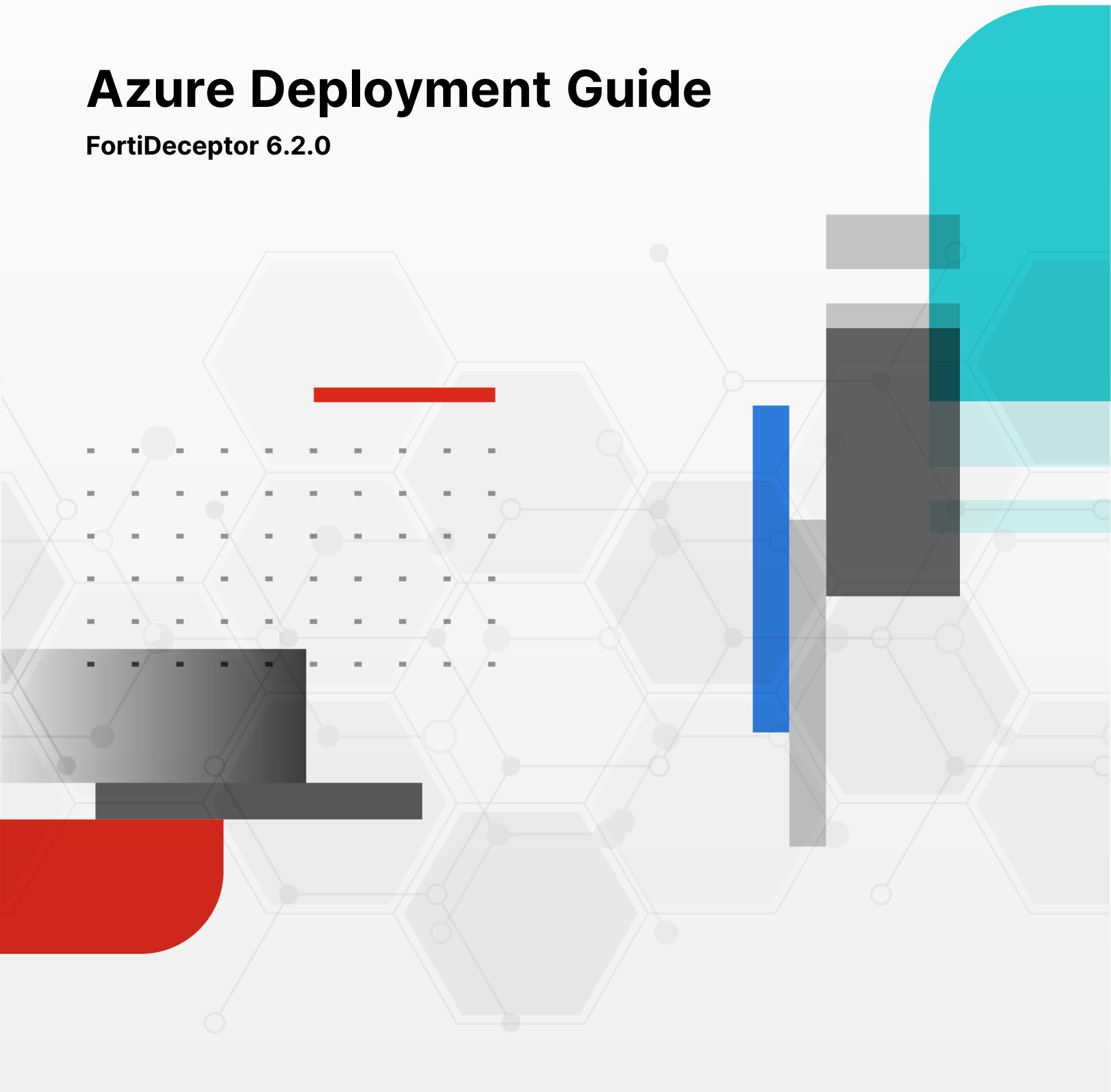
Azure Deployment Guide

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

October 23, 2025
FortiDeceptor 6.2.0 Azure Deployment Guide
00-610-769881-20251023

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-10-03	Initial release.
2025-10-23	Updated Configuring the Azure client on page 29, Configuring FortiDeceptor Manager on page 32, Managing cloud clients on page 33, and Deploying decoys on page 35.

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/.

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

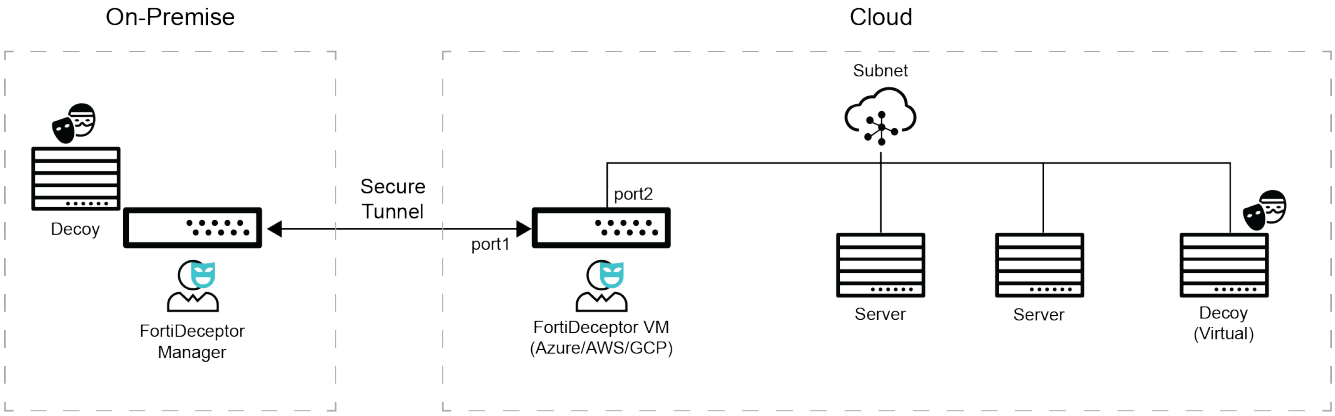
For more information, see the FortiDeceptor product data sheet available on the Fortinet web site, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiDeceptor.pdf.

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
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)	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.

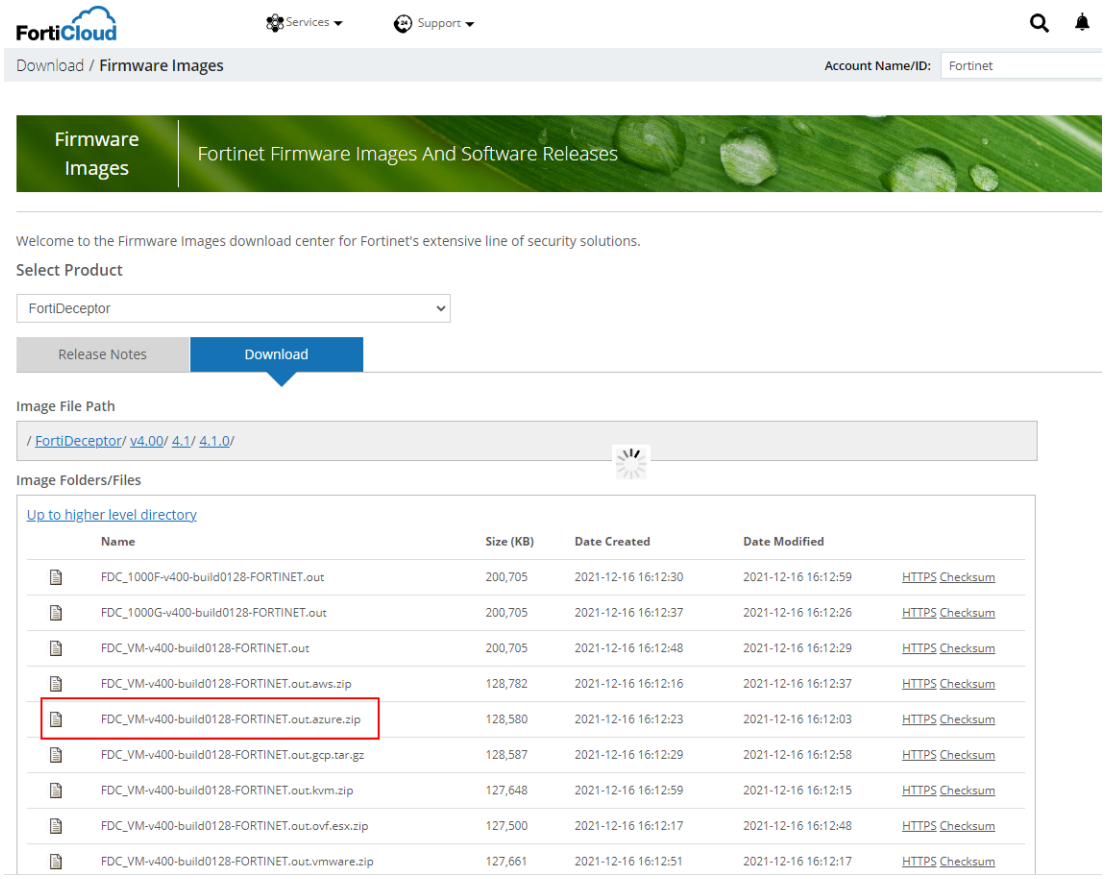
Preparing the FortiDeceptor image

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*



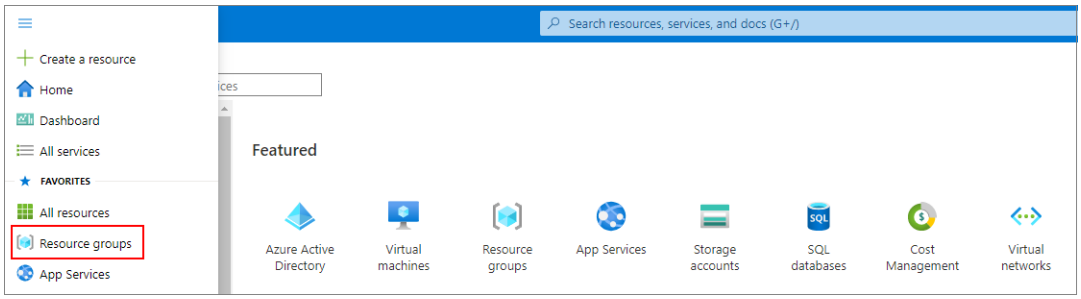
7. Extract the `.zip` file.

Creating resource groups

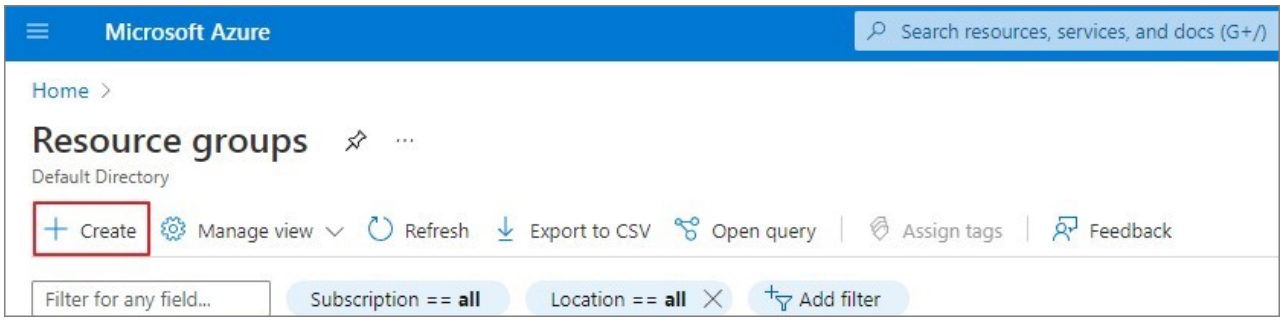
Create a resource group and then add your resources. This allows you to deploy, update, and delete the resources as a group.

