



Cisco FTD v7.0 on ASA 5500 and ISA 3000 and FTDv with FMC/FMCv

Common Criteria Supplemental User Guide

Version 0.3

January 23, 2023

Prepared by:



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

Table of Contents

1	INTRODUCTION	6
1.1	COMMON CRITERIA (CC) EVALUATED CONFIGURATION	7
1.2	SCOPE OF EVALUATION	8
1.3	REFERENCES	9
1.4	DOCUMENTATION REFERENCES	10
2	OPERATIONAL ENVIRONMENT	11
2.1	OPERATIONAL ENVIRONMENT COMPONENTS	11
2.2	ENVIRONMENTAL ASSUMPTIONS	11
3	BEFORE INSTALLATION	14
4	INSTALLATION AND CONFIGURATION	15
4.1	FMC INSTALLATION	15
4.1.1	<i>FMC Fundamentals</i>	15
4.1.2	<i>FMC Installation</i>	15
4.2	FMC INITIAL CONFIGURATION	16
4.2.1	<i>Configure Authentication</i>	16
4.2.2	<i>Configure the Pre-Login Banner</i>	16
4.2.3	<i>Configure the Clock</i>	16
4.2.4	<i>Configure SSH Public-Key Authentication</i>	17
4.2.5	<i>Configure SSH ReKey Configuration (optional)</i>	17
4.2.6	<i>Configure Inactivity Timeout Settings</i>	18
4.2.7	<i>Configure Logging</i>	18
4.2.8	<i>Configure Local Storage of Audit Log Messages</i>	19
4.2.9	<i>Configure Use of a Remote Logging Server</i>	19
4.2.10	<i>Configure Access Lists for Remote Administration</i>	19
4.2.11	<i>Disable the REST API</i>	20
4.2.12	<i>CC Mode and FIPS Mode</i>	20
4.2.13	<i>Configure CLI Lockdown on FMC</i>	21
4.2.14	<i>Logging into the Appliance</i>	21
4.2.15	<i>Logout</i>	23
4.2.16	<i>Restrict Access and Enable CC Mode</i>	23
4.2.17	<i>Configure Syslog over TLS for FMC and FTD</i>	25
4.3	FTD INSTALLATION	30
4.4	FTD INITIAL CONFIGURATION	31
4.4.1	<i>Ensure FTD is Managed by FMC</i>	31
4.4.2	<i>Enable CC Mode and FIPS Mode</i>	31
4.4.3	<i>Common Criteria (CC) Mode</i>	32
4.4.4	<i>Configure Authentication</i>	34
4.4.5	<i>Configure the Pre-Login Banner</i>	35
4.4.6	<i>Configure the Clock</i>	35
4.4.7	<i>Configure Inactivity Timeout Settings</i>	35
4.4.8	<i>Disable the HTTP (HTTPS) Server</i>	35
4.4.9	<i>Configure Logging</i>	36
4.4.10	<i>Configure CLI Lockdown on FTD</i>	40
4.4.11	<i>FTD Logout</i>	41
5	FTD ACCESS CONTROL POLICIES	42
5.1	FTD INTERFACE MODES: FIREWALL, IPS-ONLY, OR IDS-ONLY	42

5.1.1	<i>Firewall and VPN Gateway Interfaces</i>	43
5.1.2	<i>Passive Interfaces (IDS-only interfaces)</i>	44
5.1.3	<i>Inline Interface Sets (IPS-only interfaces)</i>	44
5.2	CONFIGURE ACCESS CONTROL POLICIES	44
5.2.1	<i>Access Control Policies (ACP)</i>	44
5.2.2	<i>Access Control Rules</i>	47
6	MANAGEMENT FUNCTIONS	53
6.1	MANAGE THE FMC AUDIT LOG AND SYSLOG	53
6.1.1	<i>View Audit Log and Syslog via GUI</i>	54
6.1.2	<i>View Audit Log and Syslog via CLI</i>	55
6.2	AUDITABLE EVENTS	56
6.2.1	<i>Logs of Intrusion and Firewall Events</i>	79
6.3	MANAGEMENT OF INTRUSION EVENTS	80
6.3.1	<i>Viewing Intrusion Events</i>	80
6.3.2	<i>Searching Intrusion Events</i>	84
6.3.3	<i>Sorting and filtering Intrusion Events</i>	84
6.4	DEVICE REGISTRATION	85
6.4.1	<i>Device Registration On FTD</i>	87
6.4.2	<i>Device Registration On FMC</i>	87
6.5	CUSTOM WEB SERVER CERTIFICATE	88
6.5.1	<i>Generating an HTTPS Server Certificate Signing Request</i>	88
6.5.2	<i>Importing HTTPS Server Certificate</i>	89
6.6	USER AND ROLE MANAGEMENT	89
6.6.1	<i>Viewing User Accounts</i>	89
6.6.2	<i>Adding New User Accounts</i>	90
6.6.3	<i>Modifying and Deleting User Accounts</i>	92
6.6.4	<i>Unlocking FMC Accounts</i>	93
6.7	CHANGE PASSWORD	93
6.7.1	<i>Configure Password via GUI</i>	93
6.7.2	<i>Configure Password via CLI</i>	94
6.7.3	<i>Password Recovery Procedures</i>	94
6.8	CONFIGURE TIME SYNCHRONIZATION	95
6.8.1	<i>Setting the Time Manually</i>	95
6.9	CONFIGURE LOGIN BANNER	96
6.10	INACTIVITY TIMEOUT SETTING	96
6.10.1	<i>Session Timeout Record</i>	97
6.11	PRODUCT UPGRADE	97
6.11.1	<i>To Update the FMC:</i>	99
6.11.2	<i>To Update Managed Devices:</i>	99
7	SELF-TESTS	101
1	INTRODUCTION	6
1.1	COMMON CRITERIA (CC) EVALUATED CONFIGURATION	7
1.2	SCOPE OF EVALUATION	8
1.3	REFERENCES	9
1.4	DOCUMENTATION REFERENCES	10
2	OPERATIONAL ENVIRONMENT	11
2.1	OPERATIONAL ENVIRONMENT COMPONENTS	11

2.2	ENVIRONMENTAL ASSUMPTIONS	11
3	BEFORE INSTALLATION	14
4	INSTALLATION AND CONFIGURATION	15
4.1	FMC INSTALLATION	15
4.1.1	<i>FMC Fundamentals</i>	15
4.1.2	<i>FMC Installation</i>	15
4.2	FMC INITIAL CONFIGURATION	16
4.2.1	<i>Configure Authentication</i>	16
4.2.2	<i>Configure the Pre-Login Banner</i>	16
4.2.3	<i>Configure the Clock</i>	16
4.2.4	<i>Configure SSH Public-Key Authentication</i>	17
4.2.5	<i>Configure SSH ReKey Configuration (optional)</i>	17
4.2.6	<i>Configure Inactivity Timeout Settings</i>	18
4.2.7	<i>Configure Logging</i>	18
4.2.8	<i>Configure Local Storage of Audit Log Messages</i>	19
4.2.9	<i>Configure Use of a Remote Logging Server</i>	19
4.2.10	<i>Configure Access Lists for Remote Administration</i>	19
4.2.11	<i>Disable the REST API</i>	20
4.2.12	<i>CC Mode and FIPS Mode</i>	20
4.2.13	<i>Configure CLI Lockdown on FMC</i>	21
4.2.14	<i>Logging into the Appliance</i>	21
4.2.15	<i>Logout</i>	23
4.2.16	<i>Restrict Access and Enable CC Mode</i>	23
4.2.17	<i>Configure Syslog over TLS for FMC and FTD</i>	25
4.3	FTD INSTALLATION	30
4.4	FTD INITIAL CONFIGURATION	31
4.4.1	<i>Ensure FTD is Managed by FMC</i>	31
4.4.2	<i>Enable CC Mode and FIPS Mode</i>	31
4.4.3	<i>Common Criteria (CC) Mode</i>	32
4.4.4	<i>Configure Authentication</i>	34
4.4.5	<i>Configure the Pre-Login Banner</i>	35
4.4.6	<i>Configure the Clock</i>	35
4.4.7	<i>Configure Inactivity Timeout Settings</i>	35
4.4.8	<i>Disable the HTTP (HTTPS) Server</i>	35
4.4.9	<i>Configure Logging</i>	36
4.4.10	<i>Configure CLI Lockdown on FTD</i>	40
4.4.11	<i>FTD Logout</i>	41
5	FTD ACCESS CONTROL POLICIES	42
5.1	FTD INTERFACE MODES: FIREWALL, IPS-ONLY, OR IDS-ONLY	42
5.1.1	<i>Firewall and VPN Gateway Interfaces</i>	43
5.1.2	<i>Passive Interfaces (IDS-only interfaces)</i>	44
5.1.3	<i>Inline Interface Sets (IPS-only interfaces)</i>	44
5.2	CONFIGURE ACCESS CONTROL POLICIES	44
5.2.1	<i>Access Control Policies (ACP)</i>	44
5.2.2	<i>Access Control Rules</i>	47
6	MANAGEMENT FUNCTIONS	53
6.1	MANAGE THE FMC AUDIT LOG AND SYSLOG	53
6.1.1	<i>View Audit Log and Syslog via GUI</i>	54
6.1.2	<i>View Audit Log and Syslog via CLI</i>	55

6.2	AUDITABLE EVENTS	56
6.2.1	<i>Logs of Intrusion and Firewall Events</i>	79
6.3	MANAGEMENT OF INTRUSION EVENTS	80
6.3.1	<i>Viewing Intrusion Events</i>	80
6.3.2	<i>Searching Intrusion Events</i>	84
6.3.3	<i>Sorting and filtering Intrusion Events</i>	84
6.4	DEVICE REGISTRATION	85
6.4.1	<i>Device Registration On FTD</i>	87
6.4.2	<i>Device Registration On FMC</i>	87
6.5	CUSTOM WEB SERVER CERTIFICATE	88
6.5.1	<i>Generating an HTTPS Server Certificate Signing Request</i>	88
6.5.2	<i>Importing HTTPS Server Certificate</i>	89
6.6	USER AND ROLE MANAGEMENT	89
6.6.1	<i>Viewing User Accounts</i>	89
6.6.2	<i>Adding New User Accounts</i>	90
6.6.3	<i>Modifying and Deleting User Accounts</i>	92
6.6.4	<i>Unlocking FMC Accounts</i>	93
6.7	CHANGE PASSWORD	93
6.7.1	<i>Configure Password via GUI</i>	93
6.7.2	<i>Configure Password via CLI</i>	94
6.7.3	<i>Password Recovery Procedures</i>	94
6.8	CONFIGURE TIME SYNCHRONIZATION	95
6.8.1	<i>Setting the Time Manually</i>	95
6.9	CONFIGURE LOGIN BANNER	96
6.10	INACTIVITY TIMEOUT SETTING	96
6.10.1	<i>Session Timeout Record</i>	97
6.11	PRODUCT UPGRADE	97
6.11.1	<i>To Update the FMC:</i>	99
6.11.2	<i>To Update Managed Devices:</i>	99
7	SELF-TESTS	101

1 Introduction

The Cisco Firepower Threat Defense (FTD) System is a next-generation Firewall (NGFW) that combines both SNORT® open source and proprietary technology and firewall and VPN functionality. The system is used to filter and monitor all incoming and outgoing network traffic for security events and violations. All packets on the monitored network are scanned, decoded, preprocessed and compared against a set of access control and intrusion rules to determine whether inappropriate traffic, such as system attacks, is being passed over the network. The system then notifies a designated administrator of these attempts and/or blocks the malicious traffic. The system generates these alerts when deviations of the expected network behavior are detected and when there is a match to a known attack pattern.

In addition, the system also provides real-time contextual awareness, advanced malware protection, and security intelligence for blocking malicious URLs and IP addresses. The Cisco FTD System is an integrated suite of network security and traffic management products, deployed either on purpose-built platforms or as a software solution. In a typical deployment, multiple traffic-sensing managed Devices (i.e., sensors) installed on network segments monitor traffic for analysis and report to a managing Firepower Management Center (FMC). Deployed inline, Devices can affect the flow of traffic.

The Firepower Management Center provides a centralized management console with web interface that you can use to perform administrative, management, analysis, and reporting tasks. You can also use a CLI on the Devices to perform setup, basic analysis, and configuration tasks.

This document is a supplement to the Cisco administrative guidance, which is comprised of the installation and administration documents identified in section 1.3. This document supplements those manuals by specifying how to install, configure and operate this product in the Common Criteria evaluated configuration. This document is referred to as the operational user guide in the Network Device collaborative Protection Profile (NDcPP) and meets all the required guidance assurance activities from the CPP_ND_v2.2e, MOD_IPS_V1.0, MOD_CPP_FW_1.4E and MOD_VPNGW_V1.1.

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.

Accessing the shell should be limited to authorized administrators for pre-operational setup (for example, Security Technical Implementation Guide (STIG) compliance testing), for troubleshooting, or regular maintenance.

In addition, the Threat license must be purchased and activated to use all the IPS features to meet the IPS requirements for Common Criteria. Optionally (beyond the scope of IPS requirements for Common Criteria), to use the malware protection feature Malware license is required, and to use URL filtering capability URL Filtering license is required.

Audience

This document is written for administrators configuring the Cisco FTD system running software version 7.0.x. 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.

1.2 Scope of Evaluation

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

The following features and protocols are not evaluated:

- Shell Access – The shell access is only allowed for pre-operational installation, configuration, and post-operational maintenance and trouble shooting.
- REST API – This feature is not evaluated as part of the evaluation. REST API relies on HTTPS as the underlying communication protocol and can be used to build a management interface. This feature is not tested and is out of scope.
- Timeout Exemption Option - The use of the “Exempt from Browser Session Timeout” setting is not permitted. This allows a user to be exempted from the inactivity timeout feature.
- Any features not associated with SFRs in claimed NDcPP and PP modules – NDcPP forbids adding additional requirements to the Security Target (ST). If additional functionalities are mentioned in the ST, it is for completeness only.

1.3 References

CC-evaluated Software and Hardware:

Table 1: TOE Series and Models

Software: <ul style="list-style-type: none">• FTD/FTDv 7.0• FMC/FMCv 7.0
Firepower Management Center (FMC) appliances: <ul style="list-style-type: none">• FMC1000-K9• FMC2500-K9• FMC4500-K9• FMC1600-K9• FMC2600-K9; and• FMC4600-K9• FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3.
Firepower Threat Defense (FTD) appliances: <ul style="list-style-type: none">• Cisco 5500 Series (5508-X and 5516-X)• ISA 3000 (ISA 3000-4C and ISA 3000-2C2F)• FTDv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3, and other general-purpose computing platforms with Intel processors.• FTDv running on NFVIS 4.4 on the ENCS 5406, 5408, and 5412.

1.4 Documentation References

The Cisco FTD documentation set includes online help and PDF files. The following product guidance documents are provided online or by request:

Table 2: Document References

<i>Cisco FTD 7.0 on ASA 5500 and ISA (Industrial Security Appliance) 3000 and FTDv with FMC/FMCv Common Criteria Supplemental User Guide [This Document]</i>
<i>Cisco Firepower Release Notes, Version 7.0, Last updated: August 10, 2022</i> https://www.cisco.com/c/en/us/td/docs/security/firepower/70/relnotes/firepower-release-notes-700.html
<i>Cisco Firepower Management Center 1000, 2500, and 4500 Hardware Installation Guide [FMC-HIG1]</i> https://www.cisco.com/c/en/us/td/docs/security/firepower/1000_2500_4500/hw/guide/b_install_guide_1000_2500_4500.html
<i>Cisco Firepower Management Center 1600, 2600, and 4600 Hardware Installation Guide [FMC-HIG2]</i> https://www.cisco.com/c/en/us/td/docs/security/firepower/fmc-1600-2600-4600/hw/guide/install-fmc-1600-2600-4600.html
<i>Cisco Firepower Management Center Upgrade Guide, Version 6.0 – 7.0. Last updated: March 1, 2022 [FMC-UG]</i> https://www.cisco.com/c/en/us/td/docs/security/firepower/upgrade/fpmc-upgrade-guide.html
<i>FMC Getting Started Guides [FMC-GS]</i> <i>Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide, Last updated: June 6, 2022</i> https://www.cisco.com/c/en/us/td/docs/security/firepower/hw/getting-started/fmc-1600-2600-4600/fmc-1600-2600-4600.html
<i>Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide, Last updated: April 6, 2020</i> https://www.cisco.com/c/en/us/td/docs/security/firepower/hw/getting-started/fmc-1000-2500-4500/fmc-1000-2500-4500.html
<i>Cisco Secure Firewall Management Center Virtual Getting Started Guide, Last updated: August 26, 2022</i> https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/vmware/fmcv/FMCv-quick.html
<i>Firepower Management Center Configuration Guide, Version 7.0, Last updated: August 2, 2022 [FMC-CG]</i> https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70.html
<i>Cisco Secure Firewall Threat Defense Command Reference, Last updated: June 6, 2022 [FTD-CLI]</i> https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html
<i>Cisco Secure Firewall Threat Defense Syslog Messages, Last updated: February 22, 2021</i> https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html [FTD-SYSLOG]

Online help can be accessed in two ways:

- By selecting Product Support > Select a Product
- Search for the Product

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.

NOTE! The management network should be physically or logically separated (e.g., VLANs) from the monitored network.

- Audit server (**Required**) – The system can be configured to deliver audit records to an external log server.

NOTE! It is recommended that the audit server is physically or logically separated (e.g., VLANs) from the monitored network. It can be on the same trusted internal network as the management network.

- 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.
- Remote Tunnel Endpoint - This includes any peer with which the TOE participates in tunneled communications. Remote tunnel endpoints may be any device or software client that supports IPsec tunneling. Both VPN clients and VPN gateways can be considered to be remote tunnel endpoints.

2.2 Environmental Assumptions

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

Table 3: 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.

Environment Security Objective	Operational Environment Security Objective Definition	Administrator Responsibility
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.
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.

Environment Security Objective	Operational Environment Security Objective Definition	Administrator Responsibility
OE.RESIDUAL_INFORMATION	<p>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.</p>	<p>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.</p>
OE.VM_CONFIGURATION	<p>For vNDs, the Security Administrator ensures that the VS and VMs are configured to</p> <ul style="list-style-type: none"> • 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). <p>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.</p>	<p>Security administrators ensure that all the unused inter-VM configurations are turned off and only the TOE VM is running on the hypervisor to reduce the attacks surface.</p>
OE.CONNECTIONS	<p>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.</p>	<p>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.</p>

3 Before Installation

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

- Locate the Cisco FTD 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. This management interface is separate from the data interface described in the section “Passive vs Inline”.
- Identify the specific management workstation IP addresses that can be allowed to access appliances. Restrict access to the appliance to only those specific hosts using the Access Lists feature.
- To safeguard the FMC, user must deploy the FMC on a protected internal network. Although the FMC is configured to have only the necessary services and ports available, user must make sure that attacks cannot reach it from outside the access control.
- Connect the management interface of managed Devices to the same protect internal network as the FMC. This allows the administrators to securely control the Device from the FMC and aggregate the event data generated on the managed Device’s network segment.
- By default, several ports are open to allow the system to take advantage of additional features and functionality. The following table lists these ports. Note that DHCP on ports 67 and 68 is disabled by default.

Ports	Description	Protocol	Direction	Open the port to ...
22	SSH	TCP	Bidirectional	Allow a secure remote connection to the appliance.
53	DNS	TCP	Outbound	Use DNS.
67, 68	DHCP	UDP	Outbound	Use DHCP. Disabled by default.
443	HTTPS	TCP	Bidirectional	Allow a secure remote connection to the appliance. Required Download software updates.
514	SYSLOG	UDP	Outbound	Send alerts to a remote syslog server. The remote syslog server must allow port 6514 to be opened.
8305	TLS	TCP	Bidirectional	Allow for Device management. Required

4 Installation and Configuration

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

4.1 FMC Installation

4.1.1 *FMC Fundamentals*

FMC includes an operating system, and applications including an SSH server (for remote administration via CLI), a web server (for remote administration via WebUI from a web browser), and database (for storage of policies and audit messages). FMC is primarily configured via the WebUI, and in the CC-evaluated configuration the vast majority of CLI functionality is disabled. Regardless, it may occasionally be necessary to login to the CLI (via console or SSH) to perform some system maintenance, such as shutting down or restarting the appliance. Be aware that the default username for the CLI and the WebUI are the same, 'admin', and have the same default password, 'Admin123', but they are separate accounts, so when their default passwords are changed the new password for each admin account should be unique.

Note: All the FMC installation and configuration guidance described in this document is applicable to physical FMC appliances and virtual FMC (FMCv) appliances. For additional deployment instructions specific to FMCv refer to [FMC-GS].

4.1.2 *FMC Installation*

To complete installation and initial configuration of FMC:

- 1) Refer to the correct FMC Hardware Installation Guide, [FMC-HIG1] or [FMC-HIG2], for your hardware model to complete the tasks of mounting the appliance, connecting the console cable, and connecting power.
- 2) If the appliance was installed with an earlier version of FMC, follow instructions in the [FMC-UG] to upgrade to FMC 7.0.
- 3) Refer to the correct FMC Getting Started Guide [FMC-GS] for your hardware model and follow instructions in the sections listed here:
 - a) Follow "Install the Management Center for Versions 6.5 and Later" to:
 - i) Ensure version 7.0 is installed (it can be updated later to 7.0.x)
 - ii) Ensure cables are connected
 - iii) (Skip) "Add Classic Licenses..." (Licensing will be configured in the next section.)
 - b) Follow "Configure FMC Administrative Settings" to:
 - i) Login to the WebUI.
 - ii) Create Individual User Accounts (these are administrative accounts).
 - iii) Configure Time Settings
 - iv) Configure Smart Licensing for the FMC. (Use of either Smart Licensing or Universal Licenses will enable the FMC to allocate licenses automatically to any managed FTD.)
 - v) (Optional) Schedule System Updates and Backups

- c) (Skip) “Add Managed Devices to FMC” (Skip this section for now because these steps will be covered later when one or more FTDs have is installed.)
- d) (Partially optional) Perform these steps in “Set Up Alternate FMC Access”:
 - i) (Optional) Set Up Serial Access
 - ii) DO NOT follow the steps under “Set Up Lights Out Management”. This feature uses the IPMI protocol for remote authentication, and the IPMI protocol is not secure enough to be used in the CC-evaluated configuration.
- e) (Optional) Preconfigure FMCs
- f) (Optional) Managing the Firepower Management Center User the System Restore Utility
- g) DO NOT Erase the Hard Drive unless you intent to fully reinstall the appliance, or return it to Cisco, or dispose of it.

4.2 FMC Initial Configuration

4.2.1 Configure Authentication

FMC has two local user stores with separately maintained accounts, one set is used for CLI access, and the other is used for WebUI/GUI access. The default username and password for the CLI administrative and the GUI administrator are the same, the user name is ‘admin’, and the default password is ‘Admin123’, but the default password is changed during initial setup, so after initial setup the passwords for each ‘admin’ account should continue to be unique. The passwords are stored hashed using Approved SHA-512 with a 32-bit salt value.

To change the GUI admin password, or to create additional GUI accounts, refer to the “Add an Internal User Account” section in the “User Accounts for Management Access” chapter of [FMC-CG].

4.2.2 Configure the Pre-Login Banner

Create a custom login banner that will appear during login attempts via CLI or GUI. Banners can contain any printable characters except the less-than symbol (<) and the greater-than symbol (>). To configure the pre-login banner for FMC refer to the “Login Banners” section of [FMC-CG], which is summarized here:

- 1) Login to the FMC WebUI.
- 2) Navigate to **System > Configuration > Login Banner**.
- 3) In the **Custom Login Banner** field enter the login banner text you want to use.
- 4) Click **Save**.

4.2.3 Configure the Clock

In the CC-certified configuration, the FMC clock may only be set manually, it is not permissible for FMC to use an NTP server. To ensure NTP is disabled and to set the date, time, and timezone, refer to section [6.8 Configure Time Synchronization](#) in this document.

4.2.4 Configure SSH Public-Key Authentication

Perform the following steps on a remote workstation:

1. Log into the remote management host (the host that will use its SSH client to connect to a Firepower appliance).
2. Regenerate or regenerate an ECDSA SSH keypair on the remote host:

```
cd ~
ssh-keygen -t ecdsa -b 256
Generating public/private ecdsa key pair.
Enter file in which to save the key (/home/admin/.ssh/id_ecdsa):
[Press Enter to accept the default file path and filename.]
[If the file already exists, type "y" and Enter to replace it.]
/home/admin/.ssh/id_ecdsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase): [leave it blank, press Enter]
Enter same passphrase again: [leave it blank, press Enter]
Your identification has been saved in /home/admin/.ssh/id_ecdsa.
Your public key has been saved in /home/admin/.ssh/id_ecdsa.pub.
The key fingerprint is:
<fingerprint> admin@<hostname>
```

3. Log into the Firepower appliance (FMC or FTD) as admin and use the 'expert' command to access the Linux shell.

4. Copy the public key from the remote host to the Firepower appliance.

```
cd ~/.ssh
scp <username-on-remote-host>@<IP-address-of-remote-host>:~/.ssh/id_ecdsa.pub .
touch ~/.ssh/authorized_keys
cat id_ecdsa.pub >> ~/.ssh/authorized_keys
exit
exit
```

5. The public key will now be used the next time you login via SSH from that remote host.

4.2.5 Configure SSH ReKey Configuration (optional)

When CC mode is enabled, the SSH rekeying will occur approximately at 1 hour of time or after 1 GB of data has been transmitted, whichever occurs first. To change these values to be smaller, the administrator can configure these during the pre-operational state **ONLY** using the local management connection:

1. Login locally to shell with the default **admin** account using the password created during the initial setup process.

NOTE! If you are on a sensor, the **>** will be displayed. Type the command **expert** to access the shell from the CLI.

2. The shell prompt **<username>@<hostname>:~\$** is displayed.
3. Type command **sudo -i** to gain root access.

A warning message is displayed about root privilege (first time only).

4. Enter the same password as in step 1.
5. The shell prompt `<username>@<hostname>:~#` is displayed.
6. Type the command `vi /etc/ssh/sshd_config` to modify the SSH daemon configuration file.
7. Modify “RekeyLimit 1G 1h” to the desired values. For example, “RekeyLimit 1G 30m”

WARNING! Do not set the time to be greater than one hour or the volume to be greater than 1 GB.

8. Type `/etc/rc.d/init.d/sshd restart` to restart the SSH server.

4.2.6 Configure Inactivity Timeout Settings

By default, all user sessions (web-based and CLI) automatically log out after 60 minutes (1 hour) of inactivity, though the limit is configurable separately for CLI sessions (shell timeout) and for WebUI sessions (browser session timeout). Users with Administrator Role can change the inactivity timeout value in the system policy to meet their security needs.

Note: The FMC WebUI supports the ability to exempt individual WebUI accounts that don't have the 'administrator' role from having the Browser Session Timeout apply to their sessions, but to adhere to the CC-evaluated configuration do not exempt any account from the Browser Session Timeout, regardless of the role(s) assigned to that account.

To configure the Shell Timeout (for CLI) and the Browser Session Timeout (for WebUI) for FMC refer to section [6.10 Inactivity Timeout Setting](#) of this document. For further explanation refer to the “Configure Session Timeouts” section of [FMC-CG].

4.2.7 Configure Logging

Audit messages on FMC are stored separately in two main categories: the “System Log” stores syslog messages (for system-level events, including CLI login/logout events); and the “Audit Log” stores messages as database records (for configuration changes via WebUI or CLI, and for IPS events). System messages are viewable via the WebUI under **System > Monitoring > Syslog**, and audit messages are viewable via the WebUI under **System > Monitoring > Audit**.

