# Reimage Procedures



# About Disaster Recovery

You may need to reset the configuration, reinstall the image, recover the FXOS password, or completely reimage the system. See the following available procedures:

- Erase the configuration and restart the system with the same image—All configurations are removed, and thethreat defense is reinstalled using the current image. Note that after performing this procedure, you will have to reconfigure the system, including admin password and connectivity information. See Reimage the System with the Base Install Software Version, on page 2.

- Perform a factory reset from ROMMON (admin password recovery)—All configurations are removed, and threat defense is reinstalled using the current image. Note that after performing this procedure, you will have to reconfigure the system, including admin password and connectivity information. See Perform a Factory Reset from ROMMON (Password Reset), on page 4.

- Reimage the system with a new version—All configurations are removed, and threat defense is reinstalled using the a new software image. Note that after performing this procedure, you will have to reconfigure the system, including admin password and connectivity information. See Reimage the System with a New Software Version, on page 6.

**Note** You cannot perform a downgrade to the previous major version using this procedure. You must use the Perform a Complete Reimage, on page 17 instead.

- Reformat the SSD File System—Reformats the SSD if you see disk corruption messages. All configurations are removed. Note that after performing this procedure, you will have to reconfigure the system, including admin password and connectivity information. See Reformat the SSD File System (Firepower 2100), on page 9.
- Boot from ROMMON—Boots FXOS from ROMMON if you cannot boot up. You can then reformat the eMMC and reinstall the software image. This procedure retains all configuration. See Boot from ROMMON, on page 10.
- Erase all configuration and images—This option restores your system to its factory default settings, and erases the images. The procedure requires you to boot the system over TFTP, download the threat defense software, and reconfigure the entire system. See Perform a Complete Reimage, on page 17.
- Change the admin password—This procedure lets you change the admin password from the threat defense CLI. See Change the Admin Password, on page 21.
- Change the admin password if threat defense is offline—This procedure lets you change the admin password from FXOS. See Change the Admin Password if Threat Defense is Offline, on page 22. Note that if the threat defense is online, you must change the admin password using the threat defense CLI.

# Reimage the System with the Base Install Software Version

This procedure erases all configuration except the base install software version setting. When the system comes back up after the erase configuration operation, it will run with the startup version of threat defense.

If your current running version is an upgrade-only image, you will have to re-upgrade your threat defense after performing this procedure. For example, version 6.2.2.x is an upgrade-only image. If you elect to perform this procedure on your 6.2.2.x system, then the base install package (version 6.2.1.x) will be reinstalled, and you will need to re-upgrade to version 6.2.2.x using the Secure Firewall Management Center or Secure Firewall device manager. In this case, the FXOS version may not revert back to a lower version. This mismatch may cause failures in a High Availability configuration. For this scenario, we recommended that you perform a complete reimage of the system (see Perform a Complete Reimage, on page 17 for more information).

**Note** After performing this procedure, the admin password is reset to **Admin123**.

### Before you begin

- Verify that you are in the FXOS CLI context. If you connect to the Firepower 1000/2100, Secure Firewall 3100, or Secure Firewall 4200 device via serial console, you will automatically connect to the FXOS CLI context. If you are in the threat defense CLI context, you must first switch to the FXOS CLI context with the **connect fxos** command.
- Take note of your appliance management IP address configuration and copy the information shown from the following command:

```
firepower # scope fabric a
firepower /fabric-interconnect # show detail
```

- Take note of your threat defense base install version using the following commands. The Startup Version column shows your base install version. The Running Version shows any upgrades you applied to the base install version.

```
firepower# scope ssa
firepower /ssa # show app-instance
Application Name     Slot ID    Admin State     Operational State    Running Version
Startup Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- ------------------
ftd                  1          Enabled         Online               6.2.2.49
6.2.1.341       Not Applicable
```

- Disassociate your devices from Smart Licensing.
- Deregister your devices from the cloud tenant (if applicable). See Deregister From Cloud, on page 23.
- To reimage your Secure Firewall 3100 device to threat defense 7.3.0 version, you must have ROMMON version 1.1.08 or above. If the current ROMMON version is less than 1.1.08, you must upgrade ROMMON by upgrading to ASA 9.19 or later. You can also use the management center or device manager to upgrade the threat defense to 7.3.0 (see Threat Defense Reimage for more information).
- You cannot reimage the Secure Firewall 3100 device to threat defense 7.4 using the base install software version due to the introduction of a single image for installation and upgrading of the threat defense image. Instead, perform a complete reimage of the system. For more information, see Perform a Complete Reimage, on page 17.

### Procedure

**Step 1** In the FXOS CLI, connect to local-mgmt:

firepower # **connect local-mgmt**

**Step 2** Erase all configuration:

firepower(local-mgmt) # **erase configuration**

**Example:**

```
firepower(local-mgmt)# erase configuration
All configurations will be erased and system will reboot. Are you sure? (yes/no):yes
Removing all the configuration. Please wait....
Configurations are cleaned up. Rebooting....
```

**Step 3** Once the system comes back up, you can check the state of the application with the **show app-instance** command. Note that the password login is now set to the default **admin/Admin123**.

