

FortiManager - Azure Cookbook

Version 6.2

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

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

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



November 25, 2021

FortiManager 6.2 Azure Cookbook

02-620-611721-20211125

TABLE OF CONTENTS

About FortiManager for Azure	4
Instance type support	4
Models	4
Licensing	4
Order types	5
Creating a support account	5
Registering and downloading your license	5
Deploying FortiManager-VM on Azure	6
Creating a FortiManager-VM	7
Connecting to FortiManager	12
Adding a disk to the FortiManager-VM for logging (optional)	13
Security Fabric connector integration with Azure	17
Creating fabric connector objects for Microsoft Azure	17
Configuring a dynamic firewall address for a Fabric connector	18
Importing address names to a Fabric connector	18
Creating an IP policy	19
Installing a policy package	20
Change log	21

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

You can deploy FortiManager for Azure as a virtual machine. Supported instances are from the General-purpose instance types. Currently FortiManager for Azure supports the Dsv3, Dv3, Dsv2, and Dv2-series up to 16 vCPU.

Supported instances may change without notice. For up-to-date information on each instance type, see the following:

- [General purpose virtual machine sizes](#)
- [FortManager Centralized Security Management](#)

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 5](#)
- [Creating a support account on page 5](#)

- [Registering and downloading your license on page 5](#)

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 5](#). Also see *Support* on the FortiManager BYOL [marketplace product page](#).

Creating a support account

FortiManager for Azure supports BYOL licensing models.

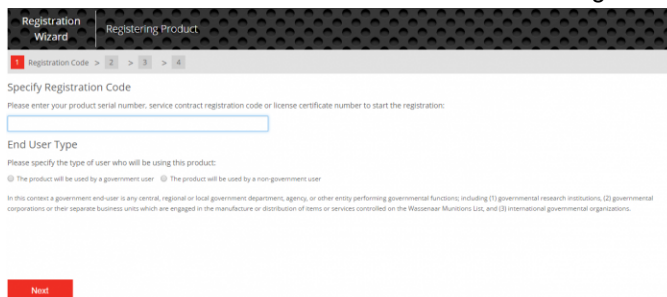
For BYOL, you typically order a combination of products and services, including support entitlement.

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 5](#).

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 FortiManager-VM on Azure

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

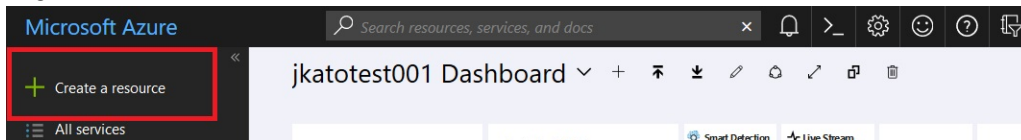
1. [Creating a FortiManager-VM on page 7](#)
2. [Connecting to FortiManager on page 12](#)
3. [Adding a disk to the FortiManager-VM for logging \(optional\) on page 13](#)

Creating a FortiManager-VM

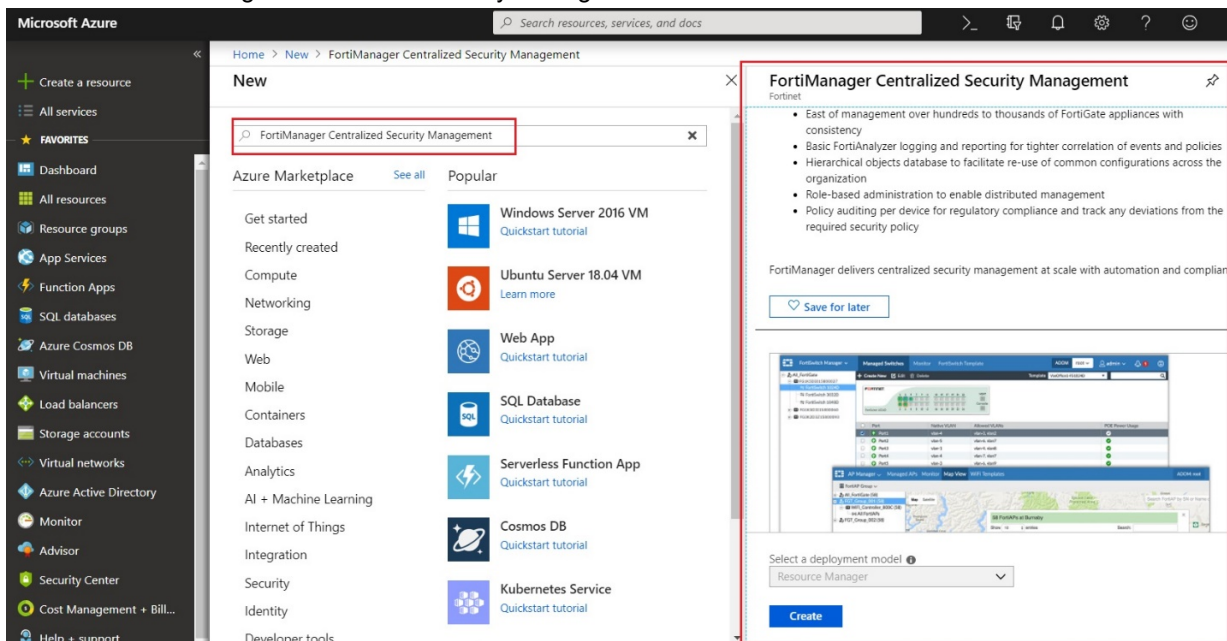
To create a FortiManager-VM on Azure:

