



# FortiOS - Azure Administration Guide

Version 6.4

**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](mailto:techdoc@fortinet.com)



August 25, 2021

FortiOS 6.4 Azure Administration Guide

01-640-615183-20210825

# TABLE OF CONTENTS

<b>About FortiGate-VM for Azure</b>	<b>6</b>
Instance type support	6
Region support	8
Models	10
Licensing	11
Order types	11
Creating a support account	12
Verifying the license type	13
Migrating a FortiGate-VM instance between license types	14
Obtaining a FortiCare-generated license for Azure on-demand instances	15
<b>Deploying FortiGate-VM on Azure</b>	<b>18</b>
Azure services and components	18
Deploying FortiGate-VM from a VHD image file	19
Deploying FortiGate with a custom ARM template	19
Invoking a custom ARM template	20
Bootstrapping the FortiGate CLI at initial bootup using user data	25
Bootstrapping the FortiGate CLI and BYOL license at initial bootup using user data	26
Deploying FortiGate-VM using Azure PowerShell	30
Running PowerShell to deploy FortiGate-VM	30
Bootstrapping the FortiGate CLI and BYOL license at initial bootup using user data	35
Deploying FortiGate-VM from the marketplace	37
Deploying FortiGate-VM on regional Azure clouds	39
Enabling accelerated networking on the FortiGate-VM	39
Upgrading FortiOS	41
<b>Deploying autoscaling on Azure</b>	<b>42</b>
Prerequisites	43
Before you begin	43
Requirements when using an existing VNet	44
Obtaining the deployment package	44
Deploying FortiGate Autoscale for Azure	45
Creating a template deployment	45
Configurable variables	49
Uploading files to the Storage account	55
Verifying the deployment	57
Security features for network communication	61
Starting a VMSS	65
Connecting to the FortiGate-VM instances	68
Troubleshooting	70
Determining the FortiGate Autoscale release version	70
Election of the primary FortiGate was not successful	70
Locating deployment Outputs	70
Redeploying with an existing VNet fails	71
Resetting the elected primary FortiGate	72
Stack has stopped working	72

Troubleshooting using Application Insights .....	72
Troubleshooting using environment variables .....	72
<b>Appendix .....</b>	<b>74</b>
FortiGate Autoscale for Azure features .....	74
Cloud-init .....	77
Architectural diagrams .....	77
Upgrading the deployment .....	83
Document history .....	93
<b>Single FortiGate-VM deployment .....</b>	<b>94</b>
Registering and downloading your license .....	94
Deploying the FortiGate-VM .....	95
Connecting to the FortiGate-VM .....	97
Azure routing and network interfaces .....	97
Using public IP addresses .....	98
<b>HA for FortiGate-VM on Azure .....</b>	<b>105</b>
Building blocks .....	105
Architecture .....	109
Subscribing to the FortiGate-VM .....	110
<b>SDN connector integration with Azure .....</b>	<b>111</b>
Configuring an SDN connector in Azure .....	111
Azure SDN connector service principal configuration requirements .....	111
Configuring an SDN connector using a managed identity .....	113
Azure portal .....	115
Configuring an Azure SDN connector for Azure resources .....	117
Azure SDN connector using ServiceTag and Region filter keys .....	119
Troubleshooting Azure SDN connector .....	121
SDN connector in Azure Kubernetes (AKS) .....	122
<b>SDN connector in Azure Stack .....</b>	<b>123</b>
<b>VPN for FortiGate-VM on Azure .....</b>	<b>126</b>
Connecting a local FortiGate to an Azure VNet VPN .....	126
Connecting a local FortiGate to an Azure FortiGate via site-to-site VPN .....	133
Configuring the local FortiGate .....	133
Configuring the Azure FortiGate .....	136
vWAN .....	140
vWAN architecture diagram .....	141
Creating the vWAN .....	142
Adding VNet connections to the vWAN hub .....	143
Deploying the vWAN ARM template .....	144
Completing the prerequisites .....	144
Uploading Remote_sites.txt to a storage account .....	145
Deploying the ARM template .....	146
Associating VPN sites with the vWAN hub .....	146
Verifying vWAN configuration .....	146
Configuring integration with Azure AD domain services for VPN .....	147
Configuring FortiClient VPN with multifactor authentication .....	151

---

<b>Azure AD acting as SAML IdP</b>	<b>156</b>
SAML SSO login for FortiOS administrators with Azure AD acting as SAML IdP	156
Configuring SAML SSO login for SSL VPN web mode with Azure AD acting as SAML IdP	156
<b>Azure Sentinel</b>	<b>161</b>
Sending FortiGate logs for analytics and queries	161
<b>Change log</b>	<b>162</b>

# About FortiGate-VM for Azure

By combining stateful inspection with a comprehensive suite of powerful security features, FortiGate Next Generation Firewall (NGFW) technology delivers complete content and network protection. This solution is available for deployment on Microsoft Azure.

In addition to advanced features such as an extreme threat database, vulnerability management, and flow-based inspection, features including application control, firewall, antivirus, IPS, web filter, and VPN work in concert to identify and mitigate the latest complex security threats.

FortiGate-VM for Azure supports active/passive high availability (HA) configuration with FortiGate-native unicast HA synchronization between the primary and secondary nodes. When the FortiGate-VM detects a failure, the passive firewall instance becomes active and uses Azure API calls to configure its interfaces/ports.

FortiGate-VM also supports active/active HA using Azure Load Balancer (LB).

Highlights of FortiGate-VM for Azure include the following:

- Delivers complete content and network protection by combining stateful inspection with a comprehensive suite of powerful security features.
- IPS technology protects against current and emerging network-level threats. In addition to signature-based threat detection, IPS performs anomaly-based detection, which alerts users to any traffic that matches attack behavior profiles.
- New Docker application control signatures protect your container environments from newly emerged security threats. See [FortiGate-VM on a Docker environment](#).

## Instance type support

FortiGate supports the following instance types on Azure.

Supported instances on the Azure marketplace listing may change without notice and may vary between bring your own license (BYOL) and pay as you go (PAYG). Instance types of the A- and D-series no longer appear as deployable instances at the time you install the FortiGate virtual machine (VM) on the marketplace launcher. FortiGate supports compute optimized instances (F-series, Fs-series, and Fsv2-series) and general purpose instances (Dv2-series, DSv2-series, Dv3-series, and DSv3-series).

For up-to-date information on each instance type, see the following links:

- [Sizes for Linux virtual machines in Azure](#)
- [Compute optimized virtual machine sizes](#)
- [General purpose virtual machine sizes](#)

The following table provides information on compute-optimized instance types:

Instance type	vCPU	Max NIC	FortiGate minimum order (BYOL)
F-series			

Instance type	vCPU	Max NIC	FortiGate minimum order (BYOL)
Standard_F1	1	2	FG-VM01 or FG-VM01v
Standard_F2	2	2	FG-VM02 or FG-VM02v
Standard_F4	4	4	FG-VM04 or FG-VM04v
Standard_F8	8	8	FG-VM08 or FG-VM08v
Standard_F16	16	8	FG-VM16 or FG-VM16v
<b>Fs-series</b>			
Standard_F1s	1	2	FG-VM01 or FG-VM01v
Standard_F2s	2	2	FG-VM02 or FG-VM02v
Standard_F4s	4	4	FG-VM04 or FG-VM04v
Standard_F8s	8	8	FG-VM08 or FG-VM08v
Standard_F16s	16	8	FG-VM16 or FG-VM16v
<b>Fsv2-series</b>			
Standard_F2s_v2	2	2	FG-VM02 or FG-VM02v
Standard_F4s_v2	4	2	FG-VM04 or FG-VM04v
Standard_F8s_v2	8	4	FG-VM08 or FG-VM08v
Standard_F16s_v2	16	4	FG-VM16 or FG-VM16v
Standard_F32s_v2	32	8	FG-VM32 or FG-VM32v

The following table provides information on general purpose instance types:

Instance type	vCPU	Max NIC	FortiGate minimum order (BYOL)
<b>Dv2-series</b>			
Standard_D1_v2	1	2	FG-VM01 or FG-VM01v
Standard_D2_v2	2	2	FG-VM02 or FG-VM02v
Standard_D3_v2	4	4	FG-VM04 or FG-VM04v
Standard_D4_v2	8	8	FG-VM08 or FG-VM08v
Standard_D5_v2	16	8	FG-VM16 or FG-VM16v
<b>Dv3-series</b>			
Standard_D2_v3	2	2	FG-VM02 or FG-VM02v
Standard_D4_v3	4	2	FG-VM04 or FG-VM04v
Standard_D8_v3	8	4	FG-VM08 or FG-VM08v

Instance type	vCPU	Max NIC	FortiGate minimum order (BYOL)
Standard_D16_v3	16	8	FG-VM16 or FG-VM16v
Standard_D32_v3	32	8	FG-VM32 or FG-VM32v
<b>DSv2-series</b>			
Standard_DS1_v2	1	2	FG-VM01 or FG-VM01v
Standard_DS2_v2	2	2	FG-VM02 or FG-VM02v
Standard_DS3_v2	4	4	FG-VM04 or FG-VM04v
Standard_DS4_v2	8	8	FG-VM08 or FG-VM08v
Standard_DS5_v2	16	8	FG-VM16 or FG-VM16v
<b>Dsv3-series</b>			
Standard_D2s_v3	2	2	FG-VM02 or FG-VM02v
Standard_D4s_v3	4	2	FG-VM04 or FG-VM04v
Standard_D8s_v3	8	4	FG-VM08 or FG-VM08v
Standard_D16s_v3	16	8	FG-VM16 or FG-VM16v
Standard_D32s_v3	32	8	FG-VM32 or FG-VM32v

FortiOS 6.4.3 and later versions support hot-adding vCPU and RAM. However, Azure may not support this. See [Resize a virtual machine using the Azure portal or PowerShell](#).

## Region support

Azure region support can mean one of the following:

- FortiGate-VM is available for purchase in a specific region.
- You can deploy FortiGate-VM on the data center located in the chosen region within the Azure portal. They are the “locations”.
- You can deploy FortiGate-VM on regional Azure, such as in China, Germany, and U.S. Gov. Each has its own URL domain.

FortiGate-VM is available for purchase in all regions where Azure is commercially available. See the [Azure pricing FAQ](#).

In terms of the location where you deploy FortiGate-VM, ensure that quota is available. Some limits, such as VM cores, exist at a regional level. See [Azure subscription and service limits, quotas, and constraints](#). You can also request that Microsoft increase VM cores if necessary, as explained at [Quota increase requests](#). Choose the instance types supported to deploy FortiGate-VM ([Instance type support on page 6](#)).

## Locations

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation bar includes 'Create a resource', 'All services', 'Dashboard', 'Resource groups', 'All resources', 'Recent', 'App Services', 'Virtual machines (classic)', 'Virtual machines', 'SQL databases', 'Cloud services (classic)', 'Subscriptions', and 'Azure Active Directory'. The main content area displays 'All resources' under 'azurestorefortinet (Default Directory)'. A search bar at the top says 'Search resources, services, and docs'. Below it, there are buttons for '+ Add', 'Edit columns', 'Refresh', 'Assign Tags', and 'Delete'. A message box states 'Subscription filtering behaviour has now changed. To learn more click here.' A 'Subscriptions' section shows 'All 2 selected' with a table of resources. To the right, a 'All locations' dropdown menu is open, listing various Azure regions with checkboxes. A secondary pane on the right lists 'SUBSCRIPTION' names and their corresponding regions.

NAME	TYPE	RESOURCE GROUP
ABays-Recovery-Vault	Recovery Services vault	ABays-UK-1
ad.twomblys.com	Azure AD Domain Services	DomainServicesWUS
adabsaisdiag625	Storage account	adabsais
adabsais-vnet	Virtual network	adabsais
ADJ-SEA-NET	Virtual network (classic)	Default-Networking
afaingdiag708	Storage account	afaing
afaing-vnet	Virtual network	afaing

LOCATION	SUBSCRIPTION
Select all	Fortinet Engineering
Australia East	Fortinet Engineering
Australia Southeast	Pay-As-You-Go
Brazil South	Pay-As-You-Go
Canada Central	Pay-As-You-Go
Canada East	Pay-As-You-Go
Central India	Pay-As-You-Go
Central US	Pay-As-You-Go
East Asia	Fortinet Engineering
East US	Pay-As-You-Go
East US 2	Pay-As-You-Go

## Azure regional quota for vCPU cores

The screenshot shows the Microsoft Azure portal interface. The left navigation bar is identical to the previous screenshot. The main content area shows 'Subscriptions > Fortinet Engineering - Usage + quotas'. A search bar at the top says 'quota'. Below it, a message says 'You can use each Microsoft Azure resource up to its quota. Each subscription has separate quotas and usage is tracked per subscription. If you reach a quota cap, you can request an increase via Help + Support. Learn more'. A 'Request Increase' button is visible. The main area displays a table of 'QUOTA' entries with columns for 'PROVIDER', 'LOCATION', and 'USAGE'. Each row shows the provider (Microsoft.Compute), location, and current usage percentage relative to the quota.

QUOTA	PROVIDER	LOCATION	USAGE
Standard F Family vCPUs	Microsoft.Compute	UK South	40 % 8 of 20
Standard FSv2 Family vCPUs	Microsoft.Compute	Australia Southeast	40 % 4 of 10
Standard FSv2 Family vCPUs	Microsoft.Compute	East US	40 % 4 of 10
Standard FS Family vCPUs	Microsoft.Compute	UK South	30 % 6 of 20
Standard F Family vCPUs	Microsoft.Compute	Central US	25 % 10 of 40
Standard FS Family vCPUs	Microsoft.Compute	Brazil South	20 % 2 of 10
Standard FS Family vCPUs	Microsoft.Compute	Canada East	20 % 2 of 10
Standard FS Family vCPUs	Microsoft.Compute	North Europe	20 % 2 of 10
Standard F Family vCPUs	Microsoft.Compute	West Europe	10 % 1 of 10

## Models

FortiGate-VM is available with different CPU and RAM sizes and you can deploy it on various private and public cloud platforms. The following table shows the models conventionally available to order, also known as BYOL models. See [Order types on page 11](#).

Model name	vCPU minimum	vCPU maximum
FG-VM01/01v/01s	1	1
FG-VM02/02v/02s	1	2
FG-VM04/04v/04s	1	4
FG-VM08/08v/08s	1	8
FG-VM16/16v/16s	1	16



The v-series and s-series do not support virtual domains (VDOMs) by default. To add VDOMs, you must separately purchase perpetual VDOM addition licenses. You can add and stack VDOMs up to the maximum supported number after initial deployment.

Generally, there are RAM size restrictions to FortiGate-VM BYOL licenses. However, these restrictions do not apply to Azure deployments. Any RAM size with certain CPU models are allowed. Licenses are based on the number of CPUs (the number of vCPU cores for Azure) only.

Previously, platform-specific models such as FortiGate-VM for Azure with an Azure-specific orderable menu existed. However, the common model now applies to all supported platforms.

For information about each model's order information, capacity limits, and adding VDOMs, see the [FortiGate-VM datasheet](#).

The primary requirement for the provisioning of a virtual FortiGate may be the number of interfaces it can accommodate rather than its processing capabilities. In some cloud environments, the options with a high number of interfaces tend to have high numbers of vCPUs.

The licensing for FortiGate-VM does not restrict whether the FortiGate can work on a VM instance in a public cloud that uses more vCPUs than the license allows. The number of vCPUs indicated by the license does not restrict the FortiGate-VM from working, regardless of how many vCPUs are included in the virtual instance. However, only the licensed number of vCPUs process traffic and management tasks. The rest of the vCPUs are unused.

The following shows an example for FGT-VM08:

License	1 vCPU	2 vCPU	4 vCPU	8 vCPU	16 vCPU	32 vCPU
FGT-VM08	OK	OK	OK	OK	The FortiGate-VM uses eight vCPUs used for traffic and management. It does not use the rest.	The FortiGate-VM uses eight vCPUs used for traffic and management. It does not use the rest.

You can provision a VM instance based on the number of interfaces you need and license the FortiGate-VM for only the processors you need.

## Licensing

You must have a license to deploy FortiGate-VM for Azure:

### Order types

On Azure, there are usually two order types: BYOL and PAYG.

BYOL offers perpetual (normal series and v-series) and annual subscription (s-series) licensing as opposed to PAYG, which is an hourly subscription available with marketplace-listed products. BYOL licenses are available for purchase from resellers or your distributors, and the publicly available price list, which is updated quarterly, lists prices. BYOL licensing provides the same ordering practice across all private and public clouds, no matter what the platform is. You must activate a license for the first time you access the instance from the GUI or CLI before you can start using various features.

With a PAYG subscription, the FortiGate-VM becomes available for use immediately after you create the instance. The marketplace product page mentions term-based prices (hourly or annual).

In both BYOL and PAYG, cloud vendors charge separately for resource consumption on computing instances, storage, and so on, without the use of software running on top of it (in this case FortiGate).

For BYOL, you typically order a combination of products and services, including support entitlement. New s-series SKUs contain the VM base and service bundle entitlements for easier ordering. PAYG includes support, for which you must contact Fortinet Support with your customer information. See *Plans* on the [marketplace product page](#).

To purchase PAYG, all you need to do is subscribe to the product on the marketplace. However, you must contact Fortinet Support with your customer information to obtain support entitlement. See [Creating a support account on page 12](#).



PAYG FortiGate-VM instances do not support the use of virtual domains (VDOMs). If you plan to use VDOMs, deploy BYOL instances instead.

---



PAYG and BYOL licensing and payment models are not interchangeable. For example, once you spin up a FortiGate-VM PAYG instance, you cannot inject a BYOL license on the same VM. Likewise, you cannot convert a FortiGate-VM BYOL instance to PAYG.

---

When using a FortiGate-VM on-demand instance prior to version 6.4.2, the FortiOS GUI may display expiry dates for FortiGuard services. However, these expiries are automatically extended for as long as the on-demand instance's lifespan. You do not need to be concerned about the expiry of FortiGuard services. For example, the following screenshot shows 2038/01/02.

## About FortiGate-VM for Azure

The screenshot shows the FortiGuard Distribution Network interface under the System > FortGuard tab. The left sidebar includes options like Dashboard, Security Fabric, FortiView, Network, System (Administrators, Admin Profiles, Firmware, Settings), HA, SNMP, Replacement Messages, FortGuard (selected), and Advanced. The main panel displays 'License Information' with a table:

Entitlement	Status
FortiCare Support	Not Supported
Firmware & General Updates	Licensed - expires on 2038/01/02
Application Control Signatures	Version 16.00975
Device & OS Identification	Version 1.00110
Internet Service Database Definitions	Version 7.01212
Intrusion Prevention	Licensed - expires on 2038/01/02
IPS Definitions	Version 16.00975
IPS Engine	Version 5.00021

FortiOS 6.4.2 and later versions do not display dates.

The screenshot shows the FortiGuard Distribution Network interface under the System > FortGuard tab. The left sidebar includes options like Dashboard, Security Fabric, Network, System (Administrators, Admin Profiles, Firmware, Settings), HA, SNMP, Replacement Messages, FortGuard (selected), Feature Visibility, and Certificates. The main panel displays 'License Information' with a table:

Entitlement	Status
FortiCare Support	Not Registered
Virtual Machine	Valid
Firmware & General Updates	Licensed
Intrusion Prevention	Licensed
AntiVirus	Licensed
Web Filtering	Licensed
Outbreak Prevention	Licensed
SD-WAN Network Monitor	Not Licensed
Security Rating	Licensed

## Creating a support account

FortiGate-VM for Azure supports both PAYG and BYOL licensing models. See [Order types on page 11](#).

PAYG users do not need to register from the FortiGate GUI. If you are using a PAYG licensing model and need to ask technical questions to support, obtain support entitlement by contacting [Fortinet Customer Support](#) after creating the FortiGate-VM instance in Azure, and by providing the following information:

- Your FortiGate-VM instance's serial number
- Your Fortinet account's email ID. If you do not have a Fortinet account, you can create one at [Customer Service & Support](#).

## BYOL

You must obtain a license to activate the FortiGate-VM. If you have not activated the license, you see the license upload screen when you log into the FortiGate-VM and cannot proceed to configure the FortiGate-VM.

You can obtain licenses for the BYOL licensing model through any Fortinet partner. If you do not have a partner, contact [azuresales@fortinet.com](mailto:azuresales@fortinet.com) for assistance in purchasing a license.

After you purchase a license or obtain an evaluation license (60-day term), you receive a PDF with an activation code.

### To register a BYOL license:

1. Go to [Customer Service & Support](#) and create a new account or log in with an existing account.
2. Go to *Asset > Register/Activate* to start the registration process.
3. In the *Registration* page, enter your license activation code, then select *Next* to continue registering the product.
4. If you register the S-series subscription model, the site prompts you to select one of the following:
  - a. Click *Register* to newly register the code to acquire a new serial number with a new license file.
  - b. Click *Renew* to renew and extend the licensed period on top of the existing serial number, so that all features on the VM node continue working uninterrupted upon license renewal.
5. At the end of the registration process, download the license (.lic) file to your computer. You upload this license later to activate the FortiGate-VM.

After registering a license, Fortinet servers may take up to 30 minutes to fully recognize the new license. When you upload the license (.lic) file to activate the FortiGate-VM, if you get an error that the license is invalid, wait 30 minutes and try again.

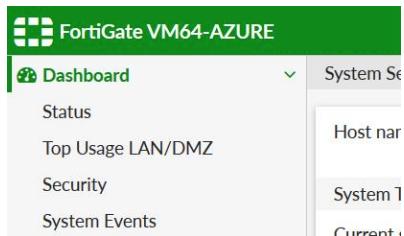
### PAYG

### To register a PAYG license:

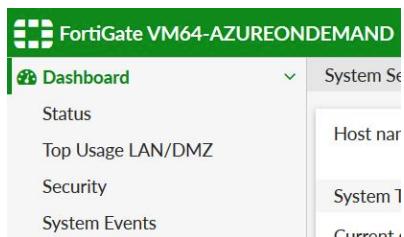
1. Deploy and boot the FortiGate-VM PAYG instance and log into the FortiGate-VM GUI management console.
2. From the Dashboard, copy the VM's serial number.
3. Go to [Customer Service & Support](#) and create a new account or log in with an existing account.
4. Go to *Asset > Register/Activate* to start the registration process.
5. In the *Registration* page, enter the serial number, and select *Next* to continue registering the product.
6. After completing registration, contact [Fortinet Customer Support](#) and provide your FortiGate-VM instance's serial number and the email address associated with your Fortinet account.

## Verifying the license type

The top left corner of the FortiOS GUI indicates the FortiGate license type. The following is the GUI for a BYOL instance:



The following is the GUI for a PAYG instance:



You can also run the `get system status` command. For a BYOL instance, the output is as follows:

## About FortiGate-VM for Azure

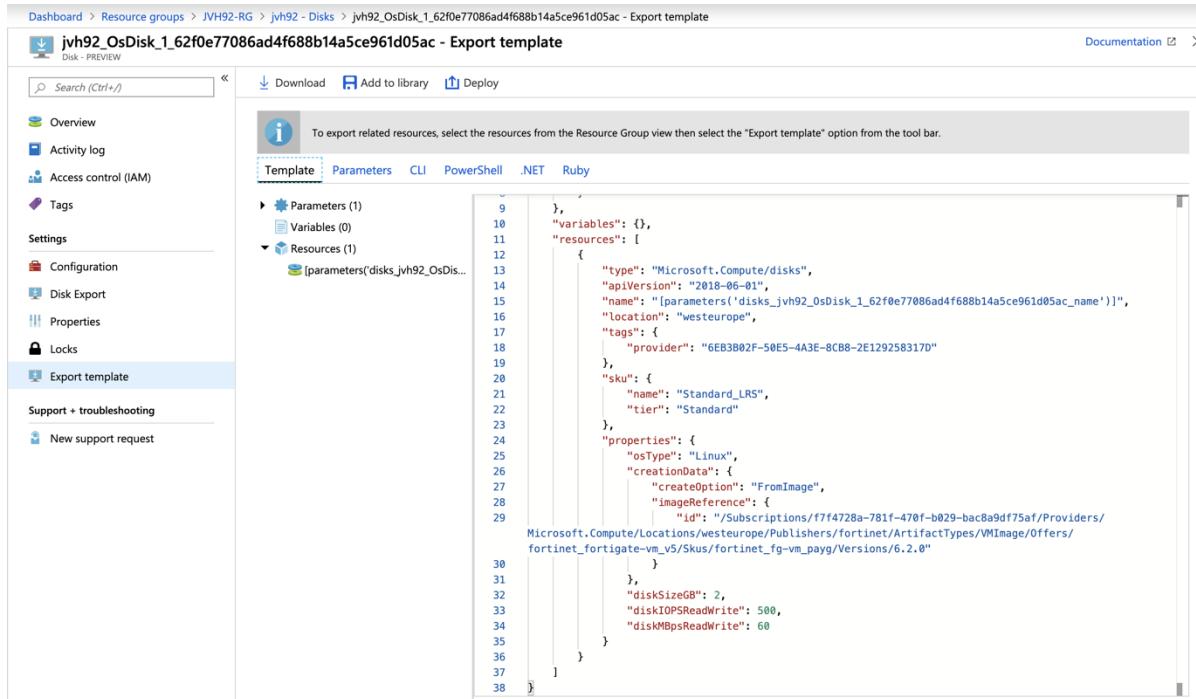
Version: FortiGate-VM64-AZURE v6.4.0, build1579, 200330 (GA)

For a PAYG instance, the output is as follows:

Version: FortiGate-VM64-AZUREONDEMAND v6.4.0, build1579, 200330 (GA)

By opening the OS disk, you can also verify the image used during deployment, which indicates the license type. The deployment process clones the disk from a disk image that Fortinet has provided to the Azure marketplace.

Open your deployed VM's OS disk and select *Export template*. In the template, search for `imageReference`. For a BYOL instance, this URI contains `fortinet_fg-vm`. For a PAYG instance, it contains `fortinet_fg-vm_payg_20190624`.



```
Dashboard > Resource groups > Jvh92-RG > jvh92 - Disks > jvh92_OsDisk_1_62f0e77086ad4f688b14a5ce961d05ac - Export template
Disk - PREVIEW
jvh92_OsDisk_1_62f0e77086ad4f688b14a5ce961d05ac - Export template
Documentation X
Search (Ctrl+)
Download Add to library Deploy
Template Parameters CLI PowerShell .NET Ruby
Parameters (1)
Variables (0)
Resources (1)
[parameters('disks_jvh92_OsDis...
9 },
10 "variables": {},
11 "resources": [
12   {
13     "type": "Microsoft.Compute/disks",
14     "apiVersion": "2018-06-01",
15     "name": "[parameters('disks_jvh92_OsDisk_1_62f0e77086ad4f688b14a5ce961d05ac_name')]",
16     "location": "westeurope",
17     "tags": {
18       "provider": "6EB3B02F-50E5-4A3E-8CB8-2E129258317D"
19     },
20     "sku": {
21       "name": "Standard_LRS",
22       "tier": "Standard"
23     },
24     "properties": {
25       "osType": "Linux",
26       "creationData": {
27         "createOption": "FromImage",
28         "imageReference": {
29           "id": "/Subscriptions/f7f4728a-781f-470f-b029-bac8a9df75af/Providers/
Microsoft.Compute/locations/westeurope/publishers/fortinet/artifactTypes/vmImage/offers/
fortinet_fortigate-vm_v5/skus/fortinet_fg-vm_payg/versions/6.2.0"
30         }
31       },
32       "diskSizeGB": 2,
33       "diskIOPSReadWrite": 500,
34       "diskMBpsReadWrite": 60
35     }
36   }
37 ]
38 }
```

## Migrating a FortiGate-VM instance between license types

When deploying a FortiGate-VM on public cloud, you determine the license type (PAYG or BYOL) during deployment. The license type is fixed for the VM's lifetime. The image that you use to deploy the FortiGate-VM on the public cloud marketplace predetermines the license type.

Migrating a FortiGate-VM instance from one license type to another requires a new deployment. You cannot simply switch license types on the same VM instance. However, you can migrate the configuration between two VMs running as different license types. There are also FortiOS feature differences between PAYG and BYOL license types. For example, a FortiGate-VM PAYG instance is packaged with Unified Threat Management protection and does not support VDOMs, whereas a FortiGate-VM BYOL instance supports greater protection levels and features depending on its contract.

### To migrate FortiOS configuration to a FortiGate-VM of another license type:

1. Connect to the FortiOS GUI or CLI and back up the configuration. See [Configuration backups](#).
2. Deploy a new FortiGate-VM instance with the desired license type. You can deploy the instance using one of the following methods:

- [Azure marketplace](#)
- [Azure CLI](#)
- [Deploying FortiGate-VM using Azure PowerShell on page 30](#)
- [ARM templates](#)
- [Terraform templates](#)

If deploying a BYOL instance, you must purchase a new license from a Fortinet reseller. You can apply the license after deployment via the FortiOS GUI or bootstrap the license and configuration during initial bootup using custom data as described in [Bootstrapping the FortiGate CLI and BYOL license at initial bootup using user data on page 35](#).

3. Restore the configuration on the FortiGate-VM instance that you deployed in step 2. As with the license, you can inject the configuration during initial bootup. Alternatively, you can restore the configuration in the FortiOS GUI as described in [Configuration backups](#).
4. If you deployed a PAYG instance in step 2, register the license. To receive support for a PAYG license, you must register the license as described in [Creating a support account on page 12](#).

## Obtaining a FortiCare-generated license for Azure on-demand instances

New Azure on-demand and upgraded instances can retrieve a FortiGate serial number and license from FortiCare servers. Using the serial number, users can register the device to their account and start using FortiToken and FortiGate Cloud services.

The FortiGate-VM must be able to reach FortiCare to receive a valid on-demand license. Ensure connectivity to FortiCare (<https://directregistration.fortinet.com/>) by checking all related setup on the virtual network, subnet, network security group, route table, public IP addresses, and so on.

This feature is only available for FortiOS 6.4.2 and later versions.

### To verify cloudinit automatically obtained a license for a newly-deployed instance:

```
# diagnose debug cloudinit show
>> Load VM metadata document
>> Requesting FortiCare license: FGTAZXXXXXXXXXX
>> VM license install succeeded. Rebooting firewall.

# diagnose debug vm-print-license
SerialNumber: FGTAZXXXXXXXXXX
CreateDate: Wed Jul 29 16:48:34 2020
Key: yes
Cert: yes
Key2: yes
Cert2: yes
Model: PG (20)
CPU: 2147483647
MEM: 2147483647

# execute vm-license
PAYG license exists.
```

If in a closed network, the command execution resembles the following, as the `execute vm-license` command attempts to get a license from FortiCare.

```
# diagnose debug cloudinit show
```

```
# diagnose debug vm-print-license
SerialNumber: FGTAZXXXXXXXXXXXX
CreateDate: 1597362903
Model: PG (20)
CPU: 2147483647
MEM: 2147483647

# execute vm-license
This operation will reboot the system !
Do you want to continue? (y/n)
```

```
Load VM metadata document
Requesting FortiCare license: FGTAZXXXXXXXXXXXX
```

If the FortiGate-VM connects to FortiCare successfully, the following message displays.

```
VM license install succeeded. Rebooting firewall.
```

### To obtain a license for an upgraded instance or instance from a closed network:

If you created the FortiGate-VM in a closed environment or it cannot reach FortiCare, the FortiGate-VM self-generates a local license as in previous FortiOS versions. You can obtain a FortiCare license, ensure that the FortiGate-VM can connect to FortiCare, then run the `execute vm-license` command to obtain the license from FortiCare.

```
# execute vm-license
This operation will reboot the system !
Do you want to continue? (y/n)y

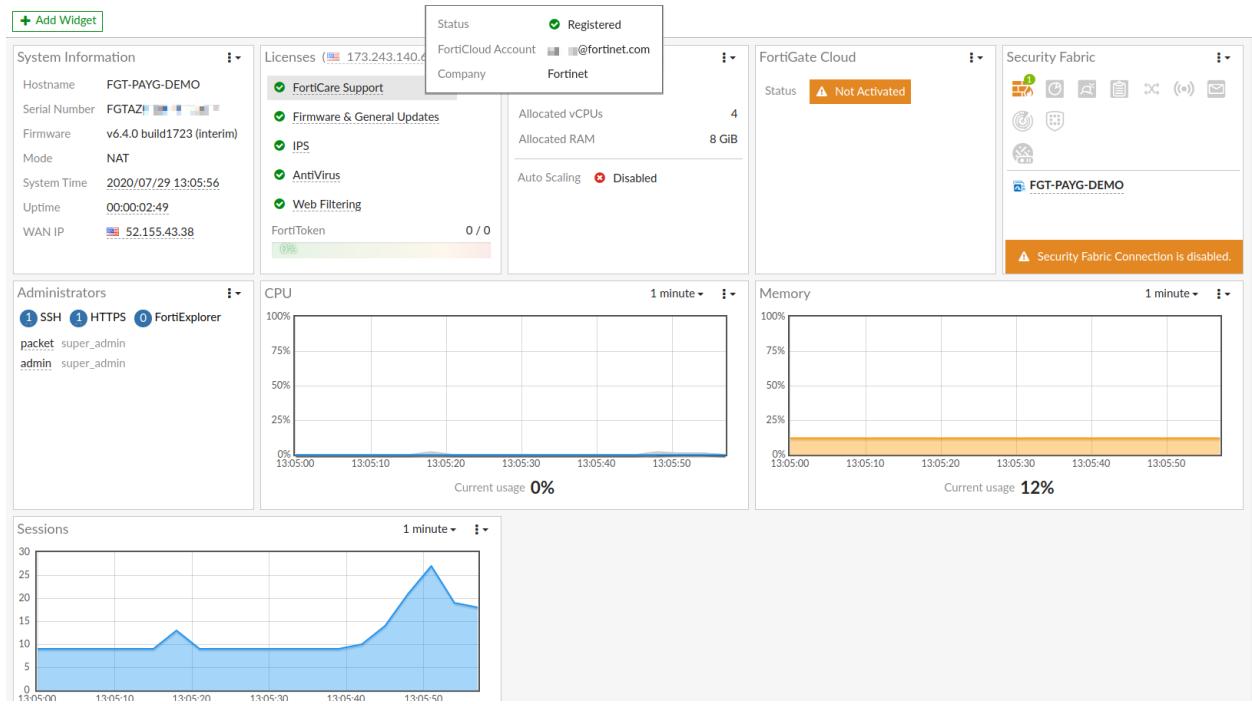
Load VM metadata document
Requesting FortiCare license: FGTAZXXXZXXXXXX
VM license install succeeded. Rebooting firewall.
```

### To register the serial number:

1. Register the license using the serial number in FortiCare (see [Creating a support account on page 12](#)).
2. Obtain the VM ID:
  - In FortiOS, run `diagnose test application azd 6` and search for the VM Instance ID.
  - In Azure, run `az vm show -g Resource-Group-Name -n PAYG-VM-Name --query vmId` -o tsv.  
It may take up to an hour for the registration status to synchronize and update in the FortiOS GUI.

## About FortiGate-VM for Azure

3. Go Dashboard > Status and in the Licenses widget verify the *FortiCare Support* status.



4. Once the registration is complete, you can log in to a [FortiGate Cloud](#) account and download the two free tokens that come standard with FortiGates (see [FortiTokens](#)).

# Deploying FortiGate-VM on Azure

You can deploy FortiGate-VM NGFW for Azure as a virtual appliance in Azure cloud (Infrastructure as a Service (IaaS)). See [Overview](#).

## Azure services and components

FortiGate-VM for Azure is a Linux VM instance. The following table lists Azure services and components required to be understood when deploying FortiGate-VM. All services and components listed relate to ordinary FortiGate-VM single instance deployment or FortiGate-native active-passive HA deployment.

Service/component	Description
Azure Virtual Network (VNet)	This is where the FortiGate-VM and protected VMs are situated and users control the network. When you deploy FortiGate-VM, you can configure relevant network settings.
VM	FortiGate-VM for Azure is a customized Linux VM instance.
Subnets, route tables	You must appropriately configure the FortiGate-VM with subnets and route tables to handle traffic. When deploying from the marketplace launcher, there are two subnets for the FortiGate-VM labeled <code>PublicFacingSubnet</code> and <code>InsideSubnet</code> by default.
Resource group	A group of resources where the FortiGate-VM is deployed
Availability Set	An availability set is a logical grouping capability that you can use in Azure to ensure that the VM resources you place within it are isolated from each other when they are deployed within an Azure datacenter. Usually a set intends to accommodate multiple VMs.
Public DNS IP address	You must allocate at least one public IP address to the FortiGate-VM to access and manage it over the Internet.
Security groups	Unlike AWS, you cannot configure Azure security groups at the time of FortiGate-VM deployment. All traffic is allowed inbound to, or outbound from, the subnet, or network interface by default. See <a href="#">Default security rules</a> .
VHD	A special type of deployable image used for Azure. As long as you deploy FortiGate-VM from the marketplace launcher, you do not need VHD files. However, you can launch FortiGate-VM (BYOL) directly from the FortiGate-VM VHD image file instead of using the marketplace. Ask <a href="mailto:azuresales@fortinet.com">azuresales@fortinet.com</a> to find out where you can obtain the VHD images if needed.
ARM Templates	You can deploy FortiGate-VM instances in two ways: <ol style="list-style-type: none"><li>Find the FortiGate-VM product listing on the marketplace and launch from it. You do not necessarily see Azure Resource Manager (ARM) templates onscreen but they are used on the backend. You can also download the templates once the deployment process proceeds.</li></ol>

Service/component	Description
	<p>2. Launch custom deployment in the Azure portal. Upload ARM templates of your choice that deploy FortiGate with your desirable topology and configuration.</p> <p>ARM templates are available on <a href="#">GitHub</a>.</p> <p>Fortinet-provided ARM templates are not supported within the regular Fortinet technical support scope. Contact <a href="mailto:azuresales@fortinet.com">azuresales@fortinet.com</a> with questions.</p>
Load Balancer	<p>A network LB automatically distributes traffic across multiple FortiGate-VM instances when configured properly. Topologies differ depending on how you distribute incoming and outgoing traffic.</p> <p>Fortinet provides a FortiGate marketplace product listing that automatically comes along with 2 FortiGate-VM nodes and LB. Check out <a href="#">FortiGate Next-Generation Firewall for Azure LB HA</a>.</p>

## Deploying FortiGate-VM from a VHD image file

You can deploy FortiGate using custom templates or PowerShell from VHD image files.

VHD image files are available from [Fortinet Customer Service & Support](#). Go to *Support > VM Image*, then select *FortiGate* as the *Product* and *Azure* for the *Platform*. The file name is FGT\_VM64\_AZURE-v6-buildXXXX-FORTINET.out.hyperv.zip, where XXXX is the build number.

Once the download is complete, unzip the file and locate the fortios.vhd file. Upload the fortios.vhd file to your blob/storage location as required by your deployment templates.

At a given time, [Fortinet Customer Service & Support](#) hosts only the two latest major versions with two minor versions each. To obtain older files, navigate to *Support > Firmware Images*, select *FortiGate* as the *Product*, then go to the *Download* tab. Go to the desired version and download the FGT\_VM64\_AZURE-v6-buildXXXX-FORTINET.out.hyperv.zip file.

## Deploying FortiGate with a custom ARM template

You can deploy a FortiGate-VM (BYOL) outside the marketplace product listing using a custom ARM template in the Azure portal. This is an alternative method for if you want to deploy FortiGate-VM on instance types/sizes that you cannot find on the FortiGate-VM marketplace launcher. Some instance types of your choice may not properly boot up or run due to lack of official FortiGate-VM instance support.

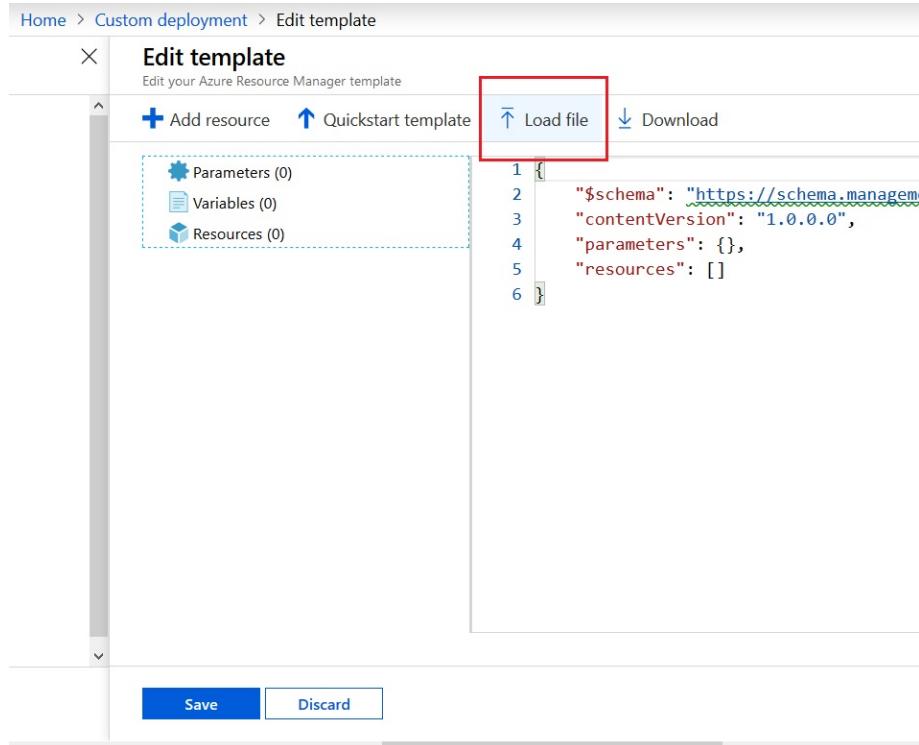
There is a bare minimum set of templates available for your deployment.

You can also specify bootstrapping FortiGate CLI commands within the template and run them at the time of initial bootup.

## Invoking a custom ARM template

To invoke a custom ARM template:

1. Log in to the Azure portal and go to *Custom deployment*.
2. Click *Build your own template in the editor*.
3. From [GitHub](#), copy and paste the template content, or download the template file and load it into the *Edit template* window.



**4. Ensure that the template is shown in the screen. Click Save.**

The screenshot shows the Azure Resource Manager template editor. On the left, there's a tree view of resources: Parameters (21), Variables (13), and Resources (10). The Resources section is highlighted with a red box. On the right, the JSON code for the template is displayed, also enclosed in a red box. The code defines parameters for location, admin username, and admin password.

```

1 {
2   "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
3   "contentVersion": "1.0.0.0",
4   "parameters": {
5     "location": {
6       "type": "string",
7       "metadata": {
8         "description": "location - same as above"
9       }
10    },
11    "adminUsername": {
12      "type": "string",
13      "metadata": {
14        "description": "Username for the FortiGate virtual appliance."
15      }
16    },
17    "adminPassword": {
18      "type": "securestring",
19      "metadata": {
20        "description": "Password for the FortiGate virtual appliance."
21      }
22  }
}

```

At the bottom, there are 'Save' and 'Discard' buttons.

