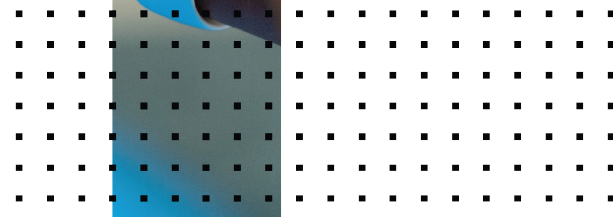
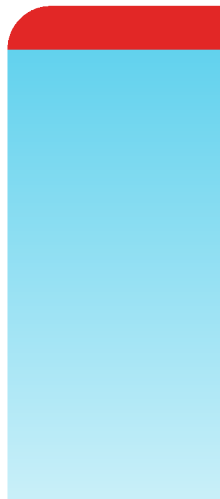


AWS Installation Guide

FortiSIEM 6.3.3



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

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

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



10/04/2023

FortiSIEM 6.3.3 AWS Installation Guide

TABLE OF CONTENTS

Change Log	4
Fresh Installation	5
Pre-Installation Checklist	5
All-in-one Installation	6
Launch an Instance Using FortiSIEM 6.3.3 AMI	7
Configure FortiSIEM via GUI	11
Upload the FortiSIEM License	16
Choose an Event Database	17
Cluster Installation	18
Install Supervisor	18
Install Workers	19
Register Workers	20
Install Collectors	21
Register Collectors	21
Install Log	25

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.
07/06/2021	Revision 14: Released document for 6.3.0.
08/26/2021	Revision 15: Released document for 6.3.1.
09/28/2021	Revision 16: Updated volume type information for 6.x guides.
10/15/2021	Revision 17: Released document for 6.3.2.
11/17/2021	Revision 18: Updated Register Collectors instructions for 6.x guides.
12/22/2021	Revision 19: Released document for 6.3.3.
10/20/2022	Revision 20: 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">• without UEBA – 24GB• with UEBA - 32GB Recommended <ul style="list-style-type: none">• without UEBA – 32GB• with UEBA - 64GB	OS – 25GB OPT – 100GB CMDDB – 60GB SVN – 60GB Local Event database – based on need
Supervisor (Cluster)	Minimum – 12 Recommended - 32	Minimum <ul style="list-style-type: none">• without UEBA – 24GB• with UEBA - 32GB Recommended <ul style="list-style-type: none">• without UEBA – 32GB• with UEBA - 64GB	OS – 25GB OPT – 100GB CMDDB – 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](#).

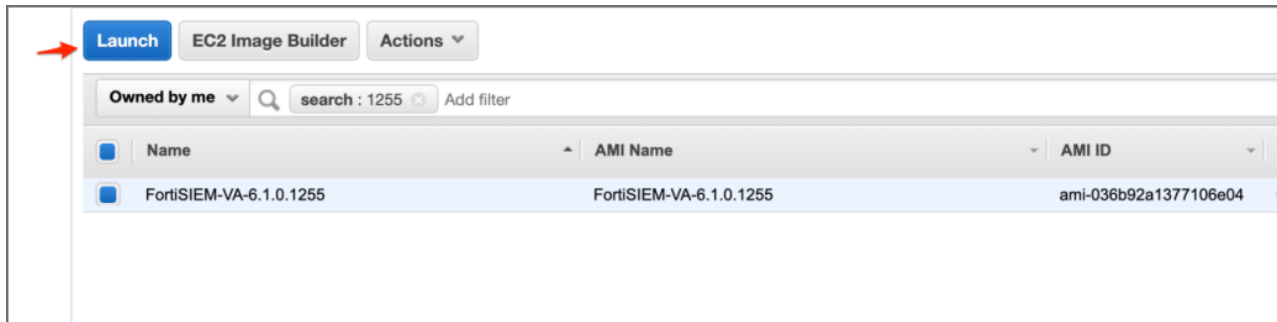
All-in-one Installation

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 6.3.3 AMI](#)
- [Configure FortiSIEM via GUI](#)
- [Upload the FortiSIEM License](#)
- [Choose an Event Database](#)

Launch an Instance Using FortiSIEM 6.3.3 AMI

1. Navigate to the EC2 AMIs page and find FortiSIEM 6.3.3 AMI (or in AWS Marketplace after the GA release).
2. Launch FortiSIEM-6.3.3.0348.

