AWS Installation Guide

FortiSIEM 6.2.0

FORTINET

TABLE OF CONTENTS

Change Log

Date	Change Description
05/09/2019	Initial release of ForiSIEM - AWS Installation Guide
03/22/2019	Revision 2: updated instructions for Service Provider deployments.
11/11/2019	Revision 3: small change to installation instructions for FortiSIEM and FortiSIEM Report Server.
03/30/2020	Released document for 5.3.0.
08/15/2020	Revision 4: Updated deployment and installation for FortiSIEM 6.1 on AWS.
10/6/2020	Initial release of AWS Installation and Configuration Guide.
11/03/2020	Revision 5: Release of AWS Installation and Configuration Guide for 6.1.1.
12/03/2020	Revision 6: Small addition to Pre-Installation Checklist.
12/07/2020	Revision 7: Small addition to Register Collectors.
02/04/2021	Revision 8: Migration update.
03/23/2021	Revision 9: Released document for 6.2.0.
04/16/2021	Revision 10: Minor update to Run the Backup Script and Shutdown System section.
04/22/2021	Revision 11: Added Install Log section.
05/07/2021	Revision 12: Released document for 6.2.1.
06/07/2021	Revision 13: Updated Elasticsearch screenshot for 6.2.x guides.
09/28/2021	Revision 14: Updated volume type information for 6.x guides.
11/18/2021	Revision 15: Updated Register Collectors for 6.2.x guides.
08/18/2022	Revision 16: Updated All-in-one Installation section.
10/20/2022	Revision 17: Updated Register Collectors instructions for 6.x guides.

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.
- Deployment type – Enterprise or Service Provider. The Service Provider deployment provides multi-tenancy.
- Whether FIPS should be enabled
- Install type:
    - All-in-one with Supervisor only, or
    - Cluster with Supervisor and Workers
- Storage type
    - Online – Local or NFS or Elasticsearch
    - Archive – NFS or HDFS
- 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.
- Before beginning FortiSIEM deployment, you must configure external storage
- Determine hardware requirements and choose AWS instance type accordingly:

Node	vCPU	RAM	Local Disks
Supervisor (All in one)	Minimum – 12 Recommended - 32	Minimum • without UEBA – 24GB • with UEBA - 32GB Recommended • without UEBA – 32GB • with UEBA - 64GB	OS – 25GB OPT – 100GB CMDB – 60GB SVN – 60GB Local Event database – based on need
Supervisor (Cluster)	Minimum – 12 Recommended - 32	Minimum • without UEBA – 24GB • with UEBA - 32GB Recommended • without UEBA – 32GB • with UEBA - 64GB	OS – 25GB OPT – 100GB CMDB – 60GB SVN – 60GB

Node	vCPU	RAM	Local Disks
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

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

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

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

- *For NFS deployment, see FortiSIEM - NFS Storage Guide here.*
- *For Elasticsearch deployment, see FortiSIEM - Elasticsearch Storage Guide here.*

All-in-one Installation

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

- Launch an instance using FortiSIEM 6.2.0 AMI
- Configure FortiSIEM via GUI
- Upload the FortiSIEM License
- Choose an Event Database

Launch an Instance Using FortiSIEM 6.2.0 AMI

1. Navigate to the EC2 AMIs page and find FortiSIEM 6.2.0 AMI (or in AWS Marketplace after the GA release).
2. Launch FortiSIEM-6.2.0.0219.
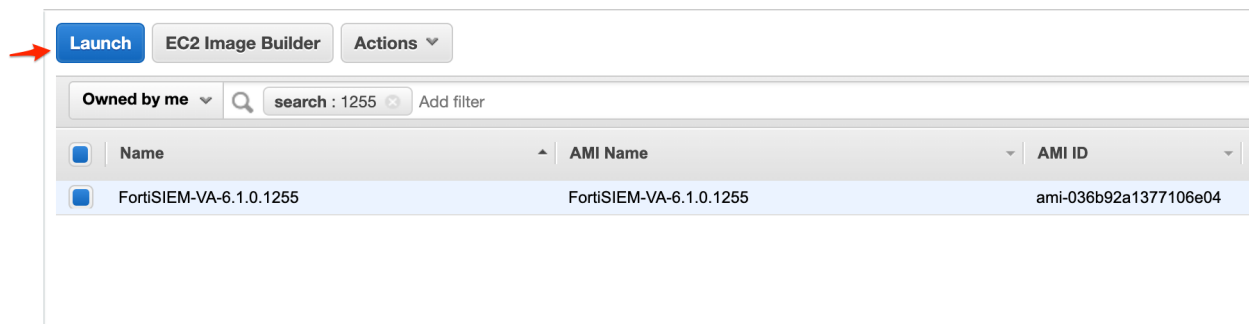
3. Go to **Step 3: Configure Instance Details** in AWS Services. Configure instance details such as VPC, Subnet, IP, etc. Click **Next**.

