

Azure Guide

FortiSandbox 4.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



May 03, 2021

FortiSandbox 4.0 Azure Guide

34-40-714970-20210503

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	14
Creating storage accounts	16
Creating network interfaces	17
Creating a data disk	19
Creating a FortiSandbox VM using the Azure CLI	20
Importing Azure settings into FortiSandbox	22
Uploading rating engine	22
Optional: Using a custom VM on Azure	26
Interaction with a custom VM clone during scan	29
Optional: Using a prebuilt custom VM on Azure	32
Optional: Creating a custom Windows 10 VM	33
Optional: Using HA-Cluster	34
Configuring an HA cluster	34
Change Log	37

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.

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 10 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.
 - Some 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.

Advantages

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

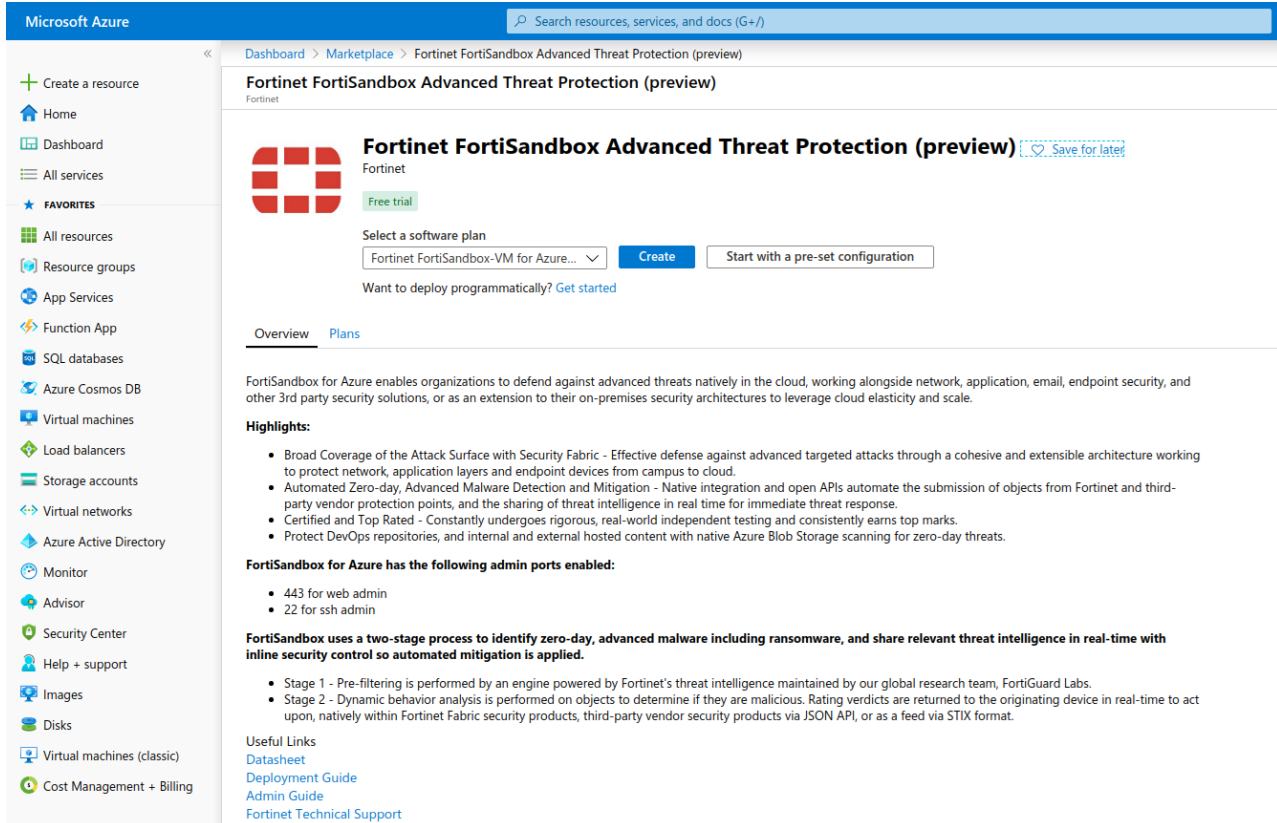
Limitations

- 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

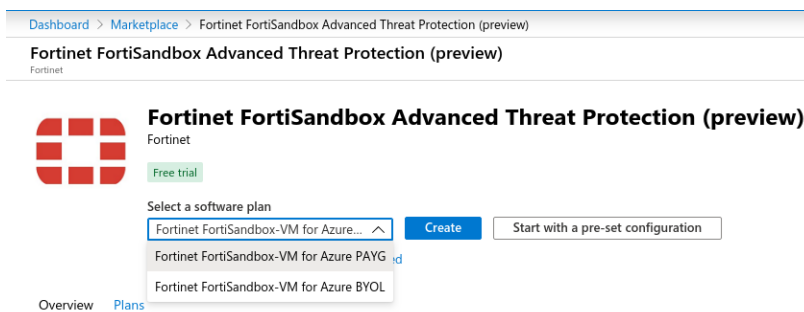
[Datasheet](#)

[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.

5. Click **Review + Create**.
6. 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

Standard A4 v2 by Microsoft
Terms of use | Privacy policy

Not covered by credits ⓘ
0.0000 USD/hr

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	jliang

DISKS

OS disk type	Standard SSD
Use managed disks	Yes

NETWORKING

Create Previous Next Download a template for automation

7. 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-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

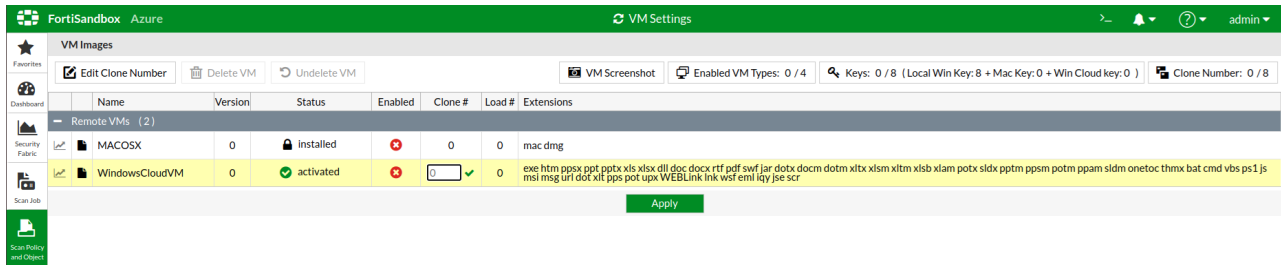
Last Updated: 04-15 23:06

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.