**5. Edit the parameters:**

- Click *Edit parameters*.
- Copy and paste the parameters from [GitHub](#), or download the file as in step 3. You can manually edit the fields.

The screenshot shows the Azure Resource Manager parameter editor. The 'Load file' button is highlighted with a red box. The JSON code is identical to the one in the previous screenshot, but it includes parameter values: location, adminUsername, adminPassword, FortiGateName, FortiGateImageSKU, and FortiGateImageVersion, all set to an empty string (""). At the bottom, there are 'Save' and 'Discard' buttons.

```

1 {
2   "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
3   "contentVersion": "1.0.0.0",
4   "parameters": {
5     "location": {
6       "value": ""
7     },
8     "adminUsername": {
9       "value": ""
10    },
11    "adminPassword": {
12      "value": ""
13    },
14    "FortiGateName": {
15      "value": ""
16    },
17    "FortiGateImageSKU": {
18      "value": ""
19    },
20    "FortiGateImageVersion": {
21      "value": ""
22    }
}

```

- c. Click **Save**.
6. Complete the following fields:

Field	Description
<b>Basics</b>	
Subscription	Enter the subscription that is entitled to purchase marketplace products of your choice. Generally, selecting a subscription that your organization has configured to not be able to purchase Azure resources is advisable. Ensure that you specify the appropriate subscription.
Resource Group	You must create a new resource group. Click <i>Create New</i> and enter a nonexistent resource group.
Location	From the dropdown list, select a region to deploy the FortiGate-VM and related resources.
<b>Settings</b>	
Location	Manually specify the same location as the above by entering the region.
Admin Username	Specify an administrator login name that can log into the FortiGate management console. Azure does not allow names such as root or admin.
Admin Password	Specify an administrator password with some character complexity. The password must be between 12 and 72 characters and contain at least three of the following: one lower-case character, one upper-case character, one number, and one special character.
FortiGate Name	Specify the FortiGate-VM instance name or FortiGate hostname that can be identified on the Azure portal.
FortiGate Image SKU	Leave this as-is.
FortiGate Image version	Select a version. Note that this version points to the one that the FortiGate marketplace listing supports. As the template may contain obsolete versions, specifying <i>Latest</i> is recommended.
Instance Type	Choose an instance type based on the number of virtual CPU cores. Recommended types are the following compute instances: <ul style="list-style-type: none"> <li>• Standard_F1</li> <li>• Standard_F2</li> <li>• Standard_F4</li> <li>• Standard_F8</li> <li>• Standard_F1s</li> <li>• Standard_F2s</li> <li>• Standard_F4s</li> <li>• Standard_F8s</li> <li>• Standard_F16s</li> <li>• Standard_F2s_v2</li> <li>• Standard_F4s_v2</li> <li>• Standard_F8s_v2</li> <li>• Standard_F16s_v2</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>• Standard_F32s_v2</li> <li>• Standard_F64s_v2</li> <li>• Standard_F72s_v2</li> </ul> <p>Instances with over 32 vCPU requires a FG-VMUL license that can support an unlimited number of CPU cores.</p>
Public IP New or Existing or None	Choose <i>New</i> .
Public IP Address Name	Enter a name to distinguish the public IP address.
Public IP Resource Group	Ensure you specify the same resource group as entered in <i>Basics &gt; Resource Group</i> above.
Public IP Address Type	Select <i>Static</i> .
Vnet New or Existing	Select <i>New</i> .
Net Name	Specify the same name as the resource group name.
Vnet Address Prefix	Specify a CIDR that does not overlap with your existing Vnet CIDRs.
Subnet1Name	Enter a name to distinguish the public subnet.
Subnet1Prefix	Specify a CIDR that belongs to the Vnet Address Prefix above.
Subnet2Name	Enter a name to distinguish the private/protected subnet.
Subnet2Prefix	Specify another CIDR that belongs to the Vnet Address Prefix above.
Fortinet Tags	Leave as-is.
Artifacts Base URL	Leave as-is.

## Deploying FortiGate-VM on Azure

The screenshot shows the 'Custom deployment' wizard in the Azure portal. On the left is a dark sidebar with navigation links like 'Create a resource', 'All services', 'Favorites', 'Dashboard', 'Resource groups', etc. The main area has a title 'Custom deployment' with a sub-instruction 'Deploy from a custom template'. A 'TEMPLATE' section shows a 'Customized template' with '10 resources'. Below are sections for 'BASICS' (Subscription: 'yourresourcegrp01', Resource group: '(New) yourresourcegrp01', Location: 'UK West') and 'SETTINGS' (Location: 'UK West', Admin Username: 'youradmin', Admin Password: masked, Forti Gate Name: 'yourfgname01', Image SKU: 'fortinet\_fg-vm', Image Version: 'latest', Instance Type: 'Standard\_F2s\_v2', Public IP: 'new', Public IP Address Name: 'yourpubIP', Public IP Resource Group: 'yourresourcegrp01', Public IP Address Type: 'Static', Vnet: 'new', Vnet Name: 'yournewvnet01', Vnet Resource Group: 'yourresourcegrp01', Vnet Address Prefix: '10.88.0.0/16', Subnet1Name: 'yoursubnet1', Subnet1Prefix: '10.88.1.0/24', Subnet2Name: 'yoursubnet2', Subnet2Prefix: '10.88.2.0/24', Fortinet Tags: '["provider": "6EB3B02F-50E5-3A9D-777A-9258317D"]', Artifacts Base URI: 'https://raw.githubusercontent.com/fortinetclouddev/FortigateAzureTemplate/6.0.4'). At the bottom are 'TERMS AND CONDITIONS' (links to 'Azure Marketplace Terms' and 'Azure Marketplace'), a terms and conditions agreement checkbox ('I agree to the terms and conditions stated above'), and a 'Purchase' button.

7. Select the *I agree to the terms and conditions stated above* checkbox. Click **Purchase**. It takes about 10-15 minutes to deploy the FortiGate-VM and related resources. If you encounter an issue, resolve the issue and retry the deployment.
8. After successful deployment, connect to the FortiGate instance using the credentials specified above. See [Connecting to the FortiGate-VM](#).

## Bootstrapping the FortiGate CLI at initial bootup using user data

You can run FortiGate CLI commands at initial bootup by using custom cloud-init.

1. Download the [ARM template](#) and open in a text editor.
2. Find the variables section and the userData statement as shown. The line number may be different than in the screenshot.
3. After concat, specify FortiGate CLI commands. If they are run across multiple lines (in the FortiGate CLI, these commands are run by using the *Enter* key), separate each line with a backslash and \n and enclose the whole statement with single quotes.

```

167      "description": "Base URL of the solution template gallery package",
168      "artifactsBaseUrl": ""
169    }
170  },
171  "variables": {
172    "subnet1Ref": "[resourceId(parameters('vnetResourceGroup'), 'Microsoft.Network/virtualNetworks/subnets', parameters('vnetName'), parameters('publicIPID'))]",
173    "subnet2Ref": "[resourceId(parameters('vnetResourceGroup'), 'Microsoft.Network/virtualNetworks/subnets', parameters('vnetName'), parameters('publicIPID'))]",
174    "routeTable1Name": "[concat(parameters('FortiGateName'), '-', parameters('Subnet1Name'), '-routes-', uniquestring(deployment().name))]",
175    "routeTable2Name": "[concat(parameters('FortiGateName'), '-', parameters('Subnet2Name'), '-routes-', uniquestring(deployment().name))]",
176    "network_NIC_fg11_Name": "[concat(parameters('FortiGateName'), '-Nic0-', uniquestring(deployment().name))]",
177    "network_NIC_fg11_Id": "[resourceId('Microsoft.Network/networkInterfaces', variables('network_NIC_fg11_Name'))]",
178    "network_NIC_fg12_Name": "[concat(parameters('FortiGateName'), '-Nic1-', uniquestring(deployment().name))]",
179    "network_NIC_fg12_Id": "[resourceId('Microsoft.Network/networkInterfaces', variables('network_NIC_fg12_Name'))]",
180    "compute_AvailabilitySet_FG_Name": "[concat(parameters('FortigateName'), '-AvailabilitySet-', uniquestring(deployment().name))]",
181    "compute_AvailabilitySet_FG_Id": "[resourceId('Microsoft.Compute/availabilitySets', variables('compute_AvailabilitySet_FG_Name'))]",
182    "updateIPURI": "[concat(parameters('ArtifactsBaseURI'), '/update-nic.json')]",
183    "virtualNetworkSetupURI": "[concat(parameters('ArtifactsBaseURI'), '/netsetup.json')]",
184    "userData": "[concat('config system global\nset timezone 03\nend\n')]"
185  },
186  "resources": [
187    {
188      "apiVersion": "2018-02-01",
189    }
190  ]
}

```

The example above is the same as executing the following in the FortiGate CLI:

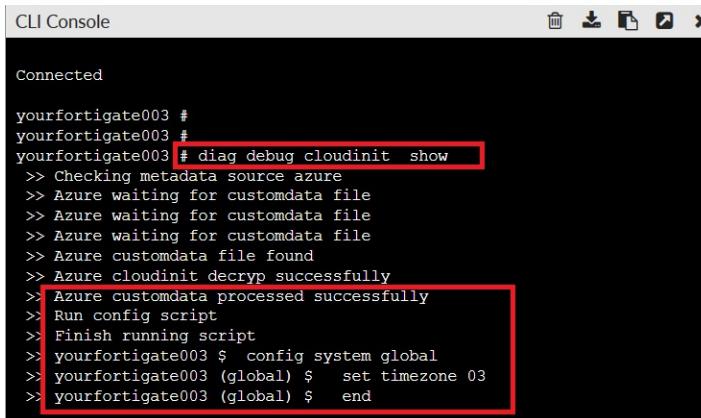
```
config system global
  set timezone 03
end
```

4. Load the file as shown in [Invoking a custom ARM template on page 20](#).

5. After deployment, log into the FortiGate.

6. Check if the command was successfully run:

- a. In the CLI console, enter `diag debug cloudinit show`. If the cloud-init was successful, the CLI shows Azure customdata processed successfully. The FortiGate CLI command syntax must be correct.



```
Connected

yourfortigate003 #
yourfortigate003 #
yourfortigate003 # diag debug cloudinit show
>> Checking metadata source azure
>> Azure waiting for customdata file
>> Azure waiting for customdata file
>> Azure waiting for customdata file
>> Azure customdata file found
>> Azure cloudinit decryp successfully
>> Azure customdata processed successfully
>> Run config script
>> Finish running script
>> yourfortigate003 $ config system global
>> yourfortigate003 (global) $ set timezone 03
>> yourfortigate003 (global) $ end
```

If the CLI command fails, you see an error message with `diag debug cloudinit show` as above. Resolve it and try again.

- b.** Check the timezone by running config system global and get commands.

```
security-rating-result-submission: enable
security-rating-run-on-schedule: enable
send-pmtu-icmp : enable
snat-route-change : disable
special-file-23-support: disable
--More--      ssd-trim-freq : weekly
ssd-trim-hour : 1
ssd-trim-min : Random
ssd-trim-weekday : sunday
ssh-kex-shal : enable
ssl-min Proto-version: TLSv1-2
ssl-static-key-ciphers: enable
sslvpn-cipher-hardware-acceleration: enable
sslvpn-kxp-hardware-acceleration: enable
sslvpn-max-worker-count: 1
sslvpn-plugin-version-check: enable
strict-dirty-session-check: enable
strong-crypto : enable
switch-controller : disable
switch-controller-reserved-network: 169.254.0.0 255.255.0.0
sys-perf-log-interval: 5
tcp-halfclose-timer : 120
tcp-halfopen-timer : 10
tcp-option : enable
tcp-timewait-timer : 1
timezone : (GMT-9:00) Alaska
traffic-priority : tos
```

As expected, the timezone was changed. This means the bootstrapping CLI command worked.

## Bootstrapping the FortiGate CLI and BYOL license at initial bootup using user data

You can run FortiGate CLI commands and a BYOL license at initial bootup by using custom cloud-init. Use the following sample ARM templates:

- [Template](#)
- [Parameters](#)

For details on using a custom ARM template, see [Deploying FortiGate with a custom ARM template on page 19](#).

First, you must create two text files: one for FortiGate CLI configuration and another for a license file.

1. Create a CLI configuration file:
  - a. In a text editor, create a text file that contains CLI commands like the following:
 

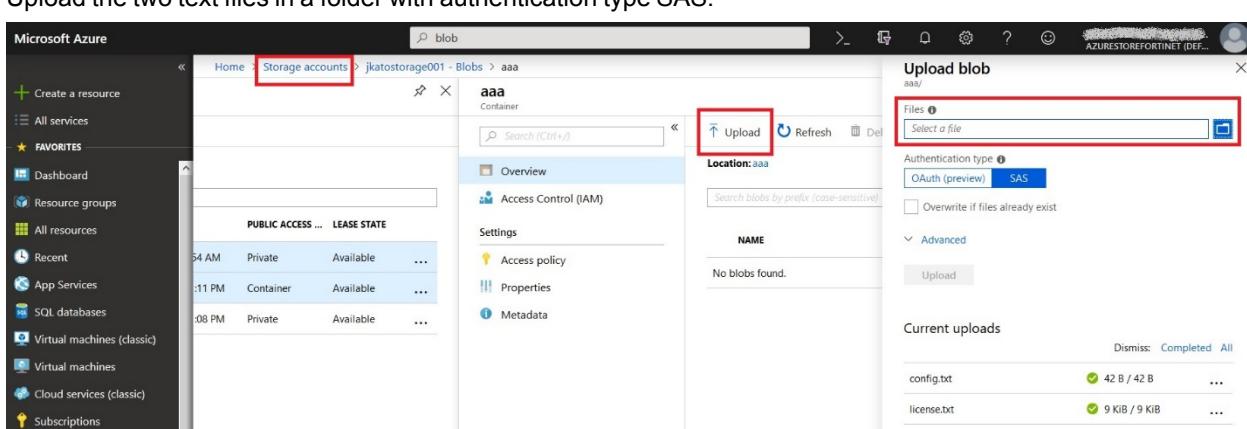
```
config system global
          set timezone 03
          end
```
  - b. Save the file as config.txt or another desired name. This example sets the timezone as GMT-9 Alaska.
2. Create a license text file:
  - a. Download a FortiGate license from [Customer Service & Support](#) and save the file as license.txt or any other desired name. The file contains content that resembles the following:

## Deploying FortiGate-VM on Azure

3. Place both text files on your Azure blob.
  4. In this example, you are required to have the following:
    - Storage account

- Private container in the blob

Upload the two text files in a folder with authentication type SAS.



5. Copy and paste the SAS URLs into the parameters file:
    - a. After uploading, click the menu icon beside config.text. Click Generate SAS to create an SAS URL link. Repeat this step with the license.txt file.

## Deploying FortiGate-VM on Azure

**jkatostorage1**  
Container

Search (Ctrl+)

Upload Refresh Delete Acquire lease Break lease

**Location:** jkatostorage1 / abc

Search blobs by prefix (case-sensitive)  Show deleted blobs

NAME	MODIFIED	ACCESS TIER	BLOB TYPE	SIZE	LEASE STATE
[..]					
<input checked="" type="checkbox"/> config.txt	11/30/2018, 3:38:11 PM	Hot (Inferred)	Block		<div style="display: flex; align-items: center;"><span>View/edit blob</span> </div>
<input type="checkbox"/> license.txt	11/30/2018, 3:37:38 PM	Hot (Inferred)	Block		<div style="display: flex; align-items: center;"><span>Download</span> </div>

**More options**

- View/edit blob
- Download
- Blob properties
- Generate SAS**
- View snapshots
- Create snapshot
- Acquire lease
- Break lease
- Delete

- b.** Copy the SAS URLs.

The screenshot shows the Azure Storage Accounts blade. On the left, a sidebar lists various services: Create a resource, All services, Favorites, Dashboard, Resource groups, All resources, Recent, App Services, SQL databases, Virtual machines (classic), Virtual machines, Cloud services (classic), Subscriptions, Storage accounts, Azure Active Directory, Monitor, Security Center, Cost Management + Billing, Help + support, and Advisor. The 'Storage accounts' item is highlighted.

The main area displays the 'jkatstorage1' storage account. Under the 'Containers' section, 'jkatstorage1' is selected. The 'Overview' tab is active, showing the location as 'jkatstorage1/abc'. A search bar at the top says 'Search (Ctrl+F)'. Below it, there are sections for 'Access Control (IAM)', 'Settings' (with 'Access policy', 'Properties', and 'Metadata' options), and a list of blobs: 'config.txt' and 'license.txt' (selected). A 'Show deleted blobs' checkbox is also present.

On the right, the 'abc/license.txt' blob details page is shown. It includes tabs for Overview, Snapshots, Edit blob, and Generate SAS (which is highlighted with a red box). Below these tabs, a note explains what a Shared Access Signature (SAS) is. The 'Permissions' dropdown is set to 'Read'. The 'Start and expiry date/time' section shows 'Start: 2018-12-03 08:05:33 AM (UTC-0800) --- Current Time Zone ---' and 'Expiry: 2018-12-03 04:06:53 PM (UTC-0800) --- Current Time Zone ---'. The 'Allowed IP addresses' field is empty. The 'Allowed protocols' section has 'HTTPS' selected. The 'Signing key' dropdown is set to 'Key 1'. At the bottom, a large blue button labeled 'Generate blob SAS token and URL' is visible, along with the generated SAS token and URL.

- c. Paste the SAS URLs into the `configURI` and `licenseURI` sections of the `parameters-BYOL-CLI-and-license-json` file as shown:

```
        "configURI": {
            "value": "https://jkatostorage001.blob.core.windows.net/jkatostorage1/abc/config.txt?sp=r&st=2018-12-03T14:20:12Z&se=2018-12-03T22:20:12Z&spr=https&sv=2017-11-09&sr=c"
        },
        "licenseURI": {
            "value": "https://jkatostorage001.blob.core.windows.net/jkatostorage1/abc/license.txt?sp=r&st=2018-12-03T14:21:34Z&se=2018-12-03T22:21:34Z&spr=https&sv=2017-11-09&sr=c"
        }
    },
    "id": "jkatostorage1"
}
```

- 6. Review all template fields. Ensure the following:**

- a. Your chosen subscription is entitled to purchase the marketplace product.
  - b. The same location is entered under *Settings* and under *Basics*. Ensure that the location has sufficient quota to accommodate the FortiGate-VM with the desired number of CPU cores. For details, see [Region support on page 8](#).
  - c. A new resource group is created and the same name is entered under *Public IP Resource Group* and *Vnet Resource Group*.

## Deploying FortiGate-VM on Azure

- d. The *Fortinet Tags* field is automatically populated. There is no need to manually input information into this field. If this field is empty or shows an error, reload the browser, then load the template and parameter files again.
- e. The license and config files' SAS URLs are not expired.

Once all fields are entered, the template should resemble the following:

The screenshot shows the 'Custom deployment' wizard in the Azure portal. The left sidebar lists various Azure services. The main pane shows a 'Customized template' with 10 resources. The configuration details are as follows:

Setting	Value
* Subscription	BYOL [dropdown]
* Resource group	(New) jkatorsgrp006 Create new
* Location	Korea South
* Location	Korea South
* Admin Username	fortiadmin
* Admin Password	[REDACTED]
* Forti Gate Name	yourfortigate006
Forti Gate Image SKU	fortinet_fg-vm
Forti Gate Image Version	6.0.3
Instance Type	Standard_F1
Public IP New Or Existing Or None	new
Public IP Address Name	publicip-fortigate
Public IP Resource Group	jkATORSGRP006
Public IP Address Type	Static
Vnet New Or Existing	new
* Vnet Name	yourssgroup006
Vnet Resource Group	jkATORSGRP006
Vnet Address Prefix	10.8.0.0/16
Subnet1Name	PublicFacingSubnet
Subnet1Prefix	10.8.0.0/24
Subnet2Name	InsideSubnet
Subnet2Prefix	10.8.1.0/24
* Config URI	<a href="https://jkatostorage001.blob.core.windows.net/jkatostorage1/abc/config.txt?sp=r...">https://jkatostorage001.blob.core.windows.net/jkatostorage1/abc/config.txt?sp=r...</a>
* License URI	<a href="https://jkatostorage001.blob.core.windows.net/jkatostorage1/abc/license.txt?sp=r...">https://jkatostorage001.blob.core.windows.net/jkatostorage1/abc/license.txt?sp=r...</a>
Artifacts Base URI	<a href="https://gallery.azure.com/artifact/20151001/fortinet.fortigate-singlevmfortig...">https://gallery.azure.com/artifact/20151001/fortinet.fortigate-singlevmfortig...</a>
Fortinet Tags	{"provider": "6EB3B02F-50E5-4A3E-8CB8-2E129258317D"}

**TERMS AND CONDITIONS**

Azure Marketplace Terms | Azure Marketplace

By clicking "Purchase," I (a) agree to the applicable legal terms associated with the offering; (b) authorize Microsoft to charge or bill my current payment method for the fees associated with the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); and (c) agree that, if the deployment involves 3rd party offerings, Microsoft may share my contact information and other details of such deployment with the publisher of that offering.

I agree to the terms and conditions stated above

**Purchase**

7. Select the checkbox to agree to the terms, then click *Purchase*.

8. After deployment is complete, log into the FortiGate by accessing [https://<IP\\_address>](https://<IP_address>) in your browser.
9. If the license was successfully loaded, you should see the dashboard. If you are prompted to upload a license, this means that bootstrapping the license failed. In this case, you can manually upload the license file, and once the system completes rebooting, log in and invoke the CLI from the dashboard. To check why bootstrapping failed, run the `diag debug cloudinit show` command. See [Bootstrapping the FortiGate CLI at initial bootup using user data on page 25](#).

```
yourfortigate030 # diag debug cloudinit show
>> Checking metadata source azure
>> Azure waiting for customdata file
>> Azure waiting for customdata file
>> Azure waiting for customdata file
>> Azure customdata file found
>> Azure cloudinit decryp successfully
>> Azure Fos-instance-id: 9106ebbe-4840-443f-b951-2993af73cd3a
>> Azure couldn't find mime link
>> Azure trying to get license from: https://jkatostorage001.blob.core.windows.net/fortigate/fortigate.lic
>> Azure download license successfully
>> Azure trying to get config script from https://jkatostorage001.blob.core.windows.net/fortigate/config.lic
>> Azure download config script successfully
>> Azure customdata processed successfully
>> Run config script
>> Finish running script
>> yourfortigate030 $ config system global
>> yourfortigate030 (global) $ set timezone 03
>> yourfortigate030 (global) $ end
```

## Deploying FortiGate-VM using Azure PowerShell

You can deploy FortiGate-VM (BYOL) outside the marketplace product listing using Azure PowerShell. This is an alternative method for if you want to deploy FortiGate-VM on instance types/sizes that are not found on the FortiGate marketplace launcher. Some instance types of your choice may not properly boot up or run due to lack of official FortiGate instance support.

You can also specify bootstrapping FortiGate CLI commands as part of a bootstrapping configuration file that is passed in PowerShell at the time of initial bootup.

That you have thorough knowledge of PowerShell and various Azure services and features to adopt this deployment method is expected.

## Running PowerShell to deploy FortiGate-VM

The instructions assume that PowerShell is already installed on the Windows machine. For details on installing and running PowerShell, see [Install Azure PowerShell on Windows with PowerShellGet](#).

1. Log into a Windows machine and invoke the PowerShell console.
2. Obtain the sample PowerShell script file from [GitHub](#).
3. You must edit the content according to your own Azure environment. The ps1 file contains comments for sections that require modification. Editing the file using Visual Studio with the PowerShell extension installed is recommended. In the `$vmsize` field, enter the desired instance type based on the number of virtual CPU cores. One of the sections you must modify is the `$vmsize` field. Enter the desired instance type here. Recommended types are the following compute-optimized instances:
  - a. Standard\_F1
  - b. Standard\_F2
  - c. Standard\_F4

- d. Standard\_F8
  - e. Standard\_F1s
  - f. Standard\_F2s
  - g. Standard\_F4s
  - h. Standard\_F8s
  - i. Standard\_F16s
  - j. Standard\_F2s\_v2
  - k. Standard\_F4s\_v2
  - l. Standard\_F8s\_v2
  - m. Standard\_F16s\_v2
  - n. Standard\_F32s\_v2
  - o. Standard\_F64s\_v2
  - p. Standard\_F72s\_v2
- 



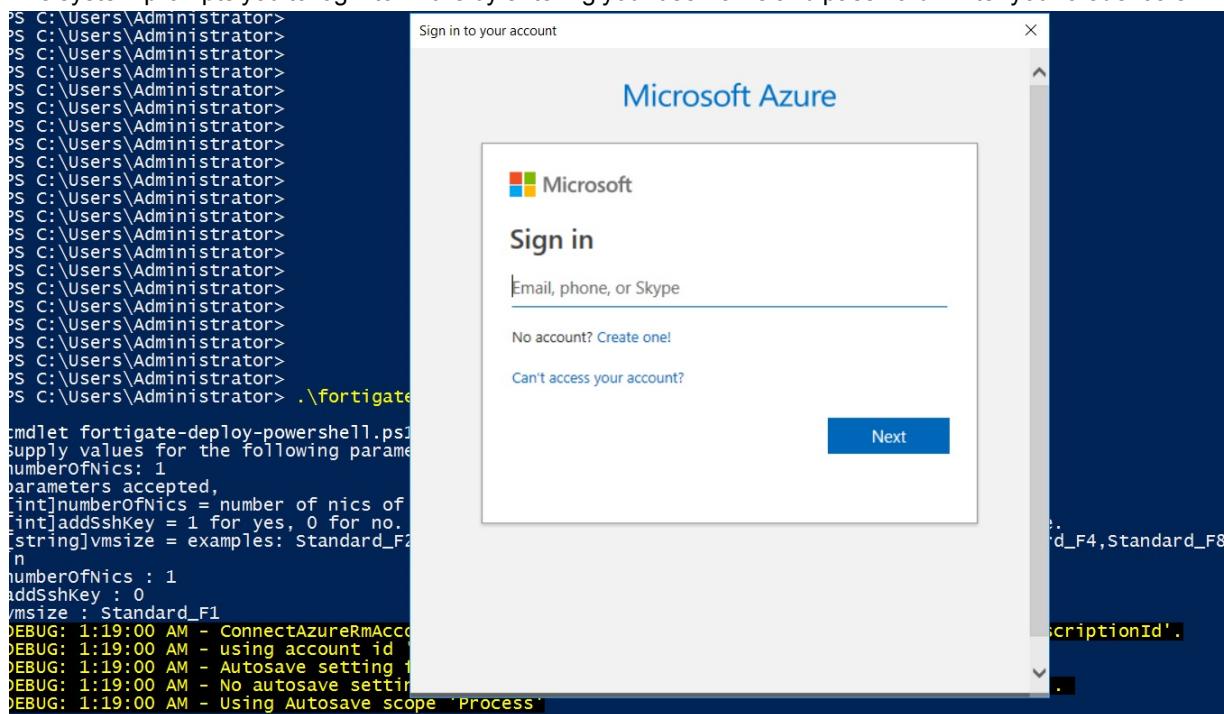
Instances with over 32 vCPU require a FG-VMUL license, which can support an unlimited number of CPU cores.

---

4. This sample file can deploy the FortiGate-VM in an existing VNet under an existing resource group. Before running the ps1 file, you must create the following Azure elements:
  - a. A resource group
  - b. A VNet with a subnet. If you attach more than one NIC to the FortiGate-VM, create as many subnets as the number of NICs before running the ps1 file.
  - c. A container to copy your FortiGate-VM image file
  - d. A blob where to create an OS and a data disk file to launch a FortiGate-VM instance
5. You must manually create security groups and route tables after deploying the FortiGate-VM, as the sample ps1 file does not create these.
6. Download the FortiGate-VM vhd image:
  - a. Go to [Customer Service & Support > Download > VM Images](#).
  - b. From the *Select Product* dropdown list, select *FortiGate*.
  - c. From the *Select Platform* dropdown list, select *Azure*.
  - d. Download the *FGT\_VM64\_AZURE-v6-buildXXXX-FORTINET.out.hyperv.zip* file.
  - e. Unzip the downloaded file. Place the *fortios.vhd* file in the C:\Azure\vhds directory. You can change the path using the \$sourceVhd parameter in the ps1 file.
7. Run the ps1 file. In this example, the filename is *fortigate-deploy-powershell.ps1*.

```
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator> .\fortigate-deploy-powershell.ps1
```

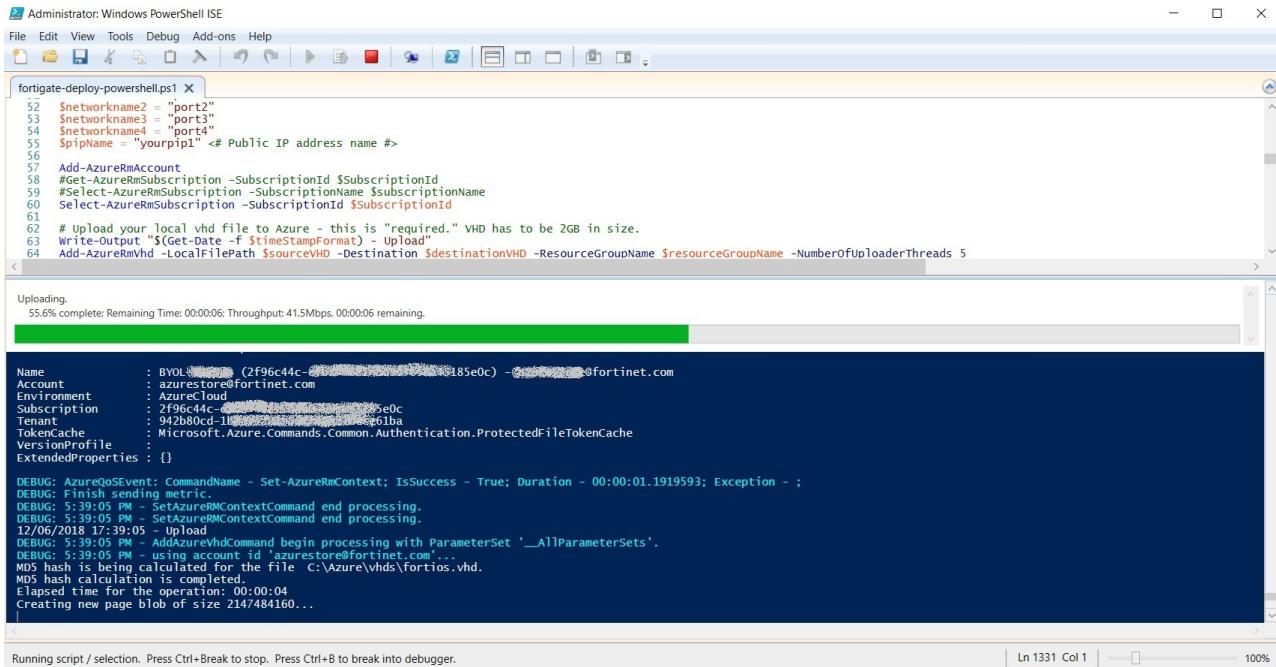
- a. The system prompts you for a number of network instances. Enter a number between 1 and 4.
- b. The system prompts you to log into Azure by entering your username and password. Enter your credentials.



- c. The execution continues. If you encounter an error (shown in red), resolve it, manually clean up newly generated files, then retry the execution. If you do not clean up the files, the next execution attempt results in an error. Manually clean up files by doing the following:
  - i. Remove files created in your container and blob under your storage account.
  - ii. Remove network resources created under your specified resource group.
  - iii. Diagnostic files are created under your storage account. Remove these files if they are unnecessary.

The sample ps1 file is provided for your reference. If you need to modify or author it as required by your organization, you are expected to be able to do so on your own.

## Deploying FortiGate-VM on Azure



```
Administrator:Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
fortigate-deploy-powershell.ps1 X
52 $networkname2 = "port2"
53 $networkname3 = "port3"
54 $networkname4 = "port4"
55 $ipName = "yourip1" <# Public IP address name #>
56
57 Add-AzureRmAccount
58 #Get-AzureRmSubscription -SubscriptionId $SubscriptionId
59 #Select-AzureRmSubscription -SubscriptionName $SubscriptionName
60 Select-AzureRmSubscription -SubscriptionId $SubscriptionId
61
62 # Upload your local vhd file to Azure - this is "required." VHD has to be 2GB in size.
63 Write-Output $(Get-Date -f $TimeStampFormat) -Upload"
64 Add-AzureRmVhd -LocalFilePath $sourceVHD -Destination $destinationVHD -ResourceGroupName $ResourceGroupName -NumberOfUploaderThreads 5

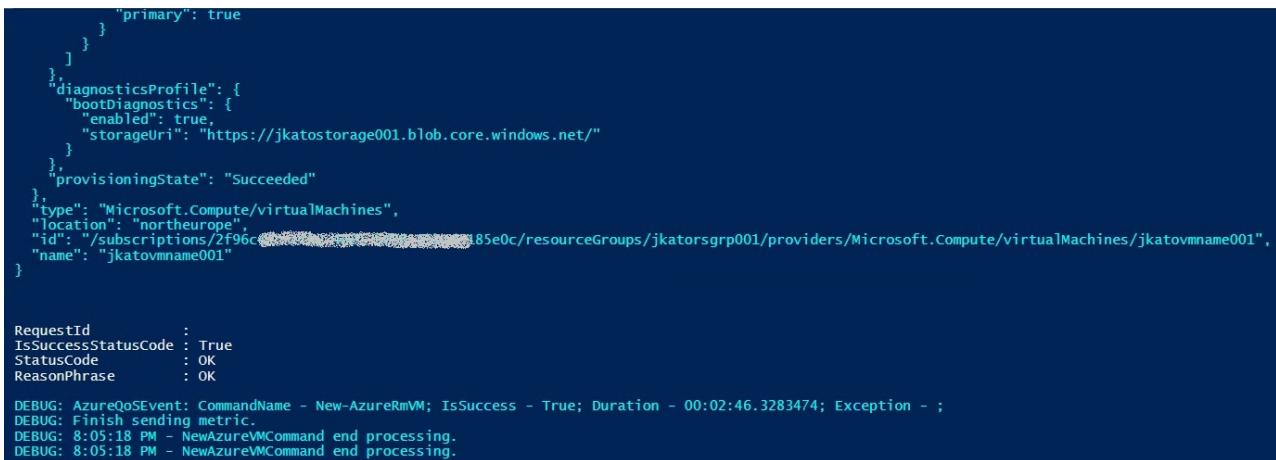
Uploading.
55.6% complete: Remaining Time: 00:00:06 Throughput: 41.5Mbps. 00:00:06 remaining.

Name          : BYOLVM001 (2f96c44c-0000-0000-0000-000000000000) - jkatov@fortinet.com
Account       : azurestore@fortinet.com
Environment   : AzureCloud
Subscription  : 2f96c44c-0000-0000-0000-000000000000
Tenant        : 942b80cd-1b00-4e00-8661-000000000000
TokenCache    : Microsoft.Azure.Commands.Common.Authentication.ProtectedFileTokenCache
VersionProfile: 
ExtendedProperties: {}

DEBUG: AzureQoSEvent: CommandName - Set-AzureRmContext; IsSuccess - True; Duration - 00:00:01.1919593; Exception - ;
DEBUG: Finish sending metric.
DEBUG: 5:39:05 PM - SetAzureRMContextCommand end processing.
DEBUG: 5:39:05 PM - SetAzureRMContextCommand end processing.
12/06/2017 8:05:05 PM - Upload
DEBUG: 5:39:05 PM - Add-AzureVhdCommand begin processing with ParameterSet 'AllParameterSets'.
DEBUG: 5:39:05 PM - using account id 'azurestore@fortinet.com'.
MD5 hash is being calculated for the file C:\Azure\vhds\fortios.vhd.
MD5 hash calculation is completed.
Elapsed time for the operation: 00:00:04
Creating new page blob of size 2147484160...
|
```

Running script / selection. Press Ctrl+Break to stop. Press Ctrl+B to break into debugger.

Execution takes about ten minutes to complete.



```

    "primary": true
  }
]
},
"diagnosticsProfile": {
  "bootDiagnostics": {
    "enabled": true,
    "storageUri": "https://jkatostorage001.blob.core.windows.net/"
  }
},
"provisioningState": "Succeeded"
},
"type": "Microsoft.Compute/virtualMachines",
"location": "northeurope",
"id": "/subscriptions/2f96c44c-0000-0000-0000-000000000000/resourceGroups/jkatorsgrp001/providers/Microsoft.Compute/virtualMachines/jkatovmname001",
"name": "jkatovmname001"
}

RequestId      :
IsSuccessStatusCode : True
StatusCode      : OK
ReasonPhrase    : OK

DEBUG: AzureQoSEvent: CommandName - New-AzureRmVM; IsSuccess - True; Duration - 00:02:46.3283474; Exception - ;
DEBUG: Finish sending metric.
DEBUG: 8:05:18 PM - NewAzureVMCommand end processing.
DEBUG: 8:05:18 PM - NewAzureVMCommand end processing.
```

## Deploying FortiGate-VM on Azure

### 8. Access the FortiGate-VM after executing the ps1 file:

- Navigate to the resource group and click the specified VM name.

NAME	TYPE	LOCATION
jkatostorage001	Storage account	North Europe
jkatovmname001	Virtual machine	North Europe
jkatovnet001	Virtual network	North Europe
port1	Network interface	North Europe
port2	Network interface	North Europe
yourpip1	Public IP address	North Europe

- Click the FortiGate-VM hostname and find its public IP address.

Resource group [\[change\]](#)  
jkatorsgrp001

Status  
Running

Location  
North Europe

Subscription (change)  
BYOL [change]

Subscription ID  
2f96c44c-  
5e0c

Computer name  
jkatovmname001

Operating system  
Linux

Size  
Standard F1 (1 vcpus, 2 GB memory)

Public IP address  
137.116.235.185

Virtual network/subnet  
jkatovnet001/jkatosubnet001

DNS name  
Configure

Tags (change)  
Click here to add tags

Show data for last: 1 hour 6 hours 12 hours 1 day 7 days 30 days

CPU (average) Network (total)

- In a browser, access <https://<public IP address>>. Enter the admin username and password specified in the ps1

file to log in.



## Bootstrapping the FortiGate CLI and BYOL license at initial bootup using user data

This section explains how to add bootstrapping of FortiGate CLI commands and BYOL license at the time of initial bootup as part of PowerShell deployment.

It is expected that you have thorough knowledge of PowerShell and various Azure services and features to adopt this deployment method. You should be able to author a ps1 file on your own as required by your organization.

You can find a sample PowerShell script that works with bootstrapping on [GitHub](#).

### To bootstrap the FortiOS CLI and BYOL license at initial bootup using user data:

1. Create a directory on your PC with the path C:\Azure\misc.
2. Create a MIME text file named azureinit.conf in the C:\Azure\misc directory. You can change the directory path and file name using the \$customdataFile = C:\Azure\misc\azureinit.conf parameter in the ps1 file. azureinit.conf is the text file in MIME format that includes both FortiGate CLI commands and license file content. You can download a sample azureinit.conf from [GitHub](#).
3. You can download a license file from [Customer Service & Support](#) after registering your product code. Copy and paste the content of your license file to replace the license portion of azureinit.conf. FortiGate-VM license content resembles the following:

```
-----BEGIN FGT VM LICENSE-----
QAAAABUjZtrwJdUje/8C5dNVn0mVYlw70ZlwXPPTG7Vm2KKwYyL4+qL0gED6/q
SQSPKwpTF1XjAuRGtGyX1vTaTpXgGQA1pwFdJnS6TwJ6vt7K1d8ncuaa3bCw
s8XpmL1zvje4//+c9nqh4fN/KyDweE1pDMalsOcm0B0rU8H01Dkx+rgceCs3QZ5
ELStRnvX11/oXqT8/gor657ZdybxlvzPwvWJDYSSAsT+QK8BHJ+xFhLjhkzbZ4eZU
Hd01ICSm7WEVY5kaud43sZ9XE5txPEInah3yXgtId24pnV683G4EHCKAdGyMTP
QqdqBMcKt5aei0ooGAOX8D62C52jh+r1+tkdpR5YHoVYZHU95hBCNjBrozbhmkNk
NogYuadQeh28MDtpvzxnb24mlfDQMTjysQuCtwzJzimBnvSbo7XNq/irTs20nfB
N03p1zy77MDguxpCB/3ve18qAxoqbLS7aQHQ7qNURL25Mdwcfd11Abfz7TM0
bnRWhz3n5VJUIp+eIf1v84yfwccJ1+IZAPohql3DGBt4uvRFV6yndV13wZG6h
eV4LIHKJ5T25/b14m9I fqEXEsSKKKPn7H2wdyroBdw+VLnT9Hk+3Ht3Tl29AZ+
+DMERh+Bo0WnHG3y5do6B+Wi+CIuxqmIIaoLnDyH5bcGU92/GApufF08dI
+3DNLc6ZkDpqfj2t179dHoIVxG6SBu5C6131OsSwJhg+r6x+YAfP0/ktuIvh
NeAFiJveJrbZBJAu1qnjzNc9Wt7Rg9lvdNvwVK16Afop2Kt+icfxRL1gySqwdo
b56XyJbIqAwb/JLa6EkmZDrn3swQ4H9K
-----END FGT VM LICENSE-----
```

4. In the example ps1 file, the FortiGate CLI command is shown as the following:

```
config system global
set timezone 03
end
```

This example sets the timezone as GMT-9 Alaska. You can replace these lines with your own set of CLI commands.

5. After editing the sample ps1 file to reflect your own Azure environments and azureinit.conf file as required, run the ps1 file. It reads the conf file and passes FortiGate CLI commands and the license to the FortiGate-VM deployment using cloud-init user data.
6. After the ps1 file execution ends, log into the FortiGate by accessing [https://<IP\\_address>](https://<IP_address>) in your browser.
7. The system displays the dashboard instead of a license upload window, since the license is already activated.

The screenshot shows the FortiGate VM64-Azure dashboard. The left sidebar has a 'Main' section with links to Security Fabric, FortiView, Network, System, Policy & Objects, Security Profiles, VPN, and User & Device. The main area is divided into three sections: 'System Information' (Hostname: jkatovmname001, Serial Number: FGVM000000161405, Firmware: v6.0.3 build0200 (GA), Mode: NAT (Flow-based), System Time: 2018/12/06 22:51:45, Uptime: 00:00:02:21, WAN IP: Unknown), 'Licenses' (FortiCare Support, Firmware & General Updates, IPS, AntiVirus, Web Filtering), and 'Virtual Machine' (FGVM00 License, Allocated vCPUs: 1 / 1, 100%, Allocated RAM: 2 GiB).

