Cisco FXOS 2.10 on Firepower 4100 and 9300 Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration

Version 0.3

July 5, 2022

Prepared by:

Cisco Systems, Inc.,

170 West Tasman Drive, San Jose,

CA 95134-1706 USA

Table of Contents

1 Introduction 6
1.1 Common Criteria (CC) Evaluated Configuration 7
1.2 References 8
2 Operational Environment 10
2.1 Operational Environment Components 10
2.2 Environmental Assumptions 11
3 Before Installation 12
4 Assurance Activity Configuration 14
4.1 Logging into the Appliance 14
4.1.1 Log In or Out of the Firepower Chassis Manager 14
4.1.2 Login to CLI Remotely 15
4.1.3 Login to CLI Locally 15
4.1.4 Logout 16
4.2 Auditable Events 17
4.3 Enable FIPS and CC Mode 26
4.3.1 Enable FIPS Mode 26
4.3.2 Enable Common Criteria (CC) Mode 26
4.3.3 Generate the SSH Host Key 27
4.4 Configure Secure Connection with Audit Server and AAA Server 28
4.4.1 Configure Syslog via CLI 28
4.4.2 Configure Syslog via GUI 30
4.4.3 Configure LDAP via CLI 33
4.4.4 Configure RADIUS via CLI 34
4.4.5 Configure TACACS+ via CLI 35
4.4.6 Configure LDAP via GUI 36
4.4.7 Configure RADIUS via GUI 37
4.4.8 Configure TACACS+ via GUI 38
4.4.9 Configure IPsec Secure Channel 39
4.4.10 Configure Static CRL for a Trustpoint 42
4.4.11 Set the LDAP Keyring Certificate 46
4.5 Management Functions 47
4.5.1 IP Management and Pre-Login Banner 47
4.5.1.1 Changing the Management IP Address 47

4.5.1.2 Changing the Application Management IP 48
4.5.1.3 Creating the Pre-Login Banner 49
4.5.2 Image Management 50
4.5.2.1 Download Images from Cisco.com 50
4.5.2.2 Copy Platform Bundle Image to the FXOS Chassis via CLI 50
4.5.2.3 Verifying the Integrity of an Image 51
4.5.2.4 Upload Platform Bundle Image via GUI 51
4.5.2.5 Update the Platform Bundle Image via CLI 51
4.5.2.6 Update the Platform Bundle Image via GUI 52
4.5.2.7 Copy Application Image to FXOS Chassis 52
4.5.2.8 Update Application Image via CLI 53
4.5.2.9 Update Application Image via GUI 53
4.5.3 User and Role Management 54
4.5.4 Selecting the Default Authentication Service via CLI 55
4.5.5 Selecting the Default Authentication Service via GUI 56
4.5.6 Set the Maximum Number of Login Attempts 57
4.5.7 Configure the Minimum Password Length 58
4.5.8 Enable Password Strength Check 58
4.5.9 Create a Local User Account via CLI 59
4.5.10 Create a Local User Account via GUI 60
4.5.11 Delete a Local User Account via CLI 60
4.5.12 Delete a Local User Account via GUI 61
4.5.13 Configure Time Synchronization 62
4.5.13.1 View the Configured Date and Time via CLI 62
4.5.13.2 View the Configured Date and Time via GUI 62
4.5.13.3 Set the Time Zone via CLI 63
4.5.13.4 Set the Time Zone via GUI 63
4.5.13.5 Set the Date and Time Using NTP via CLI 63
4.5.13.6 Set the Date and Time Using NTP via GUI 64
4.5.13.7 Set the Date and Time Manually via CLI 64
4.5.13.8 Set the Date and Time Manually via GUI 64
4.5.14 Configure SSH Access 66
4.5.14.1 Configure SSH via CLI 66
4.5.14.2 Configure SSH via GUI 66
4.5.15 Configure PKI 67

4.5.15.1 Certificates and Trust Points 67
4.5.15.2 Creating a Key Ring 68
4.5.15.3 Creating a Certificate Request for a Key Ring 69
4.5.15.4 Creating a Trust Point 70
4.5.15.5 Importing a Certificate into a Key Ring 70
4.5.15.6 Deleting a Key Ring 71
4.5.15.7 Deleting a Trust Point 71
4.5.15.8 Configuring HTTPS 71
4.5.16 Logical Device Management 73
4.5.16.1 Create a ASA Logical Device via CLI 73
4.5.16.2 Create a ASA Logical Device via GUI 74
4.5.16.3 Delete a ASA Logical Device via CLI 75
4.5.16.4 Delete a ASA Logical Device via GUI 75
4.6 Self-Tests 76

1 Introduction

The Cisco Firepower eXtensible Operating System (FXOS) chassis[1] is a next-generation platform for network and content security solutions. The FXOS chassis is part of the Cisco Application Centric Infrastructure (ACI) Security Solution and provides an agile, open, secure platform that is built for scalability, consistent control, and simplified management.

The FXOS chassis provides the following features:

- Modular chassis-based security system−provides high performance, flexible input/output configurations, and scalability.
- Firepower Chassis Manager−graphical user interface provides streamlined, visual representation of current chassis status and simplified configuration of chassis features.
- FXOS CLI−provides command-based interface for configuring features, monitoring chassis status, and accessing advanced troubleshooting features.

The Cisco firepower (FP) 9300 security appliance is a modular, scalable, carrier-grade appliance that includes the Chassis (including fans and power supply), Supervisor Blade (to manage the security application running on the security module), network module (optional) and security module that contains the security application which in this evaluation is the ASA. The FP4100 Series appliance is a complete standalone, bundle unit that contains everything required above in one appliance. To manage the FP 9300 and 4100 Series appliances, FXOS provides a command-line interface (CLI) and a web GUI known as the firepower chassis manager. The ASA installed on the security module is managed separately and is described in the corresponding document specified in section 1.3.

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 Network Device Collaborative Protection Profile (NDcPP) and meets all the required guidance assurance activities from the NDcPP.

[1] Also known as the Supervisor Blade

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. These 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 Component	Hardware Configurations	Software Version
FP 4110 **FP 4112** **FP 4115** **FP 4120** **FP 4125** **FP 4140** **FP 4145** **FP 4150**	The Firepower 4100 chassis contains the following components: • Network module 1 with eight fixed SFP+ ports (1G and 10G connectivity), the management port, RJ-45 console port, Type A USB port, PID and S/N card, locator indicator, and power switch • Two network modules slots (network module 2 and network module 3) • Two (1+1) redundant power supply module slots • Six fan module slots • Two SSD bays	FXOS release 2.10 and ASA release 9.16

FP 9300	The Firepower 9300 chassis contains the following components:
	• Firepower 9300 Supervisor—Chassis supervisor module
	  ○ Management port
	  ○ RJ-45 console port
	  ○ Type A USB port
	  ○ Eight ports for 1 or 10 Gigabit Ethernet SFPs (fiber and copper)
	• Firepower 9300 Security Module—Up to three security modules
	• 800 GB of solid state storage per security blade (2 x 800 GB solid state drives running RAID1)
	• Firepower Network Module—Two single-wide network modules or one double-wide network module
	• Two power supply modules (AC or DC)
	• Four fan modules
		FXOS release 2.10 and ASA release 9.16

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 Firepower 4100 Getting Started Guide, May 18, 2021 *https://www.cisco.com/c/en/us/td/docs/security/asa/quick_start/fp4100/asa-firepower4100-gsg.html*
Cisco Firepower 9300 Getting Started Guide, May 26, 2021 *https://www.cisco.com/c/en/us/td/docs/security/asa/quick_start/fp9300/asa-firepower9300-gsg.html*
Cisco Firepower 4100/9300 FXOS CLI Configuration Guide, 2.10(1), September 1, 2021 *https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos2101/cli-guide/b_CLI_ConfigGuide_FXOS_2101.html*
Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager Configuration Guide, 2.10(1), September 1, 2021 *https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos2101/web-guide/b_GUI_FXOS_ConfigGuide_2101.html*
Cisco Firepower 4110, 4120, 4140, and 4150 Hardware Installation Guide, September 13, 2021 *https://www.cisco.com/c/en/us/td/docs/security/firepower/4100/hw/guide/b_install_guide_4100.html* *Cisco Firepower 4112, 4115, 4125, and 4145 Hardware Installation Guide, September 16, 2021* *https://www.cisco.com/c/en/us/td/docs/security/firepower/41x5/hw/guide/install-41x5.html*
Cisco Firepower 9300 Hardware Installation Guide, September 13, 2021 *https://www.cisco.com/c/en/us/td/docs/security/firepower/9300/hw/guide/b_install_guide_9300.html*
Cisco Adaptive Security Appliance (ASA) 9.16 on Firepower 4100 and 9300 Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration, October 22, 2021
Cisco FXOS 2.10 on Firepower 4100 and 9300 Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration [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 – The system can be configured to deliver audit records to an external log server.
- Authentication servers – The system can be configured to utilize external authentication 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.
- NTP server – The system can be configured to obtain time from a trusted time source.
- 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_INFORMATION	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 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 4100 and 9300. 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 for the Common Criteria evaluated configuration.

For initial setup instructions for the Firepower 4100 and 9300 appliance, including how to set IP addresses, etc, refer to the "Getting Started" chapter of the *Cisco FXOS Firepower Chassis Manager Configuration Guide*. Before continuing with the steps outlined below, complete the setup steps described in the "Initial Configuration" section of that chapter to change the password, and to configure network settings including the IP address.

4.1 Logging into the Appliance

4.1.1 Log In or Out of the Firepower Chassis Manager

1) To log in to the Firepower Chassis Manager:

   a. Using a supported browser, enter the following URL in the address bar: https://<chassis_mgmt_ip_address>

      where <*chassis_mgmt_ip_address*> is the IP address or host name of the FXOS chassis that you entered during initial configuration.

Supported Web Browser
Mozilla Firefox – Version 42 and later
Google Chrome – Version 47 and later
Microsoft Internet Explorer—Version 11 and later

   b. Enter your username and password.

NOTE! Observe the password is not displayed.

   c. Click **Login**

      The Overview page 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
```

4.1.2 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 Login to CLI Locally

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

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

4.1.4 Logout

To logout from a CLI session (console or SSH):

Ensure that the CLI focus is at the top-level of the CLI (not in a sublevel 'scope', nor in the local-mgmt CLI), then use the "exit" command to terminate the session. If the CLI focus is in the local-mgmt CLI (as indicated by seeing "local-mgmt" in the command prompt, use the "exit" command to return from the local-mgmt CLI to the main FXOS CLI. If the CLI focus is in a sublevel 'scope', use the "end" or "top" command to return to the highest level of the CLI, then use the "exit" command to terminate the session. Note, using the "exit" command while in a CLI sublevel (scope) will move to the next higher level of the CLI, same as using the "up" command.