**Example:**

```
firepower# scope ssa

firepower /ssa # show app-instance
Application Name     Slot ID    Admin State     Operational State    Running Version Startup
 Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- ------------------
```

```
ftd                  1          Disabled        Installing
6.2.1-1314     Not Applicable
```

**Note** It may take more than 10 minutes for the application installation to complete. Once the threat defense is back online, the Operational State of the **show app-instance** command displays as Online:

**Example:**

```
firepower /ssa # show app-instance
Application Name     Slot ID    Admin State     Operational State    Running Version Startup
 Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- ------------------
ftd                  1          Enabled         Online               6.2.1.10140
```

### What to do next

Complete the setup tasks in the getting started guide, and upgrade to latest version if necessary.

# Perform a Factory Reset from ROMMON (Password Reset)

If you cannot log into FXOS (either because you forgot the password, or the SSD disk1 file system was corrupted), you can restore the FXOS and threat defense configuration to the factory default using ROMMON. The admin password is reset to the default **Admin123**. If you know the password, and want to restore the factory default configuration from within FXOS, see Reimage the System with the Base Install Software Version, on page 2.

### Before you begin

- To reimage your Secure Firewall 3100 device to threat defense 7.3.0 version, you must have ROMMON version 1.1.08 or above. If the current ROMMON version is less than 1.1.08, you must upgrade ROMMON by upgrading to ASA 9.19 or later. You can also use the management center or device manager to upgrade threat defense version to 7.3.0 (see Threat Defense Reimage for more information).

### Procedure

**Step 1** Power on the device. When you see the following prompt, hit ESC to stop the boot.

```
Example:
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

**Step 2** Verify the ROMMON version:

rommon 1 > **show info**

**Example:**

Firepower 1000 and 2100 devices

```
rommon 1 > show info
```

```
Cisco System ROMMON, Version 1.0.06, RELEASE SOFTWARE
Copyright (c) 1994-2017  by Cisco Systems, Inc.
Compiled Wed 11/01/2017 18:38:59.66 by builder
```

Secure Firewall 3100 devices

```
rommon 1 > show info
Cisco System ROMMON, Version 1.1.08 , RELEASE SOFTWARE
Copyright (c) 1994-2022  by Cisco Systems, Inc.
Compiled Fri 06/10/2022 10:25:43.78 by Administrator
```

Secure Firewall 4200 devices

```
Cisco System ROMMON, Version 1.0.15, RELEASE SOFTWARE
Copyright (c) 1994-2023  by Cisco Systems, Inc.
Compiled Thu 06/15/2023 14:41:54.43 by builder
```

**Step 3** Factory reset the device.

For ROMMON version 1.0.06 or later:

rommon 2 > **factory-reset**

For ROMMON version 1.0.04:

rommon 2 > **password_reset**

**Example:**

Firepower 1000 and 2100 devices

```
rommon 2 > factory-reset
Warning: All configuration will be permanently lost with this operation
         and application will be initialized to default configuration.
         This operation cannot be undone after booting the application image.

         Are you sure you would like to continue ? yes/no [no]: yes
         Please type 'ERASE' to confirm the operation or any other value to cancel: ERASE

Performing factory reset...
File size is 0x0000001b
Located .boot_string
Image size 27 inode num 16, bks cnt 1 blk size 8*512

Rommon will continue to boot disk0: fxos-k8-fp2k-lfbff.2.3.1.132.SSB
Are you sure you would like to continue ? yes/no [no]: yes
File size is 0x0817a870
Located fxos-k8-fp2k-lfbff.2.3.1.132.SSB
```

**Example:**

Secure Firewall 3100 devices

```
rommon 2 > factory-reset
Warning: All configuration will be permanently lost with this operation
         and application will be initialized to default configuration.
         This operation cannot be undone after booting the application image.

         Are you sure you would like to continue ? yes/no [no]: yes
         Please type 'ERASE' to confirm the operation or any other value to cancel: ERASE

Performing factory reset...
File size is 0x0000001b
Located .boot_string
Image size 27 inode num 16, bks cnt 1 blk size 8*512

Rommon will continue to boot disk0: Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-4.sh.REL.tar
Are you sure you would like to continue ? yes/no [no]: yes
```

```
File size is 0x0817a870
Located Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-4.sh.REL.tar
```

**Example:**

Secure Firewall 4200 devices

```
rommon 2 > factory-reset
Warning: All configuration will be permanently lost with this operation
         and application will be initialized to default configuration.
         This operation cannot be undone after booting the application image.

         Are you sure you would like to continue ? yes/no [no]: yes
         Please type 'ERASE' to confirm the operation or any other value to cancel: ERASE

Performing factory reset...
File size is 0x0000001b
Located .boot_string
Image size 27 inode num 16, bks cnt 1 blk size 8*512

Rommon will continue to boot disk0: Cisco_Secure_FW_TD_4200-7.4.0-1044.sh.DEV.tar
Are you sure you would like to continue ? yes/no [no]: yes
File size is 0x0817a870
Located Cisco_Secure_FW_TD_4200-7.4.0-1044.sh.DEV.tar
```

**Step 4** If the system does not prompt you to boot, enter the **boot** command:

rommon 3 > **boot**

---

### What to do next

Complete the setup tasks in the getting started guide.

# Reimage the System with a New Software Version

This procedure allows you to reimage the system with a new software version. After performing this procedure, you will need to reconfigure the management IP address and other configuration parameters on the device. If you want to upgrade the software without erasing your configuration, see the upgrade guide.

**Note** You cannot perform a downgrade to the previous major version using this procedure. You must use the Perform a Complete Reimage, on page 17 instead.

**Note** After performing this procedure, the admin password is reset to **Admin123**.

### Before you begin

- Verify that you are in the FXOS CLI context. If you connect to the Firepower 1000/2100, Secure Firewall 3100, or or Secure Firewall 4200 device via serial console, you will automatically connect to the FXOS CLI context. If you are in the threat defense CLI context, you must first switch to the FXOS CLI context with the **connect fxos** command.

- Take note of your appliance management IP address configuration, and copy the information shown from the following command:

```
firepower # scope fabric a
firepower /fabric-interconnect # show detail
```

- Disassociate your devices from Smart Licensing.
- Deregister your devices from the cloud tenant (if applicable). See Deregister From Cloud, on page 23.
- To reimage your Secure Firewall 3100 device to threat defense version 7.3.0, you must have ROMMON version 1.1.08 or above. If the current ROMMON version is less than 1.1.08, you must upgrade ROMMON by upgrading to ASA 9.19 or later. You can also use the management center or device manager to upgrade threat defense version to 7.3.0 (see Threat Defense Reimage for more information).

### Procedure

**Step 1** Download the software bundle to your local computer, or to a USB flash drive.

**Step 2** If using a USB drive, insert the USB drive into the USB port on the appliance.

**Step 3** In FXOS, enter the system scope and verify the current version running on your system:

firepower # **scope system**

firepower /system # **show version detail**

**Step 4** Enter the firmware scope:

firepower # **scope firmware**

**Step 5** Download the new software package. If you are using a USB drive to download the software package, use the following syntax:

firepower # **scope firmware**

firepower /firmware # **download image** usbA:*image_name*

Note that the *image_name* is the output from the **show version detail** command in step 3, above.

For example:

firepower /firmware # **download image** usbA:cisco-ftd-fp2k.6.2.1-36.SPA

**Note** In version 7.3+, the threat defense install and upgrade package for Secure Firewall 3100 is a combined package. You can use the `.REL.tar` file instead of `.SPA` file for the described procedure.

You can also use FTP, SCP, SFTP, or TFTP to copy the threat defense software package to the device:

firepower /firmware # **download image** *tftp/ftp/scp/sftp***:***//path to the image, including the server root /image name*

Example for Firepower 1000 and 2100 devices:

```
firepower /firmware # download image tftp://example.cisco.com/fxos-2k.6.2.1-1314.SPA
```

Example for Secure Firewall 3100 devices:

```
firepower /firmware # download image scp://example.cisco.com/auto/Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-14.sh.REL.tar
```

Example for Secure Firewall 4200 devices:

```
firepower-4215 /firmware # download image tftp://172.29.185.101:/Cisco_Secure_FW_TD_4200-7.4.0-1044.sh.REL.tar
```

**Note** When performing a file transfer via FTP/TFTP/SCP/SFTP, you must provide an absolute path to the image, including the server root, as the system prepends a forward slash to the filename provided in the download image request.

You can optionally use a FQDN in place of the IP address.

**Step 6** Display the download task to monitor the download progress:

firepower /firmware #**show download-task**

Once Downloaded displays in the output of the Status column, the download is complete.

**Example:**

Secure Firewall 3100 devices:

```
firepower 3110 /firmware # show download task
File Name Protocol Server Port Userid State
--------- -------- ------ ---- ------------
Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-14.sh.REL.tar
          Scp 172.23.205.217 0 <xxxxxx> Downloaded
```

**Example:**

Secure Firewall 4200 devices:

```
firepower-4215 /firmware # show download-task

Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    Cisco_Secure_FW_TD_4200-7.4.0-1044.sh.REL.tar
              Tftp     172.29.185.101           0                 Downloading
```

**Step 7** Once the download is complete, display the software packages installed on your system and copy the displayed bundle image version from the output:

firepower /firmware # **show package**

**Example:**

Firepower 1000 and 2100 devices

```
firepower /firmware # show package
Name                                          Package-Vers
--------------------------------------------- ------------
cisco-ftd-fp2k.6.2.1-1314.SPA                 6.2.1-1314
```

In the above example, **6.2.1-1314** is the security pack version.

**Example:**

Secure Firewall 3100 devices

```
firepower 3110 /firmware # show package
Name                                             Package Vers
```

```
-------------------------------------------  ---------------
Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-14.sh.REL.tar      7.3.0-14
```

**Example:**

Secure Firewall 4200 devices

```
firepower-4215 /firmware # show package
Name                                          Package-Vers
--------------------------------------------- ------------
Cisco_Secure_FW_TD_4200-7.4.0-1044.sh.REL.tar 7.4.0-1044
```

In the above example, **7.3.0-14** is the security pack version.

**Step 8** Enter the auto-install scope:

firepower /firmware # **scope auto-install**

**Step 9** Install the new application software package (where the *version* is the output from show package, above):

firepower /firmware/auto-install # **install security-pack version** *version*

**Example:**