To ensure the year is included in the time stamp for the audit messages, modify the `syslog-ng-tls.conf` file by adding the following:

```
template timestamp {
    template ("${ISODATE $HOST $MSGHDR$MSG\n");
};
```

```
options {
    fips_mode (1);
    cc_mode (1);
    proto-template(timestamp);
};
```

The `syslog-tls.conf.tt` file (`/usr/local/sf/htdocs/html_templates/stig/syslog-tls.conf.tt`) should also be edited to add the following change to restrict the supported ciphers for the TLS connection between the FMC/FMCv and the external syslog server to the ones listed in the ST and section **Error! Reference source not found.** of this document –

```
cipher-suite("ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:AES256-SHA256:AES128-SHA256")
```

4.2.8 Configure Local Storage of Audit Log Messages

The local storage of system (syslog) messages (those viewable under **System > Monitoring > Syslog**) is not configurable.

To ensure that the year is also included in the locally stored audit records, modify the `/etc/syslog-ng.conf` file by adding the following to the beginning of the file:

```
options {  
    ts-format(rfc3339);  
};
```

To review the current storage limits for messages stored in the database (those viewable under **System > Monitoring > Audit**), look in the WebUI under **System > Configuration > Database**. The database that holds the events related to administrative actions via the WebUI are stored in the “Audit Event Database”. To configure these values click on **Help > Online** while viewing that page, or refer to guidance in the “Database Event Limits” section of [FMC-CG].

4.2.9 Configure Use of a Remote Logging Server

The system (syslog) messages that are stored locally (those viewable under **System > Monitoring > Syslog**) can also be configured to be transmitted to a remote logging server. Once use of a remote audit server has been configured, messages will be simultaneously written locally and transmitted to the remote server. Enabling use of a remote audit server will not result on previously generated messages being transmitted to that server.

To enable transmission of audit messages to a remote server, follow the instructions in section 4.2.17 Configure Syslog over TLS for FMC and FTD of this document. Additional guidance can be found in the “Stream Audit Logs to Syslog” section of [FMC-CG], and the “Audit Log Certificate” section of [FMC-CG].

4.2.10 Configure Access Lists for Remote Administration

By default FMC will accept incoming SSH and HTTPS connections from any source IP address, but FMC can be configured to only allow incoming SSH and HTTPS connections from specified IP subnets or IP addresses. To configure those rules, use the **System > Configuration > Access List** page of the WebUI, and refer to the “Configure an Access List” section of [FMC-CG] for further instructions.

To avoid disruption of SSH and HTTPS connectivity, it is recommended to new rules to allow SSH (port 22) and HTTPS (port 443) from necessary subnets/addresses before deleting the default rule that allows those ports from all source addresses.

Inbound connectivity using SNMP is disabled by default (not permitted by any Access List rule) and inbound SNMP access must remain disabled in the CC-evaluated confirmation, so do not create any rule that would allow inbound SNMP.

4.2.11 Disable the REST API

Use the FMC WebUI to disable the FMC REST API by unchecking the “Enable REST API” box under: **System > Configuration > REST API Preferences > Enable REST API.**

4.2.12 CC Mode and FIPS Mode

Enabling CC Mode on FMC is required to enable automated locking of the default ‘admin’ account when it’s used to login remotely via the WebUI. For a summary of other characteristics of CC Mode, and for instructions to enable CC mode, refer to the “Security Certifications Compliance Characteristics” section of [FMC-CG].

Warning: After enabling FIPS Mode or CC Mode on FMC those modes cannot be disabled. Disabling these modes would require reinstallation of FMC.

Enabling CC mode will restrict the SSH algorithms¹, SSH rekey, TLS versions and TLS cipher suites (including elliptical curves) to the Approved ones claimed in the Security Target. There are additional features such as enabling the power-up integrity HMAC-SHA-512 self-test, enabling FIPS mode, and other TLS required checks such as the ones specified in section 6 of RFC 6125. To be in the evaluated configuration, you must enable CC Mode. Note: Use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE

IMPORTANT! After you enable this setting, you cannot disable it. If you need to do so, contact Support for assistance.

IMPORTANT! The FMC will not receive data from a managed Device unless both are operating in CC mode. Therefore, you must enable CC mode on the FMC first, then its managed Devices.

1. Login with Administrator Role.
2. Depending on whether you are configuring audit log streaming for a Firepower Management Center or a managed Device:
 - Management Center—Choose **System > Configuration.**
 - Managed Device—Choose **Devices > Platform Settings** and create or edit a Firepower policy.
3. Click UCAPL/CC Compliance.
4. Choose **CC** from the drop-down list.
5. Click **Save.**
6. Click **Deploy** if you are configuring these settings for the managed Devices. Select the Device(s) you want to deploy the setting to and click **Deploy** again. Remember, you need to enable CC Mode first on the FMC!

NOTE! System automatically reboots when you enable CC compliance. The FMC reboots when you save the system configuration; managed Devices reboot when you deploy the configuration.

¹ aes128-cbc, aes256-cbc, AEAD_AES_128_GCM, AEAD_AES_256_GCM are the approved encryption algorithms, hmac-sha1, hmac-sha2-256, hmac-sha2-512, AEAD_AES_128_GCM, AEAD_AES_256_GCM are the approved hmac algorithms and diffie-hellman-group14-sha1 (supported by FTD and FMC) are the only allowed key exchange methods.

Audit Record:

2016-11-15 19:54:52 admin

Enable UCAPL/CC Compliance

Enable CC mode

10.128.120.41

4.2.13 Configure CLI Lockdown on FMC

During this initial configuration the CLI access will become greatly limited from the default behavior, and once that change has been made, nearly all administrative activity will be performed via the GUI. By default, the default CLI shell is a Linux shell with ability to traverse the Linux file system. Access to that shell must be disabled in the CC-evaluated configuration. For further information about the FMC CLI, refer to the “Firepower Management Center Command Line Reference” section of [FMC-CG].

- 1) To lock-down the CLI access, complete these steps:

Warning: Before completing the next step, ensure there is no need to access the Linux filesystem shell. Before completing the next step the Linux shell is still accessible by using the “expert” command. After completing the next step use of the “expert” command will be disabled.

Note: Note, access to the Linux shell is required for regenerating the SSH key pair (described in section 4.2.4), and for changing the SSH rekey limits (described in section 4.2.5).

Note: As of FMC version 6.5 the default shell available via console or SSH is the FMC CLI shell, not the Linux shell, so this FMC GUI page is no longer available or necessary: System > Configuration > Console Configuration.

Warning: If you need to access the Linux shell after this step, you need to contact Cisco TAC for assistance.

- 2) Login to the CLI (via console or SSH) as admin.
- 3) Use the “system lockdown” command, where “lockdown” is one of the options after “system” as shown here:

```
> system ?
generate-troubleshoot Run troubleshoot
lockdown              Remove access to bash shell
reboot                Reboot the device
restart               Restart the device
shutdown              Shutdown the device
>
```

4.2.14 Logging into the Appliance

4.2.14.1 Login Remotely to GUI Web Interface

The FMC has a web interface that user can use to perform administrative, management, and analysis tasks. User can access the web interface by logging into the appliance using a web browser. The following table lists web browser compatibility.

Firefox 52.0 and later	JavaScript, cookies, Transport Layer Security (TLS) v1.1 and 1.2
Microsoft Internet Explorer 10 and 11, or later	JavaScript, cookies, Transport Layer Security (TLS) v1.1/v1.2, 128-bit encryption, Active scripting security setting, Compatibility View, set Check for newer versions of stored pages to Automatically .
Google Chrome 57 and later	JavaScript, cookies Note: The Chrome browser does not cache static content, such as images, CSS, or Javascript, with the system-provided self-signed certificate. This may cause the system to redownload static content when you refresh. To avoid this, add a self-signed certificate to the trust store of the browser/OS or use another web browser.

In addition, for managed Devices, a CLI is provided to manage the devices. This interface provides only a subset of the operations provided by the web interface. It is highly recommended that the users use the web interface over the CLI. All appliances, regardless of series or models, can access the shell bash (different from CLI) but this will remove the appliances from the evaluated configuration.

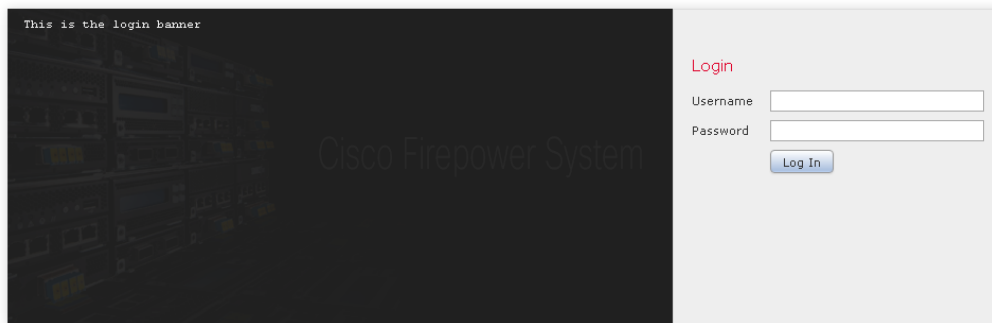
If you are the first user to log into the appliance after it is installed, you must log in using the factory-default administrative (**admin**) user account to complete the initial setup process. The default password for the 'admin' account is 'Admin123' and both FMC and FTD will force that password to be changed during initial login. By default, your session automatically logs out after 60 minutes of inactivity, unless you are viewing a page (such as an unpaused dashboard) that periodically communicates with the web server on the appliance.

1. Direct your web browser to <https://hostname/>, where hostname corresponds to the host name of the appliance. You can also use the IP address of the appliance.

The Login page appears.

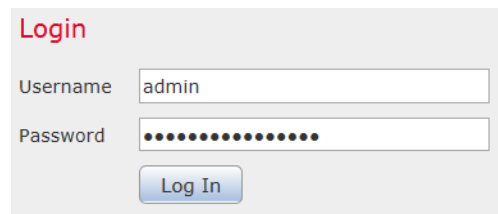


For technical/system questions, e-mail tac@cisco.com or call us at 1-800-553-2447 or 1-408-526-7209



NOTE! Observe the login banner under the Cisco Firepower logo.

2. In the **Username** and **Password** fields, type your username and password.

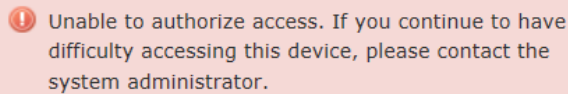


NOTE! Observe the password is not displayed.

3. Click **Log In**.

The default start page appears if the authentication is successful.

If authentication fails, the following error message is displayed:



Unable to authorize access. If you continue to have difficulty accessing this device, please contact the system administrator.

Audit Record:

2013-02-26 17:52:01	admin	Login	Login Success	10.4.10.227
2013-02-26 17:51:55	admin	Login	Login Failed	10.4.10.227

4.2.14.2 Login Locally (via serial console) to CLI

To login locally to FMC, connect to the console port of FMC.

4.2.15 Logout

To logout of FMC GUI:

1. For web session, from the drop-down list under your username, select **Log Out**.
2. Close the web browser.
3. For CLI, type the command **exit**.

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.

To logout of FMC CLI, the user can use the "exit" or "logout" commands.

4.2.16 Restrict Access

The system by default only supports SSH and HTTPS security protocols for management. Telnet and HTTP are not supported for management and cannot be enabled. SNMPv3 is supported but is not permitted for management—only for sending SNMP traps for alerting. 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 mode is enabled. While not required by the NDcPP, the administrator should configure access list to control which computers can access the appliances on specific ports.

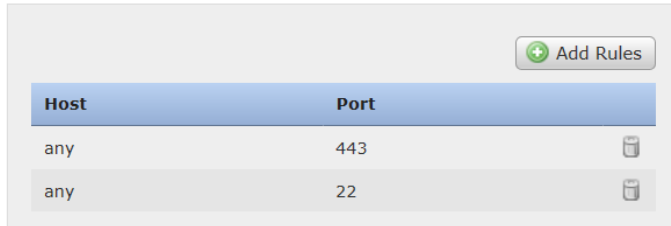
IMPORTANT! By default, access to the appliance is **not** restricted. To operate the appliance in a more secure environment, consider adding access to the appliance for specific IP addresses and then deleting the default **any** option.

By default, port 443 (HTTPS), which is used to access the web interface, and port 22 (SSH), which is used to access the command line, are enabled for any IP address. The access list is part of the system policy. Administrator can specify the access list either by creating a new system policy or by editing an existing system policy. In either case, the access list does not take effect until the system policy is applied.

1. Login with Administrator Role.

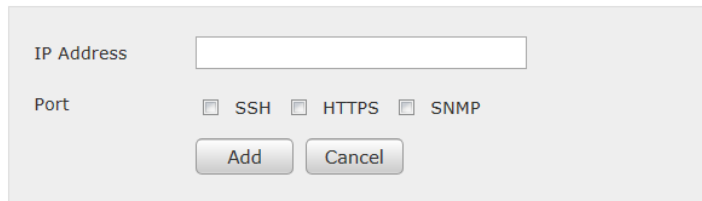
2. Depending on whether you are configuring audit log streaming for a Firepower Management Center or a managed Device:
 - Management Center—Choose **System > Configuration**.
 - Managed Device—Choose **Devices > Platform Settings** and create or edit a Firepower policy.
3. Click Access List.

The Access List page appears.



4. Click **Add Rules**.

The Add IP Address page appears.



5. In the IP Address field, you have the following options, depending on the IP addresses you want to add:
 - An exact IP address (for example, 10.6.50.81)
 - An IP address range using CIDR (for example, 192.168.0.0/16)
 - Any IP address using **any** term
6. Select **SSH** or **HTTPS** or both of these options to specify which ports you want to enable for these IP addresses.

WARNING! SNMP management must not be enabled in the evaluated configuration. SNMP cannot be used for management. However, encrypted SNMPv3 traps are allowed for alerting only.

7. Click **Add**.
8. Click the delete icon () to remove the permissive rules.

IMPORTANT! If you delete access for the IP address that you are currently using to connect to the appliance interface, and there is no entry for “IP=any port=443”, you will lose access to the system when you save (for FMC) or deploy (for Device) the setting.

9. Click **Save**.
10. Click **Deploy** if you are configuring these settings for the managed Devices. Select the Device(s) you want to deploy the setting to and click **Deploy** again.

Audit Record:

[2013-02-27 16:09:15](#) [admin](#) [System > Local > System Policy > Access List > Modified: Host\(Port\) any\(443\), any\(22\) > any\(443\), any\(22\), 10.5.61.80\(22\), 10.5](#)

Note: The Source IP field in the audit event above is cut off.

4.2.17 Configure Syslog over TLS for FMC and FTD

Administrator can configure the system so it can transmit audit and syslog records securely to an external audit server (Suggestion: syslog-ng, version 3.7 or later) while storing the audit and syslog records locally. The audit server must be functional and accessible before the appliance can send the audit records. The instructions in the section describe how to install X.509v3 certificates to enable syslog over TLS for messages generated by FMC and FTD. The FMC will start sending audit records over TLS once you save these settings on FMC. The FTD does not send audit records over TLS until you save the Platform Settings on FMC and deploy the updated Platform Settings to FTD and complete additional configuration steps described in section 4.4.9 Configure Logging).

To securely transmit log messages to an audit server, Transport Layer Security (TLS) is used between the Firepower system components (FMC and FTD) and the syslog-ng server. To securely send the logs to a trusted audit server, there are two requirements:

- Import a signed audit client certificate for the system. You can generate a certificate request based on your system information and the identification information you supply. Send the resulting request to a certificate authority to request a client certificate. After you have a signed certificate from a certificate authority (CA), you can import it.
- Configure the communication channel with the audit server (i.e., syslog-ng) to use TLS.

To verify the certificate status, configure the system to load one or more certificate revocation lists (CRLs). The system compares the server certificate against those listed in the CRLs. If a server offers a certificate that is listed in a CRL as a revoked certificate, the connection fails.

NOTE! If you choose to verify certificates using CRLs, the system uses the same CRLs to validate both the audit client and audit server certificates.

The Key establishment parameters for each of the TLS connections for FMC are as follows –

1. FMC/FMCv (HTTPS/TLS server for remote administration)- 2048-bit RSA and ECDHE secp256r1, secp384r1 and secp521r1
2. FMC/FMCv and FTD/FTDv (communications between FMC and FTD) – 2048-bit RSA and ECDHE secp256r1, secp384r1 and secp521r1

Audit log connection fails if the audit server certificate does not meet either one of the following criteria:

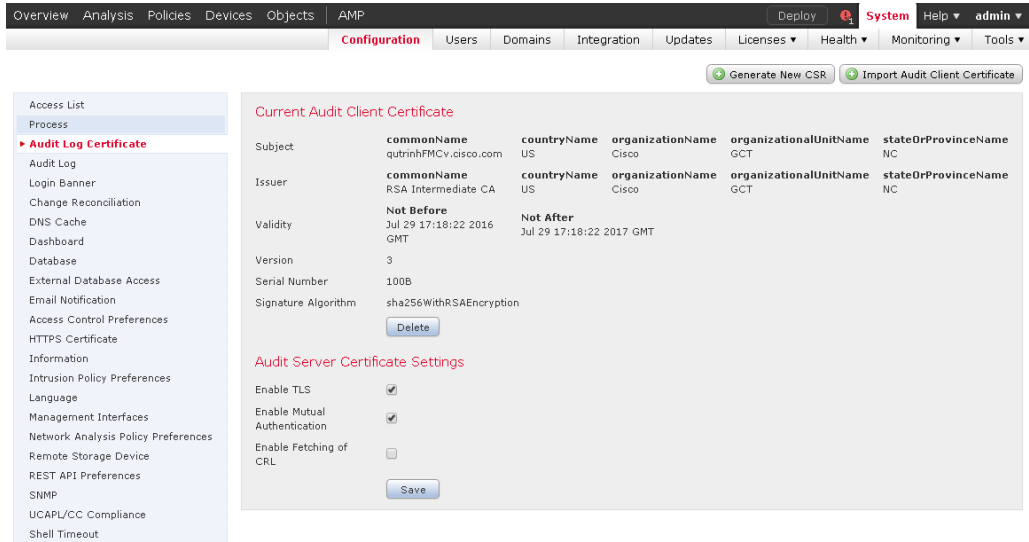
- The certificate is not signed by the CA with cA flag set to TRUE.
- The certificate is not signed by a trusted CA in the certificate chain.
- The certificate Subject Alternative Name (SAN) does not match the expected hostname (i.e., reference identifier).
- The certificate has been revoked or modified.

To view the client audit certificate:

1. Login with Administrator Role.
2. Depending on whether you are configuring audit log streaming for a Firepower Management Center (FMC) or a managed Device (FTD):
 - Management Center (FMC) —Choose **System > Configuration**.

- Managed Device (FTD) —Choose **Devices > Platform Settings** and create or edit a Firepower policy.

3. Select Audit Log Certificate.



Audit Record:

2016-11-15 20:22:55 admin System > Configuration > Configuration > /admin/audit_cert.cgi Page View 10.128.120.41

To generate a Certificate Signing Request (CSR):

1. Login with Administrator Role.
2. Depending on whether you are configuring audit log streaming for a Firepower Management Center or a managed Device:
 - Management Center (FMC) —Choose **System > Configuration**.
 - Managed Device (FTD) —Choose **Devices > Platform Settings** and create or edit a Firepower policy.
3. Select Audit Log Certificate.
4. Click Generate New CSR.
5. Enter a country code in the **Country Name (two-letter code)** field.
6. Enter a state or province postal abbreviation in the **State or Province** field.
7. Enter a Locality or City.
8. Enter an Organization name.
9. Enter an Organization Unit (Department) name.
10. Enter the fully qualified domain name for which you want to request a certificate in the **Common Name** field.

NOTE! If the CN and the DNS hostname do not match, the secure audit log connection will fail.

11. Click Generate.

12. Open a new blank file with a text editor.
13. Copy the entire block of text in the certificate request, including the *BEGIN CERTIFICATE REQUEST* and *END CERTIFICATE REQUEST* lines, and paste it into a blank text file.
14. Save the file with extensions .csr.
15. Click **Close**.

IMPORTANT! This method will automatically generate a RSA 2048-bits key pair and embed the public key in the CSR. In this case, you do not need to import the private key. However, if you generate the RSA key pair externally, then you will need to import the private RSA key.

To import the audit client certificate (on the FTD, use the command “configure audit_cert import”):

1. Login with Administrator Role.
2. Depending on whether you are configuring audit log streaming for a Firepower Management Center or a managed Device:
 - Management Center (FMC) —Choose **System > Configuration**.
 - Managed Device (FTD) —Choose **Devices > Platform Settings** and create or edit a Firepower policy.

3. Select Audit Log Certificate.
4. Click Import Audit Client Certificate.
5. Open the client certificate in a text editor, copy the entire block of text, including the *BEGIN CERTIFICATE* and *END CERTIFICATE* lines. Paste this text into the **Client Certificate** field.

IMPORTANT! The audit client certificate is expected to have the cA flag set to TRUE and critical. Other expected fields include: TLS Web Client Authentication (for X509v3 Extended Key Usage) and Digital Signature, Non Repudiation, Key Encipherment (for X509v3 Key Usage).

6. To import a private RSA key, open the private key file and copy the entire block of text, including the *BEGIN <KEY TYPE> PRIVATE KEY* and *END <KEY TYPE> PRIVATE KEY* lines. Paste this text into the **Private Key** field. If the key pair is generated internally, this field is not required.
7. Open each intermediate CA certificate and the root CA certificate, and copy the entire block of text for each, and paste it into the **Certificate Chain** field (concatenate as needed). The audit server certificate is signed by one of these CA in the chain.

IMPORTANT! The CA certificate must have the cA flag set to TRUE and critical.

WARNING! The audit client certificate is validated against the CA or CA certificates in the chain. The import will fail if the validation fails.

8. Click **Save**.
9. Click **Deploy** if you are configuring these settings for the managed Devices. Select the Device(s) you want to deploy the setting to and click **Deploy** again.

The system supports validating audit server certificates using imported CRLs in Distinguished Encoding Rules (DER) format.

If you choose to use CRLs, to ensure that the list of revoked certificates stays current, you can create a scheduled task to update the CRLs. The system displays the most recent refresh of the CRLs.

If you choose CRLs, the system uses the same CRLs to validate both audit client certificates and HTTPS certificate to secure the HTTPS connection between the system and a web browser. When the TOE cannot establish a connection for the validity check using CRL or the OCSP responder for verification, the FTD IPsec connections will reject the certificate when transmitting messages to the syslog server, while all FTD and FMC TLS connections will accept the certificate and the trusted channel will be established. If TLS sessions fail due to inability to contact the CRL or OCSP server (FTD only), restore connectivity to the CRL or OCSP server before reattempting to establish the TLS sessions.

4.2.17.1 Enable Syslog over TLS and Mutual Authentication

Enable TLS and mutual authentication with the audit server (i.e., syslog-ng):

1. Login with Administrator Role.
2. Depending on whether you are configuring audit log streaming for a Firepower Management Center or a managed Device:
 - Management Center (FMC) —Choose **System > Configuration**.
 - Managed Device (FTD) —Choose **Devices > Platform Settings** and create or edit a Firepower policy.
3. Select Audit Log Certificate.
4. Choose **Enable TLS** to use Transport Layer Security to send the audit and syslog log to an external audit server.

WARNING! This setting is required in the evaluated configuration.

5. Choose Enable Mutual Authentication.

WARNING! This setting is required in the evaluated configuration.

NOTE! If you enable mutual authentication without importing a valid audit client certificate, the secure audit log connection will fail.

6. You have two options:
 - To verify server certificate using one or more CRLs, select **Enable Fetching of CRL** and continue with Step 6. This setting is required in the evaluated configuration.
 - To accept server certificate without revocation check, skip to Step 9.
7. Enter a valid URL to an existing CRL file and click **Add CRL**. Repeat to up to 25 CRLs.

NOTE! Do not copy and paste the URL. Enter the URL manually.

8. Click **Refresh CRL** to load the current CRL or CRLs from the specified URL or URLs. Enabling fetching of the CRL creates a scheduled task to regularly update the CRL or CRLs. Edit the task to set the frequency of the update.
9. Click **Save**.
10. Click **Deploy** if you are configuring these settings for the managed Devices. Select the Device(s) you want to deploy the setting to and click **Deploy** again.

NOTE! Mutual authentication on the FTD has not been tested as part of the evaluation.

4.2.17.2 Specify the external audit server:

1. Login with Administrator Role.
2. Depending on whether you are configuring audit log streaming for a Firepower Management Center or a managed Device:
 - Management Center (FMC) —Choose **System > Configuration**.
 - Managed Device (FTD) —Choose **Devices > Platform Settings** and create or edit a Firepower policy.
3. Select Audit Log.
4. Select Enabled from the Send Audit Log to Syslog drop-down menu.
5. Specify the destination host for the audit information by using its fully qualified name (e.g., syslog.cisco.com, which will be used as its reference identifier) of the syslog server in the **Host** field. The default port (514) would be used but when TLS is enabled, port 6514 will be used.
6. Click **Save**.
7. Click **Deploy** if you are configuring these settings for the managed Devices. Select the Device(s) you want to deploy the setting to and click **Deploy** again.

Audit Record:

2016-11-15 20:34:07	admin	Devices > Platform Settings > Audit Log Settings > Modified: Send Audit Log to Syslog Disabled > enabled	Save	10.128.120.41
2016-11-15 20:34:07	admin	Devices > Platform Settings > Audit Log Settings > Modified: Host > 172.18.152.193	Save	10.128.120.41

4.2.17.3 Configure the external audit server (i.e., syslog-ng daemon):

1. Login as authorized administrator.
2. Install syslog-ng with version 3.7² or later.
3. Edit the syslog-ng configuration file by adding the following section below.

```
vi /etc/syslog-ng/syslog-ng.conf
```

It maybe a different path depending on OS.

Or you can search for it. "find / -name syslog-ng.conf"

```
source s_network_TLS {
  tcp( port(6514)
    tls(
      key-file("/etc/ssl/server.key.pem") # Private key of audit server certificate
      cert-file("/etc/ssl/server.cert.pem") # Audit server certificate
      ca-dir("/etc/ssl") # Location of the CA certificates and symbolic links. See below
```

² Another option is rsyslog with stunnel but this configuration is not described in this document.

```
    ### openssl x509 -noout -hash -in rootCA.pem
    ### ln -s rootCA.pem 2e286222.0
    ### This is the CA that signed the audit client certificate and other CA(s) in the chain.
    ### All CA certs must have basic constraints CA flag set to TRUE and critical
    cipher-suite(AES128-SHA) # e.g., TLS Ciphersuite to be supported by the server
    ssl-options(no-ssl2, no-ssl3, no-tls1) # no-ssl2, no-ssl3, no-tls1, no-tls11, no-tls12
    peer-verify(required-trusted) # required-trusted for mutual auth, optional-trusted for no auth
)
);
};

destination d_local {
    file("/var/log/remote_messages"); # The remote syslog file location can be configured here
};

log {
    source(s_network_TLS); destination(d_local);
};
```

NOTE! When CC mode is enabled, the TLS version and cipher suites will be limited to the ones claimed in the Security Target. The audit server setting must include those versions and cipher suites, or the secure audit log connection will fail.

4. Restart the syslog-ng server and make sure there is no error message.
`/etc/rc.d/init.d/syslog-ng restart` # Command may be different depending on the OS.
5. Use netstat to make sure the syslog-ng is listening.
`netstat -an | grep 6514`
6. Make sure port 6514 is opened by the firewall to allow the connection.

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

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

4.3 FTD Installation

To install FTD, refer to the appropriate guidance documents for each hardware model as listed here.

ASA 5508-X and ASA 5516-X:

- a) Refer to the [Cisco ASA 5508-X and ASA 5516-X Hardware Installation Guide](#) to mount the appliance, connect the console cable, and connect power.

