



Cisco Firepower 4100/9300 FXOS CLI Configuration Guide, 2.6(1)

First Published: 2019-03-13

Last Modified: 2020-07-02

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)

© 2019–2020 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1	Introduction to the Security Appliance	1
	About the Firepower Security Appliance	1
	How the Logical Device Works with the Firepower 4100/9300	1
	Supported Applications	2
	Monitoring Chassis Health	2

CHAPTER 2	CLI Overview	5
	Managed Objects	5
	Command Modes	5
	FXOS CLI Connects Diagram	7
	Object Commands	8
	Complete a Command	9
	Command History	9
	Commit, Discard, and View Pending Commands	9
	Inline Help for the CLI	10
	CLI Session Limits	10

CHAPTER 3	Getting Started	11
	Task Flow	11
	Initial Configuration	11
	Initial Configuration Using Console Port	12
	Low-Touch Provisioning Using Management Port	14
	Accessing the FXOS CLI	18

CHAPTER 4	License Management for the ASA	21
	About Smart Software Licensing	21

Smart Software Licensing for the ASA	21
Smart Software Manager and Accounts	22
Offline Management	22
Permanent License Reservation	22
Satellite Server	22
Licenses and Devices Managed per Virtual Account	23
Evaluation License	23
Smart Software Manager Communication	23
Device Registration and Tokens	24
Periodic Communication with the License Authority	24
Out-of-Compliance State	24
Smart Call Home Infrastructure	24
Prerequisites for Smart Software Licensing	25
Guidelines for Smart Software Licensing	25
Defaults for Smart Software Licensing	25
Configure Regular Smart Software Licensing	26
(Optional) Configure the HTTP Proxy	26
(Optional) Delete the Call Home URL	27
Register the Firepower 4100/9300 chassis with the License Authority	28
Change Cisco Success Network Enrollment	29
Configure a Smart License Satellite Server for the Firepower 4100/9300 chassis	30
Configure Permanent License Reservation	31
Install the Permanent License	31
(Optional) Return the Permanent License	32
Monitoring Smart Software Licensing	33
History for Smart Software Licensing	34
CHAPTER 5	User Management 37
	User Accounts 37
	Guidelines for Usernames 38
	Guidelines for Passwords 39
	Guidelines for Remote Authentication 40
	User Roles 42
	Password Profile for Locally Authenticated Users 42

Select the Default Authentication Service	43
Configuring the Session Timeout	45
Configuring the Absolute Session Timeout	46
Configuring the Role Policy for Remote Users	47
Enabling Password Strength Check for Locally Authenticated Users	48
Set the Maximum Number of Login Attempts	48
View and Clear User Lockout Status	49
Configuring the Maximum Number of Password Changes for a Change Interval	50
Configure Minimum Password Length Check	51
Configuring a No Change Interval for Passwords	52
Configuring the Password History Count	52
Creating a Local User Account	53
Deleting a Local User Account	56
Activating or Deactivating a Local User Account	56
Clearing the Password History for a Locally Authenticated User	57

CHAPTER 6

Image Management 59

About Image Management	59
Downloading Images from Cisco.com	60
Downloading a FXOS Software Image to the Firepower 4100/9300 chassis	60
Verifying the Integrity of an Image	62
Upgrading the FXOS Platform Bundle	63
Downloading a Logical Device Software Image to the Firepower 4100/9300 chassis	64
Updating the Image Version for a Logical Device	66
Firmware Upgrade	68

CHAPTER 7

Security Certifications Compliance 69

Security Certifications Compliance	69
Generate the SSH Host Key	70
Configure IPSec Secure Channel	71
Configure Static CRL for a Trustpoint	77
About the Certificate Revocation List Check	78
Configure CRL Periodic Download	82
Set the LDAP Key Ring Certificate	84

Enable Client Certificate Authentication 85

CHAPTER 8

System Administration 87

Changing the Management IP Address 87

Changing the Application Management IP 89

Changing the Firepower 4100/9300 Chassis Name 92

Install a Trusted Identity Certificate 92

Auto-Import Certificate Update 98

Pre-Login Banner 101

Creating the Pre-Login Banner 101

Modifying the Pre-Login Banner 102

Deleting the Pre-Login Banner 103

Rebooting the Firepower 4100/9300 Chassis 103

Powering Off the Firepower 4100/9300 Chassis 104

Restoring the Factory Default Configuration 104

Enabling Locator LED 105

CHAPTER 9

Platform Settings 107

Setting the Date and Time 107

Viewing the Configured Date and Time 108

Setting the Time Zone 108

Setting the Date and Time Using NTP 110

Deleting an NTP Server 113

Setting the Date and Time Manually 113

Configuring SSH 114

Configuring TLS 118

Configuring Telnet 120

Configuring SNMP 121

About SNMP 121

SNMP Notifications 122

SNMP Security Levels and Privileges 122

Supported Combinations of SNMP Security Models and Levels 122

SNMPv3 Security Features 123

SNMP Support 123

Enabling SNMP and Configuring SNMP Properties	124
Creating an SNMP Trap	125
Deleting an SNMP Trap	127
Creating an SNMPv3 User	128
Deleting an SNMPv3 User	130
Viewing Current SNMP Settings	130
Configuring HTTPS	131
Certificates, Key Rings, and Trusted Points	131
Creating a Key Ring	132
Regenerating the Default Key Ring	133
Creating a Certificate Request for a Key Ring	134
Creating a Certificate Request for a Key Ring with Basic Options	134
Creating a Certificate Request for a Key Ring with Advanced Options	135
Creating a Trusted Point	137
Importing a Certificate into a Key Ring	138
Configuring HTTPS	140
Changing the HTTPS Port	141
Restarting HTTPS	142
Deleting a Key Ring	143
Deleting a Trusted Point	143
Disabling HTTPS	144
Configuring AAA	144
About AAA	145
Setting Up AAA	146
Configuring LDAP Providers	147
Configuring RADIUS Providers	151
Configuring TACACS+ Providers	154
Verifying Remote AAA Server Configurations	157
Configuring Syslog	158
Configuring DNS Servers	161
Enable FIPS Mode	162
Enable Common Criteria Mode	163
Configure the IP Access List	164
Add a MAC Pool Prefix and View MAC Addresses for Container Instance Interfaces	165

Add a Resource Profile for Container Instances	167
Configure a Network Control Policy	170
Configure the Chassis URL	173
Modifying Weak Key Exchange Algorithms	174
Setting FIPS/CC Mode	174
Setting Cipher Suite	175

CHAPTER 10

Interface Management 177

About Interfaces	177
Chassis Management Interface	177
Interface Types	178
FXOS Interfaces vs. Application Interfaces	179
Hardware Bypass Pairs	181
Jumbo Frame Support	182
Shared Interface Scalability	182
Shared Interface Best Practices	183
Shared Interface Usage Examples	185
Viewing Shared Interface Resources	191
Inline Set Link State Propagation for the FTD	192
Guidelines and Limitations for Interfaces	192
Configure Interfaces	195
Configure a Physical Interface	195
Add an EtherChannel (Port Channel)	197
Add a VLAN Subinterface for Container Instances	200
Configure Breakout Cables	202
Configure a Flow Control Policy	203
Monitoring Interfaces	205
Troubleshooting Interfaces	207
History for Interfaces	213

CHAPTER 11

Logical Devices 215

About Logical Devices	215
Standalone and Clustered Logical Devices	215
Logical Device Application Instances: Container and Native	216

Container Instance Interfaces	216
How the Chassis Classifies Packets	216
Classification Examples	217
Cascading Container Instances	220
Typical Multi-Instance Deployment	221
Automatic MAC Addresses for Container Instance Interfaces	222
Container Instance Resource Management	223
Performance Scaling Factor for Multi-Instance Capability	223
Container Instances and High Availability	223
Requirements and Prerequisites for Logical Devices	223
Requirements and Prerequisites for Hardware and Software Combinations	224
Requirements and Prerequisites for Clustering	225
Requirements and Prerequisites for High Availability	226
Requirements and Prerequisites for Container Instances	227
Guidelines and Limitations for Logical Devices	228
General Guidelines and Limitations	228
Clustering Guidelines and Limitations	229
Add a Standalone Logical Device	234
Add a Standalone ASA	234
Add a Standalone FTD	240
Add a High Availability Pair	251
Add a Cluster	251
About Clustering on the Firepower 4100/9300 Chassis	252
Primary and Secondary Unit Roles	252
Cluster Control Link	252
Management Network	254
Management Interface	254
Spanned EtherChannels	254
Inter-Site Clustering	255
Add an ASA Cluster	256
Create an ASA Cluster	256
Add More Cluster Members	264
Add a FTD Cluster	265
Create a FTD Cluster	265

Add More Cluster Nodes	278
Configure Radware DefensePro	279
About Radware DefensePro	279
Prerequisites for Radware DefensePro	279
Guidelines for Service Chaining	280
Configure Radware DefensePro on a Standalone Logical Device	280
Configure Radware DefensePro on an Intra-Chassis Cluster	284
Open UDP/TCP Ports and Enable vDP Web Services	288
Configure TLS Crypto Acceleration	289
About TLS Crypto Acceleration	289
Guidelines and Limitations for TLS Crypto Acceleration	289
Enable TLS Crypto Acceleration on One Container Instance	291
View the Status of TLS Crypto Acceleration	294
Manage Logical Devices	294
Connect to the Console of the Application	294
Delete a Logical Device	296
Remove a Cluster Node	297
Delete an Application Instance that is not Associated with a Logical Device	299
Change an Interface on a FTD Logical Device	300
Change an Interface on an ASA Logical Device	301
Monitoring Logical Devices	303
Examples for Inter-Site Clustering	304
Spanned EtherChannel Routed Mode Example with Site-Specific MAC Addresses	305
Spanned EtherChannel Transparent Mode North-South Inter-Site Example	306
Spanned EtherChannel Transparent Mode East-West Inter-Site Example	307
History for Logical Devices	308

CHAPTER 12
Security Module/Engine Management 313

About FXOS Security Modules/Security Engine	313
Decommissioning a Security Module	314
Acknowledge a Security Module/Engine	314
Power-Cycling a Security Module/Engine	315
Reinitializing a Security Module/Engine	316
Acknowledge a Network Module	317

Taking a Network Module Offline or Online 317

Blade Health Monitoring 319

CHAPTER 13

Configuration Import/Export 321

About Configuration Import/Export 321

Setting an Encryption Key for Configuration Import/Export 322

Exporting an FXOS Configuration File 323

Scheduling Automatic Configuration Export 325

Setting a Configuration Export Reminder 327

Importing a Configuration File 327

CHAPTER 14

Troubleshooting 331

Packet Capture 331

Backplane Port Mappings 331

Guidelines and Limitations for Packet Capture 332

Creating or Editing a Packet Capture Session 333

Configuring Filters for Packet Capture 336

Starting and Stopping a Packet Capture Session 337

Downloading a Packet Capture File 338

Deleting Packet Capture Sessions 339

Testing Network Connectivity 340

Troubleshooting Management Interface Status 341

Determine Port Channel Status 342

Recovering from a Software Failure 344

Recovering from a Corrupted File System 349

Restoring the Factory Default Configuration when the Admin Password is Unknown 359

Disaster Recovery of a Firepower Threat Defense Cluster Member 361

Generating Troubleshooting Log Files 364

FXOS Enic Devcmd Failure Logs 366

Enabling Module Core Dumps 369

Finding the Serial Number of the Firepower 4100/9300 Chassis 370

Rebuild RAID Virtual Drive 371

Identify Issues with the SSD 373



CHAPTER 1

Introduction to the Security Appliance

- [About the Firepower Security Appliance, on page 1](#)
- [Monitoring Chassis Health, on page 2](#)

About the Firepower Security Appliance

The Cisco Firepower 4100/9300 chassis is a next-generation platform for network and content security solutions. The Firepower 4100/9300 chassis is part of the Cisco Application Centric Infrastructure (ACI) Security Solution and provides an agile, open, secure platform that is built for scalability, consistent control, and simplified management.

The Firepower 4100/9300 chassis provides the following features:

- Modular chassis-based security system—provides high performance, flexible input/output configurations, and scalability.
- Firepower Chassis Manager—graphical user interface provides streamlined, visual representation of current chassis status and simplified configuration of chassis features.
- Firepower eXtensible Operating System (FXOS) CLI—provides command-based interface for configuring features, monitoring chassis status, and accessing advanced troubleshooting features.
- FXOS REST API—allows users to programmatically configure and manage their chassis.

How the Logical Device Works with the Firepower 4100/9300

The Firepower 4100/9300 runs its own operating system on the supervisor called the Firepower eXtensible Operating System (FXOS). The on-the-box Firepower Chassis Manager provides simple, GUI-based management capabilities. You configure hardware interface settings, smart licensing (for the ASA), and other basic operating parameters on the supervisor using the FXOS CLI.

A logical device lets you run one application instance and also one optional decorator application to form a service chain. When you deploy the logical device, the supervisor downloads an application image of your choice and establishes a default configuration. You can then configure the security policy within the application operating system.

Logical devices cannot form a service chain with each other, and they cannot communicate over the backplane with each other. All traffic must exit the chassis on one interface and return on another interface to reach

another logical device. For container instances, you can share data interfaces; only in this case can multiple logical devices communicate over the backplane.

Supported Applications

You can deploy logical devices on your chassis using the following application types.

FTD

The Firepower Threat Defense provides next-generation firewall services, including stateful firewalling, routing, VPN, Next-Generation Intrusion Prevention System (NGIPS), Application Visibility and Control (AVC), URL filtering, and malware defense.

You can manage the Firepower Threat Defense using the FMC, a full-featured, multidevice manager on a separate server.

ASA

The ASA provides advanced stateful firewall and VPN concentrator functionality in one device. You can manage the ASA using one of the following managers:

- ASDM—A single device manager included on the device.
- CLI
- CDO—A cloud-based, multidevice manager.
- CSM—A multidevice manager on a separate server.

Radware DefensePro (Decorator)

You can install Radware DefensePro (vDP) to run in front of the ASA or the Firepower Threat Defense as a decorator application. vDP is a KVM-based virtual platform that provides distributed denial-of-service (DDoS) detection and mitigation capabilities on the Firepower 4100/9300. Traffic from the network must first pass through the vDP before reaching the ASA or the Firepower Threat Defense.

Monitoring Chassis Health

You can use the **show environment summary** command to view the following pieces of information that show the overall health for the Firepower 4100/9300 chassis:

- Total Power Consumption—Total power consumed in watts.
- Inlet Temperature—Ambient system temperature in Celsius.
- CPU Temperature—Processor temperature in Celsius.
- Power Supply Type—AC or DC.
- Power Supply Input Feed Status—Input status (Ok, Fault).
- Power Supply Output Status—12V output status (Ok, Fault).
- Power Supply Overall Status—Overall health of PSU (Operable, Removed, Thermal problem).

- Fan Speed RPM—Highest RPM of both fans in single fan tray.
- Fan Speed Status—Fan speed (Slow, Ok, High, Critical).
- Fan Overall Status—Overall health of Fan (Operable, Removed, Thermal problem)
- Blade Total Power Consumption—Total power consumed by security module/engine in watts.
- Blade Processor Temperature—Highest temperature in Celsius of processors on security module/engine.

Procedure

-
- Step 1** Connect to the FXOS CLI (see [Accessing the FXOS CLI, on page 18](#)).
- Step 2** Enter chassis mode:
Firepower-chassis# **scope chassis 1**
- Step 3** To view a summary of the chassis health, enter the following command:
Firepower-chassis /chassis # **show environment summary**
-

Example

```
Firepower-chassis# scope chassis 1
Firepower-chassis /chassis # show environment summary

Chassis INFO :

Total Power Consumption: 638.000000
Inlet Temperature (C): 32.000000
CPU Temperature (C): 47.000000
Last updated Time: 2017-01-05T23:34:39.115

PSU 1:
Type: AC
Input Feed Status: Ok
12v Output Status: Ok
Overall Status: Operable
PSU 2:
Type: AC
Input Feed Status: Ok
12v Output Status: Ok
Overall Status: Operable

FAN 1
Fan Speed RPM (RPM): 3168
Speed Status: Ok
Overall Status: Operable
FAN 2
Fan Speed RPM (RPM): 3388
Speed Status: Ok
Overall Status: Operable
FAN 3
Fan Speed RPM (RPM): 3168
Speed Status: Ok
```

```
Overall Status: Operable
FAN 4
Fan Speed RPM (RPM): 3212
Speed Status: Ok
Overall Status: Operable
```

```
BLADE 1:
Total Power Consumption: 216.000000
Processor Temperature (C): 58.000000
BLADE 2:
Total Power Consumption: 222.000000
Processor Temperature (C): 62.500000
```



CHAPTER 2

CLI Overview

- [Managed Objects, on page 5](#)
- [Command Modes, on page 5](#)
- [FXOS CLI Connects Diagram, on page 7](#)
- [Object Commands, on page 8](#)
- [Complete a Command, on page 9](#)
- [Command History, on page 9](#)
- [Commit, Discard, and View Pending Commands, on page 9](#)
- [Inline Help for the CLI, on page 10](#)
- [CLI Session Limits, on page 10](#)

Managed Objects

The FXOS uses a managed object model, where managed objects are abstract representations of physical or logical entities that can be managed. For example, chassis, security modules, network modules, ports, and processors are physical entities represented as managed objects, and licenses, user roles, and platform policies are logical entities represented as managed objects.

Managed objects may have one or more associated properties that can be configured.

Command Modes

The CLI is organized into a hierarchy of command modes, with 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 **up** 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.



Note

Most command modes are associated with managed objects, so you must create an object before you can access the mode associated with that object. You use **create** and **enter** commands to create managed objects for the modes being accessed. The **scope** commands do not create managed objects and can only access modes for which managed objects already exist.

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

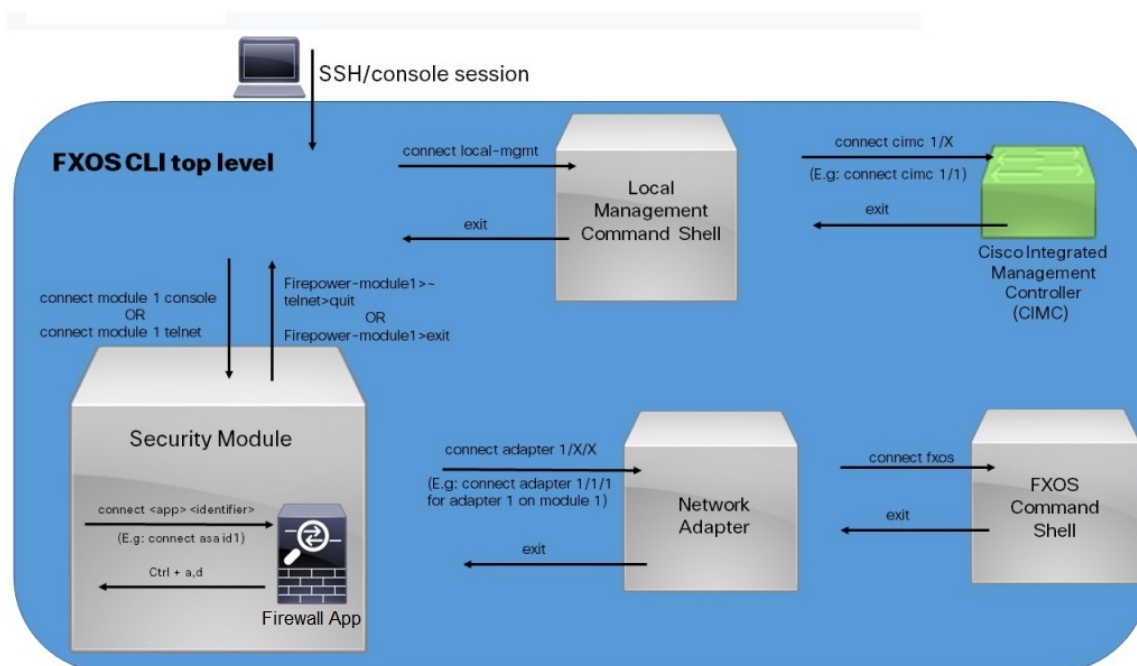
Mode Name	Commands Used to Access	Mode Prompt
EXEC	top command from any mode	#
Adapter	scope adapter command from EXEC mode	/adapter #
Cabling	scope cabling command from EXEC mode	/cabling #
Chassis	scope chassis command from EXEC mode	/chassis #
Ethernet server domain	scope eth-server command from EXEC mode; this command and all subcommands are currently not supported	/eth-server #
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 #
Host Ethernet interface	scope host-eth-if command from EXEC mode Note This command and all subcommands are not supported at this level; the Host Ethernet interface commands are available in /adapter # mode.	/host-eth-if #
License	scope license command from EXEC mode	/license #
Monitoring	scope monitoring command from EXEC mode	/monitoring #
Organization	scope org command from EXEC mode	/org #
Packet capture	scope packet-capture command from EXEC mode	/packet-capture #
Security	scope security command from EXEC mode	/security #

Mode Name	Commands Used to Access	Mode Prompt
Server	scope server command from EXEC mode	/server #
Service profile	scope service-profile command from EXEC mode Note Do not alter or configure service profiles; that is, do not use the create , set , or delete subcommand sets.	/service-profile #
SSA	scope ssa command from EXEC mode	/ssa #
System	scope system command from EXEC mode	/system #
Virtual HBA	scope vhba command from EXEC mode Note This command and all subcommands are currently not supported.	/vhba #
Virtual NIC	scope vnic command from EXEC mode	/vnic #

FXOS CLI Connects Diagram

The following diagram outlines the various commands that can be executed from the FXOS CLI top level to access the FXOS command shell, local management command shell, network adapter, CIMC, and security module CLI.

Figure 1: Firepower 4100/9300 FXOS CLI Connects Diagram



Object Commands

Four general commands are available for object management:

- **create** *object*
- **delete** *object*
- **enter** *object*
- **scope** *object*

You can use the **scope** command with any managed object, whether a permanent object or a user-instantiated object. The other commands allow you to create and manage user-instantiated objects. For every **create** *object* command, a corresponding **delete** *object* and **enter** *object* command exists.

In the management of user-instantiated objects, the behavior of these commands depends on whether the object exists, as described in the following tables:

Table 2: Command Behavior If The Object Does Not Exist

Command	Behavior
create <i>object</i>	The object is created and its configuration mode, if applicable, is entered.
delete <i>object</i>	An error message is generated.
enter <i>object</i>	The object is created and its configuration mode, if applicable, is entered.

Command	Behavior
scope <i>object</i>	An error message is generated.

Table 3: Command Behavior If The Object Exists

Command	Behavior
create <i>object</i>	An error message is generated.
delete <i>object</i>	The object is deleted.
enter <i>object</i>	The configuration mode, if applicable, of the object is entered.
scope <i>object</i>	The configuration mode of the object is entered.

Complete a Command

You can use the **Tab** key in any mode to complete a command. Partially typing a command name and pressing **Tab** causes the command to be displayed in full or to the point where you must enter another keyword or an argument value.

Command History

The CLI stores all commands used in the current session. You can step through the previously used commands by using the up-arrow or down-arrow keys. The up-arrow key moves to the previous command in the history, and the down-arrow key moves to the next command in the history. When you get to the end of the history, pressing the down-arrow key does nothing.

You can enter any command in the history again by stepping through the history to recall that command and then pressing **Enter**. The command is entered as if you had manually typed it. You can also recall a command and change it before you press **Enter**.

Commit, Discard, and View Pending Commands

When you enter a configuration command in the CLI, the command is not applied until you enter the **commit-buffer** command. Until committed, a configuration command is pending and can be discarded by entering a **discard-buffer** command.

You can accumulate pending changes in multiple command modes and apply them together with a single **commit-buffer** command. You can view the pending commands by entering the **show configuration pending** command in any command mode.



Note All pending commands are checked for validity. However, if any queued command fails during commit, the remaining commands are applied; failed commands are reported in an error message.

While any commands are pending, an asterisk (*) appears before the command prompt. The asterisk disappears when you enter the **commit-buffer** command.

The following example shows how the prompts change during the command entry process:

```
Firepower# scope system
Firepower /system # scope services
Firepower /system/services # create ntp-server 192.168.200.101
Firepower /system/services* # show configuration pending
  scope services
+   create ntp-server 192.168.200.101
  exit
Firepower /system/services* # commit-buffer
Firepower /system/services #
```

Inline Help for the CLI

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

If you have not entered anything at the prompt, entering ? lists all available commands for the mode you are in. With a partially entered command, entering ? lists all keywords and arguments available at your current position in the command syntax.

CLI Session Limits

FXOS limits the number of CLI sessions that can be active at one time to 32 total sessions. This value is not configurable.



CHAPTER 3

Getting Started

- [Task Flow, on page 11](#)
- [Initial Configuration, on page 11](#)
- [Accessing the FXOS CLI, on page 18](#)

Task Flow

The following procedure shows the basic tasks that should be completed when configuring your Firepower 4100/9300 chassis.

Procedure

- | | |
|----------------|---|
| Step 1 | Configure the Firepower 4100/9300 chassis hardware (see the Cisco Firepower Security Appliance Hardware Installation Guide). |
| Step 2 | Complete the initial configuration (see Initial Configuration, on page 11). |
| Step 3 | Set the Date and Time (see Setting the Date and Time, on page 107). |
| Step 4 | Configure a DNS server (see Configuring DNS Servers, on page 161). |
| Step 5 | Register your product license (see License Management for the ASA, on page 21). |
| Step 6 | Configure users (see User Management, on page 37). |
| Step 7 | Perform software updates as required (see Image Management, on page 59). |
| Step 8 | Configure additional platform settings (see Platform Settings, on page 107). |
| Step 9 | Configure interfaces (see Interface Management, on page 177). |
| Step 10 | Create logical devices (see Logical Devices, on page 215). |
-

Initial Configuration

Before you can use Firepower Chassis Manager or the FXOS CLI to configure and manage your system, you must perform some initial configuration tasks. You can perform the initial configuration using the FXOS CLI accessed through the console port or using SSH, HTTPS, or REST API accessed through the management port (this procedure is also referred to as low-touch provisioning).

Initial Configuration Using Console Port

The first time that you access the Firepower 4100/9300 chassis using the FXOS CLI, you will encounter a setup wizard that you can use to configure the system.



Note To repeat the initial setup, you need to erase any existing configuration using the following commands:

```
Firepower-chassis# connect local-mgmt  
firepower-chassis(local-mgmt)# erase configuration
```

You must specify only one IPv4 address, gateway, and subnet mask, or only one IPv6 address, gateway, and network prefix for the single management port on the Firepower 4100/9300 chassis. You can configure either an IPv4 or an IPv6 address for the management port IP address.

Before you begin

1. Verify the following physical connections on the Firepower 4100/9300 chassis:
 - The console port is physically connected to a computer terminal or console server.
 - The 1 Gbps Ethernet management port is connected to an external hub, switch, or router.

For more information, refer to the hardware installation guide.

2. Verify that the console port parameters on the computer terminal (or console server) attached to the console port are as follows:
 - 9600 baud
 - 8 data bits
 - No parity
 - 1 stop bit
3. Gather the following information for use with the setup script:
 - New admin password
 - Management IP address and subnet mask
 - Gateway IP address
 - Subnets from which you want to allow HTTPS and SSH access (you are prompted for "IP block" addresses)
 - Hostname and domain name
 - DNS server IP address

Procedure

Step 1 Power on the chassis.

Step 2 Connect to the serial console port using a terminal emulator.

The Firepower 4100/9300 includes an RS-232-to-RJ-45 serial console cable. You might need to use a third party serial-to-USB cable to make the connection. Use the following serial parameters:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit

Step 3 Complete the system configuration as prompted.

Note

You can optionally enter the debug menu at any time during initial configuration to debug any setup issues or abort configurations and reboot the system. To enter the debug menu, press Ctrl-C. To exit the debug menu, press Ctrl-D twice. Note that anything you type in the interim between pressing Ctrl-D the first time and pressing it a second time will run after the second time Ctrl-D is pressed.

Example:

```
---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Only minimal configuration including IP connectivity to
the FXOS Supervisor is performed through these steps.

Type Ctrl-C at any time for more options or to abort configuration
and reboot system.
To back track or make modifications to already entered values,
complete input till end of section and answer no when prompted
to apply configuration.

You have chosen to setup a new Security Appliance.
Continue? (yes/no): y

Enforce strong password? (yes/no) [y]: n

Enter the password for "admin": Farscape&32
Confirm the password for "admin": Farscape&32
Enter the system name: firepower-9300

Supervisor Mgmt IP address : 10.80.6.12

Supervisor Mgmt IPv4 netmask : 255.255.255.0

IPv4 address of the default gateway : 10.80.6.1

Do you want to configure IP block for ssh access? (yes/no) [y]: y

SSH IP block address : 10.0.0.0
```

```

SSH IPv4 block netmask : 255.0.0.0

Do you want to configure IP block for https access? (yes/no) [y]: y

HTTPS IP block address : 10.0.0.0

HTTPS IPv4 block netmask : 255.0.0.0

Configure the DNS Server IP address? (yes/no) [n]: y

DNS IP address : 10.164.47.13

Configure the default domain name? (yes/no) [n]: y

Default domain name : cisco.com

Following configurations will be applied:

Switch Fabric=A
System Name=firepower-9300
Enforced Strong Password=no
Supervisor Mgmt IP Address=10.89.5.14
Supervisor Mgmt IP Netmask=255.255.255.192
Default Gateway=10.89.5.1
SSH Access Configured=yes
    SSH IP Address=10.0.0.0
    SSH IP Netmask=255.0.0.0
HTTPS Access Configured=yes
    HTTPS IP Address=10.0.0.0
    HTTPS IP Netmask=255.0.0.0
DNS Server=72.163.47.11
Domain Name=cisco.com

Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): y
Applying configuration. Please wait... Configuration file - Ok
.....

Cisco FPR Series Security Appliance
firepower-9300 login: admin
Password: Farscape&32
Successful login attempts for user 'admin' : 1
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2019, Cisco Systems, Inc. All rights reserved.

[...]

firepower-chassis#

```

Low-Touch Provisioning Using Management Port

When your Firepower 4100/9300 chassis boots up, if it does not find the startup configuration, the device enters the Low-Touch Provisioning mode in which the device locates a Dynamic Host Control Protocol (DHCP) server and then bootstraps itself with its management interface IP address. You can then connect through the management interface to configure the system using SSH, HTTPS, or the FXOS REST API.



Note To repeat the initial setup, you need to erase any existing configuration using the following commands:

```
Firepower-chassis# connect local-mgmt  
firepower-chassis(local-mgmt)# erase configuration
```

You must specify only one IPv4 address, gateway, and subnet mask, or only one IPv6 address, gateway, and network prefix for the single management port on the Firepower 4100/9300 chassis. You can configure either an IPv4 or an IPv6 address for the management port IP address.

Before you begin

Gather the following information for use with the setup script:

- New admin password
- Management IP address and subnet mask
- Gateway IP address
- Subnets from which you want to allow HTTPS and SSH access (you are prompted for "IP block" addresses)
- Hostname and domain name
- DNS server IP address

Procedure

Step 1 Configure your DHCP server to assign an IP address to management port of the Firepower 4100/9300 chassis.

The DHCP client request from the Firepower 4100/9300 chassis will contain the following:

- The management interface's MAC address.
- DHCP option 60 (vendor-class-identifier)—Set to "FPR9300" or "FPR4100".
- DHCP option 61 (dhcp-client-identifier)—Set to the Firepower 4100/9300 chassis serial number. This serial number can be found on a pull-out tab on the chassis.

Step 2 Power on the Firepower 4100/9300 chassis.

If the startup configuration is not found when the chassis boots up, the device enters the Low-Touch Provisioning mode.

Step 3 To configure your system using HTTPS:

a) Using a supported browser, enter the following URL in the address bar:

`https://<ip_address>/api`

where *<ip_address>* is the IP address of the management port on the Firepower 4100/9300 chassis that was assigned by your DHCP server.

Note

For information on supported browsers, refer to the release notes for the version you are using (see <http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.html>).

- b) When prompted, log in with the username **install** and the password `<chassis_serial_number>`.
The `<chassis_serial_number>` can be obtained by inspecting a tag on the chassis.
- c) Complete the system configuration as prompted.
 - Strong password enforcement policy (for strong password guidelines, see [User Accounts, on page 37](#)).
 - Password for the admin account.
 - System name
 - Supervisor Management IPv4 address and subnet mask, or IPv6 address and prefix.
 - Default gateway IPv4 or IPv6 address.
 - Host/network address and netmask/prefix from which SSH access is allowed.
 - Host/network address and netmask/prefix from which HTTPS access is allowed.
 - DNS Server IPv4 or IPv6 address.
 - Default domain name.
- d) Click **Submit**.

Step 4

To configure your system using SSH:

- a) Connect to the management port using the following command:

```
ssh install@<ip_address>
```

where `<ip_address>` is the IP address of the management port on the Firepower 4100/9300 chassis that was assigned by your DHCP server.

- b) When prompted, log in with the password **Admin123**.
- c) Complete the system configuration as prompted.

Note

You can optionally enter the debug menu at any time during initial configuration to debug any setup issues or abort configurations and reboot the system. To enter the debug menu, press Ctrl-C. To exit the debug menu, press Ctrl-D twice. Note that anything you type in the interim between pressing Ctrl-D the first time and pressing it a second time will run after the second time Ctrl-D is pressed.

Example:

```
---- Basic System Configuration Dialog ----
```

```
This setup utility will guide you through the basic configuration of
the system. Only minimal configuration including IP connectivity to
the FXOS Supervisor is performed through these steps.
```

```
Type Ctrl-C at any time for more options or to abort configuration
and reboot system.
```

```
To back track or make modifications to already entered values,
complete input till end of section and answer no when prompted
to apply configuration.
```



```

You have chosen to setup a new Security Appliance.
Continue? (yes/no): y

Enforce strong password? (yes/no) [y]: n

Enter the password for "admin": Farscape&32
Confirm the password for "admin": Farscape&32
Enter the system name: firepower-9300

Supervisor Mgmt IP address : 10.80.6.12

Supervisor Mgmt IPv4 netmask : 255.255.255.0

IPv4 address of the default gateway : 10.80.6.1

Do you want to configure IP block for ssh access? (yes/no) [y]: y

SSH IP block address : 10.0.0.0

SSH IPv4 block netmask : 255.0.0.0

Do you want to configure IP block for https access? (yes/no) [y]: y

HTTPS IP block address : 10.0.0.0

HTTPS IPv4 block netmask : 255.0.0.0

Configure the DNS Server IP address? (yes/no) [n]: y

DNS IP address : 10.164.47.13

Configure the default domain name? (yes/no) [n]: y

Default domain name : cisco.com

Following configurations will be applied:

Switch Fabric=A
System Name=firepower-9300
Enforced Strong Password=no
Supervisor Mgmt IP Address=10.89.5.14
Supervisor Mgmt IP Netmask=255.255.255.192
Default Gateway=10.89.5.1
SSH Access Configured=yes
SSH IP Address=10.0.0.0
SSH IP Netmask=255.0.0.0
HTTPS Access Configured=yes
HTTPS IP Address=10.0.0.0
HTTPS IP Netmask=255.0.0.0
DNS Server=72.163.47.11
Domain Name=cisco.com

Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): y
Applying configuration. Please wait... Configuration file - Ok
.....

Initial Setup complete, Terminating sessions
.Connection to <ip_address> closed.

```

Step 5 To configure your system using the FXOS REST API:

Use the following examples for configuring the system using the REST API. For more information, see <https://developer.cisco.com/site/ssp/firepower/>.

Note

The attributes `dns`, `domain_name`, `https_net`, `https_mask`, `ssh_net`, and `ssh_mask` are optional. All other attributes are mandatory for REST API configuration.

IPv4 REST API example:

```
{
  "fxosBootstrap": {
    "dns": "1.1.1.1",
    "domain_name": "cisco.com",
    "mgmt_gw": "192.168.0.1",
    "mgmt_ip": "192.168.93.3",
    "mgmt_mask": "255.255.0.0",
    "password1": "admin123",
    "password2": "admin123",
    "strong_password": "yes",
    "system_name": "firepower-9300",
    "https_mask": "2",
    "https_net": "::",
    "ssh_mask": "0",
    "ssh_net": "::"
  }
}
```

IPv6 REST API example

```
{
  "fxosBootstrap": {
    "dns": "2001::3434:4343",
    "domain_name": "cisco.com",
    "https_mask": "2",
    "https_net": "::",
    "mgmt_gw": "2001::1",
    "mgmt_ip": "2001::2001",
    "mgmt_mask": "64",
    "password1": "admin123",
    "password2": "admin123",
    "ssh_mask": "0",
    "ssh_net": "::",
    "strong_password": "yes",
    "system_name": "firepower-9300"
  }
}
```

Accessing the FXOS CLI

You can connect to the FXOS CLI using a terminal plugged into the console port. Verify that the console port parameters on the computer terminal (or console server) attached to the console port are as follows:

- 9600 baud
- 8 data bits

- No parity
- 1 stop bit

You can also connect to the FXOS CLI using SSH and Telnet. The FXOS supports up to eight simultaneous SSH connections. To connect with SSH, you need to know the hostname or IP address of the Firepower 4100/9300 chassis.

Use one of the following syntax examples to log in with SSH, Telnet, or Putty:



Note SSH log in is case-sensitive.

From a Linux terminal using SSH:

- **ssh ucs-auth-domain \username@ {UCSM-ip-address | UCMS-ipv6-address}**

```
ssh ucs-example\jsmith@192.0.20.11
ssh ucs-example\jsmith@2001::1
```
- **ssh -l ucs-auth-domain \username {UCSM-ip-address | UCSM-ipv6-address | UCSM-host-name}**

```
ssh -l ucs-example\jsmith 192.0.20.11
ssh -l ucs-example\jsmith 2001::1
```
- **ssh {UCSM-ip-address | UCSM-ipv6-address | UCSM-host-name} -l ucs-auth-domain \username**

```
ssh 192.0.20.11 -l ucs-example\jsmith
ssh 2001::1 -l ucs-example\jsmith
```
- **ssh ucs-auth-domain \username@ {UCSM-ip-address | UCSM-ipv6-address}**

```
ssh ucs-ldap23\jsmith@192.0.20.11
ssh ucs-ldap23\jsmith@2001::1
```

From a Linux terminal using Telnet:



Note Telnet is disabled by default. See [Configuring Telnet, on page 120](#) for instructions on enabling Telnet.

- **telnet ucs-UCSM-host-name ucs-auth-domain \username**

```
telnet ucs-qa-10
login: ucs-ldap23\bladmin
```
- **telnet ucs- {UCSM-ip-address | UCSM-ipv6-address} ucs-auth-domain \username**

```
telnet 10.106.19.12 2052
ucs-qa-10-A login: ucs-ldap23\bladmin
```

From a Putty client:

- Login as: **ucs-auth-domain \username**

```
Login as: ucs-example\jsmith
```



Note If the default authentication is set to local, and the console authentication is set to LDAP, you can log in to the fabric interconnect from a Putty client using **ucs-local\admin**, where admin is the name of the local account.



CHAPTER 4

License Management for the ASA

- About Smart Software Licensing, on page 21
- Prerequisites for Smart Software Licensing, on page 25
- Guidelines for Smart Software Licensing, on page 25
- Defaults for Smart Software Licensing, on page 25
- Configure Regular Smart Software Licensing, on page 26
- Configure a Smart License Satellite Server for the Firepower 4100/9300 chassis, on page 30
- Configure Permanent License Reservation, on page 31
- Monitoring Smart Software Licensing, on page 33
- History for Smart Software Licensing, on page 34

About Smart Software Licensing

Cisco Smart Licensing is a flexible licensing model that provides you with an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across your organization. And it's secure—you control what users can access. With Smart Licensing you get:

- **Easy Activation:** Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more PAKs (Product Activation Keys).
- **Unified Management:** Cisco License Central provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.
- **License Flexibility:** Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

To use Smart Licensing, you must first set up a Smart Account on Cisco Software Central (software.cisco.com).

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide

Smart Software Licensing for the ASA

For the ASA application on the Firepower 4100/9300 chassis, Smart Software Licensing configuration is split between the Firepower 4100/9300 chassis supervisor and the application.

- Firepower 4100/9300 chassis—Configure all Smart Software Licensing infrastructure in the supervisor, including parameters for communicating with the License Authority. The Firepower 4100/9300 chassis itself does not require any licenses to operate.



Note Inter-chassis clustering requires that you enable the same Smart Licensing method on each chassis in the cluster.

- ASA Application—Configure all license entitlements in the application.



Note Cisco Transport Gateway is not supported on Firepower 4100/9300 security appliances.

Smart Software Manager and Accounts

When you purchase 1 or more licenses for the device, you manage them in the Cisco Smart Software Manager:

<https://software.cisco.com/#module/SmartLicensing>

The Smart Software Manager lets you create a master account for your organization.



Note If you do not yet have an account, click the link to [set up a new account](#). The Smart Software Manager lets you create a master account for your organization.

By default, your licenses are assigned to the *Default Virtual Account* under your master account. As the account administrator, you can optionally create additional virtual accounts; for example, you can create accounts for regions, departments, or subsidiaries. Multiple virtual accounts let you more easily manage large numbers of licenses and devices.

Offline Management

If your devices do not have Internet access, and cannot register with the License Authority, you can configure offline licensing.

Permanent License Reservation

If your devices cannot access the internet for security reasons, you can optionally request permanent licenses for each ASA. Permanent licenses do not require periodic access to the License Authority. Like PAK licenses, you will purchase a license and install the license key for the ASA. Unlike a PAK license, you obtain and manage the licenses with the Smart Software Manager. You can easily switch between regular smart licensing mode and permanent license reservation mode.

You can obtain a license that enables all features: Standard tier with maximum Security Contexts and the Carrier license. The license is managed on the Firepower 4100/9300 chassis, but you also need to request the entitlements in the ASA configuration so that the ASA allows their use.

Satellite Server

If your devices cannot access the internet for security reasons, you can optionally install a local Smart Software Manager satellite server as a virtual machine (VM). The satellite provides a subset of Smart Software Manager functionality, and allows you to provide essential licensing services for all your local devices. Only the satellite

needs to connect periodically to the main License Authority to sync your license usage. You can sync on a schedule or you can sync manually.

Once you download and deploy the satellite application, you can perform the following functions without sending data to Cisco SSM using the Internet:

- Activate or register a license
- View your company's licenses
- Transfer licenses between company entities

For more information, see the Smart Software Manager satellite installation and configuration guides on [Smart Account Manager satellite](#).

Licenses and Devices Managed per Virtual Account

Licenses and devices are managed per virtual account: only that virtual account's devices can use the licenses assigned to the account. If you need additional licenses, you can transfer an unused license from another virtual account. You can also transfer devices between virtual accounts.

Only the Firepower 4100/9300 chassis registers as a device, while the ASA applications in the chassis request their own licenses. For example, for a Firepower 9300 chassis with 3 security modules, the chassis counts as one device, but the modules use 3 separate licenses.

Evaluation License

The Firepower 4100/9300 chassis supports two types of evaluation license:

- Chassis-level evaluation mode—Before the Firepower 4100/9300 chassis registers with the Licensing Authority, it operates for 90 days (total usage) in evaluation mode. The ASA cannot request specific entitlements in this mode; only default entitlements are enabled. When this period ends, the Firepower 4100/9300 chassis becomes out-of-compliance.
- Entitlement-based evaluation mode—After the Firepower 4100/9300 chassis registers with the Licensing Authority, you can obtain time-based evaluation licenses that can be assigned to the ASA. In the ASA, you request entitlements as usual. When the time-based license expires, you need to either renew the time-based license or obtain a permanent license.



Note

You cannot receive an evaluation license for Strong Encryption (3DES/AES); only permanent licenses support this entitlement.

Smart Software Manager Communication

This section describes how your device communicates with the Smart Software Manager.

Device Registration and Tokens

For each virtual account, you can create a registration token. This token is valid for 30 days by default. Enter this token ID plus entitlement levels when you deploy each chassis, or when you register an existing chassis. You can create a new token if an existing token is expired.

At startup after deployment, or after you manually configure these parameters on an existing chassis, the chassis registers with the Cisco License Authority. When the chassis registers with the token, the License Authority issues an ID certificate for communication between the chassis and the License Authority. This certificate is valid for 1 year, although it will be renewed every 6 months.

Periodic Communication with the License Authority

The device communicates with the License Authority every 30 days. If you make changes in the Smart Software Manager, you can refresh the authorization on the device so the change takes place immediately. Or you can wait for the device to communicate as scheduled.

You can optionally configure an HTTP proxy.

The Firepower 4100/9300 chassis must have internet access either directly or through an HTTP proxy at least every 90 days. Normal license communication occurs every 30 days, but with the grace period, your device will operate for up to 90 days without calling home. After the grace period, you must contact the Licensing Authority, or you will not be able to make configuration changes to features requiring special licenses; operation is otherwise unaffected.



Note If your device is unable to communicate with the license authority for one year, the device will enter an unregistered state but will not lose any previously enabled strong encryption capabilities.

Out-of-Compliance State

The device can become out of compliance in the following situations:

- Over-utilization—When the device uses unavailable licenses.
- License expiration—When a time-based license expires.
- Lack of communication—When the device cannot reach the Licensing Authority for re-authorization.

To verify whether your account is in, or approaching, an Out-of-Compliance state, you must compare the entitlements currently in use by your Firepower 4100/9300 chassis against those in your Smart Account.

In an out-of-compliance state, you will not be able to make configuration changes to features requiring special licenses, but operation is otherwise unaffected. For example, existing contexts over the Standard license limit can continue to run, and you can modify their configuration, but you will not be able to add a *new* context.

Smart Call Home Infrastructure

By default, a Smart Call Home profile exists in the FXOS configuration that specifies the URL for the Licensing Authority. You cannot remove this profile. Note that the only configurable option for the License profile is the destination address URL for the License Authority. Unless directed by Cisco TAC, you should not change the License Authority URL.



Note Cisco Transport Gateway is not supported on Firepower 4100/9300 security appliances.

Prerequisites for Smart Software Licensing

- Note that this chapter only applies to ASA logical devices on the Firepower 4100/9300 chassis. For more information on licensing for Firepower Threat Defense logical devices, see the FMC Configuration Guide.
- Create a master account on the Cisco Smart Software Manager:
<https://software.cisco.com/#module/SmartLicensing>
If you do not yet have an account, click the link to [set up a new account](#). The Smart Software Manager lets you create a master account for your organization.
- Purchase 1 or more licenses from the [Cisco Commerce Workspace](#). On the home page, search for your platform in the **Find Products and Solutions** search field. Some licenses are free, but you still need to add them to your Smart Software Licensing account.
- Ensure internet access or HTTP proxy access from the chassis, so the chassis can contact the Licensing Authority.
- Configure a DNS server so the chassis can resolve the name of the Licensing Authority.
- Set the time for the chassis.
- Configure the Smart Software Licensing infrastructure on the Firepower 4100/9300 chassis before you configure the ASA licensing entitlements.

Guidelines for Smart Software Licensing

ASA Guidelines for Failover and Clustering

Each Firepower 4100/9300 chassis must be registered with the License Authority or satellite server. There is no extra cost for secondary units. For permanent license reservation, you must purchase separate licenses for each chassis.

Defaults for Smart Software Licensing

The Firepower 4100/9300 chassis default configuration includes a Smart Call Home profile called “SLProfile” that specifies the URL for the Licensing Authority.

```
scope monitoring
  scope callhome
    scope profile SLProfile
      scope destination SLDest
```

```
set address https://tools.cisco.com/its/service/oddce/services/DDCEService
```

Smart Licensing uses either Smart Call Home or Smart Transport as the transport mechanism to communicate with the Cisco Smart Software Manager (CSSM) server. By default, the Firepower 4100/9300 chassis uses Smart Transport as the transport mechanism.



Note If you downgrade your FXOS version to a version earlier than 2.16, Call Home becomes the default transport type.

Configure Regular Smart Software Licensing

To communicate with the Cisco License Authority, you can optionally configure an HTTP proxy. To register with the License Authority, you must enter the registration token ID in the Firepower 4100/9300 chassis. The registration token ID can be obtained from your Smart Software License account.

Procedure

-
- Step 1** (Optional) [Configure the HTTP Proxy, on page 26.](#)
 - Step 2** (Optional) [Delete the Call Home URL, on page 27](#)
 - Step 3** [Register the Firepower 4100/9300 chassis with the License Authority, on page 28.](#)
-

(Optional) Configure the HTTP Proxy

If your network uses an HTTP proxy for internet access, you must configure the proxy address for Smart Software Licensing. This proxy is also used for Smart Transport and Smart Call Home in general.



Note HTTP proxy with authentication is not supported.

Procedure

-
- Step 1** (For Call home): Enable the HTTP proxy:
 - a) Enter **scope monitoring** mode:
scope license
 - b) Enter **scope callhome** mode:
scope callhome

Example:

```
scope monitoring
scope callhome
```

Step 2 Set the proxy URL:

set http-proxy-server-url *url*

Here, *url* is the http or https address of the proxy server.

Example:

```
set http-proxy-server-url https://10.1.1.1
```

Step 3 Set the port:

set http-proxy-server-port *port*

Example:

```
set http-proxy-server-port 443
```

Step 4 Enable the HTTP proxy server. (Use this command for enabling or disabling the HTTP proxy):

set http-proxy-server-enable {on | off}

Example:

```
set http-proxy-server-enable on
```

Step 5 Commit the buffer:

commit-buffer

(Optional) Delete the Call Home URL

Use the following procedure to delete a previously configured Call Home URL.

Procedure

Step 1 Enter the monitoring scope:

scope monitoring

Step 2 Enter the callhome scope:

scope callhome

Step 3 Look for the SLProfile:

scope profile SLProfile

Step 4 Show the destination:

show destination

Example:

```
SLDest https https://tools.cisco.com/its/oddce/services/DDCEService
```

Step 5 Delete the URL:

delete destination SLDest

Step 6 Commit the buffer:

commit-buffer

Register the Firepower 4100/9300 chassis with the License Authority

When you register the Firepower 4100/9300 chassis, the License Authority issues an ID certificate for communication between the Firepower 4100/9300 chassis and the License Authority. It also assigns the Firepower 4100/9300 chassis to the appropriate virtual account. Normally, this procedure is a one-time instance. However, you might need to later re-register the Firepower 4100/9300 chassis if the ID certificate expires because of a communication problem, for example.

Procedure

Step 1 In the Smart Software Manager or the Smart Software Manager Satellite, request and copy a registration token for the virtual account to which you want to add this Firepower 4100/9300 chassis.

For more information on how to request a registration token using the Smart Software Manager Satellite, see (<https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html>).

Step 2 Enter the registration token on the Firepower 4100/9300 chassis:

scope license

register idtoken *id-token*

Example:

```
scope license
  register idtoken ZGFmNWM5NjgtYmNjYS00ZWl3L
WE3NGItMWJkOGExZjIxNGQ0LTE0NjI2NDYx%0AMDIzNT
V8N3R0dXMlZ0NjWkdPR214eFZhMldBOS9CVnNEYnVKM1
g3R3dvemRD%0AY29NQTO%3D%0A
```

Step 3 To later unregister the device, enter:

scope license

deregister

Deregistering the Firepower 4100/9300 chassis removes the device from your account. All license entitlements and certificates on the device are removed. You might want to deregister to free up a license for a new Firepower 4100/9300 chassis. Alternatively, you can remove the device from the Smart Software Manager.

Step 4 To renew the ID certificate and update the entitlements on all security modules, enter:

scope license

scope licdebug

renew

By default, the ID certificate is automatically renewed every 6 months, and the license entitlement is renewed every 30 days. You might want to manually renew the registration for either of these items if you have a limited window for Internet access, or if you make any licensing changes in the Smart Software Manager.

Change Cisco Success Network Enrollment

You enable Cisco Success Network when you register the Firepower 4100/9300 with the Cisco Smart Software Manager. After that, use the following procedure to view or change enrollment status.



Note Cisco Success Network does not work in evaluation mode.

Procedure

Step 1 Enter the system scope.

scope system

Example:

```
Firepower# scope system
Firepower /system #
```

Step 2 Enter the services scope.

scope services

Example:

```
Firepower /system # scope services
Firepower /system/services #
```

Step 3 Enter the telemetry scope.

scope telemetry

Example:

```
Firepower /system/services # scope telemetry
Firepower /system/services/telemetry #
```

Step 4 Enable or disable the Cisco Success Network feature.

{enable | disable}

Example:

```
Firepower /system/services/telemetry # enable
```

Step 5

Verify the Cisco Success Network status in the Firepower 4100/9300 Chassis.

show detail

Example:

Verify that the **Admin State** shows the correct status of Cisco Success Network.

```
Telemetry:
  Admin State: Enabled
  Oper State: Registering
  Error Message:
  Period: 86400
  Current Task: Registering the device for Telemetry
  (FSM-STAGE:sam:dme:CommTelemetryDataExchSeq:RegisterforTelemetry)
```

Example:

Verify that the **Oper State** shows **OK**, which indicates that telemetry data is sent.

```
Telemetry:
  Admin State: Enabled
  Oper State: Ok
  Error Message:
  Period: 86400
  Current Task:
```

Configure a Smart License Satellite Server for the Firepower 4100/9300 chassis

The following procedure shows how to configure the Firepower 4100/9300 chassis to use a Smart License satellite server.

Before you begin

- Complete all prerequisites listed in the [Prerequisites for Smart Software Licensing, on page 25](#).
- Deploy and set up a Smart Software Satellite Server:
Download the [Smart License Satellite](#) OVA file from Cisco.com and install and configure it on a VMwareESXi server. For more information, see the [Smart Software Manager satellite Install Guide](#).
- Verify that the FQDN of the Smart License Satellite can be resolved by your internal DNSserver.
- Verify whether the satellite trustpoint is already present:

scope security

show trustpoint

Note that the trustpoint is added by default in FXOS version 2.4(1) and later. If the trustpoint is not present, you must add one manually using the following steps:

1. Go to <http://www.cisco.com/security/pki/certs/clrca.cer> and copy the entire body of the SSL certificate (from "-----BEGIN CERTIFICATE-----" to "-----END CERTIFICATE-----") into a place you can access during configuration.
2. Enter security mode:
scope security
3. Create and name a trusted point:
create trustpoint *trustpoint_name*
4. Specify certificate information for the trust point. Note: the certificate must be in Base64 encoded X.509 (CER) format.
set certchain *certchain*

For the *certchain* variable, paste the certificate text that you copied in step 1.

If you do not specify certificate information in the command, you are prompted to enter a certificate or a list of trust points defining a certification path to the root certificate authority (CA). On the next line following your input, type **ENDOFBUF** to finish.
5. Commit the configuration:
commit-buffer

Configure Permanent License Reservation

You can assign a permanent license to your Firepower 4100/9300 chassis. This universal reservation allows you to use any entitlement for an unlimited count on your device.



Note Before you begin, you must purchase the permanent licenses so they are available in the Smart Software Manager. Not all accounts are approved for permanent license reservation. Make sure you have approval from Cisco for this feature before you attempt to configure it.

Install the Permanent License

The following procedure shows how to assign a permanent license to your Firepower 4100/9300 chassis.

Procedure

- | | |
|---------------|---|
| Step 1 | From the FXOS CLI, enable license reservation:
scope license
enable reservation |
| Step 2 | Scope to the license reservation: |

scope license

scope reservation

Step 3 Generate a reservation request code:

request universal

show license resvcode

Step 4 Go to the Smart Software Manager Inventory screen in the Cisco Smart Software Manager portal, and click the **Licenses** tab:

<https://software.cisco.com/#SmartLicensing-Inventory>

The **Licenses** tab displays all existing licenses related to your account, both regular and permanent.

Step 5 Click **License Reservation**, and type the generated reservation request code into the box.

Step 6 Click **Reserve License**.

The Smart Software Manager generates an authorization code. You can download the code or copy it to the clipboard. At this point, the license is now in use according to the Smart Software Manager.

If you do not see the **License Reservation** button, then your account is not authorized for permanent license reservation. In this case, you should disable permanent license reservation and re-enter the regular smart license commands.

Step 7 In the FXOS CLI, enter the licensing scope:

scope license

Step 8 Enter the reservation scope:

scope reservation

Step 9 Enter the authorization code:

install code

Your Firepower 4100/9300 chassis is now fully licensed with PLR.

Step 10 Enable feature entitlements on the ASA logical device. See the [ASA licensing chapter](#) to enable entitlements.

(Optional) Return the Permanent License

If you no longer need a permanent license, you must officially return it to the Smart Software Manager using this procedure. If you do not follow all steps, the license stays in an in-use state and cannot be used elsewhere.

Procedure

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

scope license

Step 2 Enter the reservation scope:

scope reservation

Step 3 Return the permanent license:

return

The Firepower 4100/9300 chassis immediately becomes unlicensed and moves to the Evaluation state.

Step 4 View and copy the return reservation code:

show license resvcode

Step 5 View and copy the FXOS universal device identifier (UDI) so you can find your FXOS instance in the Smart Software Manager:

show license udi

Step 6 Go to the Smart Software Manager Inventory screen, and click on the **Product Instances** tab:

<https://software.cisco.com/#SmartLicensing-Inventory>

Step 7 Search for your Firepower 4100/9300 chassis using its universal device identifier (UDI).

Step 8 Choose **Actions > Remove**, and type the generated return reservation code into the box.

Step 9 Click **Remove Product Instance**.

The permanent license is returned to the available pool.

Step 10 Reboot the system. For details on how to reboot your Firepower 4100/9300 chassis, see [Rebooting the Firepower 4100/9300 Chassis, on page 103](#).

Monitoring Smart Software Licensing

See the following commands for viewing license status:

- **show license all**

Displays the state of Smart Software Licensing, Smart Agent version, UDI information, Smart Agent state, global compliance status, the entitlements status, licensing certificate information and schedule Smart Agent tasks.

**Note**

Migration from QuoVadis Root CA 2 to the IdenTrust Commercial Root CA 1 for SSL certificates affects smart licensing of FXOS. For FXOS 2.8.x or later, the issue can be resolved using the auto-import feature without an upgrade to the FXOS software. For devices that run any version of FXOS software, the issue can be resolved using the manual certificate import procedure without an upgrade to the FXOS software. For more information, see [FXOS: QuoVadis Root CA 2 Decommission Might Affect Smart Licensing](#).

- **show license status**
- **show license techsupport**

History for Smart Software Licensing

Feature Name	Releases	Description
Smart Licensing using Smart Transport	2.16	<p>Smart Transport is the new transport mechanism used by Smart Licensing to communicate with the Cisco Smart Software Manager (CSSM) server. Smart Transport uses a direct URL to send Smart License messages to the CSSM server. In Firepower 4100/9300 chassis, the transport type is set to Smart Transport by default. You can change it to Call Home from the FXOS CLI.</p> <p>New and modified commands: scope transport, set transport, set transport smart, set transport-url, set transport callhome, show license transport.</p>
Cisco Success Network	2.7.1	<p>Cisco Success Network is a user-enabled cloud service. When you enable Cisco Success Network, a secure connection is established between the Firepower 4100/9300 chassis and the Cisco cloud to stream usage information and statistics. Streaming telemetry provides a mechanism that selects data of interest from the ASA and transmits it in a structured format to remote management stations to do the following:</p> <ul style="list-style-type: none"> • Inform you of available unused features that can improve the effectiveness of the product in your network • Inform you of additional technical support services and monitoring that might be available for your product • Help Cisco improve our products <p>Once you enroll in the Cisco Success Network, the chassis establishes and maintains the secure connection at all times. You can turn off this connection at any time by disabling Cisco Success Network, which disconnects the device from the Cisco Success Network cloud.</p> <p>We introduced the following commands:</p> <p>scope telemetry {enable disable}</p> <p>We introduced the following screens:</p> <p>System > Licensing > Cisco Success Network</p>

Feature Name	Releases	Description
Cisco Smart Software Licensing for the Firepower 4100/9300 chassis	1.1(1)	<p>Smart Software Licensing lets you purchase and manage a pool of licenses. Smart licenses are not tied to a specific serial number. You can easily deploy or retire devices without having to manage each unit's license key. Smart Software Licensing also lets you see your license usage and needs at a glance. Smart Software Licensing configuration is split between the Firepower 4100/9300 chassis supervisor and the security module.</p> <p>We introduced the following commands: deregister, register idtoken, renew, scope callhome, scope destination, scope licdebug, scope license, scope monitoring, scope profile, set address, set http-proxy-server-enable on, set http-proxy-server-url, set http-proxy-server-port, show license all, show license status, show license techsupport</p>



CHAPTER 5

User Management

- [User Accounts, on page 37](#)
- [Guidelines for Usernames, on page 38](#)
- [Guidelines for Passwords, on page 39](#)
- [Guidelines for Remote Authentication, on page 40](#)
- [User Roles, on page 42](#)
- [Password Profile for Locally Authenticated Users, on page 42](#)
- [Select the Default Authentication Service, on page 43](#)
- [Configuring the Session Timeout, on page 45](#)
- [Configuring the Absolute Session Timeout, on page 46](#)
- [Configuring the Role Policy for Remote Users, on page 47](#)
- [Enabling Password Strength Check for Locally Authenticated Users, on page 48](#)
- [Set the Maximum Number of Login Attempts, on page 48](#)
- [View and Clear User Lockout Status, on page 49](#)
- [Configuring the Maximum Number of Password Changes for a Change Interval, on page 50](#)
- [Configure Minimum Password Length Check, on page 51](#)
- [Configuring a No Change Interval for Passwords, on page 52](#)
- [Configuring the Password History Count, on page 52](#)
- [Creating a Local User Account, on page 53](#)
- [Deleting a Local User Account, on page 56](#)
- [Activating or Deactivating a Local User Account, on page 56](#)
- [Clearing the Password History for a Locally Authenticated User, on page 57](#)

User Accounts

User accounts are used to access the system. You can configure up to 48 local user accounts. Each user account must have a unique username and password.

Admin Account

The admin account is a default user account and cannot be modified or deleted. This account is the system administrator or superuser account and has full privileges. There is no default password assigned to the admin account; you must choose the password during the initial system setup.

The admin account is always active and does not expire. You cannot configure the admin account as inactive.

Locally Authenticated User Accounts

A locally authenticated user account is authenticated directly through the chassis and can be enabled or disabled by anyone with admin or AAA privileges. Once a local user account is disabled, the user cannot log in. Configuration details for disabled local user accounts are not deleted by the database. If you reenable a disabled local user account, the account becomes active again with the existing configuration.

Remotely Authenticated User Accounts

A remotely authenticated user account is any user account that is authenticated through LDAP, RADIUS, or TACACS+ . All remote users are initially assigned the **Read-Only** role by default.

If a user maintains a local user account and a remote user account simultaneously, the roles defined in the local user account override those maintained in the remote user account.

The fallback authentication method is to use the local database. This fallback method is not configurable.



Note When remote authentication is set as the default authentication method, you cannot log in to Firepower Chassis Manager with the local user account, even though, local authentication is set, by default, as the fallback authentication method in case the remote authentication server becomes unavailable. Thus, you cannot use local and remote user account interchangeably.

See the following topics for more information on guidelines for remote authentication, and how to configure and delete remote authentication providers:

- [Guidelines for Remote Authentication, on page 40](#)
- [Configuring LDAP Providers, on page 147](#)
- [Configuring RADIUS Providers, on page 151](#)
- [Configuring TACACS+ Providers, on page 154](#)

Expiration of User Accounts

You can configure user accounts to expire at a predefined time. When the expiration time is reached, the user account is disabled.

By default, user accounts do not expire.

After you configure a user account with an expiration date, you cannot reconfigure the account to not expire. You can, however, configure the account with the latest expiration date available.

Guidelines for Usernames

The username is also used as the login ID for Firepower Chassis Manager and the FXOS CLI. When you assign login IDs to user accounts, consider the following guidelines and restrictions:

- The login ID can contain between 1 and 32 characters, including the following:
 - Any alphabetic character
 - Any digit

- _ (underscore)
 - - (dash)
 - . (dot)
-
- The login ID must be unique.
 - The login ID must start with an alphabetic character. It cannot start with a number or a special character, such as an underscore.
 - The login ID is case-sensitive.
 - You cannot create an all-numeric login ID.
 - After you create a user account, you cannot change the login ID. You must delete the user account and create a new one.

Guidelines for Passwords

A password is required for each locally authenticated user account. A user with admin or AAA privileges can configure the system to perform a password strength check on user passwords. If the password strength check is enabled, each user must have a strong password.

We recommend that each user have a strong password. If you enable the password strength check for locally authenticated users, the FXOS rejects any password that does not meet the following requirements:

- Must contain a minimum of 8 characters and a maximum of 80 characters.



Note

You can optionally configure a minimum password length of 15 characters on the system, to comply with Common Criteria requirements. For more information, see [Configure Minimum Password Length Check, on page 51](#).

- Must include at least one uppercase alphabetic character.
- Must include at least one lowercase alphabetic character.
- Must include at least one non-alphanumeric (special) character.
- Must not contain a space.
- Must not contain a character that is repeated more than 3 times consecutively, such as aaabbb.
- Must not contain three consecutive numbers or letters in any order, such as passwordABC or password321.
- Must not be identical to the username or the reverse of the username.
- Must pass a password dictionary check. For example, the password must not be based on a standard dictionary word.
- Must not contain the following symbols: \$ (dollar sign), ? (question mark), and = (equals sign).



Note This restriction applies whether the password strength check is enabled or not.

- Must not be blank for local user and admin accounts.

Guidelines for Remote Authentication

If a system is configured for one of the supported remote authentication services, you must create a provider for that service to ensure that the Firepower 4100/9300 chassis can communicate with the system. The following guidelines impact user authorization:

User Accounts in Remote Authentication Services

User accounts can exist locally in the Firepower 4100/9300 chassis or in the remote authentication server.

You can view the temporary sessions for users who log in through remote authentication services from the Firepower Chassis Manager or the FXOS CLI.

User Roles in Remote Authentication Services

If you create user accounts in the remote authentication server, you must ensure that the accounts include the roles those users require for working in the Firepower 4100/9300 chassis and that the names of those roles match the names used in FXOS. Based on the role policy, a user might not be allowed to log in, or is granted only read-only privileges.

User Attributes in Remote Authentication Providers

For RADIUS and TACACS+ configurations, you must configure a user attribute for the Firepower 4100/9300 chassis in each remote authentication provider through which users log in to Firepower Chassis Manager or the FXOS CLI. This user attribute holds the roles and locales assigned to each user.

When a user logs in, FXOS does the following:

1. Queries the remote authentication service.
2. Validates the user.
3. If the user is validated, checks the roles and locales assigned to that user.

The following table contains a comparison of the user attribute requirements for the remote authentication providers supported by FXOS:

Authentication Provider	Custom Attribute	Schema Extension	Attribute ID Requirements
LDAP	Optional	<p>You can choose to do one of the following:</p> <ul style="list-style-type: none"> Do not extend the LDAP schema and configure an existing, unused attribute that meets the requirements. Extend the LDAP schema and create a custom attribute with a unique name, such as CiscoAVPair. 	<p>The Cisco LDAP implementation requires a unicode type attribute.</p> <p>If you choose to create the CiscoAVPair custom attribute, use the following attribute ID: 1.3.6.1.4.1.9.287247.1</p> <p>A sample OID is provided in the following section.</p>
RADIUS	Optional	<p>You can choose to do one of the following:</p> <ul style="list-style-type: none"> Do not extend the RADIUS schema and use an existing, unused attribute that meets the requirements. Extend the RADIUS schema and create a custom attribute with a unique name, such as cisco-avpair. 	<p>The vendor ID for the Cisco RADIUS implementation is 009 and the vendor ID for the attribute is 001.</p> <p>The following syntax example shows how to specify multiples user roles and locales if you choose to create the cisco-avpair attribute:</p> <pre>shell:roles="admin,aaa" shell:locales="L1,abc". Use a comma "," as the delimiter to separate multiple values.</pre>
TACACS+	Required	You must extend the schema and create a custom attribute with the name cisco-av-pair.	<p>The cisco-av-pair name is the string that provides the attribute ID for the TACACS+ provider.</p> <p>The following syntax example shows how to specify multiples user roles and locales when you create the cisco-av-pair attribute:</p> <pre>cisco-av-pair=shell:roles="admin aaa" shell:locales*"L1 abc". Using an asterisk (*) in the cisco-av-pair attribute syntax flags the locale as optional, preventing authentication failures for other Cisco devices that use the same authorization profile. Use a space as the delimiter to separate multiple values.</pre>

Sample OID for LDAP User Attribute

The following is a sample OID for a custom CiscoAVPair attribute:

```
CN=CiscoAVPair,CN=Schema,
CN=Configuration,CN=X
objectClass: top
objectClass: attributeSchema
cn: CiscoAVPair
distinguishedName: CN=CiscoAVPair,CN=Schema,CN=Configuration,CN=X
instanceType: 0x4
uSNCreated: 26318654
attributeID: 1.3.6.1.4.1.9.287247.1
attributeSyntax: 2.5.5.12
isSingleValued: TRUE
showInAdvancedViewOnly: TRUE
adminDisplayName: CiscoAVPair
adminDescription: UCS User Authorization Field
oMSyntax: 64
LDAPDisplayName: CiscoAVPair
name: CiscoAVPair
objectCategory: CN=Attribute-Schema,CN=Schema,CN=Configuration,CN=X
```

User Roles

The system contains the following user roles:

Administrator

Complete read-and-write access to the entire system. The default admin account is assigned this role by default and it cannot be changed.

Read-Only

Read-only access to system configuration with no privileges to modify the system state.

Operations

Read-and-write access to NTP configuration, Smart Call Home configuration for Smart Licensing, and system logs, including syslog servers and faults. Read access to the rest of the system.

AAA Administrator

Read-and-write access to users, roles, and AAA configuration. Read access to the rest of the system.

Password Profile for Locally Authenticated Users

The password profile contains the password history and password change interval properties for all locally authenticated users. You cannot specify a different password profile for each locally authenticated user.

Password History Count

The password history count allows you to prevent locally authenticated users from reusing the same password over and over again. When this property is configured, the Firepower chassis stores passwords that were previously used by locally authenticated users up to a maximum of 15 passwords. The passwords are stored in reverse chronological order with the most recent password first to ensure that the only the oldest password can be reused when the history count threshold is reached.

A user must create and use the number of passwords configured in the password history count before being able to reuse one. For example, if you set the password history count to 8, a locally authenticated user cannot reuse the first password until after the ninth password has expired.

By default, the password history is set to 0. This value disables the history count and allows users to reuse previously passwords at any time.

If necessary, you can clear the password history count for a locally authenticated user and enable reuse of previous passwords.

Password Change Interval

The password change interval enables you to restrict the number of password changes a locally authenticated user can make within a given number of hours. The following table describes the two configuration options for the password change interval.

Interval Configuration	Description	Example
No password change allowed	<p>This option does not allow passwords for locally authenticated users to be changed within a specified number of hours after a password change.</p> <p>You can specify a no change interval between 1 and 745 hours. By default, the no change interval is 24 hours.</p>	<p>For example, to prevent passwords from being changed within 48 hours after a locally authenticated user changes his or her password, set the following:</p> <ul style="list-style-type: none"> • Change during interval to disable • No change interval to 48
Password changes allowed within change interval	<p>This option specifies the maximum number of times that passwords for locally authenticated users can be changed within a pre-defined interval.</p> <p>You can specify a change interval between 1 and 745 hours and a maximum number of password changes between 0 and 10. By default, a locally authenticated user is permitted a maximum of 2 password changes within a 48 hour interval.</p>	<p>For example, to allow a password to be changed a maximum of once within 24 hours after a locally authenticated user changes his or her password, set the following:</p> <ul style="list-style-type: none"> • Change during interval to enable • Change count to 1 • Change interval to 24

Select the Default Authentication Service

Procedure

-
- Step 1** Enter security mode:
Firepower-chassis # **scope security**
- Step 2** Enter default authorization security mode:
Firepower-chassis /security # **scope default-auth**

Step 3 Specify the default authentication:

Firepower-chassis /security/default-auth # **set realm** *auth-type*

where *auth-type* is one of the following keywords:

- **ldap**—Specifies LDAP authentication
- **local**—Specifies local authentication
- **none**—Allows local users to log on without specifying a password
- **radius**—Specifies RADIUS authentication
- **tacacs**—Specifies TACACS+ authentication

Note

If Default Authentication and Console Authentication are both set to use the same remote authentication protocol (RADIUS, TACACS+, or LDAP), you cannot change certain aspects of that server's configuration (for example, deleting that server, or changing its order of assignment) without updating these user settings.

Step 4 (Optional) Specify the associated provider group, if any:

Firepower-chassis /security/default-auth # **set auth-server-group** *auth-serv-group-name*

Step 5 (Optional) Specify the maximum amount of time allowed between refresh requests for a user in this domain:

Firepower-chassis /security/default-auth # **set refresh-period** *seconds*

Specify an integer between 0 and 600. The default is 600 seconds.

If this time limit is exceeded, FXOS considers the web session to be inactive, but it does not terminate the session.

Step 6 (Optional) Specify the maximum amount of time that can elapse after the last refresh request before FXOS considers a web session to have ended:

Firepower-chassis /security/default-auth # **set session-timeout** *seconds*

Specify an integer between 0 and 600. The default is 600 seconds.

Note

If you set two-factor authentication for a RADIUS or TACACS+ realm, consider increasing the **session-refresh** and **session-timeout** periods so that remote users do not have to reauthenticate too frequently.

Step 7 (Optional) Set the authentication method to two-factor authentication for the realm:

Firepower-chassis /security/default-auth # **set use-2-factor** **yes**

Note

Two-factor authentication applies only to the RADIUS and TACACS+ realms.

Step 8 Commit the transaction to the system configuration:

commit-buffer

Example

The following example sets the default authentication to RADIUS, the default authentication provider group to provider1, enables two-factor authentications, sets the refresh period to 300 seconds (5 minutes), the session timeout period to 540 seconds (9 minutes), and enables two-factor authentication. It then commits the transaction.

```
Firepower-chassis# scope security
Firepower-chassis /security # scope default-auth
Firepower-chassis /security/default-auth # set realm radius
Firepower-chassis /security/default-auth* # set auth-server-group provider1
Firepower-chassis /security/default-auth* # set use-2-factor yes
Firepower-chassis /security/default-auth* # set refresh-period 300
Firepower-chassis /security/default-auth* # set session-timeout 540
Firepower-chassis /security/default-auth* # commit-buffer
Firepower-chassis /security/default-auth #
```

Configuring the Session Timeout

You can use the FXOS CLI to specify the amount of time that can pass without user activity before the Firepower 4100/9300 chassis closes user sessions. You can configure different settings for console sessions and for HTTPS, SSH, and Telnet sessions.

You can set a timeout value up to 3600 seconds (60 minutes). The default value is 600 seconds. To disable this setting, set the session timeout value to 0.



Note If the refresh-period is not set to zero while setting the session timeout value to 0, an error message `Update failed:[For Default Authentication, Refresh Period cannot be greater than Session Timeout]` will be displayed. This is because you must first set refresh-period to 0 and then the session-timeout to 0.

Procedure

-
- Step 1** Enter security mode:
Firepower-chassis # **scope security**
 - Step 2** Enter default authorization security mode:
Firepower-chassis /security # **scope default-auth**
 - Step 3** Set the idle timeout for HTTPS, SSH, and Telnet sessions:
Firepower-chassis /security/default-auth # **set session-timeout** *seconds*
 - Step 4** (Optional) Set the idle timeout for console sessions:
Firepower-chassis /security/default-auth # **set con-session-timeout** *seconds*
 - Step 5** Commit the transaction to the system configuration:

```
Firepower-chassis /security/default-auth # commit-buffer
```

Step 6 (Optional) View the session and absolute session timeout settings:

```
Firepower-chassis /security/default-auth # show detail
```

Example:

```
Default authentication:
  Admin Realm: Local
  Operational Realm: Local
  Web session refresh period(in secs): 600
  Idle Session timeout (in secs) for web, ssh, telnet sessions: 600
  Absolute Session timeout (in secs) for web, ssh, telnet sessions: 3600
  Serial Console Session timeout(in secs): 600
  Serial Console Absolute Session timeout(in secs): 3600
  Admin Authentication server group:
  Operational Authentication server group:
  Use of 2nd factor: No
```

Configuring the Absolute Session Timeout

The Firepower 4100/9300 chassis has an absolute session timeout setting that closes user sessions after the absolute session timeout period has passed, regardless of session use. This absolute timeout functionality is global across all forms of access including serial console, SSH, and HTTPS.

You can separately configure the absolute session timeout for serial console sessions. This allows for disabling the serial console absolute session timeout for debugging needs while maintaining the timeout for other forms of access.

The absolute timeout value defaults to 3600 seconds (60 minutes) and can be changed using the FXOS CLI. To disable this setting, set the absolute session timeout value to 0.

Procedure

Step 1 Enter security mode:

```
Firepower-chassis # scope security
```

Step 2 Enter default authorization security mode:

```
Firepower-chassis /security # scope default-auth
```

Step 3 Set the absolute session timeout:

```
Firepower-chassis /security/default-auth # set absolute-session-timeout seconds
```

Step 4 (Optional) Set a separate console absolute session timeout:

```
Firepower-chassis /security/default-auth # set con-absolute-session-timeout seconds
```

Step 5 Commit the transaction to the system configuration:

```
Firepower-chassis /security/default-auth # commit-buffer
```

Step 6 (Optional) View the session and absolute session timeout settings:

Firepower-chassis /security/default-auth # **show detail**

Example:

```
Default authentication:
Admin Realm: Local
Operational Realm: Local
Web session refresh period(in secs): 600
Idle Session timeout (in secs) for web, ssh, telnet sessions: 600
Absolute Session timeout (in secs) for web, ssh, telnet sessions: 3600
Serial Console Session timeout(in secs): 600
Serial Console Absolute Session timeout(in secs): 3600
Admin Authentication server group:
Operational Authentication server group:
Use of 2nd factor: No
```

Configuring the Role Policy for Remote Users

By default, read-only access is granted to all users logging in to Firepower Chassis Manager or the FXOS CLI from a remote server using the LDAP, RADIUS, or TACACS+ protocols. For security reasons, it might be desirable to restrict access to those users matching an established user role.

You can configure the role policy for remote users in the following ways:

assign-default-role

When a user attempts to log in and the remote authentication provider does not supply a user role with the authentication information, the user is allowed to log in with a read-only user role.

This is the default behavior.

no-login

When a user attempts to log in and the remote authentication provider does not supply a user role with the authentication information, access is denied.

Procedure

Step 1 Enter security mode:

Firepower-chassis # **scope security**

Step 2 Specify whether user access to Firepower Chassis Manager and the FXOS CLI should be restricted based on user roles:

Firepower-chassis /security # **set remote-user default-role** {**assign-default-role** | **no-login**}

Step 3 Commit the transaction to the system configuration:

Firepower-chassis /security # **commit-buffer**

Example

The following example sets the role policy for remote users and commits the transaction:

```
Firepower-chassis# scope security
Firepower-chassis /security # set remote-user default-role no-login
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

Enabling Password Strength Check for Locally Authenticated Users

If the password strength check is enabled, the FXOS does not permit a user to choose a password that does not meet the guidelines for a strong password (see [Guidelines for Passwords, on page 39](#)).

Procedure

Step 1 Enter security mode:

```
Firepower-chassis # scope security
```

Step 2 Specify whether the password strength check is enabled or disabled:

```
Firepower-chassis /security # set enforce-strong-password {yes | no}
```

Example

The following example enables the password strength check:

```
Firepower-chassis# scope security
Firepower-chassis /security # set enforce-strong-password yes
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

Set the Maximum Number of Login Attempts

You can configure the maximum number of failed login attempts allowed before a user is locked out of the Firepower 4100/9300 chassis for a specified amount of time. If a user exceeds the set maximum number of login attempts, the user is locked out of the system. No notification appears indicating that the user is locked out. In this event, the user must wait the specified amount of time before attempting to log in.

Perform these steps to configure the maximum number of login attempts.

**Note**

- All types of user accounts (including admin) are locked out of the system after exceeding the maximum number of login attempts.
- The default maximum number of unsuccessful login attempts is 0. The default amount of time the user is locked out of the system after exceeding the maximum number of login attempts is 30 minutes (1800 seconds).
- For steps to view a user's lockout status and to clear the user's locked out state, see [View and Clear User Lockout Status, on page 49](#).

This option is one of a number offered for achieving Common Criteria certification compliance on your system. For more information, see [Security Certifications Compliance, on page 69](#).