To create a resource group:

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

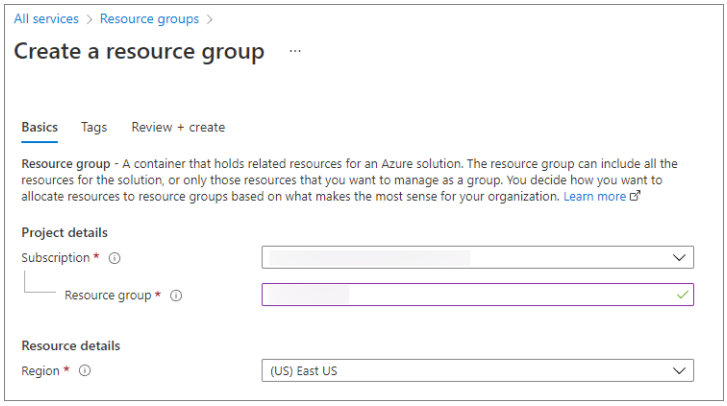


2. Click *Create*.



3. Select or enter the following property values:

Subscription	Select an Azure subscription.
Resource group	Enter a name for the resource group.
Region	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.

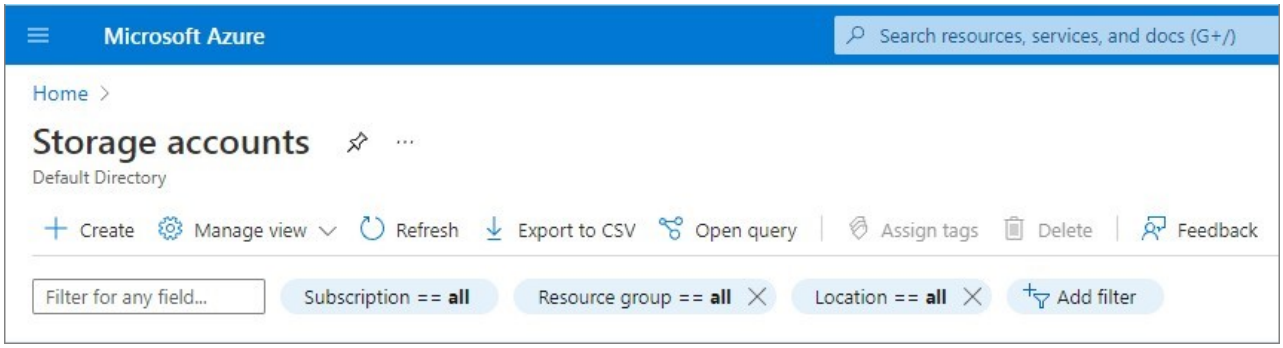


4. Click *Review + Create*. The resource group is validated.
5. Click *Create*.

Uploading FortiDeceptor VHD to Azure

To upload FortiDeceptor VHD to Azure:

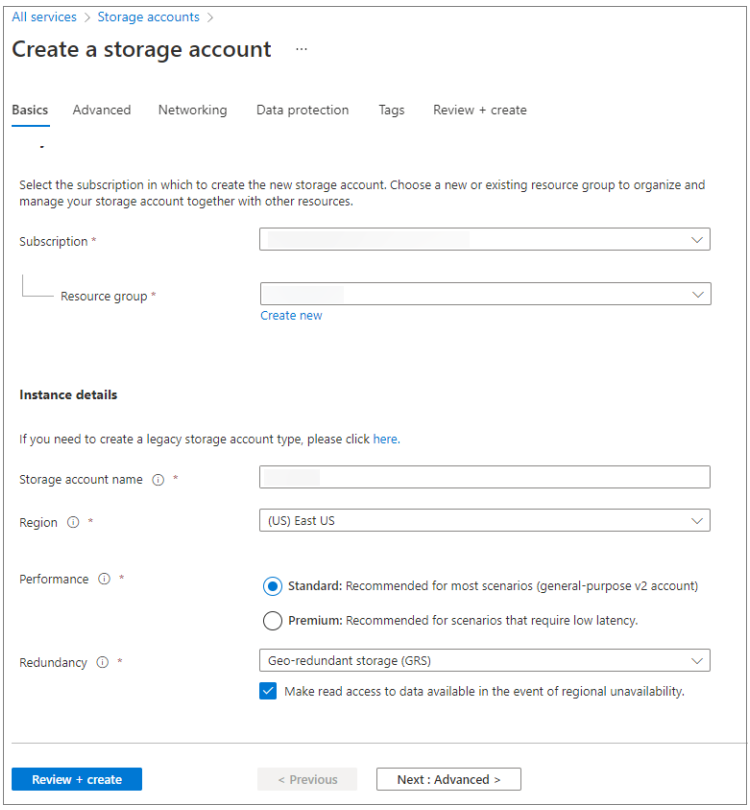
1. In the portal menu, click *Storage accounts*.
2. On the *Storage accounts* page, click *Create*. The *Create a storage account* page opens.



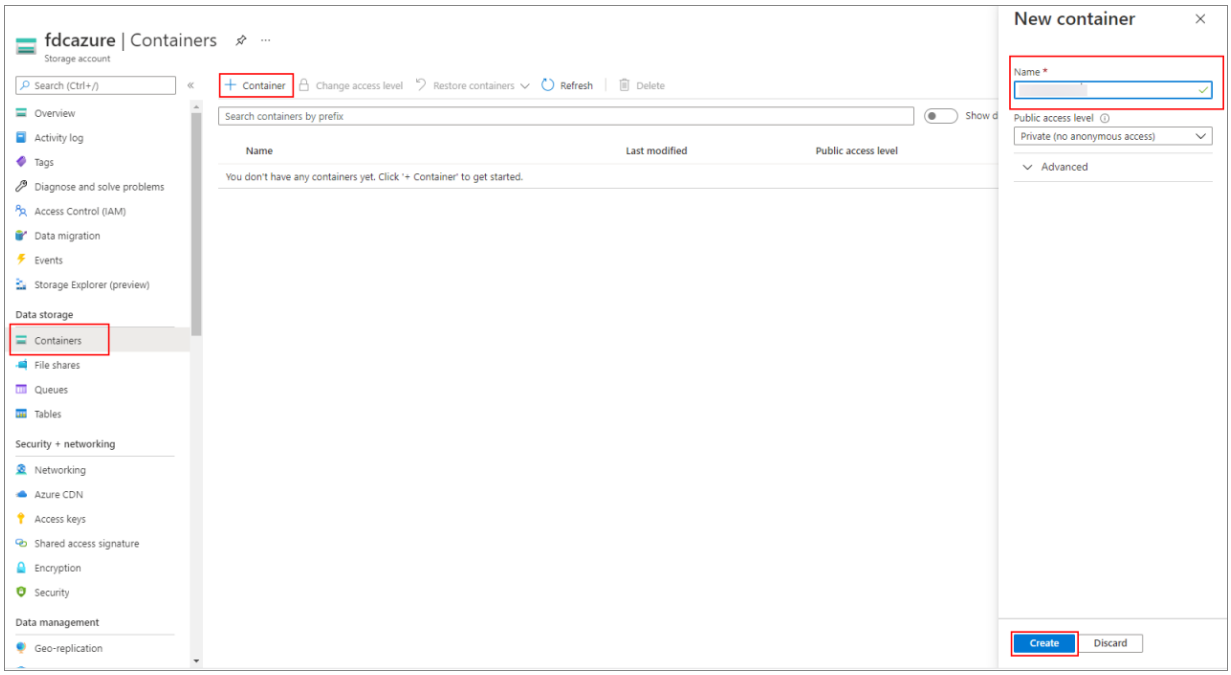
3. In the *Basics* tab, configure the storage account details. The image below shows the basic configuration for FortiDeceptor.

4.

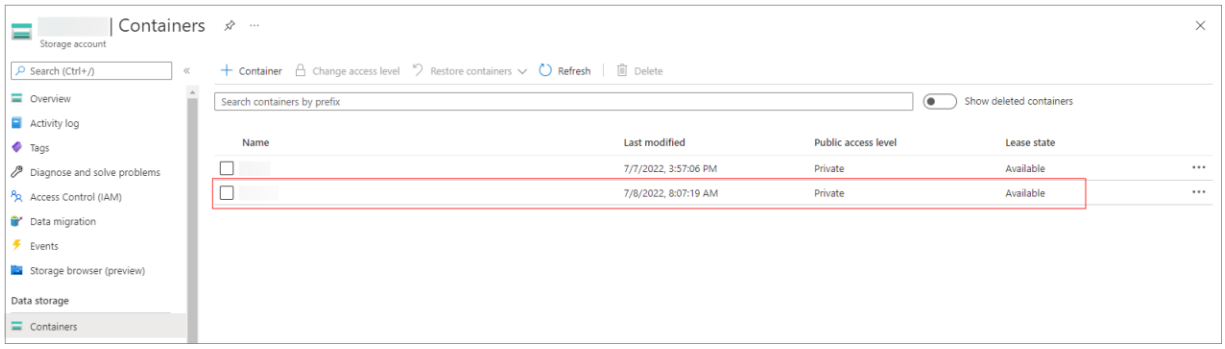
Subscription	Select a subscription from the dropdown.
Resource group	Select a resource group from the dropdown.
Storage account name	Enter a name for the storage account.
Region	Select a region from the dropdown.
Performance	Select *Standard: Recommended for most scenarios (general-purpose v2 account)*.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



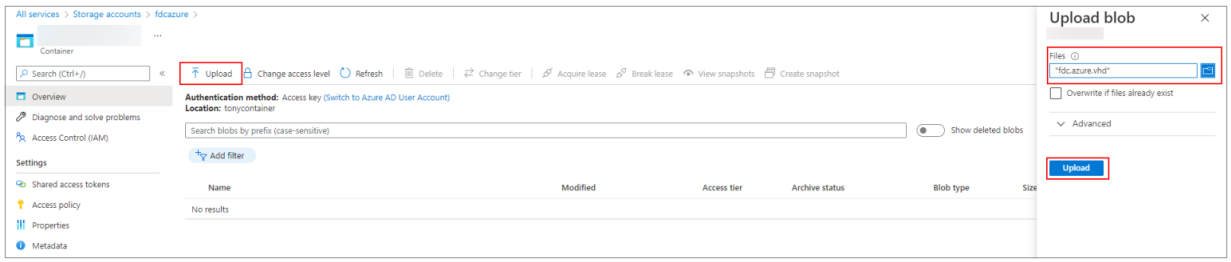
5. Click *Review + Create*. The account is validated.
6. Click *Create*.
7. Create a storage container to upload FortiDeceptor VHD.
   a. Open the storage account you created.
   b. In the portal menu, go to *Data storage > Containers*.
   c. Click *+Container*. The *New container* pane opens.
   d.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



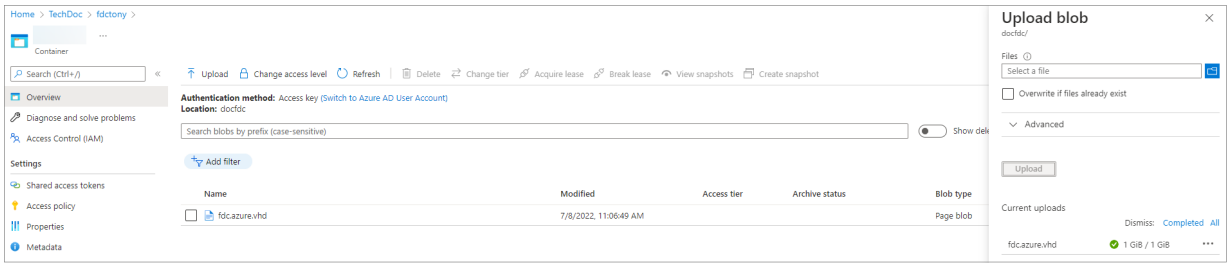
8. Upload FortiDeceptor VHD to the container.
   a. In the containers list, click the container you created.



   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.