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:

- Set a FortiManager-VM name in the *FortiManager instance name* field.
- Under *FortiManager Version*, select the desired version.
- Set a *FortiManager administrative username*. This name cannot be admin or root.
- Choose 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.
- 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.
- Create a new *Resource group*. Currently, it is not possible to select an existing resource group for a Microsoft Azure Marketplace template set if it is not empty, so you must create a new one.

- g. Set a *Location* for the VM. Click *OK*.

Create FortiManager Centrali... X

Basics X

- 1 Basics
Configure basic settings >
- 2 Network and Instance Settings
Configure the network and inst... >
- 3 FortiManager IP address assign...
Configure Public IP Address >
- 4 Summary
FortiManager Centralized Secu... >
- 5 Buy >

* FortiManager instance name ⓘ
jkatofmg600t013 ✓

FortiManager Version ⓘ
FortiManager 5.6.3 (BYOL)
FortiManager 6.0.0 (BYOL)

* FortiManager administrative username ⓘ
[Empty field]

* FortiManager password ⓘ
[Empty field]

* Confirm password
[Empty field]

Subscription
BYOL-DevOps

* Resource group ⓘ
(New) jkatorsgrp013
[Create new](#)

* Location
North Europe

OK

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

- Select *Virtual network*. You can either create a new virtual network (VNet) or select an existing one.
- In the *Address space* field, accept the default values or specify your own. Click *OK*.

Create FortiManager Centrali... X

Network and instance settings X

- 1 Basics
Done ✓
- 2 Network and Instance Settings
Configure the network and inst... >
- 3 FortiManager IP address assign...
Configure Public IP Address >
- 4 Summary
FortiManager Centralized Secu... >
- 5 Buy >

* Virtual network ⓘ
(new) FortiManagerVNet >

Subnet ⓘ
Configure subnets ⓘ

* Virtual machine size ⓘ
1x Standard F2s_v2 >

OK

Choose virtual network X

These are the virtual networks in the selected subscription and location 'North Europe'.

+ Create new

- atwomblyexistingvnet
atwomblyexistingvnet
- AzureStack-VNET
ThomasAzureStack
- bmac121516rgvnet
bmac121516rg
- charles_zhang_ftnt
charles_zhang_ftnt
- checkpointtest
checkpointtest
- ellentestnortheurope1
ellentestnortheurope1
- FAZRG-vnet-NE
FAZRG-NE

Create virtual network X

* Name
FortiManagerVNet

* Address space
10.52.0.0/16
10.52.0.0 - 10.52.255.255 (65536 addresses)

OK

5. In the *Subnet* section, the *Subnet* name and *Subnet* address prefix are pre-defined and you should not need to change the default values. Click *OK*.

The screenshot displays the 'Create FortiManager Centralized Security' wizard in the Azure portal. The wizard has five steps: 1. Basics (Done), 2. Network and Instance Settings (active), 3. FortiManager IP address assignments, 4. Summary, and 5. Buy. In the 'Network and instance settings' step, the 'Virtual network' is '(new) FortiManagerVNet' and the 'Virtual machine size' is '1x Standard F2s_v2'. A 'Subnet' configuration window is open, showing 'Subnet' as the name and '10.52.0.0/24' as the address prefix. The 'Subnet' window has an 'OK' button at the bottom.

