Cisco FXOS 2.6 on Firepower 4100/9300 for FTD Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration

Version 1.1

May 24, 2021

Prepared by:

Cisco Systems, Inc.,
170 West Tasman Drive, San Jose,
CA 95134-1706 USA

Table of Contents

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 FTD. 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 FTD installed on the security module is managed separately and is described in the corresponding document specified in Section 1.2.

This document is a supplement to the Cisco administrative guidance, which is comprised of the installation and administration documents identified in Section 1.2. 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 CPP_ND_v2.2e, EP_IPS_v2.11, MOD_CPP_FW_1.4E and MOD_VPNGW_V1.1.

[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 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 2.6 and FTD release 6.4
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 2.6 and FTD release 6.4

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 4110, 4120, 4130, and 4140 Hardware Installation Guide, Last updated: August 21, 2020 *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, Last updated: August 21, 2020 *https://www.cisco.com/c/en/us/td/docs/security/firepower/41x5/hw/guide/install-41x5.html*
Cisco Firepower 9300 Hardware Installation Guide, Last updated August 24, 2020 *https://www.cisco.com/c/en/us/td/docs/security/firepower/9300/hw/guide/b_install_guide_9300.html*
Cisco Firepower 4100/9300 Upgrade Guide, Last updated: August 7, 2020 *https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/upgrade/b_FXOSUpgrade.html*
Cisco FXOS CLI Configuration Guide, 2.6(1), July 2, 2020 *https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos261/cli-guide/b_CLI_ConfigGuide_FXOS_261.html*
Cisco FXOS Firepower Chassis Manager Configuration Guide, 2.6(1), July 2, 2020 *https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos261/web-guide/b_GUI_FXOS_ConfigGuide_261.html*
FTD (NGFW) v6.4 on Firepower 4100 and 9300 Series with FMC and FMCv Common Criteria Supplemental User Guide, April 7, 2021 [FTD-CC]
Cisco FXOS 2.6 on Firepower 4100/9300 for FTD 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.
- Certificate Authority (CA) server – The system can be configured to import X.509v3 certificates from a CA, e.g., for TLS connection to syslog server.
- DNS server – The system supports domain name service in the network.

2.2 Environmental Assumptions

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

Table 2: Operational Environment Security Measures

Environment Security Objective	Operational Environment Security Objective Definition	Administrator Responsibility
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	Administrators must ensure the system is installed and maintained within a secure physical location. This can include a secured building with key card access or within the physical control of an authorized administrator in a mobile environment.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.	Administrators must not add any general-purpose computing capabilities (e.g., compilers or user applications) to the system.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.	Administrators must configure the security devices in the Operation environment of the TOE to secure the network.
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.	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.

Environment Security Objective	Operational Environment Security Objective Definition	Administrator Responsibility
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 wherever they may be.
OE.COMPONENTS_RUNNING	For distributed TOEs the Security Administrator ensures that the availability of every TOE component is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. The Security Administrator also ensures that it is checked as appropriate for every TOE component that the audit functionality is running properly.	For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.
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 networking equipment when the equipment is discarded or removed from its operational environment. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

Environment Security Objective	Operational Environment Security Objective Definition	Administrator Responsibility
OE.VM_CONFIGURATION	For vNDs, the Security Administrator ensures that the VS and VMs are configured to • reduce the attack surface of VMs as much as possible while supporting ND functionality (e.g., remove unnecessary virtual hardware, turn off unused inter-VM communications mechanisms), and • correctly implement ND functionality (e.g., ensure virtual networking is properly configured to support network traffic, management channels, and audit reporting). The VS should be operated in a manner that reduces the likelihood that vND operations are adversely affected by virtualization features such as cloning, save/restore, suspend/resume, and live migration. If possible, the VS should be configured to make use of features that leverage the VS's privileged position to provide additional security functionality. Such features could include malware detection through VM introspection, measured VM boot, or VM snapshot for forensic analysis.	The Administrator must ensure that the TOE VMs are properly configured to support network traffic and all unnecessary communications are turned off.
OE.CONNECTIONS	TOE administrators will ensure that the TOE is installed in a manner that will allow the TOE to effectively enforce its policies on network traffic of monitored networks.	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

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 as specified in the NDcPP.

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.

The default password for the 'admin' account is Admin123, and must be changed during first login.

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	Username.
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	Distributed TOE audit generation	Actual Audited Event
Reproduced from CPP_ND_v2.2E			
FAU_GEN.1	Startup and shutdown events	FMC, FXOS and FTD	**FTD**: Syslog Startup: <date> <time> <host> syslog-ng[62850]: syslog-ng starting up; version='3.6.2' Syslog Stopping: <date> <time> <host> syslog-ng[12061]: syslog-ng shutting down; version='3.6.2' **FMC**: Syslog Startup: <date> <time> <host> syslog-ng[25980]: syslog-ng starting up; version='3.7.3' Syslog Stop: <date> <time> <host> syslog-ng[13011]: syslog-ng shutting down; version='3.7.3' **FXOS**: Syslog Startup: <date> <time> <host>: <date> <time> <timezone>: %DAEMON-7-SYSTEM_MSG: Done _init function - syslog[7580] Syslog Stop: <date> <time> <host>: <date> <time> <timezone>: %FPRM-6-AUDIT: [admin][admin][modification][web_10456_A][1694235][sys/svc-ext/syslog/client-primary][adminState(Old:enabled, New:disabled)][] Syslog Remote Destination <ip-address> modified
FCO_CPC_EXT.1	Enabling communications between a pair of components. Disabling communications between a pair of components	FMC and FTD	**FTD:** Enabling: <date> <time> <host>: SF-IMS[15479]: [16265] sftunneld:sf_ssl [INFO] Successfully connected using SSL to: '10.6.16.116' Disabling: <date> <time> <host>: SF-IMS[38115]: [41665] sfmbservice:sfmb_service [INFO] Connection closed to host 10.6.16.116 **FMC:** Enable: <date> <time> <host>: mojo_server.pl: <host>: <user>@10.6.16.47, Devices > Device Management, Add Device - 10.6.16.221 Disable: <date> <time> <host>: mojo_server.pl: <host>: <user>@10.6.16.47, Devices > Device Management, Delete Device - fp4140ftd **FXOS:** Not applicable.
FCS_HTTPS_EXT.1	Failure to establish an HTTPS session.	FMC and FXOS	See FCS_TLSS_EXT.1. **FTD:** Not applicable.

SFR	Auditable Event	Distributed TOE audit generation	Actual Audited Event
			FMC: <date> <time> <host> syslog-ng[23928]: SSL error while writing stream; tls_error='SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure' **FXOS:** <date> <time> <host>: <date> <time> <timezone>:%USER-6-SYSTEM_MSG: [ssl:info] [pid 8001:tid 1739586368] [client 10.6.16.45:59026] AH02008: SSL library error 1 in handshake (server 10.6.16.218:443) - httpd[8001]
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA. Session Establishment with peer Reason for failure. \ Entire packet contents of packets transmitted/received during session establishment.	FTD and FXOS	**FTD:** Valid Connection: <date> <time> <host> %FTD-6-602303: IPSEC: An outbound LAN-to-LAN SA (SPI= 0xC5A0801B) between 192.168.144.221 and 192.168.144.46 (user= 192.168.144.46) has been created. No Proposal Chosen / IKE weaker than ESP: <date> <time> <host> %FTD-4-750003: Local:192.168.144.221:500 Remote:192.168.144.46:500 Username:Unknown IKEv2 Negotiation aborted due to ERROR: Failed to find a matching policy Invalid Certificate: <date> <time> <host> %FTD-3-717027: Certificate chain failed validation. No suitable trustpoint was found to validate chain. <date> <time> <host> %FTD-3-751006: Local:192.168.144.221:500 Remote:192.168.144.46:500 Username:192.168.144.46 IKEv2 Certificate authentication failed. Error: Certificate authentication failed <date> <time> <host> %FTD-4-750003: Local:192.168.144.221:500 Remote:192.168.144.46:500 Username:192.168.144.46 IKEv2 Negotiation aborted due to ERROR: Auth exchange failed Mismatched Identifier: <date> <time> <host> %FTD-4-717037: Tunnel group search using certificate maps failed for peer certificate: serial number: 00A2, subject name: e=server-dn-org-w-null-ecdsa@gossamersec.com,cn=tl15-16x.example.com,o=GCT, issuer_name: e=subsubca-ecdsa@gossamersec.com,cn=subsubca-ecdsa,o=GCT,l=Catonsville,st=MD,c=US. Packet contents (snippet): <date> <time> <host> %FTD-7-711001: IKEv2-PROTO-5: (4): Next payload: SA, version: 2.0 <date> <time> <host> %FTD-7-711001: (4): Exchange type: IKE_SA_INIT, flags: INITIATOR <date> <time> <host> %FTD-7-711001: (4): Message id: 0, length: 498 <date> <time> <host> %FTD-7-711001: (4): #012Payload contents: <date> <time> <host> %FTD-7-711001: (4): SA <date> <time> <host> %FTD-7-711001: (4): Next payload: KE, reserved: 0x0, length: 132 <date> <time> <host> %FTD-7-711001: (4): last proposal: 0x0, reserved: 0x0, length: 128#012 Proposal: 1, Protocol id: IKE, SPI size: 0, #trans: 14 <date> <time> <host> %FTD-7-711001: (4): last transform: 0x3, reserved: 0x0: length: 12#012 type: 1, reserved: 0x0, id: AES-CBC **FMC:** Not applicable. **FXOS:** Valid Connection: <date> <time> <host>: <date> <time> <timezone>: %AUTHPRIV-6-SYSTEM_MSG: 05[IKE] CHILD_SA gctipsec{5} established with SPIs c370afd2_i cc80cfa9_o and TS 10.6.16.218/32 === 10.6.16.43/32 - charon-custom

