Cisco Firepower 2100 ASA Platform Mode FXOS Configuration Guide

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 NONINFRINGEMENT 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.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

CONTENTS

CHAPTER 3

CHAPTER 1

Introduction to FXOS for Firepower 2100 ASA Platform Mode

The Firepower 2100 is a single-application appliance for the Secure Firewall ASA. The Firepower 2100 runs an underlying operating system called the Secure Firewall eXtensible Operating System (FXOS).

You can run the Firepower 2100 in the following modes:

- Appliance mode (the default)—Appliance mode lets you configure all settings in the ASA. Only advanced troubleshooting commands are available from the FXOS CLI.
- Platform mode—When in Platform mode, you must configure basic operating parameters and hardware interface settings in FXOS. These settings include enabling interfaces, establishing EtherChannels, NTP, image management, and more. You can use the Secure Firewall Chassis Manager (formerly Firepower Chassis Manager) web interface or FXOS CLI. You can then configure your security policy in the ASA operating system using Adaptive Security Device Manager (ASDM) or the ASA CLI.

This guide describes the available FXOS settings for Platform Mode only.

ASA and FXOS Management

The ASA and FXOS operating systems share the Management 1/1 interface. This interface has separate IP addresses for connecting to ASA and to FXOS.

Note This interface is called Management 1/1 in the ASA; in FXOS, you might see it displayed as MGMT, management0, or other similar names. This guide refers to this interface as Management 1/1 for consistency and simplicity.

Some functions must be monitored on FXOS and others on the ASA, so you need to make use of both operating systems for ongoing maintenance. For initial configuration on FXOS, you can connect to the default 192.168.45.45 IP address using SSH or your browser (https://192.168.45.45).

For initial configuration of the ASA, you can connect using ASDM to https://192.168.45.1/admin. In ASDM, you can later configure SSH access from any interface.

Both operating systems are available from the console port. Initial connection accesses the FXOS CLI. You can access the ASA CLI using the **connect asa** command.

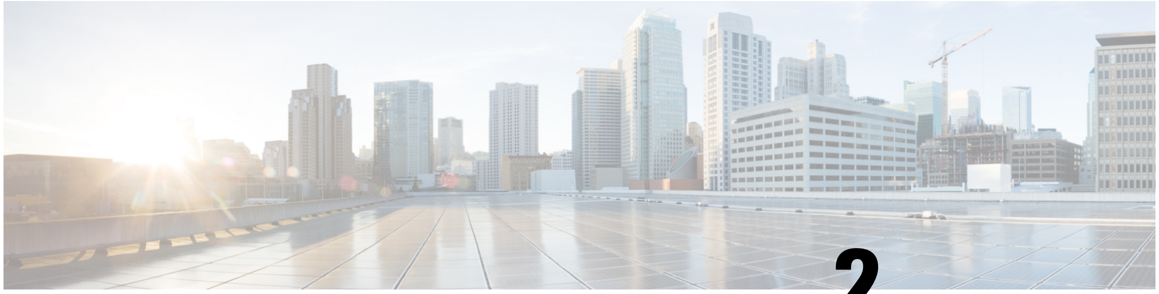
You can also allow FXOS management from ASA data interfaces; configure SSH, HTTPS, and SNMP access. This feature is useful for remote management.

Unsupported Features

The following FXOS features are not supported on the Firepower 2100:

- Backup and restore FXOS configuration
- External AAA Authentication for FXOS

  Note that when you connect to the ASA console from FXOS (**connect asa**), then ASA AAA configuration for console access applies (**aaa authentication serial console**).



CHAPTER 2

Chassis Manager Settings

The Firepower 2100 runs FXOS to control basic operations of the device. You can use the GUI chassis manager or the FXOS CLI to configure these functions; this document covers the chassis manager. Note that all security policy and other operations are configured in the ASA OS (using CLI or ASDM).

Overview

On the **Overview** tab, you can easily monitor the status of the Firepower 2100. The **Overview** tab provides the following elements:

- Device Information—The top of the **Overview** tab contains the following information about the Firepower 2100:
    - Chassis name—Shows the name assigned to the chassis. By default, the name is **firepower-***model*, for example, firepower-2140. This name appears in the CLI prompt. To change the chassis name, use the FXOS CLI **scope system / set name** command.
    - IP address—Shows the management IP address assigned to the chassis.
    - Model—Shows the Firepower 2100 model.
    - Version—Shows the ASA version number running on the chassis.
    - Operational State—Shows the operable status for the chassis.
    - Chassis uptime—Shows the elapsed time since the system was last restarted.
    - Uptime Information Icon—Hover over the icon to see uptime for the chassis and for the ASA security engine.
- Visual Status Display—Below the Device Information section is a visual representation of the chassis that shows the components that are installed in the chassis and provides a general status for those

components. You can hover over the ports that are shown in the Visual Status Display to get additional information such as interface name, speed, type, admin state, and operational state.

- Detailed Status Information—Below the Visual Status Display is a table containing detailed status information for the chassis. The status information is broken up into these sections: Faults, Interfaces, Devices, and Inventory. You can see a summary for each of those sections above the table and you can see additional details for each of those sections by clicking on the summary area for the information you want to view.

  The system provides the following detailed status information for the chassis:

  - **Faults**—Lists the faults that have been generated in the system. The faults are sorted by severity: Critical, Major, Minor, Warning, and Info. For each fault that is listed, you can see the severity, a description of the fault, the cause, the number of occurrences, and the time of the most recent occurrence. You can also see whether the fault has been acknowledged or not.

    You can click on any of the faults to see additional details for the fault or to acknowledge the fault.

    Note Once the underlying cause of the fault has been addressed, the fault will automatically be cleared from the listing during the next polling interval. If a user is working on a resolution for a specific fault, they can acknowledge the fault to let other users know that the fault is currently being addressed.

  - **Interfaces**—Lists the interfaces installed in the system and shows the interface name, operational status, administrative status, number of received bytes, and number of transmitted bytes.

    You can click on any interface to see a graphical representation of the number of input and output bytes for that interface over the last fifteen minutes.

  - **Devices**— Shows the ASA, and provides the following details: device name, device state, application, operational state, administrative state, image version, and management IP address.

  - **Inventory**—Lists the components installed in the chassis and provides relevant details for those components, such as: **component** name, number of cores, installation location, operational status, operability, capacity, power, thermal, serial number, model number, part number, and vendor.

Interfaces

You can manage physical interfaces in FXOS. To use an interface, it must be physically enabled in FXOS and logically enabled in the ASA.

The Firepower 2100 has support for jumbo frames enabled by default. The maximum MTU is 9184.

Note If you change the interfaces in FXOS after you enable failover (by adding or removing a network module, or by changing the EtherChannel configuration, for example), make the interface changes in FXOS on the standby unit, and then make the same changes on the active unit.

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.

Configure Interfaces

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 ASA.

Procedure

Step 1 Click the **Interfaces** tab.

Step 2 To enable or disable an interface, click the **Admin State** slider. A check mark shows it as enabled, while an X shows it as disabled.

Note The Management 1/1 interface shows as **MGMT** in this table.

Step 3 Click the **Edit** pencil icon for the interface for which you want to edit the speed or duplex.

Note You can only enable or disable the Management 1/1 interface; you cannot edit its properties.

Step 4 Check the **Enable** check box to enable the interface.

Step 5 From the **Admin Speed** drop-down list, choose the speed of the interface.

Step 6 Click the **Auto Negotiation Yes** or **No** radio button.

Step 7 From the **Admin Duplex** drop-down list, choose the duplex of the interface.

Step 8 Click **OK**.

Add an EtherChannel

An EtherChannel (also known as a port-channel) can include up to 8 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.

Note EtherChannel member ports are visible on the ASA, but you can only configure EtherChannels and port membership in FXOS.

If you change the EtherChannel configuration after you enable failover, make the interface changes in FXOS on the standby unit, and then make the same changes on the active unit.

Note The ASA does not support LACP rate fast; LACP always uses the normal rate.

Before you begin

The Firepower 2100 supports EtherChannels in Link Aggregation Control Protocol (LACP) Active or On mode. By default, the LACP mode is set to Active; you can change the mode to On at the CLI. We suggest setting the connecting switch ports to Active mode for the best compatibility.

Procedure

Step 1 Click the **Interfaces** tab.

Step 2 Click **Add Port Channel** above the interfaces table.

Step 3 In the **Port Channel ID** field, enter an ID for the port channel. Valid values are between 1 and 47.

Step 4 Check the **Enable** check box to enable the port channel.

Ignore the **Type** drop-down list; the only available type is **Data**.

Step 5 From the **Admin Speed** drop-down list, choose the speed for all member interfaces.

If you choose interfaces that are not capable of the speed (and other settings that you choose), the fastest possible speed is automatically applied.

Step 6 Click the **Auto Negotiation Yes** or **No** radio button for all member interfaces.

Step 7 **Admin Duplex** drop-down list, choose the duplex for all member interfaces.

Step 8 In the **Available Interface** list, select the interface you want to add, and click **Add Interface**.

You can add up to 8 interfaces.

Tip You can add multiple interfaces at one time. To select multiple individual interfaces, click on the desired interfaces while holding down the **Ctrl** key. To select a range of interfaces, select the first interface in the range, and then, while holding down the **Shift** key, click to select the last interface in the range.

Note When you assign an interface to an EtherChannel, then the ASA configuration retains the original interface 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.

For example, after you assign Ethernet1/4 to Port-channel7 in FXOS, Ethernet1/4 still shows as an available interface in the ASA OS, and any configuration for Ethernet1/4 is retained. If you enter **show interface ethernet1/4**, the ASA shows that the interface is “not associated with the Supervisor”. Use the **no interface ethernet1/4** command to remove the extraneous configuration.

Step 9 Click **OK**.

Monitoring Interfaces

On the **Interfaces** tab, you can view the status of the installed interfaces on the chassis. The lower section contains a table of the interfaces installed in the chassis. The upper section shows a visual representation of the interfaces that are installed in the chassis. You can hover over any of the interfaces in the upper section to get additional information about the interface.

The interfaces are color coded to indicate their current status:

- Green—The operational state is Up.
- Dark Grey—The admin state is Disabled.
- Red—The operational state is Down.
- Light Grey—The SFP is not installed.

Logical Devices

The **Logical Devices** page shows information and status about the ASA. You can also disable or renable the ASA for troubleshooting purposes using the slider (a check mark shows it as enabled, while an X shows it as disabled).

The header for the ASA provides the **Status**:

- **ok**—The logical device configuration is complete.
- **incomplete-configuration**—The logical device configuration is incomplete.

The logical device area also provides more detailed **Status** for the ASA:

- **Online**—The ASA is running and operating.
- **Offline**—The ASA is stopped and inoperable.
- **Installing**—The ASA installation is in progress.
- **Not Installed**—The ASA is not installed.
- **Install Failed**—The ASA installation failed.

- **Starting**—The ASA is starting up.
- **Start Failed**—The ASA failed to start up.
- **Started**—The ASA started successfully, and is waiting for app agent heartbeat.
- **Stopping**—The ASA is in the process of stopping.
- **Stop Failed**—The ASA was unable to be brought offline.
- **Not Responding**—The ASA is unresponsive.
- **Updating**—The ASA software upgrade is in progress.
- **Update Failed**—The ASA software upgrade failed.
- **Update Succeeded**—The ASA software upgrade succeeded.

Platform Settings

The **Platform Settings** tab lets you set basic operations for FXOS including the time and administrative access.

NTP: Set the Time

You can set the clock manually, or use an NTP server (recommended). You can configure up to four NTP servers.

Before you begin

- NTP is configured by default with the following Cisco NTP servers: 0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org,2.sourcefire.pool.ntp.org.
- If you use a hostname for the NTP server, you must configure a DNS server. See DNS: Configure DNS Servers, on page 18.

Procedure

Step 1 Click the **Platform Settings** tab, and click **NTP** in the left-hand navigation.

The **Time Synchronization** tab is selected by default.

Step 2 To use an NTP server:

a) Click the **Use NTP Server** radio button.

b) (Optional) (ASA 9.10(1) and later) Check the **NTP Server Authentication: Enable** check box if you need to authenticate with the NTP server.

Click **Yes** to require an authentication key ID and value.

Only SHA1 is supported for NTP server authentication.

c) Click **Add** to identify up to 4 NTP servers by IP address or hostname.

If you use a hostname for the NTP server, configure a DNS server later in this procedure.

d) (ASA 9.10(1) and later) Enter the NTP server's **Authentication Key** ID and **Authentication Value**.

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.

e) Click **Save** to save the server.

Step 3 To set the time manually:

a) Click the **Set Time Manually** radio button.
b) Click the **Date** drop-down list to display a calendar, and then set the date using the controls available in the calendar.
c) Use the corresponding drop-down lists to specify the time as hours, minutes, and **AM/PM**.

Step 4 Click the **Current Time** tab, and from the **Time Zone** drop-down list, choose the appropriate time zone for the chassis.

Step 5 Click **Save**.

Note If you modify the system time by more than 10 minutes, the system will log you out and you will need to log in to the Secure Firewall chassis manager again.

SSH: Configure SSH

The following procedure describes how to enable or disable SSH access to the chassis, and to enable the chassis as an SSH client. The SSH server and client are enabled by default.

Procedure

Step 1 Choose **Platform Settings** > **SSH** > **SSH Server**.

Step 2 To enable the SSH server to provide SSH access to the chassis, check the **Enable SSH** check box.

Step 3 For the server **Encryption Algorithm**, check the check boxes for each allowed encryption algorithm.

Step 4 For the server **Key Exchange Algorithm**, check the check boxes for each allowed Diffie-Hellman (DH) key exchange.

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 5 For the server **Mac Algorithm**, check the check boxes for each allowed integrity algorithm.

Step 6 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.

Step 7 For the server **Volume Rekey Limit**, set the amount of traffic in KB allowed over the connection before FXOS disconnects the session.

Step 8 For the server **Time Rekey Limit**, set the minutes for how long an SSH session can be idle before FXOS disconnects the session.

Step 9 Click **Save**.

Step 10 Click the **SSH Client** tab to customize the FXOS chassis SSH client.

Step 11 For the **Strict Host Keycheck**, choose **enable**, **disable**, or **prompt** to control SSH host key checking.

- **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 For the client **Encryption Algorithm**, check the check boxes for each allowed encryption algorithm.

Step 13 For the client **Key Exchange Algorithm**, check the check boxes for each allowed Diffie-Hellman (DH) key exchange.

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 For the client **Mac Algorithm**, check the check boxes for each allowed integrity algorithm.

Step 15 For the client **Volume Rekey Limit**, set the amount of traffic in KB allowed over the connection before FXOS disconnects the session.

Step 16 For the client **Time Rekey Limit**, set the minutes for how long an SSH session can be idle before FXOS disconnects the session.

Step 17 Click **Save**.

SNMP: Configure SNMP

Use the **SNMP** page to configure the Simple Network Management Protocol (SNMP) on the chassis.

About SNMP

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.

- 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.

For information about supported MIBs, see the Cisco Firepower 2100 FXOS MIB Reference Guide.

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.

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 1: 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.

Model	Level	Authentication	Encryption	What Happens
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
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 supported MIBs, see the Cisco Firepower 2100 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

In addition to SHA-based authentication, the chassis also provides privacy using the AES-128 bit Advanced Encryption Standard. 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 80 characters.

Configure SNMP

Enable SNMP, add traps and SNMPv3 users.

Procedure

Step 1 Choose **Platform Settings** > **SNMP**.

