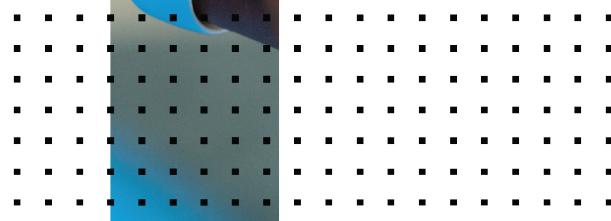
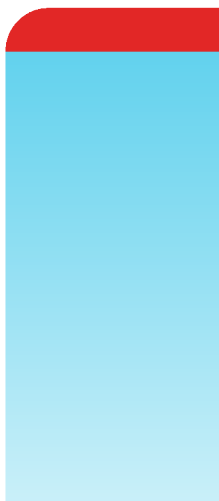


# AWS Installation Guide

FortiSIEM 6.2.1



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



10/04/2023

FortiSIEM 6.2.1 AWS Installation Guide

---

# TABLE OF CONTENTS

<b>Change Log</b> .....	<b>4</b>
<b>Fresh Installation</b> .....	<b>5</b>
Pre-Installation Checklist .....	5
All-in-one Installation .....	6
Launch an Instance Using FortiSIEM 6.2.1 AMI .....	6
Configure FortiSIEM via GUI .....	11
Upload the FortiSIEM License .....	15
Choose an Event Database .....	15
Cluster Installation .....	16
Install Supervisor .....	16
Install Workers .....	18
Register Workers .....	18
Install Collectors .....	19
Register Collectors .....	19
<b>Install Log</b> .....	<b>23</b>

# 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 <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

Node	vCPU	RAM	Local Disks
Workers	Minimum – 8	Minimum – 16GB	OS – 25GB
	Recommended - 16	Recommended – 24GB	OPT – 100GB
Collector	Minimum – 4	Minimum – 4GB	OS – 25GB
	Recommended – 8 ( based on load)	Recommended – 8GB	OPT – 100GB

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

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

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

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

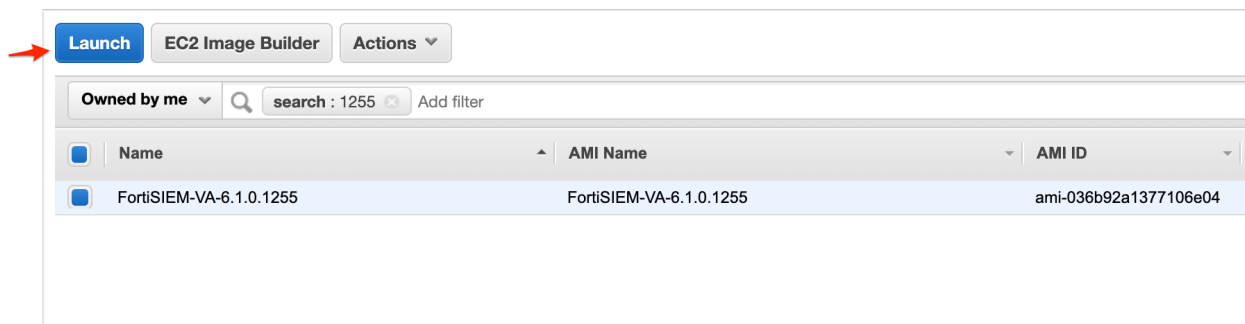
## All-in-one Installation

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

- [Launch an instance using FortiSIEM 6.2.1 AMI](#)
- [Configure FortiSIEM via GUI](#)
- [Upload the FortiSIEM License](#)
- [Choose an Event Database](#)

## Launch an Instance Using FortiSIEM 6.2.1 AMI

1. Navigate to the EC2 AMIs page and find FortiSIEM 6.2.1 AMI (or in AWS Marketplace after the GA release).
2. Launch FortiSIEM-6.2.1.0223.



