Ciena SAOS R10.9.1 on the 3926 with Large NFV Compute Server Service Aggregation Platform

CC Guidance Supplement

Version: 1.1
Date: 17 February 2025

Prepared By:
Ciena Corporation
7035 Ridge Rd,
Hanover, MD 21076

Revision History

Version	Date	Change
0.1	May 21, 2024	Initial Version
0.2	June 21, 2024	Added MACSEC section
0.3	October 9, 2024	Updated based on gossamer v2 comments
0.4	November 12, 2024	Corrected Figure 1
0.5	November 26, 2024	Updated auditable events and updated TOE naming to be consistent with the ST
1.0	January 29, 2025	Addressed checkout review comments
1.1	February 17, 2025	Addressed additional checkout review comments

List of Tables

1 Introduction

This document provides supporting evidence of an evaluation of a specific Target of Evaluation (TOE), Ciena SAOS R10.9.1 on the 3926 with Large NFV Compute Server Service Aggregation Platform. This Operational User Guidance with Preparative Procedures addresses the administration of the TOE software and hardware and describes how to install, configure, and maintain the TOE in the Common Criteria evaluated configuration.
This Operational User Guidance with Preparative Procedures documents the administration the Ciena SAOS R10.9.1 on the 3926 with Large NFV Compute Server Service Aggregation Platform. The TOE is comprised of both software and hardware. The hardware is comprised of the following model series: 3926 and Large NFV Compute Server.

1.1 Audience

This document is intended for users, such as network technicians and system administrators, who will install the 3926 into a packet networking environment.
It assumes that the intended users possess basic knowledge of, but not limited to:

- Proper hardware installation
- Proper hardware diagnostics
- Ethernet concepts
- IEEE standards
- IETF standards
- Open Systems Interconnection (OSI) Seven Layer Model
- Local Area Networks (LAN)
- Virtual Local Area Networks
- Ethernet Passive Optical Networks (EPON)

1.2 Purpose

This document is the Operational User Guidance with Preparative Procedures for the Common Criteria evaluation. It was written to highlight the specific TOE configuration and administrator functions and interfaces that are necessary to configure and maintain the TOE in the Common Criteria evaluated configuration. The evaluated configuration is the configuration of the TOE that satisfies the requirements as defined in the Security Target (ST). This document covers all of the security functional requirements specified in the ST and as summarized in Section 3 of this document. This document does not mandate configuration settings for the features of the TOE that are outside the evaluation scope, such as information flow polices and access control, which should be set according to your organizational security policies.

This document is not meant to detail specific actions performed by the administrator but rather is a road map for identifying the appropriate locations within Cisco documentation to get the specific details for configuring and maintaining C8000 operations. All security relevant commands to manage the TSF data are provided within this documentation within each functional section.

1.3 Document References

This section lists the Ciena Systems documentation. All documents are posted on the NIAP website along with the CC certificate NIAP: Product Compliant List (niap-ccevs.org).

AGD[1] *Ciena SAOS R10.9.1 on the 3926 with Large NFV Compute Server Service Aggregation Platform CC Guidance Supplement*
AGD[2] *3926_10.9.1_security*
AGD[3] *3926_10.9.1_administration*
AGD[4] DNFVI_10.9.1_installation

1.4 Acronyms

Table 1: Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
DHCP	Dynamic Host Configuration Protocol
HTTPS	Hyper-Text Transport Protocol Secure
IT	Information Technology
NACM	NETCONF/YANG access control model
NDcPP	collaborative Protection Profile for Network Devices
OS	Operating System
PP	Protection Profile
SAOS	Service Aggregation Operating System
ST	Security Target
TCP	Transmission Control Protocol
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy

2 The TOE and the Operational Environment

2.1 Assumptions

- The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
- 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. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).
- A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
- The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.

  For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
- 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.
- The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
- The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

2.2 Security Measures for the Operational Environment

Proper operation of the TOE requires functionality from the 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.

Table 2: IT Environment Security Objectives

IT Environment Security Objective Definition	Administrator Responsibility
Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment	Administrators must ensure the TOE is installed and maintained within a secure physical location. This can include a secured building with key card access or within the physical control of an authorized administrator in a mobile environment.
There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.	Administrators will make sure there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE.
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.	None
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.	Administrators must be properly trained in the usage and proper operation of the TOE and all the provided functionality per the implementing organization's operational security policies. These administrators must follow the provided guidance.
The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.	Administrators must regularly update the TOE to address any known vulnerabilities.
The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.	Administrators must protect their access credentials where ever they may be.
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.	Administer must follow guidance on how to securely protect sensitive residual information on equipment discarded or removed.

2.3 TOE Overview

The TOE is Ciena SAOS R10.9.1 on the 3926 with Large NFV Compute Server Service Aggregation Platform. It is a non-distributed, non-virtual network device which implements routing and switching functionalities for enterprise, mobility, and converged network architectures. In these architectures, the TOE can be deployed in the access, aggregation, or core of the network. The TOE uses a Linux based container architecture for its SAOS Network Operating System and includes the SAOS 10.9.1 operating system executed on the Ciena SAOS R10.9.1 on the 3926 with Large NFV Compute Server Service

Aggregation Platform. The TOE implements the general functionality of a router/switch consistent with the collaborative Protection Profile for Network Devices v2.2E and MACSEC consistent with Protection Module for MACSEC Ethernet Encryption Version 1.0. The TOE implements controlled connectivity between two subnetworks and a management interface. All network traffic between the connected subnetworks is controlled by the TOE and the authorized administrators may manage the TOE using the management interface.

The management interface is a Command Line Interface (CLI) which may be accessed locally or remotely. Local access is via a console port which is a Serial EIA-561 (RJ-45) or a USB-C port. It allows management of the TOE from a workstation physically connected to the TOE. Remote management is over Secure Shell (SSH). SSH implements a secure remote login over a network connection and allows protected CLI and Network Configuration Protocol (NETCONF) access to the TOE.

All administrators are identified and authenticated using a username and password or based on SSH public key authentication. Access is only granted, and the user assigned to the role administrator upon successful authentication. Authentication is implemented locally. Authentication of TLS peers is done using X.509 Public Key Certificates. The validity of the X.509 public key certificates is verified using the Online Certificate Status Protocol (OCSP).

In addition to the management ports for local and remote access by the administrators, the variants of the TOE also implement a different number of network ports for the interconnection of different subnetworks. The network ports are physically separate from the management ports and administrative access may not take place from the network interconnection ports.

The TOE does not protect the data flowing through itself. The TOE is only to be deployed in a secure data center and to only be physically accessible by trusted administrators. Administrators are trusted to operate the TOE in accordance with the security guidance at all times and not attempt to circumvent or suppress the security functions and mechanisms of the TOE.

2.4 TOE Description

2.4.1 TOE Hardware

The TOE is the Ciena SAOS 10.9.1 software executed on the 3926 Service Aggregation Platform and Large NFV FRU summarized in the following Table. The same software is executed on each platform. The various models of the TOE differ in performance and number of ports, but all run the same OS version 10.9.1 software. The TOE is available in two form factors:

1. A rack-mount appliance with a variable number of replaceable modules or 'blades', and
2. Large NFV Compute Server, a field-replaceable unit (FRU) housed in the 3926

Table 3: TOE Hardware Platforms

Models/Platform	1G/10G SFP+	Processors	Power Options
3926	6	4x1.5GHz ARM Cortex A53	AC, DC
Large NFV compute server (FRU)	--	Intel XEON D1548, 8CORE	--

2.5 The Evaluated Configuration

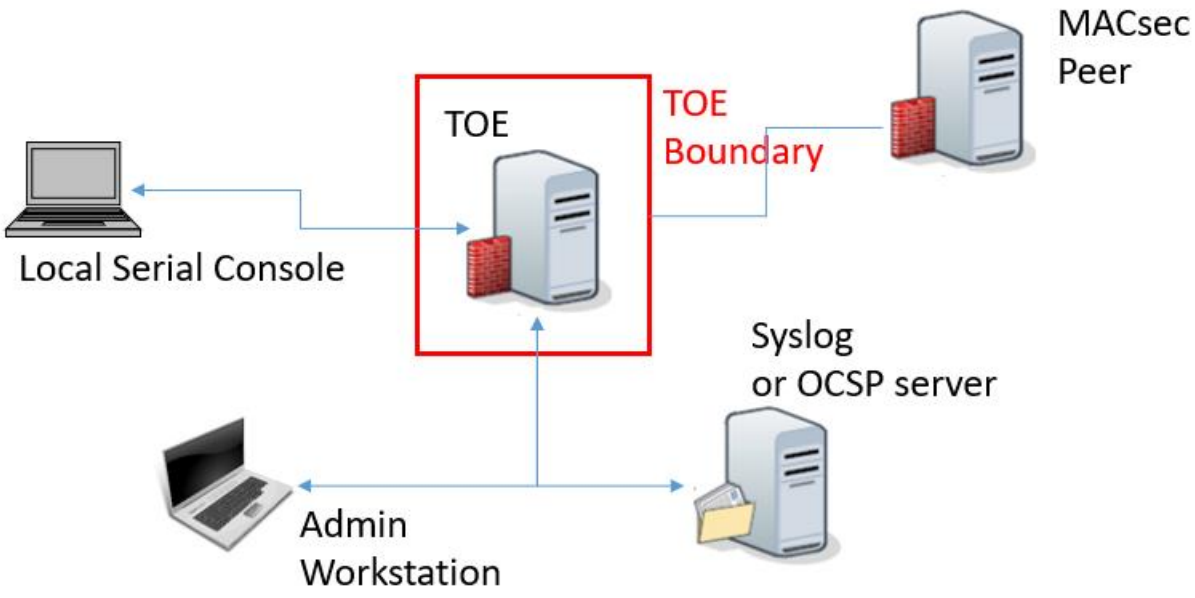
The TOE is the complete network appliance, or a Large NFV Compute Server comprised of TOE software, TOE hardware and TOE security guidance:

- TOE software is Ciena SAOS 10.9.1,
- TOE hardware is MACsec on the 3926 Service Aggregation Platform and Large NFV FRU, and
- The TOE security guidance is the *Ciena SAOS R10.9.1 on the 3926 with Large NFV Compute Server Service Aggregation Platform CC Guidance Supplement*

The TOE is deployed in an environment that includes the IT components illustrated in the following figure. The TOE itself is delivered as an appliance or an FRU with the software installed. The administrator of the TOE may verify the TOE software and, if necessary, download and install the correct version.

The physical boundary of the TOE is illustrated below. The TOE implements a TLS Client and SSH Server for secure connectivity to the components of the environment. Each component of the environment is required to implement the corresponding client and/or server. The remote management workstation is required to implement a SSH Client for accessing the TOE, and the audit server must include a TLS Server for which the TOE can connect using the TLS Client.

Figure 1: TOE Boundary and Operational Environment



The environmental components described below are required to operate the TOE in the evaluated configuration.

Table 4: Environmental Components

Component	Purpose/Description
Audit server (Mandatory)	The audit server supports syslog messages over TLSv1.2 to receive the audit files from the TOE. The audit data is stored in the remote audit server for redundancy purposes.
OCSP Server (Mandatory)	Validity of the certificates the TOE uses for asserting the authenticity of the TLS peers is verified using OCSP. Communication with an OCSP Server is over HTTP.
Management Workstation (Mandatory)	A workstation used by an administrator to manage the TOE locally or remotely. The remote management station must include a SSHv2 client.

2.5.1 Product Functionality not Included in the Scope of the Evaluation

The following product functionality is not covered by the evaluation:

- Telnet is not included and must be disabled.
- Telemetry Client must not be used.
- SNMP is not evaluated and must be disabled.
- FTP to upload or download files/configuration is not evaluated and must be disabled.

3 SECURE ACCEPTANCE OF THE TOE

In order to ensure the correct TOE is received, the TOE should be examined to ensure that it has not been tampered with during delivery.

- Verify that the TOE software and hardware were not tampered with during delivery by performing the following actions.
- Personnel involved in installation must be trained in and have experience with router installations.
- Follow site standards regarding system weight when unpacking and maneuvering the chassis.
- Inspect the shipping container for physical damage. If any components of the chassis are found to be damaged, use the instructions in “Return of materials”, shipped with the chassis, to return the damaged items to Ciena.

Requirements

The chassis has a modular and scalable design that enables flexibility for various deployment and future upgrade scenarios.

The following table provides the ordering information for the selectable parts necessary to complete the chassis.

Table 5: Selectable Parts

Part number	Description	Notes
170-3926-905	3926, MACSEC, (2) 100 MbE/1GbE SFP, (6) 10/1 GbE SFP+,(1) OPTION SLOT, SAOS 10.X,EXT. TEMP, (2) SLOTS AC/DCPWR SUPRouter, Base unit (MACsec model)	Chassis Note: Port 7 and port 8 supports MACsec functionality.
170-0014-900	AC PLUGGABLE POWER SUPPLY, WIDE RANGE 120/240VAC power supply unit	Power units can be AC or DC, however, the combination of AC and DC units in the same chassis is not supported.
170-0013-900	DC PLUGGABLE POWER SUPPLY, WIDE RANGE 24/48VDC power distribution unit	
The AC power variant of the chassis requires an AC power cable that matches the local requirements for your installation site. The AC power supplies have an IEC C14 power connector. To connect properly, an AC power cord must end with an IEC C13 or a Universal C13 power connector.		
170-0111-900	AC POWER CORD, IEC C13, AUTO LOCK, AUSTRALIA, TYPE I	Australia
170-0112-900	AC POWER CORD, IEC C13, AUTO LOCK, SWITZERLAND, TYPE J	Switzerland
170-0113-900	AC POWER CORD, IEC C13, AUTO LOCK, EUROPE, TYPE F	Europe
170-0114-900	AC POWER CORD, IEC C13, AUTO LOCK, NORTH AMERICA, TYPE B	North America
170-0115-900	AC POWER CORD, IEC C13, AUTO LOCK, UNITED KINGDOM, TYPE G	United Kingdom
170-0116-900	AC POWER CORD, IEC C13, AUTO LOCK, UNIVERSAL IEC C14	Universal

	SFP and SFP+ optic modules	
	Faceplate cabling	Cat-5E STP and cabling to match SFP and SFP+ connectors.

Table 6: Optional and Replacement Parts

Part number	Description	Notes
170-0602-903	19 INCHES RACK MOUNT EARS,FOR USE W/ 1RU CHASSIS,INCLUDES CABLE MANAGEMENT BRACKETS	The chassis ships with a 19-inch rack mount kit. All kits include mounting brackets, cable management brackets, and screws.
170-0354-900	21 INCHES ETSI RACK MOUNT EARS	
170-0603-903	23 INCHES RACK MOUNT EARS,FOR USE W/ 1RU CHASSIS,INCLUDES CABLE MANAGEMENT BRACKETS	
FRU modules for standard and MACsec models		
170-0176-900	3926, (6) DS1/E1, (4) DS3/E3 AND (4) OC3/12 STM1/4 OR (1) OC48/STM16 TDM MODULE	For proper cooling, the FRU bay must be populated with a FRU module or the included FRU filler cover.
170-0184-900	(16)1GE MODULE	
170-0121-901	SMALL NFV COMPUTE SERVER FRU FOR 3906MVI & 3926, BROADWELL D-1508, 8GB RAM, 120GB SSD	
170-0122-901	MEDIUM NFV COMPUTE SERVER FRU FOR 3906MVI & 3926, BROADWELL D-1527, 16GB RAM, 120GB SSD	
170-0122-903	MEDIUM NFV COMPUTE SERVER FRU FOR 3906MVI & 3926, BROADWELL D-1527, 16GB RAM, 480GB SSD	
170-0128-900	LARGE NFV COMPUTE SERVER FRU FOR 3906 & 3926, BROADWELL D-1548, 16GB RAM, 120GB SSD	
170-0128-901	LARGE NFV COMPUTE SERVER FRU FOR 3906MVI & 3926, BROADWELL D-1548, 32GB RAM, 480GB SSD	
170-0128-903	LARGE NFV COMPUTE SERVER FRU FOR 3906MVI/3926, BROADWELL D-1548, 64GB RAM, 1.9TB SSD	

Overview

The following items are shipped:

- 3926 chassis mounting bracket kit for a four-post, 19-inch rack which contains:
  - two brackets
  - two cable supports

- six 8-32 x 0.250-inch length flat head Phillips screws used to attach the brackets to the side of the chassis

- ten 8-32 x 0.250-inch length truss head Phillips screws used to attach the sliding inner track brackets to the side of the chassis
- two 8-32 x 0.500-inch length pan head Phillips screws used to attach the cable guides

Steps

- Verify the shipping container contents against the shipping invoice.
- Compare the labels on the shipping containers with the information on the packing list.
- Record any discrepancies.
- Remove the cardboard box and zip lock bag from the shipping container. Carefully lift the chassis out of the cardboard box.
- Remove the foam block from the chassis.
- Remove the chassis out of the ESD bag.
- Ensure that the shipping container is empty.
- Dispose of shipping container in accordance with site requirements.

If there are **Then** discrepancies and/or missing components notify Ciena® Global Product Support and have the following information available:

- shipping invoice number
- model and serial number of the damaged item
- description of the discrepancy
- effect of the discrepancy on the installation

Inspecting for damage

- Lists documents to review prior to installation.
- Reviews chassis and rack requirements.
- Reviews clearances required for proper ventilation.
- Describes proper handling procedures for the chassis.

Required documents are:

- Installation Specification (IS) and Bill of Materials (BOM)
- Regional, customer, and site-specific regulatory, installation, and safety Requirements.
- Ciena® Standard Cleaning and Equipment Safety Practices (009-2003- 121)
- Ciena® Installation Workmanship Standards (009-7B03-000)
- Telcordia Electromagnetic Compatibility and Electrical Safety GR-1089-CORE
- Telcordia Generic Installation Standards GR-1275 CORE
- European Telecommunications Standards Institute (ETSI) 300 119

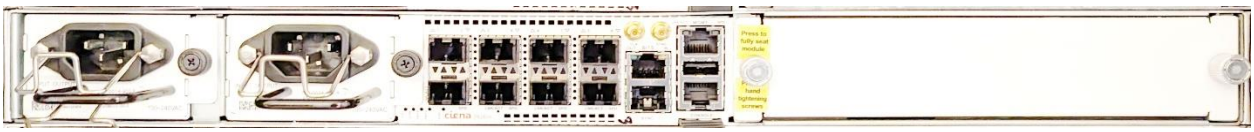
Equipment Engineering

- European Telecommunication Standard for equipment practice

Chassis size and installation options

- The chassis occupies one rack unit (RU) of a standard 19-inch equipment rack.
- The chassis is designed so that all interface cabling connections are located on the front faceplate.

Figure 2: Sample TOE



Airflow and installation clearance requirements

The chassis contains five hot-swappable fan trays, visible from the back of the chassis. These fans draw fresh air through the inflow vents on the front of the chassis and exhaust it at the rear of the chassis. Ensure that air vents on the front and rear of the chassis are not obstructed in any way. To provide sufficient clearance for cabling and airflow, ensure that the following clearances recommended by NEBS are provided:

- Front of chassis: 3 in. (8 cm)
- Rear of chassis: 3 in. (8 cm)

Required tools and equipment

The following tools and equipment are required whenever handling the chassis and must be available at the installation site:

- ESD-guard wrist strap
- ESD-guard heel grounders
- A Phillips screwdriver of suitable size to accommodate the rack screws
- Flat head screwdriver
- Anti-static bag or anti-static box

3.1 Physical Installation of the TOE

Follow AGD[2] 3926_10.9.1_security for hardware installation for all models except the DNFVIs. For those models, follow AGD[4] DNFVI_10.9.1_installationfor installation.

3.2 Default Crypto Configuration

The system is automatically configured to support the values identified in the Security Target.

Specifically, the following values are automatically supported and therefore do not require any action by the administrator to define or configure what is supported by the TOE.

- Supports the selected key generation scheme(s) and key size(s) for all cryptographic protocols defined in the Security Target (FCS_CKM.1).
- Supports the selected key establishment scheme(s) for all cryptographic protocols defined in the Security Target (FCS_CKM.2).
- Supports the selected modes and key size(s) defined in the Security Target supported by the TOE for data encryption/decryption (FCS_COP.1/DataEncryption).
- Supports the selected cryptographic algorithm and key size defined in the Security Target supported by the TOE for signature services (FCS_COP.1/SigGen).

- Supports the selected hash sizes for all cryptographic protocols defined in the Security Target (FCS_COP.1/Hash).
- Supports the values used by the HMAC function: key length, hash function used, block size, and output MAC length used defined in the Security Target supported by the TOE for keyed hash function (FCS_COP.1/KeyedHash).
- Supports the RBG functionality specified in the Security Target (FCS_RBG_EXT.1).

TOE destroys plaintext cryptographic keys stored in volatile storage by a single overwrite with zeroes. Plaintext keys stored in the non-volatile storage are destroyed by the SAOS overwriting the storage location of the key with a single overwrite of zeroes.

The above key destruction methods apply to all configurations and circumstances, except one. The only situation where the key destruction may be prevented would be if the system suffers a crash or loss of power. This situation only impacts the keys that are stored in the filesystem. Since the TOE is inaccessible in this situation, administrative zeroization cannot be performed. The keys stored in filesystem are not directly accessible to any user or administrator.

4 ACCESSING THE TOE

System access to the system can be established by means of:

- console port. The console port is used to access the system by means of a laptop PC. The serial console port is a Serial EIA-561 (RJ-45) or USBC port. The console port allows for local CLI access to the system (Section 4.1).
- Secure Shell (SSH). SSH provides remote login for remote CLI access to the system and perform SFTP file transfers. SSH verifies and grants access to login requests by encrypting user ID and passwords or through public key encryption. SSH/SFTP is supported over IPv4 (Section 5).

