Cisco FXOS 2.6 on Firepower 2100 Series

Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration

Version 0.4

December 7, 2020

Prepared by:

Cisco Systems, Inc.,

170 West Tasman Drive, San Jose,

CA 95134-1706 USA

Table of Contents

1 Introduction

The Firepower 2100 is a single-application appliance for the ASA. The Firepower 2100 runs an underlying operating system called the Firepower eXtensible Operating System (FXOS). You must configure basic operating parameters and hardware interface settings in FXOS. These settings include enabling interfaces, establishing EtherChannels, NTP, image management, and more.

This document is a supplement to the Cisco administrative guidance, which is comprised of the installation and administration documents identified in section 1.3. This document supplements those manuals by specifying how to install, configure and operate this product in the Common Criteria evaluated configuration. This document is referred to as the operational user guide in the Firewall collaborative Protection Profile (FWcPP) and meets all the required guidance assurance activities from the FWcPP.

To configure FXOS into its Common Criteria certified configuration, use the FXOS CLI as described in this document. To configure the ASA into its Common Criteria certified configuration, follow the instructions provided in a separate document, "*Cisco Adaptive Security Appliance (ASA) 9.12 on Firepower 2100 Series Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration*."

1.1 Common Criteria (CC) Evaluated Configuration

The following sections describe the scope of evaluation, required configuration, assumptions, and operational environment that the system must be in to ensure a secure deployment. To ensure the system is in the CC evaluated configuration, the users must do the following:

- Configure all the required system settings and default policy as documented in this guide.
- Disable all the features that would violate the cPP requirements or would make the system vulnerable to attacks as documented in this guide.
- Ensure all the environmental assumptions in section 2 are met.
- Ensure that your operational environment is consistent with section 2.
- Follow the guidance in this document.

Scope of Evaluation / Prohibited Features

The list below identifies features or protocols that are not evaluated and must remain disabled. Note that this does not mean the features cannot be used in the evaluated configuration. It means that the features were not evaluated and/or validated by an independent third party and the functional correctness of the implementation is vendor assertion.

The following features and protocols are not evaluated, and are prohibited from use:

- Telnet for management purposes: Telnet passes authentication credentials in clear text and is disabled by default.
- Use of SNMP to access FXOS: Use of SNMP is prohibited by Common Criteria, and is disabled by default.
- FXOS REST API: Allows users to programmatically configure and manage their chassis. The APIs are not evaluated. Access to the REST API is disabled when TLS is disabled.

1.2 References

TOE (Target of Evaluation) References

Table 1: TOE Series and Models

TOE Configuration	Hardware Configurations	Software Version
FP2110 **FP2120** **FP2130** **FP2140**	The Cisco ASA Adaptive Security Appliance on FP2100 provides high-performance firewall and VPN services and 4-12 Gigabit Ethernet interfaces, and support for up to 10,000 VPNs.	ASA release 9.12.3 FXOS release 2.6

Documentation References

The Cisco Firepower System documentation set includes online help and PDF files.

The following product guidance documents are provided online or by request:

Cisco ASA for Firepower 2100 Series Getting Started Guide *https://www.cisco.com/c/en/us/td/docs/security/asa/quick_start/fp2100/asa-2100-gsg.html*
Cisco ASA Upgrade Guide: https://www.cisco.com/c/en/us/td/docs/security/asa/upgrade/asa-upgrade.html, specifically, the section "Upgrade the ASA on the Firepower 2100": https://www.cisco.com/c/en/us/td/docs/security/asa/upgrade/asa-upgrade/asa-appliance-asav.html#topic_ybn_b55_bbb
Cisco FXOS CLI Configuration Guide, 2.6(1), Last Updated: July 2, 2020 *https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos261/cli-guide/b_CLI_ConfigGuide_FXOS_261.html*
Cisco FXOS Firepower Chassis Manager Configuration Guide, 2.6(1), Last Updated: July 2, 2020 *https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos261/web-guide/b_GUI_FXOS_ConfigGuide_261.html*
Cisco Firepower 2100 Series Hardware Installation Guide, June 7, 2020 *https://www.cisco.com/c/en/us/td/docs/security/firepower/2100/hw/guide/b_install_guide_2100.html*
Cisco Adaptive Security Appliance (ASA) 9.12 on Firepower 2100 Series Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration, July 9, 2020
Cisco FXOS 2.6 on Firepower 2100 Series Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration, July 10, 2020 [This Document]

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

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

The most up-to-date versions of the documentation can be accessed on the Cisco Support web site (http://www.cisco.com/c/en/us/support/index.html).

2 Operational Environment

This section describes the components in the environment and assumptions made about the environment.

2.1 Operational Environment Components

The system can be configured to rely on and utilize a number of other components in its operational environment.

- Management Workstation (**Required**) – The system supports Command Line Interface (CLI) and web access and as such an administrator would need a terminal emulator or SSH client (supporting SSHv2) or web browser (supporting HTTPS) to utilize those administrative interfaces.
- Audit server – In the CC-certified configuration, FXOS will send its logging messages to ASA, and ASA will securely transmit those messages to external log servers.
- Certificate Authority (CA) server – The system can be configured to import X.509v3 certificates from a CA, e.g., for TLS connection to syslog server.
- DNS server – The system supports domain name service in the network.

2.2 Environmental Assumptions

The assumptions state the specific conditions that are expected to be met by the operational environment and administrators.