To see how bootstrapping went, check if the command was successfully run. Open the CLI console and enter `diag cloudinit show`.

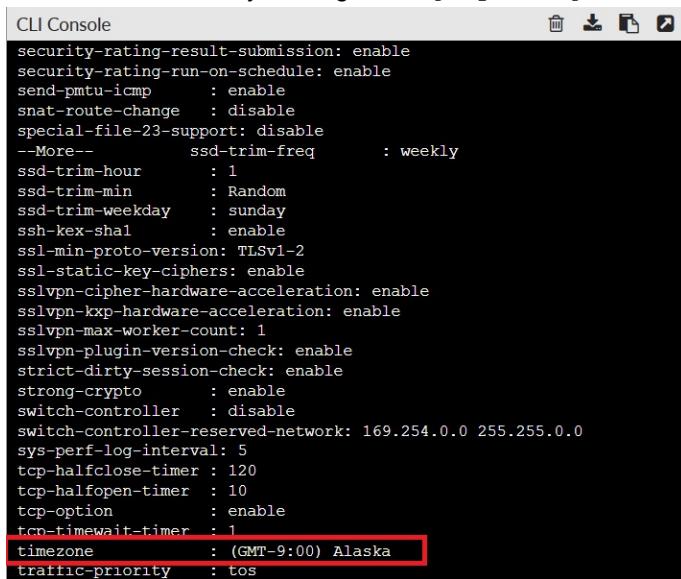
If the cloud-init was run successfully, the CLI shows Azure customdata processed successfully.

The screenshot shows the CLI Console with the message 'Connected'. The command `diag cloudinit show` is entered, and its output is displayed in a red box. The output shows the process of checking metadata source, waiting for customdata files, finding the file, decrypting it, parsing config and VM license scripts, and running them. The final step shows the configuration of system global settings (timezone 03) being applied.

```
jkatovmname001 # diag cloudinit show
>> Checking metadata source azure
>> Azure waiting for customdata file
>> Azure waiting for customdata file
>> Azure waiting for customdata file
>> Azure customdata file found
>> Azure cloudinit decryp successfully
>> MIME parsed config script
>> MIME parsed VM license
>> Azure customdata processed successfully
>> Run config script
>> Finish running script
>> jkatovmname001 $ config system global
>> jkatovmname001 (global) $ set timezone 03
>> jkatovmname001 (global) $ end
```

If you see an error with this `diagnose` command, resolve it and try again by editing `azureinit.conf`. There may be a syntax error.

8. Check the timezone by running `config system global` and `get` commands.



```

CLI Console
security-rating-result-submission: enable
security-rating-run-on-schedule: enable
send-pmtu-icmp : enable
snat-route-change : disable
special-file-23-support: disable
--More--      ssd-trim-freq : weekly
ssd-trim-hour : 1
ssd-trim-min : Random
ssd-trim-weekday : sunday
ssh-kex-sha1 : enable
ssl-min Proto-version: TLSv1-2
ssl-static-key-ciphers: enable
sslypn-cipher-hardware-acceleration: enable
sslypn-kxp-hardware-acceleration: enable
sslypn-max-worker-count: 1
sslypn-plugin-version-check: enable
strict-dirty-session-check: enable
strong-crypto : enable
switch-controller : disable
switch-controller-reserved-network: 169.254.0.0 255.255.0.0
sys-perf-log-interval: 5
tcp-halfclose-timer : 120
tcp-halfopen-timer : 10
tcp-option : enable
tcp-timewait-timer : 1
timezone : (GMT-9:00) Alaska
traffic-priority : tos

```

The timezone was changed to Alaska as expected, meaning that the bootstrapping CLI command was successful. This assumes that you used the default FortiGate CLI command in step 4. If you modified the command, test it accordingly.

## Deploying FortiGate-VM from the marketplace

### To deploy FortiGate-VM from the marketplace:

1. In the Azure marketplace, search for and select Fortinet FortiGate Next-Generation Firewall.
2. From *Select a plan*, select the desired deployment plan. Click *Create*.
3. On the *Basics* tab, configure the parameters according to your requirements:
  - a. From the *Subscription* dropdown list, select your subscription.
  - b. In *Resource group*, select an existing resource group or create a new one.
  - c. From the *Region* dropdown list, select the desired region.
  - d. In the *FortiGate administrative username* and *password* fields, enter the username and password for the FortiGate administrative profile.
  - e. In the *Fortigate Name Prefix* field, assign a naming prefix for your FortiGate resources.
  - f. From the *Fortigate Image SKU* dropdown list, select BYOL or PAYG.
  - g. From the *Fortigate Image Version* dropdown list, select the FortiGate version to deploy.

**h. Click *Next: Instance Type >*.**

Home > Fortinet FortiGate Next-Generation Firewall (preview) >  
Create Fortinet FortiGate Next-Generation Firewall ...

Basics Instance Type Networking Public IP Advanced Review + create

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

Subscription \* ⓘ PAYG-DevOps

Resource group \* ⓘ Create new

**Instance details**

Region \* ⓘ East US

FortiGate administrative username \* ⓘ

FortiGate password \* ⓘ

Confirm password \* ⓘ

Fortigate Name Prefix \* ⓘ

Fortigate Image SKU ⓘ Bring Your Own License

Fortigate Image Version ⓘ latest

**Review + create** < Previous **Next : Instance Type >**

4. On the *Instance Type* tab, select an appropriately sized instance type. Click *Next: Networking >*.
5. On the *Networking* tab, configure the parameters according to your requirements:
  - a. In *Virtual network*, select an existing VNet or create a new one. The FortiGate-VM requires a public and private interface for Internet edge protection.
  - b. Enable or disable *Accelerated Networking*, which refers to SR-IOV support. This depends on the instance type that you selected.
  - c. Click *Next: Public IP >*.
6. On the *Public IP* tab, create a new public IP address or create a new one. Click *Next: Advanced >*.
7. On the *Advanced* tab, configure the parameters according to your requirements:
  - a. If you want FortiManager to manage this FortiGate, enable *Connect to FortiManager* and provide the FortiManager IP address and serial number in the *FortiManager IP address* and *FortiManager Serial Number* fields.
  - b. If you want to provide initial configuration to the FortiGate, enter the desired commands in the *Custom Data* field. These commands are executed during initial bootup.

## Deploying FortiGate-VM on Azure

Home > Fortinet FortiGate Next-Generation Firewall >  
Create Fortinet FortiGate Next-Generation Firewall ...

Basics Instance Type Networking Public IP Advanced Review + create

FortiManager  
Connect to FortiManager

Connect to FortiManager \*  yes  no

FortiManager IP address

FortiManager Serial Number

Custom Data  
Pass a configuration file into the virtual machine while it is being provisioned. This is additional to the configuration for this architecture.

Custom Data  Add you required additional configuration here.

**i** The default configuration already included in this deployment can be found on our github page. [View](#)

- c. To provide a BYOL license file for the FortiGate, upload it using the *FortiGate License* field. The license file is ignored if you selected PAYG in step 3. Click *Next: Review + create* >.
8. Once validation completes, confirm all values, then click *Create*. Azure creates the resources accordingly.

## Deploying FortiGate-VM on regional Azure clouds

In addition to "global" Azure support, FortiGate-VM supports "regional" Azure support, including China, Germany, and U.S. Gov. FortiGate-VM deployment on regional Azure clouds requires dedicated subscription accounts as they are not covered by global Azure and services are run under URL domains unique to the regional Azure cloud.

FortiGate-VM is not available on regional Azure cloud marketplaces. Instead, you can deploy FortiGate-VM (BYOL) having a VHD file ready and instantiating a FortiGate-VM instance using your PowerShell or ARM deployment templates by pointing to the VHD file.

You can download the VHD file from [Fortinet Customer Service & Support](#). Go to *Download > VM Image*, then select *FortiGate* as the *Product* and *Azure* for the *Platform*. The file name is FGT\_VM64\_AZURE-v6-buildXXXX-FORTINET.out.hyperv.zip, where XXXX is the build number.

Once the download is complete, unzip the file and locate the fortios.vhd file. Upload the fortios.vhd file to your blob/storage location as required by your deployment templates.

## Enabling accelerated networking on the FortiGate-VM

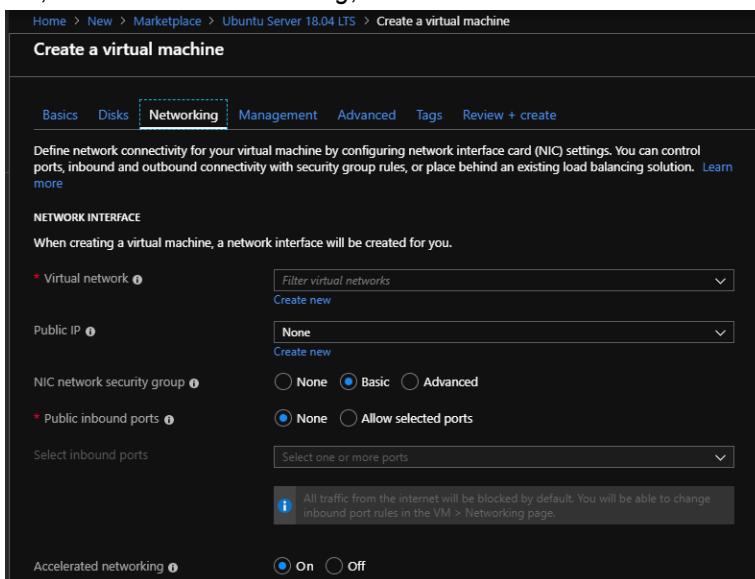
Azure supports SR-IOV, which accelerates networking by allowing VM NICs to bypass the hypervisor and go directly to the PCIe card underneath. FortiOS must understand when it is using SR-IOV and change networking to accommodate SR-IOV.

Azure refers to SR-IOV as *Accelerated Networking*. You can check if it is enabled by checking the NIC attached to the VM through the GUI or CLI.

This feature is available for FortiOS 6.2.1 and later versions.

### To configure accelerated networking:

1. You can enable accelerated networking when instantiating a new VM, or enable it after the VM has been created.  
Do one of the following:
  - a. To enable accelerated networking using the GUI, create a new VM or select an existing VM. On the *Networking* tab, for *Accelerated networking*, select *On*.



- b. To enable accelerated networking using the CLI:

```
root@mail:/home/azure/images# az network nic update -g <Resource group name> -n <NIC Name> --accelerated-networking true
{
  "dnsSettings": {
    "appliedDnsServers": [],
    "dnsServers": [],
    "internalDnsNameLabel": null,
    "internalDomainNameSuffix": "k41kcrl04yeezbyeswqimbxshb.fx.internal.cloudapp.net",
    "internalFqdn": null
  },
  "enableAcceleratedNetworking": true,
```

On the FortiOS side, a virtual interface is created in the format of sriovslv(number) for each NIC that has accelerated networking enabled:

```
<VM name> # fnsysctl ifconfig
port1 Link encap:Ethernet HWaddr 00:0D:3A:B4:87:70
        inet addr:172.29.0.4 Bcast:172.29.0.255 Mask:255.255.255.0
                UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                RX packets:5689 errors:0 dropped:0 overruns:0 frame:0
                TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
                collisions:0 txqueuelen:1000
                RX bytes:1548978 (1.5 MB) TX bytes:0 (0 Bytes)
sriovslv0 Link encap:Ethernet HWaddr 00:0D:3A:B4:87:70
        UP BROADCAST RUNNING SLAVE MULTICAST MTU:1500 Metric:1
        RX packets:35007 errors:0 dropped:0 overruns:0 frame:0
```

```
TX packets:33674 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:34705194 (33.1 MB) TX bytes:10303956 (9.8 MB)
```

The NIC shows the driver as `hv_netvsc` with accelerated networking enabled or disabled:

```
<VM name> # diagnose hardware deviceinfo nic port1  
Name: port1  
Driver: hv_netvsc
```

The FortiOS GUI does not display the virtual interface:

	Status	Name	Members	IP/Netmask	Type	Access	Ref.
Physical (2)		port1		172.29.0.4/255.255.255.0	Physical Interface	PING HTTPS SSH FMG-Access	0
		port2		0.0.0.0.0/0.0.0.0	Physical Interface		0

To check if accelerated networking is enabled using the GUI:

1. In the Azure management console, go to the desired VM, then *Networking*.
2. Select the desired NIC. In this example, accelerated networking is shown as enabled.

To check if accelerated networking is enabled using the CLI:

```
root@mail:/home/azure/images# az network nic show -g <Resource group name> -n <NIC name>
```

Check that the following displays as part of the output: "enableAcceleratedNetworking": true,

## Upgrading FortiOS

For the recommended upgrade path, see [Upgrade Path Tool](#). For PAYG, select *FortiGate-VM-AZUREONDEMAND*. For BYOL, select *FortiGate-VM-AZURE*. Select the current and target upgrade versions to see the upgrade path.

# Deploying autoscaling on Azure

You can deploy FortiGate virtual machines (VMs) to support autoscaling on Azure. Existing resources can be included when specified during the deployment. By integrating FortiAnalyzer, you can consolidate logging and reporting for your FortiGate cluster. Fortinet provides a FortiGate Autoscale for Azure deployment package to facilitate the deployment.

Multiple FortiGate-VM instances form a Virtual Machine Scale Sets (VMSS) to provide highly efficient clustering at times of high workloads. FortiGate Autoscale for Azure incorporates one or more VMSS, network related components, and Azure Function App scripts. FortiGate-VM instances are scaled out automatically according to predefined workload levels. When a spike in traffic occurs, FortiGate instances are automatically added to the VMSS. Autoscaling is achieved by using FortiGate-native high availability (HA) features such as `config-sync`, which synchronizes operating system (OS) configurations across multiple FortiGate-VM instances at the time of scale-out events.

FortiGate Autoscale for Azure is available with FortiOS 6.4.5 and supports any combination of On-Demand (PAYG) and Bring Your Own License (BYOL) instances.

FortiAnalyzer 6.2.5 or FortiAnalyzer 6.4.5 can be incorporated into Fortinet FortiGate Autoscale to use extended features that include storing logs into FortiAnalyzer.

# Prerequisites

Installing and configuring FortiGate Autoscale for Azure requires knowledge of the following:

- Configuring a FortiGate using the CLI
- Azure deployment templates
- Azure Functions

It is expected that FortiGate Autoscale for Azure will be deployed by DevOps engineers or advanced system administrators who are familiar with the above.

## Before you begin

Before starting the deployment, the following steps must be carried out:

1. Log into your Azure account. If you do not already have one, [create one](#) by following the on-screen instructions.
2. [Create a service principal](#) for Autoscale to interact with the different Azure services. The creation of the service principal may be done by a different Azure account.

The service principal requires *read* and *write* permissions which can be granted by adding the *Contributor* role to the service principal. In order to grant the service principal such permissions, the Azure account used to create the service principal requires the following permissions:



- *Microsoft.Authorization/roleAssignments/write* (to add role assignments)
- *Microsoft.Authorization/roleAssignments/delete* (to remove role assignments)

These permissions are included in the roles *User Access Administrator* and *Owner*. For details, refer to the Microsoft article [Add or remove role assignments using Azure RBAC and the Azure portal](#).

Note the following items as you need them to deploy the Function App:

Item	Where to find it	Relevant FortiOS parameter
Application ID	You can find this item in Azure Active Directory > App registrations > (your app).	Service Principal App ID on page 53
Application secret	Only appears once. You cannot retrieve the application secret.	Service Principal App Secret on page 53
Object ID	Open the Azure CLI and enter the command <code>az ad sp show --id &lt;the service principal client id&gt;</code> . The object ID displayed may differ from the object ID displayed in Azure Active Directory > App registrations > (your-app). Use the value from the AzureCLI.	Service Principal Object ID on page 53

For details on the FortiOS parameters, see [Configurable variables on page 49](#).

3. Confirm that you have a valid subscription to the [PAYG and/or BYOL marketplace listings](#) for FortiGate, as required for your deployment.



Without the valid subscriptions, the deployment will fail with errors.

## Requirements when using an existing VNet

When using an existing VNet, ensure that the following FortiGate Autoscale for Azure requirements have been satisfied.

- IP address ranges in the VNets satisfy the Microsoft requirements listed in the article [What address ranges can I use in my VNets?](#)
- The VNet must contain 4 subnets.
  - The FortiGate VMSS will be deployed in one of the subnets. This subnet must:
    - be a clean subnet (i.e. is not used by any other resource.)
    - have two service endpoints that have been manually enabled, one for *Microsoft.AzureCosmosDB*, and one for *Microsoft.Web*.
    - should have its name specified in the [Subnet 1 Name on page 54](#) parameter.
  - The 3 other subnets will be protected by the FortiGate VMSS.
- Route tables have been created to route traffic between the FortiGate VMSS subnet and the other subnets.
- One network security group is associated with the 4 subnets in the VNet.
- (Optional) One available (i.e. not associated with any resource) public IP address to be used for the external load balancer that will be created during template deployment.
  - This IP address must be of the 'standard' SKU in order to match the VMSS.
  - This requirement is optional as a new IP address can be created during template deployment, as specified by the [Frontend IP Deployment Method on page 51](#) parameter.
- All of the above components above reside in the same resource group.

## Obtaining the deployment package

The FortiGate Autoscale for Azure deployment package is located in the Fortinet Autoscale for Azure [GitHub project](#). Navigate to the [project release page](#) and download `fortigate-autoscale-azure.zip` for the latest version.

Unzip this file on your local PC. Extracted content used in the deployment is described below:

Extracted Item	Description
assets	This folder contains <code>configset</code> files which can be modified as needed to meet your network requirements. For details on the allowable modifications, refer to the bullet for <i>The Blob Containers</i> in the section <a href="#">Appendix &gt; Major components on page 74</a> . In the section <a href="#">Uploading files to the Storage account on page 55</a> these files are loaded as the initial configuration of a new FortiGate-VM instance.
templates	This folder contains deployment templates. The files <code>deploy_fortigate_azure_autoscale.hybrid_licensing.*</code> are used to deploy FortiGate Autoscale for Azure.
<code>fortigate-autoscale-azure-funcapp.zip</code>	This is the function source file. This file should be uploaded to a file host online so that it is accessible to Azure. During the deployment you will specify the URL to this file in the parameter <a href="#">Package Res URL on page 53</a> .

# Deploying FortiGate Autoscale for Azure

Deploying FortiGate Autoscale for Azure involves [Creating a template deployment on page 45](#) and [Uploading files to the Storage account on page 55](#).

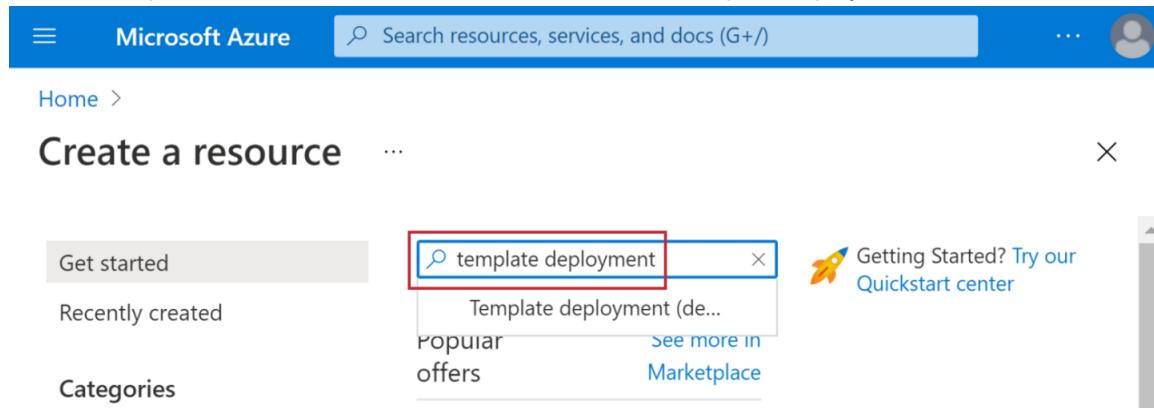
## To deploy FortiGate Autoscale for Azure:

1. Create a template deployment using the template file `deploy_fortigate_autoscale.hybrid_licensing.json` and the parameter file `deploy_fortigate_autoscale.hybrid_licensing.params.json`.
2. Upload configset files to the Storage account.
3. If you will be using BYOL instances, upload license files to the Storage account.
4. Verify the deployment as described in the section [Verifying the deployment on page 57](#).
5. Start the VMSS as described in the section [Starting a VMSS on page 65](#).

## Creating a template deployment

### To create a template deployment:

1. In the Azure portal, select *Create a resource* and search for "Template deployment".



2. Click **Create**.

The screenshot shows the Microsoft Azure Marketplace interface. At the top, there is a search bar with the placeholder "Search resources, services, and docs (G+/-)" and a user profile icon. Below the search bar, the breadcrumb navigation shows "Home > Create a resource > Marketplace". The main title "Marketplace" is displayed with a close button "X". On the left, a sidebar lists "Recently created", "Service Providers", and "Private Offers + Plans". Under "Categories", "Get Started" is highlighted, while "AI + Machine Learning", "Analytics", and "Blockchain" are listed below. A search filter bar at the top right contains a search icon, the text "template deployment", a clear button "X", and a "Add filter" button. The main content area displays the results for "template deployment", stating "Showing results for 'template deployment'." and "Showing 1 to 20 of 58 results.". The first result is "Template deployment (deploy using custom templates)" by Microsoft, categorized as an "Azure Service". It includes a description: "Customize your template and build for the cloud". A "Create" button is visible, which is highlighted with a red border in the screenshot.

3. Click **Build your own template in the editor**.

The screenshot shows the "Custom deployment" template creation page in the Microsoft Azure Marketplace. The top navigation is identical to the previous screenshot. The main title is "Custom deployment" with a close button "X". Below it, the sub-title "Deploy from a custom template" is shown. At the top, there are three tabs: "Select a template" (which is underlined), "Basics", and "Review + create". A descriptive text states: "Automate deploying resources with Azure Resource Manager templates in a single, coordinated operation. Create or select a template below to get started." followed by a link "Learn more about template deployment". At the bottom, a button labeled "Build your own template in the editor" is highlighted with a red border and a pencil icon.

4. Click *Load file* to load the provided template file; then click *Save*.

The screenshot shows the Microsoft Azure portal interface for editing an ARM template. At the top, there's a blue header bar with the Microsoft Azure logo, a search bar, and a user profile icon. Below the header, the breadcrumb navigation shows: Home > Create a resource > Marketplace > Custom deployment >. The main title is "Edit template". On the left, there are three buttons: "+ Add resource", "Quickstart template", and "Load file" (which is highlighted with a red box). Below these are sections for "Parameters (0)", "Variables (0)", and "Resources (0)". The central area contains a code editor with the following JSON template:

```

1  {
2    "$schema": "https://schema.management.
3    azure.com/schemas/2019-04-01/
4    deploymentTemplate.json#",
5    "contentVersion": "1.0.0.0",
6    "parameters": {},
7    "resources": []
}

```

At the bottom, there are two buttons: "Save" (highlighted with a red box) and "Discard".

5. (Optional) In the *Custom deployment* screen, click *Edit parameters*.

The screenshot shows the Microsoft Azure portal interface for a custom deployment. The title is "Custom deployment". The breadcrumb navigation is identical to the previous screen: Home > Create a resource > Marketplace >. Below the title, it says "Deploy from a custom template". There are three tabs at the top: "Select a template", "Basics" (which is underlined), and "Review + create". Under "Template", there are four options: "Customized template" (with a preview icon and "22 resources"), "Edit template" (with a pencil icon), "Edit parameters" (which is highlighted with a red box), and "Visualize".

Click *Load file* to load a predefined `.params.json` file; then click *Save*.

The screenshot shows the 'Edit parameters' step in the Azure portal. At the top, there's a navigation bar with 'Microsoft Azure', a search bar, and a user profile icon. Below it, the breadcrumb path is 'Home > Create a resource > Marketplace > Custom deployment >'. The main title is 'Edit parameters' with a close button 'X'. Underneath, there are two buttons: 'Load file' (highlighted with a red box) and 'Download'. A code editor displays a JSON template:

```

1  {
2    "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentParameters.json#",
3    "contentVersion": "1.0.0.0",
4    "parameters": {

```

At the bottom are 'Save' and 'Discard' buttons.

**6.** Review and update parameters; then click *Review + create*.

The screenshot shows the 'Custom deployment' step in the Azure portal. At the top, there's a navigation bar with 'Microsoft Azure', a search bar, and a user profile icon. Below it, the breadcrumb path is 'Home > Create a resource > Marketplace >'. The main title is 'Custom deployment' with a close button 'X'. It says 'Deploy from a custom template' and shows a 'Customized template' section with 22 resources. There are three buttons: 'Edit template', 'Edit parameters' (highlighted with a red box), and 'Visualize'. The 'Project details' section asks to select a subscription and resource group. The 'Subscription' dropdown shows 'FortiGate Autoscale'. The 'Resource group' dropdown shows 'FortiGate Autoscale' with a 'Create new' link. The 'Instance details' section asks for a region, with 'Europe West' selected. At the bottom are 'Review + create' (highlighted with a red box), '< Previous', and 'Next : Review + create >' buttons.

*Project details* are described as follows:

- **Subscription:** The Azure subscription FortiGate Autoscale for Azure will be deployed in.
- **Resource group:** The resource group FortiGate Autoscale for Azure will be deployed in. In the section [Configurable variables on page 49](#), this will be referred to as the *Autoscale resource group*.

Parameters under *Instance details* are described in the section [Configurable variables on page 49](#).

**7.** If parameter validation has not passed, click *Previous* and make the necessary corrections.

8. Review the Azure Marketplace Terms, optionally review the parameters again, and click *Create*.

The screenshot shows the Microsoft Azure portal interface for a custom deployment. At the top, there's a blue header bar with the Microsoft Azure logo, a search bar, and a user profile icon. Below the header, the breadcrumb navigation shows: Home > Create a resource > Marketplace > Custom deployment. The main title is "Custom deployment" with a subtitle "Deploy from a custom template". A green banner at the top indicates "Validation Passed". Below the banner, there are three tabs: "Select a template", "Basics", and "Review + create", with "Review + create" being the active tab. Under "Review + create", there are sections for "Summary" (Customized template, 22 resources) and "Terms" (links to Azure Marketplace Terms and Azure Marketplace). A large text block details the terms of service for creating the deployment. At the bottom, there are three buttons: "Create" (highlighted with a red border), "< Previous", and "Next".

## Configurable variables

Following is a list of variables used during deployment and referenced throughout this guide.

Parameter name	Default value	Description
Region	Requires input	The region in which the FortiGate Autoscale for Azure resources will be deployed in. Not every resource is available in every region.

Parameter name	Default value	Description
Access Restriction IP Range	Requires input	<p>Specify IP ranges (single IPv4 address or Classless Inter-Domain Routing (CIDR) range) to allow access from the Internet or from your on-premises network to the CosmosDB and Function App. Specify at least one entry for security purposes. For multiple entries, each entry must be separated by a comma and no trailing comma is allowed.</p> <p> 0.0.0.0/0 accepts connections from any IP address. We recommend that you use a constrained CIDR range to reduce the potential of inbound attacks from unknown IP addresses.</p>
Admin Password	Requires input	FortiGate administrator password on all VMs as well as the FortiAnalyzer if FortiAnalyzer integration is enabled. Must be between 11 and 26 characters and must include at least one uppercase letter, one lowercase letter, one digit, and one special character such as (! @ # \$ %).
Admin Username	azureadmin	FortiGate administrator username on all VMs as well as the FortiAnalyzer if FortiAnalyzer integration is enabled.
BYOL Instance Count	2	<p>The number of FortiGate instances the BYOL VMSS should have at any time. For High Availability in BYOL-only and Hybrid use cases, ensure at least 2 FortiGates are in the group. For specific use cases, set to 0 for PAYG-only, and &gt;= 2 for BYOL-only or hybrid licensing.</p> <p> Users can set the size to less than or equal to the number of valid licenses they own and the number should not exceed the <i>Max BYOL Instance Count</i>. Licenses can be purchased from FortiCare.</p>
FortiAnalyzer Autoscale Admin Password	Requires input	Password for the <a href="#">FortiAnalyzer Autoscale Admin Username on page 50</a> . The password must conform to the FortiAnalyzer password policy and have a minimum length of 8 and a maximum length of 128. If you need to enable KMS encryption, refer to the documentation.
FortiAnalyzer Autoscale Admin Username	Requires input	The name of the secondary administrator-level account in the FortiAnalyzer, which FortiGate Autoscale uses to connect to the FortiAnalyzer to authorize any FortiGate device in the Auto Scaling group. To conform to the FortiAnalyzer naming policy, the user name can only contain numbers, lowercase letters, uppercase letters, and hyphens. It cannot start or end with a hyphen (-).
FortiAnalyzer Custom Private IP Address	Requires input	The custom private IP address to be used by the FortiAnalyzer. Must be within the Public subnet 1 CIDR range. Required if <a href="#">FortiAnalyzer Integration Options on page 51</a> is set to 'yes'. If <a href="#">FortiAnalyzer Integration Options on page 51</a> is set to 'no', any input will be ignored.
FortiAnalyzer Instance Type	Requires input	Size of the FortiAnalyzer-VM.

Parameter name	Default value	Description
		 Not all instance types are supported. Review <a href="#">FortiAnalyzer instance type support</a> prior to selecting an instance.
FortiAnalyzer Integration Options	yes	Choose 'yes' to incorporate FortiAnalyzer into FortiGate Autoscale for Azure to use extended features that include storing logs into FortiAnalyzer.
FortiAnalyzer Version	6.4.5	FortiAnalyzer version supported by FortiGate Autoscale for Azure.
FortiGate PSK Secret	Requires input	The secret key used by FortiGate instances to securely communicate with each other. Must contain numbers and letters and may contain special characters. Maximum length is 128.
		 Changes to the PSK secret after FortiGate Autoscale for Azure has been deployed are not reflected here. For new instances to be spawned with the changed PSK secret, this environment variable will need to be manually updated.
FOS Version	6.4.5	FortiOS version supported by FortiGate Autoscale for Azure.
Frontend IP Deployment Method	create new public IP address	Deployment method for the Frontend Public IP address for the external load balancer. If set to 'create new public IP address', the IP address will be deployed to the resource group where the VNet is located. If set to 'use existing public IP address', the existing IP address must reside in the same resource group as the VNet and it must be of the 'standard' SKU in order to match the VMSS. Please refer to the section <a href="#">Requirements when using an existing VNet on page 44</a> .
Frontend IP Name	Requires input	Name of the Frontend Public IP address. When the <a href="#">Frontend IP Deployment Method on page 51</a> parameter is set to 'create new public IP address', this parameter can be left empty and a name will be generated.
Heart Beat Delay Allowance	30	The maximum amount of time (in seconds) allowed for network latency of the FortiGate heartbeat arriving at the Autoscale handler function. Minimum is 30.
Heart Beat Interval	60	The length of time (in seconds) that the FortiGate waits between sending heartbeat requests to the Autoscale handler function. Minimum is 30. Maximum is 120.
Heart Beat Loss Count	3	Number of consecutively lost heartbeats. When the Heart Beat Loss Count has been reached, the VM is deemed unhealthy and failover activities will commence.
Instance Type	Standard_F4	Size of the VMs in the VMSS. For assistance in choosing the size, refer to the Microsoft article <a href="#">Compute optimized virtual machine sizes</a> .

Parameter name	Default value	Description
Key Vault Name	Requires input	Name of the Key Vault to be used by FortiGate Autoscale. This parameter can be left empty and a name will be generated. If specified, the name must be globally unique and not belong to a Key Vault in the soft deleted state.
Load Balancer IP	10	The last octet of the Frontend Private IP address to be used by the Load Balancer. For example, if set to 10, the Private IP address for the Load Balancer in the subnet with prefix 10.0.1.0/24 would be 10.0.1.10.
Max BYOL Instance Count	2	<p>Maximum number of FortiGate instances in the BYOL VMSS.</p> <p>Maximum number of FortiGate instances in the BYOL VMSS. For specific use cases, set to 0 for PAYG-only, and <math>\geq 2</math> for BYOL-only or hybrid licensing. This number must be greater than or equal to the <a href="#">Min BYOL Instance Count on page 52</a>.</p>  <p>Users can set the size to match the number of valid licenses they own. Licenses can be purchased from FortiCare.</p>
Max PAYG Instance Count	6	<p>Maximum number of FortiGate instances in the PAYG VMSS. For specific use cases, set to 0 for BYOL-only, <math>\geq 2</math> for PAYG-only, and <math>\geq 0</math> for hybrid licensing. This number must be greater than or equal to the <a href="#">Min PAYG Instance Count on page 52</a>.</p>  <p>For BYOL-only and hybrid licensing deployments, this parameter must be at least 2. If set to 1 and the instance fails to work, the current FortiGate configuration will be lost.</p>
Min PAYG Instance Count	0	<p>Minimum number of FortiGate instances in the PAYG VMSS. For specific use cases, set to 0 for BYOL-only, <math>\geq 2</math> for PAYG-only, and <math>\geq 0</math> for hybrid licensing.</p>  <p>For PAYG-only deployments, this parameter must be at least 2. If it is set to 1 and the instance fails to work, the current FortiGate configuration will be lost.</p>
Network Security Group Name	Conditionally requires input	Name of the Network Security Group associated with the subnets in the VNet. Required when using an existing VNet. The value should match the name of the existing Network Security Group associated with the subnets in the VNet. When creating a new VNet, you may specify a name for the Network Security Group. If left empty, a name will be generated.

Parameter name	Default value	Description
PAYG Instance Count	0	The number of FortiGate instances the PAYG VMSS should have at any time. For High Availability in a PAYG-only use case, ensure at least 2 FortiGates are in the group. For specific use cases, set to 0 for BYOL-only, >= 2 for PAYG-only, and >= 0 for hybrid licensing.
Package Res URL	Requires input	The public URL of the function source file named <code>fortigate-autoscale-azure-funcapp.zip</code> , and can be found inside <code>fortigate-autoscale-azure.zip</code> . The public URL of the deployment package zip file that contains the resource used to deploy the Function App. The default URL points to the GitHub release corresponding to this ARM template contentVersion.
		 This URL must be accessible by Azure.
Primary Election Timeout	90	The maximum time (in seconds) to wait for the election of the primary instance to complete.
Resource Name Prefix	Requires input	The prefix for all applicable resource names. Can only contain lowercase letters and numbers. Maximum length is 10.
Scale In Threshold	20	Percentage of CPU utilization at which scale-in should occur.
Scale Out Threshold	80	Percentage of CPU utilization at which scale-out should occur.
Service Plan Tier	Premium (P1V2)	The pricing tier for the function service plan.
		 The Free plan is for trial and demo only. Do not use it in a production environment.
Service Principal App ID	Requires input	<p><i>Application ID</i> for the Registered app used as the Autoscale Function App API request service principal.</p> <p>This is the value that was noted when creating a service principal in the section <a href="#">Prerequisites on page 43</a>.</p>
Service Principal App Secret	Requires input	<p>Password (<i>Authentication key</i>) for the Registered app used as the Autoscale Function App API request service principal.</p> <p>This is the value that was noted when creating a service principal in the section <a href="#">Prerequisites on page 43</a>.</p>
Service Principal Object ID	Requires input	<p><i>Object ID</i> for the Registered app used as the Autoscale Function App API request service principal.</p> <p>This is the value that was noted when creating a service principal in the section <a href="#">Prerequisites on page 43</a>.</p>
Storage Account Type	Standard_LRS	Storage account type.

Parameter name	Default value	Description
Subnet 1 Name	Conditionally requires input	
Subnet 2 Name	Conditionally requires input	The <i>Subnet # Name</i> parameters specify the name of the subnet. <ul style="list-style-type: none"> <li><i>Subnet 1</i> is the subnet in which to deploy the FortiGate VMSS.</li> <li><i>Subnets 2-4</i> are the subnets to be protected by the FortiGate.</li> </ul>
Subnet 3 Name	Conditionally requires input	
Subnet 4 Name	Conditionally requires input	 Required when using an existing VNet. Values should match the subnet of the target VNet. When creating a new VNet, any input value will be ignored.
Subnet 1 Address Range	10.0.0.0/24	The <i>Subnet # Address Range</i> parameters define the address range for the subnet, in CIDR notation. The address range must be contained by the address space of the virtual network as defined in <a href="#">VNet Address Space on page 54</a> . After deployment, the address range of a subnet which is in use can't be edited.
Subnet 2 Address Range	10.0.1.0/24	
Subnet 3 Address Range	10.0.2.0/24	
Subnet 4 Address Range	10.0.3.0/24	 Required when using an existing VNet. Values should match the address range of the target VNet. When creating a new VNet, any input value will be ignored.
VNet Address Space	10.0.0.0/16	IP address space of the VNet in CIDR notation. E.g. 10.0.0.0/16. Required when using an existing VNet; the value should match the address space of the target VNet.
VNet Deployment Method	create new	Options for Virtual Network (VNet) deployment: <ul style="list-style-type: none"> <li>create new</li> <li>use existing</li> </ul>
		 The VNet resource group (specified in the <a href="#">VNet Resource Group Name on page 54</a> parameter) must be in the same region as the Autoscale resource group (specified in the <i>Resource group</i> parameter). If using an existing VNet, refer to the section <a href="#">Requirements when using an existing VNet on page 44</a> .
VNet Name	Conditionally requires input	Name of the Azure VNet to connect to FortiGate Autoscale. Required when using an existing VNet. When creating a new VNet, this parameter can be left empty and a name will be generated.
VNet Resource Group Name	Conditionally requires input	Name of the resource group that contains the VNet and related network components.

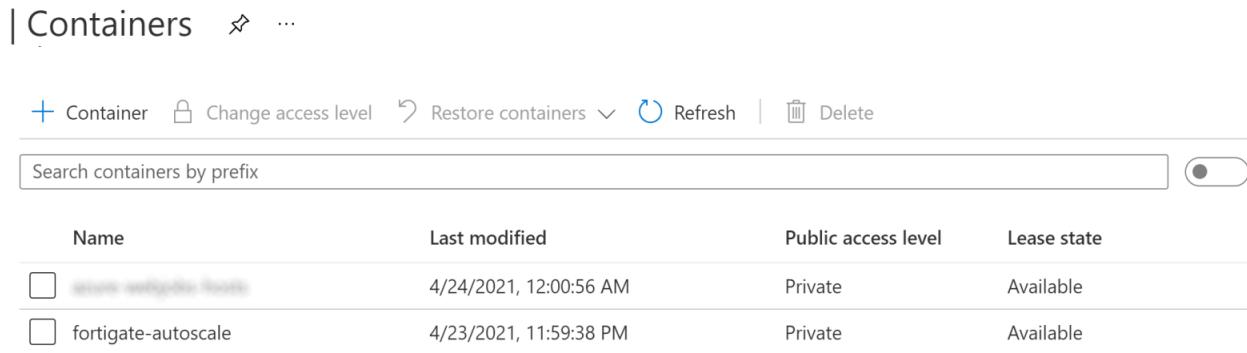
Parameter name	Default value	Description
		Required if the VNet is not in the Autoscale resource group (specified in the parameter <i>Resource group</i> ). If not specified, the Autoscale resource group will be used. For details, refer to the description for the parameter <a href="#">VNet Deployment Method</a> on page 54. This resource group must be in the same region as the Autoscale resource group.

## Uploading files to the Storage account

The template deployment will create the storage container `fortigate-autoscale` in the resource group you selected or created in step 6 of the section [Creating a template deployment](#) on page 45.

### To upload files to the storage container:

- From the Resource group, load the Storage account by clicking its name.
- From the Storage account navigation column, under *Data storage*, click *Containers*. The `fortigate-autoscale` container will be listed.



Name	Last modified	Public access level	Lease state
<input type="checkbox"/> www-autoscale-hosts	4/24/2021, 12:00:56 AM	Private	Available
<input type="checkbox"/> fortigate-autoscale	4/23/2021, 11:59:38 PM	Private	Available

- Click the `fortigate-autoscale` container.
- Click *Upload*.

5. In the *Upload blob*, click *Advanced* to display more options.

The screenshot shows the 'Upload blob' interface with the 'Advanced' section expanded. Key settings include:

- Authentication type:** Account key (selected)
- Blob type:** Block blob
- Upload .vhd files as page blobs (recommended):** Checked
- Block size:** 4 MB
- Upload to folder:** (empty input field)
- Encryption scope:** Use existing default container scope (selected)

At the bottom is a large 'Upload' button.

6. Specify the folder to upload to in *Upload to folder*:

- For *configset* files, enter assets/configset.
- For *license* files, enter assets/license-files/fortigate.

7. Select a file or files to upload:

- For *configset* files, select all the files in the *configset* folder of the deployment package.
- For *license* files, select your BYOL license file(s).

If you provide two license files with the same content, only one of them will be used, the other one will be ignored.



If you upload a file with the same name but different content, there are two outcomes:

- If the old license has not been distributed, the new file completely replaces the old one
- If the old license has been distributed, the new file is treated as a new license. The old license is still valid, but it cannot be redistributed in the future.

8. Click *Upload*.

## Verifying the deployment

FortiGate Autoscale for Azure deploys the following components:

- 1 Public Load balancer
  - This load balancer will be associated with the FortiGate subnet and the Frontend Public IP address to receive inbound traffic.
- 1 Internal Load balancer
  - This load balancer will be associated with all 4 subnets.
- 1 Network security group (associated with all 4 subnets)
- 1 Virtual machine scale set for BYOL
- 1 Virtual machine scale set for PAYG
- 1 Virtual machine for FortiAnalyzer (only if deployed with FortiAnalyzer integration)
- 1 Virtual network
- 1 Public IP address
- 3 Route tables
- 1 Azure Cosmos DB account
- 1 Function App
- 1 Application Insights (automatically enabled if your region supports it)
- 1 App Service plan
- 2 Disk components for use by FortiAnalyzer (only if deployed with FortiAnalyzer integration)
- 1 Key vault
- 1 Storage account

For deployments that have two resource groups, the network related components are deployed to the VNet resource group and the DB, Storage account, and Function App related components are deployed to the Autoscale resource group.

FortiGate Autoscale for Azure is fully deployed once you verify the following components:

- [the Function App](#)
- [the database](#)
- [the primary election](#)

### To load a resource group:

1. In the Azure console, from the left navigation column, select *Resource groups*.
2. Locate the resource group you wish to load by scrolling through the list or by using one or more of the name, subscription, and location filters. In the example below, this is *fgtasg-rg*.

The screenshot shows the Microsoft Azure Resource Groups page. At the top, there's a search bar with the placeholder "Search resources, services, and docs (G+ /)". Below the search bar, there are navigation links for "Home > Resource groups". A red box highlights the search term "fgtasg-rg" in the search bar. The main content area displays a single resource group entry:

- Name:** fgtasg-rg
- Subscription:** == all
- Location:** == all
- Add filter**

Below the search bar, it says "Showing 1 to 1 of 1 records." There are grouping and view dropdowns set to "No grouping" and "List view". The resource group details are shown in a table:

Name	Subscription	Location	...
fgtasg-rg	Central US	Central US	...

