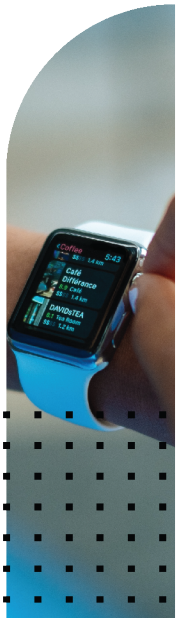
Azure Administration Guide

FortiManager 7.0.0



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

December 21, 2023
FortiManager 7.0.0 Azure Administration Guide
02-700-705457-20231221

TABLE OF CONTENTS

About FortiManager for Azure

FortiManager's security-operationalized visibility across your Fortinet Security Fabric enables true security effectiveness and foresight to identify and understand the scope of threats and facilitates actionable responses and risk remediation.

Quantifiable security solution information produces measurable accountability and uses those ratings to compare your security preparedness internally and to that of your industry peers.

Centralized change management helps you update policies and objects, maintain provisioning templates and easily configure changes to your APs, switches, SD-WAN and SDN connectors and more, to mitigate security events and apply configuration changes and policy updates.

Network administrators can better control their network by logically grouping devices into administrative domains (ADOMs), effectively applying policies and distributing content security/firmware updates. FortiManager is one of several versatile network security management products that provide diversity of deployment types, growth flexibility, advanced customization through APIs, and simple licensing, all through central management and configuration.

Instance type support

FortiManager supports the following instance types on Azure.

Supported instances on the Azure marketplace listing may change without prior notice.

FortiManager has a minimum requirement of 4 vCPU and 8GB of RAM on an instance.

Instance Types of A- and D-series may no longer appear as deployable at the time you install the FortiManager virtual machine (VM) via the Azure Marketplace.

For up-to-date information on each instance type, see the following links:

- Sizes for virtual machines in Azure
- General purpose virtual machine sizes
- Previous generations of virtual machine sizes

The following table shows all instance types currently supported on FortiManager:

Instance Type	vCPU	RAM (GB)
Dsv2 Series		
Standard_DS4_v2	8	28
Standard_DS5_v2	16	56
Dv3 Series		
Standard_D4_v3	4	16

Instance Type	vCPU	RAM (GB)
Standard_D8_v3	8	32
Standard_D16_v3	16	64
Standard Dav4 Series		
Standard_D4a_v4	4	16
Standard_D8a_v4	8	32
Standard_D16a_v4	16	64
Standard_D32a_v4	32	128
Standard_D48a_v4	48	192
Standard_D64a_v4	64	256
Standard_D96a_v4	96	384
Standard Dasv4 Series		
Standard_D4as_v4	4	16
Standard_D8as_v4	8	32
Standard_D16as_v4	16	64
Standard_D32as_v4	32	128
Standard_D48as_v4	48	192
Standard_D64as_v4	64	256
Standard_D96as_v4	96	384
Dasv4 Series		
D4as_v4	4	16
D8as_v4	8	32
D16as_v4	16	64
D32as_v4	32	128
D48as_v4	48	192
D64as_v4	64	256
D96as_v4	96	384

Previous Generation Instance Types	vCPU	RAM (GB)
Previous Generation		
Standard_A6 (retiring soon)	4	28
Standard_A7 (retiring soon)	8	56

Previous Generation Instance Types	vCPU	RAM (GB)
Standard_A8_v2	8	16
Standard_D4	8	28
Standard_DS4	8	28

Models

FortiManager-VM is licensed based on the number of managed devices, amount of logging per day, and storage capacity. Refer to price lists and order SKUs available through your resellers/distributors. These are also referred to as bring your own license (BYOL) models.

FortiManager-VM can be deployed using different CPU and RAM sizes and launched on various private and public cloud platforms.

Licensing

You must have a license to deploy FortiManager for Azure. The following sections provide information on licensing FortiManager for Azure:

- Order types on page 6
- Creating a support account on page 6
- Registering and downloading your license on page 7

Order types

On Azure, there is only one order type available for FortiManager: BYOL. Currently pay as you go/on-demand (PAYG) is not listed.

BYOL is annual perpetual licensing, as opposed to PAYG, which is an hourly subscription available with marketplace-listed products. BYOL licenses are available for purchase from resellers or your distributors, and prices are listed in the publicly available price list that is updated quarterly. BYOL licensing provides the same ordering practice across all private and public clouds, no matter the platform. You must activate a license the first time you access the instance from the GUI or the CLI before you start using features.

For BYOL, you typically order a combination of products and services.

See Creating a support account on page 6. Also see *Support* on the FortiManager BYOL marketplace product page.

Creating a support account

FortiManager for Azure supports BYOL licensing models.

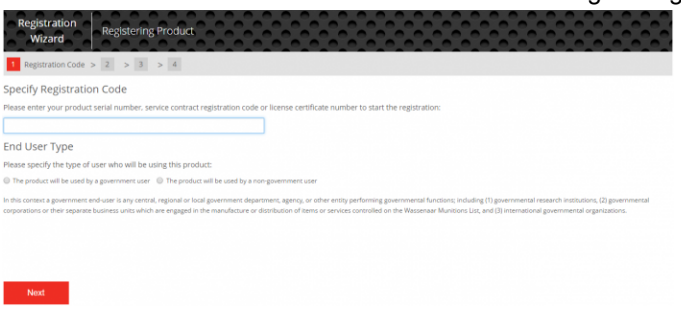
For BYOL, you typically order a combination of products and services, including support entitlement.

You must create a FortiCare support account and obtain a license to activate the product through the FortiCare support portal. If you have not activated the license, you will see the license upload screen when logging into FortiManager and cannot proceed to configure FortiManager. See Registering and downloading your license on page 7.

Registering and downloading your license

Licenses for the BYOL licensing model can be obtained through any Fortinet partner. After you purchase a license or obtain an evaluation license (60-day term), you will receive a PDF with an activation code.

1. Go to Customer Service & Support and create a new account or log in with an existing account.
2. Go to *Asset* > *Register/Renew* to start the registration process. In the *Specify Registration Code* field, enter your license activation code and select *Next* to continue registering the product. Enter your details in the other fields.



