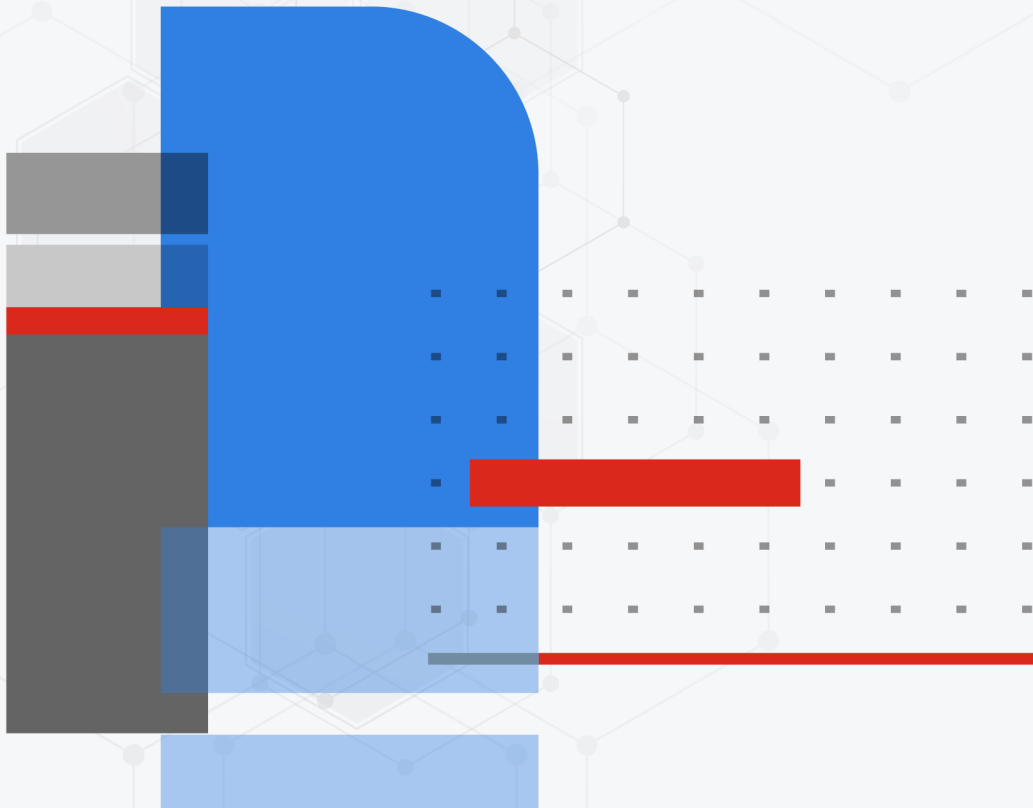




Google Cloud Platform (GCP) Installation Guide

FortiSIEM 6.7.1



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



10/03/2023

FortiSIEM 6.7.1 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	7
Configure FortiSIEM	14
Upload the FortiSIEM License	20
Configure an Event Database	21
Final Check	21
Cluster Installation	22
Install Supervisor	23
Install Workers	25
Register Workers	26
Create ClickHouse Topology (Optional)	28
Install Collectors	28
Register Collectors	28
Install Manager	31
Register Instances to Manager	31
Install Log	34

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.
05/09/2022	Release of FortiSIEM - Google Cloud Platform Installation Guide for 6.5.0.
07/26/2022	Release of FortiSIEM - Google Cloud Platform Installation Guide for 6.6.0.
08/18/2022	Updated All-in-one Installation section.
09/12/2022	Release of FortiSIEM - Google Cloud Platform Installation Guide for 6.5.1.
09/14/2022	Release of FortiSIEM - Google Cloud Platform Installation Guide for 6.6.1.
09/19/2022	Release of FortiSIEM - Google Cloud Platform Installation Guide for 6.6.2.
10/20/2022	Updated Register Collectors instructions for 6.x guides.
12/06/2022	Updated Configure FortiSIEM via GUI section.
01/03/2023	Release of FortiSIEM - Google Cloud Platform Installation Guide for 6.7.0.
02/13/2023	Release of FortiSIEM - Google Cloud Platform Installation Guide for 6.7.1.
02/21/2023	Pre-Installation Checklist, Choose an Event Database, Install Supervisor, Install Workers and Register Workers sections updated for 6.7.x Guides. Added Create ClickHouse Topology (Optional) and Final Check sections to 6.7.x Guides.
03/07/2023	Release of FortiSIEM - Google Cloud Platform Installation Guide for 6.7.2.
03/28/2023	Release of FortiSIEM - Google Cloud Platform Installation Guide for 6.7.3.
04/11/2023	Release of FortiSIEM - Google Cloud Platform Installation Guide for 6.7.4.
05/18/2023	Updated Import FortiSIEM GCP Image into Google Cloud Image section.
05/22/2023	Release of FortiSIEM - Google Cloud Platform Installation Guide for 6.7.5.
06/16/2023	Release of FortiSIEM - Google Cloud Platform Installation Guide for 6.7.6.
07/13/2023	Release of FortiSIEM - Google Cloud Platform Installation Guide for 6.7.7.
09/12/2023	Release of FortiSIEM - Google Cloud Platform Installation Guide for 6.7.8.

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.
- Choose deployment type – Enterprise or Service Provider. The Service Provider deployment provides multi-tenancy.
- Determine whether FIPS should be enabled
- Choose install type:
 - All-in-one with FortiSIEM Manager
 - Cluster with Manager, Supervisor and Workers
 - All-in-one with Supervisor only, or
 - Cluster with Supervisor and Workers
- Choose storage type
 - Online - There are 4 choices
 - ClickHouse - Recommended for most deployments. Please see [ClickHouse Reference Architecture](#) for more information.
 - EventDB on local disk
 - EventDB on NFS
 - Elasticsearch
 - Archive – There are 2 choices
 - EventDB on NFS
 - HDFS
- Determine hardware requirements:

Node	vCPU	RAM	Local Disks
Manager	Minimum – 16 Recommended - 32	Minimum <ul style="list-style-type: none">• 24GB Recommended <ul style="list-style-type: none">• 32GB	OS – 25GB OPT – 100GB CMDB – 60GB SVN – 60GB
Supervisor (All in one)	Minimum – 12 Recommended - 32	Minimum <ul style="list-style-type: none">• without UEBA – 24GB	OS – 25GB OPT – 100GB

Node	vCPU	RAM	Local Disks
		<ul style="list-style-type: none"> with UEBA - 32GB Recommended <ul style="list-style-type: none"> without UEBA – 32GB with UEBA - 64GB 	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
Collector	Minimum – 4 Recommended – 8 (based on load)	Minimum – 4GB Recommended – 8GB	OS – 25GB OPT – 100GB

- If your Online event database is external (e.g. EventDB on NFS or Elasticsearch), then you must configure external storage before proceeding to FortiSIEM deployment.
 - For NFS deployment, see [here](#).
 - For Elasticsearch deployment, see [here](#).
- If your Online event database is internal, that is, inside Supervisor or Worker nodes, then you need to determine the size of the disks based on your EPS and event retention needs.
 - For EventDB on local disk, see [here](#).
 - For ClickHouse, see [here](#).
- 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.

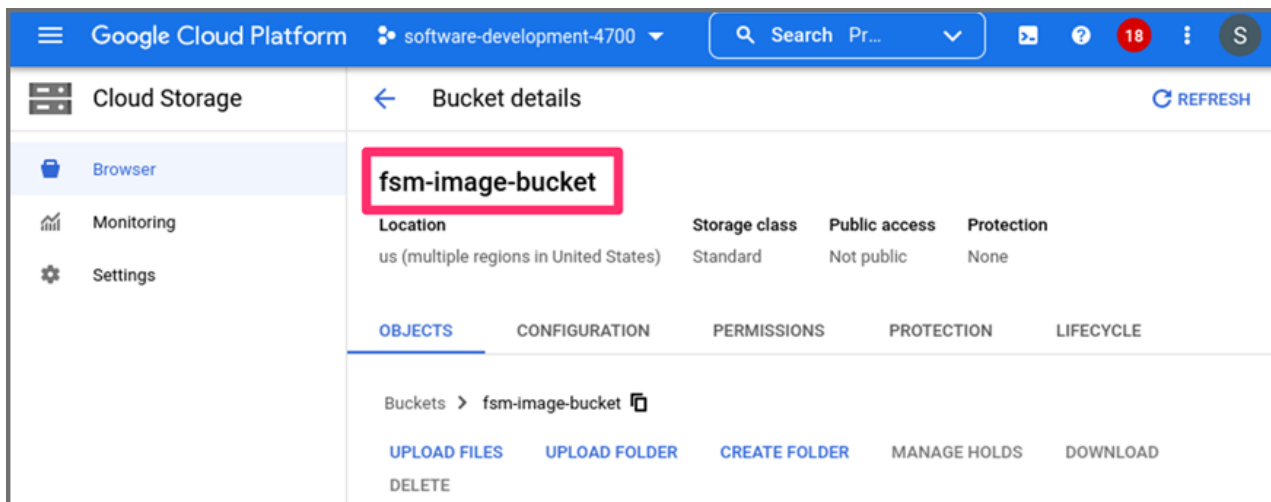
All-in-one Installation

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

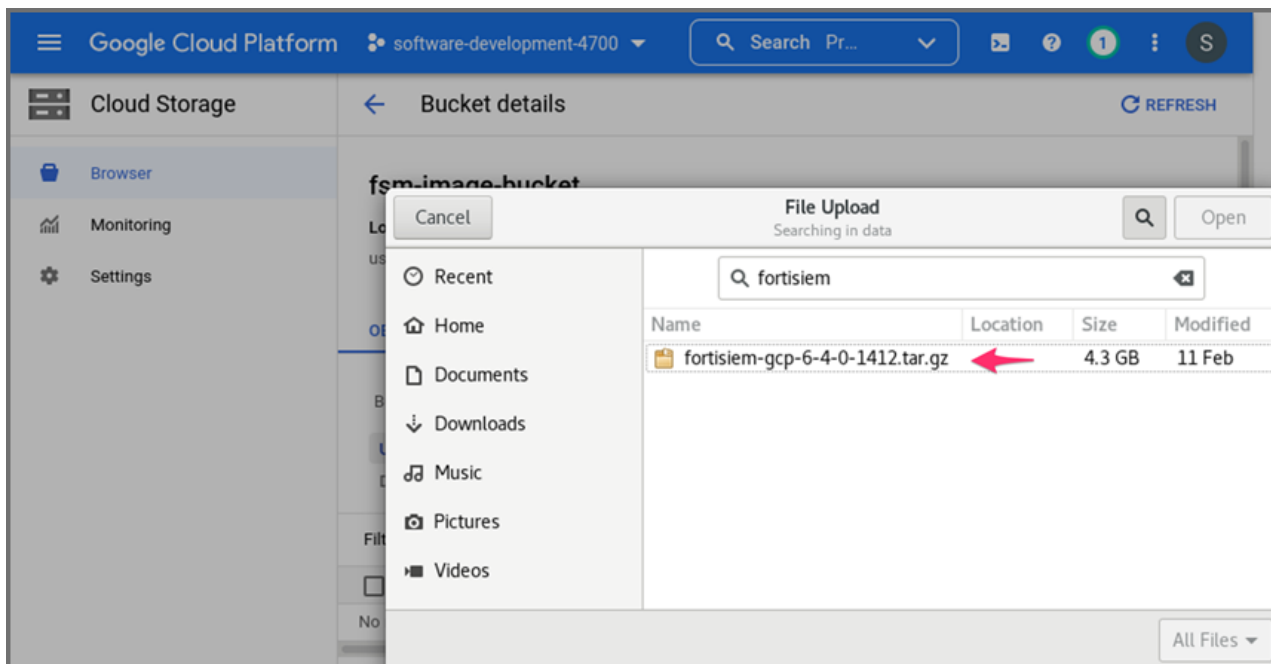
- [Import FortiSIEM GCP Image into Google Cloud Image](#)
- [Configure FortiSIEM](#)
- [Upload the FortiSIEM License](#)
- [Configure an Event Database](#)
- [Final Check](#)