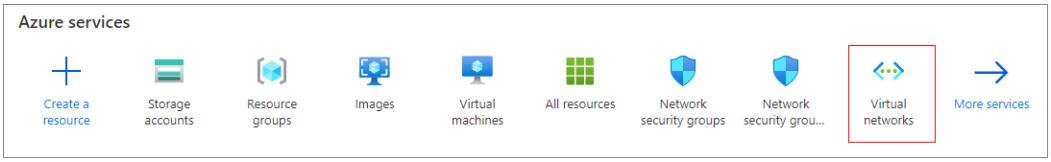
Preparing the network

Creating a virtual network

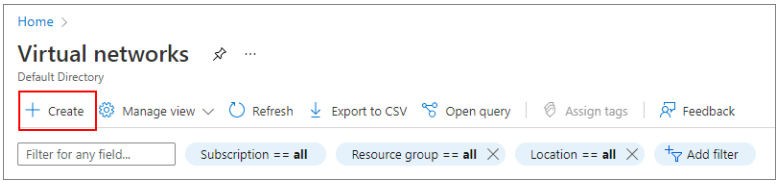
Create a virtual network and add several subnets for FortiDeceptor management and deployment.

To create a virtual network:

1. Create a Virtual Network.
   a. In the portal menu, click *Virtual networks*.

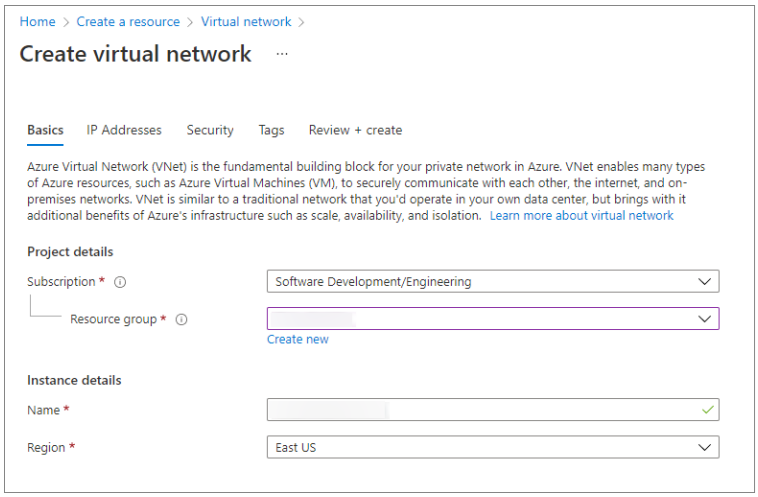


   b. In the *Virtual Networks* page, click *Create*.

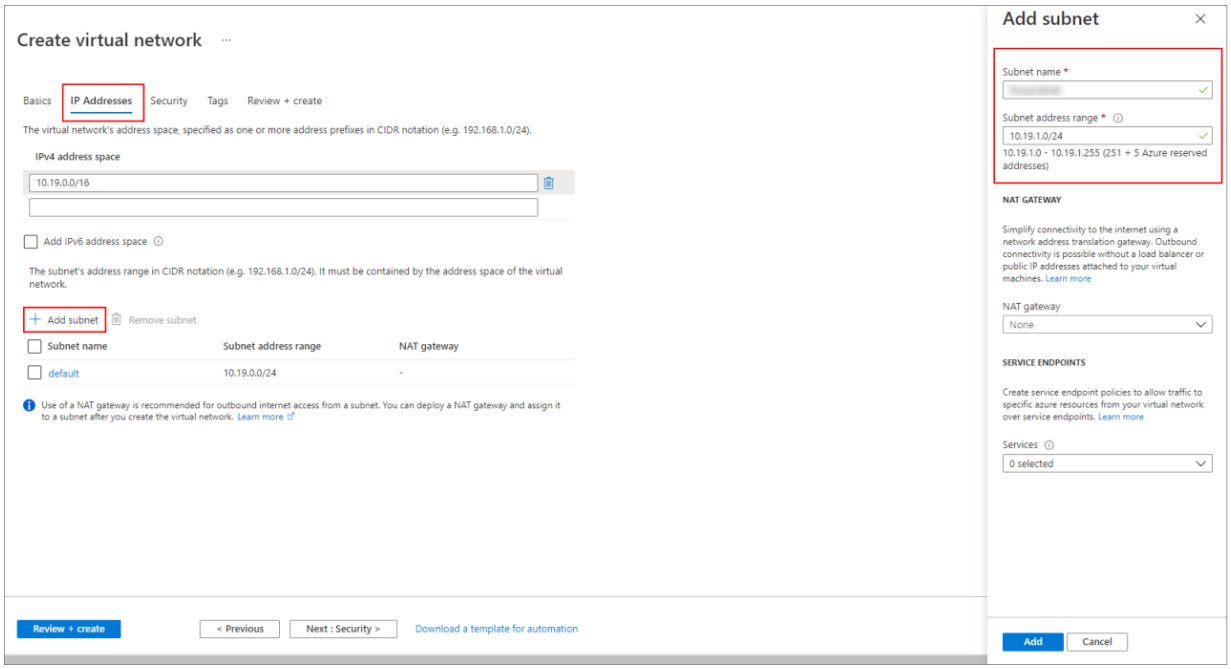


   c. In the *Basics* tab, configure the network details.

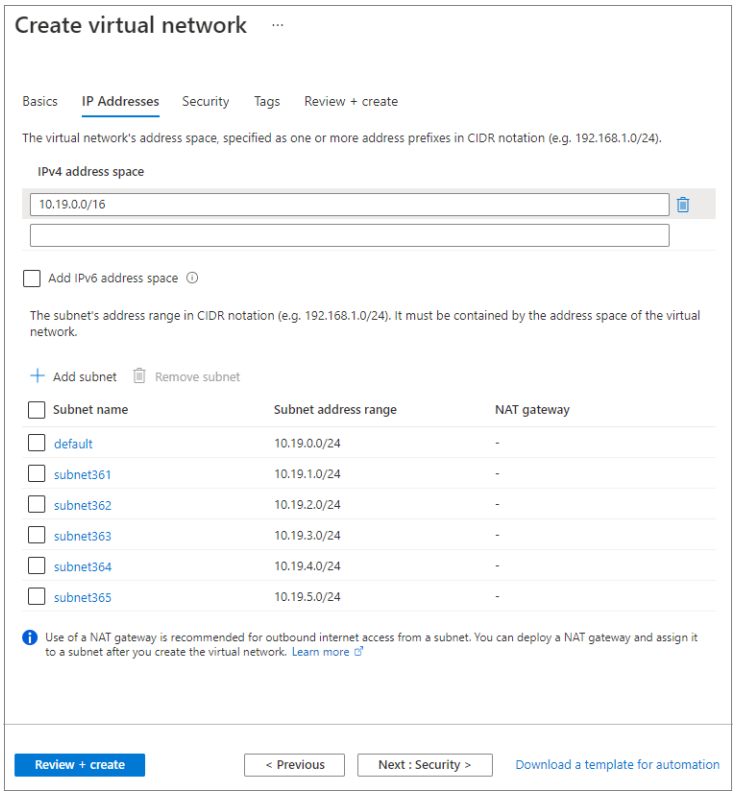
Subscription	Select a subscription from the dropdown.
Resource group	Select a resource group from the dropdown.
Name	Enter a name for the instance.
Region	Select a region from the dropdown.



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*.

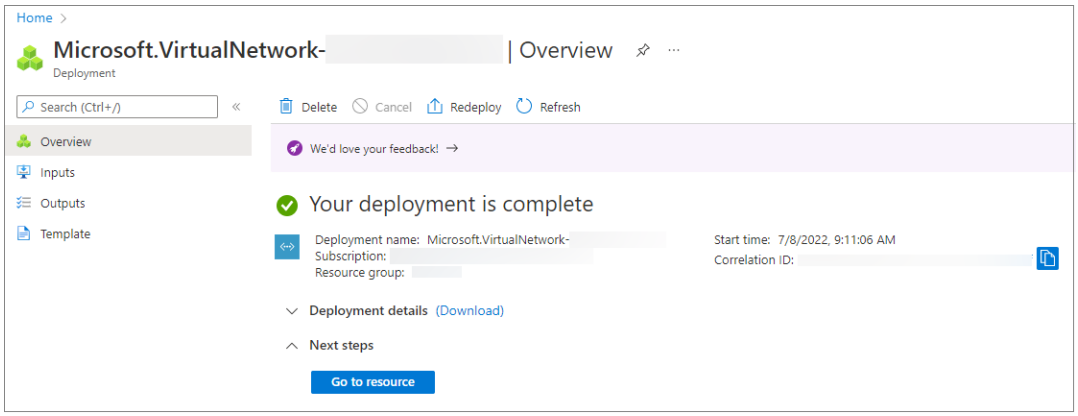


e. (Optional) Add additional subnets. You can add up to six subnets.



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

g. Click *Create*. The virtual network is created.

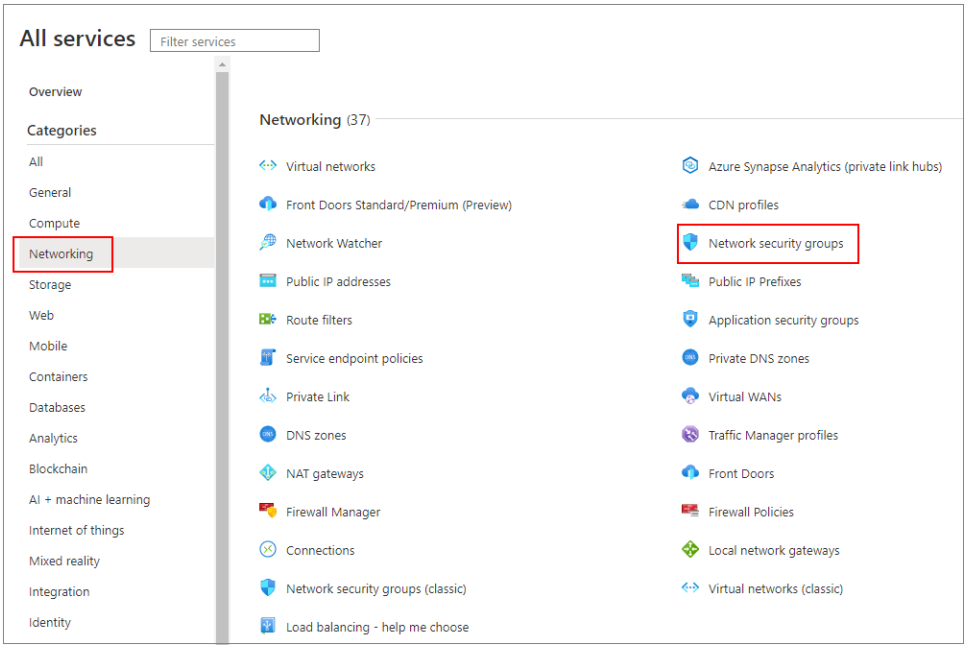


Creating network security groups and rules

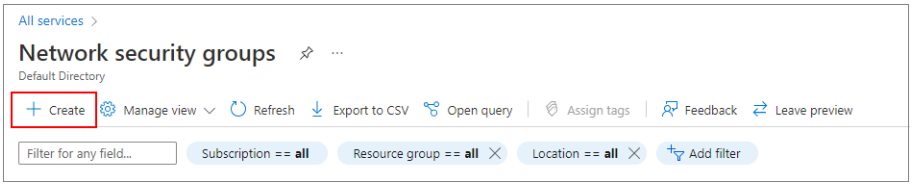
Create a network security group and add security rules for filtering network traffic to and from FortiDeceptor in a virtual network.

