

FortiSandbox - Azure Guide

Version 3.0.0

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://fortiguard.com/>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



June 07, 2019

FortiSandbox 3.0.0 Azure Guide

34-252-540161-20190607

TABLE OF CONTENTS

About FortiSandbox VM on Azure	4
About Deployment Models	4
Choosing the FortiSandbox VM Basic deployment model	4
Choosing the FortiSandbox VM Advanced deployment model	5
Deploying FortiSandbox VM on Azure (Basic)	6
FortiSandbox VM and WindowsCloudVMs topology	11
FortiSandbox VM Port Usage	11
Deploying FortiSandbox VM on Azure (Advanced)	13
Creating a resource group	14
Creating virtual networks	15
Creating storage accounts	16
Creating a DNS zone through the Azure CLI	17
Creating network security groups	18
Creating network interfaces	20
Creating a FortiSandbox VM using the Azure CLI	21
Importing Azure settings into FortiSandbox	22
Optional: Using a custom VM on Azure	23
Optional: Creating a custom VM on Azure	24
Change Log	31

About FortiSandbox VM on Azure

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

FortiSandbox is available on the Azure Marketplace. This guide provides users with an easy-to follow, step-by-step guide for successful deployment.

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

About Deployment Models

You can configure your FortiSandbox VM on Azure using either an Advanced or Basic deployment model. Before proceeding with deployment, please choose the right deployment model for your needs.

- [Choosing the Basic deployment model](#)
- [Choosing the Advanced deployment model](#)

Choosing the 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 takes advantage of the Azure Setup Wizard to guide you through the setup process with step-by-step instructions. Deployment takes approximately 10 minutes to complete.

Advantages:

- Single Wizard page where you can enter all of the information required for launching a FortiSandbox VM.
- Only simple information is required: resource group name, VM name, VM region, VM size, username, your SSH key or user password.
- The setup wizard automatically creates and deploys the following resources: storage account, virtual network, network interface, public IP address, and the virtual machine instance.

Limitations:

- The FortiSandbox VM is only created with one network interface.
 - Some HA features require at least two network interfaces.*
 - It is possible to add a second network interface, however, it requires a shutdown of the VM on the portal, followed by the manual creation and attaching of the new network interface.
- Basic deployment can only support sandboxing analysis using Windows Cloud VMs.
- Basic deployment models cannot run custom Windows VMs for analysis.

Choosing the FortiSandbox VM Advanced deployment model

To use advanced features of the FortiSandbox VM, including custom VMs and HA features, you can select the Advanced deployment model. Advanced deployment requires you to manually create all of the resources needed. It is recommended only for individuals with a good understanding of Azure and practical experience working with the cloud. Deployment takes approximately one hour to complete.

Advantages:

- Gives you full control to customize the resources required to deploy the VM.
- Advanced deployment supports the use custom Windows VMs.
- Advanced deployment supports HA features.*

Limitations:

- Requires advanced knowledge of deploying VMs in the Azure infrastructure.
- The detailed guide must be followed carefully to ensure successful deployment.
- All components must be deployed manually on the Azure portal.
- Longer deployment times.

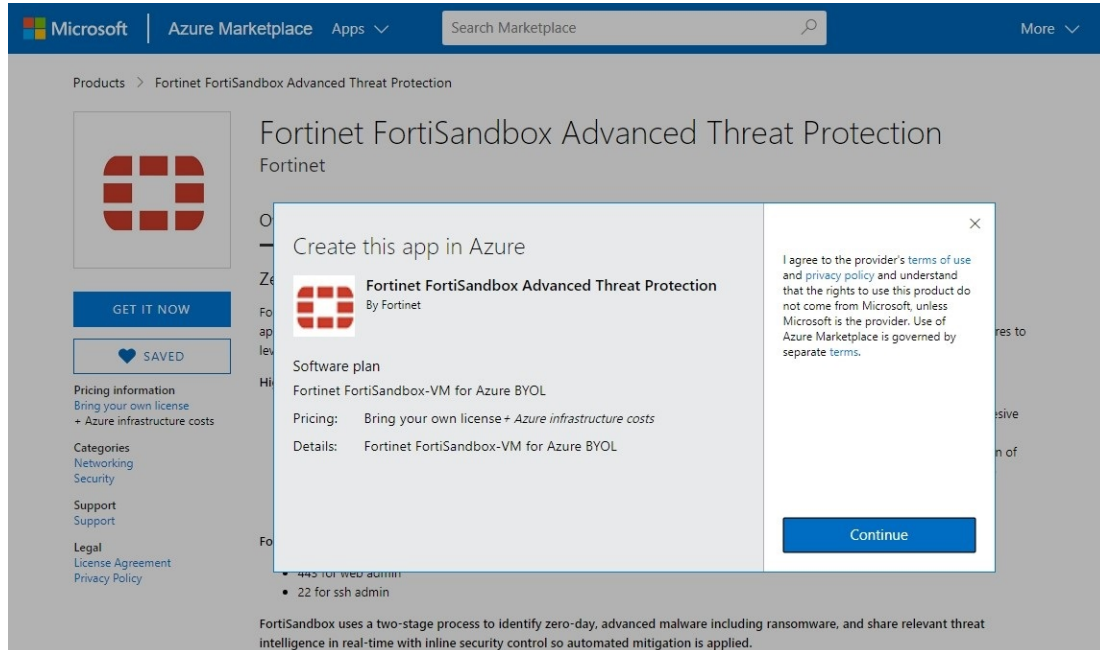


*Ha features: Currently, only clustering is supported on Azure. High Availability mode is not currently supported.

Deploying FortiSandbox VM on Azure (Basic)

