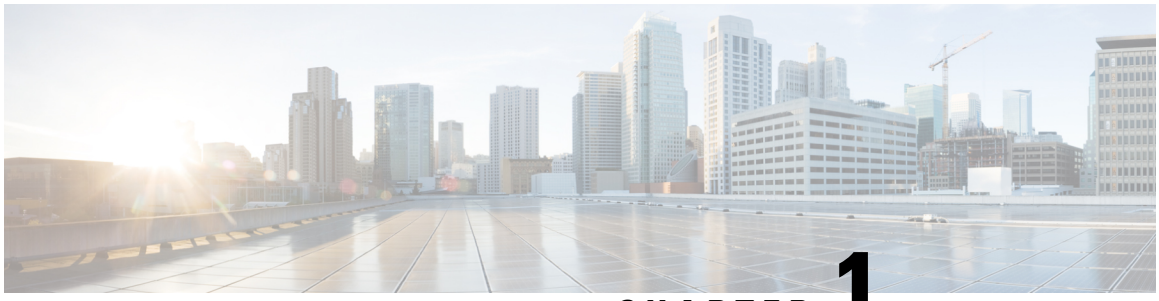
Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 with Firepower Threat Defense

First Published: 2017-05-15

Last Modified: 2021-06-14

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

About the Firepower 1000/2100 Security Appliance CLI

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.

Note The CLI on the SSH client management port defaults to Firepower Threat Defense. You can get to the FXOS CLI using the **connect fxos** 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 **connect ftd** 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.

For more information about the Firpower Threat Defense CLI, see the Command Reference for Firpower Threat Defense (http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html).

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.

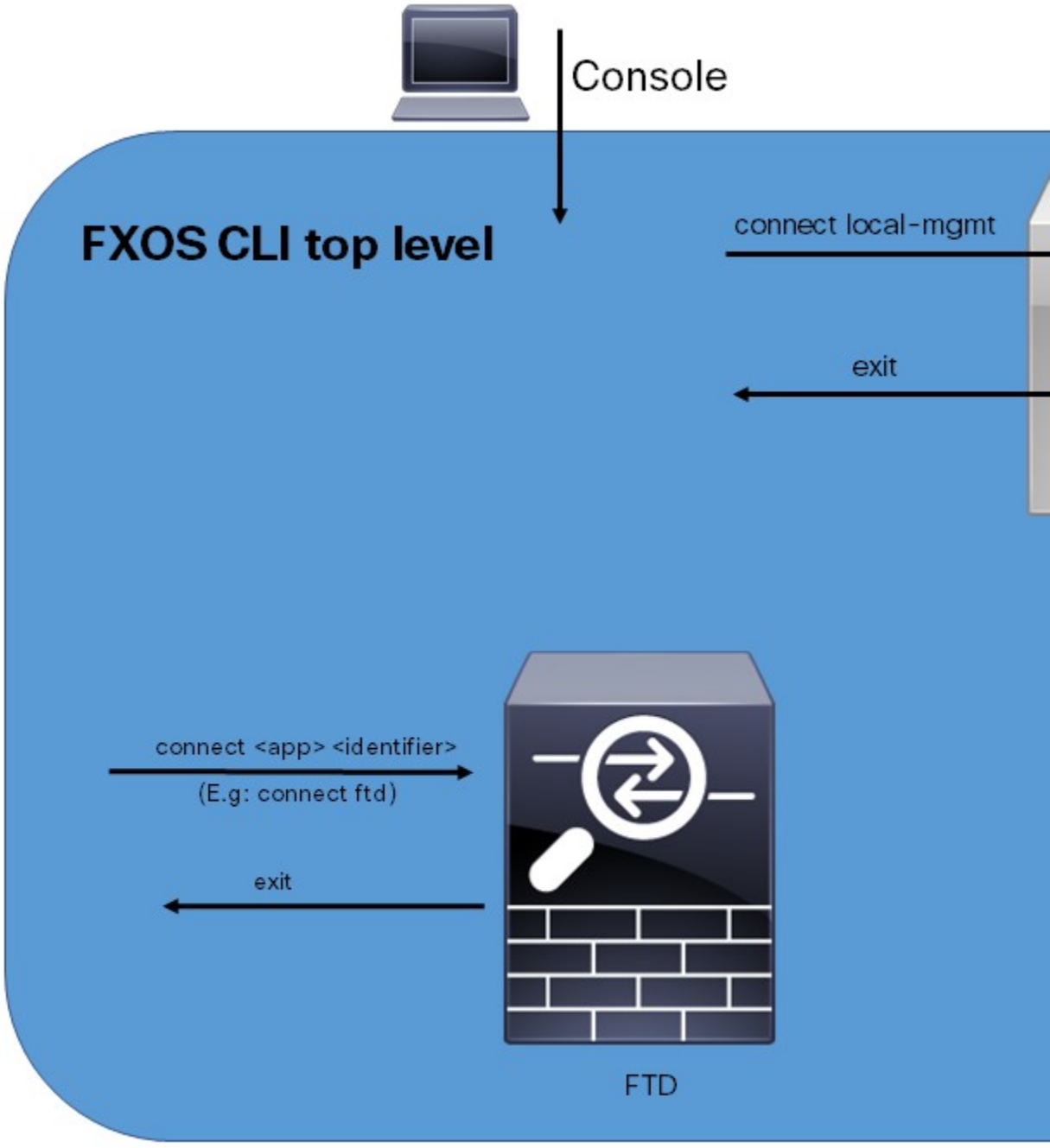
The following table lists the main command modes, the commands used to access each mode, and the CLI prompt associated with each mode.

