FortiSIEM - 3500F Hardware Configuration Guide

Version 6.1.2

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

11/14/2023
FortiSIEM 6.1.2 3500F Hardware Configuration Guide

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.
03/26/2021	Revision 7: Updated migration instructions for 6.1.2.
05/19/2021	Revision 8: Updated Factory Reset section for 6.1.2.
06/21/2021	Revision 9: Updated Factory Reset section for 6.1.2.
11/19/2021	Revision 10: Updated Register Collectors section for 6.1.2
10/20/2022	Revision 11: Updated Register Collectors instructions for 6.x guides.

Appliance Setup

Follow the steps below to setup FSM-3500F appliance.

- All-in-one Installation
- Cluster Installation

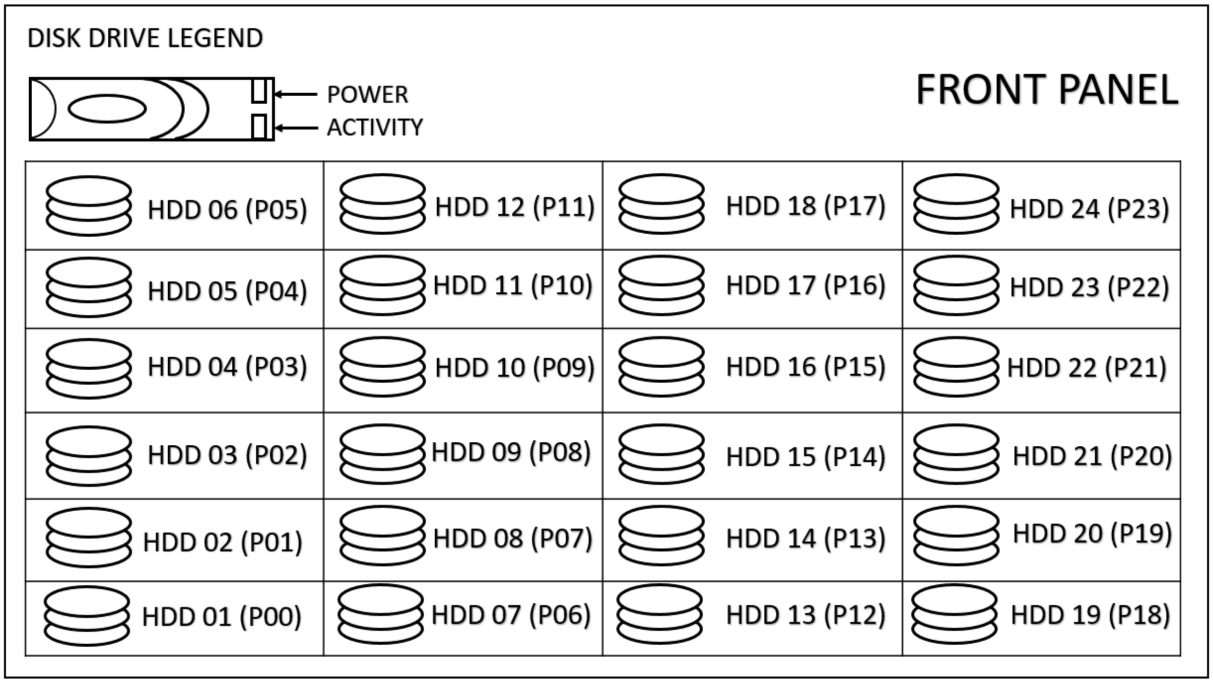
All-in-one Installation

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

- Step 1: Rack mount the FSM-3500F appliance
- Step 2: Power On the FSM-3500F appliance
- Step 3: Verify System Information
- Step 4: Configure FortiSIEM via GUI
- Step 5: Generate the FortiSIEM FSM-3500F 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-3500F appliance

1. Follow FortiSIEM 3500F QuickStart Guide here to mount FSM-3500F into the rack.
2. Insert Hard Disks positions as shown below:



HDD 06 (P05)	HDD 12 (P11)	HDD 18 (P17)	HDD 24 (P23)
HDD 05 (P04)	HDD 11 (P10)	HDD 17 (P16)	HDD 23 (P22)
HDD 04 (P03)	HDD 10 (P09)	HDD 16 (P15)	HDD 22 (P21)
HDD 03 (P02)	HDD 09 (P08)	HDD 15 (P14)	HDD 21 (P20)
HDD 02 (P01)	HDD 08 (P07)	HDD 14 (P13)	HDD 20 (P19)
HDD 01 (P00)	HDD 07 (P06)	HDD 13 (P12)	HDD 19 (P18)

3. Connect FSM-3500F 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-3500F appliance

1. Make sure the FSM-3500F device is connected to a Power outlet and an Ethernet cable is connected to Port0.
2. Power On the FSM-3500F device.

FSM-3500F 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-3500F 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.

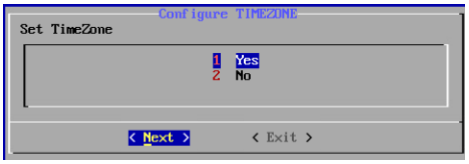
4. Use these commands to check the hardware information. After running each command, ensure that there are no errors in the displayed output.

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.

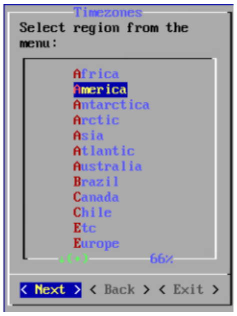
1. Log in as user `root` with the password you set in Step 3 above.
2. At the command prompt, go to `/usr/local/bin` and enter `configFSM.sh`, for example:
   `# configFSM.sh`
3. In the console, select **1 Set Timezone** and then press **Next**.



Configure TIMEZONE

Set TimeZone

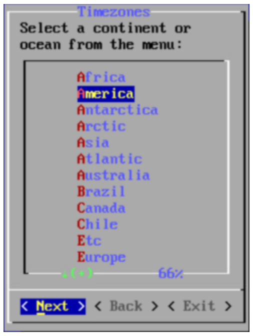
4. Select your **Region**, and press **Next**.



Timezones

Select region from the menu:

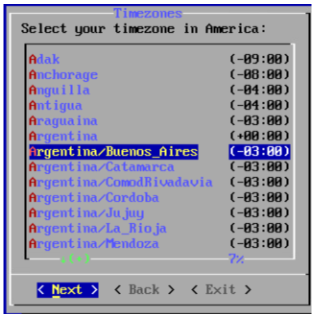
5. Select your **Country**, and press **Next**.



Timezones

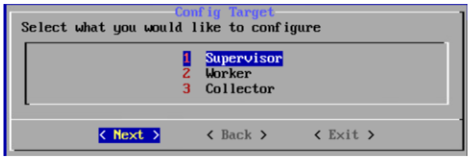
Select a continent or ocean from the menu:

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



```
Select your timezone in America:

Adak                          (-09:00)
Anchorage                     (-08:00)
Anguilla                      (-04:00)
Antigua                       (-04:00)
Araguaina                     (-03:00)
Argentina                     (+00:00)
Argentina/Buenos_Aires        (-03:00)
Argentina/Catamarca           (-03:00)
Argentina/ComodRivadavia      (-03:00)
Argentina/Cordoba             (-03:00)
Argentina/Jujuy               (-03:00)
Argentina/La_Rioja            (-03:00)
Argentina/Mendoza             (-03:00)
```

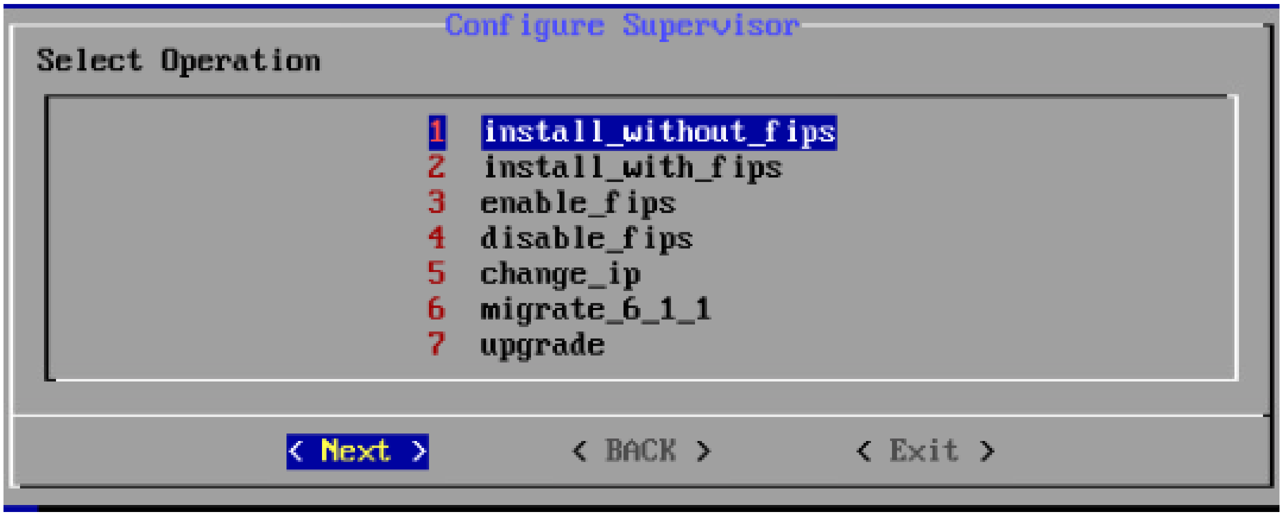
7. Select **1 Supervisor**. Press **Next**.



```
Select what you would like to configure

1  Supervisor
2  Worker
3  Collector
```

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.

