

FortiManager - GCP Cookbook

Version 6.4.0

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdocs@fortinet.com



April 09, 2020

FortiManager 6.4.0 GCP Cookbook

02-640-621429-20200409

TABLE OF CONTENTS

About FortiManager for GCP	4
Machine type support	4
Models	4
Licensing	4
Order types	5
Creating a support account	5
Registering and downloading licenses	5
Deploying FortiManager on GCP	7
Registering and downloading your license	8
Connecting to the FortiManager-VM	9
Adding a disk to the FortiManager-VM for logging	10
Security Fabric connector integration with GCP	15
Creating a GCP Fabric connector	15
Importing address names to a Fabric connectors	16
Creating IP policies	16
Installing policy packages	17
Change log	19

About FortiManager for GCP

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.

Machine type support

FortiManager for GCP can be deployed as VM instances. Supported machine types may change without notice.

Currently FortiManager supports standard machine types, high memory machine types, and high CPU machine types with minimum 2 vCPUs and 7.5 GB of RAM and maximum 96 vCPUs and 624 GB of RAM in the predefined machine type lineup. You can also customize the combination of vCPU and RAM sizes within this range. More details on predefined machine types can be found [here](#).

Latest supported machine types can be seen under machine type selection if you try to launch FortiManager from the marketplace listing or Compute Engine portal.

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 GCP. The following sections provide information on licensing FortiManager for GCP:

- [Order types on page 5](#)
- [Creating a support account on page 5](#)
- [Registering and downloading licenses on page 5](#)

Order types

FortiManager for GCP supports only Bring Your Own License (BYOL). There is no Pay As You Go/On-Demand (PAYG) subscription available yet.

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 what the platform is. You must activate a license for the first time you access the instance from the GUI or CLI before you can start using various features.

Creating a support account

FortiManager-VM for GCP 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.

Registering and downloading licenses

Licenses for the BYOL licensing model can be obtained through any Fortinet partner. If you don't have a partner, contact gcp-sales@fortinet.com for assistance in purchasing a license.

After you purchase a license or obtain an evaluation license, 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.

Registration Wizard Registering Product

1 Registration Code > 2 > 3 > 4

Specify Registration Code

Please enter your product serial number, service contract registration code or license certificate number to start the registration:

End User Type

Please specify the type of user who will be using this product:

The product will be used by a government user The product will be used by a non-government user

In this context a government end-user is any central, regional or local government department, agency, or other entity performing governmental functions; including (1) governmental research institutions, (2) governmental corporations or their separate business units which are engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List, and (3) international governmental organizations.

Next

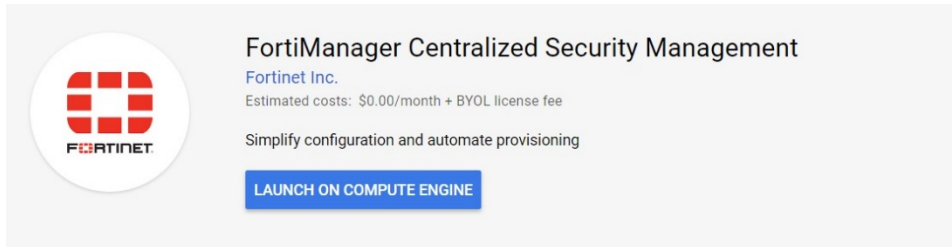
3. In the *Specify Registration Code* field, enter your license activation code, then select *Next* to continue registering the product.
4. Enter your details in the other fields as required.
5. At the end of the registration process, download the license (.lic) file to your computer. You will upload this license later to activate the FortiManager-VM.

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 on GCP

To deploy FortiManager on GCP:

1. In the Google Cloud marketplace Cloud Launcher, find *FortiManager Centralized Security Management*.



FortiManager Centralized Security Management
Fortinet Inc.
Estimated costs: \$0.00/month + BYOL license fee
Simplify configuration and automate provisioning
[LAUNCH ON COMPUTE ENGINE](#)

Runs on
Google Compute Engine

Type
Single VM
BYOL

Last updated
7/3/18, 7:26 PM

Category
Networking

Overview

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 response and remediation of risks.

- Quantifiable Security solution information produce measureable accountability, and use 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.

