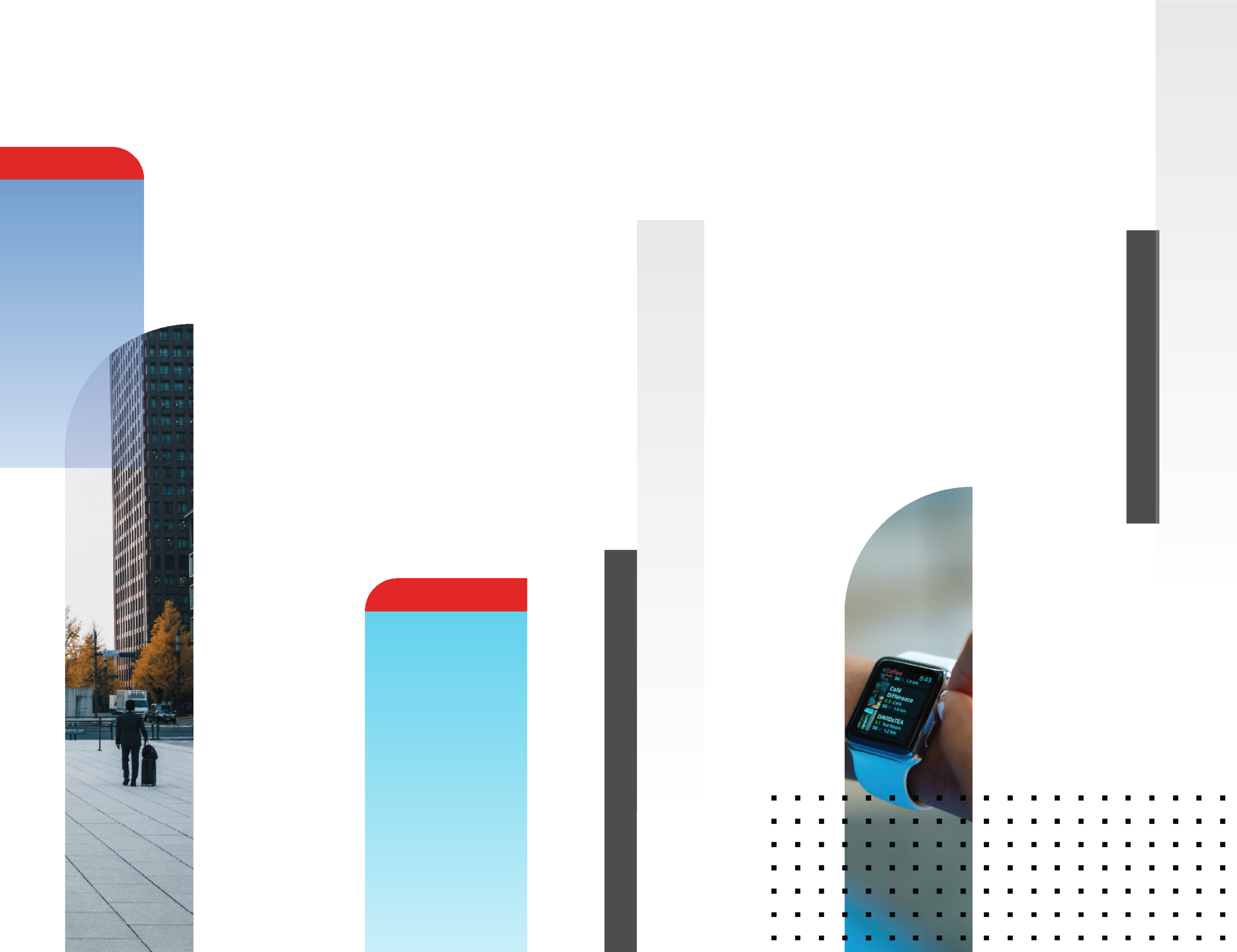
Azure Guide

FortiSandbox 4.4.0 - 4.4.4



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
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

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

March 18, 2024
FortiSandbox 4.4.0 - 4.4.4 Azure Guide
34-440-969156-20240318

TABLE OF CONTENTS

About FortiSandbox VM for Azure

Fortinet’s FortiSandbox on Azure enables organizations to defend against advanced threats in the cloud. It works with network, email, endpoint, and other security measures, or as an extension of on-premise security architecture to leverage scale with complete control.

FortiSandbox is available on the Azure Marketplace.

You can install FortiSandbox on Azure as a standalone zero-day threat prevention or you can configure it to work with your existing FortiGate, FortiMail, or FortiWeb Azure instances to identify malicious and suspicious files, ransomware, and network threats.

You can create custom VMs using pre-configured VMs, your own ISO image, or Red Hat VMs on VirtualBox. For more information, contact Fortinet Customer Service & Support.

This document contains images from the Microsoft Azure interface. Some images and text strings may not reflect the current Azure version. Where possible, we have noted the version the image is based on.

For the most accurate Azure information, please refer to the product documentation.

Nested deployments

Starting in FortiSandbox version 4.4.4, only *Nested* BYOL deployments from the marketplace are supported. Please use the HyperV model image to upgrade going forward.

What is the difference between a nested and non-nested BYOL deployment?

A Nested BYOL Azure FortiSandbox will run guest VMs inside the appliance allowing for more control for those VMs. Nested BYOL also support more types of VMs, including the Default VM, Optional VM, Customized VM and Cloud VM.

A Non-Nested BYOL runs VMs outside the appliance. Non-nested BYOL and PAYG only support Customized VM and Cloud VM.

BYOL deployments before version 4.4.4

BYOL appliances deployed before version 4.4.4 are now referred to as *Non-Nested BYOL*. These appliances can still be upgraded with the Azure model image.

Deploying a nested BYOL

The deployment process for nested and non-nested BYOL are essentially the same with minor variations, specifically:

- Minimum system requirements
- Deploying FortiSandbox on Azure with the GUI
- Setting up the local VM
- Configuring a HA cluster

Any variations to the process are indicated within the deployment steps.

Deployment mode

You can configure your FortiSandbox VM on Azure using following modes:

Basic Mode

Basic Mode is the fastest and easiest way to deploy a FortiSandbox VM on Azure. It uses the Azure setup wizard to guide you through the setup process with step-by-step instructions.

Advanced Mode

Advanced Mode uses the advanced features of the FortiSandbox VM including custom VMs and HA features. It requires you to manually create all the resources you need. This mode is recommended for customers with experience working with Azure and the cloud. To use custom VMs, including pre-configured VMs, your own ISO image, or Red Hat VMs on VirtualBox, contact Fortinet Customer Service & Support.

Comparison chart:

	Basic Mode	Advanced Mode
HA	• A single setup wizard page where you can enter all the information for launching a FortiSandbox VM. • Only simple information is required: resource group name, VM name, VM region, VM size, username, and your SSH key or user password. • The setup wizard automatically creates and deploys resources such as storage account, virtual network, network interface, public IP address, and the virtual machine instance.	• Gives you full control to customize the resources required to deploy the VM. • Supports custom Windows VMs. • Supports HA features.
Deployment time	Approximately 20 minutes.	Approximately one hour.
Limitations	• The FortiSandbox VM is created with only one network interface. • HA features require at least two network interfaces. • If you want to add a second network interface, you must shut down the VM and then manually create and attach the	• Takes longer to deploy. • Requires advanced knowledge of deploying VMs in Azure. • Must deploy all components manually in Azure. • Must follow instructions carefully for a successful deployment.

	Basic Mode	Advanced Mode
	new network interface. • Supports sandboxing analysis using Windows Cloud VMs only. • Does not support custom Windows VMs.	

Licensing

Fortinet offers the FortiSandbox VM00 model (FSA-VM00) for your private cloud deployment solution.

The FSA-VM00 is a base license. You need to purchase the required Windows license keys to activate enabled Windows VMs with a minimum of 1 and maximum of 8 licenses. Ton increase capacity, the FSA-VM00 is capable of using the Windows Cloud VM with a minimum of 5 and maximum of 200 VMs.

Ordering and registering licenses

Licenses can be purchased through a Fortinet Authorized Reseller or directly from Fortinet. After placing an order for FortiSandbox VM, Fortinet sends a license registration code to the email address used to place the order. Use this license registration code to register the FortiSandbox VM with Customer Service & Support at https://support.fortinet.com.

After registration, you can download the license file. You will need this file to activate your FortiSandbox. You can configure basic network settings using CLI commands to complete the deployment. When the license file is uploaded and validated, the engines will be downloaded short after. Then, the system will be fully functional.

More information

Purchasing a license	Contact your Fortinet Authorized Reseller, or visit https://www.fortinet.com/how_to_buy/
FortiSandbox Ordering Guide	Visit https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-fortisandbox.pdf
FortiSandbox product Datasheet	Visit https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf
Hardware recommendations	See Minimum system requirements on page 9.

Minimum system requirements

When configuring your FortiSandbox hardware settings, use the following table as a guide with consideration for future expansion.

Technical Specification	Details			
	On-Premise (Private) Cloud	Public Cloud - BYOL (Non-nested)	Public Cloud - PAYG	Public Cloud BYOL (Nested)
Hypervisor Support	VMware ESXi Microsoft Hyper-V Windows server 2016 and 2019	AWS Azure		Azure
HA Support	FortiSandbox 3.2 or later			
Virtual CPUs (min / max)	4/Unlimited Fortinet recommends four virtual CPUs plus the number of VM clones.	4/16 Fortinet recommends following virtual CPUs based on the number of VM Clones: 0-4 clones - 4 cores, 5-32 clones - 8 cores, 33-100 clones - 16 cores, 101+ clones - 16 cores or higher. Pick up the appropriate Instance Type.		8/Unlimited Fortinet 8 virtual CPUs plus the number of VM clones.
Virtual Memory (min / max)	16 GB / 32 GB Fortinet recommends following virtual memory based on the number of VM Clones: 0-4 clones - 24 GB 5-8 clones - 32 GB	8 GB / 64 GB Recommended: Following virtual memory based on the number of VM Clones: 0-4 clones - 8 GB, 5-32 clones - 16 GB, 33-100 clones - 32 GB, 101+ clones - 64 GB. Pick the appropriate Instance Type.		32GB/64GB Fortinet recommends following virtual memory based on the number of VM Clones: 0-4 clones - 24 GB 5-8 clones - 32 GB
Virtual Storage (min / max)	200 GB / 16 TB Fortinet recommends at least 500 GB for a production environment.			
Virtual Network Interfaces	Recommended: 4 and above	Recommended: 2 and above		Recommended: 3 and above
VM Clones Support (Min/Max)	0[1]/ 8 (Local VMs) and 200 (Cloud VMs)	0[1] / 216[2]	0[1] / 128[3]	0[1]/ 8 (Local VMs) and 200 (Cloud VMs)

[1] For HA-Cluster deployment setup configured as Primary node acting as a dispatcher.

[2] Can enable any of the Custom VM or Cloud VM types up to the total seat count which is based on a combination of Windows licenses (max of 8), BYOL (8) and Cloud VMs (max of 200).

[3] Total seat count is based on the number of cores multiplied by 4. Maximum VMs is 128 since the highest available vCPU on PAYG is 32. CloudVMs can also be added on top and registered, however, this is not advised due to product serial number changes after shutdown.

Set up the Azure environment for FortiSandbox

Before deploying a FortiSandbox instance, some basic steps are required to setup and run the Azure environment.

To start, log into the Azure management portal with a user account that has enough privileges to create a new resource group.

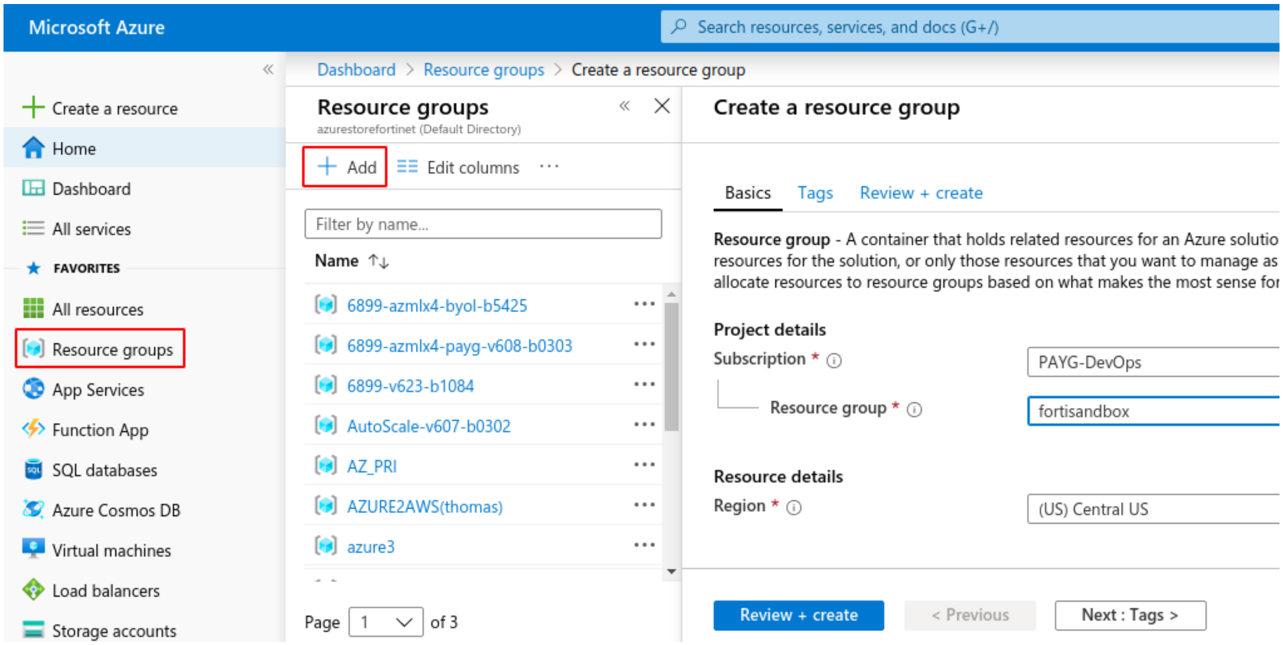
To set up the Azure environment for deployment:

1. Create a resource group on page 11
2. Create network security groups on page 12
3. Create virtual networks on page 13
4. Create storage accounts on page 15
5. Create network interfaces on page 17
6. Create a data disk on page 19

Create a resource group

To create resource groups in Azure:

1. In the Azure portal, click *Resource groups* in the left pane.
2. Click *Add* to create a new empty resource group.



Resource group - A container that holds related resources for an Azure solutio resources for the solution, or only those resources that you want to manage as allocate resources to resource groups based on what makes the most sense for

Subscription * PAYG-DevOps

Resource group * fortisandbox

Region * (US) Central US

3. Enter the following information:

Subscription	Select a subscription.

Resource group	Name of the resource group.
Region	Select a resource group location.

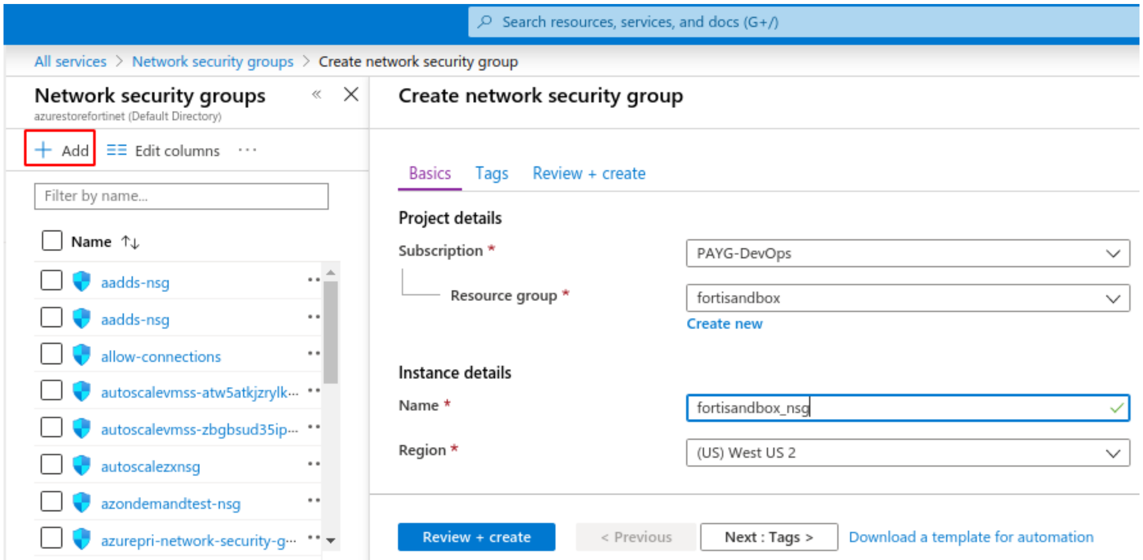
Create network security groups

Create two network security groups:

- The first security group must have inbound rules allowing for HTTPS, SSH traffic, OFTP, FortiGuard, FTP and RDP.
- The second security group must have inbound rules allowing for FTP and RDP.

To create network security groups in Azure:

1. In the Azure portal, click *Network security groups* in the left pane.
2. Click *Add* to create a new network security group for FortiSandbox port1 subnet (the management subnet).



Search resources, services, and docs (G+/)
All services > Network security groups > Create network security group
Network security groups
azurestorefortinet (Default Directory)
+ Add
Edit columns
Filter by name...
Name
aadds-nsg
aadds-nsg
allow-connections
autoscalevmss-atw5atkjzrylk...
autoscalevmss-zbgbsud35ip...
autoscalezxnsg
azondemandtest-nsg
azurepri-network-security-g...
Create network security group
Basics
Tags
Review + create
Review + create
< Previous
Next : Tags >
Download a template for automation

Project details

Subscription * PAYG-DevOps

Resource group * fortisandbox

Create new

Instance details

Name * fortisandbox_nsg

Region * (US) West US 2

3. Enter the following information:

Subscription	Select a subscription type.
Resource group	Select the resource group you created in the Create a resource group step.
Name	Name of the network security group.
Region	Select the location you used when you set up the resource group.

4. Repeat these steps to create a second network security group for the FortiSandbox port2 subnet (FSA reserved port2 for firmware instance to communicate with local Windows or Linux clones).
5. Go to the security groups and configure the inbound rules:
   - Network security group one: HTTPS (TCP 443), SSH traffic (TCP 22), OFTP traffic (TCP 514). Optional: ICAP traffic (TCP 1344), ICAP over SSL (TCP 11344), RDP to VM interaction (FortiSandbox reserved 9833).

- Network security group two: FTP (TCP 21).

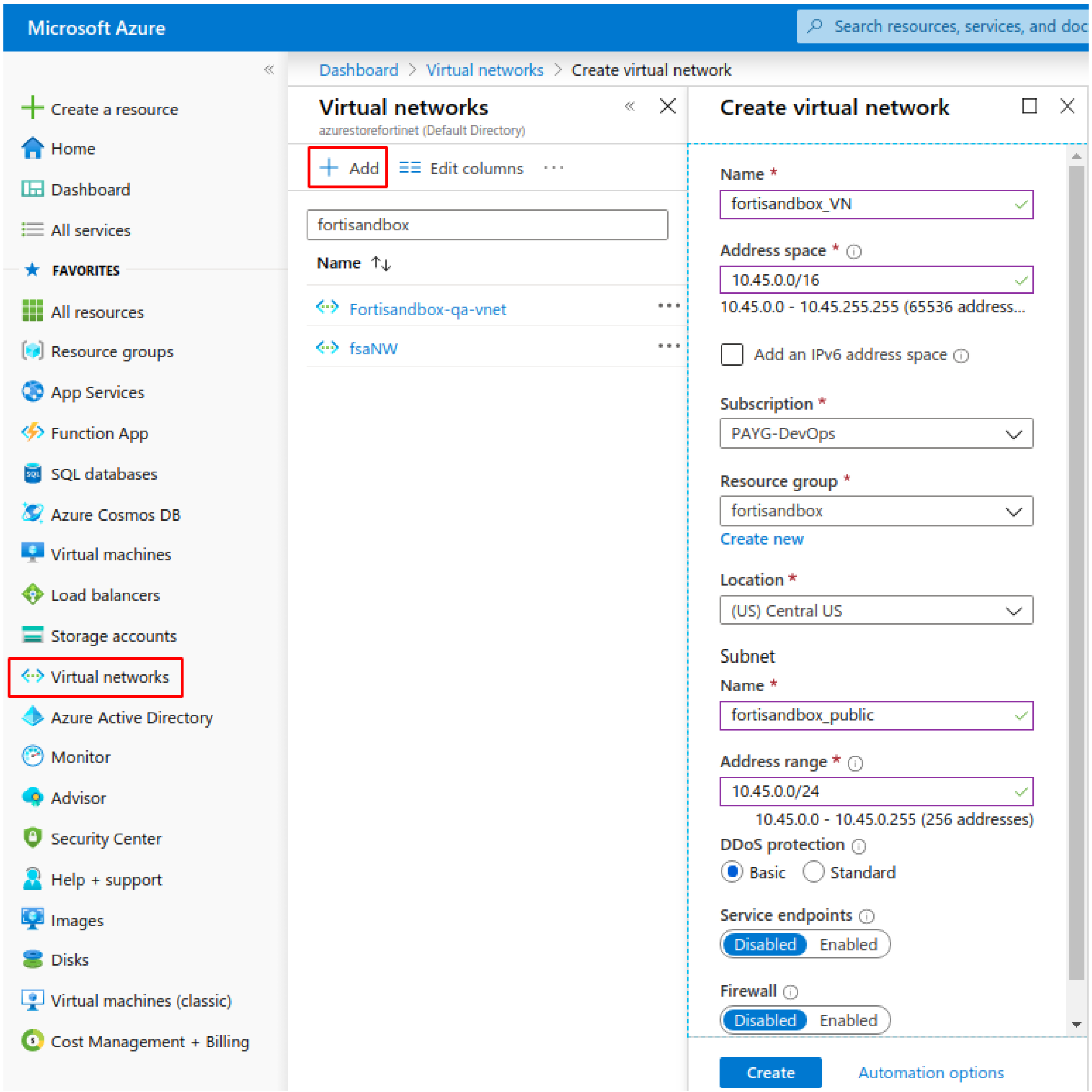
> If you choose to use Windows cloud clones located in Fortinet Data Center, the network security group for port2 subnet is not required.