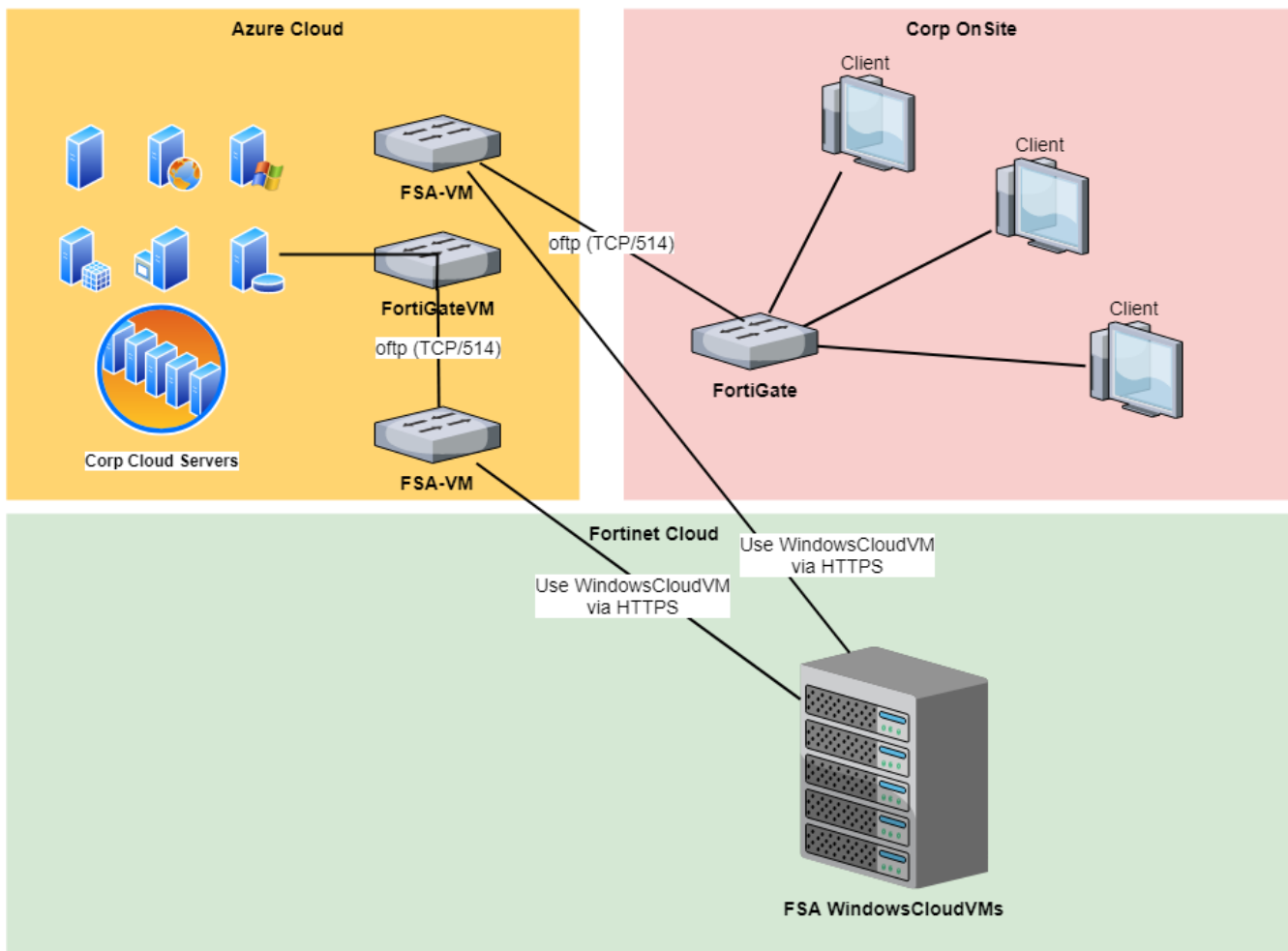
3. Go to *Scan Policy and Object > VM Settings* and select the *WindowsCloudVM*.

- 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. [Creating a FortiSandbox VM using the Azure CLI](#)
8. [Importing Azure settings into FortiSandbox](#)
9. [Optional: Using a custom VM on Azure](#)
10. [Optional: Using a prebuilt custom VM on Azure](#)
11. [Optional: Creating a custom Windows 10 VM](#)
12. [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 for creating a new resource group. The left-hand navigation pane shows the 'Resource groups' option highlighted. The main content area is divided into two sections. The top section, titled 'Resource groups', shows a list of existing resource groups with columns for Name and a three-dot menu. An 'Add' button is highlighted with a red box. The bottom section, titled 'Create a resource group', shows the 'Basics' tab selected. It contains 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, and OFTP.
- 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 the management port 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.
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.

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 displays the Microsoft Azure portal interface for creating a new virtual network. The left-hand navigation pane shows the 'Virtual networks' option selected. The main content area is divided into two sections: a list of existing virtual networks and a 'Create virtual network' form. In the list, the 'Add' button is highlighted with a red box. The 'Create virtual network' form is filled out with the following details:

- 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

The 'Create' button is visible at the bottom of the form.

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 port1 (the management subnet).
Subnet Address range	Enter a class C network (xxx.xxx.x.x/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.

The screenshot shows the Azure portal interface for creating a new storage account. On the left, the 'Storage accounts' option is highlighted in the navigation pane. The main area displays a list of existing storage accounts with names like 'aamdiddiag639', 'adabsaisdiag625', etc. A red box highlights the '+ Add' button. To the right, the 'Create storage account' wizard is open, showing the 'Basics' tab. The form includes fields for Subscription (Pay-As-You-Go), Resource group (jsmith-westus-fsa-3.0), Storage account name, Location (Canada Central), Performance (Standard), Account kind (StorageV2), Replication (Read-access geo-redundant storage), and Access tier (Hot). The 'Review + create' button is at the bottom.

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	Read-access geo-redundant storage.

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. The left sidebar displays the 'Network interfaces' section under 'All services', with the 'Add' button highlighted in a red box. The main area is titled 'Create network interface' and contains the following configuration 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
- Private IP address (IPv6)**: (unchecked)
- Subscription ***: PAYG-DevOps
- Resource group ***: fortisandbox (with a 'Create new' link below it)
- 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.