```
firepower 3110 /firmware/auto install # install security pack version 7.3.0-14
…
firepower /firmware # connect ftd
> show version
-----------------[ firepower 3100 ]-----------------
Model : Cisco Secure Firewall 3110 Threat Defense (80) Version 7.3.0 (Build
```

**Step 10** Enter **yes** when prompted.

The system reboots, then installs the latest software bundle.

### What to do next

Complete the setup tasks in the getting started guide.

# Reformat the SSD File System (Firepower 2100)

If you successfully logged into FXOS, but you see disk corruption error messages, you can reformat SSD1 where the FXOS and threat defense configuration is stored. This procedure restores the FXOS configuration to the factory default. The admin password is reset to the default **Admin123**. This procedure also resets the threat defense configuration.

This procedure does not apply to the Firepower 1000 and Secure Firewall 3100, which do not allow you to erase the SSD while still retaining the startup image.

### Procedure

**Step 1** Connect to the FXOS CLI from the console port.

**Step 2** Reformat SSD1.

**connect local-mgmt**

**format ssd1**

**Step 3** Complete the setup tasks in the getting started guide.

# Boot from ROMMON

If you cannot boot the device, it will boot into ROMMON where you can boot FXOS from a USB or TFTP image. After booting into FXOS, you can then reformat the eMMC (the internal flash device that holds the software images). After you reformat, then you need to re-download the images to the eMMC. This procedure retains all configuration, which is stored on the separate ssd1.

The eMMC file system might get corrupted because of a power failure or other rare condition.

### Before you begin

- You must have console access for this procedure.
- To reimage your Secure Firewall 3100 device to threat defense version 7.3.0, you must have ROMMON version 1.1.08 or above. If the current ROMMON version is less than 1.1.08, you must upgrade ROMMON by upgrading to ASA 9.19 or later. You can also use the management center or device manager to upgrade threat defense version to 7.3.0 (see Threat Defense Reimage for more information).

### Procedure

**Step 1** If you cannot boot up, the system will boot into ROMMON. If it does not automatically boot into ROMMON, press **Esc** during the bootup when prompted to reach the ROMMON prompt. Pay close attention to the monitor.

**Example:**

```
*******************************************************************************
Cisco System ROMMON, Version 1.0.06, RELEASE SOFTWARE
Copyright (c) 1994-2018  by Cisco Systems, Inc.
Compiled Thu 04/06/2018 12:16:16.21 by builder
*******************************************************************************

Current image running: Boot ROM0
Last reset cause: ResetRequest
DIMM_1/1 : Present
DIMM_2/1 : Present

Platform FPR-2130 with 32768 MBytes of main memory
BIOS has been successfully locked !!
MAC Address: 0c:75:bd:08:c9:80

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

Press **Esc** at this point.

**Step 2** Boot from an image on a USB drive, or boot over the network using TFTP.

**Note** For 6.4 and earlier, if you boot FXOS from ROMMON, and the currently-installed image is also bootable, make sure you boot the same version as the currently-installed image. Otherwise, an FXOS/threat defense version mismatch will cause the threat defense to crash. In 6.5 and later, booting FXOS from ROMMON prevents threat defense from loading automatically.

**Note** You can also boot the kickstart from ROMMON using a FAT32 formatted USB media device inserted into the USB slot on the front panel of the Firepower 1000/2100 or Secure Firewall 3100/4200 device. If the USB device is inserted while the system is running, you will need to reboot the system before it will recognize the USB device.

**If you want to boot from Firepower 1000/2100 USB:**

**boot disk1:**/*path*/*filename*

The device boots up to the FXOS CLI. Use the **dir disk1:** command to view the disk contents.

**Example:**

```
rommon 1 > dir disk1:
rommon 2 > boot disk1:/cisco-ftd-fp2k.6.4.0.SPA
```

**If you want to boot from Secure Firewall 3100/4200 USB:**

**boot usb:**/*path*/*filename*

The device boots up to the FXOS CLI. Use the **dir usb:** command to view the disk contents.

**Example:**

```
rommon 1 > dir usb:
rommon 2 > boot usb:/cisco-ftd-fp3k.7.1.0.SPA
```

**If you want to boot from TFTP:**

Set the network settings for Management 1/1, and load the threat defense package using the following ROMMON commands.

**address** *management_ip_address*

**netmask** *subnet_mask*

**server** *tftp_ip_address*

**gateway** *gateway_ip_address*

**file***path*/*filename*

**set**

**sync**

**tftp -b**

The FXOS image downloads and boots up to the CLI.

See the following information:

- **set**—Shows the network settings. You can also use the **ping** command to verify connectivity to the server.
- **sync**—Saves the network settings.
- **tftp -b**—Loads FXOS.

**Example:**

Firepower 1000 and 2100 devices

```
rommon 1 > address 10.86.118.4
rommon 2 > netmask 255.255.252.0
rommon 3 > server 10.86.118.21
rommon 4 > gateway 10.86.118.1
rommon 5 > file cisco-ftd-fp2k.6.4.0.SPA
rommon 6 > set
ROMMON Variable Settings:
  ADDRESS=10.86.118.4
  NETMASK=255.255.252.0
  GATEWAY=10.86.118.21
  SERVER=10.86.118.21
  IMAGE=cisco-ftd-fp2k.6.4.0.SPA
  CONFIG=
  PS1="rommon ! > "

rommon 7 > sync
rommon 8 > tftp -b
Enable boot bundle: tftp_reqsize = 268435456

             ADDRESS: 10.86.118.4
             NETMASK: 255.255.252.0
             GATEWAY: 10.86.118.21
              SERVER: 10.86.118.1
               IMAGE: cisco-ftd-fp2k.6.4.0.SPA
             MACADDR: d4:2c:44:0c:26:00
           VERBOSITY: Progress
               RETRY: 40
          PKTTIMEOUT: 7200
             BLKSIZE: 1460
            CHECKSUM: Yes
                PORT: GbE/1
             PHYMODE: Auto Detect

link up
Receiving cisco-ftd-fp2k.6.4.0.SPA from 10.86.118.21!!!!!!!!
[…]
```

