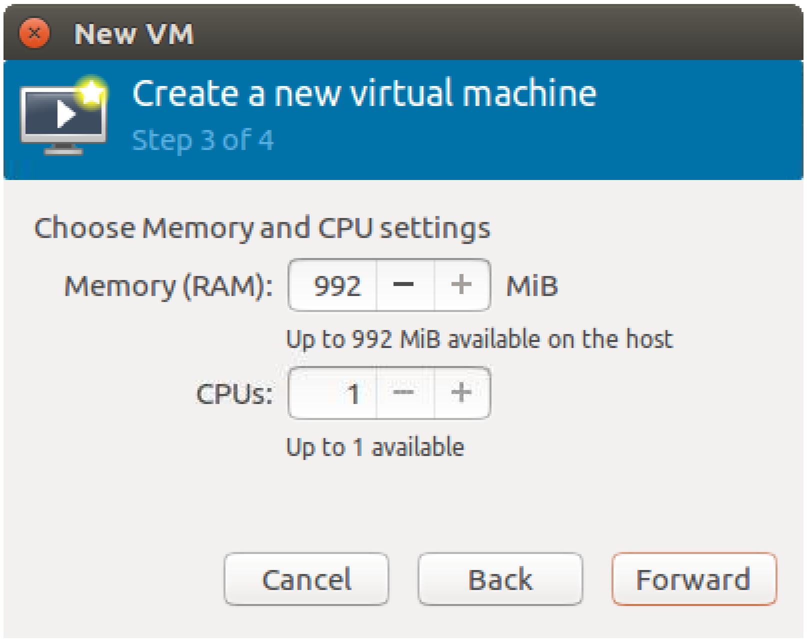
/home/techdocs/Downloads/FAC_VM_KVM-v

Choose an operating system type and version

OS type: Linux

Version: Ubuntu 16.04

6. Specify the amount of memory and number of CPUs to allocate to this virtual machine. The amounts must not exceed your license limits. For more information on your license limits, see Licensing.
Select *Forward*.



Choose Memory and CPU settings

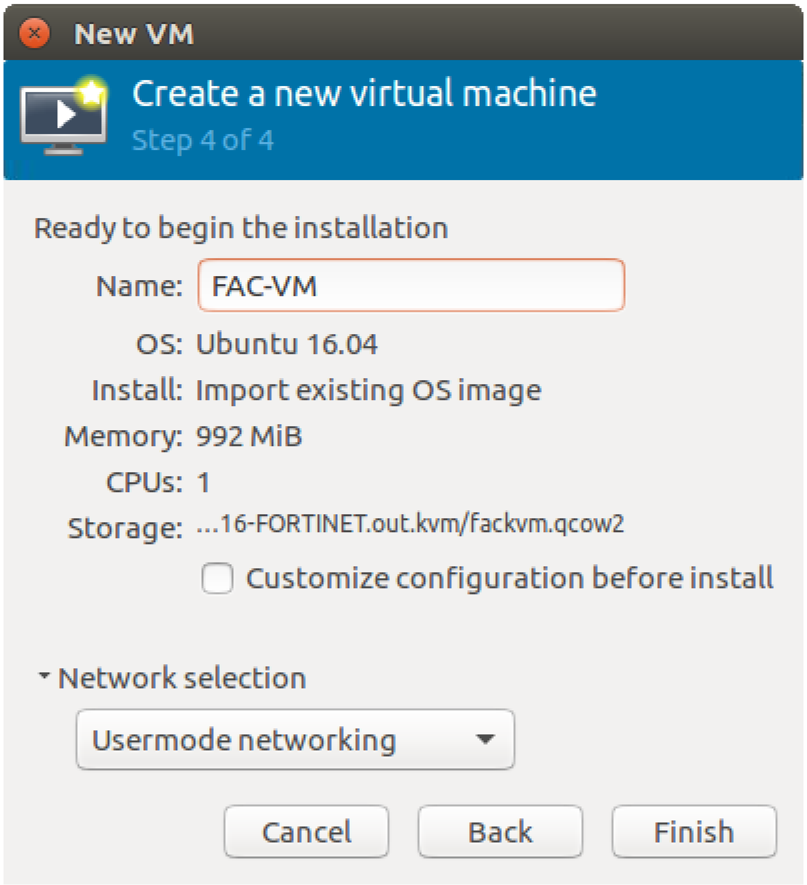
Memory (RAM): 992 MiB

Up to 992 MiB available on the host

CPUs: 1

Up to 1 available

7. On the last page, enter a *Name* for the VM (in this case, *FAC-VM*).
   A new virtual machine includes one network adapter by default. Set *Network selection* to *Usermode networking*. Alternatively, set a specific MAC address for the virtual network interface by selecting *Specify shared device name*.