SFR	Auditable Event	Distributed TOE audit generation	Actual Audited Event
			No Proposal Chosen: <date> <time> <host>: <date> <time> <timezone>: %AUTHPRIV-6-SYSTEM_MSG: 13[IKE] received NO_PROPOSAL_CHOSEN notify error - charon-custom Invalid Certificate/Mismatched identifier: <date> <time> <host>: <date> <time> <timezone>: %AUTHPRIV-6-SYSTEM_MSG: 05[IKE] no trusted RSA public key found for '10.6.16.46' - charon-custom IKE weaker than ESP: <date> <time> <host>: <date> <time> <timezone>: %AUTHPRIV-6-SYSTEM_MSG: 13[IKE] IKE SA key size (128) is less then CHILD SA key size (256), sa strength violation - charon-custom
FCS_NTP_EXT.1	Configuration of a new time server Removal of configured time server Identity if new/removed time server		**FXOS:** New Server Configuration: <date> <time> <host>: <date> <time> <timezone>: %FPRM-6-AUDIT: [admin][admin][creation][web_30674_A][1585436][sys/svc-ext/datetime-svc/ntp-10.6.16.46][name:10.6.16.46, sha1KeyId:0][] NTP server 10.6.16.46 created Server Removal: <date> <time> <host>: <date> <time> <timezone>: %FPRM-6-AUDIT: [admin][admin][deletion][web_12725_A][614179][sys/svc-ext/datetime-svc/ntp-10.6.16.46][sys/svc-ext/datetime-svc/ntp-10.6.16.46][] NTP server 10.6.16.46 deleted

SFR	Auditable Event	Distributed TOE audit generation	Actual Audited Event
FCS_SSHS_EXT.1	Failure to establish an SSH session	FTD, FMC and FXOS	**FTD:** Valid Connection: <date> <time> <host> sshd[41573]: pam_unix(sshd:session): session opened for user admin by (uid=0) Bad Cipher: <date> <time> <host> sshd[55627]: Unable to negotiate with 10.6.16.46 port 43416: no matching cipher found. Their offer: aes256-ctr [preauth] Bad Auth Alg: <date> <time> <host> sshd[54346]: Unable to negotiate with 10.6.16.46 port 43334: no matching host key type found. Their offer: ecdsa-sha2-nistp256 [preauth] Bad MAC Alg: <date> <time> <host> sshd[50873]: Unable to negotiate with 10.6.16.46 port 42804: no matching MAC found. Their offer: hmac-sha1-96 [preauth] Bad Kex Alg: <date> <time> <host> sshd[52528]: Unable to negotiate with 10.6.16.46 port 43132: no matching key exchange method found. Their offer: ecdh-sha2-nistp256,ext-info-c [preauth] **FMC:** Bad Cipher: <date> <time> <host> sshd[30273]: Unable to negotiate with 10.6.16.46 port 46850: no matching cipher found. Their offer: aes256-ctr [preauth] Bad Auth Alg: <date> <time> <host> sshd[30885]: Unable to negotiate with 10.6.16.46 port 47588: no matching host key type found. Their offer: ecdsa-sha2-nistp521-cert-v01@openssh.com [preauth] Bad MAC Alg: <date> <time> <host> sshd[11527]: Unable to negotiate with 10.6.16.46 port 48128: no matching MAC found. Their offer: hmac-sha1-96 [preauth] Bad Kex Alg: <date> <time> <host> sshd[12992]: Unable to negotiate with 10.6.16.46 port 48538: no matching key exchange method found. Their offer: ecdh-sha2-nistp256,ext-info-c [preauth] **FXOS:** Bad Cipher: <date> <time> <host>: <date> <time> <timezone>: %DAEMON-6-SYSTEM_MSG: Unable to negotiate with 10.6.16.16 port 51450: no matching cipher found. Their offer: aes256-gcm@openssh.com - sshd[12020] Bad Auth Alg: <date> <time> <host>: <date> <time> <timezone>: %DAEMON-6-SYSTEM_MSG: Unable to negotiate with 10.6.16.16 port 52940: no matching host key type found. Their offer: ecdsa-sha2-nistp384-cert-v01@openssh.com - sshd[24181] Bad MAC Alg: <date> <time> <host>: <date> <time> <timezone>: %DAEMON-6-SYSTEM_MSG: Unable to negotiate with 10.6.16.16 port 51778: no matching MAC found. Their offer: hmac-sha1-96 - sshd[12773] Bad Kex Alg: <date> <time> <host>: <date> <time> <timezone>: %DAEMON-6-SYSTEM_MSG: Unable to negotiate with 10.6.16.16 port 52188: no matching key exchange method found. Their offer: ecdh-sha2-nistp256,ext-info-c - sshd[14838]

SFR	Auditable Event	Distributed TOE audit generation	Actual Audited Event
FCS_TLSC_EXT.1	Failure to establish a TLS Session Reason for failure	FTD and FMC	**FTD:** General Failure: <date> <time> <host> SF-IMS[11103]: [2045] sftunneld:sf_ssl [WARN] VerifyConnect:Failed to authenticate or to be authenticated by peer '10.6.16.46' Invalid EKU: <date> <time> <host> SF-IMS[48689]: [48743] sftunneld:sf_ssl [WARN] Base Peer Certificate from fcfc1b00-b171-11e9-82b8-1272d6bd24fc does not meet Cisco Common Criteria, Upgrade it to 6.1.0. Invalid Identifier: <date> <time> <host> SF-IMS[10576]: [10585] sftunneld:sf_ssl [ERROR] CERT subject_title(77777777-7777-7777-7777-777777777777) did not match connected peer uuid(fcfc1b00-b171-11e9-82b8-1272d6bd24fc) Invalid Purpose: <date> <time> <host> %FTD-3-717009: Certificate validation failed. Peer certificate key usage is invalid, serial number: 0085, subject name: e=server-no-auth-eku-rsa@gossamersec.com,cn=tl15-16x.example.com,o=GCT,l=Catonsville,st=MD,c=US. Unknown Cipher: <date> <time> <host> EDT: %FTD-7-725014: SSL lib error. Function: ssl3_get_server_hello Reason: unknown cipher returned Invalid TLS version: <date> <time> <host> EDT: %FTD-7-725014: SSL lib error. Function: ssl3_get_server_hello Reason: wrong ssl version Wrong Curve: <date> <time> <host> %FTD-7-725014: SSL lib error. Function: ssl3_get_key_exchange Reason: wrong curve Certificate Verification Failure: <date> <time> <host> %FTD-3-717009: Certificate validation failed. No suitable trustpoints found to validate certificate serial number: 0081, subject name: e=server-issued-by-unacceptable-rsa@gossamersec.com,cn=tl15-16x.example.com,o=GCT,l=Catonsville,st=MD,c=US, issuer name: cn=rootca-unacceptable-rsa,e=rootca-unacceptable-rsa@gossamersec.com,o=GCT,l=Catonsville,st=MD,c=US Identifier Match Failed: <date> <time> <host> %FTD-3-725019: Server certificate for SSL session outside:192.168.144.221/62273 to 192.168.144.46/6514 did not match reference identity: syslogserver <date> <time> <host> %FTD-7-725014: SSL lib error. Function: ssl3_get_server_certificate Reason: certificate verify failed **FMC:** General Failure: <date> <time> <host> SF-IMS[19567]: [24222] sftunneld:sf_ssl [ERROR] Connect:SSL handshake failed Invalid EKU: <date> <time> <host> SF-IMS[2896]: [2903] sftunneld:sf_ssl [WARN] Peer Certificate from 1d492c4c-cb33-11e9-95d4-de72c62116a8 does not meet Cisco Common Criteria, Upgrade it to 6.1.0 and re-register to the manager. Invalid Identifier:

SFR	Auditable Event	Distributed TOE audit generation	Actual Audited Event
			<date> <time> <host> SF-IMS[22517]: [22781] sftunneld:sf_ssl [ERROR] CERT subject_title(77777777-7777-7777-7777-777777777777) did not match connected peer uuid(1d492c4c-cb33-11e9-95d4-de72c62116a8) **FXOS:** Not applicable.
FCS_TLSC_EXT.2	Failure to establish an TLS Session	FTD and FMC	**FTD:** General Failure: <date> <time> <host> syslog-ng[24933]: SSL error while writing stream; tls_error='SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure' Invalid Purpose: <date> <time> <host> syslog-ng[64066]: X509 Certificate Validation; depth='0', ok='0', errnum='26', error='unsupported certificate purpose' <date> <time> <host> syslog-ng[64120]: SSL error while writing stream; tls_error='SSL routines:ssl3_get_server_certificate:invalid purpose' Wrong Cipher sent by server: <date> <time> <host> syslog-ng[5370]: SSL error while writing stream; tls_error='SSL routines:ssl3_get_key_exchange:bad signature' Unknown Cipher: <date> <time> <host> syslog-ng[73232]: SSL error while writing stream; tls_error='SSL routines:ssl3_get_server_hello:unknown cipher returned' Invalid TLS version: <date> <time> <host> syslog-ng[691]: SSL error while writing stream; tls_error='SSL routines:ssl3_get_server_hello:wrong ssl version' Bad signature: <date> <time> <host> syslog-ng[2291]: SSL error while writing stream; tls_error='rsa routines:RSA_private_encrypt:bad signature' Certificate Verification Failure: <date> <time> <host> syslog-ng[5280]: SSL error while writing stream; tls_error='SSL routines:ssl3_get_server_certificate:certificate verify failed' Digest check failed: <date> <time> <host> syslog-ng[6173]: SSL error while writing stream; tls_error='SSL routines:ssl3_get_finished:digest check failed' Decryption Failed: <date> <time> <host> syslog-ng[7009]: SSL error while writing stream; tls_error='SSL routines:SSL3_GET_RECORD:decryption failed or bad record mac' **FMC:** Bad Cipher and General Failure: <date> <time> <host> syslog-ng[6506]: SSL error while writing stream; tls_error='SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure' Invalid Purpose: <date> <time> <host> syslog-ng[6506]: SSL error while writing stream; tls_error='SSL routines:ssl3_get_server_certificate:invalid purpose' Wrong Cipher sent by server: <date> <time> <host> syslog-ng[6506]: internal() messages are looping back, preventing loop by suppressing all internal messages until the current message is processed; trigger-msg=", first-suppressed-