6. Configure the outbound rules: Allow traffic to go out.

Create virtual networks

To create virtual networks in Azure:

1. In the Azure portal, select *Virtual networks* in the left pane.
2. Select *Add* to create a new virtual network.



Name * fortisandbox_VN

Address space * 10.45.0.0/16

10.45.0.0 - 10.45.255.255 (65536 address...

☐ Add an IPv6 address space

Subscription * PAYG-DevOps

Resource group * fortisandbox

Create new

Location * (US) Central US

Subnet

Name * fortisandbox_public

Address range * 10.45.0.0/24

10.45.0.0 - 10.45.0.255 (256 addresses)

DDoS protection ● Basic ○ Standard

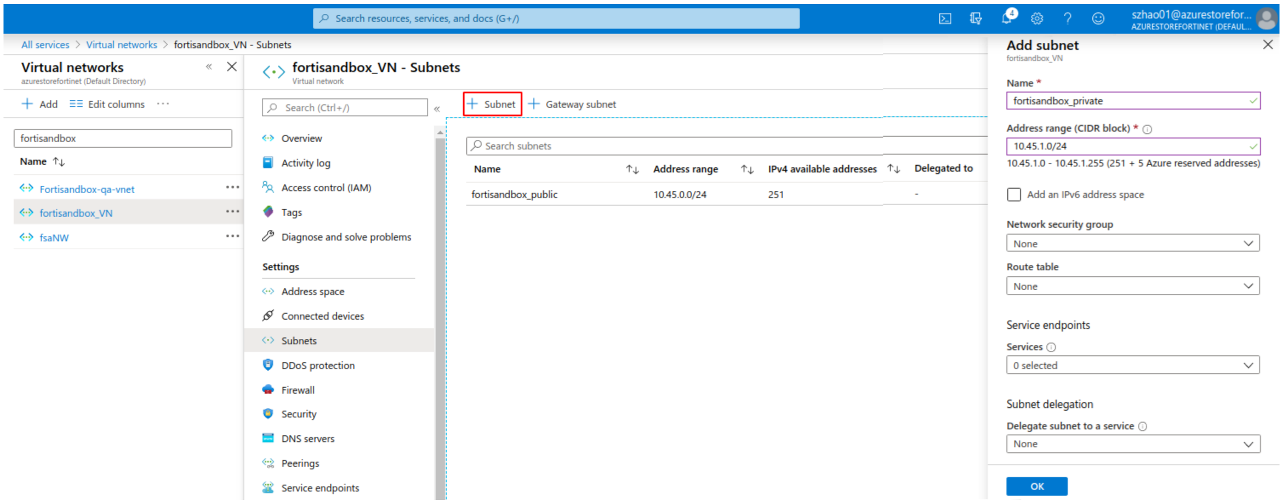
Service endpoints [✓ Disabled] Enabled

Firewall [✓ Disabled] Enabled

3. Enter the following information:

Name	Name of the virtual network.
Address space	Use an Azure suggested unused class B network (`xxx.xxx.0.0/16`) or enter your preferred unused class B network. The address space should cover all the IP ranges this resource group will use.
Subscription	Select your subscription type.
Resource group	Select the resource group you created in the Create a resource group step.
Location	Select the location you used when you set up the resource group.
Subnet Name	Name of port1 (the management port) subnet.
Subnet Address range	Enter a class C address range (`xxx.xxx.xxx.0/24`) within the virtual network.
DDoS protection	Basic.
Service endpoints	Disabled.

4. Click *Create*.
5. Create one additional subnet in the virtual network:
   - Enter the subnet name for FSA port2 (the local VM clones communication port), and assign another class C address range (xxx.xxx.xxx.0/24).



Name	Address range	IPv4 available addresses	Delegated to
fortisandbox_public	10.45.0.0/24	251	-

Add subnet
fortisandbox_VN

Name *: fortisandbox_private

Address range (CIDR block) *: 10.45.1.0/24

10.45.1.0 - 10.45.1.255 (251 + 5 Azure reserved addresses)

☐ Add an IPv6 address space

Network security group: None

Route table: None

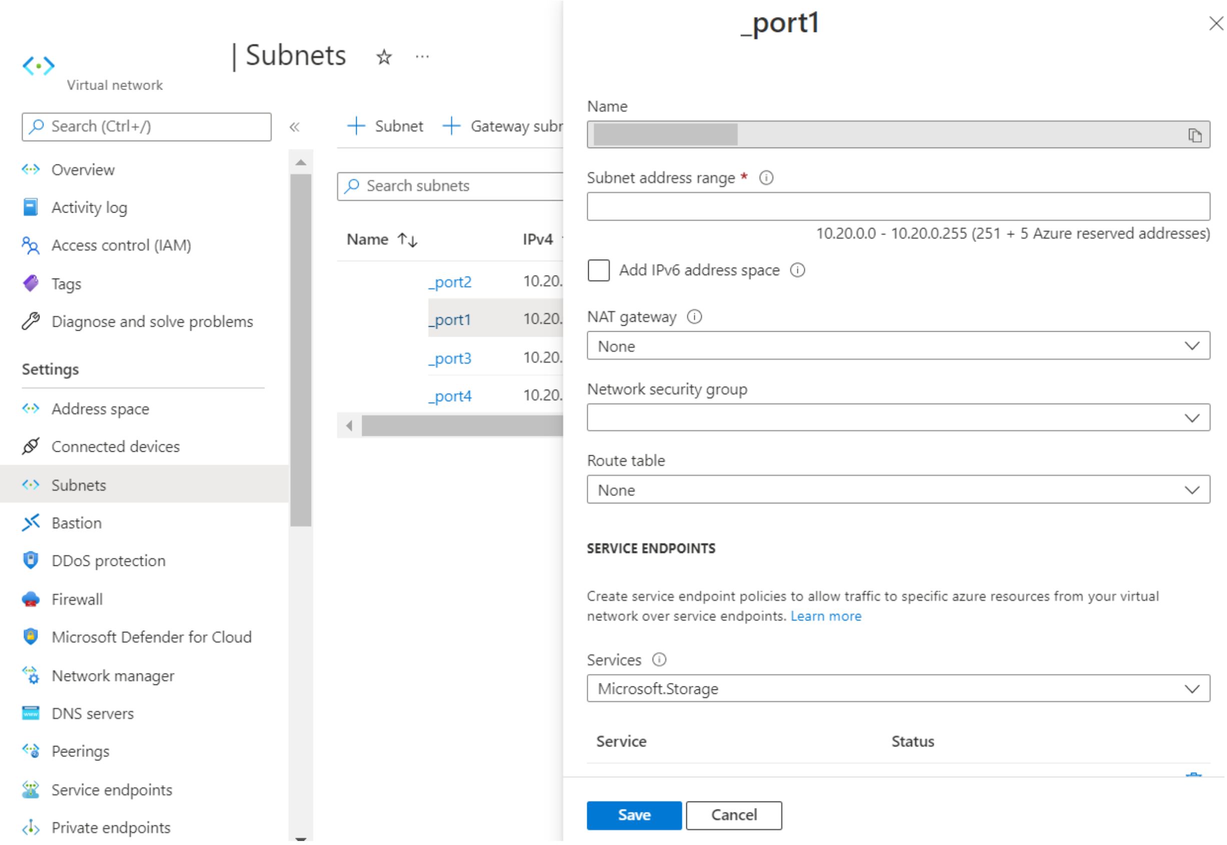
Service endpoints

Services: 0 selected

Subnet delegation

Delegate subnet to a service: None

6. Associate network security group to subnet.
   a. Associate the network security group for FortiSandbox port1 subnet to port1 subnet
   b. Associate the network security group for FortiSandbox port2 subnet to port2 subnet



Name ↑↓	IPv4
_port2	10.20.
_port1	10.20.
_port3	10.20.
_port4	10.20.

_port1

Name

[redacted]

Subnet address range *

10.20.0.0 - 10.20.0.255 (251 + 5 Azure reserved addresses)

□ Add IPv6 address space

NAT gateway: None

Network security group:

Route table: None

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. Learn more

Services: Microsoft.Storage

Service	Status

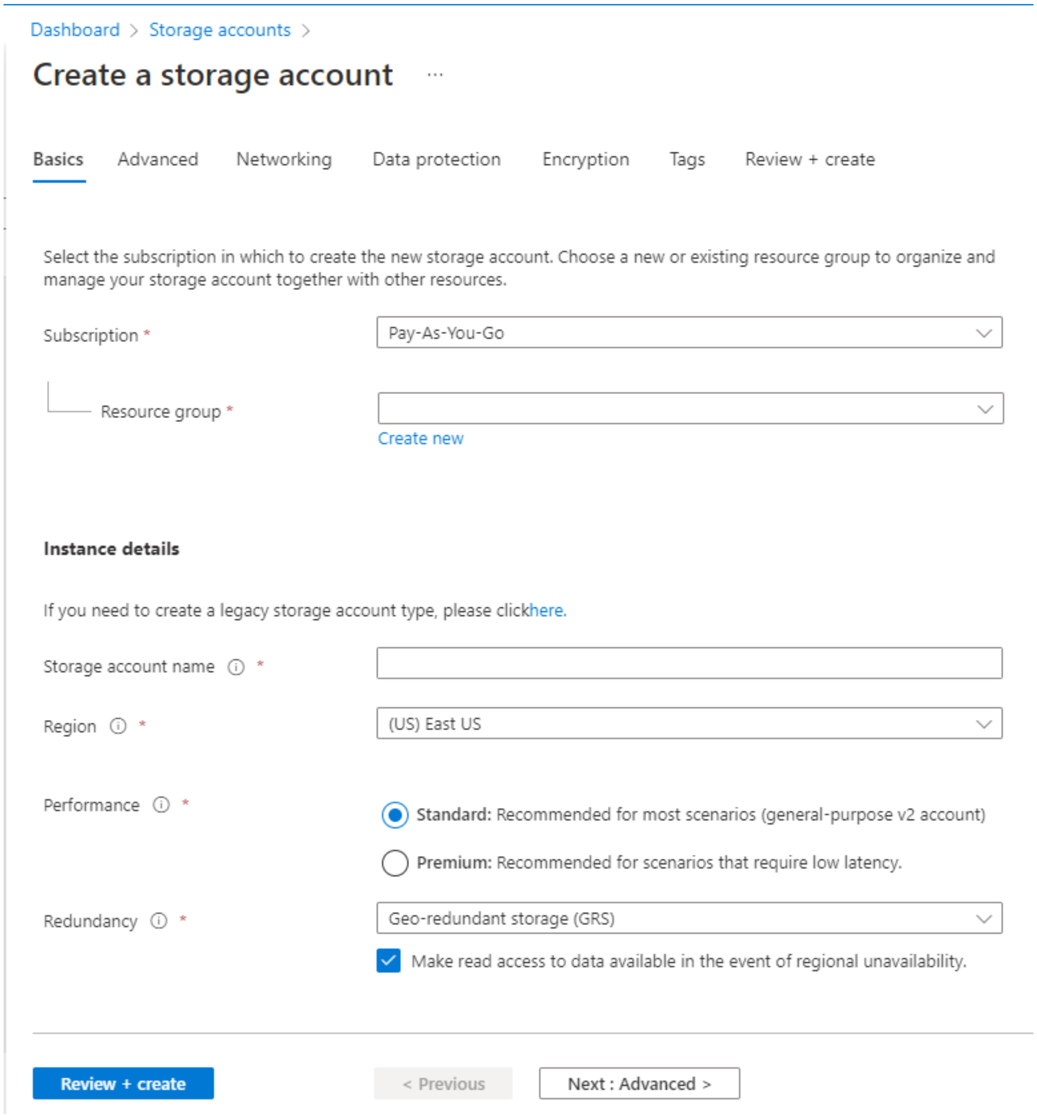
Create storage accounts

Create two storage accounts:

- The first storage account is for storing the FortiSandbox firmware image (Storage Account).
- The second storage account is for storing diagnostic information (Monitor Account), such as FortiSandbox diagnostic screenshots, console of FortiSandbox VM and VM clone diagnostic screenshots during job scans.

To create storage accounts in Azure:

1. In the Azure portal, click *Storage accounts* in the left pane.
2. Click *Add* to create a new storage account.



Create a storage account ...

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription * Pay-As-You-Go

Resource group *

Instance details

If you need to create a legacy storage account type, please clickhere.

Storage account name ⓘ *

Region ⓘ * (US) East US

Performance ⓘ *

● **Standard:** Recommended for most scenarios (general-purpose v2 account)

○ **Premium:** Recommended for scenarios that require low latency.

Redundancy ⓘ * Geo-redundant storage (GRS)

☑ Make read access to data available in the event of regional unavailability.

3. Enter the following information for each account:

Subscription	Select your subscription type.
Resource group	Select the resource group you created in the Create a resource group step.
Storage account name	Name of the storage account.
Location	Select the location you used when you set up the resource group.
Performance	Standard.
Replication	Geo-Redundant Storage (GRS).

4. Select *Review + Create*.
5. Repeat these steps to create a second storage account.

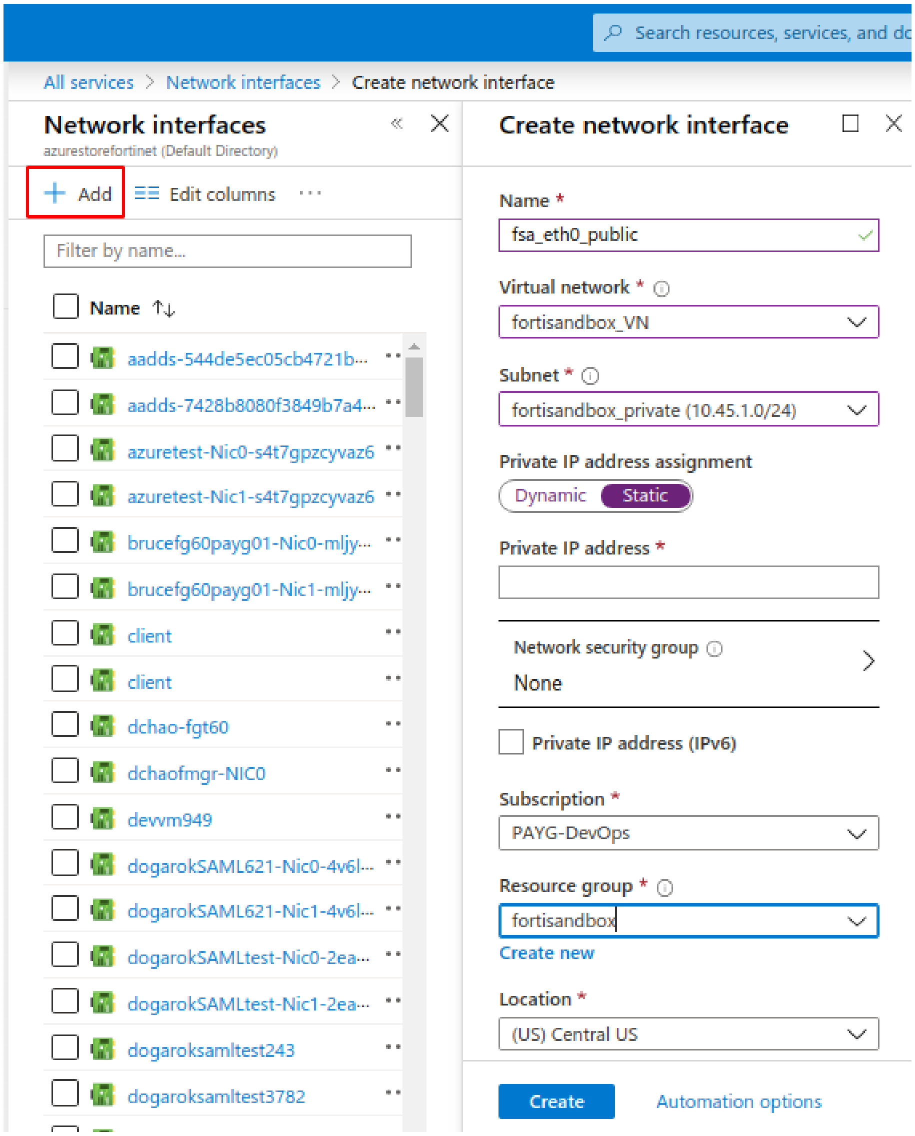
Create network interfaces

Create the following network interfaces:

- The first network interface is for FortiSandbox *port1*.
- The second network interface is for FortiSandbox *port2*.
- If needed, you can create more network interfaces, such as for client devices to submit files, or inter-communications between HA Cluster nodes. To do that, more network security groups and virtual networks might be needed.

To create a network interface in Azure:

1. In the Azure portal, click *Network interfaces* in the left pane.
2. Click *Add* to create a new network interface.



Search resources, services, and dc
All services > Network interfaces > Create network interface
Network interfaces
azurestorefortinet (Default Directory)
+ Add
Edit columns
Filter by name...
Name
Create network interface
Create
Automation options

aadds-544de5ec05cb4721b...
aadds-7428b8080f3849b7a4...
azuretest-Nic0-s4t7gpzcyvaz6
azuretest-Nic1-s4t7gpzcyvaz6
brucefg60payg01-Nic0-mljy...
brucefg60payg01-Nic1-mljy...
client
client
dchao-fgt60
dchaofmgr-NIC0
devvm949
dogarokSAML621-Nic0-4v6l...
dogarokSAML621-Nic1-4v6l...
dogarokSAMLtest-Nic0-2ea...
dogarokSAMLtest-Nic1-2ea...
dogaroksamltest243
dogaroksamltest3782

Name *: fsa_eth0_public

Virtual network *: fortisandbox_VN

Subnet *: fortisandbox_private (10.45.1.0/24)

Private IP address assignment: Dynamic [✓ Static]

Private IP address *:

Network security group: None

□ Private IP address (IPv6)

Subscription *: PAYG-DevOps

Resource group *: fortisandbox

Create new

Location *: (US) Central US

3. Enter the following information:

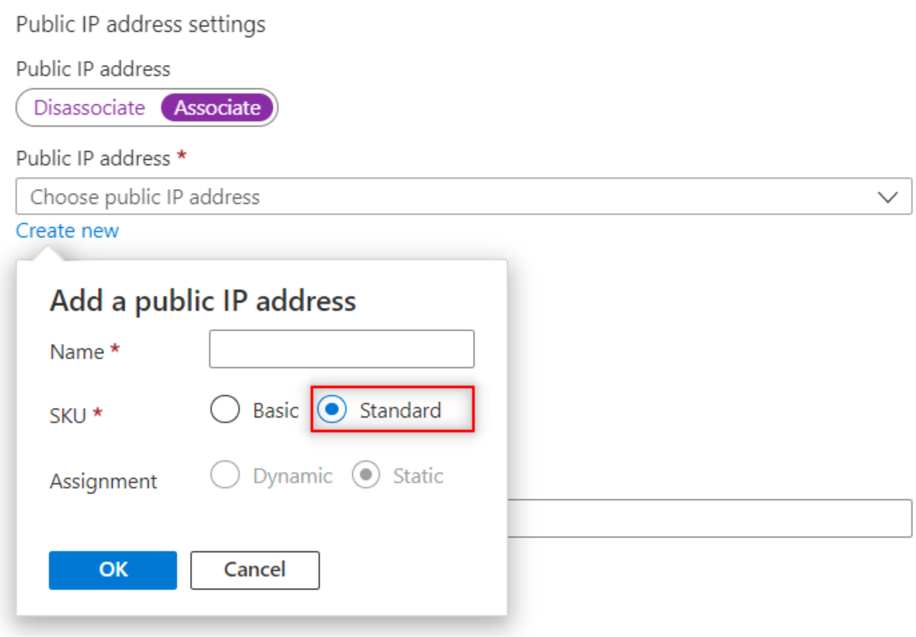
Name	VM name.
Virtual network	Select your Virtual Network.
Subnet	One subnet under your Virtual Network. Each interface you create must be on a different subnet.
Private IP address assignment	Static.
Private IP address	Self-defined static IP address.
Network security group	Select the security group you created.
Private IP address (IPv6)	Unchecked.
Subscription	Subscription type.
Resource group	The resource group you created in the Create a resource group step.
Location	Select the same location used while setting up the resource group.

