

Google Cloud Platform (GCP) Installation Guide

FortiSIEM 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 TRAINING & CERTIFICATION PROGRAM

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

FORTINET TRAINING 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



10/04/2023

FortiSIEM 6.4.0 Google Cloud Platform (GCP) Installation Guide

TABLE OF CONTENTS

Change Log	4
Fresh Installation	5
Pre-Installation Checklist	5
All-in-one Installation	6
Import FortiSIEM GCP Image into Google Cloud Image	6
Configure FortiSIEM via GUI	14
Upload the FortiSIEM License	20
Choose an Event Database	20
Cluster Installation	21
Install Supervisor	21
Install Workers	23
Register Workers	23
Install Collectors	24
Register Collectors	24
Install Log	28

Change Log

Date	Change Description
02/28/2022	Initial version of FortiSIEM - Google Cloud Platform Installation Guide (6.4.0).
05/03/2022	Added step (step 13) to Import FortiSIEM GCP Image into Google Cloud Image section.
05/23/2022	Initial version of FortiSIEM - Google Cloud Platform Installation Guide (6.4.1).
08/18/2022	Updated All-in-one Installation section.
10/20/2022	Updated Register Collectors instructions for 6.x guides.
12/06/2022	Updated Configure FortiSIEM via GUI section.
12/14/2022	Initial version of FortiSIEM - Google Cloud Platform Installation Guide (6.4.2).
05/18/2023	Updated Import FortiSIEM GCP Image into Google Cloud Image section.
09/01/2023	Initial version of FortiSIEM - Google Cloud Platform Installation Guide (6.4.3).

Fresh Installation

- [Pre-Installation Checklist](#)
- [All-in-one Installation](#)
- [Cluster Installation](#)

Pre-Installation Checklist

Before you begin, check the following:

- Ensure that your system can connect to the network. You will be asked to provide a DNS Server and a host that can be resolved by the DNS Server and responds to ping. The host can either be an internal host or a public domain host like google.com.
- Deployment type – Enterprise or Service Provider. The Service Provider deployment provides multi-tenancy.
- Whether FIPS should be enabled
- Install type:
 - All-in-one with Supervisor only, or
 - Cluster with Supervisor and Workers
- Storage type
 - Online – Local or NFS or Elasticsearch
 - Archive – NFS or HDFS
- Before beginning FortiSIEM deployment, you must configure external storage
- Determine hardware requirements:

Node	vCPU	RAM	Local Disks
Supervisor (All in one)	Minimum – 12 Recommended - 32	Minimum <ul style="list-style-type: none">• without UEBA – 24GB• with UEBA - 32GB Recommended <ul style="list-style-type: none">• without UEBA – 32GB• with UEBA - 64GB	OS – 25GB OPT – 100GB CMDB – 60GB SVN – 60GB Local Event database – based on need
Supervisor (Cluster)	Minimum – 12 Recommended - 32	Minimum <ul style="list-style-type: none">• without UEBA – 24GB• with UEBA - 32GB Recommended <ul style="list-style-type: none">• without UEBA – 32GB• with UEBA - 64GB	OS – 25GB OPT – 100GB CMDB – 60GB SVN – 60GB
Workers	Minimum – 8 Recommended - 16	Minimum – 16GB Recommended – 24GB	OS – 25GB OPT – 100GB

Node	vCPU	RAM	Local Disks
Collector	Minimum – 4	Minimum – 4GB	OS – 25GB
	Recommended – 8 (based on load)	Recommended – 8GB	OPT – 100GB

Note: compared to FortiSIEM 5.x, you need one more disk (OPT) which provides a cache for FortiSIEM.

For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when `configFSM.sh` runs.

Before proceeding to FortiSIEM deployment, you must configure the external storage.

- For NFS deployment, see *FortiSIEM - NFS Storage Guide* [here](#).
- For Elasticsearch deployment, see *FortiSIEM - Elasticsearch Storage Guide* [here](#).

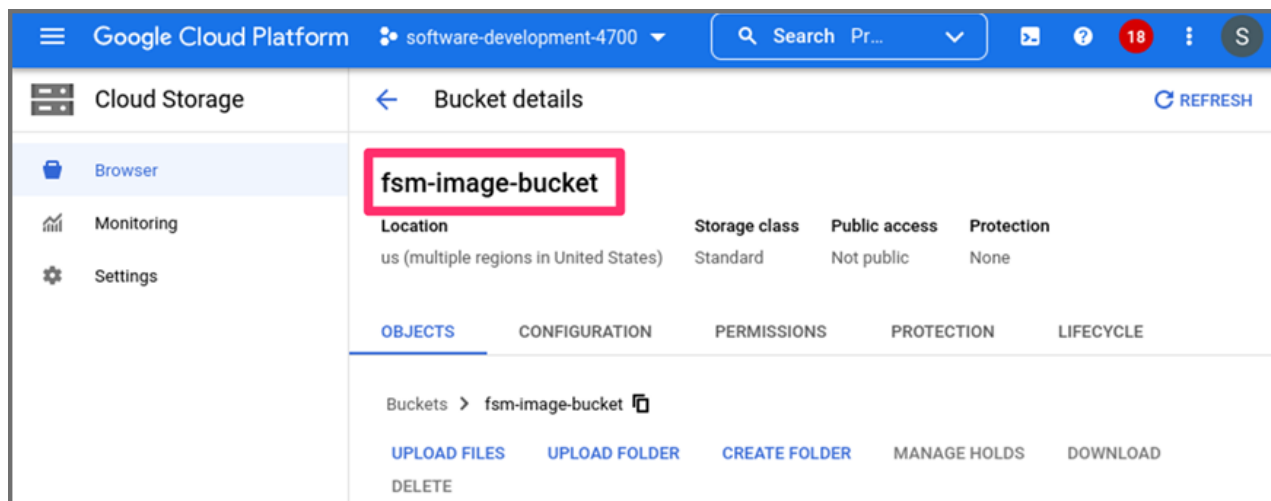
All-in-one Installation

This is the simplest installation with a single Virtual Appliance. If storage is external, then you must configure external storage before proceeding with installation.

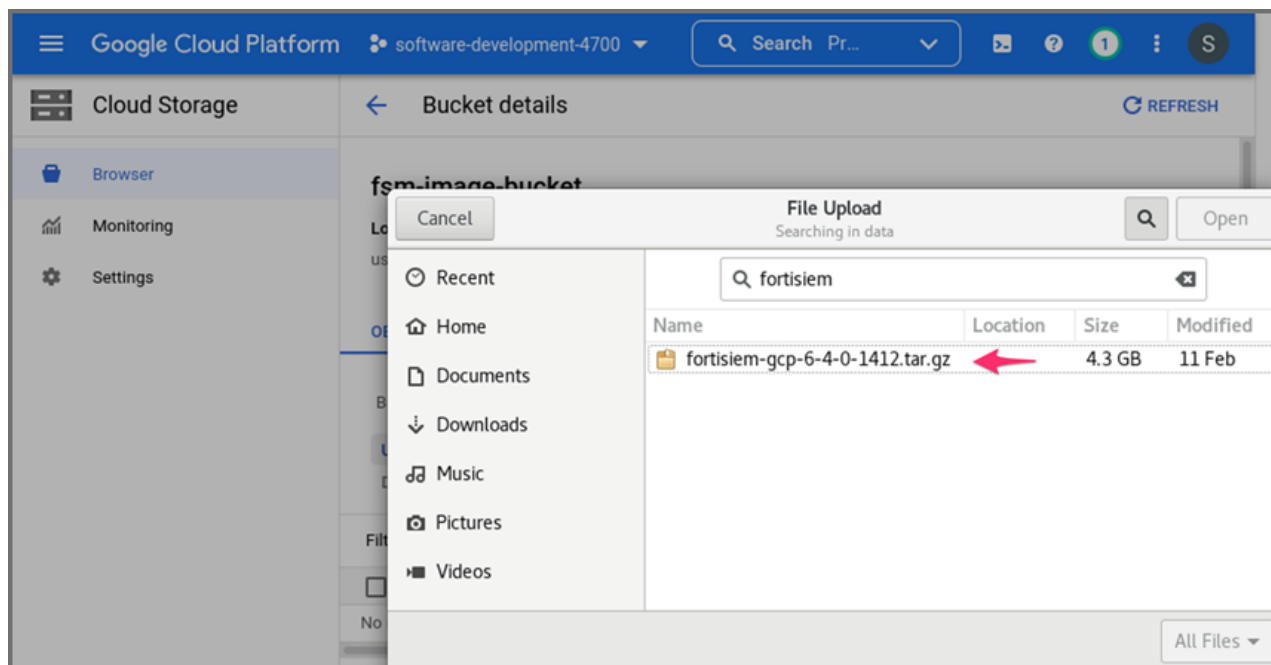
- [Import FortiSIEM GCP Image into Google Cloud Image](#)
- [Configure FortiSIEM via GUI](#)
- [Upload the FortiSIEM License](#)
- [Choose an Event Database](#)

