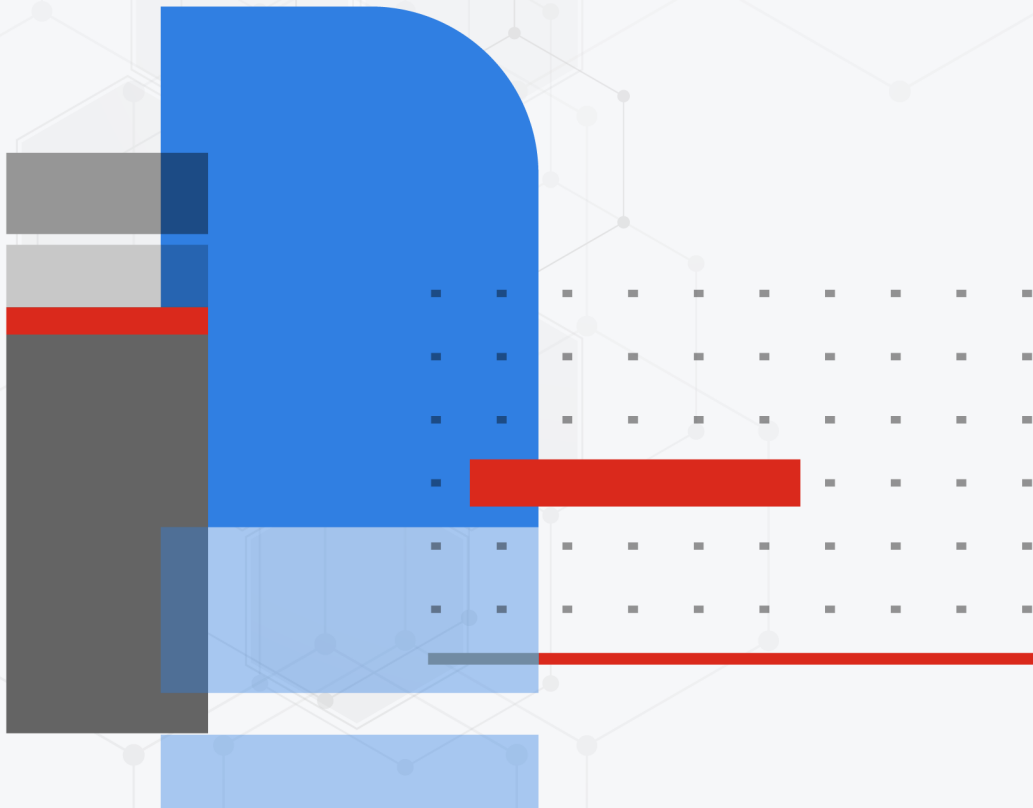


# AWS Installation Guide

FortiSIEM 6.7.0



**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](mailto:techdoc@fortinet.com)



10/03/2023

FortiSIEM 6.7.0 AWS Installation Guide

---

# TABLE OF CONTENTS

<b>Change Log</b> .....	<b>4</b>
<b>Fresh Installation</b> .....	<b>6</b>
Pre-Installation Checklist .....	6
All-in-one Installation .....	7
Launch an Instance Using FortiSIEM 6.7.0 AMI .....	8
Configure FortiSIEM .....	12
Upload the FortiSIEM License .....	18
Configure an Event Database .....	19
Final Check .....	19
Cluster Installation .....	20
Install Supervisor .....	21
Install Workers .....	23
Register Workers .....	24
Create ClickHouse Topology (Optional) .....	26
Install Collectors .....	26
Register Collectors .....	26
Install Manager .....	29
Register Instances to Manager .....	29
<b>Install Log</b> .....	<b>32</b>

# Change Log

Date	Change Description
05/09/2019	Initial release of ForiSIEM - AWS Installation Guide
03/22/2019	Updated instructions for Service Provider deployments.
11/11/2019	Small change to installation instructions for FortiSIEM and FortiSIEM Report Server.
03/30/2020	Released document for 5.3.0.
08/15/2020	Updated deployment and installation for FortiSIEM 6.1 on AWS.
10/6/2020	Initial release of AWS Installation and Configuration Guide.
11/03/2020	Release of AWS Installation and Configuration Guide for 6.1.1.
12/03/2020	Small addition to Pre-Installation Checklist.
12/07/2020	Small addition to Register Collectors.
02/04/2021	Migration update.
03/23/2021	Released document for 6.2.0.
04/16/2021	Minor update to Run the Backup Script and Shutdown System section.
04/22/2021	Added Install Log section.
05/07/2021	Released document for 6.2.1.
06/07/2021	Updated Elasticsearch screenshot for 6.2.x guides.
07/06/2021	Released document for 6.3.0.
08/26/2021	Released document for 6.3.1.
09/28/2021	Updated volume type information for 6.x guides.
10/15/2021	Released document for 6.3.2.
11/17/2021	Updated Register Collectors instructions for 6.x guides.
12/22/2021	Released document for 6.3.3.
01/18/2022	Released document for 6.4.0.
05/09/2022	Released document for 6.5.0.
07/26/2022	Released document for 6.6.0.
08/18/2022	Updated All-in-one Installation section.
09/12/2022	Released document for 6.5.1.

Date	Change Description
09/14/2022	Released document for 6.6.1.
09/19/2022	Released document for 6.6.2.
10/20/2022	Updated Register Collectors instructions for 6.x guides.
01/03/2023	Released document for 6.7.0.
02/13/2023	Released document for 6.7.1.
02/24/2023	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	Released document for 6.7.2.
03/28/2023	Released document for 6.7.3.
04/11/2023	Released document for 6.7.4.
05/22/2023	Released document for 6.7.5.
06/16/2023	Released document for 6.7.6.
07/13/2023	Released document for 6.7.7.
09/12/2023	Released document for 6.7.8.

# Fresh Installation

This section describes how to install FortiSIEM for the current release.

- [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 can respond to a 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 the storage type for Supervisor, Worker, and/or Collector
  - Online storage - 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 storage – There are 2 choices
    - EventDB on NFS
    - HDFS
- Fortinet recommends that you do not choose AWS Spot instances for Supervisor and Worker nodes. Such instances can go down at any time with short notice, causing instability and performance issues.
- Determine hardware requirements and choose AWS instance type accordingly:

Node	vCPU	RAM	Local Disks
Manager	Minimum – 16 Recommended - 32	Minimum <ul style="list-style-type: none"><li>• 24GB</li></ul> Recommended <ul style="list-style-type: none"><li>• 32GB</li></ul>	OS – 25GB OPT – 100GB CMDB – 60GB

Node	vCPU	RAM	Local Disks
			SVN – 60GB
Supervisor (All in one)	Minimum – 12 Recommended - 32	Minimum <ul style="list-style-type: none"> <li>without UEBA – 24GB</li> <li>with UEBA - 32GB</li> </ul> Recommended <ul style="list-style-type: none"> <li>without UEBA – 32GB</li> <li>with UEBA - 64GB</li> </ul>	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"> <li>without UEBA – 24GB</li> <li>with UEBA - 32GB</li> </ul> Recommended <ul style="list-style-type: none"> <li>without UEBA – 32GB</li> <li>with UEBA - 64GB</li> </ul>	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.