- b) If reimaging is required, refer to the “Reimage the ASA 5500-X or ISA 3000” section of the [Cisco ASA and Firepower Threat Defense Reimage Guide](#).
- c) Refer to the “Firepower Threat Defense Deployment with FMC” chapter of the [Cisco ASA 5508-X and 5516-X Getting Started Guide](#) to connect power and cabling, complete the initial configuration, and register the FTD with an FMC.

ISA 3000:

- a) Refer to the [Cisco ISA 3000 Industrial Security Appliance Hardware Installation Guide](#) to mount the appliance, connect the console cable, and connect power.
- b) If reimaging is required, refer to the “Reimage the ASA 5500-X or ISA 3000” section of the [Cisco ASA and Firepower Threat Defense Reimage Guide](#).
- c) Refer to the “Firepower Threat Defense Deployment with FMC” chapter of the [Cisco ISA 3000 Getting Started Guide](#) to connect power and cabling, complete the initial configuration, and register the FTD with an FMC.

FTDv:

- a) Refer to the [Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide](#) and the [Cisco Firepower Threat Defense Virtual for KVM Getting Started Guide](#) to mount the appliance, connect the console cable, and connect power.
Refer to the “Managing the Firepower Threat Defense Virtual with the Firepower Management Center” chapter of the [Cisco Secure Firewall Firepower Threat Defense Virtual for VMware Getting Started Guide](#) and the [Cisco Secure Firewall Firepower Threat Defense Virtual for KVM Getting Started Guide](#) to connect power and cabling, complete the initial configuration, and register the FTD with an FMC.

4.4 FTD Initial Configuration

Unless indicated otherwise within the text below, the instructions in this section are applicable to FTD running on all hardware platforms.

4.4.1 *Ensure FTD is Managed by FMC*

If the FTD ‘manager’ was not configured on FTD via the setup wizard that runs on FTD during initial login, the manager can be configured later using the “configure manager add” command. Refer to the “Firepower Threat Defense Deployment with FMC” chapter of the platform-specific [Getting Started Guide](#) [FMC-GS] to configure licensing, and register the FTD with an FMC.

Once an FTD has been joined with an FMC, removing the FTD from FMC (using the “configure manager delete” command on FTD) would remove the FTD from its CC-evaluated configuration. If it becomes necessary to remove an FTD from FMC, the FTD must be re-joined with the same or different FMC (configured in accordance with this guide), and the FTD Platform Policy must be deployed to the FTD to return the FTD to the CC-evaluated configuration.

4.4.2 *Enable CC Mode and FIPS Mode*

CC Mode is not enabled by default, but must be enabled in the CC-evaluated configuration. After CC Mode is enabled, the mode cannot be disabled nor changed to another mode. Enabling either CC Mode will implicitly also enable FIPS Mode. For an overview of the of the non-default security features enforced when CC Mode is enabled, refer to the “Security Certifications Compliance Characteristics” section of [FMC-CG].

Warning: After enabling FIPS Mode or CC Mode on FTD those modes cannot be disabled. Disabling these modes would require reinstallation of FTD.

4.4.3 Common Criteria (CC) Mode

Enabling CC mode will limit algorithms used for HTTPS/TLS and SSH to ones listed below and will implicitly enable FIPS Mode. To enable CC mode, refer to the “Enable Security Certifications Compliance” section of [FMC-CG] and follow instructions to configure the “FTD device” as summarized here:

- 1) In FMC, navigate to Devices > Platform Settings and create a Firepower Threat Defense Policy if one has not already been created for your FTD.
- 2) In FMC, navigate to Devices > Platform Settings > UCAPL/CC Compliance, and set the compliance mode to “CC”.
- 3) Click “Save”.
- 4) Deploy the Platform Policy to the FTD. This will result in rebooting the FTD, and regenerating SSH keys on the FTD. SSH will be limited to SSHv2 with these algorithms:
 - Encryption: aes128-cbc, aes256-cbc, AEAD_AES_128_GCM, and AEAD_AES_256_GCM
 - HMAC: hmac-sha1, hmac-sha2-256, hmac-sha2-512, AEAD_AES_128_GCM, and AEAD_AES_256_GCM
 - DH: diffie-hellman-group14-sha1
- 5) In FMC, navigate to Devices > Platform Settings > SSL > Add ...
Version: Default
Security Level: Custom
Under Available Algorithms select one or more of these choices and click the Add button so they appear under Selected Algorithms.
 - ECDHE-ECDSA-AES256-GCM-SHA384
 - ECDHE-ECDSA-AES128-GCM-SHA256
 - ECDHE-ECDSA-AES256-SHA384
 - ECDHE-ECDSA-AES128-SHA256Click “Save”
Click “Deploy”

This will allow the FTD TLS client to only use the selected algorithms.

The TLS ciphersuites used between the FMC/FMCv TLS client and the remote syslog server are limited to:

- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 (TLSv1.2, TLSv1.1)
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246 (TLSv1.2, TLSv1.1)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 (TLSv1.2 only)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 (TLSv1.2 only)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 (TLSv1.2, TLSv1.1)

The TLS ciphersuites used between FTD and FMC are limited to:

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 (TLSv1.2 only)
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268 (TLSv1.2 only)
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 (TLSv1.2 only)
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246 (TLSv1.2 only)
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288 (TLSv1.2 only)
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288 (TLSv1.2 only)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492 (TLSv1.2 only)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492 (TLSv1.2 only)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 (TLSv1.2 only)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 (TLSv1.2 only)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 (TLSv1.2 only)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 (TLSv1.2 only)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492 (TLSv1.2 only)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492 (TLSv1.2 only)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 (TLSv1.2 only)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 (TLSv1.2 only)
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 (TLSv1.2 only)
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 (TLSv1.2 only)

The TLS ciphersuites used between the FTD TLS client and a remote syslog server are limited to:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 (TLSv1.2, TLSv1.1)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 (TLSv1.2, TLSv1.1)
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 (TLSv1.2 only)
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 (TLSv1.2 only)

The TLS ciphersuites used between the FTD OS TLS client and a remote syslog server are limited to:

- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 (TLSv1.2, TLSv1.1)
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246 (TLSv1.2, TLSv1.1)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 (TLSv1.2 only)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 (TLSv1.2 only)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 (TLSv1.2, TLSv1.1)

The following cryptographic algorithms are used for implementing the IPsec protocol ESP as defined by RFC 4303 –

- AES-CBC-128 (RFC 3602)
- AES-CBC-256 (RFC 3602)
- AES-GCM-128 (RFC 4106)
- AES-GCM-256 (RFC 4106)

The following Secure Hash Algorithm (SHA)-based HMAC are used for implementing the IPsec protocol ESP –

- HMAC-SHA-1
- HMAC-SHA-256
- HMAC-SHA-384
- HMAC-SHA-512

Note: The web server on FTD (Firepower Device Manager, FDM) is disabled whenever FTD is managed by (has been registered to) an FMC.

4.4.4 Configure Authentication

FTD supports multiple locally stored administrative accounts, each of which is assigned one of two roles, either “config” (read-write) or “basic” (read-only). Accounts can only be managed via the “ftd” shell. Each account can be configured with its own parameters. The chapter – “Using the Command Line Interface (CLI)” in [FTD-CLI] provides instructions for logging into the FTD appliance via SSH.

At minimum, to adhere to the CC-evaluated configuration, the default ‘admin’ account must be configured according to the settings listed below. To configure FTD accounts, refer to the commands referenced below as described in [FTD-CLI] for the commands begin with “configure user”, e.g. “configure user access” or “configure user aging”:

- 1) Access Level: Any setting is acceptable (either “config” or “basic”).
 - a) The access level of the default ‘admin’ account cannot be changed, it’s set to ‘config’.
 - b) If additional accounts are created, specify the access level by using the “configure user add” command.
- 2) Aging: (optional) Any setting is acceptable.
- 3) ForceReset: (optional) To force a user to change their password at their next login, use the “configure user forcereset” command.
- 4) MaxFailedLogins: Set this limit using the “configure user maxfailedlogins” command.
 - a) For the default ‘admin’ account, and another custom accounts, set the value to a positive integer (from 1-99).
 - b) If that limit of consecutive failed logins occurs, the account will be locked until unlocked by another administrative account that has its access level set to ‘config’.

Note: When an account is locked due to the maximum number of failed login attempts being exceeded, the CLI outputs a message reporting that the account is locked due to a specified number of authentication failures. The user should be aware that there is an error/bug in the output message which always specifies the number of failures as being 1 more than the actual number of authentication failures. Or in other words, the actual number of authentication failures is 1 less than the number reported by the output message.

- 5) MinPasswdLen: Set to eight (8) or greater using the “configure user minpasswdlen” command. The maximum allowable value assigned to minpasswdlen is 32.
- 6) StrengthCheck: Set to “enable” using the “configure user strengthcheck” command. Once this setting is enabled for a user, the strength check will be enforced the next time that user resets their password (the strength check cannot be enforced on passwords that were set prior to enabling StrengthCheck for that user).
- 7) Unlock: (as needed) To unlock an FTD account that has become locked due to exceeding the MaxFailedLogins limit use the “configure user unlock” command. When an account is locked due to exceeding the limit, output of the “show user” command will show “Yes” under the “Lock” column, and will show “No” after unlocking the account, as shown in the screenshot below.

```
> show user lockme
Login      UID    Auth Access  Enabled Reset   Exp Warn  Str Lock Max
lockme    1001  Local Config Enabled  No    Never N/A  Dis Yes  3

> configure user unlock lockme

> show user lockme
Login      UID    Auth Access  Enabled Reset   Exp Warn  Str Lock Max
lockme    1001  Local Config Enabled  No    Never N/A  Dis No  3

>
```

The passwords are stored in a hashed form using Approved SHA-512 with a 32-bit salt value.

4.4.5 Configure the Pre-Login Banner

Configure a pre-login banner that will be displayed prior to entering the administrator password during login to FTD. For an overview of Platform Settings, and how to assign Platform Settings to an FTD, refer to the “Platform Settings Policies” chapter in [FMC-CG]. To configure a pre-login banner for FTD, in FMC navigate to **Devices > Platform Settings > Banner**, enter the login banner in the pre-login banner, and click Save, then deploy the updated Platform Settings to all FTD devices to which the Platform Settings have been assigned. For more detail, refer to the “Configure Banners” subsection of the “Platform Settings for Firepower Threat Defense” section in [FMC-CG].

4.4.6 Configure the Clock

The FTD on the ASA 5500-X and ISA3000 platforms and FTDv must be configured to synchronize their clocks with FMC. To configure each FTD to receive clock updates from FMC, configure the Platform Settings for each FTD and deploy the updated Platform Settings to each FTD by following these steps:

1. Login to FMC with Administrator Role.
2. Choose **Devices > Platform Settings** and create or edit a Firepower or FTD policy.
3. On the left, select **Time Synchronization**.
4. Select **Via NTP from Management Center**.
5. Click **Save**.
6. Click **Deploy** if you are configuring these settings for the managed Devices. Select the Device(s) you want to deploy the setting to and click **Deploy** again.

Note: The NTP protocol is used over TLS (FPT_ITT.1) to synchronize the time between the TOE components. There is no NTP server/listener on FMC that would be accessible outside that TLS channel for FPT_ITT.

4.4.7 Configure Inactivity Timeout Settings

Enable inactivity timeouts for administrative sessions on FTD by following instructions in the “Configure Global Timeouts” section of [FMC-CG], and adhere to these parameters:

- Set the “Console Timeout” to 5 or more minutes (configurable from 5-1440 minutes). Note: the “console timeout” value applies to all CLI access, including serial console and SSH.
- Setting any other timeout value is optional in the CC-evaluated configuration.

4.4.8 Disable the HTTP (HTTPS) Server

The FTD has a built-in web server with a WebUI for remote administration, but that interactive WebUI is disabled once the FTD is configured to be ‘managed’ by an FMC. Though the WebUI remains enabled by default to support the ability for authenticated administrators to download packet capture files. Use the FMC WebUI to disable the FTD HTTP (HTTPS) server by unchecking the “Enable HTTP Server” box under: **Devices > Platform Settings > (edit any and all applicable platform settings) > HTTP > Enable HTTP Server** (uncheck the box), then click Save, then deploy the update to each applicable FTD.

4.4.9 Configure Logging

FTD generates audit messages from three internal sources, each of which uses a separate mechanism to transmit messages from FTD to another host. In all cases, once use of a remote audit server has been configured, messages will be simultaneously written locally and transmitted to the remote server(s). Enabling use of a remote audit server will not result on previously generated messages being transmitted to that server.

- 1) System event messages: These messages include system-level events including clock changes, and authentication of administrators to the FTD CLI. These messages are sent from the FTD OS TLS client to an external syslog server.
- 2) Firewall (Access Control Policy): These messages can be viewed in the local logging buffer of FTD using the command “show logging”. These messages are sent from the FTD TLS client to an external syslog server. In addition, these messages can optionally be configured to also be sent over TLS from FTD to FMC where they would be viewable in FMC as they are stored in the connection database.
- 3) VPN messages: These messages can be viewed in the local logging buffer of FTD using the command “show logging”. These messages are sent from the FTD TLS client to an external syslog server. In addition, these messages can optionally be configured to also be sent over TLS from FTD to FMC where they would be viewable in FMC via System > Monitoring > Syslog.
- 4) IPS messages: These messages are automatically transmitted over TLS by FTD to FMC for storage, and are viewable via the “Audit Log” within FMC. IPS messages generated on FTD are temporarily stored locally on FTD in a database prior to transmission to FMC, so if the connection from FTD to FMC is interrupted the IPS messages will be transmitted once connectivity is restored.

4.4.9.1 Transmit FTD System Messages to a Syslog Server

The FTD OS TLS client implementation is configured through the FTD’s command line and sends audit events such as SSH login, console login, etc. to an external syslog server. Mutual authentication is supported. To transmit FTD system messages to a remote syslog server, follow these instructions:

- 1) Configure use of certificates if enabling syslog-over-TLS:
 - a) To display the syslog certificate if present: **show audit-cert**
 - b) Import the certificates (the CA chain, the client cert and the client key): **configure audit_cert import**
 - i) **Note:** Import the audit certificate chain first (option 2) before importing the client certificate and private key (option 1).
 - c) If necessary, delete the syslog server certs: **configure audit_cert delete**
- 2) Configure one or more syslog servers:
 - a) Display the current syslog server information if present: **show syslog-config**
 - b) Configure the syslog server details on the FTD: **configure syslog_server setup**
 - i) First it prompts for the server host.
 - ii) Next it asks if you want TLS enabled.

- iii) Next it asks if you want Mutual Authentication enabled. The option – “No” should be selected.
- iv) **Note 1:** If the syslog server entry is defined by its FQDN, it must be resolvable via DNS.
- v) **Note 2:** The syslog server must be configured correctly to receive syslog messages from FTD.
- c) If desired, disable the syslog config (server details remain on FTD, and can be re-enabled):
configure syslog_server disable
- d) If desired, re-enable a syslog server, if it had been disabled: **configure syslog_server enable**
- e) If desired, disable the syslog server config and deletes the config: **configure syslog_server delete**
- f) Modify the syslog-tls.conf.tt file (/ngfw/usr/local/sf/htdocs/html_templates/stig/syslog-tls.conf.tt) to add the following change to restrict the supported ciphers for the TLS connection between the FTD OS TLS client and the syslog server to the ones listed in the ST and section 4.4.3 of this document – cipher-suite("ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:AES256-SHA256:AES128-SHA256")

4.4.9.2 Transmit Firewall and VPN Messages to a Syslog Server

The FTD TLS Client is configured by the FMC and is the main audit system for audits generated by FTD. It sends audit events such as IPsec and login messages to the external syslog server. Mutual authentication is not supported. To configure firewall and VPN messages to be sent to a remote syslog server, refer to the “Configure Syslog Logging for FTD Devices” section of [FMC-UG], configuring at least the parameters summarized here:

- 1) In FMC, navigate to **Devices > Platform Settings > Syslog**.
- 2) On the “Logging Setup” tab, click the “Enable Logging” box.
- 3) On the “Logging Destinations” tab, configure at least one entry with the logging destination of “Syslog Servers”.
- 4) On the “Syslog Servers” tab, add at least one syslog server. Use of “secure syslog” (syslog-over-TLS) by clicking the “Enable secure syslog” box is allowed in the CC-evaluated configuration, but it has some constraints:
 - a) Connections between the FTD and the syslog-over-TLS server cannot occur via the FTD’s ‘management’ interface, these connections must use one of the FTD’s data interfaces (specified as a “security zone” or a “named interface”).
 - b) Use of X.509v3 certificates is required, including:
 - i) Generating a device certificate for the FTD. For instructions to load syslog server certificates, refer to the “Managing FTD Certificates” section of [FMC-CG].
 - ii) Installing the FTD’s device certificate to the syslog server.

4.4.9.3 Configure FTD (via FMC) to send syslog over TLS

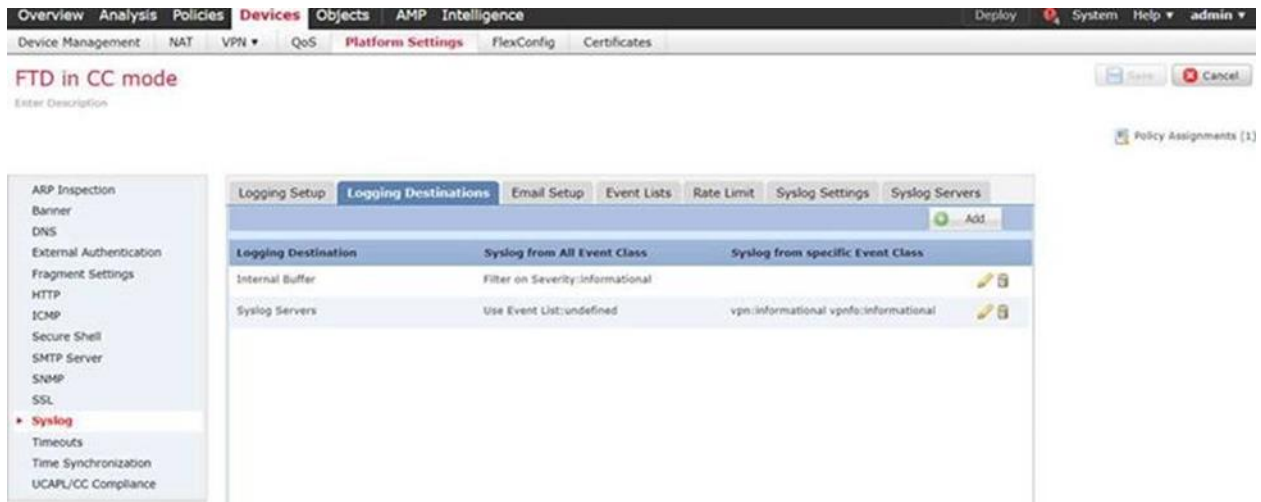
Syslog Severity Levels

Level Number	Severity Level	Description
--------------	----------------	-------------

0	Emergencies	System is unusable.
1	Alert	Immediate action is needed.
2	Critical	Critical conditions
3	Error	Error conditions
4	Warning	Warning conditions
5	Notification	Normal but significant conditions
6	Informational	Informational messages only
7	Debugging	Debugging messages only

1. Login with Administrator Role.
2. Choose **Devices > Platform Settings** and create or edit a FTD policy.
3. Click **Syslog** (FTD only).
4. Click the **Logging Setup** tab to enable logging and configure logging settings. You must enable logging for the system to generate syslog messages for data plane events.
 - a. **Enable Logging**—Turns on data plane system logging for FTD.
 - b. **Send debug messages as syslogs**—Redirects all the debug trace output to the syslog. The syslog message does not appear in the console if this option is enabled. Therefore, to see debug messages, you must enable logging at the console and configure it as the destination for the debug syslog message number and logging level. The syslog message number used is 711011. Default logging level for this syslog is debug.
 - c. **Memory Size of Internal Buffer**—Specify the size of the internal buffer to which syslog messages are saved if the logging buffer is enabled. When the buffer fills up, it is overwritten. The default is 4096 bytes. The range is 4096 to 52428800.
 - d. (Optional) Enable VPN logging by checking the **Enable Logging to FMC** checkbox. Choose the syslog severity level for VPN messages from the **Logging Level** drop-down list.
 - e. Click **Save**.
5. Click the **Logging Destinations** tab to enable logging to specific destinations and to specify filtering on message severity level, event class, or on a custom event list.
 - a. Click **Add** to enable a destination and apply a logging filter, or edit an existing destination.
 - b. In the **Logging Destinations** dialog box, select a destination and configure the filter to use for a destination:
 - i. Choose the destination you are enabling in the **Logging Destination** drop-down list. You can create one filter per destination: Console, E-Mail, Internal buffer, SNMP trap, SSH Sessions, and Syslog servers.
 - ii. In **Event Class**, choose the filter that will apply to all classes not listed in the table. You can configure these filters.
 1. **Filter on severity**—Select the severity level. Messages at this level or higher are sent to the destination.

2. **Use Event List**—Select the event list that defines the filter. You create these lists on the **Event Lists** tab
3. **Disable Logging**—Prevents messages from being sent to this destination.
- iii. If you want to create filters per event class, click **Add** to create a new filter, or edit an existing filter, and select the event class and severity level to limit messages in that class. Click **OK** to save the filter. The GUI will show a summary of the Logging Destination configuration, as in this screenshot:



- iv. Click **Save** to save changes to the Platform Settings.
6. Click the **Syslog Settings** tab to specify the logging facility, enable the inclusion of a timestamp, and enable other settings to setup a server as a syslog destination.
 - a. Select a system log facility for syslog servers to use as a basis to file messages in the **Facility** drop-down list.
 - b. Check the **Enable timestamp on each syslog message** check box to include the date and time a message was generated in the syslog message.
 - c. If you want to add a Device identifier to syslog messages (which is placed at the beginning of the message), check the **Enable Syslog Device ID** check box and then select the type of ID.
 - d. Click **OK** and **Save**.
7. Click the **Syslog Servers** tab to specify the IP address, protocol used, format, and security zone for the syslog server that is designated as a logging destination.
 - a. Check the **Allow user traffic to pass when TCP syslog server is down** check box, to allow traffic if any syslog server that is using the TCP protocol is down.
 - b. Enter a size of the queue for storing syslog messages on the security appliance when syslog server is busy in the **Message queue size (messages)** field. The minimum is 1 message. The default is 512. Specify 0 to allow an unlimited number of messages to be queued (subject to available block memory).
 - c. Click **Add** to add a new syslog server

- i. In the **IP Address** drop-down list, select a network host object that contains the IP address of the syslog server.
- ii. Choose the protocol (either TCP or UDP) and enter the port number for communications between the FTD and the syslog server. The default ports are 514 for UDP, 1470 for TCP. Valid non-default port values for either protocol are 1025 through 65535.
- iii. Check the **Enable Secure Syslog** check box to encrypt the connection between the Device and server using TLS over TCP.

You must select TCP as the protocol to use this option. You must also upload the certificate required to communicate with the syslog server on the **Devices > Certificates** page. Finally, upload the certificate from the FTD to the syslog server to complete the secure relationship and allow it to decrypt the traffic.

- iv. Add the zones that contain the interfaces used to communicate with the syslog server. For interfaces not in a zone, you can type the interface name into the field below the **Selected Zones/Interface** list and click **Add**. These rules will be applied to a Device only if the Device includes the selected interfaces or zones.

NOTE! *If the syslog server is on the network attached to the physical Management interface, you must type the name of that interface into the **Interface Name** field below the **Selected Security Zones** list and click **Add**. You must also configure this name (if not already configured), and an IP address, for the Diagnostic interface (edit the Device from the Device Management page and select the Interfaces tab).*

- v. Click **OK**.
8. After you save the changes, click **Deploy** to deploy the policy to assigned Devices. The changes are not active until you deploy them.

4.4.9.4 Configure FTD to configure timestamps

To ensure the year is included in the time stamp for the audit messages, perform the following steps:

- Click the Syslog Settings tab to specify the logging facility, enable the inclusion of a timestamp, and enable other settings to setup a server as a syslog destination.
- Select a system log facility for syslog servers to use as a basis to file messages in the Facility drop-down list.
- Check the Enable timestamp on each syslog message check box to include the date and time a message was generated in the syslog message.
- If you want to add a Device identifier to syslog messages (which is placed at the beginning of the message), check the Enable Syslog Device ID check box and then select the type of ID.
- Click OK and Save.

4.4.10 Configure CLI Lockdown on FTD

By default, the FTD shell allows use of the “expert” command to transmission from the ‘ftd’ shell to a Linux shell. This access must be disabled in the CC-evaluated configuration. Once this access is disabled, any future access to the Linux shell will require contacting Cisco TAC and completing a challenge-

response key exchange that will temporarily re-enable access to the Linux shell for troubleshooting purposes. Once access to the Linux shell is reactivated the FTD is no longer considered to be in the CC-evaluated configuration. To prohibit use of the 'expert' command, use the "system lockdown-sensor" command as described in [FTD-CLI].

4.4.11 FTD Logout

To logout of FTD CLI and FTD SSH CLI, type "exit".

Audit Record:

[2013-02-26 18:26:30](#) [admin](#) [Logout](#)

[Logout_Success](#)

[10.4.10.227](#)

5 FTD Access Control Policies

5.1 FTD Interface Modes: Firewall, IPS-Only, or IDS-Only

FTD interfaces can be configured in firewall mode, which is the default mode for FTD interfaces (where the interface Mode is set to “None”); or FTD interfaces can be in an IPS (Inline Sets) or IDS mode (Passive). When configured as an IPS or IDS interface, the primary functionality of the interface is to provide IPS functionality such as deep packet inspection, IPS signature matching, malware detection, URL filtering, etc.

Configuring interfaces in IPS or IDS modes is permitted in the CC-evaluated configuration, and if any FTD interfaces are configured as IPS-only or IDS interfaces there some essential caveats to ensuring the FTD is operating in the CC-evaluated configuration:

- 1) The FTD must have at least two interfaces that are configured in firewall mode.
- 2) VPN gateway functionality is only supported on interfaces configured in firewall mode.
- 3) Interfaces configured as Inline sets can be configured to enforce CC-evaluated traffic flow controls with respect to firewall functionality, but not VPN gateway functionality.
- 4) Interfaces configured in Passive mode (or ERSPAN mode) do not violate CC-evaluated traffic flow controls because such interfaces do not forward traffic, nor do Passive interfaces support or enforce any CC-evaluated traffic flow controls because they cannot forward traffic and cannot function as VPN gateway endpoints.

In a Passive mode, an FTD interface will only receive traffic, and will not forward that traffic to any other interface (thus functioning as a sensor interface of an IDS). When configured as an Inline set or in firewall mode, the interface will forward network traffic flows across the FTD (if such traffic is explicitly permitted by Access Control Policies (ACP). One FTD can have multiple interface configurations, for example, where two interfaces are configured as inline pair, and a third interface is configured as passive, and other interfaces are configured in regular firewall mode.