Step 2 In the **SNMP** area, complete the following fields:

Name	Description
Admin State check box	Whether SNMP is enabled or disabled. Enable this service only if your system includes integration with an SNMP server.
Port field	The port on which the Firepower chassis communicates with the SNMP host. You cannot change the default port.
Community/Username field	The default SNMP v1 or v2 community name or SNMP v3 username the Firepower chassis includes on any trap messages it sends to the SNMP host. Enter an alphanumeric string between 1 and 32 characters. Do not use @ (at sign), \ (backslash), " (double quote), ? (question mark) or an empty space. The default is `public`. Note that if the **Community/Username** field is already set, the text to the right of the empty field reads **Set: Yes**. If the **Community/Username** field is not yet populated with a value, the text to the right of the empty field reads **Set: No**.
System Administrator Name field	The contact person responsible for the SNMP implementation. Enter a string of up to 255 characters, such as an email address or a name and telephone number.
Location field	The location of the host on which the SNMP agent (server) runs. Enter an alphanumeric string up to 510 characters.

Step 3 In the **SNMP Traps** area, click **Add**.

Step 4 In the **Add SNMP Trap** dialog box, complete the following fields:

Name	Description
Host Name field	The hostname or IP address of the SNMP host to which the Firepower chassis should send the trap.
Community/Username field	The SNMP v1 or v2 community name or the SNMP v3 username the Firepower chassis includes when it sends the trap to the SNMP host. This must be the same as the community or username that is configured for the SNMP service. Enter an alphanumeric string between 1 and 32 characters. Do not use @ (at sign), \ (backslash), " (double quote), ? (question mark) or an empty space.

Name	Description
Port field	The port on which the Firepower chassis communicates with the SNMP host for the trap. Enter an integer between 1 and 65535.
Version field	The SNMP version and model used for the trap. This can be one of the following: • **V1** • **V2** • **V3**
Type field	If you select **V2** or **V3** for the version, the type of trap to send. This can be one of the following: • **Traps** • **Informs**
v3 Privilege field	If you select **V3** for the version, the privilege associated with the trap. This can be one of the following: • **Auth**—Authentication but no encryption • **Noauth**—No authentication or encryption • **Priv**—Authentication and encryption

Step 5 Click **OK** to close the **Add SNMP Trap** dialog box.

Step 6 In the **SNMP Users** area, click **Add**.

Step 7 In the **Add SNMP User** dialog box, complete the following fields:

Name	Description
Name field	The username assigned to the SNMP user. Enter up to 32 letters or numbers. The name must begin with a letter and you can also specify _ (underscore), . (period), @ (at sign), and - (hyphen).
Auth Type field	The authorization type: **SHA**.
Use AES-128 check box	If checked, this user uses AES-128 encryption.
Password field	The password for this user.
Confirm Password field	The password again for confirmation purposes.
Privacy Password field	The privacy password for this user.
Confirm Privacy Password field	The privacy password again for confirmation purposes.

Step 8 Click **OK** to close the **Add SNMP User** dialog box.

Step 9 Click **Save**.

HTTPS: Change the 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.

Before you begin

Do not change the HTTPS port from 443 if you enable HTTPS access on ASA data interfaces; only the default port is supported.

Procedure

Step 1 Choose **Platform Settings** > **HTTPS**.

Step 2 Enter the port to use for HTTPS connections in the **Port** field. Specify an integer between 1 and 65535. This service is enabled on port 443 by default.

Step 3 Click **Save**.

The Firepower chassis is configured with the HTTPS port specified.

After changing the HTTPS port, all current HTTPS sessions are closed. Users will need to log back in to the Secure Firewall 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 Firepower chassis that you entered during initial configuration and <*chassis_mgmt_port*> is the HTTPS port you have just configured.

DHCP: Configure the DHCP Server for Management Clients

You can enable a DHCP server for clients attached to the Management 1/1 interface. By default, the server is enabled with the following address range: 192.168.45.10-192.168.45.12. If you want to change the management IP address, you must disable DHCP. You can then reenable DHCP for the new network.

Procedure

Step 1 Choose **Platform Settings** > **DHCP**.

Step 2 Check the **Enable DHCP service** check box.

Step 3 Enter the **Start IP** and **End IP** addresses.

Step 4 Click **Save**.

Syslog: Configure Syslog Messaging

Logs are useful both in routine troubleshooting and in incident handling. You can send syslog messages to the Firepower 2100 console, SSH session, or a local file.

These syslog messages apply only to the FXOS chassis. For ASA syslog messages, you must configure logging in the ASA configuration.

Note Remote destinations are not supported.

Procedure

Step 1 Choose **Platform Settings** > **Syslog**.

Step 2 Configure Local Destinations:

a) Click the **Local Destinations** tab.

b) Complete the following fields:

Name	Description
Console	
Admin State	Check the **Enable** check box to display syslog messages on the console.
Level	Click the lowest message level that you want displayed on the console. The Firepower chassis displays that level and above. • **Emergencies** • **Alerts** • **Critical**
Platform	
Admin State	Platform syslogs are always enabled.

Name	Description
Level	Choose the lowest message level that you want displayed. The Firepower chassis displays that level and above. The default is **Informational**. • **Emergencies** • **Alerts** • **Critical** • **Errors** • **Warnings** • **Notifications** • **Information** • **Debugging**
File	
Admin State	Check the **Enable** check box to save syslog messages to a file.
Level	Choose the lowest message level that you want saved. The system saves that level and above. • **Emergencies** • **Alerts** • **Critical** • **Errors** • **Warnings** • **Notifications** • **Information** • **Debugging**
Name	Set the name of the file, up to 16 characters.
Size	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.

c) Click **Save**.

Step 3 Configure Local Sources:

a) Click the **Local Sources** tab.

b) Complete the following fields:

Name	Description
Faults Admin State	Whether system fault logging is enabled or not. If the **Enable** check box is checked, the Firepower chassis logs all system faults.
Audits Admin State	Whether audit logging is enabled or not. If the **Enable** check box is checked, the Firepower chassis logs all audit log events.
Events Admin State	Whether system event logging is enabled or not. If the **Enable** check box is checked, the Firepower chassis logs all system events.

c) Click **Save**.

DNS: Configure DNS Servers

You need to specify a DNS server if the system requires resolution of hostnames to IP addresses. You can configure up to four DNS servers. When you configure multiple DNS servers, the system searches for the servers only in any random order.

Before you begin

- DNS is configured by default with the following OpenDNS servers: 208.67.222.222, 208.67.220.220.

Procedure

Step 1 Choose **Platform Settings** > **DNS**.

Step 2 Check the **Enable DNS Server** check box.

Step 3 For each DNS server that you want to add, up to a maximum of four, enter the IP address of the DNS server in the **DNS Server** field and click **Add**.

Step 4 Click **Save**.

Step 5 Click the **Domain Name Configuration** tab, enter the **Domain name** that you want the chassis to append as a suffix to unqualified names, and click **Add**.

For example, if you set the domain name to “example.com” and specify a syslog server by the unqualified name of “jupiter,” then the chassis qualifies the name to “jupiter.example.com.”

FIPS and Common Criteria: Enable FIPS and Common Criteria Mode

Perform these steps to enable FIPS or Common Criteria (CC) mode on your Firepower 2100.

You must also separately enable FIPS mode on the ASA using the **fips enable** command. On the ASA, there is not a separate setting for Common Criteria mode; any additional restrictions for CC or UCAPL compliance must be configured in accordance with Cisco security policy documents.

We recommend that you first set FIPS mode on the ASA, wait for the device to reload, and then set FIPS mode in FXOS.

Procedure

Step 1 Choose **Platform Settings** > **FIPS and Common Criteria**.

Step 2 Enable **FIPS** by checking the **Enable** checkbox.

Step 3 Enable **Common Criteria** by checking the **Enable** checkbox.

When you enable Common Criteria, the **FIPS Enable** check box is enabled by default.

Step 4 Click **Save**.

Step 5 Follow the prompt to reboot the system.

Access List: Configure Management Access

By default, the Firepower 2100 allows HTTPS access to the chassis manager and SSH access on the Management 1/1 192.168.45.0/24 network. If you want to allow access from other networks, or to allow SNMP, you must add or change the Access Lists.

For each block of IP addresses (v4 or v6), You can configure up to 25 different subnets for each service.

Procedure

Step 1 Choose **Platform Settings** > **Access List**.

Step 2 In the **IPv4 Access List** area:

a) Click **Add**.

b) Enter values for the following:

- **IP Address**—Sets the IP address. Enter **0.0.0.0** to allow all networks.
- **Prefix Length**—Sets the subnet mask. Enter **0** to allow all networks.
- **Protocol**—Choose **HTTPS**, **SNMP**, or **SSH**.

c) Click **OK**.

d) Repeat these steps to add additional networks per service.

Step 3 In the **IPv6 Access List** area:

a) Click **Add**.

b) Enter values for the following:

- **IP Address**—Sets the IP address. Enter :: to allow all networks.
- **Prefix Length**—Sets the prefix length. Enter **0** to allow all networks.
- **Protocol**—Choose **HTTPS**, **SNMP**, or **SSH**.

c) Click **OK**.

d) Repeat these steps to add additional networks per service.

Step 4 Click **Save**.

System Updates

This task applies to a standalone ASA. If you want to upgrade a failover pair, see the Cisco ASA Upgrade Guide. The upgrade process typically takes between 20 and 30 minutes.

The ASA, ASDM, and FXOS images are bundled together into a single package. Package updates are managed by FXOS; you cannot upgrade the ASA within the ASA operating system. You cannot upgrade ASA and FXOS separately from each other; they are always bundled together.

The exception is for ASDM, which you can upgrade from within the ASA operating system, so you do not need to only use the bundled ASDM image. ASDM images that you upload manually do not appear in the FXOS image list; you must manage ASDM images from the ASA.

Note When you upgrade the bundle, the ASDM image in the bundle replaces the previous ASDM bundle image because they have the same name (**asdm.bin**). But if you manually chose a different ASDM image that you uploaded (for example, **asdm-782.bin**), then you continue to use that image even after a bundle upgrade. To make sure that you are running a compatible version of ASDM, you should either upgrade ASDM before you upgrade the bundle, or you should reconfigure the ASA to use the bundled ASDM image (**asdm.bin**) just before upgrading the ASA bundle.

Before you begin

Make sure the image you want to upload is available on your local computer.

Procedure

Step 1 Choose **System** > **Updates**.

The **Available Updates** page shows a list of the packages that are available on the chassis.

Step 2 Click **Upload Image**.

Step 3 Click **Browse** to navigate to and select the image that you want to upload.

Step 4 Click **Upload**.

The selected image is uploaded to the chassis. The integrity of the image is automatically verified when a new image is added to the chassis. If you want to manually verify it, click **Verify** (check mark icon).

Step 5 Select the ASA package you want to upgrade to, and click **Upgrade**.

Step 6 Click **Yes** to confirm that you want to proceed with installation, or click **No** to cancel the installation.

You will be logged out of the chassis manager during the upgrade.

User Management

User accounts are used to access the Firepower 2100 chassis. These accounts work for chassis manager and for SSH access. The ASA has separate user accounts and authentication.

About User Accounts

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. The default password is **Admin123**.

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

Locally-Authenticated User Accounts

You can configure up to 48 local user accounts. Each user account must have a unique username and password.

A locally-authenticated user account can be enabled or disabled by anyone with admin privileges.

Guidelines for User Accounts

Usernames

The username is used as the login ID for the Secure Firewall chassis manager and the FXOS CLI. When you assign login IDs, 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.

Passwords

A password is required for each locally-authenticated user account. A user with admin 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, FXOS rejects any password that does not meet the following requirements:

- Must contain a minimum of 8 characters and a maximum of 127 characters.

  Note You can optionally configure a minimum password length of 15 characters on the system, to comply with Common Criteria requirements.

- 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 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).
- Must not be blank.

Add a User

Add local users for chassis manager and FXOS CLI access.

Procedure

Step 1 Choose **System** > **User Management**.

Step 2 Click the **Local Users** tab.

Step 3 Click **Add User** to open the **Add User** dialog box.

Step 4 Complete the following fields with the required information about the user:

- **User Name**—Sets the username. This name must be unique and meet the guidelines and restrictions for user account names (see Guidelines for User Accounts, on page 21). After you save the user, the login ID cannot be changed. You must delete the user account and create a new one.
- **First Name**—Sets the first name of the user. This field can contain up to 32 characters.
- **Last Name**—The last name of the user. This field can contain up to 32 characters.
- **Email**—Sets the email address for the user.
- **Phone Number**—Sets the telephone number for the user.
- **Password** and **Confirm Password**—Sets the password associated with this account. If you enable the password strength check,the password must be strong, and FXOS rejects any password that does not

meet the strength check requirements (see Configure User Settings, on page 23 and Guidelines for User Accounts, on page 21).

- **Account Status**—Sets the status to **Active** or **Inactive**.
- **User Role**—Sets the role that represents the privileges you want to assign to the user account. All users are assigned the **Read-Only** role by default, and this role cannot be deselected. To assign the Admin role, click **Admin** in the window so that it is highlighted. The Admin role allows read-and-write access to the configuration. 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.
- **Account Expires**—Sets that this account expires. The account cannot be used after the date specified in the **Expiry Date** field. 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. By default, user accounts do not expire.
- **Expiry Date**—The date on which the account expires. The date should be in the format yyyy-mm-dd. Click the calendar icon at the end of this field to view a calendar that you can use to select the expiration date.

Step 5 Click **Add**.

Step 6 To deactivate a user:

a) For the user you want to deactivate, click the **Edit** (✎).

The admin user account is always set to active, and you cannot inactivate it.

b) In the **Account Status** area, click the **Inactive** radio button.

c) Click **Save**.

Configure User Settings

You can configure global settings for all users.

Procedure

Step 1 Choose **System** > **User Management**.

Step 2 Click the **Settings** tab.

Step 3 Complete the following fields.

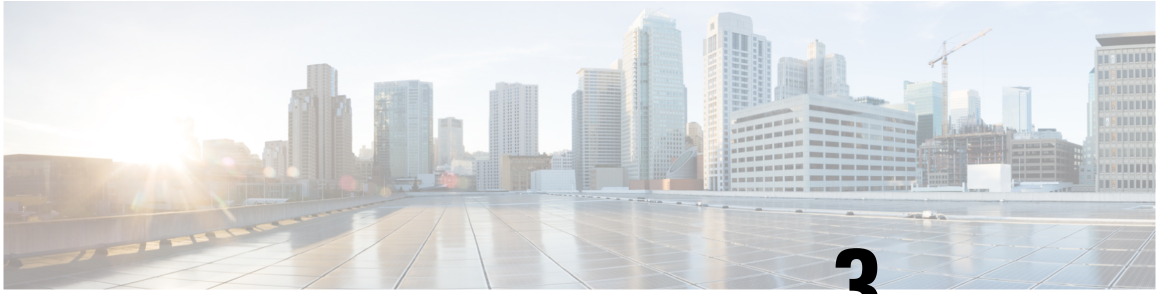
- **Default Authentication**—The default method by which a user is authenticated during remote login. This can be one of the following:
  - **Local**—The user account must be defined locally on the chassis.
  - **None**—If the user account is local to the chassis, no password is required when the user logs in remotely.

