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 16.

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 19). 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 21 and Guidelines for User Accounts, on page 19).

- **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 19). 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