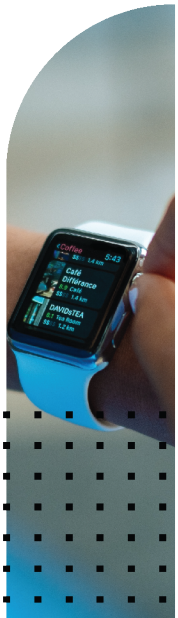
MS Hyper-V Administration Guide

FortiAuthenticator 6.4.0



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 6.4.0 MS Hyper-V Administration Guide
23-640-734874-20221102

TABLE OF CONTENTS

Change Log **4**
Introduction **5**
Architecture 5
FortiAuthenticator-VM Overview **7**
Licensing 7
System requirements 8
VM requirements 9
FortiAuthenticator-VM sizing guidelines 9
Register FortiAuthenticator-VM on FortiCloud 10
Download the FortiAuthenticator-VM software 11
MS Hyper-V deployment package contents 11
Unlicensed FortiAuthenticator-VM 13
FortiAuthenticator-VM Deployment **15**
Deploying FortiAuthenticator-VM on MS Hyper-V 15
Power on your FortiAuthenticator-VM 19
Initial Configuration **20**
FortiAuthenticator-VM console access 20
Connect to the FortiAuthenticator-VM GUI 21
Upload the FortiAuthenticator-VM license file 21
Configure your FortiAuthenticator-VM 23

Change Log

Date	Change Description
2021-08-05	Initial release.
2021-09-08	Updated FortiAuthenticator-VM console access on page 20.
2022-11-02	Updated Licensing on page 7 and System requirements on page 8.

Introduction

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, TACACS+ 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.

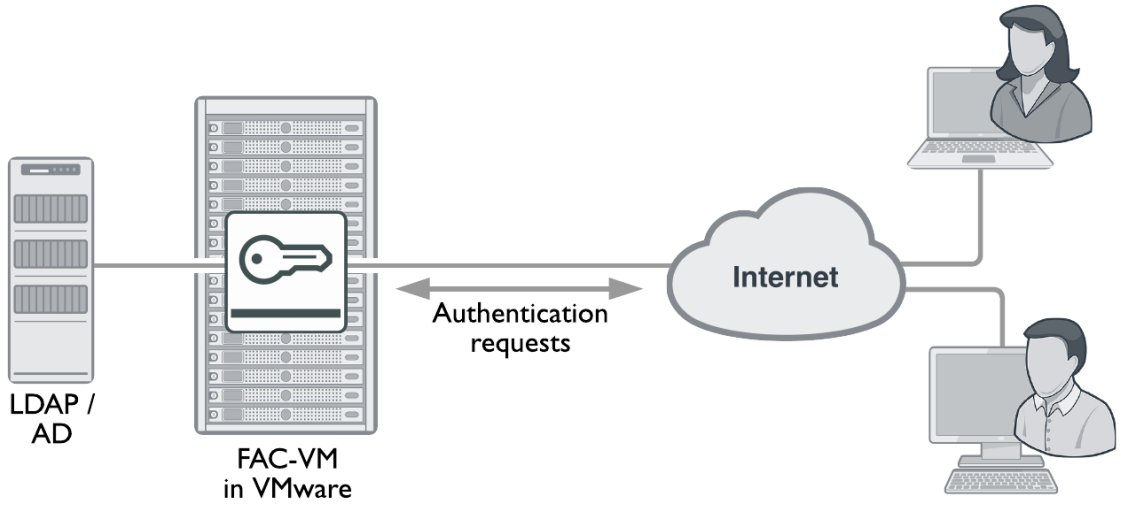
Failure to protect the FortiAuthenticator may result in compromised authentication databases.

This document includes an overview of the FortiAuthenticator-VM, its deployment with MS Hyper-V, 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.

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 8
- Register FortiAuthenticator-VM on FortiCloud on page 10
- Download the FortiAuthenticator-VM software on page 11
- Unlicensed FortiAuthenticator-VM on page 13

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 environment supported:

- Microsoft Hyper-V Server 2010 and 2016

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)				

Note: For information on the maximum number of configuration objects that can be added to the configuration database for different FortiAuthenticator virtual machine (VM) configurations, see the *FortiAuthenticator 6.4 Release Notes* on the Fortinet Docs Library.

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, your virtual machine manager must be installed and configured. The installation instructions for FortiAuthenticator-VM assume you are familiar with both VM platforms and their related terminology. FortiAuthenticator-VM includes support for:

- Microsoft Hyper-V 2010 and Hyper-V 2016

For the latest information on virtualization software support, see the corresponding *FortiAuthenticator Release Notes* on the Fortinet Docs Library.

Upgrade to the latest stable server update and patch release.

VM requirements

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.

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.

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. Go to the FortiCloud portal and create a new account or log in with an existing account.
2. In *Asset Management*, select *Register Product*, or click the *Register More* button.
3. Provide your registration code:
   a. Enter your product serial number, service contract registration code, or license certificate number.
   b. Choose your end user type as either a government or non-government user.
   c. Click *Next*.
4. Specify your registration information:
   a. If you have purchased a support contract for your product, enter the support contract.
   b. Enter a description to help identify the product.
   c. Enter the IP address of the FortiAuthenticator VM.
   d. Select a *Fortinet Partner*.
   e. Specify the asset group.
   f. Click *Next*.