- **Password Strength Check**—If checked, all local user passwords must conform to the guidelines for a strong password (see Guidelines for User Accounts, on page 21). The strong password check is enabled by default.
- **History Count**—The number of unique passwords a user must create before the user can reuse a previously used password. The history count is in reverse chronological order with the most recent password first to ensure that only the oldest password can be reused when the history count threshold is reached. This value can be anywhere from 0 to 15. You can set the **History Count** field to 0 to disable the history count and allow users to reuse previously used passwords.
- **Change Interval**—The number of hours over which the number of password changes specified in the **Change Count** field are enforced. 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. Check the check box to enable this feature.
- **Change Count**—The maximum number of times a locally authenticated user can change his or her password during the Change Interval. This value can be anywhere from 0 to 10.
- **No Change Interval**—The minimum number of hours that a locally authenticated user must wait before changing a newly created password. This value can be anywhere from 1 to 745 hours. Check the check box to enable this feature.
- **Passphrase Expiration Days**—Set the expiration between 1 and 9999 days. By default, expiration is disabled.
- **Passphrase Expiration Warning Period**—Set the number of days before expiration to warn the user about their password expiration at each login, between 0 and 9999. The default is 14 days.
- **Expiration Grace Period**—Set the number of days a user has to change their password after expiration, between 0 and 9999. The default is 3 days.
- **Password Reuse Interval**—Set the number of days before you can reuse a password, between 1 and 365. The default is 15 days. If you enable both the **History Count** and the **Password Reuse Interval**, then both requirements must be met. For example, if you set the history count to 3, and the reuse interval to 10 days, then you can change your password only after 10 days have passed, and you have changed your password 3 times.

Step 4 Click **Save**.

History for Chassis Manager Settings

Feature	Version	Details
User password improvements	9.13(1)	We added password security improvements, including the following: • User passwords can be up to 127 characters. The old limit was 80 characters. • Strong password check is enabled by default. • Prompt to set admin password. • Password expiration. • Limit password reuse. New/Modified screens: • **System** > **User Management** > **Local Users** • **System** > **User Management** > **Settings**
Support for NTP Authentication on the Firepower 2100	9.10(1)	You can now configure SHA1 NTP server authentication in FXOS. New/Modified chassis manager screens: **Platform Settings** > **NTP** > **NTP Server Authentication: Enable** check box, **Authentication Key** field, **Authentication Value** field



CHAPTER 3

FXOS CLI Settings

The Firepower 2100 runs FXOS to control basic operations of the device. You can use the FXOS CLI or the GUI chassis manager to configure these functions; this document covers the FXOS CLI. Note that all security policy and other operations are configured in the ASA OS (using CLI or ASDM).

CLI and Configuration Management

The Secure Firewall eXtensible Operating System (FXOS) operates differently from the ASA CLI. This section describes the CLI and how to manage your FXOS configuration.

About the CLI

FXOS uses a managed object model, where managed objects are abstract representations of physical or logical entities that can be managed. For example, chassis, 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.

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. You can use the **enter** *object* command to create new objects and edit existing objects, so you can use it instead of the **create** *object* command, which will give an error if an object already exists.

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

Connect to the ASA or FXOS Console

The Firepower 2100 console port connects you to the FXOS CLI. From the FXOS CLI, you can then connect to the ASA console, and back again. If you SSH to FXOS, you can also connect to the ASA CLI; a connection from SSH is not a console connection, so you can have multiple ASA connections from an FXOS SSH connection. Similarly, if you SSH to the ASA, you can connect to the FXOS CLI.

You can only have one console connection at a time. When you connect to the ASA console from the FXOS console, this connection is a persistent console connection, not like a Telnet or SSH connection.

Procedure

Step 1 Connect your management computer to the console port. The Firepower 2100 ships with a DB-9 to RJ-45 serial cable, so you will need a third party serial-to-USB cable to make the connection. Be sure to install any necessary USB serial drivers for your operating system. Use the following serial settings:

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

You connect to the FXOS CLI. Enter the user credentials; by default, you can log in with the **admin** user and the default password, **Admin123**.

Step 2 Connect to the ASA:

connect asa

Example:

```
firepower-2110# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

Step 3 To return to the FXOS console, enter **Ctrl+a**, **d**.

Connect to FXOS with SSH

You can connect to FXOS on Management 1/1 with the default IP address, 192.168.45.45. If you configure remote management (the ASA **fxos permit** command), you can also connect to the data interface IP address on the non-standard port, by default, 3022.

To connect using SSH to the ASA, you must first configure SSH access according to the ASA general operations configuration guide.

You can connect to the ASA CLI from FXOS, and vice versa.

FXOS allows up to 8 SSH connections.

Before you begin

To change the management IP address, see Change the FXOS Management IP Addresses or Gateway, on page 95.

Procedure

Step 1 On the management computer connected to Management 1/1, SSH to the management IP address (by default https://192.168.45.45, with the username: **admin** and password: **Admin123**).

You can log in with any username (see Add a User, on page 22). If you configure remote management, SSH to the ASA data interface IP address on port 3022 (the default port).

Step 2 Connect to the ASA CLI.

connect asa

To return to the FXOS CLI, enter **Ctrl+a**, **d**.

Example:

```
firepower-2110# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

Step 3 If you SSH to the ASA (after you configure SSH access in the ASA), connect to the FXOS CLI.

connect fxos

You are prompted to authenticate for FXOS; use the default username: **admin** and password: **Admin123**. To return to the ASA CLI, enter **exit** or type **Ctrl-Shift-6**, **x**.

Example:

```
ciscoasa# connect fxos
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.

FXOS 2.2(2.32) kp2110

firepower-2110 login: admin
Password: Admin123
Last login: Sat Jan 23 16:20:16 UTC 2017 on pts/1
Successful login attempts for user 'admin' : 4
Cisco Firepower Extensible Operating System (FX-OS) Software

[…]

firepower-2110#
firepower-2110# exit
Remote card closed command session. Press any key to continue.
Connection with fxos terminated.
Type help or '?' for a list of available commands.
```

```
ciscoasa#
```

Commit, Discard, and View Pending Commands

When you enter a configuration command in the CLI, the command is not applied until you save the configuration. Until committed, a configuration command is pending and can be discarded. While any commands are pending, an asterisk (*) appears before the command prompt. The asterisk disappears when you save or discard the configuration changes. You can accumulate pending changes in multiple command modes and apply them together. You can view the pending commands in any command mode.

Procedure

Step 1 View pending configuration changes.

show configuration pending

Example:

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enter ntp-server 10.1.1.1
firepower-2110 /system/services/ntp-server* # show configuration pending
+enter ntp-server 10.1.1.1
+    set ntp-sha1-key-id 0
+!   set ntp-sha1-key-string
+exit
firepower-2110 /system/services/ntp-server* #
```

Step 2 Save the configuration.

commit-buffer

Note Committing multiple commands all together is not a singular operation. If any command fails, the successful commands are applied despite the failure. Failed commands are reported in an error message.

Example:

```
firepower-2110 /system/services/ntp-server* # commit-buffer
firepower-2110 /system/services/ntp-server #
```

Step 3 Discard configuration changes.

discard-buffer

Example:

```
firepower-2110 /system/services/ntp-server* # discard-buffer
```

```
firepower-2110 /system/services/ntp-server #
```

Example

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

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enter ntp-server 10.1.1.1
firepower-2110 /system/services/ntp-server* # show configuration pending
+enter ntp-server 10.1.1.1
+    set ntp-sha1-key-id 0
+!   set ntp-sha1-key-string
+exit
firepower-2110 /system/services/ntp-server* #
firepower-2110 /system/services/ntp-server* # commit-buffer
firepower-2110 /system/services/ntp-server #
```

Save and Filter Show Command Output

You can save the output of **show** commands by redirecting the output to a text file. You can filter the output of **show** commands by piping the output to filtering commands.

Saving and filtering output are available with all **show** commands but are most useful when dealing with commands that produce a lot of text. For example, you can show all or parts of the configuration by using the **show configuration** command. Copying the configuration output provides a way to backup and restore a configuration.

Note Show commands do not show the secrets (password fields), so if you want to paste a configuration into a new device, you will have to modify the show output to include the actual passwords.

Filter Show Command Output

To filter the output of a **show** command, use the following subcommands. Note that in the following syntax description, the initial vertical bar | after the **show** command is the pipe character and is part of the command, not part of the syntax description. The filtering options are entered after the command's initial | character.

show *command* **|** {**begin** *expression* | **count** | **cut** *expression* | **egrep** *expression* | **end** *expression* | **exclude** *expression* | **grep** *expression* | **head** | **include** *expression* | **last** | **less** | **no-more** | **sort** *expression* | **tr** *expression* | **uniq** *expression* | **wc** }

Filtering Options

These are the filtering subcommands:

- **begin**—Finds the first line that includes the specified pattern, and display that line and all subsequent lines.

- **count**—Counts the number of lines.
- **cut**—Removes (“cut”) portions of each line.
- **egrep**—Displays only those lines that match the extended-type pattern.
- **end**—Ends with the line that matches the pattern.
- **exclude**—Excludes all lines that match the pattern and show all other lines.
- **grep**—Displays only those lines that match the pattern.
- **head**—Displays the first lines.
- **include**—Displays only those lines that match the pattern.
- **last**—Displays the last lines.
- **less**—Filters for paging.
- **no-more**—Turns off pagination for command output.
- **sort**—Sorts the lines (stream sorter).
- **tr**—Translates, squeezes, and/or deletes characters.
- **uniq**—Discards all but one of successive identical lines.
- **wc**—Displays a count of lines, words, and characters.

expression

An expression, or pattern, is typically a simple text string. Do not enclose the expression in single or double-quotes—these will be seen as part of the expression. Also, trailing spaces will be included in the expression.

Note Several of these subcommands have additional options that let you further control the filtering. For example, with **show configuration | head** and **show configuration | last**, you can use the **lines** keyword to change the number of lines displayed; the default is 10. As another example, with **show configuration | sort**, you can add the option **-u** to remove duplicate lines from the output. (Complete descriptions of these options is beyond the scope of this document; refer to the FXOS help output for the various commands, and to the appropriate Linux help, for more information.)

Examples

The following example shows how to determine the number of lines currently in the system event log:

```
FP9300-A# show sel 1/1 | count
3008
FP9300-A#
```

The following example shows how to display lines from the system event log that include the string “error”:

```
FP9300-A# show sel 1/1 | include error
968 | 05/15/2016 16:46:25 | CIMC | System Event DDR4_P2_H2_EC
C #0x99 | Upper critical - going high | Asserted | Reading 20
```

```
000 >= Threshold 20000 error
FP9300-A#
```

Related Topics

Save Show Command Output, on page 33

Save Show Command Output

You can save the output of **show** commands by redirecting the output to a text file.

show *command* [> { **ftp:** | **scp:** | **sftp:** | **tftp:** | **volatile:** | **workspace:** }] | [>> { **volatile:** | **workspace:** }]

Syntax Description

> { **ftp:** | **scp:** | **sftp:** | **tftp:** | **volatile:** | **workspace:** }	Redirects the **show** command output to a specified text file using the selected transport protocol. After you enter the command, you are queried for remote server name or IP address, user name, file path, and so on. If you press **Enter** at this point, the output is saved locally.
>> { **volatile:** | **workspace:** }	Appends the **show** command output to the appropriate text file, which must already exist.

Example

The following example attempts to save the current configuration to the system workspace; a configuration file already exists, which you can choose to overwrite or not.

```
FP9300-A# show configuration > workspace
File already exists, overwrite (y/n)?[n]n
Reissue command with >> if you want to append to existing file

FP9300-A#
```

Related Topics

Filter Show Command Output, on page 31

Interfaces

You can manage physical interfaces in FXOS. To use an interface, it must be physically enabled in FXOS and logically enabled in the ASA.

The Firepower 2100 has support for jumbo frames enabled by default. The maximum MTU is 9184.

For information about the Management interfaces, see ASA and FXOS Management, on page 1.

Configure Interfaces

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 ASA. Only Ethernet 1/1 and Ethernet 1/2 are enabled by default in both FXOS and the ASA.

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 eth-uplink and then fabric a mode.

scope eth-uplink

scope fabric a

Example:

```
firepower-2110# scope eth-uplink
firepower-2110 /eth-uplink # scope fabric a
firepower-2110 /eth-uplink/fabric #
```

Step 2 Enable the interface.

enter interface *interface_id*

enable

Example:

```
firepower-2110 /eth-uplink/fabric # enter interface Ethernet1/8
firepower-2110 /eth-uplink/fabric/interface # enable
firepower-2110 /eth-uplink/fabric/interface* #
```

Step 3 Enable or disable autonegotiation.

set auto-negotiation {**on** | **off**}

For RJ-45 interfaces, the default setting is **on**.

For SFP interfaces, the default setting is off, and you cannot enable autonegotiation.

Example:

```
firepower-2110 /eth-uplink/fabric/interface* # set auto-negotiation off
```

Step 4 Set the interface speed if you disable autonegotiation.

set admin-speed {**10mbps** | **100mbps** | **1gbps** | **10gbps**}

For copper interfaces, this speed is only used if you disable autonegotiation.

Example:

```
firepower-2110 /eth-uplink/fabric/interface* # set admin-speed 1gbps
```

Step 5 Set the interface duplex mode.

set admin-duplex {**fullduplex** | **halfduplex**}

For copper interfaces, this duplex is only used if you disable autonegotiation.

Example:

```
firepower-2110 /eth-uplink/fabric/interface* # set admin-duplex halfduplex
```

Step 6 Save the configuration.

commit-buffer

Example:

```
firepower-2110 /eth-uplink/fabric/interface* # commit-buffer
firepower-2110 /eth-uplink/fabric/interface #
```

Example

```
firepower-2110# scope eth-uplink
firepower-2110 /eth-uplink* # scope fabric a
firepower-2110 /eth-uplink/fabric* # enter interface ethernet1/6
firepower-2110 /eth-uplink/fabric/interface* # enable
firepower-2110 /eth-uplink/fabric/interface* # set flow-control-policy FlowControlPolicy23
firepower-2110 /eth-uplink/fabric/interface* # commit-buffer
firepower-2110 /eth-uplink/fabric/interface #
```

Add an EtherChannel

An EtherChannel (also known as a port-channel) can include up to 8 member interfaces of 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.

Note EtherChannel member ports are visible on the ASA, but you can only configure EtherChannels and port membership in FXOS.

Note The ASA does not support LACP rate fast; LACP always uses the normal rate.

Before you begin

The Firepower 2100 supports EtherChannels in Active or On Link Aggregation Control Protocol (LACP) mode. By default, the LACP mode is set to Active; you can change the mode to On at the CLI. We suggest setting the connecting switch ports to Active mode for the best compatibility.

Procedure

Step 1 Enter eth-uplink and then fabric a mode.

scope eth-uplink

scope fabric a

Example:

```
firepower-2110# scope eth-uplink
firepower-2110 /eth-uplink # scope fabric a
firepower-2110 /eth-uplink/fabric #
```

Step 2 Enable the port-channel.

enter port-channel *id*

enable

Set the *id* to an integer between 1 and 47.

Example:

```
firepower-2110 /eth-uplink/fabric # enter port-channel 1
firepower-2110 /eth-uplink/fabric/port-channel* # enable
```

Step 3 Assign member interfaces.

enter member-port *interface_id*

Example:

```
firepower-2110 /eth-uplink/fabric/port-channel* # enter member-port ethernet1/1
firepower-2110 /eth-uplink/fabric/port-channel/member-port* # exit
firepower-2110 /eth-uplink/fabric/port-channel* # enter member-port ethernet1/2
firepower-2110 /eth-uplink/fabric/port-channel/member-port* # exit
firepower-2110 /eth-uplink/fabric/port-channel* # enter member-port ethernet1/3
firepower-2110 /eth-uplink/fabric/port-channel/member-port* # exit
firepower-2110 /eth-uplink/fabric/port-channel* # enter member-port ethernet1/4
firepower-2110 /eth-uplink/fabric/port-channel/member-port* # exit
firepower-2110 /eth-uplink/fabric/port-channel* #
```

Step 4 (Optional) Set the LACP mode.

set port-channel-mode {**active** | **on**}

The default is Active mode.

