500F Collector Configuration Guide

FortiSIEM 6.7.0

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

01/03/2024
FortiSIEM 6.7.0 500F Collector Configuration Guide

TABLE OF CONTENTS

Appliance Setup

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

Fresh Installation

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

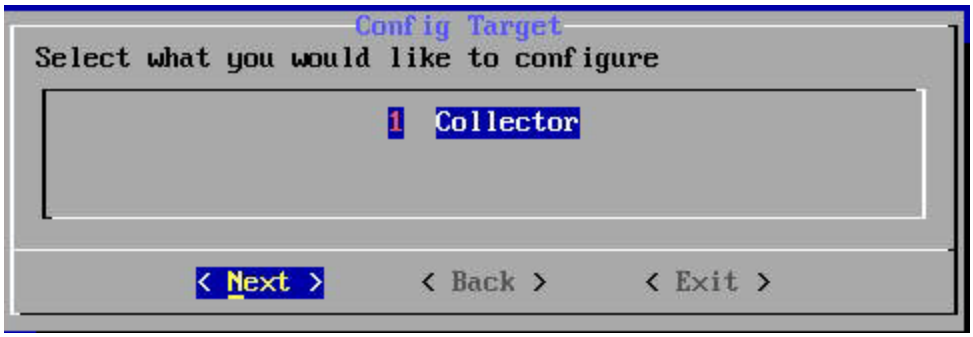
1. Log in as user root with the password you set in Step 3 above.
2. At the command prompt, go to `/usr/local/bin`, and enter `configFSM.sh`. For example:
   ```
   # configFSM.sh
   ```
   A simple GUI will open.
3. In the GUI, select **1 Set Timezone**, and then press **Next**.

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

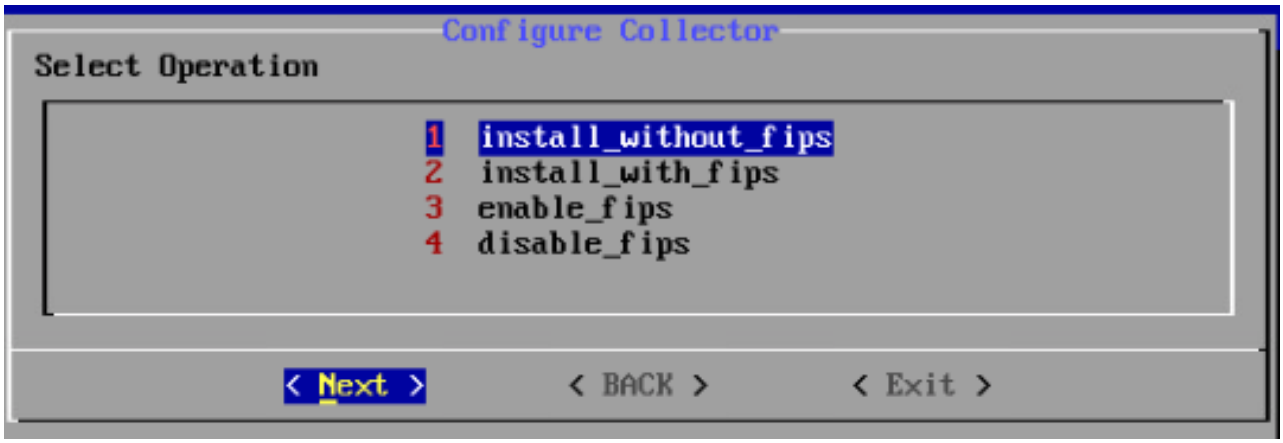
5. Select your **Country**, and press **Next**.

