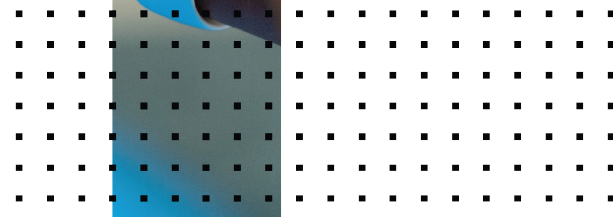


Azure Guide

FortiSandbox 4.2.1



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 25, 2023

FortiSandbox 4.2.1 Azure Guide

34-421-829490-20230425

TABLE OF CONTENTS

About FortiSandbox VM for Azure	4
Preparing for deployment	5
Licensing	5
Minimum system requirements	6
Port usage	7
Deployment	8
Set up the Azure environment for FortiSandbox	8
Create a resource group	9
Create network security groups	9
Create virtual networks	11
Create storage accounts	13
Create network interfaces	15
Create a data disk	17
Deploy FortiSandbox VM on Azure (PAYG / BYOL)	17
Deploy FortiSandbox instance on Azure using the GUI	17
Deploy FortiSandbox instance on Azure using the CLI	24
Prepare FortiSandbox for scanning contents	25
Upload the license file	25
Import Azure settings into FortiSandbox	26
Import using Account Authentication	26
Import using Service Principal	28
(Optional) Create an App registration	31
Advanced configurations	36
Set up the local custom VM	36
Using HA-Cluster	41
Configure an HA cluster	42
Appendix A - Reduce scan time in custom Windows VM	45
Appendix B - How to re-size the Data Disk	46
Change Log	50

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.

Preparing for deployment

Prepare for deployment by reviewing the following information:

- [Licensing on page 5](#)
- [Minimum system requirements on page 6](#)
- [Port usage on page 7](#)

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. To 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 6 .

Minimum system requirements

Before deploying the FortiSandbox virtual appliance, install and configure the latest stable release of VMware vSphere ESXi Hypervisor software. Supported versions are ESXi version 5.1 to 7.0.1.

Access VMware vSphere using a web browser or install the VMware vSphere client.

In VMware, you can expose full CPU virtualization to the guest operating system so that applications that require hardware virtualization can run on virtual machines without binary translation or paravirtualization. For more information, see https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.vm_admin.doc/GUID-2A98801C-68E8-47AF-99ED-00C63E4857F6.html.

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	Public Cloud - PAYG
Hypervisor Support	VMware ESXi Microsoft Hyper-V Windows server 2016 and 2019		AWS 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.	
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.	
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	
VM Clones Support (Min/Max)	0 ¹ / 8 (Local VMs) and 200 (Cloud VMs)	0 ¹ / 216 ²	0 ¹ / 128 ³

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.

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*.

Deployment

To deploy FortiSandbox-VM:

- ☐ [Set up the Azure environment for FortiSandbox on page 8](#)
- ☐ [Deploy FortiSandbox VM on Azure \(PAYG / BYOL\) on page 17](#)
- ☐ [Prepare FortiSandbox for scanning contents on page 25](#)
- ☐ [Import Azure settings into FortiSandbox on page 26](#)

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.