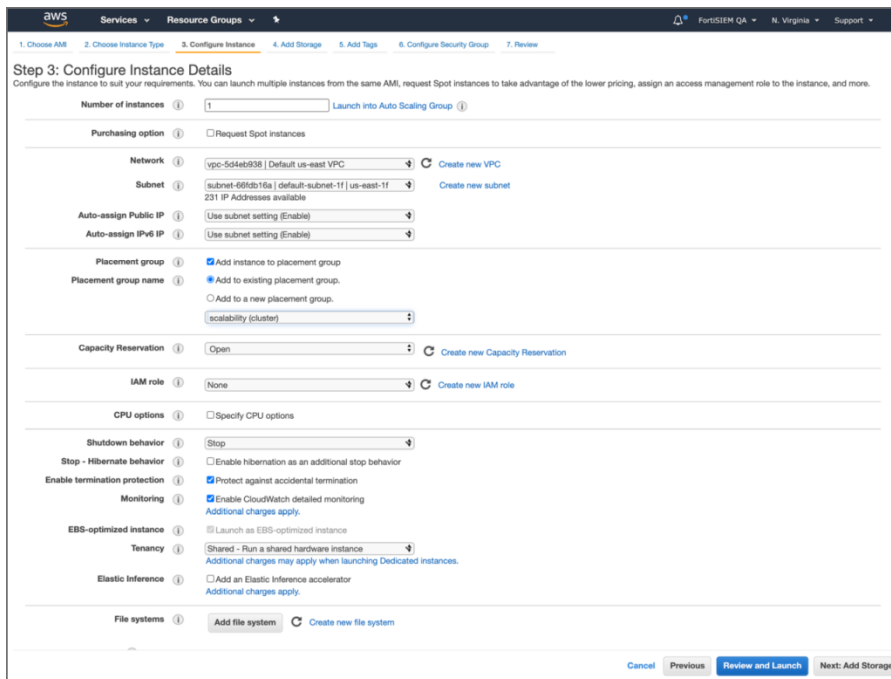


3. Go to **Step 3: Configure Instance Details** in AWS Services. Configure instance details such as VPC, Subnet, IP, etc. Click **Next**.

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**.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

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-0b341032a6aaf1b17a	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

[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.

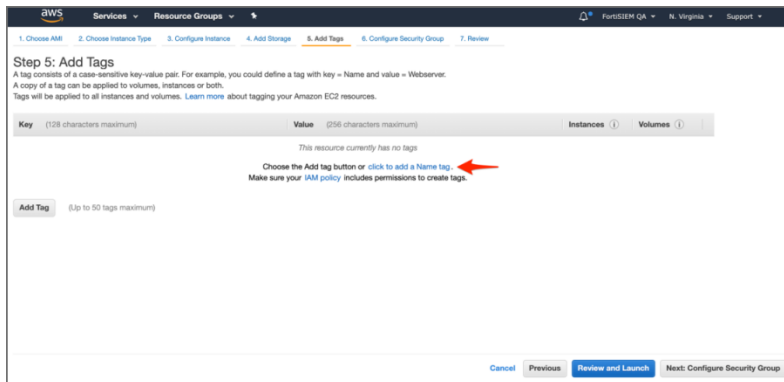
Use these partition values:

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)