3. At the end of the registration process, download the license (.lic) file to your computer. You will upload this license later to activate the FortiManager-VM.
4. After registering a license, Fortinet servers may take up to 30 minutes to fully recognize the new license. When you upload the license (.lic) file to activate the FortiManager-VM, if you get an error that the license is invalid, wait 30 minutes and try again.

Deploying a FortiManager-VM on Azure

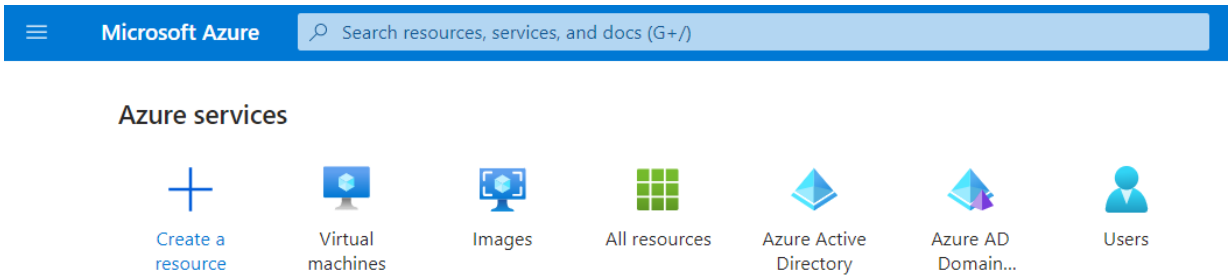
Deploying a FortiManager-VM on Azure consists of the following steps:

1. Creating a FortiManager-VM on page 9
2. Connecting to FortiManager on page 13
3. Adding a disk to the FortiManager-VM (optional) on page 14

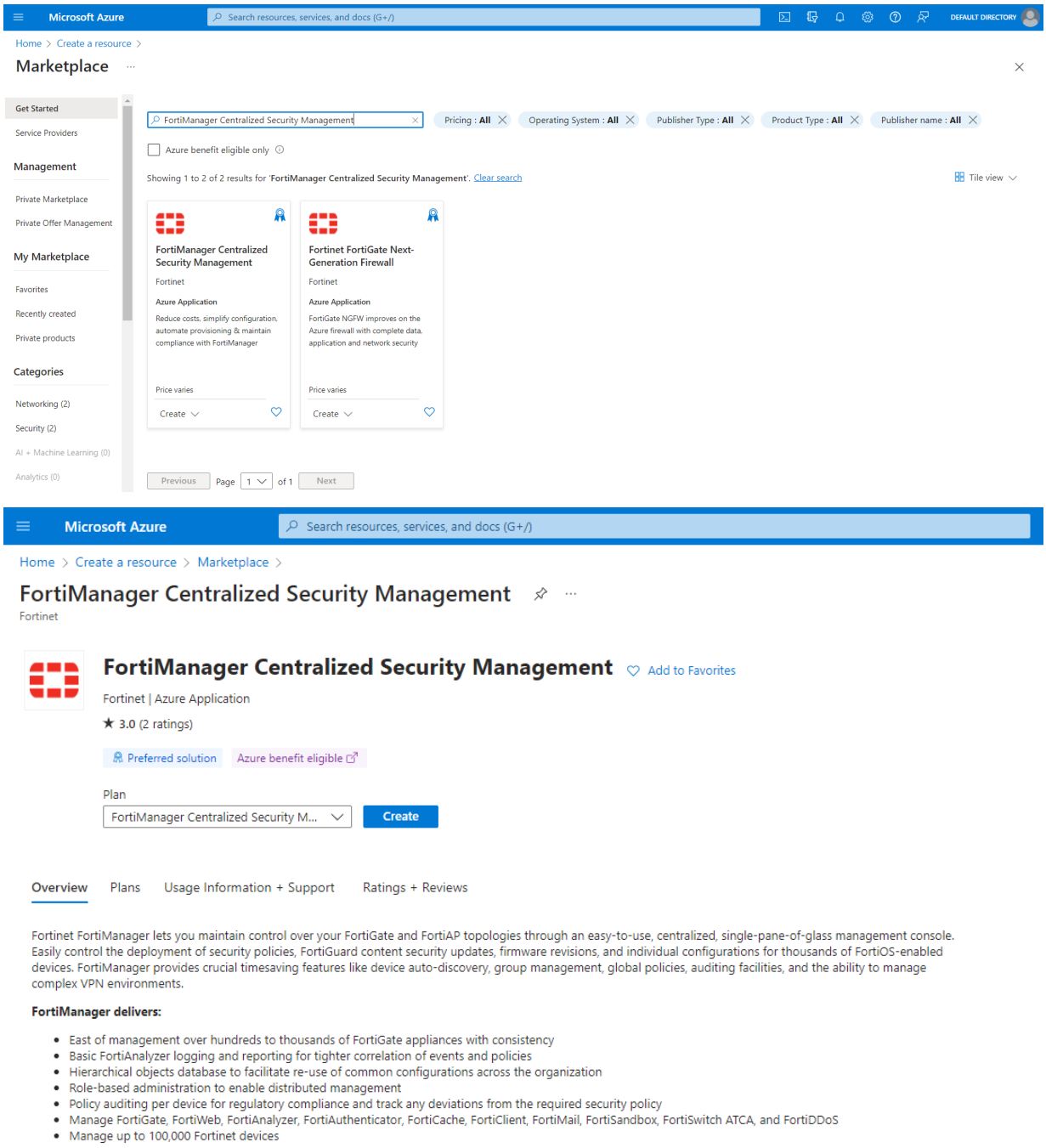
Creating a FortiManager-VM

To create FortiManager-VM on Azure:

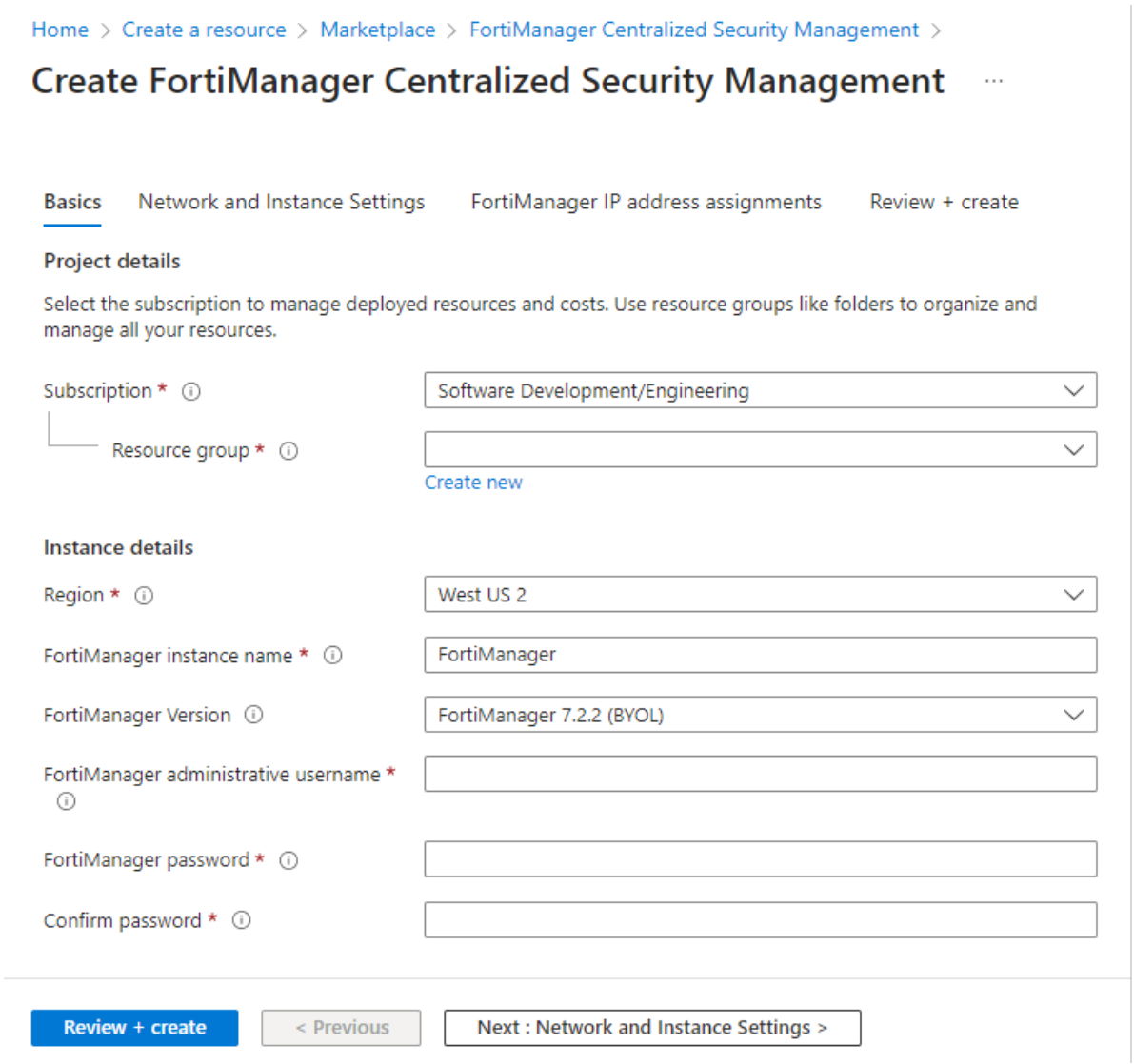
1. Find the FortiManager-VM in the Microsoft Azure Portal:
   a. Log into the Microsoft Azure Portal and click *Create a resource*.



   b. Search for FortiManager Centralized Security Management and select it from the search results.

