



Cisco FXOS Troubleshooting Guide for 1000/1200/2100/3100/4200 with Threat Defense

First Published: 2017-05-15

Last Modified: 2025-05-13

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2025 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1	About the Firepower 1000/2100, Secure Firewall 1200/3100/4200 Security Appliance CLI	1
	FXOS CLI Hierarchy	1
	Online Help for the CLI	3

CHAPTER 2	Global FXOS CLI Commands	5
	Global FXOS CLI Commands	5

CHAPTER 3	FXOS CLI Troubleshooting Commands	7
	FXOS CLI Chassis Mode Troubleshooting Commands	7
	FXOS CLI Eth-Uplink Mode Troubleshooting Commands	12
	FXOS CLI Fabric Interconnect Mode Troubleshooting Commands	15
	Connect Local-Mgmt Troubleshooting Commands for the Secure Firewall 3100	18
	Connect Local-Mgmt Troubleshooting Commands for the Secure Firewall 4200 in Appliance Mode	30
	FXOS CLI Security Services Mode Troubleshooting Commands	39
	Secure Firewall 1200/3100/4200 CLI Monitoring Mode Troubleshooting Commands	40
	Packet Capture for Secure Firewall 3100/4200	41
	Guidelines and Limitations for Packet Capture	41
	Creating or Editing a Packet Capture Session	42
	Deleting Packet Capture Sessions	45

CHAPTER 4	Image Management	47
	About Disaster Recovery	47
	Reimage the System with the Base Install Software Version	48
	Perform a Factory Reset from ROMMON (Password Reset)	50
	Reimage the System with a New Software Version	52
	Download a Package for Multi-Instance Mode	55

Reformat the SSD File System (Firepower 2100) 56

Boot from ROMMON 57

Perform a Complete Reimage 64

Change the Admin Password 68

Change the Admin Password if Threat Defense is Offline 69

Deregister From Cloud 70

History for FXOS Troubleshooting 71



CHAPTER

1

About the Firepower 1000/2100, Secure Firewall 1200/3100/4200 Security Appliance CLI

This troubleshooting guide explains the Firepower eXtensible Operating System (FXOS) command line interface (CLI) for the Firepower 1000 , Firepower 2100, Secure Firewall 1200, Secure Firewall 3100, and Secure Firewall 4200 security appliance series.



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

The CLI on the Firepower 1000/2100, Secure Firewall 1200, Secure Firewall 3100, or Secure Firewall 4200 console port defaults to the FXOS CLI prompt. You can get to the 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, Firepower 2100, Secure Firewall 1200, Secure Firewall 3100, or Secure Firewall 4200 series device.

If threat defense is installed on your Firepower 1000/2100, Secure Firewall 1200, Secure Firewall 3100 device, or Secure Firewall 4200, 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 threat defense CLI, see the [Command Reference for threat defense](#).

- [FXOS CLI Hierarchy, on page 1](#)
- [Online Help for the CLI, on page 3](#)

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.

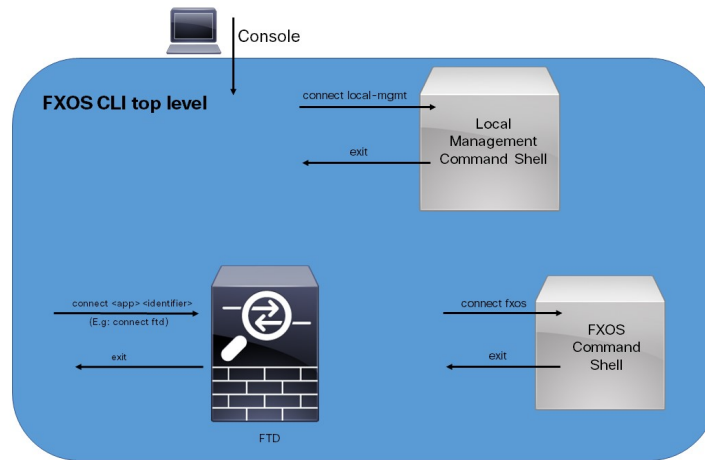
The following table lists the main command modes, the commands used to access each mode, and the CLI prompt associated with each mode.

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 and Secure Firewall 3100 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, on page 5](#)

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: <pre>acknowledge fault 1</pre> Where <i>id</i> 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: <pre>connect ftd</pre>

Command	Description
connect fxos [admin]	<p>The [admin] keyword allows connecting to the FXOS in privileged mode, where users can run additional commands.</p> <p>For example, to generate the Firepower eXtensible Operating System (FXOS) show-tech file:</p> <pre> firewall# connect fxos admin Configuring session. . Connecting to FXOS. 1 firepower-3140# connect local-mgmt Warning: network service is not available when entering 'connect local-mgmt' firepower-3140(local-mgmt)# show tech-support fprm <CR> > Redirect it to a file >> Redirect it to a file in append mode brief Brief detail Detail Pipe command output to filter </pre> </pre>
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.
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, on page 7](#)
- [FXOS CLI Eth-Uplink Mode Troubleshooting Commands, on page 12](#)
- [FXOS CLI Fabric Interconnect Mode Troubleshooting Commands, on page 15](#)
- [Connect Local-Mgmt Troubleshooting Commands for the Secure Firewall 3100, on page 18](#)
- [Connect Local-Mgmt Troubleshooting Commands for the Secure Firewall 4200 in Appliance Mode, on page 30](#)
- [FXOS CLI Security Services Mode Troubleshooting Commands, on page 39](#)
- [Secure Firewall 1200/3100/4200 CLI Monitoring Mode Troubleshooting Commands, on page 40](#)
- [Packet Capture for Secure Firewall 3100/4200, on page 41](#)

FXOS CLI Chassis Mode Troubleshooting Commands

Use the following chassis mode FXOS CLI commands to troubleshoot issues with your 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

```



Note When you remove dual fan module for Secure Firewall 3100 devices, to view the actual status of the fan, use the **show environment basic** and **show environment expand** commands.

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, 2120, Secure Firewall 3100, and Secure Firewall 4200 devices.

scope fan-module

Enters the fan mode on Firepower 2130, 2140, Secure Firewall 3100, and Secure Firewall 4200 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, Secure Firewall 3100, and 4200 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 statistics. 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/npucpu-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 system.

show detail

Displays detailed information about your Firepower 1000/2100, Secure Firewall 3100, or Secure Firewall 4200 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
    
```

FXR2100 /eth-uplink/fabric # show port-channel

Port Channel:

State	Port Channel Id	Name	Port Type	Admin State	Oper
Link Down	1	Port-channel1	Data	Disabled	Down

FXR2100 /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 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 card

Displays information on a fabric card details. This command can be used to display the network module details.

For example:

```
# firepower-4225 /fabric-interconnect # show card detail expand

Fabric Card:
  Id: 2
  Description: 2-port 100 Gigabit Ethernet Expansion Module
  Number of Ports: 2
  Admin State: Enabled
  State: Online
  Vendor: Cisco Systems, Inc.
  Model: FPR-X-NM-2X100G
  Serial (SN): FJZ26390V7D
  Perf: N/A
  Operability: Operable
  Overall Status: Online
  Power State: Online
  Presence: Equipped
  Thermal Status: N/A
  Voltage Status: N/A
  Current Task:
```

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 inventory expand

Displays all fabric card details. This command can be used to display the network module details.

```

firepower-4225 /fabric-interconnect # show inventory expand
A:

```

Fabric Card:

Slot	Description	Num Ports	State	PID	Serial (SN)
0	Logical Slot for Management Interface	2	N/A	FPR-4225	FJZ26345ZGZ
1	Cisco FPR 4225 Base Module	8	On	FPR-4225	FJZ26345ZGZ
3	4-port 200 Gigabit Ethernet Expansion Module	4	Online	FPR-X-NM-4X200G	FJZ25430132

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
  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 Secure Firewall 3100

In addition to the existing debugging commands, CLIs specific to Secure Firewall 3100 are explained in this section below.

Use the following connect local-mgmt mode FXOS CLI commands to troubleshoot issues with your Secure Firewall 3100. To access connect local-mgmt mode, enter:

```
FPR3100# connect local-mgmt
```

show portmanager

Displays detailed information about switched, packets, SFP-FEC counters, digital optical monitoring, QOS functionality, CPSS AP, and Cyclic log dumps.

For example:

The following CLI displays the FXOS port manager switch hardware TCAM rules dump in vtcam-tti:

```

firepower-3140(local-mgmt)# show portmanager switch forward-rules hardware vtcam-tti
detail
VTCAM_RULE_ID  VLAN  SRC_PORT  PORTCHANNEL_ID  FLAGS  MODE  REF_COUNT
1              21     0         2                0      2     5         3
2              3078   0         0                0      0     0         1
3              3077   0         0                0      0     0         1
4              3076   0         0                0      0     0         1
5              3075   0         0                0      0     0         1
6              3074   0         0                0      0     0         1
7              3073   0         0                0      0     0         1
8              1       0         0                0      0     0         1
9              18     102        0                0      24    8         1
10             5       157        0                0      24    8         1
11             31      0         12               0      2     5         3
12             15     105        0                0      24    8         1
13             9       111        0                0      24    8         1
14             13     107        0                0      24    8         1
15             26      0         7                0      2     5         3
16             29      0         10               0      2     5         3
17             23      0         4                0      2     5         3
18             19     101        0                0      24    8         1
19             30      0         11               0      2     5         3

```

20	28	0	9	0	2	5	3
21	4	156	0	0	24	8	1
22	34	0	15	0	2	5	3
23	6	158	0	0	24	8	1
24	8	112	0	0	24	8	1
25	24	0	5	0	2	5	3
26	14	106	0	0	24	8	1
27	32	0	13	0	2	5	3
28	25	0	6	0	2	5	3
29	12	0	0	9	6	5	2
30	20	0	1	0	2	5	3
31	11	109	0	0	24	8	1
32	27	0	8	0	2	5	3
33	17	103	0	0	24	8	1
34	22	0	3	0	2	5	3
35	16	104	0	0	24	8	1
36	3	0	19	0	26	8	1
37	35	0	16	0	2	5	3
38	33	0	14	0	2	5	3
39	7	159	0	0	24	8	1
40	2	0	17	0	26	8	1
41	10	110	0	0	24	8	1

The following CLI displays the FXOS port manager switch VLANs output:

```
firepower-3140(local-mgmt)# show portmanager switch vlans
VLAN          Ports          Tag          MAC-Learning
FDB-mode
-----
1             0/17,19       pop_outer_tag Control
FID
2             0/1-16,18    outer_tag0_inner_tag1 Control
FID
              0/20         pop_outer_tag
3             0/1-16,18    outer_tag0_inner_tag1 Control
FID
4             0/1-16,18    outer_tag0_inner_tag1 Control
FID
5             0/1-16,18    outer_tag0_inner_tag1 Control
FID
6             0/1-16,18    outer_tag0_inner_tag1 Control
FID
7             0/1-16,18    outer_tag0_inner_tag1 Control
FID
8             0/1-16,18    outer_tag0_inner_tag1 Control
FID
```

The following CLI helps you to to check port-channel interface summary:

```
firepower-3140(local-mgmt)# show por
portchannel portmanager

firepower-3140(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
-----
3   Po3 (U)      Eth       LACP      Eth1/3 (P)
2   Po2 (U)      Eth       LACP      Eth1/2 (P)

LACP KeepAlive Timer:
-----
Channel  PeerKeepAliveTimerFast
-----
3   Po3 (U)      False
2   Po2 (U)      False

Cluster LACP Status:
-----
Channel  ClusterSpanned  ClusterDetach  ClusterUnitID  ClusterSysID
-----
3   Po3 (U)      False          False           0
2   Po2 (U)      False          False           0