To create a network security group and add rules:

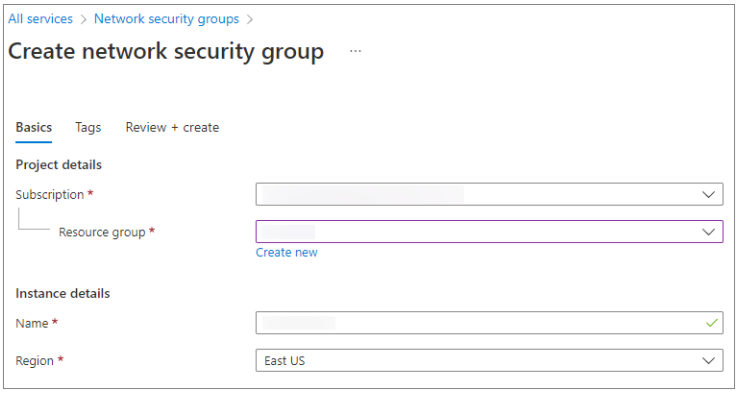
1. From the *Home* page, click *Create a resource*.
2. In the navigation menu, click *Networking* > *Network security groups*.



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

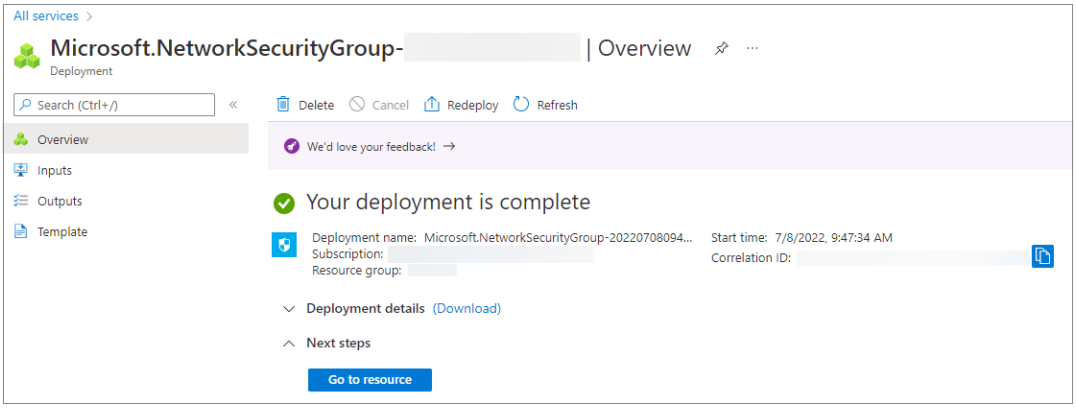


4. Configure the network security group settings and click *Review + Create*. The security group is validated.

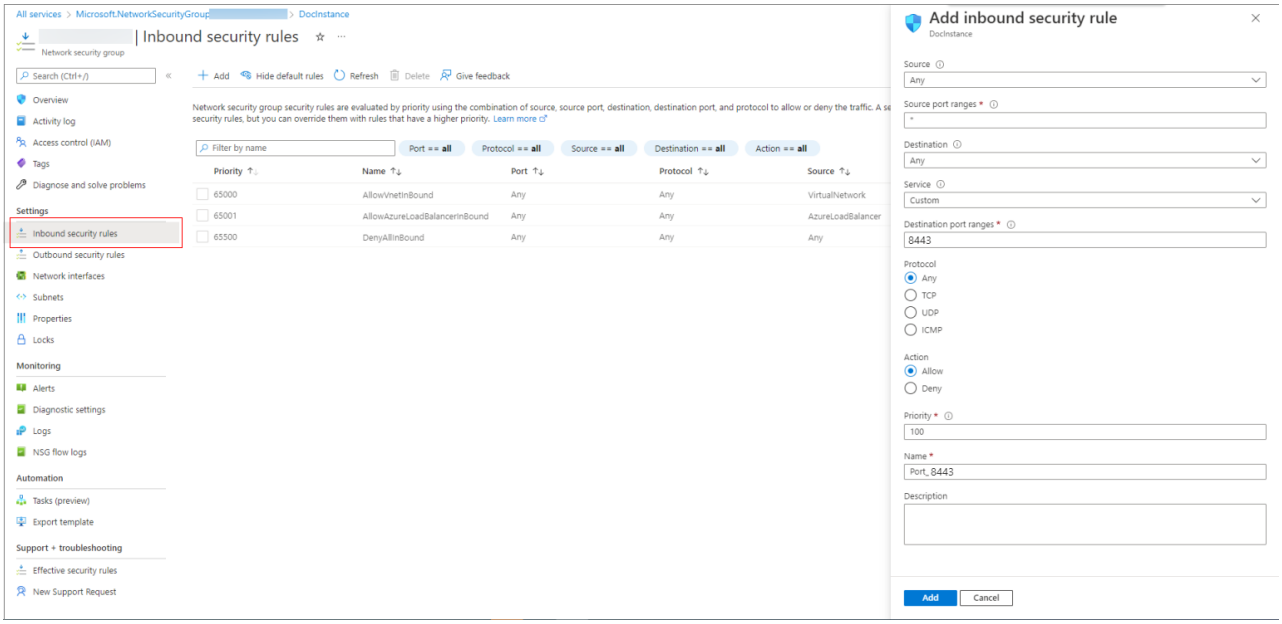


5. Click *Create*. The security group is created.

6. Click *Go to resource*.

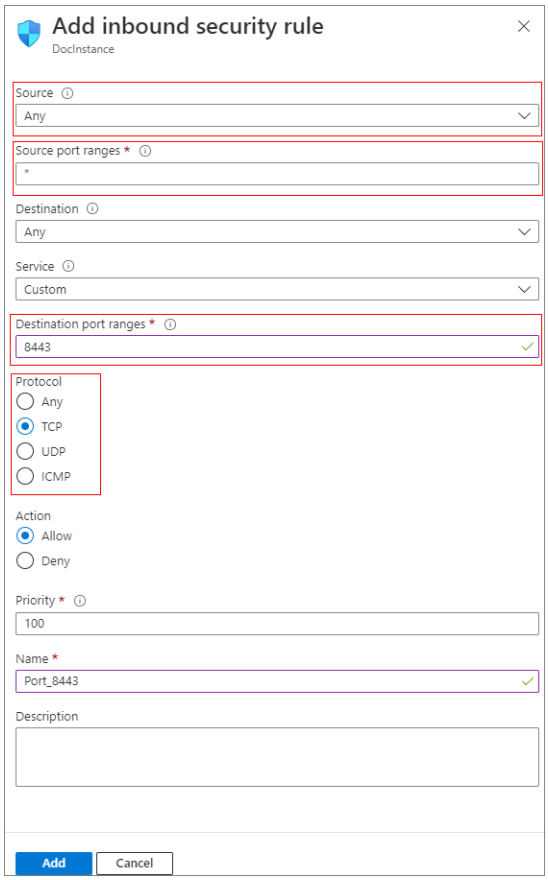


7. In the menu go to *Settings* > *Inbound security rules* and click *Add*. The *Add inbound security rule* pane opens.

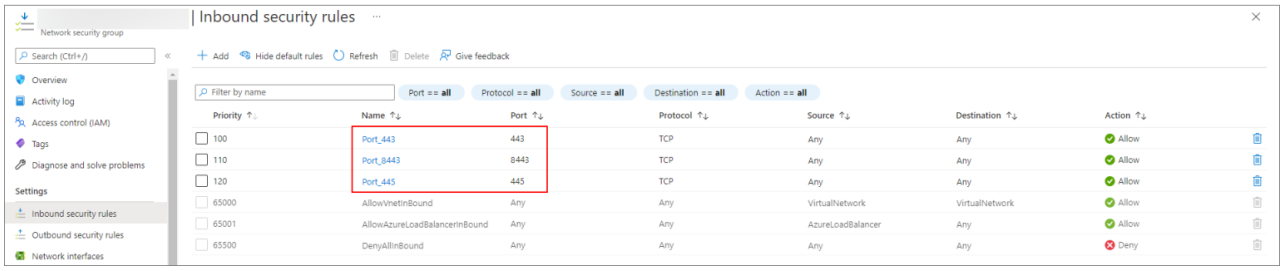


8. Configure the *Source*, *Source port ranges*, and *Destination port ranges*, and click *Add*.

Source	Select a source from the dropdown.
Source port ranges	Enter the port source ranges.
Destination port ranges	Enter the destination port ranges. 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 is enables the FortiDeceptor Manager to communicate with the cloud clients.
Protocol	Select *TCP*.



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

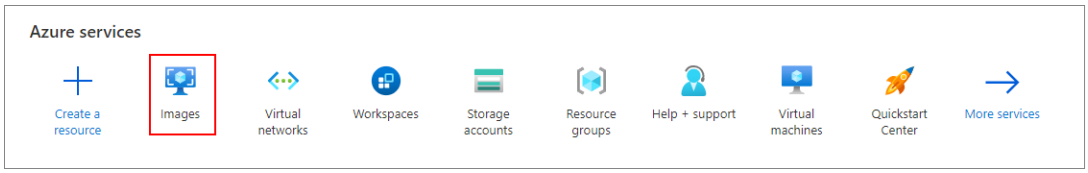


Create VM with the FortiDeceptor VHD

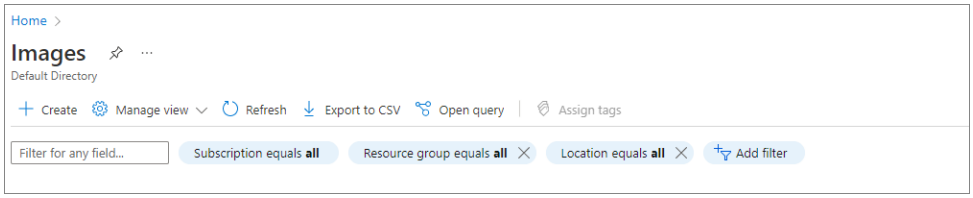
Create a virtual machine and specify the details of the image, disk and network.

To create an image the VHD:

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

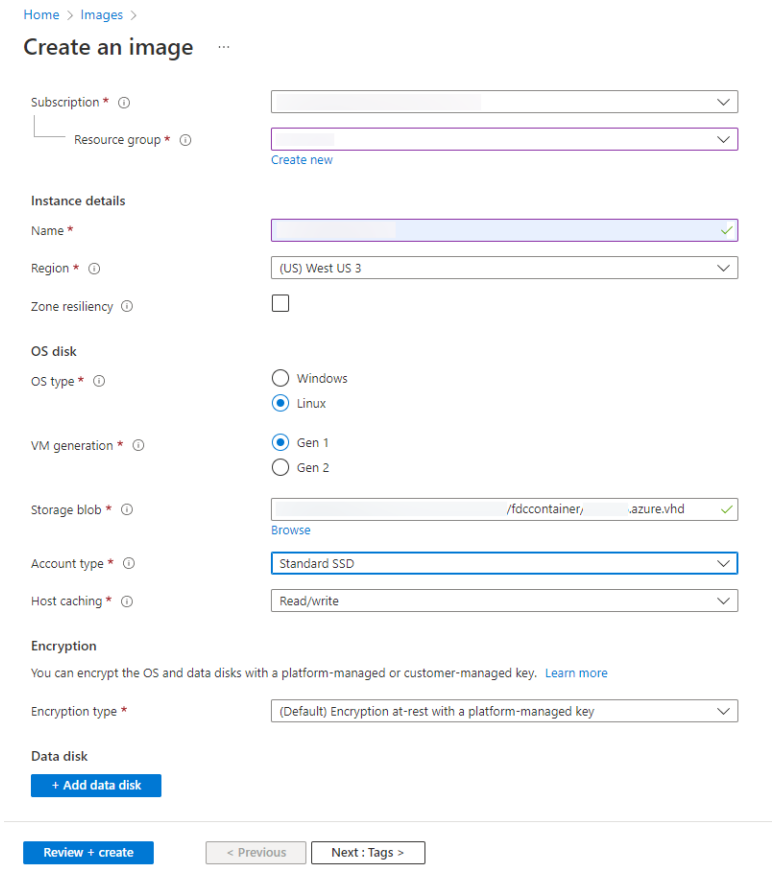


2. Click *Create*.

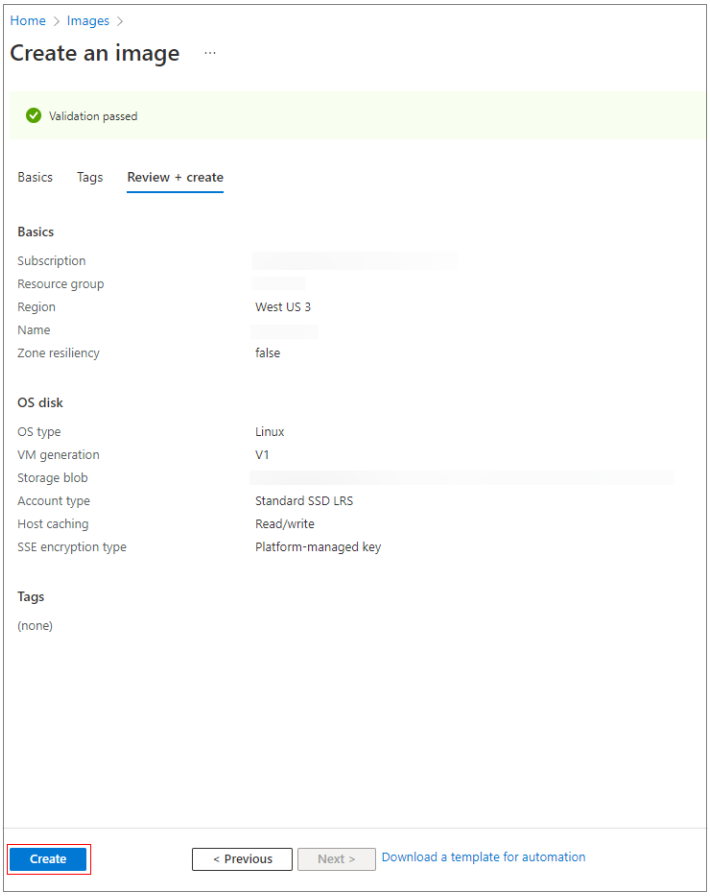


3. Configure the following settings and click *Review + Create*.

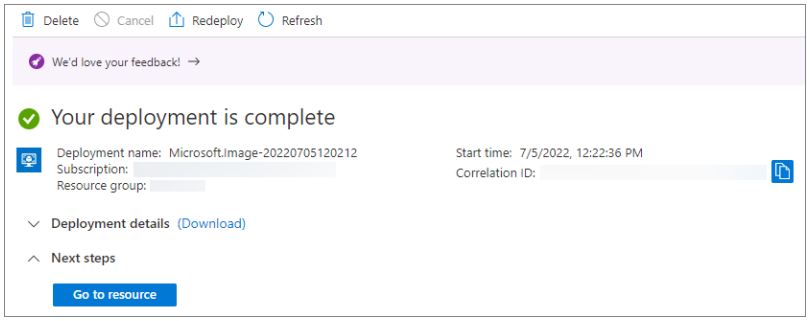
Subscription	Select a subscription from the dropdown.
Resource group	Select a resource group from the dropdown.
OS type	Linux
VM generation	Gen1
Storage blog	https://.../xxxcontainer/fdc.azure.vhd
Account type	Standard SSD
Host caching	Read/write


Home > Images >
Create an image
Subscription *
Resource group *
Create new
Instance details
Name *
Region *
(US) West US 3
Zone resiliency
OS disk
OS type *
Windows
Linux
VM generation *
Gen 1
Gen 2
Storage blob *
/fdccontainer/ .azure.vhd
Browse
Account type *
Standard SSD
Host caching *
Read/write
Encryption
You can encrypt the OS and data disks with a platform-managed or customer-managed key. Learn more
Encryption type *
(Default) Encryption at-rest with a platform-managed key
Data disk
+ Add data disk
Review + create
< Previous
Next : Tags >

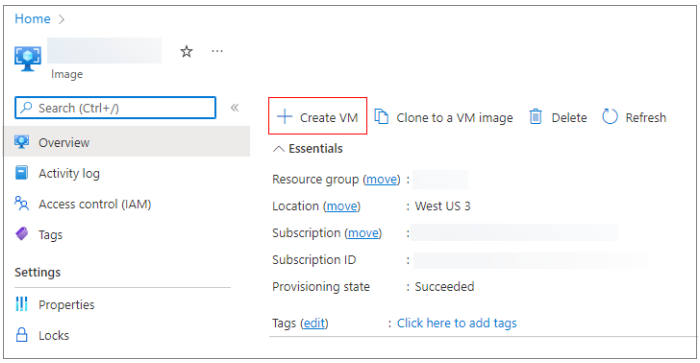
4. Click *Create*.



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

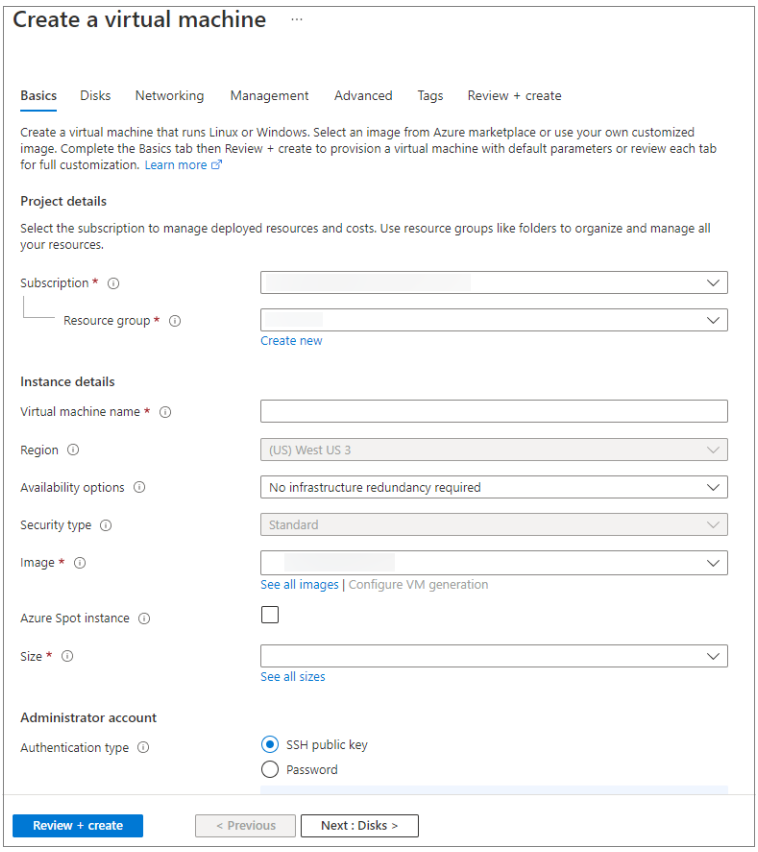


6. Click *Create VM*.

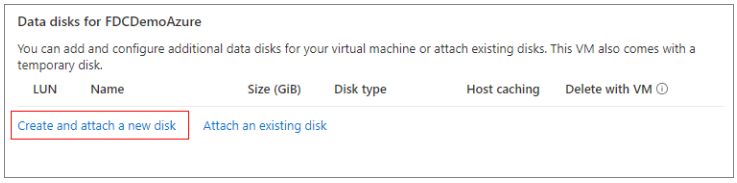


7. In the *Basics* tab, configure the following settings:

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

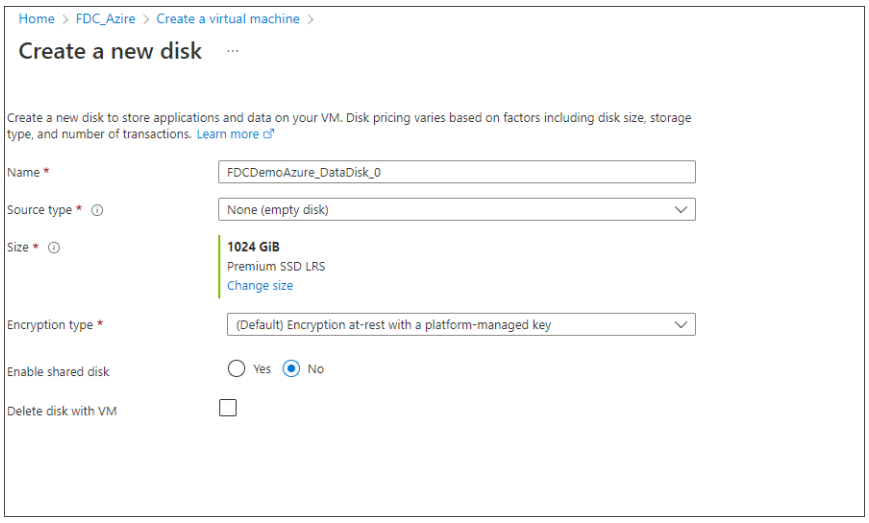


8. Click *Disks* tab.
   a. Scroll down to *Data disks for <vm_name >* and click *Create and attach a new disk*.



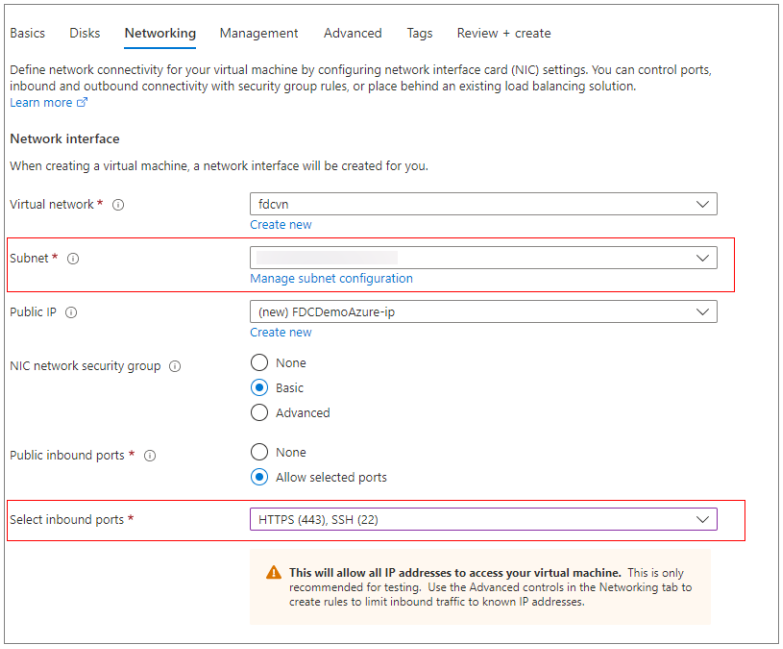
   b. Configure the following settings and click *OK*.

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



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

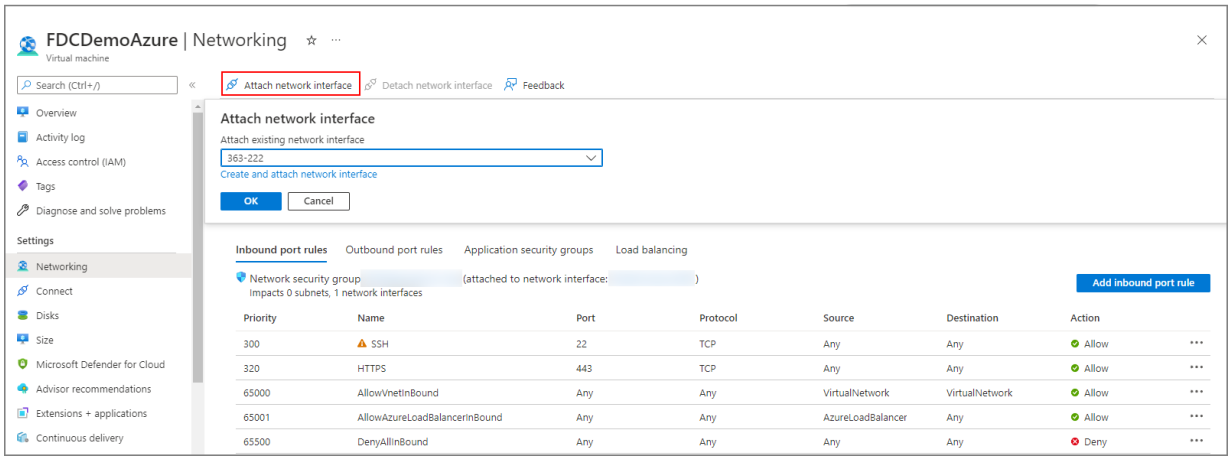
Subnet	Select the subnet.
Select inbound ports	Select *HTTPS (443)*, *SSH (22)*.