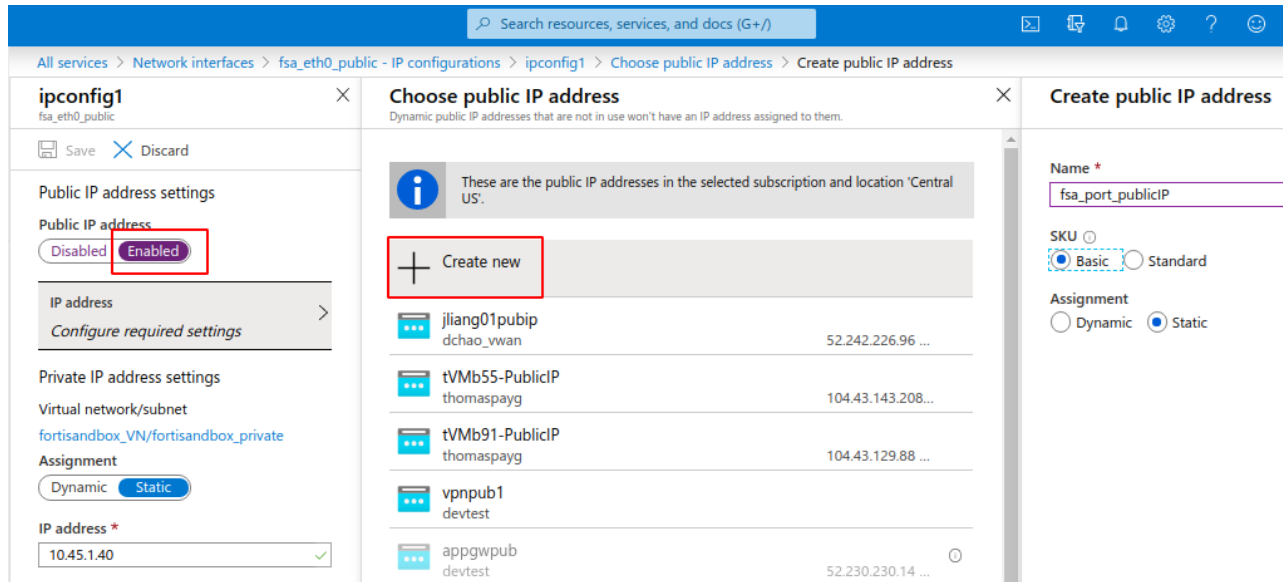


If you create multiple network security groups, the one associated with the FSA port1 interface must be under the security group which includes HTTPS (TCP 443), SSH traffic (TCP 22), OFTP traffic (TCP 514), and the one associated with the FSA port2 interface must be under the security group which includes FTP.

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

The screenshot shows the Azure portal interface for configuring a network interface. The breadcrumb trail is: All services > Network interfaces > fsa_eth0_public - IP configurations > ipconfig1. The left sidebar shows the 'Settings' section with 'IP configurations' highlighted. The main area displays the 'IP configurations' settings for 'fsa_eth0_public'. The 'IP forwarding' is set to 'Disabled'. The 'Virtual network' is 'fortisandbox_VN'. The 'Subnet' is 'fortisandbox_private (10.45.1.0/24)'. Below this is a table of IP configurations:

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

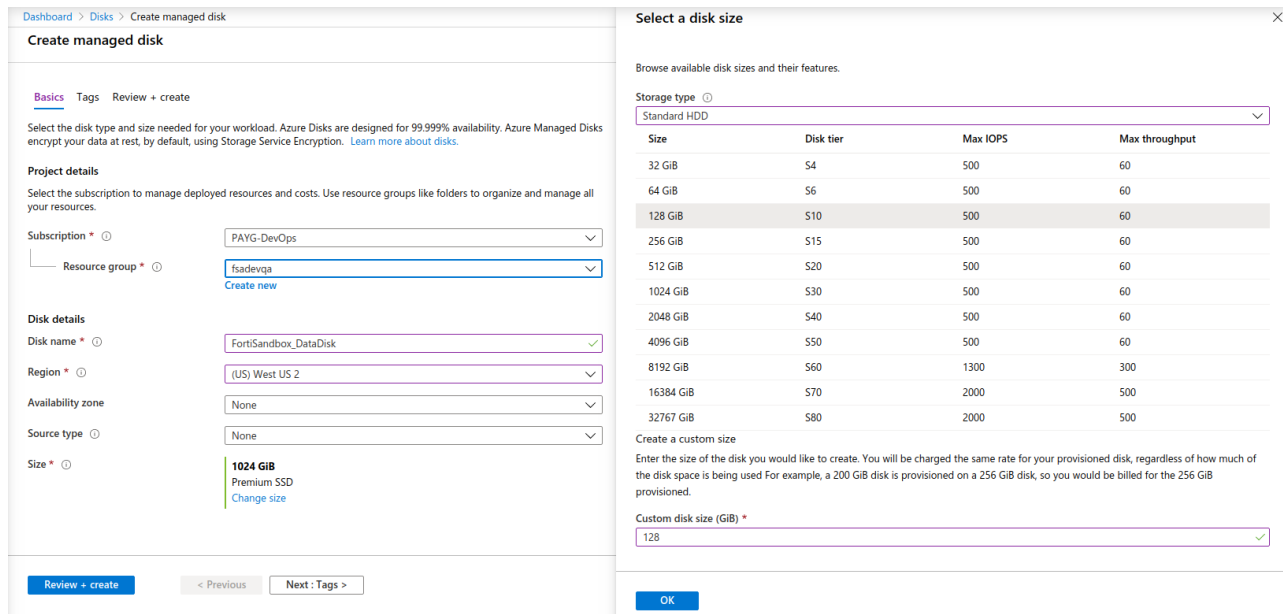


Creating a data disk

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.