SFR	Auditable Event	Distributed TOE audit generation	Actual Audited Event
			msg='SSL error while writing stream; tls_error=\'SSL routines:ssl3_get_server_hello:wrong cipher returned\" Unknown Cipher: <date> <time> <host> syslog-ng[6506]: internal() messages are looping back, preventing loop by suppressing all internal messages until the current message is processed; trigger-msg='', first-suppressed-msg='SSL error while writing stream; tls_error=\'SSL routines:ssl3_get_server_hello:unknown cipher returned\" Invalid TLS version: <date> <time> <host> syslog-ng[6506]: internal() messages are looping back, preventing loop by suppressing all internal messages until the current message is processed; trigger-msg='', first-suppressed-msg='SSL error while writing stream; tls_error=\'SSL routines:ssl3_get_server_hello:wrong ssl version\" Wrong Curve: <date> <time> <host> syslog-ng[6506]: SSL error while writing stream; tls_error='SSL routines:ssl3_get_key_exchange:wrong curve' Certificate Verification Failure: <date> <time> <host> syslog-ng[17342]: SSL error while writing stream; tls_error='SSL routines:ssl3_get_server_certificate:certificate verify failed'
FCS_TLSS_EXT.1	Failure to establish an TLS Session	FMC, FXOS and FTD	**FTD:** See FCS_TLSC_EXT.1 **FMC:** No Shared Cipher: <date> <time> <host> [ssl:info] [pid 20165] SSL Library Error: error:1408A0C1:SSL routines:ssl3_get_client_hello:no shared cipher -- Too restrictive SSLCipherSuite or using DSA server certificate? Invalid Key Exchange: <date> <time> <host> [ssl:info] [pid 27692] SSL Library Error: error:1408B09F:SSL routines:ssl3_get_client_key_exchange:length mismatch Digest Check Failed: <date> <time> <host> [ssl:info] [pid 26496] SSL Library Error: error:1408C095:SSL routines:ssl3_get_finished:digest check failed Wrong Block Cipher Pad: <date> <time> <host> [ssl:info] [pid 24541] SSL Library Error: error:1408F081:SSL routines:SSL3_GET_RECORD:block cipher pad is wrong Wrong Version: <date> <time> <host> [ssl:info] [pid 27589] SSL Library Error: error:1408A10B:SSL routines:ssl3_get_client_hello:wrong version number General Failure: <date> <time> <host> syslog-ng[23928]: SSL error while writing stream; tls_error='SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure' ITT: <date> <time> <host> SF-IMS[19567]: [11420] sftunneld:sf_ssl [ERROR] Accept:SSL handshake failed **FXOS:**

SFR	Auditable Event	Distributed TOE audit generation	Actual Audited Event
			No Shared Cipher: <date> <time> <host>: <date> <time> <timezone>: %USER-6-SYSTEM_MSG: [ssl:info] [pid 7998:tid 1909455680] SSL Library Error: error:1408A0C1:SSL routines:ssl3_get_client_hello:no shared cipher -- Too restrictive SSLCipherSuite or using DSA server certificate? - httpd[7998] Invalid Key Exchange: <date> <time> <host>: <date> <time> <timezone>: %USER-6-SYSTEM_MSG: [ssl:info] [pid 7998:tid 1903164224] SSL Library Error: error:1408B09F:SSL routines:ssl3_get_client_key_exchange:length mismatch - httpd[7998] Digest Check Failed: <date> <time> <host>: <date> <time> <timezone>: %USER-6-SYSTEM_MSG: [ssl:info] [pid 7998:tid 1902115648] SSL Library Error: error:1408C095:SSL routines:ssl3_get_finished:digest check failed - httpd[7998] Wrong Block Cipher Pad: <date> <time> <host>: <date> <time> <timezone>: %USER-6-SYSTEM_MSG: [ssl:info] [pid 7998:tid 1898969920] SSL Library Error: error:1408F081:SSL routines:SSL3_GET_RECORD:block cipher pad is wrong - httpd[7998] Wrong version: <date> <time> <host>: <date> <time> <timezone>: %USER-6-SYSTEM_MSG: [ssl:info] [pid 8009:tid 1881144128] SSL Library Error: error:14076129:SSL routines:SSL23_GET_CLIENT_HELLO:only tls allowed in fips mode - httpd[8009] General Failure: <date> <time> <host>: <date> <time> <timezone>: %USER-6-SYSTEM_MSG: [ssl:info] [pid 8001:tid 1739586368] [client 10.6.16.45:59026] AH02008: SSL library error 1 in handshake (server 10.6.16.218:443) - httpd[8001] <date> <time> <host>: <date> <time> <timezone>: %DAEMON-3-SYSTEM_MSG: error: maximum authentication attempts exceeded for admin2 from 10.6.16.15 port 55990 ssh2 - sshd[10714]
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	FMC, FXOS and FTD	**FTD:** SSH: <date> <time> <host> sshd[24776]: error: maximum authentication attempts exceeded for testuser from 10.6.16.46 port 45216 ssh2 [preauth] **FMC:** TLS: <date> <time> <host> login.cgi: <host>: testuser@10.6.16.45, Login, Login Failed <date> <time> <host> login.cgi: <host>: testuser@10.6.16.45, Login, Account Locked **FXOS:** SSH: <date> <time> <host>: <date> <time> <timezone>: %DAEMON-3-SYSTEM_MSG: error: maximum authentication attempts exceeded for admin2 from 10.6.16.15 port 55990 ssh2 - sshd[10714] TLS: <date> <time> <host>: <date> <time> <timezone>: %AUTHPRIV-3-SYSTEM_MSG: pam_tally2(aaa:auth): conversation failed - aaad <date> <time> <host>: <date> <time> <timezone>: %AUTHPRIV-5-SYSTEM_MSG: pam_tally2(aaa:auth): user tempuser (2007) tally 3, deny 2 - aaad

SFR	Auditable Event	Distributed TOE audit generation	Actual Audited Event
			<date> <time> <host>: <date> <time> <timezone>: %AUTHPRIV-5-SYSTEM_MSG: pam_unix(aaa:auth): authentication failure; logname= uid=0 euid=0 tty= ruser= rhost= user=tempuser – aaad
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	FMC, FXOS and FTD	**FTD:** Console Success: Not applicable (enforced by FXOS). Console Failure: Not applicable (enforced by FXOS). SSH Login Success: <date> <time> <host> sshd[16163]: Accepted keyboard-interactive/pam for admin from 10.6.16.46 port 50556 ssh2 <date> <time> <host> sshd[16163]: pam_unix(sshd:session): session opened for user admin by (uid=0) SSH Login Failure: <date> <time> <host> sshd[14773]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.6.16.46 user=admin <date> <time> <host> sshd[14733]: error: PAM: Authentication failure for admin from 10.6.16.46 SSH Public Key Success: <date> <time> <host>sshd[66781]: Accepted publickey for admin from 10.6.16.46 port 50550 ssh2: RSA SHA256:2cnR+gpbgVVqxRqHpKi0cDRrp1wKDqeXjuLYYsjEeis <date> <time> <host> sshd[66781]: pam_unix(sshd:session): session opened for user admin by (uid=0) SSH Public Key Failure: <date> <time> <host> sshd[51258]: Postponed keyboard-interactive for admin from 10.6.16.46 port 50544 ssh2 [preauth] **FMC:** Console Login Success: <date> <time> <host> login[7684]: pam_unix(login:session): session opened for user admin by LOGIN(uid=0) Console Login Failure: <date> <time> <host> login[7684]: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=/dev/ttyS0 ruser= rhost= user=admin <date> <time> <host>login[7684]: FAILED LOGIN (1) on '/dev/ttyS0' FOR 'admin', Authentication failure SSH Login Success: <date> <time> <host> sshd[6518]: Accepted keyboard-interactive/pam for admin from 10.6.16.46 port 47680 ssh2 <date> <time> <host> sshd[6518]: pam_unix(sshd:session): session opened for user admin by (uid=0) SSH Login Failure: <date> <time> <host> sshd[6354]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.6.16.46 user=admin <date> <time> <host> sshd[6351]: error: PAM: Authentication failure for admin from 10.6.16.46 SSH Public Key Success: <date> <time> <host> sshd[23895]: Accepted publickey for admin from 10.6.16.46 port 52474 ssh2: RSA SHA256:f0h+AIMnU4GtMnLhx4+l1TsjNL78E1XSdTZVGl6AdFU <date> <time> <host> sshd[23895]: pam_unix(sshd:session): session opened for user admin by (uid=0) SSH Public Key Failure:

SFR	Auditable Event	Distributed TOE audit generation	Actual Audited Event
			<date> <time> <host> sshd[24147]: Operating in CiscoSSL FIPS mode\n <date> <time> <host> sshd[24147]: Postponed keyboard-interactive for admin from 10.6.16.46 port 52476 ssh2 [preauth] WebUI Success: <date> <time> <host> login.cgi: <host>: <user>@10.6.16.45, Login, Login Success WebUI Failure: <date> <time> <host> login.cgi: <host>: <user>@10.6.16.45, Login, Login Failed **FXOS:** Console Success: <date> <time> <host>: <date> <time> <timezone>: %FPRM-6-AUDIT: [session][internal][creation][internal][1692857][sys/user-ext/sh-login-admin-ttyS0_1_18512][id:ttyS0_1_18512, name:admin, policyOwner:local][] Fabric A: local user admin logged in from console Console Failure: <date> <time> <host>: <date> <time> <timezone>: %AUTHPRIV-3-SYSTEM_MSG: pam_aaa:Authentication failed from console – login SSH Success: <date> <time> <host>: <date> <time> <timezone>: %FPRM-6-AUDIT: [session][internal][creation][internal][1692860][sys/user-ext/sh-login-admin-pts_0_1_18813][id:pts_0_1_18813, name:admin, policyOwner:local][] Fabric A: local user admin logged in from 192.168.144.46 SSH Failure: <date> <time> <host>: <date> <time> <timezone>: %AUTHPRIV-3-SYSTEM_MSG: pam_aaa:Authentication failed from 192.168.144.46 - sshd[17813] SSH Public Key Success: <date> <time> <host>: <date> <time> <timezone>: %FPRM-6-AUDIT: [session][internal][creation][internal][1712515][sys/user-ext/sh-login-testpub-pts_1_1_24183][id:pts_1_1_24183, name:testpub, policyOwner:local][] Fabric A: local user testpub logged in from 192.168.144.46 SSH Public Key Failure: <date> <time> <host>: <date> <time> <timezone>: %DAEMON-6-SYSTEM_MSG: Failed publickey for testpub from 192.168.144.46 port 60874 ssh2 - sshd[25022] Web UI Success: <date> <time> <host>: <date> <time> <timezone>: %FPRM-6-AUDIT: [session][internal][creation][internal][1692864][sys/user-ext/web-login-admin-web_17208_A][id:web_17208_A, name:admin, policyOwner:local][] Web A: local user admin logged in from 10.6.16.47 Web UI Failure: <date> <time> <host>: <date> <time> <timezone>: %AUTHPRIV-3-SYSTEM_MSG: pam_aaa:Authentication failed from 10.6.16.47 - httpd[8016]
FIA_UAU_EXT.2	All use of the identification and authentication mechanism.	FMC, FXOS and FTD	See FIA_UIA_EXT.1