Table 2: Operational Environment Security Measures

Environment Security Objective	Operational Environment Security Objective Definition	Administrator Responsibility
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	Administrators must ensure the system is installed and maintained within a secure physical location. This can include a secured building with key card access or within the physical control of an authorized administrator in a mobile environment.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.	Administrators must not add any general-purpose computing capabilities (e.g., compilers or user applications) to the system.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all guidance documentation in a trusted manner.	Administrators must be properly trained in the usage and proper operation of the system and all the enabled functionality. These administrators must follow the provided guidance.
OE.UPDATES	The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.	Administrators must regularly update the system to address any known vulnerabilities.
OE.ADMIN_CREDENTIALS_ SECURE	The administrator’s credentials (private key) used to access the TOE must be protected on any other platform on which they reside.	Administrators must protect their access credentials where ever they may be.
OE.RESIDUAL_INFORMA TION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on firewall equipment when the equipment is discarded or removed from its operational environment.	Administrators must ensure that there is no unauthorized access to sensitive information on firewall equipment.

3 Before Installation

Before you install your appliance, Cisco highly recommends that the users must consider the following:

- Secure the Cisco FirePOWER 2100 System appliance in a lockable rack within a secure location that prevents access by unauthorized personnel.
- Allow only trained and qualified personnel to install, replace, administer, or service the Cisco appliance.
- Always connect the management interface to a secure internal management network that is protected from unauthorized access.

Audience

This document is written for administrators configuring the Cisco Firepower system 2100. This document assumes you are familiar with networks and network terminology, that you are a trusted individual, and that you are trained to use the Internet and its associated terms and applications.

4 Assurance Activity Configuration

This section has the required guidance and settings as specified in the FWcPP.

NOTE! This interface is called Management 1/1 in the ASA; in FXOS, you might see it 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.

4.1.1 Login to CLI Locally

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

Authenticate to the FXOS CLI using locally defined accounts on the FXOS. The default account is 'admin'.

From the FXOS CLI it is possible to connect to the console interface of the ASA using the command:

```
connect asa
```

4.1.2 Login to CLI Remotely

You can also connect to the FXOS CLI using SSH. The Firepower eXtensible Operating System supports up to eight simultaneous SSH connections. To connect with SSH, you need to know the hostname or IP address of the FXOS chassis.

Use one of the following syntax examples to log in with SSH client:

1) Initiate a SSHv2 connection to the appliance at *hostname*, where hostname corresponds to the host name of the appliance. You can also use the IP address of the appliance.

   ```
   ssh ucs-auth-domain\\username@{ip-address | ipv6-address | hostname}
   ```

   ```
   ssh ucs-example\\jsmith@192.0.20.11
   ```

   ```
   ssh ucs-example\\jsmith@2001::1
   ```

   ```
   ssh {ip-address | ipv6-address | hostname} -l ucs-auth-domain\\username
   ```

   ```
   ssh 192.0.20.11 -l ucs-example\\jsmith
   ```

   ```
   ssh 2001::1 -l ucs-example\\jsmith
   ```

2) Type your password and press `Enter`.

   NOTE! Observe the password is not displayed.

   The standard command prompt appears if the authentication was successful.

   If authentication fails, access will be denied.

Audit Record:

```
Creation Time: 2015-07-09T08:20:17.030
User: internal
Session ID: internal
ID: 3330860
Action: Creation
Description: Fabric A: local user admin logged in from 172.23.33.113
Affected Object: sys/user-ext/sh-login-admin-pts_5_1_15135
Trigger: Session
Modified Properties: id:pts_5_1_15135, name:admin, policyOwner:local
```

4.1.3 Logout

To terminate the FXOS CLI session, type ‘end’ (to confirm you’re at the top level of the CLI), then ‘exit’ (to terminate the session):

```
end

exit
```

4.2 Auditable Events

The appliances that are part of the Cisco FP 2100 System generate an audit record for each user interaction with the web interface, and also record system status messages in the system log. For the CLI, the appliance also generates an audit record for every action executed.

Each appliance generates an audit event for each user interaction with the web interface and CLI command executed. Each event includes at least a timestamp, the user name of the user whose action generated the event, a source IP, and text describing the event. The common fields are described in the table below. The required auditable events are also provided in the table below.

Name	Description
Creation Time	The date and time of the audit event.
User	The type of user.
Session ID and ID	The session ID associated with the session.
Action	The type of action.
Description	More information about the audit event including user, component (if applicable), event type (success or failure), etc. See table below for examples.
Affected Object (if any)	The component that is affected.
Trigger	The user role associated with the user.
Modified Properties (if any)	The system properties that were changed by the event.

Note: When ASA is installed on the Firepower 2100 Series, syslog messages generated by FXOS are internally forwarded to ASA, so ASA is securely transmitting the ASA and FXOS messages to remote syslog servers. Both ASA and FXOS syslog messages appear in the local logging buffer in ASA. There's a small delay between generation of messages by FXOS and internal forwarding of those messages from FXOS to ASA, and the messages received from FXOS by ASA contain the FXOS timestamp when the event occurred, followed by the ASA timestamp when the event was received and rewritten to the ASA log. The format of syslog messages generated by FXOS is different from those generated by ASA; messages generated by FXOS will show two timestamps (one when generated by FXOS, and one when received by ASA), and syslog message from FXOS will be labeled with "%FPRM-6-*", where '*' indicates the source of the FXOS message, such as AUDIT, or EVENT. For a listing of ASA syslog events relevant to the CC-certified configuration, refer to, "*Cisco Adaptive Security Appliance (ASA) 9.12 on Firepower 2100 Series Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration*."

