FortiSIEM 3500F Hardware 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

08/24/2020
FortiSIEM 5.3.3 3500F Hardware Configuration Guide

TABLE OF CONTENTS

FortiSIEM 3500F Hardware Configuration Guide **1**
Change Log **4**
Appliance Setup **5**
Step 1: Rack mount the FSM-3500F appliance 5
Step 2: Power On the FSM-3500F appliance 5
Step 3: Verify System Information 6
Step 4: Configure Network 6
Step 5: Generate FortiSIEM FSM-3500F License Key file from FortiCare 7
Step 6: Register FortiSIEM License 7
Step 7: Accessing FortiSIEM UI 7
Step 8: Using FortiSIEM 7
Factory Reset **8**
Step 1: Uninstall FortiSIEM application 8
Step 2: Reinstall FortiSIEM application 8
Upgrading FortiSIEM **9**
Appliance Re-image **10**
Step 1: Create Bootable Linux Image 10
Step 2: Copy FortiSIEM Appliance image to USB 10
Step 3: Prepare 3500F by removing FSM 11
Step 4: Configure 3500F BIOS to Boot into USB Drive 11
Step 5: Re-image 3500F boot drive from USB Linux 11

Change Log

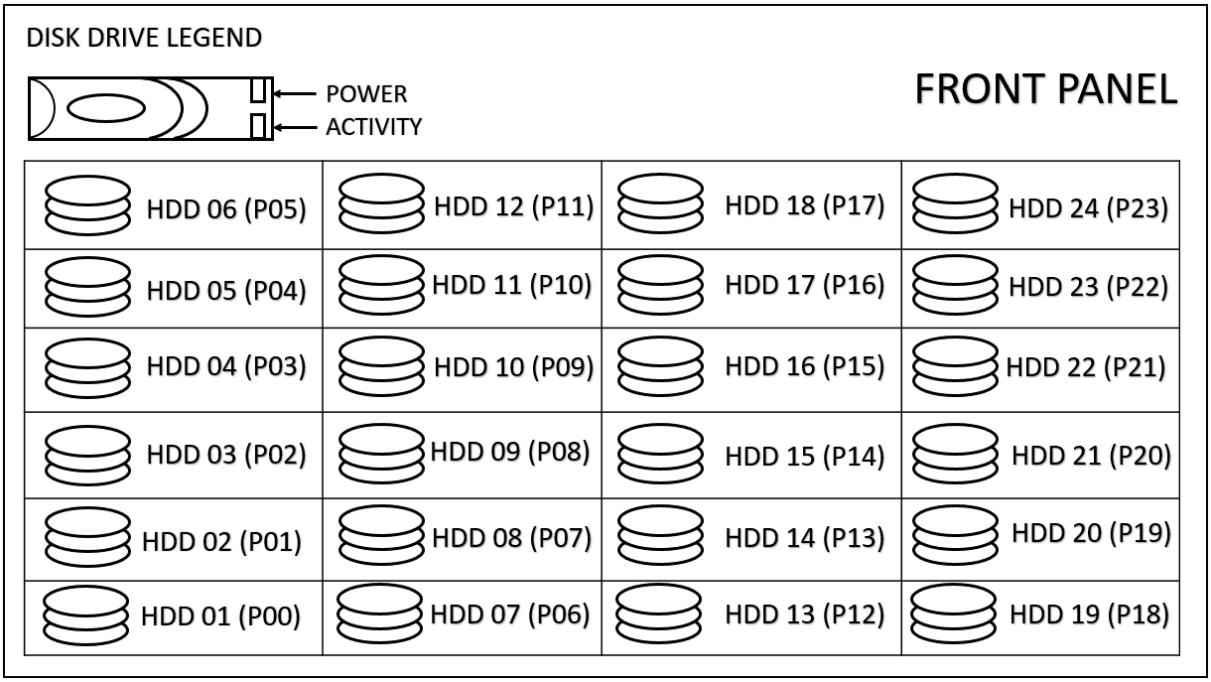
Date	Description
03/30/2018	Initial release of this guide.
06/13/2019	Revision 1: Updated instructions for "Using FortiSIEM".
09/11/2019	Revision 2: Changed the location where you obtain images to https://support.fortinet.com.
08/24/2020	Revision 3: Minor edits.

Appliance Setup

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

Step 1: Rack mount the FSM-3500F appliance

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



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 CLI (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'.
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.

5.

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: Generate FortiSIEM FSM-3500F License Key file from FortiCare

1. Obtain the Hardware Serial Number from FSM-3500F appliance.
2. Follow 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 VM in Step 4.
2. Access FortiSIEM VM 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 VM in Step 4.
2. Access FortiSIEM VM 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: Using FortiSIEM

Refer to the "Setting Event Storage" section in the User Guide for detailed information about using FortiSIEM and understanding the storage options.

Factory Reset

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

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 application.

Step 2: Reinstall FortiSIEM application

1. Power on the hardware.
2. Login as '*root*' without password 'ProspectHills'.
3. To configure RAID, run `execute format disk`.
4. To check Hardware status and RAID information, run `diagnose hardware info`.
5. To install FortiSIEM, run `execute factoryreset`.
   This script takes 5 minutes to complete FortiSIEM installation.
6. To configure network on FortiSIEM, stop FortiSIEM services by running `sudo execute preparebox`.
   This script will stop running FortiSIEM services and power offs the hardware.

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

Upgrading FortiSIEM

For upgrading FortiSIEM from v4.10.0 to v5.0.1, refer to the section 'Upgrading a FortiSIEM Single Node Deployment' in the 'Upgrade Guide' here.

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 4GB 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 Appliance image to USB

1. Connect 8GB 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-5.3.3.1677.zip`

5. Safely remove the USB drive from the desktop or laptop by unmounting it through the Operating System.

Step 3: Prepare 3500F by removing FSM

1. Connect to the console/SSH of the FortiSIEM appliance.
2. Run the following command: `execute fsm-clean`
3. After `fsm-clean` is complete, format RAID by executing the command: `execute format disk`
4. Power-off the FortiSIEM appliance.

Step 4: Configure 3500F BIOS to Boot into USB Drive

1. Connect the 4GB 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 3500F 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-5.3.3.1677.zip | dd of=/dev/sdb status=progress`
10. Once this is completed, power off the FortiSIEM appliance using the following command:
    `shutdown -h now`
11. After shutdown, remove both USB drives from the FortiSIEM appliance.
12. Power on the FortiSIEM appliance.
13. Reinstall the FortiSIEM application (as in Factory Reset - step 2).

Copyright© (Undefined variable: FortinetVariables.Copyright Year) Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.