SFR	Auditable Event	Distributed TOE audit generation	Actual Audited Event
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate Any addition, replacement or removal of trust anchors in the TOE's trust store Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store	FMC, FXOS and FTD	**FTD:** TLS: Trust Anchor Addition: <date> <time> <host> %FTD-5-111008: User 'enable_1' executed the 'crypto ca trustpoint rootca-rsa-no-revocation' command. <date> <time> <host> %FTD-5-111010: User 'enable_1', running 'N/A' from IP 0.0.0.0, executed 'crypto ca trustpoint rootca-rsa-no-revocation' <date> <time> <host> %FTD-5-111008: User 'enable_1' executed the 'crypto ca authenticate rootca-rsa-no-revocation nointeractive' command. <date> <time> <host> %FTD-5-111010: User 'enable_1', running 'N/A' from IP 0.0.0.0, executed 'crypto ca authenticate rootca-rsa-no-revocation nointeractive' <date> <time> <host> %FTD-5-111008: User 'enable_1' executed the 'crypto ca enroll rootca-rsa-no-revocation noconfirm' command. Trust Anchor Deletion: <date> <time> <host> %FTD-5-111008: User 'enable_1' executed the 'no crypto ca trustpoint rootca-rsa-no-revocation noconfirm' command. <date> <time> <host> %FTD-5-111010: User 'enable_1', running 'N/A' from IP 0.0.0.0, executed 'no crypto ca trustpoint rootca-rsa-no-revocation noconfirm' Expired cert: <date> <time> <host> %FTD-7-711001: #012CRYPTO_PKI: Certificate expired or not-yet-valid Corrupt ASN.1: <date> <time> <host>: %FTD-7-725014: SSL lib error. Function: ssl3_get_server_certificate Reason: ASN1 lib Invalid Ca or Signature: <date> <time> <host> %FTD-3-717027: Certificate chain failed validation. Certificate chain is either invalid or not authorized. Revoked cert using CRL: <date> <time> <host> %FTD-3-717027: Certificate chain failed validation. Certificate is revoked. Revoked cert using OCSP: <date> <time> <host> %FTD-7-711001: #012CRYPTO_PKI: OCSP polling for trustpoint rootca-rsa-ocsp succeeded. Certificate status is REVOKED. No CRLSign Purpose: <date> <time> <host> %FTD-7-711001: CRYPTO_PKI:check_key_usage: Incorrect KeyUsage (188) for usage type: CRL Signing No OCSPSign Purpose: <date> <time> <host> %FTD-7-711001: #012CRYPTO_PKI: OCSP response is not signed by the peer_cert CA, a trusted certificate or a delegated responder. Invalid Chain: <date> <time> <host> %FTD-3-717027: Certificate chain failed validation. No suitable trustpoint was found to validate chain. Explicit EC Certificate: <date> <time> <host> %FTD-3-717027: Certificate chain failed validation. Certificate chain is either invalid or not authorized. <date> <time> <host> %FTD-7-725014: SSL lib error. Function: ssl3_get_server_certificate Reason: certificate verify failed <date> <time> <host> %FTD-7-725014: SSL lib error. Function: ssl3_connect Reason: unknown state IPsec:

SFR	Auditable Event	Distributed TOE audit generation	Actual Audited Event
			Expired cert: <date> <time> <host> %FTD-3-717009: Certificate validation failed. Certificate date is out-of-range, serial number: 72, subject name: e=server-expired-ecdsa@gossamersec.com,cn=tl15-16x.example.com,o=GCT,l=Catonsville,st=MD,c=US. Corrupt ASN.1: <date> <time> <host> %FTD-3-751006: Local:192.168.144.221:500 Remote:192.168.144.46:500 Username:Unknown IKEv2 Certificate authentication failed. Error: Failed to populate peer certificate chain for validation Invalid Signature: <date> <time> <host> %FTD-3-717027: Certificate chain failed validation. Certificate is either invalid or not authorized, serial number: 5A, subject name: e=server-ecdsa@gossamersec.com,cn=tl15-16x.example.com,o=GCT,l=Catonsville,st=MD,c=US. Invalid CA: <date> <time> <host> %FTD-3-717009: Certificate validation failed. No suitable trustpoints found to validate certificate serial number: 7A, subject name: e=server-issued-by-no-basic-constraints-ecdsa@gossamersec.com,cn=tl15-16x.example.com,o=GCT,l=Catonsville,st=MD,c=US, issuer name: e=subsubca-no-basic-constraints-ecdsa@gossamersec.com,cn=subsubca-no-basic-constraints-ecdsa,o=GCT,l=Catonsville,st=MD,c=US . CRL Revoked cert: <date> <time> <host> %FTD-3-717009: Certificate validation failed. Certificate is revoked, serial number: 00B0, subject name: e=server-revoked-ecdsa@gossamersec.com,cn=tl15-16x.example.com,o=GCT,l=Catonsville,st=MD,c=US. OCSP Revoked cert: <date> <time> <host> %FTD-3-717027: Certificate chain failed validation. Generic error occurred, serial number: 1D, subject name: e=subca-revoked-ecdsa@gossamersec.com,cn=subca-revoked-ecdsa,o=GCT,l=Catonsville,st=MD,c=US. No OCSP/CRL signing purpose: <date> <time> <host> %FTD-3-717032: OCSP status check failed. Reason: Failed to verify OCSP response. <date> <time> <host> %FTD-3-717027: Certificate chain failed validation. Revocation status check polling failed for certificate, serial number: 09, subject name: e=subca-ecdsa@gossamersec.com,cn=subca-ecdsa,o=GCT,l=Catonsville,st=MD,c=US. Invalid Chain: <date> <time> <host> %FTD-3-717027: Certificate chain failed validation. No suitable trustpoint was found to validate chain. Explicit EC Certificate: <date> <time> <host> %FTD-3-717027: Certificate chain failed validation. Certificate chain is either invalid or not authorized.

SFR	Auditable Event	Distributed TOE audit generation	Actual Audited Event
			<date> <time> <host> %FTD-3-751006: Local:192.168.144.221:500 Remote:192.168.144.46:500 Username:192.168.144.46 IKEv2 Certificate authentication failed. Error: Certificate authentication failed **FMC:** TLS: Trust Anchor Addition: <date> <time> <host> SF-IMS[14865]: HTTPSCert:InstallCertificate [INFO] Cert Added: F5_client-TOE-00-rsa_rootca-rsa Trust Anchor Deletion: <date> <time> <host> SF-IMS[13985]: HTTPSCert:DeleteCertificate [INFO] Cert Deleted: F1_client-TOE-00-rsa_rootca-rsa Expired cert: <date> <time> <host> syslog-ng[5115]: X509 Certificate Validation; depth='0', ok='0', errnum='10', error='certificate has expired' Corrupt ASN.1: <date> <time> <host> syslog-ng[5403]: SSL error while writing stream; tls_error='asn1 encoding routines:ASN1_CHECK_TLEN:wrong tag' Invalid Signature: <date> <time> <host> syslog-ng[5697]: X509 Certificate Validation; depth='0', ok='0', errnum='7', error='certificate signature failure' Invalid CA: <date> <time> <host> syslog-ng[10519]: X509 Certificate Validation; depth='1', ok='0', errnum='24', error='invalid CA certificate' Revoked cert: <date> <time> <host> syslog-ng[9301]: X509 Certificate Validation; depth='0', ok='0', errnum='23', error='certificate revoked' Invalid Chain: <date> <time> <host> syslog-ng[15124]: X509 Certificate Validation; depth='1', ok='0', errnum='19', error='self signed certificate in certificate chain' Explicit EC Certificate: <date> <time> <host> syslog-ng[2338]: Certificate validation failed; subject='emailAddress=server-issued-by-explicit-ecdsa@gossamersec.com, CN=tl15-16x.example.com, O=GCT, L=Catonsville, ST=MD, C=US', issuer='emailAddress=subsubca-explicit-ecdsa@gossamersec.com, CN=subsubca-explicit-ecdsa, O=GCT, L=Catonsville, ST=MD, C=US', error='certificate signature failure', depth='0' Sep 15 18:21:42 <host> syslog-ng[2338]: SSL error while writing stream; tls_error='(null):ECDSA_verify:(null)' **FXOS:** Trust Anchor Addition: <date> <time> <host>: <date> <time> <timezone>: %FPRM-6-AUDIT: [admin][admin][creation][ttyS0_1_18512][1694196][sys/pki-ext/tp-rsa-unaccept][certChain:-----BEGIN CERTIFICATE----- MIIEnzCCA4egAwIBAgIDAQABMA0GCSqGSIb3DQEBCwUAMIHvMQswCQYDVQQGEwJV UzELMAkGA1UECAwCTUQxFDASBgNVBAcMC0NhdG9uc3ZpbGxlMTYwNAYJKoZIhvcN AQkBFidyb290Y2

