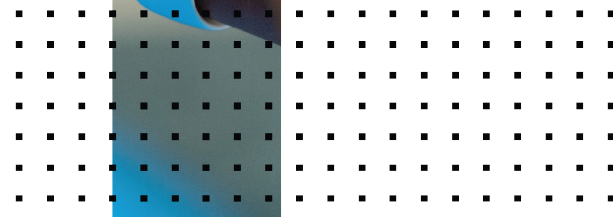


Azure Guide

FortiSandbox 4.2.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



April 12, 2022

FortiSandbox 4.2.0 Azure Guide

34-420-757791-20220412

TABLE OF CONTENTS

Overview	4
Deployment models	4
FortiSandbox VM basic deployment model	4
FortiSandbox VM advanced deployment model	5
Deploying FortiSandbox VM on Azure (Basic)	6
FortiSandbox VM and Windows Cloud VMs topology	10
FortiSandbox VM Port Usage	11
Deploying FortiSandbox VM on Azure (Advanced)	12
Creating a resource group	12
Creating network security groups	13
Creating virtual networks	15
Creating storage accounts	16
Creating network interfaces	18
Creating a data disk	21
Re-size the Data Disk (highly-recommended)	22
Importing Azure settings into FortiSandbox	26
Uploading the rating and tracer engine	26
Reduce scan time in custom Windows VM	30
Optional: Using HA-Cluster	31
Configuring an HA cluster	31
Change Log	34

Overview

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](#).

Deployment models

You can configure your FortiSandbox VM on Azure using a basic or advanced deployment model.

FortiSandbox VM basic deployment model

The FortiSandbox basic deployment model is the fastest and easiest way to deploy a FortiSandbox VM on Azure. Basic deployment uses the Azure setup wizard to guide you through the setup process with step-by-step instructions. Deployment takes approximately 20 minutes.

Advantages

- 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.

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 new network interface.
- Supports sandboxing analysis using Windows Cloud VMs only.
- Does not support custom Windows VMs.

FortiSandbox VM advanced deployment model

To use the advanced features of the FortiSandbox VM including custom VMs and HA features, use the advanced deployment model. Advanced deployment requires you to manually create all the resources you need. This model is recommended for people who have experience working with Azure and the cloud. Deployment takes approximately one hour.

To use custom VMs, including pre-configured VMs, your own ISO image, or Red Hat VMs on VirtualBox, contact [Fortinet Customer Service & Support](#).

Advantages

- Gives you full control to customize the resources required to deploy the VM.
- Supports custom Windows VMs.
- Supports HA features.

Limitations

- 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.

Deploying FortiSandbox VM on Azure (Basic)

To deploy FortiSandbox VM on Azure with Windows Cloud VMs:

1. Go to Azure Marketplace and search for *Fortinet FortiSandbox*.

Microsoft Azure

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

Dashboard > Marketplace > Fortinet FortiSandbox Advanced Threat Protection (preview)

Fortinet FortiSandbox Advanced Threat Protection (preview)

Fortinet

Free trial

Select a software plan

Fortinet FortiSandbox-VM for Azure... Create Start with a pre-set configuration

Want to deploy programmatically? Get started

Overview Plans

FortiSandbox for Azure enables organizations to defend against advanced threats natively in the cloud, working alongside network, application, email, endpoint security, and other 3rd party security solutions, or as an extension to their on-premises security architectures to leverage cloud elasticity and scale.

Highlights:

- Broad Coverage of the Attack Surface with Security Fabric - Effective defense against advanced targeted attacks through a cohesive and extensible architecture working to protect network, application layers and endpoint devices from campus to cloud.
- Automated Zero-day, Advanced Malware Detection and Mitigation - Native integration and open APIs automate the submission of objects from Fortinet and third-party vendor protection points, and the sharing of threat intelligence in real time for immediate threat response.
- Certified and Top Rated - Constantly undergoes rigorous, real-world independent testing and consistently earns top marks.
- Protect DevOps repositories, and internal and external hosted content with native Azure Blob Storage scanning for zero-day threats.

FortiSandbox for Azure has the following admin ports enabled:

- 443 for web admin
- 22 for ssh admin

FortiSandbox uses a two-stage process to identify zero-day, advanced malware including ransomware, and share relevant threat intelligence in real-time with inline security control so automated mitigation is applied.

- Stage 1 - Pre-filtering is performed by an engine powered by Fortinet's threat intelligence maintained by our global research team, FortiGuard Labs.
- Stage 2 - Dynamic behavior analysis is performed on objects to determine if they are malicious. Rating verdicts are returned to the originating device in real-time to act upon, natively within Fortinet Fabric security products, third-party vendor security products via JSON API, or as a feed via STIX format.

Useful Links

[Datasheet](#)

[Deployment Guide](#)

[Admin Guide](#)

[Fortinet Technical Support](#)

2. Select a software plan and then click *Create* to start the setup wizard.
If you select *Fortinet FortiSandbox-VM for Azure BYOL*, you must provide your own licenses.

Dashboard > Marketplace > Fortinet FortiSandbox Advanced Threat Protection (preview)

Fortinet FortiSandbox Advanced Threat Protection (preview)

Fortinet

Free trial

Select a software plan

Fortinet FortiSandbox-VM for Azure... Create Start with a pre-set configuration

Fortinet FortiSandbox-VM for Azure PAYG

Fortinet FortiSandbox-VM for Azure BYOL

Overview Plans

3. In the setup wizard, click *Create*.

4. Configure the virtual machine.

Microsoft Azure

Search resources, services, and docs (G+)

Dashboard > Marketplace > Fortinet FortiSandbox Advanced Threat Protection (preview) > Create a virtual machine

Create a virtual machine

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 * ⓘ fsareleaseqa [Create new](#)

Instance details

Virtual machine name * ⓘ

Region * ⓘ (US) West US 2

Availability options ⓘ No infrastructure redundancy required

Image * ⓘ Fortinet FortiSandbox-VM for Azure BYOL [Browse all public and private images](#)

