Cisco Secure Network Analytics (SNA) 7.5 Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration

Version 1.0

June 23, 2026

Prepared by:

Cisco Systems, Inc.,

170 West Tasman Drive, San Jose,

CA 95134-1706 USA

Table of Contents

Tables

Figures

1 Introduction

1.1 Audience

The intended audience for this guide includes Network and Security Administrators and other personnel who are responsible for installing and configuring Cisco Secure Network Analytics (SNA) products in accordance with the Common Criteria (CC) evaluated configuration to satisfy the security requirements of the collaborative Protection Profile for Network Devices (NDcPP). 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 Purpose

This document provides guidance for the secure installation and secure use of Cisco Secure Network Analytics (SNA) appliances such that the system deployment will be satisfy the requirements of the Common Criteria (CC) evaluated configuration.

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

1.3 Document References

The Cisco Secure Network Analytics (SNA) documentation set includes online help and PDF files.

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

Table 1: Document References

[SNA-DS] Cisco Secure Network Analytics **Data Sheet** Date: January 10, 2024 *https://www.cisco.com/c/en/us/products/collateral/security/stealthwatch/datasheet-c78-739398.pdf*
[SNA-RN] Cisco Secure Network Analytics **Release Notes** 7.5.2 Document version 1_2, April 25, 2025 *https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/release_notes/7_5_Release_Notes/7_5_2_Release_Notes_DV_1_2.pdf*
[SNA-LG] Cisco Secure Network Analytics Smart Software **Licensing Guide** 7.5 Document version 1.0, February 14, 2025 *https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/license/7_5_2_Smart_Software_Licensing_Guide_DV_1_0.pdf*
[SNA-HIG] Cisco Stealthwatch x3xx Series **Hardware Installation Guide** Document version 1_6, April 28, 2026 https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/x3xx_Hardware_Appliance_Installation_DV_1_6.pdf

[SNA-VEIG] Cisco Secure Network Analytics **Virtual Edition Appliance Installation Guide** 7.5.2 Document version 5_0, September 24, 2025 *https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/7_5_2_VE_Appliance_Installation_Guide_DV_5_0.pdf*
[SNA-UG] Cisco Secure Network Analytics **Update Guide** 7.5.2 Document version 1_1, February 20, 2025 *https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/update_guides/7_5_2_Update_Guide_DV_1_1.pdf*
[SNA-CG] Cisco Secure Network Analytics **System Configuration Guide** 7.5.2 Document version 2_0, May 2, 2025 *https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/7_5_2_System_Configuration_Guide_DV_2_0.pdf*
[SNA-SSL/TLS] Cisco Secure Network Analytics **SSL/TLS Certificates for Managed Appliances** 7.5.2 Document Version: 2_0, May 2, 2025 *https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/certificates/7_5_2_SSL_TLS_Certificates_for_Managed_Appliances_Guide_DV_2_0.pdf*

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

1.4 Hardware, Software, and Functionality

1.4.1 CC-evaluated Hardware and Software

The table below lists the physical and virtual appliances and software within the boundary of the CC-evaluated TOE (Target of Evaluation).

Table 2: SNA Appliances and Software

Component (Appliance)	Hardware Configurations	Software Version
SNA Manager	Any one of: • ST-SMC2300-K9 • L-ST-SMC-VE-K9	7.5
SNA Flow Collector (FC)	Any one or more of: • ST-FC4300-K9 • L-ST-FC-VE-K9	7.5
SNA Flow Sensor (FS)	Any one or more of: • ST-FS1300-K9 • ST-FS3300-K9 • ST-FS4300-K9 • L-ST-FS-VE-K9	7.5

1.4.2 Excluded Functionality

The list below identifies features or protocols that are not evaluated and must remain disabled in the CC-evaluated configuration. These features were not evaluated and/or validated by an independent third party and the functional correctness of the implementation is vendor assertion.

Table 3: Excluded Functionality

Functionality	Description of Excluded Functionality
Non-FIPS 140-3 mode of operation	This mode of operation includes non-FIPS allowed operations.
Admin UI file browser endpoint	Admin UI file browser endpoint is not supported.
Authentication	Only Local Authentication and LDAP (over TLS) are supported for the CC-evaluated configuration.
CSV reports	Comma-Separated Values (CSV) files reports are not available when Security Label is used. **Note:** This includes flow reports.
Integrations with SNA	This functionality is not supported for compliance, including: addons, SNA Apps, Cognitive Intelligence, ISE, Google Analytics, SecureX, SNA Cloud, Data Exporter (DEX)/Flow Forwarder, and Customer Success Metrics.
Internet Proxy	NTLM authentication is not supported when FIPS encryption libraries are enabled.
Packet Analyzer	Use of Packet Analyzer is not supported.
RADIUS and TACACS+, Including creating and authenticating users	RADIUS and TACACS+ are not supported. (LDAP over TLS is supported.)
Manager Failover	Manager Failover, where one Manager serves as a backup to the other, is not supported.
SNA Threat Intelligence Feed	The Threat Intelligence Feed should not be enabled.
SSH	Use of SSH is not permitted in the CC-evaluated configuration.

1.5 Operational Environment

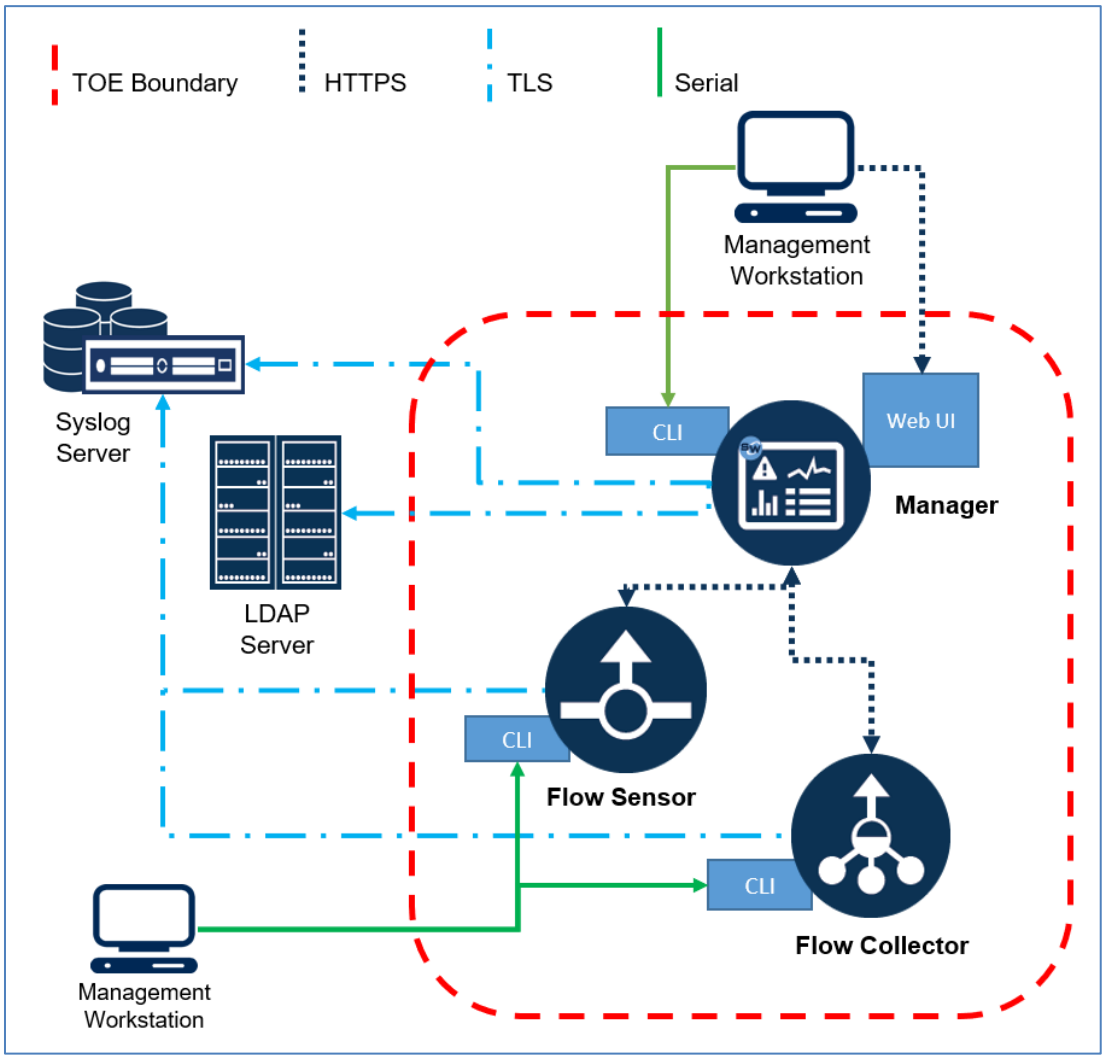
The system can be configured to rely on and utilize a number of other components in its operational environment.

- Management Workstation (required): The system supports Command Line Interface (CLI) and web access. An administrator needs a terminal emulator (to support serial console access), and a web browser (supporting HTTPS) to utilize those administrative interfaces.
- Audit server (required): The system will be configured to deliver audit records to an external log server using syslog over TLS.
- Authentication servers (optional): The system can be configured to utilize external authentication servers (LDAP over TLS).
- Certificate Authority (CA) server (required): The system can be configured to import X.509v3 certificates from a CA (e.g. to allow SNA appliances to authenticate each other, and to allow SNA appliances to validate certificates of syslog servers and LDAP servers).
- NTP server (required): The system can be configured to obtain time from an external trusted time source using NTPv4 with SHA1 authentication.
- DNS server (recommended): The system supports domain name service in the network.

1.6 Sample Network Topology

The diagram below shows sample deployment and network connectivity.

Figure 1: SNA Deployment Example (showing TOE boundary)



Note: The diagram above shows one of each appliance (Manager, FC, and FS), where each appliance can be either physical or virtual.

1.7 Cryptography for FIPS and CC

Use Compliance Mode to enable encryption libraries for the Federal Information Processing Standard (FIPS) and Common Criteria. Each SNA appliance contains two cryptographic modules, the CiscoSSL FIPS Provider Cryptographic Implementation version 8.0 (8.0.221), and the Cisco BC Cryptographic Implementation version 2.0.0.

1.7.1 FIPS

In the United States, FIPS defines and provides security and interoperability requirements for computer systems that are used by the following:

- Federal government agencies.
- Federal contractors.
- Organizations that process information using a computer or telecommunications system on behalf of the federal government to accomplish a federal function.

When you enable FIPS Encryption Libraries, the appliance is configured with FIPS compliant algorithms and requirements, including the following:

- The Bouncy Castle crypto library restricts the cipher suites that can be used by Java. This affects all JVM-based components of the appliance. (Note: Bouncy Castle is used for the LDAP-over-TLS connection.)
- The CiscoSSH client and sshd, the OpenSSH server process, are configured to run with a restricted set of cipher suites. (Note: SSH is disabled in the evaluated configuration.)
- Nginx is configured to run with a restricted set of cipher suites.
- SNA checks the appliance for user passwords hashed with MD5. You cannot enable FIPS encryption libraries on the appliance if they are detected.

IMPORTANT: Make sure you enable FIPS Encryption Libraries on every appliance in the system so they can communicate. By default, SNA disables FIPS Encryption Libraries.

1.7.2 Common Criteria

Common Criteria is used with FIPS; it is an international standard for computer security certification. Refer to ISO/IEC 15408 for details.

When you enable Common Criteria Encryption Libraries, the appliance is configured with Common Criteria compliant algorithms and requirements described in the following lists. There are no further configuration options available to restrict ciphersuites or algorithms listed below.

NOTE: SSH is to remain disabled on all appliances for them to remain in the evaluated Common Criteria configuration.

When FIPS and CC modes are enabled, TLS will use the following ciphersuites and signature algorithms.

- TLS client ciphersuites for TLS 1.2:
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS client ciphersuites for TLS 1.3:
  - TLS_AES_128_GCM_SHA256
  - TLS_AES_256_GCM_SHA384
  - TLS_AES_128_CCM_SHA256
- TLS clients present signature_algorithms extension with support for these algorithms:
  - rsa_pkcs1 with sha256(0x0401)
  - rsa_pkcs1 with sha384(0x0501)
  - rsa_pkcs1 with sha512(0x0601)
  - ecdsa_secp256r1 with sha256(0x0403)
  - ecdsa_secp384r1 with sha384(0x0503)
  - ecdsa_secp521r1 with sha512(0x0603)
  - rsa_pss_rsae with sha256(0x0804)

    - rsa_pss_rsae with sha384(0x0805)
    - rsa_pss_rsae with sha512(0x0806)
    - rsa_pss_pss with sha256(0x0809)
    - rsa_pss_pss with sha384(0x080a)
    - rsa_pss_pss with sha512(0x080b)
- TLS server ciphersuites:
    - TLS_ECDHE_RSA_AES_128_GCM_SHA256
    - TLS_ECDHE_RSA_AES_256_GCM_SHA384
    - TLS_AES_128_GCM_SHA256
    - TLS_AES_256_GCM_SHA384
    - TLS_AES_128_CCM_SHA256
- TLS server signature algorithms:
    - rsa_pkcs1 with sha256(0x0401)
    - rsa_pkcs1 with sha384(0x0501)
    - rsa_pkcs1 with sha512(0x0601)
    - ecdsa_secp256r1 with sha256(0x0403)
    - ecdsa_secp384r1 with sha384(0x0503)
    - ecdsa_secp521r1 with sha512(0x0603)
    - rsa_pss_rsae with sha256(0x0804)
    - rsa_pss_rsae with sha384(0x0805)
    - rsa_pss_rsae with sha512(0x0806)
    - rsa_pss_pss with sha256(0x0809)
    - rsa_pss_pss with sha384(0x080a)
    - rsa_pss_pss with sha512(0x080b)

When FIPS and CC modes are enabled, the following constraints are enforced for TLS:

- For all TLS functionality, only TLSv1.2 and TLSv1.3 are supported, and all other versions are rejected.
- For TLS functionality, the supported cipher suites include ECDHE_ECDSA and ECDHE_RSA AES-GCM suites for TLS 1.2 clients; AES-GCM and AES-CCM suites for TLS 1.3 clients; ECDHE_RSA AES-GCM suites for TLS 1.2 servers; and AES-GCM and AES-CCM suites for TLS 1.3 servers. Supported TLS signature algorithms include RSA PKCS#1, RSA-PSS RSAE, RSA-PSS PSS, and ECDSA using secp256r1, secp384r1, and secp521r1 with SHA-256, SHA-384, and SHA-512.
- TLS client supported groups (Supported Elliptic Curves Extension) for syslog-over-TLS and LDAP-over-TLS are: secp256r1, secp384r1, secp521r1, ffdhe3072, ffdhe4096. TLS client supported groups (Supported Elliptic Curves Extension) for inter-appliance connections are: secp256r1, secp384r1, secp521r1, ffdhe2048, ffdhe3072, ffdhe4096. The supported groups listed here are presented in the Client Hello by default. This behavior is not configurable.
- TLS server supported groups (Supported Elliptic Curves Extension) for remote administration and inter-appliance communication are: secp256r1, secp384r1, secp521r1, ffdhe2048, ffdhe3072, and ffdhe4096.
- TLS session resumption/renegotiation behavior is not configurable. The WebUI supports session resumption based on session tickets (per RFC 5077), the inter-appliance connections support session resumption (using session IDs per RFC 5246 for TLSv1.2, and per RFC 8446 for TLSv1.3). Pre-shared keys (PSKs) are used only within TLS 1.3 session resumption with forward secrecy. Out-of-band provisioning of PSKs is not supported or permitted.