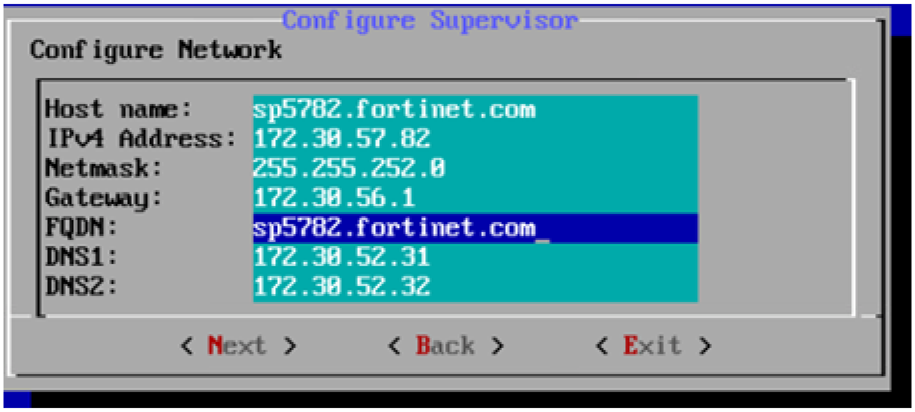


```
Select Operation

1  install_without_fips
2  install_with_fips
3  enable_fips
4  disable_fips
5  change_ip
6  migrate_6_1_1
7  upgrade
```

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

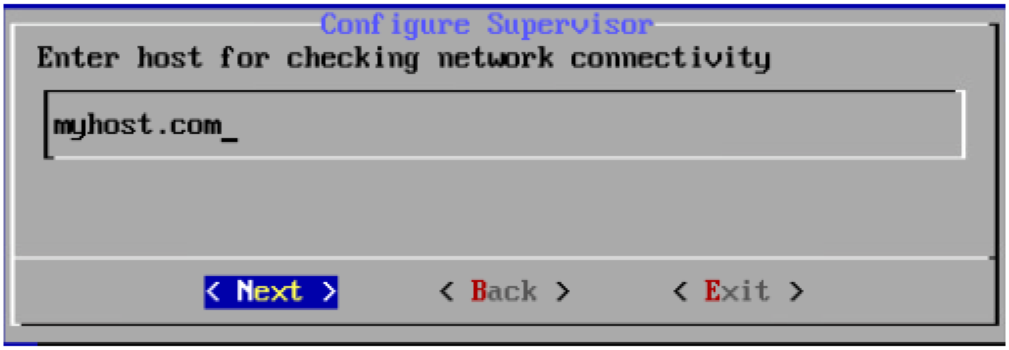
Option	Description
FQDN	Fully-qualified domain name
DNS1, DNS2	Addresses of the DNS servers


Configure Supervisor

Configure Network

```
Host name:     sp5782.fortinet.com
IPv4 Address:  172.30.57.82
Netmask:       255.255.252.0
Gateway:       172.30.56.1
FQDN:          sp5782.fortinet.com_
DNS1:          172.30.52.31
DNS2:          172.30.52.32
```

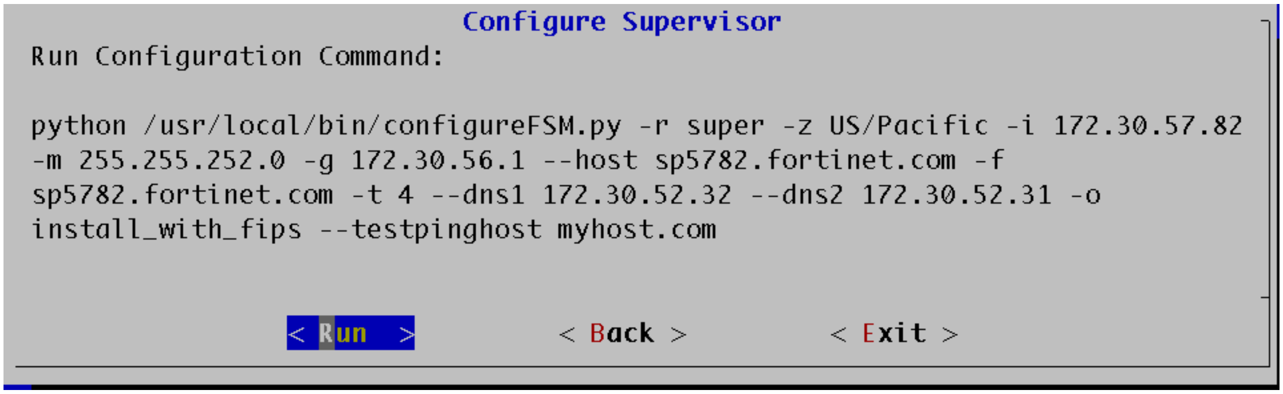
10. Test network connectivity by entering a host name that can be resolved by your DNS Server (entered in the previous step) and responds to ping. The host can either be an internal host or a public domain host like google.com. In order for the migration to complete, the system still needs https connectivity to FortiSIEM OS update servers: `os-pkgs-cdn.fortisiem.fortinet.com` and `os-pkgs-c8.fortisiem.fortinet.com`. Press **Next**.


Configure Supervisor

Enter host for checking network connectivity

```
myhost.com_
```

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**.