Procedure

-
- Step 1** From the FXOS CLI, enter security mode:
- scope security**
- Step 2** Set the maximum number of unsuccessful login attempts.
- set max-login-attempts** *num_attempts*
- The *num_attempts* value is any integer from 0-10.
- Step 3** Specify the amount of time (in seconds) the user should remain locked out of the system after reaching the maximum number of login attempts:
- set user-account-unlock-time**
- unlock_time*
- Step 4** Commit the configuration:
- commit-buffer**
-

View and Clear User Lockout Status

Admin users can view and clear the locked out status of users that have been locked out of the Firepower 4100/9300 chassis after exceeding the maximum number of failed login attempts specified in the Maximum Number of Login Attempts CLI setting. For more information, see [Set the Maximum Number of Login Attempts, on page 48](#).

Procedure

-
- Step 1** From the FXOS CLI, enter security mode:

scope security

Step 2 Display the user information (including lockout status) of the user in question:

Firepower-chassis /security # **show local-user** *user* **detail**

Example:

```
Local User user:
First Name:
Last Name:
Email:
Phone:
Expiration: Never
Password:
User lock status: Locked
Account status: Active
User Roles:
Name: read-only
User SSH public key:
```

Step 3 (Optional) Clear the user's lock out status:

Firepower-chassis /security # **scope local-user** *user*

Firepower-chassis /security/local-user # **clear lock-status**

Configuring the Maximum Number of Password Changes for a Change Interval

Procedure

Step 1 Enter security mode:

Firepower-chassis # **scope security**

Step 2 Enter password profile security mode:

Firepower-chassis /security # **scope password-profile**

Step 3 Restrict the number of password changes a locally authenticated user can make within a given number of hours:

Firepower-chassis /security/password-profile # **set change-during-interval** **enable**

Step 4 Specify the maximum number of times a locally authenticated user can change his or her password during the Change Interval:

Firepower-chassis /security/password-profile # **set change-count** *pass-change-num*

This value can be anywhere from 0 to 10.

- Step 5** Specify the maximum number of hours over which the number of password changes specified in the **Change Count** field are enforced:

```
Firepower-chassis /security/password-profile # set change-interval num-of-hours
```

This value can be anywhere from 1 to 745 hours.

For example, if this field is set to 48 and the **Change Count** field is set to 2, a locally authenticated user can make no more than 2 password changes within a 48 hour period.

- Step 6** Commit the transaction to the system configuration:

```
Firepower-chassis /security/password-profile # commit-buffer
```

Example

The following example enables the change during interval option, sets the change count to 5, sets the change interval to 72 hours, and commits the transaction:

```
Firepower-chassis # scope security
Firepower-chassis /security # scope password-profile
Firepower-chassis /security/password-profile # set change-during-interval enable
Firepower-chassis /security/password-profile* # set change-count 5
Firepower-chassis /security/password-profile* # set change-interval 72
Firepower-chassis /security/password-profile* # commit-buffer
Firepower-chassis /security/password-profile #
```

Configure Minimum Password Length Check

If you enable minimum password length check, you must create passwords with the specified minimum number of characters. For example, if the *min_length* option is set to 15, you must create passwords using 15 characters or more. This option is one of a number that allow for Common Criteria certification compliance on your system. For more information, see [Security Certifications Compliance](#).

Perform these steps to configure the minimum password length check.

Procedure

- Step 1** From the FXOS CLI, enter security mode:

```
scope security
```

- Step 2** Specify the minimum password length:

```
set min-password-length min_length
```

- Step 3** Commit the configuration:

```
commit-buffer
```

Configuring a No Change Interval for Passwords

Procedure

-
- Step 1** Enter security mode:
Firepower-chassis # **scope security**
- Step 2** Enter password profile security mode:
Firepower-chassis /security # **scope password-profile**
- Step 3** Disable the change during interval feature:
Firepower-chassis /security/password-profile # **set change-during-interval disable**
- Step 4** Specify the minimum number of hours that a locally authenticated user must wait before changing a newly created password:
Firepower-chassis /security/password-profile # **set no-change-interval** *min-num-hours*
This value can be anywhere from 1 to 745 hours.
This interval is ignored if the **Change During Interval** property is not set to **Disable**.
- Step 5** Commit the transaction to the system configuration:
Firepower-chassis /security/password-profile # **commit-buffer**
-

Example

The following example disables the change during interval option, sets the no change interval to 72 hours, and commits the transaction:

```
Firepower-chassis # scope security
Firepower-chassis /security # scope password-profile
Firepower-chassis /security/password-profile # set change-during-interval disable
Firepower-chassis /security/password-profile* # set no-change-interval 72
Firepower-chassis /security/password-profile* # commit-buffer
Firepower-chassis /security/password-profile #
```

Configuring the Password History Count

Procedure

-
- Step 1** Enter security mode:

```
Firepower-chassis # scope security
```

Step 2 Enter password profile security mode:

```
Firepower-chassis /security # scope password-profile
```

Step 3 Specify the number of unique passwords that a locally authenticated user must create before that user can reuse a previously used password:

```
Firepower-chassis /security/password-profile # set history-count num-of-passwords
```

This value can be anywhere from 0 to 15.

By default, the **History Count** field is set to 0, which disables the history count and allows users to reuse previously used passwords at any time.

Step 4 Commit the transaction to the system configuration:

```
Firepower-chassis /security/password-profile # commit-buffer
```

Example

The following example configures the password history count and commits the transaction:

```
Firepower-chassis # scope security
Firepower-chassis /security # scope password-profile
Firepower-chassis /security/password-profile # set history-count 5
Firepower-chassis /security/password-profile* # commit-buffer
Firepower-chassis /security/password-profile #
```

Creating a Local User Account

Procedure

Step 1 Enter security mode:

```
Firepower-chassis# scope security
```

Step 2 Create the user account:

```
Firepower-chassis /security # create local-user local-user-name
```

where *local-user-name* is the account name to be used when logging into this account. This name must be unique and meet the guidelines and restrictions for user account names (see [Guidelines for Usernames, on page 38](#)).

After you create the user, the login ID cannot be changed. You must delete the user account and create a new one.

Step 3 Specify whether the local user account is enabled or disabled:

```
Firepower-chassis /security/local-user # set account-status {active|inactive}
```

Step 4 Set the password for the user account:

```
Firepower-chassis /security/local-user # set password
```

Enter a password: *password*

Confirm the password: *password*

If password strength check is enabled, a user's password must be strong and the FXOS rejects any password that does not meet the strength check requirements (see [Guidelines for Passwords, on page 39](#)).

Note

Passwords must not contain the following symbols: \$ (dollar sign), ? (question mark), and = (equals sign). This restriction applies whether the password strength check is enabled or not.

Step 5 (Optional) Specify the first name of the user:

```
Firepower-chassis /security/local-user # set firstname first-name
```

Step 6 (Optional) Specify the last name of the user:

```
Firepower-chassis /security/local-user # set lastname last-name
```

Step 7 (Optional) Specify the date that the user account expires. The *month* argument is the first three letters of the month name.

```
Firepower-chassis /security/local-user # set expiration month day-of-month year
```

Note

After you configure a user account with an expiration date, you cannot reconfigure the account to not expire. You can, however, configure the account with the latest expiration date available.

Step 8 (Optional) Specify the user e-mail address.

```
Firepower-chassis /security/local-user # set email email-addr
```

Step 9 (Optional) Specify the user phone number.

```
Firepower-chassis /security/local-user # set phone phone-num
```

Step 10 (Optional) Specify the SSH key used for passwordless access.

```
Firepower-chassis /security/local-user # set sshkey ssh-key
```

Step 11 All users are assigned the *read-only* role by default and this role cannot be removed. For each additional role that you want to assign to the user:

```
Firepower-chassis /security/local-user # create role role-name
```

where *role-name* is the role that represents the privileges you want to assign to the user account (see [User Roles, on page 42](#)).

Note

Changes in user roles and privileges do not take effect until the next time the user logs in. If a user is logged in when you assign a new role to or remove an existing role from a user account, the active session continues with the previous roles and privileges.

Step 12 To remove an assigned role from the user:

```
Firepower-chassis /security/local-user # delete role role-name
```

All users are assigned the *read-only* role by default and this role cannot be removed.

Step 13

Commit the transaction.

```
Firepower-chassis security/local-user # commit-buffer
```

Example

The following example creates the user account named kikipopo, enables the user account, sets the password to foo12345, assigns the admin user role, and commits the transaction:

```
Firepower-chassis# scope security
Firepower-chassis /security # create local-user kikipopo
Firepower-chassis /security/local-user* # set account-status active
Firepower-chassis /security/local-user* # set password
Enter a password:
Confirm the password:
Firepower-chassis /security/local-user* # create role admin
Firepower-chassis /security/local-user* # commit-buffer
Firepower-chassis /security/local-user #
```

The following example creates the user account named lincey, enables the user account, sets an OpenSSH key for passwordless access, assigns the aaa and operations user roles, and commits the transaction.

```
Firepower-chassis# scope security
Firepower-chassis /security # create local-user lincey
Firepower-chassis /security/local-user* # set account-status active
Firepower-chassis /security/local-user* # set sshkey "ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAuo9VQ2CmWBI9/S1f30klCWjnV3lgdXMzO0WU15iPw851kdQqap+NFuNmHcb4K
iaQB8X/PDdmtlxQQcawclj+k8f4VcOelBx1sGk5luq51s1ob1VOIEwcKEL/h51rdbN1I8y3SS9I/gGiBZ9ARlop9LDpD
m8HPh2LOgyH7Ei1MI8="
Firepower-chassis /security/local-user* # create role aaa
Firepower-chassis /security/local-user* # create role operations
Firepower-chassis /security/local-user* # commit-buffer
Firepower-chassis /security/local-user #
```

The following example creates the user account named jforlenz, enables the user account, sets a Secure SSH key for passwordless access, and commits the transaction.

```
Firepower-chassis# scope security
Firepower-chassis /security # create local-user jforlenz
Firepower-chassis /security/local-user* # set account-status active
Firepower-chassis /security/local-user* # set sshkey
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
User's SSH key:
> ---- BEGIN SSH2 PUBLIC KEY ----
>AAAAB3NzaC1yc2EAAAABIwAAAIEAuo9VQ2CmWBI9/S1f30klCWjnV3lgdXMzO0WU15iPw8
>51kdQqap+NFuNmHcb4KiaQB8X/PDdmtlxQQcawclj+k8f4VcOelBx1sGk5luq51s1ob1VO
>IEwcKEL/h51rdbN1I8y3SS9I/gGiBZ9ARlop9LDpDm8HPh2LOgyH7Ei1MI8=
> ---- END SSH2 PUBLIC KEY ----
> ENDOFBUF
Firepower-chassis /security/local-user* # commit-buffer
Firepower-chassis /security/local-user #
```

Deleting a Local User Account

Procedure

-
- Step 1** Enter security mode:
Firepower-chassis# **scope security**
- Step 2** Delete the local-user account:
Firepower-chassis /security # **delete local-user** *local-user-name*
- Step 3** Commit the transaction to the system configuration:
Firepower-chassis /security # **commit-buffer**
-

Example

The following example deletes the foo user account and commits the transaction:

```
Firepower-chassis# scope security
Firepower-chassis /security # delete local-user foo
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

Activating or Deactivating a Local User Account

You must be a user with admin or AAA privileges to activate or deactivate a local user account.

Procedure

-
- Step 1** Enter security mode:
Firepower-chassis# **scope security**
- Step 2** Enter local-user security mode for the user you want to activate or deactivate:
Firepower-chassis /security # **scope local-user** *local-user-name*
- Step 3** Specify whether the local user account is active or inactive:
Firepower-chassis /security/local-user # **set account-status** {**active** | **inactive**}
- Note**
The admin user account is always set to active. It cannot be modified.
- Step 4** Commit the transaction to the system configuration:


```
Firepower-chassis /security/local-user # commit-buffer
```

Example

The following example enables a local user account called accounting:

```
Firepower-chassis# scope security  
Firepower-chassis /security # scope local-user accounting  
Firepower-chassis /security* # commit-buffer  
Firepower-chassis /security #
```

Clearing the Password History for a Locally Authenticated User

Procedure

- Step 1** Enter security mode:
- ```
Firepower-chassis # scope security
```
- Step 2** Enter local user security mode for the specified user account:
- ```
Firepower-chassis /security # scope local-user user-name
```
- Step 3** Clear the password history for the specified user account:
- ```
Firepower-chassis /security/local-user # clear password-history
```
- Step 4** Commit the transaction to the system configuration:
- ```
Firepower-chassis /security/local-user # commit-buffer
```
-

Example

The following example clears the password history and commits the transaction:

```
Firepower-chassis # scope security  
Firepower-chassis /security # scope local-user admin  
Firepower-chassis /security/local-user # clear password-history  
Firepower-chassis /security/local-user* # commit-buffer  
Firepower-chassis /security/local-user #
```




CHAPTER 6

Image Management

- [About Image Management, on page 59](#)
- [Downloading Images from Cisco.com, on page 60](#)
- [Downloading a FXOS Software Image to the Firepower 4100/9300 chassis, on page 60](#)
- [Verifying the Integrity of an Image, on page 62](#)
- [Upgrading the FXOS Platform Bundle, on page 63](#)
- [Downloading a Logical Device Software Image to the Firepower 4100/9300 chassis, on page 64](#)
- [Updating the Image Version for a Logical Device, on page 66](#)
- [Firmware Upgrade, on page 68](#)

About Image Management

The Firepower 4100/9300 chassis uses two basic types of images:



Note All images are digitally signed and validated through Secure Boot. Don't modify the image in any way or you receive a validation error.

- **Platform Bundle**—The platform bundle is a collection of multiple independent images that operate on the Supervisor and security module/engine. The platform bundle is a FXOS software package.
- **Application**—Application images are the software images you want to deploy on the security module/engine of the Firepower 4100/9300 chassis. Application images are delivered as Cisco Secure Package files (CSP) and are stored on the supervisor until deployed to a security module/engine as part of logical device creation or in preparation for later logical device creation. You can have multiple different versions of the same application image type stored on the Supervisor.



Note

- If you are upgrading both the Platform Bundle image and one or more Application images, you must upgrade the Platform Bundle first.
- If you're installing an ASA application in the device, you can delete the images of the existing application Firepower Threat Defense and vice versa. When you try to delete all the Firepower Threat Defense images, at least one image deletion will be denied with an error message `Invalid operation as no default Firepower Threat Defense/ASA APP will be left. Please select a new default Firepower Threat Defense app.` In order to delete all the Firepower Threat Defense images, you must leave the default image alone and delete the rest of the images and then finally delete the default image.

Downloading Images from Cisco.com

Download FXOS and application images from Cisco.com so you can upload them to the chassis.

Before you begin

You must have a Cisco.com account.

Procedure

-
- Step 1** Using a web browser, navigate to <http://www.cisco.com/go/firepower9300-software> or <http://www.cisco.com/go/firepower4100-software>.
The software download page for the Firepower 4100/9300 chassis is opened in the browser.
- Step 2** Find and then download the appropriate software image to your local computer.
-

Downloading a FXOS Software Image to the Firepower 4100/9300 chassis

You can use FTP, HTTP/HTTPS, SCP, SFTP, or TFTP to copy the FXOS software image to the Firepower 4100/9300 chassis.

Before you begin

Collect the following information that you will need to import a configuration file:

- IP address and authentication credentials for the server from which you are copying the image
- Fully qualified name of the FXOS image file



Note Starting with FXOS 2.8.1 the HTTP/HTTPS are supported for firmware and application image downloads.

Procedure

-
- Step 1** Enter firmware mode:
- ```
Firepower-chassis # scope firmware
```
- Step 2** Download the FXOS software image:
- ```
Firepower-chassis /firmware # download image URL
```
- Specify the URL for the file being imported using one of the following syntax:
- `ftp://username@hostname/path/image_name`
 - `http://username@hostname/path/image_name`
 - `https://username@hostname/path/image_name`
 - `scp://username@hostname/path/image_name`
 - `sftp://username@hostname/path/image_name`
 - `tftp://hostname:port-num/path/image_name`
 - `usbA://hostname:port-num/path/image_name`
- Step 3** To monitor the download process:
- ```
Firepower-chassis /firmware # show package image_name detail
```
- 

## Example

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-fxos-k9.2.14.1.94.SPA
Firepower-chassis /firmware # show package fxos-k9.2.14.1.94.SPA detail
Download task:
 File Name: fxos-k9.2.14.1.94.SPA
 Protocol: scp
 Server: 192.168.1.1
 Userid:
 Path:
 Downloaded Image Size (KB): 510304
 State: Downloading
 Current Task: downloading image fxos-k9.2.14.1.94.SPA from
192.168.1.1 (FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

The following example copies an image using the HTTP/HTTPS protocol:

```

Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
https://user@192.168.1.1/images/fxos-k9.1.1.1.119.SPA
Firepower-chassis /firmware # show download task

Download task:
File Name Protocol Server Port Userid State

fxos-k9.2.14.1.94.SPA
 Https 192.168.1.1 0 Downloaded
fxos-k9.2.14.1.94.SPA
 Http sjc-ssp-artifac 0 Downloaded

Firepower-chassis /firmware # show package fxos-k9.2.14.1.94.SPA detail
Download task:
 File Name: fxos-k9.1.1.1.119.SPA
 Protocol: https
 Server: 192.168.1.1
 Userid:
 Path:
 Downloaded Image Size (KB): 510304
 State: Downloading
 Current Task: downloading image fxos-k9.2.14.1.94.SPA from
192.168.1.1 (FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)

```

## Verifying the Integrity of an Image

The integrity of the image is automatically verified when a new image is added to the Firepower 4100/9300 chassis. If needed, you can use the following procedure to manually verify the integrity of an image.

### Procedure

- 
- Step 1** Connect to the FXOS CLI (see [Accessing the FXOS CLI, on page 18](#)).
  - Step 2** Enter firmware mode:  
Firepower-chassis# **scope firmware**
  - Step 3** List images:  
Firepower-chassis /firmware # **show package**
  - Step 4** Verify the image:  
Firepower-chassis /firmware # **verify platform-pack version** *version\_number*  
*version\_number* is the version number of the FXOS platform bundle you are verifying--for example, 1.1(2.51).
  - Step 5** The system will warn you that verification could take several minutes.  
Enter **yes** to confirm that you want to proceed with verification.
  - Step 6** To check the status of the image verification:

Firepower-chassis /firmware # **show validate-task**

---

# Upgrading the FXOS Platform Bundle

## Before you begin

Download the platform bundle software image from Cisco.com (see [Downloading Images from Cisco.com, on page 60](#)) and then download that image to the Firepower 4100/9300 chassis (see [Downloading a Logical Device Software Image to the Firepower 4100/9300 chassis, on page 64](#)).



### Note

The upgrade process typically takes between 20 and 30 minutes.

If you are upgrading a Firepower 9300 or 4100 Series security appliance that is running a standalone logical device or if you are upgrading a Firepower 9300 security appliance that is running an intra-chassis cluster, traffic will not traverse through the device while it is upgrading.

If you are upgrading Firepower 9300 or 4100 Series security appliance that is part of an inter-chassis cluster, traffic will not traverse through the device being upgraded while it is upgrading. However, the other devices in the cluster will continue to pass traffic.

---

## Procedure

---

- Step 1** Connect to the FXOS CLI (see [Accessing the FXOS CLI, on page 18](#)).
- Step 2** Enter firmware mode:  
Firepower-chassis# **scope firmware**
- Step 3** Enter auto-install mode:  
Firepower-chassis /firmware # **scope auto-install**
- Step 4** Install the FXOS platform bundle:  
Firepower-chassis /firmware/auto-install # **install platform platform-vers version\_number**  
*version\_number* is the version number of the FXOS platform bundle you are installing--for example, 1.1(2.51).
- Step 5** The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.  
  
Enter **yes** to confirm that you want to proceed with verification.
- Step 6** Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.  
  
The FXOS unpacks the bundle and upgrades/reloads the components.

- Step 7** To monitor the upgrade process:
- Enter **scope firmware**.
  - Enter **scope auto-install**.
  - Enter **show fsm status expand**.

## Downloading a Logical Device Software Image to the Firepower 4100/9300 chassis

You can use FTP, HTTP/HTTPS, SCP, SFTP, or TFTP to copy the logical device software image to the Firepower 4100/9300 chassis.

### Before you begin

Collect the following information that you will need to import a configuration file:

- IP address and authentication credentials for the server from which you are copying the image
- Fully qualified name of the software image file



**Note** FXOS 2.8.1 and later versions support HTTP/HTTPS protocols for firmware and application image downloads.

### Procedure

- Step 1** Enter Security Services mode:  
Firepower-chassis # **scope ssa**
- Step 2** Enter Application Software mode:  
Firepower-chassis /ssa # **scope app-software**
- Step 3** Download the logical device software image:  
Firepower-chassis /ssa/app-software # **download image URL**
- Specify the URL for the file being imported using one of the following syntax:
- **ftp://username@hostname/path**
  - **http://username@hostname/path**
  - **https://username@hostname/path**
  - **scp://username@hostname/path**
  - **sftp://username@hostname/path**
  - **tftp://hostname:port-num/path**



**Note**

Do not use tftpdnld to install the image as it throws error.

- Step 4** To monitor the download process:  
Firepower-chassis /ssa/app-software # **show download-task**
- Step 5** To view the downloaded applications:  
Firepower-chassis /ssa/app-software # **up**  
Firepower-chassis /ssa # **show app**
- Step 6** To view details for a specific application:  
Firepower-chassis /ssa # **scope app application\_type image\_version**  
Firepower-chassis /ssa/app # **show expand**

**Example**

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task
```

Downloads for Application Software:

| File Name              | Protocol | Server      | Userid | State      |
|------------------------|----------|-------------|--------|------------|
| cisco-asa.9.4.1.65.csp | Scp      | 192.168.1.1 | user   | Downloaded |

```
Firepower-chassis /ssa/app-software # up
```

```
Firepower-chassis /ssa # show app
```

Application:

| Name | Version  | Description | Author | Deploy Type | CSP Type    | Is Default App |
|------|----------|-------------|--------|-------------|-------------|----------------|
| asa  | 9.4.1.41 | N/A         |        | Native      | Application | No             |
| asa  | 9.4.1.65 | N/A         |        | Native      | Application | Yes            |

```
Firepower-chassis /ssa # scope app asa 9.4.1.65
```

```
Firepower-chassis /ssa/app # show expand
```

Application:

```
Name: asa
Version: 9.4.1.65
Description: N/A
Author:
Deploy Type: Native
CSP Type: Application
Is Default App: Yes
```

App Attribute Key for the Application:

```
App Attribute Key Description
```

```

cluster-role This is the role of the blade in the cluster
mgmt-ip This is the IP for the management interface
mgmt-url This is the management URL for this application

Net Mgmt Bootstrap Key for the Application:
Bootstrap Key Key Data Type Is the Key Secret Description

PASSWORD String Yes The admin user password.

Port Requirement for the Application:
Port Type: Data
Max Ports: 120
Min Ports: 1

Port Type: Mgmt
Max Ports: 1
Min Ports: 1

Mgmt Port Sub Type for the Application:
Management Sub Type

Default

Port Type: Cluster
Max Ports: 1
Min Ports: 0
Firepower-chassis /ssa/app #

```

## Updating the Image Version for a Logical Device

Use this procedure to upgrade the ASA application image to a new version, or set the Firepower Threat Defense application image to a new startup version that will be used in a disaster recovery scenario.

When you change the startup version on a Firepower Threat Defense logical device using Firepower Chassis Manager or the FXOS CLI, the application does not immediately upgrade to the new version. The logical device startup version is the version that Firepower Threat Defense reinstalls to in a disaster recovery scenario. After initial creation of a Firepower Threat Defense logical device, you do not upgrade the Firepower Threat Defense logical device using Firepower Chassis Manager or the FXOS CLI. To upgrade a Firepower Threat Defense logical device, you must use FMC. See the System Release Notes for more information:  
<http://www.cisco.com/c/en/us/support/security/defense-center/products-release-notes-list.html>.

Also, note that any updates to the Firepower Threat Defense logical device will not be reflected on the **Logical Devices > Edit and System > Updates** pages in Firepower Chassis Manager. On these pages, the version shown indicates the software version (CSP image) that was used to create the Firepower Threat Defense logical device.



**Note** When you set the startup version for Firepower Threat Defense, startup version of the application gets updated. Hence, you must manually reinstall the application or reinitialize the blade to apply the selected version. This procedure is not the equivalent of upgrading or downgrading the Firepower Threat Defense software, rather a complete reinstallation (reimage). Therefore, the application gets deleted and the existing configuration gets lost.

When you change the startup version on an ASA logical device, the ASA upgrades to that version and all configuration is restored. Use the following workflows to change the ASA startup version, depending on your configuration:



**Note** When you set the startup version for ASA, the application gets automatically restarted. This procedure is the equivalent of upgrading or downgrading the ASA software (existing configuration gets preserved).

ASA High Availability -

1. Change the logical device image version(s) on the standby unit.
2. Make the standby unit active.
3. Change the application version(s) on the other unit.

ASA Inter-Chassis Cluster -

1. Change the startup version on the data unit.
2. Make the data unit the control unit.
3. Change the startup version on the original control unit (now data).

### Before you begin

Download the application image you want to use for the logical device from Cisco.com (see [Downloading Images from Cisco.com, on page 60](#)) and then download that image to the Firepower 4100/9300 chassis (see [Downloading a Logical Device Software Image to the Firepower 4100/9300 chassis, on page 64](#)).

If you are upgrading both the Platform Bundle image and one or more Application images, you must upgrade the Platform Bundle first.

### Procedure

- 
- Step 1** Enter Security Services mode:  
Firepower-chassis # **scope ssa**
- Step 2** Set the scope to the security module you are updating:  
Firepower-chassis /ssa # **scope slot slot\_number**
- Step 3** Set the scope to the application you are updating:  
Firepower-chassis /ssa/slot # **scope app-instance app\_template**
- Step 4** Set the Startup version:  
Firepower-chassis /ssa/slot/app-instance # **set startup-version version\_number**

If you are setting the application startup version on a Firepower Threat Defense logical device, the following warning message appears:

13254: Warning: FXOS upgrades are not supported for Firepower Threat Defense. The specified version will be used only if Firepower Threat Defense needs to be reinstalled.

#### Example:

```
firepower /ssa/slot/app-instance # set startup-version 6.2.2.81
13254: Warning: FXOS upgrades are not supported for ftd. The specified version will be
used only if ftd needs to be reinstalled.
```

### Step 5

Commit the configuration:

#### **commit-buffer**

Commits the transaction to the system configuration. The application image is updated and the application restarts.

#### Example

The following example updates the software image for an ASA running on security module 1. Notice that you can use the **show** command to view the update status.

```
Firepower-chassis# scope ssa
Firepower-chassis /ssa # scope slot 1
Firepower-chassis /ssa/slot # scope app-instance asa
Firepower-chassis /ssa/slot/app-instance # set startup-version 9.4.1.65
Firepower-chassis /ssa/slot/app-instance* # show configuration pending
 enter app-instance asa
+ set startup-version 9.4.1.65
 exit
Firepower-chassis /ssa/slot/app-instance* # commit-buffer
Firepower-chassis /ssa/slot/app-instance # show
```

Application Instance:

| Application Name | Admin State | Operational State | Running Version | Startup Version |
|------------------|-------------|-------------------|-----------------|-----------------|
| asa              | Enabled     | Updating          | 9.4.1.41        | 9.4.1.65        |

```
Firepower-chassis /ssa/slot/app-instance #
Firepower-chassis /ssa/slot/app-instance # show
```

Application Instance:

| Application Name | Admin State | Operational State | Running Version | Startup Version |
|------------------|-------------|-------------------|-----------------|-----------------|
| asa              | Enabled     | Online            | 9.4.1.65        | 9.4.1.65        |

```
Firepower-chassis /ssa/slot/app-instance #
```

## Firmware Upgrade

For information about upgrading the firmware on your Firepower 4100/9300 chassis, see the [Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide](#).



## CHAPTER 7

# Security Certifications Compliance

---

- [Security Certifications Compliance, on page 69](#)
- [Generate the SSH Host Key, on page 70](#)
- [Configure IPSec Secure Channel, on page 71](#)
- [Configure Static CRL for a Trustpoint, on page 77](#)
- [About the Certificate Revocation List Check, on page 78](#)
- [Configure CRL Periodic Download, on page 82](#)
- [Set the LDAP Key Ring Certificate, on page 84](#)
- [Enable Client Certificate Authentication, on page 85](#)

## Security Certifications Compliance

United States federal government agencies are sometimes required to use only equipment and software complying with security standards established by the U.S. Department of Defense and global certification organizations. The Firepower 4100/9300 chassis supports compliance with several of these security certification standards.

See the following topics for steps to enable features that support compliance with these standards:

- [Enable FIPS Mode](#)
- [Enable Common Criteria Mode](#)
- [Configure IPSec Secure Channel, on page 71](#)
- [Configure Static CRL for a Trustpoint, on page 77](#)
- [About the Certificate Revocation List Check, on page 78](#)
- [Configure CRL Periodic Download, on page 82](#)
- [Setting the Date and Time Using NTP, on page 110](#)
- [Set the LDAP Key Ring Certificate, on page 84](#)
- [Configure the IP Access List, on page 164](#)
- [Enable Client Certificate Authentication, on page 85](#)
- [Configure Minimum Password Length Check](#)

- [Set the Maximum Number of Login Attempts, on page 48](#)



**Note** Note that these topics discuss enabling certifications compliance on the Firepower 4100/9300 chassis only. Enabling certification compliance on the Firepower 4100/9300 chassis does not automatically propagate compliance to any of its attached logical devices.

## Generate the SSH Host Key

Prior to FXOS release 2.0.1, the existing SSH host key created during initial setup of a device was hard-coded to 1024 bits. To comply with FIPS and Common Criteria certification, you must destroy this old host key and generate a new one. See [Enable FIPS Mode](#) or [Enable Common Criteria Mode](#) for more information.

Perform these steps to destroy the old SSH host key and generate a new certifications-compliant one.

### Procedure

**Step 1** From the FXOS CLI, enter services mode:

```
scope system
```

```
scope services
```

**Step 2** Delete the SSH host key:

```
delete ssh-server host-key
```

**Step 3** Commit the configuration:

```
commit-buffer
```

**Step 4** Set the SSH host key size to 2048 bits:

```
set ssh-server host-key rsa 2048
```

**Step 5** Commit the configuration:

```
commit-buffer
```

**Step 6** Create a new SSH host key:

```
create ssh-server host-key
```

```
commit-buffer
```

**Step 7** Confirm the new host key size:

```
show ssh-server host-key
```

```
Host Key Size: 2048
```

# Configure IPSec Secure Channel

IPSec is a framework of open standards developed by the Internet Engineering Task Force (IETF). It creates secure, authenticated, and reliable communication over IP networks. The IPSec security service provides:

- Connectionless Integrity – Assurance the received traffic has not been modified.
- Data origin authentication – Assurance the traffic is sent by legitimate party.
- Confidentiality (encryption) – Assurance the user's traffic is not examined by non-authorized parties.
- Access control – Prevention of unauthorized use of a resource.

IPSec Secure Channel supports the following algorithms:

- Phase 1

```
aes128gcm16-prfsha384-prfsha512-prfsha256-prfsha1-ecp256-ecp384-ecp521-modp2048-modp3072-modp4096
aes128-aes192-aes256-sha256-sha384-sha1_160-sha1-sha512-prfsha384-prfsha512-prfsha256-prfsha1-ecp256-ecp384-ecp521
aes128-aes192-aes256-sha256-sha384-sha1_160-sha1-sha512-prfsha384-prfsha512-prfsha256-prfsha1-modp2048-modp3072-modp4096
```

- Phase 2

- Only AES SHA based encryption algorithms are supported. (DES and MD5 are not supported)
- Supported DH groups are 14,15,16,19,20, and 21.



**Note** IPSec connections can only be initiated from FXOS. FXOS does not accept incoming IPSec connection requests.

IPsec tunnels are sets of SAs that FXOS establishes between peers. The SAs specify the protocols and algorithms to apply to sensitive data and also specify the keying material that the peers use. IPsec SAs control the actual transmission of user traffic. SAs are unidirectional, but are generally established in pairs (inbound and outbound).

IPSec on Chassis Manager has two modes:

## Transport Mode

IP Header, IPSec Header, TCP Header, Data

## Tunnel Mode

New IP Header, IPSec Header, Original IP Header, TCP Header, Data

IPSec's operation can be broken down into five main steps:

1. Traffic Selection – Interesting traffic which matches IPSec policy starts the IKE process. For example, traffic can be selected using src/dst host IP or subnet. Alternatively, user also can trigger IKE process through admin command.
2. IKE Phase 1 – authenticate IPSec peers and to setup a secure channel to enable IKE exchanges
3. IKE phase 2 – negotiate SAs to set up the IPSec tunnel. SA stands for Security Association, it is a relationship between IPSec end-points that describe what security services are used to protect data traffic.

4. Data transfer – Data packets are encrypted and encapsulated in IPSec header using parameters and keys stored in the SA
5. IPSec tunnel termination – IPSec SAs terminate through deletion or by timing out.

You can configure IPSec on your Firepower 4100/9300 chassis to provide end-to-end data encryption and authentication service on data packets going through the public network. This option is one of a number offered for achieving Common Criteria certification compliance on your system. For more information, see [Security Certifications Compliance, on page 69](#).

**Note**

- If you are using an IPSec secure channel in FIPS mode, the IPSec peer must support RFC 7427.
- If you elect to configure enforcement of matching cryptographic key strength between IKE and SA connections (set sa-strength-enforcement to yes in the below procedure):

|                               |                                                                                                                                                                                                                                                      |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| If SA enforcement is enabled  | then when IKE negotiated key size is less than ESP negotiated key size, the connection fails.<br><br>then when IKE negotiated key size is large or equal than ESP negotiated key size, SA enforcement check passes and the connection is successful. |
| If SA enforcement is disabled | then SA enforcement check passes and the connection is successful.                                                                                                                                                                                   |

Perform these steps to configure an IPSec secure channel.

**Procedure**

- 
- Step 1** From the FXOS CLI, enter security mode:  
**scope security**
- Step 2** Create the keyring:  
**enter keyring ssp**  
**! create certreq subject-name *subject-name* ip *ip***
- Step 3** Enter the associated certificate request information:  
**enter certreq**
- Step 4** Set the country:  
**set country *country***
- Step 5** Set the DNS:  
**set dns *dns***
- Step 6** Set the email:



**set e-mail** *email*

**Step 7** Set the IP information:

**set ip** *ip-address*

**set ipv6** *ipv6*

**Step 8** Set the locality:

**set locality** *locality*

**Step 9** Set the organization name:

**set org-name** *org-name*

**Step 10** Set the organization unit name:

**set org-unit-name** *org-unit-name*

**Step 11** Set the password:

**! set password**

**Step 12** Set the state:

**set state** *state*

**Step 13** Set the subject name for the certreq:

**set subject-name** *subject-name*

**Step 14** Exit:

**exit**

**Step 15** Set the modulus:

**set modulus** *modulus*

**Step 16** Set the regeneration for the certificate request:

**set regenerate** { *yes* / *no* }

**Step 17** Set the trustpoint:

**set trustpoint** *interca*

**Step 18** Exit:

**exit**

**Step 19** Enter the newly created trustpoint:

**enter trustpoint** *interca*

**Step 20** Generate certificate signing request:

**set certchain**

**Example:**

```

-----BEGIN CERTIFICATE-----
MIIF3TCCA8WgAwIBAgIBADANBgkqhkiG9w0BAQsFADBwMQswCQYDVQQGEwJVUzEL
MAkGA1UECAwCQ0ExDDAKBgNVBACMA1NKQzEOMAwGA1UECgwFQ2l2Y28xDTALBgNV
BAsMBFNUQlUxXzAJBgNVBAMMAkNBMR0wGAYJKoZIhvcNAQkBFgtzc3Bac3NwLm5l
dDAeFw0xNjEyMDgxOTMzNTJaFw0yNjEyMDYxOTMzNTJaMHAxCzAJBgNVBAYTAiVT
MQswCQYDVQQIDAJDQTEMAAoGA1UEBwwDU0pDMQ4wDAYDVQQKDAVDAxNjBzENMAAG
A1UECwwEU1RCVTELMakGA1UEAwCQ0ExGjAYBgkqhkiG9w0BCQEWc3Nzc3Bz3Au
bmV0MIIICjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCGKCAgEA2ukWyMLQuLqTvhq7
zFb3Oz/iyDG/ui6mrLIYn8wE3E39XcXA1/x9IHCmxFKNJdD7EbsggfOuy0Bj+Y4s
+uZ1VapBXV/JrAie7bNn3ZYrL29yuyOrlqoi9k9gL/oRBzH18BwBwGHBOz3hGrSK
Yc2yhsq9y/6yI3nSuLZm6ybmUKjTa+B4YuhDTz4hl/I9x/J5nbGiab3vLDKss1nO
xP9+1+Lc690Vl8/mNPWdjCjDI+U/L9keYs/rbZdRSeXy9kMae42+4FIRHDJjPcSN
Yw1g/gcR2F7QUKRygKckJKXDX2QliGYSetlSHj18O87o5s/pmQAWWRGkKpfDv3oH
cMPgI2T9rC0D8NNcgPXj9PFKfexoGNGwNT085fK3kjgModWbdeMG3EihxEEOUPD0
Fdu0HrTM5lVwb+vr5wE9HsAiMJ8UuujmHqH5mlwyy3Me+cEDHo0hLeNs+AFrQEXQ
e9S+KZC/dq/9zOLpRsVqSfIsAuVl/QdPDbWShjflE/fP2Wj01PqXywQydzymVvgE
wEZaoFg+mlGJm0+q4RDvnpzEviOYNsAGmOkILh5HQ/eYDcxvd0qbORWb31H32ySl
Ila6UTT9+vnND1f838fxvNvr8nyGD2S/LVaxnZIO4jcSIvtdizbbT8u5B4VcLKIC
x0vkqj06RvNZJ52sUaD9C3UodTUCAwEAAaOBgTB/MC8GA1UdHwQoMCYwJKAioCCG
Hmh0dHA6Lyl8xOTluMTY4LjQuMjkvcM9vdGNhLmNybDAdBgNVHQ4EFgQU7Jg01A74
jpx8U0APk76pVfYQQ5AwHwYDVR0jBBgwFoAU7Jg01A74jpx8U0APk76pVfYQQ5Aw
DAYDVR0TBAAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAgEAvI8ky2jiXc4wPiMuxIfY
W7DRmszPUWQ7edor7yxuQzHLVFFOwYRudsyXbv7INR3rJ/X1cRQj9+KidWWVxpo
pFahRhZyXvZ10DHKLzGTQS3jiHgrF3Z8ohWbL15L7PEDlrxMBoJvabPeQRgTmY/n
XZJ7qRYbypO3gUMCaCZ12raJc3/DlpBQ29yweCbUkc9qiHKA0IbnvAxoroHWmBld
94LrJcggfMQTuNJQszJiVVysYJfZ+utlDp2QwfdDv7B0JkwTbjdwRSfotEbc5R18n
BNXYHqXuoNMmqbS3KjCLXcH6xIN8t+UkfP89hvJt/flUj+s/VJSVZWk4tAWvR7wl
QngCKRjW6FYpzeyNBctiJ07wO+Wt4e3KhIjJDYvA9hFixWcVGdf2r6QW5BYbgGOK
DkHb/gdr/bcdLBKN/PtSJ+prSrpBSa6rJX8D9UmfhqN/3f+sS1fm4qWORJc6G2
gAcg7AjEQ/0do512vAl8p8idOg/Wv1O17mavzLpcue05cwMCX9fKxKZZ/+7Pk19Y
ZrXS6uMn/CGnViptn0w+uJ1IRj1oulk+/ZyPtBvFHUKFRnhoWj5SMFyds2laatyI
47N2ViaZBxhU3GICaH+3O+8rs9Kkz9tBZDSnEJVZA6yxaNCVP1bRUO20G3oRTmSx
8iLBJN+BXggxMmG8ssHisgw=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFqDCCA5CgAwIBAgIBBDANBgkqhkiG9w0BAQsFADBwMQswCQYDVQQGEwJVUzEL
MAkGA1UECAwCQ0ExDDAKBgNVBACMA1NKQzEOMAwGA1UECgwFQ2l2Y28xDTALBgNV
BAsMBFNUQlUxXzAJBgNVBAMMAkNBMR0wGAYJKoZIhvcNAQkBFgtzc3Bac3NwLm5l
dDAeFw0xNjEyMTUyMTM0NTRaFw0yNjEyMTM0NTRaMHwxCzAJBgNVBAYTAiVT
MQswCQYDVQQIDAJDQTEPMAoGA1UECgwGbmV3c3RnMRAwDgYDVQQLEDAuZXdzZGJl
MRMwEQYDVQQDDAAppbnRlcm0xLWNhMSgwJgYJKoZIhvcNAQkBFhlpbmRlcm0xLWNh
QGludGVybTEtY2EubmV0MIIICjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCGKCAgEA
wLpNnyEx5I4P8uDoWKWF3IZsegiHLANSodxuAUmhmwKekd0OpZZxHMw1wSO4IBX5
4itJS0xyXFzPmeptG3OXvNqCcsT+4BXI3DoGgPMULccc4NesHeg2z8+q3SPA6uZh
iseWNVKfUjixbQEBterWBiSkNZuOz1cpuBn34gtgeFFoCEXN+EZVpPESiancDVh
8pCPliPc/08ZJ3o9GW2j0eHJN84sgulEDL812ROejQvpmfGUGuq11stkIuh+wB+V
VRhUBVG7pV57I6DHeeRp6cDMLXaM3iMTelhdShyo5YUaRJMAk/t8KcqtGXfuLII
E2AkxKXeeveR9n6cpQd5JiNzCT/t9IQL/T/CCqMICRXLfPLCS9o5SS02B6QFgcTZ
yKR6hsmwe22wpK8QI7/5oWNXl0lb96hHJ7RPbG7RXYqmcLiXY/d2j9/RuNoPJawI
hLkfh0ldPA28xlnfIB1azCmMmdPcBO6cbUQfCj5hSmk3StVQKjGJcJaujz55TGGd1
GjnxDMX9twzw7Ee51895Xmtr24qqaCXJoW/dPhcIIXRdJPMsTJ4yPG0BieuRwd0p
i8w/rFwbHvz4C9Fthw1JrRxH1yeHJHrLIZgJ5txSaVUIgrgVCJaf6/jrRRWoRJwt
AzvzYq12dZPCeEAYgP7JcaQpvdpuDgq++NgBtygiqECAwEAAANBMD8wDAYDVR0T
BAUwAwEB/zAvBgNVHR8EKDAmMCSglqAghh5odHRwOi8vMTkyLjE2OC40LjI5L2lu
dGVybS5jcmwwDQYJKoZIhvcNAQELBQADggIBAG/XujJh5G5UWo+cwTSitAezWbJA
h1dAiXZ/OYWZSxkFRliErKdupLqL0ThjX/wRfFeXbrBQwm5kWAUUDr97D1Uz+2A
8LC5I8SWKXmyf0jUtsnEQbDZb33oVL7yXJk/A0SF0jihpPheMA+YRazalT9xj9KH

```

```

PE7nHCJMbb2ptrHUyvBrKSYrSeEqOpQU2+otnFyV3rS9aelgVjuaWyaWOc3lZ1Oi
CC2tJvY3NnM56j5iesxUCeY/SZ2/ECXN7RRBViLHmA3gFKmWf3xeNiKkxmJCxOaa
UWPC1x2V66I8DG9uUzlWyd79O2dy52aAphAHC6hqlzb6v+gw1Tld7UxaqVd8CD5W
ATjNs+ifkJS1h5ERxHjgcurZXOpR+NWPwF+UDzbMXxx+KAAXCI6ltCd8Pb3wOUC3
PKvwEXalcCcxGx71eRLpWPZFyEoi4N2NGE9OXRjz0K/KERZgNhsIW3bQMjcw3aX6
OXskEuKgsayctnWyxVqNnqvpuZ06kqyubh4+ZgGKZ5LNEXYmGNz3oED1rUN636Tw
SjGAPHgeROzyTFDixCei6aROIgDP/Hwvb0/+uThIe89g8WZ0djTKFUM8uBO3f+II
/cbuyBO1+JrDMq8NkAjkIjlp1c3WbfCue/qewtcfUBYZ4i53a56UNF5Ef0rpy/8
B/+07Me/p2y9Luqa
-----END CERTIFICATE-----
ENDOFBUF

```

**Step 21** Show the certificate signing request:

**show certreq**

**Example:**

```

Firepower-chassis# /security/keyring # show certreq
Certificate request subject name: SSP
Certificate request ip address: 192.168.0.111
Certificate request FI A ip address: 0.0.0.0
Certificate request FI B ip address: 0.0.0.0
Certificate request e-mail name:
Certificate request ipv6 address: ::
Certificate request FI A ipv6 address: ::
Certificate request FI B ipv6 address: ::
Certificate request country name: US
State, province or county (full name): CA
Locality name (eg, city): SJC
Organisation name (eg, company): Cisco
Organisational Unit Name (eg, section): Sec
DNS name (subject alternative name):
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIICwTCCAakCAQAwVTElMAkGA1UEBhMCVVMxGzAJBgNVBAGMAkNBMQwwCgYDVQQH
DANTSkMxMjAMBgNVBAoMBUNpc2NvMQ0wCwYDVQQLDARTVEJVMQwwCgYDVQQDDANT
U1AwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDQ292Rq3t0laoxPbfE
p/TKr6rxFhPqSSbtm6sXer//VZFIDTWODockDItuf4Kja215mIS0RyvEYVeRgAs
wbN459wm0BASd8xCjIhsuHDV7yHu539BnvRW6Q2o+gHeSRwckqjCIK/tsIxsPkV0
6OduZYXk2bnsLW6tNk3uzOIT2Q0FcZ1ET66C8fyyKWTrmvcZjDjkMm2nDFsPLX9
39TYPltDkJE3PocqyaCqmT4uobOuvQeLJh/efkBvwhb4BF8vwzRpHWTdjjU5YnR1
qiR4q7j1RmzVFxCDY3IVP/KDBoa5NyCLEUZECP5QCQFDzIRETZwVOKtxUVG0Nljd
K5TxAgMBAAGgJzAIBgkqhkiG9w0BCQ4xGDAWMBQGA1UdEQQNMAuCA1NTUlcEwKgA
rjANBgkqhkiG9w0BAQsFAAOCAQEArBoInxXkBYNlVeEoFCqKttu3+Hc7UdyoRM
2L2pjx5OHbQICC+8NRVRMYujTnp67BWuUZZI03dGP4/lbN6bC9P3CvkZdKUsJkN0
m1Ye9dgz7MO/KEcosarmoM19WB8LlweVdt6ycSdJzs9shOxwT6TAZPwL7gq/1ShF
RJh6sq5W9p6E0SjYefK62E7MatRjDjS8DXoxj6gfn9DqK15iVpkK2QqT5rneSGj+
R+20TcUnT0h/S5K/bySEM/3U1gFxQCOzbzPuHkj28kXAVczmTxXEkJBFLVduWNo6
DT3u0xImiPR1sqW1jpMwbhC+ZGDtvgKjKHToagup9+8R9IMcBQ==
-----END CERTIFICATE REQUEST-----

```

**Step 22** Enter IPSec mode:

**scope ipsec**

**Step 23** Set the log verbose level:

**set log-level** *log\_level*

**Step 24** Create and enter an IPSec connection:

**enter connection** *connection\_name*

**Step 25** Set IPSec mode to tunnel or transport:

**set mode** *tunnel\_or\_transport*

**Step 26** Set the local IP address:

**set local-addr** *ip\_address*

**Step 27** Set the remote IP address:

**set remote-addr** *ip\_address*

**Step 28** If using tunnel mode, set the remote subnet:

**set remote-subnet** *ip/mask*

**Step 29** (Optional) Set the remote identity:

**set remote-ike-ident** *remote\_identity\_name*

**Step 30** Set the keyring name:

**set keyring-name** *name*

**Step 31** (Optional) Set the keyring password:

**set keyring-passwd** *passphrase*

**Step 32** (Optional) Set the IKE-SA lifetime in minutes:

**set ike-rekey-time** *minutes*

The *minutes* value can be any integer between 60-1440, inclusive.

**Step 33** (Optional) Set the Child SA lifetime in minutes (30-480):

**set esp-rekey-time** *minutes*

The *minutes* value can be any integer between 30-480, inclusive.

**Step 34** (Optional) Set the number of retransmission sequences to perform during initial connect:

**set keyringtries** *retry\_number*

The *retry\_number* value can be any integer between 1-5, inclusive.

**Step 35** (Optional) Enable or disable the certificate revocation list check:

**set revoke-policy** { *relaxed* / *strict* }

**Step 36** Enable the connection:

**set admin-state** *enable*

**Step 37** Reload connections:

**reload-conns**

Connections that were previously not established are retried. Established connections remain untouched.

**Step 38** (Optional) Add the existing trustpoint name to IPsec:

**create authority** *trustpoint\_name*

**Step 39** Configure the enforcement of matching cryptographic key strength between IKE and SA connections:

**set sa-strength-enforcement** *yes\_or\_no*

---

## Configure Static CRL for a Trustpoint

Revoked certifications are kept in the Certification Revocation List (CRL). Client applications use the CRL to check the authentication of a server. Server applications utilize the CRL to grant or deny access requests from client applications which are no longer trusted.

You can configure your Firepower 4100/9300 chassis to validate peer certificates using Certification Revocation List (CRL) information. This option is one of a number offered for achieving Common Criteria certification compliance on your system. For more information, see [Security Certifications Compliance, on page 69](#).

Perform these steps to validate peer certificates using CRL information.

### Procedure

---

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

**scope security**

**Step 2** Enter trustpoint mode:

**scope trustpoint** *trustname*

**Step 3** Enter revoke mode:

**scope revoke**

**Step 4** Download the CRL file(s):

**import crl** *protocol://user\_id@CA\_or\_CRL\_issuer\_IP/tmp/DoDCA/CRL1.crl*

**Note**

DER format static CRL is not supported in FXOS. You must convert the DER format CRL file to PEM format using the following command:

```
openssl crl -in filename.crl -inform DER -outform PEM -out crl.pem
```

**Step 5** (Optional) Show the status of the import process of CRL information:

**show import-task detail**

**Step 6** Set the certificate revocation method to CRL-only:

```
set certrevokemethod {crl}
```

## About the Certificate Revocation List Check

You can configure your Certificate Revocation List (CRL) check mode to be either strict or relaxed in IPSec, HTTPS, and secure LDAP connections.

FXOS harvests dynamic (non-static) CRL information from the CDP information of an X.509 certificate, which indicates dynamic CRL information. System administration downloads static CRL information manually, which indicates local CRL information in the FXOS system. FXOS processes dynamic CRL information against the current processing certificate in the certificate chain. The static CRL is applied to the whole peer certificate chain.

For steps to enable or disable certificate revocation checks for your secure IPSec, LDAP, and HTTPS connections, see [Configure IPSec Secure Channel](#), [Creating an LDAP Provider](#) and [Configuring HTTPS](#).



### Note

- If the Certificate Revocation Check Mode is set to Strict, static CRL is only applicable when the peer certificate chain has a level of 1 or higher. (For example, when the peer certificate chain contains only the root CA certificate and the peer certificate signed by the root CA.)
- When configuring static CRL for IPSec, the Authority Key Identifier (authkey) field must be present in the imported CRL file. Otherwise, IPSec considers it invalid.
- Static CRL takes precedence over Dynamic CRL from the same issuer. When FXOS validates the peer certificate, if a valid (determined) static CRL of the same issuer exists, FXOS ignores the CDP in the peer certificate.
- Strict CRL checking is enabled by default in the following scenarios:
  - Newly created secure LDAP provider connections, IPSec connections, or Client Certificate entries
  - Newly deployed FXOS chassis managers (deployed with an initial starting version of FXOS 2.3.1.x or later)

The following tables describe the connection results, depending on your certificate revocation list check setting and certificate validation.

**Table 4: Certificate Revocation Check Mode set to Strict without a local static CRL**

| Without local static CRL               | LDAP Connection                    | IPSec Connection                   | Client Certificate Authentication  |
|----------------------------------------|------------------------------------|------------------------------------|------------------------------------|
| Checking peer certificate chain        | Full certificate chain is required | Full certificate chain is required | Full certificate chain is required |
| Checking CDP in peer certificate chain | Full certificate chain is required | Full certificate chain is required | Full certificate chain is required |

| Without local static CRL                                                                   | LDAP Connection                      | IPSec Connection                                                                                       | Client Certificate Authentication    |
|--------------------------------------------------------------------------------------------|--------------------------------------|--------------------------------------------------------------------------------------------------------|--------------------------------------|
| CDP checking for Root CA certificate of the peer certificate chain                         | Yes                                  | Not applicable                                                                                         | Yes                                  |
| Any certificate validation failure in the peer certificate chain                           | Connection fails with syslog message | Connection fails with syslog message                                                                   | Connection fails with syslog message |
| Any certificate revoked in the peer certificate chain                                      | Connection fails with syslog message | Connection fails with syslog message                                                                   | Connection fails with syslog message |
| One CDP is missing in the peer certificate chain                                           | Connection fails with syslog message | Peer certificate:<br>connection fails with syslog message<br><br>Intermediate CAs:<br>connection fails | Connection fails with syslog message |
| One CDP CRL is empty in the peer certificate chain with valid signature                    | Connection succeeds                  | Connection succeeds                                                                                    | Connection fails with syslog message |
| Any CDP in the peer certificate chain cannot be downloaded                                 | Connection fails with syslog message | Peer certificate:<br>Connection fails with syslog message<br><br>Intermediate CA:<br>connection fails  | Connection fails with syslog message |
| Certificate has CDP, but the CDP server is down                                            | Connection fails with syslog message | Peer certificate:<br>Connection fails with syslog message<br><br>Intermediate CA:<br>connection fails  | Connection fails with syslog message |
| Certificate has CDP, server is up, and CRL is on CDP, but the CRL has an invalid signature | Connection fails with syslog message | Peer certificate:<br>Connection fails with syslog message<br><br>Intermediate CA:<br>connection fails  | Connection fails with syslog message |

**Table 5: Certificate Revocation Check Mode set to Strict with a local static CRL**

| With local static CRL                  | LDAP Connection                    | IPSec Connection                   |
|----------------------------------------|------------------------------------|------------------------------------|
| Checking peer certificate chain        | Full certificate chain is required | Full certificate chain is required |
| Checking CDP in peer certificate chain | Full certificate chain is required | Full certificate chain is required |

| With local static CRL                                                                                                     | LDAP Connection                      | IPSec Connection                                                                                          |
|---------------------------------------------------------------------------------------------------------------------------|--------------------------------------|-----------------------------------------------------------------------------------------------------------|
| CDP checking for Root CA certificate of the peer certificate chain                                                        | Yes                                  | Not applicable                                                                                            |
| Any certificate validation failure in the peer certificate chain                                                          | Connection fails with syslog message | Connection fails with syslog message                                                                      |
| Any certificate revoked in the peer certificate chain                                                                     | Connection fails with syslog message | Connection fails with syslog message                                                                      |
| One CDP is missing in the peer certificate chain (Certificate Chain level is 1)                                           | Connection succeeds                  | Connection succeeds                                                                                       |
| One CDP CRL is empty in the peer certificate chain (Certificate Chain level is 1)                                         | Connection succeeds                  | Connection succeeds                                                                                       |
| Any CDP in the peer certificate chain cannot be downloaded (Certificate Chain level is 1)                                 | Connection succeeds                  | Connection succeeds                                                                                       |
| Certificate has CDP, but the CDP server is down (Certificate Chain level is 1)                                            | Connection succeeds                  | Connection succeeds                                                                                       |
| Certificate has CDP, server is up, and CRL is on CDP, but the CRL has an invalid signature (Certificate Chain level is 1) | Connection succeeds                  | Connection succeeds                                                                                       |
| Peer Certificate Chain level is higher than 1                                                                             | Connection fails with syslog message | If combined with CDP, connection succeeds<br><br>If there is no CDP, connection fails with syslog message |

Table 6: Certificate Revocation Check Mode set to Relaxed without a local static CRL

| Without local static CRL                                           | LDAP Connection        | IPSec Connection       | Client Certificate Authentication |
|--------------------------------------------------------------------|------------------------|------------------------|-----------------------------------|
| Checking peer certificate chain                                    | Full certificate chain | Full certificate chain | Full certificate chain            |
| Checking CDP in the peer certificate chain                         | Full certificate chain | Full certificate chain | Full certificate chain            |
| CDP checking for Root CA certificate of the peer certificate chain | Yes                    | Not applicable         | Yes                               |



| Without local static CRL                                                                   | LDAP Connection                      | IPSec Connection                     | Client Certificate Authentication    |
|--------------------------------------------------------------------------------------------|--------------------------------------|--------------------------------------|--------------------------------------|
| Any certificate validation failure in the peer certificate chain                           | Connection fails with syslog message | Connection fails with syslog message | Connection fails with syslog message |
| Any certificate revoked in the peer certificate chain                                      | Connection fails with syslog message | Connection fails with syslog message | Connection fails with syslog message |
| One CDP is missing in the peer certificate chain                                           | Connection succeeds                  | Connection succeeds                  | Connection fails with syslog message |
| One CDP CRL is empty in the peer certificate chain with valid signature                    | Connection succeeds                  | Connection succeeds                  | Connection succeeds                  |
| Any CDP in the peer certificate chain cannot be downloaded                                 | Connection succeeds                  | Connection succeeds                  | Connection succeeds                  |
| Certificate has CDP, but the CDP server is down                                            | Connection succeeds                  | Connection succeeds                  | Connection succeeds                  |
| Certificate has CDP, server is up, and CRL is on CDP, but the CRL has an invalid signature | Connection succeeds                  | Connection succeeds                  | Connection succeeds                  |

**Table 7: Certificate Revocation Check Mode set to Relaxed with a local static CRL**

| With local static CRL                                                           | LDAP Connection                      | IPSec Connection                     |
|---------------------------------------------------------------------------------|--------------------------------------|--------------------------------------|
| Checking peer certificate chain                                                 | Full certificate chain               | Full certificate chain               |
| Checking CDP in the peer certificate chain                                      | Full certificate chain               | Full certificate chain               |
| CDP checking for Root CA certificate of the peer certificate chain              | Yes                                  | Not applicable                       |
| Any certificate validation failure in the peer certificate chain                | Connection fails with syslog message | Connection fails with syslog message |
| Any certificate revoked in the peer certificate chain                           | Connection fails with syslog message | Connection fails with syslog message |
| One CDP is missing in the peer certificate chain (Certificate Chain level is 1) | Connection succeeds                  | Connection succeeds                  |

| With local static CRL                                                                                                     | LDAP Connection                      | IPSec Connection                                                                                          |
|---------------------------------------------------------------------------------------------------------------------------|--------------------------------------|-----------------------------------------------------------------------------------------------------------|
| One CDP CRL is empty in the peer certificate chain (Certificate Chain level is 1)                                         | Connection succeeds                  | Connection succeeds                                                                                       |
| Any CDP in the peer certificate chain cannot be downloaded (Certificate Chain level is 1)                                 | Connection succeeds                  | Connection succeeds                                                                                       |
| Certificate has CDP, but the CDP server is down (Certificate Chain level is 1)                                            | Connection succeeds                  | Connection succeeds                                                                                       |
| Certificate has CDP, server is up, and CRL is on CDP, but the CRL has an invalid signature (Certificate Chain level is 1) | Connection succeeds                  | Connection succeeds                                                                                       |
| Peer Certificate Chain level is higher than 1                                                                             | Connection fails with syslog message | If combined with CDP, connection succeeds<br><br>If there is no CDP, connection fails with syslog message |

## Configure CRL Periodic Download

You can configure your system to periodically download a (CRL) so that a new CRL is used every 1 to 24 hours to validate certificates.

You can use the following protocols and interfaces with this feature:

- FTP
- SCP
- SFTP
- TFTP
- USB



### Note

- SCEP and OCSP are not supported.
- You can only configure one periodic download per CRL.
- One CRL is supported per trustpoint.



**Note** You can only configure the period in one-hour intervals.

Perform these steps to configure CRL periodic download.

### Before you begin

Ensure that you have already configured your Firepower 4100/9300 chassis to validate peer certificates using (CRL) information. For more information, see [Configure Static CRL for a Trustpoint, on page 77](#).

### Procedure

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

**scope security**

**Step 2** Enter trustpoint mode:

**scope trustpoint**

**Step 3** Enter revoke mode:

**scope revoke**

**Step 4** Edit the revoke configuration:

**sh config**

**Step 5** Set your preferred configuration:

#### Example:

```
set certrevokemethod crl
set crl-poll-filename rootCA.crl
set crl-poll-path /users/myname
set crl-poll-period 1
set crl-poll-port 0
set crl-poll-protocol scp
! set crl-poll-pwd
set crl-poll-server 182.23.33.113
set crl-poll-user myname
```

**Step 6** Exit the configuration file:

**exit**

**Step 7** (Optional) Test the new configuration by downloading a new CRL:

#### Example:

```
Firepower-chassis /security/trustpoint/revoke # sh import-task
```

Import task:

| File Name | Protocol | Server | Port | Userid | State |
|-----------|----------|--------|------|--------|-------|
|           |          |        |      |        |       |

```

rootCA.crl Scp 182.23.33.113 0 myname Downloading
```

## Set the LDAP Key Ring Certificate

You can configure a secure LDAP client key ring certificate to support a TLS connection on your Firepower 4100/9300 chassis. This option is one of a number offered for achieving Common Criteria certification compliance on your system. For more information, see [Security Certifications Compliance, on page 69](#).



**Note** If Common Criteria mode is enabled, you must have SSL enabled, and you must use the server DNS information to create the key ring certificate.

If SSL is enabled for the LDAP server entry, key ring information is referenced and checked when forming a connection.

LDAP server information has to be DNS information in the CC mode for the secure LDAP connection (with SSL enabled).

Perform these steps to configure a secure LDAP client key ring certificate:.

### Procedure

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

```
scope security
```

**Step 2** Enter LDAP mode:

```
scope ldap
```

**Step 3** Enter LDAP server mode:

```
enter server {server_ip/server_dns}
```

**Step 4** Set the LDAP key ring:

```
set keyring keyring_name
```

**Step 5** Commit the configuration:

```
commit-buffer
```

# Enable Client Certificate Authentication

You can enable your system to use a client certificate in conjunction with LDAP to authenticate a user for HTTPS access. The default authentication configuration on the Firepower 4100/9300 chassis is credential-based.



**Note** If certificate authentication is enabled, that is the only form of authentication permitted for HTTPS. Certificate revocation check is not supported with the FXOS 2.1.1 release of the client certificate authentication feature.

The following requirements must be met by the Client Certificate to use this feature:

- The username must be included in the X509 attribute Subject Alternative Name - Email.
- The client certificate must be signed by a root CA that has had its certificate imported into a trustpoint on the Supervisor.

## Procedure

**Step 1** From the FXOS CLI, enter services mode:

**scope system**

**scope services**

**Step 2** (Optional) View your options for HTTPS authentication:

**set https auth-type**

**Example:**

```
Firepower-chassis /system/services # set https auth-type
cert-auth Client certificate based authentication
cred-auth Credential based authentication
```

**Step 3** Set your HTTPS authentication to client-based:

**set https auth-type cert-auth**

**Step 4** Commit the configuration:

**commit-buffer**





## CHAPTER 8

# System Administration

---

- [Changing the Management IP Address, on page 87](#)
- [Changing the Application Management IP, on page 89](#)
- [Changing the Firepower 4100/9300 Chassis Name, on page 92](#)
- [Install a Trusted Identity Certificate, on page 92](#)
- [Auto-Import Certificate Update, on page 98](#)
- [Pre-Login Banner, on page 101](#)
- [Rebooting the Firepower 4100/9300 Chassis, on page 103](#)
- [Powering Off the Firepower 4100/9300 Chassis, on page 104](#)
- [Restoring the Factory Default Configuration, on page 104](#)
- [Enabling Locator LED, on page 105](#)

## Changing the Management IP Address

### Before you begin

You can change the management IP address on the Firepower 4100/9300 chassis from the FXOS CLI.



---

**Note** After changing the management IP address, you will need to reestablish any connections to Firepower Chassis Manager or the FXOS CLI using the new address.

---

### Procedure

---

- Step 1** Connect to the FXOS CLI (see [Accessing the FXOS CLI, on page 18](#)).
- Step 2** To configure an IPv4 management IP address:
- a) Set the scope for fabric-interconnect a:  
Firepower-chassis# **scope fabric-interconnect a**
  - b) To view the current management IP address, enter the following command:  
Firepower-chassis /fabric-interconnect # **show**

c) Enter the following command to configure a new management IP address and gateway:

```
Firepower-chassis /fabric-interconnect # set out-of-band ip ip_address netmask network_mask gw gateway_ip_address
```

d) Commit the transaction to the system configuration:

```
Firepower-chassis /fabric-interconnect* # commit-buffer
```

**Step 3** To configure an IPv6 management IP address:

a) Set the scope for fabric-interconnect a:

```
Firepower-chassis# scope fabric-interconnect a
```

b) Set the scope for management IPv6 configuration:

```
Firepower-chassis /fabric-interconnect # scope ipv6-config
```

c) To view the current management IPv6 address, enter the following command:

```
Firepower-chassis /fabric-interconnect/ipv6-config # show ipv6-if
```

d) Enter the following command to configure a new management IP address and gateway:

```
Firepower-chassis /fabric-interconnect/ipv6-config # set out-of-band ipv6 ipv6_address ipv6-prefix prefix_length ipv6-gw gateway_address
```

**Note**

Only IPv6 Global Unicast addresses are supported as the chassis's IPv6 management address.

e) Commit the transaction to the system configuration:

```
Firepower-chassis /fabric-interconnect/ipv6-config* # commit-buffer
```

## Example

The following example configures an IPv4 management interface and gateway:

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # show
```

| Fabric Interconnect: |             |             |               |                  |                  |  |
|----------------------|-------------|-------------|---------------|------------------|------------------|--|
| ID                   | OOB IP Addr | OOB Gateway | OOB Netmask   | OOB IPv6 Address | OOB IPv6 Gateway |  |
| Prefix               | Operability |             |               |                  |                  |  |
| A                    | 192.0.2.112 | 192.0.2.1   | 255.255.255.0 | ::               | ::               |  |
| 64                   | Operable    |             |               |                  |                  |  |

```
Firepower-chassis /fabric-interconnect # set out-of-band ip 192.0.2.111 netmask 255.255.255.0 gw 192.0.2.1
Warning: When committed, this change may disconnect the current CLI session
Firepower-chassis /fabric-interconnect* #commit-buffer
Firepower-chassis /fabric-interconnect #
```

The following example configures an IPv6 management interface and gateway:



```

Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # scope ipv6-config
Firepower-chassis /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
 IPv6 Address Prefix IPv6 Gateway

 2001::8998 64 2001::1
Firepower-chassis /fabric-interconnect/ipv6-config # set out-of-band ipv6 2001::8999
ipv6-prefix 64 ipv6-gw 2001::1
Firepower-chassis /fabric-interconnect/ipv6-config* # commit-buffer
Firepower-chassis /fabric-interconnect/ipv6-config #

```

## Changing the Application Management IP

You can change the management IP address on the application(s) attached to your Firepower 4100/9300 chassis from the FXOS CLI. To do so, you must first change the IP information at the FXOS platform level, then change the IP information at the application level.



**Note** Changing the application management IP will result in a service interruption.

### Procedure

- 
- Step 1** Connect to the FXOS CLI. (See [Accessing the FXOS CLI, on page 18](#)).
- Step 2** Scope to the logical device:
- ```

scope ssa
scope logical-device logical_device_name

```
- Step 3** Scope to the management bootstrap and configure the new management bootstrap parameters. Note that there are differences between deployments:
- For standalone configuration of an ASA logical device:
- Enter the logical device management bootstrap:


```

scope mgmt-bootstrap asa

```
 - Enter the IP mode for the slot:


```

scope ipv4_or_6 slot_number default

```
 - (IPv4 only) Set the new IP address:


```

set ip ipv4_address mask network_mask

```
 - (IPv6 only) Set the new IP address:


```

set ip ipv6_address prefix-length prefix_length_number

```
 - Set the gateway address:

set gateway *gateway_ip_address*

- f) Commit the configuration:

commit-buffer

For a clustered configuration of ASA logical devices:

- a) Enter the cluster management bootstrap:

scope cluster-bootstrap *asa*

- b) (IPv4 only) Set the new virtual IP:

set virtual ipv4 *ip_address* **mask** *network_mask*

- c) (IPv6 only) Set the new virtual IP:

set virtual ipv6 *ipv6_address* **prefix-length** *prefix_length_number*

- d) Set the new IP pool:

set ip pool *start_ip* *end_ip*

- e) Set the gateway address:

set gateway *gateway_ip_address*

- f) Commit the configuration:

commit-buffer

For standalone and clustered configurations of Firepower Threat Defense:

- a) Enter the logical device management bootstrap:

scope mgmt-bootstrap *ftd*

- b) Enter the IP mode for the slot:

scope ipv4_or_6 *slot_number* **firepower**

- c) (IPv4 only) Set the new IP address:

set ip *ipv4_address* **mask** *network_mask*

- d) (IPv6 only) Set the new IP address:

set ip *ipv6_address* **prefix-length** *prefix_length_number*

- e) Set the gateway address:

set gateway *gateway_ip_address*

- f) Commit the configuration:

commit-buffer

Note

For a clustered configuration, you must set the new IP address for each application attached to the Firepower 4100/9300 chassis. If you have an inter-chassis cluster or a HA configuration, you must repeat these steps for each application on both chassis.

Step 4

Clear the management bootstrap information for each application:

- a) Scope to ssa mode:
scope ssa
- b) Scope to the slot:
scope slot *slot_number*
- c) Scope to the application instance:
scope app-instance *asa_or_ftd*
- d) Clear the management bootstrap information:
clear-mgmt-bootstrap
- e) Commit the configuration:
commit-buffer

Step 5 Disable the application:

disable
commit-buffer

Note

For a clustered configuration, you must clear and disable the management bootstrap information for each application attached to the Firepower 4100/9300 chassis. If you have an inter-chassis cluster or a HA configuration, you must repeat these steps for each application on both chassis.

Step 6 When the application is offline and the slot comes online again, re-enable the application.

- a) Scope back to ssa mode:
scope ssa
- b) Scope to the slot:
scope slot *slot_number*
- c) Scope to the application instance:
scope app-instance *asa_or_ftd*
- d) Enable the application:
enable
- e) Commit the configuration:
commit-buffer

Note

For a clustered configuration, you must repeat these steps to re-enable each application attached to the Firepower 4100/9300 chassis. If you have an inter-chassis cluster or a HA configuration, you must repeat these steps for each application on both chassis.

Changing the Firepower 4100/9300 Chassis Name

You can change the name used for your Firepower 4100/9300 chassis from the FXOS CLI.

Procedure

Step 1 Connect to the FXOS CLI (see [Accessing the FXOS CLI, on page 18](#)).

Step 2 Enter the system mode:

```
Firepower-chassis-A# scope system
```

Step 3 To view the current name:

```
Firepower-chassis-A /system # show
```

Step 4 To configure a new name:

```
Firepower-chassis-A /system # set name device_name
```

Step 5 Commit the transaction to the system configuration:

```
Firepower-chassis-A /fabric-interconnect* # commit-buffer
```

Example

The following example changes the devices name:

```
Firepower-chassis-A# scope system
Firepower-chassis-A /system # set name New-name
Warning: System name modification changes FC zone name and redeploys them non-disruptively
Firepower-chassis-A /system* # commit-buffer
Firepower-chassis-A /system # show

Systems:
  Name           Mode           System IP Address System IPv6 Address
  -----
  New-name       Stand Alone  192.168.100.10    ::
New-name-A /system #
```

Install a Trusted Identity Certificate

After initial configuration, a self-signed SSL certificate is generated for use with the Firepower 4100/9300 chassis web application. Because that certificate is self-signed, client browsers do not automatically trust it. The first time a new client browser accesses the Firepower 4100/9300 chassis web interface, the browser will throw an SSL warning, requiring the user to accept the certificate before accessing the Firepower 4100/9300 chassis. You can use the following procedure to generate a Certificate Signing Request (CSR) using the FXOS

CLI and install the resulting identity certificate for use with the Firepower 4100/9300 chassis. This identity certificate allows a client browser to trust the connection, and bring up the web interface with no warnings.

Procedure

-
- Step 1** Connect to the FXOS CLI. (See [Accessing the FXOS CLI](#), on page 18).
- Step 2** Enter the security module:
- scope security**
- Step 3** Create a keyring:
- create keyring** *keyring_name*
- Step 4** Set a modulus size for the private key:
- set modulus** *size*
- Step 5** Commit the configuration:
- commit-buffer**
- Step 6** Configure the CSR fields. The certificate can be generated with basic options (for example, a subject-name), and optionally more advanced options that allow information like locale and organization to be embedded in the certificate. Note that when you configure the CSR fields, the system prompts for a certificate password.
- create certreq** **subject-name** *subject_name*
- password*
- set country** *country*
- set state** *state*
- set locality** *locality*
- set org-name** *organization_name*
- set org-unit-name** *organization_unit_name*
- set subject-name** *subject_name*
- Step 7** Commit the configuration:
- commit-buffer**
- Step 8** Export the CSR to provide to your certificate authority. The certificate authority uses the CSR to create your identity certificate.
- a) Show the full CSR:
- show certreq**
- b) Copy the output starting with (and including) "-----BEGIN CERTIFICATE REQUEST-----", ending with (and including) "-----END CERTIFICATE REQUEST-----":

Example:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC6zCCAQMCAQAwdzELMAkGA1UEBhMCVVMxEzARBgNVBAGMCkNhbG1mb3JuaWEe
```

```
ETAPBgNVBACMFNhb3NlMRYwFAYDVQQKDA1DaXNjbyBTeXN0ZW1zMQwwCgYD
VQQLDANUQUMxGjAYBgNVBAMMEWZwNDEyMC50ZXN0LmxvY2FsMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs0ON5gagkfZ2fi4JVEANG+7YGgcHbnUt7LpV
yMChnKOPjBwkUMNQAlmQsRQDcbJ232/sK0fMSnyqOL8JzC7itxeVEZRyz7/ax7W
GNveg/XP+zd03nt4GXM63FsrPcPmA7EwgqDSLoShtBEV10hhf4+Nw4pKCZ+eSSkS
JkTB1ZHaKV9bttYg3kf/UEUUGk/EyrVq3B+u2DsooPVq76mTm8BwYMqHbJEv4Pmu
RjWE88yEvVwH7JTEij9OvxbatjDjVSJHZBURtCanvyBvGuLP/Q/Nmv3Lo3G9ITbL
L5gIYZVatTxp6HTUezH2MIIzOavU6d1tB9rnyxgGth5dPV0dhQIDAQABOC8wLQYJ
KoZIHvcNAQkOMSAwHjAcBgNVHREFTATghFmcDQxMjAudGVzdC5sb2NhbdANBgkq
hkiG9w0BAQsFAAOCAQEAZUfCbwx9vt5aVDcL+tATu5xFE3LA3l0ck6Gj1Nv6W/6r
jBNLxusYilrZZcW+CgnvNs4ArqYGyNVBySOavJO/VvQ1KfyxxJlOIkyx3RzEjgK0
zzzyoyrG+EZXCSHiraS8HuWvE2wFM2wwWNtHWtvcQy55+/hDPD2Bv8pQOC2Zng3I
kLfGldxWflxAxLzf5J+AuIQ0CM5HzM9Zm8zREoWT+xHtLSqAqg/aCuomN9/vEwyU
OYfoJmVAgC6AZyUnMfUfCoyuLpLwgkxBOgyaRdnea5RhiGjYQ2lDXyDjEXp7rCx9
+6bvD1ln70JCegHdCWtP75SaNyaBEPkO0365rTckbw==
-----END CERTIFICATE REQUEST-----
```

Step 9 Exit the certreq mode:

exit

Step 10 Exit the keyring mode:

exit

Step 11 Provide the CSR output to the Certificate Authority in accordance with the Certificate Authority's enrollment process. If the request is successful, the Certificate Authority sends back an identity certificate that has been digitally signed using the CA's private key.

Step 12 **Note**

All identity certificates must be in Base64 format to be imported into FXOS. If the identity certificate chain received from the Certificate Authority is in a different format, you must first convert it with an SSL tool such as OpenSSL.

Create a new trustpoint to hold the identity certificate chain.

create trustpoint *trustpoint_name*

Step 13 Enter the identity certificate chain you received from the Certificate Authority in step 11, following the instructions on screen.

