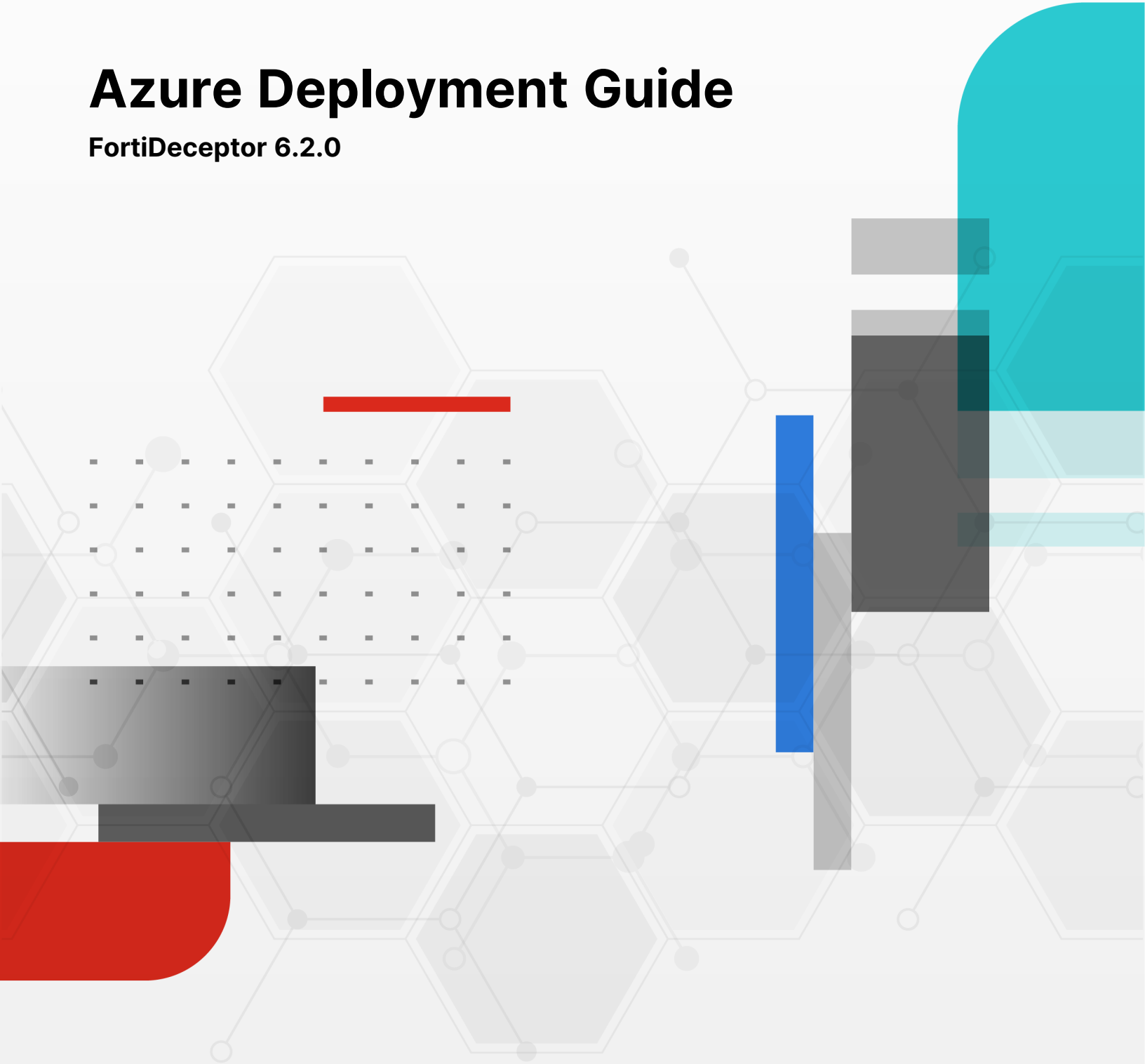


# Azure Deployment Guide

FortiDeceptor 6.2.0



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO LIBRARY**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

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

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD LABS**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

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

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



October 23, 2025

FortiDeceptor 6.2.0 Azure Deployment Guide

00-610-769881-20251023

# TABLE OF CONTENTS

<b>Change Log</b> .....	<b>4</b>
<b>About FortiDeceptor VM on Azure</b> .....	<b>5</b>
<b>Licensing</b> .....	<b>6</b>
<b>FortiDeceptor Cloud topology</b> .....	<b>7</b>
<b>Minimum system requirements</b> .....	<b>8</b>
<b>Deploying FortiDeceptor on Azure</b> .....	<b>9</b>
Preparing the FortiDeceptor image .....	9
Creating resource groups .....	10
Uploading FortiDeceptor VHD to Azure .....	12
Preparing the network .....	15
Creating a virtual network .....	15
Creating network security groups and rules .....	17
Create VM with the FortiDeceptor VHD .....	20
<b>Configuring the FortiDeceptor Manager and Azure Client</b> .....	<b>29</b>
Configuring the Azure client .....	29
<b>Configuring FortiDeceptor Manager</b> .....	<b>32</b>
Managing cloud clients .....	33
Configuring the deployment network .....	34
Deploying decoys .....	35

# Change Log

Date	Change Description
2025-10-03	Initial release.
2025-10-23	Updated <a href="#">Configuring the Azure client on page 29</a> , <a href="#">Configuring FortiDeceptor Manager on page 32</a> , <a href="#">Managing cloud clients on page 33</a> , and <a href="#">Deploying decoys on page 35</a> .

# About FortiDeceptor VM on Azure

FortiDeceptor VM is a 64-bit virtual appliance version of FortiDeceptor that is deployed in a virtual machine environment. Once the virtual appliance is deployed and set up, you can manage FortiDeceptor VM via its GUI in a web browser on your management computer.

This document provides information about deploying a FortiDeceptor VM in Microsoft Azure environments. This includes how to configure the virtual hardware settings of the virtual appliance. This guide presumes the reader has a thorough understanding of virtualization servers.

This document does not cover configuration and operation of the virtual appliance after it has been successfully installed and started. For that information, see the [FortiDeceptor Administration Guide](#) in the [Fortinet Document Library](#).

# Licensing

Fortinet offers the FortiDeceptor in a stackable license model. This model allows you to expand your VM solution as your environment expands. For information on purchasing a FortiDeceptor license, contact your Fortinet Authorized Reseller, or visit [https://www.fortinet.com/how\\_to\\_buy/](https://www.fortinet.com/how_to_buy/).

When configuring your FortiDeceptor, ensure that you configure hardware settings as outlined in the following table and consider future expansion. Contact your Fortinet Authorized Reseller for more information.

Technical Specification	Details
Azure Support	Standard B2s for 2 nics Standard A8 v2 for 6 nics
Virtual CPUs (min / max)	4/ Unlimited
Virtual Network Interfaces	2-6
Virtual Memory (min / max)	8GB / Unlimited
Virtual Storage (min / max)	HDD 50GB/ 16TB

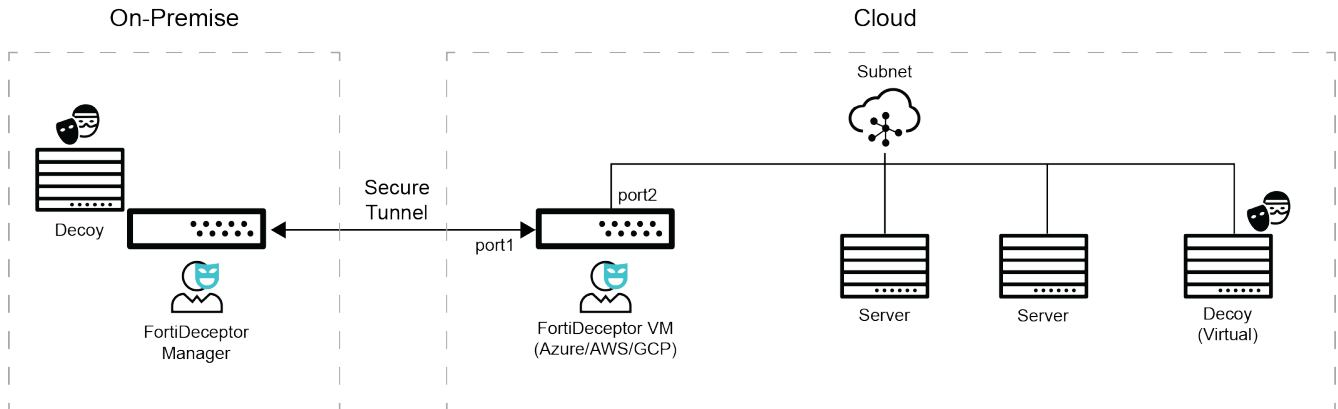
For more information, see the FortiDeceptor product data sheet available on the Fortinet web site, <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiDeceptor.pdf>.

After placing an order for FortiDeceptor, a license registration code is sent to the email address used in the order form. Use the license registration code provided to register the FortiDeceptor with Customer Service & Support at <https://support.fortinet.com>.

Upon registration, you can download the license file. You will need this file to activate your FortiDeceptor. You can configure basic network settings from the CLI to complete the deployment. Once the license file is uploaded and validated, the CLI and GUI will be fully functional.

# FortiDeceptor Cloud topology

The cloud appliance is deployed over the public infrastructure but uses a different method for decoy deployment. This new method requires less HW requirements for the cloud appliance itself.



The cloud decoy deployment method is as follows:

- The cloud appliance will be deployed over the cloud infrastructure.
- An on-premise FortiDeceptor Manager will manage the cloud appliance over a propriety network tunnel.
- The propriety network tunnel allows managing the cloud appliance and decoy deployment provisioning over layer2 tunnel communication over layer3.
- The cloud appliance network interfaces will hold IP addresses in the cloud segment. Each IP address represents a network decoy.
- The network decoy will run on the on-premise FortiDeceptor Manager and use the same IP address as the cloud appliance network interfaces.
- The cloud IP address will tunnel over Layer2 to the IP address on the on-premise FortiDeceptor Manager.
- The idea is to run a light appliance in the cloud while running the actual network decoys inside the on-premise FortiDeceptor Manager in a sandbox mode. The cloud network is isolated from the rest of the decoys, the on-premise networks.