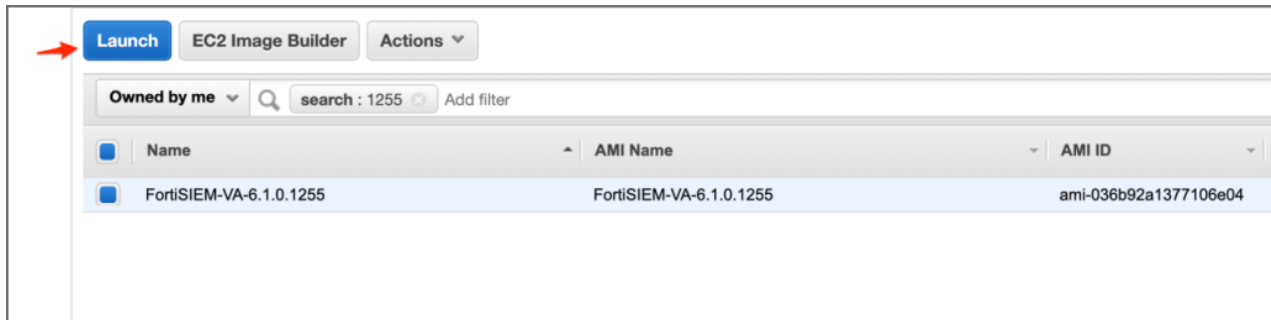
## All-in-one Installation

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

- [Launch an instance using FortiSIEM 6.7.0 AMI](#)
- [Configure FortiSIEM](#)
- [Upload the FortiSIEM License](#)
- [Configure an Event Database](#)
- [Final Check](#)

## Launch an Instance Using FortiSIEM 6.7.0 AMI

1. Navigate to the EC2 AMIs page and find FortiSIEM 6.7.0 AMI (or in AWS Marketplace after the GA release).
2. Launch FortiSIEM-6.7.0.1716.

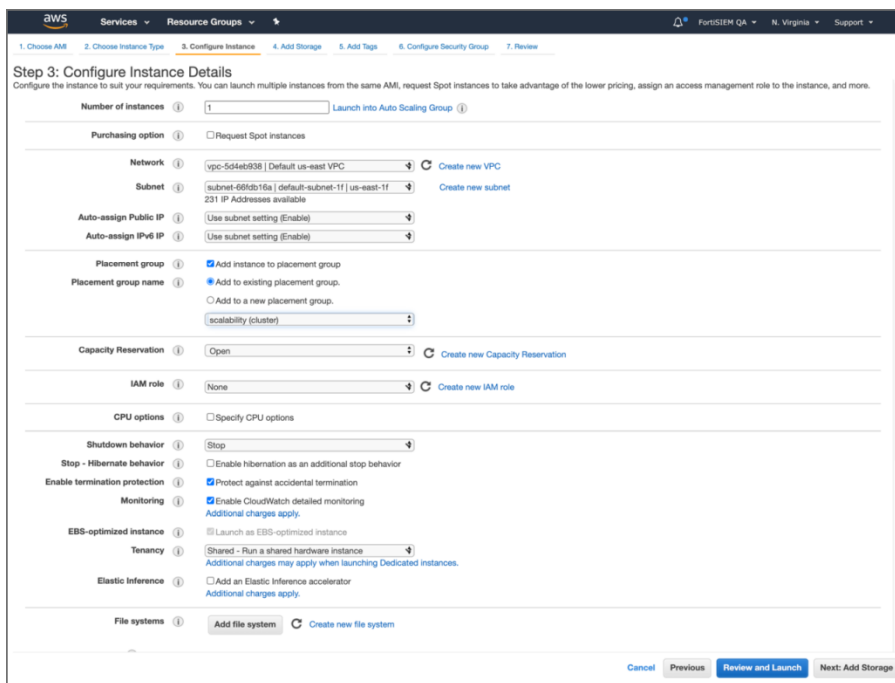


3. Go to **Step 3: Configure Instance Details** in AWS Services. Configure instance details such as VPC, Subnet, IP, etc. Click **Next**.

**Note:** If you are planning to also assign global IPv6 address to your instance, then AWS has instructions on how to create an IPv6-enabled VPC in the following article:

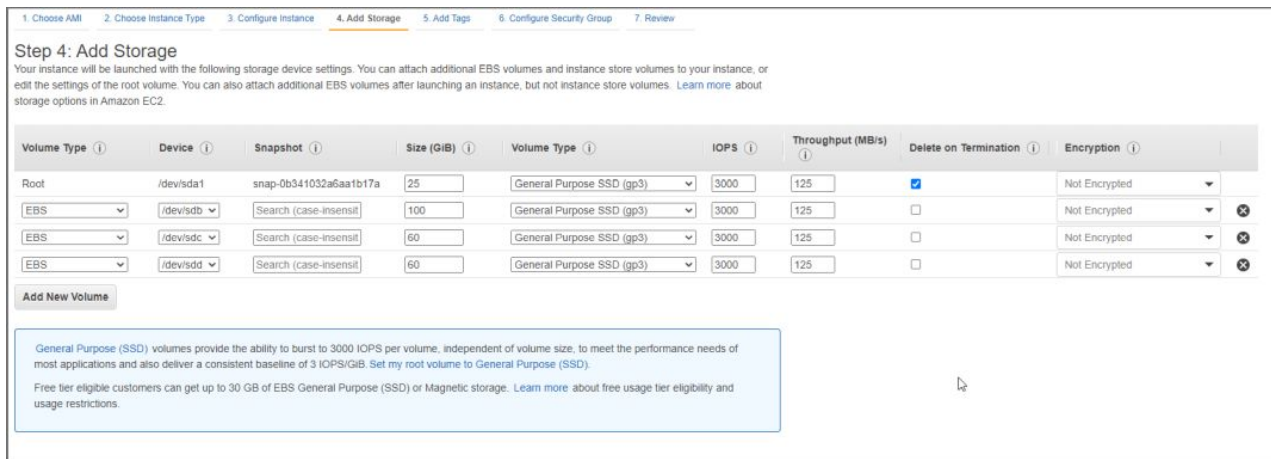
<https://docs.aws.amazon.com/vpc/latest/userguide/get-started-ipv6.html>

For IPv6 configuration, choose **IPv6-enabled VPC** and **IPv6-enabled subnet** in the step 3 **Configure Instance Details**. Also, choose **Auto-assign IPv6 IP** to **Enable**.



4. In **Step 4: Add Storage**, add additional disks in the **Add Storage** page. These will be used for the additional partitions in the virtual appliance. An All In One deployment requires the [following additional partitions](#). Then click **Next**.





**Note:** If you plan to onboard greater than 500 devices, or 5000 eps, please consider increasing IOPS and Throughput for the disk used to mount /cmdb in FortiSIEM.

For instance, you can run the following command once FortiSIEM is initially deployed to determine which disk mounts the cmdb folder.

```
[admin@6 data-definition]$ lsblk | grep cmdb
└─sdc1 8:33 0 60G 0 part /cmdb
```

In this case /dev/sdc.