- Click the name to load the resource group *Overview* page. In the example deployment, the VNet resource group is the same as the Autoscale resource group.

The screenshot shows the Microsoft Azure Resource Group Overview page for the resource group "fgtasg-rg". The top navigation bar includes "Home > Resource groups > fgtasg-rg". The main content area displays the following information:

- Subscription:** (change)
- Deployment Status:** Deployments Succeeded
- Subscription ID:** [redacted]
- Tags:** (change) Click here to add tags

Below this, there's a filtering section with dropdowns for "Type == all" and "Location == all", and a "Add filter" button. It also shows "Showing 1 to 15 of 15 records." and a "Show hidden types" link. The main table lists 15 resources:

Name	Type	Location
fgtasg01-external-load-balancer	Load balancer	West US
fgtasg01-internal-load-balancer	Load balancer	West US
fgtasg01-network-security-group	Network security group	West US
fgtasg01byol	Virtual machine scale set	West US
fgtasg01ipay	Virtual machine scale set	West US
fgtasg01 -virtual-network	Virtual network	West US
fgtasg01 -virtual-network-ext-lb-public-ip	Public IP address	West US
fgtasg01 -virtual-network-subnet1-route-table	Route table	West US
fgtasg01 -virtual-network-subnet2-route-table	Route table	West US
fgtasg01 -virtual-network-subnet3-route-table	Route table	West US
fgtasg01 dba001	Azure Cosmos DB account	West US
fgtasg01 funcapp	Function App	West US
fgtasg01 funcapp-insights	Application Insights	West US
fgtasg01 funcapp-service-plan	App Service plan	West US
fgtasg01 sta001	Storage account	West US

## To verify the Function App:

1. From the Autoscale resource group *Overview* page, load the Function App by clicking the name of the item of type *Function App*.
2. From the navigation column, select *Functions*.

The screenshot shows the Microsoft Azure Functions blade for the 'funcapp' function app. The left sidebar has 'funcapp | Functions' selected. The main area displays four functions in a table:

Name	Trigger	Status	...
byol-license	HTTP	Enabled	...
faz-auth-handler	HTTP	Enabled	...
faz-auth-scheduler	Timer	Enabled	...
fgt-as-handler	HTTP	Enabled	...

You should see four functions on the right:

- *byol-license*: The function to distribute BYOL licenses.
- *faz-auth-handler*: The function to handle authorization of FortiGate in the FortiAnalyzer.
- *faz-auth-scheduler*: The function to handle authorization of FortiGate in the FortiAnalyzer on a timely basis.
- *fgt-as-handler*: The main autoscaling function.

## To verify the database:

1. From the Autoscale resource group *Overview* page, click the *Azure Cosmos DB account* name.
2. From the navigation column, click *Data Explorer*.
3. Expand the database *FortiGateAutoscale*.

You will see the following database and tables:

- *Database*: FortiGateAutoscale
- *Tables*:
  - ApiRequestCache
  - Autoscale
  - CustomLog
  - FortiAnalyzer
  - LicenseStock
  - LicenseUsage
  - PrimaryElection
  - Settings

The database *Data Explorer* page will look as shown below:

The screenshot shows the Microsoft Azure Data Explorer interface. At the top, there's a blue header bar with the Microsoft Azure logo, a search bar, and a user profile icon. Below the header, the navigation path is "All services > Resource groups > fgtasg-rg > fgtasg01 > dba001". The main title is "dba001 | Data Explorer". On the left, a sidebar menu includes "Overview", "Activity log", "Access control (IAM)", "Tags", "Diagnose and solve problems", "Quick start", "Notifications", and "Data Explorer", with "Data Explorer" highlighted by a red box. Other menu items like "Settings" and "Features" are also visible. The main content area has a "SQL API" tab selected. Under "Scale", a table named "FortiGateAutoscale" is listed, also highlighted by a red box. To the right, a large "Welcome to Cosmos DB" message is displayed, followed by the text "Globally distributed, multi-model database for any scale". There are "Start" and "Next" buttons at the bottom right.

### To verify the primary election:

The elected primary FortiGate-VM will be logged in the CosmosDB *FortiGateAutoscale* in the table *FortiGatePrimaryElection*.

1. Expand the *FortiGatePrimaryElection* table and click on *Items*.
2. There will be one item in the table, select it.

```

1 "id": "fgtasg01byol:69d23a23-bafe-47f5-88fa-43a30d394379",
2 "scalingGroupName": "fgtasg01byol",
3 "ip": "10.0.0.4",
4 "vmId": "69d23a23-bafe-47f5-88fa-43a30d394379",
5 "virtualNetworkId": "fgtasg01-autoscale-reserved-vnet-ea",
6 "subnetId": "subnets/subnet1",
7 "voteEndTime": 1626894015952,
8 "voteState": "done",
9 "_rid": "qN4FAKARch0CAAAAAAAA==",
10 "_self": "dbs/qN4FAA=/colls/qN4FAKARch0=/docs/qN4FAKARch0=qN4FAKARch0=_rid=qN4FAKARch0CAAAAAAAA==/_ts=1626894015952",
11 "_etag": "\"00002d0e-0000-0100-0000-60f86ebf0000\"",
12 "_attachments": "attachments/",
13 "_ts": 1626894015952
14
15

```

- *id* is the unique identifier of a database record.
- *scalingGroupName* is the name of the Scale Set in which the primary FortiGate-VM is located.
- *ip* is the primary private IP address of the current primary FortiGate-VM.
- *vmId* is the index of the FortiGate-VM in the Scale Set.
- *virtualNetworkId* is the ID of the Virtual Network in which the primary FortiGate-VM instance is located.
- *subnetId* is the ID of the subnet in which the primary FortiGate-VM is located.
- *voteEndTime* is the Unix time stamp for when this primary election should expire if the vote state cannot change to *done* by this time.
- *voteState* is the state of the voting process.
  - *pending*: election of the primary instance is still in progress. You should wait for its completion. At this point in time, the final primary instance is not yet known.
  - *done*: the primary election process has completed.

## Security features for network communication

Security features are automatically enabled and configured as described in the following sections.

### Database

Firewalls are set for IP address ranges and the VNet. The firewall only allow interactions with the DB tables from the FortiGate subnet, Function App additional outbound IP addresses, and user-defined IPv4 IP ranges.

To view the firewalls, load the Cosmos DB. From the *Settings* section of the left navigation tree, click *Networking* and then click *Firewall and virtual networks*.

The screenshot shows the Azure portal interface for managing a Cosmos DB account named 'fgtasg01'. The current view is 'dba001 - Firewall and virtual networks'. At the top, there are tabs for 'Allow access from' (with 'Selected networks' selected), 'Virtual networks' (with '+ Add existing virtual network' and '+ Add new virtual network' buttons), and a table listing virtual network entries. One entry for 'fgtasg01' is highlighted with a red border. Below this, the 'Firewall' section allows adding IP ranges, with a list of outbound IP addresses from Function Apps. The first address, '0.0.0.0/0', is also highlighted with a red border. At the bottom, there are sections for 'Exceptions' with checkboxes for 'Accept connections from within public Azure datacenters' and 'Allow access from Azure Portal'.

Virtual Network	Subnet	Address range	Endpoint Status	Resource Group	Subscription
> fgtasg01	...	10.0.0.0/16		fgtasg-rg	[redacted]

IP (Single IPv4 or CIDR range)	...
0.0.0.0/0	...
104. [redacted] .55	...
40. 137	...
40. .40	...
40. 54	...
40. 103	...
40. 196	...
40. 145	...
40. .99	...

The IP addresses listed in the Firewall section include the set of all possible Function App outbound IP addresses as obtained from the *Additional Outbound IP Addresses* field of the Function App *Properties*. To view these IP addresses, load the Function App, click the *Platform features* tab and then click *Properties*. Each IP address in the list has been added as an entry in the Cosmos DB firewall.

Home > fgtasg-rg > fgtasg01 funcapp > Properties

**Properties**

fgtasg01 funcapp

Status	Running
URL	fgtasg01 funcapp.azurewebsites.net
Virtual IP address	104. .55
Mode	Consumption
<b>Additional Outbound IP Addresses</b>	
104. .55,40. .137,40. .40,40. .54,40. .103,40. .196,40. .145,40. .99 	



If Function App *Additional Outbound IP Addresses* change, the Cosmos DB firewall must be manually updated so that each IP address has a corresponding entry in the Cosmos DB firewall. Any IP address not listed in the Cosmos DB firewall will be blocked, thus causing the Autoscale function to be blocked. For details on when Function App outbound IP addresses change, refer to the Microsoft article [When outbound IPs change](#).

## Function App

Requests are restricted by source. Incoming requests are only allowed from the FortiGate subnet and from user-defined IPv4 IP ranges.

To view *Access Restrictions*, load the Function App. In the right hand pane, click the *Platform features* tab and then click *All settings*. From the *Settings* section of the left navigation tree, click *Networking* and then click *Configure Access Restrictions*.

Home > fgtasg01 funcapp > fgtasg01 funcapp - Networking > Access Restrictions

## Access Restrictions

Remove Refresh

### Access Restrictions

Access restrictions allow you to define lists of allow/deny rules to control traffic to your app. Rules are evaluated in priority order. If there are no rules defined then your app will accept traffic from any address. [Learn more](#)

fgtasg01	funcapp.azurewebsites.net	fgtasg01	funcapp.scm.azurewebsites.net	
	Add rule			
Priority	Name	Source	Endpoint status	Action
100	allow-FortiGate-subnet	fgtasg01 -virtual-netw...	Enabled	Allow ...
101	allow-external-ipv4-1	0.0.0.0/0		Allow ...
2147483647	Deny all	Any		Deny

## Virtual Network

The service endpoints for Azure services are enabled. Service endpoints should be enabled for the minimum number of Azure services required for Autoscale.

Home > fgtasg-rg > fgtasg01 -virtual-network - Service endpoints

### -virtual-network - Service endpoints

fgtasg01 Virtual network

Search (Ctrl+ /) Add Filter service endpoints

Service	Subnet	Status	Locations
Microsoft.AzureCosmo...	1 fgtasg01 -virtual...	Succeeded *	...
Microsoft.Web	1 fgtasg01 -virtual...	Succeeded *	...

Tags  
Diagnose and solve problems  
Settings  
DNS servers  
Peerings  
**Service endpoints**   
Private endpoints

## Starting a VMSS

Your deployment will have two Virtual machine scale sets (VMSS), one for BYOL instances and one for PAYG instances. For deployments using only one instance type, start that VMSS. For Hybrid licensing deployments, start both VMSS.

### To start a VMSS:

1. Load the resource group that contains the VMSS. In deployments with one resource group, this value is specified in the *Resource group* parameter in step 6 of the section [Creating a template deployment on page 45](#). If your deployment has a separate resource group for the VNet, load that one instead. That resource group is specified in the [VNet Resource Group Name on page 54](#) parameter.
2. Load the *Virtual machine scale set* by clicking its name.
3. From the Virtual machine scale set account navigation column, under *Settings*, click *Scaling*.
4. Under *Choose how to scale your resource*, click *Custom autoscale*.
5. Click *Save*.

The BYOL *Custom autoscale* appears as shown in the image:

The screenshot shows the Azure portal interface for managing a Virtual Machine Scale Set named 'fgtasg01byol - Scaling'. The left sidebar lists various settings like Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. The 'Scaling' tab is selected and highlighted with a red box. The main content area shows the 'Choose how to scale your resource' section with two options: 'Manual scale' (radio button unselected) and 'Custom autoscale' (radio button selected and highlighted with a blue box). The 'Custom autoscale' section displays the following details:

- Autoscale setting name:** fgtasg01 -autoscale-payg
- Resource group:** fgtasg-rg
- Instance count:** 0
- Default profile:** fgtasg01 -deployed-profile (with a delete icon)
- Delete warning:** The very last or default recurrence rule cannot be deleted. Instead, you can disable autoscale to turn off autoscale.
- Scale mode:** Scale based on a metric (radio button unselected) / Scale to a specific instance count (radio button selected and highlighted with a blue box).
- Instance count:** 2
- Schedule:** This scale condition is executed when none of the other scale condition(s) match

**Add a scale condition**

The PAYG *Custom autoscale* appears as shown in the image:

Home > Resource groups > fgtasg-rg > fgtasg01payg - Scaling

## fgtasg01payg - Scaling

Virtual machine scale set

Configure Run history JSON Notify Diagnostics logs

**Choose how to scale your resource**

Manual scale: Maintain a fixed instance count

Custom autoscale: Scale on any schedule, based on any metrics

**Custom autoscale**

Autoscale setting name: fgtasg01 -autoscale-payg  
 Resource group: fgtasg-rg  
 Instance count: 0

**Default** fgtasg01 -deployed-profile

Delete warning: The very last or default recurrence rule cannot be deleted. Instead, you can disable autoscale to turn off autoscale.

Scale mode:  Scale based on a metric  Scale to a specific instance count

Scale out

When	fgtasg01byol	(Average) Percentage CPU > 80	Increase count by 1
Or	fgtasg01payg	(Average) Percentage CPU > 80	Increase count by 1

Rules

Scale in

When	fgtasg01byol	(Average) Percentage CPU < 20	Decrease count by 1
And	fgtasg01payg	(Average) Percentage CPU < 20	Decrease count by 1

+ Add a rule

Instance limits

Minimum	0	Maximum	6	Default	0
---------	---	---------	---	---------	---

Schedule: This scale condition is executed when none of the other scale condition(s) match

+ Add a scale condition

## Connecting to the FortiGate-VM instances

To connect to a FortiGate-VM, you can use SSH commands or the web GUI using HTTPS with the IPv4 public IP address.

From the resource group *Overview* page, click the external load balancer name to load it. From the navigation column, click *Inbound NAT Rules*. For each instance in the scale set you will see two rules:

- One rule for SSH access to the instance.
- One rule for HTTPS access to the instance.

The *Inbound NAT Rules* page will look as shown below:

The screenshot shows the Inbound NAT Rules page for the load balancer 'fgtasg01-external-load-balancer'. The URL in the browser is 'Home > Resource groups > fgtasg-rg > fgtasg01-external-load-balancer - Inbound NAT rules'. The page title is 'fgtasg01-external-load-balancer - Inbound NAT rules'. There is a search bar labeled 'Search inbound NAT rules' and a 'Add' button. The main table lists two rules:

NAME	IP VERSION	DESTINATION	TARGET	SERVICE
fgtasg01byollpnatpoolhttps.4	IPv4	52.137.95.22	fgtasg01byol (instance 4)	Custom (TCP/400... ...)
fgtasg01byollpnatpoolssh.4	IPv4	52.137.95.22	fgtasg01byol (instance 4)	Custom (TCP/500... ...)

To access a FortiGate-VM instance, you need the Frontend IP address and port number of the instance you wish to connect to. The Frontend IP address is listed on the *Inbound NAT Rules* page. To obtain the port number, click the entry for the method you will use to access the instance (SSH or HTTPS). The port number will be listed midway down the page. (The IP address is also listed).

An example of an SSH access rule is shown below:

## fgtasg01byollpnatpoolhttps.4

D1-external-load-balancer

Save  Discard  Delete

NAT rule name

fgtasg01byollpnatpoolhttps.4

Frontend IP address i

LoadBalancerFrontEnd (52.137.95.22)



IP Version i

IPv4

Service

Custom



Protocol

TCP  UDP

\* Port

50030

Target virtual machine i



Network IP configuration i

fgtasg01config (10.0.0.4)



Port mapping i

Default  Custom

Floating IP (direct server return) i

Disabled  Enabled

\* Target port

22

# Troubleshooting

## Determining the FortiGate Autoscale release version

To determine the release version of a deployment, navigate to the *Microsoft.Template Outputs* by following the steps in [Locating deployment Outputs on page 70](#). The release version is in the `deploymentPackageVersion`.

## Election of the primary FortiGate was not successful

If the election of the primary FortiGate is not successful, reset the elected primary FortiGate. If the reset does not solve the problem, please contact support.

## Locating deployment Outputs

1. Load the resource group *Overview* page. For details, refer to the section [To load a resource group: on page 57](#).
2. Click the link under *Deployments*.

The screenshot shows the Microsoft Azure Resource Group Overview page for a resource group named "fgtasg-rg". The top navigation bar includes the Microsoft Azure logo, a search bar, and user profile icons. Below the header, the resource group name "fgtasg-rg" is displayed along with its type ("Resource group") and a copy icon. A navigation menu on the left shows "Home > fgtasg-rg". The main content area displays "Essentials" information: "Subscription (change)" (with a "Subscription ID" link), "Deployments" (status "Succeeded" highlighted with a red box), and "Location" (East US). Action buttons at the top include "Add", "Edit columns", "Delete resource group", "Refresh", "Export to CSV", "Open query", and "JSON View".

3. From the *Deployments* page, click the *Microsoft.Template*.

The screenshot shows the Microsoft Azure Deployments page for the "fgtasg-rg" resource group. The top navigation bar includes the Microsoft Azure logo, a search bar, and user profile icons. The left sidebar shows "Tags", "Events", "Settings", and "Deployments" (which is selected and highlighted with a grey background). The main content area shows a table of deployments. The first deployment listed is "Microsoft.Template", which has a status of "Succeeded" (indicated by a green checkmark). Other columns in the table include "Deployment name" (empty) and "Status" (Succeeded).

- In the navigation column, click *Outputs*.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Resource groups > fgtasg-rg > Microsoft.Template

## Microsoft.Template | Outputs

Deployment

Search (Ctrl+ /) cmdDeleteVNetComponents

Overview az account set -s ...

Inputs

Outputs deploymentPackageVersion

Template 3.3.0

## Redeploying with an existing VNet fails

Prior to redeploying with your existing VNet, you must ensure that the VNet meets the Requirements when using an existing VNet on page 44. You must also perform a VNet related cleanup using the following steps:

- Load the deployment Outputs for the VNet resource group. If your deployment only has one resource group, this is the Autoscale resource group.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Resource groups > fgtasg-rg > Microsoft.Template

## Microsoft.Template | Outputs

Deployment

Search (Ctrl+ /) cmdDeleteVNetComponents

Overview az account set -s ...

Inputs

Outputs deploymentPackageVersion

Template 3.3.0

- Copy the value of `cmdDeleteVNetComponents` and run it as an Azure CLI command (click `>_` to launch the CLI) to perform the required cleanup.
- If your deployment has two resource groups, delete the Autoscale resource group. Otherwise, delete the following components:
  - Azure Cosmos DB account
  - App Service

- Application Insights (if present)
  - App Service plan
  - Storage account
4. Delete the following components from the VNet resource group:
- the Public Load balancer
  - the Internal Load balancer
  - the Virtual machine scale set for BYOL
  - the Virtual machine scale set for PAYG
  - the Public IP address (if created by the autoscale deployment and you don't want to reuse it)

## Resetting the elected primary FortiGate

To reset the elected primary FortiGate, navigate to the CosmosDB *FortiGateAutoscale* and open the table *FortiGatePrimaryElection* and delete the only item in the table.

A new primary FortiGate will be elected and a new record will be created as a result.

For details on locating the CosmosDB *FortiGateAutoscale* and the table *FortiGatePrimaryElection*, refer to the section [Verifying the deployment on page 57](#).

## Stack has stopped working

If the stack stops working when it previously used to work, look up the Function App *Additional Outbound IP Addresses* and ensure that each listed IP address has a corresponding entry in the Cosmos DB firewall. Any IP address not listed in the Cosmos DB firewall will be blocked, thus causing the Autoscale function to be blocked.

For details on how the Cosmos DB firewall is configured, refer to the section [Security features for network communication on page 61](#).

For details on when Function App outbound IP addresses change, refer to the Microsoft article [When outbound IPs change](#).

## Troubleshooting using Application Insights

Application Insights can help you troubleshoot the deployment. It is automatically enabled if your region supports it.

## Troubleshooting using environment variables

Environment variables are available to assist in troubleshooting the current FortiGate Autoscale deployment. These variables and details on how to use them are listed in the section [Troubleshooting environment variables on page 76](#)

1. Load the Function App. For detailed steps, refer to the Function App portion of the section [Verifying the deployment on page 57](#).

2. Under *Configured features*, click *Configuration*.

The screenshot shows the Azure portal interface for managing a Function App. The left sidebar lists various resources like Storage, SQL, and Log Analytics. The main area shows the 'Overview' tab for the 'fgtasg01 funcapp' under the 'fgtasg-rg' resource group. Key details include:

- Status: Running
- Subscription ID: [redacted]
- Resource group: fgtasg-rg
- URL: <https://fgtasg01...funcapp.azurewebsites.net>
- Location: [redacted]
- App Service plan / pricing tier: [redacted]

Below the overview, there's a section titled 'Configured features' with a 'Configuration' button highlighted with a red box.

3. Edit settings as needed.

The screenshot shows the 'Application settings' page for the 'fgtasg01 funcapp'. The 'Application settings' tab is selected. It includes a note about encrypted transmission and a table for managing application settings:

Name	Value	Deployment slot setting	Delete	Edit
[empty]	[empty]	[empty]	[empty]	[empty]

At the bottom, there's a note with a lightbulb icon: "Changing environment variables other than the troubleshooting ones can cause unexpected behavior. Modify them at your own risk."

# Appendix

## FortiGate Autoscale for Azure features

### Major components

- *The Function App.* The Function App handles all the autoscaling features including: primary/secondary role assignment, license distribution, and failover management.
- *The BYOL Scale Set.* This scale set contains 0 to many FortiGate-VMs of the BYOL licensing model and is a VMSS with a fixed size. Users can set the size to match the number of valid licenses they own. Licenses can be purchased from FortiCare.



For BYOL-only and hybrid licensing deployments, the *BYOL instance Count* must be at least 2. These FortiGate-VMs are the main instances and are fixed and running 7x24. If it is set to 1 and the instance fails to work, the current FortiGate-VM configuration will be lost.

- *The PAYG Scale Set.* The Scale Set contains 0 to many FortiGate-VMs of the PAYG licensing model and will dynamically scale-out or scale-in based on the scaling metrics specified by the parameters *Scale Out Threshold* and *Scale in Threshold*.



For PAYG-only deployments, the *PAYG instance Count* must be at least 2. These FortiGate-VMs are the main instances and are fixed and running 7x24. If it is set to 1 and the instance fails to work, the current FortiGate-VM configuration will be lost.

- *The Blob Containers.*

- The *configset* container contains files that are loaded as the initial configuration of a new FortiGate-VM instance.
  - *baseconfig* is the base configuration. This file can be modified as needed to meet your network requirements. Placeholders such as {SYNC\_INTERFACE} are explained in the [Configset placeholders on page 75](#) table below.
  - *httproutingpolicy* and *httpsroutingpolicy* are provided as part of the base configset - for a common use case - and specify the FortiGate firewall policy for VIPs for *http* routing and *https* routing respectively. This common use case includes a VIP on port 80 and a VIP on port 443 with a policy that points to an internal load balancer.
  - *extrastaticroute* is empty by default. Configurations for static routes can be added if they are needed in a network. An example of manually adding a static route:

```
# config router static
  edit 1
    set dst 168.63.129.16 255.255.255.255
    set gateway <subnet gateway>
    set priority <any number>
    set device "<port name>"
  next
end
```
- The *fgt-asg-license* container contains the BYOL license files.

- *Database tables*. These tables are required to store information such as health check monitoring, primary election, state transitions, etc. These records should not be modified unless required for troubleshooting purposes.
- *Networking Components*.
  - One virtual network
  - Two Load Balancers (with names ending with *-external-load-balancer* and *-internal-load-balancer*)
  - One network security group (with a name ending with *-network-security-group*)
  - One public IP address
  - Four route tables

## Configset placeholders

When the FortiGate-VM requests the configuration from the Autoscaling handler function, the placeholders in the table below will be replaced with actual values for the Autoscaling group.

Placeholder	Type	Description
{SYNC_INTERFACE}	Text	The interface for FortiGate-VMs to synchronize information. Specify as port1, port2, port3, etc. All characters must be lowercase.
{CALLBACK_URL}	URL	The full URL of the Autoscaling handler function.
{PSK_SECRET}	Text	The Pre-Shared Key used in FortiOS.
{ADMIN_PORT}	Number	The admin port will be replaced with 443.
{HEART_BEAT_INTERVAL}	Number	The time interval (in seconds) that the FortiGate-VM waits between sending heartbeat requests to the Autoscale handler function.  This placeholder is only in the hybrid licensing deployment.

## Function App environment variables

### Azure infrastructure related environment variables

The variables in the table below hold information that enables the function to use the required Azure services. Changing their values may cause services to be unreachable by the function. Modify them at your own risk.

Variable name	Description
RESOURCE_GROUP	Name of the resource group where the template is deployed in.
CLIENT_ID	Descriptions of these variables are identical to those of the related parameters which are described in the section <a href="#">Configurable variables on page 49</a> .
CLIENT_SECRET	<ul style="list-style-type: none"> <li>• REST_APP_ID: <a href="#">Service Principal App ID on page 53</a></li> <li>• REST_APP_SECRET: <a href="#">Service Principal App Secret on page 53</a></li> <li>• WEBSITE_RUN_FROM_ZIP: <a href="#">Package Res URL on page 53</a></li> </ul>
WEBSITE_RUN_FROM_ZIP	
AUTOSCALE_DB_PRIMARY_KEY	This is the CosmosDB account access key automatically created with the CosmosDB account.

Variable name	Description
TENANT_ID	The Azure Directory ID for the Active Directory of your current subscription.
SUBSCRIPTION_ID	Your Azure Subscription ID.
AUTOSCALE_DB_ACCOUNT	The CosmosDB account created for the current FortiGate Autoscale deployment.
AZURE_STORAGE_ACCOUNT	This is the Blob Storage account name automatically created during the deployment.
AZURE_STORAGE_ACCESS_KEY	This is the Blob Storage account access key automatically created with the Blob Storage account.

## FortiGate Autoscale required environment variables

Changing the values of the following variables can cause unexpected function behavior. Modify them at your own risk.

Variable name	Description
UNIQUE_ID	Reserved, empty string.
CUSTOM_ID	Reserved, empty string.
RESOURCE_TAG_PREFIX	An Autoscaling feature variable that is automatically created. Reserved for future use.
AUTOSCALE_KEY_VAULT_NAME	Name of the Key Vault service.

## Troubleshooting environment variables

The following variables assist in troubleshooting the current FortiGate Autoscale deployment.

Variable name	Description
DEBUG_SAVE_CUSTOM_LOG	Set to <i>true</i> to save script logs to the DB table <i>CUSTOM_LOG</i> . This is the default behavior. Set to <i>false</i> to disable this feature.
DEBUG_LOGGER_OUTPUT_QUEUE_ENABLED	Set to <i>true</i> to concatenate all log output into one (1) log item in the Azure logging system. Set to <i>false</i> for every log output to have its own log item in the Azure logging system. This is the default behavior.
DEBUG_LOGGER_TIMEZONE_OFFSET	Set to the UTC offset of the current deployment location for a better logging display time.

For details on how to modify the troubleshooting environment variables, refer to the section [Troubleshooting using environment variables on page 72](#).

## Cloud-init

In Auto Scaling, a FortiGate uses the `cloud-init` feature to pre-configure the instances when they first come up. During template deployment, an internal API Gateway endpoint will be created.

A FortiGate sends requests to the endpoint to retrieve necessary configuration after initialization.

Use this FOS CLI command to display information for your devices:

```
# diagnose debug cloudinit show
```

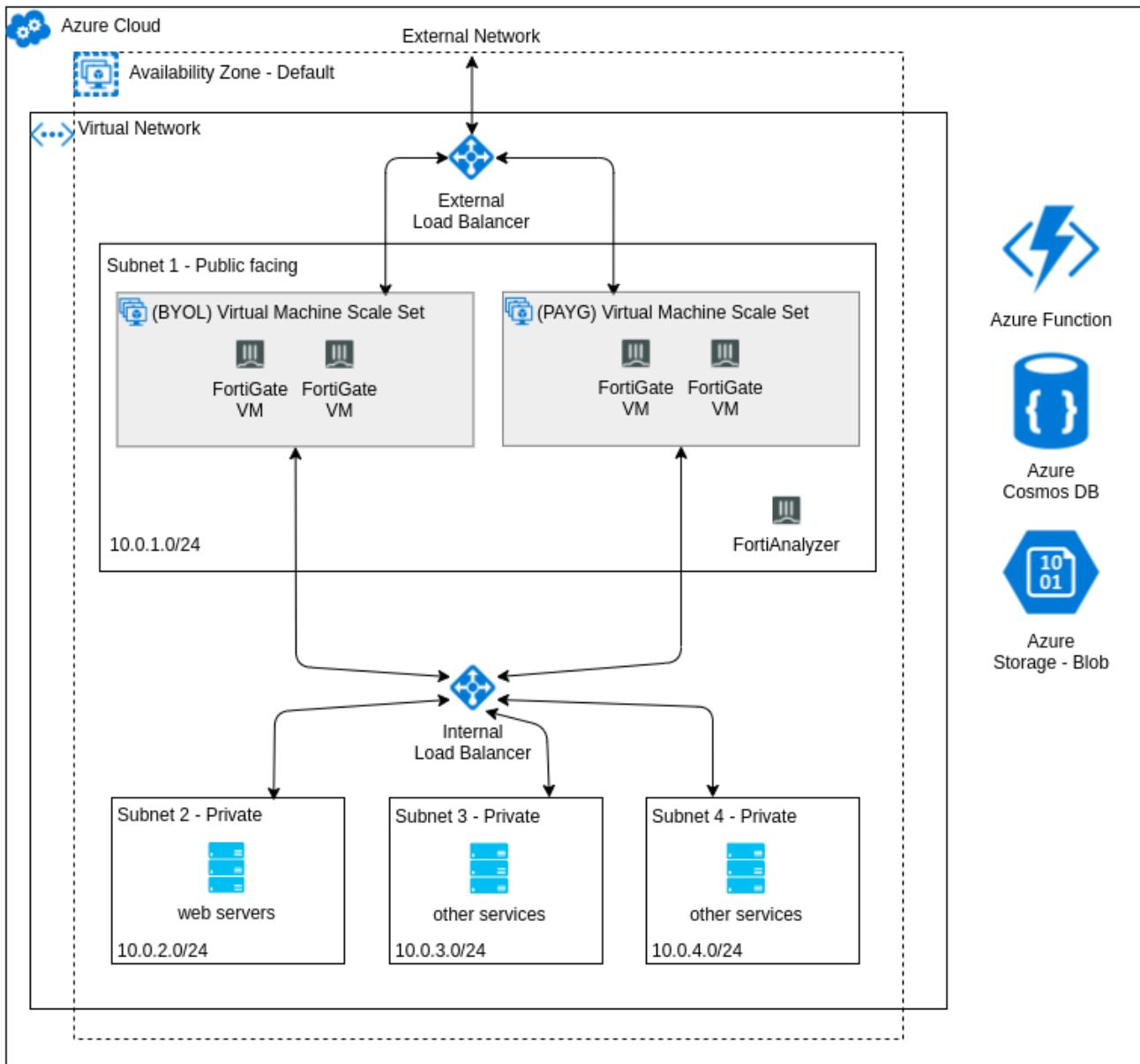
VPN output can be retrieved with this FOS CLI command:

```
# diagnose vpn tun list
```

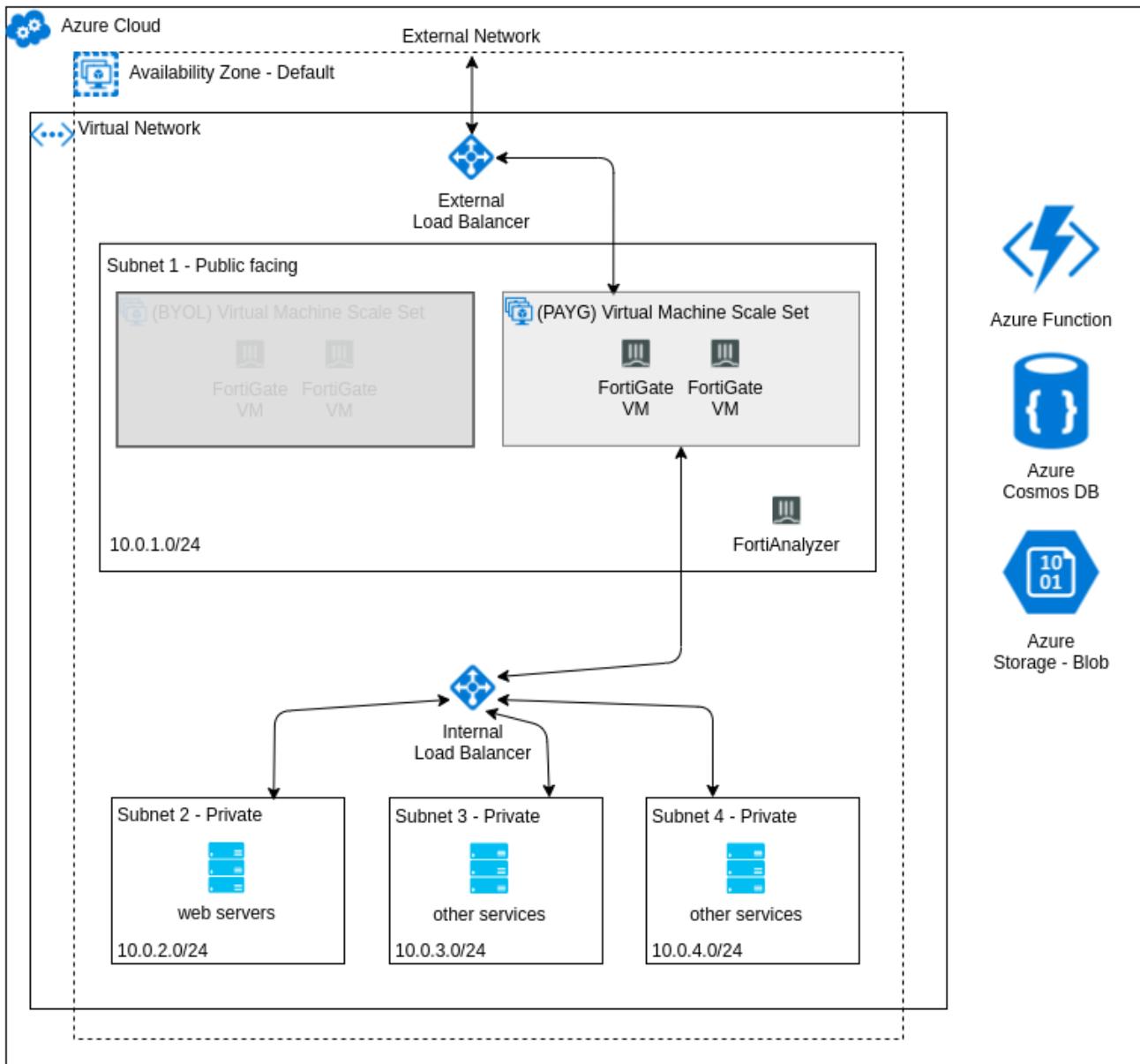
## Architectural diagrams

The following diagrams illustrate the different aspects of the architecture of FortiGate Autoscale for Azure.

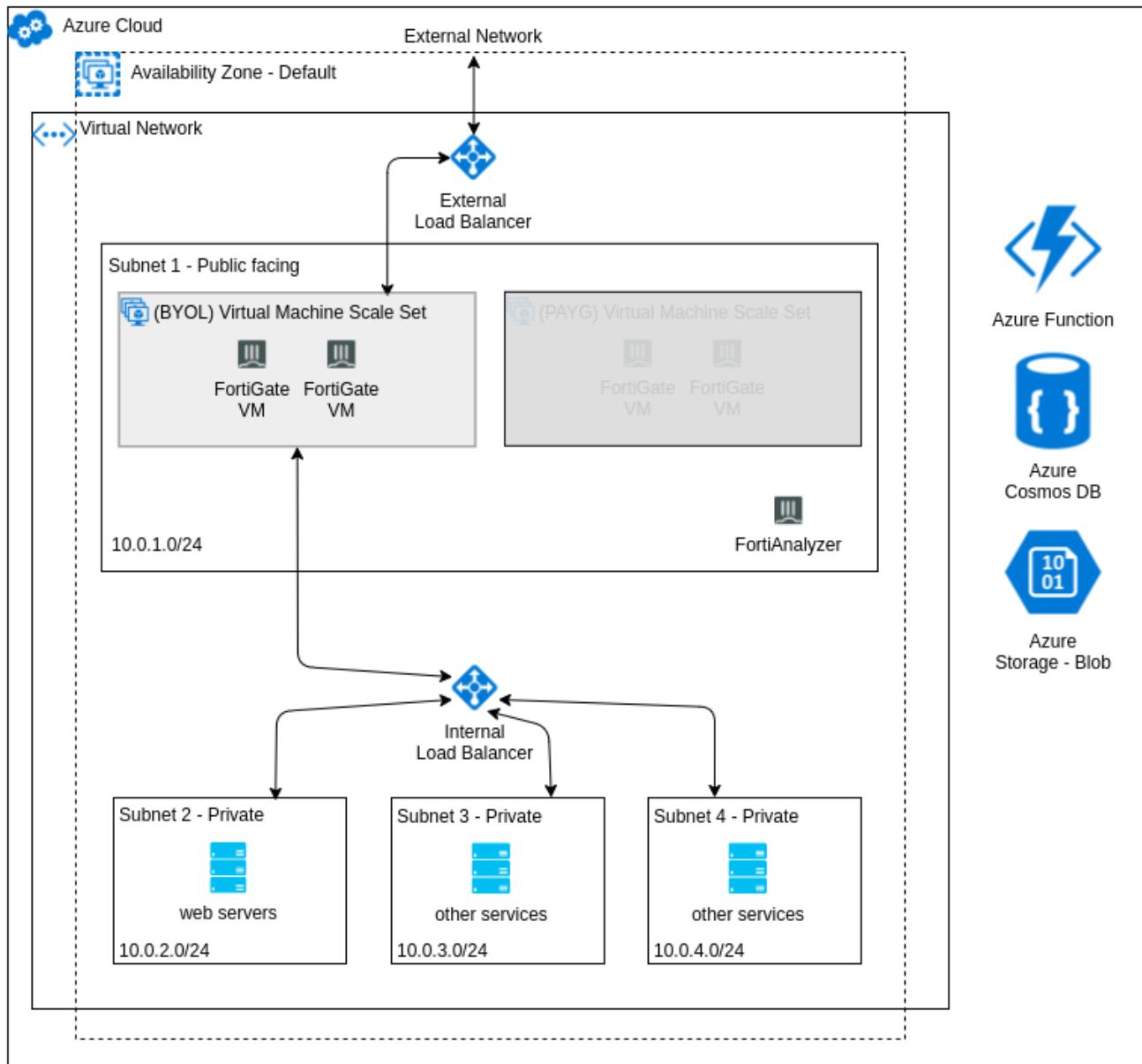
## FortiGate Autoscale for Azure architecture (hybrid licensing)



## FortiGate Autoscale for Azure architecture (PAYG instances only)

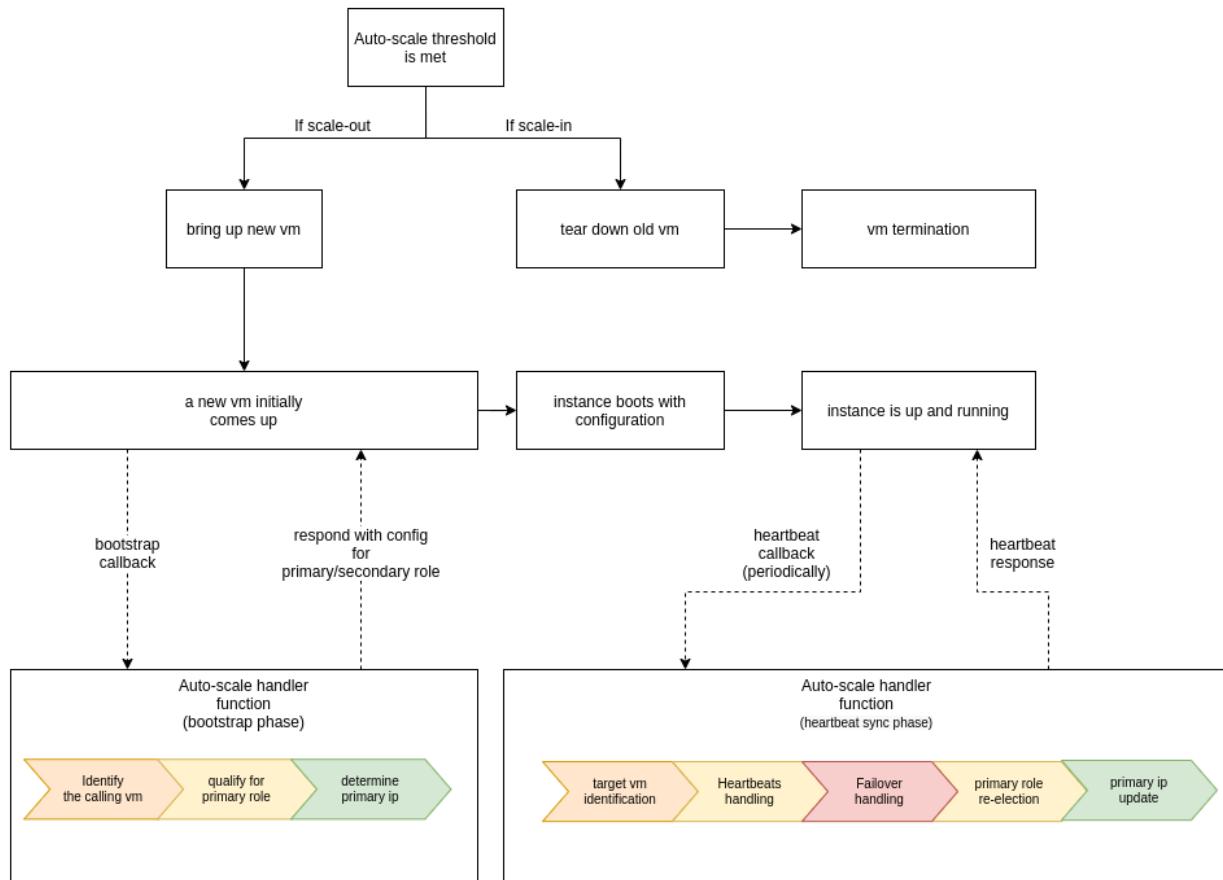


## FortiGate Autoscale for Azure architecture (BYOL instances only)



## Autoscale handler flowchart

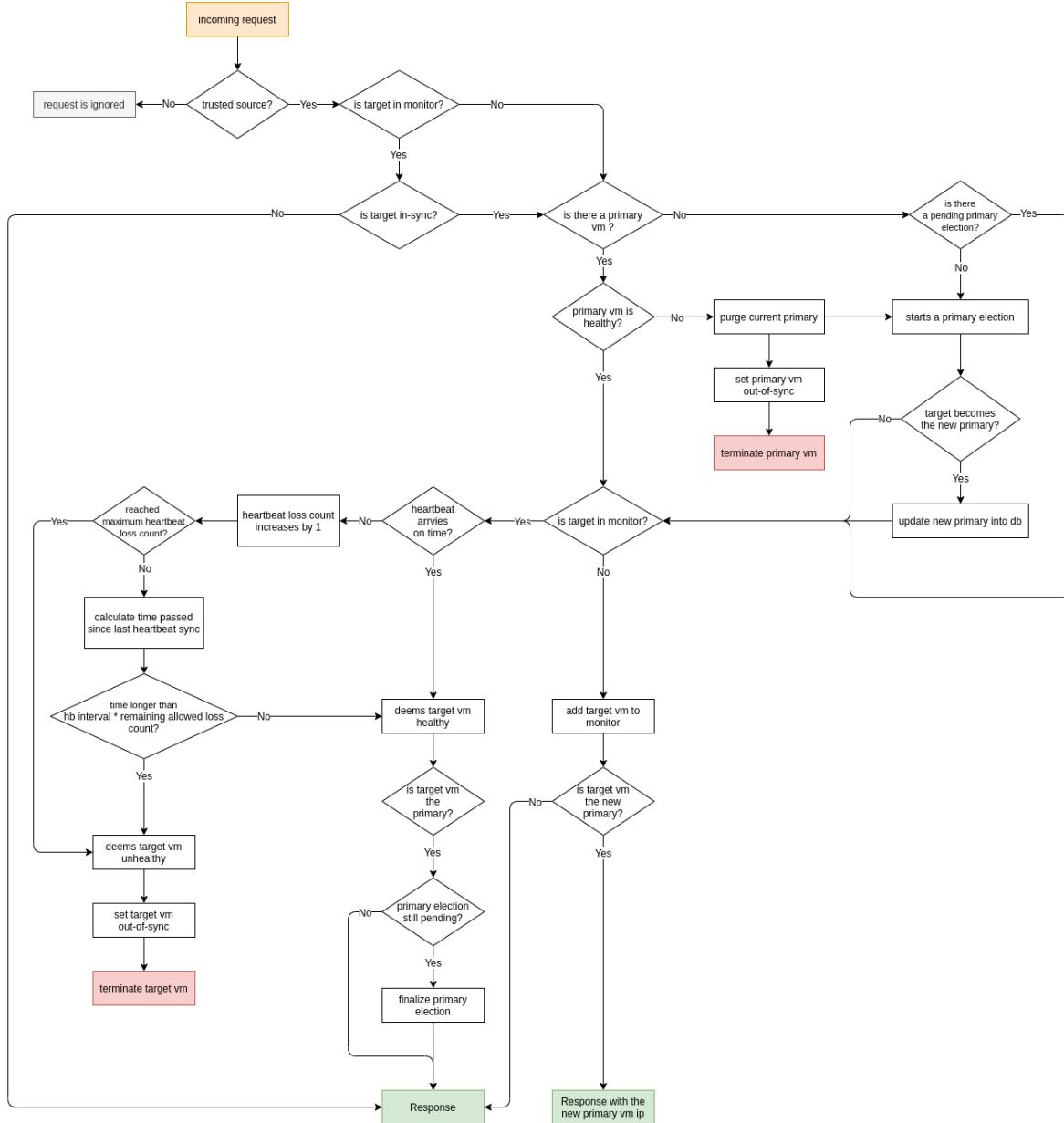
### Autoscale handler flowchart



## Primary election

### FortiGate Autoscale

with heartbeat response & failover management



## Upgrading the deployment

An existing FortiGate Autoscale for Azure deployment can be upgraded in one specific scenario:

- It was deployed with the 2.0.9 template.