While the cloud appliance uses different hardware requirements, the on-premise FortiDeceptor Manager HW requirements that should serve the cloud appliance decoys is the same concept as today.

# Minimum system requirements

The following are the minimum system requirements for deploying decoys with FortiDeceptor for Azure:

Technical Specification	Details
<b>Azure Support</b>	Standard B2s for 2 nics Standard A8 v2 for 6 nics
<b>Virtual CPUs (min / max)</b>	4/ Unlimited
<b>Virtual Network Interfaces</b>	2-6
<b>Virtual Memory (min / max)</b>	8GB / Unlimited
<b>Virtual Storage (min / max)</b>	Cloud manager: HDD 500GB/ 16TB Cloud clients: HDD 50GB/ 16TB

# Deploying FortiDeceptor on Azure

To deploy FortiDeceptor VM on Azure, download the FortiDeceptor image file for Azure from FortiCloud. Next you will create resource groups in the Azure portal and upload the FortiDeceptor VHD. After the VHD is uploaded, prepare the network and then create the VM with FortiDeceptor VHD.

## To deploy FortiDeceptor VM on Azure:

1. Prepare the FortiDeceptor image.
2. Create resource groups.
3. Upload FortiDeceptor VHD to Azure.
4. Prepare the network.
5. Create the VM.

## Preparing the FortiDeceptor image

Download the image archive file for the Azure platform. and unzip it to get image file for *fdc.azure.vhd*.

## To download the FortiDeceptor image:

1. Log in to [FortiCloud](#).
2. In the banner, click *Support > Downloads > Firmware Download*. The *Download/Firmware Images* page opens.
3. From the *Select Product* dropdown, select *FortiDeceptor*.
4. Click the *Download* tab.
5. In the *Image File Path* section, click the image folder until you reach the image page.

6. Select *FDC\_VM-vx.x.x-buildxxxx-FORTINET.out.azure.zip*

FortiCloud Services Support

Download / Firmware Images Account Name/ID: Fortinet

Firmware Images Fortinet Firmware Images And Software Releases

Welcome to the Firmware Images download center for Fortinet's extensive line of security solutions.

Select Product

FortiDeceptor

Release Notes Download

Image File Path

/ FortiDeceptor/ v4.00/ 4.1/ 4.1.0/

Image Folders/Files

[Up to higher level directory](#)

Name	Size (KB)	Date Created	Date Modified	
FDC_1000F-v400-build0128-FORTINET.out	200,705	2021-12-16 16:12:30	2021-12-16 16:12:59	<a href="#">HTTPS Checksum</a>
FDC_1000G-v400-build0128-FORTINET.out	200,705	2021-12-16 16:12:37	2021-12-16 16:12:26	<a href="#">HTTPS Checksum</a>
FDC_VM-v400-build0128-FORTINET.out	200,705	2021-12-16 16:12:48	2021-12-16 16:12:29	<a href="#">HTTPS Checksum</a>
FDC_VM-v400-build0128-FORTINET.out.aws.zip	128,782	2021-12-16 16:12:16	2021-12-16 16:12:37	<a href="#">HTTPS Checksum</a>
FDC_VM-v400-build0128-FORTINET.out.azure.zip	128,580	2021-12-16 16:12:23	2021-12-16 16:12:03	<a href="#">HTTPS Checksum</a>
FDC_VM-v400-build0128-FORTINET.out.gcp.tar.gz	128,587	2021-12-16 16:12:29	2021-12-16 16:12:58	<a href="#">HTTPS Checksum</a>
FDC_VM-v400-build0128-FORTINET.out.kvm.zip	127,648	2021-12-16 16:12:59	2021-12-16 16:12:15	<a href="#">HTTPS Checksum</a>
FDC_VM-v400-build0128-FORTINET.out.ovf.esx.zip	127,500	2021-12-16 16:12:17	2021-12-16 16:12:48	<a href="#">HTTPS Checksum</a>
FDC_VM-v400-build0128-FORTINET.out.vmware.zip	127,661	2021-12-16 16:12:51	2021-12-16 16:12:17	<a href="#">HTTPS Checksum</a>

7. Extract the .zip file.

## Creating resource groups

Create a resource group and then add your resources. This allows you to deploy, update, and delete the resources as a group.

**To create a resource group:**

1. Log in to the Azure portal and go to *Resource groups*.

Search resources, services, and docs (G+)

Create a resource

Home

Dashboard

All services

FAVORITES

All resources

Resource groups

App Services

Featured

Azure Active Directory

Virtual machines

Resource groups

App Services

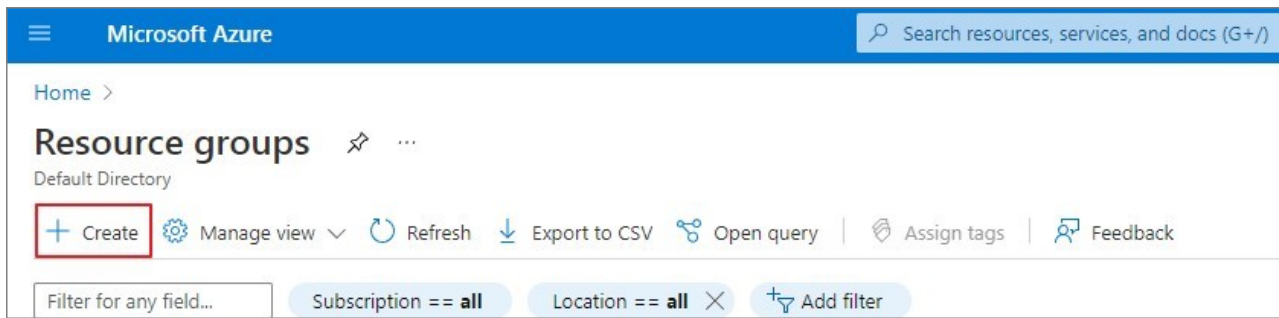
Storage accounts

SQL databases

Cost Management

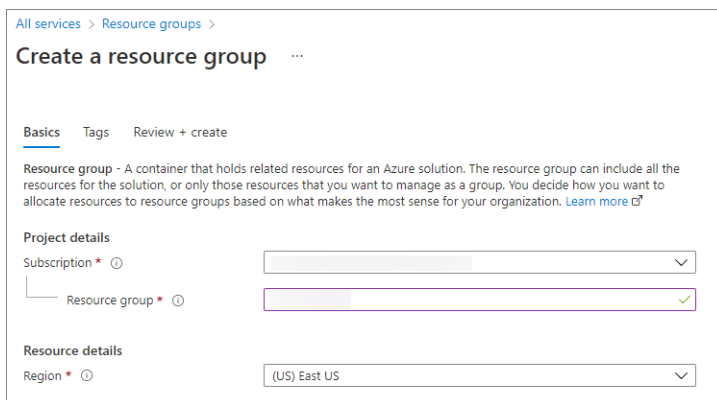
Virtual networks

2. Click *Create*.



3. Select or enter the following property values:

<b>Subscription</b>	Select an Azure subscription.
<b>Resource group</b>	Enter a name for the resource group.
<b>Region</b>	Specify an Azure location. This location is where the resource group stores metadata about the resources. For compliance reasons, you may want to specify where that metadata is stored. We recommend that you specify a location where most of your resources will be stored. Using the same location can simplify your template.

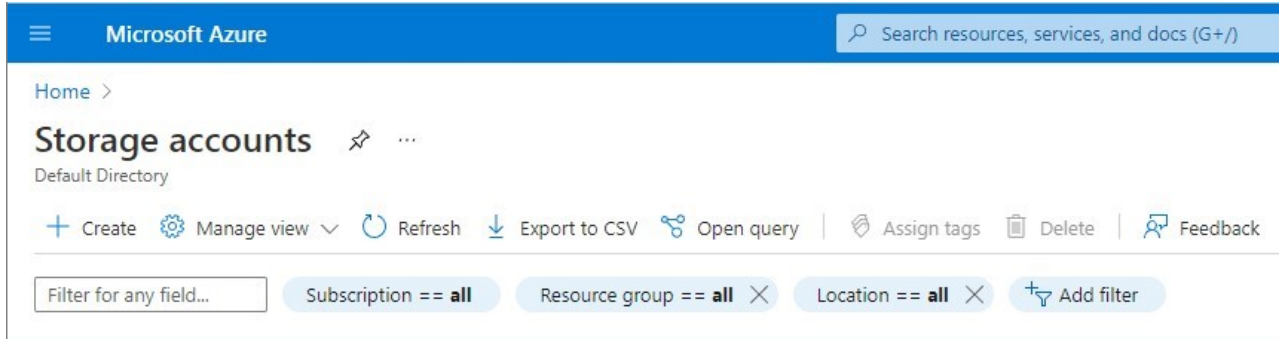


4. Click *Review + Create*. The resource group is validated.
5. Click *Create*.

# Uploading FortiDeceptor VHD to Azure

## To upload FortiDeceptor VHD to Azure:

1. In the portal menu, click *Storage accounts*.
2. On the *Storage accounts* page, click *Create*. The *Create a storage account* page opens.