```
FP9300-A# connect local-mgmt
FP9300-A(local-mgmt)# exit
FP9300-A# scope system
FP9300-A /system # scope security
FP9300-A /security # exit
FP9300-A# scope system
FP9300-A /system # scope services
FP9300-A /system/services # scope web-session-limits
FP9300-A /system/services/web-session-limits # up
FP9300-A /system/services # up
FP9300-A /system # up
FP9300-A# scope system
FP9300-A /system # scope services
FP9300-A /system/services # end
FP9300-A# exit

This is the custom PRE-login-banner for FXOS!
FP9300-A login:
```

To logout from a WebUI session:

1) For web session, point at your username in the navigation bar and then select **Logout**.
2) Close the web browser.

IMPORTANT! For security purpose, always logout as instructed above when you are finished using the management interface. Do NOT rely solely on the inactivity timeout feature.

4.2 Auditable Events

The appliances that are part of the Cisco FP 4100 and 9300 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.

SFR	Auditable Event	Actual Audited Event
FAU_GEN.1	Startup and shutdown events	[2]%FPRM-6-AUDIT: [*USERNAME*][*USERNAME*][modification][web_45842_A][1385040][sys/svc-ext/syslog/client-secondary][adminState(Old:disabled, New:enabled)][] Syslog Remote Destination *IP_ADDRESS* modified %FPRM-6-AUDIT: [*USERNAME*][*USERNAME*][modification][web_42962_A][1383935][sys/svc-ext/syslog/client-primary][adminState(Old:enabled, New:disabled)][] Syslog Remote Destination *IP_ADDRESS* modified
FCS_HTTPS_EXT.1	Failure to establish an HTTPS session.	%AUTHPRIV-5-SYSTEM_MSG: Login failed for user - httpd[10690] %AUTHPRIV-3-SYSTEM_MSG: pam_aaa:Authentication failed from IP_ADDRESS - httpd[10690]
	Successful establishment and termination of an HTTP session.	%USER-7-SYSTEM_MSG: Got user name - httpd[8407] %USER-7-SYSTEM_MSG: remote host: IP_ADDRESS - httpd[8407] %USER-7-SYSTEM_MSG: user [USERNAME] authenticated - httpd[8407] %USER-7-SYSTEM_MSG: result->context->protocol 11 - httpd[8407] %USER-7-SYSTEM_MSG: local/none authentication - httpd[8407] %USER-7-SYSTEM_MSG: set_roles_pam_env_var: Entering, user [USERNAME] - httpd[8407] %USER-7-SYSTEM_MSG: set_roles_pam_env_var: user's roles 3 - httpd[8407] %USER-7-SYSTEM_MSG: set_roles_pam_env_var: role list env var: UCSM_SESSION_ROLES=network-admin read-only [USERNAME] - httpd[8407] %USER-7-SYSTEM_MSG: UCSM_SESSION_ROLES - network-admin read-only [USERNAME] - httpd[8407] %USER-7-SYSTEM_MSG: set_locales_pam_env_var: Entering, user [USERNAME] - httpd[8407] %USER-7-SYSTEM_MSG: user [USERNAME] authenticated - httpd[10690]
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA.	%AUTHPRIV-6-SYSTEM_MSG: 05[IKE] IKE_SA test2[3] established between *IP_ADDRESS* [C=US, ST=CA, O=cisco, OU=STBU, CN=*D_NAME*]...*IP_ADDRESS* [C=US, O=Luo, CN=*D_NAME*] - charon-custom %AUTHPRIV-6-SYSTEM_MSG: 15[IKE] IKE SA key size (128) is less then CHILD SA key size (256), sa strength violation - charon-custom %AUTHPRIV-6-SYSTEM_MSG: 15[IKE] failed to establish CHILD_SA, keeping IKE_SA - charon-custom

[2] Actual date and time are not shown.

SFR	Auditable Event	Actual Audited Event
		2017 Jan 31 10:10:04 mio4-A %AUTHPRIV-6-SYSTEM_MSG: 15[IKE] sending DELETE for ESP CHILD_SA with SPI cd365fb3 - char on-custom %AUTHPRIV-6-SYSTEM_MSG: 13[IKE] received NO_PROPOSAL_CHOSEN notify, no CHILD_SA built - charon-custom
	Session Establishment with peer.	%AUTHPRIV-6-SYSTEM_MSG: 13[IKE] IKE_SA [IKE_SA] established between *IP_ADDRESS [C=US, ST=CA, O=cisco, OU=STBU, CN=D_NAME]...IP_ADDRESS [C=US, O=Luo, CN=D_NAME]* - charon-custom
	Rekey scheduled	%AUTHPRIV-6-SYSTEM_MSG: 05[IKE] scheduling rekeying in 3420s - charon-custom %AUTHPRIV-6-SYSTEM_MSG: 15[IKE] received AUTH_LIFETIME of 9850s, scheduling reauthentication in 8410s - charon-custom
	Rekey successful	%AUTHPRIV-6-SYSTEM_MSG: 10[IKE] IKE_SA gssipsec[2] rekeyed between IP_ADDRESS [C=US, ST=CA, O=cisco, OU=STBU, CN=D_NAME]...IP_ADDRESS [C=US, O=Luo, CN=D_NAME] - charon-custom
	Termination of the trusted channel.	%AUTHPRIV-6-SYSTEM_MSG: 08[IKE] sending DELETE for ESP CHILD_SA with SPI c8ec7f64 - charon-custom
FCS_NTP_EXT.1	Configuration of a new time server	%FPRM-6-AUDIT: [admin][admin][creation][web_21103_A][3766944][sys/svc-ext/datetime-svc/ntp-*IP_ADDRESS*][name:*IP_ADDRESS*, sha1KeyId:0][] NTP server *IP_ADDRESS* created
	Removal of configured time server	%FPRM-6-AUDIT: [admin][admin][deletion][web_21103_A][3766833][sys/svc-ext/datetime-svc/ntp-*IP_ADDRESS*][sys/svc-ext/date time-svc/ntp-*IP_ADDRESS*][] NTP server *IP_ADDRES*S deleted
FCS_SSHS_EXT.1	Failure to establish an SSH session	%AUTHPRIV-3-SYSTEM_MSG: pam_aaa:Authentication failed for user *USERNAME* from *IP_ADDRESS* - sshd[3094]
	Successful SSH Rekey	%DAEMON-7-SYSTEM_MSG: debug1: set_newkeys: rekeying - sshd[29140]
	Establishment of SSH session	%DAEMON-7-SYSTEM_MSG: debug1: userauth-request for user [USERNAME] service ssh-connection method none - sshd[6844] %DAEMON-7-SYSTEM_MSG: debug1: PAM: initializing for "[USERNAME]" - sshd[7348]
	Termination of the trusted channel.	%AUTHPRIV-6-SYSTEM_MSG: pam_unix(sshd:session): session closed for user *USERNAME* – sshd[25700]

SFR	Auditable Event	Actual Audited Event
FCS_TLSS_EXT.1	Failure to establish an TLS Session	%FPRM-6-AUDIT: [session][internal][creation][internal][211634][sys/user-ext/web-login-admin-web_60027_A][id:web_60027_A, name: *USERNAME* policyOwner:local][] Web A: local user *USERNAME* logged in from *IP_ADDRESS* %FPRM-6-AUDIT: [session][internal][deletion][internal][1205449][sys/user-ext/user- *USERNAME* / term-web_27244_A][sys/user-ext/user- *USERNAME* /term-web_27244_A][] Fabric A: user *USERNAME* terminated session id ttyS0_1_3038 %AUTHPRIV-3-SYSTEM_MSG: pam_aaa:Authentication failed for user *USERNAME* from *IP_ADDRESS* - httpd[8515] %AUTHPRIV-5-SYSTEM_MSG: pam_unix(aaa:auth): authentication failure; logname= uid=0 euid=0 tty= ruser= rhost= user= *USERNAME* – aaad %LOCAL0-6-SYSTEM_MSG: authentication failed - httpd[8501] %AUTHPRIV-3-SYSTEM_MSG: pam_aaa:Authentication failed for user *USERNAME* from *IP_ADDRESS* - httpd[8501] %AUTHPRIV-5-SYSTEM_MSG: Login failed for user *USERNAME* - httpd[8501] %USER-6-SYSTEM_MSG: [ssl:info] [pid 8926:tid 1823603600] [client *IP_ADDRESS*:60782] AH02008: SSL library error 1 in handshake (server *IP_ADDRESS*:443) - httpd[8926] %USER-6-SYSTEM_MSG: [ssl:info] [pid 8926:tid 1823603600] SSL Library Error: error:14076129:SSL routines:SSL23_GET_CLIENT_HELLO:only tls allowed in fips mode - httpd[8926] %USER-6-SYSTEM_MSG: [ssl:info] [pid 8926:tid 1823603600] [client *IP_ADDRESS*:60782] AH01998: Connection closed to child 124 with abortive shutdown (server *IP_ADDRESS*:443) - httpd[8926] %USER-6-SYSTEM_MSG: [ssl:info] [pid 8431:tid 1936718656] SSL Library Error: error:1420918C:SSL routines:tls_early_post_process_client_hello:version too low - httpd[8431] %USER-6-SYSTEM_MSG: [ssl:info] [pid 8458:tid 1929345856] SSL Library Error: error:14094416:SSL routines:ssl3_read_bytes:sslv3 alert certificate unknown (SSL alert number 46) - httpd[8458]

SFR	Auditable Event	Actual Audited Event
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	%AUTHPRIV-5-SYSTEM_MSG: pam_tally2(aaa:auth): user <*username*> (2004) tally <*count-of-failed-logins*>, deny <*failed-login-limit-at-which-account-was-locked*> - aaad
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 via console ("ttyS0" = console): %FPRM-6-AUDIT: [session][internal][creation][internal][126610][sys/user-ext/sh-login-*USERNAME*-ttyS0_1_12542][id:ttyS0_1_12542, name:*USERNAME*, policyOwner:local][] Fabric A: local user *USERNAME* logged in from console Failed login via console ("null" = console): %AUTHPRIV-5-SYSTEM_MSG: FAILED LOGIN 1 FROM (null) FOR *USERNAME*, Authentication failure - login Successful login via SSH ("pts" = SSH): %FPRM-6-AUDIT: [session][internal][creation][internal][126614][sys/user-ext/sh-login-*USERNAME*-pts_0_1_13390][id:pts_0_1_13390, name:*USERNAME*, policyOwner:local][] Fabric A: local user *USERNAME* logged in from *IP-ADDRESS* Failed login via SSH: %DAEMON-6-SYSTEM_MSG: Failed none for *USERNAME* from *IP-ADDRESS* port 49224 ssh2 - sshd[13284] Successful login via WebUI ("web" = WebUI): %FPRM-6-AUDIT: [session][internal][creation][internal][126605][sys/user-ext/web-login-*USERNAME*-web_55167_A][id:web_55167_A, name: *USERNAME*, policyOwner:local][] Web A: local user *USERNAME* logged in from *IP-ADDRESS* Failed login via WebUI: %USER-6-SYSTEM_MSG: [ssl:info] [pid 31244:tid 1892854672] [client IP-ADDRESS:58079] AH01964: Connection to child 58 established (server IP-ADDRESS:443) - httpd[31244] %USER-6-SYSTEM_MSG: authentication failed for *USERNAME* - httpd[31244]
FIA_X509_EXT.1	Unsuccessful attempt to validate a certificate	%AUTHPRIV-6-SYSTEM_MSG: 11[IKE] sending end entity cert "C=US, ST=CA, O=Cisco, OU=STBU, CN=*D_NAME*" - charon-custom %AUTHPRIV-6-SYSTEM_MSG: 11[IKE] establishing CHILD_SA test - charon-custom %AUTHPRIV-6-SYSTEM_MSG: 07[IKE] received AUTHENTICATION_FAILED notify error - charon-custom

SFR	Auditable Event	Actual Audited Event
	Add Trust Anchor	%FPRM-6-AUDIT: [admin][admin][creation][pts_0_1_12446][3297308][sys/pki-ext/tp-rootca-rsa][name:*[NAME]*, policyOwner:local][] Trustpoint *[NAME]* created
	Remove Trust Anchor	%FPRM-6-AUDIT: [admin][admin][deletion][pts_0_1_6835][3868135][sys/pki-ext/tp-rootca-rsa][sys/pki-ext/tp-[*NAME]][]* Trustpoint *[NAME]* deleted
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update	%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
FMT_MOF.1/ Services	Starting and stopping of services.	FPRM-6-AUDIT: [*USERNAME*][*USERNAME*][modification][web_45842_A][1385040][sys/svc-ext/syslog/client-secondary][adminState(Old:disabled, New:enabled)][] Syslog Remote Destination *IP_ADDRESS* modified %FPRM-6-AUDIT: [*USERNAME*][*USERNAME*][modification][web_42962_A][1383935][sys/svc-ext/syslog/client-primary][adminState(Old:enabled, New:disabled)][] Syslog Remote Destination *IP_ADDRESS* modified
FMT_MTD.1/CoreData	All management activities of TSF data.	%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 %AUTHPRIV-5-SYSTEM_MSG: *USERNAME* : TTY=ttyS0 ; PWD=/bootflash/sysdebug/coremgmt/sam_dump ; USER=root ; COMMAND=*command* – sudo
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 %FPRM-6-EVENT: [E4195489][3114177][transition][internal][] [FSM:END]: downloading image or file fxos-k9.2.10.1.166.SPA from (FSM:sam:dme:FirmwareDownloaderDownload) %FPRM-6-AUDIT: [admin][admin][modification][pts_1_1_25144][3114439][org-root/fw-infra-pack-

SFR	Auditable Event	Actual Audited Event
		default][forceDeploy(Old:no, New:no), infraBundleVersion(Old:2.10(1.159), New:2.10(1.166))][] InfraPack default modified. Policy owner is local. Infra bundle version is 2.10(1.166)
FPT_STM_EXT.1	Changes to the time.	Manually changing the time zone: %FPRM-6-AUDIT: [admin][admin][modification][pts_0_1_26657][126418][sys/svc-ext/datetime-svc][timezone(Old:America/Los_Angeles, New:America/New_York)][] Date and Time information modified Manually setting the clock: %FPRM-6-AUDIT: [admin][admin][modification][internal][126452][aaa-log][aaa-log][] switch A: cmd: previous time: Sat May 19 17:56:18 EDT 2018 new time: set clock Sat May 19 17:20:00 2018, logged in from <*ip-addr*> on term /dev/pts/0: Local mgmt command executed Manually set an NTP server: %FPRM-6-AUDIT: [admin][admin][creation][pts_0_1_12018][126489][sys/svc-ext/datetime-svc/ntp-<*ntp-hostname*>][name: <*ntp-hostname*>, sha1KeyId:0][] NTP server <*ntp-hostname*> created Clock updated by NTP server: %DAEMON-5-SYSTEM_MSG: NTP clock update from <*ntp-server-ip*>, time before update deab1b54.b1a7909d Sat, May 19 2018 17:53:24.693, time after update deab1bc1.d0d6f9de Sat, May 19 2018 17:55:13.815 - ntpd[13468]
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	%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.3	The termination of a remote session by the session locking mechanism.	Idle timeout termination of SSH session (“pts” = SSH): %FPRM-6-AUDIT: [session][internal][deletion][internal][1204385][sys/user-ext/user- *USERNAME* /term-pts_0_1_12413][sys/user-ext/user- *USERNAME* /term-pts_0_1_12413][] Fabric A: system terminated session id pts_0_1_12413 of user *USERNAME* due to idle timeout Idle timeout termination of WebUI session: %FPRM-6-AUDIT: [session][internal][deletion][internal][1204232][sys/user-ext/remoteuser- *USERNAME* /term-web_16073_A][sys/user-ext/remoteuser- *USERNAME* /term-web_16073_A][] Web A: system terminated Web session id web_16073_A of user *USERNAME* due to idle timeout
FTA_SSL.4	The termination of an interactive session.	Logout from console: %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

SFR	Auditable Event	Actual Audited Event
		Logout from SSH: %FPRM-6-AUDIT: [session][internal][deletion][internal][126619][sys/user-ext/user-*USERNAME*/term-pts_0_1_22214][sys/user-ext/user-*USERNAME*/term-pts_0_1_22214][] Fabric A: user *USERNAME* terminated session id pts_0_1_22214 Logout from WebUI: %FPRM-6-AUDIT: [session][internal][deletion][internal][126606][sys/user-ext/user-*USERNAME*/term-web_55167_A][sys/user-ext/user-*USERNAME*/term-web_55167_A][] Web A: user *USERNAME* terminated session id web_55167_A
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	**IPSec** %AUTHPRIV-6-SYSTEM_MSG: 05[IKE] IKE_SA test2[3] established between *IP_ADDRESS* [C=US, ST=CA, O=cisco, OU=STBU, CN=*D_NAME*]...*IP_ADDRESS* [C=US, O=Luo, CN=*D_NAME*] - charon-custom 2017 Jan 31 10:10:04 mio4-A %AUTHPRIV-6-SYSTEM_MSG: 15[IKE] sending DELETE for ESP CHILD_SA with SPI cd365fb3 - char on-custom %AUTHPRIV-6-SYSTEM_MSG: 15[IKE] failed to establish CHILD_SA, keeping IKE_SA - charon-custom **TLS** %USER-6-SYSTEM_MSG: [ssl:info] [pid 8926:tid 1823603600] [client *IP_ADDRESS*:60782] AH01964: Connection to child 124 established (server *IP_ADDRESS*:443) - httpd[8926] %USER-6-SYSTEM_MSG: [ssl:info] [pid 8926:tid 1823603600] [client *IP_ADDRESS*:60782] AH01998: Connection closed to child 124 with abortive shutdown (server *IP_ADDRESS*:443) - httpd[8926] %USER-6-SYSTEM_MSG: [ssl:info] [pid 8926:tid 1823603600] SSL Library Error: error:14076129:SSL routines:SSL23_GET_CLIENT_HELLO:only tls allowed in fips mode - httpd[8926] %USER-6-SYSTEM_MSG: [ssl:info] [pid 8431:tid 1936718656] SSL Library Error: error:1420918C:SSL routines:tls_early_post_process_client_hello:version too low - httpd[8431]
FTP_TRP.1/Admin	Initiation of the trusted channel.	**SSH**

SFR	Auditable Event	Actual Audited Event
	Termination of the trusted channel. Failures of the trusted path functions.	%FPRM-6-AUDIT: [session][internal][creation][internal][213987][sys/user-ext/sh-login-admin-pts_0_1_4614][id:pts_0_1_4614, name:*USERNAME*, policyOwner:local][] Fabric A: local user *USERNAME* logged in from *IP_ADDRESS* %AUTHPRIV-6-SYSTEM_MSG: pam_unix(sshd:session): session closed for user *USERNAME* – sshd[25700] %AUTHPRIV-3-SYSTEM_MSG: pam_aaa:Authentication failed for user *USERNAME* from *IP_ADDRESS* - sshd[3094] %DAEMON-6-SYSTEM_MSG: input_userauth_request: invalid user temp - sshd[31864] **HTTPS** %FPRM-6-AUDIT: [session][internal][creation][internal][211634][sys/user-ext/web-login-admin-web_60027_A][id:web_60027_A, name: *USERNAME*, policyOwner:local][] Web A: local user *USERNAME* logged in from *IP_ADDRESS* %FPRM-6-AUDIT: [session][internal][deletion][internal][1205449][sys/user-ext/user- *USERNAME* / term-web_27244_A][sys/user-ext/user- *USERNAME* n/term-web_27244_A][] Fabric A: user *USERNAME* terminated session id ttyS0_1_3038 %AUTHPRIV-3-SYSTEM_MSG: pam_aaa:Authentication failed for user *USERNAME* from *IP_ADDRESS* - httpd[8515]

4.3 Enable FIPS and CC Mode

The system by default only supports SSH and HTTPS security protocols for management. Telnet and HTTP are not supported for management and should not be enabled. SNMPv3 is supported but is not permitted for management—only for sending SNMP traps. The system is required to support only the cipher suites, version, and protocols claimed in the Security Target. HTTPS, TLS, and SSH connection settings are configured automatically when CC and FIPS mode are enabled.

4.3.1 Enable FIPS Mode

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