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

**Step 3: Configure Instance Details**  
 Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

- Number of instances:** 1 (Launch into Auto Scaling Group)
- Purchasing option:**  Request Spot instances
- Network:** vpc-5d4eb938 | Default us-east VPC (Create new VPC)
- Subnet:** subnet-66fdb16a | default-subnet-1f | us-east-1f (Create new subnet) (231 IP Addresses available)
- Auto-assign Public IP:** Use subnet setting (Enable)
- Auto-assign IPv6 IP:** Use subnet setting (Enable)
- Placement group:**  Add instance to placement group
- Placement group name:**  Add to existing placement group.  Add to a new placement group. (scalability (cluster))
- Capacity Reservation:** Open (Create new Capacity Reservation)
- IAM role:** None (Create new IAM role)
- CPU options:**  Specify CPU options
- Shutdown behavior:** Stop
- Stop - Hibernate behavior:**  Enable hibernation as an additional stop behavior
- Enable termination protection:**  Protect against accidental termination
- Monitoring:**  Enable CloudWatch detailed monitoring (Additional charges apply)
- EBS-optimized instance:**  Launch as EBS-optimized instance
- Tenancy:** Shared - Run a shared hardware instance (Additional charges may apply when launching Dedicated instances)
- Elastic Inference:**  Add an Elastic Inference accelerator (Additional charges apply)
- File systems:** Add file system (Create new file system)

Buttons: Cancel, Previous, **Review and Launch**, Next: Add Storage

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**.

**Step 4: Add Storage**  
 Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/sda1	snap-0b341032a6aa1b17a	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 type="checkbox"/>	Not Encrypted
EBS	/dev/sdc	Search (case-insensit)	60	General Purpose SSD (gp3)	3000	125	<input type="checkbox"/>	Not Encrypted
EBS	/dev/sdd	Search (case-insensit)	60	General Purpose SSD (gp3)	3000	125	<input type="checkbox"/>	Not Encrypted

Buttons: Add New Volume

**General Purpose (SSD) volumes provide the ability to burst to 3000 IOPS per volume, independent of volume size, to meet the performance needs of most applications and also deliver a consistent baseline of 3 IOPS/GiB. Set my root volume to General Purpose (SSD).**  
 Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

**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.

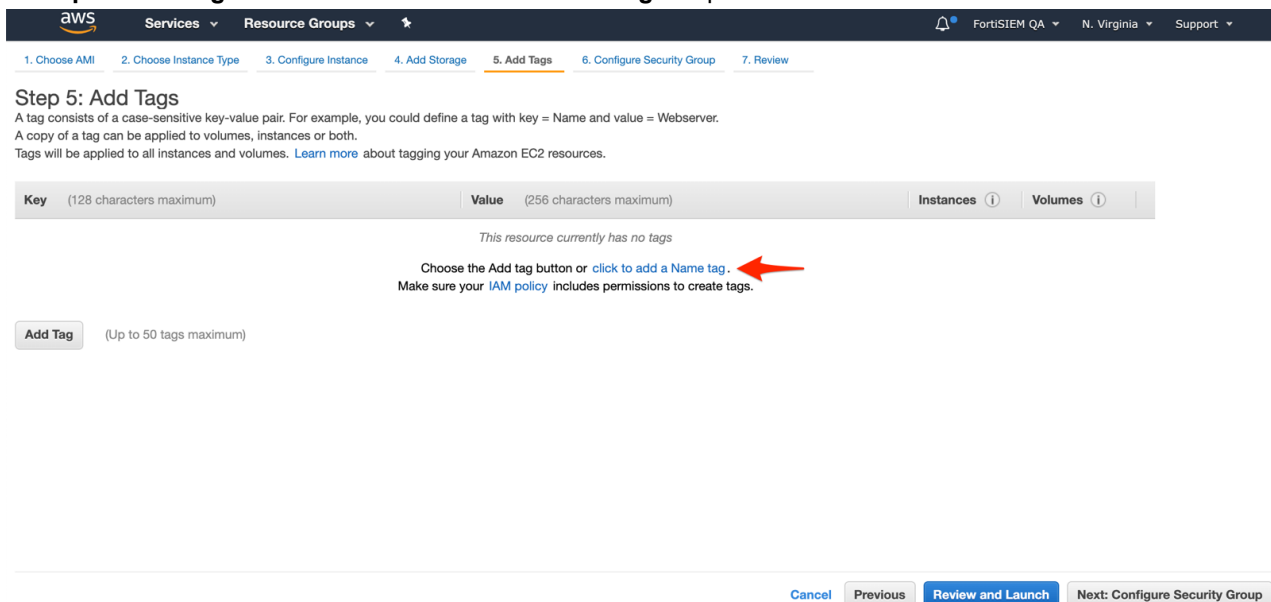
Use these partition values:

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.

