FortiSIEM - 500F Collector Configuration Guide

Version 6.1.2

01/03/2024
FortiSIEM 6.1.2 500F Collector Configuration Guide

TABLE OF CONTENTS

Appliance Setup

This document describes how to setup the FSM-500F appliance.

- Fresh Installation
- Factory Reset
- Upgrading FortiSIEM Collector
- Appliance Re-image

Fresh Installation

- Step 1: Rack mount the FSM-500F Appliance
- Step 2: Power On the FSM-500F Appliance
- Step 3: Verify System Information
- Step 4: Configure FortiSIEM via GUI
- Step 5: Register Collectors
- Step 6: Using FortiSIEM

Step 1: Rack mount the FSM-500F Appliance

1. Follow FortiSIEM 500F QuickStart Guide to mount FSM-500F into rack.
2. Connect FSM-500F to the network by connecting an Ethernet cable to Port1.

Before proceeding to the next step, connecting Ethernet cable to Port1 is required for Network configuration.

Step 2: Power On the FSM-500F Appliance

1. Make sure the FSM-500F device is connected to a Power outlet and an Ethernet cable is connected to Port1.
2. Power On the FSM-500F device.

Step 3: Verify System Information

1. Connect to the FSM-500F appliance using VGA port or Console port.
2. Login as user `root` with password `ProspectHills`.
3. You will be asked to change your password. Once you change the password, you will be logged out. Login again with your new password.

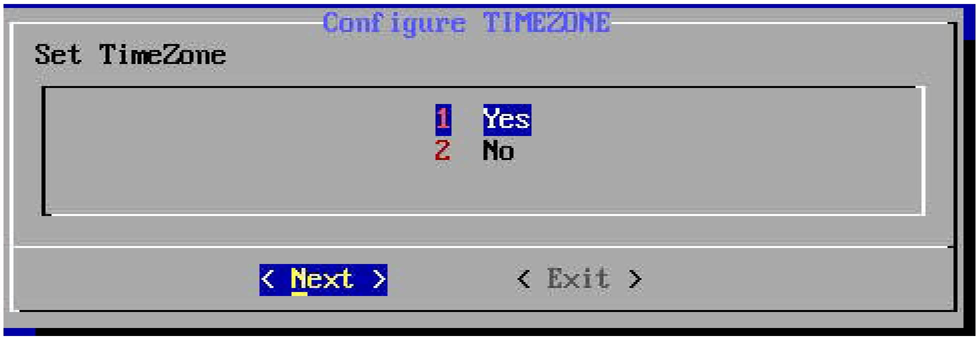
Note this password—you will need it in a later step.

4. Run `get` to check the available FortiSIEM commands.
5. Use the below 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

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`
   A simple GUI will open.
3. In the GUI, select **1 Set Timezone** and then press **Next**.

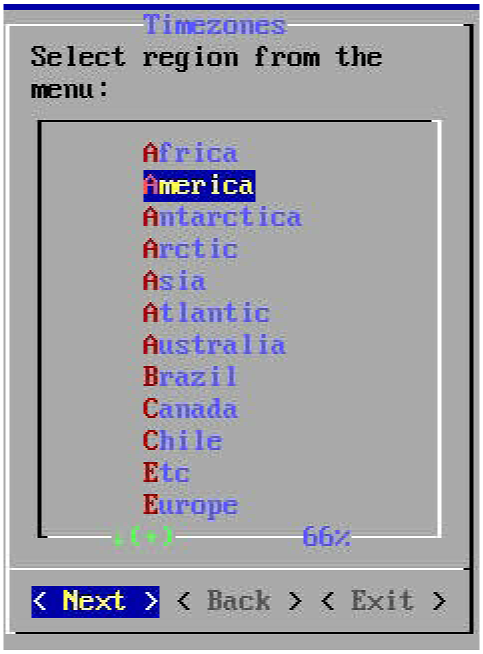


Configure TIMEZONE

Set TimeZone

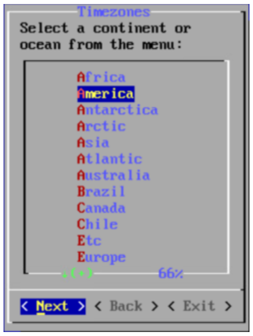
1 Yes
2 No

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



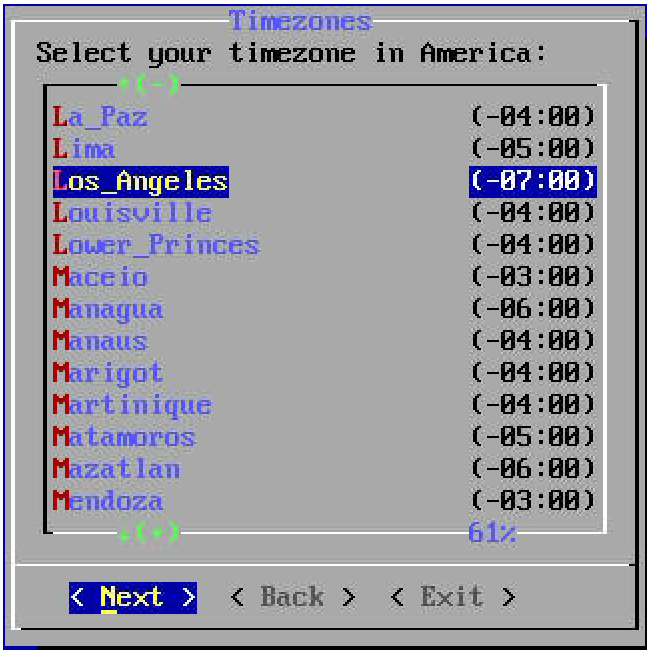
Select region from the menu:

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



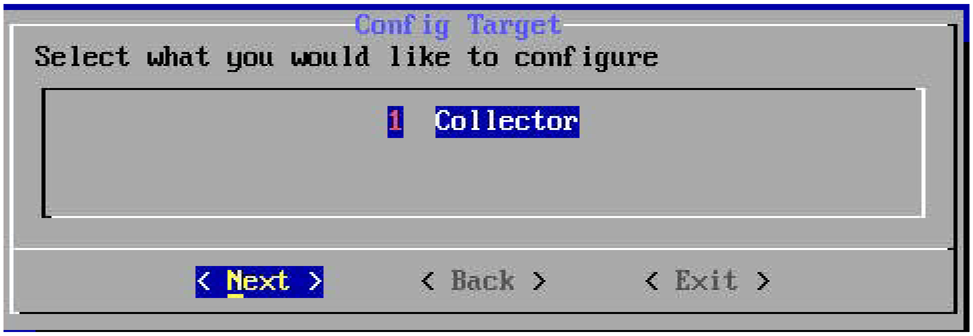
Select a continent or ocean from the menu:

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



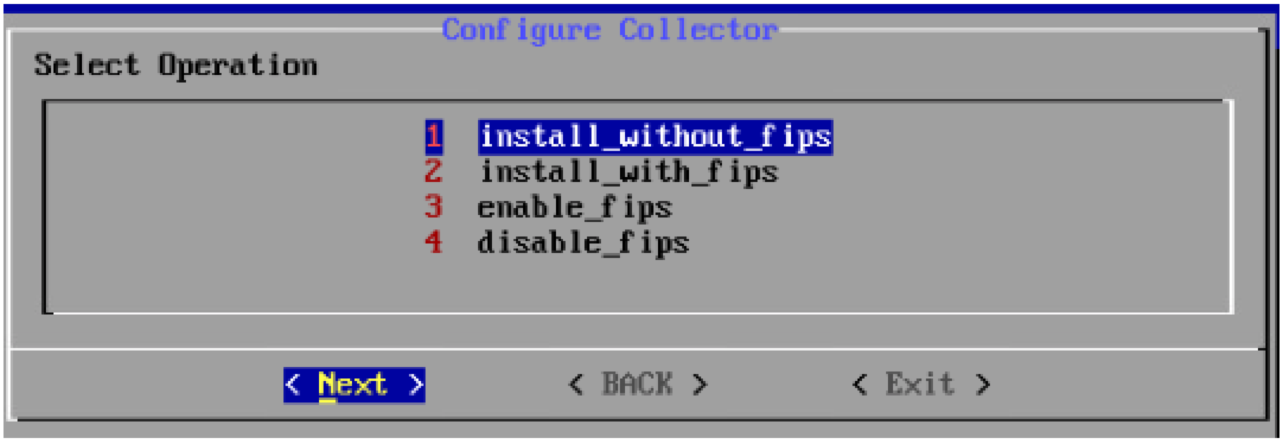
```
                 Timezones
Select your timezone in America:
  ┌───↑(-)──────────────────────────┐
  │La_Paz                  (-04:00) │
  │Lima                    (-05:00) │
  │Los_Angeles             (-07:00) │
  │Louisville              (-04:00) │
  │Lower_Princes           (-04:00) │
  │Maceio                  (-03:00) │
  │Managua                 (-06:00) │
  │Manaus                  (-04:00) │
  │Marigot                 (-04:00) │
  │Martinique              (-04:00) │
  │Matamoros               (-05:00) │
  │Mazatlan                (-06:00) │
  │Mendoza                 (-03:00) │
  └───↓(+)─────────────────61%──────┘

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

7. Select **1 Collector**. Press **Next.**



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

                    1  Collector


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

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

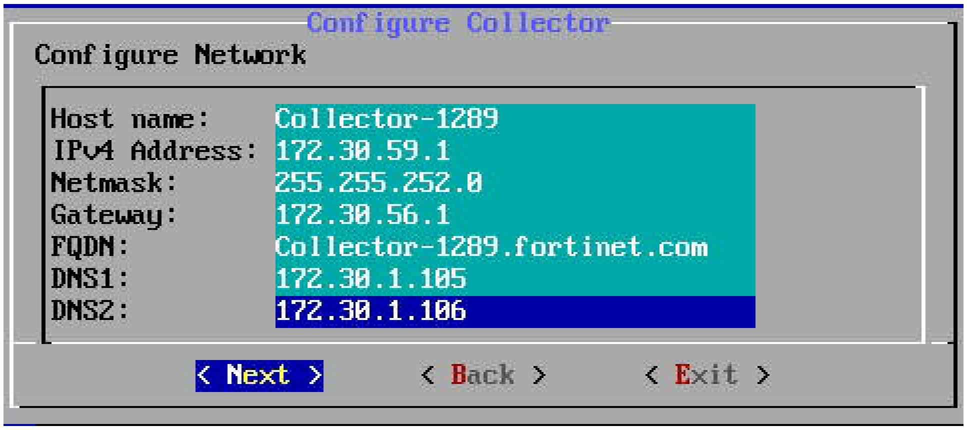


```
                    Configure Collector
Select Operation

                       1  install_without_fips
                       2  install_with_fips
                       3  enable_fips
                       4  disable_fips


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

9. When prompted, enter the information for these network components to configure the Static IP address: **IP Address**, **Netmask**, **Gateway**, **DNS Server(s).**Configure the network by entering the following fields.
Press **Next.**

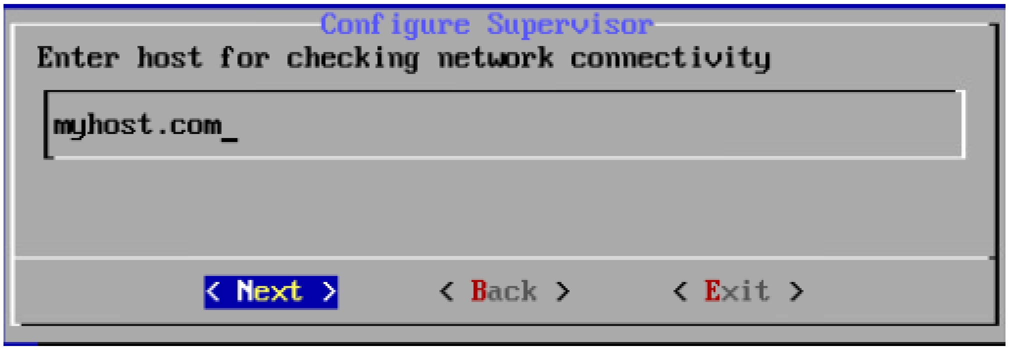
Note the IP Address—you will need it in a later step.

Option	Description
Host Name	Collector's host name
IPv4 Address	The Collector's IPv4 address
NetMask	The Collector's subnet
Gateway	Network gateway address
FQDN	Fully-qualified domain name
DNS1, DNS2	Addresses of DNS server 1 and DNS server 2



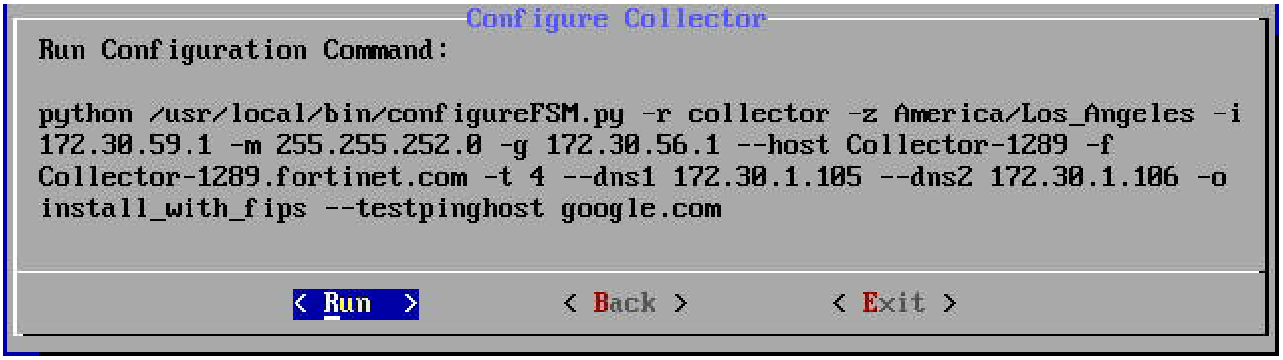
```
Configure Collector
Configure Network

Host name:     Collector-1289
IPv4 Address:  172.30.59.1
Netmask:       255.255.252.0
Gateway:       172.30.56.1
FQDN:          Collector-1289.fortinet.com
DNS1:          172.30.1.105
DNS2:          172.30.1.106
```

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**.



```
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**.



```
Run Configuration Command:

python /usr/local/bin/configureFSM.py -r collector -z America/Los_Angeles -i
172.30.59.1 -m 255.255.252.0 -g 172.30.56.1 --host Collector-1289 -f
Collector-1289.fortinet.com -t 4 --dns1 172.30.1.105 --dns2 172.30.1.106 -o
install_with_fips --testpinghost google.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 server 1 and DNS server 2.
-o	Installation option.
-z	Time zone. Examples of possible values are **US/Pacific**, **Asia/Shanghai**, **Europe/London**, or **Africa/Tunis**
--testpinghost	The URL used to test connectivity

Once the configuration is complete, the system reboots automatically.

Step 5: Register Collectors

Collectors can be deployed in Enterprise or Service Provider environments.

- Enterprise Deployments
- Service Provider Deployments

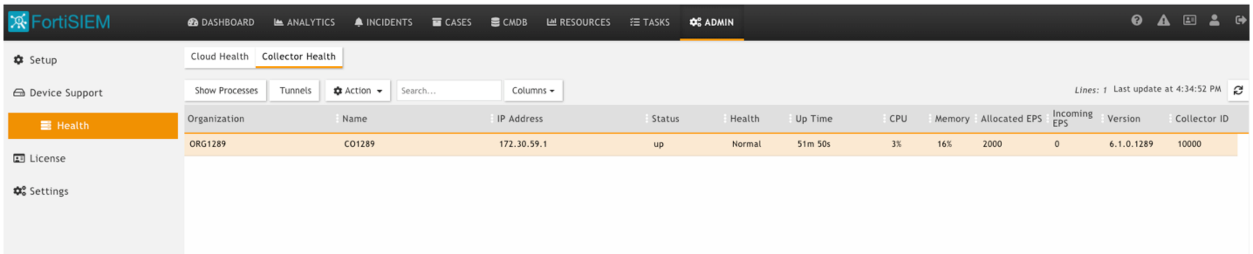
Enterprise Deployments

For enterprise deployments, follow these steps:

1. Log in to Supervisor with **Admin** privileges.
2. Go to **ADMIN > Settings > System > Event Worker**.
   a. Enter the IP of the Worker node. If a Supervisor node is only used, then enter the IP of the Supervisor node. Multiple IP addresses can be entered on separate lines. In this case, the Collectors will load balance the upload of events to the listed Event Workers.
   Note: Rather than using IP addresses, a DNS name is recommended. The reasoning is, should the IP addressing change, it becomes a matter of updating the DNS rather than modifying the Event Worker IP addresses in FortiSIEM.
   b. Click **OK**.
3. Go to **ADMIN > Setup > Collectors** and add a Collector by entering:
   a. **Name** – Collector name.
   b. **Guaranteed EPS** – This is the EPS that the Collector will always be able to send. It could send more if there is excess EPS available.
   c. **Start Time** and **End Time** – set to **Unlimited**.
4. SSH to the Collector and run following script to register Collectors:

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

   The password should be enclosed in single quotes to ensure that any non-alphanumeric characters are escaped.
   a. Set *`user`* and *`password`* using the admin user name and password for the Supervisor.
   b. Set *`Super IP or Host`* as the Supervisor's IP address.
   c. Set *`Organization`*. For Enterprise deployments, the default name is Super.
   d. Set *`CollectorName`* from Step 2a.
   The Collector will reboot during the Registration.
5. Go to **ADMIN > Health > Collector Health** to see the Collector status.