Ready to begin the installation

Name: FAC-VM

OS: Ubuntu 16.04

Install: Import existing OS image

Memory: 992 MiB

CPUs: 1

Storage: ...16-FORTINET.out.kvm/fackvm.qcow2

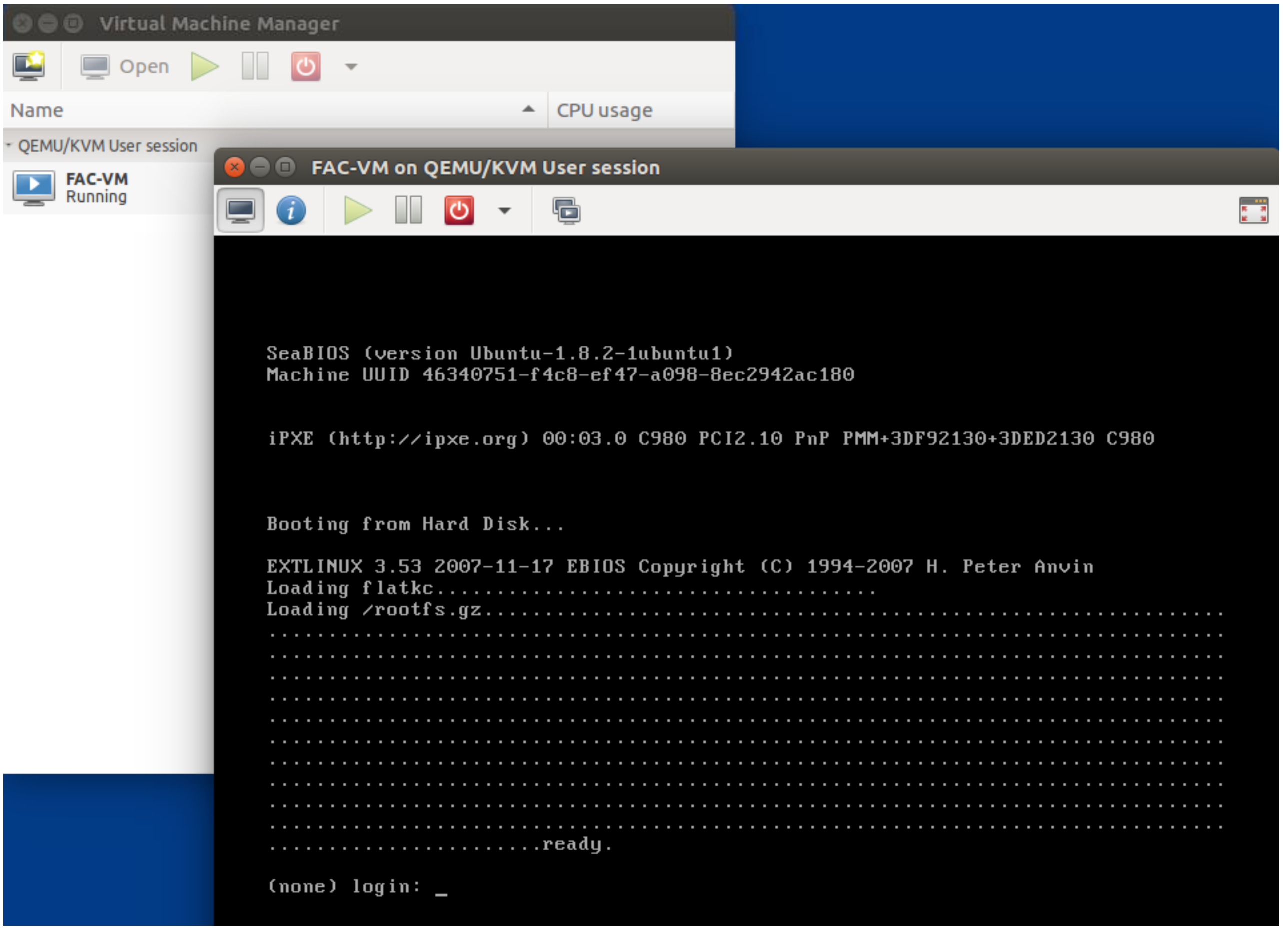
☐ Customize configuration before install

Network selection

Usermode networking

Then select *Finish*.

You new VM will be created an open, prompting login.



```
SeaBIOS (version Ubuntu-1.8.2-1ubuntu1)
Machine UUID 46340751-f4c8-ef47-a098-8ec2942ac180


iPXE (http://ipxe.org) 00:03.0 C980 PCI2.10 PnP PMM+3DF92130+3DED2130 C980



Booting from Hard Disk...

EXTLINUX 3.53 2007-11-17 EBIOS Copyright (C) 1994-2007 H. Peter Anvin
Loading flatkc.....................................
Loading /rootfs.gz..............................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
.......................ready.

(none) login: _
```

Resizing the virtual disk

To resize the disk, and adjust partitions, you must set up the libvirt guest filesystem utilities. The command used to resize the disk, on an Ubuntu host with qcow2 file images, is `virt-resize`.

Import factors to know about this method are the following:

- This is a libvirt utility.
- It can both expand a guest disk and expand the partitions at the same time.
- It copies the disk, which is beneficial if you wish to keep a backup.