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
```

The options are described in the following table.

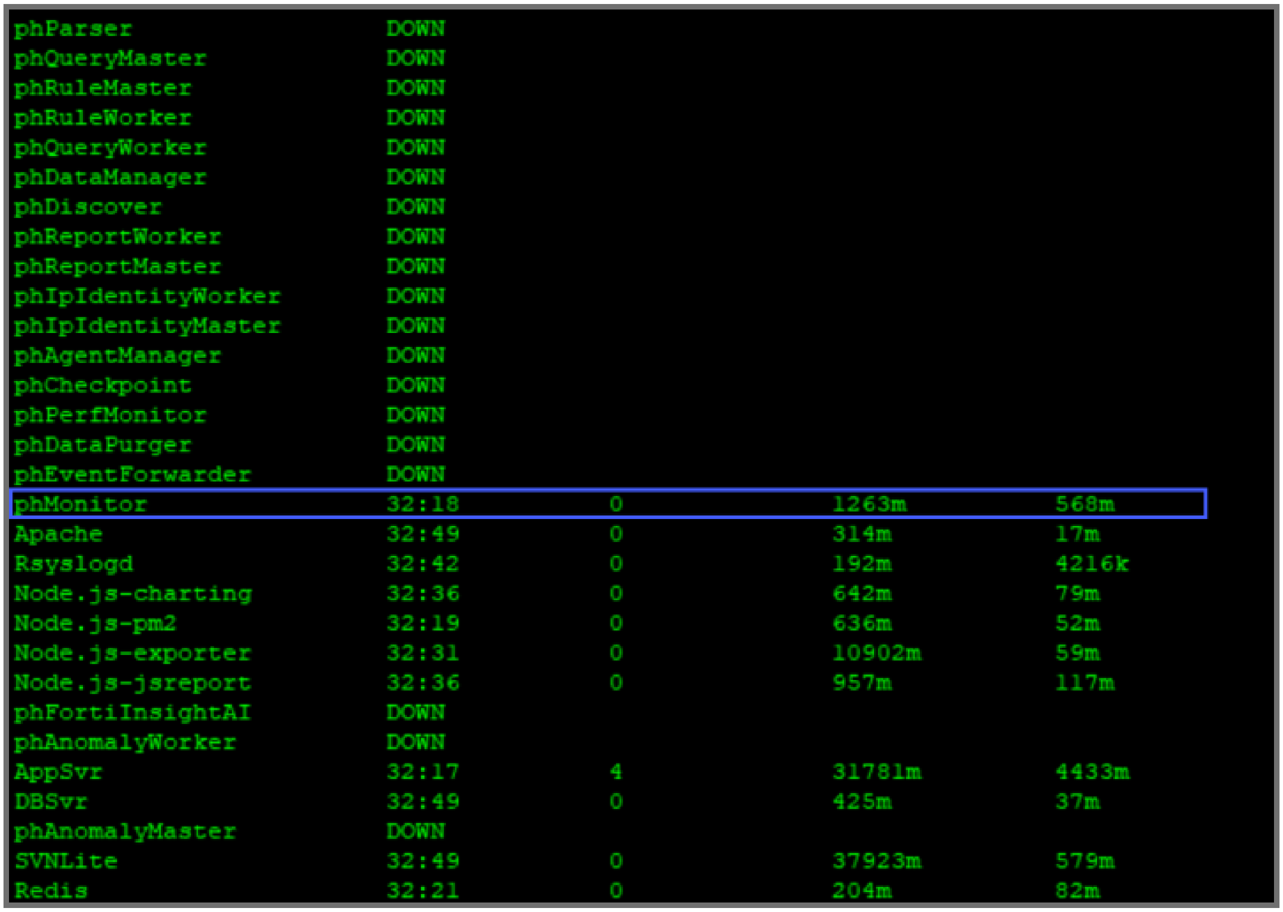
Option	Description
-r	The FortiSIEM component being configured
-z	The time zone being configured
-i	IPv4-formatted address
-m	Address of the subnet mask
-g	Address of the gateway server used
--host	Host name
-f	FQDN address: fully-qualified domain name
-t	The IP type. The values can be either **4** (for **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 **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-3500F License Key file from FortiCare

1. Obtain the Hardware Serial Number from FSM-3500F 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

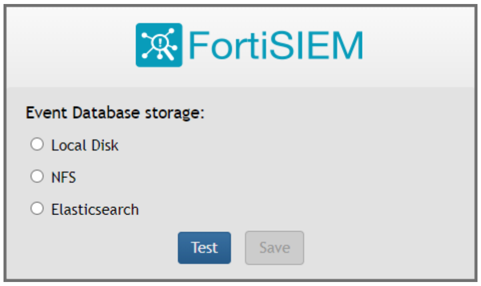
1. Note the IP Address assigned to FortiSIEM in Step 4.
2. Access FortiSIEM from browser (`https://<FortiSIEM-IP>`).
3. Upload the license file obtained from Step 5 and select the **License Type** based on your deployment (note this choice can only be made once and is not reversible):
   - Enterprise 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. You will be asked to choose between **Local Disk**, **NFS** or **Elasticsearch** options. For more details, see Configuring Storage.



Event Database storage:

○ Local Disk

○ NFS

○ Elasticsearch

Cluster Installation

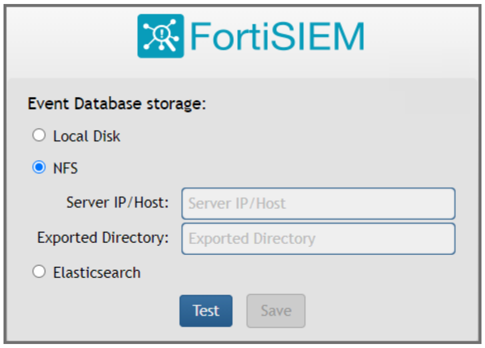
For larger installations, you can choose Worker nodes and external storage (NFS or Elasticsearch).

- 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



Event Database storage:

○ Local Disk

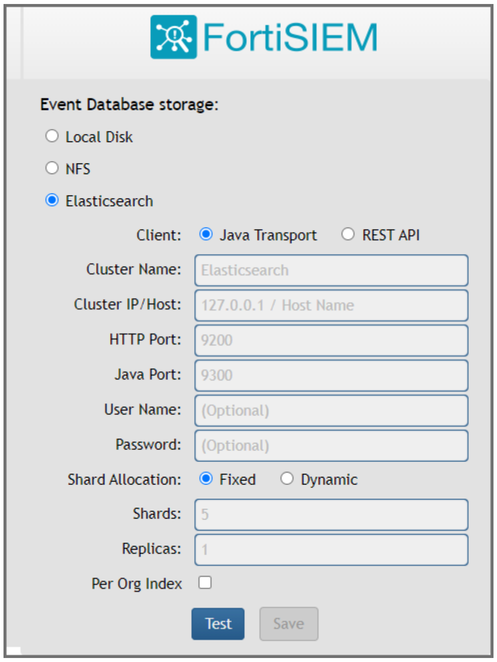
● NFS

Server IP/Host: Server IP/Host

Exported Directory: Exported Directory

○ Elasticsearch

Elasticsearch



Event Database storage:

○ Local Disk

○ NFS

● Elasticsearch

Client: ● Java Transport ○ REST API

Cluster Name: Elasticsearch

Cluster IP/Host: 127.0.0.1 / Host Name

HTTP Port: 9200

Java Port: 9300

User Name: (Optional)

Password: (Optional)

Shard Allocation: ● Fixed ○ Dynamic

Shards: 5

Replicas: 1

Per Org Index □

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

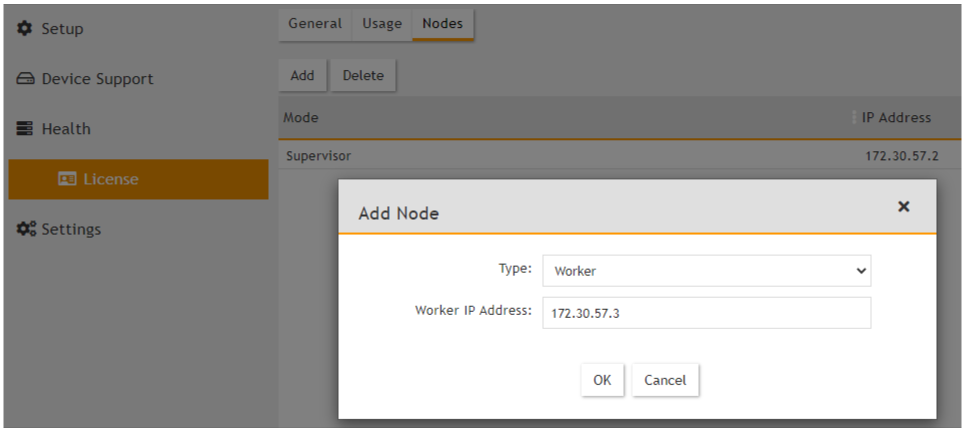
Installing Workers

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.

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



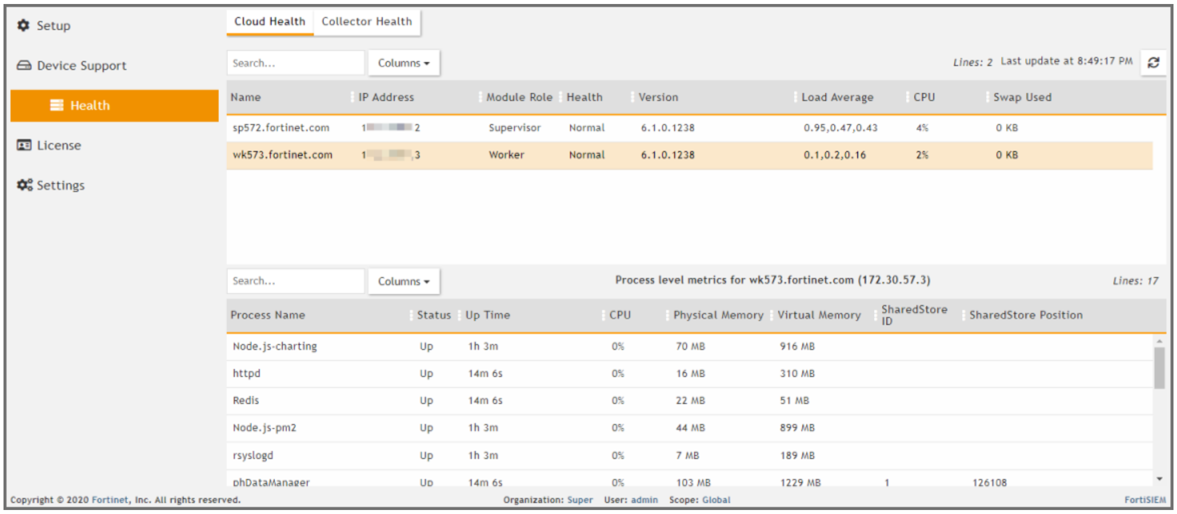
Mode	IP Address
Supervisor	172.30.57.2

Add Node

Type: Worker

Worker IP Address: 172.30.57.3

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



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

Name	IP Address	Module Role	Health	Version	Load Average	CPU	Swap Used
sp572.fortinet.com	1[redacted]2	Supervisor	Normal	6.1.0.1238	0.95,0.47,0.43	4%	0 KB
wk573.fortinet.com	1[redacted]3	Worker	Normal	6.1.0.1238	0.1,0.2,0.16	2%	0 KB

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

Process Name	Status	Up Time	CPU	Physical Memory	Virtual Memory	SharedStore ID	SharedStore Position
Node.js-charting	Up	1h 3m	0%	70 MB	916 MB		
httpd	Up	14m 6s	0%	16 MB	310 MB		
Redis	Up	14m 6s	0%	22 MB	51 MB		
Node.js-pm2	Up	1h 3m	0%	44 MB	899 MB		
rsyslogd	Up	1h 3m	0%	7 MB	189 MB		
phDataManager	Up	14m 6s	0%	103 MB	1229 MB	1	126108

Copyright © 2020 Fortinet, Inc. All rights reserved. Organization: Super User: admin Scope: Global FortiSIEM

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.

Registering Collectors

Collectors can be deployed in Enterprise or Service Provider environments.

- Enterprise Deployments
- Service Provider Deployments

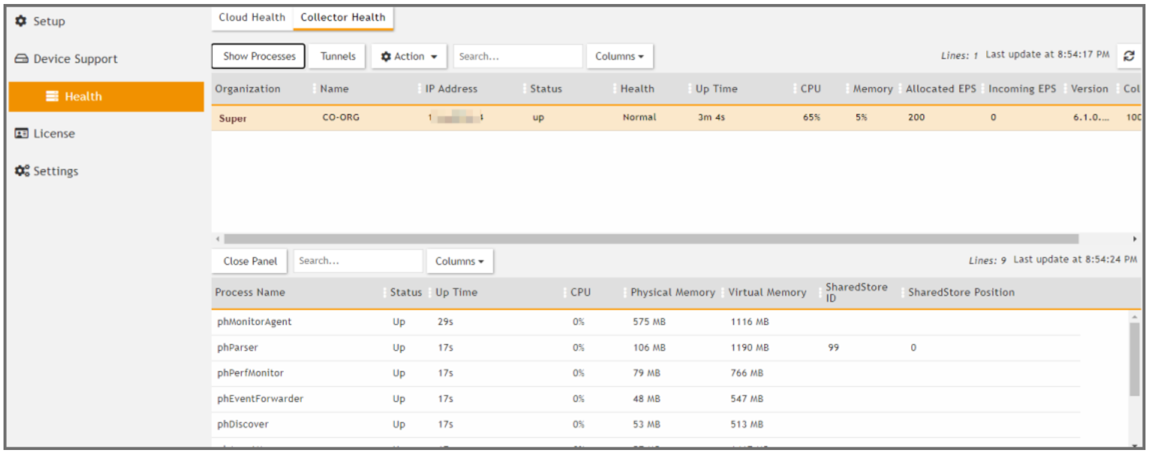
Enterprise Deployments

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 > 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:

```
# /opt/phoenix/bin/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.



