

# Reimage a Secure Firewall Threat Defense for 1000, 2100 and 3100 Series

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Before You Begin](#)

[Configure](#)

[Validation](#)

## Introduction

This document describes an example of a reimage procedure for the Secure Firewall Threat Defense (formerly Firepower Threat Defense).

## Prerequisites

## Requirements

Cisco recommends knowledge of these topics:

- There are no specific requirements for this guide

## Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure Firewall Threat Defense 2110 (FTD) Version 7.2.4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Background Information

Specific requirements for this document include:

- A console cable connected on the FTD
- A TFTP Server with the installation package (.SPA) already uploaded

This reimage procedure is supported on appliances:

- Cisco Secure Firewall Threat Defense 1000 Series
- Cisco Secure Firewall Threat Defense 2100 Series
- Cisco Secure Firewall Threat Defense 3100 Series

# Before You Begin

1. A reimage procedure erases all previous configurations. To restore any configurations, generate a backup before you start this procedure.
2. This procedure only applies for Firewalls running FTD software.
3. Verify the model is compatible with this procedure.

# Configure

## Step 1. Format the appliance:

- I. Connect to the console port of your appliance and create a console connection.
- II. Log into the FXOS chassis CLI.
- III. Type **connect local-mgmt** to move to the management console.
- III. Use the command **format everything** to delete all configurations and boot images on the appliance.
- III. Type **yes** to confirm the procedure

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

## Step 2. Interrupt the boot process by pressing **ESC** key to enter ROMMON mode:

```
*****
Cisco System ROMMON, Version 1.0.12, RELEASE SOFTWARE
Copyright (c) 1994-2019 by Cisco Systems, Inc.
Compiled Mon 06/17/2019 16:23:23.36 by builder
*****

Current image running: Boot ROM0
Last reset cause: ResetRequest (0x00001000)
DIMM_1/1 : Present
DIMM_2/1 : Absent

Platform FPR-2110 with 16384 Mbytes of main memory
BIOS has been successfully locked !!
MAC Address: 18:59:f5:d9:6a:00

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.

rommon 1 >
```

## Step 3. Fill the network and remote storage parameters with your configurations to prepare for the TFTP download:

- I. The parameters needed to be filled are:
  - A. ADDRESS=*ip\_address*
  - B. NETMASK=*netmask*
  - C. GATEWAY=*gateway\_ip*
  - D. SERVER=*remote\_storage\_server*
  - E. IMAGE=*path\_to\_the\_file*



change the appliance password:

```
firepower-2110 login: admin
Password:
Successful login attempts for user 'admin' : 1
Enter new password:
Confirm new password:
Your password was updated successfully.
```

---

**Note:** This error can get displayed while the initial setup is occurring however, it is going to be cleared after you install the threat defense software as described in later steps.

---

```
Jun 14 21:37:17 firepower-2110 FPRM: <<%FPRM-2-DEFAULT_INFRA_VERSION_MISSING>>
nfra-version-missing][org-root/fw-infra-pack-default] Bundle version in firmware
re-install
```

**Step 8.** Configure the IP of the management interface:

- I. Move to the fabric scope with the command **scope fabric-interconnect a**
- II. Set the management IP configuration with the command **set out-of-band static ip ip netmask netmask gw gateway**

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect # set out-of-band static ip 10.122.187.168 netmask 255.255.255.0 gw 10.122.187.161
Warning: When committed, this change may disconnect the current CLI session.
Use commit-buffer command to commit the changes.
firepower-2110 /fabric-interconnect* # commit-buffer
```

**Step 9.** Download the Threat Defense installation package:

- I. Move to firmware scope with the command **scope firmware**
- II. Download the installation package:
  - A. If you are using a USB you can use the command **download image usbA:package\_name**
  - B. If you are using a supported remote storage server you can use the command **download image tftp/ftp/scp/sftp://path\_to\_your\_package**

```
firepower-2110# scope firmware
firepower-2110 /firmware # download image tftp://10.207.204.10/cisco-ftd-fp2k.7.2.4-165.SP1
firepower-2110 /firmware # █
```

---

**Note:** When using remote storage servers, it is required to use absolute paths on the syntax of the command as displayed on the example.

---

**Step 10.** Validate the download progress with the command **show download-task:**

```
firepower-2110 /firmware # show download-task
Download task:
  File Name Protocol Server Port Userid State
  -----
  cisco-ftd-fp2k.7.2.4-165.SPA
  Tftp 10.207.204.10 0 Downloaded
```

**Note:** Once the download state transitions to *Downloaded* you can proceed to the next step.

**Step 11.** Review that the package is already on the firmware list with command **show package**:

```
firepower-2110 /firmware # show package
Name Package-Vers
-----
cisco-ftd-fp2k.7.2.4-165.SPA 7.2.4-165
```

**Note:** Copy the *package version* as it is going to be used on the installation of the Threat Defense software.

**Step 12.** Install the Threat Defense software to finalize the reimage:

- I. Move to the install scope with command **scope auto-install**.
- II. Proceed with the install of the threat defense software with command **install security-pack version version force**
- III. Two confirmation prompts are going to appear on the console, please confirm both of them by typing **yes**.

```
firepower-2110 /firmware # scope auto-install
firepower-2110 /firmware/auto-install # install security-pack version 7.2.4 force

Invalid software pack
Please contact technical support for help 5

The system is currently installed with security software package not set, which has:
- The platform version: not set
If you proceed with the upgrade 7.2.4-165, it will do the following:
- upgrade to the new platform version 2.12.0.499
- install with CSP ftd version 7.2.4.165
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

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

Triggered the install of software package version 7.2.4-165
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
```

**Caution:** The reimage process takes up to 45 minutes, be aware that the firewall is going to reboot while installing.

# Validation

Validate the upgrade process with the command **show detail**:

```
firepower-2110 /firmware/auto-install # show detail
Firmware Auto-Install:
  Package-Vers: 7.2.4-165
  Oper State: Scheduled
  Installation Time: 2023-06-14T22:07:28.777
  Upgrade State: Validating Images
  Upgrade Status: validating the software package
  Validation Software Pack Status:
  Firmware Upgrade Status: Ok
  Firmware Upgrade Message:
  Current Task: Validating the application pack(FSM-STAGE:sam:dme:FirmwareSyst
emDeploy:ValidateApplicationPack)
firepower-2110 /firmware/auto-install # █
```