Import FortiSIEM GCP Image into Google Cloud Image

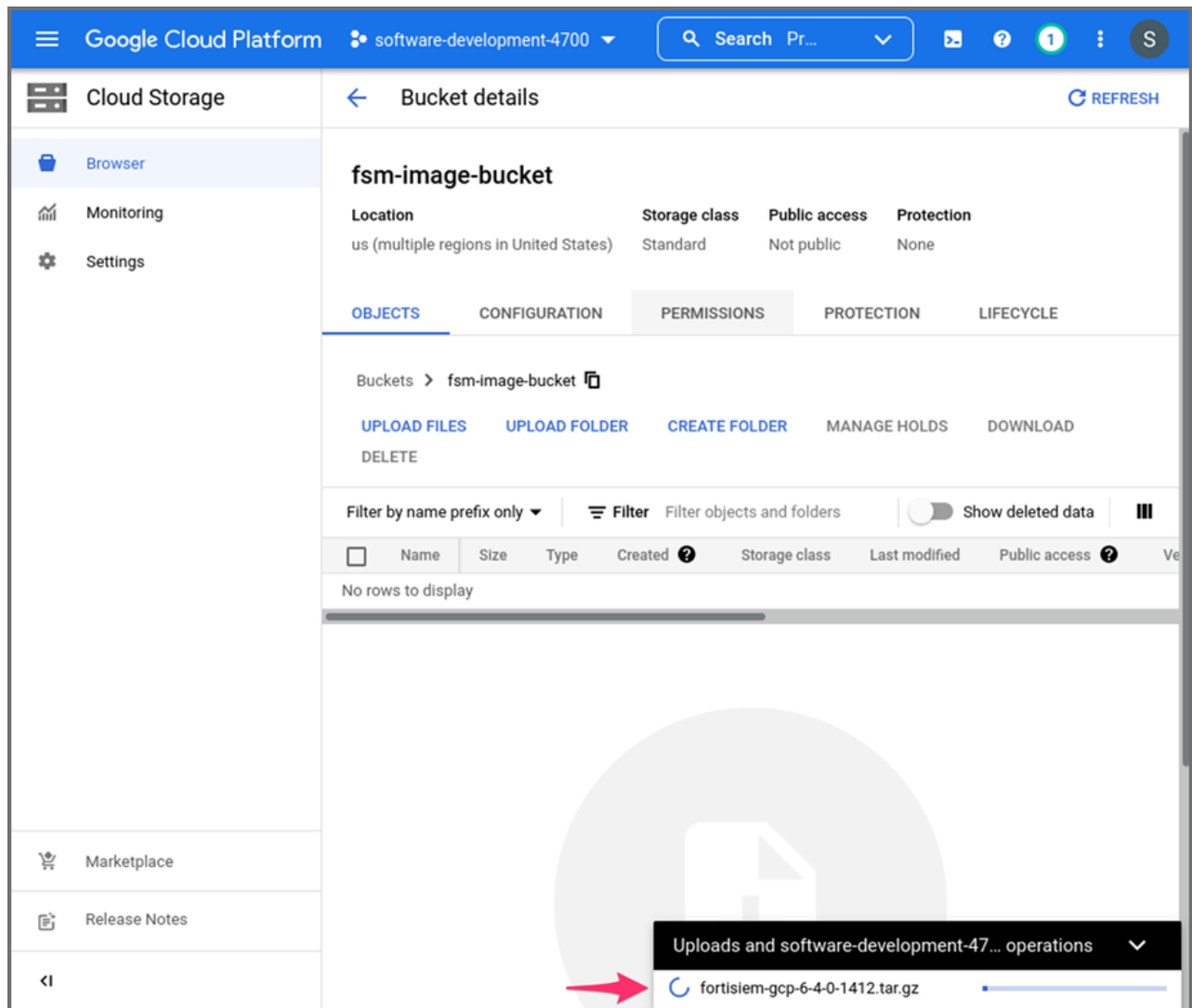
1. Go to the Fortinet Support website <https://support.fortinet.com> to download the GCP package `fortisiem-gcp-6-4-0-1412.tar.gz`. See [Downloading FortiSIEM Products](#) for more information on downloading products from the support website.
2. Identify the Google Cloud storage bucket where you plan to upload the FortiSIEM GCP image. Refer to the Google Cloud documentation on how to create a storage bucket in the appropriate location/region. For example: `fsm-image-bucket`.



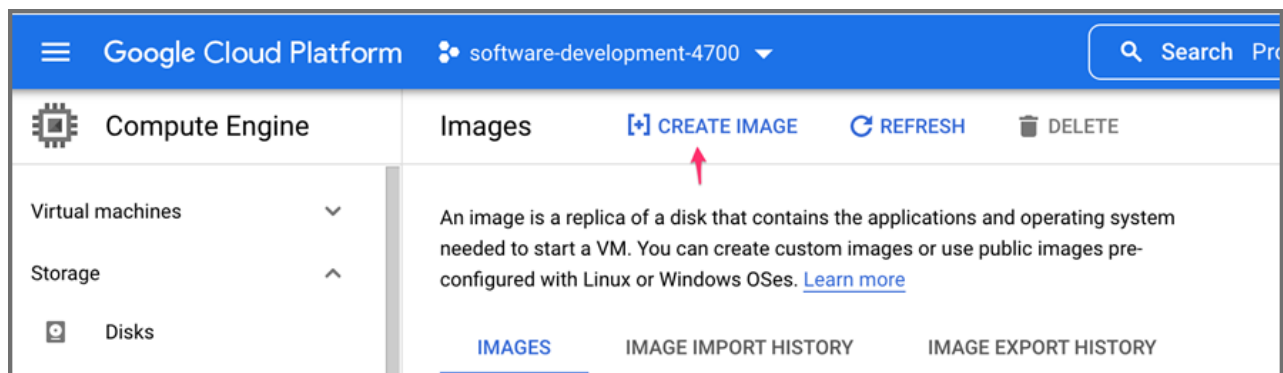
3. Click **UPLOAD FILES** and navigate to the downloaded FortiSIEM gcp image file - fortisiem-gcp-6-4-0-1412.tar.gz.



4. Wait for upload to complete by keeping track of the progress information/bar.

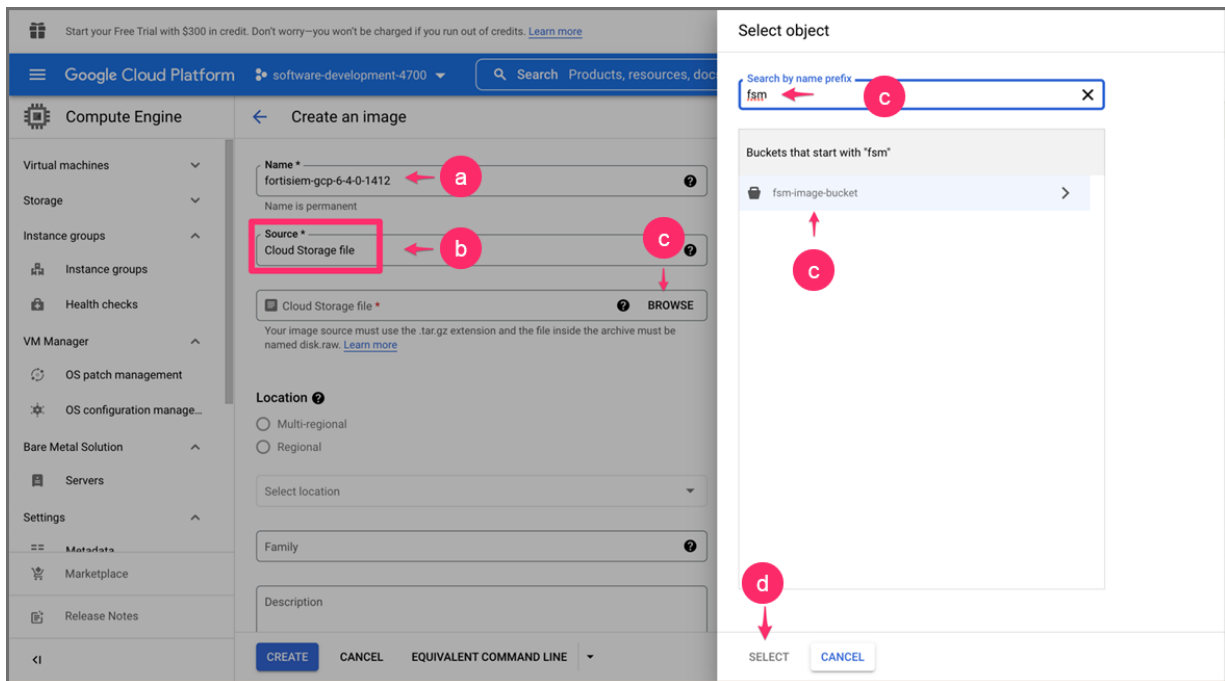


5. Once the upload is complete, navigate to Google Cloud Images service.
6. Click **CREATE IMAGE**.



7. From the Create an image section, take the following steps.
 - a. In the **Name** field, enter the name of the image as `fortisiem-gcp-6-4-0-1412` (lowercase alphanumeric with dashes allowed only).