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	[redacted]	up	Normal	3m 4s	65%	5%	200	0	6.1.0....	10C

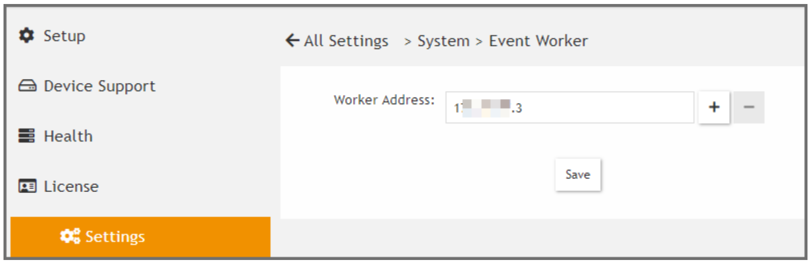
Lines: 9 Last update at 8:54:24 PM

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		

Service Provider Deployments

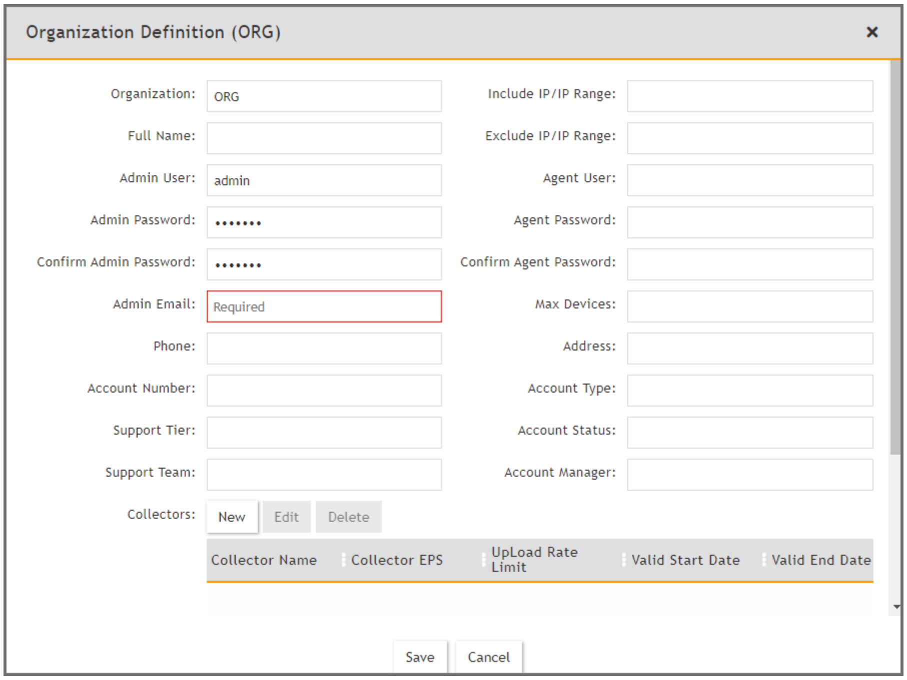
For Service Provider deployments, follow these steps.

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**.



Worker Address: 1[redacted].3

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

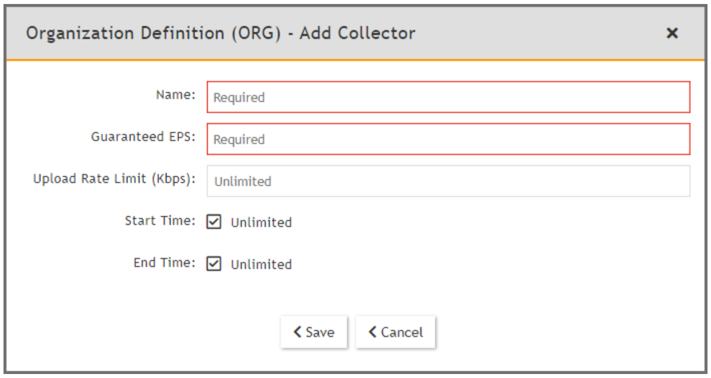


Organization:	ORG	Include IP/IP Range:	
Full Name:		Exclude IP/IP Range:	
Admin User:	admin	Agent User:	
Admin Password:	•••••••	Agent Password:	
Confirm Admin Password:	•••••••	Confirm Agent Password:	
Admin Email:	Required	Max Devices:	
Phone:		Address:	
Account Number:		Account Type:	
Support Tier:		Account Status:	
Support Team:		Account Manager:	

Collectors:

Collector Name	Collector EPS	UpLoad Rate Limit	Valid Start Date	Valid End Date

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

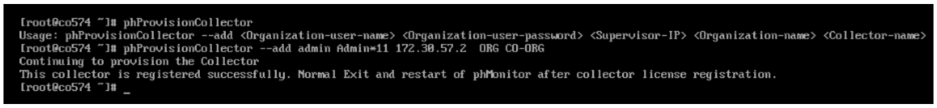
End Time: ☑ Unlimited

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>`*

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

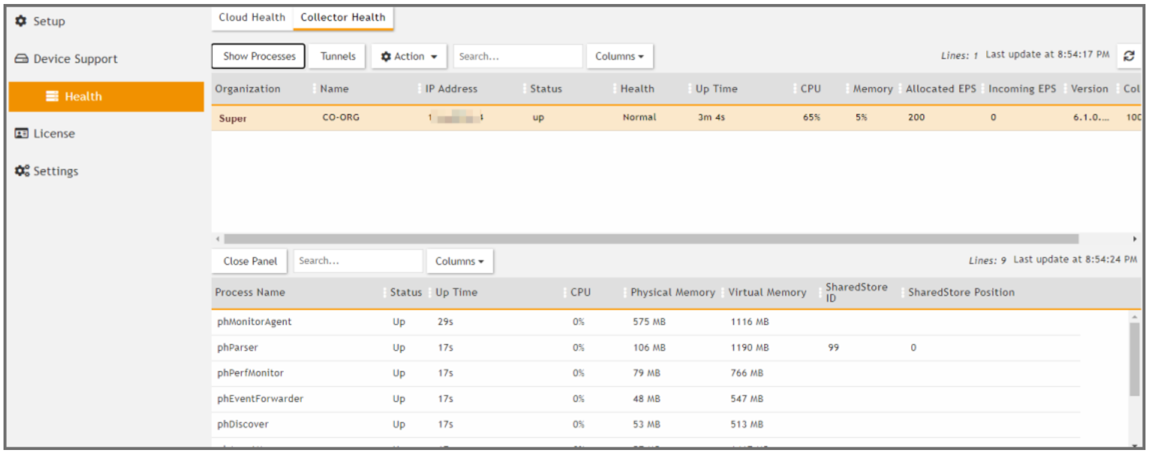
   a. Set `user` and `password` using the admin user name and password for the Organization that the Collector is going to be registered to.
   b. Set `Super IP or Host` as the Supervisor's IP address.
   c. Set `Organization` as the name of an organization created on the Supervisor.
   d. Set `CollectorName`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



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	[redacted]	up	Normal	3m 4s	65%	5%	200	0	6.1.0....	10C

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		

Factory Reset

Follow the steps below to perform factory reset on FortiSIEM FSM-3500F.

- 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.
5. Run the same command again, `execute factoryreset --force`, to complete factory reset.
6. Run `execute fsm-load`. This script takes a few minutes to complete FortiSIEM installation.
7. Reboot and run `/user/local/bin/configFSM.sh` to install FortiSIEM.

Follow the steps under Appliance Setup to configure FSM-3500F.

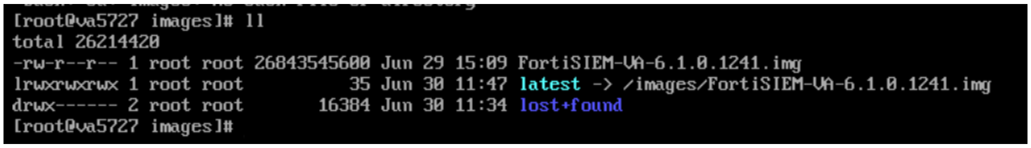
Migrating from 5.3.x or 5.4.x to 6.1.2

This section describes how upgrade the 3500F appliance from FortiSIEM 5.3.x or 5.4.x to FortiSIEM 6.1.2. FortiSIEM performs migration in-place, via a bootloader. There is no need to create a new image or copy disks. The bootloader shell contains the new version of FortiSIEM.

- Pre-Migration Checklist
- Migrate All-in-one

Pre-Migration Checklist

To perform the migration, the following prerequisites must be met:

1. Make sure your system can connect to the Internet.
2. Make sure you are running a 5.3.x or 5.4.x version of FortiSIEM. If you are not running these versions, first upgrade to any of these versions and then apply the procedures below.
3. Delete the Worker from the Super GUI.
4. Stop/Shutdown the Worker.
5. Make sure the `/data` directory (`/`) has at least 25+ GB of available space to store the new image.
6. Log in to your FSM as `root` and run the following commands:
   ```
   # mkdir -p /data/images
   # ln -s /data/images /images
   ```
   or if using NFS or Elasticsearch storage:
   ```
   # mkdir -p /svn/images
   # ln -s /svn/images /images
   ```
7. Go to the `/images` directory. Download the 6.1.2 hardware image from the support site, then unzip it. For example:
   ```
   # unzip FSM_Full_All_RAW_HARDWARE_6.1.2_build0119.zip
   ```
   Note: The image size is about 25GB after extracting.
8. Create a soft link to `images`, for example:
   ```
   # ln -sf /images/FortiSIEM-RAW-Hardware-6.1.2.0119.img /images/latest
   ```
9. Enter the `ll` command to ensure `latest` link is defined, for example:
   ```
   # ll
   ```
   
   ```
   [root@va5727 images]# ll
   total 26214420
   -rw-r--r-- 1 root root 26843545600 Jun 29 15:09 FortiSIEM-VA-6.1.0.1241.img
   lrwxrwxrwx 1 root root          35 Jun 30 11:47 latest -> /images/FortiSIEM-VA-6.1.0.1241.img
   drwx------ 2 root root       16384 Jun 30 11:34 lost+found
   [root@va5727 images]#
   ```