Import FortiSIEM GCP Image into Google Cloud Image

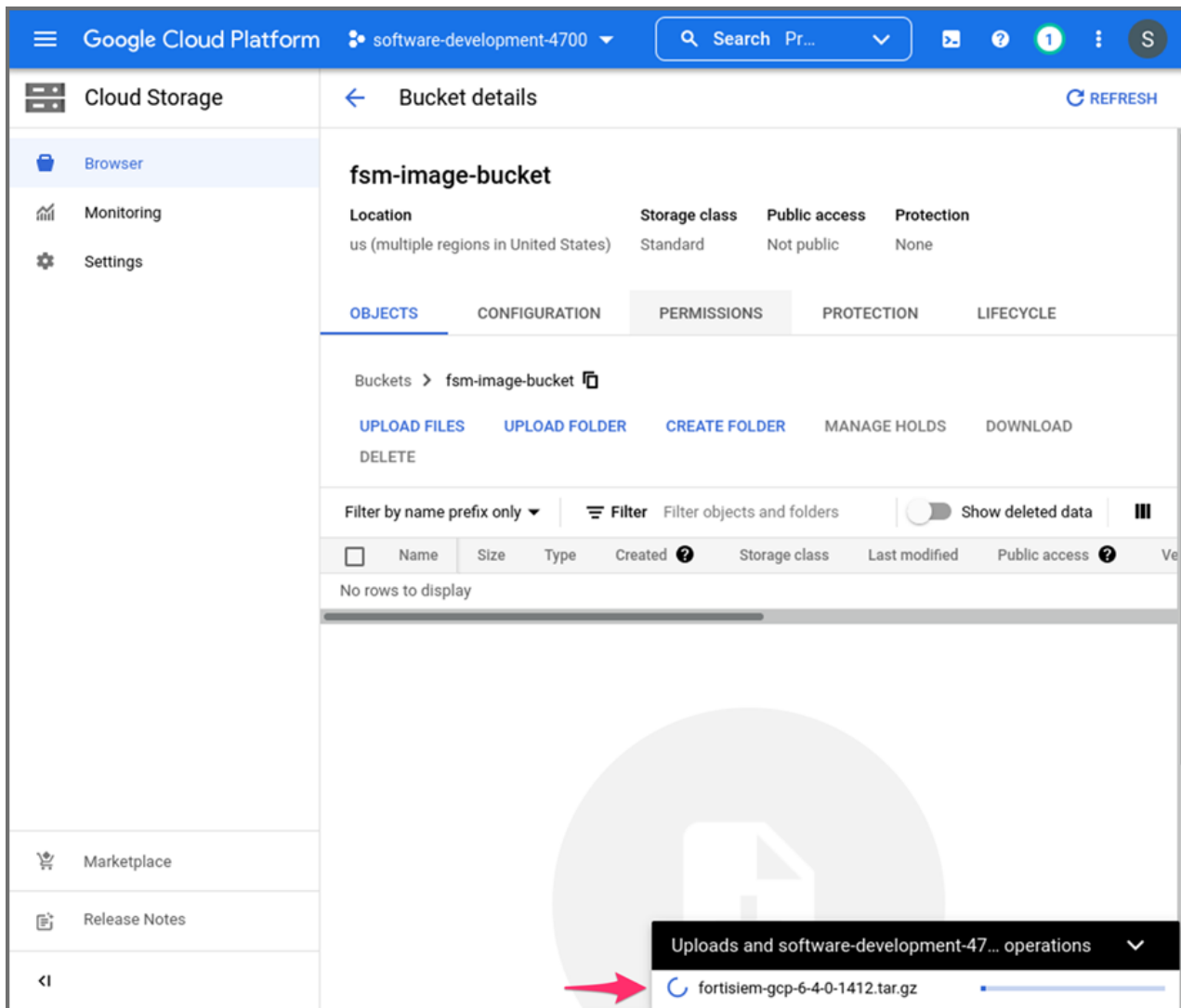
1. Go to the Fortinet Support website <https://support.fortinet.com> to download the GCP package fortisiem-gcp-6-7-1-1725.tar.gz. See [Downloading FortiSIEM Products](#) for more information on downloading products from the support website.
2. Identify the Google Cloud storage bucket where you plan to 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.



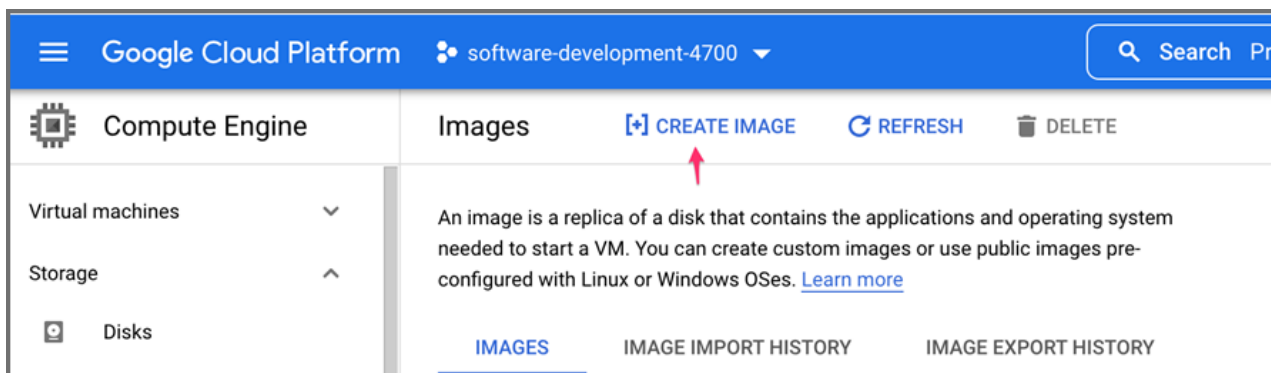
3. Click **UPLOAD FILES** and navigate to the downloaded FortiSIEM gcp image file - fortisiem-gcp-6-7-1-1725.tar.gz.