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. The *Fortinet Product Registration Agreement* page displays. Select the check box to indicate that you have read, understood, and accepted the service contract. Click *Next*.
6. The *Verification* page displays. Select the checkbox to indicate that you accept the terms. Click *Confirm*. Registration is now complete and your registration summary is displayed.
7. On the *Registration Complete* page, download the license file (`.lic`) to your computer. You will upload this license to activate the FortiAuthenticator VM.

To edit the FortiAuthenticator-VM IP address:

1. In *Asset Management*, go to *Product List*.
   The *View Products* page opens.
2. Select the FortiAuthenticator-VM serial number.
3. In the *Product Information* pane, Select *Edit* to change the description, partner information, and IP address of your FortiAuthenticator-VM.
   The *Edit Product Information* page opens.

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.

- FAC_VM-vxxx-build0xxx-FORTINET.out.hyperv.zip

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:

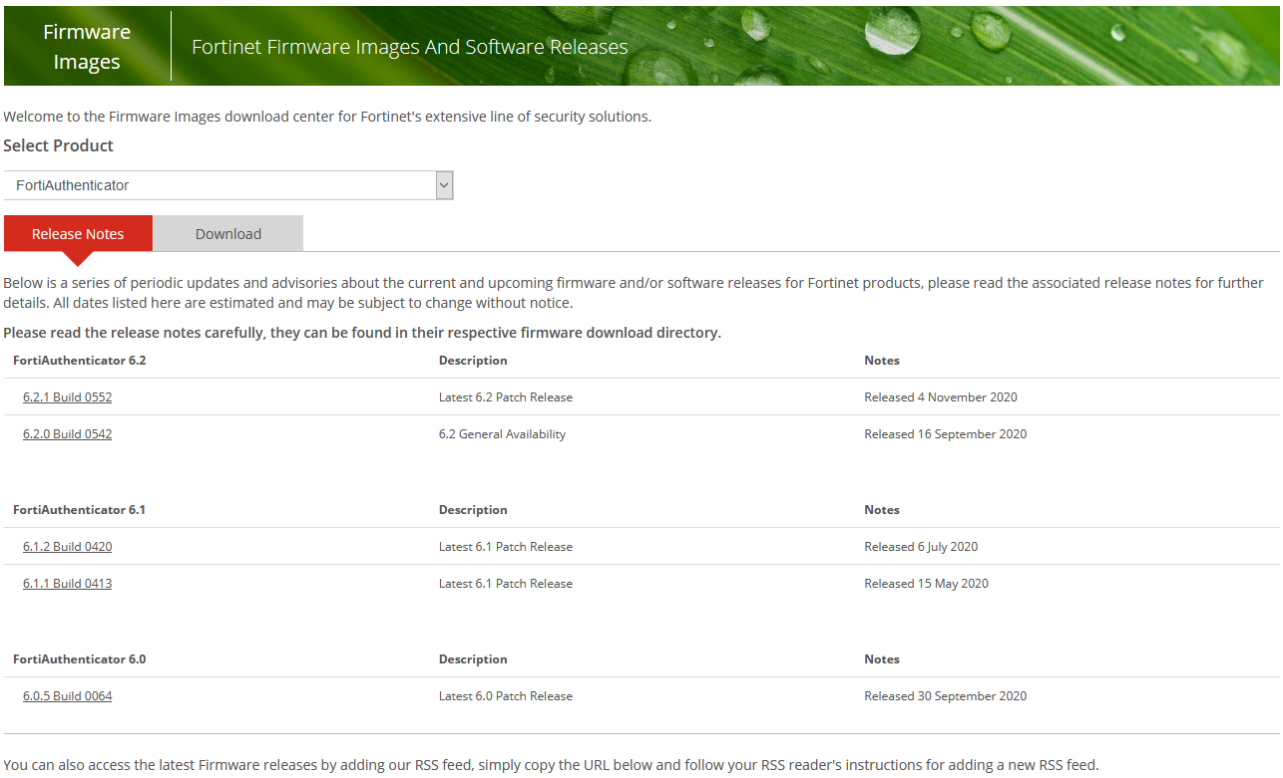
- **Snapshots folder**:
  - Optionally, Hyper-V stores snapshots of the FortiAuthenticator-VM state here.
- **Virtual Hard Disks folder**:
  - DATADRIVE.vhd: The FortiAuthenticator-VM log disk in VHD format.
  - fac.vhd: The FortiAuthenticator-VM system hard disk in VHD format.
- **Virtual Machines folder**: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

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.