Example:

```
firepower-2110 /eth-uplink/fabric/port-channel* # set port-channel-mode on
```

Step 5 (Optional) Set the interface speed for all members of the port-channel to override the properties set on the individual interfaces.

set speed {**10mbps** | **100mbps** | **1gbps** | **10gbps**}

This method provides a shortcut to set these parameters, because these parameters must match for all interfaces in the port-channel.

Example:

```
firepower-2110 /eth-uplink/fabric/port-channel* # set speed 1gbps
```

Step 6 (Optional) For copper ports, set the interface duplex mode for all members of the port-channel to override the properties set on the individual interfaces.

set duplex {**fullduplex** | **halfduplex**}

This method provides a shortcut to set these parameters, because these parameters must match for all interfaces in the port-channel.

Example:

```
firepower-2110 /eth-uplink/fabric/port-channel* # set duplex fullduplex
```

Step 7 (Optional) Configure a description up to 256 characters.

set descr "*text***"**

Example:

```
firepower-2110 /eth-uplink/fabric/port-channel* # set descr "Inside Interface"
```

Step 8 Save the configuration.

commit-buffer

Example:

```
firepower-2110 /eth-uplink/fabric/port-channel* # commit-buffer
firepower-2110 /eth-uplink/fabric/port-channel #
```

Example

The following example adds 3 interfaces to an EtherChannel, sets the LACP mode to on, and sets the speed and a flow control policy:

```
firepower-2110# scope eth-uplink
firepower-2110 /eth-uplink # scope fabric a
firepower-2110 /eth-uplink/fabric #
firepower-2110 /eth-uplink/fabric # enter port-channel 1
firepower-2110 /eth-uplink/fabric/port-channel* # enable
firepower-2110 /eth-uplink/fabric/port-channel* # enter member-port ethernet2/1
firepower-2110 /eth-uplink/fabric/port-channel/member-port* # exit
firepower-2110 /eth-uplink/fabric/port-channel* # enter member-port ethernet2/2
firepower-2110 /eth-uplink/fabric/port-channel/member-port* # exit
firepower-2110 /eth-uplink/fabric/port-channel* # enter member-port ethernet2/3
firepower-2110 /eth-uplink/fabric/port-channel/member-port* # exit
firepower-2110 /eth-uplink/fabric/port-channel* # set port-channel-mode on
firepower-2110 /eth-uplink/fabric/port-channel* # set speed 10gbps
```

```
firepower-2110 /eth-uplink/fabric/port-channel* # commit-buffer
firepower-2110 /eth-uplink/fabric/port-channel #
```

Monitoring Interfaces

View the status of installed interfaces on the chassis.

Procedure

Step 1 Enter eth-uplink and then fabric a mode.

scope eth-uplink

scope fabric a

Example:

```
firepower-2110# scope eth-uplink
firepower-2110 /eth-uplink # scope fabric a
firepower-2110 /eth-uplink/fabric #
```

Step 2 Display the installed interfaces on the chassis.

show interface

Member interfaces in EtherChannels do not appear in this list.

Example:

```
firepower-2110 /eth-uplink/fabric # show interface

Interface:
    Port Name       Port Type          Admin State Oper State       State Reason
    --------------- ------------------ ----------- ---------------- ------------
    Ethernet1/1     Mgmt               Enabled     Up
    Ethernet1/2     Data               Enabled     Link Down        Link failure
 or not-connected
    Ethernet1/3     Data               Enabled     Up
    Ethernet1/4     Data               Enabled     Sfp Not Present  Unknown
    Ethernet1/6     Data               Enabled     Sfp Not Present  Unknown
    Ethernet1/7     Data               Enabled     Sfp Not Present  Unknown
    Ethernet1/8     Data               Disabled    Sfp Not Present  Unknown
    Ethernet2/1     Data               Enabled     Up
    Ethernet2/2     Data               Enabled     Up
    Ethernet2/4     Data               Enabled     Up
    Ethernet2/5     Data               Enabled     Up
    Ethernet2/6     Data               Enabled     Up
    Ethernet3/2     Data               Enabled     Up
    Ethernet3/4     Data               Enabled     Up
```

Platform Settings

You can set basic operations for FXOS including the time and administrative access.

Set the Date and Time

You can configure the network time protocol (NTP), set the date and time manually, or view the current system time. Clock settings are automatically synced between the Firepower 2100 chassis and the ASA OS.

Set 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. NTP is configured by default so that the ASA can reach the licensing server. You can configure up to four NTP servers. The Firepower 2100 uses NTP version 3.

Procedure

Step 1 Enter system and then services mode.

scope system

scope services

Example:

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services #
```

Step 2 Add the NTP server.

enter ntp-server {*hostname* | *ip_addr* | *ip6_addr*}

Example:

```
firepower-2110 /system/services # enter ntp-server 192.168.6.5
firepower-2110 /system/services/ntp-server* #
```

Step 3 (Optional) (ASA 9.10(1) and later) 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.

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-2110 /system/services/ntp-server* # set ntp-sha1-key-string 11
firepower-2110 /system/services/ntp-server* # set ntp-sha1-key-string
NTP SHA-1 key string: 7092334a7809ab9873124c08123df9097097fe72
firepower-2110 /system/services/ntp-server* # exit
firepower-2110 /system/services* # enable authentication
```

Step 4 Set the time zone.

set timezone

You are prompted to enter a number corresponding to your continent, country, and time zone region. Enter the appropriate information at each prompt.

Example:

```
firepower-2110 /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 2018.
Universal Time is now:  Wed Jun 24 14:39:25 UTC 2018.
Is the above information OK?
1) Yes
2) No
#? 1
firepower-2110 /system/services* #
```

Step 5 Save the configuration.

commit-buffer

Example:

```
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

Step 6 View the clock details.

- View the synchronization status for all configured NTP servers.

show ntp-server [*hostname* | *ip_addr* | *ip6_addr*]

```
firepower-2110 /system/services # show ntp-server

NTP server hostname:
    Name                 Time Sync Status
    -------------------- ----------------
    0.sourcefire.pool.nt Unreachable Or Invalid Ntp Server
    1.sourcefire.pool.nt Unreachable Or Invalid Ntp Server
    2.sourcefire.pool.nt Unreachable Or Invalid Ntp Server
```

- View the synchronization status for a specific NTP server.

  enter ntp-server {*hostname* | *ip_addr* | *ip6_addr*}

  show detail

  exit

```
firepower-2110 /system/services # enter ntp-server 0.sourcefire.pool.ntp.org
firepower-2110 /system/services/ntp-server # show detail

NTP server hostname:
    Name: 0.sourcefire.pool.ntp.org
    Time Sync Status: Unreachable Or Invalid Ntp Server
    Error Msg: Failed to translate domain name to IP, please verify the domain name or
 check if DNS server is configured.

firepower-2110 /system/services/ntp-server # exit
firepower-2110 /system/services #
```

- View the configured time zone.

  show timezone

```
firepower-2110 /system/services # show timezone
Timezone: America/Los_Angeles
```

- View the configured date and time.

  show clock

```
firepower-2110 /system/services # show clock
Wed Apr 18 08:49:35 PDT 2018
```

Example

The following example configures an NTP server with the IP address 192.168.200.101.

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enter ntp-server 192.168.200.101
firepower-2110 /system/services/ntp-server* # commit-buffer
```

```
firepower-2110 /system/services/ntp-server #
```

Set the Date and Time Manually

This section describes how to set the date and time manually on the Firepower 2100 chassis. System clock modifications take effect immediately. 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 and then services mode.

scope system

scope services

Example:

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services #
```

Step 2 Set the time and date.

set clock *month day year hour min sec*

- *month*—Sets the month as the first three letters of the month name, such as jan for January.
- *day*—Sets the day, between 1 and 31.
- *year*—Sets the year as 4 digits, such as 2018.
- *hour*—Sets the hour in 24-hour format, where 7 pm is entered as 19.
- *min*—Sets the minutes between 0 and 59.
- *sec*—Sets the seconds between 0 and 59.

System clock modifications take effect immediately. You do not need to commit the buffer.

Example:

```
firepower-2110 /system/services # set clock apr 18 2018 9 39 30
Wed Apr 18 09:39:30 PDT 2018
firepower-2110 /system/services #
```

Step 3 Set the time zone.

set timezone

You are prompted to enter a number corresponding to your continent, country, and time zone region. Enter the appropriate information at each prompt.

Example:

```
firepower-2110 /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 2018.
Universal Time is now:  Wed Jun 24 14:39:25 UTC 2018.
Is the above information OK?
1) Yes
2) No
#? 1
firepower-2110 /system/services* #
```

Step 4 Save the configuration.

commit-buffer

Example:

```
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

Step 5 View the clock details.

- View the configured time zone.

  show timezone

  ```
  firepower-2110 /system/services # show timezone
  Timezone: America/Los_Angeles
  ```

- View the configured date and time.

  show clock

  ```
  firepower-2110 /system/services # show clock
  Wed Apr 18 08:49:35 PDT 2018
  ```

Example

The following example configures the system clock.

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # set clock jun 24 2015 15 27 00
firepower-2110 /system/services #
```

Set the Chassis Name

Before you begin

You can set the name used for your Firepower 2100 from the FXOS CLI.

Procedure

Step 1 Enter system mode:

scope system

Example:

```
firepower-2110# scope system
firepower-2110 /system #
```

Step 2 View the current name.

show

Example:

```
firepower-2110 /system # show
Systems:
    Name       Mode        System IP Address System IPv6 Address
    ---------- ----------- ----------------- -------------------
    firepower-2110
               Stand Alone 10.122.203.17     ::
```

Step 3 Configure a new name.

set name *device_name*

Example:

```
firepower-2110 /system # set name fp2110-2
Warning: System name modification changes FC zone name and redeploys them non-disruptively
firepower-2110 /system* #
```

Step 4 Save the configuration.

commit-buffer

Example:

```
firepower-2110 /system* # commit-buffer
firepower-2110 /system #
fp2110-2 /system #
```

Example

The following example changes the device name:

```
firepower-2110# scope system
firepower-2110 /system # set name New-name
Warning: System name modification changes FC zone name and redeploys them non-disruptively
firepower-2110 /system* # commit-buffer
firepower-2110 /system # show

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

Configure the Domain Name

The Firepower 2100 appends the domain name as a suffix to unqualified names. For example, if you set the domain name to “example.com” and specify a syslog server by the unqualified name of “jupiter,” then the Firepower 2100 qualifies the name to “jupiter.example.com.”

Procedure

Step 1 Enter system and then services mode.

scope system

scope services

Example:

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services #
```

Step 2 Set the domain name.

set domain-name *name*

Example:

```
firepower-2110 /system/services # set domain-name example.com
firepower-2110 /system/services* #
```

Step 3 Save the configuration.

commit-buffer

Example:

```
firepower-2110 /system/services* # commit-buffer
```

```
firepower-2110 /system/services #
```

Example

The following example sets the domain name to example.com:

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # set domain-name example.com
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

Configure DNS Servers

You need to specify a DNS server if the system requires resolution of hostnames to IP addresses. When you configure multiple DNS servers, the system searches for the servers only in any random order. DNS is required to communicate with the NTP server.

Before you begin

DNS is configured by default with the following OpenDNS servers: 208.67.222.222, 208.67.220.220.

Procedure

Step 1 Enter system and then services mode.

scope system

scope services

Example:

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services #
```

Step 2 Add up to 4 DNS servers.

enter dns {*ipv4_addr* | *ipv6_addr*}

Example:

```
firepower-2110 /system/services* # enter dns 10.10.5.6
firepower-2110 /system/services* # enter dns 192.168.7.2
```

Step 3 Save the configuration.

commit-buffer

Example:

```
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

Examples

The following example configures a DNS server with the IPv4 address 192.168.200.105:

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enter dns 192.168.200.105
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

The following example configures a DNS server with the IPv6 address 2001:db8::22:F376:FF3B:AB3F:

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enter dns 2001:db8::22:F376:FF3B:AB3F
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

The following example deletes the DNS server with the IP address 192.168.200.105:

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # delete dns 192.168.200.105
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

Add a Pre-Login Banner

With a pre-login banner, when a user logs into the Secure Firewall chassis manager, the browser 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 terminal displays the banner text before it prompts for the password.

Procedure

Step 1 Enter security mode, and then banner mode.

scope security

scope banner

Example:

```
firepower-2110# scope security
firepower-2110 /security # scope banner
firepower-2110 /security/banner #
```

Step 2 Create a pre-login banner.

enter pre-login-banner

Example:

```
firepower-2110 /security/banner # enter pre-login-banner
firepower-2110 /security/banner/pre-login-banner* #
```

Step 3 Specify the message that FXOS displays to the user before they log into the chassis manager or the FXOS CLI.

set message

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+c** to cancel out of the set message dialog.

Example:

```
firepower-2110 /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 2100
>**Unauthorized use is prohibited**
>ENDOFBUF
firepower-2110 /security/banner/pre-login-banner* #
```

Step 4 Save the configuration.

commit-buffer

Example:

```
firepower-2110 /security/banner/pre-login-banner* # commit-buffer
firepower-2110 /security/banner/pre-login-banner #
```

Example

The following example creates the pre-login banner:

```
firepower-2110# scope security
firepower-2110 /security # scope banner
firepower-2110 /security/banner # create pre-login-banner
firepower-2110 /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 2110
>**Unauthorized use is prohibited**
>Contact admin@example.com for information.
>ENDOFBUF
firepower-2110 /security/banner/pre-login-banner* # commit-buffer
firepower-2110 /security/banner/pre-login-banner #
```

Configure SSH

The following procedure describes how to enable or disable SSH access to FXOS. SSH is enabled by default.

Before you begin

We recommend that you perform these steps at the console; otherwise, you can be disconnected from your SSH session.

Procedure

Step 1 Enter system and then services mode.

scope system

scope services

Example:

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services #
```

Step 2 To configure SSH access to the chassis, do one of the following:

- Allow SSH access to the chassis.

  enable ssh-server

- Disallow SSH access to the chassis.

  disable ssh-server

Example:

```
firepower-2110 /system/services # disable ssh-server
firepower-2110 /system/services* #
```

Step 3 Set the encryption algorithm.

set ssh-server encrypt-algorithm *protocols*

Set one or more of the following protocols, separated by spaces or commas:

- 3des-cbc
- aes128-cbc

- aes128-ctr
- aes128-gcm_openssh_com
- aes192-cbc
- aes192-ctr
- aes256-cbc
- aes256-ctr
- aes256-gcm_openssh_com
- chacha20-poly1305_openssh_com

All protocols are allowed by default.

Example:

```
firepower-2110 /system/services* # set ssh-server encrypt-algorithm aes256-ctr,aes256-cbc
```

Step 4 Set the key exchange algorithm.

set ssh-server kex-algorithm *algorithms*

Set one or more of the following algorithms, separated by spaces or commas:

- curve25519-sha256
- curve25519-sha256_libssh_org
- diffie-hellman-group14-sha1
- diffie-hellman-group14-sha256
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521

All protocols are allowed by default.

Example:

```
firepower-2110 /system/services* # set ssh-server kex-algorithm
diffie-hellman-group14-sha256,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
```

Step 5 Set the integrity algorithm.

set ssh-server mac-algorithm *protocols*

Set one or more of the following protocols, separated by spaces or commas:

- hmac-sha1
- hmac-sha2-256
- hmac-sha2-512

All protocols are allowed by default.

Example:

```
firepower-2110 /system/services* # set ssh-server mac-algorithm hmac-sha2-512
```

Step 6 Set the server host key.

set ssh-server host-key rsa *modulus*

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.