Table 1: Main Command Modes and Prompts

Mode Name	Commands Used to Access	Mode Prompt
EXEC	**top** command from any mode	#
chassis	**scope chassis** command from EXEC mode	/chassis #
Ethernet uplink	**scope eth-uplink** command from EXEC mode	/eth-uplink #
fabric-interconnect	**scope fabric-interconnect** command from EXEC mode	/fabric-interconnect #
firmware	**scope firmware** command from EXEC mode	/firmware #
monitoring	**scope monitoring** command from EXEC mode	/monitoring #
organization	**scope org** command from EXEC mode	/org #
security	**scope security** command from EXEC mode	/security #
server	**scope server** command from EXEC mode	/server #
ssa	**scope ssa** command from EXEC mode	/ssa #
system	**scope system** command from EXEC mode	/system #

The following diagram outlines the commands that can be executed from the FXOS CLI top level to access the FXOS command shell, local management command shell, and Firepower Threat Defense CLI. Note that console access is required.

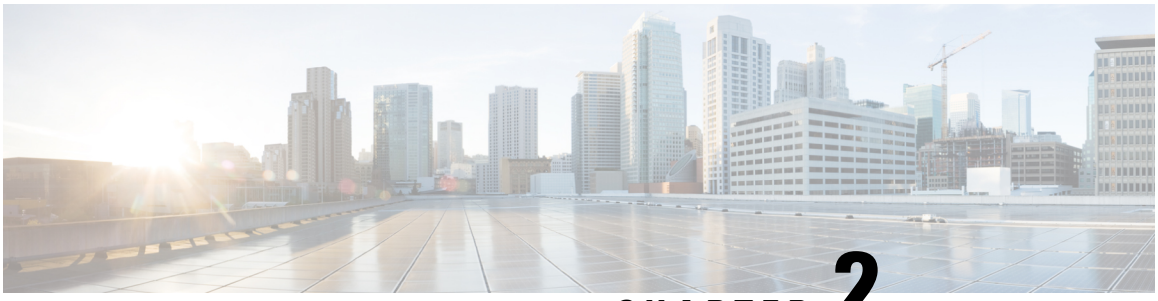
Figure 1: Firepower 1000/2100 FXOS CLI Connect Diagram



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.