4. Repeat these steps to create the network interfaces you need.

If you have created multiple network security groups:

- The group associated with the FSA port1 interface must be one included in HTTPS (TCP 443), SSH traffic (TCP 22), OFTP traffic (TCP 514).
- The group associated with the FSA port2 interface must be one including FTP(TCP 21).

Associate the network interface used for the FSA management port (port1) with the *Public IP* address in the IP configuration section.



Public IP address settings

Public IP address

Disassociate [✓ Associate]

Public IP address *

Choose public IP address

Create new

Add a public IP address

Name *

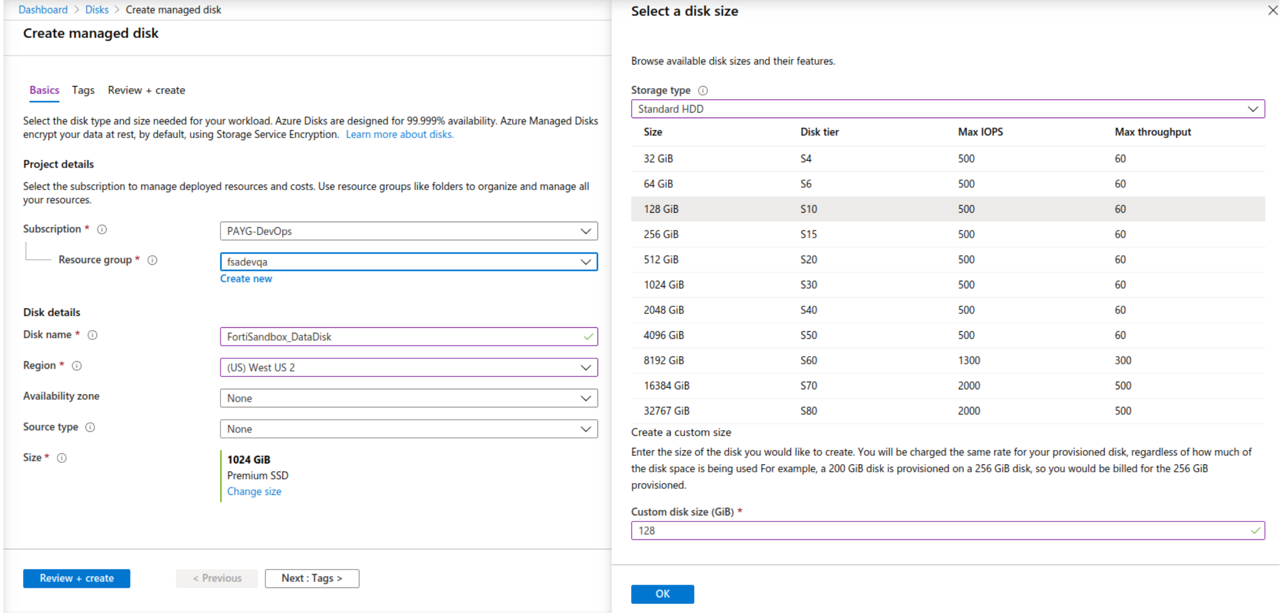
SKU * ○ Basic ● Standard

Assignment ○ Dynamic ● Static

Create a data disk

To create a data disk:

1. In the Azure portal, click *Disks* in the left pane.
2. Click *Add* to create a data disk of at least 200GB.



Create managed disk

Select the disk type and size needed for your workload. Azure Disks are designed for 99.999% availability. Azure Managed Disks encrypt your data at rest, by default, using Storage Service Encryption. Learn more about disks.

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 * : fsadevqa

Create new

Disk details

Disk name * : FortiSandbox_DataDisk

Region * : (US) West US 2

Availability zone : None

Source type : None

Size * : 1024 GiB
Premium SSD
Change size

Select a disk size

Browse available disk sizes and their features.

Storage type : Standard HDD

Size	Disk tier	Max IOPS	Max throughput
32 GiB	S4	500	60
64 GiB	S6	500	60
128 GiB	S10	500	60
256 GiB	S15	500	60
512 GiB	S20	500	60
1024 GiB	S30	500	60
2048 GiB	S40	500	60
4096 GiB	S50	500	60
8192 GiB	S60	1300	300
16384 GiB	S70	2000	500
32767 GiB	S80	2000	500

Create a custom size

Enter the size of the disk you would like to create. You will be charged the same rate for your provisioned disk, regardless of how much of the disk space is being used For example, a 200 GiB disk is provisioned on a 256 GiB disk, so you would be billed for the 256 GiB provisioned.

Custom disk size (GiB) * : 128

Keep monitoring the usage of data disk, expand the data disk size when needed. For more information, see the FortiSandbox *Best Practices and Troubleshooting Guide*.

Deploy FortiSandbox VM on Azure (PAYG / BYOL)

You can deploy FortiSandbox VM using the Azure GUI or CLI:

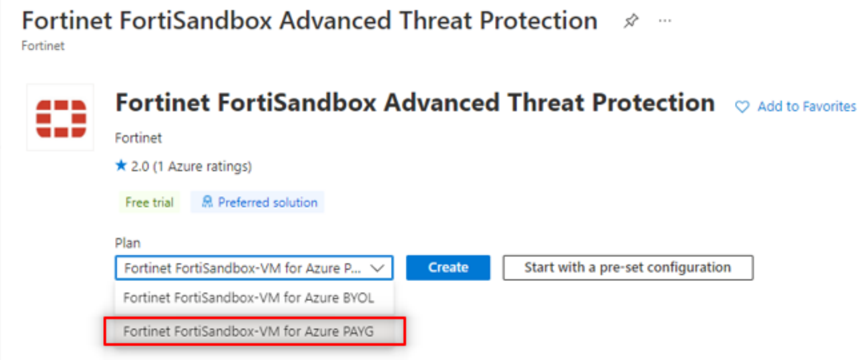
- Deploy FortiSandbox instance on Azure using the GUI
- Deploy FortiSandbox instance on Azure using the CLI

Deploy FortiSandbox instance on Azure using the GUI

Starting in FortiSandbox version 4.4.4, only nested BOYL deployments from the marketplace are supported. For more information, see Nested deployments on page 5.

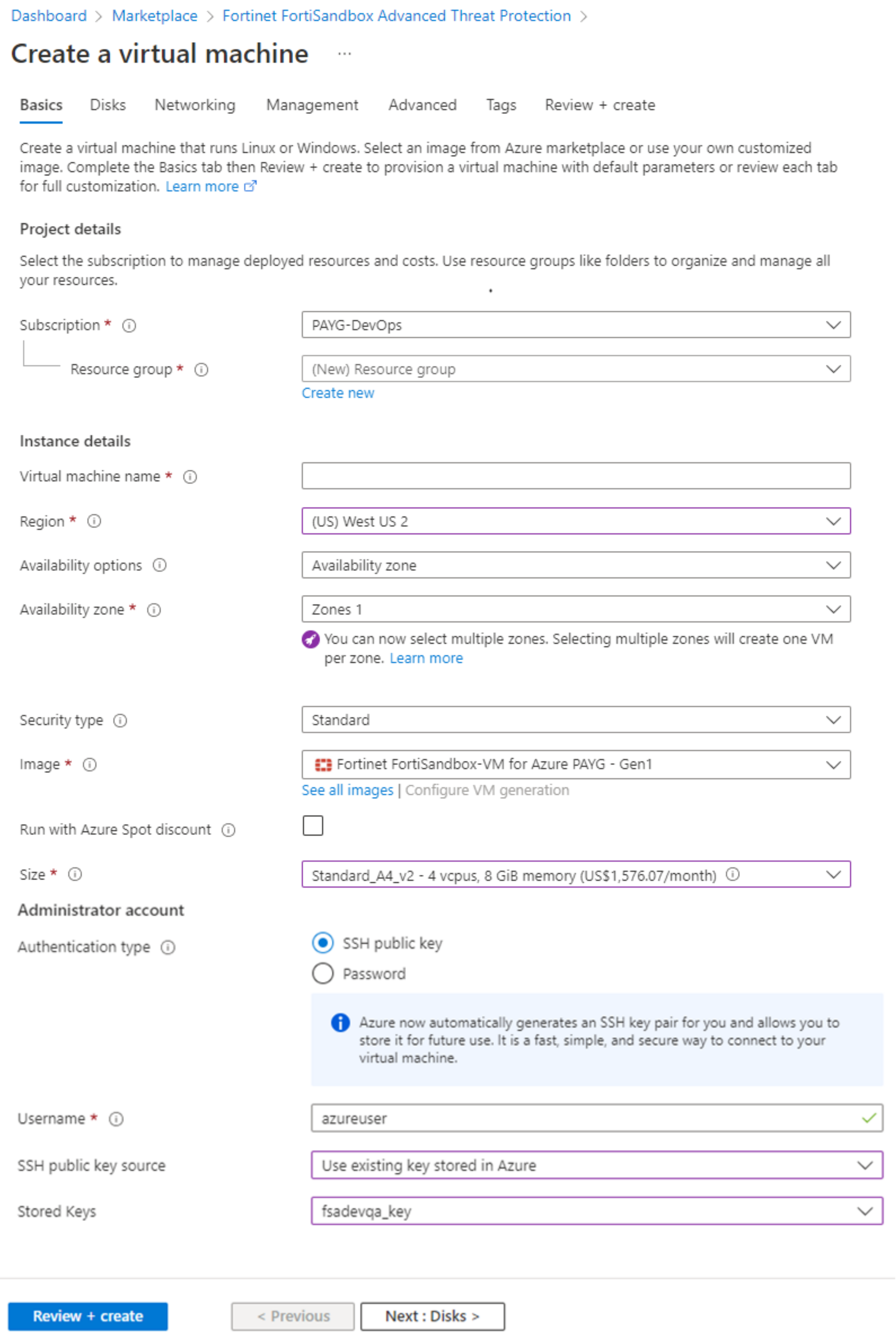
To deploy FortiSandbox on Azure with the GUI:

1. Go to *Azure Marketplace* and search for *Fortinet FortiSandbox*.
2. From the *Plan* dropdown, select *Fortinet FortiSandbox-VM for Azure PAYG* or *Fortinet FortiSandbox-VM for Azure BYOL* and click *Create*.


Fortinet FortiSandbox Advanced Threat Protection
Fortinet
Fortinet FortiSandbox Advanced Threat Protection
Add to Favorites
Fortinet
★ 2.0 (1 Azure ratings)
Free trial
Preferred solution
Plan
Fortinet FortiSandbox-VM for Azure P...
Create
Start with a pre-set configuration
Fortinet FortiSandbox-VM for Azure BYOL
Fortinet FortiSandbox-VM for Azure PAYG

3. On the *Create a virtual machine*, configure the settings in the *Basics* tab.

Resource group	Choose the one created for FSA.
Virtual machine name	Name of the FSA VM.
Region	The region should be same as the resource group.
Size	Select the VM instance type. The type should be close to the resource recommendations as shown in the table above. FortiSandbox on Azure uses the temporary disk (provided free by the VM) to store and process job files. A secondary disk is not required. For nested BYOL, please select *Standard_D8s_v3* and above. Use the guidelines in the Minimum system requirements to choose the correct size.
Authentication type	Click *Password* or *SSH public key*.



Dashboard > Marketplace > Fortinet FortiSandbox Advanced Threat Protection >

Create a virtual machine ...

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

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more

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 * ⓘ: (New) Resource group

Create new

Instance details

Virtual machine name * ⓘ:

Region * ⓘ: (US) West US 2

Availability options ⓘ: Availability zone

Availability zone * ⓘ: Zones 1

You can now select multiple zones. Selecting multiple zones will create one VM per zone. Learn more

Security type ⓘ: Standard

Image * ⓘ: Fortinet FortiSandbox-VM for Azure PAYG - Gen1

See all images | Configure VM generation

Run with Azure Spot discount ⓘ: □

Size * ⓘ: Standard_A4_v2 - 4 vcpus, 8 GiB memory (US$1,576.07/month) ⓘ

Administrator account

Authentication type ⓘ:

● SSH public key

○ Password

Azure now automatically generates an SSH key pair for you and allows you to store it for future use. It is a fast, simple, and secure way to connect to your virtual machine.

Username * ⓘ: azureuser ✓

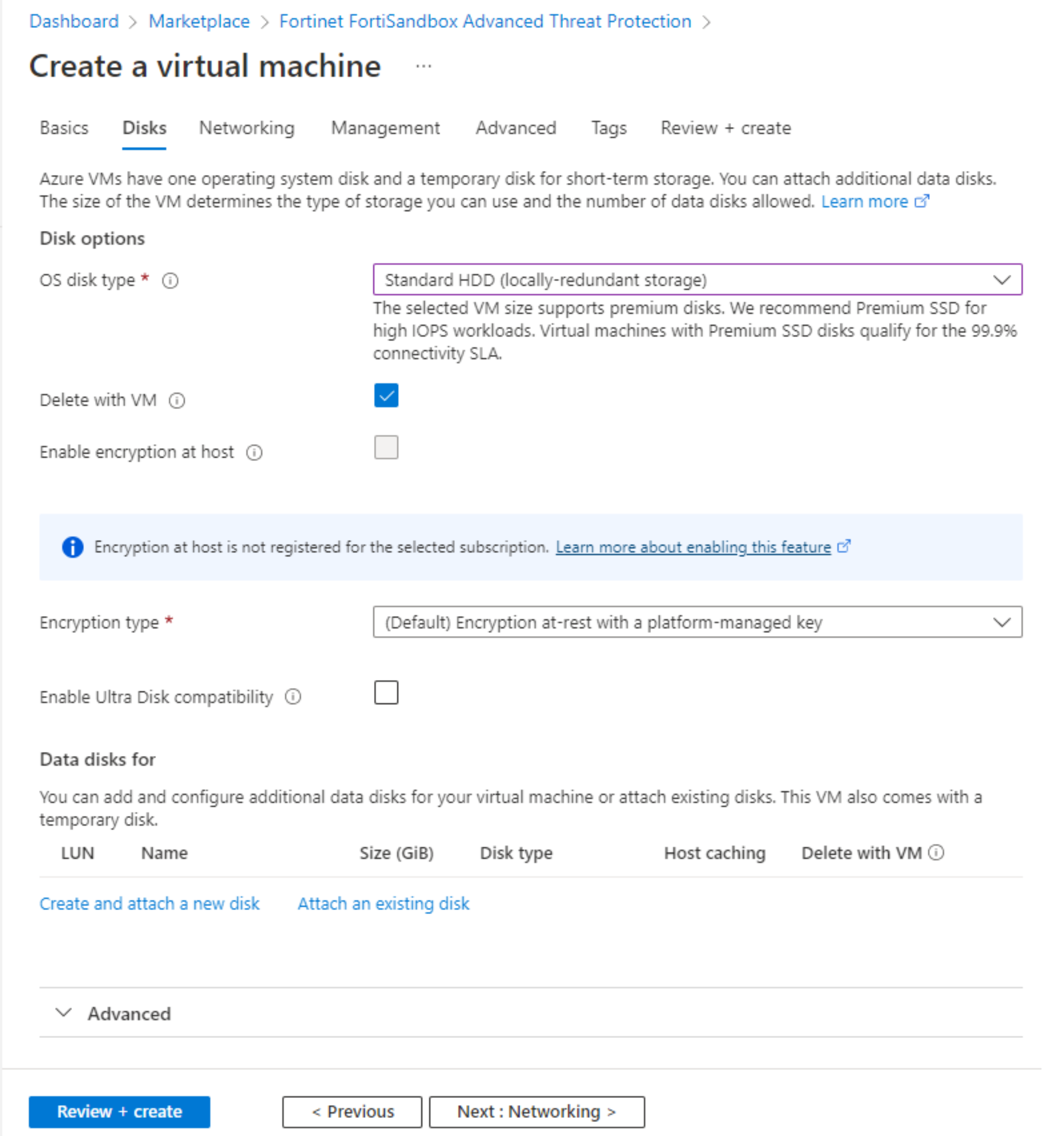
SSH public key source: Use existing key stored in Azure

Stored Keys: fsadevqa_key

4. Click the *Disks* tab to configure the disks.

OS disk type	Select the disk type depending on your needs.

	Note: This option is only available in version 4.4.3.
Data disk for	Select *Create and attach a new disk* or *Attach an existing disk*.



Dashboard > Marketplace > Fortinet FortiSandbox Advanced Threat Protection >

Create a virtual machine ...

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

Disk options

OS disk type * : Standard HDD (locally-redundant storage)

The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

Delete with VM ☑

Enable encryption at host □

Encryption at host is not registered for the selected subscription. Learn more about enabling this feature

Encryption type * : (Default) Encryption at-rest with a platform-managed key

Enable Ultra Disk compatibility □

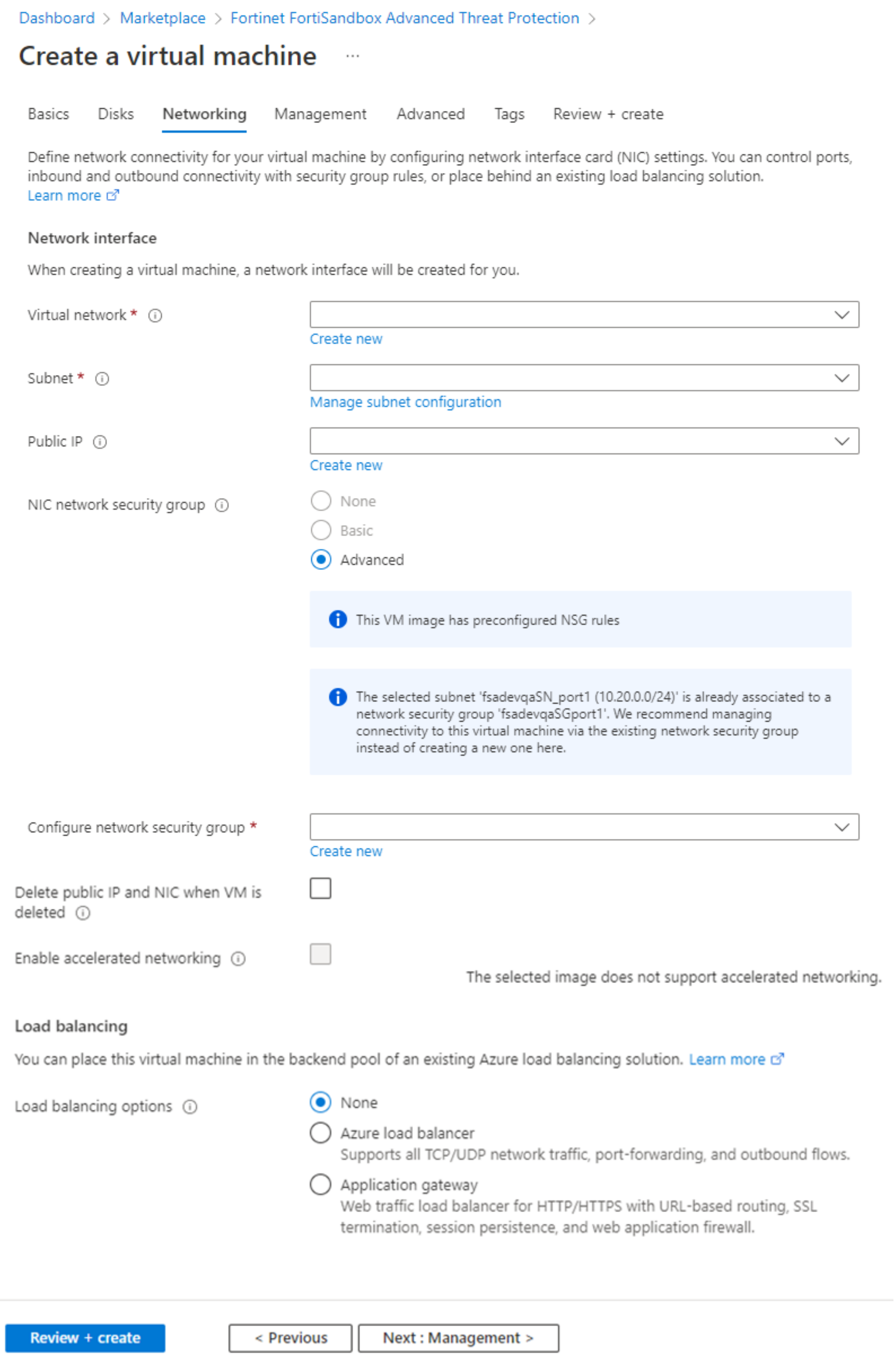
Data disks for

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

LUN	Name	Size (GiB)	Disk type	Host caching	Delete with VM

5. Click the *Network* tab to configure the network interface.

Virtual Network	Select the Virtual Network which you created for FortiSandbox.
Subnet	Select the subnet you created for FortiSandbox port1.
Public IP	Create a new for FortiSandbox port1, , or use an existing IP.
Configure network security group	Select the security group you created for FortiSandbox and allowed access to FortiSandbox port1.