**Ping to troubleshoot connectivity to the server:**

```
rommon 1 > ping 10.86.118.21
Sending 10, 32-byte ICMP Echoes to 10.86.118.21 timeout is 4 seconds
!!!!!!!!!!
Success rate is 100 percent (10/10)
rommon 2 >
```

**Example:**

Secure Firewall 3100 devices

```
rommon 1 > show info

Cisco System ROMMON, Version 1.1.08, RELEASE SOFTWARE
Copyright (c) 1994-2022  by Cisco Systems, Inc.
Compiled Fri 06/10/2022 10:25:43.78 by Administrator
*******************************************************************************

rommon 2 > ADDRESS=172.16.0.50
rommon 3 > NETMASK=255.255.255.0
```

```
rommon 4 > GATEWAY=172.16.0.254
rommon 5 > SERVER=172.23.37.186
rommon 6 > IMAGE=image_dir/Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-4.sh.REL.tar
rommon 7 > set
    ADDRESS=172.16.0.50
    NETMASK=255.255.255.0
    GATEWAY=172.16.0.254
    SPEED=10000
    SERVER=172.23.37.186
    IMAGE= image_dir/Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-4.sh.REL.tar
    CONFIG=
    PS1="rommon ! > "
    FIRMWARE_VERSION=1.3.5

rommon 8 > sync
rommon 9 > tftp -b
Enable boot bundle: tftp_reqsize = 402653184

             ADDRESS: 172.16.0.50
             NETMASK: 255.255.255.0
             GATEWAY: 172.16.0.254
              SERVER: 172.23.37.186
               IMAGE: image_dir/Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-4.sh.REL.tar
           VERBOSITY: Progress
               RETRY: 40
          PKTTIMEOUT: 7200
             BLKSIZE: 1460
            CHECKSUM: Yes
                PORT: 10G/1
             PHYMODE: Auto Detect
.=====…
+-------------------------------------------------------------------+
+------------------------- SUCCESS ---------------------------------+
+-------------------------------------------------------------------+
|                                                                   |
|             LFBFF signature authentication passed !!!             |
|                                                                   |
+-------------------------------------------------------------------+
LFBFF signature verified.
```

**Step 3** Log in to FXOS using your current admin password.

**Note** If you do not know your credentials, or cannot log in due to disk corruption, you should perform a factory reset using the ROMMON **factory-reset** command (see Perform a Factory Reset from ROMMON (Password Reset), on page 4). After performing the factory reset, restart this procedure to boot into FXOS, and log in with the default credentials (**admin**/**Admin123**).

**Step 4** Reformat the eMMC.

**connect local-mgmt**

**format emmc**

Enter **yes**.

**Example:**

```
firepower-2110# connect local-mgmt
firepower-2110(local-mgmt)# format emmc
All bootable images will be lost.
Do you still want to format? (yes/no):yes
```

```
firepower-3110# connect local-mgmt
firepower-3110(local-mgmt)# format emmc
All bootable images will be lost.
Do you still want to format? (yes/no):yes
```

**Step 5** Re-download and boot the threat defense package.

**Note** If you previously performed a factory reset because you could not log in, then your configuration was restored to the factory default configuration. This reset means that your network settings were changed to the default. To restore your network settings, perform initial setup according to the getting started guide. After you re-establish network connectivity, continue with this procedure.

a) Download the package. Because you booted temporarily from USB/usb or TFTP, you must still download the image to the local disk.

**scope firmware**

**download image** *url*

**show download-task**

Specify the URL for the file being imported using one of the following:

- **ftp:**//*username@server*/[*path*/]*image_name*
- **scp:**//*username@server*/[*path*/]*image_name*
- **sftp:**//*username@server*/[*path*/]*image_name*
- **tftp:**//*server*[**:***port*]/[*path*/]*image_name*
- **usbA:**/*path*/*filename*

**Example:**

Firepower 1000 and 2100 devices

```
firepower-2110# scope firmware
firepower-2110 /firmware # download image tftp://10.86.118.21/cisco-asa-fp2k.9.8.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
firepower-2110 /firmware # show download-task
Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.8.2.SPA
              Tftp     10.88.29.21             0                 Downloaded
```

**Example:**

Secure Firewall 3100 devices

```
firepower-3110# scope firmware
firepower-3110 /firmware # download image
scp://172.23.205.217/auto/Cisco_FTD_SSP_FP3K_Upgrade 7.3.0-14.sh.REL.tar
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
firepower-3110 /firmware # show download-task
Download task:
```

```
File Name     Protocol     Server            Port     Userid     State
---------     --------     ---------------   ----     ------     -----
Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-14.sh.REL.tar 7.3.0-14.sh.REL.tar
              Scp          172.23.205.217     0                  Downloaded
```

b) When the package finishes downloading (**Downloaded** state), boot the package.