4.1 CONSOLE CONNECTION

4.1.1 CONSOLE ADMINISTRATION RJ-45

Log in through the RJ-45 CONSOLE port to establish a CLI session through the console port.

Table 7: Cable required to connect to console port

System	Console port	Cable
MACsec on the 3926 Service Aggregation Platform and Large NFV FRU	RJ-45	null modem cable with a male DB-9 connector on the PC side and a male RJ-45 cable to connect to the RJ-45 connector on the side

Ensure that the system is:

- properly grounded and installed
- powered on

Overview

The following table lists the terminal settings to use when configuring the connected terminal for all systems.

Table 8: Terminal settings

Terminal setting	Value
Character size	8
Parity	None
Stop bit	1
Control	None

The following table lists the baud rate for the terminal by system.

Table 9: Baud rate by system

System	Baud Rate
3926	9600 bps

Note: Configuration changes are immediately saved to the running configuration.

Steps

1. Plug the RJ-45 end of the Null modem cable into the CONSOLE port.
2. Connect a terminal or PC running terminal emulation software to the CONSOLE port using the recommended cable.

Note: The serial console port does not support connectivity to a modem.

3. At the prompt, configure the connected terminal.
4. When the login prompt is displayed, press Enter and enter the default username and password.
5. Access the configuration CLI:
   ```
   config
   ```

Example

The following command logs in as the default user.

```
login: diag
Password: ciena123

System response:
!!! This is a private network. Any unauthorized access or use will lead to
prosecution!!!
SAOS. The next generation in switching software.
```

Example

The following command logs in as the default user.

```
login: diag
Password: ciena123
System response:
!!! This is a private network. Any unauthorized access or use will
lead to prosecution!!!
SAOS. The next generation in switching software.
```

4.1.2 Configure the Hostname

Set the system hostname. The new hostname is displayed after the next login.

Requirements

This procedure is performed from the user context node.

Overview

The following table lists the parameter for setting the system hostname.

Table 10: Parameter for setting the system hostname

Parameter	Valid values	Description
hostname	string	The system hostname is a string of up to 253 characters.

Steps

1. Access configuration mode:
   ```
   config
   ```
2. Set the system hostname:
   ```
   system config hostname <hostname>
   ```

Example

The following example sets the system hostname to system2.

```
config
system config hostname system2
```

4.1.3 BOOT VERIFICATION

- If required, retrieve and install the correct software load from the ManifestURL.
  - If the manifest specifies a new base OS, then the installation of new software will involve a system reboot to load the new base OS.
  - After the correct base OS is running, the remaining software is updated to the correct software load from the ManifestURL.
- Applies the user configuration.

- Use the show software command to display information about the router, including image names, uptime, and other system information.
  ```
  CGSI3926> sh software
  ```

5 Configuring the Remote Management Interface (SSHv2)

The TOE only implements SSHv2 to support remote client administrative management. The TOE implements a SSH server which allows SSHv2 connection between a remote management station and the TOE. A CLI which implements the management interface of the TOE is available to a remote administration over an encrypted SSHv2 channel. The remote users (remote administrator) must initiate connection to the TOE using the SSH Client of the remote management station.

The default configuration of the SSH servers supports a more permissive set of SSH connection settings than the TOE's evaluated configuration, so it is necessary to configure a restriction of the settings in order for the product to be in its evaluated configuration.

- The TOE implements both public key authentication and password-based authentication. Public key authentication methods supported are ssh-rsa, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, and ecdsa-sha2-nistp521. Any other authentication algorithm requests are rejected (Section 5.2.3). The TOE at initialization of the console port, is configured with a username and password authentication. Configuring publickey is optional.
- The TOE examines all packets for size and drops any packets greater than 32768 bytes accordance with RFC 4253. This packet size is the default value and does not need to be configured.

The remaining parameters must be configured to get the TOE in the evaluated configuration.

- For symmetric encryption, the TOE allows aes128-ctr, aes256-ctr, aes128-gcm@openssh.com, and aes256-gcm@openssh.com. Requests for any other algorithms are rejected (Section 5.2.4)
- For SSH transport implementation, the TOE allows hmac-sha1, hmac-sha2-256, hmac-sha2-512 and implicit. Requests for any other algorithms are rejected. We need to enable the same on TOE (Section 5.2.5).
- The SSHv2 implementation of the TOE enforces to only allow the diffie-hellman-group14-sha1, ecdh-sha2-nistp256, diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, ecdhsha2-nistp384, ecdh-sha2-nistp521 key exchange methods. We need to enable the same on TOE (Section 5.2.6).
- The TOE implements Time-based rekey as well as traffic based rekey. For both traffic-based rekeying and time-based rekeying, the TOE rekeys for the administrative configured value. The TOE will begin re-key based upon the first threshold reached (Section 5.2.7 and Section 5.2.8).

5.1 Configure Remote Interface and Administration Protocols

Configure a remote management interface to provide an IP connection to the system.

Overview

Up to two remote management interfaces are permitted.

Table 11: Parameters for configuring the remote management interface.

Parameters	Valid values	Description
name	remote	Specifies the remote interface.
role	management	Specifies the role of the interface.
admin-status	true | false	Allows the remote interface to be administratively shut down (disabled).
mtu_size	64..9216 Default: 1514	Specifies the maximum transmission unit (MTU) size.
type	ip	For an L3 interface select ip or loopback ***Note:*** The evaluated configuration requires the remote interface to be of type ip
fd_name	string	Specifies the forwarding domain name for the underlay binding.
ip_address	IP address	Specifies the IP address to assign to the interface
ip_version	ipv4 | ipv6	Specifies whether the IP address is an IPv4 or IPv6 address.
prefix_length	1..32 for IPv4, 1..128 for IPv6	Specifies, in bits, the length of the subnet prefix for the specified IP address.

Steps

1. Enter configuration mode:
   `config`
2. Create the remote interface:
   `oc-if:interfaces interface remote config role management mtu <mtu_size> admin-status true type ip`
3. Specify the forwarding domain for the underlay binding:
   `oc-if:interfaces interface remote config underlaybinding fd <fd_name>`
4. Assign an IP address and set the prefix length:
   `oc-if:interfaces interface remote <ip_version> addresses address <ip_address> config ip <ip> prefix-length <prefix_length>`

Example

The following example creates a remote interface with an IPv4 address on the default forwarding domain, remote-fd. All traffic received on VLAN 127 is forwarded to the interface named remote.

```
oc-if:interfaces interface remote config role management mtu 1500
admin-status true type ip
oc-if:interfaces interface remote config underlay-binding fd remote-fd
oc-if:interfaces interface remote ipv4 addresses address 10.10.10.10
config ip 10.10.10.10 prefix-length 32
```

5.2 SSH Public Key Configuration

Install an SSH user public key on the SSH server to authenticate and initiate connection with the SSH client.

Overview

Public keys are stored on the system at /mnt/secure/ssh-server/users as <user>.pub. If the downloaded public key uses the SSH2 format, then it is converted to the openSSH format and stored on the system. After conversion the downloaded SSH2 format public key is deleted.

5.2.1 Installing an SSH User Public Key

The following table describes the parameters for installing an SSH user public key.

Table 12: Parameters for installing an SSH user public key

Parameter	Valid values	Description
user	string	Specifies the shell user for whom the public key is being installed.
filename	filepath	Specifies the path to the public key file.
server-type	ftp-server | http-server	Specifies a list of supported servers to download the public key.
address	IPv4 address Format: x.x.x.x	Specifies the host IP. ***Note:*** the device accepts both IPv4 and IPv6 as input parameters. The evaluated configuration requires only IPv4.
login-id	string	Specifies the login ID of the download server.
password	string	Specifies the password of the download server.
url	string	Specifies the transfer protocol, IP address/ hostname, port, path to the public key file, user name, and password.

Steps

1. Install an SSH user public key.

```
system ssh-server user-pubkey install user-name <user> filename
<filename> [server-type <server-type>] address <address> [login
<login-id> password
<password>]
OR
system ssh-server user-pubkey install user-name <user> url <url>
```

Example

The following examples installs an SSH user public key using the individual parameters of the command.

```
system ssh-server user-pubkey install user-name diag filename
/home/ubuntu/opensshKey.pub server-type ftp-server address 192.0.2.2 login
diag password diag
```

The following examples installs an SSH user public key using the URL parameter.

```
system ssh-server user-pubkey install user-name diag url
http://192.0.2.2:8000/rsa_diag.pub
```

5.2.2 Enabling SSH Public Key Authentication

Enable SSH public key authentication to enable logging on to an SSH server using a public/private key pair.

Overview

The following table describes the parameter for enabling SSH public key authentication.

Table 13: Parameter for enabling SSH public key authentication

Parameter	Valid values	Description
public-key-authentication	enabled | disabled	Sets the state of public key authentication.

Steps

1. Enter configuration mode:
   ```
   config
   ```
2. Enable SSH public key authentication.
   ```
   system ssh-server config public-key-authentication <public-key-
   authentication>
   ```

Example

The following example enables SSH public key authentication.

```
config
system ssh-server config public-key-authentication enabled
```

Note: Disabling SSH public key authentication will take the TOE out of its evaluated configuration.

5.2.3 Configure the PKA authentication Implementation

Configure PKA authentication algorithm.

Table 14: Parameter for configuring the PKA Algorithms

Parameter	Valid Values	Description
pka-algoritm	ssh-rsa, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521	Specifies the pka algorithms. ***Note***: the evaluated configuration requires this parameter to be the values listed in the Valid Values column.

Steps

1. Enter configuration mode:
   `config`
2. Enable SSH public key authentication.
   `system ssh-server config pka-algorithm <pka-algorithm>`

Example

The following command enables SSH public key authentication:

```
config
system ssh-server config pka-algorithm ssh-rsa ecdsa-sha2-nistp256
ecdsa-sha2-nistp384 ecdsa-sha2-nistp521
```

5.2.4 Configure Encryption Algorithms

Configure the encryption algorithms to allow the specific encryption algorithms to be used during the SSH handshake.

Table 15: Encryption Algorithm Parameters

Parameter	Valid Values	Description
encryption-algorithm	aes-128-ctr, aes-256-ctr, aes128-gcm-openssh.com, aes256-gcm-openssh.com	Specifies the encryption algorithms. ***Note***: the evaluated configuration requires this parameter to be configured to the values listed in the Valid Values.

Steps

1. Enter configuration mode:
   `config`
2. Configure encryption algorithms.
   `system ssh-server config encryption-algorithm <encryption-algorithm>`

Example

The following command configures the SSH encryption algorithms in the evaluated configuration.

```
config
```

```
system ssh-server config encryption-algorithm aes-128-ctr aes-256-ctr
aes128-gcm-openssh.com aes256-gcm-openssh.com
```

5.2.5 Configure MAC Algorithms

Configure the MAC algorithms to provide message authentication.

Table 16: MAC Algorithm Parameters

Parameter	Valid Values	Description
mac-algorithm	hmac-sha2-256, hmac-sha2-512, hmac-sha1	Specifies the MAC algorithms. ***Note***: the evaluated configuration requires this parameter to be configured to the values listed.

Steps

1. Enter configuration mode:
   ```
   config
   ```
2. Configure key exchange algorithms.
   ```
   system ssh-server config mac-algorithm <mac-algorithm>
   ```

Example

The following command configures the SSH MAC algorithms in the evaluated configuration.

```
config
system ssh-server config mac-algorithm hmac-sha2-256-etm hmac-sha2-512-
etm hmac-sha1
```

5.2.6 Configure Key Exchange Algorithms

Configure Key Exchange algorithms to allow the specific key exchange algorithm to be used during the SSH handshake.

Table 17: Key Exchange Algorithm Parameters

Parameter	Valid Values	Description
kex-algorithm	ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group14-sha1, diffie-hellman-group14-sha256, diffie-hellman-group16-sha512	Specifies the key exchange algorithms. ***Note***: the evaluated configuration requires this parameter to be configured to the values.

Steps

1. Enter configuration mode:
   ```
   config
   ```

2. Configure key exchange algorithms.
   ```
   system ssh-server config kex-algorithm <kex-algorithm>
   ```

Example

The following command configures the SSH key exchange algorithms in the evaluated configuration.

```
system ssh-server config kex-algorithm ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group14-sha1 diffie-hellman-group14-sha256 diffie-hellman-group16-sha512
```

5.2.7 Configure the Rekey Time

Configure the rekey time to specify the maximum amount of time in seconds after which the session key can be renegotiated.

Table 18: Rekey Time Parameters

Parameter	Valid Values	Description
rekey-time	3600	Specifies the time between SSH session key renegotiations. Rekey is measured in seconds. ***Note***: the evaluated configuration requires this parameter to be configured to 3600

Steps

1. Enter configuration mode:
   ```
   config
   ```
2. Configure the rekey time.
   ```
   system ssh-server config rekey-time <rekey-time>
   ```

Example

The following command configures the SSH rekey time to the evaluated configuration.

```
config
system ssh-server config rekey-time 3600
```

5.3 Idle Session Termination

The evaluated configuration requires the Administrator to set a session termination configuration for an SSH session that has been inactive for an Administrative configurable amount of time. This configuration will apply to both the console and remote administrative logins. To set the SSH idle timeout perform the following command.

Steps

1. Enter configuration mode:
   ```
   config
   ```
2. Set the SSH idle timeout:
   ```
   system ssh-server config timeout <1-65535>
   ```

Example

The following example command sets the SSH idle timeout to one minute, that is, 60 seconds.

```
config
system ssh-server config timeout 60
```

Note: Despite the name of this command, this applies to the console port also.

6 CONFIGURING TLS COMMUNICATION

The TOE communicates with the syslog server using TLS. Configuration of a syslog server is optional. To enable communication with the audit server the TOE requires the administrator to define:

- a TLS Profile,
- a TLS Service Profile, and
- a Peer Authentication Profile.

The steps required to configure TLS information are described below.

6.1 CONFIGURING TLS COMMUNICATION

6.1.1 CREATE A TLS PROFILE

A TLS Profile defines the minimum TLS version, cipher suites, elliptic curves, and session timeout value for a TLS connection. A TLS Profile must be configured for the evaluated configuration because the default values of the TLS version, cipher suites, and elliptic curves are not supported by the TOE.

Table 19: TLS Profile Parameters

Parameters	Valid Values	Description
profile-name	string	Identifies the profile.
tls-version	tls-1.2	Sets the minimum TLS version. ***Note***: The evaluated configuration requires this parameter to be configured to tls-1.2.
cipher-suite	TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Identifies the cipher suites to use for the profile. Cipher suites are listed in order of priority. ***Note***: The evaluated configuration requires this parameter to be configured to the cipher suites defined in the ST.

elliptic-curve	secp256r1, secp384r1, secp521r1	Identifies the elliptic curves to use for the cipher suites. Elliptic curves are listed in order of priority. ***Note***: The evaluated configuration requires this parameter must be configured to the elliptic curves defined in the ST.
session-resumption-timeout	60-86400 The default value is 3600	Sets the timeout for the session. The timeout is set to avoid reusing stale sessions without a fresh authentication.

Steps

1. Enter configuration mode:
   ```
   config
   ```
2. Specify the name of the TLS profile:
   ```
   hello-params tls-profiles tls-profile <name>
   ```
3. Set the minimum TLS version for the profile named syslog-tls:
   ```
   hello-params <profile_name> tls-versions tls-version tls-1.2
   ```
4. Set the TLS cipher suites for the profile named syslog-tls:
   ```
   hello-params <profile_name> cipher-suites cipher-suite <cipher_suite>
   ```
5. Set the elliptic curves for the profile:
   ```
   hello-params <profile_name> elliptic-curves elliptic-curve
   <elliptic_curve>
   ```
6. Set the timeout for the session of the profile:
   ```
   hello-params <profile_name> session-resumption-timeout <timeout>
   ```

Example

The following commands configure a TLS profile named syslog-tls with the minimum TLS version of TLSv1.2; the elliptic curves of secp256r1, secp384r1, and secp521r1; the timeout of 3600; and the cipher suites of TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268, TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492, TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246, TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246, TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288, TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289, and TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289.

```
config
hello-params tls-profiles tls-profile syslog-tls
hello-params syslog-tls tls-versions tls-version tls-1.2
```

```
hello-params syslog-tls cipher-suites cipher-suite
TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_ SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
hello-params syslog-tls elliptic-curves elliptic-curve secp256r1
secp384r1 secp521r1
hello-params syslog-tls session-resumption-timeout 3600
```

6.1.2 Create a Peer Authentication Profile

Next, the evaluated configuration requires the Administrator to create a Peer Authentication Profile. A Peer Authentication Profile defines which operations to perform upon reception of the Server's certificate (Syslog Server). If a Peer Authentication Profile is not defined, the Server's certificate will not be validated and the Server will automatically be successfully authenticated.

Table 20: Peer Authentication Profile Parameters

Parameters	Valid values	Description
peer-auth-profile-name	string	Specifies the profile name
check-cert-expiry	true	Determines whether the certificate is checked for expiry. ***Note:*** Must be set to true for the evaluated configuration.
check-fingerprint	true | false	Enables or disables check-fingerprint. ***Note:*** Not functionality included in the evaluated configuration.
fingerprint-list	SHA-1, SHA-256	Specifies the hashing algorithm. ***Note:*** Is ignored if Check-fingerprint is set to false.

Steps

1. Enter configuration mode:
   `config`
2. Specify the name of the peer authentication profile:
   `pkix peer-auth-profiles peer-auth-profile <peer-auth-profile-name>`

3. Set the check for expiration is performed on the Server's X.509 certificate. This must be set to true for the evaluated configuration.
   ```
   pkix peer-auth-profiles peer-auth-profile <peer-auth-profile-name>
   check-cert-expiry true
   ```
4. Set the check fingerprint to false. This functionality is not included in the evaluated configuration. Therefore, the confirmation can be true or false.
   ```
   pkix peer-auth-profiles peer-auth-profile <peer-auth-profile-name>
   check-fingerprint <check_fingerprint>
   ```
5. Set the list of acceptable certificate fingerprints. This is ignored if check-fingerprint is set to false.
   ```
   pkix peer-auth-profiles peer-auth-profile <peer-auth-profile-name>
   fingerprint-list <fingerprint>
   ```

Example

The following example creates a peer authentication profile named baseConf.

```
config
pkix peer-auth-profiles peer-auth-profile baseConf
pkix peer-auth-profiles peer-auth-profile baseConf check-cert-expiry
true
pkix peer-auth-profiles peer-auth-profile baseConf check-fingerprint
true
pkix peer-auth-profiles peer-auth-profile baseConf sha-1 sha-256
```

6.1.3 CREATING A TLS SERVICE PROFILE

Next, define a TLS Service Profile that references the TLS profile and TLS Peer Authentication Profile defined above.

Table 21: TLS Service Profile Parameters

Parameters	Valid values	Description
tls-service-profiles	string	Identifies the TLS profile. Configures the TLS connection parameters. TLS profiles reference cipher suites and elliptic curves. Refer to section 6.1.1 to define this field.
tls-peer-auth-profile-name	string	Identifies the peer authentication profile. This identifies how to authenticate the Server's certificate. ***Note:*** This must be defined for the evaluated configuration. If left null, the Server's certificates will not be validated. Refer to section 6.1.2 to define this field.

tls-certificate-name	string	Identifies the TLS certificate. Provides the certificate and key that establishes the identity of the system. The TLS certificate name is a reference to a certificate and private key stored in the system PKIX. It is used to identify the system to its TLS peer. ***Note:*** This can be left to null because mutual authentication is not supported by the evaluated configuration.

Steps

1. Enter configuration mode:
   ```
   config
   ```
2. Identify the TLS Profile
   ```
   tls-service-profiles <tls-service-profile-name> tls-profile-name <tls-profile>
   ```
3. Identify the peer authentication profile.
   ```
   tls-service-profiles <tls-service-profile-name> tls-peer-auth-profile-name <peer-auth-profile>
   ```
4. Identify the TLS certificate.
   ```
   tls-service-profiles <tls-service-profile-name> tls-certificate-name <certificate>
   ```

Example

The following example assigns the profile components to the TLS service profile named test.

```
config
tls-service-profiles test tls-profile-name syslog-tls
tls-service-profiles test tls-peer-auth-profile-name baseConf
```

6.1.4 CONFIGURE THE REKEY LIMIT

Configure the rekey limit to specify the maximum amount of data that can be transmitted before the session key renegotiated.

Table 22: Rekey Limit Parameter

Parameter	Valid Values	Description
rekey-limit	1G	Specifies the amount of data between SSH session key renegotiations. ***Note***: the evaluated configuration requires this parameter to be configured to 1G.

Steps

1. Enter configuration mode:
   `config`
2. Configure the rekey limit.
   `system ssh-server config rekey-limit <rekey-limit>`

Example

The following command configures the SSH rekey limit to the evaluated configuration.

```
config
system ssh-server config rekey-limit 1G
```

6.2 X.509 CERTIFICATES

The TOE uses X.509 certificates for communication with the syslog server. The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication of external TLS peers. There are two categories of X.509 certificates:

- System certificates are stored in a global directory that SAOS uses to identify itself.
- Trust store of Certificate Authority (CA) certificates that are used to verify the identity of peers.

The TOE validates certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation supporting a minimum path length of three certificates.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TOE validates a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TOE validates the revocation status of the certificate using Online Certificate Status Protocol (OCSP) as specified in RFC 6960.
- The TOE validates the extendedKeyUsage field according to the following rules:
  - Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
  - Server certificates presented for TLS must have the Server Authentication purpose (idkp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
  - Client certificates presented for TLS must have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.

- OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (idkp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

The TOE does not use X.509 certificates for trusted updates, hence the requirement for Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field is trivially satisfied.

Certificate validity is checked on each certificate validation. If the validation of the certificate fails because the OCSP Server cannot be connected to, the certificate shall not be accepted. Certificates are validated upon receipt from the server (Syslog) and when they are loaded onto the TOE. If the connection fails, the Administrator should check the physical connections and reenable the OCSP client with the following command after entering config mode: `hello-params baseConf ocsp-state enabled`. Where `baseConf` is the TLS Profile for the OCSP Server.

By default, the TOE supports SAN extension and checks SAN extension over CN when present. The TOE ignores CN when SAN is present. When SAN is not present, the TOE falls back to CN check. FQDN is supported in both SAN and CN while IP address is only supported in SAN.

By default, the TOE supports wildcards in certificates for DN names. The wildcard must be in the left-most label of the presented identifier and can only cover one level of subdomains. For the reference identifier without a left-most label as in the certificate, the connection will fail, i.e., awesome.com doesn't match *.awesome.com. The TLS client does not support certificate pinning.

The syslog connection fails if the audit server certificate does not meet any one of the following criteria:

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

6.2.1 Configure the Certificates Required for the TOE

To configure the certificates required for the TOE, perform the following steps.

- **Install a CA certificate:**

```
pkix-ca install ca-cert-name <ca_cert_name> remote-file-uri
scp://<server_ip>/<cert_path>/<ca.cert> login-id <login_id> password
<login_password>
```

The following example installs a CA certificate named test.

```
pkix-ca install ca-cert-name test remote-file-uri
scp://192.0.2.0/certs/ SaosCertificate.pem login-id User1 password abc
```

- **Install a device certificate and private key as required by the network plan.**

Install a device certificate and private key:

```
pkix-certificates install <cert_name> remote-file-uri
scp://<server_ip>/<cert_path>/<device.p12> login-id <login_id> password
<login_password> cert-passphrase <cert_pass_phrase>
```

The following example installs a device certificate and private key.

```
pkix-certificates install TestCa remote-file-uri
scp://192.0.2.0/certs/TestClient.p12 login-id User1 password abc cert-
passphrase test
```

- **Generate a private key and certificate signing request on the system, sign the certificate externally, and install the certificate as required.**

Generate a private key and certificate signing request on the system, sign the certificate externally, and install the certificate:

```
pkix-csr generate cert-name <cert_name> algorithm-identifier <algorithm-identifier> remote-fileuri
ftp://server_ip/<path>/<cert.cnf> cert-passphrase <cert_passPhrase>
```

The following example generates a private key and certificate signing request.

```
pkix-csr generate cert-name testCsrGen algorithm-identifier pkix-types:rsa1024
remote-file-uri ftp://1.2.3.4/certs/ClientCert.pem certpassphrase test
```

- **Enable check-fingerprint:**

```
config
pkix peer-auth-profiles peer-auth-profile <peer-auth-profile> check-fingerprint <true|false>
```

The following example enables check-fingerprint for a peer authentication profile named baseConf.

```
config
pkix peer-auth-profiles peer-auth-profile baseConf check-fingerprint true
```

- **Display a CA certificate:**

```
show pkix
```

- **Display a device certificate and private key:**

```
show pkix
```

- **Display all certificates on the system:**

```
show pkix
```

The following example displays all certificates installed on the system.

```
> show pkix
+---------------------- CA CERTIFICATES ----------------------+
| Name                 | Value                               |
+----------------------+-------------------------------------+
| CA Name              | rootCert                            |
| Subject Common Name  | test2CA                             |
| Issuer Common Name   | test2CA                             |
| Valid Until          | Aug 22 07:22:29 2039 UTC (19 years) |
+----------------------+-------------------------------------+

+---- CERTIFICATE REVOCATION LISTS ---+
| Name              | Value           |
+-------------------+-----------------+
| No Entries                          |
+-------------------+-----------------+

+------------------- DEVICE CERTIFICATES ------------------+
| Name                 | Value                             |
```

```
+---------------------+-------------------------------------+
| Certificate Name    | server_cert                         |
| Algorithm ID        | rsa1024                             |
| Private Key         | present                             |
| Subject Common Name | server                              |
| Issuer Common Name  | test2CA                             |
| Valid Until         | Sep 5 07:30:35 2020 UTC (2 months)  |
+---------------------+-------------------------------------+
```

O Display the status of check-fingerprint and the fingerprint-list:

```
show tls
```

The following example displays the status of check-fingerprint and the fingerprint-list for peer authentication profiles.

```
show tls
+----------- TLS SERVICE PROFILES -----------+
| Name                    | Value            |
+-------------------------+------------------+
| Service Profile Name    | test             |
| TLS Profile Name        | tls-profile      |
| Peer Auth Profile Name | peer-auth-profile |
| Certificate Name        | server_cert      |
+-------------------------+------------------+

+--------------------------------- PEER AUTH PROFILES ---------------------------------+
| Name              | Value                                                            |
+-------------------+------------------------------------------------------------------+
| Profile Name      | peer-auth-profile                                                |
| Check Expiry      | False                                                            |
| Check IP/Host     | False                                                            |
| Check Fingerprint | True                                                             |
| IP/Host List      | TLS_Client_NoAia                                                 |
| Fingerprint List  | sha-1:E1:11:69:1B:92:39:62:7C:7C:E9:10:10:E8:47:48:B8:F5:B9:23:16 |
+-------------------+------------------------------------------------------------------+

+--------------------------- HELLO PARAMS ---------------------------+
| Name                           | Value                             |
+--------------------------------+-----------------------------------+
| Profile Name                   | tls-profile                       |
| Protocol Versions              | tls-1.2                           |
| Cipher Suites                  | ecdhe-rsa-with-aes-256-gcm-sha384 |
| Elliptic Curves                | secp384r1                         |
| Sess. Resumption Timeout (s)   | 3600                              |
| OCSP State                     | enabled                           |
| NONCE State                    | enabled                           |
| Default OCSP Responder URL     | -                                 |
+--------------------------------+-----------------------------------+
```

O Add entries to ip-host-list:

```
config
pkix peer-auth-profiles peer-auth-profile https-peerauth-profile ip-host-list
<ip-address|hostname> <ipaddress| hostname> <ip-address|hostname>
```

The following example adds 10.33.80.81 and three host entries to the iphost-list.

```
config
pkix peer-auth-profiles peer-auth-profile https-peer-auth-profile ip-hostlist
10.33.80.81 eit-21.ca.stalab.ciena.com entry1 entry2 entry3
exit
show tls
+----------- TLS SERVICE PROFILES ----------+
| Name                   | Value            |
+------------------------+------------------+
| Service Profile Name   | baseConf         |
| TLS Profile Name       | baseConf         |
| Peer Auth Profile Name | baseConf         |
| Certificate Name       | testCert         |
+------------------------+------------------+

+------------ PEER AUTH PROFILES ------------+
| Name          | Value                      |
+---------------+----------------------------+
| Profile Name  | https-peer-auth-profile    |
| Check Expiry  | True                       |
| Check IP/Host | True                       |
| IP/Host List  | 10.33.80.81                |
|               | eit-21.ca.stalab.ciena.com |
|               | entry1                     |
|               | entry2                     |
|               | entry3                     |
+---------------+----------------------------+

+---------------------------- HELLO PARAMS ----------------------------+
| Name                          | Value                                |
+-------------------------------+--------------------------------------+
| Profile Name                  | baseConf                             |
| Protocol Versions             | tls-1.2                              |
| Cipher Suites                 | ecdhe-ecdsa-with-aes-256-gcm-sha384, |
|                               | ecdhe-ecdsa-with-aes-256-cbc-sha384, |
|                               | ecdhe-ecdsa-with-aes-128-cbc-sha256, |
|                               | rsa-with-aes-256-gcm-sha384,         |
|                               | rsa-with-aes-256-cbc-sha256,         |
|                               | rsa-with-aes-256-cbc-sha,            |
|                               | ecdhe-rsa-with-aes-128-gcm-sha256,   |
|                               | ecdhe-rsa-with-aes-128-cbc-sha256,   |
|                               | rsa-with-aes-128-gcm-sha256,         |
|                               | rsa-with-aes-128-cbc-sha,            |
|                               | rsa-with-3des-ede-cbc-sha            |
| Elliptic Curves               | secp521r1, secp384r1, secp256r1      |
| Sess. Resumption Timeout (s)  | 3600                                 |
+-------------------------------+--------------------------------------+
```

- **Enable check IP/host:**

```
pkix peer-auth-profiles peer-auth-profile <peer-profile-name> check-ip-host
true
```

6.3 THE OCSP SERVER

Online Certificate Status Protocol (OCSP) is used to maintain the security of a server and other network resources. When a user attempts to access a server, OCSP sends a request for certificate status information. The server sends back a response of current, expired or unknown. The protocol specifies the syntax for communication between the server (which contains the certificate status) and the client application (which is informed of that status). OCSP is an Internet Protocol used to obtain the revocation status of a digital certificate. Messages that are communicated through OCSP are encoded in ASN.1 and are usually communicated over HTTP. The HTTP protocol complies with RFC 2818. The request/response nature of these messages results in OCSP servers being termed OCSP responders.

The TOE communicates with the OCSP Server via HTTP over TCP. The OCSP Server is a required server in the TOE's evaluated configuration.

6.3.1 CONFIGURE THE OCSP SERVER

The following sections describe the steps to configure the OCSP Server.

- **Modify the OCSP default responder URL.**

```
config
hello-params <profile-name> default-ocsp-responder-url <URL>
```

The following example modifies the OCSP default responder URL for the TLS profile named baseConf.

```
config
hello-params baseConf default-ocsp-responder-url http://203.0.113.4:80
```

- **Modify the OCSP state.**

```
config
hello-params <profile-name> ocsp-state <enabled|disabled>
```

The following example enables the OCSP state for the TLS profile named baseConf.

```
config
hello-params baseConf ocsp-state enabled
```

- **Modify the nonce state.**

```
config
hello-params <profile-name> nonce-state <enabled|disabled>
```

The following example modifies the nonce state for the TLS profile named baseConf.

```
config
hello-params baseConfig nonce-state enabled
```

6.3.2 OCSP SERVER REQUIREMENTS

The OCSP Server, provided by the operational environment, must be loaded with the following certificates:

- Self-certificate (system cert) signed by the issuer (CA authority)
- Root certificate who signed the system certificate
- Root certificate of the client who is trying to initiate the connection

O Add entries to ip-host-list:

```
config
pkix peer-auth-profiles peer-auth-profile <https-peer-auth-profile> ip-host-
list <ip-address|hostname> <ipaddress| hostname> <ip-address|hostname>
```

The following example adds 10.33.80.81 and three host entries to the ip-host-list.

```
config
pkix peer-auth-profiles peer-auth-profile https-peer-auth-profile ip-hostlist
10.33.80.81 eit-21.ca.stalab.ciena.com entry1 entry2 entry3
exit
show tls
+----------- TLS SERVICE PROFILES ----------+
| Name                   | Value            |
+------------------------+------------------+
| Service Profile Name   | baseConf         |
| TLS Profile Name       | baseConf         |
| Peer Auth Profile Name | baseConf         |
| Certificate Name       | testCert         |
+------------------------+------------------+

+------------ PEER AUTH PROFILES ------------+
| Name          | Value                      |
+---------------+----------------------------+
| Profile Name  | https-peer-auth-profile    |
| Check Expiry  | True                       |
| Check IP/Host | True                       |
| IP/Host List  | 10.33.80.81                |
|               | eit-21.ca.stalab.ciena.com |
|               | entry1                     |
|               | entry2                     |
|               | entry3                     |
+---------------+----------------------------+

+---------------------------- HELLO PARAMS ----------------------------+
| Name                          | Value                                |
+-------------------------------+--------------------------------------+
| Profile Name                  | baseConf                             |
| Protocol Versions             | tls-1.2                              |
| Cipher Suites                 | ecdhe-ecdsa-with-aes-256-gcm-sha384, |
|                               | ecdhe-ecdsa-with-aes-256-cbc-sha384, |
|                               | ecdhe-ecdsa-with-aes-128-cbc-sha256, |
|                               | rsa-with-aes-256-gcm-sha384,         |
|                               | rsa-with-aes-256-cbc-sha256,         |
|                               | rsa-with-aes-256-cbc-sha,            |
|                               | ecdhe-rsa-with-aes-128-gcm-sha256,   |
|                               | ecdhe-rsa-with-aes-128-cbc-sha256,   |
|                               | rsa-with-aes-128-gcm-sha256,         |
|                               | rsa-with-aes-128-cbc-sha,            |
|                               | rsa-with-3des-ede-cbc-sha            |
| Elliptic Curves               | secp521r1, secp384r1, secp256r1      |
```

```
| Sess. Resumption Timeout (s) | 3600                                  |
+------------------------------+---------------------------------------+
```

Enable check IP/host:

```
pkix peer-auth-profiles peer-auth-profile <peer-profile-name> check-ip-host
true
```

Note: The ip-host-list can be checked in both the SAN and CN, with the SAN taking priority if present. The use of wildcards in certificates is supported for hostname but not ip addresses.

7 Clock Management

The TOE implements a hardware clock for local date and time. The clock may be configured to use a locally configured time The time is used for producing time stamps which are included in audit records and to check the X.509 certificate expiration. The TOE also uses the clock to implement the session time out timers for each interactive session (lockout) and to terminate each interactive session which exceeds the maximum allowed inactivity time and to ensure proper monitoring of the system and equipment.

The evaluated configuration requires the clock be set either locally or remotely.

Note: Ensure that the clock on the system is correct before obtaining licenses. If the clock is not correct, licenses are not processed.

7.1 Manually Setting the Local Clock

To set the system time locally, perform the following steps.

Steps

1. Set the system time:

```
system set clock <current datetime>
```

Example

1. The following example sets the system time to 2019-08-21T22:25:00Z. •

```
system set clock 2019-08-21T22:25:00Z
```

2. Verify that the date and time were set correctly:

• `show clock`

```
-----------+------------- SYSTEM CLOCK -------+
| Key | Value |
+--------------+-------------------------+
| Clock | 2019-08-21T22:25:00Z |
+--------------+-------------------------+
```

8 MACSEC Configuration

Media Access Control Security (MACsec) is an IEEE standard 802.1AE-2018 that defines a protocol for providing security for Ethernet LANs. It offers authenticity and integrity and optional encryption of the Layer 2 payload.

The MACsec functionality installed in the hardware uses the MACsec Key

Agreement (MKA) protocol. The MKA protocol is defined as part of the IEEE Standard 802.1X-2010 and generates and distributes the symmetric cryptographic keys.

MACsec uses Extensible Authentication Protocol over LAN (EAPoL) messages to establish MKA sessions and encryption and decryption.

Decryption is achieved using the generated Secure Association Key (SAK).

MACsec offers three protection modes:

- confidentiality protection by means of encryption and decryption
- integrity protection by means of integrity check value (ICV)
- replay protection

MACsec is supported on the system at a line-rate of 1 Gbps and 10 Gbps on ETTP ports 7 and 8.

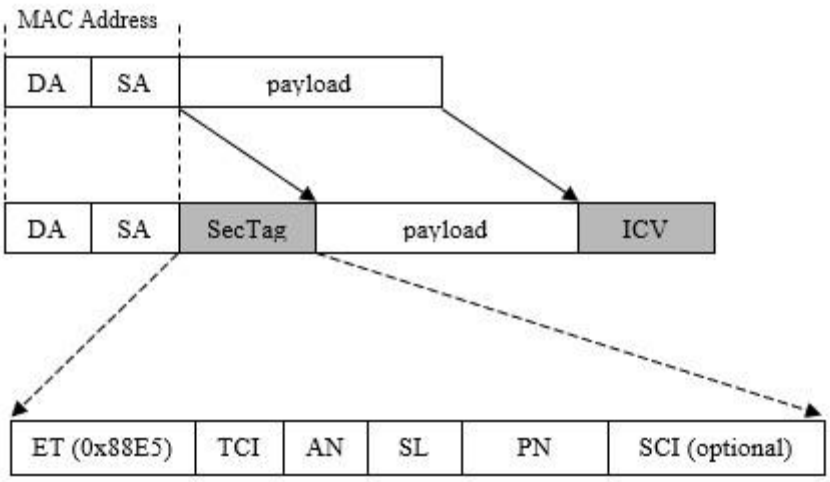
Note: MACSEC is disabled by default and there are no MKA policies configured by the TOE.

8.1 MACsec Frame Format

MACsec offers authenticity and integrity and optional encryption of the Layer 2 payload.

The following figure shows the MACsec frame format.

Figure 1: MACsec Frame Format



When a packet goes through a MACsec device, the following occurs:

- On transmit: a SecTag header with the Ethertype 0x88e5 is prepended at the start of the packet. The ICV is computed over the entire packet (including the SecTag and the Ethernet MAC addresses) and appended at the end of the packet. The payload is optionally encrypted.
- On receive: The format of the packet and SecTag is checked, the cryptographic signature is verified, and the data is decrypted.

After validation, the MACsec-specific parts of the packets, that is, SecTag and ICV, are stripped, and the packets undergo service-specific processing.

8.2 Connection Association

A Connection Association (CA) is a security relationship that is established and maintained by key agreement protocols. The CA comprises a fully-connected subset of the service access points in stations attached to a single Local Area Network (LAN) or Wide Area Network that are supported by

MACsec. MACsec connection-association end-points are MAC Security Entities (SecYs). SecY is the entity that operates the MAC Security protocol within a system.

A MACsec service can be associated with

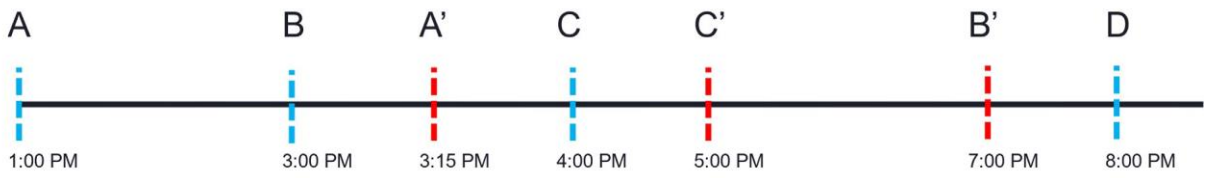
- an ETTP: all frames transmitted by the ETTP are MACsec encapsulated with the exception of frames configured as an exclude-protocol and MKA frames
- a flow-point: all frames transmitted by the flow-point are MACsec encapsulated with the exception of frames configured as an excludeprotocol and MKA frames

8.3 Hitless CA Key (CAK) Rollover

CAK rollover is the transition from the expiry of one key to the next valid starting time for the next key. With hitless CAK rollover, the next rollover happens as soon as the next valid key is found.

The following figure shows four keys: A, B, C and D. The blue dashed lines indicate the starting time of the key and red dashed lines indicate the expiry time. Key A is valid as of 1:00 PM and ends at 3:15 PM. Key B is valid as of 3:00 PM and ends at 7:00 PM. There is an overlap of 15 minutes during which both key A and key B are valid. CA rolls over from key A to key B at 3:00 PM. Similarly, it again rolls over from key B to key C at 4:00 PM and rolls back from key C to key B again at 5:00 PM.

Figure 2: Key Start and Expiry



An overlap time does not exist between key B and key D: key B expires at 7:00 PM and key D starts at 8:00 PM. Therefore, a valid key does not exist during the period of 7:00 PM to 8:00 PM. At 7:00 PM the CA session is operationally down becasue there is no valid key. It does not automatically come up at 8:00 PM unless a user toggles the MACsec or CA session. Even if key B expires at 7:00 PM and key D also starts at 7:00 PM, a probability exists where the rollover is not successful. There must be at least some overlap of time between two consecutive keys. Ciena recommends an overlap of 30 seconds between two consecutive keys.

8.4 MACsec Configuration Topologies

The following table lists supported MACsec network configuration topologies.

Table 23: Configuration topologies

Topology	Association	Description
Hop by hop	ETTP	SecYs are directly connected by means of a single hop where MKA frames are transmitted with a standard DMAC and ethertype value.
End to end ETTP-based service	ETTP	SecYs are connected to each other over one or more hops where MKA frames are transmitted with a non-standard DMAC or ethertype value. Both can be non-standard, but at least one (DMAC or ethertype) must be non-standard.
End to end flow point based service	flow point	SecYs are connected to each other over one or more hops where MKA frames are transmitted with a non-standard DMAC or ethertype value. Both can be non-standard, but at least one (DMAC or ethertype) must be non-standard.

8.5 Configuring the MACsec Key Agreement Protocol Using the CLI

Configure the MACsec key agreement protocol (MKA) as required by the network plan.

Overview

The following table lists the parameters for configuring an MKA.

Table 24: Parameters for configuring an MKA

Parameters	Valid values	Description
key-chain	string	Specifies the name of the key chain.
mka-key	2 - 64 hex-value of even number of bits with a maximum length of 64 bits	Identifies the Connectivity Association Key name (CKN), which identifies the CAK.
key	hex-value of 32 (for 128 bit cmac) or 64 bits (for 256 bit cmac)	Identifies the CAK, which is a secret key possessed by members of a given CA.
cryptographic-algorithm	AES_128_CMAC| AES_256_CMAC The default value is AES_128_CMAC.	Specifies the MKA cryptographic authentication algorithm.