- b. From the **Source** drop-down list, choose **Cloud Storage file**.
- c. Click **BROWSE** and browse to the storage bucket where you uploaded the image tar.gz file.
- d. Select the bucket, and then select the uploaded file `fortisiem-gcp-6-4-0-1412.tar.gz`.

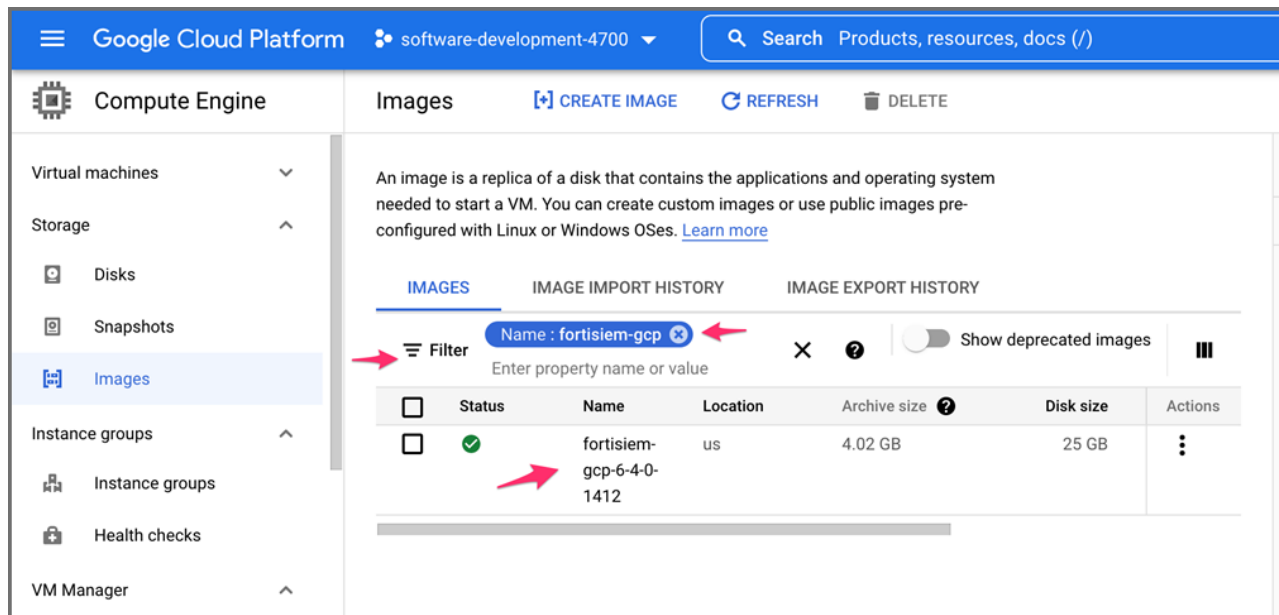


- e. For **Location**, select **Multi-regional**, and choose your location. You can leave the rest of the options as default unless you have specific requirements to change them.
- f. When done, click **CREATE**.

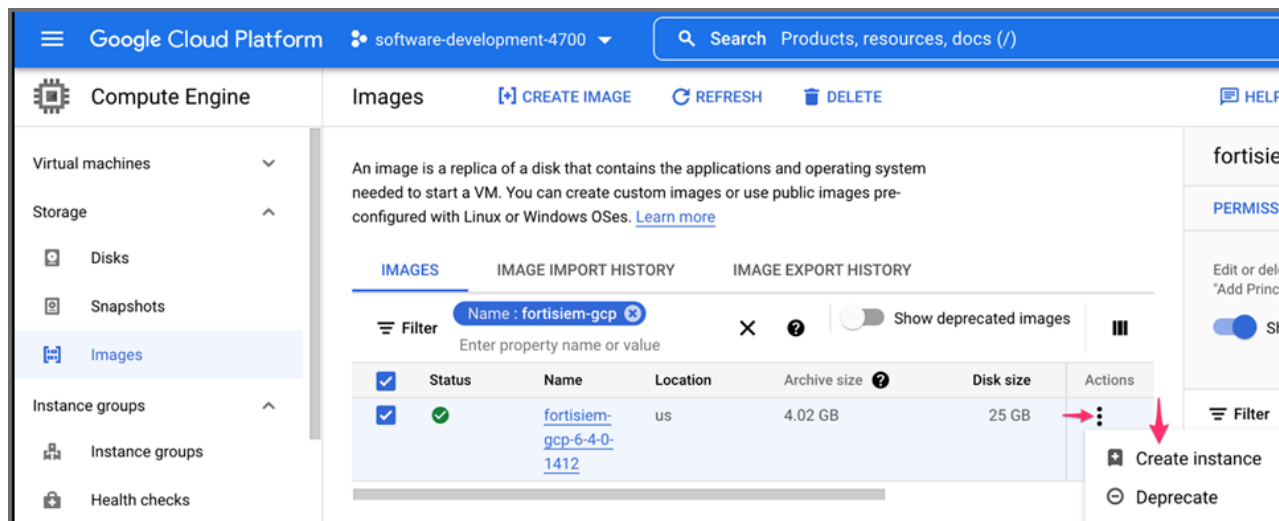
The screenshot shows the Google Cloud Platform 'Create an image' form. The left sidebar contains the 'Compute Engine' menu with sub-items: Virtual machines, Storage, Instance groups, Instance groups, Health checks, VM Manager, OS patch management, OS configuration manage..., Bare Metal Solution, Servers, Settings, Metadata, Marketplace, and Release Notes. The main form area is titled 'Create an image' and contains the following fields and options:

- Name ***: A text input field containing 'fortisiem-gcp-6-4-0-1412'. A red circle 'a' with an arrow points to the end of the text.
- Source ***: A dropdown menu with 'Cloud Storage file' selected. A red circle 'b' with an arrow points to the dropdown.
- Cloud Storage file ***: A text input field containing 'fsm-image-bucket/fortisiem-gcp-6-4-0-1412.tar.gz'. A red circle 'd' with an arrow points to the end of the text. A 'BROWSE' button is to the right.
- Location ?**: Radio buttons for 'Multi-regional' (selected) and 'Regional'. A red circle 'e' with an arrow points to the 'Multi-regional' option.
- Select location**: A dropdown menu with 'us (multiple regions in United States)' selected. A red circle 'e' with an arrow points to the dropdown.
- Family**: A text input field.
- Description**: A text area.
- CREATE**: A blue button. A red circle 'f' with an arrow points to the button.
- CANCEL**: A text button.
- EQUIVALENT COMMAND LINE**: A text button.

8. Click on **Filter**, select **Name** and type in `fortisiem-gcp` to see the image you have created. Make sure this image exists.