The examples below show formatting differences between messages generated by ASA (the first example) and messages generated by FXOS. Both messages would appear in the ASA logging buffer and both would be transmitted (by ASA) to remote syslog hosts.

Mar 23 09:15:49 <*IP-address-of-ASA*> %ASA-6-605005: Login permitted from *source-address* /*source-port* to *interface:destination* /*service* for user "*username* "

Mar 23 09:36:42 <*IP-address-of-ASA*> %ASA-6-199018: Apr 23 09:36:42 <*hostname-of-FXOS*> FPRM: <<%%FPRM-6-AUDIT>> [session][internal][creation][internal][<*message-sequence-number*>][sys/user-ext/sh-login-admin-ttyS0_1_24059][id:ttyS0_1_24059, name:<*username*>, policyOwner:local][] Fabric A: local user <*username*> logged in from console

Table 3: Auditable Events Certified Under Common Criteria

SFR	Auditable Event	Actual Audited Event
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	See FIA_UAU_EXT.2.
FIA_UAU_EXT.2	All use of the identification and authentication mechanism.	Successful login: %FPRM-6-AUDIT: [session][internal][creation][internal][213524][sys/user-ext/sh-login-admin-ttyS0_1_6336][id:ttyS0_1_6336, name: *USERNAME*, policyOwner:local][] Fabric A: local user *USERNAME* logged in from console Failed login attempt: %AUTHPRIV-3-SYSTEM_MSG: pam_aaa:Authentication failed for user *USERNAME* from console - login
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update	Initiation of the download (initiates image integrity verification): %FPRM-6-EVENT>> [E4195702][228645][transition][admin][] [FSM:BEGIN]: downloading image <*filename*> from <*server*>(FSM:sam:dme:FirmwareDownloaderDownload)#012 %FPRM-6-AUDIT>> [admin][admin][creation][ttyS0_1_5015][228609][sys/fw-catalogue/dnld-<*filename*>][adminState:idle, fileName: <*filename*>, port:0, protocol:scp, pwd:****, remotePath:/FP2k, server:<*servername*>, user:<*username*>][] Downloader <*filename*> created#012 Failure result of validating an update (image integrity verification is automatic during unpacking after download): %FPRM-6-EVENT>> [E4195705][228630][transition][internal][] [FSM:STAGE:FAILED]: unpacking image <*filename*> on primary(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:UnpackLocal)#012 Successful result of validating an update image: %FPRM-6-EVENT>> [E4195706][228703][transition][internal][] [FSM:STAGE:STALE-SUCCESS]: deleting downloadable <*filename*> on local(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:DeleteLocal)#012 %FPRM-6-EVENT>> [E4195874][228707][transition][internal][] [FSM:END]: downloading image <*filename*> from <server>(FSM:sam:dme:FirmwareDownloaderDownload)#012 Initiation of the upgrade (automatically initiates reloading to new image): %FPRM-6-AUDIT>> [admin][admin][modification][ttyS0_1_5015][228721][org-root/fw-infra-pack-default][infraBundleVersion(Old:9.12.3.9, New:9.12.3.12)][] InfraPack default modified. Policy owner is local. Infra bundle version is 9.12.3.12#012

SFR	Auditable Event	Actual Audited Event
FMT_MTD.1/Core Data	All management activities of TSF data.	Configuring the login banner: %FPRM-6-AUDIT: [*USERNAME*][*USERNAME*][creation][pts_0_1_16141][229312][sys/user-ext/pre-login-banner][message:This is a CC test banner , policyOwner:local][] PreLoginBanner created Modification of logging level: %ASA-5-199017: Apr 30 00:55:16 fp2130-upper syslog_utils: Set the system log level to: information#012
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	%FPRM-6-EVENT: [E4197594][213626][transition][internal][] [FSM:STAGE:SKIP]: Request to upgrade software on server 1/1(FSM-STAGE:sam:dme:ComputePhysicalAssociate:updateSspOsSoftware) *IP_ADDRESS* 24/01 14:32:21.966 %FPRM-6-EVENT: [E4195294][315220][transition][internal][] [FSM:STAGE:ASYNC]: unpacking image fxos-k9.2.0.1.135.SPA on primary(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:UnpackLocal) *IP_ADDRESS* 24/01 16:17:34.001 %FPRM-6-EVENT: [E4195293][181179][transition][internal][] [FSM:STAGE:REMOTE-ERROR]: Result: end-point-failed Code: ERR-DNLD-invalid-image Message: invalid image#(sam:dme:FirmwareDownloaderDownload:Local) *IP_ADDRESS* 24/01 14:02:54.555
FPT_STM.1	Changes to the time.	Changing the clock manually: %FPRM-6-AUDIT>> [admin][admin][modification][internal][227669][aaa-log][aaa-log][] switch A: cmd: set clock apr 16 2018 16 25 00 , logged in from console on term /dev/ttyS0: Local mgmt command executed#012 Changing the time zone: %FPRM-6-AUDIT>> [admin][admin][modification][ttyS0_1_5379][227538][sys/svc-ext/datetime-svc][timezone(Old:EST, New:America/New_York)][] Date and Time information modified#012 Creating an NTP server: %FPRM-6-AUDIT>> [admin][admin][creation][pts_0_1_21878][227489][sys/svc-ext/datetime-svc/ntp-<ntp-server-name>][name: <ntp-server-name>][] NTP server <ntp-server-name> created#012 Deleting an NTP server: %FPRM-6-AUDIT>> [admin][admin][deletion][ttyS0_1_5379][227581][sys/svc-ext/datetime-svc/ntp-<ntp-server-name>][sys/svc-ext/datetime-svc/<ntp-server-name>][] NTP server <ntp-server-name> deleted#012 Synchonizing time with an NTP server: %ASA-5-199017: Apr 30 01:47:58 octeon ssp_ntpd[5701]: INFO: ntpd: [HRBLK 7], trigger periodic step sync#012 %ASA-5-199017: Apr 30 01:48:15 octeon ssp_ntpd[5771]: INFO: ASA NOTIFY NTP STEP SYNC SUCCESSFUL, NTFY_CNT:12#012