Migrate All-in-one Installation

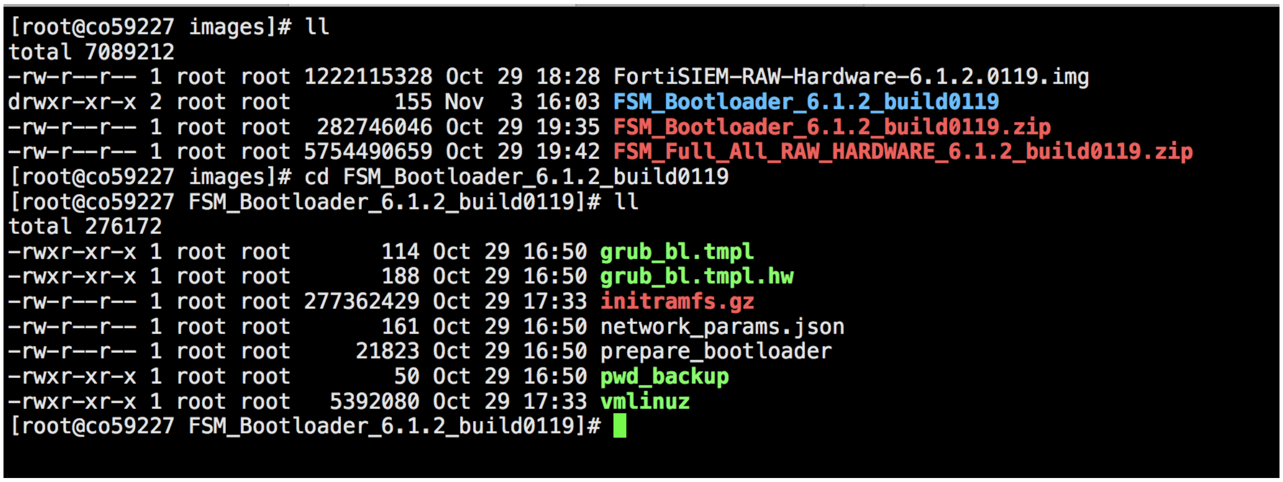
- Download the Bootloader
- Prepare the Bootloader

- Load the FortiSIEM 6.1.2 Image
- Migrate to FortiSIEM 6.1.2

Download the Bootloader

Install and configure the FortiSIEM bootloader to start migration. Follow these steps:

1. Download the bootloader `FSM_Bootloader_6.1.2_build0119.zip` from the support site and copy it to the `/images` directory.
2. Unzip the file, for example:
   `# unzip FSM_Bootloader_6.1.2_build0119.zip`



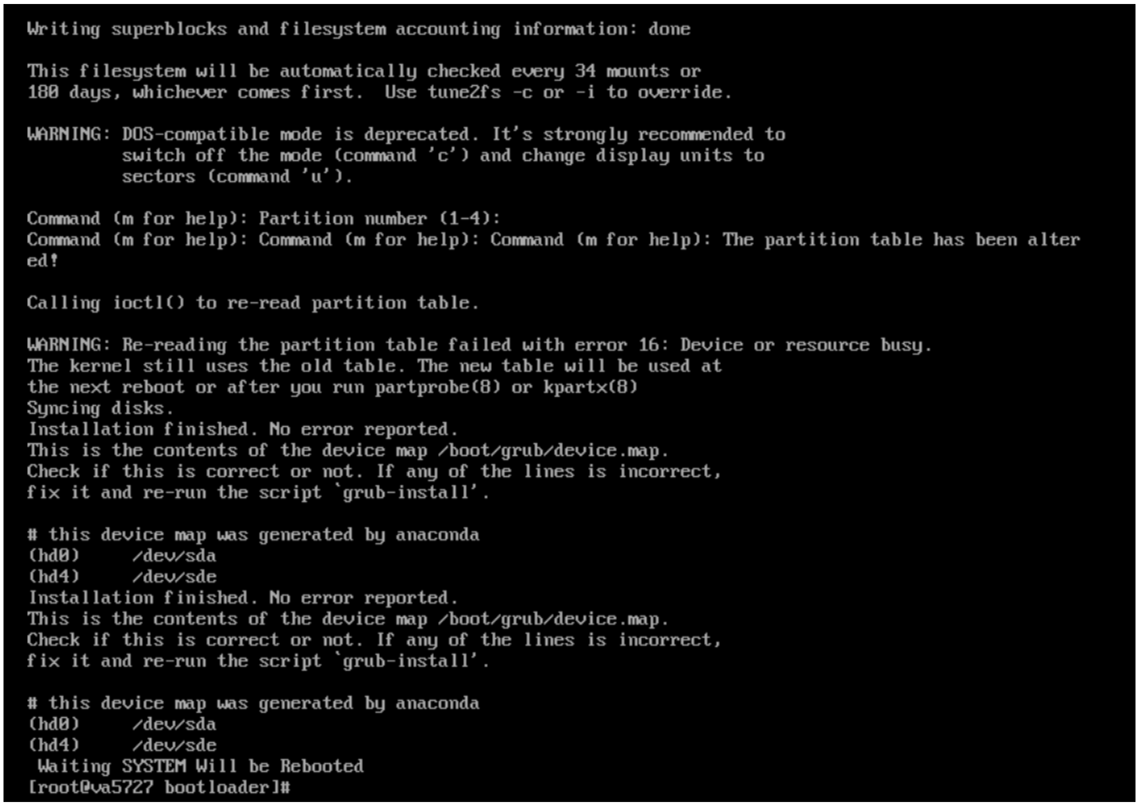
```
[root@co59227 images]# ll
total 7089212
-rw-r--r-- 1 root root 1222115328 Oct 29 18:28 FortiSIEM-RAW-Hardware-6.1.2.0119.img
drwxr-xr-x 2 root root        155 Nov  3 16:03 FSM_Bootloader_6.1.2_build0119
-rw-r--r-- 1 root root  282746046 Oct 29 19:35 FSM_Bootloader_6.1.2_build0119.zip
-rw-r--r-- 1 root root 5754490659 Oct 29 19:42 FSM_Full_All_RAW_HARDWARE_6.1.2_build0119.zip
[root@co59227 images]# cd FSM_Bootloader_6.1.2_build0119
[root@co59227 FSM_Bootloader_6.1.2_build0119]# ll
total 276172
-rwxr-xr-x 1 root root       114 Oct 29 16:50 grub_bl.tmpl
-rwxr-xr-x 1 root root       188 Oct 29 16:50 grub_bl.tmpl.hw
-rw-r--r-- 1 root root 277362429 Oct 29 17:33 initramfs.gz
-rw-r--r-- 1 root root       161 Oct 29 16:50 network_params.json
-rw-r--r-- 1 root root     21823 Oct 29 16:50 prepare_bootloader
-rwxr-xr-x 1 root root        50 Oct 29 16:50 pwd_backup
-rwxr-xr-x 1 root root   5392080 Oct 29 17:33 vmlinuz
[root@co59227 FSM_Bootloader_6.1.2_build0119]# 
```

Prepare the Bootloader

Follow these steps to run the `prepare_bootloader` script:

1. Go to the `bootloader` directory, for example:
   `# cd /images/FSM_Bootloader_6.1.2_build0119`
2. Run the `prepare_bootloader` script to install and configure the bootloader. This script installs, configures, and reboots the system. The script may take a few minutes to complete.
   `# sh prepare_bootloader`

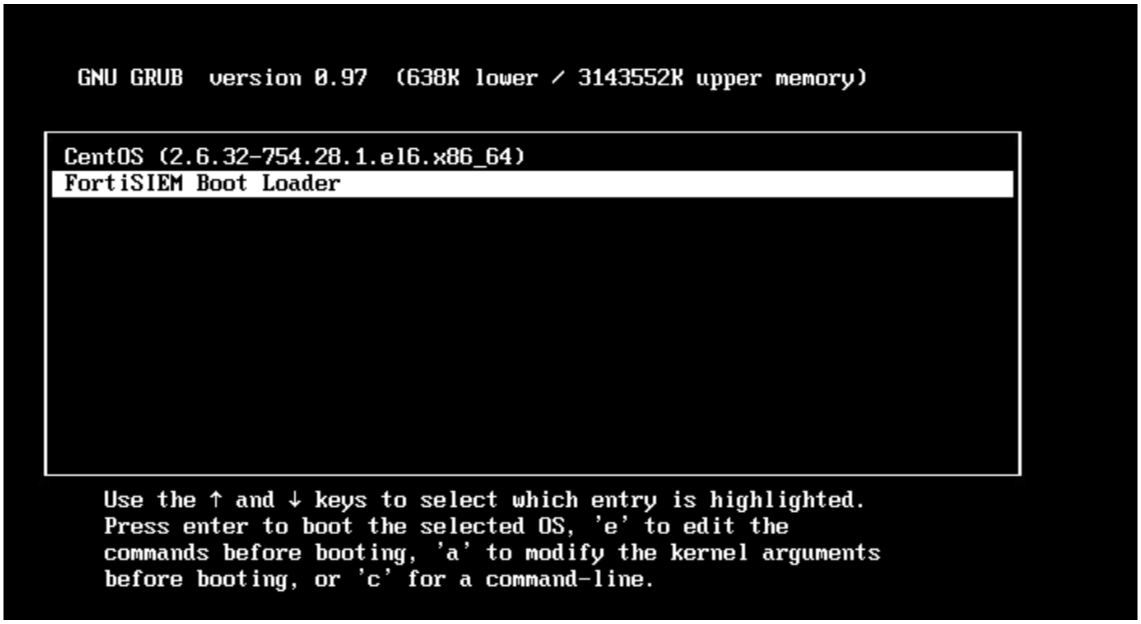
3. The script will open the FortiSIEM bootloader shell.



```
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 34 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.

WARNING: DOS-compatible mode is deprecated. It's strongly recommended to
         switch off the mode (command 'c') and change display units to
         sectors (command 'u').

Command (m for help): Partition number (1-4):
Command (m for help): Command (m for help): Command (m for help): The partition table has been alter
ed!

Calling ioctl() to re-read partition table.

WARNING: Re-reading the partition table failed with error 16: Device or resource busy.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.
Installation finished. No error reported.
This is the contents of the device map /boot/grub/device.map.
Check if this is correct or not. If any of the lines is incorrect,
fix it and re-run the script `grub-install'.

# this device map was generated by anaconda
(hd0)     /dev/sda
(hd4)     /dev/sde
Installation finished. No error reported.
This is the contents of the device map /boot/grub/device.map.
Check if this is correct or not. If any of the lines is incorrect,
fix it and re-run the script `grub-install'.

# this device map was generated by anaconda
(hd0)     /dev/sda
(hd4)     /dev/sde
 Waiting SYSTEM Will be Rebooted
[root@va5727 bootloader]#
```

Note: you might have to reboot the system manually if auto-reboot does not work.