Install utilities package

1. Open the VMM *Terminal* and enter the following command to install the libvirt file system utilities package:
   ```
   sudo apt-get install libguestfs-tools
   ```
2. To see if the libvirt utility is functional, you will need to run a test. Enter the following command:
   ```
   sudo apt-get install libguestfs-tools
   ```
   If you see `===== TEST FINISHED OK =====`, it is functional.

3. If you don't see the successful test-finished command return, you will need to repair it. In this case, enter the following command:
   ```
   sudo update-guestfs-appliance
   ```
4. Run the test again (the command from step two) to verify that it works.

Resize disk and partition

1. Shutdown the guest VM.
2. Review the current sizing and view the partition name you want to expand by using the following libvirt utility command:
   ```
   sudo virt-filesystems --long --parts --blkdevs -h -a <name-of-guest-disk-file>
   ```
3. Enter the following command to increase the output disk size. This example increases the disk size by 20GB:
   ```
   sudo qemu-img create -f qcow2 -o preallocation=metadata outdisk 20G
   ```
4. Enter the following command to copy the old disk to the new disk, while expanding the suitable partition:
   ```
   sudo virt-resize --expand <name-of-partition> indisk outdisk
   ```
5. When finished, make sure to rename the indisk file to an appropriate name, such as "backup", while you rename the new outdisk as "indisk".
6. Reboot the guest and test the new disk. When a successful test is complete, you are free to delete the original backup file if you wish.

Configuring the number of virtual CPUs

By default, the virtual appliance is configured to use one (1) virtual CPU (vCPU).

To change the number of vCPUs:

1. Shutdown the guest VM.
2. Right-click the VM and go to *Open* > *Show virtual hardware details* > *CPUs*.
3. Under *Topology*, enable *Manually set CPU topology* and select the number of virtual *Sockets*, the number of *Cores* per socket, and number of *Threads*.
4. Select *Apply* to save the settings.

Configuring the memory limit

VMM measures its memory by mebibytes (MiB).

To change the memory limit:

1. Shutdown the guest VM.
2. Right-click the VM and go to *Open* > *Show virtual hardware details* > *Memory*.
3. Enter the *Maximum allocation* in MiB to allocate to the VM instance.
4. Select *Apply* to save the settings.

Deploying FortiAuthenticator-VM on Nutanix

Once you have downloaded the `out.kvm.zip` file and extracted the virtual hard drive image file `fackvm.qcow2` and the data drive image `datadrive.qcow2`, you can create the virtual machine in your Nutanix environment.

To upload the FortiAuthenticator deployment image to Nutanix:

1. Launch the Prism Element web console.
2. Go to *Settings* > *Image Configuration*.
3. Upload the FortiAuthenticator image by clicking *Upload Image*.
4. In the *Name* field, enter *FortiAuthenticator*.
5. In the *Image Type* dropdown list, ensure that *Disk* is selected.
6. In the *Storage Container*, select the storage container to use.
7. In the *Image Source* pane, click *Upload a file*.
8. Select the `fackvm.qcow2` image file downloaded in To obtain the deployment image.
9. Click *Save*.
10. Follow the above steps (2-10) to upload the FortiAuthenticator data drive image `datadrive.qcow2` with its name as *FortiAuthenticator-DataDrive*.
    Wait a few minutes, then refresh the browser. You will find the newly created VM image in the image list. Confirm that its state is active.

To create the FortiAuthenticator-VM from the image file:

1. In Prism Element web console, go to *VM* > *Create VM*.
2. For *General Configuration* and *Compute Details*, enter the following configuration information:
   a. In the *NAME* field, enter the desired name for VM, for example FortiAuthenticator-VM.
   b. In the VCPU(S) field, enter 2.
   c. In the MEMORY field, enter 8.
3. By default, a CD-ROM is listed under *Disks*. Delete the CD-ROM.
   You must create a boot disk and a data disk for the VM.
4. Create the boot disk:
   a. Click *Add New Disk*.
   b. The boot disk will be cloned from the VM image uploaded. In the *OPERATION* dropdown, select *Clone from Image Service*.
   c. In the *BUS TYPE* dropdown, select *SCSI*.
   d. In the *IMAGE* dropdown, select the FortiAuthenticator disk image uploaded in To upload the FortiAuthenticator deployment image to Nutanix.
   e. Click *Add*. The boot disk has been added.
5. Create the data disk by clicking *Add New Disk* and follow the steps in 4 with *FortiAuthenticator-DataDrive* as the image.
6. Add a network interface for the VM:
   a. Under *Network Adapters (NIC)*, click *Add New NIC*.
   b. Under *VLAN NAME*, select *NR_PRT_STATIC* and click *Add*.
   c. Click *Save*.
   The system displays a *Successfully submitted Create operation* message when the VM has been created successfully with no error.

Configure FortiAuthenticator-VM hardware settings

Before powering on your FortiAuthenticator-VM you must configure the virtual memory, virtual CPU, and virtual disk (VMDK) configuration, and map the virtual network adapters.

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

To see information on how to similarly configure FortiAuthenticator KVM on an Ubuntu host running Virtual Machine Manager, see Resizing the virtual disk and other sections in the KVM deployment example.