Steps

1. Enter config mode:
   `config`
2. Configure a key chain name:
   `macsec key-chains key-chain <key-chain>`
3. Configure the Connectivity Association Key name (CAK):
   `mka-keys mka-key <mka-key>`
4. Configure a key name:
   `key <key>`
5. Configure the cryptographic-algorithm:
   `cryptographic-algorithm <cryptographic-algorithm>`

Example

The following example configures a key-chain named KC2 with the mka-key 02 with key fedcba98765432100123456789abcdef0123456789abcdef0123456789abcdef. The key-chain named KC2 with the mka-key 02 is then configured with the default cryptographic algorithm.

```
config
macsec key-chains key-chain KC2 mka-keys mka-key 02 key
fedcba98765432100123456789abcdef0123456789abcdef0123456789abcdef
macsec key-chains key-chain KC2 mka-keys mka-key 02 cryptographic-
algorithm AES_128_CMAC
```

8.6 Configuring the MACsec Profile Using the CLI

Overview

The following table lists the parameters for configuring the MACsec profile.

Table 25: Parameters for Configuring the MACsec Profile

Parameters	Valid values	Description
profile	string	Specifies the MACsec profile name.
macsec-cipher-suite	GCM_AES_128|GCM_AES_256 The default value is GCM_AES_128	Specifies the cipher suite mechanism to be used by hardware to encrypt the data. ***Note:*** The evaluated configuration requires this parameter to have a value of GCM_AES_128 or GCM_AES_256.

confidentiality-offset	0_BYTES|30_BYTES|50_BYTES The default value is 0 BYTES	Specifies the number of octets in an Ethernet frame that are sent in unencrypted plain text. ***Note:*** The evaluated configuration requires this parameter to have a value of 0 BYTES.
replay-window-size	0..0xffffffff The default value is 0	Specifies the number of out-of-order packets that can be accepted. Setting this parameter provides replay protection. The replay protection mechanism is used where all frames within the service of a CA are deemed to be received in order, that is, MACsec hop-by-hop configurations and network configurations where the CA is configured on an isolated, dedicated, and uncongested end-to-end service. To avoid frame loss on an end-to-end network configuration, configure the replay-window-size to 65535.
additional-bytes-in-clear	0 The default value is 0	Specifies the number of additional bytes that are clear text. These bytes are not encrypted. ***Note:*** The evaluated configuration requires this parameter to have a value of 0.
encryption-on	false | true The default value is true	Specifies whether encryption is enabled or disabled. ***Note:*** The evaluated configuration requires this parameter to have a value of true.

key-server-priority	0-255 The default value is 16	Specifies the key server that is elected through the MKA protocol to transport a succession of SAKs for use by MACsec to the other member(s) of a CA.
sak-rekey-interval	0|30-65535 The default value is 0	Specifies the time interval for which the Secure Association Key (SAK) is valid. A new SAK is generated after every sak-rekey-interval period. Limit the average number of rekeys each minute to 64 or less. For example, if 512 CAs are configured, and they all have the same sak-rekey-interval, configure the sak-rekey-interval to at least 480 seconds (8 minutes).

Steps

1. Enter config mode:
   `config`
2. Configure a MACsec profile name:
   `macsec macsec-profiles profile <profile>`
3. Configure the macsec-cipher-suite:
   `macsec-cipher-suite <macsec-cipher-suite>`
4. Configure the confidentiality-offset:
   `confidentiality-offset <confidentiality-offset>`
5. Configure encryption:
   `encryption-on <encryption-on>`
6. Configure the replay-window-size:
   `replay-window-size <replay-window-size>`
7. Configure key-server-priority:
   `key-server-priority <key-server-priority>`
8. Configure sak-rekey-interval:
   `sak-rekey-interval <sak-rekey-interval>`

Example

The following example configures a MACsec profile named pf2 with confidentiality offset 0_BYTES, encryption enabled, a key server priority 10, cipher suite GCM_AES_128, a replay window size of 2, and an SAK rekey interval of 600.

```
config
```

```
macsec macsec-profiles profile pf2 confidentiality-offset 0_BYTES
encryption-on true key-server-priority 10 macsec-cipher-suite
GCM_AES_128 replay-window-size 2 sak-rekey-interval 600
```

8.7 Configuring the MACsec Interface Using CLI

Configure the MACsec interface as required by the network plan.

Overview

The following table lists the parameters for configuring the MACsec interface.

Table 26: Parameters for Configuring the MACsec Interface

Parameters	Valid values	Description
interface	string	Specifies interface name mapped to the ETTP interface. ***Note:*** The evaluated configuration requires this parameter to have a value of 7 or 8.
strict-mode-on	true | false The default value is false	Specify true so that only MACsec-enabled frames are transmitted or received. Specify false so the ETTP can transmit and receive either MACsec-enabled frames or non-MACsec frames. ***Note:*** The evaluated configuration requires this parameter to have a value of true.
exclude-protocols	e-lmi, esmc, garp-block, lacp, lamp, link-oam, lldp, pause, port-auth, ptp, ptp-peer-delay, xstp The default value is none	Specifies the list of protocols that are excluded from encryption during transmit and receive.

Steps

1. Enter config mode:
   `config`
2. Configure a MACSec interface name:
   `macsec config interfaces interface <interface>`
3. Configure strict-mode-on:
   `strict-mode-on <strict-mode-on>`
4. Configure exclude-protocols:
   `exclude protocols <exclude-protocols>`

Example

The following example configures the MACsec interface 8 with the strict mode on and the lacp protocol excluded from encryption during transmit and receive.

```
config
macsec config interfaces interface 8 strict-mode-on true exclude-
protocols lacp
```

8.8 Configuring the MACsec Connection Association Using the CLI

Configure the MACsec interface as required by the network plan.

Overview

The following table lists the parameters for configuring the MACsec interface.

Table 27: Parameters for Configuring a MACsec Connection Association

Parameters	Valid values	Description
connection-association	string	Specifies the connection association name, which is SecY.
macsec-admin-state	enabled | disabled The default value is enabled.	Specifies the MACsec admin state at the CA level.
destination-address	multicast MAC address | chassis MAC address of the peer	Specifies the destination MAC address of MKA frames transmitted by the system.
key-chain	string	Specifies the key chain. Note that this is a mandatory parameter.
macsec-profile	string	Specifies the MACsec profile. Note that this is a mandatory parameter.
ettp-name	string	Specifies the type of connection. Ettp-name and flow-point are mutually exclusive. ***Note:*** The evaluated configuration requires this parameter to be 7 or 8.
flow-point	string	Specifies the type of connection. Flow-point and ettp-name are mutually exclusive.

compatibility-mode	string	Compatibility flag to facilitate MACsec interoperability.
icv-validation-on	true | false The default value is true	Enable or disable ICV validation.
ring-name	string	Specifies the G.8032 Ring name.
data-member	string	Specifies the G.8032 Ring Data Member name of the service.
erp-instance-name	string	Specifies the G.8032 Ring Erp Instance name.
include-sci	true | false The default value is false	Indicates inclusion of the Secure Channel Identifier (SCI) tag in the Security TAG (SecTAG) field of the MACsec header.
mka-ethertype	integer The default value is 0x888E	User configured Ether-type for the EAPoL PDUs. This configuration is at CA level and over-ride the configuration at interface level, i.e. if CA level ether-type is not configured then interface ether-type config will be applied. If CA ether-type is configured then CA level ether-type will be applied for that CA.
sak-event-logging-on	true | false The default is false	Enable or disable event logging for SAK rekey.

Steps

1. Enter config
   `config`
2. Configure the connection-association name:
   `macsec config connection-association <connection-association>`
3. Enable/disable the MACsec admin state:
   `macsec-admin-state <macsec-admin-state>`
4. Associate the key-chain:
   `key-chain <key-chain>`
5. Associate the macsec-profile:
   `macsec-profile <macsec-profile>`
6. Configure the connection-type:
   `ettp-name <ettp-name>`

Example

The following example configures a connection association named CA2 where the admin state at the CA level is enabled and associates it to keychain KC2, MACsec profile pf2, and ettp-name 8.

```
config
macsec config connection-association CA2 macsec-admin-state enabled
key-chain KC2 macsec-profile pf2 ettp-name 8
```

8.9 Configuring the Start Date and Time for MACsec Keychain Validity

Configure the start date and time for MACsec keychain validity as required by the network plan.

Requirements

Ensure that the local time between peers is synchronized.

To ensure a smooth transition, peers have a buffer of 25 seconds during CAK rollover. The MACsec connection drops If the rollover does not take place during this period.

Overview

The following table lists the parameters for configuring the start date and time for MACsec keychain validity.

Table 28: Parameters for Configuring the Start Date and Time for MACsec Keychain Validity

Parameters	Valid values	Description
key-chain	string	Specifies the name of the key chain.
mka-key	2 - 64 hex-value of even number of bits with a maximum length of 64 bits	Identifies the Connectivity Association Key name (CKN), which identifies the CAK.
key	4 | 32 |64 hex value with a length of 4, 32 or 64 bits	Identifies the CAK, which is a secret key possessed by members of a given CA.
valid-date-time	YYYY-MM-DDTHH:MM:SSZ | VALID_IMMEDIATELY | DISABLED The default value is VALID_IMMEDIATELY.	Specifies the starting date and time from which the keychain is valid. Specify VALID_IMMEDIATELY to set the keychain to be valid immediately. A keychain set to DISABLED is not considered for rollover.

Steps

1. Enter config mode
   ```
   config
   ```

2. Specify the date and time at which the keychain is valid:
   ```
   mac-sec key-chains key-chain <key-chain> mka-keys mka-key <mka-key>
   valid-date-time <valid-date-time>
   ```

Example

The following example configures a keychain named KC-1 with the mka-key as ABCD1236 with key 1234567890123456789012345678 90BB to become valid at 19 October 2023 at 19:39 hours.

```
config
macsec key-chains key-chain KC-1 mka-keys mka-key ABCD1236 key
1234567890123456789012345678 90BB valid-date-time 2023-10-19T19:39:00Z
```

8.10 Configuring the Date and Time for a MACsec Keychain to Expire Using the CLI

Configure the date and time for a MACsec keychain as required by the network plan.

Requirements

Ensure that local time between peers is synchronized.

To ensure a smooth transition, peers have a buffer of 25 seconds during CAK rollover. The MACsec connection drops If the rollover does not take place during this period.

Overview

The following table lists the parameters for configuring the date and time for a MACSec keychain to expire.

Table 29: Parameters for Configuring the Date and Time for a MACsec Keychain to Expire

Parameters	Valid values	Description
key-chain	string	Specifies the name of the key chain.
mka-key	2-64 hex-value of even number of bits with a maximum length of 64 bits	Identifies the Connectivity Association Key name (CAK), which identifies the CAK.
key	4 | 32 | 64 hex value with a length of 4, 32 or 64 bits	Identifies the CAK, which is a secret key possessed by members of a given CA.
expiration-date-time	YYYY-MM-DDTHH:MM:SSZ | NO_EXPIRATION The default value is NO_EXPIRATION	Specifies the date and time at which the keychain expires. If a value for the expiration-date-time parameter is not specified, the keychain never expires. The value of the expiration-date-time parameter must be greater than the value of the valid-date-time parameter.

Steps

1. Enter config mode:
   ```
   config
   ```
2. Specify the date and time at which the keychain expires:
   ```
   mac-sec key-chains key-chain <key-chain> mka-keys mka-key <mka-key>
   expiration-date-time <expiration-date-time>
   ```

Example

The following example configures a keychain named KC-1 with the mka-key as ABCD1236 with key 1234567890123456789012345678 90BB to expire on 19 October 2023 at 19:35:00 hours.

```
config
macsec key-chains key-chain KC-1 mka-keys mka-key ABCD1236 key
1234567890123456789012345678 90BB expiration-date-time 2023-10-
19T19:35:00Z
```

8.11 Configuring Multiple Keys in a MACsec Keychain Using the CLI

Configure multiple keys in a MACsec keychain as required by the network plan.

Requirements

Ensure that the keychains are cached on the system.

Overview

The following table lists the parameters for configuring multiple MACsec keychains in a CA keychain.

Table 30: Parameters for Configuring Multiple Keychains in a CA Keychain Cached on the Device

Parameters	Valid values	Description
key-chain	string	Specifies the name of the key chain.
mka-key	2 - 64 hex-value of even number of bits with a maximum length of 64 bits	Identifies the Connectivity Association Key name (CKN), which identifies the CAK.
key	4 | 32 | 64 hex value with a length of 4, 32 or 64 bits	Identifies the CAK, which is a secret key possessed by members of a given CA.
valid-date-time	YYYY-MM-DDTHH:MM:SSZ | VALID_IMMEDIATELY | DISABLED The default value is VALID_IMMEDIATELY.	Specify the starting date and time from which the keychain is valid. Specify VALID_IMMEDIATELY to set the keychain to be valid immediately. Specify DISABLED to disable the key. A key set to DISABLED is not considered for rollover.

expiration-date-time	YYYY-MMDDTHH:MM:SSZ| NO_EXPIRATION The default value is NO_EXPIRATION.	Specify the date and time at which the keychain expires. If a value for the expiration-date-time parameter is not specified, the keychain never expires. Specify NO_EXPIRATION to set the keychain to never expire.

Steps

1. Enter config mode:
   ```
   config
   ```
2. Configure multiple keys in a keychain:
   ```
   macsec key-chains key-chain <key-chain> mka-keys mka-key <mka-key> key
   <key> valid-date-time <valid-date-time> expiration-date-time <valid-
   expiration-time>
   ```

Example

The following example configures a keychain named KC-1 with the mka-key as ABCD1235 with key 1234567890123456789012345678 90BB to become valid on 19 October 2023 at 13:03:25 hours and expire on 19 October 2023 at 13:10:25 hours.

```
config
macsec key-chains key-chain KC-1 mka-keys mka-key ABCD1235 key
1234567890123456789012345678 90BB valid-date-time 2023-10-19T13:03:25Z
expiration-date-time 2023-10-13T13:10:25Z
```

The following example configures a keychain named KC-1 with the mka-key as ABCD1234 with key 1234567890123456789012345678 90AA to become immediately valid and expire on 13 October 2023 at 13:12:25 hours.

```
config
macsec key-chains key-chain KC-1 mka-keys mka-key ABCD1234 key
1234567890123456789012345678 90AA valid-date-time VALID_IMMEDIATELY
expiration-date-time 2023-10-13T13:12:25Z
```

The following example configures a keychain named KC-1 with the mka-key as ABCD1236 with key 1234567890123456789012345678 90CC to become valid on 13 October 2023 at 13:03:25 hours and never expire.

```
config
macsec key-chains key-chain KC-1 mka-keys mka-key ABCD1236 key
1234567890123456789012345678 90CC valid-date-time 2023-10-13T13:03:25Z
expiration-date-time NO_EXPIRATION
```

8.12 Enabling a Key in a MACsec Keychain Using the CLI

Enable a key in a MACsec keychain to enable a key that has been set to DISABLED.

Overview

The key does not need to be explicitly enabled. The key is enabled if it has a valid configuration and the valid-date-time is not set to DISABLED.

The following table lists the parameters to enable a key in a MACsec keychain.

Table 31: Parameters to Enable a Key in a MACsec Keychain

Parameters	Valid values	Description
key-chain	string	Specifies the name of the key chain.
mka-key	2 – 64 hex-value of even number of bits with a maximum length of 64	Identifies the Connectivity Association Key name (CKN), which identifies the CAK.
valid-date-time	YYYY-MM-DDTHH:MM:SSZ | VALID_IMMEDIATELY	Specify the starting date and time from which the keychain is valid to enable the key in the keychain Specify VALID_IMMEDIATELY to set the key-chain to be valid immediately.

Steps

1. Enter config mode:
   ```
   config
   ```
2. Enable a key in a MACsec keychain:
   ```
   macsec key-chains key-chain <key-chain> mka-keys mka-key <mka-key>
   valid-date-time <valid-date-time>
   ```

Example

The following example specifies that the key named KC-1 with the mka-key as ABCD1235 to be enabled starting 13 October 2023 at 13:12:25 hours.

```
config
macsec key-chains key-chain KC-1 mka-keys mka-key ABCD1235 valid-date-
time 2023-10-13T13:12:25Z
```

8.13 Disabling a Key in a MACsec Keychain Using the CLI

Disable a key in a MACsec keychain when it is no longer required.

Overview

The following table lists the parameters to disable a key in a MACsec keychain.

Table 32: Parameters to Disable a Key in a MACsec Keychain

Parameters	Valid values	Description

key-chain	string	Specifies the name of the key chain.
mka-key	2 – 64 hex-value of even number of bits with a maximum length of 64	Identifies the Connectivity Association Key name (CKN), which identifies the CAK.
valid-date-time	DISABLED	Specify DISABLED to disable the key in the keychain. A key set to DISABLED is not considered for rollover.

Steps

1. Enter config mode:
   ```
   config
   ```
2. Disable a key in a MACsec keychain:
   ```
   macsec key-chains key-chain <key-chain> mka-keys mka-key <mka-key>
   valid-date-time <valid-date-time>
   ```

Example

The following example specifies that the key named KC-1 with the mka-key as ABCD1235 to be disabled.

```
config
macsec key-chains key-chain KC-1 mka-keys mka-key ABCD1235 valid-date-
time DISABLED
```

8.14 Deleting a Key in a MACsec Keychain Using the CLI

Delete a key in a MACsec keychain when it is no longer required. Deleting an active key immediately drops the session.

Overview

The following table lists the parameters to delete a key in a MACsec keychain.

Table 33: Parameters to Delete a Key in a MACsec Keychain

Parameters	Valid values	Description
key-chain	string	Specifies the name of the key chain.
mka-key	2 - 64 hex-value of even number of bits with a maximum length of 64	Identifies the Connectivity Association Key name (CKN), which identifies the CAK.

Steps

1. Enter config mode:
   ```
   config
   ```
2. Delete a key in a MACsec keychain:
   ```
   no macsec key-chains key-chain <key-chain> mka-keys mka-key <mka-key>
   ```

Example

The following example deletes a key named KC-1 with the mka-key as ABCD1236.

```
config
no macsec key-chains key-chain KC-1 mka-keys mka-key ABCD1236
```

8.15 Displaying MACsec Key-Chains Using the CLI

Display MACsec key-chains to learn more about the configuration.

Overview

The following table lists the parameter for displaying MACsec key-chains.

Table 34: Parameter for Displaying MACsec Key-Chains

Parameters	Valid values	Description
key-chain	string	Specifies the key chain.

Steps

1. Display MACsec key-chains:
   ```
   show macsec key-chains key-chain <key-chain>
   ```

Example

The following example displays the MACsec key-chain for the key-chain named KC-1.

```
show macsec key-chains key-chain KC-1
+------------- KEY-CHAIN -------------+
| Key-Chain       | KC-1               |
+-----------------+--------------------+
| MKA Name        | ABCD1234           |
| MKA Crypto Algo | AES_128_CMAC       |
| Start Time      | VALID_IMMEDIATELY  |
| Expiry Time     | NO_EXPIRATION      |
+-----------------+--------------------+
```

8.16 Displaying MACsec Profiles Using the CLI

Display the MACsec profiles to learn more about the configuration.

Overview

The following table lists the parameter for displaying MACsec profiles.

Table 35: Parameter for Displaying MACsec Profiles

Parameters	Valid values	Description
profile	string	Specifies the MACsec profile.

Steps

1. Display MACsec profiles:
   ```
   show macsec profiles profile <profile>
   ```

Example

The following example displays the MACsec profile named fp-xpn-pf.

```
show macsec profiles profile fp-xpn-pf

+-------------- MACSEC-PROFILES --------------+
| KEY                        | VALUE           |
+----------------------------+-----------------+
| Profile Name               | fp-xpn-pf       |
| Cipher Suite               | GCM_AES_XPN_256 |
| Conf Offset                | 0_BYTES         |
| Replay Window Size         | 2               |
| Additional Bytes In Clear  | 0               |
| Encryption                 | True            |
| Key Server Priority        | 100             |
| SAK Rekey Interval         | 240             |
+----------------------------+-----------------+
```

8.17 Displaying MACsec Interfaces Using the CLI

Display information for MACsec interfaces to learn more about the configuration.

Overview

The following table lists the parameter for displaying MACsec interfaces.

Table 36: Parameter for Displaying MACsec Interfaces

Parameters	Valid values	Description
interface	string	Specifies the interface. ***Note:*** The evaluated configuration requires this parameter to be 7 or 8.

Steps

1. Display MACsec interfaces:
   ```
   show macsec interfaces interface <interface>
   ```

Example

The following example displays information for the MACsec interface 7.

```
show macsec interfaces interface 7

+--------- MACSEC-INTERFACES ----------+
| Parameter             | Value       |
+-----------------------+-------------+
| Interface Name        | 7           |
| Strict Mode           | False       |
```

```
| Exclude Protocols     |              |
+-----------------------+--------------+
| Interface Statistics  |              |
+-----------------------+--------------+
| In Control Packets    | 37696        |
| In Data Packets       | 217836886    |
| In Dropped Packets    | 0            |
| In Errored Packets    | 0            |
| In Unicast Packets    | 217836886    |
| In Multicast Packets  | 37253        |
| In Broadcast Packets  | 0            |
| In Octets             | 331118237430 |
| Out Control Packets   | 36879        |
| Out Data Packets      | 122949124    |
| Out Dropped Packets   | 0            |
| Out Errored Packets   | 0            |
| Out Unicast Packets   | 0            |
| Out Multicast Packets | 36818        |
| Out Broadcast Packets | 0            |
| Out Octets            | 186815738557 |
+-----------------------+--------------+
```

8.18 Displaying MACsec Connection Associations Using the CLI

Display the MACsec connection associations to learn more about the configuration.

Overview

The following table lists the parameter for displaying MACsec connection associations.