**Step 5: Add Tags**  
 A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.  
 A copy of a tag can be applied to volumes, instances or both.  
 Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key	Value	Instances	Volumes
Name	FSM-610-Super	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Add another tag** (Up to 50 tags maximum)

Cancel Previous **Review and Launch** Next: Configure Security Group

- 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**.

**Step 6: Configure Security Group**  
 A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group:  Create a new security group  
 Select an existing security group

Security group name: launch-wizard-43  
 Description: launch-wizard-43 created 2020-07-15T12:43:00.232-07:00

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop
HTTPS	TCP	443	Custom 0.0.0.0, ::/0	e.g. SSH for Admin Desktop

**Add Rule**

**Warning**  
 Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Cancel Previous **Review and Launch**

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

**Step 7: Review Instance Launch**  
Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

**Warning:** Improve your instances' security. Your security group, launch-wizard-43, is open to the world. Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

**Warning:** Your instance configuration is not eligible for the free usage tier. To launch an instance that's eligible for the free usage tier, check your AMI selection, instance type, configuration options, or storage devices. Learn more about [free usage tier](#) eligibility and usage restrictions. [Don't show me this again](#)

**AMI Details** [Edit AMI](#)  
FortiSIEM-VA-6.1.0.1255 - ami-036b92a1377106e04  
FortiSIEM-VA-6.1.0.1255 with drivers for all instance types  
Root Device Type: ebs Virtualization type: hvm

**Instance Type** [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
m5.4xlarge	60	16	64	EBS only	Yes	Up to 10 Gigabit

[Cancel](#) [Previous](#) [Launch](#)