Resizing the virtual disk (vDisk)

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

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

The FortiAuthenticator-VM package that you downloaded includes pre-sized VMDK (Virtual Machine Disk Format) files of 1GB for disk 1 (for the OS) and 60GB for disk 2 data, which is large enough for most small deployments. This can be extended if necessary. 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:

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

These options affect the possible size of each vDisk.

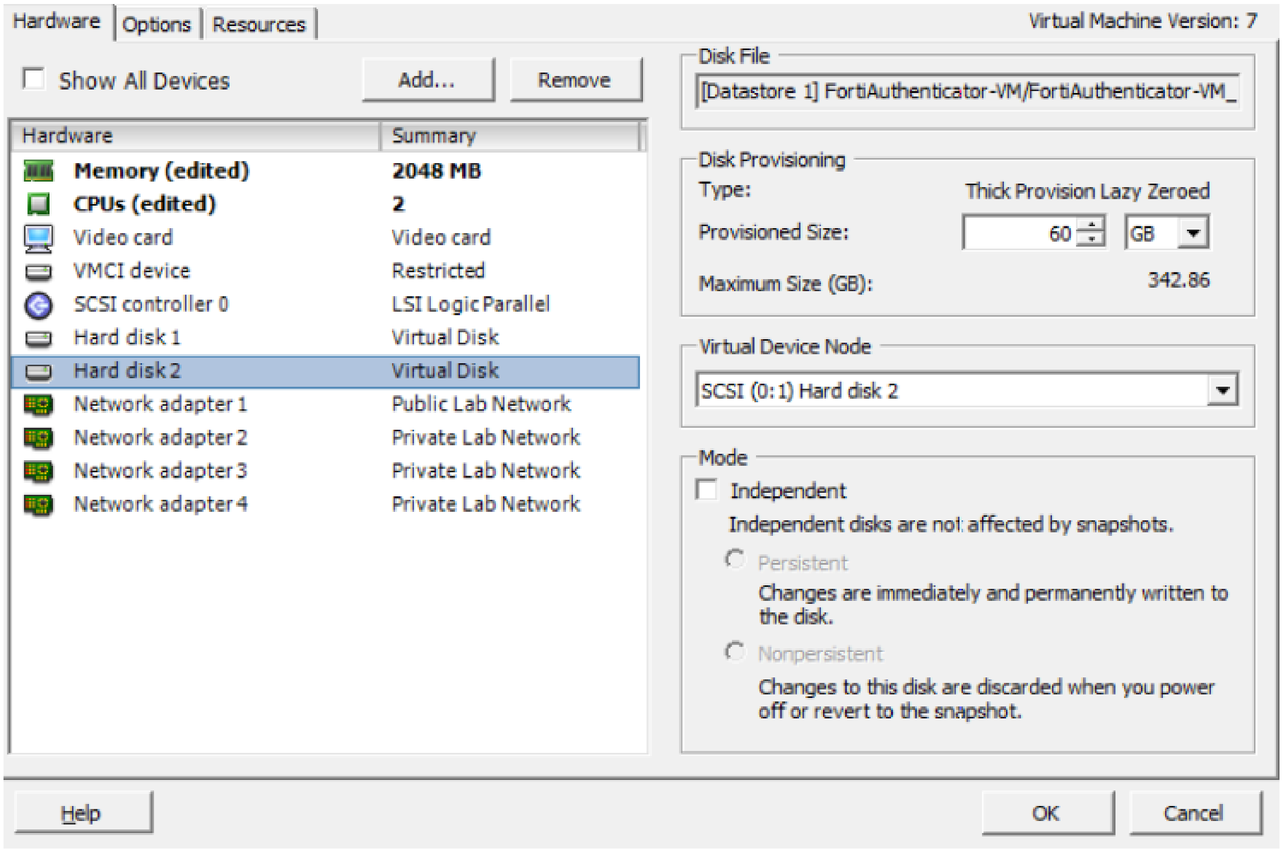
For example, if you have an 800GB datastore which has been formatted with 1MB block size, you cannot size a single vDisk greater than 256GB on your FortiAuthenticator-VM.

Consider also that, depending on the size of your organization's network, you might require more or less storage for the user database and logging.

For more information on vDisk sizing, see http://communities.vmware.com/docs/DOC-11920.

To resize the vDisk:

1. In the VMware vSphere Client, right-click the name of the virtual appliance, and select *Edit Settings*.
   The *Virtual Machine Properties* page is displayed.



Virtual Machine Version: 7

□ Show All Devices

Hardware	Summary
Memory (edited)	**2048 MB**
CPUs (edited)	**2**
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
Network adapter 1	Public Lab Network
Network adapter 2	Private Lab Network
Network adapter 3	Private Lab Network
Network adapter 4	Private Lab Network

Disk File
[Datastore 1] FortiAuthenticator-VM/FortiAuthenticator-VM_

Disk Provisioning
Type: Thick Provision Lazy Zeroed
Provisioned Size: 60 GB
Maximum Size (GB): 342.86

Virtual Device Node
SCSI (0:1) Hard disk 2

Mode
□ Independent
Independent disks are not affected by snapshots.
○ Persistent
Changes are immediately and permanently written to the disk.
○ Nonpersistent
Changes to this disk are discarded when you power off or revert to the snapshot.