9. Click on the 3 dots below the **Actions** column and click **Create instance**.



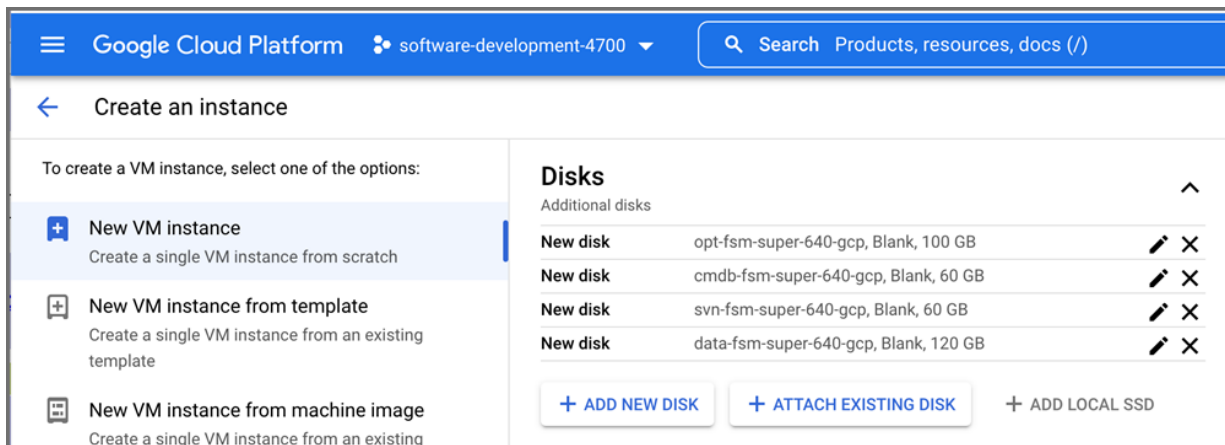
10. Choose defaults for all remaining items until the **Firewall** section. Choose **Allow HTTPS Traffic**.
11. For the **Networking** section, you can leave it as default unless you need to change some values.
12. In the **Disks** section, add an extra three disks by clicking **Add NEW DISK**. Assign to them, the disk image size of 100GB, 60GB, and 60GB respectively with **Disk source** type as blank, appropriate Disk type – Balanced, Extreme, SSD, or Standard (Refer to Google Cloud documentation for details on performance differences). Click **Save** to save the result. Make sure to name your disks properly so each disk can be found/identified easily.

Disk	Size	Disk Name
Disk 2	100GB	/opt

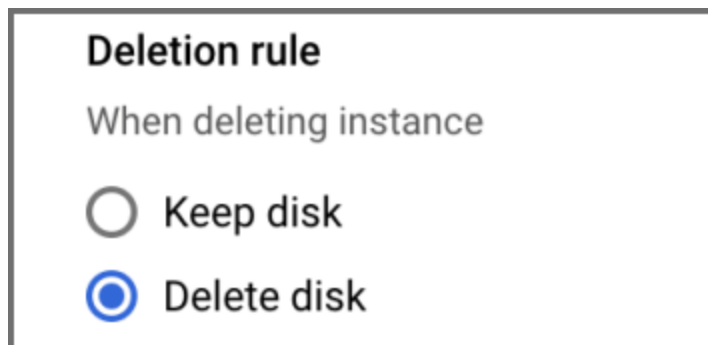
Disk	Size	Disk Name
		For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when <code>configFSM.sh</code> runs.
Disk 3	60GB	/cmdb
Disk 4	60GB	/svn
Disk 5	60GB+	/data (see the following note)

Note on Hard Disk 5

- Add a 5th disk if using local storage in an All In One deployment. Otherwise, a separate NFS share or Elasticsearch cluster must be used for event storage.
- 60GB is the minimum event DB disk size for small deployments, provision significantly more event storage for higher EPS deployments. See the [FortiSIEM Sizing Guide](#) for additional information.
- NFS or Elasticsearch event DB storage is mandatory for multi-node cluster deployments.



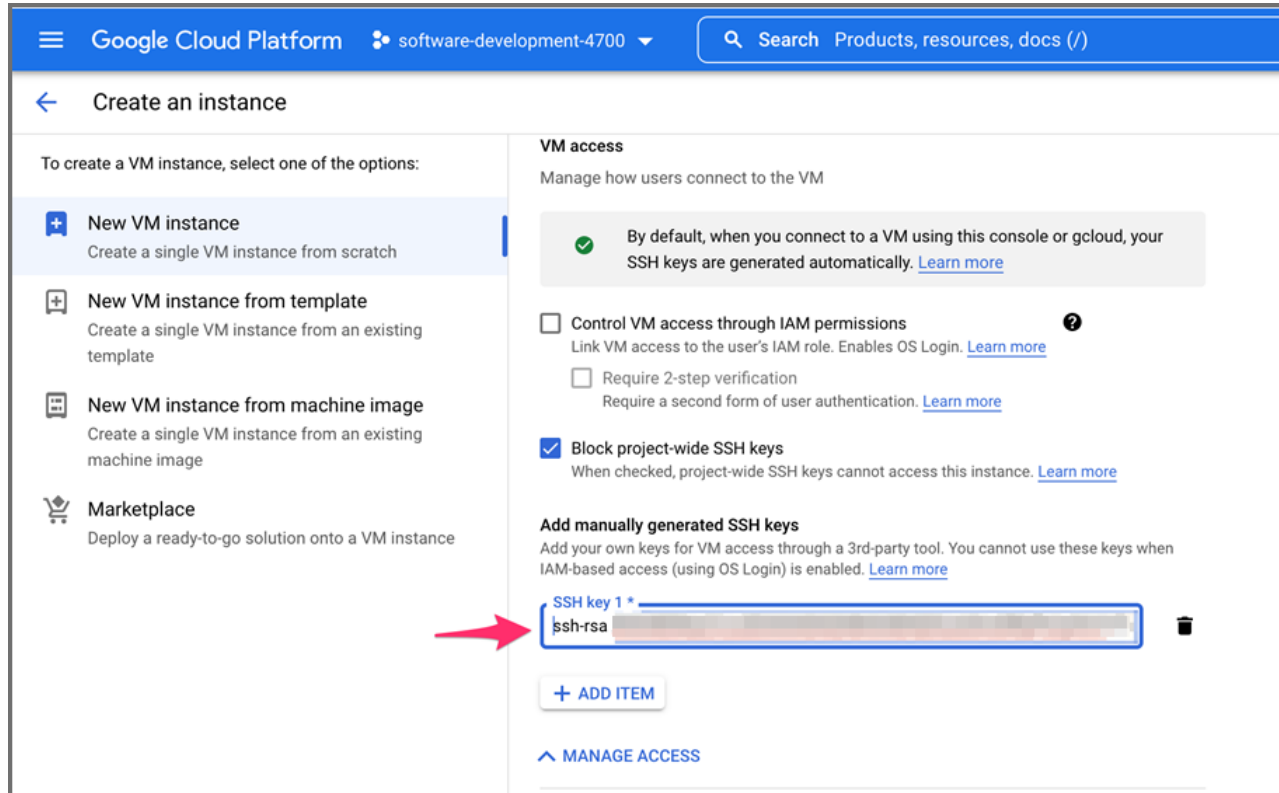
13. Under **Deletion rule**, select **Delete disk**.



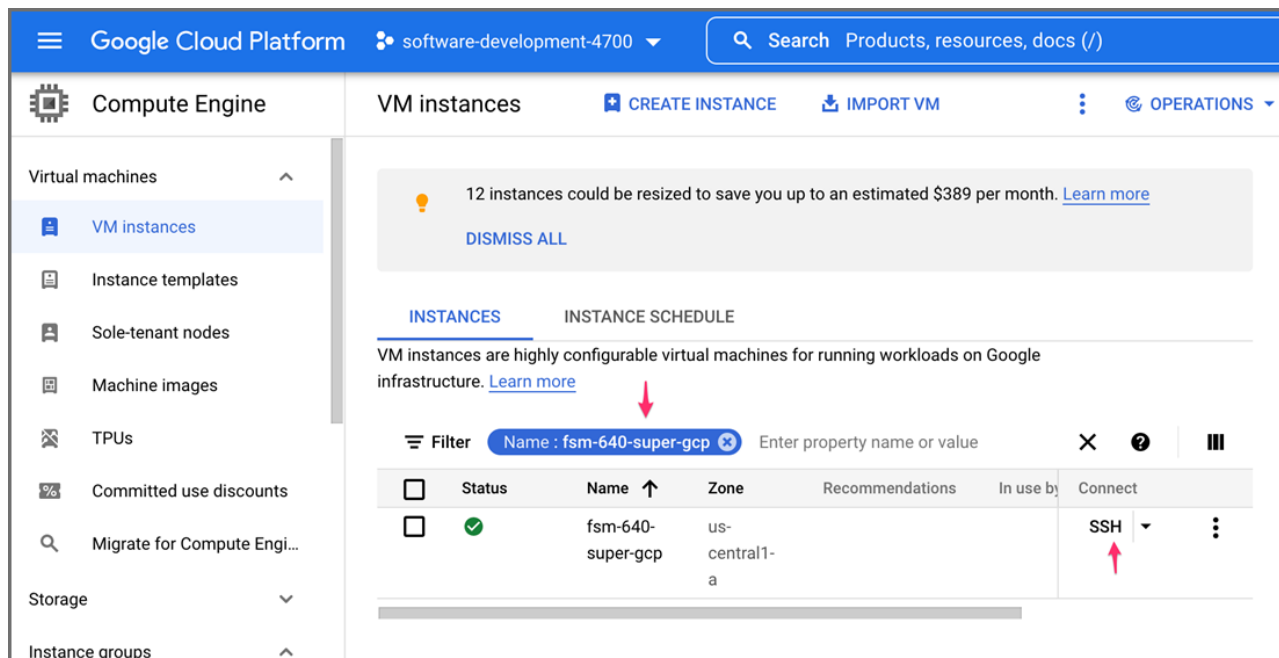
14. Under the **Security** section, select **Manage Access**. If you would like to ssh access the instance from your own terminal, then you will need to provide manually generated ssh public keys (RSA or DSA) with a user name at the end like below.

```
ssh-rsa <public-key> <username>
```