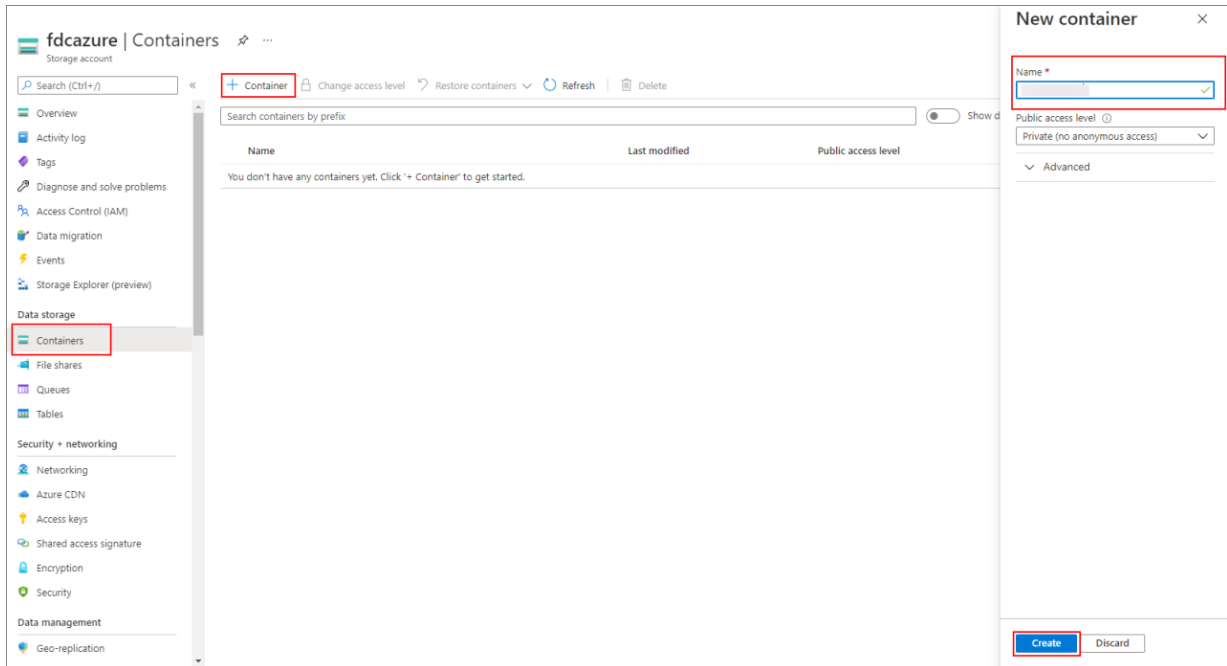


3. In the *Basics* tab, configure the storage account details. The image below shows the basic configuration for FortiDeceptor.

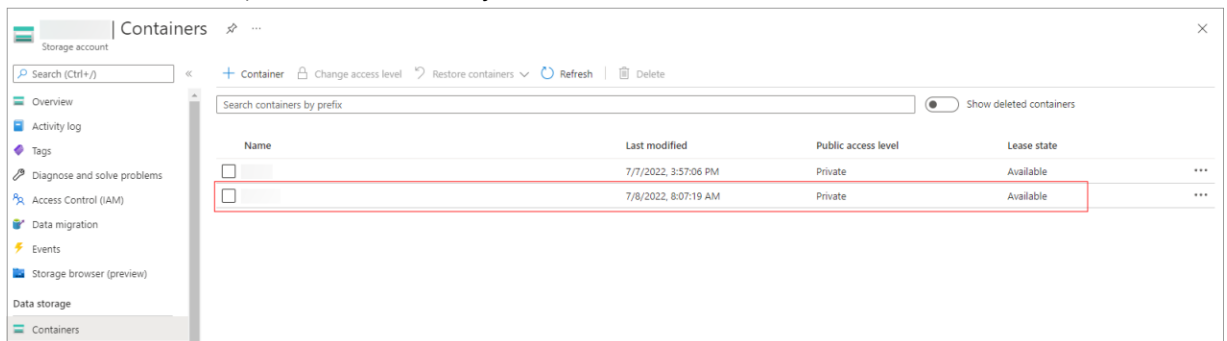
4. <b>Subscription</b>	Select a subscription from the dropdown.
<b>Resource group</b>	Select a resource group from the dropdown.
<b>Storage account name</b>	Enter a name for the storage account.
<b>Region</b>	Select a region from the dropdown.
<b>Performance</b>	Select <i>Standard: Recommended for most scenarios (general-purpose v2 account)</i> .
<b>Redundancy</b>	Select <i>Geo-redundant storage (GRS)</i> .
<b>Make read access to data available in the event of regional unavailability</b>	Enable.

The screenshot shows the 'Create a storage account' page in the Azure portal. The page is titled 'Create a storage account' and has tabs for 'Basics', 'Advanced', 'Networking', 'Data protection', 'Tags', and 'Review + create'. The 'Basics' tab is selected. Below the tabs, there is a instruction: '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.' There are two dropdown menus: 'Subscription \*' and 'Resource group \*'. Below these is the 'Instance details' section. It contains a link: 'If you need to create a legacy storage account type, please click [here](#).' There are four fields: 'Storage account name \*' (text input), 'Region \*' (dropdown menu showing '(US) East US'), 'Performance \*' (radio buttons for 'Standard: Recommended for most scenarios (general-purpose v2 account)' and 'Premium: Recommended for scenarios that require low latency.'), and 'Redundancy \*' (dropdown menu showing 'Geo-redundant storage (GRS)' with a checked checkbox for 'Make read access to data available in the event of regional unavailability.'). At the bottom, there are three buttons: 'Review + create' (blue), '< Previous', and 'Next: Advanced >'.

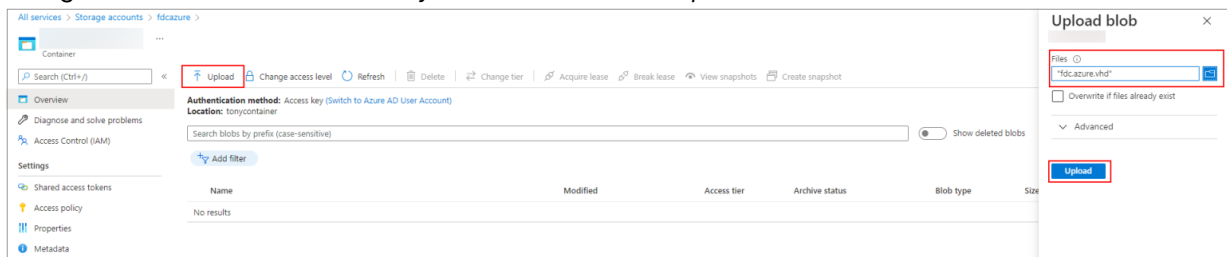
5. Click *Review + Create*. The account is validated.
6. Click *Create*.
7. Create a storage container to upload FortiDeceptor VHD.
  - a. Open the storage account you created.
  - b. In the portal menu, go to *Data storage > Containers*.
  - c. Click *+Container*. The *New container* pane opens.
  - d. Type a *Name* for your new container and set the *Public access level*.
  - e. Click *Create*.



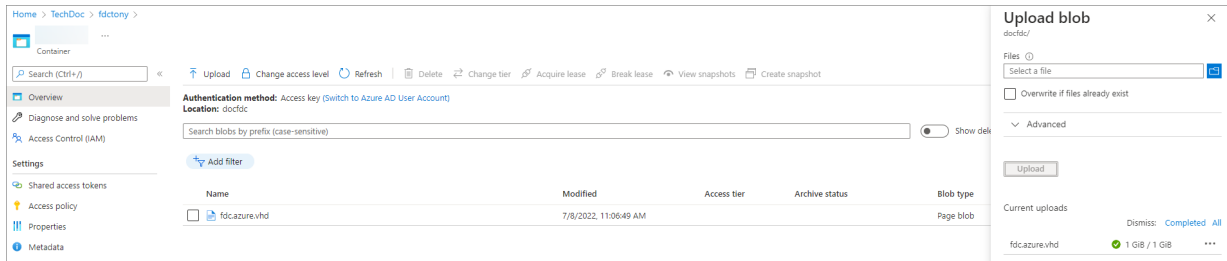
8. Upload FortiDeceptor VHD to the container.
  - a. In the containers list, click the container you created.



- b. Click *Upload*. The *Upload blob* pane opens.
- c. Navigate to the `fdc.azure.vhd` on your device and click *Upload*.



The .vhd file is added to the container.



## Preparing the network

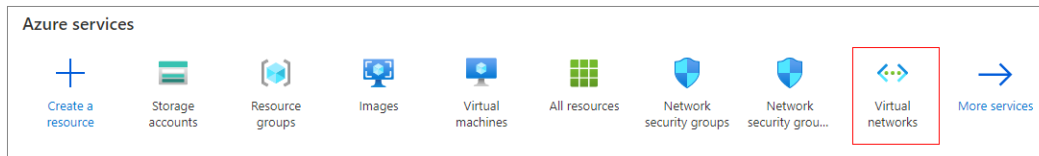
### Creating a virtual network

Create a virtual network and add several subnets for FortiDeceptor management and deployment.

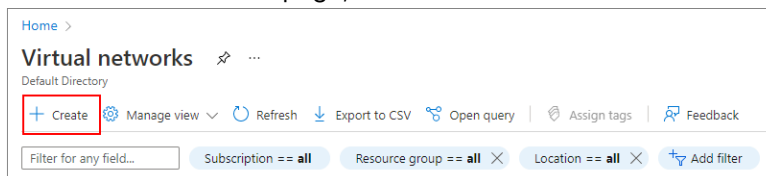
**To create a virtual network:**

1. Create a Virtual Network.

- a. In the portal menu, click *Virtual networks*.

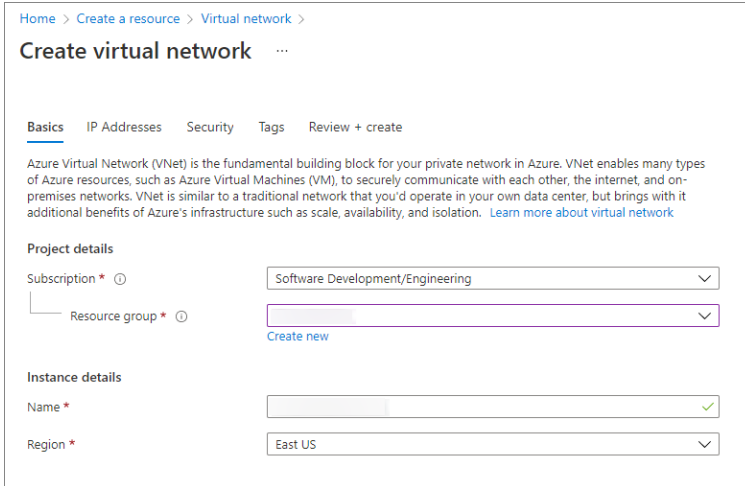


- b. In the *Virtual Networks* page, click *Create*.