2. Click *LAUNCH ON COMPUTE ENGINE*.
3. Configure the variables as required:

Deployment name	Enter the name of the FortiManager-VM to appear in the Compute Engine portal.
Zone	Choose the zone to deploy the FortiManager to.
Machine type	Choose the instance type required.
Boot disk type	Choose the desired boot disk type.
Boot disk size in GB	Leave as-is at 10 GB. Note you must add additional disks for logging in later steps.
Network name	Select the network located in the selected zone.
Subnetwork name	Select the subnet where the FortiManager resides. Currently the Cloud Launcher solution supports one network interface.
Firewall	Leave all selected, or allow at least HTTPS if the strictest security is allowed in your network as the first setup. Change firewall settings as needed later.

External IP

Select *Ephemeral*. You will need to access the FortiManager management GUI via this public IP address.

Leave the other options as shown.

4. Click *Deploy*. When deployment is complete, the screen appears as below.

FortiManager Centralized Security Management
Solution provided by Fortinet Inc.

Site address	https://34.120.100.443/ L
Admin user	admin
Admin password (Temporary)	XXXXXXXXXX
Instance	jkato-fmg-564-test002
Instance zone	us-central1-f
Instance machine type	n1-standard-2

More about the software

Get started with FortiManager Centralized Security Management

Visit the site

Suggested next steps

Registering and downloading your license

Licenses for the BYOL licensing model can be obtained through any Fortinet partner. If you don't have a partner, contact gcp-sales@fortinet.com for assistance in purchasing a license.

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.

Registration Wizard Registering Product

Registration Code > 2 > 3 > 4

Specify Registration Code

Please enter your product serial number, service contract registration code or license certificate number to start the registration:

End User Type

Please specify the type of user who will be using this product:

The product will be used by a government user The product will be used by a non-government user

In this context a government end user is any central, regional or local government department, agency, or other entity performing governmental functions, including (1) governmental research institutions, (2) governmental corporations or their separate business units which are engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List, and (3) international governmental organizations.

Next

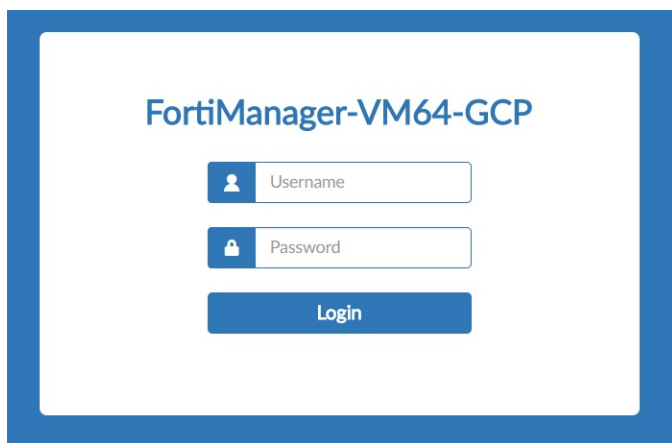
3. At the end of the registration process, download the license (.lic) file to your computer. You will upload this license later to activate the FortiManager-VM.

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.