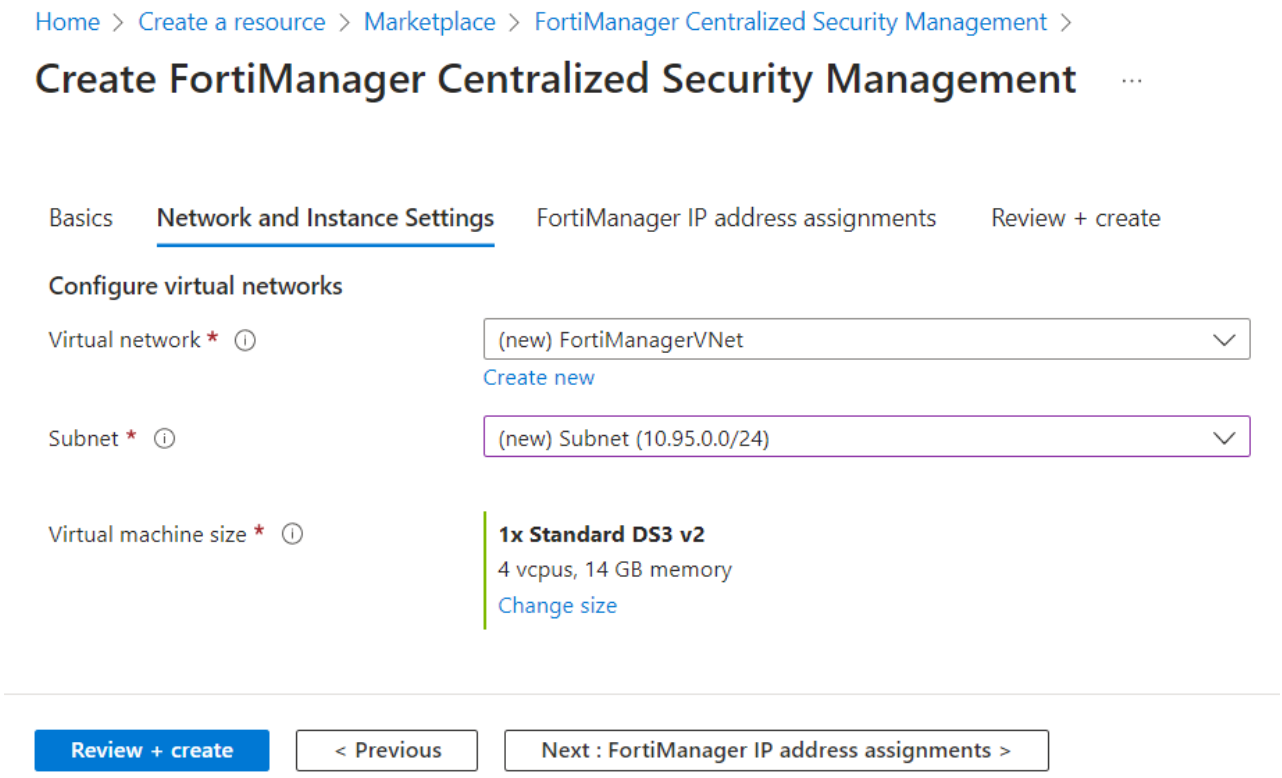


2. Click *Create*.
3. Configure the *Basics* section:



a. Select the appropriate *Subscription* from the dropdown list. You may have only one option here. Ensure your organization's subscription allows you to purchase the product.
b. Select the *Resource group*. You can either create a new resource group or select an existing one.
c. Select the appropriate *Region* for the deployment.
d. Enter a FortiManager-VM name in the *FortiManager instance name* field.
e. Under *FortiManager Version*, select the desired version.
f. Set a *FortiManager administrative username*. This name cannot be *admin* or *root*.
g. Enter a *FortiManager password* for the new account and confirm the password. For security reasons, it is not possible to reset this password through the Microsoft Azure portal, so make sure that you remember the password.
h. Click *Next: Network and Instance Settings*.

4. Configure the *Network and Instance Settings* section:



a. Select the *Virtual network*. You can either create a new virtual network (VNet) or select an existing one.

b. Select the *Subnet* where the FortiManager-VM will be deployed.

c. In *Virtual machine size*, select the appropriate VM size for your deployment. In the Microsoft Azure Marketplace, the FortiManager-VMs come in a variety of sizes. Each VM size within each series has different limits for the amount of memory, number of NICS, maximum number of data disks, size of cache, and maximum IOPS and bandwidth.

d. Click *Next: FortiManager IP address assignments*.

5. Configure the *FortiManager IP address assignments* section:

a. Select *First public IP address resource name*. You can either create a new public IP address or select an existing one.

b. In the *Public IP address type* field, select *Dynamic* or *Static*. It usually fine to accept the default value.

c. Click *Next: Review + create*.

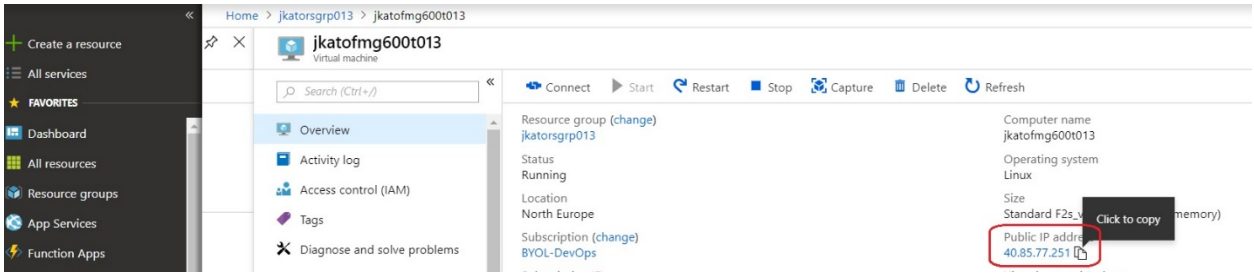
6. Wait for validation to pass, then click *Create*. If an error occurs at this stage, resolve it or contact Microsoft support.

Azure deploys the FortiManager-VM and displays a success message upon completion. The deployment may take 30 minutes or longer to complete.

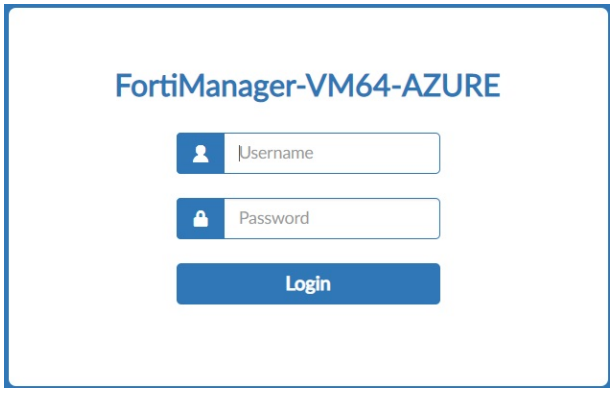
FortiManager-VM requires a minimum disk size of 500GB. By default, a log disk of 1 TB is automatically allocated to a FortiManager-VM instance.

Connecting to FortiManager

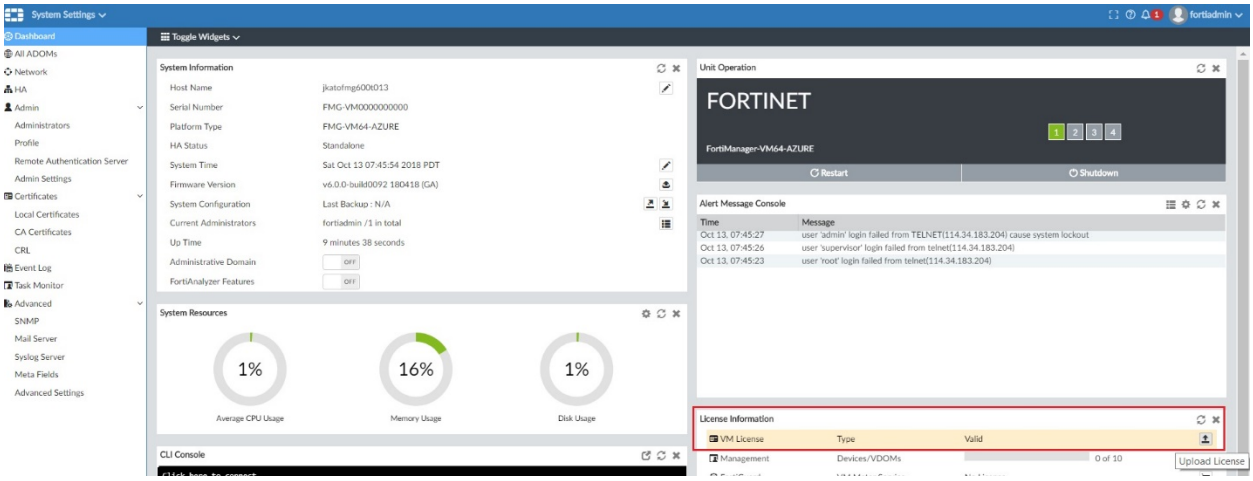
1. To connect to the FortiManager-VM, you must find its public IP address.