CHAPTER 2

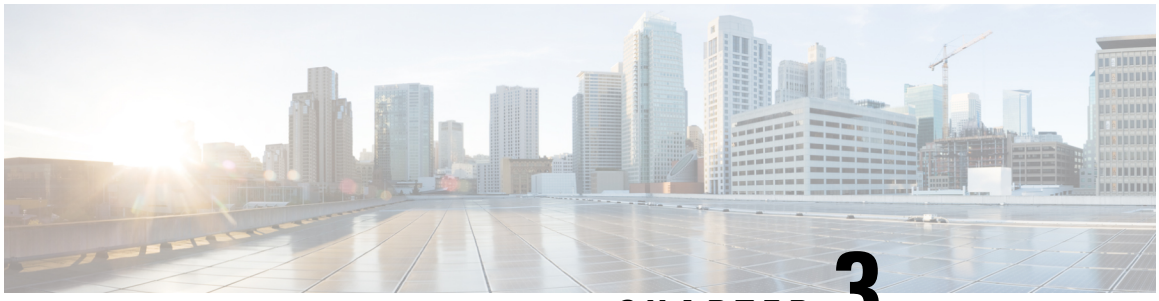
Global FXOS CLI Commands

Global FXOS CLI Commands

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

Command	Description
acknowledge fault	Acknowledges a fault. Command syntax: For example: `acknowledge fault 1` Where *id* is the fault identification number. The range of valid values is 0 to 9223372036854775807.
clear	Clears managed objects.
commit-buffer	Commits transaction buffer.
connect	Connect to another CLI. For example: `connect ftd`
discard-buffer	Discard transaction buffer.
end	Go to exec mode.
exit	Exit from command interpreter.
scope	Enters a new mode.
set	Sets property values.
show	Shows system information.
terminal	Terminal.
top	Goes to the top of the mode.

Command	Description
ucspe-copy	Copies a file in UCSPE.
up	Goes up one mode.
where	Shows information about the current mode.
backup	Backup.



CHAPTER 3

FXOS CLI Troubleshooting Commands

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:
                ID  Overall Status           Capacity (MB)
                --- ------------------------ -------------
                  1 Operable                 16384
                  2 Operable                 16384
            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
```

show environmentbasic

Displays chassis and CPU temperature data.

For example:

```
FPR2100 /chassis # show environment basic
     ***************  Chassis Temps  ***************
     Inlet temperature is 75 degrees Celsius

     ***************  CPU Data  ***************
     Core Temperature 0 is 93 degrees Celsius
     Core Temperature 1 is 93 degrees Celsius
     Core Temperature 2 is 94 degrees Celsius
     Core Temperature 3 is 92 degrees Celsius
```

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
---------- --------------- ----------------- ----------- -----------
         1 FPR-2140        Cisco Systems, In JAD201005FC 0.1
```

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:

```
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
    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-PWR-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 statatistics. For example:

```
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
    Suspect: No
    Speed (RPM): 17280
    Thresholded: 0
    Time Collected: 2016-11-14T21:19:46.317
    Monitored Object: sys/chassis-1/fan-module-1-1/fan-2/stats
    Suspect: No
    Speed (RPM): 17340
    Thresholded: 0
    Time Collected: 2016-11-14T21:19:46.317
    Monitored Object: sys/chassis-1/fan-module-1-1/fan-3/stats
    Suspect: No
    Speed (RPM): 17280
    Thresholded: 0
    Time Collected: 2016-11-14T21:19:46.317
    Monitored Object: sys/chassis-1/fan-module-1-1/fan-4/stats
    Suspect: No
    Speed (RPM): 17280
    Thresholded: 0
Psu Stats:
    Time Collected: 2016-11-14T21:19:46.318
    Monitored Object: sys/chassis-1/psu-1/stats
    Suspect: No
    Input Current (A): 0.000000
    Input Power (W): 8.000000
    Input Voltage (V): 0.000000
    Psu Temp1 (C): 32.000000
    Psu Temp2 (C): 36.000000
    Psu Temp3 (C): 32.000000
    Fan Speed (RPM): 0
    Thresholded: 0
    Time Collected: 2016-11-14T21:19:46.318
    Monitored Object: sys/chassis-1/psu-2/stats
    Suspect: No
    Input Current (A): 0.374000
    Input Power (W): 112.000000
    Input Voltage (V): 238.503006
    Psu Temp1 (C): 36.000000
    Psu Temp2 (C): 47.000000
    Psu Temp3 (C): 47.000000
    Fan Speed (RPM): 2240
    Thresholded: 0
CPU Env Stats:
    Time Collected: 2016-11-14T21:19:46.317
    Monitored Object: sys/chassis-1/blade-1/board/cpu-1/env-stats
    Suspect: No
    Temperature (C): 46.000000
    Thresholded: 0
```