```
scope system
scope security
```

2) Enable FIPS mode:

```
enable fips-mode
```

3) Commit the configuration:

```
commit-buffer
```

4) Reboot the system:

```
connect local-mgmt
reboot
```

IMPORTANT! Prior to FXOS release 2.0.1, the existing SSH host key created during first-time setup of a device was set to 1024 bits. To comply with FIPS and Common Criteria certification requirements, you must destroy this old host key and generate a new one using the procedure detailed in Generate the SSH Host Key (see below). If you performed first-time setup using FXOS 2.0.1 or later, you do not have to generate a new host key.

4.3.2 Enable Common Criteria (CC) Mode

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

```
scope system
scope security
```

2) Enable FIPS mode:

```
enable cc-mode
```

3) Commit the configuration:

```
commit-buffer
```

4) Reboot the system:

```
connect local-mgmt
reboot
```

4.3.3 Generate the SSH Host Key

To delete an existing ssh-server host-key, and create a new one:

1) From the FXOS CLI, enter the services mode:

   scope system

   scope services

2) Delete the SSH Host key:

   delete ssh-server host-key

3) Commit the configuration:

   commit-buffer

4) Set the SSH Host Key size to 2048 bits:

   set ssh-server host-key rsa 2048

5) Commit the configuration:

   commit-buffer

6) Create a new SSH host-key:

   create ssh-server host-key

   commit-buffer

7) Confirm the new Host Key size:

   show ssh-server host-key

   Host Key Size: 2048

Using the “delete ssh-server host-key” command will zeroize (overwrite) the existing key. The “show ssh-server host-key” command can be used to show whether the key has been zeroized (overwritten), which occurs after using the “commit-buffer” command. No further steps are necessary to ensure they keys are destroyed in accordance with CC requirements.

Example:

```
FP9300-A# scope system
FP9300-A /system # scope services
FP9300-A /system/services # delete ssh-server host-key
FP9300-A /system/services* # show ssh-server host-key
Host Key Size: 2048
Deleted: No
FP9300-A /system/services* # commit-buffer
FP9300-A /system/services # show ssh-server host-key
Host Key Size: 2048
Deleted: Yes
FP9300-A /system/services #
```

4.4 Configure Secure Connection with Audit Server and AAA Server

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. The syslog events are set to the local store and syslog server simultaneously, if external syslog server is configured. In the evaluation configuration, syslog traffic must be sent to the syslog server over IPsec.

To view the local syslog messages,

```
Firepower-chassis# connect fxos
Firepower-chassis(fxos)# show logging logfile
```

4.4.1 Configure Syslog via CLI

1) Enter monitoring mode:

```
Firepower-chassis# scope monitoring
```

2) Enable or disable the sending of syslogs to the console:

```
Firepower-chassis /monitoring # {enable | disable} syslog console
```

3) Optional) Select the lowest message level that you want displayed. If syslogs are enabled, the system displays that level and above on the console. The level options are listed in order of decreasing urgency. The default level is Critical.

```
Firepower-chassis /monitoring # set syslog console level {emergencies |
alerts | critical}
```

4) Enable or disable the monitoring of syslog information by the operating system:

```
Firepower-chassis /monitoring # {enable | disable} syslog monitor
```

5) **(**Optional) Select the lowest message level that you want displayed. If the monitor state is enabled, the system displays that level and above. The level options are listed in order of decreasing urgency. The default level is Critical.

```
Firepower-chassis /monitoring # set syslog monitor level {emergencies |
alerts | critical | errors | warnings | notifications | information |
debugging}
```

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

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

```
Firepower-chassis /monitoring # {enable | disable} syslog file
```

7) Specify the name of the file in which the messages are logged. Up to 16 characters are allowed in the file name.