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

**Select an existing key pair or create a new key pair** ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

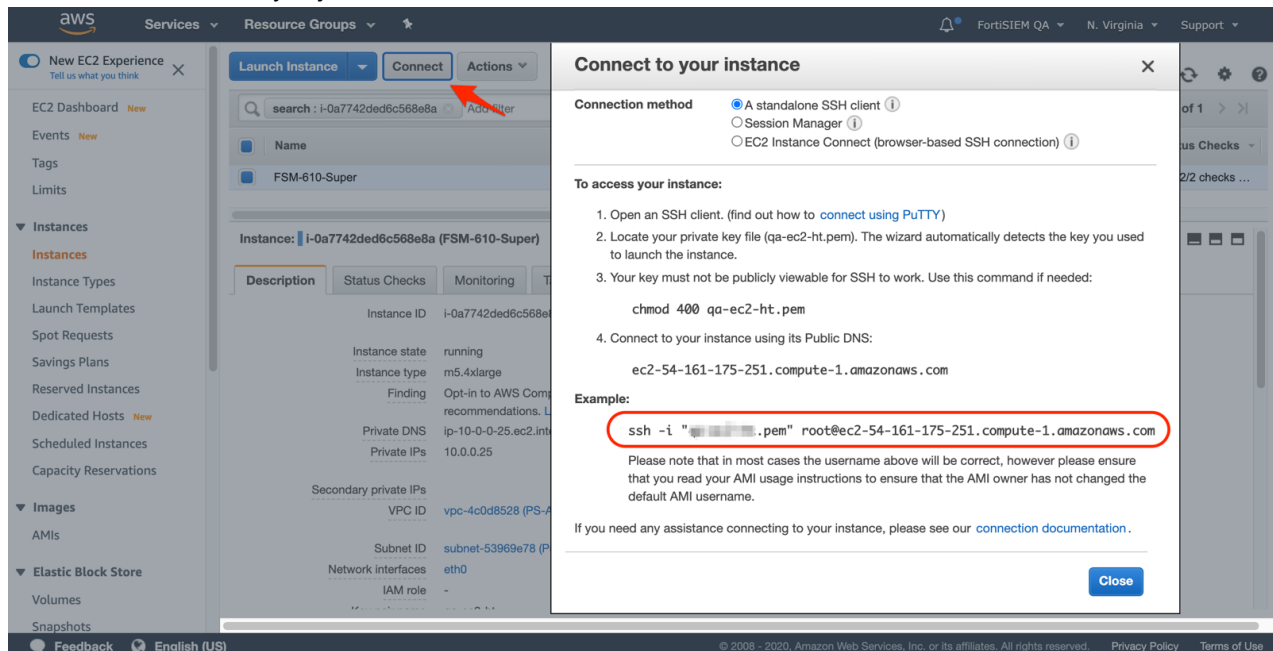
Choose an existing key pair ▼

**Select a key pair**

I acknowledge that I have access to the selected private key file (qa-ec2-ht.pem), and that without this file, I won't be able to log into my instance.

[Cancel](#) [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

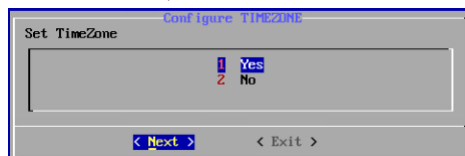
## Configure FortiSIEM via GUI

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

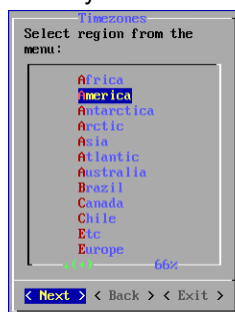
1. At the `root` command prompt, go to `/usr/local/bin` and enter `configFSM.sh`, for example:

```
# configFSM.sh
```

2. In VM console, select **1 Set Timezone** and then press **Next**.



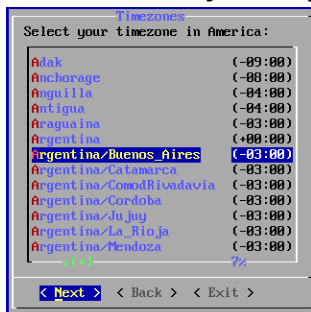
3. Select your **Location**, and press **Next**.



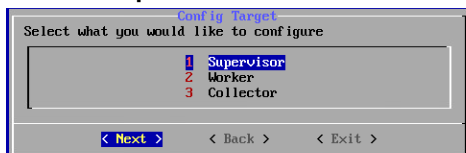
4. Select your **Continent**, and press **Next**.