- The security events log level for a variety of security events is modified, including when a management channel is created or deleted.

When you enable Common Criteria Encryption Libraries, the appliance is configured with Common Criteria compliant algorithms and requirements, including the following:

- The Bouncy Castle crypto library is configured to comply with Common Criteria and FIPS 140-3 standards. This affects all JVM-based components of the SNA appliance. The Bouncy Castle implementation deprecates insecure algorithms, including MD5 hashing, and attempts to use these deprecated algorithms may generate errors in log files.
- The cryptographic libraries (CiscoSSL and Bouncy Castle) perform mandatory startup self-tests as required by FIPS 140-3. If any of these self-tests fail, the appliance will fail to boot completely, and all TLS-dependent processes (both TLS server and TLS client) will remain inactive.
    - If the failure occurs on the Manager appliance, the Web UI will remain disabled.
    - If the failure occurs on any other appliance, its status will be reported as a communication failure in Central Management.
    - On the appliance experiencing the failure, administrators should log in through the console to troubleshoot the issue and then contact Cisco Support for assistance.

2 Secure Acceptance of the TOE

The following steps must be performed to confirm that the correct TOE is received:

1) For physical appliances:
   a) Before unpacking any physical components of the TOE, inspect the physical packaging the equipment was delivered in. Verify that the external cardboard packing is printed with the Cisco Systems, Inc. logo and motifs. If it is not, contact the supplier of the equipment (Cisco Systems, Inc. or an authorized Cisco distributor/partner).
   b) Verify that the packaging tape has not been opened and resealed. If the package appears to have been resealed, contact the supplier of the equipment (Cisco Systems, Inc. or an authorized Cisco distributor/partner).
   c) Verify that a white tamper-resistant, tamper-evident Cisco Systems, Inc. bar coded label is applied to the external cardboard box. This label provides information regarding contents of the box, including product number and serial number. If the label is not applied, contact the supplier of the equipment (Cisco Systems, Inc. or an authorized Cisco distributor/partner).
   d) Verify the serial number of the TOE provided on the separately mailed invoice matches the serial number on the shipping documentation and the white label affixed to the outside of the box. If the serial numbers do not match, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).
   e) Verify that the box was shipped from the expected equipment supplier (Cisco Systems, Inc. or an authorized Cisco distributor/partner). This can be done by verifying with the supplier that they shipped the box with the courier company that delivered the box and that the consignment number for the shipment, matches that used on the delivery. Verification of the courier should be performed by a mechanism that does not involve the equipment delivery, such as verification of the phone/FAX number or other online tracking service.
   f) Once the TOE is unpacked, inspect the unit. Verify that the serial number displayed on the unit matches the serial number on the shipping documentation and invoice. If the serial numbers do not match, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).
2) Download the evaluated version of the CC software image from Cisco.com (https://software.cisco.com). NOTE: The physical appliances ship from Cisco with a software image pre-installed; however, this may not be the CC-evaluated version so updating the software is recommended.
3) Verify that the downloaded software has not been modified or corrupted. Use a hash generation utility to compute a SHA-512 hash. Compare the generated hash with the SHA-512 hash associated with the downloaded file, see Table 4 below for this hash value. If the SHA-512 hashes do not match, contact Cisco Technical Assistance Center (TAC), https://www.cisco.com/c/en/us/support/index.html. If the hash values match, proceed with the installation and configuration of the TOE, section 3 below.
4) Power-on each appliance. Confirm the image loads correctly, all internal power-on self-tests complete successfully, and the cryptographic export warning is displayed.
5) Validate that each appliance is running the CC evaluated version of software by viewing the version via the CLI, or the GUI.
6) Validate and activate the software license [SNA-LG]. The software license determines available functionality. It is assumed the end-user has acquired a permanent license.

Note: A permanent license is recommended as it is valid for the lifetime of the system on which it is installed.

Note: Periodically software updates (bug fixes, including resolution of CVEs) are posted on Cisco.com (https://software.cisco.com) and customers are notified that updates are available (if continuing support was purchased). Follow the above steps to download and verify all software updates.

3 Secure Installation

This section provides guidance for installing and configuring SNA using the SNA x3xx Series Hardware Installation Guide [SNA-HIG], the SNA Virtual Edition (VE) Appliance Installation Guide [SNA-VEIG], and the Secure Network Analytics System Configuration Guide [SNA-CG].

Administrator: We address the administrator in this guide as "you" to lead you directly through the compliance configuration.

3.1 Site Preparation

3.1.1 Physical Preparation

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

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

Before you begin the installation, make sure you have the following components:

Component	Notes
SNA Manager	Physical or virtual appliance.
SNA Flow Collector (FC)	Physical and/or virtual appliance(s).
SNA Flow Sensor (FS)	Physical and/or virtual appliance(s).
LDAP Server	Required for CC. Confirm the LDAP server supports LDAP over TLS.
Syslog Server	Required for CC. Confirm the Syslog server supports Syslog over TLS.
Power Supplies	Refer to the "Power Supply Considerations" in the hardware installation guides.
Network Test Access Port (TAP), Switched Port Analyzer (SPAN), or hubs	Refer to the hardware installation guides for more detail.
Documentation	Listed in the ***Document References*** section of this document.

3.1.2 Network Preparation

For a secure installation, ensure the following considerations are satisfied:

- **Open Ports for Firewalls:** Use the [SNA-HIG] "Communication Ports" section to configure the network firewall in the environment. Confirm the list of required ports are open with unrestricted access.
- **Network Devices:** Configure the TAP, SPAN, or hubs to operate with the Flow Sensor as described in the [SNA-HIG] "Flow Sensor 1300, 3300, 4300" section.

- **Specifications:** For detailed information about each appliance, refer to SNA Specification Sheets available here: https://www.cisco.com/c/en/us/support/security/stealthwatch/products-technical-reference-list.html.
- **Location:** The Manager, FC, and FS do not need to be collocated because they communicate with each other over secure channels (TLS). Likewise, the SNA appliances do not need to be collocated with their syslog servers or LDAP servers because communication between the SNA appliances and those servers also uses TLS.

3.2 Connectivity and Powering On

3.2.1 Console Access

Initial configuration requires use of the console port to configure networking.

- **Physical Appliances:** For details about console ports on all physical appliances, refer to the "Connecting to your Appliance" section of [SNA_HIG].
- **Virtual Appliances:** For console access on all virtual appliances, refer to the "Booting from the ISO" section in [SNA-VEIG], and "Configuring Your Environment Using First Time Setup" sections in [SNA-CG].

3.2.2 First Time Setup and System Administration

To ensure appliances are properly configured for local and remote/network access complete the following steps.

- **Connecting to the Network:** Refer to the "Connecting Your Appliances to the Network" section in [SNA-HIG] for more information.
- **Powering On:** Once you make all network connections, you can power on the appliances.
- **First Time Setup:** For each appliance, follow the instructions in the "Configuring Your Environment Using First Time Setup" section of [SNA-CG], which will include configuring:
    - Setting IP address, subnet mask, and gateway.
    - Setting NTP and DNS servers.
    - Changing the sysadmin and admin passwords from their defaults.
- **System administration:** Once the first-time setup procedures have been completed, subsequent administration activities via WebUI. To login to the WebUI follow instructions in the "Central Management (Managing your Appliances)" section of [SNA-CG].

3.2.3 Adding Appliances / Joining Appliances to the SNA Manager

After you connect each appliance to the network, configure each appliance using the Appliance Setup Tool. Follow instructions in the "Appliance Configuration Requirement" and "Configuring your Appliances" sections in [SNA-CG] to configure the DNS server and NTP server for each appliance, and to connect each new managed appliance to the Manager.

Adding an appliance cannot be initiated by the Manager, it must be initiated by the administrator performing the initial configuration of the Flow Collectors, and/or Flow Sensors. You will need the Manager administrator credentials to register your appliances with Central Management.

- Flow Collectors: When you set up a Flow Collector, you will enter the Manager administrator credentials and the flow collection port number for NetFlow or sFlow.
- Flow Sensors: When you set up a Flow Sensor, you will select a Flow Collector in your configuration and enter the Manager administrator credentials. After you complete the Appliance Setup Tool for all appliances, configure the Application ID and Payload on the Flow Sensor.

During the initial TLS session, the Manager and the new appliance exchange their unique X.509v3 certificates. Once the certificates have been exchanged, the new appliance has been joined with the Manager. All subsequent (automated) communications between the Manager and managed appliances use TLS with X.509v3 certificates for authentication.

When adding appliances, follow the instructions provided in the “Configure the Appliances in Order" section in the [SNA-CG].

Make sure you:

- configure the Manager (via “Central Management” in the WebUI) first,
- configure one appliance at a time in the correct order, and
- confirm the appliance status displays as **Connected** in Central Management before you configure the next appliance.

Set up your appliances so they are managed by the Manager. During the initial configuration process, specify that the new appliance will be managed by the Manager, and then provide the following:

- the IP address or hostname of the Manager
- a valid Manager administrator username and password to authenticate to the Manager

If you are unable to add appliances to the Manager, the connection could have failed due to the following:

- a network connectivity error - Make sure you reestablish a network connection, and then continue adding appliances.
- incorrect information provided - Make sure you have the correct information (such as the IP address or hostname of the Manager, etc.), and then continue adding appliances.

For further information about adding appliances to the Manager, refer to the “Adding an Appliance to Central Management” section of [SNA-CG].

3.2.4 Connection Recovery

If a connection fails between the Manager and the managed appliances, the connections will automatically retry and restore connectivity. No additional action is required from the SNA administrator other than to restore network connectivity within the operational environment. Connections will always be temporarily unavailable when appliances are rebooting.

3.2.5 Updating Software and Firmware

SNA Software Updates

All appliances (physical and virtual) start with 7.5.2-20250121.1527 installed from one of these installation images:

- **SMC**-7.5.2-20250121.1527-833bbd1d6ff3-0.iso

- **FlowCollector**-NetFlow-7.5.2-20250121.1527-833bbd1d6ff3-0.iso
- **FlowSensor**-7.5.2-20250121.1527-833bbd1d6ff3-0.iso

Once all appliances are joined to the Manager, use the Manager WebUI (Central Management > Update Manager) to update each appliance (starting with the Manager itself) to 7.5.2 using one of these update files:

- **update-smc**-ROLLUP20260214-7.5.2-v2-01.swu
- **update-fcnf**-ROLLUP20260214-7.5.2-v2-01.swu
- **update-fsuf**-ROLLUP20260214-7.5.2-v2-01.swu

UCS Server Firmware Updates

Whether using SNA hardware appliances (e.g. SMC2300, etc.) or SNA virtual appliances, all the underlying hardware platforms are Cisco UCS servers. This firmware does not implement any of the security functionality covered by the Common Criteria evaluation, but ensuring the UCS hardware is running current firmware will avoid potential issues with system stability.

For physical appliances, ensure firmware (including CIMC, BIOS, and drivers) is updated on each appliance (using the same update procedures as for the ROLLUP), and will result in the CIMC running firmware 4.3(2.240009):

- patch-common-SNA-**FIRMWARE**-20240305-v2-01.swu

For virtual appliances, ensure the Cisco UCS host is upgraded to the same version above or newer, e.g.:

- **ucs**-c225m6-huu-4.3.2.240009.iso

3.3 Configuration for Common Criteria Compliance

To configure SNA for CC compliance, complete the following activities (described in 4 Secure Configuration of this document) in the order shown in this list. Make sure you follow the instructions in each section based on your compliance requirements.

1. Configure **Certificates**
2. Enable **Compliance Mode (FIPS and Common Criteria)**
3. Configure **LDAP**
4. Configure **Audit Log Destination**
5. Enable **AIDE**
6. Configure **Login Banners**
7. Configure **Protected Sessions Time-Out**
8. Define the **Password Policy**
9. Configure **Session Settings (Account Lockout)**
10. Disable **External Services**
11. Configure **NTP**

12. Configure **Local Authentication**
13. **Apply Settings**

> **Note:** We are starting this compliance configuration in maintenance mode. You will configure every appliance in your SNA system. This includes installing compliant certificates, changing and enabling configuration settings, and rebooting. During these changes, the system will be unavailable, and you can experience network connection problems. It is important to configure SNA for compliance at a time that will cause the least amount of disruption.