SFR	Auditable Event	Distributed TOE audit generation	Actual Audited Event
			<date> <time> <host>: <date> <time> <timezone>: %FPRM-6-EVENT: [E4195252][1694197][transition][internal][] [FSM:STAGE:STALE-SUCCESS]: keyring configuration on primary(FSM-STAGE:sam:dme:PkiEpUpdateEp:SetKeyRingLocal) Trust Anchor Deletion: <date> <time> <host>: <date> <time> <timezone>: %FPRM-6-AUDIT: [admin][admin][deletion][ttyS0_1_18512][1694209][sys/pki-ext/tp-rsa-unaccept][sys/pki-ext/tp-rsa-unaccept][] Trustpoint rsa-unaccept deleted <date> <time> <host>: <date> <time> <timezone>: %FPRM-6-AUDIT: [admin][admin][deletion][ttyS0_1_18512][1694210][sys/pki-ext/tp-rsa-unaccept][sys/pki-ext/tp-rsa-unaccept][] TP non-retrievable(265:777) Revocation deleted <date> <time> <host>: <date> <time> <timezone>: %FPRM-6-EVENT: [E4195252][1694211][transition][internal][] [FSM:STAGE:STALE-SUCCESS]: keyring configuration on primary(FSM-STAGE:sam:dme:PkiEpUpdateEp:SetKeyRingLocal) IPsec: Expired cert: <date> <time> <host>: <date> <time> <timezone>: %AUTHPRIV-6-SYSTEM_MSG: 01[CFG] subject certificate invalid (valid from Apr 22 11:30:52 2020 to Apr 22 11:35:00 2020) - charon-custom Corrupt ASN.1 / Invalid Signature / Invalid CA / Invalid Chain: <date> <time> <host>: <date> <time> <timezone>: %AUTHPRIV-6-SYSTEM_MSG: 04[IKE] no trusted RSA public key found for '10.6.16.46' - charon-custom Revoked cert: <date> <time> <host>: <date> <time> <timezone>: %AUTHPRIV-6-SYSTEM_MSG: 15[CFG] certificate was revoked on Apr 22 15:31:59 UTC 2020, reason: unspecified - charon-custom Invalid Revocation Signing Certificate: <date> <time> <host>: <date> <time> <timezone>: %AUTHPRIV-6-SYSTEM_MSG: 08[CFG] constraint check failed: RULE_CRL_VALIDATION is FAILED, but requires at least GOOD - charon-custom
FIA_X509_EXT.1/ITT	Unsuccessful attempt to validate a certificate Any addition, replacement or removal of trust anchors in the TOE's trust store Reason for failure of certificate validation	FMC and FTD	**FTD:** Trust Anchor Addition: Refer to FIA_X509_EXT.1/Rev Trust Anchor Deletion: Refer to FIA_X509_EXT.1/Rev Expired cert: <date> <time> <host> SF-IMS[34769]: [41667] sftunneld:sf_ssl [ERROR] err 10:certificate has expired Corrupt ASN.1: <date> <time> <host> SF-IMS[34769]: [61309] sftunneld:sf_ssl [WARN] Could not receive Message: General read error Invalid Signature: <date> <time> <host> SF-IMS[34769]: [66389] sftunneld:sf_ssl [ERROR] err 7:certificate signature failure Invalid CA: <date> <time> <host> SF-IMS[38801]: [38810] sftunneld:sf_ssl [ERROR] err 19:self signed certificate in certificate chain <date> <time> <host> SF-IMS[41546]: [42675] sftunneld:sf_ssl [ERROR] err 24:invalid CA certificate Invalid Chain:

SFR	Auditable Event	Distributed TOE audit generation	Actual Audited Event
	Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store		<date> <time> <host> SF-IMS[16940]: [16948] sftunneld:sf_ssl [ERROR] err 19:self signed certificate in certificate chain **FMC:** Trust Anchor Addition: <date> <time> <host> SF-IMS[14865]: HTTPSCert:InstallCertificate [INFO] Cert Added: F5_client-TOE-00-rsa_rootca-rsa Trust Anchor Deletion: <date> <time> <host> SF-IMS[13985]: HTTPSCert:DeleteCertificate [INFO] Cert Deleted: F1_client-TOE-00-rsa_rootca-rsa Expired cert: <date> <time> <host> SF-IMS[28844]: [25530] sftunneld:sf_ssl [ERROR] err 10:certificate has expired Corrupt ASN.1: <date> <time> <host> SF-IMS[28844]: [25959] sftunneld:sf_ssl [ERROR] SSL_renegotiate error: 1: error:00000001:lib(0):func(0):reason(1) Invalid Signature: <date> <time> <host> SF-IMS[28844]: [25984] sftunneld:sf_ssl [ERROR] err 7:certificate signature failure Invalid CA: <date> <time> <host> SF-IMS[28844]: [26310] sftunneld:sf_ssl [ERROR] err 24:invalid CA certificate Invalid Chain: <date> <time> <host> SF-IMS[1278]: [1285] sftunneld:sf_ssl [ERROR] err 20:unable to get local issuer certificate **FXOS:** Not applicable.
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update	FTD, FMC and FXOS	**FTD:** See FPT_TUD_EXT.1 **FMC:** <date> <time> <host> SF-IMS[27507]: [27507] Cisco_Firepower_Mgmt_Center_Patch-6.4.0.1-17:000_start/100_start_messages.sh [INFO] Upgrade starting **FXOS:** <date> <time> <host>: <date> <time> <timezone>: %FPRM-6-EVENT: [E4196668][1683931][transition][internal][] [FSM:BEGIN]: Firmware Upgrade of FPR system(FSM:sam:dme:FirmwareSystemDeploy)
FMT_SMF.1	All management activities of TSF data.	FTD, FMC and FXOS	**FTD:** <date> <time> <host> sfdccsm: fmcv-new2: <user>@10.6.16.47, Devices > Platform Settings > Platform Settings Editor, Modified: Banner#000x0a#000x00 <date> <time> <host> sfdccsm: fmcv-new2: <user>@10.6.16.47, Devices > Platform Settings > Platform Settings Editor, Modified: Timeouts#000x0a#000x00

SFR	Auditable Event	Distributed TOE audit generation	Actual Audited Event
			Ability to verify updates: <date> <time> <host> sudo: www : TTY=unknown ; PWD=/usr/local/sf/htdocs/admin ; USER=root ; COMMAND=/usr/local/sf/bin/verify_signed_image.sh -m -s /var/tmp/sigstatus_uFHnPAWr -i /var/sf/updates/Cisco_FTD_SSP_Patch-6.4.0.1-17.sh.REL.tar <date> <time> <host> sudo: admin : TTY=pts/0 ; PWD=/home/admin ; USER=root ; COMMAND=/usr/local/sf/bin/cli_usrmgr maxf testuser 5 <date> <time> <host> sfdccsm: <host>: <user>@10.6.16.47, Devices > Platform Settings > Platform Settings Editor, Modified: SSL IKE SA lifetime: <date> <time> <host> sfdccsm: fmcv-new2: <user>@10.6.16.47, Objects > Object Management > IKEv2_Policy, save gct-aes-sha ESP SA lifetime: <date> <time> <host> sfdccsm: fmcv-new2: <user>@10.6.16.47, Device > VPN > FTD S2S, Update VPN Topology Entry gctvpn <date> <time> <host> sfdccsm: <host>: <user>@10.6.16.47, Device > Certificates, Add new Certificate - rootca-ecdsa-no-revocation on device fp4140ftd <date> <time> <host> sfdccsm: <host>: <user>@10.6.16.47, Device > Certificates, Display Certificate List **FMC:** <date> <time> <host> platformSettingEdit.cgi: <host>: <user>@10.6.16.45, Devices > Platform Settings > Login Banner > Modified: Custom Login Banner This is a GCT banner to test FTA_TAB.1. > This is a GCT banner to test FTA_TAB.1 <date> <time> <host> platformSettingEdit.cgi: <host>: <user>@10.6.16.45, Shell Timeout, Browser/Shell timeout changed Ability to verify updates: <date> <time> <host> sudo: www : TTY=unknown ; PWD=/usr/local/sf/htdocs/admin ; USER=root ; COMMAND=/usr/local/sf/bin/verify_signed_image.sh -m -s /var/tmp/sigstatus_ujPyp8Pv -i /var/sf/updates/Cisco_Firepower_Mgmt_Center_Hotfix_BG-6.4.0.10-2.sh.REL.tar <date> <time> <host> user.cgi: <host>: <user>@10.6.16.45, System > Local > User Management > Users, Edited user – testuser <date> <time> <host> sfdccsm: <host>: <user>@10.6.16.47, Devices > Platform Settings > Platform Settings Editor, Modified: SSL IKE SA lifetime: <date> <time> <host> sfdccsm: <host>: <user>@10.6.16.47, Objects > Object Management > IKEv2_Policy, save aes-vpn-algs ESP SA lifetime: <date> <time> <host> sfdccsm: <host>: <user>@10.6.16.47, Device > VPN > FTD S2S, Update VPN Topology Entry gct-vpn <date> <time> <host> SF-IMS[2124]: HTTPSCert:InstallCertificate [INFO] Certificate Chain added <date> <time> <host> SF-IMS[2124]: HTTPSCert:InstallCertificate [INFO] Cert Added: 010D_client-TOE-00-rsa_rootca-rsa **FXOS:** <date> <time> <host>: <date> <time> <timezone>: %FPRM-6-AUDIT: [admin][admin][creation][ttyS0_1_21358][537599][sys/user-ext/pre-login-banner][message:GCT Test Banner! , policyOwner:local][] PreLoginBanner created