```
Time Collected: 2016-11-14T21:19:46.317
Monitored Object: sys/chassis-1/blade-1/npu/cpu-1/env-stats
Suspect: No
Temperature (C): 38.000000
Thresholded: 0
```

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:
```

scope fabric a

Enters the eth-uplink interface mode. From this mode, you can view port channel, statistics, and interface information.
For example:

```
FPR2100 /eth-uplink/fabric # 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            State Reason
```

```
    -------------- ---------------- ------------------           -----------
      ----------------           ------------
    1               Port-channel1    Data               Disabled
 Link Down                       Down

FPR2100 /eth-uplink/fabric/port-channel # show stats
Ether Error Stats:
    Time Collected: 2016-11-14T21:27:16.386
    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:
    Time Collected: 2016-11-14T21:27:16.386
    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:
    Time Collected: 2016-11-14T21:27:16.386
    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:
    Time Collected: 2016-11-14T21:27:16.386
    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:
   Time Collected: 2016-11-14T21:27:16.386
    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
FPR2100 /eth-uplink/fabric/interface # show stats
Ether Error Stats:
    Time Collected: 2016-11-14T21:27:46.395
```

```
    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:
    Time Collected: 2016-11-14T21:27:46.395
    Monitored Object: sys/switch-A/slot-1/switch-ether/port-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): 7180
    Symbol (errors): 0
    SQE Test (errors): 0
    Thresholded: 0
Ether Pause Stats:
    Time Collected: 2016-11-14T21:27:46.395
    Monitored Object: sys/switch-A/slot-1/switch-ether/port-1/pause-stats
    Suspect: No
    Recv Pause (pause): 0
    Xmit Pause (pause): 0
    Resets (resets): 0
    Thresholded: 0
Ether Rx Stats:
    Time Collected: 2016-11-14T21:27:46.395
    Monitored Object: sys/switch-A/slot-1/switch-ether/port-1/rx-stats
    Suspect: No
    Total Packets (packets): 604527
    Unicast Packets (packets): 142906
    Multicast Packets (packets): 339031
    Broadcast Packets (packets): 122590
    Total Bytes (bytes): 59805045
    Jumbo Packets (packets): 0
    Thresholded: 0
Ether Tx Stats:
    Time Collected: 2016-11-14T21:27:46.395
    Monitored Object: sys/switch-A/slot-1/switch-ether/port-1/tx-stats
    Suspect: No
    Total Packets (packets): 145018
    Unicast Packets (packets): 145005
    Multicast Packets (packets): 0
    Broadcast Packets (packets): 13
    Total Bytes (bytes): 13442404
    Jumbo Packets (packets): 0
    Thresholded: 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.

```
firepower /firmware # show package  cisco-ftd-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-ftd-fp2k.6.2.0.175-314i.SSA             Scp      172.29.191.78
   0 danp            Downloaded
       cisco-ftd-fp2k.6.2.0.175-318i.SSA              Scp      172.29.191.78
   0 danp            Downloaded
        cisco-ftd-fp2k.6.2.0.175-319i.SSA             Scp      172.29.191.78
   0 danp            Downloaded
```

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
    Time stamp: 2016-11-15T19:42:29.854
    State: Failed
    Transfer Rate (KB/s): 0.000000
    Current Task: deleting downloadable test.SSA on
local(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:DeleteLocal)
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
        Timestamp: 2016-11-15T19:42:29.854
        Try: 2
        Progress (%): 0
        Current Task: deleting downloadable test.SSA on
local(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:DeleteLocal)

    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
    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-PWR-AC-400
    VID: V01
    Vendor: Cisco Systems, Inc
    Serial (SN): LIT2010CAFE
    Type: AC
    Fan Status: Ok
```

Connect Local-Mgmt Troubleshooting Commands for the Firepower 2100 in Platform Mode

Use the following connect local-mgmt mode FXOS CLI commands to troubleshoot issues with your Firepower 2100 in Platform mode. To access connect local-mgmt mode, enter:

FPR2100# **connect local-mgmt**

show lacp

Displays detailed information about EtherChannel LACP.
For example:

```
FPR2100(local-mgmt)# show lacp neighborFlags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group: 11

Partner (internal) information:

          Partner                Partner                       Partner
Port      System ID              Port Number     Age         Flags
Eth1/1    32768,286f.7fec.5980   0x10e           13 s        FA


          LACP Partner           Partner           Partner
          Port Priority        Oper Key        Port State
          32768                0x16            0x3f

          Port State Flags Decode:
```

```
          Activity:   Timeout:   Aggregation:   Synchronization:
          Active      Long       Yes            Yes

          Collecting:   Distributing:   Defaulted:   Expired:
          Yes           Yes             No          No

          Partner                Partner                      Partner
Port      System ID             Port Number     Age          Flags
Eth1/2    32768,286f.7fec.5980  0x10f           5  s         FA

          LACP Partner           Partner           Partner
          Port Priority        Oper Key        Port State
          32768                0x16            0x3f

          Port State Flags Decode:
          Activity:   Timeout:   Aggregation:   Synchronization:
          Active      Long       Yes            Yes

          Collecting:   Distributing:   Defaulted:   Expired:
          Yes           Yes             No          No


FP2100(local-mgmt)# show lacp counters

             LACPDUs         Marker      Marker Response    LACPDUs
Port       Sent   Recv     Sent   Recv    Sent    Recv      Pkts Err
--------------------------------------------------------------------------
Channel group: 11
Eth1/1     4435   3532     0      0        0      0         0
Eth1/2     4566   3532     0      0        0      0         0
```