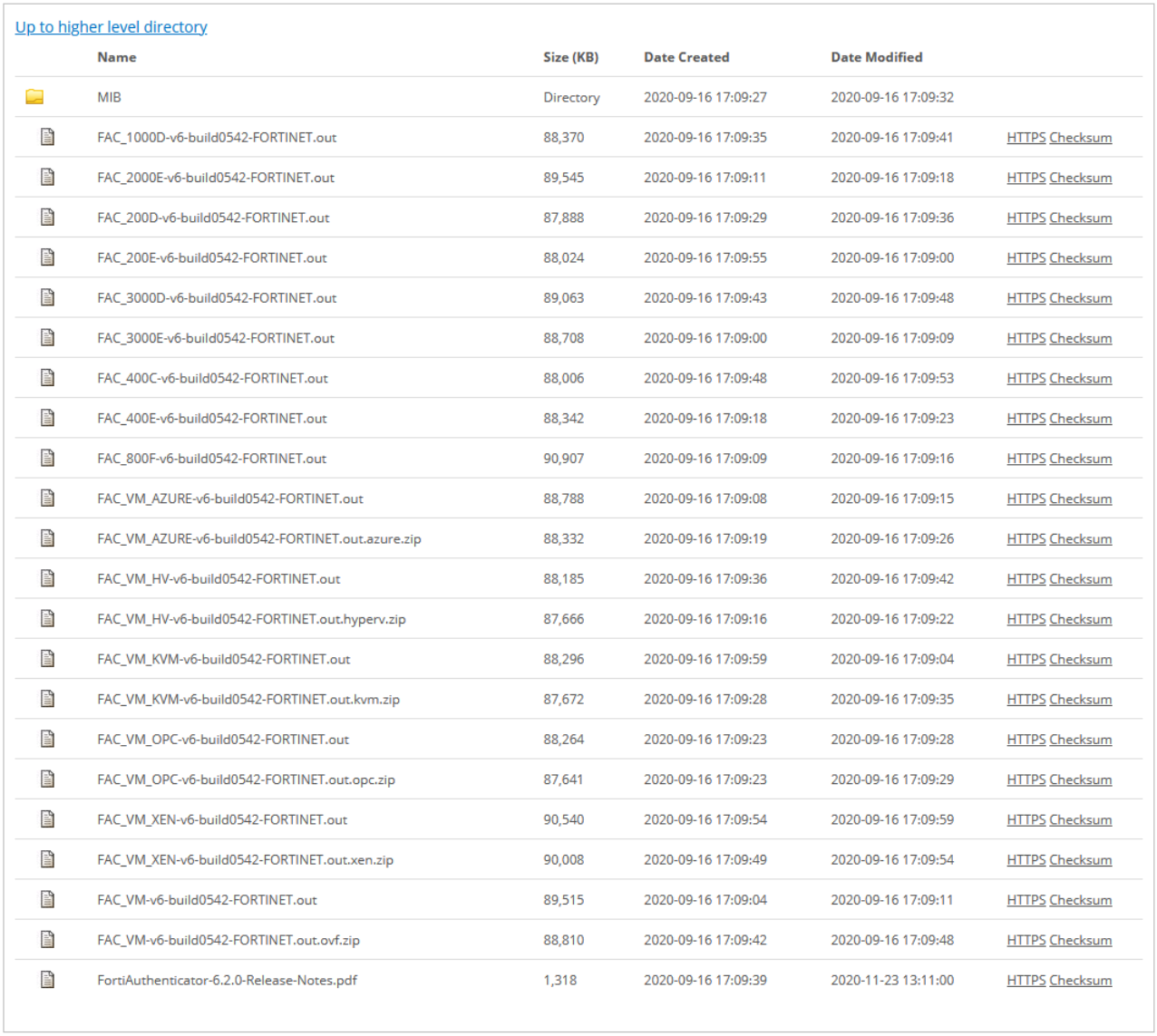
You can download the FortiAuthenticator Release Notes available on the Fortinet web site.

To download the FortiAuthenticator-VM .zip package:

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



2. In the *Firmware Images* page, select **FortiAuthenticator**.
3. On the *Download* tab, 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	
MIB	Directory	2020-09-16 17:09:27	2020-09-16 17:09:32	
FAC_1000D-v6-build0542-FORTINET.out	88,370	2020-09-16 17:09:35	2020-09-16 17:09:41	HTTPS Checksum
FAC_2000E-v6-build0542-FORTINET.out	89,545	2020-09-16 17:09:11	2020-09-16 17:09:18	HTTPS Checksum
FAC_200D-v6-build0542-FORTINET.out	87,888	2020-09-16 17:09:29	2020-09-16 17:09:36	HTTPS Checksum
FAC_200E-v6-build0542-FORTINET.out	88,024	2020-09-16 17:09:55	2020-09-16 17:09:00	HTTPS Checksum
FAC_3000D-v6-build0542-FORTINET.out	89,063	2020-09-16 17:09:43	2020-09-16 17:09:48	HTTPS Checksum
FAC_3000E-v6-build0542-FORTINET.out	88,708	2020-09-16 17:09:00	2020-09-16 17:09:09	HTTPS Checksum
FAC_400C-v6-build0542-FORTINET.out	88,006	2020-09-16 17:09:48	2020-09-16 17:09:53	HTTPS Checksum
FAC_400E-v6-build0542-FORTINET.out	88,342	2020-09-16 17:09:18	2020-09-16 17:09:23	HTTPS Checksum
FAC_800F-v6-build0542-FORTINET.out	90,907	2020-09-16 17:09:09	2020-09-16 17:09:16	HTTPS Checksum
FAC_VM_AZURE-v6-build0542-FORTINET.out	88,788	2020-09-16 17:09:08	2020-09-16 17:09:15	HTTPS Checksum
FAC_VM_AZURE-v6-build0542-FORTINET.out.azure.zip	88,332	2020-09-16 17:09:19	2020-09-16 17:09:26	HTTPS Checksum
FAC_VM_HV-v6-build0542-FORTINET.out	88,185	2020-09-16 17:09:36	2020-09-16 17:09:42	HTTPS Checksum
FAC_VM_HV-v6-build0542-FORTINET.out.hyperv.zip	87,666	2020-09-16 17:09:16	2020-09-16 17:09:22	HTTPS Checksum
FAC_VM_KVM-v6-build0542-FORTINET.out	88,296	2020-09-16 17:09:59	2020-09-16 17:09:04	HTTPS Checksum
FAC_VM_KVM-v6-build0542-FORTINET.out.kvm.zip	87,672	2020-09-16 17:09:28	2020-09-16 17:09:35	HTTPS Checksum
FAC_VM_OPC-v6-build0542-FORTINET.out	88,264	2020-09-16 17:09:23	2020-09-16 17:09:28	HTTPS Checksum
FAC_VM_OPC-v6-build0542-FORTINET.out.opc.zip	87,641	2020-09-16 17:09:23	2020-09-16 17:09:29	HTTPS Checksum
FAC_VM_XEN-v6-build0542-FORTINET.out	90,540	2020-09-16 17:09:54	2020-09-16 17:09:59	HTTPS Checksum
FAC_VM_XEN-v6-build0542-FORTINET.out.xen.zip	90,008	2020-09-16 17:09:49	2020-09-16 17:09:54	HTTPS Checksum
FAC_VM-v6-build0542-FORTINET.out	89,515	2020-09-16 17:09:04	2020-09-16 17:09:11	HTTPS Checksum
FAC_VM-v6-build0542-FORTINET.out.ovf.zip	88,810	2020-09-16 17:09:42	2020-09-16 17:09:48	HTTPS Checksum
FortiAuthenticator-6.2.0-Release-Notes.pdf	1,318	2020-09-16 17:09:39	2020-11-23 13:11:00	HTTPS Checksum

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

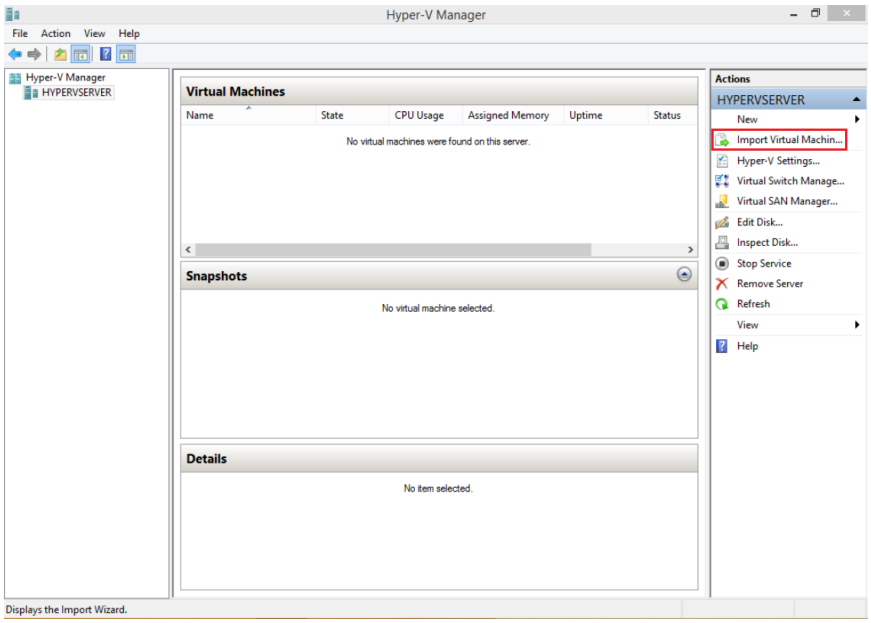
- Deploying FortiAuthenticator-VM on MS Hyper-V
- Power on your FortiAuthenticator-VM