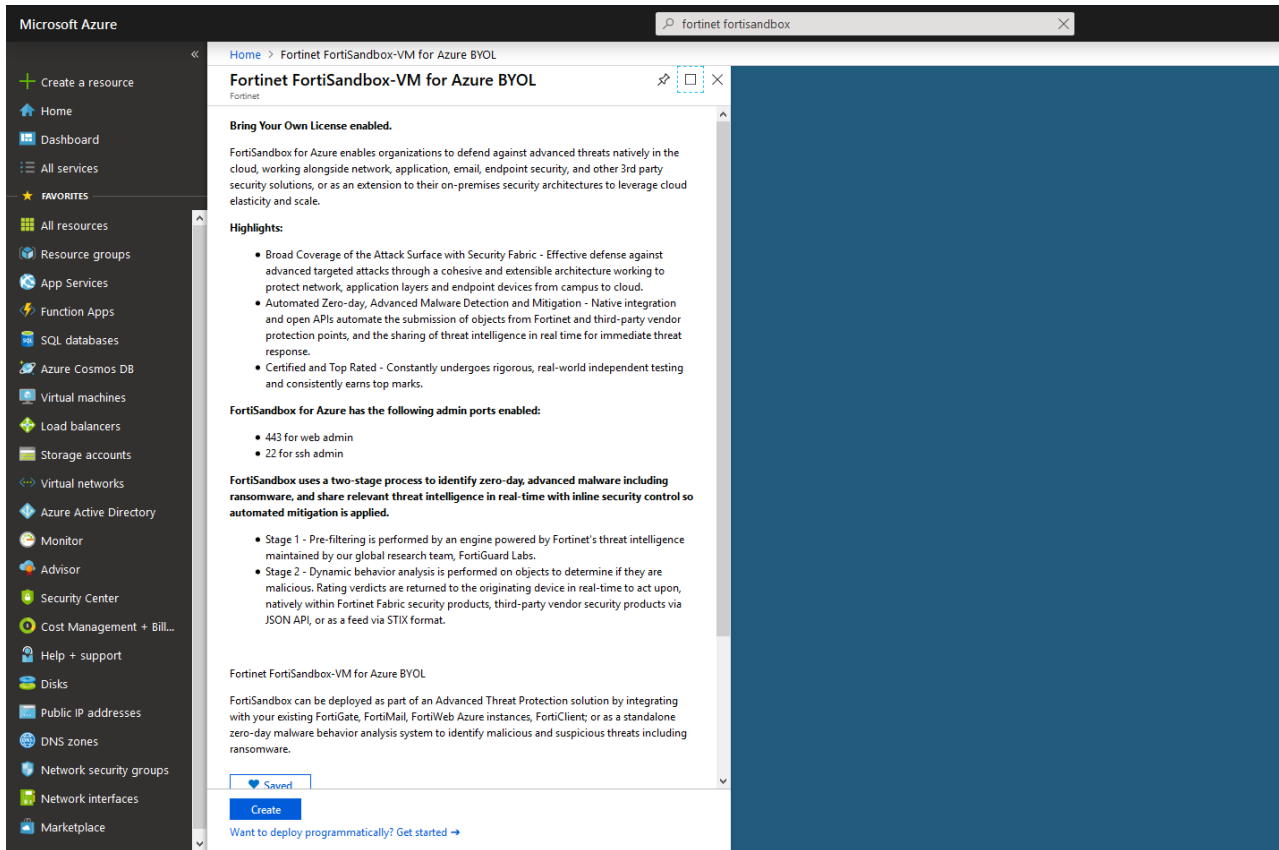
To deploy FortiSandbox VM on Azure with Windows Cloud VMs:

1. Search *Fortinet FortiSandbox* on Azure Marketplace.




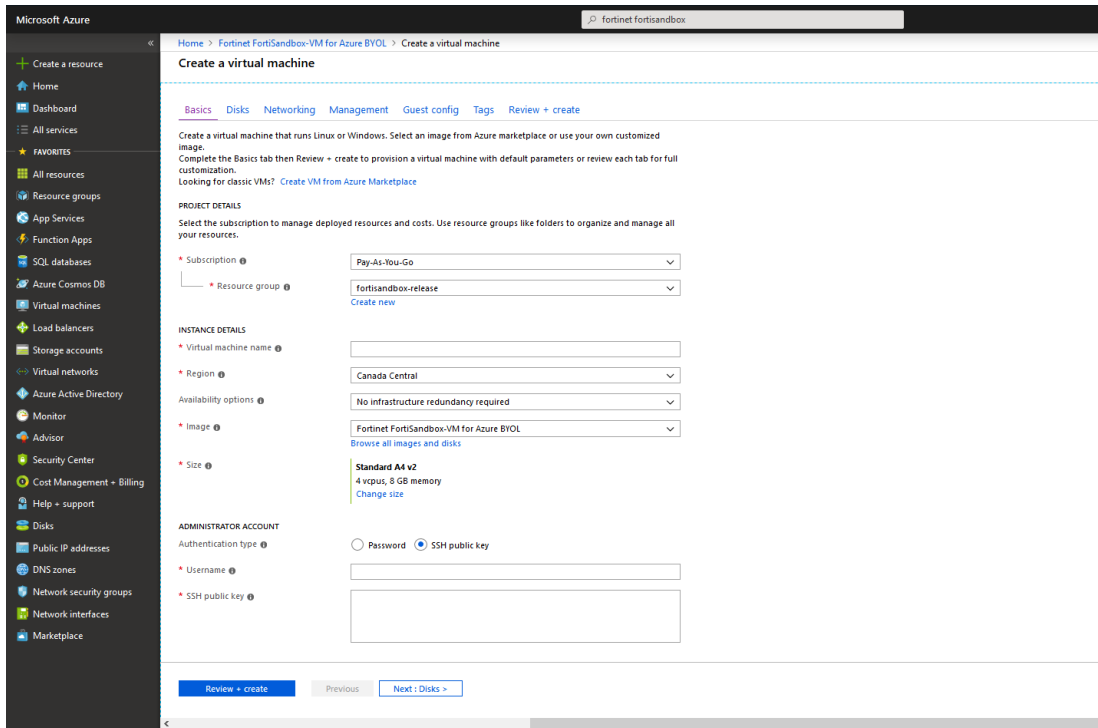
2. Select *GET IT Now* and confirm the terms of use by selecting *Continue*. The setup wizard will launch.