Azure Spot instance ⓘ ☐ Yes ☒ No

Size * ⓘ **Standard A4 v2**
4 vcpus, 8 GiB memory (US\$118.30/month) [Change size](#)

Administrator account

Authentication type ⓘ ☐ Password ☒ SSH public key

Username * ⓘ

SSH public key * ⓘ

[Learn more about creating and using SSH keys in Azure](#)

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

Resource group	Create a new resource group.
Virtual machine name	Name of the VM.
Region	VM region.
Size	Select the VM instance type. We recommend <i>Standard A4 v2</i> for speed and storage capacity. FortiSandbox on Azure uses the temporary disk (provided free by the VM) to store and process job files. A secondary disk is not required.
Authentication type	Click <i>Password</i> or <i>SSH public key</i> .
Username	Enter a secondary admin user; the default <i>Admin</i> user is always created.

- Click **Review + Create**.
- When the setup wizard has validated your information, click **Create**.
Wait a few minutes for the FortiSandbox VM to become available.

Microsoft Azure

Search resources, services, and docs

Home > Fortinet FortiSandbox-VM for Azure BYOL > Create a virtual machine

Create a virtual machine

✓ Validation passed

Basics Disks Networking Management Guest config Tags **Review + create**

PRODUCT DETAILS

Fortinet FortiSandbox-VM for Azure BYOL by Fortinet
Terms of use | Privacy policy

Not covered by credits ⓘ
0.0000 USD/hr

Standard A4 v2 by Microsoft
Terms of use | Privacy policy

Subscription credits apply ⓘ
0.2060 USD/hr
Pricing for other VM sizes

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same bill my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party Azure Marketplace Terms for additional details.

BASICS

Subscription	Pay-As-You-Go
Resource group	fortisandbox-release
Virtual machine name	fsavmtest
Region	Canada Central
Availability options	No infrastructure redundancy required
Authentication type	Password
Username	jiliang

DISKS

OS disk type	Standard SSD
Use managed disks	Yes

NETWORKING

Create Previous Next Download a template for automation

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

Dashboard > CreateVm-fortinet.fortinet_fortisandbox_vm-fortin-20200115152558 - Overview

CreateVm-fortinet.fortinet_fortisandbox_vm-fortin-20200115152558 - Overview

Deployment

Search (Ctrl+/) Delete Cancel Redeploy Refresh

Overview

Inputs
Outputs
Template

✓ Your deployment is complete

Deployment name: CreateVm-fortinet.fortinet_fortisandbox_vm-fo... Start time: 1/15/2020, 3:37:07 PM
Subscription: PAYG-DevOps Correlation ID: 85d4751f-434c-413a-98fe-95fa098d1390
Resource group: tsadevqa

▼ Deployment details (Download)

^ Next steps

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

Go to resource

8. Use the *Public IP address* assigned to the FortiSandbox to access from HTTPS.

Dashboard > CreateVm-fortinet.fortinet_fortisandbox_vm-fortin-20200115152558 - Overview > FortiSandbox

FortiSandbox
Virtual machine

Search (Ctrl+/) << Connect Start Restart Stop Capture Delete Refresh

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
- Networking
- Disks

Resource group (change) : fsadevqa

Status : Running

Location : West US 2

Subscription (change) : PAYG-DevOps

Subscription ID : 4f27b38c-ad3f-43d8-a9a3-01182e5e2f9a

Computer name : (not available)

Operating system : Linux

Size : Standard A4 v2 (4 vcpus, 8 GiB memory)

Tags (change) : [Click here to add tags](#)

Azure Spot : N/A

Public IP address : 52.250.7.37

Private IP address : 10.10.0.4

Public IP address (IPv6) : -

Private IP address (IPv6) : -

Virtual network/subnet : fsadevqaVN/fsadevqa-10.10.0.0

DNS name : [Configure](#)

Scale Set : N/A

9. Get the default admin password for the FortiSandbox VM using the Azure CLI command `az vm list -output tsv -g [Your resource group]`.
The VM-ID UUID is the default password for Admin access.

```
sylvia@sylvia-OptiPlex-3050:~$ az vm list --output tsv -g fsadevqa |grep FortiSandbox_release
None None None None None None /subscriptions/4f27b38c-ad3f-43d8-a9a3-01182e5e2f9a/resourceGroups/fsadevqa/providers/Microsoft.Compute/virtualMachines/fsadevqa/FortiSandbox_release
Microsoft.Compute/virtualMachines None b041078a-ccc8-444e-b037-c1aeca9c977b None None Succeeded None fsadevqa None
```

To apply the VM00 license and enable Windows Cloud VMs:

1. Log into FortiSandbox with the username *admin* and the password you retrieved from the CLI in the previous step.
2. Go to *FortiSandbox > Dashboard* and click *Upload License* to upload your license.

FortiSandbox Azure Status > admin

System Information

- Firmware Version: v4.0.0.build0037 (Interim)
- Hostname: FSA-VM0000000000
- Serial Number: FSA-VM0000000000
- System Configuration: Last Backup: N/A
- System Time: 2021-04-15 23:09:37 UTC
- Unit Type: Standalone
- Uptime: 0 day(s) 0 hour(s) 11 minute(s)
- Username: admin

System Resources

- CPU Usage: 0%
- Memory Usage: 33%
- Disk Usage: 14.82%

Reboot Shutdown

Licenses

- FortiSandbox-Azure
 - Windows VM
 - Windows Cloud VM
 - MacOS Cloud VM
 - Customized VM
 - Mail Transfer Agent Service

