2000F Hardware Configuration Guide

FortiSIEM 6.2.1
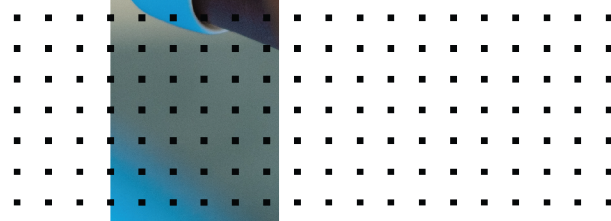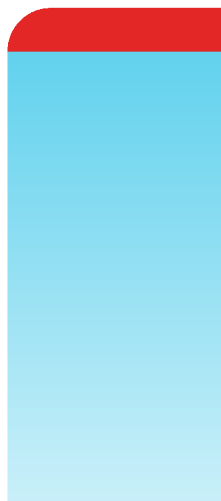
FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO LIBRARY

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 LABS

https://www.fortiguard.com

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com

F::RTINET®

TABLE OF CONTENTS

Change Log

Date	Description
03/30/2018	Initial release of this guide.
06/13/2019	Revision 1: Updated instructions for "Using FortiSIEM".
09/11/2019	Revision 2: Changed the location where you obtain images to https://support.fortinet.com.
08/15/2020	Revision 3: Added new sections for "Configuring FortiSIEM via a GUI", "Choose an Event Database", and "Cluster Installation".
10/09/2020	Revision 4: Added migration instructions.
11/11/2020	Revision 5: Release for 6.1.2.
12/08/2020	Revision 6: Small addition to Register Collectors.
03/23/2021	Revision 6: Release for 6.2.0.
04/20/2021	Revision 7: Updated Step 8: Choose an Event Database for 6.2.0.
05/06/2021	Revision 8: Release for 6.2.1.
05/19/2021	Revision 9: Updated Factory Reset section for 6.2.x.
06/07/2021	Updated Elasticsearch screenshot for 6.2.x guides.
07/09/2021	Updated step 5 in Step 2: Reinstall FortiSIEM application for 6.2.x guides.
11/18/2021	Revision 10: Updated Register Collectors instructions for 6.2.x guides.
10/20/2022	Updated Register Collectors instructions for 6.x guides.

FortiSIEM 6.2.1 2000F Hardware Configuration Guide
Fortinet Inc.

4

Appliance Setup

Follow the steps below to setup FSM-2000F appliance.

- All-in-one Installation
- Cluster Installation

All-in-one Installation

Follow these steps to install all of the FortiSIEM components at one time.

- Step 1: Rack mount the FSM-2000F appliance
- Step 2: Power On the FSM-2000F appliance
- Step 3: Verify System Information
- Step 4: Configure FortiSIEM via GUI
- Step 5: Generate the FortiSIEM FSM-2000F License Key file
- Step 6: Register the FortiSIEM License
- Step 7: Accessing FortiSIEM UI
- Step 8: Choose an Event Database

Step 1: Rack mount the FSM-2000F appliance

1. Follow FortiSIEM 2000F QuickStart Guide here to mount FSM-2000F into the rack.
2. Insert Hard Disks positions as shown below:
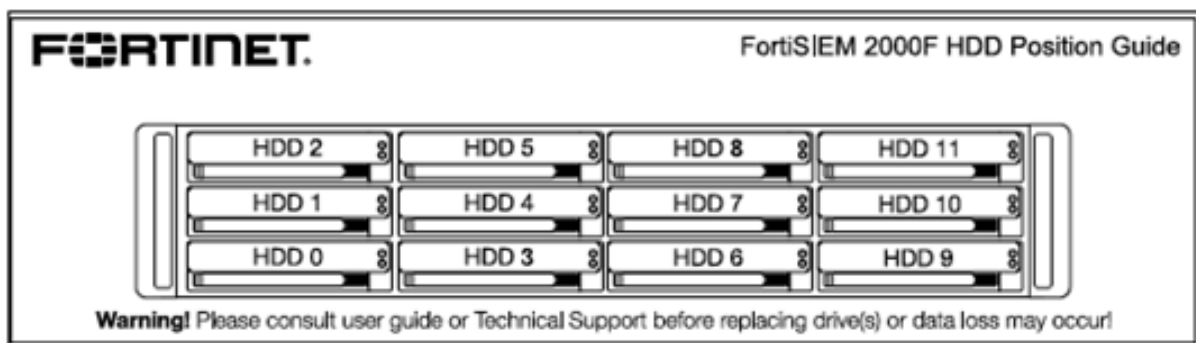
3. Connect FSM-2000F to the network by connecting an Ethernet cable to Port0.