```

The following CLI displays the port-channel load-balancing method:

```

firepower-3140(local-mgmt)# show portchannel load-balance
PortChannel Load-Balancing Configuration:
    src-dst ip-l4port
PortChannel Load-Balancing Configuration Used Per-Protocol:
Non-IP: src-dst mac
    IP: src-dst ip-l4port

```

The following CLI displays the status of FXOS system processes:

```

firepower-3140(local-mgmt)# show pmon state

SERVICE NAME          STATE      RETRY (MAX)  EXITCODE    SIGNAL     CORE
-----
svc_sam_dme            running    0 (4)        0           0         no
svc_sam_dcosAG        running    0 (4)        0           0         no
svc_sam_portAG        running    0 (4)        0           0         no
svc_sam_statsAG       running    0 (4)        0           0         no
httpd.sh              running    0 (4)        0           0         no
svc_sam_sessionmgrAG  running    0 (4)        0           0         no
sam_core_mon          running    0 (4)        0           0         no
svc_sam_svcmonAG      running    0 (4)        0           0         no
svc_sam_serviceOrchAG running    0 (4)        0           0         no
svc_sam_appAG         running    0 (4)        0           0         no
svc_sam_envAG         running    0 (4)        0           0         no
svc_sam_npuAG         running    0 (4)        0           0         no
svc_sam_eventAG       running    0 (4)        0           0         no

```

The following CLI displays switch hardware TCAM rules dump in vcam-tti stage matching ethernet 1/1 port:

```

firepower-3140(local-mgmt)# show portmanager switch forward-rules hardware vcam-tti
ethernet 1 1
RULE_ID  VLAN  SRC_PORT  PC_ID  SRC_ID  MODE  PAK_CNT
1        20    0 1       0      101   0      151

```

The following CLI displays switch hardware TCAM rules dump in vcam-tti stage matching vlan 0:

```

firepower-3140(local-mgmt)# show portmanager switch forward-rules hardware vcam-tti
vlan 0
RULE_ID  VLAN  SRC_PORT  PC_ID  SRC_ID  MODE  PAK_CNT

```

1	2	0	17	0	17	0	1709
2	3	0	19	0	19	0	1626
3	4	0	16	0	0	0	0
4	5	0	15	0	0	0	0
5	6	0	14	0	0	0	0
6	7	0	13	0	0	0	0
7	8	0	12	0	0	0	0
8	9	0	11	0	0	0	0
9	10	0	10	0	0	0	0
10	11	0	9	0	0	0	0
11	12	0	8	0	0	0	0
12	13	0	7	0	0	0	0
13	14	0	6	0	0	0	0
14	15	0	5	0	0	0	0
15	16	0	4	0	0	0	0
16	17	0	3	0	0	0	0
17	18	0	2	0	0	0	0
18	19	0	1	0	0	0	0
19	20	0	1	0	101	0	166
20	21	0	2	0	102	0	1597
21	22	0	3	0	103	0	0
22	23	0	4	0	104	0	0
23	24	0	5	0	105	0	0
24	25	0	6	0	106	0	0
25	26	0	7	0	107	0	0
26	27	0	8	0	108	0	0
27	28	0	9	0	109	0	0
28	29	0	10	0	110	0	0
29	30	0	11	0	111	0	0
30	31	0	12	0	112	0	0
31	32	0	13	0	159	0	0
32	33	0	14	0	158	0	0
33	34	0	15	0	157	0	0
34	35	0	16	0	156	0	0
35	1	0	17	0	0	0	0

The following CLI displays detailed information about hardware MAC-filter / EM stage rules:

```
firepower-3140(local-mgmt)# show portmanager switch forward-rules hardware mac-filter
detail
```

```
EM Entry-No : 1
```

```

VLAN          : 0
SRC_PORT      : 17
PC_ID         : 0
SRC_ID        : 17
DST_PORT      : 19
HW_ID         : 3072
ACT_CMD       : 0
PCL_ID        : 1
REDIRECT_CMD  : 1
BYPASS_BRG    : 1
CND_INDEX     : 3074
PACKET_COUNT  : 1977
DMAC          : 00:00:00:00:00:00
```

```
EM Entry-No : 2
```

```

VLAN          : 0
SRC_PORT      : 19
PC_ID         : 0
SRC_ID        : 19
```

```

DST_PORT      : 17
HW_ID         : 3074
ACT_CMD       : 0
PCL_ID        : 1
REDIRECT_CMD  : 1
BYPASS_BRG    : 1
CND_INDEX     : 3075
PACKET_COUNT  : 1858
DMAC          : 00:00:00:00:00:00

```

The following CLI displays switch hardware TCAM rules dump in mac-filter stage matching ethernet 1/9 port:

```

firepower-3140(local-mgmt)# show portmanager switch forward-rules hardware mac-filter
ethernet 1 9
VLAN  SRC_PORT  PC_ID  SRC_ID  DST_PORT  PKT_CNT  DMAC
1      0           9      0      109      1536     0 1:80:c2:0:0:2

```

The following CLI displays detailed information about software MAC-filter:

```

firepower-3140(local-mgmt)# show portmanager switch forward-rules software mac-filter
detail
VLAN  SRC_PORT  PORTCHANNEL_ID  DST_PORT  FLAGS  MODE  DMAC
1     0        17              0         19     26    8 0:0:0:0:0:0
2     0        9               0         1536   2     5 1:80:c2:0:0:2
3     104      0               0         4      24    8 0:0:0:0:0:0
4     0        7               0         1536   2     5 1:80:c2:0:0:2
5     101     0               0         1      24    8 0:0:0:0:0:0
6     0        1               0         1536   2     5 1:80:c2:0:0:2
7     0        3               0         1536   2     5 1:80:c2:0:0:2
8     106     0               0         6      24    8 0:0:0:0:0:0
9     158     0               0         14     24    8 0:0:0:0:0:0
10    0        13              0         1536   2     5 1:80:c2:0:0:2
11    0        14              0         1536   2     5 1:80:c2:0:0:2
12    0        6               0         1536   2     5 1:80:c2:0:0:2
13    0        8               0         1536   2     5 1:80:c2:0:0:2
14    112     0               0         12     24    8 0:0:0:0:0:0
15    107     0               0         7      24    8 0:0:0:0:0:0
16    0        19              0         17     26    8 0:0:0:0:0:0
17    0        12              0         1536   2     5 1:80:c2:0:0:2
18    0        5               0         1536   2     5 1:80:c2:0:0:2
19    102     0               0         2      24    8 0:0:0:0:0:0
20    156     0               0         16     24    8 0:0:0:0:0:0
21    103     0               0         3      24    8 0:0:0:0:0:0
22    0        11              0         1536   2     5 1:80:c2:0:0:2
23    157     0               0         15     24    8 0:0:0:0:0:0
24    111     0               0         11     24    8 0:0:0:0:0:0
25    0        10              0         1536   2     5 1:80:c2:0:0:2
26    108     0               0         8      24    8 0:0:0:0:0:0
27    159     0               0         13     24    8 0:0:0:0:0:0
28    110     0               0         10     24    8 0:0:0:0:0:0
29    105     0               0         5      24    8 0:0:0:0:0:0
30    0        2               0         1536   2     5 1:80:c2:0:0:2
31    0        4               0         1536   2     5 1:80:c2:0:0:2
32    0        16              0         1536   2     5 1:80:c2:0:0:2
33    109     0               0         9      24    8 0:0:0:0:0:0
34    0        15              0         1536   2     5 1:80:c2:0:0:2

```

The following CLI displays switch software DB rules in mac-filter stage matching ethernet1/9 port:

```

firepower-3140(local-mgmt)# show portmanager switch forward-rules software mac-filter
ethernet 1 9

```

VLAN	SRC_PORT	PORTCHANNEL_ID	DST_PORT	FLAGS	MODE	DMAC
1	0	9	0	1536	2	5 1:80:c2:0:0:2

The following CLI displays detailed information about switch bridge engine packet drops:

```
firepower-3140(local-mgmt)# show portmanager switch counters bridge
Bridge Ingress Drop Counter: 2148
No Bridge Ingress Drop
```

The following CLI displays details on hardware switch packet counters:

```
firepower-3140(local-mgmt)# show portmanager switch counters packet-trace
```

Counter	Description
goodOctetsRcv	Number of ethernet frames received that are not bad ethernet frames or MAC Control pkts
badOctetsRcv	Sum of lengths of all bad ethernet frames received
gtBrgInFrames	Number of packets received
gtBrgVlanIngFilterDisc	Number of packets discarded due to VLAN Ingress Filtering
gtBrgSecFilterDisc	Number of packets discarded due to Security Filtering measures
gtBrgLocalPropDisc	Number of packets discarded due to reasons other than VLAN ingress and Security filtering
dropCounter	Ingress Drop Counter
outUcFrames	Number of unicast packets transmitted
outMcFrames	Number of multicast packets transmitted. This includes registered multicasts, unregistered multicasts and unknown unicast packets
outBcFrames	Number of broadcast packets transmitted
brgEgrFilterDisc	Number of IN packets that were Bridge Egress filtered
txqFilterDisc	Number of IN packets that were filtered due to TxQ congestion
outCtrlFrames	Number of out control packets (to cpu, from cpu and to analyzer)
egrFrwDropFrames	Number of packets dropped due to egress forwarding restrictions
goodOctetsSent	Sum of lengths of all good ethernet frames sent from this MAC

Counter	Source port- 0/0	Destination port- 0/0
goodOctetsRcv	---	---
badOctetsRcv	---	---
Ingress counters		
gtBrgInFrames	6650	6650
gtBrgVlanIngFilterDisc	0	0
gtBrgSecFilterDisc	0	0
gtBrgLocalPropDisc	0	0
dropCounter	2163	Only for source-port
Egress counters		
outUcFrames	0	0
outMcFrames	2524	2524
outBcFrames	1949	1949
brgEgrFilterDisc	14	14
txqFilterDisc	0	0
outCtrlFrames	0	0
egrFrwDropFrames	0	0
goodOctetsSent	---	---

The following CLI displays detailed informatin about the switch traffic for CPU:

```
firepower-3140(local-mgmt)# show portmanager switch traffic cpu
```

```

Dev/RX queue  packets  bytes
-----
0/0           0         0
0/1           0         0
0/2           0         0
0/3           0         0
0/4           0         0
0/5           0         0
0/6           0         0
0/7           0         0      #

```

The following CLI displays details on hardware switch port traffic:

```
firepower-3140(local-mgmt)# show portmanager switch traffic port
```

```

max-rate - pps that the port allow with packet size=64
actual-tx-rate - pps that egress the port (+ % from 'max')
actual-rx-rate - pps that ingress the port(+ % from 'max')

```

```

Dev/Port  max-rate  actual-tx-rate  actual-rx-rate
-----
0/1       1488095  (0%) ---        (0%) ---
0/2       1488095  (0%) ---        (0%) ---
0/3       14880    (0%) ---        (0%) ---
0/4       14880    (0%) ---        (0%) ---
0/5       14880    (0%) ---        (0%) ---
0/6       14880    (0%) ---        (0%) ---
0/7       14880    (0%) ---        (0%) ---
0/8       14880    (0%) ---        (0%) ---
0/9       14880952 (0%) ---        (0%) ---
0/10      14880952 (0%) ---        (0%) ---
0/11      14880952 (0%) ---        (0%) ---
0/12      14880952 (0%) ---        (0%) ---
0/13      14880952 (0%) ---        (0%) ---
0/14      14880952 (0%) ---        (0%) ---
0/15      1488095  (0%) ---        (0%) ---
0/16      1488095  (0%) ---        (0%) ---
0/17      14880952 (0%) ---        (0%) ---
0/18      74404761 (0%) ---        (0%) ---
0/19      37202380 (0%) ---        (0%) ---
0/20      37202380 (0%) ---        (0%) ---