SFR	Auditable Event	Actual Audited Event
		%ASA-5-771002: CLOCK: System clock set, source: FXOS, IP: 203.0.113.1, before: 01:47:59.939 EDT Mon Apr 30 2018, after: 01:48:00.000 EDT Mon Apr 30 2018
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism	Admin session timeout: %FPRM-6-AUDIT: [session][internal][deletion][internal][1313572][sys/user-ext/user-*USERNAME* /term-ttyS0_1_7995][sys/user-ext/user-admin/term-ttyS0_1_7995][] Fabric A: system terminated session id ttyS0_1_7995 of user *USERNAME* due to idle timeout
FTA_SSL.4	The termination of an interactive session.	Admin session logout: %FPRM-6-AUDIT: [session][internal][deletion][internal][1205445][sys/user-ext/user-*USERNAME* /term-ttys0_1_3038][sys/user-ext/user- *USERNAME* /term-ttys0_1_3038][] Fabric A: user *USERNAME* terminated session id ttyS0_1_3038

4.3 Enable FIPS and CC 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.

Cisco recommends first enabling FIPS mode on the ASA, waiting for the ASA to reload, and then set FIPS mode in FXOS.

Enable FIPS Mode in FXOS:

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

```
scope system
    scope security
```

Step 2 Enable FIPS mode:

```
enable fips-mode
```

Step 3 Commit the configuration:

```
commit-buffer
```

Step 4 Reboot the system:

```
connect local-mgmt
reboot
```

Enable CC-Mode in FXOS

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

```
scope system
    scope security
```

Step 2 Enable Common Criteria mode:

```
enable cc-mode
```

Step 3 Commit the configuration:

```
commit-buffer
```

Step 4 Reboot the system:

```
connect local-mgmt
reboot
```

4.4 Configure Logging

System logging is a method of collecting messages from devices to a server running a syslog daemon. Logging to a central syslog server helps in aggregation of logs and alerts. By default, a syslog service accepts messages and stores them in the local files, or prints them according to a simple configuration file. This form of logging provides protected long-term storage for logs. Logs are useful both in routine troubleshooting and in incident handling. In FXOS on Firepower 2100 Series appliances, log messages generated by FXOS are written to local files within FXOS and copied to the ASA's syslog service for the ASA to securely transmit the messages to a remote syslog server,

Transmission of syslog messages directly from FXOS to a remote syslog host is disabled by default and must remain disabled:

```
scope monitoring
    disable syslog remote-destination
    commit-buffer
```

System logging is enabled by default, and should remain enabled, though the system level can be changed as desired. The messages file is not intended to be viewed via FXOS, all of the messages written to the file are automatically forwarded to the ASA logging buffer, for ASA to transmit to remote syslog servers:

```
scope monitoring
    enable syslog file
    set syslog file level <level> name messages size 4194304
    commit-buffer
```

Configure logging sources and logging level (optional):

```
scope monitoring
    enable syslog source audits
    enable syslog source events
    enable syslog source faults
    set syslog platform level [level]
    commit-buffer
```

Where 'level' is one of these named levels:

emergencies	0
alerts	1
critical	2
errors	3
warnings	4
notifications	5
information	6
debugging	7

Configure logging to console (optional):

```
scope monitoring
    enable syslog console
    set syslog console level [0-7]
    commit-buffer
```

4.5 Management Functions

4.5.1 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.

```
scope eth-uplink
   scope fabric a
      show interface
```

Sample output:

```
Interface:
    Port Name      Port Type          Admin State Oper State       State
Reason
    -------------- ------------------ ----------- ---------------- ----------
--
    Ethernet1/1    Data               Enabled     Up               Up
    Ethernet1/2    Data               Enabled     Link Down        Down
    Ethernet1/3    Data               Disabled    Link Down        Down
    Ethernet1/4    Data               Disabled    Link Down        Down
    Ethernet1/5    Data               Disabled    Link Down        Down
    Ethernet1/6    Data               Disabled    Link Down        Down
    Ethernet1/7    Data               Disabled    Link Down        Down
    Ethernet1/8    Data               Disabled    Link Down        Down
    Ethernet1/9    Data               Disabled    Link Down        Down
    Ethernet1/10   Data               Disabled    Link Down        Down
    Ethernet1/11   Data               Disabled    Link Down        Down
    Ethernet1/12   Data               Disabled    Link Down        Down
    Ethernet1/13   Data               Disabled    Link Down        Down
    Ethernet1/14   Data               Disabled    Link Down        Down
    Ethernet1/15   Data               Disabled    Link Down        Down
    Ethernet1/16   Data               Disabled    Link Down        Down
```

To configure and enable an interface:

```
scope eth-uplink
   scope fabric a
      scope interface 1 3
            set admin-speed speed
            set admin-duplex [fullduplex | halfduplex]
            enable
            commit-buffer
```

4.5.2 Change the FXOS Management IP Address

You can change the management IP address on the Firepower 2100 chassis from the FXOS CLI. The default address is 192.168.45.45. Typically, the FXOS Management 1/1 IP address will be on the same subnet as the ASA Management 1/1 IP address; be sure to also change the ASA IP address on the ASA.