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.
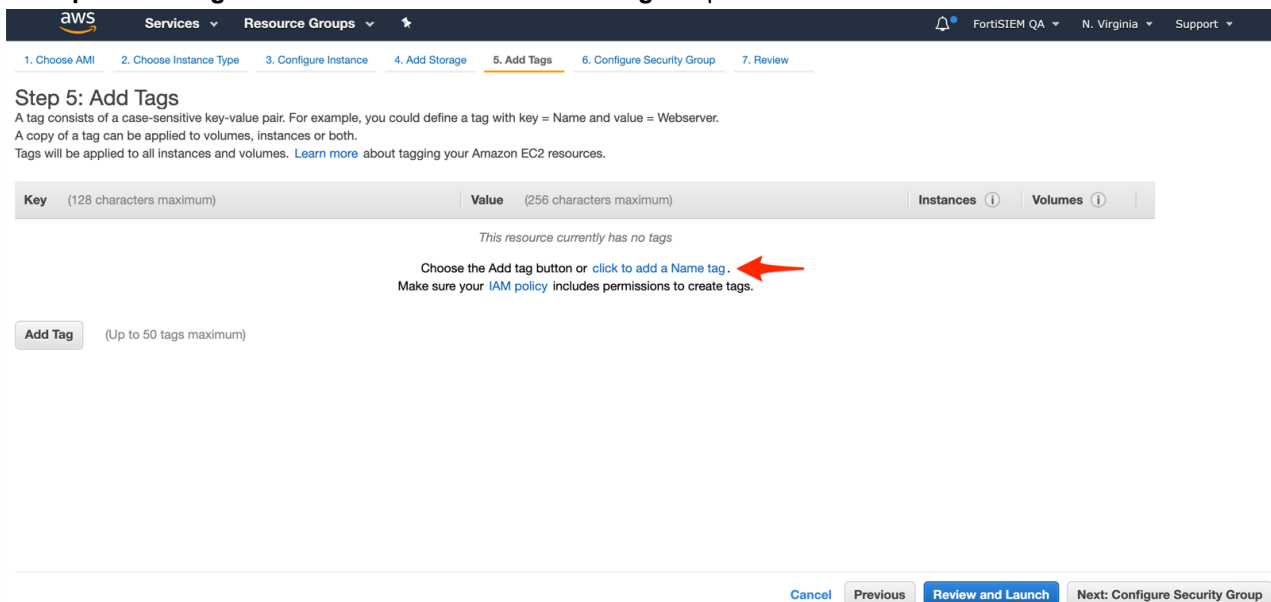
Use these partition values:

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

Add a new Name Tag.

6. 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**.