3.4 Making Changes Once in the CC-Evaluated Configuration

3.4.1 Changing Network Configurations

Any changes to the network configuration, including changing the hostname, the domain name, the IP Address, subnet, default gateway, etc. will result in the appliance regenerating its identity cert which will likely result in loss of communication with other SNA appliances. Before making such changes, following the instructions mentioned in section 3.4.2 (Removing or Re-Adding Appliances) to remove the appliance from Central Management, then reference these additional instructions as necessary:

- Changing the Host Name: Follow the instructions in the SNA Online Help, "Host Naming" section, or refer to “Changing the Host Name or Network Domain Name” in [SNA-SSL/TLS].
- Changing the Network Domain Name: Follow the instructions in the SNA Online Help, "Network Interfaces" section, or refer to “Changing the Host Name or Network Domain Name” in [SNA-SSL/TLS].
- To change the IP address, follow the instructions in the SNA Online Help, "Network Interfaces" section, or refer to “Changing the Appliance IP Address” in [SNA-SSL/TLS].

Note: The SystemConfig utility allows changing networking modes (e.g. between ipv4-only, ipv6-only, and dual stack). Changing the network mode while operating appliances in CC mode risks communication outages in certain scenarios. Specifically, if the change introduces a new appliance IP address (e.g. going to dual stack or switching between the two "ipvx-only" options), but the appliance identity certificates in use don't have the new IP address, the host identity checks will start failing and cause communication outages. To avoid this situation, a warning screen is displayed during the network mode change (if the appliance is in CC mode) that warns of potential connectivity breakage. If needing to proceed with such a change, ensure all appliances identity certificates already have all relevant SANs (FQDN + IP address) before making the switch or take all appliances out of CC mode, change the network mode and certs, and then re-enable CC mode.

3.4.2 Removing or Re-Adding Appliances

Follow instructions in the “Removing an Appliance from Central Management” section of [SNA-CG]. After an appliance is removed, no further data will be exchanged between the appliances without completing a new registration process.

After adding or re-adding appliances to the Central Management, complete the instructions in this SNA CC Configuration Guide to reconfigure your SNA appliances for CC compliance. Make sure you configure all the items listed in **Configuration for Common Criteria Compliance**.

4 Secure Configuration

To configure the settings described in this section, first follow these steps to navigate to the pages within Central Management:

1. Login to the SNA Manager.
2. Click the **Configure** tab.
3. Under **Global Settings**, select **Central Management**.
4. On the **Inventory** page, click the **Ellipsis** icon in the **Actions** column for the appliance.
5. Select Edit Appliance Configuration.
6. See additional instructions in the sub-sections below.

4.1 Certificates

Each SNA appliance is installed with a unique, self-signed appliance identity certificate. For compliance, replace the Cisco default certificate with a new, compliant appliance identity certificate on every appliance in your SNA cluster.

The communication of the appliances in your SNA cluster is authenticated using x.509v3 certificates.

Certificate Overview

- **Appliance Identity Certificates**: You can manage the appliance identity certificate in Central Management by selecting the **Inventory** tab, clicking the **Ellipsis** icon in the **Actions** column, and then selecting **Edit Appliance Configuration** to get to the Appliance Configuration page.
    - On the Appliance Configuration page for the appliance, locate the **SSL/TLS Appliance Identity** section, which allows you to view the current certificate, generate a CSR, and replace the appliance identity certificate.
- **Trust Stores**: You can manage the Trust Store certificates for the selected appliance in Central Management by selecting the **Inventory** tab, clicking the **Ellipsis** icon in the **Actions** column, and then selecting **Edit Appliance Configuration** to get to the Appliance Configuration page.
    - From the Appliance Configuration page, select the **General** tab and locate the **Trust Stores** section, where you can add or delete certificates for the appliance's Trust Store.
- **New Certificates**: When you replace an appliance identity certificate, the data related to the old certificate and appliance identity is destroyed automatically. For details, refer to **Resetting Factory Defaults (RFD)**.

Best Practices

- **Review Procedures:** Before you get started, review the procedures in **Certificates** to understand the certificates requirements and instructions. It is a detailed process that must be done correctly for your system to work.
- **Friendly Names:** These procedures include naming new certificates. Make sure each certificate name is unique. Do not duplicate any certificate names in your cluster.
- **Connected:** After you apply settings, review the **Central Management** > **Inventory** page. Make sure the Appliance Status displays as **Connected** before you edit the next appliance configuration.

4.1.1 Review Appliance Identity Certificate Requirements

In the next procedure, you can choose to generate a Certificate Signing Request (CSR) in Central Management or skip the CSR if you already have certificates from a Certificate Authority. Make sure you review the certificate requirements before you proceed.

Make sure each appliance identity certificate meets the requirements shown in the table below and that the Common Name and/or Subject Alternative Name matches the FQDN for identity certificates.

Important: If certificates do not meet the requirements described in the table below, the SNA appliances may loose connectivity with each other or may need to be reinstalled or returned to factory defaults (RFD) and reconfigured.

Table 4: Appliance Identity Certificate Requirements

Requirement	Details
Signed by Certificate Authority (CA)	Make sure the appliance identity certificate is signed by a Certificate Authority (the CA certs will be installed to trust store of each SNA appliance). Self-signed certificates are not compliant.
Certificate Chain Length (2 or more)	The certificate chain length must be at least 2: • Root (1 root) • Intermediate (0 or more intermediaries)
Extension: Basic Constraints	Target certificate (appliance identity certificate): CA set to No/False Each appliance identity certificate must include the X509v3 Basic Constraints field and that field must contain: CA:FALSE Chain certificate (root and intermediaries): CA set to Yes/True Each CA certificate in the PKI chain must include the X509v3 Basic Constraints field and that field must contain: CA:TRUE
Extended Key Usage	Make sure the appliance identity certificate can be used as a client (clientAuth) and server (serverAuth) identity certificate. If you use the SNA CSR procedure, the CSR includes this information.
Format	PEM (.cer, .crt, .pem) or PKCS#12 (.p12, .pfx, .pks)

IPv4 Address and/or IPv6 Address as a Subject Alternative Name Field	Make sure the appliance identity certificate includes the appliance IP address as one of the Subject Alternative Names (SAN).
Host Name as a Subject Alternative Name Field	Make sure the appliance identity certificate includes the appliance host name as one of the Subject Alternative Names. This should be a fully qualified domain name.
RSA Key Length	We only support RSA keys; make sure the key length of all certs (appliance identity certs and CA certs) is 4096 bits.
Date Range	Make sure the certificate dates are current and not expired.

Note: Whether you generate the CSR in Central Management or skip the CSR, make sure each appliance identity certificate meets the requirements shown in this table.

4.1.2 Generate Certificate Signing Requests

Use the following instructions to prepare the Certificate Signing Request (CSR).

Note: If you do not need to generate a CSR, skip this section and go to **Add Certificates to the Trust Stores.**

1. Open Central Management.
2. On the Inventory page, click the Ellipsis icon in the Actions column for the appliance.
3. Select Edit Appliance Configuration.
4. Locate the SSL/TLS Appliance Identity section.
5. Click Update Identity.
6. Do you need to generate a CSR (Certificate Signing Request)? Select Yes. Click Next.
7. Select a compliant RSA Key Length that is supported by your Certificate Authority.

Note: Make sure you replace the default RSA 8192 bit self-signed identity certificate with the RSA 4096 bit CA-signed identity certificate.

8. Complete the fields (optional) in the Generate a CSR section:
   - Organization
   - Organizational Unit
   - Locality or City
   - State or Province
   - Country Code
   - Email Address
9. Click Generate a CSR. The generation process can take several minutes.

Note: If you click **Cancel** after you generate a CSR, or anytime while you are waiting for the CA certificate, the canceled CSR will be invalid. Generate a new CSR in this case.

10. Click Download CSR.
11. Repeat Steps 1 through 10 for every appliance to generate the CSR.
12. Provide the downloaded CSRs to the same Certification Authority.

4.1.3 Add Certificates to the Trust Stores

Use the following instructions to add the appliance identity certificate and certificate chain (root and intermediate) to the appliance Trust Stores. These steps will result in ***adding*** additional trusted certificates (appliance certs and CA certs) to each appliance's trust store so that each appliance can explicitly trust the new certs of other appliances ***before*** each appliance starts identifying itself to other appliances using its new certificate.

Configuration Order: Make sure you follow the selection order in these instructions to update the Trust Stores of your managed appliances before you update the Manager Trust Store.

1. Open **Central Management.**
2. On the **Inventory** page, click the **Ellipsis** icon in the **Actions** column for the appliance.

   Order: Select your appliances in the following order:

   - Flow Collector
   - Flow Sensor
   - Manager
3. Select **Edit Appliance Configuration**.
4. On the Appliance Configuration page, on the **General** tab, locate the **Trust Store** section.

   Use this table to add the appliance identity certificate and certificate chain (root and intermediate) to the required Trust Stores.

   Table 5: Appliance Identity Trust Store Requirements

Identity Certificate	Details	Add Certificates to Trust Store
Flow Collector	Add the Flow Collector certificates to the Flow Collector Trust Store and the Manager Trust Store.	- CA Chain - Flow Collector - Manager
Flow Sensor	Add the Flow Sensor certificates to the Flow Sensor Trust Store and the Manager Trust Store.	- CA Chain - Flow Sensor - Manager
Manager	Add the Manager certificates to the Manager Trust Store and the Trust Store of every appliance in the Central Management appliance inventory.	- CA Chain - Manager - Flow Collectors - Flow Sensors

5. Click **Add New**.
6. In the **Friendly Name** field, enter a name for the certificate.
7. Click **Choose File**. Select the new appliance certificate.
8. Click **Add Certificate**.
9. Beside the Certificate Chain File field, click **Choose File**, then locate the chain file (or root CA cert if the appliance cert was signed by a root CA),
10. Confirm the new certificate is shown in the Trust Store list.
11. Repeat steps 5 through 10 to add all required certificates the appliance Trust store.
12. Click **Apply Settings** then click **Apply Changes**. Follow the on-screen prompts.
13. On the **Inventory** page, make sure the appliance finishes the configuration changes and the Appliance Status returns to **Connected** before you proceed to the next step.
14. Repeat these steps to add certificates to the next appliance Trust Store in your cluster.

4.1.4 Replace the Appliance Identity Certificates

Make sure you add all required certificates to the appliance Trust Stores before you replace the appliance identity certificates in this section.

After you have added all required certificates to the required appliance Trust Stores, you are ready to replace the appliance identity certificates. Use the following instructions to replace the appliance identity certificate on every appliance in your cluster.

1. On the Central Management > **Inventory** page, click the Ellipsis icon in the Actions column for the appliance.

Order: Update the appliance identity in the following order:

- Flow Collector
- Flow Sensor
- Manager

Make sure you follow the order to update the appliance identity.

2. Select **Edit Appliance Configuration**.
3. On the **Appliance** tab, locate the **SSL/TLS Appliance Identity** section.
4. If you generated a CSR in Central Management, go to step 5.

If you skipped the CSR in Central Management, click **Update Identity**. Select **No**, and click **Next**.

5. In the **Friendly Name** field, enter a name for the certificate.
6. Click **Choose File**. Select the new appliance identity certificate.

Click Choose File next to the Certificate Chain File field.

Select the complete chain file (that includes the intermediate CA and root CA certificates).

Click **Replace Identity**.

7. Click **Apply Settings** then click **Apply Changes**. Follow the on-screen prompts. The appliance reboots automatically.
8. On the **Inventory** page, make sure the appliance finishes the configuration changes and the Appliance Status returns to **Connected** before you proceed to the next step.
9. Review the SSL/TLS Appliance Identity list. Confirm the new certificate is shown.
10. Repeat these steps to update the appliance identity on the next appliance in your cluster.

> Make sure each appliance finishes the configuration changes and returns to Connected before proceeding to the next appliance.

11. If you've replaced the appliance identity certificate on every appliance in your cluster, go to the next section.

4.1.5 Delete Cisco Default Appliance Identity Certificates

After you replace the appliance identity certificates and confirm your appliances are Connected, delete the old (Cisco default) appliance identity certificates from the appliance Trust Stores.

> Do not delete the old (Cisco default) certificates until you've added the new certificates (identity, root, and chain) and fully completed the preceding procedures.

Use the following instructions to delete a certificate from the appliance Trust Store.

Trust Stores: See the Appliance Identity Trust Store Requirements table to review where the certificates are located.

1. On the **Inventory** page, click the **Ellipsis** icon in the **Actions** column for the appliance. Select your appliances in the following order:
    - Flow Collector
    - Flow Sensor
    - Manager
2. Select **Edit Appliance Configuration**.
3. On the **Inventory > General** tab, locate the Trust Store section.
4. On the **Trust Store** list, locate the Cisco default identity certificate (will have key length of 8192 bits) you want to delete.
5. Click **Delete**.
6. Repeat steps 4 and 5 to delete any additional Cisco default identity certificates from the appliance Trust store.
7. Click **Apply Settings** then click **Apply Changes**. Follow the on-screen prompts.
8. Connected: On the **Inventory** page, make sure the appliance finishes the configuration changes and the **Appliance Status** returns to **Connected** before you proceed to the next step.
9. Repeat these steps to delete certificates from the next appliance Trust Store in your cluster.

4.1.6 Review External Service Certificate Requirements

If you are planning to enable Syslog or LDAP, you need to add the required certificates to the correct Trust Stores.

Before you add any external (non-SNA) certificates to the Trust Stores, make sure they meet these Common Criteria requirements.

When you add a certificate to your appliance Trust Store, your appliance trusts that identity and allows communication with it. Make sure each external (non-SNA) certificate meets the requirements shown in this table.

Table 6: External Service Certificate Requirements

Requirement	Details
Signed by Certificate Authority (CA)	Make sure the certificate is signed by a Certificate Authority. Self-signed certificates are not compliant.
Certificate Chain Length (2 or more)	Certificate chain length must be at least 2: - Root (1 root) - Intermediate (0 or more intermediaries)
Extension: Basic Constraints	Target certificate (appliance identity certificate): CA set to No/False Chain certificate (root and intermediaries): CA set to Yes/True
Extended Key Usage	Make sure the certificate can be used as a server (serverAuth) certificate. If you use the SNA CSR procedure, the CSR includes this information. Make sure the OSCP Responder's certificate has the OSCP Signing EKU field if OSCP will be used. Make sure the Syslog server's certificate contains only one of either a CRL Distribution Point URI or an OCSP Responder URI, but not both. Make sure the CA certificate contains the cRLSign key usage if CRL will be used. **Exclude clientAuth:** Make sure the certificate is not used as a client (clientAuth) certificate.
Format	PEM (.cer, .crt, .pem) or PKCS#12 (.p12, .pfx, .pks)
IP Address as a Subject Alternative Name Field	Make sure the certificate includes the appliance IP address as one of the Subject Alternative Names.
Host Name as a Subject Alternative Name Field	Make sure the certificate includes the appliance host name as one of the Subject Alternative Names.