Dashboard > Marketplace > Fortinet FortiSandbox Advanced Threat Protection >

Create a virtual machine ...

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

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

Network interface

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

Virtual network * ⓘ
Create new

Subnet * ⓘ
Manage subnet configuration

Public IP ⓘ
Create new

NIC network security group ⓘ
○ None
○ Basic
● Advanced

This VM image has preconfigured NSG rules

The selected subnet 'fsadevqaSN_port1 (10.20.0.0/24)' is already associated to a network security group 'fsadevqaSGport1'. We recommend managing connectivity to this virtual machine via the existing network security group instead of creating a new one here.

Configure network security group *
Create new

Delete public IP and NIC when VM is deleted ⓘ □

Enable accelerated networking ⓘ □
The selected image does not support accelerated networking.

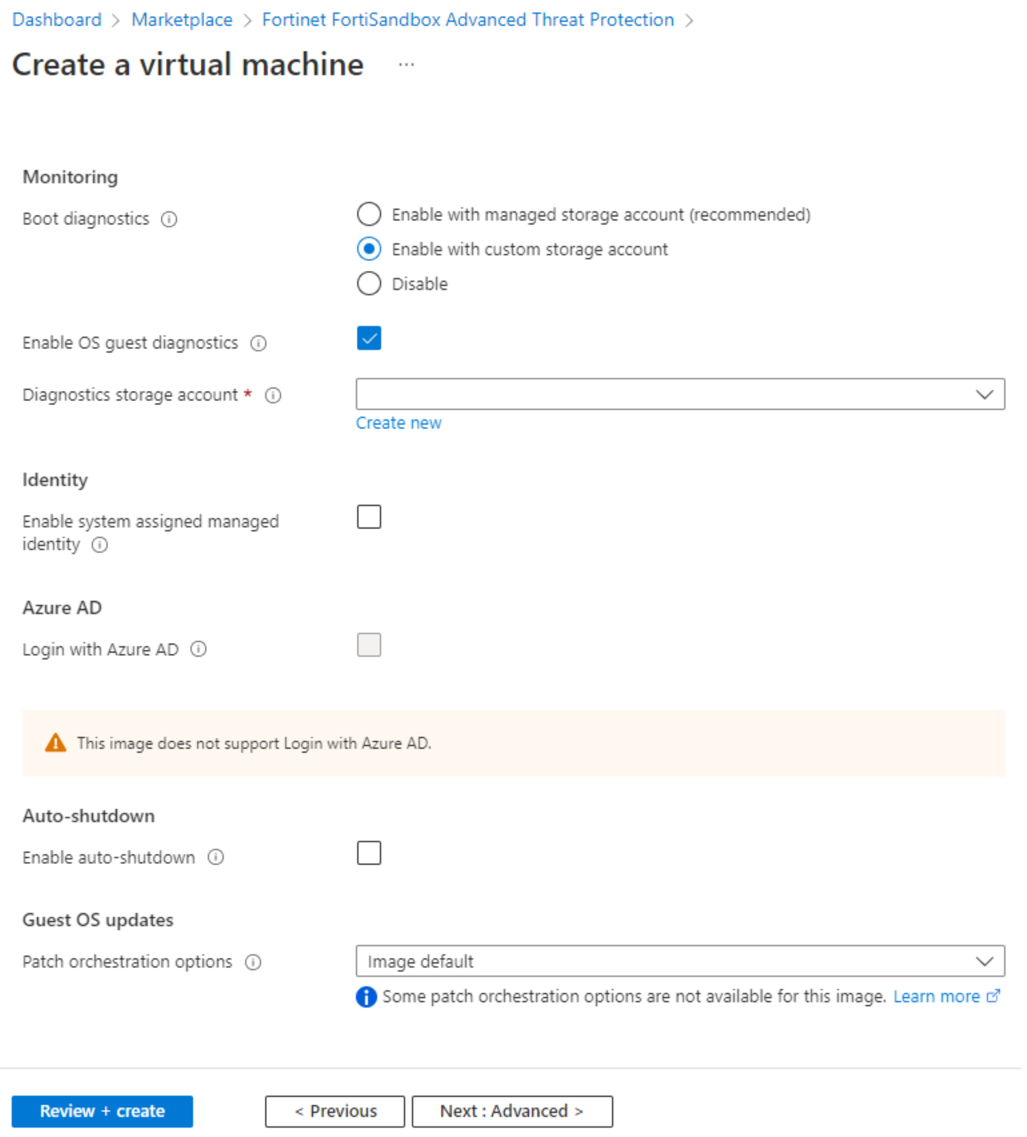
Load balancing

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

Load balancing options ⓘ
● None
○ Azure load balancer
Supports all TCP/UDP network traffic, port-forwarding, and outbound flows.
○ Application gateway
Web traffic load balancer for HTTP/HTTPS with URL-based routing, SSL termination, session persistence, and web application firewall.

6. It is high recommended you enable certain diagnostics settings. Click the *Management* tab to configure these diagnostics settings.

Boot diagnostics	Enable with custom storage account.
Enable OS guest diagnostics	Enable.
Diagnostics storage account	Choose the debug storage account.



Dashboard > Marketplace > Fortinet FortiSandbox Advanced Threat Protection >

Create a virtual machine ...

Monitoring

Boot diagnostics ⓘ
○ Enable with managed storage account (recommended)
● Enable with custom storage account
○ Disable

Enable OS guest diagnostics ⓘ ☑

Diagnostics storage account * ⓘ
Create new

Identity

Enable system assigned managed identity ⓘ □

Azure AD

Login with Azure AD ⓘ □

This image does not support Login with Azure AD.

Auto-shutdown

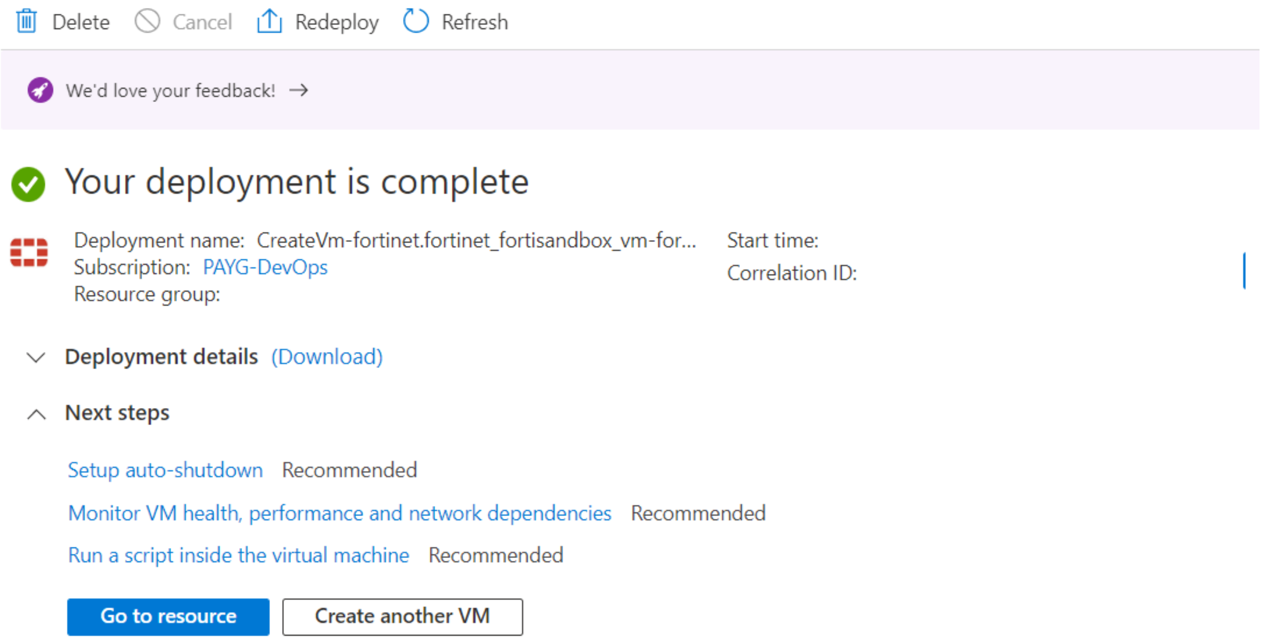
Enable auto-shutdown ⓘ □

Guest OS updates

Patch orchestration options ⓘ Image default
Some patch orchestration options are not available for this image. Learn more

7. Click *Review + Create*.
8. Wait for the setup wizard to validate your information and click *Create*.

9. When the VM is available, click *Go to resource* to go to the VM.

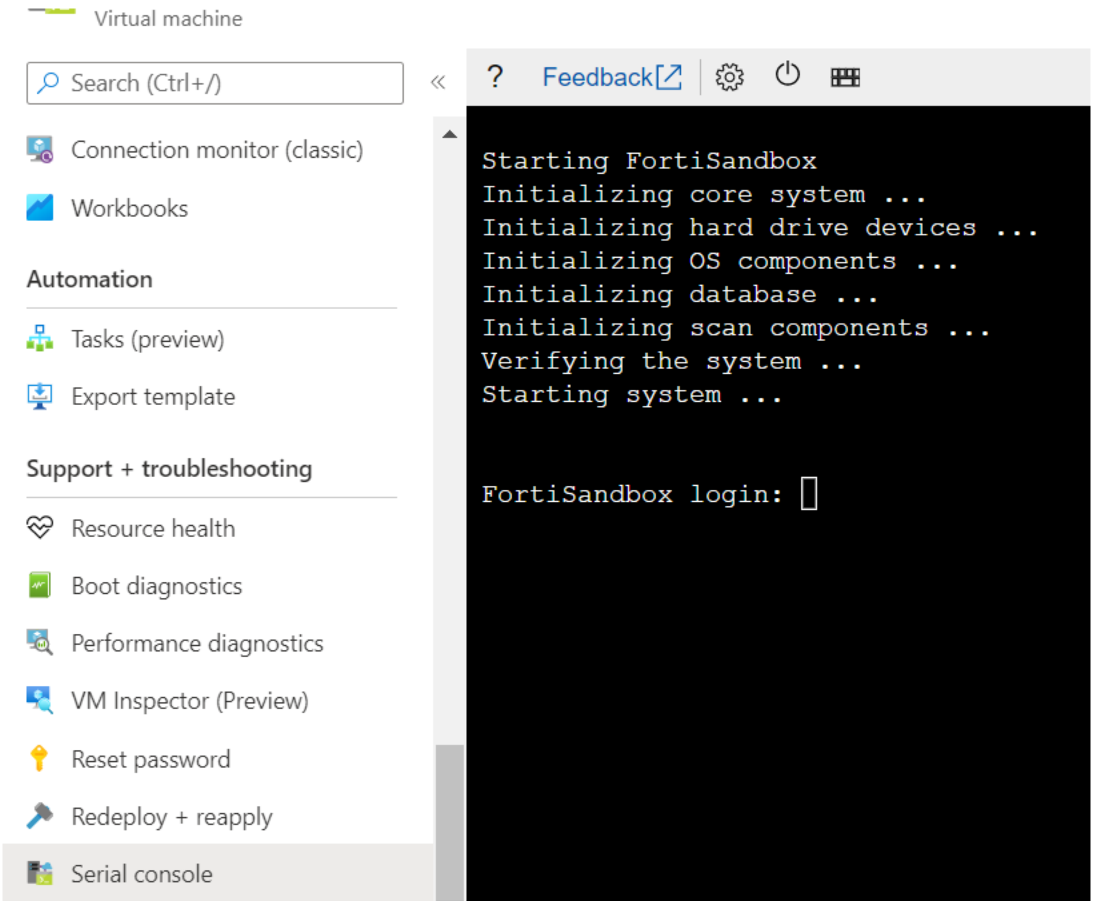


Your deployment is complete

Deployment name: CreateVm-fortinet.fortinet_fortisandbox_vm-for...
Subscription: PAYG-DevOps
Resource group:
Start time:
Correlation ID:

Setup auto-shutdown Recommended
Monitor VM health, performance and network dependencies Recommended
Run a script inside the virtual machine Recommended

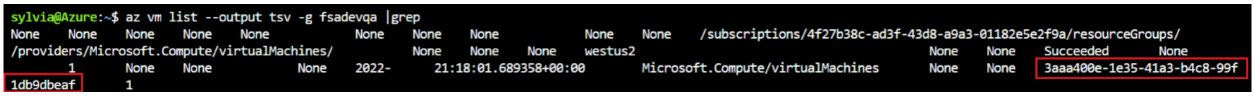
10. Use the Public IP address assigned to the FortiSandbox port1 via HTTPS once the FSA OS boots up completely via its console.



```
Starting FortiSandbox
Initializing core system ...
Initializing hard drive devices ...
Initializing OS components ...
Initializing database ...
Initializing scan components ...
Verifying the system ...
Starting system ...


FortiSandbox login:
```

11. Get the default admin password for the FortiSandbox VM using the Azure CLI command:
    ```
    az vm list --output tsv -g <resource group name> |grep <FortiSandbox-VM name>
    ```
    The VM-ID UUID is the default password for Admin access



```
sylvia@Azure:~$ az vm list --output tsv -g fsadevqa |grep
None    None    None    None    None          None    None    None          None    None    /subscriptions/4f27b38c-ad3f-43d8-a9a3-01182e5e2f9a/resourceGroups/
/providers/Microsoft.Compute/virtualMachines/         None    None    None    westus2                                 None    None    Succeeded       None
        1       None    None            None    2022-      21:18:01.689358+00:00        Microsoft.Compute/virtualMachines       None    None    3aaa400e-1e35-41a3-b4c8-99f
1db9dbeaf       1
```

12. Prepare FortiSandbox for scanning contents. See Import Azure settings into FortiSandbox on page 30.

To set up configuration and guest VM installation:

1. In the Azure portal of the new FortiSandbox, open the console via *Menu* > *Help* > *Serial console*.
2. Log in as FortiSandbox admin:
   - PAYG and Non-Nested BYOL: Use the VM ID for the password.
   - Nested BYOL: By default there is no password.
3. FortiSandbox will prompt you to create a new password.
4. Check that the IP of port1 and default gateway is set with the CLI `show`.
5. If the IP of port1 and default gateway are set, you can skip the next step.
6. Set up the private IP of port1 (such as `10.0.0.5`) and default gateway (such as `10.0.0.1`).
7. Log into the GUI.
8. Go to *Dashboard* > *Status* > *License*
   - For PAYG and Non-Nested BYOL, the unit type is *Azure*.

     FortiSandbox-Azure

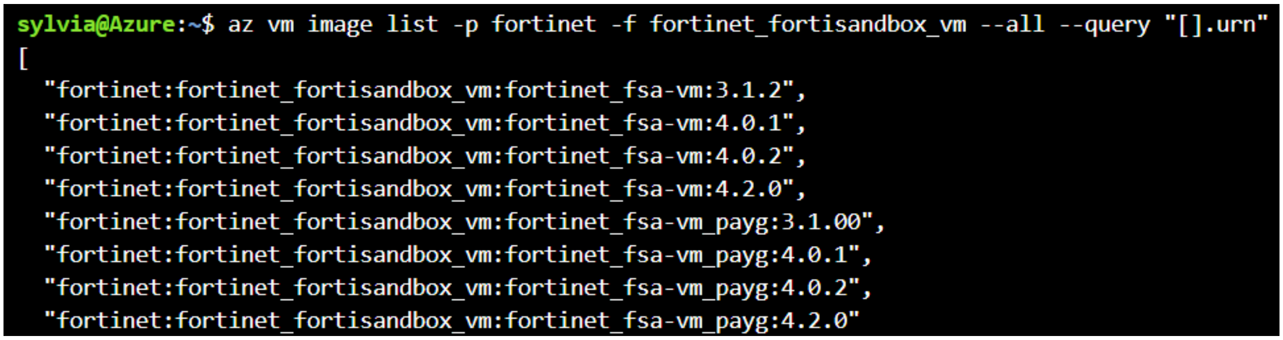
   - While for Nested BYOL, the unit should display *HyperV*.

     FortiSandbox-HYPERV

Deploy FortiSandbox instance on Azure using the CLI

To create the VM using the Azure CLI:

1. Since the Marketplace URN is subject to change without notice, you can get the latest FortiSandbox image URN with the following command:
   ```
   az vm image list -p fortinet -f fortinet_fortisandbox_vm --all --query "[].urn"
   ```



```
sylvia@Azure:~$ az vm image list -p fortinet -f fortinet_fortisandbox_vm --all --query "[].urn"
[
  "fortinet:fortinet_fortisandbox_vm:fortinet_fsa-vm:3.1.2",
  "fortinet:fortinet_fortisandbox_vm:fortinet_fsa-vm:4.0.1",
  "fortinet:fortinet_fortisandbox_vm:fortinet_fsa-vm:4.0.2",
  "fortinet:fortinet_fortisandbox_vm:fortinet_fsa-vm:4.2.0",
  "fortinet:fortinet_fortisandbox_vm:fortinet_fsa-vm_payg:3.1.00",
  "fortinet:fortinet_fortisandbox_vm:fortinet_fsa-vm_payg:4.0.1",
  "fortinet:fortinet_fortisandbox_vm:fortinet_fsa-vm_payg:4.0.2",
  "fortinet:fortinet_fortisandbox_vm:fortinet_fsa-vm_payg:4.2.0"
```

2. Create the Azure FortiSandbox with the Azure CLI from the Azure Marketplace with the network interfaces and data disk for the FortiSandbox you created.
   a. Create the Azure FortiSandbox BYOL.
      ```
      az vm create --resource-group [resource group name] --name [ FortiSandbox_BYOL_VM
           name] --image "fortinet:fortinet_fortisandbox_vm:fortinet_fsa-vm:4.2.0" --size
           [vm size] --nics [NIC for port1] [NIC for port2] [NIC for port3] [NIC for
           port4] --attach-data-disks [attach_data_disks_name] --location [location_of_
           resource_group_for_FSA] --boot-diagnostics-storage [boot_diagnostics_storage_
           container_name] --verbose
      ```
   b. Create the Azure FortiSandbox PAYG.
      ```
      az vm create --resource-group [resource group name] --name [ FortiSandbox_PAYG_VM
           name] --image "fortinet:fortinet_fortisandbox_vm:fortinet_fsa-vm_payg:4.2.0" --
           size [vm size] --nics [NIC for port1] [NIC for port2] [NIC for port3] [NIC for
           port4] --attach-data-disks [attach_data_disks_name] --location [location_of_
           resource_group_for_FSA] --boot-diagnostics-storage [boot_diagnostics_storage_
           container_name] --verbose
      ```
3. Get the default admin password for the FortiSandbox VM using the following Azure CLI command:
   ```
   az vm list --output tsv -g <resource group name> |grep <FortiSandbox-VM name>
   ```
   The VM-ID UUID is the default password for Admin access.
4. Prepare FortiSandbox for scanning contents. See Import Azure settings into FortiSandbox on page 30.

Prepare FortiSandbox for scanning contents

To prepare the FortiSandbox instance for scannning:

1. Upload the license file on page 28
   Upload the license file using the GUI. After the file is uploaded, verify the rating and tracer engines were downloaded and installed.
2. Import Azure settings into FortiSandbox on page 30
   You can use either the Account Authorization or Service Principal methods to import the settings in FortiSandbox 3.2.0 or later.
3. (Optional) Create an App registration on page 35
   Creating an App registration is required if the FortiSandbox instance is using the Service Principal method to communicate with the Azure portal.

Upload the license file

Before using the FortiSandbox VM you must enter the license file that you downloaded from the Customer Service & Support portal upon registration. After the license has been validated, verify the rating and tracer engines were downloaded and installed.

To upload the license file:

1. Log in to the FortiSandbox VM GUI and locate the *System Information* widget on the dashboard.
2. In the *VM License* field, select *Upload License*. The *VM License Upload* page opens.
3. Select *Browse*, locate the VM license file (`.lic`) on your computer, then select *OK* to upload the license file.
   A reboot message will be shown, then the FortiSandbox system will reboot and load the license file.
4. Refresh your browser and log back in to the FortiSandbox(username *admin*, no password).
   The VM registration status appears as valid in the *System Information* widget once the license has been validated.