```

The following CLI displays detailed information about SFP-FEC Counters matching ethernet 1/13 port:

```

firepower-3140(local-mgmt)# show portmanager counters ethernet 1 13
  Good Octets Received           : 2153
  Bad Octets Received           : 0
  MAC Transmit Error            : 0
  Good Packets Received         : 13
  Bad packets Received          : 0
  BRDC Packets Received        : 0
  MC Packets Received           : 13
  .....
  .....
  txqFilterDisc                 : 0
  linkchange                     : 1
  FcFecRxBlocks                 : 217038081
  FcFecRxBlocksNoError          : 217038114
  FcFecRxBlocksCorrectedError   : 0
  FcFecRxBlocksUnCorrectedError : 0

```

```

FcFecRxBlocksCorrectedErrorBits           : 0
FcFecRxBlocksCorrectedError0              : 0
FcFecRxBlocksCorrectedError1              : 0
FcFecRxBlocksCorrectedError2              : 0
FcFecRxBlocksCorrectedError3              : 0
FcFecRxBlocksUnCorrectedError0            : 0
FcFecRxBlocksUnCorrectedError1            : 0
FcFecRxBlocksUnCorrectedError2            : 0
FcFecRxBlocksUnCorrectedError3            : 0
    
```

The following CLI displays detailed information about SFP-FEC Counters matching ethernet 1/14 port:

```

firepower-3140(local-mgmt)# show portmanager counters ethernet 1 14
  Good Octets Received           : 2153
  Bad Octets Received            : 0
  MAC Transmit Error             : 0
  Good Packets Received          : 13
  Bad packets Received           : 0
  BRDC Packets Received          : 0
  MC Packets Received            : 13
  .....
  .....
  txqFilterDisc                  : 0
  linkchange                      : 1
  RsFeccorrectedFecCodeword      : 0
  RsFecuncorrectedFecCodeword    : 10
  RsFecsymbolError0              : 5
  RsFecsymbolError1              : 0
  RsFecsymbolError2              : 0
  RsFecsymbolError3              : 0
    
```

The following CLI displays detailed information on the Digital Optical Monitoring information matching ethernet 1/5 port:

```

firepower-4245(local-mgmt)# show portmanager port-info ethernet 1 5
  ....
  ....
  DOM info:
  =====:

  Status/Control Register: 0800
  RX_LOS State: 0
  TX_FAULT State: 0
  Alarm Status: 0000
  No active alarms
  Warning Status: 0000
  No active warnings
    
```

THRESHOLDS		high alarm	high warning	low warning	low alarm
Temperature	C	+075.000	+070.000	+000.000	-05.000
Voltage	V	003.6300	003.4650	003.1350	002.9700
Bias Current	mA	012.0000	011.5000	002.0000	001.0000
Transmit power	mW	034.6740	017.3780	002.5120	001.0000
Receive power	mW	034.6740	017.3780	001.3490	000.5370

```

Environmental Information - raw values
Temperature: 38.84 C
Supply voltage: 33703 in units of 100uVolt
Tx bias: 3499 in units of 2uAmp
Tx power: 0.1 dBm (10251 in units of 0.1 uW)
Rx power: -0.9 dBm (8153 in units of 0.1 uW)
DOM (256 bytes of raw data in hex)
=====
0x0000 : 4b 00 fb 00 46 00 00 00 8d cc 74 04 87 5a 7a 76
0x0010 : 17 70 01 f4 16 76 03 e8 87 72 03 e8 43 e2 09 d0
0x0020 : 87 72 02 19 43 e2 05 45 00 00 00 00 00 00 00 00
0x0030 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0040 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0050 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 86
0x0060 : 26 54 83 a7 0d ab 28 0b 1f d9 00 00 00 00 00 08
0x0070 : 00 00 03 00 00 00 00 00 08 f3 00 00 00 00 00 01
0x0080 : 49 4e 55 49 41 43 53 45 41 41 31 30 2d 33 33 38
0x0090 : 38 2d 30 31 56 30 31 20 01 00 46 00 00 00 00 e3
0x00a0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x00b0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x00c0 : 53 46 50 2d 31 30 2f 32 35 47 2d 43 53 52 2d 53
0x00d0 : 20 20 20 20 30 38 00 00 00 00 00 00 00 00 00 d1
0x00e0 : 1e 20 2a 2a 31 34 29 36 00 00 00 00 00 00 00 00
0x00f0 : 00 00 00 00 00 56 00 00 ff ff ff ff 00 00 00 cf
=====
PHY Data:
PAGE IFC OFFSET VALUE | PAGE IFC OFFSET VALUE
-----

```

The following CLI displays detailed information about the parameters set for the packet capture:

```

firepower-3140(local-mgmt)# show portmanager switch pktcap-rules software
Software DB rule:1
Slot= 1
Interface= 12
Breakout-port= 0
Protocol= 6
Ethertype= 0x0000
Filter_key= 0x00000040
Session= 1
Vlan= 0
SrcPort= 0
DstPort= 0
SrcIp= 0.0.0.0
DstIp= 0.0.0.0
SrcIpv6= ::
DestIpv6= ::
SrcMacAddr= 00:00:00:00:00:00
DestMacAddr= 00:00:00:00:00:00

```

The following CLI displays detailed information on the FXOS port manager switch hardware TCAM rules:

```

firepower-3140(local-mgmt)# show portmanager switch pktcap-rules hardware
Hardware DB rule:1
Hw_index= 15372
Rule_id= 10241
Cnc_index= 1
Packet_count= 0
Slot= 1
Interface= 12
Protocol= 6

```

```

Ethertype= 0x0000
Vlan= 0
SrcPort= 0
DstPort= 0
SrcIp= 0.0.0.0
DstIp= 0.0.0.0
SrcIpv6= ::
DestIpv6= ::
SrcMacAddr= 00:00:00:00:00:00
DestMacAddr= 00:00:00:00:00:00

```

The following displays detailed information about the QOS functionality:

```

firepower(local-mgmt)# show portmanager switch qos-rule policer counters
Policer_type  green(pass_count)  yellow(pass_count)  red(drop_count)
-----
OSPF
780
Policer_type  green(pass_count)  yellow(pass_count)  red(drop_count)
-----
CCL_CLU
Policer_type  green(pass_count)  yellow(pass_count)  red(drop_count)
-----
BFD
Policer_type  green(pass_count)  yellow(pass_count)  red(drop_count)
-----
HA
Policer_type  green(pass_count)  yellow(pass_count)  red(drop_count)
-----
CCL_CONTROL

```

Category	Green (pass_count)	Yellow (pass_count)	Red (drop_count)
OSPF	102025351	17832	590
CCL_CLU	0	0	0
BFD	61343307	0	0
HA	0	0	0
CCL_CONTROL	0	0	0

The following CLI verifies if the high priority traffic is hitting the TCAM:

```

firepower(local-mgmt)# show portmanager switch qos-rule counters
Rule_no  Rule_id  Rule_type  pass_count
-----
1  9218  SW_QOS_BFD  0
Rule_no  Rule_id  Rule_type  pass_count
-----
2  9216  SW_QOS_OSPF  102633941
Rule_no  Rule_id  Rule_type  pass_count
-----
3  9217  SW_QOS_BFD  61343307

```

The following CLI displays the CPU statistics as per queue per device matching ethernet 1/10 port:

```

firepower(local-mgmt)# show queuing interface ethernet 1 10
Queue  Traffic-type  Scheduler-type  oper-bandwidth  Destination
-----
3  Data  WRR  100  Application
4  CCL-CLU  SP  0  Application
5  BFD  SP  0  Application
6  OSPF  SP  0  Application
7  CCL-CONTROL/HA/LACP_Tx  SP  0  Application
0  packet-capture  N/A  0  CPU
7  LACP Rx  N/A  0  CPU
Port 1/10 Queue Statistics:
Queue 0:
  Number of packets passed : 0
  Number of packets dropped: 0
Queue 1:

```

```

Number of packets passed :           0
Number of packets dropped:           0
Queue 2:
  Number of packets passed :           0
  Number of packets dropped:           0
Queue 3:
  Number of packets passed :          466420167
  Number of packets dropped:           0
Queue 4:
  Number of packets passed :           0
  Number of packets dropped:           0
Queue 5:
  Number of packets passed :           0
  Number of packets dropped:           0
Queue 6:
  Number of packets passed :          41536261
  Number of packets dropped:           0
Queue 7:
  Number of packets passed :           912
  Number of packets dropped:           0
CPU Statistics:
Queue 2:
  Number of packets passed :          180223
  Number of packets dropped:           0
Queue 7:
  Number of packets passed :           1572
  Number of packets dropped:           0

```

The following CLI displays the CPU statistics as per queue per device matching internal 1/1 port:

```

firepower(local-mgmt)# show queuing interface internal 1 1
Queue      Traffic-type      Scheduler-type  oper-bandwidth  Destination
-----
3          Data              WRR             100             Application
4          CCL-CLU           SP              0              Application
5          BFD               SP              0              Application
6          OSPF              SP              0              Application
7  CCL-CONTROL/HA/LACP_Tx  SP              0              Application
0  packet-capture      N/A             0              CPU
7          LACP_Rx           N/A             0              CPU
Port 1/18 Queue Statistics:
Queue 0:
  Number of packets passed :           0
  Number of packets dropped:           0
Queue 1:
  Number of packets passed :           0
  Number of packets dropped:           0
Queue 2:
  Number of packets passed :           0
  Number of packets dropped:           0
Queue 3:
  Number of packets passed :           17
  Number of packets dropped:           0
Queue 4:
  Number of packets passed :           0
  Number of packets dropped:           0
Queue 5:
  Number of packets passed :           0
  Number of packets dropped:           0
Queue 6:
  Number of packets passed :          5151
  Number of packets dropped:           0

```

```
Queue 7:
  Number of packets passed :      17345
  Number of packets dropped:         0
CPU Statistics:
Queue 2:
  Number of packets passed :      180223
  Number of packets dropped:         0
Queue 7:
  Number of packets passed :        1572
  Number of packets dropped:         0
Note:The CPU statistics are per Queue per Device
```

The following CLI displays detailed information about dump AP log option :

```
firepower-3110(local-mgmt)# dump portmanager switch ap-log
requested log has been dumped to /opt/cisco/platform/logs/portmgr.out*

firepower-3110(local-mgmt)# dump portmanager switch cyclic-log
requested log has been dumped to /opt/cisco/platform/logs/portmgr.out*
```

The following CLI displays detailed information on enabling or disabling verbose logging for port manager:

```
firepower-3110(local-mgmt)# debug portmanager switch
all Enable or Disable verbose logging for switch

firepower-3110(local-mgmt)# debug portmanager switch all
firepower-3110(local-mgmt)#

firepower-3110(local-mgmt)# no debug portmanager switch all
firepower-3110(local-mgmt)#
```

The following CLI displays detailed information on port-based packet drops for eight traffic classes/queues:

```
firepower-3110(local-mgmt)# show portmanager switch tail-drop-allocated buffers all
-----
```

Per Port and Traffic Class								
Port	Per port	TC0	TC1	TC2	TC3	TC4	TC5	TC6
TC7								
0/1	10	10	0	0	0	0	0	0
0								
0/2	15	5	5	5	0	0	0	0
0								
0/3	0	0	0	0	0	0	0	0
0								
0/4	80	0	0	0	0	0	0	0
80								
0/5	0	0	0	0	0	0	0	0
0								
0/6	0	0	0	0	0	0	0	0
0								
0/7	200	25	25	50	0	0	25	50
25								
0/8	0	0	0	0	0	0	0	0
0								

```
-----
```

The following CLI displays dropped packet counts due to tti-lookup0:

```
firepower-3110(local-mgmt)# show portmanager switch default-rule-drop-counter tti-lookup0
```

Rule_id	cnc_index	packet_count
1	1	4

The following CLI displays dropped packet counts due to ipcl-lookup0:

```
firepower-3110(local-mgmt)# show portmanager switch default-rule-drop-counter ipcl-lookup0
```

Rule_id	cnc_index	packet_count
4096	0	114

Connect Local-Mgmt Troubleshooting Commands for the Secure Firewall 4200 in Appliance Mode

In addition to the existing debugging commands, CLIs specific to Secure Firewall 3100 are explained in this section below.