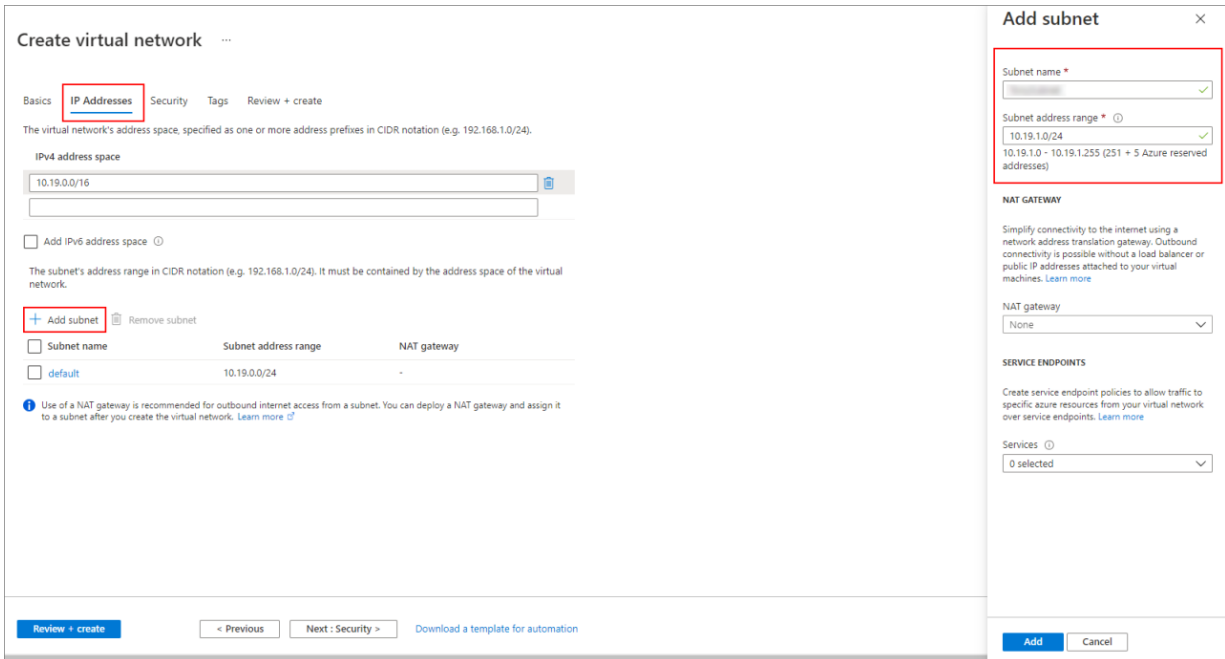


- c. In the *Basics* tab, configure the network details.

<b>Subscription</b>	Select a subscription from the dropdown.
<b>Resource group</b>	Select a resource group from the dropdown.
<b>Name</b>	Enter a name for the instance.
<b>Region</b>	Select a region from the dropdown.



2. Create Subnets in the Virtual Network.
  - a. Click the *IP Addresses* tab.
  - b. Configure the *IPv4 address space*.
  - c. Click *Add subnet*. The *Add subnet* pane opens.
  - d. Configure the *Subnet address range* and click *Add*.



- e. (Optional) Add additional subnets. You can add up to six subnets.

**Create virtual network** ...

Basics **IP Addresses** Security Tags Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space

10.19.0.0/16

Add IPv6 address space ⓘ

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

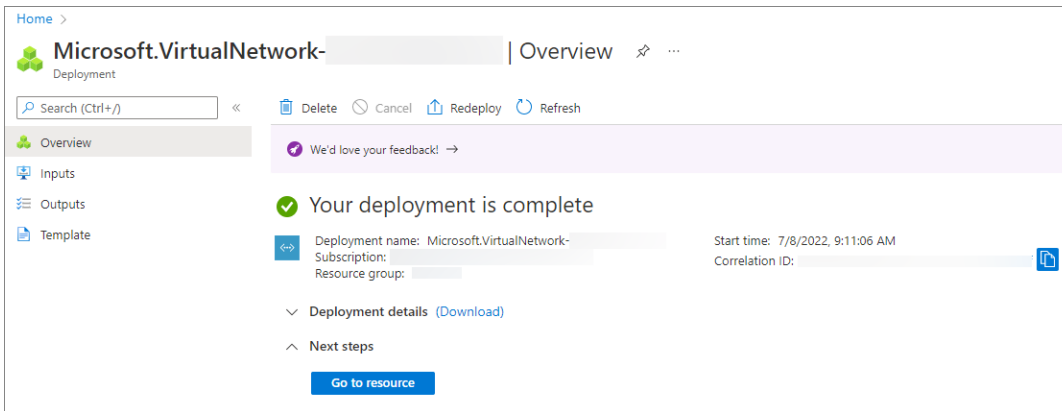
+ Add subnet Remove subnet

<input type="checkbox"/> Subnet name	Subnet address range	NAT gateway
<input type="checkbox"/> default	10.19.0.0/24	-
<input type="checkbox"/> subnet361	10.19.1.0/24	-
<input type="checkbox"/> subnet362	10.19.2.0/24	-
<input type="checkbox"/> subnet363	10.19.3.0/24	-
<input type="checkbox"/> subnet364	10.19.4.0/24	-
<input type="checkbox"/> subnet365	10.19.5.0/24	-

**i** Use of a NAT gateway is recommended for outbound internet access from a subnet. You can deploy a NAT gateway and assign it to a subnet after you create the virtual network. [Learn more](#) ⓘ

**Review + create** < Previous Next: Security > Download a template for automation

- f. Click *Review + Create*. The virtual network is validated.
- g. Click *Create*. The virtual network is created.

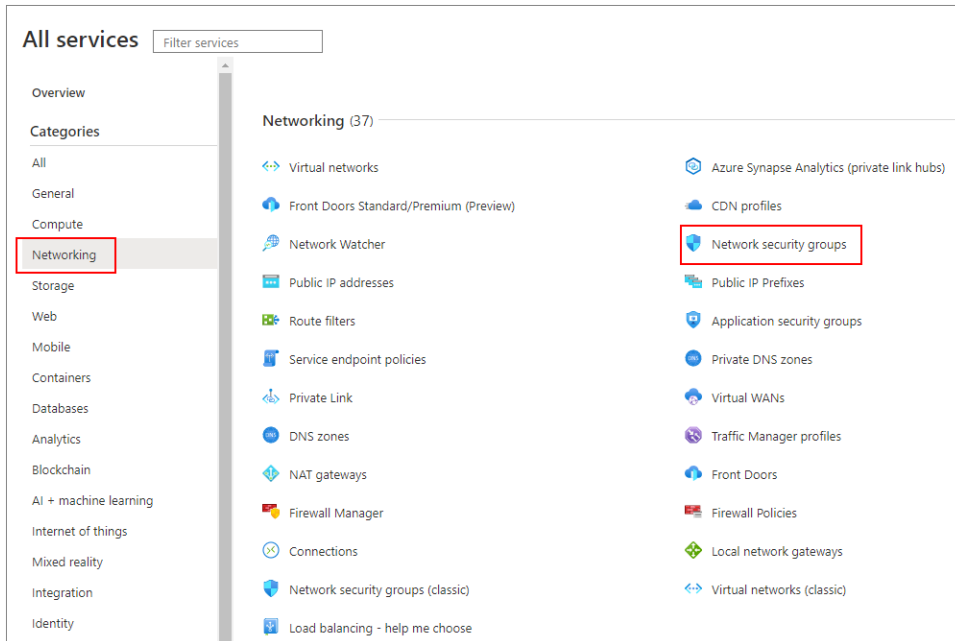


## Creating network security groups and rules

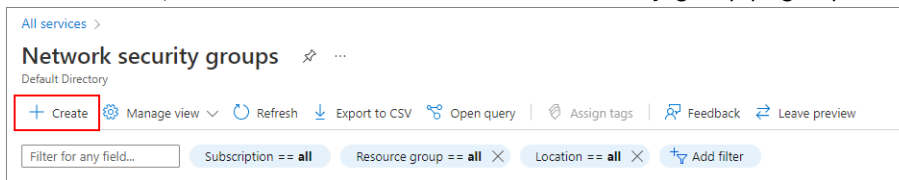
Create a network security group and add security rules for filtering network traffic to and from FortiDeceptor in a virtual network.

**To create a network security group and add rules:**

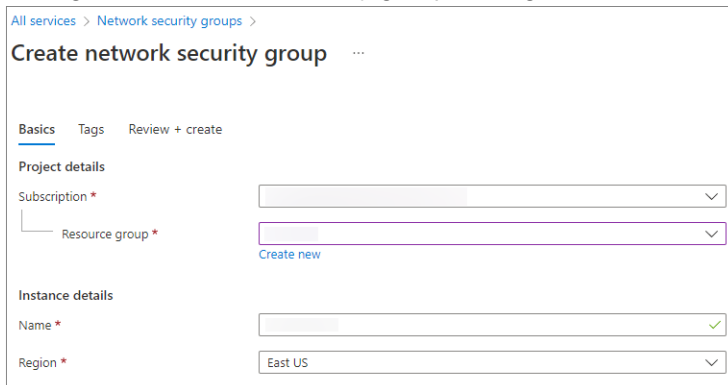
1. From the *Home* page, click *Create a resource*.
2. In the navigation menu, click *Networking > Network security groups*.