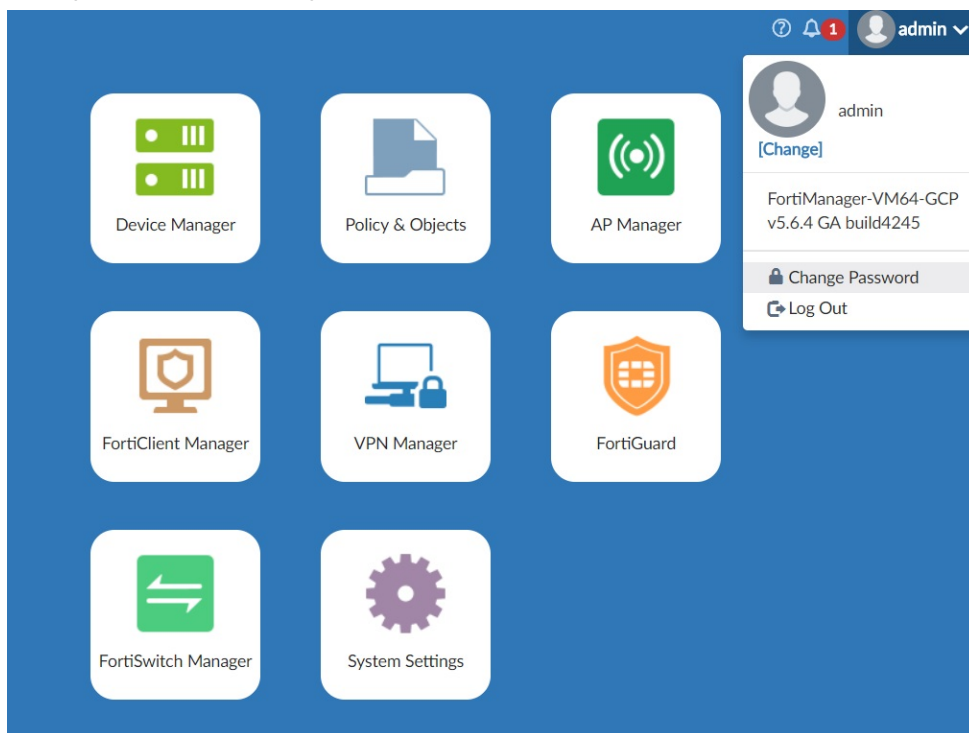
Connecting to the FortiManager-VM

To connect to the FortiManager-VM, you need your login credentials and the FortiManager-VM's public DNS address. From the previous step, there is a temporary admin password automatically generated on the Google Cloud.

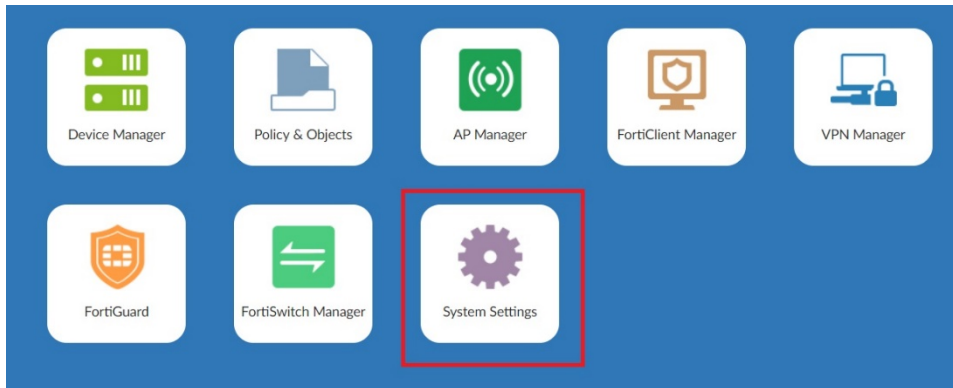
1. Connect to the FortiManager using your browser. You will see a certificate error message from your browser, which is normal because the default FortiManager certificate is self-signed and not recognized by browsers. Proceed past this error.



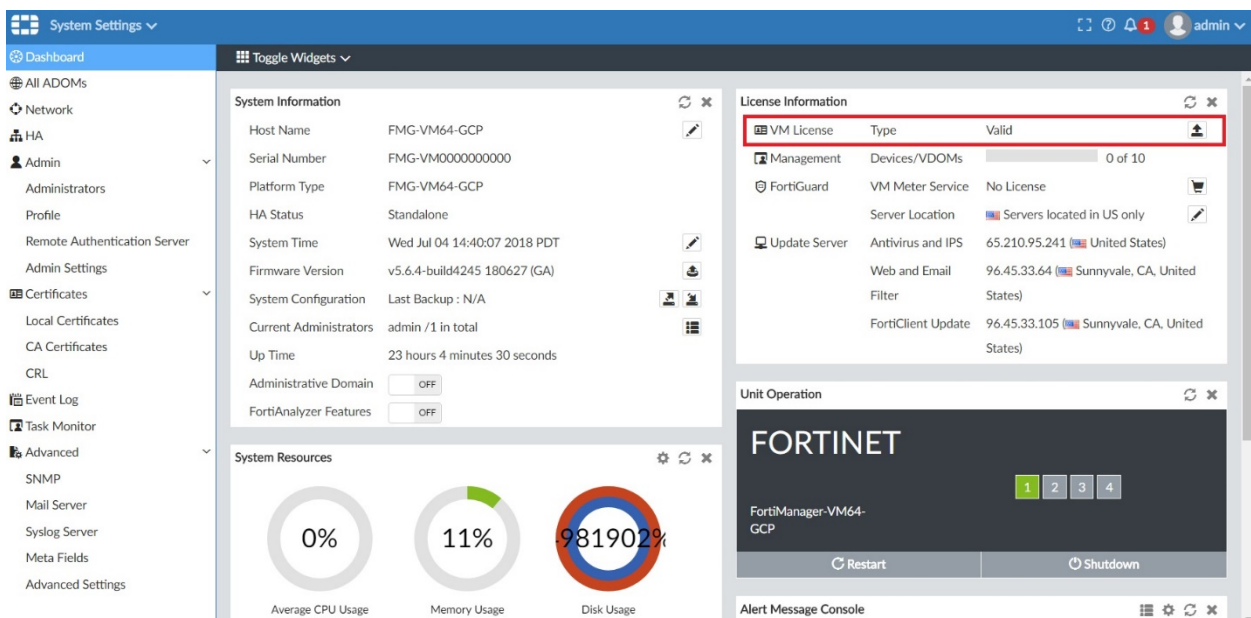
2. Log into the FortiManager-VM with the username *admin* and the supplied temporary password.
3. After you log in, click *admin* in the top-right corner to change the password. You are encouraged to change the initial password as soon as possible.



