Overview of the Firepower 1000/2100 Security Appliance FXOS CLI

This troubleshooting guide explains the Firepower eXstensible Operating System (FXOS) command line interface (CLI) for the Firepower 1000 and Firepower 2100 security appliance series.

The CLI on the SSH client management port defaults to Firepower Threat Defense. You can get to the FXOS CLI using the `connectfxos` command.

The CLI on the Firepower 1000/2100 console port defaults to the FXOS CLI prompt. You can get to the Firepower Threat Defense CLI using the `connectftd` command.

Once logged into the FXOS CLI, you can use the commands described below to view and troubleshoot the FXOS platform for your Firepower 1000 or Firepower 2100 series device.

If Firepower Threat Defense is installed on your Firepower 1000/2100 device, the FXOS CLI does not allow you to modify the configuration. If you attempt to perform any configuration changes with the FXOS CLI, the `commit-buffer` command returns an error.


FXOS CLI Hierarchy

The FXOS CLI is organized into a hierarchy of command modes, with the EXEC mode being the highest-level mode of the hierarchy. Higher-level modes branch into lower-level modes. You use `create`, `enter`, and `scope`
commands to move from higher-level modes to modes in the next lower level, and you use the `exit` command to move up one level in the mode hierarchy. You can also use the `top` command to move to the top level in the mode hierarchy.

Each mode contains a set of commands that can be entered in that mode. Most of the commands available in each mode pertain to the associated managed object.

The CLI prompt for each mode shows the full path down the mode hierarchy to the current mode. This helps you to determine where you are in the command mode hierarchy, and it can be an invaluable tool when you need to navigate through the hierarchy.

The following table lists the main command modes, the commands used to access each mode, and the CLI prompt associated with each mode.

**Table 1: Main Command Modes and Prompts**

<table>
<thead>
<tr>
<th>Mode Name</th>
<th>Commands Used to Access</th>
<th>Mode Prompt</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXEC</td>
<td><code>top</code> command from any mode</td>
<td>#</td>
</tr>
<tr>
<td>chassis</td>
<td><code>scope chassis</code> command from EXEC mode</td>
<td>/chassis #</td>
</tr>
<tr>
<td>Ethernet uplink</td>
<td><code>scope eth-uplink</code> command from EXEC mode</td>
<td>/eth-uplink #</td>
</tr>
<tr>
<td>fabric-interconnect</td>
<td><code>scope fabric-interconnect</code> command from EXEC mode</td>
<td>/fabric-interconnect #</td>
</tr>
<tr>
<td>firmware</td>
<td><code>scope firmware</code> command from EXEC mode</td>
<td>/firmware #</td>
</tr>
<tr>
<td>monitoring</td>
<td><code>scope monitoring</code> command from EXEC mode</td>
<td>/monitoring #</td>
</tr>
<tr>
<td>organization</td>
<td><code>scope org</code> command from EXEC mode</td>
<td>/org #</td>
</tr>
<tr>
<td>security</td>
<td><code>scope security</code> command from EXEC mode</td>
<td>/security #</td>
</tr>
<tr>
<td>server</td>
<td><code>scope server</code> command from EXEC mode</td>
<td>/server #</td>
</tr>
<tr>
<td>ssa</td>
<td><code>scope ssa</code> command from EXEC mode</td>
<td>/ssa #</td>
</tr>
<tr>
<td>system</td>
<td><code>scope system</code> command from EXEC mode</td>
<td>/system #</td>
</tr>
</tbody>
</table>
Online Help for the CLI

At any time, you can type the `?` character to display the options available at the current state of the command syntax.