> Before proceeding to the next step, connecting Ethernet cable to Port0 is required for Network configuration.

Step 2: Power On the FSM-2000F appliance

1. Make sure the FSM-2000F device is connected to a Power outlet and an Ethernet cable is connected to Port0.
2. Power On the FSM-2000F device.

> FSM-2000F appliance does not have a default IP address. To connect to the GUI, an IP address must be configured using the GUI (Step 4).

Step 3: Verify System Information

1. Connect to the FSM-2000F appliance using VGA port or Console port.
2. Login as 'root' user with password `ProspectHills`. You will be required to change the password. Remember this password for future use. Once you change the password, you will be logged out. Login again with your new password.
3. Run `get` to check the available FortiSIEM commands.
4. Use these commands to check the hardware information. After running each command, ensure that there are no errors in the displayed output.

| Command	Description
`get system status`	Displays system name, version and serial number.
`diagnose hardware info`	Displays system hardware information like CPUs, Memory and RAID information.
`diagnose interface detail port0`	Displays interface status.

Step 4: Configure FortiSIEM via GUI

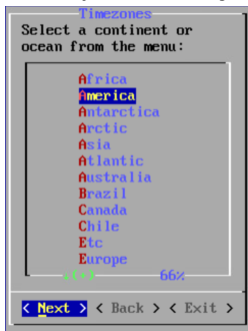Follow these steps to configure FortiSIEM by using a simple GUI.

1. Log in as user `root` with the password you set in Step 3 above.
2. At the command prompt, go to `/usr/local/bin` and enter `configFSM.sh`, for example:
   `# configFSM.sh`
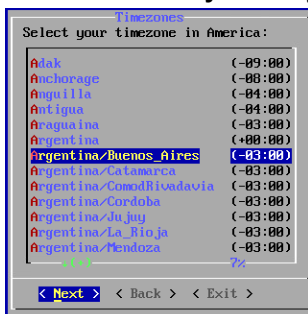3. In the console, select **1 Set Timezone** and then press **Next**.
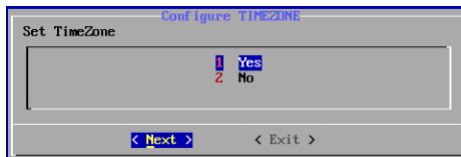
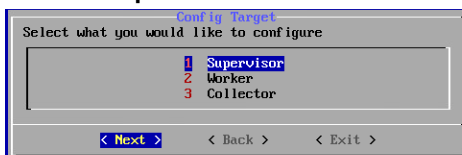4. Select your **Region**, and press **Next**.
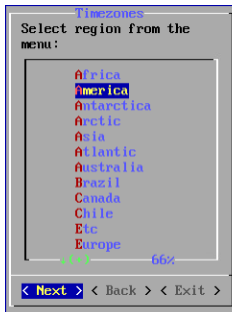
5. Select your **Country**, and press **Next**.

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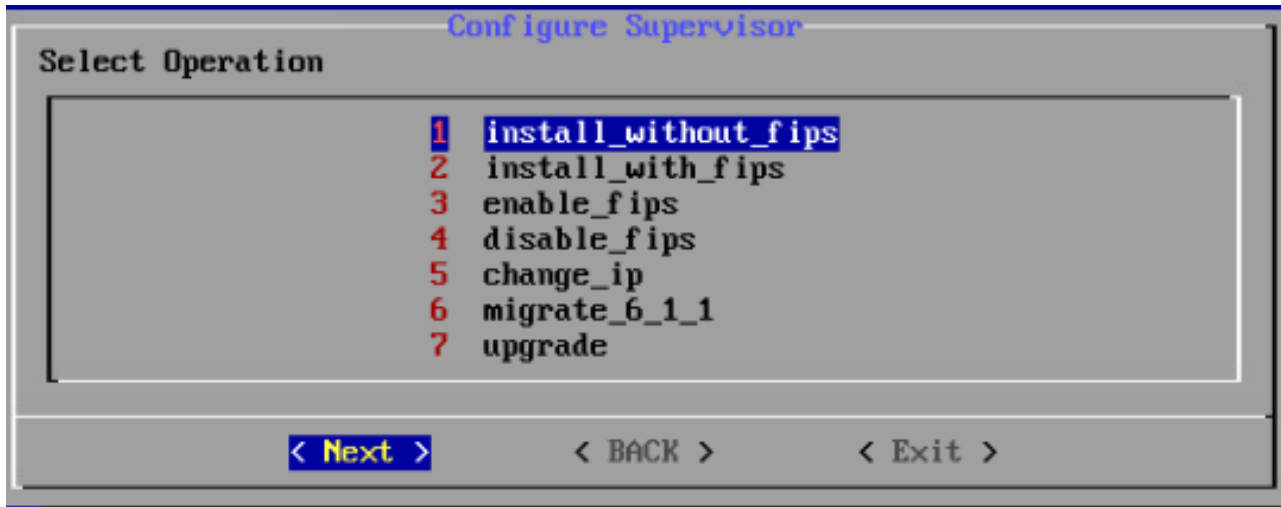