You can go into EBS volumes in AWS, and increase the IOPS to 5000, and Throughput to 400MB/s to be more in line with SSD performance.

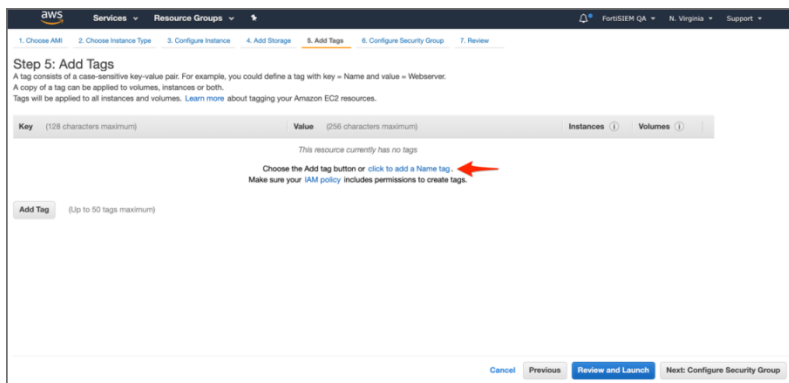
Use these partition values:

Volume Name	Size	Disk Name
EBS Volume 2	100GB	/opt 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.
EBS Volume 3	60GB	/cmdb
EBS Volume 4	60GB	/svn
EBS Volume 5	60GB+	/data (see the following note)

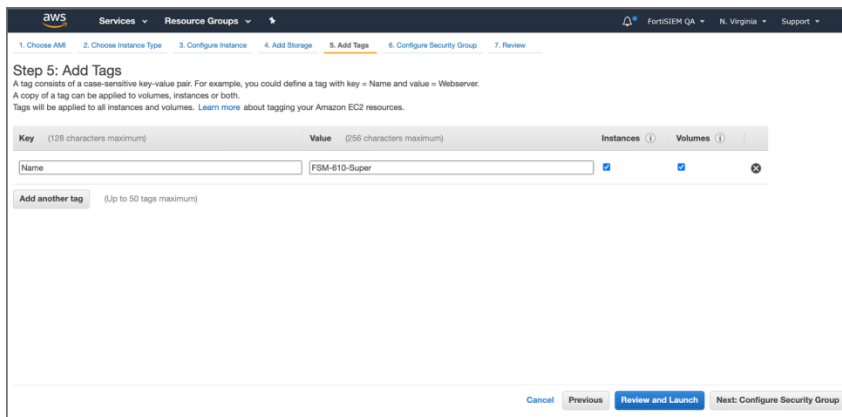
**Note on EBS Volume 5:**

- Add the 5th EBS Volume 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.
- Choose GP3 volume type for all volumes (GP3 is better than GP2 at a slightly lower cost). For the CMDB partition, you can choose to modify your volume type and IOPS based on your system workload if you see the consistently high IOPS requirement in your deployment.

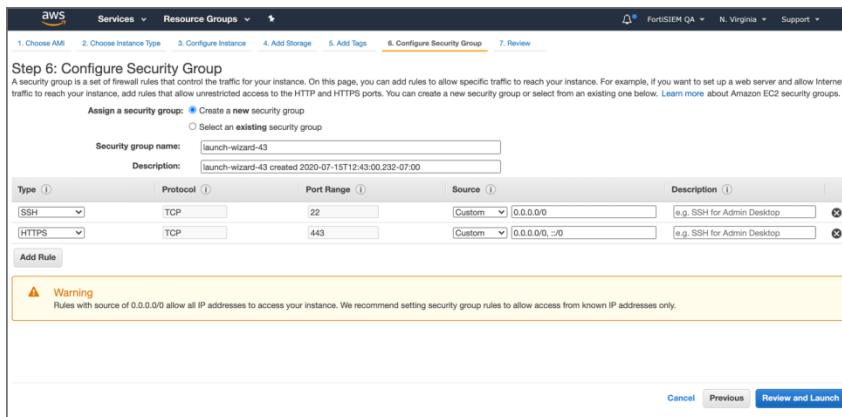
5. In **Step 5: Add Tags**: click **click to add a new Name Tag** and provide a name for the instance. Click **Next**.



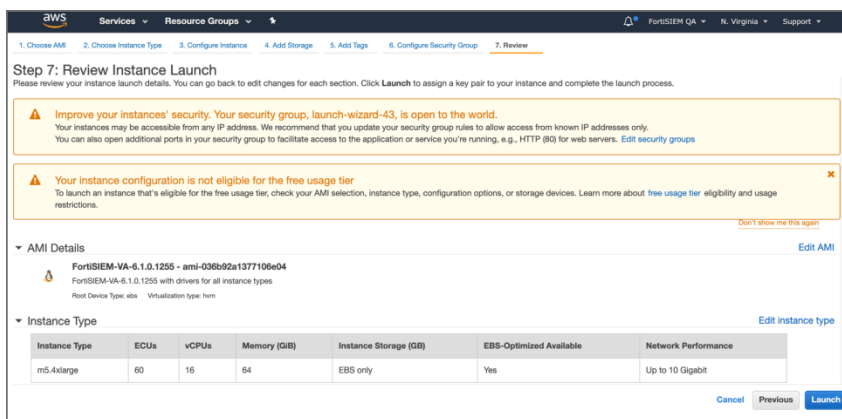
6. Add a new Name Tag.



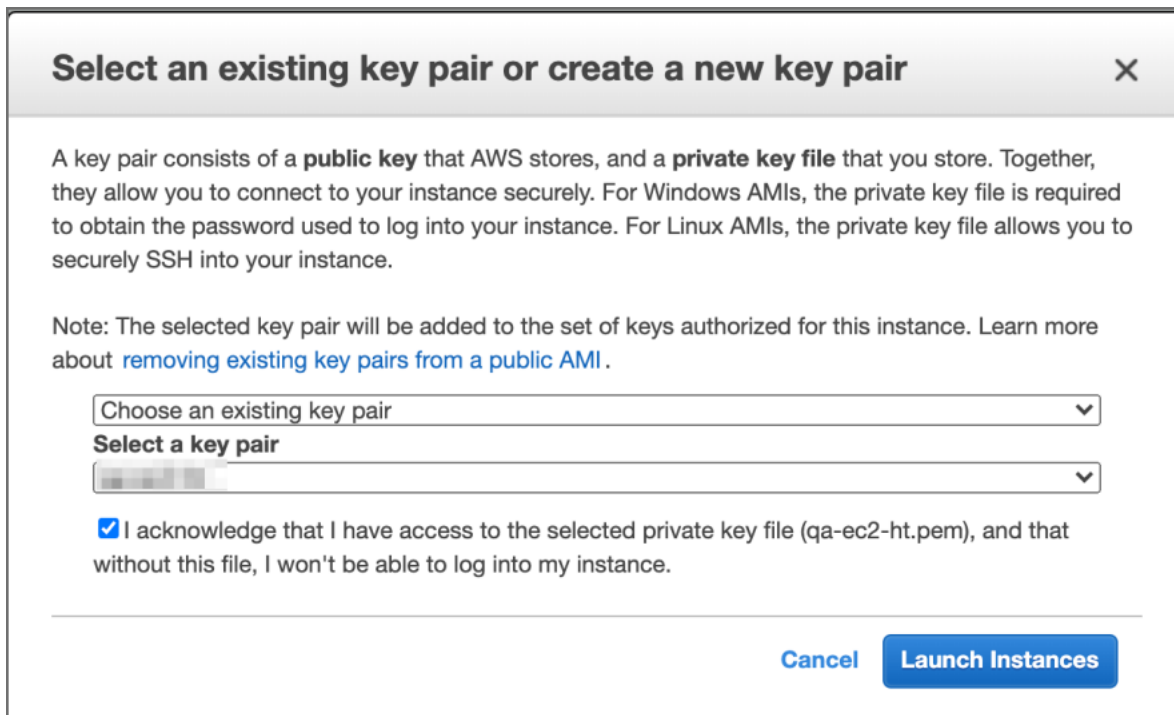
7. In **Step 6: Configure Security Group**, add the allowed inbound protocols for your instance. You will need ssh and https to begin with. Depending on whether this node will receive syslog or other inbound data, you may need to open additional protocols/ports. Click **Review and Launch**.