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

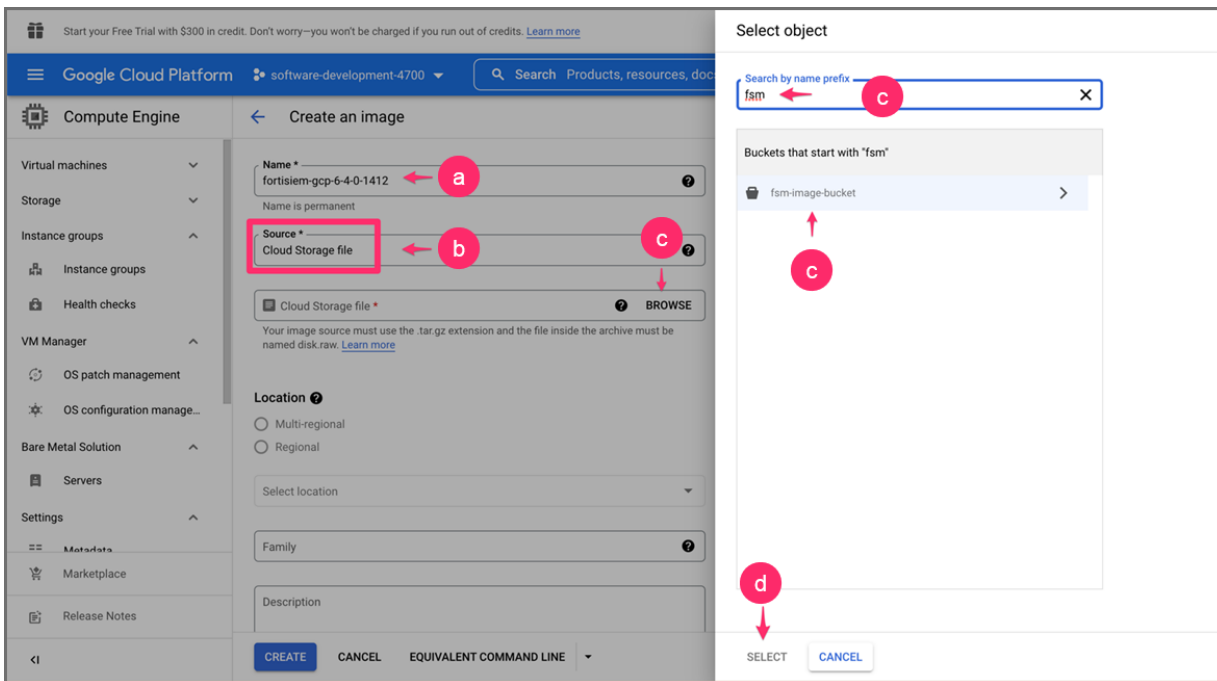


5. Once the upload is complete, navigate to Google Cloud Images service.
6. Click **CREATE IMAGE**.

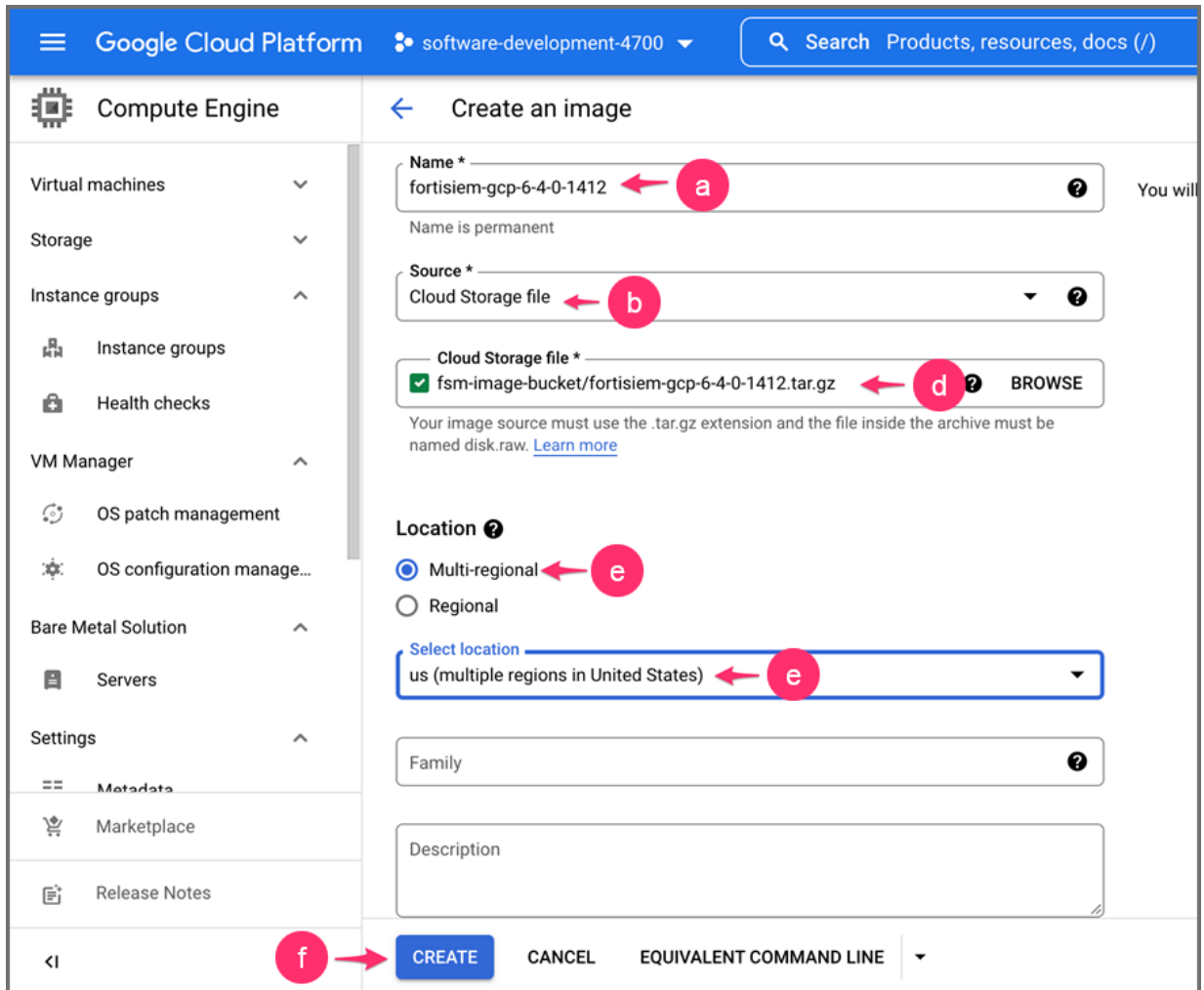


7. From the Create an image section, take the following steps.
 - a. In the **Name** field, enter the name of the image as `fortisiem-gcp-6-7-1-1725` (lowercase alphanumeric with dashes allowed only).

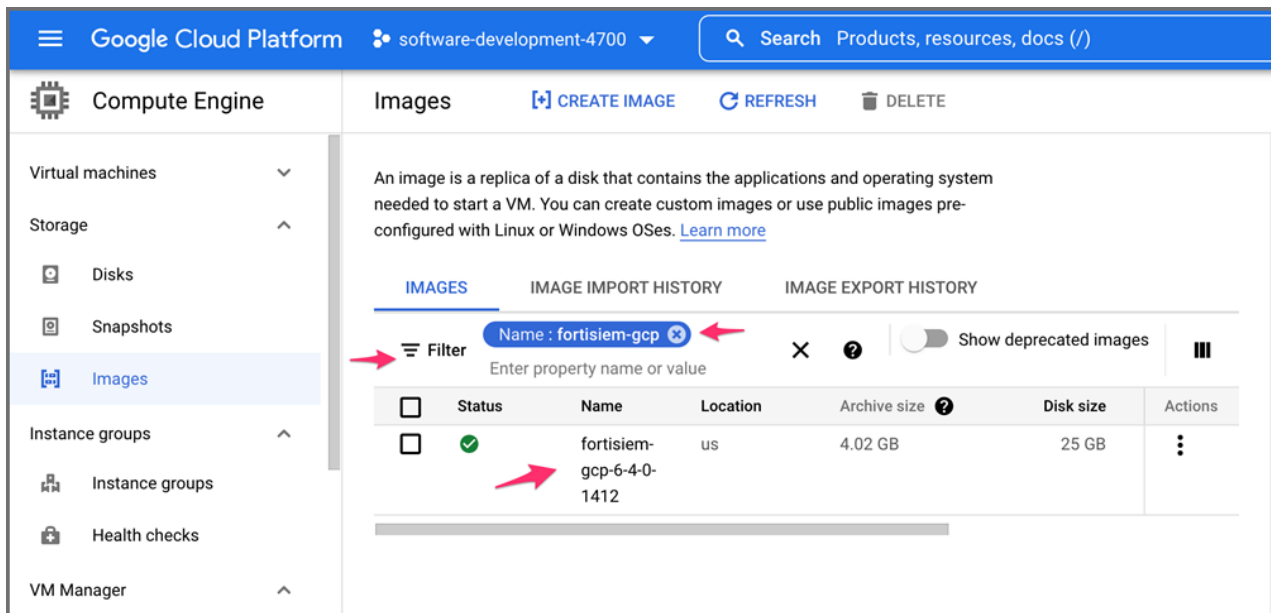
- b. From the **Source** drop-down list, choose **Cloud Storage file**.
- c. Click **BROWSE** and browse to the storage bucket where you uploaded the image tar.gz file.
- d. Select the bucket, and then select the uploaded file `fortisiem-gcp-6-7-1-1725.tar.gz`.



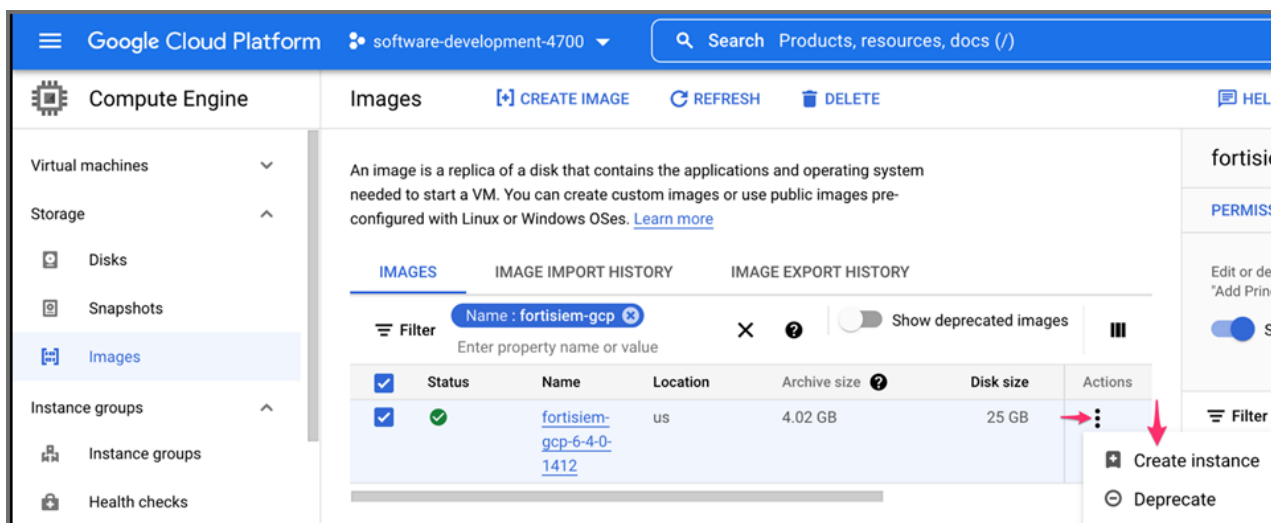
- e. For **Location**, select **Multi-regional**, and choose your location. You can leave the rest of the options as default unless you have specific requirements to change them.
- f. When done, click **CREATE**.



- 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**.



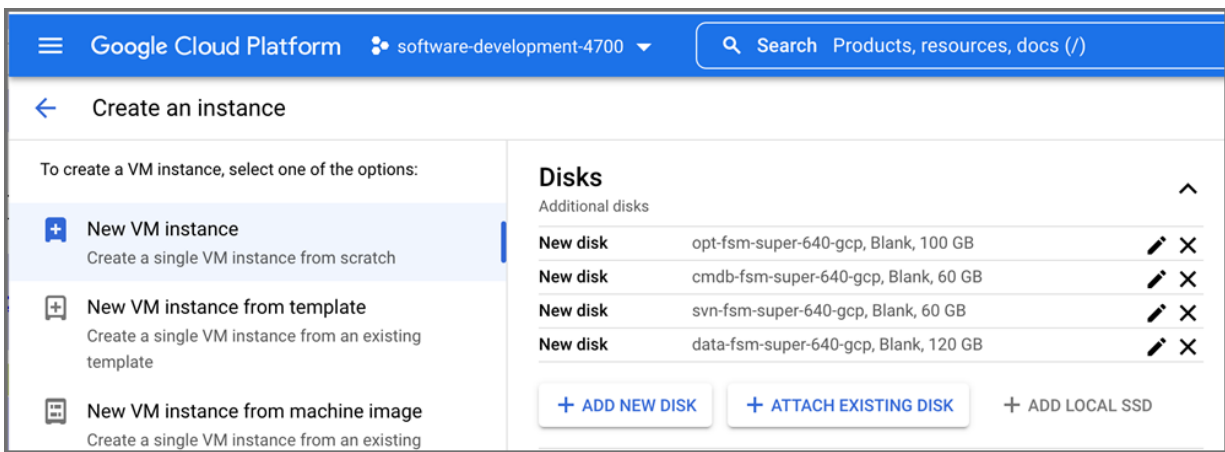
- 10. Choose defaults for all remaining items until the **Firewall** section. Choose **Allow HTTPS Traffic**.
- 11. For the **Networking** section, you can leave it as default unless you need to change some values.
- 12. In the **Disks** section, add an extra three disks by clicking **Add NEW DISK**. 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