RSA Key Length	We only support RSA keys. Make sure your key is 4096 bits.
Date Range	Make sure the certificate dates are current and not expired.

4.1.7 Add External Service Certificates to the Trust Stores

If you are planning to enable Syslog or LDAP, review the External Service Trust Store Requirements table to determine the Trust Store requirements for your system.

Table 7: External Service Trust Store Requirements

Remote Server/Service	Certificate Type	Trust Stores
Syslog Server	Add the root CA certificate (that signed the Syslog certificate chain) to the Trust Stores. Make sure your server and certificates meet Common Criteria requirements.	All appliances in your SNA cluster
LDAP Server	Add the root CA certificate (that signed the LDAP certificate chain) to the Trust Stores. Make sure your server and certificates meet Common Criteria requirements.	Manager

Use the following instructions to add your server/service certificates to the appliance Trust Stores based on the External Service Trust Store Requirements table.

1. Open Central Management.
2. On the Inventory page, click the **Ellipsis** icon in the **Actions** column for the appliance.

   Order: If you have to add the certificates to more than one appliance Trust Store, select your appliances in the following order:

   - Flow Collector
   - Flow Sensor
   - Manager
3. S87lect **Edit Appliance Configuration**.
4. On the **Inventory** > **General** tab, locate the Trust Store section.
5. Click **Add New**.
6. In the **Friendly Name** field, enter a name for the certificate.
7. Click **Choose File**. Select the new certificate.
8. Click **Add Certificate**. Confirm the new certificate is shown in the Trust Store list.
9. Repeat steps 5 through 8 to add all required certificates the appliance Trust store.

10. Click **Apply Settings** then click **Apply Changes**. Follow the on-screen prompts.
11. On the **Inventory** page, make sure the appliance finishes the configuration changes and the Appliance Status returns to **Connected** before you add certificates to the next appliance.
12. Repeat these steps to add certificates to the next appliance Trust Store in your cluster.
13. If you have added all required certificates to the Trust Stores, go to the next section.

4.2 Compliance Mode (FIPS and Common Criteria)

4.2.1 Overview

Use Compliance Mode to enable encryption libraries for the Federal Information Processing Standard (FIPS) and Common Criteria (CC). Refer to section 1.7 of this document for further details regarding the impact of enabling FIPS and CC modes.

4.3 Enabling Compliance Encryption Libraries (FIPS, CC)

Use Compliance Mode to enable encryption libraries for FIPS and Common Criteria.

The following features are not available when FIPS encryption libraries are enabled: TACACS+, RADIUS, and Internet Proxy NTLM authentication.

The following features are not available when Common Criteria encryption libraries are enabled: See **Excluded Functionality** for details.

Complete the following instructions on every appliance in your SNA cluster, starting with each FC, then each FS, and finally configuring the Manager.

1. Confirm your Trust Stores are updated and your appliance identity certificates are replaced as specified in the **Certificates** procedure.
2. Open **Central Management**.
3. On the **Inventory** page, click the **Ellipsis** icon in the **Actions** column for the appliance.
4. Select **Edit Appliance Configuration**.
5. Select the **General** tab.
6. Locate the **Compliance Mode** section.
7. **Confirm Prerequisites**: Read the prerequisites and confirm you have completed all steps and are ready to enable FIPS and Common Criteria encryption libraries.
    - If you have completed all steps in the **Certificates** procedure, check the Trust Stores and appliance identity replacement check boxes.
    - Read the warning.
    - If you are ready to enable FIPS and Common Criteria encryption libraries, type the following digits: **12358**
    - Click **Continue**.
8. Check the **Enable FIPS Encryption Libraries** check box.
9. Check the **Enable Common Criteria Encryption Libraries** check box.
10. Click **Apply Settings** then click **Apply Changes**.

11. Follow the on-screen prompts. The appliance reboots automatically.
12. On the **Central Management > Inventory** page, make sure the appliance finishes the configuration changes and the Appliance Status returns to Connected. Repeat these instructions to enable FIPS and Common Criteria encryption libraries on the next appliance in your cluster.
13. If you've enabled compliance encryption libraries (FIPS, Common Criteria) on all appliances in your SNA cluster, go to the next section.

4.4 LDAP

The Lightweight Directory Access Protocol (LDAP) provides a method for remote user authentication.

Use the following instructions to configure and enable LDAP on the Manager.

Default: LDAP is disabled by default.

Recommendation: Before you get started, review the instructions for enabling LDAP. The procedure includes installing certificates and restarting the appliance. It is important to enable LDAP at a time that will cause the least amount of disruption.

4.4.1 Add the Certificate to the Trust Stores

Confirm you've added the LDAP server certificate to the Manager Trust Store using **Review External Service Certificate Requirements** and **Add External Service Certificates to the Trust Stores**.

4.4.2 Configure the LDAP Settings

Follow these instructions to configure your LDAP settings.

1. Open the Manager main dashboard and navigate to Configure > **Global > User Management**.
2. Select the **Authentication and Authorization** tab.
3. Click **Create > Authentication Service > LDAP**.
4. Complete the following fields:

Field	Notes
Friendly Name	Enter a name for the LDAP server.
Description	Enter a description for the LDAP server.
Server Address	Enter the fully qualified domain name or IP server address for the LDAP server.
Port	Enter the port designated for secure LDAP communication (LDAP over TLS). A commonly used TCP port for LDAP is 636.

5. In the Certificate Revocation field, select Hard Fail to be compliant. This will enable certificate revocation checking of the server's certificate using either CRL or OCSP, depending on which is defined within the server's certificate.
6. Complete the following fields:

Field	Notes
Bind User	Enter the administrative user ID used to connect to the LDAP Server. SNA does not support added or repeated comma characters in the Bind User field. Make sure you do not enter additional or repetitive commas if using a Distinguished Name (DN) as part of the Bind User name.
Password	Enter the password for the Bind User.
Confirm Password	Re-enter the exact characters of the Password you just entered.
Base Accounts	Enter the Distinguished Name (DN). The DN applies to the branch of the directory in which searches for users should begin. It is often the top of directory tree (your domain), but you can also specify a sub-tree within the directory. The Bind User and the users you are authenticating should be accessible from Base Accounts. For example: DC=example,DC=com

7. Click **Save.**

4.4.3 Add an LDAP User

1. Open **User Management**.
2. Select **Create > User**.

   For instructions, click the User icon, and select Online Help. For details about adding users, see "Configuring Users."

3. In the **User Name** field, enter the user name. The **Full Name** and **Email** fields are optional.
4. In the **Authentication Service** field, select your LDAP server.
5. In Role Settings, check the Primary Admin check box, if applicable, and select a Data Role.

   For instructions, click the User icon, and select Online Help. For details about web roles, see "Assign a Data Role."

6. Click Save and then confirm the newly added user appears in the list of users.

4.4.4 Troubleshooting LDAP Connectivity

Your LDAP server connection could have failed due to the following reasons, in which case you should take the action described here:

- In case of a network connectivity error, make sure you reestablish a network connection.
- In case you provided incorrect configuration information, make sure your addresses and credentials are valid and then try again to connect.

- In case the server's certificate is invalid or has have been revoked, ensure the server is using a valid certificate, and that the CRL or OCSP server is accessible then try again to connect.

4.5 Audit Log Destination

Use Audit Log Destination to configure a secure destination for all messages using Syslog over TLS (Transport Layer Security).

4.5.1 Prepare for Configuration

Confirm you've added the Syslog server certificate to the appliance Trust Stores using the requirements and procedure in **Review External Service Certificate Requirements** and **Add External Service Certificates to the Trust Stores**.

4.5.2 Configure the Audit Log Destination Settings

1. Open **Central Management**.
2. On the Inventory page, click the **Ellipsis** icon in the **Actions** column for the appliance.
3. Select **Edit Appliance Configuration**.
4. On the **Network Services** tab, locate the **Audit Log Destination (Syslog Over TLS)** section.
5. In the **IP Address** field, enter the IP address of the remote Syslog server.
6. In the **Destination Port** field, enter the port number that the appliance uses to provide audit trail information.

   Destination Port Default: 6514/TCP
7. Under **Certificate Revocation**, select **Hard Fail** to be compliant. This will enable certificate revocation checking of the server's certificate using either CRL or OCSP, depending on which is defined within the server's certificate.
8. Click **Apply Settings**.

   If the delivery fails, check the Audit Log. Also, check the Trust Store to confirm the Syslog SSL/TLS certificate is shown.
9. Review the inventory in **Central Management > Inventory**. Confirm the Appliance Status is shown as Connected. Repeat these instructions to configure Audit Log Destination on the next appliance in your cluster.
10. If you've configured Audit Log Destination on all appliances in your SNA cluster, go to the next section.

4.5.3 Enable Syslog Compliance and Certificate Path Debug Logging

Use the following instructions to establish Syslog server compliance and certificate path debug logging for the selected appliance. If Syslog is enabled, all logs related to compliance will be saved in the remote Syslog server.

1. Log in to the appliance console as sysadmin.
2. The System Configuration utility (menu-driven text-based interface) will start automatically.
3. Select **Security** from the Main Menu.

4. Select **Syslog Compliance** from the Security menu.
5. Select **Enable**. You can press the space bar on your keyboard to select it.
6. Select **OK**.
7. Select **Certificate Path Debug Log** from the Security menu.
8. Select **Enable.** You can press the space bar on your keyboard to select it.
9. Select **OK**.
10. Repeat these instructions to enable Syslog Compliance on the next appliance in your deployment.
11. When you've enabled Syslog Compliance on all SNA appliances in your deployment, go to the next section.

4.5.4 Troubleshooting Syslog Connectivity

Your syslog server connection could have failed due to the following reasons, in which case you should take the action described here:

- In case of a network connectivity error, make sure you reestablish a network connection.
- In case you provided incorrect configuration information, make sure your addresses and credentials are valid and then try again to connect.
- In case the server's certificate is invalid or has have been revoked, ensure the server is using a valid certificate, and that the CRL or OCSP server is accessible then try again to connect.

4.6 AIDE

The Advanced Intrusion Detection Environment (AIDE) is a host baselining system that detects modifications of critical files on a system. When it is enabled, AIDE runs an audit of the current system once a day. It compares the hash sum and permissions of each monitored file on the current file system against the values stored in the appliance database.

Each SNA appliance runs AIDE independently and generates audit log messages separately. You can review each audit log messages for each appliance through Central Management. Each appliance is uniquely identified by its hostname as recorded in the messages transmitted to the Syslog servers.

When the daily AIDE job completes, an audit log message that indicates whether any changes were detected is recorded in the audit log.

If no changes are detected, this message displays: **System baseline check passed, all files match baseline**.

If changes were detected, this message displays: **AIDE found differences between database and file system!** Following this message, there will be a list of the files that were changed. Review the list to make sure none of the file types are applicable to CC. The following file extensions do not apply to CC: .pod, .enc, .h, .exe, .txt, .xml, .csv, .log, .ini, .gfs, and .pyc.

> If there are other file types on the list, contact Cisco Support to determine whether the file changes are impacting CC security functionality. Make sure you maintain or reestablish CC security functionality.

Use the following instructions to Enable AIDE.

1. Select the **Appliance** tab.

2. Locate the **Advanced Intrusion Detection Environment** section.
3. Check the **Enable AIDE** check box.

   The appliance initializes a database within 1 hour.

4.7 Login Banners

Configure a login banner for each appliance through **Central Management**:

1. Select the **General** tab.
2. Locate the **Opening Message** section.
3. In the **Opening Message** field, type the message to be displayed prior to login.
   - Language: The message can be in any language and contain any supported UNICODE character other than the angle brackets (< >) or single quote (') symbols.
   - Character Limit: 120 alphanumeric characters and spaces maximum.

4.8 Protected Sessions Time-Out

Use Protected Sessions Time-Out to set the number of minutes administrator privileges can be used before the session times out. When the time expires, the user is prompted to re-authenticate the administrator session.

Make sure you also specify how long an administrator session can be inactive before the user is automatically logged out. The user can continue to use parts of the appliance that do not require administrator access.

For instructions, click the User icon, and select Online Help. For details about session time-out, see "Protected Sessions Time-Out."

1. Locate the **Protected Sessions Time-Out** section.
2. In the **Request User Re-Authentication for Administrator-Only Functions After** field, enter the number of minutes limit for an administrator session before re-authentication is required.
   - **Default**: The default setting is 1440 minutes (24 hours). The default is implemented when you install the appliance or upgrade the software (for example, from a major version 6.x to 7.x, etc.).
   - **Range**: 2 to 1440 minutes
   - **0:** If you enter 0, the administrator session never expires.
3. In the **Log Out User Due to Inactivity After** field, enter the number of minutes a session can be in an idle state with no activity.
   - **Default**: The default setting is 0; it must be changed for compliance.
   - **Range**: 2 to 1440 minutes
   - **0:** If you do not change the default of 0, the administrator session never expires.

Note: The Security Lockout rules do not apply to the admin or sysadmin accounts.

4.9 Password Policy

The password policy configuration applies to all user interfaces. Configure password complexity to a minimum of 8 characters (15 or greater is recommended industry best practice), which include at least one uppercase letter, lowercase letter, number, and special character.

Use the following instructions to define password complexity for users.