Deploying FortiAuthenticator-VM on MS Hyper-V

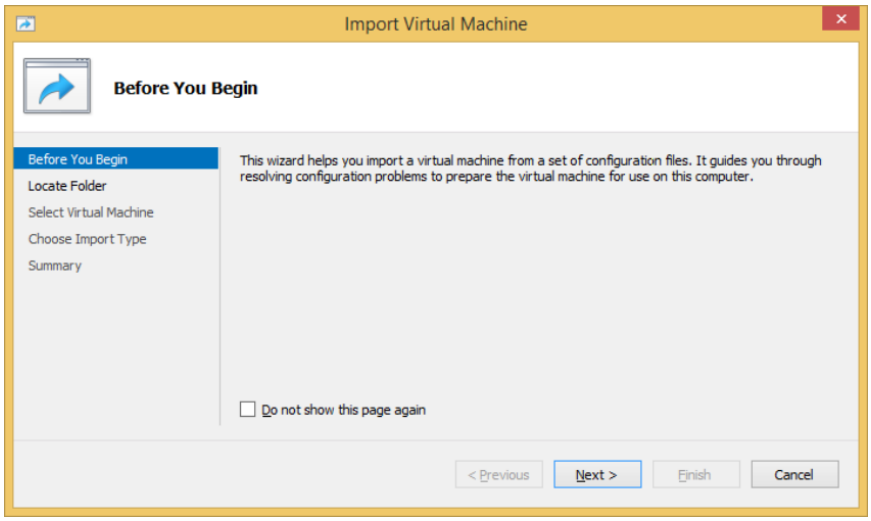
Once you have downloaded the `out.hyperv.zip` file and extracted the package contents to a folder on your management computer, you can deploy the VHD package to your MS Hyper-V environment.

To deploy the FortiAuthenticator VHD template:

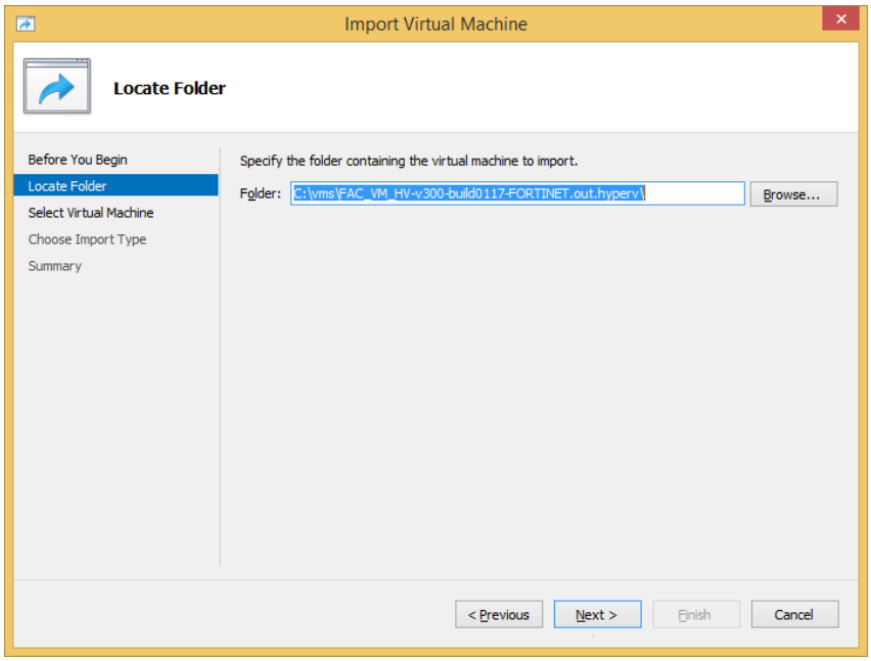
1. As an administrator, launch the Hyper-V Manager and connect to your Hyper-V Server.
2. Select the server in the right-hand menu and select *Import Virtual Machine*.



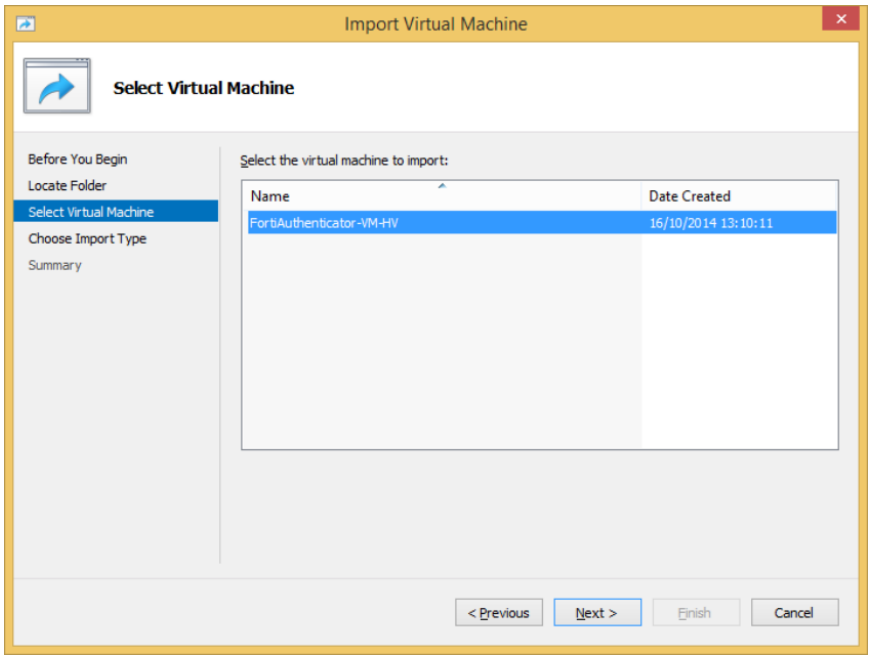
The *Import Virtual Machine* page opens. Select *Next* to begin the VM Import process.