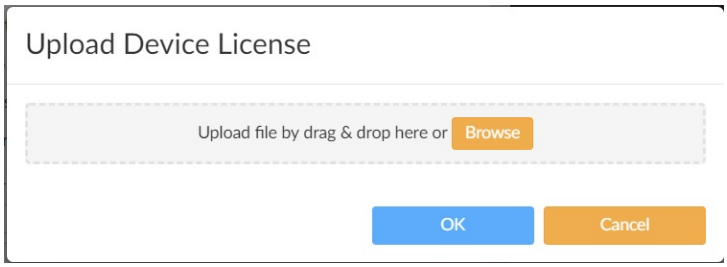
2. Connect to the FortiManager-VM using your browser and the FortiManager-VM IP address. Log into the FortiManager-VM with the configured *FortiManager administrative username* and *password*.



3. Go to *System Settings*. On the *License Information* widget, click the button on the right



4. Upload your license (.lic) file to activate the FortiManager-VM. Restart the FortiManager-VM and log in again.



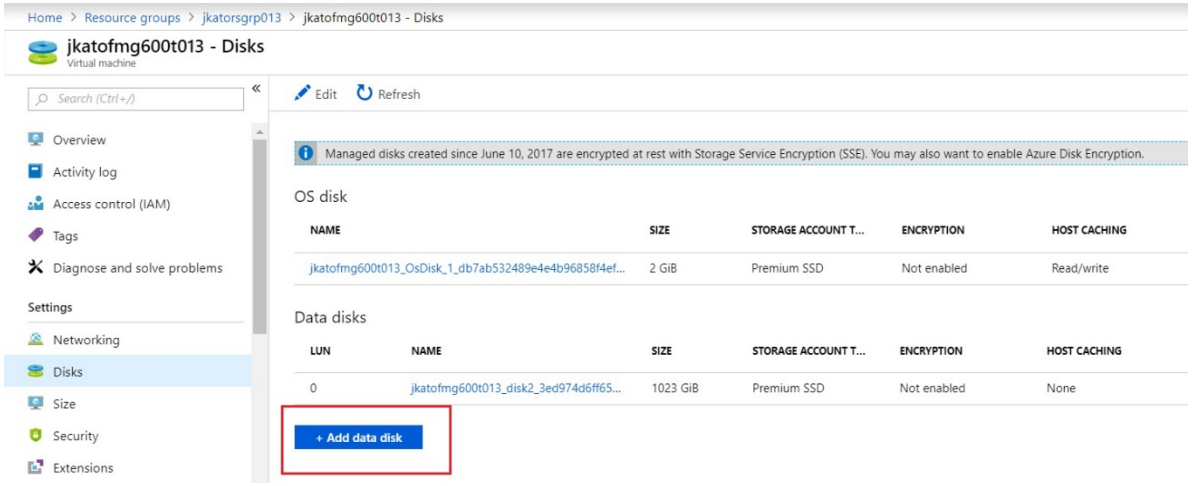
5. After you log in, you will see that the license has been uploaded. You need to wait for authentication with the registration servers. This can take up to 30 minutes.
6. Select *Return*. You will now see the FortiManager-VM dashboard.

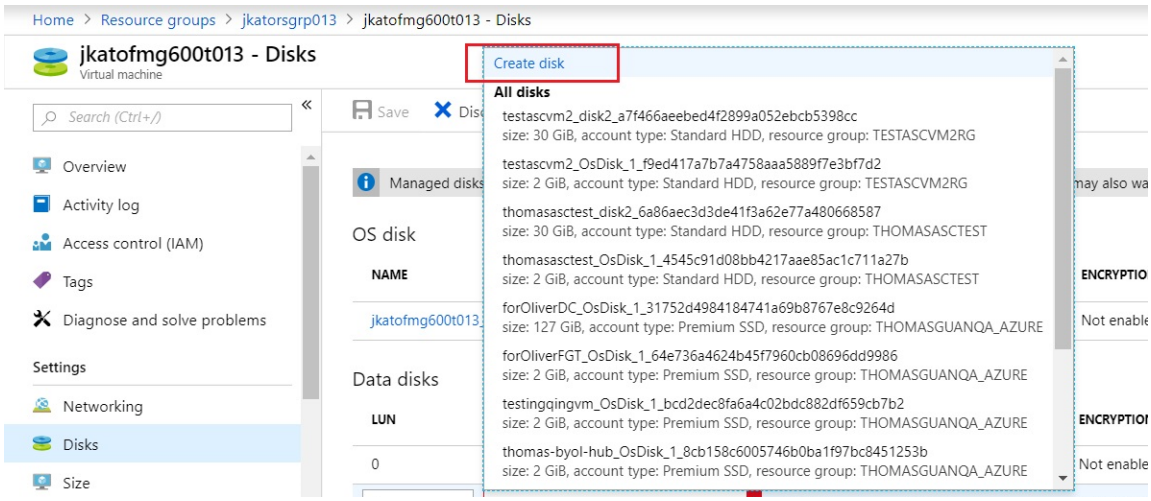
Adding a disk to the FortiManager-VM (optional)

In the future or depending on your license requirements, you may need to add more disks to your FortiManager-VM instances.