Creating a FortiSandbox VM using the Azure CLI

To create the VM using the Azure CLI:

1. Because the Marketplace URN is subject to change without notice, get the latest FortiSandbox image URN using this command.

```
az vm image list -p fortinet -f fortinet_fortisandbox_vm --all --query "[].urn"
```

```
sylvia@sylvia-OptiPlex-3050:~$ 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_payg:3.1.00"
]
```

2. Create the Azure FortiSandbox using Azure CLI from the Azure Marketplace with the network interfaces 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:3.1.2" --size [vm size] --nics [NIC for port1] [NIC for port2] [NIC for port3] --attach-data-disks [attach_data_disks_name] --boot-diagnostics-storage [boot_diagnostics_storage_container_name] --generate-ssh-keys --verbose
```

```
sylvia@sylvia-OptiPlex-3050:~$ az vm create --resource-group fsadevqa --name FortiSandbox_release --image "fortinet:fortinet_fortisandbox_vm:fortinet_fsa-vm:3.1.2" --size Standard_A4 --nics FortiSandbox_Port1 FortiSandbox_Port2 FortiSandbox_Port3 FortiSandbox_Port4 --attach-data-disks FortiSandbox_DataDisk --boot-diagnostics-storage fsadevqa02debug --generate-ssh-keys --verbose
Use existing SSH public key file: /home/sylvia/.ssh/id_rsa.pub
Accepted: vm_deploy_QMWhFnZVzZeubnC715u2bmW7VjWw (Microsoft.Resources/deployments)
Accepted: FortiSandbox_release_OsDisk_1_adcd36909ee425ea19ca43464785986 (Microsoft.Compute/disks)
- Running ..
{
  "fqdns": "",
  "id": "/subscriptions/4f27b38c-ad3f-43d8-a9a3-01182e5e2f9a/resourceGroups/fsadevqa/providers/Microsoft.Compute/virtualMachines/FortiSandbox_release",
  "location": "westus2",
  "macAddress": "00-0D-3A-C3-42-25,00-0D-3A-C3-47-02,00-0D-3A-C3-45-C4,00-0D-3A-C3-4B-0D",
  "powerState": "VM running",
  "privateIpAddress": "10.20.0.12,10.20.1.12,10.20.2.12,10.20.3.12",
  "publicIpAddress": "13.66.226.102",
  "resourceGroup": "fsadevqa",
  "zones": ""
}
```

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:3.1.00" --size [vm size] --nics [NIC for port1] [NIC for port2] [NIC for port3] --attach-data-disks [attach_data_disks_name] --boot-diagnostics-storage [boot_diagnostics_storage_container_name] --generate-ssh-keys --verbose
```

3. Get the default admin password for the FSA VM using the Azure CLI.

The VM-ID UUID is the default password for admin access.

```
az vm list --output tsv -g [resource group name]
```

```
sylvia@sylvia-OptiPlex-3050:~$ az vm list --output tsv -g fsadevqa | grep FortiSandbox_release
None None None None None /subscriptions/4f27b38c-ad3f-43d8-a9a3-01182e5e2f9a/resourceGroups/fsadevqa/providers/Microsoft.Compute/virtualMachines/FortiSandbox_release
None None None None None westus2 FortiSandbox_release
Microsoft.Compute/virtualMachines None a041078a-ccc8-444e-b037-c1aeca977b None None Succeeded None fsadevqa None
```

4. Log into FortiSandbox using the default username *admin* and the password you retrieved in the previous step.

5. Go to the Azure portal and verify that the data disk is attached to FortiSandbox.

Dashboard > Resource groups > fsadevqa > FortiSandbox_release | Disks

FortiSandbox_release | Disks

Managed disks created since June 10, 2017 are encrypted at rest with Storage Service Encryption (SSE). You may also want to enable Azure Disk Encryption.

Ultra Disk compatibility is not available for this location.

Disk settings

Enable Ultra Disk compatibility ☐ Yes ☒ No

OS disk

Name	Size	Storage account type	Encryption	Host caching
FortiSandbox_release_OsDisk_1_adcda36969ee425ea19ca43464785986	1 GiB	Standard HDD	Not enabled	Read/write

Data disks

LUN	Name	Size	Storage account type	Encryption	Host caching
0	FortiSandbox_DataDisk	64 GiB	Standard HDD	Not enabled	None

+ Add data disk

6. In the FortiSandbox Dashboard, upgrade the firmware to the latest GA image.

FortiSandbox Azure

Dashboard

System Information

Unit Type	Standalone
Host Name	FSAVM0I000013113 [Change]
Serial Number	FSAVM0I000013113
System Time	Wed Jan 15 18:27:40 2020 PST [Change]
Firmware Version	[All firmwares]
VM License	✓ [Upload License]
System Configuration	Last Backup: N/A [Backup/Restore]
Current User	admin
Uptime	0 day(s) 5 hour(s) 55 minute(s)
Windows VM	⚠
FDN Download Server	✓
Community Cloud Server	✓
Web Filtering Server	✓
Antivirus DB Contract	✓ 2020-07-19
Web Filtering Contract	✓ 2020-07-19

Importing Azure settings into FortiSandbox

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

Uploading rating engine

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

To manually upload the rating engine:

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

Module Name	Current Version	Last Check Time	Last Update Time	Last Check Status
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
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
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
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
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: 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 engine is not available or up-to-date, manually upload the rating 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	Standard_B1s, the minimum size. <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*.

The screenshot shows the FortiSandbox Azure Config page. The top navigation bar includes 'FortiSandbox Azure', 'Azure Config', 'Regular Mode', and a user profile 'admin'. The left sidebar contains various system management icons, with 'System' highlighted. The main content area is titled 'Configure Azure' and contains an 'Edit' form. The form fields are as follows:

- Account Type: Microsoft Azure account email (dropdown menu)
- Microsoft Azure account email: [text input]
- Microsoft Azure account password: [text input]
- Location: [text input]
- Subscription ID: [text input]
- Resource group: [text input]
- Storage account: [text input]
- Storage account access key: [text input]
- Monitor storage account: [text input]
- Monitor account access key: [text input]
- Network security group: [text input]
- Virtual network: [text input]
- Subnet: [text input]
- VM Type: [text input]

At the bottom of the form are three buttons: 'Previous' (disabled), 'Test Connection' (disabled), and 'Submit' (active).

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	Standard_B1s, the minimum size. <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.

Optional: Using a custom VM on Azure

FortiSandbox Azure supports custom VMs. You can provide a VHD image of a custom VM and the FortiSandbox firmware can load the VM image and use it for sample analysis.

For information on setting up a custom VM on Azure, see the custom VM image section in the *FortiSandbox Administration Guide* to do the following:

- Create a custom VHD image using virtualization software such as VirtualBox.
- Prepare the OS installation package.
- Install software and components on the custom VM image.
- Set up the VM image environment.