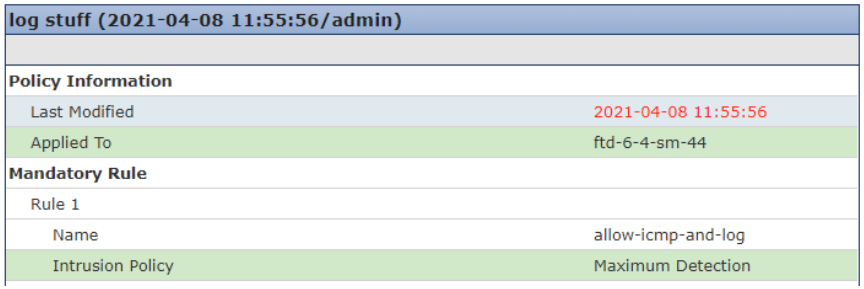
SFR	Auditable Event	Distributed TOE audit generation	Actual Audited Event
			<date> <time> <host>: <date> <time> <timezone>: %FPRM-6-AUDIT: [admin][admin][modification][pts_1_1_8348][1174156][sys/auth-realm/default-auth][conSessionTimeout(Old:3600, New:60), sessionTimeout(Old:3600, New:60)][] Default authentication configuration modified <date> <time> <host>: <date> <time> <timezone>: %FPRM-6-EVENT: [E4195293][1683673][transition][internal][] [FSM:STAGE:STALE-SUCCESS]: downloading image or file fxos-k9.2.6.1.204.SPA from (FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local) <date> <time> <host>: <date> <time> <timezone>: %FPRM-6-EVENT: [E4196668][1683931][transition][internal][] [FSM:BEGIN]: Firmware Upgrade of FPR system(FSM:sam:dme:FirmwareSystemDeploy) <date> <time> <host>: <date> <time> <timezone>: %FPRM-6-EVENT: [E4195249][1692764][transition][internal][] [FSM:STAGE:STALE-SUCCESS]: user configuration to primary(FSM-STAGE:sam:dme:AaaUserEpUpdateUserEp:SetUserLocal) <date> <time> <host>: <date> <time> <timezone>: %FPRM-6-AUDIT: [admin][admin][modification][ttyS0_1_8443][1740427][sys/pki-ext/keyring-default][regen(Old:no, New:yes)][] Keyring default modified <date> <time> <host>: <date> <time> <timezone>: %FPRM-6-AUDIT: [admin][admin][modification][ttyS0_1_24085][1692728][sys/ipsec-ext/conn-gctipsec][ikeRekeyTime(Old:240, New:60)][] Ipsec Connection gctipsec modified <date> <time> <host>: <date> <time> <timezone>: %FPRM-6-AUDIT: [admin][admin][modification][ttyS0_1_24085][1692736][sys/ipsec-ext/conn-gctipsec][espRekeyTime(Old:60, New:45)][] Ipsec Connection gctipsec modified <date> <time> <host>: <date> <time> <timezone>: %FPRM-6-EVENT: [E4195252][1692716][transition][internal][] [FSM:STAGE:STALE-SUCCESS]: keyring configuration on primary(FSM-STAGE:sam:dme:PkiEpUpdateEp:SetKeyRingLocal)
FPT_ITT.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions. Identification of the initiator and target of failed trusted channels establishment attempt.	FTD and FMC	**FTD:** Initiation: <date> <time> <host> SF-IMS[12866]: [12873] sfmbservice:sfmb_service [INFO] Established connection to peer 10.6.16.223 Termination: <date> <time> <host> SF-IMS[60163]: [47010] sfmbservice:sfmb_service [INFO] Connection closed to host 10.6.16.223 Failure: <date> <time> <host> SF-IMS[34769]: [68858] sftunneld:sf_ssl [ERROR] Connect:SSL handshake failed **FMC:** Initiation: <date> <time> <host> SF-IMS[19106]: [19420] sfmbservice:sfmb_service [INFO] Established connection to peer 10.6.16.221 Termination: <date> <time> <host> SF-IMS[22235]: [25609] sfmbservice:sfmb_service [INFO] Connection closed to host 10.6.16.221 Failure: <date> <time> <host> SF-IMS[9336]: [2438] sftunneld:sf_ssl [ERROR] Connect:SSL handshake failed

SFR	Auditable Event	Distributed TOE audit generation	Actual Audited Event
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	FMC, FXOS and FTD	**FTD:** Initiation: <date> <time> <host> SF-IMS[6266]: [6266] sftunneld:stream_file [INFO] INITIATED SRC: : File copy 0 % completed, 0 bytes of file copied out of 0 Success: <date> <time> <host> SF-IMS[6266]: [6266] sftunneld:stream_file [INFO] ELASTIC_FSTREAM status:: File copy 100 % completed, 99891200 bytes of file copied out of 99891200 <date> <time> <host> SF-IMS[6266]: [6266] sftunneld:control_services [INFO] FSTREAM_STATUS: Sending back task status 'Completed' Failure: <date> <time> <host> SF-IMS[13645]: update.cgi:ProcessUpdateUpload [ERROR] update failed signature verification: file = Cisco_Firepower_Mgmt_Center_Patch-6.4.0.1-17.sh.REL-no_sig.tar **FMC:** Initiation: <date> <time> <host> SF-IMS[27507]: [27507] Cisco_Firepower_Mgmt_Center_Patch-6.4.0.1-17:000_start/100_start_messages.sh [INFO] Upgrade starting Success: <date> <time> <host> SF-IMS[32329]: [32329] Cisco_Firepower_Mgmt_Center_Patch-6.4.0.1-17:999_finish/999_z_complete_upgrade_message.sh [INFO] Upgrade complete Failure: <date> <time> <host> SF-IMS[27569]: update.cgi:ProcessUpdateUpload [ERROR] update failed signature verification: file = Cisco_Firepower_Mgmt_Center_Patch-6.4.0.10-95.sh.REL-modified.tar **FXOS:** Initiation: <date> <time> <host>: <date> <time> <timezone>: %FPRM-6-EVENT: [E4196668][1683931][transition][internal][] [FSM:BEGIN]: Firmware Upgrade of FPR system(FSM:sam:dme:FirmwareSystemDeploy) Success: <date> <time> <host>: <date> <time> <timezone>: %FPRM-6-EVENT: [E4197943][1684261][transition][internal][] [FSM:STAGE:END]: Update FPRM(FSM-STAGE:sam:dme:MgmtControllerUpdateSwitch:UpdateManager) Failure: <date> <time> <host>: <date> <time> <timezone>: %FPRM-6-EVENT: [E4195293][818485][transition][internal][] [FSM:STAGE:REMOTE-ERROR]: Result: end-point-failed Code: ERR-DNLD-invalid-image Message: invalid image#(sam:dme:FirmwareDownloaderDownload:Local) <date> <time> <host>: <date> <time> <timezone>: %FPRM-6-EVENT: [E4195293][818487][transition][internal][] [FSM:STAGE:FAILED]: downloading image or file fxos-k9.2.6.1.157.badSig.SPA from (FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
FPT_STM_EXT.1	Discontinuous changes to time -	FMC, FXOS and FTD	**FTD:**

SFR	Auditable Event	Distributed TOE audit generation	Actual Audited Event
	either Administrator actuated or changed via an automated process For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).		<date> <time> <host> %FTD-5-771002: CLOCK: System clock set, source: Chassis SSPXRU, IP: 127.128.254.1, before: 10:17:23.999 EDT Sun Sep 27 2020, after: 10:08:10.000 EDT Mon Sep 9 2019 **FMC:** <date> <time> <host> mojo_server.pl: <host>: <user>@10.6.16.47, Updated time to Thu 31 Jan 2019 04:30:00 AM EST from Wed 03 Jun 2020 02:05:31 PM EDT, Save **FXOS:** <date> <time> <host>: <date> <time> <timezone>: %FPRM-6-AUDIT: [admin][admin][modification][internal][1574934][aaa-log][aaa-log][] switch A: cmd: previous time: Wed Jun 3 13:33:22 EDT 2020 new time: set clock Tue Jan 1 11:30:00 2019, logged in from console on term /dev/ttyS0: Local mgmt command executed
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	FMC and FXOS	**FTD:** Not applicable (enforced by FXOS). **FMC:** <date> <time> <host> expire-session.pl: <host>: <user>@local, Session Expiration, Session terminated on ttyS0 due to inactivity (admin) **FXOS:** <date> <time> <host>: <date> <time> <timezone>: %FPRM-6-AUDIT: [session][internal][deletion][internal][1174239][sys/user-ext/user-admin/term-pts_1_1_13310][sys/user-ext/user-admin/term-pts_1_1_13310][] Fabric A: system terminated session id pts_1_1_13310 of user admin due to idle timeout
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	FTD, FMC and FXOS	**FTD:** SSH Idle Timeout: <date> <time> <host> sshd[29904]: Received disconnect from 10.6.16.46 port 51368:11: disconnected by user <date> <time> <host> sshd[29904]: Disconnected from user admin 10.6.16.46 port 51368 **FMC:** WebUI Session Lock: <date> <time> <host> expire-session.pl: <host>: <user>@Default User IP, Session Expiration, Session expired due to inactivity (admin) SSH Session Lock: <date> <time> <host> expire-session.pl: <host>: <user>@10.6.16.46, Session Expiration, Session terminated on pts/0 due to inactivity (admin) <date> <time> <host> sshd[1700]: pam_unix(sshd:session): session closed for user admin **FXOS:**

SFR	Auditable Event	Distributed TOE audit generation	Actual Audited Event
			WebUI: <date> <time> <host>: <date> <time> <timezone>: %FPRM-6-AUDIT: [session][internal][deletion][internal][1174397][sys/user-ext/user-admin/term-web_54651_A][sys/user-ext/user-admin/term-web_54651_A][] Web A: system terminated Web session id web_54651_A of user admin due to idle timeout SSH: <date> <time> <host>: <date> <time> <timezone>: %FPRM-6-AUDIT: [session][internal][deletion][internal][549174][sys/user-ext/user-admin/term-ttyS0_1_10103][sys/user-ext/user-admin/term-ttyS0_1_10103][] Fabric A: system terminated session id ttyS0_1_10103 of user admin due to idle timeout
FTA_SSL.4	The termination of an interactive session.	FTD, FMC and FXOS	**FTD:** Console logout: Not applicable (enforced by FXOS). SSH Logout: <date> <time> <host> sshd[51899]: Received disconnect from 10.6.16.46 port 42314:11: disconnected by user <date> <time> <host> sshd[51899]: Disconnected from user admin 10.6.16.46 port 42314 **FMC:** WebUI Logout: <date> <time> <host> login.cgi: <host>: <user>@10.6.16.45, Logout, Logout Success Console Logout: <date> <time> <host> login[5660]: pam_unix(login:session): session closed for user admin SSH Logout: <date> <time> <host> sshd[7843]: Received disconnect from 10.6.16.46 port 47538:11: disconnected by user <date> <time> <host> sshd[7843]: Disconnected from 10.6.16.46 port 47538 <date> <time> <host> sshd[7837]: pam_unix(sshd:session): session closed for user admin **FXOS:** Console Logout: <date> <time> <host>: <date> <time> <timezone>: %AUTHPRIV-6-SYSTEM_MSG: pam_unix(login:session): session closed for user admin - login SSH Logout: <date> <time> <host>: <date> <time> <timezone>: %AUTHPRIV-6-SYSTEM_MSG: pam_unix(sshd:session): session closed for user admin - sshd[17776] WebUI Logout: <date> <time> <host>: <date> <time> <timezone>: %FPRM-6-AUDIT: [session][internal][deletion][internal][514507][sys/user-ext/user-admin/term-web_40033_A][sys/user-ext/user-admin/term-web_40033_A][] Web A: user admin terminated session id web_40033_A
FTP_ITC.1	Initiation of the trusted channel.	FMC, FXOS and FTD	All of the failure audits are covered in FCS_TLSC_EXT and FCS_TLSS_EXT. **FTD:**