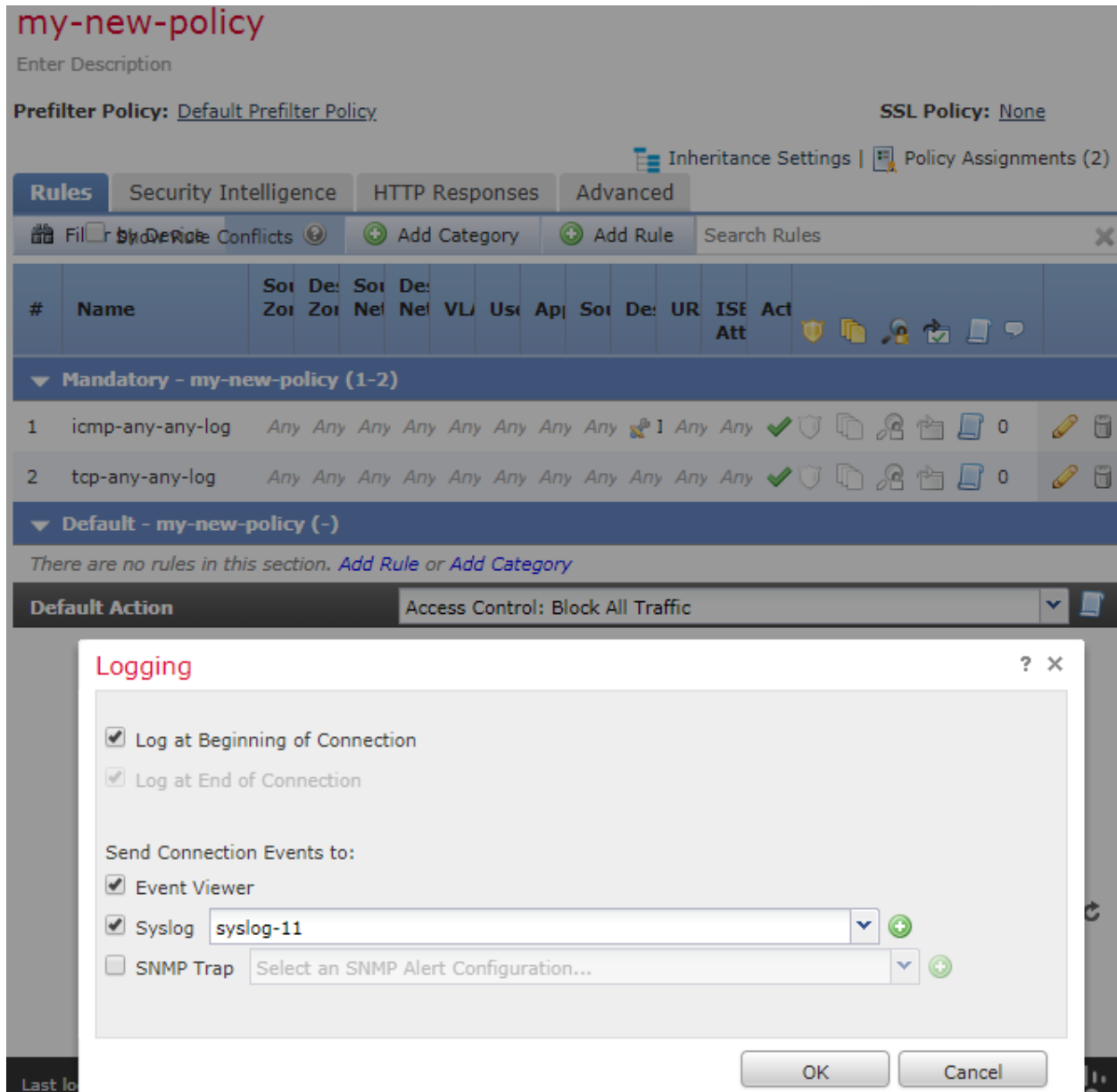
Traffic policies are defined in terms of network “zones”, also called “Security Zones,” which in turn are associated with FTD interfaces. So, an Access Control Policy may be defined to allow traffic from “zone0” to “zone1”, though those zones may be mapped to interfaces labeled “outside” and “inside” on one FTD and the same zones can also be mapped to interfaces labeled “int1” and “int2” of another FTD which enforces the same policy.

There are multiple types of policies that can be layered to apply to the same traffic flows (same zone-to-zone mappings). Having one type of policy applied to a zone/interface is sufficient to allow traffic flow. Traffic flow policy types include Prefilter, Access Control, and Intrusion policies.

Prefilter policies are sub-policies of Access Control policies, and every Access Control policy has an associated Prefilter policy, which is used to define rules for encapsulated traffic. There is no default action for nonencapsulated traffic; if a nonencapsulated connection does not match any prefilter rules, the system continues with applying rules in the Access Control policy. A Prefilter policy can contain multiple rules, which are enforced in the sequence they appear in the policy (the first rule that matches the traffic is the one that’s applied).

No FTD interface will forward traffic until policies have been configured and applied to that interface. Traffic will not be forwarded unless it’s explicitly permitted by at least one policy rule, thus an implicit “deny-all” rule is applied to all interfaces to which any traffic filtering rule has been applied. The implicit deny-all rule is executed after all admin-defined rules have been executed, and will result in dropping all

traffic that has not been explicitly permitted, or explicitly denied. If an administrator wants to log all denied traffic, a rule entry should be added that denies all traffic and logs it, e.g. by either adding a rule at the end of a policy to explicitly drop and log all traffic, or by setting the Default Action for the policy to block all traffic, and enabling logging for the default rule, as show in this example:



5.1.1 Firewall and VPN Gateway Interfaces

FTD interfaces configured as firewall interfaces (including interface types labeled as ASA, Routed, or Switched), are interfaces that enforce the CC-evaluated traffic flow controls related to firewall functionality and VPN gateway functionality. Each of these interfaces will:

- 1) Be associated with a single Security Zone.
- 2) Enforce Access Control Policies, which are defined in terms of Security Zones.
- 3) Function as an VPN Gateway interface if an IP address has been assigned to the interface.

5.1.2 Passive Interfaces (IDS-only interfaces)

Through passive interfaces the FTD monitors traffic flowing across a network using a switch SPAN or mirror port. The SPAN or mirror port allows for traffic to be copied from other ports on the switch. This provides the system visibility within the network without being in the flow of network traffic. Passive interfaces receive all traffic unconditionally, and no traffic received on these interfaces is retransmitted.

5.1.3 Inline Interface Sets (IPS-only interfaces)

Inline Sets of interfaces on the FTD support traffic flows across the FTD, binding two ports together. This allows the system to be installed in any network environment without the configuration of adjacent network Devices. Inline interfaces receive all traffic unconditionally, but all traffic received on these interfaces is retransmitted out of an inline set unless explicitly dropped.

5.2 Configure Access Control Policies

An Access Control Policy (ACP) determines how the system handles traffic on the monitored network. Administrators can configure one or more access control policies, which they can then apply to one or more managed Devices. Each Device can have only one applied policy though. Access control rules can be added to a policy to provide granular control how traffic is handled and logged.

For each rule, administrator can specify a rule *action*, that is, whether to trust, block, or inspect matching traffic with an intrusion policy. Each rule contains a set of conditions that identify the specific traffic you want to control. Rules can be simple or complex, matching traffic by any combination of security zone, IP address, application, protocols, ports, etc. The system matches traffic to access control rules in order; the first matched rule handles the traffic.

5.2.1 Access Control Policies (ACP)

On the Access Control Policy page (**Policies > Access Control**) administrator can view all the current access control policies by name and optional description and the following status information:

- When a policy is up to date on targeted Devices, in green text.
- When a policy is out of date on targeted Devices, in red text.

The default access control policy blocks all traffic from entering your network.

The TOE supports all IPv4 protocols excluding Protocol 2 (IGMP) which is not routable and thus will not be forwarded by the TOE.

The TOE supports the following 15 IPv6 protocols:

- Transport Layer Protocol 4 - IPv4 encapsulation
- Transport Layer Protocol 6 - Transmission Control
- Transport Layer Protocol 8 - Exterior Gateway Protocol
- Transport Layer Protocol 9 - any private interior gateway
- Transport Layer Protocol 17 - User Datagram
- Transport Layer Protocol 41 - IPv6 encapsulation
- Transport Layer Protocol 46 - Reservation Protocol
- Transport Layer Protocol 47 - General Routing Encapsulation

- Transport Layer Protocol 49 - BNA
- Transport Layer Protocol 58 - ICMP for IPv6
- Transport Layer Protocol 59 - No Next Header for IPv6
- Transport Layer Protocol 88 - TCF
- Transport Layer Protocol 89 - EIGRP
- Transport Layer Protocol 105 - SCPS Transport Layer Protocol
- Transport Layer Protocol 112 - Virtual Router Redundancy Protocol

All other IPv6 protocols from the RFC Values for IPv4 and IPv6 table in the MOD VPNGW SD v1.1 are dropped by default by the TOE.

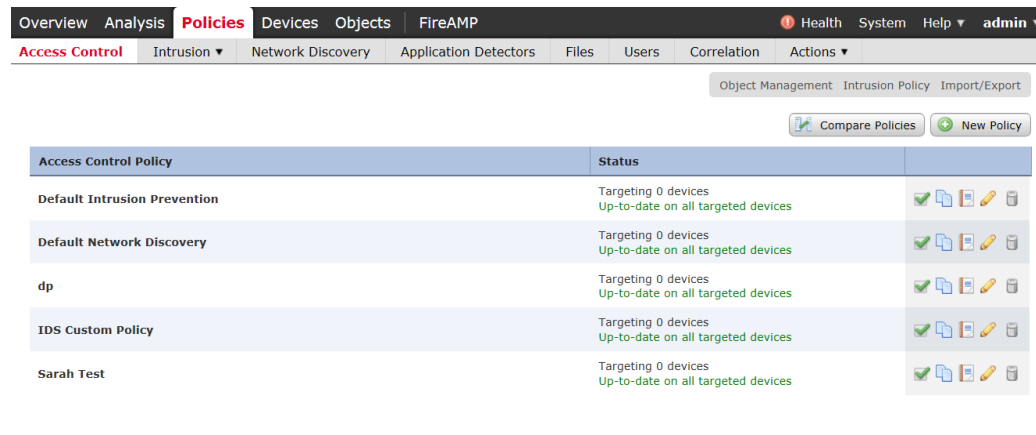
5.2.1.1 Essential ACP Elements for the CC-Evaluated Configuration

To satisfy the traffic flow control claims for the CC-evaluated configuration, every deployed ACP must at minimum include rules that define the “Network” (source and destination IP addresses), and *should* include “Ports” (source and/or destination port numbers), as well as identification of “Zones” (which are logical representations of networks, mapped to physical interfaces of each FTD to which the ACP can be applied). Any use of other ACP features (including VPN tags, Users, URL, etc.) is not relevant to supporting the CC-evaluated traffic flow control functionality, nor do any of those features interfere with Network-based or Port-based traffic flow control functionality.

5.2.1.2 Creating an Access Control Policy

When you create a new access control policy you must, at minimum, give it a unique name and specify a default action. Although you are not required to identify the policy targets at policy creation time, you must perform this step before you can apply the policy.

1. Login with Administrator Role or Access Admin.
2. Select Policies > Access Control.



3. Click New Policy.

4. In the **Name:** field, type a unique name for the new policy. Optionally, type a description in the **Description:** field.

5. Specify the default action.

WARNING! Leave the default **Block all traffic** in the evaluated configuration.

6. Select the Devices where you want to apply the policy. Click on the managed Device(s) you want the policy to applied to. Then click on **Add to Policy** button.

7. Specify the initial **Default Action:**

- Block all traffic creates a policy with the Access Control: Block All Traffic default action.
- **Intrusion Prevention** creates a policy with the **Intrusion Prevention: Balanced Security and Connectivity** default action, associated with the default intrusion variable set.


8. Click **Save**.

9. Click **Deploy** and select the Device(s) you want to deploy the setting to and click **Deploy** again.

5.2.1.3 Editing an Access Control Policy

1. Login with Administrator Role.

2. Select Policies > Access Control.


3. Click the edit icon () next to the access control policy you want to configure.

The Policy Edit page appears.

The screenshot shows the Cisco FTD web interface. At the top, there are navigation tabs: Overview, Analysis, Policies (selected), Devices, Objects, and FireAMP. Below these are sub-tabs for Access Control, Intrusion, Network Discovery, Application Detectors, Files, Users, Correlation, and Actions. The main content area is titled 'Sarah Test' and includes buttons for Save, Cancel, and Save and Apply. Below the title, there are tabs for Rules, Targets (0), Security Intelligence, HTTP Responses, and Advanced. A search bar and 'Add Rule' button are visible. A table of rules is displayed, with one rule named 'empty port rule' having a 'Trust' action. The table has columns for #, Name, Source Zones, Dest Zones, Source Netw..., Dest Netw..., VLAN..., Users, Appli..., Ports, URLs, and Action. Below the table, there are sections for Administrator Rules, Standard Rules, and Root Rules, all of which are currently empty. At the bottom, there is a 'Default Action' dropdown set to 'Access Control: Block All Traffic' and a pagination bar showing 'Displaying 1 - 1 of 1 rules'.

4. Make changes to the policy and click **Save**.
5. Click **Deploy** and select the Device(s) you want to deploy the setting to and click **Deploy** again.

5.2.1.4 Deleting an Access Control Policy

1. Login with Administrator Role.
2. Select Policies > Access Control.
3. Click the delete icon () next to the policy you want to delete.
4. Click **OK** to confirm.



5.2.2 Access Control Rules

A set of access control rules is a key component of an access control policy. Access control rules allow administrator to manage, in a granular fashion, which traffic can enter the network, exit it, or cross from within without leaving it. Within an access control policy, the system matches traffic to rules in top-down order by rule number. In addition to its rule order and some other basic attributes, each rule has the following major components:

- A set of rule *conditions* that identifies the specific traffic you want to control.
- A rule *action*, which determines how the system handles traffic that meets the rule's conditions.
- Intrusion *inspection* option, which allow you to examine allowed traffic with intrusion policy.
- The *logging* option, which allow you to keep a record (event log) of the matching traffic.

The access control policy's default action defines the default action (for example, block all traffic) for the policy.

5.2.2.1 Creating and Editing Access Control Rules

1. Login with Administrator Role or Access Admin.
2. Select Policies > Access Control.
3. Click the edit icon () next to the access control policy you want to configure.
4. Add a new rule or edit an existing rule:
 - To add a new rule, click **Add Rule**.
 - To edit an existing rule, click the edit icon () next to the rule you want to edit.

Either the Add Rule or Editing Rule page appears.

The screenshot displays the 'Add Rule' configuration interface. At the top, there is a 'Name' field, an 'Enabled' checkbox, and an 'Insert into Category' dropdown menu set to 'Standard Rules'. Below this, the 'Action' is set to 'Allow', and there are status indicators for 'IPS: no policies', 'Files: no inspection', and 'Logging: no logging'. The main area is divided into tabs: 'Zones', 'Networks', 'VLAN Tags', 'Users', 'Applications', 'Ports', and 'URLs'. The 'Zones' tab is selected, showing a list of 'Available Zones' (External, External-1, Internal, Internal-1) on the left. In the center, there are 'Add to Source' and 'Add to Destination' buttons. On the right, there are two empty boxes for 'Source Zones (0)' and 'Destination Zones (0)', both currently containing the text 'any'.

5. Configure the following rule components:
 - You must provide a unique rule **Name**.
 - Specify whether the rule is **Enabled**.
 - Specify the rule position.
 - Select a rule **Action**³.
 - Configure the rule's conditions⁴.
 - Configure the rule's **Inspection** option.
 - Specify **Logging** option.
 - Add **Comments**.

6. Click **Add** or **Save**.

Your changes are saved. You must deploy the updated ACP to an FTD for the changes to take effect.

³ The CC-evaluated actions are Allow and Block.

⁴ The CC-evaluated conditions are Zones, Networks, and Ports. The other conditions are presented for completeness only.



5.2.2.2 Understanding Rule Conditions

Administrators can set an ACP rule to match traffic meeting any of the conditions described in the following table:


Condition	Description
Zones	A configuration of one or more interfaces where you can apply policies. Zones provide a mechanism for classifying traffic on source and destination interfaces, and you can add source and destination zone conditions to rules.
Networks	Any combination of individual IPv4 and IPv6 addresses, CIDR blocks, and/or networks (by default, any). The system also supports Network Objects as described in Section 4, page 148 in the Cisco 3D System User Guide.
VLAN Tags	A number from 0 to 4094 that identifies traffic on your network by VLAN.
Applications	Applications provided by Cisco, user-defined applications, and application filters you create using the object manager.
Ports	Source and Destination ports. ICMPv4 and ICMPv6 type and code. Transport protocol ports, including individual and group port objects you create based on transport protocols ⁵ . The system supports Port Objects as described in Section 4, page 170 in the Cisco 3D System User Guide.
URLs	Cisco-provided URLs grouped by category and reputation, literal URLs, and any individual and group URL objects you create using the object manager.

To support the dynamic session establishment capability for FTP, you first need to create an access control rule that allows traffic to destination port “FTP”. You can also configure the logging for this rule. This will enable the FTP application detector to allow the FTP data connection without an additional explicit rule.

5.2.2.3 Deleting Access Control Rules

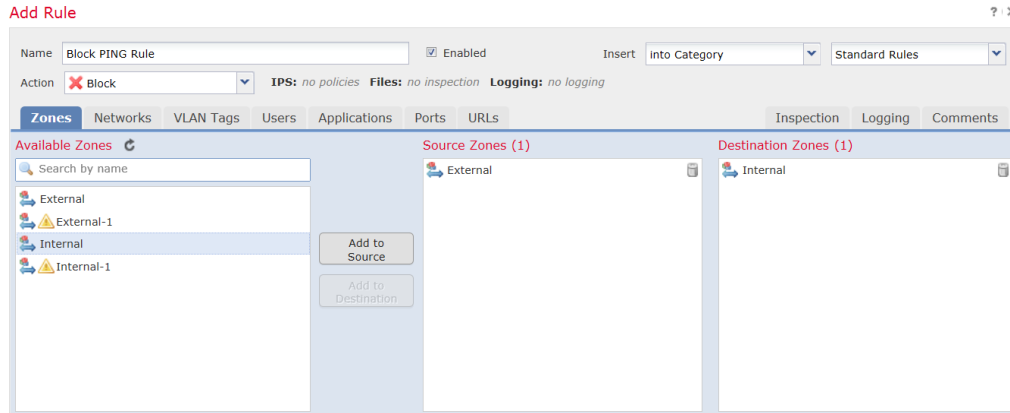
1. Login with Administrator Role.
2. Select Policies > Access Control.
3. Click the edit icon () next to the access control policy you want to configure.
4. Click the delete icon () next to the access control rule you want to delete.
5. Click **OK** to confirm.
6. Click **Save**.

The following example demonstrates how to block all Ping (ICMP echo request) from the external network to internal network and log the connection attempt.

1. Login with Administrator Role.
2. Select Policies > Access Control.
3. Click the edit icon () next to the access control policy you want to configure.
4. Click **Add Rule**.
5. Type a name for the rule.

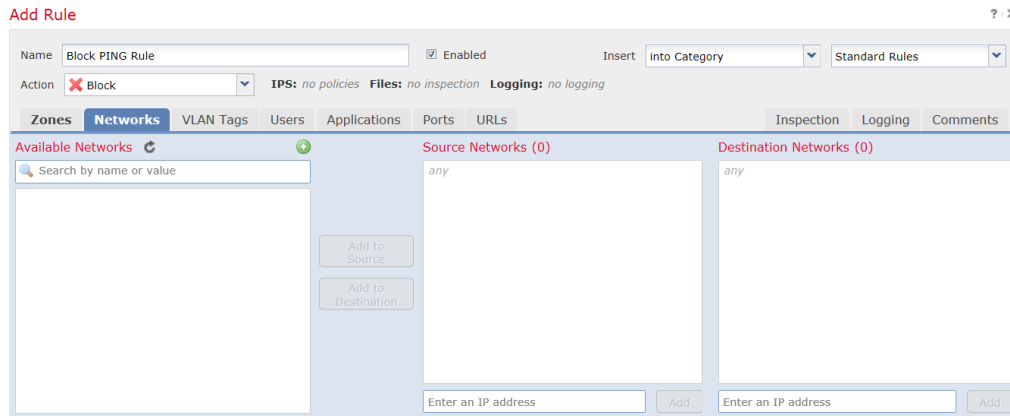
⁵ We support all the protocol-specific attributes required in the FWPP.

6. Leave the **Enabled** checkbox selected.
7. Let the rule get inserted into standard rules.
8. Select **Block** from drop-down list for the rule action.
9. On the **Zones** tab, select the **External** zone as the source zone and the **Internal** zone as the destination zone. You can click and drag or use the buttons.

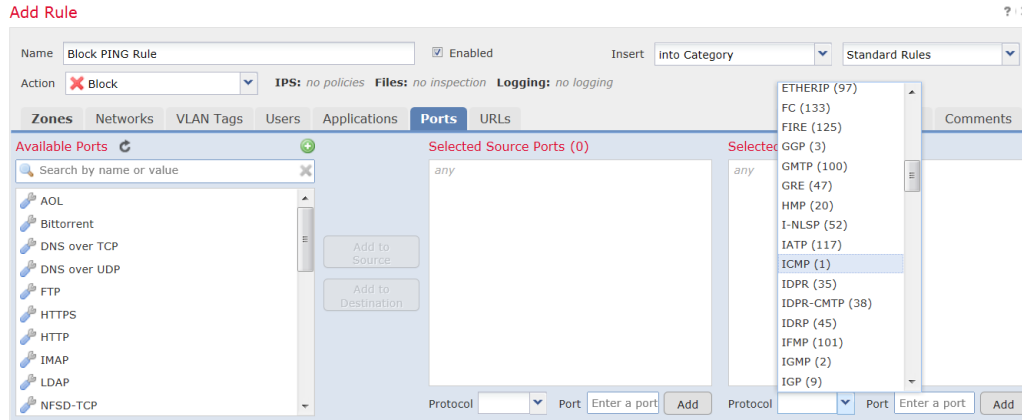


10. On the **Networks** tab, select **any** as the source network and **any** as the destination network.

For granular control, you can enter IP address or range of IP addresses for source and destination networks. The system also supports IPv6 addresses as well.

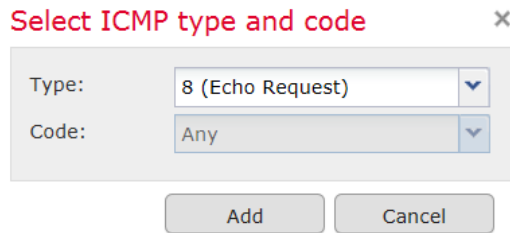


11. On the **Ports** tab, in the second **Protocol** fields, select **ICMP(1)**.

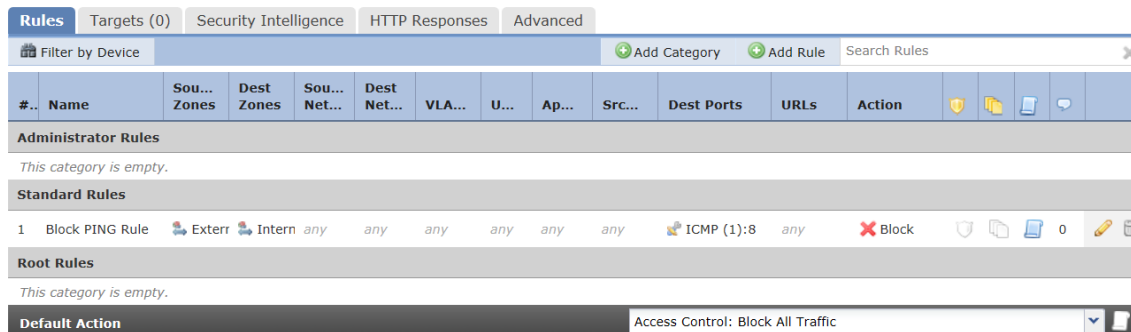


The Select ICMP type and code pop-up window appears.

12. In the **Type:** field, select **8 (Echo Request)**.



13. Click **Add**.
14. On the Logging tab, check Log at Beginning of Connection.
15. In the Send Connection Events to: field, check the FMC.
16. Click **Add**.



17. Click **Save**.

5.2.2.4 Modification of Which Mode Is Active on an FTD Interface

1. Login with Administrator Role.
2. Select Device > Device Management.
3. Edit an interface (e.g., eth1).

4. To change an interface mode, change the interface from **Inline** to **Passive**.
5. Click **Save**.

5.2.2.5 Dynamic Session Establishment

The TOE supports TCP and UDP protocols that require dynamic establishment of secondary network sessions like FTP and the establishment of the sessions along with the dynamical definition of the rule are treated as auditable events. The TOE will manage establishment and teardown of the following protocols in accordance with the RFC for each protocol:

- FTP (File Transfer Protocol) is a TCP protocol supported in either active or passive mode:
 - In active mode the client initiates the control session, and the server initiates the data session to a client port provided by the client;
 - For active FTP to be allowed through the TOE, the firewall rules must explicitly permit the control session from the client to the server, and “inspect ftp” must be enabled. The TOE will then explicitly permit a control session to be initiated from the client to the server, and implicitly permit data sessions to be initiated from the server to the client while the control session is active.
 - In passive (PASV) mode, the client initiates the control session, and the client also initiates the data session to a secondary port provided to the client by the server.

For passive FTP to be permitted through the TOE, the firewall rules must explicitly permit the control session from the client to the server, and “inspect ftp” must be enabled with the “match passive-ftp” option enabled. That feature will cause the TOE to look for the PASV or EPSV commands in the FTP control traffic and for the server’s destination port, and dynamically permit the data session.

6 Management Functions

6.1 Manage the FMC Audit Log and Syslog

FMCs and managed Devices log read-only auditing information for user activity. Audit logs are presented in a standard event view that allows administrator to view, sort, and filter audit log messages based on any item in the audit view. Administrator can delete and report on audit information and can view detailed reports of the changes that users make. These messages can be configured to be transmitted directly to a remote syslog server, in which case each message will be simultaneously transmitted to the remote logging server as the message is written locally.

The appliance includes an internal log database implementation that can be used to store and review audit records locally. When the audit log is full, the oldest audit records are overwritten by the newest audit records. In addition, the appliance also includes a local syslog storage in `/var/log/messages`. Similar to the audit log, when the syslog is full, the oldest syslog messages are overwritten by the newest one.

For the Audit Log, the events are stored in partitioned event tables. FMC will prune (i.e., delete) the oldest partition table whenever the oldest partition can be pruned without reducing the number of stored events below the configured event retention level. The default retention level for the Audit Event Database is 100,000 and is configurable from 1-100,000 (configurable via System > Configuration > Database > Audit Event Database > Maximum Audit Events). Setting the retention level (the “Maximum Audit Events” value) sets the amount of records that will be retained after a periodic pruning. Records are stored across multiple partition tables that each have a minimum size of 10,000 records, and the periodic pruning can only remove entire partition tables, not subsets of tables. So, for example, if the retention level is set to 5000, the actual number of currently stored audit events would need to exceed 15,000 records (10,000 in the older partition table, and 5,000+ in the newer partition table) before the older table can be deleted while retaining 5,000+ of the most recent records.

NOTE! To change the maximum number of entries, go to System > Configuration > Database > Audit Event Database > Maximum Audit Events

For syslog, the logs are stored in `/var/log/messages` and FMC uses a ‘logrotate’ implementation to rotate logs weekly or when the log file size exceeds 25 MB. After the maximum number of backlog files is reached, the oldest is deleted and the numbers on the other backlogs file are incremented.

NOTE! To prevent losing audit records, set up an audit server to send a copy of the audit and syslog records to.

To prevent the losing of critical audit records, the administrators can configure the system to transmit all the audit events (i.e., audit log and syslog) in real-time over a secure TLS connection or an IPsec connection (FTD-only) to an external audit server in the operational environment. When an audit event is generated, it is sent to the local storage and external audit server simultaneously. This ensures that current audit events can be viewed locally while all events, new or old, are stored off-line as required by the NDcPP.

Note that the protection of the audit records stored at the external audit server is the responsibility of the operational environment. The TOE is only responsible for the secure communication channel. It is recommended that the audit server is physically or logically separated (e.g., VLANs) from the other networks.

The TOE can be configured to export syslog records to an administrator-specified, external syslog server. The TOE can be configured to encrypt the communications with an external syslog server using IPsec or TLS. FMC transmits syslog over TLS and FTD transmits syslog over TLS and IPsec.