**show package**

**scope auto-install**

**install security-pack version** *version*

In the **show package** output, copy the **Package-Vers** value for the **security-pack version** number. The chassis installs the ASA image and reboots.

**Example:**

Firepower 1000 and 2100 devices

```
firepower 2110 /firmware # show package
Name                                          Package-Vers
--------------------------------------------- ------------
cisco-asa-fp2k.9.8.2.SPA                      9.8.2
firepower 2110 /firmware # scope auto-install
firepower 2110 /firmware/auto-install # install security-pack version 9.8.2
The system is currently installed with security software package not set, which has:
   - The platform version: not set
If you proceed with the upgrade 9.8.2, it will do the following:
   - upgrade to the new platform version 2.2.2.52
   - install with CSP asa version 9.8.2
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Attention:
   If you proceed the system will be re-imaged. All existing configuration will be lost,

   and the default configuration applied.
Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.8.2
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
```

**Example:**

Secure Firewall 3100 devices

```
firepower 3110 /firmware # show package
Name                                           Package-Vers
---------------------------------------------- -------------
Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-14.sh.REL.tar 7.3.0-14
firepower 3110 /firmware # scope auto-install
firepower 3110 /firmware/auto-install # install security-pack version 9.19.0
The system is currently installed with security software package not set, which has:
   - The platform version: not set
If you proceed with the upgrade 9.19.2, it will do the following:
```

```
   - upgrade to the new platform version 7.0.3-14
   - install with CSP asa version 9.19.2
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Attention:
   If you proceed the system will be re-imaged. All existing configuration will be lost,

   and the default configuration applied.
Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.19.0
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
```

**Step 6** Wait for the chassis to finish rebooting (5-10 minutes).

Although FXOS is up, you still need to wait for the ASA to come up (5 minutes). Wait until you see the following messages:

Firepower 1000 and 2100 devices

```
firepower-2110#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.8.2.2 ...
Verifying signature for cisco-asa.9.8.2.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
...
```

Secure Firewall 3100 devices

```
firepower-3110#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.19.0.0__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.19.0.0 ...
Verifying signature for cisco-asa.9.19.0.0 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.19.0.0__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
...
```

# Perform a Complete Reimage

This procedure reformats the entire system, erases the images, and returns it to its factory default settings. After performing this procedure, you must download the new software images and reconfigure your system.

**Note** After performing this procedure, the admin password is reset to **Admin123**.

**Note** Downgrade of FXOS images is not supported. The only Cisco-supported method of downgrading an image version of FXOS is to perform a complete re-image of the device. Following are the implications of re-imaging your device:

- The configuration of your existing device is lost.
- You must configure all ASA license entitlements in your new version.
- Backup restore is not supported.

### Before you begin

- Deregister your devices from the cloud tenant (if applicable). See Deregister From Cloud, on page 23.
- Verify that you are in the FXOS CLI context. If you connect to the Firepower 1000/2100 or Secure Firewall 3100/4200 device via serial console, you will automatically connect to the FXOS CLI context. If you are in the threat defense CLI context, you must first switch to the FXOS CLI context with the **connect fxos** command.
- To reimage your Secure Firewall 3100 device to threat defense version 7.3.0, you must have ROMMON version 1.1.08 or above. If the current ROMMON version is less than 1.1.08, you must upgrade ROMMON by upgrading to ASA 9.19 or later. You can also use the management center or device manager to upgrade the threat defense version to 7.3.0 (see Threat Defense for more information).
- Obtain the threat defense software.

**Note** A Cisco.com login and Cisco service contract are required.

***Table 1: Threat Defense Software***

| Threat Defense Model | Download Location | Packages |
|---|---|---|
| Firepower 1000 series | See: https://www.cisco.com/go/ftd-software | |
| | **Threat Defense package**<br>Choose your *model* > **Firepower Threat Defense Software** > *version*. | The package has a filename like cisco-ftd-fp1k.6.4.0.**SPA**. |

| Threat Defense Model | Download Location | Packages |
|---|---|---|
| Firepower 2100 series | See: https://www.cisco.com/go/ftd-software | |
| | **Threat Defense package**<br>Choose your *model* > **Firepower Threat Defense Software** > *version*. | The package has a filename like cisco-ftd-fp2k.6.2.2.**SPA**. |
| Secure Firewall 3100 series | See: https://www.cisco.com/go/ftd-software | |
| | **Threat Defense package**<br>Choose your *model* > **Firepower Threat Defense Software** > *version*. | • 7.3 and later—The package has a filename like Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-01.sh.REL.**tar**<br>• 7.2—The package has a filename like cisco-ftd-fp3k.7.1.0.**SPA**. |
| Secure Firewall 4200 series | See: https://www.cisco.com/go/ftd-software | |
| | **Threat Defense package**<br>Choose your *model* > **Firepower Threat Defense Software** > *version*. | The package has a filename like Cisco_Secure_FW_TD_4200-7.4.0-01.sh.REL.**tar** |

### Procedure

**Step 1** In the FXOS CLI, connect to local-mgmt:

firepower # **connect local-mgmt admin**

**Step 2** Format the system:

firepower(local-mgmt) # **format everything**

**Example:**

```
firepower(local-mgmt)# format
  emmc        eMMC Flash Device
  everything  Format All storage devices
  ssd1        Primary SSD Disk
  ssd2        Secondary SSD Disk


firepower(local-mgmt)# format everything
All configuration and bootable images will be lost.
Do you still want to format? (yes/no):yes
```

**Step 3** When you see the following prompt, hit ESC to stop the boot.

**Example:**

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

**Step 4** The system reboots and stops at the ROMMON prompt.

**Note** The device will first try to ARP for the gateway IP. If you connect the device directly to your TFTP server, you must set the gateway IP and the server IP to the same IP.