Table 37: Parameter for Displaying MACsec Connection Associations

Parameters	Valid values	Description
connection-association	string	Specifies the connection-association association.

Steps

Display MACsec connection-associations:

1. Display MACsec connection-associations:
   ```
   show macsec connection-associations connection-association <connection-association>
   ```

Example

The following example displays information for the MACsec connection association named CA-2.

```
show macsec connection-associations connection-association CA-2
+-------------------- CONNECTION-ASSOCIATION --------------------+
| Parameter                               | Value                |
+-----------------------------------------+----------------------+
| CA Name                                 | CA-2                 |
| Admin State                             | enabled              |
```

```
| Oper State                              | disabled              |
| Oper State Reason                       | Peer Not Found.       |
| Key Server                              | True                  |
| Destination Address                     | 01:80:C2:00:00:03     |
| Mka Ethertype                           | 0x888e                |
| Macsec Profile                          | PFL-2                 |
| Key Chain Name                          | KC-2                  |
| Active CKN                              | 00000000000000001002  |
| Include SCI                             | False                 |
| Compatibility Mode                      |                       |
| Service Type                            | Flow Point            |
| Service Name                            | FP-8.2                |
+-----------------------------------------+-----------------------+
| Peer Secure Channel                     |                       |
+-----------------------------------------+-----------------------+
| Mac Address                             |                       |
| Port Identifier                         |                       |
+-----------------------------------------+-----------------------+
| MKA Statistics                          |                       |
+-----------------------------------------+-----------------------+
| In EAPOL MKA invalid CKN Len Frames     | 0                     |
| In EAPOL MKA invalid Frames             | 0                     |
| In EAPOL MKA Frames                     | 0                     |
| Out EAPOL MKA Frames                    | 80759                 |
| In Version Mismatch Frames              | 0                     |
| In CKN Mismatch Frames                  | 0                     |
| In ICV Mismatch Frames                  | 0                     |
+-----------------------------------------+-----------------------+
| Data Statistics                         |                       |
+-----------------------------------------+-----------------------+
| In Valid Packets                        | 0                     |
| In Error Packets                        | 0                     |
| In Transform Error Packets              | 0                     |
| In Control Packets                      | 0                     |
| In Untagged Packets                     | 0                     |
| In No Tag Packets                       | 0                     |
| In Bad Tag Packets                      | 0                     |
| In No SCI Packets                       | 0                     |
| In Unknown Packets                      | 0                     |
| In Unused SA Packets                    | 0                     |
| In Unused SA Discarded Packets          | 0                     |
| In Overrun Discarded Packets            | 0                     |
| In Unchecked Packets                    | 0                     |
| In Invalid Packets                      | 0                     |
| In Invalid with Sectag C-bit=1 Packets  | 0                     |
| In Delayed Packets                      | 0                     |
| In Late Packets                         | 0                     |
| In Decrypted Octets                     | 0                     |
| In Validated Octets                     | 0                     |
| Out Encrypted Packets                   | 0                     |
| Out Protected Packets                   | 0                     |
| Out Control Packets                     | 0                     |
| Out Untagged Packets                    | 0                     |
```

```
| Out Transform Error Packets            | 0                    |
| Out Too Long Discarded Packets         | 0                    |
| Out Encrypted Octets                   | 0                    |
| Out Protected Octets                   | 0                    |
+----------------------------------------+----------------------+
```

9 System Logging

The TOE is able to generate audit records that are stored internally within the TOE whenever an audited event occurs, as well as simultaneously offloaded to an external syslog server.

The administrator can set the level of the audit records to be stored in a local buffer, displayed on the console, sent to the syslog server, or all of the above.

9.1 Audit Records Description

The TOE generates an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include, cryptography related events, identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in Table 43: Audit Events and Sample RecordTable 43). Each of the events is specified in syslog records in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred.
Additionally, the startup and shutdown of the audit functionality is audited. The local audit trail consists of the individual audit records; one audit record for each event that occurred. The audit record can contain up to 80 characters and a percent sign (%), which follows the time-stamp information. The audit fields in each audit event will contain at a minimum the following:
Example
Audit Event: Nov 22 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self-test info: (AES encryption/decryption ... passed)

Date: Nov 22
Time: 13:55:59
Type of event: %CRYPTO-6-SELF_TEST_RESULT
Subject identity: Available when the command is run by an authorized TOE administrator user such as “user: lab”. In cases where the audit event is not associated with an authorized user, an IP address may be provided for the NonTOE endpoint and/ or TOE.
Outcome (Success or Failure): Success may be explicitly stated with “success” or “passed” contained within the audit event or is implicit in that there is not a failure or error message.
More specifically for failed logins, a “Login failed” will appear in the audit event. For successful logins, a “Login success” will appear in the associated audit event. For failed events “failure” will be denoted in the audit event. For other audit events a detailed description of the outcome may be given in lieu of an explicit success or failure.
Additional Audit Information: As described in Column 3 of Table 43.

As noted above, the information includes at least all of the required information. Example audit events are included in Table 43. The auditable events that result from administrative actions are included in Table 43 and are designated with 'Administrative Actions' within the Auditable Events column.

9.2 Turn Logging On/Off

The evaluated configuration requires the TOE to generate audit records. Therefore, the Administrator must perform the following command:

The following example shows how to enable configuration logging:

- `config`
- `syslog log-actions remote-syslog-tls admin-state enabled`

The following example shows how to disable configuration logging:

- `config`
- `syslog log-actions remote-syslog-tls admin-state disabled`

9.3 Local Logs

The local log buffer is circular. By default, newer messages overwrite older messages after the buffer is full. Administrators are instructed to monitor the log buffer using the show "ls -lh auth.log*" command to view the audit records. The first message displayed is the oldest message in the buffer.

When configured for a syslog backup the TOE will simultaneously offload events from a separate buffer to the external syslog server. This buffer is used to queue events to be sent to the syslog server if the connection to the server is lost. It is a circular buffer, so when the events overrun the storage space overwrites older events.

```
diag@CGSI3926.ui:/mnt/log/central-logger$ ls -lh auth.log*
-rw-r----- 1 root logs  32K May 26 18:09 auth.log
-rw-r----- 1 root logs  912 Oct 17  2022 auth.log-20221017-1665999761.gz
-rw-r----- 1 root logs  12K Nov 17  2022 auth.log-20221117-1668678792.gz
-rw-r----- 1 root logs 497K Apr 13 18:00 auth.log-20230413-1681408801.gz
-rw-r----- 1 root logs  57K May  3 07:33 auth.log-20230503-1683100859.gz
-rw-r----- 1 root logs  568 May  3 09:33 auth.log-20230503-1683109320.gz
-rw-r----- 1 root logs 1.7K May  3 10:58 auth.log-20230503-1683111542
diag@CGSI3926.ui:/mnt/log/central-logger$
```

9.3.1 Viewing Log Events

To view the audit logs on the console, use the following command to display all logs:

```
CGSI3926> log view events
```

9.3.2 Deleting Audit Records

Only authorized administrators may view and clear audit records using the CLI which is the sole interface to the management functions of the TOE. Protected access to the local audit records is configured by default and therefore, does not need an administrator action at startup. This only clears the cli view of log events and does not clear the physical logs files in /mnt/log/central-logger.

```
CGSI3926> log clear events
Successfully cleared events logs
CGSI3926>
```

9.4 CONFIGURING SYSLOG

To protect against audit data loss the TOE must be configured to send the audit records securely (through TLS) to an external Secure Syslog Server. By default, system messages are logged to the console and the logfile for the evaluated configuration all of the severity levels are set to ensure all required audit events related to the TOE Security Functions are audited and sent to the syslog server.

1. Enter configuration mode:
   `config`
2. Enable logging:
   `syslog log-actions remote-syslog-tls admin-state <enable|disable>`
3. Identify the IP address of the syslog server:
   `syslog log-actions remote-syslog-tls destination <ip address or DNS>`
4. Assign a TLS Profile to the connection:
   `syslog log-actions remote-syslog-tls tls-service-profile <profile name>`
5. Set TLS timeout. The units for this parameter are seconds. The default is 6 seconds.
   `syslog log-actions remote-syslog-tls timeout 6`

The parameter `tls-service-profile` points to a TLS Profile. Refer to section 6 to create a TLS Profile.

If any of the established trusted channels/paths are unintentionally broken, the connection will need to be re-established following the configuration settings as described in this section.

9.5 CONFIGURING LOG LEVEL

Table 38: Log Level

Parameter	Valid values	Description
Address	IP address	Specifies the IP address of the secure syslog destination.
Severity	alert, critical, debug, emergency, error, info, notice, warning	Sets the severity of secure syslog destination. ***Note:*** the evaluated configuration requires all values set.

Steps

1. Enter configuration mode:
   `config`
2. Configure the severity of secure syslog messages.

```
syslog log-action remote-syslog-tls destination <address> severity
<severity>
```

Example

1. Configure the severity of secure syslog messages for the evaluated configuration.

```
config
syslog log-action remote-syslog-tls destination 10.1.5.200 severity
alert critical debug emergency error info notice warning
```

9.6 LOGGING PROTECTION

To protect against audit data loss the TOE must be configured to send the audit records securely (through TLS) to an external Secure Syslog Server. By default, system messages are logged to the console and the logfile, for the evaluated configuration the severity level must be set to “debugging” to ensure all required audit events related to the TOE Security Functions are audited and sent to the syslog server.

It is recommended that the implemented syslog server complies with the standards documented. It is also expected that the software is the current version and is regularly updated with the latest patches.

Using a secure TLS connection for Syslog Server is required in the evaluated configuration: TLS 1.2 with support for the following ciphers. For information on configuring the cipher suite refer to Chapter 6, Transport Layer Security in [1].

Logging of all required audit events related to TOE security functions must be enabled in the evaluated configuration.

Note: To get some of the required audit records with the required information, debugging may need to be turned on/configured. In doing so, a large amount of audit records may be generated. To configure syslog in the evaluated configuration the following commands must be executed.

The following steps are required to configure a syslog server.

1. Assign a TLS profile to syslog.
   - `config`
   - `syslog log-actions remote-syslog-tls tls-service-profile <profile name>`
2. Enable remote logging.
   - `syslog log-actions remote-syslog-tls admin-state enabled`
3. Identify the syslog server.
   - `syslog log-actions remote-syslog-tls destination <Syslog TLS server IP address or a DNS domain name>`
4. Set the timeout for syslog TLS server response (in seconds)
   - `syslog log-actions remote-syslog-tls timeout 6`

9.6.1 LOGGING TO SYSLOG SERVER VIA TLS

Once the above steps are complete, then logging to the syslog server via TLS needs to be setup. To protect against audit data loss the TOE must be configured to send the audit records securely (via TLS) to an external Secure Syslog Server. You can use the server hostname for this configuration. Based on the

configured severity, the router sends syslogs to the server. Logging severity options include alerts, critical, debugging, emergencies, errors, informational, notifications and warnings.

1. Enter configuration mode:
   `config`
2. Configure the name of the TLS service profile list:
   `tls-service-profiles <tls-service-profile-name>`
3. Identify the name of the certificate:
   `tls-service-profiles <tls_service_profile_name> tls-certificate-name <tls_certificate_name>`
4. Identify the name of the peer authentication profile:
   `tls-service-profiles <tls_service_profile_name> tls-peer-auth-profile-name <tle_peer_auth_profile_name>`
5. Identify the name of the hello-params profile:
   `tls-service-profiles <tls_service_profile_name> tls-profile-name <tls_profile_name>`
6. Configure the name of the user defined peer authentication profile:
   `pkix peer-auth-profiles peer-auth-profile <peer_auth_profile_name>`
7. Set ip/host checks:
   `pkix peer-auth-profiles peer-auth-profile <peer_auth_profile_name> check-ip-host true`
8. Identify the list of acceptable server connections:
   `pkix peer-auth-profiles peer-auth-profile <peer_auth_profile_name> ip-host-list <ip_address>`

392639263926392639263926

Check the TLS configuration by following command and output

```
CGSI3926> sh tls
+------------ TLS SERVICE PROFILES -----------+
| Name                    | Value              |
+-------------------------+--------------------+
| Service Profile Name    | syslog-tls-service |
| TLS Profile Name        | syslog-tls         |
| Peer Auth Profile Name | syslog-profile     |
| Certificate Name        | device_cert        |
+-------------------------+--------------------+

+-------------- PEER AUTH PROFILES ----------+
| Name                         | Value          |
+------------------------------+----------------+
| Profile Name                 | syslog-profile |
| Check Expiry                 | True           |
| Check IP/Host                | False          |
| Check Fingerprint            | False          |
| Strict Extended Key Usage | False          |
| IP/Host List                 | 10.1.5.207     |
| Fingerprint List             | -              |
+------------------------------+----------------+

 +---------------------------- HELLO PARAMS ----------------------------+
| Name                           | Value                                 |
+--------------------------------+---------------------------------------+
```

```
| Profile Name                 | tls-profile                          |
| Protocol Versions            | tls-1.2                              |
| Cipher Suites                | rsa-with-aes-128-cbc-sha,            |
|                              | rsa-with-aes-256-cbc-sha,            |
|                              | rsa-with-aes-128-cbc-sha256,         |
|                              | rsa-with-aes-256-cbc-sha256,         |
|                              | rsa-with-aes-128-gcm-sha256,         |
|                              | rsa-with-aes-256-gcm-sha384,         |
|                              | ecdhe-rsa-with-aes-128-cbc-sha,      |
|                              | ecdhe-rsa-with-aes-256-cbc-sha,      |
|                              | ecdhe-rsa-with-aes-128-cbc-sha256,   |
|                              | ecdhe-rsa-with-aes-256-cbc-sha384,   |
|                              | ecdhe-rsa-with-aes-128-gcm-sha256,   |
|                              | ecdhe-rsa-with-aes-256-gcm-sha384    |
| Elliptic Curves              | secp256r1,secp384r1,secp521r1        |
| Sess. Resumption Timeout (s) | 3600                                 |
| OCSP State                   | enabled                              |
| NONCE State                  | enabled                              |
| Default OCSP Responder URL   | -                                    |
+------------------------------+--------------------------------------+

CGSI3926>
```

10 User Account Configuration and Management

The TOE provides administrative users with a CLI to interact with and manage the security functions of the TOE.
Once the device is successfully installed the Ciena devices perform authentication using the local database. For the evaluated configuration the TOE does not support remote authentication (TACACS and RADIUS).

The TOE requires successful identification and authentication of each administrator prior to granting them access to the TOE. Access to the TOE is given to the user by making available a shell in which the user can execute CLI commands. Without access to the shell, the CLI is not accessible to the user and, consequently, administrator accesses are not possible. There are no management functions other than those accessible through the CLI.

The only access the TOE allows prior to the successful identification and authentication of the user is the access banner displayed at each login prompt.

10.1 Default User Login

The system is pre-configured with a default user account, diag, and password, ciena123. This default user account is common to all Ciena packet networking products and is not confidential. Ciena recommends that this default user account is deleted to protect the system upon startup.

When the initial login prompt is displayed, press **Enter** and enter the default username and password.

Example

```
login: diag
Password: ciena123
System response:
!!! This is a private network. Any unauthorized access or use will lead
to prosecution!!!
SAOS. The next generation in switching software.
```

10.2 Login Banners

The evaluated configuration requires the TOE to display an advisory notice and consent warning message regarding use of the TOE before any logon completion. The **login banner** command configures the banner for both SSH and local sessions. For a password-based SSH remote connection, the banner is displayed after the username and before the password prompts (except for the initial login). For a public key based SSH remote connection, the banner is displayed after successful authentication. For local access to the TOE, the banner is displayed before the prompt for the username. As displayed above, the default banner is:

```
!!! This is a private network. Any unauthorized access or use will lead
to prosecution!!!
SAOS. The next generation in switching software.
```

Steps

1. Enter configuration mode:
   ```
   config
   ```

2. Set the system welcome-banner:
   `system config login-banner <banner-text>`

Example

The following example sets the system welcome-banner to “This is a banner”:

```
config
system config login-banner “This is a banner”
```

Note: Display of the Login banner is the only service that is available prior to identification and authentication. No configuration is required to ensure that the access to services is limited prior to login.

10.3 Local User Groups

User privileges are controlled using the NETCONF/YANG access control model (NACM). The local user’s read and write privileges are managed through NACM groups. Each group has fine grained rule lists that restrict users of each group to perform certain functions/privileges. These rule lists are defined relative to the YANG data models. Refer to RFC 8341 for details on NACM and user group authorization.

By default, the system has the following three pre-defined NACM groups:

- Limited (read only)
- Admin (can make significant system changes and modify the configuration, but cannot modify user accounts or authorizations)
- Super (can make significant system changes and modify the configuration, including user accounts or authorizations)

Note: The evaluated configuration supports only one administrative role, Security Administrator. Users that belong to “Super” or “admin” groups have administrative privileges and assume the role of Security Administrator. The TOE also supports a single non-administrative role: Read-Only User. Users that belong to “Limited” group have read-only privileges. Read-Only User cannot make any changes to the TOE configuration.

10.4 Local User Roles

In addition to the NACM group, there is another aspect of a user account authorization: the user’s role. Most users are restricted to interacting with the system through the YANG-modeled NETCONF or CLI interfaces. Specially privileged users, however, can access the underlying base Linux system for special diagnostic purposes. This diagnostic role is not needed for normal system management, and this role should be restricted to users who need this special diagnostic level of access.

The following table describes local user roles.

Table 39: Local User Roles

Role	Description
SYSTEM_ROLE_USER	Allows access to the underlying system through NETCONF or the CLI.

SYSTEM_ROLE_DIAG	Allows access to the underlying base Linux shell as well as through the normal NETCONF or CLI.

Note: NETCONF access and the SYSTEM_ROLE_DIAG role are not included in the evaluated configuration.

10.5 Username Authentication, Authorization, and Accounting (AAA)

The TOE supports multiple AAA Servers supporting AAA services including TACACS, RADUIS, and RADSEC. The TOE, in its evaluated configuration only supports local management of users/passwords.

Note: Configuring remote authentication will take the TOE out of the evaluated configuration.

10.6 Passwords Rules

The user password-policy establishes a policy that user passwords must adhere to.

The user password-policy configures the following but is not limited to:

- if dictionary words can be used within passwords
- if the username or its reverse can be used within the associated account password
- the minimum number of uppercase, lowercase, numeric, special and total characters in account passwords
- the maximum number of times a character can be consecutively repeated in a password

The evaluated configuration requires passwords to be a minimum length of 1-128 characters (inclusive) and composed of any combination of upper and lower case letters, numbers, and the following special characters: *"!", "@", "#", "$", "%", "^", "&", "*", "(", ")", "", "+", "", "-", "", "/", ":", ",", "<", "=", ">", "[", "\", "]", " _ ", "`", "{", "}", "<space>", and "~"*.

10.6.1 Configure the user password-policy to the TOE.

The following commands provide an example of implementing a company's password-policy rules. Consult your company's individual password-policy rules before configuring the password policy commands.

Note: For more information about password policy commands refer to your Ciena platform's Administration SAOS 10.7.1 Guide.

Note: to configure the TOE in the evaluated configuration the Administrator must set the minimum length of the passwords.

Steps

1. Enter configuration mode:
   `config`
2. Configure the minimum length of the password:
   `system aaa authentication password-policy config min-length <integer>`
3. Configure the minimum number of lower-case characters:
   `system aaa authentication password-policy config min-lowercase-chars <integer>`

4. Configure the minimum number of numeric characters:
   ```
   system aaa authentication password-policy config min-numeric-chars
   <integer>
   ```
5. Configure the minimum number of special characters:
   ```
   system aaa authentication password-policy config min-special-chars
   <integer>
   ```
6. Configure the minimum number of upper-case characters:
   ```
   system aaa authentication password-policy config min-uppercase-chars
   <integer>
   ```
7. Configure whether dictionary words are disallowed:
   ```
   system aaa authentication password-policy config disallow-dict-words
   <on|off>
   ```
8. Configure whether including the username as part of the password is disallowed:
   ```
   system aaa authentication password-policy config disallow-username
   <on|off>
   ```
9. Configure the maximum number of repeated characters:
   ```
   system aaa authentication password-policy config max-repeated-chars
   <integer>
   ```
10. Configure the number of preceding passwords that are disallowed when setting a new password for that user:
    ```
    system aaa authentication password-policy config past-password-history
    <integer>
    ```

Example

The following example configures the user password-policy. In this example, the password may not contain dictionary words, username or its reverse. It also requires that the password be at least 10 characters long and contain at least one lowercase character and one numeric character. It does not require the password to contain any special characters, nor does it set the past-password-history parameter.

```
config
system aaa authentication password-policy config disallow-dict-words on
system aaa authentication password-policy config disallow-username on
system aaa authentication password-policy config min-length 10
system aaa authentication password-policy config min-lowercase-chars 1
system aaa authentication password-policy config min-numeric-chars 1
system aaa authentication password-policy config minspecial-chars 0
```

10.7 PROTECTED AUTHENTICATION FEEDBACK

The TOE does not provide any feedback for the password characters entered other than a config mode save failed message if the password does not meet the configured password policies.. This is by default and does not require any configuration.

10.8 User Management Commands

10.8.1 Creating a New User

When a new user is created, it must be added to one of the existing NACM groups or a new NACM group must be created that has the appropriate rules to allow the user to read and write data. The default user groups are as follows:

- Limited (read only)
- Admin (can make significant system changes and modify the configuration, but cannot modify user accounts or authorizations)
- Super (can make significant system changes and modify the configuration, including user accounts or authorizations)

Note: Users that belong to “Super” or “admin” groups have administrative privileges and assume the role of Security Administrator. The TOE also supports a single non-administrative role: Read-Only User. Users that belong to “Limited” group have read-only privileges. Read-Only User cannot make any changes to the TOE configuration.