2. Select the *Hardware* tab and select *Hard Disk 2*.
3. Select *Remove*.
4. Select *Add*.
   The *Add Hardware* page is displayed.
5. In the list of device types, select *Hard Disk* and select *Next*.
6. Select *Create a new virtual disk* and select *Next*.
7. In *Disk Size*, enter the size of the vDisk in GB and select *Next*.
8. Select the bottom option in *Virtual Device Node*, select *IDE (0:1)* from the drop-down list, then select *Next*.
9. Select *Finish* to close the *Add Hardware* page and then select OK to save the settings to Virtual Machine Properties.

Configuring the number of virtual CPUs (vCPUs)

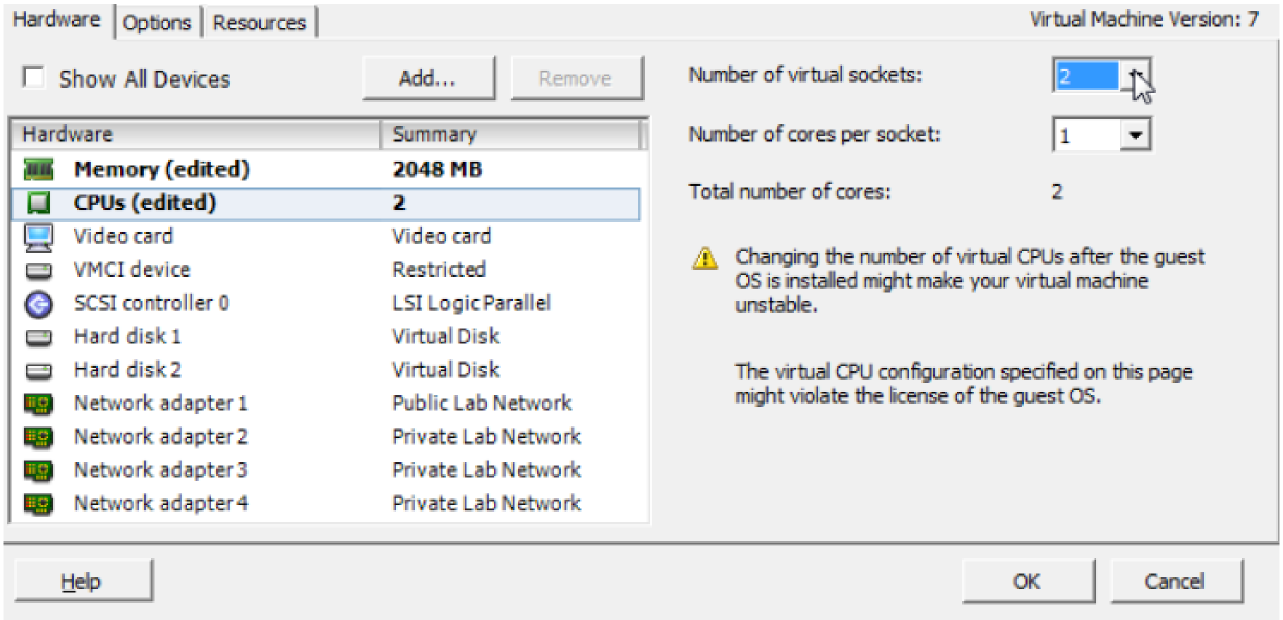
By default, the virtual appliance is configured to use 2 vCPUs. FortiAuthenticator-VM is not restricted to how many vCPUs can be configured so you can increase the number according to your requirements (e.g., you can allocate 2, 4, or 8 vCPUs).

If you need to increase or decrease the vCPUs after the initial boot, power off FortiAuthenticator-VM, adjust the number of vCPUs, then power on the VM.

For more information on vCPUs, visit http://www.vmware.com/products/vsphere-hypervisor/index.html for VMware vSphere documentation.

To change the number of vCPUs:

1. In the VMware vSphere Client, right-click the name of the virtual appliance, and select *Edit Settings*.
   The *Virtual Machine Properties* page is displayed.



Hardware	Summary
Memory (edited)	**2048 MB**
CPUs (edited)	**2**
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
Network adapter 1	Public Lab Network
Network adapter 2	Private Lab Network
Network adapter 3	Private Lab Network
Network adapter 4	Private Lab Network

Number of virtual sockets: 2

Number of cores per socket: 1

Total number of cores: 2

⚠ Changing the number of virtual CPUs after the guest OS is installed might make your virtual machine unstable.

The virtual CPU configuration specified on this page might violate the license of the guest OS.