show portchannel

Displays detailed information about EtherChannels.
For example:

```
FPR2100(local-mgmt)# show portchannel summary
Flags:  D - Down        P - Up in port-channel (members)
I - Individual  H - Hot-standby (LACP only)
s - Suspended   r - Module-removed
S - Switched    R - Routed
U - Up (port-channel)
M - Not in use. Min-links not met
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------------
11    Po11(U)     Eth      LACP      Eth1/1(P)    Eth1/2(P)
```

show portmanager

Displays detailed information about physical interfaces.
For example:

```
FPR2100(local-mgmt)# show portmanager counters ethernet 1 1
Good Octets Received                          : 105503260
Bad Octets Received                           : 0
MAC Transmit Error                            : 0
Good Packets Received                         : 1376050
Bad Packets Received                          : 0
BRDC Packets Received                         : 210
MC Packets Received                           : 1153664
```

```
Size 64                                          : 1334830
Size 65 to 127                                   : 0
Size 128 to 255                                  : 0
Size 256 to 511                                  : 41220
Size 512 to 1023                                 : 0
Size 1024 to Max                                 : 0
Good Octets Sent                                 : 0
Good Packets Sent                                : 0
Excessive Collision                              : 0
MC Packets Sent                                  : 0
BRDC Packets Sent                                : 0
Unrecognized MAC Received                        : 0
FC Sent                                          : 0
Good FC Received                                 : 0
Drop Events                                      : 0
Undersize Packets                                : 0
Fragments Packets                                : 0
Oversize Packets                                 : 0
Jabber Packets                                   : 0
MAC RX Error Packets Received                    : 0
Bad CRC                                          : 0
Collisions                                       : 0
Late Collision                                   : 0
bad FC Received                                  : 0
Good UC Packets Received                         : 222176
Good UC Packets Sent                             : 0
Multiple Packets Sent                            : 0
Deferred Packets Sent                            : 0
Size 1024 to 15180                               : 0
Size 1519 to Max                                 : 0
txqFilterDisc                                    : 0
linkChange                                       : 1
```

```
FPR2100(local-mgmt)# show portmanager port-info ethernet 1 1
port_info:
        if_index:    0x1081000
        type:        PORTMGR_IPC_MSG_PORT_TYPE_PHYSICAL
        mac_address: 2c:f8:9b:1e:8f:d6
        flowctl:     PORTMGR_IPC_MSG_FLOWCTL_NONE
        role:        PORTMGR_IPC_MSG_PORT_ROLE_NPU
        admin_state: PORTMGR_IPC_MSG_PORT_STATE_ENABLED
        oper_state:  PORTMGR_IPC_MSG_PORT_STATE_UP
        admin_speed: PORTMGR_IPC_MSG_SPEED_AUTO
        oper_speed:  PORTMGR_IPC_MSG_SPEED_1GB
        admin_mtu:   9216
        admin_duplex: PORTMGR_IPC_MSG_PORT_DUPLEX_AUTO
        oper_duplex: PORTMGR_IPC_MSG_PORT_DUPLEX_FULL
        pc_if_index: 0x0
        pc_membership_status: PORTMGR_IPC_MSG_MMBR_NOT_MEMBER
        pc_protocol: PORTMGR_IPC_MSG_PORT_CHANNEL_PRTCL_NONE
        native_vlan: 101
        num_allowed_vlan: 1
                allowed_vlan[0]: 101
        PHY Data:
        PAGE IFC OFFSET VALUE  | PAGE IFC OFFSET VALUE
        ---- --- ------ -----  | ---- --- ------ -----
         0    0  0x0000 0x1140 |  0    0  0x0001 0x796d
         0    0  0x0002 0x0141 |  0    0  0x0003 0x0ee1
         0    0  0x0004 0x03e3 |  0    0  0x0005 0xc1e1
         0    0  0x0006 0x000f |  0    0  0x0007 0x2001
         0    0  0x0008 0x4f08 |  0    0  0x0009 0x0f00
```

```
  0     0  0x000a 0x3800 |  0     0  0x000f 0x3000
  0     0  0x0010 0x3070 |  0     0  0x0011 0xac08
  0     0  0x0012 0x0000 |  0     0  0x0013 0x1c40
  0     0  0x0014 0x8020 |  0     0  0x0015 0x0000
 18     0  0x001b 0x0000 |
```