SFR	Auditable Event	Distributed TOE audit generation	Actual Audited Event
	Termination of the trusted channel. Failure of the trusted channel functions. Identification of the initiator and target of failed trusted channels establishment attempt		Initiation of Syslog over TLS (Lina) sessions: <date> <time> <host> EDT: %FTD-6-725001: Starting SSL handshake with server outside:192.168.144.221/52679 to 192.168.144.46/6514 for TLS session Termination of Syslog over TLS (Lina) sessions: <date> <time> <host> EDT: %FTD-6-725007: SSL session with server outside:192.168.144.221/65429 to 192.168.144.46/6514 terminated Initiation of Syslog over TLS (FTDOS) sessions: <date> <time> <host> syslog-ng[59354]: syslog-ng starting up; version='3.6.2' Termination of Syslog over TLS (FTDOS) sessions: <date> <time> <host> syslog-ng[59256]: syslog-ng shutting down; version='3.6.2' Initiation of IPSec sessions: <date> <time> <host> EDT: %FTD-7-302015: Built inbound UDP connection 547 for outside:192.168.144.46/4500 (192.168.144.46/4500) to identity:192.168.144.221/4500 (192.168.144.221/4500) Termination of IPSec sessions: <date> <time> <host> EDT: %FTD-7-302016: Teardown UDP connection 547 for outside:192.168.144.46/4500 to identity:192.168.144.221/4500 duration 0:00:05 bytes 3020 **FMC:** Initiation/Establishment of Syslog over TLS sessions: <date> <time> <host> syslog-ng[4946]: Syslog connection established; fd='17', server='AF_INET(10.6.16.46:6514)', local='AF_INET(0.0.0.0:0)' Termination of Syslog over TLS sessions: <date> <time> <host> syslog-ng[4946]: Syslog connection broken; fd='17', server='AF_INET(10.6.16.46:6514)', time_reopen='60' **FXOS:** Initiation of IPsec sessions: <date> <time> <host>: <date> <time> <timezone>: %AUTHPRIV-6-SYSTEM_MSG: 10[IKE] initiating IKE_SA gctipsec[20] to 10.6.16.43 - charon-custom Termination of IPSec sessions: <date> <time> <host>: <date> <time> <timezone>: %AUTHPRIV-6-SYSTEM_MSG: 10[IKE] deleting IKE_SA gctipsec[2] between 10.6.16.218[CN=10.6.16.218]...10.6.16.43[10.6.16.43] - charon-custom
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failures of the trusted path functions.	FTD, FMC and FXOS	**FTD:** Covered in FCS_SSHS_EXT.1, FIA_UIA_EXT.1, FTA_SSL.4 **FMC:** Covered in FCS_SSHS_EXT.1, FIA_UIA_EXT.1, FTA_SSL.4 and FCS_TLSS_EXT.1 **FXOS:** Covered in FCS_SSHS_EXT.1, FIA_UIA_EXT.1, FTA_SSL.4 and FCS_TLSS_EXT.1

SFR	Auditable Event	Distributed TOE audit generation	Actual Audited Event
Reproduced from EP_IPS_V2.11			
FMT_SMF[IPS]	Modification of an IPS policy element.	FMC	<date> <time> <host> ActionQueueScrape.pl: <host>: <user>@<ip>, Intrusion Policy > <policy>> rule_configs, Changed BO_SERVER_TRAFFIC_DETECT (105:3) to "Generate events" (from "Drop and generate events")
IPS_ABD_EXT.1[IPS]	Inspected traffic matches an anomaly-based IPS policy.	FTD	<date> <time> <host> SFIMS : %FTD-5-430001: Protocol: <proto>, SrcIP: <ip>, DstIP: <ip>, SrcPort: <port>, DstPort: <port>, Priority: <pri>, GID: <gid>, SID: <sid>, Revision: <rev>, Message: \"<message>\", Classification: <class>, User: <user>, ACPolicy: <access-control-policy>, NAPPolicy: <network-analysis-policy>, InlineResult: <allowed|blocked>
IPS_IPB_EXT.1[IPS]	Inspected traffic matches a list of known-good or known-bad addresses applied to an IPS policy.	FTD	<date> <time> <host> %FTD-7-430002: DeviceUUID: 1d492c4c-cb33-11e9-95d4-de72c62116a8, AccessControlRuleAction: Block, AccessControlRuleReason: IP Block, SrcIP: 50.50.50.1, DstIP: 104.237.139.111, SrcPort: 1425, DstPort: 80, Protocol: tcp, IngressInterface: outside, EgressInterface: inside, ACPolicy: IPB Configuration, Prefilter Policy: Default Prefilter Policy_1, InitiatorPackets: 1, ResponderPackets: 0, InitiatorBytes: 54, ResponderBytes: 0, NAPPolicy: No Rules Active, SecIntMatchingIP: Source, IPReputationSICategory: BAD_SRC
IPS_NTA_EXT.1[IPS]	Modification of which IPS policies are active on a TOE interface. Enabling/disabling a TOE interface with IPS policies applied. Modification of which mode(s) is/are active on a TOE interface.	FTD	This sample shows modification of an access control policy “log stuff” by user “admin” where the intrusion policy associated with Rule 1 of the access control policy was changed to “Maximum Detection” and the updated policy was applied to an FTD named “ftd-6-4-sm-44”.  log stuff (2021-04-08 11:55:56/admin) Policy Information Last Modified 2021-04-08 11:55:56 Applied To ftd-6-4-sm-44 Mandatory Rule Rule 1 Name allow-icmp-and-log Intrusion Policy Maximum Detection
IPS_SBD_EXT.1[IPS]	Inspected traffic matches a signature-based IPS rule with logging enabled.	FTD	<date> <time> <host> SFIMS : %FTD-5-430001: Protocol: <proto>, SrcIP: <ip>, DstIP: <ip>, SrcPort: <port>, DstPort: <port>, Priority: <pri>, GID: <gid>, SID: <sid>, Revision: <rev>, Message: \"<message>\", Classification: <class>, User: <user>, ACPolicy: <access-control-policy>, NAPPolicy: <network-analysis-policy>, InlineResult: <allowed|blocked>
Reproduced from the mod_cpp_fw_v1.4e			

SFR	Auditable Event	Distributed TOE audit generation	Actual Audited Event
FFW_RUL_EXT.1[FW]	Application of rules configured with the 'log' operation Source and destination addresses Source and destination ports Transport Layer Protocol TOE Interface	FTD	<date> <time> <host> %FTD-7-430002: AccessControlRuleAction: Block, SrcIP: 2001:192:168:144::16, DstIP: 2001:10:1:1::1, ICMPType: Unknown, ICMPCode: Unknown, Protocol: ipv6-icmp, IngressInterface: outside, EgressInterface: inside, EgressZone: SYSLOG, ACPolicy: FFW_RUL_EXT.1.1, AccessControlRuleName: 3, Prefilter Policy: Default Prefilter Policy_3, User: No Authentication Required, InitiatorPackets: 0, ResponderPackets: 0, InitiatorBytes: 0, ResponderBytes: 0, NAPPolicy: No Rules Active <date> <time> <host> %FTD-7-430002: AccessControlRuleAction: Allow, SrcIP: 2001:192:168:144::16, DstIP: 2001:10:1:2::1, ICMPType: Echo Request, ICMPCode: No Code, Protocol: ipv6-icmp, IngressInterface: outside, EgressInterface: inside, EgressZone: SYSLOG, ACPolicy: FFW_RUL_EXT.1.1, AccessControlRuleName: 4, Prefilter Policy: Default Prefilter Policy_3, User: No Authentication Required, Client: ICMP for IPv6 client, ApplicationProtocol: ICMP for IPv6, InitiatorPackets: 1, ResponderPackets: 0, InitiatorBytes: 78, ResponderBytes: 0, NAPPolicy: Balanced Security and Connectivity
FFW_RUL_EXT.2[FW]	Dynamical definition of rule Establishment of a session	FTD	<date> <time> <host> %FTD-7-430002: AccessControlRuleAction: Allow, SrcIP: 192.168.144.16, DstIP: 10.6.8.15, SrcPort: 47328, DstPort: 21, Protocol: tcp, IngressInterface: outside, EgressInterface: inside, EgressZone: SYSLOG, ACPolicy: FFW_RUL_EXT.2 (Testlab5 Target), AccessControlRuleName: 1, Prefilter Policy: Default Prefilter Policy_2, User: No Authentication Required, InitiatorPackets: 2, ResponderPackets: 1, InitiatorBytes: 140, ResponderBytes: 74, NAPPolicy: Balanced Security and Connectivity
FMT_SMF.1/FFW[FW]	All management activities of TSF data (including creation, modification and deletion of firewall rules).	FMC	<date> <time> <host>: <date> sfdccsm: <host>: admin19@10.6.16.90, Policies > Access Control > Access Control > Firewall Policy Editor, Save Policy FFW_RUL_EXT.1.6/1.7/1.10
Reproduced from the mod_vpngw_v1.1			

SFR	Auditable Event	Distributed TOE audit generation	Actual Audited Event
FPF_RUL_EXT.1[VPN]	Application of rules configured with the 'log' operation	FMC, FTD	<date> <time> <host> %FTD-7-430002: AccessControlRuleAction: Allow, SrcIP: 192.168.144.7, DstIP: 10.10.7.1, SrcPort: 0, DstPort: 0, Protocol: pup, IngressInterface: outside, EgressInterface: inside, EgressZone: SYSLOG, ACPolicy: FPF_RUL_EXT.1.7, AccessControlRuleName: 1, Prefilter Policy: Block_IP-in-IP, User: No Authentication Required, InitiatorPackets: 1, ResponderPackets: 0, InitiatorBytes: 34, ResponderBytes: 0, NAPPolicy: custom Allow All <date> <time> <host> %FTD-7-430002: AccessControlRuleAction: Block, SrcIP: 192.168.144.8, DstIP: 10.10.8.1, SrcPort: 0, DstPort: 0, Protocol: ipencap, IngressInterface: outside, EgressInterface: inside, EgressZone: SYSLOG, ACPolicy: FPF_RUL_EXT.1.7, Prefilter Policy: Block_IP-in-IP, Tunnel or Prefilter Rule: 5, User: No Authentication Required, InitiatorPackets: 0, ResponderPackets: 0, InitiatorBytes: 0, ResponderBytes: 0, NAPPolicy: No Rules Active

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. 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. **Note**: Use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE

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

For plaintext keys in FXOS the TOE destroys the reference to the keys stored in volatile memory directly followed by a request for garbage collection, and the TOE destroys the abstraction that represents the key for keys stored in non-volatile storage the TSF. 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. The secret keys used for symmetric encryption, private keys, and CSPs used to generate keys, are zeroized immediately after use (for IPsec VPN functions, within FTD only), or on system shutdown (for all other functions). For plaintext keys unrelated to IPsec VPN: the TOE destroys the reference to the keys stored in volatile memory directly followed by a request for garbage collection; the TOE destroys the abstraction that represents the key for keys stored in non-volatile storage the TSF. When an administrator using the FMC WebUI initiates deletion of keys (e.g. certificates and their associated keys), the actual key destruction is delayed at the physical layer until those instructions are pushed from FMC to FTD and implemented on FTD.