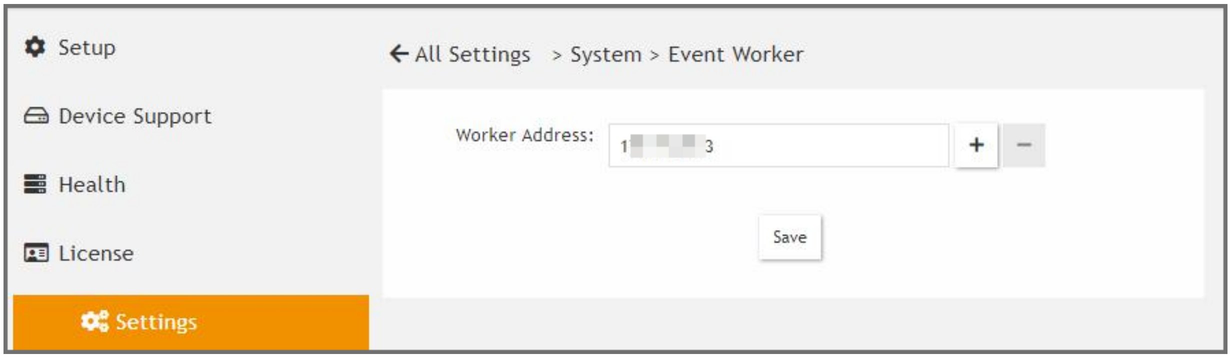
Organization	Name	IP Address	Status	Health	Up Time	CPU	Memory	Allocated EPS	Incoming EPS	Version	Collector ID
ORG1289	CO1289	172.30.59.1	up	Normal	51m 50s	3%	16%	2000	0	6.1.0.1289	10000

Service Provider Deployments

For Service Provider deployments, follow these steps.

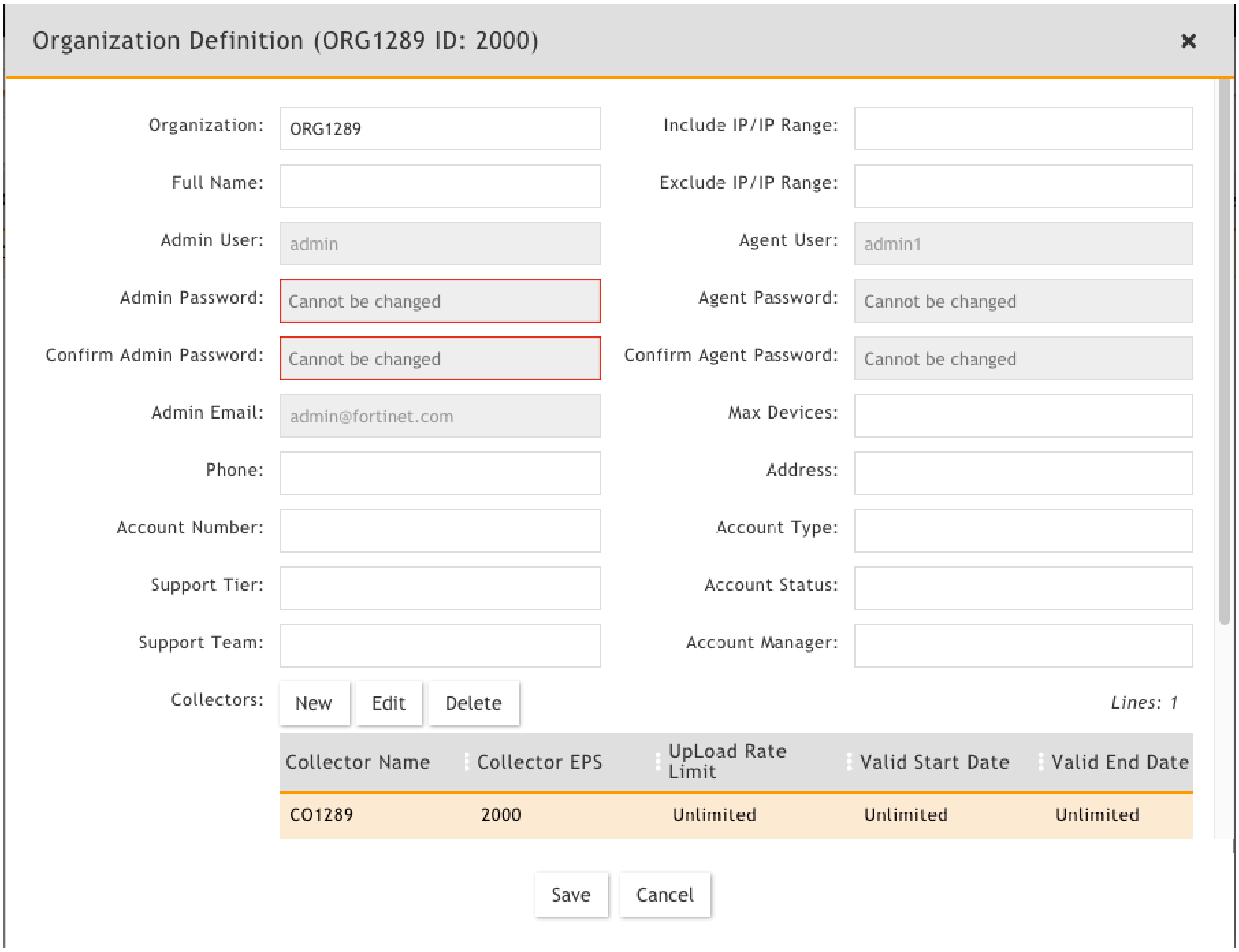
1. Log in to Supervisor with **Admin** privileges.
2. Go to **ADMIN > Settings > System > Event Worker**.
   a. Enter the IP of the Worker node. If a Supervisor node is only used, then enter the IP of the Supervisor node. Multiple IP addresses can be entered on separate lines. In this case, the Collectors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