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 name the same as `VM_image_name`.
- Do not use special characters in the name.
- Do not use reserved FortiSandbox VM names starting with `WIN7`, `WIN8`, or `WIN10`.



Do not use the `set admin-port` command to set port2 as the administrative port.

To install the Azure local custom VM from a blob:

1. Install the Azure local custom VM with the CLI command: `azure-vm-customized`.
2. Check *Azure Config* for the FortiSandbox firmware image storage account information.
3. Create a Blob container (with anonymous read access only) in this storage account.
4. Upload your custom VM VHD to this page blob container.
5. Install the VM from blob as the default type.

You can ignore the `-t` option.

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

To install the Azure local custom VM from snapshot:

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

```
azure-vm-customized -cn -tsnapshot -b[snapshot name] -vo[OS type] -vn[VM name]
```

To install the Azure local custom VM from disk:

1. Install the Azure local 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[disk name] -vo[OS type] -vn[VM name]
```

To use a custom VM on Azure:

1. On the FSA Azure web GUI, go to *Scan Policy and Object > VM Settings* and change *Clone #* to 1.
You can change the *Clone #* to a higher number after the VM clone is completely prepared and you have scanned a sample.

Name	Version	Status	Enabled	Clone #	Load #	Extensions
Customized VMs (1)						
customWin10	1	activated	✓	1	0	
Remote VMs (2)						
MACOSX	0	activated	✗	0	0	mac dmg
WindowsCloudVM	0	activated	✗	0	0	exe htm pptx ppt pptx xls xlsx dll doc docx rtf pdf swf jar dotx docm dotm xltb xlsb xltm xlam potx sldx pptm ppsm potm ppam slidem onetoc thmx bat cmd vbs ps1 js msi msg uri dot xlt pps pot upx WEblink link wsf emi kty jse scr

- In a new FSA CLI window, check the VM clone initialization using the `diagnose-debug vminit` command. The FSA Azure *Dashboard* shows a green indicator for *Windows VM*.

The screenshot displays the FortiSandbox Azure Dashboard. The left sidebar contains navigation icons for Favorites, Dashboard (selected), Security Fabric, Scan Job, Scan Policy and Object, System, and Log & Report. The main content area is divided into two sections: System Information and Licenses.

System Information

Firmware Version	v4.0.0,build0037 (Interim)
Hostname	FSAVM0I000014835
Serial Number	FSAVM0I000016321
System Configuration	Last Backup: N/A
System Time	2021-04-15 19:02:16 PDT
Unit Type	Standalone
Uptime	0 day(s) 0 hour(s) 42 minute(s)
Username	admin

Licenses

- FortiSandbox-Azure
 - Windows VM
 - Windows Cloud VM
 - MacOS Cloud VM
 - Customized VM
 - Mail Transfer Agent Service