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

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. These messages can be configured to be transmitted directly to a remote syslog server 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**.

4.4.3 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 and NTP traffic must be sent over IPsec as configured below. If IPsec connection between FXOS and remote syslog or NTP servers is unintentionally broken the FXOS will automatically attempt to re-initiate the IPsec connection until connectivity is restored, no administrative action is required other than resolving any connectivity issues in the networks, including restoring connectivity between FXOS and any CRL distribution points used for authentication of the IPsec endpoint.

To ensure syslog 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*. NAT traversal is supported in IKEv2 by default.

Note: On the Firepower 4100 and 9300 platforms, FTD 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 FTD will always secure syslog in TLS.

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

   `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) Enable or disable the certificate revocation list check. If IPsec sessions fail due to inability to contact the CRL server, restore connectivity to the CRL server before reattempting to establish the IPsec sessions.:

set revoke-policy [*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/ This value must be set to "yes" in the CC-evaluated configuration:

set sa-strength-enforcement [*yes* **]**

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
- **IPsec Mode**: tunnel, transport
    - set mode {tunnel |transport}
- **IKEv2 Mode***: main mode

- **IKEv2 Ciphers***:
    - **Encryption algorithms**: AES-CBC-128, AES-CBC-256, AES-GCM-128.
    - **Integrity algorithms**: SHA-1
    - **DH Groups**: 14
- **ESP Ciphers***:
    - **Encryption algorithms:** AES-CBC-128, AES-CBC-256
    - **Integrity algorithms:** 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*
- **IKEv2 SA Life Time:** Configurable up to 24 hours. Only time is supported.
    - set ike-rekey-time *minutes*
- **IKEv2 Child SA Life Time:** Configurable up to 8 hours. Only time is supported.
    - set esp-rekey-time *minutes*

```
* Not configurable
```

To define rules for matching the DN of the IPsec peer certificate:

First, create a certificate map via FMC (Objects > Object Management > VPN > Certificate Map), and add a rule to the certificate map to match the "Alternative Subject" field of the certificate to a value (DN).

Next, associate the certificate map with the tunnel, depending on tunnel type:

- Remote Access VPN (Devices > VPN > Remote Access > Advanced > Certificate Maps > check "Use the configured rules to match a certificate to a Connection Profile > Add Mapping > Certificate Map Name)

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) 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.

4.5 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_|_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 prompts for 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. Digital signatures (RSA only) are used to verify software/firmware update files (to ensure they have not been modified from the originals distributed by Cisco) before they are used to update the applicable TOE components. The update process will fail if the digital signature verification process fails.

- 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.

To see which version is currently running:

- WebUI: The version is displayed at the top of the Overview page.
- CLI: Use the "show version" command.

Updates can be loaded to FXOS via WebUI (uploading) or CLI (downloading) and be stored locally to be installed at a later time (see instructions later in this section). To see which updates are available for installation:

- WebUI: The list of uploaded updates is displayed on the Available Updates page (System > Updates).
- CLI: Use the "show bundle" command (scope firmware > show bundle).

As an automated step of the image upload process (whether uploading images via WebUI or CLI) the integrity of the image is verified through use of RSA digital signature verification. If the image verification fails the file will not be stored locally, and will not be listed (via WebUI or CLI) as being available for installation, thus invalid images cannot be installed. If an image fails the integrity check, re-download the update file from software.cisco.com, and try again to load the image to FXOS. If image verification continues to fail, contact Cisco TAC for assistance. If the image fails an integrity check or cannot be saved to FXOS for any other reason (e.g. lack of storage space, or loss of connectivity) an error will be displayed. If the error indicates a connectivity error, resolve the connectivity issue and reattempt to copy the file. If the error indicates a lack of storage space, remove unneeded update images and reattempt to copy the file.

- WebUI: The error will be displayed once the Upload Image step completes.
- CLI: The error will be indicated in the output of "show download-task detail" (scope firmware > show download-task detail).

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.

While and update is in progress the current running version will continue to be show as described above, and the installation status will show the version being installed, which will become the active version when the system reboots after installation. To see the status of the installation of an update:

- WebUI: Watch the Available Updates page as the installation progresses.
- CLI: Use the "show fsm status" command (scope firmware > scope auto-install > show fsm status).

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

Login to FXOS as the 'admin' account (with full privileges) to perform these and other installation steps.

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 (i.e. FTD) 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 (i.e. FTD) 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 (i.e. the FTD image):

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

6) To view details for a specific applications (i.e. the FTD image):

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

Sample:

```
Firepower-chassis /ssa # scope app ftd 6.4.0-10
```

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 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.

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.

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:

• **local**—Specifies local 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. The "session-timeout" setting applies to the WebUI only, while the "con-session-timeout" setting applies to all CLI access through the serial console as well as via SSH.

```
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 300 and 3600 seconds. The default is 3600 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.

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.

- 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'.

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) 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
```

Please refer to the ***Cisco Firepower 4100/9300 FXOS CLI Configuration Guide, 2.6(1)***[2] **– Chapter – Logical Devices** for password recovery procedures.

4.5.7 Configure the Minimum Password Length

In the evaluated configuration, 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. The passwords are stored hashed using Approved SHA-512.

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

In the evaluated configuration, FXOS does not permit a user to choose a password that does not meet the guidelines for strong password.

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

```
scope security
```

2) Enable the password strength check:

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

[2] https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos261/cli-guide/b_CLI_ConfigGuide_FXOS_261/logical_devices.html?bookSearch=true

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 be between 8 to 80 characters long.
- Must not contain the following symbols: $ (dollar sign), ? (question mark), and = (equals sign)
- The following alphanumeric characters can be a part of the password - [“!”, “@”, “#”, “%”, “^”, “&”, “*”, “(“, “)”, “ ” ‘ ` (double or single quote/apostrophe), + (plus), - (minus), , (comma), . (period), / (forward-slash), \ (back-slash), | (vertical-bar or pipe), : (colon), ; (semi-colon), < > (less-than, greater-than inequality signs), [ ] (square-brackets), { } (braces or curly-brackets),^ (caret), _ (underscore), and ~ (tilde).

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.

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.

IMPORTANT! NTP settings are not synced between the Firepower chassis and any applications (i.e. FTD) installed on the chassis. To ensure proper function, you must configure the same NTP settings on the Firepower chassis and on the applications (i.e. FTD) 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 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 characters 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.

4.5.13.6 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**.

4.5.13.7 Setting the Date and Time Using NTP

Use the CLI to configure an IPsec tunnel to secure NTP communications. Refer to section 4.4.3 Configure IPsec Secure Channel of this guide to configure IPsec. Ensure that the IP addresses of all configured NTP servers would be reachable only via the configured IPsec tunnel.

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 will be configured to tunnel NTP over IPsec, and the IPsec tunnel will not allow multicast or broadcast packets to reach FXOS.

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.

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. Note, in the CC-evaluated configuration the ssh-server rekey-limit volume must not be set greater than 1GB (no greater than 1000000 KB), and the time must not be set greater than one hour (no greater than 60 minutes):

```
Firepower /system/services # set ssh-server rekey-limit volume [KB (no
greater than 1000000] time [Minutes (no greater than 60)]
```

7) Commit the transaction to the system configuration:

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

NOTE! For SSH connections, the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. Rekey occurs after any of the thresholds are reached. SSH connections will be dropped if the TOE receives a packet larger than 262,149 bytes.

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

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

Certificates

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

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 TLS mutual authentication), you must generate a certificate request through FXOS and submit the request to a trust point.

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

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:

```
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
```

Note: This key generation process results in private keys stored in binary format. The private keys are stored in locations that are not accessible via any administrative interface, and only the unique identification of each key's associated PKI certificate is visible, via: **scope security > show keyring detail)**.

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 common name associated with the request:

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

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

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

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

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

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

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

8) Specify the IP address of the FXOS chassis:

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

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

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

10) Specify the organization requesting the certificate:

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

11) Specify the organizational unit:

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

12)
13) Specify an optional password for the certificate request:

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

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

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

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

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

16) Commit the transaction:

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

17) 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 Configuring HTTPS

IMPORTANT! After you complete the HTTPS configuration, including changing the port and key ring to be used by HTTPS, all current HTTP and HTTPS sessions are closed without warning as soon as you save or commit the transaction.

1) Enter system mode:

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

2) Enter system services mode:

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

3) Enter the HTTPS service:

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

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

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

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

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

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

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

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

ciphersuite-mode can be one of the following keywords:

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

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

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

cipher-suites can contain up to 256 characters and must conform to the OpenSSL Cipher Suite specifications. You cannot use any spaces or special characters except ! (exclamation point), + (plus

sign), - (hyphen), and : (colon).For details, see http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite

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

8) Commit the transaction:

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

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

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_RSA_WITH_AES_256_CBC_ SHA as defined in RFC 3268
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
- 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
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289

The Key establishment parameters TLS connections for FXOS are as follows –

FXOS (HTTPS/TLS) - 2048-bit RSA, DHE 2048 and ECDHE secp256r1, secp384r1, secp521r1

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 and an error message indicating a self-test failure will be displayed via the serial console CLI. (Note, in the case of FTD on the Firepower 4100 and 9300 platforms, use the "connect module" command from the FXOS/MIO CLI to access the FTD console as described in [FTD-CC].) 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 self-testing includes cryptographic algorithm tests (known-answer tests) that feed pre-defined data to cryptographic modules and confirm the resulting output from the modules match expected values, and firmware integrity tests that verify the digital signature of the code image using RSA-2048 with SHA-512.

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

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