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

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



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



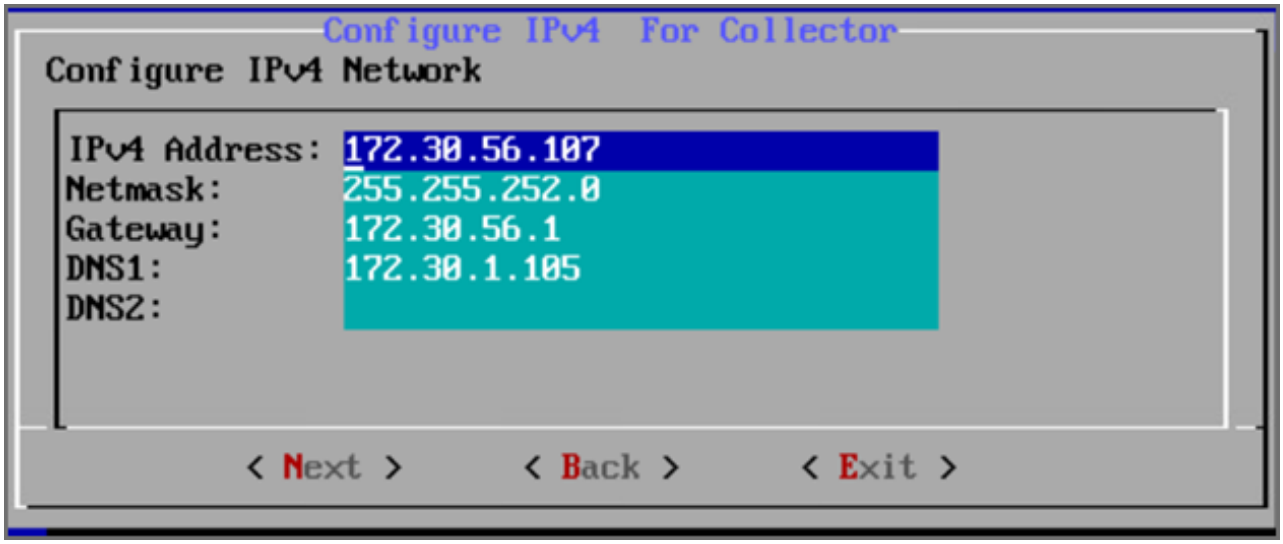
9. Determine whether your network supports IPv4-only, IPv6-only, or both IPv4 and IPv6 (Dual Stack). Choose **1** for IPv4-only, choose **2** for IPv6-only, or choose **3** for both IPv4 and IPv6.

10. If you choose **1** (IPv4) or choose **3** (Both IPv4 and IPv6), and press **Next**, then you will move to step 11. If you choose **2** (IPv6), and press **Next**, then skip to step 12.
11. 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: Configuring a DNS Server to resolve external addresses as updates to remote repositories will be required in

the future.

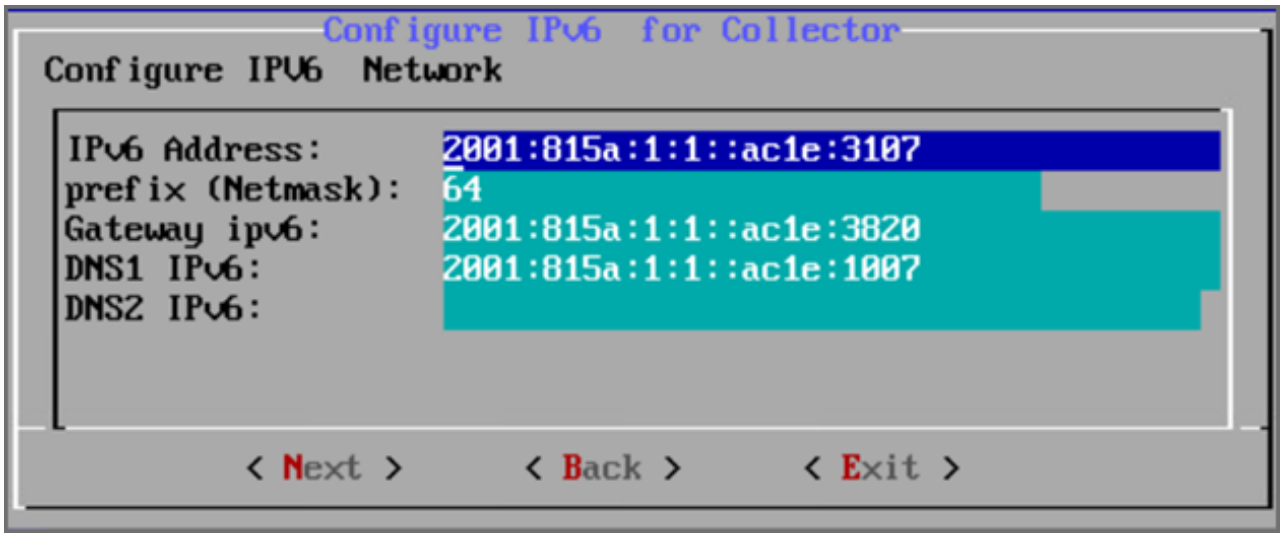
Note the IP Address—you will need it in a later step.