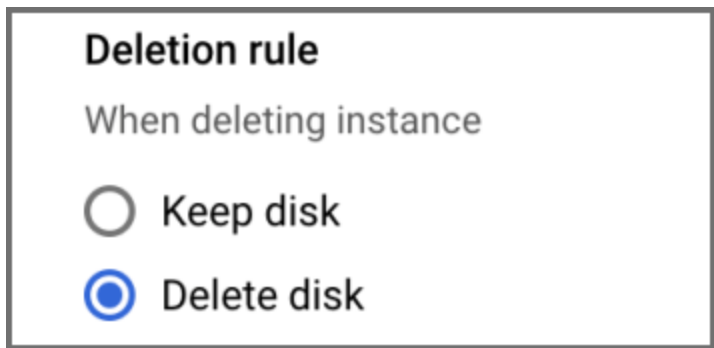
Disk	Size	Disk Name
		For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when <code>configFSM.sh</code> runs.
Disk 3	60GB	/cldb
Disk 4	60GB	/svn
Disk 5	60GB+	/data (see the following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

Note on Hard Disk 5:

- Add the 5th disk only if using EventDB on local storage or ClickHouse. In all other cases, this disk is not required. ClickHouse is recommended for most deployments. Please see [ClickHouse Reference Architecture](#) for more information.
- For EventDB on local disk, choose a disk based on your EPS and event retention policy. See [EventDB Sizing Guide](#) for guidance. 60GB is the minimum.
- For ClickHouse, choose disks based on the number of Tiers and disks on each Tier. These depend on your EPS and event retention policy. See [ClickHouse Sizing Guide](#) for guidance. For example, you can choose 1 large disk for Hot Tier. Or you can choose 2 Tiers - Hot Tier comprised of one or more SSD disks and Warm Tier comprised of one or more magnetic hard disks.
-



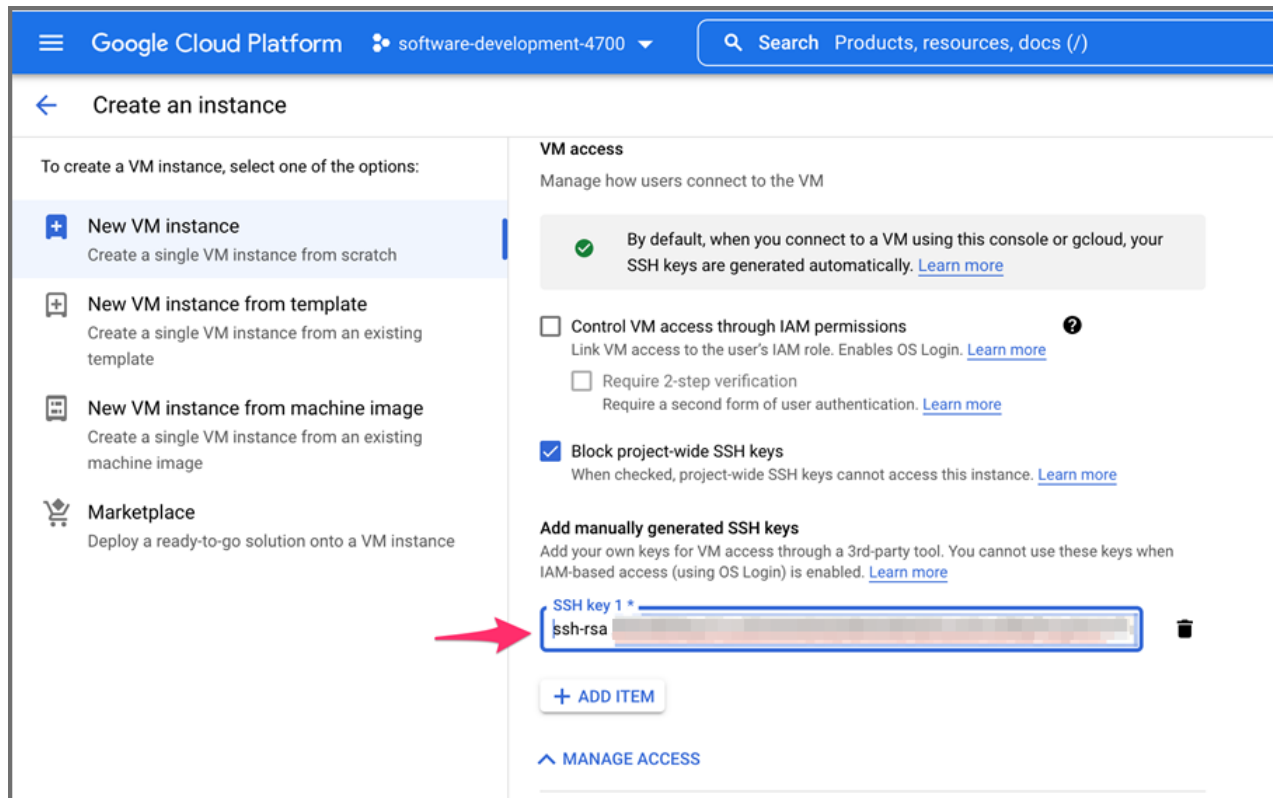
13. Under **Deletion rule**, select **Delete disk**.



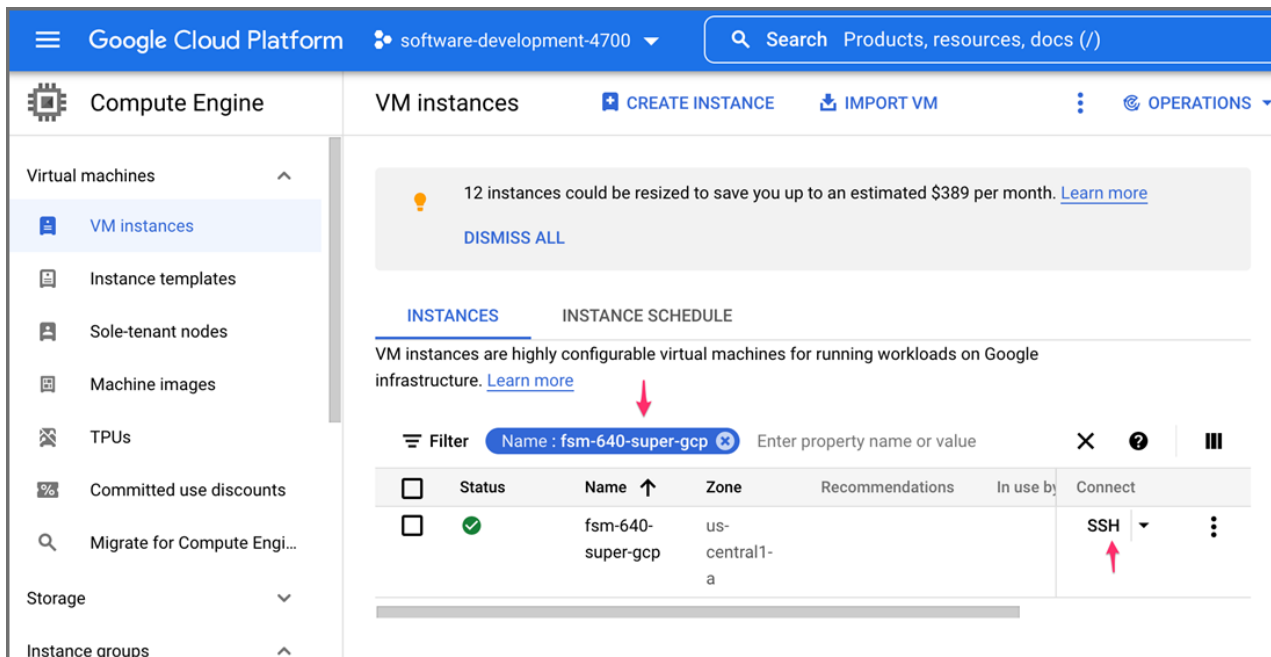
- Under the **Security** section, select **Manage Access**. If you would like to ssh access the instance from your own terminal, then you will need to provide manually generated ssh public keys (RSA or DSA) with a user name at the end like below

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

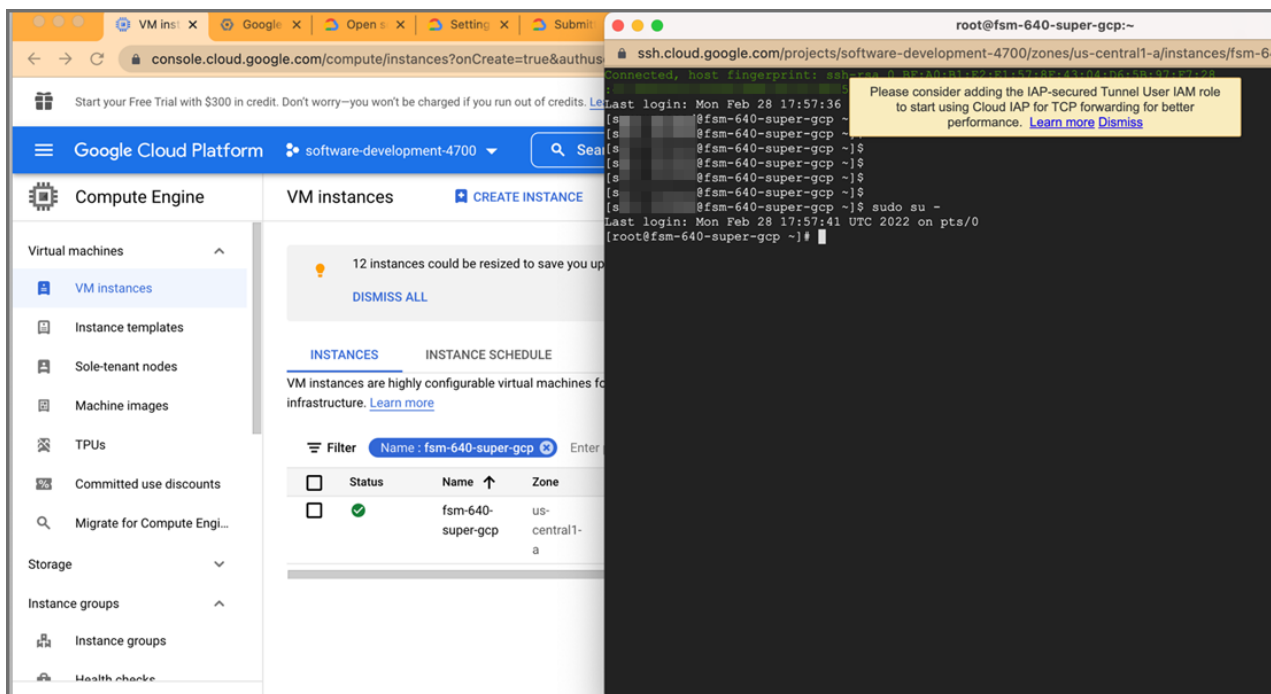
If you only wish to connect to the instance from GCP's browser based terminal, you should choose **Control VM access through IAM permissions**.