To determine which template was used in your deployment, refer to the section [Determining the FortiGate Autoscale release version on page 70](#).



Read these instructions completely before starting an upgrade.

A deployment with the 2.0.9 template can be upgraded only to the 3.3.2 template. During the upgrade, users can optionally consolidate logging and reporting for the FortiGate cluster by integrating FortiAnalyzer 6.2.5 or FortiAnalyzer 6.4.5.

### Prerequisites

- Linux Operating System
- NodeJS 14
- Azure CLI
- FortiGate Autoscale for Azure upgrade templates

### Obtaining the templates

The FortiGate Autoscale for Azure upgrade templates are located in the Fortinet Autoscale for Azure [GitHub project](#). Navigate to the [project release page](#) and download `fortigate-autoscale-azure.zip` for the release *2.0.9 upgrade (3.3.2)*.

Unzip this file on your local PC. The `templates` folder will contain these files:

- `upgrade_fortigate_autoscale_from_2.0.9_to_3.3.2.preparation.json`  
This template prepares the environment for the upgrade.
- `upgrade_fortigate_autoscale_from_2.0.9_to_3.3.2.json`  
This template performs the upgrade from the 2.0.9 template to the 3.3.2 template and pairs with the optional parameter template.
- (optional) `upgrade_fortigate_autoscale_from_2.0.9_to_3.3.2.params.json`  
This parameter template pairs with the upgrade template.
- `upgrade_fortigate_autoscale_from_2.0.9_to_3.3.2.cleanup.json`  
This template finalizes the upgrade process.

### Before you start

Upgrading the deployment requires values from the existing 2.0.9 deployment. The following sections describe how to locate these values.

## Locating values from the 2.0.9 deployment

1. Navigate to the *Microsoft.Template Overview* by following the steps 1-3 of the section [Locating deployment Outputs on page 70](#).
2. On the *Overview* page, note the value for the parameter *Subscription* as you will need it for the upgrade.

The screenshot shows the Microsoft Azure Deployment Overview page for a deployment named "Microsoft.Template-20210721112145". The status message "Your deployment is complete" is displayed. Key parameters shown include:

- Deployment name: Microsoft.Template-20210721112145
- Start time: 7/21/2021
- Correlation ID: [redacted]
- Subscription: [redacted] (highlighted with a red box)
- Resource group: [redacted]

Navigation links on the left include: Overview (highlighted), Inputs, Outputs (highlighted), and Template. A "Go to resource group" button is at the bottom.

3. Click *Outputs* and note the values for the parameters *resourceGroupName* and *vNetResourceGroupName* as you will need them for the upgrade.

The screenshot shows the Microsoft Azure Deployment Outputs page for the same deployment. The "Outputs" tab is selected. Key parameters shown include:

- resourceGroupName: [redacted] (highlighted with a red box)
- storageAccountName: [redacted]
- uniqueResourceNamePrefix: [redacted]
- vNetResourceGroupName: [redacted] (highlighted with a red box)

Navigation links on the left include: Overview, Inputs, Outputs (highlighted), and Template.

4. Click *Inputs*.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the Microsoft Azure logo, a search bar, and a user profile icon. Below the header, the URL 'Home > Microsoft.Template-20210721112145' is visible. The main content area has a title 'Microsoft.Template-20210721112145 | Inputs'. On the left, there's a sidebar with tabs: 'Overview' (disabled), 'Inputs' (selected and highlighted with a red border), 'Outputs' (disabled), and 'Template'. The main pane displays three input parameters: 'accessRestrictionIPRange', 'adminPassword', and 'adminUsername', each with a small edit icon to its right. Red boxes are drawn around each of these three parameters.

5. Make note of values on this page as you will need them for the upgrade.

## Upgrade iteration

*Upgrade Iteration* is an important parameter throughout the entire process. The allowable values for *Upgrade Iteration* are limited to the numbers 2 thru 9. This value is used to form a unique name for the new resources related to the upgrade. If there are errors during the upgrade, the entire stack can be rolled back - the *Upgrade Iteration* value is used to remove the resources which were created.

When performing the upgrade for the first time, set *Upgrade Iteration* to 2. If errors occur, rollback the upgrade and start over with *Upgrade Iteration* set to 3. Repeat if necessary, increasing the value of *Upgrade Iteration* each time.



When a deployment is rolled back, the Key Vault will be **soft-deleted**. Once the Key Vault is permanently deleted, the *Upgrade Iteration* number can be reused. To permanently delete the Key Vault, open the AzureCLI and run the `upgradeIterationCmdDeleteKeyVaultPermanent` command from the *Outputs* of the cleanup template.

## Performing the upgrade

The upgrade solution described here is a rollback-capable solution for preparing, creating, and removing resources. The steps below will guide you through the upgrade process.



Before starting an upgrade, ensure that the values for the 2.0.9 template deployment have been located.

1. Deploy the preparation template as described in the section [Deploying the preparation template on page 86](#).
2. Deploy the upgrade template as described in the section [Deploying the upgrade template on page 86](#).

- Verify the newly deployed resources. For details, refer to the section [Verifying the deployment on page 89](#).



Do not start the BYOL or PAYG VMSS until you initialize the database. In other words, ensure the instance number of the VMSS is set to 0.

- Initialize the database. For details, refer to the section [Initializing the database on page 89](#).
- Start the two new VMSS. For details, refer to the section [Starting a VMSS on page 65](#).
- Observe the FortiGate-VMs running in the two VMSS and ensure they are running correctly.
- Deploy the cleanup template. For details, refer to the section [Deploying the cleanup template on page 91](#).

## Deploying the preparation template

- Create a template deployment using the preparation template. For details, refer to the section [Creating a template deployment on page 45](#). When prompted for parameters, use values as described in the table below:

Parameter display name	2.0.9 template Input	2.0.9 template Output	Value to use
Subscription	*	*	
Resource group		resourceGroupName	Use the value from the 2.0.9 template deployment. Do not change it.
Resource Name Prefix	resourceNamePrefix		
Vnet Resource Group Name		vNetResourceGroupName	
Region	*	*	This value cannot be changed. It is tied to the Resource group.
Upgrade Iteration	*	*	Refer to the section <a href="#">Upgrade iteration on page 85</a> .

\* indicates that there isn't a value present in the 2.0.9 template Inputs or Outputs.

- When deployment of the preparation template has completed, navigate to the *Outputs*. For details, refer to the section [Locating deployment Outputs on page 70](#).
- Copy the `cmdUpdateAllInOne` command.
- Open a terminal in your Linux OS.
- Log in to your Azure account with the command `az login`.
- Run the command `cmdUpdateAllInOne`.
- Wait for the command to be fully finished.

## Deploying the upgrade template

- Create a template deployment using the upgrade template. For details, refer to the section [Creating a template deployment on page 45](#). For descriptions of the variables, refer to the section [Configurable variables on page 49](#). When prompted for parameters, use values as described in the table used when creating a template deployment with the preparation template and from the table below:

Parameter display name	2.0.9 template Input	Value to use
Access Restriction IP Range	accessRestrictionIPRange	Use the value from the 2.0.9 template deployment. May be adjusted to meet the new needs.
Admin Password	adminPassword	Requires manual input. The value from the 2.0.9 template deployment is recommended; a new value may be entered.
Admin Username	adminUsername	Use the value from the 2.0.9 template deployment.
BYOL Instance Count	byollInstanceCount	Use the value from the 2.0.9 template deployment. May be adjusted to meet the new needs.
FOS Version	fosVersion	Use values from the drop-down list. The latest version is recommended.
Forti Analyzer Autoscale Admin Password	*	
Forti Analyzer Autoscale Admin Username	*	
Forti Analyzer Custom Private IP Address	*	Follow the instructions in the parameter description.
Forti Analyzer Instance Type	*	
Forti Analyzer Integration Options	*	
Forti Analyzer Version	*	
Forti Gate PSK Secret	fortiGatePSKSecret	Requires manual input. The value from the 2.0.9 template deployment is recommended; a new value may be entered.
Heart Beat Delay Allowance		
Heart Beat Interval	heartBeatInterval	Use the value from the 2.0.9 template deployment. May be adjusted to meet the new needs.
Heart Beat Loss Count	heartBeatLossCount -	
Instance Type	instanceType -	
Key Vault Name	*	Follow the instructions in the parameter description.

Parameter display name	2.0.9 template Input	Value to use
Max BYOL Instance Count	maxBYOLInstanceCount	
Max PAYG Instance Count	maxPAYGInstanceCount	Use the value from the 2.0.9 template deployment. May be adjusted to meet the new needs.
Min BYOL Instance Count	minBYOLInstanceCount	
Min PAYG Instance Count	minPAYGInstanceCount	
PAYG Instance Count	PAYGInstanceCount	
Package Res URL	packageResURL	Use the template default value. Do not change it.
Primary Election Timeout	masterElectionTimeout	Use the value from the 2.0.9 template deployment. May be adjusted to meet the new needs.
Scale In Threshold	scaleInThreshold	
Scale Out Threshold	scaleOutThreshold	
Service Plan Tier	*	Follow the instructions in the parameter description.
Service Principal App ID	restAppID	Use the value from the 2.0.9 template deployment. Do not change it
Service Principal App Secret	restAppSecret	
Service Principal Object ID	*	Follow the instructions in the parameter description.
Storage Account Type	storageAccountType	Use the value from the 2.0.9 template deployment. May be adjusted to meet the new needs.
Subnet1Name	subnet1Name	
Subnet2Name	subnet2Name	
Subnet3Name	subnet3Name	Follow the instructions in the parameter description.
Subnet4Name	subnet4Name	
Vnet Address Space	vnetAddressSpace	Use the value from the 2.0.9 template deployment. Do not change it.
Vnet Name	vnetName	

If the deployment does not complete successfully, go to the section [Troubleshooting the upgrade on page 92](#).

2. Upload `configset` files to the Storage account. For details, refer to the section [Uploading files to the Storage account on page 55](#).
3. If you will be using BYOL instances, upload `license` files to the Storage account.



License files from the 2.0.9 deployment can be reused . However, re-using a license will invalidate the FortiGate which is currently using the license.

## Verifying the deployment

The FortiGate Autoscale for Azure 3.3.2 template will be deployed into the Resource Group and a new set of the following 6 resources will be created:

- Function App
- App Service plan
- Application Insights
- Storage account
- Azure Cosmos DB account
- Virtual machine scale set (BYOL)
- Virtual machine scale set (PAYG)

These resources will be created with the same name as the previous 2.0.9 resources with the iteration number appended. For example, if the Upgrade Iteration is 2, the number appended is 002. Verify that they have been created. For details on verifying components, refer to the section [Verifying the deployment on page 57](#).

## Initializing the database



Do not scale out the BYOL or PAYG VMSS until you initialize the database.

1. Navigate to the `fgt-as-handler` function. For details on how to do this, refer to the section [To verify the Function App: on page 59](#).
2. Click *Get Function Url* to obtain the Function URL:

The screenshot shows the Azure Functions blade for a function named 'fgt-as-handler'. In the top navigation bar, there is a 'Get Function Url' button. A modal dialog box titled 'Get Function Url' is open, showing the URL field populated with 'https://[REDACTED]p002.azurewebsites.net/api/fgt-as-handler?code=[REDACTED]'. The entire URL field is highlighted with a red box. The background of the portal shows other function keys and resource groups.

- 
3. Open a web browser to run the URL. The expected response is an error as shown below:



## This page isn't working

**102.azurewebsites.net** is currently unable to handle this request.

HTTP ERROR 500

[Reload](#)

- 
4. Navigate to the cosmos DB account of the current upgrade iteration. For details on how to do this, refer to steps 1 and 2 in the section [To verify the database: on page 59](#).
5. On the right hand side, expand the database *FortiGateAutoscale*.
6. Expand the container *Settings*.
7. Click on *Items*.

8. Confirm that the Settings container has items.

id	IsSettingKey
additional-config-set-na...	additional-config-set-na...
autoscale-function-exte...	autoscale-function-exte...
autoscale-function-max...	autoscale-function-max...
autoscale-handler-url	autoscale-handler-url
asset-storage-name	asset-storage-name
asset-storage-key-prefix	asset-storage-key-prefix
byol-scaling-group-desi...	byol-scaling-group-desi...
byol-scaling-group-min...	byol-scaling-group-min...
custom-asset-directory	custom-asset-directory
byol-scaling-group-name	byol-scaling-group-name
byol-scaling-group-max...	byol-scaling-group-max...
custom-asset-container	custom-asset-container
enable-external-elb	enable-external-elb
enable-hybrid-licensing	enable-hybrid-licensing
enable-internal-elb	enable-internal-elb
enable-second-nic	enable-second-nic
enable-vm-info-cache	enable-vm-info-cache
heartbeat-delay-allowa...	heartbeat-delay-allowa...
heartbeat-interval	heartbeat-interval
heartbeat-loss-count	heartbeat-loss-count
primary-election-timeout	primary-election-timeout

## Deploying the cleanup template

1. Create a template deployment using the cleanup template. For details, refer to the section [Creating a template deployment on page 45](#). When prompted for parameters, use values as described in the table below:

Parameter display name	2.0.9 template Input	2.0.9 template Output	Value to use
Subscription	*	*	
Resource group		resourceGroupName	Use the value from the 2.0.9 template deployment. Do not change it.
Resource Name Prefix	resourceNamePrefix		
Vnet Resource Group Name		vNetResourceGroupName	
Region	*	*	This value cannot be changed. It is tied to the Resource group.

Parameter display name	2.0.9 template Input	2.0.9 template Output	Value to use
Upgrade Iteration	*	*	Use the iteration number for the upgrade iteration you want to continue with

\* indicates that there isn't a value present in the 2.0.9 template Inputs or Outputs.

2. When deployment of the cleanup template has completed, navigate to the *Outputs*.
3. Copy the command appropriate for your activity:
  - To finalize the upgrade, copy the `cleanUpOldComponentCmdDeleteAllInOne` command.
  - To roll back the upgrade, copy the `upgradeIterationCmdDeleteAllInOne` command.
4. Open a terminal in your Linux OS.
5. Log in to your Azure account with the command `az login`.
6. Run the copied command.
7. Wait for the command to be fully finished.

## Troubleshooting the upgrade

As long as an upgrade process isn't finalized, it is regarded as an incomplete upgrade iteration. Reasons for not finalizing can include errors and user intervention.

In the case of an incomplete upgrade iteration, roll back the upgrade iteration and perform the upgrade again with a different value for *Upgrade Iteration*. It is suggested that the value be increased by 1 with each successive deployment.

### Rolling back an incomplete upgrade iteration

Users have the option of rolling back an upgrade iteration by deploying the cleanup template. When deployed, newly created resources related to the upgrade iteration will be released. It is recommended to rollback right away before starting a new upgrade iteration. This option must be used if all the allowable *Upgrade Iteration* values (2-9) have been used up.



When a deployment is rolled back, the Key Vault will be [soft-deleted](#). Once the Key Vault is permanently deleted, the *Upgrade Iteration* number can be reused. To permanently delete the Key Vault, open the Azure CLI and run the `upgradeIterationCmdDeleteKeyVaultPermanent` command from the *Outputs* of the cleanup template.

## Document history

Template	Date Released	Details
special release	August 25, 2021	This special release is for upgrading from the 2.0.9 template to the 3.3.2 template.
3.3.2	June 11, 2021	Documentation was not updated.
3.3.0	May 25, 2021	Added support for FortiAnalyzer.
3.1.1	February 4, 2021	Added support for FortiOS 6.4.3. Removed support for FortiOS 6.2.x.
3.0.0	September 23, 2020	Added support for FortiOS 6.2.3.
2.0.5	February 25, 2020	Added support for FortiOS 6.0.9.
2.0	October 8, 2019	FortiGate Autoscale 2.0.0 General Availability Added support for Hybrid Licensing (any combination of BYOL and/or PAYG instances).
1.0	April 19, 2019	FortiGate Autoscale General Availability Supports auto scaling for PAYG instances only. Requires FortiOS 6.0.6 or FortiOS 6.2.1. Documentation is no longer maintained and is only available as a PDF: <ul style="list-style-type: none"><li>• <a href="#">Deploying auto scaling on Azure 1.0</a></li></ul>

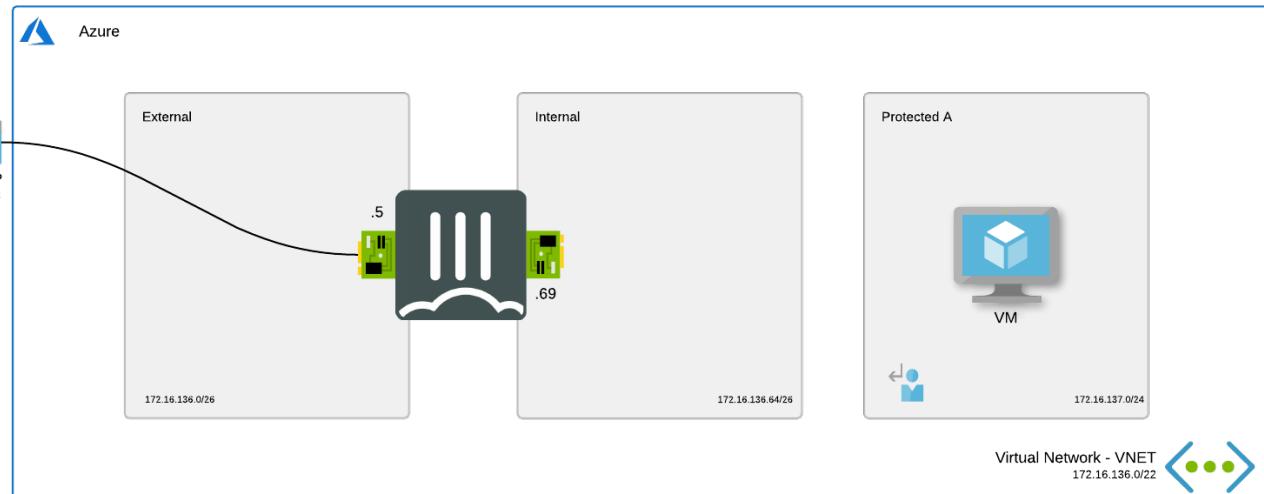
# Single FortiGate-VM deployment

You can deploy FortiGate-VM NGFW for Azure as a virtual appliance in the Azure cloud (IaaS). This section shows you how to install and configure a single instance FortiGate-VM in Azure to provide a full NGFW/unified threat management (UTM) security solution in front of Azure IaaS resources.

This section covers the deployment of simple web servers, but you can use this deployment type for any type of public resource protection with only slight modifications. With this architecture as a starting point, you can implement more advanced solutions, including multilayered solutions.

The example in this document creates three subnets:

Subnet	Description
Subnet1	External subnet used to connect the FortiGate-VM to the Internet.
Subnet2	Internal subnet used as a transit network to one or multiple protected networks containing backend services, such as the web server.
Subnet3	Protected subnet used to deploy services. You can deploy multiples of these subnets. The traffic is sent to the FortiGate for inspection using UDR.



## Registering and downloading your license

FortiGate-VM for Azure supports both BYOL and PAYG licensing models. If you are deploying a FortiGate-VM in the Azure marketplace with BYOL, you must obtain a license to activate it.

You can obtain licenses through any Fortinet partner. If you do not have a partner, contact [azuresales@fortinet.com](mailto:azuresales@fortinet.com) for assistance in purchasing a license.

See [Creating a support account on page 12](#).

## Deploying the FortiGate-VM

There are different deployment methods for the FortiGate-VM related to the different deployment methods that the Azure platform supports. This guide focuses on the Azure portal. This offers a convenient and guided deployment. For more automated deployment, ARM templates or Terraform are available on the Fortinet GitHub.

### To deploy the FortiGate-VM:

1. In the Azure dashboard, select *Create a resource* and search for FortiGate.
2. Locate the Fortinet FortiGate Next-Generation Firewall listing and select it.
3. From the *Select a plan* dropdown list, select *Single VM*. Click *Create*.
4. Configure the options on the *Basics* tab according to your requirements:
  - a. For *Resource Group*, create a new resource group or select an existing one. Deploying the solution to a new or empty resource group is recommended. You can deploy the solution to an existing resource group that already contains resources, but this may overwrite existing resources.
  - b. From the *Region* dropdown list, select the desired region. FortiGate-VM is available in all public regions of Azure and the China and Gov regions. Availability depends on the access rights of the Azure subscription used for deployment.
  - c. In the *FortiGate administrative username* field, enter the username that will be used to manage the FortiGate. The username cannot be a common username such as root, admin, or administrator. After deployment, you can reset the username and password from the Azure portal interface, resulting in a system reboot.
  - d. In the *FortiGate password* field, enter the password used to manage the FortiGate via the GUI or CLI. The password must be at least twelve characters and contain one or more of the following tokens: uppercase letters, lowercase letters, digits, and special characters: ~!@#\$%^&\* \_+=`|\(){}[];"<>,.?/.
  - e. In the *Fortigate Name Prefix* field, enter the desired prefix. All resources will contain the prefix in their name.
  - f. From the *Fortigate Image SKU* dropdown list, select the license type. PAYG is billed through Azure as an additional charge to compute usage.
  - g. From the *Fortigate Image Version* dropdown list, select the desired FortiGate version. The default option installs the latest FortiGate version.

Create Fortinet FortiGate Next-Generation Firewall ...

The screenshot shows the 'Create Fortinet FortiGate Next-Generation Firewall' wizard in the Azure portal, specifically the 'Basics' step. The top navigation bar includes 'Basics', 'Instance Type', 'Networking', 'Public IP', 'Advanced', and 'Review + create'. Below this, the 'Project details' section asks for a subscription and resource group. A note says: 'Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.' The 'Subscription' dropdown is set to 'EMEA-CSE'. The 'Resource group' dropdown is set to '(New) FGTDODC-RG', with a 'Create new' link below it. The 'Instance details' section contains fields for 'Region', 'FortiGate administrative username', 'FortiGate password', 'Confirm password', 'Fortigate Name Prefix', 'Fortigate Image SKU', and 'Fortigate Image Version'. Most fields have validation icons (green checkmarks or exclamation marks). The 'Region' dropdown is set to 'West Europe'. The 'FortiGate administrative username' is 'azureuser'. The 'FortiGate password' and 'Confirm password' fields both show masked text. The 'Fortigate Name Prefix' is 'FGT'. The 'Fortigate Image SKU' is 'Bring Your Own License'. The 'Fortigate Image Version' is 'latest'.

5. For *Instance Type*, select the instance type according to the purchased BYOL license or the anticipated cost per hour. Licensing is based on the number of utilized vCPUs. You can resize the VM later if needed. See [Instance type support on page 6](#).
6. On the *Networking* tab, configure the following:
  - a. Configure the networks. You can deploy the FortiGate in an existing VNet or create a new VNet. If deploying to an existing VNet, you must already have three subnets to use for the FortiGate-VM. The FortiGate-VM requires a public and private interface for Internet edge protection. Ensuring that the external and internal subnets of the FortiGate are empty or do not contain other networking devices that require routing is recommended.
  - b. Enable *Accelerated Networking* if desired. You can enable this option to have a direct path from the VM to the Azure infrastructure NIC and allows for better performance. This is only available for specific instance types. See [Enabling accelerated networking on the FortiGate-VM on page 39](#).

### Create Fortinet FortiGate Next-Generation Firewall

The screenshot shows the 'Networking' tab of the Fortinet FortiGate creation wizard. It includes sections for 'Configure Internal Networking' and 'Configure virtual networks'. Under 'Configure virtual networks', there are dropdown menus for 'Virtual network' (set to 'FGT-VNET'), 'External Subnet' (set to 'ExternalSubnet (172.16.136.0/26)'), 'Internal subnet' (set to 'InternalSubnet (172.16.136.64/26)'), and 'Protected subnet' (set to 'ProtectedSubnet (172.16.137.0/24)'). Below these, a note explains the subnet roles. Under 'Accelerated networking', it shows 'Enabled' selected. A note below explains the requirement for supported instance sizes.

Basics Instance Type Networking Public IP Advanced Review + create

Configure Internal Networking

Create a new or select an existing virtual network with the required subnets.

Configure virtual networks

Virtual network \* ⓘ FGT-VNET  
Create new

External Subnet \* ⓘ ExternalSubnet (172.16.136.0/26)  
Manage subnet configuration

Internal subnet \* ⓘ InternalSubnet (172.16.136.64/26)  
Manage subnet configuration

Protected subnet \* ⓘ ProtectedSubnet (172.16.137.0/24)  
Manage subnet configuration

**i** The external subnet will have a public IP attached to the FortiGate network interface. The internal subnet is a transit subnet containing only the FortiGate interfaces for traffic to and from the internal networks. Internal systems should be installed in a protected subnet with user defined route configuration.

Accelerated networking

Enables SR-IOV support allowing direct access from the NIC in the Azure infrastructure to the FortiGate VM.  
[Learn more](#)

Accelerated Networking ⓘ  Enabled  Disabled

**i** Accelerated Networking is supported on most general purpose and compute-optimized instance sizes with 2 or more vCPUs. On instances that support hyperthreading, Accelerated Networking is supported on VM instances with 4 or more vCPUs. Deployment with the accelerated networking feature enabled on a host that doesn't support it will result in a failure to connect to it. The accelerated networking can be disabled after deployment from the Azure Portal or Azure CLI.

7. On the *Public IP* tab, create a new public IP address or select an existing unattached public IP address. The public IP address can be a basic or standard SKU public IP address. A highly available setup requires a standard SKU public IP address. Upgrading from a basic to a standard SKU public IP address is supported. See [Upgrade public IP addresses](#).
8. On the *Advanced* tab, configure the following:
  - a. In the *FortiManager* section, provide FortiManager details if desired. During deployment, the FortiGate can reach out and register itself to a FortiManager using the provided details.
  - b. In the *Custom Data* field, add additional configuration if desired. This provides a configuration to the FortiGate during deployment. For example, you can enter FortiOS CLI commands.
  - c. If using a BYOL license, upload the license so that it can be provided during deployment to the FortiGate.

**9.** Launch the FortiGate deployment:

- a. You are finished configuring the options. Once validation is passed, click *OK*.
- 



If you want to download the template, click *Download template and parameters*.

- 
- b. Click *Create*. After deploying the template, you should see the deployment progress and the parameters and template that Azure is progressing. Once deployed, the new resources show in the resource group.

## Connecting to the FortiGate-VM

### To connect to the FortiGate-VM:

1. Open the FGTPublicIP resource and copy the IP address that Azure assigned.
2. In a web browser, connect to the IP address using HTTPS on port 443. You can also use an SSH client on port 22.
3. The system displays a warning that the certificate is not trusted. This is expected since the FortiGate-VM is using a self-signed certificate. If desired, replace the certificate with a signed certificate.
4. Sign in with the credentials specified in the Azure template parameters.
5. If you chose a BYOL deployment, you must upload a license and reboot the FortiGate-VM before continuing. See [Registering and Downloading](#).

## Azure routing and network interfaces

On the Azure platform and the FortiGate-VM, the private IP addresses of both interfaces are configured using static assignment using deployment.

In the static routing, a default route has been configured towards the default gateway of the external network on port1. All internal networks are routed to the internal/transit network on port2. The gateway IP address on the Microsoft side is always the first IP address in the subnet IP address range.

Azure uses the 168.63.129.16 address for various services. You can configure an additional route to ensure that this traffic always leaves via port1. See [What is IP address 168.63.129.16?](#)

During deployment, a route table is created and attached to the protected subnet. This routing table contains three user-defined routes. The default route 0.0.0.0/0 points to the FortiGate-VM internal IP address. This catches all traffic except for the virtual network traffic and sends it to the FortiGate-VM for inspection.

The virtual network is created as well and forces traffic for additional protected networks to pass through the FortiGate-VM. As Azure applies these subnet routes to each VM, an additional route is needed for the local subnet to send its traffic directly to the VNet. If this route is omitted, you will have microsegmentation sending all traffic between the VMs in the protected subnet also via the FortiGate-VM.

If no internal segmentation is required, you can delete the VNet routes.

Verify that the route table is attached to the ProtectedSubnet. Also ensure that the UDR routes include the destination networks.

## Single FortiGate-VM deployment

To verify and troubleshoot routing, the effective route tables can be requested from each network interface of a running VM. The screenshot shows that the default routes have been invalidated by the UDR deployed within the FortiGate.

The screenshot shows the Azure portal interface for a FortiGate-VM named fgtlnx617. The left sidebar contains navigation links for Home, FGTLNX, Overview, Activity log, Access control (IAM), Tags, Settings (IP configurations, DNS servers, Network security group, Properties, Locks), Monitoring (Alerts, Metrics, Diagnostic settings), Automation (Tasks (preview), Export template), and Support + troubleshooting (Effective security rules, Effective routes). The 'Effective routes' link under Support + troubleshooting is highlighted. The main content area displays the 'Effective routes' table for the 'Network interface (fgtlnx617)' with the associated route table set to 'FGT-RT-PROTECTED'. The table has columns for Source, State, Address Prefixes, Next Hop Type, Next Hop IP Address, and User Defined Route Name. The data is as follows:

Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address	User Defined Route Name
User	Active	172.16.137.0/24	Virtual network	-	Subnet
Default	Invalid	172.16.136.0/22	Virtual network	-	-
Default	Invalid	0.0.0.0/0	Internet	-	-
User	Active	172.16.136.0/22	Virtual appliance	172.16.136.68	VirtualNetwork
User	Active	0.0.0.0/0	Virtual appliance	172.16.136.68	Default

## Using public IP addresses

Azure does not publicly route IP addresses within a VNet, so you cannot assign a public IP address to another VM and still filter that traffic through a FortiGate-VM on Azure. Instead, you must assign the public IP addresses to the vNICs associated with the FortiGate-VM, then configure the FortiGate-VM to forward that traffic. Further, in most cases, Azure provides 1:1 NAT between the assigned public IP address and the assigned local IP address. Thus, the FortiGate-VM must forward packets using the local IP address.

A single FortiGate-VM deployment from the Azure marketplace includes one Azure IP address configuration containing a public IP address and a local IP address. Azure performs 1:1 NAT between the two as traffic enters and exits the VNet. This configuration is called an instance-level public IP address. All types of protocols are forwarded using NAT from an external public IP address to the FortiGate private IP address that is linked to it in the network interface on Azure.

The following shows the default Azure vNIC and FortiOS configurations:

## Single FortiGate-VM deployment

Home > Resource groups > FGTDOC-RG > FGT-FGT-A

**FGT-FGT-A | Networking** X

Virtual machine

Search (Cmd+)/<> Attach network interface Detach network interface

Overview Activity log Access control (IAM) Tags Diagnose and solve problems

Settings Networking

IP configuration: ipconfig1 (Primary)

Network Interface: FGT-FGT-A-Nic1 Effective security rules Troubleshoot VM connection issues Topology

Virtual network/subnet: FGT-VNET/ExternalSubnet NIC Public IP: 51.137.82.25 NIC Private IP: 172.16.136.4 Accelerated networking: Enabled

Inbound port rules Outbound port rules Application security groups Load balancing

Network security group FGT-hynhxqfuhcouy-NSG (attached to network interface: FGT-FGT-A-Nic1)  
Impacts 0 subnets, 2 network interfaces Add inbound port rule

Priority	Name	Port	Protocol	Source	Destination
100	AllowAllInbound	Any	Any	Any	Any
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowAzureLoadBalancerInBou...	Any	Any	AzureLoadBalancer	Any
65500	DenyAllInBound	Any	Any	Any	Any

Home > Resource groups > FGTDOC-RG > FGT-FGT-A > FGT-FGT-A-Nic1 >

**ipconfig1** ...

FGT-FGT-A-Nic1

Save Discard

Public IP address settings

Public IP address Disassociate Associate

Public IP address \* FGTPublicIP (51.137.82.25) Create new

Private IP address settings

Virtual network/subnet FGT-VNET/ExternalSubnet

Assignment Dynamic Static

IP address \* 172.16.136.4

## Single FortiGate-VM deployment

Name  Alias

Type  Physical Interface

VRF ID  Role

Address

Addressing mode  Manual  DHCP  Auto-managed by FortiIPAM

IP/Netmask

Secondary IP address

Administrative Access

IPv4  HTTPS  FMG-Access  FTP  HTTP  SSH  RADIUS Accounting  PING  SNMP  Security Fabric Connection

Receive LLDP  Use VDOM Setting  Enable  Disable

Transmit LLDP  Use VDOM Setting  Enable  Disable

DHCP Server

Network

Device detection  Security mode

Traffic Shaping

Outbound shaping profile

Miscellaneous

Comments  8/255

Status  Enabled  Disabled

To use this public IP address for public access to an internal server, you must configure a virtual IP address, which enables a DNAT conversion of packets, and a policy to allow the traffic.

Edit Virtual IP

VIP type IPv4

Name  Comments  0/255

Color  Change

Network

Interface  Type Static NAT

External IP address/range  Mapped IP address/range

Optional Filters

Port Forwarding

Protocol  TCP  UDP  SCTP  ICMP

External service port  Map to port

The external IP address matches the local IP address assigned to port1. The mapped IP address in this case is the internal web server's IP address, and only TCP port 80 is set to forward. You can also use PAT here to modify the original destination port in cases where there is a mismatch with the internal server's destination port. Using this feature, you can configure multiple virtual IP addresses to internal web servers using TCP port 80 by using custom external ports (8080 in this example). However, for each assigned local IP address, you can only use any given external TCP port once.

## Single FortiGate-VM deployment

The screenshot shows the FortiGate policy configuration screen. A new policy named "InboundHTTP" is being created. The configuration includes:

- Name:** InboundHTTP
- Incoming Interface:** port1
- Outgoing Interface:** port2
- Source:** all
- Destination:** Port80to ProtectedServer
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (selected)
- Inspection Mode:** Flow-based (selected)
- Firewall / Network Options:** NAT is disabled. Protocol Options are set to PROT default.
- Security Profiles:** AntiVirus, Web Filter, DNS Filter, Application Control, IPS, and File Filter are all disabled.
- SSL Inspection:** SSL no-inspection is selected.

Here the policy is set to allow traffic coming in port1 to exit port2 if it is destined to the previously created virtual IP address.

To add a public IP address, create a new IP address configuration for the vNIC in the Azure portal. Click the *Add* button in *IP configurations* in the vNIC resource view.

The screenshot shows the "Add IP configuration" dialog for a vNIC named "FGT-FGT-A-Nic1". The configuration includes:

- Name:** ipconfig2
- Type:** Primary
- Private IP address settings:** Allocation is set to Static, and the IP address is 172.16.136.5.
- Public IP address:** Disassociate is selected.
- Public IP address \***: Choose public IP address (dropdown menu) and Create new (button).
- Add a public IP address dialog:** Name is FGT-PIP2, SKU is Standard, Assignment is Static. Buttons: OK and Cancel.

A note at the bottom of the main dialog states: "Primary IP configuration already exists".

## Single FortiGate-VM deployment

---

The new local address should be static and must be in the same subnet as the primary IP address configuration. Enable the public IP address and create a new public IP address resource or select an existing one. If you have an existing public IP address assigned to an internal server, you can first dissociate it from that vNIC, then assign it here.

Once you have configured both IP addresses on the Azure side, you can create an additional virtual IP address on the FortiGate-VM. You do not need to modify the interface configuration on the FortiGate-VM.

The screenshot shows the 'Edit Virtual IP' dialog box. The 'VIP type' is set to 'IPv4'. The 'Name' field contains 'SecondPIP'. The 'Comments' field is empty. The 'Color' button is visible. Under the 'Network' section, the 'Interface' dropdown is set to 'port1'. The 'Type' is 'Static NAT'. The 'External IP address/range' field contains '172.16.136.5'. The 'Mapped IP address/range' field contains '172.16.137.5'. Below the main form, there are two collapsed sections: 'Optional Filters' and 'Port Forwarding'.

In this example, port forwarding is not enabled. You can enable port forwarding if you want to forward only a specific TCP or UDP port or port range. If you do not enable port forwarding, this enables forwarding of all ports designated to the new public IP address to the internal server, in this case at 172.16.137.5.

## Single FortiGate-VM deployment

The screenshot shows the 'New Policy' configuration window. The policy details are as follows:

- Name:** InboundServer2
- Incoming Interface:** port1
- Outgoing Interface:** port2
- Source:** all
- Destination:** SecondPIP
- Schedule:** always
- Action:** ACCEPT (selected)
- Inspection Mode:** Flow-based (selected)
- Firewall / Network Options:** NAT is enabled.
- Protocol Options:** PROT default
- Security Profiles:** AntiVirus, Web Filter, DNS Filter, Application Control, IPS, File Filter are disabled.
- SSL Inspection:** SSL no-inspection
- Logging Options:** Log Allowed Traffic (Security Events selected), Generate Logs when Session Starts, Capture Packets are enabled.
- Comments:** Write a comment... (0/1023)
- Enable this policy:** Enabled (green switch)

This policy matches the new virtual IP address destination and also allows all services to be forwarded. You can repeat this process for adding as many public IP addresses as needed, although you may run into Azure quota limitations.

When configuring an outbound rule for your server, you can create a general rule. All traffic will be NATed behind the external interface private IP address. Azure will SNAT these packets subsequently to the linked instance-level public IP address.

Outgoing traffic for the secondary server behind the secondary VIP, without the port configuration, will automatically SNAT behind the external IP address in the VIP.

## Single FortiGate-VM deployment

New Policy

Name	Outbound
Incoming Interface	port2
Outgoing interface	port1
Source	all
Destination	all
Schedule	always
Service	ALL
Action	<input checked="" type="radio"/> ACCEPT <input type="radio"/> DENY
Inspection Mode	<input checked="" type="radio"/> Flow-based <input type="radio"/> Proxy-based
Firewall / Network Options	
NAT	<input checked="" type="radio"/>
IP Pool Configuration	<input type="radio"/> Use Outgoing Interface Address <input checked="" type="radio"/> Use Dynamic IP Pool
Preserve Source Port	<input type="radio"/>
Protocol Options	PROT default <input type="button" value="edit"/>

# HA for FortiGate-VM on Azure

You can use FortiGate-VM in different scenarios to protect assets that are deployed in Azure virtual networks:

- Secure hybrid cloud
- Cloud security services hub
- Logical intent-based segmentation
- Secure remote access

See [Fortinet Use Cases for Microsoft Azure](#) for a general overview of different public cloud use cases.