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



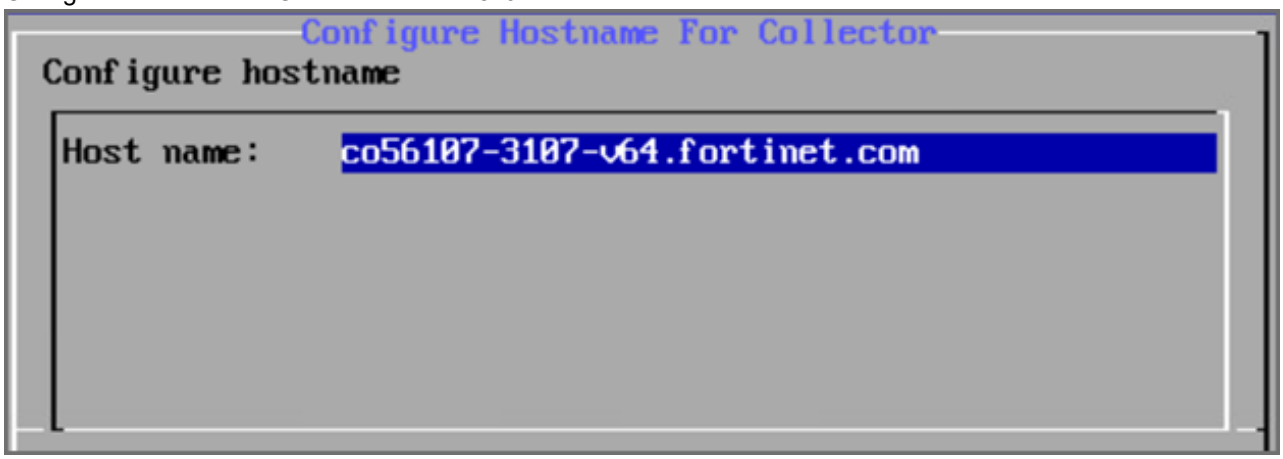
12. If you chose **1** in step 9, then you will need to skip to step 13. If you chose **2** or **3** in step 9, then you will configure the IPv6 network by entering the following fields, then press **Next**.

Option	Description
IPv6 Address	The Collector's IPv6 address
prefix (Netmask)	The Collector's IPv6 prefix
Gateway ipv6	IPv6 Network gateway address
DNS1 IPv6, DNS2 IPv6	Addresses of the IPv6 DNS server 1 and DNS server2



Note: If you chose option **3** in step 9 for both IPv4 and IPv6, then even if you configure 2 DNS servers for IPv4 and IPv6, the system will only use the first DNS server from IPv4 and the first DNS server from the IPv6 configuration.
Note: In many dual stack networks, IPv4 DNS server(s) can resolve names to both IPv4 and IPv6. In such environments, if you do not have an IPv6 DNS server, then you can use public IPv6 DNS servers or use IPv4-mapped IPv6 address.