6. In the *Virtual machine size* section, 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. Click **OK**.
7. Configure the *FortiManager IP address assignments* section:
 - a. Select *First public IP address resource name*. In the *Name* field, set a name for the FortiManager's public IP address.
 - b. In the *SKU* field, select *Basic* or *Standard*. Click **OK**. Generally it is fine to accept the default value.
 - c. In the *Public IP address type* field, select *Dynamic* or *Static*. Click **OK**. Again, it usually fine to accept the default value.
 - d. Click **OK** twice.

Create FortiManager Centrali... X

1 Basics Done ✓

2 Network and Instance Settings Done ✓

3 FortiManager IP address assign... Configure Public IP Address >

4 Summary FortiManager Centralized Secu... >

5 Buy >

IP assignment X

First public IP address resource na... (new) FortiManager-PublicIP >

Public IP address type **Static** Dynamic

OK

Choose public IP address X

Dynamic public IP addresses that are not in use won't have an IP address assigned to them.

These are the public IP addresses in the selected subscription and location 'North Europe'.

Create new

None

atwomblyexistingpip2 atwomblyexistingvnet

ondemandpip_6 fazrg

atwomblyexistingpip atwomblyexistingvnet 13.69.186.94 (St...

AzS-HOST1-IP ThomasAzureStack 40.113.4.252 (D...

bmac121516rgpublicip bmac121516rg 40.85.133.249 (S...

CheckPoint checkpointtest

FGTAMgmtPublicIP jkatorsgrp012 52.142.113.205 (...)

FGTAPClusterPublicIP jkatorsgrp012 52.142.113.243 (...)

FGTBMgmtPublicIP jkatorsgrp012 52.142.113.242 (...)

fmgzure-northE

OK

Create public IP address X

Name FortiManager-PublicIP

SKU **Basic** Standard

Assignment **Dynamic** Static

OK

8. Wait for validation to pass, then select OK. If an error occurs at this stage, resolve it or contact Microsoft support.

Summary X

Validation passed

Basics

Subscription BYOL-DevOps

Resource group jkatorsgrp013

Location North Europe

FortiManager instance name jkatofmg600t013

FortiManager Version FortiManager 6.0.0 (BYOL)

FortiManager administrative us... fortidadmin

FortiManager password *****

Network and instance settings

Virtual network FortiManagerVNet

Subnet Subnet

Subnet address prefix 10.52.0.0/24

Virtual machine size Standard F2s_v2

IP assignment

First public IP address resource ... FortiManager-PublicIP

Domain Name -

Public IP address type Static

OK

Download template and parameters



By default, a log disk of 1 TB is automatically allocated to a FortiManager-VM instance.

9. Select **Create** to buy the FortiManager-VM instance from Microsoft Azure. Once the FortiManager-VM is deployed, you will see a "Deployment succeeded" message. The deployment may take 30 minutes or longer to complete.

Create

FortiManager Centralized Security Management

by Fortinet

[Terms of use](#) | [privacy policy](#)

Deploying this template will result in various actions being performed, which may include the deployment of one or more Azure resources or Marketplace offerings and/or transmission of the information you provided as part of the deployment process to one or more parties, as specified in the template. You are responsible for reviewing the text of the template to determine which actions will be performed and which resources or offerings will be deployed, and for locating and reviewing the pricing and legal terms associated with those resources or offerings.

Current retail prices for Azure resources are set forth [here](#) and may not reflect discounts applicable to your Azure subscription.

Prices for Marketplace offerings are set forth [here](#), and the legal terms associated with any Marketplace offering may be found in the Azure portal; both are subject to change at any time prior to deployment.

Neither subscription credits nor monetary commitment funds may be used to purchase non-Microsoft offerings. These purchases are billed separately. If any Microsoft products are included in a Marketplace offering (e.g., Windows Server or SQL Server), such products are licensed by Microsoft and not by any third party.

Template deployment is intended for advanced users only. If you are uncertain which actions will be performed by this template, which resources or offerings will be deployed, or what prices or legal terms pertain to those resources or offerings, do not deploy this template.

Terms of use

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) provided above as well as the legal terms and privacy statement(s) associated with each Marketplace offering that will be deployed using this template, and (b) authorize Microsoft to charge or bill my current payment method for the deployment of this template.