7. Select **1 Supervisor**. Press **Next**.

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

---

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

9. Configure the network by entering the following fields. Note the IP Address--you will need it in a later step. Press **Next**.
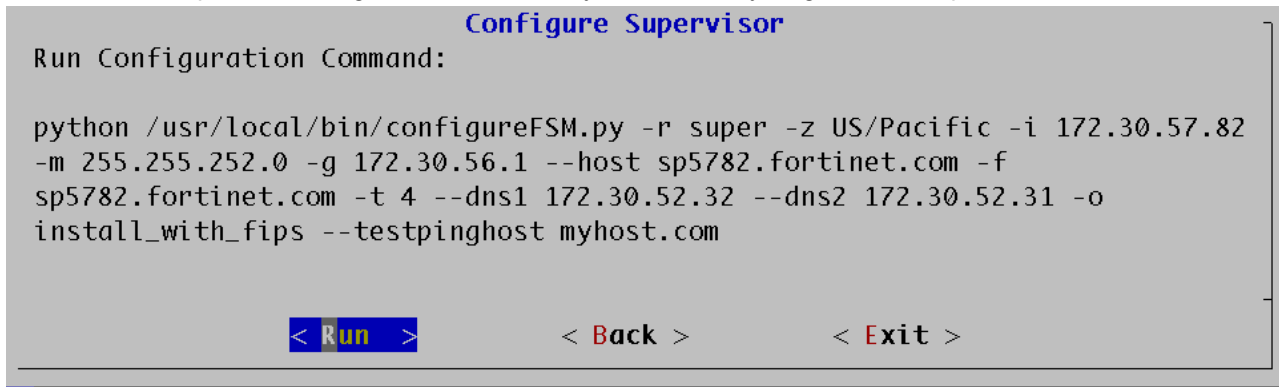
Option	Description
Host Name	The Supervisor's host name
IPv4 Address	The Supervisor's IPv4 address
NetMask	The Supervisor's subnet
Gateway	Network gateway address
FQDN	Fully-qualified domain name
DNS1, DNS2	Addresses of the DNS servers
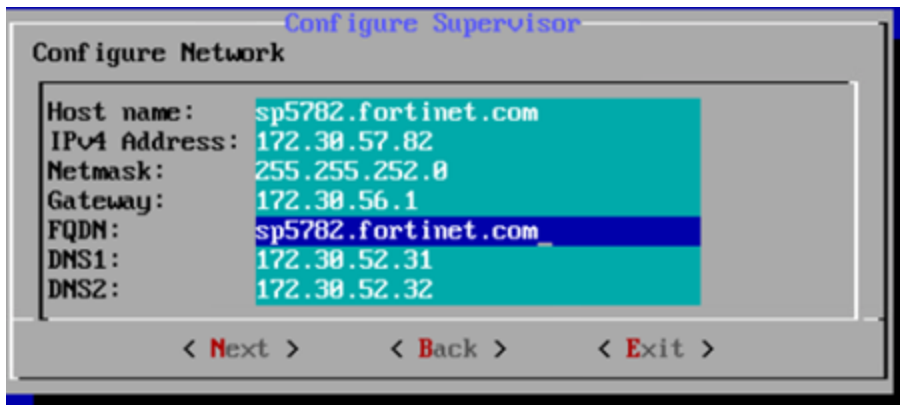
10. Test network connectivity by entering a host name that can be resolved by your DNS Server (entered in the previous step) and responds to ping. The host can either be an internal host or a public domain host like `google.com`. For the migration to complete, the system still needs https connectivity to FortiSIEM OS update servers: `os-pkgs-cdn.fortisiem.fortinet.com` and `os-pkgs-c8.fortisiem.fortinet.com`. Press **Next**.