- Leave **Management** and **Tenancy** sections with their default values unless you need to change it per your needs.
- Click **Create**.
- 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.



- 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.



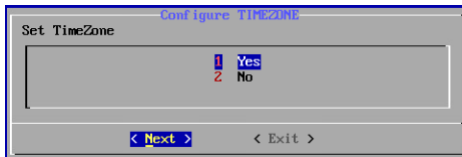
At this point, you can continue configuring FortiSIEM by using the GUI.

Configure FortiSIEM

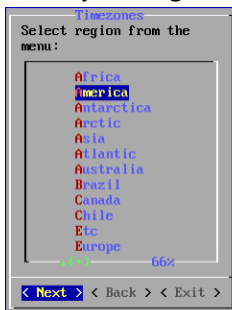
Follow these steps to configure FortiSIEM.

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**.



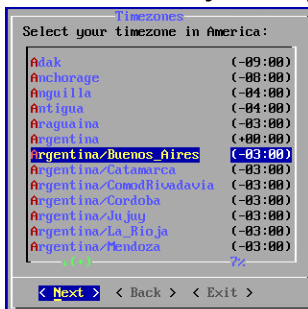
3. Select your **Region**, and press **Next**.



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



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



6. If installing a Supervisor, select **1 Supervisor**. Press **Next**.
 If installing a Worker, select **2 Worker**, and press **Next**.
 If installing a Collector, select **3 Collector**, and press **Next**.
 If Installing FortiSIEM Manager, select **4 FortiSIEM Manager**, and press **Next**.
 If Installing FortiSIEM Supervisor Follower, select **5 Supervisor Follower** and press **Next**.
Note: The appliance type cannot be changed once it is deployed, so ensure you have selected the correct option.



Regardless of whether you select **FortiSIEM Manager**, **Supervisor**, **Supervisor Follower**, **Worker**, or **Collector**, you will see the same series of screens with only the header changed to reflect your target installation, unless noted otherwise.

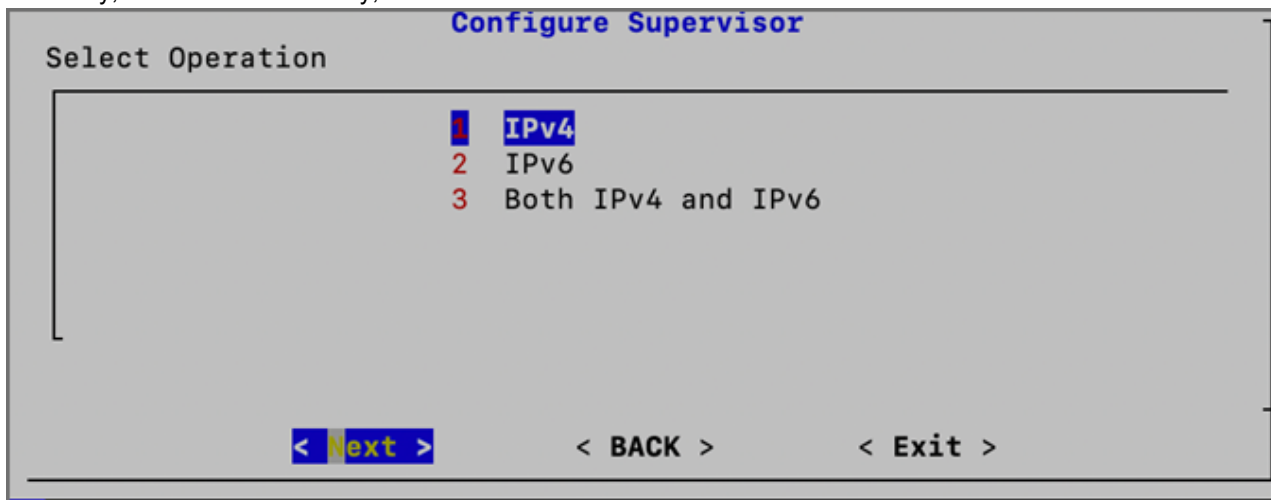
A dedicated ClickHouse Keeper uses a Worker, so first install a Worker and then in later steps configure the Worker as a ClickHouse Keeper.

- 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.

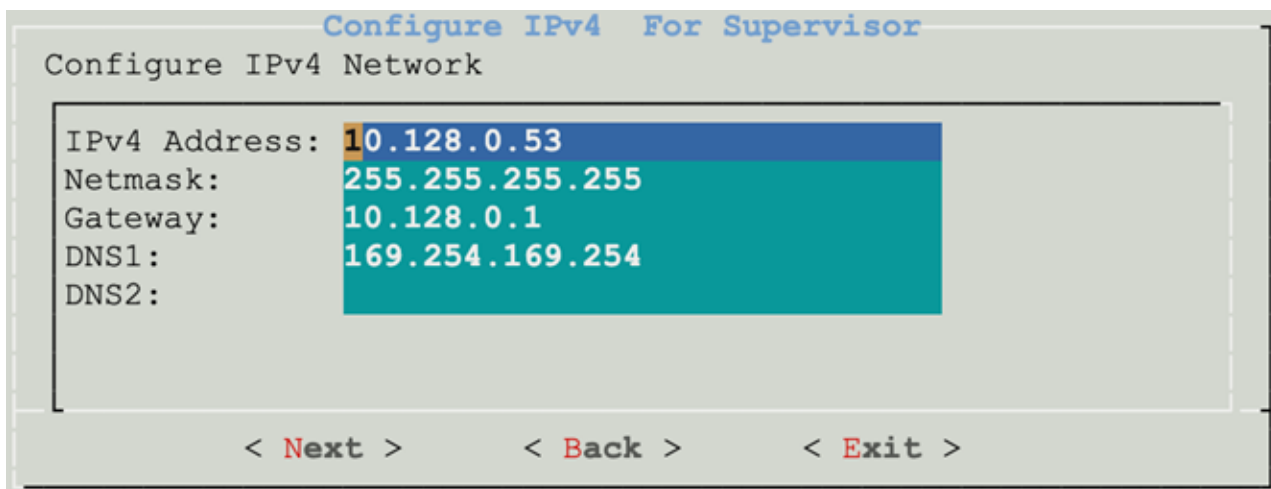


8. Determine whether your network supports IPv4-only, IPv6-only, or both IPv4 and IPv6 (Dual Stack). Choose **1** for IPv4-only, choose **2** for IPv6-only, or choose **3** for both IPv4 and IPv6.



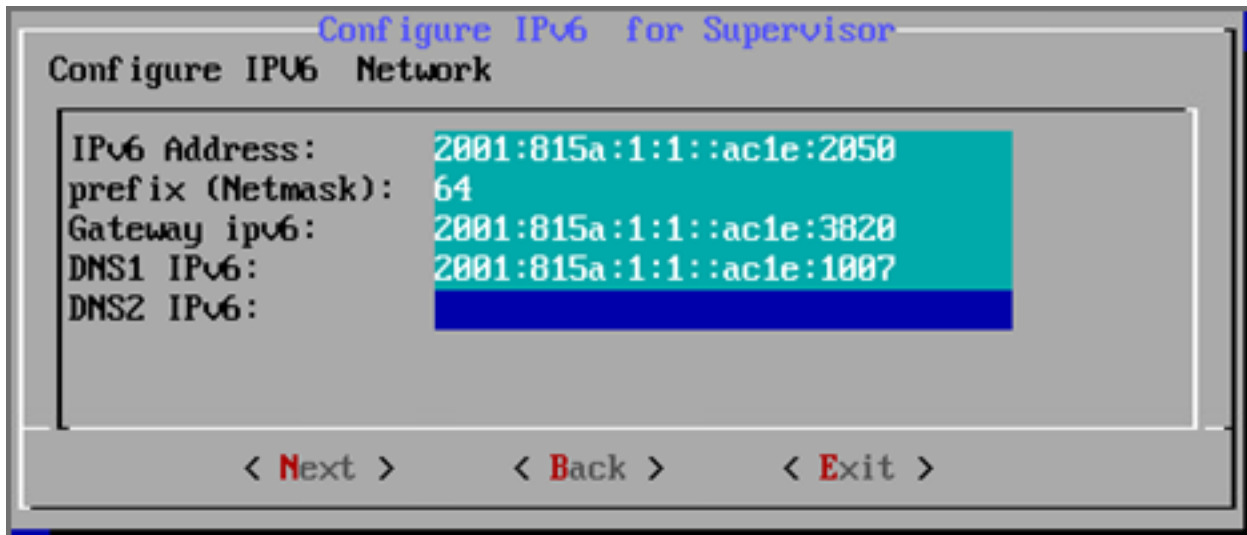
9. If you choose **1** (IPv4) or choose **3** (Both IPv4 and IPv6), and press **Next**, then you will move to step 11. If you choose **2** (IPv6), and press **Next**, then skip to step 12.
10. Configure the network by entering the following fields. Press **Next**.

Option	Description
IPv4 Address	The Manager/Supervisor/Worker/Collector's IPv4 address
NetMask	The Manager/Supervisor/Worker/Collector's IPv4 subnet
Gateway	IPv4 Network gateway address
DNS1, DNS2	Addresses of the IPv4 DNS server 1 and DNS server2



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**.

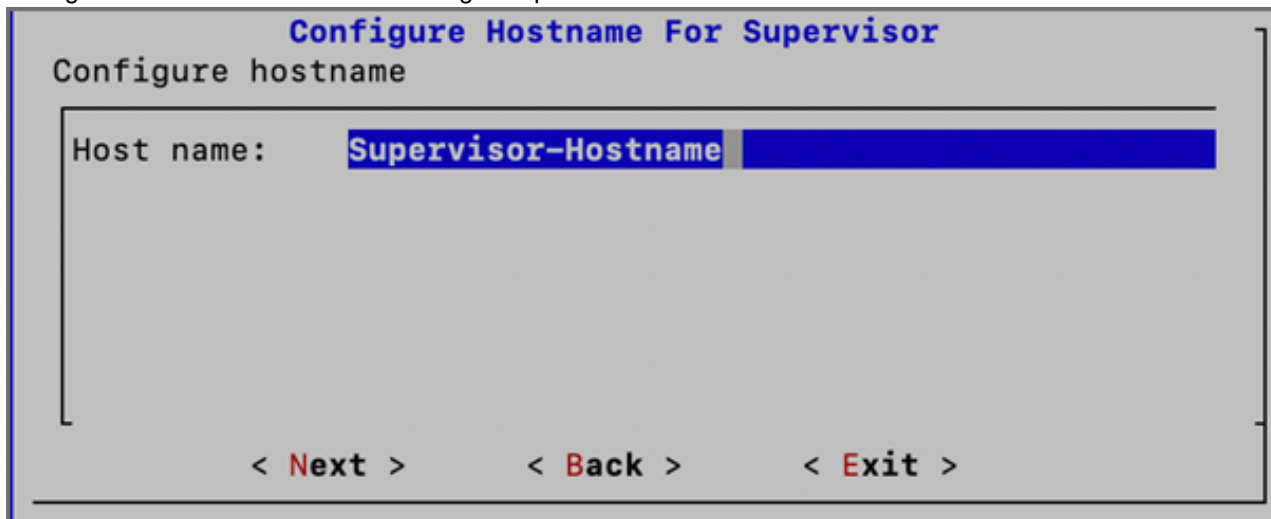
Option	Description
IPv6 Address	The Manager/Supervisor/Worker/Collector's IPv6 address
prefix (Netmask)	The Manager/Supervisor/Worker/Collector's IPv6 prefix
Gateway ipv6	IPv6 Network gateway address
DNS1 IPv6, DNS2 IPv6	Addresses of the IPv6 DNS server 1 and DNS server2



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.