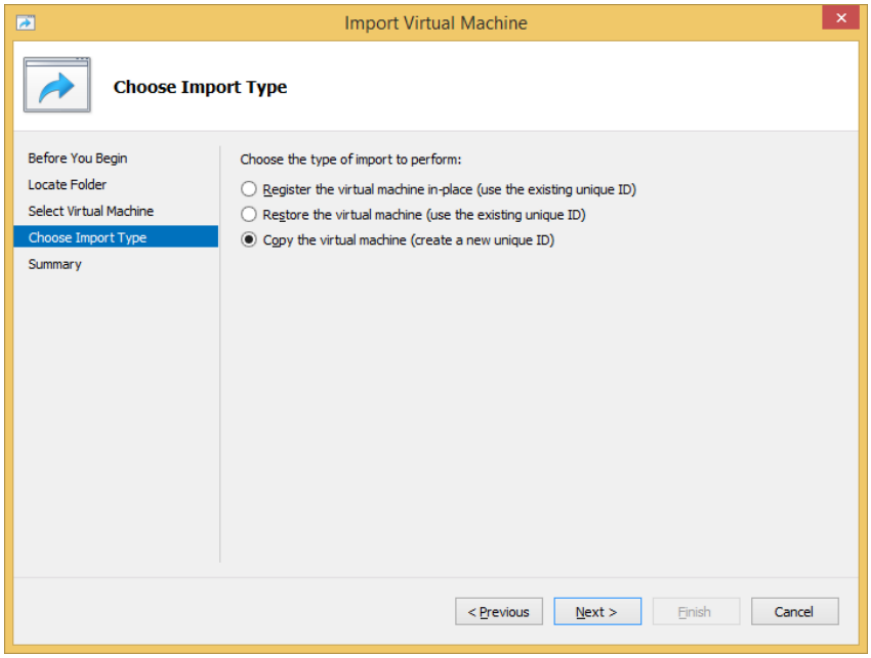
3. Enter the location of the VM to be imported. This is the location of the folder that you extracted the FortiAuthenticator `hyperv.zip` file to.



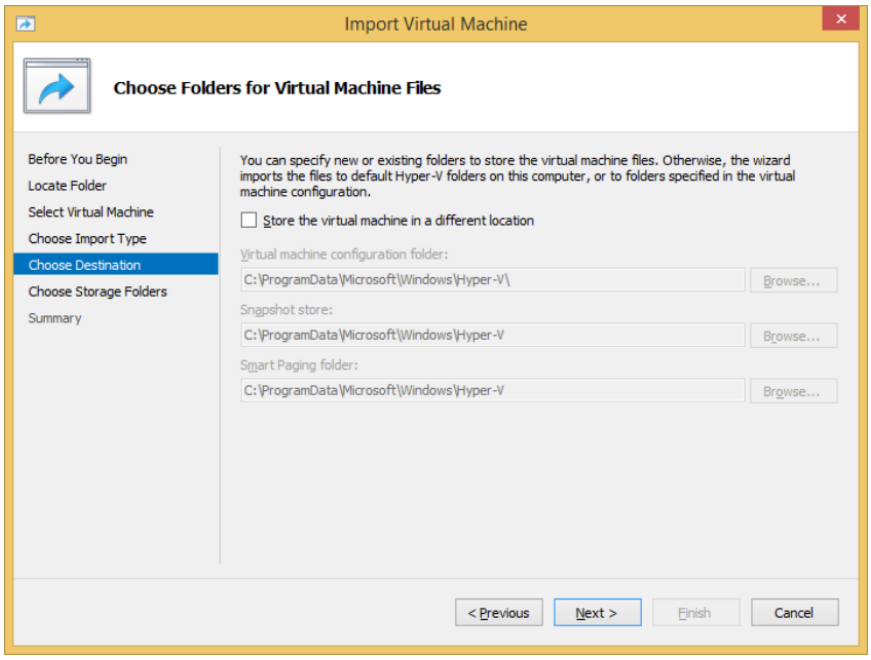
4. Select the FortiAuthenticator-VM and select *Next*.