Note

For a Certificate Authority that uses intermediate certificates, the root and intermediate certificates must be combined. In a text file, paste the root certificate at the top, followed by each intermediate certificate in the chain, including all BEGIN CERTIFICATE and END CERTIFICATE flags. Copy and paste that entire text block into the trustpoint.

set certchain

Example:

```
firepower /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
>-----BEGIN CERTIFICATE-----
>MIICDTCABOgAwIBAgIQYIutxPDPw6BOP3uKNgJHZDAKBggqhkiG9w0BAQDAjBTMRUw
>EwYKZCZImiZPyLQGBGRYFbG9jYWwxGDAWBoJkiaJk/IsZAEZFghuYWF1c3RpbjEg
>MB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMjUwNzI4MTc1NjU2
>WhcNMjA0NzI4MTc1NjU2WjBTMRUwEwYKZCZImiZPyLQGBGRYFbG9jYWwxGDAWBoJ
>kiaJk/IsZAEZFghuYWF1c3RpbjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4t
>UEMtQ0EwWTATBgqhkiG9w0BAQIBBggqhkiG9w0BAQIBBwNCAASvEA27V1Enq1gMtLkvJ6rx
```

```
>GXRpXWIEyuiBM4eQROqZKnkeJUkm1xmqlubaDHPJ5TMGfJQYszLBRJPq+mdrKcDl
>o2kwZzATBgkrBgEEAYI3FAIEBh4EAEMAQTAOBgNVHQ8BAf8EBAMCAYYwDwYDVR0T
>AQH/BAUwAwEB/zAdBgNVHQ4EFgQUyInbDHPPrFwEEBcbxGSgQW7pOVikwEAYJKwYB
>BAGCNxUBBAMCAQAwCgYIKoZIzj0EAwIDSAAwRQIhAP++QJTUmniB/AxPDDN63Lqy
>18odMD0FTkG4p3Tb/2yMAiAtMYh1svlgCxsQVOW0xZVRugSdoOak6n7wCjTFX9jr
>RA==
>-----END CERTIFICATE-----
>ENDOFBUF
```

- Step 14** Commit the configuration:
- commit-buffer**
- Step 15** Exit the trustpoint mode:
- exit**
- Step 16** Enter the keyring mode:
- scope keyring** *keyring_name*
- Step 17** Associate the trustpoint created in step 13 with the keyring that was created for the CSR:
- set trustpoint** *trustpoint_name*
- Step 18** Import the signed identity certificate for the server.
- set cert**
- Step 19** Paste the contents of the identity certificate provided by the Certificate authority:

Example:

Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:

```
>-----BEGIN CERTIFICATE-----
>MIIE8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAACjAKBgqhkJOPQODAjbT
>MRUwEwYKCZImiZPyLGBGRYFbG9jYWwwGDAWBgoJkiaJk/IsZAEZFghuYWF1c3Rp
>bJEGMB4GA1UEAxMxbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTYwNDI4MTMw
>OTU0WWhnMTgwNDI4MTMwOTU0WjB3MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2Fz
>aWZvcml5TERMA8GA1UEBxMIU2FuIEpvc2UxZjAUBGNVBA0TDUNpc2NvIFN5c3Rl
>bXNkDDAKBgNVBAStA1RBQzEaMBGGA1UEAxMRZnA0MTIwLnRlc3QubG9jYWwwggEi
>MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+LglUQA0b7tga
>BwdudS3sulXIwKGo48mMHCRCw1ADWZCxFANxsnbfb+wrR8xKfKo4vwnMLuK3F5U
>R1HLpV9rHtYY296D9c/7N3Tee3gZczrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
>ikoJn55JKRImRMHVkdopX1u21iDeR/9QRRSCT8TKtWrCH67YOyig9WrvqZObwHBg
>yodskS/g+a5GNYTzzIS9XAfsLMSKP06/Ftq2MONVikdkFRG0Jqe/IG8a4s/9D82a
>/cujcb0hNssvmAhh1Vq1PGnodNR7MfYwgjM5q9Tp3W0H2ufLGaa2H109XR2FAGMB
>AAGjggJYMIICVDAcBgNVHREFTATghFmcDQxMjAudGVzdC5sb2NhbdAdBgNVHQ4E
>FgQU/1WpstIEYExs8D1ZWcuHwZPtU5QwHwYDVR0jBBgwFoAUyInbDHPPrFwEEBcbx
>GSgQW7pOVikwgdwGA1UdHwSB1DCB0TCBzqCBY6CByIaBxWkYXA6Ly8vQ049bmFh
>dXN0aW4tTkFBVVNUSU4tUEMtQ0E049bmFhdXN0aW4tcGMsQ049Q0RQLENOPVB1
>YmxpYyUyMetleSUyMFN1cnZpY2VzLENOPVN1cnZpY2VzLENOPUNvbmZpZ3VyYXRp
>b24sREM9bmFhdXN0aW4sREM9bG9jYWw/Y2VydG1maWNhdGVSSXZvY2F0aW9uTG1z
>dD9iYXN1P29iamVjdENsYXNzPWNSTERpc3RyaWJldGlvb1BvaW50IHMBggrBgEF
>BQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKGgaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B
>QVVTVE1OLVBDLUNBLENOPUFJQSxDTj1QdWJsawMlMjBLZXklMjBTZXJ2aWN1cyxDTj1TZXJ2aWN1cyxDTj1Db25maWdlcmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2Fs
>P2NBQ2VydG1maWNhdGU/YmFzZT9vYmplY3RDbGFzZzljZXJ0aWZpY2F0aW9uQXV0
>aG9yaXR5MCEGCSsGAQQBgjcUAQgQUHhIAVwB1AGIAUwB1AHIAAdgB1AHIAwDgYDVVR0P
>AQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAoGCCcGSM49BAMCA0gAMEUC
>IFew7NcJirEtFRvyxjkQ4/dVo2oI6CRB308WQbYHNUu/AiEA7UdObiSJBG/PBZjm
```

```
>sgoIK60akbjotOTvUdUd9b6K1Uw=
>-----END CERTIFICATE-----
>ENDOFBUF
```

Step 20 Exit the keyring mode:

```
exit
```

Step 21 Exit the security mode:

```
exit
```

Step 22 Enter the system mode:

```
scope system
```

Step 23 Enter the services mode:

```
scope services
```

Step 24 Configure the FXOS web service to use the new certificate:

```
set https keyring keyring_name
```

Step 25 Commit the configuration:

```
commit-buffer
```

Step 26 Display the keyring associated with the HTTPS server. It should reflect the keyring name created in step 3 of this procedure. If the screen output displays the default keyring name, the HTTPS server has not yet been updated to use the new certificate:

```
show https
```

Example:

```
fp4120 /system/services # show https
Name: https
  Admin State: Enabled
  Port: 443
  Operational port: 443
  Key Ring: firepower_cert
  Cipher suite mode: Medium Strength
  Cipher suite: ALL:!ADH:!EXPORT40:!EXPORT56:!LOW:!RC4:!MD5:!IDEA:+HIGH:+MEDIUM:+EXP:+eNULL
```

Step 27 Display the contents of the imported certificate, and verify that the **Certificate Status** value displays as **Valid**:

```
scope security
```

```
show keyring keyring_name detail
```

Example:

```
fp4120 /security # scope security
fp4120 /security # show keyring firepower_cert detail
Keyring firepower_cert:
  RSA key modulus: Mod2048
  Trustpoint CA: firepower_chain
  Certificate status: Valid
  Certificate:
  Data:
```



```

Version: 3 (0x2)
Serial Number:
    45:00:00:00:0a:de:86:55:16:82:24:f3:be:00:00:00:00:00:0a
Signature Algorithm: ecdsa-with-SHA256
Issuer: DC=local, DC=naaustin, CN=naaustin-NAAUSTIN-PC-CA
Validity
    Not Before: Apr 28 13:09:54 2016 GMT
    Not After : Apr 28 13:09:54 2018 GMT
Subject: C=US, ST=California, L=San Jose, O=Cisco Systems, OU=TAC,
CN=fp4120.test.local
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
    Modulus:
        00:b3:43:8d:e6:06:a0:91:f6:76:7e:2e:09:54:40:
        0d:1b:ee:d8:1a:07:07:6e:75:2d:ec:ba:55:c8:c0:
        a1:9c:a3:8f:26:30:70:91:43:0d:40:0d:66:42:c4:
        50:0d:c6:c9:db:7d:bf:b0:ad:1f:31:29:f2:a8:e2:
        fc:27:30:bb:8a:dc:5e:54:46:51:cb:3e:ff:6b:1e:
        d6:18:db:de:83:f5:cf:fb:37:74:de:7b:78:19:73:
        3a:dc:5b:2b:3d:c3:e6:03:b1:30:82:a0:d2:2e:84:
        a1:b4:11:15:d7:48:61:7f:8f:8d:c3:8a:4a:09:9f:
        9e:49:29:12:26:44:c1:d5:91:da:29:5f:5b:b6:d6:
        20:de:47:ff:50:45:14:82:4f:c4:ca:b5:6a:dc:1f:
        ae:d8:3b:28:a0:f5:6a:ef:a9:93:9b:c0:70:60:ca:
        87:6c:91:2f:e0:f9:ae:46:35:84:f3:cc:84:bd:5c:
        07:ec:94:c4:8a:3f:4e:bf:16:da:b6:30:e3:55:22:
        47:64:15:11:b4:26:a7:bf:20:6f:1a:e2:cf:fd:0f:
        cd:9a:fd:cb:a3:71:bd:21:36:cb:2f:98:08:61:95:
        5a:b5:3c:69:e8:74:d4:7b:31:f6:30:82:33:39:ab:
        d4:e9:dd:6d:07:da:e7:cb:18:06:b6:1e:5d:3d:5d:
        1d:85
    Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Subject Alternative Name:
        DNS:fp4120.test.local
    X509v3 Subject Key Identifier:
        FF:55:A9:B2:D8:84:60:4C:6C:F0:39:59:59:CB:87:67:03:ED:BB:94
    X509v3 Authority Key Identifier:
        keyid:C8:89:DB:0C:73:EB:17:01:04:05:C6:F1:19:28:10:5B:BA:4E:54:89
    X509v3 CRL Distribution Points:
        Full Name:
            URI:ldap:///CN=naaustin-NAAUSTIN-PC-CA,CN=naaustin-pc,CN=CDP,
            CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=naaustin,
            DC=local?certificateRevocationList?base?objectClass=cRLDistributionPoint

Authority Information Access:
    CA Issuers - URI:ldap:///CN=naaustin-NAAUSTIN-PC-CA,CN=AIA,
    CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=naaustin,
    DC=local?cACertificate?base?objectClass=certificationAuthority
1.3.6.1.4.1.311.20.2:
    ...W.e.b.S.e.r.v.e.r
X509v3 Key Usage: critical
    Digital Signature, Key Encipherment
X509v3 Extended Key Usage:
    TLS Web Server Authentication
Signature Algorithm: ecdsa-with-SHA256
    30:45:02:20:57:b0:ec:d7:09:8a:b1:2d:15:1b:f2:c6:39:10:
    e3:f7:55:a3:6a:08:e8:24:41:df:4f:16:41:b6:07:35:4b:bf:
    02:21:00:ed:47:4e:6e:24:89:04:6f:cf:05:98:e6:b2:0a:08:
    2b:ad:1a:91:b8:e8:b4:e4:ef:51:d5:1d:f5:be:8a:d5:4c
-----BEGIN CERTIFICATE-----
MIIE8DCCBJagAwIBAgITRQAAAArehlUWgiTzvGAAAAAACjAKBggqhkJOPQQDAjBT
MRUwEwYKCZImiZPyLGBRfYbG9jYXNjaWwGDAWBGoJkiaJk/IsZAEZFghuYWF1c3Rp

```

```

bjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTYwNDI4MTMw
OTU0WhcNMTgwNDI4MTMwOTU0WjB3MQswCQYDVQGEwJVUzETMBEGA1UECBMKQ2Fs
aWZvcn5pYTERMA8GA1UEBxMIU2FuIEpvc2UxYjAUBgNVBAoTDUNpc2NvIFN5c3Rl
bXMxDDAKBgNVBAsTA1RBQzEaMBGGA1UEAxMRZnA0MTIwLnRlc3QubG9jYWwwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+LglUQA0b7tga
BwdudS3sulXIwKGco48mMHCQRw1ADWZCxFANxsnfb+wrR8xKfKo4vwnMLuK3F5U
R1HLpV9rHtYY296D9c/7N3Tee3gZczrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
ikoJn55JKRImRMHVkdopXlu2liDeR/9QRRSCT8TKtWrcH67YOyig9WrvqZObwHBg
yodskS/g+a5GNYTzzIS9XAfslMSKP06/Ftq2MONVIkdkFRG0Jqe/IG8a4s/9D82a
/cujcb0hNssvmAhh1Vq1PGnodNR7MfYwgjM5q9Tp3W0H2ufLGAa2H109XR2FAgMB
AAGjggJYMIICVDACBgNVHREEFTATghFmcDQxMjAudGVzdC5sb2NhbdAdBgNVHQ4E
FgQU/1WpstIEYExs8D1ZWcuHwPtu5QwHwYDVR0jBBgwFoAUyInbDHPFwEEBcbx
GSgQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzqCBY6CByIaBxWxkYXA6Ly8vQ049bmFh
dXN0aW4tTkFBVVNUSU4tUEMtQ0EsQ049bmFhdXN0aW4tcGMsQ049Q0RQLENOPVB1
YmxpYyUyMETleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRp
b24sREM9bmFhdXN0aW4sREM9bG9jYWw/Y2VydGlmawNhdGVSSXZvY2F0aW9uTG1z
dD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJldGlvb1BvaW50MIHMBggrBgEF
BQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKGgaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B
QVVTVElOLVBDLUNBLENOPUFJQSxDTj1QdWJsawMlMjBLZXklmjbTZXJ2aWNlcyxDTj1
TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2Fs
P2NBQ2VydGlmawNhdGU/YmFzZT9vYmplY3RDbGFzc1jZXJ0aWZpY2F0aW9uQXV0
aG9yaXR5MCEGCSSGAQQBgjcUAUgQUHhIAVwBLAGIAUwB1AHIAdgB1AHIdgYDVR0P
AQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0AMEUC
IFew7NcJirEtFRvyxjkQ4/dVo2oI6CRB308WQbYHNuU/AiEA7UdObiSJBG/PBZjm
sgoIK60akbjotOtvUdUd9b6K1Uw=
-----END CERTIFICATE-----

```

Zeroized: No

What to do next

To verify that the new trusted certificate is presented, navigate to the Firepower Chassis Manager by entering https://<FQDN_or_IP>/ in the address bar of a web browser.



Note

Browsers also verify the subject-name of a certificate against the input in the address bar. If the certificate is issued to the fully qualified domain name, it must be accessed that way in the browser. If it is accessed via IP address, a different SSL error is thrown (Common Name Invalid) even if the trusted certificate is used.

Auto-Import Certificate Update

When the Cisco certificate server changes its identity certificate to leverage a different root CA, the connectivity for the Smart Licensing on 4100 or 9300s running the ASA devices gets broken. Because the licensing connectivity is handled by the supervisor instead of Lina on the application, the Smart Licensing function fails. For FXOS-based devices, the issue can be resolved using the auto-import feature without an upgrade to the FXOS software.

By default, the auto-import feature is disabled. You can use the following procedure to enable the auto-import feature using the FXOS CLI.

Before you begin

DNS server should be configured to reach the [cisco certificate server](#).

Procedure

Step 1 Connect to the FXOS CLI.

Step 2 Enter the security module:

scope security

Step 3 Enable the auto-import feature.

enter tp-auto-import

Example:

```
FXOS# scope security
FXOS /security # enter tp-auto-import
FXOS /security #
```

Step 4 Commit the configuration.

commit-buffer

Step 5 Verify the auto-import status

show detail

Example:

Successful auto-import:

```
FXOS /security/tp-auto-import #
FXOS /security/tp-auto-import # show detail
Trustpoints auto import source URL: http://www.cisco.com/security/pki/trs/ios_core.p7b
TrustPoints auto import scheduled time : 22:00
Last Importing Status : Success, Imported with 23 TrustPoint(s)
TrustPoints auto Import function : Enabled
FXOS /security/tp-auto-import #
```

Auto-import failure:

```
FXOS /security/tp-auto-import #
FXOS /security/tp-auto-import # show detail
Trustpoints auto import source URL: http://www.cisco.com/security/pki/trs/ios_core.p7b
TrustPoints auto import scheduled time : 22:00
Last Importing Status : Failure
TrustPoints auto Import function : Enabled
FXOS /security/tp-auto-import #
```

Step 6 Configure the tp-auto-import feature. Set the import-time-hour.

set import-time-hour *hour* import-time-min *minutes*

Example:

```
FXOS /security/tp-auto-import # set
import-time-hour Trustpoints auto import hour time
FXOS /security/tp-auto-import # set import-time-hour
0-23 Import Time Hour
FXOS /security/tp-auto-import # set import-time-hour 7 import-time-min
0-59 Import Time Min
```

```

FXOS /security/tp-auto-import # set import-time-hour 7 import-time-min 20
<CR>
FXOS /security/tp-auto-import # set import-time-hour 7 import-time-min 20
FXOS /security/tp-auto-import* # commit-buffer
FXOS /security/tp-auto-import #

```

Note

The auto-import source URL is fixed and you must change the import time detail to minute per day. Import occurs everyday on the scheduled time of the day. If hours and minutes are not set then the certificate import occurs only once while enabling it. Certificates get downloaded as a bundle into the box under the path /opt/certstore which can only be accessed through secure-login option. Along with the bundle (ios_core.p7b), individual certificates (AutoTP1 to AutoTPn) get extracted automatically.

Step 7 After the auto-import configuration completion, enter show detail command.

show detail**Example:**

```

FXOS /security/tp-auto-import # show detail
Trustpoints auto import source URL: http://www.cisco.com/security/pki/trs/ios_core.p7b
TrustPoints auto import scheduled time : 07:20
Last Importing Status : Success, Imported with 23 TrustPoint(s)
TrustPoints auto Import function : Enabled

```

Note

The maximum certificates that can be imported is 30. Each import re-iterates for 6 times if there is any connectivity issue to Cisco Certificate Server and then updates the last importing status in the show command.

Step 8 (Optional) To disable the auto-import feature, enter the delete auto-import command.

delete tp-auto-import**Example:**

```

FXOS /security #
FXOS /security # delete tp-auto-import
FXOS /security* # commit-buffer
FXOS /security # show detail
security mode:
  Password Strength Check: No
  Minimum Password Length: 8
  Is configuration export key set: No
  Current Task:
FXOS /security # scope tp-auto-import
Error: Managed object does not exist
FXOS /security #
FXOS /security # enter tp-auto-import
FXOS /security/tp-auto-import* # show detail
FXOS /security/tp-auto-import* #

```

Note

If you disable the auto-import feature, certificates that are imported remain persistent till the time there is no change in the build. Certificates get removed if you disable the auto-import feature and then downgrade/upgrade the build.

Pre-Login Banner

With a pre-login banner, when a user logs into Firepower Chassis Manager, the system displays the banner text and the user must click **OK** on the message screen before the system prompts for the username and password. If a pre-login banner is not configured, the system goes directly to the username and password prompt.

When a user logs into the FXOS CLI, the system displays the banner text, if configured, before it prompts for the password.

Creating the Pre-Login Banner

Procedure

-
- | | |
|---------------|---|
| Step 1 | Connect to the FXOS CLI (see Accessing the FXOS CLI, on page 18). |
| Step 2 | Enter security mode:

Firepower-chassis# scope security |
| Step 3 | Enter banner security mode:

Firepower-chassis /security # scope banner |
| Step 4 | Enter the following command to create a pre-login banner:

Firepower-chassis /security/banner # create pre-login-banner |
| Step 5 | Specify the message that FXOS should display to the user before they log into Firepower Chassis Manager or the FXOS CLI:

Firepower-chassis /security/banner/pre-login-banner* # set message

Launches a dialog for entering the pre-login banner message text. |
| Step 6 | At the prompt, type a pre-login banner message. You can enter any standard ASCII character in this field. You can enter multiple lines of text with each line having up to 192 characters. Press Enter between lines.

On the line following your input, type ENDOFBUF and press Enter to finish.

Press Ctrl and C to cancel out of the set message dialog. |
| Step 7 | Commit the transaction to the system configuration:

Firepower-chassis /security/banner/pre-login-banner* # commit-buffer |
-

Example

The following example creates the pre-login banner:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
```

```

Firepower-chassis /security/banner # create pre-login-banner
Firepower-chassis /security/banner/pre-login-banner* # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>Welcome to the Firepower Security Appliance
>**Unauthorized use is prohibited**
>ENDOFBUF
Firepower-chassis /security/banner/pre-login-banner* # commit-buffer
Firepower-chassis /security/banner/pre-login-banner #

```

Modifying the Pre-Login Banner

Procedure

-
- Step 1** Connect to the FXOS CLI (see [Accessing the FXOS CLI, on page 18](#)).
- Step 2** Enter security mode:
 Firepower-chassis# **scope security**
- Step 3** Enter banner security mode:
 Firepower-chassis /security # **scope banner**
- Step 4** Enter pre-login-banner banner security mode:
 Firepower-chassis /security/banner # **scope pre-login-banner**
- Step 5** Specify the message that FXOS should display to the user before they log into Firepower Chassis Manager or the FXOS CLI:
 Firepower-chassis /security/banner/pre-login-banner # **set message**
 Launches a dialog for entering the pre-login banner message text.
- Step 6** At the prompt, type a pre-login banner message. You can enter any standard ASCII character in this field. You can enter multiple lines of text with each line having up to 192 characters. Press **Enter** between lines.
 On the line following your input, type **ENDOFBUF** and press **Enter** to finish.
 Press **Ctrl** and **C** to cancel out of the set message dialog.
- Step 7** Commit the transaction to the system configuration:
 Firepower-chassis /security/banner/pre-login-banner* # **commit-buffer**
-

Example

The following example modifies the pre-login banner:

```

Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # scope pre-login-banner
Firepower-chassis /security/banner/pre-login-banner # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.

```

```
Enter prelogin banner:
>Welcome to the Firepower Security Appliance
>**Unauthorized use is prohibited**
>ENDOFBUF
Firepower-chassis /security/banner/pre-login-banner* # commit-buffer
Firepower-chassis /security/banner/pre-login-banner #
```

Deleting the Pre-Login Banner

Procedure

-
- | | |
|---------------|---|
| Step 1 | Connect to the FXOS CLI (see Accessing the FXOS CLI , on page 18). |
| Step 2 | Enter security mode:

Firepower-chassis# scope security |
| Step 3 | Enter banner security mode:

Firepower-chassis /security # scope banner |
| Step 4 | Delete the pre-login banner from the system:

Firepower-chassis /security/banner # delete pre-login-banner |
| Step 5 | Commit the transaction to the system configuration:

Firepower-chassis /security/banner* # commit-buffer |
-

Example

The following example deletes the pre-login banner:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # delete pre-login-banner
Firepower-chassis /security/banner* # commit-buffer
Firepower-chassis /security/banner #
```

Rebooting the Firepower 4100/9300 Chassis

Procedure

-
- | | |
|---------------|--|
| Step 1 | Enter chassis mode:

scope chassis 1 |
| Step 2 | Enter the following command to reboot the chassis: |

```
reboot [reason] [no-prompt]
```

Note

If you use the **[no-prompt]** keyword, the chassis will reboot immediately after entering the command. If you do not use the **[no-prompt]** keyword, the system will not reboot until you enter the **commit-buffer** command.

The system will gracefully shut down any logical devices configured on the system and then power down each security module/engine before finally powering down and then restarting the Firepower 4100/9300 chassis. This process takes approximately 15-20 minutes.

Step 3 To monitor the reboot process:

```
scope chassis 1
```

```
show fsm status
```

Powering Off the Firepower 4100/9300 Chassis

Procedure

Step 1 Enter chassis mode:

```
scope chassis 1
```

Step 2 Enter the following command to power down the chassis:

```
shutdown [reason] [no-prompt]
```

Note

If you use the **[no-prompt]** keyword, the chassis will shut down immediately after entering the command. If you do not use the **[no-prompt]** keyword, the system will not shut down until you enter the **commit-buffer** command.

The system will gracefully shut down any logical devices configured on the system and then power down each security module/engine before finally powering down the Firepower 4100/9300 chassis. This process takes approximately 15-20 minutes. After the chassis has successfully shut down, you can then physically unplug the power on the chassis.

Step 3 To monitor the shutdown process:

```
scope chassis 1
```

```
show fsm status
```

Restoring the Factory Default Configuration

You can use the FXOS CLI to restore your Firepower 4100/9300 chassis to factory default configuration.



Note This process erases all user configuration from the chassis including any logical device configuration. After completing this procedure, you will need to reconfigure the system (see [Initial Configuration, on page 11](#)).

Procedure

-
- Step 1** (Optional) The **erase configuration** command does not remove the Smart License configuration from the chassis. If you also want to remove the Smart License configuration, perform the following steps:
- scope license**
- deregister**
- Deregistering the Firepower 4100/9300 chassis removes the device from your account. All license entitlements and certificates on the device are removed.
- Step 2** Connect to the local-management shell:
- connect local-mgmt**
- Step 3** Enter the following command to erase all user configuration from your Firepower 4100/9300 chassis and restore the chassis to its original factory default configuration:
- erase configuration**
- The system prompts you to verify that you are sure you want to erase all user configuration.
- Step 4** Confirm that you want to erase the configuration by entering **yes** at the command prompt. The system will erase all user configuration from your Firepower 4100/9300 chassis and then reboot the system.
-

Enabling Locator LED

The Locator LED helps you to locate a unit that needs physical attention. You can use the FXOS CLI to enable the Locator LED.

Procedure

-
- Step 1** Connect to the FXOS CLI.
- Step 2** To enable the Locator LED:
- Set the scope for fabric-interconnect a:
Firepower-chassis# **scope fabric-interconnect a**
 - To view the current Locator LED status, enter the following command:
Firepower-chassis# **show locator-led**

- c) Enter the following command to enable the Locator LED:

```
Firepower-chassis# enable locator-led
```

- d) Commit the transaction to the system configuration:

```
Firepower-chassis# commit-buffer
```



CHAPTER 9

Platform Settings

- [Setting the Date and Time, on page 107](#)
- [Configuring SSH, on page 114](#)
- [Configuring TLS, on page 118](#)
- [Configuring Telnet, on page 120](#)
- [Configuring SNMP, on page 121](#)
- [Configuring HTTPS, on page 131](#)
- [Configuring AAA, on page 144](#)
- [Verifying Remote AAA Server Configurations, on page 157](#)
- [Configuring Syslog, on page 158](#)
- [Configuring DNS Servers, on page 161](#)
- [Enable FIPS Mode, on page 162](#)
- [Enable Common Criteria Mode, on page 163](#)
- [Configure the IP Access List, on page 164](#)
- [Add a MAC Pool Prefix and View MAC Addresses for Container Instance Interfaces, on page 165](#)
- [Add a Resource Profile for Container Instances, on page 167](#)
- [Configure a Network Control Policy, on page 170](#)
- [Configure the Chassis URL, on page 173](#)
- [Modifying Weak Key Exchange Algorithms, on page 174](#)

Setting the Date and Time

Use the CLI commands described below to configure the network time protocol (NTP) on the system, to set the date and time manually, or to view the current system time.

NTP settings are automatically synced between the Firepower 4100/9300 chassis and any logical devices installed on the chassis.



Note

If you are deploying Firepower Threat Defense on the Firepower 4100/9300 chassis, you must configure NTP on the Firepower 4100/9300 chassis so that Smart Licensing will work properly and to ensure proper timestamps on device registrations. You should use the same NTP server for both the Firepower 4100/9300 chassis and the FMC, but note that you cannot use FMC as the NTP server for the Firepower 4100/9300 chassis.

If you are using NTP, you can view the overall synchronization status on the **Current Time** tab, or you can view the synchronization status for each configured NTP server by looking at the Server Status field in the **NTP Server** table on the **Time Synchronization** tab. If the system is unable to synchronize with a particular NTP server, you can hover over the information icon next to the Server Status for more information.

Viewing the Configured Date and Time

Procedure

-
- Step 1** Connect to the FXOS CLI (see [Accessing the FXOS CLI, on page 18](#)).
- Step 2** To view the configured time zone:
- ```
Firepower-chassis# show timezone
```
- Step 3** To view the configured date and time:
- ```
Firepower-chassis# show clock
```
-

Example

The following example shows how to display the configured time zone and current system date and time:

```
Firepower-chassis# show timezone
Timezone: America/Chicago
Firepower-chassis# show clock
Thu Jun  2 12:40:42 CDT 2016
Firepower-chassis#
```

Setting the Time Zone

Procedure

-
- Step 1** Enter system mode:
- ```
Firepower-chassis# scope system
```
- Step 2** Enter system services mode:
- ```
Firepower-chassis /system # scope services
```
- Step 3** Set the time zone:
- ```
Firepower-chassis /system/services # set timezone
```
- At this point, you are prompted to enter a number corresponding to your continent, country, and time zone region. Enter the appropriate information at each prompt.

When you have finished specifying the location information, you are prompted to confirm that the correct time zone information is being set. Enter **1** (yes) to confirm, or **2** (no) to cancel the operation.

**Step 4**

To view the configured time zone:

```
Firepower-chassis /system/services # top
```

```
Firepower-chassis# show timezone
```

**Example**

The following example configures the time zone to the Pacific time zone region, commits the transaction, and displays the configured time zone:

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # set timezone
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa 4) Arctic Ocean 7) Australia 10) Pacific Ocean
2) Americas 5) Asia 8) Europe
3) Antarctica 6) Atlantic Ocean 9) Indian Ocean
#? 2
Please select a country.
1) Anguilla 28) Haiti
2) Antigua & Barbuda 29) Honduras
3) Argentina 30) Jamaica
4) Aruba 31) Martinique
5) Bahamas 32) Mexico
6) Barbados 33) Montserrat
7) Belize 34) Nicaragua
8) Bolivia 35) Panama
9) Brazil 36) Paraguay
10) Canada 37) Peru
11) Caribbean Netherlands 38) Puerto Rico
12) Cayman Islands 39) St Barthelemy
13) Chile 40) St Kitts & Nevis
14) Colombia 41) St Lucia
15) Costa Rica 42) St Maarten (Dutch part)
16) Cuba 43) St Martin (French part)
17) Curacao 44) St Pierre & Miquelon
18) Dominica 45) St Vincent
19) Dominican Republic 46) Suriname
20) Ecuador 47) Trinidad & Tobago
21) El Salvador 48) Turks & Caicos Is
22) French Guiana 49) United States
23) Greenland 50) Uruguay
24) Grenada 51) Venezuela
25) Guadeloupe 52) Virgin Islands (UK)
26) Guatemala 53) Virgin Islands (US)
27) Guyana
#? 49
Please select one of the following time zone regions.
1) Eastern Time
2) Eastern Time - Michigan - most locations
3) Eastern Time - Kentucky - Louisville area
4) Eastern Time - Kentucky - Wayne County
5) Eastern Time - Indiana - most locations
6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
```

```

7) Eastern Time - Indiana - Pulaski County
8) Eastern Time - Indiana - Crawford County
9) Eastern Time - Indiana - Pike County
10) Eastern Time - Indiana - Switzerland County
11) Central Time
12) Central Time - Indiana - Perry County
13) Central Time - Indiana - Starke County
14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
15) Central Time - North Dakota - Oliver County
16) Central Time - North Dakota - Morton County (except Mandan area)
17) Central Time - North Dakota - Mercer County
18) Mountain Time
19) Mountain Time - south Idaho & east Oregon
20) Mountain Standard Time - Arizona (except Navajo)
21) Pacific Time
22) Pacific Standard Time - Annette Island, Alaska
23) Alaska Time
24) Alaska Time - Alaska panhandle
25) Alaska Time - southeast Alaska panhandle
26) Alaska Time - Alaska panhandle neck
27) Alaska Time - west Alaska
28) Aleutian Islands
29) Hawaii
#? 21

```

The following information has been given:

```

United States
Pacific Time

```

```

Therefore timezone 'America/Los_Angeles' will be set.
Local time is now: Wed Jun 24 07:39:25 PDT 2015.
Universal Time is now: Wed Jun 24 14:39:25 UTC 2015.
Is the above information OK?
1) Yes
2) No
#? 1
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services # top
Firepower-chassis# show timezone
Timezone: America/Los_Angeles (Pacific Time)
Firepower-chassis#

```

## Setting the Date and Time Using NTP

NTP is used to implement a hierarchical system of servers that provide a precisely synchronized time among network systems. This kind of accuracy is required for time-sensitive operations, such as validating CRLs, which include a precise time stamp. You can configure up to four NTP servers.

**Note**

- FXOS uses NTP version 3.
- If the stratum value of an external NTP server is 13 or greater, FXOS rejects the NTP server and the server will be marked as failed. Thus, synchronization between the application instance and the NTP server is not possible on the FXOS chassis.

If you have set up your own NTP server, you can find its stratum value in the `/etc/ntp.conf` file on the server. If the NTP server has stratum value of 13 or greater you can either change the stratum value in the `ntp.conf` file and restart the server or use a different NTP server (for example: `pool.ntp.org`). Once the NTP server stratum value is configured less than 13, you must remove the NTP server configuration and add it back on FXOS chassis to resync the application instance with NTP server.

**Before you begin**

If you use a hostname for the NTP server, you must configure a DNS server. See [Configuring DNS Servers, on page 161](#).

**Procedure**

- 
- Step 1** Enter system mode:
- ```
Firepower-chassis# scope system
```
- Step 2** Enter system services mode:
- ```
Firepower-chassis /system # scope services
```
- Step 3** Configure the system to use the NTP server with the specified hostname, IPv4, or IPv6 address:
- ```
Firepower-chassis /system/services # create ntp-server {hostname / ip-addr / ip6-addr}
```
- Step 4** (Optional) Configure NTP authentication.
- Only SHA1 is supported for NTP server authentication. Obtain the key ID and value from the NTP server. For example, to generate the SHA1 key on NTP server Version 4.2.8p8 or later with OpenSSL installed, enter the **ntp-keygen -M** command, and then view the key ID and value in the `ntp.keys` file. The key is used to tell both the client and server which value to use when computing the message digest.
- Note**
The SHA1 authentication key value must be in HEX format.
- a) Set the SHA1 Key ID.

```
set ntp-sha1-key-id key_id
```
 - b) Set the SHA1 Key String.

```
set ntp-sha1-key-string
```

You are prompted for the key string.
 - c) Exit `ntp-server` mode.

exit

d) Enable NTP authentication.

enable ntp-authentication

Example:

```
firepower /system/services/ntp-server* # set ntp-sha1-key-string 11
firepower /system/services/ntp-server* # set ntp-sha1-key-string
NTP SHA-1 key string: 7092334a7809ab9873124c08123df9097097fe72
firepower /system/services/ntp-server* # exit
firepower /system/services* # enable authentication
```

Step 5 Commit the transaction to the system configuration:

Firepower-chassis /system/services # **commit-buffer**

Step 6 To view the synchronization status for all configured NTP servers:

Firepower-chassis /system/services # **show ntp-server**

Step 7 To view the synchronization status for a specific NTP server:

Firepower-chassis /system/services # **scope ntp-server** {hostname | ip-addr | ip6-addr}

Firepower-chassis /system/services/ntp-server # **show detail**

Example

The following example configures an NTP server with the IP address 192.168.200.101 and commits the transaction:

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # create ntp-server 192.168.200.101
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

The following example configures an NTP server with the IPv6 address 4001::6 and commits the transaction:

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # create ntp-server 4001::6
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```


Deleting an NTP Server

Procedure

-
- | | |
|---------------|--|
| Step 1 | Enter system mode:
Firepower-chassis# scope system |
| Step 2 | Enter system services mode:
Firepower-chassis /system # scope services |
| Step 3 | Delete the NTP server with the specified hostname, IPv4, or IPv6 address:
Firepower-chassis /system/services # delete ntp-server {hostname ip-addr ip6-addr} |
| Step 4 | Commit the transaction to the system configuration:
Firepower-chassis /system/services # commit-buffer |
-

Example

The following example deletes the NTP server with the IP address 192.168.200.101 and commits the transaction:

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # delete ntp-server 192.168.200.101
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

The following example deletes the NTP server with the IPv6 address 4001::6 and commits the transaction:

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # delete ntp-server 4001::6
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

Setting the Date and Time Manually

This section describes how to set the date and time manually on the chassis. System clock modifications take effect on the chassis immediately.

**Note**

- After you manually set the chassis date and time, it could take some time for the change to be reflected in the installed logical device(s).
- When you change the time on the chassis by more than two hours, you must reboot the device as soon as possible, for example in a maintenance window, to avoid any malfunction.

**Note**

If the system clock is currently being synchronized with an NTP server, you will not be able to set the date and time manually.

Procedure

Step 1 Enter system mode:

```
Firepower-chassis# scope system
```

Step 2 Enter system services mode:

```
Firepower-chassis /system # scope services
```

Step 3 Configure the system clock:

```
Firepower-chassis /system/services # set clock month day year hour min sec
```

For month, use the first three digits of the month. Hours must be entered using the 24-hour format, where 7 pm would be entered as 19.

System clock modifications take effect immediately. You do not need to commit the buffer.

Example

The following example configures the system clock:

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # set clock jun 24 2015 15 27 00
Firepower-chassis /system/services #
```

Configuring SSH

The following procedure describes how to enable or disable SSH access to the chassis, how to enable the FXOS chassis as an SSH client, and how to configure the various algorithms used by SSH for encryption, key exchange, and message authentication for both the SSH server and SSH client.

SSH is enabled by default.

Procedure

- Step 1** Enter system mode:
Firepower-chassis # **scope system**
- Step 2** Enter system services mode:
Firepower-chassis /system # **scope services**
- Step 3** To configure SSH access to the chassis, do one of the following:
- To allow SSH access to the chassis, enter the following command:
Firepower-chassis /system/services # **enable ssh-server**
 - To disallow SSH access to the chassis, enter the following command:
Firepower-chassis /system/services # **disable ssh-server**
- Step 4** Configure encryption algorithms for the server:
Firepower-chassis /system/services # **set ssh-server encrypt-algorithm** *encrypt_algorithm*

Example:

```
Firepower /system/services # set ssh-server encrypt-algorithm ?
 3des-cbc      3des Cbc
aes128-cbc     Aes128 Cbc
aes128-ctr     Aes128 Ctr
aes192-cbc     Aes192 Cbc
aes192-ctr     Aes192 Ctr
aes256-cbc     Aes256 Cbc
aes256-ctr     Aes256 Ctr
```

Example:

Note

- 3des-cbc is not supported in Common Criteria. If Common Criteria mode is enabled on the FXOS chassis, you cannot use 3des-cbc as an encryption algorithm.
- The following encryption algorithms are not enabled by default:

```
aes128-cbc
aes192-cbc
aes265-cbc
```

- Step 5** Configure the server Diffie-Hellman (DH) key exchange algorithms:
Firepower-chassis /system/services # **set ssh-server kex-algorithm**

Example:

```
Firepower /system/services # set ssh-server kex-algorithm
diffie-hellman-group1-sha1  Diffie Hellman Group1 Sha1
diffie-hellman-group14-sha1 Diffie Hellman Group14 Sha1
```

The DH key exchange provides a shared secret that cannot be determined by either party alone. The key exchange is combined with a signature and the host key to provide host authentication. This key-exchange method provides explicit server authentication. For more information about using DH key-exchange methods, see RFC 4253.

Step 6 Set the server mac algorithms:

Firepower-chassis /system/services # **set ssh-server mac-algorithm**

Example:

```
Firepower /system/services # set ssh-server mac-algorithm
  hmac-shal      Hmac Shal
  hmac-shal-160  Hmac Shal 160
  hmac-shal-96   Hmac Shal 96
  hmac-sha2-256  Hmac Sha2 256
  hmac-sha2-512  Hmac Sha2 512
```

Step 7 For the server host key, enter the modulus size for the RSA key pairs.

The modulus value (in bits) is in multiples of 8 from 1024 to 2048. The larger the key modulus size you specify, the longer it takes to generate an RSA key pair. We recommend a value of 2048.

Firepower-chassis /system/services # **set ssh-server host-key rsa modulus_value**

Example:

```
Firepower /system/services # set ssh-server host-key rsa ?
<1024-2048> Enter number of bits (in multiples of 8)
Firepower /system/services # set ssh-server host-key rsa 2048
```

Step 8 For the server volume rekey limit, set the amount of traffic in KB allowed over the connection before FXOS disconnects from the session:

Firepower-chassis /system/services # **set ssh-server rekey-limit volume KB_of_Traffic**

Example:

```
Firepower /system/services # set /system/services # set ssh-server rekey-limit volume ?
100-4194303 Max volume limit in KB
```

Step 9 For the server time rekey limit, set the number of minutes that an SSH session can be idle before FXOS disconnects the session:

Firepower-chassis /system/services # **set ssh-server rekey-limit time minutes**

Example:

```
Firepower /system/services # set /system/services # set ssh-server rekey-limit time ?
10-1440 Max time limit in Minutes
```

Step 10 Commit the transaction to the system configuration:

Firepower /system/services # **commit-buffer**

Step 11 Configure strict host keycheck, to control SSH host key checking:

Firepower /system/services # **ssh-client stricthostkeycheck enable/disable/prompt**

Example:

```
Firepower /system/services # set ssh-client stricthostkeycheck enable
```

- **enable**-The connection is rejected if the host key is not already in the FXOS known hosts file. You must manually add hosts at the FXOS CLI using the **enter ssh-host** command in the system/services scope.

- **prompt**-You are prompted to accept or reject the host key if it is not already stored on the chassis.
- **disable**-(The default) The chassis accepts the host key automatically if it was not stored before.

Step 12 Configure encryption algorithms for the client:

Firepower-chassis /system/services # **set ssh-client encrypt-algorithm** *encrypt_algorithm*

Example:

```
Firepower /system/services # set ssh-client encrypt-algorithm ?
3des-cbc      3des Cbc
aes128-cbc    Aes128 Cbc
aes128-ctr    Aes128 Ctr
aes192-cbc    Aes192 Cbc
aes192-ctr    Aes192 Ctr
aes256-cbc    Aes256 Cbc
aes256-ctr    Aes256 Ctr
```

Note

- 3des-cbc is not supported in Common Criteria. If Common Criteria mode is enabled on the FXOS chassis, you cannot use 3des-cbc as an encryption algorithm.
- The following encryption algorithms are not enabled by default:

```
aes128-cbc
aes192-cbc
aes256-cbc
```

Step 13 Configure the client Diffie-Hellman (DH) key exchange algorithms:

Firepower-chassis /system/services # **set ssh-client kex-algorithm**

Example:

```
Firepower /system/services # set ssh-client kex-algorithm
curve25519-sha256      curve25519-sha256
curve25519-sha256_libssh_org  curve25519-sha256@libssh.org
diffie-hellman-group14-sha1 diffie-hellman-group14-sha1
diffie-hellman-group14-sha256 diffie-hellman-group14-sha256
ecdh-sha2-nistp256      ecdh-sha2-nistp256
ecdh-sha2-nistp384      ecdh-sha2-nistp384
ecdh-sha2-nistp521      ecdh-sha2-nistp521
```

The DH key exchange provides a shared secret that cannot be determined by either party alone. The key exchange is combined with a signature and the host key to provide host authentication. This key-exchange method provides explicit server authentication. For more information about using DH key-exchange methods, see RFC 4253.

Step 14 Set the client mac algorithms:

Firepower-chassis /system/services # **set ssh-client mac-algorithm**

Example:

```
Firepower /system/services # set ssh-client mac-algorithm
hmac-sha1      Hmac Sha1
hmac-sha1-160  Hmac Sha1 160
hmac-sha1-96   Hmac Sha1 96
hmac-sha2-256  Hmac Sha2 256
hmac-sha2-512  Hmac Sha2 512
```

Step 15 For the client host key, enter the modulus size for the RSA key pairs.

The modulus value (in bits) is in multiples of 8 from 1024 to 2048. The larger the key modulus size you specify, the longer it takes to generate an RSA key pair. We recommend a value of 2048.

Firepower-chassis /system/services # **set ssh-client host-key rsa modulus_value**

Example:

```
Firepower /system/services # set ssh-client host-key rsa ?
<1024-2048> Enter number of bits (in multiples of 8)
Firepower /system/services # set ssh-client host-key rsa 2048
```

Step 16 For the client volume rekey limit, set the amount of traffic in KB allowed over the connection before FXOS disconnects from the session:

Firepower-chassis /system/services # **set ssh-client rekey-limit volume KB_of_Traffic**

Example:

```
Firepower /system/services # set /system/services # set ssh-client rekey-limit volume ?
100-4194303 Max volume limit in KB
```

Step 17 For the client time rekey limit, set the number of minutes that an SSH session can be idle before FXOS disconnects the session:

Firepower-chassis /system/services # **set ssh-client rekey-limit time minutes**

Example:

```
Firepower /system/services # set /system/services # set ssh-client rekey-limit time ?
10-1440 Max time limit in Minutes
```

Step 18 Commit the transaction to the system configuration:

Firepower /system/services # **commit-buffer**

Example

The following example enables SSH access to the chassis and commits the transaction:

```
Firepower# scope system
Firepower /system # scope services
Firepower /system/services # enable ssh-server
Firepower /system/services* # commit-buffer
Firepower /system/services #
```

Configuring TLS

The Transport Layer Security (TLS) protocol provides privacy and data integrity between two communicating applications. You can use the FXOS CLI to configure the minimum TLS version allowed when the FXOS chassis communicates with external devices. Newer TLS versions provide more secure communications, older TLS versions allow for backward compatibility with older applications.

For example, if the minimum TLS version configured on your FXOS chassis is v1.1, and a client browser is configured to only run v1.0, then the client will not be able to open a connection with the FXOS Chassis Manager via HTTPS. As such, peer applications and LDAP servers must be configured appropriately.

This procedure shows how to configure and view the minimum version of TLS allowed for communication between FXOS chassis and an external device.

**Note**

- As of the FXOS 2.3(1) release, the default minimum TLS version for the FXOS chassis is v1.1.

Procedure

Step 1 Enter system mode:

```
Firepower-chassis# scope system
```

Step 2 View the TLS version options available to your system:

```
Firepower-chassis /system # set services tls-ver
```

Example:

```
Firepower-chassis /system #
Firepower-chassis /system # set services tls-ver
    v1_0  v1.0
    v1_1  v1.1
    v1_2  v1.2
```

Step 3 Set the minimum TLS version:

```
Firepower-chassis /system # set services tls-ver version
```

Example:

```
Firepower-chassis /system #
Firepower-chassis /system # set services tls-ver v1_2
```

Step 4 Commit the configuration:

```
Firepower-chassis /system # commit-buffer
```

Step 5 Show the minimum TLS version configured on your system:

```
Firepower-chassis /system # scope services
```

```
Firepower-chassis /system/services # show
```

Example:

```
Firepower-chassis /system/services # show
Name: ssh
    Admin State: Enabled
    Port: 22
Kex Algo: Diffie Hellman Group1 Sha1,Diffie Hellman Group14 Sha1
Mac Algo: Hmac Sha1,Hmac Sha1 96,Hmac Sha2 512,Hmac Sha2 256
Encrypt Algo: 3des Cbc,Aes256 Cbc,Aes128 Cbc,Aes192 Cbc,Aes256 Ctr,Aes128 Ctr,Aes192 Ctr
Auth Algo: Rsa
    Host Key Size: 2048
Volume: None Time: None
Name: telnet
    Admin State: Disabled
    Port: 23
```

```

Name: https
  Admin State: Enabled
  Port: 443
  Operational port: 443
  Key Ring: default
  Cipher suite mode: Medium Strength
  Cipher suite: ALL:!ADH:!EXPORT40:!EXPORT56:!LOW:!RC4:!MD5:!IDEA:+HIGH:+MEDIU
M:+EXP:+eNULL
  Https authentication type: Cert Auth
  Crl mode: Relaxed
TLS:
  TLS version: v1.2

```

Configuring Telnet

The following procedure describes how to enable or disable Telnet access to the chassis. Telnet is disabled by default.



Note Telnet configuration is currently only available using the CLI.

Procedure

- Step 1** Enter system mode:
Firepower-chassis # **scope system**
- Step 2** Enter system services mode:
Firepower-chassis /system # **scope services**
- Step 3** To configure Telnet access to the chassis, do one of the following:
- To allow Telnet access to the chassis, enter the following command:
Firepower-chassis /system/services # **enable telnet-server**
 - To disallow Telnet access to the chassis, enter the following command:
Firepower-chassis /system/services # **disable telnet-server**
- Step 4** Commit the transaction to the system configuration:
Firepower /system/services # **commit-buffer**
-

Example

The following example enables Telnet and commits the transaction:


```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /services # enable telnet-server
Firepower-chassis /services* # commit-buffer
Firepower-chassis /services #
```

Configuring SNMP

This section describes how to configure the Simple Network Management Protocol (SNMP) on the chassis. See the following topics for more information:

About SNMP

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network.

The SNMP framework consists of three parts:

- An SNMP manager—The system used to control and monitor the activities of network devices using SNMP.
- An SNMP agent—The software component within the chassis that maintains the data for the chassis and reports the data, as needed, to the SNMP manager. The chassis includes the agent and a collection of MIBs. To enable the SNMP agent and create the relationship between the manager and agent, enable and configure SNMP in the Firepower Chassis Manager or the FXOS CLI.
- A managed information base (MIB)—The collection of managed objects on the SNMP agent.

The chassis supports SNMPv1, SNMPv2c and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security. SNMP is defined in the following:

- RFC 3410 (<http://tools.ietf.org/html/rfc3410>)
- RFC 3411 (<http://tools.ietf.org/html/rfc3411>)
- RFC 3412 (<http://tools.ietf.org/html/rfc3412>)
- RFC 3413 (<http://tools.ietf.org/html/rfc3413>)
- RFC 3414 (<http://tools.ietf.org/html/rfc3414>)
- RFC 3415 (<http://tools.ietf.org/html/rfc3415>)
- RFC 3416 (<http://tools.ietf.org/html/rfc3416>)
- RFC 3417 (<http://tools.ietf.org/html/rfc3417>)
- RFC 3418 (<http://tools.ietf.org/html/rfc3418>)
- RFC 3584 (<http://tools.ietf.org/html/rfc3584>)



Note Be aware that SNMP versions 1 and 2c have serious known security issues: they transmit all information without encryption, including the community string, which serves as the only form of authentication in these versions.

SNMP Notifications

A key feature of SNMP is the ability to generate notifications from an SNMP agent. These notifications do not require that requests be sent from the SNMP manager. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of connection to a neighbor router, or other significant events.

The chassis generates SNMP notifications as either traps or informs. Traps are less reliable than informs because the SNMP manager does not send any acknowledgment when it receives a trap, and the chassis cannot determine if the trap was received. An SNMP manager that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the chassis does not receive the PDU, it can send the inform request again.

However, informs are available only with SNMPv2c, which is considered insecure, and is not recommended.



Note The ifindex order on the interface that uses SNMP does not change after you reboot the FXOS. However, the index number on the FXOS disk usage OID changes when you reboot the FXOS.

SNMP Security Levels and Privileges

SNMPv1, SNMPv2c, and SNMPv3 each represent a different security model. The security model combines with the selected security level to determine the security mechanism applied when the SNMP message is processed.

The security level determines the privileges required to view the message associated with an SNMP trap. The privilege level determines whether the message needs to be protected from disclosure or authenticated. The supported security level depends upon which security model is implemented. SNMP security levels support one or more of the following privileges:

- noAuthNoPriv—No authentication or encryption
- authNoPriv—Authentication but no encryption
- authPriv—Authentication and encryption

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

Supported Combinations of SNMP Security Models and Levels

The following table identifies what the combinations of security models and levels mean.

Table 8: SNMP Security Models and Levels

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication. Note While you can configure it, FXOS does not support use of <code>noAuthNoPriv</code> with SNMP version 3.
v3	authNoPriv	HMAC-SHA	No	Provides authentication based on the HMAC Secure Hash Algorithm (SHA).
v3	authPriv	HMAC-SHA	DES	Provides authentication based on the HMAC-SHA algorithm. Provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.

SNMPv3 Security Features

SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. SNMPv3 authorizes management operations only by configured users and encrypts SNMP messages. The SNMPv3 User-Based Security Model (USM) refers to SNMP message-level security and offers the following services:

- Message integrity—Ensures that messages have not been altered or destroyed in an unauthorized manner and that data sequences have not been altered to an extent greater than can occur non-maliciously.
- Message origin authentication—Ensures that the claimed identity of the user on whose behalf received data was originated is confirmed.
- Message confidentiality and encryption—Ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.

SNMP Support

The chassis provides the following support for SNMP:

Support for MIBs

The chassis supports read-only access to MIBs.

For information about the specific MIBs available and where you can obtain them, see the [Cisco FXOS MIB Reference Guide](#).

Authentication Protocol for SNMPv3 Users

The chassis supports the HMAC-SHA-96 (SHA) authentication protocol for SNMPv3 users.

AES Privacy Protocol for SNMPv3 Users

The chassis uses Advanced Encryption Standard (AES) as one of the privacy protocols for SNMPv3 message encryption and conforms with RFC 3826.

The privacy password, or priv option, offers a choice of DES or 128-bit AES encryption for SNMP security encryption. If you enable AES-128 configuration and include a privacy password for an SNMPv3 user, the chassis uses the privacy password to generate a 128-bit AES key. The AES privacy password can have a minimum of eight characters. If the passphrases are specified in clear text, you can specify a maximum of 64 characters.

Enabling SNMP and Configuring SNMP Properties

Procedure

-
- Step 1** Enter monitoring mode:
- ```
Firepower-chassis# scope monitoring
```
- Step 2** Enable SNMP:
- ```
Firepower-chassis /monitoring # enable snmp
```
- Step 3** (Optional) Enter SNMP community mode:
- ```
Firepower-chassis /monitoring # set snmp community
```
- After you enter the **set snmp community** command, you are prompted to enter the SNMP community name.
- When you specify an SNMP community name, you are also automatically enabling SNMP versions 1 and 2c for polling requests from the SNMP remote manager.
- Note**
- Be aware that SNMP versions 1 and 2c have serious known security issues: they transmit all information without encryption, including the community string, which serves as the only form of authentication in these versions.
- Step 4** Specify the SNMP community name; this community name is used as a SNMP password. The community name can be any alphanumeric string up to 32 characters.
- ```
Firepower-chassis /monitoring # Enter a snmp community: community-name
```
- There can be only one community name; however, you can use **set snmp community** to overwrite the existing name. To delete an existing community name (also disabling SNMP versions 1 and 2c for polling requests from the SNMP remote manager), enter **set snmp community** but do not type a community string; that is, simply press **Enter** again. After you commit the buffer, **show snmp** output will include the line `Is Community Set: No`.
- Step 5** Specify the system contact person responsible for SNMP. The system contact name can be any alphanumeric string up to 255 characters, such as an email address or name and telephone number.

```
Firepower-chassis /monitoring # set snmp syscontact system-contact-name
```

- Step 6** Specify the location of the host on which the SNMP agent (server) runs. The system location name can be any alphanumeric string up to 512 characters.

```
Firepower-chassis /monitoring # set snmp syslocation system-location-name
```

- Step 7** Commit the transaction to the system configuration:

```
Firepower-chassis /monitoring # commit-buffer
```

Example

The following example enables SNMP, configures an SNMP community named `SnmpCommSystem2`, configures a system contact named `contactperson`, configures a contact location named `systemlocation`, and commits the transaction:

```
Firepower-chassis# scope ssa
Firepower-chassis# show app-instance
App Name    Identifier Slot ID    Admin State Oper State    Running Version Startup Version
Deploy Type Turbo Mode Profile Name Cluster State    Cluster Role
-----
ftd          ftd1          1          Enabled    Online          7.2.0.82      7.2.0.82
Native      No              Not Applicable  None
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # enable snmp
Firepower-chassis /monitoring # set snmp adminappinstance slot 1 appname ftd id ftd1 enable
no
Firepower-chassis /monitoring* # set snmp community
Enter a snmp community: SnmpCommSystem2
Firepower-chassis /monitoring* # set snmp syscontact contactperson1
Firepower-chassis /monitoring* # set snmp syslocation systemlocation
Firepower-chassis /monitoring* # commit-buffer
Firepower-chassis /monitoring #
```

What to do next

Create SNMP traps and users.

Creating an SNMP Trap

The following procedure describes how to create SNMP traps.



Note You can define up to eight SNMP traps.

Procedure

-
- Step 1** Enter monitoring mode:
Firepower-chassis# **scope monitoring**
- Step 2** Enable SNMP:
Firepower-chassis /monitoring # **enable snmp**
- Step 3** Create an SNMP trap with the specified host name, IPv4 address, or IPv6 address.
Firepower-chassis /monitoring # **create snmp-trap** {hostname | ip-addr | ip6-addr}
- Step 4** Specify the SNMP community string, or version 3 user name, to be used with the SNMP trap:
Firepower-chassis /monitoring/snmp-trap # **set community** community-name
- Specifies the SNMPv1/v2c community string, or the SNMPv3 user name, to permit access to the trap destination. You are queried for the community name after you enter this command. The name can be up to 32 characters with no spaces; the name is not displayed as you type.
- Step 5** Specify the port to be used for the SNMP trap:
Firepower-chassis /monitoring/snmp-trap # **set port** port-num
- Step 6** Specify the SNMP version and model used for the trap:
Firepower-chassis /monitoring/snmp-trap # **set version** {v1 | v2c | v3}
- Note**
Be aware that SNMP versions 1 and 2c have serious known security issues: they transmit all information without encryption, including the community string, which serves as the only form of authentication in these versions.
- Step 7** (Optional) Specify the type of trap to send.
Firepower-chassis /monitoring/snmp-trap # **set notificationtype** {traps | informs}
- This can be:
- **traps** if you select v2c or v3 for the version.
 - **informs** if you select v2c for the version.
- Note**
An inform notification can be sent only if you select v2c for the version.
- Step 8** (Optional) If you select v3 for the version, specify the privilege associated with the trap:
Firepower-chassis /monitoring/snmp-trap # **set v3privilege** {auth | noauth | priv}
- This can be:
- **auth**—Authentication but no encryption.

- **noauth**—No authentication or encryption. Note that while you can specify it, FXOS does not support this security level with SNMPv3.
- **priv**—Authentication and encryption.

Step 9 Commit the transaction to the system configuration:

```
Firepower-chassis /monitoring/snmp-trap # commit-buffer
```

Example

The following example enables SNMP, creates an SNMP trap using an IPv4 address, specifies that the trap will use the `SnmpCommSystem2` community on port 2, sets the version to v3, sets the notification type to traps, sets the v3 privilege to priv, and commits the transaction:

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # enable snmp
Firepower-chassis /monitoring* # create snmp-trap 192.168.100.112
Firepower-chassis /monitoring/snmp-trap* # set community SnmpCommSystem2
Firepower-chassis /monitoring/snmp-trap* # set port 2
Firepower-chassis /monitoring/snmp-trap* # set version v3
Firepower-chassis /monitoring/snmp-trap* # set notificationtype traps
Firepower-chassis /monitoring/snmp-trap* # set v3privilege priv
Firepower-chassis /monitoring/snmp-trap* # commit-buffer
Firepower-chassis /monitoring/snmp-trap #
```

The following example enables SNMP, creates an SNMP trap using an IPv6 address, specifies that the trap will use the `SnmpCommSystem3` community on port 2, sets the version to v3, sets the notification type to traps, sets the v3 privilege to priv, and commits the transaction:

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # enable snmp
Firepower-chassis /monitoring* # create snmp-trap 2001::1
Firepower-chassis /monitoring/snmp-trap* # set community SnmpCommSystem3
Firepower-chassis /monitoring/snmp-trap* # set port 2
Firepower-chassis /monitoring/snmp-trap* # set version v3
Firepower-chassis /monitoring/snmp-trap* # set notificationtype traps
Firepower-chassis /monitoring/snmp-trap* # set v3privilege priv
Firepower-chassis /monitoring/snmp-trap* # commit-buffer
Firepower-chassis /monitoring/snmp-trap #
```

Deleting an SNMP Trap

Procedure

- Step 1** Enter monitoring mode:
- ```
Firepower-chassis# scope monitoring
```
- Step 2** Delete the SNMP trap with the specified hostname or IP address:

```
Firepower-chassis /monitoring # delete snmp-trap {hostname | ip-addr}
```

**Step 3** Commit the transaction to the system configuration:

```
Firepower-chassis /monitoring # commit-buffer
```

### Example

The following example deletes the SNMP trap at IP address 192.168.100.112 and commits the transaction:

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # delete snmp-trap 192.168.100.112
Firepower-chassis /monitoring* # commit-buffer
Firepower-chassis /monitoring #
```

## Creating an SNMPv3 User

### Procedure

**Step 1** Enter monitoring mode:

```
Firepower-chassis# scope monitoring
```

**Step 2** Enable SNMP:

```
Firepower-chassis /monitoring # enable snmp
```

**Step 3** Create an SNMPv3 user:

```
Firepower-chassis /monitoring # create snmp-user user-name
```

After you enter the **create snmp-user** command, you are prompted to enter a password.

The FXOS rejects any password that does not meet the following requirements:

- Must contain a minimum of 8 characters and a maximum of 80 characters.
- Must contain only letters, numbers, and the following characters:  
~!@#%^&\*()\_+{}[]\|:;'"<>./
- Must not contain the following symbols: \$ (dollar sign), ? (question mark), or = (equals sign).
- Must contain at least five different characters.
- Must not contain too many consecutively incrementing or decrementing numbers or letters. For example, the string "12345" has four such characters, and the string "ZYXW" has three. If the total number of such characters exceeds a certain limit (typically more than around 4-6 such occurrences), the simplicity check will fail.

### Note



The consecutively incrementing or decrementing character count is not reset when non-incrementing or decrementing characters are used in between. For example, abcd&!21 will fail the password check, but abcd&!25, will not.

**Step 4** Specify the use of SHA authentication:

```
Firepower-chassis /monitoring/snmp-user # set auth [sha | sha224 | sha256 | sha358]
```

**Step 5** Enable or disable the use of AES-128 encryption:

```
Firepower-chassis /monitoring/snmp-user # set aes-128 {no | yes}
```

By default, AES-128 encryption is disabled.

SNMPv3 does not support DES. If you leave AES-128 disabled, no privacy encryption will be done and any configured privacy password will have no effect.

**Note**

You cannot poll SNMPv3 FXOS device from certain NMS monitoring applications when SNMPv3 with Authpriv (DES) is enabled. If you upgrade the device from a version that supported using DES previously, you must recreate the users using AES to poll the SNMPv3 FXOS device.

**Step 6** Specify the user password:

```
Firepower-chassis /monitoring/snmp-user # set password
```

After you enter the **set password** command, you are prompted to enter and confirm the password.

**Step 7** Commit the transaction to the system configuration:

```
Firepower-chassis /monitoring/snmp-user # commit-buffer
```

---

### Example

The following example enables SNMP, creates an SNMPv3 user named snmp-user14, enables AES-128 encryption, sets the password and privacy password, and commits the transaction:

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # enable snmp
Firepower-chassis /monitoring* # create snmp-user snmp-user14
Password:
Firepower-chassis /monitoring/snmp-user* # set aes-128 yes
Firepower-chassis /monitoring/snmp-user* # set priv-password
Enter a password:
Confirm the password:
Firepower-chassis /monitoring/snmp-user* # commit-buffer
Firepower-chassis /monitoring/snmp-user #
```

## Deleting an SNMPv3 User

### Procedure

- 
- Step 1** Enter monitoring mode:  
Firepower-chassis# **scope monitoring**
- Step 2** Delete the specified SNMPv3 user:  
Firepower-chassis /monitoring # **delete snmp-user** *user-name*
- Step 3** Commit the transaction to the system configuration:  
Firepower-chassis /monitoring # **commit-buffer**
- 

### Example

The following example deletes the SNMPv3 user named snmp-user14 and commits the transaction:

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # delete snmp-user snmp-user14
Firepower-chassis /monitoring* # commit-buffer
Firepower-chassis /monitoring #
```

## Viewing Current SNMP Settings

Use the following CLI commands to display current SNMP settings, users and traps.




---

**Note** The ifIndex order on the interface of FXOS that uses SNMP does not change after you reboot the FXOS.

---

### Procedure

- 
- Step 1** Enter monitoring mode:  
firepower# **scope monitoring**
- Step 2** Display the current SNMP settings:  
firepower/monitoring # **show snmp**
- ```
Name: snmp
  Admin State: Enabled
  Port: 161
  Is Community Set: Yes
  Sys Contact: R_Admin
  Sys Location:
```

Step 3 List the currently defined SNMPv3 users:

```
firepower/monitoring # show snmp-user
```

```
SNMPv3 User:
  Name                               Authentication type
  -----
  snmp-user1                         Sha
  testuser                           Sha
  snmp-user2                         Sha
```

Step 4 List the currently defined SNMP traps:

```
firepower/monitoring # show snmp-trap
```

```
SNMP Trap:
  SNMP Trap                          Port      Community  Version  V3 Privilege  Notification Type
  -----
  trap1_informs                     162      ****      V2c      Noauth       Informs
  192.168.10.100                    162      ****      V3       Noauth       Traps
```

Example

This example show how to display detailed information about a specific SNMPv3 user:

```
firepower /monitoring # show snmp-user snmp-user1 detail
```

```
SNMPv3 User:
  Name: snmp-user1
  Authentication type: Sha
  Password: ****
  Privacy password: ****
  Use AES-128: Yes
firepower /monitoring #
```

Configuring HTTPS

This section describes how to configure HTTPS on the Firepower 4100/9300 chassis.



Note You can change the HTTPS port using Firepower Chassis Manager or the FXOS CLI. All other HTTPS configuration can only be done using the FXOS CLI.

Certificates, Key Rings, and Trusted Points

HTTPS uses components of the Public Key Infrastructure (PKI) to establish secure communications between two devices, such as a client's browser and the Firepower 4100/9300 chassis.

Encryption Keys and Key Rings

Each PKI device holds a pair of asymmetric Rivest-Shamir-Adleman (RSA) encryption keys, one kept private and one made public, stored in an internal key ring. A message encrypted with either key can be decrypted with the other key. To send an encrypted message, the sender encrypts the message with the receiver's public key, and the receiver decrypts the message using its own private key. A sender can also prove its ownership of a public key by encrypting (also called 'signing') a known message with its own private key. If a receiver can successfully decrypt the message using the public key in question, the sender's possession of the corresponding private key is proven. Encryption keys can vary in length, with typical lengths from 512 bits to 2048 bits. In general, a longer key is more secure than a shorter key. FXOS provides a default key ring with an initial 2048-bit key pair, and allows you to create additional key rings.

The default key ring certificate must be manually regenerated if the cluster name changes or the certificate expires.

Certificates

To prepare for secure communications, two devices first exchange their digital certificates. A certificate is a file containing a device's public key along with signed information about the device's identity. To merely support encrypted communications, a device can generate its own key pair and its own self-signed certificate. When a remote user connects to a device that presents a self-signed certificate, the user has no easy method to verify the identity of the device, and the user's browser will initially display an authentication warning. By default, FXOS contains a built-in self-signed certificate containing the public key from the default key ring.

Trusted Points

To provide stronger authentication for FXOS, you can obtain and install a third-party certificate from a trusted source, or trusted point, that affirms the identity of your device. The third-party certificate is signed by the issuing trusted point, which can be a root certificate authority (CA) or an intermediate CA or trust anchor that is part of a trust chain that leads to a root CA. To obtain a new certificate, you must generate a certificate request through FXOS and submit the request to a trusted point.



Important The certificate must be in Base64 encoded X.509 (CER) format.

Creating a Key Ring

FXOS supports a maximum of 8 key rings, including the default key ring.

Procedure

-
- Step 1** Enter security mode:
Firepower-chassis # **scope security**
 - Step 2** Create and name the key ring:
Firepower-chassis # **create keyring** *keyring-name*
 - Step 3** Set the SSL key length in bits:

```
Firepower-chassis # set modulus {mod1024 | mod1536 | mod2048 | mod512}
```

Step 4 Commit the transaction:

```
Firepower-chassis # commit-buffer
```

Example

The following example creates a keyring with a key size of 1024 bits:

```
Firepower-chassis# scope security
Firepower-chassis /security # create keyring kr220
Firepower-chassis /security/keyring* # set modulus mod1024
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring #
```

What to do next

Create a certificate request for this key ring.

Regenerating the Default Key Ring

The default key ring certificate must be manually regenerated if the cluster name changes or the certificate expires.



Note The default keyring is only used by FCM on FXOS.

Procedure

Step 1 Enter security mode:

```
Firepower-chassis # scope security
```

Step 2 Enter key ring security mode for the default key ring:

```
Firepower-chassis /security # scope keyring default
```

Step 3 Regenerate the default key ring:

```
Firepower-chassis /security/keyring # set regenerate yes
```

Step 4 Commit the transaction:

```
Firepower-chassis # commit-buffer
```

Example

The following example regenerates the default key ring:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring default
Firepower-chassis /security/keyring* # set regenerate yes
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring #
```

Creating a Certificate Request for a Key Ring

Creating a Certificate Request for a Key Ring with Basic Options

Procedure

-
- | | |
|---------------|---|
| Step 1 | Enter security mode:

Firepower-chassis # scope security |
| Step 2 | Enter configuration mode for the key ring:

Firepower-chassis /security # scope keyring <i>keyring-name</i> |
| Step 3 | Create a certificate request using the IPv4 or IPv6 address specified, or the name of the fabric interconnect. You are prompted to enter a password for the certificate request.

Firepower-chassis /security/keyring # create certreq {ip [<i>ipv4-addr</i> <i>ipv6-v6</i>] subject-name <i>name</i> } |
| Step 4 | Commit the transaction:

Firepower-chassis /security/keyring/certreq # commit-buffer |
| Step 5 | Display the certificate request, which you can copy and send to a trust anchor or certificate authority:

Firepower-chassis /security/keyring # show certreq |
-

Example

The following example creates and displays a certificate request with an IPv4 address for a key ring, with basic options:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq ip 192.168.200.123 subject-name sjc04
Certificate request password:
Confirm certificate request password:
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name:
```

```

Certificate request country name:
State, province or county (full name):
Locality (eg, city):
Organization name (eg, company):
Organization Unit name (eg, section):
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZ04UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHO4SwccAUXQ5Zngf45YtX1Wsy1wUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNlECSEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHU003Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWicTWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGx1DNqoN+odCXPc5kjoxD01ZTL09H
BA==
-----END CERTIFICATE REQUEST-----

Firepower-chassis /security/keyring #

```

What to do next

- Copy the text of the certificate request, including the BEGIN and END lines, and save it in a file. Send the file with the certificate request to a trust anchor or certificate authority to obtain a certificate for the key ring.
- Create a trusted point and set the certificate chain for the certificate of trust received from the trust anchor.

Creating a Certificate Request for a Key Ring with Advanced Options

Procedure

- | | |
|---------------|--|
| Step 1 | Enter security mode:
Firepower-chassis # scope security |
| Step 2 | Enter configuration mode for the key ring:
Firepower-chassis /security # scope keyring <i>keyring-name</i> |
| Step 3 | Create a certificate request:
Firepower-chassis /security/keyring # create certreq |
| Step 4 | Specify the country code of the country in which the company resides:
Firepower-chassis /security/keyring/certreq* # set country <i>country name</i> |
| Step 5 | Specify the Domain Name Server (DNS) address associated with the request:
Firepower-chassis /security/keyring/certreq* # set dns <i>DNS Name</i> |
| Step 6 | Specify the email address associated with the certificate request:
Firepower-chassis /security/keyring/certreq* # set e-mail <i>E-mail name</i> |
| Step 7 | Specify the IP address of the Firepower 4100/9300 chassis: |

```
Firepower-chassis /security/keyring/certreq* # set ip {certificate request ip-address/certificate request ip6-address }
```

Step 8 Specify the city or town in which the company requesting the certificate is headquartered:

```
Firepower-chassis /security/keyring/certreq* # set locality locality name (eg, city)
```

Step 9 Specify the organization requesting the certificate:

```
Firepower-chassis /security/keyring/certreq* # set org-name organization name
```

Step 10 Specify the organizational unit:

```
Firepower-chassis /security/keyring/certreq* # set org-unit-name organizational unit name
```

Step 11 Specify an optional password for the certificate request:

```
Firepower-chassis /security/keyring/certreq* # set password certificate request password
```

Step 12 Specify the state or province in which the company requesting the certificate is headquartered:

```
Firepower-chassis /security/keyring/certreq* # set state state, province or county
```

Step 13 Specify the fully qualified domain name of the Firepower 4100/9300 chassis:

```
Firepower-chassis /security/keyring/certreq* # set subject-name certificate request name
```

Step 14 Commit the transaction:

```
Firepower-chassis /security/keyring/certreq # commit-buffer
```

Step 15 Display the certificate request, which you can copy and send to a trust anchor or certificate authority:

```
Firepower-chassis /security/keyring # show certreq
```

Example



Note We recommend not to commit buffer with a "set dns" or "set subject-name" without FQDN for releases earlier than 2.7. If you try to create a certification requirement with a DNS or subject name that is not a FQDN, it will throw an error.

The following example creates and displays a certificate request with an IPv4 address for a key ring, with advanced options:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq
Firepower-chassis /security/keyring/certreq* # set "ip 192.168.200.123"
Firepower-chassis /security/keyring/certreq* # set subject-name "sjc04"
Firepower-chassis /security/keyring/certreq* # set country "US"
Firepower-chassis /security/keyring/certreq* # set dns "bg1-samc-15A"
Firepower-chassis /security/keyring/certreq* # set email "test@cisco.com"
Firepower-chassis /security/keyring/certreq* # set locality "new york city"
Firepower-chassis /security/keyring/certreq* # set org-name "Cisco Systems"
Firepower-chassis /security/keyring/certreq* # set org-unit-name "Testing"
```



```

Firepower-chassis /security/keyring/certreq* # set state "new york"
Firepower-chassis /security/keyring/certreq* # commit-buffer
Firepower-chassis /security/keyring/certreq # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name: test@cisco.com
Certificate request country name: US
State, province or county (full name): New York
Locality name (eg, city): new york city
Organization name (eg, company): Cisco
Organization Unit name (eg, section): Testing
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKnlt8qMZ04UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHO4SwccAUXQ5Zngf45YtXlWsywUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNlECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHU003Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWICtWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA7l8S+V8ndXr1HejiQGx1DNqoN+odCXPC5kjoXD0lZTL09H
BA==
-----END CERTIFICATE REQUEST-----

Firepower-chassis /security/keyring/certreq #

```

What to do next

- Copy the text of the certificate request, including the BEGIN and END lines, and save it in a file. Send the file with the certificate request to a trust anchor or certificate authority to obtain a certificate for the key ring.
- Create a trusted point and set the certificate chain for the certificate of trust received from the trust anchor.

Creating a Trusted Point

Procedure

- | | |
|---------------|---|
| Step 1 | Enter security mode:
Firepower-chassis # scope security |
| Step 2 | Create a trusted point:
Firepower-chassis /security # create trustpoint <i>name</i> |
| Step 3 | Specify certificate information for this trusted point:
Firepower-chassis /security/trustpoint # set certchain [<i>certchain</i>] |

If you do not specify certificate information in the command, you are prompted to enter a certificate or a list of trustpoints defining a certification path to the root certificate authority (CA). On the next line following your input, type **ENDOFBUF** to finish.

Important

The certificate must be in Base64 encoded X.509 (CER) format.

- Step 4** Commit the transaction:
- ```
Firepower-chassis /security/trustpoint # commit-buffer
```

### Example

The following example creates a trusted point and provides a certificate for the trusted point:

```
Firepower-chassis# scope security
Firepower-chassis /security # create trustpoint tPoint10
Firepower-chassis /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMDCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADBOMQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGx1IEluYy4xEzARBGNVBAsT
> ClRlc3QgR3JvdXAuGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWZHVzZXJAZXhhbXBsZS5jb20wZGZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YccYU
> ZgAMivvyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBKOND1
> GmbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAGMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG6lCaJoJaVMhzC1903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSSxRetysOhqHmp9+CLv8FDuy1CDYfuaLtlvWvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3nO4MIGeBgNVHSMEgZYwgZOAFLlNjtcEMyZ+f7+3yh42
> 1ido3nO4oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAcT
> ClNhbnRhIENsYXJhMRswGQYDVQQKEwJ0dW92YSBTeXN0ZW1zIEluYy4xFDASBgNV
> BAStC0VuZ21uZWVyaW5nMQswDQYDVQQDEwZ0ZXN0Q0GCAQAwdAYDVR0TBAAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAahWaRwXNR6B4g6Lsnr+fptHv+WWhB5fKqGQqXc
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8copP1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/trustpoint* # commit-buffer
Firepower-chassis /security/trustpoint #
```

### What to do next

Obtain a key ring certificate from the trust anchor or certificate authority and import it into the key ring.

## Importing a Certificate into a Key Ring

### Before you begin

- Configure a trusted point that contains the certificate chain for the key ring certificate.
- Obtain a key ring certificate from a trust anchor or certificate authority.



#### Note

If you change the certificate in a key ring that has already been configured on HTTPS, you must restart HTTPS in order for the new certificate to take effect. For more information, see: [Restarting HTTPS, on page 142](#).

## Procedure

- 
- Step 1** Enter security mode:  
Firepower-chassis # **scope security**
- Step 2** Enter configuration mode for the key ring that will receive the certificate:  
Firepower-chassis /security # **scope keyring** *keyring-name*
- Step 3** Specify the trusted point for the trust anchor or certificate authority from which the key ring certificate was obtained:  
Firepower-chassis /security/keyring # **set trustpoint** *name*
- Step 4** Launch a dialog for entering and uploading the key ring certificate:  
Firepower-chassis /security/keyring # **set cert**
- At the prompt, paste the certificate text that you received from the trust anchor or certificate authority. On the next line following the certificate, type **ENDOFBUF** to complete the certificate input.
- Important**  
The certificate must be in Base64 encoded X.509 (CER) format.
- Step 5** Commit the transaction:  
Firepower-chassis /security/keyring # **commit-buffer**
- 

## Example

The following example specifies the trust point and imports a certificate into a key ring:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # set trustpoint tPoint10
Firepower-chassis /security/keyring* # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
> -----BEGIN CERTIFICATE-----
> MIIB/zCCAwgCAQAwgZkxCzAJBgNVBAYTA1VTMQswCQYDVQQIEwJDQTEVMBMGA1UE
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGx1IEluYy4xEzARBgNVBASt
> C1Rlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivYCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgd4VBKOND1
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG6lCaJoJaVMhzC190306Mg51zqlzXcz75+VFj2I6rH9asckCl3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtlvLWvfhevskV0j6
> mK3Ku+YiORnv6DhxrOoqau8r/hyI/L4317IPN1HhOi3oha4=
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring #
```

**What to do next**

Configure your HTTPS service with the key ring.

## Configuring HTTPS

**Caution**

After you complete the HTTPS configuration, including changing the port and key ring to be used by HTTPS, all current HTTP and HTTPS sessions are closed without warning as soon as you save or commit the transaction.

**Procedure**

- 
- Step 1** Enter system mode:  
Firepower-chassis# **scope system**
- Step 2** Enter system services mode:  
Firepower-chassis /system # **scope services**
- Step 3** Enable the HTTPS service:  
Firepower-chassis /system/services # **enable https**
- Step 4** (Optional) Specify the port to be used for the HTTPS connection:  
Firepower-chassis /system/services # **set https port** *port-num*
- Step 5** (Optional) Specify the name of the key ring you created for HTTPS:  
Firepower-chassis /system/services # **set https keyring** *keyring-name*
- Step 6** (Optional) Specify the level of Cipher Suite security used by the domain:  
Firepower-chassis /system/services # **set https cipher-suite-mode** *cipher-suite-mode*  
*cipher-suite-mode* can be one of the following keywords:
- **high-strength**
  - **medium-strength**
  - **low-strength**
  - **custom**—Allows you to specify a user-defined Cipher Suite specification string.
- Step 7** (Optional) If **cipher-suite-mode** is set to **custom**, specify a custom level of Cipher Suite security for the domain:  
Firepower-chassis /system/services # **set https cipher-suite** *cipher-suite-spec-string*  
*cipher-suite-spec-string* can contain up to 256 characters and must conform to the OpenSSL Cipher Suite specifications. You cannot use any spaces or special characters except ! (exclamation point), + (plus sign), - (hyphen), and : (colon). For details, see [http://httpd.apache.org/docs/2.0/mod/mod\\_ssl.html#sslcipher-suite](http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslcipher-suite).

For example, the medium strength specification string FXOS uses as the default is:

**ALL: !ADH: !EXPORT56: !LOW: RC4+RSA: +HIGH: +MEDIUM: +EXP: +eNULL**

#### Note

This option is ignored if **cipher-suite-mode** is set to anything other than **custom**.

**Step 8** (Optional) Enable or disable the certificate revocation list check:

**set revoke-policy { relaxed | strict }**

**Step 9** Commit the transaction to the system configuration:

Firepower-chassis /system/services # **commit-buffer**

#### Example

The following example enables HTTPS, sets the port number to 443, sets the key ring name to kring7984, sets the Cipher Suite security level to high, and commits the transaction:

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # enable https
Firepower-chassis /system/services* # set https port 443
Warning: When committed, this closes all the web sessions.
Firepower-chassis /system/services* # set https keyring kring7984
Firepower-chassis /system/services* # set https cipher-suite-mode high
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

## Changing the HTTPS Port

The HTTPS service is enabled on port 443 by default. You cannot disable HTTPS, but you can change the port to use for HTTPS connections.

#### Procedure

**Step 1** Enter system mode:

Firepower-chassis # **scope system**

**Step 2** Enter system services mode:

Firepower-chassis /system # **scope services**

**Step 3** Specify the port to use for HTTPS connections:

Firepower-chassis /system/services # **set https port port-number**

Specify an integer between 1 and 65535 for *port-number*. HTTPS is enabled on port 443 by default.

**Step 4** Commit the transaction to the system configuration:

Firepower /system/services # **commit-buffer**

After changing the HTTPS port, all current HTTPS sessions are closed. Users will need to log back in to the Firepower Chassis Manager using the new port as follows:

**`https://<chassis_mgmt_ip_address>:<chassis_mgmt_port>`**

where `<chassis_mgmt_ip_address>` is the IP address or host name of the chassis that you entered during initial configuration and `<chassis_mgmt_port>` is the HTTPS port you have just configured.

### Example

The following example sets the HTTPS port number to 443 and commits the transaction:

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # set https port 444
Warning: When committed, this closes all the web sessions.
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

## Restarting HTTPS

If you change the certificate in a key ring that has already been configured on HTTPS, you must restart HTTPS in order for the new certificate to take effect. Use the following procedure to reset HTTPS with an updated keyring.

### Procedure

- 
- Step 1** Enter system mode:  
Firepower-chassis# **scope system**
  - Step 2** Enter system services mode:  
Firepower-chassis /system # **scope services**
  - Step 3** Set the HTTPS key ring back to its default value:  
Firepower-chassis /system/services # **set https keyring default**
  - Step 4** Commit the transaction to the system configuration:  
Firepower-chassis /system/services # **commit-buffer**
  - Step 5** Wait five seconds.
  - Step 6** Set HTTPS with the key ring you created:  
Firepower-chassis /system/services # **set https keyring** *keyring-name*
  - Step 7** Commit the transaction to the system configuration:

```
Firepower-chassis /system/services # commit-buffer
```

---

## Deleting a Key Ring

### Procedure

---

- Step 1** Enter security mode:  
Firepower-chassis # **scope security**
- Step 2** Delete the named key ring:  
Firepower-chassis /security # **delete keyring** *name*
- Step 3** Commits the transaction:  
Firepower-chassis /security # **commit-buffer**
- 

### Example

The following example deletes a key ring:

```
Firepower-chassis# scope security
Firepower-chassis /security # delete keyring key10
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

## Deleting a Trusted Point

### Before you begin

Ensure that the trusted point is not used by a key ring.