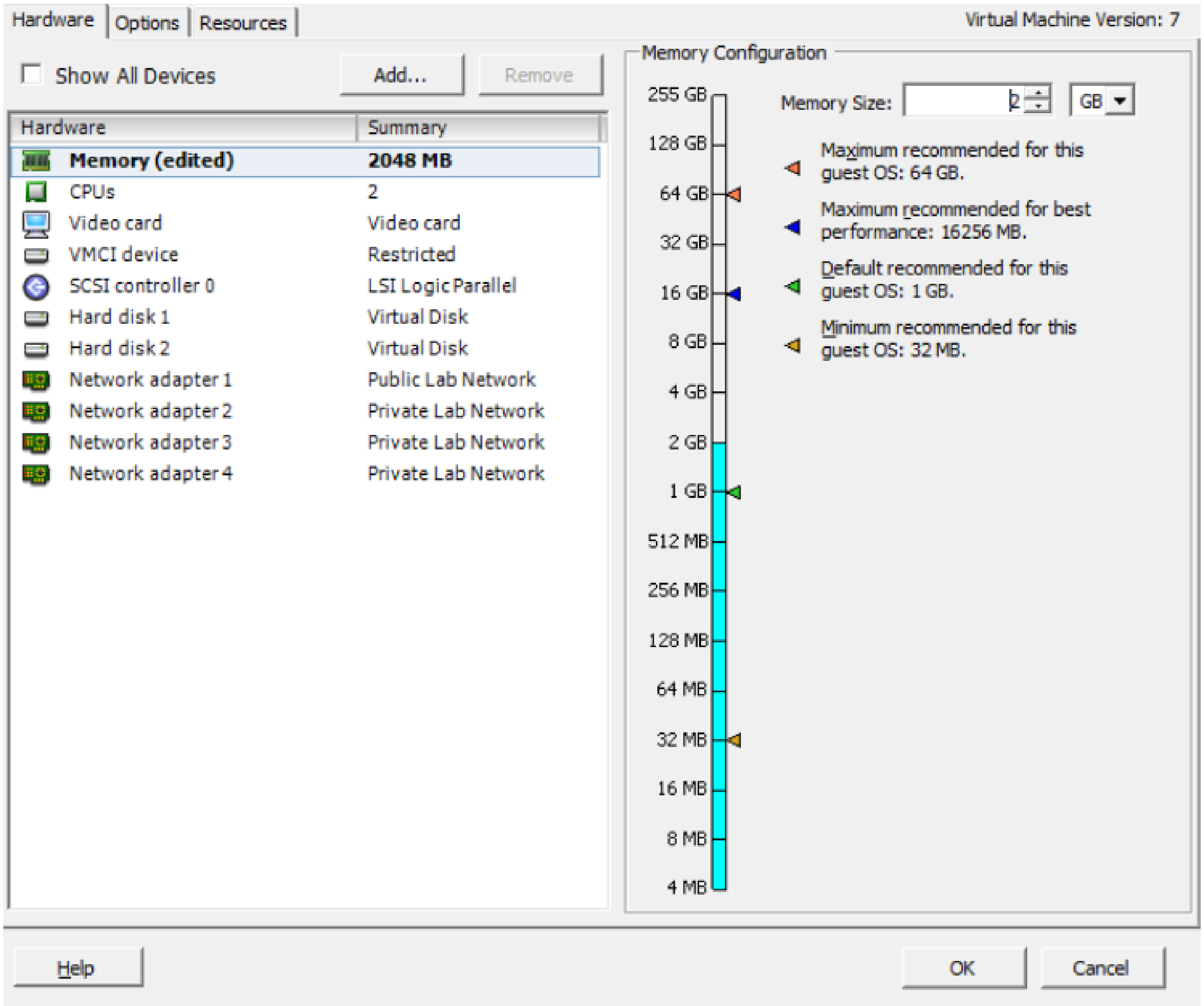
2. Select the *Hardware* tab and select CPUs.
3. Select the number of virtual sockets and the number of cores per socket.
4. Select *OK* to save the settings to Virtual Machines Properties.

Configuring the virtual RAM (vRAM) limit

FortiAuthenticator-VM comes pre-configured to use 512MB of vRAM. You can change this value. The valid range is from 512MB to 16GB.

To change the amount of vRAM:

1. In the VMware vSphere Client, right-click the name of the virtual appliance, and select *Edit Settings*.
   The *Virtual Machine Properties* page is displayed.



Hardware	Summary
Memory (edited)	**2048 MB**
CPUs	2
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
Network adapter 1	Public Lab Network
Network adapter 2	Private Lab Network
Network adapter 3	Private Lab Network
Network adapter 4	Private Lab Network

Memory Size: 2 GB

Maximum recommended for this guest OS: 64 GB.

Maximum recommended for best performance: 16256 MB.

Default recommended for this guest OS: 1 GB.

Minimum recommended for this guest OS: 32 MB.

2. Select the *Hardware* tab and select *Memory*.
3. Enter the maximum memory in GB to allocate to the VM instance.
4. Select *OK* to save the settings to Virtual Machine Properties.

Mapping the virtual NICs (vNICs) to physical NICs

Appropriate mappings of the FortiAuthenticator-VM ports to physical ports depends on your existing virtual environment. Often, the default bridging vNICs work, and do not need to be changed.

If you are unsure of your network mappings, try bridging first before non-default vNIC modes such as NAT or host-only networks. The default bridging vNIC mappings are appropriate where each of the host's guest virtual machines should have their own IP addresses on your network. The most common exceptions to this rule are for VLANs and the transparent modes.