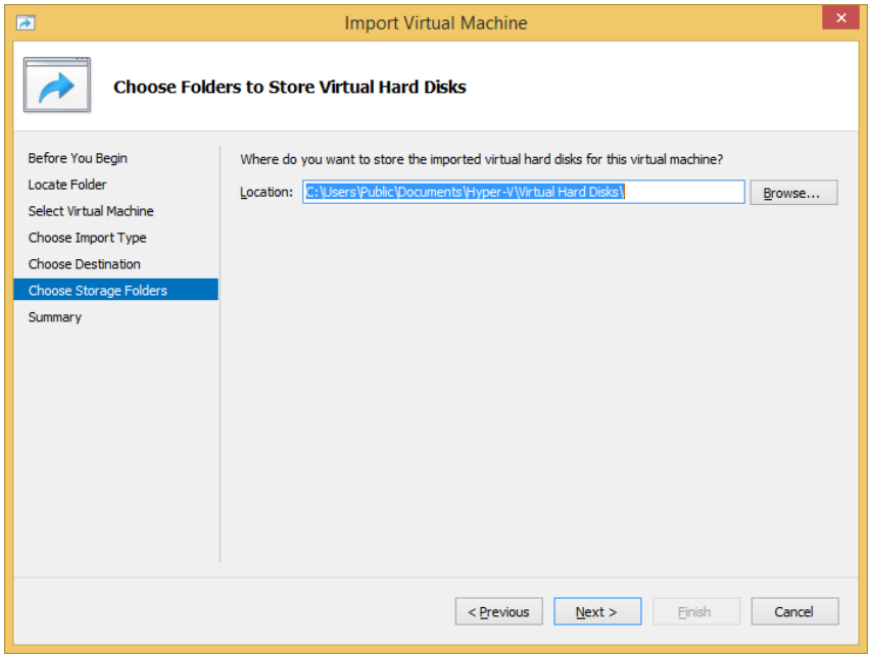
5. For the import type, choose *Copy the virtual machine* and select *Next*.



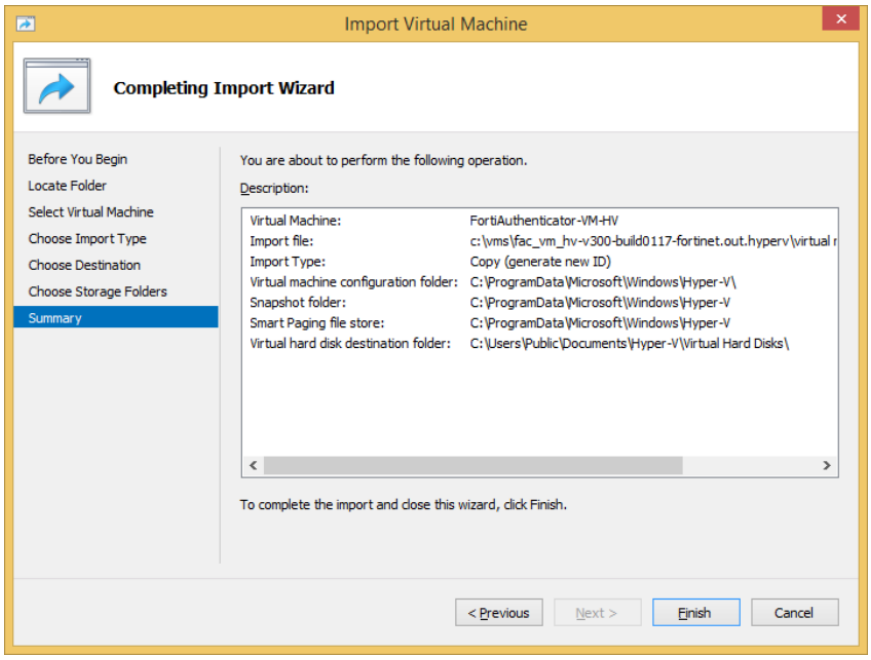
6. Select *Next* if you wish to use the default storage location settings, or specify your own.



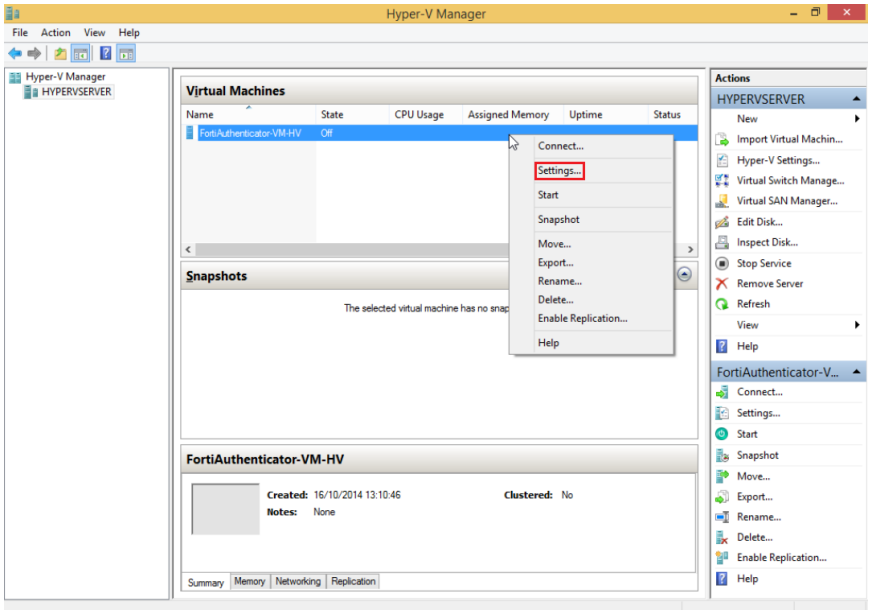
7. Select *Next* if you wish to use the default VM hard disk storage settings, or specify your own.



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



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...*.



Power on your FortiAuthenticator-VM

You can now power on your FortiAuthenticator-VM.