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

If the IP address in the license file and the IP address configured in the FortiSandbox do not match, you will receive an error message when you log back into the VM.
If this occurs, you will need to change the IP address in the Customer Service & Support portal to match the management IP and re-download the license file.

Verifying the rating and tracer engines

Once the FortiSandbox VM license has been validated, the rating and tracer engines will download automatically from FortiGuard Distribution Network (FDN) and install within an hour. If your FortiSandbox is not able to reach FDN, log on to support site to download the engines and upload them manually to the system.

To verify the engines downloaded:

1. Go to *System* > *FortiGuard*.
2. In the *Sandbox Rating Engine* and *Sandbox Tracer Engine* rows:
   - Check the *Last Update Time*.
   - Verify the *Last Check Status* is *Successful*.

To download the rating and tracer engines from the Customer Support site:

This task is only required when the engines do not download and install automatically.

1. Log in to FortiCloud.
2. In the banner, click *Support* > *Service Updates*.
3. In the left navigation pane, click FortiSandbox.
4. In the *Engine* column, click the link to download the file.

To upload the engine file:

This task is only required when the engines do not download and install automatically.

1. Go to *System* > *FortiGuard*.
2. Next to *Upload Package File* click *Select File*.
3. Navigate to file location on your device and click *Open*.
4. Click *Submit*.

Import Azure settings into FortiSandbox

In FortiSandbox v3.2.0 and higher, you can import Azure settings using the *Account Authentication* method or the *Service Principal* method. The Azure settings are required from Microsoft to log into the Azure portal, control the Virtual Machines and communication between network interfaces.

In FortiSandbox Azure, there are features require operations on the Azure portal. These include:

- HA failover with cluster IP transferred to new Primary.
- Import/install/activate/delete/startup/shutdown/communicate Customized VMs

Import using Account Authentication

To import Azure account authentication:

1. Go to the FortiSandbox GUI.
2. Click *System* > *Azure Config*.

The Azure email account should be the *Owner* of the resource group of FortiSandbox.

Account Type	Select *Microsoft Azure account email* which means use account authentication to import.
Microsoft Azure account email	Your user ID.
Microsoft Azure account password	Your user password.
Location	Select the location you used to set up the resource group.
Subscription ID	Your subscription ID.
Resource group	The resource group. The User ID, password, location, Subscription ID and Resource group will be used to log into the Azure portal.
Storage account	Storage account name. This name will be used to import/install/activate/delete/startup/shutdown/communicate Customized VMs.
Storage account access key	Storage account access key. This access key will be used to import/install/activate/delete/startup/shutdown/communicate Customized VMs.

Monitor storage account	Monitor account name. This name will be used to import/install/activate/delete/startup/shutdown/communicate Customized VMs.
Monitor account access key	Monitor account access key. This access key will be used to import/install/activate/delete/startup/shutdown/communicate Customized VMs.
Network security group	The security group you created for FortiSandbox port2. This port2 in FortiSandbox Azure is used to communicate with Virtual Machines in FortiSandbox. The network security group will be used to import/install/activate/delete/startup/shutdown/communicate Customized VMs, and HA Cluster failover.
Virtual Network	Name of the virtual network you crated. The Virtual Network name will be used to import/install/activate/delete/startup/shutdown/communicate Customized VMs, and HA Cluster failover.
Subnet	The subnet you created for the FortiSandbox port2 interface. This port2 in FortiSandbox Azure is used to communicate with Virtual Machines in FortiSandbox. The subnet name will be used to import/install/activate/delete/startup/shutdown/communicate Customized VMs, and HA Cluster failover.
VM type	The VM type of custom VM clone(s). • Minimum: *Standard_B2ms* • Recommended: *Standard_B2ms*
Allow Hot-Standby VM	After *Allow Hot-Standby VM* is enabled, FortiSandbox will perform VM initialization again to apply changes to existing custom VM clones or prepare new clone(s). See Appendix B - Reduce scan time in custom Windows VM on page 56
Disk Type	The disk storage type of the new installed custom VM. Disk Types: • Standard_LRS • Premium_LRS • StandardSSD_LRS After the custom VM is created, please go to Azure patrol to check the *Disks >Storage type* of the VM.
Idle time before deallocate custom VM instance in minutes	FortiSandbox will deallocate the custom VM instance after it remains idle from job scan until the idle timeout value (minutes). By clicking *Enabled*, an idle time must be entered, otherwise, *0* means disabled. :

> If the Idle time is enabled, the *Allow Hot-Standby VM* must be disabled.

3. Click *Test Connection* to verify the connection is accessible and authentication is valid.
4. Click *Submit*.

Import using Service Principal

To import the Azure settings using Service Principal, get the client and tenant IDs from the Azure portal and then enter them into FortiSandbox using the GUI.

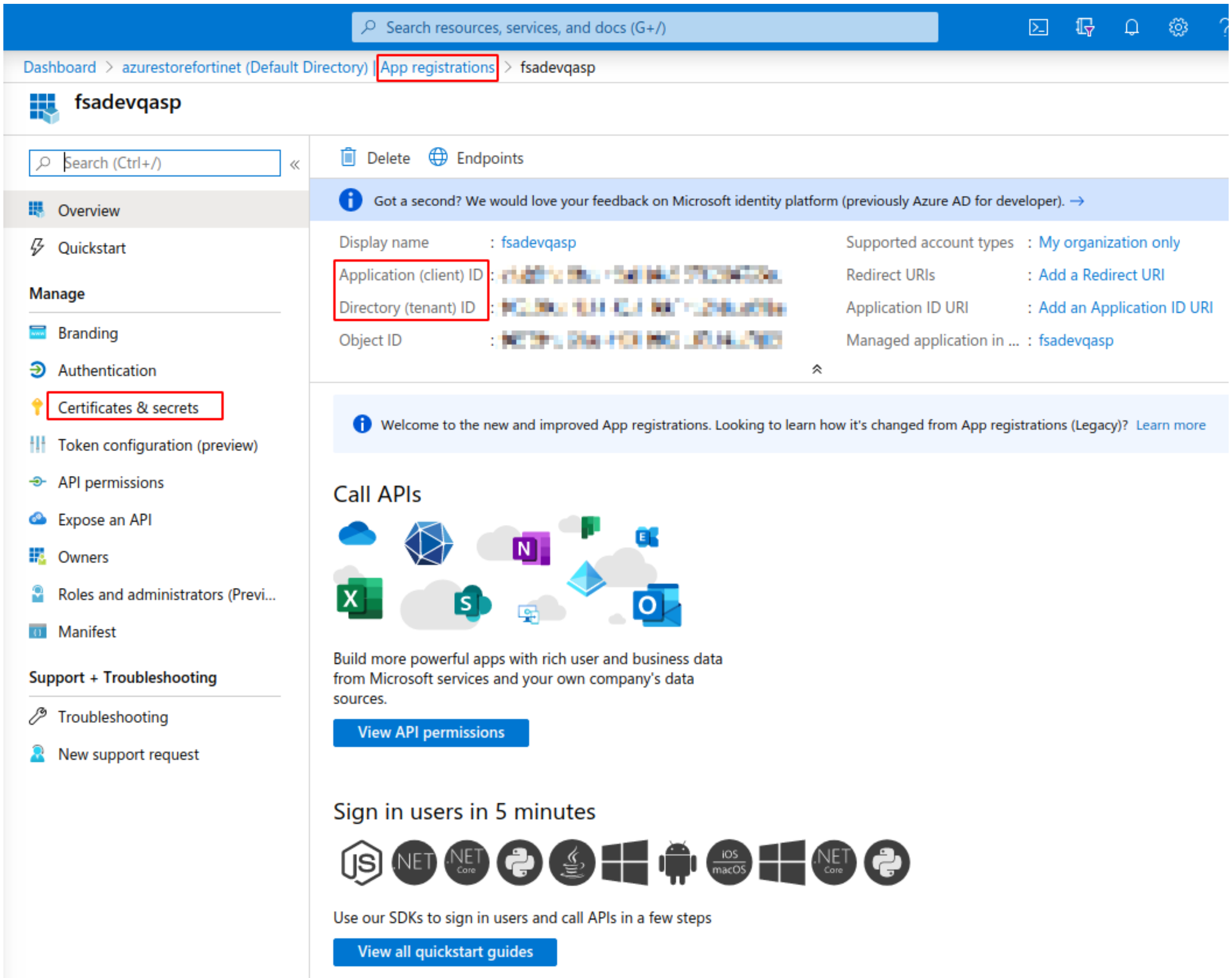
Requirements:

- Create an App registration in the Azure portal

To get client and tenant IDs in the Azure portal:

1. In the Azure portal, go to *Azure Active Directory* > *App registrations* and locate the service principal information in the application you created.
   For information, see (Optional) Create an App registration on page 35.
2. Go to *Manage* > *Certificates & Secrets*. The service principal information is located in the *Application (client) ID* and

Directory (tenant) ID fields.



Search resources, services, and docs (G+/)
Dashboard > azurestorefortinet (Default Directory) > App registrations > fsadevqasp
fsadevqasp
Search (Ctrl+/)
Overview
Quickstart
Manage
Branding
Authentication
Certificates & secrets
Token configuration (preview)
API permissions
Expose an API
Owners
Roles and administrators (Previ...
Manifest
Support + Troubleshooting
Troubleshooting
New support request
Delete
Endpoints
Call APIs
View API permissions
Sign in users in 5 minutes
View all quickstart guides

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Display name	: fsadevqasp	Supported account types	: My organization only
Application (client) ID	: [redacted]	Redirect URIs	: Add a Redirect URI
Directory (tenant) ID	: [redacted]	Application ID URI	: Add an Application ID URI
Object ID	: [redacted]	Managed application in ...	: fsadevqasp

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

Use our SDKs to sign in users and call APIs in a few steps

To import Azure service principal in FortiSandbox:

1. In FortiSandbox, go to *System* > *Azure Config*.
2. In FortiSandbox, enter the following Azure configuration settings and then click *Submit*.

Account Type	Select *Client ID*, which means use service Principal to import.
Client id	Enter the *Application (client) ID* from the Azure portal.
Client Secret	Enter the client secret.
Location	The location you used to set up the resource group.
Tenant id	Enter the *Directory (tenant) ID* from the Azure portal.
Subscription ID	Your subscription ID.
Resource group	Resource group.

	The *Client ID*, *Client Secret*, *Location*, *Subscription ID* and *Resource group* will be used to log into the Azure portal.
Storage account	Storage account name. This name will be used to import/install/activate/delete/startup/shutdown/communicate Customized VMs.
Storage account access key	Storage account access key. This key will be used to import/install/activate/delete/startup/shutdown/communicate Customized VMs.
Monitor storage account	Monitor account name. This account will be used to import/install/activate/delete/startup/shutdown/communicate Customized VMs.
Monitor account access key	Monitor account access key. This key will be used to import/install/activate/delete/startup/shutdown/communicate Customized VMs.
Network security group	The security group you created for FortiSandbox port2. This port2 in FortiSandbox Azure is used to communicate with Virtual Machines in FortiSandbox. The network security group will be used to import/install/activate/delete/startup/shutdown/communicate Customized VMs, and HA Cluster failover.
Virtual network	Name of the virtual network you created. Virtual Network name will be used to import/install/activate/delete/startup/shutdown/communicate Customized VMs, and HA Cluster failover.
Subnet	Use the subnet created for the local Windows or Linux VM communication (port2) if one exists. Otherwise, select the management subnet. This port2 in FortiSandbox Azure is used to communicate with Virtual Machines in FortiSandbox. Subnet name will be used to import/install/activate/delete/startup/shutdown/communicate Customized VMs, and HA Cluster failover.
VM Type	The VM type of custom VM clone(s). • Minimum: *Standard_B2ms* • Recommended: *Standard_B2ms*
Allow Hot-Standby VM	After *Allow Hot-Standby VM* is enabled, FortiSandbox will perform VM initialization again to apply changes to existing custom VM clones or prepare new clone(s). See Appendix B - Reduce scan time in custom Windows VM on page 56
Disk Type	The disk storage type of the new installed custom VM. Disk Types:

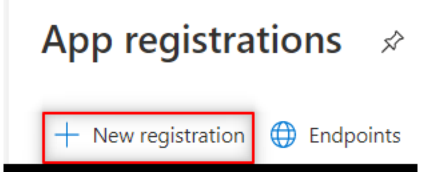
	- Standard_LRS - Premium_LRS - StandardSSD_LRS After the custom VM is created, please go to Azure patrol to check the *Disks >Storage type* of the VM.
Idle time before deallocate custom VM instance in minutes	FortiSandbox will deallocate the custom VM instance after it remains idle from job scan until the idle timeout value (minutes). By clicking *Enabled*, an idle time must be entered, otherwise, *0* means disabled. If the Idle time is enabled, the *Allow Hot-Standby VM* must be disabled.

(Optional) Create an App registration

This task is only required when the FortiSandbox instance is using the Service Principle method to communicate with the Azure platform.

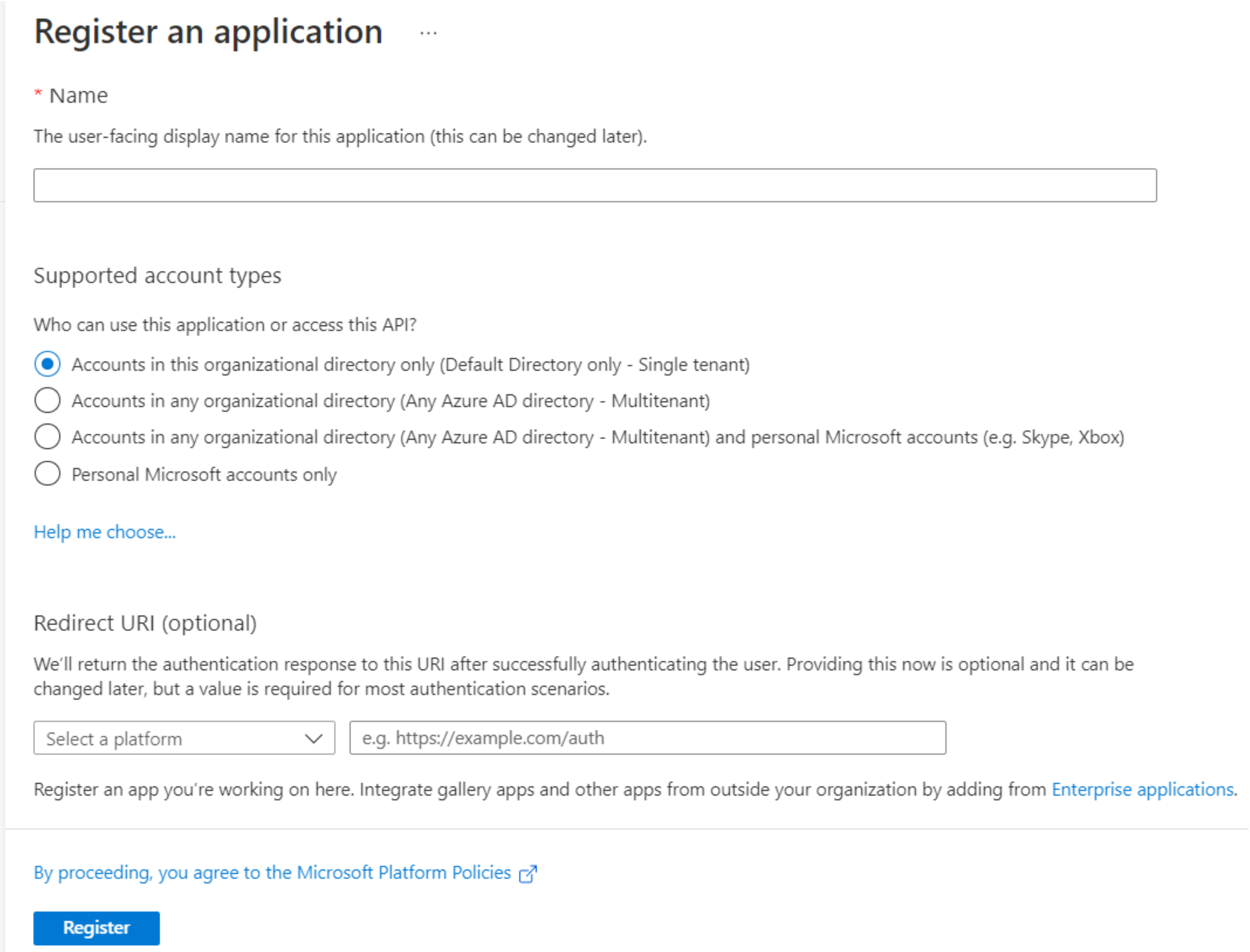
To create an App registration:

1. Log in to the Azure portal.
2. Go to *Azure Active Directory* > *App registrations* and click *New registration*.



3. Register a new application.

Name	Enter the application display name.
Supported account types	Select *Accounts in this organizational directory only (Default Directory only – Single tenant)*.
Redirect URI	This section is optional.



Register an application ···

* Name

The user-facing display name for this application (this can be changed later).

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Default Directory only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

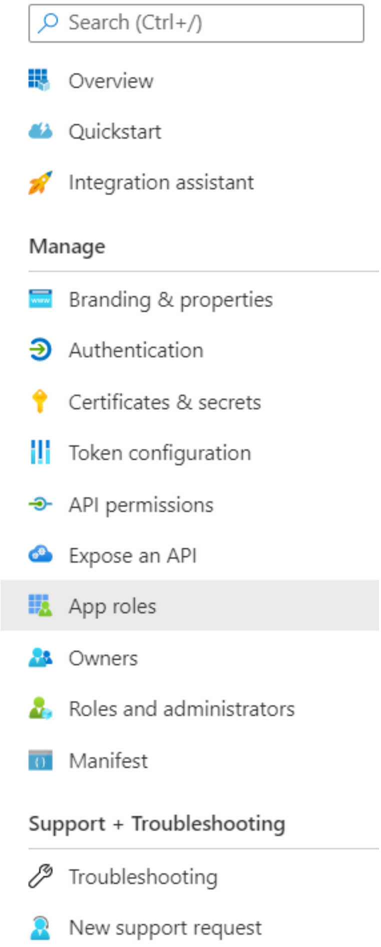
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform | e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

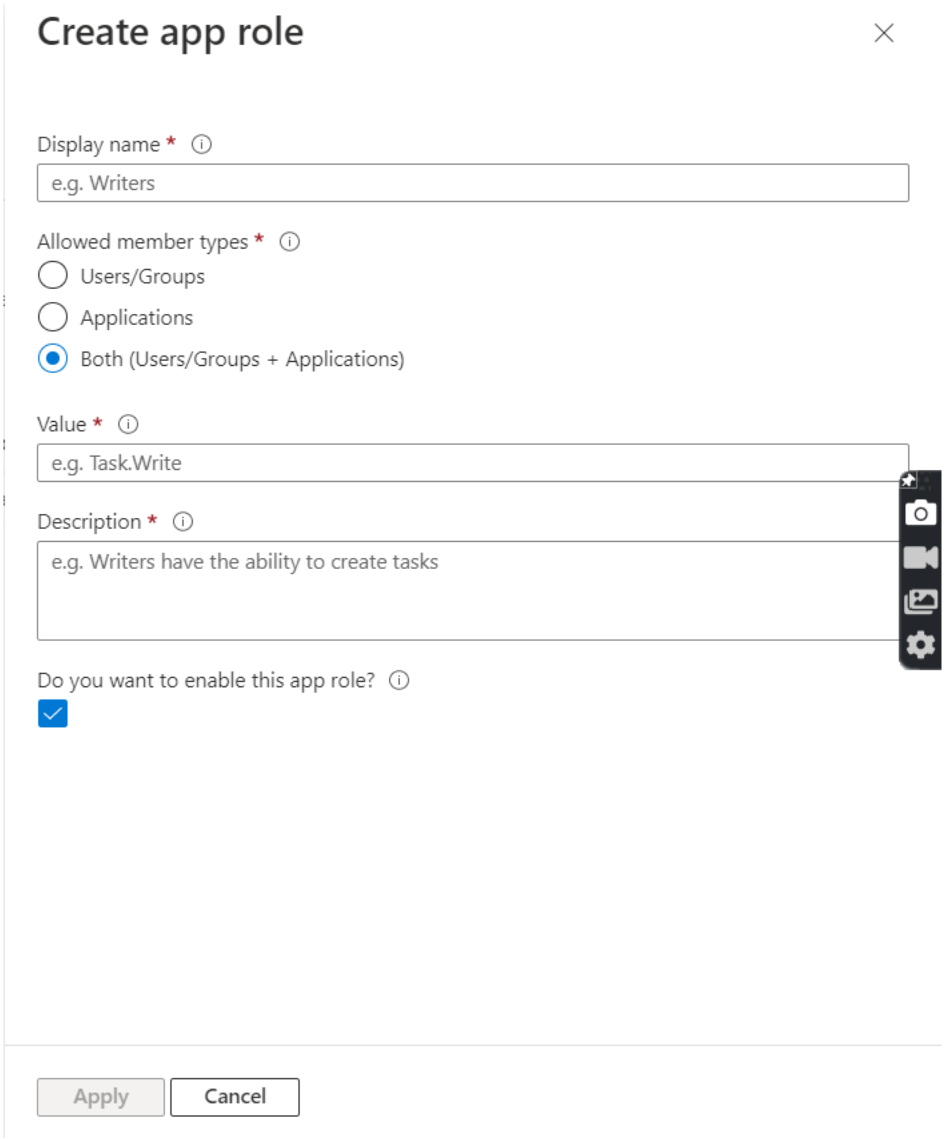
By proceeding, you agree to the Microsoft Platform Policies

4. Go to *Manage* > *App Roles*.



5. Click *Create app role* and configure the following settings:

Display name	Enter the display name for the app role.
Allowed member types	Select *Both (Users/Groups + Applications)*.