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

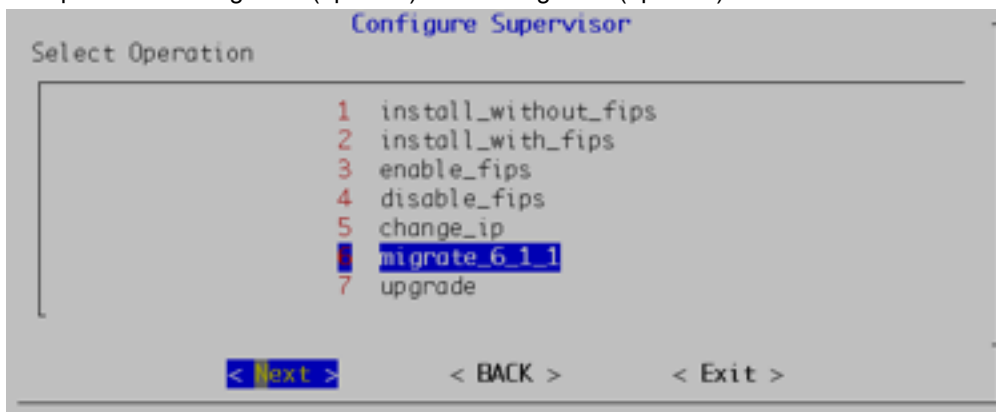


6. Select **1 Supervisor**. Press **Next**.



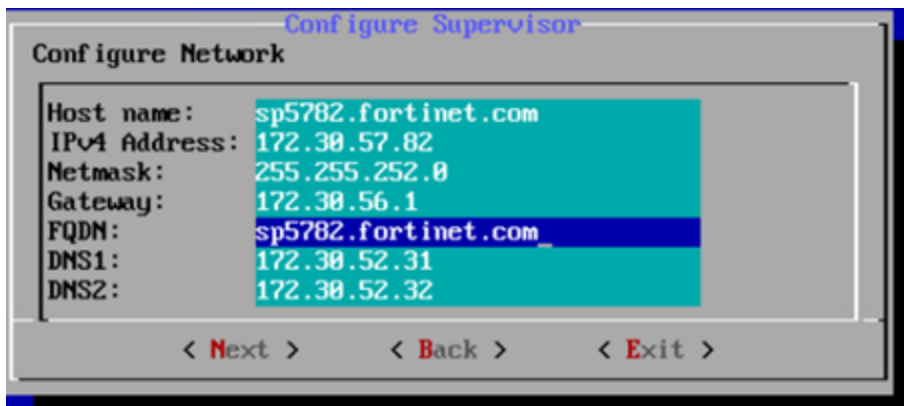
Regardless of whether you select **Supervisor**, **Worker**, or **Collector**, you will see the same series of screens.

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.



- 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



- 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**.



- 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 <b>4</b> (for <b>ipv4</b> ) or <b>6</b> (for <b>v6</b> ) <b>Note:</b> the <b>6</b> value is not currently supported.
--dns1, --dns2	Addresses of the DNS server 1 and DNS server 2.
-o	Installation option ( <b>install_without_fips</b> , <b>install_with_fips</b> , <b>enable_fips</b> , <b>disable_fips</b> , <b>change_ip</b> , or <b>migrate_6_1_0</b> )
-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 host used to test connectivity

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

## Upload the FortiSIEM License



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

You will now be asked to input a license.