Initial Configuration

Before you can connect to the FortiAuthenticator-VM GUI you must configure basic network settings via the console in your 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 20
- Connect to the FortiAuthenticator-VM GUI on page 21
- Upload the FortiAuthenticator-VM license file on page 21
- Configure your FortiAuthenticator-VM on page 23

FortiAuthenticator-VM console access

To enable GUI access to the FortiAuthenticator-VM you must configure basic network settings of the FortiAuthenticator-VM in the client console.

To configure basic network settings in FortiAuthenticator-VM:

1. Power on your virtual machine, and enter the VM *Console*.
2. At the FortiAuthenticator-VM login prompt enter the username `admin` and password.
   The default password is no password. You will be prompted to create a new password.
3. 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-gui https-api ssh
   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

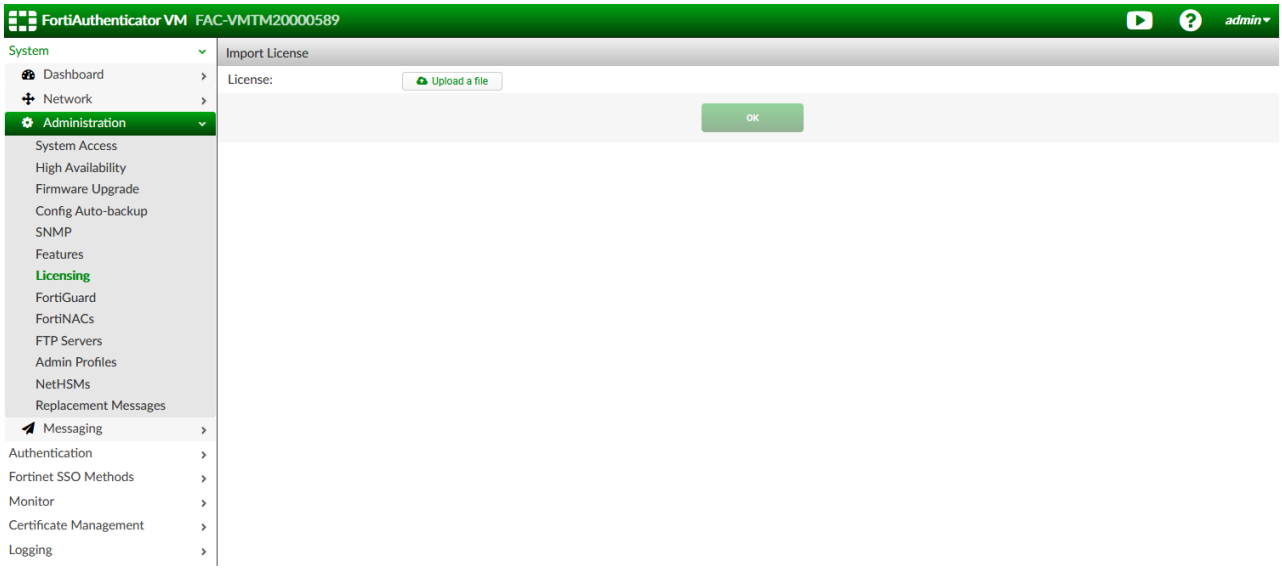
Every FortiAuthenticator-VM includes a five-user evaluation license. During this time the FortiAuthenticator-VM operates in evaluation mode. Before using the FortiAuthenticator-VM you must enter the license file that you downloaded from FortiCloud upon registration.

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:

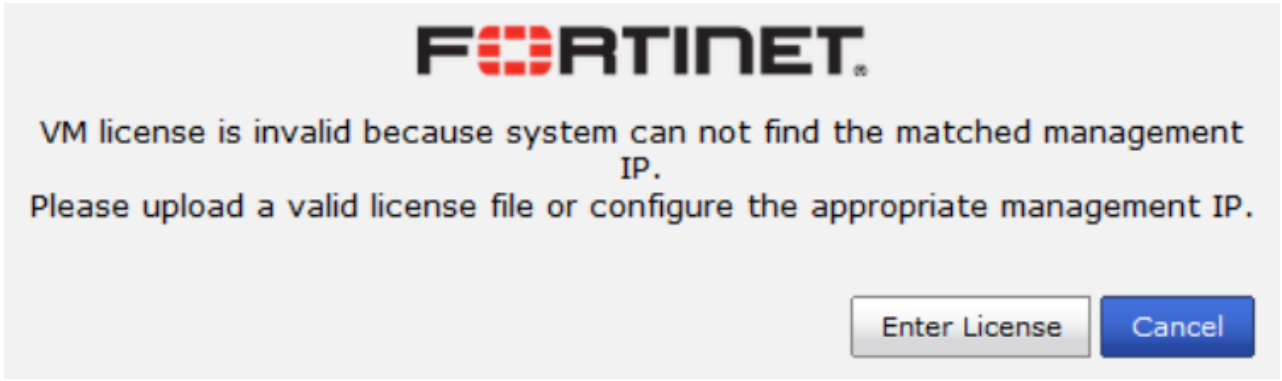
1. Log into the FortiAuthenticator-VM.
2. Go to *System* > *Administration* > *Licensing*.
   The *Import License* page opens.



3. Select *Upload a 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.



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.

www.fortinet.com

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.