



FortiAuthenticator - Azure Deployment Guide

Version 6.1.0

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/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



March 28, 2020

FortiAuthenticator 6.1.0 Azure Deployment Guide

23-610-621025-20200328

TABLE OF CONTENTS

Change log	4
About FortiAuthenticator on Azure	5
Overview	5
Azure instance type support	5
Licensing	6
Deploying FortiAuthenticator on Azure	8
Creating a FortiAuthenticator-VM	8
Connecting to FortiAuthenticator	13
Installing a valid license	14
Registering and downloading your license	14
Upload the license file to FortiAuthenticator-VM	15
Upgrading FortiAuthenticator firmware	15

Change log

Date	Change Description
2020-03-28	Initial release.

About FortiAuthenticator on Azure

Overview

FortiAuthenticator is designed specifically to provide authentication services for firewalls, SSL and IPsec VPNs, wireless access points, switches, routers, and servers. FortiAuthenticator includes Remote Authentication Dial-In User Service (RADIUS) and Lightweight Directory Access Protocol (LDAPv3) server authentication methods, and Security Assertion Markup Language (SAML), which is used for exchanging authentication and authorization data between an Identity Provider (IdP) and a Service Provider (SP). Authentication servers are an important part of an enterprise network, controlling access to protected network assets, and tracking user activity to comply with security policies.

FortiAuthenticator is not a firewall; it requires either a FortiGate-VM "virtual" or FortiGate "hardware" appliance to provide firewall-related services. Multiple FortiGate appliances 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 Fortinet Single Sign-On (FSSO) Agent on a Windows Active Directory (AD) network.

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

Azure instance type support

It is recommended to deploy FortiAuthenticator-VM on an Azure instance type with a minimum of 2 vCPUs, and a memory size of 8 GB or larger. This is because FortiAuthenticator-VM requires that at least two data disks are configured, including one primary data disk for the image and a secondary disk for user data. When selecting an instance type for your deployment, consider your use case for FortiAuthenticator and the requirements to support it.

For up-to-date information on each instance type, see [Sizes for Linux virtual machines in Azure](#).

The following table provides information on general purpose instance types:

Instance type	vCPU	Max NIC	FortiAuthenticator-VM license
B-series			
Standard_B2ms	2	3	FAC-VM-100-UG or FAC-VM-1000-UG
Standard_B4ms	4	4	FAC-VM-100-UG, FAC-VM-1000-UG or FAC-VM-10000-UG

Instance type	vCPU	Max NIC	FortiAuthenticator-VM license
Standard_B8ms	8	4	FAC-VM-10000-UG or FAC-VM-100000-UG
Standard_B12ms	12	6	FAC-VM-100000-UG
Dsv3-series			
Standard_D2s_v3	2	2	FAC-VM-100-UG or FAC-VM-1000-UG
Standard_D4s_v3	4	2	FAC-VM-1000-UG or FAC-VM-10000-UG
Standard_D8s_v3	8	4	FAC-VM-10000-UG or FAC-VM-100000-UG
Standard_D16s_v3	16	8	FAC-VM-100000-UG
Standard_D32s_v3	32	8	FAC-VM-100000-UG
Dv3-series			
Standard_D2_v3	2	2	FAC-VM-100-UG or FAC-VM-1000-UG
Standard_D4_v3	4	2	FAC-VM-1000-UG or FAC-VM-10000-UG
Standard_D8_v3	8	4	FAC-VM-10000-UG or FAC-VM-100000-UG
Standard_D16_v3	16	8	FAC-VM-100000-UG
Standard_D32_v3	32	8	FAC-VM-100000-UG
Dv2-series			
Standard_D3_v2	4	4	FAC-VM-1000-UG or FAC-VM-10000-UG
Standard_D4_v2	8	8	FAC-VM-10000-UG or FAC-VM-100000-UG
Standard_D5_v2	16	8	FAC-VM-100000-UG
Av2-series			
Standard_A2_v2	2	2	FAC-VM-100-UG
Standard_A4_v2	4	4	FAC-VM-100-UG or FAC-VM-1000-UG
Standard_A2m_v2	2	2	FAC-VM-100-UG or FAC-VM-1000-UG
Standard_A4m_v2	4	4	FAC-VM-10000-UG or FAC-VM-100000-UG
Standard_A8m_v2	8	8	FAC-VM-100000-UG

Licensing

FortiAuthenticator for Azure supports the bring your own license (BYOL) model.