Use the following connect local-mgmt mode FXOS CLI commands to troubleshoot issues with your Secure Firewall 3100 in Appliance mode. To access connect local-mgmt mode, enter:

```
FPR 4200# connect local-mgmt
```

show portmanager

Displays detailed information about switched, packets, SFP-FEC counters, digital optical monitoring, QOS functionality, CPSS AP, and Cyclic log dumps.

For example:

The following CLI displays the FXOS port manager switch hardware TCAM rules dump in vtcam-tti:

```
firepower(local-mgmt)# show portmanager switch forward-rules hardware vtcam-tti
```

	RULE_ID	VLAN	NUM_MPLS_LABELS	SRC_PORT	PC_ID	SRC_ID	MODE	PAK_CNT
1	2	0	0	10	0	10	0	1951
2	3	0	0	14	0	14	0	19
3	4	0	0	9	0	9	0	227505
4	5	0	0	13	0	13	0	103587
5	6	0	0	8	0	0	0	0
6	7	0	0	7	0	0	0	0
7	8	0	0	6	0	0	0	0
8	9	0	0	5	0	0	0	0
9	10	0	0	4	0	0	0	0
10	11	0	0	3	0	0	0	0
11	12	0	0	2	0	0	0	0
12	13	0	0	1	0	0	0	607
13	14	0	0	44	0	0	0	0
14	15	0	0	40	0	0	0	0
15	16	0	0	36	0	0	0	0
16	17	0	0	32	0	0	0	0
17	30	0	0	1	0	101	1	2120
18	18	0	0	1	0	101	0	306
19	19	0	0	2	0	102	0	2429

20	20	0	0	3	0	103	0	0
21	21	0	0	4	0	104	0	0
22	22	0	0	5	0	105	0	0
23	23	0	0	6	0	106	0	0
24	24	0	0	7	0	107	0	0
25	25	0	0	8	0	108	0	0
26	26	0	0	32	0	117	0	0
27	27	0	0	36	0	121	0	0
28	28	0	0	40	0	125	0	0
29	29	0	0	44	0	129	0	0
30	1	0	0	9	0	0	0	1875
31	8193	0	1	0	0	0	0	0
32	8194	0	2	0	0	0	0	0
33	8195	0	3	0	0	0	0	0
34	8196	0	4	0	0	0	0	0
35	8197	0	5	0	0	0	0	0
36	8198	0	6	0	0	0	0	0

The following CLI displays switch hardware TCAM rules dump in vtcam-tti stage matching vlan 0:

```
firepower(local-mgmt)# show portmanager switch forward-rules hardware vtcam-tti
```

	RULE_ID	VLAN	NUM_MPLS_LABELS	SRC_PORT	PC_ID	SRC_ID	MODE	PAK_CNT
1	2	0	0	10	0	10	0	1961
2	3	0	0	14	0	14	0	19
3	4	0	0	9	0	9	0	227517
4	5	0	0	13	0	13	0	103683
5	6	0	0	8	0	0	0	0
6	7	0	0	7	0	0	0	0
7	8	0	0	6	0	0	0	0
8	9	0	0	5	0	0	0	0
9	10	0	0	4	0	0	0	0
10	11	0	0	3	0	0	0	0
11	12	0	0	2	0	0	0	0
12	13	0	0	1	0	0	0	617
13	14	0	0	44	0	0	0	0
14	15	0	0	40	0	0	0	0
15	16	0	0	36	0	0	0	0
16	17	0	0	32	0	0	0	0
17	30	0	0	1	0	101	1	2156
18	18	0	0	1	0	101	0	306
19	19	0	0	2	0	102	0	2466
20	20	0	0	3	0	103	0	0
21	21	0	0	4	0	104	0	0
22	22	0	0	5	0	105	0	0
23	23	0	0	6	0	106	0	0
24	24	0	0	7	0	107	0	0
25	25	0	0	8	0	108	0	0
26	26	0	0	32	0	117	0	0
27	27	0	0	36	0	121	0	0
28	28	0	0	40	0	125	0	0
29	29	0	0	44	0	129	0	0
30	1	0	0	9	0	0	0	1875
31	8193	0	1	0	0	0	0	0
32	8194	0	2	0	0	0	0	0
33	8195	0	3	0	0	0	0	0
34	8196	0	4	0	0	0	0	0
35	8197	0	5	0	0	0	0	0
36	8198	0	6	0	0	0	0	0

The following CLI displays switch hardware TCAM rules dump in mac-filter stage matching ethernet 1/9 port:

```

firepower(local-mgmt)# show portmanager switch forward-rules hardware mac-filter
      VLAN  SRC_PORT  PC_ID  SRC_ID  DST_PORT  PKT_CNT  DMAC
1         0         44      0      129     1536      0  1:80:c2:0:0:2
2         0         44      0      129     1536      0  ff:ff:ff:ff:ff:ff
3         0          2      0      102     1536      0  ba:db:ad:f0:2:8f
4         0          4      0      104     1536      0  ff:ff:ff:ff:ff:ff
5         0          4      0      104     1536      0  1:80:c2:0:0:2
6         0          5      0      105     1536      0  1:80:c2:0:0:2
7         0          5      0      105     1536      0  ff:ff:ff:ff:ff:ff
8         0         13      0       13         9    103735  0:0:0:0:0:0
9         0         32      0      117     1536      0  ba:db:ad:f0:2:9e
10        0          7      0      107     1536      0  ff:ff:ff:ff:ff:ff
11        0          7      0      107     1536      0  1:80:c2:0:0:2
12        0          6      0      106     1536      0  1:80:c2:0:0:2
13        0          6      0      106     1536      0  ff:ff:ff:ff:ff:ff
14        0         14      0       14         10      19  0:0:0:0:0:0
15        0         10      0       14        14    1979  0:0:0:0:0:0
16        0         44      0      129     1536      0  ba:db:ad:f0:2:a1
17        0          9      0       9         13   1227537  0:0:0:0:0:0
18        0          8      0      108     1536      0  1:80:c2:0:0:2
19        0          8      0      108     1536      0  ff:ff:ff:ff:ff:ff
20        0          1      0      101     1536      0  ff:ff:ff:ff:ff:ff
21        0          1      0      101     1536      0  1:80:c2:0:0:2
22        0          3      0      103     1536      0  1:80:c2:0:0:2
23        0          1      0      101     1536    2183  1:0:0:0:0:0
24        0          3      0      103     1536      0  ff:ff:ff:ff:ff:ff
25        0          2      0      102     1536      23  ff:ff:ff:ff:ff:ff
26        0          2      0      102     1536      0  1:80:c2:0:0:2
27        0         32      0      117     1536      0  ff:ff:ff:ff:ff:ff
28        0         32      0      117     1536      0  1:80:c2:0:0:2
29        0         40      0      125     1536      0  ff:ff:ff:ff:ff:ff
30        0         40      0      125     1536      0  1:80:c2:0:0:2
31        0          7      0      107     1536      0  ba:db:ad:f0:2:94
32        0          5      0      105     1536      0  ba:db:ad:f0:2:92
33        0         36      0      121     1536      0  1:80:c2:0:0:2
34        0          4      0      104     1536      0  ba:db:ad:f0:2:91
35        0         36      0      121     1536      0  ff:ff:ff:ff:ff:ff
36        0          8      0      108     1536      0  ba:db:ad:f0:2:95
37        0          6      0      106     1536      0  ba:db:ad:f0:2:93
38        0          3      0      103     1536      0  ba:db:ad:f0:2:90
39        0         36      0      121     1536      0  ba:db:ad:f0:2:9f
40        0          1      0      101     1536      32  ba:db:ad:f0:2:8e
41        0         40      0      125     1536      0  ba:db:ad:f0:2:a0

```

The following CLI displays detailed information about software MAC-filter:

```

firepower-4225(local-mgmt)# show portmanager switch forward-rules software mac-filter
      NATIVE_VLAN  VLAN  SRC_PORT  PORTCHANNEL_ID  DST_PORT  FLAGS  MODE  DMAC
1         0         106      6           0         1536      2     5
1:80:c2:0:0:2
2         0         105      5           0         1536      2     5
ff:ff:ff:ff:ff:ff
3         0         105      5           0         1536      2     5
1:80:c2:0:0:2
4         0         121      0           0          36      24     8
0:0:0:0:0:0
5         0         106      6           0         1536      2     5
ff:ff:ff:ff:ff:ff
6         0         121     36           0         1536      2     5
1:80:c2:0:0:2
7         0         117     32           0         1536      2     5
1:80:c2:0:0:2

```

8	0	125	40	0	1536	2	5
ff:ff:ff:ff:ff:ff							
9	0	129	0	0	44	24	8
0:0:0:0:0:0							
10	0	117	32	0	1536	2	5
ff:ff:ff:ff:ff:ff							
11	0	103	3	0	1536	2	5
1:80:c2:0:0:2							
12	0	102	2	0	1536	2	5
ff:ff:ff:ff:ff:ff							
13	0	117	0	0	32	24	8
0:0:0:0:0:0							
14	0	107	0	0	7	24	8
0:0:0:0:0:0							
15	0	101	1	0	1536	2	5
ba:db:ad:f0:2:8e							
16	0	107	7	0	1536	2	5
ff:ff:ff:ff:ff:ff							
17	0	106	6	0	1536	2	5
ba:db:ad:f0:2:93							
18	0	105	0	0	5	24	8
0:0:0:0:0:0							
19	0	102	0	0	2	24	8
0:0:0:0:0:0							
20	0	104	4	0	1536	2	5
ba:db:ad:f0:2:91							
21	0	107	7	0	1536	2	5
ba:db:ad:f0:2:94							
22	0	129	44	0	1536	2	5
1:80:c2:0:0:2							
23	0	102	2	0	1536	2	5
1:80:c2:0:0:2							
24	0	121	36	0	1536	2	5
ff:ff:ff:ff:ff:ff							
25	0	1	13	0	9	26	8
0:0:0:0:0:0							
26	0	108	8	0	1536	2	5
1:80:c2:0:0:2							
27	0	101	1	0	1536	2	5
ff:ff:ff:ff:ff:ff							
28	0	2	10	0	14	26	8
0:0:0:0:0:0							
29	0	101	1	0	1536	2	5
1:80:c2:0:0:2							
30	0	1	9	0	13	26	8
0:0:0:0:0:0							
31	0	129	44	0	1536	2	5
ff:ff:ff:ff:ff:ff							
32	0	125	0	0	40	24	8
0:0:0:0:0:0							
33	0	108	8	0	1536	2	5
ba:db:ad:f0:2:95							
34	0	2	14	0	10	26	8
0:0:0:0:0:0							
35	0	129	44	0	1536	2	5
ba:db:ad:f0:2:a1							
36	0	103	0	0	3	24	8
0:0:0:0:0:0							
37	0	104	0	0	4	24	8
0:0:0:0:0:0							
38	0	104	4	0	1536	2	5
ff:ff:ff:ff:ff:ff							
39	0	107	7	0	1536	2	5
1:80:c2:0:0:2							

```

40          0      104      4          0      1536      2      5
1:80:c2:0:0:2
41          0      101      1          0      1536      18      8
0:0:0:0:0:0
42          0      101      0          0          1      24      8
0:0:0:0:0:0
43          0      108      8          0      1536      2      5
ff:ff:ff:ff:ff:ff
44          0      121      36         0      1536      2      5
ba:db:ad:f0:2:9f
45          0      117      32         0      1536      2      5
ba:db:ad:f0:2:9e
46          0      105      5          0      1536      2      5
ba:db:ad:f0:2:92
47          0      125      40         0      1536      2      5
ba:db:ad:f0:2:a0
48          0      125      40         0      1536      2      5
1:80:c2:0:0:2
49          0      108      0          0          8      24      8
0:0:0:0:0:0
50          0      106      0          0          6      24      8
0:0:0:0:0:0
51          0      103      3          0      1536      2      5
ba:db:ad:f0:2:90
52          0      102      2          0      1536      2      5
ba:db:ad:f0:2:8f
53          0      103      3          0      1536      2      5
ff:ff:ff:ff:ff:ff