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

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

9. Select the instance that you just created and click **Connect**.
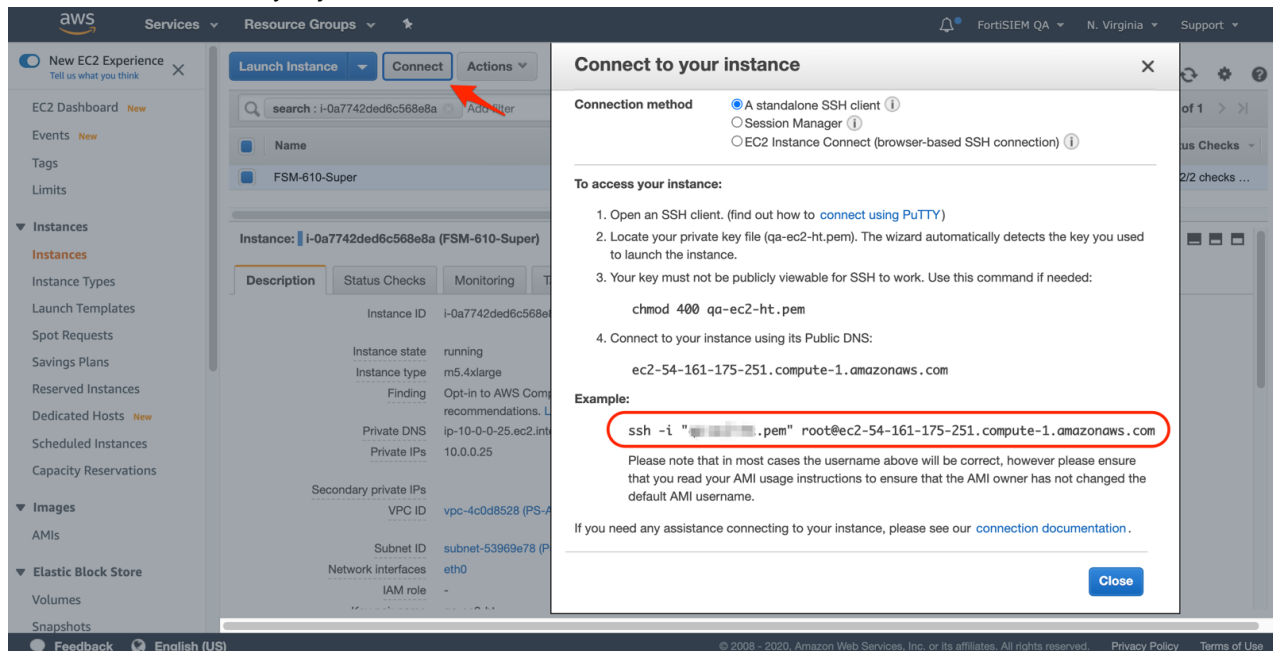
10. Using the example above in the **Connect** popup, ssh to the instance you created. Replace `root` user with `ec2-user`. Once logged in, you can execute the `sudo su -` command to become root user

Configure FortiSIEM via GUI

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**.
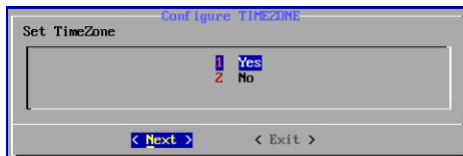
3. Select your **Location**, and press **Next**.
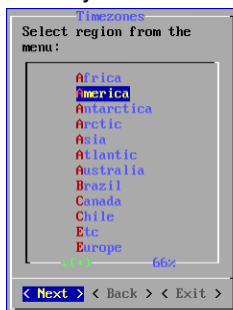
4. Select your **Continent**, and press **Next**.
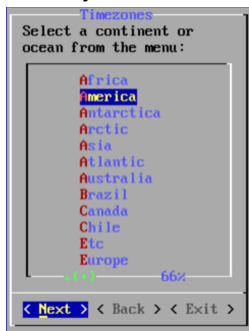
5. Select the **Country** and **City** for your timezone, and press **Next**.
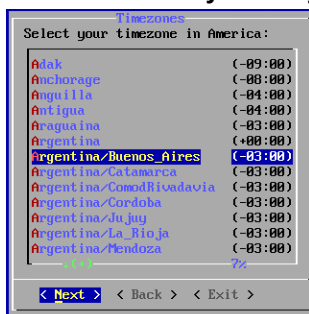
6. Select **1 Supervisor**. Press **Next**.
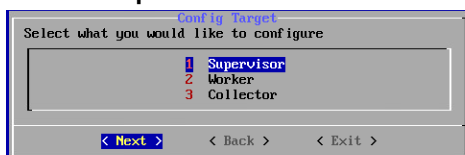
> Regardless of whether you select **Supervisor**, **Worker**, or **Collector**, you will see the same series of screens.