1) Connect to the console port. We recommend that you connect to the console port to avoid losing your connection.
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.

3) Configure an IPv4 management IP address, and optionally the gateway.
    a. Set the scope for fabric-interconnect a.

```
scope fabric-interconnect a
```

    b. View the current management IP address.

```
    show
```

    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.

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
```

    b. View the current management IPv6 address.

```
    show ipv6-if
```

    c. Configure a new management IPv6 address and gateway:

```
    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.

5) (Optional) Reenable the IPv4 DHCP server.

```
scope system
    scope services
        enable dhcp-server start_ip_address end_ip_address
```

6) Save the configuration.

```
        commit-buffer
```

4.5.3 Set the Time

You can set the clock manually. NTP is not supported in the CC-Certified configuration.

To view the clock settings on FXOS:

Step 1 Connect to the FXOS CLI

Step 2 To view the configured time zone:

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

Step 3 To view the configured date and time:

```
Firepower-chassis# show clock
```

To set the time zone on FXOS:

Step 1 Enter system mode:

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

Step 2 Enter system services mode:

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

Step 3 Set the time zone:

```
Firepower-chassis /system/services # set timezone
```

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

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

Step 4 To view the configured time zone:

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

To manually set the time on FXOS:

Step 1 Enter system mode:

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

Step 2 Enter system services mode:

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

Step 3 Configure the system clock:

```
Firepower-chassis /system/services # set clock month day year hour min sec
```

For month, use the first three digits of the month. Hours must be entered using the 24-hour format, where 7pm would be entered as 19.

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

4.5.4 User Management

User accounts are used to access the FXOS of the Firepower 2100 Series appliance. The ASA has separate user accounts and authentication.

About User Accounts

Up to 48 local user accounts can be created, including the default ‘admin’ account. Each account must have a unique username and password.

Account Types

Admin Account

The admin account is a default user account and cannot be modified or deleted. This account is the system administrator 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

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

User Roles

The system contains the following user roles:

Administrator

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

Read-Only

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

Expiration of User Accounts (optional)

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

By default, user accounts do not expire.

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

Guidelines for User Accounts

Usernames

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

- The login ID can contain between 1 and 32 characters, including the following:
    - Any alphabetic character
    - Any digit
    - _ (underscore)
    - -(dash)
    - . (dot)
- The login ID must be unique.
- The login ID must start with an alphabetic character. It cannot start with a number or a special character, such as an underscore.
- The login ID is case-sensitive.
- You cannot create an all-numeric login ID.
- After you create a user account, you cannot change the login ID. You must delete the user account and create a new one.

Passwords

A password is required for each locally authenticated user account. The CC-certification requires that a minimum password be configured. For instructions to set a minimum password length, see the "Configuring Minimum Password Length" section of this document.

In the CC-certified configuration it's optional to 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.

To enable FXOS to require strong passwords:

```
scope security
    set enforce-strong-password yes
```

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 80 characters.
- 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 for local user and admin accounts.

4.5.4.1 Set the Default Authentication Service

In the CC-certified configuration, FXOS on Firepower 2100 Series must be configured to use locally-defined accounts.

```
scope security
    scope default-auth
    set realm local
    commit-buffer
```

4.5.4.2 Creating a Pre-Login Banner

Step 1 Connect to the FXOS CLI
Step 2 Enter security mode:

Firepower-chassis# **scope security**

Step 3 Enter banner security mode:

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

Step 4 Enter the following command to create a pre-login banner:

Firepower-chassis /security/banner # **create pre-login-banner**

Step 5 Specify the message that FXOS should display to the user before they log into Firepower Chassis Manager or the FXOS CLI:

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

Launches a dialog for entering the pre-login banner message text.

Step 6 At the prompt, type a pre-login banner message.

You can enter any standard ASCII character in this field.

You can enter multiple lines of text with each line having up to 192 characters.

Press Enter between lines.

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

Press Ctrl and C to cancel out of the set message dialog.

Step 7 Commit the transaction to the system configuration:

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

The following example creates the pre-login banner:

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

```
Firepower-chassis /security/banner/pre-login-banner #
```

4.5.4.3 Configuring the Session Timeout

In the CC-certified configuration, FXOS must be configured to terminate administrative sessions after a period of inactivity.

Configuring the Session Timeout for the FXOS Console

Step 1 Enter security mode:

Firepower-chassis # **scope security**

Step 2 Enter default authorization security mode:

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

Step 3 (Optional) Set the idle timeout for console sessions:

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

Step 4 (Optional) View the session and absolute session timeout settings:

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

4.5.4.4 Set the Maximum Number of Login Attempts (optional)

In the CC-certified configuration, accounts used for remote administration must be configured to lock after some number of consecutive failed login attempts. For instructions to configure this feature on ASA (not optional), refer to, "*Cisco Adaptive Security Appliance (ASA) 9.12 on Firepower 2100 Series Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration*".