3. In the toolbar, click *Create*. The *Create network security group* page opens.

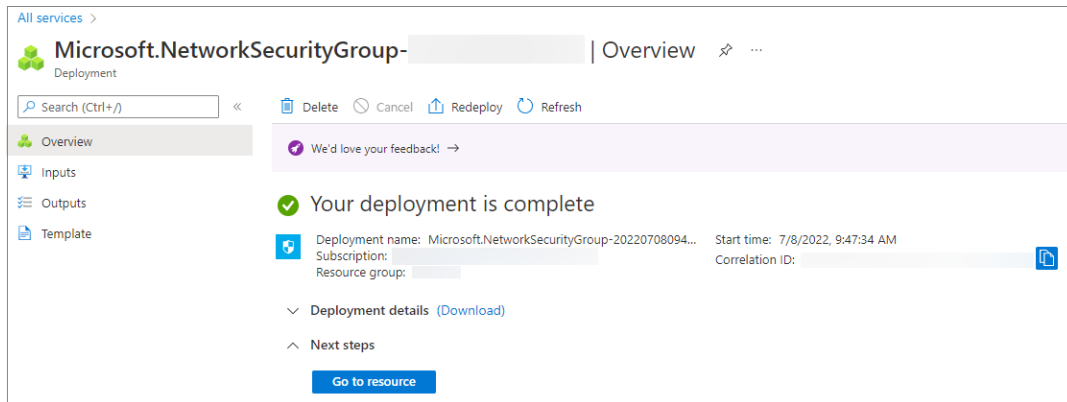


4. Configure the network security group settings and click *Review + Create*. The security group is validated.

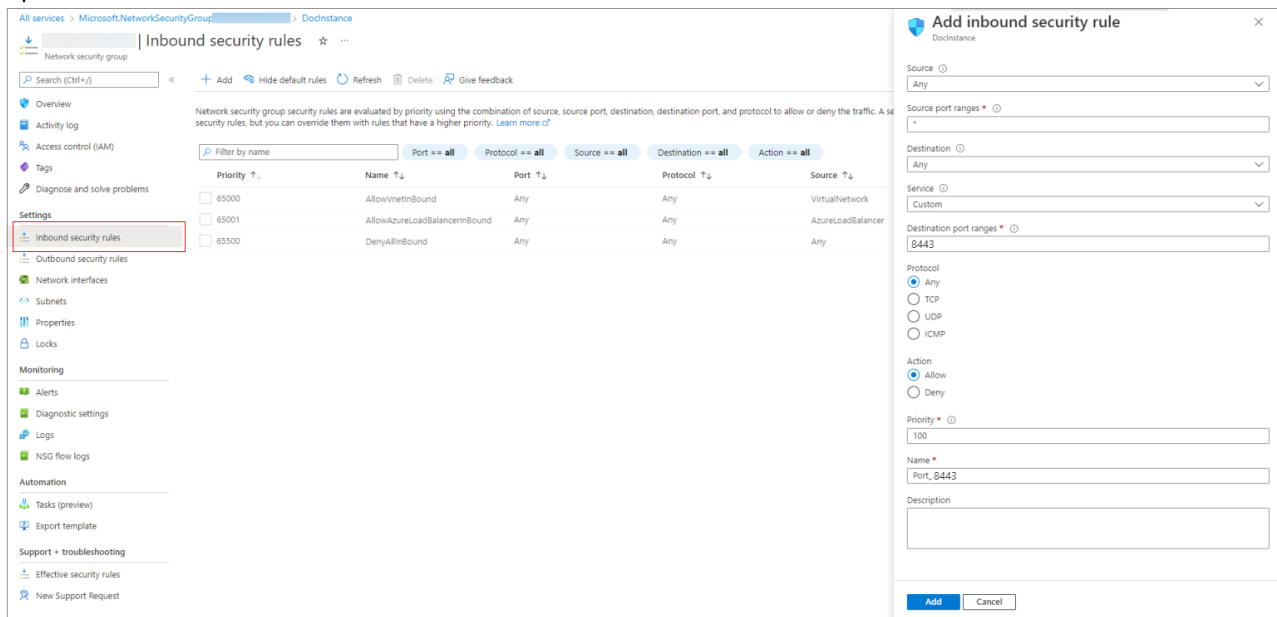


5. Click *Create*. The security group is created.


6. Click *Go to resource*.



7. In the menu go to *Settings > Inbound security rules* and click *Add*. The *Add inbound security rule* pane opens.



8. Configure the *Source*, *Source port ranges*, and *Destination port ranges*, and click *Add*.

<b>Source</b>	Select a source from the dropdown.
<b>Source port ranges</b>	Enter the port source ranges.
<b>Destination port ranges</b>	Enter the destination port ranges.
	 <p>Make sure to enable an inbound rule for port 22, 443 and 8443 for the client's first interface/port1 to manage FortiDeceptor cloud appliances. This enables the FortiDeceptor Manager to communicate with the cloud clients.</p>
<b>Protocol</b>	Select <i>TCP</i> .

**Add inbound security rule**

Source: Any

Source port ranges: \*

Destination: Any

Service: Custom

Destination port ranges: 8443

Protocol:  TCP

Action:  Allow

Priority: 100

Name: Port\_8443

Description:

**Add** Cancel

9. (Optional) Open additional ports. For example, you can enable port 443, 445, 80, and add other inbound/outbound rules as needed.

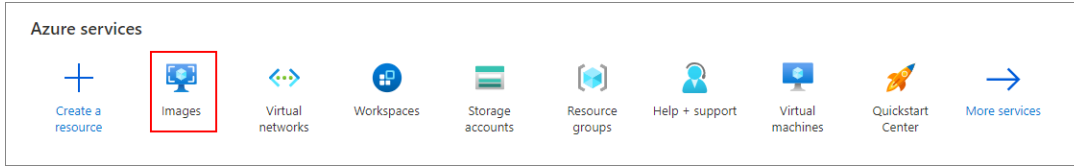
Priority	Name	Port	Protocol	Source	Destination	Action
100	Port_443	443	TCP	Any	Any	Allow
110	Port_8443	8443	TCP	Any	Any	Allow
120	Port_445	445	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

## Create VM with the FortiDeceptor VHD

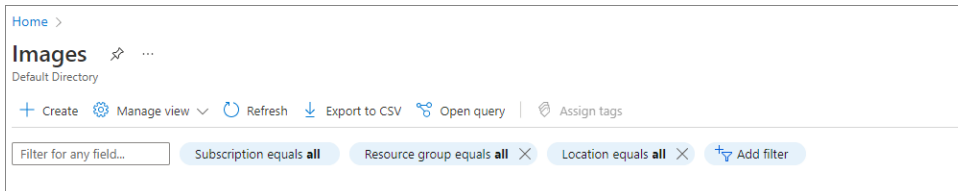
Create a virtual machine and specify the details of the image, disk and network.

**To create an image the VHD:**

1. In the portal menu, click *Images*.



2. Click *Create*.



3. Configure the following settings and click *Review + Create*.

<b>Subscription</b>	Select a subscription from the dropdown.
<b>Resource group</b>	Select a resource group from the dropdown.
<b>OS type</b>	Linux
<b>VM generation</b>	Gen1
<b>Storage blob</b>	https://.../xxxcontainer/fdc.azure.vhd
<b>Account type</b>	Standard SSD
<b>Host caching</b>	Read/write

[Home](#) > [Images](#) >

## Create an image

Subscription \* ⓘ

Resource group \* ⓘ  [Create new](#)

**Instance details**

Name \*

Region \* ⓘ

Zone resiliency ⓘ

**OS disk**

OS type \* ⓘ  Windows  Linux

VM generation \* ⓘ  Gen 1  Gen 2

Storage blob \* ⓘ   [Browse](#)

Account type \* ⓘ

Host caching \* ⓘ

**Encryption**

You can encrypt the OS and data disks with a platform-managed or customer-managed key. [Learn more](#)

Encryption type \*

**Data disk**

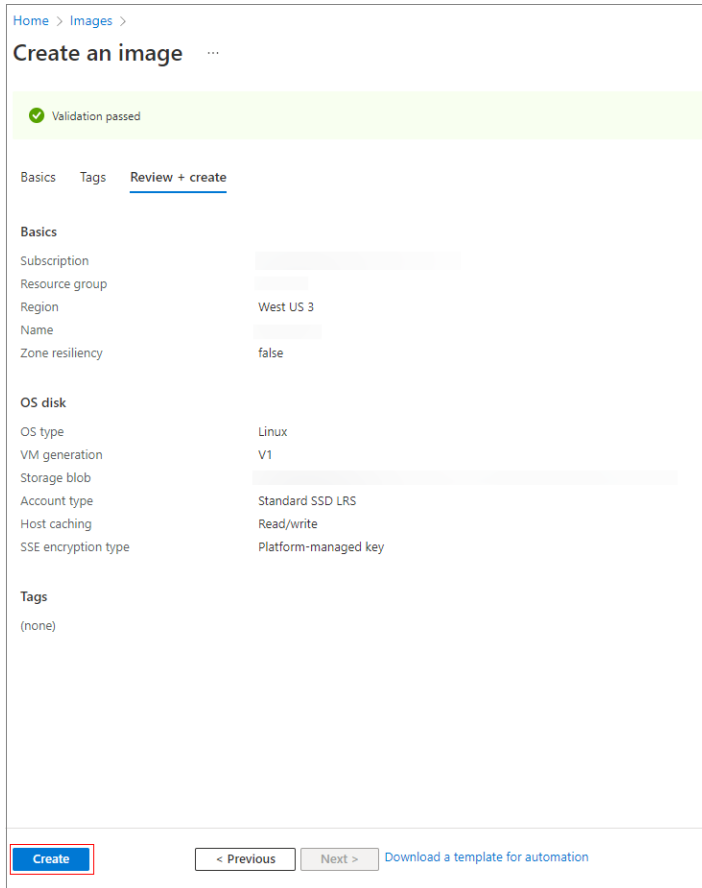
[+ Add data disk](#)

[Review + create](#)

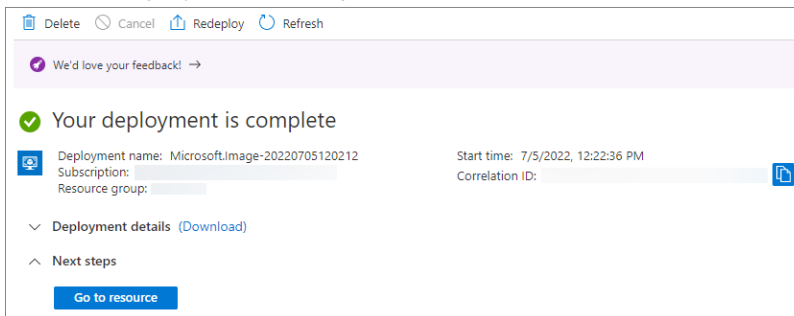
[< Previous](#)

[Next : Tags >](#)

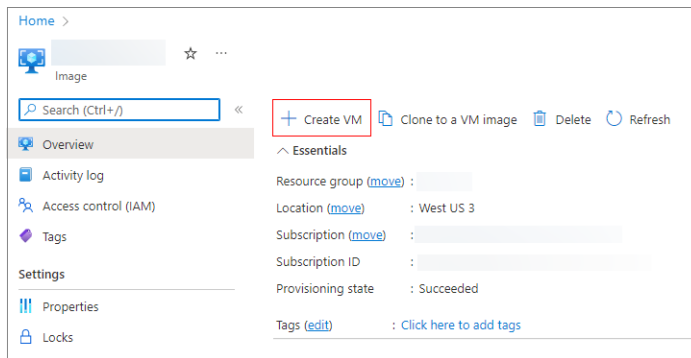
4. Click *Create*.