Enter the parameters as follows:

rommon 2 >**ADDRESS=***address*

rommon 3 > **NETMASK=***netmask*

rommon 4 > **GATEWAY=***gateway*

rommon 5 > **SERVER=***server*

rommon 6 > **IMAGE=***image*

**Note** To boot threat defense or ASA bundle, use the tftp -b command.

**Step 5** Set the configuration:

rommon 7 > **set**

**Step 6** Sync the new configuration:

rommon 8 > **sync**

**Step 7** Test ICMP connectivity from the ROMMON to the TFTP server IP.

rommon 9 > **ping** *server IP*

**Note** Ping from the TFTP server IP to the management IP will fail. This is expected behavior.

**Step 8** Boot the threat defense software image:

**tftp -b**

**Note** The following error may display once the system boots back up:

```
firepower-2110 : <<%%FPRM-2-DEFAULT_INFRA_VERSION_MISSING>>
[F1309][critical][default-infra-version-missing][org-root/fw-infra-pack-default]
Bundle version in firmware package is empty, need to re-install
```

```
firepower-3105 FPRM: <<%FPRM-2-DEFAULT_INFRA_VERSION_MISSING>>
[F1309][critical][default-infra-version-missing][org-root/fw-infra-pack-default]

Bundle version in firmware package is empty, need to re-install
```

This error condition clears as soon as you install the new threat defense software package version as described later in this procedure.

**Step 9** Once the system comes up, log in as admin/Admin123 and reconfigure the management IP address:

a) Enter the fabric-interconnect scope:

firepower#/ **scope fabric-interconnect a**

b) Set the new management IP information:

firepower /fabric-interconnect # **set out-of-band static ip** *ip* **netmask** *netmask* **gw** *gateway*

c) Commit the configuration:

**commit-buffer**

**Note** If you encounter the following error, you must disable DHCP before committing the change. Follow the steps below to disable DHCP.

```
firepower /fabric-interconnect* # commit-buffer
Error: Update failed: [Management ipv4 address (IP <ip> / net mask <netmask> ) is not in
the same network of current DHCP server IP range <ip - ip>. Either disable DHCP server first
 or config with a different ipv4 address.]
```

a) firepower /fabric-interconnect # **exit**
b) firepower # **scope system**
c) firepower #/system **scope services**
d) firepower #/system/services **disable dhcp-server**
e) firepower #/system/services **commit-buffer**
f) Once the DHCP server is disabled, you can go back and set the new management IP.

**Step 10** Download the new threat defense application software package. If you are using a USB drive to download the software package, use the following syntax:

firepower # **scope firmware**

firepower /firmware # **download image** usbA:*image_name*

For example:

firepower /firmware # **download image** usbA:cisco-ftd-fp2k.6.2.1-36.SPA

You can also use TFTP to copy the threat defense software package to the device:

firepower /firmware # **download image** *tftp***://***path to the image, including the server root /image name*

Example for Firepower 1000 and 2100 devices:

```
firepower /firmware # download image tftp://example.cisco.com/fxos-2k.6.2.1-36.SPA
```

Example for Secure Firewall 3100 and 4200 devices:

```
firepower /firmware # download image tftp://172.23.205.217/auto/Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-14.sh.REL.tar
```

**Note** When performing a file transfer via FTP/TFTP/SCP/SFTP, you must provide an absolute path to the image, including the server root, as the system prepends a forward slash to the filename provided in the download image request.

You can optionally use a FQDN in place of the IP address.

**Step 11** Make sure that the download progress shown automatically in the command output or by entering the **download-task** command shows the State as Downloaded:

firepower /firmware # **show download-task**

**Example:**

```
firepower-3110 /firmware # show download task
File Name     Protocol     Server         Port     Userid     State
---------     --------     ------         ----     ------     -----
Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-14.sh.REL.tar
              Scp         172.23.205.217     0                Downloaded
```

**Step 12** Display the downloaded package version:

firepower /firmware # **show package**

**Example:**

```
firepower /firmware # show package
Name                                          Package-Vers
--------------------------------------------- ------------
cisco-ftd-fp2k.6.2.1-1314.SPA                 6.2.1-1314
```

```
firepower-3110 /firmware # show package
Name                                             Package-Vers
---------------------------------------------       ---------------
Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-14.sh.REL.tar       7.3.0-14
```

**Step 13** Enter the auto-install scope:

firepower /firmware # **scope auto-install**

**Step 14** Install the new software application package (where *version* is the version output from the **show package** command):

firepower /firmware/auto-install # **install security-pack version** *version* **force**

**Step 15** After the software package is installed, continue with the setup instructions in the getting started guide for your hardware platform.

# Change the Admin Password

After reimaging your device, the admin password is reset to Admin123. You will be prompted to change the password when you first log in. If you want to change the password later, use this threat defense CLI procedure to change the admin password to a new string.