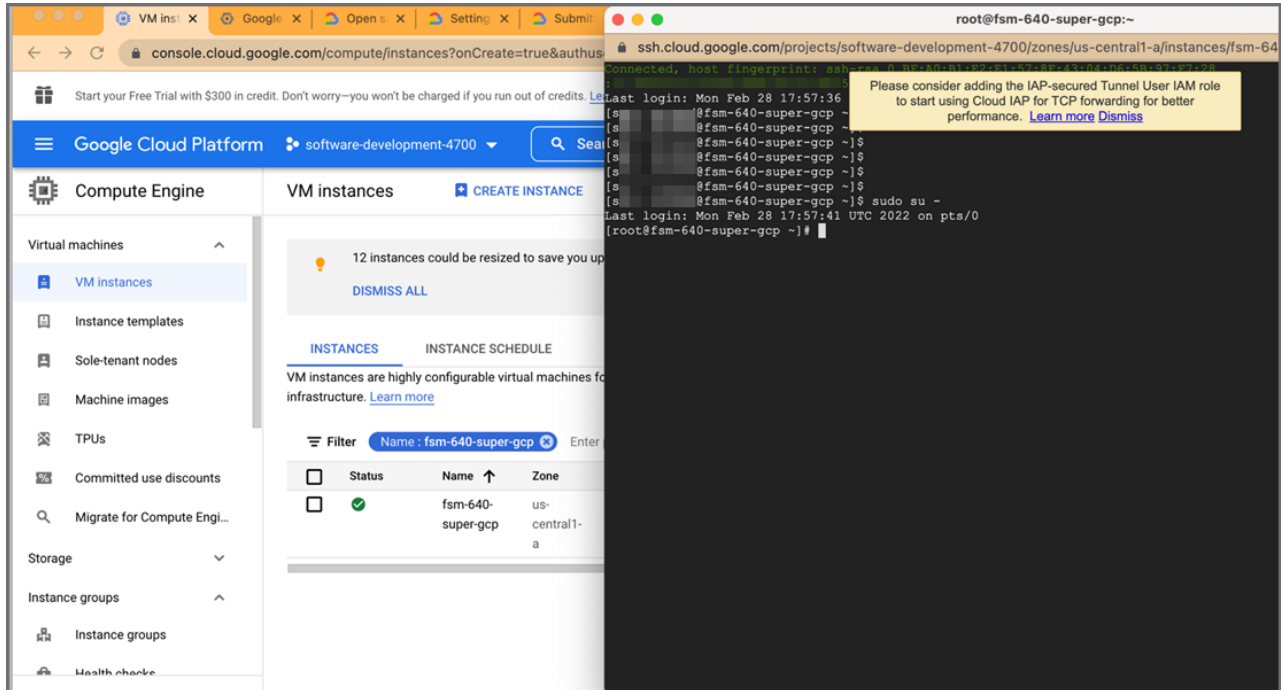
If you only wish to connect to the instance from GCP's browser based terminal, you should choose **Control VM access through IAM permissions**.



15. Leave **Management** and **Tenancy** sections with their default values unless you need to change it per your needs.
16. Click **Create**.
17. The **VM Instances** page should now appear. In the Name Filter, enter your VM instance name, for example, fsm-640-super-gcp. This will show your instance. You can click on **SSH** button.



18. When you click on **SSH**, you will be logged in on the browser based ssh console. You can now run `sudo su -` to get to root.

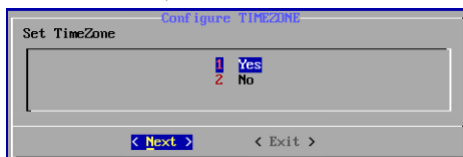


At this point, you can continue configuring FortiSIEM by using the GUI.

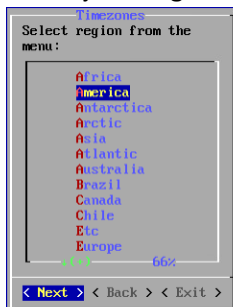
Configure FortiSIEM via GUI

Follow these steps to configure FortiSIEM by using a simple GUI.

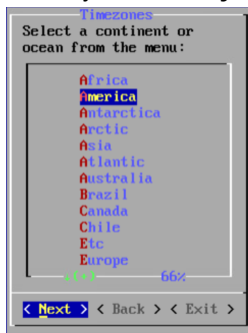
1. At the command prompt, go to `/usr/local/bin` and enter `configFSM.sh`, for example:
`configFSM.sh`
2. In VM console, select **1 Set Timezone** and then press **Next**.



3. Select your **Region**, and press **Next**.



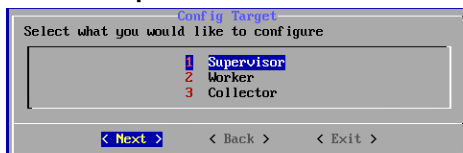
4. Select your **Country**, and press **Next**.



5. Select the **Country** and **City** for your timezone, and press **Next**.



6. Select **1 Supervisor**. Press **Next**.



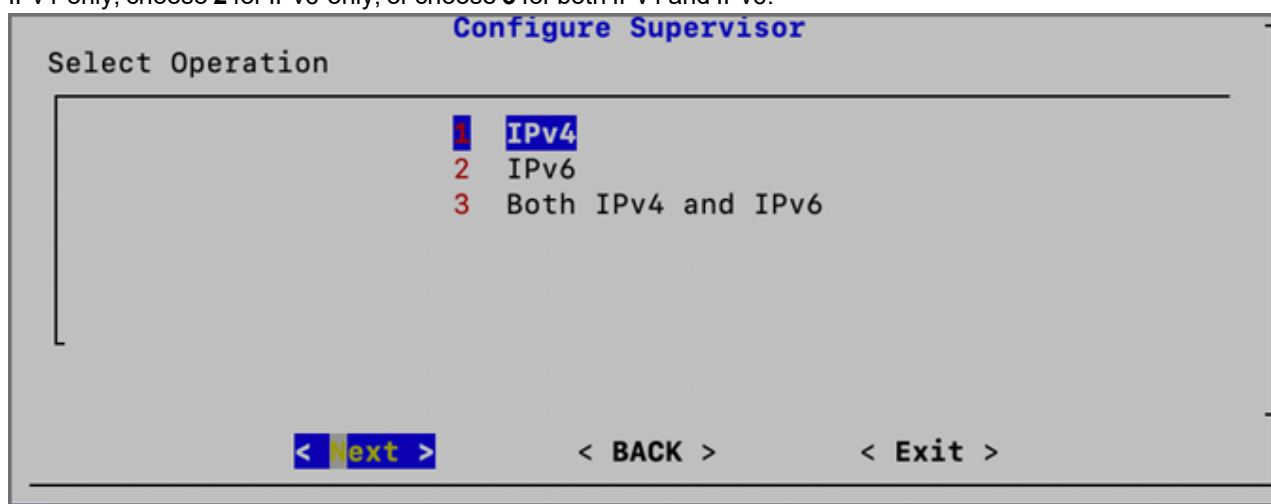
Regardless of whether you select **Supervisor**, **Worker**, or **Collector**, you will see the same series of screens.

7. If you want to enable FIPS, then choose **2**. Otherwise, choose **1**. You have the option of enabling FIPS (option **3**) or disabling FIPS (option **4**) later.

Note: After Installation, a 5th option to change your network configuration (**5 change_network_config**) is available. This allows you to change your network settings and/or host name.



8. Determine whether your network supports IPv4-only, IPv6-only, or both IPv4 and IPv6 (Dual Stack). Choose **1** for IPv4-only, choose **2** for IPv6-only, or choose **3** for both IPv4 and IPv6.