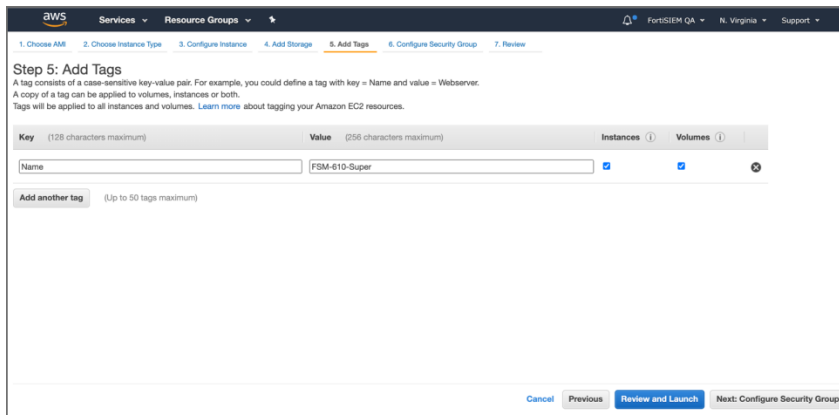
Note on EBS Volume 5:

- 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**.



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**.

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:

Description:

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](#)

8. 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
FortiSIEM-VA-6.1.0.1255 - ami-036b92a1377106e04
Root Device Type: ebs Virtualization type: hvm [Edit AMI](#)

Instance Type
[Edit instance type](#)

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

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

9. 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](#).

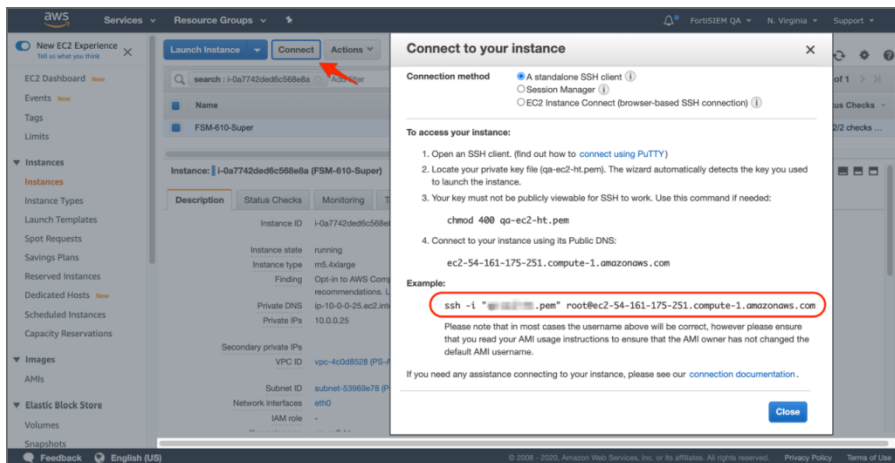
Choose an existing key pair

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](#)

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.

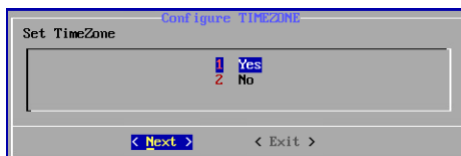
Note: If you are going to assign and use a global IPv6 address to your instance in addition to IPv4, then you will need to perform additional steps and reboot the instance. Take the following steps:

- 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.

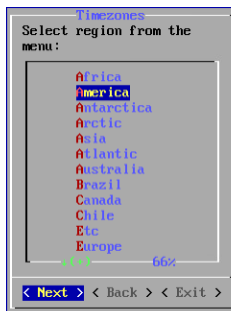
Configure FortiSIEM via GUI

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

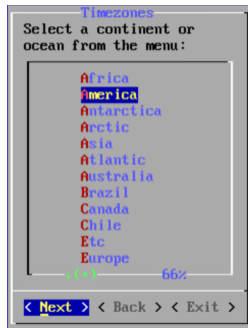
1. At the root command prompt, go to `/usr/local/bin` and enter `configFSM.sh`, for example:
`# configFSM.sh`
2. In VM console, select **1 Set Timezone** and then press **Next**.



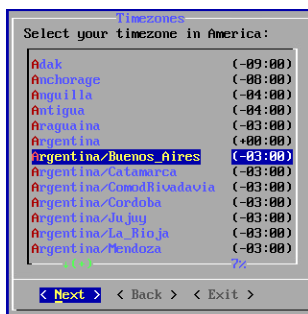
3. Select your **Location**, and press **Next**.