1. Open a Web browser and log in to the FortiSIEM UI.
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/phenix/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: 65782100k total, 10366036k used, 55336064k free, 4352k buffers
Swap: 2621436k total, 0k used, 2621436k free, 2469820k 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              1303m          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
phIdentityWorker  41:41           0              1027m          50m
phIdentityMaster  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
phBackendPackager 41:41           0              1125m          65m
phDataPurger      41:41           0              580m           58m
phEventForwarder  41:41           0              540m           46m
phMonitor         37:24           0              2000m          53m
apache            01:10:40        0              310m           16m
Node.js-charting  01:10:19        0              910m           71m
Node.js-pm2       01:10:13        0              0              26m
AppSvc            01:10:07        0              15172m         3026m
DBSvc             01:10:38        0              317m           30m
phInomaJy        01:00:07        0              307m           64m
phFortiInsightAI 01:10:40        0              23432m         430m
Redis             01:10:10        0              55m            25m
```

## Cluster Installation

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

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

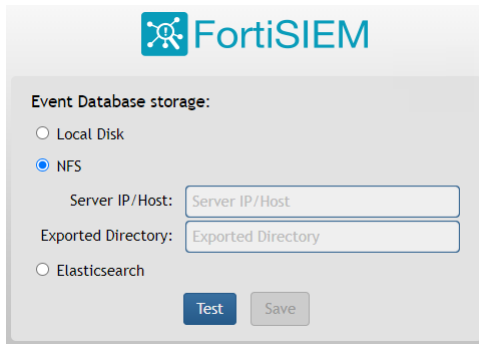
## Install Supervisor

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

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

### NFS





**FortiSIEM**

Event Database storage:

- Local Disk
- NFS
- Elasticsearch

Server IP/Host:

Exported Directory:

### Elasticsearch



**FortiSIEM**

Event Database storage:

- Local Disk
- NFS
- Elasticsearch

ES Service Type:  Native  Amazon  Elastic Cloud

URL:

REST Port:

User Name:

Password:

Confirm Password:

Shard Allocation:  Fixed  Dynamic

Shards:

Replicas:

Per Org Index

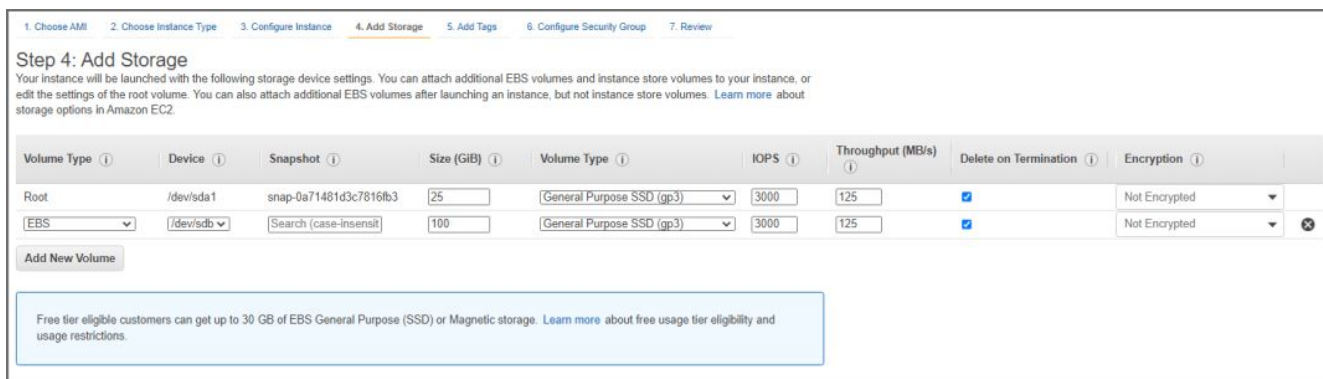
You must choose external storage listed in [Choose an Event Database](#).

## 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

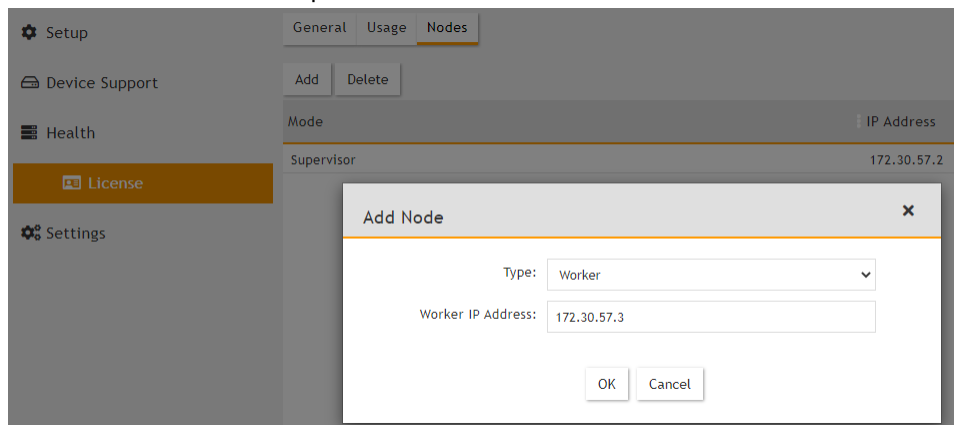
For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when `configFSM.sh` runs.



## 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.

The screenshot shows the FortiSIEM system health interface. On the left is a navigation menu with 'Health' selected. The main area is divided into two sections. The top section, 'Collector Health', displays a table with columns: Name, IP Address, Module Role, Health, Version, Load Average, CPU, and Swap Used. It lists two collectors: 'sp572.fortinet.com' (Supervisor, Normal) and 'wk573.fortinet.com' (Worker, Normal). The bottom section, 'Process level metrics for wk573.fortinet.com (172.30.57.3)', shows a table with columns: Process Name, Status, Up Time, CPU, Physical Memory, Virtual Memory, SharedStore ID, and SharedStore Position. Processes listed include Node.js-charting, httpd, Redis, Node.js-pm2, rsyslogd, and ohDataManaeer.