- VM Status (2)
 - customWin10 (highlighted with a red box)
 - WindowsCloudVM
- Services
 - Antivirus
 - Web Filtering
 - Industrial Security Service

At the bottom of the Licenses section, there are five icons: a plus sign (+), a refresh icon, a save icon, a document icon, and a printer icon.

- To associate file extensions to the custom VM, go to *Scan Policy and Object > Scan Profile* to the *VM Association* tab.

Interaction with a custom VM clone during scan

1. Go to *Scan Job > File On-Demand* or *URL on-Demand* and click *Submit File* or *Submit File/URL*.
2. Enable *Force to scan the file inside VM* or *Force to scan the url inside VM*.
3. Select *Force to scan inside the following VMs* and select the custom VM.
4. Enable *Allow Interaction*.

Submit New File
✕

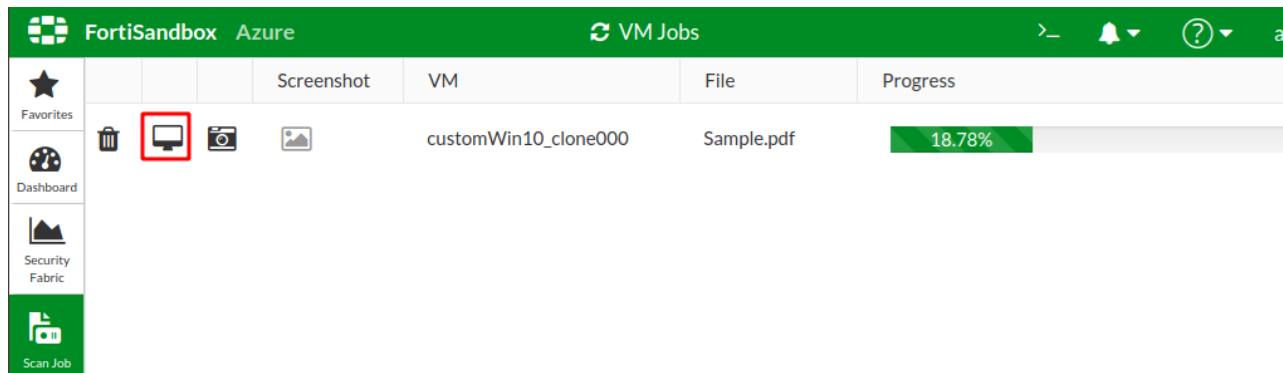
Please upload sample file or archived sample files. The following archive formats are supported: .tar, .z, .xz, .gz, .tar.gz, .tgz, .zip, .bz2, .tar.bz2, .tar.Z, .7z, .rar, .lzh, .ace

Warning: Please be aware that only one VM type can be selected when 'Allow Interaction' is enabled




Select a file:	<input type="button" value="Choose file"/> FSAVM4713450316.pdf <small>Maximum 200 MBs</small>
Possible password(s) for archive/office file:	<input style="width: 100%;" type="text"/> <small>One possible password for each line. Please use ASCII format password without empty space.</small>
Comments:	<input style="width: 100%;" type="text"/> <small>Optional comments for later reference</small>
Skip result of:	<input type="checkbox"/> Static Scan <input type="checkbox"/> AV Scan <input type="checkbox"/> Community Cloud Query
<input checked="" type="checkbox"/> Force to scan the file inside VM	
<input type="radio"/> Follow VM Association settings in Scan Profile <input checked="" type="radio"/> Force to scan inside the following VMs <div style="margin-left: 20px;"> <input checked="" type="checkbox"/> customWin10x64 </div> <div style="margin-left: 20px; border: 2px solid red; padding: 2px; display: inline-block;"> <input checked="" type="checkbox"/> Allow Interaction <small>Interact with VM during on-demand scan</small> </div>	
<input type="checkbox"/> Record scan process in video if VMs involve	
<input type="checkbox"/> Add sample to threat package <small>Add file to Malware Package if it meets settings in Package Options</small>	
<input type="checkbox"/> Enable AI <small>Enable AI mode for this scanning</small>	

5. Click *Submit*.
6. Go to *Scan Policy and Object > VM Settings* and wait for the *VM Interaction* icon to be enabled.
7. When the *VM Interaction* icon is enabled, click the icon to establish an RDP tunnel.
The RDP port 9833 is reserved.

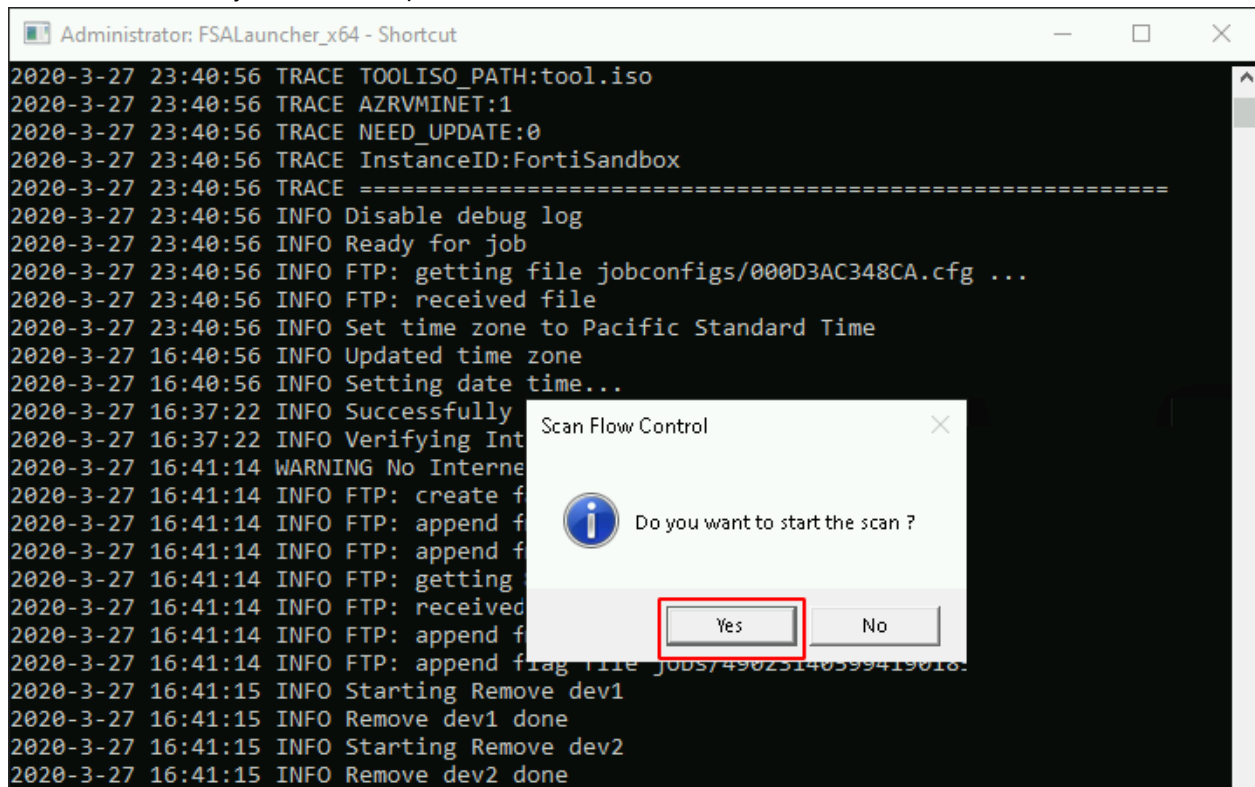