9. If you choose **1** (IPv4) or choose **3** (Both IPv4 and IPv6), and press **Next**, then you will move to step 11. If you choose **2** (IPv6), and press **Next**, then skip to step 12.
10. Configure the network by entering the following fields. Press **Next**.

Option	Description
IPv4 Address	The Supervisor's IPv4 address
NetMask	The Supervisor's subnet
Gateway	Network gateway address
DNS1, DNS2	Addresses of the DNS servers

Configure IPv4 For Supervisor

Configure IPv4 Network

IPv4 Address: 10.128.0.53
 Netmask: 255.255.255.255
 Gateway: 10.128.0.1
 DNS1: 169.254.169.254
 DNS2:

< **Next** > < **Back** > < **Exit** >

11. If you chose **1** in step 9, then you will need to skip to step 13. If you chose **2** or **3** in step 9, then you will configure the IPv6 network by entering the following fields, then press **Next**.

Option	Description
IPv6 Address	The Supervisor's IPv6 address
prefix (Netmask)	The Supervisor's IPv6 prefix
Gateway ipv6	IPv6 Network gateway address
DNS1 IPv6, DNS2 IPv6	Addresses of the IPv6 DNS server 1 and DNS server2

Configure IPv6 for Supervisor

Configure IPv6 Network

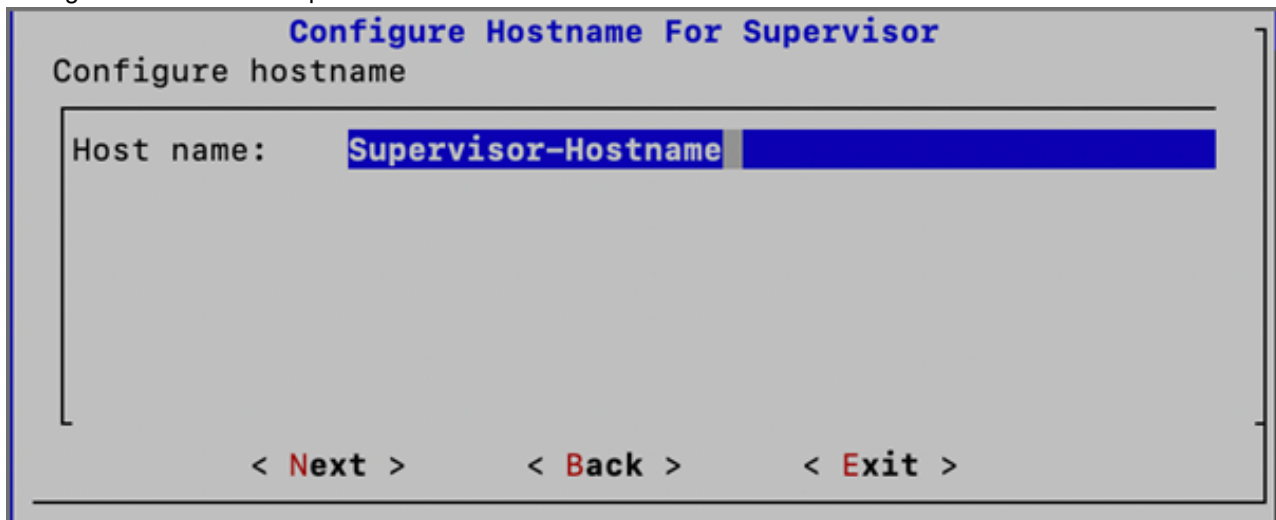
IPv6 Address: 2001:815a:1:1::ac1e:2050
 prefix (Netmask): 64
 Gateway ipv6: 2001:815a:1:1::ac1e:3020
 DNS1 IPv6: 2001:815a:1:1::ac1e:1007
 DNS2 IPv6:

< **Next** > < **Back** > < **Exit** >

Note: If you chose option **3** in step 9 for both IPv4 and IPv6, then even if you configure 2 DNS servers for IPv4 and IPv6, the system will only use the first DNS server from IPv4 and the first DNS server from the IPv6 configuration.

Note: In many dual stack networks, IPv4 DNS server(s) can resolve names to both IPv4 and IPv6. In such environments, if you do not have an IPv6 DNS server, then you can use public IPv6 DNS servers or use IPv4-mapped IPv6 address.

12. Configure Hostname for Supervisor. Press **Next**.



Configure Hostname For Supervisor

Configure hostname

Host name: **Supervisor-Hostname**

< **Next** > < **Back** > < **Exit** >

Note: FQDN is no longer needed.

13. Test network connectivity by entering a host name that can be resolved by your DNS Server (entered in the previous step) and can respond to a ping. The host can either be an internal host or a public domain host like google.com. Press **Next**.

Note: By default, "google.com" is shown for the connectivity test, but if configuring IPv6, you must enter an accessible internally approved IPv6 DNS server, for example: "ipv6-dns.fortinet.com"

Note: When configuring both IPv4 and IPv6, only testing connectivity for the IPv6 DNS is required because the IPV6 takes higher precedence. So update the host field with an approved IPv6 DNS server.



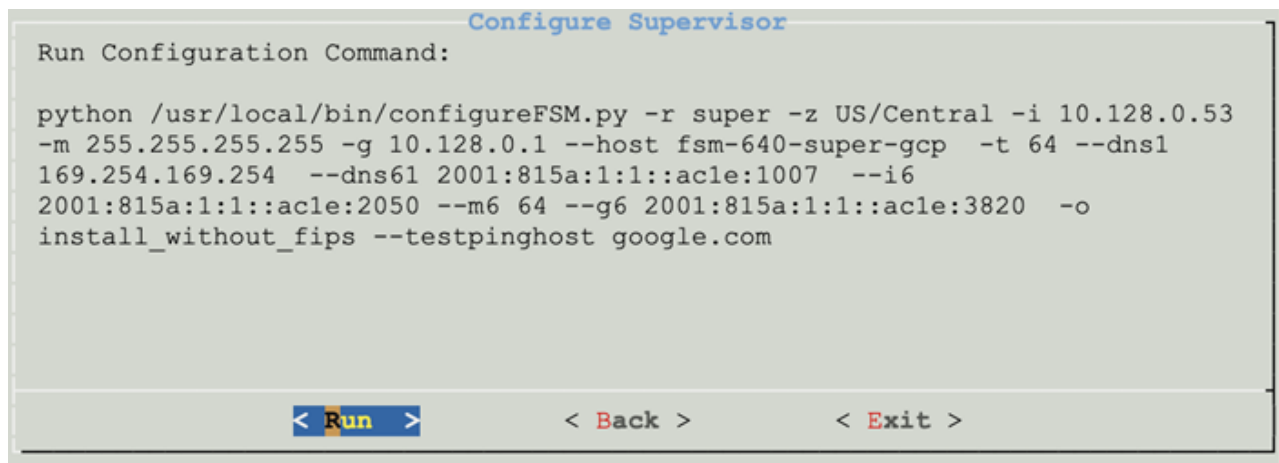
Configure Supervisor

Enter host for checking network connectivity

ipv6-dns.fortinet.com

< **Next** > < **Back** > < **Exit** >

14. The final configuration confirmation is displayed. Verify that the parameters are correct. If they are not, then press **Back** to return to previous dialog boxes to correct any errors. If everything is OK, then press **Run**.



The options are described in the following table.

Option	Description
-r	The FortiSIEM component being configured
-z	The time zone being configured
-i	IPv4-formatted address
-m	Address of the subnet mask
-g	Address of the gateway server used
--host	Host name
-f	FQDN address: fully-qualified domain name
-t	The IP type. The values can be either 4 (for ipv4) or 6 (for v6) or 64 (for both ipv4 and ipv6).
--dns1, --dns2	Addresses of the DNS servers
--i6	IPv6-formatted address
--m6	IPv6 prefix
--g6	IPv6 gateway
-o	Installation option (install_without_fips , install_with_fips , enable_fips , disable_fips , change_network_config *) *Option only available after installation.
-z	Time zone. Possible values are US/Pacific , Asia/Shanghai , Europe/London , or Africa/Tunis
--testpinghost	The URL used to test connectivity

- It will take some time for this process to finish. When it is done, proceed to [Upload the FortiSIEM License](#). If the VM fails, you can inspect the `ansible.log` file located at `/usr/local/fresh-install/logs` to try and identify the problem.

Upload the FortiSIEM License



Before proceeding, make sure that you have obtained valid FortiSIEM license from Forticare. For more information, see the [Licensing Guide](#).