- Configure Hostname for FortiSIEM Manager/Supervisor/Worker/Collector. Press **Next**.



Note: FQDN is no longer needed.

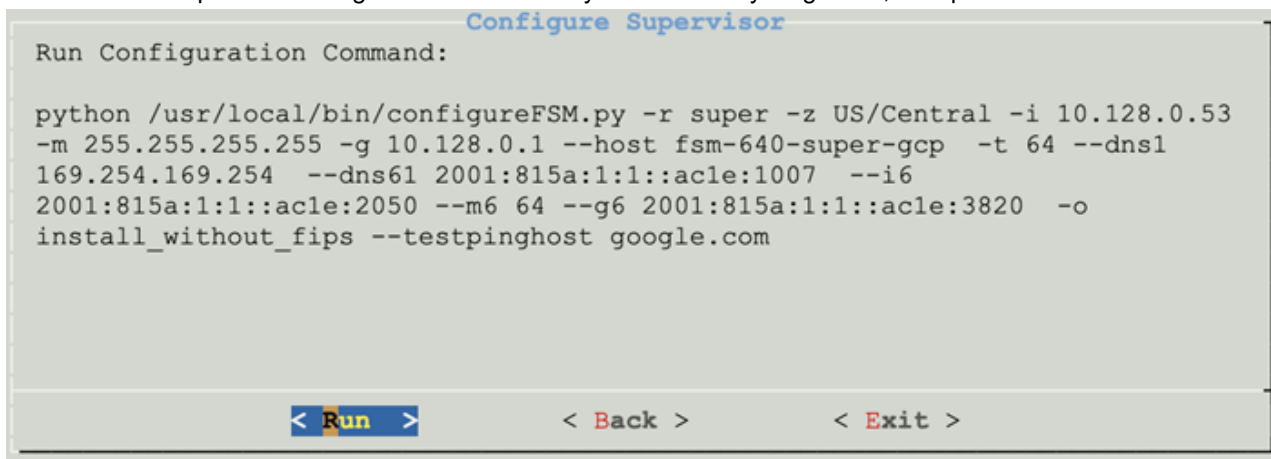
- Test network connectivity by entering a host name that can be resolved by your DNS Server (entered in the previous step) and can respond to a ping. The host can either be an internal host or a public domain host like google.com. Press **Next**.

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.



- 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

Option	Description
-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
--testinghost	The URL used to test connectivity

15. 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.

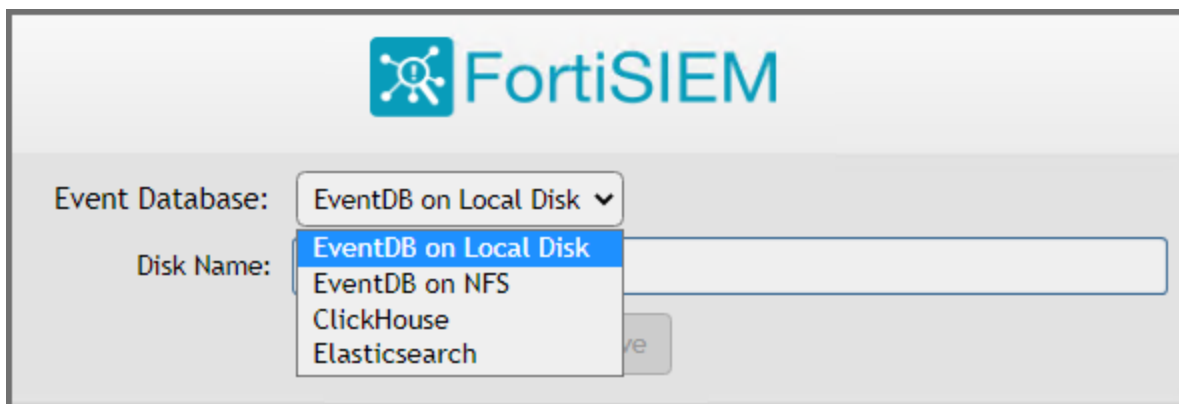
1. Open a Web browser and log in to the FortiSIEM UI. Use link `https://<supervisor-ip>` to login. Please note that if you are logging into FortiSIEM with an IPv6 address, you should input `https://[IPv6 address]` on the browser tab.
2. The License Upload dialog box will open.

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.
For FortiSIEM Manager, **License Type** is not an available option, and will not appear. At this point, FortiSIEM Manager installation is complete. You will not be taken the Event Database Storage page, so you can skip **Configure an Event Database**.
Note: The FortiSIEM Manager license allows a certain number of instances that can be registered to FortiSIEM Manager.
6. Proceed to [Configure an Event Database](#).

Configure an Event Database

Choose the event database.



The screenshot shows the FortiSIEM configuration interface. At the top, the FortiSIEM logo is displayed. Below it, there are two dropdown menus. The first is labeled 'Event Database:' and is currently set to 'EventDB on Local Disk'. The second is labeled 'Disk Name:' and is open, showing a list of options: 'EventDB on Local Disk', 'EventDB on NFS', 'ClickHouse', and 'Elasticsearch'. The 'EventDB on Local Disk' option is highlighted in blue. To the right of the 'Disk Name' dropdown, there is a text input field and a 'Save' button.

If the Event Database is one of the following options, additional disk configuration is required.

- **ClickHouse:** See Case 2 in [Creating ClickHouse Online Storage](#).
Recommended for most deployments. Please see [ClickHouse Reference Architecture](#) for more information.
- **EventDB on Local Disk:** See Case 2 in [Creating EventDB Online Storage](#).

Final Check

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
```

For the Supervisor, Supervisor Follower, Worker and Collector, 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, 0.6%ni, 91.4%id, 0.6%wa, 0.2%hi, 0.1%si, 0.0%st
Mem: 65702190k total, 10366036k used, 55336054k free, 4352k buffers
Swap: 2621436k total, 0k used, 2621436k free, 2465020k cached

PROCESS                UPTIME                CPU%                VIRT_MEM            RES_MEM
phParser                41:23                 0                   2176m                550m
phQueryMaster           41:41                 0                   1020m                77m
phAlertMaster           41:41                 0                   1079m                504m
phAlertWorker           41:41                 0                   1363m                205m
phQueryWorker           41:41                 0                   1383m                279m
phDataManager           41:41                 0                   1419m                205m
phDiscover              41:41                 0                   513m                 53m
phReportWorker          41:41                 0                   1433m                95m
phReportMaster          41:41                 0                   602m                 67m
phIdentityWorker        41:41                 0                   1027m                50m
phIdentityMaster        41:41                 0                   491m                 39m
phAgentManager          41:41                 0                   1425m                54m
phCheckpoint            42:31                 0                   325m                 39m
phEventManager           41:41                 0                   702m                 70m
phReportLoader          41:41                 0                   769m                270m
phBeaconEventPackager   41:41                 0                   1125m                65m
phDataPurger            41:41                 0                   588m                 50m
phEventForwarder        41:41                 0                   540m                 46m
phMonitor               37:24                 0                   2000m                57m
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
AppSvr                  01:10:07              0                   15172m               3026m
DBSvr                   01:10:30              0                   317m                 30m
phAnomaly               01:00:07              0                   907m                 64m
phFortiInsightAI        01:10:40              0                   23432m               430m
Redis                   01:10:10              0                   55m                  25m
```

For FortiSIEM Manager, the response should look similar to the following.

```
Every 1.0s: /opt/phoenix/bin/phstatus.py
System uptime: 11:34:52 up 1 day, 1:39, 2 users, load average: 0.00, 0.00, 0.92
Tasks: 5 total, 0 running, 5 sleeping, 0 stopped, 0 zombie
Cpu(s): 8 cores, 7.2%us, 0.2%sy, 0.0%ni, 92.3%id, 0.0%wa, 0.1%hi, 0.1%si, 0.0%st
Mem: 24468724k total, 6696192k used, 16212508k free, 5248k buffers
Swap: 26058744k total, 0k used, 26058744k free, 2352072k cached

PROCESS                UPTIME                CPU%                VIRT_MEM            RES_MEM
phMonitor              20:57:20              0                   1130m                64m
Apache                 1-01:20:00            0                   305m                 16m
Rsyslogd               1-01:38:42            0                   192m                 7388k
AppSvr                 1-01:38:34            5                   11153m               4182m
DBSvr                  1-01:38:43            0                   425m                 39m
```

Cluster Installation

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

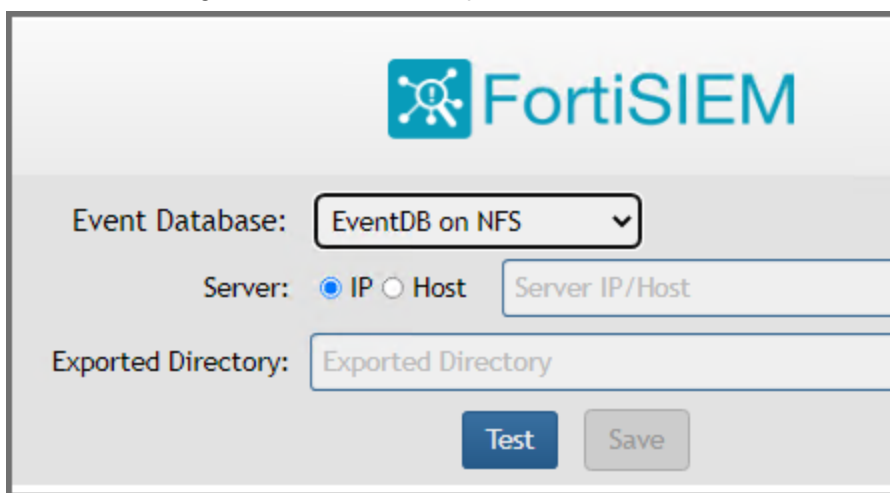
- [Install Supervisor](#)
- [Install Workers](#)
- [Register Workers](#)
- [Create ClickHouse Topology \(Optional\)](#)

- [Install Collectors](#)
- [Register Collectors](#)
- [Install Manager](#)
- [Register Instances to Manager](#)

Install Supervisor

Follow the steps in [All-in-one Installation](#), except with the following differences.