1. Locate the **Password Policy** section (Configure > Central Management > Edit Appliance Configuration (via ellipsis) > General (tab) > **Password Policy**).
2. Configure your password policy to meet the following compliance requirements:

Table 8: General (password policy settings)

Field	Criteria	Default Values	CC Compliance Requirements
Password **Minimum** Character Length	characters	8	8 minimum (15 or greater is recommended)
Password **Maximum** Character Length	characters	256	15 or greater (up to 256)
Password expires after	days	0	0 or greater
Number of previous passwords disallowed	passwords	1	3 or greater
Minimum number of days allowed between password changes	days	0	0 or greater

Table 9: Password Complexity

Field	Characters	Default Values	CC Compliance Requirements
Minimum Number of Upper Case Letters in Password	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z	0	0 or greater (1 or more recommended)
Minimum Number of Lower Case Letters in Password	a b c d e f g h i j k l m n o p q r s t u v w x y z	0	0 or greater (1 or more recommended)
Minimum Numbers in Password	1 2 3 4 5 6 7 8 9 0	0	0 or greater (1 or more recommended)

Minimum Number of Symbols in Password	< > . , ? / ' " \ | : ; ` ~ ! @ # $ % ^ & * ( ) - _ + = { } [ ]	0	0 or greater (1 or more recommended)
Number of characters different from previous password		4	0 or greater

4.10 Session Settings (Account Lockout)

Two of the fields in the Session Settings section are also required for compliance (Configure > Central Management > Edit Appliance Configuration (via ellipsis) > General (tab) > **Session Settings**). The account lockout rules do not apply to the admin and sysadmin users. This needs to be enabled in the evaluated configuration.

Table 10: Session Settings

Field	Description	Criteria	Default Values	CC Compliance Requirements
Number of unsuccessful attempts	The number of unsuccessful sign-on attempts before security lockout occurs.	numbers	0	Greater than zero (1-10)
Duration of lockout	The duration in minutes of the security lockout.	minutes	0	Greater than zero
Maximum Number Of Concurrent Sessions	The maximum number of concurrent sessions allowed for any account	number of sessions	0	Any value is allowed (configurable from 0 to 5 where zero means unlimited)

4.11 External Services

Use the following instructions to disable External Services, which are enabled by default.

1. In **Configuration Management**, navigate to the **General** tab.
2. Locate the **External Services** section.

   For an appliance to be compliant, all fields in the External Services section must be disabled.

3. Uncheck all checkboxes (includes Cisco Security Cloud Control, Customer Success Metrics, and Threat Feed).
4. Click **Apply Settings**.

4.12 NTP

During initial setup, when using the Appliance Setup Tool to join appliances to the Manager, each appliance was configured with at least one NTP server. To satisfy requirements for the CC-evaluated configuration, each NTP server must be configured to use authentication. Follow these instructions to configure NTPv4 authentication using SHA1.

To add, delete or modify NTP settings:

1. In **Configuration Management**, navigate to the **Network Services** tab.
2. Locate the **NTP Server** section.
3. To add an NTP server click **Add New**.
4. To delete an NTP server click the **Ellipsis** then click **Delete**.
    - At least one NTP server must be configured, so if only one NTP server has been configured, it cannot be deleted. If more than one NTP server has been configured, then clicking the **Ellipsis** will show a **Delete** option.
    - Select an NTP server or add a custom server to your appliance configuration. If you add a custom server, configure DNS Server and/or Local Resolution.
    - To keep the time up-to-date, the system checks your NTP servers periodically. For details, review **Appliance Support > Audit Logs**.
    - To add authentication, go to **Appliance Support > Audit Logs** to confirm the NTP server communication status and system time changes are successful. If authentication failed, you do not have a connection with that server. Delete the NTP server and add it again (note: if there is only one NTP server configured it cannot be deleted; to delete the one configured NTP server first create another NTP server connection then delete the original one).
5. To enable NTPv4 SHA1 authentication click the **Ellipsis** then click **Authenticate Connection** and enter the Key ID and Key Value, then click **Apply Authentication** then click **Apply Settings** in the top right corner of the interface.
6. Repeat these steps as needed for each SNA appliance.

> **Note**: By default, the NTP client in SNA appliances will not accept broadcast or multicast NTP packets to update the clock. This default setting satisfies the CC requirement and is not configurable.

4.13 Local Authentication

Use the following instructions to configure your appliances for local authentication as required for CC compliance.

4.13.1 Disable the Admin User Account

The evaluated Common Criteria configuration requires the default admin user account be disabled because the Security Lockout rules do not apply to the admin user account.

In the event that all non-default local administrative accounts become locked, they can be reenabled:

- by either waiting for the lockout duration to expire, or

- by temporarily re-enabling the default admin user account to unlock other accounts, and then immediately re-disabling the default admin user account

Use the following instructions to disable the default admin user account on all appliances in your SNA cluster.

Make sure there is a user who will still have access to the Web UI.

1. Log in to the appliance console as sysadmin.
   - **Physical Appliances:** For details about console access for physical appliances, refer to the [SNA-HIG].
   - **Virtual Appliances:** For console access on all virtual appliances, refer to the "Booting from the ISO" and "Configuring the IP Addresses" sections in the [SNA-VEIG].
2. Type your password, and press Enter.
3. Select **Advanced**, and press Enter.
4. Select **Admin User**, and press Enter.
5. Follow the on-screen prompts to disable the admin user account.
6. Repeat these instructions to disable the admin user account on all appliances in your SNA cluster.

4.13.2 Accessing the Linux Shell via the Console

In previous versions of SNA it was possible to access the Linux shell as root, but that access is disabled by default in SNA 7.5.x. Accessing the Linux shell can only be performed with the assistance of Cisco TAC, and accessing the Linux shell as root will remove the TOE from its CC-certified configuration.

4.13.3 Disable SSH Access

Use the following instructions to disable SSH and Root SSH in the Web UI.

1. Log in to the Manager as the admin account or equivalent.
2. Open Central Management.
3. Click the **Ellipsis** icon in the **Actions** column for the appliance.
4. Select **Edit Appliance Configuration**.
5. On the **Appliance** tab, locate the **SSH** section.
6. Uncheck the **Enable SSH** check box.
7. Leave the **Enable Sysadmin User** checkbox checked.
8. Click **Apply** Settings.
9. Repeat these instructions to disable SSH on all appliances in your SNA cluster.

4.14 Apply Settings

Use the following instructions to apply your configuration changes to the selected appliance.

1. Click **Apply** Settings.
2. Follow the on-screen prompts. The appliance reboots automatically.

3. **Connected**: Review the inventory in **Central Management > Inventory**. Confirm the Appliance Status is shown as Connected. Go to **Secure Management** to configure the next appliance in your SNA cluster.

5 Secure Management

5.1 Scope

The evaluation is limited in scope to the secure management features described in the following:

- collaborative Protection Profile for Network Devices (NDcPP) v3.0e (06-December-2023) for Common Criteria

To change your configuration or review configurations that are excluded from compliance, refer to **Excluded Functionality** for details.

5.2 Documentation

Refer to the **Document References** list to review SNA built-in Help and guides.

5.3 Reviewing the Software Version

After you finish the installation and configuration, you can verify the software version in any of the following ways:

- Manager Web UI: Click the **User** icon and select **About**.
- Update Manager: Navigate to **Central Management > Update Manager** to review the software version installed on each appliance.

The running version also displays across the top of **System Configuration** utility (when logged in as sysadmin via the local console).

5.4 User Management

SNA has two default accounts: the ‘sysadmin’ account can only login via CLI, and the ‘admin’ that can only login via WebUI. Additional local WebUI accounts can be created to access the WebUI, and LDAPS can be enabled to allow remote (AAA/LDAP) accounts to login via WebUI. Accounts with access to WebUI must be assigned to one of two “data roles” (read & write, or read-only), and two one or more “Web Roles”. The web roles determine which web pages can be accessed, and the data roles determine whether the account will be able to modify configuration settings on those web pages.

The term “Authorized Administrator” refers to any user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore, has the appropriate privileges to perform the requested functions. Therefore, semi-privileged administrators with only a subset of privileges may also manage and modify TOE data based on the privileges assigned.

The TOE provides the ability for Authorized Administrators to access TOE data, such as user accounts and roles, audit data, audit server information, configuration data, security attributes login banners, inactivity timeout values, password complexity setting, TOE updates and session thresholds via the CLI. The TOE restricts the access to manage TSF data that can affect security functions of the TOE to the Authorized Administrator/Security Administrator roles.

Manual software updates can only be done by the authorized administrator through the WebUI. These updates include software upgrades. The Security Administrators (a.k.a Authorized Administrators) can query the software version running on the TOE, and can initiate updates to (replacements of) software images. When software updates are made available by Cisco, the Authorized Administrators can obtain, verify the integrity of, and install those updates.

To configure local users:

1. From the main Manager screen, click the Gear icon.
2. Click User Management.
3. Use the WebUI to create, modify or delete accounts.

User Management allows you to do the following:

- create or delete user accounts
- enable or disable user accounts
- enter or change passwords
- view web role permissions
- edit user accounts
- configure web roles
- configure data roles

5.5 Terminating User Sessions

Use the following instructions to terminate console sessions and Web UI user sessions.

5.5.1 Terminate Your Console Session

Use the following instructions to terminate your console session.

> When you log into the appliance console as sysadmin, you can only access the System Configuration utility. You cannot access a command prompt.

1. Press the Tab key to navigate to Cancel or Exit.
2. Click Cancel or Exit until you've exited the session, and a login prompt displays.

5.5.2 Terminate Your Web UI Session

Use the following instructions to terminate your user session in the Web UI.

1. Click the User icon in the toolbar in the upper right corner.
2. Select Logout.

> Make sure you terminate the user account on every appliance in your SNA cluster in the Web UI.

5.5.3 Terminate Another User's Active Web UI Session

Use the following instructions to terminate another user's Web UI session in SNA.

> You cannot delete the default admin user account active (Admin) or your own user account.

1. Open **User Management**.
2. Locate the user name in the list.
3. You can delete or disable the user:
   - **Delete**: Click the **Ellipsis** icon in the **Actions** column. Select **Delete**.

- **Disable**: Click the status button to turn it off.

4. Open **Central Management**.
5. On the **Inventory** page, click the **Ellipsis** icon in the **Actions** column.

   Select Reboot.

   - **Order**: Reboot your Manager last.
   - **Unavailable**: The appliance is unavailable while it reboots. You will see an error message if you try to use the appliance before it is finished rebooting.
6. Repeat steps 4 and 5 to reboot every appliance in Central Management.

5.6 Syslog and Audit Logs

5.6.1 Syslog

When Syslog Compliance is enabled, SNA compliance logs are saved in the remote Syslog server. The data is determined by the logs from each appliance. Some of the logs are as follows:

For more information, see **Security Relevant Events**.

Syslog Field	Description
Syslog Time	The date and time the message was created by Syslog.
Local Host	Name of appliance where the event occurred.
AuditLogger: user	**Audit Logger:** the process that is sending events to the Syslog server. **User:** the process that created the audit event.
Audit ID	The ID assigned to the event.
Date	Date and time the event occurred.
User	The role of the user who performed the action, or the role at which the process is active if no user is associated with the action.
IP Address	The IP address of the device used to perform the action.
Success or Failure	**Yes:** The action was completed. **No:** The action was not completed.
Message	The details of the event and this information can vary based on the specific event.

5.6.2 Audit Logs

You can also review the audit logs for a selected appliance in Central Management.

- **Web UI:** To review the audit logs in Central Management, click the **Ellipsis** icon in the **Actions** column, select **Support**, and then select the **Audit Logs** tab.
- **Details:** Click the **User** icon and select **Online Help**.
- **Sort and Filter:** You can sort the audit logs by clicking on each column or filter the data.
- **Event Details:** See **Security Relevant Events** for more information.

Audit Log Column	Description
Date/Time	The date and time the data was recorded.
Category	**Management:** basic management and configuration changes. **IDS:** intrusion detection functions. **Audit:** auditing and system level functions. **I&A:** user identification and authentication. **Security:** user maintenance and lockout.
Event	The ID assigned to the event. Provide the Event ID if you contact Cisco Support.
Event Details	The description of the event.
User Name	The user login name associated with the event. The user ID is displayed in parentheses.
User Location	The IP address of the device used to perform the action.
Process Name (PID)	The component that issued the log message. The process ID reported by the component is displayed in parentheses.
Success	**Yes:** The action was completed. **No:** The action was not completed.

5.6.3 Audit Log History

In addition to transmitting logs to an external Syslog server, each SNA appliance saves audit messages locally to an audit log file. When the audit log file reaches the maximum size (5MB), a new audit log file is created. A log rotation job runs nightly; and if the active log has grown to 5 MB, it is rotated. This results in the oldest records being purged to allow space new records to be written.

5.7 Product Updates

To update your SNA appliances, open **Central Management > Update Manager**:

- **Instructions**: For an overview of steps, click the **Help** icon. Select **Online Help**. When SNA update or patch files become available, download and follow the instructions in [SNA-UG].
- **Software Updates:** Software updates can be downloaded from the Cisco software download site at https://software.cisco.com.
- **Checksum Comparison:** When you download the software update files to the management computer, note the SHA-512 checksum displayed on the download page. Run a command on your local workstation (such as "sha512sum") to calculate the checksum. Compare the result with the checksum on the download page. Then, upload the file to the Update Manager.

If the result does not match the checksum, don't upload the file to the Manager. Attempt to download the file again from https://software.cisco.com; and if the calculated checksum still does not match the expected checksum, then contact Cisco Support.

- **Software Version**: Go to **Central Management > Update Manager** to review the software version installed on each appliance. The Update Manager also shows the last reboot, version ready to install, and the update status.
- **Order:** Make sure you update the appliances in order as described in [SNA-UG].

SNA does not support concurrent uploading of SWU files to the Manager.

- **Appliance Status:** Make sure each appliance completes the update and that the appliance status is shown as Connected before you update the next appliance in your cluster.
- **Success/Failure:** If the software update fails, **Installation Failed** displays in the Update Status column. The failure could be caused by a loss of network connectivity during the upload or a failure of the digital signature verification that's performed when the patch or update is uploaded to the Manager.

5.7.1 Installation Failed

After you complete the offline verification of the integrity of the SWU file, upload each of the SWU files to the Manager. If the Update Status column displays Installation Failed, follow these instructions:

1. Click the **Ellipsis** icon in the **Actions** column.
2. Click > **View Update Log**.
3. Review the log for errors.

If the upload fails, review these possible reasons:

- You were attempting to upload more than one SWU file at a time. To resolve:
  - Make sure all of your uploads are stopped.
  - Upload each SWU file separately, and in order.
  - Wait for that status of each upload to change from Processing to Success before uploading the next file.
- There is insufficient disk space to upload the SWU files. To resolve:
  - Make sure there is sufficient space available.