### Procedure

---

- Step 1** Enters security mode:  
Firepower-chassis# **scope security**
- Step 2** Delete the named trusted point:  
Firepower-chassis /security # **delete trustpoint** *name*
- Step 3** Commits the transaction:

```
Firepower-chassis /security # commit-buffer
```

---

### Example

The following example deletes a trusted point:

```
Firepower-chassis# scope security
Firepower-chassis /security # delete trustpoint tPoint10
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

## Disabling HTTPS

### Procedure

---

- Step 1** Enter system mode:  
Firepower-chassis# **scope system**
  - Step 2** Enter system services mode:  
Firepower-chassis /system # **scope services**
  - Step 3** Disable the HTTPS service:  
Firepower-chassis /system/services # **disable https**
  - Step 4** Commit the transaction to the system configuration:  
Firepower-chassis /system/services # **commit-buffer**
- 

### Example

The following example disables HTTPS and commits the transaction:

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # disable https
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

## Configuring AAA

This section describes authentication, authorization, and accounting. See the following topics for more information:



## About AAA

Authentication, Authorization and Accounting (AAA) is a set of services for controlling access to network resources, enforcing policies, assessing usage, and providing the information necessary to bill for services. Authentication identifies the user. Authorization implements policies that determine which resources and services an authenticated user may access. Accounting keeps track of time and data resources that are used for billing and analysis. These processes are considered important for effective network management and security.

### Authentication

Authentication provides a way to identify each user, typically by having the user enter a valid user name and valid password before access is granted. The AAA server compares the user's provided credentials with user credentials stored in a database. If the credentials are matched, the user is permitted access to the network. If the credentials do not match, authentication fails and network access is denied.

You can configure the Firepower 4100/9300 chassis to authenticate administrative connections to the chassis, including the following sessions:

- HTTPS
- SSH
- Serial console

### Authorization

Authorization is the process of enforcing policies: determining what types of activities, resources, or services each user is permitted to access. After authentication, a user may be authorized for different types of access or activity.

### Accounting

Accounting measures the resources a user consumes during access, which may include the amount of system time or the amount of data that a user has sent or received during a session. Accounting is carried out through the logging of session statistics and usage information, which is used for authorization control, billing, trend analysis, resource utilization, and capacity planning activities.

### Interaction Between Authentication, Authorization, and Accounting

You can use authentication alone, or with authorization and accounting. Authorization always requires a user to be authenticated first. You can use accounting alone, or with authentication and authorization.

### Supported Types of Authentication

FXOS supports the following types of user Authentication:

- **Remote** – The following network AAA services are supported:
  - LDAP
  - RADIUS
  - TACACS+

- **Local** – The chassis maintains a local database that you can populate with user profiles. You can use this local database instead of AAA servers to provide user authentication, authorization, and accounting.

### User Roles

FXOS supports local and remote Authorization in the form of user-role assignment. The roles that can be assigned are:

- **Admin** – Complete read-and-write access to the entire system. The default admin account is assigned this role by default and it cannot be changed.
- **AAA Administrator** – Read-and-write access to users, roles, and AAA configuration. Read access to the rest of the system.
- **Operations** – Read-and-write access to NTP configuration, Smart Call Home configuration for Smart Licensing, and system logs, including syslog servers and faults. Read access to the rest of the system.
- **Read-Only** – Read-only access to system configuration with no privileges to modify the system state.

See [User Management, on page 37](#) for more information about local users and role assignments.

## Setting Up AAA

These steps provide a basic outline for setting up Authentication, Authorization and Accounting (AAA) on a Firepower 4100/9300 appliance.

1. Configure the desired type(s) of user authentication:

- **Local** – User definitions and local authentication are part of [User Management, on page 37](#).
- **Remote** – Configuring remote AAA server access is part of Platform Settings, specifically:
  - [Configuring LDAP Providers, on page 147](#)
  - [Configuring RADIUS Providers, on page 151](#)
  - [Configuring TACACS+ Providers, on page 154](#)




---

**Note** If you will be using remote AAA servers, be sure to enable and configure AAA services on the remote servers before configuring remote AAA server access on the chassis.

---

2. Specify the default authentication method—this also is part of [User Management, on page 37](#).




---

**Note** If Default Authentication and Console Authentication are both set to use the same remote authentication protocol (RADIUS, TACACS+, or LDAP), you cannot change certain aspects of that server's configuration (for example, deleting that server, or changing its order of assignment) without updating these user settings.

---

## Configuring LDAP Providers

### Configuring Properties for LDAP Providers

The properties that you configure in this task are the default settings for all provider connections of this type. If an individual provider includes a setting for any of these properties, the FXOS uses that setting and ignores the default setting.

If you are using Active Directory as your LDAP server, create a user account in the Active Directory server to bind with the FXOS. This account should be given a non-expiring password.

#### Procedure

- 
- |               |                                                                                                                                                                                                                                                                                                                                              |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Enter security mode:<br>Firepower-chassis# <b>scope security</b>                                                                                                                                                                                                                                                                             |
| <b>Step 2</b> | Enter security LDAP mode:<br>Firepower-chassis /security # <b>scope ldap</b>                                                                                                                                                                                                                                                                 |
| <b>Step 3</b> | Restrict database searches to records that contain the specified attribute:<br>Firepower-chassis /security/ldap # <b>set attribute</b> <i>attribute</i>                                                                                                                                                                                      |
| <b>Step 4</b> | Restrict database searches to records that contain the specified distinguished name:<br>Firepower-chassis /security/ldap # <b>set basedn</b> <i>distinguished-name</i>                                                                                                                                                                       |
| <b>Step 5</b> | Restrict database searches to records that contain the specified filter:<br>Firepower-chassis /security/ldap # <b>set filter</b> <i>filter</i><br><br>where <i>filter</i> is the filter attribute to use with your LDAP server, for example <i>cn=\$userid</i> or <i>sAMAccountName=\$userid</i> . The filter must include <i>\$userid</i> . |
| <b>Step 6</b> | Set the amount of time the system will wait for a response from the LDAP server before noting the server as down:<br>Firepower-chassis /security/ldap # <b>set timeout</b> <i>seconds</i>                                                                                                                                                    |
| <b>Step 7</b> | Commit the transaction to the system configuration:<br>Firepower-chassis /security/ldap # <b>commit-buffer</b>                                                                                                                                                                                                                               |
- 

#### Example

The following example sets the LDAP attribute to CiscoAvPair, the base distinguished name to "DC=cisco-firepower-aaa3,DC=qalab,DC=com", the filter to sAMAccountName=\$userid, and the timeout interval to 5 seconds, and commits the transaction:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope ldap
Firepower-chassis /security/ldap # set attribute CiscoAvPair
```

```
Firepower-chassis /security/ldap* # set basedn "DC=cisco-firepower-aaa3,DC=qalab,DC=com"
Firepower-chassis /security/ldap* # set filter sAMAccountName=$userid
Firepower-chassis /security/ldap* # set timeout 5
Firepower-chassis /security/ldap* # commit-buffer
Firepower-chassis /security/ldap #
```




---

**Note** User login will fail if the DN for an LDAP user exceeds 255 characters.

---

### What to do next

Create an LDAP provider.

## Creating an LDAP Provider

Follow these steps to define and configure a LDAP provider—that is, a specific remote server providing LDAP-based AAA services for this appliance.




---

**Note** The FXOS supports a maximum of 16 LDAP providers.

---

### Before you begin

If you are using Active Directory as your LDAP server, create a user account in the Active Directory server to bind with the FXOS. This account should be given a non-expiring password.

## Procedure

- 
- |               |                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Enter security mode:<br>Firepower-chassis# <b>scope security</b>                                                                                                                                                                                                                                                                                                                           |
| <b>Step 2</b> | Enter security LDAP mode:<br>Firepower-chassis /security # <b>scope ldap</b>                                                                                                                                                                                                                                                                                                               |
| <b>Step 3</b> | Create an LDAP server instance and enter security LDAP server mode:<br>Firepower-chassis /security/ldap # <b>create server</b> <i>server-name</i><br><br>If SSL is enabled, the <i>server-name</i> , typically an IP address or FQDN, must exactly match a Common Name (CN) in the LDAP server's security certificate. Unless an IP address is specified, a DNS server must be configured. |
| <b>Step 4</b> | (Optional) Set an LDAP attribute that stores the values for the user roles and locales:<br>Firepower-chassis /security/ldap/server # <b>set attribute</b> <i>attr-name</i><br><br>This property is always a name-value pair. The system queries the user record for the value that matches this attribute name.                                                                            |

This value is required unless a default attribute has been set for LDAP providers.

- Step 5** (Optional) Set the specific distinguished name in the LDAP hierarchy where the server should begin a search when a remote user logs in and the system attempts to get the user's DN based on their user name:

Firepower-chassis /security/ldap/server # **set basedn** *basedn-name*

The length of the base DN can be a maximum of 255 characters minus the length of CN=username, where username identifies the remote user attempting to access Firepower Chassis Manager or the FXOS CLI using LDAP authentication.

This value is required unless a default base DN has been set for LDAP providers.

- Step 6** (Optional) Set the distinguished name (DN) for an LDAP database account that has read and search permissions for all objects under the base DN:

Firepower-chassis /security/ldap/server # **set binddn** *binddn-name*

The maximum supported string length is 255 ASCII characters.

- Step 7** (Optional) Restrict the LDAP search to user names that match the defined filter.

Firepower-chassis /security/ldap/server # **set filter** *filter-value*

where *filter-value* is the filter attribute to use with your LDAP server; for example *cn=\$userid* or *sAMAccountName=\$userid*. The filter must include *\$userid*.

This value is required unless a default filter has been set for LDAP providers.

- Step 8** Specify the password for the LDAP database account specified for Bind DN:

Firepower-chassis /security/ldap/server # **set password**

To set the password, press **Enter** after typing the **set password** command and enter the key value at the prompt.

You can enter any standard ASCII characters except for space, \$ (section sign), ? (question mark), or = (equal sign).

- Step 9** (Optional) Specify the order in which the FXOS uses this provider to authenticate users:

Firepower-chassis /security/ldap/server # **set order** *order-num*

- Step 10** (Optional) Specify the port used to communicate with the LDAP server. The standard port number is 389.

Firepower-chassis /security/ldap/server # **set port** *port-num*

- Step 11** Enable or disable the use of encryption when communicating with the LDAP server:

Firepower-chassis /security/ldap/server # **set ssl** {**yes** | **no**}

The options are as follows:

- **yes** —Encryption is required. If encryption cannot be negotiated, the connection fails.
- **no** —Encryption is disabled. Authentication information is sent as clear text.

LDAP uses STARTTLS. This allows encrypted communication using port 389.

- Step 12** Specify the length of time in seconds the system will spend trying to contact the LDAP database before it times out:

```
Firepower-chassis /security/ldap/server # set timeout timeout-num
```

Enter an integer from 1 to 60 seconds, or enter 0 (zero) to use the global timeout value specified for LDAP providers. The default is 30 seconds.

**Step 13** Specify the vendor that is providing the LDAP provider or server details:

```
Firepower-chassis /security/ldap/server # set vendor {ms-ad | openldap}
```

The options are as follows:

- **ms-ad**—LDAP provider is Microsoft Active Directory.
- **openldap**—LDAP provider is not Microsoft Active Directory.

**Step 14** (Optional) Enable the certification revocation list check:

```
Firepower-chassis /security/ldap/server # set revoke-policy {strict | relaxed}
```

#### Note

This configuration only takes effect if the SSL connection is enabled.

**Step 15** Commit the transaction to the system configuration:

```
Firepower-chassis /security/ldap/server # commit-buffer
```

### Example

The following example creates an LDAP server instance named 10.193.169.246, configures the binddn, password, order, port, SSL settings, vendor attribute, and commits the transaction:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope ldap
Firepower-chassis /security/ldap* # create server 10.193.169.246
Firepower-chassis /security/ldap/server* # set binddn
"cn=Administrator,cn=Users,DC=cisco-firepower-aaa3,DC=qalab,DC=com"
Firepower-chassis /security/ldap/server* # set password
Enter the password:
Confirm the password:
Firepower-chassis /security/ldap/server* # set order 2
Firepower-chassis /security/ldap/server* # set port 389
Firepower-chassis /security/ldap/server* # set ssl yes
Firepower-chassis /security/ldap/server* # set timeout 30
Firepower-chassis /security/ldap/server* # set vendor ms-ad
Firepower-chassis /security/ldap/server* # commit-buffer
Firepower-chassis /security/ldap/server #
```

The following example creates an LDAP server instance named 12:31:71:1231:45b1:0011:011:900, configures the binddn, password, order, port, SSL settings, vendor attribute, and commits the transaction:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope ldap
Firepower-chassis /security/ldap* # create server 12:31:71:1231:45b1:0011:011:900
Firepower-chassis /security/ldap/server* # set binddn
"cn=Administrator,cn=Users,DC=cisco-firepower-aaa3,DC=qalab,DC=com"
Firepower-chassis /security/ldap/server* # set password
Enter the password:
```

```

Confirm the password:
Firepower-chassis /security/ldap/server* # set order 1
Firepower-chassis /security/ldap/server* # set port 389
Firepower-chassis /security/ldap/server* # set ssl yes
Firepower-chassis /security/ldap/server* # set timeout 45
Firepower-chassis /security/ldap/server* # set vendor ms-ad
Firepower-chassis /security/ldap/server* # commit-buffer
Firepower-chassis /security/ldap/server #

```

## Deleting an LDAP Provider

### Procedure

- 
- |               |                                                                                                                |
|---------------|----------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Enter security mode:<br>Firepower-chassis# <b>scope security</b>                                               |
| <b>Step 2</b> | Enter security LDAP mode:<br>Firepower-chassis /security # <b>scope ldap</b>                                   |
| <b>Step 3</b> | Delete the specified server:<br>Firepower-chassis /security/ldap # <b>delete server</b> <i>serv-name</i>       |
| <b>Step 4</b> | Commit the transaction to the system configuration:<br>Firepower-chassis /security/ldap # <b>commit-buffer</b> |
- 

### Example

The following example deletes the LDAP server called ldap1 and commits the transaction:

```

Firepower-chassis# scope security
Firepower-chassis /security # scope ldap
Firepower-chassis /security/ldap # delete server ldap1
Firepower-chassis /security/ldap* # commit-buffer
Firepower-chassis /security/ldap #

```

## Configuring RADIUS Providers

### Configuring Properties for RADIUS Providers

The properties that you configure in this task are the default settings for all provider connections of this type. If an individual provider includes a setting for any of these properties, the FXOS uses that setting and ignores this default setting.

### Procedure

- 
- |               |                      |
|---------------|----------------------|
| <b>Step 1</b> | Enter security mode: |
|---------------|----------------------|

```
Firepower-chassis# scope security
```

**Step 2** Enter security RADIUS mode:

```
Firepower-chassis /security # scope radius
```

**Step 3** (Optional) Specify the number of times to retry contacting the RADIUS server before noting the server as down:

```
Firepower-chassis /security/radius # set retries retry-num
```

**Step 4** (Optional) Set the amount of time the system will wait for a response from the RADIUS server before noting the server as down:

```
Firepower-chassis /security/radius # set timeout seconds
```

**Step 5** Commit the transaction to the system configuration:

```
Firepower-chassis /security/radius # commit-buffer
```

### Example

The following example sets the RADIUS retries to 4, sets the timeout interval to 30 seconds, and commits the transaction:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope radius
Firepower-chassis /security/radius # set retries 4
Firepower-chassis /security/radius* # set timeout 30
Firepower-chassis /security/radius* # commit-buffer
Firepower-chassis /security/radius #
```

### What to do next

Create a RADIUS provider.

## Creating a RADIUS Provider

Follow these steps to define and configure a RADIUS provider—that is, a specific remote server providing RADIUS-based AAA services for this appliance.



**Note** The FXOS supports a maximum of 16 RADIUS providers.

### Procedure

**Step 1** Enter security mode:

```
Firepower-chassis# scope security
```

**Step 2** Enter security RADIUS mode:



Firepower-chassis /security # **scope radius**

- Step 3** Create a RADIUS server instance and enter security RADIUS server mode:

Firepower-chassis /security/radius # **create server** *server-name*

- Step 4** (Optional) Specify the port used to communicate with the RADIUS server.

Firepower-chassis /security/radius/server # **set authport** *authport-num*

- Step 5** Set the RADIUS server key:

Firepower-chassis /security/radius/server # **set key**

To set the key value, press **Enter** after typing the **set key** command and enter the key value at the prompt.

You can enter any standard ASCII characters except for space, \$ (section sign), ? (question mark), or = (equal sign).

- Step 6** (Optional) Specify when in the order this server will be tried:

Firepower-chassis /security/radius/server # **set order** *order-num*

- Step 7** (Optional) Set the number of times to retry communicating with the RADIUS server before noting the server as down:

Firepower-chassis /security/radius/server # **set retries** *retry-num*

- Step 8** Specify the length of time in seconds the system will wait for a response from the RADIUS server before noting the server as down:

Firepower-chassis /security/radius/server # **set timeout** *seconds*

#### Tip

It is recommended that you configure a higher **Timeout** value if you select two-factor authentication for RADIUS providers.

- Step 9** Commit the transaction to the system configuration:

Firepower-chassis /security/radius/server # **commit-buffer**

### Example

The following example creates a server instance named `radiusserv7`, sets the authentication port to 5858, sets the key to `radiuskey321`, sets the order to 2, sets the retries to 4, sets the timeout to 30, and commits the transaction:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope radius
Firepower-chassis /security/radius # create server radiusserv7
Firepower-chassis /security/radius/server* # set authport 5858
Firepower-chassis /security/radius/server* # set key
Enter the key: radiuskey321
Confirm the key: radiuskey321
Firepower-chassis /security/radius/server* # set order 2
Firepower-chassis /security/radius/server* # set retries 4
Firepower-chassis /security/radius/server* # set timeout 30
```

```
Firepower-chassis /security/radius/server* # commit-buffer
Firepower-chassis /security/radius/server #
```

## Deleting a RADIUS Provider

### Procedure

- 
- Step 1** Enter security mode:  
Firepower-chassis# **scope security**
- Step 2** Enter security RADIUS mode:  
Firepower-chassis /security # **scope RADIUS**
- Step 3** Delete the specified server:  
Firepower-chassis /security/radius # **delete server** *serv-name*
- Step 4** Commit the transaction to the system configuration:  
Firepower-chassis /security/radius # **commit-buffer**
- 

### Example

The following example deletes the RADIUS server called radius1 and commits the transaction:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope radius
Firepower-chassis /security/radius # delete server radius1
Firepower-chassis /security/radius* # commit-buffer
Firepower-chassis /security/radius #
```

## Configuring TACACS+ Providers

### Configuring Properties for TACACS+ Providers

The properties that you configure in this task are default settings for all provider connections of this type. If an individual provider configuration includes a setting for any of these properties, the FXOS uses that setting and ignores this default setting.




---

**Note** The FXOS chassis does not support command accounting for the Terminal Access Controller Access-Control System Plus (TACACS+) protocol.

---

### Procedure

- 
- Step 1** Enter security mode:

```
Firepower-chassis# scope security
```

**Step 2** Enter security TACACS+ mode:

```
Firepower-chassis /security # scope tacacs
```

**Step 3** (Optional) Set the amount of time the system will wait for a response from the TACACS+ server before noting the server as down:

```
Firepower-chassis /security/tacacs # set timeout seconds
```

Enter an integer from 1 to 60 seconds. The default value is 5 seconds.

**Step 4** Commit the transaction to the system configuration:

```
Firepower-chassis /security/tacacs # commit-buffer
```

### Example

The following example sets the TACACS+ timeout interval to 45 seconds and commits the transaction:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope tacacs
Firepower-chassis /security/tacacs # set timeout 45
Firepower-chassis /security/tacacs* # commit-buffer
Firepower-chassis /security/tacacs #
```

### What to do next

Create a TACACS+ provider.

## Creating a TACACS+ Provider

Follow these steps to define and configure a TACACS+ provider—that is, a specific remote server providing TACACS-based AAA services for this appliance.



**Note** The FXOS supports a maximum of 16 TACACS+ providers.

### Procedure

**Step 1** Enter security mode:

```
Firepower-chassis# scope security
```

**Step 2** Enter security TACACS+ mode:

```
Firepower-chassis /security # scope tacacs
```

**Step 3** Create a TACACS+ server instance and enter security TACACS+ server mode:

```
Firepower-chassis /security/tacacs # create server server-name
```

- Step 4** Specify the TACACS+ server key:
- Firepower-chassis /security/tacacs/server # **set key**
- To set the key value, press **Enter** after typing the **set key** command and enter the key value at the prompt. You can enter any standard ASCII characters except for space, § (section sign), ? (question mark), or = (equal sign).
- Step 5** (Optional) Specify when in the order this server will be tried:
- Firepower-chassis /security/tacacs/server # **set order** *order-num*
- Step 6** Specify the time interval that the system will wait for a response from the TACACS+ server before noting the server as down:
- Firepower-chassis /security/tacacs/server # **set timeout** *seconds*
- Tip**  
It is recommended that you configure a higher timeout value if you select two-factor authentication for TACACS+ providers.
- Step 7** (Optional) Specify the port used to communicate with the TACACS+ server:
- Firepower-chassis /security/tacacs/server # **set port** *port-num*
- Step 8** Commit the transaction to the system configuration:
- Firepower-chassis /security/tacacs/server # **commit-buffer**
- 

### Example

The following example creates a server instance named tacacsserv680, sets the key to tacacskey321, sets the order to 4, sets the authentication port to 5859, and commits the transaction:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope tacacs
Firepower-chassis /security/tacacs # create server tacacsserv680
Firepower-chassis /security/tacacs/server* # set key
Enter the key: tacacskey321
Confirm the key: tacacskey321
Firepower-chassis /security/tacacs/server* # set order 4
Firepower-chassis /security/tacacs/server* # set port 5859
Firepower-chassis /security/tacacs/server* # commit-buffer
Firepower-chassis /security/tacacs/server #
```

## Deleting a TACACS+ Provider

### Procedure

- 
- Step 1** Enter security mode:
- Firepower-chassis# **scope security**
- Step 2** Enter security TACACS+ mode:

```
Firepower-chassis /security # scope tacacs
```

**Step 3** Delete the specified server:

```
Firepower-chassis /security/tacacs # delete server serv-name
```

**Step 4** Commit the transaction to the system configuration:

```
Firepower-chassis /security/tacacs # commit-buffer
```

### Example

The following example deletes the TACACS+ server called tacacs1 and commits the transaction:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope tacacs
Firepower-chassis /security/tacacs # delete server tacacs1
Firepower-chassis /security/tacacs* # commit-buffer
Firepower-chassis /security/tacacs #
```

## Verifying Remote AAA Server Configurations

The following sections describe how to use the FXOS CLI to determine the current configuration for the various remote AAA servers.

### Determining Current FXOS Authentication Configuration

The following example shows you how to use the **show authentication** command to determine the current FXOS authentication settings. In this example, LDAP is the default mode of authentication.

```
firepower# scope security
firepower /security # show authentication
Console authentication: Local
Operational Console authentication: Local
Default authentication: Ldap
Operational Default authentication: Ldap
Role Policy For Remote Users: Assign Default Role
firepower /security #
```

### Determining Current LDAP Configuration

The following example shows you how to use the **show server detail** command in ldap mode to determine the current LDAP configuration settings.

```
firepower# scope security
firepower /security # scope ldap
firepower /security/ldap # show server detail

LDAP server:
 Hostname, FQDN or IP address: 10.48.53.132
 Descr:
 Order: 1
 DN to search and read: CN=cisco,CN=Users,DC=fxosldapuser,DC=lab
 Password:
```

```

Port: 389
SSL: No
Key:
Cipher Suite Mode: Medium Strength
Cipher Suite:
AL:DH:EP:AEZ56-BC3A:EDHSA-ES-BC3A:EDHDS-ES-BC3A:DES-BC3A:DH:DES:EXPORT40:EXPORT56:LOW:RC4:MD5:IDEA:HIGH:MEDIUM:EXP:NULL

CRL: Relaxed
Basedn: CN=Users,DC=fxosldapuser,DC=lab
User profile attribute: CiscoAVPair
Filter: cn=$userid
Timeout: 30
Ldap Vendor: MS AD
firepower /security/ldap #

```

### Determining Current RADIUS Configuration

The following example shows you how to use the **show server detail** command in radius mode to determine the current RADIUS configuration settings.

```

firepower# scope security
firepower /security # scope radius
firepower /security/radius # show server detail

RADIUS server:
 Hostname, FQDN or IP address: 10.48.17.199
 Descr:
 Order: 1
 Auth Port: 1812
 Key: ****
 Timeout: 5
 Retries: 1
firepower /security/radius #

```

### Determining Current TACACS+ Configuration

The following example shows you how to use the **show server detail** command in tacacs mode to determine the current TACACS+ configuration settings.

```

firepower# scope security
firepower /security # scope tacacs
firepower /security/tacacs # show server detail

TACACS+ server:
 Hostname, FQDN or IP address: 10.48.17.199
 Descr:
 Order: 1
 Port: 49
 Key: ****
 Timeout: 5
firepower /security/tacacs #

```

## Configuring Syslog

System logging is a method of collecting messages from devices to a server running a syslog daemon. Logging to a central syslog server helps in aggregation of logs and alerts. A syslog service accepts messages and stores

them in files, or prints them according to a simple configuration file. This form of logging provides protected long-term storage for logs. Logs are useful both in routine troubleshooting and in incident handling.

## Procedure

- 
- Step 1** Enter monitoring mode:  
Firepower-chassis# **scope monitoring**
- Step 2** Enable or disable the sending of syslogs to the console:  
Firepower-chassis /monitoring # {**enable** | **disable**} **syslog console**
- Step 3** (Optional) Select the lowest message level that you want displayed. If syslogs are enabled, the system displays that level and above on the console. The level options are listed in order of decreasing urgency. The default level is Critical.  
Firepower-chassis /monitoring # **set syslog console level** {**emergencies** | **alerts** | **critical**}
- Step 4** Enable or disable the monitoring of syslog information by the operating system:  
Firepower-chassis /monitoring # {**enable** | **disable**} **syslog monitor**
- Step 5** (Optional) Select the lowest message level that you want displayed. If the monitor state is enabled, the system displays that level and above. The level options are listed in order of decreasing urgency. The default level is Critical.  
Firepower-chassis /monitoring # **set syslog monitor level** {**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}
- Note**  
Messages at levels below Critical are displayed on the terminal monitor only if you have entered the **terminal monitor** command.
- Step 6** Enable or disable the writing of syslog information to a syslog file:  
Firepower-chassis /monitoring # {**enable** | **disable**} **syslog file**
- Step 7** Specify the name of the file in which the messages are logged. Up to 16 characters are allowed in the file name.  
Firepower-chassis /monitoring # **set syslog file name** *filename*
- Step 8** (Optional) Select the lowest message level that you want stored to a file. If the file state is enabled, the system stores that level and above in the syslog file. The level options are listed in order of decreasing urgency. The default level is Critical.  
Firepower-chassis /monitoring # **set syslog file level** {**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}
- Step 9** (Optional) Specify the maximum file size, in bytes, before the system begins to write over the oldest messages with the newest ones. The range is 4096 to 4194304 bytes.  
Firepower-chassis /monitoring # **set syslog file size** *filesize*
- Step 10** Configure sending of syslog messages to up to three external syslog servers:

- a) Enable or disable the sending of syslog messages to up to three external syslog servers:

```
Firepower-chassis /monitoring # {enable | disable} syslog remote-destination {server-1 | server-2 | server-3}
```

- b) (Optional) Select the lowest message level that you want stored to the external log. If the remote-destination is enabled, the system sends that level and above to the external server. The level options are listed in order of decreasing urgency. The default level is Critical.

```
Firepower-chassis /monitoring # set syslog remote-destination {server-1 | server-2 | server-3} level {emergencies | alerts | critical | errors | warnings | notifications | information | debugging}
```

- c) Specify the hostname or IP address of the specified remote syslog server. Up to 256 characters are allowed in the hostname.

```
Firepower-chassis /monitoring # set syslog remote-destination {server-1 | server-2 | server-3} hostname hostname
```

- d) (Optional) Specify the facility level contained in the syslog messages sent to the specified remote syslog server.

```
Firepower-chassis /monitoring # set syslog remote-destination {server-1 | server-2 | server-3} facility {local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7}
```

### Step 11

Configure the local sources. Enter the following command for each of the local sources you want to enable or disable:

```
Firepower-chassis /monitoring # {enable | disable} syslog source {audits | events | faults}
```

This can be one of the following:

- **audits**—Enables or disables the logging of all audit log events.
- **events**—Enables or disables the logging of all system events.
- **faults**—Enables or disables the logging of all system faults.

### Step 12

Commit the transaction:

```
Firepower-chassis /monitoring # commit-buffer
```

### Example

This example shows how to enable the storage of syslog messages in a local file and commits the transaction:

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # disable syslog console
Firepower-chassis /monitoring* # disable syslog monitor
Firepower-chassis /monitoring* # enable syslog file
Firepower-chassis /monitoring* # set syslog file name SysMsgsFirepower
Firepower-chassis /monitoring* # set syslog file level notifications
Firepower-chassis /monitoring* # set syslog file size 4194304
Firepower-chassis /monitoring* # disable syslog remote-destination server-1
Firepower-chassis /monitoring* # disable syslog remote-destination server-2
Firepower-chassis /monitoring* # disable syslog remote-destination server-3
```



```
Firepower-chassis /monitoring* # commit-buffer
Firepower-chassis /monitoring #
```

## Configuring DNS Servers

You need to specify a DNS server if the system requires resolution of host names to IP addresses. For example, you cannot use a name such as `www.cisco.com` when you are configuring a setting on the chassis if you do not configure a DNS server. You would need to use the IP address of the server, which can be either an IPv4 or an IPv6 address. You can configure up to four DNS servers.



**Note** When you configure multiple DNS servers, the system searches for the servers only in any random order. If a local management command requires DNS server lookup, it can only search for three DNS servers in random order.

### Procedure

- 
- Step 1** Enter system mode:
- ```
Firepower-chassis # scope system
```
- Step 2** Enter system services mode:
- ```
Firepower-chassis /system # scope services
```
- Step 3** To create or delete a DNS server, enter the appropriate command as follows:
- To configure the system to use a DNS server with the specified IPv4 or IPv6 address:  

```
Firepower-chassis /system/services # create dns {ip-addr | ip6-addr}
```
  - To delete a DNS server with the specified IPv4 or IPv6 address:  

```
Firepower-chassis /system/services # delete dns {ip-addr | ip6-addr}
```
- Step 4** Commit the transaction to the system configuration:
- ```
Firepower /system/services # commit-buffer
```
-

Example

The following example configures a DNS server with the IPv4 address 192.168.200.105 and commits the transaction:

```
Firepower-chassis# scope system  
Firepower-chassis /system # scope services  
Firepower-chassis /system/services # create dns 192.168.200.105  
Firepower-chassis /system/services* # commit-buffer  
Firepower-chassis /system/services #
```

The following example configures a DNS server with the IPv6 address 2001:db8::22:F376:FF3B:AB3F and commits the transaction:

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # create dns 2001:db8::22:F376:FF3B:AB3F
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

The following example deletes the DNS server with the IP address 192.168.200.105 and commits the transaction:

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # delete dns 192.168.200.105
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

Enable FIPS Mode

Perform these steps to enable FIPS mode on your Firepower 4100/9300 chassis.

Procedure

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

scope security

Step 2 Enable FIPS mode:

enable fips-mode

Step 3 Commit the configuration:

commit-buffer

Step 4 Reboot the system:

connect local-mgmt

reboot

When the FIPS Mode is enabled, it limits the key sizes and the algorithms allowed. The MIO uses CiscoSSL and the FIPS Object Module (FOM) for its cryptographic needs. It makes FIPS validation easier compared to ASA's proprietary cryptographic library implementation and HW acceleration.

What to do next

Prior to FXOS release 2.0.1, the existing SSH host key created during first-time setup of a device was hard coded to 1024 bits. To comply with FIPS and Common Criteria certification requirements, you must destroy this old host key and generate a new one using the procedure detailed in [Generate the SSH Host Key](#). If you do not perform these additional steps, you will not be able to connect to the Supervisor using SSH after the device has rebooted with FIPS mode enabled. If you performed initial setup using FXOS 2.0.1 or later, you do not have to generate a new host key.

Enable Common Criteria Mode

Perform these steps to enable Common Criteria mode on your Firepower 4100/9300 chassis.

Procedure

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

scope security

Step 2 Enable Common Criteria mode:

enable cc-mode

Step 3 Commit the configuration:

commit-buffer

Step 4 Reboot the system:

connect local-mgmt

reboot

Common Criteria is an international standard for computer security. CC focuses on certificates, auditing, logging, passwords, TLS, SSH, etc. It essentially assumes FIPS compliance. Similar to FIPS, Cisco contracts with NIST accredited lab vendors to perform testing and submission to NIAP.

When the CC Mode is enabled, it limits the list of algorithms, cipher suites, and features that are needed to be supported. The MIO is evaluated against the Network Device Collaborative Protection Profile (NDcPP). CiscoSSL can only enforce part of the requirements most of which are covered in the [CC compliance guide](#).

What to do next

Prior to FXOS release 2.0.1, the existing SSH host key created during first-time setup of a device was hard coded to 1024 bits. To comply with FIPS and Common Criteria certification requirements, you must destroy this old host key and generate a new one using the procedure detailed in [Generate the SSH Host Key](#). If you do not perform these additional steps, you will not be able to connect to the Supervisor using SSH after the device has rebooted with Common Criteria mode enabled. If you performed initial setup using FXOS 2.0.1 or later, you do not have to generate a new host key.

Configure the IP Access List

By default, the Firepower 4100/9300 chassis denies all access to the local web server. You must configure your IP Access List with a list of allowed services for each of your IP blocks.

The IP Access List supports the following protocols:

- HTTPS
- SNMP
- SSH

For each block of IP addresses (v4 or v6), up to 100 different subnets can be configured for each service. A subnet of 0 and a prefix of 0 allows unrestricted access to a service.

Procedure

Step 1 From the FXOS CLI, enter the services mode:

```
scope system
```

```
scope services
```

Step 2 Create an IP block for the services you want to enable access for:

For IPv4:

```
create ip-block ip prefix [0-32] [http | snmp | ssh]
```

For IPv6:

```
create ipv6-block ip prefix [0-128] [http | snmp | ssh]
```

Example

The following example shows how to create, enter, and verify an IPv4 address block to provide SSH access:

```
firepower # scope system
firepower /system # scope services
firepower /system/services # enter ip-block 192.168.200.101 32 ssh
firepower /system/services/ip-block* # commit-buffer
firepower /system/services/ip-block # up
firepower /system/services # show ip-block
```

Permitted IP Block:

IP Address	Prefix Length	Protocol
0.0.0.0	0	https
0.0.0.0	0	snmp
0.0.0.0	0	ssh
192.168.200.101	32	ssh

```
firepower /system/services #
```

The following example shows how to create, enter and verify an IPv6 address block to provide SSH access::

```
firepower # scope system
firepower /system # scope services
firepower /system/services # create ipv6-block 2001:DB8:1::1 64 ssh
firepower /system/services/ipv6-block* # commit-buffer
firepower /system/services/ipv6-block # up
firepower /system/services # show ipv6-block
```

```
Permitted IPv6 Block:
  IPv6 Address Prefix Length Protocol
  -----
  ::                      0 https
  ::                      0 snmp
  ::                      0 ssh
  2001:DB8:1::1          64 ssh
firepower /system/services #
```

Add a MAC Pool Prefix and View MAC Addresses for Container Instance Interfaces

The FXOS chassis automatically generates MAC addresses for container instance interfaces, and guarantees that a shared interface in each instance uses a unique MAC address. The FXOS chassis generates the MAC address using the following format:

A2xx.yyzz.zzzz

Where xx.yy is a user-defined prefix or a system-defined prefix, and zz.zzzz is an internal counter generated by the chassis. The system-defined prefix matches the lower 2 bytes of the first MAC address in the burned-in MAC address pool that is programmed into the IDPROM. Use **connect fxos**, then **show module** to view the MAC address pool. For example, if the range of MAC addresses shown for module 1 is b0aa.772f.f0b0 to b0aa.772f.f0bf, then the system prefix will be f0b0.

See [Automatic MAC Addresses for Container Instance Interfaces, on page 222](#) for more information.

This procedure describes how to view the MAC addresses and how to optionally define the prefix used in generation.



Note If you change the MAC address prefix after you deploy logical devices, you may experience traffic interruption.

Procedure

Step 1 Enter Security Services mode, and then Auto MAC pool mode.

```
scope ssa
```

```
scope auto-macpool
```

Example:

```
Firepower# scope ssa
Firepower /ssa # scope auto-macpool
Firepower /ssa/auto-macpool #
```

Step 2 Set the MAC address prefix used in generating the MAC addresses.

set prefix prefix

- *prefix*—Enter a decimal value between 1 and 65535. This prefix is converted to a four-digit hexadecimal number, and used as part of the MAC address.

For an example of how the prefix is used, if you set a prefix of 77, then the chassis converts 77 into the hexadecimal value 004D (yyxx). When used in the MAC address, the prefix is reversed (xxyy) to match the chassis native form:

A24D.00zz.zzzz

For a prefix of 1009 (03F1), the MAC address is:

A2F1.03zz.zzzz

Example:

```
Firepower /ssa/auto-macpool # set prefix 65
Firepower /ssa/auto-macpool* #
```

Step 3 Save the configuration.

commit-buffer

Example:

```
Firepower /ssa/auto-macpool* # commit-buffer
Firepower /ssa/auto-macpool #
```

Step 4 View MAC address assignments.

show mac-address

Example:

```
Firepower /ssa/auto-macpool # show mac-address
Mac Address Item:
  Mac Address      Owner Profile      Owner Name
  -----
  A2:46:C4:00:00:1E ftd13              Port-channel14
  A2:46:C4:00:00:20 ftd14              Port-channel15
  A2:46:C4:00:01:7B ftd1               Ethernet1/3
  A2:46:C4:00:01:7C ftd12              Port-channel11
  A2:46:C4:00:01:7D ftd13              Port-channel14
  A2:46:C4:00:01:7E ftd14              Port-channel15
  A2:46:C4:00:01:7F ftd1               Ethernet1/2
  A2:46:C4:00:01:80 ftd12              Ethernet1/2
  A2:46:C4:00:01:81 ftd13              Ethernet1/2
  A2:46:C4:00:01:82 ftd14              Ethernet1/2
  A2:46:C4:00:01:83 ftd2               Ethernet3/1/4
  A2:46:C4:00:01:84 ftd2               Ethernet3/1/1
  A2:46:C4:00:01:85 ftd2               Ethernet3/1/3
  A2:46:C4:00:01:86 ftd2               Ethernet3/1/2
```

A2:46:C4:00:01:87	ftd2	Ethernet1/2
A2:46:C4:00:01:88	ftd1	Port-channel21
A2:46:C4:00:01:89	ftd1	Ethernet1/8

Example

The following example sets the MAC prefix to 33.

```
Firepower# scope ssa
Firepower /ssa # scope auto-macpool
Firepower /ssa/auto-macpool # set prefix 33
Firepower /ssa/auto-macpool* # commit-buffer
Firepower /ssa/auto-macpool #
```

Add a Resource Profile for Container Instances

To specify resource usage per container instance, create one or more resource profiles. When you deploy the logical device/application instance, you specify the resource profile that you want to use. The resource profile sets the number of CPU cores; RAM is dynamically allocated according to the number of cores, and disk space is set to 40 GB per instance.

- The minimum number of cores is 6.



Note Instances with a smaller number of cores might experience relatively higher CPU utilization than those with larger numbers of cores. Instances with a smaller number of cores are more sensitive to traffic load changes. If you experience traffic drops, try assigning more cores.

- You can assign cores as an even number (6, 8, 10, 12, 14 etc.) up to the maximum. Note that we do not recommend using 8 cores; performance for 8 cores is only slightly better than for 6 cores.
- The maximum number of cores available depends on the security module/chassis model; see [Requirements and Prerequisites for Container Instances](#), on page 227.

The chassis includes a default resource profile called "Default-Small," which includes the minimum number of cores. You can change the definition of this profile, and even delete it if it is not in use. Note that this profile is created when the chassis reloads and no other profile exists on the system.

Changing the resource profile after you assign it is disruptive. See the following guidelines:

- You cannot change the resource profile settings if it is currently in use. You must disable any instances that use it, then change the resource profile, and finally reenable the instance.
- If you change the resource profile settings after you add the Firepower Threat Defense instance to the FMC, then update the inventory for each unit on the FMC. Choose **Devices > Device Management**, click **Edit** (✎) for the instance, then click **Refresh** (🔄) on the **Device > Inventory Details** area.

- If you assign a different profile to an instance, it reboots.
- If you assign a different profile to instances in an established high-availability pair, which requires the profile to be the same on both units, you must:
 1. Break high availability.
 2. Assign the new profile to both units.
 3. Re-establish high availability.

Procedure

Step 1 Enter Security Services mode.

scope ssa

Example:

```
Firepower# scope ssa
Firepower /ssa #
```

Step 2 Create the resource profile.

enter resource-profile name

- *name*—Sets the name of the profile between 1 and 64 characters. Note that you cannot change the name of this profile after you add it.

Example:

```
Firepower /ssa # enter resource-profile gold
Firepower /ssa/resource-profile* #
```

Step 3 Enter a description.

set description description

- *description*—Sets the description of the profile up to 510 characters. Use quotes (") around phrases with spaces.

Example:

```
Firepower /ssa/resource-profile* # set description "highest level"
```

Step 4 Set the number of CPU cores.

set cpu-core-count cores

- *cores*—Sets the number of cores for the profile, between 6 and the maximum, depending on your chassis, as an even number.

Example:


```
Firepower /ssa/resource-profile* # set cpu-core-count 14
```

Step 5 Save the configuration.

commit-buffer

Example:

```
Firepower /ssa/resource-profile* # commit-buffer
Firepower /ssa/resource-profile #
```

Step 6 View resource profile assignments from security services mode.

show resource-profile user-defined

Example:

```
Firepower /ssa # show resource-profile user-defined
Profile Name      Is In Use  CPU Logical Core Count  Description
-----
bronze            No         6                        low end device
gold              No         14                       highest
silver            No         10                       mid-level
```

Step 7 View resource usage for the security module/engine slot.

show monitor detail

Example:

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # show monitor detail
Monitor:
  OS Version:
  CPU Total Load 1 min Avg: 18.959999
  CPU Total Load 5 min Avg: 19.080000
  CPU Total Load 15 min Avg: 19.059999
  Memory Total (MB): 252835
  Memory Free (MB): 200098
  Memory Used (MB): 52738
  CPU Cores Total: 72
  CPU Cores Available: 30
  Memory App Total (MB): 226897
  Memory App Available (MB): 97245
  Data Disk Total (MB): 1587858
  Data Disk Available (MB): 1391250
  Secondary Disk Total (MB): 0
  Secondary Disk Available (MB): 0
  Disk File System Count: 7
  Blade Uptime:
  Last Updated Timestamp: 2018-05-23T14:26:06.132
```

Step 8 View resource allocation for the application instance.

show resource detail

Example:

```

Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd ftd1
Firepower /ssa/slot/app-instance # show resource detail
Resource:
    Allocated Core NR: 10
    Allocated RAM (MB): 32413
    Allocated Data Disk (MB): 49152
    Allocated Binary Disk (MB): 3907
    Allocated Secondary Disk (MB): 0

```

Example

The following example adds three resource profiles.

```

Firepower# scope ssa
Firepower /ssa # enter resource-profile basic
Firepower /ssa/resource-profile* # set description "lowest level"
Firepower /ssa/resource-profile* # set cpu-core-count 6
Firepower /ssa/resource-profile* # exit
Firepower /ssa # enter resource-profile standard
Firepower /ssa/resource-profile* # set description "middle level"
Firepower /ssa/resource-profile* # set cpu-core-count 10
Firepower /ssa/resource-profile* # exit
Firepower /ssa # enter resource-profile advanced
Firepower /ssa/resource-profile* # set description "highest level"
Firepower /ssa/resource-profile* # set cpu-core-count 12
Firepower /ssa/resource-profile* # commit-buffer
Firepower /ssa/resource-profile #

```

Configure a Network Control Policy

To permit the discovery of non-Cisco devices, FXOS supports the *Link Layer Discovery Protocol (LLDP)*, a vendor-neutral device discovery protocol that is defined in the IEEE 802.1ab standard. LLDP allows network devices to advertise information about themselves to other devices on the network. This protocol runs over the data-link layer, which allows two systems running different network layer protocols to learn about each other.

LLDP is a one-way protocol that transmits information about the capabilities and current status of a device and its interfaces. LLDP devices use the protocol to solicit information only from other LLDP devices.

To enable this functionality on your FXOS chassis, you can configure a network control policy, which specifies LLDP transmission and receiving behavior. Once a network control policy is created, it needs to be assigned to an interface. You can enable LLDP on any front interface, including fixed ports, EPM ports, port channels, and break out ports.

**Note**

- LLDP is not configurable on dedicated management ports.
- Internal backplane ports that connect to the blade have LLDP enabled by default, with no option to disable. All other ports have LLDP disabled by default.

Procedure

Step 1 Enter the organization scope.

scope org

Example:

```
Firepower # scope org
```

Step 2 Create and enable the network control policy.

create nw-ctrl-policy *nw-policy*

Example:

```
Firepower /org # create nw-ctrl-policy nw-policy
```

Step 3 Enable LLDP.

enable lldp {*receive* | *transmit*}

Example:

```
Firepower /org/nw-ctrl-policy* # enable lldp receive
Firepower /org/nw-ctrl-policy* # disable lldp transmit
```

Step 4 Commit the configuration:

commit-buffer

Example:

```
Firepower /eth-uplink/fabric/interface* # commit-buffer
Firepower /eth-uplink/fabric/interface #
```

Step 5 Specify whether to enable or disable LLDP for receiving/transmitting.

enable lldp *receive/transmit*

commit-buffer

Example:

```
Firepower /org/nw-ctrl-policy* # enable lldp receive
Firepower /org/nw-ctrl-policy* # disable lldp transmit
Firepower /org/nw-ctrl-policy* # commit-buffer
```

```
Firepower /org/nw-ctrl-policy* # enable lldp receive
Firepower /org/nw-ctrl-policy* # disable lldp transmit
Firepower /org/nw-ctrl-policy* # commit-buffer
```

Step 6 Use the following commands to apply the network control policy to an interface.

a) Enter the interface:

scope eth-uplink

scope fabric a

scope interface *interface_id*

```
Firepower # scope eth-uplink
Firepower /eth-uplink # scope fabric a
Firepower /eth-uplink/fabric # enter interface Ethernet3/1
```

b) Set the network control policy:

set nw-ctrl-policy *nw-policy*

commit-buffer

```
Firepower /eth-uplink/fabric/interface # set nw-ctrl-policy nw-policy
Firepower /eth-uplink/fabric/interface* # commit-buffer
MIO-5 /eth-uplink/fabric/interface # show detail
```

c) View the change:

show detail

```
Firepower /eth-uplink/fabric/interface # show detail
Interface:
  Port Name: Ethernet3/1
  User Label:
  Port Type: Data
  Admin State: Enabled
  Oper State: Sfp Not Present
  State Reason: Unknown
  flow control policy: default
  Auto negotiation: No
  Admin Speed: 100 Gbps
  Oper Speed: 100 Gbps
  Admin Duplex: Full Duplex
  Oper Duplex: Full Duplex
  Ethernet Link Profile name: default
  Oper Ethernet Link Profile name: fabric/lan/eth-link-prof-default
  Uddl Oper State: Admin Disabled
  Inline Pair Admin State: Enabled
  Inline Pair Peer Port Name:
  Allowed Vlan: All
  Network Control Policy: nw-policy
  Current Task:
```

d) Commit the configuration:

commit-buffer

Example:

```
Firepower /eth-uplink/fabric/interface* # commit-buffer
Firepower /eth-uplink/fabric/interface #
```

Configure the Chassis URL

You can specify a management URL so that you can easily open Firepower Chassis Manager for an Firepower Threat Defense instance directly from FMC. If you do not specify a chassis management URL, the chassis name is used instead.

If you change the chassis URL settings after you add the Firepower Threat Defense instance to the FMC, then update the inventory for each unit on the **Devices > Device Management > Device > System > Inventory** dialog box.

Procedure

Step 1 Enter the system mode:

scope system

Example:

```
Firepower# scope system
Firepower /system #
```

Step 2 To configure a new chassis name:

set name *chassis_name*

- *chassis_name*—Sets the name of the chassis between 1 and 60 characters.

Example:

```
Firepower /system # set name Firepower_chassis
```

Step 3 To configure the management URL:

set mgmt-url *management_url*

- *management_url*—Sets the URL that FMC should use to connect to an Firepower Threat Defense instance within Firepower Chassis Manager. The URL must start with https://. If you do not specify a chassis management URL, the chassis name is used instead.

Example:

```
Firepower /system # set mgmt-url https://192.168.1.55
```

Step 4 Save the configuration.

commit-buffer**Example:**

```
Firepower /system* # commit-buffer
Firepower /system #
```

Step 5 View configuration settings.

show detail**Example:**

```
Firepower_chassis /system # show detail

Systems:
  Name: Firepower_chassis
  Mode: Stand Alone
  System IP Address: 192.168.1.10
  System IPv6 Address: ::
  System Owner:
  System Site:
  Description for System:
  Chassis Mgmt URL: https://192.168.1.55
```

Modifying Weak Key Exchange Algorithms

You can mitigate the weak key exchange algorithms used on the equipment by:

- [Setting FIPS mode](#)
- [Setting cipher suite mode](#)

Setting FIPS/CC Mode

Procedure

-
- Step 1** From the FXOS CLI, enter the security mode:
scope security
- Step 2** Enable FIPS mode:
enable fips-mode
- Step 3** Commit the configuration:
commit-buffer
-

Setting Cipher Suite

Procedure

- Step 1** Enter system mode:
Firepower-chassis# **scope system**
- Step 2** Enter system services mode:
Firepower-chassis /system # **scope services**
- Step 3** View the HTTPS service:
Firepower-chassis /system/services # **show https**
- Step 4** Set the Cipher Suite mode:
Firepower-chassis /system/services # **set https cipher-suite-mode custom**
- Step 5** Set the Cipher Suite string
Firepower-chassis /system/services # **set https cipher-suite *******
- Step 6** Commit the settings to the system configuration:
Firepower-chassis /system/services # **commit-buffer**
-



CHAPTER 10

Interface Management

- [About Interfaces, on page 177](#)
- [Guidelines and Limitations for Interfaces, on page 192](#)
- [Configure Interfaces, on page 195](#)
- [Monitoring Interfaces, on page 205](#)
- [Troubleshooting Interfaces, on page 207](#)
- [History for Interfaces, on page 213](#)

About Interfaces

The Firepower 4100/9300 chassis supports physical interfaces, VLAN subinterfaces for container instances, and EtherChannel (port-channel) interfaces. EtherChannel interfaces can include up to 16 member interfaces of the same type.

Chassis Management Interface

The chassis management interface is used for management of the FXOS Chassis by SSH or Firepower Chassis Manager. This interface is separate from the mgmt-type interface that you assign to the logical devices for application management.

To configure parameters for this interface, you must configure them from the CLI. See also [Changing the Management IP Address, on page 87](#). To view information about this interface in the FXOS CLI, connect to local management and show the management port:

```
Firepower # connect local-mgmt
```

```
Firepower(local-mgmt) # show mgmt-port
```

Note that the chassis management interface remains up even if the physical cable or SFP module are unplugged, or if the **mgmt-port shut** command is performed, or if the logical device is offline.



Note The chassis management interface does not support jumbo frames.

Interface Types

Physical interfaces, VLAN subinterfaces for container instances, and EtherChannel (port-channel) interfaces can be one of the following types:

- **Data**—Use for regular data. Data interfaces cannot be shared between logical devices, and logical devices cannot communicate over the backplane to other logical devices. For traffic on Data interfaces, all traffic must exit the chassis on one interface and return on another interface to reach another logical device.
- **Data-sharing**—Use for regular data. Only supported with container instances, these data interfaces can be shared by one or more logical devices/container instances (Firepower Threat Defense only). Each container instance can communicate over the backplane with all other instances that share this interface. Shared interfaces can affect the number of container instances you can deploy. Shared interfaces are not supported for bridge group member interfaces (in transparent mode or routed mode), inline sets, passive interfaces, or failover links.
- **Mgmt**—Use to manage application instances. These interfaces can be shared by one or more logical devices to access external hosts; logical devices cannot communicate over this interface with other logical devices that share the interface. You can only assign one management interface per logical device. Depending on your application and manager, you can later enable management from a data interface; but you must assign a Management interface to the logical device even if you don't intend to use it after you enable data management.



Note Mgmt interface change will cause reboot of the logical device, for example one change mgmt from e1/1 to e1/2 will cause the logical device to reboot to apply the new management.

- **Eventing**—Use as a secondary management interface for Firepower Threat Defense devices. To use this interface, you must configure its IP address and other parameters at the Firepower Threat Defense CLI. For example, you can separate management traffic from events (such as web events). See the [management center configuration guide](#) for more information. Eventing interfaces can be shared by one or more logical devices to access external hosts; logical devices cannot communicate over this interface with other logical devices that share the interface.



Note A virtual Ethernet interface is allocated when each application instance is installed. If the application does not use an eventing interface, then the virtual interface will be in an admin down state.

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- **Cluster**—Use as the cluster control link for a clustered logical device. By default, the cluster control link is automatically created on Port-channel 48. The Cluster type is only supported on EtherChannel interfaces.



Note This chapter discusses *FXOS* VLAN subinterfaces only. You can separately create subinterfaces within the FTD application. See [FXOS Interfaces vs. Application Interfaces](#), on page 179 for more information.

FXOS Interfaces vs. Application Interfaces

The Firepower 4100/9300 manages the basic Ethernet settings of physical interfaces, VLAN subinterfaces for container instances, and EtherChannel (port-channel) interfaces. Within the application, you configure higher level settings. For example, you can only create EtherChannels in FXOS; but you can assign an IP address to the EtherChannel within the application.

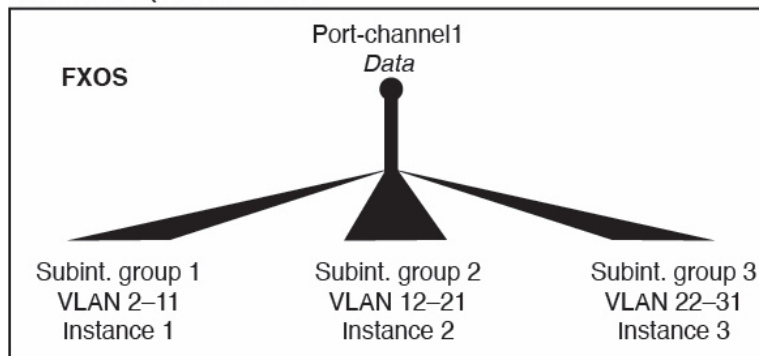
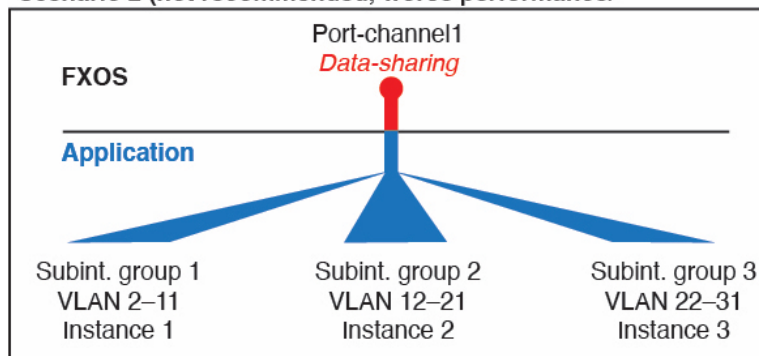
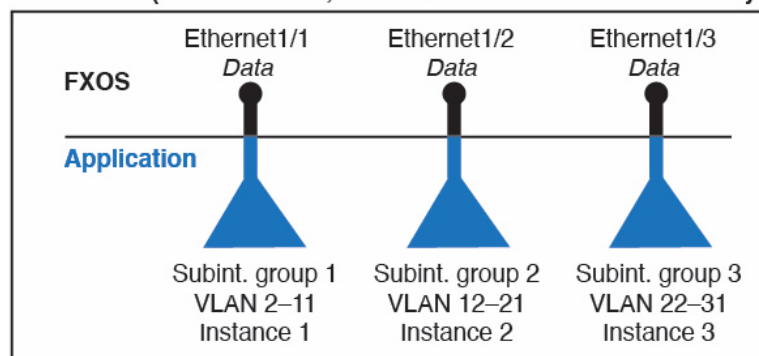
The following sections describe the interaction between FXOS and the application for interfaces.

VLAN Subinterfaces

For all logical devices, you can create VLAN subinterfaces within the application.

For container instances only, you can *also* create VLAN subinterfaces in FXOS. Application-defined subinterfaces are not subject to the FXOS limit. Choosing in which operating system to create subinterfaces depends on your network deployment and personal preference. For example, to share a subinterface, you must create the subinterface in FXOS. Another scenario that favors FXOS subinterfaces comprises allocating separate subinterface groups on a single interface to multiple instances. For example, you want to use Port-channel1 with VLAN 2–11 on instance A, VLAN 12–21 on instance B, and VLAN 22–31 on instance C. If you create these subinterfaces within the application, then you would have to share the parent interface in FXOS, which may not be desirable. See the following illustration that shows the three ways you can accomplish this scenario:

Figure 2: VLANs in FXOS vs. the Application for Container Instances

Scenario 1 (recommended)**Scenario 2 (not recommended, worse performance)****Scenario 3 (recommended, but lacks EtherChannel redundancy)****Independent Interface States in the Chassis and in the Application**

You can administratively enable and disable interfaces in both the chassis and in the application. For an interface to be operational, the interface must be enabled in both operating systems. Because the interface state is controlled independently, you may have a mismatch between the chassis and application.

The default state of an interface within the application depends on the type of interface. For example, the physical interface or EtherChannel is disabled by default within the application, but a subinterface is enabled by default.

Hardware Bypass Pairs

For the Firepower Threat Defense, certain interface modules on the Firepower 9300 and 4100 series let you use the Hardware Bypass feature for Firepower Threat Defense inline set interfaces. Hardware Bypass ensures that traffic continues to flow between an inline interface pair during a power outage. This feature can be used to maintain network connectivity in the case of software or hardware failures. The Hardware Bypass feature is configured within the Firepower Threat Defense application; no configuration is available in FXOS.

You do not need to use these interfaces as Hardware Bypass pairs; they can be used as regular interfaces for both the ASA and the Firepower Threat Defense applications. Note that Hardware Bypass-capable interfaces cannot be configured for breakout ports. If you want to use the Hardware Bypass feature, do not configure the ports as EtherChannels; otherwise, you can include these interfaces as EtherChannel members in regular interface mode.

When Hardware Bypass is enabled on an inline pair, switch bypass is attempted first. If the bypass configuration fails due a switch error, physical bypass is enabled.



Note Hardware Bypass (FTW) is not supported on the Firepower Threat Defense installed in service-chaining with third-party applications, such as VDP/Radware.



Note Do not enable Hardware Bypass and link state propagation for the same inline set.

The Firepower Threat Defense supports Hardware Bypass for interface pairs on specific network modules on the following models:

- Firepower 9300
- Firepower 4100 series

The supported Hardware Bypass network modules for these models include:

- Firepower 6-port 1G SX FTW Network Module single-wide (FPR-NM-6X1SX-F)
- Firepower 6-port 10G SR FTW Network Module single-wide (FPR-NM-6X10SR-F)
- Firepower 6-port 10G LR FTW Network Module single-wide (FPR-NM-6X10LR-F)
- Firepower 2-port 40G SR FTW Network Module single-wide (FPR-NM-2X40G-F)
- Firepower 8-port 1G Copper FTW Network Module single-wide (FPR-NM-8X1G-F)

Hardware Bypass can only use the following port pairs:

- 1 & 2
- 3 & 4
- 5 & 6
- 7 & 8

Jumbo Frame Support

The Firepower 4100/9300 chassis has support for jumbo frames enabled by default. To enable jumbo frame support on a specific logical device installed on the Firepower 4100/9300 chassis, you will need to configure the appropriate MTU settings for the interfaces on the logical device.

The maximum MTU that is supported for the application on the Firepower 4100/9300 chassis is 9184.



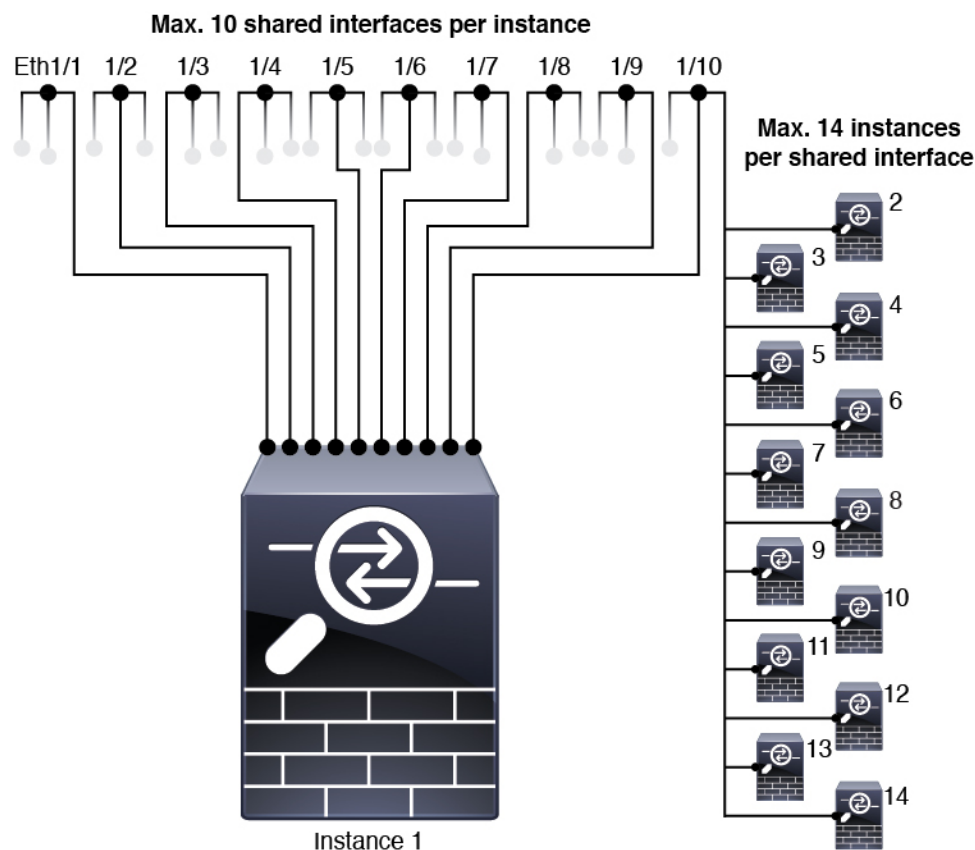
Note The chassis management interface does not support jumbo frames.

Shared Interface Scalability

Instances can share data-sharing type interfaces. This capability lets you conserve physical interface usage as well as support flexible networking deployments. When you share an interface, the chassis uses unique MAC addresses to forward traffic to the correct instance. However, shared interfaces can cause the forwarding table to grow large due to the need for a full mesh topology within the chassis (every instance must be able to communicate with every other instance that is sharing the same interface). Therefore, there are limits to how many interfaces you can share.

In addition to the forwarding table, the chassis maintains a VLAN group table for VLAN subinterface forwarding. Depending on the number of parent interfaces and other deployment decisions, you can create up to 500 VLAN subinterfaces.

See the following limits for shared interface allocation:



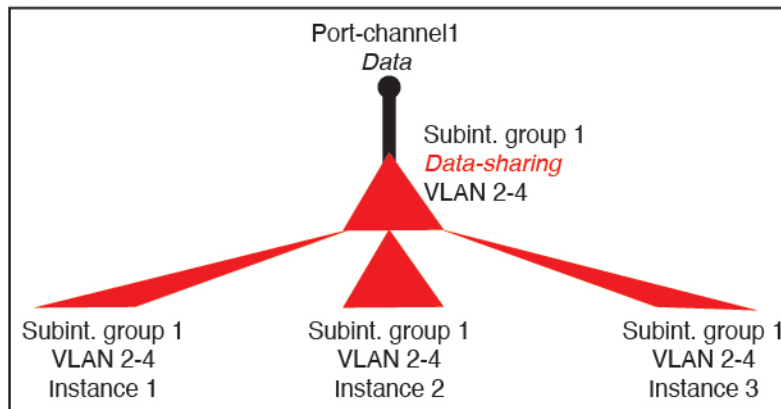
Shared Interface Best Practices

For optimal scalability of the forwarding table, share as few interfaces as possible. Instead, you can create up to 500 VLAN subinterfaces on one or more physical interfaces and then divide the VLANs among the container instances.

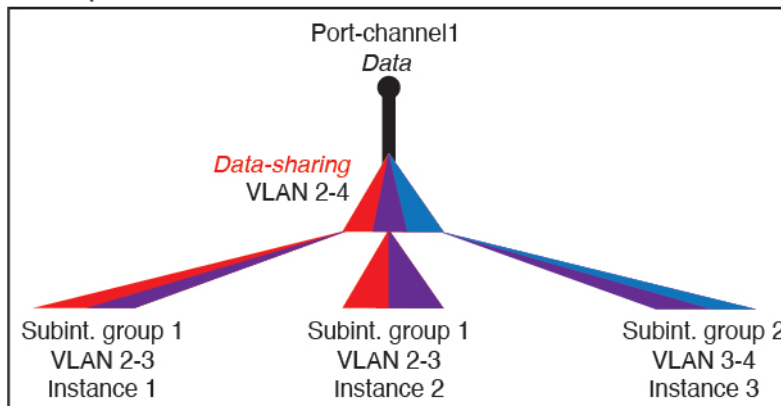
When sharing interfaces, follow these practices in the order of most scalable to least scalable:

1. Best—Share subinterfaces under a single parent, and use the same set of subinterfaces with the same group of instances.

For example, create a large EtherChannel to bundle all of your like-kind interfaces together, and then share subinterfaces of that EtherChannel: Port-Channel1.2, 3, and 4 instead of Port-Channel2, Port-Channel3, and Port-Channel4. When you share subinterfaces from a single parent, the VLAN group table provides better scaling of the forwarding table than when sharing physical/EtherChannel interfaces or subinterfaces across parents.

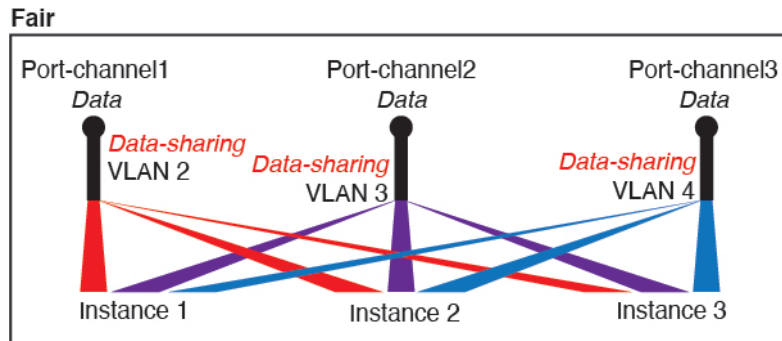
Figure 3: Best: Shared Subinterface Group on One Parent**Best**

If you do not share the same set of subinterfaces with a group of instances, your configuration can cause more resource usage (more VLAN groups). For example, share Port-Channel1.2, 3, and 4 with instances 1, 2, and 3 (one VLAN group) instead of sharing Port-Channel1.2 and 3 with instances 1 and 2, while sharing Port-Channel1.3 and 4 with instance 3 (two VLAN groups).

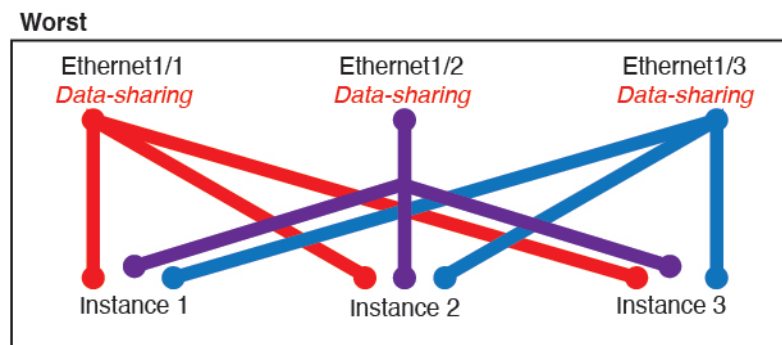
Figure 4: Good: Sharing Multiple Subinterface Groups on One Parent**Good (uses more resources)**

2. Fair—Share subinterfaces across parents.

For example, share Port-Channel1.2, Port-Channel2.3, and Port-Channel3.4 instead of Port-Channel2, Port-Channel4, and Port-Channel4. Although this usage is not as efficient as only sharing subinterfaces on the same parent, it still takes advantage of VLAN groups.

Figure 5: Fair: Shared Subinterfaces on Separate Parents

3. Worst—Share individual parent interfaces (physical or EtherChannel).
This method uses the most forwarding table entries.

Figure 6: Worst: Shared Parent Interfaces

Shared Interface Usage Examples

See the following tables for examples of interface sharing and scalability. The below scenarios assume use of one physical/EtherChannel interface for management shared across all instances, and another physical or EtherChannel interface with dedicated subinterfaces for use with High Availability.

- [Table 9: Physical/EtherChannel Interfaces and Instances on a Firepower 9300 with Three SM-44s, on page 186](#)
- [Table 10: Subinterfaces on One Parent and Instances on a Firepower 9300 with Three SM-44s, on page 187](#)
- [Table 11: Physical/EtherChannel Interfaces and Instances on a Firepower 9300 with One SM-44, on page 189](#)
- [Table 12: Subinterfaces on One Parent and Instances on a Firepower 9300 with One SM-44, on page 190](#)

Firepower 9300 with Three SM-44s

The following table applies to three SM-44 security modules on a 9300 using only physical interfaces or EtherChannels. Without subinterfaces, the maximum number of interfaces are limited. Moreover, sharing multiple physical interfaces uses more forwarding table resources than sharing multiple subinterfaces.

Each SM-44 module can support up to 14 instances. Instances are split between modules as necessary to stay within limits.

Table 9: Physical/EtherChannel Interfaces and Instances on a Firepower 9300 with Three SM-44s

Dedicated Interfaces	Shared Interfaces	Number of Instances	% Forwarding Table Used
32: <ul style="list-style-type: none"> • 8 • 8 • 8 • 8 	0	4: <ul style="list-style-type: none"> • Instance 1 • Instance 2 • Instance 3 • Instance 4 	16%
30: <ul style="list-style-type: none"> • 15 • 15 	0	2: <ul style="list-style-type: none"> • Instance 1 • Instance 2 	14%
14: <ul style="list-style-type: none"> • 14 (1 ea.) 	1	14: <ul style="list-style-type: none"> • Instance 1-Instance 14 	46%
33: <ul style="list-style-type: none"> • 11 (1 ea.) • 11 (1 ea.) • 11 (1 ea.) 	3: <ul style="list-style-type: none"> • 1 • 1 • 1 	33: <ul style="list-style-type: none"> • Instance 1-Instance 11 • Instance 12-Instance 22 • Instance 23-Instance 33 	98%
33: <ul style="list-style-type: none"> • 11 (1 ea.) • 11 (1 ea.) • 12 (1 ea.) 	3: <ul style="list-style-type: none"> • 1 • 1 • 1 	34: <ul style="list-style-type: none"> • Instance 1-Instance 11 • Instance 12-Instance 22 • Instance 23-Instance 34 	102% DISALLOWED
30: <ul style="list-style-type: none"> • 30 (1 ea.) 	1	6: <ul style="list-style-type: none"> • Instance 1-Instance 6 	25%
30: <ul style="list-style-type: none"> • 10 (5 ea.) • 10 (5 ea.) • 10 (5 ea.) 	3: <ul style="list-style-type: none"> • 1 • 1 • 1 	6: <ul style="list-style-type: none"> • Instance 1-Instance2 • Instance 2-Instance 4 • Instance 5-Instance 6 	23%

Dedicated Interfaces	Shared Interfaces	Number of Instances	% Forwarding Table Used
30: <ul style="list-style-type: none"> • 30 (6 ea.) 	2	5: <ul style="list-style-type: none"> • Instance 1-Instance 5 	28%
30: <ul style="list-style-type: none"> • 12 (6 ea.) • 18 (6 ea.) 	4: <ul style="list-style-type: none"> • 2 • 2 	5: <ul style="list-style-type: none"> • Instance 1-Instance2 • Instance 2-Instance 5 	26%
24: <ul style="list-style-type: none"> • 6 • 6 • 6 • 6 	7	4: <ul style="list-style-type: none"> • Instance 1 • Instance 2 • Instance 3 • Instance 4 	44%
24: <ul style="list-style-type: none"> • 12 (6 ea.) • 12 (6 ea.) 	14: <ul style="list-style-type: none"> • 7 • 7 	4: <ul style="list-style-type: none"> • Instance 1-Instance2 • Instance 2-Instance 4 	41%

The following table applies to three SM-44 security modules on a 9300 using subinterfaces on a single parent physical interface. For example, create a large EtherChannel to bundle all of your like-kind interfaces together, and then share subinterfaces of that EtherChannel. Sharing multiple physical interfaces uses more forwarding table resources than sharing multiple subinterfaces.

Each SM-44 module can support up to 14 instances. Instances are split between modules as necessary to stay within limits.

Table 10: Subinterfaces on One Parent and Instances on a Firepower 9300 with Three SM-44s

Dedicated Subinterfaces	Shared Subinterfaces	Number of Instances	% Forwarding Table Used
168: <ul style="list-style-type: none"> • 168 (4 ea.) 	0	42: <ul style="list-style-type: none"> • Instance 1-Instance 42 	33%
224: <ul style="list-style-type: none"> • 224 (16 ea.) 	0	14: <ul style="list-style-type: none"> • Instance 1-Instance 14 	27%
14: <ul style="list-style-type: none"> • 14 (1 ea.) 	1	14: <ul style="list-style-type: none"> • Instance 1-Instance 14 	46%

Dedicated Subinterfaces	Shared Subinterfaces	Number of Instances	% Forwarding Table Used
33: <ul style="list-style-type: none"> • 11 (1 ea.) • 11 (1 ea.) • 11 (1 ea.) 	3: <ul style="list-style-type: none"> • 1 • 1 • 1 	33: <ul style="list-style-type: none"> • Instance 1-Instance 11 • Instance 12-Instance 22 • Instance 23-Instance 33 	98%
70: <ul style="list-style-type: none"> • 70 (5 ea.) 	1	14: <ul style="list-style-type: none"> • Instance 1-Instance 14 	46%
165: <ul style="list-style-type: none"> • 55 (5 ea.) • 55 (5 ea.) • 55 (5 ea.) 	3: <ul style="list-style-type: none"> • 1 • 1 • 1 	33: <ul style="list-style-type: none"> • Instance 1-Instance 11 • Instance 12-Instance 22 • Instance 23-Instance 33 	98%
70: <ul style="list-style-type: none"> • 70 (5 ea.) 	2	14: <ul style="list-style-type: none"> • Instance 1-Instance 14 	46%
165: <ul style="list-style-type: none"> • 55 (5 ea.) • 55 (5 ea.) • 55 (5 ea.) 	6: <ul style="list-style-type: none"> • 2 • 2 • 2 	33: <ul style="list-style-type: none"> • Instance 1-Instance 11 • Instance 12-Instance 22 • Instance 23-Instance 33 	98%
70: <ul style="list-style-type: none"> • 70 (5 ea.) 	10	14: <ul style="list-style-type: none"> • Instance 1-Instance 14 	46%
165: <ul style="list-style-type: none"> • 55 (5 ea.) • 55 (5 ea.) • 55 (5 ea.) 	30: <ul style="list-style-type: none"> • 10 • 10 • 10 	33: <ul style="list-style-type: none"> • Instance 1-Instance 11 • Instance 12-Instance 22 • Instance 23-Instance 33 	102% DISALLOWED

Firepower 9300 with One SM-44

The following table applies to the Firepower 9300 with one SM-44 using only physical interfaces or EtherChannels. Without subinterfaces, the maximum number of interfaces are limited. Moreover, sharing multiple physical interfaces uses more forwarding table resources than sharing multiple subinterfaces.

The Firepower 9300 with one SM-44 can support up to 14 instances.

Table 11: Physical/EtherChannel Interfaces and Instances on a Firepower 9300 with One SM-44

Dedicated Interfaces	Shared Interfaces	Number of Instances	% Forwarding Table Used
32: <ul style="list-style-type: none"> • 8 • 8 • 8 • 8 	0	4: <ul style="list-style-type: none"> • Instance 1 • Instance 2 • Instance 3 • Instance 4 	16%
30: <ul style="list-style-type: none"> • 15 • 15 	0	2: <ul style="list-style-type: none"> • Instance 1 • Instance 2 	14%
14: <ul style="list-style-type: none"> • 14 (1 ea.) 	1	14: <ul style="list-style-type: none"> • Instance 1-Instance 14 	46%
14: <ul style="list-style-type: none"> • 7 (1 ea.) • 7 (1 ea.) 	2: <ul style="list-style-type: none"> • 1 • 1 	14: <ul style="list-style-type: none"> • Instance 1-Instance 7 • Instance 8-Instance 14 	37%
32: <ul style="list-style-type: none"> • 8 • 8 • 8 • 8 	1	4: <ul style="list-style-type: none"> • Instance 1 • Instance 2 • Instance 3 • Instance 4 	21%
32: <ul style="list-style-type: none"> • 16 (8 ea.) • 16 (8 ea.) 	2	4: <ul style="list-style-type: none"> • Instance 1-Instance 2 • Instance 3-Instance 4 	20%
32: <ul style="list-style-type: none"> • 8 • 8 • 8 • 8 	2	4: <ul style="list-style-type: none"> • Instance 1 • Instance 2 • Instance 3 • Instance 4 	25%

Dedicated Interfaces	Shared Interfaces	Number of Instances	% Forwarding Table Used
32: <ul style="list-style-type: none"> • 16 (8 ea.) • 16 (8 ea.) 	4: <ul style="list-style-type: none"> • 2 • 2 	4: <ul style="list-style-type: none"> • Instance 1-Instance 2 • Instance 3-Instance 4 	24%
24: <ul style="list-style-type: none"> • 8 • 8 • 8 	8	3: <ul style="list-style-type: none"> • Instance 1 • Instance 2 • Instance 3 	37%
10: <ul style="list-style-type: none"> • 10 (2 ea.) 	10	5: <ul style="list-style-type: none"> • Instance 1-Instance 5 	69%
10: <ul style="list-style-type: none"> • 6 (2 ea.) • 4 (2 ea.) 	20: <ul style="list-style-type: none"> • 10 • 10 	5: <ul style="list-style-type: none"> • Instance 1-Instance 3 • Instance 4-Instance 5 	59%
14: <ul style="list-style-type: none"> • 12 (2 ea.) 	10	7: <ul style="list-style-type: none"> • Instance 1-Instance 7 	109% DISALLOWED

The following table applies to the Firepower 9300 with one SM-44 using subinterfaces on a single parent physical interface. For example, create a large EtherChannel to bundle all of your like-kind interfaces together, and then share subinterfaces of that EtherChannel. Sharing multiple physical interfaces uses more forwarding table resources than sharing multiple subinterfaces.

The Firepower 9300 with one SM-44 can support up to 14 instances.