Create app role

Display name * ⓘ

e.g. Writers

Allowed member types * ⓘ

○ Users/Groups

○ Applications

● Both (Users/Groups + Applications)

Value * ⓘ

e.g. Task.Write

Description * ⓘ

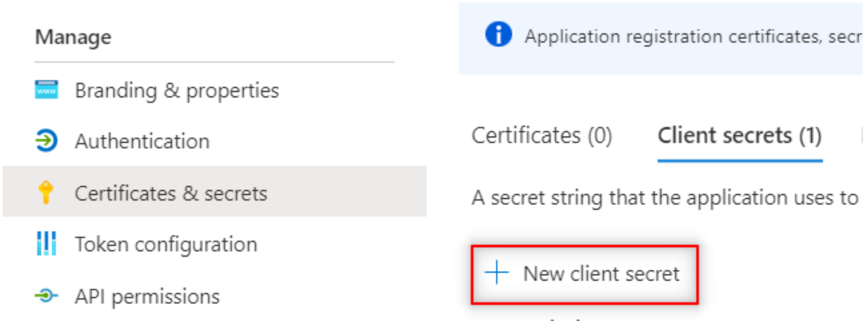
e.g. Writers have the ability to create tasks

Do you want to enable this app role? ⓘ

☑

Apply   Cancel

6. Go to *Manage* > *Certificates & secrets* and click create a *New client secret*.



7. Go to *API permissions*. As a minimum requirement, the following items should be granted API permissions.
   For items:

Azure Service Management	This is for managing deployments, hosted services, and storage accounts.
Azure Storage	This is for programmatic access to the Blob, Queue, Table, and File services in Azure or in the development environment via the storage emulator.

a. Click *Add a permission*.
b. Click the item name.
c. Click the *Delegated permission* tab.
d. Select `user_impersonation`.
e. Click *Add permissions*.

For Microsoft Graph:

Files	*ReadWrite* This allows FortiSandbox to read, create, update, and delete the signed-in user's files.
User	*Read* This allows FortiSandbox to read the signed-in user's information.

a. Click *Add a permission*.
b. Click the item name.
c. Click the *Delegated permission* tab.
d. Select the permissions.
e. Click *Add permissions*.

Set up the local VM

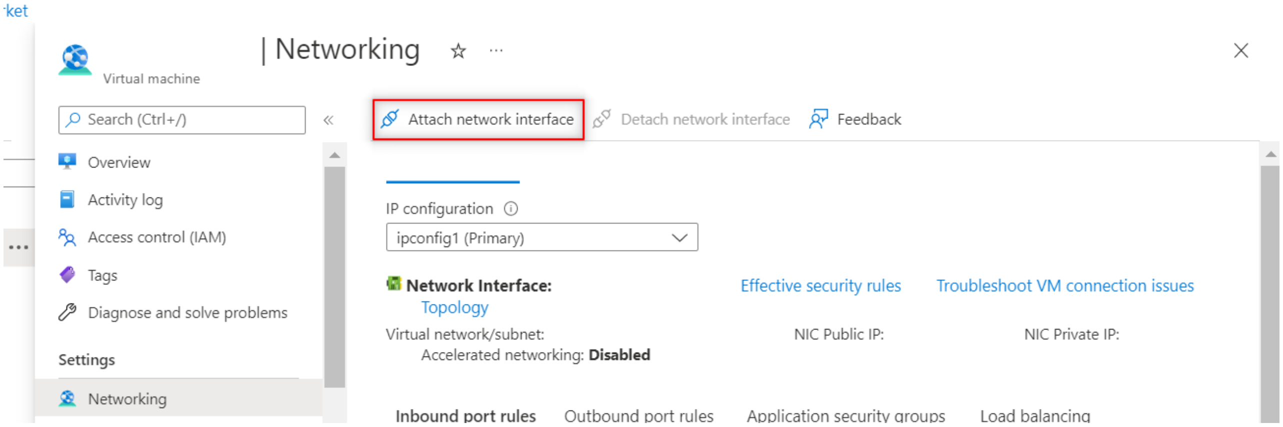
To create a custom Windows VM for Azure, follow steps in Custom VM Guide which can be found in the Fortinet Developer Network or is available on request from Customer Support.

To prepare the network interface for custom VM:

1. Shutdown the FortiSandbox VM instance from the Azure Portal.
2. Create interfaces fro port2 and port3 to install the VMs. For information, see *To create a network interface in Azure* in Create network interfaces on page 17.

PAYG and non-nested BYOL	Use port2 to communicate with local Windows or Linux clones.
Nested BYOL	Two interfaces are required: • Interface 2: port2 • Interface 3: port3

3. Attach this network interface to FortiSandbox VM instance as FSA Port2.



IP configuration ⓘ ipconfig1 (Primary)

Network Interface:

Virtual network/subnet:

Accelerated networking: **Disabled**

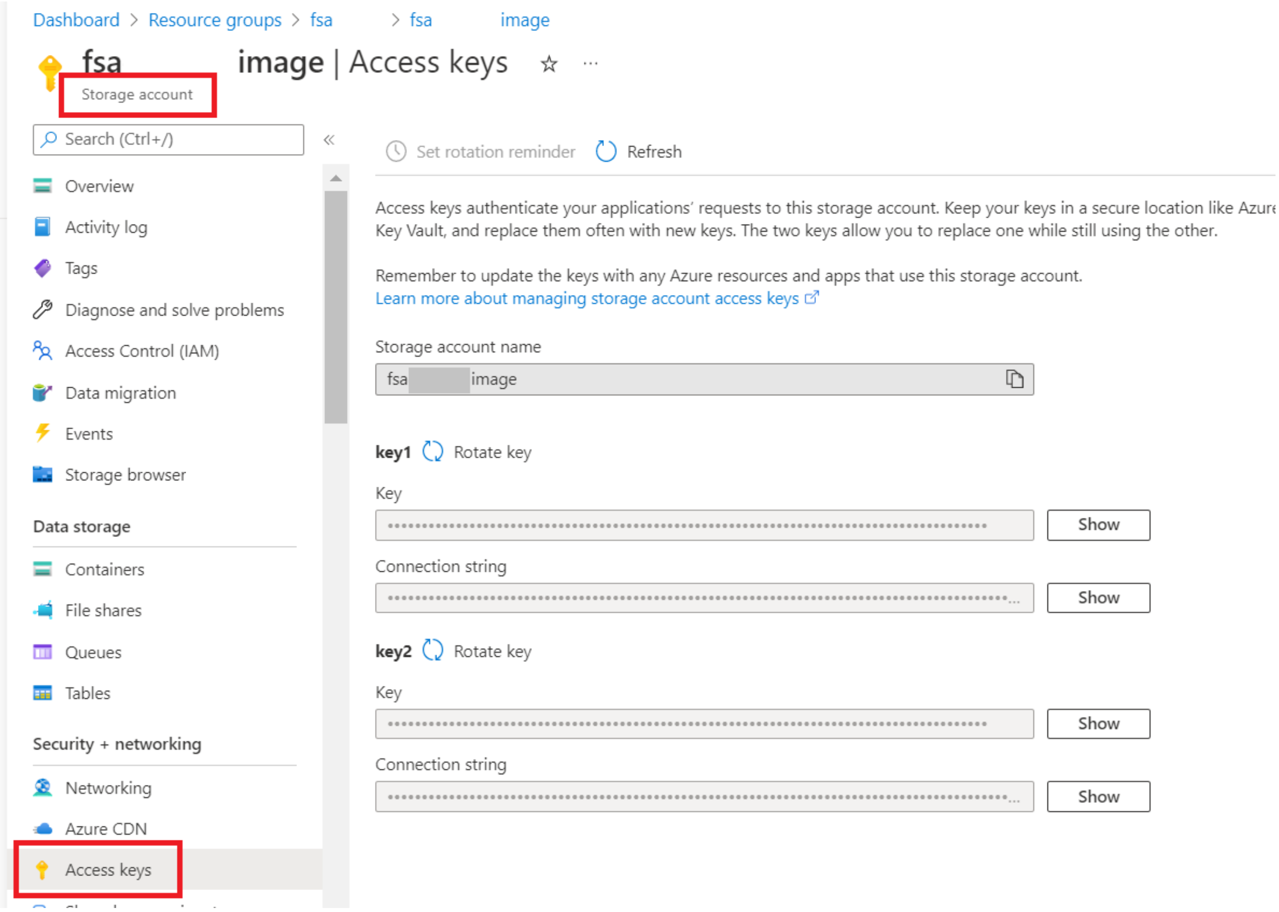
NIC Public IP:

NIC Private IP:

4. Start the FortiSandbox VM instance from Azure Portal
5. On the FortiSandbox GUI, go to *System* > *Interfaces* to verify that the network interface is attached.

To prepare the environment for installing the custom VM:

1. Check your Azure Config for the FortiSandbox firmware image storage account.
2. Go to *Resource group* > *Storage account* > *Access keys* to find your blob key.



Access keys authenticate your applications' requests to this storage account. Keep your keys in a secure location like Azure Key Vault, and replace them often with new keys. The two keys allow you to replace one while still using the other.

Remember to update the keys with any Azure resources and apps that use this storage account.
Learn more about managing storage account access keys

Storage account name: fsa[redacted]image

Key: ••

Connection string: ••...

Key: ••

Connection string: ••...

3. Create a storage blob for the custom VM image.
   a. Create a blob container (with anonymous read access) in this storage account.
   b. Upload the activated prebuilt custom VM image VHD to this blob container.

To install a custom VM using CLI:

1. Go to the FortiSandbox firmware CLI.
2. Import the VHD image with the CLI:
   - For PAYG and non-nested BYOL use `azure-vm-customized`
   - For nested BYOL use `vm-customized`

- From v3.2.0, FortiSandbox Azure supports installing custom VMs from Azure snapshot and Azure disks.
- Use a meaningful custom VM name and keep the same name as `VM_image_name`.
- Do not use:
  - Special characters in the name.
  - Reserved FortiSandbox VM names starting with WIN7, WIN8, or WIN10.
  - The `set admin-port` command to set port2 as the administrative port.

To install custom VM from a blob for the Azure PAYG and non-nested BYOL:

1. Install the Azure custom VM with the CLI command: `azure-vm-customized`
2. Install the VM from a blob as the default type.

```
azure-vm-customized -cn -tblob -f[blob container name] -b[VM_image_name.vhd] -vo[OS
type] -vn[VM name]
```

To install custom VM from disk for the Azure PAYG and non-nested BYOL:

1. Install the Azure custom VM with the CLI command: `azure-vm-customized`
2. Verify that your disk is under the same resource group as FortiSandbox and related resources.
3. Install the VM from disk with the `-t` option.

```
azure-vm-customized -cn -tdisk -b[VM_image_disk_name] -vo[OS type] -vn[VM name]
```

To install the Azure nested BYOL Guest VM:

To install the firmware license, the IP in the license must be the same as the Port1’s private IP you set up in the console. After the license is installed, please wait a couple of minutes for the engine to install. By default, the engines will be installed automatically. If Port1’s connection to the FDN server is not available, the rating and tracer engines should be installed manually.

To support the VM, you will need to set up two more networks: port2 and port3. You can use the default IPs.

To install the Guest VM:

- Please follow the instructions in, *VM Settings* in the *FortiSandbox Administration Guide*.

If port1’s connection to Fortinet’s image server is not available, the image should be installed with the CLI command: `fw-upgrade`

To install the Guest VM in air-gapped mode:

The VM cannot be activated online If FortiSandbox is in air-gapped mode. To activate the VM, do the following:

1. Go to *Log & Report* > *Events* > *VM Event*.
2. Search for the failure of activation with an installation ID log.
3. Call the Microsoft Activation Center to get the confirmation ID.
4. Use the CLI to add the confirmation ID:
   ```
   confirm-id -a -k<windows/office key> -c<confirmation ID> -n<VM name>
   ```

The re-initialization of the VM will start automatically. Please refer to Hyper-V Admin Guide for other operations.

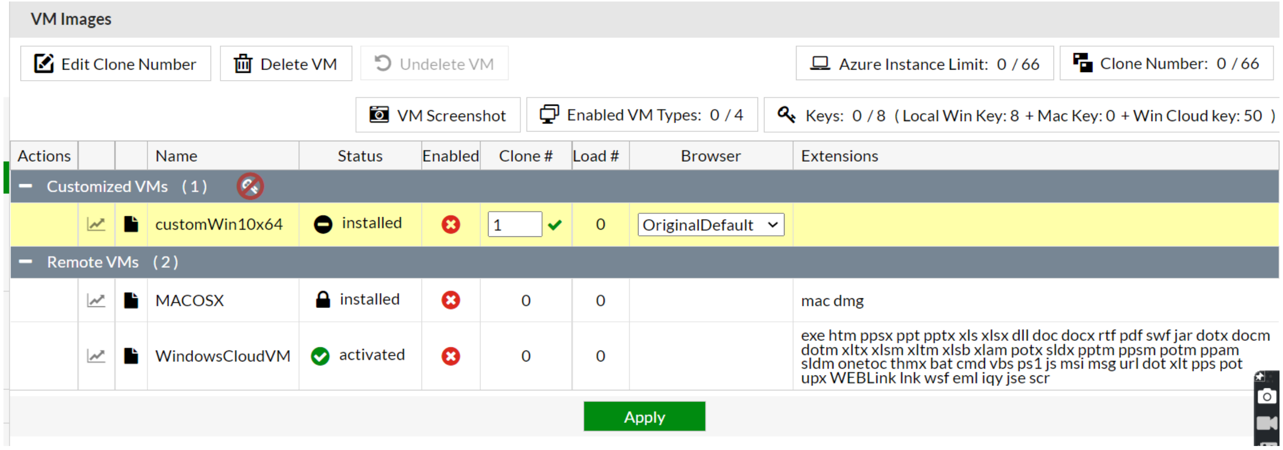
For PAYG and non-nested BYOL: The customized VMs use `vhd` file.

For nested BYOL: The customized VMs use `vdi` file. They are in a different format.

Test FortiSandbox instance with a file scan:

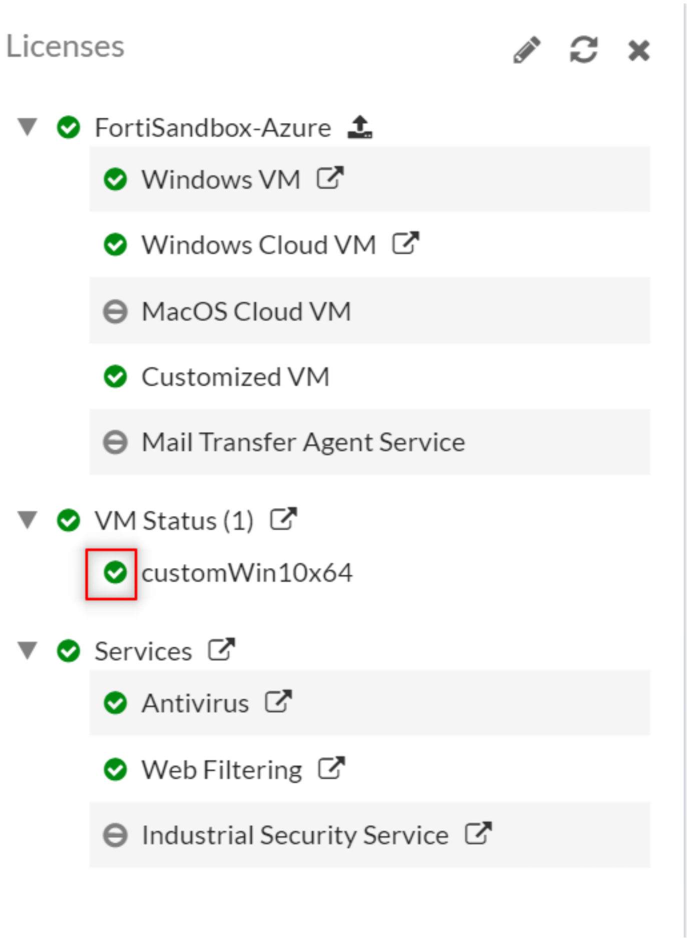
To verify the configuration is successful, perform an on-demand file scan with a Windows VM clone.

1. On the FortiSandbox GUI, go to *Scan Policy and Object* > *VM Settings* and change *Clone #* to `1`. Expand the clone number after vminit is completed.



Actions			Name	Status	Enabled	Clone #	Load #	Browser	Extensions
Customized VMs (1)									
			customWin10x64	installed	☒	1 ✓	0	OriginalDefault	
Remote VMs (2)									
			MACOSX	installed	☒	0	0		mac dmg
			WindowsCloudVM	✓ activated	☒	0	0		exe htm ppsx ppt pptx xls xlsx dll doc docx rtf pdf swf jar dotx docm dotm xltx xlsm xltm xlsb xlam potx sldx pptm ppsm potm ppam sldm onetoc thmx bat cmd vbs ps1 js msi msg url dot xlt pps pot upx WEBLink lnk wsf eml iqy jse scr

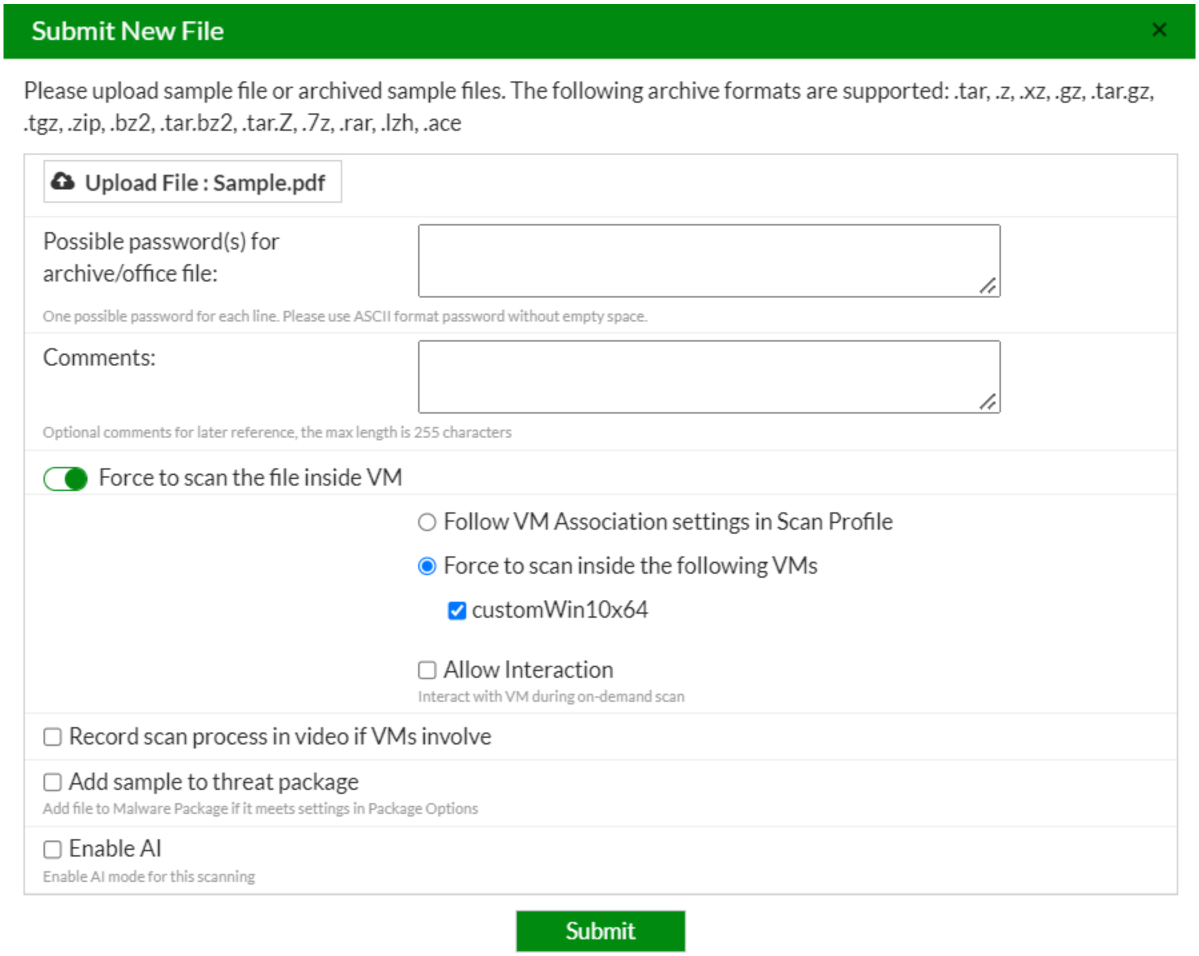
2. In a new CLI window, check the VM clone initialization using the command: `diagnose-debug vminit`
3. After vminit is done, on the FortiSandbox GUI, go to the *Dashboard* to verify there is a green checkmark beside *Custom VM*.