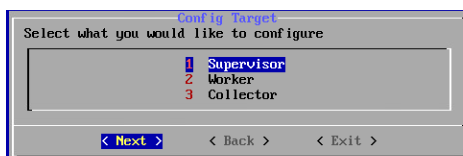
4. Select your **Continent**, and press **Next**.



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.

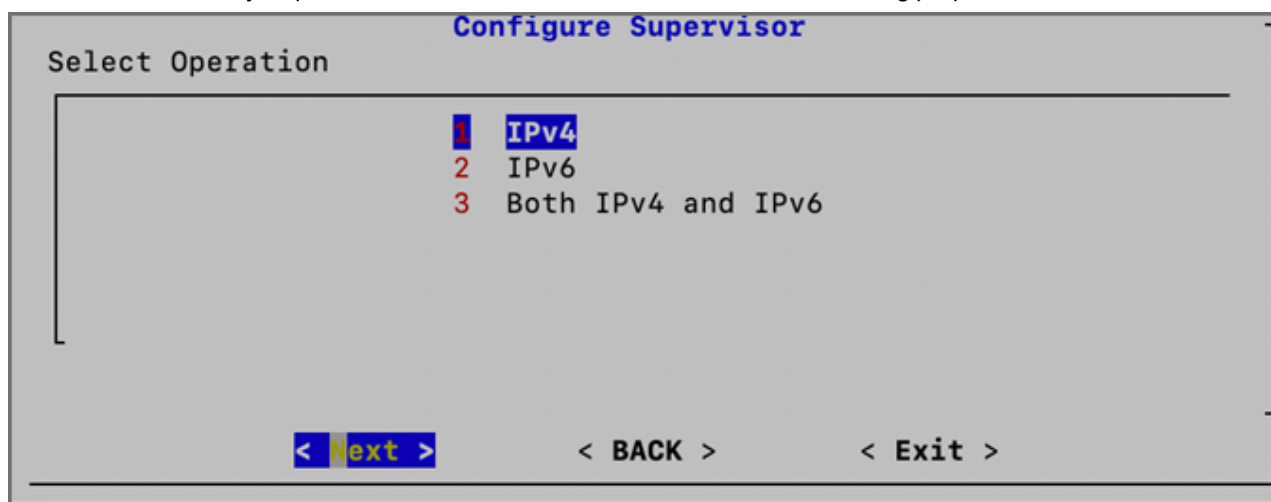
7. If you want to enable FIPS, then choose **2 install_with_fips**. Otherwise, choose **1 install_without_fips**. You have the option of enabling FIPS (option **3**) or disabling FIPS (option **4**) later.

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



8. Determine whether your network supports IPv4-only, 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.



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

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

```

Configure IPv4 For Supervisor
Configure IPv4 Network

IPv4 Address: 172.30.57.52
Netmask:      255.255.252.0
Gateway:      172.30.56.1
DNS1:         172.30.1.105
DNS2:         172.30.1.106

< Next >      < Back >      < Exit >

```

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 Supervisor's IPv6 address
prefix (Netmask)	The Supervisor'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 Supervisor, 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**.

Configure Supervisor

Enter host for checking network connectivity

myhost.com_

< Next >
< Back >
< Exit >

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**.