If you have not typed anything at the prompt, typing `?` lists all available commands for the mode you are in. If you have partially typed a command, typing `?` lists all available keywords and arguments available at your current position in the command syntax.
Global FXOS CLI Commands

The following commands are global for all modes in the FXOS CLI.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>acknowledge fault</td>
<td>Acknowledges a fault. Command syntax:</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>acknowledge fault 1</td>
</tr>
<tr>
<td></td>
<td>Where id is the fault identification number. The range of valid values is 0</td>
</tr>
<tr>
<td></td>
<td>to 9223372036854775807.</td>
</tr>
<tr>
<td>clear</td>
<td>Clears managed objects.</td>
</tr>
<tr>
<td>commit-buffer</td>
<td>Commits transaction buffer.</td>
</tr>
<tr>
<td>connect</td>
<td>Connect to another CLI.</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>connect ftd</td>
</tr>
<tr>
<td>discard-buffer</td>
<td>Discard transaction buffer.</td>
</tr>
<tr>
<td>end</td>
<td>Go to exec mode.</td>
</tr>
<tr>
<td>exit</td>
<td>Exit from command interpreter.</td>
</tr>
<tr>
<td>scope</td>
<td>Enters a new mode.</td>
</tr>
<tr>
<td>set</td>
<td>Sets property values.</td>
</tr>
<tr>
<td>show</td>
<td>Shows system information.</td>
</tr>
<tr>
<td>terminal</td>
<td>Terminal.</td>
</tr>
<tr>
<td>top</td>
<td>Goes to the top of the mode.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>ucspe-copy</td>
<td>Copies a file in UCSPE.</td>
</tr>
<tr>
<td>up</td>
<td>Goes up one mode.</td>
</tr>
<tr>
<td>where</td>
<td>Shows information about the current mode.</td>
</tr>
<tr>
<td>backup</td>
<td>Backup.</td>
</tr>
</tbody>
</table>
CHAPTER 3

FXOS CLI Troubleshooting Commands

• FXOS CLI Chassis Mode Troubleshooting Commands, on page 7
• FXOS CLI Eth-Uplink Mode Troubleshooting Commands, on page 11
• FXOS CLI Fabric Interconnect Mode Troubleshooting Commands, on page 14
• FXOS CLI Security Services Mode Troubleshooting Commands, on page 17

FXOS CLI Chassis Mode Troubleshooting Commands

Use the following chassis mode FXOS CLI commands to troubleshoot issues with your Firepower 1000/2100 system.

**show environment**

Displays environment information for the chassis.

For example:

```
FPR2100 /chassis # show environment expand detail
Chassis 1:
Overall Status: Power Problem
  Operability: Operable
  Power State: Ok
  Thermal Status: Ok
PSU 1:
  Overall Status: Powered Off
  Operability: Unknown
  Power State: Off
  Voltage Status: Unknown
PSU 2:
  Overall Status: Operable
  Operability: Operable
  Power State: On
  Voltage Status: Ok
Tray 1 Module 1:
  Overall Status: Operable
  Operability: Operable
  Power State: On
Fan 1:
  Overall Status: Operable
  Operability: Operable
  Power State: On
Fan 2:
  Overall Status: Operable
  Operability: Operable
  Power State: On
Fan 3:
```
Overall Status: Operable
Operability: Operable
Power State: On
Fan 4:
Overall Status: Operable
Operability: Operable
Power State: On
Server 1:
Overall Status: Ok
Memory Array 1:
Current Capacity (MB): 32768
Populated: 2
DIMMs:
<table>
<thead>
<tr>
<th>ID</th>
<th>Overall Status</th>
<th>Capacity (MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Operable</td>
<td>16384</td>
</tr>
<tr>
<td>2</td>
<td>Operable</td>
<td>16384</td>
</tr>
</tbody>
</table>
CPU 1:
Presence: Equipped
Cores: 8
Product Name: Intel(R) Xeon(R) CPU D-1548 @ 2.00GHz
Vendor: GenuineIntel
Thermal Status: OK
Overall Status: Operable
Operability: Operable

**scope fan**
Enters the fan mode on Firepower 2110 and 2120 devices.

**scope fan-module**
Enters the fan mode on Firepower 2130 and 2140 devices. From this mode, you can display detailed information about the chassis fan.