```

The following CLI displays detailed information about switch bridge engine packet drops:

```

firepower-4225(local-mgmt)# show portmanager switch counters bridge
Bridge Ingress Drop Counter: 4688
No Bridge Ingress Drop

```

The following CLI displays details on hardware switch packet counters:

```

how portmanager switch counters packet-trace

```

```

firepower-4225(local-mgmt)# show portmanager switch counters packet-trace

```

Counter	Description
goodOctetsRcv	Number of ethernet frames received that are not bad ethernet frames or MAC Control pkts
badOctetsRcv	Sum of lengths of all bad ethernet frames received
gtBrgInFrames	Number of packets received
gtBrgVlanIngFilterDisc	Number of packets discarded due to VLAN Ingress Filtering
gtBrgSecFilterDisc	Number of packets discarded due to Security Filtering measures
gtBrgLocalPropDisc	Number of packets discarded due to reasons other than VLAN ingress and Security filtering
dropCounter	Ingress Drop Counter
outUcFrames	Number of unicast packets transmitted
outMcFrames	Number of multicast packets transmitted. This includes registered multicasts, unregistered multicasts and unknown unicast packets
outBcFrames	Number of broadcast packets transmitted
brgEgrFilterDisc	Number of IN packets that were Bridge Egress filtered
txqFilterDisc	Number of IN packets that were filtered due to TxQ congestion
outCtrlFrames	Number of out control packets (to cpu, from cpu and to analyzer)

```

egrFrwDropFrames      Number of packets dropped due to egress
                      forwarding restrictions
goodOctetsSent        Sum of lengths of all good ethernet
                      frames sent from this MAC

      Counter          Source port- 0/0    Destination port- 0/0
-----
goodOctetsRcv         ---
badOctetsRcv          ---

                                Ingress counters
gtBrgInFrames         1341132
gtBrgVlanIngFilterDisc 0
gtBrgSecFilterDisc    0
gtBrgLocalPropDisc    0
dropCounter           4699                Only for source-port

                                Egress counters
outUcFrames           1329593
outMcFrames           4594
outBcFrames           2237
brgEgrFilterDisc     9
txqFilterDisc         0
outCtrlFrames         0
egrFrwDropFrames     0
mcFifoDropPkts       0
mcFilterDropPkts     0

goodOctetsSent        ---
    
```

The following CLI displays detailed informatin about the switch traffic for CPU:

```

firepower-4225(local-mgmt)# show portmanager switch traffic cpu

Dev/RX queue  packets  bytes
-----
Dev/RX queue  packets  bytes
-----
0/0           0        0
0/1           0        0
0/2           0        0
0/3           0        0
0/4           0        0
0/5           0        0
0/6           0        0
0/7           0        0
    
```

The following CLI displays details on hardware switch port traffic:

```

firepower-4225(local-mgmt)# show portmanager switch traffic port

max-rate - pps that the port allow with packet size=64
actual-tx-rate - pps that egress the port (+ % from 'max')
actual-rx-rate - pps that ingress the port(+ % from 'max')

Dev/Port  max-rate  actual-tx-rate  actual-rx-rate
-----
0/1       1488095  (0%)---        (0%)---
0/2       1488095  (0%)---        (0%)---
    
```

0/3	14880	(0%) ---	(0%) ---
0/4	14880	(0%) ---	(0%) ---
0/5	14880	(0%) ---	(0%) ---
0/6	14880	(0%) ---	(0%) ---
0/7	14880	(0%) ---	(0%) ---
0/8	14880	(0%) ---	(0%) ---
0/9	14880952	(0%) ---	(0%) ---
0/10	14880952	(0%) ---	(0%) ---
0/11	14880952	(0%) ---	(0%) ---
0/12	14880952	(0%) ---	(0%) ---
0/13	14880952	(0%) ---	(0%) ---
0/14	14880952	(0%) ---	(0%) ---
0/15	1488095	(0%) ---	(0%) ---
0/16	1488095	(0%) ---	(0%) ---
0/17	14880952	(0%) ---	(0%) ---
0/18	74404761	(0%) ---	(0%) ---
0/19	37202380	(0%) ---	(0%) ---
0/20	37202380	(0%) ---	(0%) ---

The following CLI displays detailed information about SFP-FEC Counters matching ethernet 1/13 port:

```
firepower-4225(local-mgmt)# show portmanager counters ethernet 1 13
Good Octets Received           : 2153
Bad Octets Received           : 0
MAC Transmit Error            : 0
Good Packets Received         : 13
Bad packets Received         : 0
BRDC Packets Received         : 0
MC Packets Received           : 13
.....
.....
txqFilterDisc                  : 0
linkchange                     : 1
FcFecRxBlocks                 : 217038081
FcFecRxBlocksNoError          : 217038114
FcFecRxBlocksCorrectedError   : 0
FcFecRxBlocksUnCorrectedError : 0
FcFecRxBlocksCorrectedErrorBits : 0
FcFecRxBlocksCorrectedError0  : 0
FcFecRxBlocksCorrectedError1  : 0
FcFecRxBlocksCorrectedError2  : 0
FcFecRxBlocksCorrectedError3  : 0
FcFecRxBlocksUnCorrectedError0 : 0
FcFecRxBlocksUnCorrectedError1 : 0
FcFecRxBlocksUnCorrectedError2 : 0
FcFecRxBlocksUnCorrectedError3 : 0
```

The following CLI displays detailed information about SFP-FEC Counters matching ethernet 1/14 port:

```
firepower-4225(local-mgmt)# show portmanager counters ethernet 1 14
Good Octets Received           : 2153
Bad Octets Received           : 0
MAC Transmit Error            : 0
Good Packets Received         : 13
Bad packets Received         : 0
BRDC Packets Received         : 0
MC Packets Received           : 13
.....
.....
txqFilterDisc                  : 0
linkchange                     : 1
```

```
RsFeccorrectedFecCodeword           : 0
RsFecuncorrectedFecCodeword         : 10
RsFecsymbolError0                   : 5
RsFecsymbolError1                   : 0
RsFecsymbolError2                   : 0
RsFecsymbolError3                   : 0
```

The following CLI displays detailed information on the Digital Optical Monitoring information matching ethernet 1/5 port:

```
firepower-4245(local-mgmt)# show portmanager port-info ethernet 1 5
....
....
      DOM info:
      =====:

      Status/Control Register: 0800
          RX_LOS State: 0
          TX_FAULT State: 0
      Alarm Status: 0000
      No active alarms
      Warning Status: 0000
      No active warnings

THRESHOLDS
          high alarm   high warning   low warning   low alarm
Temperature    C    +075.000    +070.000    +000.000    -05.000
Voltage        V     003.6300    003.4650    003.1350    002.9700
Bias Current   mA     012.0000    011.5000    002.0000    001.0000
Transmit power mW  034.6740    017.3780    002.5120    001.0000
Receive power  mW  034.6740    017.3780    001.3490    000.5370

Environmental Information - raw values
Temperature: 38.84 C
Supply voltage: 33703 in units of 100uVolt
Tx bias: 3499 in units of 2uAmp
Tx power: 0.1 dBm (10251 in units of 0.1 uW)
Rx power: -0.9 dBm (8153 in units of 0.1 uW)
DOM (256 bytes of raw data in hex)
=====
0x0000 : 4b 00 fb 00 46 00 00 00 8d cc 74 04 87 5a 7a 76
0x0010 : 17 70 01 f4 16 76 03 e8 87 72 03 e8 43 e2 09 d0
0x0020 : 87 72 02 19 43 e2 05 45 00 00 00 00 00 00 00 00
0x0030 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0040 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0050 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 86
0x0060 : 26 54 83 a7 0d ab 28 0b 1f d9 00 00 00 00 08 00
0x0070 : 00 00 03 00 00 00 00 00 08 f3 00 00 00 00 00 01
0x0080 : 49 4e 55 49 41 43 53 45 41 41 31 30 2d 33 33 38
0x0090 : 38 2d 30 31 56 30 31 20 01 00 46 00 00 00 00 e3
0x00a0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x00b0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x00c0 : 53 46 50 2d 31 30 2f 32 35 47 2d 43 53 52 2d 53
0x00d0 : 20 20 20 20 30 38 00 00 00 00 00 00 00 00 00 d1
0x00e0 : 1e 20 2a 2a 31 34 29 36 00 00 00 00 00 00 00 00
0x00f0 : 00 00 00 00 00 56 00 00 ff ff ff ff 00 00 00 cf
=====
PHY Data:
```

```
PAGE IFC OFFSET VALUE | PAGE IFC OFFSET VALUE
-----
```

The following CLI displays detailed information about the parameters set for the packet capture:

```
firepower-4225(local-mgmt)# show portmanager switch pktcap-rules software
Software DB rule:1
Slot= 1
Interface= 12
Breakout-port= 0
Protocol= 6
Ethertype= 0x0000
Filter_key= 0x00000040
Session= 1
Vlan= 0
SrcPort= 0
DstPort= 0
SrcIp= 0.0.0.0
DstIp= 0.0.0.0
SrcIpv6= ::
DestIpv6= ::
SrcMacAddr= 00:00:00:00:00:00
DestMacAddr= 00:00:00:00:00:00
```

The following CLI displays detailed information on the FXOS port manager switch hardware TCAM rules:

```
firepower-4225(local-mgmt)# show portmanager switch pktcap-rules hardware
Hardware DB rule:1
Hw_index= 15372
Rule_id= 10241
Cnc_index= 1
Packet_count= 0
Slot= 1
Interface= 12
Protocol= 6
Ethertype= 0x0000
Vlan= 0
SrcPort= 0
DstPort= 0
SrcIp= 0.0.0.0
DstIp= 0.0.0.0
SrcIpv6= ::
DestIpv6= ::
SrcMacAddr= 00:00:00:00:00:00
DestMacAddr= 00:00:00:00:00:00
```

The following CLI displays detailed information on port-based packet drops for eight traffic classes/queues:

```
firepower-4225(local-mgmt)# show portmanager switch tail-drop-allocated buffers all
-----
```

Per Port and Traffic Class									
Port	Per port	TC0	TC1	TC2	TC3	TC4	TC5	TC6	TC7
0/1	10	10	10	10	10	10	10	10	10
10									
0/2	15	15	15	15	10	10	10	10	10
10									
0/3	10	10	10	10	10	10	10	10	10
10									

0/4	80	0	0	0	0	0	0	0
80								
0/5	0	0	0	0	0	0	0	0
0								
0/6	0	0	0	0	0	0	0	0
0								
0/7	200	25	25	50	0	0	25	50
25								
0/8	0	0	0	0	0	0	0	0
0								

The following CLI displays dropped packet counts due to tti-lookup0:

```
firepower-4225(local-mgmt)# show portmanager switch default-rule-drop-counter tti-lookup0
```

Rule_id	cnc_index	packet_count
1	1	4

FXOS CLI Security Services Mode Troubleshooting Commands

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

show app

Displays information about the applications attached to your Firepower 1000/2100 or Secure Firewall 3100 device.