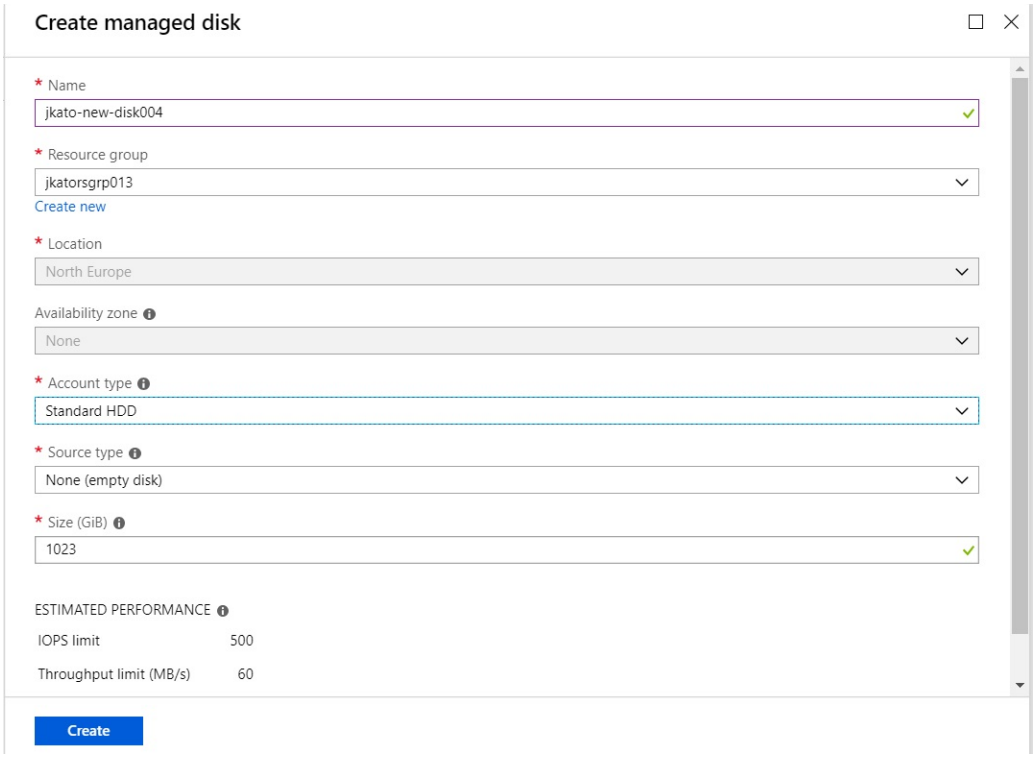
For details about Azure disks, refer to Azure Managed Disks Overview.

1. Click *Add data disk* > *Create disk*.

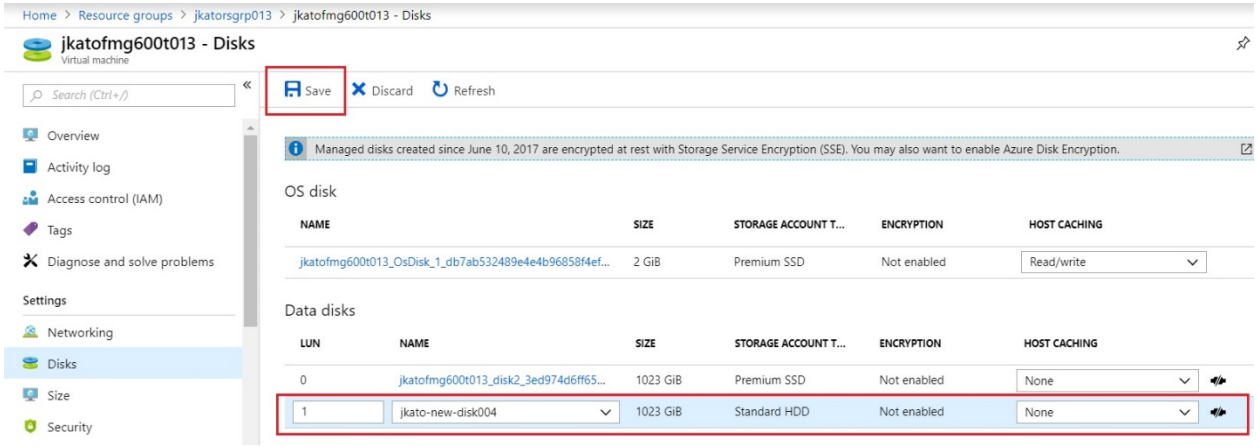




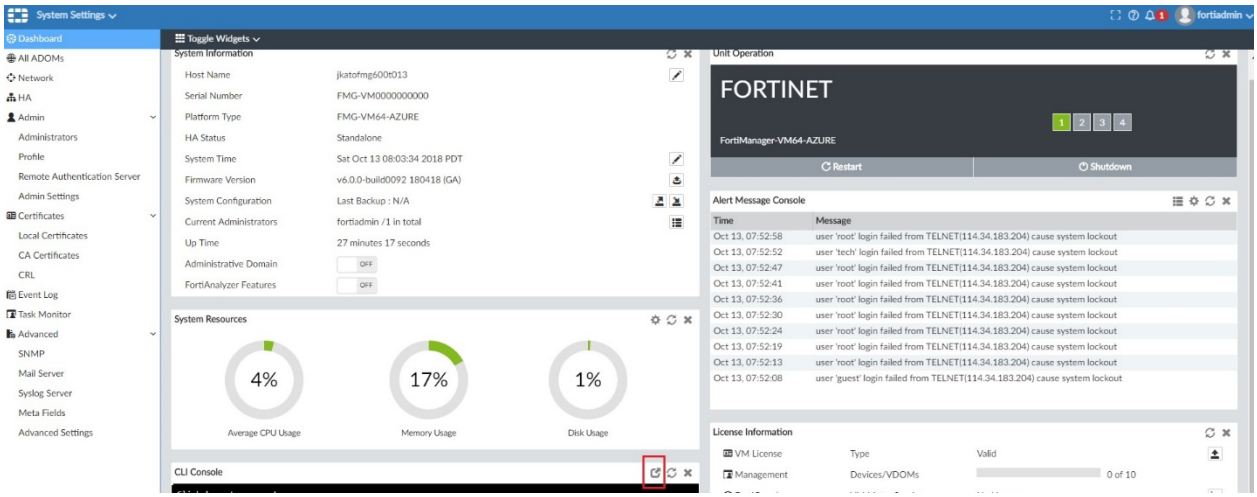
2. Create and configure an additional empty disk as shown below. Click *Create*.