- Refer to the "Check the Available Disk Space" section in [SNA-UG].
- Expand the available disk space, if needed.

5.7.2 Troubleshooting a Failed Installation

Common reasons update files and patches fail to upload:

- Lack of disk space:
  - If this occurs, the update log indicates **No space left on device**.
  - To resolve this issue, expand the appliance disk space by following the instructions in the "Data Storage" section of [SNA-CG].
- Loss of network connectivity between the Manager and the managed appliances during the transfer of the update file or patch from the Manager to the managed appliances.
  - If this occurs, restore the network connectivity and retry installing the update or patch.
- l Target appliance fails a readiness check during installation:
  - This can occur if the minimum amount of time hasn't transpired since the previous reboot of the Manager or FC, or if a service fails to stop cleanly when preparing to install the update.
  - If this occurs, the Update Status shows Installation Failed and the update log indicates **Unexpected exit status!**. To resolve these issues, wait for the necessary minimum time since the previous reboot of the target appliance, and retry to install the update. If the error occurs again, then contact Cisco Support.

5.8 Resetting Factory Defaults (RFD)

When you reset factory defaults on an appliance, sensitive data is destroyed automatically.

- SSH host keys

SSH is not enabled in the evaluated Common Criteria configuration.

- Appliance identity certificate information
- Appliance web server ephemeral key seeds
- Central Management identity configuration
- Any trusted private keys for external web servers

For further instructions, refer to [SNA-CG].

Make sure you RFD each appliance twice to completely erase data.

6 Security Relevant Events

As log messages are sent to the remote Syslog server, the messages are also written to local circular log files that can be reviewed on each appliance console. Each local file is rotated, or replaced, when it reaches 5 MB. A log rotation job runs nightly; and if the active log has grown to 5 MB, it is rotated. This results in the oldest records being purged to allow space new records to be written.

When you enable Syslog Compliance (via the System Configuration utility accessible via the console) and configure the Syslog servers for each SNA appliance, all log messages will be sent to a remote Syslog server.

> Note: Error messages that indicate connection failures to Syslog servers won't be sent to the remote Syslog server.

You can also view the log messages for all appliances in the Audit Log, which you access through Central Management in the Manager.

Most log messages have a similar format regardless of whether they were generated for the Manager or other appliances. Some Manager log messages are different, particularly for events regarding communications between the Manager and other appliances. The table specifies which log messages are generated by the Manager and which are generated by other appliances.

Log messages typically display in the following format:

```
<date-time> <hostname> <process>[process-id]: <metadata>,<user>(<userid>),
<message-detail>
```

The term "metadata" includes date-time and/or process numbers. Additionally, log messages might indicate Syslog severity level; for example, INFO, ERROR, etc.

> Log message samples in this table contain generic message field identifiers instead of actual details such as timestamps, host names, and IP addresses.

The following table provides descriptions of audit logs messages.

Table 11: Audit Log Messages

Requirements	Auditable Events	SNA Examples
FAU_GEN.1	Startup of the audit functions	<date-time> <hostname> syslog-ng[<pid>]: AuditLogger: syslog- ng/<pid>,***4021***, <yyyy-mm-ddThh:mm:ssTZD+<offset>,root(0), localhost,1,***Audit log service started***
	Shutdown of the audit functions	<date-time> <hostname> syslog-ng[<pid>]: AuditLogger: syslog-ng/<pid>,***4022***,<timestamp>,root(0),localhost,1,***Audit log service stopped***
FAU_STG_EXT.1	Configuration of local audit settings.	Initiate change of audit settings: <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: svc-cm-configuration/1,1506,<timestamp>,<username>,<remote-ip>,1,***Initiated change appliance configuration widget auditLogDestination*** Change audit server IP: <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: osaxsd/<pid>,1100,<timestamp>,root(0),localhost,1,***System Service syslog has changed these settings: AUDIT_EXT_IP = <audit-server-ip>*** Change revocation-check behavior:

		<date-time> <hostname> AuditLogger[<pid>]: AuditLogger: osaxsd/<pid>,1100,<timestamp>,root(0),localhost,1,***System Service syslog has changed these settings: AUDIT_EXT_OCSP_CHECK_MODE = Hard Fail***
FCO_CPC_EXT.1	Enable and disable communication between pairs of components	<date-time> <hostname> AuditLogger[<pid>]: AuditLogger: svc-cm-inventory/1,1207,<timestamp>,<username>,<remote-ip>,1,***Appliance "<appliance-ip>" added to Central Manager*** <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: svc-cm-inventory/1,1208,<timestamp>,<username>,<remote-ip>,1,***Appliance "<appliance-ip>" deleted from Central Manager***
FCS_HTTPS_ EXT.1	Failure to establish HTTPS session	**Manager Appliance:** *(not applicable to other appliances)* <date-time> <hostname> <metadata> ***SSL_do_handshake() failed (SSL: error:0A0000C1:SSL routines::no shared cipher)*** while SSL handshaking, client: <remote-ip>, server: 0.0.0.0:443 **Unknown protocol:** <date-time> <hostname> <metadata> ***SSL_do_handshake() failed (SSL: error:0A0000FC:SSL routines::unknown protocol)*** while SSL handshaking, client: <remote-ip>, server: 0.0.0.0:443
FCS_NTP_EXT.1	Configuration of a new time server	Add an NTP server <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: svc-cm-configuration/1,1507,<timestamp>,<username>,<remote-ip>,1,***SMC: Initiated change appliance configuration widget ntp*** <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: osaxsd/<pid>,1100,<timestamp>,jetty(996),localhost,1,***NTP server: <ntp-server-ip> was verified successfully*** Replace an NTP server by replacing its IP address: <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: osaxsd/<pid>,1100,<timestamp>,root(0),localhost,1,***System Service time has changed these settings: ENABLED = yes, SERVER = ['<existing-ntp-server-ip>__1', '<new-ntp-server-ip>__2']***
	Removal of configured time server	Remove an NTP server (where <ntp-server-id-number> must be greater than 1): <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: svc-cm-configuration/1,1507,<timestamp>,<username>,<remote-ip>,1,***SMC: Initiated change appliance configuration widget ntp*** <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: osaxsd/<pid>,1100,<timestamp>,root(0),localhost,1,***System Service time has changed these settings: ENABLED = yes, SERVER = ['<remaining-ntp-server-ip>__1']***
FCS_TLSC_ EXT.1	Failure to establish TLS session	LDAP Over TLS: Paired failure banner: <date-time> <hostname> <metadata> INFO c.l.sws.smc.auth.LdapSessionFactory - ***Failed to establish TLS connection to <ldap-server>.*** Invalid or unknown ciphersuite: <date-time> <hostname> <metadata> ***ERR_04120_TLS_HANDSHAKE_ERROR The TLS handshake failed, reason: Unspecified: illegal_parameter(47); ServerHello selected invalid cipher suite*** Wrong TLS version: <date-time> <hostname> <metadata> ***ERR_04120_TLS_HANDSHAKE_ERROR The TLS handshake failed, reason: Unspecified: protocol_version(70)*** Missing serverAuth EKU: <date-time> <hostname> <metadata> ***ERR_04120_TLS_HANDSHAKE_ERROR The TLS handshake failed, reason: Failed to verify certification path: Certificate doesn't support 'serverAuth' ExtendedKeyUsage*** Bad curve or FFDHE parameter: <date-time> <hostname> <metadata> ***ERR_04120_TLS_HANDSHAKE_ERROR The TLS handshake failed, reason: Unspecified: illegal_parameter(47)***

		Corrupt verify or finished message: <date-time> <hostname> <metadata> ***ERR_04120_TLS_HANDSHAKE_ERROR The TLS handshake failed, reason: Unspecified: decrypt_error(51)*** Unexpected message: <date-time> <hostname> <metadata> ***ERR_04120_TLS_HANDSHAKE_ERROR The TLS handshake failed, reason: Unspecified: unexpected_message(10); Opaque handshake(22)*** Bad reference identifier: <date-time> <hostname> <metadata> ***ERR_04120_TLS_HANDSHAKE_ERROR The TLS handshake failed, reason: Unspecified: Failed hostname verification to <ldap-server>***
FCS_TLSC_ EXT.2	Failure to establish TLS session	Syslog Over TLS: Invalid ciphersuite: <date-time> <hostname> <metadata> ***Logging to External Audit Log Destination failed [host= <syslog-server-ip>:6514] - org.bouncycastle.tls.TlsFatalAlert: illegal_parameter(47); ServerHello selected invalid cipher suite*** Wrong TLS version: <date-time> <hostname> <metadata> ***Logging to External Audit Log Destination failed [host= <syslog-server-ip>:6514] - org.bouncycastle.tls.TlsFatalAlert: protocol_version(70)*** Missing serverAuth EKU: <date-time> <hostname> <metadata> ***Logging to External Audit Log Destination failed [host= <syslog-server-ip>:6514] - java.security.cert.CertPathValidatorException: Certificate doesn't support 'serverAuth' ExtendedKeyUsage*** Bad signature: <date-time> <hostname> <metadata> ***Logging to External Audit Log Destination failed [host= <syslog-server-ip>:6514] - org.bouncycastle.tls.TlsFatalAlert: decrypt_error(51)*** Unexpected message: <date-time> <hostname> <metadata> ***Logging to External Audit Log Destination failed [host= <syslog-server-ip>:6514] - org.bouncycastle.tls.TlsFatalAlert: unexpected_message(10); Opaque handshake(22)*** Bad reference identifier: <date-time> <hostname> <metadata> ***Logging to External Audit Log Destination failed [host= <syslog-server-ip>:6514] - java.security.cert.CertificateException: certificate for peer <syslog-server-ip> not found in trust store*** FPT_ITT (inter-appliance) communications via TLS: <date-time> <hostname> <metadata> ***SSL_do_handshake() failed (SSL: error:0A0000F8:SSL routines::unknown cipher returned) while SSL handshaking to upstream,*** *client: ::ffff:<client-ip>, server: localhost, request: "<request>", subrequest: "/internal/service/auth", upstream: "https://<appliance-ip>:443/token/v2/service-authenticate/<service>", host: "appliance-gateway:8008"* <date-time> <hostname> <metadata> ***SSL_do_handshake() failed (SSL: error:0A000102:SSL routines::unsupported protocol) while SSL handshaking to upstream,*** *client: ::ffff:<client-ip>, server: localhost, request: "<request>", subrequest: "/internal/service/auth", upstream: "https://<appliance-ip>:443/token/v2/service-authenticate/<service>", host: "appliance-gateway:8008"* <date-time> <hostname> <metadata> ***CiscoSSL error encountered: unsuitable certificate purpose. while SSL handshaking to upstream,*** *client: ::ffff:<client-ip>, server: localhost, request: "<request>", subrequest: "/internal/service/auth", upstream: "https://<appliance-ip>:443/token/v2/service-authenticate/<service>", host: "appliance-gateway:8008"* <date-time> <hostname> <metadata> ***SSL_do_handshake() failed (SSL: error:0A00017F:SSL routines::wrong certificate type) while SSL handshaking to upstream,*** *client: ::ffff:<client-ip>, server: localhost, request: "<request>", subrequest: "/internal/service/auth", upstream: "https://<appliance-ip>:443/token/v2/service-authenticate/<service>", host: "appliance-gateway:8008"* <date-time> <hostname> <metadata> ***SSL_do_handshake() failed (SSL: error:02000068:rsa routines::bad signature error:1C880004:Provider routines::RSA lib error:0A00007B:SSL routines::bad signature) while SSL handshaking to upstream,*** *client: ::ffff:<client-ip>, server: localhost, request: "<request>", subrequest: "/internal/service/auth", upstream: "https://<appliance-ip>:443/token/v2/service-authenticate/<service>", host: "appliance-gateway:8008"* <date-time> <hostname> <metadata> ***SSL_do_handshake() failed (SSL: error:0A00006C:SSL routines::bad key share) while SSL handshaking to upstream,***