Example:

```
firepower-2110 /system/services* # set ssh-server host-key rsa 2048
```

Step 7 Set the server rekey limit to set the volume (amount of traffic in KB allowed over the connection) and time (minutes for how long an SSH session can be idle) before FXOS disconnects the session.

set ssh-server rekey-limit volume {*kb* | **none**} **time** {*minutes* | **none**}

- **volume** *kb*—Sets the maximum amount of traffic between 100 and 4194303 KB. The default is no limit (none).
- **time** *minutes*—Sets the maximum time between 10 and 1440 minutes. The default is no limit (none).
- **none**—Disables the limit. This setting is the default.

Example:

```
firepower-2110 /system/services* # set ssh-server rekey-limit volume none time 1440
```

Step 8 Save the configuration.

commit-buffer

Example:

```
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

Example

The following example enables SSH access to the chassis:

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enable ssh-server
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

Configure Certificates, Key Rings, and Trusted Points for HTTPS or IPSec

HTTPS and IPSec use components of the Public Key Infrastructure (PKI) to establish secure communications between two devices, such as a client's browser and the Firepower 2100.

About 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 2100.

Encryption Keys and Key Rings

Each PKI device holds a pair of asymmetric Rivest-Shamir-Adleman (RSA) encryption keys or Elliptic Curve Digital Signature Algorithm (ECDSA) 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 RSA key ring with an initial 2048-bit key pair, and allows you to create additional key rings.

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.

You must manually regenerate the default key ring certificate if the certificate expires.

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.

Note The certificate must be in Base64 encoded X.509 (CER) format.

Install a Trusted Identity Certificate

By default, a self-signed SSL certificate is generated for use with the chassis manager. Because that certificate is self-signed, client browsers do not automatically trust it. The first time a new client browser accesses the chassis manager, the browser shows an SSL warning, which requires the user to accept the certificate before accessing the chassis manager. 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 chassis manager. This identity certificate allows a client browser to trust the connection, and bring up the web interface with no warnings. FXOS supports a maximum of 8 key rings, including the **default** key ring.

Before you begin

Configure DNS Servers, on page 48.

Procedure

Step 1 Enter security mode.

scope security

Example:

```
firepower-2110# scope security
firepower-2110 /security #
```

Step 2 Define a trusted point for the certificate you want to add to the key ring.

create trustpoint *name*

Example:

```
firepower-2110 /security # create trustpoint trust1
firepower-2110 /security/trustpoint* #
```

Step 3 Paste in the certificate chain. Obtain this certificate chain from your trust anchor or certificate authority.

set certchain [*certchain*]

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. The certificate must be in Base64 encoded X.509 (CER) format.

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 the entire text block at the FXOS CLI.

Example:

```
firepower-2110 /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMDCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3nO4MIGeBgNVHSMEgZYwgZOAFLlNjtcEMyZ+f7+3yh42
> 1ido3nO4oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAcT
> C1NhbnRhIENsYXJhMRswGQYDVQQKExJOdW92YSBTeXN0ZW1zIEluYy4xFDASBgNV
> BAsTC0VuZ2luZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0Q0GCAQAwDAYDVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8copP1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
firepower-2110 /security/trustpoint* #
```

Step 4 Exit trustpoint mode.

exit

Example:

```
firepower-2110 /security/trustpoint* # exit
firepower-2110 /security* #
```

Step 5 Create the key ring.

create keyring *keyring_name*

Example:

```
firepower-2110 /security # create keyring keyring1
firepower-2110 /security/keyring* #
```

Step 6 Set the key type to RSA (the default) or ECDSA.

set keypair-type {**rsa** | **edcsa**}

Example:

```
firepower-2110 /security/keyring* # set keypair-type edcsa
```

Step 7 (For RSA) Set the SSL key length in bits.

set modulus {**mod1536** | **mod2048** | **mod2560** | **mod3072** | **mod3584** | **mod4096**}

Example:

```
firepower-2110 /security/keyring* # set modulus mod2048
```

Step 8 (For EDCSA) Set the elliptic curve.

set elliptic-curve {**secp256r1** | **secp384r1** | **secp384r1**}

Example:

```
firepower-2110 /security/keyring* # set elliptic-curve secp384r1
```

Step 9 Create a certificate request.

create certreq

Example:

```
firepower-2110 /security/keyring* # create certreq
firepower-2110 /security/keyring/certreq* #
```

Step 10 Set a certificate password.

set password

Example:

```
firepower-2110 /security/keyring/certreq* # set password
Certificate request password: diagonalapple
Confirm certificate request password: diagonalapple
```

Step 11 Specify the IP address or FQDN of the Firepower 2100.

set {**ip** | **ipv6**} {*ipv_address* | *fqdn*}

You can configure multiple IP addresses.

Example:

```
firepower-2110 /security/keyring/certreq* # set ip 10.10.9.2
```

Step 12 Specify the fully qualified domain name of the chassis used for DNS lookups of your chassis.

set subject-name *fqdn*

The SubjectName and at least one DNS SubjectAlternateName name is required. The SubjectName is automatically added as the DNS SubjectAlternateName.

Example:

```
firepower-2110 /security/keyring/certreq* # set subject-name firepower1.example.com
```

Step 13 (Optional) Configure advanced options.

a) Specify the 2-letter country code of the country in which the company resides.

   set country *country_name*

   Example:

   ```
   firepower-2110 /security/keyring/certreq* # set country us
   ```

b) Specify the Subject Alternative Name to apply this certificate to another hostname.

   set dns *subject_alt_name*

   You can configure multiple DNS names.

   Example:

```
firepower-2110 /security/keyring/certreq* # set dns firepower2.example.com
```

c) Specify the email address associated with the certificate request.

set e-mail *E-mail_name*

You can configure multiple email addresses.

Example:

```
firepower-2110 /security/keyring/certreq* # set e-mail admin@example.com
```

d) Specify the city or town in which the company requesting the certificate is headquartered.

set locality *locality_name*

Example:

```
firepower-2110 /security/keyring/certreq* # set locality boulder
```

e) Specify the organization requesting the certificate.

set org-name *organization_name*

Example:

```
firepower-2110 /security/keyring/certreq* # set org-name Example.com
```

f) Specify the organizational unit.

set org-unit-name *organizational_unit_name*

Example:

```
firepower-2110 /security/keyring/certreq* # set org-unit-name engineering
```

g) Specify the state or province in which the company requesting the certificate is headquartered.

set state *state_province_or_county*

Example:

```
firepower-2110 /security/keyring/certreq* # set state co
```

Step 14 Save the configuration.

commit-buffer

Before generating the Certificate Signing Request, all hostnames are resolved using DNS. If any hostname fails to resolve, the command errors out.

Example:

```
firepower-2110 /security/keyring/certreq* # commit-buffer
firepower-2110 /security/keyring/certreq #
```

Step 15 Display the certificate request, copy the request, and send it to the trust anchor or certificate authority.

show certreq

Copy the text of the certificate request, including the BEGIN and END lines, and save it in a file.

Example:

```
firepower-2110 /security/keyring/certreq # show certreq
Certificate request subject name: firepower1.example.com
Certificate request ip address: 10.10.10.9
Certificate request e-mail name:
Certificate request ipv6 address: ::
Certificate request country name:
State, province or county (full name):
Locality name (eg, city):
Organisation name (eg, company):
Organisational Unit Name (eg, section):
DNS name (subject alternative name):
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIICoDCCAYgCAQAwITEfMB0GA1UEAwwWZmlyZXBvd2VyMS5leGFtcGxlLmNvbTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALJM7bmSCJte3gAU9DgDVN3E
tEfrbf0hMeLYgs5qkkvW7T8x3gHKn2Lwk4wFFAdHPxceVZwaBnXW8F5MFzdtyBY+
Du+RkpraLtle4HEMdNw1rnoDcv4ZHmbK47XYR1SFXSzer5lOXptGbOCloUn34L6/
pKlDlfV+1L+LlDYD++RG2DhbekWcFk13loZvCVhw99Wmc4X7CsypKY4uGH3lAwnl
/TF32ORXi0t2GXju6kbqUahhxN2kGxL7+4eLBeA/ninajCkJDIGJlnXuFa2ArfbF
39p+3UuVzcc9V/OH6d+buLjmQvtn+DwoPQhCVDYlNt+p3ZgnqnJWULNLBPMlof0C
AwEAAaA6MDgGCSqGSIb3DQEJDjErMCkwJwYDVR0RBCAwHoIWZmlyZXBvd2VyMS5l
eGFtcGxlLmNvbYcECgoKCTANBgkqhkiG9w0BAQsFAAOCAQEAjBw8lEb6cRapyMh/
Dfiyuet4wT0QmXQKy3xLXQjv6RGb5SOf3NkcaNvcx3KuKJwoJQGhdRV4Jhk4rgmT
QmlWX4rY7B2MFUwf6qSaj/E5W0N0RQg+5aZ/hZjPGV3zcuzY6yfixxXBpoPAirZQ
2luPaa21+HR4LTDInRj0127xMIkeKmv7AHSjyMoJdgs8DGJilTwPy93kZV//Iq9P
LrnKR7gpsXzXOoK6PTxP3pwhC21qjdmevn3ICPjDI68AtqjAuB15p/T2l+GFi/gB
XJMx2Mm9qiope3FEXIGH2ZhbJ+P7oBfGzgx2EHSI8H98O8a9uO8WV2yd/dKtv2IG
ICxHEw==
-----END CERTIFICATE REQUEST-----
```

Step 16 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 17 Exit certreq mode.

exit

Example:

```
firepower-2110 /security/keyring/certreq # exit
firepower-2110 /security/keyring #
```

Step 18 Specify the trusted point that you created earlier.

set trustpoint *name*

Example:

```
firepower-2110 /security/keyring # set trustpoint trust1
firepower-2110 /security/keyring* #
```

Step 19 Upload the certificate you obtained from the trust anchor or certificate authority.

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.

Note The certificate must be in Base64 encoded X.509 (CER) format.

Example:

```
firepower-2110 /security/keyring* #
```

Step 20 Save the configuration.

commit-buffer

Example:

```
firepower-2110 /security/keyring* # commit-buffer
firepower-2110 /security/keyring #
```

Step 21 Display the contents of the imported certificate, and verify that the **Certificate Status** value displays as **Valid**.

show keyring *keyring_name* **detail**

Example:

```
firepower-2110 /security #  scope security
firepower-2110 /security #  show keyring kr1 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
MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3Rp
bjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTYwNDI4MTMw
OTU0WhcNMTgwNDI4MTMwOTU0WjB3MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2Fs
aWZvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxFjAUBgNVBAoTDUNpc2NvIFN5c3Rl
bXMxDDAKBgNVBAsTA1RBQzEaMBgGA1UEAxMRZnA0MTIwLnRlc3QubG9jYWwwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+LglUQA0b7tga
BwdudS3sulXIwKGco48mMHCRQw1ADWZCxFANxsnbfb+wrR8xKfKo4vwnMLuK3F5U
RlHLPv9rHtYY296D9c/7N3Tee3gZczrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
ikoJn55JKRImRMHVkdopX1u21iDeR/9QRRSCT8TKtWrcH67YOyig9WrvqZObwHBg
yodskS/g+a5GNYTzzIS9XAfslMSKP06/Ftq2MONVIkdkFRG0Jqe/IG8a4s/9D82a
/cujcb0hNssvmAhhlVq1PGnodNR7MfYwgjM5q9Tp3W0H2ufLGAa2Hl09XR2FAgMB
AAGjggJYMIICVDAcBgNVHREEFTATghFmcDQxMjAudGVzdC5sb2NhbDAdBgNVHQ4E
FgQU/1WpstiEYExs8DlZWcuHZwPtu5QwHwYDVR0jBBgwFoAUyInbDHPrFwEEBcbx
GSgQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzqCBy6CByIaBxWxkYXA6Ly8vQ049bmFh
dXN0aW4tTkFBVVNUSU4tUEMtQ0EsQ049bmFhdXN0aW4tcGMsQ049Q0RQLENOPVB1
YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRp
b24sREM9bmFhdXN0aW4sREM9bG9jYWw/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlz
dD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHMBggrBgEF
BQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKGgaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B
QVVTVElOLVBDLUNBLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxD
Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2Fs
P2NBQ2VydGlmaWNhdGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0
aG9yaXR5MCEGCSsGAQQBgjcUAgQUHhIAVwBlAGIAUwBlAHIAdgBlAHIwDgYDVR0P
AQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0gAMEUC
IFew7NcJirEtFRvyxjkQ4/dVo2oI6CRB308WQbYHNUu/AiEA7UdObiSJBG/PBZjm
sgoIK60akbjotOTvUdUd9b6K1Uw=
-----END CERTIFICATE-----

    Zeroized: No
```

Example

The following example adds a certificate to a new key ring.

```
firepower-2110# scope security
firepower-2110 /security # enter trustpoint tPoint10
firepower-2110 /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMDCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3nO4MIGeBgNVHSMEgZYwgZOAFLlNjtcEMyZ+f7+3yh42
> 1ido3nO4oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAcT
> C1NhbnRhIENsYXJhMRswGQYDVQQKExJOdW92YSBTeXN0ZW1zIEluYy4xFDASBgNV
> BAsTC0VuZ2luZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0Q0GCAQAwDAYDVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8copP1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
firepower-2110 /security/trustpoint* # exit
firepower-2110 /security* # enter keyring kr220
firepower-2110 /security/keyring* # set modulus mod1024
firepower-2110 /security/keyring* # enter certreq
Certificate request password: peonygarage
Confirm certificate request password: peonygarage
firepower-2110 /security/keyring/certreq* # set ip 192.168.200.123
firepower-2110 /security/keyring/certreq* # set subject-name sjc04.example.com
firepower-2110 /security/keyring/certreq* # commit-buffer
firepower-2110 /security/keyring/certreq # show certreq
Certificate request subject name: sjc04.example.com
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
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
```

```
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXD0lZTL09H
BA==
-----END CERTIFICATE REQUEST-----

firepower-2110 /security/keyring/certreq # exit
firepower-2110 /security/keyring #
firepower-2110 /security/keyring # set trustpoint tPoint10
firepower-2110 /security/keyring* # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
> -----BEGIN CERTIFICATE-----
> MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
> -----END CERTIFICATE-----
> ENDOFBUF
firepower-2110 /security/keyring* # commit-buffer
firepower-2110 /security/keyring #
```

Regenerate the Default Key Ring Certificate

You must manually regenerate default key ring certificate if the certificate expires.

Procedure

Step 1 Enter security mode.

scope security

Example:

```
firepower-2110# scope security
firepower-2110 /security #
```

Step 2 Enetr the default key ring.

enter keyring default

Example:

```
firepower-2110 /security # enter keyring default
firepower-2110 /security/keyring #
```

Step 3 Regenerate the default key ring:

set regenerate yes

Example:

```
firepower-2110 /security/keyring # set regenerate yes
```

Step 4 Save the configuration.

commit-buffer

Example:

```
firepower-2110 /security/keyring* # commit-buffer
firepower-2110 /security/keyring #
```

Example

The following example regenerates the default key ring:

```
firepower-2110# scope security
firepower-2110 /security # enter keyring default
firepower-2110 /security/keyring # set regenerate yes
firepower-2110 /security/keyring* # commit-buffer
firepower-2110 /security/keyring #
```

Configure HTTPS

The HTTPS service is enabled on port 443 by default. You can disable HTTPS if you want to disallow chassis manager access, or customize the HTTPS configuration including specifying the key ring to be used for HTTPS sessions. By default, the Firepower 2100 uses the default key ring with a self-signed certificate.

Note 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 and then services mode.

scope system

scope services

Example:

```
firepower-2110# scope system
firepower-2110 /system # scope services
Firepower-chassis /system/services #
```

Step 2 To configure HTTPS access to the chassis, do one of the following:

- Allow HTTPS access to the chassis.

  enable https

- Disallow HTTPS access to the chassis.

  disable https

Example:

```
firepower-2110 /system/services # disable https
firepower-2110 /system/services* #
```

Step 3 (Optional) Specify the HTTPS port. Port 443 is the default port.

set https port *port_num*

Example:

```
Firepower-chassis /system/services* # set https port 4443
```

Step 4 (Optional) Specify the name of a key ring you added. See Install a Trusted Identity Certificate, on page 54.

set https keyring *keyring_name*

Example:

```
Firepower-chassis /system/services* # set https keyring kr1
```

Step 5 (Optional) Specify the level of Cipher Suite security used by the domain.

set https cipher-suite-mode *cipher_suite_mode*

The *cipher_suite_mode* can be one of the following keywords:

- **high-strength**
- (Default) **medium-strength**
- **low-strength**
- **custom**—Lets you specify a user-defined Cipher Suite specification string using the **set https cipher-suite** command.

Example:

```
Firepower-chassis /system/services* # set https cipher-suite-mode high-strength
```

Step 6 (Optional) If you set the cipher suite mode to **custom**, specify the custom cipher suite.

set https cipher-suite *cipher_suite_string*

The *cipher_suite_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#sslciphersuite.

For example, the medium strength specification string FXOS uses as the default is: **`ALL:!ADH:!EXPORT56:!LOW:RC4+RSA:+HIGH:+MEDIUM:+EXP:+eNULL`**

Example:

```
Firepower-chassis /system/services* # set https cipher-suite
DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256
```

Step 7 Set the SSL version.

set https access-protocols *comma_separated_values*

comma_separated_values include:

- **tlsv1**
- **tlsv1.1**
- **tlsv1.2**
- **sslv3**

Note Newer browsers do not support SSLv3, so you should also specify other protocols. If you only specify SSLv3, you may see an error in your browser indicating an unsupported security protocol version.

Step 8 (Optional) Enable or disable the certificate revocation list check.

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

Example:

```
Firepower-chassis /system/services* # set revoke-policy strict
```

Step 9 Save the configuration.

commit-buffer

Example:

```
Firepower-chassis /system/services* # commit-buffer
firepower-2110 /system/services #
```

Example

The following example enables HTTPS, sets the port number to 4443, sets the key ring name to kring7984, and sets the Cipher Suite security level to high:

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # enable https
Firepower-chassis /system/services* # set https port 4443
```

```
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 #
```

Configure an IPSec Secure Channel

You can configure an IPSec tunnel to encrypt management traffic. The Firepower 2100 supports the following ciphers and algorithms:

Table 2: IKE and ESP Ciphers and Algorithms

Type	Values
Ciphers	aes128, aes192, aes256, aes128gcm16
Pseudo-Random Function (PRF) (IKE only)	prfsha1, prfsha384, prfsha512, prfsha256
Integrity Algorithms	sha1, sha256, sha384, sha512, sha1_160
Diffie-Hellman Groups	modp2048, curve25519, ecp256, ecp384, ecp521, modp3072, modp4096

Note curve25519 is not supported in FIPS or Common Criteria mode.

Before you begin

For FIPS mode, the IPSec peer must support RFC 7427.

Procedure

Step 1 Install a Trusted Identity Certificate, on page 54.

Step 2 Enter security and then IPSec mode:

scope security

scope ipsec

Example:

```
Firepower-2110# scope security
Firepower-2110 /security # scope ipsec
Firepower-2110 /security/ipsec #
```

Step 3 (Optional) Set the log verbose level:

set log-level *0-4*

Example:

```
Firepower-2110 /security/ipsec # set log-level 3
Firepower-2110 /security/ipsec* #
```

Step 4 (Optional) Configure the enforcement of matching cryptographic key strength between IKE and SA connections:

set sa-strength-enforcement {**yes** | **no**}

- **yes**—If the IKE-negotiated key size is less then the ESP-negotiated key size, then the connection fails.
- **no**—The SA enforcement check passes, and the connection is successful.

Example:

```
Firepower-2110 /security/ipsec # set sa-strength-enforcement yes
Firepower-2110 /security/ipsec* #
```

Step 5 Create and enter an IPSec connection:

create connection *connection_name*

Step 6 Set IPSec mode to tunnel or transport:

set mode *tunnel_or_transport*

Step 7 Set the local IP address:

set local-address *ip_address*

Step 8 Set the remote IP address:

set remote-address *ip_address*

You can specify the remote address as an FQDN if you configured the DNS server (see Configure DNS Servers, on page 48).

Example:

```
Firepower-2110 /security/ipsec/connection* # set remote-address
```

Step 9 If using tunnel mode, set the remote subnet:

set remote-subnet *ip/mask*

Step 10 Set the remote identity:

set remote-ike-id *remote_identity_name*

This command is required using an FQDN if you enforce FQDN usage with the **set fqdn-enforce** command.

Example:

```
Firepower-2110 /security/ipsec/connection* # set remote-ike-id charlesdarwin.cisco.com
```

Step 11 Enforce FQDN usage.

set fqdn-enforce {**none** | **remote-ike-id**}

You must configure DNS (see Configure DNS Servers, on page 48) if you enable this feature. Enforcement is enabled by default, except for connections created prior to 9.13(1); you must manually enable enforcement for those old connections.

You must configure a valid Remote IKE ID (**set remote-ike-id**) in FQDN format. If you disable FQDN enforcement, the Remote IKE ID is optional, and can be set in any format (FQDN, IP Address, Subject Name, and so on).

Example:

```
Firepower-2110 /security/ipsec/connection* # set fqdn-enforce remote-ike-id
```

Step 12 Set the keyring name:

set keyring-name *name*

Step 13 (Optional) Set the keyring password:

set keyring-passwd *passphrase*

Step 14 (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 15 (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 16 (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 17 (Optional) Enable or disable the certificate revocation list check:

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

Step 18 Enable the connection:

set admin-state enable

Step 19 Reload connections:

reload-conns

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

Step 20 (Optional) Add the existing trustpoint name to IPsec:

create authority *trustpoint_name*

Configure Management Access

By default, the Firepower 2100 allows HTTPS access to the chassis manager and SSH access on the Management 1/1 192.168.45.0/24 network. If you want to allow access from other networks, or to allow SNMP, you must add or change the Access Lists.

Procedure

Step 1 Enter system and then services mode.

scope system

scope services

Example:

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services #
```

Step 2 Create an access list for the services to which you want to enable access.

For IPv4:

enter ip-block *ip prefix_length* {**https** | **snmp** | **ssh**}

For IPv6:

enter ipv6-block *ip prefix_length* **https** | **snmp** | **ssh**}

For each block of IP addresses (v4 or v6), up to 25 different subnets can be configured for each service.

- *ip*—A subnet of 0.0.0.0 and a prefix of 0 allows unrestricted access to a service.
- *prefix_length*—For IPv4, the prefix length is from 0 to 32. For IPv6, the prefix length is from 0 to 128.

Example:

```
firepower-2110 /system/services # enter ip-block 0.0.0.0 0 https
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 10.0.0.0 8 ssh
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 192.168.0.0 16 ssh
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 10.10.3.0 24 snmp
firepower-2110 /system/services/ip-block* #
```

Step 3 Save the configuration.

commit-buffer

Example:

```
firepower-2110 /system/services/ip-block* # commit-buffer
```

```
firepower-2110 /system/services/ip-block #
```

Examples

IPv4:

```
firepower-2110 # scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enter ip-block 10.1.1.0 24 https
firepower-2110 /system/services/ip-block* # commit-buffer
firepower-2110 /system/services/ip-block # exit
firepower-2110 /system/services # enter ip-block 10.2.1.0 24 ssh
firepower-2110 /system/services/ip-block* # commit-buffer
firepower-2110 /system/services/ip-block # exit
firepower-2110 /system/services # enter ip-block 10.3.1.0 24 snmp
firepower-2110 /system/services/ip-block* # commit-buffer
firepower-2110 /system/services/ip-block # exit
firepower-2110 /system/services # show ip-block
Permitted IP Block:
    IP Address      Prefix Length Protocol
    --------------- ------------- --------
    10.1.1.0        24            Https
    10.2.1.0        24            Ssh
    10.3.1.0        24            Snmp
```

IPv6:

```
firepower-2110 /system/services # enter ipv6-block 2001:0DB8:BA98:: 64 ssh
firepower-2110 /system/services/ipv6-block* # commit-buffer
firepower-2110 /system/services/ipv6-block # exit
firepower-2110 /system/services # enter ipv6-block 2001:0DB8:BA98:: 64 snmp
firepower-2110 /system/services/ipv6-block* # commit-buffer
firepower-2110 /system/services/ipv6-block # exit
firepower-2110 /system/services # enter ipv6-block 2001:0DB8:BA98:: 64 https
firepower-2110 /system/services/ipv6-block* # commit-buffer
firepower-2110 /system/services/ipv6-block # exit
firepower-2110 /system/services # show ipv6-block
Permitted IPv6 Block:
    IPv6 Address Prefix Length Protocol
    ------------ ------------- --------
    2001:0DB8:BA98::   64      Https
    2001:0DB8:BA98::   64      Snmp
    2001:0DB8:BA98::   64      Ssh
```

Configure the DHCP Server for Management Clients

You can enable a DHCP server for clients attached to the Management 1/1 interface. By default, the server is enabled with the following address range: 192.168.45.10-192.168.45.12. If you want to change the management IP address, you must disable DHCP (see Change the FXOS Management IP Addresses or Gateway, on page 95). You can then reenable DHCP for the new network.

Procedure

Step 1 Enter system and then services mode.

scope system

scope services

Example:

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services #
```

Step 2 To configure the DHCP server, do one of the following:

- Enable the DHCP server.

  enable dhcp-server *start_ip end_ip*

- Disable the DHCP server.

  disable dhcp-server

Example:

```
firepower-2110 /system/services # enable dhcp-server 10.10.10.5 10.10.10.50
firepower-2110 /system/services* #
```

Step 3 Save the configuration.

commit-buffer

Example:

```
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

Example

The following example enables the DHCP server:

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enable dhcp-server 192.168.1.8 192.168.1.40
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

Configure Syslog Messaging

Logs are useful both in routine troubleshooting and in incident handling. You can send syslog messages to the Firepower 2100 console, SSH session, or a local file.

These syslog messages apply only to the FXOS chassis. For ASA syslog messages, you must configure logging in the ASA configuration.

Procedure

Step 1 Enter monitoring mode.

scope monitoring

Example:

```
firepower-2110# scope monitoring
firepower-2110 /monitoring #
```

Step 2 Configure the local sources that generate syslog messages.

- **enable syslog source** {**audits** | **events** | **faults**}
- **disable syslog source** {**audits** | **events** | **faults**}

Example:

```
firepower-2110 /monitoring # disable syslog source audits
firepower-2110 /monitoring* # enable syslog source events
firepower-2110 /monitoring* # enable syslog source faults
```

Step 3 Send syslog messages to the console.

a) Enable or disable the sending of syslogs to the console.

- **enable syslog console**
- **disable syslog console**

Example:

```
firepower-2110 /monitoring* # enable syslog console
```

b) Select the lowest message level that you want displayed on the console.

set syslog console level {**emergencies** | **alerts** | **critical**}

The system displays this level and above on the console. The level options are listed in order of decreasing urgency. The default level is Critical.

Example:

```
firepower-2110 /monitoring* # set syslog console level alerts
```

Step 4 Send syslog messages to an SSH session.

a) Enable or disable sending syslog messages to an SSH session.

- **enable syslog monitor**
- **disable syslog monitor**

Example:

```
firepower-2110 /monitoring* # enable syslog monitor
```

b) Select the lowest message level that you want displayed in an SSH session.

set syslog monitor level {**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}

The system displays this level and above. The level options are listed in order of decreasing urgency. The default level is Critical.

Note Messages at levels below Critical are displayed on the terminal monitor only if you have entered the **terminal monitor** command.

Example:

```
firepower-2110 /monitoring* # set syslog monitor level alerts
```

Step 5 Send syslog messages to a file.

a) Enable or disable the writing of syslog information to a syslog file.

- **enable syslog file**
- **disable syslog file**

Example:

```
firepower-2110 /monitoring* # enable syslog file
```

b) Specify the name of the file in which the messages are logged.

set syslog file name *filename*

Up to 16 characters are allowed in the file name.

Example:

```
firepower-2110 /monitoring* # set syslog file name syslog1
```

c) Select the lowest message level that you want stored to a file.

set syslog file level {**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}

The system stores this level and above in the syslog file. The level options are listed in order of decreasing urgency. The default level is Critical.

Example:

```
firepower-2110 /monitoring* # set syslog file level debugging
```

d) Specify the maximum file size, in bytes, before the system begins to write over the oldest messages with the newest ones.

set syslog file size *filesize*

The range is 4096 to 4194304 bytes.

Example:

```
firepower-2110 /monitoring* # set syslog file size 60000
```

Step 6 Save the configuration.

commit-buffer

Example:

```
firepower-2110 /monitoring* # commit-buffer
firepower-2110 /monitoring #
```

Example

This example shows how to enable the storage of syslog messages in a local file:

```
firepower-2110# scope monitoring
firepower-2110 /monitoring # disable syslog console
firepower-2110 /monitoring* # disable syslog monitor
firepower-2110 /monitoring* # enable syslog file
firepower-2110 /monitoring* # set syslog file name SysMsgsFirepower
firepower-2110 /monitoring* # set syslog file level notifications
firepower-2110 /monitoring* # set syslog file size 4194304
firepower-2110 /monitoring* # commit-buffer
firepower-2110 /monitoring #
```

Enable SNMP

This section describes how to configure the Simple Network Management Protocol (SNMP) on the chassis.

About SNMP

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.
- 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.

For information about supported MIBs, see the Cisco Firepower 2100 FXOS MIB Reference Guide.

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.

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 3: 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.
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 supported MIBs, see the Cisco Firepower 2100 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

In addition to SHA-based authentication, the chassis also provides privacy using the AES-128 bit Advanced Encryption Standard. 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 80 characters.

Configure SNMP

Enable SNMP, add traps and SNMPv3 users.

Procedure

Step 1 Enter monitoring mode.

scope monitoring

Example:

```
firepower-2110# scope monitoring
firepower-2110 /monitoring #
```

Step 2 Enable SNMP.

enable snmp

Example:

```
firepower-2110 /monitoring # enable snmp
firepower-2110 /monitoring* #
```

Step 3 Set the SNMP community name.

set snmp community

You are prompted to enter the SNMP community name. The community name can be any alphanumeric string up to 32 characters.

Example:

```
firepower-2110 /monitoring* # set snmp community
Enter a snmp community: community1
firepower-2110 /monitoring* #
```

Step 4 Specify the system contact person responsible for SNMP.

set snmp syscontact *system-contact-name*

The system contact name can be any alphanumeric string up to 255 characters, such as an email address or name and telephone number.

Example:

```
firepower-2110 /monitoring* # set snmp syscontact jcrichton@example.com
firepower-2110 /monitoring* #
```

Step 5 Specify the location of the host on which the SNMP agent (server) runs.

set snmp syslocation *system-location-name*

The system location name can be any alphanumeric string up to 512 characters.

Example:

```
firepower-2110 /monitoring* # set snmp syslocation boulder, co
firepower-2110 /monitoring* #
```

Step 6 Create an SNMPv3 user.

a) Specify the username and password.

enter snmp-user *user-name*

You are prompted to enter the password.

Example:

```
firepower-2110 /monitoring* # enter snmp-user jcrichton
Password: aerynsun
firepower-2110 /monitoring/snmp-user* #
```

b) Enable AES-128 encryption.

set aes-128 {**no** | **yes**}

By default, AES-128 encryption is disabled.

Example:

```
firepower-2110 /monitoring/snmp-user* # set aes-128 yes
firepower-2110 /monitoring/snmp-user* #
```

c) Specify the user privacy password.

set priv-password

You are prompted to enter and confirm the privacy password.

Example:

```
firepower-2110 /monitoring/snmp-user* # set priv-password
Enter a password: moyahome
Confirm the password: moyahome
firepower-2110 /monitoring/snmp-user* #
```

d) Exit SNMP user mode.

exit

Example:

```
firepower-2110 /monitoring/snmp-user* # exit
firepower-2110 /monitoring* #
```

Step 7 Add an SNMP trap.

a) Create the SNMP trap.

enter snmp-trap {*hostname* | *ip-addr* | *ip6-addr*}

Example:

```
firepower-2110 /monitoring* # enter snmp-trap 10.10.10.67
firepower-2110 /monitoring/snmp-trap* #
```

b) Specify the SNMP community name to be used for the SNMP trap.

set community *community-name*

Example:

```
firepower-2110 /monitoring/snmp-trap* # set community community1
firepower-2110 /monitoring/snmp-trap* #
```

c) Specify the port to be used for the SNMP trap.

set port *port-num*

Example:

```
firepower-2110 /monitoring/snmp-trap* # set port 3434
firepower-2110 /monitoring/snmp-trap* #
```

d) Specify the SNMP version and model used for the trap.

set version {**v1** | **v2c** | **v3**}

Example:

```
firepower-2110 /monitoring/snmp-trap* # set version v2c
firepower-2110 /monitoring/snmp-trap* #
```

e) (Optional) Specify the type of trap to send.

set notificationtype {**traps** | **informs**}

- **traps**—Sets the type to traps if you select v2c or v3 for the version.
- **informs**—Sets the type to informs if you select v2c for the version.

Example:

```
firepower-2110 /monitoring/snmp-trap* # set notificationtype informs
firepower-2110 /monitoring/snmp-trap* #
```

f) (Optional) If you select v3 for the version, specify the privilege associated with the trap.

set v3privilege {**auth** | **noauth** | **priv**}

- **auth**—Enables authentication but no encryption
- **noauth**—Does not enable authentication or encryption
- **priv**—Enables authentication and encryption

Example:

```
firepower-2110 /monitoring/snmp-trap* # set v3privilege priv
```

```
firepower-2110 /monitoring/snmp-trap* #
```

g) Exit SNMP trap mode.

exit

Example:

```
firepower-2110 /monitoring/snmp-trap* # exit
firepower-2110 /monitoring* #
```

Step 8 Save the configuration.

commit-buffer

Example:

```
firepower-2110 /monitoring* # commit-buffer
firepower-2110 /monitoring #
```

Example

The following example enables SNMP.

```
firepower-2110# scope monitoring
firepower-2110 /monitoring # enable snmp
firepower-2110 /monitoring* # set snmp community
Enter a snmp community: SnmpCommSystem2
firepower-2110 /monitoring* # set snmp syscontact contactperson1
firepower-2110 /monitoring* # set snmp syslocation systemlocation
firepower-2110 /monitoring* # enter snmp-user snmp-user14
Password: happy
firepower-2110 /monitoring/snmp-user* # set aes-128 yes
firepower-2110 /monitoring/snmp-user* # set priv-password
Enter a password: ecstatic
Confirm the password: ecstatic
firepower-2110 /monitoring/snmp-user* # exit
firepower-2110 /monitoring* #
firepower-2110 /monitoring* # enter snmp-trap 192.168.100.112
firepower-2110 /monitoring/snmp-trap* # set community SnmpCommSystem2
firepower-2110 /monitoring/snmp-trap* # set port 12009
firepower-2110 /monitoring/snmp-trap* # set version v3
firepower-2110 /monitoring/snmp-trap* # set notificationtype traps
firepower-2110 /monitoring/snmp-trap* # set v3privilege priv
firepower-2110 /monitoring/snmp-trap* # exit
firepower-2110 /monitoring* #
firepower-2110 /monitoring* # enter snmp-trap 2001::1
firepower-2110 /monitoring/snmp-trap* # set community SnmpCommSystem3
firepower-2110 /monitoring/snmp-trap* # set port 12009
firepower-2110 /monitoring/snmp-trap* # set version v3
firepower-2110 /monitoring/snmp-trap* # set notificationtype traps
firepower-2110 /monitoring/snmp-trap* # set v3privilege priv
firepower-2110 /monitoring/snmp-trap* # commit-buffer
firepower-2110 /monitoring/snmp-trap #
```

Enable FIPS and Common Criteria Mode

Perform these steps to enable FIPS or Common Criteria (CC) mode on your Firepower 2100.

You must also separately enable FIPS mode on the ASA using the **fips enable** command. On the ASA, there is not a separate setting for Common Criteria mode; any additional restrictions for CC or UCAPL compliance must be configured in accordance with Cisco security policy documents.

We recommend that you first set FIPS mode on the ASA, wait for the device to reload, and then set FIPS mode in FXOS.

Procedure

Step 1 Enter security mode.

scope security

Example:

```
firepower-2110# scope security
firepower-2110 /security #
```

Step 2 Enable FIPS mode.

enable fips-mode

Example:

```
firepower-2110 /security # enable fips-mode
Warning: Connectivity to one or more services may be denied when committed. Please consult
 the product's FIPS Security Policy documentation.
WARNING: A reboot of the system is required in order for the system to be operating in a
FIPS approved mode.
firepower-2110 /security* #
```

Step 3 Enable Common Criteria mode.

enable cc-mode

Example:

```
firepower-2110 /security* # enable cc-mode
Warning: Connectivity to one or more services may be denied when committed. Please consult
 the product's CC Security Policy documentation.
WARNING: A reboot of the system is required in order for the system to be operating in a
CC approved mode.
```

Step 4 Save the configuration.

commit-buffer

Example:

```
firepower-2110 /security* # commit-buffer
```

```
firepower-2110 /security #
```

Step 5 Reboot the system.

scope chassis 1

reboot

Example:

```
firepower-2110 /security # scope chassis 1
firepower-2110 /chassis # reboot
```

User Management

User accounts are used to access the Firepower 2100 chassis. These accounts work for chassis manager and for SSH access. The ASA has separate user accounts and authentication.

About User Accounts

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. The default password is **Admin123**.

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

Locally-Authenticated User Accounts

You can configure up to 48 local user accounts. Each user account must have a unique username and password.

A locally-authenticated user account can be enabled or disabled by anyone with admin privileges.

Guidelines for User Accounts

Usernames

The username is used as the login ID for the Secure Firewall chassis manager and the FXOS CLI. When you assign login IDs, 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.

Passwords

A password is required for each locally-authenticated user account. A user with admin 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, FXOS rejects any password that does not meet the following requirements:

- Must contain a minimum of 8 characters and a maximum of 127 characters.

Note You can optionally configure a minimum password length of 15 characters on the system, to comply with Common Criteria requirements.

- 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 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).
- Must not be blank.

Add a User

Add local users for chassis manager and FXOS CLI access.

Before you begin

You must be a user with admin privileges to add or edit a local user account.

Procedure

Step 1 Enter security mode:

scope security

Example:

```
firepower-2110# scope security
firepower-2110 /security #
```

Step 2 Create the user account:

enter local-user *local-user-name*

- *local-user-name*—Sets 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 User Accounts, on page 83).

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

Example:

```
firepower-2110 /security # enter local-user johncrichton
firepower-2110 /security/local-user* #
```

Step 3 Specify whether the local user account is active or inactive:

set account-status {**active**| **inactive**}

By default, the user is active.

Example:

```
firepower-2110 /security/local-user* # set account-status inactive
```

Step 4 Set the password for the user account:

set password

Enter a password: *password*

Confirm the password: *password*

If you enable the password strength check, the password must be strong, and FXOS rejects any password that does not meet the strength check requirements (see Configure User Settings, on page 87 and Guidelines for User Accounts, on page 83).

Example:

```
firepower-2110 /security/local-user* # set password
Enter a password: aeryn
Confirm the password: aeryn
firepower-2110 /security/local-user* #
```

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

set firstname *first-name*

Example:

```
firepower-2110 /security/local-user* # set firstname John
```

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

set lastname *last-name*

Example:

```
firepower-2110 /security/local-user* # set lastname Crichton
```

Step 7 (Optional) Specify the date that the user account expires.

set expiration *month* *day-of-month* *year*

- *month*—Sets the month as the first three letters of the month name.

The account cannot be used after the date specified. 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.

By default, user accounts do not expire.

Example:

```
firepower-2110 /security/local-user* # set expiration oct 10 2019
```

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

set email *email-addr*

Example:

```
firepower-2110 /security/local-user* # set email jcrichton@example.com
```

Step 9 (Optional) Specify the user phone number.

set phone *phone-num*

Example:

```
firepower-2110 /security/local-user* # set phone 303-555-7891
```

Step 10 (Optional) Assign the admin role to the user.

enter role admin

All users are assigned the **read-only** role by default, and this role cannot be removed. The **admin** role allows read-and-write access to the configuration.

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.

Example:

```
firepower-2110 /security/local-user* # enter role admin
```

Step 11 Save the configuration.

commit-buffer

Example:

```
firepower-2110 security/local-user* # commit-buffer
firepower-2110 security/local-user #
```

Examples

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

```
firepower-2110# scope security
firepower-2110 /security # create local-user aerynsun
firepower-2110 /security/local-user* # set password
Enter a password: rygel
Confirm the password: rygel
firepower-2110 /security/local-user* # enter role admin
firepower-2110 /security/local-user* # commit-buffer
firepower-2110 /security/local-user #
```

Configure User Settings

You can configure global settings for all users.

Procedure

Step 1 Enter security mode:

scope security

Example:

```
firepower-2110# scope security
firepower-2110 /security #
```

Step 2 Enable or disable the password strength check.

set enforce-strong-password {**yes** | **no**}

If the password strength check is enabled, the Firepower 2100 does not permit a user to choose a password that does not meet the guidelines for a strong password (see Guidelines for User Accounts, on page 83). The strong password check is enabled by default.

Example:

```
firepower-2110 /security # set enforce-strong-password yes
firepower-2110 /security* #
```

Step 3 Enter password-profile mode.

scope password-profile

Example:

```
firepower-2110 /security* # scope password-profile
firepower-2110 /security/password-profile* #
```

Step 4 Configure the minimum password length.

set min-password-length *min_length*

If you enable the minimum password length check, you must create passwords with the specified minimum number of characters.

Example:

```
firepower-2110 /security/password-profile* # set min-password-length 8
```

Step 5 Enable or disable whether a locally-authenticated user can make password changes within a given number of hours.

Allow changes:

set change-interval *num-of-hours*

set change-count *pass-change-num*

- *num_of_hours*—Sets the number of hours during which the number of password changes are enforced, between 1 and 745 hours.
- *pass_change_num*—Sets the maximum number of times that a locally-authenticated user can change their password during the change interval, between 0 and 10.

To disallow changes, set the **set change-interval** to **disabled**.

Example:

```
firepower-2110 /security/password-profile* # set change-count 2
firepower-2110 /security/password-profile* # set change-interval 24
```

Disallow changes:

set no-change-interval *min_num_hours* }

- *min_num_hours*—Set the minimum number of hours that a locally-authenticated user must wait before changing a newly created password, between 1 and 745.

To allow changes, set the **set no-change-interval** to **disabled**.

Example:

```
firepower-2110 /security/password-profile* # set no-change-interval 1
```

Step 6 Set password reuse requirements.

set history-count {*num_of_passwords* | **disabled**}

set password-reuse-interval {*days* | **disabled**}

- *num_of_passwords*—Specify the number of unique passwords that a locally-authenticated user must create before that user can reuse a previously-used password, between 0 and 15. By default, the minumum number is 0, which disables the history count and allows users to reuse previously-used passwords.
- *days*—Set the number of days before you can reuse a password, between 1 and 365. The default is 15 days.

If you enable both commands, then both requirements must be met. For example, if you set the history count to 3, and the reuse interval to 10 days, then you can change your password only after 10 days have passed, and you have changed your password 3 times.

Example:

```
firepower-2110 /security/password-profile* # set history-count 5
firepower-2110 /security/password-profile* # set password-reuse-interval 120
```

Step 7 Set password expiration settings.

set password-expiration {*days* | **never**}

set expiration-warning-period *days*

set expiration-grace-period *days*

- **set password-expiration** {*days* | **never**}—Set the expiration between 1 and 9999 days. By default, expiration is disabled (**never**).
- **set expiration-warning-period** *days*—Set the number of days before expiration to warn the user about their password expiration at each login, between 0 and 9999. The default is 14 days.
- **set expiration-grace-period** *days*—Set the number of days a user has to change their password after expiration, between 0 and 9999. The default is 3 days.

Example:

```
firepower-2110 /security/password-profile* # set password-expiration 120
firepower-2110 /security/password-profile* # set expiration-warning-period 5
firepower-2110 /security/password-profile* # set expiration-grace-period 5
```

Step 8 Set the absolute session timeout for all forms of access including serial console, SSH, and HTTPS.

scope default-auth

set absolute-session-timeout *seconds*

- *seconds*—Sets the absolute timeout value in seconds, between 0 and 7200. The default is 3600 seconds (60 minutes). To disable this setting, set the value to 0.

Example:

```
firepower-2110 /security* scope default-auth#
firepower-2110 /security/default-auth* # set absolute-session-timeout 7200
```

Step 9 Save the configuration.

commit-buffer

Example:

```
firepower-2110 /security/default-auth* # commit-buffer
firepower-2110 /security/default-auth #
```

Example

The following example sets many user requirements:

```
firepower-2110 # scope security
firepower-2110 /security # set enforce-strong-password yes
firepower-2110 /security* # scope password-profile
firepower-2110 /security/password-profile* # set change-during-interval enable
firepower-2110 /security/password-profile* # set change-count 5
firepower-2110 /security/password-profile* # set change-interval 72
firepower-2110 /security/password-profile* # set history-count 5
firepower-2110 /security/password-profile* # commit-buffer
firepower-2110 /security/password-profile #
```

System Administration

You can upgrade the ASA package, reload, or power off the chassis.

Upgrade the Image

This task applies to a standalone ASA. If you want to upgrade a failover pair, see the Cisco ASA Upgrade Guide. The upgrade process typically takes between 20 and 30 minutes.

The ASA, ASDM, and FXOS images are bundled together into a single package. Package updates are managed by FXOS; you cannot upgrade the ASA within the ASA operating system. You cannot upgrade ASA and FXOS separately from each other; they are always bundled together.

The exception is for ASDM, which you can upgrade from within the ASA operating system, so you do not need to only use the bundled ASDM image. ASDM images that you upload manually do not appear in the FXOS image list; you must manage ASDM images from the ASA.

Note When you upgrade the bundle, the ASDM image in the bundle replaces the previous ASDM bundle image because they have the same name (**asdm.bin**). But if you manually chose a different ASDM image that you uploaded (for example, **asdm-782.bin**), then you continue to use that image even after a bundle upgrade. To make sure that you are running a compatible version of ASDM, you should either upgrade ASDM before you upgrade the bundle, or you should reconfigure the ASA to use the bundled ASDM image (**asdm.bin**) just before upgrading the ASA bundle.

Before you begin

Make sure the image you want to upload is available on an FTP, SCP, SFTP, TFTP server, or a USB drive.

Procedure

Step 1 Connect to the FXOS CLI, either the console port (preferred) or using SSH. If you connect at the console port, you access the FXOS CLI immediately. Enter the FXOS login credentials. The default username is **admin** and the default password is **Admin123**.

If you connect to the ASA management IP address using SSH, enter **connect fxos** to access FXOS.

Step 2 Download the package to the chassis.

a) Enter firmware mode.

scope firmware

Example:

```
firepower-2110# scope firmware
firepower-2110 /firmware#
```

b) Download the package.

download image *url*

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

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

Example:

```
firepower-2110 /firmware # download image tftp://10.88.29.181/cisco-asa-fp2k.9.8.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
```

c) Monitor the download process.

show download-task

Example:

```
firepower-2110 /firmware # show download

Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.8.2.SPA
              Tftp     10.88.29.181             0                 Downloaded
    cisco-asa-fp2k.9.8.2.2.SPA
              Tftp     10.88.29.181             0                 Downloading
firepower-2110 /firmware #
```

Step 3 When the new package finishes downloading (**Downloaded** state), boot the package.

a) View the version number of the new package.

show package

Example:

```
firepower-2110 /firmware # show package
Name                                          Package-Vers
--------------------------------------------- ------------
cisco-asa-fp2k.9.8.2.SPA                      9.8.2
cisco-asa-fp2k.9.8.2.2.SPA                    9.8.2.2
firepower-2110 /firmware #
```

b) Install the package.

scope auto-install

install security-pack version *version*

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

Example:

```
firepower 2110 /firmware # scope auto-install
firepower-2110 /firmware/auto-install # install security-pack version 9.8.2.2

The system is currently installed with security software package 9.8.2, which has:
   - The platform version: 2.2.2.52
   - The CSP (asa) version: 9.8.2
If you proceed with the upgrade 9.8.2.2, it will do the following:
   - upgrade to the CSP asa version 9.8.2.2

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

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Attention:
   If you proceed the system will be re-imaged. All existing configuration will be lost,

   and the default configuration applied.
```

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

Triggered the install of software package version 9.8.2.2
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
firepower-2110 /firmware/auto-install #
```

Note Ignore the message, "All existing configuration will be lost, and the default configuration applied." The configuration will not be erased, and the default configuration is not applied. The default configuration is only applied during a reimage, not an upgrade.