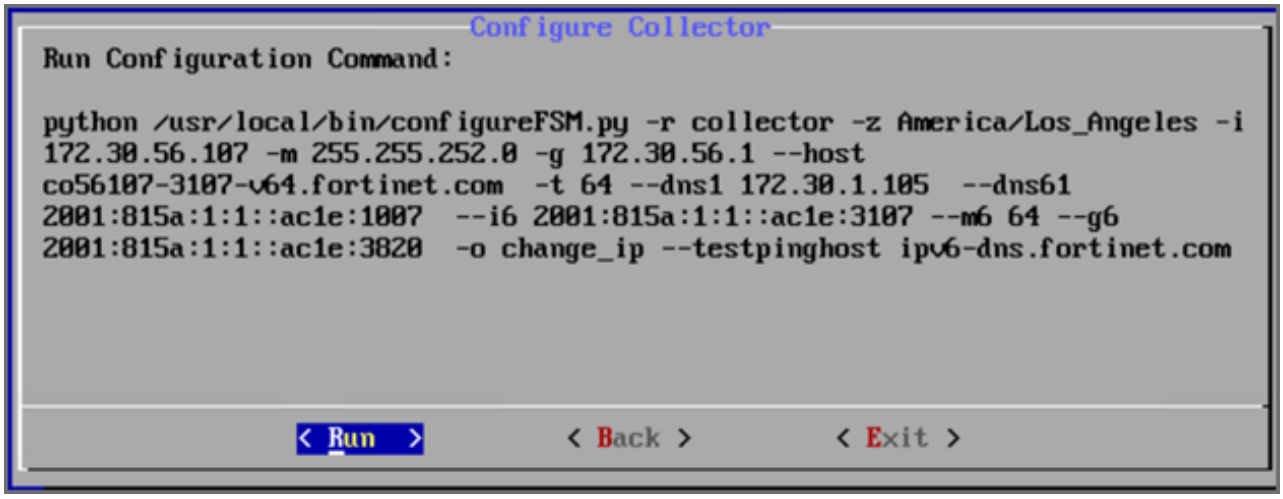
13. Configure Hostname for Collector. Press **Next**.



Note: FQDN is no longer needed.

14. 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 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**.
Note: By default, “google.com” is shown for the connectivity test, but if configuring IPv6, you must enter an accessible internally approved IPv6 DNS server, for example: “ipv6-dns.fortinet.com"
Note: When configuring both IPv4 and IPv6, only testing connectivity for the IPv6 DNS is required because the IPV6 takes higher precedence. So update the host field with an approved IPv6 DNS server.

15. 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**) or **64** (for both ipv4 and ipv6).
--dns1, --dns2	Addresses of the DNS servers

Option	Description
--i6	IPv6-formatted address
--m6	IPv6 prefix
--g6	IPv6 gateway
-o	Installation option.
-z	Time zone. 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

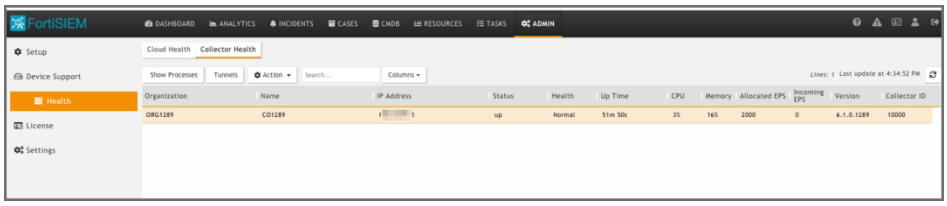
Enterprise Deployments

For enterprise deployments, follow these steps:

1. Log in to Supervisor with **Admin** privileges.
2. Go to **ADMIN > Settings > System > Cluster Config**.
   a. Enter the IP of the Worker node in the **Event Upload Workers** column. 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 **Save**.
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.