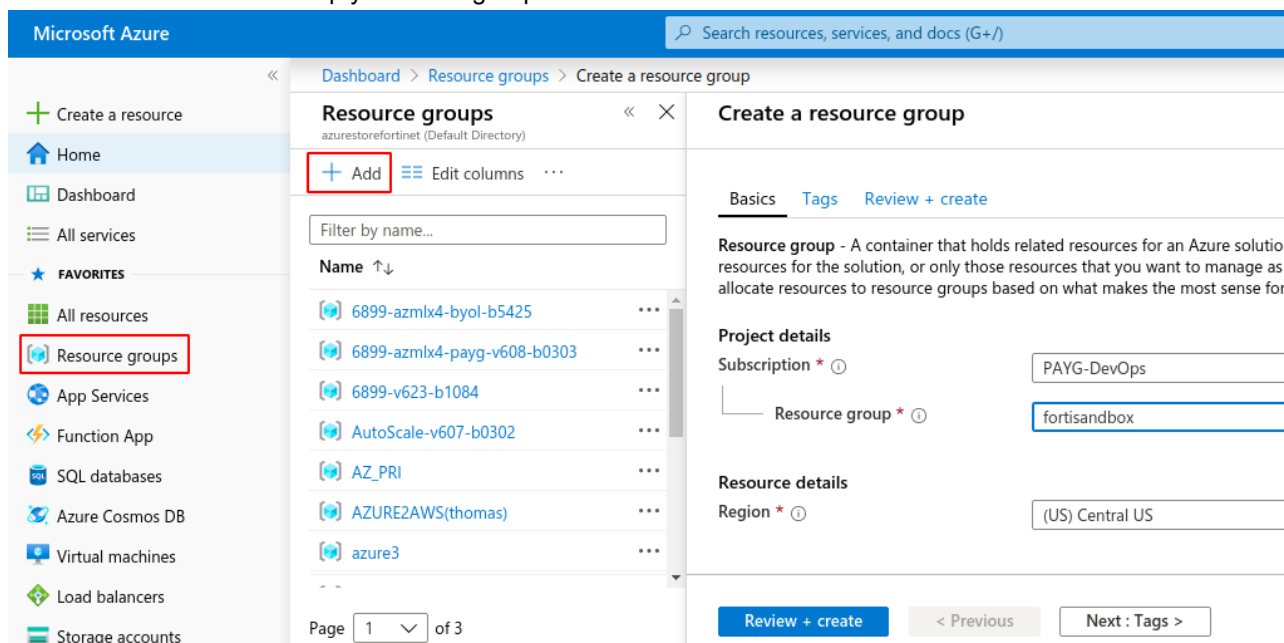
To set up the Azure environment for deployment:

1. [Create a resource group on page 9](#)
2. [Create network security groups on page 9](#)
3. [Create virtual networks on page 11](#)
4. [Create storage accounts on page 13](#)
5. [Create network interfaces on page 15](#)
6. [Create a data disk on page 17](#)

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.



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).

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.

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

- Name:** fortisandbox_VN
- Address space:** 10.45.0.0/16 (10.45.0.0 - 10.45.255.255 (65536 addresses...))
- Subscription:** PAYG-DevOps
- Resource group:** fortisandbox
- 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
- Service endpoints:** Disabled
- Firewall:** Disabled

3. Enter the following information:

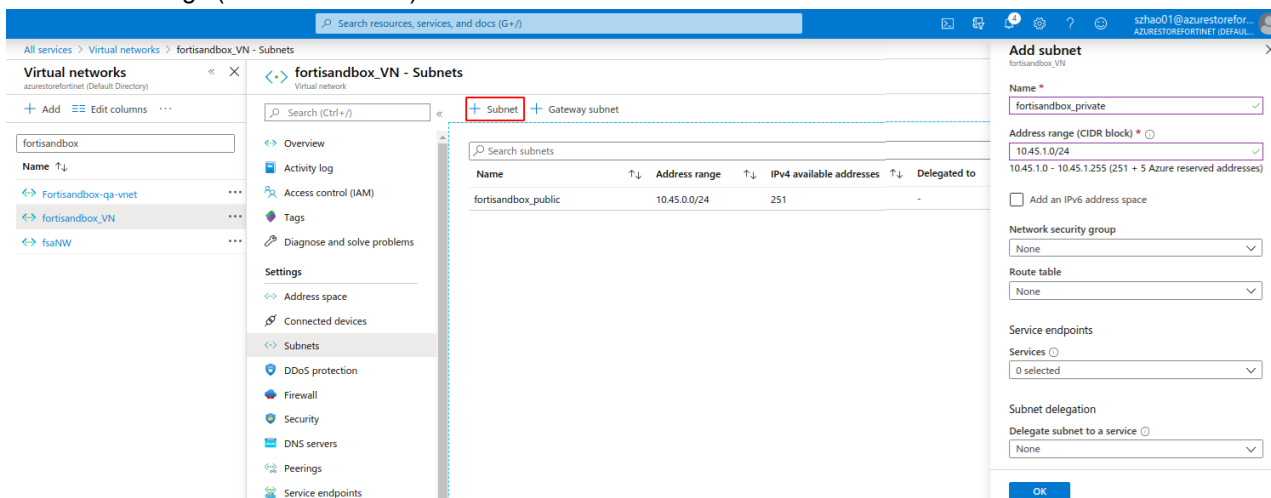
Name	Name of the virtual network.
Address space	Use an Azure suggested unused class B network (xxx.xxx.0.0/16) or enter your preferred unused class B network. The address space should cover all the IP ranges this resource group will use.
Subscription	Select your subscription type.

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*.