Licenses can be obtained through any Fortinet partner. If you don't have a reseller partner, you can find a local Fortinet reseller partner by visiting the [Find a Partner](#) portal and performing a search in the following regions:

- Asia Pacific, Australia, and New Zealand
- EMEA (Europe, Middle East, and Africa)
- Latin America and Caribbean
- North America
- North America: US Federal

You can also contact azuresales@fortinet.com for assistance in purchasing a license.

This license model is stackable, allowing you to expand your VM solution as your environment expands. For additional information on the FortiAuthenticator stackable license model, see the [FortiAuthenticator datasheet](#).

Deploying FortiAuthenticator on Azure

Creating a FortiAuthenticator-VM

This section details how to create and launch a FortiAuthenticator-VM from Azure Marketplace.

Locate Fortinet FortiAuthenticator ID Access Management in the Microsoft Azure Marketplace:

1. From the [Microsoft Azure Portal](#), click **Create a resource**.
2. In the search field, search for `FortiAuthenticator` and select **Fortinet FortiAuthenticator ID Access Management**.
3. Under **Fortinet FortiAuthenticator ID Access Management**, click **Create**.

Configure the basics:

1. In the **Basics** tab, under **Project details**, configure the following settings:
 - a. For **Subscription**, confirm that you have selected a valid subscription from the dropdown menu.
 - b. For **Resource group**, select **Create new** to create a new resource group.



Selecting an existing resource group will often cause the deployment to fail due to the fact that Azure does not allow deployment of resources into existing resource groups that are not empty.

2. Under **Instance details**, configure the following settings:
 - a. For **Virtual machine name**, provide a name for your FortiAuthenticator-VM instance.
 - b. For **Region**, select a region.
 - c. For **Availability options**, select an option applicable to your use case.
 - d. For **Image**, ensure that **FortiAuthenticator VM (BYOL)** is selected.
 - e. For **Size**, select an instance type that is capable of supporting your use case for FortiAuthenticator.

For recommended instance types, see [Azure instance type support on page 5](#)

Create a virtual machine

[Basics](#) [Disks](#) [Networking](#) [Management](#) [Advanced](#) [Tags](#) [Review + create](#)

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Looking for classic VMs? [Create VM from Azure Marketplace](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

* Subscription ? ▼

* Resource group ? ▼
[Create new](#)

Instance details

* Virtual machine name ? ✓

* Region ? ▼

Availability options ? ▼

* Image ? ▼
[Browse all public and private images](#)

* Size ? **Standard B2ms**
 2 vcpus, 8 GiB memory
[Change size](#)

3. Under **Administrator account**, configure the following settings:
 - a. For **Authentication type**, select whether the administrator will use a password or an SSH key for authentication.
 - b. For **Username**, type an administrator username for the VM.
 - c. If Password is selected for Authentication type, in the **Password** and **Confirm Password** fields, type a password for the administrator.
 Note: The username and password will be used to log into FortiAuthenticator-VM after it is deployed.

Administrator account

Authentication type ? Password SSH public key

* Username ? ✓


* Password ? ✓



* Confirm password ? ✓



[Review + create](#) [< Previous](#) [Next : Disks >](#)

- d. If SSH public key is selected for Authentication type, in the **SSH public key** field, provide an RSA public key in the single-line format or the multi-line PEM format. For information on generating an RSA public key, see [Create and use an SSH public-private key pair for Linux VMs in Azure](#).

Administrator account

Authentication type  Password SSH public key

* Username  

* SSH public key  

[Review + create](#) [< Previous](#) [Next : Disks >](#)

Attach an additional disk:

1. Click **Next : Disks**.
2. Under **Disk options**, for **OS disk type**, select a disk type. For logging, an additional disk is needed.
3. Under **Data disks**, click **Create and attach a new disk**.
4. Under **Create a new disk**, configure the following:
 - a. For **Name**, specify a name for the new disk.
 - b. For **Source type**, ensure that **None (empty disk)** is selected.
 - c. For **Size**, select a disk size that supports your usage patterns. For storage guidelines based on user count, see FortiAuthenticator-VM sizing guidelines in the [Release Notes](#).
- d. Click **OK**.
The new disk is added to the virtual machine.