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

8. Configure the network by entering the following fields. Press **Next**.

Option	Description
Host Name	The Supervisor's host name
IPv4 Address	The Supervisor's IPv4 address
NetMask	The Supervisor's subnet
Gateway	Network gateway address
FQDN	Fully-qualified domain name
DNS1, DNS2	Addresses of the DNS servers
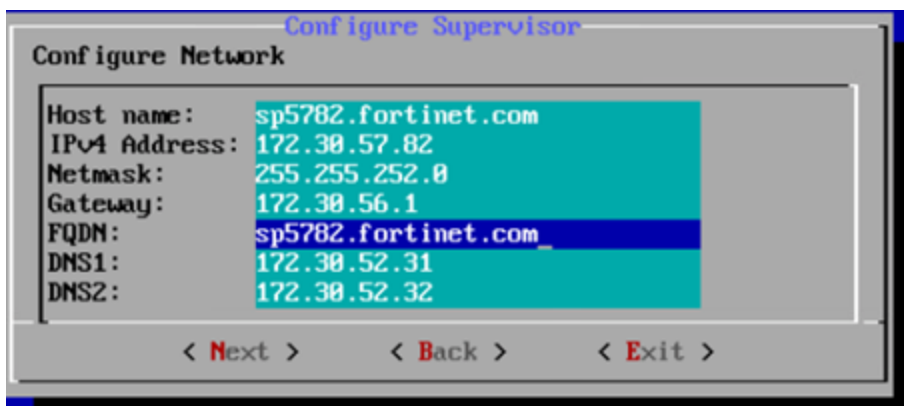
9. Test network connectivity by entering a host name that can be resolved by your DNS Server (entered in the previous step) and can respond to a ping. The host can either be an internal host or a public domain host like google.com. Press **Next**.

10. 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**.

```
                        Configure Supervisor
Run Configuration Command:

python /usr/local/bin/configureFSM.py -r super -z US/Pacific -i 172.30.57.82
-m 255.255.252.0 -g 172.30.56.1 --host sp5782.fortinet.com -f
sp5782.fortinet.com -t 4 --dns1 172.30.52.32 --dns2 172.30.52.31 -o
install_with_fips --testpinghost myhost.com




       < Run  >              < Back >           < Exit >
```

The options are described in the following table.

Option	Description
-r	The FortiSIEM component being configured
-z	The time zone being configured
-i	IPv4-formatted address
-m	Address of the subnet mask
-g	Address of the gateway server used
--host	Host name
-f	FQDN address: fully-qualified domain name
-t	The IP type. The values can be either **4** (for **ipv4**) or **6** (for **v6**) **Note:** the **6** value is not currently supported.
--dns1, --dns2	Addresses of the DNS server 1 and DNS server 2.
-o	Installation option (**install_without_fips**, **install_with_fips**, **enable_fips**, **disable_fips**, **change_ip**, or **migrate_6_1_0**)
-z	Time zone. Possible values are **US/Pacific**, **Asia/Shanghai**, **Europe/London**, or **Africa/Tunis**
--testpinghost	The host used to test connectivity

11. 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.
2. The License Upload dialog box will open.

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

Choose an Event Database

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

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

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

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

The response should be similar to the following.