Connectivity and Services

Scan Performance - Last 4 Hours

Scanned: 0 Total Scanned

Performance: 0s / 0s Avg/Max Processing Wait Time

Security: 0 AI Detected, 0 0-day Malware, 0 Known Malware, 0 Suspicious URL

Scan Statistics - Last 24 Hours

Inputs	Pending	Processing	Malicious	High Risk	Medium Risk	Low Risk	Clean	Other	Total
Device	0	0	0	0	0	0	0	0	0
Adapter	0	0	0	0	0	0	0	0	0
On Demand	0	0	0	0	0	0	0	0	0
Network Share	0	0	0	0	0	0	0	0	0
Sniffer	0	0	0	0	0	0	0	0	0
URL	0	0	0	0	0	0	0	0	0
All Sources	0	0	0	0	0	0	0	0	0

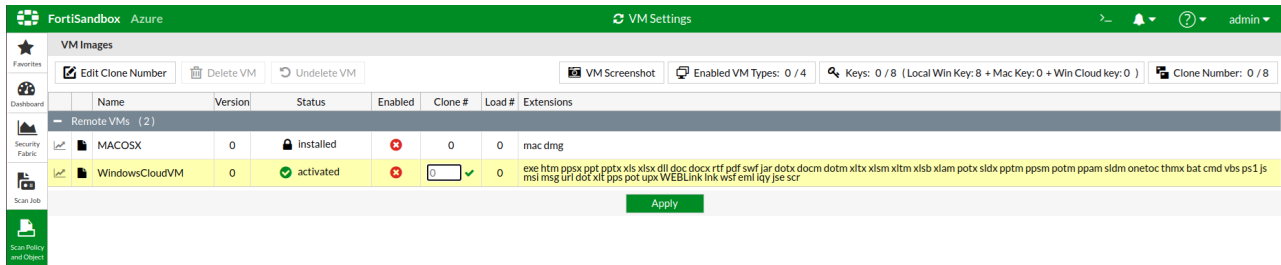
Last Updated: 04-15 23:06

When a license file is loaded, the FortiSandbox Azure instance reboots.

When the FortiSandbox Azure instance finishes rebooting, the *VM License* icon changes to green.

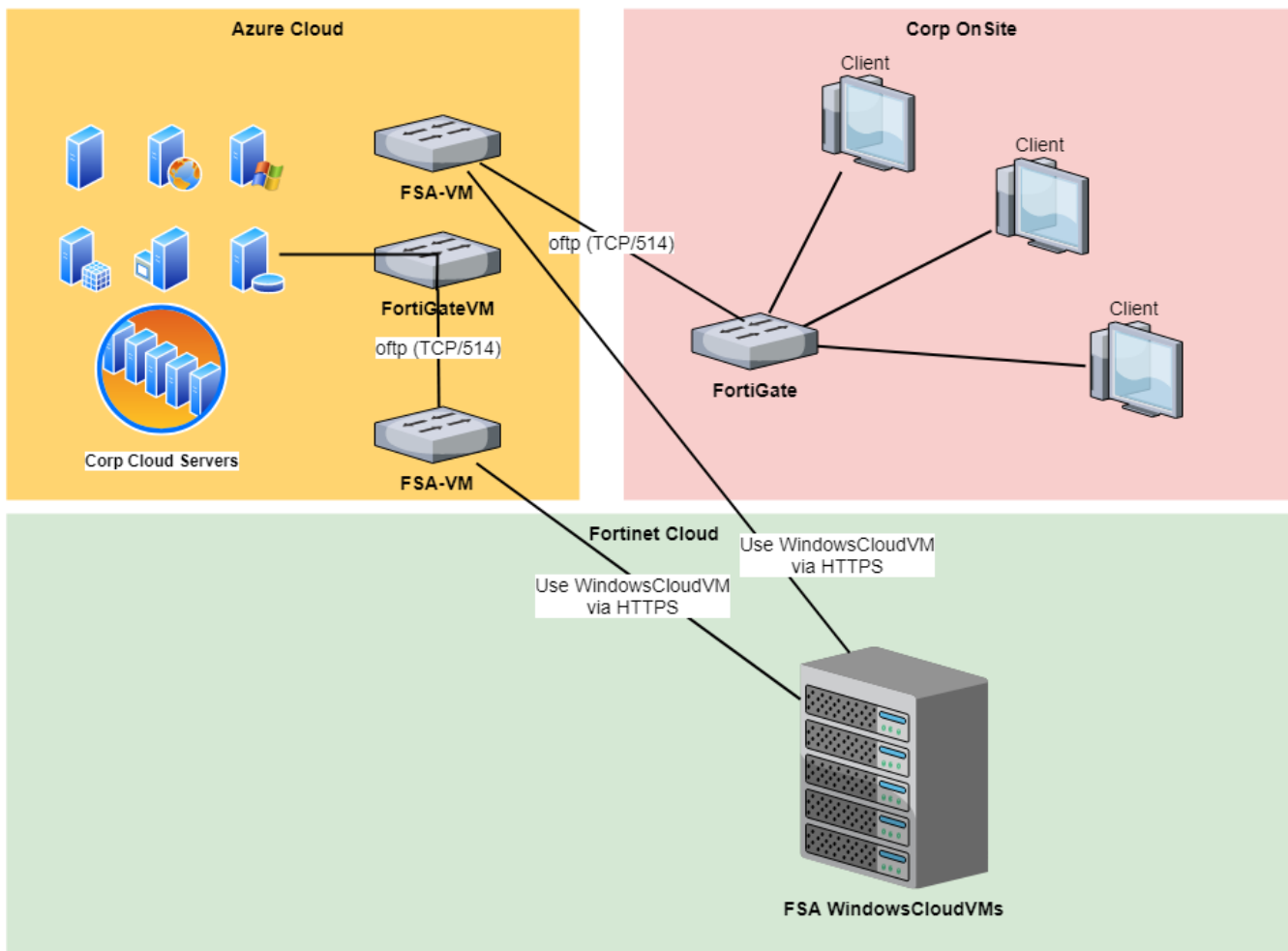
3. Go to *Scan Policy and Object > VM Settings* and select the *WindowsCloudVM*.