```
Firepower-chassis /monitoring # set syslog file name filename
```

8) (Optional) Select the lowest message level that you want stored to a file. If the file state is enabled, the system stores that level and above in the syslog file. The level options are listed in order of decreasing urgency. The default level is Critical.

```
Firepower-chassis /monitoring # set syslog file level {emergencies |
alerts | critical | errors | warnings | notifications | information |
debugging}
```

9) (Optional) Specify the maximum file size, in bytes, before the system begins to write over the oldest messages with the newest ones. The range is 4096 to 4194304 bytes.

```
Firepower-chassis /monitoring # set syslog file size filesize
```

10) Configure sending of syslog messages to up to three external syslog servers:
    a) Enable or disable the sending of syslog messages to up to three external syslog servers:

```
Firepower-chassis /monitoring # {enable | disable} syslog remote-
destination {server-1  server-2 | server-3}
```

    b) (Optional) Select the lowest message level that you want stored to the external log. If the remote-destination is enabled, the system sends that level and above to the external server. The level options are listed in order of decreasing urgency. The default level is Critical.

```
Firepower-chassis /monitoring # set syslog remote-destination
{server-1 | server-2 | server-3} level{emergencies | alerts |
critical | errors | warnings | notifications | information |
debugging}
```

    c) Specify the hostname or IP address of the specified remote syslog server. Up to 256 characters are allowed in the hostname. In the evaluated configuration, follow the instructions in “Configure IPsec Secure Channel” section to secure the syslog traffic.

```
Firepower-chassis /monitoring # set syslog remote-destination
{server-1 | server-2 | server-3} hostname hostname
```

    d) (Optional) Specify the facility level contained in the syslog messages sent to the specified remote syslog server.

```
Firepower-chassis /monitoring # set syslog remote-destination
{server-1 | server-2 | server-3} facility {local0 | local1 | local2
| local3 | local4 | local5 | local6 | local7}
```

11) Configure the local sources. Enter the following command for each of the local sources you want to enable or disable:

```
Firepower-chassis /monitoring # {enable | disable} syslog source
{audits | events | faults}
```

This can be one of the following:

- **audits**−Enables or disables the logging of all audit log events.
- **events**−Enables or disables the logging of all system events.
- **faults**−Enables or disables the logging of all system faults.

12) Commit the transaction:

```
Firepower-chassis /monitoring # commit-buffer
```

4.4.2 Configure Syslog via GUI

1) Choose **Platform Settings** > **Syslog**.
2) Configure Local Destinations:
   a) Click the **Local Destinations** tab.
   b) On the **Local Destinations** tab, complete the following fields:

Name	Description
Console Section	
Admin State field	Whether the Firepower chassis displays syslog messages on the console. Check the **Enable** check box if you want to have syslog messages displayed on the console as well as added to the log. If the **Enable** check box is unchecked, syslog messages are added to the log but are not displayed on the console.
Level field	If you checked the **Enable** check box for **Console - Admin State**, select the lowest message level that you want displayed on the console. The Firepower chassis displays that level and above on the console. This can be one of the following: • **Emergencies** • **Alerts** • **Critical**
Monitor Section	
Admin State field	Whether the Firepower chassis displays syslog messages on the monitor. Check the **Enable** check box if you want to have syslog messages displayed on the monitor as well as added to the log. If the **Enable** check box is unchecked, syslog messages are added to the log but are not displayed on the monitor.
Level drop-down list	If you checked the **Enable** check box for **Monitor - Admin State**, select the lowest message level that you want displayed on the monitor. The system displays that level and above on the monitor.

	This can be one of the following: • **Emergencies** • **Alerts** • **Critical** • **Errors** • **Warnings** • **Notifications** • **Information** • **Debugging**

c) Click **Save**.

3) Configure Remote Destinations:

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

b) On the **Remote Destinations** tab, complete the following fields for up to three external logs that can store messages generated by the Firepower chassis:

By sending syslog messages to a remote destination, you can archive messages according to the available disk space on the external syslog server.

Name	Description
Admin State field	Check the **Enable** check box if you want to have syslog messages stored in a remote log file.
Level drop-down list	Select the lowest message level that you want the system to store. The system stores that level and above in the remote file. This can be one of the following: • **Emergencies** • **Alerts** • **Critical** • **Errors** • **Warnings** • **Notifications** • **Information** • **Debugging**
Hostname/IP Address field	The hostname or IP address on which the remote log file resides. You must configure a DNS server if you use a hostname rather than an IP address.
Facility drop-down list	Choose a system log facility for syslog servers to use as a basis to file messages. This can be one of the following: • **Local0** • **Local1** • **Local2** • **Local3** • **Local4** • **Local5** • **Local6**

	• **Local7**

c) Click **Save**.

4) Configure Local Sources:
a) Click the **Local Sources** tab.

b) On the **Local Sources** tab, complete the following fields:

Name	Description
Faults Admin State field	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 field	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 field	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**.

The AAA server is a network server that is used for access control. Authentication identifies the user. Authorization implements policies that determine which resources and services an authenticated user may access. Accounting keeps track of time and data resources that are used for billing and analysis. The Firepower chassis maintains a local database that you can populate with user profiles. You can use a local database instead of AAA servers to provide user authentication, authorization, and accounting.

4.4.3 Configure LDAP via CLI

1) Enter security mode:

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

2) Enter security LDAP mode:

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

3) Create an LDAP server instance and enter security LDAP server mode:

   ```
   Firepower-chassis /security/ldap # create server server-name
   ```

   If SSL is enabled, the *server-name* , typically an IP address or FQDN, must exactly match a Common Name (CN) in the LDAP server's security certificate. Unless an IP address is specified, a DNS server must be configured.

4) (Optional) Set an LDAP attribute that stores the values for the user roles and locales:

   ```
   Firepower-chassis /security/ldap/server # set attribute attr-name
   ```

   This property is always a name-value pair. The system queries the user record for the value that matches this attribute name.

   This value is required unless a default attribute has been set for LDAP providers.

5) (Optional) Set the specific distinguished name in the LDAP hierarchy where the server should begin a search when a remote user logs in and the system attempts to get the user's DN based on their username:

   ```
   Firepower-chassis /security/ldap/server # set basedn basedn-name
   ```

   The length of the base DN can be set to a maximum of 255 characters minus the length of CN=username, where username identifies the remote user attempting to access Firepower Chassis Manager or the FXOS CLI using LDAP authentication.

   This value is required unless a default base DN has been set for LDAP providers.

6) (Optional) Set the distinguished name (DN) for an LDAP database account that has read and search permissions for all objects under the base DN:

   ```
   Firepower-chassis /security/ldap/server # set binddn binddn-name
   ```

   The maximum supported string length is 255 ASCII characters.

7) (Optional) Restrict the LDAP search to user names that match the defined filter.

   ```
   Firepower-chassis /security/ldap/server # set filter filter-value
   ```

   This value is required unless a default filter has been set for LDAP providers.

8) Specify the password for the LDAP database account specified for Bind DN:

   ```
   Firepower-chassis /security/ldap/server # set password
   ```

You can enter any standard ASCII characters except for space, § (section sign), ? (question mark), or = (equal sign).

To set the password, press **Enter** after typing the **set password** command and enter the key value at the prompt.

9) (Optional) Specify the order in which the Firepower eXtensible Operating System uses this provider to authenticate users:

```
Firepower-chassis /security/ldap/server # set order order-num
```

10) (Optional) Specify the port used to communicate with the LDAP server. The standard port number is 389.

```
Firepower-chassis /security/ldap/server # set port port-num
```

11) Enable or disable the use of encryption when communicating with the LDAP server:

```
Firepower-chassis /security/ldap/server # set ssl {yes | no}
```

The options are as follows:

· **yes** −Encryption is required. If encryption cannot be negotiated, the connection fails.

· **no** −Encryption is disabled. Authentication information is sent as clear text.

LDAP uses STARTTLS. This allows encrypted communication using port 389.

NOTE: In the evaluated configuration, LDAP must be tunneled over IPsec.

12) Specify the length of time in seconds the system should spend trying to contact the LDAP database before it times out:

```
Firepower-chassis /security/ldap/server # set timeout timeout-num
```

Enter an integer from 1 to 60 seconds, or enter 0 (zero) to use the global timeout value specified for LDA providers. The default is 30 seconds.

13) Specify the vendor that is providing the LDAP provider or server details:

```
Firepower-chassis /security/ldap/server # set vendor {ms-ad | openldap}
```

The options are as follows:

· **ms-ad**−LDAP provider is Microsoft Active Directory

· **openldap**−LDAP provider is not Microsoft Active Directory

14) Commit the transaction to the system configuration:

```
Firepower-chassis /security/ldap/server # commit-buffer
```

4.4.4 Configure RADIUS via CLI

1) Enter security mode:

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

2) Enter security RADIUS mode:

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

3) Create a RADIUS server instance and enter security RADIUS server mode:

```
Firepower-chassis /security/radius # create server server-name
```

4) (Optional) Specify the port used to communicate with the RADIUS server.

```
Firepower-chassis /security/radius/server # set authport authport-num
```

5) Set the RADIUS server key:

```
Firepower-chassis /security/radius/server # set key
```

To set the key value, press **Enter** after typing the **set key** command and enter the key value at the prompt.

6) (Optional) Specify when in the order this server will be tried:

```
Firepower-chassis /security/radius/server # set order order-num
```

7) (Optional) Set the number of times to retry communicating with the RADIUS server before noting the server as down:

```
Firepower-chassis /security/radius/server # set retries retry-num
```

8) Specify the time interval that the system should wait for a response from the RADIUS server before noting the server as down:

```
Firepower-chassis /security/radius/server # set timeout seconds
```

9) Commit the transaction to the system configuration:

```
Firepower-chassis /security/radius/server # commit-buffer
```

4.4.5 Configure TACACS+ via CLI

1) Enter security mode:

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

2) Enter security TACACS+ mode:

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

3) Create a TACACS+ server instance and enter security TACACS+ server mode:

```
Firepower-chassis /security/tacacs # create server server-name
```

4) Specify the TACACS+ server key:

```
Firepower-chassis /security/tacacs/server # set key
```

To set the key value, press **Enter** after typing the **set key** command and enter the key value at the prompt.

5) (Optional) Specify when in the order this server will be tried:

```
Firepower-chassis /security/tacacs/server # set order order-num
```

6) Specify the time interval that the system should wait for a response from the TACACS+ server before noting the server as down:

```
Firepower-chassis /security/tacacs/server # set timeout seconds
```

7) (Optional) Specify the port used to communicate with the TACACS+ server:

```
Firepower-chassis /security/tacacs/server # set port port-num
```

8) Commit the transaction to the system configuration:

```
Firepower-chassis /security/tacacs/server # commit-buffer
```

4.4.6 Configure LDAP via GUI

1) Choose **Platform Settings** > **AAA**.
2) Click the **LDAP** tab.
3) For each LDAP provider that you want to add:
   a) In the **LDAP Providers** area, click **Add**.
   b) In the **Add LDAP Provider** dialog box, complete the following fields:

Name	Description
Hostname/FDQN (or IP Address) field	The hostname or IP address on which the LDAP provider resides. If SSL is enabled, this field must exactly match a Common Name (CN) in the security certificate of the LDAP database.
Order field	The order in which the Firepower eXtensible Operating System uses this provider to authenticate users. Enter an integer between 1 and 16, or enter lowest-available or 0 (zero) if you want the Firepower eXtensible Operating System to assign the next available order based on the other providers defined in Firepower Chassis Manager or the FXOS CLI.
Bind DN field	The distinguished name (DN) for an LDAP database account that has read and search permissions for all objects under the base DN. The maximum supported string length is 255 ASCII characters.
Base DN field	The specific distinguished name in the LDAP hierarchy where the server should begin a search when a remote user logs in and the system attempts to get the user's DN based on their username. The length of the base DN can be set to a maximum of 255 characters minus the length of CN=$userid, where $userid identifies the remote user attempting to access Firepower Chassis Manager or the FXOS CLI using LDAP authentication. This value is required unless a default base DN has been set on the **LDAP** tab.
Port field	The port through which Firepower Chassis Manager or the FXOS CLI communicates with the LDAP database. The standard port number is 389.
Enable SSL check box	If checked, encryption is required for communications with the LDAP database. If unchecked, authentication information will be sent as clear text. LDAP uses STARTTLS. This allows encrypted communication using port 389.
Filter field	The LDAP search is restricted to those user names that match the defined filter.

	This value is required unless a default filter has been set on the **LDAP** tab.
Attribute field	An LDAP attribute that stores the values for the user roles and locales. This property is always a name-value pair. The system queries the user record for the value that matches this attribute name. This value is required unless a default attribute has been set on the **LDAP** tab.
Key field	The password for the LDAP database account specified in the **Bind DN** field. You can enter any standard ASCII characters except for space, § (section sign), ? (question mark), or = (equal sign).
Confirm Key field	The LDAP database password repeated for confirmation purposes.
Timeout field	The length of time in seconds the system should spend trying to contact the LDAP database before it times out. Enter an integer from 1 to 60 seconds, or enter 0 (zero) to use the global timeout value specified on the **LDAP** tab. The default is 30 seconds.
Vendor field	This selection identifies the vendor that is providing the LDAP provider or server details: • If the LDAP provider is Microsoft Active Directory, select **MS AD**. • If the LDAP provider is not Microsoft Active Directory, select **Open LDAP**. The default is Open LDAP.

c) Click **OK** to close the **Add LDAP Provider** dialog box.

4) Click **Save**.

4.4.7 Configure RADIUS via GUI

1) Choose **Platform Settings** > **AAA**.
2) Click the **RADIUS** tab.
3) For each RADIUS provider that you want to add:
   a) In the **RADIUS Providers** area, click **Add**.
   b) In the **Add RADIUS Provider** dialog box, complete the following fields:

Name	Description
Hostname/FDQN (or IP Address) field	The hostname or IP address on which the RADIUS provider resides.
Order field	The order in which the Firepower eXtensible Operating System uses this provider to authenticate users.

	Enter an integer between 1 and 16, or enter lowest-available or 0 (zero) if you want the Firepower eXtensible Operating System to assign the next available order based on the other providers defined in Firepower Chassis Manager or the FXOS CLI.
Key field	The SSL encryption key for the database.
Confirm Key field	The SSL encryption key repeated for confirmation purposes.
Authorization Port field	The port through which Firepower Chassis Manager or the FXOS CLI communicates with the RADIUS database. The valid range is 1 to 65535. The standard port number is 1700.
Timeout field	The length of time in seconds the system should spend trying to contact the RADIUS database before it times out. Enter an integer from 1 to 60 seconds, or enter 0 (zero) to use the global timeout value specified on the **RADIUS** tab. The default is 5 seconds.
Retries field	The number of times to retry the connection before the request is considered to have failed. If desired, enter an integer between 0 and 5. If you do not specify a value, Firepower Chassis Manager uses the value specified on the **RADIUS** tab.

c) Click **OK** to close the **Add RADIUS Provider** dialog box.

4) Click **Save**.

4.4.8 Configure TACACS+ via GUI

1) Choose **Platform Settings** > **AAA**.
2) Click the **TACACS** tab.
3) For each TACACS provider that you want to add:
   a) In the **TACACS Providers** area, click **Add**.
   b) In the **Add TACACS Provider** dialog box, complete the following fields:

Name	Description
Hostname/FDQN (or IP Address) field	The hostname or IP address on which the TACACS+ provider resides.
Order field	The order in which the Firepower eXtensible Operating System uses this provider to authenticate users. Enter an integer between 1 and 16, or enter lowest-available or 0 (zero) if you want the Firepower eXtensible Operating System to assign the next available order based on the other providers defined in Firepower Chassis Manager or the FXOS CLI.
Key field	The SSL encryption key for the database.
Confirm Key field	The SSL encryption key repeated for confirmation purposes.

Port field	The port through which Firepower Chassis Manager or the FXOS CLI communicates with the TACACS+ database. Enter an integer between 1 and 65535. The default port is 49.
Timeout field	The length of time in seconds the system should spend trying to contact the TACACS+ database before it times out. Enter an integer from 1 to 60 seconds, or enter 0 (zero) to use the global timeout value specified on the **TACACS+** tab. The default is 5 seconds.

c) Click **OK** to close the **Add TACACS+ Provider** dialog box.

4) Click **Save**.

4.4.9 Configure IPsec Secure Channel

Configure IPsec on FXOS to provide end-to-end data encryption and authentication service on data packets going through the public network. In the Common Criteria certified configuration, FXOS syslog traffic must be sent over IPsec as configured below. In addition, communication with NTP server and the following AAA protocols must also be protected using IPsec: LDAP, TACACS and RADIUS.

To ensure syslog and AAA traffic from FXOS is secured in IPsec, ensure the IP addresses of those remote servers are included in the "set remote-addr" or "set remote-subnet" commands described below, which makes them part of the Security Policy Database (SPD), which is also described below. For more comprehensive guidance, refer to the "Configure IPSec Secure Channel" section of the "Security Certifications Compliance" chapter of the *Cisco FXOS CLI Configuration Guide*.

Note: On the Firepower 4100 and 9300 platforms, ASA and FXOS generate separate syslog messages and each transmit their messages separately to remote syslog servers over their own secure channels, which do not interfere with each other. FXOS will always secure syslog in IPsec, while ASA can be configured to transmit syslog via TLS, or IPsec or both (TLS over IPsec).

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

```
scope system
scope security
```

2) Enter the IPSec mode:

```
scope ipsec
```

3) Set the log verbose level:

```
set log-level log_level
```

4) Create or enter an IPSec connection:

```
enter connection connection_name
```

5) Set IPSec mode to tunnel or transport:

```
set mode tunnel_or_transport
```

6) Set local IP address:

```
set local-addr ip_address
```

7) Set remote IP address:

set remote-addr *ip_address*

8) If using tunnel mode, set remote subnet:

set remote-subnet *ip/mask*

9) (Optional) Set remote identity:

set remote-ike-ident *remote_identity_name*

10) Set keyring name:

set keyring-name *name*

11) (Optional) Set keyring password:

set keyring-passwd *passphrase*

12) (Optional) Set IKE-SA lifetime in minutes:

set ike-rekey-time *minutes*

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

13) (Optional) Set Child SA lifetime in minutes (30-480):

set esp-rekey-time *minutes*

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

14) (Optional) Set the number of retransmission sequences to perform during initial connect:

set keyringtries *retry_number*

The *retry_number* value can be any integer between 1-5, inclusive.

15) (Optional) Enable or disable the certificate revocation list check:

set revoke-policy [*relaxed* **|** *strict***]**

16) Enable the connection:

set admin-state enable

17) Reload all connections:

reload-conns

18) (Optional) Add existing trustpoint name to IPsec:

create authority *trustpoint_name*

19) Configure the enforcement of matching cryptographic key strength between IKE and SA connections:

set sa-strength-enforcement [*yes* **|** *no***]**

If SA enforcement is enabled (*yes*)	When IKE negotiated key size is less then ESP negotiated key size, the connection fails. When IKE negotiated key size is larger or equal to the ESP negotiated key size, SA enforcement check passes and the connection is successful.
If SA enforcement is disabled (*no*)	SA enforcement check automatically passes and the connection is successful.

When CC mode is enabled, FXOS supports the following:

- **IKE version***: version 2
    - NAT traversal for ESP packets to pass through one or more NAT devices, is enabled by default.
- **IPsec Mode**: tunnel, transport
    - set mode {tunnel |transport}
- **IKEv2 Mode***: main mode
- **IKEv2 Ciphers***:
    - **Encryption algorithms**: AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128
    - **Integrity algorithms**: HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512. Additionally, FXOS supports HMAC-SHA1-96, a truncated version of HMAC-SHA-1.
    - **DH Groups**: 14, 19 and 20
- **ESP Ciphers***:
    - **Encryption algorithms:** AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128
    - **Integrity algorithms:** HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512. Additionally, FXOS supports HMAC-SHA1-96, a truncated version of HMAC-SHA-1.
- **Authentication**: X.509v3 certificates
    - create authority *trustpoint_name*
- **Traffic Selector**: remote host or subnet
    - set local-addr *ip_address*
    - set remote-addr *ip_address*
    - set remote-subnet *ip/mask*
    - set remote-ike-ident *remote_identity_name*
- **IKE SA Life Time:** Configurable up to 24 hours. Only time is supported.
    - set ike-rekey-time *minutes*
- **IKE Child SA Life Time:** Configurable up to 8 hours. Only time is supported.
    - set esp-rekey-time *minutes*

`* Not configurable`

Note: In CC mode, the FXOS expects an ESP cipher without a DH group for the initial IKE exchange, and an ESP cipher with a DH group for an ESP rekey. For an ESP rekey to be successful, the peer must be configured to use BOTH an ESP cipher with and without an associated DH group. Example: "aes128-sha1, aes128-sha1-modp2048"

Security Policy Database (SPD)

In FXOS, the SPDs are pretty simple because FXOS is not operating as a VPN gateway, and the SPDs are just based on IP addresses, so the type of traffic being tunneled (syslog, LDAP, etc.) is irrelevant to the tunneling decisions.

- The local-addr is the local management IP.
- The remote-addr is the IP of the IPsec peer (in tunnel mode or transport mode).
- A remote-subnet is applicable only in tunnel mode, and defines the subnet that would be reachable beyond the remote-addr.
- Outbound traffic will be **encrypted** when the source address is local-addr, ***and***:
    - the destination address is the remote-addr (in tunnel or transport mode); ***or***
    - the destination address is on the remote-subnet (in tunnel mode).
- Outbound traffic will **bypass** the tunnel if:
    - the destination address is ***not*** the remote-addr; ***and***
    - the destination address is ***not*** on the remote-subnet.
- Inbound traffic will be **dropped** if:
    - the source address (prior to decryption) is on the remote-subnet (in tunnel mode); ***or***
    - the source address is the remote-address, ***and*** the packets are ***not*** IKE or ESP.

4.4.10 Configure Static CRL for a Trustpoint

Revoked certificates are maintained in the Certificate Revocation List (CRL). Use the following procedure to configure your FXOS chassis to validate peer certificates using CRL information.

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

   `scope system`

   `scope security`

2) Enter the trustpoint mode:

   `scope trustpoint` *`trustname`*

3) Enter the revoke mode:

   `scope revoke`

4) Download the CRL file(s):

   `import crl` *`protocol://user_id@CA_or_CRL_issuer_IP`*`/tmp/`*`DoDCA1CRL1.crl`*

5) (Optional) Show status for import process of CRL information:

   `show import-task detail`

6) Set the certificate revocation method to CRL-only:

   `set certrevokemethod {crl}`

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

Dynamic (non-static) CRL information is harvested from the CDP information of an X.509 certificate, and indicates dynamic CRL information. Static CRL information is downloaded by system administration manually, and indicates local CRL information in the FXOS system. The dynamic CRL information is only processed against the current processing certificate in the certificate chain. The static CRL is applied to the whole peer certificate chain.

For steps to enable or disable certificate revocation checks for your secure LDAP and IPSec connections, see Configure IPSec Secure Channel and Creating an LDAP Provider.

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

Table 3 Certificate Revocation Check Mode set to Strict without a local static CRL

Without local static CRL	**LDAP Connection**	**IPSec Connection**
Checking peer's certificate chain	Full certificate chain is required	Full certificate chain is required
Checking CDP in peer's certificate chain	Full certificate chain is required	Full certificate chain is required
CDP checking for Root CA certificate of the peer's certificate chain	Yes	Not applicable
Any certificate validation failure in the peer's certificate chain	Connection fails with syslog message	Connection fails with syslog message
Any certificate revoked in the peer's certificate chain	Connection fails with syslog message	Connection fails with syslog message
One CDP is missing in the peer's certificate chain	Connection fails with syslog message	Peer certificate: connection fails with syslog message Intermediate CAs: connection succeeds
One CDP CRL is empty in the peer's certificate chain with valid signature	Connection fails with syslog message	Connection succeeds
Any CDP in the peer's certificate chain cannot be downloaded	Connection fails with syslog message	Peer certificate: Connection fails with syslog message Intermediate CAs: connection succeeds
Certificate has CDP, but the CDP server is down	Connection fails with syslog message	Peer certificate: Connection fails with syslog message Intermediate CAs: connection succeeds

Certificate has CDP, server is up, and CRL is on CDP, but the CRL has an invalid signature	Connection fails with syslog message	Peer certificate: Connection fails with syslog message Intermediate CAs: connection succeeds

Table 4 Certificate Revocation Check Mode set to Strict with a local static CRL

With local static CRL	LDAP Connection	IPSec Connection
Checking peer certificate chain	Full certificate chain is required	Full certificate chain is required
Checking CDP in peer certificate chain	Full certificate chain is required	Full certificate chain is required
CDP checking for Root CA certificate of the peer certificate chain	Yes	Not applicable
Any certificate validation failure in the peer certificate chain	Connection fails with syslog message	Connection fails with syslog message
Any certificate revoked in the peer certificate chain	Connection fails with syslog message	Connection fails with syslog message
One CDP is missing the peer certificate chain	Connection succeeds	Connection succeeds
One CDP CRL is empty in the peer certificate chain with valid signature	Connection succeeds	Connection succeeds
Any CDP in the peer certificate chain cannot be downloaded	Connection succeeds	Connection succeeds
Certificate has CDP, but the CDP server is down	Connection succeeds	Connection succeeds
Certificate has CDP, server is up, and CRL is on CDP, but the CRL has an invalid signature	Connection succeeds	Connection succeeds

Table 5 Certificate Revocation Check Mode set to Relaxed without a local static CRL

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

Any certificate validation failure in the peer certificate chain	Connection fails with syslog message	Connection fails with syslog message
Any certificate revoked in the peer certificate chain	Connection fails with syslog message	Connection fails with syslog message
One CDP is missing the peer certificate chain	Connection succeeds	Connection succeeds
One CDP CRL is empty in the peer certificate chain with valid signature	Connection succeeds	Connection succeeds
Any CDP in the peer certificate chain cannot be downloaded	Connection succeeds	Connection succeeds
Certificate has CDP, but the CDP server is down	Connection succeeds	Connection succeeds
Certificate has CDP, server is up, and CRL is on CDP, but the CRL has an invalid signature	Connection succeeds	Connection succeeds

Table 6 Certificate Revocation Check Mode set to Relaxed with a local static CRL

With local static CRL	**LDAP Connection**	**IPSec Connection**
Checking peer certificate chain	Full certificate chain	Full certificate chain
Checking CDP in peer certificate chain	Full certificate chain	Full certificate chain
CDP checking for Root CA certificate of the peer certificate chain	Yes	Not applicable
Any certificate validation failure in the peer certificate chain	Connection fails with syslog message	Connection fails with syslog message
Any certificate revoked in the peer certificate chain	Connection fails with syslog message	Connection fails with syslog message
One CDP is missing the peer certificate chain	Connection succeeds	Connection succeeds
One CDP CRL is empty in the peer certificate chain with valid signature	Connection succeeds	Connection succeeds
Any CDP in the peer certificate chain cannot be downloaded	Connection succeeds	Connection succeeds
Certificate has CDP, but the CDP server is down	Connection succeeds	Connection succeeds

Certificate has CDP, server is up, and CRL is on CDP, but the CRL has an invalid signature	Connection succeeds	Connection succeeds

4.4.11 Set the LDAP Keyring Certificate

Use the following procedure to set a secure LDAP client keyring certificate in order to support a TLS connection on your FXOS chassis.

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

   `scope system`

   `scope security`

2) Enter the LDAP mode:

   `scope ldap`

3) Enter the LDAP server:

   `enter server` *`server_ip`*

4) Set the LDAP keyring:

   `set keyring` *`keyring_name`*

5) Commit the configuration:

   `commit buffer`

The administrator is responsible for maintaining the connection between the system and audit/AAA server. If the connection is unintentionally broken, the administrator should perform the following steps to diagnose and fix the problem:

- Check the physical network cables.
- Check that the audit or AAA server is still running.
- Reconfigure the audit or AAA server settings.
- If all else fail, reboot the system and audit or AAA server.

4.5 Management Functions

4.5.1 IP Management and Pre-Login Banner

4.5.1.1 Changing the Management IP Address

You can change the management IP address on the FXOS chassis from the FXOS CLI.

1) Connect to the FXOS CLI.
2) To configure an IPv4 management IP address:
   a) Set the scope for fabric-interconnect a:

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

   b) To view the current management IP address, enter the following command:

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

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

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

   d) Commit the transaction to the system configuration:

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

3) To configure an IPv6 management IP address:
   a) Set the scope for fabric-interconnect a:

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

   b) Set the scope for management IPv6 configuration:

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

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

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

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

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

e) Commit the transaction to the system configuration:

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

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

4.5.1.2 Changing the Application Management IP

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

1) Connect to the FXOS CLI.
2) Scope the security module:

```
scope slot slot_number
```

3) Configure the new management bootstrap parameters.

```
set virtual ip ip_address mask network_mask gateway gateway_ip_address
For clustered configuration:
set virtual ip ip_address pool start_ip end_ip mask network_mask gateway
gateway_ip_address
```

4) Scope the application.

```
scope app-instance asa_or_ftd
```

5) Clear the management bootstrap information.

```
clear mgmt-bootstrap
```

6) Exit management bootstrap configuration scope.

```
Exit
```

7) Commit the configuration:

```
commit-buffer
```

8) Connect to the console of the security module.
9) Change the virtual IP, mask, and gateway values to the exact values used in step 3.

```
set virtual ip ip_address netmask network_mask gw gateway_ip_address
For clustered configuration:
set virtual ipv ip_address pool start_ip end_ip mask network_mask gateway
gateway_ip_address
```

10) Commit the configuration:

```
commit-buffer
```

4.5.1.3 Creating the Pre-Login Banner

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

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

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

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

3) Enter banner security mode:

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

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

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

   To modify existing login banner, use **scope** instead of **create**.
   To delete existing login banner, use **delete** instead of **create**.

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.
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.
7) Commit the transaction to the system configuration:

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

4.5.2 Image Management

The FXOS chassis uses two basic types of images:

- Platform Bundle—The Firepower platform bundle is a collection of multiple independent images that operate on the Firepower Supervisor and Firepower security module/engine. The platform bundle is a Firepower eXtensible Operating System software package.

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

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

WARNING! All images are digitally signed and validated through Secure Boot. Do not modify the image in any way or you will receive a validation error.

4.5.2.1 Download Images from Cisco.com

Using a web browser, navigate to http://www.cisco.com/go/firepower9300-software or http://www.cisco.com/go/firepower4100-software

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

Find and then download the appropriate software image to your local computer.

4.5.2.2 Copy Platform Bundle Image to the FXOS Chassis via CLI

Step 1 Enter firmware mode:

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

Download the FXOS software image:

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

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

- ftp:// username@hostname / path
- scp:// username@hostname / path
- sftp:// username@hostname / path

To monitor the download process:

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

4.5.2.3 Verifying the Integrity of an Image

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 platform-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
```

4.5.2.4 Upload Platform Bundle Image via GUI

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

1) Choose **System** > **Updates**.

   The Available Updates page shows a list of the Firepower eXtensible Operating System platform bundle images and application images that are available on the chassis.

2) Click **Upload Image** to open the Upload Image dialog box.
3) Click **Browse** to navigate to and select the image that you want to upload.
4) Click **Upload**.

   The selected image is uploaded to the FXOS chassis.

5) For certain software images you will be presented with an end-user license agreement after uploading the image. Follow the system prompts to accept the end-user license agreement.

4.5.2.5 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 FXOS platform bundle:

```
Firepower-chassis /firmware/auto-install # install platform platform-vers version_number
```

   version_number is the version number of the FXOS platform bundle you are installing--for example, 1.1(2.51).

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

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

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

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:

   a) Enter **`scope firmware.`**

   b) Enter **`scope auto-install.`**

   c) Enter **`show fsm status expand.`**

4.5.2.6 Update the Platform Bundle Image via GUI

1) Choose **System** > **Updates**.

   The Available Updates page shows a list of the Firepower eXtensible Operating System platform bundle images and application images that are available on the chassis.

2) Click **Upgrade** for the FXOS platform bundle to which you want to upgrade.

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

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

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

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

4.5.2.7 Copy Application Image to FXOS Chassis

1) Enter Security Services mode:

   ```
   Firepower-chassis# scope ssa
   ```

2) Enter Application Software mode:

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

3) Download the logical device software image:

   ```
   Firepower-chassis /ssa/app-software# download image URL
   ```

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

   · **ftp**://*username@hostname*/*path*

- **scp**://*username@hostname/path*
- **sftp**://*username@hostname/path*
- **tftp**://*hostname*:*port-num/path*

4) To monitor the download process:

```
Firepower-chassis /ssa/app-software# show download-task
```

5) To view the downloaded applications:

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

6) To view details for a specific applications:

```
Firepower-chassis /ssa# scope app application_type image_version
Firepower-chassis /ssa/app# show expand
```

Sample:

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

4.5.2.8 Update Application Image via CLI

1) Enter Security Services mode:

```
Firepower-chassis # scope ssa
```

2) Set the scope to the security module you are updating:

```
Firepower-chassis /ssa # scope slot slot_number
```

3) Set the scope to the application you are updating:

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

4) Set the Startup version to the version you want to update:

```
Firepower-chassis /ssa/slot/app-instance # set startup-version
version_number
```

5) Commit the configuration:

```
commit-buffer
```

4.5.2.9 Update Application Image via GUI

1) Choose **Logical Devices** to open the Logical Devices page.

   The Logical Devices page shows a list of configured logical devices on the chassis. If no logical devices have been configured, a message stating so is shown instead.

2) Click **Update Version** for the logical device that you want to update to open the **Update Image Version** dialog box.
3) For the **New Version**, choose the software version to which you want to update.
4) Click **OK**.

4.5.3 User and Role Management

User accounts are used to access the system. Up to 48 local user accounts can be configured. Each user account must have a unique username and password.

Admin Account

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

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

Locally Authenticated User Accounts

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

Remotely Authenticated User Accounts

A remotely authenticated user account is any user account that is authenticated through LDAP, RADIUS, or TACACS+.

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

User Roles

The system contains the following user roles:

- **Administrator**

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

- **Read-Only**

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

- **Operations**

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

- **AAA Administrator**

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

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]}**

4.5.4 Selecting the Default Authentication Service via CLI

1) Enter security mode:

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

2) Enter default authorization security mode:

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

3) Specify the default authentication:

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

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

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

4) Specify the maximum amount of time that can elapse after the last refresh request before the Firepower eXtensible Operating System considers a session to have ended.