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

System uptime:  21:12:02 up  1:11,  1 user,  load average: 0.16, 0.20, 0.36
Tasks: 27 total, 0 running, 26 sleeping, 0 stopped, 0 zombie
Cpu(s): 16 cores, 6.2%us, 2.1%sy, 0.0%ni, 91.4%id, 0.0%wa, 0.2%hi, 0.1%si, 0.0%st
Mem: 65702100k total, 10366036k used, 55336064k 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
phRuleMaster         41:41         0           1079m          504m
phRuleWorker         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           603m           67m
phIpIdentityWorker   41:41         0           1027m          58m
phIpIdentityMaster   41:41         0           491m           39m
phAgentManager       41:41         0           1425m          54m
phCheckpoint         42:31         0           325m           34m
phPerfMonitor        41:41         0           702m           70m
phReportLoader       41:41         0           769m           270m
phBeaconEventPackager 41:41        0           1125m          65m
phDataPurger         41:41         0           588m           58m
phEventForwarder     41:41         0           540m           46m
phMonitor            37:24         0           2880m          53m
Apache               01:10:40      0           310m           16m
Node.js-charting     01:10:19      0           916m           71m
Node.js-pm2          01:10:13      0           0              26m
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         438m
Redis                01:10:18      0           55m            25m
```

Cluster Installation

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

- Install Supervisor
- Install Workers
- Register Workers
- Install Collectors
- Register Collectors

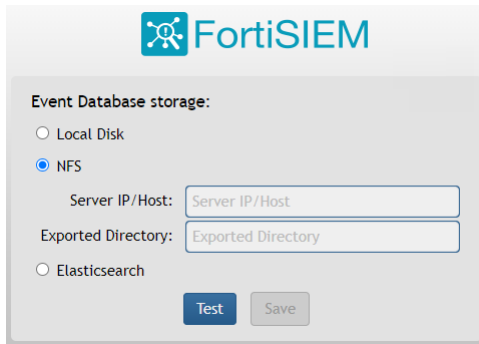# Install Supervisor

Follow the steps in All-in-one Install with two differences:

- Setting up hardware - you do not need to add an EBS Volume 5 for Event database.
- Setting up an Event database - Configure the cluster for either NFS or Elasticsearch.
 **NFS**

Elasticsearch

You must choose external storage listed in Choose an Event Database.

Install Workers

Once the Supervisor is installed, follow the same steps in All-in-one Install to install a Worker except you need to only choose OS and OPT disks. The recommended CPU and memory settings for Worker node, and required hard disk settings are:

- CPU = 8
- Memory = 24 GB
- Two hard disks:
   - OS – 25GB
    - OPT – 100GB
      For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when `configFSM.sh` runs.
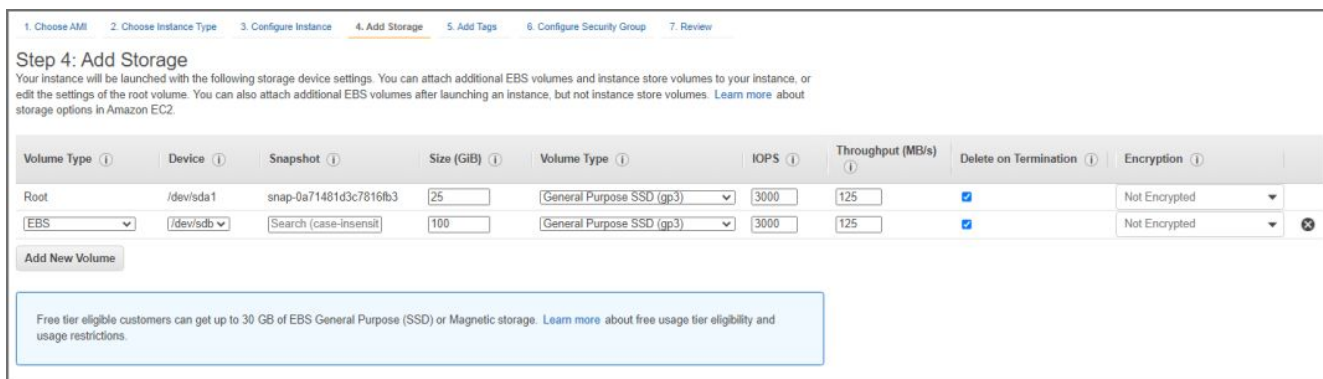
Register Workers

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

1. Go to **ADMIN > License > Nodes**.
2. Select **Worker** from the drop-down list and enter the Worker's IP address. Click **Add**.
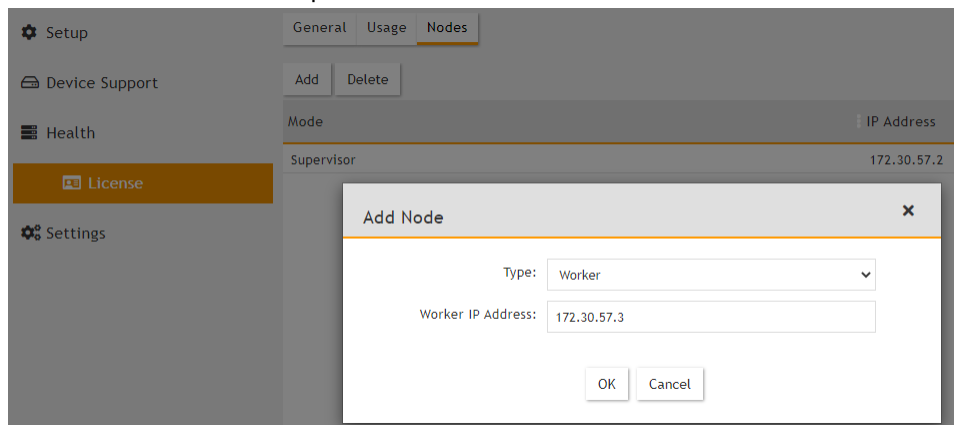
3. See **ADMIN > Health > Cloud Health** to ensure that the Workers are up, healthy, and properly added to the

system.

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 CPU and memory settings for Collector node, and required hard disk settings are:

- CPU = 4
- Memory = 8GB
- Two hard disks:
  - OS – 25GB
  - OPT – 100GB
    For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when `configFSM.sh` runs.

Register Collectors

Collectors can be deployed in Enterprise or Service Provider environments.

- Enterprise Deployments
- Service Provider Deployments

Enterprise Deployments

For Enterprise deployments, follow these steps.

1. Log in to Supervisor with 'Admin' privileges.
2. Go to **ADMIN > Settings > System > Event Worker**.
   a. Enter the IP of the Worker node. If a Supervisor node is only used, then enter the IP of the Supervisor node. Multiple IP addresses can be entered on separate lines. In this case, the Collectors will load balance the upload of events to the listed Event Workers.
   Note: Rather than using IP addresses, a DNS name is recommended. The reasoning is, should the IP addressing change, it becomes a matter of updating the DNS rather than modifying the Event Worker IP addresses in FortiSIEM.
   b. Click **OK**.
3. Go to **ADMIN > Setup > Collectors** and add a Collector by entering:
   a. **Name** – Collector Name
   b. **Guaranteed EPS** – this is the EPS that Collector will always be able to send. It could send more if there is excess EPS available.
   c. **Start Time** and **End Time** – set to **Unlimited**.
4. SSH to the Collector and run following script to register Collectors:
   ```
   phProvisionCollector --add <user> '<password>' <Super IP or Host> <Organization>
   <CollectorName>
   ```
   The password should be enclosed in single quotes to ensure that any non-alphanumeric characters are escaped.