- Click *Edit Clone Number* to assign a clone number and enable the Windows Cloud VM.



As with FortiSandbox appliance, the FortiSandbox license must be generated matching the port1 IP of the instance. Go to *System > Interfaces* to check the port1 IP address assigned by Azure.

FortiSandbox VM and Windows Cloud VMs topology



FortiSandbox VM Port Usage

Type	Service	Port
FortiGate	OFTP	TCP/514
FortiClient	File Analysis	TCP/514
Others	SSH CLI Management	TCP/22
	Telnet CLI Management	TCP/23
	Web Admin	TCP/80, TCP/443
	OFTP Communication with FortiGate and FortiMail	TCP/514
	Third-Party Proxy Server for ICAP Servers (ICAP)	TCP/1344
	Third-Party Proxy Server for ICAP Servers (ICAPS)	TCP/11344
FortiGuard	FortiGuard Distribution Servers	TCP/8890
	FortiGuard Web Filtering Servers	UDP/53, UDP/8888
FortiSandbox Community Cloud	Upload Detected Malware Information	TCP/443, UDP/53
FortiSandbox WindowsCloudVM	Serving WindowsVM on cloud for FSA-VM to perform sandboxing	TCP/443

Deploying FortiSandbox VM on Azure (Advanced)

To deploy FortiSandbox VM on Azure to support Windows Cloud VMs and custom VMs, perform the following procedures.

1. [Creating a resource group](#)
2. [Creating network security groups](#)
3. [Creating virtual networks](#)
4. [Creating storage accounts](#)
5. [Creating network interfaces](#)
6. [Creating a data disk](#)
7. [Re-size the Data Disk \(highly-recommended\)](#)
8. [Importing Azure settings into FortiSandbox](#)
9. [Optional: Using HA-Cluster](#)

Creating 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.

The screenshot displays the Microsoft Azure portal interface. On the left, the navigation pane shows 'Resource groups' highlighted. The main content area is titled 'Resource groups' and includes a table of existing groups. A red box highlights the '+ Add' button. The right-hand pane shows the 'Create a resource group' wizard. The 'Basics' tab is active, showing fields for 'Subscription' (set to 'PAYG-DevOps'), 'Resource group' (set to 'fortisandbox'), and 'Region' (set to '(US) Central US'). The 'Review + create' button is visible at the bottom right.

3. Enter the following information:

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

Creating 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).

3. Enter the following information:

Subscription	Select a subscription type.
Resource group	Select the resource group you created in the Creating 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 custom VM communication hardcoded).

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).



Alternatively, you can create only one network security group with the inbound rules allowing for HTTPS, SSH traffic, OFTP, FTP, and RDP.

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

Creating 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.

The screenshot shows the Microsoft Azure portal interface. On the left, the 'Virtual networks' option is highlighted in the navigation pane. The main area displays the 'Virtual networks' list with an 'Add' button. The 'Create virtual network' form is open on the right, showing the following configuration:

- Name:** fortisandbox_VN
- Address space:** 10.45.0.0/16
- Subscription:** PAYG-DevOps
- Resource group:** fortisandbox
- Location:** (US) Central US
- Subnet Name:** fortisandbox_public
- Address range:** 10.45.0.0/24
- DDoS protection:** Basic
- Service endpoints:** Disabled
- Firewall:** Disabled

3. Enter the following information:

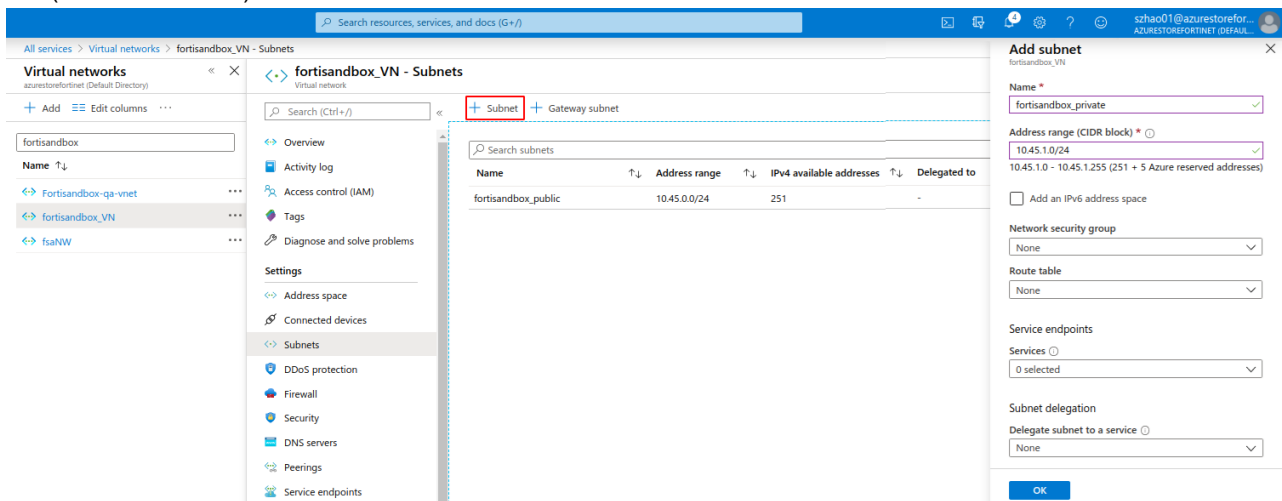
Name	Name of the virtual network.
Address space	Use an Azure suggested unused class B network (xxx.xxx.0.0/16) or enter your preferred unused class B network.
Subscription	Select your subscription type.

Resource group	Select the resource group you created in the Creating a resource group step.
Location	Select the location you used when you set up the resource group.
Subnet Name	Name of FSA subnet port1 (the management subnet).
Subnet Address range	Enter a class C network (xxx . xxx . x . 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 custom VM subnet), and assign another class C network (xxx.xxx.xxx.0/24) in that network.