5. After the deployment is complete, click *Go to resource*.



6. Click *Create VM*.



7. In the *Basics* tab, configure the following settings:

<b>Subscription</b>	Select a subscription from the dropdown.
<b>Resource group</b>	Select the group that contains the VHD image.
<b>Virtual machine name</b>	Enter a name for the virtual machine.
<b>Images</b>	Select the FortiDeceptor image from the list. The image is uploaded for you when you create the VM from the image.
<b>Size</b>	Select the image size from the list. Different sizes support different Max NICs. To learn which size is suitable for your VM see, <a href="https://docs.microsoft.com/en-us/azure/virtual-machines/sizes-general">https://docs.microsoft.com/en-us/azure/virtual-machines/sizes-general</a> .
<b>Authentication type</b>	Select <i>SSH public key</i> or <i>Password</i> .
<b>Select inbound ports</b>	Select <i>HTTPS (443)</i> , <i>SSH (22)</i> .
<b>License type</b>	Select <i>Other</i> .

8. Click *Disks* tab.

- a. Scroll down to *Data disks for <vm\_name >* and click *Create and attach a new disk*.

- b. Configure the following settings and click *OK*.

<b>Name</b>	Enter a name for the disk.
<b>Source type</b>	Select <i>None (empty disk)</i> .
<b>Size</b>	Select a size greater than 50 GiB.
<b>Encryption type</b>	Select (Default) Encryption at-rest with a platform-managed key.
<b>Enable shared disk</b>	Select <i>No</i> .
<b>Delete disk with VM</b>	Enable.

Home > FDC\_Azure > Create a virtual machine >

### Create a new disk

Create a new disk to store applications and data on your VM. Disk pricing varies based on factors including disk size, storage type, and number of transactions. [Learn more](#)

Name \*

Source type \*

Size \*   
 Premium SSD LRS  
[Change size](#)

Encryption type \*

Enable shared disk  Yes  No

Delete disk with VM

9. Click the *Networking* tab and configure the following settings:

- Subnet** Select the subnet.
- Select inbound ports** Select *HTTPS (443), SSH (22)*.

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

Public inbound ports \*  None  Allow selected ports

**Select inbound ports \***

**⚠ This will allow all IP addresses to access your virtual machine.** This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

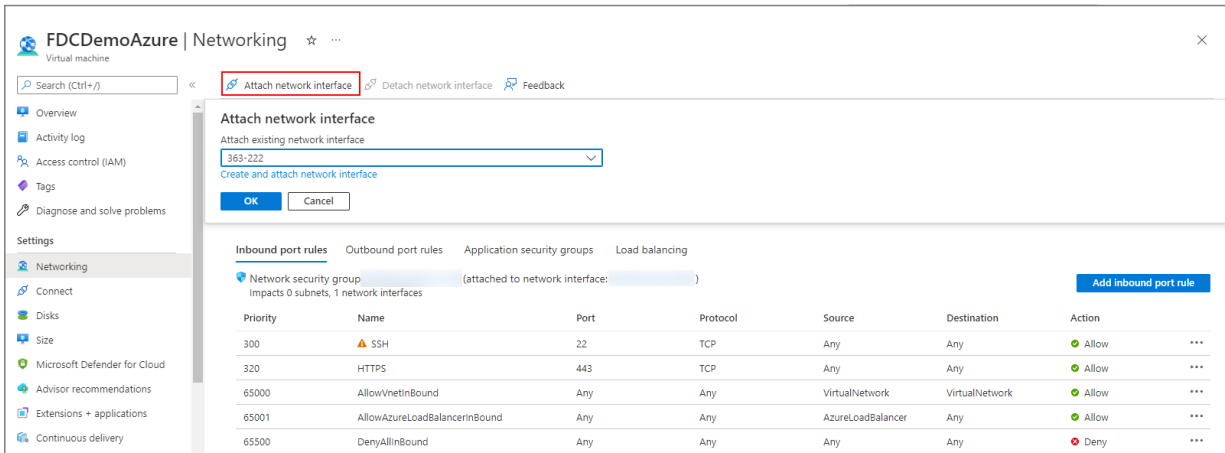
- 10. (Optional) Click the *Management* tab update the diagnostics settings.
- 11. Click *Review + Create* to create the virtual machine.



You may encounter an *OS Provisioning* error during deployment. This error can be ignored.

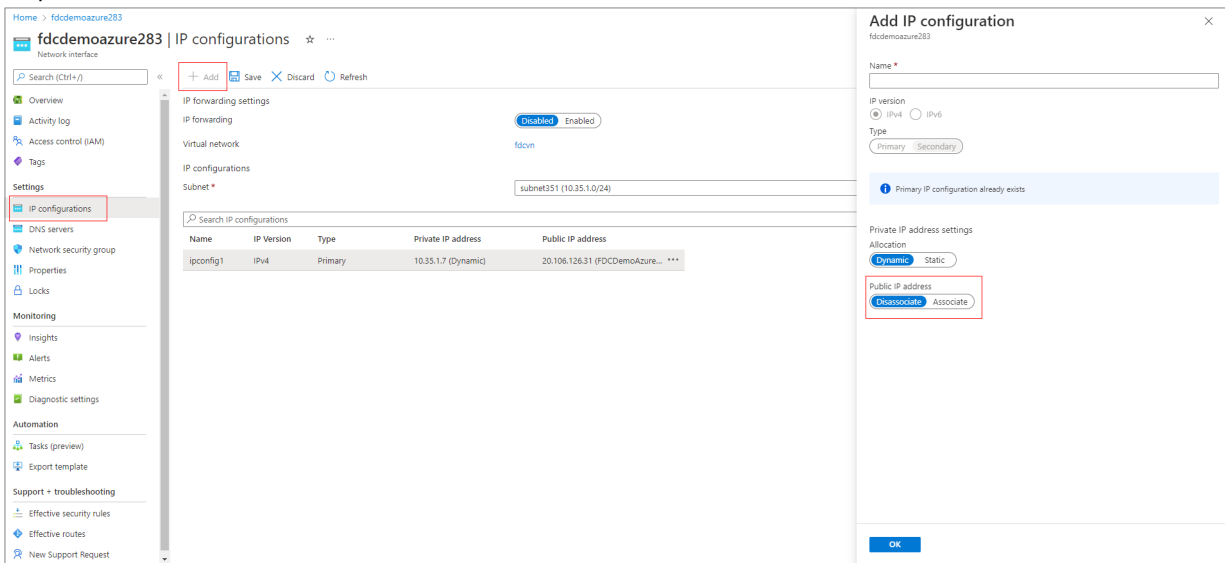
**12. Attach more interfaces.**

- a. Go to *Home > Virtual machines*, and click the VM to open it.
- b. Click *Stop*.
- c. Go to *Settings > Networking* and open the virtual machine you created.
- d. Click *Attach network interfaces* and then select the interface you want to attach. You must configure a minimum of two NICs. You can attach up to six interfaces.



**13. Associate the public IP to Port1.**

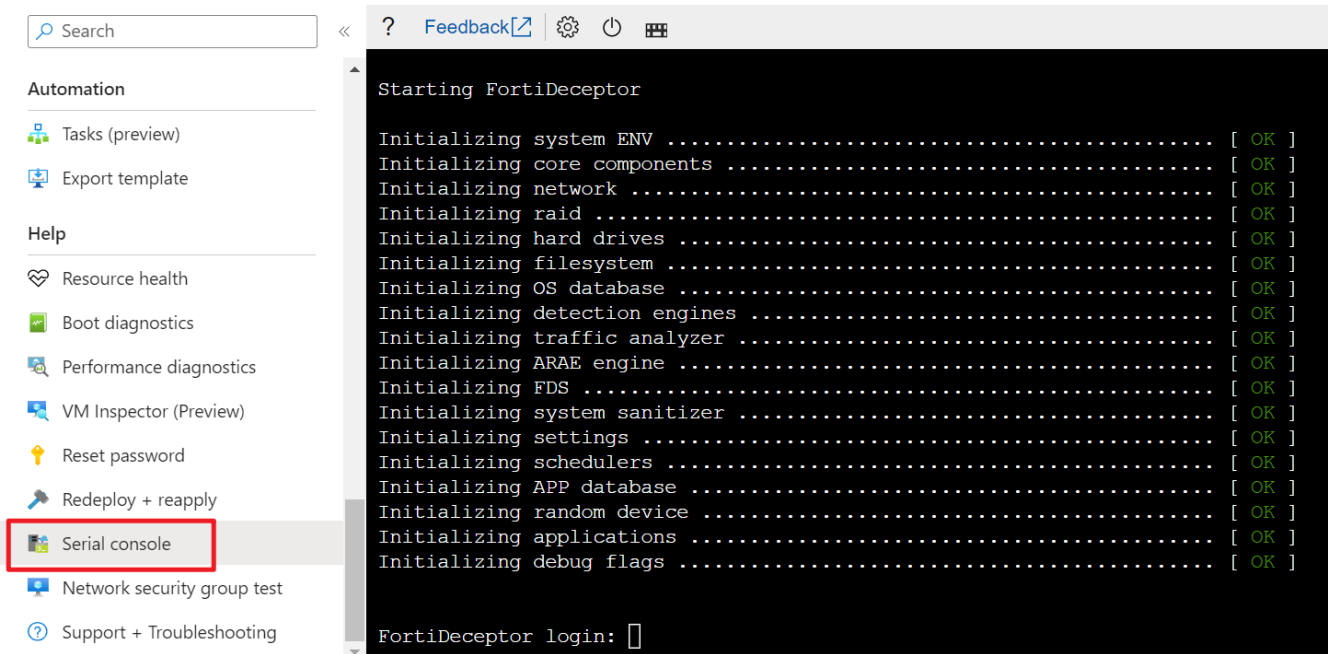
- a. Go to *Home* and open the Network Interface
- b. Go to *Settings > IP configurations*.
- c. Click *Add*. The *Add IP configuration* pane opens.
- d. Under *Public IP address* select *Associate*. Binding the cloud client with static public IP address is required.