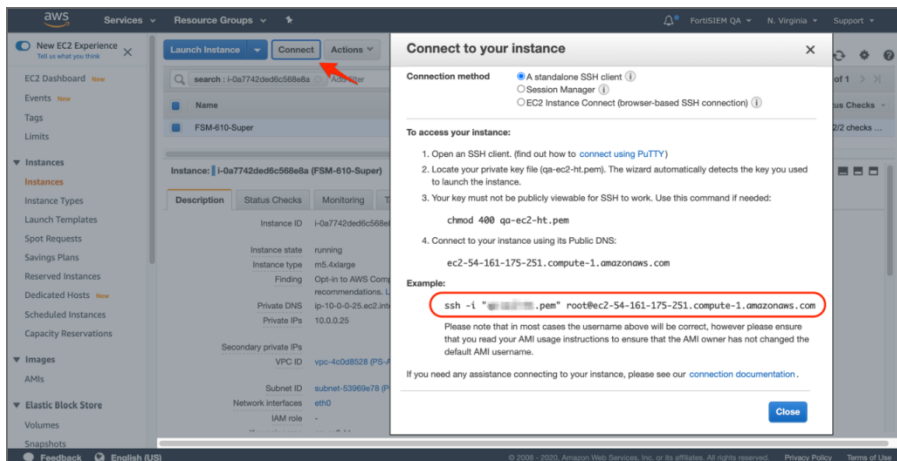
8. In **Step 7: Review Instance Launch**, click **Launch**.



9. Select an existing key pair or create a new key pair, then click **Launch Instances**.



10. Select the instance that you just created and click **Connect**.



11. Using the example above in the **Connect** popup, ssh to the instance you created. Replace `root` user with `ec2-user`. Once logged in, you can execute the `sudo su -` command to become root user.

**Note:** If you are going to assign and use a global IPv6 address to your instance in addition to IPv4, then you will need to perform additional steps and reboot the instance. Take the following steps:

- a. Add the following lines to the file `/etc/sysconfig/network-scripts/ifcfg-eth0`.
 

```
IPV6INIT=yes
IPV6_FAILURE_FATAL=no
```
- b. Run the following command to add service `dhcpv6-client` to the firewall rules (DHCP v6 works differently than v4)
 

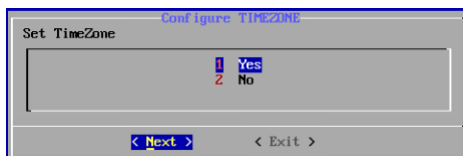
```
firewall-cmd --zone=fortisiem --permanent --add-service=dhcpv6-client
```
- c. Reboot the VM.

## Configure FortiSIEM

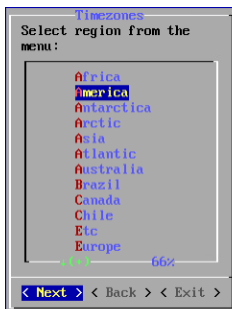
Follow these steps to configure FortiSIEM by using a simple GUI.

1. At the root 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**.



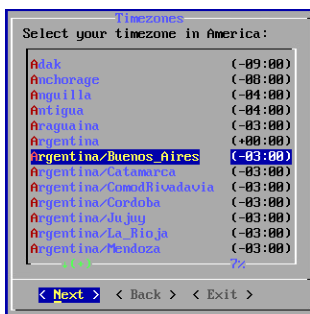
3. Select your **Location**, and press **Next**.



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



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



6. If installing Supervisor, select **1 Supervisor**, and 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.

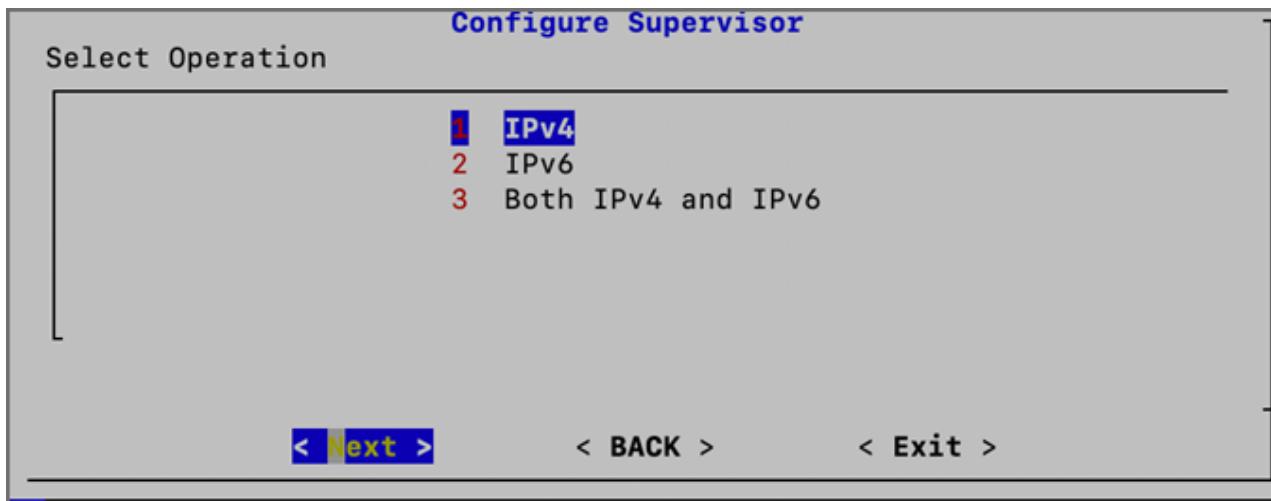
- If you want to enable FIPS, then choose **2 install\_with\_fips**. Otherwise, choose **1 install\_without\_fips**. You have the option of enabling FIPS (option **3**) or disabling FIPS (option **4**) later.