Using *class B* (xxx.xxx.0.0/16) and *class C* (xxx.xxx.0.24) in the table above is an example of a common use case. You can adjust the network range for your needs.

Creating 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 VM 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.

[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 *

Resource group * [Create new](#)

Instance details

If you need to create a legacy storage account type, please click [here](#).

Storage account name ⓘ *

Region ⓘ *

Performance ⓘ *

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

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

Redundancy ⓘ *

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

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

3. Enter the following information for each account:

Subscription	Select your subscription type.
Resource group	Select the resource group you created in the Creating 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.
Account kind	Use the default or change according to your needs.
Replication	Geo-Redundant Storage (GRS).

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

Creating network interfaces

Create the following network interfaces:

- The first network interface is for FortiSandbox *port1*.
- The second network interface is for FortiSandbox *port2*.
- If you want to use HA-Cluster on multiple FortiSandbox Azure units, create a third network interface is for FortiSandbox *port3*.

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.

The screenshot shows the Azure portal interface for creating a new network interface. On the left, the 'Network interfaces' list is visible, and the 'Add' button is highlighted with a red box. The main area displays the 'Create network interface' form with the following configuration:

- Name ***: fsa_eth0_public
- Virtual network ***: fortisandbox_VN
- Subnet ***: fortisandbox_private (10.45.1.0/24)
- Private IP address assignment**: Static (selected)
- Private IP address ***: (empty field)
- Network security group**: None
- Subscription ***: PAYG-DevOps
- Resource group ***: fortisandbox
- Location ***: (US) Central US

At the bottom, there is a 'Create' button and a link for 'Automation options'.

3. Enter the following information:

Name	VM name.
Virtual network	Select your VNet.
Subnet	One subnet under your VNet. 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 Creating 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 create multiple network security groups, the one associated with the FSA port1 interface must be under the security group which includes HTTPS (TCP 443), SSH traffic (TCP 22), OFTP traffic (TCP 514), and the one associated with the FSA port2 interface must be under the security group which includes FTP.

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

Search resources, services, and docs (G+)

All services > Network interfaces > fsa_eth0_public - IP configurations > ipconfig1

fsa_eth0_public - IP configurations

Network interface

Search (Ctrl+/)

+ Add Save Discard

Overview

Activity log

Access control (IAM)

Tags

Settings

IP configurations

DNS servers

Network security group

Properties

IP forwarding settings

IP forwarding: Disabled Enabled

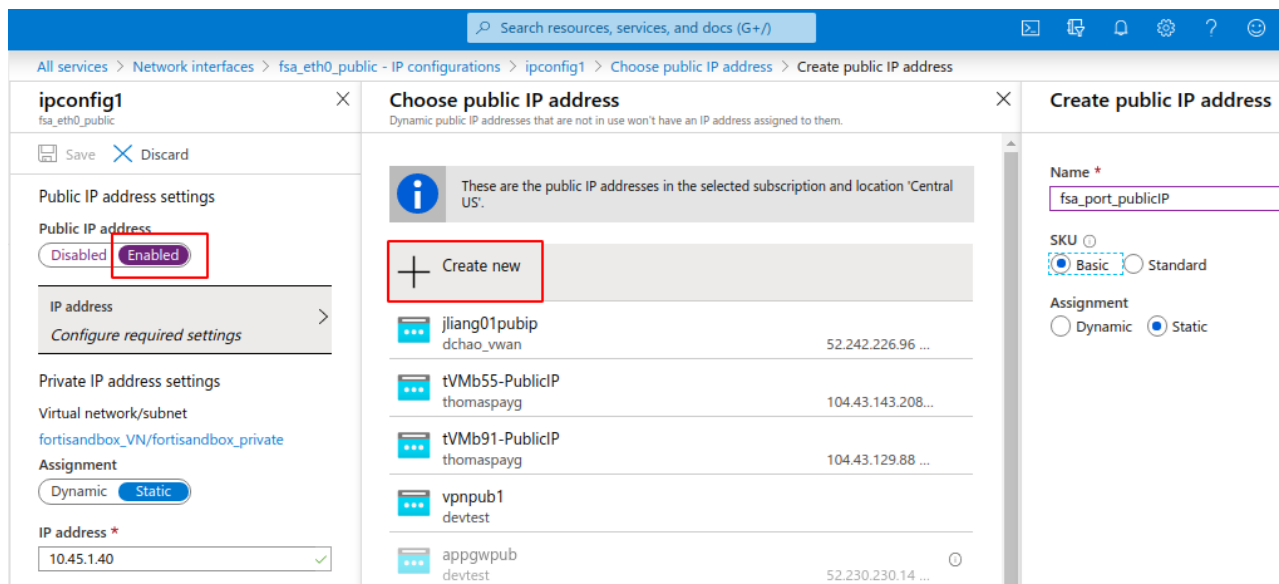
Virtual network: fortisandbox_VN

IP configurations

Subnet *: fortisandbox_private (10.45.1.0/24)

Search IP configurations

Name	IP Version	Type	Private IP address	Public IP address
ipconfig1	IPv4	Primary	10.45.1.40 (Static)	- ***