The audit records are also stored locally and when the local storage is full, the newest data will overwrite the oldest data. On FMC, log messages (those generated locally and those forwarded from FTD) are stored locally on FMC in a database. Different message types are stored separately in local databases, and each local store has a separately configurable size limit (configurable in FMC via System > Configuration > Database). Audit events recording FMC administrator actions are stored in the Audit Event Database, network traffic events transmitted from FTD to FMC are stored in separate databases on FMC: firewall events (triggered by Access Control Policy rules) are stored in Connection Database; VPN events are stored in the VPN Troubleshooting Database; and the IPS events are stored in Intrusion Event Database.

Messages generated by FTD, including FTD system messages, firewall events, and VPN events are stored locally on FTD and are immediately transmitted from FTD to an external syslog server. As mentioned in the preceding paragraph, the firewall, VPN and IPS events are directly sent to FMC for retention in the FMC databases via secure TLS channel (Note: The IPS events are not stored locally on FTD but are transmitted to an external syslog server via the FMC. IPS events generated on FTD are temporarily stored locally on FTD in a database prior to transmission to FMC). If the connection between FTD and FMC is interrupted, the IPS messages are transmitted once connectivity is restored. As the system, firewall event and VPN event messages are generated by FTD, they are immediately transmitted from FTD to a remote syslog server and stored in a local buffer (buffer size configurable from 4096-52428800 bytes) which overwrites old messages with new ones when storage limits are reached. The local logs are viewable from the FTD CLI shell by using “show logging”.

6.1.1 View Audit Log and Syslog via GUI

The “Audit Log” on the FMC contains the log messages related to administrative actions performed on the FMC.

1. Login with Administrator Role.
2. Select System > Monitoring > Audit.

Time	User	Subsystem	Message	Source IP
2016-08-09 17:05:12	admin	System > Users > Users	Page View	10.82.178.11
2016-08-09 17:01:20	admin	Devices > Device Management > Devices	Page View	10.82.178.11
2016-08-09 17:01:08	admin	Devices > Device Management	Page View	10.82.178.11
2016-08-09 16:59:35	admin	Policies > Access Control > Access Control	Page View	10.82.178.11
2016-08-09 16:56:21	admin	Devices > Platform Settings > Platform Edit	Page View	10.82.178.11
2016-08-09 16:56:16	admin	Devices > Platform Settings	Page View	10.82.178.11
2016-08-09 16:56:14	admin	Devices > Device Management	Page View	10.82.178.11
2016-08-09 16:51:18	admin	Policies > Access Control > Access Control > Firewall Policy Editor	Save Policy Default	10.82.178.11
2016-08-09 16:50:52	admin	Policies > Access Control > Access Control > Firewall Policy Editor	Page View	10.82.178.11
2016-08-09 16:50:17	admin	Policies > Access Control > Access Control	Page View	10.82.178.11

3. The System log (syslog) page provides administrator with system log information for the appliance. The system log displays each message generated by the system. The following items are listed in order:
 - Date that the message was generated.
 - Time that the message was generated.
 - Host that generated the message.
 - The message itself⁶.
4. Select System > Monitoring > Syslog.

The screenshot shows the Cisco FTD web interface with the following elements:

- Navigation Bar:** Overview, Analysis, Policies, Devices, Objects, AMP, Deploy, System, Help, admin.
- Sub-Menu:** Configuration, Users, Domains, Integration, Updates, Licenses, Health, Monitoring > Syslog, Tools.
- Filters:** Case-sensitive, Exclusion, and a search box with a 'Go' button.
- Messages List:**
 - Aug 09 2016 17:08:58 qutrinhfMCv sudo: pam_unix(sudo:session): session closed for user root
 - Aug 09 2016 17:08:58 qutrinhfMCv sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
 - Aug 09 2016 17:08:58 qutrinhfMCv sudo: www : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/bin/chown www:www /var/log/CSMAgent.log
 - Aug 09 2016 17:08:46 qutrinhfMCv sudo: pam_unix(sudo:session): session closed for user root
 - Aug 09 2016 17:08:46 qutrinhfMCv sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
 - Aug 09 2016 17:08:46 qutrinhfMCv sudo: www : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/bin/chown www:www /var/log/CSMAgent.log
 - Aug 09 2016 17:08:43 qutrinhfMCv sudo: pam_unix(sudo:session): session closed for user root
 - Aug 09 2016 17:08:43 qutrinhfMCv sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
 - Aug 09 2016 17:08:43 qutrinhfMCv sudo: www : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/bin/chown www:www /var/log/CSMAgent.log
 - Aug 09 2016 17:08:41 qutrinhfMCv mojo_server.pl: [test] qutrinhfMCv.cisco.com: admin@10.82.178.11, System > Monitoring > Syslog, Go
 - Aug 09 2016 17:08:40 qutrinhfMCv sudo: pam_unix(sudo:session): session closed for user root
 - Aug 09 2016 17:08:40 qutrinhfMCv sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
 - Aug 09 2016 17:08:40 qutrinhfMCv sudo: www : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/bin/chown www:www /var/log/CSMAgent.log
 - Aug 09 2016 17:08:40 qutrinhfMCv syslog-ng[11131]: Syslog connection broken; fd='20', server='AF_INET(172.18.152.193:6514)', time_reopen='60'
 - Aug 09 2016 17:08:40 qutrinhfMCv syslog-ng[11131]: I/O error occurred while writing; fd='20', error='Broken pipe (32)'
 - Aug 09 2016 17:08:40 qutrinhfMCv syslog-ng[11131]: SSL error while writing stream; tls_error='SSL routines:ssl3_get_server_certificate:certificate verify failed'

Audit Record:

2013-02-26 18:28:08	admin	System > Monitoring > Audit	Page View	10.4.10.227
2013-02-26 18:31:28	admin	System > Monitoring > Syslog	Page View	10.4.10.227

6.1.2 View Audit Log and Syslog via CLI

The command `show audit-log` and `show syslog [filter] [number of lines]` displays the audit log in reverse chronological order; the most recent audit log events are listed first.

Access

Basic

Syntax

show audit-log

⁶ The message includes the user or source IP only if applicable. In most cases, the system generated the system log not the user and most of the time, the source IP address is the IP address of the appliance (i.e., system process resides on the system).

Example

➤ show audit-log

Audit Record:


```
Audit Log Output:
time           : 1361905822 (Tue Feb 26 19:10:22 2013)
event_type     : Default Action
subsystem      : Command Line
actor          : admin
message        : Executed root-view- show audit-log
result         : Success
action_source_ip : 10.4.10.227
action_destination_ip : Default Target IP
-----
time           : 1361901223 (Tue Feb 26 17:53:43 2013)
event_type     : Session terminated due to inactivity (admin)
subsystem      : Session Expiration
actor          : admin
message        : Session terminated due to inactivity (admin)
result         : Success
action_source_ip : 10.4.33.204
action_destination_ip : 10.5.60.81
-----
time           : 1361900652 (Tue Feb 26 17:44:12 2013)
event_type     : Default Action
subsystem      : Command Line
actor          : admin
>
```

6.2 Auditable Events




The appliances that are part of the Cisco FTD 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 command 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.

Table 4: WebUI Audit Log Fields

Time	Time and date that the appliance generated the audit record.
User	User name of the user that triggered the audit event.
Subsystem	<p>Menu path the user followed to generate the audit record. For example, System > Monitoring > Audit is the menu path to view the audit log.</p> <p>In a few cases where a menu path is not relevant, the Subsystem field displays only the event type. For example, Login classifies user login attempts or Command Line classifies a command executed.</p>
Message	<p>Action the user performed.</p> <p>For example, Page View signifies that the user simply viewed the page indicated in the Subsystem, while Save means that the user clicked the Save button on the page. If the Subsystem field is Command Line, the Message field will show the command executed.</p> <p>Changes made to the Cisco 3D System appear with a compare icon () that you can click to see a summary of the changes.</p>
Source IP	IP address of the host used by the user.

Examples of audit log events for web interface and CLI:

	Time ✕	User ✕	Subsystem ✕	Message ✕	Source IP ✕
	 2013-02-27 12:03:29	admin	Overview > Dashboards > Summary Dashboard	Page View	10.2.100.243
	 2013-02-27 12:03:24	admin	Audit Log Events	Delete	10.2.100.243
	 2013-02-27 12:03:24	admin	System > Monitoring > Audit	Page View	10.2.100.243
	 2013-02-27 12:02:15	admin	System > Monitoring > Audit	Page View	10.2.100.243
	 2013-02-27 12:01:30	admin	Login	Login Success	10.2.100.243
	 2013-02-27 12:01:16	admin	System > Local > Configuration > Time	Page View	10.2.100.243
	 2013-02-27 12:01:10	admin	Logout	Logout Success	10.2.100.243
	 2013-02-27 12:01:01	admin	Operations > System Settings	Save	10.2.100.243
	 2013-02-27 12:00:53	admin	System > Local > User Management > Users	Page View	10.2.100.243
	 2013-02-27 12:00:52	admin	System > Local > User Management > Users	 Edited user - tester:221	10.2.100.243
	 2013-02-27 12:00:39	admin	System > Local > User Management > Users > Edit User	Page View	10.2.100.243

The table below shows sample audit events required for Common Criteria evaluation. For other messages refer to [FTD-SYSLOG].

Table 5: Sample syslog Messages

SFR	Auditable Event	Generated by	Actual Audited Event
Reproduced from CPP_ND_v2.2E			
FAU_GEN.1	Startup and shutdown events	FMC, and FTD	<p>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'</p> <p>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'</p>
FCO_CPC_EXT.1	<p>Enabling communications between a pair of components.</p> <p>Disabling communications between a pair of components</p>	FMC and FTD	<p>FTD: Enabling: <date> <time> <host>: SF-IMS[15479]: [16265] sftunnel: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</p> <p>FMC: Enable: <date> <time> <host>: mojo_server.pl: <host>: <user>@172.16.16.47, Devices > Device Management, Add Device - 172.16.16.221 Disable: <date> <time> <host>: mojo_server.pl: <host>: <user>@172.16.16.47, Devices > Device Management, Delete Device - fp4140ftd</p>
FCS_HTTPS_EXT.1	Failure to establish an HTTPS session.	FMC	<p>See FCS_TLSS_EXT.1.</p> <p>FTD: Not applicable.</p> <p>FMC: <date> <time> <host> syslog-ng[23928]: SSL error while writing stream; tls_error='SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure'</p>
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA.	FTD	<p>FTD: <u>Valid Connection:</u></p>

SFR	Auditable Event	Generated by	Actual Audited Event
	<p>Session Establishment with peer</p> <p>Reason for failure. \ Entire packet contents of packets transmitted/received during session establishment.</p>		<pre> <date> <time> <host> %FTD-6-602303: IPSEC: An outbound LAN-to-LAN SA (SPI= 0xC28EE9BA) between 192.168.144.94 and 192.168.144.50 (user= 192.168.144.50) has been created. No Proposal Chosen / IKE weaker than ESP: <date> <time> <host> %FTD-4-750003 Local:192.168.144.94:500 Remote:192.168.144.91:500 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:192.168.144.94:4500 Remote:192.168.144.91:4500 Username:192.168.144.91 IKEv2 Certificate authentication failed. Error: Certificate authentication failed <date> <time> <host> %FTD-4-750003: Local:192.168.144.94:4500 Remote:192.168.144.91:4500 Username:192.168.144.91 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: 00A4, subject name: e=server-dn-org-w-null- ecdsa@gossamersec.com,cn=tl19-16x.example.com,o=GSS, issuer_name: e=subsubca- ecdsa@gossamersec.com,cn=subsubca-ecdsa,o=GSS,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. </pre>

SFR	Auditable Event	Generated by	Actual Audited Event
FCS_SSHS_EXT.1	Failure to establish an SSH session	FTD, and FMC	<p>FTD: <u>Valid Connection:</u> <date> <time> <host> sshd[41573]: pam_unix(sshd:session): session opened for user admin by (uid=0) <u>Bad Cipher:</u> <date> <time> <host> sshd[55627]: Unable to negotiate with 10.6.16.46 port 43416: no matching cipher found. Their offer: aes256-ctr [preauth] <u>Bad Auth Alg:</u> <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] <u>Bad MAC Alg:</u> <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] <u>Bad Kex Alg:</u> <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: <u>Bad Cipher:</u> <date> <time> <host> sshd[30273]: Unable to negotiate with 10.6.16.46 port 46850: no matching cipher found. Their offer: aes256-ctr [preauth] <u>Bad Auth Alg:</u> <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] <u>Bad MAC Alg:</u> <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] <u>Bad Kex Alg:</u> <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]</p>
FCS_TLSC_EXT.1	Failure to establish a TLS Session Reason for failure	FTD and FMC	<p>FTD: General Failure: <date> <time> <host> %FTD-6-725006: Device failed SSL handshake with server diagnostic:172.16.16.194/32068 to 172.16.16.91/6514 <date> <time> <host> syslog-ng[2934]: SSL error while writing stream; tls_error='SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake 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:</p>

SFR	Auditable Event	Generated by	Actual Audited Event
			<p><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:</p> <p><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) <u>Invalid Purpose:</u></p> <p><date> <time> <host> %FTD-7-725014: SSL lib error. Function: tls_process_server_certificate Reason: certificate verify failed</p> <p><date> <time> <host>syslog-ng[2527]: Certificate validation failed; subject='<subject>', issuer='<issuer>', error='unsupported certificate purpose', depth=0' <u>Unknown Cipher:</u></p> <p><date> <time> <host> %FTD-7-725014: SSL lib error. Function: set_client_ciphersuite Reason: unknown cipher returned</p> <p><date> <time> <host> syslog-ng[1821]: SSL error while writing stream; tls_error='SSL routines:set_client_ciphersuite:unknown cipher returned', location='/ngfw/etc/syslog-ng.d/syslog-tls.conf:17:9' <u>Invalid TLS version:</u></p> <p><date> <time> <host> %FTD-7-725014: SSL lib error. Function: ssl_choose_client_version Reason: unsupported protocol</p> <p><date> <time> <host> syslog-ng[2527]: SSL error while writing stream; tls_error='SSL routines:ssl_choose_client_version:unsupported protocol', location='/ngfw/etc/syslog-ng.d/syslog-tls.conf:17:9' <u>Wrong Curve:</u></p> <p><date> <time> <host> %FTD-7-725014: SSL lib error. Function: tls_process_ske_ecdhe Reason: wrong curve</p> <p><u>Certificate Verification Failure:</u></p> <p><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</p> <p><u>Identifier Match Failed:</u></p> <p><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</p> <p><date> <time> <host> %FTD-7-725014: SSL lib error. Function: ssl3_get_server_certificate Reason: certificate verify failed</p> <p><u>Bad signature:</u></p>

SFR	Auditable Event	Generated by	Actual Audited Event
			<p><date> <time> <host> syslog-ng[2527]: SSL error while writing stream; tls_error='rsa routines:int_rsa_verify:bad signature', location='/ngfw/etc/syslog-ng.d/syslog-tls.conf:17:9'</p> <p><date> <time> <host> %FTD-7-725014: SSL lib error. Function: tls_process_key_exchange Reason: bad signature\n</p> <p><u>Bad Finished Message:</u></p> <p><date> <time> <host> %FTD-7-725014: SSL lib error. Function: tls_process_finished Reason: digest check failed\n</p> <p><u>Digest Check Failed:</u></p> <p><date> <time> <host> syslog-ng[6173]: SSL error while writing stream; tls_error='SSL routines:ssl3_get_finished:digest check failed'</p> <p><u>Decryption Failed:</u></p> <p><date> <time> <host> syslog-ng[7009]: SSL error while writing stream; tls_error='SSL routines:SSL3_GET_RECORD:decryption failed or bad record mac'</p> <p>FMC:</p> <p><u>General Failure:</u></p> <p><date> <time> <host> SF-IMS[19567]: [24222] sftunneld:sf_ssl [ERROR] Connect:SSL handshake failed</p> <p><u>Invalid EKU:</u></p> <p><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.</p> <p><u>Invalid Identifier:</u></p> <p><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)</p> <p>With Mutual authentication supported:</p> <p><u>Bad Cipher and General Failure:</u></p> <p><date> <time> <host> syslog-ng[6506]: SSL error while writing stream; tls_error='SSL routines:ssl3_read_bytes:ssl3 alert handshake failure', location='/etc/syslog-ng.d/syslog-tls.conf:17:9'</p> <p><u>Invalid Purpose:</u></p> <p><date> <time> <host> syslog-ng[6506]: X509 Certificate Validation; depth='0', ok='0', errnum='26', error='unsupported certificate purpose'</p> <p><u>Unknown/Wrong Cipher:</u></p> <p><date> <time> <host> syslog-ng[6506]: SSL error while writing stream; tls_error='SSL routines:set_client_ciphersuite:unknown cipher returned', location='/etc/syslog-ng.d/syslog-tls.conf:17:9'</p> <p><u>Invalid TLS version:</u></p>

SFR	Auditable Event	Generated by	Actual Audited Event
			<p><date> <time> <host> syslog-ng[23039]: SSL error while writing stream; tls_error='SSL routines:ssl_choose_client_version:unsupported protocol', location='/etc/syslog-ng.d/syslog-tls.conf:17:9'</p> <p><u>Wrong Curve:</u></p> <p><date> <time> <host> syslog-ng[6506]: SSL error while writing stream; tls_error='SSL routines:tls_process_ske_ecdhe:wrong curve', location='/etc/syslog-ng.d/syslog-tls.conf:17:9'</p> <p>Certificate Verification Failure:</p> <p><date> <time> <host> syslog-ng[17342]: SSL error while writing stream; tls_error='SSL routines:ssl3_get_server_certificate:certificate verify failed'</p>
FCS_TLSS_EXT.1	Failure to establish an TLS Session	FMC, and FTD	<p>FTD: See FCS_TLSC_EXT.1</p> <p>FMC: <u>No Shared Cipher/Invalid Key Exchange:</u> <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?</p> <p><u>Digest Check Failed:</u> <date> <time> <host> [ssl:info] [pid 15536:tid 22427868288768] SSL Library Error: error:1416C095:SSL routines:tls_process_finished:digest check failed</p> <p><u>Wrong Version:</u> <date> <time> <host> [ssl:info] [pid 15536:tid 22427857782528] SSL Library Error: error:142090FC:SSL routines:tls_early_post_process_client_hello:unknown protocol</p> <p><u>General Failure:</u> <date> <time> <host> [ssl:info] [pid 17833:tid 22427853580032] [client 172.16.16.91:50570] AH02008: SSL library error 1 in handshake (server 172.16.16.116:443)</p> <p>ITT: <date> <time> <host> SF-IMS[19567]: [11420] sftunneld:sf_ssl [ERROR] Accept:SSL handshake failed</p>
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	FMC, and FTD	<p>FTD: <u>SSH:</u> <date> <time> <host> sshd[24776]: error: maximum authentication attempts exceeded for testuser from 10.6.16.46 port 45216 ssh2 [preauth]</p> <p>FMC: <u>TLS:</u> <date> <time> fmc1600 mojo_server.pl: fmc1600: testuser@127.0.0.1, Login, Login Failed <date> <time> mc1600 mojo_server.pl: fmc1600: Invalid User@127.0.0.1, Login, Login Failed</p>

SFR	Auditable Event	Generated by	Actual Audited Event
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	FMC, and FTD	<p>FTD:</p> <p><u>Console Success:</u> <date> <time> <host> login[21794]: pam_unix(login:session): session opened for user admin by LOGIN(uid=0)</p> <p><u>Console Failure:</u> <date> <time> <host> login[23764]: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=/dev/ttyS0 ruser= rhost= user=admin <date> <time> <host> login[23764]: FAILED LOGIN (1) on '/dev/ttyS0' FOR 'admin', Authentication failure</p> <p><u>SSH Login Success:</u> <date> <time> <host> %FTD-5-199017: sshd[2776]: Accepted keyboard-interactive/pam for admin from 172.16.16.91 port 53660 ssh2#012 <date> <time> <host> sshd[16163]: pam_unix(sshd:session): session opened for user admin by (uid=0)</p> <p><u>SSH Login Failure:</u> <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> %FTD-5-199017: sshd[2638]: error: PAM: Authentication failure for admin from 172.16.16.91 #012</p> <p><u>SSH Public Key Success:</u> <date> <time> <host>sshd[66781]: Accepted publickey for admin from 10.6.16.46 port 50550 ssh2: RSA SHA256:2cnR+gpbgVVqxRqHpKi0cDRp1wKDqeXjuLYYsjEeis <date> <time> <host> sshd[66781]: pam_unix(sshd:session): session opened for user admin by (uid=0)</p> <p><u>SSH Public Key Failure:</u> <date> <time> <host> sshd[21381]: Connection closed by authenticating user admin 172.16.16.91 port 55736 [preauth]#012</p> <p>FMC:</p> <p><u>Console Login Success:</u> <date> <time> <host> login[7684]: pam_unix(login:session): session opened for user admin by LOGIN(uid=0)</p> <p><u>Console Login Failure:</u> <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</p> <p><u>SSH Login Success:</u></p>

SFR	Auditable Event	Generated by	Actual Audited Event
			<pre> <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+1TsjNL78E1XSdTZVGI6AdFU <date> <time> <host> sshd[23895]: pam_unix(sshd:session): session opened for user admin by (uid=0) SSH Public Key Failure: <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 </pre>
FIA_UAU_EXT.2	All use of the identification and authentication mechanism.	FMC, and FTD	See FIA_UIA_EXT.1
FIA_X509_EXT.1/Rev	<p>Unsuccessful attempt to validate a certificate</p> <p>Any addition, replacement or removal of trust anchors in the TOE's trust store</p> <p>Reason for failure of certificate validation</p>	FMC, and FTD	<p>FTD:</p> <p><u>TLS:</u></p> <p><u>Trust Anchor Addition:</u></p> <pre> <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. </pre> <p><u>Trust Anchor Deletion:</u></p>

SFR	Auditable Event	Generated by	Actual Audited Event
	<p>Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store</p>		<p><date> <time> <host> %FTD-5-111008: User 'enable_1' executed the 'no crypto ca trustpoint rootca-rsa-no-revocation noconfirm' command.</p> <p><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'</p> <p><u>Expired cert:</u></p> <p><date> <time> <host> syslog-ng[2527]: Certificate validation failed; subject='<subject>', issuer='<issuer>', error='certificate has expired', depth='0'</p> <p><date> <time> <host> %FTD-3-717027: Certificate chain failed validation. Certificate chain date is out-of-range.</p> <p><u>Corrupt ASN.1:</u></p> <p><date> <time> <host>: syslog-ng[2527]: SSL error while writing stream; tls_error='asn1 encoding routines:asn1_check_tlen:wrong tag', location='/ngfw/etc/syslog-ng.d/syslog-tls.conf:17:9'</p> <p><date> <time> <host>: %FTD-7-725014: SSL lib error. Function: ssl3_get_server_certificate Reason: ASN1 lib</p> <p><u>Invalid Ca or Signature:</u></p> <p><date> <time> <host> %FTD-3-717027: Certificate chain failed validation. Certificate chain is either invalid or not authorized.</p> <p><u>Revoked cert using CRL:</u></p> <p><date> <time> <host> syslog-ng[2185]: Certificate validation failed; subject='<subject>', issuer='<issuer>', error='certificate revoked', depth='0'</p> <p><date> <time> <host> %FTD-3-717027: Certificate chain failed validation. Certificate is revoked.</p> <p><u>Revoked cert using OCSP:</u></p> <p><date> <time> <host> %FTD-7-711001: #012CRYPTO_PKI: OCSP polling for trustpoint rootca-rsa-ocsp succeeded. Certificate status is REVOKED.</p> <p><u>No CRLSign Purpose:</u></p> <p><date> <time> <host> %FTD-3-717009: Certificate validation failed. serial number: 96, subject name: emailAddress=server-issued-by-no-crl-key-usage-ecdsa@gossamersec.com,CN=tl2116x.example.com,O=GSS,L=Catonsville,ST=MD,C=US.</p> <p><u>No OCSPSign Purpose:</u></p> <p><date> <time> <host> %FTD-3-717032: OCSP status check failed. Reason: Failed to verify OCSP response.</p> <p><u>Invalid Chain:</u></p> <p><date> <time> <host> %FTD-3-717027: Certificate chain failed validation. No suitable trustpoint was found to validate chain.</p> <p><date> <time> <host> syslog-ng[2527]: SSL error while writing stream; tls_error='SSL routines:tls_process_server_certificate:certificate verify failed', location='/ngfw/etc/syslog-ng.d/syslog-tls.conf:17:9'</p> <p><u>Explicit EC Certificate:</u></p>

SFR	Auditable Event	Generated by	Actual Audited Event
			<p><date> <time> <host> %FTD-3-717027: Certificate chain failed validation. Generic validation failure occurred.</p> <p><u>IPsec:</u></p> <p><u>Expired cert:</u></p> <p><date> <time> <host> %FTD-3-717009: Certificate validation failed. Certificate date is out-of-range</p> <p><u>Corrupt ASN.1:</u></p> <p><date> <time> <host> %FTD-4-750003: Local:192.168.144.92:4500 Remote:192.168.144.91:4500 Username:Unknown IKEv2 Negotiation aborted due to ERROR: Auth exchange failed</p> <p><u>Invalid Signature:</u></p> <p><date> <time> <host> %FTD-3-717027: Certificate chain failed validation. Certificate is either invalid or not authorized</p> <p><u>Invalid CA:</u></p> <p><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 .</p> <p><u>CRL Revoked cert:</u></p> <p><date> <time> <host> %FTD-3-717027: Certificate chain failed validation. Certificate is revoked.</p> <p><u>OCSP Revoked cert:</u></p> <p><date> <time> <host> %FTD-3-717032: OCSP status check failed. Reason: Certificate is revoked.</p> <p><u>No OCSP/CRL signing purpose:</u></p> <p><date> <time> <host> %FTD-3-717032: OCSP status check failed. Reason: Failed to verify OCSP response.</p> <p><date> <time> <host> %FTD-7-711001: Certificate verification error: key usage does not include CRL signing</p> <p><u>Invalid Chain:</u></p> <p><date> <time> <host> %FTD-3-717027: Certificate chain failed validation. No suitable trustpoint was found to validate chain.</p> <p><u>Explicit EC Certificate:</u></p> <p><date> <time> <host> %FTD-3-717027: Certificate chain failed validation. Generic validation failure occurred.</p> <p>FMC:</p> <p><u>TLS:</u></p> <p><u>Trust Anchor Addition:</u></p> <p><date> <time> <host> SF-IMS[14865]: HTTPSCert:InstallCertificate [INFO] Cert Added: F5_client-TOE-00-rsa_rootca-rsa</p> <p><u>Trust Anchor Deletion:</u></p>