**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.



- Determine whether your network supports IPv4-only, or Both IPv4 and IPv6 (Dual Stack). Choose **1** for IPv4-only, or choose **3** for Both IPv4 and IPv6. Press **Next**.

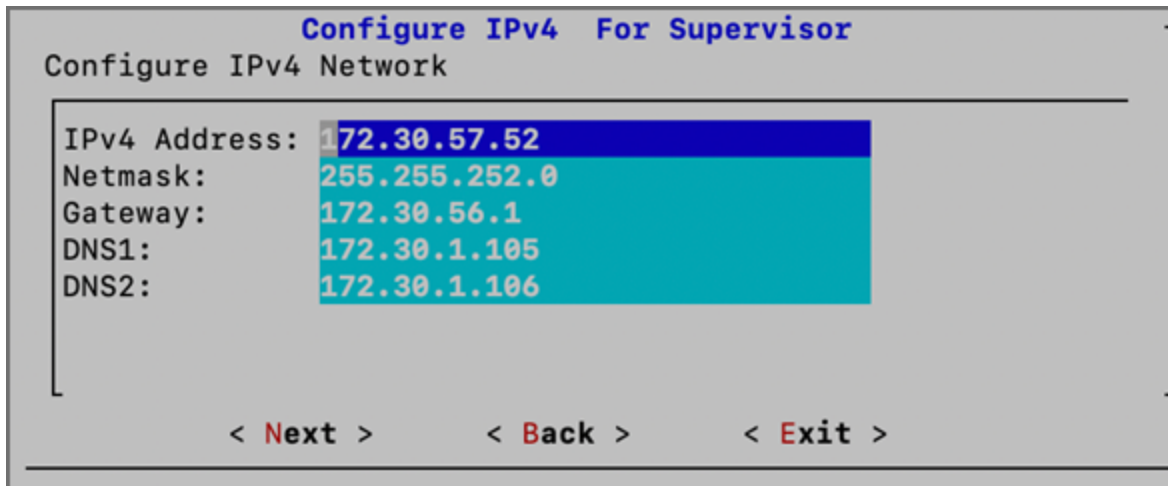
**Note:** In AWS, do not choose option 2 (IPv-6 only), because you will end up with a status check failure. AWS infrastructure currently requires that the VM has an IPv4 address for its monitoring purpose.



- First you will configure the IPv4 network by entering the following fields, then press **Next**.

Option	Description
IPv4 Address	The Manager/Supervisor/Worker/Collector's

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



10. If you chose **1** in step 8, then you will need to skip to step 11. If you chose **3** in step 8, then you will also 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 IPv6 DNS server 1 and 2

```
Configure IPv6 for Supervisor
Configure IPV6 Network

IPv6 Address: 2600:1f18:1014:6520:804d:e099:cd63:c04f
prefix (Netmask): 128
Gateway ipv6: fe80::c0f:cff:fe1e:392d
DNS1 IPv6: 2001:4860:4860::8888
DNS2 IPv6: 2001:4860:4860::8844

< Next >      < Back >      < Exit >
```

**Note:** If you chose option **3** in step 8 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 IPv6 configuration.

**Note:** In AWS 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 such as Google DNS.

11. Configure Hostname for the FortiSIEM Manager, Supervisor, Worker, or Collector, then press **Next**.

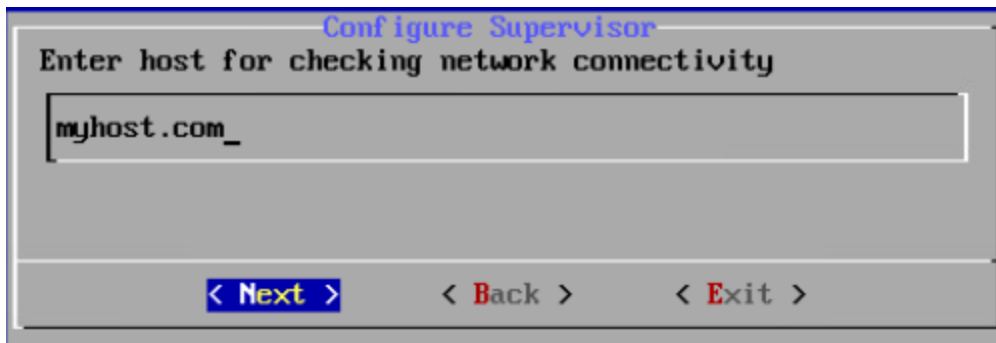
```
Configure Hostname For Supervisor
Configure hostname

Host name: Supervisor-Hostname

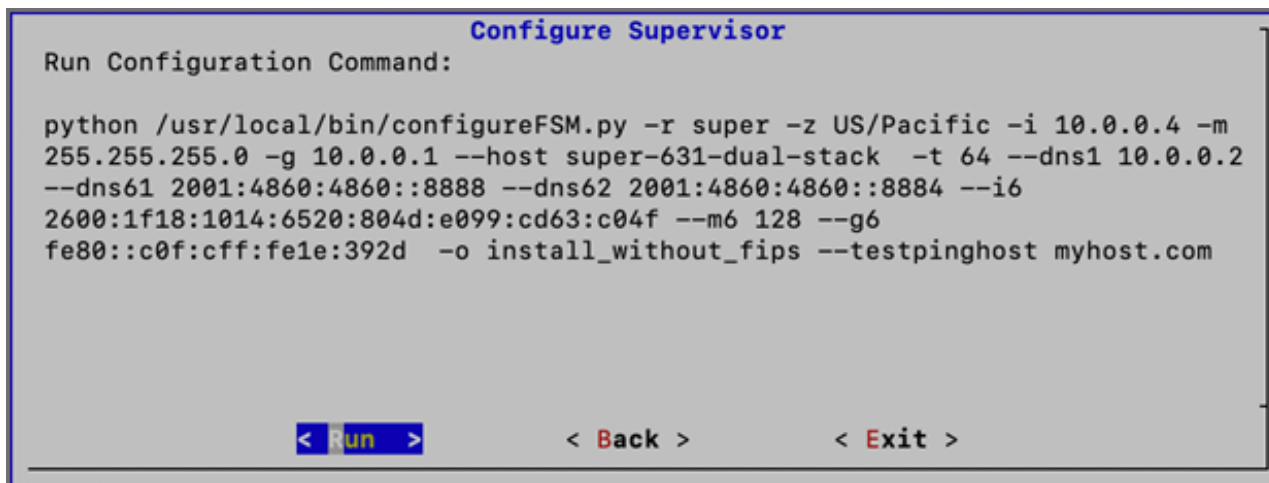
< Next >      < Back >      < Exit >
```

12. 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**.





13. 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 <b>4</b> (for <b>IPv4</b> ) or <b>6</b> (for <b>IPv6</b> ) or <b>64</b> (for both <b>IPv4</b> and <b>IPv6</b> )
--dns1, --dns2	Addresses of the DNS server 1 and DNS server 2.
--i6	IPv6-formatted address
--m6	IPv6 prefix

Option	Description
--g6	IPv6 gateway
-o	Installation option ( <b>install_without_fips</b> , <b>install_with_fips</b> , <b>enable_fips</b> , <b>disable_fips</b> , <b>change_network_config*</b> ) *Option only available after installation.
-z	Time zone. Possible values are <b>US/Pacific</b> , <b>Asia/Shanghai</b> , <b>Europe/London</b> , or <b>Africa/Tunis</b>
--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.