Item	Description
Good Octets Received	Number of ethernet frames received that are not bad ethernet frames
Bad Octets Received	Sum of lengths of all bad ethernet frames received
MAC Transmit Error	Number of frames not transmitted correctly or dropped due to internal MAC Tx error
Good Packets Received	The number of bad frames received
Bad Packets Received	The number of bad frames received
BRDC Packets Received	The number of good frames received that have a Broadcast destination MAC address
MC Packets Received	The number of good frames received that have a Multicast destination MAC address
Good Octets Sent	The sum of lengths of all Ethernet frames sent
Good Packets Sent	The number of good frames sent
Excessive Collision	The number of collision events seen by the MAC not including those counted in Single, Multiple, Excessive, or Late. This counter is applicable in half-duplex only
MC Packets Sent	The number of good frames send that have a Multicast destination MAC address
BRDC Packets Sent	The number of good frames send that have a Broadcast destination MAC address
Unrecognized MAC Received	Number of received MAC Control frames that are not Flow control frames.
FC sent	Number of Flow Control frames sent.
Good FC Received	Number of good IEEE 802.3x Flow Control packets received.
Drop Events	Number of packets dropped
Undersize Packets	Number of undersize packets received
Fragments Packets	Number of fragments received.
Oversize Packets	Number of oversize packets received

Item	Description
Jabber Packets	Number of jabber packets received
MAC RX Error Packets Received	Number of Rx Error events seen by the receive side of the MAC
Bad CRC	Number of packets received with bad CRC
Collisions	Number of late collisions seen by the MAC
Late collison	Total number of late collisions seen by the MAC
Bad FC Received	Number of bad IEEE 802.3x Flow Control packets received
Good UC Packets Received	Number of Ethernet Unicast frames received
Good UC Packets Sent	Number of Ethernet Unicast frames sent
Multiple Packets Sent	Valid Frame transmitted on half-duplex link that encountered more then one collision. Byte count and cast are valid.
Deferred Packets Sent	Valid frame transmitted on half-duplex link with no collisions, but where the frame transmission was delayed due to media being busy. Byte count and cast are valid.
Size 1024 to 15180	The number of received and transmitted, good and bad frames that are 1024 to 1518 bytes in size
Size 1519 to Max	The number of received and transmitted, good and bad frames that are more than 1519 bytes in size
txqFilterDisc	Number of IN packets that were filtered due to TxQ
linkChange	number of link up or link down changes for the port

```
FPR2100(local-mgmt)# show portmanager switch mac-filters
port ix          MAC               mask        action      packets       bytes

00   0ba  2C:F8:9B:1E:8F:D7  FF:FF:FF:FF:FF:FF  FORWARD
     0c9  01:80:C2:00:00:02  FF:FF:FF:FF:FF:FF  FORWARD
     0cc  2C:F8:9B:1E:8F:F7  FF:FF:FF:FF:FF:FF  FORWARD
     0cf  FF:FF:FF:FF:FF:FF  FF:FF:FF:FF:FF:FF  FORWARD
     b70  00:00:00:00:00:00  01:00:00:00:00:00  DROP         222201    14220864
     bb8  01:00:00:00:00:00  01:00:00:00:00:00  DROP        1153821    91334968

01   0bd  2C:F8:9B:1E:8F:D6  FF:FF:FF:FF:FF:FF  FORWARD
     0c0  01:80:C2:00:00:02  FF:FF:FF:FF:FF:FF  FORWARD
     0c3  2C:F8:9B:1E:8F:F6  FF:FF:FF:FF:FF:FF  FORWARD
     0c6  FF:FF:FF:FF:FF:FF  FF:FF:FF:FF:FF:FF  FORWARD         210       13440
     b73  00:00:00:00:00:00  01:00:00:00:00:00  DROP         222201    14220864
     bbb  01:00:00:00:00:00  01:00:00:00:00:00  DROP        1153795    91281055
<...>
```

```
FPR2100(local-mgmt)# show portmanager switch status
Dev/Port         Mode        Link   Speed  Duplex  Loopback Mode
---------  ----------------  -----  -----  ------  -------------

0/0             QSGMII        Up     1G     Full    None
0/1             QSGMII        Up     1G     Full    None
0/2             QSGMII       Down    1G     Half    None
0/3             QSGMII       Down    1G     Half    None
0/4             QSGMII       Down    1G     Half    None
0/5             QSGMII       Down    1G     Half    None
0/6             QSGMII        Up     1G     Full    None
0/7             QSGMII       Down    1G     Half    None
0/48            QSGMII       Down    1G     Half    None
0/49            QSGMII       Down    1G     Half    None
0/50            QSGMII       Down    1G     Half    None
0/51            QSGMII       Down    1G     Half    None
0/52              KR          Up     40G    Full    None
0/56            SR_LR        Down    10G    Full    None
0/57            SR_LR        Down    10G    Full    None
0/58            SR_LR        Down    10G    Full    None
0/59            SR_LR        Down    10G    Full    None
0/64            SR_LR        Down    10G    Full    None
0/65            SR_LR        Down    10G    Full    None
0/66            SR_LR        Down    10G    Full    None
0/67            SR_LR        Down    10G    Full    None
0/68            SR_LR        Down    10G    Full    None
0/69            SR_LR        Down    10G    Full    None
0/70            SR_LR        Down    10G    Full    None
0/71            SR_LR        Down    10G    Full    None
0/80              KR          Up     10G    Full    None
0/81              KR         Down    10G    Full    None
0/83              KR          Up     10G    Full    None
```