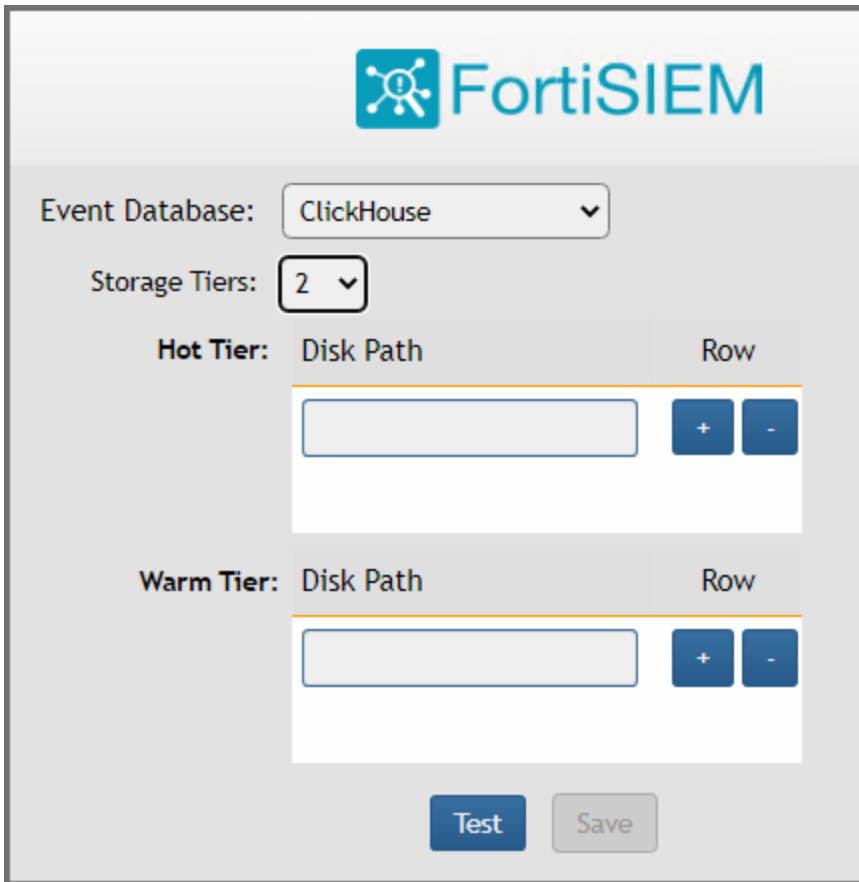
1. Event Database choices are **EventDB on NFS**, **ClickHouse**, or **Elasticsearch**.
2. If you choose **EventDB on NFS**
 - a. Disk 5 is not required (From [Import FortiSIEM GCP Image into Google Cloud Image Step 12](#)).
 - b. You need to configure NFS after license upload.



The screenshot shows the FortiSIEM configuration interface. At the top, there is the FortiSIEM logo. Below it, the 'Event Database' is set to 'EventDB on NFS' in a dropdown menu. Underneath, the 'Server' configuration has 'IP' selected with a radio button, and a text input field labeled 'Server IP/Host'. Below that, there is a text input field labeled 'Exported Directory'. At the bottom of the form, there are two buttons: 'Test' (in blue) and 'Save' (in grey).

3. If you choose **ClickHouse**
 - a. You need to create disks during [Import FortiSIEM GCP Image into Google Cloud Image Step 12](#) based on the role of the Supervisor node in the ClickHouse cluster. See the [ClickHouse Sizing Guide](#) for details.

- b. You need to configure disks after license upload.



The screenshot shows the FortiSIEM configuration interface. At the top, the FortiSIEM logo is displayed. Below it, the 'Event Database' is set to 'ClickHouse'. The 'Storage Tiers' are set to '2'. There are two sections for configuring storage tiers: 'Hot Tier' and 'Warm Tier'. Each section has a 'Disk Path' field and a 'Row' field. The 'Hot Tier' section has a text input field and two buttons, '+' and '-'. The 'Warm Tier' section also has a text input field and two buttons, '+' and '-'. At the bottom of the form, there are two buttons: 'Test' and 'Save'.

- 4. If you choose **Elasticsearch**, define Elasticsearch endpoints after license upload. See the [Elasticsearch Sizing Guide](#) for details.

The screenshot shows the FortiSIEM configuration interface. At the top is the FortiSIEM logo. Below it, the 'Event Database' is set to 'Elasticsearch'. The 'ES Service Type' is set to 'Native'. The 'Endpoint' section is a table with columns for 'URL', 'Ingest', 'Query', and 'Row'. The 'URL' column contains 'https://'. The 'Ingest' and 'Query' columns have checkboxes checked. The 'Row' column has '+' and '-' buttons. Below the table are fields for 'REST Port' (443), 'User Name' (Optional), 'Password' (Optional), and 'Confirm Password'. The 'Shard Allocation' is set to 'Dynamic'. The 'Shards' field is 5 and 'Replicas' is 1. There is a 'Per Org Index' checkbox which is unchecked. At the bottom are 'Test' and 'Save' buttons.

Endpoint:	URL	Ingest	Query	Row
	https://	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	+ -

Install Workers

Once the Supervisor is installed, take the same steps in [All-in-one Installation](#) to install a Worker with the following differences.

1. Choose appropriate CPU and memory for the Worker nodes based on Sizing guide.
2. Two hard disks for Operating Systems and FortiSIEM Application:
 - 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.

3. If you are running ClickHouse, then create additional data disks based on the role of the Worker in ClickHouse topology. If it is a Keeper node, then a smaller disk is needed. If it is a data node, then a bigger disk is needed based on your EPS and retention policy. See ClickHouse Sizing Guide for details.

Sizing Guide References:

- [ClickHouse Sizing Guide](#)
- [EventDB Sizing Guide](#)
- [Elasticsearch Sizing Guide](#)

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 **Mode** drop-down list and enter the following information:
 - a. In the **Host Name** field, enter the Worker's host name.
 - b. In the **IP Address** field, enter the Worker's IP address.
 - c. If you are running ClickHouse, then select the number for Storage Tiers from the **Storage Tiers** drop-down list, and input disk paths for disks in each Tier in the **Disk Path** fields.

For **Disk Path**, use one of the following CLI commands to find the disk names.

```
fdisk -l
```

or

```
lsblk
```

When using `lsblk` to find the disk name, please note that the path will be `/dev/<disk>`. As an example, `/dev/vdc`.

- d. Click **Test**.

Add Node
✕

Mode: Worker ▼

Host Name:

IP Address:

Running On: VM ▼

Storage Tiers: 2 ▼

Hot Tier:

Disk Path	Mounted On	Row
<input style="width: 100%;" type="text"/>	/data-clickhouse-hot-1	+ -

Warm Tier:

Disk Path	Mounted On	Row
<input style="width: 100%;" type="text"/>	/data-clickhouse-warm-1	+ -

Test
Save
Cancel

- e. If the test succeeds, then click **Save**.
- 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

License

Settings

Name	IP Address	Module Role	Health	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

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		
phDataManaaer	Up	14m 6s	0%	103 MB	1229 MB	1	126108

Copyright © 2020 Fortinet, Inc. All rights reserved.
Organization: Super
User: admin
Scope: Global
FortiSIEM

Create ClickHouse Topology (Optional)

If you are running ClickHouse, you need to configure ClickHouse topology by specifying which nodes belong to ClickHouse Keeper and Data Clusters. Follow the steps in [Configuring ClickHouse Topology](#).

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 > Cluster Config**.
 - a. Enter the IP of the Worker node in the **Event Upload Workers** column. 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 **Save**.
 - c. In the **Supervisors** column, enter the IP of the Supervisor node and click **Save**.
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:

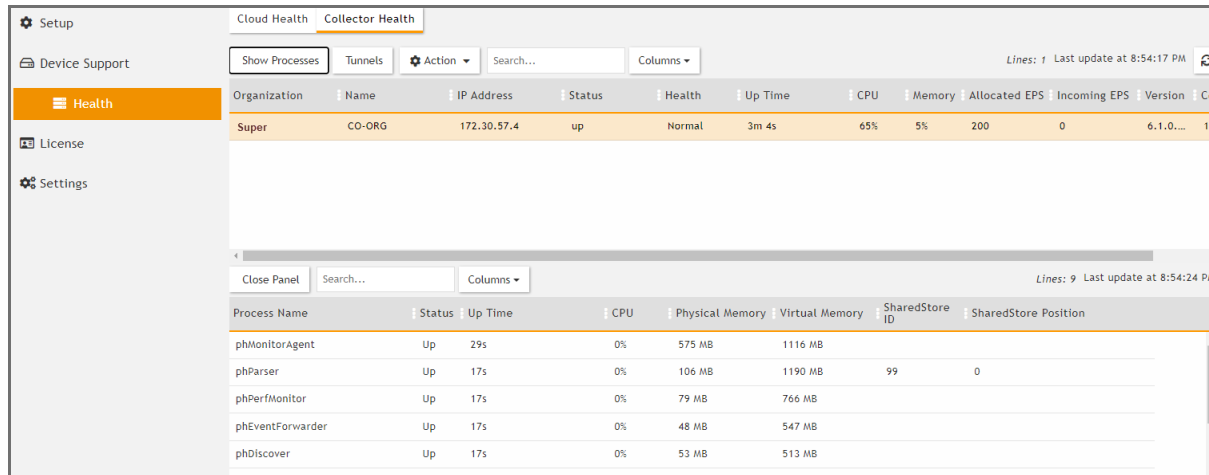
```
phProvisionCollector --add <user> '<password>' <Super IP or Host> <Organization>
<CollectorName>
```

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.