**Procedure**

**Step 1** Connect to the threat defense application CLI:

firepower-chassis # **connect ftd**

**Step 2** Verify that the admin user account is present in the **users** table:

> **show user**

**Example:**

```
> show user
Login UID Auth Access Enabled Reset Exp Warn Str Lock Max
admin 100 Local Config Enabled No Never N/A Dis No 0
```

**Step 3** Set the new password for the admin user account:

firepower-chassis # **configure user password admin**

**Example:**

```
> configure user password admin
Enter current password:
```

```
Enter new password for user admin:
Confirm new password for user admin:
```

# Change the Admin Password if Threat Defense is Offline

After reimaging your device, the admin password is reset to Admin123. You will be prompted to change the password when you first log in. If you want to change the password later, use this procedure to change the admin password to a new string if threat defense is offline or otherwise unavailable. Note that if threat defense is online, you will need to change the admin password using the threat defense CLI (see Change the Admin Password, on page 21).

**Note** The procedure to change the admin password via the FXOS CLI depends on the version of threat defense you are currently running.

### Before you begin

- Verify that you are in the FXOS CLI context. If you connect to the Firepower 1000/2100 or Secure Firewall 3100 device via serial console, you will automatically connect to the FXOS CLI context. If you are in the threat defense CLI context, you must first switch to the FXOS CLI context with the **connect fxos** command.

### Procedure

**Step 1** From the FXOS CLI, enter the security scope:

firepower # **scope security**

**Step 2** (Firepower Version 6.4 and later) You must reauthenticate the old admin password in order to set a new password:

firepower /security* # **set password**

**Example:**

```
FPR-2120# scope security
FPR-2120# /security # set password
Enter old password:
Enter new password:
Confirm new password:
firepower-2120 /security* # commit-buffer
```

(Firepower Version 6.3 and earlier) View the current list of local users. If you have just reimaged your device, admin will be the only user in this list:

firepower /security # **show local-user**

**Example:**

```
FPR-2120# scope security
FPR-2120 /security # show local-user
```

```
User Name       First Name      Last name
--------------- --------------- ---------
admin
```

a) (Firepower Version 6.3 and earlier) Enter the admin local user scope:

firepower /security # **enter local-user admin**

b) (Firepower Version 6.3 and earlier) Set the new password for user admin:

firepower /security/local-user # **set password**

**Example:**

```
FPR-2100 /security # enter local-user admin
FPR-2100 /security/local-user # set password
Enter a password: cisco
Confirm the password: cisco
```

**Step 3** Commit the configuration:

firepower /security/local-user* # **commit-buffer**

# Deregister From Cloud

If you reimage or factory reset your Firepower 1000/2100 or Secure Firewall 3100 device for a new purpose (for example, for transfer to a new group within your company, or after purchasing the device from a third party vendor), you may need to deregister the device from the cloud tenancy.

If you have access to the cloud (CDO) account to which the device was registered, log into that account and delete the Firepower 1000/2100 or Secure Firewall 3100 device.

If you do not have access to the cloud account, use the following procedure to deregister your Firepower 1000/2100 or Secure Firewall 3100 device from the cloud tenancy using the FXOS CLI.

### Before you begin

- Verify that you are in the FXOS CLI context. If you connect to the Firepower 1000/2100 or Secure Firewall 3100 device via serial console, you will automatically connect to the FXOS CLI context. If you are in the threat defense CLI context, you must first switch to the FXOS CLI context with the **connect fxos** command.
- Verify whether your device has access to the cloud:

  ```
  firepower # scope fabric a
  firepower /fabric-interconnect # show detail
  ```

  If no management IP address displays in the `show detail` output, you must first configure a management IP for your device:

  1. Enter the fabric interconnect scope:

     firepower # **scope fabric-interconnect**

  2. Set the new management IP information:

     firepower /fabric-interconnect # **set out-of-band static ip** *ip* **netmask** *netmask* **gateway** *gateway*

3. Commit the configuration:

   firepower /fabric-interconnect # **commit buffer**

### Procedure

**Step 1** Connect to the local-management command shell:

firepower # **connect local**

**Step 2** Deregister your device from the cloud:

firepower(local-mgmt)# **cloud deregister**

### Example

```
firepower # connect local
firepower(local-mgmt) # cloud deregister
```

# History for Firepower 1000/2100 and Secure Firewall 3100/4200 FXOS Troubleshooting

| Feature Name | Platform Releases | Description |
|---|---|---|
| Packet capture for mac-filter dropped packets from switch | Secure Firewall 7.4.1 | For Secure Firewall 3100 and 4100 devices, you can now capture mac-filter dropped packets from switch using the **set drop mac-filter** FXOS CLI command. |
| Switch Packet Path | Firepower 7.1 | You can now troubleshoot your Secure Firewall 3100 device for the switch packet path issues using the `portmanager` FXOS CLI command |
| Cloud deregister | Firepower 6.7 | You can now deregister your Firepower 1000/2100 device from your cloud tenant using the `cloud deregister` FXOS CLI command |
| Changing the admin password | Firepower 6.4 | In Firepower versions 6.4 and later on Firepower 1000/2100 devices, you must reauthenticate the old admin password before setting a new admin password. |