3. Save the disk.



4. Log into the FortiManager-VM management GUI console.
5. Go to *System Settings*. Invoke the CLI console.



6. In the command prompt window, enter `exec lvm info`. The newly added disk appears as `Unused`.

```
jkatofmg600t013 # exec lvm info
LVM Status: OK

Disk1  :         Used     1072GB
Disk2  :       Unused     1072GB
Disk3  :  Unavailable        0GB
Disk4  :  Unavailable        0GB
Disk5  :  Unavailable        0GB
Disk6  :  Unavailable        0GB
Disk7  :  Unavailable        0GB
Disk8  :  Unavailable        0GB
Disk9  :  Unavailable        0GB
Disk10 :  Unavailable        0GB
Disk11 :  Unavailable        0GB
Disk12 :  Unavailable        0GB
Disk13 :  Unavailable        0GB
Disk14 :  Unavailable        0GB
Disk15 :  Unavailable        0GB
```

7. Enter `exec lvm extend` to incorporate the disk to the FortiManager system. Entering `y` reboots the instance.

```
jkatofmg600t013 #
jkatofmg600t013 # exec lvm extend
Disk2 will be added to LVM.
This operation will need to reboot the system.
Do you want to continue? (y/n)
```

8. Navigate to the FortiManager dashboard. You will see now that the available disk size has changed. You can also run `exec lvm info` again in the CLI to see that the additional disk is now in use.

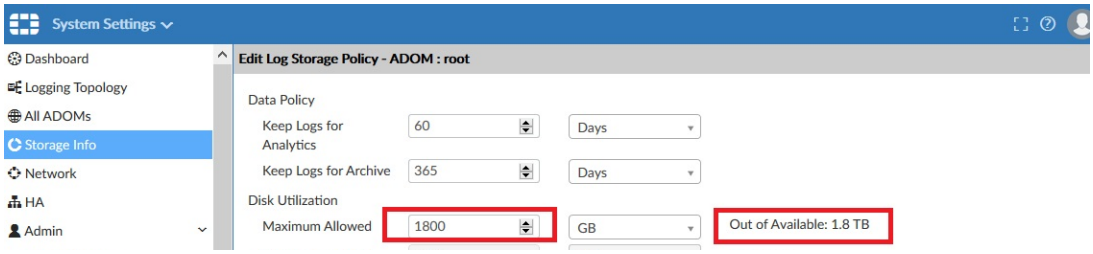
```
jkatofmg600t013 #
jkatofmg600t013 # exec lvm info
LVM Status: OK

Disk1  :         Used     1072GB
Disk2  :         Used     1072GB
Disk3  :  Unavailable        0GB
Disk4  :  Unavailable        0GB
Disk5  :  Unavailable        0GB
Disk6  :  Unavailable        0GB
Disk7  :  Unavailable        0GB
Disk8  :  Unavailable        0GB
Disk9  :  Unavailable        0GB
Disk10 :  Unavailable        0GB
Disk11 :  Unavailable        0GB
Disk12 :  Unavailable        0GB
Disk13 :  Unavailable        0GB
Disk14 :  Unavailable        0GB
Disk15 :  Unavailable        0GB
```

The FortiManager system reserves a certain portion of disk space for system use and unexpected quota overflow. The remaining space is available for allocation to devices. Reports are stored in the reserved space. The following describes the reserved disk quota relative to the total available disk size (other than the root device):

- Small disk (equal to 500 GB): reserves 20% or 50 GB of disk space, whichever is smaller.
- Medium disk (less than or equal to 1 TB): reserves 15% or 100 GB of disk space, whichever is smaller.
- Medium to large disk (less than or equal to 5 TB): reserves 10% or 200 GB of disk space, whichever is smaller.
- Large disk (less than 5 TB): reserves 5% or 300 GB of disk space, whichever is smaller.

9. Configure the consumable disk space for logging. 200 GB is reserved. Therefore, 1.8 TB is available for consumption out of the 2 TB of disks.



Security Fabric connector integration with Azure

You can use FortiManager to create Fabric connectors for Azure, and then install the Fabric connectors to FortiOS.

The Fabric connectors in FortiManager define the type of connector and include information for FortiOS to communicate with and authenticate with the products. In some cases the FortiGate must communicate with products through the Fabric connector, and in other cases the FortiGate communicates directly with the products.

FortiOS works without the Fabric connector to communicate directly with Azure.

Following is an overview of creating an Azure Fabric connector using FortiManager:

1. Create an Azure Fabric connector object. See Creating fabric connector objects for Microsoft Azure on page 18.
2. Create dynamic firewall address objects. See Configuring a dynamic firewall address for a Fabric connector on page 19.
3. Import address names from Azure to the Fabric connector. See Importing address names to a Fabric connector on page 19. FortiManager imports the address names and converts them to dynamic firewall address objects. The objects do not include IP addresses and display in *Firewall Objects* > *Addresses*.
4. In the policy package where you will create the new policy, create an IPv4 policy and include the dynamic firewall address objects for Azure. See Creating an IP policy on page 20.
5. Install the policy package to FortiOS. See Installing a policy package on page 21.
   FortiOS communicates with Azure to dynamically populate the firewall address objects with IP addresses.

Creating fabric connector objects for Microsoft Azure

With FortiManager, you can create a fabric connector for Microsoft Azure. You cannot import address names from Microsoft Azure to the fabric connector. Instead you must manually create dynamic firewall objects that you can use in policies. When you install the policies to one or more FortiGate units, FortiGate uses the information to communicate with Microsoft Azure and dynamically populate the objects with IP addresses. Fortinet SDN Connector is not required for this configuration.

When you create a fabric connector for Microsoft Azure, you are specifying how FortiGate can communicate directly with Microsoft Azure.

If ADOMs are enabled, you can create one fabric connector per ADOM.