4. In the FortiSIEM bootloader shell, choose **FortiSIEM Boot Loader**. Press Return.

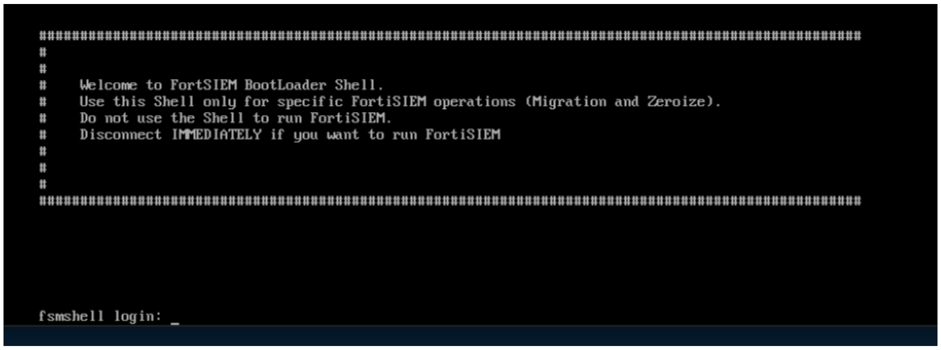


```
    GNU GRUB  version 0.97  (638K lower / 3143552K upper memory)

  CentOS (2.6.32-754.28.1.el6.x86_64)
  FortiSIEM Boot Loader

      Use the ↑ and ↓ keys to select which entry is highlighted.
      Press enter to boot the selected OS, 'e' to edit the
      commands before booting, 'a' to modify the kernel arguments
      before booting, or 'c' for a command-line.
```

Load the FortiSIEM 6.1.2 Image

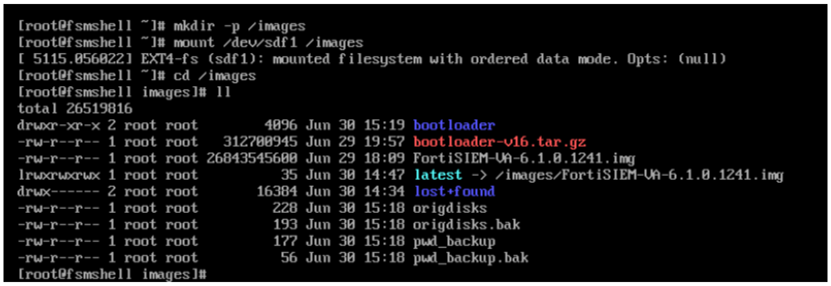
Follow these steps to load the FortiSIEM image:

1. Log in to the bootloader shell as user `root` with password `ProspectHills`.



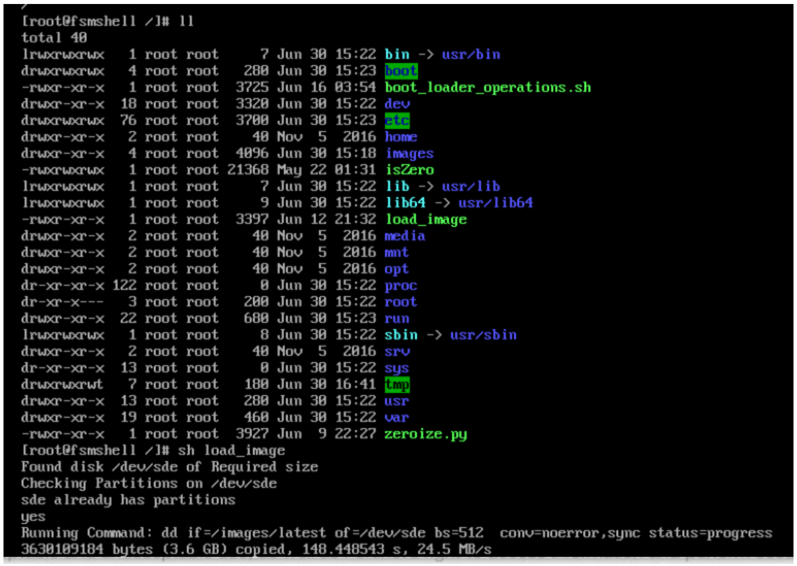
```
####################################################################################################
#
#
#    Welcome to FortSIEM BootLoader Shell.
#    Use this Shell only for specific FortiSIEM operations (Migration and Zeroize).
#    Do not use the Shell to run FortiSIEM.
#    Disconnect IMMEDIATELY if you want to run FortiSIEM
#
#
#
####################################################################################################



fsmshell login: _
```

2. Create and mount the `/data` directory:
   a. Create a `/data` directory, for example:
      ```
      # mkdir -p /data
      ```
      or if using NFS or Elasticsearch storage:
      ```
      # mkdir -p /svn
      ```
   b. Mount the `sdf1` (the 50GB disk) to the `/data` directory, for example:
      ```
      # mount /dev/mapper/FSIEM3500F-phx_data /data
      ```
      or if using NFS or Elasticsearch storage:
      ```
      # mount/dev/mapper/FSIEM3500F-phx_svn /svn
      ```
   c. Create a symbolic link to `images` from `data`:
      ```
      # ln -sf /data/images /images
      ```
      or if using NFS or Elasticsearch storage:
      ```
      # ln -sf /svn/images /images
      ```
   d. Change to the `/images` directory, for example:
      ```
      # cd /images
      ```
   e. Run the `ll` command to check disk usage.
      ```
      # ll
      ```
      These steps are illustrated in the following screen shot.



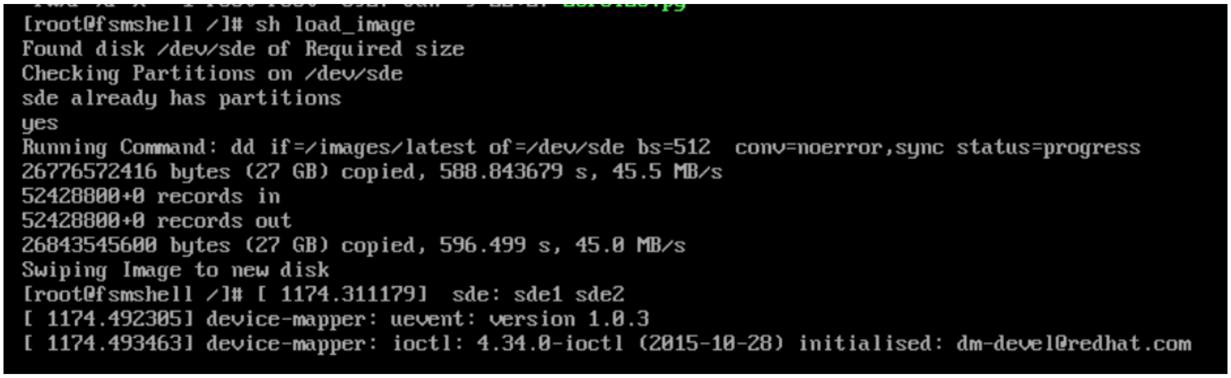
```
[root@fsmshell ~]# mkdir -p /images
[root@fsmshell ~]# mount /dev/sdf1 /images
[ 5115.056022] EXT4-fs (sdf1): mounted filesystem with ordered data mode. Opts: (null)
[root@fsmshell ~]# cd /images
[root@fsmshell images]# ll
total 26519816
drwxr-xr-x 2 root root        4096 Jun 30 15:19 bootloader
-rw-r--r-- 1 root root   312700945 Jun 29 19:57 bootloader-v16.tar.gz
-rw-r--r-- 1 root root 26843545600 Jun 29 18:09 FortiSIEM-VA-6.1.0.1241.img
lrwxrwxrwx 1 root root          35 Jun 30 14:47 latest -> /images/FortiSIEM-VA-6.1.0.1241.img
drwx------ 2 root root       16384 Jun 30 14:34 lost+found
-rw-r--r-- 1 root root         228 Jun 30 15:18 origdisks
-rw-r--r-- 1 root root         193 Jun 30 15:18 origdisks.bak
-rw-r--r-- 1 root root         177 Jun 30 15:18 pwd_backup
-rw-r--r-- 1 root root          56 Jun 30 15:18 pwd_backup.bak
[root@fsmshell images]#
```