Create

Microsoft Azure

Search resources, services, and docs

Create a resource

All services

FAVORITES

Dashboard

All resources

My Dashboard

New dashboard

Upload

Download

Edit

Share

Full screen

Clone

Help + support

Resources

Resources

Resources

Notifications

More events in the activity log →

Deployment in progress...

Deployment to resource group 'jkatorsgrp013' is in progress.

by me

Notifications

More events in the activity log →

Dismiss all ...

Deployment succeeded

Deployment 'fortinet.fortimanagerfortimanager-20181013073442' to resource group 'jkatorsgrp013' was successful.

Go to resource group

Pin to dashboard

by me

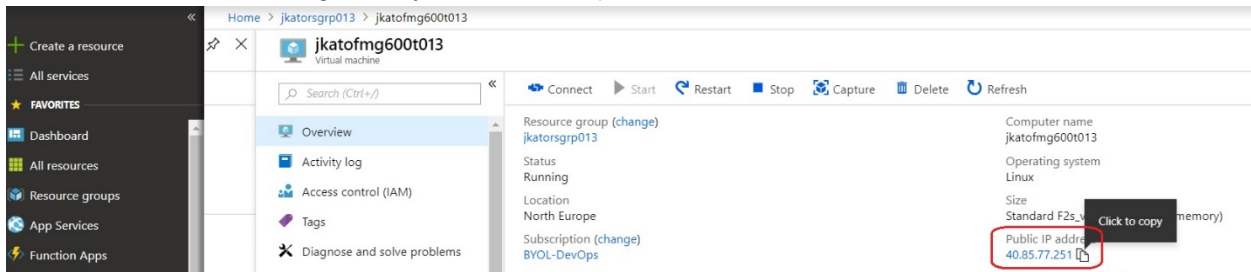
a few seconds ago



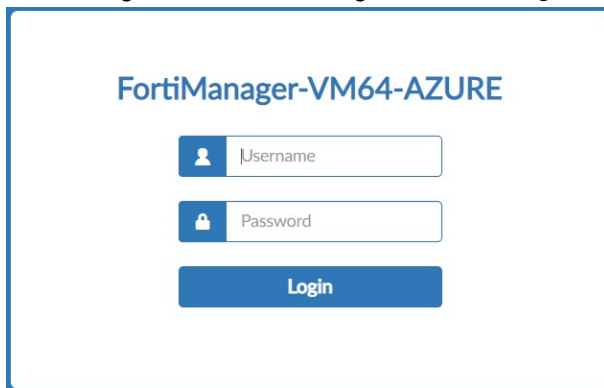
The terms of use you see at the time of your deployment may differ from the screenshot above.

Connecting to FortiManager

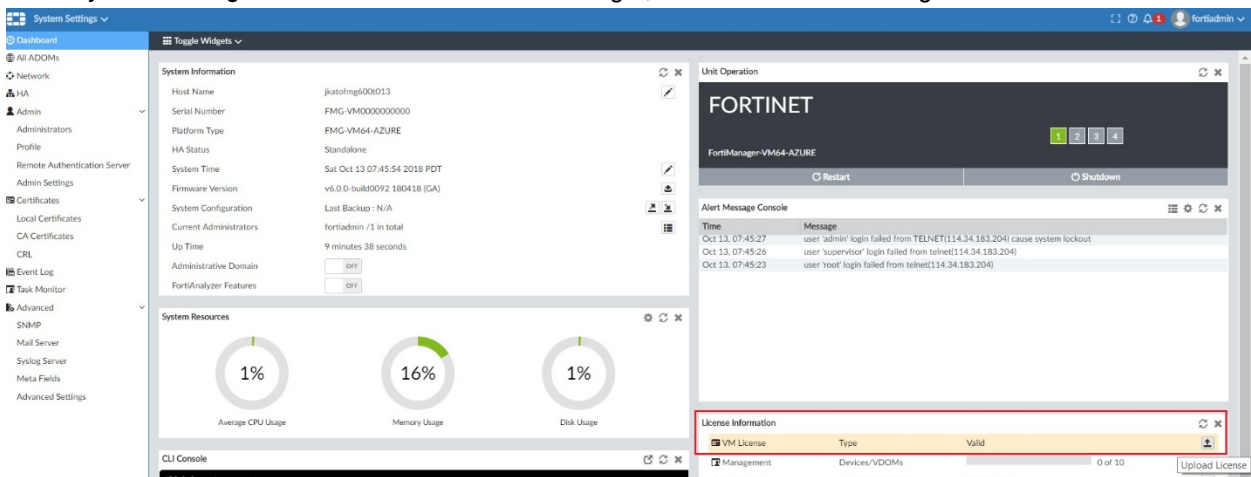
1. To connect to the FortiManager-VM, you must find its public IP address.