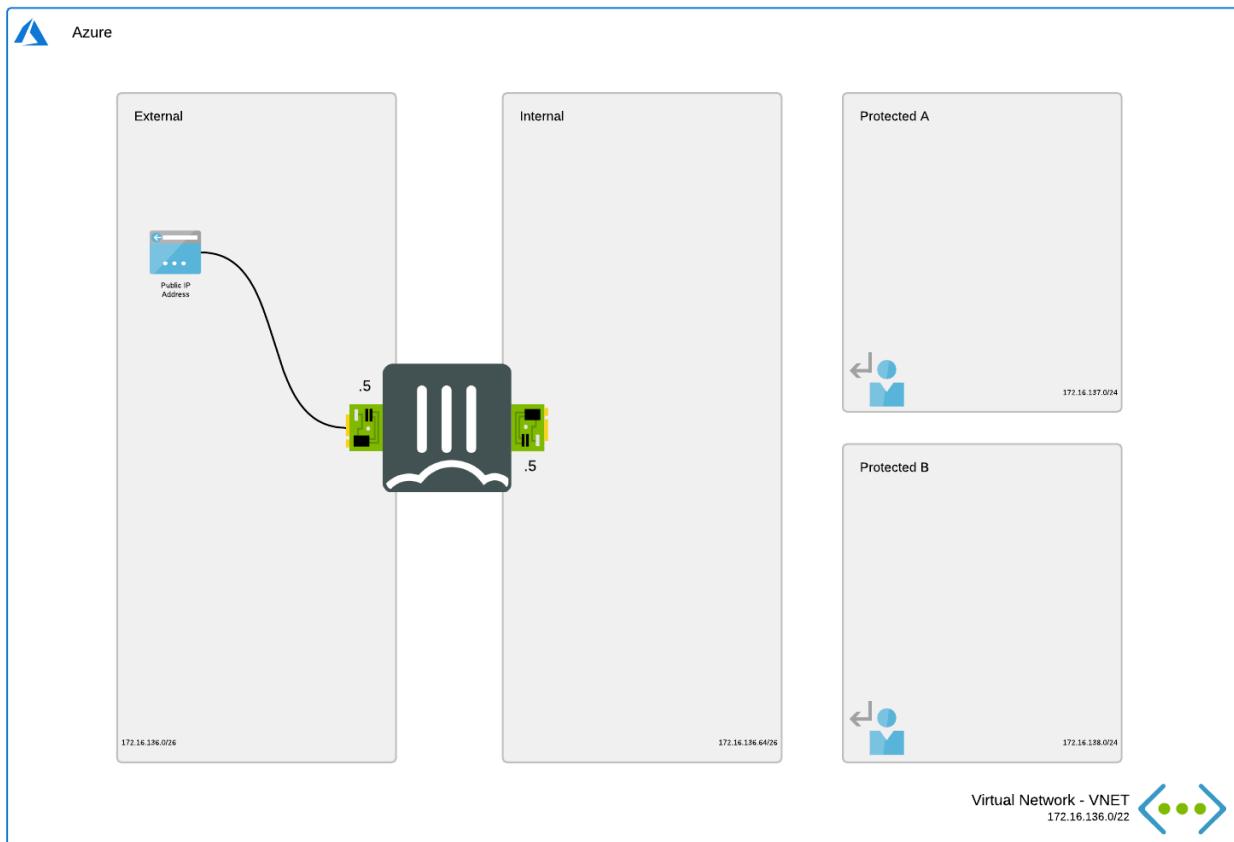
When designing a reliable architecture in Azure, you must take resiliency and high availability (HA) into account. See Microsoft's [Overview of the reliability pillar](#). Running the FortiGate next generation firewall inside Azure offers different reliability levels depending on the building blocks used.

Microsoft offers different [SLAs](#) on Azure based on the deployment that you use:

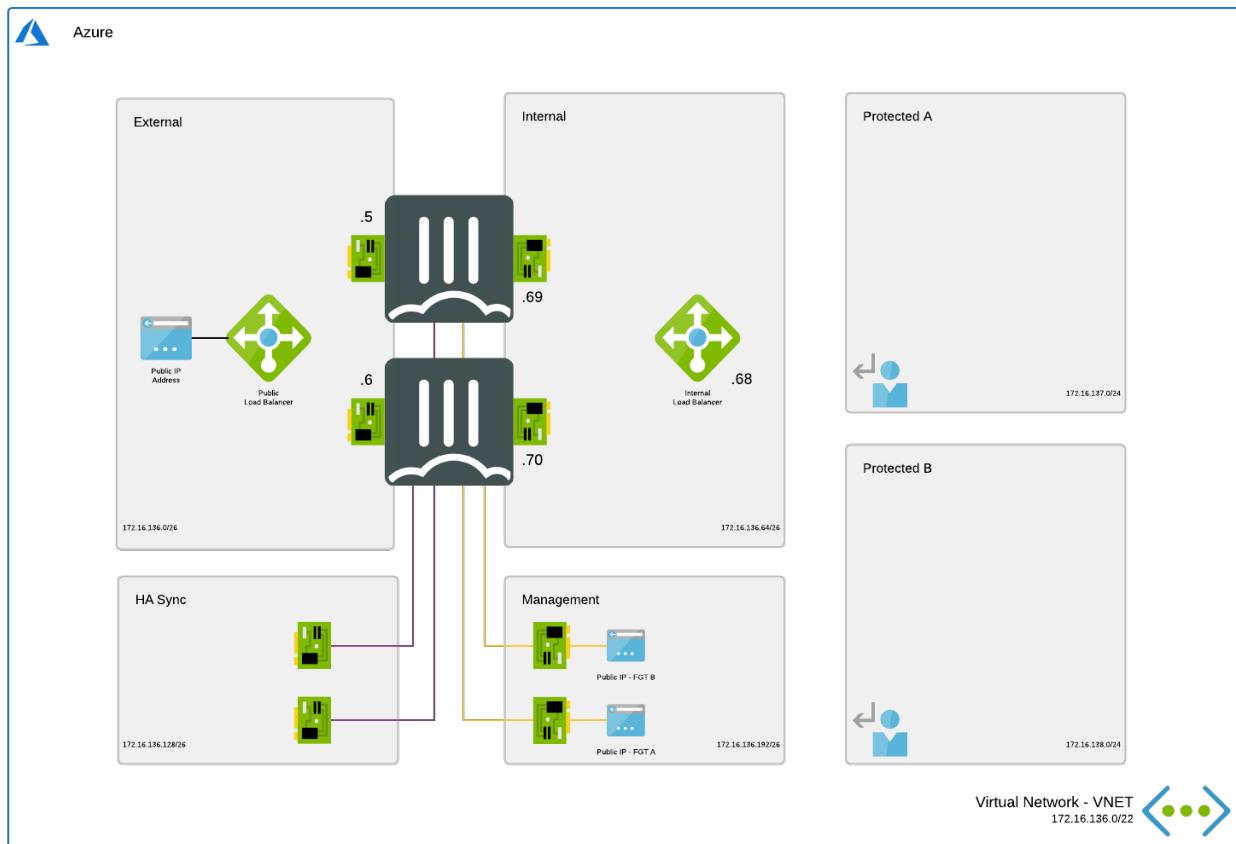
- [Availability Zone \(AZ\)](#) (different datacenter in the same region): 99.99%
- Availability Set (different rack and power): 99.95%
- Single VM with premium SSD: 99.9%

## Building blocks

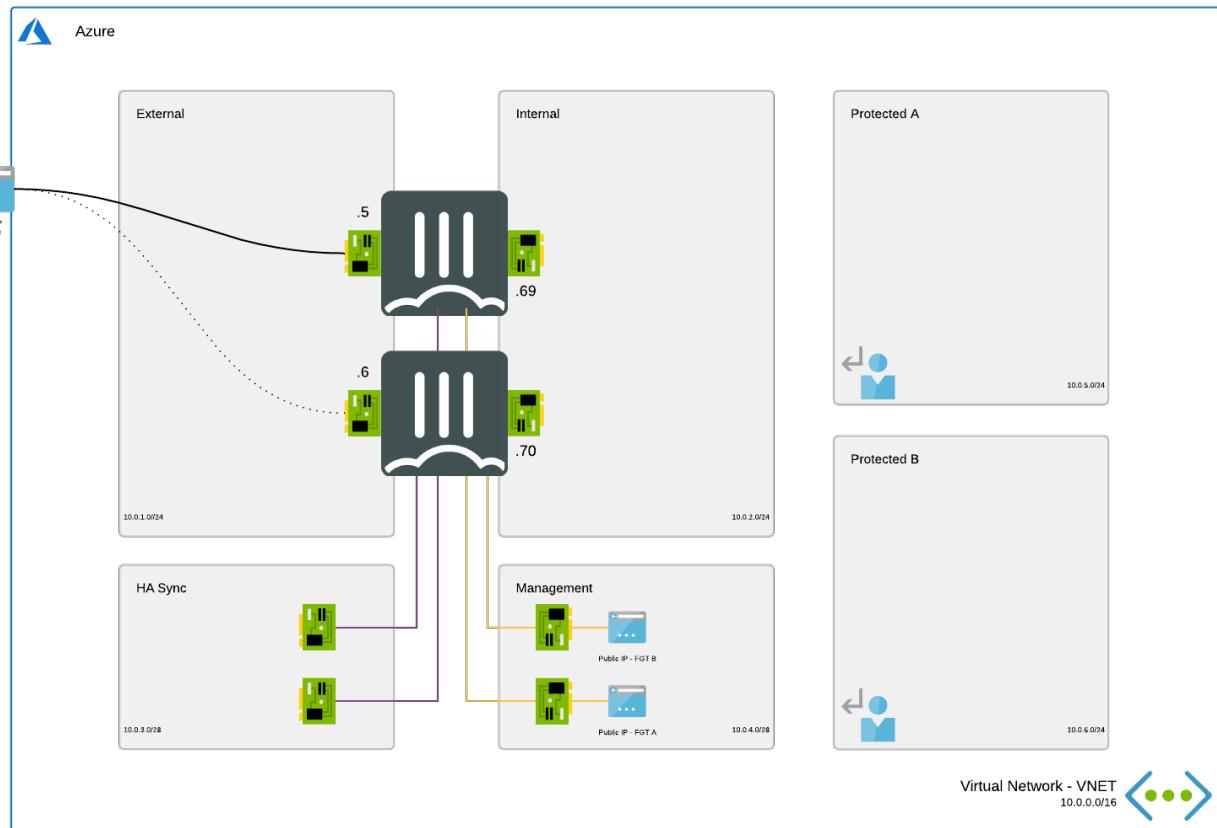
- **Single VM:** This single FortiGate-VM processes all the traffic and becomes a single point of failure during operations and upgrades. You can also use this block in an architecture with multiple regions where a FortiGate is deployed in each region. This setup provides an SLA of 99.9% when using a premium SSD disk. See [Single FortiGate-VM deployment](#).



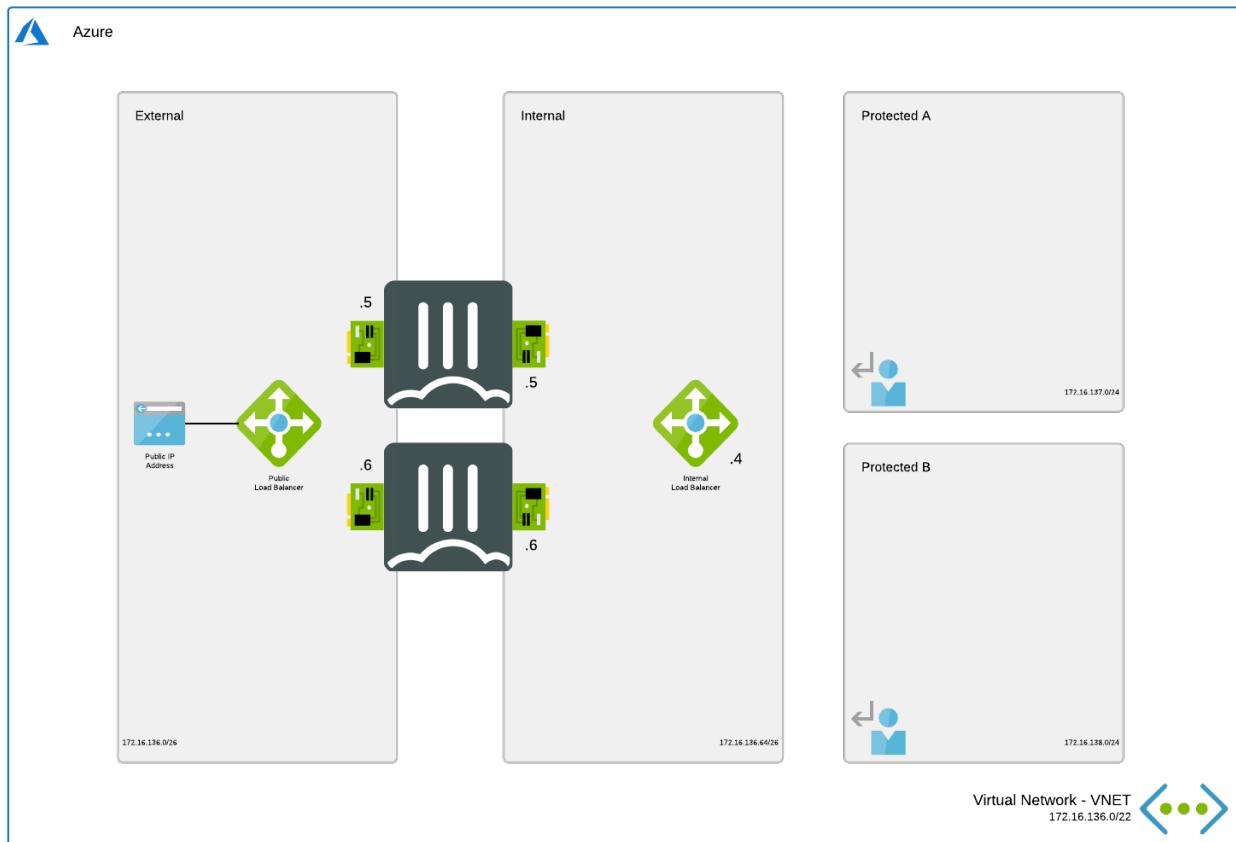
- **Active-passive with external and internal Azure load balancer:** This design deploys two FortiGate-VMs in active-passive mode connected using Unicast FGCP HA protocol. In this setup, the Azure load balancer handles traffic failover using a health probe towards the FortiGate-VMs. The failover times are based on the health probe of the Azure load balancer: 2 failed attempts per 5 seconds with a maximum of 15 seconds. The public IP addresses are configured on the Azure load balancer and provide ingress and egress flows with inspection from the FortiGate. Microsoft provides [guidance](#) on this architecture.



- **Active-passive HA with SDN connector failover:** This design deploys two FortiGate-VMs in active-passive mode connected using the Unicast FGCP HA protocol. This protocol synchronizes the configuration. On failover, the passive FortiGate takes control and issues API calls to Azure to shift the public IP address and update the internal user-defined routing to itself. Shifting the public IP address and gateway IP addresses of the routes takes time for Azure to complete. Microsoft provides a [general architecture](#). In FortiGate's case, the API calls logic is built-in instead of requiring additional outside logic like Azure Functions or ZooKeeper nodes.



- Active-active with external and internal Azure load balancer:** This design deploys two FortiGate-VMs in active-active as two independent systems. In this setup, the Azure load balancer handles traffic failover using a health probe towards the FortiGate-VMs. The public IP addresses are configured on the Azure load balancer and provide ingress and egress flows with inspection from the FortiGate. You can use a FortiManager or local replication to synchronize configuration in this setup. Microsoft provides [guidance](#) on this architecture.



By default, these building blocks use availability sets. The [Availability Zone templates](#) are also available for a higher SLA.

## Architecture

You can deploy the FortiGate-VM in Azure in different architectures. Each architecture has specific properties that can be advantages or disadvantages in your environment:

Architecture	Description
Single VNet	All building blocks above are ready to deploy in a new or existing VNet. Select your block to get started.
Cloud Security Services Hub (VNet peering)	With VNet peering, you can have different islands deploying different services managed by different internal and/or external teams, while maintaining a single point of control going to on-premise, other clouds, or public Internet. The VNets are connected in a hub-spoke setup where the hub controls all traffic. See <a href="#">VNET Peering</a> .
Autoscaling	For applications that are fluid in the amount of resources they consume, you can deploy the FortiGate-VM in an autoscaling architecture. See <a href="#">Deploying autoscaling on Azure</a> on page 42.

## Subscribing to the FortiGate-VM

See [Deploying FortiGate-VM from the marketplace on page 37](#).

# SDN connector integration with Azure

## Configuring an SDN connector in Azure

In this section, you configure FortiGate SDN connector for use with Azure.

In the FortiGate interface, these connectors are called SDN connectors and are SDN connectors that provide integration and orchestration of Fortinet products with key SDN solutions. The Fortinet Security Fabric provides visibility into your security posture across multiple cloud networks, spanning private, public, and Software as a Service (SaaS) clouds. In software-defined networks like Azure, dynamic objects and resources can be cumbersome to secure using traditional firewall policies. By using the SDN connector for use with the Azure IaaS, changes to attributes in the Azure environment can be automatically updated in the Security Fabric. This helps integrate and orchestrate FortiOS IPv4 policies going forward.

Before installing and configuring the Azure SDN connector, the following Azure infrastructure and Fortinet FortiGate-VM components should be in place:

- A valid Azure account and subscription. The account can be one that your organization established or simply one of the [free trial options available from Azure](#). If you do not specify the resource group, you can find all resources that the account has access to.
- You should have a FortiGate-VM deployed in Azure
- An IPv4 outbound policy from the FortiGate-VM on port2 (internal) to port1 (external)
- A VM instance of a resource in the Azure environment

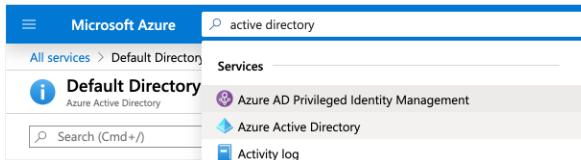
This section describes configuring an Azure SDN connector to connect the FortiGate to connect to the Azure backend. This allows easy reference of dynamic Azure objects when creating FortiOS firewall policies. If the FortiGate is a virtual device in one of those environments, it is likely to be the only connector configured.

## Azure SDN connector service principal configuration requirements

To configure an Azure SDN connector using service principal authentication, you must obtain the tenant and client IDs and client secret from the Azure portal.

### To obtain the tenant and client IDs and client secret:

1. Go to the Azure portal. You can find information required to configure the Azure SDN connector, such as the tenant and client IDs and client secret, in the Azure portal. Find the tenant and client IDs:
  - a. In the Azure portal, search for active directory. Click the *Azure Active Directory* service.



- b. Go to *App registration*.
- c. Click *New registration*.
- d. In the *Name* field, enter the desired name. In this example, the name is fgtsdn.

- e. Click *Register*.
- f. The overview of the newly created app registration shows the tenant and client ID that the Azure SDN connector requires.

The screenshot displays two windows side-by-side. The top window is the 'App registrations' page in the Azure portal, showing details for a registration named 'fgtsdn'. The bottom window is the 'Edit Fabric Connector' screen in the FortiGate VM64-AZUREONDEMAND interface, specifically for the 'Public SDN' connector.

**Azure Portal - App registrations:**

- Display name:** fgtsdn
- Application (client) ID:** 9d71fff0-afb4-421e-af7b-ecf21e11ea11
- Directory (tenant) ID:** 83a7137e-fed0-4aef-9c0b-1a0a8a0a0a0a
- Supported account types:** [dropdown]
- Redirect URLs:** [dropdown]
- Application ID URI:** [dropdown]

**FortiGate VM64-AZUREONDEMAND - VM-FGT - Edit Fabric Connector:**

- Connector Settings:**
  - Name: fgtsdn
  - Status: Enabled (selected)
  - Update Interval: Use Default
- Azure Connector:**
  - Server region: Global
  - Tenant ID: 83a7137e-fed0-4aef-9c0b-1a0a8a0a0a0a
  - Client ID: 9d71fff0-afb4-421e-af7b-ecf21e11ea11
  - Client secret: [redacted] (Note: This field is required.)
  - Resource path: [dropdown]

## 2. Assign a role to the fgtsdn application:

- a. In the Azure portal, search for subscriptions to assign the level of scope to assign this application to.
- b. Click *Pay-As-You-Go*.
- c. Go to *Access control (IAM)*.
- d. Click *Add role assignment*.
- e. From the *Role* dropdown list, select *Contributor*.
- f. In the *Select* field, enter the app name. In this example, it is fgtsdn.
- g. Click *Save*.

## 3. Generate the client secret value:

- a. Repeat steps 5a-b.
- b. Click the fgtsdn user.
- c. Go to *Certificates & secrets*.
- d. Click the *New client secret* button.
- e. In the *Description* field, enter the desired description.
- f. Under *Expires*, select the desired expiry period.
- g. Click *Add*.

- Copy the newly created client secret value in to the *Client secret* field in FortiOS.

#### Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret		Description	Expires	Value
fgtsdn			12/31/2299	yu0xg450-Gue...[REDACTED]

The screenshot shows the FortiGate VM64-AZUREONDEMAND interface. On the left, there's a navigation sidebar with various options like Dashboard, Security Fabric, Physical Topology, Logical Topology, Security Rating, Automation, Settings, and Fabric Connectors. Under Fabric Connectors, 'Public SDN' is selected. In the main pane, there's a section for 'Microsoft Azure'. It shows a Microsoft Azure logo with a checkmark. Below it, under 'Connector Settings', there's a form with fields: Name (fgtsdn), Status (Enabled, checked; Disabled), and Update Interval (Use Default). Under 'Azure Connector', there are dropdowns for Server region (Global) and Client secret, which contains the value 'yu0xg450-Gue...[REDACTED]'. There's also a Resource path field with a visibility toggle.

## Configuring an SDN connector using a managed identity

The Azure Active Directory managed identities for Azure resources feature solves the problem of storing service principal credentials in cloud applications like FortiGate NGFW VMs running in Azure.

Instead of authentication using service principal credentials, the SDN connector uses a service principal that the system assigns. The system creates the service principal when you enable managed identities on the VM. Afterward, Azure AD manages the service principal until you destroy the VM.

## Configuring a managed identity on Azure

You can enable managed identities on Azure during or after deployment:

- Enabling managed identities on Azure during deployment on page 113
- Enabling managed identities on Azure after deployment on page 114

After deployment, you must give the FortiGate-VM access to Azure resources. See [Azure portal on page 115](#).

## Enabling managed identities on Azure during deployment

On the Azure platform, you can enable managed identities from the Azure portal as well as ARM templates during deployment, Azure CLI, PowerShell, or Azure Cloud Shell.

To enable system-assigned managed identities, the Microsoft.Compute/virtualMachines resource for the FortiGate must have the "identity" property added at the same level as the "type": "Microsoft.Compute/virtualMachines" property.

```
"identity": {
    "type": "SystemAssigned"
},
```

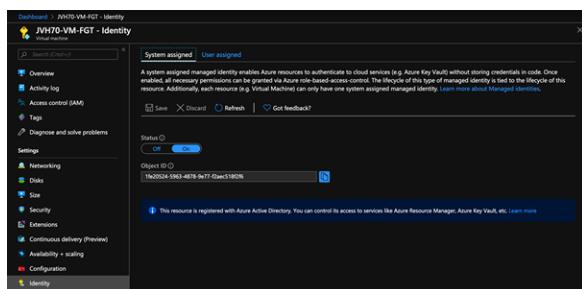
See [Configure managed identities for Azure resources on an Azure VM using a template](#).

## Enabling managed identities on Azure after deployment

On a FortiGate previously deployed on Azure, you can enable managed identities using different interaction methods, including the Azure portal, Azure CLI, PowerShell, or a REST API.

### Azure portal

The most common method is to use the Azure portal. In the FortiGate-VM resource in the Azure portal, go to *Identity*. On the *System assigned* tab, toggle the *Status* to *On*.



### Azure CLI

You can adapt the following command to reflect your VM and resource group names. You can use this command in the Azure CLI installed on Azure Cloud Shell or your local system:

```
az vm identity assign -g myResourceGroup -n myVm
```

See [Configure managed identities for Azure resources on an Azure VM using Azure CLI](#).

### Access control

After deployment, you must give the FortiGate-VM access to Azure resources. The SDN connector has two functions:

Function	Description
Dynamic address	The SDN connector can search for private and/or public IP addresses based on different properties, such as tag, VM name, network security group, resource group, and location in the current Azure subscription. You must assign the reader role to the resources that the SDN connector needs access to.
HA	One HA setup includes moving public IP addresses from the active to the passive FortiGate-VM. You must update the user-defined routes to point to the passive FortiGate-VM private IP address. These actions require elevated access to some resources.

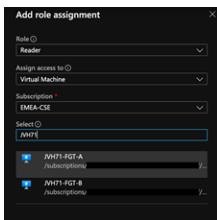
If you want to resolve dynamic addresses in multiple subscriptions in a Cloud Security Services HUB (VNet peering), you must assign the Reader role to each subscription.

### Dynamic address

You must assign the Reader role to the whole subscription, as the SDN connector needs access to all resources in the subscription.

#### To assign access control in the Azure portal:

1. In the Azure portal, go to *Access control (IAM)*.
2. Click *Add a role assignment*.
3. From the *Role* dropdown list, select *Reader*.
4. From the *Assign access to* dropdown list, select *Virtual Machine*.
5. From the *Select* dropdown list, select the desired FortiGate-VM.



#### To assign access control in the Azure CLI:

You must assign the role to both FortiGate-VMs in an active-active or active-passive setup. You must apply the Reader role since the VM principal ID must be retrieved. This action assigns required access rights for the service principal that Azure AD is managing specific for the FortiGate-VM to access Azure resources in the Azure subscription.

```
$ spID=$(az resource list -n {<FortiGate-VM name>} --query [*].identity.principalId --out tsv)
$ az role assignment create --assignee $spID --role 'Reader' --scope /subscriptions/{Azure subscription ID}
```

### HA

## Azure portal

In case of active-passive failover using the SDN connector, the FortiGate-VMs should have write access with the Network Contributor role to the following resources:

- FortiGate-VM network interfaces
- Routing tables that point to the FortiGate-VM internal interface
- Network security group attached to the FortiGate-VM network interface NIC1
- Public IP address attached to the FortiGate-VM network interface NIC1
- VNet or subnet that has the public IP address attached

The Network Contributor access rights are used to update the routing tables and public IP address in case of failover.

### To assign access control in the Azure CLI:

For HA, the SDN connector requires additional rights on different Azure resources. You can use the Network Contributor role or a more precise custom role.

You must assign the Fortinet FortiGate SDN Connector RW role to both FortiGate-VMs when in an active-active or active-passive setup. You must apply this role since the VM principal ID must be retrieved. This action assigns required access rights for the service principal that Azure AD is managing specific for the FortiGate-VM to access Azure resources in the Azure subscription.

Create a JSON file that contains the following:

```
{
  "Name": "Fortinet FortiGate SDN Fabric Connector RW",
  "IsCustom": true,
  "Description": "Role to update the public ip addres and user defined routes",
  "Actions": [
    "*/*",
    "Microsoft.Network/routeTables/write",
    "Microsoft.Network/routeTables/routes/write",
    "Microsoft.Network/routeTables/routes/delete",
    "Microsoft.Network/publicIPAddresses/write",
    "Microsoft.Network/publicIPAddresses/join/action",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/virtualNetworks/subnets/join/action"
  ],
  "DataActions": [],
  "NotActions": [],
  "NotDataActions": [],
  "AssignableScopes": [
    "/subscriptions/{<Azure subscription ID>}"
  ]
}
```

This action assigns required access rights for the service principal that Azure AD is managing specific for the FortiGate-VM to access Azure resources in the Azure subscription.

```
$ az role definition create --role-definition azure_SDN_iamrole_rw.json
$ spID=$(az resource list -n {<FortiGate-VM name>} --query [*].identity.principalId --out tsv)
$ az role assignment create --assignee $spID --role 'Reader' --scope /subscriptions/{Azure subscription ID}
```

### Configuring the managed identity on the FortiGate-VM

You must enable the SDN connector using the CLI. You do not need to add a tenant ID, client ID, or client key as the connector retrieves these automatically from the Azure instance metadata service.

```
config system sdn-connector
  edit AzureSDN
    set type azure
  end
end
```

## Configuring an Azure SDN connector for Azure resources

IP address resolving functionality is available for the following Azure resources:

- VM network interfaces (including VMSS)
- Internet-facing load balancers
- Internal load balancers
- Application gateways

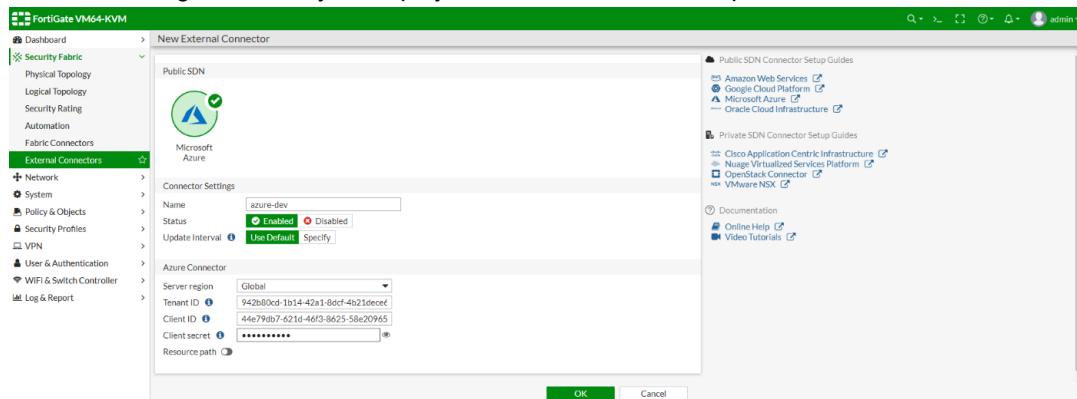


VPN gateways are currently not supported.

The following example demonstrates configuring an internet-facing load balancer.

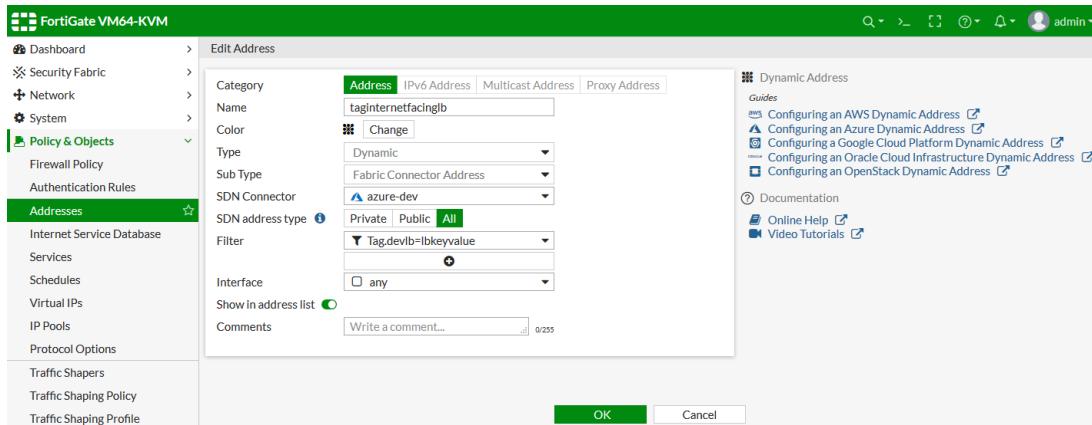
### To configure an internet-facing load balancer address in the GUI:

1. Configure the Azure SDN connector:
  - a. Go to *Security Fabric > External Connectors*.
  - b. Click *Create New*, and select *Microsoft Azure*.
  - c. Enter the settings based on your deployment, and click *OK*. The update interval is in seconds.



2. Create the dynamic firewall address:
  - a. Go to *Policy & Objects > Addresses*.
  - b. Click *Create New > Address* and enter a name.
  - c. Configure the following settings:
    - i. For *Type*, select *Dynamic*.
    - ii. For *Sub Type*, select *Fabric Connector Address*.
    - iii. For *SDN Connector*, select *azure-dev*.
    - iv. For *SDN address type*, select *All*.
    - v. For *Filter*, enter *Tag.devlb=lbkeyvalue*.

**d. Click OK.**



The corresponding IP addresses are dynamically updated and resolved after applying the tag filter.

**3. Ensure that the connector resolves the dynamic firewall IP address:**

**a. Go to *Policy & Objects* > *Addresses*.**

**b. In the address table, hover over the address created in step 2 to view what IP it resolves to:**

tagapplicationgate	tagInternetfacinglb resolves to:	Dynamic (AZURE)
taginternallb		• 52.230.230.83 Dynamic (AZURE)
taginternetfacinglb		Dynamic (AZURE)

**c. In Azure, verify to confirm the IP address matches:**

Resource group (change) : devtest	Backend pool : bepool (2 virtual machines)
Location : Central US	Health probe : tcpProbe (Tcp:80)
Subscription (change) : PAYG-DevOps	Load balancing rule : LBRule (Tcp:80)
Subscription ID : 4f24f274f24f-4343-aaaa-011010101011	NAT rules : 2 inbound
SKU : Standard	Public IP address : 52.230.230.83 (devlb)
Tags (change) : devlb : lbkeyvalue	

### To configure an internet-facing load balancer in the CLI:

**1. Configure the Azure SDN connector:**

```
config system sdn-connector
  edit "azure-dev"
    set status enable
    set type azure
    set azure-region global
    set tenant-id "942b80cd-1b14-42a1-8dcf-4b21dece61ba"
    set client-id "44e79db7-621d-46f3-8625-58e209654e58"
    set client-secret xxxxxxxxxxxx
    set update-interval 60
  next
end
```

**2. Create the dynamic firewall address:**

```
config firewall address
  edit "taginternetfacinglb"
    set type dynamic
    set sdn "azure-dev"
    set filter "Tag.devlb=lbkeyvalue"
    set sdn-addr-type all
  next
end
```

The corresponding IP addresses are dynamically updated and resolved after applying the tag filter.

**3. Confirm that the connector resolves the dynamic firewall IP address:**

```
config firewall address
    edit "taginternetfacinglb"
        show
            config firewall address
                edit "taginternetfacinglb"
                    set uid df391760-3bb6-51ea-f775-421df18f368d
                    set type dynamic
                    set sdn "azure-dev"
                    set filter "Tag.devlb=lbkeyvalue"
                    set sdn-addr-type all
                    config list
                        edit "52.230.230.83"
                        next
                    end
                next
            end
        next
    end
```

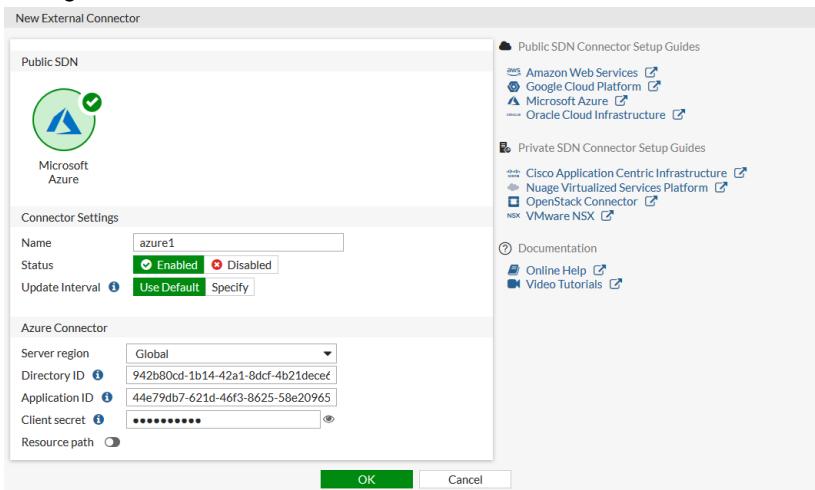
## Azure SDN connector using ServiceTag and Region filter keys

The *ServiceTag* and *Region* filter keys can be used in Azure SDN connectors to filter service tag IP ranges. These can be used in dynamic firewall addresses.

**To use the new filters keys in the GUI:**

**1. Create an Azure SDN connector:**

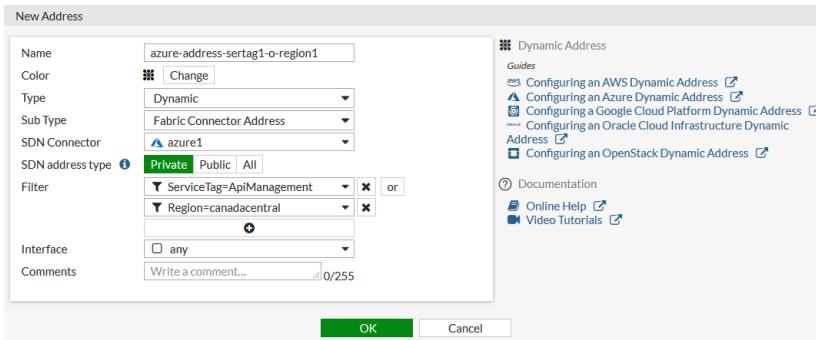
- a. Go to *Security Fabric > External Connectors* and click *Create New*.
- b. Select *Microsoft Azure*.
- c. Configure the connector:



- d. Click **OK**.

2. Create a dynamic firewall address for the Azure connector, filtering based on the servicetag and region:

- Go to *Policy & Objects > Addresses* and click *Create New > Address*.
- Configure the address, adding two filters: *ServiceTag=ApiManagement* and *Region=canadacentral*:



- Click **OK**.

- Hover over the cursor over the address name to see the dynamic IP addresses that are resolved by the connector:

### To use the new filters keys in the CLI:

- Create an Azure SDN connector:

```
config system sdn-connector
  edit "azure1"
    set type azure
    set tenant-id "942b80cd-1b14-42a1-8dcf-4b21dece61ba"
    set client-id "44e79db7-621d-46f3-8625-58e209654e58"
    set client-secret xxxxxxxx
  next
end
```

- Create a dynamic firewall address for the Azure connector, filtering based on the servicetag and region:

```
config firewall address
  edit "azure-address-sertag1-o-region1"
    set type dynamic
    set sdn "azure1"
    set color 2
    set filter "ServiceTag=ApiManagement | Region=canadacentral"
```

```
    next
end
```

### 3. View the dynamic IP addresses that are resolved by the connector:

```
# show firewall address azure-address-sertag1
config firewall address
    edit "azure-address-sertag1"
        set uuid 50a0afd4-b1bf-51ea-651b-f9ba7f6db455
        set type dynamic
        set sdn "azure1"
        set color 2
        set filter "ServiceTag=ApiManagement | Region=canadacentral"
        config list
            edit "102.133.0.79/32"
            next
            edit "102.133.130.197/32"
            next
            ...
            edit "13.78.108.176/28"
            next
            edit "13.86.102.66/32"
            next
            ...
        end
    next
end
```

## Troubleshooting Azure SDN connector



Output messages may differ depending on your setup.

You can use the `diagnose system sdn status` command to view the status of your SDN connectors.

You can check if API calls are made successfully by running the following commands in the CLI:

```
diagnose debug enable
diagnose debug application azd -1
```

```
jkatofgtha6p-A # diagnose debug enable
jkatofgtha6p-A # diagnose debug application azd -1
Debug messages will be on for 30 minutes.
```

Open the FortiGate GUI in your browser. Try to disable, then enable the SDN connector.

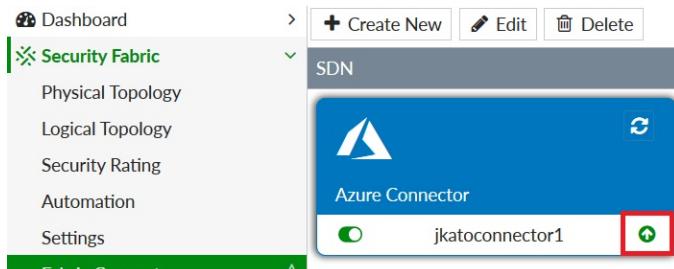
Wait a few minutes. If you did not configure the SDN connector correctly, the CLI displays the following error:

```
jkatofgtha6p-A #
jkatofgtha6p-A # azure sdn connector doing update
getting token
{"error":"invalid_client","error_description":"AADSTS70002: Error validating
get token failed
azd failed to get token
azd failed to get ip addr list
safeguard_fn() -1701
azure sdn connector doing update
getting token
{"error":"invalid_client","error_description":"AADSTS70002: Error validating
get token failed
azd failed to get token
azd failed to get ip addr list
safeguard_fn() -1701
```

Check the following and see if any required configuration is missing or incorrect:

- Did you enter all required fields such as tenant ID, client ID, client secret, subscription ID, and resource groups without error?
- Create a new client secret, then use the new secret for configuration.
- Does the registered app have access to the resource group?

Once you have successfully configured the SDN connector, the indicator turns green and the CLI output no longer shows an error when enabling and disabling the SDN connector.



```
azure sdn connector doing update
getting token
token size:1158
token expire on:1544973259
```

## SDN connector in Azure Kubernetes (AKS)

Azure SDN connectors support dynamic address groups based on Azure Kubernetes (AKS) filters. See the [FortiOS Administration Guide](#).

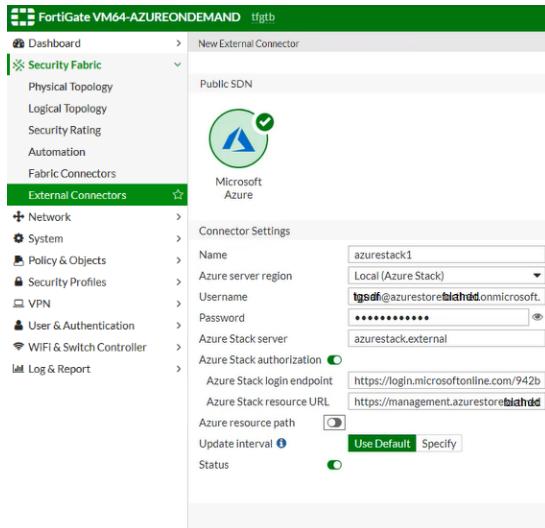
# SDN connector in Azure Stack

FortiOS automatically updates dynamic addresses for Azure Stack on-premise environments using an Azure Stack SDN connector, including mapping the following attributes from Azure Stack instances to dynamic address groups in FortiOS:

- vm
- tag
- size
- securitygroup
- vnet
- subnet
- resourcegroup
- vmss

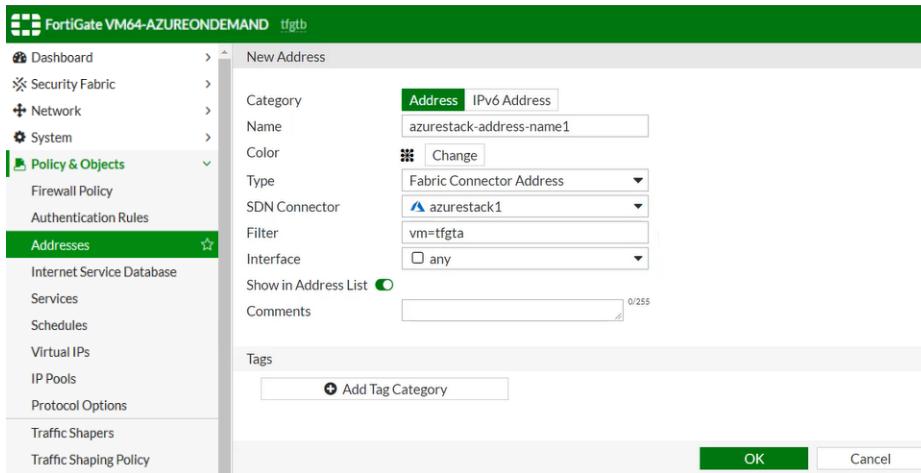
## To configure Azure Stack SDN connector using the GUI:

1. Configure the Azure Stack SDN connector:
  - a. Go to *Security Fabric > External Connectors*.
  - b. Click *Create New*, and select *Microsoft Azure*.
  - c. Configure as shown, substituting the Azure Stack settings for your deployment. The update interval is in seconds.