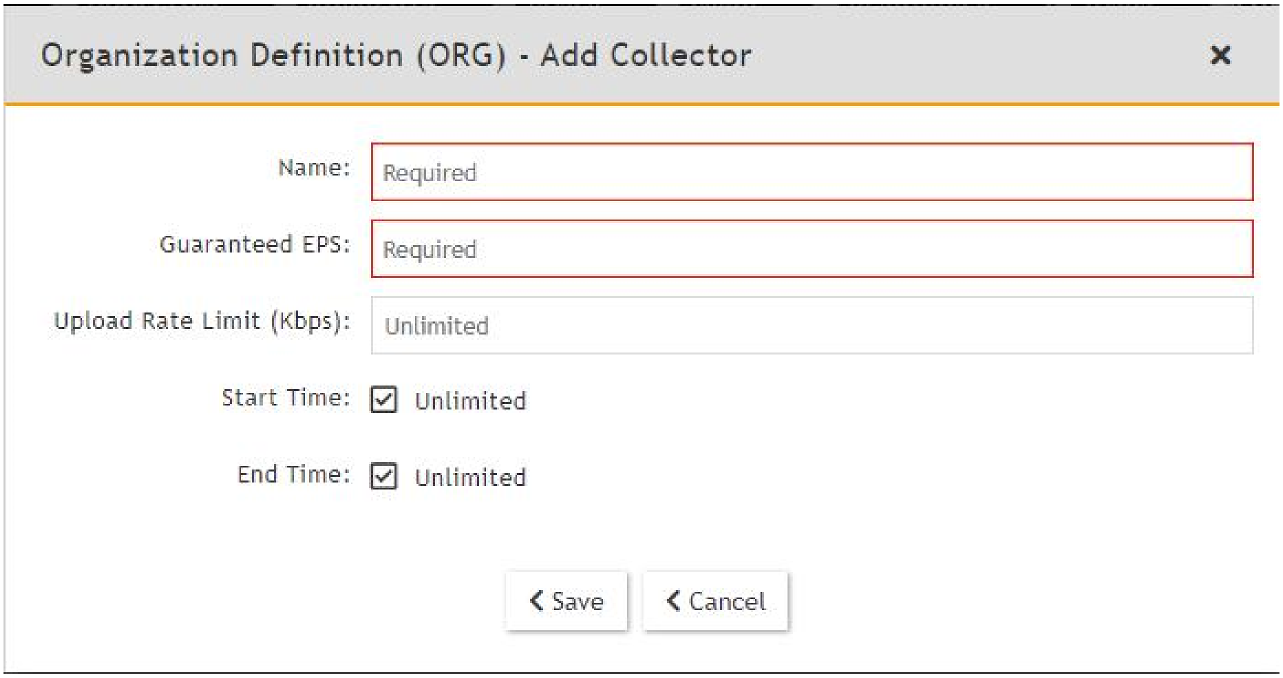
Organization Definition (ORG1289 ID: 2000)

Organization:	ORG1289	Include IP/IP Range:	
Full Name:		Exclude IP/IP Range:	
Admin User:	admin	Agent User:	admin1
Admin Password:	Cannot be changed	Agent Password:	Cannot be changed
Confirm Admin Password:	Cannot be changed	Confirm Agent Password:	Cannot be changed
Admin Email:	admin@fortinet.com	Max Devices:	
Phone:		Address:	
Account Number:		Account Type:	
Support Tier:		Account Status:	
Support Team:		Account Manager:	

Collectors: *Lines: 1*

Collector Name	Collector EPS	UpLoad Rate Limit	Valid Start Date	Valid End Date
CO1289	2000	Unlimited	Unlimited	Unlimited

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:

```
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 by command line, for example:

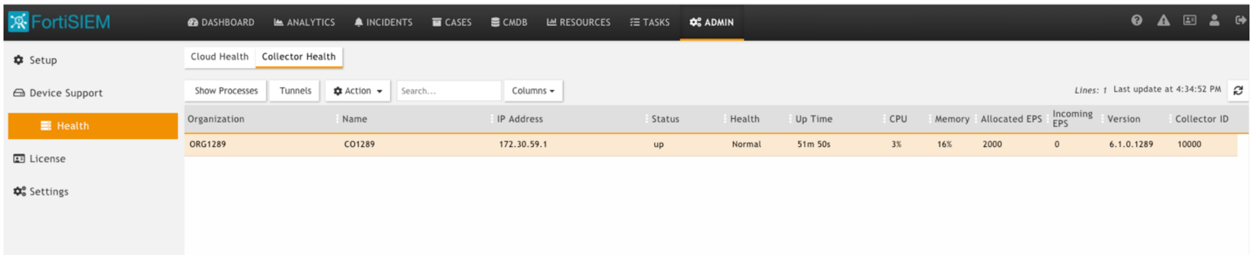
      ```
      # phProvisionCollector --add admin Admin*11 172.30.53.130 ORG1289 CO1289
      ```

      A message will display after the completion:

      ```
         Continuing to provision the Collector
         This collector is registered successfully. Normal Exit and restart of phMonitor
              after collector license registration.
      ```

      The Collector will reboot during the Registration.

8. Go to **ADMIN > Health > Collector Health** to see the status of the Collector.



Organization	Name	IP Address	Status	Health	Up Time	CPU	Memory	Allocated EPS	Incoming EPS	Version	Collector ID
ORG1289	CO1289	172.30.59.1	up	Normal	51m 50s	3%	16%	2000	0	6.1.0.1289	10000

Step 6: Using FortiSIEM

Refer to the FortiSIEM User Guide for detailed information about using FortiSIEM.

Factory Reset

Follow the steps below to perform factory reset on FortiSIEM FSM-500F.

Step 1: Uninstall FortiSIEM application

1. Connect FortiSIEM device using VGA or Console port.
2. Login as ‘root’ user with password 'ProspectHills'.
3. To check the available FortiSIEM commands, run `get`.
4. To uninstall FortiSIEM, run `execute fsm-clean`.
   This script will uninstall FortiSIEM Collector.

Step 2: Reinstall FortiSIEM application

1. Power on the hardware.
2. Login as ‘root’ user with password 'ProspectHills'.
3. To check Hardware status and RAID information, run `diagnose hardware info`.
   Note: RAID Information is NOT applicable to FSM-500F model.
4. To install FortiSIEM Collector, run ‘`execute factoryreset`’.
   Note: This script takes 5 minutes to complete FortiSIEM Collector installation.

Follow the steps under Appliance Setup **to configure FSM-500F.**

Upgrading FortiSIEM Collector

For upgrading FortiSIEM Collector, refer to the *Upgrade Guide.*

Appliance Re-image

Ensure that the following prerequisites are met before re-imaging FortiSIEM.

Hardware	Software
Peripherals • USB Keyboard • USB Mouse • VGA Monitor **USB Thumbdrive** • 4 GB Thumbdrive (for Linux installation) • 8 GB Thumbdrive (for FortiSIEM appliance image)	• Ubuntu Desktop Setup Files • Rufus (Bootable USB Utility) • FortiSIEM Appliance Image

Follow the below steps to re-image FortiSIEM.

Step 1: Create Bootable Linux Image

1. Connect 4 GB USB drive to the system (desktop or laptop).
2. Open Rufus.
3. Select the following settings for the USB:
   a. **Partition scheme and target system type**: MBR partition scheme for BIOS or UEFI
   b. **File system**: FAT32
   c. **Cluster size**: 4096 bytes (Default)
   d. **Quick Format**: Enable
   e. **Create a bootable disk using**: ISO image
4. Click on the 'CD-ROM' icon and select the Ubuntu Setup ISO.
5. Click **Start** and allow Rufus to complete.
   Once finished, the disk is ready to boot.
   Note: Alternatively, you can use the Ubuntu guide for creating a USB drive with Ubuntu.

Step 2: Copy FortiSIEM Collector image to USB

1. Connect 8 GB USB Drive to the system (desktop or laptop).
2. Open **Windows Explorer** > right-click **Drive** > click **Format**.
3. Select the following options:
   a. **File system**: NTFS
   b. **Allocation unit size**: 4096 bytes
   c. **Quick Format**: Enable
4. Copy the image file to USB drive. For example:
   `FSM_Full_All_RAW_HARDWARE_6.1.2.0119.zip`
5. Safely remove the USB drive from the desktop or laptop by unmounting it through the operating system.

Step 3: Prepare 500F by removing FSM

1. Connect to the console/SSH of the FortiSIEM appliance.
2. Run the following command: `execute fsm-clean`
3. Allow this command to run and power-off the FortiSIEM appliance.

Step 4: Configure 500F BIOS to Boot into USB Drive

1. Connect the 4 GB USB drive to the FortiSIEM appliance.
2. Power on the FortiSIEM appliance.
3. During the boot screen, press **F11** to login to the boot options.
4. Select the option to enter into the BIOS set up.
5. Select the option for Boot options.

6. Select the 'USB drive'.
7. Save the options and quit set up.

Step 5: Re-image 500F boot drive from USB Linux

1. Power on FortiSIEM appliance.
2. Once the FortiSIEM appliance loads from the USB drive, click **Try Ubuntu**.
3. Connect the 8GB USB drive to the FortiSIEM appliance.
4. Open a terminal.
5. Type the following command to identify the FortiSIEM boot disk (29.5GB): `sudo fdisk -l`.
   Note: This drive will be referred as `/dev/sdb` in the following steps.
6. Enter into root while in the terminal using the following command:
   `sudo -s`
7. Determine the mount point of this drive by using the following command:
   `df -l`
   Note: For this guide, the assumption for the 8GB mount point is: `/media/ubuntu/123456789/*`
8. Copy the image from the 8GB disk to the FortiSIEM boot disk.
9. Extract the zipped raw image and copy the image into SATA disk (32GB). For example, use the command:

   ```
   # unzip -c FSM_Full_All_RAW_HARDWARE_6.1.2.0119.zip | dd of=/dev/sdb bs=1M
   status=progress
   ```

10. Once this is completed, power off the FortiSIEM appliance using the following commands:
    `shutdown -h now`
11. After shutdown, remove both USB drives from the FortiSIEM appliance.
12. Power on FortiSIEM appliance.
13. Reinstall FortiSIEM application (as in Factory Reset - step 2).

Migrating from Pre-6.1.2 to 6.1.2

This section describes how upgrade the 500F Collector appliance from any older FortiSIEM version to 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 Collector Installation

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 the `/opt` directory `# mount /dev/mapper/FSIEM500F-phx_opt` disk exists.
3. Log in to your FSM as `root` and run the following commands:
   ```
   # mkdir -p /opt/images
   # ln -s /opt/images /images
   ```
4. 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_0119.
   ```
5. Create a soft link to `images`, for example:
   ```
   # ln -sf /images/FortiSIEM-RAW-Hardware-6.1.2.0119.img /images/latest
   ```