The login credentials is reserved. Username is *Administrator* and password is *FortiSandbox*.



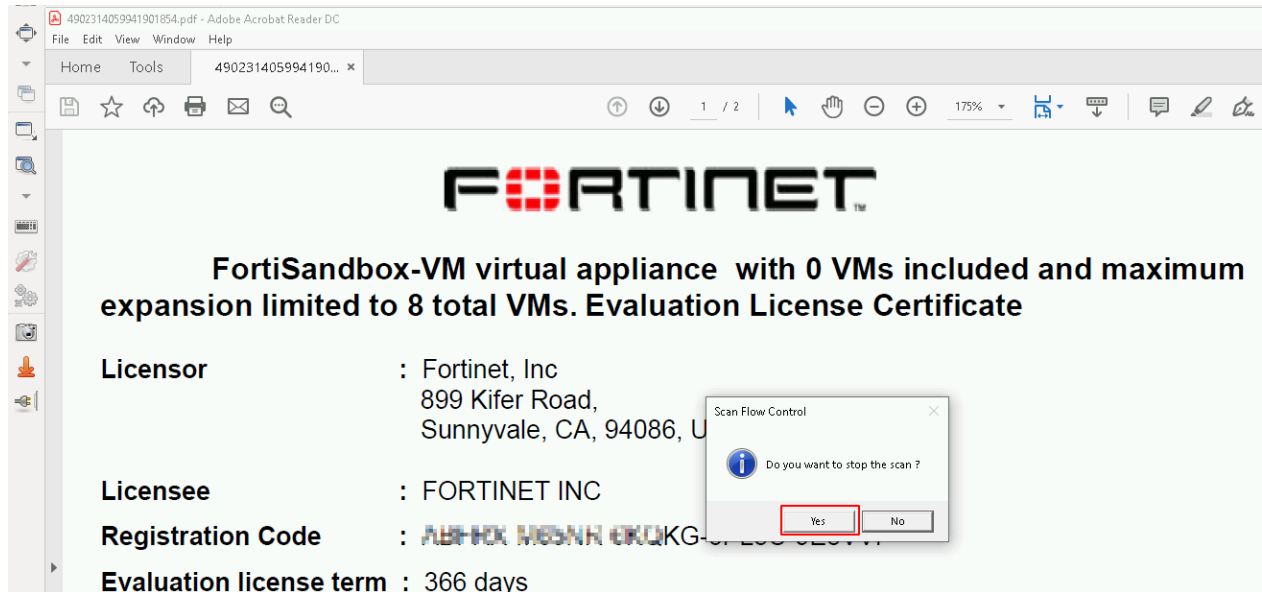
You can also establish an RDP tunnel by going to *Scan Policy and Object > VM Settings* and clicking *VM Screenshot*. When the icon in the *Interaction* column is enabled, click the icon to establish an RDP tunnel.

VM ScreenShot			
Name	Interaction	ScreenShot	PNG Link
customWin10x64_clone000			

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



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



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

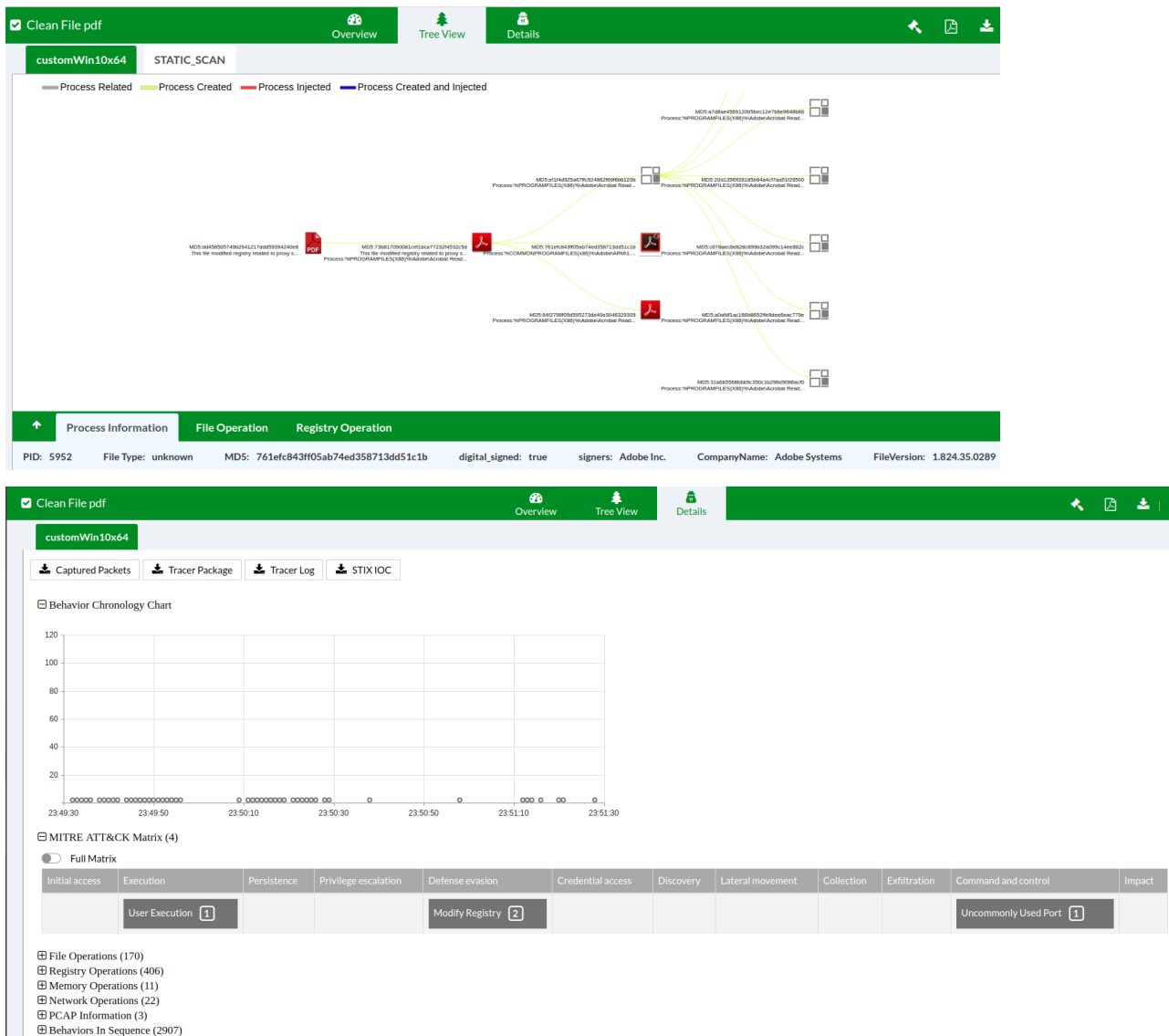
The screenshot shows the FortiSandbox interface with the 'Details' tab selected. The interface is divided into two main sections: 'Basic Information' and 'Details Information'.

Basic Information:

Received:	Mar 27 2020 16:37:12
Started:	Mar 27 2020 16:37:15-07:00
Status:	Done
Rated By:	VM Engine
Submit Type:	On-Demand
Digital Signature:	Yes
AI Mode:	OFF
SIMNET:	OFF
Virus Total:	Q

Details Information:

Downloaded From:	FSAVM4713450316.pdf
File Size:	11678 (bytes)
MD5:	448fedf13fb3827fdc6a8270eacfaef
SHA1:	0c5fb95ef3c93d7bf7fd2b8a3b37cd16512f5940
SHA256:	a5c42d83c9fe80bd31e8da8f4e985b60ca85c61c87128883449fae2be6cc05e7
ID:	4902314059941901854
Submitted By:	admin
Submitted Filename:	FSAVM4713450316.pdf
Filename:	FSAVM4713450316.pdf
Received:	Mar 27 2020 16:37:12
Scan Start Time:	Mar 27 2020 16:37:15-07:00
VM Scan Start Time:	Mar 27 2020 16:37:22-07:00
VM Scan End Time:	Mar 27 2020 16:52:25-07:00
VM Scan Time:	903 seconds
Scan End Time:	Mar 27 2020 16:52:43-07:00
Total Scan Time:	928 seconds
Scan Unit:	FSAVM0I000014855
Specified VMs:	customWin10x64
Launched OS:	customWin10x64



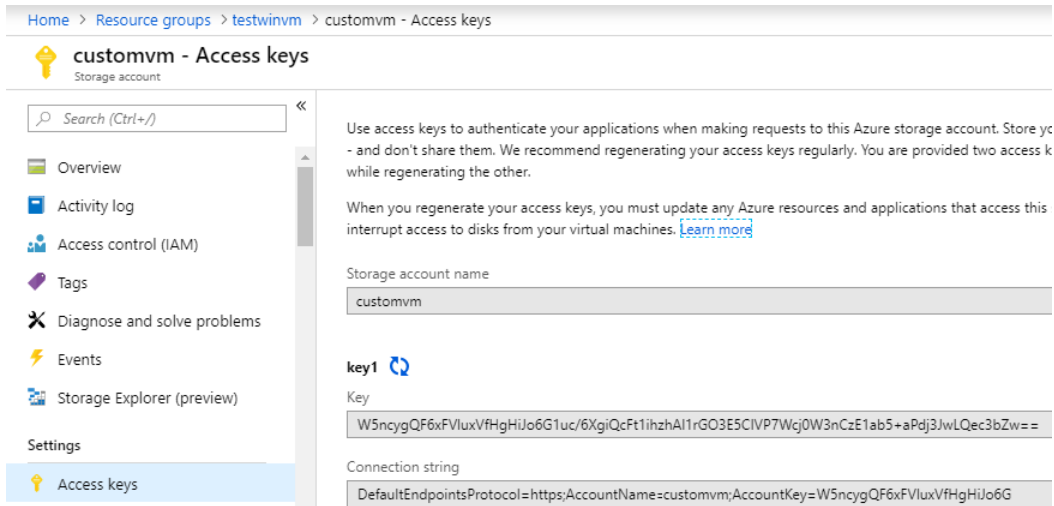
Optional: Using a prebuilt custom VM on Azure

Up to v3.1.2, FortiSandbox only supports Windows7_64 and Windows7 custom VM images.

To create a storage blob for the custom image:

1. Create a new *Resource group* in the Azure portal.
2. In the new resource group, create a *Storage account*.

3. Go to **Resource group > Storage account > Access keys** to find your blob key.



4. Create a **Blob** on the storage account.

5. Download the prebuilt custom VM.

- For the WIN7X86 prebuilt custom VM, download from <https://fortisandbox.blob.core.windows.net/customvm-v1/WIN7X86VM.vhd?se=2025-01-01&sp=rl&spr=https&sv=2018-03-28&sr=c&sig=f65ICG19rIDjYCKbIIZ8EcUzcMii6WrDPCgxQUOeohQ%3D>
- For the WIN7X64 prebuilt custom VM, download from <https://fortisandbox.blob.core.windows.net/customvm-v1/WIN7X64VM.vhd?se=2025-01-01&sp=rl&spr=https&sv=2018-03-28&sr=c&sig=f65ICG19rIDjYCKbIIZ8EcUzcMii6WrDPCgxQUOeohQ%3D>

6. Upload the prebuilt custom VM to your new blob.