		client: ::ffff:<client-ip>, server: localhost, request: "<request>", subrequest: "/internal/service/auth", upstream: "https://<appliance-ip>:443/token/v2/service-authenticate/<service>", host: "appliance-gateway:8008" <date-time> <hostname> <metadata> ***SSL_do_handshake() failed (SSL: error:0A000095:SSL routines::digest check failed) while SSL handshaking to upstream,*** *client: ::ffff:<client-ip>, server: localhost, request: "<request>", subrequest: "/internal/service/auth", upstream: "https://<appliance-ip>:443/token/v2/service-authenticate/<service>", host: "appliance-gateway:8008"* <date-time> <hostname> <metadata> ***SSL_read() failed (SSL: error:0A0000F4:SSL routines::unexpected message) while reading response header from upstream,*** *client: ::ffff:<client-ip>, server: localhost, request: "<request>", subrequest: "/internal/service/auth", upstream: "https://<appliance-ip>:443/token/v2/service-authenticate/<service>", host: "appliance-gateway:8008"* <date-time> <hostname> <metadata> ***IP address mismatches presented certificate for connection: <appliance-ip>.***
FCS_TLSS_ EXT.1	Failure to establish TLS session	TLS for Remote Administration (applicable only to the Manager): No shared cipher: <date-time> <hostname> <metadata> ***SSL_do_handshake() failed (SSL: error:0A0000C1:SSL routines::no shared cipher) while SSL handshaking****, client: <remote-ip>, server: 0.0.0.0:443* Unknown protocol: <date-time> <hostname> <metadata> ***SSL_do_handshake() failed (SSL: error:0A0000FC:SSL routines::unknown protocol) while SSL handshaking****, client: <remote-ip>, server: 0.0.0.0:443* Version too low: <date-time> <hostname> <metadata> ***SSL_do_handshake() failed (SSL: error:0A00018C:SSL routines::version too low) while SSL handshaking****, client: <remote-ip>, server: 0.0.0.0:443* No suitable key share: <date-time> <hostname> <metadata> ***SSL_do_handshake() failed (SSL: error:0A000065:SSL routines::no suitable key share) while SSL handshaking****, client: <remote-ip>, server: 0.0.0.0:443* Digest check failed: <date-time> <hostname> <metadata> ***SSL_do_handshake() failed (SSL: error:0A000095:SSL routines::digest check failed) while SSL handshaking****, client: <remote-ip>, server: 0.0.0.0:443* Renegotiation rejected: <date-time> <hostname> <metadata> ***SSL_do_handshake() failed (SSL: error:0A000150:SSL routines::renegotiation encoding err) while SSL handshaking****, client: <remote-ip>, server: 0.0.0.0:443* FPT_ITT (inter-appliance) communications via TLS (on all appliances): No shared cipher: <date-time> <hostname> <metadata> ***SSL_do_handshake() failed (SSL: error:0A0000C1:SSL routines::no shared cipher) while SSL handshaking****, client: <remote-appliance-ip>, server: 0.0.0.0:443* No suitable key share: <date-time> <hostname> <metadata> ***SSL_do_handshake() failed (SSL: error:0A000065:SSL routines::no suitable key share) while SSL handshaking****, client: <remote-appliance-ip>, server: 0.0.0.0:443* Bad signature: <date-time> <hostname> <metadata> ***SSL_do_handshake() failed (SSL: error:02000085:rsa routines::first octet invalid error:1C880004:Provider routines::RSA lib error:0A00007B:SSL routines::bad signature) while SSL handshaking****, client: <remote-appliance-ip>, server: 0.0.0.0:443* Digest check failed: <date-time> <hostname> <metadata> ***SSL_do_handshake() failed (SSL: error:0A000095:SSL routines::digest check failed) while SSL handshaking****, client: <remote-appliance-ip>, server: 0.0.0.0:443* Renegotiation rejected: <date-time> <hostname> <metadata> ***SSL_read() failed (SSL: error:0A0000F4:SSL routines::unexpected message) while waiting for request****, client: <remote-appliance-ip>, server: 0.0.0.0:443* Bad reference identifier: <date-time> <hostname> <metadata> ***IP address mismatches presented certificate for connection: <remote-appliance-ip>. while SSL handshaking****, client: <remote-appliance-ip>, server: 0.0.0.0:443*
FCS_TLSS_ EXT.2	Failure to establish TLS Session	**TLS Server Communication (between SNA appliances):**

		See FCS_TLSS_EXT.1 for audit records.
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded	<date-time> <hostname> AuditLogger<metadata>,<username>,<remote-ip-address>,0,***Login failed: User Disabled***
FIA_UIA_EXT.1	All use of the identification and authentication mechanism	**Manager Remote Administration):** Remote Auth Success <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: svc-token-authority/1,4002,<timestamp>,<username>,<remote-ip>,1,***Login successful*** Remote Auth LDAP Success <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: svc-legacy-auth/17,4002,<timestamp>,<username>,<remote-ip>,1,***Login successful*** Remote Auth Failure (local password failure) <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: svc-legacy-auth/18,4003,<timestamp>,<username>,<remote-ip>,0,***Login failed: Incorrect Credentials*** Remote Auth Failure (LDAP authentication failure) <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: svc-legacy-auth/17,4003,<timestamp>,<username>,<remote-ip>,0,***Login failed: Incorrect Credentials*** **All Appliances (Local Administration):** Local Auth Success <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: osaxsd/<pid>,4002,<timestamp>,sysadmin(75),127.0.0.1,1,***Login on Console successfu*** Local Auth Failure <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: osaxsd/<pid>,4003,<timestamp>,sysadmin(75),127.0.0.1,0,***Login on Console failed: Incorrect Password***
FIA_UAU_EXT.2	All use of the identification and authentication mechanism	See for FIA_UIA_EXT.1 for audit records.
FIA_X509_ EXT.1/ITT and FIA_X509_ EXT.1/rev	Unsuccessful attempt to validate a certificate	Manager (Operating as a TLS Client): <date-time> <hostname> <metadata> ***Certificate has been revoked, reason: UNSPECIFIED, revocation date: <timestamp>, authority: <certificate-DN>*** <date-time> <hostname> <metadata> ***Unable to determine revocation status due to network error*** <date-time> <hostname> <metadata> ***java.security.cert.CertPathValidatorException: Responder's certificate is not authorized to sign OCSP responses*** <date-time> <hostname> <metadata> ***ERR_04120_TLS_HANDSHAKE_ERROR The TLS handshake failed, reason: Certificate expired: Certificate expired at <timestamp> (compared to <timestamp>)***

		<date-time> <hostname> <metadata> ***SSL_do_handshake() failed (SSL: error:0A0000F8:SSL routines::unknown cipher returned) while SSL handshaking to upstream,*** *client: ::ffff:<client-ip>, server: localhost, request: "<request>", subrequest: "/internal/service/auth", upstream: "https://<appliance-ip>:443/token/v2/service-authenticate/<service>", host: "appliance-gateway:8008"* <date-time> <hostname> <metadata> ***SSL_do_handshake() failed (SSL: error:0A000102:SSL routines::unsupported protocol) while SSL handshaking to upstream,*** *client: ::ffff:<client-ip>, server: localhost, request: "<request>", subrequest: "/internal/service/auth", upstream: "https://<appliance-ip>:443/token/v2/service-authenticate/<service>", host: "appliance-gateway:8008"* <date-time> <hostname> <metadata> ***CiscoSSL error encountered: unsuitable certificate purpose. while SSL handshaking to upstream,*** *client: ::ffff:<client-ip>, server: localhost, request: "<request>", subrequest: "/internal/service/auth", upstream: "https://<appliance-ip>:443/token/v2/service-authenticate/<service>", host: "appliance-gateway:8008"*
		FC, FS (Operating as a TLS Client): <date-time> <hostname> <metadata> ***Certificate has been revoked, reason: UNSPECIFIED, revocation date: <timestamp>, authority: <certificate-DN>*** <date-time> <hostname> <metadata> ***Unable to determine revocation status due to network error*** <date-time> <hostname> <metadata> ***java.security.cert.CertPathValidatorException: Responder's certificate is not authorized to sign OCSP responses*** <date-time> <hostname> <metadata> ***ERR_04120_TLS_HANDSHAKE_ERROR The TLS handshake failed, reason: Certificate expired: Certificate expired at <timestamp> (compared to <timestamp>)*** <date-time> <hostname> <metadata> ***SSL_do_handshake() failed (SSL: error:0A0000F8:SSL routines::unknown cipher returned) while SSL handshaking to upstream,*** *client: ::ffff:<client-ip>, server: localhost, request: "<request>", subrequest: "/internal/service/auth", upstream: "https://<appliance-ip>:443/token/v2/service-authenticate/<service>", host: "appliance-gateway:8008"* <date-time> <hostname> <metadata> ***SSL_do_handshake() failed (SSL: error:0A000102:SSL routines::unsupported protocol) while SSL handshaking to upstream,*** *client: ::ffff:<client-ip>, server: localhost, request: "<request>", subrequest: "/internal/service/auth", upstream: "https://<appliance-ip>:443/token/v2/service-authenticate/<service>", host: "appliance-gateway:8008"* <date-time> <hostname> <metadata> ***CiscoSSL error encountered: unsuitable certificate purpose. while SSL handshaking to upstream,*** *client: ::ffff:<client-ip>, server: localhost, request: "<request>", subrequest: "/internal/service/auth", upstream: "https://<appliance-ip>:443/token/v2/service-authenticate/<service>", host: "appliance-gateway:8008"*
		All Appliances (Operating as a TLS server): <date-time> <hostname> <metadata> ***CiscoSSL error encountered: certificate has expired. while SSL handshaking, client: <remote-ip>, server: 0.0.0.0:443*** <date-time> <hostname> <metadata> ***CiscoSSL error encountered: invalid CA certificate. while SSL handshaking, client: <remote-ip>, server: 0.0.0.0:443*** <date-time> <hostname> <metadata> ***CiscoSSL error encountered: self-signed certificate in certificate chain. while SSL handshaking,*** *client: <remote-ip>, server: 0.0.0.0:443* <date-time> <hostname> <metadata> ***SSL_do_handshake() failed (SSL: error:068000A8:asn1 encoding routines::wrong tag error:0688010A:asn1 encoding routines::nested asn1 error:Type=X509_CINF error:0688010A:asn1 encoding routines::nested asn1 error:Field=cert_info, Type=X509 error:0A08000D:SSL routines::ASN1 lib) while SSL handshaking,*** *client: <remote-ip>, server: 0.0.0.0:443* <date-time> <hostname> <metadata> ***CiscoSSL error encountered: certificate signature failure. while SSL handshaking,*** *client: <remote-ip>, server: 0.0.0.0:443*

FIA_X509_ EXT.1/ITT and FIA_X509_EXT.1/ Rev	Any addition, replacement, or removal of trust anchors in the TOE's trust store	<date-time> <hostname> AuditLogger[<pid>]: AuditLogger: svc-cm-configuration/1,1506,<timestamp>,<username>,<remote-ip>,1,***Initiated change appliance configuration widget trustStore*** <date-time> <hostname> <metadata>,cm-agent,<appliance-ip>,1,***Successfully added certificate to trust store. Friendly name(s): [<certificate-names>]*** <date-time> <hostname> <metadata>,cm-agent,<appliance-ip>,1,***Trust store successfully synchronized. Following certificates are going to be removed: [<certificate-names-or-uuid>]***
Additional messages applicable to FIA_ X509_ EXT.1/Rev (not applicable to FIA_X509_ EXT.1/ITT)	Unsuccessful attempt to validate a certificate	Syslog Over TLS (all appliances): <date-time> <hostname> <metadata> ***Certificate has been revoked, reason: UNSPECIFIED, revocation date: <timestamp>, authority: <certificate-DN>*** <date-time> <hostname> <metadata> ***Unable to determine revocation status due to network error*** <date-time> <hostname> <metadata> ***java.security.cert.CertPathValidatorException: Responder's certificate is not authorized to sign OCSP responses*** <date-time> <hostname> <metadata> ***ERR_04120_TLS_HANDSHAKE_ERROR The TLS handshake failed, reason: Certificate expired: Certificate expired at <timestamp> (compared to <timestamp>)***
		LDAP Over TLS (Manager only): <date-time> <hostname> <metadata> ***Certificate has been revoked, reason: UNSPECIFIED, revocation date: <timestamp>, authority: <certificate-DN>*** <date-time> <hostname> <metadata> ***Unable to determine revocation status due to network error*** <date-time> <hostname> <metadata> ***java.security.cert.CertPathValidatorException: Responder's certificate is not authorized to sign OCSP responses*** <date-time> <hostname> <metadata> ***ERR_04120_TLS_HANDSHAKE_ERROR The TLS handshake failed, reason: Certificate expired: Certificate expired at <timestamp> (compared to <timestamp>)***
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update	**Logged by the Manager:** <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: svc-cm-update/1,1210,<timestamp>,<username>,<remote-ip>,1,***SWU image <filename>.swu uploaded to Central Manager.*** <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: svc-cm-update/1,1216,<timestamp>,<username>,<remote-ip>,1,***The 'install' action of SWU <filename>.swu is initiated on appliance <uuid>***
FMT_SMF.1	All management activities of TSF data	**Administer the TOE locally and remotely:** See FIA_UIA_EXT.1 (for all appliances), and FTP_TRP.1/Admin (for Manager only). **Configure the access banner:** <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: svc-cm-configuration/1,1507,<timestamp>,<username>,<remote-ip>,1,***<appliance-role>: Initiated change appliance configuration widget openingMessage*** <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: osaxsd/<pid>,1100,<timestamp>,root(0),localhost,1,***System Service bannermsg has changed these settings: BANNERMSG = <banner-message>***

		Configure the session inactivity time before session termination: <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: svc-cm-configuration/1,1507,<timestamp>,<username>,<remote-ip>,1,***<appliance-role>: Initiated change appliance configuration widget sessionTimeout*** <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: osaxsd/<pid>,1100,<timestamp>,root(0),localhost,1,***System Service session has changed these settings: idle_timeout_seconds = <seconds>*** **Update the TOE:** See FMT_MOF.1/ManualUpdate and FPT_TUD_EXT.1. **Configuring Authentication Failure Parameters (Manager only):** <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: svc-cm-configuration/1,1507,<timestamp>,<username>,<remote-ip>,1,***SMC: Initiated change appliance configuration widget securityLockout*** <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: svc-cm-agent/<pid>,1100,<timestamp>,jetty(996),localhost,1,***Session settings, security lockout account lock configurations updated successfully: Number of unsuccessful attempts: <n>, Duration of Lockout: <n> minutes, Login Info Popup: Enabled*** <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: osaxsd/<pid>,1100,<timestamp>,root(0),localhost,1,***System Service systemconfig has changed these settings: DISPLAY_FAILED_LOGINS = <yes-or-no>*** **Start and Stop Services:** Manager only: <date-time> <hostname> <metadata> INFO c.l.l.a.c.ldap.LdapConfigManager - ***Updating LDAP Server <ldap-server>*** <date-time> <hostname> <metadata> INFO c.l.sws.smc.auth.LDAPAuthProvider - ***LDAP verification succeeded to <ldap-server-fqdn>.*** All appliances: See Configure Audit Behavior. **Configure Audit Behavior:** <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: svc-cm-configuration/1,1506,<timestamp>,<username>,<remote-ip>,1,***Initiated change appliance configuration widget auditLogDestination*** <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: osaxsd/<pid>,1100,<timestamp>,root(0),localhost,1,***System Service syslog has changed these settings: AUDIT_EXT_IP = <audit-server-ip>*** <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: osaxsd/<pid>,1100,<timestamp>,root(0),localhost,1,***System Service syslog has changed these settings: AUDIT_EXT_OCSP_CHECK_MODE = <mode>*** **Configure Cryptographic Functionality:** See FIA_X509_ EXT.1/ITT and FIA_X509_EXT.1/rev regarding any addition, replacement, or removal of trust anchors in the TOE's trust store. Also see Start and Stop Services in this row.