**14. Start the VM.**

- a. Go to *Home* and click the VM to open it.
- b. Click *Start*.
- c. Go to *Home > Virtual machines*. Select your VM from the list.

d. Go to *Support + troubleshooting* > *Serial console* to access the VM with the Serial Console.



# Configuring the FortiDeceptor Manager and Azure Client

Configure the Azure client and then add FortiDeceptor as a cloud appliance. After the appliance is added, configure the deployment network and deploy the decoys.



We recommend setting up a security policy and trusted host to ensure the FortiDeceptor is running in a safe environment.

## To configure FortiDeceptor and Azure client:

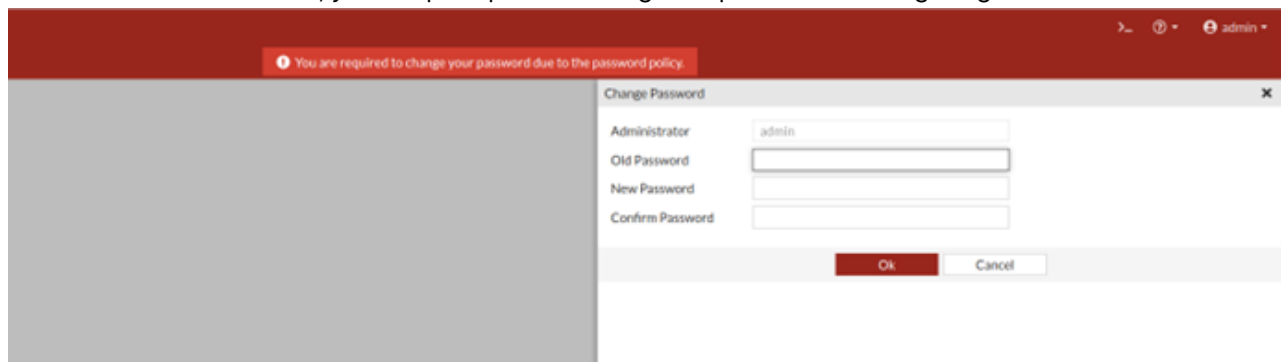
1. [Configuring the Azure client on page 29](#)
2. [Configuring FortiDeceptor Manager on page 32](#)
3. [Managing cloud clients on page 33](#)
4. [Configuring the deployment network on page 34](#)
5. [Deploying decoys on page 35](#)

## Configuring the Azure client

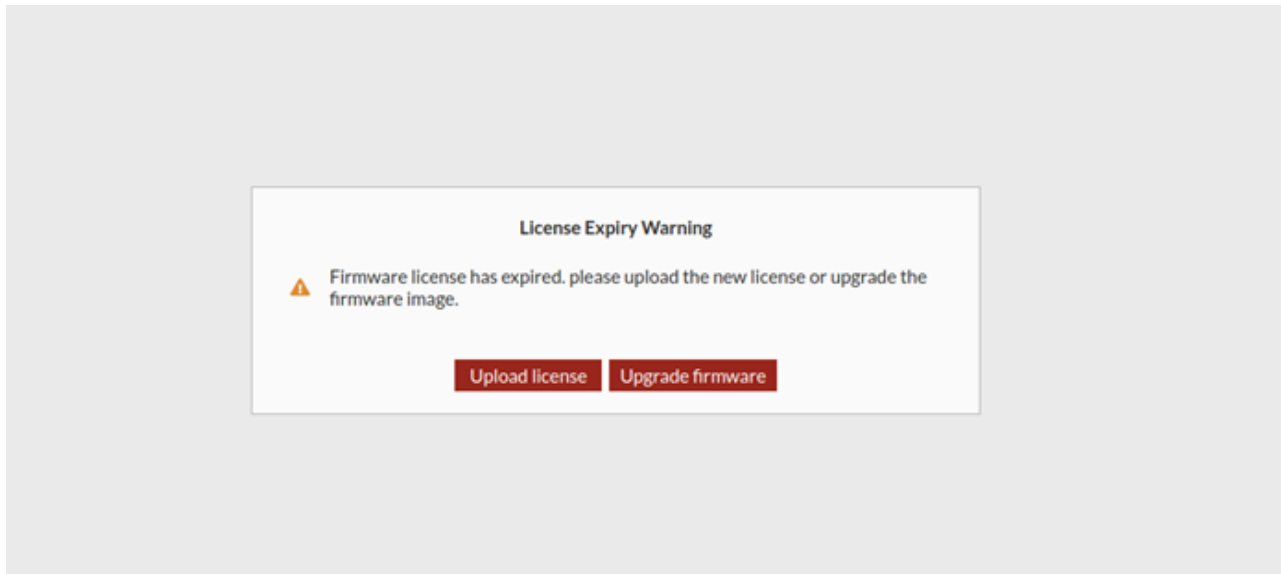
Go to the Azure client with the public IP to upload a valid license. Change the default password and get the authentication key for deployment.

### To configure the Azure client:

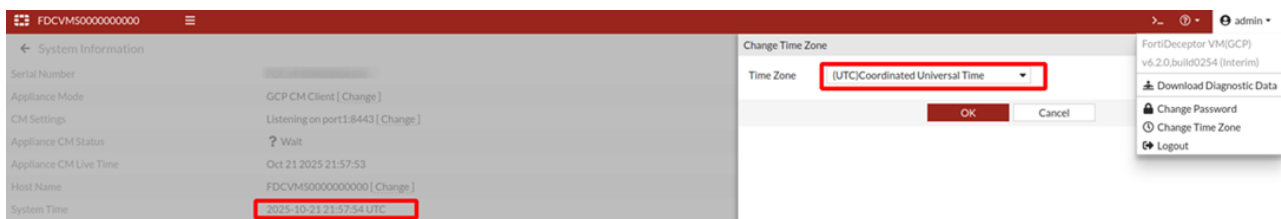
1. Log in to the Azure client with the public IP address. By default, the *admin* user account has no password.
2. After the instance reboots, you are prompted to change the password and log in again.



3. After logging in, the FortiDeceptor instance prompts you to upload the license file. Click *Upload License* to navigate to the file and click *Submit*. After the file submitted FortiDeceptor will reboot.



4. After logging in, the dashboard shows the system time based on the time zone settings in the Administrator menu.



5. Change the Host Name.
- a. Go to *Dashboard > System information > Host Name* and click *Change*. The *Edit Host Name* field opens.
  - b. In the *New Name* field, enter a the new Host Name.
6. Configure the client in the CM settings:
- a. Go to *Dashboard > System Information*. Locate *CM Settings* and click *Change*
  - b. In the CM Settings, select *Wait for connections from manager*.
  - c. Configure the *Listening Interface*, *Port*, and *Encryption Method*. The *Encryption Method* must be the same as the FortiDeceptor Manager
  - d. Click *OK*.

CM Settings

Connection Type \*  Connect to manager  Wait connections from manager

Listening Interface \*

Port \*

Encryption Method \*

- Plaintext
- AES128CBC
- AES192CBC
- AES256CBC

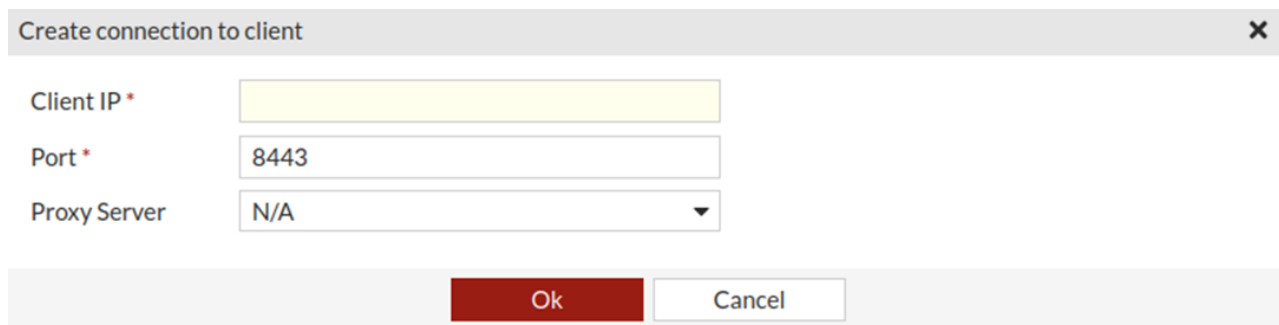
Cancel

# Configuring FortiDeceptor Manager

Connect to the remote CM Client and apply the encryption method chosen earlier to add Azure FortiDeceptor as a cloud appliance.

## To configure FortiDeceptor manager:

1. Go to *Dashboard > System Information*. Locate *CM Settings* and click *Change*.
2. In the *CM Settings*, select *Connect to remote CM client*.
3. Configure the *Client IP* (Azure appliance IP), *Port*, and *Proxy Server* if one has been configured on the FortiDeceptor.



Create connection to client ✕

Client IP \*

Port \*

Proxy Server

4. Click *Ok*. If successful the Azure appliance IP will appear in *CM Setting > CM Communication Setting* in the *Client IP* table
5. Configure one or more *Supported Encryption Methods*. Make sure the method selected on the client is among those enabled on the manager.