Licenses

- ✓ FortiSandbox-Azure
  - ✓ Windows VM
  - ✓ Windows Cloud VM
  - ⊖ MacOS Cloud VM
  - ✓ Customized VM
  - ⊖ Mail Transfer Agent Service
- ✓ VM Status (1)
  - ✓ customWin10x64
- ✓ Services
  - ✓ Antivirus
  - ✓ Web Filtering
  - ⊖ Industrial Security Service

4. To associate file extensions to the custom VM, go to *Scan Policy and Object*> *Scan Profile* and click the *VM Association* tab.
5. Test the installation:
   a. Go to *Scan Job* > *File On-Demand* > *Submit File*.
   b. Select the file and click *Submit*. For example, select *Sample.pdf*. If the file you send to FortiSandbox is not harmful, the rating is *Clean*.



Submit New File

Please upload sample file or archived sample files. The following archive formats are supported: .tar, .z, .xz, .gz, .tar.gz, .tgz, .zip, .bz2, .tar.bz2, .tar.Z, .7z, .rar, .lzh, .ace

Upload File : Sample.pdf

Possible password(s) for archive/office file:

One possible password for each line. Please use ASCII format password without empty space.

Comments:

Optional comments for later reference, the max length is 255 characters

Force to scan the file inside VM

○ Follow VM Association settings in Scan Profile

● Force to scan inside the following VMs

☑ customWin10x64

□ Allow Interaction

Interact with VM during on-demand scan

□ Record scan process in video if VMs involve

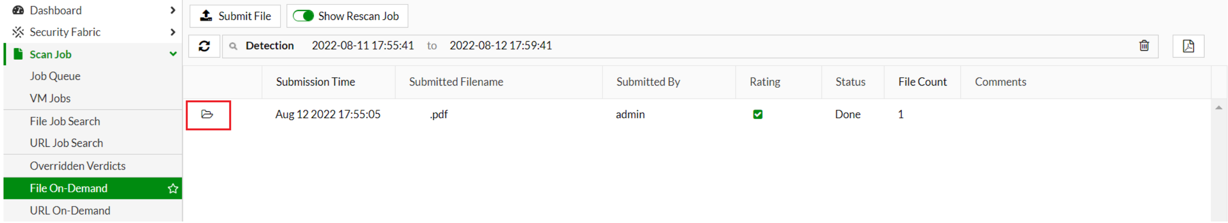
□ Add sample to threat package

Add file to Malware Package if it meets settings in Package Options

□ Enable AI

Enable AI mode for this scanning

c. When the scan is finished, click the *View File* icon to view job details.

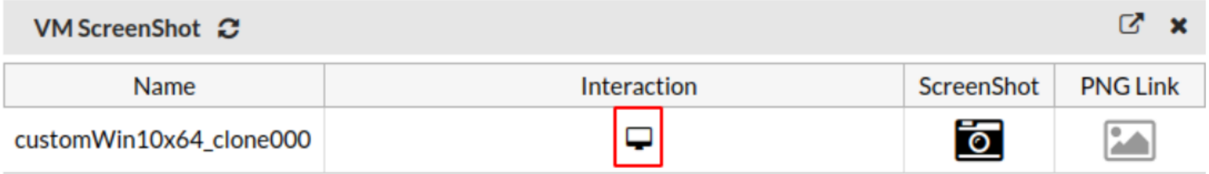


Detection 2022-08-11 17:55:41 to 2022-08-12 17:59:41

	Submission Time	Submitted Filename	Submitted By	Rating	Status	File Count	Comments
	Aug 12 2022 17:55:05	.pdf	admin	✓	Done	1	

6. (Optional) Interaction with a custom VM clone during scan:
   a. Go to *Scan Job > File On-Demand* or *URL on-Demand* and click *Submit File* or *Submit File/URL*.
   b. Enable *Force to scan the file inside VM* or *Force to scan the url inside VM*.
   c. Select *Force to scan inside the following VMs* and select the custom VM.
   d. Click *Submit*.
   e. Go to *Scan Policy and Object> VM Settings* and click *VM Screenshot*.

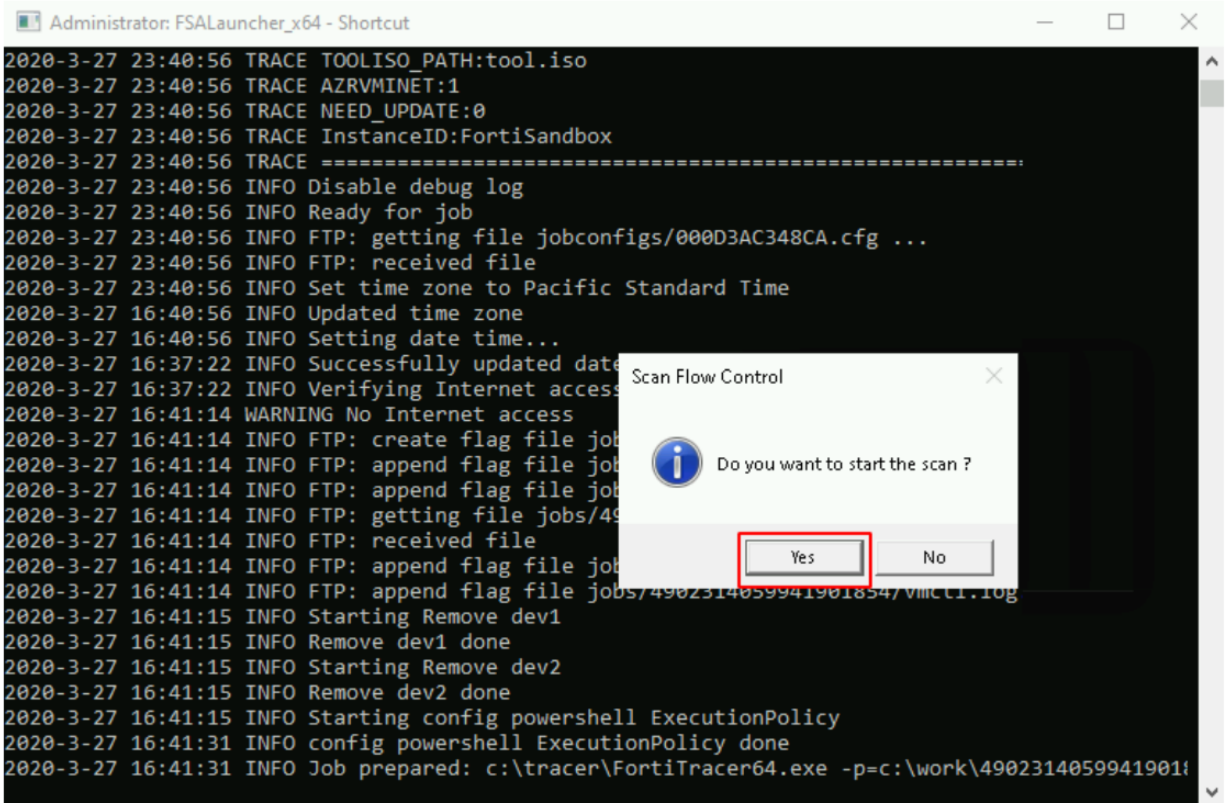
f. When the icon in the *Interaction* column is enabled, click the icon to establish an RDP tunnel.



VM ScreenShot

Name	Interaction	ScreenShot	PNG Link
customWin10x64_clone000	🖥	📷	🖼

g. Click *Yes* to manually start the scan process with VM Interaction.



```
2020-3-27 23:40:56 TRACE TOOLISO_PATH:tool.iso
2020-3-27 23:40:56 TRACE AZRVMINET:1
2020-3-27 23:40:56 TRACE NEED_UPDATE:0
2020-3-27 23:40:56 TRACE InstanceID:FortiSandbox
2020-3-27 23:40:56 TRACE ===========================================================
2020-3-27 23:40:56 INFO Disable debug log
2020-3-27 23:40:56 INFO Ready for job
2020-3-27 23:40:56 INFO FTP: getting file jobconfigs/000D3AC348CA.cfg ...
2020-3-27 23:40:56 INFO FTP: received file
2020-3-27 23:40:56 INFO Set time zone to Pacific Standard Time
2020-3-27 16:40:56 INFO Updated time zone
2020-3-27 16:40:56 INFO Setting date time...
2020-3-27 16:37:22 INFO Successfully updated date
2020-3-27 16:37:22 INFO Verifying Internet access
2020-3-27 16:41:14 WARNING No Internet access
2020-3-27 16:41:14 INFO FTP: create flag file job
2020-3-27 16:41:14 INFO FTP: append flag file job
2020-3-27 16:41:14 INFO FTP: append flag file job
2020-3-27 16:41:14 INFO FTP: getting file jobs/49
2020-3-27 16:41:14 INFO FTP: received file
2020-3-27 16:41:14 INFO FTP: append flag file job
2020-3-27 16:41:14 INFO FTP: append flag file jobs/4902314059941901854/vmctl.log
2020-3-27 16:41:15 INFO Starting Remove dev1
2020-3-27 16:41:15 INFO Remove dev1 done
2020-3-27 16:41:15 INFO Starting Remove dev2
2020-3-27 16:41:15 INFO Remove dev2 done
2020-3-27 16:41:15 INFO Starting config powershell ExecutionPolicy
2020-3-27 16:41:31 INFO config powershell ExecutionPolicy done
2020-3-27 16:41:31 INFO Job prepared: c:\tracer\FortiTracer64.exe -p=c:\work\4902314059941901
```

Scan Flow Control

Do you want to start the scan ?

h. When the FortiSandbox tracer engine displays the PDF sample, you can click *Yes* to manually stop the scan process.

i. When the scan is finished, go to the job details page to view the scan results.

(Optional) Using HA-Cluster

You can set up multiple FortiSandbox Azure instances in a load-balancing HA (high availability) cluster.

From version 3.2.0, FortiSandbox Azure supports the same custom VMs running on an HA cluster.

Before setting up HA cluster in Azure, ensure you know how HA clustering works in FortiSandbox. For information on FortiSandbox HA clusters, see the FortiSandbox Administration Guide.

Configure an HA cluster

Create the primary (formerly master) node first, then create the secondary (formerly primary slave) and worker (formerly slave or regular slave) nodes.

If you are using HA-Cluster without failover, the secondary node is optional.

Ensure the HA-Cluster meets the following requirements:

- Use the same scan environment on all nodes. For example, install the same set of Windows VMs on each node so that the same scan profiles can be used and controlled by the primary node.
- Run the same firmware build on all nodes.
- Set up a dedicated network interface (such as port2) for each node for custom VMs.
- Set up a dedicated network interface (such as port3) for each node for internal HA-Cluster communication.
- Set up ports for internal internal HA-Cluster communication:
  - For FortiSandbox PAYG, port2 is used for custom VMs and port3 for internal HA-Cluster communication.
  - For FortiSandbox non-nested BYOL, port2 is used for custom VMs and port3 for internal HA-Cluster communication.
  - For FortiSandbox nested BYOL, port2 is for internal HA-Cluster communication and port3 for custom VMs. Both are hardcoded.

The following are recommendations for the HA-Cluster:

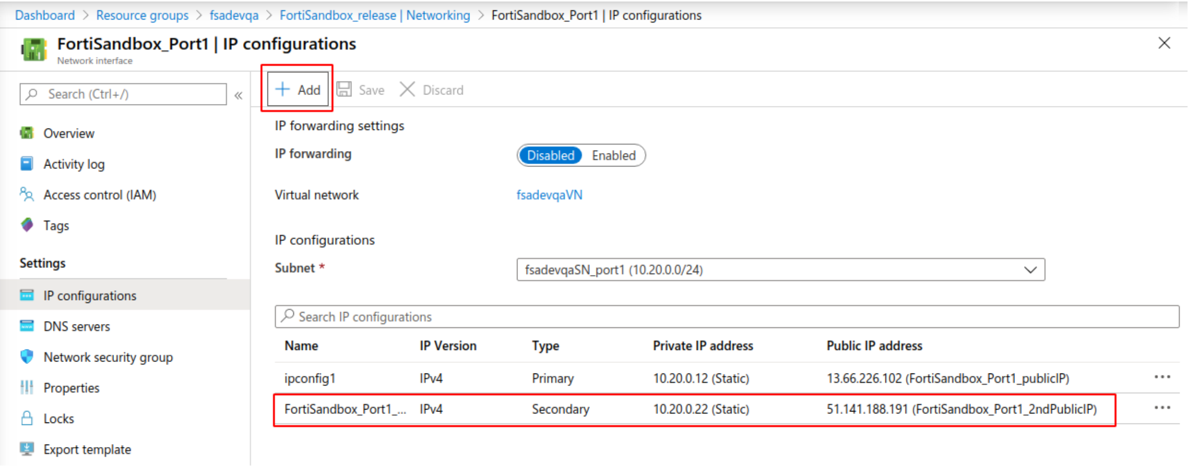
- Put interfaces on the same virtual network.
- Use a static IP address in the same subnet for each network port.
- Do not use the `set admin-port` command to set port1 or any other administrative port as the internal HA-Cluster communication port.

To create multiple FortiSandbox instances on Azure:

1. Create at least thee network interfaces on Azure for each FortiSandbox Azure.
2. In *Network security group*, open these ports for HA communication.

   ```
   TCP 2015 0.0.0.0/0
   TCP 2018 0.0.0.0/0
   ```

3. On the Azure portal, add a secondary IP address on the primary node as an external HA-Cluster communication IP address.
   a. Go to the primary node's port1 network interface.
   b. Go to *IP configurations* and click *Add*.
   c. Add a secondary static *Private IP address*.
   d. Optional: you can add a new static *Public IP address* for external HA-Cluster communication.
   In a failover, this HA-Cluster IP address will be used on the new primary node.



IP forwarding settings

IP forwarding: Disabled | Enabled

Virtual network: fsadevqaVN

IP configurations

Subnet *: fsadevqaSN_port1 (10.20.0.0/24)

Search IP configurations

Name	IP Version	Type	Private IP address	Public IP address
ipconfig1	IPv4	Primary	10.20.0.12 (Static)	13.66.226.102 (FortiSandbox_Port1_publicIP)
FortiSandbox_Port1_...	IPv4	Secondary	10.20.0.22 (Static)	51.141.188.191 (FortiSandbox_Port1_2ndPublicIP)

To import Azure settings into the FortiSandbox HA-Cluster:

1. Log into each node of the FortiSandbox GUI using the public IP address.
2. Follow the instructions on Import Azure settings into FortiSandbox on page 30 to configure the *Azure Config* page for both the primary and secondary.
3. Repeat for every node in the cluster.

To configure the HA cluster in FortiSandbox using CLI commands:

In this example, *10.20.0.22/24* is an HA external communication IP address. The secondary private IP address is on the primary node's port1 network interface.

The examples are for FortiSandbox PAYG and non-nested BYOL. For nested BYOL, please use **port2** instead of port3.

1. Configure the primary node using these CLI commands:

```
hc-settings -sc -tM -nMyHAPrimary -cClusterName -p123 -iport3
hc-settings -si -iport1 -a10.20.0.22/24
```

2. Configure the secondary node:

```
hc-settings -sc -tP -nMyPWorker -cClusterName -p123 -iport3
hc-worker -a -sPrimary_Port3_private_IP -p123
```

3. Configure the first worker:

```
hc-settings -sc -tR -nMyRWorker1 -cClusterName -p123 -iport3
hc-worker -a -sPrimary_Port3_private_IP -p123
```

4. If needed, configure additional regular workers:

```
hc-settings -sc -tR -nMyRWorker2 -cClusterName -p123 -iport3
hc-worker -a -sPrimary_Port3_private_IP -p123
```

To check the status of the HA cluster:

1. On the primary node, enter this command to view the status of all units in the cluster.

   ```
   hc-status -l
   ```

To use a custom VM on an HA-Cluster:

1. Install the Azure local custom VMs from the primary node onto each worker node using the FortiSandbox CLI command `azure-vm-customized`.
   All options must be the same when installing custom VMs on an HA-Cluster, including `-vn[VM name]`.

   For example, on the primary node, install the custom VM from blob and set the VM name `hawin10vm`.

   ```
   azure-vm-customized -cn -f[blob container name] -b[VM_image_name.vhd] -vo[OS type] -
   vnhawin10vm
   ```

   On the secondary node, keep all options the same as the primary node.

   ```
   azure-vm-customized -cn -f[blob container name same as primary node] -b[VM_image_
   name.vhd same as primary node] -vo[OS type] -vnhawin10vm
   ```

   On the worker node, also keep all options the same as the primary node.

   ```
   azure-vm-customized -cn -f[blob container name same as primary node] -b[VM_image_
   name.vhd same as primary node] -vo[OS type] -vnhawin10vm
   ```

2. Install the Azure local custom VMs from the primary node onto each worker node with the FortiSandbox CLI command:
   - For PAYG and non-nested BYOL use `azure-vm-customized`
   - For nested BYOL use `vm-customized`
3. In a new CLI window, check the VM clone initialization using the `diagnose-debug vminit` command.
4. In the FortiSandbox GUI, go to the *Dashboard* to verify there is a green checkmark beside *Windows VM*.
5. To associate file extensions to the custom VM, go to *Scan Policy and Object* > *Scan Profile* to the *VM Association* tab.

You can now submit scan jobs from the primary node. HA-Cluster supports VM Interaction on each node.

Best practices

Checklist for deploying FortiSandbox on Azure:

Task	Description
Creating a resource group	Azure resource group is a container that holds related resources for an Azure solution. Go to *Azure Portal* > *Resource groups* > *Access control (IAM)* > *Role assignments*. Verify the administrator has the minimum ''Role assignments for this resource group: • Owner, scope = this resource If you need to launch local custom VM clones, the Access control should grant administrator these Role assignments: • Virtual Machine Contributor, scope = this resource • API Management Service Contributor, scope = this resource
Creating network security groups	Go to Azure Portal > Network security groups. • Verify a security group is available for FortiSandbox firmware (Port1). • Verify the Resource group and the Region is the one your created. • Optional: a security group is available for port2 if local custom VM clones is used).
Creating virtual networks and one default subnet	• Go to *Azure Portal* > *Virtual networks*. Ensure the *Resource group* and the *Region* is the one you created. • Go to *Azure Portal* > *Virtual networks*. Select the *Virtual network* created. Under *Subnets*,ensure the default first subnet is for FortiSandbox firmware (Port1) and is associated with the security group for FortiSandbox Port1.
Optional: Creating multiple subnets in the virtual network	• Verify the second subnet is available for FortiSandbox custom VM (Port2). The third subnet is available for FortiSandbox HA-Cluster mode (Port3). • Go to Azure Portal > Virtual networks. Select the 'Virtual network' you created. Under Subnets, ensure the different subnets are associated with different network security groups if needed.
Creating two storage accounts	Go to *Azure Portal* > *Storage accounts*. • The first storage account is for storing FortiSandbox images. The second storage account is for debugging. • Ensure the *Resource group* and the *Region* is the one your created and the *Redundancy is Geo-Redundant Storage (GRS)*.
Optional: Creating multiple FSA network interfaces	Go to *Azure Portal* > *Network interfaces*. • Ensure the different network interfaces for FortiSandbox are deployed in different subnets and associated with different security groups if needed.