For example:
```
FPR2100 /chassis # show fan-module expand detail
Fan Module:
Tray: 1
Module: 1
Overall Status: Operable
Operability: Operable
Power State: On
Presence: Equipped
Product Name: Cisco Firepower 2000 Series Fan Tray
PID: FPR2K-FAN
Vendor: Cisco Systems, Inc
Fan:
ID: 1
Overall Status: Operable
Operability: Operable
Power State: On
Presence: Equipped
ID: 2
Overall Status: Operable
Operability: Operable
Power State: On
Presence: Equipped
```

**show inventory**
Displays inventory information such as the chassis number, vendor, and serial number.
Note: This command only applies to Firepower 2130 and 3140 devices.
For example:
```
FPR2100 /chassis # show inventory
Chassis PID Vendor Serial (SN) HW Revision
```
**show inventory expand**

Displays detailed inventory information about FRUable components such as the chassis, PSU, and network modules.

For example:

```
FPR2100 /chassis # show inventory expand detail
Chassis 1:
  Product Name: Cisco Firepower 2000 Appliance
  PID: FPR-2130
  VID: V01
  Vendor: Cisco Systems, Inc
  Model: FPR-2130
  Serial (SN): JAD2012091X
  HW Revision: 0.1
  PSU 1:
    Presence: Equipped
    Product Name: Cisco Firepower 2000 Series AC 400W Power Supply
    PID: FPR2K-PWR-AC-400
    VID: V01
    Vendor: Cisco Systems, Inc
    Serial (SN): LIT2010CAFE
    HW Revision: 0
  PSU 2:
    Presence: Equipped
    Product Name: Cisco Firepower 2000 Series AC 400W Power Supply
    PID: FPR2K-PWR-AC-400
    VID: V01
    Vendor: Cisco Systems, Inc
    Serial (SN): LIT2010CAFE
    HW Revision: 0
  Fan Modules:
    Tray 1 Module 1:
      Presence: Equipped
      Product Name: Cisco Firepower 2000 Series Fan Tray
      PID: FPR2K-FAN
      Vendor: Cisco Systems, Inc
  Fans:
    ID Presence
    -- --------
    1 Equipped
    2 Equipped
    3 Equipped
    4 Equipped
  Fabric Card 1:
    Description: Cisco SSP FPR 2130 Base Module
    Number of Ports: 16
    State: Online
    Vendor: Cisco Systems, Inc.
    Model: FPR-2130
    HW Revision: 0
    Serial (SN): JAD2012091X
    Perf: N/A
    Operability: Operable
    Overall Status: Operable
    Power State: Online
    Presence: Equipped
    Thermal Status: N/A
    Voltage Status: N/A
  Fabric Card 2:
    Description: 8-port 10 Gigabit Ethernet Expansion Module
    Number of Ports: 8
```
State: Online
Vendor: Cisco Systems, Inc.
Model: FPR-NM-8X10G
HW Revision: 0
Serial (SN): JAD19510AKD
Perf: N/A
Operability: Operable
Overall Status: Operable
Power State: Online
Presence: Equipped
Thermal Status: N/A
Voltage Status: N/A

```scope psu
Enters the power supply unit mode. From this mode, you can view detailed information about the power supply unit.
For example:
```
```cpp
FPR2100 /chassis # show psu expand detail
PSU:
PSU: 1
Overall Status: Powered Off
Operability: Unknown
Power State: Off
Presence: Equipped
Voltage Status: Unknown
Product Name: Cisco Firepower 2000 Series AC 400W Power Supply
PID: FPR2K-FWR-AC-400
VID: V01
Vendor: Cisco Systems, Inc
Serial (SN): LIT2010CAFE
Type: AC
Fan Status: Ok
PSU: 2
Overall Status: Operable
Operability: Operable
Power State: On
Presence: Equipped
Voltage Status: Ok
Product Name: Cisco Firepower 2000 Series AC 400W Power Supply
PID: FPR2K-FWR-AC-400
VID: V01
Vendor: Cisco Systems, Inc
Serial (SN): LIT2010CAFE
Type: AC
Fan Status: Ok
```

```scope stats
Enters the stats mode. From this mode, you can view detailed information about the chassis statistics.
For example:
```
```cpp
FPR2100 /chassis # show stats
Chassis Stats:
  Time Collected: 2016-11-14T21:19:46.317
  Monitored Object: sys/chassis-1/stats
  Suspect: No
  Outlet Temp1 (C): 43.000000
  Outlet Temp2 (C): 41.000000
  Inlet Temp (C): 30.000000
  Internal Temp (C): 34.000000
  Thresholded: 0
Fan Stats:
  Time Collected: 2016-11-14T21:19:46.317
  Monitored Object: sys/chassis-1/fan-module-1-1/fan-1/stats
```
FXOS CLI Eth-Uplink Mode Troubleshooting Commands