Configure Supervisor

Run Configuration Command:

```
python /usr/local/bin/configureFSM.py -r super -z US/Pacific -i 10.0.0.4 -m
255.255.255.0 -g 10.0.0.1 --host super-631-dual-stack -t 64 --dns1 10.0.0.2
--dns61 2001:4860:4860::8888 --dns62 2001:4860:4860::8884 --i6
2600:1f18:1014:6520:804d:e099:cd63:c04f --m6 128 --g6
fe80::c0f:cff:fe1e:392d -o install_without_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 IPv6) or 64 (for both IPv4 and IPv6)
--dns1, --dns2	Addresses of the DNS server 1 and DNS server 2.
--i6	IPv6-formatted address
--m6	IPv6 prefix
--g6	IPv6 gateway
-o	Installation option (install_without_fips , install_with_fips , enable_fips , disable_fips , change_network_config*) *Option only available after installation.
-Z	Time zone. Possible values are US/Pacific , Asia/Shanghai , Europe/London , or Africa/Tunis
--testpinghost	The URL used to test connectivity

14. 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

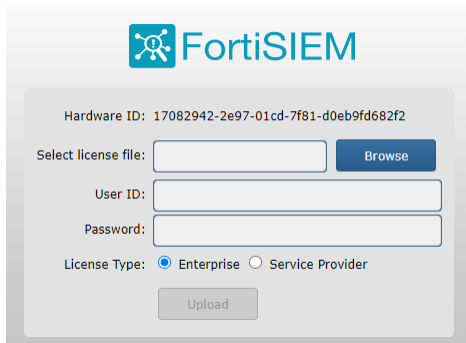


Before proceeding, make sure that you have obtained valid FortiSIEM license from Forticare. For more information, see the [Licensing Guide](#).

You will now be asked to input a license.

1. Open a Web browser and log in to the FortiSIEM UI. Please note that if you are logging into FortiSIEM with an IPv6 address, you should input `https://[IPv6 address]` on the browser tab.

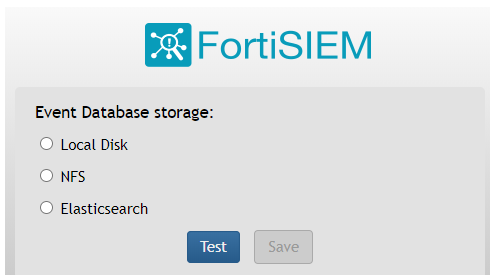
2. The License Upload dialog box will open.

The image shows the FortiSIEM License Upload dialog box. At the top is the FortiSIEM logo. Below it, the Hardware ID is displayed as 17082942-2e97-01cd-7f81-d0eb9fd682f2. There is a text input field for 'Select license file:' with a 'Browse' button to its right. Below that are text input fields for 'User ID:' and 'Password:'. At the bottom, there is a 'License Type' section with two radio buttons: 'Enterprise' (which is selected) and 'Service Provider'. An 'Upload' button is located at the very bottom of the dialog.

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](#).

The image shows the FortiSIEM Event Database Storage configuration page. It features the FortiSIEM logo at the top. Below the logo, the text 'Event Database storage:' is followed by three radio button options: 'Local Disk', 'NFS', and 'Elasticsearch'. At the bottom of the page, there are two buttons: 'Test' and 'Save'.

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, 25 sleeping, 0 stopped, 0 zombie
Cpu(s): 16.0% user, 6.2% sys, 2.1% id, 0.0% ni, 91.4% si, 0.0% wa, 0.2% hi, 0.1% st, 0.0% bsd
Mem: 65702100k total, 10366036k used, 55336064k free, 4352k buffers
Swap: 2621436k total, 0k used, 2621436k free, 2465028k cached
```

PROCESS	UPTIME	CPU%	VRT_MEM	RES_MEM
phParser	41:23	0	2176m	550m
phQueryMaster	41:41	0	1820m	77m
phIndexMaster	41:41	0	1879m	584m
phIndexWorker	41:41	0	1363m	205m
phQueryWorker	41:41	0	1383m	279m
phDataManager	41:41	0	1419m	205m
phDiscover	41:41	0	513m	53m
phReportWorker	41:41	0	1433m	95m
phReportMaster	41:41	0	602m	67m
phIdentityWorker	41:41	0	1827m	58m
phIdentityMaster	41:41	0	491m	39m
phAgentManager	41:41	0	1425m	54m
phCheckpoint	42:31	0	325m	39m
phEventMonitor	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	2800m	55m
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
nginx	01:10:07	0	15172m	3026m
DBSoc	01:10:30	0	317m	30m
phnomaly	01:00:07	0	907m	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).