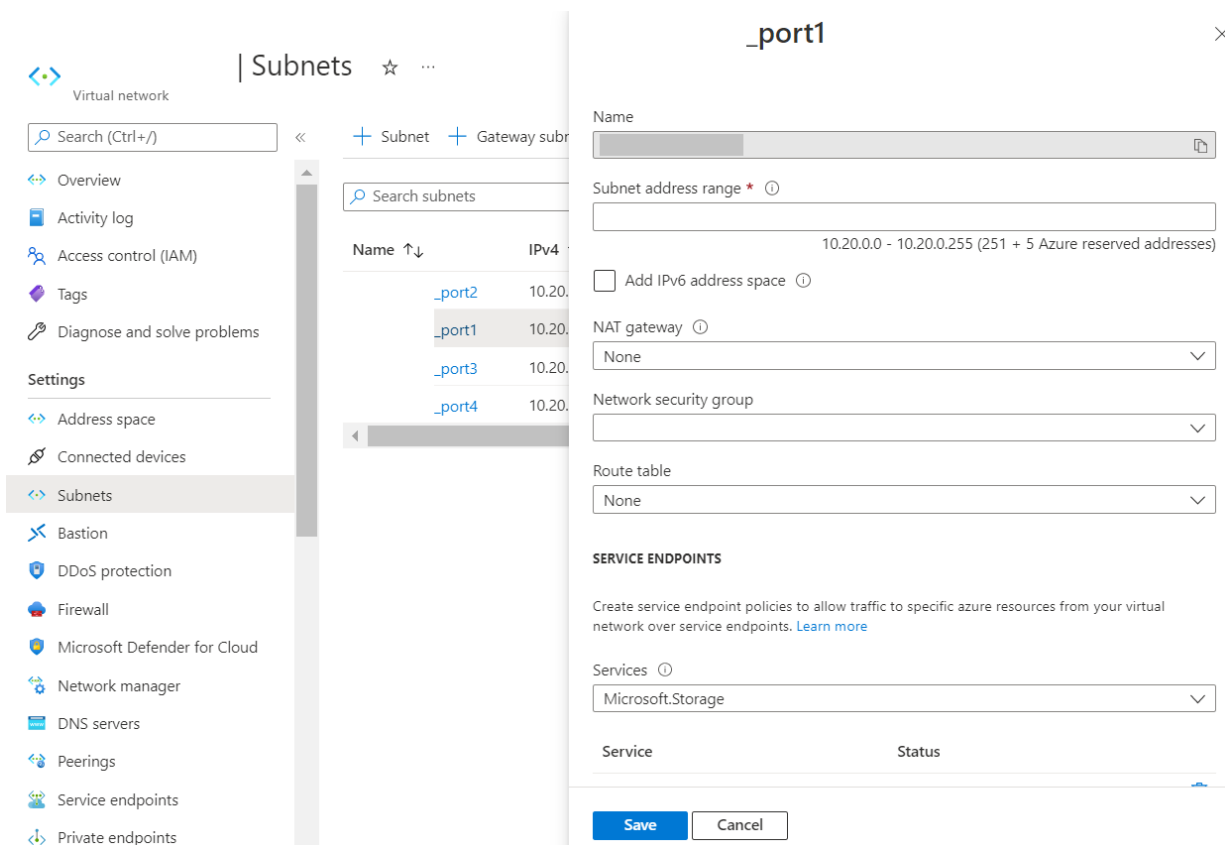
5. Create one additional subnet in the virtual network:

- 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).



6. Associate network security group to subnet.

- Associate the network security group for FortiSandbox port1 subnet to port1 subnet
- Associate the network security group for FortiSandbox port2 subnet to port2 subnet



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.

[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 *

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 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.

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

- Name ***: fsa_eth0_public
- Virtual network ***: fortisandbox_VN
- Subnet ***: fortisandbox_private (10.45.1.0/24)
- Private IP address assignment**: Dynamic (selected), Static
- 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 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

OK

Cancel

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

Project details

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

Subscription *

Resource group * [Create new](#)

Disk details

Disk name *

Region *

Availability zone

Source type

Size * [Change size](#)

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

Select a disk size

Browse available disk sizes and their features.