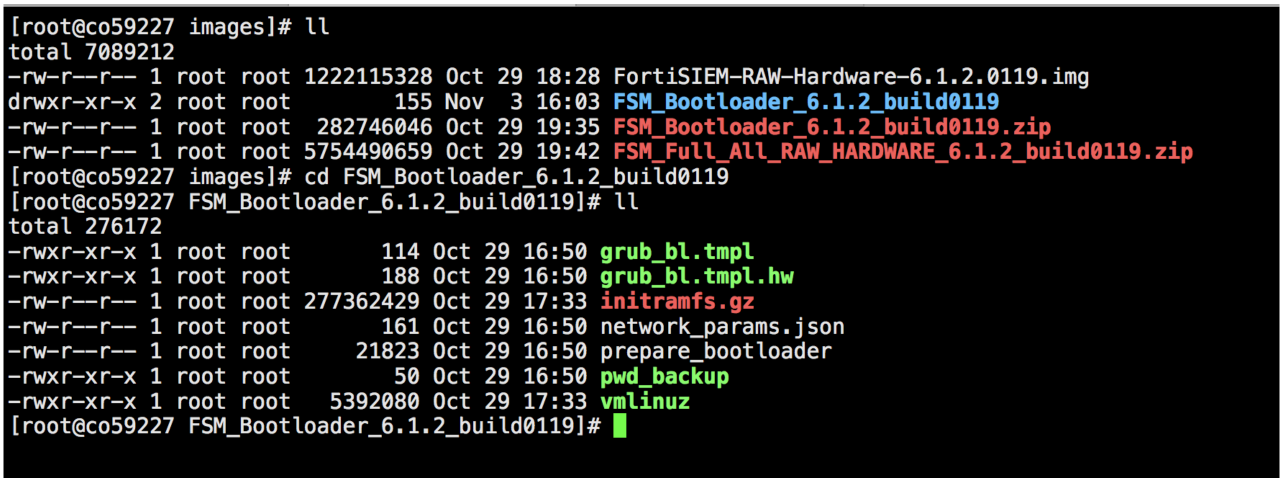
Migrate Collector Installation

- Download the Bootloader
- Prepare the Bootloader
- Load the FortiSIEM 6.1.2 Image
- Migrate to FortiSIEM 6.1.2
- Restore the HTTP Password File From Backup
- Re-Register to the Supervisor
- Reboot the Appliance

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
   ```

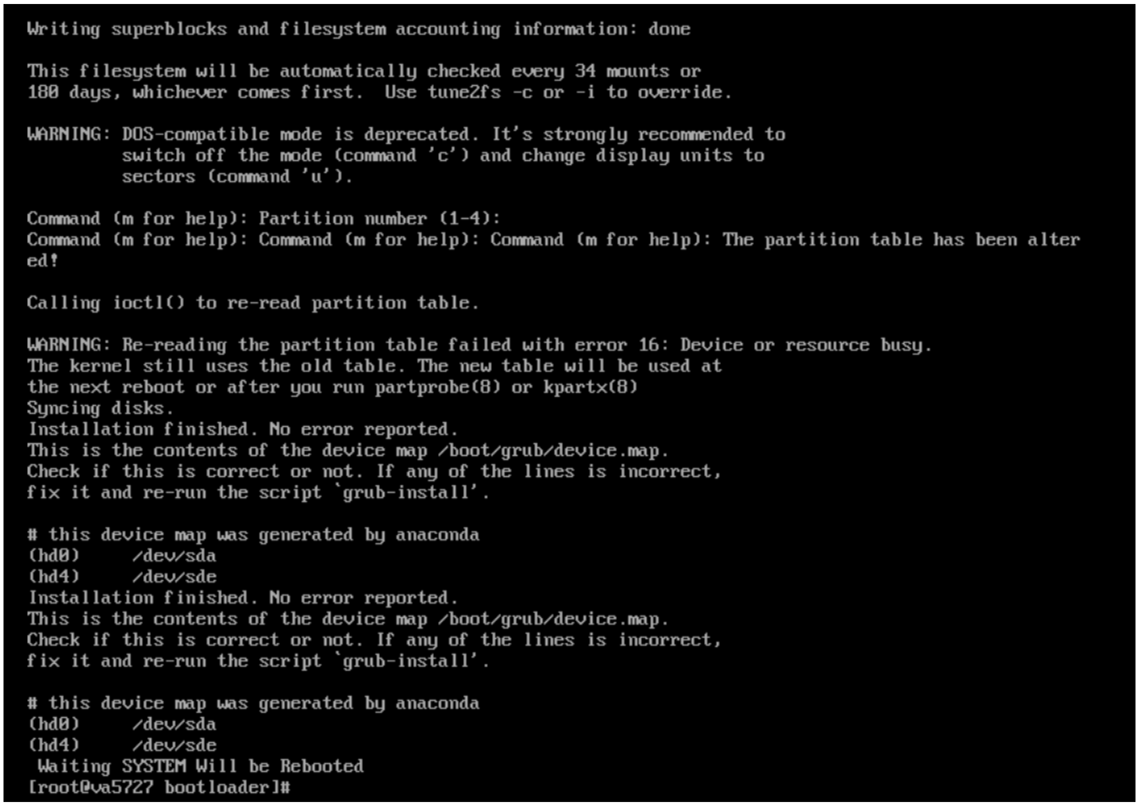


```
[root@co59227 images]# ll
total 7089212
-rw-r--r-- 1 root root 1222115328 Oct 29 18:28 FortiSIEM-RAW-Hardware-6.1.2.0119.img
drwxr-xr-x 2 root root        155 Nov  3 16:03 FSM_Bootloader_6.1.2_build0119
-rw-r--r-- 1 root root  282746046 Oct 29 19:35 FSM_Bootloader_6.1.2_build0119.zip
-rw-r--r-- 1 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:

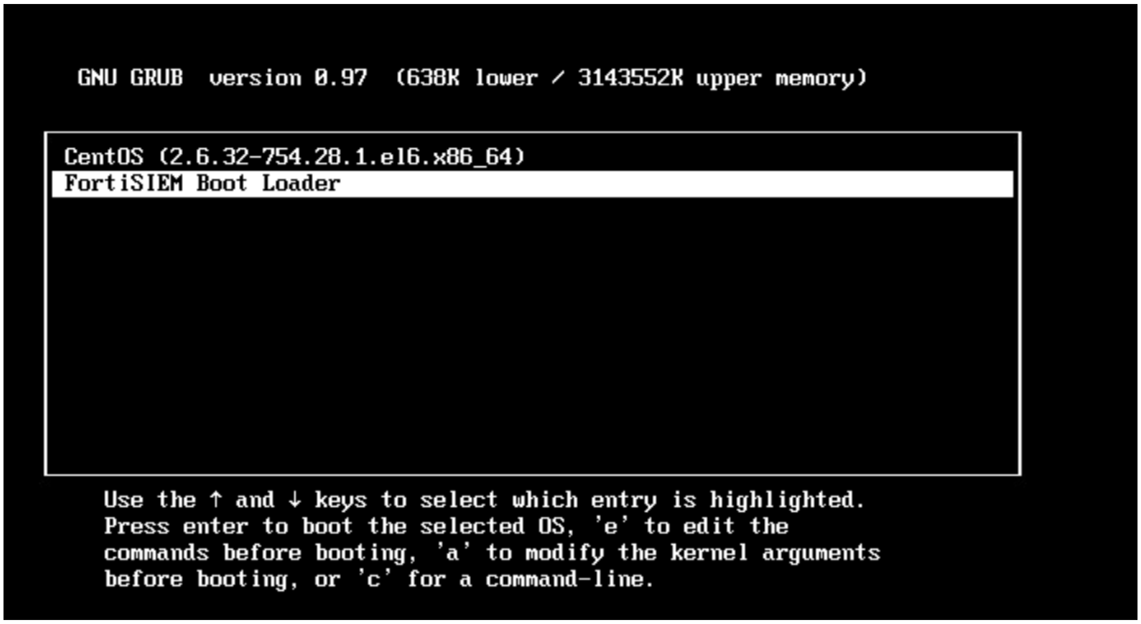
1. Go to the `bootloader` directory, for example:
   `# cd /images/FSM_Bootloader_6.1.2_build0119`
2. Run the `prepare_bootloader` script to install and configure the bootloader. This script installs, configures, and reboots the system. The script may take a few minutes to complete.
   `# sh prepare_bootloader`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

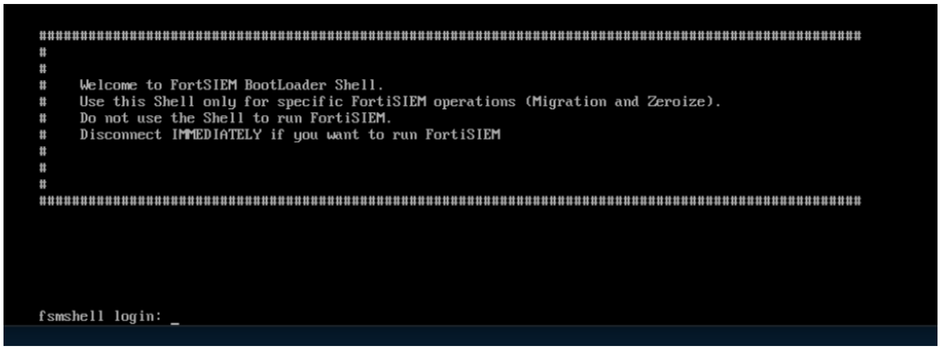


```
   GNU GRUB  version 0.97  (638K lower / 3143552K upper memory)

  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

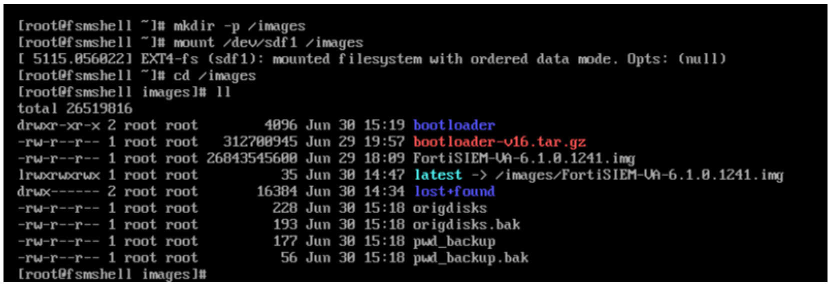
Follow these steps to load the FortiSIEM image:

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



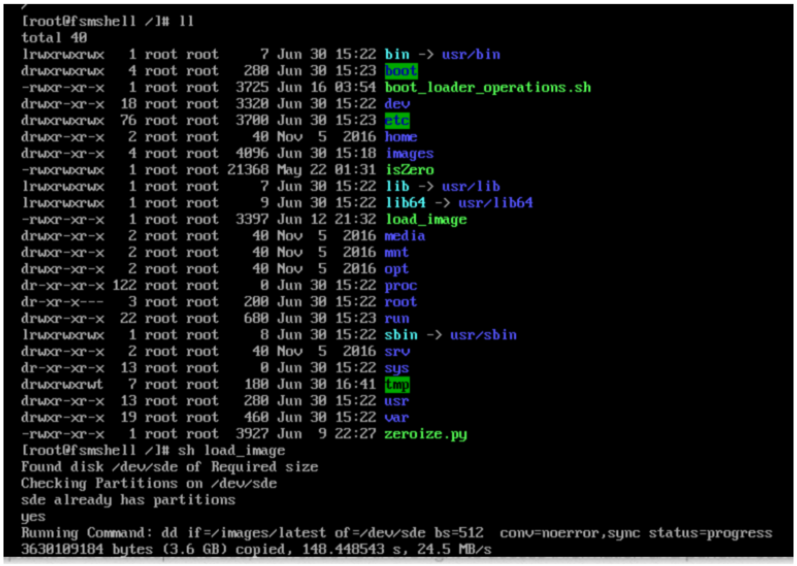
```
####################################################################################################
#
#
#    Welcome to FortSIEM BootLoader Shell.
#    Use this Shell only for specific FortiSIEM operations (Migration and Zeroize).
#    Do not use the Shell to run FortiSIEM.
#    Disconnect IMMEDIATELY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



fsmshell login: _
```

2. Mount the `/opt` directory:
   a. Mount the `/opt` directory, for example:
      `# mount /dev/mapper/FSIEM500F-phx_opt /opt`
   b. Create a symbolic link to images from `opt`:
      `# ln -sf /opt/images /images`
   c. Change to the `/images` directory, for example:
      `# cd /images`
   d. Run the `ll` command to check disk usage.
      `# ll`
      These steps are illustrated in the following screen shot.



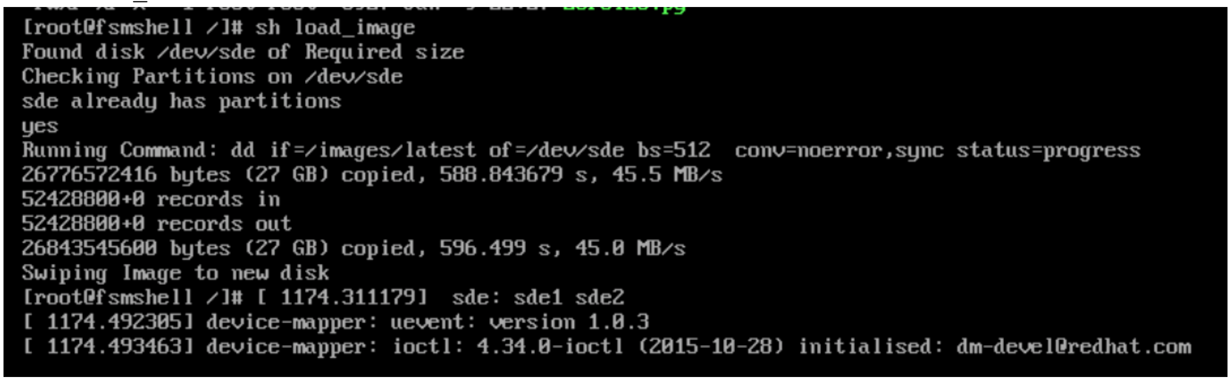
```
[root@fsmshell ~]# mkdir -p /images
[root@fsmshell ~]# mount /dev/sdf1 /images
[ 5115.056022] EXT4-fs (sdf1): mounted filesystem with ordered data mode. Opts: (null)
[root@fsmshell ~]# cd /images
[root@fsmshell images]# ll
total 26519816
drwxr-xr-x 2 root root        4096 Jun 30 15:19 bootloader
-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`