The following table describes the parameters for creating a new user account.

Table 40: New User Account Parameters

Parameter	Valid values	Description
User	String	Specifies the name associated with the user account.
Config role	SYSTEM_ROLE_DIAG SYSTEM_ROLE_USER	Indicates the access level associated with the user account. • SYSTEM_ROLE_DIAG: allows access to Linux • SYSTEM_ROLE_USER: allows access to yp-shell
password password	string	Specifies the password associated with the user account. The password is displayed in clear text and stored as a hash. The password must be in quotation marks when the password contains special characters.
password-hashed password	string	Specifies the password associated with the user account. The password is hashed when it is entered.

Perform the following steps to create a new user account.

Steps

1. Enter configuration mode:
   `config`
2. Create a new account.
   `system aaa authentication users user <user> config role`

```
<SYSTEM_ROLE_DIAG|SYSTEM_ROLE_USER> username <user> <password|password-hashed> <password>
```

3. Exit configuration mode:
   ```
   exit
   ```
4. Verify the newly created account by display the accounts in the system.
   ```
   show aaa users
   ```
5. Repeat the previous steps to create another user account.

Example

The following example creates a new user account User1 with the role of SYSTEM_ROLE_USER and the password of changeme.

```
config
system aaa authentication users user User1 config role SYSTEM_ROLE_USER
username User1 password changeme
```

10.8.2 Adding a User to a Group

Add users to a group. All the users in a group have the same access privileges.

The following table describes the parameters to add a user to a group.

Table 41: Parameters for adding a user to a group

Parameters	Valid values	Description
group	super, admin, limited	Specifies the group that the user will be part of. ***Note:*** the evaluated configuration requires this parameter must be configured to the group values specified here (super, admin, and limited).
user-name	String	Specifies the user name being added.

Steps

1. Enter configuration mode:
   ```
   config
   ```
2. Add a user to a group:
   ```
   nacm groups group <group> user-name <user-name>
   ```

Example

The following example adds the user user1 to the super group.

```
config
nacm groups group super user-name user1
```

For more information about user account configuration and management refer to your Ciena platform's Administration SAOS 10.7.1 Guide.

10.8.3 USER SESSION TERMINATION

The TOE allows termination of a user's own interactive session using the 'exit' command. This command applies to both local and remote sessions.

Example:

```
exit
```

10.9 USER LOCKOUT POLICY

The evaluated configuration requires that the administrator configure a lockout policy. This policy will lockout users for an administrator configured amount of time after an administrator defined number of failed consecutive login attempts.

The evaluated configuration requires the Administrator to configure the user lockout-policy to set a level of sequential login failures to lock the account until the lockout period has expired. Only SSH protocol is supported for configuration of user lockout attributes.

Note: Administrator lockouts are not applicable to the local console. Local administrators cannot be locked out and have the ability to unlock other users by using the local console.

The lockout policy applies only to remote users.

Steps

1. Enter configuration mode:
   `config`
2. Configure the number of failed login attempts before lockout:
   `system aaa authentication lockout-policy config fail-limit <integer>`
   Note: The configurable integer is in the range 1-5.
3. Configure the duration of the lockout:
   `system aaa authentication lockout-policy config lockout-time <integer>`
   Note: The value in integer is for seconds as unit.

Example

The following two commands lock out users for one minute after three failed login attempts.

```
config
system aaa authentication lockout-policy config fail-limit 3
system aaa authentication lockout-policy config lockout-time 60
```

11 SELF-TESTS

The TOE runs a suite of self-tests during:

- during initial start-up (on power on),

The TOE is required to perform at least the following self-tests:

- Verification of the integrity of the firmware and executable software of the TOE
- Verification of the correct operation of the cryptographic functions necessary to fulfil any of the SFRs.

Specifically, the TOE runs the following tests:

- Check of flash access and content with CRC (i.e, integrity check),
- Check of various Field-programmable gate array (FPGA) devices access and sanity
    - Verify control FPGA by writing a known value to a scratchpad area and verify it can be read back
- Probe the PCI bus and verify the devices are present as expected for that board type,
- Sanity check of memory to ensure no corruption
    - Error correction code (ECC) memory uncorrectable error verification, and check the appropriate memory size is reported by the driver for the board type
- Check of FANS for operational state
    - Verify fans presence and fans are not stalled on the 3926 devices via status information queried from the controlling FPGA
    - Verify power supply voltage and current operating values are within specification as queried from controlling FPGA
- Crypto KAT/self-test (including AES, SHS, HMAC, RSA, ECDSA and DRBG)

If the self-tests fail, the failure will be reported on the workstation's screen and the system will halt. If any self-test fails, the Administrator should contact Ciena support at www.ciena.com.

12 PRODUCT UPDATES

System software is retrieved from the Ciena Support Portal in the form of an archive file that includes a folder structure with various versioned software artifacts in it. The artifacts for a particular package are the complete set for that package, potentially including artifacts that were initially released in prior packages. Note that the versions of artifacts inside the package are not related to the version of the package itself. The following table lists terms used for upgrading software.

Table 42: Terms used for upgrading software

Term	Description
artifact	Typically a container, but can also refer to a package
manifest	A file that specifies the universe of artifacts for a particular software release or package.
download	The retrieval of an artifact or artifacts from the file server to the local cache on the system.
install	Potentially unpacking artifacts from the local cache and preparing them for activation, for example, getting them into the docker registry.
activate	Switching over to new artifacts so that they become the running set. Activation also means tearing down the current running artifacts or replacing them as needed. Activation of new artifacts happens automatically as part of the installation process. An administrator can also manually activate the previously installed artifacts to revert to a previous version if required.

To make a package available to the system on a network, the package is unpacked to a file server or web server at a URL which is accessible to the system.

For example, if you are using an FTP server, you might keep all Ciena artifacts at ftp://ftp.example.com/ciena. If that URL refers to the directory path /var/ftp/ciena on the ftp.example.com server, then you would unpack the zip archive there. You have two choices:

- Keep all packages segregated. For example, unpack `saos-10-00-00-0131-packages.zip` to `/var/ftp/ciena/saos-10-00-00-0131`.

  To install this package, refer to it by means of the URL `ftp://ftp.example.com/ciena/saos-10-00-00-0131-packages/saos-10-00-00-0131.yml`. Unpack `saos-10-00-00-0142-packages.zip to /var/ftp/ciena/saos-10-00-00-0142` and refer to it in the same way.

- Keep the union of all packages. This reduces the disk space needed on the FTP server by keeping only one copy of any given artifact. For example, unpack both `saos-10-00-00-0131packages.zip` and `saos-10-00-00-0142-packages.zip` to `/var/ftp/ciena`. Refer to `saos-10-00-00-0131-packages.zip` as `ftp://ftp.example.com/ciena/saos-10-00-00-0131.yml`, and to `saos-10-00-00-0142-packages.zip` as `ftp://ftp.example.com/ciena/saos-10-00-00-0142.yml`. When unpacking an archive, do not overwrite any files that already exist in the extract location.

A .sha256 file is provided as a separate download from the Ciena Support Portal to help ensure the integrity of the provided image. The administrator can calculate the hash of the update image off box (e.g. using the Windows PowerShell) prior to install and match it against the .sha256 hash file to confirm the image is valid. If the hash matches the administrator can proceed with the installation. If the hash does not match the administrator should not proceed with the installation and instead should contact Ciena support at www.ciena.com.

12.1 Updating the TOE

The TOE can be updated from the File Server.

Steps:

- `software install url <url>`

Where:
`<url> = https://<IP address of the File Server>/<filename of the new download>`

The following is an example of installing an image with new download named saos-10-07-01-0289-RS12.yml from the file server with IP address of 10.1.5.208.

```
CGSI3926>
CGSI3926> software install url https://10.1.5.208/saos-10-07-01-0289-RS12.yml tls-service-profile syslog-tls-service
```

12.2 Secure Acceptance of the TOE

When the TOE is updated, the TOE will display messages to the workstation indicating the success and or failure of the upload.

12.2.1 Successful Upload

The following shows an example of successful installation.

Example

1. Upgrade the TOE by accessing the image from the file server.

```
CGSI3926>
CGSI3926> software install url https://10.1.5.210/saos-10-07-01-0289-RS12.yml tls-service-profile service-tls
+---------- SOFTWARE PACKAGES ----------+
| Name                      | Value       |
+---------------------------+-------------+
| Available packages:       |             |
|   saos-10-07-01-0283-RS11 | activated   |
|   saos-10-07-01-0289-RS12 | downloading |
+---------------------------+-------------+
CGSI3926>
```

2. The system will report that it is downloading the image.

```
show software
```

```
Available packages:       |
  saos-10-07-01-0283-RS11 | activated
  saos-10-07-01-0289-RS12 | downloading, pulling 09 of 34: localhost:5000/cn-container-feds-docker-aarch64:01-07-01-0289
```

3. The TOE will report that the image is being installed.

```
show software
```

```
Available packages:       |
  saos-10-07-01-0283-RS11 | activated
  saos-10-07-01-0289-RS12 | installing, installing evernight-generic-arm-aarch64-01-07-01-0289-upgrade.sh on standby bank
```

Note that once the “software install” command has been issued, there is no other administrative action required. The TOE will automatically install, reboot and activate the new image (boots with the new image). During reboot all traffic interfaces along with the out of band management port will cease to operate.

12.3 VERIFYING THE TOE VERSION

To verify the current version of the TOE, perform the following command:

```
show software
```

The following displays an example output of the show software command.

```
CGSI3926> show software
+---------------------------------- SOFTWARE STATE ----------------------------------+
| Name                        | Value                                                 |
+-----------------------------+-------------------------------------------------------+
| Current operation           | idle                                                  |
| RPC Status                  | idle                                                  |
| Running package version     | saos-10-07-01-0283-RS11                               |
| Package build info          | Wed Sep 06 12:36:45 2023 autouser oncs-pnjenkins-agent008 |
| Active bootchain            | 01-07-01-0283                                         |
| Software signing            | Enabled                                               |
```

13 SECURITY RELEVANT EVENTS

Table 43: Audit Events and Sample Record

Requirement	Auditable Event	Additional Audit Record Contents	Audit Logs
FAU_GEN.1	Start-up and shut-down of the audit functions.	None	**Start-up and shut-down of audit functions:** The audit function starts up and shuts down with the TOE. **Start-up of audit function:** CC-3926-905-MACSEC> log view events **Shut-down of audit function:** CC-3926-905-MACSEC> log view events
	Administrative login and logout.	Name of user account shall be logged if individual user accounts are required for Administrators	**Administrative login:** CC-3926-905-MACSEC> log view events INFO 2024-02-12 21:46:16.177325 cn-node-evtbroker Identity(chassis): Incoming connection from 172.16.16.254 : 59172 INFO 2024-02-12 21:46:19.244926 cn-node-evtbroker Identity(chassis): User successfully logged in from IP 172.16.16.254 user name 'admin' **Administrative logout:** CC-3926-905-MACSEC> log view events INFO 2024-02-12 21:46:29.104123 cn-node-evtbroker Identity(chassis): User logged out from IP 172.16.16.254 user name 'admin' INFO 2024-02-12 21:46:35.242126 cn-node-evtbroker Identity(chassis) sshd Session '172.16.16.254:59172' for User 'admin' authentication-method Local logged out
	Ability to administer the TOE locally and remotely.	Failed login attempt & Successful login attempt	**Failed login attempt via Local Console:** CC-3926-905-MACSEC> log view events INFO 2024-02-13 06:30:51.550053 cn-node-evtbroker Identity(chassis): Login failure event alert for admin from Local:ttyPS0 CC-3926-905-MACSEC> log view security INFO 2024-02-13 06:30:40.284188 login pam_unix(login:session): session closed for user admin INFO 2024-02-13 06:30:49.520240 login pam_succeed_if(login:auth): requirement "tty =~ /dev/tty*" was met by user "admin" NOTIF 2024-02-13 06:30:51.429989 login pam_unix(login:auth): authentication failure; logname=admin uid=0 euid=0 tty=/dev/ttyPS0 ruser= rhost= user=admin NOTIF 2024-02-13 06:30:53.731026 login FAILED LOGIN (1) on '/dev/ttyPS0' FOR 'admin', Authentication failure

			Failed login attempt via SSH: CC-3926-905-MACSEC> log view security INFO 2024-09-06 17:40:16.403255 sshd pam_succeed_if(sshd:auth): requirement "tty =~ /dev/tty*" not met by user "admin" NOTIF 2024-09-06 17:40:16.429898 sshd pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh:58200 ruser= rhost=172.16.16.254 user=admin INFO 2024-09-06 17:40:18.217740 sshd Failed password for admin from 172.16.16.254 port 58200 ssh2 INFO 2024-09-06 17:40:22.094088 sshd pam_succeed_if(sshd:auth): requirement "tty =~ /dev/tty*" not met by user "admin" INFO 2024-09-06 17:40:24.058417 sshd Failed password for admin from 172.16.16.254 port 58200 ssh2 **Successful login attempt via Local Console:** CC-3926-905-MACSEC> log view events INFO 2024-02-13 06:31:06.133774 cn-node-evtbroker Identity(chassis): Login success event alert for admin from Local:ttyPS0 CC-3926-905-MACSEC> log view security INFO 2024-02-13 06:31:03.581016 login pam_succeed_if(login:auth): requirement "tty =~ /dev/tty*" was met by user "admin" INFO 2024-02-13 06:31:06.149553 login pam_unix(login:session): session opened for user admin by admin(uid=0) **Successful login attempt via SSH:** CC-3926-905-MACSEC> log view events INFO 2024-09-06 18:38:35.943043 cn-node-evtbroker Identity(chassis): Login success event alert for admin from 172.16.16.254:58212 INFO 2024-09-06 18:38:36.064628 cn-node-evtbroker Identity(chassis): User successfully logged in from IP 172.16.16.254 user name 'admin' CC-3926-905-MACSEC> log view security INFO 2024-09-06 18:40:39.153751 sshd pam_succeed_if(sshd:auth): requirement "tty =~ /dev/tty*" not met by user "admin" INFO 2024-09-06 18:40:39.457448 sshd Accepted password for admin from 172.16.16.254 port 58214 ssh2 INFO 2024-09-06 18:40:39.467686 sshd pam_unix(sshd:session): session opened for user admin by (uid=0)
	Ability to configure the access banner.	None	CC-3926-905-MACSEC> log view events NOTIF 2024-02-13 06:51:44.375562 cn-node-evtbroker Netconf(chassis): Session ID: 503; Username: admin; Client IP: 127.0.0.1; Target XPath: /oc-sys:system/oc-sys:config/oc-sys:motd-banner; Edit Operation: create

	Ability to configure the session inactivity time before session termination or locking.	None	**Local Console session termination:** CC-3926-905-MACSEC> log view events NOTIF 2024-09-06 19:06:12.237195 cn-node-evtbroker Netconf(chassis): Session ID: 262; Username: admin; Client IP: 127.0.0.1; Target XPath: /oc-sys:system/oc-sys:ssh-server/oc-sys:config/oc-sys:timeout; Edit Operation: create **SSH session termination:** CC-3926-905-MACSEC> log view events NOTIF 2024-09-06 19:03:55.408625 cn-node-evtbroker Netconf(chassis): Session ID: 267; Username: admin; Client IP: 172.16.16.254; Target XPath: /oc-sys:system/oc-sys:ssh-server/oc-sys:config/oc-sys:timeout; Edit Operation: create
	Ability to update the TOE, and to verify the updates using [hash comparison] capability prior to installing those updates.	None	**Verify the updates using [hash comparison] capability prior to installing those updates:** Not applicable as the hash validation of the image is performed off box by an administrator. **Ability to update the TOE:** CC-3926-905-MACSEC> log view troubleshoot INFO 2024-09-03 17:46:46.300356 xgrade-ng Operation requested: {'operation': 'install', 'options': {'manifest_url': 'http://172.16.16.254/saos-10-09-01-0220-packages/saos-10-09-01-0220.yml', 'defer_activation': False, 'manifest_hash_algorithm': 'sha-256'}} INFO 2024-09-03 18:02:40.804259 xgrade-ng finished operation: {'operation': 'install', 'options': {'manifest_url': 'http://172.16.16.254/saos-10-09-01-0220-packages/saos-10-09-01-0220.yml', 'defer_activation': False, 'manifest_hash_algorithm': 'sha-256', 'RTSC_required': None}, 'package_name': 'saos-10-09-01-0220', 'retries': 0, 'operation_timeout': 1555, 'latest_log': 'installing /mnt/config/image/evernight-generic-arm-aarch64-01-09-01-0220-upgrade.sh on standby bank'}
	Ability to configure the authentication failure parameters for FIA_AFL.1.	None	CC-3926-905-MACSEC> log view events NOTIF 2024-09-06 19:14:53.179119 cn-node-evtbroker Netconf(chassis): Session ID: 267; Username: admin; Client IP: 172.16.16.254; Target XPath: /oc-sys:system/oc-sys:aaa/oc-sys:authentication/ciena-oc-aaa:lockout-policy; Edit Operation: create
	Ability to modify the behavior of the transmission of audit data to an external IT entity.	None	CC-3926-905-MACSEC> log view events NOTIF 2024-02-13 07:18:11.911679 cn-node-evtbroker Netconf(chassis): Session ID: 497; Username: admin; Client IP: 172.16.16.254; Target XPath: /syslog:syslog/syslog:log-actions/ciena-syslog-tls:remote-syslog-tls/ciena-syslog-tls:admin-state; Edit Operation: merge

	Ability to manage the cryptographic keys.	None	**Install:** CC-3926-905-MACSEC> log view events INFO 2024-09-04 19:32:06.928077 cn-node-evtbroker Identity(chassis): User Pubkey admin.pub is successfully installed by admin from 172.16.16.254 CC-3926-905-MACSEC> log view security EMERG 2024-09-04 19:32:06.922240 netconfd-pro User Pubkey admin.pub is successfully installed by admin from 172.16.16.254 **Edit:** CC-3926-905-MACSEC> log view events INFO 2024-09-04 19:38:05.087221 cn-node-evtbroker Identity(chassis): User Pubkey admin.pub is successfully changed by admin from 172.16.16.254 CC-3926-905-MACSEC> log view security EMERG 2024-09-04 19:38:05.076692 netconfd-pro User Pubkey admin.pub is successfully changed by admin from 172.16.16.254 **Remove:** CC-3926-905-MACSEC> log view events INFO 2024-09-04 19:13:51.459781 cn-node-evtbroker Identity(chassis): User Pubkey admin.pub is successfully deleted by admin from 172.16.16.254 CC-3926-905-MACSEC> log view security EMERG 2024-09-04 19:13:51.449548 netconfd-pro User Pubkey admin.pub is successfully deleted by admin from 172.16.16.254
	Ability to configure the cryptographic functionality.	None	CC-3926-905-MACSEC> log view events INFO 2024-09-04 19:38:05.087221 cn-node-evtbroker Identity(chassis): User Pubkey admin.pub is successfully changed by admin from 172.16.16.254
	Ability to set the time which is used for time stamps.	None	CC-3926-905-MACSEC> log view events INFO 2024-02-13 07:30:00.024093 cn-node-evtbroker System(chassis): Clock change alert; configured-value: 2024-02-13T07:30:00Z
	Ability to configure thresholds for SSH rekeying.	None	CC-3926-905-MACSEC> log view events NOTIF 2024-09-06 19:34:32.521196 cn-node-evtbroker Netconf(chassis): Session ID: 268; Username: admin; Client IP: 172.16.16.254; Target XPath: /oc-sys:system/oc-sys:ssh-server/oc-sys:config/ciena-oc-sys:rekey-time; Edit Operation: create
	Ability to configure the reference identifier for the peer.	None	**Add:** CC-3926-905-MACSEC> log view events NOTIF 2024-09-04 19:50:07.585068 cn-node-evtbroker Netconf(chassis): Session ID: 256; Username: admin; Client IP: 172.16.16.254; Target XPath: /syslog:syslog/syslog:log-actions/ciena-syslog-tls:remote-syslog-tls/ciena-syslog-tls:destination[ciena-syslog-tls:address="172.16.16.254"]; Edit Operation: create