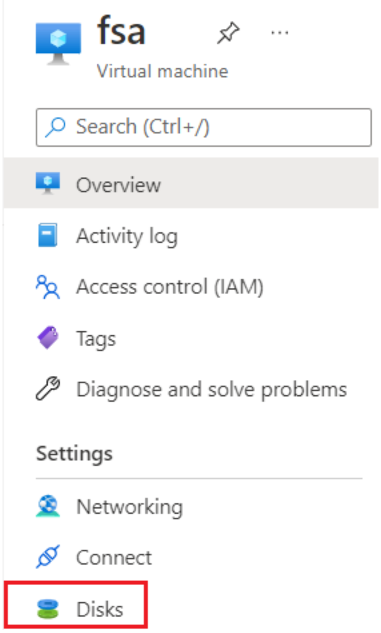
Task	Description
Optional: Setting up App registrations for the client id option of Azure Config on FortiSandbox GUI	• Go to *Azure Portal* > *App registrations* > *App roles*. Ensure the *App roles* allowed member types are Both (*Users/Groups* + *Applications*). • Go to *Azure Portal* > *App registrations* > *Certificates & secrets* > *Client secret*. Ensure the *Expires* is valid. • Go to *Azure Portal* > *App registrations* > *API permissions*. Ensure the minimum API permissions are as follows: • *Azure Service Management: Delegated*, Granted for FortiSandbox • *Azure Storage: Delegated*, Granted for FortiSandbox. • *Microsoft Graph*: Files.*ReadWrite, User*.Read • App roles: The *App roles* you created, Granted for FortiSandbox

How to re-size the Data Disk

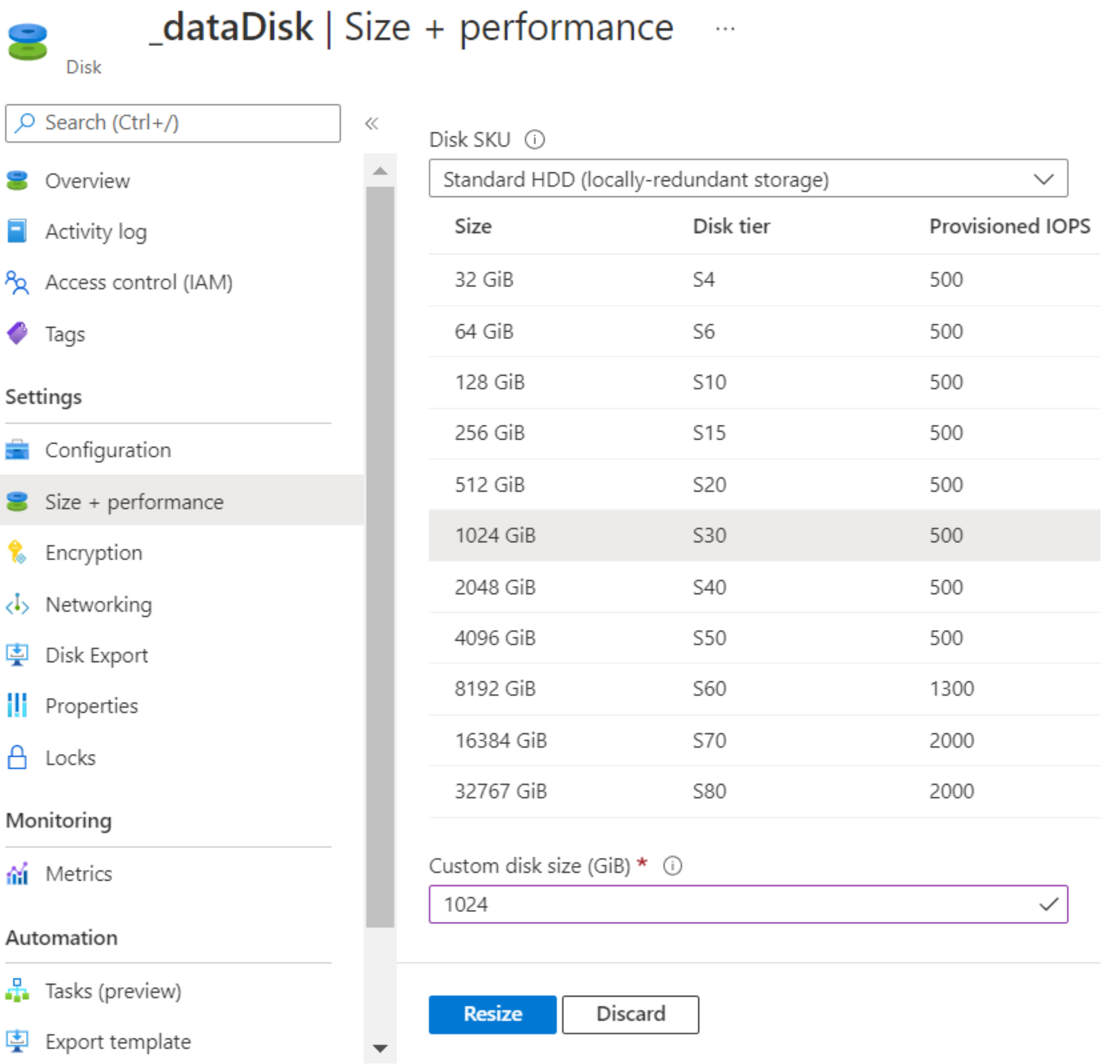
Use the *Size + performance* settings to maintain the data disk on FortiSandbox on Azure and monitor the disk usage to ensure the data disk does not break.

Scenario 1: Modify FSA data disk without data lost and before disk broken

1. On the Azure Portal, stop the FortiSandbox instance.
2. Go to *FSA Virtual Machine* > *Overview* > *Disks* > *datadisk* > *Size + performance*.



3. Expand Disk SKU and click *Resize*.



Disk SKU ⓘ

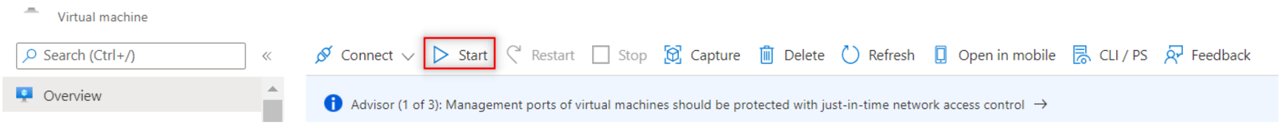
Standard HDD (locally-redundant storage)

Size	Disk tier	Provisioned IOPS
32 GiB	S4	500
64 GiB	S6	500
128 GiB	S10	500
256 GiB	S15	500
512 GiB	S20	500
1024 GiB	S30	500
2048 GiB	S40	500
4096 GiB	S50	500
8192 GiB	S60	1300
16384 GiB	S70	2000
32767 GiB	S80	2000

Custom disk size (GiB) * ⓘ

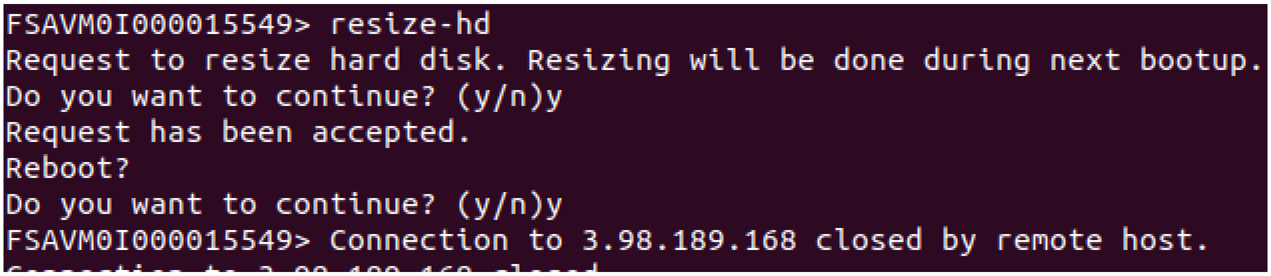
1024

4. Refresh the Azure Portal and ensure the disk size has been updated.
5. On the Azure Portal, start FortiSandbox.



Advisor (1 of 3): Management ports of virtual machines should be protected with just-in-time network access control →

6. Run the following CLI command: `resize-hd`

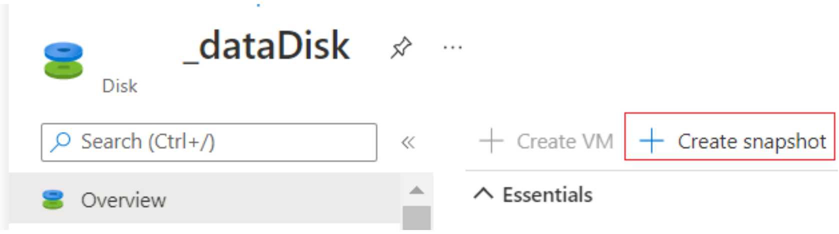


```
FSAVM0I000015549> resize-hd
Request to resize hard disk. Resizing will be done during next bootup.
Do you want to continue? (y/n)y
Request has been accepted.
Reboot?
Do you want to continue? (y/n)y
FSAVM0I000015549> Connection to 3.98.189.168 closed by remote host.
```

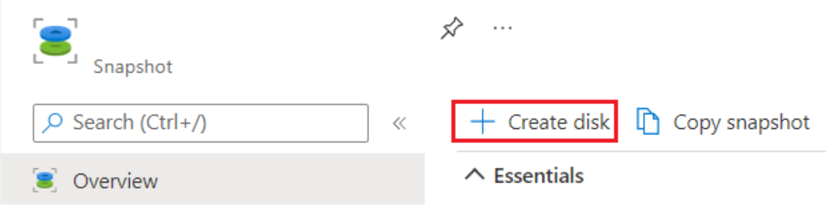
7. After FortiSandbox reboots, run the CLI command `status` commnad to verify the `Disk Size` is correct.

Scenario 2: Detach/Attach a new FortiSandbox data disk without losing data

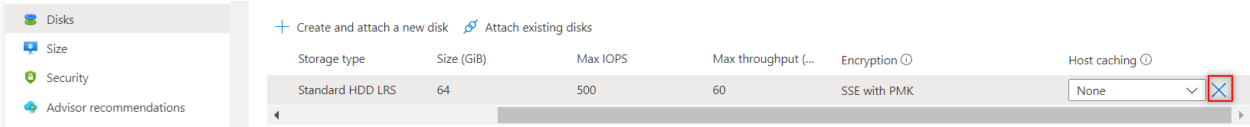
1. On the Azure Portal, stop the FortiSandbox instance.
2. Go to *Data disk* > *Create snapshot*.



3. Use the snap shot to create a data disk and set the size to *256G* or more if needed.

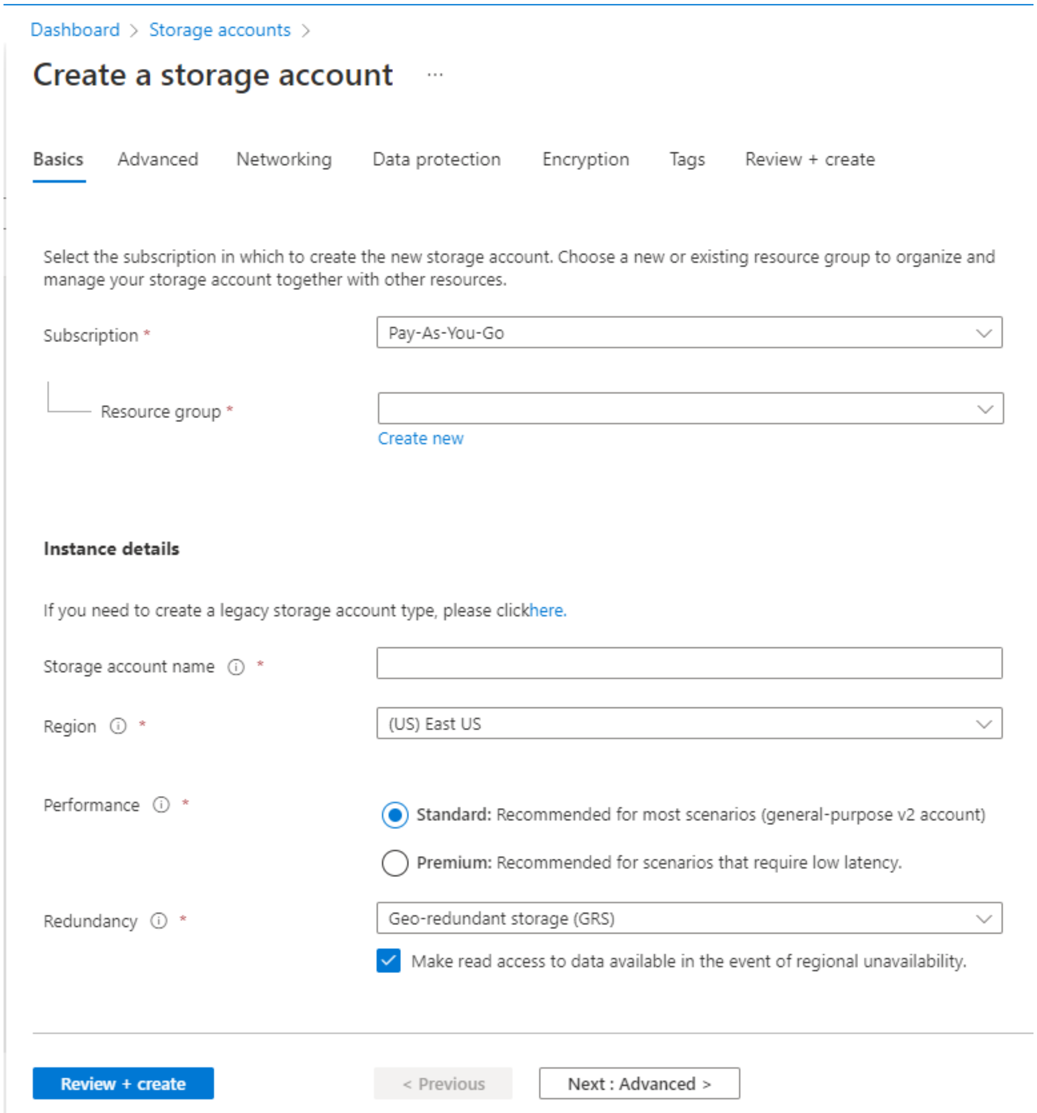


4. Detach the old data disk.



Storage type	Size (GiB)	Max IOPS	Max throughput (...	Encryption ⓘ	Host caching ⓘ
Standard HDD LRS	64	500	60	SSE with PMK	None

5. Attach the new data disk you created from the snap shot.



Dashboard > Storage accounts >

Create a storage account ...

Basics | Advanced | Networking | Data protection | Encryption | Tags | Review + create

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription *: Pay-As-You-Go

Resource group *:
Create new

Instance details

If you need to create a legacy storage account type, please clickhere.

Storage account name ⓘ *:

Region ⓘ *: (US) East US

Performance ⓘ *:
● **Standard:** Recommended for most scenarios (general-purpose v2 account)
○ **Premium:** Recommended for scenarios that require low latency.

Redundancy ⓘ *: Geo-redundant storage (GRS)
☑ Make read access to data available in the event of regional unavailability.

6. Refresh the Azure Portal, and confirm the disk has been updated.
   a. Run the CLI command: `resize-hd`.
   b. After FortiSandbox reboots use the CLI command `status` to verify the `Disk Size` is correct.

Appendix A - Port usage

FortiSandbox requires the following ports to be accessible:

- 21 (FTP, for FSA communication with VM clone(s))
- 22 (if SSH access is needed)
- 443 (HTTPS)
- 514 (if Fortinet Fabric devices such as FortiGate and FortiMail need to submit jobs)
- 9833 (for on-demand interactive scans)

For more port information, see Port Information section of the *FortiSandboxAdministration Guide*.

Appendix B - Reduce scan time in custom Windows VM

When a file is sent to a local Windows clone for dynamic scan, it takes time to boot up the clone from power-off state. You can keep the custom VM clones running to reduce scan time.

To reduce the scan time in a custom Windows VM:

1. Go to *System* > *Azure Config* and enable *Allow Hot-Standby VM*. After *Allow Hot-Standby VM* is enabled, FortiSandbox will perform `vminit` again to apply changes to existing custom VM clones or prepare new clone(s).

   Allow Hot-Standby VM ☑ Enabled

   When *Hot-Standby VM* enabled, the VM clones instance will be stopped if FortiSandbox is shutdown.

2. After the clone initiation is done, go to the *Azure EC2* console to check that the clone(s) keep running with /without a scan job. Allow 2-3 minutes for a custom VM clone to restore status after a scan job is done. Afterwards, the clone will keep running, and standby for the next scan job to reduce VM scan time.

To improve the performance of this feature, we recommend enabling more clones than the maximum concurrent dynamic scan jobs, so when a new dynamic scan job is started, there are stand-by clones available immediately.

Appendix C: Setting up an HA Cluster IP based on Azure Load Balancer

You can also use Azure Load Balancer to set up an HA Cluster IP. With the Public Load Balancer, there is a public IP which will be our Cluster IP. The Cluster IP will always point to the Primary unit.

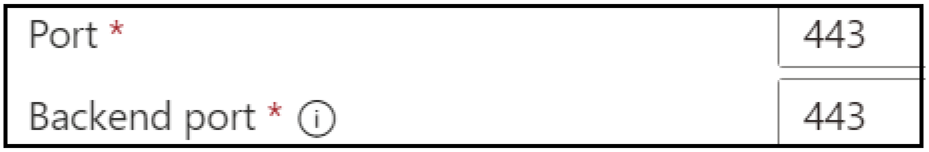
The Load Balancer we build for FortiSandbox Cluster will use port 514 to do the health check for all the units in the backend pool. Normally a rule is used to define how incoming traffic is distributed to all the instances within the backend pool. Since only Primary is listening port 514 in Cluster which will be the only instance that can pass the health check, then the given frontend IP will always point to Primary.

To set up the load balancer:

1. In the Azure portal of the Primary FortiSandbox, click menu *Load Balancing*.
2. Click *Add load balancing* to add a new Load Balancer, then select *Create new* > *Load balancer*.
3. Enter the following parameters:

Load balancer name	The Load balancer name, such as `fsa-lb`.
Type	Select *Public* for this case. this will be the cluster IP.
Protocol	Select *TCP* .
Load balancer rule	The Load balancer rule here is used to build the first rule. You can use any port to suit your needs. In this case, we will use: • **Port**: 443 • **Backend Port**: 443 Port 443 is for HTTPs.

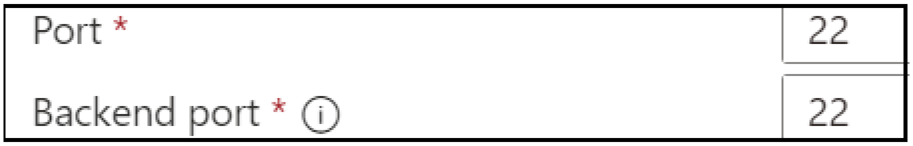
4. After the Load balancer builds successfully, click the load balancer name and check all the parameters.
5. In the *Overview* of the load balancer, Azure will automatically generate *Backend pool*, *Load balancing rule*, and *Health probe* with the prefix of the load balancer name such as `fsa-lb-xxxx`. You will need to check each setting one-by-one to ensure they match your requirements.
6. Click the menu *Fronted IP configuration* in the portal. One IP configuration should be listed with the public IP.
7. Click the menu *Backend pool*. Add the interface of the secondary port1. If you need to change the unit type of a cluster node from Worker to Secondary, we recommend adding all the interfaces of cluster nodes in the pool.
8. Click the *Load balancing* rule. There should be a rule generated by Azure. Click the rule and make sure both *Port* and *Backend port* is *443*.



Port * 443

Backend port * 443

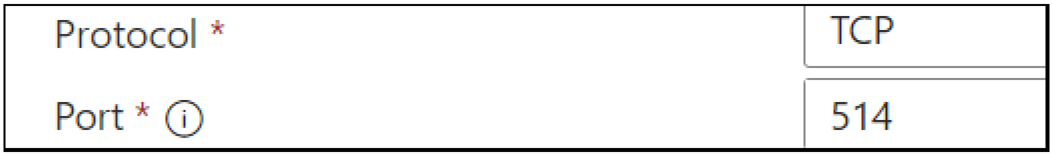
If you want to use SSH to log in for some CLI operations, create one more rule for SSH by clicking *Add*. For the new rule, set *Port* as *22* and *Backend port* as *22*.



Port *	22
Backend port * ⓘ	22

If there are other ports that need to be accessed, you can add rules for them as well. Such as for a FortiGate connection, create rule for port 514.

9. Click the *Health probe*. Verify the *Protocol* is *TCP* and the *Port* is *514* which will be used to do the health check.



Protocol *	TCP
Port * ⓘ	514

10. Log in with the public IP of the Load Balancer. It will point to the Primary unit even after failover has occurred.

Change Log

Date	Change Description
2023-11-28	Initial release.
2024-03-18	Added Nested deployments on page 5 Updated Minimum system requirements on page 9, Deploy FortiSandbox VM on Azure (PAYG / BYOL) on page 20, Set up the local VM on page 40 Set up the local VM on page 40and (Optional) Using HA-Cluster on page 46.

FORTINET®

www.fortinet.com