3. On the Setup Wizard, select *Create* to proceed.

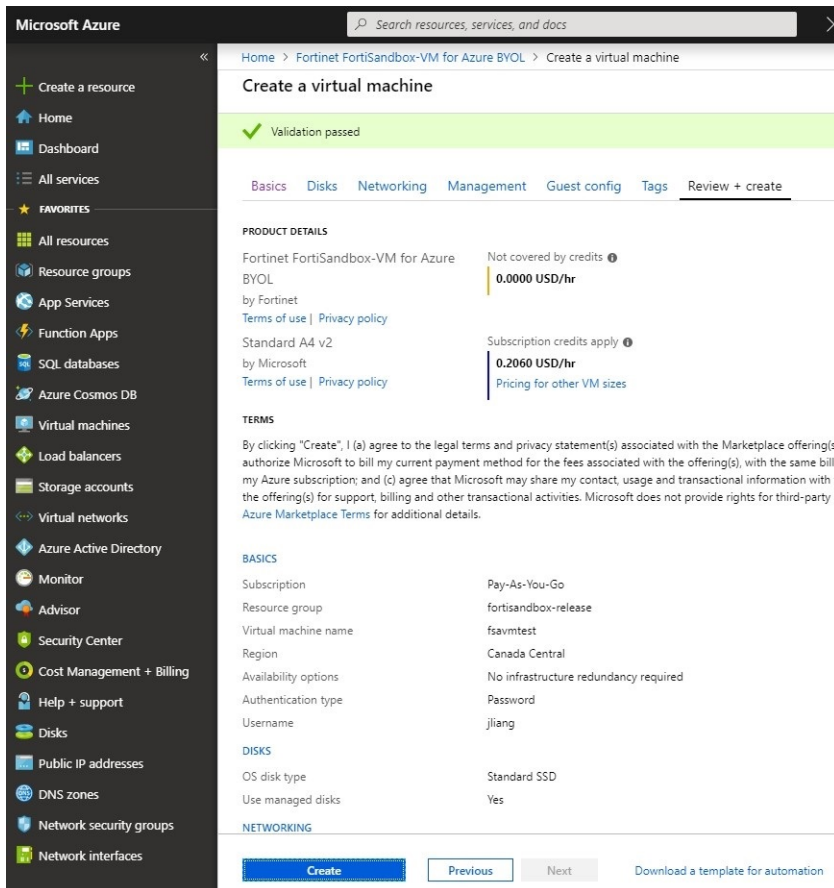


4. Enter the required information into the Wizard:

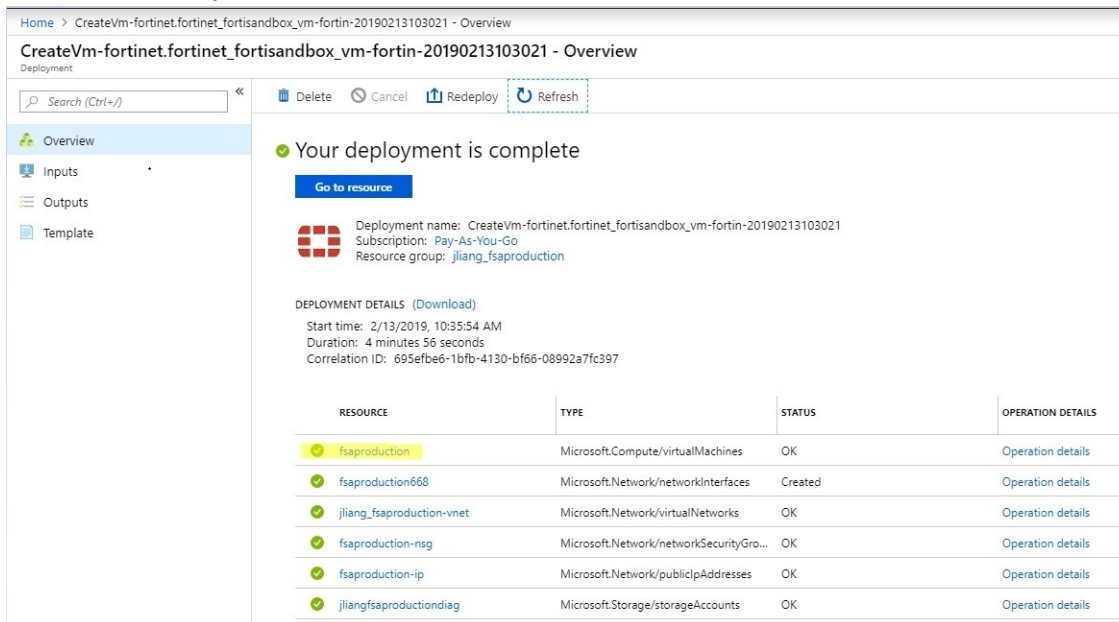
Resource group	Create a new resource group.
Virtual machine name	Provide the name for this VM.
Region	Select your VM region.
Size	Adjust the VM instance type; recommended Standard A4 v2 for speed and storage capacity.
	 <p>The FSA on Azure uses the temporary disk (freely provided by the VM) to store and process job files. A secondary disk is not required.</p>
Username	A secondary admin user; the default <i>Admin</i> user is always created.
Authentication type	The SSH public key or password being used.



5. Select **Review + Create**.
Once the Setup Wizard has validated your information, select **Create**.



6. Your FortiSandbox VM should become available within five minutes. Once available, click the link to go to the virtual machine. You can find the public IP address assigned to the FortiSandbox that you can use for access from HTTPS.



Home > CreateVm-fortinet.fortinet_fortisandbox_vm-fortin-20190213103021 - Overview

CreateVm-fortinet.fortinet_fortisandbox_vm-fortin-20190213103021 - Overview

Deployment

Search (Ctrl+/)

Delete Cancel Redeploy Refresh

Overview

Inputs

Outputs

Template

Your deployment is complete

Go to resource

Deployment name: CreateVm-fortinet.fortinet_fortisandbox_vm-fortin-20190213103021
Subscription: Pay-As-You-Go
Resource group: jliang_fsaproductio

DEPLOYMENT DETAILS (Download)

Start time: 2/13/2019, 10:35:54 AM
Duration: 4 minutes 56 seconds
Correlation ID: 695efbe6-1bfb-4130-bf66-08992a7fc397

RESOURCE	TYPE	STATUS	OPERATION DETAILS
fsaproductio	Microsoft.Compute/virtualMachines	OK	Operation details
fsaproductio668	Microsoft.Network/networkInterfaces	Created	Operation details
jliang_fsaproductio-vnet	Microsoft.Network/virtualNetworks	OK	Operation details
fsaproductio-nsg	Microsoft.Network/networkSecurityGro...	OK	Operation details
fsaproductio-ip	Microsoft.Network/publicIPAddresses	OK	Operation details
jliangfsaproductiodiag	Microsoft.Storage/storageAccounts	OK	Operation details

7. Get the default admin password for the FortiSandbox VM through the Azure CLI. The VM-ID UUID is the default password for Admin access.

```
jason@Azure:~$ az vm list --output tsv -g jliang azurefsa_resource
None None None /subscriptions/dfcad4bd-550b-4572-8404-d541c6cf306b/resourceGroups/jliang
g_azurefsa_resource/providers/Microsoft.Compute/virtualMachines/jliangfsavm None None None e
astus jliangfsavm Succeeded jliang_azurefsa_resource None M
icrosoft.Compute/virtualMachines 972a2831-045c-4618-9c07-be7c639b None
jason@Azure:~$
```

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 the FortiSandbox *Dashboard* and select *Upload License*. Once a license file has been loaded, the FortiSandbox Azure instance will be rebooted.

FortiSandbox Azure

System Information

- Unit Type: Standalone
- Host Name: FSAAZR0009D91A0C [Change]
- Serial Number: FSAAZR0009D91A0C
- System Time: Tue Mar 5 00:36:32 2019 UTC [Change]
- Firmware Version: v3.0.0.build5032 (GA)[Update]
- VM License: [Upload License]
- System Configuration: Last Backup: N/A [Backup/Restore]
- Current User: admin
- Uptime: 0 day(s) 0 hour(s) 6 minute(s)
- Windows VM:
- FDN Download Server:
- Community Cloud Server:
- Web Filtering Server:
- Antivirus DB Contract: No Contract
- Web Filtering Contract: No Contract

Threats Distributed 24 Hours

Customized Threat Distribution

3. Go to *Virtual Machine > VM Images* and select the *WindowsCloudVM*.
4. Select *Edit Clone Number* to assign a clone number and enable the Windows Cloud VM.

FortiSandbox Azure VM Images

What are you looking for?