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.

Upload Device License

Upload file by drag & drop here or [Browse](#)

[OK](#) [Cancel](#)

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 for logging (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*.

Home > Resource groups > jkatorsgrp013 > jkatofmg600t013 - Disks

jkato

Virtual machine

Search (Ctrl+J)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Networking

Disks

Size

Security

Extensions

Edit Refresh

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

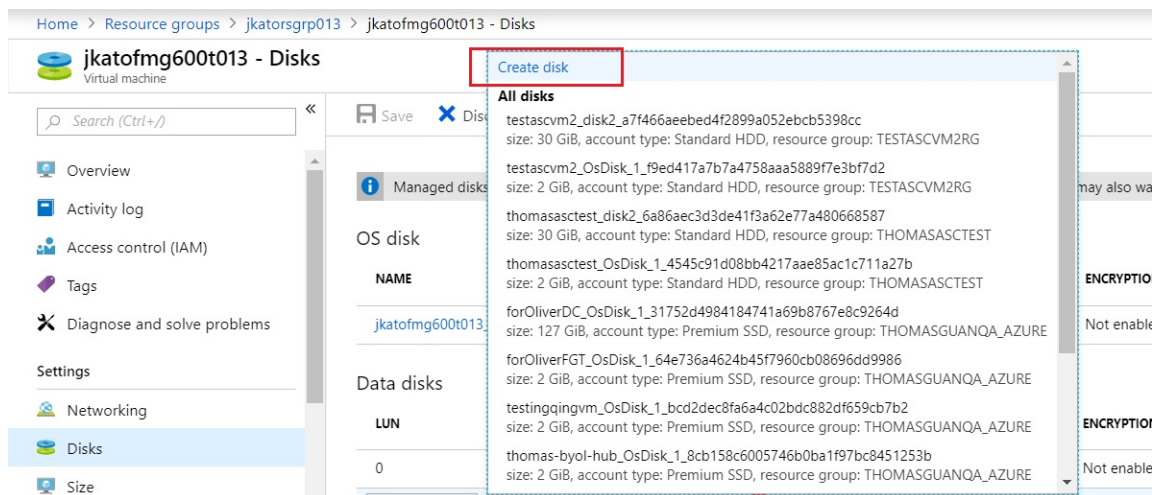
OS disk

NAME	SIZE	STORAGE ACCOUNT T...	ENCRYPTION	HOST CACHING
jkato	2 GiB	Premium SSD	Not enabled	Read/write

Data disks

LUN	NAME	SIZE	STORAGE ACCOUNT T...	ENCRYPTION	HOST CACHING
0	jkato	1023 GiB	Premium SSD	Not enabled	None

+ Add data disk



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

Create managed disk

Name

jkato-new-disk004

Resource group

jkatorsgrp013

Location

North Europe

Availability zone

None

Account type

Standard HDD

Source type

None (empty disk)

Size (GiB)

1023

ESTIMATED PERFORMANCE

IOPS limit

500

Throughput limit (MB/s)

60

Create

3. Save the disk.

Home > Resource groups > jkatofmgrp013 > jkatofmg600t013 - Disks

jkatofmg600t013 - Disks

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

OS disk

NAME	SIZE	STORAGE ACCOUNT T...	ENCRYPTION	HOST CACHING
jkatofmg600t013_OsDisk_1_db7ab532489e4e4b96858f4ef...	2 GiB	Premium SSD	Not enabled	Read/write

Data disks

LUN	NAME	SIZE	STORAGE ACCOUNT T...	ENCRYPTION	HOST CACHING
0	jkatofmg600t013_disk2_3ed974d6ff65...	1023 GiB	Premium SSD	Not enabled	None
1	jkato-new-disk004	1023 GiB	Standard HDD	Not enabled	None

4. Log into the FortiManager-VM management GUI console.

5. Go to *System Settings*. Invoke the CLI console.

System Settings

Dashboard

System Information

Host Name: jkatofmg600t013

Serial Number: FMG-VM0000000000

Platform Type: FMG-VM64-AZURE

HA Status: Standalone

System Time: Sat Oct 13 08:03:34 2018 PDT

Firmware Version: v6.0.0-build0092.180418 (GA)