Table 12: Subinterfaces on One Parent and Instances on a Firepower 9300 with One SM-44

Dedicated Subinterfaces	Shared Subinterfaces	Number of Instances	% Forwarding Table Used
112: <ul style="list-style-type: none"> • 112 (8 ea.) 	0	14: <ul style="list-style-type: none"> • Instance 1-Instance 14 	17%
224: <ul style="list-style-type: none"> • 224 (16 ea.) 	0	14: <ul style="list-style-type: none"> • Instance 1-Instance 14 	17%
14: <ul style="list-style-type: none"> • 14 (1 ea.) 	1	14: <ul style="list-style-type: none"> • Instance 1-Instance 14 	46%

Dedicated Subinterfaces	Shared Subinterfaces	Number of Instances	% Forwarding Table Used
14: <ul style="list-style-type: none"> • 7 (1 ea.) • 7 (1 ea.) 	2: <ul style="list-style-type: none"> • 1 • 1 	14: <ul style="list-style-type: none"> • Instance 1-Instance 7 • Instance 8-Instance 14 	37%
112: <ul style="list-style-type: none"> • 112 (8 ea.) 	1	14: <ul style="list-style-type: none"> • Instance 1-Instance 14 	46%
112: <ul style="list-style-type: none"> • 56 (8 ea.) • 56 (8 ea.) 	2: <ul style="list-style-type: none"> • 1 • 1 	14: <ul style="list-style-type: none"> • Instance 1-Instance 7 • Instance 8-Instance 14 	37%
112: <ul style="list-style-type: none"> • 112 (8 ea.) 	2	14: <ul style="list-style-type: none"> • Instance 1-Instance 14 	46%
112: <ul style="list-style-type: none"> • 56 (8 ea.) • 56 (8 ea.) 	4: <ul style="list-style-type: none"> • 2 • 2 	14: <ul style="list-style-type: none"> • Instance 1-Instance 7 • Instance 8-Instance 14 	37%
140: <ul style="list-style-type: none"> • 140 (10 ea.) 	10	14: <ul style="list-style-type: none"> • Instance 1-Instance 14 	46%
140: <ul style="list-style-type: none"> • 70 (10 ea.) • 70 (10 ea.) 	20: <ul style="list-style-type: none"> • 10 • 10 	14: <ul style="list-style-type: none"> • Instance 1-Instance 7 • Instance 8-Instance 14 	37%

Viewing Shared Interface Resources

To view forwarding table and VLAN group usage, enter the **show detail** command under **scope fabric-interconnect**. For example:

```
Firepower# scope fabric-interconnect
Firepower /fabric-interconnect # show detail
```

```
Fabric Interconnect:
ID: A
Product Name: Cisco FPR9K-SUP
PID: FPR9K-SUP
VID: V02
Vendor: Cisco Systems, Inc.
Serial (SN): JAD104807YN
HW Revision: 0
Total Memory (MB): 16185
```

```

OOB IP Addr: 10.10.5.14
OOB Gateway: 10.10.5.1
OOB Netmask: 255.255.255.0
OOB IPv6 Address: ::
OOB IPv6 Gateway: ::
Prefix: 64
Operability: Operable
Thermal Status: Ok
Ingress VLAN Group Entry Count (Current/Max): 0/500
Switch Forwarding Path Entry Count (Current/Max): 16/1021
Current Task 1:
Current Task 2:
Current Task 3:

```

Inline Set Link State Propagation for the FTD

An inline set acts like a bump on the wire, and binds two interfaces together to slot into an existing network. This function allows the system to be installed in any network environment without the configuration of adjacent network devices. Inline interfaces receive all traffic unconditionally, but all traffic received on these interfaces is retransmitted out of an inline set unless explicitly dropped.

When you configure an inline set in the Firepower Threat Defense application and enable link state propagation, the Firepower Threat Defense sends inline set membership to the FXOS chassis. Link state propagation means that the chassis automatically brings down the second interface in the inline interface pair when one of the interfaces in an inline set goes down. When the downed interface comes back up, the second interface automatically comes back up, also. In other words, if the link state of one interface changes, the chassis senses the change and updates the link state of the other interface to match it. Note that the chassis requires up to 4 seconds to propagate link state changes. Link state propagation is especially useful in resilient network environments where routers are configured to reroute traffic automatically around network devices that are in a failure state.



Note Do not enable Hardware Bypass and link state propagation for the same inline set.

Guidelines and Limitations for Interfaces

VLAN Subinterfaces

- This document discusses *FXOS* VLAN subinterfaces only. You can separately create subinterfaces within the FTD application. See [FXOS Interfaces vs. Application Interfaces, on page 179](#) for more information.
- Subinterfaces (and the parent interfaces) can only be assigned to container instances.



Note If you assign a parent interface to a container instance, it only passes untagged (non-VLAN) traffic. Do not assign the parent interface unless you intend to pass untagged traffic.

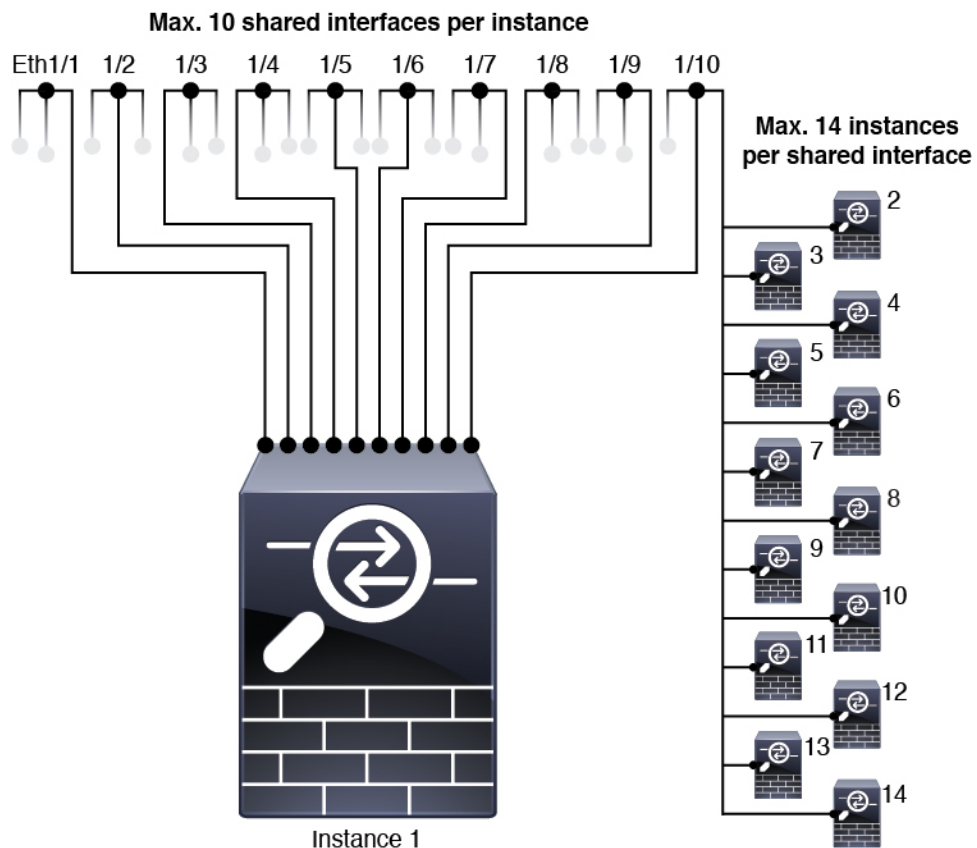
- Subinterfaces are supported on Data or Data-sharing type interfaces.

- You can create between 250 and 500 subinterfaces per chassis using up to 500 VLAN IDs, depending on your network deployment.
- See the following limitations within the logical device application; keep these limitations in mind when planning your interface allocation.
 - You cannot use subinterfaces for an Firepower Threat Defense inline set or as a passive interface.
 - If you use a subinterface for the failover link, then all subinterfaces on that parent, and the parent itself, are restricted for use as failover links. You cannot use some subinterfaces as failover links, and some as regular data interfaces.

Data-sharing Interfaces

- You cannot use a data-sharing interface with a native instance.
- Maximum 14 instances per shared interface. For example, you can allocate Ethernet1/1 to Instance1 through Instance14.

Maximum 10 shared interfaces per instance. For example, you can allocate Ethernet1/1.1 through Ethernet1/1.10 to Instance1.



- See the following limitations within the logical device application; keep these limitations in mind when planning your interface allocation.
 - You cannot use a data-sharing interface with a transparent firewall mode device.

- You cannot use a data-sharing interface with Firepower Threat Defense inline sets or passive interfaces.
- You cannot use a data-sharing interface for the failover link.

Inline Sets for FTD

- Supported for physical interfaces (both regular and breakout ports) and EtherChannels. Subinterfaces are not supported.
- Link state propagation is supported.
- Do not enable Hardware Bypass and link state propagation for the same inline set.

Hardware Bypass

- Supported for the Firepower Threat Defense; you can use them as regular interfaces for the ASA.
- The Firepower Threat Defense only supports Hardware Bypass with inline sets.
- Hardware Bypass-capable interfaces cannot be configured for breakout ports.
- You cannot include Hardware Bypass interfaces in an EtherChannel and use them for Hardware Bypass; you can use them as regular interfaces in an EtherChannel.
- Hardware Bypass is not supported with High Availability.
- Do not enable Hardware Bypass and link state propagation for the same inline set.

Default MAC Addresses

For native instances:

Default MAC address assignments depend on the type of interface.

- Physical interfaces—The physical interface uses the burned-in MAC address.
- EtherChannels—For an EtherChannel, all interfaces that are part of the channel group share the same MAC address. This feature makes the EtherChannel transparent to network applications and users, because they only see the one logical connection; they have no knowledge of the individual links. The port-channel interface uses a unique MAC address from a pool; interface membership does not affect the MAC address.

For container instances:

- MAC addresses for all interfaces are taken from a MAC address pool. For subinterfaces, if you decide to manually configure MAC addresses, make sure you use unique MAC addresses for all subinterfaces on the same parent interface to ensure proper classification. See [Automatic MAC Addresses for Container Instance Interfaces, on page 222](#).

Configure Interfaces

By default, physical interfaces are disabled. You can enable interfaces, add EtherChannels, add VLAN subinterfaces, edit interface properties, and configure breakout ports.



Note

Configure a Physical Interface

You can physically enable and disable interfaces, as well as set the interface speed and duplex. To use an interface, it must be physically enabled in FXOS and logically enabled in the application.



Note

- For QSFP40G-CUxM, auto-negotiation is always enabled by default and you cannot disable it.
 - If you replace an SFP on a port with a different SFP module, the speed, duplex, and auto-negotiation of the interface is not updated automatically. You must manually re-configure the interface.
-

Before you begin

- Interfaces that are already a member of an EtherChannel cannot be modified individually. Be sure to configure settings before you add it to the EtherChannel.

Procedure

Step 1 Enter interface mode.

scope eth-uplink

scope fabric a

Step 2 Enable the interface.

enter interface *interface_id*

enable

Example:

```
Firepower /eth-uplink/fabric # enter interface Ethernet1/8
Firepower /eth-uplink/fabric/interface # enable
```

Note

Interfaces that are already a member of a port-channel cannot be modified individually. If you use the **enter interface** or **scope interface** command on an interface that is a member of a port channel, you will receive

an error stating that the object does not exist. You should edit interfaces using the **enter interface** command before you add them to a port-channel.

Step 3 (Optional) Set Debounce Time.

set debounce-time 5000 {Enter a value between 0-15000 milli-seconds}

Example:

```
Firepower /eth-uplink/fabric/interface # set debounce-time 5000
```

Example:

Note

Configuring Debounce Time is not supported on 1G interfaces.

Step 4 (Optional) Set the interface type.

set port-type {data | data-sharing | mgmt | firepower-eventing | cluster}

Example:

```
Firepower /eth-uplink/fabric/interface # set port-type mgmt
```

The **data** keyword is the default type. The **data-sharing** type is only supported with container instances. Do not choose the **cluster** keyword; by default, the cluster control link is automatically created on Port-channel 48.

Step 5 Enable or disable autonegotiation, if supported for your interface.

set auto-negotiation {on | off}

Example:

```
Firepower /eth-uplink/fabric/interface* # set auto-negotiation off
```

If a peer switch connecting to the port over a 50G cable does not support auto-negotiation, ensure to disable auto-negotiation on the switch and the platform interface as well. For example, N9K-C93400LD-H1 does not support auto-negotiation on a 50G cable. Hence, for the port to be connected you must disable the default auto-negotiation on the platform and the switch:

Example:

```
N5-50G-SW(config-if) # speed 50000
N5-50G-SW(config-if) # no negotiate auto
```

Step 6 Set the interface speed.

set admin-speed {1gbps | 10gbps | 40gbps | 100gbps}

Example:

```
Firepower /eth-uplink/fabric/interface* # set admin-speed 1gbps
```

Step 7 Set the interface duplex mode.

```
set admin-duplex {fullduplex | halfduplex}
```

Example:

```
Firepower /eth-uplink/fabric/interface* # set admin-duplex halfduplex
```

- Step 8** If you edited the default flow control policy, it is already applied to interfaces. If you created a new policy, apply it to the interface. See [Configure a Flow Control Policy, on page 203](#).

```
set flow-control-policy name
```

Example:

```
Firepower /eth-uplink/fabric/interface* # set flow-control-policy flow1
```

- Step 9** Save the configuration.

```
commit-buffer
```

Example:

```
Firepower /eth-uplink/fabric/interface* # commit-buffer  
Firepower /eth-uplink/fabric/interface #
```

Add an EtherChannel (Port Channel)

An EtherChannel (also known as a port channel) can include up to 16 member interfaces of the same media type and capacity, and must be set to the same speed and duplex. The media type can be either RJ-45 or SFP; SFPs of different types (copper and fiber) can be mixed. You cannot mix interface capacities (for example 1GB and 10GB interfaces) by setting the speed to be lower on the larger-capacity interface. The Link Aggregation Control Protocol (LACP) aggregates interfaces by exchanging the Link Aggregation Control Protocol Data Units (LACPDUs) between two network devices.

You can configure each physical Data or Data-sharing interface in an EtherChannel to be:

- **Active**—Sends and receives LACP updates. An active EtherChannel can establish connectivity with either an active or a passive EtherChannel. You should use the active mode unless you need to minimize the amount of LACP traffic.
- **On**—The EtherChannel is always on, and LACP is not used. An “on” EtherChannel can only establish a connection with another “on” EtherChannel.



Note It may take up to three minutes for an EtherChannel to come up to an operational state if you change its mode from On to Active or from Active to On.

Non-data interfaces only support active mode.

LACP coordinates the automatic addition and deletion of links to the EtherChannel without user intervention. It also handles misconfigurations and checks that both ends of member interfaces are connected to the correct

channel group. “On” mode cannot use standby interfaces in the channel group when an interface goes down, and the connectivity and configurations are not checked.

When the Firepower 4100/9300 chassis creates an EtherChannel, the EtherChannel stays in a **Suspended** state for Active LACP mode or a **Down** state for On LACP mode until you assign it to a logical device, even if the physical link is up. The EtherChannel will be brought out of this **Suspended** state in the following situations:

- The EtherChannel is added as a data or management interface for a standalone logical device
- The EtherChannel is added as a management interface or cluster control link for a logical device that is part of a cluster
- The EtherChannel is added as a data interface for a logical device that is part of a cluster and at least one unit has joined the cluster

Note that the EtherChannel does not come up until you assign it to a logical device. If the EtherChannel is removed from the logical device or the logical device is deleted, the EtherChannel will revert to a **Suspended** or **Down** state.

Procedure

Step 1 Enter interface mode:

scope eth-uplink

scope fabric a

Step 2 Create the port-channel:

create port-channel *id*

enable

Step 3 Assign member interfaces:

create member-port *interface_id*

You can add up to 16 member interfaces of the same media type and capacity. The member interfaces must be set to the same speed and duplex, and must match the speed and duplex that you configured for this port channel. The media type can be either RJ-45 or SFP; SFPs of different types (copper and fiber) can be mixed. You cannot mix interface capacities (for example 1GB and 10GB interfaces) by setting the speed to be lower on the larger-capacity interface.

Example:

```
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
```

Step 4 (Optional) Set the interface type.

set port-type {**data** | **data-sharing** | **mgmt** | **firepower-eventing** | **cluster**}

Example:

```
Firepower /eth-uplink/fabric/port-channel # set port-type data
```

The **data** keyword is the default type. The **data-sharing** type is only supported with container instances. Do not choose the **cluster** keyword unless you want to use this port-channel as the cluster control link instead of the default.

Step 5 Set the required interface speed for members of the port-channel.

set speed {**10mbps** | **100mbps** | **1gbps** | **10gbps** | **40gbps** | **100gbps**}

If you add a member interface that is not at the specified speed, it will not successfully join the port channel. The default is **10gbps**.

Example:

```
Firepower /eth-uplink/fabric/port-channel* # set speed 1gbps
```

Step 6 (Optional) Set the required duplex for members of the port-channel.

set duplex {**fullduplex** | **halfduplex**}

If you add a member interface that is configured with the specified duplex, it will not successfully join the port channel. The default is **fullduplex**.

Example:

```
Firepower /eth-uplink/fabric/port-channel* # set duplex fullduplex
```

Step 7 Enable or disable autonegotiation, if supported for your interface.

set auto-negotiation {**on** | **off**}

Example:

```
Firepower /eth-uplink/fabric/interface* # set auto-negotiation off
```

Step 8 Set the LACP port-channel mode for data and data-sharing interfaces.

For non-Data and non-data-sharing interfaces, the mode is always active.

set port-channel-mode {**active** | **on**}

Example:

```
Firepower /eth-uplink/fabric/port-channel* # set port-channel-mode on
```

Step 9 If you edited the default flow control policy, it is already applied to interfaces. If you created a new policy, apply it to the interface. See [Configure a Flow Control Policy, on page 203](#).

set flow-control-policy *name*

Example:

```
Firepower /eth-uplink/fabric/interface* # set flow-control-policy flow1
```

Step 10

Commit the configuration:

commit-buffer

Add a VLAN Subinterface for Container Instances

You can add between 250 and 500 VLAN subinterfaces to the chassis, depending on your network deployment.

VLAN IDs per interface must be unique, and within a container instance, VLAN IDs must be unique across all assigned interfaces. You can reuse VLAN IDs on *separate* interfaces as long as they are assigned to different container instances. However, each subinterface still counts towards the limit even though it uses the same ID.

This document discusses *FXOS* VLAN subinterfaces only. You can separately create subinterfaces within the FTD application.

Procedure

Step 1

Enter fabric a mode.

scope eth-uplink

scope fabric a

Example:

```
Firepower# scope eth-uplink
Firepower /eth-uplink # scope fabric a
Firepower /eth-uplink/fabric #
```

Step 2

Enter the interface to which you want to add the subinterface.

enter {interface | port-channel} interface_id

You cannot add a subinterface to a physical interface that is currently allocated to a logical device. If other subinterfaces of the parent are allocated, you can add a new subinterface as long as the parent interface itself is not allocated.

Subinterfaces are supported on data or data-sharing type interfaces.

Example:

```
Firepower /eth-uplink/fabric # enter interface Ethernet1/8
Firepower /eth-uplink/fabric/interface #
```

Step 3

Create the subinterface.

enter subinterface id

- *id*—Set the ID between 1 and 4294967295. This ID will be appended to the parent interface ID as *interface_id.subinterface_id*. For example, if you add a subinterface to Ethernet1/1 with the ID of 100, then the subinterface ID will be: Ethernet1/1.100. This ID is not the same as the VLAN ID, although you can set them to match for convenience.

Example:

```
Firepower /eth-uplink/fabric/interface # enter subinterface 100
Firepower /eth-uplink/fabric/interface/subinterface* #
```

Step 4 Set the VLAN.**set vlan *id***

- *id*—Set the VLAN ID between 1 and 4095.

Example:

```
Firepower /eth-uplink/fabric/interface/subinterface* # set vlan 100
```

Step 5 Set the interface type.**set port-type {data | data-sharing}****Example:**

```
Firepower /eth-uplink/fabric/interface/subinterface* # set port-type data
```

The type is independent of the parent interface type; you can have a data-sharing parent and a data subinterface, for example. The default type is data.

Step 6 Save the configuration.**commit-buffer****Example:**

```
Firepower /eth-uplink/fabric/interface/subinterface* # commit-buffer
Firepower /eth-uplink/fabric/interface/subinterface #
```

Example

The following example creates 3 subinterfaces on Ethernet 1/1, and sets them to be data-sharing interfaces.

```
Firepower# scope eth-uplink
Firepower /eth-uplink # scope fabric a
Firepower /eth-uplink/fabric # enter interface Ethernet1/1
Firepower /eth-uplink/fabric/interface # enter subinterface 10
Firepower /eth-uplink/fabric/interface/subinterface* # set vlan 10
Firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
Firepower /eth-uplink/fabric/interface/subinterface* # exit
```

```
Firepower /eth-uplink/fabric/interface # enter subinterface 11
Firepower /eth-uplink/fabric/interface/subinterface* # set vlan 11
Firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
Firepower /eth-uplink/fabric/interface/subinterface* # exit
Firepower /eth-uplink/fabric/interface # enter subinterface 12
Firepower /eth-uplink/fabric/interface/subinterface* # set vlan 12
Firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
Firepower /eth-uplink/fabric/interface/subinterface* # commit-buffer
Firepower /eth-uplink/fabric/interface/subinterface #
```

Configure Breakout Cables

The following procedure shows how to configure breakout cables for use with the Firepower 4100/9300 chassis. You can use a breakout cable to provide four 10 Gbps ports in place of a single 40 Gbps port.

Before you begin

Hardware Bypass-capable interfaces cannot be configured for breakout ports.

Procedure

Step 1 To create a new breakout, use the following commands:

- a) Enter cabling mode:

scope cabling

scope fabric a

- b) Create the breakout:

create breakout *network_module_slot* *port*

Example:

```
Firepower /cabling/fabric/ # create breakout 2 1
```

- c) Commit the configuration:

commit-buffer

This will cause an automatic reboot. If you are configuring more than one breakout, you should create all of them before you issue the commit-buffer command.

Step 2 To enable/configure the breakout ports, use the following commands:

- a) Enter interface mode:

scope eth-uplink

scope fabric a

scope aggr-interface *network_module_slot* *port*

Note

Interfaces that are already a member of a port-channel cannot be modified individually. If you use the **enter interface** or **scope interface** command on an interface that is a member of a port channel, you will receive an error stating that the object does not exist. You should edit interfaces using the **enter interface** command before you add them to a port-channel.

- b) Use the **set** command to configure the interface speed and port type.
Use the **enable** or **disable** command to set the administrative state of the interface.
- c) Commit the configuration:
commit-buffer

Configure a Flow Control Policy

Flow control policies determine whether the Ethernet ports send and receive IEEE 802.3x pause frames when the receive buffer for a port fills. These pause frames request that the transmitting port stop sending data for a few milliseconds until the buffer clears. For flow control to work between devices, you must enable the corresponding receive and send flow control parameters for both devices.

The default policy disables send and receive control, and sets the priority to autonegotiate.

Procedure

- Step 1** Enter eth-uplink and then flow-control mode.

scope eth-uplink

scope flow-control

Example:

```
firepower-4110# scope eth-uplink
firepower-4110 /eth-uplink # scope flow-control
firepower-4110 /eth-uplink/flow-control #
```

- Step 2** Edit or create a flow control policy.

enter policy *name*

If you want to edit the default policy, enter **default** for the name.

Example:

```
firepower-4110 /eth-uplink/flow-control # enter policy default
firepower-4110 /eth-uplink/flow-control/policy* #
```

- Step 3** Set the priority.

set prio {auto | on}

The priority sets whether to negotiate or enable PPP for this link.

Example:

```
firepower-4110 /eth-uplink/flow-control/policy* # set prio on
```

Step 4 Enable or disable flow control receive pauses.**set receive {on | off}**

- **on**—Pause requests are honored and all traffic is halted on that uplink port until the network cancels the pause request.
- **off**—Pause requests from the network are ignored and traffic flow continues as normal.

Example:

```
firepower-4110 /eth-uplink/flow-control/policy* # set receive on
```

Step 5 Enable or disable flow control send pauses.**set send {on | off}**

- **on**—The Firepower 4100/9300 sends a pause request to the network if the incoming packet rate becomes too high. The pause remains in effect for a few milliseconds before traffic is reset to normal levels.
- **off**—Traffic on the port flows normally regardless of the packet load.

Example:

```
firepower-4110 /eth-uplink/flow-control/policy* # set send on
```

Step 6 Save the configuration.**commit-buffer****Example:**

```
firepower-4110 /eth-uplink/flow-control/policy* # commit-buffer  
firepower-4110 /eth-uplink/flow-control/policy #
```

Example

The following example configures a flow control policy.

```
firepower-4110# scope eth-uplink  
firepower-4110 /eth-uplink # scope flow-control  
firepower-4110 /eth-uplink/flow-control # enter policy FlowControlPolicy23  
firepower-4110 /eth-uplink/flow-control/policy* # set prio auto  
firepower-4110 /eth-uplink/flow-control/policy* # set receive on  
firepower-4110 /eth-uplink/flow-control/policy* # set send on  
firepower-4110 /eth-uplink/flow-control/policy* # commit-buffer  
firepower-4110 /eth-uplink/flow-control/policy #
```

Monitoring Interfaces



Note There can be a difference between the FXOS and Firepower Threat Defense/ASA interface utilization due to fragmentation drops in the Firepower Threat Defense/ASA. To view fragmentation drops, see the Firepower Threat Defense/ASA **show asp drop** and **show fragment** commands.

• show interface

Shows interface status.



Note Interfaces that act as ports in port channels do not appear in this list.

```
Firepower# scope eth-uplink
Firepower /eth-uplink # scope fabric a
Firepower /eth-uplink/fabric # show interface
```

```
Interface:
  Port Name      Port Type      Admin State Oper State
  Allowed Vlan State Reason
  -----
  Ethernet1/2    Data           Enabled      Up
  All
  Ethernet1/4    Mgmt           Enabled      Up
  All
  Ethernet1/5    Data           Enabled      Up
  Untagged
  Ethernet1/7    Firepower Eventing Enabled      Up
  All
  Ethernet1/8    Data           Disabled     Sfp Not Present
  All           Unknown
  Ethernet2/1    Data           Disabled     Sfp Not Present
  All           Unknown
  Ethernet2/2    Data           Disabled     Sfp Not Present
  All           Unknown
  Ethernet2/3    Data           Disabled     Sfp Not Present
  All           Unknown
  Ethernet2/4    Data           Disabled     Sfp Not Present
  All           Unknown
  Ethernet2/5    Data           Disabled     Sfp Not Present
  All           Unknown
  Ethernet2/6    Data           Disabled     Sfp Not Present
  All           Unknown
  Ethernet2/7    Data           Disabled     Sfp Not Present
  All           Unknown
  Ethernet2/8    Data           Disabled     Sfp Not Present
  All           Unknown
```

• show port-channel

Shows port-channel status.

```
Firepower# scope eth-uplink
Firepower /eth-uplink # scope fabric a
Firepower /eth-uplink/fabric # show port-channel
```

Port Channel:

Port Channel Id	Name	Port Type	Admin State	Oper State
1	Port-channel1	Data	Enabled	Up
2	Port-channel2	Data	Enabled	Failed
48	Port-channel48	Cluster	Enabled	Up

• show detail

View forwarding table and VLAN group usage for shared interfaces.

```
Firepower# scope fabric-interconnect
DFirepower /fabric-interconnect # show detail
```

Fabric Interconnect:

```
ID: A
Product Name: Cisco FPR9K-SUP
PID: FPR9K-SUP
VID: V02
Vendor: Cisco Systems, Inc.
Serial (SN): JAD104807YN
HW Revision: 0
Total Memory (MB): 16185
OOB IP Addr: 10.10.5.14
OOB Gateway: 10.10.5.1
OOB Netmask: 255.255.255.0
OOB IPv6 Address: ::
OOB IPv6 Gateway: ::
Prefix: 64
Operability: Operable
Thermal Status: Ok
Ingress VLAN Group Entry Count (Current/Max): 0/500
Switch Forwarding Path Entry Count (Current/Max): 16/1021
Current Task 1:
Current Task 2:
Current Task 3:
```

• show subinterface

Shows subinterfaces for a given interface.

```
Firepower# scope eth-uplink
Firepower /eth-uplink # scope fabric a
Firepower /eth-uplink/fabric # enter interface ethernet1/8
Firepower /eth-uplink/fabric/interface # show subinterface
```

Sub Interface:

Sub-If Id	Sub-Interface Name	VLAN	Port Type
10	Ethernet1/8.10	11	Data
11	Ethernet1/8.11	12	Data

- **show mac-address**

Shows MAC address assignments for container instance interfaces.

```
Firepower# scope ssa
Firepower /ssa # scope auto-macpool
Firepower /ssa/auto-macpool # show mac-address
Mac Address Item:
  Mac Address      Owner Profile      Owner Name
  -----
A2:46:C4:00:00:1E  ftdl3              Port-channel14
A2:46:C4:00:00:20  ftdl4              Port-channel15
A2:46:C4:00:01:7B  ftd1               Ethernet1/3
A2:46:C4:00:01:7C  ftdl2              Port-channel11
A2:46:C4:00:01:7D  ftdl3              Port-channel14
A2:46:C4:00:01:7E  ftdl4              Port-channel15
A2:46:C4:00:01:7F  ftd1               Ethernet1/2
A2:46:C4:00:01:80  ftdl2              Ethernet1/2
A2:46:C4:00:01:81  ftdl3              Ethernet1/2
A2:46:C4:00:01:82  ftdl4              Ethernet1/2
A2:46:C4:00:01:83  ftd2               Ethernet3/1/4
A2:46:C4:00:01:84  ftd2               Ethernet3/1/1
A2:46:C4:00:01:85  ftd2               Ethernet3/1/3
A2:46:C4:00:01:86  ftd2               Ethernet3/1/2
A2:46:C4:00:01:87  ftd2               Ethernet1/2
A2:46:C4:00:01:88  ftd1               Port-channel121
A2:46:C4:00:01:89  ftd1               Ethernet1/8
```

Troubleshooting Interfaces

Error: The Switch Forwarding Path has 1076 entries and exceeds the limit of 1024. If you are adding an interface, reduce the number of shared interfaces assigned to logical devices, reduce the number of logical devices sharing interfaces, or use non-shared subinterfaces instead. If you are deleting a subinterface, you are seeing this message because the remaining configuration is no longer optimized to fit within the Switch Forwarding Path table. See the FXOS configuration guide for troubleshooting information about the deletion use case. Use 'show detail' under scope 'fabric-interconnect' to view the current Switch Forwarding Path Entry Count.

If you see this error when trying to delete a shared subinterface from a logical device, it is because your new configuration is not following this guideline for shared subinterfaces: use the same set of subinterfaces with the same group of logical devices. If you delete a shared subinterface from one logical device, you can end up with more VLAN groups and therefore less efficient usage of the forwarding table. To work around this situation, you need to add and delete shared subinterfaces simultaneously using the CLI so that you maintain the same set of subinterfaces for the same group of logical devices.

See the following scenarios for more information. These scenarios start with the following interfaces and logical devices:

- Shared subinterface set on the same parent: Port-Channel1.100 (VLAN 100), Port-Channel1.200 (VLAN 200), Port-Channel1.300 (VLAN 300)
- Logical device group: LD1, LD2, LD3, and LD4

Scenario 1: Remove a subinterface from one logical device, but leave it assigned to other logical devices

Do not remove the subinterface. Instead, just disable it in the application configuration. If you have to remove the subinterface, you will need to reduce the number of shared interfaces in general to continue to fit in the forwarding table.

Scenario 2: Remove all subinterfaces in the set from one logical device

Remove all subinterfaces in the set from the logical device at the CLI, and then save the configuration so that the removal is simultaneous.

1. View the VLAN groups for reference. In the following output, group 1 includes VLAN 100, 200, and 300, representing the 3 shared subinterfaces.

```
firepower# connect fxos
[...]
firepower(fxos)# show ingress-vlan-groups
ID   Class ID   Status      INTF      Vlan Status
1    1           configured
100  present
200  present
300  present
2048 512        configured
0    present
2049 511        configured
0    present
firepower(fxos)# exit
firepower#
```

2. View the shared subinterfaces assigned to the logical device you want to change.

```
firepower# scope ssa
firepower /ssa # scope logical-device LD1
firepower /ssa/logical-device # show external-port-link
```

External-Port Link:			
Name	Port or Port Channel Name	Port Type	App Name
Description			
Ethernet14_ftd	Ethernet1/4	Mgmt	ftd
PC1.100_ftd	Port-channel1.100	Data Sharing	ftd
PC1.200_ftd	Port-channel1.200	Data Sharing	ftd
PC1.300_ftd	Port-channel1.300	Data Sharing	ftd

3. Remove the subinterfaces from the logical device, and then save the configuration.

```
firepower /ssa/logical-device # delete external-port-link PC1.100_ftd
firepower /ssa/logical-device* # delete external-port-link PC1.200_ftd
firepower /ssa/logical-device* # delete external-port-link PC1.300_ftd
firepower /ssa/logical-device* # commit-buffer
firepower /ssa/logical-device #
```

If you had committed the configuration in the middle, you would have ended up with 2 VLAN groups, which could have generated the switch forwarding path error and prevented you from saving the configuration.

Scenario 3: Remove a subinterface from all logical devices in the group

Remove the subinterface from all logical devices in the group at the CLI, and then save the configuration so that the removal is simultaneous. For example:

1. View the VLAN groups for reference. In the following output, group 1 includes VLAN 100, 200, and 300, representing the 3 shared subinterfaces.

```
firepower# connect fxos
[...]
firepower(fxos)# show ingress-vlan-groups
ID   Class ID   Status      INTF      Vlan Status
1    1           configured
                                100 present
                                200 present
                                300 present

2048 512       configured
                                0   present

2049 511       configured
                                0   present
```

2. View the interfaces assigned to each logical device, and note the shared subinterfaces in common. If they are on the same parent interface, they will belong to one VLAN group, and should match the **show ingress-vlan-groups** list. In Firepower Chassis Manager, you can hover over each shared subinterface to see which instances it is allocated to.

Figure 7: Instances per shared interface

All Interfaces Hardware Bypass					
Interface	Type	Admin Speed	Operational Speed	Instances	VLAN
MGMT	Management				
Port-channel1	data	1gbps	1gbps		
Port-channel1.100	data-sharing			LD4...	100
Port-channel1.200	data-sharing			LD4...	
Port-channel1.300	data-sharing			LD4...	300
Ethernet1/3					
Port-channel2	data	1gbps	1gbps		

Interface is shared by 4 instances:
LD4
LD3
LD2
LD1

At the CLI, you can view characteristics of all logical devices, including the allocated interfaces.

```
firepower# scope ssa
firepower /ssa # show logical-device expand

Logical Device:
  Name: LD1
  Description:
  Slot ID: 1
  Mode: Standalone
  Oper State: Ok
  Template Name: ftd

External-Port Link:
  Name: Ethernet14_ftd
  Port or Port Channel Name: Ethernet1/4
  Port Type: Mgmt
  App Name: ftd
  Description:
```

```
Name: PC1.100_ftd
Port or Port Channel Name: Port-channel1.100
Port Type: Data Sharing
App Name: ftd
Description:
```

```
Name: PC1.200_ftd
Port or Port Channel Name: Port-channel1.200
Port Type: Data Sharing
App Name: ftd
Description:
```

```
System MAC address:
  Mac Address
  -----
  A2:F0:B0:00:00:25
```

```
Name: PC1.300_ftd
Port or Port Channel Name: Port-channel1.300
Port Type: Data Sharing
App Name: ftd
Description:
```

[...]

```
Name: LD2
Description:
Slot ID: 1
Mode: Standalone
Oper State: Ok
Template Name: ftd
```

```
External-Port Link:
  Name: Ethernet14_ftd
  Port or Port Channel Name: Ethernet1/4
  Port Type: Mgmt
  App Name: ftd
  Description:
```

```
Name: PC1.100_ftd
Port or Port Channel Name: Port-channel1.100
Port Type: Data Sharing
App Name: ftd
Description:
```

```
Name: PC1.200_ftd
Port or Port Channel Name: Port-channel1.200
Port Type: Data Sharing
App Name: ftd
Description:
```

```
System MAC address:
  Mac Address
  -----
  A2:F0:B0:00:00:28
```

```
Name: PC1.300_ftd
Port or Port Channel Name: Port-channel1.300
Port Type: Data Sharing
App Name: ftd
Description:
```

[...]

```
Name: LD3
Description:
Slot ID: 1
Mode: Standalone
Oper State: Ok
Template Name: ftd

External-Port Link:
  Name: Ethernet14_ftd
  Port or Port Channel Name: Ethernet1/4
  Port Type: Mgmt
  App Name: ftd
  Description:

  Name: PC1.100_ftd
  Port or Port Channel Name: Port-channel1.100
  Port Type: Data Sharing
  App Name: ftd
  Description:

  Name: PC1.200_ftd
  Port or Port Channel Name: Port-channel1.200
  Port Type: Data Sharing
  App Name: ftd
  Description:

System MAC address:
  Mac Address
  -----
  A2:F0:B0:00:00:2B

  Name: PC1.300_ftd
  Port or Port Channel Name: Port-channel1.300
  Port Type: Data Sharing
  App Name: ftd
  Description:
```

[...]

```
Name: LD4
Description:
Slot ID: 1
Mode: Standalone
Oper State: Ok
Template Name: ftd

External-Port Link:
  Name: Ethernet14_ftd
  Port or Port Channel Name: Ethernet1/4
  Port Type: Mgmt
  App Name: ftd
  Description:

  Name: PC1.100_ftd
  Port or Port Channel Name: Port-channel1.100
  Port Type: Data Sharing
  App Name: ftd
  Description:

  Name: PC1.200_ftd
  Port or Port Channel Name: Port-channel1.200
  Port Type: Data Sharing
  App Name: ftd
  Description:
```

```

System MAC address:
  Mac Address
  -----
  A2:F0:B0:00:00:2E

Name: PC1.300_ftd
Port or Port Channel Name: Port-channel1.300
Port Type: Data Sharing
App Name: ftd
Description:

[...]

```

3. Remove the subinterface from each logical device, and then save the configuration.

```

firepower /ssa # scope logical device LD1
firepower /ssa/logical-device # delete external-port-link PC1.300_ftd
firepower /ssa/logical-device* # exit
firepower /ssa* # scope logical-device LD2
firepower /ssa/logical-device* # delete external-port-link PC1.300_ftd
firepower /ssa/logical-device* # exit
firepower /ssa* # scope logical-device LD3
firepower /ssa/logical-device* # delete external-port-link PC1.300_ftd
firepower /ssa/logical-device* # exit
firepower /ssa* # scope logical-device LD4
firepower /ssa/logical-device* # delete external-port-link PC1.300_ftd
firepower /ssa/logical-device* # commit-buffer
firepower /ssa/logical-device #

```

If you had committed the configuration in the middle, you would have ended up with 2 VLAN groups, which could have generated the switch forwarding path error and prevented you from saving the configuration.

Scenario 4: Add a subinterface to one or more logical devices

Add the subinterface to *all* logical devices in the group at the CLI, and then save the configuration so that the addition is simultaneous.

1. Add the subinterface to each logical device, and then save the configuration.

```

firepower# scope ssa
firepower /ssa # scope logical-device LD1
firepower /ssa/logical-device # create external-port-link PC1.400_ftd Port-channel1.400
ftd
firepower /ssa/logical-device/external-port-link* # exit
firepower /ssa/logical-device* # exit
firepower /ssa # scope logical-device LD2
firepower /ssa/logical-device # create external-port-link PC1.400_ftd Port-channel1.400
ftd
firepower /ssa/logical-device/external-port-link* # exit
firepower /ssa/logical-device* # exit
firepower /ssa # scope logical-device LD3
firepower /ssa/logical-device # create external-port-link PC1.400_ftd Port-channel1.400
ftd
firepower /ssa/logical-device/external-port-link* # exit
firepower /ssa/logical-device* # exit
firepower /ssa # scope logical-device LD4
firepower /ssa/logical-device # create external-port-link PC1.400_ftd Port-channel1.400
ftd
firepower /ssa/logical-device/external-port-link* # commit-buffer

```

```
firepower /ssa/logical-device/external-port-link #
```

If you had committed the configuration in the middle, you would have ended up with 2 VLAN groups, which could have generated the switch forwarding path error and prevented you from saving the configuration.

2. You can check that the Port-channel1.400 VLAN ID was added to VLAN group 1.

```
firepower /ssa/logical-device/external-port-link # connect fxos
[...]
firepower(fxos)# show ingress-vlan-groups
ID   Class ID  Status      INTF      Vlan Status
1    1          configured
                                200 present
                                100 present
                                300 present
                                400 present
2048 512      configured
                                0   present
2049 511      configured
                                0   present
firepower(fxos)# exit
firepower /ssa/logical-device/external-port-link #
```

History for Interfaces

Feature Name	Platform Releases	Feature Information
VLAN subinterfaces for use with container instances	2.4.1	<p>To provide flexible physical interface use, you can create VLAN subinterfaces in FXOS and also share interfaces between multiple instances.</p> <p>Note Requires Firepower Threat Defense Version 6.3 or later.</p> <p>New/Modified commands: create subinterface, set vlan, show interface, show subinterface</p> <p>New/Modified FMC screens:</p> <p>Devices > Device Management > Edit icon > Interfaces tab</p>
Data-sharing interfaces for container instances	2.4.1	<p>To provide flexible physical interface use, you can share interfaces between multiple instances.</p> <p>Note Requires Firepower Threat Defense Version 6.3 or later.</p> <p>New/Modified commands: set port-type data-sharing, show interface</p>
Support for data EtherChannels in On mode	2.4.1	<p>You can now set data and data-sharing EtherChannels to either Active LACP mode or to On mode. Other types of EtherChannels only support Active mode.</p> <p>New/Modified commands: set port-channel-mode</p>

Feature Name	Platform Releases	Feature Information
Support for EtherChannels in Firepower Threat Defense inline sets	2.1.1	You can now use EtherChannels in a Firepower Threat Defense inline set.
Inline set link state propagation support for the Firepower Threat Defense	2.0.1	<p>When you configure an inline set in the Firepower Threat Defense application and enable link state propagation, the Firepower Threat Defense sends inline set membership to the FXOS chassis. Link state propagation means that the chassis automatically brings down the second interface in the inline interface pair when one of the interfaces in an inline set goes down.</p> <p>New/Modified commands: show fault grep link-down, show interface detail</p>
Support for Hardware bypass network modules for the Firepower Threat Defense	2.0.1	<p>Hardware Bypass ensures that traffic continues to flow between an inline interface pair during a power outage. This feature can be used to maintain network connectivity in the case of software or hardware failures.</p> <p>New/Modified FMC screens:</p> <p>Devices > Device Management > Interfaces > Edit Physical Interface</p>
Firepower-eventing type interface for Firepower Threat Defense	1.1.4	<p>You can specify an interface as firepower-eventing for use with the Firepower Threat Defense. This interface is a secondary management interface for Firepower Threat Defense devices. To use this interface, you must configure its IP address and other parameters at the Firepower Threat Defense CLI. For example, you can separate management traffic from events (such as web events). See the "Management Interfaces" section in the FMC configuration guide <i>System Configuration</i> chapter.</p> <p>New/Modified FXOS commands: set port-type firepower-eventing, show interface</p>



CHAPTER 11

Logical Devices

- [About Logical Devices, on page 215](#)
- [Requirements and Prerequisites for Logical Devices, on page 223](#)
- [Guidelines and Limitations for Logical Devices, on page 228](#)
- [Add a Standalone Logical Device, on page 234](#)
- [Add a High Availability Pair, on page 251](#)
- [Add a Cluster, on page 251](#)
- [Configure Radware DefensePro, on page 279](#)
- [Configure TLS Crypto Acceleration, on page 289](#)
- [Manage Logical Devices, on page 294](#)
- [Monitoring Logical Devices, on page 303](#)
- [Examples for Inter-Site Clustering, on page 304](#)
- [History for Logical Devices, on page 308](#)

About Logical Devices

A logical device lets you run one application instance (either ASA or Firepower Threat Defense) and also one optional decorator application (Radware DefensePro) to form a service chain.

When you add a logical device, you also define the application instance type and version, assign interfaces, and configure bootstrap settings that are pushed to the application configuration.



Note For the Firepower 9300, you can install different application types (ASA and Firepower Threat Defense) on separate modules in the chassis. You can also run different versions of an application instance type on separate modules.

Standalone and Clustered Logical Devices

You can add the following logical device types:

- **Standalone**—A standalone logical device operates as a standalone unit or as a unit in a High Availability pair.

- **Cluster**—A clustered logical device lets you group multiple units together, providing all the convenience of a single device (management, integration into a network) while achieving the increased throughput and redundancy of multiple devices. Multiple module devices, like the Firepower 9300, support intra-chassis clustering. For the Firepower 9300, all three modules must participate in the cluster.

Logical Device Application Instances: Container and Native

Application instances run in the following deployment types:

- **Native instance**—A native instance uses all of the resources (CPU, RAM, and disk space) of the security module/engine, so you can only install one native instance.
- **Container instance**—A container instance uses a subset of resources of the security module/engine, so you can install multiple container instances. Multi-instance capability is only supported for the Firepower Threat Defense using FMC; it is not supported for the ASA.



Note Multi-instance capability is similar to ASA multiple context mode, although the implementation is different. Multiple context mode partitions a single application instance, while multi-instance capability allows independent container instances. Container instances allow hard resource separation, separate configuration management, separate reloads, separate software updates, and full Firepower Threat Defense feature support. Multiple context mode, due to shared resources, supports more contexts on a given platform. Multiple context mode is not available on the Firepower Threat Defense.

For the Firepower 9300, you can use a native instance on some modules, and container instances on the other module(s).

Container Instance Interfaces

To provide flexible physical interface use for container instances, you can create VLAN subinterfaces in FXOS and also share interfaces (VLAN or physical) between multiple instances. Native instances cannot use VLAN subinterfaces or shared interfaces. See [Shared Interface Scalability, on page 182](#) and [Add a VLAN Subinterface for Container Instances, on page 200](#).



Note This document discusses *FXOS* VLAN subinterfaces only. You can separately create subinterfaces within the FTD application. See [FXOS Interfaces vs. Application Interfaces, on page 179](#) for more information.

How the Chassis Classifies Packets

Each packet that enters the chassis must be classified, so that the chassis can determine to which instance to send a packet.

- **Unique Interfaces**—If only one instance is associated with the ingress interface, the chassis classifies the packet into that instance. For bridge group member interfaces (in transparent mode or routed mode), inline sets, or passive interfaces, this method is used to classify packets at all times.

- **Unique MAC Addresses**—The chassis automatically generates unique MAC addresses for all interfaces, including shared interfaces. If multiple instances share an interface, then the classifier uses unique MAC addresses assigned to the interface in each instance. An upstream router cannot route directly to an instance without unique MAC addresses. You can also set the MAC addresses manually when you configure each interface within the application. However, even if you are not sharing a subinterface, if you manually configure MAC addresses, make sure you use unique MAC addresses for all subinterfaces on the same parent interface to ensure proper classification.



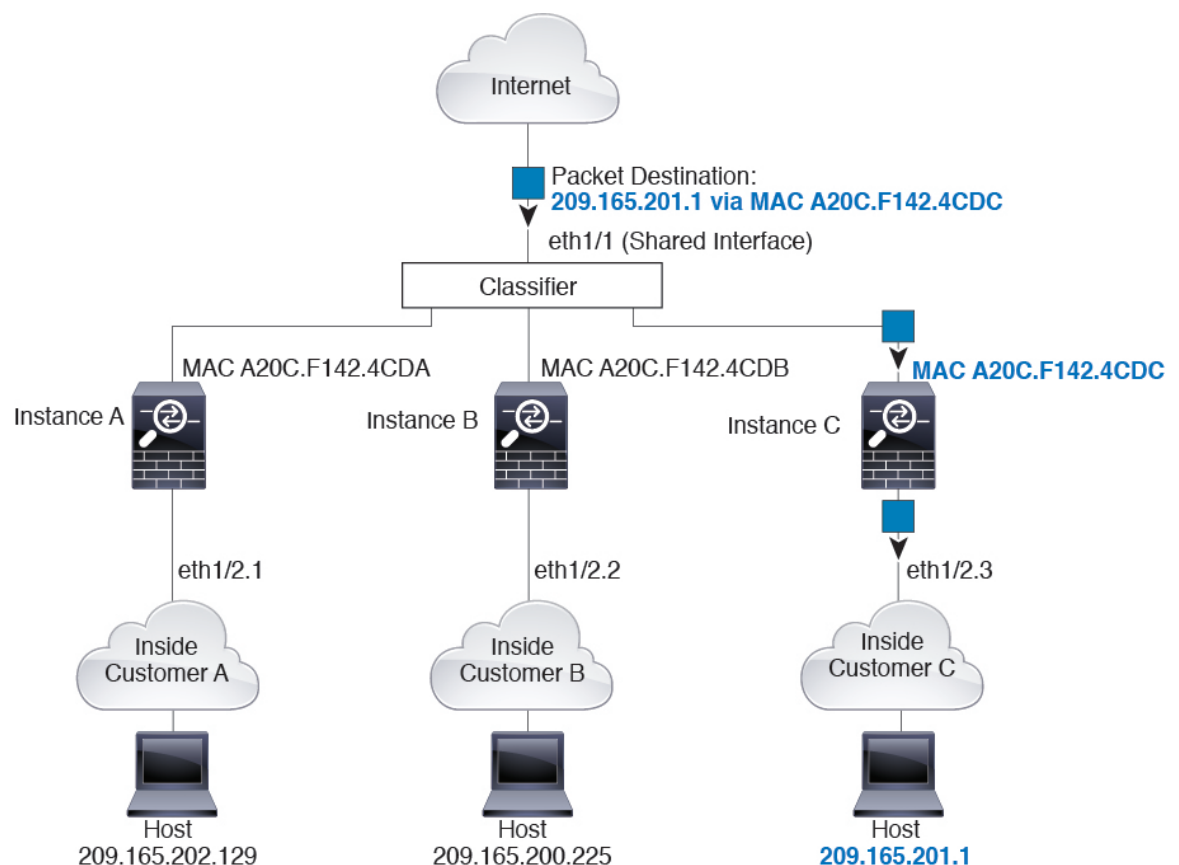
Note If the destination MAC address is a multicast or broadcast MAC address, the packet is duplicated and delivered to each instance.

Classification Examples

Packet Classification with a Shared Interface Using MAC Addresses

The following figure shows multiple instances sharing an outside interface. The classifier assigns the packet to Instance C because Instance C includes the MAC address to which the router sends the packet.

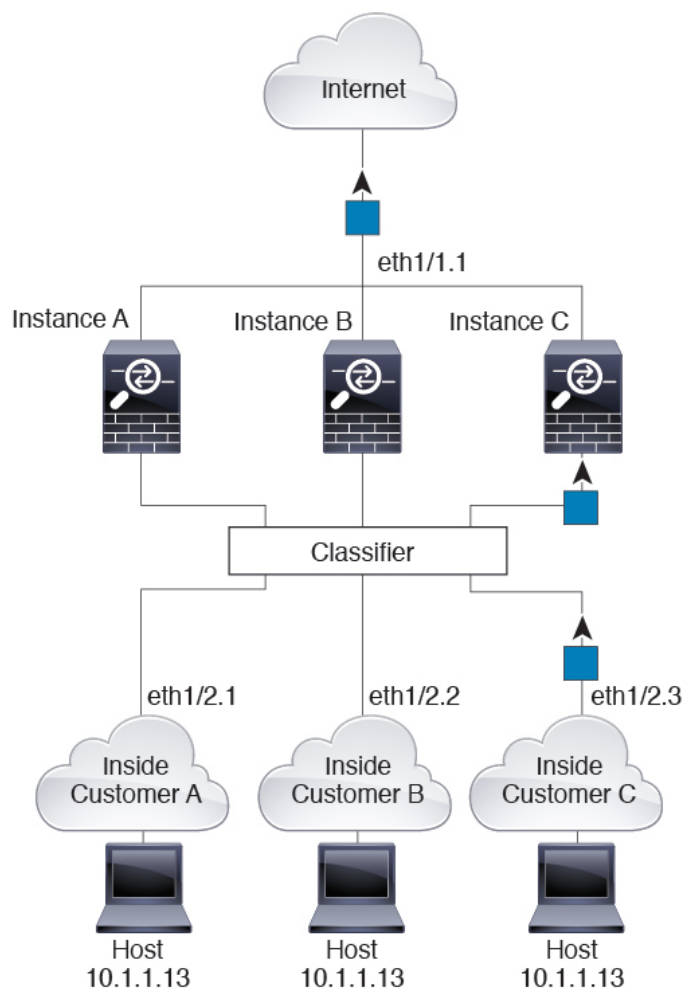
Figure 8: Packet Classification with a Shared Interface Using MAC Addresses



Incoming Traffic from Inside Networks

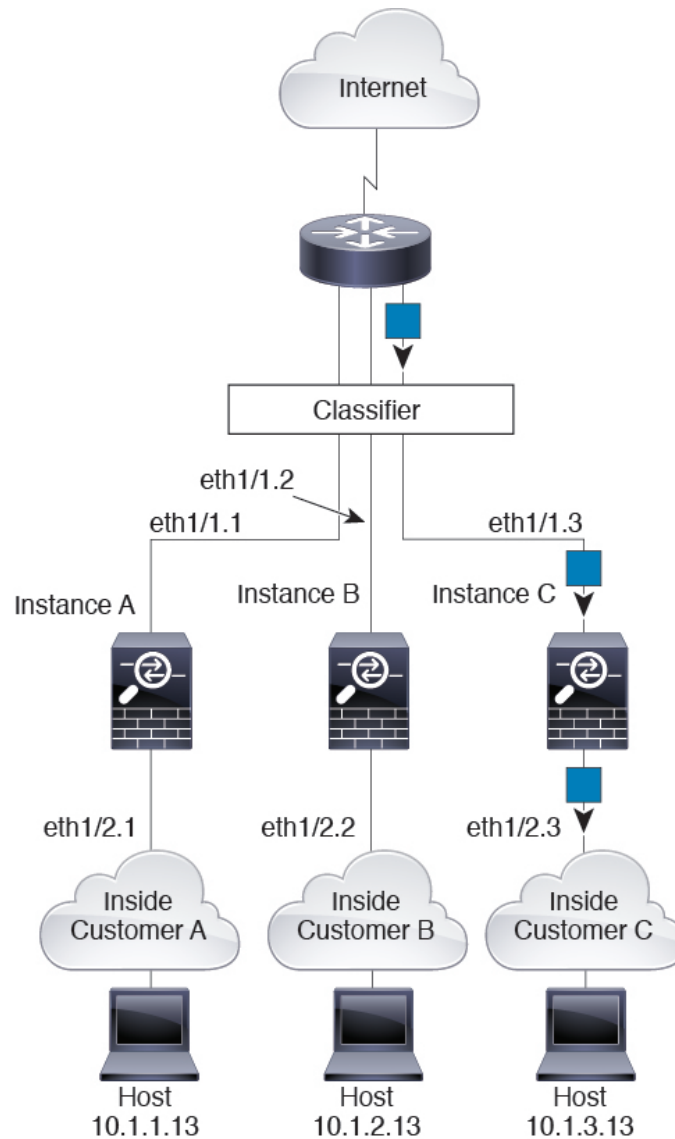
Note that all new incoming traffic must be classified, even from inside networks. The following figure shows a host on the Instance C inside network accessing the internet. The classifier assigns the packet to Instance C because the ingress interface is Ethernet 1/2.3, which is assigned to Instance C.

Figure 9: Incoming Traffic from Inside Networks



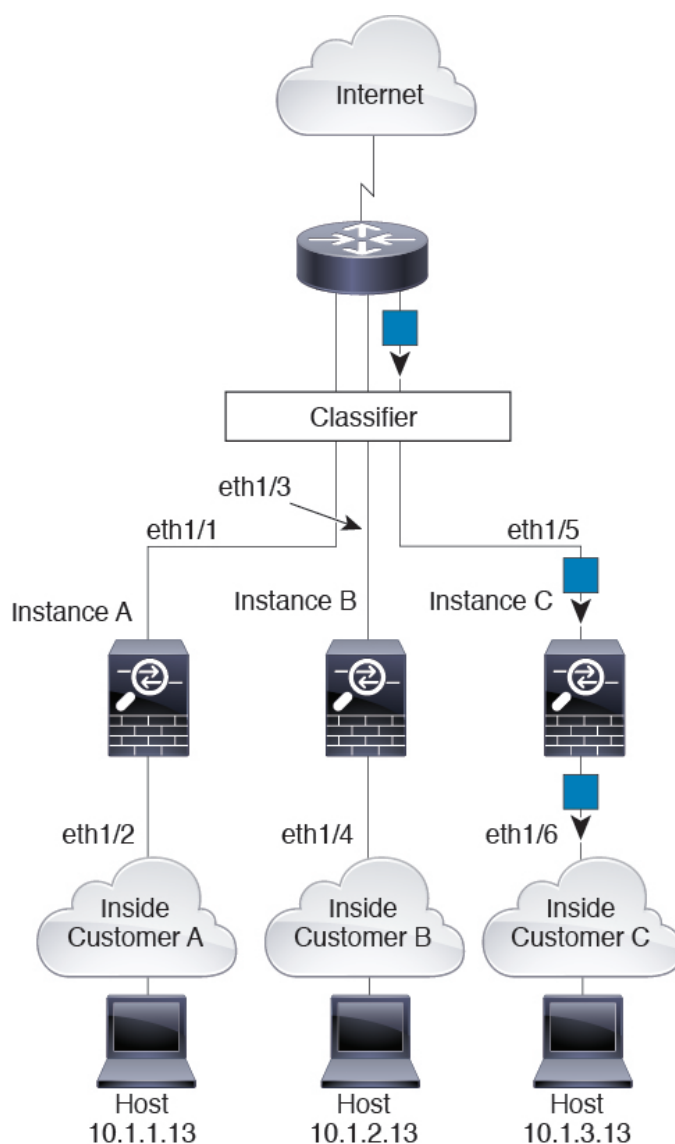
Transparent Firewall Instances

For transparent firewalls, you must use unique interfaces. The following figure shows a packet destined to a host on the Instance C inside network from the internet. The classifier assigns the packet to Instance C because the ingress interface is Ethernet 1/2.3, which is assigned to Instance C.

Figure 10: Transparent Firewall Instances**Inline Sets**

For inline sets, you must use unique interfaces and they must be physical interfaces or EtherChannels. The following figure shows a packet destined to a host on the Instance C inside network from the internet. The classifier assigns the packet to Instance C because the ingress interface is Ethernet 1/5, which is assigned to Instance C.

Figure 11: Inline Sets

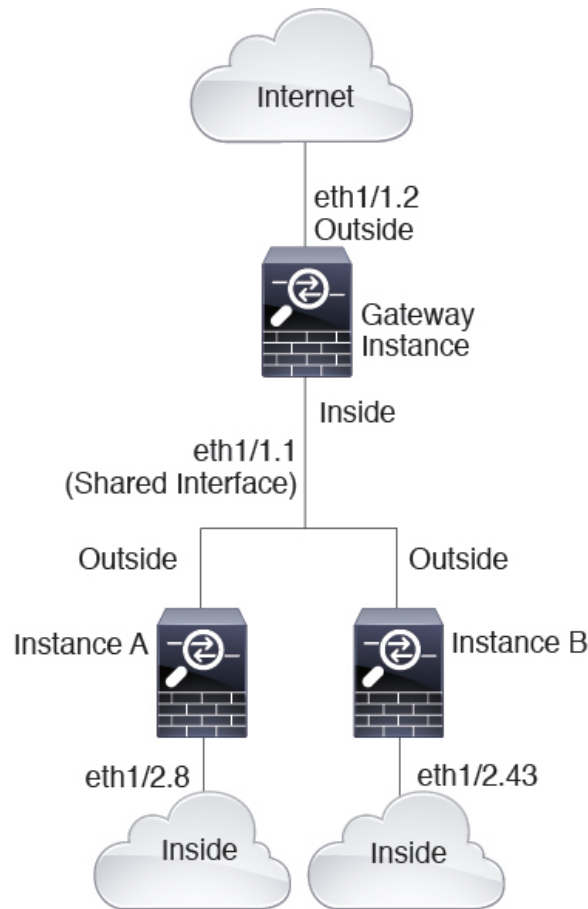


Cascading Container Instances

Placing an instance directly in front of another instance is called *cascading instances*; the outside interface of one instance is the same interface as the inside interface of another instance. You might want to cascade instances if you want to simplify the configuration of some instances by configuring shared parameters in the top instance.

The following figure shows a gateway instance with two instances behind the gateway.

Figure 12: Cascading Instances



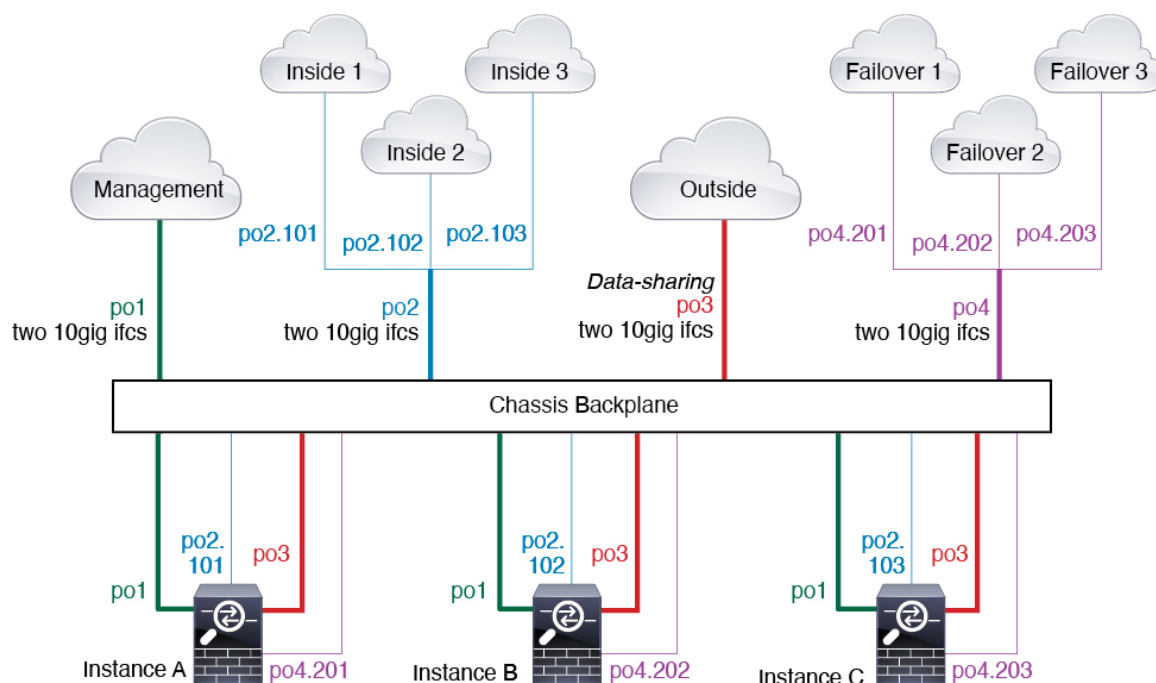
Note Do not use cascading instances (using a shared interface) with High Availability. After a failover occurs and the standby unit rejoins, MAC addresses can overlap temporarily and cause an outage. You should instead use unique interfaces for the gateway instance and inside instance using an external switch to pass traffic between the instances.

Typical Multi-Instance Deployment

The following example includes three container instances in routed firewall mode. They include the following interfaces:

- **Management**—All instances use the Port-Channel1 interface (management type). This EtherChannel includes two 10 Gigabit Ethernet interfaces. Within each application, the interface uses a unique IP address on the same management network.
- **Inside**—Each instance uses a subinterface on Port-Channel2 (data type). This EtherChannel includes two 10 Gigabit Ethernet interfaces. Each subinterface is on a separate network.

- Outside—All instances use the Port-Channel3 interface (data-sharing type). This EtherChannel includes two 10 Gigabit Ethernet interfaces. Within each application, the interface uses a unique IP address on the same outside network.
- Failover—Each instance uses a subinterface on Port-Channel4 (data type). This EtherChannel includes two 10 Gigabit Ethernet interfaces. Each subinterface is on a separate network.



Automatic MAC Addresses for Container Instance Interfaces

The chassis automatically generates MAC addresses for instance interfaces, and guarantees that a shared interface in each instance uses a unique MAC address.

If you manually assign a MAC address to a shared interface within the instance, then the manually-assigned MAC address is used. If you later remove the manual MAC address, the autogenerated address is used. In the rare circumstance that the generated MAC address conflicts with another private MAC address in your network, we suggest that you manually set the MAC address for the interface within the instance.

Because autogenerated addresses start with A2, you should not start manual MAC addresses with A2 due to the risk of overlapping addresses.



Note Even if you are not sharing a subinterface, if you manually configure MAC addresses, make sure you use unique MAC addresses for all subinterfaces on the same parent interface to ensure proper classification.

The chassis generates the MAC address using the following format:

A2xx.yyzz.zzzz

Where xx.yy is a user-defined prefix or a system-defined prefix, and zz.zzzz is an internal counter generated by the chassis. The system-defined prefix matches the lower 2 bytes of the first MAC address in the burned-in

MAC address pool that is programmed into the IDPROM. Use **connect fxos**, then **show module** to view the MAC address pool. For example, if the range of MAC addresses shown for module 1 is b0aa.772f.f0b0 to b0aa.772f.f0bf, then the system prefix will be f0b0.

The user-defined prefix is an integer that is converted into hexadecimal. For an example of how the user-defined prefix is used, if you set a prefix of 77, then the chassis converts 77 into the hexadecimal value 004D (yyxx). When used in the MAC address, the prefix is reversed (xxyy) to match the chassis native form:

A24D.00zz.zzzz

For a prefix of 1009 (03F1), the MAC address is:

A2F1.03zz.zzzz

Container Instance Resource Management

To specify resource usage per container instance, create one or more resource profiles in FXOS. When you deploy the logical device/application instance, you specify the resource profile that you want to use. The resource profile sets the number of CPU cores; RAM is dynamically allocated according to the number of cores, and disk space is set to 40 GB per instance. To view the available resources per model, see [Requirements and Prerequisites for Container Instances, on page 227](#). To add a resource profile, see [Add a Resource Profile for Container Instances, on page 167](#).

Performance Scaling Factor for Multi-Instance Capability

The maximum throughput (connections, VPN sessions, and TLS proxy sessions) for a platform is calculated for a native instance's use of memory and CPU (and this value is shown in **show resource usage**). If you use multiple instances, then you need to calculate the throughput based on the percentage of CPU cores that you assign to the instance. For example, if you use a container instance with 50% of the cores, then you should initially calculate 50% of the throughput. Moreover, the throughput available to a container instance may be less than that available to a native instance.

For detailed instructions on calculating the throughput for instances, see <https://www.cisco.com/c/en/us/products/collateral/security/firewalls/white-paper-c11-744750.html>.

Container Instances and High Availability

You can use High Availability using a container instance on 2 separate chassis; for example, if you have 2 chassis, each with 10 instances, you can create 10 High Availability pairs. Note that High Availability is not configured in FXOS; configure each High Availability pair in the application manager.

For detailed requirements, see [Requirements and Prerequisites for High Availability, on page 226](#) and [Add a High Availability Pair, on page 251](#).



Note Clustering is not supported.

Requirements and Prerequisites for Logical Devices

See the following sections for requirements and prerequisites.

Requirements and Prerequisites for Hardware and Software Combinations

The Firepower 4100/9300 supports multiple models, security modules, application types, and high availability and scalability features. See the following requirements for allowed combinations.

Firepower 9300 Requirements

The Firepower 9300 includes 3 security module slots and multiple types of security modules. See the following requirements:

- **Security Module Types**—You can install modules of different types in the Firepower 9300. For example, you can install the SM-48 as module 1, SM-40 as module 2, and SM-56 as module 3.
- **Native and Container instances**—When you install a container instance on a security module, that module can only support other container instances. A native instance uses all of the resources for a module, so you can only install a single native instance on a module. You can use native instances on some modules, and container instances on the other module. For example, you can install a native instance on module 1 and module 2, but container instances on module 3.
- **Clustering**—All security modules in the cluster, whether it is intra-chassis or inter-chassis, must be the same type. You can have different quantities of installed security modules in each chassis, although all modules present in the chassis must belong to the cluster including any empty slots. For example, you can install 2 SM-40s in chassis 1, and 3 SM-40s in chassis 2. You cannot use clustering if you install 1 SM-48 and 2 SM-40s in the same chassis.
- **High Availability**—High Availability is only supported between same-type modules on the Firepower 9300. However, the two chassis can include mixed modules. For example, each chassis has an SM-40, SM-48, and SM-56. You can create High Availability pairs between the SM-40 modules, between the SM-48 modules, and between the SM-56 modules.
- **ASA and FTD application types**—You can install different application types on separate modules in the chassis. For example, you can install ASA on module 1 and module 2, and FTD on module 3.
- **ASA or FTD versions**—You can run different versions of an application instance type on separate modules, or as separate container instances on the same module. For example, you can install the FTD 6.3 on module 1, FTD 6.4 on module 2, and FTD 6.5 on module 3.

Firepower 4100 Requirements

The Firepower 4100 comes in multiple models. See the following requirements:

- **Native and Container instances**—When you install a container instance on a Firepower 4100, that device can only support other container instances. A native instance uses all of the resources for a device, so you can only install a single native instance on the device.
- **Clustering**—All chassis in the cluster must be the same model.
- **High Availability**—High Availability is only supported between same-type models.
- **ASA and FTD application types**—The Firepower 4100 can only run a single application type.
- **The FTD container instance versions**—You can run different versions of Firepower Threat Defense as separate container instances on the same module.

Requirements and Prerequisites for Clustering

Cluster Model Support

- ASA on the Firepower 9300—Maximum 16 modules. For example, you can use 1 module in 16 chassis, or 2 modules in 8 chassis, or any combination that provides a maximum of 16 modules. Note that all modules in a chassis must belong to the cluster. Supported for intra-chassis, inter-chassis, and inter-site clustering.
- ASA on the Firepower 4100 series—Maximum 16 chassis. Supported for inter-chassis and inter-site clustering.
- FTD on the Firepower 9300—Maximum 6 modules. For example, you can use 2 modules in 3 chassis, or 3 modules in 2 chassis, or any combination that provides a maximum of 6 modules. Note that all modules in a chassis must belong to the cluster. Supported for intra-chassis and inter-chassis clustering.
- FTD on the Firepower 4100 series—Maximum 6 chassis. Supported for inter-chassis clustering.
- Radware DefensePro—Supported for intra-chassis clustering with the ASA.
- Radware DefensePro—Supported for intra-chassis clustering with the Firepower Threat Defense.

Clustering Hardware and Software Requirements

All chassis in a cluster:

- For the Firepower 4100: All chassis must be the same model. For the Firepower 9300: All security modules must be the same type. For example, if you use clustering, all modules in the Firepower 9300 must be SM-40s. You can have different quantities of installed security modules in each chassis, although all modules present in the chassis must belong to the cluster including any empty slots.
- Must run the identical FXOS and application software except at the time of an image upgrade. Mismatched software versions can lead to poor performance, so be sure to upgrade all nodes in the same maintenance window.
- Must include the same interface configuration for interfaces you assign to the cluster, such as the same Management interface, EtherChannels, active interfaces, speed and duplex, and so on. You can use different network module types on the chassis as long as the capacity matches for the same interface IDs and interfaces can successfully bundle in the same spanned EtherChannel. Note that all data interfaces must be EtherChannels in clusters with multiple chassis. If you change the interfaces in FXOS after you enable clustering (by adding or removing interface modules, or configuring EtherChannels, for example), then perform the same changes on each chassis, starting with the data nodes, and ending with the control node.
- Must use the same NTP server. For Firepower Threat Defense, the FMC must also use the same NTP server. Do not set the time manually.
- ASA: Each FXOS chassis must be registered with the License Authority or satellite server. There is no extra cost for data nodes. For permanent license reservation, you must purchase separate licenses for each chassis. For Firepower Threat Defense, all licensing is handled by the FMC.

Switch Requirements for Inter-Chassis Clustering

- Be sure to complete the switch configuration and successfully connect all the EtherChannels from the chassis to the switch(es) before you configure clustering on the Firepower 4100/9300 chassis.
- For supported switch characteristics, see [Cisco FXOS Compatibility](#).

Sizing the Data Center Interconnect for Inter-Site Clustering

You should reserve bandwidth on the data center interconnect (DCI) for cluster control link traffic equivalent to the following calculation:

$$\frac{\text{\# of cluster members per site}}{2} \times \text{cluster control link size per member}$$

If the number of members differs at each site, use the larger number for your calculation. The minimum bandwidth for the DCI should not be less than the size of the cluster control link for one member.

For example:

- For 4 members at 2 sites:
 - 4 cluster members total
 - 2 members at each site
 - 5 Gbps cluster control link per member

Reserved DCI bandwidth = 5 Gbps (2/2 x 5 Gbps).

- For 6 members at 3 sites, the size increases:
 - 6 cluster members total
 - 3 members at site 1, 2 members at site 2, and 1 member at site 3
 - 10 Gbps cluster control link per member

Reserved DCI bandwidth = 15 Gbps (3/2 x 10 Gbps).

- For 2 members at 2 sites:
 - 2 cluster members total
 - 1 member at each site
 - 10 Gbps cluster control link per member

Reserved DCI bandwidth = 10 Gbps (1/2 x 10 Gbps = 5 Gbps; but the minimum bandwidth should not be less than the size of the cluster control link (10 Gbps)).

Requirements and Prerequisites for High Availability

- The two units in a High Availability Failover configuration must:
 - Be on a separate chassis; intra-chassis High Availability for the Firepower 9300 is not supported.

- Be the same model.
- Have the same interfaces assigned to the High Availability logical devices.
- Have the same number and types of interfaces. All interfaces must be preconfigured in FXOS identically before you enable High Availability.
- High Availability is only supported between same-type modules on the Firepower 9300; but the two chassis can include mixed modules. For example, each chassis has an SM-56, SM-48, and SM-40. You can create High Availability pairs between the SM-56 modules, between the SM-48 modules, and between the SM-40 modules.
- For container instances, each unit must use the same resource profile attributes.
- For container instances: Do not use cascading instances (using a shared interface) with High Availability. After a failover occurs and the standby unit rejoins, MAC addresses can overlap temporarily and cause an outage. You should instead use unique interfaces for the gateway instance and inside instance using an external switch to pass traffic between the instances.
- For other High Availability system requirements, see the application configuration guide chapter for High Availability.

Requirements and Prerequisites for Container Instances

For information about high-availability or clustering requirements with multi-instance, see [Requirements and Prerequisites for High Availability, on page 226](#) and see [Requirements and Prerequisites for Clustering, on page 225](#).

Supported Application Types

- The FTD

Maximum Container Instances and Resources per Model

For each container instance, you can specify the number of CPU cores to assign to the instance. RAM is dynamically allocated according to the number of cores, and disk space is set to 40 GB per instance.

Table 13: Maximum Container Instances and Resources per Model

Model	Max. Container Instances	Available CPU Cores	Available RAM	Available Disk Space
Firepower 4110	3	22	53 GB	125.6 GB
Firepower 4115	7	46	162 GB	308 GB
Firepower 4120	3	46	101 GB	125.6 GB
Firepower 4125	10	62	162 GB	644 GB
Firepower 4140	7	70	222 GB	311.8 GB
Firepower 4145	14	86	344 GB	608 GB

Model	Max. Container Instances	Available CPU Cores	Available RAM	Available Disk Space
Firepower 4150	7	86	222 GB	311.8 GB
Firepower 9300 SM-24 security module	7	46	226 GB	656.4 GB
Firepower 9300 SM-36 security module	11	70	222 GB	640.4 GB
Firepower 9300 SM-40 security module	13	78	334 GB	1359 GB
Firepower 9300 SM-44 security module	14	86	218 GB	628.4 GB
Firepower 9300 SM-48 security module	15	94	334 GB	1341 GB
Firepower 9300 SM-56 security module	18	110	334 GB	1314 GB

FMC Requirements

For all instances on a Firepower 4100 chassis or Firepower 9300 module, you must use the same FMC due to the licensing implementation.

Guidelines and Limitations for Logical Devices

See the following sections for guidelines and limitations.

General Guidelines and Limitations

Firewall Mode

You can set the firewall mode to routed or transparent in the bootstrap configuration for the Firepower Threat Defense and ASA.

High Availability

- Configure high availability within the application configuration.
- You can use any data interfaces as the failover and state links. Data-sharing interfaces are not supported.

Multi-Instance and Context Mode

- Multiple context mode is only supported on the ASA.
- Enable multiple context mode in the ASA after you deploy.

- Multi-instance capability with container instances is only available for the Firepower Threat Defense.
- For Firepower Threat Defense container instances, a single FMC must manage all instances on a security module/engine.
- You can enable TLS crypto acceleration on one container instance.
- For Firepower Threat Defense container instances, the following features are not supported:
 - Clustering
 - Radware DefensePro link decorator
 - FTD configuration backup and restore using the FMC
 - FMC UCAPL/CC mode
 - Flow offload to hardware

Clustering Guidelines and Limitations

Switches for Clustering

- Make sure connected switches match the MTU for both cluster data interfaces and the cluster control link interface. You should configure the cluster control link interface MTU to be at least 100 bytes higher than the data interface MTU, so make sure to configure the cluster control link connecting switch appropriately. Because the cluster control link traffic includes data packet forwarding, the cluster control link needs to accommodate the entire size of a data packet plus cluster traffic overhead. In addition, we do not recommend setting the cluster control link MTU between 2561 and 8362; due to block pool handling, this MTU size is not optimal for system operation.
- For Cisco IOS XR systems, if you want to set a non-default MTU, set the IOS XR interface MTU to be 14 bytes higher than the cluster device MTU. Otherwise, OSPF adjacency peering attempts may fail unless the **mtu-ignore** option is used. Note that the cluster device MTU should match the IOS XR *IPv4* MTU. This adjustment is not required for Cisco Catalyst and Cisco Nexus switches.
- On the switch(es) for the cluster control link interfaces, you can optionally enable Spanning Tree PortFast on the switch ports connected to the cluster unit to speed up the join process for new units.
- On the switch, we recommend that you use one of the following EtherChannel load-balancing algorithms: **source-dest-ip** or **src-dst-mixed-ip-port** (see the Cisco Nexus OS and Cisco IOS-XE **port-channel load-balance** command). Do not use a **vlan** keyword in the load-balance algorithm because it can cause unevenly distributed traffic to the devices in a cluster.
- If you change the load-balancing algorithm of the EtherChannel on the switch, the EtherChannel interface on the switch temporarily stops forwarding traffic, and the Spanning Tree Protocol restarts. There will be a delay before traffic starts flowing again.
- Switches on the cluster control link path should not verify the L4 checksum. Redirected traffic over the cluster control link does not have a correct L4 checksum. Switches that verify the L4 checksum could cause traffic to be dropped.
- Port-channel bundling downtime should not exceed the configured keepalive interval.

- On Supervisor 2T EtherChannels, the default hash distribution algorithm is adaptive. To avoid asymmetric traffic in a VSS design, change the hash algorithm on the port-channel connected to the cluster device to fixed:

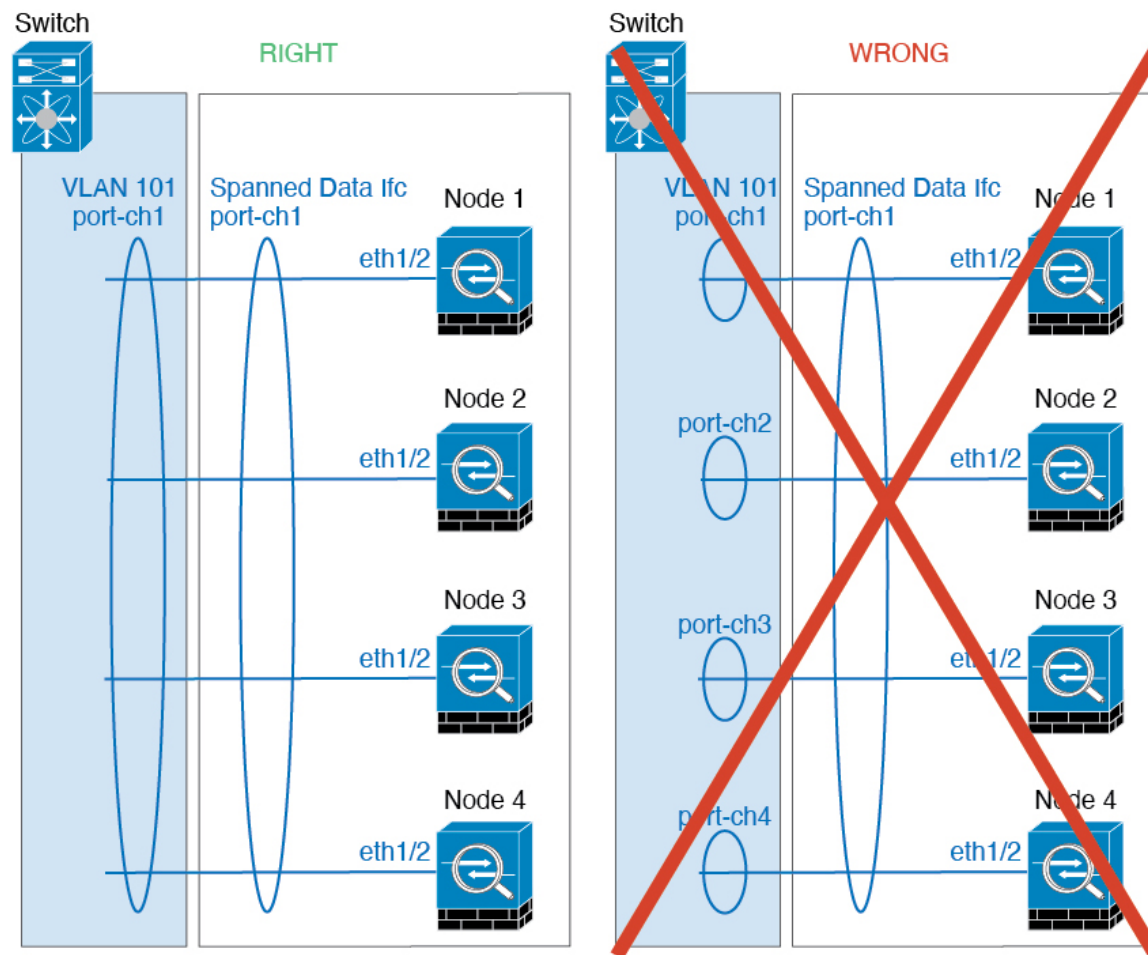
```
router(config)# port-channel id hash-distribution fixed
```

Do not change the algorithm globally; you may want to take advantage of the adaptive algorithm for the VSS peer link.