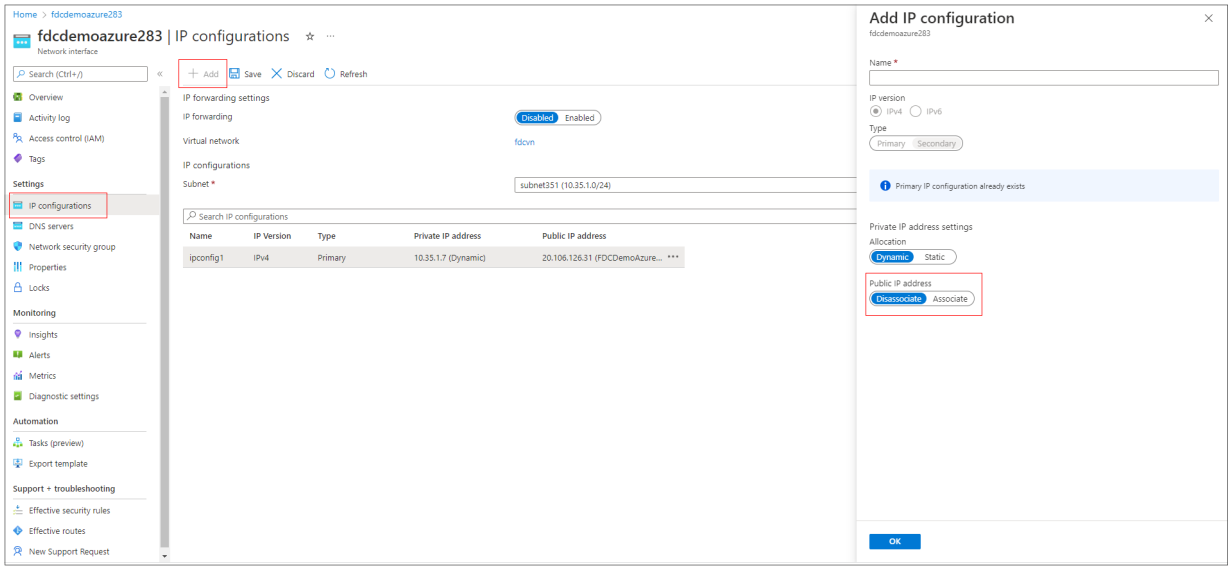
10. (Optional) Click the *Management* tab update the diagnostics settings.
11. Click *Review + Create* to create the virtual machine.

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 the select the interface you want to attach. You must configure a minimum of two NICs. You can attach up to six interfaces.

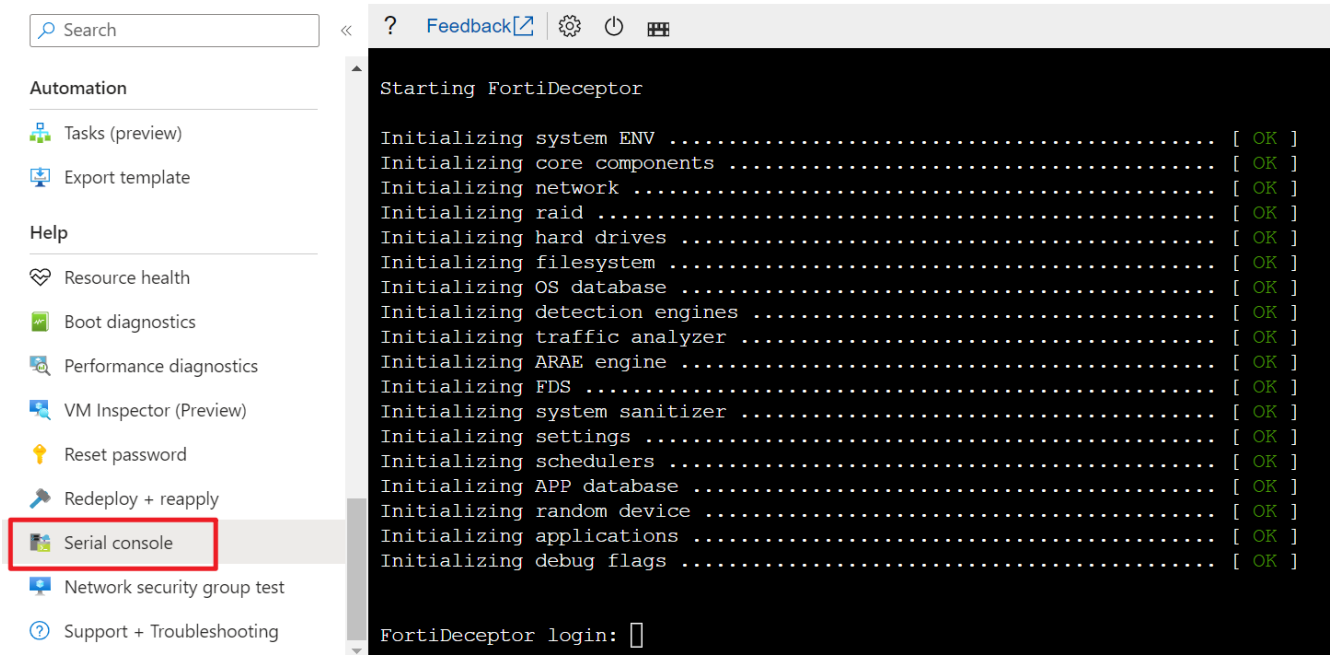


13. Associate the public IP to Port1.
    a. Go to *Home* and open the Network Interface
    b. Go to *Settings* > *IP configurations*.
    c. Click *Add*. The *Add IP configuration* pane opens.
    d. Under *Public IP address* select *Associate*. Binding the cloud client with static public IP address 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:

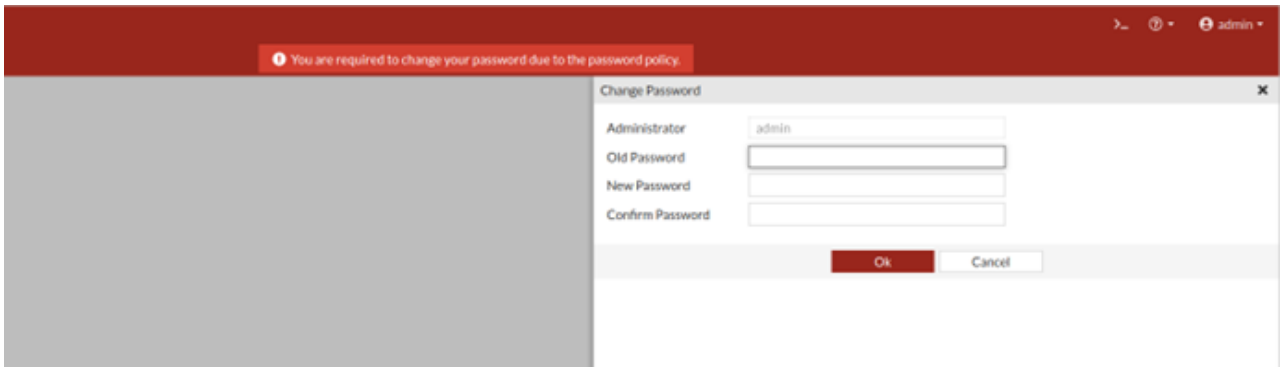
1. Configuring the Azure client on page 29
2. Configuring FortiDeceptor Manager on page 32
3. Managing cloud clients on page 33
4. Configuring the deployment network on page 34
5. Deploying decoys on page 35

Configuring the Azure client

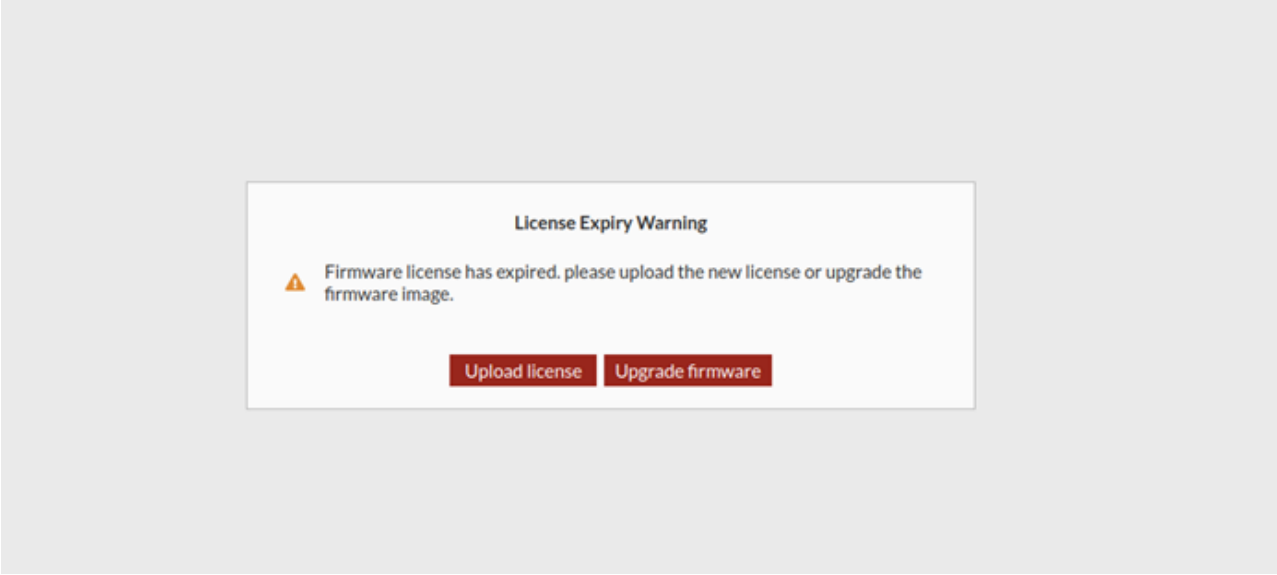
Go to the Azure client with the public IP to upload a valid license. Change the default password and get the authentication key for deployment.

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.

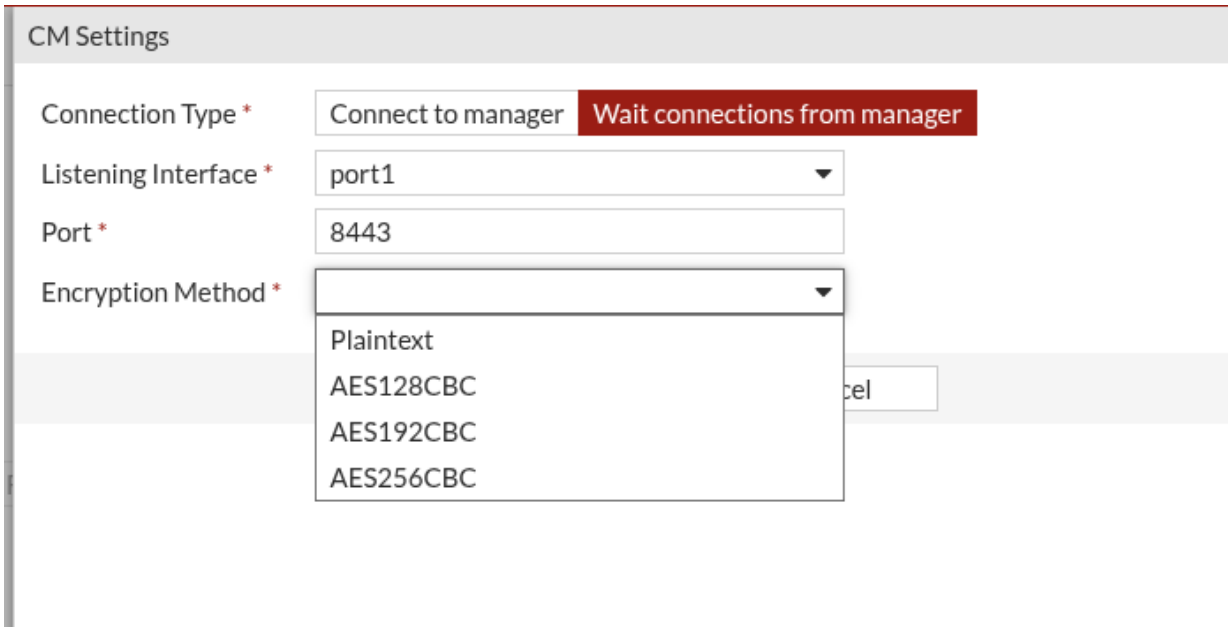


3. After logging in, the FortiDeceptor instance prompts you to upload the license file. Click *Upload License* to navigate to the file and click *Submit*. After the file submitted FortiDeceptor will reboot.