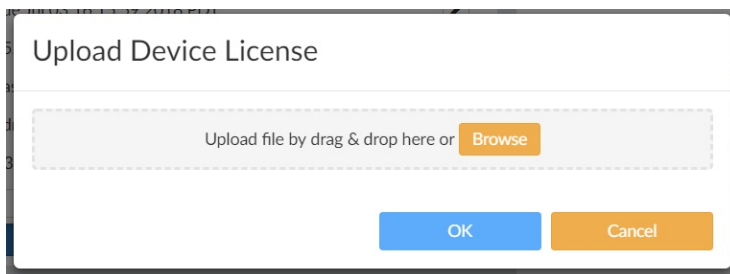
- After logging in again, go to *System Settings*.



- On the *Dashboard*, click the *Upload License* button in the *License Information* widget.



- Upload the license file (.lic) from the PC to activate the FortiManager-VM. The system automatically restarts. After it restarts, wait about 30 minutes until the license is fully registered at Fortinet, then log in again.



Adding a disk to the FortiManager-VM for logging

You are required to add another disk to store logs.

1. Log into the GCP Compute Engine.
2. Go to the *Disks* page.
3. Create a blank disk in the same zone where the FortiManager-VM resides. Disk size varies depending on the license.

Google Cloud Platform Dev Project 001

← Create a disk

Name

Description (Optional)

Region Zone

Type

Source type

Size (GB)

Estimated performance

Operation type	Read	Write
Sustained random IOPS limit	150.00	300.00
Sustained throughput limit (MB/s)	24.00	24.00

Encryption
Data is encrypted automatically. Select an encryption key management solution.

Google-managed key
No configuration required

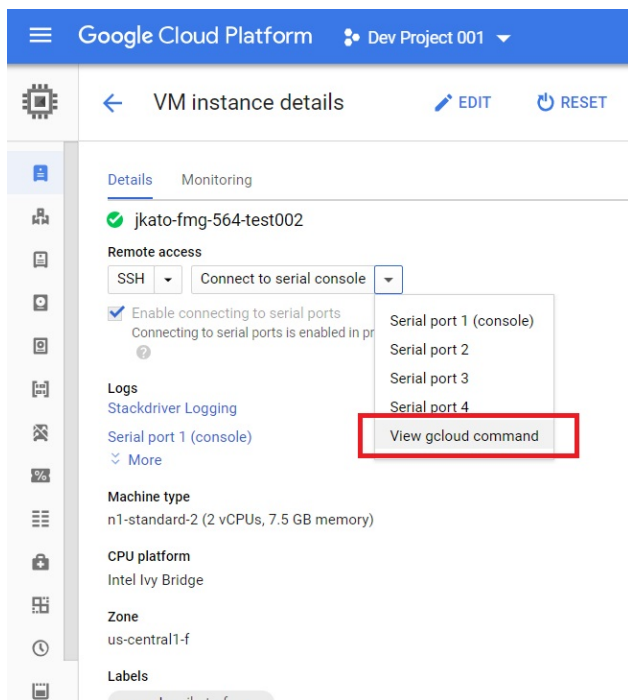
Customer-managed key
Manage via Google Cloud Key Management Service