VM Images

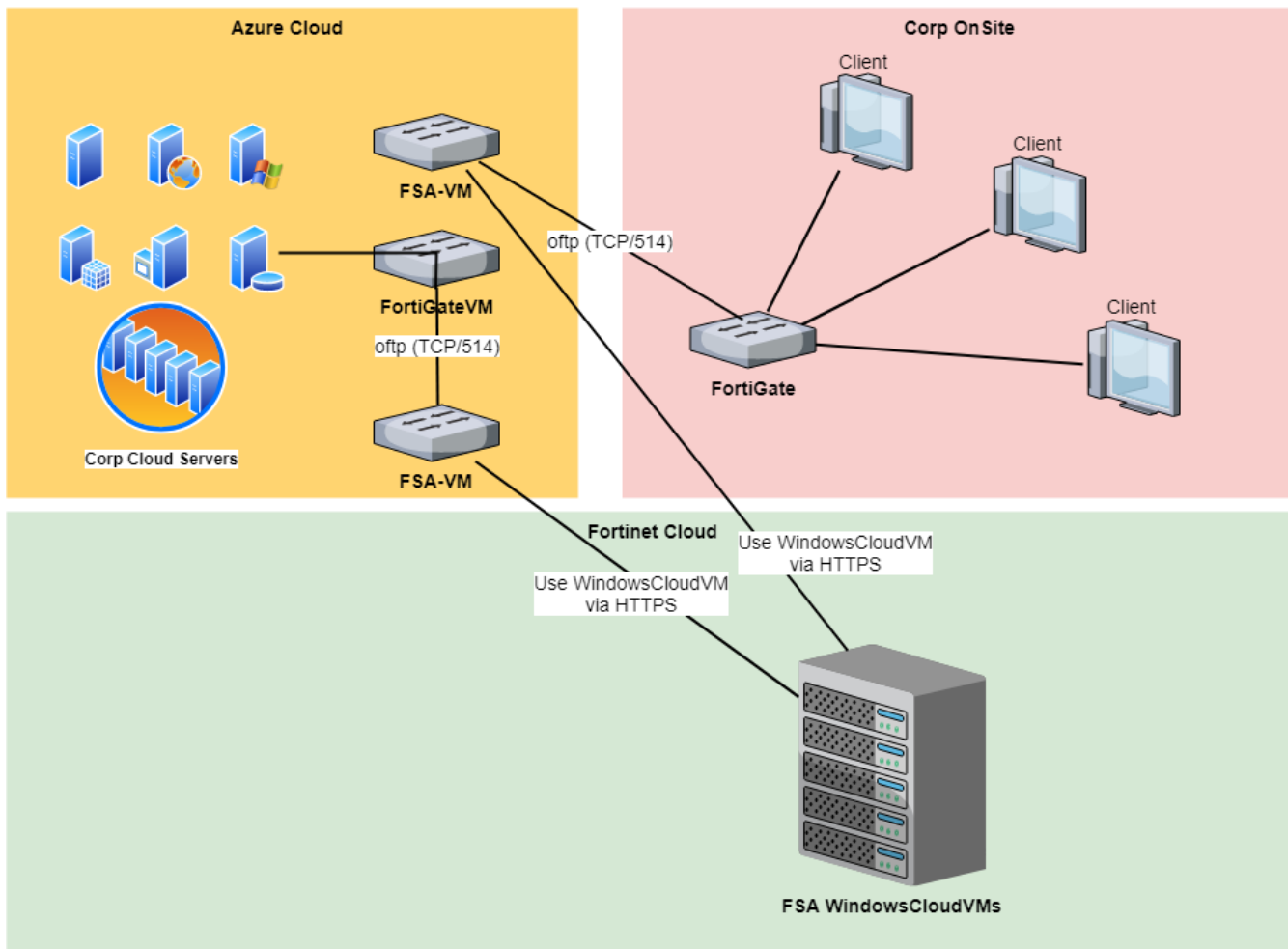
Edit Clone Number

Name	Version	Status	Enabled	Clone #	Load #	Extensions
Remote VMs (2)						
MACOSX	0	installed	<input checked="" type="checkbox"/>	0	0	mac dmg
WindowsCloudVM	0	installed	<input checked="" type="checkbox"/>	<input type="text" value="0"/>	0	exe php tiff gif png tnef asf htm ppsx unk cdf ico ppt vcf com jpeg pptx dotx docm dotm xltx xltm xlsb xlam potx sltx pptm ppsm potm p dot xlt pps pot upx WEBLink lnk jarlib httnnojs wsf eml pub mht mime



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

FortiSandbox VM and WindowsCloudVMs topology



FortiSandbox VM Port Usage

Type	Service	Port
FortiGate	OFTP	TCP/514
FortiClient	File Analysis	TCP/514

Type	Service	Port
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)

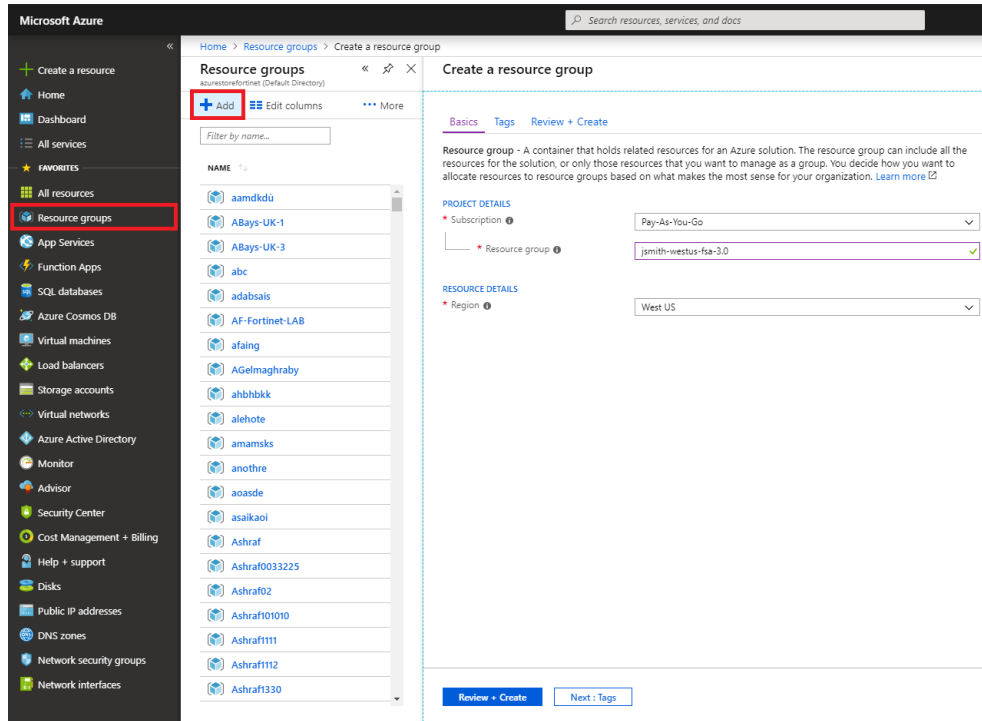
To deploy FortiSandbox VM on Azure to support Windows Cloud VMs and custom VMs:

1. [Creating a resource group](#)
2. [Creating virtual networks](#)
3. [Creating storage accounts](#)
4. [Creating a DNS zone through the Azure CLI](#)
5. [Creating network security groups](#)
6. [Creating network interfaces](#)
7. [Creating a FortiSandbox VM using the Azure CLI on page 21](#)
8. [Importing Azure settings into FortiSandbox](#)
9. [Optional: Using a custom VM on Azure on page 23](#)
10. [Optional: Creating a custom VM on Azure on page 24](#)

Creating a resource group

To create resource groups in Azure:

1. In the Azure portal, select *Resource Group* from the left navigation pane.
2. Select *Add* to create a new empty resource group.