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*.

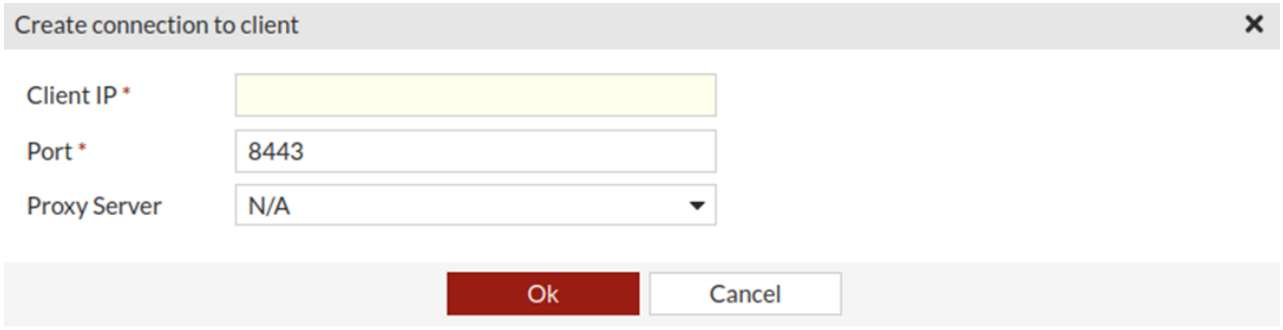

CM Settings
Connection Type *
Connect to manager
Wait connections from manager
Listening Interface *
port1
Port *
8443
Encryption Method *
Plaintext
AES128CBC
AES192CBC
AES256CBC

Configuring FortiDeceptor Manager

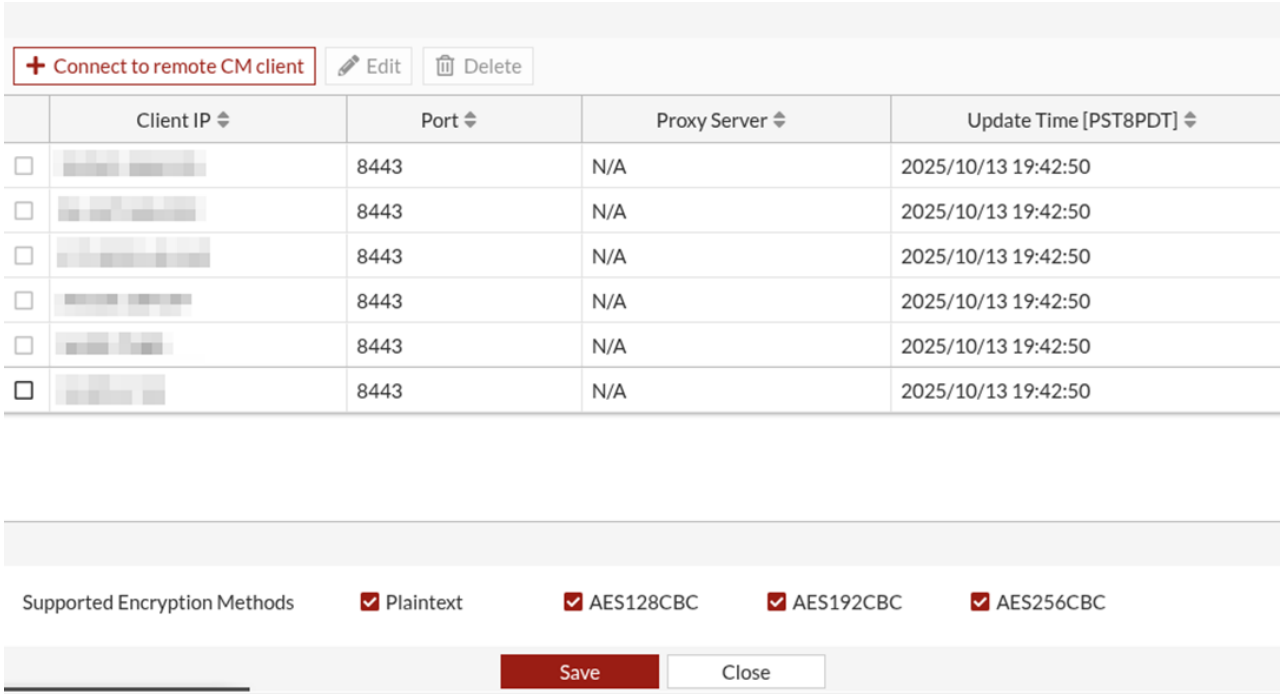
Connect to the remote CM Client and apply the encryption method chosen earlier to add Azure FortiDeceptor as a cloud appliance.

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.



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.



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
Delete	Pause the selected clients and then permanently delete related data in the manager's local database, including OS, network settings, decoys, and lures.
Refresh	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*.

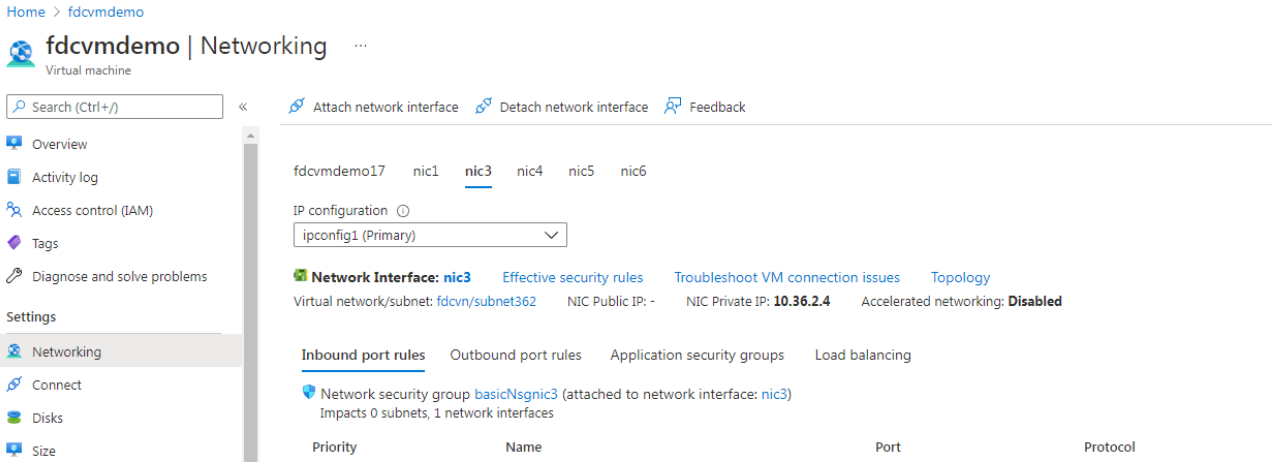
To change a cloud client from the current manager to another local manager:

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:

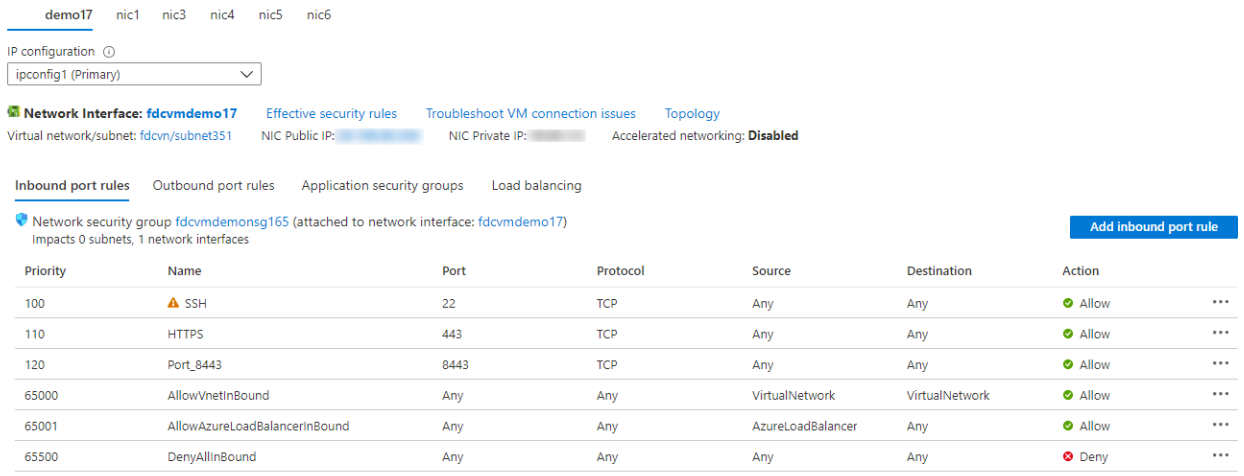
1. In FortiDeceptor Go to *Deception* > *Deployment Network*.
2. Verify that *Azure* appears in the *Application* column and the *Status* is *Initialized*.

Example:

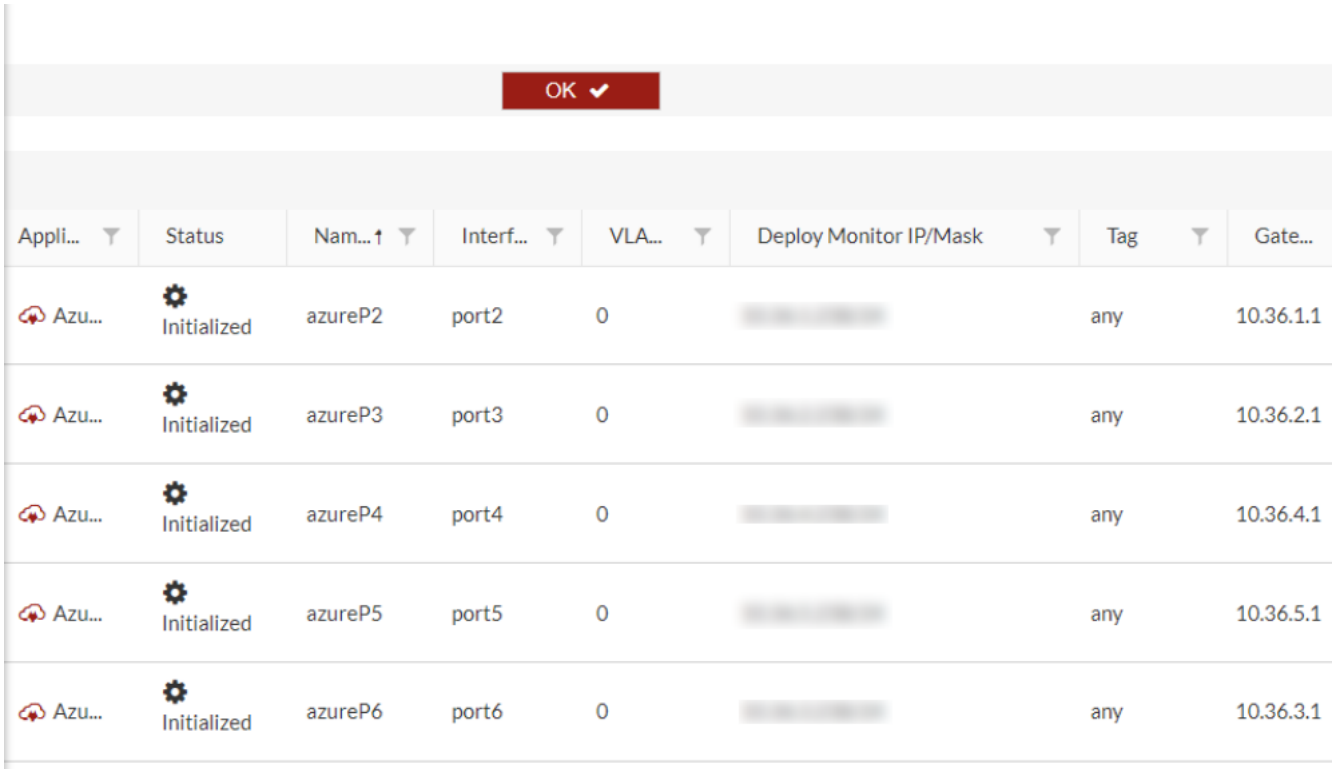
In the images below:

- 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*



FortiDeceptor Manager > Deployment Network.