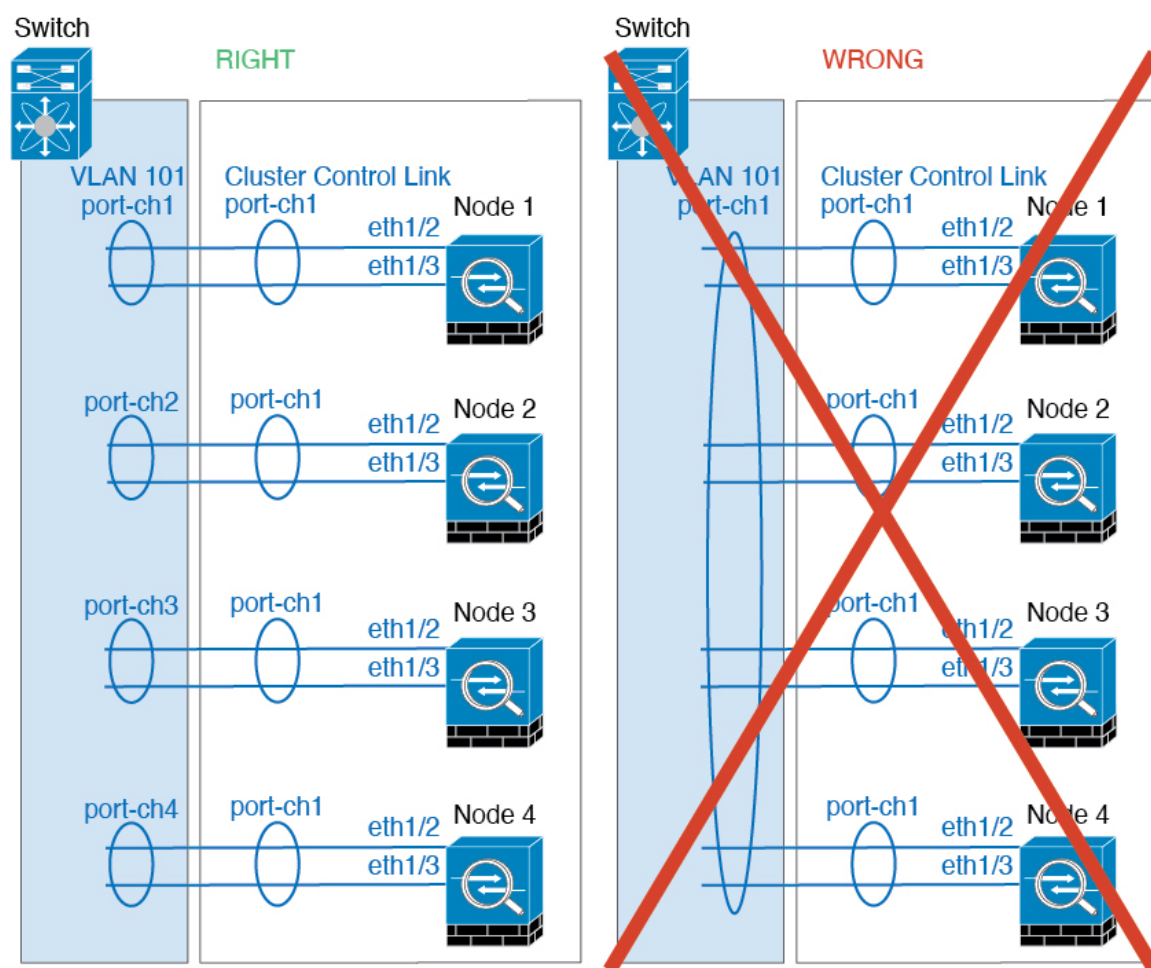
- Firepower 4100/9300 clusters support LACP graceful convergence. So you can leave LACP graceful convergence enabled on connected Cisco Nexus switches.
- When you see slow bundling of a Spanned EtherChannel on the switch, you can enable LACP rate fast for an individual interface on the switch. FXOS EtherChannels have the LACP rate set to fast by default. Note that some switches, such as the Nexus series, do not support LACP rate fast when performing in-service software upgrades (ISSUs), so we do not recommend using ISSUs with clustering.

EtherChannels for Clustering

- In Catalyst 3750-X Cisco IOS software versions earlier than 15.1(1)S2, the cluster unit did not support connecting an EtherChannel to a switch stack. With default switch settings, if the cluster unit EtherChannel is connected cross stack, and if the control unit switch is powered down, then the EtherChannel connected to the remaining switch will not come up. To improve compatibility, set the **stack-mac persistent timer** command to a large enough value to account for reload time; for example, 8 minutes or 0 for indefinite. Or, you can upgrade to more a more stable switch software version, such as 15.1(1)S2.
- Spanned vs. Device-Local EtherChannel Configuration—Be sure to configure the switch appropriately for Spanned EtherChannels vs. Device-local EtherChannels.
 - Spanned EtherChannels—For cluster unit *Spanned* EtherChannels, which span across all members of the cluster, the interfaces are combined into a single EtherChannel on the switch. Make sure each interface is in the same channel group on the switch.



- **Device-local EtherChannels**—For cluster unit *Device-local* EtherChannels including any EtherChannels configured for the cluster control link, be sure to configure discrete EtherChannels on the switch; do not combine multiple cluster unit EtherChannels into one EtherChannel on the switch.



Inter-Site Clustering

See the following guidelines for inter-site clustering:

- The cluster control link latency must be less than 20 ms round-trip time (RTT).
- The cluster control link must be reliable, with no out-of-order or dropped packets; for example, you should use a dedicated link.
- Do not configure connection rebalancing; you do not want connections rebalanced to cluster members at a different site.
- The does not encrypt forwarded data traffic on the cluster control link because it is a dedicated link, even when used on a Data Center Interconnect (DCI). If you use Overlay Transport Virtualization (OTV), or are otherwise extending the cluster control link outside of the local administrative domain, you can configure encryption on your border routers such as 802.1AE MacSec over OTV.
- The cluster implementation does not differentiate between members at multiple sites for incoming connections; therefore, connection roles for a given connection may span across sites. This is expected behavior. However, if you enable director localization, the local director role is always chosen from the same site as the connection owner (according to site ID). Also, the local director chooses a new owner

at the same site if the original owner fails (Note: if the traffic is asymmetric across sites, and there is continuous traffic from the remote site after the original owner fails, then a node from the remote site might become the new owner if it receives a data packet within the re-hosting window.).

- For director localization, the following traffic types do not support localization: NAT or PAT traffic; SCTP-inspected traffic; Fragmentation owner query.
- For UDP long-lived flows in a North-South deployment, routing loops can occur if nodes at the original flow owner site fail and then come back up, after which the flow is directed back to the original site. If the new owner at the other site doesn't have a route to the destination, it will route the flow back to the internet, causing a loop. In this case, use the **clear conn** command on the new owner to force the flow to be reestablished.
- For transparent mode, if the cluster is placed between a pair of inside and outside routers (AKA North-South insertion), you must ensure that both inside routers share a MAC address, and also that both outside routers share a MAC address. When a cluster member at site 1 forwards a connection to a member at site 2, the destination MAC address is preserved. The packet will only reach the router at site 2 if the MAC address is the same as the router at site 1.
- For transparent mode, if the cluster is placed between data networks and the gateway router at each site for firewalling between internal networks (AKA East-West insertion), then each gateway router should use a First Hop Redundancy Protocol (FHRP) such as HSRP to provide identical virtual IP and MAC address destinations at each site. The data VLANs are extended across the sites using Overlay Transport Virtualization (OTV), or something similar. You need to create filters to prevent traffic that is destined to the local gateway router from being sent over the DCI to the other site. If the gateway router becomes unreachable at one site, you need to remove any filters so traffic can successfully reach the other site's gateway.
- For transparent mode, if the cluster is connected to an HSRP router, you must add the router HSRP MAC address as a static MAC address table entry on the . When adjacent routers use HSRP, traffic destined to the HSRP IP address will be sent to the HSRP MAC Address, but return traffic will be sourced from the MAC address of a particular router's interface in the HSRP pair. Therefore, the MAC address table is typically only updated when the ARP table entry for the HSRP IP address expires, and the sends an ARP request and receives a reply. Because the 's ARP table entries expire after 14400 seconds by default, but the MAC address table entry expires after 300 seconds by default, a static MAC address entry is required to avoid MAC address table expiration traffic drops.
- For routed mode using Spanned EtherChannel, configure site-specific MAC addresses. Extend the data VLANs across the sites using OTV, or something similar. You need to create filters to prevent traffic that is destined to the global MAC address from being sent over the DCI to the other site. If the cluster becomes unreachable at one site, you need to remove any filters so traffic can successfully reach the other site's cluster nodes. Dynamic routing is not supported when an inter-site cluster acts as the first hop router for an extended segment.

Additional Guidelines

- When adding a unit to an existing cluster, or when reloading a unit, there will be a temporary, limited packet/connection drop; this is expected behavior. In some cases, the dropped packets can hang connections; for example, dropping a FIN/ACK packet for an FTP connection will make the FTP client hang. In this case, you need to reestablish the FTP connection.
- If you use a Windows 2003 server connected to a Spanned EtherChannel interface, when the syslog server port is down, and the server does not throttle ICMP error messages, then large numbers of ICMP

messages are sent back to the cluster. These messages can result in some units of the cluster experiencing high CPU, which can affect performance. We recommend that you throttle ICMP error messages.

- We recommend connecting EtherChannels to a VSS, vPC, StackWise, or StackWise Virtual for redundancy.
- Within a chassis, you cannot cluster some security modules and run other security modules in standalone mode; you must include all security modules in the cluster.
- For decrypted TLS/SSL connections, the decryption states are not synchronized, and if the connection owner fails, then decrypted connections will be reset. New connections will need to be established to a new unit. Connections that are not decrypted (they match a do-not-decrypt rule) are not affected and are replicated correctly.

Defaults

- The cluster health check feature is enabled by default with the holdtime of 3 seconds. Interface health monitoring is enabled on all interfaces by default.
- The cluster auto-rejoin feature for a failed cluster control link is set to unlimited attempts every 5 minutes.
- The cluster auto-rejoin feature for a failed data interface is set to 3 attempts every 5 minutes, with the increasing interval set to 2.
- Connection replication delay of 5 seconds is enabled by default for HTTP traffic.

Add a Standalone Logical Device

Standalone logical devices can be used alone or as high availability units. For more information about high availability usage, see [Add a High Availability Pair, on page 251](#).

Add a Standalone ASA

Standalone logical devices work either alone or in a High Availability pair. On the Firepower 9300 with multiple security modules, you can deploy either a cluster or standalone devices. The cluster must use all modules, so you cannot mix and match a 2-module cluster plus a single standalone device, for example.

You can deploy a routed or transparent firewall mode ASA from the Firepower 4100/9300 chassis.

For multiple context mode, you must first deploy the logical device, and then enable multiple context mode in the ASA application.

Before you begin

- Download the application image you want to use for the logical device from Cisco.com, and then download that image to the Firepower 4100/9300 chassis.



Note For the Firepower 9300, you can install different application types (ASA and FTD) on separate modules in the chassis. You can also run different versions of an application instance type on separate modules.

- Configure a management interface to use with the logical device. The management interface is required. Note that this management interface is not the same as the chassis management port that is used only for chassis management (in FXOS, you might see it displayed as MGMT, management0, or other similar names).
- Gather the following information:
 - Interface IDs for this device
 - Management interface IP address and network mask
 - Gateway IP address

Procedure

Step 1 Enter security services mode.

scope ssa

Example:

```
Firepower# scope ssa
Firepower /ssa #
```

Step 2 Set the application instance image version.

a) View available images. Note the Version number that you want to use.

show app

Example:

```
Firepower /ssa # show app
```

Name	Version	Author	Supported Deploy Types	CSP Type	Is Default
asa	9.9.1	cisco	Native	Application	No
asa	9.10.1	cisco	Native	Application	Yes
ftd	6.2.3	cisco	Native	Application	Yes
ftd	6.3.0	cisco	Native, Container	Application	Yes

b) Set the scope to the security module/engine slot.

scope slot *slot_id*

The *slot_id* is always 1 for the Firepower 4100, and 1, 2, or 3 for the Firepower 9300.

Example:

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot #
```

c) Create the application instance.

enter app-instance *asa device_name*

The *device_name* can be between 1 and 64 characters. You will use this device name when you create the logical device for this instance.

Example:

```
Firepower /ssa/slot # enter app-instance asa ASA1
Firepower /ssa/slot/app-instance* #
```

- d) Set the ASA image version.

set startup-version *version*

Example:

```
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
```

- e) Exit to slot mode.

exit

Example:

```
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* #
```

- f) Exit to ssa mode.

exit

Example:

```
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

Example:

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa ASA1
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

Step 3 Create the logical device.

enter logical-device *device_name* **asa** *slot_id* **standalone**

Use the same *device_name* as the application instance you added earlier.

Example:

```
Firepower /ssa # enter logical-device ASA1 asa 1 standalone
Firepower /ssa/logical-device* #
```

Step 4 Assign the management and data interfaces to the logical device. Repeat for each interface.

create external-port-link *name interface_id asa*

set description *description*

exit

- *name*—The name is used by the Firepower 4100/9300 chassis supervisor; it is not the interface name used in the ASA configuration.
- *description*—Use quotes (") around phrases with spaces.

The management interface is not the same as the chassis management port. You will later enable and configure the data interfaces on the ASA, including setting the IP addresses.

Example:

```
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
```

Step 5 Configure the management bootstrap information.

- a) Create the bootstrap object.

create mgmt-bootstrap *asa*

Example:

```
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- b) Specify the firewall mode, routed or transparent.

create bootstrap-key **FIREWALL_MODE**

set value {**routed** | **transparent**}

exit

In routed mode, the device is considered to be a router hop in the network. Each interface that you want to route between is on a different subnet. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices.

The firewall mode is only set at initial deployment. If you re-apply the bootstrap settings, this setting is not used.

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
```

```
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- c) Specify the admin and enable password.

create bootstrap-key-secret PASSWORD

set value

Enter a value: *password*

Confirm the value: *password*

exit

Example:

The pre-configured ASA admin user and enable password is useful for password recovery; if you have FXOS access, you can reset the admin user password if you forget it.

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- d) Configure the IPv4 management interface settings.

create ipv4 slot_id default

set ip ip_address mask network_mask

set gateway gateway_address

exit

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.34 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- e) Configure the IPv6 management interface settings.

create ipv6 slot_id default

set ip ip_address prefix-length prefix

set gateway gateway_address

exit

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
```

```
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

f) Exit the management bootstrap mode.

exit

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

Step 6 Save the configuration.

commit-buffer

The chassis deploys the logical device by downloading the specified software version and pushing the bootstrap configuration and management interface settings to the application instance. Check the status of the deployment using the **show app-instance** command. The application instance is running and ready to use when the **Admin State is Enabled** and the **Oper State is Online**.

Example:

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
```

App Name	Identifier	Slot ID	Admin State	Oper State	Running Version	Startup Version
Deploy Type	Profile Name	Cluster	State	Cluster Role		
asa	asa1	2	Disabled	Not Installed		9.12.1
Native			Not Applicable	None		
ftd	ftd1	1	Enabled	Online	6.4.0.49	6.4.0.49
Container	Default-Small		Not Applicable	None		

Step 7 See the ASA configuration guide to start configuring your security policy.

Example

```
Firepower# scope ssa
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa MyDevice1
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* # create logical-device MyDevice1 asa 1 standalone
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
```

```

Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value transparent
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: secretglassine
Confirm the value: secretglassine
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # commit-buffer
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key #

```

Add a Standalone FTD

Standalone logical devices work either alone or in a High Availability pair. On the Firepower 9300 with multiple security modules, you can deploy either a cluster or standalone devices. The cluster must use all modules, so you cannot mix and match a 2-module cluster plus a single standalone device, for example.

You can use native instances on some modules, and container instances on the other module(s).

Before you begin

- Download the application image you want to use for the logical device from Cisco.com, and then download that image to the Firepower 4100/9300 chassis.



Note For the Firepower 9300, you can install different application types (ASA and FTD) on separate modules in the chassis. You can also run different versions of an application instance type on separate modules.

- Configure a management interface to use with the logical device. The management interface is required. Note that this management interface is not the same as the chassis management port that is used only for chassis management (in FXOS, you might see it displayed as MGMT, management0, or other similar names).
- You must also configure at least one Data type interface. Optionally, you can also create a firepower-eventing interface to carry all event traffic (such as web events). See [Interface Types, on page 178](#) for more information.
- For container instances, if you do not want to use the default profile, add a resource profile according to [Add a Resource Profile for Container Instances, on page 167](#).
- For container instances, before you can install a container instance for the first time, you must reinitialize the security module/engine so that the disk has the correct formatting. An existing logical device will be deleted and then reinstalled as a new device, losing any local application configuration. If you are replacing a native instance with container instances, you will need to delete the native instance in any case. You cannot automatically migrate a native instance to a container instance. See [Reinitializing a Security Module/Engine, on page 316](#) for more information.
- Gather the following information:

- Interface IDs for this device
- Management interface IP address and network mask
- Gateway IP address
- FMC IP address and/or NAT ID of your choosing
- DNS server IP address
- Firepower Threat Defense hostname and domain name

Procedure

Step 1 Enter security services mode.

scope ssa

Example:

```
Firepower# scope ssa
Firepower /ssa #
```

Step 2 Accept the end-user license agreement for the Firepower Threat Defense version you want to use. You only need to perform this step if you have not already accepted the EULA for this version.

a) View available images. Note the Version number that you want to use.

show app

Example:

```
Firepower /ssa # show app
```

Name	Version	Author	Supported Deploy Types	CSP Type	Is Default
App					
asa	9.9.1	cisco	Native	Application	No
asa	9.10.1	cisco	Native	Application	Yes
ftd	6.2.3	cisco	Native	Application	Yes
ftd	6.3.0	cisco	Native,Container	Application	Yes

b) Set the scope to the image version.

scope app ftd *application_version*

Example:

```
Firepower /ssa # scope app ftd 6.2.3
Firepower /ssa/app #
```

c) Accept the license agreement.

accept-license-agreement

Example:

```
Firepower /ssa/app # accept-license-agreement
```

```
End User License Agreement: End User License Agreement
```

```
Effective: May 22, 2017
```

This is an agreement between You and Cisco Systems, Inc. or its affiliates ("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the individual or legal entity licensing the Software under this EULA. "Use" or "Using" means to download, install, activate, access or otherwise use the Software. "Software" means the Cisco computer programs and any Upgrades made available to You by an Approved Source and licensed to You by Cisco. "Documentation" is the Cisco user or technical manuals, training materials, specifications or other documentation applicable to the Software and made available to You by an Approved Source. "Approved Source" means (i) Cisco or (ii) the Cisco authorized reseller, distributor or systems integrator from whom you acquired the Software. "Entitlement" means the license detail; including license metric, duration, and quantity provided in a product ID (PID) published on Cisco's price list, claim certificate or right to use notification. "Upgrades" means all updates, upgrades, bug fixes, error corrections, enhancements and other modifications to the Software and backup copies thereof.

```
[...]
```

Please "commit-buffer" if you accept the license agreement, otherwise "discard-buffer".

```
Firepower /ssa/app* #
```

- d) Save the configuration.

commit-buffer

Example:

```
Firepower /ssa/app* # commit-buffer
Firepower /ssa/app #
```

- e) Exit to security services mode.

exit

Example:

```
Firepower /ssa/app # exit
Firepower /ssa #
```

Step 3 Set the application instance parameters, including the image version.

- a) For container instances, view available resource profiles. To add a profile, see [Add a Resource Profile for Container Instances, on page 167](#).

show resource-profile

Note the profile name you want to use.

Example:

```
Firepower /ssa # show resource-profile
```

Profile Name	App Name	App Version	Is In Use	Security Model	CPU Logical Core
Count RAM Size (MB)	Default Profile	Profile Type	Description		

bronze	N/A	N/A	No	all
6	N/A	No	Custom	low end device
silver 1	N/A	N/A	No	all
8	N/A	No	Custom	mid-level

- b) Set the scope to the security module/engine slot.

scope slot *slot_id*

The *slot_id* is always 1 for the Firepower 4100, and 1, 2, or 3 for the Firepower 9300.

Example:

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot #
```

- c) Create the application instance.

enter app-instance ftd *device_name*

The *device_name* can be between 1 and 64 characters. You will use this device name when you create the logical device for this instance.

Example:

```
Firepower /ssa/slot # enter app-instance ftd FTD1
Firepower /ssa/slot/app-instance* #
```

- d) For a container instance, set the application instance type to container.

set deploy-type container

A container instance uses a subset of resources of the security module/engine, so you can install multiple container instances. A native instance uses all of the resources (CPU, RAM, and disk space) of the security module/engine, so you can only install one native instance.

You cannot change the instance type after you save the configuration. The default type is **native**.

Example:

```
Firepower /ssa/slot/app-instance* # set deploy-type container
```

- e) For a container instance, set the resource profile.

set resource-profile-name *name*

This profile name must already exist.

If you later assign a different resource profile, then the instance will reload, which can take approximately 5 minutes. Note that for established High Availability pairs, if you assign a different-sized resource profile, be sure to make all members the same size as soon as possible.

Example:

```
Firepower /ssa/slot/app-instance* # set resource-profile-name bronze
```

- f) Set the Firepower Threat Defense image version.

set startup-version *version*

Enter the version number that you noted earlier in this procedure when you accepted the EULA.

Example:

```
Firepower /ssa/slot/app-instance* # set startup-version 6.3.0
```

- g) Exit to slot mode.

exit

Example:

```
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* #
```

- h) (Optional) Create the Radware DefensePro instance for the Firepower 4110 or 4120, which require you to create the application instance before you create the logical device (Radware DefensePro is not supported with container instances).

enter app-instance vdp *device_name*

exit

Set the *device_name* to match the Firepower Threat Defense application instance. After you complete the logical device configuration, you must continue configuring the Radware DefensePro decorator in a service chain with the Firepower Threat Defense logical device. See [Configure Radware DefensePro on a Standalone Logical Device, on page 280](#), starting with step 4.

Example:

```
Firepower /ssa/slot* # enter app-instance vdp FTD1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* #
```

- i) Exit to ssa mode.

exit

Example:

```
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

Example:

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd MyDevice1
Firepower /ssa/slot/app-instance* # set deploy-type container
Firepower /ssa/slot/app-instance* # set resource-profile-name silver 1
Firepower /ssa/slot/app-instance* # set startup-version 6.3.0
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
```

```
Firepower /ssa* #
```

Step 4 Create the logical device.

enter logical-device *device_name* **ftd** *slot_id* **standalone**

Use the same *device_name* as the application instance you added earlier.

Example:

```
Firepower /ssa # enter logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* #
```

Step 5 Assign the management and data interfaces to the logical device. Repeat for each interface.

create external-port-link *name* *interface_id* **ftd**

set description *description*

exit

- *name*—The name is used by the Firepower 4100/9300 chassis supervisor; it is not the interface name used in the Firepower Threat Defense configuration.
- *description*—Use quotes (") around phrases with spaces.

The management interface is not the same as the chassis management port. You will later enable and configure the data interfaces in FMC, including setting the IP addresses.

You can only assign up to 10 data-sharing interfaces to a container instance. Also, each data-sharing interface can be assigned to at most 14 container instances.

Example:

```
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 ftd
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 ftd
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 ftd
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
```

Step 6 Configure the management bootstrap parameters.

These settings are meant for initial deployment only, or for disaster recovery. For normal operation, you can later change most values in the application CLI configuration.

a) Create the bootstrap object.

create mgmt-bootstrap **ftd**

Example:

```
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- b) Specify the IP address or hostname or NAT ID of the managing FMC:

Set one of the following:

- **enter bootstrap-key FIREPOWER_MANAGER_IP**
set value *IP_address*
exit
- **enter bootstrap-key FQDN**
set value *fmc_hostname*
exit
- **enter bootstrap-key NAT_ID**
set value *nat_id*
exit

Normally, you need both IP addresses (along with a registration key) for both routing purposes and for authentication: the FMC specifies the device IP address, and the device specifies the FMC IP address. However, if you only know one of the IP addresses, which is the minimum requirement for routing purposes, then you must also specify a unique NAT ID on both sides of the connection to establish trust for the initial communication and to look up the correct registration key. You can specify any text string as the NAT ID, from 1 to 37 characters. The FMC and device use the registration key and NAT ID (instead of IP addresses) to authenticate and authorize for initial registration.

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREPOWER_MANAGER_IP
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.10.10.7
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- c) Specify the firewall mode, routed or transparent.

create bootstrap-key FIREWALL_MODE

set value {**routed** | **transparent**}

exit

In routed mode, the device is considered to be a router hop in the network. Each interface that you want to route between is on a different subnet. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices.

The firewall mode is only set at initial deployment. If you re-apply the bootstrap settings, this setting is not used.

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- d) Specify the key to be shared between the device and the FMC. You can choose any passphrase for this key between 1 and 37 characters; you will enter the same key on the FMC when you add the Firepower Threat Defense.

create bootstrap-key-secret REGISTRATION_KEY

set value

Enter a value: *registration_key*

Confirm the value: *registration_key*

exit

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret
REGISTRATION_KEY
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: gratuitousapples
Confirm the value: gratuitousapples
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- e) Specify the admin password. This password is used for the admin user for CLI access.

create bootstrap-key-secret PASSWORD

set value

Enter a value: *password*

Confirm the value: *password*

exit

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- f) Specify the fully qualified hostname.

create bootstrap-key FQDN

set value fqdn

exit

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FQDN
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value ftdl.cisco.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- g) Specify a comma-separated list of DNS servers.

create bootstrap-key DNS_SERVERS**set value** *dns_servers***exit**

The Firepower Threat Defense uses DNS if you specify a hostname for the FMC, for example.

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.9.8.7,10.9.6.5
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- h) Specify a comma-separated list of search domains.

create bootstrap-key SEARCH_DOMAINS**set value** *search_domains***exit****Example:**

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
cisco.com,example.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- i) (Optional) For a container instance, permit Expert Mode from Firepower Threat Defense SSH sessions. Expert Mode provides Firepower Threat Defense shell access for advanced troubleshooting.

create bootstrap-key PERMIT_EXPERT_MODE**set value** {yes | no}**exit**

- **yes**—Users who access this container instance directly from an SSH session can enter Expert Mode.
- **no**—Only users who access the container instance from the FXOS CLI can enter Expert Mode.

By default for container instances, Expert Mode is only available to users who access the Firepower Threat Defense CLI from the FXOS CLI. This limitation is only applied to container instances to increase isolation between instances. Use Expert Mode only if a documented procedure tells you it is required, or if the Cisco Technical Assistance Center asks you to use it. To enter this mode, use the **expert** command in the Firepower Threat Defense CLI.

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key PERMIT_EXPERT_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value yes
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- j) Configure the IPv4 management interface settings.

create ipv4 slot_id firepower


```
set ip ip_address mask network_mask
```

```
set gateway gateway_address
```

```
exit
```

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.34 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- k) Configure the IPv6 management interface settings.

```
create ipv6 slot_id firepower
```

```
set ip ip_address prefix-length prefix
```

```
set gateway gateway_address
```

```
exit
```

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- l) Exit the management bootstrap mode.

```
exit
```

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

Step 7 Save the configuration.

commit-buffer

The chassis deploys the logical device by downloading the specified software version and pushing the bootstrap configuration and management interface settings to the application instance. Check the status of the deployment using the **show app-instance** command. The application instance is running and ready to use when the **Admin State is Enabled** and the **Oper State is Online**.

Example:

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
```

App Name	Identifier	Slot ID	Admin State	Oper State	Running Version	Startup Version
Deploy Type	Profile Name	Cluster State	Cluster Role			

asa	asal	2	Disabled	Not Installed		9.12.1
	Native		Not Applicable	None		
ftd	ftdl	1	Enabled	Online	6.4.0.49	6.4.0.49
	Container	Default-Small	Not Applicable	None		

Step 8 See the FMC configuration guide to add the Firepower Threat Defense as a managed device and start configuring your security policy.

Example

```
Firepower# scope ssa
Firepower /ssa* # scope app ftd 6.3.0
Firepower /ssa/app* # accept-license-agreement
Firepower /ssa/app* # commit-buffer
Firepower /ssa/app # exit
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd MyDevice1
Firepower /ssa/slot/app-instance* # set deploy-type container
Firepower /ssa/slot/app-instance* # set resource-profile-name silver 1
Firepower /ssa/slot/app-instance* # set startup-version 6.3.0
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* # create logical-device MyDevice1 ftd 1 standalone
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 ftd
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 ftd
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 ftd
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREPOWER_MANAGER_IP
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.0.0.100
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret REGISTRATION_KEY
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: juniorwindowpane
Confirm the value: juniorwindowpane
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: secretglassine
Confirm the value: secretglassine
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FQDN
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value ftd.cisco.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 192.168.1.1
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
```

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value search.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # commit-buffer
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key #
```

Add a High Availability Pair

FTD or ASA High Availability (also known as failover) is configured within the application, not in FXOS. However, to prepare your chassis for high availability, see the following steps.

Before you begin

See [Requirements and Prerequisites for High Availability, on page 226](#).

Procedure

Step 1 Allocate the same interfaces to each logical device.

Step 2 Allocate 1 or 2 data interfaces for the failover and state link(s).

These interfaces exchange high availability traffic between the 2 chassis. We recommend that you use a 10 GB data interface for a combined failover and state link. If you have available interfaces, you can use separate failover and state links; the state link requires the most bandwidth. You cannot use the management-type interface for the failover or state link. We recommend that you use a switch between the chassis, with no other device on the same network segment as the failover interfaces.

For container instances, data-sharing interfaces are not supported for the failover link. We recommend that you create subinterfaces on a parent interface or EtherChannel, and assign a subinterface for each instance to use as a failover link. Note that you must use all subinterfaces on the same parent as failover links. You cannot use one subinterface as a failover link and then use other subinterfaces (or the parent interface) as regular data interfaces.

Step 3 Enable High Availability on the logical devices.

Step 4 If you need to make interface changes after you enable High Availability, perform the changes on the standby unit first, and then perform the changes on the active unit.

Note

For the ASA, if you remove an interface in FXOS (for example, if you remove a network module, remove an EtherChannel, or reassign an interface to an EtherChannel), then the ASA configuration retains the original commands so that you can make any necessary adjustments; removing an interface from the configuration can have wide effects. You can manually remove the old interface configuration in the ASA OS.

Add a Cluster

Clustering lets you group multiple devices together as a single logical device. A cluster provides all the convenience of a single device (management, integration into a network) while achieving the increased

throughput and redundancy of multiple devices. The Firepower 9300, which includes multiple modules, supports intra-chassis clustering where you group all modules within a single chassis into a cluster. You can also use inter-chassis clustering, where multiple chassis are grouped together; inter-chassis clustering is the only option for single module devices like the Firepower 4100 series.

About Clustering on the Firepower 4100/9300 Chassis

When you deploy a cluster on the Firepower 4100/9300 chassis, it does the following:

- Creates a *cluster-control link* (by default, port-channel 48) for node-to-node communication.

For a cluster isolated to security modules within one Firepower 9300 chassis, this link utilizes the Firepower 9300 backplane for cluster communications.

For clustering with multiple chassis, you need to manually assign physical interface(s) to this EtherChannel for communications between chassis.

- Creates the cluster bootstrap configuration within the application.

When you deploy the cluster, the chassis supervisor pushes a minimal bootstrap configuration to each unit that includes the cluster name, cluster control link interface, and other cluster settings. Some parts of the bootstrap configuration may be user-configurable within the application if you want to customize your clustering environment.

- Assigns data interfaces to the cluster as *Spanned* interfaces.

For a cluster isolated to security modules within one Firepower 9300 chassis, spanned interfaces are not limited to EtherChannels, like it is for clustering with multiple chassis. The Firepower 9300 supervisor uses EtherChannel technology internally to load-balance traffic to multiple modules on a shared interface, so any data interface type works for Spanned mode. For clustering with multiple chassis, you must use Spanned EtherChannels for all data interfaces.



Note Individual interfaces are not supported, with the exception of a management interface.

- Assigns a management interface to all units in the cluster.

See the following sections for more information about clustering.

Primary and Secondary Unit Roles

One member of the cluster is the primary unit. The primary unit is determined automatically. All other members are secondary units.

You must perform all configuration on the primary unit only; the configuration is then replicated to the secondary units.

Cluster Control Link

The cluster control link is automatically created using the Port-channel 48 interface.

For a cluster isolated to security modules within one Firepower 9300 chassis, this interface has no member interfaces. This Cluster type EtherChannel utilizes the Firepower 9300 backplane for cluster communications. For clustering with multiple chassis, you must add one or more interfaces to the EtherChannel.

For a cluster with two chassis, do not directly connect the cluster control link from one chassis to the other chassis. If you directly connect the interfaces, then when one unit fails, the cluster control link fails, and thus the remaining healthy unit fails. If you connect the cluster control link through a switch, then the cluster control link remains up for the healthy unit.

Cluster control link traffic includes both control and data traffic.

Size the Cluster Control Link

If possible, you should size the cluster control link to match the expected throughput of each chassis so the cluster control link can handle the worst-case scenarios.

Cluster control link traffic is comprised mainly of state update and forwarded packets. The amount of traffic at any given time on the cluster control link varies. The amount of forwarded traffic depends on the load-balancing efficacy or whether there is a lot of traffic for centralized features. For example:

- NAT results in poor load balancing of connections, and the need to rebalance all returning traffic to the correct units.
- When membership changes, the cluster needs to rebalance a large number of connections, thus temporarily using a large amount of cluster control link bandwidth.

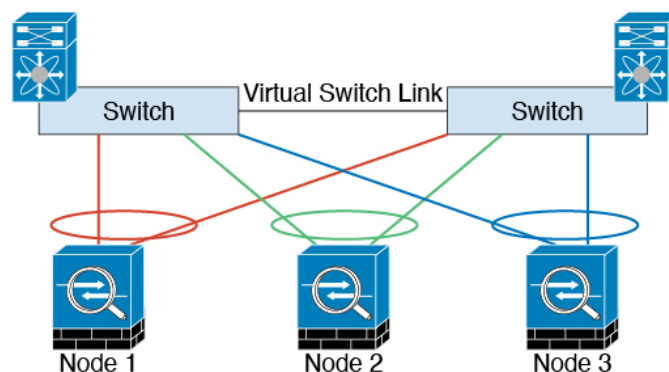
A higher-bandwidth cluster control link helps the cluster to converge faster when there are membership changes and prevents throughput bottlenecks.



Note If your cluster has large amounts of asymmetric (rebalanced) traffic, then you should increase the cluster control link size.

Cluster Control Link Redundancy

The following diagram shows how to use an EtherChannel as a cluster control link in a Virtual Switching System (VSS), Virtual Port Channel (vPC), StackWise, or StackWise Virtual environment. All links in the EtherChannel are active. When the switch is part of a redundant system, then you can connect firewall interfaces within the same EtherChannel to separate switches in the redundant system. The switch interfaces are members of the same EtherChannel port-channel interface, because the separate switches act like a single switch. Note that this EtherChannel is device-local, not a Spanned EtherChannel.



Cluster Control Link Reliability for Inter-Chassis Clustering

To ensure cluster control link functionality, be sure the round-trip time (RTT) between units is less than 20 ms. This maximum latency enhances compatibility with cluster members installed at different geographical sites. To check your latency, perform a ping on the cluster control link between units.

The cluster control link must be reliable, with no out-of-order or dropped packets; for example, for inter-site deployment, you should use a dedicated link.

Cluster Control Link Network

The Firepower 4100/9300 chassis auto-generates the cluster control link interface IP address for each unit based on the chassis ID and slot ID: `127.2.chassis_id.slot_id`. You can customize this IP address when you deploy the cluster. The cluster control link network cannot include any routers between units; only Layer 2 switching is allowed. For inter-site traffic, Cisco recommends using Overlay Transport Virtualization (OTV).

Management Network

We recommend connecting all units to a single management network. This network is separate from the cluster control link.

Management Interface

You must assign a Management type interface to the cluster. This interface is a special *individual* interface as opposed to a Spanned interface. The management interface lets you connect directly to each unit.

For the ASA, the Main cluster IP address is a fixed address for the cluster that always belongs to the current primary unit. You must configure a range of addresses so that each unit, including the current primary unit, can use a Local address from the range. The Main cluster IP address provides consistent management access to an address; when a primary unit changes, the Main cluster IP address moves to the new primary unit, so management of the cluster continues seamlessly. The Local IP address is used for routing, and is also useful for troubleshooting. For example, you can manage the cluster by connecting to the Main cluster IP address, which is always attached to the current primary unit. To manage an individual member, you can connect to the Local IP address. For outbound management traffic such as TFTP or syslog, each unit, including the primary unit, uses the Local IP address to connect to the server.

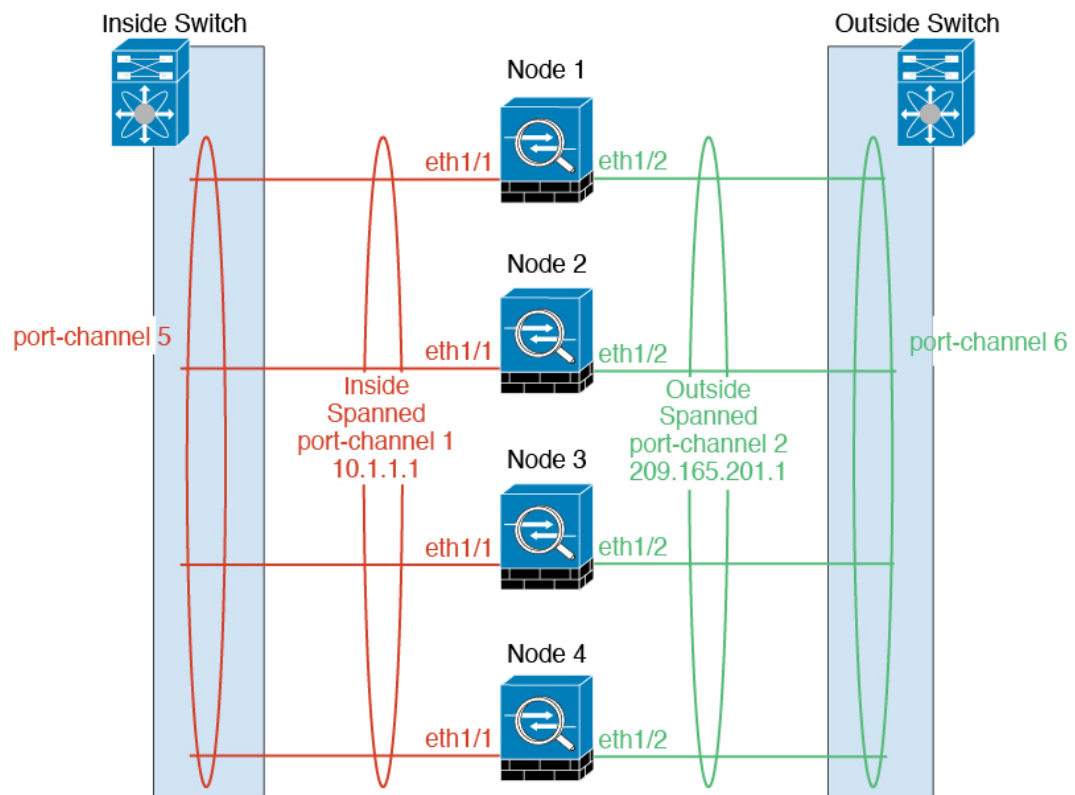
For the Firepower Threat Defense, assign a management IP address to each unit on the same network. Use these IP addresses when you add each unit to the FMC.

Spanned EtherChannels

You can group one or more interfaces per chassis into an EtherChannel that spans all chassis in the cluster. The EtherChannel aggregates the traffic across all the available active interfaces in the channel.

A Spanned EtherChannel can be configured in both routed and transparent firewall modes. In routed mode, the EtherChannel is configured as a routed interface with a single IP address. In transparent mode, the IP address is assigned to the BVI, not to the bridge group member interface.

The EtherChannel inherently provides load balancing as part of basic operation.



Inter-Site Clustering

For inter-site installations, you can take advantage of clustering as long as you follow the recommended guidelines.

You can configure each cluster chassis to belong to a separate site ID.

Site IDs work with site-specific MAC addresses and IP addresses. Packets egressing the cluster use a site-specific MAC address and IP address, while packets received by the cluster use a global MAC address and IP address. This feature prevents the switches from learning the same global MAC address from both sites on two different ports, which causes MAC flapping; instead, they only learn the site MAC address. Site-specific MAC addresses and IP address are supported for routed mode using Spanned EtherChannels only.

Site IDs are also used to enable flow mobility using LISP inspection, director localization to improve performance and reduce round-trip time latency for inter-site clustering for data centers, and site redundancy for connections where a backup owner of a traffic flow is always at a different site from the owner.

See the following sections for more information about inter-site clustering:

- Sizing the Data Center Interconnect—[Requirements and Prerequisites for Clustering](#), on page 225
- Inter-Site Guidelines—[Clustering Guidelines and Limitations](#), on page 229
- Inter-Site Examples—[Examples for Inter-Site Clustering](#), on page 304

Add an ASA Cluster

You can add a single Firepower 9300 chassis as an intra-chassis cluster, or add multiple chassis for inter-chassis clustering. For inter-chassis clustering, you must configure each chassis separately. Add the cluster on one chassis; you can then enter most of the same settings on the next chassis.

Create an ASA Cluster

Set the scope to the image version.

You can easily deploy the cluster from the Firepower 4100/9300 chassis supervisor. All initial configuration is automatically generated for each unit.

For clustering on multiple chassis, you must configure each chassis separately. Deploy the cluster on one chassis; you can then copy the bootstrap configuration from the first chassis to the next chassis for ease of deployment.

In a Firepower 9300 chassis, you must enable clustering for all 3 module slots, even if you do not have a module installed. If you do not configure all 3 modules, the cluster will not come up.

For multiple context mode, you must first deploy the logical device, and then enable multiple context mode in the ASA application.

Before you begin

- Download the application image you want to use for the logical device from Cisco.com, and then upload that image to the Firepower 4100/9300 chassis.
- Gather the following information:
 - Management interface ID, IP address, and network mask
 - Gateway IP address

Procedure

Step 1 Configure interfaces.

Step 2 Enter security services mode.

scope ssa

Example:

```
Firepower# scope ssa
Firepower /ssa #
```

Step 3 Set the application instance image version.

a) View available images. Note the Version number that you want to use.

show app

Example:


```

Firepower /ssa # show app
      Name      Version      Author      Supported Deploy Types CSP Type      Is Default
App -----
-----
      asa        9.9.1        cisco       Native        Application No
      asa        9.10.1       cisco       Native        Application Yes
      ftd        6.2.3        cisco       Native        Application Yes
      ftd        6.3.0        cisco       Native,Container Application Yes

```

- b) Set the scope to the image version.

scope app asa application_version

Example:

```

Firepower /ssa # scope app asa 9.10.1
Firepower /ssa/app #

```

- c) Set this version as the default.

set-default

Example:

```

Firepower /ssa/app # set-default
Firepower /ssa/app* #

```

- d) Exit to ssa mode.

exit

Example:

```

Firepower /ssa/app* # exit
Firepower /ssa* #

```

Example:

```

Firepower /ssa # scope app asa 9.12.1
Firepower /ssa/app # set-default
Firepower /ssa/app* # exit
Firepower /ssa* #

```

Step 4 Create the cluster.

enter logical-device device_name asa slots clustered

- *device_name*—Used by the Firepower 4100/9300 chassis supervisor to configure clustering settings and assign interfaces; it is not the cluster name used in the security module configuration. You must specify all three security modules, even if you have not yet installed the hardware.
- *slots*—Assigns the chassis modules to the cluster. For the Firepower 4100, specify **1**. For the Firepower 9300, specify **1,2,3**. You must enable clustering for all 3 module slots in a Firepower 9300 chassis, even if you do not have a module installed. If you do not configure all 3 modules, the cluster will not come up.

Example:

```
Firepower /ssa # enter logical-device ASA1 asa 1,2,3 clustered
Firepower /ssa/logical-device* #
```

Step 5 Configure the cluster bootstrap parameters.

These settings are meant for initial deployment only, or for disaster recovery. For normal operation, you can later change most values in the application CLI configuration.

- a) Create the cluster bootstrap object.

enter cluster-bootstrap**Example:**

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* #
```

- b) Set the chassis ID.

set chassis-id id

Each chassis in the cluster needs a unique ID.

- c) For inter-site clustering, set the site ID between 1 and 8.

set site-id number.

To remove the site ID, set the value to **0**.

Example:

```
Firepower /ssa/logical-device/cluster-bootstrap* # set site-id 1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

- d) Configure an authentication key for control traffic on the cluster control link.

set key**Example:**

```
Firepower /ssa/logical-device/cluster-bootstrap* # set key
Key: diamonddogs
```

You are prompted to enter the shared secret.

The shared secret is an ASCII string from 1 to 63 characters. The shared secret is used to generate the key. This option does not affect datapath traffic, including connection state update and forwarded packets, which are always sent in the clear.

- e) Set the cluster interface mode.

set mode spanned-etherchannel

Spanned EtherChannel mode is the only supported mode.

Example:

```
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* #
```

- f) Set the cluster group name in the security module configuration.

set service-type *cluster_name*

The name must be an ASCII string from 1 to 38 characters.

Example:

```
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

- g) (Optional) Set the cluster control link IP network.

set cluster-control-link network *a.b.0.0*

By default, the cluster control link uses the 127.2.0.0/16 network. However, some networking deployments do not allow 127.2.0.0/16 traffic to pass. In this case, you can specify a /16 address on a unique network for the cluster.

- *a.b.0.0*—Specify any /16 network address, except for loopback (127.0.0.0/8) and multicast (224.0.0.0/4) addresses. If you set the value to 0.0.0.0, then the default network is used: 127.2.0.0.

The chassis auto-generates the cluster control link interface IP address for each unit based on the chassis ID and slot ID: *a.b.chassis_id.slot_id*.

Example:

```
Firepower /ssa/logical-device/cluster-bootstrap* # set cluster-control-link network
10.10.0.0
```

- h) Configure the management IP address information.

This information is used to configure a management interface in the security module configuration.

1. Configure a pool of Local IP addresses, one of which will be assigned to each cluster unit for the interface.

set ipv4 pool *start_ip end_ip*

set ipv6 pool *start_ip end_ip*

Include at least as many addresses as there are units in the cluster. Note that for the Firepower 9300, you must include 3 addresses per chassis, even if you do not have all module slots filled. If you plan to expand the cluster, include additional addresses. The Virtual IP address (known as the Main cluster IP address) that belongs to the current control unit is *not* a part of this pool; be sure to reserve an IP address on the same network for the Main cluster IP address. You can use IPv4 and/or IPv6 addresses.

2. Configure the Main cluster IP address for the management interface.

set virtual ipv4 *ip_address mask mask*

set virtual ipv6 *ip_address prefix-length prefix*

This IP address must be on the same network as the cluster pool addresses, but not be part of the pool.

3. Enter the network gateway address.

```
set ipv4 gateway ip_address
```

```
set ipv6 gateway ip_address
```

Example:

```
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 gateway 10.1.1.254
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 pool 10.1.1.11 10.1.1.27
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 gateway 2001:DB8::AA
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 pool 2001:DB8::11 2001:DB8::27
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv4 10.1.1.1 mask
255.255.255.0
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv6 2001:DB8::1
prefix-length 64
```

- i) Exit the cluster bootstrap mode.

```
exit
```

Example:

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* # set chassis-id 1
Firepower /ssa/logical-device/cluster-bootstrap* # set key
Key: f@arscape
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* # exit
Firepower /ssa/logical-device/* #
```

Step 6 Configure the management bootstrap parameters.

These settings are meant for initial deployment only, or for disaster recovery. For normal operation, you can later change most values in the application CLI configuration.

- a) Create the management bootstrap object.

```
enter mgmt-bootstrap asa
```

Example:

```
Firepower /ssa/logical-device* # enter mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- b) Specify the admin and enable password.

```
create bootstrap-key-secret PASSWORD
```

```
set value
```

Enter a value: *password*

Confirm the value: *password*

```
exit
```

Example:

The pre-configured ASA admin user and enable password is useful for password recovery; if you have FXOS access, you can reset the admin user password if you forget it.

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- c) Specify the firewall mode, routed or transparent.

create bootstrap-key FIREWALL_MODE

set value {routed | transparent}

exit

In routed mode, the device is considered to be a router hop in the network. Each interface that you want to route between is on a different subnet. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices.

The firewall mode is only set at initial deployment. If you re-apply the bootstrap settings, this setting is not used.

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- d) Exit the management bootstrap mode.

exit

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

Step 7 Save the configuration.

commit-buffer

The chassis deploys the logical device by downloading the specified software version and pushing the bootstrap configuration and management interface settings to the application instance. Check the status of the deployment using the **show app-instance** command. The application instance is running and ready to use when the **Admin State** is **Enabled** and the **Oper State** is **Online**.

Example:

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
```

App Name	Identifier	Slot ID	Admin State	Oper State	Running Version	Startup Version
Deploy Type	Profile Name	Cluster	State	Cluster Role		
ftd	cluster1	1	Enabled	Online	7.3.0.49	7.3.0.49
Native			In Cluster	Data Node		
ftd	cluster1	2	Enabled	Online	7.3.0.49	7.3.0.49
Native			In Cluster	Control Node		
ftd	cluster1	3	Disabled	Not Available		7.3.0.49
Native			Not Applicable	None		

Step 8 To add another chassis to the cluster, repeat this procedure except you must configure a unique **chassis-id** and the correct **site-id**; otherwise, use the same configuration for both chassis.

Make sure the interface configuration is the same on the new chassis. You can export and import FXOS chassis configuration to make this process easier.

Step 9 Connect to the control unit ASA to customize your clustering configuration.

Example

For chassis 1:

```
scope eth-uplink
  scope fabric a
    enter port-channel 1
    set port-type data
    enable
    enter member-port Ethernet1/1
    exit
    enter member-port Ethernet1/2
    exit
    exit
  enter port-channel 2
  set port-type data
  enable
  enter member-port Ethernet1/3
  exit
  enter member-port Ethernet1/4
  exit
  exit
  enter port-channel 3
  set port-type data
  enable
  enter member-port Ethernet1/5
  exit
  enter member-port Ethernet1/6
  exit
  exit
  enter port-channel 4
  set port-type mgmt
  enable
  enter member-port Ethernet2/1
  exit
  enter member-port Ethernet2/2
  exit
  exit
  enter port-channel 48
  set port-type cluster
```

```

        enable
        enter member-port Ethernet2/3
        exit
    exit
exit
commit-buffer

scope ssa
    enter logical-device ASA1 asa "1,2,3" clustered
    enter cluster-bootstrap
        set chassis-id 1
        set ipv4 gateway 10.1.1.254
        set ipv4 pool 10.1.1.11 10.1.1.27
        set ipv6 gateway 2001:DB8::AA
        set ipv6 pool 2001:DB8::11 2001:DB8::27
        set key
        Key: f@arscape
        set mode spanned-etherchannel
        set service-type cluster1
        set virtual ipv4 10.1.1.1 mask 255.255.255.0
        set virtual ipv6 2001:DB8::1 prefix-length 64
    exit
exit
scope app asa 9.5.2.1
    set-default
    exit
commit-buffer

```

For chassis 2:

```

scope eth-uplink
    scope fabric a
        create port-channel 1
        set port-type data
        enable
        create member-port Ethernet1/1
        exit
        create member-port Ethernet1/2
        exit
    exit
    create port-channel 2
    set port-type data
    enable
    create member-port Ethernet1/3
    exit
    create member-port Ethernet1/4
    exit
    exit
    create port-channel 3
    set port-type data
    enable
    create member-port Ethernet1/5
    exit
    create member-port Ethernet1/6
    exit
    exit
    create port-channel 4
    set port-type mgmt
    enable
    create member-port Ethernet2/1
    exit
    create member-port Ethernet2/2

```

```

        exit
    exit
    create port-channel 48
        set port-type cluster
        enable
        create member-port Ethernet2/3
        exit
    exit
    exit
    exit
commit-buffer

scope ssa
    enter logical-device ASA1 asa "1,2,3" clustered
    enter cluster-bootstrap
        set chassis-id 2
        set ipv4 gateway 10.1.1.254
        set ipv4 pool 10.1.1.11 10.1.1.15
        set ipv6 gateway 2001:DB8::AA
        set ipv6 pool 2001:DB8::11 2001:DB8::19
        set key
        Key: f@rscape
        set mode spanned-etherchannel
        set service-type cluster1
        set virtual ipv4 10.1.1.1 mask 255.255.255.0
        set virtual ipv6 2001:DB8::1 prefix-length 64
        exit
    exit
scope app asa 9.5.2.1
    set-default
    exit
commit-buffer

```

Add More Cluster Members

Add or replace the ASA cluster member.



Note This procedure only applies to adding or replacing a *chassis*; if you are adding or replacing a module to a Firepower 9300 where clustering is already enabled, the module will be added automatically.

Before you begin

- Make sure your existing cluster has enough IP addresses in the management IP address pool for this new member. If not, you need to edit the existing cluster bootstrap configuration on each chassis before you add this new member. This change causes a restart of the logical device.
- The interface configuration must be the same on the new chassis. You can export and import FXOS chassis configuration to make this process easier.
- For multiple context mode, enable multiple context mode in the ASA application on the first cluster member; additional cluster members will inherit the multiple context mode configuration automatically.

Procedure

-
- Step 1** Click the **Copy config** check box, and click **OK**. If you uncheck this check box, you must manually enter the settings to match the first chassis configuration.
- Step 2** To add another chassis to the cluster, repeat the procedure in [Create an ASA Cluster, on page 256](#) except you must configure a unique **chassis-id** and the correct **site-id**; otherwise, use the same configuration for the new chassis.
-

Add a FTD Cluster

You can add a cluster to a single Firepower 9300 chassis that is isolated to security modules within the chassis, or you can use multiple chassis.

For clusters on multiple chassis, you must configure each chassis separately. Add the cluster on one chassis; you can then enter most of the same settings on the next chassis.

Create a FTD Cluster

You can easily deploy the cluster from the Firepower 4100/9300 chassis supervisor. All initial configuration is automatically generated for each unit.

For clustering on multiple chassis, you must configure each chassis separately. Deploy the cluster on one chassis; you can then copy the bootstrap configuration from the first chassis to the next chassis for ease of deployment.

In a Firepower 9300 chassis, you must enable clustering for all 3 module slots, even if you do not have a module installed. If you do not configure all 3 modules, the cluster will not come up.

Before you begin

- Download the application image you want to use for the logical device from Cisco.com, and then upload that image to the Firepower 4100/9300 chassis.
- Gather the following information:
 - Management interface ID, IP addresses, and network mask
 - Gateway IP address
 - FMC IP address and/or NAT ID of your choosing
 - DNS server IP address
 - FTD hostname and domain name

Procedure

-
- Step 1** Configure interfaces.

Step 2 Enter security services mode.

scope ssa

Example:

```
Firepower# scope ssa
Firepower /ssa #
```

Step 3 Set the default image version.

a) View available images. Note the Version number that you want to use.

show app

Example:

```
Firepower /ssa # show app
```

Name	Version	Author	Supported Deploy Types	CSP Type	Is Default
App					
-----	-----	-----	-----	-----	-----
asa	9.9.1	cisco	Native	Application	No
asa	9.10.1	cisco	Native	Application	Yes
ftd	6.2.3	cisco	Native	Application	Yes
ftd	6.3.0	cisco	Native,Container	Application	Yes

b) Set the scope to the image version.

scope app ftd *application_version*

Example:

```
Firepower /ssa # scope app ftd 6.2.3
Firepower /ssa/app #
```

c) Accept the license agreement.

accept-license-agreement

Example:

```
Firepower /ssa/app # accept-license-agreement
```

```
End User License Agreement: End User License Agreement
```

```
Effective: May 22, 2017
```

This is an agreement between You and Cisco Systems, Inc. or its affiliates ("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the individual or legal entity licensing the Software under this EULA. "Use" or "Using" means to download, install, activate, access or otherwise use the Software. "Software" means the Cisco computer programs and any Upgrades made available to You by an Approved Source and licensed to You by Cisco. "Documentation" is the Cisco user or technical manuals, training materials, specifications or other documentation applicable to the Software and made available to You by an Approved Source. "Approved Source" means (i) Cisco or (ii) the Cisco authorized reseller, distributor or systems integrator from whom you acquired the Software. "Entitlement" means the license detail; including license metric, duration, and quantity provided in a product ID (PID) published on Cisco's price list, claim certificate or right to use notification.

"Upgrades" means all updates, upgrades, bug fixes, error corrections, enhancements and other modifications to the Software and backup copies thereof.

[...]

Please "commit-buffer" if you accept the license agreement, otherwise "discard-buffer".

```
Firepower /ssa/app* #
```

- d) Set this version as the default.

set-default

Example:

```
Firepower /ssa/app # set-default
Firepower /ssa/app* #
```

- e) Save the configuration.

commit-buffer

Example:

```
Firepower /ssa/app* # commit-buffer
Firepower /ssa/app #
```

- f) Exit to ssa mode.

exit

Example:

```
Firepower /ssa/app* # exit
Firepower /ssa* #
```

Example:

```
Firepower /ssa # scope app ftd 6.3.0.21
Firepower /ssa/app # set-default
Firepower /ssa/app* # accept-license-agreement
Firepower /ssa/app* # exit
Firepower /ssa* #
```

Step 4 Create the cluster:

enter logical-device *device_name* ftd slots clustered

- *device_name*—Used by the Firepower 4100/9300 chassis supervisor to configure clustering settings and assign interfaces; it is not the cluster name used in the security module configuration.
- *slots*—Assigns the chassis modules to the cluster. For the Firepower 4100, specify **1**. For the Firepower 9300, specify **1,2,3**. You must enable clustering for all 3 module slots in a Firepower 9300 chassis, even if you do not have a module installed. If you do not configure all 3 modules, the cluster will not come up.

Example:

```
Firepower /ssa # enter logical-device FTD1 ftd 1,2,3 clustered
Firepower /ssa/logical-device* #
```

Step 5 Configure the cluster bootstrap parameters.

These settings are meant for initial deployment only, or for disaster recovery. For normal operation, you can later change most values in the application CLI configuration.

- a) Create the cluster bootstrap object.

enter cluster-bootstrap

Example:

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* #
```

- b) Set the chassis ID.

set chassis-id *id*

Each chassis in the cluster needs a unique ID.

- c) For inter-site clustering, set the site ID between 1 and 8.

set site-id *number*.

To remove the site ID, set the value to **0**.

Example:

```
Firepower /ssa/logical-device/cluster-bootstrap* # set site-id 1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

- d) Configure an authentication key for control traffic on the cluster control link.

set key

Example:

```
Firepower /ssa/logical-device/cluster-bootstrap* # set key
Key: diamonddogs
```

You are prompted to enter the shared secret.

The shared secret is an ASCII string from 1 to 63 characters. The shared secret is used to generate the key. This option does not affect datapath traffic, including connection state update and forwarded packets, which are always sent in the clear.

- e) Set the cluster interface mode.

set mode spanned-etherchannel

Spanned EtherChannel mode is the only supported mode.

Example:

```
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
```

```
Firepower /ssa/logical-device/cluster-bootstrap* #
```

- f) Set the cluster group name in the security module configuration.

set service-type *cluster_name*

The name must be an ASCII string from 1 to 38 characters.

Example:

```
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

- g) (Optional) Set the cluster control link IP network.

set cluster-control-link network *a.b.0.0*

By default, the cluster control link uses the 127.2.0.0/16 network. However, some networking deployments do not allow 127.2.0.0/16 traffic to pass. In this case, you can specify a /16 address on a unique network for the cluster.

- ***a.b.0.0***—Specify any /16 network address, except for loopback (127.0.0.0/8) and multicast (224.0.0.0/4) addresses. If you set the value to 0.0.0.0, then the default network is used: 127.2.0.0.

The chassis auto-generates the cluster control link interface IP address for each unit based on the chassis ID and slot ID: *a.b.chassis_id.slot_id*.

Example:

```
Firepower /ssa/logical-device/cluster-bootstrap* # set cluster-control-link network
10.10.0.0
```

- h) Exit the cluster bootstrap mode.

exit

Example:

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* # set chassis-id 1
Firepower /ssa/logical-device/cluster-bootstrap* # set key
Key: f@arscape
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* # exit
Firepower /ssa/logical-device/* #
```

Step 6 Configure the management bootstrap parameters.

These settings are meant for initial deployment only, or for disaster recovery. For normal operation, you can later change most values in the application CLI configuration.

- a) Create the management bootstrap object.

enter mgmt-bootstrap *ftd*

Example:

```
Firepower /ssa/logical-device* # enter mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- b) Specify the IP address or hostname or NAT ID of the managing FMC.

Set one of the following:

- **enter bootstrap-key FIREPOWER_MANAGER_IP**
set value *IP_address*
exit
- **enter bootstrap-key FQDN**
set value *fmc_hostname*
exit
- **enter bootstrap-key NAT_ID**
set value *nat_id*
exit

Normally, you need both IP addresses (along with a registration key) for both routing purposes and for authentication: the FMC specifies the device IP address, and the device specifies the FMC IP address. However, if you only know one of the IP addresses, which is the minimum requirement for routing purposes, then you must also specify a unique NAT ID on both sides of the connection to establish trust for the initial communication and to look up the correct registration key. You can specify any text string as the NAT ID, from 1 to 37 characters. The FMC and device use the registration key and NAT ID (instead of IP addresses) to authenticate and authorize for initial registration.

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key NAT_ID
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value sc0rpius15
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- c) Specify the firewall mode, routed or transparent.

```
create bootstrap-key FIREWALL_MODE
set value {routed | transparent}
exit
```

In routed mode, the device is considered to be a router hop in the network. Each interface that you want to route between is on a different subnet. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices.

The firewall mode is only set at initial deployment. If you re-apply the bootstrap settings, this setting is not used.

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
```

```
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- d) Specify the key to be shared between the device and the FMC.

enter bootstrap-key-secret REGISTRATION_KEY

set value

Enter a value: *registration_key*

Confirm the value: *registration_key*

exit

You can choose any text string for this key between 1 and 37 characters; you will enter the same key on the FMC when you add the Firepower Threat Defense.

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret
REGISTRATION_KEY
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: gratuitousapples
Confirm the value: gratuitousapples
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- e) Specify a password for the Firepower Threat Defense admin user for CLI access.

enter bootstrap-key-secret PASSWORD

set value

Enter a value: *password*

Confirm the value: *password*

exit

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- f) Specify the fully qualified hostname.

enter bootstrap-key FQDN

set value fqdn

exit

Valid characters are the letters from a to z, the digits from 0 to 9, the dot (.), and the hyphen (-); maximum number of characters is 253.

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FQDN
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
ftdcluster1.example.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- g) Specify a comma-separated list of DNS servers.

enter bootstrap-key DNS_SERVERS

set value *dns_servers*

exit

The Firepower Threat Defense uses DNS if you specify a hostname for the FMC, for example.

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.9.8.7,10.9.6.5
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- h) Specify a comma-separated list of search domains.

enter bootstrap-key SEARCH_DOMAINS

set value *search_domains*

exit

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
cisco.com,example.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- i) Configure the management IP addresses for each security module in the cluster.

Note

For the Firepower 9300, you must set the IP address for all 3 module slots in a chassis, even if you do not have a module installed. If you do not configure all 3 modules, the cluster will not come up.

To create an IPv4 management interface object:

1. Create the management interface object.

enter ipv4 *slot_id* **firepower**

2. Set the gateway address.

set gateway *gateway_address*

3. Set the IP address and mask.

set ip *ip_address* **mask** *network_mask*

4. Exit the management IP mode.

exit

5. Repeat for the remaining modules in the chassis.

To create an IPv6 management interface object:

1. Create the management interface object.

enter ipv6 slot_id firepower

2. Set the gateway address.

set gateway gateway_address

3. Set the IP address and prefix.

set ip ip_address prefix-length prefix

4. Exit the management IP mode.

exit

5. Repeat for the remaining modules in the chassis.

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.34 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 2 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.35 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 3 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.36 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 2 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 3 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3212
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- j) Exit the management bootstrap mode.

exit

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

Example:

```
Firepower /ssa/logical-device* # enter mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key FIREPOWER_MANAGER_IP
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.0.0.100
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # enter bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key-secret REGISTRATION_KEY
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Value: ziggy$tardust
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Value: $pidersfrommars
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key FQDN
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value example.cisco.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 192.168.1.1
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value example.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter ipv4 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter ipv4 2 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.32 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter ipv4 3 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.33 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

Step 7 Save the configuration.

commit-buffer

The chassis deploys the logical device by downloading the specified software version and pushing the bootstrap configuration and management interface settings to the application instance. Check the status of the deployment using the **show app-instance** command. The application instance is running and ready to use when the **Admin State is Enabled** and the **Oper State is Online**.

Example:

```
Firepower /ssa/logical-device* # commit-buffer
```

```

Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
App Name   Identifier Slot ID   Admin State Oper State   Running Version Startup Version
Deploy Type Profile Name Cluster State   Cluster Role
-----
ftd        cluster1   1       Enabled   Online       7.3.0.49      7.3.0.49
Native
ftd        cluster1   2       Enabled   Online       7.3.0.49      7.3.0.49
Native
ftd        cluster1   3       Disabled  Not Available 7.3.0.49
Native

```

Step 8 To add another chassis to the cluster, repeat this procedure except you must configure unique **chassis-id** and management IP addresses, as well as the correct **site-id**; otherwise, use the same configuration for both chassis.

Make sure the interface configuration is the same on the new chassis. You can export and import FXOS chassis configuration to make this process easier.

Step 9 Add the control unit to the FMC using the management IP address.

All cluster units must be in a successfully-formed cluster on FXOS prior to adding them to FMC.

The FMC then automatically detects the data units.

Example

```

scope eth-uplink
  scope fabric a
    enter port-channel 1
    set port-type data
    enable
    create member-port Ethernet1/1
    exit
    create member-port Ethernet1/2
    exit
    exit
  enter port-channel 2
  set port-type data
  enable
  create member-port Ethernet1/3
  exit
  create member-port Ethernet1/4
  exit
  exit
  enter port-channel 3
  set port-type firepower-eventing
  enable
  create member-port Ethernet1/5
  exit
  create member-port Ethernet1/6
  exit
  exit
  enter port-channel 4
  set port-type mgmt
  enable
  create member-port Ethernet2/1
  exit

```

```

        enter member-port Ethernet2/2
        exit
    exit
enter port-channel 48
    set port-type cluster
    enable
    enter member-port Ethernet2/3
    exit
    exit
exit
exit
commit-buffer

scope ssa
    enter logical-device FTD1 ftd "1,2,3" clustered
    enter cluster-bootstrap
        set chassis-id 1
        set key cluster_key
        set mode spanned-etherchannel
        set service-type ftd-cluster
        exit
    enter mgmt-bootstrap ftd
        enter bootstrap-key FIREPOWER_MANAGER_IP
            set value 10.0.0.100
            exit
        enter bootstrap-key FIREWALL_MODE
            set value transparent
            exit
        enter bootstrap-key-secret REGISTRATION_KEY
            set value
                Value: alladinsane
            exit
        enter bootstrap-key-secret PASSWORD
            set value
                Value: widthofacircle
            exit
        enter bootstrap-key FQDN
            set value ftd.cisco.com
            exit
        enter bootstrap-key DNS_SERVERS
            set value 192.168.1.1
            exit
        enter bootstrap-key SEARCH_DOMAINS
            set value search.com
            exit
        enter ipv4 1 firepower
            set gateway 10.0.0.1
            set ip 10.0.0.31 mask 255.255.255.0
            exit
        enter ipv4 2 firepower
            set gateway 10.0.0.1
            set ip 10.0.0.32 mask 255.255.255.0
            exit
        enter ipv4 3 firepower
            set gateway 10.0.0.1
            set ip 10.0.0.33 mask 255.255.255.0
            exit
        exit
    exit
scope app ftd 6.0.0.837
    accept-license-agreement
    set-default
    exit

```

```
commit-buffer
```

For chassis 2:

```
scope eth-uplink
  scope fabric a
    enter port-channel 1
    set port-type data
    enable
    create member-port Ethernet1/1
    exit
    create member-port Ethernet1/2
    exit
    exit
  enter port-channel 2
  set port-type data
  enable
  create member-port Ethernet1/3
  exit
  create member-port Ethernet1/4
  exit
  exit
  enter port-channel 3
  set port-type firepower-eventing
  enable
  create member-port Ethernet1/5
  exit
  create member-port Ethernet1/6
  exit
  exit
  enter port-channel 4
  set port-type mgmt
  enable
  create member-port Ethernet2/1
  exit
  enter member-port Ethernet2/2
  exit
  exit
  enter port-channel 48
  set port-type cluster
  enable
  enter member-port Ethernet2/3
  exit
  exit
  exit
commit-buffer

scope ssa
  enter logical-device FTD1 ftd "1,2,3" clustered
  enter cluster-bootstrap
  set chassis-id 2
  set key cluster_key
  set mode spanned-etherchannel
  set service-type ftd-cluster
  exit
  enter mgmt-bootstrap ftd
  enter bootstrap-key FIREPOWER_MANAGER_IP
  set value 10.0.0.100
  exit
  enter bootstrap-key FIREWALL_MODE
  set value transparent
  exit
```

```

enter bootstrap-key-secret REGISTRATION_KEY
  set value
    Value: alladinsane
  exit
enter bootstrap-key-secret PASSWORD
  set value
    Value: widthofacircle
  exit
enter bootstrap-key FQDN
  set value ftd.cisco.com
  exit
enter bootstrap-key DNS_SERVERS
  set value 192.168.1.1
  exit
enter bootstrap-key SEARCH_DOMAINS
  set value search.com
  exit
enter ipv4 1 firepower
  set gateway 10.0.0.1
  set ip 10.0.0.31 mask 255.255.255.0
  exit
enter ipv4 2 firepower
  set gateway 10.0.0.1
  set ip 10.0.0.32 mask 255.255.255.0
  exit
enter ipv4 3 firepower
  set gateway 10.0.0.1
  set ip 10.0.0.33 mask 255.255.255.0
  exit
exit
exit
scope app ftd 6.0.0.837
  set-default
  accept-license-agreement
  exit
commit-buffer

```

Add More Cluster Nodes

Add or replace the Firepower Threat Defense cluster node in an existing cluster. When you add a new cluster node in FXOS, the FMC adds the node automatically.



Note The FXOS steps in this procedure only apply to adding a new *chassis*; if you are adding a new module to a Firepower 9300 where clustering is already enabled, the module will be added automatically.

Before you begin

- In the case of a replacement, you must delete the old cluster node from the FMC. When you replace it with a new node, it is considered to be a new device on the FMC.
- The interface configuration must be the same on the new chassis. You can export and import FXOS chassis configuration to make this process easier.

Procedure

To add another chassis to the cluster, repeat the procedure in [Create a FTD Cluster, on page 265](#) except you must configure the following settings to be unique; otherwise, use the same configuration for both chassis.

- Chassis ID
- Management IP addresses

Also be sure to set the startup version to the currently running version on the cluster nodes.

Configure Radware DefensePro

The Cisco Firepower 4100/9300 chassis can support multiple services (for example, a firewall and a third-party DDoS application) on a single blade. These applications and services can be linked together to form a Service Chain.

About Radware DefensePro

In the current supported Service Chaining configuration, the third-party Radware DefensePro virtual platform can be installed to run in front of the ASA firewall, or in front of Firepower Threat Defense. Radware DefensePro is a KVM-based virtual platform that provides distributed denial-of-service (DDoS) detection and mitigation capabilities on the Firepower 4100/9300 chassis. When Service Chaining is enabled on your Firepower 4100/9300 chassis, traffic from the network must first pass through the DefensePro virtual platform before reaching the main ASA or Firepower Threat Defense firewall.



Note

- The Radware DefensePro virtual platform may be referred to as *Radware vDP* (virtual DefensePro), or simply *vDP*.
- The Radware DefensePro virtual platform may occasionally be referred to as a Link Decorator.
- Radware (vDP) is not supported on logical device instance type setup as container instance.

Prerequisites for Radware DefensePro

Prior to deploying Radware DefensePro on your Firepower 4100/9300 chassis, you must configure the Firepower 4100/9300 chassis to use an NTP Server with the **etc/UTC** Time Zone. For more information about setting the date and time in your Firepower 4100/9300 chassis, see [Setting the Date and Time, on page 107](#).

Guidelines for Service Chaining

Models

- ASA—The Radware DefensePro (vDP) platform is supported with ASA on the following models:
 - Firepower 9300
 - Firepower 4110
 - Firepower 4115
 - Firepower 4120
 - Firepower 4125
 - Firepower 4140
 - Firepower 4145
 - Firepower 4150
- FTD—The Radware DefensePro platform is supported with Firepower Threat Defense on the following models:
 - Firepower 9300
 - Firepower 4110—Note you must deploy the decorator at the same time as the logical device. You cannot install the decorator after the logical device is already configured on the device.
 - Firepower 4115
 - Firepower 4120—Note you must deploy the decorator at the same time as the logical device. You cannot install the decorator after the logical device is already configured on the device.
 - Firepower 4125
 - Firepower 4140
 - Firepower 4145
 - Firepower 4150

Additional Guidelines

- Service Chaining is not supported in an inter-chassis cluster configuration. However, the Radware DefensePro (vDP) application can be deployed in a standalone configuration in an inter-chassis cluster scenario.

Configure Radware DefensePro on a Standalone Logical Device

The following procedure shows how to install Radware DefensePro in a single Service Chain in front of a standalone ASA or Firepower Threat Defense logical device.

Before you begin

- Download the vDP image from Cisco.com (see [Downloading Images from Cisco.com, on page 60](#)) and then download that image to the Firepower 4100/9300 chassis (see [Downloading a Logical Device Software Image to the Firepower 4100/9300 chassis, on page 64](#)).
- You can deploy the Radware DefensePro application in a standalone configuration on an intra-chassis cluster; for intra-chassis clustering, see [Configure Radware DefensePro on an Intra-Chassis Cluster, on page 284](#).

Procedure

- Step 1** If you want to use a separate management interface for vDP, enable the interface and set it to be the mgmt type according to [Configure a Physical Interface, on page 195](#). Otherwise, you can share the application management interface.
- Step 2** Create an ASA or Firepower Threat Defense logical device in standalone configuration (see [Add a Standalone ASA, on page 234](#) or [Add a Standalone FTD, on page 240](#)). Note that if you are installing the images on a Firepower 4110 or 4120 security appliance, you must install vDP along with the Firepower Threat Defense image before you commit your configuration.
- Step 3** Enter security services mode:
- ```
Firepower# scope ssa
```
- Step 4** Create the Radware vDP instance:
- ```
Firepower /ssa # scope slot slot_id
Firepower /ssa/slot # create app-instance vdp logical_device_identifier
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot/* # exit
```
- Step 5** Commit the configuration:
- ```
commit-buffer
```
- Step 6** Verify the installation and provisioning of vDP on the security module:
- ```
Firepower /ssa # show app-instance
```

Example:

```
Firepower /ssa # show app-instance
App Name  Slot ID  Admin State Oper State  Running Version Startup Version Cluster
State    Cluster Role
-----
ftd        1          Enabled   Online     6.2.1.62      6.2.1.62      Not
Applicable None
vdp        1          Disabled  Installing 8.10.01.16-5  Not
Applicable None
```

- Step 7** (Optional) Show the available supported resource profiles:

```
Firepower /ssa/app # show resource-profile system
```

Example:

```

Firepower /ssa # show resource-profile system
Profile Name      App Name  App Version  Is In Use  Security Model  CPU Logical Core Count
RAM Size (MB)    Default Profile Profile Type Description
-----
DEFAULT-4110-RESOURCE
      vdp      8.13.01.09-2 No      FPR4K-SM-12
      4      16384 Yes      System
DEFAULT-RESOURCE  vdp      8.13.01.09-2 No      FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36,
      FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24
      6      24576 Yes      System
VDP-10-CORES      vdp      8.13.01.09-2 No      FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36,
      FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24
      10     40960 No      System
VDP-2-CORES      vdp      8.13.01.09-2 No      all
      2      8192 No      System
VDP-4-CORES      vdp      8.13.01.09-2 No      all
      4      16384 No      System
VDP-8-CORES      vdp      8.13.01.09-2 No      FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36,
      FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24
      8      32768 No      System

```

Step 8 (Optional) Set the resource profile, using one of the available profiles from the previous step:

a) Scope to slot 1:

```
Firepower /ssa*# scope slot 1
```

b) Enter the DefensePro application instance:

```
Firepower /ssa/slot* # enter app-instance vdp
```

c) Set the resource profile:

```
Firepower /ssa/slot/app-instance* # set resource-profile-name resource_profile_name
```

d) Commit the configuration:

```
Firepower /ssa/slot/app-instance* # commit-buffer
```

Step 9 Once the vDP application is installed, access the logical device:

```
Firepower /ssa # scope logical-device device_name
```

Step 10 Assign the management interface to vDP. You can use the same physical interface as for the logical device, or you can use a separate interface.

```
Firepower /ssa/logical-device # enter external-port-link name interface_id vdp
```

```
Firepower /ssa/logical-device/external-port-link* # exit
```

Step 11 Configure the external management interface settings for vDP.

a) Create the bootstrap object:

```
Firepower /ssa/logical-device* # create mgmt-bootstrap vdp
```

b) Configure the management IP address:

```
Firepower /ssa/logical-device/mgmt-bootstrap* #create ipv4 slot_id default
```

- c) Set the gateway address:

```
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* #set gateway gateway_address
```

- d) Set the IP address and mask:

```
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* #set ip ip_address mask network_mask
```

- e) Exit the management IP configuration scope:

```
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* #exit
```

- f) Exit the management bootstrap configuration scope:

```
Firepower /ssa/logical-device/mgmt-bootstrap* #exit
```

- Step 12** Edit the data interface where you want to place the vDP in front of the ASA or Firepower Threat Defense flow:

```
Firepower /ssa/logical-device* # scope external-port-link name
```

Enter the **show external-port-link** command to view interface names.

- Step 13** Add the vDP to the logical device:

```
Firepower /ssa/logical-device/external-port-link* # set decorator vdp
```

Repeat for each interface where you want to use vDP.

Note

To view the updated vDP interfaces in ASA, you must reload the ASA after adding or deleting a vDP interface.

- Step 14** Commit the configuration:

```
commit-buffer
```

- Step 15** Verify that the third-party app is set for the interface:

```
Firepower /ssa/logical-device/external-port-link* # show detail
```

Example:

```
Firepower /ssa/logical-device/external-port-link # show detail
```

```
External-Port Link:
  Name: Ethernet11_ftd
  Port or Port Channel Name: Ethernet1/1
  App Name: ftd
  Description:
  Link Decorator: vdp
```

What to do next

Set a password for the DefensePro application. Note that the application does not come online until you set a password. For more information, see the Radware DefensePro DDoS Mitigation User Guide on cisco.com.

Configure Radware DefensePro on an Intra-Chassis Cluster



Note Service Chaining is not supported in an inter-chassis cluster configuration. However, the Radware DefensePro application can be deployed in a standalone configuration in an inter-chassis cluster scenario.

Before you begin

- Download the vDP image from Cisco.com (see [Downloading Images from Cisco.com, on page 60](#)) and then download that image to the Firepower 4100/9300 chassis (see [Downloading a Logical Device Software Image to the Firepower 4100/9300 chassis, on page 64](#)).