Use the following eth-uplink mode FXOS CLI commands to troubleshoot issues with your Firepower 1000/2100 system.

`show detail`

Displays detailed information about your Firepower 1000/2100 device's Ethernet uplink.
For example:

FPR2100 /eth-uplink # show detail
Ethernet Uplink:
  Mode: Security Node
  MAC Table Aging Time (dd:hh:mm:ss): 00:04:01:40
  VLAN Port Count Optimization: Disabled
  Current Task:

```
FPR2100 /eth-uplink # show interface
```
```
Interface:
  Port Name   Port Type   Admin State  Oper State  State Reason
  ------------ ------- ------------ ------------ ------------
  Ethernet1/1  Data     Enabled       Up           Up
  Ethernet1/2  Data     Enabled       Link Down    Down
  Ethernet1/3  Data     Disabled      Link Down    Down
  Ethernet1/4  Data     Disabled      Link Down    Down
  Ethernet1/5  Data     Disabled      Link Down    Down
  Ethernet1/6  Data     Disabled      Link Down    Down
  Ethernet1/7  Data     Disabled      Link Down    Down
  Ethernet1/8  Data     Disabled      Link Down    Down
  Ethernet1/9  Data     Disabled      Link Down    Down
  Ethernet1/10 Data    Disabled      Link Down    Down
  Ethernet1/11 Data    Disabled      Link Down    Down
  Ethernet1/12 Data    Disabled      Link Down    Down
  Ethernet1/13 Data    Disabled      Link Down    Down
  Ethernet1/14 Data    Disabled      Link Down    Down
  Ethernet1/15 Data    Disabled      Link Down    Down
  Ethernet1/16 Data    Disabled      Link Down    Down
  Ethernet2/1  Data     Disabled      Link Down    Down
  Ethernet2/2  Data     Disabled      Link Down    Down
  Ethernet2/3  Data     Disabled      Link Down    Down
  Ethernet2/4  Data     Disabled      Link Down    Down
  Ethernet2/5  Data     Disabled      Link Down    Down
  Ethernet2/6  Data     Disabled      Link Down    Down
  Ethernet2/7  Data     Disabled      Link Down    Down
  Ethernet2/8  Data     Disabled      Link Down    Down
```

```
FPR2100 /eth-uplink/fabric # show port-channel
Port Channel:
  Port Channel Id  Name   Port Type  Admin State  Oper State
  --------------- --- -------- ------------ ------------
  1               Port-channel1 Data Disabled
                  Link Down
```

```
FPR2100 /eth-uplink/fabric/port-channel # show stats
Ether Error Stats:
  Monitored Object: fabric/lan/A/pc-1/err-stats
  Suspect: No
  Rcv (errors): 0
  Align (errors): 0
  Fcs (errors): 0
  Xmit (errors): 0
  Under Size (errors): 0
  Out Discard (errors): 0
  Deferred Tx (errors): 0
  Int Mac Tx (errors): 0
```
Int Mac Rx (errors): 0
Thresholded: Xmit Delta Min
Ether Loss Stats:
  Monitored Object: fabric/lan/A/pc-1/loss-stats
  Suspect: No
  Single Collision (errors): 0
  Multi Collision (errors): 0
  Late Collision (errors): 0
  Excess Collision (errors): 0
  Carrier Sense (errors): 0
  Giants (errors): 0
  Symbol (errors): 0
  SQE Test (errors): 0
  Thresholded: 0
Ether Pause Stats:
  Monitored Object: fabric/lan/A/pc-1/pause-stats
  Suspect: No
  Recv Pause (pause): 0
  Xmit Pause (pause): 0
  Resets (resets): 0
  Thresholded: 0
Ether Rx Stats:
  Monitored Object: fabric/lan/A/pc-1/rx-stats
  Suspect: No
  Total Packets (packets): 0
  Unicast Packets (packets): 0
  Multicast Packets (packets): 0
  Broadcast Packets (packets): 0
  Total Bytes (bytes): 0
  Jumbo Packets (packets): 0
  Thresholded: 0
Ether Tx Stats:
  Monitored Object: fabric/lan/A/pc-1/tx-stats
  Suspect: No
  Total Packets (packets): 0
  Unicast Packets (packets): 0
  Multicast Packets (packets): 0
  Broadcast Packets (packets): 0
  Total Bytes (bytes): 0
  Jumbo Packets (packets): 0
  Thresholded: 0
Ether Error Stats:
  Monitored Object: sys/switch-A/slot-1/switch-ether/port-1/err-stats
  Suspect: No
  Rcv (errors): 0
  Align (errors): 0
  Fcs (errors): 0
  Xmit (errors): 0
  Under Size (errors): 0
  Out Discard (errors): 0
  Deferred Tx (errors): 0
  Int Mac Tx (errors): 0
  Int Mac Rx (errors): 0
  Thresholded: Xmit Delta Min
Ether Loss Stats:
  Monitored Object: sys/switch-A/slot-1/switch-ether/port-1/loss-stats
  Suspect: No
  Single Collision (errors): 0
FXOS CLI Fabric Interconnect Mode Troubleshooting Commands