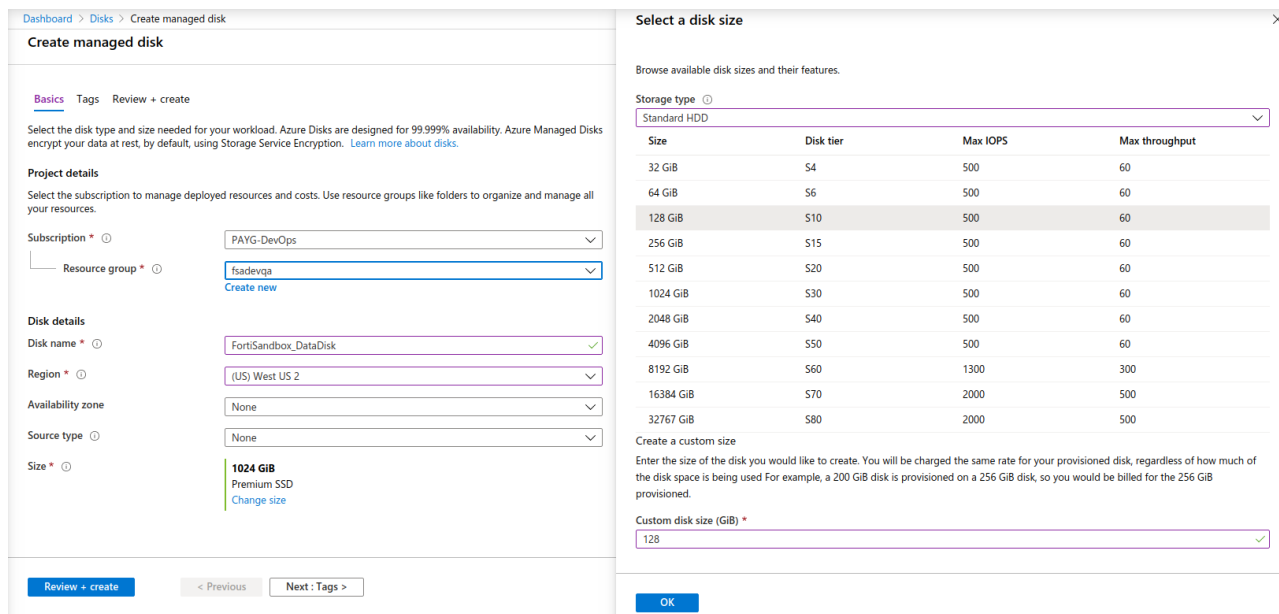


Creating a data disk

Before upgrading to v3.2.0, create a data disk and attach it to FortiSandbox.

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 64GB.





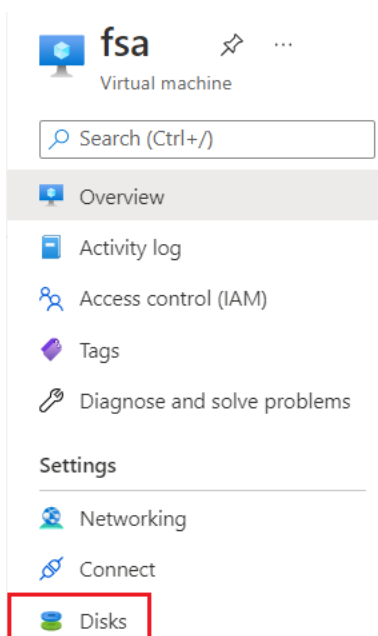
Keep monitoring the usage of data disk, expand the data disk size when needed. For more information, see the FortiSandbox [Best Practices and Troubleshooting Guide](#).

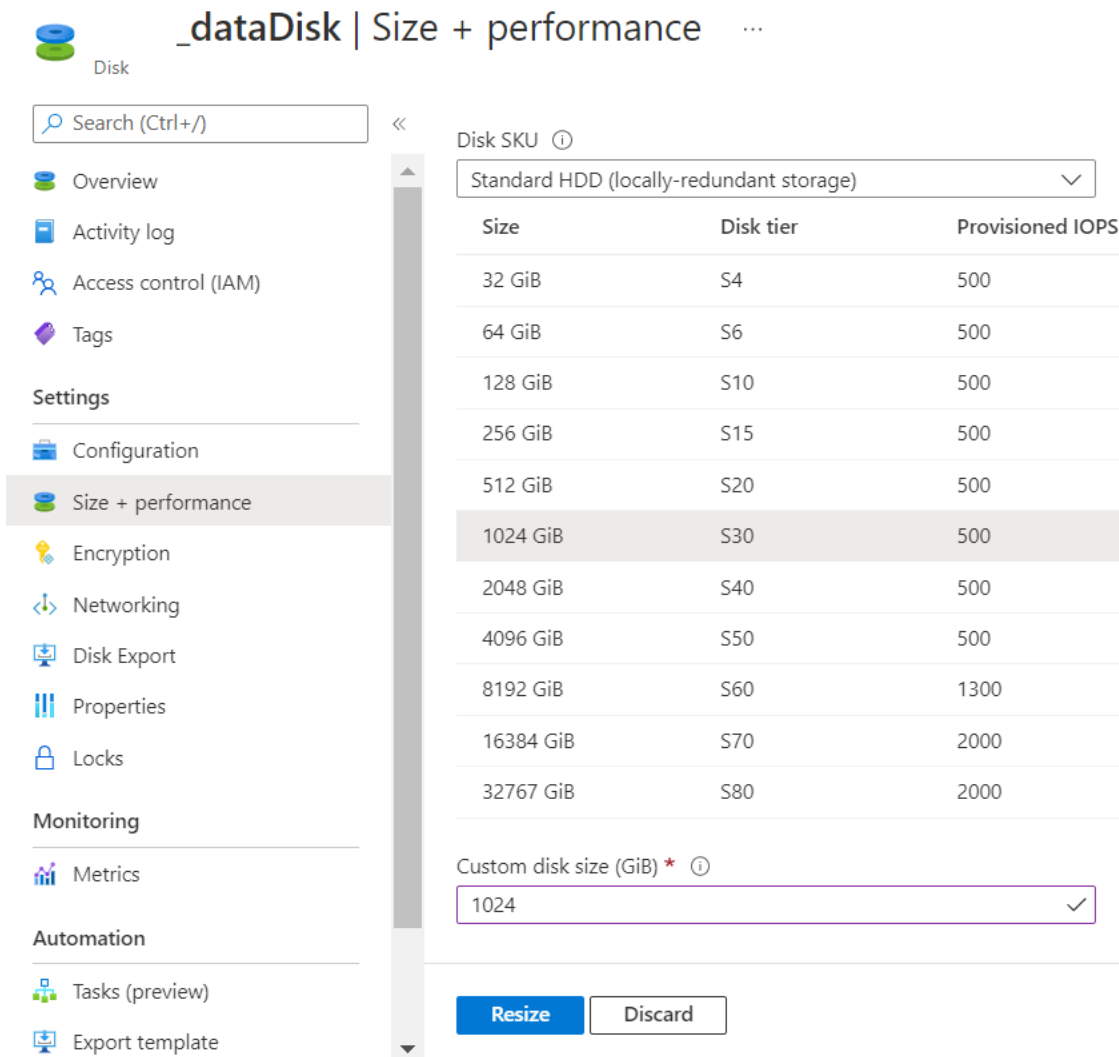
Re-size the Data Disk (highly-recommended)

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*.