SFR	Auditable Event	Generated by	Actual Audited Event
			<p><date> <time> <host> SF-IMS[13985]: HTTPSCert:DeleteCertificate [INFO] Cert Deleted: F1_client-TOE-00-rsa_rootca-rsa</p> <p><u>Expired cert:</u> <date> <time> <host> syslog-ng[5115]: X509 Certificate Validation; depth='0', ok='0', errnum='10', error='certificate has expired'</p> <p><u>Corrupt ASN.1:</u> <date> <time> <host> syslog-ng[5403]: SSL error while writing stream; tls_error='asn1 encoding routines:ASN1_CHECK_TLEN:wrong tag'</p> <p><u>Invalid Signature:</u> <date> <time> <host> syslog-ng[5697]: X509 Certificate Validation; depth='0', ok='0', errnum='7', error='certificate signature failure'</p> <p><u>Invalid CA:</u> <date> <time> <host> syslog-ng[10519]: X509 Certificate Validation; depth='1', ok='0', errnum='24', error='invalid CA certificate'</p> <p><u>Revoked cert:</u> <date> <time> <host> syslog-ng[9301]: X509 Certificate Validation; depth='0', ok='0', errnum='23', error='certificate revoked'</p> <p><u>Invalid Chain:</u> <date> <time> <host> syslog-ng[15124]: X509 Certificate Validation; depth='1', ok='0', errnum='19', error='self signed certificate in certificate chain'</p>
FIA_X509_EXT.1/ITT	<p>Unsuccessful attempt to validate a certificate</p> <p>Any addition, replacement or removal of trust anchors in the TOE's trust store</p> <p>Reason for failure of certificate validation</p> <p>Identification of certificates added, replaced or removed</p>	FMC and FTD	<p>FTD:</p> <p><u>Trust Anchor Addition:</u> Refer to FIA_X509_EXT.1/Rev</p> <p><u>Trust Anchor Deletion:</u> Refer to FIA_X509_EXT.1/Rev</p> <p><u>Expired cert:</u> <date> <time> <host> SF-IMS[34769]: [41667] sftunneld:sf_ssl [ERROR] err 10:certificate has expired</p> <p><u>Corrupt ASN.1:</u> <date> <time> <host> SF-IMS[21318]: [21341] sftunneld:sf_ssl [WARN] Could not receive Message: Closed</p> <p><u>Invalid Signature:</u> <date> <time> <host> SF-IMS[34769]: [66389] sftunneld:sf_ssl [ERROR] err 7:certificate signature failure</p> <p><u>Invalid CA:</u> <date> <time> <host> SF-IMS[41546]: [42675] sftunneld:sf_ssl [ERROR] err 24:invalid CA certificate</p> <p><u>Invalid Chain:</u> <date> <time> <host> SF-IMS[39443]: [22483] sftunneld:sf_ssl [ERROR] err 20:unable to get local issuer certificate</p>

SFR	Auditable Event	Generated by	Actual Audited Event
	as trust anchor in the TOE's trust store		<p>FMC:</p> <p><u>Trust Anchor Addition:</u> <date> <time> <host> SF-IMS[14865]: HTTPSCert:InstallCertificate [INFO] Cert Added: F5_client-TOE-00-rsa_rootca-rsa</p> <p><u>Trust Anchor Deletion:</u> <date> <time> <host> SF-IMS[13985]: HTTPSCert:DeleteCertificate [INFO] Cert Deleted: F1_client-TOE-00-rsa_rootca-rsa</p> <p><u>Expired cert:</u> <date> <time> <host> SF-IMS[28844]: [25530] sftunneld:sf_ssl [ERROR] err 10:certificate has expired</p> <p><u>Corrupt ASN.1:</u> <date> <time> <host> SF-IMS[28844]: [25959] sftunneld:sf_ssl [ERROR] SSL_renegotiate error: 1: error:00000001:lib(0):func(0):reason(1)</p> <p><u>Invalid Signature:</u> <date> <time> <host> SF-IMS[28844]: [25984] sftunneld:sf_ssl [ERROR] err 7:certificate signature failure</p> <p><u>Invalid CA:</u> <date> <time> <host> SF-IMS[28844]: [26310] sftunneld:sf_ssl [ERROR] err 24:invalid CA certificate</p> <p><u>Invalid Chain:</u> <date> <time> <host> SF-IMS[1278]: [1285] sftunneld:sf_ssl [ERROR] err 20:unable to get local issuer certificate</p>
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	FTD, FMC	<p>FTD: See FPT_TUD_EXT.1</p> <p>FMC: <date> <time> <host> SF-IMS[27507]: [27507] Cisco_Firepower_Mgmt_Center_Patch-7.0.1-55 17:000_start/100_start_messages.sh [INFO] Upgrade starting</p>
FMT_SMF.1	All management activities of TSF data.	FTD, FMC	<p>FTD:</p> <p><date> <time> <host> sfdccsm: fmcv-new2: <user>@10.6.16.47, Devices > Platform Settings > Platform Settings Editor, Modified: Banner#000x0a#000x00</p> <p><date> <time> <host> sfdccsm: fmcv-new2: <user>@10.6.16.47, Devices > Platform Settings > Platform Settings Editor, Modified: Timeouts#000x0a#000x00</p> <p>Ability to verify updates:</p> <p><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 -l /var/sf/updates/Cisco_FTD_Upgrade-7.0.5-72.sh.REL.tar</p> <p><date> <time> <host> sudo: admin : TTY=pts/0 ; PWD=/home/admin ; USER=root ; COMMAND=/usr/local/sf/bin/cli_usrmgr maxf testuser 5</p>

SFR	Auditable Event	Generated by	Actual Audited Event
		<p>This management event (ability to manage the trusted public keys database) is intended to be performed during initial setup by entering the underlying linux using the expert command. After initial setup the underlying linux is locked down as</p>	<pre> <date> <time> <host> sfdccsm: <host>: <user@172.16.16.90, Devices > Platform Settings > Platform Settings Editor, Page View#000x0a#000x00 <date> <time> <host> sfdccsm: <host>: <user@172.16.16.90, Devices > Platform Settings > Platform Settings Editor, Save Policy Syslog w/o TLS#000x0a#000x00 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 <date> <time> <host> sudo: admin : TTY=pts/0 ; PWD=/home/admin ; USER=root; COMMAND=/usr/local/sf/bin/cli_usrmgr unlock tester <date> <time> <host> %FTD-6-199018: FPRM: <<%FPRM-6-AUDIT>> [admin][clish][modification][clish][68760][sys/user-ext/user-testuser][clearLockStatus(Old:no, New:yes)][] User testuser modified#012 <date> <time> <host> cmd_log.pl: Default NGFWPolicy: admin@172.16.16.91, Command Line, Executed expert- command </pre>

SFR	Auditable Event	Generated by	Actual Audited Event
		database) is intended to be performed during initial setup by entering the underlying linux using the expert command. After initial setup the underlying linux is locked down as described in Section 4.2.11	
FPT_ITT.1, FPT_ITT.1/Join	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	<p>FTD: <u>Initiation:</u> <date> <time> <host> SF-IMS[12866]: [12873] sfmbservice:sfmb_service [INFO] Established connection to peer 10.6.16.223 <u>Termination:</u> <date> <time> <host> SF-IMS[60163]: [47010] sfmbservice:sfmb_service [INFO] Connection closed to host 10.6.16.223 <u>Failure:</u> <date> <time> <host> SF-IMS[34769]: [68858] sftunneld:sf_ssl [ERROR] Connect:SSL handshake failed</p> <p>FMC: <u>Initiation:</u> <date> <time> <host> SF-IMS[19106]: [19420] sfmbservice:sfmb_service [INFO] Established connection to peer 10.6.16.221 <u>Termination:</u> <date> <time> <host> SF-IMS[22235]: [25609] sfmbservice:sfmb_service [INFO] Connection closed to host 10.6.16.221 <u>Failure:</u> <date> <time> <host> SF-IMS[9336]: [2438] sftunneld:sf_ssl [ERROR] Connect:SSL handshake failed</p>
FPT_TUD_EXT.1	Initiation of update; result of the update	FMC, and FTD	<p>FTD: <u>Initiation:</u></p>

SFR	Auditable Event	Generated by	Actual Audited Event
	attempt (success or failure)		<p><date> <time> <host> SF-IMS[6266]: [6266] sftunnel:stream_file [INFO] INITIATED SRC: : File copy 0 % completed, 0 bytes of file copied out of 0</p> <p><u>Success:</u></p> <p><date> <time> <host> SF-IMS[6266]: [6266] sftunnel:stream_file [INFO] ELASTIC_FSTREAM status:: File copy 100 % completed, 99891200 bytes of file copied out of 99891200</p> <p><date> <time> <host> SF-IMS[6266]: [6266] sftunnel:control_services [INFO] FSTREAM_STATUS: Sending back task status 'Completed'</p> <p><u>Failure:</u></p> <p><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</p> <p><date> <time> <host> SF-IMS[18303]: update.cgi:ProcessUpdateUpload [ERROR] update is not a signed package: file = Cisco_Firepower_Threat_Defense_Virtual-7.0.5-72.tar.gz</p> <p>FMC:</p> <p><u>Initiation:</u></p> <p><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</p> <p><u>Success:</u></p> <p><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</p> <p><u>Failure:</u></p> <p><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</p> <p><date> <time> <host> SF-IMS[15473]: update.cgi:ProcessUpdateUpload [ERROR] update is not a signed package: file = Cisco_Firepower_Threat_Defense_Virtual-7.0.5-72.tar.gz</p>
FPT_STM_EXT.1	Discontinuous changes to time - 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	FMC, and FTD	<p>FTD:</p> <p><date> <time> <host> %FTD-5-771002: CLOCK: System clock set, source: FXOS, IP: 0.0.0.0, before: 03:16:11.918 UTC Sun Mar 7 2021, after: 03:25:00.000 UTC Sun Mar 7 2021</p> <p>FMC:</p> <p><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</p>

SFR	Auditable Event	Generated by	Actual Audited Event
	success and failure (e.g., IP address).		
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	FTD, FMC	<p>FTD: <date> <time> <host> %FTD-5-199017: login[3417]: pam_unix(login:session): session closed for user admin#012</p> <p>FMC: <date> <time> <host> expire-session.pl: <host>: <user>@local, Session Expiration, Session terminated on ttyS0 due to inactivity (admin)</p>
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	FTD, and FMC	<p>FTD: <u>SSH Idle Timeout:</u> <date> <time> <host> sshd[5571]: Received disconnect from 172.16.16.91:60774: 11: disconnected by user#012 <date> <time> <host> sshd[5571]: Disconnected from user admin 172.16.16.91 port 60774#012</p> <p>FMC: <u>WebUI Session Lock:</u> <date> <time> <host> expire-session.pl: <host>: <user>@Default User IP, Session Expiration, Session expired due to inactivity (admin) <u>SSH Session Lock:</u> <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> -clish: CLI terminal closed. Sending SIGINT to process group 32731: sudo /bin/kill -s 2 -32731</p>
FTA_SSL.4	The termination of an interactive session.	FTD, and FMC	<p>FTD: <u>Console logout:</u> <date> <time> <host> login[5660]: pam_unix(login:session): session closed for user admin</p> <p><u>SSH Logout:</u> <date> <time> <host> sshd[6716]: Received disconnect from 172.16.16.91:57756: 11: disconnected by user#012 <date> <time> <host> sshd[6716]: Disconnected from user admin 172.16.16.91 port 57756#012</p> <p>FMC: <u>WebUI Logout:</u> <date> <time> <host> login.cgi: <host>: <user>@10.6.16.45, Logout, Logout Success <u>Console Logout:</u> <date> <time> <host> login[5660]: pam_unix(login:session): session closed for user admin</p>

SFR	Auditable Event	Generated by	Actual Audited Event
			<p><u>SSH Logout:</u> <date> <time> <host> sshd[7843]: Received disconnect from 10.6.16.46 port 47538:11: disconnected by user <date> <time> <host> sshd[20745]: Disconnected from user admin 172.16.16.91 port 59290</p>
FTP_ITC.1	<p>Initiation of the trusted channel.</p> <p>Termination of the trusted channel.</p> <p>Failure of the trusted channel functions.</p> <p>Identification of the initiator and target of failed trusted channels establishment attempt</p>	FMC, and FTD	<p><u>All of the failure audits are covered in FCS_TLSC_EXT and FCS_TLSS_EXT.</u></p> <p>FTD: <u>Initiation of Syslog over TLS (Lina) sessions:</u> <date> <time> <host>: %FTD-6-725001: Starting SSL handshake with server diagnostic:172.16.16.194/7351 to 172.16.16.91/6514 for TLS session <u>Termination of Syslog over TLS (Lina) sessions:</u> <date> <time> <host>: %FTD-6-725007: SSL session with server diagnostic:172.16.16.194/32064 to 172.16.16.91/6514 terminated <u>Initiation of Syslog over TLS (FTDOS) sessions:</u> <date> <time> <host> syslog-ng[28545]: syslog-ng starting up; version='3.6.2' <u>Termination of Syslog over TLS (FTDOS) sessions:</u> <date> <time> <host> syslog-ng[18293]: syslog-ng shutting down; version='3.6.2' <u>Initiation of IPSec sessions:</u> <date> <time> <host> EDT: %FTD-7-302015: Built inbound UDP connection 3845 for outside:192.168.144.91/4500 (192.168.144.91/4500) to identity:192.168.144.94/4500 (192.168.144.94/4500) <u>Termination of IPSec sessions:</u> <date> <time> <host> EDT: %FTD-7-302016: Teardown UDP connection 3845 for outside:192.168.144.91/4500 to identity:192.168.144.94/4500 duration 0:00:05 bytes 3020</p> <p>FMC: <u>Initiation/Establishment of Syslog over TLS sessions:</u> <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)' <u>Termination of Syslog over TLS sessions:</u> <date> <time> <host> syslog-ng[4946]: Syslog connection broken; fd='17', server='AF_INET(10.6.16.46:6514)', time_reopen='60'</p>
FTP_TRP.1/Admin	<p>Initiation of the trusted path.</p> <p>Termination of the trusted path.</p>	FTD, FMC	<p>FTD: Covered in <u>FCS_SSHS_EXT.1, FIA_UIA_EXT.1, FTA_SSL.4</u></p> <p>FMC: Covered in <u>FCS_SSHS_EXT.1, FIA_UIA_EXT.1, FTA_SSL.4 and FCS_TLSS_EXT.1</u></p>

SFR	Auditable Event	Generated by	Actual Audited Event
	Failures of the trusted path functions.		
Reproduced from MOD_IPS_V1.0			
FAU_GEN.1/IPS[IPS]	See entries for FMT_SMF.1/IPS[IPS], IPS_ABD_EXT.1[IPS], IPS_IPB_EXT.1[IPS], IPS_NTA_EXT.1[IPS] and IPS_SBD_EXT.1[IPS]	FMC, FTD	See entries for FMT_SMF.1/IPS[IPS], IPS_ABD_EXT.1[IPS], IPS_IPB_EXT.1[IPS], IPS_NTA_EXT.1[IPS] and IPS_SBD_EXT.1[IPS]
FMT_SMF.1/IPS[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.	FMC	<u>Modification of which policies are active on TOE interface:</u> <date> <time> <host> sfdccsm: FMCv-7.0.5-65: admin@172.16.16.81, Policies > Access Control > Access Control > Policy Editor, Save Policy ABD.1 Anomaly Detection - THROUGHPUT ;Assigned to device(s) - ftd4140,fp1140ftd,ftdv-encs ;UnAssigned from device(s) - ftdv-encs is unassigned from policy Allow_All;ftd4140 is unassigned from policy Allow_All;fp1140ftd is unassigned from policy Allow_All;#000x0a#000x00 <u>Enabling/Disabling TOE interface with policy applied // Modification of active mode:</u> <date> <time> <host> sfdccsm: FMCv-7.0.5-65: admin@172.16.16.81, Devices > Device Management > NGFW Interfaces, Page View#000x0a#000x00

SFR	Auditable Event	Generated by	Actual Audited Event
	Modification of which mode(s) is/are active on a TOE interface.		<date> <time> <host> sfdccsm: FMCv-7.0.5-65: admin@172.16.16.81, Devices > Device Management > NGFW Interfaces, Save Policy fp1140#000x0a#000x00
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			
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

SFR	Auditable Event	Generated by	Actual Audited Event
Reproduced from the mod_vpngw_v1.1			
FPF_RUL_EXT.1[VPN]	Application of rules configured with the 'log' operation	FTD	<p><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</p> <p><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</p>

6.2.1 Logs of Intrusion and Firewall Events

The connection and intrusion events (hereafter, referred to as events) are generated by the “log” operation in the rule. The events are default to 100,000 entries size each (200,000 total). However, the internal database stores a maximum of 10,000,000 entries (depending on FMC models) and a minimum of 10,000 entries in the local database (to configure the size, go to System > Configuration > Database, and click on “Intrusion Event Database” or “Connection Database”). When the events log is full, the oldest events are overwritten by the newest events.

The following information is associated with each event in Table View mode:

Field	Description
Date	Time and date that the appliance generated the event record.
Access Control Rule	The access control rule that triggered the event.
Action	The configured action of the rule.
Initiator IP	The source IP address of the packet that triggered the event.
Responder IP	The destination IP address of the packet that triggered the event.
Source Port/ ICMP Type	The source port (for TCP and UDP) or ICMP type for IP of the packet that triggered the event.
Destination Port/ ICMP Code	The destination port (for TCP and UDP) or ICMP code for IP of the packet that triggered the event.
Protocol	The protocol of the packet that triggered the event.
Ingress Interface	The incoming interface of the packet.
Egress Interface	The outgoing interface of the packet.

FTD logging of firewall (Access Control Policy) events is disabled by default and can be configured via FMC (Devices > Platform Settings) to do any of: log to the local buffer (check “Enable Logging” on the “Logging Setup” tab, and add a logging destination of “Internal Buffer” on the “Logging Destination” tab); transmit messages to a syslog server (add a server on the “Syslog Servers” tab, and add a logging destination of “Syslog Servers” on the “Logging Destination” tab). Once the logging setup as been configured as described above more configuration is required to generate audit messages for traffic filtering events; to configure logging for Access Control Policy rules refer to section [5.2.2 Access Control Rules](#) of this guide. To send a copy of traffic filter events to FMC (viewable via the Audit Log event viewer), enable “Event Viewer” in the “Logging” tab of the Access Control Policy rule.

Examples of events for access control rules (viewable via System > Monitoring > Audit > Edit Search > Connection Events, which is equivalent/redirects to Analysis > Connections > Events):

<input type="checkbox"/>	▼ First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
<input type="checkbox"/>	2013-04-08 14:51:33		Block	IP Block	10.22.35.100		176.65.80.2	ITA	External	Internal	30845 / udp	58117 / udp
<input type="checkbox"/>	2013-04-08 14:51:31		Block	IP Block	10.22.240.17		65.49.70.243	USA	Internal	External	123 (ntp) / udp	123 (ntp) / udp
<input type="checkbox"/>	2013-04-08 14:51:18		Block	IP Block	10.5.32.68		64.6.144.6	USA	External	Internal	123 (ntp) / udp	123 (ntp) / udp
<input type="checkbox"/>	2013-04-08 14:51:18		Block	IP Block	10.5.32.177		65.49.70.243	USA	External	Internal	123 (ntp) / udp	123 (ntp) / udp
<input type="checkbox"/>	2013-04-08 14:51:04		Block	IP Block	10.5.56.143		64.6.144.6	USA	Internal	External	123 (ntp) / udp	123 (ntp) / udp
<input type="checkbox"/>	2013-04-08 14:50:59		Block	IP Block	10.5.59.62		65.49.70.244	USA	Internal	External	123 (ntp) / udp	123 (ntp) / udp
<input type="checkbox"/>	2013-04-08 14:50:58		Block	IP Block	10.5.32.112		4.28.136.39	CAN	External	Internal	62906 / tcp	80 (http) / tcp
<input type="checkbox"/>	2013-04-08 14:50:58		Block	IP Block	10.5.60.86		64.6.144.6	USA	External	Internal	123 (ntp) / udp	123 (ntp) / udp
<input type="checkbox"/>	2013-04-08 14:50:53		Block	IP Block	10.5.11.104		38.101.77.21	USA	External	Internal	123 (ntp) / udp	123 (ntp) / udp
<input type="checkbox"/>	2013-04-08 14:50:50		Block	IP Block	10.5.59.102		64.6.144.6	USA	Internal	External	123 (ntp) / udp	123 (ntp) / udp
<input type="checkbox"/>	2013-04-08 14:50:39		Block	IP Block	10.5.31.73		38.101.77.21	USA	Internal	External	123 (ntp) / udp	123 (ntp) / udp

Examples of connection events:

Time	Priority	Impact	Inline Result	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Message	Classification	Generator	Ingress Security Zone	Egress Security Zone	Ingress Interface	Egress Interface
2014-07-03 19:37:09	medium	0	↓	10.3.1.3	10.1.1.2	0 / ip	0 / ip	FRAG3_ANOMALY_OVERSIZE (123-5)	Attempted Denial of Service	IP:DenyGenerator	IP:external	IP2:external	isp2	isp0

Examples of intrusion events:

Message	Priority	Classification	Count
FRAG3_TINY_FRAGMENT (123:13)	medium	Attempted Denial of Service	2
FRAG3_ANOMALY_OVLP (123:8)	low	Generic Protocol Command Decode	1

6.3 Management of Intrusion Events

When the system identifies a possible intrusion, it generates an *intrusion event*, which is a record of the date, time, the type of exploit, and contextual information about the source of the attack and its target. For packet-based events, a copy of the packet or packets that triggered the event is also recorded. Managed Devices transmit their events to the Firepower Management Center where you can view the aggregated data and gain a greater understanding of the attacks against your network assets.

You can also deploy a managed Device as an inline, switched, or routed intrusion system, which allows you to configure the Device to drop or replace packets that you know to be harmful.

The initial intrusion events view differs depending on the workflow you use to access the page. You can use one of the predefined workflows, which includes one or more drill-down pages, at able view of intrusion events, and a terminating packet view, or you can create your own workflow. You can also view workflows based on custom tables, which may include intrusion events.

6.3.1 Viewing Intrusion Events

1. Log in with Administrator Role or Security Analyst.
2. Select Analysis > Intrusions > Events.

Audit Record:

2016-11-17 19:56:43 admin Analysis > Intrusion Events > Events Page View 10.128.120.41

The list below describes the intrusion event information that can be viewed, searched, filtered, and sorted by the system. In addition, basic contents such as date, time, and type can also be used to filter and sort. Note only Administrators and Intrusion Admins have access to the intrusion events.

NOTE! Some fields in the table view of intrusion events are disabled by default. To enable a field for the duration of your session, expand the search constraints, then click the column name under **Disabled Columns**.

Samples of Intrusion Event (split into 3 parts)

Time	Priority	Impact	Inline Result	Source IP	Source Country	Destination IP	Destination Country	Source Port / ICMP Type	Destination Port / ICMP Code	SSL Stat
2017-07-07 13:02:17	low	0	↓					0 / ip	0 / ip	Unkn
2017-07-07 13:02:33	low	0	↓					0 / ip	0 / ip	Unkn
2017-07-07 13:02:49	low	0	↓					0 / ip	0 / ip	Unkn
2017-07-07 13:46:09	high	0	↓	51.189.153.117	GBR	174.25.1.9	USA	0 (Echo Reply) / icmp	0 (No Code) / icmp	Unkn
2017-07-07 13:03:04	high	0	↓	79.207.141.219	DEU	174.25.1.9	USA	8 (Echo Request) / icmp	0 (No Code) / icmp	Unkn

SSL Status	VLAN ID	Message	Classification	Generator	Source User	Application Protocol	Client	Web Application
Unknown (Unknown)	0	DECODE_IPV4_DGRAM (116:1:1)	Generic Protocol Command Decode	Snort Decoder	0			
Unknown (Unknown)	0	DECODE_IPV4_INVALID_HEADER_LEN (116:2:2)	Generic Protocol Command Decode	Snort Decoder	0			
Unknown (Unknown)	0	DECODE_IPV4_DGRAM_LT_IPHDR (116:3:2)	Generic Protocol Command Decode	Snort Decoder	0			
Unknown (Unknown)	0	1:1100007:14	SBD.1.1-header	Standard Text Rule	0			
Unknown (Unknown)	0	IPv4 ID Header Field Match (1:1100005:14)	SBD.1.1-header	Standard Text Rule	0	<input type="checkbox"/> No Authentication Required	<input type="checkbox"/> ICMP	<input type="checkbox"/> ICMP client

Web Application	IOC	Application Risk	Business Relevance	Ingress Security Zone	Egress Security Zone	Device	Security Context	Ingress Interface	Egress Interface	Intrusion Policy	Access Control Policy	Access Control Rule	Network Analysis Policy
				Virtual-eth1	Virtual-eth2	NGIPSv		eth1	eth2	SBD.1.1 Header Rules	SBD.1.1 Header Fields		Net Access Policy - Comr
				Virtual-eth1	Virtual-eth2	NGIPSv		eth1	eth2	SBD.1.1 Header Rules	SBD.1.1 Header Fields		Net Access Policy - Comr
				Virtual-eth1	Virtual-eth2	NGIPSv		eth1	eth2	SBD.1.1 Header Rules	SBD.1.1 Header Fields		Net Access Policy - Comr
				Virtual-eth1	Virtual-eth2	NGIPSv		eth1	eth2	SBD.1.1 Header Rules	SBD.1.1 Header Fields		Net Access Policy - Comr
		Medium	Medium	Virtual-eth1	Virtual-eth2	NGIPSv		eth1	eth2	SBD.1.1 Header Rules	SBD.1.1 Header Fields	SBD.1.1 Header Fields	Net Access Policy - Comr

Access Control Policy

The access control policy associated with the intrusion policy where the intrusion, preprocessor, or decoder rule that generated the event is enabled.

Access Control Rule

The access control rule that invoked the intrusion policy that generated the event. Default Action indicates that the intrusion policy where the rule is enabled is not associated with a specific access control rule but, instead, is configured as the default action of the access control policy.

This field is blank if intrusion inspection was associated with neither an access control rule nor the default action, for example, if the packet was examined by the default intrusion policy.

Application Protocol

The application protocol, if available, which represents communications between hosts detected in the traffic that triggered the intrusion event.

Application Risk

The risk associated with detected applications in the traffic that triggered the intrusion event: Very High, High, Medium, Low, and Very Low. Each type of application detected in a connection has an associated risk; this field displays the highest risk of those.

Count

The number of events that match the information that appears in each row. Note that the Count field appears only after you apply a constraint that creates two or more identical rows. This field is not searchable.

Destination Country

The country of the receiving host involved in the intrusion event.

Destination IP

The IP address used by the receiving host involved in the intrusion event.

Destination Port / ICMP Code

The port number for the host receiving the traffic. For ICMP traffic, where there is no port number, this field displays the ICMP code.

Destination User

The User ID for any known user logged in to the destination host.

Device

The managed Sensor where the access control policy was deployed.

Domain

The domain of the Sensor that detected the intrusion. This field is only present if you have ever configured the Firepower Management Center for multitenancy.

Egress Interface

The egress interface of the packet that triggered the event. This interface column is not populated for a passive interface.

Egress Security Zone

The egress security zone of the packet that triggered the event. This security zone field is not populated in a passive deployment.

Email Attachments

The MIME attachment filename that was extracted from the MIME Content-Disposition header. To display attachment file names, you must enable the SMTP preprocessor [Log MIME Attachment Names](#) option. Multiple attachment filenames are supported.

Email Headers (search only)

The data that was extracted from the email header. To associate email headers with intrusion events for SMTP traffic, you must enable the SMTP preprocessor [Log Headers](#) option.

Generator

The component that generated the event.

HTTP Hostname

The hostname, if present, that was extracted from the HTTP request Host header. Note that request packets do not always include the hostname.

To associate hostnames with intrusion events for HTTP client traffic, you must enable the HTTP Inspect preprocessor [Log Hostname](#) option.

In table views, this column displays the first fifty characters of the extracted host name. You can hover your pointer over the displayed portion of an abbreviated host name to display the complete name, up to 256 bytes. You can also display the complete host name, up to 256 bytes, in the packet view.

HTTP Response Code

The HTTP status code sent in response to a client's HTTP request over the connection that triggered the event.

HTTP URI

The raw URI, if present, associated with the HTTP request packet that triggered the intrusion event. Note that request packets do not always include a URI.

To associate URIs with intrusion events for HTTP traffic, you must enable the HTTP Inspect preprocessor **Log URI** option.

To see the associated HTTP URI in intrusion events triggered by HTTPResponses, you should configure HTTP server ports in the **Perform Stream Reassembly on Both Ports** option; note, however, that this increases resource demands for traffic reassembly.