Storage type

Size	Disk tier	Max IOPS	Max throughput
32 GiB	\$4	500	60
64 GiB	\$6	500	60
128 GiB	\$10	500	60
256 GiB	\$15	500	60
512 GiB	\$20	500	60
1024 GiB	\$30	500	60
2048 GiB	\$40	500	60
4096 GiB	\$50	500	60
8192 GiB	\$60	1300	300
16384 GiB	\$70	2000	500
32767 GiB	\$80	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) *

[OK](#)



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)

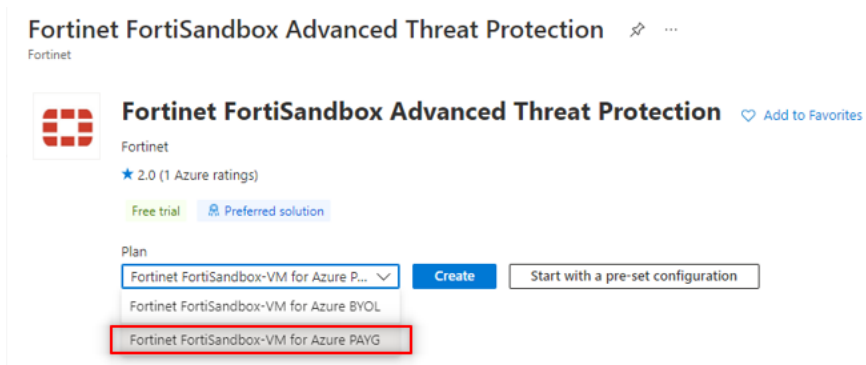
You can deploy FortiSandbox VM using the Azure GUI or CLI:

- [Deploy FortiSandbox instance on Azure using the GUI](#)
- [Deploy FortiSandbox instance on Azure using the CLI](#)

Deploy FortiSandbox instance on Azure using the GUI

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*.



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.
Authentication type	Click <i>Password</i> or <i>SSH public key</i> .

[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 *	<div>PAYG-DevOps</div>
Resource group *	<div>(New) Resource group</div> <div>Create new</div>

Instance details

Virtual machine name *	<div></div>
Region *	<div>(US) West US 2</div>
Availability options	<div>Availability zone</div>
Availability zone *	<div>Zones 1</div>
<div> You can now select multiple zones. Selecting multiple zones will create one VM per zone. Learn more</div>	
Security type	<div>Standard</div>
Image *	<div> Fortinet FortiSandbox-VM for Azure PAYG - Gen1</div> <div>See all images Configure VM generation</div>
Run with Azure Spot discount	<div><input type="checkbox"/></div>
Size *	<div>Standard_A4_v2 - 4 vcpus, 8 GiB memory (US\$1,576.07/month)</div>

Administrator account

Authentication type	<div><input checked="" type="radio"/> SSH public key</div> <div><input type="radio"/> Password</div>
<div> 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.</div>	
Username *	<div>azureuser</div>
SSH public key source	<div>Use existing key stored in Azure</div>
Stored Keys	<div>fsadevqa_key</div>

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

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

OS disk type	Select the disk type depending on your needs
Data disk for	Select <i>Create and attach a new disk</i> or <i>Attach an existing disk</i> .

Dashboard > Marketplace > Fortinet FortiSandbox Advanced Threat Protection >

Create a virtual machine ...

Basics Disks Networking Management Advanced Tags Review + create

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

Disk options

OS disk type * ⓘ 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 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 ⓘ
Create and attach a new disk Attach an existing disk					

▼ Advanced

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

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

i This VM image has preconfigured NSG rules

i 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.

Review + create

< Previous

Next : Management >

6. It is highly 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 ⓘ

 Some patch orchestration options are not available for this image. [Learn more](#)





[Review + create](#)


[< Previous](#)

[Next : Advanced >](#)


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.

 Delete  Cancel  Redeploy  Refresh

 We'd love your feedback! →

Your deployment is complete

 Deployment name: CreateVm-fortinet.fortinet_fortisandbox_vm-for... Start time:
Subscription: [PAYG-DevOps](#) Correlation ID:
Resource group:

▼ **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](#) [Create another VM](#)

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


Virtual machine


Search (Ctrl+ /)

 Connection monitor (classic)


 Workbooks


Automation


 Tasks (preview)


 Export template


Support + troubleshooting


 Resource health


 Boot diagnostics





 Performance diagnostics

 VM Inspector (Preview)

 Reset password

 Redeploy + reapply

 Serial console

Feedback    

```
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/
1          None      None      None      2022-    21:18:01.689358+00:00    Microsoft.Compute/virtualMachines      None      None      Succeeded      None
1db9dbeeaf 1          3aaa400e-1e35-41a3-b4c8-99f
```

12. Prepare FortiSandbox for scanning contents. See [Import Azure settings into FortiSandbox on page 26](#).

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 26](#).