			Remove: CC-3926-905-MACSEC> log view events NOTIF 2024-09-04 19:49:25.216573 cn-node-evtbroker Netconf(chassis): Session ID: 256; Username: admin; Client IP: 172.16.16.254; Target XPath: /syslog:syslog/syslog:log-actions/ciena-syslog-tls:remote-syslog-tls/ciena-syslog-tls:destination[ciena-syslog-tls:address="172.16.16.254"]; Edit Operation: remove
	Ability to manage TOE's trust store and designate X.509v3 certificates as trust anchors.	None	CC-3926-905-MACSEC> log view events INFO 2024-01-12 21:25:04.145312 cn-node-evtbroker User 'admin' successfully uninstalled X.509 CA certificate with name subca-rsa. Result: success
	Ability to import X.509v3 certificates to the TOE's trust store.	None	CC-3926-905-MACSEC> log view events INFO 2024-01-12 21:26:24.762338 cn-node-evtbroker User 'admin' successfully installed X.509 CA certificate with name subca-rsa. Result: success
	Ability to manage the trusted public keys database.	Managing CA certificate list	CC-3926-905-MACSEC> log view events INFO 2024-01-12 21:25:04.145312 cn-node-evtbroker User 'admin' successfully uninstalled X.509 CA certificate with name subca-rsa. Result: success INFO 2024-01-12 21:26:24.762338 cn-node-evtbroker User 'admin' successfully installed X.509 CA certificate with name subca-rsa. Result: success
	Generation/import of, changing, or deleting of cryptographic keys.	In addition to the action itself, a unique key name or key reference shall be logged	**Generate/Import:** CC-3926-905-MACSEC> log view events INFO 2024-09-04 19:32:06.928077 cn-node-evtbroker Identity(chassis): User Pubkey admin.pub is successfully installed by admin from 172.16.16.254 CC-3926-905-MACSEC> log view security EMERG 2024-09-04 19:32:06.922240 netconfd-pro User Pubkey admin.pub is successfully installed by admin from 172.16.16.254 **Remove:** CC-3926-905-MACSEC> log view events INFO 2024-09-04 19:13:51.459781 cn-node-evtbroker Identity(chassis): User Pubkey admin.pub is successfully deleted by admin from 172.16.16.254 CC-3926-905-MACSEC> log view security EMERG 2024-09-04 19:13:51.449548 netconfd-pro User Pubkey admin.pub is successfully deleted by admin from 172.16.16.254
	Resetting passwords.	None	CC-3926-905-MACSEC> log view events NOTIF 2024-01-12 14:49:27.417987 cn-node-evtbroker Netconf(chassis): Session ID: 427; Username: admin; Client IP: 172.16.16.254; Target XPath: /oc-sys:system/oc-sys:aaa/oc-sys:authentication/oc-sys:users/oc-sys:user[oc-

			sys:username="user"]/oc-sys:config/ciena-oc-sys:password; Edit Operation: create
FAU_GEN.2	None	None	
FAU_STG.1	None	None	
FAU_STG_EXT.1	Protected audit event storage.	Able to send data to audit server in encrypted format, not in plaintext format	CC-3926-905-MACSEC> log view events NOTIF 2024-09-11 15:00:17.810353 cn-node-evtbroker Netconf(chassis): Session ID: 311; Username: admin; Client IP: 172.16.16.254; Target XPath: /syslog:syslog/syslog:log-actions/ciena-syslog-tls:remote-syslog-tls/ciena-syslog-tls:destination[ciena-syslog-tls:address="172.16.16.254"]; Edit Operation: create INFO 2024-09-11 15:00:17.948294 cn-node-evtbroker SYSLOGTLS begining connection. Client: :: Server: 172.16.16.254:6514 INFO 2024-09-11 15:56:49.162859 cn-node-evtbroker Identity(chassis): ssh_set_newkeys: rekeying in for 172.16.16.254 port 35186, input30400 bytes 1787 blocks, output 103608 bytes 0 blocks INFO 2024-09-11 16:08:52.612313 cn-node-evtbroker Identity(chassis): Login success event alert for admin from Local:ttyPS0 INFO 2024-09-11 16:08:52.705768 cn-node-evtbroker SYSLOGTLS begining connection. Client: :: Server: 172.16.16.220:6514 INFO 2024-09-11 16:09:22.135824 cn-node-evtbroker TLS Client Session Module : evtbroker, Message Type : Start, Date : 2024-09-11, Time: 16:09:22.132998, Session Key : 169.254.160.9:57961_172.16.16.254:6514 , Source IP : 169.254.160.9:57961 , Destination IP: 172.16.16.254:6514 INFO 2024-09-11 16:09:22.204651 cn-node-evtbroker SYSLOGTLS X.509 certificate verified - /C=US/ST=MD/L=Catonsville/O=GSS/CN=tl45-16x.example.com Client: 169.254.160.9 Server: 172.16.16.254:6514 INFO 2024-09-11 16:09:22.727197 cn-node-evtbroker SYSLOGTLS connection established. Client: 169.254.160.9 Server: 172.16.16.254:6514 INFO 2024-09-11 16:09:22.825451 cn-node-evtbroker Identity(chassis): Incoming connection from 172.16.16.254 : 60082 INFO 2024-09-11 16:09:22.832420 cn-node-evtbroker Identity(chassis): User successfully logged in from IP 172.16.16.254 user name 'admin'
FCS_CKM.1	None	None	
FCS_CKM.2	None	None	
FCS_CKM.4	None	None	
FCS_COP.1/DataEncryption	None	None	
FCS_COP.1/Hash	None	None	
FCS_COP.1/KeyedHash	None	None	
FCS_COP.1/SigGen	None	None	

FCS_MACSEC_EXT.1	Session establishment.	Secure Channel Identifier (SCI)	CC-3926-905-MACSEC> log view events INFO 2024-06-07 17:48:14.996303 cn-node-evtbroker MACSEC Conn Assoc Status Change Event: CA: gss-connection local SCI: ac:89:d2:8c:6d:50:0001 peer SCI: 00:15:5d:00:7c:06:0001 status: Discovered INFO 2024-06-07 17:48:16.998808 cn-node-evtbroker SAK Update: CA: gss-connection, Timestamp: 2411653, Direction: 1 INFO 2024-06-07 17:48:16.999684 cn-node-evtbroker SAK Update: CA: gss-connection, Timestamp: 2411653, Direction: 0 INFO 2024-06-07 17:48:18.185406 cn-node-evtbroker Alarm_Manager(chassis): Alarm type:macsec-ca-peer-status qualifier: being CLEARED for resource:/cn-macsec:macsec-connection-association-status[connection-association-name=gss-connection] with severity:Major at time:2024-06-07T17:48:18.253597212Z
FCS_MACSEC_EXT.3	Creation and update of SAK.	Creation and update times	CC-3926-905-MACSEC> log view events INFO 2024-06-03 15:42:10.183283 cn-node-evtbroker SAK Update: CA: gss-connection, Timestamp: 2058487, Direction: 1 INFO 2024-06-03 15:42:10.293735 cn-node-evtbroker SAK Update: CA: gss-connection, Timestamp: 2058487, Direction: 0
FCS_MACSEC_EXT.1	Creation of Connectivity Association (CA).	Connectivity Association Key Names (CKNs)	CC-3926-905-MACSEC> log view events INFO 2024-06-03 18:41:18.400034 cn-node-evtbroker CA Update: CA: gss-connection, CKN: 1000
FCS_RBG_EXT.1	None	None	
FCS_SSHS_EXT.1	Failure to establish an SSH session.	Reason for failure	**No matching cipher (SSHS 1.4):** CC-3926-905-MACSEC> log view events INFO 2024-09-04 13:10:01.272960 cn-node-evtbroker Identity(chassis): Incoming connection from 172.16.16.254 : 54996 WARN 2024-09-04 13:10:02.322957 cn-node-evtbroker Identity(chassis): Unable to negotiate with 172.16.16.254 port 54996: no matching cipher found. Their offer: aes128-cbc CC-3926-905-MACSEC> log view security INFO 2024-09-04 13:14:06.449983 sshd Connection from 172.16.16.254 port 55098 on 169.254.160.10 port 22 rdomain "" INFO 2024-09-04 13:14:07.604515 sshd Unable to negotiate with 172.16.16.254 port 55098: no matching cipher found. Their offer: aes128-cbc [preauth] **No matching host key type (SSHS 1.5):** CC-3926-905-MACSEC> log view events INFO 2024-09-04 13:22:50.180997 cn-node-evtbroker Identity(chassis): Incoming connection from 172.16.16.254 : 55404 WARN 2024-09-04 13:22:51.161531 cn-node-evtbroker Identity(chassis): Unable to negotiate

			with 172.16.16.254 port 55404: no matching host key type found. Their offer: rsa-sha2-256 CC-3926-905-MACSEC> log view security INFO 2024-09-04 13:21:35.481232 sshd Connection from 172.16.16.254 port 55302 on 169.254.160.10 port 22 rdomain "" INFO 2024-09-04 13:21:36.354395 sshd Unable to negotiate with 172.16.16.254 port 55302: no matching host key type found. Their offer: rsa-sha2-256 [preauth] **No matching MAC (SSHS 1.6):** CC-3926-905-MACSEC> log view events INFO 2024-09-04 13:30:03.609962 cn-node-evtbroker Identity(chassis): Incoming connection from 172.16.16.254 : 55506 WARN 2024-09-04 13:30:04.751782 cn-node-evtbroker Identity(chassis): Unable to negotiate with 172.16.16.254 port 55506: no matching MAC found. Their offer: hmac-sha1-96 CC-3926-905-MACSEC> log view security INFO 2024-09-04 13:32:15.041243 sshd Connection from 172.16.16.254 port 55608 on 169.254.160.10 port 22 rdomain "" INFO 2024-09-04 13:32:16.008533 sshd Unable to negotiate with 172.16.16.254 port 55608: no matching MAC found. Their offer: hmac-sha1-96 [preauth] **No matching key exchange method (SSHS 1.7):** CC-3926-905-MACSEC> log view events INFO 2024-09-04 13:39:02.082767 cn-node-evtbroker Identity(chassis): Incoming connection from 172.16.16.254 : 56132 WARN 2024-09-04 13:39:03.048380 cn-node-evtbroker Identity(chassis): Unable to negotiate with 172.16.16.254 port 56132: no matching key exchange method found. Their offer: diffie-hellman-group18-sha512,ext-info-c CC-3926-905-MACSEC> log view security INFO 2024-09-04 13:41:35.634919 sshd Connection from 172.16.16.254 port 56234 on 169.254.160.10 port 22 rdomain "" INFO 2024-09-04 13:41:36.634106 sshd Unable to negotiate with 172.16.16.254 port 56234: no matching key exchange method found. Their offer: diffie-hellman-group18-sha512,ext-info-c [preauth] **Oversized packet (SSHS 1.3):** CC-3926-905-MACSEC> log view events INFO 2024-09-04 13:52:08.036002 cn-node-evtbroker Identity(chassis): Incoming connection from 172.16.16.254 : 56520 INFO 2024-09-04 13:52:09.291937 cn-node-evtbroker Identity(chassis): Login success event alert for admin from 172.16.16.254:56520

			INFO 2024-09-04 13:52:09.559586 cn-node-evtbroker Identity(chassis): User successfully logged in from IP 172.16.16.254 user name 'admin' INFO 2024-09-04 13:52:11.634018 cn-node-evtbroker Identity(chassis): Incoming connection from user admin 172.16.16.254 : 56520: message authenticat INFO 2024-09-04 13:52:11.755544 cn-node-evtbroker Identity(chassis): Logout logout event alert for admin from 172.16.16.254:56520 INFO 2024-09-04 13:52:11.852339 cn-node-evtbroker Identity(chassis) sshd Session '172.16.16.254:56520' for User 'admin' authentication-method Local logged out CC-3926-905-MACSEC> log view security INFO 2024-09-04 13:49:13.498087 sshd Connection from 172.16.16.254 port 56418 on 169.254.160.10 port 22 rdomain "" INFO 2024-09-04 13:49:14.447520 sshd rekey out after 32768000 blocks [preauth] INFO 2024-09-04 13:49:14.462830 sshd rekey in after 32768000 blocks [preauth] INFO 2024-09-04 13:49:14.546078 sshd pam_succeed_if(sshd:auth): requirement "tty =~ /dev/tty*" not met by user "admin" INFO 2024-09-04 13:49:15.011309 sshd Accepted password for admin from 172.16.16.254 port 56418 ssh2 INFO 2024-09-04 13:49:15.020613 sshd pam_unix(sshd:session): session opened for user admin by (uid=0) INFO 2024-09-04 13:49:15.023671 sshd User child is on pid 4830 INFO 2024-09-04 13:49:15.935769 sshd rekey in after 32768000 blocks INFO 2024-09-04 13:49:15.935927 sshd rekey out after 32768000 blocks INFO 2024-09-04 13:49:15.981437 sshd Starting session: shell on pts/4 for admin from 172.16.16.254 port 56418 id 0 INFO 2024-09-04 13:49:17.031696 sshd Bad packet length 262172. INFO 2024-09-04 13:49:17.032912 sshd ssh_dispatch_run_fatal: Connection from user admin 172.16.16.254 port 56418: message authentication code incorrect INFO 2024-09-04 13:49:17.036989 sshd pam_unix(sshd:session): session closed for user admin
FCS_TLSC_EXT.1	Failure to establish a TLS session.	Reason for failure	**No matching cipher (TLSC 1.1-t1):** Aug 1 19:58:08 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS begining connection. Client: :: Server: 172.16.16.254:6514

			Aug 1 19:58:08 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: TLS-6-TLSCONNECTION_EVENT: TLS Client Session Module : evtbroker, Message Type : Start, Date : 2024-08-01, Time: 19:58:08.836284, Session Key : 169.254.160.9:47935_172.16.16.254:6514 , Source IP : 169.254.160.9:47935 , Destination IP: 172.16.16.254:6514 Aug 1 19:58:08 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS Error: src: '169.254.160.9' dst: '172.16.16.254' Error: 'TLS error during handshake : sslv3 alert handshake failure Certificate: tl45-16x.example.com client-TOE-00-rsa' **Missing serverAuth EKU (TLSC 1.1-t2):** Aug 9 13:06:24 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: TLS-6-TLSCONNECTION_EVENT: TLS Client Session Module : evtbroker, Message Type : Start, Date : 2024-08-09, Time: 13:06:24.010018, Session Key : 169.254.160.9:35923_172.16.16.254:6514 , Source IP : 169.254.160.9:35923 , Destination IP: 172.16.16.254:6514 Aug 9 13:06:24 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS X.509 certificate verification fail - /C=US/ST=MD/L=Catonsville/O=GSS/CN=tl45-16x.example.com Client: 169.254.160.9 Server: 172.16.16.254:6514 Aug 9 13:06:24 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS Error: src: '169.254.160.9' dst: '172.16.16.254' Error: 'Certificate verification error : IP address mismatch Error #64 Certificate: tl45-16x.example.com client-TOE-00-rsa' Aug 9 13:06:24 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: TLS-6-TLSCONNECTION_EVENT: TLS Client Session Module : evtbroker, Message Type : Failed, Date : 2024-08-09, Time: 13:06:24.365334, Session Key : 169.254.160.9:35923_172.16.16.254:6514 , Reason : Certificate verification error : IP address mismatch Error #64 **Invalid Cert Type (TLSC 1.1-t3):** Jan 3 21:45:51 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-

			SYSLOG_TLS_EVENT: SYSLOGTLS begining connection. Client: :: Server: 172.16.16.254:6514 Jan 3 21:45:51 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: TLS-6-TLSCONNECTION_EVENT: TLS Client Session Module : evtbroker, Message Type : Start, Date : 2024-01-03, Time: 21:45:51.163287, Session Key : 169.254.160.9:34073_172.16.16.254:6514 , Source IP : 169.254.160.9:34073 , Destination IP: 172.16.16.254:6514 Jan 3 21:45:51 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS Error: src: '169.254.160.9' dst: '172.16.16.254' Error: 'TLS error during handshake : wrong certificate type Certificate: tl45-16x.example.com client-TOE-00-rsa' **NULL Ciphersuite (TLSC 1.1-t4a):** Aug 14 11:05:59 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS begining connection. Client: :: Server: 172.16.16.254:6514 Aug 14 11:05:59 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: TLS-6-TLSCONNECTION_EVENT: TLS Client Session Module : evtbroker, Message Type : Start, Date : 2024-08-14, Time: 11:05:59.006026, Session Key : 169.254.160.9:57157_172.16.16.254:6514 , Source IP : 169.254.160.9:57157 , Destination IP: 172.16.16.254:6514 Aug 14 11:05:59 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS Error: src: '169.254.160.9' dst: '172.16.16.254' Error: 'TLS error during handshake : unknown cipher returned Certificate: tl45-16x.example.com client-TOE-00-rsa' **No Proposed Cipher (TLSC 1.1-4b):** Aug 14 14:43:56 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS begining connection. Client: :: Server: 172.16.16.254:6514 Aug 14 14:43:56 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: TLS-6-TLSCONNECTION_EVENT: TLS Client Session Module : evtbroker, Message Type : Start, Date :

			2024-08-14, Time: 14:43:56.275714, Session Key : 169.254.160.9:42791_172.16.16.254:6514 , Source IP : 169.254.160.9:42791 , Destination IP: 172.16.16.254:6514 Aug 14 14:43:56 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS Error: src: '169.254.160.9' dst: '172.16.16.254' Error: 'TLS error during handshake : unknown cipher returned Certificate: tl45-16x.example.com client-TOE-00-rsa' **Invalid ECDHE Curve (TLSC 1.1-t4c):** Aug 15 20:41:50 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS begining connection. Client: :: Server: 172.16.16.254:6514 Aug 15 20:41:50 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: TLS-6-TLSCONNECTION_EVENT: TLS Client Session Module : evtbroker, Message Type : Start, Date : 2024-08-15, Time: 20:41:50.403724, Session Key : 169.254.160.9:60065_172.16.16.254:6514 , Source IP : 169.254.160.9:60065 , Destination IP: 172.16.16.254:6514 Aug 15 20:41:50 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS Error: src: '169.254.160.9' dst: '172.16.16.254' Error: 'TLS error during handshake : wrong curve Certificate: tl45-16x.example.com client-TOE-00-rsa' **Invalid TLS Version (TLSC 1.1-t5a):** Aug 14 11:07:29 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS begining connection. Client: :: Server: 172.16.16.254:6514 Aug 14 11:07:29 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: TLS-6-TLSCONNECTION_EVENT: TLS Client Session Module : evtbroker, Message Type : Start, Date : 2024-08-14, Time: 11:07:29.716880, Session Key : 169.254.160.9:54019_172.16.16.254:6514 , Source IP : 169.254.160.9:54019 , Destination IP: 172.16.16.254:6514 Aug 14 11:07:29 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS Error: src:

			'169.254.160.9' dst: '172.16.16.254' Error: 'TLS error during handshake : unsupported protocol Certificate: tl45-16x.example.com client-TOE-00-rsa' **Corrupt Server KeyEx Msg (TLSC 1.1-t5b):** Aug 15 14:06:00 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS begining connection. Client: :: Server: 172.16.16.254:6514 Aug 15 14:06:01 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: TLS-6-TLSCONNECTION_EVENT: TLS Client Session Module : evtbroker, Message Type : Start, Date : 2024-08-15, Time: 14:06:00.841204, Session Key : 169.254.160.9:48029_172.16.16.254:6514 , Source IP : 169.254.160.9:48029 , Destination IP: 172.16.16.254:6514 Aug 15 14:06:01 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS Error: src: '169.254.160.9' dst: '172.16.16.254' Error: 'TLS error during handshake : bad signature Certificate: tl45-16x.example.com client-TOE-00-rsa' **Modified Finished Message (TLSC 1.1-t6a):** Aug 14 11:08:38 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS begining connection. Client: :: Server: 172.16.16.254:6514 Aug 14 11:08:38 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: TLS-6-TLSCONNECTION_EVENT: TLS Client Session Module : evtbroker, Message Type : Start, Date : 2024-08-14, Time: 11:08:38.609116, Session Key : 169.254.160.9:52519_172.16.16.254:6514 , Source IP : 169.254.160.9:52519 , Destination IP: 172.16.16.254:6514 Aug 14 11:08:38 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS Error: src: '169.254.160.9' dst: '172.16.16.254' Error: 'TLS error during handshake : digest check failed Certificate: tl45-16x.example.com client-TOE-00-rsa' **Plaintext Finished Message (TLSC 1.1-t6b):** Aug 15 14:07:04 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76

			ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS begining connection. Client: :: Server: 172.16.16.254:6514 Aug 15 14:07:05 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: TLS-6-TLSCONNECTION_EVENT: TLS Client Session Module : evtbroker, Message Type : Start, Date : 2024-08-15, Time: 14:07:04.875158, Session Key : 169.254.160.9:58725_172.16.16.254:6514 , Source IP : 169.254.160.9:58725 , Destination IP: 172.16.16.254:6514 Aug 15 14:07:05 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS Error: src: '169.254.160.9' dst: '172.16.16.254' Error: 'TLS error during handshake : cipher operation failed Certificate: tl45-16x.example.com client-TOE-00-rsa' **Server Hello Nonce Modified (TLSC 1.1-t6c):** Aug 14 11:09:46 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS begining connection. Client: :: Server: 172.16.16.254:6514 Aug 14 11:09:46 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: TLS-6-TLSCONNECTION_EVENT: TLS Client Session Module : evtbroker, Message Type : Start, Date : 2024-08-14, Time: 11:09:46.497052, Session Key : 169.254.160.9:58231_172.16.16.254:6514 , Source IP : 169.254.160.9:58231 , Destination IP: 172.16.16.254:6514 Aug 14 11:09:46 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS Error: src: '169.254.160.9' dst: '172.16.16.254' Error: 'TLS error during handshake : sslv3 alert bad record mac Certificate: tl45-16x.example.com client-TOE-00-rsa' **No matching CN (TLSC 1.2):** Jan 4 19:48:58 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: TLS-6-TLSCONNECTION_EVENT: TLS Client Session Module : evtbroker, Message Type : Start, Date : 2024-01-04, Time: 19:48:58.951561, Session Key : 169.254.160.9:57029_172.16.16.254:6514 , Source IP : 169.254.160.9:57029 , Destination IP: 172.16.16.254:6514