3. Run the `load_image` script to swipe the old image with the new image, for example:
   a. Change to the `root` directory and check the contents, for example:
      ```
      # cd /
      # ll
      ```



```
[root@fsmshell /]# ll
total 40
lrwxrwxrwx   1 root root     7 Jun 30 15:22 bin -> usr/bin
drwxrwxrwx   4 root root   280 Jun 30 15:23 boot
-rwxr-xr-x   1 root root  3725 Jun 16 03:54 boot_loader_operations.sh
drwxr-xr-x  18 root root  3320 Jun 30 15:22 dev
drwxrwxrwx  76 root root  3700 Jun 30 15:23 etc
drwxr-xr-x   2 root root    40 Nov  5  2016 home
drwxr-xr-x   4 root root  4096 Jun 30 15:18 images
-rwxrwxrwx   1 root root 21368 May 22 01:31 isZero
lrwxrwxrwx   1 root root     7 Jun 30 15:22 lib -> usr/lib
lrwxrwxrwx   1 root root     9 Jun 30 15:22 lib64 -> usr/lib64
-rwxr-xr-x   1 root root  3397 Jun 12 21:32 load_image
drwxr-xr-x   2 root root    40 Nov  5  2016 media
drwxr-xr-x   2 root root    40 Nov  5  2016 mnt
drwxr-xr-x   2 root root    40 Nov  5  2016 opt
dr-xr-xr-x 122 root root     0 Jun 30 15:22 proc
dr-xr-x---   3 root root   200 Jun 30 15:22 root
drwxr-xr-x  22 root root   680 Jun 30 15:23 run
lrwxrwxrwx   1 root root     8 Jun 30 15:22 sbin -> usr/sbin
drwxr-xr-x   2 root root    40 Nov  5  2016 srv
dr-xr-xr-x  13 root root     0 Jun 30 15:22 sys
drwxrwxrwt   7 root root   180 Jun 30 16:41 tmp
drwxr-xr-x  13 root root   280 Jun 30 15:22 usr
drwxr-xr-x  19 root root   460 Jun 30 15:22 var
-rwxr-xr-x   1 root root  3927 Jun  9 22:27 zeroize.py
[root@fsmshell /]# sh load_image
Found disk /dev/sde of Required size
Checking Partitions on /dev/sde
sde already has partitions
yes
Running Command: dd if=/images/latest of=/dev/sde bs=512  conv=noerror,sync status=progress
3630109184 bytes (3.6 GB) copied, 148.448543 s, 24.5 MB/s
```

b. Run the `load_image` script, for example:
   `# sh load_image`



```
[root@fsmshell /]# sh load_image
Found disk /dev/sde of Required size
Checking Partitions on /dev/sde
sde already has partitions
yes
Running Command: dd if=/images/latest of=/dev/sde bs=512  conv=noerror,sync status=progress
26776572416 bytes (27 GB) copied, 588.843679 s, 45.5 MB/s
52428800+0 records in
52428800+0 records out
26843545600 bytes (27 GB) copied, 596.499 s, 45.0 MB/s
Swiping Image to new disk
[root@fsmshell /]# [ 1174.311179]  sde: sde1 sde2
[ 1174.492305] device-mapper: uevent: version 1.0.3
[ 1174.493463] device-mapper: ioctl: 4.34.0-ioctl (2015-10-28) initialised: dm-devel@redhat.com
```

c. Press Return again when the `load_image` script finishes.

d. Reboot your system manually if it does not do so automatically.

Migrate to FortiSIEM 6.1.2

Follow these steps to complete the migration process:

1. Log in to the bootloader shell as user `root` with password `ProspectHills`. You will immediately be asked to change your password.
2. Create and mount the `/images` directory from `/data`:
   a. Change directory to `root`, for example:
      `# cd /`
   b. Create the `/data` directory, for example:
      `# mkdir -p /data`
      or if using NFS or Elasticsearch storage:
      `# mkdir -p /svn`
   c. Mount the `data` directory and symlink it to `/images`, for example:
      ```
      # mount /dev/mapper/FSIEM3500F-phx_data /data
      # ln -s /data/images /images
      ```

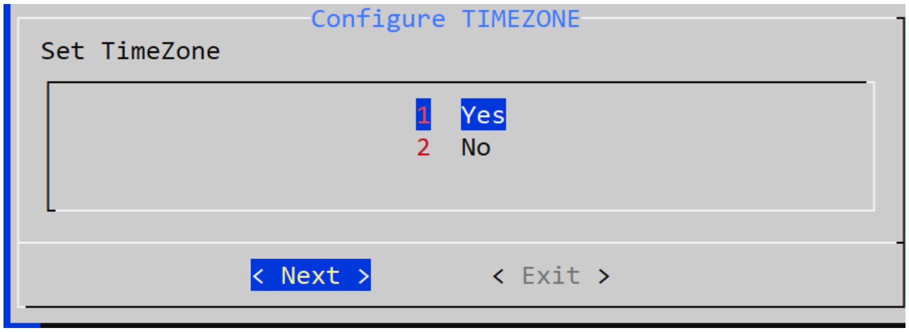
or if using NFS or Elasticsearch storage:

```
# mount /dev/mapper/FSIEM3500F-phx_svn /svn
# ln -s /svn/images /images
```

3. Run the `configFSM.sh` command to configure the migration via a GUI, for example:

```
# configFSM.sh
```

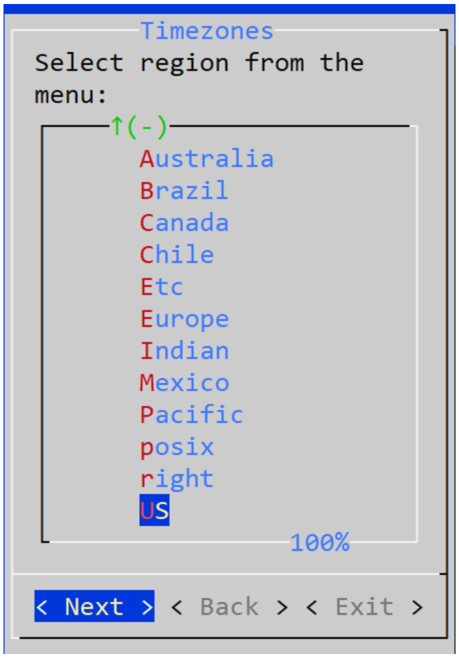
4. In the first screen of the GUI select **1 Yes** to set a timezone. Press **Next**.



Configure TIMEZONE

Set TimeZone

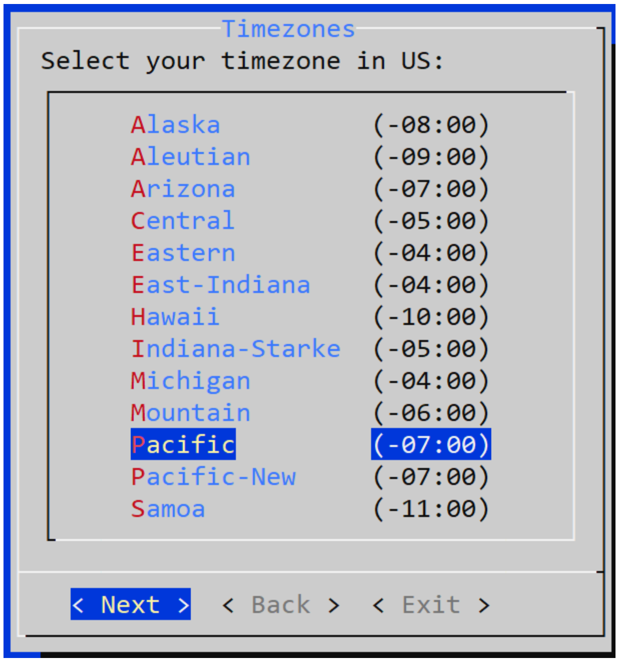
5. Select a region for the timezone. In this example, **US** is selected. Press **Next**.



Timezones

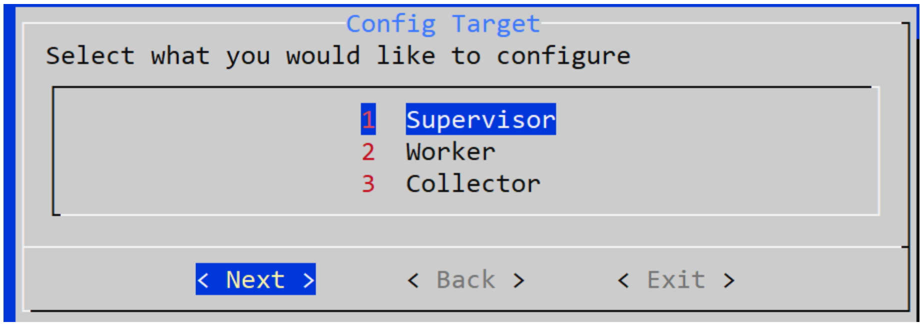
Select region from the menu:

6. Select a timezone in the selected region. In this example, **Pacific** is selected. Press **Next**.



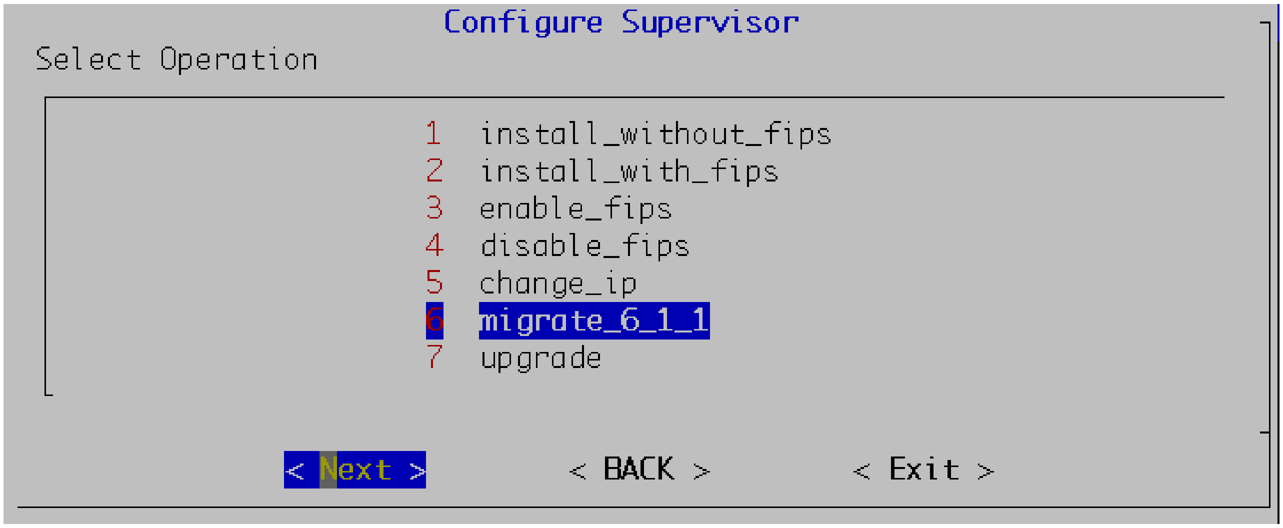
```
                     Timezones
 Select your timezone in US:

      Alaska           (-08:00)
      Aleutian         (-09:00)
      Arizona          (-07:00)
      Central          (-05:00)
      Eastern          (-04:00)
      East-Indiana     (-04:00)
      Hawaii           (-10:00)
      Indiana-Starke   (-05:00)
      Michigan         (-04:00)
      Mountain         (-06:00)
      Pacific          (-07:00)
      Pacific-New      (-07:00)
      Samoa            (-11:00)

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

7. Select a target to configure. In this example, the **Supervisor** is selected. Press **Next**.



```
                       Config Target
 Select what you would like to configure

                          1  Supervisor
                          2  Worker
                          3  Collector

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

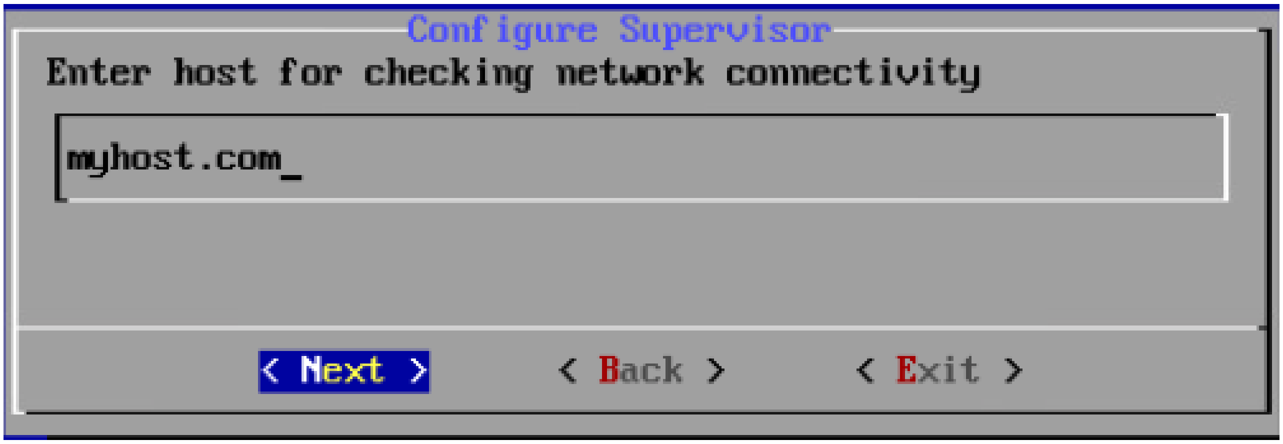
8. Select option **6 migrate_6_1_1**.



```
                     Configure Supervisor
 Select Operation

                         1  install_without_fips
                         2  install_with_fips
                         3  enable_fips
                         4  disable_fips
                         5  change_ip
                         6  migrate_6_1_1
                         7  upgrade

             < Next >        < BACK >        < Exit >
```

9. 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. In order 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**.

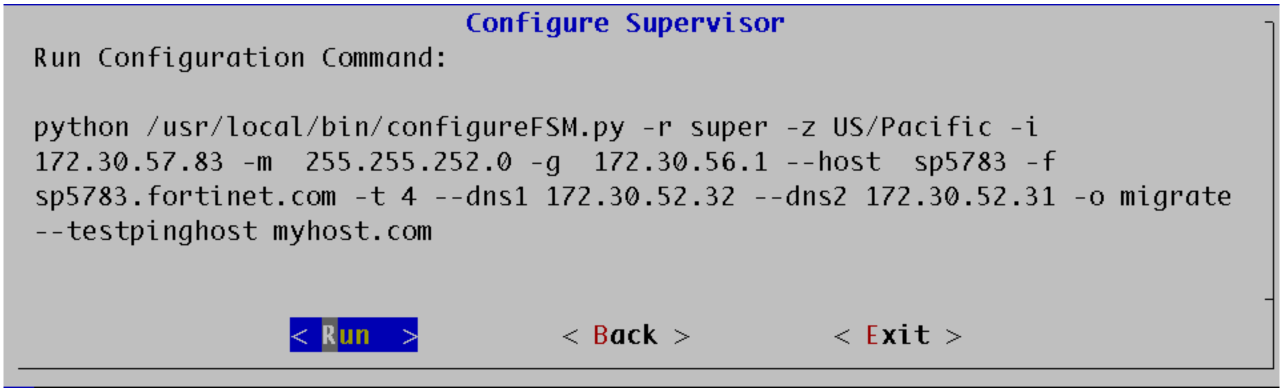


Configure Supervisor

Enter host for checking network connectivity

myhost.com_

10. Press the **Run** command to complete migration, for example:



Configure Supervisor

Run Configuration Command:

```
python /usr/local/bin/configureFSM.py -r super -z US/Pacific -i
172.30.57.83 -m  255.255.252.0 -g  172.30.56.1 --host  sp5783 -f
sp5783.fortinet.com -t 4 --dns1 172.30.52.32 --dns2 172.30.52.31 -o migrate
--testpinghost myhost.com
```

The options for the command 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 DNS server 1 and DNS server 2.
-o	Installation option.

Option	Description
-z	Time zone. Possible values are **US/Pacific**, **Asia/Shanghai**, **Europe/London**, or **Africa/Tunis**
--testpinghost	The host used to test connectivity

11. The script will take some minutes to run. When it is finished, migration is complete.
12. Log in to your system again as user `root` with your new password.
13. To ensure `phMonitor` is running, execute the `phstatus` command, for example:

```
# phstatus
```

Migrate Cluster Installation

This section provides instructions on how to migrate Supervisor, Workers, and Collectors separately in a cluster environment,

- Delete Workers
- Migrate Supervisor
- Install New Worker(s)
- Register Workers
- Set Up Collector-to-Worker Communication
- Working with Pre-6.1.0 Collectors
- Install 6.1.2 Collectors
- Register 6.1.2 Collectors

Delete Workers

1. Login to the Supervisor.
2. Go to **Admin > License > Nodes** and delete the Workers one-by-one.
3. Go to the **Admin > Cloud Health** page and make sure that the Workers are not present.
   Note that the Collectors will buffer events while the Workers are down.
4. Shutdown the Workers.
   SSH to the Workers one-by-one and shutdown the Workers.

Migrate Supervisor

Follow the steps in Migrate All-in-one Installation to migrate the supervisor node. **Note:** FortiSIEM 6.1.2 does not support Worker or Collector migration.

Install New Worker(s)

Follow the steps in Installing Workers to install new Workers. You can either keep the same IP address or change the address.

Register Workers

Follow the steps in Registering Workers to register the newly created 6.1.2 Workers to the 6.1.2 Supervisor. The 6.1.2 FortiSIEM Cluster is now ready.

Set Up Collector-to-Worker Communication

1. Go to **Admin > Systems > Settings**.
2. Add the Workers to the Event Worker or Query Worker as appropriate.
3. Click **Save**.

Working with Pre-6.1.0 Collectors

Pre-6.1.0 Collectors and agents will work with 6.1.2 Supervisor and Workers. You can install 6.1.2 collectors at your convenience.

Install 6.1.2 Collectors

FortiSIEM does not support Collector migration to 6.1.2. You can install new 6.1.2 Collectors and register them to 6.1.2 Supervisor in a specific way so that existing jobs assigned to Collectors and Windows agent associations are not lost. Follow these steps:

1. Copy the http hashed password file (`/etc/httpd/accounts/passwds`) from the old Collector.
2. Disconnect the pre-6.1.2 Collector.
3. Install the 6.1.2 Collector with the old IP address.
4. Copy the saved http hashed password file (`/etc/httpd/accounts/passwds`) from the old Collector to the 6.1.2 Collector.
   This step is needed for Agents to work seamlessly with 6.1.2 Collectors. The reason for this step is that when the Agent registers, a password for Agent-to-Collector communication is created and the hashed version is stored in the Collector. During 6.1.2 migration, this password is lost.

Register 6.1.2 Collectors

To register collectors, use the `--update` option instead of `--add` in the `phProvisionCollector` command. Other than this, use exactly the same parameters that were used to register the pre-`6.1.2` Collector. Specifically, use this form of the

`phProvisionCollector` command to register a `6.1.2` Collector and keep the old associations:

```
# /opt/phoenix/bin/phProvisionCollector --update <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.

Re-install new Windows Agents with the old `InstallSettings.xml` file. Both the migrated and the new agents will work. The new Linux Agent and migrated Linux Agent will also work.

Upgrading From 6.1.2 to 6.2.0 or Later Releases

See the standard Upgrade Guide in 6.2.0 or later releases in the 6.2 FortiSIEM Reference Manuals section. The upgrade process is the same for VM installations and hardware appliances.