Prepare FortiSandbox for scanning contents

To prepare the FortiSandbox instance for scanning:

1. [Upload the license file on page 25](#)
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 26](#)
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 31](#)
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.

- [Import using Account Authentication](#)
- [Import using Service Principal](#)

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.

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.
Storage account	Storage account name.
Storage account access key	Storage account access key.
Network security group	The security group you created for FortiSandbox port2.
Virtual Network	Name of the virtual network you created.
Subnet	The subnet you created for the FortiSandbox port2 interface.
VM type	The VM type of custom VM clone(s). <ul style="list-style-type: none">• Minimum: <i>Standard_B2ms</i>• Recommended: <i>Standard_B2ms</i>

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

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 31](#).
2. Go to *Manage > Certificates & Secrets*. The service principal information is located in the *Application (client) ID* and

Directory (tenant) ID fields.

The screenshot shows the Azure portal interface for an application registration named 'fsadevqasp'. The breadcrumb navigation at the top indicates the path: Dashboard > azurestorefortinet (Default Directory) > App registrations > fsadevqasp. The left-hand navigation pane includes sections for Overview, Quickstart, Manage (with sub-items like Branding, Authentication, Certificates & secrets, Token configuration, API permissions, etc.), and Support + Troubleshooting. The 'Certificates & secrets' item is highlighted with a red box. The main content area displays the application's details, including the Display name 'fsadevqasp', Application (client) ID, Directory (tenant) ID (highlighted with a red box), and Object ID. Other details like Supported account types, Redirect URIs, and Application ID URI are also visible. Below the details, there are sections for 'Call APIs' and 'Sign in users in 5 minutes'.

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*.

Client id	Enter the <i>Application (client) ID</i> 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 <i>Directory (tenant) ID</i> from the Azure portal.
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 you created for FortiSandbox port2.
Virtual network	Name of the virtual network you created.
Subnet	Use the subnet created for the local Windows or Linux VM communication (port2) if one exists. Otherwise, select the management subnet.
VM Type	The VM type of custom VM clone(s). <ul style="list-style-type: none">• Minimum: <i>Standard_B2ms</i>• Recommended: <i>Standard_B2ms</i>

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	




(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*.

App registrations

 New registration  Endpoints 

3. Register a new application.

Name	Enter the application display name.
Supported account types	Select <i>Accounts in this organizational directory only (Default Directory only – Single tenant)</i> .
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.

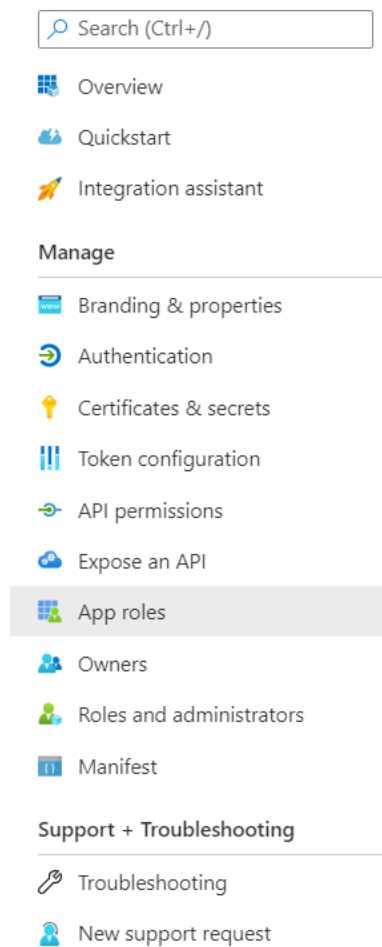
Select a platform 

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](#) 

Register

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 <i>Both (Users/Groups + Applications)</i> .

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*.

Manage

- Branding & properties
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions

Application registration certificates, secrets

Certificates (0) **Client secrets (1)**

A secret string that the application uses to

+ 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	<i>ReadWrite</i> This allows FortiSandbox to read, create, update, and delete the signed-in user's files.
User	<i>Read</i> 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*.

Advanced configurations

You can create a custom Windows VM for Azure. You also have the option of setting up multiple FortiSandbox Azure instances in a load-balancing HA (high availability) cluster.