When you deploy the FortiAuthenticator-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 FortiAuthenticator-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.

Example network mapping:

VMware vSphere			FortiAuthenticator-VM
Physical Network Adapter	**Network Mapping (vSwitch Port Group)**	**Virtual Network Adapter for FAC VM**	**Network Interface Name in GUI and CLI**
eth0	VM Network 0	Management	port1
eth1	VM Network 1	External	port2
eth0	VM Network 2	Internal (LDAP)	port3
eth0	VM Network 1	Unconfigured	port4

To map network adapters:

1. In the VMware vSphere Client, right-click the name of the virtual appliance, and select *Edit Settings*.
   The *Virtual Machine Properties* page is displayed.
2. Select the *Hardware* tab and select Network adapter 1.
3. From the Network Connection dropdown list, select the virtual network mapping for the virtual network adapter. Repeat this step for the other three network adapters. The correct mapping varies by your virtual environment's network configuration.
4. Select *OK* to save the settings to Virtual Machine Properties.

Power on your FortiAuthenticator-VM

You can now proceed to power on your FortiAuthenticator-VM. Select the name of the FortiAuthenticator-VM you deployed in the inventory list and select *Power on the virtual machine* in the *Getting Started* tab. Optionally, you can select the name of the FortiAuthenticator-VM you deployed, right-click and select *Power* > *Power On*.

Initial Configuration

Before you can connect to the FortiAuthenticator-VM GUI you must configure basic network settings via the console tab in your vSphere client. Once configured, you can connect to the FortiAuthenticator-VM GUI and upload the FortiAuthenticator-VM license file that you downloaded from FortiCloud.

The following topics are included in this section:

- FortiAuthenticator-VM console access on page 39
- Connect to the FortiAuthenticator-VM GUI on page 40
- Upload the FortiAuthenticator-VM license file on page 40
- Configure your FortiAuthenticator-VM on page 42

FortiAuthenticator-VM console access

To enable GUI access to the FortiAuthenticator-VM you must configure basic network settings of the FortiAuthenticator-VM in the vSphere Client Console tab.

To configure basic network settings in FortiAuthenticator-VM:

1. In the *Inventory* list, select the FortiAuthenticator-VM that you deployed. In the *Getting Started* tab select *Power on the virtual machine*. Optionally, you can right-click the FortiAuthenticator-VM, and select *Power* > *Power On*.
2. Select the *Console* tab.
   The *Console* window appears.
3. At the FortiAuthenticator-VM login prompt enter the username `admin` and password. The default password is no password.
4. The default `Port1` IP address is set to `192.168.1.99/24`. You can change this IP address with the following CLI command:

```
config system interface
   edit port1
      set ip <ip-address>/<netmask>
      set allowaccess https ssh gui
   next
end
config router static
   edit 0
      set device port1
      set dst 0.0.0.0/0
      set gateway <ip-gateway>
   next
end
```

FortiCloud currently does not support IPv6 for FortiAuthenticator-VM license validation. You must specify an IPv4 address in both the support portal and the port1 management interface.

Connect to the FortiAuthenticator-VM GUI

Once you have configured the port1 IP address, network mask, and default gateway, launch a web browser and enter the IP address you configured for port1.

To support HTTPS authentication, the FortiAuthenticator-VM includes a self-signed X.509 certificate, which it presents to clients whenever they initiate an HTTPS connection to the FortiAuthenticator appliance. When you connect, depending on your web browser and prior access of the FortiAuthenticator-VM, 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. TLS v1.0, TLS v1.1, and TLS v1.2 are supported.

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.

At the login page, enter the user name admin and password and select Login. The default password is no password. The GUI will appear with an Evaluation License dialog box.

By default, the GUI is accessible via HTTPS.