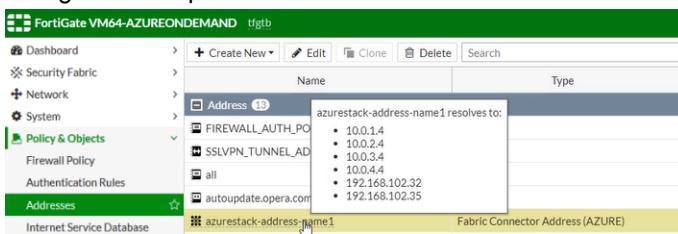


2. Create a dynamic firewall address for the configured Azure Stack SDN connector:
  - a. Go to *Policy & Objects > Addresses*.
  - b. Click *Create New*, then select *Address*.
  - c. Configure the address as shown, selecting the desired filter in the *Filter* dropdown list. In this example, the Azure Stack SDN connector will automatically populate and update IP addresses only for instances that are

named tfgtas:



3. Ensure that the Azure Stack SDN connector resolves dynamic firewall IP addresses:
  - a. Go to *Policy & Objects* > *Addresses*.
  - b. Hover over the address created in step 2 to see a list of IP addresses for instances that are named tfgtas as configured in step 2:



### To configure Azure Stack SDN connector using CLI commands:

1. Configure the Azure Stack SDN connector:

```
config system sdn-connector
  edit "azurestack1"
    set type azure
    set azure-region local
    set server "azurystack.external"
    set username "username@azurystoreexamplecompany.onmicrosoft.com"
    set password xxxxx
    set log-in endpoint "https://login.microsoftonline.com/942b80cd-1b14-42a1-8dcf-
        4b21dece61ba"
    set resource-url
      "https://management.azurestoreexamplecompany.onmicrosoft.com/12b6fedd-9364-
        4cf0-822b-080d70298323"
    set update-interval 30
  next
end
```

2. Create a dynamic firewall address for the configured Azure Stack SDN connector with the supported Azure Stack filter. In this example, the Azure Stack SDN Connector will automatically populate and update IP addresses only for instances that are named tfgtas:

```
config firewall address
  edit "azurystack-address-name1"
    set type dynamic
    set sdn "azurestack1"
```

```
        set filter "vm=tfqta"
    next
end
```

3. Confirm that the Azure Stack SDN connector resolves dynamic firewall IP addresses using the configured filter:

```
config firewall address
    edit "azurestack-address-name1"
        set type dynamic
        set sdn "azurestack1"
        set filter "vm=tfqta"
    config list
        edit "10.0.1.4"
        next
        edit "10.0.2.4"
        next
        edit "10.0.3.4"
        next
        edit "10.0.4.4"
        next
        edit "192.168.102.32"
        next
        edit "192.168.102.35"
        next
    end
next
end
```

# VPN for FortiGate-VM on Azure

## Connecting a local FortiGate to an Azure VNet VPN

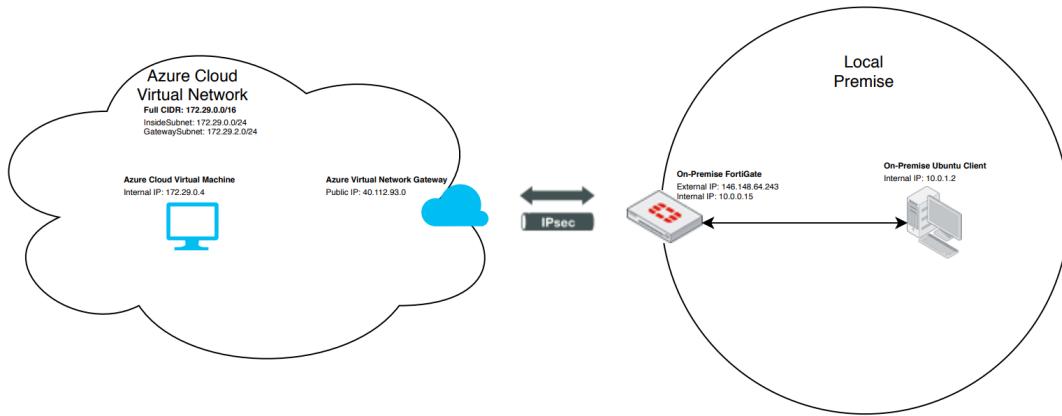
This recipe provides sample configuration of a site-to-site VPN connection from a local FortiGate to an Azure VNet VPN via IPsec VPN with static or border gateway protocol (BGP) routing.

Instances that you launch into an Azure VNet can communicate with your own remote network via site-to-site VPN between your on-premise FortiGate and Azure VNet VPN. You can enable access to your remote network from your VNet by configuring a virtual private gateway (VPG) and customer gateway to the VNet, then configuring the site-to-site VPC VPN.

The following prerequisites must be met for this configuration:

- Azure VNet with some configured subnets, routing tables, security group rules, and so on
- On-premise FortiGate with an external IP address

The following demonstrates the topology for this recipe:



This recipe consists of the following steps:

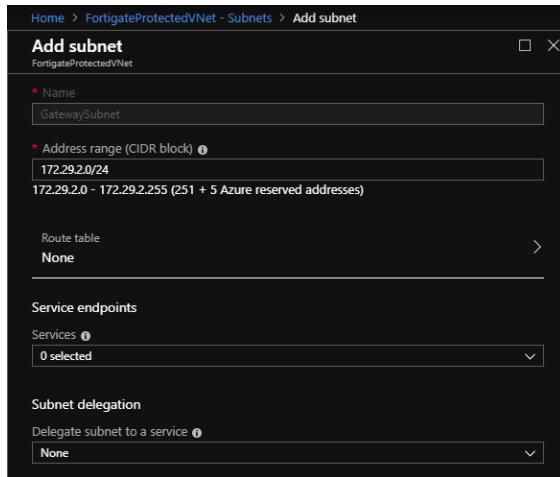
1. [Create a gateway subnet.](#)
2. [Create a VPN gateway.](#)
3. [Create a local network gateway.](#)
4. [Create a connection for the VNet gateway.](#)
5. [Configure the on-premise FortiGate.](#)
6. [Verify the connection.](#)
7. [Troubleshoot the connection.](#)

### To create a gateway subnet:

A gateway subnet is a subnet in your VNet that contains the IP addresses for the Azure VNet gateway resources and services. Azure requires a gateway subnet for VNet gateways to function.

1. In the Azure management console, go to your VNet, then *Subnets > + Gateway subnet*. You do not need to configure any fields on the *Add subnet* screen. You cannot change the name, as it must be *GatewaySubnet* for the

VNet gateway to function. Azure should automatically populate the *Address range (CIDR block)* field with a subnet within your VNet. In this example, the VNet is 172.29.0.0/16, while the subnet is 172.29.2.0/24. You do not need to configure a route table or security group unless your environment needs special handling.



### To create a VPN gateway:

You must create a VPN gateway to configure the Azure side of the VPN connection.

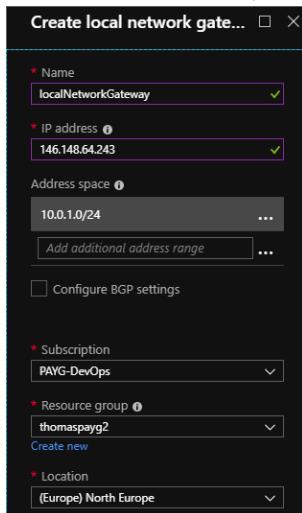
1. Go to *Create a resource*. Search for *Virtual network gateway*. Click *Create*.
2. On the *Create virtual network gateway* screen, configure the following:
  - a. From the *Subscription* dropdown list, select the correct subscription.
  - b. In the *Name* field, enter a name.
  - c. From the *Region* dropdown list, select the VNet gateway region. You should select the same region as the VNet.
  - d. For *Gateway type*, select *VPN*.
  - e. For *VPN type*, select *Policy-based*.
  - f. For *SKU*, at the time of publishing this guide, you can only select *Basic* for policy-based VPN.
  - g. From the *Virtual network* dropdown list, select the desired VNet to connect to. Azure should automatically detect the gateway subnet created earlier.
  - h. Under *PUBLIC IP ADDRESS*, create a new public IP address or select an existing public IP address for the VPN gateway.
  - i. If desired, configure BGP. The BGP peer IP address is based on the VNet gateway's gateway subnet.

Azure may take up to 45 minutes to create the VPN gateway.

### To create a local network gateway:

The local gateway refers to your local side of the VPN settings. You can configure a local network gateway to let Azure know your on-premise-side settings.

1. Go to *Create a resource*. Search for *Local network gateway*. Click *Create*.
2. On the *Create local network gateway* screen, configure the following:
  - a. In the *Name* field, enter a name.
  - b. In the *IP address* field, enter the on-premise FortiGate's external IP address.
  - c. In the *Address space* field, enter the CIDR of the network behind the on-premise FortiGate that will access the Azure VNet.
  - d. If desired, enable *Configure BGP settings*. You define the BGP peer IP address for the local network gateway, but there are restrictions. See [About BGP with Azure VPN Gateway](#).
  - e. From the *Subscription* dropdown list, select the correct subscription.
  - f. From the *Resource group* dropdown list, select the resource group. This example uses the resource group that the other resources belong to.
  - g. From the *Location* dropdown list, select the location. This example uses the location that the VNet resides in, but this is not a requirement.



### To create a connection for the VNet gateway:

A VNet gateway can have multiple connections to multiple VPN endpoints. These connections share the resource of the VNet gateway. To connect to an on-premise FortiGate, you must configure a connection.

1. Go to the *VNet gateway page* > *Connections* > *Add*.
2. On the *Add connection* screen, configure the following:
  - a. In the *Name* field, enter a name.
  - b. From the *Connection type* dropdown list, select *Site-to-site (IPsec)*.
  - c. Azure should automatically populate and lock the *Virtual network gateway* field.
  - d. For *Local network gateway*, select the local network gateway created earlier.
  - e. In the *Shared key (PSK)* field, enter the key. You must configure this on the on-premise FortiGate as well.
  - f. Azure should automatically populate and lock the *Resource group* field.

### To configure the on-premise FortiGate:

On the on-premise FortiGate, you must configure the phase-1 and phase-2 interfaces, firewall policy, and routing to complete the VPN connection. For Azure requirements for various VPN parameters, see [Configure your VPN device](#).

#### 1. Configure the phase-1 interface as follows in the FortiOS CLI:

- Set the interface to the external-facing interface.
- If your FortiGate is behind NAT, enter the interface's local private IP address for `local-gw`. Otherwise, this step is unnecessary.
- For `proposal` and Diffie-Hellman groups, use the ones that Azure supports as described in [IPsec/IKE parameters](#).
- For the remote gateway, use the VNet gateway's public IP address.
- For the PSK secret, use the one configured when creating a connection for the VNet gateway in Azure.
- If desired, configure dead peer detection. This is not necessary.

```
config vpn ipsec phasel-interface
  edit "azurephase1"
    set interface "port1"
    set local-gw 10.0.0.15
    set keylife 28800
    set peertype any
    set proposal aes256-sha256 3des-sha1 aes128-sha1 aes256-sha1
    set dhgrp 2
    set remote-gw 40.112.93.0
    set psksecret ENC
      VI0OQ084K91BwEqYp7kzBnMpEfNM1Gg5Mn1cTSfxwn4kR5Lsc7QHo0bDAUtqDQMpSrL3bbDBesSxp
      gezyTr1EbzikP5wZHU66uzrG90RARM+f2yZ1kEM1jw/X3QWl75SAIA4/eSEib3h6M2PqEYvKZf190
      /tiBihSlilBM81Rb1YFI212tNLoSatODgRGv8nXkvKVA==
    set dpd-retryinterval 10
  next
end
```

If configuring BGP routing, also run the following commands. Here, 10.1.254.1 255.255.255.255 is the local network gateway BGP peer IP address. 172.0.0.254 255.255.255.255 is the VNet gateway BGP peer IP address:

```
config vpn ipsec phasel-interface
  edit "azurephase1"
    set vdom "root"
    set ip 10.1.254.1 255.255.255.255
    set tcp-mss 1350
    set remote-ip 172.0.0.254 255.255.255.255
  next
end
```

#### 2. Configure the phase-2 interface as follows:

- For `phase1name`, enter the phase-1 interface name as configured in step 1.
- For `proposal`, use the ones that Azure supports as described in [IPsec/IKE parameters](#).
- Disable PFS. Azure does not support it on policy-based mode connections.
- You can enable auto-negotiation.
- Set the key life to 3600 seconds.
- Configure the source subnet to the one behind the on-premise FortiGate.
- Configure the destination subnet to the Azure VNet's CIDR.

```
config vpn ipsec phase2-interface
  edit "azurephase2"
    set phase1name "azurephase1"
    set proposal aes256-sha1 3des-sha1 aes256-sha256 aes128-sha1
    set pfs disable
```

```

    set auto-negotiate enable
    set keylifesecounds 3600
    set src-subnet 10.0.1.0 255.255.255.0
    set dst-subnet 172.29.0.0 255.255.0.0
next
end

```

**3. Configure ingress and egress firewall policy to the VPN interface:**

```

config firewall policy
edit 1
    set uuid cd18116c-9215-51e9-8398-3398085fff69
    set srcintf "azurephase1"
    set dstintf "port2"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
next
edit 2
    set uuid dadd6cd4-9215-51e9-288b-73a4336e9600
    set srcintf "port2"
    set dstintf "azurephase1"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
next
end

```

**4. Configure the route for traffic to enter the VPN tunnel:**

**a. Configure a static route for traffic to enter the VPN tunnel:**

```

config router static
edit 1
    set dst 172.29.0.0 255.255.0.0
    set device "azurephase1"
next
end

```

**b. Configure BGP. The example uses the following values:**

Value	Description
64521	Local network gateway BGP ASN
172.0.0.254	VNet gateway BGP peer IP address
64520	VNet gateway BGP ASN

```

config router bgp
    set as 64521
    config neighbor
        edit "172.0.0.254"
            set soft-reconfiguration enable
            set remote-as 64520
            set update-source "azurephase1"
next
end
end

```

### To verify the connection:

1. In FortiOS, go to *Monitor > IPsec Monitor* to see if the tunnel is up. If it is not up, manually bring up the tunnel.

The screenshot shows the FortiGate VM64-GCP interface with the 'IPsec Monitor' tab selected. Under the 'IPsec Monitor' section, there is a table with one row for 'azurephase1'. The columns in the table are: Name, Type, Remote Gateway, Peer ID, Incoming Data, and Outgoing Data. The 'Name' column shows 'azurephase1', 'Type' shows 'Custom', 'Remote Gateway' shows '40.112.93.0', 'Peer ID' is empty, 'Incoming Data' shows '409.96 kB' with a blue progress bar, and 'Outgoing Data' shows '206.89 kB' with a blue progress bar. At the top of the page, there is a navigation bar with 'HA: Master', a search bar, and a user dropdown for 'admin'.

2. On the Ubuntu client, conduct a ping test to a resource in the Azure VNet:

```
root@ubuntu-internal:~# ping 172.29.0.4
PING 172.29.0.4 (172.29.0.4) 56(84) bytes of data.
64 bytes from 172.29.0.4: icmp_seq=1 ttl=253 time=101 ms
64 bytes from 172.29.0.4: icmp_seq=2 ttl=253 time=101 ms
64 bytes from 172.29.0.4: icmp_seq=3 ttl=253 time=101 ms
```

3. Verify that the on-premise FortiGate forwards ICMP traffic through the Azure VPN tunnel:

```
EXAMPLE-FGT # diagnose sniffer packet any 'icmp' 4
interfaces=[any]
filters=[icmp]
9.537389 port2 in 10.0.1.2 -> 172.29.0.4: icmp: echo request
9.537453 azurephase1 out 10.0.1.2 -> 172.29.0.4: icmp: echo request
9.638766 azurephase1 in 172.29.0.4 -> 10.0.1.2: icmp: echo reply
9.638800 port2 out 172.29.0.4 -> 10.0.1.2: icmp: echo reply
```

4. If you configured BGP routing, verify the BGP connection between the peers:

```
diagnose sniffer packet azurephase1
interfaces=[azurephase1]
filters=[none]
2.608265 10.1.254.1.3965 -> 172.0.0.254.179: syn 3528484722
2.610865 172.0.0.254.179 -> 10.1.254.1.3965: syn 330055282 ack 3528484723
2.610889 10.1.254.1.3965 -> 172.0.0.254.179: ack 330055283
2.610910 10.1.254.1.3965 -> 172.0.0.254.179: psh 3528484723 ack 330055283
2.616039 172.0.0.254.179 -> 10.1.254.1.3965: psh 330055283 ack 3528484784
2.616051 10.1.254.1.3965 -> 172.0.0.254.179: ack 330055346
2.616061 172.0.0.254.179 -> 10.1.254.1.3965: psh 330055346 ack 3528484784
2.616064 10.1.254.1.3965 -> 172.0.0.254.179: ack 330055365
```

```
get router info bgp summary
BGP router identifier 10.1.1.37, local AS number 64521
BGP table version is 2
2 BGP AS-PATH entries
0 BGP community entries
Neighbor          V        AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
172.0.0.254      4       64520    1586     1596         1      0     0 00:01:08      1
Total number of neighbors 1
get router info routing-table bgp
Routing table for VRF=0
B      172.0.0.0/16 [20/0] via 172.0.0.254, azurephase1, 00:01:38
```

### To troubleshoot the connection:

If any aspects of the VPN are incorrectly configured, you must troubleshoot the Azure and on-premise FortiGate sides.

For Azure-side help, see the [Azure documentation](#).

For the on-premise FortiGate, use debugging to see possible problems:

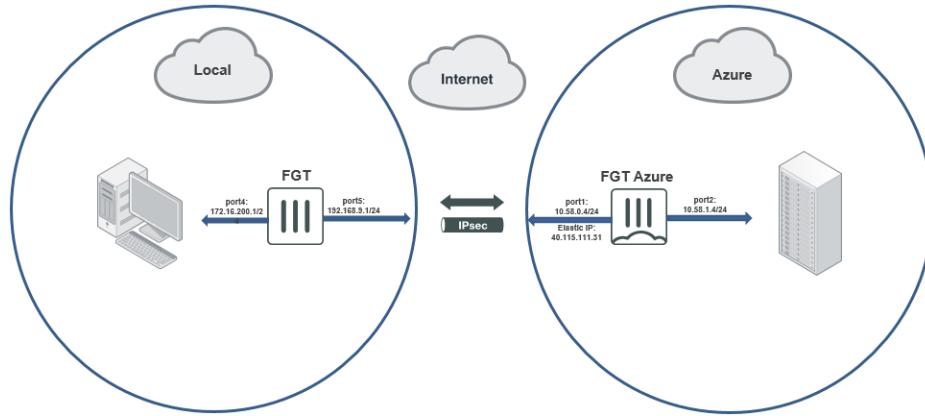
```
EXAMPLE-FGT # diagnose debug enable
EXAMPLE-FGT # diagnose debug application ike -1
Debug messages will be on for 30 minutes.
EXAMPLE-FGT # ike 0: cache rebuild start
ike 0:azurephase1: cached as static-ddns
ike 0: cache rebuild done
ike shrank heap by 106496 bytes
ike 0:azurephase1: NAT keep-alive 3 10.0.0.15->94.245.93.197:4500.
ike 0:azurephase1:125: out FF
ike 0:azurephase1:125: sent IKE msg (keepalive): 10.0.0.15:4500->94.245.93.197:4500, len=1,
id=ff00000000000000/0000000000000000
ike 0:azurephase1:azurephase2: IPsec SA connect 3 10.0.0.15->94.245.93.197:4500
ike 0:azurephase1:azurephase2: using existing connection
ike 0:azurephase1:azurephase2: config found
ike 0:azurephase1:azurephase2: IPsec SA connect 3 10.0.0.15->94.245.93.197:4500 negotiating
```

Common issues include misconfiguring the local gateway parameter, mismatching security proposals and protocols, and mismatching phase-2 source and destination subnets.

# Connecting a local FortiGate to an Azure FortiGate via site-to-site VPN

This guide provides a sample configuration of a site-to-site VPN connection from a local FortiGate to an Azure FortiGate via site-to-site IPsec VPN with static routing.

The following shows the topology for this sample configuration:



This topology consists of the following:

- A local FortiGate is located in a local environment. Determine if your FortiGate has a publicly accessible IP address or if it is behind NAT. In this sample configuration, the local FortiGate is behind NAT.
- A FortiGate located in Azure with port1 connected to WAN and port2 connected to local LAN.

This recipe consists of the following steps:

1. Configure the local FortiGate:
  - a. Configure the interfaces.
  - b. Configure a static route to connect to the Internet.
  - c. Configure IPsec VPN.
2. Configure the Azure FortiGate:
  - a. Configure the interface.
  - b. Configure IPsec VPN.
3. Bring up the VPN tunnel on the local FortiGate.
4. Verify the VPN tunnel on both the local FortiGate and the Azure FortiGate.
5. Run diagnose commands.

## Configuring the local FortiGate

### To configure the interfaces:

To configure the interfaces using the GUI, do the following:

1. In FortiOS on the local FortiGate, go to *Network > Interfaces*.
2. Edit *port5*. Set the role to *WAN* and set an *IP/Network Mask* of 192.168.5.1/255.255.255.0. This is for the interface connected to the Internet.
3. Edit *port4*. Set the role to *LAN* and set an *IP/Network Mask* of 172.16.200.1/255.255.255.0. This is for the interface connected to the local subnet.

To configure the interfaces using the CLI, run the following commands:

```
FGTA-1 # show system interface port5
config system interface
    edit "port5"
        set vdom "root"
        set ip 192.168.9.1 255.255.255.0
        set allowaccess ping https ssh
        set type physical
        set lldp-reception enable
        set role wan
        set snmp-index 7
    next
end
FGTA-1 # show system interface port4
config system interface
    edit "port4"
        set vdom "root"
        set ip 172.16.200.1 255.255.255.0
        set allowaccess ping https ssh
        set type physical
        set device-identification enable
        set lldp-transmission enable
        set role lan
        set snmp-index 6
    next
end
```

#### To configure a static route to connect to the Internet:

To configure a static route using the GUI, do the following:

1. Go to *Network > Static Routes*.
2. Click *Create New*.
3. Set the *Destination* to 0.0.0.0/0.0.0.0.
4. For the *Interface*, select *port5*.
5. Set the *Gateway Address* to 192.168.9.254.

To configure a static route using the CLI, run the following commands:

```
FGTA-1 # show router static
config router static
    edit 1
        set gateway 192.168.9.254
        set device "port5"
    next
end
```

#### To configure IPsec VPN:

To configure IPsec VPN using the GUI, do the following:

1. Go to *VPN > IPsec Wizard*.
2. Configure *VPN Setup*:
  - a. Enter the desired VPN name. In the example, this is "to\_cloud".
  - b. For *Template Type*, select *Site to Site*.
  - c. For the *Remote Device Type*, select *FortiGate*.
  - d. For *NAT Configuration*, select *This site is behind NAT*. For non dial-up situations where your local FortiGate has a public external IP address, you must choose *No NAT between sites*.
  - e. Click *Next*.
3. Configure *Authentication*:
  - a. For *Remote Device*, select *IP Address*.
  - b. Enter an IP address of 40.115.111.31, which is the Azure FortiGate's port1 public IP address.
  - c. For *Outgoing Interface*, select *port5*.
  - d. Set the *Authentication Method* to *Pre-shared Key*.
  - e. Enter a pre-shared key of 123456.
  - f. Click *Next*.
4. Configure *Policy & Routing*:
  - a. For *Local Interface*, select *port4*.
  - b. FortiOS automatically populates *Local Subnets* with 172.16.200.0/24.
  - c. Set the *Remote Subnets* to 10.58.1.0/24, which is the Azure FortiGate's port2 subnet.
  - d. For *Internet Access*, select *None*.
  - e. Click *Create*.

To configure IPsec VPN using the CLI, run the following commands:

```
FGTA-1 # show vpn ipsec phase1-interface to_cloud
config vpn ipsec phase1-interface
    edit "to_cloud"
        set interface "port5"
        set peertype any
        set net-device enable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set comments "VPN: to_cloud (Created by VPN wizard)"
        set wizard-type static-fortigate
        set remote-gw 40.115.111.31
        set psksecret ENC xxxxxxxx
    next
end
FGTA-1 # show vpn ipsec phase2-interface to_cloud
config vpn ipsec phase2-interface
    edit "to_cloud"
        set phasename "to_cloud"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm
            chacha20poly1305
        set comments "VPN: to_cloud (Created by VPN wizard)"
        set src-addr-type name
        set dst-addr-type name
        set src-name "to_cloud_local"
        set dst-name "to_cloud_remote"
    next
end
FGTA-1 # show router static
config router static
    edit 2
```

```

        set device "to_cloud"
        set comment "VPN: to_cloud (Created by VPN wizard)"
        set dstaddr "to_cloud_remote"
    next
    edit 3
        set distance 254
        set comment "VPN: to_cloud (Created by VPN wizard)"
        set blackhole enable
        set dstaddr "to_cloud_remote"
    next
end
FGTA-1 # show firewall policy
config firewall policy
    edit 1
        set name "vpn_to_cloud_local"
        set uuid ef98b6d8-41d9-51e9-20c5-7a31a66dd557
        set srcintf "port4"
        set dstintf "to_cloud"
        set srcaddr "to_cloud_local"
        set dstaddr "to_cloud_remote"
        set action accept
        set schedule "always"
        set service "ALL"
        set comments "VPN: to_cloud (Created by VPN wizard)"
    next
    edit 2
        set name "vpn_to_cloud_remote"
        set uuid ef9b260c-41d9-51e9-cf9c-0a082dc52660
        set srcintf "to_cloud"
        set dstintf "port4"
        set srcaddr "to_cloud_remote"
        set dstaddr "to_cloud_local"
        set action accept
        set schedule "always"
        set service "ALL"
        set comments "VPN: to_cloud (Created by VPN wizard)"
    next
end

```

## Configuring the Azure FortiGate

### To configure the interface:

To configure the interface using the GUI, do the following:

1. In FortiOS on the Azure FortiGate, go to *Network > Interfaces*.
2. Edit *port2*. Set the role to *LAN* and set an *IP/Network Mask* of *10.58.1.4/255.255.255.0*. This is for the interface connected to the Azure local subnet.

To configure the interfaces using the CLI, run the following commands:

```

FGT-Azure # show system interface port2
config system interface
    edit "port2"
        set vdom "root"
        set ip 10.58.1.4 255.255.255.0

```

---

```

set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response capwap
      ftm
set type physical
set snmp-index 2
next
end

```

### To configure IPsec VPN:

To configure IPsec VPN using the GUI, do the following:

1. Go to *VPN > IPsec Wizard*.
2. Configure *VPN Setup*:
  - a. Enter the desired VPN name. In the example, this is "to\_local".
  - b. For *Template Type*, select *Site to Site*.
  - c. For the *Remote Device Type*, select *FortiGate*.
  - d. For *NAT Configuration*, select *This site is behind NAT*. For non dial-up situations where your local FortiGate has a public external IP address, you must choose *No NAT between sites*.
  - e. Click *Next*.
3. Configure *Authentication*:
  - a. For *Incoming Interface*, select *port1*.
  - b. Set the *Authentication Method* to *Pre-shared Key*.
  - c. Enter a pre-shared key of 123456.
  - d. Click *Next*.
4. Configure *Policy & Routing*:
  - a. For *Local Interface*, select *port2*.
  - b. FortiOS automatically populates *Local Subnets* with 10.58.1.0/24.
  - c. Set the *Remote Subnets* to 172.16.200.0/24, which is the local FortiGate's port4 subnet.
  - d. For *Internet Access*, select *None*.
  - e. Click *Create*.

To configure IPsec VPN using the CLI, run the following commands:

```

FGT-Azure # show vpn ipsec phase1-interface
config vpn ipsec phase1-interface
    edit "to_local"
        set type dynamic
        set interface "port1"
        set peertype any
        set net-device enable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set dpd on-idle
        set comments "VPN: to_local (Created by VPN wizard)"
        set wizard-type dialup-fortigate
        set psksecret ENC xxxxxxxx
        set dpd-retryinterval 60
    next
end
FGT-Azure # show vpn ipsec phase2-interface
config vpn ipsec phase2-interface
    edit "to_local"
        set phasename "to_local"

```

```

set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm
    chacha20poly1305
set comments "VPN: to_local (Created by VPN wizard)"
set src-addr-type name
set dst-addr-type name
set src-name "to_local_local"
set dst-name "to_local_remote"
next
end
FGT-Azure # show firewall policy
config firewall policy
    edit 1
        set name "vpn_to_local_local"
        set uuid 032b6000-41f4-51e9-acb8-b7e32128bb70
        set srcintf "port2"
        set dstintf "to_local"
        set srcaddr "to_local_local"
        set dstaddr "to_local_remote"
        set action accept
        set schedule "always"
        set service "ALL"
        set comments "VPN: to_local (Created by VPN wizard)"
    next
    edit 2
        set name "vpn_to_local_remote"
        set uuid 0343ee4a-41f4-51e9-a06a-d4a15d35a0a2
        set srcintf "to_local"
        set dstintf "port2"
        set srcaddr "to_local_remote"
        set dstaddr "to_local_local"
        set action accept
        set schedule "always"
        set service "ALL"
        set comments "VPN: to_local (Created by VPN wizard)"
    next
end

```

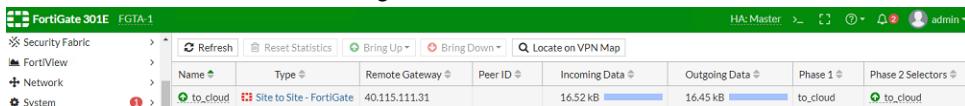
### To bring up the VPN tunnel on the local FortiGate:

The tunnel is down until you initiate connection from the local FortiGate.

1. In FortiOS on the local FortiGate, go to *Monitor > IPsec Monitor*.
2. Click the to\_cloud tunnel.
3. Click *Bring Up* to bring up the VPN tunnel.

### To verify the VPN tunnel on both the local FortiGate and the Azure FortiGate:

1. In FortiOS on the local FortiGate, go to *Monitor > IPsec Monitor*. It should look like the following:



2. In FortiOS on the Azure FortiGate, go to *Monitor > IPsec Monitor*. It should look like the following:

The screenshot shows the FortiGate VM64-Azure IPsec Monitor interface. The table displays one row for a tunnel named 'to\_local\_0'. The columns include Name, Type, Remote Gateway, Peer ID, Incoming Data, Outgoing Data, Phase 1, and Phase 2 Selectors. The 'Incoming Data' and 'Outgoing Data' columns show 53.44 kB and 28.06 kB respectively, both labeled 'to\_local'. The 'Phase 1' and 'Phase 2 Selectors' columns also show 'to\_local'.

### To run diagnose commands:

1. To show the local FortiGate's VPN status, run the following commands:

```
FGTA-1 # diagnose vpn ike gateway list
vd: root/0
name: to_cloud
version: 1
interface: port5 13
addr: 192.168.9.1:4500 -> 40.115.111.31:4500
created: 1042s ago
nat: me peer
IKE SA: created 1/1 established 1/1 time 400/400/400 ms
IPsec SA: created 1/1 established 1/1 time 130/130/130 ms
    id/spi: 365 cc00c782040e9ec9/e07668adc21bd6a7
    direction: initiator
    status: established 1042-1041s ago = 400ms
    proposal: aes128-sha256
    key: 2793ba055ddab07a-83c804230bffd8de
    lifetime/rekey: 86400/85058
    DPD sent/recv: 00000000/0000000a
FGTA-1 # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
-----
name=to_cloud ver=1 serial=2 192.168.9.1:4500->40.115.111.31:4500 dst_mtu=1500
bound_if=13 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/536 options[0218]=npu
    create_dev frag-rfc accept_traffic=1
proxyid_num=1 child_num=0 refcnt=11 ilast=18 olast=58 ad=/0
stat: rpx=1 txp=2 rxb=16516 txb=16450
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=keepalive draft=32 interval=10 remote_port=4500
proxyid=to_cloud proto=0 sa=1 ref=2 serial=1
    src: 0:172.16.200.0/255.255.255.0:0
    dst: 0:10.58.1.0/255.255.255.0:0
    SA: ref=6 options=10226 type=0 soft=0 mtu=1422 expire=42217/0B replaywin=2048
        seqno=3 esn=0 replaywin_lastseq=00000002 itn=0 qat=0
        life: type=01 bytes=0/0 timeout=42903/43200
        dec: spi=394f6923 esp=aes key=16 4ac11dd0916496e2e1edd610d83c7017
            ah=sha1 key=20 8d0c08ab1ed0d96ae29d521ed954a6bcc270f863
            enc: spi=5dc261b2 esp=aes key=16 c1b49a1251aa9bdb8b0ea205a687c794
            ah=sha1 key=20 0693c8988ef609bc410d6024e72e576366b53fef
            dec:pkts/bytes=1/16440, enc:pkts/bytes=2/16602
            npu_flag=03 npu_rgwy=40.115.111.31 npu_lgwy=192.168.9.1 npu_selid=1 dec_npuid=1 enc_npuid=1
```

2. To show the Azure FortiGate's VPN status, run the following commands:

```
FGT-Azure # diagnose vpn ike gateway list

vd: root/0
name: to_local_0
version: 1
interface: port1 3
```

---

```

addr: 10.58.0.4:4500 -> 208.91.115.10:64916
created: 1085s ago
nat: me peer
IKE SA: created 1/1 established 1/1 time 270/270/270 ms
IPsec SA: created 1/1 established 1/1 time 140/140/140 ms

id/spi: 0 cc00c782040e9ec9/e07668adc21bd6a7
direction: responder
status: established 1085-1084s ago = 270ms
proposal: aes128-sha256
key: 2793ba055ddab07a-83c804230bffd8de
lifetime/rekey: 86400/85045
DPD sent/recv: 0000000b/00000000

FGT-Azure # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
-----
name=to_local ver=1 serial=1 10.58.0.4:0->0.0.0.0:0 dst_mtu=0
bound_if=3 lgwy=static/1 tun=intf/0 mode=dialup/2 encap=none/528 options[0210]=create_
    dev frag-rfc accept_traffic=1

proxyid_num=0 child_num=1 refcnt=11 ilast=1096 olast=1096 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=0 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
-----
name=to_local_0 ver=1 serial=2 10.58.0.4:4500->208.91.115.10:64916 dst_mtu=1500
bound_if=3 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/976 options
    [03d0]=create_dev no-sysctl rgwy-chg rport-chg frag-rfc accept_traffic=1

parent=to_local index=0
proxyid_num=1 child_num=0 refcnt=14 ilast=38 olast=38 ad=/0
stat: rxp=334 txp=334 rxb=53440 txb=28056
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=11
natt: mode=keepalive draft=32 interval=10 remote_port=64916
proxyid=to_local proto=0 sa=1 ref=2 serial=1 add-route
src: 0:10.58.1.0/255.255.255.0:0
dst: 0:172.16.200.0/255.255.255.0:0
SA: ref=3 options=282 type=00 soft=0 mtu=1422 expire=42460/0B replaywin=2048
seqno=14f esn=0 replaywin_lastseq=0000014f itn=0 qat=0
life: type=01 bytes=0/0 timeout=43187/43200
dec: spi=5dc261b2 esp=aes key=16 c1b49a1251aa9bdb8b0ea205a687c794
ah=sha1 key=20 0693c8988ef609bc410d6024e72e576366b53fef
enc: spi=394f6923 esp=aes key=16 4ac11dd0916496e2e1edd610d83c7017
ah=sha1 key=20 8d0c08ab1ed0d96ae29d521ed954a6bcc270f863
dec:pkts/bytes=334/28056, enc:pkts/bytes=334/53440

```

## vWAN

Azure virtual WAN (vWAN) is an Azure-managed service that provides automated branch connectivity to and through Azure. You can leverage the Azure backbone to connect branches and enjoy branch-to-virtual network connectivity. Azure regions serve as hubs that you can use to connect your branches to.

This guide explains how to configure FortiOS to connect to Azure vWAN. It also explains how to access virtual networks in Azure and employ branch-to-branch connectivity.

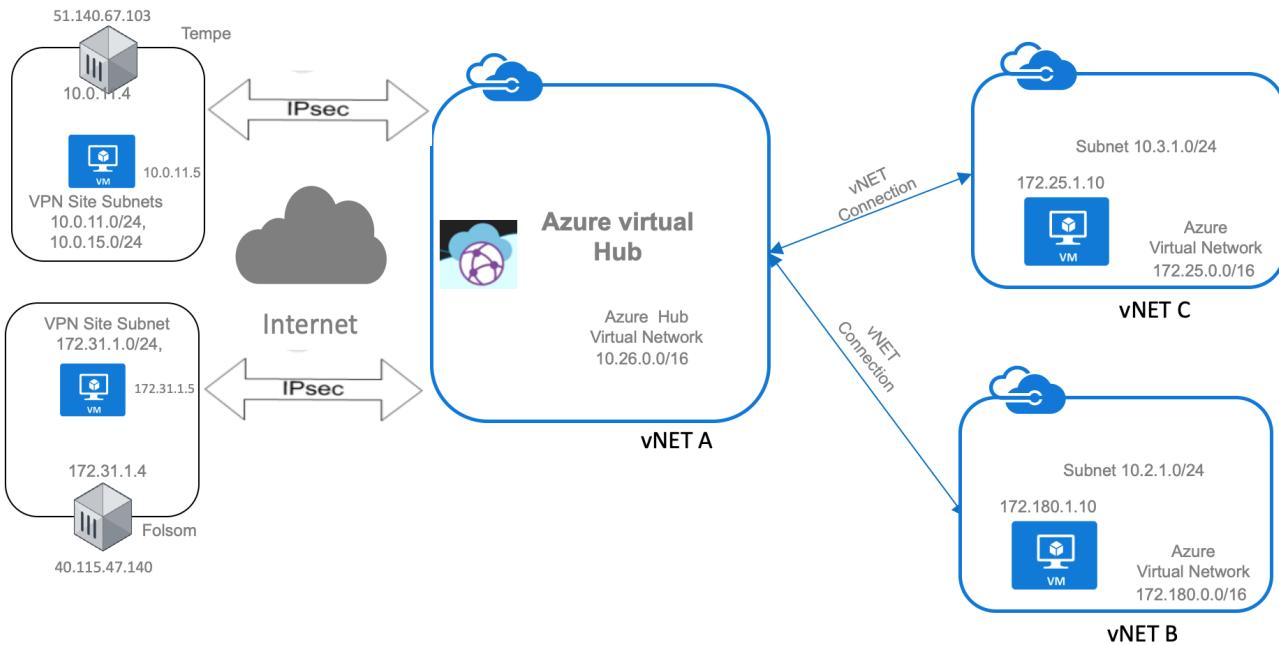
## vWAN architecture diagram

The Azure vWAN architecture consists of the following important resources:

Resource	Description
vWAN	Virtual overlay of the Azure network. It contains resources that include all links to the vWAN hub.
Virtual hub	Microsoft-managed virtual network. The hub contains various service endpoints to enable connectivity from your on-premise network (vpnsite). An Azure region can only have one hub. Creating a vWAN hub from the portal creates a virtual hub virtual network (VNet) and a virtual hub VPN gateway.  A hub gateway is not the same as a virtual network gateway that is used for ExpressRoute and VPN gateway. For example, when using vWAN, you do not create a site-to-site connection from the on-premise site directly to the virtual network. Instead, you create a site-to-site connection to the hub so that the traffic always passes through the hub gateway. Your VNets do not need their own virtual network gateway. With vWAN, your VNets can take advantage of scaling easily through the virtual hub and virtual hub gateway.
Hub VNet connection	Used to connect the hub seamlessly to the VNet. You can only connect virtual networks within the same hub region to the vWAN hub.
Site	Used only for site-to-site connection. The site resource is vpnsite. It represents your on-premise VPN device and its settings.

The following Azure vWAN architecture diagram represents remote sites Tempe and Folsom, which connect to the vWAN hub. The hub network is connected to two VNets: B and C. Connecting to the vWAN hub enables the Tempe and Folsom sites to access both VNets in Azure and to connect with each other through the vWAN hub.

Redundant VPN tunnels from each branch to the vWAN hub enhance connectivity. Border Gateway Protocol (BGP) handles routing.



## Creating the vWAN

### To create the vWAN:

1. You must create the vWAN hub within your subscription via the Azure portal. Log in to the [Azure portal](#).
2. Click *Create a new resource > Virtual WAN*.
3. Complete the fields as desired. The *Name* and *Resource group* fields do not support special characters or upper case letters. Click *Create*.
4. To enable branches to communicate with each other through the vWAN hub, go to *Configuration* and click *Allow branch to branch traffic*.
5. Go to *Hubs*, then click *+New Hub*.
6. In this example architecture, branch offices connect to the vWAN hub through IPsec VPN using site-to-site connectivity. This requires creating a VPN gateway. On the *Site to Site* tab, create a VPN gateway. Site-to-site connectivity uses the following settings. You can choose the gateway scale units depending on traffic needs.

**Create virtual hub**

✓ Validation passed

Basics Site to site Point to site ExpressRoute Routing Tags Review + create

The hub will be created under the same subscription and resource group as the vWAN.