For example:

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

Name	Version	Description	Author	Deploy Type	CSP Type	Is Default 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
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 the threat defense application on Firepower 1000/2100 or Secure Firewall 3100 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
```

Secure Firewall 1200/3100/4200 CLI Monitoring Mode Troubleshooting Commands

Use the following CLI commands to troubleshoot issues.

show

Displays the state of memory leak, process wise.
For example:

```
FPR3100 /monitoring/sysdebug/mem-leak-logging # show detail
      Process           Status      Stacktrace
-----
statsAG      Disabled   Off
dcosAG       Disabled   Off
portAG       Disabled   Off
appAG        Disabled   Off
eventAG      Disabled   Off
npuAG        Disabled   Off
sessionmgrAG Disabled   Off
svcmonAG     Disabled   Off
serviceOrchAG Disabled   Off
dme          Disabled   Off
envAG        Disabled   Off
```



Note By default, mem-leak is disabled for all UCSM processes, and stacktrace is disabled. You must enable mem-leak for the specified process to debug the memory leak issues, and enable the stacktrace for more information on the issue.

Packet Capture for Secure Firewall 3100/4200

The Packet Capture tool is a valuable asset for use in debugging connectivity and configuration issues and for understanding traffic flows through your devices. You can now use the Packet Capture CLIs to log traffic that is going through specific interfaces on your Secure Firewall 3100/4200 devices.

You can create multiple packet capture sessions, and each session can capture traffic on multiple interfaces. For each interface included in a packet capture session, a separate packet capture (PCAP) file will be created.

Guidelines and Limitations for Packet Capture

The Packet Capture tool has the following limitations:

- Packet Capture on Secure Firewall 3100/4200 series devices can capture up to 300 Mbps.
- Packet capture sessions can be created even when there is not enough storage space available to run the packet capture session. You should verify that you have enough storage space available before you start a packet capture session.
- For packet capture sessions on a single-wide 4x100Gbps or 2x100Gbps network module (part numbers FPR-NM-4X100G and FPR-NM-2X100G respectively), if the module `adminstate` is set to `off`, the capture session is automatically disabled with an “Oper State Reason: Unknown Error.” You will have to restart the capture session after the module `adminstate` is set to `on` again.

With all other network modules, packet capture sessions continue across module `adminstate` changes.

- Does not support multiple active packet capturing sessions.
- There is no option to filter based on source or destination IPv6 address.
- Filters are not effective on packets that cannot be understood by the internal switch (for example Security Group Tag and Network Service Header packets).

- You cannot capture packets for an EtherChannel as a whole. However, for an EtherChannel allocated to a logical device, you can capture packets on each member interface of the EtherChannel.
- You cannot copy or export a PCAP file while the capture session is still active.
- When you delete a packet capture session, all packet capture files associated with that session are also deleted.

Creating or Editing a Packet Capture Session

Procedure

Step 1 Enter packet capture mode:

```
firepower-4215 # scope packet-capture
```

Step 2 Create a filter.

```
firepower-4215 /packet-capture/filter* # set <filterprop filterprop_value
```

Table 2: Supported Filter Properties

ivlan	Inner VLAN ID (vlan of packet while ingressing port)
ovlan	Outer VLAN ID
srcip	Source IP Address (IPv4)
destip	Destination IP Address (IPv4)
srcport	Source Port Number
destport	Destination Port Number
protocol	IP Protocol [IANA defined Protocol values in decimal format]
ethertype	Ethernet Protocol type [IANA defined Ethernet Protocol type value in decimal format. For eg: IPv4 = 2048, IPv6 = 34525, ARP = 2054, SGT = 35081]
srcmac	Source Mac Address
destmac	Destination Mac Address

You can apply filters to any of the interfaces included in a packet capture session.

Step 3 To create or edit a packet capture session:

```
firepower-4215 /packet-capture # enter session session_name
```

Step 4 Specify the length of the packet that you want to capture for this packet capture session:

```
firepower-4215 /packet-capture/session* # set session-pcap-snaplength session_snap_length_in_bytes
```

The specified snap length must be between 64 and 9006 bytes. If you do not configure the session snap length, the default capture length is 1518 bytes.

Step 5 Specify the physical source ports that should be included in this packet capture session.

You can capture from multiple ports and can capture from both physical ports and application ports during the same packet capture session. A separate packet capture file is created for each port included in the session. You cannot capture packets for an EtherChannel as a whole. However, for an EtherChannel allocated to a logical device, you can capture packets on each member interface of the EtherChannel.

Note

To remove a port from the packet capture session, use **delete** instead of **create** in the commands listed below.

a) Specify the physical port.

```
firepower-4215 /packet-capture/session* # create {phy-port | phy-aggr-port} port_id
```

Example:

Example:

```
firepower-4215 /packet-capture/session* # create phy-port Ethernet1/1
firepower-4215 /packet-capture/session/phy-port* #
```

b) Capture packets on a subinterface.

```
firepower-4215 /packet-capture/session/phy-port* # set subinterface id
```

You can only capture packets for one subinterface per capture session, even if you have multiple subinterfaces on one or more parents. Subinterfaces for EtherChannels are not supported. If the parent interface is also allocated to the instance, you can either choose the parent interface or a subinterface; you cannot choose both.

Example:

```
firepower-4215 /packet-capture/session/phy-port* # set subinterface 100
firepower-4215 /packet-capture/session/phy-port* #
```

c) For container instances, specify the container instance name.

```
firepower-4215 /packet-capture/session/phy-port* # set app-identifier instance_name
```

Example:

```
firepower-4215 /packet-capture/session/phy-port* # set app-identifier ftd-instance1
firepower-4215 /packet-capture/session/phy-port* #
```

d) (Optional) For capturing the mac-filter dropped packets from switch, specify the mac-filter drop.

```
firepower-4215 /packet-capture/session/phy-port* # set drop {mac-filter | disable}
```

- **disable**—To disable capture of packets dropped from switch.
- **mac-filter**—To capture switch mac-filter drop

Note

The mac-filter option is supported only for the ingress packet capture direction and the default option is always **disable**.

e) (Optional) Apply the desired filter.

```
firepower-4215 /packet-capture/session/phy-port* # set {source-filter} filename
```

Note

To remove a filter from a port, use **set source-filter ""**.

- f) Repeat the steps above as needed to add all desired ports.

Step 6

Specify the application source ports that should be included in this packet capture session.

You can capture from multiple ports and can capture from both physical ports and application ports during the same packet capture session. A separate packet capture file is created for each port included in the session.

Note

To remove a port from the packet capture session, use **delete** instead of **create** in the commands listed below.

- a) Specify the application port.

```
firepower-4215 /packet-capture/session* # create app_port module_slot link_name interface_name
app_name
```

Syntax Description

module_slot	Security module in which the application is installed.
link_name	Any user descriptive name referring to the interface, for example, link1, inside_port1, etc.
interface_name	Interface attached to the application where packets need to be captured from, for example, Ethernet1/1, Ethernet2/2
app_name	Application installed on the module - ftd

- b) (Optional) Apply the desired filter.

```
firepower-4215 /packet-capture/session/phy-port* # set {source-filter} filename
```

Syntax Description

filename	The filter name from the 'create filter' command under packet-capture scope
-----------------	---

Note

To remove a filter from a port, use **set source-filter ""**.

- c) Repeat the steps above as needed to add all desired application ports.

Step 7

If you want to start the packet capture session now:

```
firepower-4215 /packet-capture/session* # enable
```

Newly created packet-capture sessions are disabled by default. Explicit enabling of a session activates the packet capture session when the changes are committed. If another session is already active, enabling a session will generate an error. You must disable the already active packet-capture session before you can enable this session.

Step 8

Commit the transaction to the system configuration:

```
firepower-4215 /packet-capture/session* # commit-buffer
```

If you enabled the packet capture session, the system will begin capturing packets. You will need to stop capturing before you can download the PCAP files from your session.

Example

```
firepower-4215 # scope packet-capture
firepower-4215 /packet-capture # create session ftdlinside
firepower-4215 /packet-capture* # create filter interfacelvlan100
firepower-4215 /packet-capture/filter* # set ivlan 100
firepower-4215 /packet-capture/filter* # set srcIP 6.6.6.6
firepower-4215 /packet-capture/filter* # set destIP 10.10.10.10
firepower-4215 /packet-capture/filter* # exit
firepower-4215 /packet-capture/session* # create phy-port Ethernet1/1
firepower-4215 /packet-capture/session/phy-port* # set drop mac-filter
firepower-4215 /packet-capture/session/phy-port* # set src-filter interfacelvlan100
firepower-4215 /packet-capture/session/phy-port* # exit
firepower-4215 /packet-capture/session* # enable
firepower-4215 /packet-capture/session* # commit-buffer
firepower-4215 /packet-capture/session #
```

Deleting Packet Capture Sessions

You can delete an individual packet capture session if it is not currently running or you can delete all inactive packet capture sessions.

Procedure

-
- Step 1** Enter packet capture mode:
- ```
firepower-4215 # scope packet-capture
```
- Step 2** To delete a specific packet capture session:
- ```
firepower-4215 /packet-capture # delete session session_name
```
- Step 3** To delete all inactive packet capture sessions:
- ```
firepower-4215/packet-capture # delete-all-sessions
```
- Step 4** Commit the transaction to the system configuration:
- ```
firepower-4215 /packet-capture* # commit-buffer
```
-

Example

```
firepower-4215 # scope packet-capture
firepower-4215 packet-capture # delete session asalinside
firepower-4215 packet-capture* # commit-buffer
firepower-4215 packet-capture #
```




CHAPTER 4

Image Management

- [About Disaster Recovery, on page 47](#)
- [Reimage the System with the Base Install Software Version, on page 48](#)
- [Perform a Factory Reset from ROMMON \(Password Reset\), on page 50](#)
- [Reimage the System with a New Software Version, on page 52](#)
- [Download a Package for Multi-Instance Mode, on page 55](#)
- [Reformat the SSD File System \(Firepower 2100\), on page 56](#)
- [Boot from ROMMON, on page 57](#)
- [Perform a Complete Reimage, on page 64](#)
- [Change the Admin Password, on page 68](#)
- [Change the Admin Password if Threat Defense is Offline, on page 69](#)
- [Deregister From Cloud, on page 70](#)
- [History for FXOS Troubleshooting, on page 71](#)

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 threat defense is reinstalled using the current image. Note that after performing this procedure, you will have to reconfigure the system, including admin password and connectivity information. See [Reimage the System with the Base Install Software Version, on page 48](#).
- Perform a factory reset from ROMMON (admin password recovery)—All configurations are removed, and threat defense is reinstalled using the current image. Note that after performing this procedure, you will have to reconfigure the system, including admin password and connectivity information. See [Perform a Factory Reset from ROMMON \(Password Reset\), on page 50](#).
- Reimage the system with a new version—All configurations are removed, and threat defense is reinstalled using the a new software image. Note that after performing this procedure, you will have to reconfigure the system, including admin password and connectivity information. See [Reimage the System with a New Software Version, on page 52](#).



Note You cannot perform a downgrade to the previous major version using this procedure. You must use the [Perform a Complete Reimage, on page 64](#) 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 56](#).
- 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 57](#).
- Erase all configuration and images—This option restores your system to its factory default settings, and erases the images. The procedure requires you to boot the system over TFTP, download the threat defense software, and reconfigure the entire system. See [Perform a Complete Reimage, on page 64](#).
- Change the admin password—This procedure lets you change the admin password from the threat defense CLI. See [Change the Admin Password, on page 68](#).
- Change the admin password if threat defense is offline—This procedure lets you change the admin password from FXOS. See [Change the Admin Password if Threat Defense is Offline, on page 69](#). Note that if the threat defense is online, you must change the admin password using the threat defense CLI.

Reimage the System with the Base Install Software Version

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

If your current running version is an upgrade-only image, you will have to re-upgrade your threat defense after performing this procedure. For example, version 6.2.2.x is an upgrade-only image. If you elect to perform this procedure on your 6.2.2.x system, then the base install package (version 6.2.1.x) will be reinstalled, and you will need to re-upgrade to version 6.2.2.x using the Secure Firewall Management Center or Secure Firewall device manager. In this case, the FXOS version may not revert back to a lower version. This mismatch may cause failures in a High Availability configuration. For this scenario, we recommended that you perform a complete reimage of the system (see [Perform a Complete Reimage, on page 64](#) for more information).



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

Before you begin

- Verify that you are in the FXOS CLI context. If you connect to the Firepower 1000/2100, Secure Firewall 1200, Secure Firewall 3100, or Secure Firewall 4200 device via serial console, you will automatically connect to the FXOS CLI context. If you are in the threat defense CLI context, you must first switch to the FXOS CLI context with the **connect fxos** command.
- Take note of your appliance management IP address configuration and copy the information shown from the following command:

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

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

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

- Disassociate your devices from Smart Licensing.
- Deregister your devices from the cloud tenant (if applicable). See [Deregister From Cloud, on page 70](#).
- To reimage your Secure Firewall 3100 device to threat defense 7.3.0 version, you must have ROMMON version 1.1.08 or above. If the current ROMMON version is less than 1.1.08, you must upgrade ROMMON by upgrading to ASA 9.19 or later. You can also use the management center or device manager to upgrade the threat defense to 7.3.0 (see [Threat Defense Reimage](#) for more information).
- You cannot reimage the Secure Firewall 3100 device to threat defense 7.4 using the base install software version due to the introduction of a single image for installation and upgrading of the threat defense image. Instead, perform a complete reimage of the system. For more information, see [Perform a Complete Reimage, on page 64](#).

Procedure

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

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

- Step 2** Erase all configuration:

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

Example:

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

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

Example:

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