This column displays the first fifty characters of the extracted URI. You can hover your pointer over the displayed portion of an abbreviated URI to display the complete URI, up to 2048bytes. You can also display the complete URI, up to 2048 bytes, in the packet view.

Ingress Interface

The ingress interface of the packet that triggered the event. Only this interface column is populated for a passive interface.

Ingress Security Zone

The ingress security zone of the packet that triggered the event. Only this security zone field is populated in a passive deployment.

Inline Result

Actions

Intrusion Policy

The intrusion policy where the intrusion, preprocessor, or decoder rule that generated the event was enabled.

Message

The explanatory text for the event. For rule-based intrusion events, the event message is pulled from the rule.

Priority

The event priority as determined by the Cisco Talos Security Intelligence and Research Group (Talos). The priority corresponds to either the value of the priority keyword or the value for the classtype keyword.

For other intrusion events, the priority is determined by the decoder or preprocessor. Valid values are high, medium, and low.

Protocol (search only)

The name or number of the transport protocol used in the connection.

Snort ID (search only)

Specify the Snort ID (SID) of the rule that generated the event or, optionally, specify the combination Generator ID (GID) and SID of the rule, where the GID and SID are separated with a colon (:) in the format GID:SID.

Source Country

The country of the sending host involved in the intrusion event.

Source IP

The IP address used by the sending host involved in the intrusion event.

Source Port / ICMP Type

The port number on the sending host. For ICMP traffic, where there is no port number, this field displays the ICMP type.

Source User

The User ID for any known user logged in to the source host.

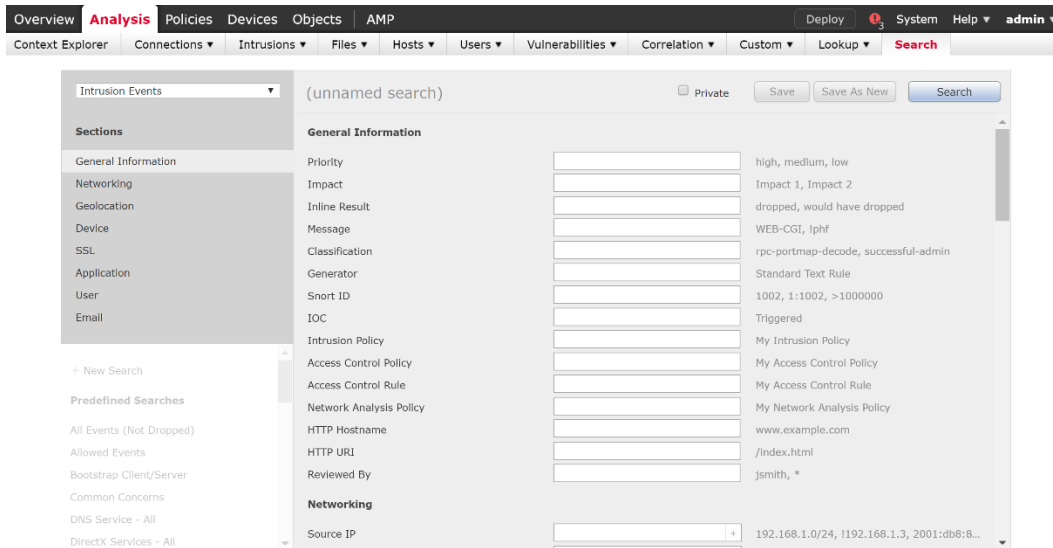
The intrusion events cannot be modified but they can be deleted by the Administrators or Intrusion Admins who have restricted access. When the intrusion events storage is full, the newest data will overwrite the oldest data.

The intrusion event database stores a maximum of 100,000 entries. When the number of intrusion event entries greatly exceeds 100,000, the appliance overwrites the oldest records from the database to reduce the number to 100,000.

NOTE! To change the maximum number of entries, go to System > Configuration > Database > Intrusion Event Database > Maximum Intrusion Events

6.3.2 Searching Intrusion Events

1. Login with Administrator Role.
2. Select Analysis > Intrusions > Events.
3. Click on the **Edit Search** link.



4. Enter the value you want to search for then click **Search**.

6.3.3 Sorting and filtering Intrusion Events

1. Login with Administrator Role.
2. Select Analysis > Intrusions > Events.
3. Click on the column name to sort the intrusion events based on that column.

4. To configure (i.e., filter) different column names, create a workflow via [Analysis > Custom > Custom Workflows](#).
5. Click Create Custom Workflow.
6. Give your workflow a descriptive name. In the **Table** drop-down, select **Intrusion Events**.
7. Click **Add Page**.
8. Set the **Sort Priority** and **Field** for each column. There are five columns to configure.

Creating Workflow

Name:

Description:

Table:

Page 1

Page Name:

Sort Type:

Column 1	Column 2	Column 3	Column 4	Column 5
Sort Priority	Field	Sort Priority	Field	Sort Priority
<input type="text" value="1"/>	<input type="text" value="Time"/>	<input type="text" value="2"/>	<input type="text" value="Source IP"/>	<input type="text" value="3"/>
<input type="text" value="4"/>	<input type="text" value="Priority"/>	<input type="text" value="5"/>	<input type="text" value="Egress Interfa"/>	<input type="text" value="Count"/>

9. Click **Save**.
10. Go back to intrusion events via [Analysis > Intrusions > Events](#).

Click on the [switch workflow](#) link and choose the workflow you created.

6.4 Device Registration

Before you manage a Device with a Firepower Management Center, you must make sure that the network settings are configured correctly on the Device. This is usually completed as part of the installation process. In addition, the management network should be an internal, trusted network separated physically or logically from the monitored network.

In order for the FMC and FTD to communicate, they must successfully complete a registration process, which requires administrative actions on the FMC and corresponding administrative actions on the FTD (refer to detailed instructions in the subsections below). Other than the steps described in the subsections below, no further configuration steps are required to join the FTD to the FMC. The administrative actions on FMC and FTD require the administrator to input a “registration key” that the two devices will use to authenticate their initial TLS communications. During the registration process, the FMC and FTD confirm they have a matching registration key, and use their initial self-signed TLS certificates to uniquely identify themselves to each other (each device certificate signed by FMC, including its own, contains a unique identifier stored as an ‘id-at-title’ attribute, which FMC and FTD each as the unique reference identifier for each other). If the authentication succeeds, the local CA within the FMC will sign and issue a new TLS certificate for the FTD and send (over the existing TLS session) the FTD’s new identity certificate and associated keys, and the FMC’s root CA cert, and the FMC’s root CA certificate and the device certificates which it signed will be used to authenticate all subsequent TLS sessions between the two devices.

If device registration fails due to mismatched registration keys, or incorrect IP address or hostname, correct the information on the FMC and/or FTD and reinitiate the registration from FMC (using the Add Device button described in the subsection below). If the connection between FMC and FTD is broken during device registration, the FMC and FTD will continue to attempt to reconnect and retry registration for up to two minutes. If the registration has not completed within two minutes, restore connectivity between the FMC and FTD and reinitiate the registration from FMC.

Note that if you registered a Firepower Management Center and a Device using IPv4 and want to convert them to IPv6, you must delete and re-register the Device.

The communication between the FMC and FTD is protected by TLSv1.2. TLS provides authentication, key exchange, encryption and integrity protection of all data transmitted between the TOE components. TLS session resumption is not supported in case the TLS connection between the TOE components is unintentionally broken. If connectivity is lost between FMC and FTD after device registration each endpoint will automatically attempt to re-initiate connection to the other until connectivity is restored, no administrative action is required other than resolving any connectivity issues in the networks between the FMC and FTD. The current status of each device can be viewed on the Device Management page (Devices > Device Management) where an icon indicates the current status (error, critical, warning, normal/recovered, or disabled). Detailed health conditions can be viewed on the Health Monitor page (System > Health > Monitor). The date and time each FTD was last seen by FMC can be viewed for each device individually by checking the Last Contacted timestamp under the status icon (Devices > Device Management > edit any device > view the Device tab > view the Management section).

The same ciphersuites are used by the TLS client and TLS server during device registration as are used during subsequent inter-device communications. The following ciphersuites are supported on the client side of the TLS implementation –

- 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_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
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

And the following ciphersuites on the server side –

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 (TLSv1.2 only)

- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268 (TLSv1.2 only)
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 (TLSv1.2 only)
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246 (TLSv1.2 only)
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288 (TLSv1.2 only)
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288 (TLSv1.2 only)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492 (TLSv1.2 only)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492 (TLSv1.2 only)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 (TLSv1.2 only)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 (TLSv1.2 only)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 (TLSv1.2 only)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 (TLSv1.2 only)

6.4.1 Device Registration On FTD

1. Login to the CLI with Administrator Role.
2. Use the “configure manager add” command. The syntax is shown below.

configure manager add {hostname | IPv4_address | IPv6_address} [registration key]

where {hostname | IPv4_address | IPv6_address} specifies the DNS hostname or IP address (IPv4 or IPv6) of the Firepower Management Center that manages this Device.

NOTE! The registration key is a one-time shared secret of your choice that you will also specify on the FMC when you register the FTD. The registration key from 8 to 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-).

3. [Optional] To de-register a manager, just enter “configure manager delete” command. It is recommended to delete the Device from the FMC first before using this command on FTD.

6.4.2 Device Registration On FMC

1. Login with Administrator Role.
2. Select Device > Device Management.
3. From the **Add** drop-down menu, choose **Add Device**.

NOTE! To de-register a Device, just click on the trash can icon next to the Device you want to remove.

4. In the **Host** field, enter the IP address or the hostname of the Device you want to add.
5. In the **Display Name** field, enter a name for the Device as you want it to display in the Firepower Management Center.
6. In the **Registration Key** field, enter the same registration key that you used when you configured the Device to be managed by the Firepower Management Center.
7. Choose licenses to apply to the Device.
8. Click **Register** to add the Device to the Firepower Management Center.

6.5 Custom Web Server Certificate

Transport Layer Security (TLS) certificates enable Firepower Management Centers and managed Devices to establish an encrypted channel between the system and a web browser. A default certificate is included with all FTD (ASA and ISA) Devices, but it is not generated by a certificate authority (CA) trusted by any globally known CA. For this reason, consider replacing it with a custom certificate signed by a globally known or internally trusted CA.

You can generate a certificate request based on your system information and the identification information you supply. You can use it to self-sign a certificate if you have an internal certificate authority (CA) installed that is trusted by your browser. You can also send the resulting request to a certificate authority to request a server certificate. After you have a signed certificate from a certificate authority (CA), you can import it.

6.5.1 Generating an HTTPS Server Certificate Signing Request

When you generate a certificate request through the local configuration HTTPS Certificate page using this procedure, you can only generate a certificate for a single system. If you install a certificate that is not signed by a globally known or internally trusted CA, you receive a security warning when you connect to the system.

1. Login with Administrator Role.
2. Select System > Configuration.
3. Click HTTPS Certificate.
4. Click Generate New CSR.
5. Enter a country code in the **Country Name (two-letter code)** field.
6. Enter a state or province postal abbreviation in the **State or Province** field.
7. Enter a Locality or City.
8. Enter an **Organization** name.
9. Enter an Organization Unit (Department) name.
10. Enter the fully qualified domain name of the server for which you want to request a certificate in the **Common Name** field.

NOTE! Enter the fully qualified domain name of the server exactly as it should appear in the certificate in the **Common Name** field. If the common name and the DNS hostname do not match, you receive a warning when connecting to the appliance.

11. Click Generate.
12. Open a text editor.
13. Copy the entire block of text in the certificate request, including the BEGIN CERTIFICATE REQUEST and END CERTIFICATE REQUEST lines, and paste it into a blank text file.
14. Save the file as servername.csr, where servername is the name of the server where you plan to use the certificate.
15. Click **Close**.

6.5.2 Importing HTTPS Server Certificate

If the signing authority that generated the certificate requires you to trust an intermediate CA, you must also supply a certificate chain (or certificate path). Please note only PEM format is supported.

1. Login with Administrator Role.
2. Select System > Configuration.
3. Click HTTPS Certificate.
4. Click Import HTTPS Certificate.
5. Open the server certificate in a text editor, copy the entire block of text, including the BEGIN CERTIFICATE and END CERTIFICATE lines. Paste this text into the **Server Certificate** field.
6. If you want to upload a private key, open the private key file and copy the entire block of text, including the BEGIN RSA PRIVATE KEY and END RSA PRIVATE KEY lines. Paste this text into the **Private Key** field.
7. Open any required intermediate certificates, copy the entire block of text for each, and paste it into the **Certificate Chain** field.
8. Click **Save**.

6.6 User and Role Management

If you have Administrator Role, you can use the web interface to view and manage user accounts on a FMC, including adding, modifying, and deleting accounts. User accounts without Administrator Role are restricted from accessing user management functions. The CLI has “show users” and “configure users” commands but they are only available for the virtual appliances. Management of the user and role is performed via web interface only. Note that all users created are TOE administrators.

On FMC, the WebUI accounts are separate from the CLI accounts. Even though they both have a default account called “admin” those accounts and their credentials are separate. If the ‘admin’ account for WebUI becomes locked (e.g., due to consecutive failed login attempts), the ‘admin’ account for CLI will remain unlocked, and vice versa. To avoid risk of lockout on FMC, restrict the source IP addresses that can initiate SSH, or disable SSH.

This remainder of this section covers configuration of FMC accounts. To configure FTD accounts, refer to section [4.4 FTD Initial Configuration](#) of this document.

6.6.1 Viewing User Accounts

From the User Management page, you can view, edit, and delete existing accounts.

1. Login with Administrator Role.
2. Select System > Users

The User Management page appears, showing each user, with options to activate, deactivate, edit, or delete the user account.

Username	Roles	Authentication Method	Password Lifetime	
admin	Administrator	Internal	Unlimited	
testuser	Discovery Admin	Internal	Unlimited	

Audit Record:

2013-02-26 18:33:35 admin System > Local > User Management > Users Page View 10.4.10.227

6.6.2 Adding New User Accounts

When you set up a new user account, you can control which parts of the system the account can access. You can set password expiration and strength settings for the user account during creation. For a local account on a Device, you can also configure the level of command line access the user will have. On the FTD, use the command “configure user add <username> [basic | configure]”. To get more CLI options, use the command “configure user ?”.

1. Login with Administrator Role.
2. Select System > Users.
3. Click Create User.

4. In the **User Name** field, type a name for the new user.

New user names must contain alphanumeric or hyphen characters with no spaces, and must be no more than 32 characters.

5. Do NOT check the Use External Authentication Method checkbox.
6. In the **Password** and **Confirm Password** fields, type a password (up to 32 alphanumeric characters). The following alphanumeric characters can be a part of the password - [" ! " , " @ " , " # " , " \$ " , " % " , " ^ " , " & " , " * " , " (" , ") " , " ' " ' ` (double or single quote/apostrophe), + (plus), - (minus), = (equal), , (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).

Note: Entering a password of more than 32 characters will result in the password automatically being truncated to 32 characters.

Strong Password Composition:

The password must be at least eight alphanumeric characters of mixed case and must include at least one numeric character and one special character. It cannot be a word that appears in a dictionary or include consecutive repeating characters.

7. Set the **Maximum Number of Failed Logins** to 1 to 99 (recommended). The default setting is 5.

Note: The account is locked if the maximum number of failed login attempts is exceeded, however, lockout does not occur unless the operator attempting to log in performs one more failed authentication over the configured maximum failed number of logins

8. Configure the user account password options. For example, set the **Minimum Password Length** to 15. The default setting is 8 and the maximum allowable is 32.
9. If you are creating a local user through the web interface of a Device, you can assign the level of **Command-Line Interface Access** for the user:
 - Select **None** to disable access to the command line for the user.
 - Select **Basic** to allow the user to log into the shell and to access a specific subset of commands.
 - Select **Configuration** to allow the user to log into the shell and use any command line option, including expert mode if that is allowed on the appliance.
10. Check the **Check Password Strength** checkbox. By default, this is not selected.


WARNING! This is a recommended evaluated configuration setting.

11. Do NOT click on the **Exempt from GUI Session Timeout** checkbox.
12. Select the access roles to grant the user.
 - "IPS Administrator" (or Administrator): Have all privileges and access.
 - "IPS Analyst" (or Intrusion Admin): Have all access to intrusion policies and network analysis privileges but cannot deploy policies
 - Access Admin: Have all access to access control policies but cannot deploy policies
 - Discovery Admin: Have all access to network discovery, application detection, and correlation features but cannot deploy policies

- Security Analyst: Have all access to security event analysis feature

13. Click **Save**.

Audit Record:

2013-02-26 18:36:08	admin	System > Local > User Management > Users	 Added user - CCuser:134	10.4.10.227
-------------------------------------	-----------------------	---	---	-----------------------------

time : 1488331638 (Wed Mar 1 01:27:18 2017)

event_type : Default Action

subsystem : Command Line

actor : admin

message : Executed root-view- configure user add tester1 config



result : Success

action_source_ip : 10.128.120.150



action_destination_ip : Default Target IP

6.6.3 Modifying and Deleting User Accounts

Administrator can modify or delete user accounts from the system at any time, with the exception of the **admin** account, which cannot be deleted. On the FTD, use the command “configure user delete <username>”. To get more CLI options, use the command “configure user ?”.

1. Login with Administrator Role.
2. Select System > Users.
3. Click the edit icon () next to the user you want to modify.
4. Modify the settings you choose and click **Save**.
5. To delete a user account, click the delete icon () next to the user you want to delete.
6. Click **OK** to confirm.
7. The user account is deleted.

Audit Record:

2013-02-26 18:38:33	admin	System > Local > User Management > Users	 Edited user - CCuser:135	10.4.10.227
2013-02-26 18:38:44	admin	System > Local > User Management > Users	 Deleted user - CCuser:136	10.4.10.227

time : 1488331670 (Wed Mar 1 01:27:50 2017)

event_type : Default Action

subsystem : Command Line

actor : admin

message : Executed root-view- configure user delete tester1

result : Success

action_source_ip : 10.128.120.150

action_destination_ip : Default Target IP

6.6.4 Unlocking FMC Accounts

If an FMC account becomes locked due to exceeding the configured Maximum Number of Failed Logins, the account will show “(Locked)” under System > Users > Users as shown in the screenshot below, and the account status icon will be gray with an X instead of blue with a checkmark. To unlock the account, click on the gray X to change it to a blue checkmark.

Username	Roles	Authentication Method	Password Lifetime	
admin	Administrator	Internal	Unlimited	
lockme	Administrator	Internal	Unlimited (Locked)	
testuser	Administrator	Internal	Unlimited	

6.7 Change Password

All user accounts are protected with a password. You can change your password⁷ at any time, and depending on the settings for your user account, you may have to change your password periodically due to password expiration. You can use either the web page or the CLI to change your password.

Note that if password strength checking is enabled, passwords must be at least eight alphanumeric characters of mixed case and must include at least one number and one special character. Passwords cannot be a word that appears in a dictionary or include consecutive repeating characters.

6.7.1 Configure Password via GUI

1. From the drop-down list under your username, select **User Preferences**.

Changing Password for: admin

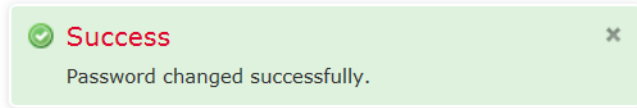
Current Password

New Password

Confirm

2. In the **Current Password** field, type your current password.
3. In the **New Password** and **Confirm** fields, type your new password.
4. Click **Change**.
5. The Success message appears.

⁷ Only user with Administrator Role can change another user's password.



Audit Record:

2013-02-26 18:40:19

admin

User Preferences > Change Password

Change

10.4.10.227

6.7.2 Configure Password via CLI

The command *configure password* allows the current user to change their password.

After issuing the command, the CLI prompts the user for their current password, then prompts the user to enter the new password twice.

Access

Basic

Syntax

configure password

Example

➤ configure password

Enter current password:

Enter new password:

Confirm new password:

Audit Record:

```

Enter current password:
Enter new password:
Confirm new password:

> show audit-log
Audit Log Output:
time           : 1361900652 (Tue Feb 26 17:44:12 2013)
event_type     : Default Action
subsystem      : Command Line
actor          : admin
message        : Executed root-view- show audit-log
result         : Success
action_source_ip : 10.4.10.227
action_destination_ip : Default Target IP
-----
time           : 1361900637 (Tue Feb 26 17:43:57 2013)
event_type     : Default Action
subsystem      : Command Line
actor          : admin
message        : Executed root-view- configure password
result         : Success
action_source_ip : 10.4.10.227
action_destination_ip : Default Target IP
-----

```

6.7.3 Password Recovery Procedures

To reset the password of FMC GUI accounts, follow instructions under “Change the Web Interface Admin Password for FMCs” in [Reset the Password of the Admin User on a Cisco Firepower System](#).

To reset the password for FMC CLI accounts, follow instructions under “Change the CLI or Shell Admin Password for FMCs and NGIPSv” in [Reset the Password of the Admin User on a Cisco Firepower System](#).

6.8 Configure Time Synchronization

An administrator can manage time synchronization on the FMC using the Time Synchronization page and the Time page. In the CC-evaluated configuration the FMC clock must be set manually, and must not use an NTP server.

Note that time settings are displayed on most pages on the FMC in local time using the time zone you set on the Time Zone page (America/New York by default), but are stored on the appliance itself using UTC time. In addition, the current time appears in UTC at the top of the Time Synchronization page (local time is displayed in the Manual clock setting option, if enabled).

6.8.1 Setting the Time Manually

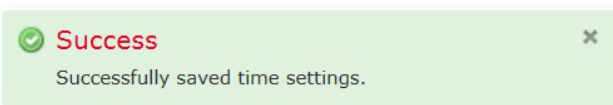
1. Login with Administrator Role.
2. Select **System > Configuration > Time Synchronization**.
3. Configure the “Set My Clock” setting to “Manually in Local Configuration”
4. Click **Save**.
5. Select **System > Configuration > Time**.

Current Setting Manual (based on System Policy [katsura system policy](#))

Current Time 2013-02-26 12:13

Set Time / / , : [America/New York](#)

6. Select the following from the **Set Time** drop-down lists:
 - Year
 - Month
 - Day
 - Hour
 - Minute
7. Click **Apply**.
8. The Success message appears.



Audit Record:

2013-02-26 17:41:02	admin	System > Local > Configuration > Time	Page View	10.4.10.227
2013-02-26 17:41:01	admin	Updated time to Tue 26 Feb 2013 05:41:00 PM EST from Tue 26 Feb 2013 06:41:47 PM EST	Save	10.4.10.227

6.9 Configure Login Banner

Administrator can create a custom login banner that appears when users log into the appliance using SSH and on the login page of the web interface. Banners can contain any printable characters except the less-than symbol (<) and the greater-than symbol (>).

1. Login with Administrator Role.
2. Depending on whether you are configuring audit log streaming for a Firepower Management Center or a managed Device:
 - Management Center—Choose **System > Configuration**.
 - Managed Device—Choose **Devices > Platform Settings** and create or edit a Firepower or FTD policy.
3. Click **Login Banner** (FP) or **Banner** (FTD).

4. In the **Custom Login Banner** field, enter the login banner you want to use with this system policy.
5. Click **Save**.
6. Click **Deploy** if you are configuring these settings for the managed Devices. Select the Device(s) you want to deploy the setting to and click **Deploy** again.

Audit Record:

2013-02-26 17:44:19 admin System > Local > System Policy > Login Banner > Modified: Custom Login Banner New Banner > This is a banner Save 10.4.10.227

6.10 Inactivity Timeout Setting

By default, all user sessions (web-based and CLI) automatically log out after 60 minutes (1 hour) of inactivity, unless you are otherwise configured to be exempt from session timeout. Users with Administrator Role can change the inactivity timeout value in the system policy to meet their security needs.

1. Login with Administrator Role.
2. Depending on whether you are configuring audit log streaming for a Firepower Management Center or a managed Device:
 - Management Center (FMC) —Choose **System > Configuration**.

- Managed Device (FTD) — Refer to section [4.4.7 Configure Inactivity Timeout Settings](#) of this document.

3. Click **Shell Timeout**. Note, the “Shell Timeout (Minutes)” value applies to all CLI access, including serial console and SSH.

Browser Settings	
Browser Session Timeout (Minutes)	<input type="text" value="60"/>
Shell Settings	
Shell Timeout (Minutes)	<input type="text" value="0"/>

4. In the **Browser Session Timeout (Minutes)** and **Shell Timeout (Minutes)** fields, enter a value from 1 – 1440 (24 hours) max. The timeout value is 1 minute plus the configured value. The value of 0 will disable this feature.

WARNING! This is a required evaluated configuration setting and must NOT be disabled.

6. Click **Save**.
7. Click **Deploy** if you are configuring these settings for the managed Devices. Select the Device(s) you want to deploy the setting to and click **Deploy** again.

Audit Record:

2013-02-26 18:11:53 admin System > Local > System Policy > User Interface > Modified: Shell Timeout (Minutes) 0 > 15 Save 10.4.10.227

6.10.1 Session Timeout Record

The system will record in the audit log when a user is logged out due to inactivity.

Audit Record:

2013-02-26 18:02:26 admin Session Expiration Session terminated due to inactivity (admin) 10.2.100.250

```
Audit Log Output:
time           : 1362178064 (Fri Mar 1 22:47:44 2013)
event_type     : Default Action
subsystem      : Command Line
actor          : admin
message        : Executed root-view- show audit-log
result         : Success
action_source_ip : 10.4.10.223
action_destination_ip : Default Target IP
-----
time           : 1362177449 (Fri Mar 1 22:37:29 2013)
event_type     : Session terminated on pts/0 due to inactivity (admin)
subsystem      : Session Expiration
actor          : admin
message        : Session terminated on pts/0 due to inactivity (admin)
result         : Success
action_source_ip : 10.4.10.223
action_destination_ip : 10.5.60.81
```

6.11 Product Upgrade

Cisco electronically distributes several different types of updates, including major and minor updates to the system software itself, as well as intrusion rule updates and VDB updates. Administrator must update the FMC before you can update the Devices they manage. Cisco recommends that you use the FMC’s web interface to update not only itself, but also the Devices it manages. Updates for FMC and FTD are uploaded to FMC prior to installation; FTD updates are initiated from FMC to FTD.

As FMC and FTD updates are uploaded to FMC the FMC automatically verifies their integrity using RSA digital signature verification. If any file fails the signature verification an “Upload failed” message will be displayed at the top-center of the page, the file will not be stored on FMC, and the file will not be listed on the Product Updates page so it cannot be installed. If the error message indicates a lack of storage space, remove unneeded update files and repeat the upload. If any other reason for failure is indicated in the Upload Failed error message, re-download the update file from software.cisco.com, and re-attempt the upload. If the upload (including image integrity verification) is successful, the uploaded file will be listed on the Product Updates page. If uploads continue to fail, contact Cisco TAC for assistance.

When stored update files are installed their integrity is verified again using RSA digital signature verification; the FMC will re-verify integrity of FMC updates, and the FTD will verify integrity of FTD updates.

The Product Updates page ([System > Updates](#)) shows the version of each update, as well as the date and time it was generated. It also indicates whether a reboot is required as part of the update. The currently running version of FMC is shown at the top of the Product Updates page. To see the currently running version of each managed FTD, view the list of managed devices ([Devices > Device Management](#)).



When administrator install or uninstall updates from a managed Device, the following capabilities may be affected:

- Traffic inspection and connection logging
- Traffic flow including switching, routing, and related functionality
- Link state

WARNING! *To ensure absolutely no packets pass through the appliance without inspection, please disconnect the managed Devices from the network during the upgrade process. Once the process has been completed and upgrade version has been verified, reconnect the managed Devices to the network.*

Therefore, upgrading and regular maintenance should be performed during off-peak hours only.