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

For both commands, specify an integer between 1 and 600 seconds. The default is 600 seconds. For the CC-certified configuration, these timeouts must be set to non-zero values; a value of zero disables the idle timeout.

5) Commit the transaction to the system configuration:

```
commit-buffer
```

The following example shows setting the idle timeout for SSH and WebUI to 66 seconds, and setting the timeout for console sessions to 33 seconds:

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # show detail

Default authentication:
    Admin Realm: Local
    Operational Realm: Local
    Web session refresh period(in secs): 600
    Session timeout(in secs) for web, ssh, telnet sessions: 600
    Absolute Session timeout(in secs) for web, ssh, telnet sessions: 3600
    Serial Console Session timeout(in secs): 600
    Serial Console Absolute Session timeout(in secs): 3600
    Admin Authentication server group:
    Operational Authentication server group:
    Use of 2nd factor: No
FP9300-A /security/default-auth # set session-timeout 66
FP9300-A /security/default-auth* # set con-session-timeout 33
FP9300-A /security/default-auth* # commit-buffer
Error: Update failed: [For Default Authentication, Refresh Period cannot be
greater than Session Timeout]
FP9300-A /security/default-auth* # set refresh-period 60
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth # show detail

Default authentication:
    Admin Realm: Local
    Operational Realm: Local
    Web session refresh period(in secs): 60
    Session timeout(in secs) for web, ssh, telnet sessions: 66
    Absolute Session timeout(in secs) for web, ssh, telnet sessions: 3600
    Serial Console Session timeout(in secs): 33
    Serial Console Absolute Session timeout(in secs): 3600
    Admin Authentication server group:
    Operational Authentication server group:
    Use of 2nd factor: No
FP9300-A /security/default-auth #
```

4.5.5 Selecting the Default Authentication Service via GUI

1) Choose **System** > **User Management**.
2) Click the **Settings** tab.
3) Complete the following fields with the required information:

Name	Description
Default Authentication field	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 Firepower chassis. • **Radius**–The user account must be defined on the RADIUS server specified for the Firepower chassis. • **TACACS**–The user account must be defined on the TACACS+ server specified for the Firepower chassis.

	• **LDAP**–The user account must be defined on the LDAP/MS-AD server specified for the Firepower chassis. • · **None**–If the user account is local to the Firepower chassis, no password is required when the user logs in remotely.

4.5.6 Set the Maximum Number of Login Attempts

This option determines the maximum number of failed login attempts allowed before a user is locked out of the FXOS chassis for a specified amount of time. If a user exceeds the set maximum number of login attempts, the user will be locked out of the system. No notification will appear indicating that the user is locked out. In this event, the user must wait the specified amount of time before attempting to log in.

- All types of user accounts (including account type 'admin') are locked out of the system after exceeding the maximum number of login attempts.
- The default maximum number of unsuccessful login attempts is '3'. The default amount of time the user is locked out of the system after exceeding the maximum number of login attempts is 30 minutes (1800 seconds).

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

   scope system

   scope security

2) Set the maximum number of unsuccessful login attempts:

   set max-login-attempts *max_login*

   The *max_login* value can be any integer from 0-10, but in the CC-certified configuration, the value must be set greater than zero.

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*

4) Commit the configuration:

   commit_buffer

To view whether an local account is locked or not:

```
scope security
  enter local-user username
    show detail
```

Sample output:

```
FP9300-A /security/local-user # show detail
Local User admin2:
    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:
FP9300-A /security #
```

To unlock a locked account (rather than waiting for the account to because automatically unlocked after the configured locking period):

```
scope security
  enter local-user username
    clear lock-status
    commit-buffer
```

4.5.7 Configure the Minimum Password Length

If this option is enabled, the FXOS chassis requires users to create passwords with a specified minimum number of characters. For example, if the *min_length* element in this option is set to '15', users must create passwords using 15 characters or greater. For the CC-certified configuration, the value can be any value from 8-80.

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

```
scope system
scope security
```

2) Enter the password profile security mode:

```
scope password-profile
```

3) Specify the minimum password length:

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

4) Commit the configuration:

```
commit-buffer
```

4.5.8 Enable Password Strength Check

If the password strength check is enabled, FXOS does not permit a user to choose a password that does not meet the guidelines for strong password. In the CC-certified configuration, enabling this feature is optional.

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

```
scope security
```

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

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

3) Commit the configuration:

```
commit-buffer
```

Guidelines for Strong Password

- 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 ABC or 321.
- Must not be identical to the username or reverse of the username.
- Must pass a password dictionary check.
- Must not contain the following symbols: $ (dollar sign), ? (question mark), and = (equals sign)
- Must be between 8 to 80 characters long.

4.5.9 Create a Local User Account via CLI

1) Enter security mode:

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

2) Create the user account:

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

Where *local-user-name* is the account name to be used when logging into this account. This name must be unique.

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

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

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

4) Set the password for the user account:

```
Firepower-chassis /security/local-user # set password
Enter a password: password
Confirm the password: password
```

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

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

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

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

7) (Optional) Specify the SSH key used for passwordless access. Note only RSA public key is currently supported.

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

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

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

Where *role-name* is the role that represents the privileges you want to assign to the user account.

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

9) To remove an assigned role from the user:

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

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

10) Commit the transaction.

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

4.5.10 Create a Local User Account via GUI

1) Choose **System** > **User Management**.
2) Click the **Local Users** tab.
3) Click **Add User** to open the **Add User** dialog box.
4) Complete the following fields with the required information:

Name	Description
User Name field	The account name that is used when logging into this account. This name must be unique.
First Name field	The first name of the user. This field can contain up to 32 characters.
Last Name field	The last name of the user. This field can contain up to 32 characters.
Password field	The password associated with this account.
Confirm Password field	The password a second time for confirmation purposes.
Account Status field	If the status is set to **Active**, a user can log into Firepower Chassis Manager and the FXOS CLI with this login ID and password.
User Role list	The role that represents the privileges you want to assign to the user account.

4.5.11 Delete a Local User Account via CLI

1) Enter security mode:

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

2) Delete the local-user account:

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

3) Commit the transaction to the system configuration:

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

4.5.12 Delete a Local User Account via GUI

1) Choose **System** > **User Management**.
2) Click the **Local Users** tab.
3) In the row for the user account that you want to delete, click **Delete**.
4) In the **Confirm** dialog box, click **Yes**.

4.5.13 Configure Time Synchronization

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

The CC-evaluated configuration requires the system to not accept broadcast and multicast NTP packets that would result in the timestamp being updated. By default FXOS will not accept NTP broadcast or multicast packets, so no additional configuration is necessary. Furthermore, FXOS must be configured to tunnel NTP over IPsec, and the IPsec tunnel will not allow multicast or broadcast packets to reach FXOS.

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

Use the GUI to enable and configure one or more NTP servers.

1) Choose **Platform Settings** > **NTP**.
2) Click the Time **Synchronization** tab.
3) Under **Set Time Source**, click **Use NTP Server**.
4) For each NTP server you want to use, up to a maximum of four, enter the IP address or hostname of the NTP server in the **NTP Server** field and click **Add**.
5) Click **Save**.

Once you click **Save** the Firepower chassis is configured with the NTP server information specified.

You can view the synchronization status of each server by looking at the **Server Status** field in the **NTP Server** table. If the system is unable to synchronize with a particular NTP server, you can hover over the information icon next to the Server Status for more information.

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 Firepower Chassis Manager again.

IMPORTANT! NTP settings are not synced between the Firepower chassis and any applications installed on the chassis. To ensure proper function, you must configure the same NTP settings on the Firepower chassis and on the applications running on the chassis.

4.5.13.1 View the Configured Date and Time via CLI

1) Connect to the FXOS CLI.
2) To view the configured time zone:

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

3) To view the configured date and time:

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

4.5.13.2 View the Configured Date and Time via GUI

1) Choose **Platform Settings** > **NTP**.

2) Click the **Current Time** tab.

   The system shows the date, time, and time zone that are configured on the device.

4.5.13.3 Set the Time Zone via CLI

1) Enter system mode:

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

2) Enter system services mode:

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

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.

4) Commit the transaction to the system configuration:

```
Firepower-chassis /system/service* # commit-buffer
```

4.5.13.4 Set the Time Zone via GUI

1) Choose **Platform Settings** > **NTP**.
2) Click the **Current Time** tab.
3) Choose the appropriate time zone for the Firepower chassis from the **Time Zone** drop-down list.

4.5.13.5 Set the Date and Time Using NTP via CLI

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

1) Enter system mode:

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

2) Enter system services mode:

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

3) Configure the system to use the NTP server with the specified hostname, IPv4, or IPv6 address:

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

4) Commit the transaction to the system configuration:

```
Firepower-chassis /system/services/ntp-server* # up
```

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

5) To view the synchronization status for all configured NTP servers:

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

4.5.13.6 Set the Date and Time Using NTP via GUI

1) Choose **Platform Settings** > **NTP**.
2) Click the **Time Synchronization** tab.
3) Under **Set Time Source**, click **Use NTP Server**.
4) For each NTP server you want to use, up to a maximum of four, enter the IP address or hostname of the NTP server in the **NTP Server** field and click **Add**.
5) Click **Save**.

4.5.13.7 Set the Date and Time Manually via CLI

This section describes how to set the date and time manually on the Firepower chassis. System clock modifications take effect immediately. If the system clock is currently being synchronized with an NTP server, you will not be able to set the date and time manually.

1) Enter system mode:

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

2) Enter system services mode:

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

3) Configure the system clock:

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

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

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

4.5.13.8 Set the Date and Time Manually via GUI

1) Choose **Platform Settings** > **NTP**.
2) Click the **Time Synchronization** tab.
3) Under **Set Time Source**, click **Set Time Manually**.
4) Click the **Date** drop-down list to display a calendar and then set the date using the controls available in the calendar.
5) Use the corresponding drop-down lists to specify the time as hours, minutes, and AM/PM.
6) Click **Save**.

4.5.14 Configure SSH Access

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

4.5.14.1 Configure SSH via CLI

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
```

FXOS supports rsa-sha2-256 and rsa-sha2-512 for SSH public key authentication. See Section 4.3.3 for generating the SSH Host Key. There is no further configuration needed.

4.5.14.2 Configure SSH via GUI

1) Choose **Platform Settings** > **SSH**.
2) To enable SSH access to the Firepower chassis, check the **Enable SSH** check box. To disable SSH access, uncheck the **Enable SSH** check box.
3) Click **Save**.

4.5.15 Configure PKI

This section describes how to configure HTTPS and IPsec on the FXOS chassis.

NOTE! You can change the HTTPS port using Firepower Chassis Manager or the FXOS CLI. All other HTTPS configuration can only be done using the FXOS CLI.

4.5.15.1 Certificates and Trust Points

IPsec uses components of the Public Key Infrastructure (PKI) to establish secure communications between two devices, such as a client's system and the FXOS chassis.

Certificates

An X509v3 certificate is a file containing a device's public key along with signed information about the device's identity. To merely support encrypted communications, a device can generate its own key pair and its own self-signed certificate. When a remote user connects to a device that presents a self-signed certificate, the user has no easy method to verify the identity of the device, and the user's browser will initially display an authentication warning. By default, FXOS contains a built-in self-signed certificate containing the public key from the default key ring.

Trust Points

To provide stronger authentication for FXOS, you can obtain and install a third-party certificate from a trusted source, or trust point that affirms the identity of your device. The third-party certificate is signed by the issuing trust point, which can be a root certificate authority (CA) or an intermediate CA or trust anchor that is part of a trust chain that leads to a root CA. To obtain a new certificate (e.g., for IPsec mutual authentication), you must generate a certificate signing request (CSR) through FXOS and submit the request to a trust point.