Use the following fabric-interconnect mode FXOS CLI commands to troubleshoot issues with your Firepower 1000/2100 system.

show card
Displays information on a fabric card.
For example:

```
FPR2100 /fabric-interconnect # show card detail expand
Fabric Card:
  Id: 1
  Description: Cisco SSP FPR 2130 Base Module
  Number of Ports: 16
  State: Online
  Vendor: Cisco Systems, Inc.
  Model: FPR-2130
  HW Revision: 0
  Serial (SN): JAD2012091X
  Perf: N/A
  Operability: Operable
  Overall Status: Operable
```
Power State: Online
Presence: Equipped
Thermal Status: N/A
Voltage Status: N/A

show image
Displays all available images.

```
firepower /firmware # show image
Name Type Version
--------------------------------------------- -------------------- -------
cisco-ftd.6.2.0.131.csp Firepower Cspapp 6.2.0.131
cisco-ftd.6.2.0.140.csp Firepower Cspapp 6.2.0.140
cisco-ftd.6.2.0.175.csp Firepower Cspapp 6.2.0.175
fxos-k8-fp2k-firmware.0.4.04.SPA Firepower Firmware 0.4.04
fxos-k8-fp2k-lfbff.82.1.1.303i.SSA Firepower System 82.1(1.303i)
fxos-k8-fp2k-npu.82.1.1.303i.SSA Firepower Npu 82.1(1.303i)
fxos-k8-fp2k-npu.82.1.1.307i.SSA Firepower Npu 82.1(1.307i)
fxos-k9-fp2k-manager.82.1.1.303i.SSA Firepower Manager 82.1(1.303i)
```