To enable account locking on FXOS (optional):

The *max_login* value must be a non-zero value from 1 through 10.

The *unlock_time* must be a number of seconds from 600-36000.

Set the Maximum Number of Login Attempts

Step 1 From the FXOS CLI, enter security mode:

scope system

scope security

Step 2 Set the maximum number of unsuccessful login attempts.

set max-login-attempts *max_login*

The max_login value is any integer from 0-10.

Step 3 Specify the amount of time (in seconds) the user should remain locked out of the system after reaching the maximum number of login attempts:

set user-account-unlock-time *unlock_time*

Step 4 Commit the configuration:

commit-buffer

4.5.4.5 View and Clear Account Lockout Status

Accounts which have become locked due to consecutive failed login attempts can be unlocked by another administrator prior to the account becoming automatically unlocked after the pre-set 'user-account-unlock-time':

View and Clear User Lockout Status

Step 1 From the FXOS CLI, enter security mode:

scope system

scope security

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

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

Example:

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

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

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

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

4.5.4.6 Configuring Minimum Password Length

In the CC-certified configuration of FXOS of Firepower 2100 Series, the minimum password length must be configured to 8 characters or greater. The configurable lengths are 8-80 characters.

```
scope security
    enable cc-mode
    commit-buffer
```

Note: For cc-mode to be enabled, a reboot is required.

```
connect local-mgmt
reboot
```

Set the minimum password length to a value of 8 or greater:

```
scope security
    set min-password-length [8-80]
```

4.5.4.7 Adding a Local Account

Add local users for FXOS CLI access.

```
scope security
    enter local-user [username]
    enter role [admin | read-only]
    set maxfailedlogins [1-9999]
    set account-status active
    set password
[password]
[password]
    commit-buffer
```

Examples:

```
Firepower /security # enter local-user admin2
Firepower /security/local-user # set password
Enter a password:
Confirm the password:
Error: Password must be minimum 8 characters

Firepower /security/local-user # set password
Enter a password:
Confirm the password:
Error: Password strength check: Password should not contain three consecutive
characters/numbers in any order.

Firepower /security/local-user # set password
Enter a password:
Confirm the password:
Error: Password strength check: Password should contain at least one
uppercase alphabetic character, one lowercase alphabetic character, and one
non-alphanumeric (special) character.

Firepower /security/local-user # set password
Enter a password:
Confirm the password:
Firepower /security/local-user* # commit-buffer
Firepower /security/local-user #
```

4.5.4.8 Deleting a Local Account

```
scope security
    delete local-user [username]
    commit-buffer
```

4.5.4.9 Setting Accounts as Active or Inactive

To deactivate an account:

```
scope security
    enter local-user [username]
    set account-status inactive
    commit-buffer
```

To re-activate an account:

```
scope security
    enter local-user [username]
    set account-status active
    commit-buffer
```

4.5.4.10 Usernames in Audit Messages

When configuring the ASA to audit commands entered by administrators, ensure that actual usernames are written into audit messages instead of generic usernames (such as “enable_15”) by following the following procedures.

Require use of usernames (and passwords) to authentication to all administrative interfaces (serial, ssh, and ASDM) by configuring “aaa authentication” for each type of interface. For more detail, refer to section, “Configure Authentication on the ASA” elsewhere in this document.

```
hostname(config)# aaa authentication serial console {LOCAL | server_group [LOCAL]}
```

```
hostname(config)# aaa authentication ssh console {LOCAL | server_group [LOCAL]}
```

```
hostname(config)# aaa authentication http console {LOCAL | server_group [LOCAL]}
```

Instead of creating an “enable password” for any privilege level, require administrators to re-enter their own password to access the higher privilege level (up to their highest authorized privilege level) using the following command.

```
hostname(config)# aaa authentication enable console {LOCAL | server_group [LOCAL]}
```

4.5.5 Configure SSH and HTTPS Access

The following procedure describes how to enable or disable SSH and HTTPS access to the Firepower chassis.

4.5.5.1 Configure SSH

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

1) Enter system mode:

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

2) Enter system services mode:

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

3) To configure SSH access to the Firepower chassis, do one of the following:

   a. To allow SSH access to the Firepower chassis, enter the following command:

   ```
   Firepower-chassis /system/services # enable ssh-server
   ```

   b. • ***To*** disallow ***SSH access to the Firepower chassis, enter the following command:***

   ```
   Firepower-chassis /system/services # disable ssh-server
   ```

4) Display the SSH settings:

```
Firepower-chassis /system/services # show ssh-sever
```

5) Set the Approved algorithms only:

```
Firepower-chassis /system/services # set ssh-server aes128-cbc aes256-cbc

Firepower-chassis /system/services # set ssh-server mac-algorithm hmac-
sha1 hmac-sha2-256 hmac-sha2-512

Firepower-chassis /system/services # set ssh-server kex-algorithm diffie-
hellman-group14-sha1
```

6) Configure the SSH Rekey limit:

```
Firepower /system/services # set ssh-server rekey-limit volume [KB] time
[Minutes]
```

7) Commit the transaction to the system configuration:

```
Firepower /system/services # commit-buffer
```

4.5.5.2 Configuring HTTPS

IMPORTANT! 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.