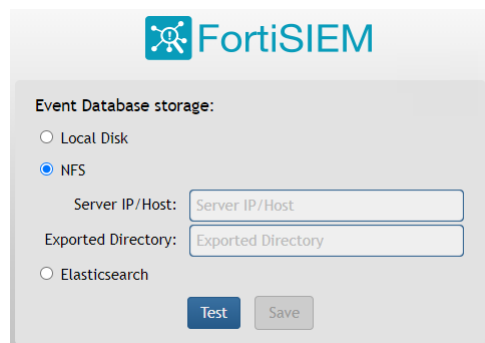
- [Install Supervisor](#)
- [Install Workers](#)
- [Register Workers](#)
- [Install Collectors](#)
- [Register Collectors](#)

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



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

Elasticsearch



The image shows the FortiSIEM configuration interface for Event Database storage. At the top is the FortiSIEM logo. Below it, the section is titled "Event Database storage:". There are three radio buttons: "Local Disk", "NFS", and "Elasticsearch", with "Elasticsearch" selected. Under "Elasticsearch", there are three radio buttons for "ES Service Type": "Native" (selected), "Amazon", and "Elastic Cloud". Below these are input fields for "URL:" (containing "https://"), "REST Port:" (containing "443"), "User Name:" (containing "(Optional)"), "Password:" (containing "(Optional)"), and "Confirm Password:". There are also radio buttons for "Shard Allocation": "Fixed" and "Dynamic" (selected). Below these are input fields for "Shards:" (containing "5") and "Replicas:" (containing "1"). At the bottom, there is a checkbox for "Per Org Index" which is unchecked. At the very bottom are "Test" and "Save" buttons.

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

Install Workers

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

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

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-0a71481d3c7816fb3	25	General Purpose SSD (gp3)	3000	125	<input checked="" type="checkbox"/>	Not Encrypted
EBS	/dev/sdb	<input type="text" value="Search (case-insensitive)"/>	100	General Purpose SSD (gp3)	3000	125	<input checked="" type="checkbox"/>	Not Encrypted

[Add New Volume](#)

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.

Register Workers

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

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

Add Node

Type: Worker

Worker IP Address: 172.30.58.9

Host Name: wk589

Save Cancel

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

The screenshot shows the FortiSIEM Cloud Health interface. On the left is a sidebar with navigation links: Setup, Device Support, Health (selected), License, and Settings. The main panel has tabs for Cloud Health and Collector Health. Under Cloud Health, there is a search bar and a 'Columns' dropdown. Below this is a table listing nodes:

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

Below the node table, there is another search bar and 'Columns' dropdown, followed by a section titled 'Process level metrics for wk573.fortinet.com (172.30.57.3)'. This section contains a table with process-level metrics:

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

At the bottom of the interface, there is a copyright notice: 'Copyright © 2020 Fortinet, Inc. All rights reserved.' and some organizational information: 'Organization: Super User: admin Scope: Global'.

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 'Step 4: Add Storage' page in the AWS Management Console. It includes a progress bar at the top with steps: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage (selected), 5. Add Tags, 6. Configure Security Group, and 7. Review. Below the progress bar, there is a description of the storage options and a table for adding storage volumes.

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

Below the table, there is a button 'Add New Volume' and a note: '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.'

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 > Settings > System > Event Worker** and enter the IP of the Supervisor node. Click **Save**.
4. 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**.
5. 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.
6. Go to **ADMIN > Health > Collector Health** for the status.

The screenshot displays the 'Collector Health' page in the FortiSIEM interface. The left sidebar contains navigation options: Setup, Device Support, Health (selected), License, and Settings. The main content area has tabs for 'Cloud Health' and 'Collector Health'. Below the tabs, there's a 'Show Processes' button and a search bar. The top table lists collector information:

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

Below this, there's a 'Close Panel' button and another search bar. The bottom table shows the status of various processes:

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: Required

Guaranteed EPS: Required

Upload Rate Limit (Kbps): Unlimited

Start Time: ☒ Unlimited

End Time: ☒ Unlimited

Save

Cancel

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

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

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

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

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

The Collector will reboot during the Registration.

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

Setup

Device Support

Health

License

Settings

Cloud Health

Collector Health

Show Processes

Tunnels

Action

Search...

Columns

Lines: 1 Last update at 8:54:17 PM

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

Close Panel

Search...

Columns

Lines: 9 Last update at 8:54:24 PM

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

Install Log

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

Errors can be found at the end of the file.



www.fortinet.com

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.