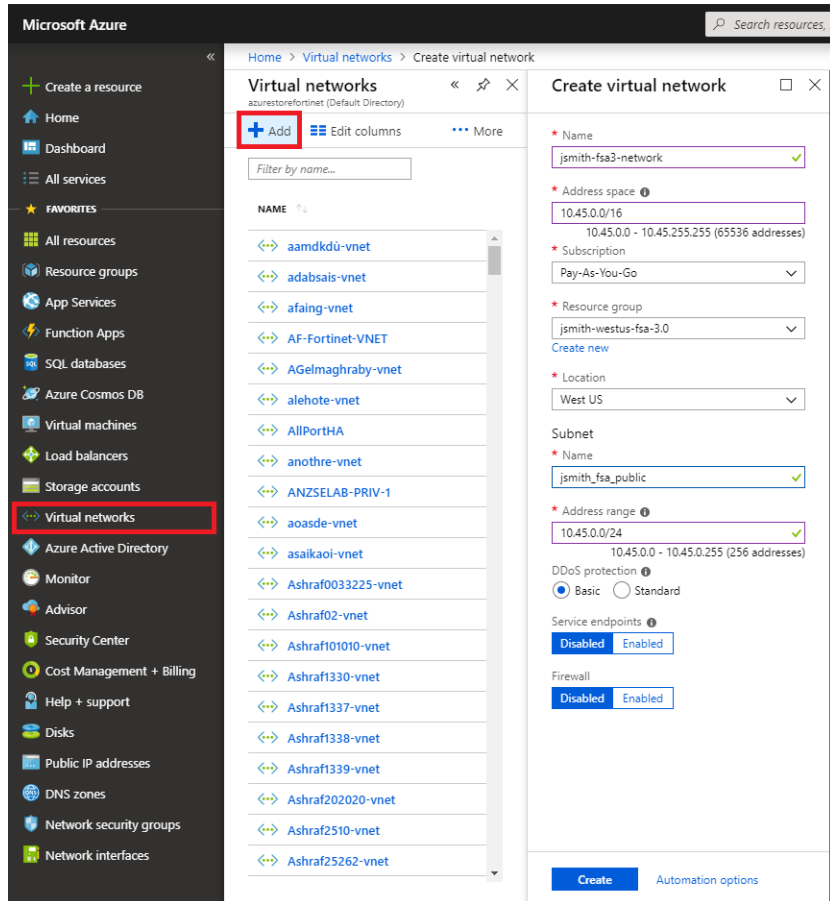
3. Enter the following information:

Resource group name	Enter a name for the resource group.
Subscription	Select a subscription option.
Resource group location	Select a resource group location.

Creating virtual networks

To create virtual networks in Azure:

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



3. Enter the following information:

Name	Enter a name for 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 same location used while setting up the resource group.
Subnet	
<ul style="list-style-type: none"> • Name 	Enter a name for the FSA port1 (the management subnet).
<ul style="list-style-type: none"> • Address Range 	Enter a class C network (xxx . xxx . x . 0 / 24) within the virtual network.

DDoS protection	Basic.
Service endpoints	Disabled.

4. Select *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.



The use of *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 as per your own needs.

Creating storage accounts

Two storage accounts must be created:

- The first is for storing the FSA firmware image (Storage Account).
- The second is for storing diagnostic information (Monitor Account), such as the VM diagnostic screenshots during job scans.

To create storage accounts in Azure:

1. In the Azure portal, select *Storage Accounts* from the left navigation pane.
2. Select *Add* to create a new storage account.

The screenshot displays the Azure portal interface for creating a new storage account. On the left-hand side, the navigation pane shows 'Storage accounts' highlighted with a red box. In the main area, the 'Storage accounts' list is visible, with the '+ Add' button highlighted by a red box. The 'Create storage account' wizard is open, showing the 'Basics' tab. The form includes the following fields and options:

- Subscription:** Pay-As-You-Go
- Resource group:** jsmith-westus-fsa-3.0
- Storage account name:** (empty field)
- Location:** Canada Central
- Performance:** Standard (selected), Premium
- Account kind:** StorageV2 (general purpose v2)
- Replication:** Read-access geo-redundant storage (RA-GRS)
- Access tier (default):** Cool, Hot (selected)

At the bottom of the form, there are buttons for 'Review + create', 'Previous', and 'Next: Advanced >'.

- Enter the following information for each account:

Name	Enter a name for the storage account.
Deployment model	Resource manager.
Account kind	Leave it as the default value or change according to your needs.
Location	Select the same location used while setting up the resource group.
Replication	Read-access geo-redundant storage.
Performance	Standard.
Secure transfer required	Disabled.
Subscription	Select your subscription type.
Resource group	Select the resource group you created in the Creating a resource group step.
Virtual networks	Disabled.
Data Lake Storage Gen 2	Disabled.

- Select *Create*.
- Repeat the steps above to create a second storage account.

Creating a DNS zone through the Azure CLI

To create a DNS zone through the Azure CLI:

- In the Azure CLI, enter the following commands:

```
az network dns zone create -g <MyAzureResourceGroup> -n fsaazure.com \
  --zone-type Private \
  --registration-vnets <myAzureVNet>
```



- n must be followed by *fsaazure.com* and cannot be replaced with any other names.

- Create an FTP DNS record set in the newly created DNS zone.
- Enter the following information:

Name	ftp
Type	A
Alias record set	No
TTL	300
TTL unit	Hours

IP address

Use the static port2 IP address of the network interface you created. You can return to this screen to update the IP after the Azure FSA instance is up, but the IP must be set correctly before VM initialization.



- A DNS zone must be created before proceeding to any steps in the following pages, otherwise, a DNS zone will always fail to be created after allocating any network address space.
 - DNS zones are used by custom VMs to communicate with the Azure FSA license; if you do not need to use a custom VM, a DNS zone is not required.
-

Creating network security groups

Two network security groups must be created:

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

To create network security groups in Azure:

1. In the Azure portal, select *Network Security Groups* from the left navigation pane.
2. Click *Add* to create a new network security group for the management port subnet.

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation pane is visible with 'Network security groups' highlighted. The main content area displays the 'Create network security group' wizard. The 'Add' button is highlighted in the top left. The form fields are as follows:

- Name:** jsmith_nsg
- Subscription:** Pay-As-You-Go
- Resource group:** jsmith-westus-fsa-3.0
- Location:** West US

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

3. Enter the following information:

Name	Enter a name for the network security group.
Subscription	Select a subscription type.
Resource group	Select 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 the steps above to create a second network security group for the FSA port2 subnet.
5. Go to the newly created security groups and configure the inbound rules to allow for the following:
 - Network security group one: *HTTPS* (TCP 443), *SSH traffic* (TCP 22), *OFTP traffic* (TCP 514), and optional: *ICAP traffic* (TCP 1344), *ICAP over SSL* (TCP 11344).
 - Network security group two: *FTP* (TCP 21) and *RDP* (TCP 3389).



Users can choose to alternatively create only one network security group with the inbound rules allowing for *HTTPS*, *SSH traffic*, *OFTP*, *FTP*, and *RDP*.