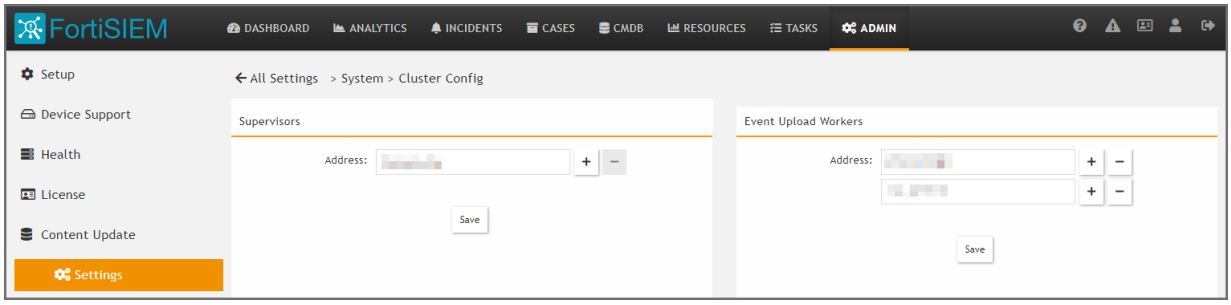
The Collector will reboot during the Registration.

5. Go to **ADMIN > Health > Collector Health** to see the Collector status.