Requirements:

- FortiManager version 6.0 ADOM or later
- FortiGate is managed by FortiManager.
- The managed FortiGate unit is configured to work with Microsoft Azure.

To create a fabric connector object for Microsoft Azure:

1. Go to *Fabric View* > *Fabric Connectors*.
2. Click *Create New*. The *Create New Fabric Connector* wizard is displayed.

3. Under *SDN*, select *Azure*, and click *Next*.
4. Configure the following options, and then click *OK*:

Name	Type a name for the fabric connector object.
Type	Displays Microsoft Azure.
Azure tenant ID	Type the tenant ID from Azure.
Azure client ID	Type the client ID from Azure.
Azure client secret	Type the client secret from Azure.
Azure subscription ID	Type the subscription ID for Azure.
Azure resource group	Type the resource group for Azure.
Update Interval (s)	Specify how often in seconds that the dynamic firewall objects should be updated.
Status	Toggle *On* to enable the fabric connector object. Toggle *OFF* to disable the fabric connector object.
Advanced Options	Expand to specify advanced options for Azure.
azure-region	Select an Azure region.

Configuring a dynamic firewall address for a Fabric connector

To configure dynamic firewall addresses for a Fabric connector:

1. Go to *Policy & Objects* > *Object Configurations*.
2. In the tree menu, go to *Firewall Objects* > *Addresses*.
3. In the content pane, click *Create New* and select *Address*.
4. Complete the following options for Microsoft Azure Fabric connectors:

Address Name	Enter a name for the firewall address object.
Type	Select *Fabric Connector Address*.
SDN	Select the Azure Fabric connector.
Filter	Enter the name of the filter.

5. Set the remaining options as required, and click *OK*.

Importing address names to a Fabric connector

After you configure a Fabric connector, you can import dynamic objects from cloud platforms, such as Azure, to the Fabric connector, and dynamic firewall address objects are automatically created.

To import address names for Azure:

1. Go to *Policy & Objects* > *Object Configurations*.
2. Go to *Security Fabric* > *Fabric Connectors*.
3. In the content pane, right-click the Azure Fabric connector, and select *Import*. The *Import SDN Connector* dialog displays.
4. Select the address names, and click *Import*. FortiManager imports the address names and converts them to dynamic firewall address objects that display on the *Firewall Objects* > *Addresses* pane.

Creating an IP policy

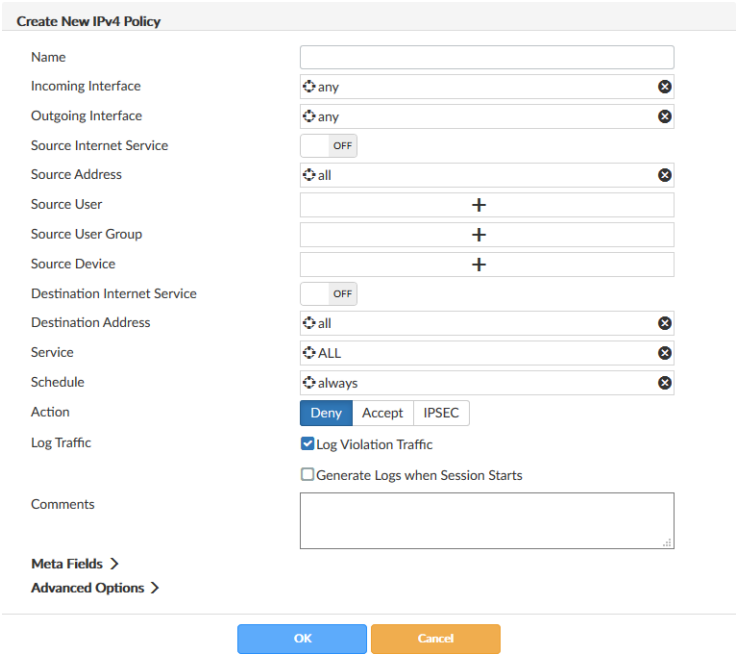
The section describes how to create new IPv4 and IPv6 policies.

IPv6 security policies are created both for an IPv6 network and a transitional network. A transitional network is a network that is transitioning over to IPv6, but must still have access to the Internet or must connect over an IPv4 network. IPv6 policies allow for this specific type of traffic to travel between the IPv6 and IPv4 networks.

On the *Policy & Objects* tab, from the *Tools* menu, select *Display Options*. In the *Policy* section, select the *IPv6 Policy* checkbox to display this option.

To create a new IPv4 or IPv6 policy:

1. Ensure that you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the tree menu for the policy package in which you will be creating the new policy, select *IPv4 Policy* or *IPv6 Policy*. If you are in the Global Database ADOM, select *IPv4 Header Policy*, *IPv4 Footer Policy*, *IPv6 Header Policy*, or *IPv6 Footer Policy*.
4. Click *Create New*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be added to the bottom of the list, but above the implicit policy. The *Create New Policy* pane opens.



5. Complete the options.
6. Click *OK* to create the policy.
   You can select to enable or disable the policy in the right-click menu. When disabled, a disabled icon will be displayed in the *Seq.#* column to the left of the number.

Installing a policy package

When installing a policy package, objects that the policy references are installed to the target device. Default or per-device mapping must exist or the installation fails.

Some objects that are not directly referenced in the policy will also be installed to the target device, such as FSSO polling objects, address and profile groups, and CA certificates.

To install a policy package to a target device:

1. Ensure you are in the ADOM that contains the policy package.
2. Go to *Policy & Objects* > *Policy Packages*.
3. Select a policy package and from the *Install* menu or right-click menu select *Install Wizard*. The *Install Wizard* opens.
4. Follow the steps in the install wizard to install the policy package. You can select to install policy package and device settings or install the interface policy only.

Change log

Date	Change description
2021-04-22	Initial release.
2021-08-20	Added note to About FortiManager for Azure on page 4.
2022-09-15	Updated Instance type support on page 4.
2023-03-07	Updated Instance type support on page 4.
2023-05-17	Updated Creating a FortiManager-VM on page 9.
2023-12-21	Updated Instance type support on page 4.

www.fortinet.com