```

Application Name      Slot ID      Admin State      Operational State      Running Version Startup
Version Cluster Oper State
-----
ftd                   1           Disabled         Installing
6.2.1-1314           Not Applicable

```

Note

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

Example:

```

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

```

What to do next

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

Perform a Factory Reset from ROMMON (Password Reset)

If you cannot log into FXOS (either because you forgot the password, or the SSD disk1 file system was corrupted), you can restore the FXOS and threat defense configuration to the factory default using ROMMON. The admin password is reset to the default **Admin123**. If you know the password, and want to restore the factory default configuration from within FXOS, see [Reimage the System with the Base Install Software Version, on page 48](#).

Before you begin

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

Procedure

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

```

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

```

Step 2 Verify the ROMMON version:

```
rommon 1 > show info
```

Example:

Firepower 1000 and 2100 devices

```
rommon 1 > show info
```

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

Secure Firewall 3100 devices

```
rommon 1 > show info
```

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

Secure Firewall 4200 devices

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

Step 3 Factory reset the device.

For ROMMON version 1.0.06 or later:

```
rommon 2 > factory-reset
```

For ROMMON version 1.0.04:

```
rommon 2 > password_reset
```

Example:

Firepower 1000 and 2100 devices

```
rommon 2 > factory-reset
```

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

```
Are you sure you would like to continue ? yes/no [no]: yes
```

```
Please type 'ERASE' to confirm the operation or any other value to cancel: ERASE
```

```
Performing factory reset...
```

```
File size is 0x0000001b
```

```
Located .boot_string
```

```
Image size 27 inode num 16, bks cnt 1 blk size 8*512
```

```
Rommon will continue to boot disk0: fxos-k8-fp2k-lfbff.2.3.1.132.SSB
```

```
Are you sure you would like to continue ? yes/no [no]: yes
```

```
File size is 0x0817a870
```

```
Located fxos-k8-fp2k-lfbff.2.3.1.132.SSB
```

Example:

Secure Firewall 3100 devices

```
rommon 2 > factory-reset
```

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

```
Are you sure you would like to continue ? yes/no [no]: yes
```

```
Please type 'ERASE' to confirm the operation or any other value to cancel: ERASE
```

```
Performing factory reset...
```

```
File size is 0x0000001b
```

```
Located .boot_string
```

```
Image size 27 inode num 16, bks cnt 1 blk size 8*512

Rommon will continue to boot disk0: Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-4.sh.REL.tar
Are you sure you would like to continue ? yes/no [no]: yes
File size is 0x0817a870
Located Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-4.sh.REL.tar
```

Example:**Secure Firewall 4200 devices**

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

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

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

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

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

```
rommon 3 > boot
```

What to do next

Complete the setup tasks in the getting started guide.

Reimage the System with a New Software Version

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



Note You cannot perform a downgrade to the previous major version using this procedure. You must use the [Perform a Complete Reimage, on page 64](#) instead.



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

Before you begin

- Verify that you are in the FXOS CLI context. If you connect to the Firepower 1000/2100, Secure Firewall 1200, Secure Firewall 3100, or Secure Firewall 4200 device via serial console, you will automatically connect to the FXOS CLI context. If you are in the threat defense CLI context, you must first switch to the FXOS CLI context with the **connect fxos** command.
- Take note of your appliance management IP address configuration, and copy the information shown from the following command:

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

- Disassociate your devices from Smart Licensing.
- Deregister your devices from the cloud tenant (if applicable). See [Deregister From Cloud, on page 70](#).
- To reimage your Secure Firewall 3100 device to threat defense version 7.3.0, you must have ROMMON version 1.1.08 or above. If the current ROMMON version is less than 1.1.08, you must upgrade ROMMON by upgrading to ASA 9.19 or later. You can also use the management center or device manager to upgrade threat defense version to 7.3.0 (see [Threat Defense Reimage](#) for more information).

Procedure

-
- Step 1** Download the software bundle to your local computer, or to a USB flash drive.
- Step 2** If using a USB drive, insert the USB drive into the USB port on the appliance.
- Step 3** In FXOS, enter the system scope and verify the current version running on your system:
- ```
firepower # scope system
firepower /system # show version detail
```
- Step 4** Enter the firmware scope:
- ```
firepower # scope firmware
```
- Step 5** Download the new software package. If you are using a USB drive to download the software package, use the following syntax:
- ```
firepower # scope firmware
firepower /firmware # download image usbA:image_name
```
- Note that the *image\_name* is the output from the **show version detail** command in step 3, above.
- For example:
- ```
firepower /firmware # download image usbA:cisco-ftd-fp2k.6.2.1-36.SPA
```
- Note**
In version 7.3+, the threat defense install and upgrade package for Secure Firewall 3100 is a combined package. You can use the `.REL.tar` file instead of `.SPA` file for the described procedure.
- You can also use FTP, SCP, SFTP, or TFTP to copy the threat defense software package to the device:

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

Example for Firepower 1000 and 2100 devices:

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

Example for Secure Firewall 3100 devices:

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

Example for Secure Firewall 4200 devices:

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

Note

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

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

Step 6

Display the download task to monitor the download progress:

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

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

Example:

Secure Firewall 3100 devices:

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

Example:

Secure Firewall 4200 devices:

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

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

Step 7

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

```
firepower /firmware # show package
```

Example:

Firepower 1000 and 2100 devices

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

```
-----
cisco-ftd-fp2k.6.2.1-1314.SPA                6.2.1-1314
```

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

Example:

Secure Firewall 3100 devices

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

Example:

Secure Firewall 4200 devices

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

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

Step 8

Enter the auto-install scope:

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

Step 9

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

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

Example:

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

Step 10

Enter **yes** when prompted.

The system reboots, then installs the latest software bundle.

What to do next

Complete the setup tasks in the getting started guide.

Download a Package for Multi-Instance Mode

This procedure lets you download an older threat defense package to a multi-instance chassis, so you can add an instance using that version. Both the FXOS and threat defense images are included in the same package, so if you upgraded the chassis FXOS version, the old, matching threat defense version will still be available for instances.

You won't be able to use a threat defense that is not compatible with the running FXOS version. For example, you cannot use a newer threat defense without upgrading your chassis first.

Before you begin

- Verify that you are in the FXOS CLI. If you connect to the device from the console, you will automatically connect to the FXOS CLI. If you SSH to the device, you will connect to the threat defense CLI, and you must use the **connect fxos** command to access the FXOS CLI.

Procedure

Step 1 Copy the package to a FTP, SCP, SFTP, or TFTP server or to a USB flash drive.

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

Step 3 Download the older software package.

firepower # **scope firmware**

firepower /firmware # **download image url**

Example:

For example, to download from a USB drive (usbA), enter:

```
firepower-3110 /firmware # download image usbA:Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-15.sh.DEV.tar
Please use the command 'show download-task' or 'show download-task detail' to check download
progress.
% Download-task Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-15.sh.DEV.tar : completed successfully.
```

For example, to download from an SCP server, enter:

```
firepower-3110 /firmware # download image
scp://example.cisco.com/auto/Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-78.sh.REL.tar
Please use the command 'show download-task' or 'show download-task detail' to check download
progress.
% Download-task Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-78.sh.DEV.tar : completed successfully.
```

Step 4 You can now use the package when you add an instance.

Reformat the SSD File System (Firepower 2100)

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

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

Procedure

-
- Step 1** Connect to the FXOS CLI from the console port.
- Step 2** Reformat SSD1.
- connect local-mgmt**
- format ssd1**
- Step 3** Complete the setup tasks in the getting started guide.
-

Boot from ROMMON

If you cannot boot the device, it will boot into ROMMON where you can boot FXOS from a TFTP server or a USB drive formatted as EXT2/3/4 or VFAT/FAT32 . After booting into FXOS, you can then reformat the eMMC (the internal flash device that holds the software images). After you reformat, then you need to re-download the images to the eMMC. This procedure retains all configuration, which is stored on the separate ssd1.

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

Before you begin

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

Procedure

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

Example:

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

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

```
Platform FPR-2130 with 32768 MBytes of main memory
```

```
BIOS has been successfully locked !!
MAC Address: 0c:75:bd:08:c9:80
```

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

Press **Esc** at this point.

Step 2 Boot from an image on a USB drive formatted as EXT2/3/4 or VFAT/FAT32, or boot over the network using TFTP.

Note

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

If you want to boot from USB:

boot -b *usb:/path/filename*

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

Note

If you insert the USB drive while the system is running, you will need to reboot the system before it will recognize the USB drive.

Example:

```
rommon 1 > dir usb:
rommon 2 > boot -b usb:/Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-172.sh.REL.tar
```

If you want to boot from TFTP:

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

ADDRESS=*management_ip_address*

NETMASK=*subnet_mask*

SERVER=*tftp_ip_address*

GATEWAY=*gateway_ip_address*

IMAGE=*path/filename*

set

sync

tftpdnld -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.
- **tftpdnld -b**—Loads FXOS.

Example:

Firepower 1000 and 2100 devices

```

rommon 1 > ADDRESS=10.86.118.4
rommon 2 > NETMASK=255.255.252.0
rommon 3 > SERVER=10.86.118.21
rommon 4 > GATEWAY=10.86.118.1
rommon 5 > FILE=cisco-ftd-fplk.7.4.1-172.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-fplk.7.4.1-172.SPA
  CONFIG=
  PS1="rommon ! > "

rommon 7 > sync
rommon 8 > tftpdnld -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-fplk.7.4.1-172.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-fplk.7.4.1-172.SPA from 10.86.118.21!!!!!!!!!!
[...]
```

Ping to troubleshoot connectivity to the server:

```

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

Example:

Secure Firewall 3100 devices

```

rommon 1 > show info

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

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

```

```

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

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

    ADDRESS: 172.16.0.50
    NETMASK: 255.255.255.0
    GATEWAY: 172.16.0.254
    SERVER: 172.23.37.186
    IMAGE: image_dir/Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-4.sh.REL.tar
    VERBOSITY: Progress
    RETRY: 40
    PKTTIMEOUT: 7200
    BLKSIZE: 1460
    CHECKSUM: Yes
    PORT: 10G/1
    PHYMODE: Auto Detect

.=====...
+-----+
+----- SUCCESS -----+
+-----+
|                                     |
|           LFBFF signature authentication passed !!!           |
|                                     |
+-----+
LFBFF signature verified.