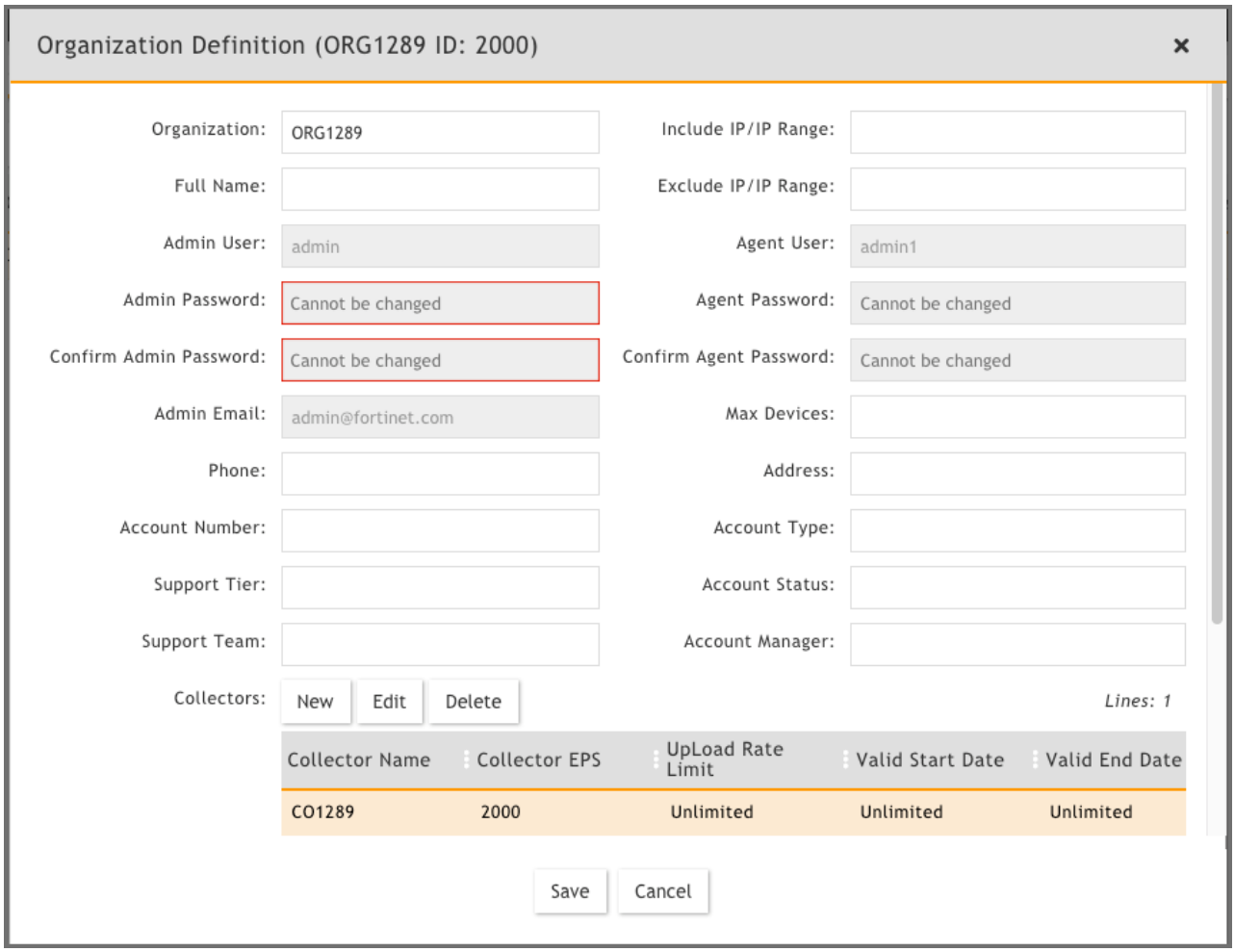


Service Provider Deployments

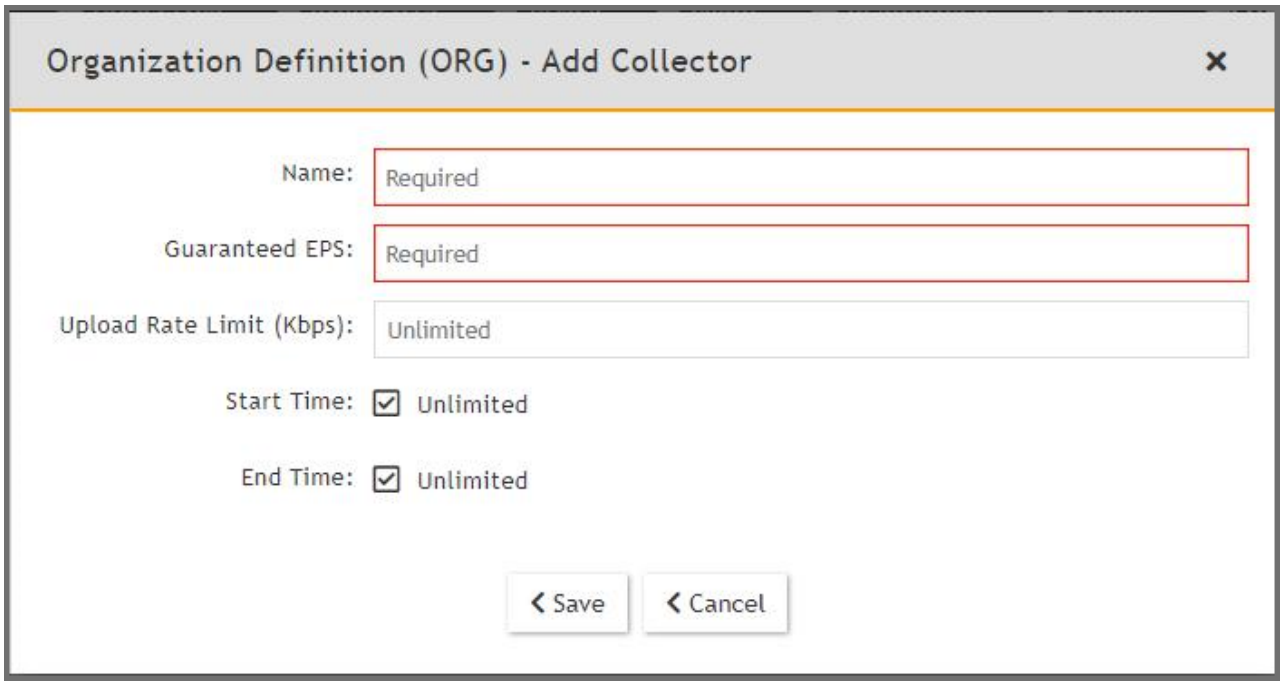
For Service Provider deployments, follow these steps.