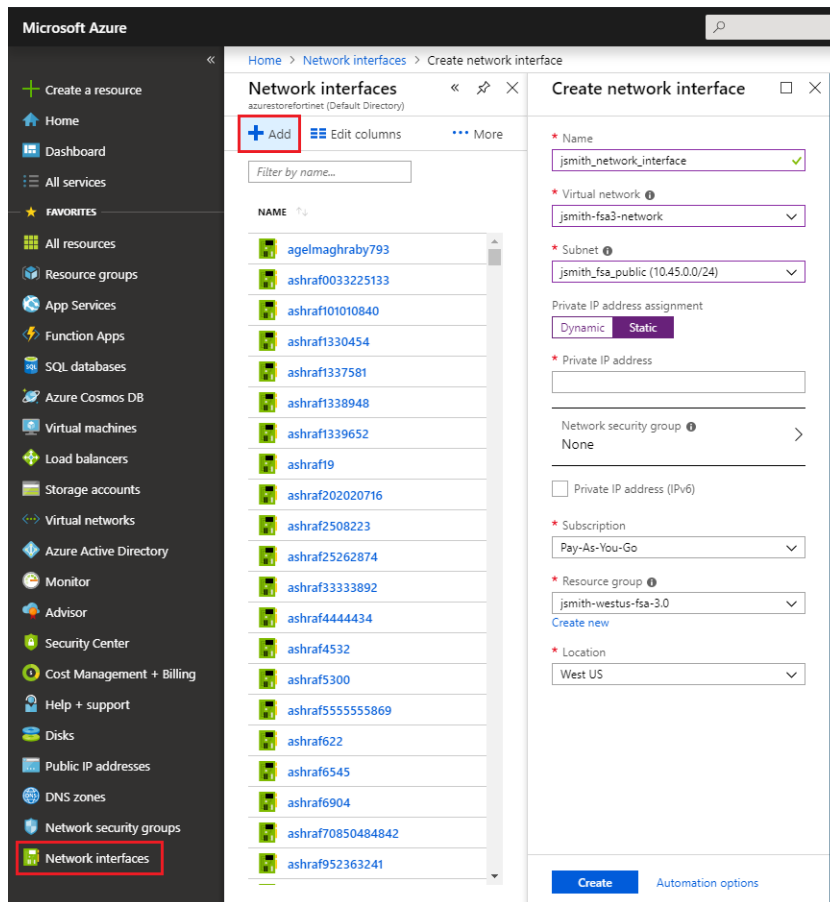
Creating network interfaces

Two network interfaces are required:

- The first is for FSA *port1*.
- The second is for FSA *port2*.

To create a network interface in Azure:

1. In the Azure portal, select *Network Interfaces* from the left navigation pane.
2. Click *Add* to create a new network interface.



3. Enter the following information:

Name	Enter your VM name.
Virtual network	Enter your VNet.
Subnet	One subnet under your VNet. Each interface you create must be in a different subnet.
Private IP address assignment	Static.
Private IP address.	Self-defined static IP address.

Network security group	None.
Private IP address (IPv6)	Unchecked.
Subscription	Select a subscription type.
Resource group	Select the resource group you created in the Creating a resource group step.
Location	Select the same location used while setting up the resource group.

- Repeat the steps above to create a second network interface.



If multiple network security groups were created, the one associated with the FSA port1 interface must be under the security group which includes *HTTPS* and *SSH*, and the one associated with the FSA port2 interface must be under the security group which includes *RDP* and *FTP*.

- Associate the network interface used for the FSA admin port (port1) with the *Public IP* address in the IP configuration section; add the private IP address of the other network interface to the IP address list of the FTP DNS record set.

Creating a FortiSandbox VM using the Azure CLI

To create the VM using the Azure CLI:

- Create the VM using the Azure CLI with FortiSandbox on the Azure Marketplace with the two network interfaces created previously.

```
az vm create --resource-group [resource group name] --location [location name] --name [vm name] \
  --image "fortinet:fortinet_fortisandbox_vm:fortinet_fsa-vm:3.0.2" --size [vm size] \
  --nics [NIC for port1] [NIC for port2] \
  --generate-ssh-keys --verbose
```

```
jason@Azure:~$ az vm create --resource-group jliang_azurefsa_resource --location eastus --name jliangfsavm \
> --image "fortinet:fortinet_fortisandbox_vm:fortinet_fsa-vm:3.0.2" --size Standard_M4_V2 \
> --nics jliang_azurefsa_nic1port jliang_azurefsa_nic2port \
> --generate-ssh-keys --verbose
Use existing SSH public key file: /home/jason/.ssh/id_rsa.pub
Accepted: vm_deploy_I7qEgYt3hcspmA2d3M3Wfo2zeUtvX9FZ (Microsoft.Resources/deployments)
Accepted: jliangfsavm_OsDisk_1_0b2e9a8d6f94c57b4298a9d00482220 (Microsoft.Compute/disks)
Succeeded: jliangfsavm (Microsoft.Compute/virtualMachines)
Succeeded: jliangfsavm (Microsoft.Compute/virtualMachines)
{
  "fqdns": "",
  "id": "/subscriptions/dfcad4bd-550b-4572-8404-d541c6cf306b/resourceGroups/jliang_azurefsa_resource/providers/Microsoft.Compute/virtualMachines/jliangfsavm",
  "location": "eastus",
  "macAddress": "00-00-3A-17-39-12,00-00-3A-17-33-C2",
  "powerState": "VM running",
  "privateIpAddress": "10.44.0.100,10.44.1.100",
  "publicIpAddress": "13.92.179.111",
  "resourceGroup": "jliang_azurefsa_resource",
  "zones": ""
}
jason@Azure:~$
```

- Get the default admin password for the FSA VM through the Azure CLI. The VM-ID UUID is the default password for admin access.

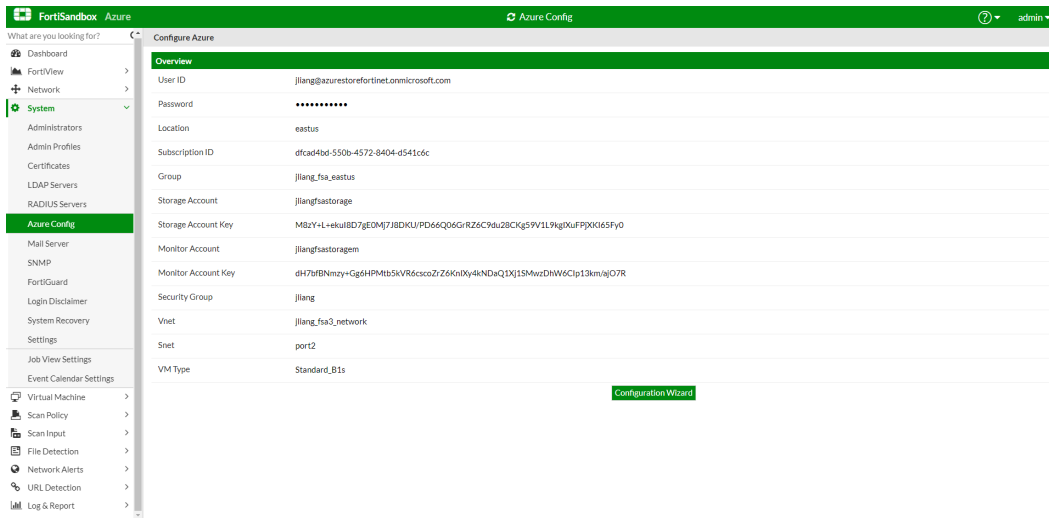
```
jason@Azure:~$ az vm list --output tsv -g jliang_azurefsa_resource
None None None /subscriptions/dfcad4bd-550b-4572-8404-d541c6cf306b/resourceGroups/jliang_azurefsa_resource/providers/Microsoft.Compute/virtualMachines/jliangfsavm None None None eastus jliangfsavm Succeeded jliang_azurefsa_resource None Microsoft.Compute/virtualMachines 972a2831-045c-4618-9c07-be7c639b None
jason@Azure:~$
```

Importing Azure settings into FortiSandbox

Once the FSA instance has been successfully deployed, you can import your Azure settings into FortiSandbox.

