FortiSIEM 500F Collector Configuration Guide

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

10/13/2020
FortiSIEM 5.4.0 500F Collector Configuration Guide

TABLE OF CONTENTS

Appliance Setup

Follow the steps below to setup FSM-500F appliance.

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 '*admin*' user without password.
3. Run `get` to check the available FortiSIEM commands.
4. 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 Network

1. On the hardware console, select **Set Timezone** and then press **Enter**.
2. Select your **Location,** and then press **Enter**.
3. Select your **Country,** and then press **Enter**.

4. Select your **Timezone,** and then press **Enter**.
5. Review your Timezone information, select **1**, and then press **Enter**.
6. When the **Configuration** screen reloads, select **Login**, and then press **Enter**.
7. Enter the default login credentials:

Login	root
Password	ProspectHills

8. Run the `vami_config_net` script to configure the network. `/opt/vmware/share/vami/vami_config_net`
9. When prompted, enter the information for these network components to configure the Static IP address: **IP Address**, **Netmask**, **Gateway**, **DNS Server**(s).

   Note: The authenticated proxy server is not supported in this version of FortiSIEM.
10. Press **Y** to accept the network configuration settings.
11. Enter the **Host name,** and then press **Enter**.
    Once the configuration is complete, the system reboots automatically.

Step 5: Register Collector

The process for registering a Collector node with your Supervisor node depends on whether you are setting up the Collector as part of an enterprise or multi-tenant deployment. For an enterprise deployment, you install the Collector within your IT infrastructure and then register it with the Supervisor. For a multi-tenant deployment, you must first create an organization and add Collectors to it before you register it with the Supervisor.

- Register the Collector with the Supervisor for Enterprise Deployments
- Create an Organization and Associate Collectors with it for Multi-Tenant Deployments

Register the Collector with the Supervisor for Enterprise Deployments

1. Log in to the Supervisor.
2. Based on the FortiSIEM GUI type (Flash/HTML5), complete the following steps:
   a. **Flash GUI**
      i. Go to **Admin** > **General Settings** > **Worker Upload** and add at least the Supervisor's IP address. This should contain a list of the Supervisor and Worker accessible IP addresses or FQDNs.
      ii. Go to **Setup Wizard** > **Event Collector** and add the Collector information from the table below.
   b. **HTML5 GUI**
      i. Go to **ADMIN** > **General Settings Worker Upload** and add at least the Supervisor's IP address. This should contain a list of the Supervisor and Worker accessible IP addresses or FQDNs.
      ii. Go to **ADMIN** > **Setup** > **Collector** and add the Collector information from the table below.

Setting	Description
Name	Name of the Collector (this will be used in step 4).
Guaranteed EPS	This is the number of Events per Second

Setting	Description
	(EPS) that this Collector will be provisioned for.
Start Time	Select **Unlimited**.
End Time	Select **Unlimited**.

3. Connect to the Collector at `https://:<IP Address of the Collector>:5480`.
4. Enter the **Name** from step 2.
5. **Userid** and **Password** are the same as the admin userid/password for the Supervisor.
6. For **Organization**, enter **Super**.
7. For **IP address**, enter the IP address of the Supervisor.
8. The Collector will reboot during the registration, and you will be able to see its status on:
   - Flash GUI: **Admin** > **Collector Health**
   - HTML5 GUI: **ADMIN** > **Health** > **Collector Health**.

Create an Organization and Associate Collectors with it for Multi-Tenant Deployments

1. Log in to the Supervisor.
2. Based on the FortiSIEM GUI type (Flash/HTML5), do the following steps:
   - Flash GUI: Go to **ADMIN > Setup** > **Organizations** and click **Add**.
   - HTML5 GUI: Go to **ADMIN**> **Setup** > **Organizations** and click **New**.
3. Enter **Organization Name/Organization**, **Admin User**, **Admin Password**, and **Admin Email**.
4. Under **Collectors**, click **New**.
5. Enter the **Collector Name**, **Guaranteed EPS**, **Start Time**, and **End Time**.
   If you select **Unlimited** for **Start Time** and **End Time**, those fields will be grayed out for text entry.
6. Click **Save**.
   The newly added organization and Collector should be listed on the **Organizations** tab.
7. In a Web browser, navigate to `https://<Collector-IP>:5480` .
8. Enter the Collector setup information.

Name	Collector Name
User ID	Organization Admin User
Password	Organization Admin Password
Cust/Org ID	Organization Name
Cloud URL	Supervisor URL

9. Click **Save.**
   The Collector will restart automatically after registration succeeds.
10. On the Supervisor interface, check that the Collector health is **Normal** under:
    - Flash GUI: **Admin** > **Collector Health**
    - HTML5 GUI: **ADMIN** > **Health** > **Collector Health**

Step 6: Using FortiSIEM

Refer to 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 from v4.10.0 to v5.0.1, refer to the section '*Upgrading Collectors*' in 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_Super-Worker_RAW_HW_VA-5.4.0.1679.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 (29.5GiB): `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_Super-Worker_RAW_HW_VA-5.4.0.1679.zip | dd of=/dev/sdb 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).