**Basics**

Region	West US
Name	HQ
Hub private address space	10.26.0.0/24

**Site to site**

Site to site (VPN gateway)	Enabled
AS Number	65515
Gateway scale units	1 scale unit - 500 Mbps x 2

**Point to site**

Point to site (VPN gateway)	Disabled
-----------------------------	----------

**ExpressRoute**

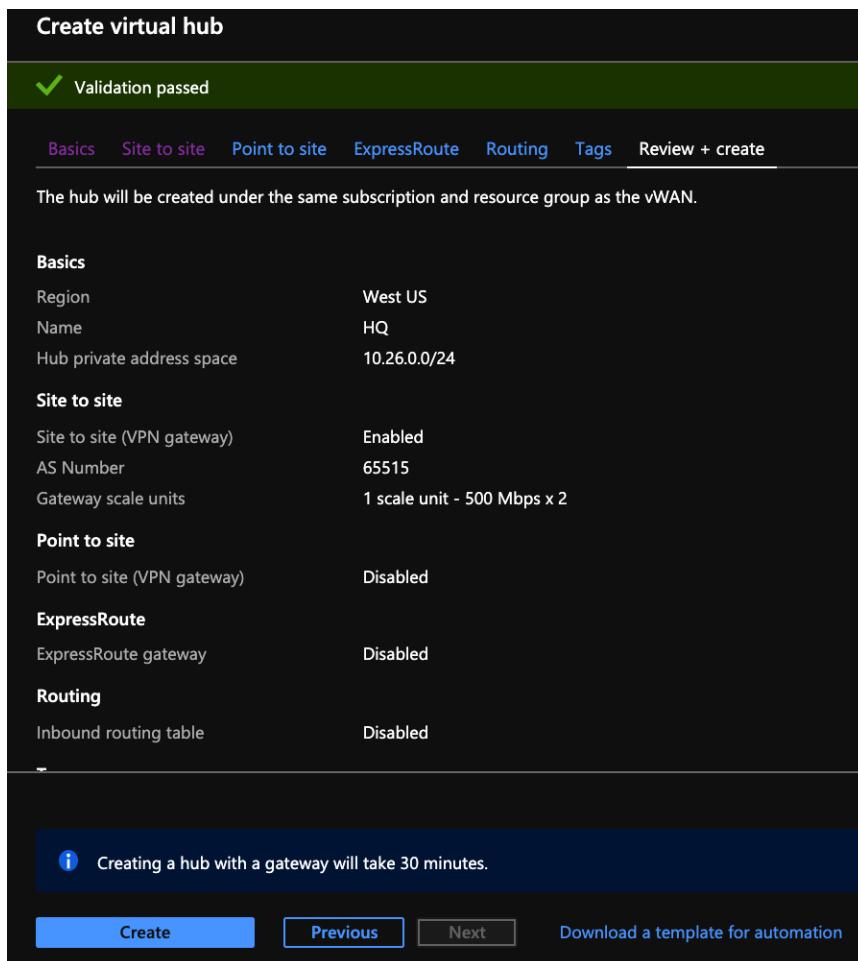
ExpressRoute gateway	Disabled
----------------------	----------

**Routing**

Inbound routing table	Disabled
-----------------------	----------

Creating a hub with a gateway will take 30 minutes.

Create Previous Next Download a template for automation



On the *Point to site* tab, you can configure settings to connect end user devices to the vWAN hub using OpenVPN and other VPN clients. On the *ExpressRoutes* tab, you can create an ExpressRoute gateway to connect ExpressRoutes to the vWAN hub. On the *Routing* tab, you can set up routing tables for advanced routing using the hub. Since the example architecture only pertains to site-to-site connection and does not use routing using the hub, point-to-site and ExpressRoute gateway creation and route tables will remain disabled.

7. Click *Create*. Creating a vWAN hub can take up to 30 minutes.

## Adding VNet connections to the vWAN hub

You must identify VNets that must connect to the vWAN hub to enable end-to-end connectivity.

### To add VNet connections to the vWAN hub:

1. On the vWAN page, go to *Virtual network connections*.
2. Click *Add connection*.
3. Select the VNets to connect to the vWAN hub. After the VNets connect to the vWAN hub, they appear as

connections.

Add connection					
HUB	HUB REGION	VIRTUAL NETWORK	VIRTUAL NETWORK CONNE...	VIRTUAL NETWORK CONNE...	...
HQ	West US	▼ Virtual networks (2)		Succeeded (2)	...
		applicationvnet	AppVnet	Succeeded	...
		security	Securityvnet	Succeeded	...

## Deploying the vWAN ARM template

You must complete the following to deploy the vWAN Azure Resource Manager template:

1. [Completing the prerequisites on page 144](#)
2. [Uploading Remote\\_sites.txt to a storage account on page 145](#)
3. [Deploying the ARM template on page 146](#)

## Completing the prerequisites

Before deploying the Azure Resource Manager (ARM) template, complete the following prerequisites:

### Creating a service principal

#### To create a service principal:

1. Log in to your Azure account.
2. Create a [service principal](#). Note the following items as you need them to deploy the Function App:

Item	Description	Relevant FortiOS parameter
Tenant ID	You can find this item in Azure Active Directory > Properties > Directory ID. A hybrid licensing deployment does not require this item.	Tenant ID
Application ID	You can find this item in Azure Active Directory > App registrations > (your app).	Service Principal ID
Application secret	Only appears once. You cannot retrieve the application secret.	Service Principal Secret

For details on the FortiOS parameters, see [Configurable variables on page 49](#).

## Obtaining vWAN details

Obtain the following details about the vWAN service:

- vWAN name
- Resource group name

## Creating the Remote\_sites.txt file

The Remote\_sites.txt file serves as the input for Azure functions. The file contains information about all sites that want to connect to vWAN. You will store the file in a storage blob. You must include the following information in the file:

- Site name (Azure uses this as an identifier)
- FortiGate public IP address
- Internal networks behind the FortiGate that need access to the vWAN
- BGP ASN and peering IP address to use
- VDOM
- Login credentials

The following is an example of the content of a Remote\_Sites.txt file:

```
1) Tempe 51.140.67.103 10.0.11.0/24,10.0.15.0/24 azureadmin Password!234 root 169.254.24.24  
    7224  
2) Folsom 40.115.47.140 172.31.1.0/24 azureadmin Password!234 root 169.254.24.25 7225
```

## Uploading Remote\_sites.txt to a storage account

### To upload Remote\_sites.txt to a storage account:

1. Create a storage account:
  - a. In the Azure portal, click *Create a resource*.
  - b. Search for "storage account" and select storage account resource creation. Click *Create*.
  - c. From the *Resource group* dropdown list, select the desired resource group, or create a new one. The storage account will reside in this location.
  - d. In the *Storage account name* field, enter a unique name. Each storage account requires a unique name as each storage account URL is unique.
  - e. (Optional) On the *Advanced Tab*, configure options to enforce access restrictions on the storage account. You can use any combination of the following options depending on the required security level or type:
    - i. (Optional) Deselect *Enable blob public access* to disable anonymous access to blobs in the storage account.
    - ii. (Optional) Select *Enable infrastructure encryption* to enable a second encryption layer when at rest. For details, see [Enable infrastructure encryption for double encryption of data](#).
    - iii. (Optional) Select *Default to Azure Active Directory authorization in the Azure portal*. When this property is enabled, the Azure portal authorizes requests to blobs, queues, and tables via RBAC. For details, see [Assign an Azure role for access to blob data](#). When this option is enabled, files may not be visible from the Azure portal GUI. You may need to use [Azure Storage Explorer](#) instead.
  - f. (Optional) From the *Replication* dropdown list, select *Locally-redundant storage (LRS)*.
  - g. Leave all other fields unchanged. Click *Review + create*.
2. Once Azure completes configuring the storage account, go to the storage account *Blobs* section. Click *+ Container*. Create a container that allows read access to blobs.
3. Click the container name, then click *Upload*.
4. In the *Files* field, select the Remote\_sites.txt file. Click *Upload*.

5. Right-click the file and select *Blob properties*.
6. Copy the value in the URL field. This is one of the ARM template parameters.

## Deploying the ARM template

### To deploy the ARM template:

1. Download the [template](#).
2. Log in to the Azure portal.
3. Click *Create new resource*.
4. Search for "template deployment" and select *Template deployment (deploy using custom templates)*. Click *Create*.
5. Click *Build your own template in the editor*. In the editor, delete the default JSON content. Paste the deploy\_vwan\_automation.json file contents. Click *Save*. The template to deploy the vWAN solution appears and you can enter the parameters described in [To create a service principal: on page 144](#).
6. Click *Create*. Once Azure completes deployment, Azure displays a function app, its corresponding application lights, a storage account, and the service plan that Azure automatically generates for Linux function apps.

## Associating VPN sites with the vWAN hub

Azure creates the VPN sites from the Remote\_sites.txt file. You must associate the sites with the vWAN hub.

### To associate VPN sites with the vWAN hub:

1. On the vWAN page, go to the *VPN sites* tab.
2. Select the desired VPN sites, then click *New hub association*.
3. Select the desired vWAN hub and PSK. The default PSK chosen during vWAN creation is used.
4. Click *Confirm*. Once Azure completes creating the association, the VPN site status displays as shown.

SITE	PUBLIC IP ADDRESS	STATUS	HUB	RESOURCE GROUP LOCATION	SITE AS NUMBER	...
Folsom	40.115.47.140	▲ See hub association status	▼ 1 hubs	West US	7225	...
Tempe	51.140.67.103	▲ See hub association status	▼ 1 hubs	West US	7224	...

Azure functions configure the remote sites with the correct VPN, BGP, and firewall policies by logging in to a FortiGate. Azure checks for new remote sites and corresponding hub associations every 30 minutes. Azure functions configure new sites and connect them to the vWAN solution. Once configuration completes, VPN site statuses change to All connected.

## Verifying vWAN configuration

The following shows FortiOS screenshots from a VPN site configured with Azure vWAN automation. You can see that the redundant VPN tunnels, corresponding IPv4 policies, and BGP routing have been created.

The BGP routing table shows that this VPN site has access not only to the connected VNets on Azure, but also other remote sites.

Type	Network	Gateway IP	Interfaces	Distance
BGP	10.26.0.0/24	10.26.0.7	Tempe0	20
BGP	169.254.24.25/32	10.26.0.7	Tempe0	20
BGP	172.25.0.0/16	10.26.0.7	Tempe0	20
BGP	172.31.1.0/24	10.26.0.7	Tempe0	20
BGP	172.180.0.0/16	10.26.0.7	Tempe0	20

Pinging from one site to another succeeds, showing communication between the two branch offices.

```
Tempe #
Tempe # Tempe # execute ping-options source 10.0.11.4
Tempe # execute ping 172.31.1.5
PING 172.31.1.5 (172.31.1.5): 56 data bytes
64 bytes from 172.31.1.5: icmp_seq=0 ttl=63 time=282.7 ms
64 bytes from 172.31.1.5: icmp_seq=1 ttl=63 time=282.9 ms
64 bytes from 172.31.1.5: icmp_seq=2 ttl=63 time=282.9 ms
64 bytes from 172.31.1.5: icmp_seq=3 ttl=63 time=282.5 ms
64 bytes from 172.31.1.5: icmp_seq=4 ttl=63 time=283.0 ms
--- 172.31.1.5 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 282.5/282.8/283.0 ms
```

## Configuring integration with Azure AD domain services for VPN

Configuring an integration with Azure AD domain services consists of the following:

### To configure Azure AD domain services:

1. In the Azure management portal, create Azure AD domain services. You can deploy it to a new or existing resource group. For information about Azure AD domain services, see [Azure AD Domain Services documentation](#). It can take up to 60 minutes for Azure to create your AD domain.

2. Go to *Azure AD Domain Services > Synchronization*. Configure whether to synchronize all Azure AD users and groups or scoped groups and members.
3. Go to *Azure AD Domain Services > Properties*. You can find IP addresses on which Azure AD domain services are running. These IP addresses must be reachable for your FortiGate for the setup to work.

4. Verify your domain in *Azure Active Directory > Custom domain names* by adding a TXT or MX record to your DNS settings.

The screenshot shows the 'Custom domain names' section of the Azure Active Directory portal. On the left, there's a sidebar with various management options like Users, Groups, and App registrations. The 'Custom domain names' option is selected. The main area displays a table with columns for NAME, STATUS, FEDERATED, and PRIMARY. Two entries are present: 'nowotarskip.pl' with a green checkmark under STATUS and 'nowotarskiptrgmail.onmicrosoft.com' with a green checkmark under STATUS.

5. Create users in *Azure Active Directory > Users > New User*. Write down the user password as it is required to log in to <https://portal.office.com> and you must change the password after initial login.

This screenshot shows the 'User' creation form. The 'Name' field contains 'testuser'. The 'User name' field contains 'testuser@nowotarskip.pl'. Under 'Profile', it says 'Not configured'. Under 'Properties', it says 'Default'. Under 'Groups', it says '0 groups selected'. Under 'Directory role', it says 'User'. At the bottom, there's a 'Password' field with 'Vogu7936' entered, a 'Show Password' checkbox checked, and a 'Save' button.

6. In *Azure Active Directory > Groups*, create a new group and assign the user created in step 5 to this group.

This screenshot shows the 'New Group' creation form. The 'Group type' is 'Security', 'Group name' is 'vpn\_access', 'Group description' is 'SSL VPN and Client to Site VPN access group', and 'Membership type' is 'Assigned'. The 'Members' section shows '1 member selected'. To the right, a 'Add members' dialog is open, showing a list with 'testuser' selected.

## To configure the FortiGate-VM for integration with Azure AD domain services:

1. In FortiOS, go to *User & Device > LDAP Servers* and configure the LDAP server based on the Azure AD domain service IP address obtained in step 3 of [To configure Azure AD domain services: on page 147](#).

2. Go to *User & Device > User Groups* and configure the user group that you will be using for the SSL VPN portal or client-to-site VPN connection based on the group that you configured in Azure AD.

3. You can also define a user in *User & Device > User Definition* that corresponds to the user that you created in step 5 of [To configure Azure AD domain services: on page 147](#). You can use this user in firewall policies for SSL VPN or client-to-site VPN connections.
4. Go to *VPN > SSL-VPN Settings* and enable an SSL VPN portal on the WAN interface. See [SSL VPN web mode for remote user](#).

**⚠️** Self-signed certificates are provided by default to simplify initial installation and testing. Acquiring a signed certificate for your installation is **HIGHLY** recommended.

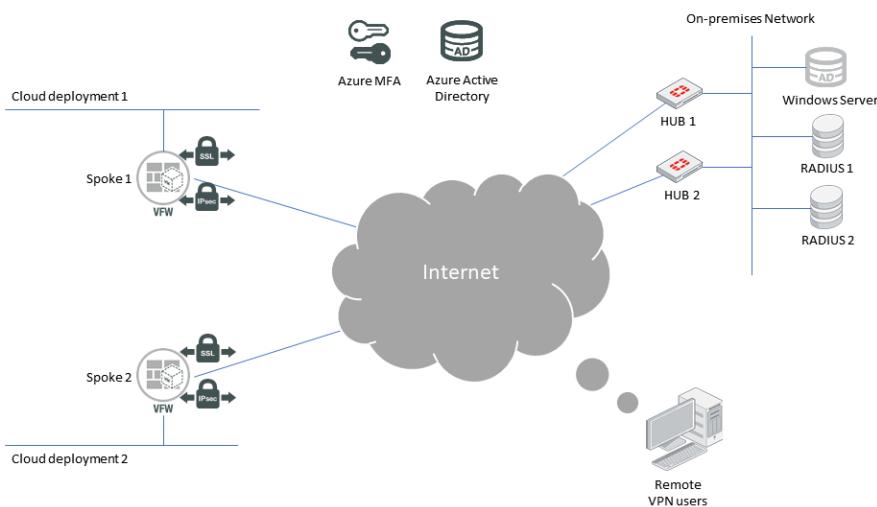
Continuing to use these certificates can result in your connection being compromised, allowing attackers to steal your information, such as credit card details.

For more information, review [Use a non-factory SSL certificate for the SSL VPN portal](#) and learn how to [Purchase and import a signed SSL certificate](#).

5. Go to *Policy & Objects* and edit the SSL VPN policy. For the source, select the user group and/or user that you configured in steps 2 and 3. Define what applications, protocols, and resources to allow for SSL VPN users.
6. Log in to the SSL VPN portal as the Azure AD user.
7. To configure client-to-site VPN access using FortiClient, go to *VPN > IPsec Wizard* and select the user group created in step 2. Azure AD creates and manages this group's members. See [FortiClient as dialup client](#) for details on configuring FortiClient.
8. You can use Azure AD users as administrator accounts to manage your FortiGate. Go to *System > Administrators* and configure a new administrator from a remote server that belongs to the remote user group on Azure AD that you configured in step 2.

## Configuring FortiClient VPN with multifactor authentication

This guide outlines how to integrate Azure multifactor authentication (MFA) to existing on-premise and cloud-based user authentication and VPN infrastructure.



This setup consists of the following components:

- On-premise Windows Servers acting as Active Directory (AD) domain controllers with domain name "qa-labs.ca" configured
- Two domain-joined network policy servers (NPS) for RADIUS service
- Cloud-deployed FortiGate-VM spoke nodes with AD VPN connection to the FortiGate-VM hub node for centralized network service accessibility

When a remote VPN user starts FortiClient for VPN connection to any spoke node, the on-premise RADIUS service verifies the user credentials. Integrating Azure MFA to the existing on-premise NPS adds the following [MFA methods](#) to the legacy username and password pairs for user authentication:

- Call to phone (wireless or landline phone numbers)
- Text message to phone
- Mobile app token
- Mobile app notification

When the on-premise AD is synced to the Azure AD and [NPS extension for Azure is integrated with the NPS](#), FortiClient VPN authentication flow results, as follows:

1. FortiClient initiates a VPN connection request to the FortiGate-VM with username and password pairs.
2. The FortiGate-VM sends a RADIUS access request message to NPS servers with several attribute value pairs (AVP) parameters, which includes username and encrypted password.
3. The NPS server connects to the local AD for primary authentication for the RADIUS request, if all NPS policies are met.
4. The local AD returns the authentication result to the NPS server. One of the following occurs:
  - a. If the credentials are incorrect, the NPS server sends a RADIUS access rejection message to the FortiGate-VM. See step 9.
  - b. If the credentials are correct, the NPS server forwards the request to the NPS extension.
5. The NPS extension triggers a request to Azure MFA for secondary authentication. Azure MFA checks if the user has MFA enabled. One of the following occurs:
  - a. If the user does not have MFA enabled, go to step 8.
  - b. If the user has MFA enabled, go to step 6.
6. Azure MFA retrieves the user details from Azure AD and performs the secondary authentication per the user's predefined methods, such as phone call, text message, mobile app notification, or mobile app one-time password. Azure MFA returns the challenge result to the NPS extension.
7. The NPS server that has the extension installed sends a RADIUS message to the FortiGate-VM. One of the following occurs:
  - a. If successful, a RADIUS access accept message is sent. Go to step 8.
  - b. If unsuccessful, a RADIUS access reject message is sent. Go to step 9.
8. The user access is granted and an encrypted VPN tunnel is established.
9. The VPN connection from FortiClient is disconnected.

This setup requires the following prerequisites:

- On-premise Windows domain controller and AD
- On-premise RADIUS service provided by NPS
- On-premise FortiGate at center, branch offices with Internet connections
- Azure subscription
- Azure MFA license
- FortiGate-VM on the cloud. Spoke 1 and Spoke 2 have VPN connections to Hub 1 and Hub 2
- Remote VPN users
- Smartphone with Microsoft Authenticator installed

The following example uses the following settings:

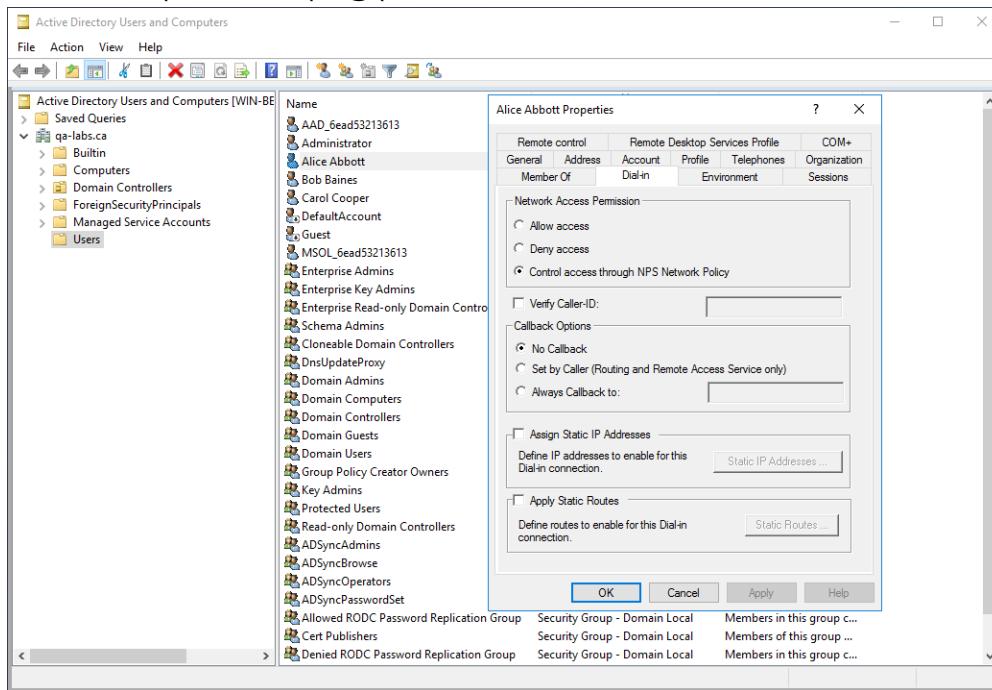
- FortiClient 6.0.9
- FortiGate-600D with FortiOS 6.2.2
- FortiGate-VM pay-as-you-go (PAYG) for Azure with FortiOS 6.2.2
- Windows Server 2016, domain controller, domain-joined NPS
- Azure PAYG-DevOps subscription

#### To configure FortiClient VPN with MFA:

1. Sign in to the Azure portal as a global administrator for the Azure AD. Add your domain name to the Azure AD as a custom domain name so that your users can keep their sign-in username unchanged.
2. Sign in to your on-premise domain controller as the domain administrator. Download and install the Azure AD connect tool to sync your domain users to Azure AD.
3. Download and install the NPS extension to your on-premise NPS server.

4. Add several usernames to your on-premise domain controller for testing purposes. All users should have dial-in control access through NPS network policy under *Network Access Permission*. This example adds the following users:

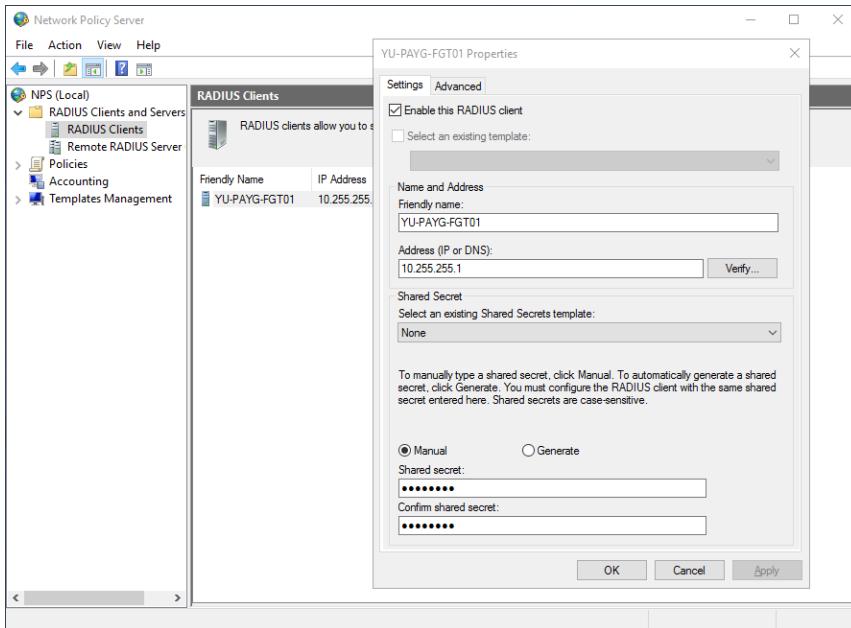
- Alice Abbott: aliceabbott@qa-labs.ca
- Bob Baines: bobbaines@qa-labs.ca
- Carol Cooper: carolcooper@qa-labs.ca



5. Go to the Azure portal. Click *Azure Active Directory > Users > Multi-Factor Authentication*. Search and enable MFA for the users you created in step 5.
6. Install Microsoft Authenticator on your smartphone.
7. Sign in to [aka.ms/MFASetup](https://aka.ms/MFASetup) as each account that you added in step 5. Enable a different MFA method for each user. This example configures the following:
- Sign in as Alice Abbott and enable text message.
  - Sign in as Bob Baines and enable mobile app token.
  - Sign in as Carol Cooper and enable mobile app notification.

## 8. Configure the on-premise NPS:

- Add the remote FortiGate-VM as a RADIUS client.



- Enable PAP as a RADIUS authentication method.

## 9. Configure dialup VPN and the SSL VPN portal on the spoke FortiGate-VM with user authenticated against on-premise RADIUS/NPS.

Azure MFA with the RADIUS NPS extension deployment supports the following password encryption algorithms used between the RADIUS client (VPN, NetScaler server, and so on) and the NPS server:

- PAP supports all Azure MFA authentication methods in the cloud: phone call, text, message, mobile app notification, and mobile app verification code.
- CHAPv2 supports phone call and mobile app notifications.
- This deployment does not support EAP.

When FortiOS authenticates a user against a remote RADIUS server, by default, it selects PAP for SSL VPN and MS-CHAPv2 for IPsec VPN. Users who have mobile app token configured as their MFA method may have trouble connecting to IPsec VPN because the mobile app notification or phone call verification may not reach them.

Select PAP for all RADIUS user authentication in your FortiGate-VM configuration:

- For IPsec VPN, run `set xauthtype pap` in your phase1-interface configuration:

```
config vpn ipsec phasel-interface
    edit "Dialup_RAS"
        set type dynamic
        set interface "port1"
        set mode aggressive
        set peertype any
        set net-device disable
        set mode-cfg enable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set dpd on-idle
        set comments "VPN: Dialup_RAS (Created by VPN wizard)"
        set wizard-type dialup-forticlient
        set xauthtype pap
        set authusgrp "Azure_MFA_Usergroup"
```

```

        set ipv4-start-ip 172.31.6.1
        set ipv4-end-ip 172.31.6.254
        set dns-mode auto
        set ipv4-split-include "Dialup_RAS_split"
        set save-password enable
        set client-auto-negotiate enable
        set client-keep-alive enable
        set psksecret Nobody_Knows
        set dpd-retryinterval 60
    next
end
• For RADIUS server settings, run set auth-type pap and set timeout 30:
config vpn ssl settings
    set servercert "qa-labs.ca"
    set idle-timeout 4800
    set tunnel-ip-pools "SSLVPN_Tunnel_172.31.7.0/24"
    set source-interface "port1"
    set source-address "all"
    set source-address6 "all"
    set default-portal "web-access"
config authentication-rule
    edit 1
        set groups "Azure_MFA_Usergroup"
        set portal "0595363 SSLVPN Portal"
    next
end
config user group
    edit "Azure_MFA_Usergroup"
        set member "on-premises_NPS"
    next
end
config user radius
    edit "on-premises_NPS"
        set server "172.31.248.16"
        set secret Nobody_Knows
        set timeout 30
        set nas-ip 10.255.255.1
        set auth-type pap
        set source-ip "10.255.255.1"
    next
end

```

### To verify that MFA is configured correctly:

```

diagnose test authserver radius on-premises_NPS pap aliceabbott@qa-labs.ca <password>
Enter Your Microsoft verification code*****
authenticate 'aliceabbott@qa-labs.ca' against 'pap' succeeded, server=primary assigned_rad_
session_id=1070819755 session_timeout=0 secs idle_timeout=0 secs!
diagnose test authserver radius on-premises_NPS pap bobbaines@qa-labs.ca <password>
authenticate 'bobbaines@qa-labs.ca' against 'pap' succeeded, server=primary assigned_rad_
session_id=1070819758 session_timeout=0 secs idle_timeout=0 secs!

```

## Azure AD acting as SAML IdP

Azure AD can act as a SAML identity provider (IdP) in the following configurations:

- [SAML SSO login for FortiOS administrators with Azure AD acting as SAML IdP on page 156](#)
- [Configuring SAML SSO login for SSL VPN web mode with Azure AD acting as SAML IdP on page 156](#)

### SAML SSO login for FortiOS administrators with Azure AD acting as SAML IdP

See [Configuring SAML SSO login for FortiGate administrators with Azure AD acting as SAML IdP](#).

### Configuring SAML SSO login for SSL VPN web mode with Azure AD acting as SAML IdP

This guide provides supplementary instructions on using SAML SSO to authenticate against Azure Active Directory (AD) with SSL VPN SAML user via web mode on top of initial configuration on Azure found in [Tutorial: Azure Active Directory single sign-on \(SSO\) integration with FortiGate SSL VPN](#).

#### To configure SAML SSO login for SSL VPN web mode with Azure AD acting as SAML IdP:

1. In FortiOS, upload the certificate as [Complete FortiGate command-line configuration describes](#).
2. In the FortiOS CLI, configure the SAML user. Ensure that identity provider (IdP)-related entries match the Azure-side configuration. The `idp-single-logout-url` value has a ? mark in the string. When entering the value in the CLI, ensure you press `Ctrl` and `V` before entering ?.

```
config user saml
  edit "ssl-azure-saml"
    set cert "Fortinet_Factory"
    set entity-id "https://<FortiGate IP address>:<Custom SSL VPN
      port>/remote/saml/metadata"
    set single-sign-on-url "https://<FortiGate IP address>:<Custom SSL VPN
      port>/remote/saml/login"
    set single-logout-url "https://<FortiGate IP address>:<Custom SSL VPN
      port>/remote/saml/logout"
    set idp-entity-id "<Azure AD identifier>"
    set idp-single-sign-on-url "<Login URL>"
    set idp-single-logout-url
      "https://login.microsoftonline.com/common/wsfederation?wa=wsignin1.0"
    set idp-cert "<Certificate imported earlier>"
    set user-name "<Azure username attribute>"

  next
end
```

In this example, assuming that the FortiGate IP address is 104.40.18.242, the commands are as follows:

```
config user saml
```

```

edit "ssl-azure-saml"
set cert "Fortinet_Factory"
set entity-id "https://104.40.18.242:10443/remote/saml/metadata"
set single-sign-on-url "https://104.40.18.242:10443/remote/saml/login"
set single-logout-url "https://104.40.18.242:10443/remote/saml/logout"
set idp-entity-id "https://sts.windows.net/04e..."
set idp-single-sign-on-url "https://login.microsoftonline.com/04e047fe-93e7-4...""
set idp-single-logout-url
    "https://login.microsoftonline.com/common/wsfederaion?wa=wsignout1.0"
set idp-cert "<Certificate imported earlier>"
set user-name "username"
next
end

```

The `user-name` attribute configured on the FortiGate entry should exactly match the `username` attribute returned by Azure AD. You can configure the list of SAML attributes returned by Azure AD under *Username Attributes & Claims* in the Azure portal.

SAML Attribute	Azure AD Property
givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
username	user.userprincipalname
Unique User Identifier	user.userprincipalname
Group	user.groups

FortiGate can map users to specific groups based on the returned SAML `user.groups` attribute. The example shows group matching based on Azure Active Directory Group ObjectId, using the `set group-name` command:

```

config user group
edit "saml-innovcenter"
set member "sslvpnazuread"
config match
edit 1
set server-name "sslvpnazuread"
set group-name "8fb8c5ee-b253-44cc-a88f-4bd62dfaf2d2"
next
end
next
end

```

You can find the full list of group claims in [Configure group claims for applications with Azure Active Directory](#).

Ensure that the configured group-name attribute on the FortiGate exactly matches the `user.groups` claim name in the Azure AD portal. See the `set group-name` command in the following:

```

config user saml
edit "sslvpnazuread"
set cert "fgt_az_saml"
set entity-id "https://vpnportal.az.ftntcloudpoc.net/remote/saml/metadata"
set single-sign-on-url "https://vpnportal.az.ftntcloudpoc.net/remote/saml/login"
set single-logout-url "https://vpnportal.az.ftntcloudpoc.net/remote/saml/logout"
set idp-entity-id "https://sts.windows.net/xxxxx-xxxxx-xxxxx-xxxxx-xxxxx/"
set idp-single-sign-on-url "https://login.microsoftonline.com/xxxxx-xxxxx-xxxxx-
xxxxx-xxxxx/saml2"
set idp-single-logout-url
    "https://login.microsoftonline.com/common/wsfederaion?wa=wsignout1.0"
set idp-cert "AzureAD_innovcenter"
set user-name "Username"
set group-name "UserGroup"

```

```
    next
end
Configure other settings:
config system global
    set remoteauthtimeout 60
end
```

**3.** Go to *VPN > SSL VPN Settings*. Configure as desired.

---



Self-signed certificates are provided by default to simplify initial installation and testing.  
Acquiring a signed certificate for your installation is **HIGHLY** recommended.

Continuing to use these certificates can result in your connection being compromised,  
allowing attackers to steal your information, such as credit card details.

For more information, review [Use a non-factory SSL certificate for the SSL VPN portal](#) and  
learn how to [Purchase and import a signed SSL certificate](#).

- 4.** Go to *Policy & Objects*. Create a new SSL VPN firewall policy or modify an existing one to apply to the group that contains the SAML user that you configured in step 2.
- 5.** Currently, a SAML user can only log in via the SSL VPN web UI portal. Log in to the portal:
  - a.** Go to <https://<FortiGate IP address>:10443> in a browser.
  - b.** Click *Single Sign-On*.
  - c.** Sign in with your Azure account and password. Once logged in, the browser redirects to the SSL VPN portal.

**To troubleshoot:**

```
diagnose debug application samld -1
diagnose debug application sslvpn -1
```

The output should resemble the following:

```
samld_send_common_reply [123]: Attr: 17, 27, magic=a8111ca2943ecd0c
samld_send_common_reply [120]: Attr: 10, 95,
    'http://schemas.microsoft.com/identity/claims/tenantid' 'xxxxxx-xxxxxx-xxxxxx-xxxxxx-
    xxxx'
samld_send_common_reply [120]: Attr: 10, 103,
    'http://schemas.microsoft.com/identity/claims/objectidentifier' 'xxxxxx-xxxxxx-xxxxxx-
    xxxx'
samld_send_common_reply [120]: Attr: 10, 128,
    'http://schemas.microsoft.com/identity/claims/identityprovider'
    'https://sts.windows.net/yyyyyy-yyyyyy-yyyyyy-yyyyyy/'
samld_send_common_reply [120]: Attr: 10, 142,
    'http://schemas.microsoft.com/claims/authnmethodsreferences'
    'http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password'
samld_send_common_reply [120]: Attr: 10, 49, 'Username'
    'mremini@innovcenter.onmicrosoft.com'
samld_send_common_reply [120]: Attr: 10, 51, 'UserGroup' '3a0e3f1c-93c6-4be6-bdbe-
    b5d28a20cf0'
samld_send_common_reply [120]: Attr: 10, 51, 'UserGroup' '8fb8c5ee-b253-44cc-a88f-
    4bd62dfaf2d2'
[924:root:5c]req: /remote/saml/start
[924:root:5c]rmt_web_auth_info_parser_common:470 no session id in auth info
[924:root:5c]rmt_web_get_access_cache:804 invalid cache, ret=4103
[924:root:5c]sslvpn_auth_check_usrgroup:2039 forming user/group list from policy.
[924:root:5c]sslvpn_auth_check_usrgroup:2145 got user (1) group (1:0).
[924:root:5c]sslvpn_validate_user_group_list:1642 validating with SSL VPN authentication
    rules (0), realm ((null)).
```

```
[924:root:5c]sslvpn_validate_user_group_list:1963 got user (1:0), group (1:0) peer group
(0).
[924:root:0]total sslvpn policy count: 1
[924:root:5c]req: /remote/saml/login
[924:root:5c]stmt: http://schemas.microsoft.com/identity/claims/tenantid
[924:root:5c]stmt: http://schemas.microsoft.com/identity/claims/objectidentifier
[924:root:5c]stmt: http://schemas.microsoft.com/identity/claims/displayname
[924:root:5c]stmt: http://schemas.microsoft.com/identity/claims/identityprovider
[924:root:5c]stmt: http://schemas.microsoft.com/claims/authnmethodsreferences
[924:root:5c]stmt: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
[924:root:5c]stmt: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
[924:root:5c]stmt: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
[924:root:5c]rmt_web_session_create:781 create web session, idx[0]
[924:root:5c]User Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:71.0) Gecko/20100101
  Firefox/71.0
[924:root:5c]deconstruct_session_id:426 decode session id ok, user=[ssl-azure-saml],group=
  [sslvpn],authserver=[],portal=[web-access],host=[208.91.115.10],realm=
  [],idx=0,auth=256,sid=1424c6b9,login=1576802935,access=1576802935,sa$1_logout_url=no
[924:root:5c]deconstruct_session_id:426 decode session id ok, user=[ssl-azure-saml],group=
  [sslvpn],authserver=[],portal=[web-access],host=[208.91.115.10],realm=
  [],idx=0,auth=256,sid=1424c6b9,login=1576802935,access=1576802935,sa$1_logout_url=no
[924:root:5c]deconstruct_session_id:426 decode session id ok, user=[ssl-azure-saml],group=
  [sslvpn],authserver=[],portal=[web-access],host=[208.91.115.10],realm=
  [],idx=0,auth=256,sid=1424c6b9,login=1576802935,access=1576802935,sa$1_logout_url=no
[924:root:5c]req: /sslvpn/portal.html
[924:root:5c]mza: 0x28587b0 /sslvpn/portal.html
[924:root:5c]deconstruct_session_id:426 decode session id ok, user=[ssl-azure-saml],group=
  [sslvpn],authserver=[],portal=[web-access],host=[208.91.115.10],realm=
  [],idx=0,auth=256,sid=1424c6b9,login=1576802935,access=1576802935,sam1_logout_url=yes
[924:root:5c]req: /dc7a2776ac5e60eb4eeda4c1de45b5cb/js/req
[924:root:5c]mza: 0x2858620 /dc7a2776ac5e60eb4eeda4c1de45b5cb/js/require_all.js
[924:root:5c]deconstruct_session_id:426 decode session id ok, user=[ssl-azure-saml],group=
  [sslvpn],authserver=[],portal=[web-access],host=[208.91.115.10],realm=
  [],idx=0,auth=256,sid=1424c6b9,login=1576802935,access=1576802935,sam1_logout_url=yes
[919:root:0]allocSSLConn:289 sconn 0x7f5962887000 (0:root)
total sslvpn policy count: 1
[925:root:0]total sslvpn policy count: 1
[923:root:7b]req: /remote/logout
[923:root:7b]deconstruct_session_id:426 decode session id ok, user=[ssl-azure-saml],group=
  [sslvpn],authserver=[],portal=[web-access],host=[208.91.115.10],realm=
  [],idx=0,auth=256,sid=a205b36,login=1576804178,access=1576804178,saml_logout_url=yes
[923:root:7b]session removed s: 0x7f5962887000 (root)
[923:root:7b]deconstruct_session_id:426 decode session id ok, user=[ssl-azure-saml],group=
  [sslvpn],authserver=[],portal=[web-access],host=[208.91.115.10],realm=
  [],idx=0,auth=256,sid=a205b36,login=1576804178,access=1576804178,saml_logout_url=no
[923:root:0]sslvpn_internal_remove_one_web_session:2848 web session (root:ssl-azure-
  saml:sslvpn:208.91.115.10:0 0) removed for User requested termination of service
[924:root:7a]rmt_check_conn_session:2129 delete connection 0x7f5962887000 w/ web session 0
[924:root:7a]Destroy sconn 0x7f5962887000, connSize=1. (root)
[924:root:7b]rmt_check_conn_session:2129 delete connection 0x7f5962888900 w/ web session 0
[924:root:7b]Destroy sconn 0x7f5962888900, connSize=0. (root)
[923:root:7c]rmt_check_conn_session:2129 delete connection 0x7f5962888900 w/ web session 0
[923:root:7c]Destroy sconn 0x7f5962888900, connSize=1. (root)
```

```
[923:root:7b]rmt_check_conn_session:2129 delete connection 0x7f5962887000 w/ web session 0
[923:root:7b]Destroy sconn 0x7f5962887000, connSize=0. (root)
[925:root:7a]SSL state:warning close notify (208.91.115.10)
[925:root:7a]sslConnGotoNextState:305 error (last state: 1, closeOp: 0)
[925:root:7a]Destroy sconn 0x7f5962887000, connSize=1. (root)
dchaofgt # [925:root:7b]SSL state:warning close notify (208.91.115.10)
[925:root:7b]sslConnGotoNextState:305 error (last state: 1, closeOp: 0)
[925:root:7b]Destroy sconn 0x7f5962888900, connSize=0. (root)
```

# Azure Sentinel

## Sending FortiGate logs for analytics and queries

See [Connect Fortinet to Azure Sentinel](#).

# Change log

Date	Change description
2020-03-31	Initial release.
2020-05-05	Updated <a href="#">Creating a support account on page 12</a> .
2020-05-08	Updated <a href="#">To configure multizone active-passive HA in Azure</a> :
2020-05-13	Added <a href="#">Verifying the license type on page 13</a> and <a href="#">Migrating a FortiGate-VM instance between license types on page 14</a> . Updated <a href="#">Order types on page 11</a> .
2020-05-15	Updated <a href="#">Order types on page 11</a> .
2020-06-05	Updated <a href="#">Checking the prerequisites</a> and <a href="#">To configure multizone active-passive HA in Azure</a> :
2020-06-08	Updated <a href="#">Connecting a local FortiGate to an Azure VNet VPN on page 126</a> .
2020-07-03	Updated <a href="#">Configuring FortiClient VPN with multifactor authentication on page 151</a> .
2020-07-09	Added <a href="#">To configure a VDOM exception</a> :
2020-08-14	Added <a href="#">Obtaining a FortiCare-generated license for Azure on-demand instances on page 15</a> .
2020-10-09	Updated <a href="#">Deploying autoscaling on Azure on page 42</a> .
2020-10-28	Updated <a href="#">Configuring SAML SSO login for SSL VPN web mode with Azure AD acting as SAML IdP on page 156</a> .
2020-10-30	Updated <a href="#">Configuring integration with Azure AD domain services for VPN on page 147</a> and <a href="#">Azure AD acting as SAML IdP on page 156</a> .
2020-11-27	Updated <a href="#">Configuring SAML SSO login for SSL VPN web mode with Azure AD acting as SAML IdP on page 156</a> .
2020-12-08	Updated <a href="#">Order types on page 11</a> . Updated <a href="#">Deploying autoscaling on Azure on page 42</a> .
2020-12-11	Updated <a href="#">Creating a support account on page 12</a> .
2021-01-06	Updated <a href="#">HA for FortiGate-VM on Azure on page 105</a> .
2021-02-04	Updated <a href="#">Configuring SAML SSO login for SSL VPN web mode with Azure AD acting as SAML IdP on page 156</a> .
2020-02-10	Updated <a href="#">Deploying autoscaling on Azure on page 42</a> .
2021-02-19	Updated <a href="#">SDN connector in Azure Stack on page 123</a> .
2021-02-23	Updated <a href="#">SDN connector integration with Azure on page 111</a> .
2021-05-14	Added <a href="#">Deploying FortiGate-VM from the marketplace on page 37</a> . Updated <a href="#">Single FortiGate-VM deployment on page 94</a> .

## Change log

---

Date	Change description
2021-05-20	Updated <a href="#">Deploying autoscaling on Azure on page 42</a> to add support for FortiAnalyzer.
2021-08-25	Updated <a href="#">Deploying autoscaling on Azure on page 42</a> to add support for upgrading from the 2.0.9 template to the 3.3.2 template.



**FORTINET**



Copyright© 2021 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.