System Configuration: Last Backup: N/A

Current Administrators: fortidadmin / 1 in total

Up Time: 27 minutes 17 seconds

Administrative Domain: OFF

FortiAnalyzer Features: OFF

System Resources

Average CPU Usage: 4%

Memory Usage: 17%

Disk Usage: 1%

CLI Console

Unit Operation

FORTINET

FortiManager-VM64-AZURE

Restart

Shutdown

Alert Message Console

Time	Message
Oct 13, 07:52:58	user 'root' login failed from TELNET(114.34.183.204) cause system lockout
Oct 13, 07:52:52	user 'tech' login failed from TELNET(114.34.183.204) cause system lockout
Oct 13, 07:52:47	user 'root' login failed from TELNET(114.34.183.204) cause system lockout
Oct 13, 07:52:41	user 'root' login failed from TELNET(114.34.183.204) cause system lockout
Oct 13, 07:52:36	user 'root' login failed from TELNET(114.34.183.204) cause system lockout
Oct 13, 07:52:30	user 'root' login failed from TELNET(114.34.183.204) cause system lockout
Oct 13, 07:52:24	user 'root' login failed from TELNET(114.34.183.204) cause system lockout
Oct 13, 07:52:19	user 'root' login failed from TELNET(114.34.183.204) cause system lockout
Oct 13, 07:52:13	user 'root' login failed from TELNET(114.34.183.204) cause system lockout
Oct 13, 07:52:08	user 'guest' login failed from TELNET(114.34.183.204) cause system lockout

License Information

VM License	Type	Valid
Management	Devices/VDOMs	0 of 10

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

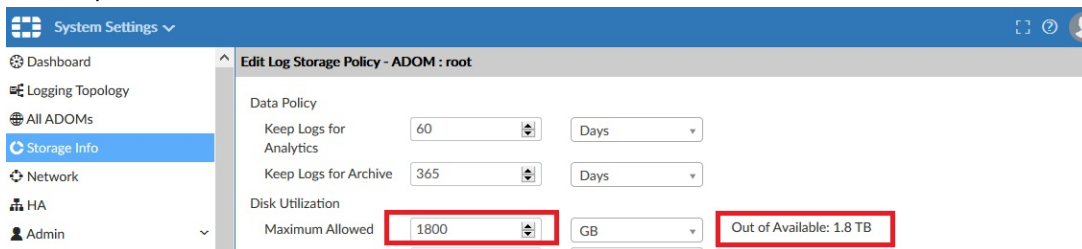
Disk1 :      Used    1072GB
Disk2 :      Used    1072GB
Disk3 : Unavailable    0GB
Disk4 : Unavailable    0GB
Disk5 : Unavailable    0GB
Disk6 : Unavailable    0GB
Disk7 : Unavailable    0GB
Disk8 : Unavailable    0GB
Disk9 : Unavailable    0GB
Disk10 : Unavailable    0GB
Disk11 : Unavailable    0GB
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 (less than or 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 17](#).
2. Create dynamic firewall address objects. See [Configuring a dynamic firewall address for a Fabric connector on page 18](#).
3. Import address names from Azure to the Fabric connector. See [Importing address names to a Fabric connector on page 18](#). 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 19](#).
5. Install the policy package to FortiOS. See [Installing a policy package on page 20](#).

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 <i>On</i> to enable the fabric connector object. Toggle <i>OFF</i> 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 <i>Fabric Connector Address</i> .
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.

Create New IPv4 Policy

Name

Incoming Interface

any

Outgoing Interface

any

Source Internet Service

OFF

Source Address

all

Source User

+

Source User Group

+

Source Device

+

Destination Internet Service

OFF

Destination Address

all

Service

ALL

Schedule

always

Action

Deny Accept IPSEC

Log Traffic

☒ Log Violation Traffic
☐ Generate Logs when Session Starts

Comments

Meta Fields >

Advanced Options >

OK

Cancel

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:

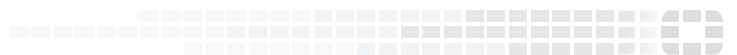
1. Ensure you are in the ADOM that contains the policy package.
2. Go to *Policy & Objects > Policy Packages*.
3. Select a policy package and from the *Install* menu or right-click menu select *Install Wizard*. The *Install Wizard* opens.
4. Follow the steps in the install wizard to install the policy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

Change log

Date	Change description
2020-02-20	Initial release.



FORTINET®



Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.