Step 4 Wait for the chassis to finish rebooting (5-10 minutes). FXOS comes up first, but you still need to wait for the ASA to come up.

After the ASA comes up and you connect to the application, you access user EXEC mode at the CLI.

Example:

```
 [...]
Cisco FPR Series Security Appliance
firepower-2140 login: admin
Password:

Successful login attempts for user 'admin' : 1
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2018, Cisco Systems, Inc. All rights reserved.
[...]

User enable_1 logged in to ciscoasa
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
[press Enter to see the prompt below:]

firepower-2140# connect asa
Attaching to ASA CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

ciscoasa>
```

Reboot the Chassis

Procedure

Step 1 Enter chassis mode.

scope chassis 1

Example:

```
firepower-2110 # scope chassis 1
firepower-2110 /chassis #
```

Step 2 Reboot the chassis.

reboot ["*reason*"] [**no-prompt**]

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

Example:

```
firepower-2110 /chassis # reboot "This system is rebooting" no-prompt
```

Step 3 Monitor the reboot process.

show fsm status

Power Off the Chassis

The chassis will gracefully shut down the ASA OS before powering off the Firepower 2100 chassis. This process takes approximately 15-20 minutes. After the chassis has successfully powered off, you can then physically unplug the power on the chassis.

Procedure

Step 1 Enter chassis mode.

scope chassis 1

Example:

```
firepower-2110 # scope chassis 1
firepower-2110 /chassis #
```

Step 2 Power off the chassis.

shutdown ["*reason*"] [**no-prompt**]

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

Example:

```
firepower-2110 /chassis # shutdown "This system is powering off" no-prompt
```

Step 3 Monitor the shutdown process.

show fsm status

Change the FXOS Management IP Addresses or Gateway

You can change the FXOS management IP address on the Firepower 2100 chassis from the FXOS CLI. The default address is 192.168.45.45. You can also change the default gateway for FXOS management traffic. The default gateway is set to 0.0.0.0, which sends FXOS traffic over the backplane to be routed through the ASA data interfaces. If you want to route traffic to a router on the Management 1/1 network instead, then you can change the gateway IP address. You must also change the access list for management connections to match your new network. If you change the gateway from the default 0.0.0.0 (the ASA data interfaces), then you will not be able to access FXOS on a data interface nor will FXOS be able to initiate traffic on a data interface. See the getting started guide for information about FXOS access on a data interface.

Typically, the FXOS Management 1/1 IP address will be on the same network as the ASA Management 1/1 IP address, so this procedure also shows how to change the ASA IP address on the ASA.

Before you begin

- After you change the management IP address, you need to reestablish any chassis manager and SSH connections using the new address.
- Because the DHCP server is enabled by default on Management 1/1, you must disable DHCP before you change the management IP address.

Procedure

Step 1 Connect to the console port (see Connect to the ASA or FXOS Console, on page 28). We recommend that you connect to the console port to avoid losing your connection.

Step 2 Disable the DHCP server.

scope system

scope services

disable dhcp-server

commit-buffer

You can reenable DHCP using new client IP addresses after you change the management IP address. You can also enable and disable the DHCP server in the chassis manager at **Platform Settings** > **DHCP**.

Example:

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # disable dhcp-server
firepower-2110 /system/services* # commit-buffer
```

Step 3 Configure an IPv4 management IP address, and optionally the gateway.

a) Set the scope for fabric-interconnect a.

   scope fabric-interconnect a

   Example:

```
firepower-2110# scope fabric-interconnect a
```

```
firepower-2110 /fabric-interconnect #
```

b) View the current management IP address.

show

Example:

```
firepower-2110 /fabric-interconnect # show

Fabric Interconnect:
   ID   OOB IP Addr     OOB Gateway    OOB Netmask    OOB IPv6 Address OOB IPv6 Gateway
 Prefix Operability
   ---- --------------- -------------- --------------- --------------- ----------------
 ------ -----------
    A    192.168.45.45    0.0.0.0        0.0.0.0          ::               ::
     64     Operable
```

c) Configure a new management IP address, and optionally a new default gateway.

set out-of-band static ip *ip_address* **netmask** *network_mask* **gw** *gateway_ip_address*

To keep the currently-set gateway, omit the **gw** keyword. Similarly, to keep the existing management IP address while changing the gateway, omit the **ip** and **netmask** keywords.

To set the gateway to the ASA data interfaces, set the **gw** to 0.0.0.0. This is the default setting.

Example:

```
firepower-2110 /fabric-interconnect # set out-of-band static ip 192.168.4.1 netmask
255.255.255.0
Warning: When committed, this change may disconnect the current CLI session
firepower-2110 /fabric-interconnect* #
```

Step 4 Configure an IPv6 management IP address and gateway.

a) Set the scope for fabric-interconnect a, and then the IPv6 configuration.

scope fabric-interconnect a

scope ipv6-config

Example:

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect # scope ipv6-config
firepower-2110 /fabric-interconnect/ipv6-config #
```

b) View the current management IPv6 address.

show ipv6-if

Example:

```
firepower-2110 /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
    IPv6 Address                        Prefix     IPv6 Gateway
    ----------------------------------- ---------- ------------
    ::                                   ::         ::
```

c) Configure a new management IPv6 address and gateway:

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

To keep the currently-set gateway, omit the **ipv6-gw** keyword. Similarly, to keep the existing management IP address while changing the gateway, omit the **ipv6** and **ipv6-prefix** keywords.

To set the gateway to the ASA data interfaces, set the **gw** to ::. This is the default setting.

Example:

```
firepower-2110 /fabric-interconnect/ipv6-config # set out-of-band static ipv6 2001:DB8::34
 ipv6-prefix 64 ipv6-gw 2001:DB8::1
firepower-2110 /fabric-interconnect/ipv6-config* #
```

Step 5 Delete and add new access lists for HTTPS, SSH, and SNMP to allow management connections from the new network.

a) Set the scope for system/services.

scope system

scope services

Example:

```
firepower-2110# scope system
firepower-2110 /system # scope services
```

b) View the current access lists.

show ip-block

Example:

```
firepower-2110 /system/services # show ip-block

Permitted IP Block:
    IP Address      Prefix Length Protocol
    --------------- ------------- --------
    192.168.45.0               24 https
    192.168.45.0               24 ssh
firepower-2140 /system/services #
```

c) Add new access lists.

For IPv4:

enter ip-block *ip_address prefix* [**http** | **snmp** | **ssh**]

For IPv6:

enter ipv6-block *ipv6_address prefix* [**https** | **snmp** | **ssh**]

For IPv4, enter **0.0.0.0** and a prefix of **0** to allow all networks. For IPv6, enter **::** and a prefix of **0** to allow all networks. You can also add access lists in the chassis manager at **Platform Settings** > **Access List**.

Example:

```
firepower-2110 /system/services # enter ip-block 192.168.4.0 24 https
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 192.168.4.0 24 ssh
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 192.168.4.0 24 snmp
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ipv6-block 2001:DB8:: 64 https
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ipv6-block 2001:DB8:: 64 ssh
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ipv6-block 2001:DB8:: 64 snmp
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* #
```

a) Delete the old access lists.

For IPv4:

delete ip-block *ip_address prefix* [**http** | **snmp** | **ssh**]

For IPv6:

delete ipv6-block *ipv6_address prefix* [**https** | **snmp** | **ssh**]

Example:

```
firepower-2110 /system/services # delete ip-block 192.168.45.0 24 https
firepower-2110 /system/services* # delete ip-block 192.168.45.0 24 ssh
firepower-2110 /system/services* #
```

Step 6 (Optional) Reenable the IPv4 DHCP server.

scope system

scope services

enable dhcp-server *start_ip_address end_ip_address*

You can also enable and disable the DHCP server in the chassis manager at **Platform Settings** > **DHCP**.

Example:

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enable dhcp-server 192.168.4.10 192.168.4.20
```

Step 7 Save the configuration.

commit-buffer

Example:

```
firepower-2110 /system/services* # commit-buffer
```

Step 8 Change the ASA address to be on the correct network. The default ASA Management 1/1 interface IP address is 192.168.45.1.

a) From the console, connect to the ASA CLI and access global configuration mode.

   connect asa

   enable

   configure terminal

   Example:

   ```
   firepower-2110# connect asa
   Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
   Type help or '?' for a list of available commands.
   ciscoasa> enable
   Password:
   The enable password is not set. Please set it now.
   Enter Password: ******
   Repeat Password: ******
   ciscoasa# configure terminal
   ciscoasa(config)#
   ```

b) Change the Management 1/1 IP address.

   interface management1/1

   ip address *ip_address mask*

   Example:

   ```
   ciscoasa(config)# interface management1/1
   ciscoasa(config-ifc)# ip address 10.86.118.4 255.255.255.0
   ```

c) Change the network that can access ASDM.

   no http 192.168.45.0 255.255.255.0 management

   http *ip_address mask* **management**

   Example:

   ```
   ciscoasa(config)# no http 192.168.45.0 255.255.255.0 management
   ciscoasa(config)# http 10.86.118.0 255.255.255.0 management
   ```

d) Save the configuration.

   write memory

e) To return to the FXOS console, enter **Ctrl+a**, **d**.

Example

The following example configures an IPv4 management interface and gateway:

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect # show

Fabric Interconnect:
```

```
    ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
 Prefix Operability
    ---- --------------- --------------- --------------- ---------------- ----------------
 ------ -----------
    A    192.168.2.112    192.168.2.1     255.255.255.0   2001:DB8::2     2001:DB8::1
  64     Operable
firepower-2110 /fabric-interconnect # set out-of-band static ip 192.168.2.111 netmask
255.255.255.0 gw 192.168.2.1
Warning: When committed, this change may disconnect the current CLI session
firepower-2110 /fabric-interconnect* # commit-buffer
firepower-2110 /fabric-interconnect #
```

The following example configures an IPv6 management interface and gateway:

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect # scope ipv6-config
firepower-2110 /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
    IPv6 Address                        Prefix     IPv6 Gateway
    ----------------------------------  ---------- ------------
    2001:DB8::2                          64         2001:DB8::1
firepower-2110 /fabric-interconnect/ipv6-config # set out-of-band static ipv6 2001:DB8::2
ipv6-prefix 64 ipv6-gw 2001:DB8::1
firepower-2110 /fabric-interconnect/ipv6-config* # commit-buffer
firepower-2110 /fabric-interconnect/ipv6-config #
```

History for FXOS CLI Settings

Feature	Version	Details
Configurable HTTPS protocol	9.13(1)	You can set the SSL/TLS versions for HTTPS acccess. New/Modified commands: **set https access-protocols**
FQDN enforcement for IPSec and Keyrings	9.13(1)	You can configure FQDN enforcement so that the FDQN of the peer needs to match the DNS Name in the X.509 Certificate presented by the peer. For IPSec, enforcement is enabled by default, except for connections created prior to 9.13(1); you must manually enable enforcement for those old connections. For keyrings, all hostnames must be FQDNs, and cannot use wild cards. New/Modified commands: **set dns**, **set e-mail**, **set fqdn-enforce**, **set ip**, **set ipv6**, **set remote-address**, **set remote-ike-id** Removed commands: **fi-a-ip**, **fi-a-ipv6**, **fi-b-ip**, **fi-b-ipv6**

Feature	Version	Details
New IPSec ciphers and algorithms	9.13(1)	We added the following IKE and ESP ciphers and algorithms (not configurable): • Ciphers—aes192. Existing ciphers include: aes128, aes256, aes128gcm16. • Pseudo-Random Function (PRF) (IKE only)—prfsha384, prfsha512, prfsha256. Existing PRFs include: prfsha1. • Integrity Algorithms—sha256, sha384, sha512, sha1_160. Existing algorithms incldue: sha1. • Diffie-Hellman Groups—curve25519, ecp256, ecp384, ecp521,modp3072, modp4096. Existing groups include: modp2048.
SSH authentication enhancements	9.13(1)	We added the following SSH server encryption algoritghms: • aes128-gcm@openssh.com • aes256-gcm@openssh.com • chacha20-poly@openssh.com We added the following SSH server key exchange methods: • diffie-hellman-group14-sha256 • curve25519-sha256 • curve25519-sha256@libssh.org • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521 New/Modified commands: **set ssh-server encrypt-algorithm**, **set ssh-server kex-algorithm**
EDCS keys for X.509 Certificates	9.13(1)	You can now use EDCS keys for certificates. Formerly, only RSA keys were supported. New/Modified commands: **set elliptic-curve**, **set keypair-type**

Feature	Version	Details
User password improvements	9.13(1)	We added password security improvements, including the following: • User passwords can be up to 127 characters. The old limit was 80 characters. • Strong password check is enabled by default. • Prompt to set admin password. • Password expiration. • Limit password reuse. • Removed the **set change-during-interval** command, and added a **disabled** option for the **set change-interval**, **set no-change-interval**, and **set history-count** commands. New/Modified commands: **set change-during-interval**, **set expiration-grace-period**, **set expiration-warning-period**, **set history-count**, **set no-change-interval**, **set password**, **set password-expiration**, **set password-reuse-interval**
The **set lacp-mode** command was changed to **set port-channel-mode**	9.10(1)	The **set lacp-mode** command was changed to **set port-channel-mode** to match the command usage in the Firepower 4100/9300. New/Modified commands: **set port-channel-mode**
Support for NTP Authentication on the Firepower 2100	9.10(1)	You can now configure SHA1 NTP server authentication in FXOS. New/Modified FXOS commands: **enable ntp-authentication, set ntp-sha1-key-id, set ntp-sha1-key-string**