1. Log in to Supervisor with **Admin** privileges.
2. Go to **ADMIN > Settings > System > Cluster Config**.
   a. Enter the IP of the Worker node in the **Event Upload Workers** column. 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 **Save**.
   c. 

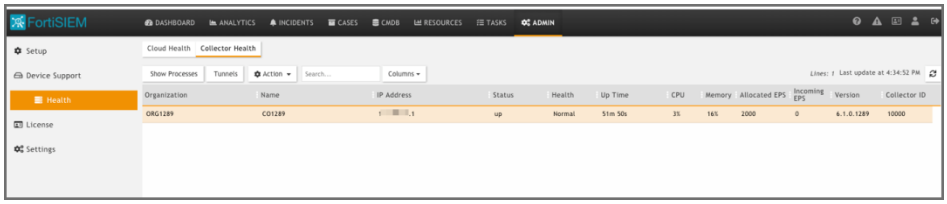
3. Go to **ADMIN > Setup > Organizations** and click **New** to add an Organization.



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:
```
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 Super.
   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.



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: Staging the FortiSIEM Collector Image

Staging can be done in one of two ways. The first is through USB. The second is through an NFS server. Follow Step 2A for staging via USB. Follow Step 2B for staging via an NFS server.

Step 2A: USB Staging

1. Connect an 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_6.7.0.1716.zip`
5. Safely remove the USB drive from the desktop or laptop by unmounting it through the operating system.

Step 2B: NFS Staging

1. Prepare an NFS server. Information on setup can be found here.
2. Download `FSM_Full_All_RAW_HARDWARE_6.7.0.1716.zip` from the support site.
3. Create and export `/FortiSIEM_HW_IMG`.
4. Upload the `FSM_Full_All_RAW_HARDWARE_6.7.0.1716.zip` to `/FortiSIEM_HW_IMG`.
5. Go to the `/FortiSIEM_HW_IMG` directory by running the following command.
   ```
   cd /FortiSIEM_HW_IMG
   ```
6. run the following command to unzip the zip file.

```
unzip -c FSM_Full_All_RAW_HARDWARE_6.7.0.1716.zip
```

7. Verify that the NFS server is reachable by the 500F appliance and is allowed to mount the sharepoint on the NFS server.

   Example: `mount -t nfs 10.0.0.1:/FortiSIEM_HW_IMG /mnt`

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 the 500F

If you followed Step 2A USB Staging, continue with Step 5A here. If you followed Step 2B NFS Staging, follow Step 5B here.

Step 5A: Reimaging from USB Staging

1. Power on the 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 to 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_6.7.0.1716.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).

Step 5B: Reimaging from NFS Server Staging

1. Power on the FortiSIEM appliance.
2. Once the FortiSIEM appliance loads from the USB drive, click **Try Unbuntu**.
3. Open a terminal.
4. Type the following command to identify the FortiSIEM boot disk (29.5GB):

   ```
   sudo fdisk -l
   ```

   Note: This drive will be referred to as `/dev/sdb` in the following steps.
5. Enter into root while in the terminal by using the following command:

   ```
   sudo -s
   ```

6. Mount the NFS share to the ubuntu boot environment.

   Note: Assuming the REMOTE site is 10.0.0.1, and remote share is: `/FortiSIEM_HW_IMG`, you would run:

   ```
   # mount -t nfs 10.0.0.1:/FortiSIEM_HW_IMG /mnt
   ```

7. Directly write the image from the NFS share to the local HDD. For example, use the command:

   ```
   # dd if=/mnt/FSM_Full_All_RAW_HARDWARE_6.7.0.1716.img of=/dev/sdb bs=1M
   status=progress
   ```

8. Once this is completed, power off the FortiSIEM appliance using the following commands:

   ```
   # shutdown -h now
   ```

9. After shutdown, remove both USB drives from the FortiSIEM appliance.
10. Power on the FortiSIEM appliance.
11. Reinstall the FortiSIEM application (as in Factory Reset - step 2).

www.fortinet.com