To import Azure settings into FSA:

1. Go to the FSA instance.
2. Select *Settings > Azure Config*.



3. Fill out the configuration form by providing the following information:

User ID	Your user ID.
Password	Your user password.
Location	Select the same location used while setting up the resource group.
Subscription ID	Your subscription ID.
Group	The resource group.
Storage account	The storage account's name.
Storage account key	The storage account's key.
Monitor account	The monitor account's name.
Monitor account key	The monitor account's key.
Security group	The security group created. If you created multiple security groups, this should be the one which allows for RDP and FTP.
Vnet	The name of the Vnet you created.
Snet	The Snet created for the FSA port2 interface.
VM type	The size of the VMs used for sandboxing. This also affects the analysis speed and instance cost when using custom VMs. In most use cases, this should be set to <i>Standard_B1s</i> .

You can use other types of VMs with the number of vCPU cores ≤ 2 .
 For more information on VM sizes, see: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-general>

4. The instance will fetch the licensing information, which can take up to three hours.
5. Once completed, upload your BYOL license if it was provided.

Optional: Using a custom VM on Azure

To use custom VM on Azure:

1. Install Azure local customized VMs with CLI command: `azure-vm-customized`.
2. In a new FSA CLI window, use the following command to check and watch for the VM initialization: `diagnose-debug vminit`.
3. On the FSA Azure web GUI, go to *Virtual Machine* > *VM Images* and update the *Clone* number and apply it.

Name	Version	Status	Enabled	Clone #	Load #	Extensions
Customized VMs (2)						
WIN7X64VMvhd	1	activated	✓	1	1	
WIN7X86VMvhd	1	activated	✓	1	1	
Remote VMs (2)						
MACOSX	0	activated	✓	1	1	mac dmg
WindowsCloudVM	0	activated	✓	1	1	exe php tiff gif png tne xltm xlsb xlsm pobx slt eml pub mht mime iso

4. In a new FSA CLI window, use the following command to check and watch for the VM clone init: `diagnose-debug vminit`.

5. The FSA Azure *Dashboard* now shows a green indicator for Windows VM.

The screenshot displays the FortiSandbox Azure dashboard. The main content area is titled "System Information" and contains a table of system details. A green checkmark is visible next to the "Windows VM" entry, indicating its status. The right sidebar shows a "Threats Distribution" map and a "Customized Threat" section.

System Information	
Unit Type	Standalone
Host Name	FSAVM0I000010235 [Change]
Serial Number	FSAVM0I000010235
System Time	Fri Dec 14 12:43:22 2018 PST [Change]
Firmware Version	v3.0.0,build5024 (GA)[Update]
VM License	✓ [Upload License]
System Configuration	Last Backup: N/A [Backup/Restore]
Current User	admin
Uptime	1 day(s) 19 hour(s) 39 minute(s)
Windows VM	✓
FDN Download Server	✓
Community Cloud Server	✓
Web Filtering Server	✓
Antivirus DB Contract	✓ 2019-04-27
Web Filtering Contract	✓ 2019-04-27
MacOS VM Contract	✓ 2019-05-13, 2 available (Up to 8)
Windows Cloud VM Contract	✓ 2019-05-13, 5 available (Up to 200)

Optional: Creating a custom VM on Azure

To create a storage blob for the custom image:

1. Create a new *Resource Group* in the *Azure portal*.
2. Create a *Storage Account* under the new *Resource Group*.

3. Locate your blob key on the *Access Keys* page.

The screenshot shows the Azure portal interface for the 'Access keys' page of a storage account named 'customvm'. The breadcrumb navigation is 'Home > Resource groups > testwinvm > customvm - Access keys'. The left sidebar contains navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Events, Storage Explorer (preview), and Settings. The 'Access keys' option is selected. The main content area displays instructions on using access keys and provides the following details:

- Storage account name:** customvm
- key1** (with a refresh icon)
 - Key:** W5ncygQF6xFVluxVfHgHjJo6G1uc/6XgiQcFt1ihzhA1rGO3E5CIVP7Wcj0W3nCzE1ab5+aPdj3JwLQec3bZw==
 - Connection string:** DefaultEndpointsProtocol=https;AccountName=customvm;AccountKey=W5ncygQF6xFVluxVfHgHjJo6G

4. Create a *Blob* on the *Storage Account*.

5. Go to the *Properties* page of the *Blob* and get the URL.

The screenshot shows the Azure portal interface for the 'Properties' page of a blob named 'win7'. The breadcrumb navigation is 'Home > Resource groups > testwinvm > customvm - Blobs > win7 - Properties'. The left sidebar contains navigation options: Overview, Access Control (IAM), Settings, Access policy, Properties (selected), and Metadata. The main content area displays the following details:

- NAME:** win7
- URL:** https://customvm.blob.core.windows.net/win7
- LAST MODIFIED:** 3/15/2019, 3:53:46 PM

6. Use the `azcopy` command in the Azure CLI to copy the prebuilt custom VM to your new blob.

- [WIN7X86 prebuilt custom VM](#)
- [WIN7X64 prebuilt custom VM](#)

```
$ azcopy --source [above_WIN7X86/WIN7X64_link] --destination \
https://[your_blob_URL]/win7/WIN7X86VM.vhd --dest-key \
[your_storage_account_key]
```


To create the custom VM:

1. In the Azure portal, go to the details page of the created image. Select *Create VM*.
2. Follow the Wizard to create a Windows VM, selecting RDP as the inbound port.

Home > Resource groups > testwinvm > win7x86imagetest > Create a virtual machine

Create a virtual machine

INSTANCE DETAILS

* Virtual machine name ⓘ	mywin7vm
* Region ⓘ	Canada Central
Availability options ⓘ	No infrastructure redundancy required
* Image ⓘ	win7x86imagetest Browse all images and disks
* Size ⓘ	Standard B1s 1 vcpu, 1 GB memory Change size

ADMINISTRATOR ACCOUNT

* Username ⓘ	
* Password ⓘ
* Confirm password ⓘ

INBOUND PORT RULES

Select which virtual machine network ports are accessible from the public internet. You can specify more list access on the Networking tab.

* Public inbound ports ⓘ	<input type="radio"/> None <input checked="" type="radio"/> Allow selected ports
* Select inbound ports	RDP

Review + create	Previous	Next : Disks >
------------------------	----------	----------------

3. Once your VM resource is ready, select the VM name and find the public IP address, then connect to it using RDP (Windows Remote Desktop Protocol).

- The deployment window will indicate that deployment is underway or has failed, however, this can be ignored as the VM will actually be up and reachable.

Home > CreateVm-win7x86imagetest-20190315173537 - Overview

CreateVm-win7x86imagetest-20190315173537 - Overview


Deployment

Search (Ctrl+/) « Delete Cancel Redeploy Refresh

- Overview
- Inputs
- Outputs
- Template



Your deployment is underway

Check the status of your deployment, manage resources, or troubleshoot deployment issues. Pin this | your dashboard to easily find it next time.


 Deployment name: [CreateVm-win7x86imagetest-20190315173537](#)
 Subscription: [Pay-As-You-Go](#)
 Resource group: [testwinvm](#)

DEPLOYMENT DETAILS [\(Download\)](#)

Start time: 3/15/2019, 5:36:25 PM
 Duration: 10 minutes 30 seconds
 Correlation ID: ac7a1126-edd1-4233-b7cc-403f73cf7b7e

RESOURCE	TYPE	STATUS	OPERATION DETAILS
 mytestvm	Microsoft.Compute/virtualMachines	Created	Operation details
 mytestvm734	Microsoft.Network/networkInterfaces	Created	Operation details

- You can check the VM status screenshot on the *Boot Diagnostics* page to confirm the status of the VM.