Create a virtual machine

Basics **Disks** Networking Management Advanced Tags Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

Disk options

* OS disk type

Enable Ultra Disk compatibility (Preview) Yes No
Ultra Disk compatibility is not available for this VM size and location.

Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	NAME	SIZE (GIB)	DISK TYPE	HOST CACHING
0	Pre-defined by the selected image			None
<input type="text" value="1"/>	FortiAuthenticatorVM_DataDisk_1	1023	Premium SSD	None

[Create and attach a new disk](#) [Attach an existing disk](#)

Advanced

[Review + create](#) [< Previous](#) [Next : Networking >](#)

Define network connectivity for your virtual machine:

1. Click **Next : Networking**.
2. Under **Network interface**, configuring the following:
 - a. For **Virtual network**, select the default or create a new virtual network.
 - b. For **Subnet**, select an available subnet.
 - c. For **Public IP**, select the default.
 - d. For **Configure network security group**, either select an existing network security group from the dropdown menu, or create a new network security group.

Create a virtual machine

Basics
Disks
Networking
Management
Advanced
Tags
Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

* Virtual network ? (new) FortiAuthenticator-group-vnet ▼
Create new

* Subnet ? (new) default (172.17.10.0/24) ▼

Public IP ? (new) FortiAuthenticatorVM-ip ▼
Create new

NIC network security group ?
 None
 Basic
 Advanced

i This VM image has preconfigured NSG rules

* Configure network security group ? (new) FortiAuthenticatorVM-nsg ▼
Create new

Accelerated networking ?
 On
 Off

The selected image does not support accelerated networking.

Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Place this virtual machine behind an existing load balancing solution?
 Yes
 No

Review + create

< Previous

Next : Management >

Configuring management options:

1. Click **Next : Management**.
2. Configure monitoring and management options for your VM as needed.

Configuring advanced options:

1. Click **Next : Advanced**.
2. Configure additional configurations, agents, scripts, or applications as needed.

Add tags:

1. Click **Next : Tags**.
2. If needed, add any tags to help you categorize your FortiAuthenticator-VM instance.

Review and create your VM:

1. Click **Next : Review + Create**.
2. Review the terms and details of your configuration.
3. Click **Create**.

Deployment of the FortiAuthenticator-VM begins. The deployment process takes an average of 10 minutes to complete, but may vary. When the deployment process is finished and the FortiAuthenticator-VM is provisioned and powered up, access the FortiAuthenticator-VM to complete the post-deployment setup. See [Connecting to FortiAuthenticator on page 13](#).

Connecting to FortiAuthenticator

To connect to the FortiAuthenticator-VM, you require the public IP address of the virtual machine, and administrator credentials set when creating the FortiAuthenticator-VM.

Locate the FortiAuthenticator-VM public IP address:

1. From the [Microsoft Azure Portal](#), click **Virtual machines**.
2. Locate and select your FortiAuthenticator-VM from the list of the virtual machines.
3. Take note of the public IP address of the virtual machine.

The screenshot shows the Azure Portal interface for a virtual machine named 'FortiAuthenticatorVM'. The left sidebar contains navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Networking, and Disks. The main area displays the VM's status as 'Running' and provides various configuration details. The 'Public IP address' field is highlighted with a red box, showing a value of '172.17.10.4'. Other details include Resource group (FortiAuthenticator-group), Location (East US 2), Subscription (PAYG-DevOps), and Subscription ID (4f27b38c-ad3f-43d8-a9a3-01182e5e2f9a).