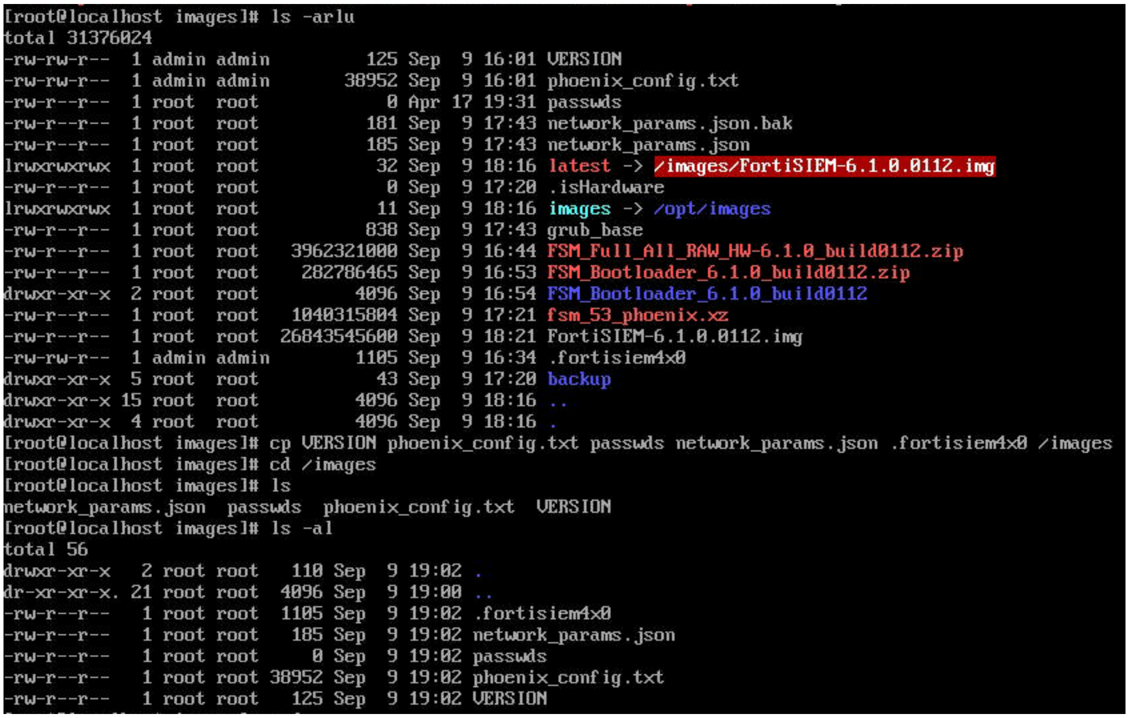
```
[root@fsmshell /]# sh load_image
Found disk /dev/sde of Required size
Checking Partitions on /dev/sde
sde already has partitions
yes
Running Command: dd if=/images/latest of=/dev/sde bs=512  conv=noerror,sync status=progress
26776572416 bytes (27 GB) copied, 588.843679 s, 45.5 MB/s
52428800+0 records 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

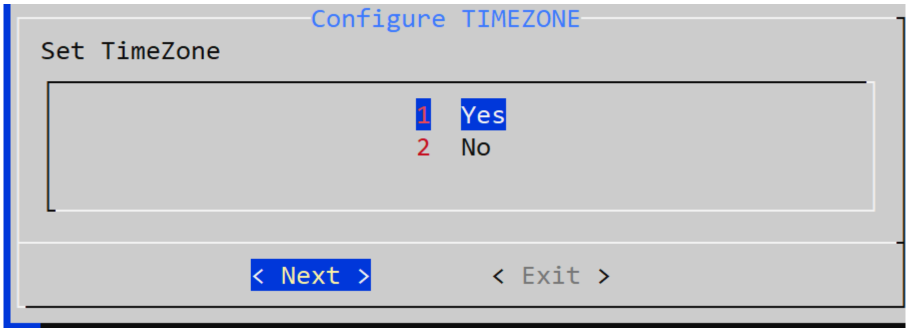
Follow these steps to complete the migration process:

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 `/opt`:
   - **a.** Change directory to `root`, for example:
     ```
     # cd /
     ```
   - **b.** Mount the `opt` directory, for example:
     ```
     # mount /dev/mapper/FSIEM500F-phx_opt /opt
     ```
   - **c.** Create images directory under `/`:
     ```
     # mkdir -p /images
     ```
   - **d.** Copy backup files to `/images` directory from `/opt/images` directory:
     ```
     # cd /opt/images
     # cp -far fsm_53_phoenix.xz VERSION phoenix_config.txt passwds network_params.json
           .fortisiem4x0 /images
     ```

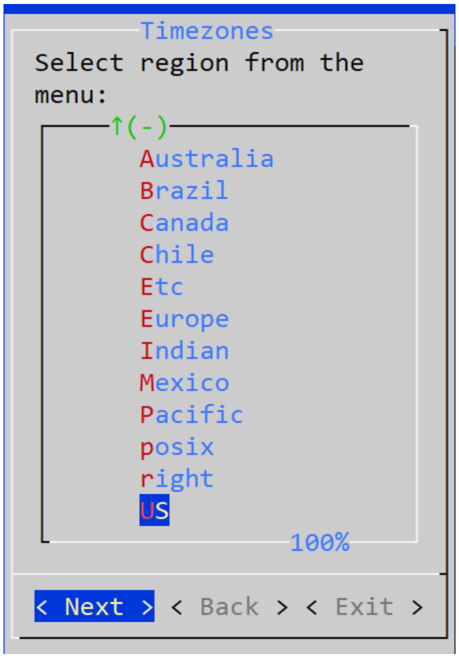


```
[root@localhost images]# ls -arlu
total 31376024
-rw-rw-r--  1 admin admin        125 Sep  9 16:01 VERSION
-rw-rw-r--  1 admin admin      38952 Sep  9 16:01 phoenix_config.txt
-rw-r--r--  1 root  root           0 Apr 17 19:31 passwds
-rw-r--r--  1 root  root         181 Sep  9 17:43 network_params.json.bak
-rw-r--r--  1 root  root         185 Sep  9 17:43 network_params.json
lrwxrwxrwx  1 root  root          32 Sep  9 18:16 latest -> /images/FortiSIEM-6.1.0.0112.img
-rw-r--r--  1 root  root           0 Sep  9 17:20 .isHardware
lrwxrwxrwx  1 root  root          11 Sep  9 18:16 images -> /opt/images
-rw-r--r--  1 root  root         838 Sep  9 17:43 grub_base
-rw-r--r--  1 root  root  3962321000 Sep  9 16:44 FSM_Full_All_RAW_HW-6.1.0_build0112.zip
-rw-r--r--  1 root  root   282786465 Sep  9 16:53 FSM_Bootloader_6.1.0_build0112.zip
drwxr-xr-x  2 root  root        4096 Sep  9 16:54 FSM_Bootloader_6.1.0_build0112
-rw-r--r--  1 root  root  1040315804 Sep  9 17:21 fsm_53_phoenix.xz
-rw-r--r--  1 root  root 26843545600 Sep  9 18:21 FortiSIEM-6.1.0.0112.img
-rw-rw-r--  1 admin admin       1105 Sep  9 16:34 .fortisiem4x0
drwxr-xr-x  5 root  root          43 Sep  9 17:20 backup
drwxr-xr-x 15 root  root        4096 Sep  9 18:16 ..
drwxr-xr-x  4 root  root        4096 Sep  9 18:16 .
[root@localhost images]# cp VERSION phoenix_config.txt passwds network_params.json .fortisiem4x0 /images
[root@localhost images]# cd /images
[root@localhost images]# ls
network_params.json  passwds  phoenix_config.txt  VERSION
[root@localhost images]# ls -al
total 56
drwxr-xr-x   2 root root   110 Sep  9 19:02 .
dr-xr-xr-x. 21 root root  4096 Sep  9 19:00 ..
-rw-r--r--   1 root root  1105 Sep  9 19:02 .fortisiem4x0
-rw-r--r--   1 root root   185 Sep  9 19:02 network_params.json
-rw-r--r--   1 root root     0 Sep  9 19:02 passwds
-rw-r--r--   1 root root 38952 Sep  9 19:02 phoenix_config.txt
-rw-r--r--   1 root root   125 Sep  9 19:02 VERSION
```

   - **e.** Unmount the `/opt` directory from `root`:
     ```
     # cd /
     # umount /opt
     ```
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**.

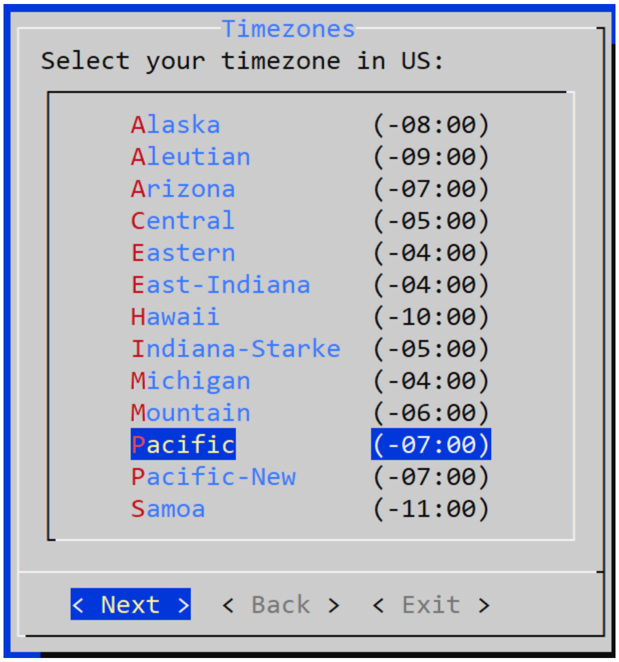


5. Select a region for the timezone. In this example, **US** is selected. Press **Next**.



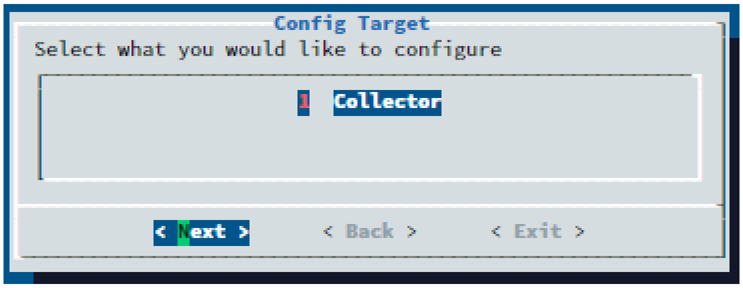
```
              Timezones
  Select region from the
  menu:
   ┌────────↑(-)────────────────┐
   │        Australia           │
   │        Brazil              │
   │        Canada              │
   │        Chile               │
   │        Etc                 │
   │        Europe              │
   │        Indian              │
   │        Mexico              │
   │        Pacific             │
   │        posix               │
   │        right               │
   │        US                  │
   └────────────────100%────────┘