1) Enter system mode:

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

2) Enter system services mode:

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

3) Enter the HTTPS service:

```
Firepower-chassis /system/services# enable https
```

4) (Optional) Specify the port to be used for the HTTPS connection:

```
Firepower-chassis /system/services# set https port port-number
```

Specify an integer between 1 and 65535 for *port-number*. HTTPS is enabled on port 443 by default.

5) (Optional) Specify the name of the key ring you created for HTTPS:

```
Firepower-chassis /system/services# set https keyring keyring-name
```

6) (Optional) Specify the level of Cipher Suite security used by the domain:

```
Firepower-chassis /system/services# set https cipher-suite-mode
ciphersuite-mode
```

ciphersuite-mode can be one of the following keywords:

- **high-strength**
- **medium-strength**
- **low-strength**
- **custom** – Specify a user-defined Cipher Suite specification string.

7) (Optional) If **cipher-suite-mode** is set to **custom**, specify a custom level of Cipher Suite security for the domain:

```
Firepower-chassis /system/services# set https cipher-suite cipher-suites
```

cipher-suites 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

In the evaluated configuration, you **MUST** configure the ciphersuites from the Approved ones listed below.

8) Commit the transaction:

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

When CC mode is enabled, the FXOS will restrict the TLS versions to 1.1 and 1.2, and ciphersuites to only the ones allowed below. (*Note: TLSv1.2 supports all the ciphersuites listed. TLSv1.1 only supports the ciphersuites with SHA.*):

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

4.5.6 Software (ASA and FXOS) Installation and Updates

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.

For reference, refer to the Cisco ASA Upgrade Guide, specifically, the section “Upgrade the ASA on the Firepower 2100”. To (optionally) upgrade just ASDM after installing the image bundle, follow the steps from that guide to “Copy the ASDM image to flash memory,” then “Set the ASDM image to use (the one you just uploaded),” then “Save the new settings to the startup configuration.”

The initiate manual update consists of several steps. On the Firepower 2100 Series appliances, updating the ASA image must be performed by upgrading both FXOS and ASA together. The ASA and FXOS images are installed together using a single image ‘bundle’.

Download Images from Cisco.com

1) Using a web browser, navigate to *https://www.cisco.com/c/en/us/support/security/firepower-2100-series/tsd-products-support-series-home.html* or to *https://software.cisco.com/download/navigator.html*.

The software download page for the FXOS chassis is opened in the browser. You must have a Cisco.com account.

2) Find and then download the appropriate software image to your local computer. Search on software.cisco.com for product name “Firepower 2100”.

Copy Platform Bundle Image to the Firepower 2100 Chassis via CLI

1) Connect to the FXOS CLI.
2) Enter firmware mode:

```
Firepower-chassis # scope firmware
```

3) Download the FXOS and ASA software image bundle to the Firepower 2100 Series appliance:

```
Firepower-chassis /firmware # download image URL
```

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

```
ftp:[//[username@]server][/path]
scp:[//[username@]server][/path]
sftp:[//[username@]server][/path]
tftp:[//server][/path]
usbA:/<path>
```

4) To monitor the download process:

```
Firepower-chassis /firmware # show package image_name detail
```

Verifying the Integrity of an Image via CLI

1) Connect to the FXOS CLI.
2) Enter firmware mode:

```
Firepower-chassis# scope firmware
```

3) List images:

```
Firepower-chassis /firmware# show package
```

4) Verify the image:

```
Firepower-chassis /firmware# verify security-pack version version_number
```

5) The system will warn you that verification could take several minutes. Enter **yes**.

6) To check the status of the image verification:

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

Update the Platform Bundle Image via CLI

1) Connect to the FXOS CLI.
2) Enter firmware mode:

```
Firepower-chassis# scope firmware
```

3) Enter auto-install mode:

```
Firepower-chassis /firmware # scope auto-install
```

4) Install the ASA platform bundle:

```
Firepower-chassis /firmware/auto-install # install security-pack version
version_number
```

version_number is the version number of the ASA version you are installing--for example, 9.12.3.12.

5) The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified platform software package.

It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Enter **yes** to confirm that you want to proceed with verification.

6) Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

The Firepower eXtensible Operating System unpacks the bundle and upgrades/reloads the components.

7) To monitor the upgrade process use the “show” or “show detail” commands:

```
scope firmware
   scope auto-install
    show detail
```

As the processes is working the output may look like this:

```
firepower-2110#
Cisco ASA: CMD=-install, CSP-ID=cisco-
asa.9.12.3.12__asa_001_JAD20280ABCXYZZR11, FLAG=''
Verifying signature for cisco-asa.9.12.3.12 ...
Verifying signature for cisco-asa.9.12.3.12 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-
asa.9.12.3.12__asa_001_JAD20280ABCXYZZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
[…]
```

When the verification process completes, the system will reboot and load the new image. The FXOS image will be loaded first, then the ASA image will automatically load.