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

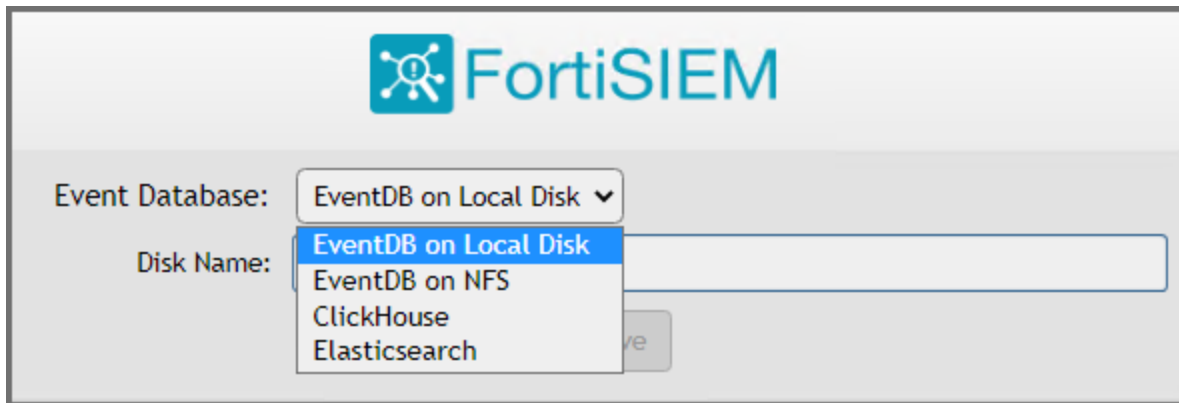
- Click **Browse** and upload the license file.  
Make sure that the **Hardware ID** shown in the License Upload page matches the license.
- For **User ID** and **Password**, choose any **Full Admin** credentials.  
For the first time installation, enter `admin` as the user and `admin*1` as the password. You will then be asked to create a new password for GUI access.
- For Supervisor, Worker, or Collector, choose **License type** as **Enterprise** or **Service Provider**. The following option will be available for first time installations. 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 fields: "Event Database:" and "Disk Name:". The "Event Database:" field has a dropdown menu with "EventDB on Local Disk" selected. The "Disk Name:" field has a dropdown menu with "EventDB on Local Disk", "EventDB on NFS", "ClickHouse", and "Elasticsearch" options. The "EventDB on Local Disk" option is highlighted in blue. To the right of the "Disk Name:" field, there is a text input field and a "Next" 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, 0.0%ni, 91.4%id, 0.0%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                   1432m                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                 01:10:38             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).

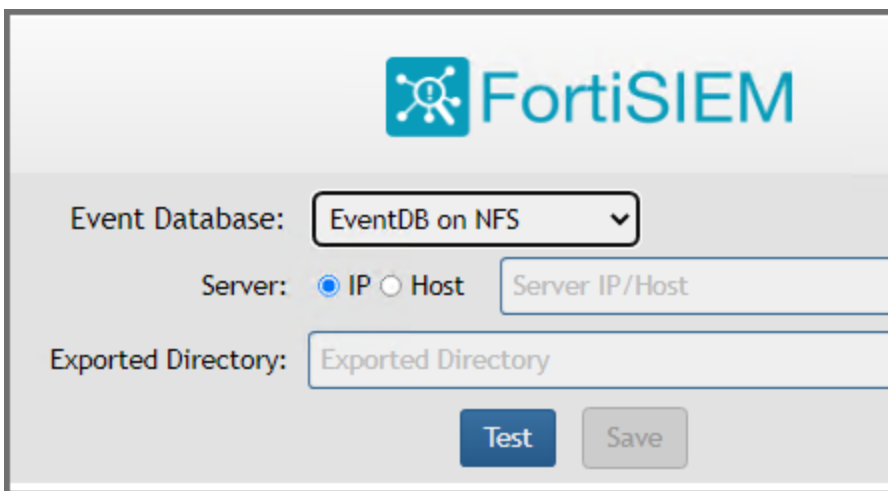
- [Install Supervisor](#)
- [Install Workers](#)
- [Register Workers](#)
- [Create ClickHouse Topology \(Optional\)](#)

- [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. EBS Volume 5 is not required (From [Launch an instance using FortiSIEM 6.7.0 AMI Step 4](#)).
  - b. You need to configure NFS after license upload.



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

3. If you choose **ClickHouse**
  - a. You need to create disks during [Launch an instance using FortiSIEM 6.7.0 AMI Step 4](#) 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 the logo, 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' input field and a 'Row' column with '+' and '-' buttons. At the bottom, there are 'Test' and 'Save' buttons.

- 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 shows 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 set to 5, and the 'Replicas' field is set to 1. The 'Per Org Index' checkbox is unchecked. At the bottom are 'Test' and 'Save' buttons.

## Install Workers

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

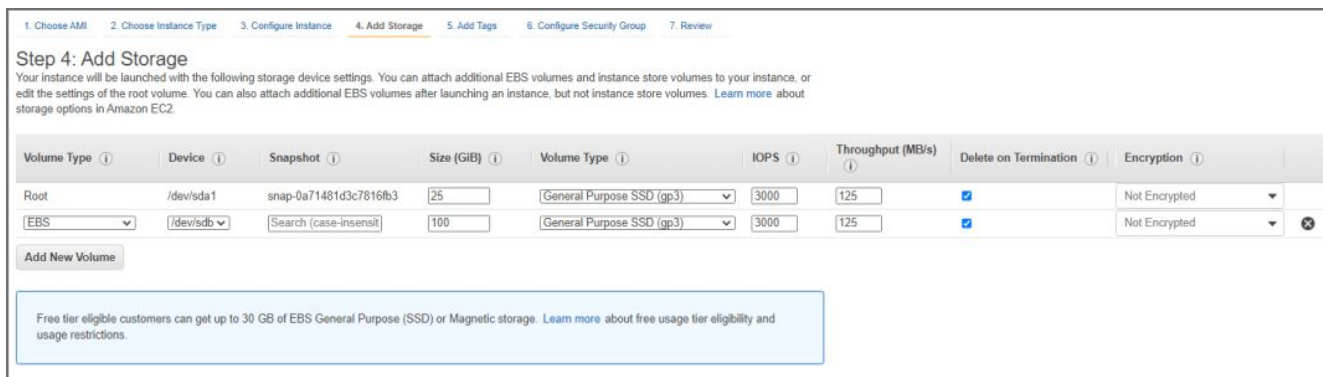
1. Choose appropriate CPU and memory for the Worker nodes based on Sizing guide.
2. Two hard disks for Operating Systems and FortiSIEM Application:
  - OS – 25GB
  - OPT – 100GB

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.