IMPORTANT! The certificate must be in Base 64 encoded X.509 (CER) format.

FXOS supports X.509v3 certificates as defined by RFC 5280 for use in authentication of a network peer using IPsec and TLS. Public key infrastructure (PKI) credentials, such as private keys and X509v3 certificates are stored in a specific location, such as NVRAM and flash memory. The identification and authentication, and authorization security functions protect an unauthorized user from gaining access to the storage.

Digital certificates provide digital identification for authentication. A digital certificate includes information that identifies a device or user, such as the common name, serial number, company, department, state, country, or IP address. CAs are trusted authorities that “sign” certificates to verify their authenticity, thereby guaranteeing the identity of the device or user. CAs issue digital certificates in the context of a PKI, which uses public-key or private-key encryption to ensure security.

For authentication using digital certificates, at least one identity certificate and its issuing CA certificate must exist in FXOS. This configuration allows multiple identities, roots, and certificate hierarchies. The FXOS evaluates third-party certificates against CRLs, also called authority revocation lists, all the way from the identity certificate up the chain of subordinate certificate authorities.

Descriptions of several different types of available digital certificates follow:

- A CA certificate is used to sign other certificates. It is self-signed and called a root certificate. A certificate that is issued by another CA certificate is called a subordinate certificate.

• CAs also issue identity certificates, which are certificates for specific systems or hosts.

An identity certificate also contains information indicating the intended use of the certificate. That is, an identity certificate intended to authenticate a TLS server or TLS client would contain a "ServerAuth" or "ClientAuth" Extended key Usage (EKU), while one intended for use by peers in an IPsec VPN would contain an "IPsec Tunnel" EKU. The identity certificate presented by a CRL provider when returning a CRL must contain the CRLsign Key Usage (KU). FXOS does not enforce any other EKU.

Network peers in the operational environment to which the FXOS will connect using TLS or IPsec, must be configured to present a valid x509v3 identity certificate issued by a PKI trusted by FXOS. For example, if audit transfer is protected by TLS, then the TLS connection offered by the audit server must provide a valid x509v3 identity certificate.

The FXOS CA integrates an independent certificate authority feature on FXOS, deploys certificates, and provides secure revocation checking of issued certificates. The FXOS CA provides a secure, configurable, in-house authority for certificate authentication with user enrollment through a website login page.

When a certificate is issued, it is valid for a fixed period of time. Sometimes a CA revokes a certificate before this time period expires; for example, because of security concerns or a change of name or association. CAs periodically issue a signed list of revoked certificates. Enabling revocation checking forces FXOS to check that the CA has not revoked a certificate each time that it uses the certificate for authentication.

When the administrator enables revocation checking, FXOS checks certificate revocation status during the PKI certificate validation process[3], using CRL checking.

With CRL checking, FXOS retrieves, parses, and caches CRLs, which provide a complete list of revoked (and unrevoked) certificates with their certificate serial numbers. FXOS evaluates certificates according to CRLs, also called authority revocation lists, from the identity certificate up the chain of subordinate certificate authorities.

CRLs

CRLs provide FXOS with one way of determining whether a certificate that is within its valid time range has been revoked by the issuing CA. CRL configuration is part of configuration of a trustpoint.

The administrator can configure FXOS to make CRL checks mandatory when authenticating a certificate by using the `revocation-check crl` command. This configuration is required to be in a Common Criteria certified configuration.

FXOS can retrieve CRLs from CAs using HTTP, SCEP, or LDAP. CRLs retrieved for each trustpoint are cached for a configurable amount of time for each trustpoint.

4.5.15.2 Creating a Key Ring

FXOS supports a maximum of 8 key rings, including the default key ring.

1) Enter security mode:

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

2) Create and name the key ring:

[3] Certificate revocation checking occurs on all certificates except self-signed Root Certificate Authorities when either CRL revocation-check has been defined for a trustpoint.

```
Firepower-chassis# create keyring keyring-name
```

3) Set the TLS or IPsec key length in bits (RSA Only):

```
Firepower-chassis# set modulus {~~mod1024 | mod1536 |~~ mode2048 ~~| mod512~~}
```

4) Commit the transaction:

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

4.5.15.3 Creating a Certificate Request for a Key Ring

1) Enter services mode:

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

2) Enter configuration mode for the key ring:

```
Firepower-chassis /security# scope keyring keyring-name
```

3) Create a certificate request:

```
Firepower-chassis /security/keyring# create certreq
```

4) Specify the country code of the country in which the company resides:

```
Firepower-chassis /security/keyring/certreq# set country country-name
```

5) Specify the Domain Name Server (DNS) address associated with the request:

```
Firepower-chassis /security/keyring/certreq# set dns DNS-name
```

6) Specify the email address associated with the certificate request:

```
Firepower-chassis /security/keyring/certreq# set e-mail email-name
```

7) Specify the IP address of the FXOS chassis:

```
Firepower-chassis /security/keyring/certreq# set ip {IPv4 | IPv6 }
```

8) Specify the city or town in which the company requesting the certificate is headquartered:

```
Firepower-chassis /security/keyring/certreq# set locality city-name
```

9) Specify the organization requesting the certificate:

```
Firepower-chassis /security/keyring/certreq# set org-name org-name
```

10) Specify the organizational unit:

```
Firepower-chassis /security/keyring/certreq# set org-unit-name org-unit-
name
```

11) Specify an optional password for the certificate request:

```
Firepower-chassis /security/keyring/certreq# set password password
```

12) Specify the state or province in which the company requesting the certificate is headquartered:

```
Firepower-chassis /security/keyring/certreq# set state state
```

13) Specify the fully qualified domain name of the FXOS chassis:

```
Firepower-chassis /security/keyring/certreq# set subject-name subject-name
```

14) Commit the transaction:

```
Firepower-chassis /security/keyring/certreq# commit-buffer
```

15) Display the certificate request, which you can copy and send to a trust anchor or certificate authority:

```
Firepower-chassis /security/keyring/certreq# show certreq
```

4.5.15.4 Creating a Trust Point

1) Enter services mode:

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

2) Create a trust point:

```
Firepower-chassis /security# create trustpoint name
```

3) Specify certificate information for this trust point:

```
Firepower-chassis /security/trustpoint# set certchain [ certchain ]
```

4) Commit the transaction:

```
Firepower-chassis /security/trustpoint# commit-buffer
```

4.5.15.5 Importing a Certificate into a Key Ring

1) Enter services mode:

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

2) Enter configuration mode for the key ring that will receive the certificate:

```
Firepower-chassis /security# scope keyring keyring-name
```

3) Specify the trust point for the trust anchor or certificate authority from which the key ring certificate was obtained:

```
Firepower-chassis /security/keyring# set trustpoint name
```

4) Launch a dialog for entering and uploading the key ring certificate:

```
Firepower-chassis /security/keyring# set cert
```

At the prompt, paste the certificate text that you received from the trust anchor or certificate authority. On the next line following the certificate, type ENDOFBUF to complete the certificate input.

5) Commit the transaction:

```
Firepower-chassis /security/keyring# commit-buffer
```

4.5.15.6 Deleting a Key Ring

A keyring can be deleted using “delete keyring <name>” command.

4.5.15.7 Deleting a Trust Point

A trust point can be deleted using “delete trustpoint <name> command.

4.5.15.8 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 1.2, and ciphersuites to only the ones allowed below.

- 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

FXOS performs key establishment using ECDSA with secp256r1, secp384rl or secp521r1 NIST curves. There is no further configuration needed.

4.5.16 Logical Device Management

When you create a logical device, the FXOS chassis supervisor deploys the logical device by downloading the specified software version and pushing the bootstrap configuration and management interface settings to the specified security module/engine, or in the case of an intra-chassis cluster, to all security modules installed in the Firepower chassis.

4.5.16.1 Create a ASA Logical Device via CLI

You can create a standalone logical device for each security module/engine installed in the FXOS chassis.

1) Enter security services mode:

```
Firepower# scope ssa
```

2) Create the logical device:

```
Firepower /ssa # create logical-device device_name asa slot_id standalone
```

3) Enter a description for the logical device:

```
Firepower /ssa/logical-device* # set description "logical device
description"
```

4) Assign the management and data interfaces to the logical device:

```
Firepower /ssa/logical-device* # create external-port-link name
interface_name asa

Firepower-chassis /ssa/logical-device/external-port-link* # exit
```

5) Configure the management bootstrap information:

a) Create bootstrap object:

```
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
```

b) Create enable password:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-
secret PASSWORD
```

c) Set password value:

```
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set
value
```

Value: *password*

d) Exit password configuration scope:

```
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
```

e) Configure management IP address:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 slot_id
default
```

f) Set gateway address:

```
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway
gateway_address
```

g) Set IP address and mask:

```
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip ip_address
mask network_mask
```

h) Exit management IP configuration scope:

```
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
```

i) Exit management bootstrap configuration scope:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
```

6) Commit the configuration:

```
commit-buffer
```

4.5.16.2 Create a ASA Logical Device via GUI

1) Choose **Logical Devices** to open the Logical Devices page.

   The Logical Devices page shows a list of configured logical devices on the chassis. If no logical devices have been configured, a message stating so is shown instead.

2) Click **Add Device** to open the **Add Device** dialog box.
3) For the **Device Name**, provide a name for the logical device.
4) For the **Template**, choose **Cisco Adaptive Security Appliance**.
5) For the **Image Version**, choose the ASA software version.
6) For the **Device Mode**, click the **Standalone** radio button.
7) Click **OK**.

   You see the Provisioning - *device name* window.

8) Expand the **Data Ports** area, and click each port that you want to assign to the device.
9) Click the device icon in the center of the screen.

   The ASA Configuration dialog box appears.

10) On the **General Information** tab, complete the following:

    a) On multiple module devices, like the Firepower 9300, choose the security module that you want to use for this logical device by clicking on it under Security Module Selection.

    b) Select the management interface to use with the logical device from the **Management Interface** drop-down list.

    c) Under DEFAULT, configure the management interface:

    This information is used to configure a management interface in the security module/engine configuration. This management IP address is also the IP address you will use to connect to ASDM.

    1 Select the type of address from the **Address Type** drop-down list.

    2 In the **Management IP** field, configure a local IP address.

    3 Enter a **Network Mask** or **Prefix Length**.

    4 Enter a **Network Gateway** address.

11) On the **Settings** tab, enter a password for the "admin" user in the **Password** field.
12) Click **OK** to close the ASA Configuration dialog box.
13) Click **Save**.

4.5.16.3 Delete a ASA Logical Device via CLI

1) Enter security services mode:

   ```
   Firepower# scope ssa
   ```

2) View details for the logical devices on the chassis:

   ```
   Firepower /ssa # show logical-device
   ```

3) For each logical device that you want to delete, enter the following command:

   ```
   Firepower /ssa # delete logical-device device_name
   ```

4) View details for the applications installed on the logical devices:

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

5) For each application that you want to delete, enter the following commands:

   a) `Firepower /ssa # scope slot slot_number`

   b) `Firepower /ssa/slot # delete app-instance application_name`

   c) `Firepower /ssa/slot # exit`

6) Commit the configuration:

   ```
   commit-buffer
   ```

4.5.16.4 Delete a ASA Logical Device via GUI

1) Choose **Logical Devices** to open the Logical Devices page.

   The Logical Devices page shows a list of configured logical devices on the chassis. If no logical devices have been configured, a message stating so is shown instead.

2) Click **Delete** for the logical device that you want to delete.
3) Click **Yes** to confirm that you want to delete the logical device.
4) Click **Yes** to confirm that you want to delete the application configuration.

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