show package
Displays all available packages.

```
firepower /firmware # show package
Name Package-Vers
--------------------------------------------- ------------
cisco-ftd-fp2k.6.2.0.131-303i.SSA 6.2(0.131-303i)
cisco-ftd-fp2k.6.2.0.140-307i.SSA 6.2(0.140-307i)
cisco-ftd-fp2k.6.2.0.140-308i.SSA 6.2(0.140-308i)
cisco-ftd-fp2k.6.2.0.175-311i.SSA 6.2(0.175-311i)
cisco-ftd-fp2k.6.2.0.175-314i.SSA 6.2(0.175-314i)
cisco-ftd-fp2k.6.2.0.175-318i.SSA 6.2(0.175-318i)
cisco-ftd-fp2k.6.2.0.175-319i.SSA 6.2(0.175-319i)
```

show package package name expand
Displays the package details.

```
show package package name expandCisco-fjd-fp2k.6.2.0.131-303i.SSA expand
Package cisco-ftd-fp2k.6.2.0.131-303i.SSA:
Images:
cisco-ftd.6.2.0.131.csp
fxos-k8-fp2k-firmware.0.4.04.SPA
fxos-k8-fp2k-lfbff.82.1.1.303i.SSA
fxos-k8-fp2k-npu.82.1.1.303i.SSA
fxos-k9-fp2k-manager.82.1.1.303i.SSA
```

scope auto-install
Enters the auto-install mode. From this mode, you can view the current FXOS upgrade state.

```
firepower /firmware/auto-install # show
Firmware Auto-Install:
Package-Vers Oper State Upgrade State
------------ ---------------------------- ------------
6.2(0.175-319i) Scheduled Installing Application
```

scope firmware
Enters the firmware mode. From this mode, you can view download task information.

For example:

```
FPR2100 /firmware # show download-task
Download task:
File Name Protocol Server
Port Userid State
-------- -------- -------
```

Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 Series Running Firepower Threat Defense
scope download-task
Enters the download-task mode. From this mode, you can view additional details about each download task and restart the download task.
For example:

Download task:
File Name: test.SSA
Protocol: Scp
Server: 172.29.191.78
Port: 0
Userid: user
Path: /tmp
Downloaded Image Size (KB): 0
State: Failed
Transfer Rate (KB/s): 0.000000
Current Task: deleting downloadable test.SSA on local
firepower /firmware/download-task # show fsm status
File Name: test.SSA
FSM 1:
Remote Result: End Point Failed
Remote Error Code: ERR MO Illegal Iterator State
Remote Error Description: End point timed out. Check for IP, port, password, disk space or network access related issues.#
Status: Download Fail
Previous Status: Download Fail
Try: 2
Progress (%): 0
Current Task: deleting downloadable test.SSA on local
firepower /firmware/download-task # restart
Password:

scope psu
Enters the power supply unit mode. From this mode, you can view detailed information about the power supply unit.
For example:

FPR2100 /chassis # show psu expand detail
PSU:
PSU: 1
Overall Status: Powered Off
Operability: Unknown
Power State: Off
Presence: Equipped
Voltage Status: Unknown
Product Name: Cisco Firepower 2000 Series AC 400W Power Supply
PID: FPR2K-PWR-AC-400
VID: V01
Vendor: Cisco Systems, Inc
Serial (SN): LIT2010CAFE
Type: AC
Fan Status: Ok
PSU: 2
FXOS CLI Security Services Mode Troubleshooting Commands

Use the following security services (ssa) mode FXOS CLI commands to troubleshoot issues with your Firepower 1000/2100 system.

**show app**

Displays information about the applications attached to you Firpower 1000/2100 device.