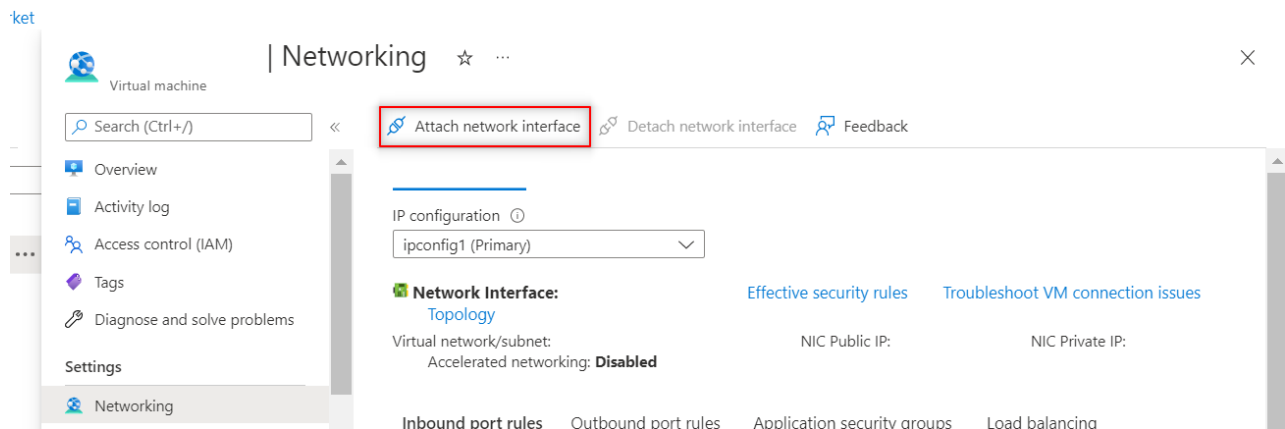
- [Set up the local custom VM on page 36](#)
- [Using HA-Cluster on page 41](#)

Set up the local custom 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. The FortiSandbox instance uses port2 to communicate with local Windows or Linux clones. For information, see [To create a network interface in Azure](#) in [Create network interfaces on page 15](#).
3. Attach this network interface to FortiSandbox VM instance as FSA Port2.



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.

Dashboard > Resource groups > fsa > fsa image | Access keys ☆ ...

Storage account

Search (Ctrl+/)

Overview

Activity log

Tags

Diagnose and solve problems

Access Control (IAM)

Data migration

Events

Storage browser

Data storage

Containers

File shares

Queues

Tables

Security + networking

Networking

Azure CDN

Access keys

Set rotation reminder Refresh

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-image

key1 Rotate key

Key
..... Show

Connection string
..... Show

key2 Rotate key

Key
..... Show

Connection string
..... Show

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 using the `azure-vm-customized` CLI command. For more information about the `vm-customized` command, see the [FortiSandbox CLI Reference Guide](#) in the Fortinet Document Library.



- 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 the Azure custom VM from a blob:

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 the Azure custom VM from disk:

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]
```

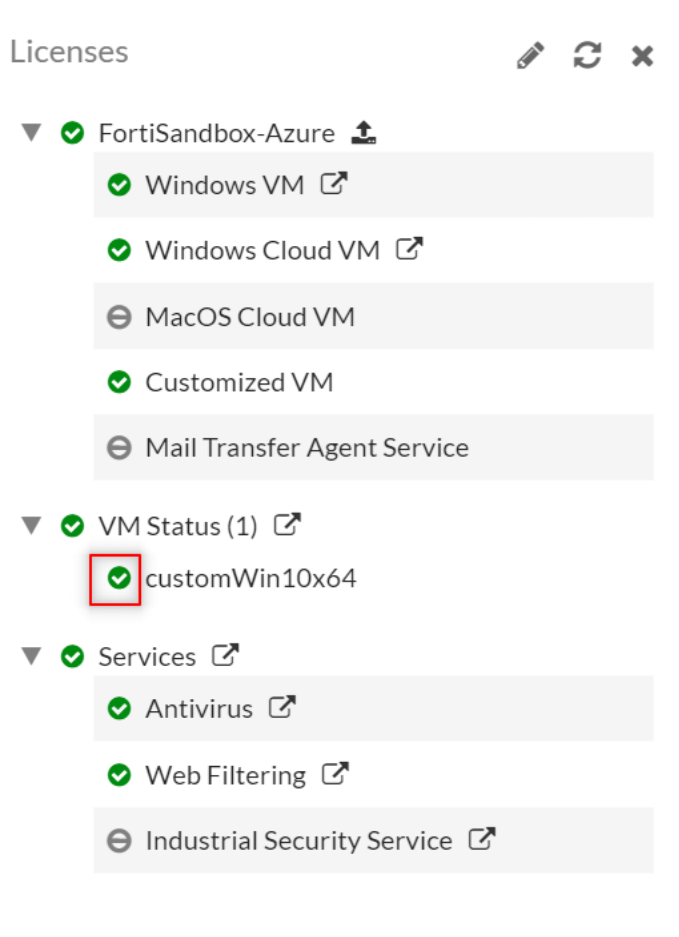
Test FortiSandbox instance with a file scan:

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 xlsx 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*.



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

Submit

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

- Dashboard
- Security Fabric
- Scan Job**
- Job Queue
- VM Jobs
- File Job Search
- URL Job Search
- Overridden Verdicts
- File On-Demand**
- URL On-Demand

Submit File
Show Rescan Job

🔄
🔍 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	

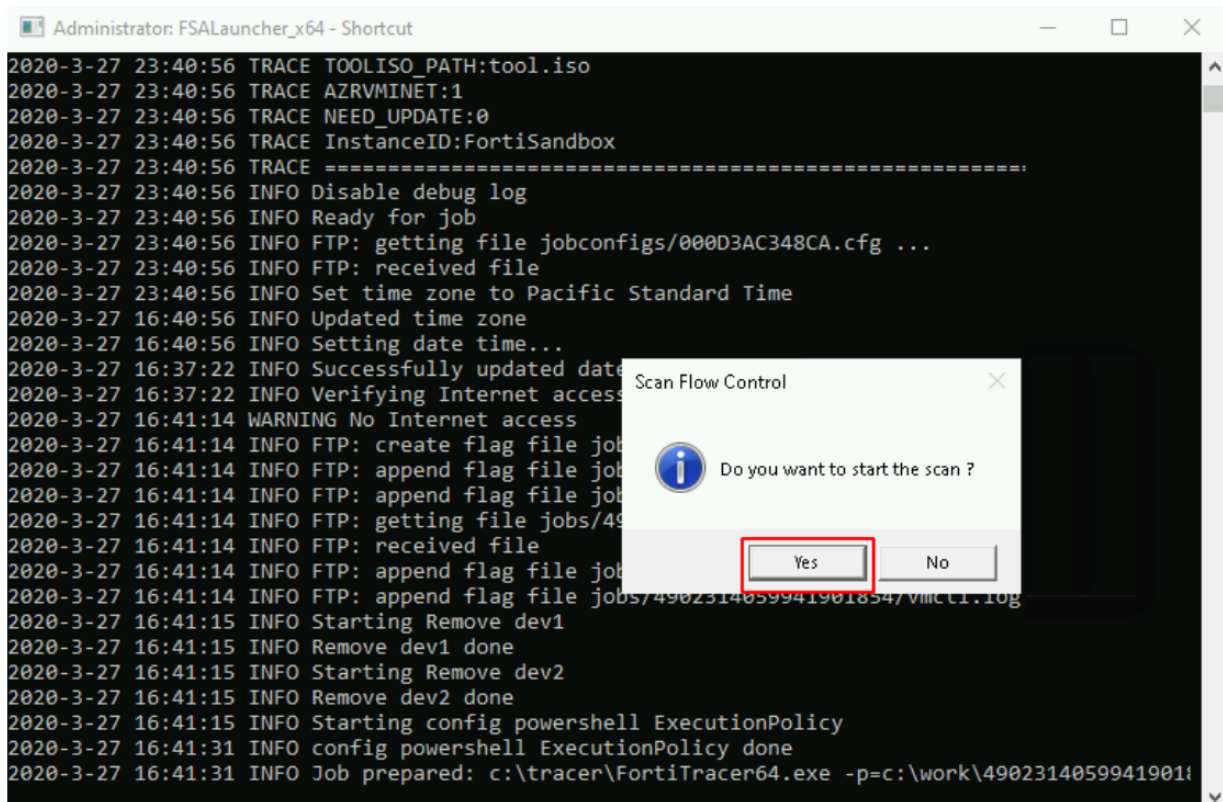
6. (Optional) Interaction with a custom VM clone during scan:

- 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.



- 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.

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.

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.

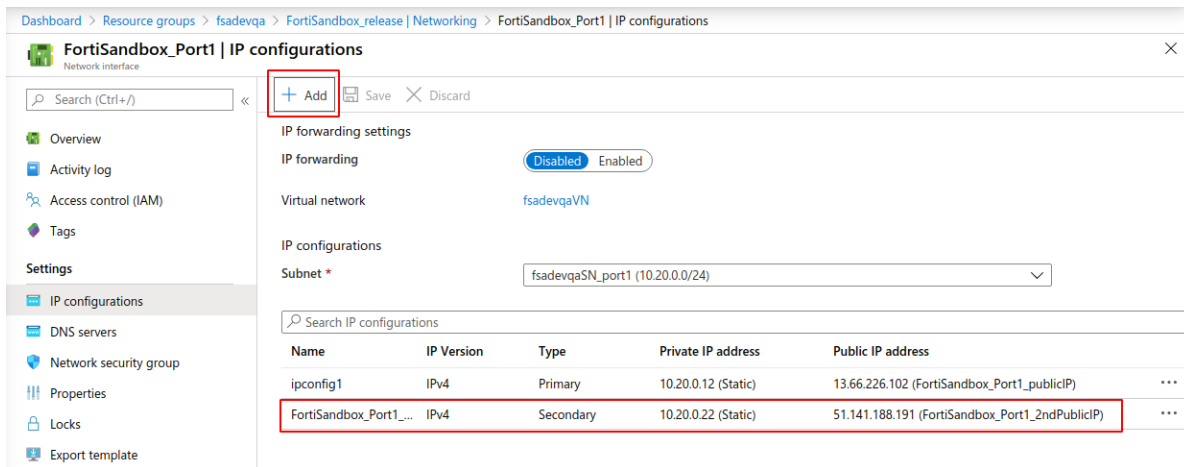
The second network interface is for the custom VM.

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.



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 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.

Appendix A - 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 Apply

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.



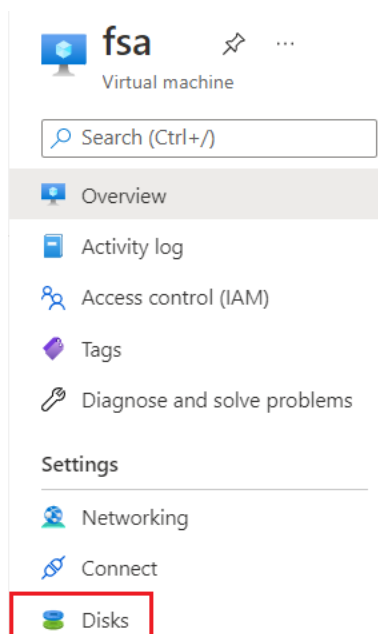
For this feature to work better we recommend enabling more clones than the maximum concurrent dynamic scan jobs, so when a new dynamic scan job is started, there are stand-by clones available immediately.

Appendix B - 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*.



- 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

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

- 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.