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

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 >
```

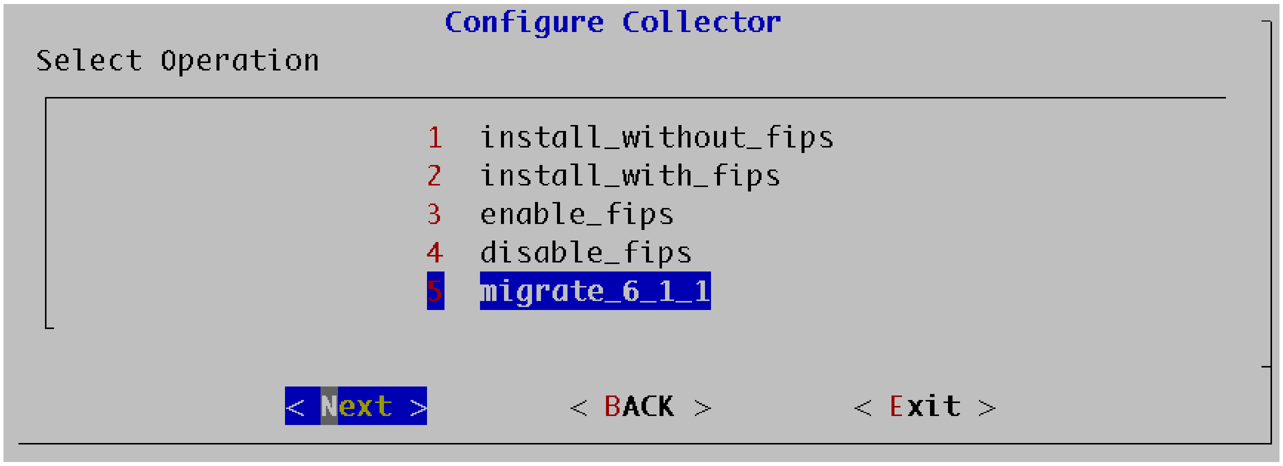
7. Select a target to configure. In this example, the **Collector** is selected. Press **Next**.



Config Target

Select what you would like to configure

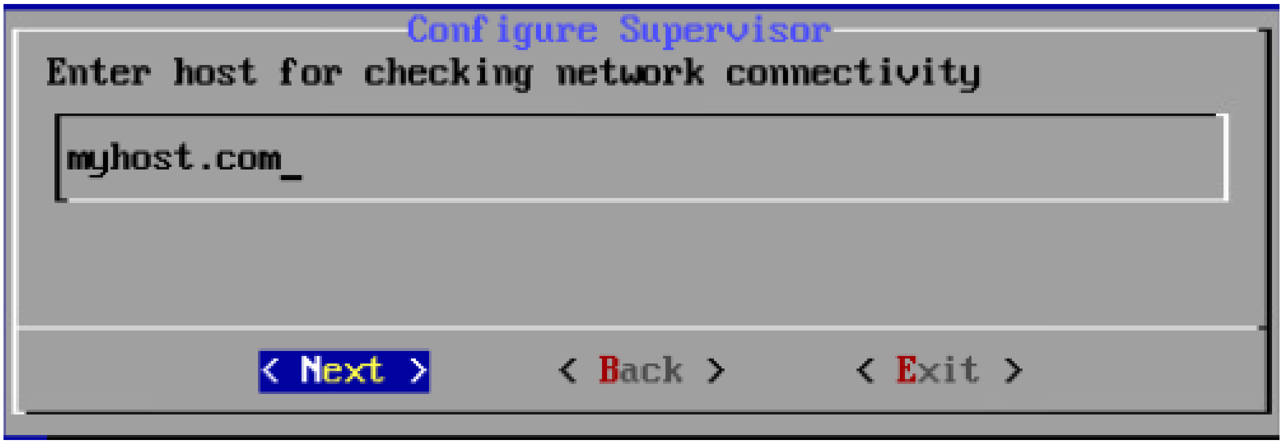
8. Select option **5 migrate_6_1_1**.



Configure Collector

Select Operation

9. Test connectivity by connecting to a well-known internet site. Press **Next**.

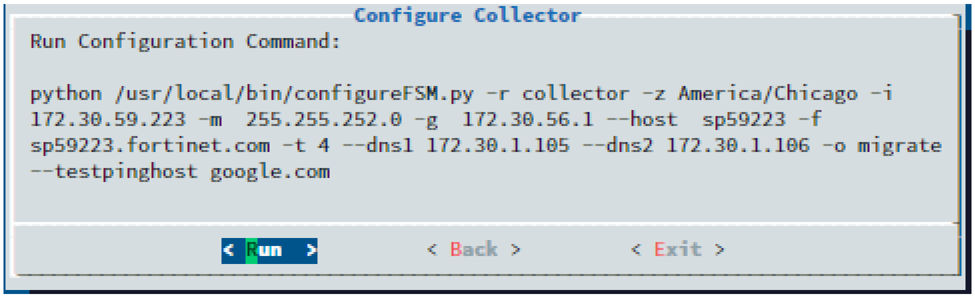


Configure Supervisor

Enter host for checking network connectivity

myhost.com_

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



Configure Collector

Run Configuration Command:

```
python /usr/local/bin/configureFSM.py -r collector -z America/Chicago -i
172.30.59.223 -m  255.255.252.0 -g  172.30.56.1 --host  sp59223 -f
sp59223.fortinet.com -t 4 --dns1 172.30.1.105 --dns2 172.30.1.106 -o migrate
--testpinghost google.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.
-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
    ```

Restore the HTTP Password File From Backup

Run the following command to restore the HTTP password file.

```
# cp -far /images/passwds /etc/httpd/accounts/
```

Make sure that the permissions are correct, for example:

```
[root@co56120 ~]# ls -la /etc/httpd/accounts/
total 8
drwxr-xr-x 2 root root 34 Nov 3 09:47 .
drwxr-xr-x 6 root root 121 Oct 29 18:02 ..
-rw-r--r-- 1 root root 62 Nov 3 13:36 passwds
```

Re-Register to the Supervisor

Run the following command; note the `update` option. This keeps old associations.

```
# /opt/phoenix/bin/phProvisionCollector --update <user> '<password>' <Super IP or Host>
```

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

Reboot the Appliance

If the appliance does not reboot automatically, then manually reboot.