For example:

```
firepower /ssa # show app
```

<table>
<thead>
<tr>
<th>Application</th>
<th>Name</th>
<th>Version</th>
<th>Description</th>
<th>Author</th>
<th>Deploy Type</th>
<th>CSP Type</th>
<th>Is Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftd</td>
<td>6.2.0.131</td>
<td>N/A</td>
<td>cisco</td>
<td>Native</td>
<td>Application No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ftd</td>
<td>6.2.0.140</td>
<td>N/A</td>
<td>cisco</td>
<td>Native</td>
<td>Application No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ftd</td>
<td>6.2.0.175</td>
<td>N/A</td>
<td>cisco</td>
<td>Native</td>
<td>Application Yes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Reimage Procedures

- Firepower 1000/2100 Series Software Reimage and Disaster Recovery Procedures, on page 19

Firepower 1000/2100 Series Software Reimage and Disaster Recovery Procedures

In some cases, you may want to reset your system to its manufacturing settings. There are four reimaging options available:

**Erase configuration and restart the system with the same Firepower Threat Defense image**
All configurations are removed and Firepower Threat Defense is reinstalled using the current running software package. Note that after performing this procedure, you will have to reconfigure the system, including admin password and connectivity information.
For the full procedure, see: Reimage the Firepower 1000/2100 System with the Base Install Software Package Version, on page 20

**Re-image the system with a new application software version**
The current Firepower Threat Defense instance is deleted and a new Firepower Threat Defense instance is installed. Note that after performing this procedure, you will have to reconfigure the system, including admin password and connectivity information.
For the full procedure, see: Reimage the Firepower 1000/2100 Series System with a New Software Package Version, on page 22

**Reimage the system to its factory default settings**
This option restores your system to its factory default settings. The procedure requires you to boot the system over tftp, download the application software, apply the software, and reconfigure the entire system.
For the full procedure, see: Perform a Complete Reimage of the Firepower 1000/2100 System, on page 23

**Reimage the system to its factory default settings (admin password recovery)**
This option restores your system to its factory default settings if the admin password is not known. The procedure requires you to interrupt the boot, factory reset the device, download the application software, apply the software, and reconfigure the entire system.
For the full procedure, see: Perform a Complete Reimage of the Firepower 1000/2100 System if the Admin Password is Unknown, on page 26
After performing any of these procedures, the admin password is reset to Admin123. Once completing a reimage of your Firepower 1000/2100 device, you must change the admin password to a new string using the steps detailed in Change the Admin Password for Firepower 1000/2100, on page 28.

**Note**

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

- You must reconfigure the system from scratch after Firepower Threat Defense comes online.
- When reverting to a lower version of a Firepower Threat Defense device using the erase configuration method, the FXOS version may not revert back to a lower version. This may cause failures in a High Availability configuration. For this scenario, we recommended that you perform a complete re-image of the system (see Perform a Complete Reimage of the Firepower 1000/2100 System, on page 23 for more information).

### Before you begin

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

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

- Take note of your Firepower Threat Defense base install version using the following commands. The Startup Version column shows your 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.
Procedure

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

```plaintext
firepower # connect local-mgmt
```

Step 2
Erase all configuration:

```plaintext
firepower(local-mgmt) # erase configuration
```

**Example:**

```plaintext
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:**

```plaintext
firepower# scope ssa
firepower /ssa # show app-instance
```

<table>
<thead>
<tr>
<th>Application Name</th>
<th>Slot ID</th>
<th>Admin State</th>
<th>Operational State</th>
<th>Running Version</th>
<th>Startup Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftd</td>
<td>1</td>
<td>Disabled</td>
<td>Installing</td>
<td>6.2.1-1314</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>

**Note**

It may take more than 10 minutes for the application installation to complete. Once Firepower Threat Defense is back online, the Operational State of the `show app-instance` command displays as Online:

**Example:**