_dataDisk | Size + performance

Search (Ctrl+/)

Overview
Activity log
Access control (IAM)
Tags
Settings
Configuration
Size + performance
Encryption
Networking
Disk Export
Properties
Locks
Monitoring
Metrics
Automation
Tasks (preview)
Export template

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

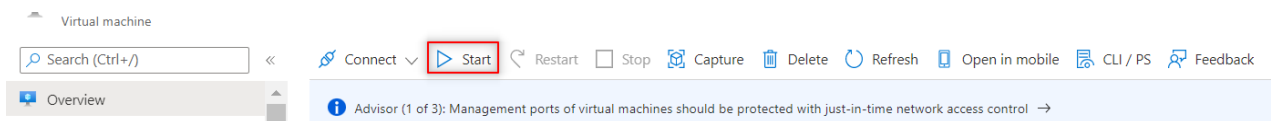
Custom disk size (GiB) * ⓘ

1024 ✓

Resize Discard

4. Refresh the Azure Portal and ensure the disk size has been updated.

5. On the Azure Portal, start FortiSandbox.



Virtual machine

Search (Ctrl+/)

Connect ▼ **Start** Restart Stop Capture Delete Refresh Open in mobile CLI / PS Feedback

Overview

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.

```

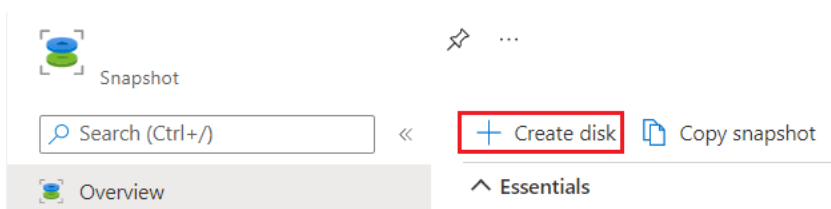
- After FortiSandbox reboots, run the CLI command `status commnad` to verify the `Disk Size` is correct.

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

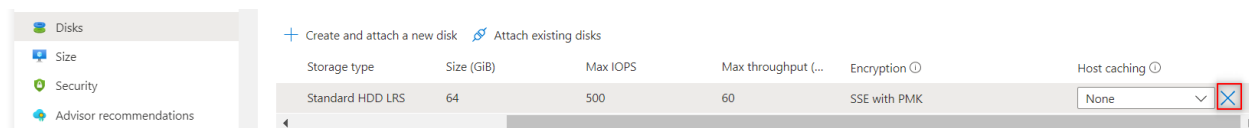
- On the Azure Portal, stop the FortiSandbox instance.
- Go to *Data disk > Create snapshot*.



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



- Detach the old data disk.



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 *

Resource group *
[Create new](#)

Instance details

If you need to create a legacy storage account type, please click [here](#).

Storage account name ⓘ *

Region ⓘ *

Performance ⓘ *

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

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

Redundancy ⓘ *

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

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

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.

Importing Azure settings into FortiSandbox

When the FSA instance is deployed, you can import your Azure settings into FortiSandbox.

Uploading the rating and tracer engine

After upgrading FortiSandbox, you must manually upload the rating and tracer engine.

To manually upload the rating and tracer engine:

1. In FortiSandbox, go to *System > FortiGuard*.
2. Beside *Upload Package File*, click *Choose file* and locate the rating or tracer engine to be uploaded.

FortiSandbox Azure		FortiGuard				>_	🔔	?	admin
	Module Name	Current Version	Last Check Time	Last Update Time	Last Check Status				
Favorites	AntiVirus Scanner	00006.00258	2021-04-15 17:15:04	2021-04-13 17:42:59	Already Up-to-date				
	AntiVirus Extended Signature	00085.04260	2021-04-15 17:15:13	2021-04-15 17:15:13	Successful				
Dashboard	AntiVirus Active Signature	00085.04770	2021-04-15 17:15:06	2021-04-15 17:15:06	Successful				
	AntiVirus Extreme Signature	00085.04500	2021-04-15 17:15:37	2021-04-15 17:15:37	Successful				
Security Fabric	Network Alerts Signature	00002.03379	2021-04-15 17:15:37	2021-04-15 16:37:28	Already Up-to-date				
	Sandbox System Tools	04000.00084	2021-04-15 17:15:37	2021-04-08 17:22:38	Already Up-to-date				
Scan Job	Sandbox Rating Engine	04000.00030	2021-04-15 17:15:37	2021-03-11 17:07:22	Already Up-to-date				
	Windows Tracer Engine	04000.00011	2021-04-15 17:15:37	2021-03-15 21:10:36	Already Up-to-date				
Scan Policy and Object	Android Tracer Engine	04000.00007	2021-04-15 17:15:37	2021-01-18 11:14:19	Already Up-to-date				
	Linux Tracer Engine	04000.00007	2021-04-15 17:15:37	2021-03-18 16:26:56	Already Up-to-date				
Upload Package File:		<input type="button" value="Choose File"/>	sandbox_engi...c1e.rating.pkg			🔄 Uploading ...			

To import Azure settings into FSA:

1. Go to the FortiSandbox GUI.
2. Click *System > Azure Config*.
If you get a warning that the rating and tracer engine is not available or up-to-date, manually upload the rating and tracer engine before doing this procedure.
3. FortiSandbox v3.2.0 and higher supports service principal and Azure account authentication methods.
 - a. If you choose service principal, get the service principal information by going to the Azure portal to the *Azure Active Directory > App registrations* to find the service principal information in the application you created.

Search resources, services, and docs (G+)

Dashboard > azurestorefortinet (Default Directory) > App registrations > fsadevqasp

fsadevqasp

Search (Ctrl+ /) << Delete Endpoints

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](#)

Call APIs

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


[View API permissions](#)

Sign in users in 5 minutes


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


[View all quickstart guides](#)


- b. Enter the following Azure configuration settings and then click *Submit*.



FortiSandbox


Azure



 Azure Config



 Favorites



 Dashboard


 Security Fabric


 Scan Job


 Scan Policy and Object


System


 Log & Report

Configure Azure

Overview

Account Type	Client id
Client ID	
Client Secret	
Location	
Tenant ID	
Subscription ID	
Resource group	
Storage account	
Storage account access key	
Monitor storage account	
Monitor account access key	
Network security group	
Virtual network	
Subnet	
VM Type	

Client id	Application (client) ID.
Client Secret	Client secret value.
Location	The location you used to set up the resource group.
Tenant id	Directory (tenant) ID.
Subscription ID	Your subscription ID.
Resource group	Resource group.
Storage account	Storage account name.

Storage account access key	Storage account access key.
Monitor storage account	Monitor account name.