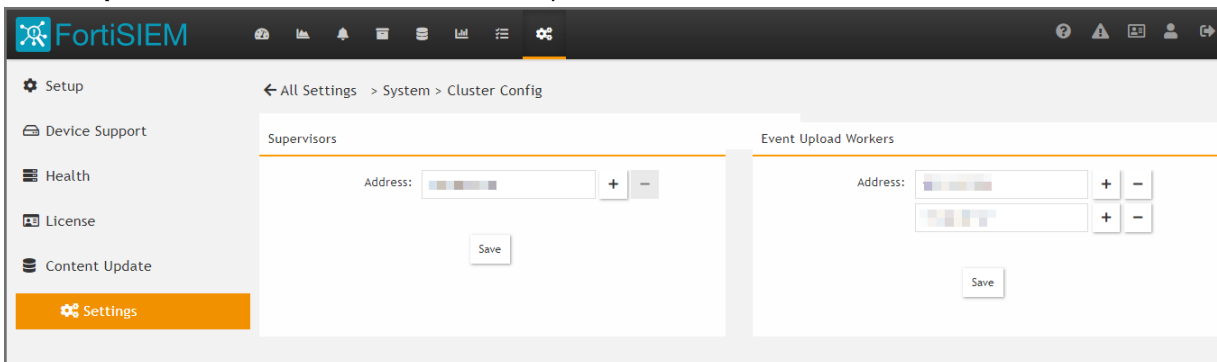


Service Provider Deployments

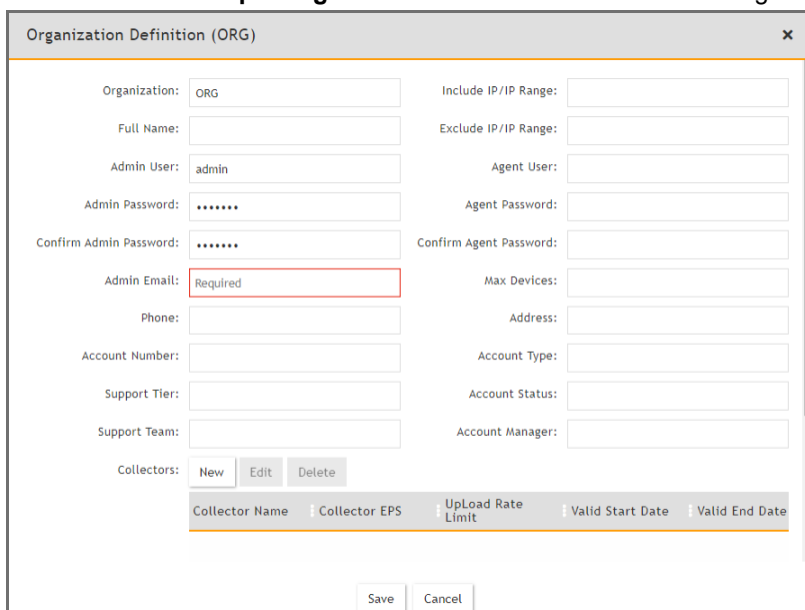
For Service Provider deployments, follow these steps.

1. Log in to Supervisor with 'Admin' privileges.
2. Go to **ADMIN > Settings > System > Cluster Config**.
 - a. Enter the IP of the Worker node in the **Event Upload Workers** column. 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 **Save**.

c. In the **Supervisors** column, enter the IP of the Supervisor node and click **Save**.



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

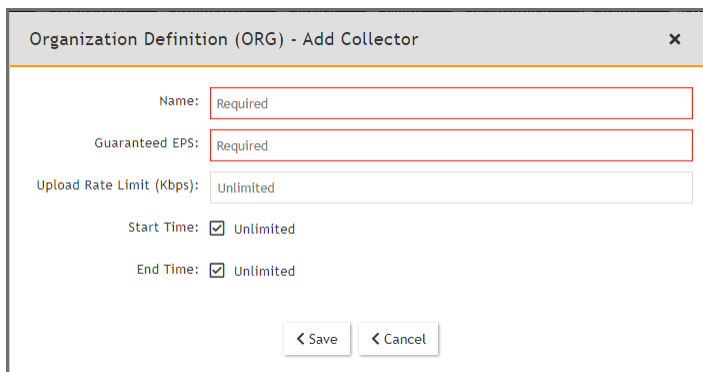


4. Enter the **Organization Name**, **Admin User**, **Admin Password**, and **Admin Email**.

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.

- Set `user` and `password` use the admin User Name and password for the Organization that the Collector is going to be registered to.
- Set `Super IP or Host` as the Supervisor's IP address.
- Set `Organization` as the name of an organization created on the Supervisor.
- 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 shows the 'Collector Health' page in the FortiSIEM interface. It displays a table of collector instances and a detailed view of the processes running on the collector.

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 Manager

Starting with release 6.5.0, you can install FortiSIEM Manager to monitor and manage multiple FortiSIEM instances. An instance includes a Supervisor and optionally, Workers and Collectors. The FortiSIEM Manager needs to be installed on a separate Virtual Machine and requires a separate license. FortiSIEM Supervisors must be on 6.5.0 or later versions.

Follow the steps in [All-in-one Install](#) to install Manager. After any Supervisor, Workers, and Collectors are installed, you add the Supervisor instance to Manager, then Register the instance to Manager. See [Register Instances to Manager](#).

Register Instances to Manager

To register your Supervisor instance with Manager, you will need to do two things in the following order.

- First, [add the instance to Manager](#)
- Then [register the instance itself to Manager](#)

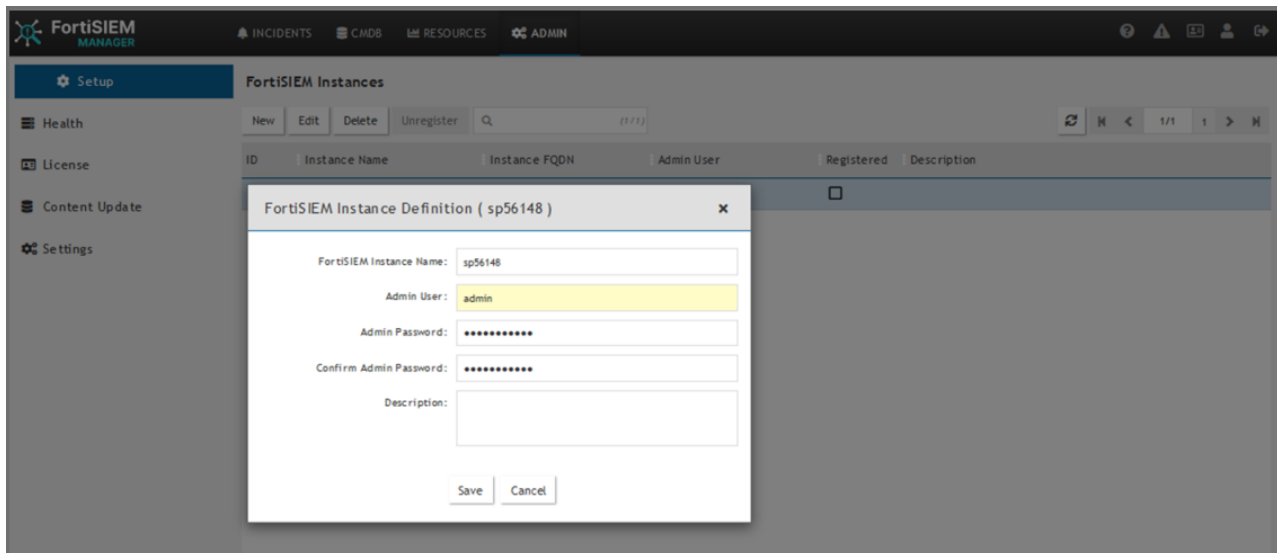
Note that Communication between FortiSIEM Manager and instances is via REST APIs over HTTP(S).

Adding Instance to Manager

You can add an instance to Manager by taking the following steps.

Note: Make sure to record the FortiSIEM Instance Name, Admin User and Admin Password, as this is needed when you register your instance.

1. Login to FortiSIEM Manager.
2. Navigate to **ADMIN > Setup**.
3. Click **New**.
4. In the **FortiSIEM Instance** field, enter the name of the Supervisor instance you wish to add.
5. In the **Admin User** field, enter the Account name you wish to use to access Manager.
6. In the **Admin Password** field, enter the Password that will be associated with the Admin User account.
7. In the **Confirm Admin Password** field, re-enter the Password.
8. (Optional) In the **Description** field, enter any information you wish to provide about the instance.
9. Click **Save**.



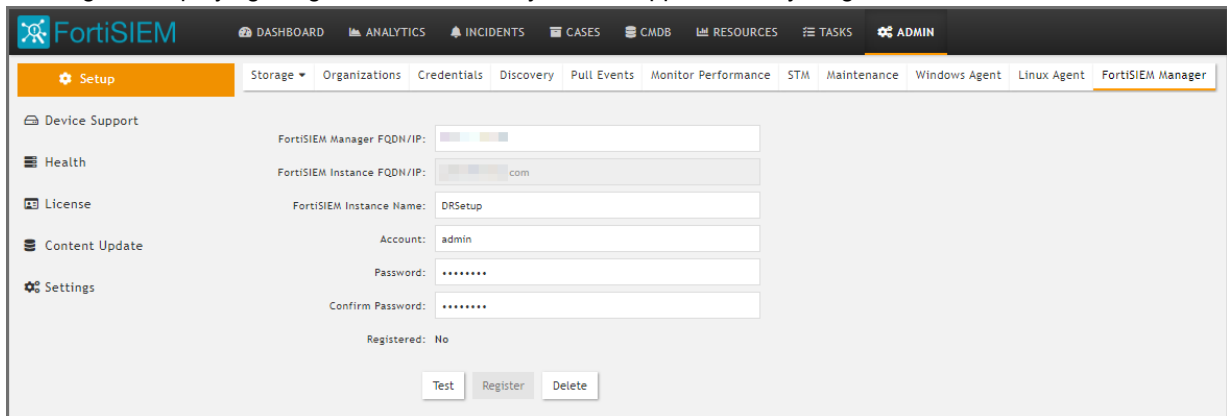
10. Repeat steps 1-9 to add any additional instances to Manager.
Now, follow the instructions in [Register the Instance Itself to Manager](#) for each instance.

Register the Instance Itself to Manager

To register your instance with Manager, take the following steps.

1. From your FortiSIEM Supervisor/Instance, navigate to **ADMIN > Setup > FortiSIEM Manager**, and take the following steps.
 - a. In the **FortiSIEM Manager FQDN/IP** field, enter the FortiSIEM Manager Fully Qualified Domain Name (FQDN) or IP address.
 - b. If the Supervisor is under a Supervisor Cluster environment, in the **FortiSIEM super cluster FQDN/IP** field, enter the Supervisor Cluster Fully Qualified Domain Name (FQDN) or IP address.
 - c. In the **FortiSIEM Instance Name** field, enter the instance name used when adding the instance to Manager.
 - d. In the **Account** field, enter the Admin User name used when adding the instance to Manager.
 - e. In the **Password** field, enter your password to be associated with the Admin User name.

- f. In the **Confirm Password** field, re-enter your password.
- g. Click **Test** to verify the configuration.
- h. Click **Register**.
A dialog box displaying "Registered successfully" should appear if everything is valid.



- i. Login to Manager, and navigate to any one of the following pages to verify registration.
 - **ADMIN > Setup** and check that the box is marked in the **Registered** column for your instance.
 - **ADMIN > Health**, look for your instance under FortiSIEM Instances.
 - **ADMIN > License**, look for your instance under FortiSIEM Instances.

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.