You can also obtain the public IP through the Azure CLI using the CLI command: `az vm list-ip-addresses -g <RESOURCE GROUP> -n <VM NAME>`

For example:

```
{contoso}5279: az vm list-ip-addresses -g CTSOFACRG -n "CTSOFACVM"
--output yaml
- virtualMachine:
  name: CTSOFACVM
  network:
    privateIpAddresses:
      - 172.16.208.4
    publicIpAddresses:
```

```
- id:
/subscriptions/2d36c33d-fcb2-4634-bc26-
65bb54358e0c/resourceGroups/CTSOFACRG/providers/Microsoft.Network/publicIPAddresses/
CTSOFACVM-ip
  ipAddress: 23.97.203.47 <-- Public IP Address
  ipAllocationMethod: Dynamic
  name: CTSOFACVM-ip
  resourceGroup: CTSOFACRG
resourceGroup: CTSOFACRG
```

Connect to the FortiAuthenticator UI:

1. In a web browser, navigate to `https://<public_IP>`.
2. When you connect, your web browser might display a security warning related to the certificate not being trusted. This warning is normal and is due to the certificate being self-signed, rather than being signed by a valid certificate authority. Verify and accept the certificate, either permanently or temporarily, and proceed to `https://<public_IP>`.
3. On the **Login** page, enter the username and password you set when you creating the FortiAuthenticator-VM.
4. Click **Login**.
The FortiAuthenticator Dashboard displays.

Installing a valid license

FortiAuthenticator-VM runs in evaluation mode until it is licensed. Before using the FortiAuthenticator-VM you must enter the license file that you download from the Fortinet Support portal upon registration.

Registering and downloading your license

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 Fortinet Support.

Upon registration, download the license file. You will need this file to activate your FortiAuthenticator-VM. You can configure basic network settings from the CLI to complete the deployment. Once the license file is uploaded, the CLI and UI are fully functional.

1. Navigate to the [Fortinet Support](#) portal and create a new account or log in with an existing account.
2. In the toolbar, click **Asset > Register/Renew** to start the registration process.
3. In the **Specify Registration Code** field, enter your license activation code and click **Next** to continue registering the product.
4. Enter the **Support Contract number**, **Product Description**, **Fortinet Partner**, and **IP address**.
As a part of the license validation process, the IP address of the FortiAuthenticator-VM instance is compared to the IP information in the license file. If a new license has been imported or the 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. Click **Next**.
The Fortinet Product Registration Agreement page displays.

6. Select the check box to indicate that you have read, understood, and accepted the service contract, and click **Next**.
The Verification page displays.
7. Select the checkbox to indicate that you accept the terms, and click **Confirm**.
8. On the **Registration Complete** page, download the license file (.lic) to your computer. You will upload this license to activate the FortiAuthenticator-VM.

Note: After registering a license, Fortinet servers can take up to 30 minutes to fully recognize the new license. When you upload the license file to activate the FortiAuthenticator-VM, if you get an error that the license is invalid, wait 30 minutes and try again.

Upload the license file to FortiAuthenticator-VM

1. Log into the FortiAuthenticator-VM from a browser.
2. Navigate to **System > Administration > Licensing**.
3. Click **Choose File** and locate the license file (.lic) on your computer. Click **OK** to upload the license file.

The VM registration status appears as valid after the license has been validated.

As a part of the license validation process, the IP address of the FortiAuthenticator-VM instance is compared to the IP information in the license file. If a new license has been imported or the 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.

Upgrading FortiAuthenticator firmware

The FortiAuthenticator image available on Azure Marketplace might not include the latest firmware available for FortiAuthenticator. Upgrade the firmware of your FortiAuthenticator-VM after deployment to ensure that you have the latest features, functionality, and fixes available.

Before performing an upgrade, it is recommended that you complete the following steps:

- Backup the system configuration. Full configuration backup is available from the FortiAuthenticator GUI or CLI. See the [FortiAuthenticator Admin Guide](#).
- Have a copy of the old FortiAuthenticator-VM firmware available.
- Review the [Release Notes](#), including the upgrade path and bug information.
- Ensure that you have the time required to complete the upgrade.

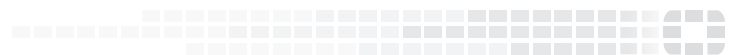
To upgrade your FortiAuthenticator-VM firmware:

1. Log into the [Fortinet Support](#) site and download the latest firmware to your local computer.
2. Log into the FortiAuthenticator-VM from a browser.
3. Navigate to **System > Administration > Firmware Upgrade**.
4. Click **Choose File**, locate the firmware image on your local computer, and click **Open**.
5. Click **OK**.

The firmware image uploads from your local computer to the FortiAuthenticator-VM, which will then reboot. For a short period of time during this reboot, the FortiAuthenticator-VM is offline and unavailable for authentication.



FORTINET[®]



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.