Procedure

- Step 1** If you want to use a separate management interface for vDP, enable the interface and set it to be the mgmt type according to [Configure a Physical Interface, on page 195](#). Otherwise, you can share the application management interface.
- Step 2** Configure an ASA intra-chassis cluster (see [Create an ASA Cluster, on page 256](#)) or a Firepower Threat Defense intra-chassis cluster (see [Create a FTD Cluster, on page 265](#)).
- Step 3** Decorate the external (client-facing) port with Radware DefensePro:
- ```
enter external-port-link name interface_name { asa | ftd }
set decorator vdp
set description ""
exit
```
- Step 4** Assign the external management port for the logical device:
- ```
enter external-port-link { mgmt_asa | mgmt_ftd } interface_id { asa | ftd }
set decorator ""
set description ""
exit
```
- Step 5** Assign the external management port for DefensePro:
- ```
enter external-port-link mgmt_vdp interface_name { asa | ftd }
set decorator ""
set description ""
```
- Step 6** (Optional) Show the available supported resource profiles:
- ```
show resource-profile system
```

Example:

```
Firepower /ssa # show resource-profile system
```

Profile Name	App Name	App Version	Is In Use	Security Model	CPU Logical Core Count
RAM Size (MB)	Default Profile	Profile Type	Description		

DEFAULT-4110-RESOURCE	vdp	8.13.01.09-2	No	FPR4K-SM-12	
4	16384	Yes	System		
DEFAULT-RESOURCE	vdp	8.13.01.09-2	No	FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24	
6	24576	Yes	System		
VDP-10-CORES	vdp	8.13.01.09-2	No	FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24	
10	40960	No	System		
VDP-2-CORES	vdp	8.13.01.09-2	No	all	
2	8192	No	System		
VDP-4-CORES	vdp	8.13.01.09-2	No	all	
4	16384	No	System		
VDP-8-CORES	vdp	8.13.01.09-2	No	FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24	
8	32768	No	System		

Step 7 (Optional) Set the resource profile using one of the available profiles from the previous step:

Note

After committing this change, the FXOS chassis reboots.

a) Scope to slot 1:

Firepower /ssa*# **scope slot 1**

b) Enter the DefensePro application instance:

Firepower /ssa/slot* # **enter app-instance vdp**

c) Set the resource profile:

Firepower /ssa/slot/app-instance* # **set resource-profile-name** *resource_profile_name*

d) Commit the configuration:

Firepower /ssa/slot/app-instance* # **commit-buffer**

Step 8 Configure cluster port channel:

enter **external-port-link** port-channel48 Port-channel48 { *asa* / *ftd* }

set **decorator** ""

set **description** ""

exit

Step 9 Configure management bootstrap for all three DefensePro instances:

enter **mgmt-bootstrap vdp**

enter **ipv4 slot_id default**

set gateway *gateway_address*

set ip *ip_address* **mask** *network_mask*

exit

Example:

```

enter mgmt-bootstrap vdp
  enter ipv4 1 default
    set gateway 172.16.0.1
    set ip 172.16.4.219 mask 255.255.0.0
  exit

  enter ipv4 2 default
    set gateway 172.16.0.1
    set ip 172.16.4.220 mask 255.255.0.0
  exit

  enter ipv4 3 default
    set gateway 172.16.0.1
    set ip 172.16.4.221 mask 255.255.0.0
  exit

```

Step 10 Exit management bootstrap configuration scope:

exit

Step 11 Enter the DefensePro application instance on the Control blade:

connect module *slot* console

connect vdp

Step 12 On the Control blade, set the management IP:

device clustering management-channel ip

Step 13 Using the IP found in the previous step, set the Control IP:

device clustering master set *management-channel ip*

Step 14 Enable the cluster:

device clustering state set enable

Step 15 Exit the application console and return to the FXOS module CLI:

Ctrl]

Step 16 Repeat steps 10, 12, 13, and 14 to set the Control blade IP found in step 11 and enable the cluster for each blade application instance.

Step 17 Commit the configuration:

commit-buffer

Note

After completing this procedure, you must verify whether the DefensePro instances are configured in a cluster.

Step 18 Validate that all DefensePro applications have joined the cluster:

device cluster show

Step 19 Use either of the following methods to verify which DefensePro instance is primary, and which one is secondary.

a) Scope the DefensePro instance and show application attributes for DefensePro only:

```

scope ssa
scope slot slot_number
scope app-instance vdp
show app-attri

```

- b) Scope the slot and show the DefensePro instance in expanded detail. This approach displays information for both logical device and vDP application instances on the slot.

```

scope ssa
scope slot_number
show app-instance expand detail

```

If the DefensePro application is online but not yet formed in a cluster, the CLI displays:

```

App Attribute:
App Attribute Key: cluster-role
Value: unknown

```

If the system displays this "unknown" value, you must enter the DefensePro application and configure the Control blade IP address to create the vDP cluster.

If the DefensePro application is online and formed in a cluster, the CLI displays:

```

App Attribute:
App Attribute Key: cluster-role
Value: primary/secondary

```

Example

```

scope ssa
  enter logical-device ld asa "1,2,3" clustered
  enter cluster-bootstrap
    set chassis-id 1
    set ipv4 gateway 172.16.0.1
    set ipv4 pool 172.16.4.216 172.16.4.218
    set ipv6 gateway 2010::2
    set ipv6 pool 2010::21 2010::26
    set key secret
    set mode spanned-etherchannel
    set name cisco
    set virtual ipv4 172.16.4.222 mask 255.255.0.0
    set virtual ipv6 2010::134 prefix-length 64
  exit
  enter external-port-link Ethernet1-2 Ethernet1/2 asa
    set decorator vdp
    set description ""
  exit
  enter external-port-link Ethernet1-3_asa Ethernet1/3 asa
    set decorator ""
    set description ""
  exit
  enter external-port-link mgmt_asa Ethernet1/1 asa
    set decorator ""
    set description ""
  exit

```

```

enter external-port-link mgmt_vdp Ethernet1/1 vdp
    set decorator ""
    set description ""
exit
enter external-port-link port-channel48 Port-channel48 asa
    set decorator ""
    set description ""
exit
enter mgmt-bootstrap vdp
    enter ipv4 1 default
        set gateway 172.16.0.1
        set ip 172.16.4.219 mask 255.255.0.0
    exit

    enter ipv4 2 default
        set gateway 172.16.0.1
        set ip 172.16.4.220 mask 255.255.0.0
    exit

    enter ipv4 3 default
        set gateway 172.16.0.1
        set ip 172.16.4.221 mask 255.255.0.0
    exit
exit
commit-buffer
scope ssa
    scope slot 1
    scope app-instance vdp
    show app-attri
    App Attribute:
        App Attribute Key: cluster-role
        Value: unknown

```

What to do next

Set a password for the DefensePro application. Note that the application does not come online until you set a password. For more information, see the Radware DefensePro DDoS Mitigation User Guide on [cisco.com](https://www.cisco.com).

Open UDP/TCP Ports and Enable vDP Web Services

The Radware APSolute Vision Manager interfaces communicate with the Radware vDP application using various UDP/TCP ports. In order for the vDP application to communicate with the APSolute Vision Manager, you must ensure that these ports are accessible and not blocked by your firewall. For more information on which specific ports to open, see the following tables in the APSolute Vision User Guide:

- **Ports for APSolute Vision Server-WBM Communication and Operating System**
- **Communication Ports for APSolute Vision Server with Radware Devices**

In order for Radware APSolute Vision to manage the Virtual DefensePro application deployed on the FXOS chassis, you must enable the vDP web service using the FXOS CLI.

Procedure

-
- Step 1** From the FXOS CLI, connect to the vDP application instance.


```
connect module slot console
```

```
connect vdp
```

Step 2 Enable vDP web services.

```
manage secure-web status set enable
```

Step 3 Exit the vDP application console and return to the FXOS module CLI.

```
Ctrl ]
```

Configure TLS Crypto Acceleration

The following topics discuss TLS crypto acceleration, how to enable it, and how to view its status using the FMCr.

The following table maps the Firepower Threat Defense and the FXOS version with the required TSL Crypto:



Note When FXOS 2.6.1 is upgraded to FXOS 2.7.x and above, FTD 6.4 does not automatically enable crypto as 6.4 is not compatible with TLS crypto.

FTD	FXOS	Crypto
6.4	2.6	Support for only one container instance (Phase 1)
6.4	2.7 and above	NA
6.5 and above	2.7 and above	Support for upto 16 container instances (Phase 2)

About TLS Crypto Acceleration

The Firepower 4100/9300 support Transport Layer Security cryptographic acceleration, which performs Transport Layer Security/Secure Sockets Layer (TLS/SSL) encryption and decryption in hardware, which greatly accelerates the following:

- TLS/SSL encryption and decryption
- VPN, including TLS/SSL and IPsec

TLS cryptographic acceleration is automatically enabled on native instances and cannot be disabled. You can enable TLS crypto acceleration on 1 FTD container instance per security engine/module as well.

Guidelines and Limitations for TLS Crypto Acceleration

Keep the following in mind if your Firepower Threat Defense has TLS crypto acceleration enabled.

Inspection engine failure

If the inspection engine is configured to preserve connections and the inspection engine fails unexpectedly, TLS/SSL traffic is dropped until the engine restarts.

This behavior is controlled by the Firepower Threat Defense command **configure snort preserve-connection {enable | disable}** command.

HTTP-only performance

Using TLS crypto acceleration on an FTD container instance that is not decrypting traffic can affect performance. We recommend you enable TLS crypto acceleration *only* on FTD container instances that decrypt TLS/SSL traffic.

Federal Information Processing Standards (FIPS)

If TLS crypto acceleration and Federal Information Processing Standards (FIPS) are both enabled, connections with the following options fail:

- RSA keys less than 2048 bytes in size
- Rivest cipher 4 (RC4)
- Single Data Encryption Standard (single DES)
- Merkle–Damgård 5 (MD5)
- SSL v3

FIPS is enabled when you configure the FMC and Firepower Threat Defenses to operate in a security certifications compliance mode. To allow connections when operating in those modes, you can either disable TLS crypto acceleration on the FTD container instance or you can configure web browsers to accept more secure options.

For more information:

- [Common Criteria](#).

High Availability (HA) and clustering

If you have high availability (HA) or clustered Firepower Threat Defenses, you must enable TLS crypto acceleration on each Firepower Threat Defense individually. One device's TLS crypto acceleration configuration is not shared with the other devices in the HA pair or cluster.

TLS heartbeat

Some applications use the *TLS heartbeat* extension to the Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) protocols defined by [RFC6520](#). TLS heartbeat provides a way to confirm the connection is still alive—either the client or server sends a specified number of bytes of data and requests the other party echo the response. If this is successful, encrypted data is sent.

When an Firepower Threat Defense managed by FMC with TLS crypto acceleration enabled encounters a packet that uses the TLS heartbeat extension, the Firepower Threat Defense takes the action specified by the FMC setting for **Decryption Errors** in the SSL policy's **Undecryptable Actions**:

- Block

- Block with reset

To determine whether applications are using TLS heartbeat, see the chapter on troubleshooting TLS/SSL rules in the *Firepower Management Center Configuration Guide*.

If TLS crypto acceleration is disabled on an FTD container instance, you can configure a **Max Heartbeat Length** in a Network Analysis Policy (NAP) in the FMC to determine how to handle TLS heartbeats.

For more information about TLS heartbeat, see the chapter on troubleshooting TLS/SSL rules in the *Firepower Management Center Configuration Guide*.

TLS/SSL oversubscription

TLS/SSL oversubscription is a state where an Firepower Threat Defense is overloaded with TLS/SSL traffic. Any Firepower Threat Defense can experience TLS/SSL oversubscription but only the Firepower Threat Defenses that support TLS crypto acceleration provide a configurable way to handle it.

When an Firepower Threat Defense managed by an FMC with TLS crypto acceleration enabled is oversubscribed, any packet received by the Firepower Threat Defense is acted on according to the setting for **Handshake Errors** in the SSL policy's **Undecryptable Actions**:

- Inherit default action
- Do not decrypt
- Block
- Block with reset

If the setting for **Handshake Errors** in the SSL policy's **Undecryptable Actions** is **Do Not decrypt** and the associated access control policy is configured to inspect the traffic, inspection occurs; decryption does *not* occur.

If a significant amount of oversubscription is occurring, you have the following options:

- Upgrade to an Firepower Threat Defense with more TLS/SSL processing capacity.
- Change your SSL policies to add **Do Not Decrypt** rules for traffic that is not a high priority to decrypt.

For more information about TLS oversubscription, see the chapter on troubleshooting TLS/SSL rules in the *Firepower Management Center Configuration Guide*.

Passive and inline tap sets not supported

TLS/SSL traffic cannot be decrypted on passive or inline tap set interfaces when TLS crypto acceleration is enabled.

Enable TLS Crypto Acceleration on One Container Instance

You can enable TLS crypto acceleration on one FTD container instance and disable it using the commands discussed in this section.

Procedure

Step 1 Show configured application instances.

scope ssa

show app-instance

exit

Example:

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

App Name	Identifier	Slot	ID	Admin State	Oper State	Running Version	Startup Version	
Deploy Type	Profile	Name	Cluster	State	Cluster Role			
ftd	container1	1		Enabled	Online	6.4.0	6.4.0	Container
	Default-Small	Not	Applicable	None				
ftd	LD2	1		Enabled	Online	6.4.0	6.4.0	Container
	Default-Small	Not	Applicable	None				
ftd	LD3	1		Enabled	Online	6.4.0	6.4.0	Container
	Default-Small	Not	Applicable	None				
ftd	LD4	1		Enabled	Online	6.4.0	6.4.0	Container
	Default-Small	Not	Applicable	None				

```
Firepower /ssa # exit
```

Step 2 Connect to the module CLI using a console connection or a Telnet connection.

connect module *slot_number* {console | telnet}

To connect to the security engine of a device that does not support multiple security modules, always use **1** as the *slot_number*.

The benefits of using a Telnet connection is that you can have multiple sessions to the module at the same time, and the connection speed is faster.

Example:

```
Firepower-9300# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
```

```
CISCO Serial Over LAN:
Close Network Connection to Exit
```

```
Firepower-module1>
```

Step 3 Enable TLS crypto acceleration on a container instance.

config hwCrypto enable *instance*

To disable it, use the **config hwCrypto disable** command.

Example:

```
config hwCrypto enable container1
```

```
WARNING!!: This command will restart the container instance. Are you sure ? [yes/NO] yes
Restarting container instance cisco-ftd.6.4.0__ftd_002_JMX1950196HL633VW108
to enable hardware crypto .... it will take some time.
```

Example

Following is an example of enabling TLS crypto acceleration on an FTD container instance named **container1** on module 1 with prompting to restart the instance:

```
Firepower-module1>scope ssa
/ssa # show app-instance
```

App Name	Identifier	Slot ID	Admin State	Oper State	Running Version	Startup Version
Deploy Type	Profile Name	Cluster	State	Cluster Role		
ftd	container1	1	Enabled	Online	6.4.0	6.4.0
Default-Small	Not Applicable	None				Container
ftd	LD2	1	Enabled	Online	6.4.0	6.4.0
Default-Small	Not Applicable	None				Container
ftd	LD3	1	Enabled	Online	6.4.0	6.4.0
Default-Small	Not Applicable	None				Container
ftd	LD4	1	Enabled	Online	6.4.0	6.4.0
Default-Small	Not Applicable	None				Container

```
/ssa # exit
```

```
Firepower-module1>connect module 1 console
Firepower-module1>config hwCrypto enable container1
```

```
WARNING!!: This command will restart the container instance. Are you sure ? [yes/NO] yes
Restarting container instance cisco-ftd.6.4.0__ftd_002_JMX1950196HL633VW108
to enable hardware crypto .... it will take some time.
```

Following is an example of disabling TLS crypto acceleration with prompting to restart the instance:

```
Firepower-module1>scope ssa
/ssa # show app-instance
```

App Name	Identifier	Slot ID	Admin State	Oper State	Running Version	Startup Version
Deploy Type	Profile Name	Cluster	State	Cluster Role		
ftd	container1	1	Enabled	Online	6.4.0	6.4.0
Default-Small	Not Applicable	None				Container
ftd	LD2	1	Enabled	Online	6.4.0	6.4.0
Default-Small	Not Applicable	None				Container
ftd	LD3	1	Enabled	Online	6.4.0	6.4.0
Default-Small	Not Applicable	None				Container
ftd	LD4	1	Enabled	Online	6.4.0	6.4.0
Default-Small	Not Applicable	None				Container

```
/ssa # exit
```

```
Firepower-module1>connect module 1 console
Firepower-module1>config hwCrypto disable
```

```
WARNING!!!: Hardware crypto will be disabled from container identifier container1.
WARNING!!!: Container instance container1 will be restarted. Are you sure ? [yes/NO] yes
Removing Hardware Crypto from Container identifier container1..
Restarting container instance cisco-ftd.6.4.0__ftd_002_JMX1950196HL633VW108 to disable
hardware crypto for identifier container1 ..... it will take some time.
```

View the Status of TLS Crypto Acceleration

This topic discusses how you can determine if TLS crypto acceleration is enabled.

Perform the following task in the FMC.

Procedure

-
- Step 1** Log in to the FMC.
 - Step 2** Click **Devices** > **Device Management**.
 - Step 3** Click **Edit** () to edit a managed device.
 - Step 4** Click **Device** page. TLS crypto acceleration status is displayed in the General section.
-

Manage Logical Devices

You can delete a logical device, convert an ASA to transparent mode, change the interface configuration, and perform other tasks on existing logical devices.

Connect to the Console of the Application

Use the following procedure to connect to the console of the application.

Procedure

-
- Step 1** Connect to the module CLI using a console connection or a Telnet connection.
connect module *slot_number* { console | telnet }
 To connect to the security engine of a device that does not support multiple security modules, always use **1** as the *slot_number*.
 The benefits of using a Telnet connection is that you can have multiple sessions to the module at the same time, and the connection speed is faster.
Example:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
```

```
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

Step 2 Connect to the application console. Enter the appropriate command for your device.

connect asa *name*

connect ftd *name*

connect vdp *name*

To view the instance names, enter the command without a name.

Example:

```
Firepower-module1> connect asa asal
Connecting to asa(asal) console... hit Ctrl + A + D to return to bootCLI
[...]
asa>
```

Example:

```
Firepower-module1> connect ftd ftd1
Connecting to ftd(ftd-native) console... enter exit to return to bootCLI
[...]
>
```

Step 3 Exit the application console to the FXOS module CLI.

- ASA—Enter **Ctrl-a, d**
- FTD—Enter **exit**
- vDP—Enter **Ctrl-], .**

Step 4 Return to the supervisor level of the FXOS CLI.

Exit the console:

- Enter **~**
You exit to the Telnet application.
- To exit the Telnet application, enter:
telnet>quit

Exit the Telnet session:

- Enter **Ctrl-], .**

Example

The following example connects to an ASA on security module 1 and then exits back to the supervisor level of the FXOS CLI.

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect asa asa1
asa> ~
telnet> quit
Connection closed.
Firepower#
```

Delete a Logical Device

Procedure

-
- | | |
|---------------|--|
| Step 1 | Enter security services mode:
Firepower# scope ssa |
| Step 2 | View details for the logical devices on the chassis:
Firepower /ssa # show logical-device |
| Step 3 | For each logical device that you want to delete, enter the following command:
Firepower /ssa # delete logical-device <i>device_name</i> |
| Step 4 | View details for the applications installed on the logical devices:
Firepower /ssa # show app-instance |
| Step 5 | For each application that you want to delete, enter the following commands:
a) Firepower /ssa # scope slot <i>slot_number</i>
b) Firepower /ssa/slot # delete app-instance <i>application_name</i>
c) Firepower /ssa/slot # exit |
| Step 6 | Commit the configuration:
commit-buffer
Commits the transaction to the system configuration. |
-

Example

```
Firepower# scope ssa
Firepower /ssa # show logical-device
```

Logical Device:

Name	Description	Slot ID	Mode	Operational State	Template Name
FTD		1,2,3	Clustered	Ok	ftd

```
Firepower /ssa # delete logical-device FTD
Firepower /ssa* # show app-instance
```

Application Name	Slot ID	Admin State	Operational State	Running Version	Startup Version
ftd	1	Disabled	Stopping	6.0.0.837	
ftd	2	Disabled	Offline	6.0.0.837	
ftd	3	Disabled	Not Available		

```
Firepower /ssa* # scope slot 1
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # scope slot 2
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # scope slot 3
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # commit-buffer
```

Remove a Cluster Node

The following sections describe how to remove nodes temporarily or permanently from the cluster.

Temporary Removal

A cluster node will be automatically removed from the cluster due to a hardware or network failure, for example. This removal is temporary until the conditions are rectified, and it can rejoin the cluster. You can also manually disable clustering.

To check whether a device is currently in the cluster, check the cluster status within the application using the **show cluster info** command:

```
ciscoasa# show cluster info
Clustering is not enabled
```

For FTD using the FMC, you should leave the device in the FMC device list so that it can resume full functionality after you reenable clustering.

- **Disable clustering in the application**—You can disable clustering using the application CLI. Enter the **cluster remove unit name** command to remove any node other than the one you are logged into. The bootstrap configuration remains intact, as well as the last configuration synced from the control node, so you can later re-add the node without losing your configuration. If you enter this command on a data node to remove the control node, a new control node is elected.

When a device becomes inactive, all data interfaces are shut down; only the Management interface can send and receive traffic. To resume traffic flow, re-enable clustering. The Management interface remains up using the IP address the node received from the bootstrap configuration. However if you reload, and the node is still inactive in the cluster, the Management interface is disabled.

To reenabling clustering, on the ASA enter **cluster group name** and then **enable**. To reenabling clustering, on the FTD enter **cluster enable**.

- Disable the application instance—At the FXOS CLI, see the following example:

```
Firepower-chassis# scope ssa
Firepower-chassis /ssa # scope slot 1
Firepower-chassis /ssa/slot # scope app-instance asa asal
Firepower-chassis /ssa/slot/app-instance # disable
Firepower-chassis /ssa/slot/app-instance* # commit-buffer
Firepower-chassis /ssa/slot/app-instance #
```

To reenabling:

```
Firepower-chassis /ssa/slot/app-instance # enable
Firepower-chassis /ssa/slot/app-instance* # commit-buffer
Firepower-chassis /ssa/slot/app-instance #
```

- Shut down the security module/engine—At the FXOS CLI, see the following example:

```
Firepower-chassis# scope service-profile server 1/1
Firepower-chassis /org/service-profile # power down soft-shut-down
Firepower-chassis /org/service-profile* # commit-buffer
Firepower-chassis /org/service-profile #
```

To power up:

```
Firepower-chassis /org/service-profile # power up
Firepower-chassis /org/service-profile* # commit-buffer
Firepower-chassis /org/service-profile #
```

- Shut down the chassis—At the FXOS CLI, see the following example:

```
Firepower-chassis# scope chassis 1
Firepower-chassis /chassis # shutdown no-prompt
```

Permanent Removal

You can permanently remove a cluster node using the following methods.

For FTD using the FMC, be sure to remove the node from the FMC device list after you disable clustering on the chassis.

- Delete the logical device—At the FXOS CLI, see the following example:

```
Firepower-chassis# scope ssa
Firepower-chassis /ssa # delete logical-device cluster1
Firepower-chassis /ssa* # commit-buffer
```

```
Firepower-chassis /ssa #
```

- Remove the chassis or security module from service—If you remove a device from service, you can add replacement hardware as a new node of the cluster.

Delete an Application Instance that is not Associated with a Logical Device

When you delete a logical device, you are prompted as to whether you want to also delete the application configuration for the logical device. If you do not delete the application configuration, you will not be able to create a logical device using a different application until that application instance is deleted. You can use the following procedure to delete an application instance from a security module/engine when it is no longer associated with a logical device.

Procedure

-
- Step 1** Enter security services mode:
- ```
Firepower# scope ssa
```
- Step 2** View details for the installed applications:
- ```
Firepower /ssa # show app-instance
```
- Step 3** For each application that you want to delete, enter the following commands:
- Firepower /ssa # **scope slot** *slot_number*
 - Firepower /ssa/slot # **delete app-instance** *application_name*
 - Firepower /ssa/slot # **exit**
- Step 4** Commit the configuration:
- ```
commit-buffer
```
- Commits the transaction to the system configuration.
- 

### 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 Stopping 6.0.0.837
6.0.0.837 Not Applicable
ftd 2 Disabled Offline 6.0.0.837
6.0.0.837 Not Applicable
ftd 3 Disabled Not Available
6.0.0.837 Not Applicable
Firepower /ssa* # scope slot 1
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # scope slot 2
```

```
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # scope slot 3
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # commit-buffer
```

## Change an Interface on a FTD Logical Device

You can allocate or unallocate an interface on the Firepower Threat Defense logical device. You can then sync the interface configuration in the FMCthe .

Adding a new interface, or deleting an unused interface has minimal impact on the Firepower Threat Defense configuration. However, deleting an interface that is used in your security policy will impact the configuration. Interfaces can be referenced directly in many places in the Firepower Threat Defense configuration, including access rules, NAT, SSL, identity rules, VPN, DHCP server, and so on. Policies that refer to security zones are not affected. You can also edit the membership of an allocated EtherChannel without affecting the logical device or requiring a sync on the FMCthe .

Deleting an interface will delete any configuration associated with that interface.

### Before you begin

- Configure your interfaces, and add any EtherChannels according to [Configure a Physical Interface, on page 195](#) and [Add an EtherChannel \(Port Channel\), on page 197](#).
- If you want to add an already-allocated interface to an EtherChannel (for example, all interfaces are allocated by default to a cluster), you need to unallocate the interface from the logical device first, then add the interface to the EtherChannel. For a new EtherChannel, you can then allocate the EtherChannel to the device.
- For clustering or High Availability, make sure you add or remove the interface on all units before you sync the configuration in the FMCthe . We recommend that you make the interface changes on the data/standby unit(s) first, and then on the control/active unit. Note that new interfaces are added in an administratively down state, so they do not affect interface monitoring.
- In mult-instance mode, for changing a sub-interface with an another sub-interface with the same vlan tag, you must first remove all the configuration (including nameif config) of the interface and then unalloacte the interface from Firepower Chassis Manager. Once unallocated, add the new interface and then use sync interfaces from the FMC.

### Procedure

- 
- Step 1** Enter security services mode:
- ```
Firepower# scope ssa
```
- Step 2** Edit the logical device:
- ```
Firepower /ssa # scope logical-device device_name
```
- Step 3** Allocate a new interface to the logical device:

```
Firepower /ssa/logical-device* # create external-port-link name interface_id ftd
```

Do not delete any interfaces yet.

**Step 4** Commit the configuration:

**commit-buffer**

Commits the transaction to the system configuration.

**Step 5** Sync the interfaces in the FMC.

a) Log into the FMC.

b) Select **Devices > Device Management** and click **Edit** () for your Firepower Threat Defense device. The **Interfaces** page is selected by default.

c) Click the **Sync Device** button on the top left of the **Interfaces** page.

d) After the changes are detected, you will see a red banner on the **Interfaces** page indicating that the interface configuration has changed. Click the **Click to know more** link to view the interface changes.

e) If you plan to delete an interface, manually transfer any interface configuration from the old interface to the new interface.

Because you have not yet deleted any interfaces, you can refer to the existing configuration. You will have additional opportunity to fix the configuration after you delete the old interface and re-run the validation. The validation will show you all locations in which the old interface is still used.

f) Click **Validate Changes** to make sure your policy will still work with the interface changes.

If there are any errors, you need to change your policy and rerun the validation.

g) Click **Save**.

h) Select the devices and click **Deploy** to deploy the policy to the assigned devices. The changes are not active until you deploy them.

**Step 6** In FXOS, unallocate an interface from the logical device:

```
Firepower /ssa/logical-device # delete external-port-link name
```

Enter the **show external-port-link** command to view interface names.

**Step 7** Commit the configuration:

**commit-buffer**

Commits the transaction to the system configuration.

**Step 8** Sync the interfaces again in the FMCthe .

---

## Change an Interface on an ASA Logical Device

You can allocate, unallocate, or replace a management interface on an ASA logical device. ASDM discovers the new interfaces automatically.

Adding a new interface, or deleting an unused interface has minimal impact on the ASA configuration. However, if you remove an allocated interface in FXOS (for example, if you remove a network module, remove an EtherChannel, or reassign an allocated interface to an EtherChannel), and the interface is used in your security policy, removal will impact the ASA configuration. In this case, the ASA configuration retains

the original commands so that you can make any necessary adjustments. You can manually remove the old interface configuration in the ASA OS.




---

**Note** You can edit the membership of an allocated EtherChannel without impacting the logical device.

---

### Before you begin

- Configure your interfaces and add any EtherChannels according to [Configure a Physical Interface, on page 195](#) and [Add an EtherChannel \(Port Channel\), on page 197](#).
- If you want to add an already-allocated interface to an EtherChannel (for example, all interfaces are allocated by default to a cluster), you need to unallocate the interface from the logical device first, then add the interface to the EtherChannel. For a new EtherChannel, you can then allocate the EtherChannel to the device.
- For clustering or failover, make sure you add or remove the interface on all units. We recommend that you make the interface changes on the data/standby unit(s) first, and then on the control/active unit. New interfaces are added in an administratively down state, so they do not affect interface monitoring.

### Procedure

- 
- Step 1** Enter security services mode:
- ```
Firepower# scope ssa
```
- Step 2** Edit the logical device:
- ```
Firepower /ssa # scope logical-device device_name
```
- Step 3** Unallocate an interface from the logical device:
- ```
Firepower /ssa/logical-device # delete external-port-link name
```
- Enter the **show external-port-link** command to view interface names.
- For a management interface, delete the current interface then commit your change using the **commit-buffer** command before you add the new management interface.
- Step 4** Allocate a new interface to the logical device:
- ```
Firepower /ssa/logical-device* # create external-port-link name interface_id asa
```
- Step 5** Commit the configuration:
- ```
commit-buffer
```
- Commits the transaction to the system configuration.
-

Monitoring Logical Devices

• show app

View available images.

```
Firepower# scope ssa
Firepower /ssa # show app
```

Name	Version	Author	Supported Deploy Types	CSP Type	Is Default
asa	9.10.1	cisco	Native	Application	Yes
ftd	6.3.0	cisco	Native, Container	Application	Yes
ftd	6.2.3	cisco	Native	Application	Yes
vdp	8.13.01.09-2	radware	Vm	Application	Yes

• show app-instance

View the application instance status and information.

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

App Name	Identifier	Slot ID	Admin State	Oper State	Running Version	Startup Version
ftd	LD1	1	Enabled	Online	6.4.0.10353	6.4.0.10353
	Container	Default-Small	Not Applicable	None		
ftd	LD2	1	Enabled	Online	6.4.0.10353	6.4.0.10353
	Container	Default-Small	Not Applicable	None		
ftd	LD3	1	Enabled	Online	6.4.0.10353	6.4.0.10353
	Container	Default-Small	Not Applicable	None		
ftd	LD4	1	Enabled	Online	6.4.0.10353	6.4.0.1056
	Container	Default-Small	Not Applicable	None		

• show logical-device

View details for logical devices.

```
Firepower# scope ssa
Firepower /ssa # show logical-device
```

Name	Description	Slot ID	Mode	Oper State	Template Name
asa1		1	Standalone	Ok	asa

• show resource-profile system

Show resource profiles for vDP.

```
Firepower# scope ssa
Firepower /ssa # show resource-profile system
```

```

Profile Name      App Name  App Version  Is In Use  Security Model  CPU Logical Core
Count RAM Size (MB)  Default Profile Profile Type Description
-----
DEFAULT-4110-RESOURCE
      vdp      8.13.01.09-2 No      FPR4K-SM-12
      4      16384 Yes      System
DEFAULT-RESOURCE  vdp      8.13.01.09-2 No      FPR9K-SM-56, FPR9K-SM-44,
FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24
      6      24576 Yes      System
VDP-10-CORES      vdp      8.13.01.09-2 No      FPR9K-SM-56, FPR9K-SM-44,
FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24
      10     40960 No      System
VDP-2-CORES      vdp      8.13.01.09-2 No      all
      2      8192 No      System
VDP-4-CORES      vdp      8.13.01.09-2 No      all
      4      16384 No      System
VDP-8-CORES      vdp      8.13.01.09-2 No      FPR9K-SM-56, FPR9K-SM-44,
FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24
      8      32768 No      System

```

- **show resource-profile user-defined**

View container instance resource profile assignments.

```

Firepower# scope ssa
Firepower /ssa # show resource-profile user-defined
Profile Name      Is In Use  CPU Logical Core Count Description
-----
bronze            No         6                low end device
gold              No         14               highest
silver            No         8                mid-level

```

- **show resource detail**

View resource allocation for the application instance.

```

Firepower# scope ssa
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd ftd1
Firepower /ssa/slot/app-instance # show resource detail
Resource:
  Allocated Core NR: 10
  Allocated RAM (MB): 32413
  Allocated Data Disk (MB): 49152
  Allocated Binary Disk (MB): 3907
  Allocated Secondary Disk (MB): 0

```

Examples for Inter-Site Clustering

The following examples show supported cluster deployments.

Spanned EtherChannel Routed Mode Example with Site-Specific MAC Addresses

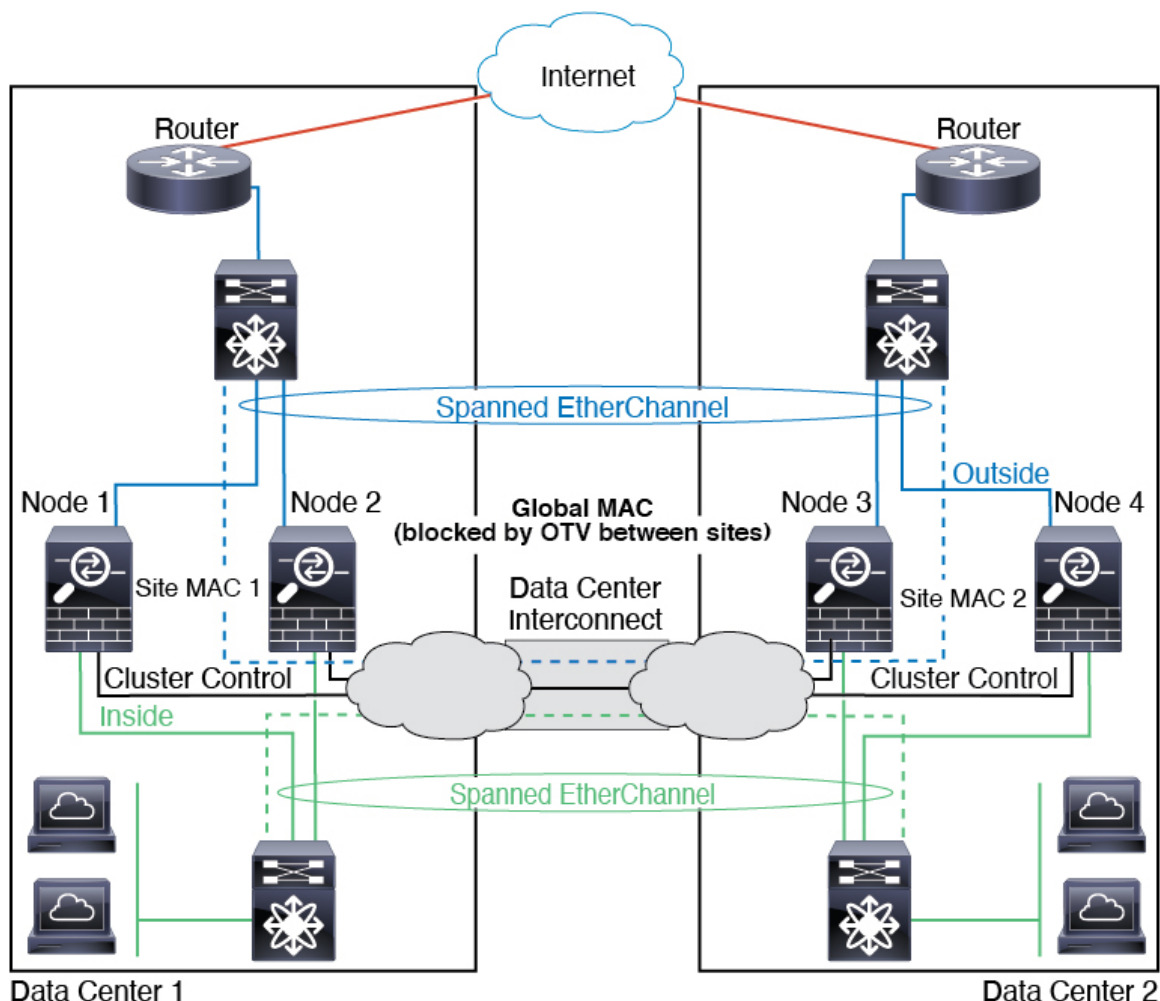
The following example shows 2 cluster members at each of 2 data centers placed between the gateway router and an inside network at each site (East-West insertion). The cluster members are connected by the cluster control link over the DCI. The cluster members at each site connect to the local switches using spanned EtherChannels for both the inside and outside networks. Each EtherChannel is spanned across all chassis in the cluster.

The data VLANs are extended between the sites using Overlay Transport Virtualization (OTV) (or something similar). You must add filters blocking the global MAC address to prevent traffic from traversing the DCI to the other site when the traffic is destined for the cluster. If the cluster nodes at one site become unreachable, you must remove the filters so traffic can be sent to the other site's cluster nodes. You should use VACLs to filter the global MAC address. Be sure to disable ARP inspection.

The cluster acts as the gateway for the inside networks. The global virtual MAC, which is shared across all cluster nodes, is used only to receive packets. Outgoing packets use a site-specific MAC address from each DC cluster. This feature prevents the switches from learning the same global MAC address from both sites on two different ports, which causes MAC flapping; instead, they only learn the site MAC address.

In this scenario:

- All egress packets sent from the cluster use the site MAC address and are localized at the data center.
- All ingress packets to the cluster are sent using the global MAC address, so they can be received by any of the nodes at both sites; filters at the OTV localize the traffic within the data center.



Spanned EtherChannel Transparent Mode North-South Inter-Site Example

The following example shows 2 cluster members at each of 2 data centers placed between inside and outside routers (North-South insertion). The cluster members are connected by the cluster control link over the DCI. The cluster members at each site connect to the local switches using spanned EtherChannels for the inside and outside. Each EtherChannel is spanned across all chassis in the cluster.

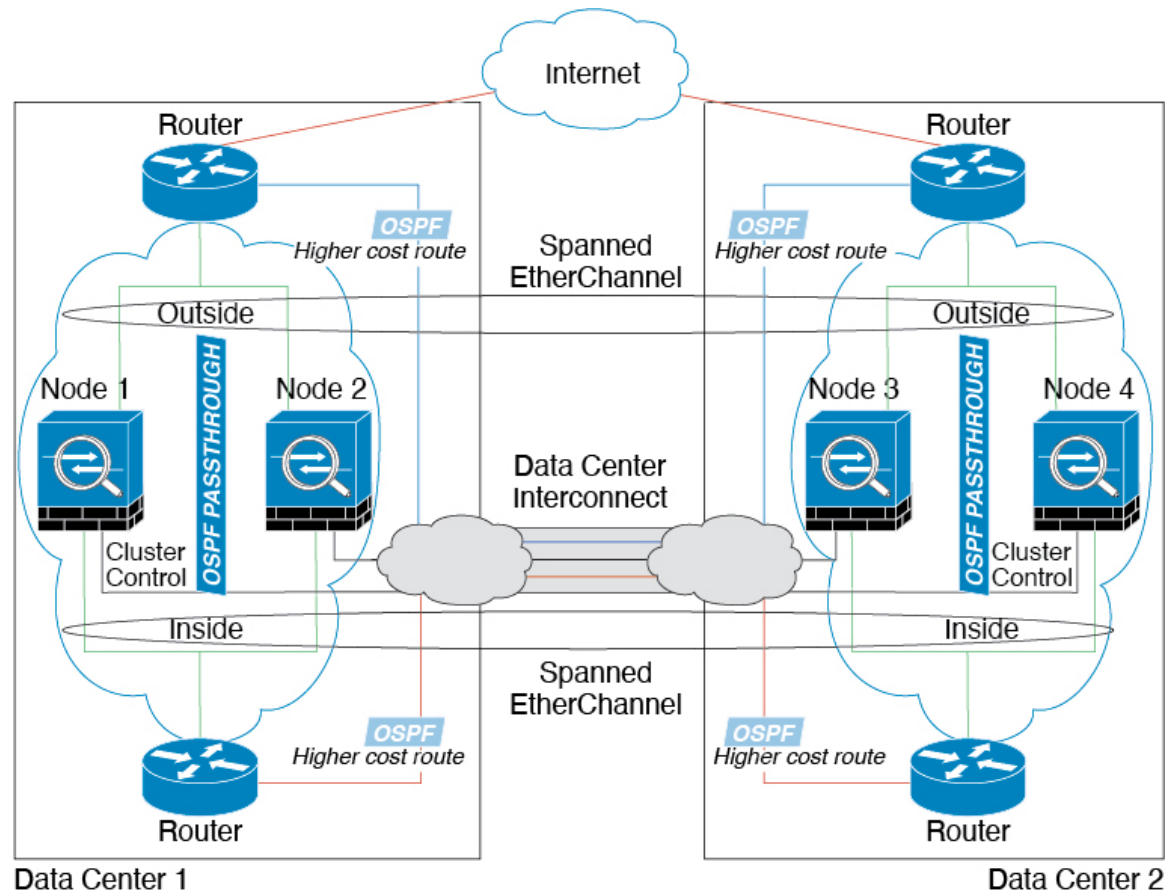
The inside and outside routers at each data center use OSPF, which is passed through the transparent ASAs. Unlike MACs, router IPs are unique on all routers. By assigning a higher cost route across the DCI, traffic stays within each data center unless all cluster members at a given site go down. The lower cost route through the ASAs must traverse the same bridge group at each site for the cluster to maintain asymmetric connections. In the event of a failure of all cluster members at one site, traffic goes from each router over the DCI to the cluster members at the other site.

The implementation of the switches at each site can include:

- Inter-site VSS, vPC, StackWise, or StackWise Virtual—In this scenario, you install one switch at Data Center 1, and the other at Data Center 2. One option is for the cluster nodes at each Data Center to only connect to the local switch, while the redundant switch traffic goes across the DCI. In this case, connections

are for the most part kept local to each datacenter. You can optionally connect each node to both switches across the DCI if the DCI can handle the extra traffic. In this case, traffic is distributed across the data centers, so it is essential for the DCI to be very robust.

- Local VSS, vPC, StackWise, or StackWise Virtual at each site—For better switch redundancy, you can install 2 separate redundant switch pairs at each site. In this case, although the cluster nodes still have a spanned EtherChannel with Data Center 1 chassis connected only to both local switches, and Data Center 2 chassis connected to those local switches, the spanned EtherChannel is essentially “split.” Each local redundant switch system sees the spanned EtherChannel as a site-local EtherChannel.

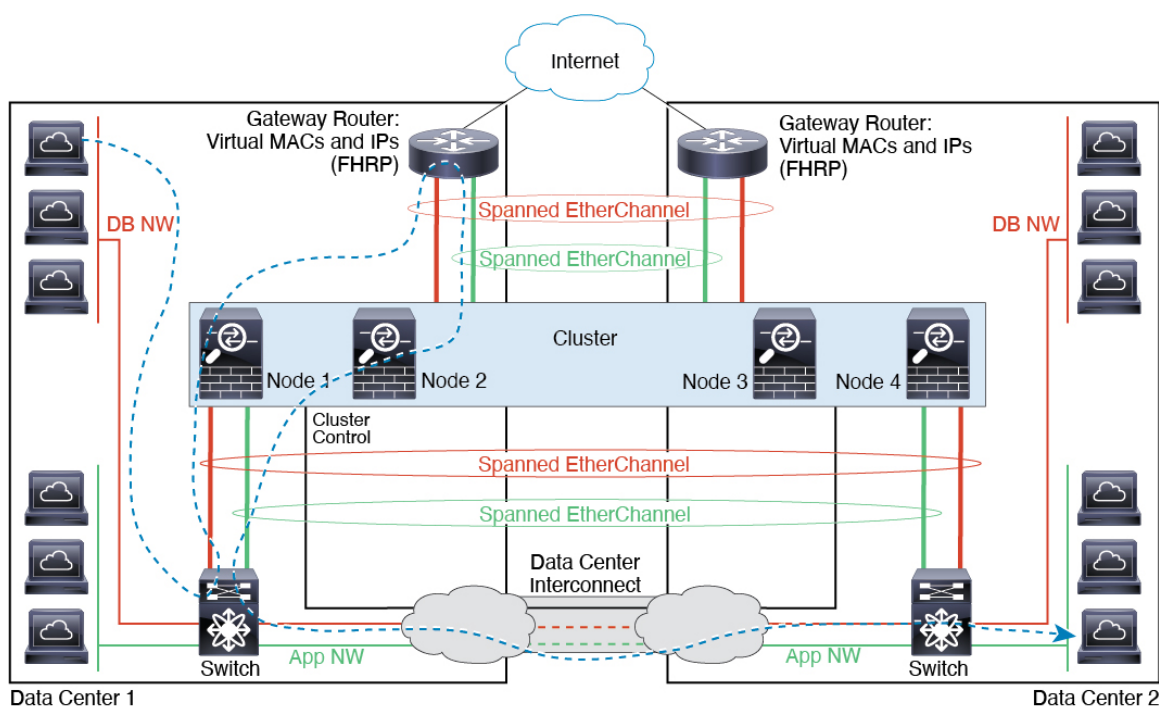


Spanned EtherChannel Transparent Mode East-West Inter-Site Example

The following example shows 2 cluster members at each of 2 data centers placed between the gateway router and two inside networks at each site, the App network and the DB network (East-West insertion). The cluster members are connected by the cluster control link over the DCI. The cluster members at each site connect to the local switches using spanned EtherChannels for both the App and DB networks on the inside and outside. Each EtherChannel is spanned across all chassis in the cluster.

The gateway router at each site uses an FHRP such as HSRP to provide the same destination virtual MAC and IP addresses at each site. A good practice to avoid unintended MAC address flapping is to statically add the gateway routers real MAC addresses to the ASA MAC address table using the **mac-address-table static outside_interface mac_address** command. Without these entries, if the gateway at site 1 communicates with

the gateway at site 2, that traffic might pass through the ASA and attempt to reach site 2 from the inside interface and cause problems. The data VLANs are extended between the sites using Overlay Transport Virtualization (OTV) (or something similar). You must add filters to prevent traffic from traversing the DCI to the other site when the traffic is destined for the gateway router. If the gateway router at one site becomes unreachable, you must remove the filters so traffic can be sent to the other site's gateway router.



History for Logical Devices

Feature Name	Platform Releases	Feature Information
Firepower 4115, 4125, and 4145	2.6.1	<p>We introduced the Firepower 4115, 4125, and 4145.</p> <p>Note Requires ASA 9.12(1). Firepower 6.4.0 requires FXOS 2.6.1.157.</p> <p>No modified commands.</p>
Firepower 9300 SM-40, SM-48, and SM-56 support	2.6.1	<p>We introduced the following three security modules: SM-40, SM-48, and SM-56.</p> <p>Note The SM-40 and SM-48 require ASA 9.12(1). The SM-56 requires ASA 9.12(2) and FXOS 2.6.1.157.</p> <p>All modules require Firepower Threat Defense 6.4 and FXOS 2.6.1.157.</p> <p>No modified commands.</p>

Feature Name	Platform Releases	Feature Information
Support for ASA and Firepower Threat Defense on separate modules of the same Firepower 9300	2.6.1	<p>You can now deploy ASA and Firepower Threat Defense logical devices on the same Firepower 9300.</p> <p>Note Requires ASA 9.12(1). Firepower 6.4.0 requires FXOS 2.6.1.157.</p> <p>No modified commands.</p>
For the Firepower Threat Defense bootstrap configuration, you can now set the NAT ID for the FMC in the Firepower Chassis Manager	2.6.1	<p>You can now set the FMC NAT ID in the Firepower Chassis Manager. Previously, you could only set the NAT ID within the FXOS CLI or Firepower Threat Defense CLI. Normally, you need both IP addresses (along with a registration key) for both routing purposes and for authentication: the FMC specifies the device IP address, and the device specifies the FMC IP address. However, if you only know one of the IP addresses, which is the minimum requirement for routing purposes, then you must also specify a unique NAT ID on both sides of the connection to establish trust for the initial communication and to look up the correct registration key. The FMC and device use the registration key and NAT ID (instead of IP addresses) to authenticate and authorize for initial registration.</p> <p>New/Modified screens:</p> <p>Logical Devices > Add Device > Settings > Firepower Management Center NAT ID field</p>
Support for SSL hardware acceleration on one Firepower Threat Defense container instance on a module/security engine	2.6.1	<p>You can now enable SSL hardware acceleration for one container instance on a module/security engine. SSL hardware acceleration is disabled for other container instances, but enabled for native instances. See the FMC configuration guide for more information.</p> <p>New/Modified commands: config hwCrypto enable, show hwCrypto</p>

Feature Name	Platform Releases	Feature Information
Multi-instance capability for Firepower Threat Defense	2.4.1	<p>You can now deploy multiple logical devices, each with a Firepower Threat Defense container instance, on a single security engine/module. Formerly, you could only deploy a single native application instance. Native instances are still also supported. For the Firepower 9300, you can use a native instance on some modules, and container instances on the other module(s).</p> <p>To provide flexible physical interface use, you can create VLAN subinterfaces in FXOS and also share interfaces between multiple instances. When you deploy a container instance, you must specify the number of CPU cores assigned; RAM is dynamically allocated according to the number of cores, and disk space is set to 40 GB per instance. This resource management lets you customize performance capabilities for each instance.</p> <p>You can use High Availability using a container instance on 2 separate chassis; for example, if you have 2 chassis, each with 10 instances, you can create 10 High Availability pairs. Clustering is not supported.</p> <p>Note Multi-instance capability is similar to ASA multiple context mode, although the implementation is different. Multiple context mode partitions a single application instance, while multi-instance capability allows independent container instances. Container instances allow hard resource separation, separate configuration management, separate reloads, separate software updates, and full Firepower Threat Defense feature support. Multiple context mode, due to shared resources, supports more contexts on a given platform. Multiple context mode is not available on the Firepower Threat Defense.</p> <p>Note Requires Firepower Threat Defense Version 6.3 or later.</p> <p>New/Modified FXOS commands: connect Firepower Threat Defense <i>name</i>, connect module telnet, create bootstrap-key PERMIT_EXPERT_MODE, create resource-profile, create subinterface, scope auto-macpool, set cpu-core-count, set deploy-type, set port-type data-sharing, set prefix, set resource-profile-name, set vlan, scope app-instance Firepower Threat Defense <i>name</i>, show cgroups container, show interface, show mac-address, show subinterface, show tech-support module app-instance, show version</p> <p>New/Modified FMC screens: Devices > Device Management > Edit icon > Interfaces tab</p>
Support for transparent mode deployment for an ASA logical device	2.4.1	<p>You can now specify transparent or routed mode when you deploy the ASA.</p> <p>New/Modified commands: enter bootstrap-key FIREWALL_MODE, set value routed, set value transparent</p>

Feature Name	Platform Releases	Feature Information
Cluster control link customizable IP Address	2.4.1	<p>By default, the cluster control link uses the 127.2.0.0/16 network. You can now set the network when you deploy the cluster in FXOS. The chassis auto-generates the cluster control link interface IP address for each unit based on the chassis ID and slot ID: <code>127.2.chassis_id.slot_id</code>. However, some networking deployments do not allow 127.2.0.0/16 traffic to pass. Therefore, you can now set a custom /16 subnet for the cluster control link in FXOS except for loopback (127.0.0.0/8) and multicast (224.0.0.0/4) addresses.</p> <p>New/Modified commands: set cluster-control-link network</p>
For the Firepower Threat Defense bootstrap configuration, you can now set the NAT ID for the FMC at the FXOS CLI	2.4.1	<p>You can now set the FMC NAT ID at the FXOS CLI. Previously, you could only set the NAT ID within the Firepower Threat Defense CLI. Normally, you need both IP addresses (along with a registration key) for both routing purposes and for authentication: the FMC specifies the device IP address, and the device specifies the FMC IP address. However, if you only know one of the IP addresses, which is the minimum requirement for routing purposes, then you must also specify a unique NAT ID on both sides of the connection to establish trust for the initial communication and to look up the correct registration key. The FMC and device use the registration key and NAT ID (instead of IP addresses) to authenticate and authorize for initial registration.</p> <p>New/Modified commands: enter bootstrap-key NAT_ID</p>
Inter-site clustering improvement for the ASA	2.1.1	<p>You can now configure the site ID for each Firepower 4100/9300 chassis when you deploy the ASA cluster. Previously, you had to configure the site ID within the ASA application; this new feature eases initial deployment. Note that you can no longer set the site ID within the ASA configuration. Also, for best compatibility with inter-site clustering, we recommend that you upgrade to ASA 9.7(1) and FXOS 2.1.1, which includes several improvements to stability and performance.</p> <p>We modified the following command: set site-id</p>
Inter-chassis clustering for 6 Firepower Threat Defense modules on the Firepower 9300	2.1.1	<p>You can now enable inter-chassis clustering for the Firepower Threat Defense on the Firepower 9300. You can include up to 6 modules. For example, you can use 1 module in 6 chassis, or 2 modules in 3 chassis, or any combination that provides a maximum of 6 modules.</p>
Support for Firepower Threat Defense clustering on the Firepower 4100	2.1.1	<p>You can cluster up to 6 chassis in an Firepower Threat Defense cluster.</p>
Support for 16 Firepower 4100 chassis in an ASA cluster	2.0.1	<p>You can cluster up to 16 chassis in an ASA cluster.</p>
Support for ASA clustering on the Firepower 4100	1.1.4	<p>You can cluster up to 6 chassis in an ASA cluster.</p>

Feature Name	Platform Releases	Feature Information
Support for intra-chassis clustering on the Firepower Threat Defense on the Firepower 9300	1.1.4	<p>The Firepower 9300 supports intra-chassis clustering with the Firepower Threat Defense application.</p> <p>We introduced the following commands: enter mgmt-bootstrap Firepower Threat Defense, enter bootstrap-key FIREPOWER_MANAGER_IP, enter bootstrap-key FIREWALL_MODE, enter bootstrap-key-secret REGISTRATION_KEY, enter bootstrap-key-secret PASSWORD, enter bootstrap-key FQDN, enter bootstrap-key DNS_SERVERS, enter bootstrap-key SEARCH_DOMAINS, enter ipv4 firepower, enter ipv6 firepower, set value, set gateway, set ip, accept-license-agreement</p>
Inter-chassis clustering for 16 ASA modules on the Firepower 9300	1.1.3	<p>You can now enable inter-chassis clustering for the ASA. You can include up to 16 modules. For example, you can use 1 module in 16 chassis, or 2 modules in 8 chassis, or any combination that provides a maximum of 16 modules.</p>
Intra-chassis Clustering for the ASA on the Firepower 9300	1.1.1	<p>You can cluster all ASA security modules within the Firepower 9300 chassis.</p> <p>We introduced the following commands: enter cluster-bootstrap, enter logical-device clustered, set chassis-id, set ipv4 gateway, set ipv4 pool, set ipv6 gateway, set ipv6 pool, set key, set mode spanned-etherchannel, set port-type cluster, set service-type, set virtual ipv4, set virtual ipv6</p>



CHAPTER 12

Security Module/Engine Management

- [About FXOS Security Modules/Security Engine, on page 313](#)
- [Decommissioning a Security Module, on page 314](#)
- [Acknowledge a Security Module/Engine, on page 314](#)
- [Power-Cycling a Security Module/Engine, on page 315](#)
- [Reinitializing a Security Module/Engine, on page 316](#)
- [Acknowledge a Network Module, on page 317](#)
- [Taking a Network Module Offline or Online, on page 317](#)
- [Blade Health Monitoring, on page 319](#)

About FXOS Security Modules/Security Engine

You can use the FXOS CLI to perform the following functions on a security module/engine:

- **Decommission (security modules only)**—Decommissioning a security module places the security module into maintenance mode. You can also decommission and then acknowledge a security module in order to correct certain fault states. See [Decommissioning a Security Module, on page 314](#).
- **Acknowledge**—Brings newly installed security modules online. See [Acknowledge a Security Module/Engine, on page 314](#).
- **Power Cycle**—Restarts the security module/engine. See [Power-Cycling a Security Module/Engine, on page 315](#).
- **Reinitialize**—Reformats the security module/engine hard disk, removing all deployed applications and configurations from the security module/engine, and then restarts the system. After reinitialization is complete, if a logical device is configured for the security module/engine, the FXOS will reinstall the application software, redeploy the logical device, and auto start the application. See [Reinitializing a Security Module/Engine, on page 316](#).



Warning

All application data on the security module/engine is deleted during reinitialization. Please back up all application data before reinitializing a security module/engine.

- **Power off/on**—Toggles the power state for the security module/engine. See [Power-Cycling a Security Module/Engine, on page 315](#).

Decommissioning a Security Module

When you decommission a security module, the security module object is deleted from the configuration and the security module becomes unmanaged. Any logical devices or software running on the security module will become inactive.

You can decommission a security module if you want to temporarily discontinue use of the security module.



Note A module must be decommissioned before it can be deleted using the `delete decommissioned` command.

Procedure

Step 1 To decommission a module, enter the `decommission server` command:

```
decommission server {ID | chassis-id/blade-id}
```

Depending on the type of device hosting the module to be decommissioned, identify it using its module ID (4100 series), or the chassis number and the module number (9300 devices).

Example:

```
FP9300-A# decommission server 1/2
FP9300-A* #
```

Step 2 Enter the `commit-buffer` command to commit the change.

You can use the `show server decommissioned` command to view a list of decommissioned modules.

Acknowledge a Security Module/Engine

When a new security module is installed into the chassis, or when an existing module is replaced with one with a different product ID (PID), you must acknowledge the security module before you can begin using it.

If the security module is showing a status of “mismatch” or “token mismatch,” this is an indication that the security module installed in the slot has data on it that does not match what was previously installed in the slot. If the security module has existing data on it and you are sure you want to use it in the new slot (in other words, the security module wasn't inadvertently installed into the wrong slot), you must reinitialize the security module before you can deploy a logical device to it.

Procedure

Step 1 Enter `fabric-interconnect` mode:

```
scope fabric-interconnect
```

- Step 2** Enter the `acknowledge slot` command after decommissioning and physically removing a module that will not be replaced, or after replacing a module with another that is not the same type (that is, with a different PID):

```
acknowledge slot
```

Example:

```
FP9300-A# scope fabric-interconnect
FP9300-A /fabric-interconnect # acknowledge slot 2
FP9300-A /fabric-interconnect* #
```

- Step 3** Commit the configuration:

```
commit-buffer
```

Power-Cycling a Security Module/Engine

Follow these steps to power-cycle a security module/engine.

Procedure

- Step 1** Enter `/service-profile` mode:

```
scope service-profile server {chassis_id>/blade_id}
```

Example:

```
FP9300-A # scope service-profile server 1/1
FP9300-A /org/service-profile #
```

- Step 2** Enter one of the `cycle` commands:

- `cycle cycle-immediate`—power-cycles the module immediately.
- `cycle cycle-wait`—the system waits for up to five minutes for the application running on the module to shut down before power-cycling the module.

Example:

```
FP9300-A /org/service-profile # cycle cycle-wait
FP9300-A /org/service-profile* #
```

- Step 3** Commit the buffer to power-cycle the module:

```
commit-buffer
```

Reinitializing a Security Module/Engine

When a security module/engine is reinitialized, the security module/engine hard disk is formatted and all installed application instances, configurations, and data are removed. After reinitialization has completed, if a logical device is configured for the security module/engine, FXOS will reinstall the application software, redeploy the logical device, and auto start the application.



Caution

All application data on the security module/engine is deleted during reinitialization. Back up all application data before reinitializing a security module/engine.

Procedure

Step 1 Enter security services mode:

```
scope ssa
```

Step 2 Enter slot mode for the desired module:

```
scope slot {slot_id}
```

Example:

```
FP9300-A # scope ssa
FP9300-A /ssa # scope slot 2
FP9300-A /ssa/slot #
```

Step 3 Enter the **reinitialize** command:

Example:

```
FP9300-A # scope ssa
FP9300-A /ssa # scope slot 2
FP9300-A /ssa/slot # reinitialize
```

Warning: Reinitializing blade takes a few minutes. All the application data on blade will get lost. Please backup application running config files before commit-buffer.

```
FP9300-A /ssa/slot* #
```

Step 4 Back up application configuration files as necessary.

Step 5 Commit the buffer to reinitialize the module:

```
commit-buffer
```

The module is restarted and all data on the module is deleted. This process can take several minutes.

Step 6 You can use the **show detail** command to check the progress of the reformatting operation, the result of the reformatting (success or failure), and an error code if the operation fails.

Acknowledge a Network Module

When a new network module is installed into the chassis, or when an existing module is replaced with one with a different product ID (PID), you must acknowledge the network module before you can begin using it.

Procedure

Step 1 Enter `scope fabric-interconnect` mode:

```
scope fabric-interconnect
```

Step 2 Enter the `acknowledge` command after installing a new module or replacing a network module with another that is not the same type (that is, with a different PID):

```
acknowledge
```

Example:

```
FPR1 /fabric-interconnect # acknowledge
      fault    Fault
      slot     Card Config Slot Id  <=====
```

Step 3 Enter the `acknowledge slot` to acknowledge the inserted slot.

```
acknowledge slot
```

Example:

```
FPR1 /fabric-interconnect # acknowledg slot 2
      0-4294967295 Slot Id
```

Step 4 Commit the configuration:

```
commit-buffer
```

Taking a Network Module Offline or Online

Follow these steps to use CLI commands to take a network module offline, or to bring it back online; used for example, when performing module online insertion and removal (OIR).



Note

- If removing and replacing a network module, follow the instructions in the “Maintenance and Upgrades” chapter of the appropriate Install Guide for your device. See <https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html>.

Procedure

- Step 1** Use the following commands to enter `/fabric-interconnect` mode and then enter `/card` mode for the module to be taken offline:

```
scope fabric-interconnect a
scope card ID
```

- Step 2** You can use the `show detail` command to view information about this card, including its current status.

- Step 3** To take the module offline, enter:

```
set adminstate offline
```

- Step 4** Enter the `commit-buffer` command to save the configuration change.

You can use the `show detail` command again to confirm that the module is offline.

- Step 5** To bring the network module back online, enter:

```
set adminstate online
commit-buffer
```

Example

```
FP9300-A# scope fabric-interconnect a
FP9300-A /fabric-interconnect # scope card 2
FP9300-A /fabric-interconnect/card # show detail
```

Fabric Card:

```
Id: 2
Description: Firepower 4x40G QSFP NM
Number of Ports: 16
State: Online
Vendor: Cisco Systems, Inc.
Model: FPR-NM-4X40G
HW Revision: 0
Serial (SN): JAD191601DE
Perf: N/A
Admin State: Online
Power State: Online
Presence: Equipped
Thermal Status: N/A
Voltage Status: N/A
```

```
FP9300-A /fabric-interconnect/card # set adminstate offline
```

```
FP9300-A /fabric-interconnect/card* # commit-buffer
```

```
FP9300-A /fabric-interconnect/card # show detail
```

Fabric Card:

```
Id: 2
Description: Firepower 4x40G QSFP NM
Number of Ports: 16
State: Offline
Vendor: Cisco Systems, Inc.
Model: FPR-NM-4X40G
HW Revision: 0
Serial (SN): JAD191601DE
```

```

Perf: N/A
Admin State: Offline
Power State: Off
Presence: Equipped
Thermal Status: N/A
Voltage Status: N/A
FP9300-A /fabric-interconnect/card #

```

Blade Health Monitoring

Failsafe is engaged on a security module or engine when a specified number of unexpected application restarts are detected on a blade to prevent an endless boot loop condition, which can cause further side effects in a redundant HA or Cluster deployment.

Blade platform performs health checks periodically and reports it to the MIO. If the blade is in failed state, you will be notified with faults and error messages.

To view the status of the slot, use the `show detail` CLI:

```

Firepower# scope ssa
Firepower /ssa # scope slot 1
Firepower /ssa/slot # show detail
Slot:
  Slot ID: 1
  Log Level: Info
  Admin State: Ok
  Oper State: Fault
  Disk Format State: Ok
  Disk Format Status:
  Clear Log Data: Available
Error Msg: Security Module is in failsafe mode. Applications are blocked from starting in
this mode. Connect to security module for troubleshooting or to disable failsafe mode. The
app-instance can also be deleted. Security Module: 1. Application: cisco-asa.99.1.20.52.

```

Troubleshooting and Debugging

You can monitor, configure, and reset the blade settings from FXOS CLI.

Use `show fault` and `show events` to monitor the security module:

```

Firepower /ssa/slot # show fault
Severity  Code      Last Transition Time      ID      Description
-----
Major    F1546    2017-08-19T12:11:18.036    801162  Security Module 1 is in failed state.
Error: Security Module is in failsafe mode. Applications are blocked from starting in this
mode. Connect to security module for troubleshooting or to disable failsafe mode. The
app-instance can also be deleted. Security Module: 1. Application: cisco-asa.99.1.20.52.

Firepower /ssa/slot # show event
Creation Time      ID      Code      Description
-----
2017-08-19T12:11:18.037    801163  E4197940  Slot 1 is in failed state. Error:Security Module
is in failsafe mode. Applications are blocked from starting in this mode. Connect to
security module for troubleshooting or to disable failsafe mode. The app-instance can also
be deleted. Security Module: 1. Application: cisco-asa.99.1.20.52.

```

To exit failsafe mode, use the `failsafe-exit` command.

```
firepower # conne loc
firepower(local-mgmt)# failsafe-exit
Configuration Successful.
```



Note We do not recommend using of `failsafe-exit` as it may lead the device to behave abnormally. Use `reload` instead of `failsafe-exit` command.

Use the following CLIs to configure the security module:

```
Firepower-module> config ?
  syslog          => Configure syslog parameters for remote server and port
  vnic            => Configure specified VNIC
  memory          => Configure memory monitor
  disk            => Configure disk monitor
  process         => Configure process cpu monitor
  maxRestart      => Configure maximum restarts CSP. 0 shall mean Disable Restart. Default
8
  restartTimeInter => Configure time in seconds to block all CSPs from starting if server
restarts maxRestart in this interval. Default 3600
  restartCounters => To reset the restart_count
```

- `config maxRestart`—Number of times a service/csp causes blade to reboot before the process manager stops starting the service. The default value is 8. The feature gets disabled if the value is set to 0 (Zero).



Note The FXOS `maxRestart` counter is increased when the logical app (ASA/FTD) is not restarted properly. After restarting the logical app for 8 times, FXOS goes to failsafe mode. To recover FXOS from failsafe mode, you need to clear the `maxRestart` counter using the **`config restartCounters reset`** command, and reboot the logical device from Firepower Chassis Manager or reload FXOS.

- `config restartTimeInterval`—The time interval during which if the app reboots more than the number of times configured in `maxRestart` then the application does not restart. Default value is 3600 seconds.
- `show maxRestart`—Shows the maximum number of blade reboots permitted (default value is 8), the current number of restarts, and the time interval allowed for maximum number of reboots.
- `config restartCounters reset`—Resets the restart counter to 0.



CHAPTER 13

Configuration Import/Export

- [About Configuration Import/Export, on page 321](#)
- [Setting an Encryption Key for Configuration Import/Export, on page 322](#)
- [Exporting an FXOS Configuration File, on page 323](#)
- [Scheduling Automatic Configuration Export, on page 325](#)
- [Setting a Configuration Export Reminder, on page 327](#)
- [Importing a Configuration File, on page 327](#)

About Configuration Import/Export

You can use the configuration export feature to export an XML file containing logical device and platform configuration settings for your Firepower 4100/9300 chassis to a remote server. You can later import that configuration file to quickly apply the configuration settings to your Firepower 4100/9300 chassis to return to a known good configuration or to recover from a system failure.

Guidelines and Restrictions

- Beginning with FXOS 2.6.1, the encryption key is now configurable. You must set the encryption key before you can export a configuration. The same encryption key must be set on the system when importing that configuration. If you modified the encryption key so that it no longer matches what was used during export, the import operation will fail. Make sure you keep track of the encryption key for each exported configuration.
- Do not modify the contents of the configuration file. If a configuration file is modified, configuration import using that file might fail.
- Application-specific configuration settings are not contained in the configuration file. You must use the configuration backup tools provided by the application to manage application-specific settings and configurations.
- When you import a configuration to the chassis, all existing configuration on the chassis (including any logical devices) are deleted and completely replaced by the configuration contained in the import file.
- Except in an RMA scenario, we recommend you only import a configuration file to the same chassis where the configuration was exported.
- The platform software version of the Firepower 4100/9300 chassis where you are importing should be the same version as when the export was taken. If not, the import operation is not guaranteed to be

successful. We recommend you export a backup configuration whenever the chassis is upgraded or downgraded.

- The Firepower 4100/9300 chassis where you are importing must have the same Network Modules installed in the same slots as when the export was taken.
- The Firepower 4100/9300 chassis where you are importing must have the correct software application images installed for any logical devices defined in the export file that you are importing.
- If the configuration file being imported contains a logical device whose application has an End-User License Agreement (EULA), you must accept the EULA for that application on the Firepower 4100/9300 chassis before you import the configuration or the operation will fail.
- To avoid overwriting existing backup files, change the file name in the backup operation or copy the existing file to another location.

**Note**

You must backup the logical APP separately as the FXOS import/export will backup only the FXOS configuration. The FXOS configuration import will cause logical device reboot and it rebuilds the device with the factory default configuration.

Setting an Encryption Key for Configuration Import/Export

When exporting configurations, FXOS encrypts sensitive data such as passwords and keys.

Beginning with FXOS 2.6.1, the encryption key is now configurable. You must set the encryption key before you can export a configuration. The same encryption key must be set on the system when importing that configuration. If you have modified the encryption key so that it no longer matches what was used during export, the import operation will fail. Make sure that you keep track of the encryption key that is used for each exported configuration.

If you are importing a configuration into FXOS 2.6.1 or later that was exported from an FXOS release prior to 2.6.1, the system will not check the encryption key and will allow the import.

**Note**

If the platform software version to which you are importing is not the same version as when the export was taken, the import operation is not guaranteed to be successful. We recommend that you export a backup configuration whenever the Firepower 4100/9300 chassis is upgraded or downgraded.

Use the 'Set Version' option and export a backup configuration whenever the Firepower Threat Defense logical appliance is upgraded to a new software so that the new startup version matches the software release of the upgraded version.

Procedure

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

**Example:**

```
Firepower# scope security
Firepower /security #
```

**Step 2**

Set the encryption key:

**set password-encryption-key**

Enter a key: *encryption\_key*

Confirm the key: *encryption\_key*

The *encryption\_key* must be 4-40 characters in length.

**Example:**

```
Firepower /security #set password-encryption-key
Enter a key:
Confirm the key:
Firepower /security* #
```

**Step 3**

Commit the configuration:

**commit-buffer****Example:**

```
Firepower /security* #commit-buffer
Firepower /security #
```

---

## Exporting an FXOS Configuration File

Use the configuration export feature to export an XML file containing logical device and platform configuration settings for your Firepower 4100/9300 chassis to a remote server.

**Before you begin**

Review the [Guidelines and Restrictions](#).

**Procedure****Step 1**

To export a configuration file to a remote server:

**scope system****export-config** *URL* **enabled****commit-buffer**

Specify the URL for the file being exported using one of the following syntax:

- **ftp**://*username@hostname/path/image\_name*

- **scp**://username@hostname / path / image\_name
- **sftp**://username@hostname / path / image\_name
- **tftp**://hostname : port-num / path / image\_name

**Note**

You must specify the full path including filename. If you do not specify a filename, a hidden file is created in the specified path.

**Example:**

```
Firepower-chassis# scope system
Firepower-chassis /system # export-config scp://user1@192.168.1.2:/export/cfg-backup.xml
enabled
Firepower-chassis /system/export-config # commit-buffer
```

**Step 2** To check the status of the export task:

**scope system**

**scope export-config** hostname

**show fsm status**

**Example:**

```
Firepower-chassis# scope system
Firepower-chassis /system # scope export-config 192.168.1.2
Firepower-chassis /system/export-config # show fsm status
```

Hostname: 192.168.1.2

```
FSM 1:
 Remote Result: Not Applicable
 Remote Error Code: None
 Remote Error Description:
 Status: Nop
 Previous Status: Backup Success
 Timestamp: 2016-01-03T15:32:08.636
 Try: 0
 Progress (%): 100
 Current Task:
```

**Step 3** To view existing export tasks:

**scope system**

**show export-config**

**Step 4** To modify an existing export task:

**scope system**

**scope export-config** hostname

Use the following commands to modify the export task:

- **{enable|disable}**
- **set description** <description>

- **set password** *<password>*
- **set port** *<port>*
- **set protocol** {ftp|scp|sftp|tftp}
- **set remote-file** *path\_and\_filename*
- **set user** *<user>*

**Step 5** To delete an export task:

**scope system**

**delete export-config** *hostname*

**commit-buffer**

---

## Scheduling Automatic Configuration Export

Use the scheduled export feature to automatically export an XML file containing logical device and platform configuration settings for your Firepower 4100/9300 chassis to a remote server. You can schedule the exports to be run daily, weekly, or every two weeks. The configuration export will be executed according to the schedule based on the when the scheduled export feature is enabled. So, for example, if you enable weekly scheduled export on a Wednesday at 10:00pm, the system will trigger a new export every Wednesday at 10:00pm.

Please review the [Guidelines and Restrictions](#) for important information about using the configuration export feature.

### Procedure

---

To create a scheduled export task:

- a) Set the scope to export policy configuration:

**scope org**

**scope cfg-export-policy default**

- b) Enable the export policy:

**set adminstate enable**

- c) Specify the protocol to use when communicating with the remote server:

**set protocol** {ftp|scp|sftp|tftp}

- d) Specify the hostname or IP address of the location where the backup file should be stored. This can be a server, storage array, local drive, or any read/write media that the Firepower 4100/9300 chassis can access through the network.

If you use a hostname rather than an IP address, you must configure a DNS server.

**set hostname** *hostname*

- e) If you are using a non-default port, specify the port number:

**set port** *port*

- f) Specify the username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP:

**set user** *username*

- g) Specify the password for the remote server username. This field does not apply if the protocol is TFTP:

**set password** *password*

- h) Specify the full path to where you want the configuration file exported including the filename. If you omit the filename, the export procedure assigns a name to the file:

**set remote-file** *path\_and\_filename*

- i) Specify the schedule on which you would like to have the configuration automatically exported. This can be one of the following: Daily, Weekly, or BiWeekly:

**set schedule** {*daily|weekly|bi-weekly*}

- j) Commit the transaction to the system configuration:

**commit-buffer**

#### Example:

```
Firepower-chassis# scope org
Firepower-chassis /org # scope cfg-export-policy default
Firepower-chassis /org/cfg-export-policy # set adminstate enable
Firepower-chassis /org/cfg-export-policy* # set protocol scp
Firepower-chassis /org/cfg-export-policy* # set hostname 192.168.1.2
Firepower-chassis /org/cfg-export-policy* # set remote-file /export/cfg-backup.xml
Firepower-chassis /org/cfg-export-policy* # set user user1
Firepower-chassis /org/cfg-export-policy* # set password
Password:
Firepower-chassis /org/cfg-export-policy* # set schedule weekly
Firepower-chassis /org/cfg-export-policy* # commit-buffer
Firepower-chassis /org/cfg-export-policy #
Firepower-chassis /org/cfg-export-policy # show detail
```

```
Config Export policy:
 Name: default
 Description: Configuration Export Policy
 Admin State: Enable
 Protocol: Scp
 Hostname: 192.168.1.2
 User: user1
 Remote File: /export/cfg-backup.xml
 Schedule: Weekly
 Port: Default
 Current Task:
```

## Setting a Configuration Export Reminder

Use the Export Reminder feature to have the system generate a fault when a configuration export hasn't been executed in a certain number of days.

By default, the export reminder is enabled with a frequency of 30 days.



**Note** If the reminder frequency is smaller than the number of days in the scheduled export policy (daily, weekly, or bi-weekly), you will receive an export-reminder fault message (“Config backup may be outdated”). For example, if your export schedule is weekly, and the reminder frequency is five days, this fault message will be issued every five days if no configuration has been exported in that time.

### Procedure

To create a configuration export reminder:

**scope org**

**scope cfg-export-reminder**

**set frequency** *days*

**set adminstate** {enable|disable}

**commit-buffer**

#### Example:

```
Firepower-chassis# scope org
Firepower-chassis /org # scope cfg-export-reminder
Firepower-chassis /org/cfg-export-reminder # set frequency 10
Firepower-chassis /org/cfg-export-reminder* # set adminstate enable
Firepower-chassis /org/cfg-export-reminder* # commit-buffer
Firepower-chassis /org/cfg-export-reminder # show detail
```

```
Config Export Reminder:
 Config Export Reminder (Days): 10
 AdminState: Enable
```

## Importing a Configuration File

You can use the configuration import feature to apply configuration settings that were previously exported from your Firepower 4100/9300 chassis. This feature allows you to return to a known good configuration or to recover from a system failure.

**Before you begin**

Review the [Guidelines and Restrictions](#).

**Procedure**

**Step 1** To import a configuration file from a remote server:

**scope system**

**import-config** *URL* **enabled**

**commit-buffer**

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

- **ftp**://username@hostname/path/image\_name
- **scp**://username@hostname/path/image\_name
- **sftp**://username@hostname/path/image\_name
- **tftp**://hostname:port-num/path/image\_name

**Example:**

```
Firepower-chassis# scope system
Firepower-chassis /system # import-config scp://user1@192.168.1.2:/import/cfg-backup.xml
enabled
Warning: After configuration import any changes on the breakout port configuration will
cause the system to reboot
Firepower-chassis /system/import-config # commit-buffer
```

**Step 2** To check the status of the import task:

**scope system**

**scope import-config** *hostname*

**show fsm status**

**Example:**

```
Firepower-chassis# scope system
Firepower-chassis /system # scope import-config 192.168.1.2
Firepower-chassis /system/import-config # show fsm status
```

Hostname: 192.168.1.2

```
FSM 1:
 Remote Result: Not Applicable
 Remote Error Code: None
 Remote Error Description:
 Status: Import Wait For Switch
 Previous Status: Import Config Breakout
 Timestamp: 2016-01-03T15:45:03.963
 Try: 0
 Progress (%): 97
 Current Task: updating breakout port configuration(FSM-STAGE:sam:dme:
```



```
MgmtImporterImport:configBreakout)
```

**Step 3** To view existing import tasks:

```
scope system
```

```
show import-config
```

**Step 4** To modify an existing import task:

```
scope system
```

```
scope import-config hostname
```

Use the following commands to modify the import task:

- **{enable|disable}**
- **set description** *<description>*
- **set password** *<password>*
- **set port** *<port>*
- **set protocol** {ftp|scp|sftp|tftp}
- **set remote-file** *path\_and\_filename*
- **set user** *<user>*

**Step 5** To delete an import task:

```
scope system
```

```
delete import-config hostname
```

```
commit-buffer
```

---





## CHAPTER 14

# Troubleshooting

---

- [Packet Capture, on page 331](#)
- [Testing Network Connectivity, on page 340](#)
- [Troubleshooting Management Interface Status, on page 341](#)
- [Determine Port Channel Status, on page 342](#)
- [Recovering from a Software Failure, on page 344](#)
- [Recovering from a Corrupted File System, on page 349](#)
- [Restoring the Factory Default Configuration when the Admin Password is Unknown, on page 359](#)
- [Disaster Recovery of a Firepower Threat Defense Cluster Member, on page 361](#)
- [Generating Troubleshooting Log Files, on page 364](#)
- [Enabling Module Core Dumps, on page 369](#)
- [Finding the Serial Number of the Firepower 4100/9300 Chassis, on page 370](#)
- [Rebuild RAID Virtual Drive, on page 371](#)
- [Identify Issues with the SSD, on page 373](#)

## Packet Capture

The Packet Capture tool is a valuable asset for use in debugging connectivity and configuration issues and for understanding traffic flows through your Firepower 4100/9300 chassis. You can use the Packet Capture tool to log traffic that is going through specific interfaces on your Firepower 4100/9300 chassis.

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.