+ Connect to remote CM client
 Edit
 Delete

	Client IP ↕	Port ↕	Proxy Server ↕	Update Time [PST8PDT] ↕
<input type="checkbox"/>	[REDACTED]	8443	N/A	2025/10/13 19:42:50
<input type="checkbox"/>	[REDACTED]	8443	N/A	2025/10/13 19:42:50
<input type="checkbox"/>	[REDACTED]	8443	N/A	2025/10/13 19:42:50
<input type="checkbox"/>	[REDACTED]	8443	N/A	2025/10/13 19:42:50
<input type="checkbox"/>	[REDACTED]	8443	N/A	2025/10/13 19:42:50
<input type="checkbox"/>	[REDACTED]	8443	N/A	2025/10/13 19:42:50

Supported Encryption Methods     Plaintext     AES128CBC     AES192CBC     AES256CBC

Save
Close

6. Click **Save**.
7. Go to *Central Management > Appliances*, select the Azure appliance and click *Approve*



Delete the previous client and add the client with new public IP once the public IP is changed.

## Managing cloud clients

To manage you cloud clients (appliances), go to *Central Management > Appliances*.

Button	Description
<b>Delete</b>	Pause the selected clients and then permanently delete related data in the manager's local database, including OS, network settings, decoys, and lures.
<b>Refresh</b>	Force re-sync all data between manager and selected clients.

### To delete a cloud appliance:

1. Go to *Dashboard > System Information*. Locate *CM Settings* and click *Change*.
2. Select the cloud appliance IP, and click *Delete*. Click *OK* in the confirmation dialog that appears
3. Click *Save*.
4. Go to *Central Management > Appliances*, then locate the relevant Azure cloud client and click *Delete*.

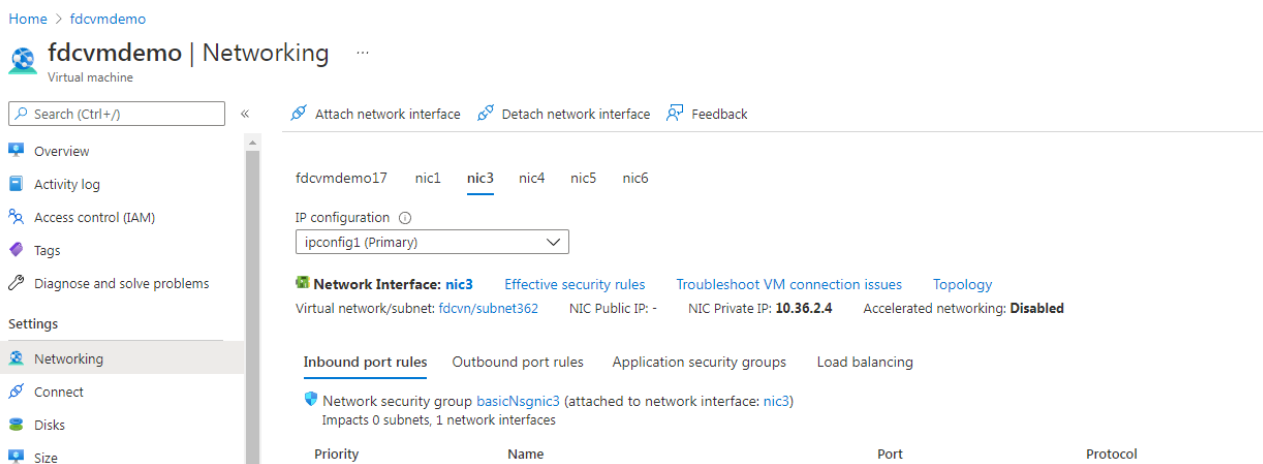
**To change a cloud client from the current manager to another local manager:**

1. Delete the cloud client from the current Manager. See [To delete a cloud appliance](#).
2. Configure the cloud client in the CM settings. See [Configuring the Azure client on page 29](#)
3. Configure the FortiDeceptor Manager. See [Configuring FortiDeceptor Manager on page 32](#)

## Configuring the deployment network

**To configure the FortiDeceptor ports in Azure:**

1. In Azure, open the VM and go to *Settings > Networking* and select an IP configuration.



2. Configure the *nic* ports to map to a port in FortiDeceptor.

**To configure the Azure ports in FortiDeceptor:**

1. In FortiDeceptor Go to *Deception > Deployment Network*.
2. Verify that *Azure* appears in the *Application* column and the *Status* is *Initialized*.

**Example:**

In the images below:

- nic1 is mapped to port2 in FortiDeceptor
- nic3 is mapped to port3 in FortiDeceptor
- nic4 is mapped to port4 in FortiDeceptor
- nic5 is mapped to port5 in FortiDeceptor
- nic6 is mapped to port6 in FortiDeceptor

*Azure VM > Settings > Network*

## Configuring FortiDeceptor Manager

demo17 nic1 nic3 nic4 nic5 nic6

IP configuration ⓘ  
ipconfig1 (Primary)

**Network Interface: fdcvmdemo17** [Effective security rules](#) [Troubleshoot VM connection issues](#) [Topology](#)  
Virtual network/subnet: fdcvn/subnet351 NIC Public IP: [redacted] NIC Private IP: [redacted] Accelerated networking: **Disabled**

[Inbound port rules](#) [Outbound port rules](#) [Application security groups](#) [Load balancing](#)

Network security group fdcvmdemonsg165 (attached to network interface: fdcvmdemo17)  
Impacts 0 subnets, 1 network interfaces Add inbound port rule

Priority	Name	Port	Protocol	Source	Destination	Action
100	SSH	22	TCP	Any	Any	Allow
110	HTTPS	443	TCP	Any	Any	Allow
120	Port_8443	8443	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

FortiDeceptor Manager > Deployment Network.

OK ✓

Appli...	Status	Nam... ↑	Interf...	VLA...	Deploy Monitor IP/Mask	Tag	Gate...
Azu...	Initialized	azureP2	port2	0	[redacted]	any	10.36.1.1
Azu...	Initialized	azureP3	port3	0	[redacted]	any	10.36.2.1
Azu...	Initialized	azureP4	port4	0	[redacted]	any	10.36.4.1
Azu...	Initialized	azureP5	port5	0	[redacted]	any	10.36.5.1
Azu...	Initialized	azureP6	port6	0	[redacted]	any	10.36.3.1

## Deploying decoys

Verify there are multiple IPs on the Azure platform and then configure the decoy on FortiDeceptor.

**To verify there are multiple IPs on the Azure platform:**

1. In Azure, select the configuration to deploy the decoys.
2. Go to *Settings > IP configurations*. The IPs are displayed in the *Private IP* column.

Home > fdcvmdemo > nic1 port2

nic1 | IP configurations ...  
Network interface

Search (Ctrl+/) << + Add Save Discard Refresh

Overview  
Activity log  
Access control (IAM)  
Tags

Settings

IP configurations  
DNS servers  
Network security group  
Properties  
Locks

Monitoring

Insights  
Alerts  
Metrics

IP forwarding settings  
IP forwarding  
Virtual network  
IP configurations  
Subnet

*i* The associated virtual machine 'fdcvmdemo' must be either stopped or

Search IP configurations

Name	IP Version	Type	Private IP
ipconfig1	IPv4	Primary	10.36.1.4
staticip2	IPv4	Secondary	10.36.1.5
ip3	IPv4	Secondary	10.36.1.7

**To locate the on the Azure platform:**

Go to *Network Setting > Properties*.



## To configure the decoy on FortiDeceptor:

1. In FortiDeceptor, go to *Deception Deployment Wizard* and create a new template.
2. In the *Configuration* tab, above *Available Deception OSes*, select the *Appliance Name*.

The screenshot shows the configuration interface for a decoy. It features several fields:
 

- Name \***: A text input field containing 'azure' with a green checkmark icon to its right.
- Appliance Name**: A dropdown menu with 'Local' selected, highlighted with a red box. It includes 'x' and 'v' icons for clearing and expanding the menu.
- Available Deception OSes \***: A dropdown menu with 'posv1' selected, including 'x' and 'v' icons.
- Selected Services \***: A dropdown menu with 'POS-WEB' selected.
- Automate Lures**: A dropdown menu with 'any' selected, including an 'x' icon.

 Below the 'Automate Lures' field is a yellow warning box with a triangle icon and the text: 'The generated lures contain random user name(s)'. At the bottom right, there are two buttons: 'Generate lures' (highlighted with a red box) and 'Clear'.

3. In the *Set Network* tab, click *Add network for Deployment* and configure the following settings:

- |                        |   |
|------------------------|---|
| <b>Deploy Network</b>  | Select the deployment network.                              |
| <b>Addressing Mode</b> | Select <i>Static</i> or <i>DHCP</i> (dynamically assigned). |

<b>Network Mask</b>	Enter the network mask.
<b>Gateway</b>	Enter the gateway IP address.
<b>MAC Address</b>	Enter the MAC address .
<b>IP Count</b>	Select the number of IP addresses allocated.
<b>Min/Max</b>	Define the range of IP addresses available in the subnet.
<b>IP Ranges</b>	Enter specific IP addresses or ranges reserved for use.



In version 6.2, cloud appliances do not appear under *Appliance Name* in the *Deployment Wizard*. To deploy decoys to cloud appliances, select a *Deploy Network* that is designated as a cloud appliance the deployment network.

---

### Add Network for Deployment ✕

Deploy Network \*  ✕ ✓

Addressing Mode \*  Static  DHCP

Network Mask \*  ✓

Gateway \*  ✓

MAC Address  ✓

IP Count \*  ✓

ℹ Please check our best practice deployment guide.

Min

Max

IP Ranges \* (1)

✓

4. Click *Done* to deploy the decoy.
5. (Optional) Deploy more decoys.
  - To deploy decoys for different interfaces, repeat [Verify there are multiple IPs on the Azure platform](#).
  - To deploy more decoys for the same interface, repeat steps 1-4.
6. Attack this decoy IP via the endpoint in the cloud and check the incidents as regular deployment.



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2025 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 Chief Legal Officer, 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.