- 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.

- Go to **ADMIN > License > Nodes**.
- Select Worker from the **Mode** drop-down list and enter the following information:
  - In the **Host Name** field, enter the Worker's host name.
  - In the **IP Address** field, enter the Worker's IP address.
  - 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 type="text"/>	/data-clickhouse-hot-1	<input type="button" value="+"/> <input type="button" value="-"/>

**Warm Tier:**

Disk Path	Mounted On	Row
<input type="text"/>	/data-clickhouse-warm-1	<input type="button" value="+"/> <input type="button" value="-"/>

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
- Device Support
- Health
- License
- Settings

Cloud Health
Collector Health

Columns ▼
Lines: 2 Last update at 8:49:17 PM

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

Columns ▼
Process level metrics for wk573.fortinet.com (172.30.57.3) Lines: 17

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		
ohDataMaanaer	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)

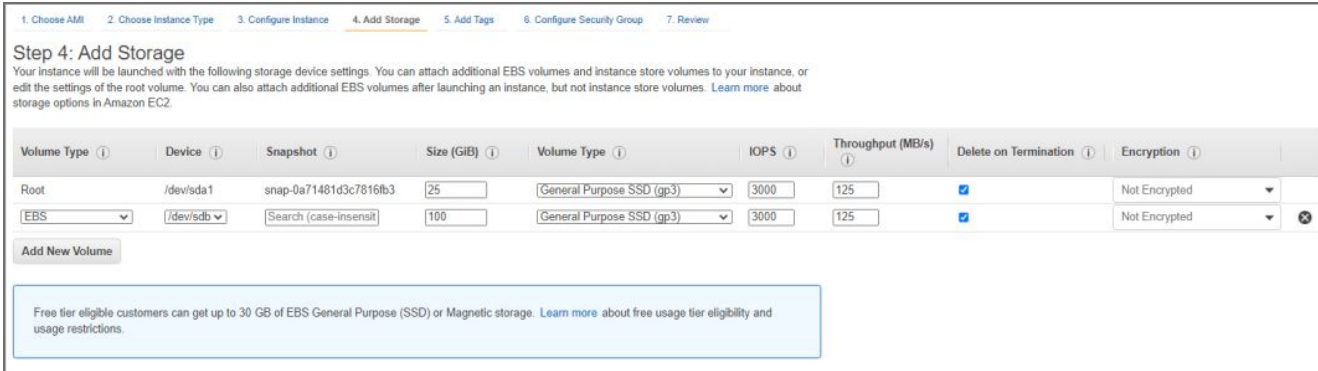
If you are running ClickHouse, you need to configure ClickHouse topology by specifying which nodes belong to ClickHouse Keeper and Data Clusters. Follow the steps in [Configuring ClickHouse Topology](#).

## Install Collectors

Once Supervisor and Workers are installed, follow the same steps in [All-in-one Install](#) to install a Collector except in [Edit FortiSIEM Hardware Settings](#), 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.



Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/sda1	snap-0a71481d3c7816fb3	25	General Purpose SSD (gp3)	3000	125	<input checked="" type="checkbox"/>	Not Encrypted
EBS	/dev/sdb	Search (case-insensit)	100	General Purpose SSD (gp3)	3000	125	<input checked="" type="checkbox"/>	Not Encrypted

## 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.

The screenshot shows the FortiSIEM interface for Collector Health. The top section displays a summary table for the 'Super' collector. Below it, a detailed view shows the status of various 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		

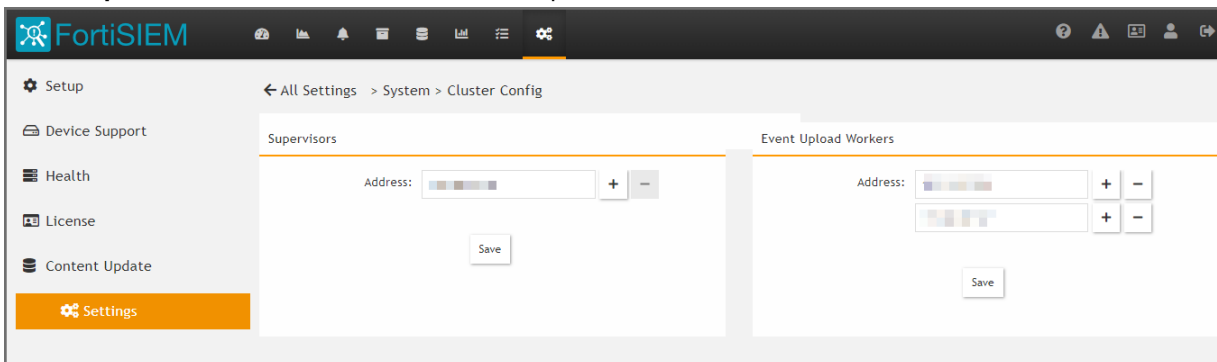
## Service Provider Deployments

For Service Provider deployments, follow these steps.

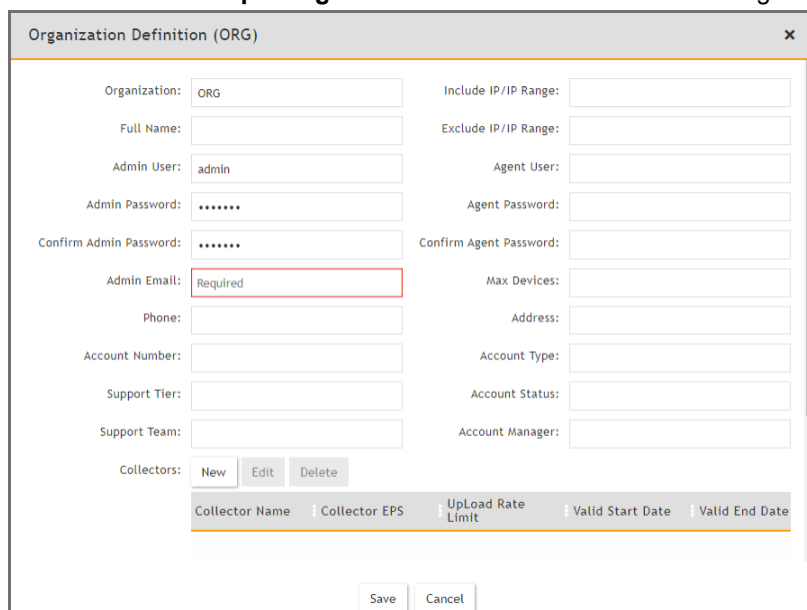
1. Log in to Supervisor with 'Admin' privileges.
2. Go to **ADMIN > Settings > System > Cluster Config**.
  - a. In the **Event Upload Workers** column, enter the IP of the Worker node. If a Supervisor node is only used, then enter the IP of the Supervisor node. Multiple IP addresses can be entered on 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 **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.