- a. Check your *Azure Config* for the FortiSandbox firmware image storage account.
- b. Create a blob container (with anonymous read access) in this storage account.
- c. Upload your custom VM VHD to this blob container.
- d. Install the prebuilt custom VM using the `azure-vm-customized` command.

Optional: Creating a custom Windows 10 VM

FortiSandbox Azure supports custom VMs. You can provide a VHD image of a custom VM and the FortiSandbox firmware can load the VM image and use it for sample analysis.

For information on setting up a custom VM on Azure, see the custom VM image section in the *FortiSandbox Administration Guide* to do the following:

- Create a custom VHD image using virtualization software such as VirtualBox.
- Prepare the OS installation package.
- Install software and components on the custom VM image.
- Set up the VM image environment.

After you have created a custom Windows 10 VM, install and apply the custom VM in FortiSandbox.

To install the custom VM:

1. Put the VM image's VHD file onto a server that supports the FTP or SCP protocol.
2. Install using the command `azure-vm-customized`.
3. After the VM is installed, enable it by setting its clone number to be higher than 0 in the *VM Image* page and associate file types in the *Scan Profile* page to scan files.
4. In a new FSA CLI window, check the VM clone initialization using the `diagnose-debug vminit` command.

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.

To create multiple FortiSandbox instances on Azure:

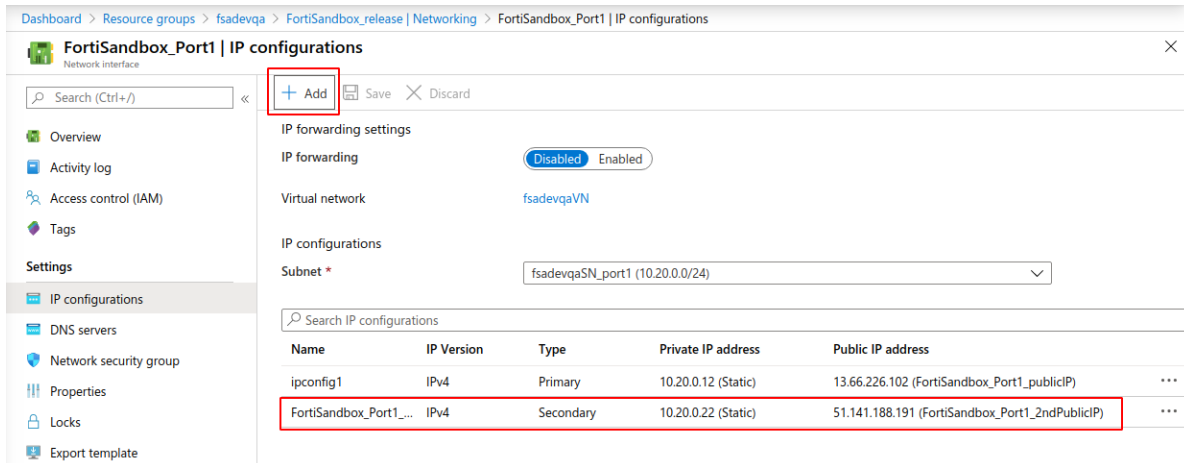
1. Create at least three network interfaces on Azure for each FortiSandbox Azure.
The second network interface is for the custom VM.
The third network interface is for HA communication.

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.

- Go to the primary node's port1 network interface.
- Go to *IP configurations* and click *Add*.
- Add a secondary static *Private IP address*.
- 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:

- Log into each node of the FortiSandbox GUI using the public IP address.
- Follow the instructions on [Importing Azure settings into FortiSandbox on page 22](#) to configure the *Azure Config* page for both the primary and secondary.
- 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.

- 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
```

- Configure the secondary node:

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

- Configure the first worker:

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

- 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
2021-05-03	Initial release.



www.fortinet.com

Copyright© 2021 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.