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
Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Defa
ult App
    ---------- ---------- ----------- ---------- ----------- ----------- -------
-------
    ftd        6.2.0.131  N/A         cisco      Native      Application No
    ftd        6.2.0.140  N/A         cisco      Native      Application No
    ftd        6.2.0.175  N/A         cisco      Native      Application Yes
```

showapp-instance

Displays information about the verified app-instance status

```
    firepower-2120 /ssa # show app-instance
Application Name     Slot ID    Admin State     Operational State    Running Version Startup
 Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
```

```
-------------- ------------------
asa                  1          Enabled         Online               9.14.2          9.14.2
         Not Applicable
```

showfault

Displays information about the fault message

```
firepower-2120 /ssa # show fault
Severity  Code     Last Transition Time     ID       Description
--------- -------- ----------------------- -------- -----------
Cleared   F16589   2021-10-11T21:58:53.200    25140 [FSM:STAGE:RETRY:]: Waiting for chassis
 object ready(FSM-STAGE:sam:dme:SmSecSvcAutoDeployCSP:WaitForChassisM
oReady)
```

show failsafe-params

The fail-safe mode for an FTD application on Firepower 1000/2100 is activated due to continuous boot loop, traceback, etc. The following parameters control the activation of the fail-safe mode:

- Max Restart—maximum number of times that an application should restart in order to activate the fail-safe mode.
- Current Reboot Count—number of times the application continuously restarted.
- Restart Time Interval (secs)—the amount of time in seconds, during which the Max Restart counter should be reached in order to trigger the fail-safe mode. If the application restarts 'Max Restart' or more times within this interval, the fail-safe mode is enabled.

For example:

```
firepower-2120-failed(local-mgmt)# show failsafe-params
Max Restart: 8
Current Reboot Count: 0
Restart Time Interval(secs): 3600
```

When the system is in the fail-safe mode:

- The system name is appended with the "-failed" string:

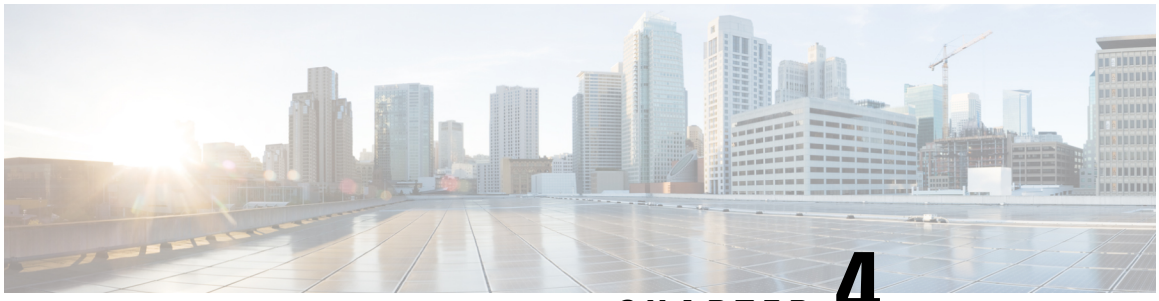
  ```
  firepower-2120-failed /ssa #
  ```

- The output of the "show failsafe-params" command in the local-mgmt command shell contains a warning message:

  ```
  firepower-2120-failed(local-mgmt)# show failsafe-params
  Max Restart: 1
  Current Reboot Count: 1
  Restart Time Interval(secs): 3600
  WARNING: System in Failsafe mode. Applications are not running!
  ```

- Operation State of the application is Offline:

  ```
  firepower-2120-failed /ssa # show app-instance
  Application Name     Slot ID    Admin State     Operational State    Running Version
  Startup Version Cluster Oper State   Cluster Role
  -------------------- ---------- --------------- -------------------- ---------------
  ---------------- -------------------- ------------
  asa                  1          Enabled         Offline <=====       9.16.2.3
  9.16.2.3        Not Applicable       None
  ```



CHAPTER 4

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 FTD 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 26.
- Perform a factory reset from ROMMON (admin password recovery)—All configurations are removed, and FTD 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 28.
- Reimage the system with a new version—All configurations are removed, and FTD 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 29.

Note You cannot perform a downgrade to the previous major version using this procedure. You must use the Perform a Complete Reimage, on page 36 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 31.
- 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 31.
- 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 FTD software, and reconfigure the entire system. See Perform a Complete Reimage, on page 36.
- Change the admin password—This procedure lets you change the admin password from the FTD CLI. See Change the Admin Password, on page 39.
- Change the admin password if FTD is offline—This procedure lets you change the admin password from FXOS. See Change the Admin Password if FTD is Offline, on page 40. Note that if FTD is online, you must change the admin password using the FTD 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 FTD.

If your current running version is an upgrade-only image, you will have to re-upgrade your FTD after performing this procedure. For example, Firepower 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 (Firepower 6.2.1.x) will be reinstalled, and you will need to re-upgrade to Firepower 6.2.2.x using Firepower Management Center or Firepower 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 36 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 device via serial console, you will automatically connect to the FXOS CLI context. If you are in the FTD 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 FTD 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 41.

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 Firepower 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 FTD 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 26.

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-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
```

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 36 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 device via serial console, you will automatically connect to the FXOS CLI context. If you are in the FTD 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 41.

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

You can also use FTP, SCP, SFTP, or TFTP to copy the Firepower 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*

For example:

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

firepower /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:

firepower /firmware # **show package**

Example:

```
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.

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*

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 FTD 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 FTD configuration.

This procedure does not apply to the Firepower 1000, which does 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.

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/FTD version mismatch will cause the FTD to crash. In 6.5 and later, booting FXOS from ROMMON prevents FTD from loading automatically.

If you want to boot from 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 TFTP:

Set the network settings for Management 1/1, and load the FTD 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:

```
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 >
```

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 28). 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
```

Step 5 Re-download and boot the FTD 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 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-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
```

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 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.
```

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-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.
...
```

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**.

Before you begin

- Deregister your devices from the cloud tenant (if applicable). See Deregister From Cloud, on page 41.
- Verify that you are in the FXOS CLI context. If you connect to the Firepower 1000/2100 device via serial console, you will automatically connect to the FXOS CLI context. If you are in the FTD CLI context, you must first switch to the FXOS CLI context with the **connect fxos** command.

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** *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:

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

For example:

```
firepower /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 11 Once the download task is complete, the **download-task** command output displays the State as Downloaded:

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

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
```

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 in step 12, above:

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

After the software package installation is complete, the system reboots while installing Firepower Threat Defense.

What to do next

Complete the setup tasks in the getting started guide.

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 FTD CLI procedure to change the admin password to a new string.

Procedure

Step 1 Connect to the FTD 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 FTD 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 FTD is offline or otherwise unavailable. Note that if FTD is online, you will need to change the admin password using the FTD CLI (see Change the Admin Password, on page 39).

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

Before you begin

- Verify that you are in the FXOS CLI context. If you connect to the Firepower 1000/2100 device via serial console, you will automatically connect to the FXOS CLI context. If you are in the FTD 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 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 device.

If you do not have access to the cloud account, use the following procedure to deregister your Firepower 1000/2100 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 device via serial console, you will automatically connect to the FXOS CLI context. If you are in the FTD 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 FXOS Troubleshooting

Feature Name	Platform Releases	Description
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.