Customer-supplied key
Manage outside of Google Cloud

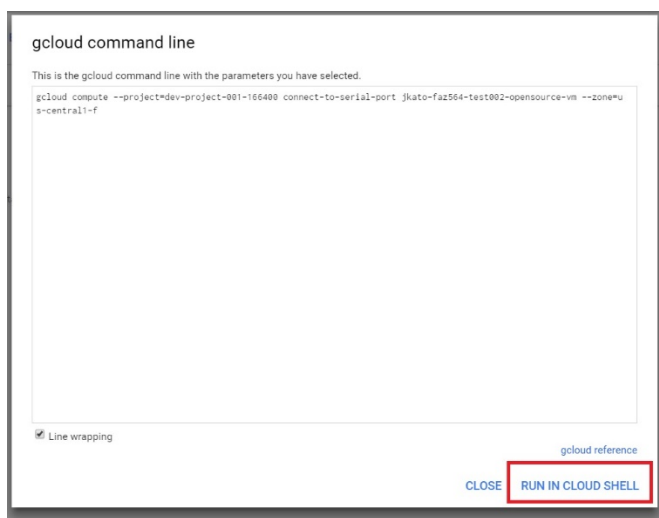
This new disk will be added once you create the new instance

Equivalent REST or command line

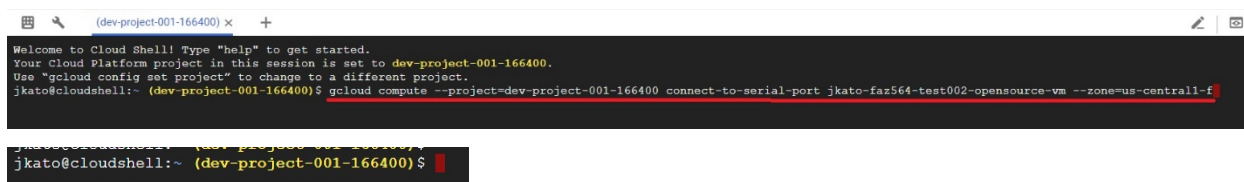
4. Click *Create*. Ensure the disk appears in the *Disks* list.
5. You must attach the disk to the FortiManager-VM instance. Navigate to the FortiManager-VM instance and start the `gcloud` command.



6. Click **RUN IN CLOUD SHELL**.



7. Delete the lines that appear in the command line.



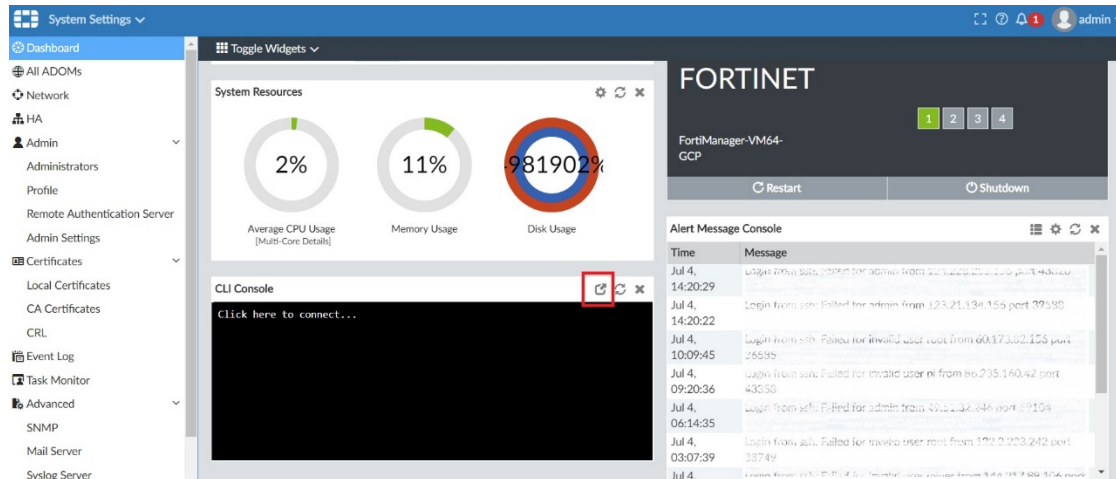
8. Enter the following command:

```
gcloud compute instances attach-disk [INSTANCE_NAME] --disk [DISK_NAME]
```

For example, the above instance has the instance name "jkato-fmg-564-test002" and disk name "jkato-fmg-564-test005". In this case, the command is as follows:

```
gcloud compute instances attach-disk jkato-fmg-564-test002 --disk jkato-fmg-564-test005
```

9. After attaching the disk, log into the FortiManager-VM management GUI.
10. Click *System Settings*. Invoke the command line by clicking the icon in the CLI Console widget.