Upload the FortiAuthenticator-VM license file

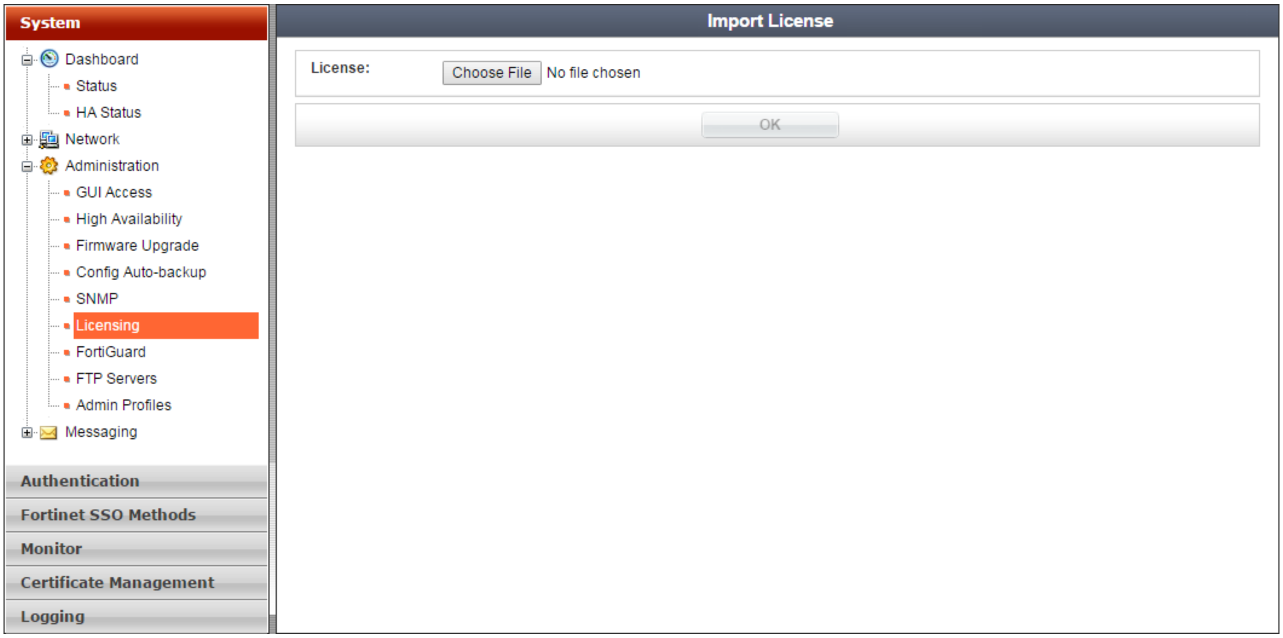
Every FortiAuthenticator-VM includes a 5-user evaluation license. During this time the FortiAuthenticator-VM operates in evaluation mode. Before using the FortiAuthenticator-VM you must enter the license file that you downloaded from FortiCloud upon registration.

Plan a maintenance window to apply the FortiAuthenticator-VM license as the VM will 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 FortiAuthenticator-VM license to support your needs.

To upload the FortiAuthenticator-VM license file:

1. Log into the FortiAuthenticator-VM.
2. Go to *System* > *Administration* > *Licensing*.
   The *Import License* page opens.

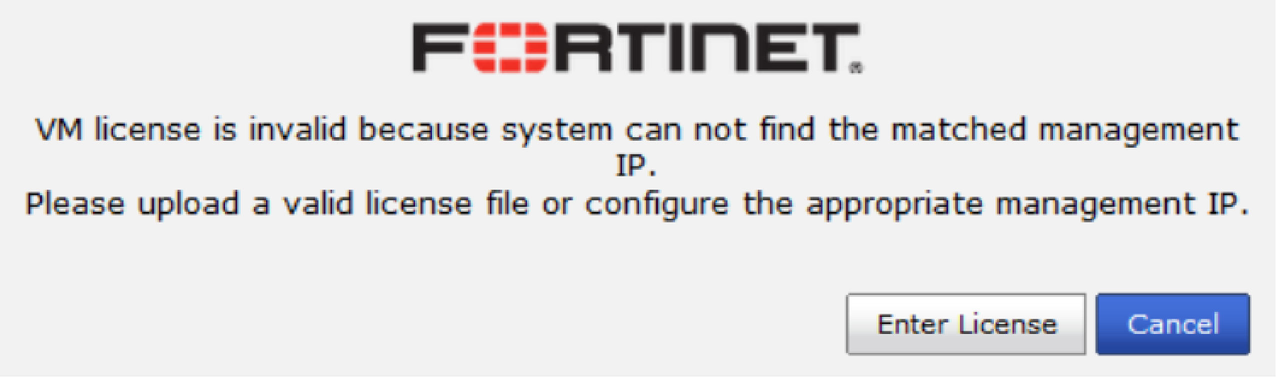


License: No file chosen

3. Select *Choose File* and locate the license file (`.lic`) on your computer. Select *OK* to upload the license file.
4. The VM registration status appears as valid once the license has been validated.

As a part of the license validation process, FortiAuthenticator-VM compares its IP address with the IP information in the license file. If a new license has been imported or the FortiAuthenticator's IP address has been changed, the FortiAuthenticator-VM must be rebooted in order for the system to validate the change and operate with a valid license.

5. If the IP address in the license file and the IP address configured in the FortiAuthenticator-VM do not match, you will receive the following error message dialog box when you log back into the VM.



VM license is invalid because system can not find the matched management IP.
Please upload a valid license file or configure the appropriate management IP.

If this occurs, you will need to change the IP address in FortiCloud to match the management IP and re-download the license file.

After an invalid license file is loaded to FortiAuthenticator-VM, the GUI will be locked until a valid license file is uploaded.

Configure your FortiAuthenticator-VM

Once the FortiAuthenticator-VM license has been validated you can begin to configure your device. For more information on configuring your FortiAuthenticator-VM see the FortiAuthenticator Administration Guide on the Fortinet Document Library.

In VM environments, it is recommended that you use the VMware *Snapshot* utility to backup the VM instance. In the event of an issue with a firmware upgrade or configuration issue, you can use the *Snapshot Manager* to revert the VM instance to a previous *Snapshot*. To create a *Snapshot*, right-click the VM instance and select *Snapshot* > *Take Snapshot*.