```

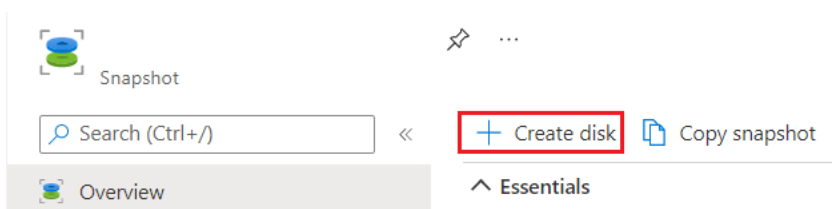
- After FortiSandbox reboots, run the CLI command `status commnad` to verify the Disk Size is correct.

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

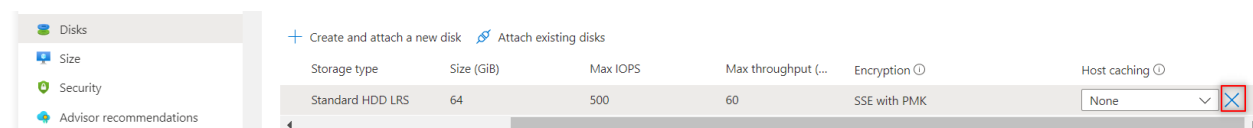
- On the Azure Portal, stop the FortiSandbox instance.
- Go to *Data disk > Create snapshot*.



- 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.

- Run the CLI command: `resize-hd`.
- After FortiSandbox reboots use the CLI command `status` to verify the Disk Size is correct.

Change Log

Date	Change Description
2022-08-17	Initial release.
2023-03-02	Updated (Optional) Create an App registration on page 31
2023-03-22	Updated Port usage on page 7



www.fortinet.com

Copyright© 2023 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.