FortiSIEM 6.2.1 2000F Hardware Configuration Guide
Fortinet Inc.

8

11. The final configuration confirmation is displayed. Verify that the parameters are correct. If they are not, then press **Back** to return to previous dialog boxes to correct any errors. If everything is OK, then press **Run**.

The options are described in the following table.

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

Option	Description
	Africa/Tunis
--testpinghost	The host used to test connectivity

12. It will take some time to complete the FortiSIEM installation. If the installation is successful, then the appliance will reboot automatically. Otherwise, the appliance 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:

```
phParser                DOWN
phQueryMaster           DOWN
phRuleMaster            DOWN
phRuleWorker            DOWN
phQueryWorker           DOWN
phDataManager           DOWN
phDiscover              DOWN
phReportWorker          DOWN
phReportMaster          DOWN
phIpIdentityWorker      DOWN
phIpIdentityMaster      DOWN
phAgentManager          DOWN
phCheckpoint            DOWN
phPerfMonitor           DOWN
phDataPurger            DOWN
phEventForwarder        DOWN
phMonitor               32:18       0       1263m      568m
Apache                  32:49       0       314m       17m
Rsyslogd                32:42       0       192m       4216k
Node.js-charting        32:36       0       642m       79m
Node.js-pm2             32:19       0       636m       52m
Node.js-exporter        32:31       0       10902m     59m
Node.js-jsreport        32:36       0       957m       117m
phFortiInsightAI        DOWN
phAnomalyWorker         DOWN
AppSvr                  32:17       4       31781m     4433m
DBSvr                   32:49       0       425m       37m
phAnomalyMaster         DOWN
SVNLite                 32:49       0       37923m     579m
Redis                   32:21       0       204m       82m
```

Step 5: Generate FortiSIEM FSM-2000F License Key file from FortiCare

1. Obtain the Hardware Serial Number from FSM-2000F appliance from FortiCare Support Services.
2. Follow FortiSIEM Licensing Guide here to generate the license key file - remember to use 'Hardware Serial Number' for Hardware ID.

Step 6: Register FortiSIEM License

1. Note the IP Address assigned to FortiSIEM in Step 4.
2. Access FortiSIEM from browser (`https://<FortiSIEM-IP>`).
3. Upload the license file obtained from Step 5 and select the **License Type** based on your deployment (note this choice can only be made once and is not reversible):
   - Enterprise for single organizations
   - Service Provider for multiple organizations
4. Click **Upload** to complete the license registration.

Step 7: Accessing FortiSIEM UI

1. Note the IP Address assigned to FortiSIEM in Step 5.
2. Access FortiSIEM from browser (`https://<FortiSIEM-IP>`).
3. Login to FortiSIEM using the default user name, password, and organization:
   - **UserID**: *admin*
   - **Password**: *admin*1*
   - **Cust/OrgID**: *super* (if shown)

Step 8: Choose an Event Database

For a fresh installation, you will be taken to the Event Database Storage page.

Option	Description
Local HW Appliance Storage	Enter the "hardware" without the quotes, to use the inbuilt storage and FortiSIEM event database.
NFS	For more details, see Configuring Storage. Using NFS will not utilize the hardware appliance storage.
Elasticsearch	For more details, see Configuring Storage. Using Elasticsearch will not utilize the hardware appliance storage.

Cluster Installation

For larger installations, you can choose Worker nodes and external storage (NFS or Elasticsearch).
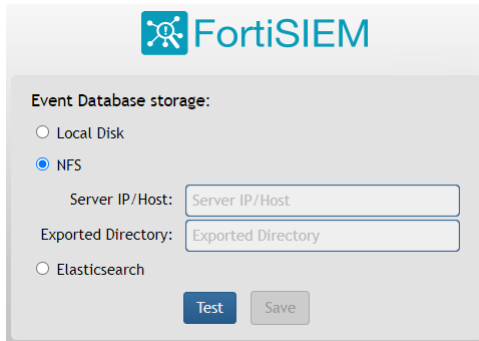
- Installing the Supervisor
- Installing Workers
- Registering Workers
- Installing Collectors
- Registering Collectors

Installing the Supervisor

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

- Setting up hardware - you do not need an event database.
- Setting up an Event database - Configure the cluster for either NFS or Elasticsearch.

  NFS

  Elasticsearch

You must choose external storage listed in Step 8: Choose an Event Database.

Installing Workers

Once the Supervisor is installed, follow the same steps in All-in-one Installation to install a Worker except that you choose **2 Worker** during Step 4: Configure FortiSIEM via GUI substep 7.