As the system is booting to the new image, a message like this will appear at the console showing the previous version and new version:

```
Cisco ASA: CMD=-upgrade, CSP-ID=cisco-
asa.9.12.3.12__asa_001_JAD20280ABCXYZZR11, FLAG='cisco-
asa.9.12.3.9__asa_001_JAD20280ABCXYZZR11

Cisco ASA begins upgrade ...
```

As the boot process continues additional output is displayed at the console, such as:

```
Cisco ASA begins upgrade ...

Verifying signature for cisco-asa.9.12.3.12 ...

Verifying signature for cisco-asa.9.12.3.12.... success


Cisco ASA: CMD=-start, CSP-ID=cisco-
asa.9.12.3.12__asa_001_JAD20280ABCXYZZR11, FLAG=''

Cisco ASA starting ...

Registering to process manager ...

Cisco ASA started successfully.
```

Once ASA has loaded, its log will contain messages about the upgrade, such as:

```
FPRM: <<%%FPRM-6-AUDIT>>
[admin][admin][modification][pts_0_1_19442][60631][org-root/fw-infra-pack-
default][infraBundleVersion(Old:9.12.3.9, New:9.12.3.12)][] InfraPack
default modified. Policy owner is local. Infra bundle version is
9.12.3.12#012
```

Verification of Image and Hardware

To verify that the security appliance software and hardware was not tampered with during delivery, perform the following steps:

Step 1: Before unpacking the security appliance, inspect the physical packaging the equipment was delivered in. Verify that the external cardboard packing is printed with the Cisco Systems logo and motifs. If it is not, contact the supplier of the equipment, Cisco Systems or an authorized Cisco distributor/partner.

Step 2: Verify that the packaging has not obviously been opened and resealed by examining the tape that seals the package. If the package appears to have been resealed, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 3: Verify that the box has a white tamper-resistant, tamper-evident Cisco Systems barcoded label applied to the external cardboard box. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This label will include the Cisco product number, serial number, and other information regarding the contents of the box.

Step 4: Note the serial number of the security appliance on the shipping documentation. The serial number displayed on the white label affixed to the outer box will be that of the security appliance. Verify the serial number on the shipping documentation matches the serial number on the separately mailed invoice for the equipment. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 5: Verify that the box was indeed shipped from the expected supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This can be done by verifying with the supplier that they shipped the box with the courier company that delivered the box and that the consignment note number for the shipment matches that used on the delivery. Also verify that the serial numbers of the items shipped match the serial numbers of the items delivered. This verification should be performed by some mechanism that was not involved in the actual equipment delivery, for example, phone/FAX or other online tracking service.

Step 6: Once the security appliance is unpacked, inspect the unit. Verify that the serial number displayed on the unit itself matches the serial number on the shipping documentation and the invoice. Also, verify the hardware received is the correct TOE model. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 7: Download a Common Criteria evaluated software image file from Cisco.com onto a trusted computer system. To access this site, you must be a registered user and you must be logged in. Software images are available from Cisco.com at: https://software.cisco.com

Step 8: Download the appropriate ASA image for the Firepower 2100, such as **`cisco-asa-fp2k.9.12.3.12.SPA`** from Cisco Connection Online (CCO) to a local server or workstation. https://software.cisco.com/download/navigator.html

Optional: Once the file is downloaded, verify that it was not tampered with by using a checksum utility such as “sha512sum” to compute an SHA512 checksum for the downloaded file and compare this with the SHA512 checksum for the image from software.cisco.com. If the checksums do not match, contact Cisco TAC.

Step 9: To copy the image to the Firepower 2100, use the “**`download image`**” command as shown earlier in this document.

Step 10: To properly verify the integrity of the binary image after downloading it to the Firepower 2100, but before installing it, use the “**`verify security-pack`**” command as shown earlier in this document. That command will calculate the checksum of the image and validate its digital signature. To check the progress and outcome of the image validation use the “show validation package” command, which should show output similar to this:

```
firepower-2110 /firmware # show validation package 9.12.3.12
Firmware Package 9.12.3.12:
    Validation Time Stamp: 2018-02-19T19:49:24.017
    Pack Name: cisco-asa-fp2k.9.12.3.12.SPA
    Validation State: Completed
    Overall Status Code: Ok
firepower-2110 /firmware #
```

Step 11: Confirm that your security appliance loads the image correctly and completes internal self-checks. After logging into the CLI, enter the **show version** command to confirm the expected version number has loaded. If the security appliance image fails to load, or if the ASA version is not as expected, contact Cisco TAC.

The following is sample output from the **show version** command output from the FXOS prompt:

```
firepower-2110# show version
Boot Loader version: 1.0.04
System version: 2.2(2.63)
Service Manager version: 2.2(2.63)
firepower-2110#
```

The following is sample output from the **show version** command output from the ASA prompt:

```
asa-fp2110# show version

Cisco Adaptive Security Appliance Software Version 9.12(3)12
Firepower Extensible Operating System Version 2.2(2.63)
Device Manager Version 7.13(1)101
```

4.6 Self-Tests

Cisco products perform a suite of FIPS 140-2 self-tests during power-up and re-boot. If any of the self-test fails, the product will not enter operational state. If this occurs, please re-boot the appliance. If the product still does not enter operational state, please contact Cisco Support (e-mail support@Cisco.com or call us at 1-800-917-4134 or 1-410-423-1901).

The following possible errors that can occur during this self-test are:

- Known Answer Test (KAT) failures
- Zeroization Test failure
- Software integrity failure

When FXOS is booting, the output to the console indicates when FIPS self-tests are being run, and the result of self-testing. Output to the console during boot will include:

```
FIPS POST Test Script

FIPS power-on self-test needed

FIPS power-on self-test running...

SUCCESS: The FIPS power-on self-test has passed
```