11. In the command line window, enter `exec lvm info`. The recently added disk is shown as *Unused*.

```

FMG-VM64-GCP # exec lvm info
LVM Status: Not-Started
LVM size: 0GB

Disk1 :      Unused      209GB
Disk2 :      Unavailable  0GB
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

```

12. Enter `exec lvm start` to start LVM disk management. Enter `y` to continue. The system reboots.

```

FMG-VM64-GCP # exec lvm start
This operation will start managing disks using LVM.
All the data on the log disk will be ERASED!
Please backup your data before starting LVM.
The unit will REBOOT.
Do you want to continue? (y/n)

```

13. Rebooting causes the connection to the CLI console and the management GUI to be lost. Repeat steps 9 to 11. The disk now appears as *Used*.

```

FMG-VM64-GCP #
FMG-VM64-GCP # exec lvm info
LVM Status: OK
LVM size: 209GB

Disk1 :      Used        209GB
Disk2 :      Unavailable  0GB
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

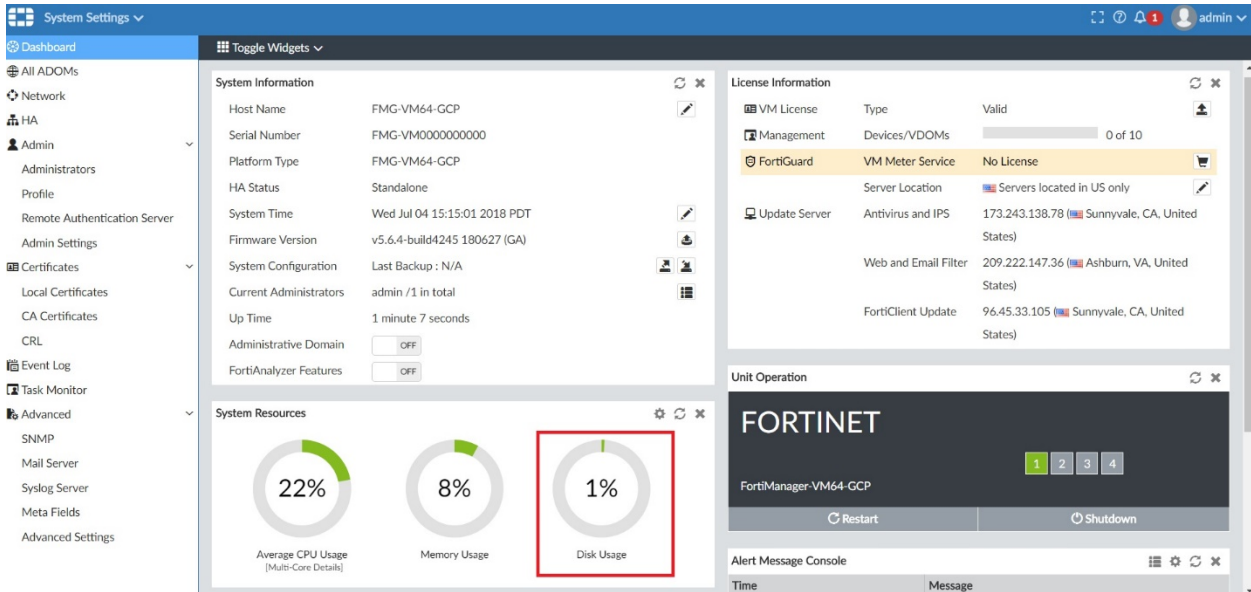
```

- Run `exec lvm extend`. This incorporates the disk into the FortiManager system.

```

FMG-VM64-GCP #
FMG-VM64-GCP # exec lvm extend
This operation will need to reboot the system.
Do you want to continue? (y/n)
    
```

- To add more disks later, follow steps 4 to 6 in [Technical Note: Extending disk space in FortiAnalyzer VM / FortiManager VM](#).
- Go to the Dashboard. You will now have sufficient disk space.



Security Fabric connector integration with GCP

You can use FortiManager to create Fabric connectors for GCP and install the Fabric connectors to FortiOS.