You will now be asked to input a license.

1. Open a Web browser and log in to the FortiSIEM UI. Use link `https://<supervisor-ip>` to login. Please note that if you are logging into FortiSIEM with an IPv6 address, you should input `https://[IPv6 address]` on the browser tab.
2. The License Upload dialog box will open.

3. Click **Browse** and upload the license file.
Make sure that the **Hardware ID** shown in the License Upload page matches the license.
4. For **User ID** and **Password**, choose any **Full Admin** credentials.
For the first time installation, enter `admin` as the user and `admin*1` as the password. You will then be asked to create a new password for GUI access.
5. Choose **License type** as **Enterprise** or **Service Provider**.
This option is available only for a first time installation. Once the database is configured, this option will not be available.
6. Proceed to [Choose an Event Database](#).

Choose an Event Database

For a fresh installation, you will be taken to the Event Database Storage page. You will be asked to choose between **Local Disk**, **NFS** or **Elasticsearch** options. For more details, see [Configuring Storage](#).

After the License has been uploaded, and the Event Database Storage setup is configured, FortiSIEM installation is complete. If the installation is successful, the VM will reboot automatically. Otherwise, the VM will stop at the failed task.

You can inspect the `ansible.log` file located at `/usr/local/fresh-install/logs` if you encounter any issues during FortiSIEM installation.

After installation completes, ensure that the `phMonitor` is up and running, for example:

```
# phstatus
```

The response should be similar to the following.

```
Every 1.0s: /opt/phoenix/bin/phstatus.py

System uptime: 21:12:02 up 1:11, 1 user, load average: 0.16, 0.20, 0.36
Tasks: 27 total, 0 running, 26 sleeping, 0 stopped, 0 zombie
Cpu(s): 16 cores, 6.2%us, 2.1%sy, 0.0%ni, 91.4%id, 0.8%wa, 0.2%hi, 0.1%si, 0.8%st
Mem: 65782180k total, 10366836k used, 5533684k free, 4352k buffers
Swap: 2621436k total, 0k used, 2621436k free, 2465820k cached
```

PROCESS	UPTIME	CPU%	UPT_MEM	RES_MEM
phParser	41:23	0	2176m	550m
phQueryMaster	41:41	0	1820m	77m
phRuleMaster	41:41	0	1079m	594m
phRuleWorker	41:41	0	1363m	205m
phQueryWorker	41:41	0	1303m	279m
phDataManager	41:41	0	1419m	205m
phDiscover	41:41	0	513m	53m
phReportWorker	41:41	0	1433m	95m
phReportMaster	41:41	0	683m	67m
phIdentityWorker	41:41	0	1827m	50m
phIdentityMaster	41:41	0	491m	39m
phAgentManager	41:41	0	1425m	54m
phCheckpoint	42:31	0	325m	34m
phPerfMonitor	41:41	0	782m	70m
phReportLoader	41:41	0	769m	270m
phBeaconEventPackager	41:41	0	1125m	65m
phDataPurger	41:41	0	580m	58m
phEventForwarder	41:41	0	540m	46m
phMonitor	37:24	0	2080m	53m
apache	01:10:40	0	310m	16m
Node.js-charting	01:10:19	0	916m	71m
Node.js-pm2	01:10:13	0	0	26m
AppSvc	01:10:07	0	15172m	3826m
DBSvc	01:10:38	0	317m	30m
phnomaly	01:08:07	0	307m	64m
phFortiInsightAI	01:10:40	0	22432m	430m
Redis	01:10:10	0	55m	25m

Cluster Installation

For larger installations, you can choose Worker nodes, Collector nodes, and external storage (NFS or Elasticsearch).

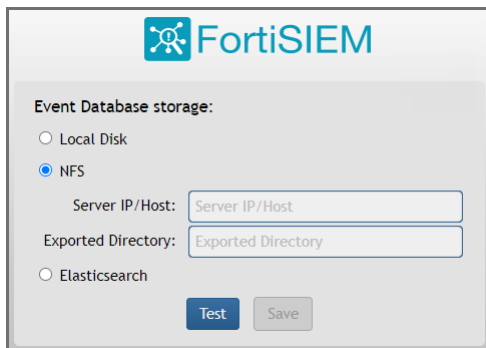
- [Install Supervisor](#)
- [Install Workers](#)
- [Register Workers](#)
- [Install Collectors](#)
- [Register Collectors](#)

Install Supervisor

Follow the steps in [All-in-one Install](#) with two differences:

- Setting up hardware - you do not need an event database.
- Setting up an Event database - Configure the cluster for either NFS or Elasticsearch.

NFS



The image shows a configuration window for FortiSIEM. At the top is the FortiSIEM logo. Below it, the section 'Event Database storage:' contains three radio button options: 'Local Disk', 'NFS' (which is selected), and 'Elasticsearch'. The 'NFS' option has two associated text input fields: 'Server IP/Host:' and 'Exported Directory:'. At the bottom of the window are two buttons: 'Test' and 'Save'.

Elasticsearch



The image shows a detailed configuration window for FortiSIEM's Elasticsearch integration. At the top is the FortiSIEM logo. Below it, the section 'Event Database storage:' contains three radio button options: 'Local Disk', 'NFS', and 'Elasticsearch' (which is selected). Under the 'Elasticsearch' option, there is a sub-section 'ES Service Type:' with three radio button options: 'Native' (selected), 'Amazon', and 'Elastic Cloud'. Below this are several input fields: 'URL:' with a text box containing 'https://' and '+'/'-' buttons; 'REST Port:' with a text box containing '443'; 'User Name:' with a text box containing '(Optional)'; 'Password:' with a text box containing '(Optional)'; and 'Confirm Password:' with an empty text box. Below these are 'Shard Allocation:' options: 'Fixed' and 'Dynamic' (selected). Then are 'Shards:' and 'Replicas:' text boxes, both containing '5' and '1' respectively. At the bottom left is a checkbox for 'Per Org Index' which is unchecked. At the bottom right are 'Test' and 'Save' buttons.

You must choose external storage listed in [Choose an Event Database](#).

Install Workers

Once the Supervisor is installed, follow the same steps in [All-in-one Install](#) to install a Worker except you need to only choose OS and OPT disks. The recommended settings for Worker node are:

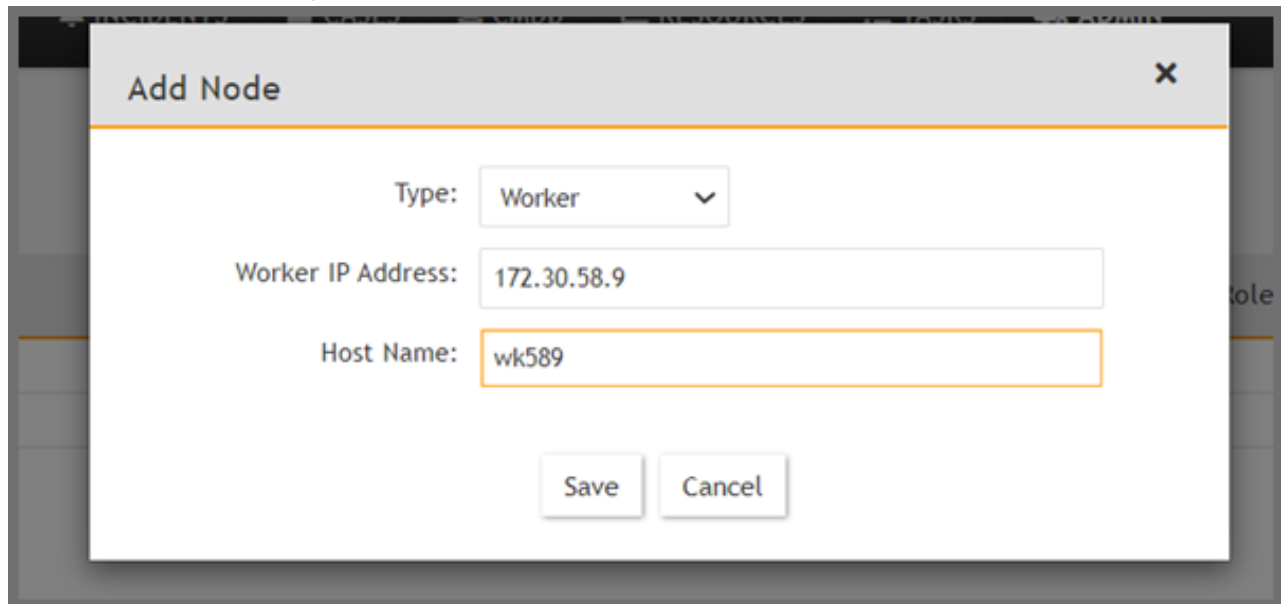
- CPU = 8
- Memory = 24 GB
- Two hard disks:
 - OS – 25GB
 - OPT – 100GB

For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when `configFSM.sh` runs.