   a. Set `user` and `password` using the admin user name and password for the Supervisor.
   b. Set `Super IP or Host` as the Supervisor's IP address.
   c. Set `Organization`. For Enterprise deployments, the default name is Super.
   d. Set `CollectorName` from Step 2a.
   The Collector will reboot during the Registration.
5. Go to **ADMIN > Health > Collector Health** for the status.
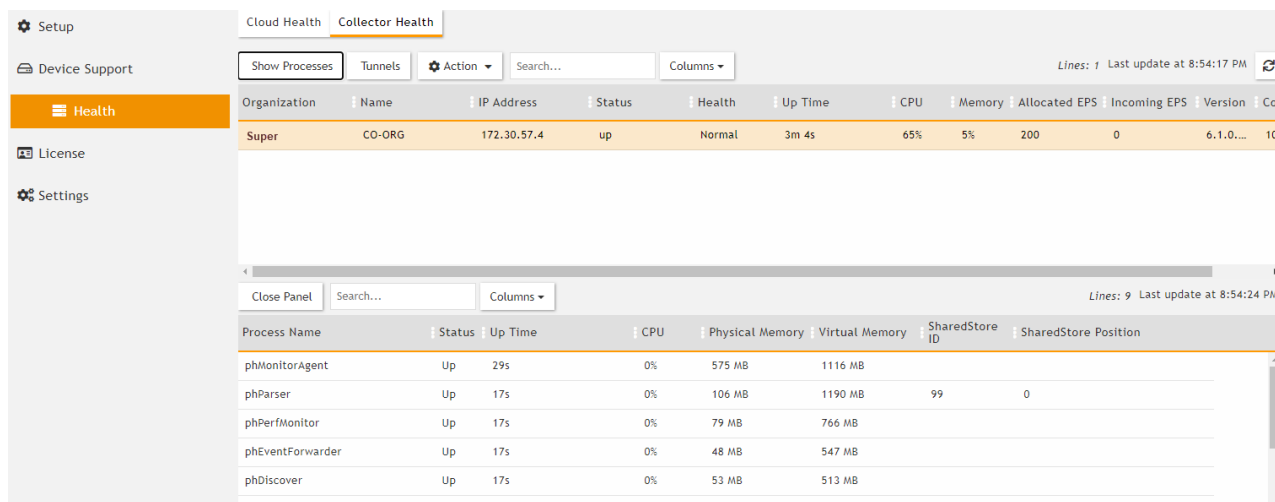
Service Provider Deployments

For Service Provider deployments, follow these steps.

1. Log in to Supervisor with 'Admin' privileges.
2. Go to **ADMIN > Settings > System > Event Worker**.
   a. Enter the IP of the Worker node. If a Supervisor node is only used, then enter the IP of the Supervisor node. Multiple IP addresses can be entered on separate lines. In this case, the Collectors will load balance the upload of events to the listed Event Workers.
   Note: Rather than using IP addresses, a DNS name is recommended. The reasoning is, should the IP addressing change, it becomes a matter of updating the DNS rather than modifying the Event Worker IP addresses in FortiSIEM.
   b. Click **OK**.
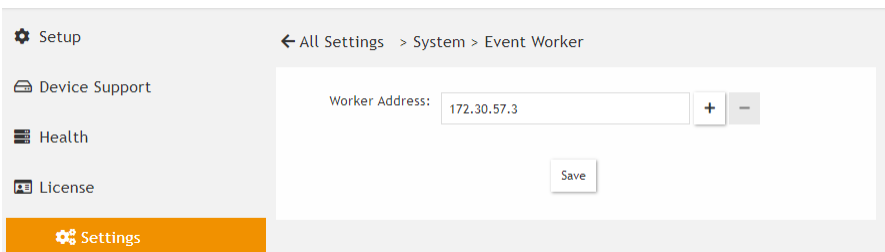
3. Go to **ADMIN > Setup > Organizations** and click **New** to add an Organization.
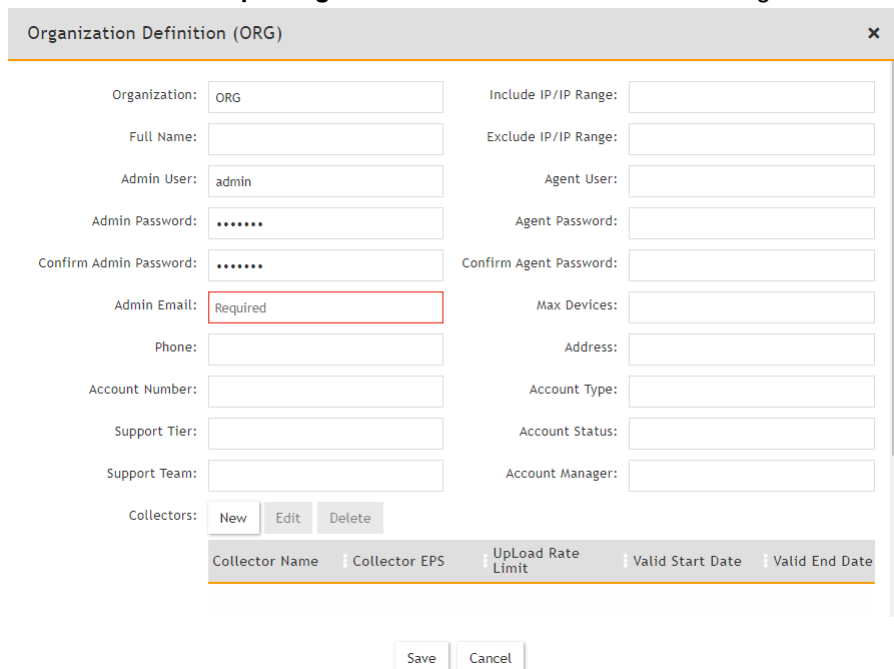
4. Enter the **Organization Name**, **Admin User**, **Admin Password**, and **Admin Email**.
5. Under **Collectors**, click **New**.
6. Enter the **Collector Name**, **Guaranteed EPS**, **Start Time**, and **End Time**.
   The last two values could be set as **Unlimited**. **Guaranteed EPS** is the EPS that the Collector will always be able to send. It could send more if there is excess EPS available.

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

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

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

    a. Set `user` and `password` using the admin user name and password for the Organization that the Collector is going to be registered to.

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

    c. Set `Organization` as the name of an organization created on the Supervisor.

    d. Set `CollectorName` from Step 6.

    The Collector will reboot during the Registration.

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

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.

FORTINET