		Configure the interaction between TOE components: See FCO_CPC_EXT.1. **Set the time which is used for timestamps:** See FPT_STM.1 **Configure the Reference Identifier for the Peer:** <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: svc-cm-configuration/1,1507,<timestamp>,<username>,<remote-ip>,1,***SMC: Initiated change appliance configuration widget auditLogDestination*** <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: svc-cm-agent/<pid>,1100,<timestamp>,jetty(996),localhost,1,***SYSLOG updated successfully in the admin context: ['Server: <syslog-server-ip>, Port: <port>, Revocation: <mode>']*** <date-time> <hostname> <metadata> INFO c.l.l.a.c.ldap.LdapConfigManager - ***Updating LDAP Server <ldap-server>*** <date-time> <hostname> <metadata> INFO c.l.sws.smc.auth.LDAPAuthProvider - ***LDAP verification succeeded to <ldap-server-fqdn>.***
		Manage the TOE's trust store and designate X.509v3 certificates as trusted: See FIA_X509_EXT.1/Rev and FIA_X509_EXT.1/ITT. **Import X.509v3 certificates to the TOE's trust store:** See FIA_X509_EXT.1/Rev and FIA_X509_EXT.1/ITT. **Generating/Import of, Changing of, or Deleting of Cryptographic Keys:** <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: svc-cm-configuration-agent/1,5046,<timestamp>,cm-agent,<ip>,1,***Created SSL cryptographic key with SHA256 <checksum> for APPLIANCE identity*** <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: svc-cm-configuration-agent/1,5047,<timestamp>,cm-agent,<ip>,1,***Deleted SSL cryptographic key with SHA256 <checksum> for APPLIANCE identity*** <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: svc-cm-configuration-agent/1,5038,<timestamp>,cm-agent,<ip>,1,***Successfully updated appliance identity. Friendly name: <certificate-name>*** **Resetting Passwords:** <u>Remote Password Change (Manager only)</u> <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: smc-server/1,5035,<timestamp>,<username>,<remote-ip>,1,***Updated user "<username>"*** <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: smc-server/1,2160,<timestamp>,<username>,<remote-ip>,1,***Updated password user "<username>"*** <u>Local Password Change (Other Appliances)</u> <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: osaxsd/<pid>,1100,<timestamp>,root(0),localhost,1,***System Service password has changed these settings: sysadmin = XXXXXX*** <u>Configure password minimum length:</u> <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: svc-cm-configuration/1,1507,<timestamp>,<username>,<remote-ip>,1,***SMC: Initiated change appliance configuration widget passwordPolicy***

		<date-time> <hostname> AuditLogger[<pid>]: AuditLogger: osaxsd/<pid>,1100,<timestamp>,root(0),localhost,1,***System Service password_policy has changed these settings: min_symbols = <n>, expiration_days = <n>, min_lowercase = <n>, min_capitals = <n>, min_numbers = <n>, min_length = <n>, max_length = <n>, diff_chars = <n>, min_days = <n>, hist_num = <n>***
FPT_ITT.1	Initiation of the trusted channel	**TLS Server (for connectivity between appliances):** <date-time> <hostname> <metadata> ***IP address matches presented certificate for connection:*** <ip-address-of-remote-appliance>. **TLS Client (for connectivity between appliances):** <date-time> <hostname> <metadata> ***Presented certificate complies with CC policy.*** while SSL handshaking to upstream, client: <client>, server: localhost, request: <request>
	Termination of the trusted channel functions	**TLS Server (for connectivity between appliances):** <date-time> <hostname> <metadata> ***client <ip-address> closed keepalive connection*** **TLS Client (for connectivity between appliances):** <date-time> <hostname> <metadata> ***client <ip-address> closed keepalive connection***
	Failure of the trusted channel functions	See FCS_TLSC_EXT.21/FCS_TLSS_EXT.1 and FIA_X509_EXT.1/ITT.
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process	**This same message is generated on the Manager and all other appliances:** <date-time> <hostname> chronyd[<pid>]: ***System clock wrong by <seconds> seconds*** <date-time> <hostname> <metadata> ***System clock was stepped by*** <seconds> seconds
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	Initiation: See FMT_MOF.1/ManualUpdate. Success: <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: osaxsd/<pid>,1100,<timestamp>,root(0),localhost,1,***Default system image area is now <image-area>*** <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: svc-cm-update/1,1217,<timestamp>,<username>,<remote-ip>,1,***SWU image <filename>.swu has been installed onto appliance <uuid>*** Failure: <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: svc-cm-update/1,1211,<timestamp>,<username>,<remote-ip>,0,***SWU image <filename>.swu failed to upload to Central Manager. Reason: Invalid Image.***
FTA_SSL.3	Termination of a remote session by the session locking mechanism	<date-time> <hostname> AuditLogger <metadata>,<username>,<remote-ip-address>,1,***The user has logged out***
FTA_SSL.4	Termination of an interactive session	**Remote Logout (Manager only):** <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: svc-token-authority/1,4004,<timestamp>,<username>,<remote-ip>,1,***The user has logged out*** **Local Logout (All Appliances)**

		<date-time> <hostname> AuditLogger[<pid>]: AuditLogger: SystemConfig/<pid>,4004,<timestamp>,sysadmin(75),localhost,1,***The user has logged out of Console***
FTA_SSL_EXT.1	Termination of a local session by the session locking mechanism	**This same message is generated on the Manager and all other appliances:** <date-time> <hostname> AuditLogger[<pid>]: AuditLogger: SystemConfig/<pid>,4005,<timestamp>,sysadmin(75),localhost,0,***The user has been logged out of SystemConfig - the idle timeout was reached.***
FTP_ITC.1	Initiation of the trusted channel	**Syslog Over TLS:** <date-time> <hostname> <metadata> ***Connection established to /<syslog-server-ip> port 6514*** **LDAP Over TLS (applicable to Manager only):** <date-time> <hostname> AuditLogger[<pid>]: svc-legacy-auth/17,4002,<timestamp>,,<remote-ip>,1,***Login Host <ldap-server-ip> verified using Subject Alternative Name successful*** <date-time> <hostname> AuditLogger[<pid>]: svc-legacy-auth/17,4002,<timestamp>,,<remote-ip>,1,***Login Valid SAN from certificate successful*** <date-time> <hostname> <metadata> INFO c.l.sws.smc.auth.LdapSessionFactory - ***TLS connection established to resolved ip address /<ldap-server-ip>.***
	Termination of of the trusted channel functions	**Syslog Over TLS:** <date-time> <hostname> syslog-ng[<pid>]: AuditLogger: syslog-ng/<pid>,4022,<timestamp>,root(0),localhost,1,***Audit log service stopped*** **LDAP Over TLS (applicable to Manager only):** <date-time> <hostname> <metadata> INFO com.lancope.sws.smc.auth.LdapSession - ***TLS connection terminated to*** <ldap-server-fqdn>.
	Failure of the trusted channel functions	**Syslog Over TLS:** See FCS_TLSC_EXT.1 & FIA_X509_EXT.1/Rev. **LDAP Over TLS (applicable to Manager only):** See FCS_TLSC_EXT.1 & FIA_X509_EXT.1/Rev.
FTP_TRP.1/Admin	Initiation of the trusted channel	See FIA_UIA_EXT.1.
	Termination of the trusted channel	See FTA_SSL.4.
	Failure of the trusted channel functions	See FCS_HTTPS_EXT.1.

FTP_TRP.1/Join	Initiation of the trusted channel	See FPT_ITT.1.
	Termination of the trusted channel functions	See FPT_ITT.1.
	Failure of the trusted channel functions	See FPT_ITT.1.

7 Security Services and Protocols

As a network performance monitoring tool, SNA has many processes that are capable of processing incoming network traffic. These processes are briefly described for each appliance, as follows.

Table 12: SNA Appliance Processes

Appliance	Process	Description
Manager	LDAP	This process allows user authentication to happen through an external LDAP or Active Directory provider. The connections are protected by TLS using a port which is configurable by the administrator. The default port for LDAP and AD services is port 636/TCP.
	HTTPS	This is the Nginx process that accepts HTTPS connections on port 443/TCP for Web UI and Client Interfaces, the management channel, and the user data channel from other appliances within the TOE. This process runs with normal user level permissions at ring 3.
	TLS Syslog	This process securely sends logs to an external server using the Syslog protocol over TLS. The default port is 6514/TCP, but it is configurable by the administrator.
Flow Collector	Stealthwatch	This is the engine that accepts NetFlow traffic through the administrator defined ports. The default port is 2055/UDP. This process runs as root as ring 3.
	HTTPS	This is only used for communications with the Manager; all remote administration is disabled for this interface.
	TLS Syslog	This process securely sends logs to an external server using the Syslog protocol over TLS. The default port is 6514/TCP, but it is configurable by the administrator.

Flow Sensor	Flow Sensor	This is the engine that captures packet level traffic from the network as a TAP or SPAN device. This process runs as a root at ring 3.
	HTTPS	This is only used for communications with the Manager; all remote administration is disabled for this interface.
	TLS Syslog	This process securely sends logs to an external server using the Syslog protocol over TLS. The default port is 6514/TCP, but it is configurable by the administrator.

For a complete list of services, protocols and ports used in SNA and refer to the Communication Ports section of [SNA-HIG] or the Communication Ports and Protocols section of [SNA-VEIG].

8 Modes of Operation

The TOE (i.e. SNA 7.5 in its CC-evaluated configuration) has multiple modes of operation; these modes are as follows:

- **Booting** – while booting, the TOE does not allow access to the administrator interfaces until the TOE software and configuration has loaded. This mode of operation automatically progresses to the Normal mode of operation. While booting, the TOE runs power-on self-tests (POST), which includes performing self-tests to confirm cryptographic operations are functioning properly.
- **Normal** - The TOE software and configuration is loaded and TOE is operating as configured. It should be noted that all levels of administrative access occur in this mode and that all TOE security functions are operating.

Following operational error, the TOE reboots (once power supply is available) and enters booting mode. The only exception to this is if there is an error during the Power on Startup Test (POST) during bootup, then the TOE will shut down.

9 Security Measures for the Operational Environment

Proper operation of SNA 7.5 in its Common Criteria certified configuration, i.e. the Target of Evaluation (TOE), requires that some security objectives be satisfied by the operational environment. It is the responsibility of the authorized administrator of the TOE to ensure that the Operational Environment provides the necessary functions and adheres to the environment security objectives listed below. The environmental security objective identifiers map to the environmental security objectives as defined in the certified Security Target (ST) document.

Table 13 Operational Environment Security Measures

Environment Security Objective (from NDcPP)	IT Environment Security Objective Definition (from NDcPP)	Administrator Responsibility
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment	The SNA appliances are assumed to be physically protected in their operational environment and not subject to physical attacks that compromise the security of, and/or interfere with, the device's physical interconnections and correct operation.
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 its own VM, and does not include other VMs or the VS.	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing.
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.	A standard, generic network device does not provide any assurance regarding the protection of traffic that traverses it.
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. 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.	The administrators for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords and credentials have sufficient strength, entropy, and lack malicious intent when administering the device.
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.	The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to 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.	The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
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	The availability of all TOE components, including their audit functionality, is maintained to reduce the risk of an undetected attack on (or

	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.	failure of) one or more TOE components.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.	The administrator must ensure that there is no unauthorized access possible for sensitive residual information (cryptographic keys, keying material, PINs, passwords, etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
OE.VM_CONFIGURATION	For vNDs, the Security Administrator ensures that the VS and VMs are configured to • reduce the attack surface of VMs as much as possible while supporting ND functionality (e.g., remove unnecessary virtual hardware, turn off unused inter-VM communications mechanisms), and • correctly implement ND functionality (e.g., ensure virtual networking is properly configured to support network traffic, management channels, and audit reporting). The VS should be operated in a manner that reduces the likelihood that vND operations are adversely affected by virtualization features such as cloning, save/restore, suspend/resume, and live migration. If possible, the VS should be configured to make use of features that leverage the VS's privileged position to provide additional security functionality. Such features could include malware detection through VM introspection, measured VM boot, or VM snapshot for forensic analysis.	The administrator must ensure the hardening of the virtualization environment by minimizing the attack surface and ensuring the robust configuration of networking, management, and audit functions. They must mitigate operational risks associated with virtualization features like live migration and cloning, while actively leveraging the system's privileged position to implement advanced security measures such as VM introspection, measured booting, and forensic snapshotting.

10 Appendix

10.1 Acronyms and Terms

This section defines the acronyms and terms.

Acronym	Definition
AIDE	Advanced Intrusion Detection Environment
API	Application Programming Interface
CA	Certificate Authority
CC	Common Criteria
CLI	Command Line Interface
CSR	Certificate Signing Request
CSV	Comma-Separated Values
DNS	Domain Name Service
FC	Flow Collector
FIPS	Federal Information Processing Standard
FP	FIPS Provider (cryptographic implementation), formerly FOM
FS	Flow Sensor
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
ISE	Identity Services Engine
ISO/IEC	International Organization for Standardization (ISO) International Electrotechnical Commission (IEC)
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
NDcPP	collaborative Protection Profile for Network Devices
NTLM	New Technology LAN Manager
OS	Operating System
PAM	Pluggable Authentication Module
PEM	Privacy Enhanced Mail
PINs	Personal Identification Numbers
RFD	Reset Factory Defaults
RSA	Rivest, Shamir, and Adelman (a public-key cryptographic system)
SKU	Stock Keeping Unit
SMC	SNA Management Console *Note: Starting with v7.4.0, the SMC was renamed to "Manager" though appliance part numbers, and installation/update filenames for version 7.5 still contain the acronym "SMC".*
SPAN	Switched Port Analyzer
SSL	Secure Sockets Layer
TACACS	Terminal Access Controller Access Control System
TAP	Test Access Port
TCP	Transmission Control Protocol
TLS	Transport Layer Security

TOE	Target of Evaluation
UDP	User Datagram Protocol
UI	User Interface
WebUI	Web User Interface (same as GUI)

10.2 Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco SNA Support
- To open a case by web: http://www.cisco.com/c/en/us/support/index.html
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers:

https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwidecontacts.html

10.3 Copyright Information