```

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

Note

If you do not know your credentials, or cannot log in due to disk corruption, you should perform a factory reset using the ROMMON **factory-reset** command (see [Perform a Factory Reset from ROMMON \(Password Reset\)](#), on page 50). After performing the factory reset, restart this procedure to boot into FXOS, and log in with the default credentials (**admin/Admin123**).

Step 4 Reformat the eMMC.

connect local-mgmt

format emmc

Enter **yes**.

Example:

```

firepower-2110# connect local-mgmt
firepower-2110(local-mgmt)# format emmc
All bootable images will be lost.

```

```
Do you still want to format? (yes/no):yes
```

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

Step 5 Configure the Management interface so you can download the image from a server.

If you use USB, you can skip this step.

a) Enter the fabric-interconnect scope:

```
scope fabric-interconnect a
```

b) Set the new management IP information:

```
set out-of-band static ip ip netmask netmask gw gateway
```

c) Commit the configuration:

```
commit-buffer
```

Example:

```
firepower# scope fabric-interconnect a
firepower /fabric-interconnect # set out-of-band static ip 10.1.1.5 netmask 255.255.255.0
gw 10.1.1.1
firepower /fabric-interconnect* # commit-buffer
```

Note

If you encounter the following error, you must disable DHCP before committing the change. Follow the commands 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.]
firepower /fabric-interconnect* # exit
firepower* # scope system
firepower /system* # scope services
firepower /system/services* # disable dhcp-server
firepower /system/services* # commit-buffer
```

Step 6 Re-download and boot the threat defense package.

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

```
scope firmware
```

```
download image url
```

```
show download-task
```

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

- **ftp://username@server/[path/]image_name**

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

Example:

Firepower 1000 and 2100 devices

```
firepower-2110# scope firmware
firepower-2110 /firmware # download image tftp://10.86.118.21/cisco-ftd-fplk.7.4.1-172.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-ftd-fplk.7.4.1-172.SPA
                        Tftp      10.88.29.21          0          Downloaded
```

Example:

Secure Firewall 3100 devices

```
firepower-3110# scope firmware
firepower-3110 /firmware # download image
scp://172.23.205.217/auto/Cisco_FTD_SSP_FP3K_Upgrade_7.3.0-14.sh.REL.tar
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
firepower-3110 /firmware # show download-task
Download task:
File Name      Protocol      Server          Port      Userid      State
-----
Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-14.sh.REL.tar 7.3.0-14.sh.REL.tar
Scp            172.23.205.217 0              Downloaded
```

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

show package**scope auto-install****install security-pack version** *version*

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

Example:

Firepower 1000 and 2100 devices

```
firepower 2110 /firmware # show package
Name                                                    Package-Vers
-----
cisco-ftd-fplk.7.4.1-172.SPA                            7.4.1-172
firepower 2110 /firmware # scope auto-install
firepower 2110 /firmware/auto-install # install security-pack version 7.4.1-172
The system is currently installed with security software package not set, which has:
- The platform version: not set
```

If you proceed with the upgrade 7.4.1-172, it will do the following:

- upgrade to the new platform version 2.14.1.23
- install with CSP ftd version 7.4.1-172

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 7.4.1-172

Install started. This will take several minutes.

For monitoring the upgrade progress, please enter 'show' or 'show detail' command.

Example:

Secure Firewall 3100 devices

```
firepower 3110 /firmware # show package
Name                                     Package-Vers
-----
Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-14.sh.REL.tar 7.3.0-14
firepower 3110 /firmware # scope auto-install
firepower 3110 /firmware/auto-install # install security-pack version 7.3.0-14
The system is currently installed with security software package not set, which has:
- The platform version: not set
If you proceed with the upgrade 7.3.0-14, it will do the following:
- upgrade to the new platform version 2.13.1.89
- install with CSP ftd version 7.3.0-14
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 7.3.0-14

Install started. This will take several minutes.

For monitoring the upgrade progress, please enter 'show' or 'show detail' command.

Step 7 Wait for the chassis to finish rebooting (5-10 minutes).

Although FXOS is up, you still need to wait for the threat defense to come up (5 minutes).

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

- To reimage your Secure Firewall 3100 device to threat defense version 7.3.0, you must have ROMMON version 1.1.08 or above. If the current ROMMON version is less than 1.1.08, you must upgrade ROMMON by upgrading to ASA 9.19 or later. You can also use the management center or device manager to upgrade the threat defense version to 7.3.0 (see Threat Defense for more information).
- You must have console access for this procedure.
- Download the threat defense package to a TFTP server or a USB drive formatted as EXT2/3/4 or VFAT/FAT32.
See: <https://www.cisco.com/go/ftd-software>
- If you use USB, install the drive before you start. If you insert the USB drive while the system is running, you will need to reboot the system before it will recognize the USB drive.

Procedure

Step 1 Deregister your devices from the cloud tenant (if applicable). See [Deregister From Cloud, on page 70](#).

Step 2 Connect to the FXOS CLI from the console port.

Log in as **admin** and the admin password.

Note

If you are in the threat defense CLI context, you must first switch to the FXOS CLI context using the **connect fxos admin** command.

Step 3 Reformat the system.

connect local-mgmt

format everything

Enter **yes**, and the device reboots.

Example:

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

Step 4 Press **Esc** during the bootup when prompted to reach the ROMMON prompt. Pay close attention to the monitor.

Example:

```
*****
Cisco System ROMMON, Version 1.0.03, RELEASE SOFTWARE
Copyright (c) 1994-2017 by Cisco Systems, Inc.
Compiled Thu 04/06/2017 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 5 Boot from the threat defense package on a USB drive formatted as EXT2/3/4 or VFAT/FAT32, or boot over the network using TFTP.

If you want to boot from USB:

boot -b *usb:/path/filename*

Note

If you insert the USB drive while the system is running, you will need to reboot the system before it will recognize the USB drive.

Use the **dir usb:** command to view the disk contents.

Example:

```
rommon 1 > dir usb:
rommon 2 > boot -b usb:/Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-01.sh.REL.tar
```

If you want to boot from TFTP:

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

ADDRESS=*management_ip_address*

NETMASK=*subnet_mask*

SERVER=*tftp_ip_address*

GATEWAY=*gateway_ip_address*

IMAGE=*path/filename*

set

sync

tftpdnld -b

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.
- **tftpdnld -b**—Loads the threat defense package.

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 > IMAGE=Cisco_FTD_SSP_FP3K_Upgrade-7.3.0-01.sh.REL.tar
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_SSP_FP3K_Upgrade-7.3.0-01.sh.REL.tar
  CONFIG=
  PS1="rommon ! > "

rommon 7 > sync
rommon 8 > tftpdnld -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_SSP_FP3K_Upgrade-7.4.1-01.sh.REL.tar
      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_SSP_FP3K_Upgrade-7.4.1-01.sh.REL.tar 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 >
```

Note

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

```
firepower-2110 : <<%FPRM-2-DEFAULT_INFRA_VERSION_MISSING>>
[Fl309][critical][default-infra-version-missing][org-root/fw-infra-pack-default]
Bundle version in firmware package is empty, need to re-install

firepower-3105 FPRM: <<%FPRM-2-DEFAULT_INFRA_VERSION_MISSING>>
[Fl309][critical][default-infra-version-missing][org-root/fw-infra-pack-default]
Bundle version in firmware package is empty, need to re-install
```

This error condition clears as soon as you install the new threat defense software package version as described later in this procedure. Press **Enter** to go to the next prompt.

Step 6 Once the system comes up, log in to FXOS using the default username: **admin** and password: **Admin123**.

Step 7 Configure the Management interface so you can download the threat defense image from a server.

If you use USB, you can skip this step.

a) Enter the fabric-interconnect scope:

```
scope fabric-interconnect a
```

b) Set the new management IP information:

```
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 commands 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.]
firepower /fabric-interconnect* # exit
firepower* # scope system
firepower /system* # scope services
firepower /system/services* # disable dhcp-server
firepower /system/services* # commit-buffer
```

Step 8 Download and boot the threat defense package. Because you booted temporarily from USB or TFTP, you must still download the image to the local disk.

a) Download the package.

```
scope firmware
```

```
download image url
```

```
show download-task
```

You can download the package from the same TFTP server or USB drive you used earlier, or another server reachable on Management 1/1. Specify the URL for the file being imported using one of the following:

Note

Make sure to specify an IP address for the server and not a hostname; FXOS cannot resolve FQDNs.

```
• ftp://username@server_ip/[path/]image_name
```

- `scp://username@server_ip[/path/]image_name`
- `sftp://username@server_ip[/path/]image_name`
- `tftp://server_ip[:port]/[/path/]image_name`
- `usbA:/path/filename`

Example:

```
firepower-2110# scope firmware
firepower-2110 /firmware # download image
tftp://10.86.118.21/Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-01.sh.REL.tar
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_FTD_SSP_FP3K_Upgrade-7.4.1-01.sh.REL.tar
          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* force

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

- Step 9** After the software package is installed, continue with the setup instructions in the getting started guide for your hardware platform.

Change the Admin Password

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

Procedure

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

```
firepower-chassis # connect ftd
```

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

```
> show user
```

Example:

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

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

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

Example:

```
> configure user password admin
Enter current password:
Enter new password for user admin:
Confirm new password for user admin:
```

Change the Admin Password if Threat Defense is Offline

After reimaging your device, the admin password is reset to Admin123. You will be prompted to change the password when you first log in. If you want to change the password later, use this procedure to change the admin password to a new string if threat defense is offline or otherwise unavailable. Note that if threat defense is online, you will need to change the admin password using the threat defense CLI (see [Change the Admin Password, on page 68](#)).



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

Before you begin

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

Procedure

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

```
firepower # scope security
```

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

```
firepower /security* # set password
```

Example:

```
FPR-2120# scope security
FPR-2120# /security # set password
Enter old password:
```

```

Enter new password:
Confirm new password:
firepower-2120 /security* # commit-buffer

```

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

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

Example:

```

FPR-2120# scope security
FPR-2120 /security # show local-user
User Name      First Name      Last name
-----
admin

```

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

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

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

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

Example:

```

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

```

Step 3 Commit the configuration:

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

Deregister From Cloud

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

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

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

Before you begin

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

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

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

1. Enter the fabric interconnect scope:


```
firepower # scope fabric-interconnect
```
2. Set the new management IP information:


```
firepower /fabric-interconnect # set out-of-band static ip ip netmask netmask gateway gateway
```
3. Commit the configuration:


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

Procedure

Step 1 Connect to the local-management command shell:

```
firepower # connect local
```

Step 2 Deregister your device from the cloud:

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

Example

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

History for FXOS Troubleshooting

Feature Name	Platform Releases	Description
Packet capture for mac-filter dropped packets from switch	7.4.1	For Secure Firewall 3100 and 4200 devices, you can now capture mac-filter dropped packets from switch using the set drop mac-filter FXOS CLI command.
Switch Packet Path	7.1	You can now troubleshoot your Secure Firewall 3100 device for the switch packet path issues using the <code>portmanager</code> FXOS CLI command
Cloud deregister	6.7	You can now deregister your Firepower 1000/2100 device from your cloud tenant using the <code>cloud deregister</code> FXOS CLI command

Feature Name	Platform Releases	Description
Changing the admin password	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.