## 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.

The screenshot shows the AWS console 'Step 4: Add Storage' configuration screen. It includes a progress bar at the top with steps: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage (active), 5. Add Tags, 6. Configure Security Group, 7. Review. Below the progress bar is the title 'Step 4: Add Storage' and a brief description. A table lists storage configurations for 'Root' and 'EBS' volumes. The 'Root' volume is 25 GB, General Purpose SSD (gp3), 3000 IOPS, 125 MB/s throughput, and is not encrypted. The 'EBS' volume is 100 GB, General Purpose SSD (gp3), 3000 IOPS, 125 MB/s throughput, and is not encrypted. There is an 'Add New Volume' button and a note about free tier eligibility.

## 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.

The screenshot shows the 'Collector Health' page in FortiSIEM. It features a table with columns for Organization, Name, IP Address, Status, Health, Up Time, CPU, Memory, Allocated EPS, Incoming EPS, Version, and Col. Below this is a detailed view of processes with columns for Process Name, Status, Up Time, CPU, Physical Memory, Virtual Memory, SharedStore ID, and SharedStore Position.

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

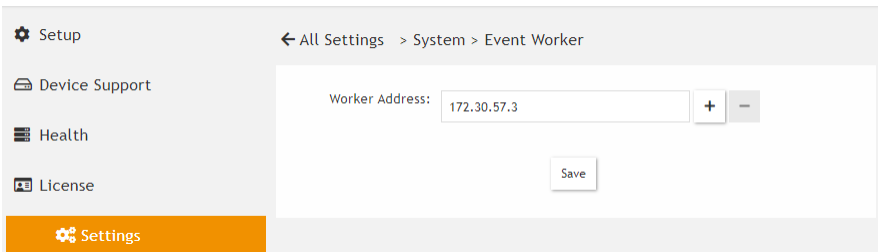
Process Name	Status	Up Time	CPU	Physical Memory	Virtual Memory	SharedStore ID	SharedStore Position
phMonitorAgent	Up	29s	0%	575 MB	1116 MB		
phParser	Up	17s	0%	106 MB	1190 MB	99	0
phPerfMonitor	Up	17s	0%	79 MB	766 MB		
phEventForwarder	Up	17s	0%	48 MB	547 MB		
phDiscover	Up	17s	0%	53 MB	513 MB		

## Service Provider Deployments

For Service Provider deployments, follow these steps.

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

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



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

4. Enter the **Organization Name**, **Admin User**, **Admin Password**, and **Admin Email**.
5. Under **Collectors**, click **New**.
6. Enter the **Collector Name**, **Guaranteed EPS**, **Start Time**, and **End Time**.  
 The last two values could be set as **Unlimited**. **Guaranteed EPS** is the EPS that the Collector will always be able to send. It could send more if there is excess EPS available.

**Organization Definition (ORG) - Add Collector** ✕

---

Name:

Guaranteed EPS:

Upload Rate Limit (Kbps):

Start Time:  Unlimited

End Time:  Unlimited

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

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

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

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

```
root@co574 ~# phProvisionCollector
Usage: phProvisionCollector --add <Organization-user-name> <Organization-user-password> <Supervisor-IP> <Organization-name> <Collector-name>
root@co574 ~# phProvisionCollector --add admin Admin=11.172.30.57.2 ORG CO-ORG
Continuing to provision the Collector
This collector is registered successfully. Normal Exit and restart of phMonitor after collector license registration.
root@co574 ~# _
```

The Collector will reboot during the Registration.

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

The screenshot shows the 'Collector Health' page in FortiSIEM. It features a table with columns: Organization, Name, IP Address, Status, Health, Up Time, CPU, Memory, Allocated EPS, Incoming EPS, Version, and Col. The table lists one collector: 'Super' with name 'CO-ORG', IP '172.30.57.4', status 'up', and health 'Normal'. Below this is a detailed view of processes with columns: Process Name, Status, Up Time, CPU, Physical Memory, Virtual Memory, SharedStore ID, and SharedStore Position. The process list includes phMonitorAgent, phParser, phPerfMonitor, phEventForwarder, and phDiscover.

## 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.