## Backplane Port Mappings

The backplane or uplink interface is an internal interface that connects the security module (SM) to the internal switch. In case of 2 backplane interfaces per module, the internal switch and the applications on the modules perform traffic load-balancing over the 2 backplane interfaces. The Firepower 4100/9300 chassis uses the following mappings for internal backplane ports:

| Platform                                    | Number of supported security modules | Backplane/uplink interfaces          | Mapped application interfaces        |
|---------------------------------------------|--------------------------------------|--------------------------------------|--------------------------------------|
| Firepower 4100 (except Firepower 4110/4112) | 1                                    | SM1:<br>Ethernet1/9<br>Ethernet1/10  | Internal-Data0/0<br>Internal-Data0/1 |
| Firepower 4110/4112                         | 1                                    | Ethernet1/9                          | Internal-Data0/0                     |
| Firepower 9300                              | 3                                    | SM1:<br>Ethernet1/9<br>Ethernet1/10  | Internal-Data0/0<br>Internal-Data0/1 |
|                                             |                                      | SM2:<br>Ethernet1/11<br>Ethernet1/12 | Internal-Data0/0<br>Internal-Data0/1 |
|                                             |                                      | SM3:<br>Ethernet1/13<br>Ethernet1/14 | Internal-Data0/0<br>Internal-Data0/1 |

## Guidelines and Limitations for Packet Capture

The Packet Capture tool has the following limitations:

- Can capture only up to 100 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.
- Captures only at the ingress stage of the internal switch.
- 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 can only capture packets for one subinterface per session, even if you have multiple subinterfaces on one or more parents.
- You cannot capture packets for an EtherChannel as a whole or for subinterfaces of an EtherChannel. However, for an EtherChannel allocated to a logical device, you can capture packets on each member

interface of the EtherChannel. If you allocate a subinterface, but not the parent interface, then you cannot capture packets on member interfaces.

- 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-chassis # **scope packet-capture**
- Step 2** Create a filter; see [Configuring Filters for Packet Capture, on page 336](#).  
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-chassis /packet-capture # **enter session** *session\_name*
- Step 4** Specify the buffer size to use for this packet capture session:  
Firepower-chassis /packet-capture/session\* # **set session-memory-usage** *session\_size\_in\_megabytes*  
The specified buffer size must be between 1 and 2048 MB.
- Step 5** Specify the length of the packet that you want to capture for this packet capture session:  
Firepower-chassis /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 6** 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. If you allocate a subinterface, but not the parent EtherChannel, then you cannot capture packets on member interfaces.

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

#### Example:

```
Firepower-chassis /packet-capture/session* # create phy-port Ethernet1/1
```

```
Firepower-chassis /packet-capture/session/phy-port* #
```

- b) Capture packets on a subinterface.

```
Firepower-chassis /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-chassis /packet-capture/session/phy-port* # set subinterface 100
Firepower-chassis /packet-capture/session/phy-port* #
```

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

```
Firepower-chassis /packet-capture/session/phy-port* # set app-identifier instance_name
```

**Example:**

```
Firepower-chassis /packet-capture/session/phy-port* # set app-identifier ftd-instance1
Firepower-chassis /packet-capture/session/phy-port* #
```

- d) Specify the application type.

```
Firepower-chassis /packet-capture/session/phy-port* # set app name
```

**Example:**

```
Firepower-chassis /packet-capture/session/phy-port* # set app ftd
Firepower-chassis /packet-capture/session/phy-port* #
```

- e) (Optional) Apply the desired filter.

```
Firepower-chassis /packet-capture/session/phy-port* # set {source-filter} filtername
```

**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 7**

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

**Syntax Description**

|                    |                                                        |
|--------------------|--------------------------------------------------------|
| <b>module_slot</b> | Security module in which the application is installed. |
|--------------------|--------------------------------------------------------|

|                       |                                                                                                                     |
|-----------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>link_name</b>      | Any user descriptive name referring to the interface, for example, link1, inside_port1, etc.                        |
| <b>interface_name</b> | Interface attached to the application where packets need to be captured from, for example, Ethernet1/1, Ethernet2/2 |
| <b>app_name</b>       | Application installed on the module - ftd, asa                                                                      |

- b) For container instances, specify the container instance name.

Firepower-chassis /packet-capture/session/app-port\* # **set app-identifier** *instance\_name*

**Example:**

```
Firepower-chassis /packet-capture/session/app-port* # set app-identifier ftd-instance1
Firepower-chassis /packet-capture/session/app-port* #
```

**Syntax Description**

|                      |                                                                                                  |
|----------------------|--------------------------------------------------------------------------------------------------|
| <b>instance_name</b> | Name of the application instance for which packet capture is required, i.e., native or container |
|----------------------|--------------------------------------------------------------------------------------------------|

- c) (Optional) Apply the desired filter.

Firepower-chassis /packet-capture/session/phy-port\* # **set {source-filter}** *filtername*

**Syntax Description**

|                   |                                                                             |
|-------------------|-----------------------------------------------------------------------------|
| <b>filtername</b> | The filter name from the 'create filter' command under packet-capture scope |
|-------------------|-----------------------------------------------------------------------------|

**Note**

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

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

**Step 8**

If you want to start the packet capture session now:

Firepower-chassis /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 9**

Commit the transaction to the system configuration:

Firepower-chassis /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-chassis# scope packet-capture
Firepower-chassis packet-capture # create session asalinside
Firepower-chassis packet-capture/session # set session-memory-usage 256
```

```

Firepower-chassis packet-capture/session* # create phy-port Ethernet3/1
Firepower-chassis packet-capture/session* # create phy-aggr-port Ethernet2/1/1
Firepower-chassis packet-capture/session* # create app-port 1 link1 Ethernet 1/1 asa
Firepower-chassis packet-capture/session* # exit
Firepower-chassis packet-capture* # create filter interfacelvlan100
Firepower-chassis packet-capture/filter* # set ivlan 100
Firepower-chassis packet-capture/filter* # set srcIP 6.6.6.6
Firepower-chassis packet-capture/filter* # set srcPort 80
Firepower-chassis packet-capture/filter* # set destIP 10.10.10.10
Firepower-chassis packet-capture/filter* # set destPort 5050
Firepower-chassis packet-capture/filter* # exit
Firepower-chassis packet-capture/session* # scope phy-port Ethernet3/1
Firepower-chassis packet-capture/session/phy-port* # set src-filter interfacelvlan100
Firepower-chassis packet-capture/session/phy-port* # exit
Firepower-chassis packet-capture/session* # scope app-port 1 link1 Ethernet1/1 asa
Firepower-chassis packet-capture/session/app-port* # set src-filter interfacelvlan100
Firepower-chassis packet-capture/session/app-port* # exit
Firepower-chassis packet-capture/session* # enable
Firepower-chassis packet-capture/session* # commit-buffer
Firepower-chassis packet-capture/session #

```

## Configuring Filters for Packet Capture

You can create filters to limit the traffic that is included in a packet capture session. You can select which interfaces should use a specific filter while creating a packet capture session.



**Note** If you modify or delete a filter that is applied to a packet capture session that is currently running, the changes will not take affect until you disable that session and then reenale it.

### Procedure

- Step 1** Enter packet capture mode:
- ```
Firepower-chassis # scope packet-capture
```
- Step 2** To create a new packet capture filter:
- ```
Firepower-chassis /packet-capture # create filter filter_name
```
- To edit an existing packet capture filter:
- ```
Firepower-chassis /packet-capture # enter filter filter_name
```
- To delete an existing packet capture filter:
- ```
Firepower-chassis /packet-capture # delete filter filter_name
```
- Step 3** Specify the filter details by setting one or more filter properties:
- ```
Firepower-chassis /packet-capture/filter* # set <filterprop filterprop_value
```

Note

You can filter using IPv4 or IPv6 addresses, but you cannot filter on both in the same packet capture session.

Table 14: Supported Filter Properties

ivlan	Inner VLAN ID (vlan of packet while ingressing port)
ovlan	Outer VLAN ID (vlan added by the Firepower 4100/9300 chassis)
srcip	Source IP Address (IPv4)
destip	Destination IP Address (IPv4)
srcipv6	Source IP Address (IPv6)
destipv6	Destination IP Address (IPv6)
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

Example

```

Firepower-chassis# scope packet-capture
Firepower-chassis packet-capture # create filter interface1vlan100
Firepower-chassis packet-capture/filter* # set ivlan 100
Firepower-chassis packet-capture/filter* # set srcip 6.6.6.6
Firepower-chassis packet-capture/filter* # set srcport 80
Firepower-chassis packet-capture/filter* # set destip 10.10.10.10
Firepower-chassis packet-capture/filter* # set destport 5050
Firepower-chassis packet-capture/filter* # commit-buffer

```

Starting and Stopping a Packet Capture Session

Procedure

-
- Step 1** Enter packet capture mode:
- ```
Firepower-chassis # scope packet-capture
```
- Step 2** Enter the scope for the packet capture session that you want to start or stop:
- ```
Firepower-chassis /packet-capture # enter session session_name
```

Step 3 To start a packet capture session:

```
Firepower-chassis /packet-capture/session* # enable [append | overwrite]
```

Note

You cannot start a packet capture session while another session is running.

While the packet capture session is running, the file size for the individual PCAP files will increase as traffic is captured. Once the Buffer Size limit is reached, the system will start dropping packets and you will see the Drop Count field increase.

Step 4 To stop a packet capture session:

```
Firepower-chassis /packet-capture/session* # disable
```

Step 5 Commit the transaction to the system configuration:

```
Firepower-chassis /packet-capture/session* # commit-buffer
```

If you enabled the packet capture session, the PCAP files for the interfaces included in the session will start collecting traffic. If the session is configured to overwrite session data, the existing PCAP data will be erased. If not, data will be appended to the existing file (if any).

Example

```
Firepower-chassis# scope packet-capture
Firepower-chassis packet-capture # scope session asalinside
Firepower-chassis packet-capture/session # enable append
Firepower-chassis packet-capture/session* # commit-buffer
Firepower-chassis packet-capture/session #
```

Downloading a Packet Capture File

You can download the Packet Capture (PCAP) files from a session to your local computer so that they can be analyzed using a network packet analyzer.

PCAP files are stored into the `workspace://packet-capture` directory and use the following naming conventions:

```
workspace://packet-capture/session-<id>/<session-name>-<interface-name>.pcap
```

Procedure

To copy a PCAP file from the Firepower 4100/9300 chassis:

Note

You should stop the packet capture session before you download the PCAP files from that session.

a) Connect to local management:

```
Firepower-chassis # connect local-mgmt
```

b) Copy the PCAP files:

```
# copy pcap_file copy_destination
```

Example

```
Firepower-chassis# connect local-mgmt
# copy workspace:/packet-capture/session-1/test-ethernet-1-1-0.pcap
scp://user@10.10.10.1:/workspace/
```

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

Example

```
Firepower-chassis# scope packet-capture
Firepower-chassis packet-capture # delete session asalinside
Firepower-chassis packet-capture* # commit-buffer
Firepower-chassis packet-capture #
```

Testing Network Connectivity

Before you begin

To test basic network connectivity by pinging another device on the network with its host name or IPv4 address, use the **ping** command. To ping another device on the network with its host name or IPv6 address, use the **ping6** command.

To trace the route to another device on the network with its host name or IPv4 address, use the **tracert** command. To trace the route to another device on the network with its host name or IPv6 address, use the **tracert6** command.

- The **ping** and **ping6** commands are available in `local-mgmt` mode.
- The **ping** command is also available in `module` mode.
- The **tracert** and **tracert6** commands are available in `local-mgmt` mode.
- The **tracert** command is also available in `module` mode.

Procedure

Step 1 Connect to `local-mgmt` or `module` mode by entering one of the following commands:

- **connect local-mgmt**
- **connect module *module-ID* {console | telnet}**

Example:

```
FP9300-A# connect local-mgmt
FP9300-A(local-mgmt)#
```

Step 2 To test basic network connectivity by pinging another device on the network with its host name or IPv4 address:

ping {*hostname* | *IPv4_address*} [**count** *number_packets*] | [**deadline** *seconds*] | [**interval** *seconds*] | [**packet-size** *bytes*]

Example:

This example shows how to connect to ping another device on the network twelve times:

```
FP9300-A(local-mgmt)# ping 198.51.100.10 count 12
PING 198.51.100.10 (198.51.100.10) from 203.0.113.5 eth0: 56(84) bytes of data.
64 bytes from 198.51.100.10: icmp_seq=1 ttl=61 time=0.264 ms
64 bytes from 198.51.100.10: icmp_seq=2 ttl=61 time=0.219 ms
64 bytes from 198.51.100.10: icmp_seq=3 ttl=61 time=0.234 ms
64 bytes from 198.51.100.10: icmp_seq=4 ttl=61 time=0.205 ms
64 bytes from 198.51.100.10: icmp_seq=5 ttl=61 time=0.216 ms
64 bytes from 198.51.100.10: icmp_seq=6 ttl=61 time=0.251 ms
64 bytes from 198.51.100.10: icmp_seq=7 ttl=61 time=0.223 ms
64 bytes from 198.51.100.10: icmp_seq=8 ttl=61 time=0.221 ms
64 bytes from 198.51.100.10: icmp_seq=9 ttl=61 time=0.227 ms
```

```
64 bytes from 198.51.100.10: icmp_seq=10 ttl=61 time=0.224 ms
64 bytes from 198.51.100.10: icmp_seq=11 ttl=61 time=0.261 ms
64 bytes from 198.51.100.10: icmp_seq=12 ttl=61 time=0.261 ms

--- 198.51.100.10 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11104ms
rtt min/avg/max/mdev = 51.005/51.062/51.164/0.064 ms

FP9300-A(local-mgmt) #
```

Step 3 To trace the route to another device on the network using its host name or IPv4 address:

traceroute {*hostname* | *IPv4_address*}

Example:

```
FP9300-A(local-mgmt) # traceroute 198.51.100.10
traceroute to 198.51.100.10 (198.51.100.10), 30 hops max, 40 byte packets
 1 198.51.100.57 (198.51.100.57) 0.640 ms 0.737 ms 0.686 ms
 2 net1-gw1-13.cisco.com (198.51.100.101) 2.050 ms 2.038 ms 2.028 ms
 3 net1-sec-gw2.cisco.com (198.51.100.201) 0.540 ms 0.591 ms 0.577 ms
 4 net1-fp9300-19.cisco.com (198.51.100.108) 0.336 ms 0.267 ms 0.289 ms

FP9300-A(local-mgmt) #
```

Step 4 (Optional) Enter **exit** to exit `local-mgmt` mode and return to the top-level mode.

Troubleshooting Management Interface Status

During initialization and configuration, if you suspect the management interface has not come up for some reason (for example, you cannot access the Chassis Manager), use the **show mgmt-port** command in the `local-mgmt` shell to determine the status of the management interface.



Note Do not use the **show interface brief** command in the `fxos` shell as it currently displays incorrect information.

Procedure

Step 1 Connect to `local-mgmt` mode by entering the following command:

- **connect local-mgmt**

Example:

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

Step 2 Use the **show mgmt-port** command to determine the status of the management interface.

Example:

```
firepower(local-mgmt)# show mgmt-port
eth0      Link encap:Ethernet  HWaddr b0:aa:77:2f:f0:a9
          inet addr:10.89.5.14  Bcast:10.89.5.63  Mask:255.255.255.192
          inet6 addr: fe80::b2aa:77ff:fe2f:f0a9/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3210912 errors:0 dropped:0 overruns:0 frame:0
          TX packets:705434 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1648941394 (1.5 GiB)  TX bytes:138386379 (131.9 MiB)

firepower(local-mgmt)#
```

You also can use the **show mgmt-ip-debug** command; however, it produces an extensive listing of interface-configuration information.

Determine Port Channel Status

You can follow these steps to determine the status of currently defined port channels.

Procedure

Step 1 Enter `/eth-uplink/fabric` mode by entering the following commands:

- **scope eth-uplink**
- **scope fabric {a | b}**

Example:

```
FP9300-A# scope eth-uplink
FP9300-A /eth-uplink # scope fabric a
FP9300-A /eth-uplink/fabric #
```

Step 2 Enter the **show port-channel** command to display a list current port channels with the administrative state and operational state for each.

Example:

```
FP9300-A /eth-uplink/fabric # show port-channel
```

```
Port Channel:
  Port Channel Id Name          Port Type      Admin
  State Oper State      State Reason
  -----
  10      Failed          Port-channel10  Data           Enabl
ed
  11      Failed          Port-channel11  Data           Enabl
ed
  12      Admin Down        Port-channel12  Data           Disab
led
  48      Up                Port-channel48  Cluster        Enabl
ed
```

```
FP9300-A /eth-uplink/fabric #
```

Step 3 Enter `/port-channel` mode to display individual port-channel and port information by entering the following command:

- `scope port-channel ID`

Example:

```
FP9300-A /eth-uplink/fabric/port-channel # top
FP9300-A# connect fxos
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2017, Cisco Systems, Inc. All rights reserved.

The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license.

<--- remaining lines removed for brevity --->

FP9300-A(fxos)#
```

Step 4 Enter the `show` command to display status information for the specified port channel.

Example:

```
FP9300-A /eth-uplink/fabric/port-channel # show

Port Channel:
  Port Channel Id Name      Port Type      Admin
  State Oper State      State Reason
  -----
  10      Port-channel10      Data          Enabl
ed      Failed          No operational members

FP9300-A /eth-uplink/fabric/port-channel #
```

Step 5 Enter the `show member-port` command to display status information for the port channel's member port(s).

Example:

```
FP9300-A /eth-uplink/fabric/port-channel # show member-port

Member Port:
  Port Name      Membership      Oper State      State Reas
on
  -----
  Ethernet2/3      Suspended      Failed          Suspended
  Ethernet2/4      Suspended      Failed          Suspended

FP9300-A /eth-uplink/fabric/port-channel #
```

A port channel does not come up until you assign it to a logical device. If the port channel is removed from the logical device, or the logical device is deleted, the port channel reverts to a Suspended state.

Step 6 To view additional port channel and LACP information, exit `/eth-uplink/fabric/port-channel` mode and enter `fxos` mode by entering the following commands:

- top
- connect fxos

Example:

Step 7 Enter the **show port-channel summary** command to display summary information for the current port channels.

Example:

```

FP9300-A(fxos)# show port-channel 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
-----
10    Po10(SD)    Eth       LACP      Eth2/3(s)  Eth2/4(s)
11    Po11(SD)    Eth       LACP      Eth2/1(s)  Eth2/2(s)
12    Po12(SD)    Eth       LACP      Eth1/4(D)  Eth1/5(D)
48    Po48(SU)    Eth       LACP      Eth1/1(P)  Eth1/2(P)

```

Additional **show port-channel** and **show lacp** commands are available in **fxos** mode. You can use these commands to display a variety of port channel and LACP information such as capacity, traffic, counters, and usage.

What to do next

See [Add an EtherChannel \(Port Channel\)](#), on page 197 for information about creating port channels.

Recovering from a Software Failure

Before you begin

In the event of software failure that prevents the system from booting successfully, you can use the following procedure to boot a new version of software. To complete this process you need to TFTP boot a kickstart image, download new system and manager images, and then boot using the new images.

The recovery images for a specific FXOS version can be obtained from Cisco.com at one of the following locations:

- Firepower 9300—<https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286287252&flowid=77282&softwareid=286287263>

- Firepower 4100 Series—<https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286305187&flowid=79423&softwareid=286287263>

The recovery images include three separate files. For example, below are the current recovery images for FXOS 2.1.1.64.

Recovery image (kickstart) for FX-OS 2.1.1.64.
fxos-k9-kickstart.5.0.3.N2.4.11.63.SPA

Recovery image (manager) for FX-OS 2.1.1.64.
fxos-k9-manager.4.1.1.63.SPA

Recovery image (system) for FX-OS 2.1.1.64.
fxos-k9-system.5.0.3.N2.4.11.63.SPA

Procedure

Step 1 Access ROMMON:

- Connect to the console port.
- Reboot the system.

The system will start loading and during the process display a countdown timer.

- Press the **Escape** key during the countdown to enter ROMMON mode.

Example:

```
Cisco System ROMMON, version 1.0.09, RELEASE SOFTWARE
Copyright (c) 1994-2015 by Cisco Systems, Inc.
Compiled Sun 01/01/1999 23:59:59.99 by user
```

```
Current image running: Boot ROM0
Last reset cause: LocalSoft
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!
```

```
Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address aa:aa:aa:aa:aa:aa
```

```
find the string ! boot bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.0.00.00.SPA
```

```
bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.0.00.00.SPA
```

```
Use BREAK, ESC or CTRL+L to interrupt boot.
use SPACE to begin boot immediately.
Boot interrupted.
```

```
rommon 1 >
```

Step 2 TFTP boot a kickstart image:

- Verify that the management IP address, management netmask, and gateway IP address are set correctly. You can see their values using the **set** command. You can test the connectivity to the TFTP server using the **ping** command.

```
rommon 1 > set
ADDRESS=
NETMASK=
```

```

GATEWAY=
SERVER=
IMAGE=
PS1="ROMMON ! > "
rommon > ADDRESS=<ip-address>
rommon > NETMASK=<network-mask>
rommon > GATEWAY=<default-gateway>

```

- b) Copy the kickstart image to a TFTP directory that is accessible from your Firepower 4100/9300 chassis.

Note

The kickstart image version number will not match the bundle version number. Information showing the mapping between your FXOS version and the kickstart image can be found on the Cisco.com software download page.

- c) Boot the image from ROMMON using the boot command:

```
boot tftp://<IP address>/<path to image>
```

Note

You can also boot the kickstart from ROMMON using a USB media device inserted into the USB slot on the front panel of the Firepower 4100/9300 chassis. If the USB device is inserted while the system is running, you will need to reboot the system before it will recognize the USB device.

The system will display a series of #'s indicating that the image is being received and will then load the kickstart image.

Example:

```

rommon 1 > set
ADDRESS=
NETMASK=
GATEWAY=
SERVER=
IMAGE=
PS1="ROMMON ! > "

rommon 2 > ADDRESS=10.0.0.2
rommon 3 > NETMASK=255.255.255.0
rommon 4 > GATEWAY=10.0.0.1
rommon 5 > ping 10.0.0.2
..!!!!!!
Success rate is 100 percent (10/10)
rommon 6 > ping 192.168.1.2
..!!!!!!
Success rate is 100 percent (10/10)

rommon 7 > boot tftp://192.168.1.2/fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA
ADDRESS: 10.0.0.2
NETMASK: 255.255.255.0
GATEWAY: 10.0.0.1
SERVER: 192.168.1.2
IMAGE: fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA

TFTP_MACADDR: aa:aa:aa:aa:aa:aa
.....

Receiving fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA from 192.168.1.2

#####
#####

```

```
#####
```

```
File reception completed.
```

Step 3 Download the recovery system and manager images that match the kickstart image you just loaded to the Firepower 4100/9300 chassis:

- a) To download the recovery system and manager images you will need to set the management IP address and gateway. You cannot download these images via USB.

```
switch(boot)# config terminal
switch(boot)(config)# interface mgmt 0
switch(boot)(config-if)# ip address <ip address> <netmask>
switch(boot)(config-if)# no shutdown
switch(boot)(config-if)# exit
switch(boot)(config)# ip default-gateway <gateway>
switch(boot)(config)# exit
```

- b) Copy the recovery system and manager images from the remote server to the bootflash:

```
switch(boot)# copy URL bootflash:
```

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

- **ftp://username@hostname/path/image_name**
- **scp://username@hostname/path/image_name**
- **sftp://username@hostname/path/image_name**
- **tftp://hostname/path/image_name**

Example:

```
switch(boot)# copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
bootflash:
```

```
switch(boot)# copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
bootflash:
```

- c) After the images have been successfully copied to the Firepower 4100/9300 chassis, make a symlink to the manager image from `nuova-sim-mgmt-nsg.0.1.0.001.bin`. This link tells the load mechanism which manager image to load. The symlink name should always be `nuova-sim-mgmt-nsg.0.1.0.001.bin` regardless of what image you are trying to load.

```
switch(boot)# copy bootflash:<manager-image>
bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin
```

Example:

```
switch(boot)# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
switch(boot)(config)# interface mgmt 0
switch(boot)(config-if)# ip address 10.0.0.2 255.255.255.0
switch(boot)(config-if)# no shutdown
switch(boot)(config-if)# exit
switch(boot)(config)# ip default-gateway 10.0.0.1
```

```

switch(boot) (config)# exit
switch(boot)# copy
  tftp://192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
  bootflash:
Trying to connect to tftp server.....
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy
  tftp://192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
  bootflash:
Trying to connect to tftp server.....
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy bootflash:fxos-k9-manager.4.1.1.69.SPA
  bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin

Copy complete, now saving to disk (please wait)...

switch(boot)#

```

Step 4 Load the system image that you just downloaded:

```
switch(boot)# load bootflash:<system-image>
```

Example:

```

switch(boot)# load bootflash:fxos-k9-system.5.0.3.N2.4.11.69.SPA
Uncompressing system image: bootflash:/fxos-k9-system.5.0.3.N2.4.11.69.SPA

```

```

Manager image digital signature verification successful
...
System is coming up ... Please wait ...

```

```

Cisco FPR Series Security Appliance
FP9300-A login:

```

Step 5 After the recovery images have loaded, enter the following commands to prevent the system from trying to load the prior images:

Note

This step should be performed immediately after loading the recovery images.

```

FP9300-A# scope org
FP9300-A /org # scope fw-platform-pack default
FP9300-A /org/fw-platform-pack # set platform-bundle-version ""
Warning: Set platform version to empty will result software/firmware incompatibility issue.
FP9300-A /org/fw-platform-pack* # commit-buffer

```

Step 6 Download and install the Platform Bundle image that you want to use on your Firepower 4100/9300 chassis. For more information, see [Image Management, on page 59](#).

Example:

```

FP9300-A# scope firmware
FP9300-A /firmware # show download-task

Download task:
  File Name Protocol Server          Port      Userid      State
  -----
  fxos-k9.2.1.1.73.SPA
    Tftp      192.168.1.2          0          Downloaded
FP9300-A /firmware # show package fxos-k9.2.1.1.73.SPA detail
Firmware Package fxos-k9.2.1.1.73.SPA:
  Version: 2.1(1.73)
  Type: Platform Bundle
  State: Active
Time Stamp: 2012-01-01T07:40:28.000
Build Date: 2017-02-28 13:51:08 UTC
FP9300-A /firmware #

```

Recovering from a Corrupted File System

Before you begin

If the Supervisor's onboard flash becomes corrupted and the system is no longer able to start successfully, you can use the following procedure to recover the system. To complete this process you need to TFTP boot a kickstart image, reformat the flash, download new system and manager images, and then boot using the new images.



Note This procedure includes reformatting the system flash. As a result, you will need to completely reconfigure your system after it has been recovered.

The recovery images for a specific FXOS version can be obtained from Cisco.com at one of the following locations:

- Firepower 9300—<https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286287252&flowid=77282&softwareid=286287263>
- Firepower 4100 Series—<https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286305187&flowid=79423&softwareid=286287263>

The recovery images include three separate files. For example, below are the recovery images for FXOS 2.1.1.64.

Recovery image (kickstart) for FX-OS 2.1.1.64.
fxos-k9-kickstart.5.0.3.N2.4.11.63.SPA

Recovery image (manager) for FX-OS 2.1.1.64.
fxos-k9-manager.4.1.1.63.SPA

Recovery image (system) for FX-OS 2.1.1.64.
fxos-k9-system.5.0.3.N2.4.11.63.SPA

Procedure

Step 1

Access ROMMON:

- a) Connect to the console port.
- b) Reboot the system.

The system will start loading and during the process display a countdown timer.

- c) Press the **Escape** key during the countdown to enter ROMMON mode.

Example:

```
Cisco System ROMMON, version 1.0.09, RELEASE SOFTWARE
Copyright (c) 1994-2015 by Cisco Systems, Inc.
Compiled Sun 01/01/1999 23:59:59.99 by user
```

```
Current image running: Boot ROM0
Last reset cause: LocalSoft
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!
```

```
Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address aa:aa:aa:aa:aa:aa
```

```
find the string ! boot bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.0.00.00.SPA
```

```
bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.0.00.00.SPA
```

```
Use BREAK, ESC or CTRL+L to interrupt boot.
use SPACE to begin boot immediately.
Boot interrupted.
```

```
rommon 1 >
```

Step 2

TFTP boot a kickstart image:

- a) Verify that the management IP address, management netmask, and gateway IP address are set correctly. You can see their values using the **set** command. You can test the connectivity to the TFTP server using the **ping** command.

```
rommon 1 > set
ADDRESS=
NETMASK=
GATEWAY=
SERVER=
IMAGE=
PS1="ROMMON ! > "
rommon > address <ip-address>
rommon > netmask <network-mask>
rommon > gateway <default-gateway>
```

- b) Copy the kickstart image to a TFTP directory that is accessible from your Firepower 4100/9300 chassis.

Note

The kickstart image version number will not match the bundle version number. Information showing the mapping between your FXOS version and the kickstart image can be found on the Cisco.com software download page.

- c) Boot the image from ROMMON using the boot command:

```
boot tftp://<IP address>/<path to image>
```

Note

You can also boot the kickstart from ROMMON using a USB media device inserted into the USB slot on the front panel of the Firepower 4100/9300 chassis. If the USB device is inserted while the system is running, you will need to reboot the system before it will recognize the USB device.

The system will display a series of #'s indicating that the image is being received and will then load the kickstart image.

Example:

```
rommon 1 > set
ADDRESS=
NETMASK=
GATEWAY=
SERVER=
IMAGE=
PS1="ROMMON ! > "

rommon 2 > address 10.0.0.2
rommon 3 > netmask 255.255.255.0
rommon 4 > gateway 10.0.0.1
rommon 5 > ping 10.0.0.2
..!!!!!!!
Success rate is 100 percent (10/10)
rommon 6 > ping 192.168.1.2
..!!!!!!!
Success rate is 100 percent (10/10)

rommon 7 > boot tftp://192.168.1.2/fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA
ADDRESS: 10.0.0.2
NETMASK: 255.255.255.0
GATEWAY: 10.0.0.1
SERVER: 192.168.1.2
IMAGE: fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA

TFTP_MACADDR: aa:aa:aa:aa:aa:aa
.....
Receiving fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA from 192.168.1.2

#####
#####
#####

File reception completed.
```

Step 3

After the kickstart image has loaded, reformat the flash using the **init system** command.

The **init system** command erases the contents of the flash including all software images downloaded to the system and all configurations on the system. The command takes approximately 20-30 minutes to complete.

Example:

```
switch(boot)# init system
```

This command is going to erase your startup-config, licenses as well as the contents of your bootflash:.

```

Do you want to continue? (y/n)  [n] y

Detected 32GB flash...
Initializing the system
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):          done
Initializing startup-config and licenses
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):          done
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):          done
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):          done
mke2fs 1.35 (28-Feb-2004)
Formatting bootflash:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):          done
Formatting SAM partition:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):          done
Formatting Workspace partition:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):          done
Formatting Sysdebug partition:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):          done

```

Step 4

Download the recovery images to the Firepower 4100/9300 chassis:

- a) To download the recovery images you will need to set the management IP address and gateway. You cannot download these images via USB.

```

switch(boot)# config terminal
switch(boot) (config)# interface mgmt 0
switch(boot) (config-if)# ip address <ip address> <netmask>
switch(boot) (config-if)# no shutdown
switch(boot) (config-if)# exit
switch(boot) (config)# ip default-gateway <gateway>
switch(boot) (config)# exit

```

- b) Copy all three recovery images from the remote server to the bootflash:

```
switch(boot)# copy URL bootflash:
```

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

- **ftp://username@hostname/path/image_name**
- **scp://username@hostname/path/image_name**
- **sftp://username@hostname/path/image_name**
- **tftp://hostname/path/image_name**

Example:

```

switch(boot)# copy
scp://<username>@192.168.1.2/recovery_images/fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA
bootflash:

switch(boot)# copy
scp://<username>@192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
bootflash:

```



```
switch(boot)# copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
bootflash:
```

- c) After the images have been successfully copied to the Firepower 4100/9300 chassis, make a symlink to the manager image from `nuova-sim-mgmt-nsg.0.1.0.001.bin`. This link tells the load mechanism which manager image to load. The symlink name should always be `nuova-sim-mgmt-nsg.0.1.0.001.bin` regardless of what image you are trying to load.

```
switch(boot)# copy bootflash:<manager-image>
bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin
```

Example:

```
switch(boot)# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.

switch(boot) (config)# interface mgmt 0
switch(boot) (config-if)# ip address 10.0.0.2 255.255.255.0
switch(boot) (config-if)# no shutdown
switch(boot) (config-if)# exit
switch(boot) (config)# ip default-gateway 10.0.0.1
switch(boot) (config)# exit
switch(boot)# copy
  tftp://192.168.1.2/recovery_images/fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA
bootflash:
Trying to connect to tftp server.....
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy
  tftp://192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
bootflash:
Trying to connect to tftp server.....
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy
  tftp://192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
bootflash:
Trying to connect to tftp server.....
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy bootflash:fxos-k9-manager.4.1.1.69.SPA
bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin

Copy complete, now saving to disk (please wait)...

switch(boot)#
```

Step 5

Reload the switch:

```
switch(boot)# reload
```

Example:

```
switch(boot)# reload
This command will reboot this supervisor module. (y/n) ? y
[ 1866.310313] Restarting system.

!! Rommon image verified successfully !!

Cisco System ROMMON, Version 1.0.11, RELEASE SOFTWARE
Copyright (c) 1994-2016 by Cisco Systems, Inc.
Compiled Wed 11/23/2016 11:23:23.47 by builder
Current image running: Boot ROM1
Last reset cause: ResetRequest
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!
BIOS has been locked !!

Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address: bb:aa:77:aa:aa:bb

autoboot: Can not find autoboot file 'menu.lst.local'
          Or can not find correct boot string !!
rommon 1 >
```

Step 6

Boot from the kickstart and system images:

```
rommon 1 > boot <kickstart-image> <system-image>
```

Note

You will likely see license manager failure messages while the system image is loading. These messages can be safely ignored.

Example:

```
rommon 1 > dir
Directory of: bootflash:\

01/01/12 12:33a <DIR>          4,096 .
01/01/12 12:33a <DIR>          4,096 ..
01/01/12 12:16a <DIR>         16,384 lost+found
01/01/12 12:27a             34,333,696 fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA
01/01/12 12:29a             330,646,465 fxos-k9-manager.4.1.1.69.SPA
01/01/12 12:31a             250,643,172 fxos-k9-system.5.0.3.N2.4.11.69.SPA
01/01/12 12:34a             330,646,465 nuova-sim-mgmt-nsg.0.1.0.001.bin
          4 File(s) 946,269,798 bytes
          3 Dir(s)

rommon 2 > boot fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA fxos-k9-system.5.0.3.N2.4.11.69.SPA
!! Kickstart Image verified successfully !!

Linux version: 2.6.27.47 (security@cisco.com) #1 SMP Thu Nov 17 18:22:00 PST 2016
[ 0.000000] Fastboot Memory at 0c100000 of size 201326592
Usage: init 0123456SsQqAaBbCcUu

INIT: version 2.86 booting

POST INIT Starts at Sun Jan 1 00:27:32 UTC 2012
S10mount-ramfs.supnuovaca Mounting /isan 3000m
```

```
Mounted /isan
Creating /callhome..
Mounting /callhome..
Creating /callhome done.
Callhome spool file system init done.
Platform is BS or QP MIO: 30
FPGA Version 0x00010500 FPGA Min Version 0x00000600
Checking all filesystems..r.r..r done.
Warning: switch is starting up with default configuration
Checking NVRAM block device ... done
.
FIPS power-on self-test passed
Unpack CMC Application software
Loading system software
Uncompressing system image: bootflash:/fxos-k9-system.5.0.3.N2.4.11.69.SPA

Manager image digital signature verification successful

...

System is coming up ... Please wait ...
nohup: appending output to `nohup.out'

---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Only minimal configuration including IP connectivity to
the Fabric interconnect and its clustering mode is performed through these steps.

Type Ctrl-C at any time to abort configuration and reboot system.
To back track or make modifications to already entered values,
complete input till end of section and answer no when prompted
to apply configuration.

You have chosen to setup a new Security Appliance. Continue? (y/n):
```

Step 7 After the images have loaded, the system will prompt you to enter initial configuration settings. For more information, see [Initial Configuration Using Console Port, on page 12](#).

Step 8 Download the Platform Bundle image that you want to use on your Firepower 4100/9300 chassis. For more information, see [Image Management, on page 59](#).

Example:

```
FP9300-A# scope firmware
FP9300-A /firmware # show download-task

Download task:
  File Name Protocol Server          Port      Userid      State
  -----
  fxos-k9.2.1.1.73.SPA
      Tftp      192.168.1.2          0          Downloaded
FP9300-A /firmware # show package fxos-k9.2.1.1.73.SPA detail
Firmware Package fxos-k9.2.1.1.73.SPA:
  Version: 2.1(1.73)
  Type: Platform Bundle
  State: Active
Time Stamp: 2012-01-01T07:40:28.000
Build Date: 2017-02-28 13:51:08 UTC
FP9300-A /firmware #
```

Step 9 Install the Platform Bundle image you downloaded in the previous step:

Note

Installation process typically takes between 15 and 20 minutes.

a) Enter auto-install mode:

```
Firepower-chassis /firmware # scope auto-install
```

b) Install the FXOS platform bundle:

```
Firepower-chassis /firmware/auto-install # install platform platform-vers version_number
```

version_number is the version number of the FXOS platform bundle you are installing--for example, 2.1(1.73).

c) The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Enter **yes** to confirm that you want to proceed with verification.

d) Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

The FXOS unpacks the bundle and upgrades/reloads the components.

e) To monitor the upgrade process:

- Enter **scope firmware**.
- Enter **scope auto-install**.
- Enter **show fsm status expand**.

Example:

```
TB10 /firmware/auto-install # show fsm status expand
```

```
FSM Status:
```

```
Affected Object: sys/fw-system/fsm
Current FSM: Deploy
Status: In Progress
Completion Time:
Progress (%): 98
```

```
FSM Stage:
```

Order	Stage Name	Status	Try
1	DeployWaitForDeploy	Success	0
2	DeployResolveDistributableNames	Skip	0
3	DeployResolveDistributable	Skip	0
4	DeployResolveImages	Skip	0
5	DeployValidatePlatformPack	Success	1
6	DeployDebundlePort	Success	0
7	DeployPollDebundlePort	Success	1
8	DeployActivateUCSM	Success	0
9	DeployPollActivateOfUCSM	Success	0
10	DeployActivateMgmtExt	Skip	0
11	DeployPollActivateOfMgmtExt	Skip	0
12	DeployUpdateIOM	Skip	0
13	DeployPollUpdateOfIOM	Skip	0
14	DeployActivateIOM	Skip	0
15	DeployPollActivateOfIOM	Skip	0

16	DeployActivateRemoteFI	Skip	0
17	DeployPollActivateOfRemoteFI	Skip	0
18	DeployWaitForUserAck	Skip	0
19	DeployActivateLocalFI	Success	0
20	DeployPollActivateOfLocalFI	In Progress	1

Note

Do not proceed to the next step until the status of the stages changes from "In Progress" to "Skip" or "Success."

Step 10

If the Platform Bundle image that you installed corresponds with the images you used for recovering your system, you must manually activate the kickstart and system images so that they will be used when loading the system in the future. Automatic activation does not occur when installing a Platform Bundle that has same images as the recovery images that were used.

- a) Set the scope for fabric-interconnect a:

```
FP9300-A# scope fabric-interconnect a
```

- b) Use the **show version** command to view the running kernel version and the running system version. You will use these strings to activate the images.

```
FP9300-A /fabric-interconnect # show version
```

Note

If the Startup-Kern-Vers and Startup-Sys-Vers are already set and match the Running-Kern-Vers and Running-Sys-Vers, you do not need to activate the images and can proceed to Step 11.

- c) Enter the following command to activate the images:

```
FP9300-A /fabric-interconnect # activate firmware
kernel-version <running_kernel_version> system-version <running_system_version>
commit-buffer
```

Note

The server status might change to "Disk Failed." You do not need to worry about this message and can continue with this procedure.

- d) Use the **show version** command to verify that the startup versions have been set correctly and to monitor the activation status for the images.

Important

Do not proceed to the next step until the status changes from "Activating" to "Ready."

```
FP9300-A /fabric-interconnect # show version
```

Example:

```
FP9300-A /firmware # top
FP9300-A# scope fabric-interconnect a
FP9300-A /fabric-interconnect # show version
Fabric Interconnect A:
  Running-Kern-Vers: 5.0(3)N2(4.11.69)
  Running-Sys-Vers: 5.0(3)N2(4.11.69)
  Package-Vers: 2.1(1.73)
  Startup-Kern-Vers:
  Startup-Sys-Vers:
  Act-Kern-Status: Ready
```

```

Act-Sys-Status: Ready
Bootloader-Vers:

FP9300-A /fabric-interconnect # activate firmware kernel-version
5.0(3)N2(4.11.69) system-version 5.0(3)N2(4.11.69)
Warning: When committed this command will reset the end-point
FP9300-A /fabric-interconnect* # commit-buffer
FP9300-A /fabric-interconnect # show version
Fabric Interconnect A:
  Running-Kern-Vers: 5.0(3)N2(4.11.69)
  Running-Sys-Vers: 5.0(3)N2(4.11.69)
  Package-Vers: 2.1(1.73)
  Startup-Kern-Vers: 5.0(3)N2(4.11.69)
  Startup-Sys-Vers: 5.0(3)N2(4.11.69)
  Act-Kern-Status: Activating
  Act-Sys-Status: Activating
  Bootloader-Vers:

FP9300-A /fabric-interconnect # show version
Fabric Interconnect A:
  Running-Kern-Vers: 5.0(3)N2(4.11.69)
  Running-Sys-Vers: 5.0(3)N2(4.11.69)
  Package-Vers: 2.1(1.73)
  Startup-Kern-Vers: 5.0(3)N2(4.11.69)
  Startup-Sys-Vers: 5.0(3)N2(4.11.69)
  Act-Kern-Status: Ready
  Act-Sys-Status: Ready
  Bootloader-Vers:

```

Step 11 Reboot the system:**Example:**

```

FP9300-A /fabric-interconnect # top
FP9300-A# scope chassis 1
FP9300-A /chassis # reboot no-prompt
Starting chassis reboot. Monitor progress with the command "show fsm status"
FP9300-A /chassis #

```

The system will power down each security module/engine before finally powering down and then restarting the Firepower 4100/9300 chassis. This process takes approximately 5-10 minutes.

Step 12 Monitor the system status. The server status should go from "Discovery" to "Config" and then finally to "Ok".**Example:**

```

FP9300-A# show server status
Server  Slot Status          Overall Status  Discovery
-----
1/1     Equipped                Discovery      In Progress
1/2     Equipped                Discovery      In Progress
1/3     Empty

```

```

FP9300-A# show server status
Server  Slot Status          Overall Status  Discovery
-----
1/1     Equipped                Config         Complete
1/2     Equipped                Config         Complete
1/3     Empty

```

```

FP9300-A# show server status
Server  Slot Status          Overall Status  Discovery
-----

```

1/1	Equipped	Ok	Complete
1/2	Equipped	Ok	Complete
1/3	Empty		

When the Overall Status is "Ok" your system has been recovered. You must still reconfigure your security appliance (including license configuration) and re-create any logical devices. For more information:

- Firepower 9300 Quick Start Guides—<http://www.cisco.com/go/firepower9300-quick>
- Firepower 9300 Configuration Guides—<http://www.cisco.com/go/firepower9300-config>
- Firepower 4100 Series Quick Start Guides—<http://www.cisco.com/go/firepower4100-quick>
- Firepower 4100 Series Configuration Guides—<http://www.cisco.com/go/firepower4100-config>

Restoring the Factory Default Configuration when the Admin Password is Unknown

This procedure returns your Firepower 4100/9300 chassis system to its default configuration settings, including the admin password. Use this procedure to reset the configurations on your device when the admin password is not known. This procedure erases any installed logical devices as well.



Note This procedure requires console access to the Firepower 4100/9300 chassis.

Procedure

- Step 1** Connect your PC to the console port using the provided console cable, and connect to the console using a terminal emulator set for 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control. For more information on the console cable, see [Cisco Firepower 9300 Hardware Installation Guide](#).
- Step 2** Power on the device. When you see the following prompt, press ESC to stop the boot.

Example:

```
!! Rommon image verified successfully !!

Cisco System ROMMON, Version 1.0.09, RELEASE SOFTWARE
Copyright (c) 1994-2015 by Cisco Systems, Inc.

Current image running: Boot ROM0
Last reset cause: ResetRequest
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!
BIOS has been locked !!

Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address: 00:00:00:00:00:00
```

```
find the string ! boot bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.3.14.69.SPA
bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.3.14.69.SPA
```

Use BREAK, ESC or CTRL+L to interrupt boot.

Use SPACE to begin boot immediately.

Boot interrupted.

```
rommon 1 >
```

Step 3 Make a note of the kickstart and system image names:

Example:

```
bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.3.14.69.SPA
```

```
bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.3.14.69.SPA
```

Step 4 Load the kickstart image:

```
rommon 1 > boot kickstart_image
```

Example:

```
rommon 1 > boot bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.3.14.69.SPA
!! Kickstart Image verified successfully !!
```

```
Linux version: 2.6.27.47 (security@cisco.com) #1 SMP Tue Nov 24 12:10:28 PST 2015
```

```
[ 0.000000] Fastboot Memory at 0c100000 of size 201326592
```

```
Usage: init 0123456SsQqAaBbCcUu
```

```
INIT: POST INIT Starts at Wed Jun 1 13:46:33 UTC 2016
```

```
can't create lock file /var/lock/mtab~302: No such file or directory (use -n flag to override)
```

```
S10mount-ramfs.supnuovaca Mounting /isan 3000m
```

```
Mounted /isan
```

```
TAC support: http://www.cisco.com/tac
```

```
Copyright (c) 2002-2015, Cisco Systems, Inc. All rights reserved.
```

The copyrights to certain works contained in this software are

owned by other third parties and used and distributed under

license. Certain components of this software are licensed under

the GNU General Public License (GPL) version 2.0 or the GNU

Lesser General Public License (LGPL) Version 2.1. A copy of each

such license is available at

<http://www.opensource.org/licenses/gpl-2.0.php> and

<http://www.opensource.org/licenses/lgpl-2.1.php>

```
switch(boot)#
```

Step 5 Enter the config terminal mode:

```
switch(boot) # config terminal
```

Example:

```
switch(boot)#
```

```
switch(boot)# config terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

Step 6 Reset the password and confirm the change:

```
switch(boot) (config) # admin-password erase
```

Note

This step erases all configurations and returns your system to its default configuration settings.

Example:

```
switch(boot) (config) # admin-password erase
```

Your password and configuration will be erased!

Do you want to continue? (y/n) [n] y

Step 7 Exit the config terminal mode:


```
switch boot) (config) # exit
```

- Step 8** Load the system image noted in step 3 of this procedure and configure your system from scratch using the [Initial Configuration Using Console Port, on page 12](#) task flow.

```
switch boot) # load system_image
```

Example:

```
switch boot) # load bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.3.14.69.SPA
```

```
Uncompressing system image: bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.3.14.69.SPA
```

Disaster Recovery of a Firepower Threat Defense Cluster Member

Use this procedure to bring a Firepower 4100/9300 cluster member with Firepower Threat Defense back online and into a cluster after a disaster recovery scenario. Note that if the Firepower Threat Defense application versions associated with the clustered units are out of sync, you will have to follow the steps outlined in [Updating the Image Version for a Logical Device, on page 66](#) to bring them up to the same version.

Before you begin

Use the configuration export feature to export an XML file containing logical device and platform configuration settings for your Firepower 4100/9300 chassis to a remote server or your local computer. For more information, see [About Configuration Import/Export, on page 321](#).

Procedure

- Step 1** Once the secondary unit is up, restore the backup. For instructions on how to import the configuration, see [Importing a Configuration File, on page 327](#). The application installation starts.
- Step 2** Accept the License Agreement.
- Step 3** If necessary, set the application startup version so that the versions on each unit in the cluster match. For instructions on how to set the application startup version, see [Updating the Image Version for a Logical Device, on page 66](#).
- Step 4** Decommission the faulty security module module from the Firepower Chassis Manager using the following steps:
 - a) Navigate to the **Security Modules** page.
 - b) Click on the **Decommission Security Module** button next to the faulty security module.

Figure 13: Decommission Security Module button



- c) Click **Yes** to confirm the change. The hardware status changes to "Mismatch".

Security Modules	Hardware State	Service State	Owner	Application	
Security Module 1	Up	Online	OK	Cisco Firepower Threat Defense	
Security Module 2	Up	Online	OK	Cisco Firepower Threat Defense	
Security Module 3	Mismatch	Not available		Cisco Firepower Threat Defense	

Step 5 Verify the security module status from FXOS CLI.

- a) In the FXOS CLI, enter chassis mode

firepower **scope chassis**

- b) Show the slot:

firepower /ssa # **show slot**

```
FPR9K-1# scope chassis
FPR9K-1 /chassis # show slot
```

Slot:

Slot ID	Slot Status	Admin State	Discovery State
1	Equipped	Acknowledged	Complete
2	Equipped	Acknowledged	Complete
3	Mismatch	Acknowledged	Compl

Note

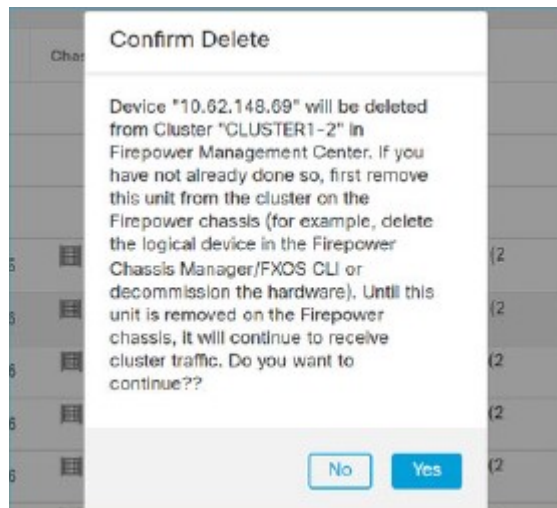
If you don't see this state, wait for 15 and try again. Even after 15 minutes the state is not **Mismatch/Acknowledged/Complete** then collect the FXOS troubleshoot files and contact Cisco TAC

Step 6 Delete the faulty module from FMC.

- a) Navigate to **Device > Device Management > Cluster** page.
b) Select the delete icon next to the faulty security module.

CLUSTER1-2						
Cluster						
10.62.148.69 (Master)	FTD on Firepower 9300 SM-36	6.4.0.6	KSEC-FPR9K-1.cisco.com:443	Base, Threat (2 more...)	basic	
10.62.148.69	FTD on Firepower 9300 SM-36	6.4.0.6	KSEC-FPR9K-1.cisco.com:443	Base, Threat (2 more...)	basic	
10.62.148.70	FTD on Firepower 9300 SM-36	6.4.0.6	KSEC-FPR9K-2:443	Base, Threat (2 more...)	basic	
10.62.148.71	FTD on Firepower 9300 SM-36	6.4.0.6	KSEC-FPR9K-2:443	Base, Threat (2 more...)	basic	
10.62.148.72	FTD on Firepower 9300 SM-36	6.4.0.6	KSEC-FPR9K-2:443	Base, Threat (2 more...)	basic	
FTD1	FTD on Firepower 9300 SM-36	6.4.0.6	KSEC-FPR9K-1.cisco.com:443	Base, Threat (2 more...)	basic	

- c) Click **Yes** to confirm the deletion.



Step 7 Physically replace the faulty security module. Follow the steps described in [Remove and Replace the Security Module](#).

Step 8 From Firepower Chassis Manager, do the following:

- a) Acknowledge the new module. For detailed steps, see [Acknowledge a Security Module/Engine, on page 314](#).
- b) Navigate to **Logical Devices** and select **Set version** for the new module.



Important

Ensure that the startup image version is also available in the chassis image repository (**System > Updates**). If it is not, upload it manually before reinitializing the new security module.

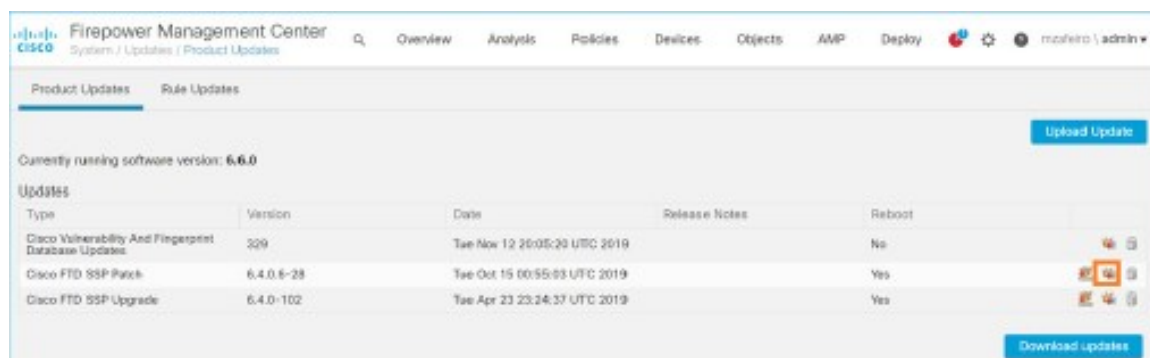
- c) Reinitialize the new security module. For detailed steps, see [Reinitializing a Security Module/Engine, on page 316](#).

Note

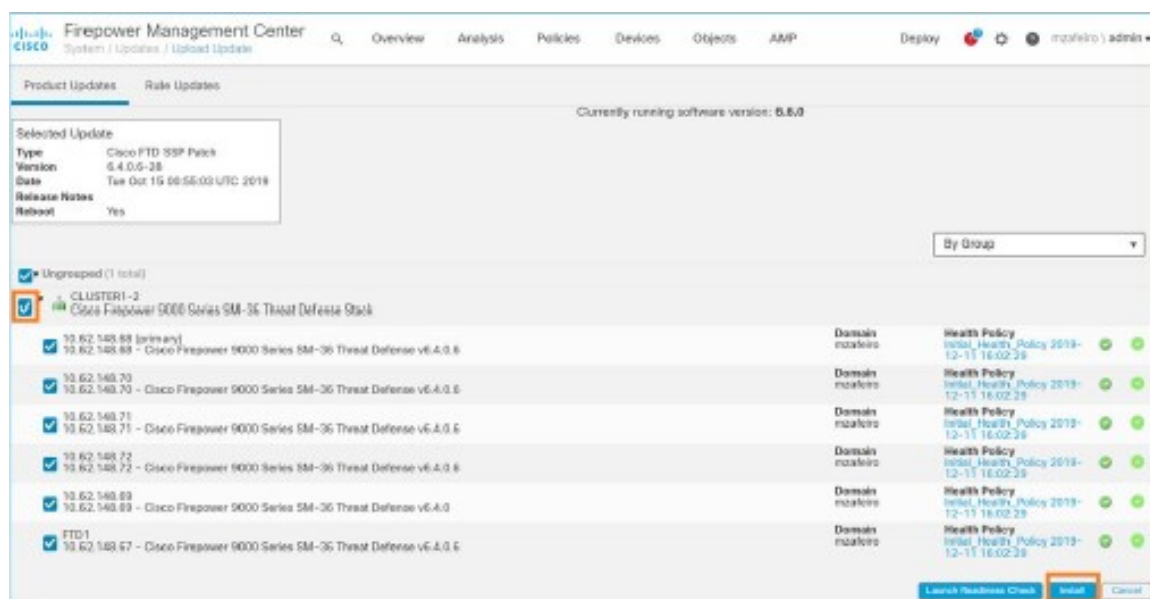
The installation lasts for 15-30 minutes (it depends on the hardware resources) and progresses through a few phases. Once the installation gets completed, the new module gets added to FMC cluster.

Step 9 From FMC, do the following:

- a) Navigate to **Updates** and install the FTD patch.



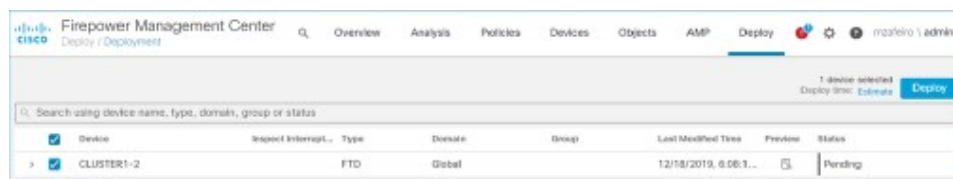
b) Select the cluster and click **Install**.



Note

FMC installs the patch only to the new security module since it is the only one that does not have the patch installed

c) Navigate to **Deploy** page, select the cluster and deploy the policy.



Generating Troubleshooting Log Files

You can generate log files to help with troubleshooting or to send to Cisco TAC if requested.

Procedure

Step 1 Connect to local management mode:

Firepower# connect local-mgmt

Step 2 (Optional) Enter the following command:

Firepower(local-mgmt)# show tech-support ?

The command output shows the components for which you can generate a troubleshooting file.

Example:

```
chassis  Chassis
fprm     Firepower Platform Management
module   Security Module
```

Step 3 Run the following command to generate a troubleshooting file:

Firepower(local-mgmt)# show tech-support <component keyword>

Make sure that you provide the required keyword for the component for which you want to generate a troubleshooting file. For example, the **fprm** keyword generates a troubleshooting file for the Platform Management.

Table 15: Components with Command Examples

Component	Command Example
Chassis	Firepower (local-mgmt)# show tech-support chassis 1
Firepower platform management	Firepower (local-mgmt)# show tech-support fprm detail
Security module	Firepower (local-mgmt)# show tech-support module 1

Example:

```
Firepower(local-mgmt)# show tech-support fprm detail
```

```
Initiating tech-support information task on FABRIC A ...
Completed initiating tech-support subsystem tasks (Total: 1)
All tech-support subsystem tasks are completed (Total: 1[received]/1[expected])
```

```
The detailed tech-support information is located at
workspace:///techsupport/20190827123535_firepower-9300_FPRM.tar
```

Similarly, you can also generate troubleshooting files from chassis and security module.

After a troubleshooting file generates, you can find the file in the workspace.

Step 4 Run the following command to confirm whether the file is generated:

dir workspace:/techsupport

Example:

```

1 34426880 Mar 05 13:10:05 2019 20190305130133_firepower-9300_FPRM.tar
1 56995840 Aug 27 05:30:37 2019 20190827052331_firepower-9300_FPRM.tar
1 56842240 Aug 27 12:42:42 2019 20190827123535_firepower-9300_FPRM.tar

```

```

Usage for workspace://
3999125504 bytes total
148488192 bytes used
3645784064 bytes free

```

Note

If you successfully generate files using all three parameters (fprm, chassis, and module), you should see them in the **/techsupport** directory.

Step 5

Run the following command.

Firepower(local-mgmt)# copy workspace:/techsupport/<troubleshooting file name> ?

The output shows the supported protocols to allow copying the troubleshooting files from FXOS to your local computer. You can use any of the supported protocols.

Example:

```

Firepower(local-mgmt)# copy workspace:/techsupport/
20190917101527_firepower-9300_FPRM.tar ?
ftp:          Dest File URI
http:         Dest File URI
https:        Dest File URI
scp:          Dest File URI
sftp:         Dest File URI
tftp:         Dest File URI
usbdrive:     Dest File URI
volatile:     Dest File URI
workspace:    Dest File URI

```

Before copying a file from FXOS to your computer, make sure that the following prerequisites are met:

- The firewall on your local computer accepts incoming connection over any necessary ports. For example, if you copy a file over Secure Shell, your computer must allow connections from any related ports, such as port 22.
- Your computer must be running the Secure Copy (SCP) service or any of the supported protocols to allow copying a file. You can find various SSH or SCP server software on the internet. However, Cisco does not provide support for installing and configuring any particular SCP server.

Step 6

Run the following command to copy the files.

Firepower(local-mgmt)# copy workspace:/techsupport/<troubleshooting file name> <supported file transfer protocol>://<username>@<destination IP address>

Example:

```

firepower-9300(local-mgmt)# copy workspace:/techsupport/
20190917101527_firepower-9300_FPRM.tar scp:/xyz@192.0.2.1

```

FXOS Enic Devcmd Failure Logs

Devcmd is a mechanism of communication between lina and Cruz firmware. You can see this error logs on the TS files within the LINA **show tech** console logs:

Log syntax: *Enic: Devmcd <devcmd #> failed with error code <error #>*

Message #184 : Enic: Devcmd 107 failed with error code 1
 Message #185 : Enic: Devcmd 9 failed with error code 1
 Message #233 : Enic: Devcmd 9 failed with error code 2

You can use the below tables to identify the devcmd and error strings found in the logs.

devcmd #	devcmd string
1	CMD_MCPU_FW_INFO_OLD
1	CMD_MCPU_FW_INFO
2	CMD_DEV_SPEC
3	CMD_STATS_CLEAR
4	CMD_STATS_DUMP
7	CMD_PACKET_FILTER
7	CMD_PACKET_FILTER_ALL
8	CMD_HANG_NOTIFY
9	CMD_MAC_ADDR/CMD_GET_MAC_ADDR
12	CMD_ADDR_ADD
13	CMD_ADDR_DEL
14	CMD_VLAN_ADD
15	CMD_VLAN_DEL
16	CMD_NIC_CFG
17	CMD_RSS_KEY
18	CMD_RSS_CPU
19	CMD_SOFT_RESET
20	CMD_SOFT_RESET_STATUS
21	CMD_NOTIFY
22	CMD_UNDI
23	CMD_OPEN
24	CMD_OPEN_STATUS
25	CMD_CLOSE
26	CMD_INIT_v1
27	CMD_INIT_PROV_INFO
28	CMD_ENABLE
28	CMD_ENABLE_WAIT
29	CMD_DISABLE

30	CMD_STATS_DUMP_ALL
31	CMD_INIT_STATUS
32	CMD_INT13
33	CMD_LOGICAL_UPLINK
34	CMD_DEINIT
35	CMD_INIT
36	CMD_CAPABILITY
37	CMD_PERBI
38	CMD_IAR
39	CMD_HANG_RESET
40	CMD_HANG_RESET_STATUS
41	CMD_IG_VLAN_REWRITE_MODE
42	CMD_PROXY_BY_BDF
43	CMD_PROXY_BY_INDEX
44	CMD_CONFIG_INFO_GET
45	CMD_INT13_ALL
46	CMD_SET_DEFAULT_VLAN
47	CMD_INIT_PROV_INFO2
48	CMD_ENABLE2
49	CMD_STATUS
50	CMD_INTR_COAL_CONVERT
51	CMD_ISCSI_DUMP_REQ
52	CMD_ISCSI_DUMP_STATUS
53	CMD_MIGRATE_SUBVNIC
54	CMD_SUBVNIC_NOTIFY
55	CMD_SET_MAC_ADDR
56	CMD_PROV_INFO_UPDATE
57	CMD_INITIALIZE_DEVCMD2
58	CMD_ADD_FILTER
59	CMD_DEL_FILTER
61-74	Queue Pair/RDMA/Overlay Offload
106	CMD_SET_FT_CFG
107	CMD_GET_FT_CFG

108	CMD_SET_FT_CTRL
109	CMD_GET_FT_CTRL
110	CMD_CFG_FQ
111	CMD_GET_SHLIF_STATS
112	CMD_CLEAR_SHLIF_STATS
113	CMD_UPDATE_RWMEM_BASE
114	CMD_SET_FT_CFG_CMP

Error Code #	Error String
1	ERR_EINVAL
2	ERR_EFAULT
3	ERR_EPERM
4	ERR_EBUSY
5	ERR_ECMDUNKNOWN
6	ERR_EBADSTATE
7	ERR_ENOMEM
8	ERR_ETIMEDOUT
9	ERR_ELINKDOWN
10	ERR_EMAXRES
11	ERR_ENOTSUPPORTED
12	ERR_EINPROGRESS

Enabling Module Core Dumps

Enabling core dumps on a module can help with troubleshooting in the event of a system crash, or to send to Cisco TAC if requested.

Procedure

Step 1 Connect to the desired module; for example:

Firepower# connect module 1 console

Step 2 (Optional) Enter the following command to view current core dump status:

Firepower-module1> show coredump detail

The command output shows current core dump status information, including whether core dump compression is enabled.

Example:

```
Firepower-module1>show coredump detail
Configured status: ENABLED.
ASA Coredump: ENABLED.
Bootup status: ENABLED.
Compress during crash: DISABLED.
```

Note

This command is available only when running ASA Logical device on appliance and not when running Firepower Threat Defense Logical device on appliance.

Step 3

Use the **config coredump** command to enable or disable core dumps, and to enable or disable core dump compression during a crash.

- Use **config coredump enable** to enable creation of a core dump during a crash.
- Use **config coredump disable** to disable core dump creation during a crash.
- Use **config coredump compress enable** to enable compression of core dumps.
- Use **config coredump compress disable** to disable core dump compression.

Example:

```
Firepower-module1>config coredump enable
Coredump enabled successfully.
ASA coredump enabled, do 'config coredump disableAsa' to disable
Firepower-module1>config coredump compress enable
WARNING: Enabling compression delays system reboot for several minutes after a system
failure. Are you sure? (y/n):
y
Firepower-module1>
```

Note

Core dump files consume disk space, and if space is running low and compression is not enabled, a core dump file may not be saved even if core dumps are enabled.

Finding the Serial Number of the Firepower 4100/9300 Chassis

You can find details about the Firepower 4100/9300 Chassis and its serial number. Note that serial number of Firepower 4100/9300 Chassis is different than serial numbers of the logical devices.

Procedure

Step 1 Enter the chassis scope:

scope chassis

Example:

```
Firepower# scope chassis
Firepower /chassis #
```

Step 2 View inventory details:

show inventory

Example:

```
Firepower /chassis # show inventory
```

The output shows the serial number and other details.

Chassis	PID	Vendor	Serial (SN)	HW Revision
1	FPR-C9300-AC	Cisco Systems Inc	JMX1950196H	0

Rebuild RAID Virtual Drive

RAID (Redundant Array of Independent Disks) is an array, or group, of multiple independent physical drives that provide high performance and fault tolerance. A drive group is a group of physical drives. These drives are managed in partitions known as virtual drives.

RAID drive groups improve data storage reliability and fault tolerance compared to single-drive storage systems. Data loss resulting from a drive failure can be prevented by reconstructing missing data from the remaining drives. RAID improves I/O performance and increases storage subsystem reliability.

If one of your RAID drives has failed or is offline, then the RAID virtual drive is considered to be in a degraded state. Use this procedure to verify whether a RAID virtual drive is in a degraded state, and temporarily set the local disk configuration protection policy to no to rebuild it if necessary.



Note When you set the local disk configuration protection policy to no, all data on the disk is destroyed.

Procedure

Step 1 Check the RAID drive status.

- a. Enter chassis mode:
scope chassis
- b. Enter server mode:
scope server 1
- c. Enter the raid controller:
scope raid-controller 1 sas
- d. View the virtual drive:
show virtual-drive

If the RAID virtual drive is degraded, the operability displays as **Degraded**. For example:

```

Virtual Drive:
  ID: 0
  Block Size: 512
  Blocks: 3123046400
  Size (MB): 1524925
  Operability: Degraded
  Presence: Equipped

```

Step 2 Set the local disk configuration policy protection to no to rebuild the RAID drive. Note - all data on the disk will be destroyed after you complete this step.

- a. Enter the organization scope:
scope org
- b. Enter the local disk configuration policy scope:
scope local-disk-config-policy ssp-default
- c. Set protect to no:
set protect no
- d. Commit the configuration:
commit-buffer

Step 3 Wait for the RAID drive to rebuild. Check the RAID rebuild status:

scope chassis 1

show server

When the RAID drive has rebuilt successfully, the slot's overall status displays as **Ok**. For example:

Example:

```

Server:
  Slot      Overall Status      Service Profile
  -----
    1  Ok                      ssp-sprof-1

```

Step 4 Once the RAID drive has rebuilt successfully, set the local disk configuration policy protection back to yes.

- a. Enter the organization scope:
scope org
- b. Enter the local disk configuration policy scope:
scope local-disk-config-policy ssp-default
- c. Set protect to yes:
set protect yes
- d. Commit the configuration:
commit-buffer

Identify Issues with the SSD

Use the following procedure to collect information and identify possible issues with the SSD installed on your device. One example symptom of an SSD issue is the Data Management Engine (DME) process failing to start.



Note When you insert a new SSD, only the basic information (Type, Model, SN, etc.) gets populated under inventory after the Blade BIOS detection. Only upon the SSP-OS upgrade completion, the Local Disk data gets populated under inventory. If the SSP-OS upgrade is still under "Updating state", the inventory shows no entry for the Local Disk and no fault messages regarding connection of the SSD.

If the output of the below logging files indicate a problem with the SSD, contact TAC (see <https://www.cisco.com/c/en/us/buy/product-returns-replacements-rma.html>).

Procedure

Step 1 Connect to the FXOS command shell:

connect fxos

Step 2 Display the nvram logging file:

show logging nvram

Example error output:

```
2020 Oct 22 13:03:26 MDCNGIPSAPL02 %$ VDC-1 %$ Oct 22 13:03:25 %KERN-2-SYSTEM_MSG:
[28175880.598580] EXT3-fs error (device sda4): ext3_get_inode_loc: unable to read inode
block - inode=14, block=6
```

Step 3 Display the logging file:

show logging logfile

Example error output:

```
2020 Oct 21 21:11:25 (none) kernel: [28118744.718445] EXT3-fs error (device sda4):
ext3_get_inode_loc: unable to read inode block - inode=14, block=6
```




INDEX

A

AAA [147–148](#), [151–152](#), [154–156](#)
 LDAP providers [147–148](#), [151](#)
 RADIUS providers [151–152](#), [154](#)
 TACACS+ providers [154–156](#)
 accessing the command line interface [18](#)
 accounts [42](#), [50](#), [52](#), [57](#)
 locally authenticated [42](#), [50](#), [52](#), [57](#)
 acknowledging Network modules [317](#)
 acknowledging security modules [314](#)
 asa [66](#), [229](#), [234](#), [256](#), [294](#), [296](#), [299](#)
 connecting to [294](#)
 creating a cluster [256](#)
 creating a clustered [229](#)
 creating a standalone asa logical device [234](#)
 deleting a logical device [296](#)
 deleting an application instance [299](#)
 exiting from connection [294](#)
 updating image version [66](#)
 asa images [59–60](#), [64](#)
 about [59](#)
 downloading from Cisco.com [60](#)
 downloading to the security appliance [64](#)
 authentication [43](#)
 default [43](#)
 authNoPriv [122](#)
 authPriv [122](#)

B

banner [101–103](#)
 pre-login [101–103](#)
 breakout cables [202](#)
 configuring [202](#)
 breakout ports [202](#)

C

call home [26](#)
 configure http proxy [26](#)
 certificate [131](#)
 about [131](#)
 chassis [11](#)
 initial configuration [11](#)

Chassis [2](#)
 monitoring health [2](#)
 Cisco Secure Package [59–60](#), [64](#)
 about [59](#)
 downloading from Cisco.com [60](#)
 downloading to the security appliance [64](#)
 cli, *See* command line interface
 CLI session limits [10](#)
 clustering [225](#), [229](#), [231](#), [253–254](#)
 cluster control link [253](#)
 redundancy [253](#)
 size [253](#)
 device-local EtherChannels, configuring on switch [231](#)
 management [254](#)
 network [254](#)
 member requirements [225](#)
 software requirements [225](#)
 spanning-tree portfast [229](#)
 upgrading software [225](#)
 clusters [229](#), [252](#), [256](#), [265](#)
 about [252](#)
 creating [229](#), [256](#), [265](#)
 command line interface [18](#)
 accessing [18](#)
 command modes [5](#)
 commands [9](#)
 history [9](#)
 communication services [124](#), [132–135](#), [137–138](#)
 HTTPS [132–135](#), [137–138](#)
 SNMP [124](#)
 community, SNMP [124](#)
 configuration import/export [321–322](#)
 encryption key [322](#)
 guidelines [321](#)
 restrictions [321](#)
 configuring [132–135](#), [137–138](#)
 HTTPS [132–135](#), [137–138](#)
 connecting to a logical device [294](#)
 console [45–46](#)
 timeout [45–46](#)
 coredumps [369](#)
 generating [369](#)
 corrupted file system [349](#)
 recovering [349](#)
 creating packet capture session [333](#)

CSP, *See* Cisco Secure Package

D

date [108, 113](#)
 setting manually [113](#)
 viewing [108](#)
 date and time [107](#)
 configuring [107](#)
 decommissioning security modules [314](#)
 deleting packet capture sessions [339](#)
 device name [92](#)
 changing [92](#)
 DNS [161](#)
 downloading packet capture file [338](#)

E

enabling [124](#)
 SNMP [124](#)
 encryption key [322](#)
 enforcing password strength [48](#)
 exiting from logical device connection [294](#)
 export configuration [321](#)

F

factory default configuration [104](#)
 restoring [104](#)
 Firepower chassis [11, 103–104](#)
 initial configuration [11](#)
 powering off [104](#)
 rebooting [103](#)
 firmware [68](#)
 upgrading [68](#)
 fpga [68](#)
 upgrading [68](#)
 ftd, *See* threat defense
 FXOS [63](#)
 upgrading the platform bundle [63](#)
 FXOS chassis, *See* Chassis

H

high-level task list [11](#)
 history, passwords [42](#)
 http proxy [26](#)
 configuring [26](#)
 HTTPS [45–46, 132–135, 137–138, 140–141, 144](#)
 certificate request [134–135](#)
 changing port [141](#)
 configuring [140](#)
 creating key ring [132](#)
 disabling [144](#)
 importing certificate [138](#)

HTTPS (*continued*)

 regenerating key ring [133](#)
 timeout [45–46](#)
 trusted point [137](#)

I

image version [66](#)
 updating [66](#)
 images [59–60, 62–64](#)
 downloading from Cisco.com [60](#)
 downloading to the Firepower security appliance [60](#)
 downloading to the security appliance [64](#)
 managing [59](#)
 upgrading the FXOS platform bundle [63](#)
 verifying integrity [62](#)
 import configuration [321](#)
 informs [122](#)
 about [122](#)
 initial configuration [11–12, 14](#)
 using Console port [12](#)
 using Management port [14](#)
 interfaces [170, 195](#)
 configuring [170, 195](#)
 properties [170, 195](#)

K

key ring [131–135, 137–138, 143](#)
 about [131](#)
 certificate request [134–135](#)
 creating [132](#)
 deleting [143](#)
 importing certificate [138](#)
 regenerating [133](#)
 trusted point [137](#)

L

LDAP [147–148, 151](#)
 LDAP providers [148, 151](#)
 creating [148](#)
 deleting [151](#)
 license [28](#)
 registering [28](#)
 license authority [28](#)
 locally authenticated users [42, 50, 52, 57](#)
 change interval [50](#)
 clearing password history [57](#)
 no change interval [52](#)
 password history count [52](#)
 password profile [42](#)
 log files [364](#)
 generating [364](#)

logical devices [66, 229, 234, 240, 256, 265, 294, 296, 299](#)
 connecting to [294](#)
 creating a cluster [229, 256, 265](#)
 creating a standalone [234, 240](#)
 deleting [296](#)
 deleting an application instance [299](#)
 exiting from connection [294](#)
 updating image version [66](#)
 low-touch provisioning [14](#)
 using Management port [14](#)

M

managed objects [5](#)
 management interface [341](#)
 status [341](#)
 management IP address [87](#)
 changing [87](#)
 monitoring chassis health [2](#)

N

Network modules [317](#)
 acknowledging [317](#)
 noAuthNoPriv [122](#)
 NTP [107, 110, 113](#)
 adding [110](#)
 configuring [107, 110](#)
 deleting [113](#)

O

object commands [8](#)

P

packet capture [331, 333, 336–339](#)
 creating packet capture session [333](#)
 deleting packet capture sessions [339](#)
 downloading PCAP file [338](#)
 filter [336](#)
 starting a packet capture session [337](#)
 stopping a packet capture session [337](#)
 password profile [42, 50, 52, 57](#)
 about [42](#)
 change interval [50](#)
 clearing password history [57](#)
 no change interval [52](#)
 password history count [52](#)
 passwords [39, 42–43, 48](#)
 change interval [43](#)
 guidelines [39](#)
 history count [42](#)
 strength check [48](#)
 PCAP, *See* packet capture

PCAP file [338](#)
 downloading [338](#)
 pending commands [9](#)
 ping [340](#)
 PKI [131](#)
 platform bundle [59–60](#)
 about [59](#)
 downloading to the Firepower security appliance [60](#)
 Platform bundle [59–60, 62–63](#)
 about [59](#)
 downloading from Cisco.com [60](#)
 downloading to the security appliance [60](#)
 upgrading [63](#)
 verifying integrity [62](#)
 policies [47](#)
 role for remote users [47](#)
 port channel [342](#)
 status [342](#)
 port channels [197](#)
 configuring [197](#)
 powering off Firepower chassis [104](#)
 pre-login banner [101–103](#)
 creating [101](#)
 deleting [103](#)
 modifying [102](#)
 profiles [42](#)
 password [42](#)

R

RADIUS [151–152, 154](#)
 RADIUS providers [152, 154](#)
 creating [152](#)
 deleting [154](#)
 rebooting [103](#)
 registering a license [28](#)
 reinitializing security modules [316](#)
 resetting security modules [315](#)
 restoring the factory default configuration [104](#)
 role policy for remote users [47](#)
 rommon [68](#)
 upgrading [68](#)
 RSA [131](#)

S

Security appliance [1](#)
 overview [1](#)
 security modules [314–317](#)
 acknowledging [314](#)
 decommissioning [314](#)
 reinitializing [316](#)
 resetting [315](#)
 taking offline [317](#)
 taking online [317](#)

- session timeout [45–46](#)
- smart call home [26](#)
 - configure http proxy [26](#)
- Smart Transport [26](#)
 - configure http proxy [26](#)
- SNMP [121–125, 127–128, 130](#)
 - about [121](#)
 - community [124](#)
 - current settings [130](#)
 - enabling [124](#)
 - notifications [122](#)
 - privileges [122](#)
 - security levels [122](#)
 - support [121, 123](#)
 - traps [125, 127](#)
 - creating [125](#)
 - deleting [127](#)
 - users [128, 130](#)
 - creating [128](#)
 - deleting [130](#)
 - Version 3 security features [123](#)
- SNMPv3 [123](#)
 - security features [123](#)
- software failure [344](#)
 - recovering [344](#)
- SSH [45–46, 114](#)
 - configuring [114](#)
 - timeout [45–46](#)
- syslog [158](#)
 - configuring local destinations [158](#)
 - configuring local sources [158](#)
 - configuring remote destinations [158](#)
- system [11](#)
 - initial configuration [11](#)
- system recovery [344, 349](#)

T

- TACACS+ [154–156](#)
- TACACS+ providers [155–156](#)
 - creating [155](#)
 - deleting [156](#)
- taking security modules offline and online [317](#)
- task flow [11](#)
- Telnet [45–46, 120](#)
 - configuring [120](#)
 - timeout [45–46](#)
- threat defense [229, 240, 265, 294, 296, 299](#)
 - connecting to [294](#)
 - creating a cluster [265](#)
 - creating a clustered [229](#)
 - creating a standalone threat defense logical device [240](#)

- threat defense (*continued*)
 - deleting a logical device [296](#)
 - deleting an application instance [299](#)
 - exiting from connection [294](#)
- Threat Defense, *See* threat defense
- threat defense images [64](#)
 - downloading to the security appliance [64](#)
- time [108, 113](#)
 - setting manually [113](#)
 - viewing [108](#)
- time zone [108, 110, 113](#)
 - setting [108, 110, 113](#)
- timeout [45–46](#)
 - console [45–46](#)
 - HTTPS, SSH, and Telnet [45–46](#)
- traceroute [340](#)
 - connectivity tests [340](#)
- traps [122, 125, 127](#)
 - about [122](#)
 - creating [125](#)
 - deleting [127](#)
- troubleshooting [341–342, 364, 369](#)
 - generating coredumps [369](#)
 - generating log files [364](#)
 - management interface [341](#)
 - port channel status [342](#)
- trusted points [131, 137, 143](#)
 - about [131](#)
 - creating [137](#)
 - deleting [143](#)

U

- upgrading the firmware [68](#)
- user accounts [42, 50, 52, 57](#)
 - password profile [42, 50, 52, 57](#)
- users [10, 37–39, 42–43, 47–48, 50, 52–53, 56–57, 128, 130](#)
 - activating [56](#)
 - CLI session limits [10](#)
 - creating [53](#)
 - deactivating [56](#)
 - default authentication [43](#)
 - deleting [56](#)
 - locally authenticated [42, 50, 52, 57](#)
 - managing [37](#)
 - naming guidelines [38](#)
 - password guidelines [39](#)
 - password strength check [48](#)
 - remote, role policy [47](#)
 - roles [42](#)
 - SNMP [128, 130](#)