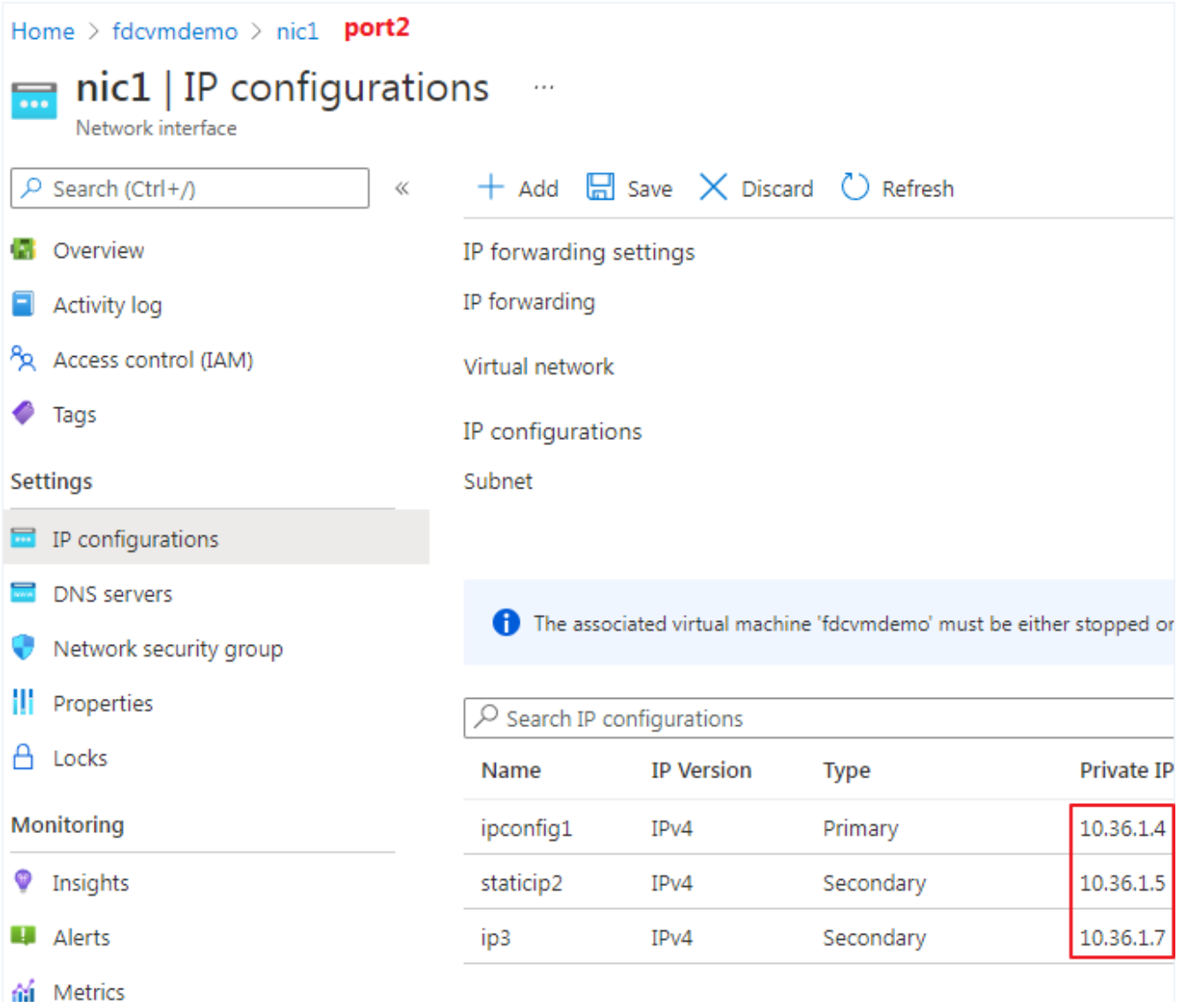


Deploying decoys

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.

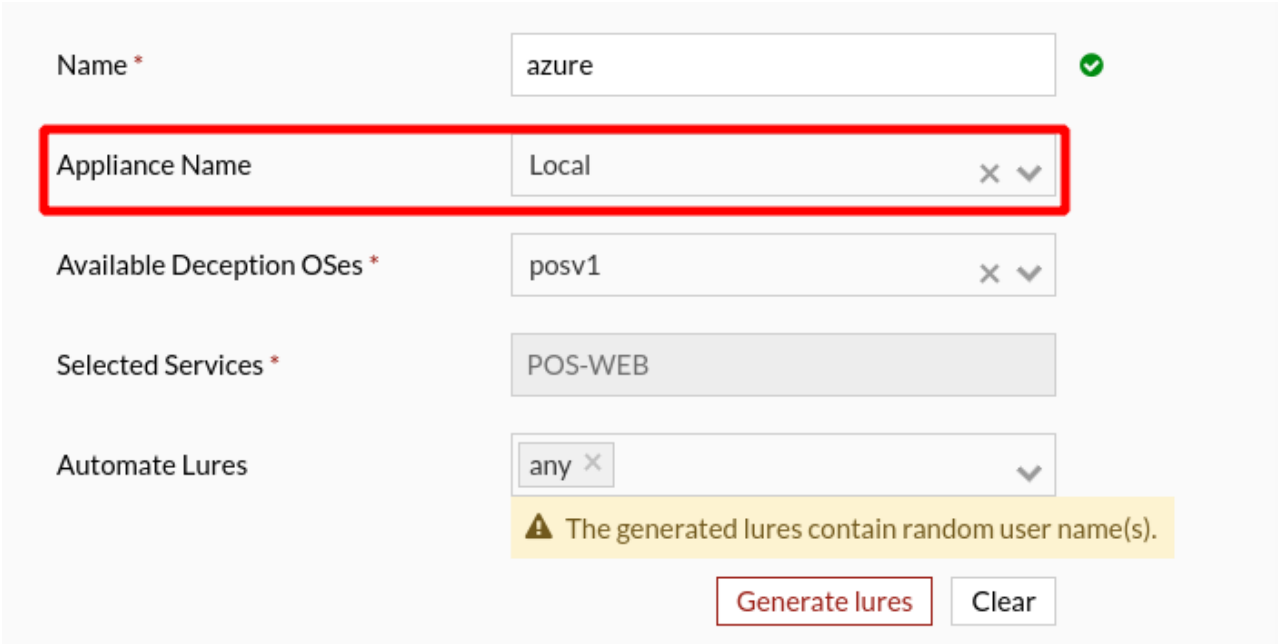


To locate the on the Azure platform:

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*.

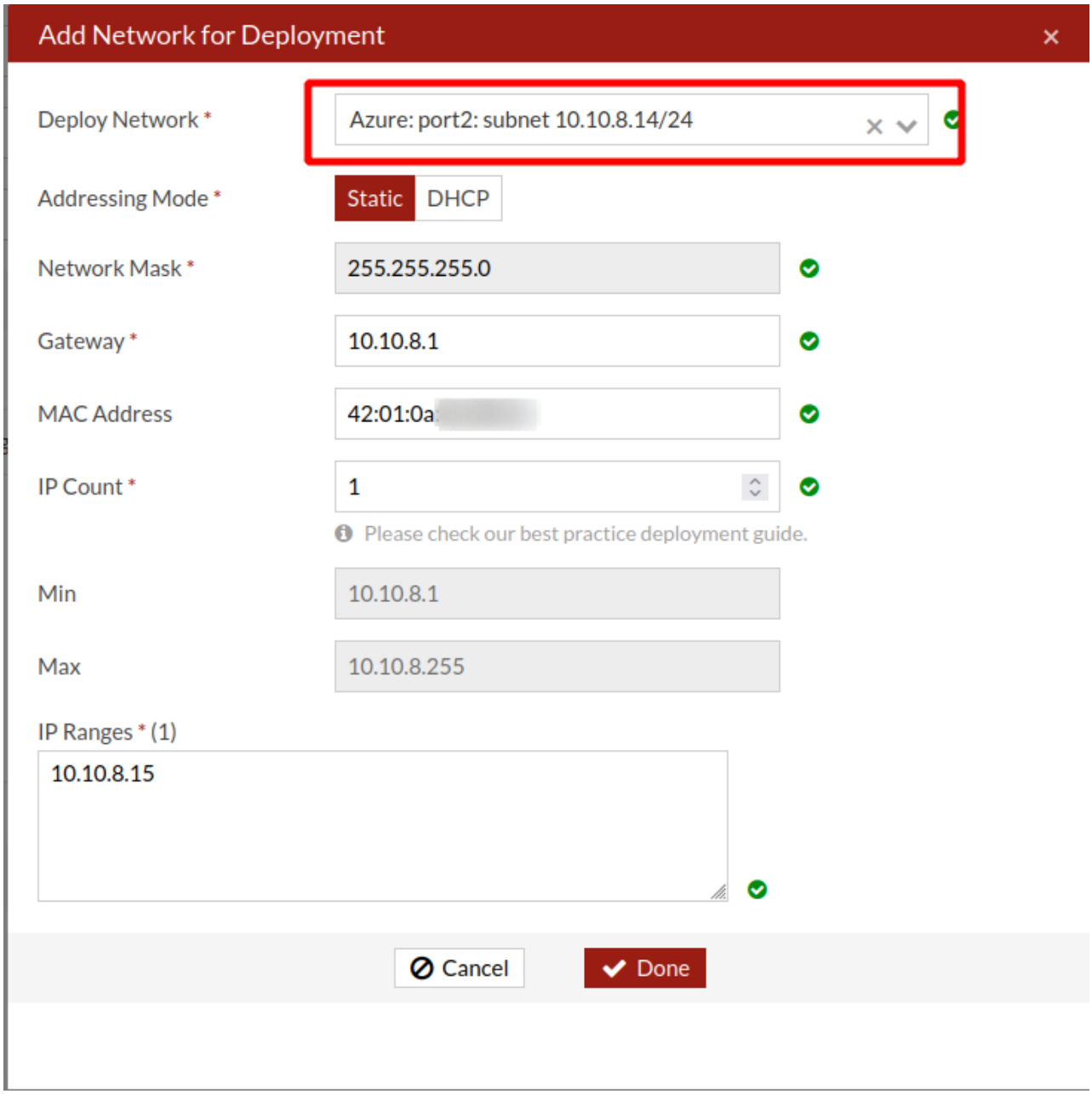


3. In the *Set Network* tab, click *Add network for Deployment* and configure the following settings:

Deploy Network	Select the deployment network.
Addressing Mode	Select *Static* or *DHCP* (dynamically assigned).

Network Mask	Enter the network mask.
Gateway	Enter the gateway IP address.
MAC Address	Enter the MAC address .
IP Count	Select the number of IP addresses allocated.
Min/Max	Define the range of IP addresses available in the subnet.
IP Ranges	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.



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