Monitor account access key	Monitor account access key.
Network security group	The security group created. If you created multiple security groups, use the one that allows RDP and FTP.
Virtual network	Name of the virtual network you created.
Subnet	The subnet you created for the FSA port2 interface.
VM Type	The VM type of custom VM clone(s), <i>Standard_B4ms</i> recommended.

4. FortiSandbox v3.2.0 and higher supports service principal and Azure account authentication methods.
- a. If you choose Azure account authentication, click *System > Azure Config*.

FortiSandbox Azure Azure Config Regular Mode admin

Configure Azure

Edit

Account Type Microsoft Azure account email

Microsoft Azure account email

Microsoft Azure account password

Location

Subscription ID

Resource group

Storage account

Storage account access key

Monitor storage account

Monitor account access key

Network security group

Virtual network

Subnet

VM Type

Previous Test Connection Submit

b. Enter the following information:

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	Resource group.
Storage account	Storage account name.
Storage account access key	Storage account access key.
Monitor storage account	Monitor account name.
Monitor account access key	Monitor account access key.
Network security group	The security group created. If you created multiple security groups, use the one that allows RDP and FTP.
Virtual network	Name of the virtual network you created.
Subnet	The subnet you created for the FSA port2 interface.
VM type	The VM type of custom VM clone(s), <i>Standard_B4ms</i> recommended.

c. Click *Test Connection* to verify the connection is accessible and authentication is valid. Then click *Submit*.**5.** When completed, upload your BYOL license if provided.

The Azure FortiSandbox will fetch the licensing information which can take up to three hours.

Reduce scan time in custom Windows VM

Keep custom VM clones running to reduce scan time.

To reduce the scan time in a custom Windows VM:

1. Go to the *Azure Config* page
2. Click *Configure Wizard* and enable *Allow Hot-Standby VM*.
3. Click *Submit*. 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

Apply

4. After `vminit` done, go to the Azure portal to check that the clone(s) are have kept running with /without a scan job. Allow 2-3 minutes for a custom VM clone to restore status after a scan job done. Afterwards, the clone will keep running and standby for the next scan job to reduce VM scan time.



It is highly recommended that enabled clone number is double or more than incoming scan jobs number.

Ensure clone(s) are keep running in the Azure portal before submitting scan jobs.

Example 1: Scan two files/urls at the same time

To scan two files/urls at the same time in windows 10x64 custom VM, it's best to have 4 running clones of Windows 10x64 custom VM.

Example 2: Scan files in a compressed file or text file

To scan files in a compressed file or urls in a text file, it's best to count the total number of files/urls before enabling the custom VM clone number. If there are 6 files included in a compressed file and you are forcing them to scan in windows 10x64 custom VM, you should enable a minimum of 12 clones windows of 10x64 custom VM. After `vminit` is complete, go to the Azure portal, and confirm that all 12 clones are running , and then submit the scan file.

Example 3: Scanning more files

If you are already scanning files/urls and need to scan more files/urls, wait until the previous jobs are completed, and custom VM clone(s) is/are restored completely. Afterwards, confirm the clones are running from the Azure portal. If all clones are restarted and running, you can submit new jobs with good performance of custom VM.

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.

Configuring 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.

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.
- FortiSandbox reserved port2 for custom VM communication hardcoded

To create multiple FortiSandbox instances on Azure:

1. Create at least three network interfaces on Azure for each FortiSandbox Azure.

The second network interface is for the custom VM.

The third network interface is for HA communication.

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.

Dashboard > Resource groups > fsadevqa > FortiSandbox_release | Networking > FortiSandbox_Port1 | IP configurations

FortiSandbox_Port1 | IP configurations

Search (Ctrl+/) « **+ Add** Save Discard

Overview
Activity log
Access control (IAM)
Tags
Settings
IP configurations
DNS servers
Network security group
Properties
Locks
Export template

IP forwarding settings
IP forwarding: Disabled Enabled
Virtual network: fsadevqaVN
IP configurations: fsadevqaSN_port1 (10.20.0.0/24)
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 [Importing Azure settings into FortiSandbox on page 26](#) 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.

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. In the FortiSandbox Azure GUI, go to *Scan Policy and Object > VM Settings* and change *Clone #* to 1 for each node. After all VM clones on all nodes are configured, you can change the *Clone #* to a higher number.
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.

Change Log

Date	Change Description
2022-04-12	Initial release.



www.fortinet.com

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