```plaintext
firepower /ssa # show app-instance
```

<table>
<thead>
<tr>
<th>Application Name</th>
<th>Slot ID</th>
<th>Admin State</th>
<th>Operational State</th>
<th>Running Version</th>
<th>Startup Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftd</td>
<td>1</td>
<td>Enabled</td>
<td>Online</td>
<td>6.2.1.10140</td>
<td></td>
</tr>
</tbody>
</table>

**What to do next**

Reconfigure the Firepower Threat Defense application and upgrade to latest version if necessary. For more information on how to set your management IP and other configuration parameters, see the Getting Started Guide for your device.
Reimage the Firepower 1000/2100 Series System with a New Software Package Version

This procedure allows you to reimage the Firepower Threat Defense on the Firepower 1000/2100 series system with a new software version. The Firepower Threat Defense application is uninstalled and then reinstalled with the latest software version. After performing this procedure, you will need to reconfigure the management IP and other configuration parameters on the device.

Note

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

Before you begin

- Take note of your appliance management IP 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.

Procedure

Step 1

Download the Firepower Threat Defense for Firepower 1000/2100 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 Service Manager, 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 Firepower 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
  ```

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
  ```

You can also use FTP, SCP, SFTP, or TFTP to copy the Firepower Threat Defense software package to the device:

  ```
  firepower /firmware # download image ftp/ftp/scp/sftp://path to the image, including the server root/image name
  ```
For example:

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

**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:

```bash
grep /firmware # show download-task
```

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

**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:

```bash
grep /firmware # show package
```

**Example:**

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

In the above example, **6.2.1-36** is the security pack version.

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

```bash
grep /firmware # scope auto-install
```

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

```bash
grep /firmware/auto-install # install security-pack version
```

**Step 10**
Enter yes when prompted.

The system reboots, then installs the latest software bundle.

---

**What to do next**
Reconfigure the Firepower Threat Defense application. For more information on how to set your management IP and other configuration parameters, see the Getting Started Guide for your device.

---

**Perform a Complete Reimage of the Firepower 1000/2100 System**

This procedure reformats the entire Firepower Threat Defense on the Firepower 1000/2100 Series system and returns it to its factory default settings. After performing this procedure, you must download the new software images and reconfigure your system from scratch.
After performing this procedure, the admin password is reset to **Admin123**.

### Procedure

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

```
firepower # connect local-mgmt
```

**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/FTP/SCP 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
```

**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/FTP/SCP server IP.
rommon 9 > ping server IP

**Note**  Pings from the TFTP/FTP/SCP server IP to the management IP will fail. This is expected behavior.

**Step 8**

Boot the Firepower 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
```

This error condition clears as soon as you install the new Firepower Threat Defense software package version (step 14 of 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 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 Firepower 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 FTP, SCP, SFTP, or TFTP to copy the Firepower Threat Defense software package to the device:
Perform a Complete Reimage of the Firepower 1000/2100 System if the Admin Password is Unknown

This procedure reformats the entire Firepower Threat Defense on the Firepower 1000/2100 Series system and returns it to its factory default settings, including the admin password. After performing this procedure, you must download the new software images and reconfigure your system from scratch.

Use this procedure to factory reset the device when the admin password is not known. If the admin password is known, use the steps detailed in Perform a Complete Reimage of the Firepower 1000/2100 System, on page 23 to factory reset the device.
After performing this procedure, the admin password is reset to **Admin123**.

**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:*  
```
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

**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:*  
```
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-1fbff.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-1fbff.2.3.1.132.SSB

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

```
rommon 3 > boot
```

The system reboots while installing Firepower Threat Defense.
What to do next

- Set a new admin password. For more information, see Change the Admin Password for Firepower 1000/2100, on page 28.

- Reconfigure the Firepower Threat Defense application. For more information on how to set your management IP and other configuration parameters, see the Getting Started Guide for your device.

Change the Admin Password for Firepower 1000/2100

After reimaging your Firepower 1000/2100 device, the admin password is reset to Admin123. Use this procedure to change the admin password to a new string.

Procedure

Step 1 From the FXOS CLI, enter the security scope:
firepower # scope security

Step 2 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-2100# scope security
FPR-2100 /security # show local-user
User Name  First Name Last name
----------------------------------  --------  -------
admin

Step 3 Enter the admin local user scope:
firepower /security # enter local-user admin

Step 4 Set the new password for user admin:
firepower /security/local-user # set password

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

Step 5 Commit the configuration:
firepower /security/local-user* # commit-buffer