Registering Workers

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

FortiSIEM 6.2.1 2000F Hardware Configuration Guide
Fortinet Inc.

13

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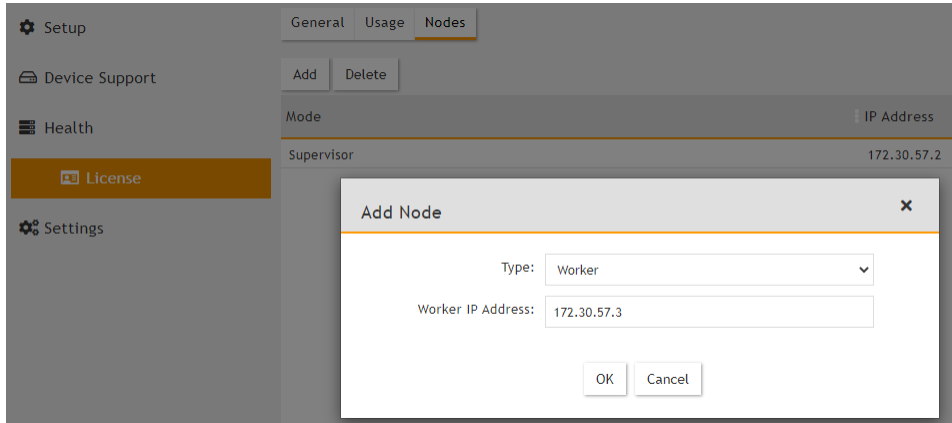
3. See **ADMIN > Health > Cloud Health** to ensure that the Workers are up, healthy, and properly added to the system.
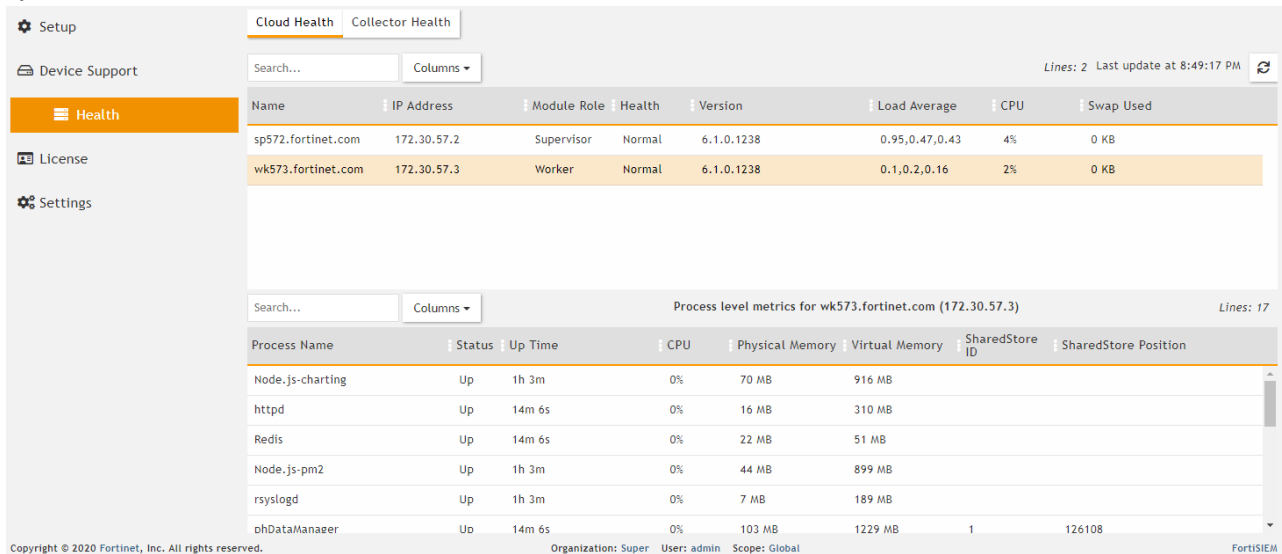
Installing Collectors

Once Supervisor and Workers are installed, follow the same steps in All-in-one Install to install a Collector except only choose OS and OPT disks. The recommended settings for Collector node are:

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

FortiSIEM 6.2.1 2000F Hardware Configuration Guide
Fortinet Inc.

14

Registering 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 > Collector** 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:
   `# /opt/phoenix/bin/phProvisionCollector --add <user> <password> <Super IP or Host> <Organization> <CollectorName>`
   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.