Register Workers

Once the Worker is up and running, add the Worker to the Supervisor node.

1. Go to **ADMIN > License > Nodes**.
2. Select **Worker** from the drop-down list and enter the Worker's IP address and host name. Click **Add**.



The screenshot shows a web-based interface for adding a new node. The dialog box is titled "Add Node" and has a close button (X) in the top right corner. It contains three input fields: "Type" with a dropdown menu currently set to "Worker", "Worker IP Address" with the value "172.30.58.9", and "Host Name" with the value "wk589". At the bottom of the dialog are two buttons: "Save" and "Cancel".

3. See **ADMIN > Health > Cloud Health** to ensure that the Workers are up, healthy, and properly added to the

system.

Setup	Cloud Health	Collector Health
Device Support	Search...	Columns
Health	Name	IP Address
License	Module Role	Health
Settings	Version	Load Average
	CPU	Swap Used
	sp572.fortinet.com	172.30.57.2
	Supervisor	Normal
	6.1.0.1238	0.95,0.47,0.43
	4%	0 KB
	wk573.fortinet.com	172.30.57.3
	Worker	Normal
	6.1.0.1238	0.1,0.2,0.16
	2%	0 KB
	Search...	Columns
	Process level metrics for wk573.fortinet.com (172.30.57.3)	
	Process Name	Status
	Up Time	CPU
	Physical Memory	Virtual Memory
	SharedStore ID	SharedStore Position
	Node.js-charting	Up
	1h 3m	0%
	70 MB	916 MB
	httpd	Up
	14m 6s	0%
	16 MB	310 MB
	Redis	Up
	14m 6s	0%
	22 MB	51 MB
	Node.js-pm2	Up
	1h 3m	0%
	44 MB	899 MB
	rsyslogd	Up
	1h 3m	0%
	7 MB	189 MB
	phDataManager	Up
	14m 6s	0%
	103 MB	1229 MB
	1	126108
Copyright © 2020 Fortinet, Inc. All rights reserved.		
Organization: Super User: admin Scope: Global		
FortiSIEM		

Install Collectors

Once Supervisor and Workers are installed, follow the same steps in [All-in-one Install](#) to install a Collector except you need to only choose OS and OPT disks. The recommended settings for Collector node are:

- CPU = 4
- Memory = 8GB
- Two hard disks:
 - OS – 25GB
 - OPT – 100GB

For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when `configFSM.sh` runs.

Register Collectors

Collectors can be deployed in Enterprise or Service Provider environments.

- [Enterprise Deployments](#)
- [Service Provider Deployments](#)

Enterprise Deployments

For Enterprise deployments, follow these steps.

1. Log in to Supervisor with 'Admin' privileges.
2. Go to **ADMIN > Settings > System > Event Worker**.
 - a. Enter the IP of the Worker node. If a Supervisor node is only used, then enter the IP of the Supervisor node. Multiple IP addresses can be entered on separate lines. In this case, the Collectors will load balance the upload

of events to the listed Event Workers.

Note: Rather than using IP addresses, a DNS name is recommended. The reasoning is, should the IP addressing change, it becomes a matter of updating the DNS rather than modifying the Event Worker IP addresses in FortiSIEM.

b. Click **OK**.

3. Go to **ADMIN > Setup > Collectors** and add a Collector by entering:

a. **Name** – Collector Name

b. **Guaranteed EPS** – this is the EPS that Collector will always be able to send. It could send more if there is excess EPS available.

c. **Start Time** and **End Time** – set to **Unlimited**.

4. SSH to the Collector and run following script to register Collectors:

```
phProvisionCollector --add <user> '<password>' <Super IP or Host> <Organization>
<CollectorName>
```

The password should be enclosed in single quotes to ensure that any non-alphanumeric characters are escaped.

a. Set **user** and **password** using the admin user name and password for the Supervisor.

b. Set **Super IP or Host** as the Supervisor's IP address.

c. Set **Organization**. For Enterprise deployments, the default name is Super.

d. Set **CollectorName** from [Step 2a](#).

The Collector will reboot during the Registration.

5. Go to **ADMIN > Health > Collector Health** for the status.

Organization	Name	IP Address	Status	Health	Up Time	CPU	Memory	Allocated EPS	Incoming EPS	Version	Col
Super	CO-ORG	172.30.57.4	up	Normal	3m 4s	65%	5%	200	0	6.1.0...	100

Process Name	Status	Up Time	CPU	Physical Memory	Virtual Memory	SharedStore ID	SharedStore Position
phMonitorAgent	Up	29s	0%	575 MB	1116 MB		
phParser	Up	17s	0%	106 MB	1190 MB	99	0
phPerfMonitor	Up	17s	0%	79 MB	766 MB		
phEventForwarder	Up	17s	0%	48 MB	547 MB		
phDiscover	Up	17s	0%	53 MB	513 MB		

Service Provider Deployments

For Service Provider deployments, follow these steps.

1. Log in to Supervisor with 'Admin' privileges.

2. Go to **ADMIN > Settings > System > Event Worker**.

a. Enter the IP of the Worker node. If a Supervisor node is only used, then enter the IP of the Supervisor node. Multiple IP addresses can be entered on separate lines. In this case, the Collectors will load balance the upload of events to the listed Event Workers.

Note: Rather than using IP addresses, a DNS name is recommended. The reasoning is, should the IP addressing change, it becomes a matter of updating the DNS rather than modifying the Event Worker IP addresses in FortiSIEM.

- b. Click **OK**.

3. Go to **ADMIN > Setup > Organizations** and click **New** to add an Organization.

4. Enter the **Organization Name**, **Admin User**, **Admin Password**, and **Admin Email**.

5. Under **Collectors**, click **New**.

6. Enter the **Collector Name**, **Guaranteed EPS**, **Start Time**, and **End Time**.

The last two values could be set as **Unlimited**. **Guaranteed EPS** is the EPS that the Collector will always be able to send. It could send more if there is excess EPS available.

7. SSH to the Collector and run following script to register Collectors:

```
phProvisionCollector --add <user> '<password>' <Super IP or Host> <Organization>
<CollectorName>
```

The password should be enclosed in single quotes to ensure that any non-alphanumeric characters are escaped.

- a. Set `user` and `password` using the admin user name and password for the Organization that the Collector is going to be registered to.
- b. Set `Super IP` or `Host` as the Supervisor's IP address.
- c. Set `Organization` as the name of an organization created on the Supervisor.
- d. Set `CollectorName` from [Step 6](#).

```

root@co574 ~]# phProvisionCollector
Usage: phProvisionCollector --add <Organization-user-name> <Organization-user-password> <Supervisor-IP> <Organization-name> <Collector-name>
root@co574 ~]# phProvisionCollector --add admin admin=11 172.30.57.2 ORG CO-ORG
Continuing to provision the Collector
This collector is registered successfully. Normal Exit and restart of phMonitor after collector license registration.
root@co574 ~]# _

```

The Collector will reboot during the Registration.

8. Go to **ADMIN > Health > Collector Health** and check the status.

The screenshot displays the FortiSIEM interface with the 'Collector Health' tab selected. The left sidebar shows navigation options: Setup, Device Support, Health (selected), License, and Settings. The main content area is divided into two sections. The top section, 'Cloud Health', shows a table with one entry for the 'Super' organization. The bottom section, 'Collector Health', shows a table of running processes.

Organization	Name	IP Address	Status	Health	Up Time	CPU	Memory	Allocated EPS	Incoming EPS	Version	Col
Super	CO-ORG	172.30.57.4	up	Normal	3m 4s	65%	5%	200	0	6.1.0...	100

Process Name	Status	Up Time	CPU	Physical Memory	Virtual Memory	SharedStore ID	SharedStore Position
phMonitorAgent	Up	29s	0%	575 MB	1116 MB		
phParser	Up	17s	0%	106 MB	1190 MB	99	0
phPerfMonitor	Up	17s	0%	79 MB	766 MB		
phEventForwarder	Up	17s	0%	48 MB	547 MB		
phDiscover	Up	17s	0%	53 MB	513 MB		

Install Log

The install ansible log file is located here: `/usr/local/fresh-install/logs/ansible.log`.

Errors can be found at the end of the file.



www.fortinet.com

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's 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. 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.