The Fabric connectors in FortiManager define the connector type 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 with the Fabric connector to communicate directly with GCP.

Following is an overview of creating Fabric connectors for GCP using FortiManager:

1. Create a Fabric connector object for GCP. See [Creating a GCP Fabric connector on page 15](#).
2. Import address names from GCP to the Fabric connector object. See [Importing address names to a Fabric connectors on page 16](#). FortiManager imports the address names and converts them to firewall address objects. The objects do not yet include IP addresses and display on the *Firewall Objects > Addresses* pane.
3. In the policy package where you will create the new policy, create an IPv4 policy and include the firewall address objects for GCP. See [Creating IP policies on page 16](#).
4. Install the policy package to FortiOS. See [Installing policy packages on page 17](#).
FortiOS communicates with GCP to dynamically populate the firewall address objects with IP addresses.

Creating a GCP Fabric connector

With FortiManager, you can create a Fabric connector for GCP, then import address names from GCP to automatically create dynamic objects that you can use in policies. When you install the policies to one or more FortiGates, FortiOS uses the information and the Fabric connector to communicate with GCP and dynamically populate the objects with IP addresses.

When you create a GCP Fabric connector, you specify how FortiOS can communicate with GCP through the Fabric connector. As a result, you are configuring communication and authentication information for the Fabric connector.

If you have enabled ADOMs, you can create multiple Fabric connectors per ADOM. Each Fabric connector requires a unique IP address.

Requirements:

- FortiManager with ADOM version 6.0 or later.
- FortiManager is managing the FortiGate.
- You have configured the managed FortiGate to work with GCP.

To create a GCP Fabric connector:

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

3. Under *SDN*, select *Google Cloud Platform*, and click *Next*. The *Google Cloud Platform* screen displays.
4. Configure the following options, and then click *OK*:

Name	Type a name for the fabric connector object.
Type	Displays Google Cloud Platform (GCP).
Project Name	Specify the Fabric connector project name.
Service Account Email	Specify the Fabric connector project name. service account email.
Private Key	Specify the Fabric connector private key.
Update Interval (s)	Specify the Fabric connector update interval: <ul style="list-style-type: none"> • Click <i>Use Default</i> to use the default interval. • Click <i>Specify</i> and specify the interval.
Status	Toggle <i>On</i> to enable the Fabric connector. Toggle <i>OFF</i> to disable the Fabric connector.

Importing address names to a Fabric connectors

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

To import address names for GCP:

1. Go to *Policy & Objects > Object Configurations*.
2. In the tree menu, go to *Security Fabric > Fabric Connectors*.
3. In the content pane, right-click the GCP Fabric connector, and select *Import*. The *Import SDN Connector* dialog box 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 IP policies

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	<input type="text"/>
Incoming Interface	<input type="text" value="any"/>
Outgoing Interface	<input type="text" value="any"/>
Source Internet Service	<input type="checkbox"/> OFF
Source Address	<input type="text" value="all"/>
Source User	<input type="text" value="+"/>
Source User Group	<input type="text" value="+"/>
Source Device	<input type="text" value="+"/>
Destination Internet Service	<input type="checkbox"/> OFF
Destination Address	<input type="text" value="all"/>
Service	<input type="text" value="ALL"/>
Schedule	<input type="text" value="always"/>
Action	<input checked="" type="radio"/> Deny <input type="radio"/> Accept <input type="radio"/> IPSEC
Log Traffic	<input checked="" type="checkbox"/> Log Violation Traffic
	<input type="checkbox"/> Generate Logs when Session Starts
Comments	<input type="text"/>

Meta Fields >
Advanced Options >

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 policy packages

When installing a policy package, objects that are referenced in the policy will be installed to the target device. Default or per-device mapping must exist or the installation will fail.



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:

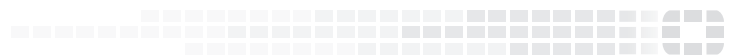
1. Ensure you are in the ADOM that contains the policy package.
2. Go to *Policy & Objects > Policy Packages*.
3. Select a policy package and from the *Install* menu or right-click menu select *Install Wizard*. The *Install Wizard* opens.
4. Follow the steps in the install wizard to install the policy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

Change log

Date	Change description
2020-04-09	Initial release.



FORTINET®



Copyright© 2020 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.