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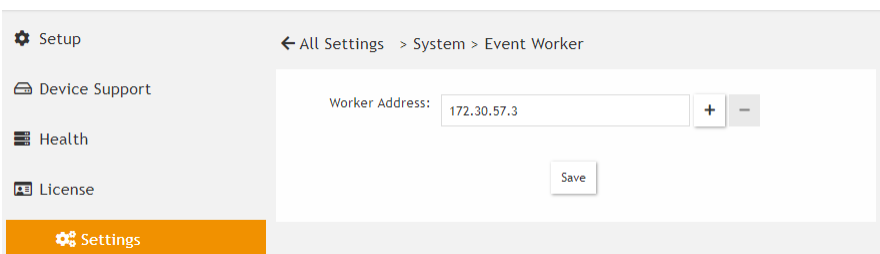
3. Go to **ADMIN > Setup > Organizations** and click **New** to add an Organization.
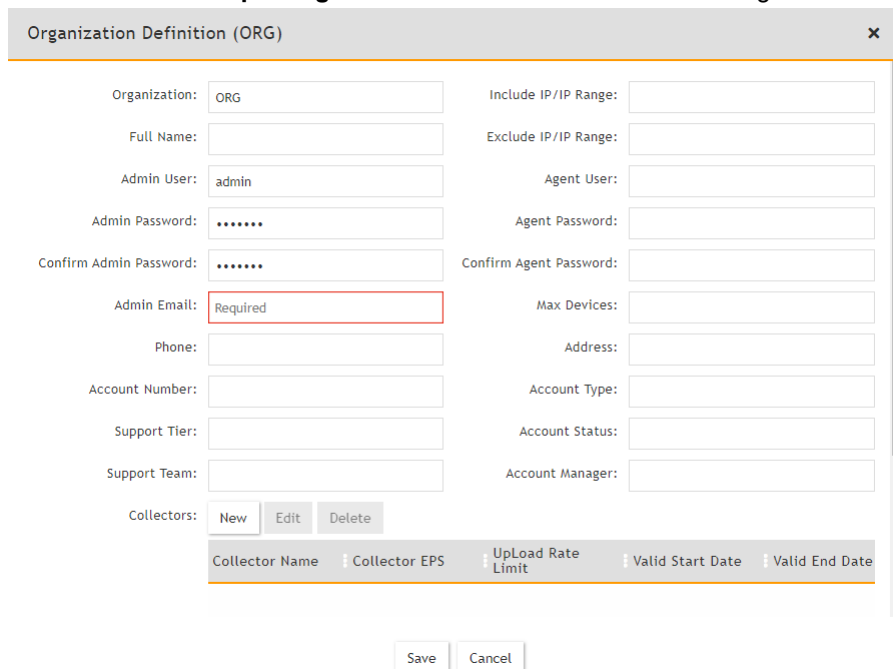
4. Enter the **Organization Name**, **Admin User**, **Admin Password**, and **Admin Email**.
5. Under **Collectors**, click **New**.
6. Enter the **Collector Name**, **Guaranteed EPS**, **Start Time**, and **End Time**.
   The last two values could be set as **Unlimited**. **Guaranteed EPS** is the EPS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

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

/opt/phoenix/bin/phProvisionCollector --add *<user>* *<password>* *<Super IP or Host>* *<Organization>* *<CollectorName>*

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.

Factory Reset

Follow the steps below to perform factory reset on FortiSIEM FSM-2000F.

- Step 1: Uninstall FortiSIEM application
- Step 2: Reinstall FortiSIEM application

Step 1: Uninstall FortiSIEM application

1. Connect FortiSIEM device using VGA or Console port.
2. Login as `root` user with the new password you set in Step 3: Verify System Information.
3. To check the available FortiSIEM commands, run `sudo get`.
4. To uninstall FortiSIEM, run `sudo execute fsm-clean`.
   This script will uninstall FortiSIEM application.
5. Reboot the system.

Step 2: Reinstall FortiSIEM application

1. Login as `root` with password `ProspectHills`. You will immediately be asked to change your password.
2. To configure RAID, run `execute format disk`.
3. To check Hardware status and RAID information, run `diagnose hardware info`.
4. To install FortiSIEM, run `execute factoryreset --force`. The command fails after partial steps. Run the same command again to complete factory reset.
   This script takes a few minutes to complete FortiSIEM installation.
5. Reboot and run `/user/local/bin/configFSM.sh` to install FortiSIEM.

Follow the steps under Appliance Setup **to configure FSM-2000F.**

FURTINET