6.11.1 To Update the FMC:

Update the FMC in one of two ways, depending on the type of update and whether your FMC has access to the Internet:

- Administrator can use the FMC to obtain the update directly from the Cisco Support Site, if your FMC has constant access to the Internet. This option is not supported for major updates and is not allowed in the evaluated configuration.
 - Administrator can manually download the update from the Cisco Support Site and then upload it to the FMC. Choose this option if your FMC does not have access to the Internet or if you are performing a major update.
1. Login with Administrator Role.
 2. Upload the update to the FMC. You have two options, depending on the type of update and whether your FMC has access to the Internet:
 - For all except major updates, and if your FMC has access to the Internet, select **System > Updates**, then click **Download Updates** to check for the latest updates on the Cisco Support Site (<https://software.cisco.com/>).
 - For major updates, or if your FMC does not have access to the Internet, you must first manually download the update from the Cisco Support Site. Select **System > Updates**, then click **Upload Update**. Browse to the update and click **Upload**.

The update is uploaded to the FMC.

WARNING! Make sure you have a valid Support account. The Cisco Support Site requires authentication and is protected using HTTPS.

3. Make sure that the appliances in your deployment are successfully communicating and that there are no issues being reported by the health monitor.
4. Select System > Updates.
5. Click the install icon () next to the update you uploaded.
6. Select the FMC and click **Install**. If prompted, confirm that you want to install the update and reboot the FMC.
7. After the update finishes, if necessary, log into the FMC.
8. Clear your browser cache and force a reload of the browser. Otherwise, the user interface may exhibit unexpected behavior.
9. Select **Help > About** and confirm that the software version is listed correctly.
10. Re-deploy the access control policies.

6.11.2 To Update Managed Devices:


1. Login with Administrator Role.
2. Download the update from the [Cisco Support Site](#).
3. Make sure that the appliances in your deployment are successfully communicating and that there are no issues being reported by the health monitor.

4. On the managing FMC, select **System > Updates**.

The Product Updates page appears.

5. Click **Upload Update** to browse to the update you downloaded, then click **Upload**.

The update is uploaded to the FMC. The Product Updates tab shows the type of update you just uploaded, its version number, and the date and time when it was generated. The page also indicates whether a reboot is required as part of the update.

6. Click the install icon () next to the update you uploaded.
7. Select the Devices where you want to install the update, then click **Install**; you can update multiple Devices at once if they use the same update. If prompted, confirm that you want to install the update and reboot the Devices.
8. On the FMC, select **Devices > Device Management** and confirm that the Devices you updated have the correct version listed.
9. Verify that the Devices you updated are successfully communicating with the FMC.

Audit Record:

2013-02-27 17:40:07	admin	System > Updates > Product Updates	Update Install	10.4.11.59
-------------------------------------	-----------------------	--	--------------------------------	----------------------------

[Successful task completion : Installing Sourcefire Vulnerability And Fingerprint Database Updates version: VDB-139 : Successful VDB Installation](#)

7 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. If this occurs, please re-boot the appliance. If the product still does not enter operational state, please contact Cisco Support (go to <https://www.cisco.com/go/offices> and click Technical Support).

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

The actual output of FIPS 140-2 self-tests can only be accessed using the shell access⁸ with root permission. The status output is located in `/var/log/openssl-selftest.log` and is displayed below:

```
FIPS-mode test application
AES-NI Enabled: No
CiscoSSL FOM 7.3sp

DRBG AES-256-CTR DF test started
DRBG AES-256-CTR DF test OK

1. Automatic power-up self test...successful
2a. AES encryption/decryption...successful
2b. AES-GCM encryption/decryption...successful
    Pairwise Consistency DH test started
    Pairwise Consistency DH test OK

3a. DH key generation test...successful
3b. ECDH key generation test...successful
    Pairwise Consistency RSA test started
    Pairwise Consistency RSA test OK
    Pairwise Consistency RSA test started
    Pairwise Consistency RSA test OK
    Pairwise Consistency RSA test started
    Pairwise Consistency RSA test OK

4. RSA key generation and encryption/decryption...successful
5. DES-ECB encryption/decryption...successful
    Pairwise Consistency DSA test started
    Pairwise Consistency DSA test OK

6. DSA key generation and signature validation...successful
7a. SHA-1 hash...successful
7b. SHA-256 hash...successful
```

⁸ Accessing the shell access with root access takes the products out of the evaluated configuration.

Cisco FTD 7.0 Preparative Procedures & Operational User Guide for Common Criteria

7c. SHA-512 hash...successful
7d. HMAC-SHA-1 hash...successful
7e. HMAC-SHA-224 hash...successful
7f. HMAC-SHA-256 hash...successful
7g. HMAC-SHA-384 hash...successful
7h. HMAC-SHA-512 hash...successful
7i. SHA3-256 hash...successful
7j. SHA3-512 hash...successful
7k. SHAAKE-128 hash...successful
7l. SHAAKE-256 hash...successful
8a. CMAC-AES-128 hash...successful
8b. CMAC-AES-192 hash...successful
8c. CMAC-AES-256 hash...successful
8e. CMAC-TDEA-3 hash...successful
8f. ECDSA key pairwise consistency check...

Testing ECDSA pairwise consistency

Pairwise Consistency ECDSA test started

Pairwise Consistency ECDSA test OK

ECDSA key generated OK, pairwise test passed.

successful as expected

8g. KBKDF SP800-108 KAT...successful
8h. KDF SNMP KAT...successful
8i. KDF SRTP KAT...successful
8j. KDF SSH KAT...successful
8k. KBF TLS KAT...successful
8l. KDF IKEv2 KAT...successful
8m. KDF PBKDF KAT...successful
8n. KBF TLS KAT...successful
8o. KBF HKDF TWO-STEP KAT...successful
8p. KBF HKDF ONE-STEP KAT...successful
9a. KAS-IFC...successful
9b. KTS_IFC...successful

Pairwise Consistency RSA test started

Pairwise Consistency RSA test OK

Pairwise Consistency RSA test started

Pairwise Consistency RSA test OK

Pairwise Consistency RSA test started

Pairwise Consistency RSA test OK

Generated 383 byte RSA private key

BN key before overwriting:

```
aa890ce32e703caf6d53b62d3886bfb8f60c1ba282f6e4e679fa0491a2205728da52938bcabc93fb76dfab0f435f7ecd070279f6f1
32802fe720c8e7fda8418cc2a6fa7a0b6e3dc6022ad12020622cca5590ec6c0839d1f5264a425ed9d84ef1e9c7da07a4d19475c0bd
e93ba357d545d3fc94f7e6ebd622e34be9f553f118c5a9644356ce1ebb6449c320cceab711053e4fd456b67d82cb714b787297f22
2108dfcce0bc38f002f5db070ca8891da7dc8fa8c1a78c2f507ce4566da544cc418b40f89ff5b8ea3ab53594ab9b902b7a93ad731c2
83093dfcc97a458125b2474bf31bff4680b5d054d95ef07cbcd27a5508350d6b926586f4b2218cc6c395eda308e93db61f6505615
bc6caf4ac6d3bfe04bb21a6049a91e6f9d775617ad9b54a8db8f4894977419ce84b8783ef288cde9ccbf892914b45b83d4318c43b
6548bb2755c1b2836a13f13c7a043fdf850ccb8fce25fdcc6e12c1dca0336c21500c78a7fcff5344e6226694e7d09f84f1d0e52ca16a
2f14851aa64be26f6b01
```

BN key after overwriting:

Cisco FTD 7.0 Preparative Procedures & Operational User Guide for Common Criteria

```
73f21b6209a7a3fb9527bf4df4f316f1ed170dd1e002b6c5cbe5a7bf9f3242d45dfbb5c97deb5f1a85a77a1e05c0d066b16c83f466e
11d42274006832ecff54b4a20c05f8ecc9b403c48c13ea097bdc2adf1279e49d784eada8df81758d63364aa7a8dbb1e8aaaa8d7747
bc906131ca309434a54a02e82e97576fbeat26e117febf3fa5247af7585a83292865dca4e1eeb466bb748c6f61a24697002c39139d
dad8b1b60206e5ade282887273c96a27bc9523fe3c8cb4db3a8132e176816c17999c9d827dc5f4a792c440261c8e77c0700dc4a44
14ebc09f2c8cda728f39b18e291f3e235b295217a97e0718ff07c59cc49361ec09fa3a531cef7c45ce570d566bd0b8bbaf2fb464659f
709a483cde64a29c61305ad2c3112dc539096357596dcde08567b750b48e57bc40a567fc464149161281e3708c6e0aeb10a71a40
30b6fd275d1d368ddc29b939c9eea4e8c87a3119c132ab43e5ce28da41cde6d12aba66bc43a489134f7d23078b28dceef72cfe9e4
ab941481d9c3fc22d95387b6b
```

char buffer key before overwriting:

```
4850f0a33aedd3af6e477f8302b10968
```

char buffer key after overwriting:

```
3ebe286315eedc05f99bc412b19ba1da
```

10. Zero-ization...

successful as expected

11. Complete DRBG health check...

DRBG AES-128-CTR DF test started

DRBG AES-128-CTR DF test OK

DRBG AES-192-CTR DF test started

DRBG AES-192-CTR DF test OK

DRBG AES-256-CTR DF test started

DRBG AES-256-CTR DF test OK

DRBG AES-128-CTR test started

DRBG AES-128-CTR test OK

DRBG AES-192-CTR test started

DRBG AES-192-CTR test OK

DRBG AES-256-CTR test started

DRBG AES-256-CTR test OK

DRBG SHA1 test started

DRBG SHA1 test OK

DRBG SHA224 test started

DRBG SHA224 test OK

DRBG SHA256 test started

DRBG SHA256 test OK

DRBG SHA384 test started

DRBG SHA384 test OK

DRBG SHA512 test started

DRBG SHA512 test OK

DRBG HMAC-SHA1 test started

DRBG HMAC-SHA1 test OK

DRBG HMAC-SHA224 test started

DRBG HMAC-SHA224 test OK

DRBG HMAC-SHA256 test started

DRBG HMAC-SHA256 test OK

DRBG HMAC-SHA384 test started

DRBG HMAC-SHA384 test OK

DRBG HMAC-SHA512 test started

DRBG HMAC-SHA512 test OK

successful as expected

12. DRBG generation check...

DRBG SHA1 test started
DRBG SHA1 test OK
DRBG SHA1 test started
DRBG SHA1 test OK
DRBG SHA1 test started
DRBG SHA1 test OK
DRBG SHA1 test started
DRBG SHA1 test OK
DRBG SHA1 test started
DRBG SHA1 test OK
DRBG SHA1 test started
DRBG SHA1 test OK
DRBG SHA1 test started
DRBG SHA1 test OK
DRBG SHA1 test started
DRBG SHA1 test OK
DRBG SHA224 test started
DRBG SHA224 test OK
DRBG SHA224 test started
DRBG SHA224 test OK
DRBG SHA224 test started
DRBG SHA224 test OK
DRBG SHA224 test started
DRBG SHA224 test OK
DRBG SHA224 test started
DRBG SHA224 test OK
DRBG SHA224 test started
DRBG SHA224 test OK
DRBG SHA224 test started
DRBG SHA224 test OK
DRBG SHA224 test started
DRBG SHA224 test OK
DRBG SHA224 test started
DRBG SHA224 test OK
DRBG SHA256 test started
DRBG SHA256 test OK
DRBG SHA256 test started
DRBG SHA256 test OK
DRBG SHA256 test started
DRBG SHA256 test OK
DRBG SHA256 test started
DRBG SHA256 test OK
DRBG SHA256 test started
DRBG SHA256 test OK
DRBG SHA256 test started
DRBG SHA256 test OK
DRBG SHA256 test started
DRBG SHA256 test OK
DRBG SHA256 test started
DRBG SHA256 test OK
DRBG SHA256 test started
DRBG SHA256 test OK
DRBG SHA384 test started
DRBG SHA384 test OK
DRBG SHA384 test started
DRBG SHA384 test OK

DRBG SHA384 test started
DRBG SHA384 test OK
DRBG SHA384 test started
DRBG SHA384 test OK
DRBG SHA384 test started
DRBG SHA384 test OK
DRBG SHA384 test started
DRBG SHA384 test OK
DRBG SHA384 test started
DRBG SHA384 test OK
DRBG SHA512 test started
DRBG SHA512 test OK
DRBG SHA512 test started
DRBG SHA512 test OK
DRBG SHA512 test started
DRBG SHA512 test OK
DRBG SHA512 test started
DRBG SHA512 test OK
DRBG SHA512 test started
DRBG SHA512 test OK
DRBG SHA512 test started
DRBG SHA512 test OK
DRBG SHA512 test started
DRBG SHA512 test OK
DRBG SHA512 test started
DRBG SHA512 test OK
DRBG HMAC-SHA1 test started
DRBG HMAC-SHA1 test OK
DRBG HMAC-SHA1 test started
DRBG HMAC-SHA1 test OK
DRBG HMAC-SHA1 test started
DRBG HMAC-SHA1 test OK
DRBG HMAC-SHA1 test started
DRBG HMAC-SHA1 test OK
DRBG HMAC-SHA1 test started
DRBG HMAC-SHA1 test OK
DRBG HMAC-SHA1 test started
DRBG HMAC-SHA1 test OK
DRBG HMAC-SHA1 test started
DRBG HMAC-SHA1 test OK
DRBG HMAC-SHA1 test started
DRBG HMAC-SHA1 test OK
DRBG HMAC-SHA224 test started
DRBG HMAC-SHA224 test OK
DRBG HMAC-SHA224 test started
DRBG HMAC-SHA224 test OK
DRBG HMAC-SHA224 test started
DRBG HMAC-SHA224 test OK
DRBG HMAC-SHA224 test started
DRBG HMAC-SHA224 test OK
DRBG HMAC-SHA224 test started
DRBG HMAC-SHA224 test OK

DRBG HMAC-SHA224 test started
DRBG HMAC-SHA224 test OK
DRBG HMAC-SHA224 test started
DRBG HMAC-SHA224 test OK
DRBG HMAC-SHA224 test started
DRBG HMAC-SHA224 test OK
DRBG HMAC-SHA256 test started
DRBG HMAC-SHA256 test OK
DRBG HMAC-SHA256 test started
DRBG HMAC-SHA256 test OK
DRBG HMAC-SHA256 test started
DRBG HMAC-SHA256 test OK
DRBG HMAC-SHA256 test started
DRBG HMAC-SHA256 test OK
DRBG HMAC-SHA256 test started
DRBG HMAC-SHA256 test OK
DRBG HMAC-SHA256 test started
DRBG HMAC-SHA256 test OK
DRBG HMAC-SHA256 test started
DRBG HMAC-SHA256 test OK
DRBG HMAC-SHA256 test started
DRBG HMAC-SHA256 test OK
DRBG HMAC-SHA256 test started
DRBG HMAC-SHA256 test OK
DRBG HMAC-SHA384 test started
DRBG HMAC-SHA384 test OK
DRBG HMAC-SHA384 test started
DRBG HMAC-SHA384 test OK
DRBG HMAC-SHA384 test started
DRBG HMAC-SHA384 test OK
DRBG HMAC-SHA384 test started
DRBG HMAC-SHA384 test OK
DRBG HMAC-SHA384 test started
DRBG HMAC-SHA384 test OK
DRBG HMAC-SHA384 test started
DRBG HMAC-SHA384 test OK
DRBG HMAC-SHA384 test started
DRBG HMAC-SHA384 test OK
DRBG HMAC-SHA384 test started
DRBG HMAC-SHA384 test OK
DRBG HMAC-SHA512 test started
DRBG HMAC-SHA512 test OK
DRBG HMAC-SHA512 test started
DRBG HMAC-SHA512 test OK
DRBG HMAC-SHA512 test started
DRBG HMAC-SHA512 test OK
DRBG HMAC-SHA512 test started
DRBG HMAC-SHA512 test OK
DRBG HMAC-SHA512 test started
DRBG HMAC-SHA512 test OK
DRBG HMAC-SHA512 test started
DRBG HMAC-SHA512 test OK
DRBG HMAC-SHA512 test started
DRBG HMAC-SHA512 test OK

DRBG HMAC-SHA512 test started
DRBG HMAC-SHA512 test OK
DRBG AES-128-CTR test started
DRBG AES-128-CTR test OK
DRBG AES-128-CTR test started
DRBG AES-128-CTR test OK
DRBG AES-128-CTR test started
DRBG AES-128-CTR test OK
DRBG AES-128-CTR test started
DRBG AES-128-CTR test OK
DRBG AES-128-CTR test started
DRBG AES-128-CTR test OK
DRBG AES-128-CTR test started
DRBG AES-128-CTR test OK
DRBG AES-192-CTR test started
DRBG AES-192-CTR test OK
DRBG AES-192-CTR test started
DRBG AES-192-CTR test OK
DRBG AES-192-CTR test started
DRBG AES-192-CTR test OK
DRBG AES-192-CTR test started
DRBG AES-192-CTR test OK
DRBG AES-192-CTR test started
DRBG AES-192-CTR test OK
DRBG AES-192-CTR test started
DRBG AES-192-CTR test OK
DRBG AES-192-CTR test started
DRBG AES-192-CTR test OK
DRBG AES-192-CTR test started
DRBG AES-192-CTR test OK
DRBG AES-256-CTR test started
DRBG AES-256-CTR test OK
DRBG AES-256-CTR test started
DRBG AES-256-CTR test OK
DRBG AES-256-CTR test started
DRBG AES-256-CTR test OK
DRBG AES-256-CTR test started
DRBG AES-256-CTR test OK
DRBG AES-256-CTR test started
DRBG AES-256-CTR test OK
DRBG AES-256-CTR test started
DRBG AES-256-CTR test OK
DRBG AES-256-CTR test started
DRBG AES-256-CTR test OK
DRBG AES-256-CTR test started
DRBG AES-256-CTR test OK
DRBG AES-128-CTR DF test started
DRBG AES-128-CTR DF test OK

DRBG AES-128-CTR DF test started
DRBG AES-128-CTR DF test OK
DRBG AES-128-CTR DF test started
DRBG AES-128-CTR DF test OK
DRBG AES-128-CTR DF test started
DRBG AES-128-CTR DF test OK
DRBG AES-128-CTR DF test started
DRBG AES-128-CTR DF test OK
DRBG AES-128-CTR DF test started
DRBG AES-128-CTR DF test OK
DRBG AES-128-CTR DF test started
DRBG AES-128-CTR DF test OK
DRBG AES-128-CTR DF test started
DRBG AES-128-CTR DF test OK
DRBG AES-192-CTR DF test started
DRBG AES-192-CTR DF test OK
DRBG AES-192-CTR DF test started
DRBG AES-192-CTR DF test OK
DRBG AES-192-CTR DF test started
DRBG AES-192-CTR DF test OK
DRBG AES-192-CTR DF test started
DRBG AES-192-CTR DF test OK
DRBG AES-192-CTR DF test started
DRBG AES-192-CTR DF test OK
DRBG AES-192-CTR DF test started
DRBG AES-192-CTR DF test OK
DRBG AES-192-CTR DF test started
DRBG AES-192-CTR DF test OK
DRBG AES-192-CTR DF test started
DRBG AES-192-CTR DF test OK
DRBG AES-192-CTR DF test started
DRBG AES-192-CTR DF test OK
DRBG AES-256-CTR DF test started
DRBG AES-256-CTR DF test OK
DRBG AES-256-CTR DF test started
DRBG AES-256-CTR DF test OK
DRBG AES-256-CTR DF test started
DRBG AES-256-CTR DF test OK
DRBG AES-256-CTR DF test started
DRBG AES-256-CTR DF test OK
DRBG AES-256-CTR DF test started
DRBG AES-256-CTR DF test OK
DRBG AES-256-CTR DF test started
DRBG AES-256-CTR DF test OK
DRBG AES-256-CTR DF test started
DRBG AES-256-CTR DF test OK
DRBG AES-256-CTR DF test started
DRBG AES-256-CTR DF test OK

successful as expected

13. Induced test failure check...

Testing induced failure of Integrity test

POST started

Integrity test failure induced

Integrity test failed as expected

Cisco FTD 7.0 Preparative Procedures & Operational User Guide for Common Criteria

POST Failed
Testing induced failure of AES-DEC test
POST started
Cipher AES-128-ECB test failure induced
Cipher AES-128-ECB test failed as expected

POST Failed
Testing induced failure of AES-ENC test
POST started
Cipher AES-128-ECB test failure induced
Cipher AES-128-ECB test failed as expected

POST Failed
Testing induced failure of DES3 test
POST started
Cipher DES-EDE3-ECB test failure induced
Cipher DES-EDE3-ECB test failed as expected

POST Failed
Testing induced failure of AES-GCM-DEC test
POST started
GCM test failure induced
GCM test failed as expected

POST Failed
Testing induced failure of AES-GCM-ENC test
POST started
GCM test failure induced
GCM test failed as expected

POST Failed
Testing induced failure of AES-CCM test
POST started
CCM test failure induced
CCM test failed as expected

POST Failed
Testing induced failure of AES-XTS test
POST started
XTS AES-128-XTS test failure induced
XTS AES-128-XTS test failed as expected
XTS AES-256-XTS test failure induced
XTS AES-256-XTS test failed as expected

POST Failed
Testing induced failure of Digest test
POST started
Digest SHA1 test failure induced
Digest SHA1 test failed as expected
Digest SHA1 test failure induced
Digest SHA1 test failed as expected
Digest SHA1 test failure induced
Digest SHA1 test failed as expected

Cisco FTD 7.0 Preparative Procedures & Operational User Guide for Common Criteria

POST Failed	
Testing induced failure of Digest test	
POST started	
	Digest SHA3-256 test failure induced
	Digest SHA3-256 test failed as expected
	Digest SHA3-256 test failure induced
	Digest SHA3-256 test failed as expected
	Digest SHA3-256 test failure induced
	Digest SHA3-256 test failed as expected
POST Failed	
Testing induced failure of HMAC test	
POST started	
	HMAC SHA1 test failure induced
	HMAC SHA1 test failed as expected
	HMAC SHA224 test failure induced
	HMAC SHA224 test failed as expected
	HMAC SHA256 test failure induced
	HMAC SHA256 test failed as expected
	HMAC SHA384 test failure induced
	HMAC SHA384 test failed as expected
	HMAC SHA512 test failure induced
	HMAC SHA512 test failed as expected
POST Failed	
Testing induced failure of CMAC test	
POST started	
	CMAC AES-128-CBC test failure induced
	CMAC AES-128-CBC test failed as expected
	CMAC AES-192-CBC test failure induced
	CMAC AES-192-CBC test failed as expected
	CMAC AES-256-CBC test failure induced
	CMAC AES-256-CBC test failed as expected
	CMAC DES-EDE3-CBC test failure induced
	CMAC DES-EDE3-CBC test failed as expected
POST Failed	
Testing induced failure of DH test	
POST started	
	DH test failure induced
	DH test failed as expected
POST Failed	
Testing induced failure of KBKDF test	
POST started	
	KBKDF test failure induced
	KBKDF test failed as expected
POST Failed	
Testing induced failure of KDF_SSH test	
POST started	

Cisco FTD 7.0 Preparative Procedures & Operational User Guide for Common Criteria

	KDF-SSH test failure induced
	KDF-SSH test failed as expected
POST Failed	
Testing induced failure of KDF_SNMP test	
POST started	
	KDF-SNMP test failure induced
	KDF-SNMP test failed as expected
POST Failed	
Testing induced failure of KDF_SRTP test	
POST started	
	KDF-SRTP test failure induced
	KDF-SRTP test failed as expected
POST Failed	
Testing induced failure of KDF_TLS test	
POST started	
	KDF-TLS test failure induced
	KDF-TLS test failed as expected
POST Failed	
Testing induced failure of KDF_TLS13 test	
POST started	
	KDF-TLS13 test failure induced
	KDF-TLS13 test failed as expected
POST Failed	
Testing induced failure of KDF_IKEV2 test	
POST started	
	KDF-IKEV2 test failure induced
	KDF-IKEV2 test failed as expected
POST Failed	
Testing induced failure of PBKDF test	
POST started	
	PBKDF test failure induced
	PBKDF test failed as expected
POST Failed	
Testing induced failure of TWO-STEP HKDF test	
POST started	
	TWO-STEP HKDF test failure induced
	TWO-STEP HKDF test failed as expected
POST Failed	
Testing induced failure of ONE-STEP HKDF test	
POST started	
	ONE-STEP HKDF test failure induced
	ONE-STEP HKDF test failed as expected
POST Failed	
Testing induced failure of KTS-IFC test	
POST started	
	KTS-IFC test failure induced

Cisco FTD 7.0 Preparative Procedures & Operational User Guide for Common Criteria

	KTS-IFC test failed as expected
POST Failed	
Testing induced failure of KAS-IFC test	
POST started	
	KAS-IFC test failure induced
	KAS-IFC test failed as expected
POST Failed	
Testing induced failure of DRBG test	
POST started	
	DRBG AES-256-CTR test failure induced
	DRBG AES-256-CTR DF test failed as expected
	DRBG AES-256-CTR test failure induced
	DRBG AES-256-CTR test failed as expected
	DRBG SHA256 test failure induced
	DRBG SHA256 test failed as expected
	DRBG HMAC-SHA256 test failure induced
	DRBG HMAC-SHA256 test failed as expected
POST Failed	
Testing induced failure of RSA-SIGN test	
POST started	
	Signature RSA test failure induced
	Signature RSA test failed as expected
POST Failed	
Testing induced failure of RSA-VERIFY test	
POST started	
	Verify RSA test failure induced
	Verify RSA test failed as expected
POST Failed	
Testing induced failure of DSA-SIGN test	
POST started	
	Signature DSA test failure induced
	Signature DSA test failed as expected
POST Failed	
Testing induced failure of DSA-VERIFY test	
POST started	
	Verify DSA test failure induced
	Verify DSA test failed as expected
POST Failed	
Testing induced failure of ECDSA-SIGN test	
POST started	
	Signature ECDSA P-256 test failure induced
	Signature ECDSA P-256 test failed as expected
POST Failed	
Testing induced failure of ECDSA-VERIFY test	
POST started	
	Verify ECDSA P-256 test failure induced

Verify ECDSA P-256 test failed as expected

POST Failed

Testing induced failure of ECDH test

POST started

ECDH P-256 test failure induced

ECDH P-256 test failed as expected

POST Failed

Testing induced failure of RSA keygen test

POST started

POST Success

Pairwise Consistency RSA test failure induced

Pairwise Consistency RSA test failed as expected

RSA key generation failed as expected.

Testing induced failure of DSA keygen test

POST started

POST Success

Pairwise Consistency DSA test failure induced

Pairwise Consistency DSA test failed as expected

DSA key generation failed as expected.

POST started

POST Success

Testing induced failure of ECDSA keygen test

Pairwise Consistency ECDSA test failure induced

Pairwise Consistency ECDSA test failed as expected

ECDSA key generation failed as expected.

POST started

POST Success

Testing induced failure of DH keygen test

Pairwise Consistency DH test failure induced

Pairwise Consistency DH test failed as expected

DH key generation failed as expected.

POST started

POST Success

Testing induced failure of DRBG CPRNG test

DRBG continuous PRNG failed as expected

POST started

POST Success

Testing induced failure of DRBG entropy CPRNG test

DRBG continuous PRNG entropy failed as expected

POST started

POST Success

Testing operation failure with DRBG entropy failure

DSA key generated OK as expected.

DRBG entropy instantiate fail failed as expected

DRBG entropy generate fail failed as expected

DRBG reseed entropy fail failed as expected

Cisco FTD 7.0 Preparative Procedures & Operational User Guide for Common Criteria

DSA signing failed as expected

ECDSA key generation failed as expected.

Induced failure test completed with 0 errors

successful as expected

All tests completed with 0 errors