Home > CreateVm-win7x86imagetest-20190315173537 - Overview > mytestvm - Boot diagnostics

mytestvm - Boot diagnostics
Virtual machine

Search (Ctrl+/) Refresh Settings

Monitoring

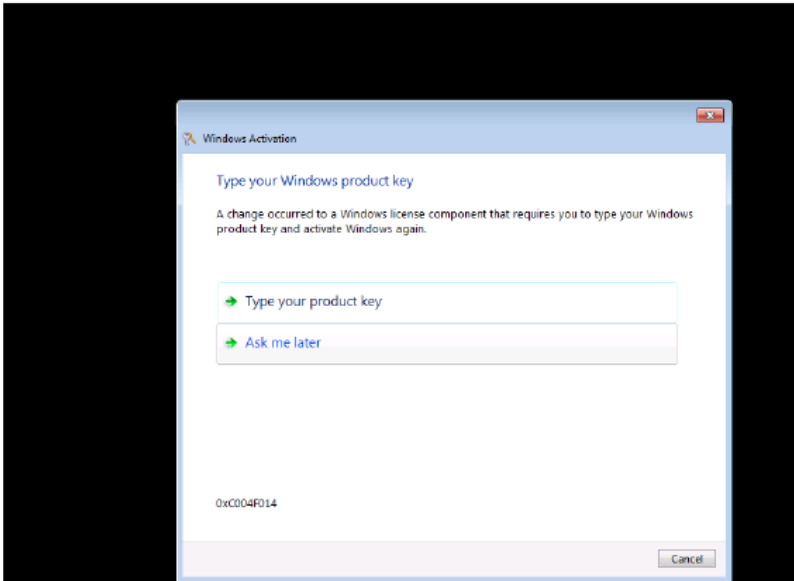
- Insights (preview)
- Alerts
- Metrics
- Diagnostics settings
- Advisor recommendations
- Logs
- Connection monitor

Support + troubleshooting

- Resource health
- Boot diagnostics**
- Performance diagnostics (Pr...
- Reset password
- Redeploy
- Serial console
- Connection troubleshoot

Screenshot Serial log

Updated: Saturday, March 16, 2019, 12:42:47 AM UTC [Download screenshot](#)



- Activate the Windows image through the Windows command prompt:

```
slmgr.vbs -ipk 00000-00000-00000-00000-00000
slmgr.vbs -ato
```

- If required, you can customize the VM.
- Shut down the VM (example: `cmd: shutdown -s -f -t 5`).
If the VM deployment task is still running, it should be canceled.

Delete Cancel Redeploy Refresh

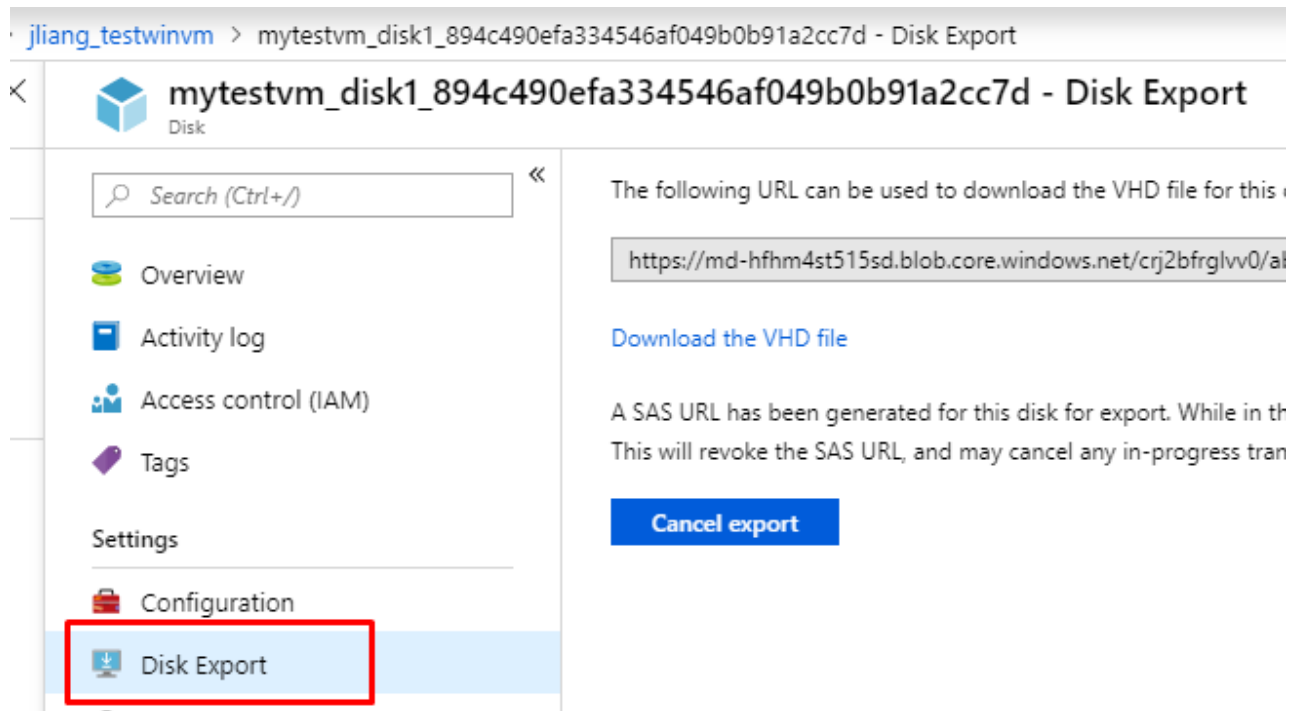
Canceled

Check the status of your deployment, manage resources, or troubleshoot deployment



Deployment name: CreateVm-win7x86imagetest-20190315173537
Subscription: [Pay-As-You-Go](#)
Resource group: [testwinvm](#)

- In the *Resource Group* pane for the VM in Azure portal, *Delete* the virtual machine. Do not delete anything else.
- Once deleted, go to the details of the disk assigned to the VM and select *Disk Export*. Confirm and generate the export download link for the VHD file.



- Use the `azcopy` command in the Azure CLI to import the customized windows VHD image into your Azure blob.

```
$ azcopy --source [above_VHD_export_link] --destination \
  https://[your_blob_URL]/win7/customizedWIN7X86VM.vhd \
  --dest-key [your_storage_account_key]
```

- The customized Windows VM is now ready for FSA Azure.

To import your custom VM into FSA Azure, use the `vm-customized` command in the FSA CLI.

For example:

```
> azure-vm-customized -cn -voWindows7_64 -vnWIN7X64VMvhd -s[Subscription ID] -g[this_
resource_group_name] -a[this_storage_account_name] -k[this_storage_account_key] -
fcustomwinvm -bcustomizedWIN7X64VM.vhd -r
```

```
> azure-vm-customized -cn -voWindows7 -vnWIN7X86VMvhd -s[Subscription ID] -g[this_
resource_group_name] -a[this_storage_account_name] -k[this_storage_account_key] -f
[this_blob_name] -bcustomizedWIN7X86VM.vhd -r
```

Change Log

Date	Change Description
2019-02-19	Initial release.
2019-03-25	Added Optional: Creating a custom VM on Azure on page 24 .
2019-06-07	Added About FortiSandbox VM on Azure on page 4 Added additional information to Deploying FortiSandbox VM on Azure (Basic) on page 6 .



FORTINET[®]



Copyright© 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.