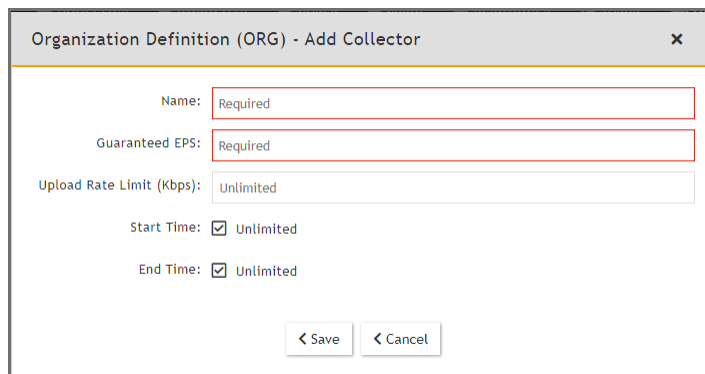


4. Enter the **Organization Name**, **Admin User**, **Admin Password**, and **Admin Email**.

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>
```

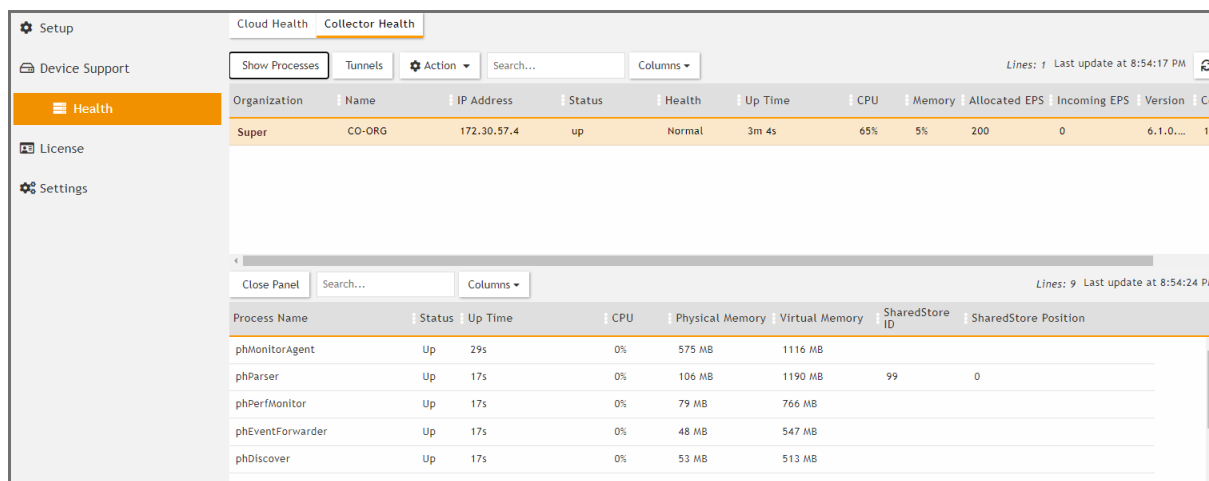
The password should be enclosed in single quotes to ensure that any non-alphanumeric characters are escaped.

- 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.



## 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](#)

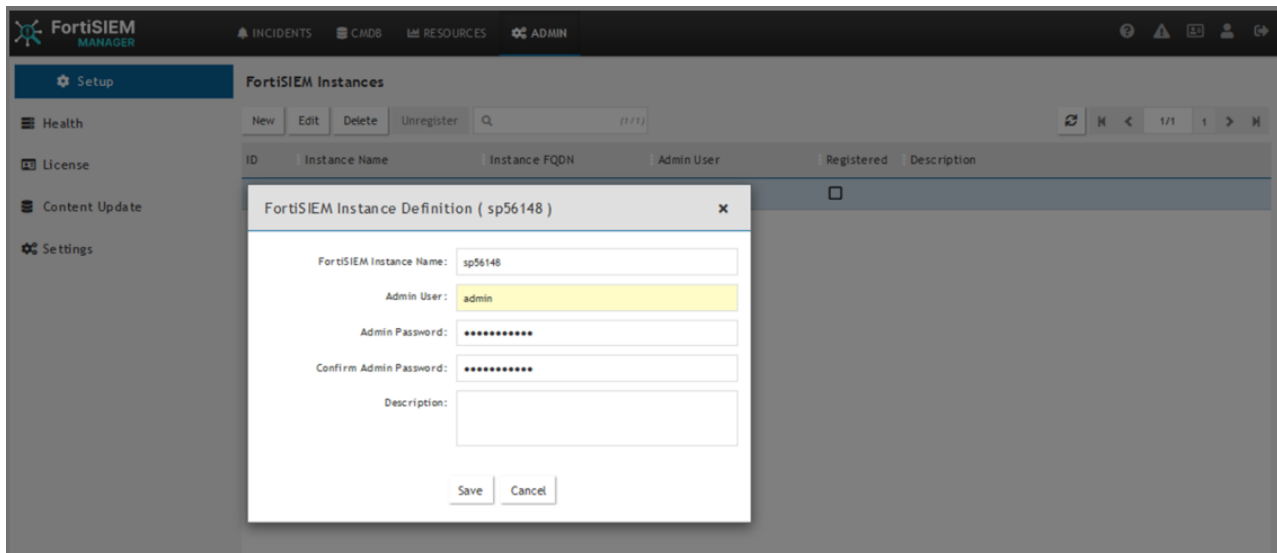
Note that Communication between FortiSIEM Manager and instances is via REST APIs over HTTP(S).

## 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**.



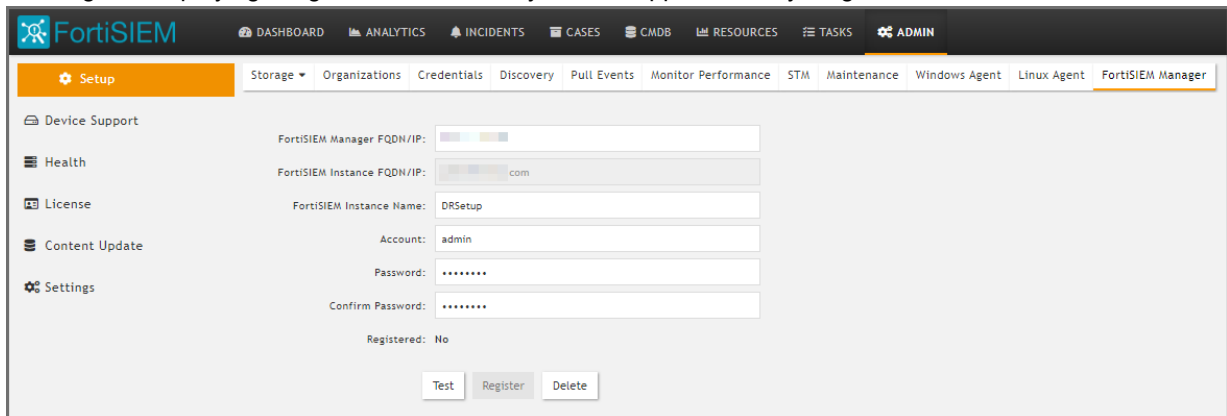
10. Repeat steps 1-9 to add any additional instances to Manager.  
Now, follow the instructions in [Register the Instance Itself to Manager](#) for each instance.

## 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](http://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.