			Jan 4 19:48:58 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: TLS-6-TLSCONNECTION_EVENT: TLS Client Session Module : evtbroker, Message Type : Failed, Date : 2024-01-04, Time: 19:48:58.974355, Session Key : 169.254.160.9:57029_172.16.16.254:6514 , Reason : Certificate verification error : hostname mismatch Error #62
FIA_AFL.1	Unsuccessful login attempt limit is met or exceeded.	Origin of the attempt (e.g., IP address)	CC-3926-905-MACSEC> log view events INFO 2024-01-12 13:59:56.966378 cn-node-evtbroker Identity(chassis): Login failure event alert for user from 172.16.16.254:44936 WARN 2024-01-12 13:59:58.545445 cn-node-evtbroker Identity(chassis): Authentication failure for user 'user' from IP 172.16.16.254 INFO 2024-01-12 14:00:08.926013 cn-node-evtbroker Maximum authentication retry reached for user user as per lockout policy.
FIA_PMG_EXT.1	None	None	
FIA_UAU.7	None	None	
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address)	Refer to audits for FIA_UIA_EXT.1 for all audits related to the use of the identification and authentication mechanism.
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address)	**Successful Console Login:** CC-3926-905-MACSEC> log view events INFO 2024-02-13 06:31:06.133774 cn-node-evtbroker Identity(chassis): Login success event alert for admin from Local:ttyPS0 CC-3926-905-MACSEC> log view security INFO 2024-02-13 06:31:03.581016 login pam_succeed_if(login:auth): requirement "tty =~ /dev/tty*" was met by user "admin" INFO 2024-02-13 06:31:06.149553 login pam_unix(login:session): session opened for user admin by admin(uid=0) **Failed Console Login:** CC-3926-905-MACSEC> log view events INFO 2024-02-13 06:30:51.550053 cn-node-evtbroker Identity(chassis): Login failure event alert for admin from Local:ttyPS0 CC-3926-905-MACSEC> log view security INFO 2024-02-13 06:30:40.284188 login pam_unix(login:session): session closed for user admin INFO 2024-02-13 06:30:49.520240 login pam_succeed_if(login:auth): requirement "tty =~ /dev/tty*" was met by user "admin" NOTIF 2024-02-13 06:30:51.429989 login pam_unix(login:auth): authentication failure; logname=admin uid=0 euid=0 tty=/dev/ttyPS0 ruser= rhost= user=admin NOTIF 2024-02-13 06:30:53.731026 login FAILED LOGIN (1) on '/dev/ttyPS0' FOR 'admin', Authentication failure

			Successful SSH Login: CC-3926-905-MACSEC> log view events INFO 2024-09-06 18:40:35.571096 cn-node-evtbroker Identity(chassis): Incoming connection from 172.16.16.254 : 58214 INFO 2024-09-06 18:38:35.943043 cn-node-evtbroker Identity(chassis): Login success event alert for admin from 172.16.16.254:58212 INFO 2024-09-06 18:38:36.064628 cn-node-evtbroker Identity(chassis): User successfully logged in from IP 172.16.16.254 user name 'admin' **Failed SSH Login:** CC-3926-905-MACSEC> log view events INFO 2024-09-06 17:40:16.534410 cn-node-evtbroker Identity(chassis): Login failure event alert for admin from 172.16.16.254:58200 WARN 2024-09-06 17:40:18.226204 cn-node-evtbroker Identity(chassis): Authentication failure for user 'admin' from IP 172.16.16.254 INFO 2024-09-06 17:40:22.214215 cn-node-evtbroker Identity(chassis): Login failure event alert for admin from 172.16.16.254:58200 WARN 2024-09-06 17:40:24.064465 cn-node-evtbroker Identity(chassis): Authentication failure for user 'admin' from IP 172.16.16.254
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate.	Reason for failure of certificate validation	**Missing Basic Constraints:** Sep 10 18:21:02 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: TLS-6-TLSCONNECTION_EVENT: TLS Client Session Module : evtbroker, Message Type : Start, Date : 2024-09-10, Time: 18:21:02.773896, Session Key : 169.254.160.9:57373_172.16.16.254:6514 , Source IP : 169.254.160.9:57373 , Destination IP: 172.16.16.254:6514 Sep 10 18:21:02 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS Error: src: '169.254.160.9' dst: '172.16.16.254' Error: 'Certificate verification error : A CA certificate is invalid. Either it is not a CA or its extensions are not consistent with the supplied purpose. Error #79 Certificate: tl45-16x.example. **Basic Constraints False for CA:** Sep 10 18:24:03 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: TLS-6-TLSCONNECTION_EVENT: TLS Client Session Module : evtbroker, Message Type : Start, Date : 2024-09-10, Time: 18:24:03.084141, Session Key : 169.254.160.9:55341_172.16.16.254:6514 , Source IP : 169.254.160.9:55341 , Destination IP: 172.16.16.254:6514

			Sep 10 18:24:03 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS Error: src: '169.254.160.9' dst: '172.16.16.254' Error: 'Certificate verification error : A CA certificate is invalid. Either it is not a CA or its extensions are not consistent with the supplied purpose. Error #79 Certificate: tl45-16x.example. **Certificate Revoked:** Jan 10 17:43:03 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS Error: src: '169.254.160.9' dst: '172.16.16.254' Error: 'Certificate verification error : Certificate Revoked Error #501 Certificate: tl45-16x.example.com client-TOE-00-rsa' Jan 10 17:45:02 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS Error: src: '169.254.160.9' dst: '172.16.16.254' Error: 'Certificate verification error : OCSP Response Failed Verification : root ca not trusted Error #501 Certificate: tl45-16x.example.com client-TOE-00-rsa' **Corrupt Certificate ASN1:** Aug 5 14:34:47 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS begining connection. Client: :: Server: 172.16.16.254:6514 Aug 5 14:34:47 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: TLS-6-TLSCONNECTION_EVENT: TLS Client Session Module : evtbroker, Message Type : Start, Date : 2024-08-05, Time: 14:34:47.854242, Session Key : 169.254.160.9:33205_172.16.16.254:6514 , Source IP : 169.254.160.9:33205 , Destination IP: 172.16.16.254:6514 Aug 5 14:34:47 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS Error: src: '169.254.160.9' dst: '172.16.16.254' Error: 'TLS error during handshake : wrong tag Certificate: tl45-16x.example.com client-TOE-00-rsa' **Corrupt Certificate Signature:** Sep 10 18:08:18 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: TLS-6-TLSCONNECTION_EVENT: TLS Client Session

			Module : evtbroker, Message Type : Start, Date : 2024-09-10, Time: 18:08:17.911202, Session Key : 169.254.160.9:43271_172.16.16.254:6514 , Source IP : 169.254.160.9:43271 , Destination IP: 172.16.16.254:6514 Sep 10 18:08:18 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS X.509 certificate verification fail - /C=US/ST=MD/L=Catonsville/O=GSS/CN=tl45-16x.example.com Client: 169.254.160.9 Server: 172.16.16.254:6514 Sep 10 18:08:18 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS Error: src: '169.254.160.9' dst: '172.16.16.254' Error: 'TLS error during handshake : invalid padding Certificate: tl45-16x.example.com client-TOE-00-rsa' **Corrupt Public Key:** Jan 4 01:43:17 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS begining connection. Client: :: Server: 172.16.16.254:6514 Jan 4 01:43:17 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: TLS-6-TLSCONNECTION_EVENT: TLS Client Session Module : evtbroker, Message Type : Start, Date : 2024-01-04, Time: 01:43:17.379784, Session Key : 169.254.160.9:36233_172.16.16.254:6514 , Source IP : 169.254.160.9:36233 , Destination IP: 172.16.16.254:6514 Jan 4 01:43:17 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS X.509 certificate verification fail - /C=US/ST=MD/L=Catonsville/O=GSS/CN=tl45-16x.example.com Client: 169.254.160.9 Server: 172.16.16.254:6514 Jan 4 01:43:17 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS Error: src: '169.254.160.9' dst: '172.16.16.254' Error: 'TLS error during handshake : bad signature Certificate: tl45-16x.example.com client-TOE-00-rsa' **Invalid Chain:** Jan 4 20:15:52 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76

			ac:89:d2:8c:6d:40: TLS-6-TLSCONNECTION_EVENT: TLS Client Session Module : evtbroker, Message Type : Start, Date : 2024-01-04, Time: 20:15:51.949913, Session Key : 169.254.160.9:51701_172.16.16.254:6514 , Source IP : 169.254.160.9:51701 , Destination IP: 172.16.16.254:6514 Jan 4 20:15:52 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: TLS-6-TLSCONNECTION_EVENT: TLS Client Session Module : evtbroker, Message Type : Failed, Date : 2024-01-04, Time: 20:15:51.970318, Session Key : 169.254.160.9:51701_172.16.16.254:6514 , Reason : Certificate verification error : The certificate chain could be built up using the untrusted certificates but the root could not be found locally. Error #19 **No OCSP Sign:** Aug 5 14:30:14 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS begining connection. Client: :: Server: 172.16.16.254:6514 Aug 5 14:30:14 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: TLS-6-TLSCONNECTION_EVENT: TLS Client Session Module : evtbroker, Message Type : Start, Date : 2024-08-05, Time: 14:30:14.002302, Session Key : 169.254.160.9:51389_172.16.16.254:6514 , Source IP : 169.254.160.9:51389 , Destination IP: 172.16.16.254:6514 Aug 5 14:30:14 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: TLS-6-TLSCONNECTION_EVENT: TLS Client Session Module : evtbroker, Message Type : Failed, Date : 2024-08-05, Time: 14:30:14.156396, Session Key : 172.16.16.254:6514_169.254.160.9:51389 , Reason : OCSP Response Failed Verification Aug 5 14:30:14 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS Error: src: '169.254.160.9' dst: '172.16.16.254' Error: 'Certificate verification error : OCSP Response Failed Verification : root ca not trusted Error #501 Certificate: tl45-16x.example.com client-TOE-00-rsa' **Unreachable Revocation Server:** Sep 10 17:04:28 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: TLS-6-TLSCONNECTION_EVENT: TLS Client Session

			Module : evtbroker, Message Type : Start, Date : 2024-09-10, Time: 17:04:27.785016, Session Key : 169.254.160.9:60317_172.16.16.254:6514 , Source IP : 169.254.160.9:60317 , Destination IP: 172.16.16.254:6514 Sep 10 17:04:28 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: TLS-6-TLSCONNECTION_EVENT: TLS Client Session Module : evtbroker, Message Type : Failed, Date : 2024-09-10, Time: 17:04:27.884826, Session Key : 172.16.16.254:6514_169.254.160.9:60317 , Reason : OCSP Responder Unreachable Sep 10 17:04:28 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS Error: src: '169.254.160.9' dst: '172.16.16.254' Error: 'Certificate verification error : OCSP Responder Unreachable Error #501 Certificate: client-TOE-00-rsa' Sep 10 17:04:28 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: TLS-6-TLSCONNECTION_EVENT: TLS Client Session Module : evtbroker, Message Type : Failed, Date : 2024-09-10, Time: 17:04:27.886388, Session Key : 169.254.160.9:60317_172.16.16.254:6514 , Reason : Certificate verification error : OCSP Responder Unreachable Error #501 **Certificate Expired:** Jan 4 01:40:41 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: IDENTITY-6-SYSLOG_TLS_EVENT: SYSLOGTLS Error: src: '169.254.160.9' dst: '172.16.16.254' Error: 'Certificate verification error : The certificate has expired: that is the notAfter date is before the current time. Error #10 Certificate: tl45-16x.example.com client-TOE-00-rsa'
	Any addition, replacement, or removal of trust anchors in the TOE's trust store.	Identification of certificates added, replaced, or removed as trust anchor in the TOE's trust store	**Addition/Replacement:** CC-3926-905-MACSEC> log view events INFO 2024-01-04 21:14:30.691890 cn-node-evtbroker User 'admin' successfully installed X.509 CA certificate with name subca-rsa. Result: success **Removal:** CC-3926-905-MACSEC> log view events INFO 2024-01-10 16:46:29.145312 cn-node-evtbroker User 'admin' successfully uninstalled X.509 CA certificate with name subca-rsa. Result: success
FIA_X509_EXT.2	None	None	
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update.	None	CC-3926-905-MACSEC> log view troubleshoot INFO 2024-09-03 17:46:46.300356 xgrade-ng Operation requested: {'operation': 'install',

			'options': {'manifest_url': 'http://172.16.16.254/saos-10-09-01-0220-packages/saos-10-09-01-0220.yml', 'defer_activation': False, 'manifest_hash_algorithm': 'sha-256'}} INFO 2024-09-03 18:02:40.804259 xgrade-ng finished operation: {'operation': 'install', 'options': {'manifest_url': 'http://172.16.16.254/saos-10-09-01-0220-packages/saos-10-09-01-0220.yml', 'defer_activation': False, 'manifest_hash_algorithm': 'sha-256', 'RTSC_required': None}, 'package_name': 'saos-10-09-01-0220', 'retries': 0, 'operation_timeout': 1555, 'latest_log': 'installing /mnt/config/image/evernight-generic-arm-aarch64-01-09-01-0220-upgrade.sh on standby bank'}
FMT_MOF.1/CoreData	None	None	
FMT_MOF.1/CryptoKeys	None	None	
FMT_SMF.1	All management activities of TSF data.	Ability to administer the TOE locally and remotely	**Failed login attempt via Local Console:** CC-3926-905-MACSEC> log view events INFO 2024-02-13 06:30:51.550053 cn-node-evtbroker Identity(chassis): Login failure event alert for admin from Local:ttyPS0 CC-3926-905-MACSEC> log view security INFO 2024-02-13 06:30:40.284188 login pam_unix(login:session): session closed for user admin INFO 2024-02-13 06:30:49.520240 login pam_succeed_if(login:auth): requirement "tty =~ /dev/tty*" was met by user "admin" NOTIF 2024-02-13 06:30:51.429989 login pam_unix(login:auth): authentication failure; logname=admin uid=0 euid=0 tty=/dev/ttyPS0 ruser= rhost= user=admin NOTIF 2024-02-13 06:30:53.731026 login FAILED LOGIN (1) on '/dev/ttyPS0' FOR 'admin', Authentication failure **Successful login attempt via Local Console:** CC-3926-905-MACSEC> log view events INFO 2024-09-06 18:40:35.571096 cn-node-evtbroker Identity(chassis): Incoming connection from 172.16.16.254 : 58214 INFO 2024-09-06 18:38:35.943043 cn-node-evtbroker Identity(chassis): Login success event alert for admin from 172.16.16.254:58212 INFO 2024-09-06 18:38:36.064628 cn-node-evtbroker Identity(chassis): User successfully logged in from IP 172.16.16.254 user name 'admin' **Failed login attempt via SSH:** CC-3926-905-MACSEC> log view security INFO 2024-09-06 17:40:16.403255 sshd pam_succeed_if(sshd:auth): requirement "tty =~ /dev/tty*" not met by user "admin"

			NOTIF 2024-09-06 17:40:16.429898 sshd pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh:58200 ruser= rhost=172.16.16.254 user=admin INFO 2024-09-06 17:40:18.217740 sshd Failed password for admin from 172.16.16.254 port 58200 ssh2 INFO 2024-09-06 17:40:22.094088 sshd pam_succeed_if(sshd:auth): requirement "tty =~ /dev/tty*" not met by user "admin" INFO 2024-09-06 17:40:24.058417 sshd Failed password for admin from 172.16.16.254 port 58200 ssh2 **Successful login attempt via SSH:** CC-3926-905-MACSEC> log view security INFO 2024-09-06 18:40:39.153751 sshd pam_succeed_if(sshd:auth): requirement "tty =~ /dev/tty*" not met by user "admin" INFO 2024-09-06 18:40:39.457448 sshd Accepted password for admin from 172.16.16.254 port 58214 ssh2 INFO 2024-09-06 18:40:39.467686 sshd pam_unix(sshd:session): session opened for user admin by (uid=0)
		Ability to configure the access banner	CC-3926-905-MACSEC> log view events NOTIF 2024-02-13 14:59:30.264195 cn-node-evtbroker Netconf(chassis): Session ID: 560; Username: admin; Client IP: 172.16.16.254; Target XPath: /oc-sys:system/oc-sys:config/oc-sys:motd-banner; Edit Operation: create
		Ability to configure the session inactivity time before session termination or locking	**Local Console:** CC-3926-905-MACSEC> log view events NOTIF 2024-09-06 19:06:12.237195 cn-node-evtbroker Netconf(chassis): Session ID: 262; Username: admin; Client IP: 127.0.0.1; Target XPath: /oc-sys:system/oc-sys:ssh-server/oc-sys:config/oc-sys:timeout; Edit Operation: create **SSH:** CC-3926-905-MACSEC> log view events NOTIF 2024-02-09 18:58:22.838097 cn-node-evtbroker Netconf(chassis): Session ID: 482; Username: admin; Client IP: 172.16.16.254; Target XPath: /oc-sys:system/oc-sys:ssh-server/oc-sys:config/oc-sys:timeout; Edit Operation: create
		Ability to update the TOE, and to verify the updates using [hash comparison] capability prior to installing those updates	**Verify the updates using [hash comparison] capability prior to installing those updates:** Not applicable as the hash validation of the image is performed off box by an administrator. **Ability to update the TOE:** CC-3926-905-MACSEC> log view troubleshoot INFO 2024-09-03 17:46:46.300356 xgrade-ng Operation requested: {'operation': 'install', 'options': {'manifest_url':

			'http://172.16.16.254/saos-10-09-01-0220-packages/saos-10-09-01-0220.yml', 'defer_activation': False, 'manifest_hash_algorithm': 'sha-256'}} INFO 2024-09-03 18:02:40.804259 xgrade-ng finished operation: {'operation': 'install', 'options': {'manifest_url': 'http://172.16.16.254/saos-10-09-01-0220-packages/saos-10-09-01-0220.yml', 'defer_activation': False, 'manifest_hash_algorithm': 'sha-256', 'RTSC_required': None}, 'package_name': 'saos-10-09-01-0220', 'retries': 0, 'operation_timeout': 1555, 'latest_log': 'installing /mnt/config/image/evernight-generic-arm-aarch64-01-09-01-0220-upgrade.sh on standby bank'}
		Ability to configure the authentication failure parameters for FIA_AFL.1	CC-3926-905-MACSEC> log view events NOTIF 2024-09-06 19:14:53.179119 cn-node-evtbroker Netconf(chassis): Session ID: 267; Username: admin; Client IP: 172.16.16.254; Target XPath: /oc-sys:system/oc-sys:aaa/oc-sys:authentication/ciena-oc-aaa:lockout-policy; Edit Operation: create
		Ability to modify the behavior of the transmission of audit data to an external IT entity	CC-3926-905-MACSEC> log view events NOTIF 2024-02-13 07:18:11.911679 cn-node-evtbroker Netconf(chassis): Session ID: 497; Username: admin; Client IP: 172.16.16.254; Target XPath: /syslog:syslog/syslog:log-actions/ciena-syslog-tls:remote-syslog-tls/ciena-syslog-tls:admin-state; Edit Operation: merge
		Ability to manage the cryptographic keys	**Install:** CC-3926-905-MACSEC> log view events INFO 2024-09-04 19:32:06.928077 cn-node-evtbroker Identity(chassis): User Pubkey admin.pub is successfully installed by admin from 172.16.16.254 CC-3926-905-MACSEC> log view security EMERG 2024-09-04 19:32:06.922240 netconfd-pro User Pubkey admin.pub is successfully installed by admin from 172.16.16.254 **Edit:** CC-3926-905-MACSEC> log view events INFO 2024-09-04 19:38:05.087221 cn-node-evtbroker Identity(chassis): User Pubkey admin.pub is successfully changed by admin from 172.16.16.254 CC-3926-905-MACSEC> log view security EMERG 2024-09-04 19:38:05.076692 netconfd-pro User Pubkey admin.pub is successfully changed by admin from 172.16.16.254 **Remove:** CC-3926-905-MACSEC> log view events INFO 2024-09-04 19:13:51.459781 cn-node-evtbroker Identity(chassis): User Pubkey

			admin.pub is successfully deleted by admin from 172.16.16.254 CC-3926-905-MACSEC> log view security EMERG 2024-09-04 19:13:51.449548 netconfd-pro User Pubkey admin.pub is successfully deleted by admin from 172.16.16.254
		Ability to configure thresholds for SSH rekeying	CC-3926-905-MACSEC> log view events NOTIF 2024-09-06 19:34:32.521196 cn-node-evtbroker Netconf(chassis): Session ID: 268; Username: admin; Client IP: 172.16.16.254; Target XPath: /oc-sys:system/oc-sys:ssh-server/oc-sys:config/ciena-oc-sys:rekey-time; Edit Operation: create
		Ability to set the time which is used for time stamps	CC-3926-905-MACSEC> log view events INFO 2024-02-13 08:30:56.191128 cn-node-evtbroker Identity(chassis): Login success event alert for admin from Local:ttyPS0 INFO 2024-02-13 07:30:00.024093 cn-node-evtbroker System(chassis): Clock change alert; configured-value: 2024-02-13T07:30:00Z
		Ability to manage the TOE's trust store and designate X.509v3 certificates as trust anchors	CC-3926-905-MACSEC> log view events INFO 2024-01-08 20:02:26.691890 cn-node-evtbroker User 'admin' successfully installed X.509 CA certificate with name subca-rsa. Result: success INFO 2024-01-12 21:25:04.145312 cn-node-evtbroker User 'admin' successfully uninstalled X.509 CA certificate with name subca-rsa. Result: success
		Ability to manage the trusted public keys database	CC-3926-905-MACSEC> log view events INFO 2024-01-08 20:02:26.691890 cn-node-evtbroker User 'admin' successfully installed X.509 CA certificate with name subca-rsa. Result: success INFO 2024-01-12 21:25:04.145312 cn-node-evtbroker User 'admin' successfully uninstalled X.509 CA certificate with name subca-rsa. Result: success
FMT_SMR.2	None	None	
FPT_APW_EXT.1	None	None	
FPT_RPL.1	Detected replay attempt.	None	May 28 16:10:47 CC-3926-905-MACSEC cn-node-evtbroker[cn-evt-broker] 172.16.16.76 ac:89:d2:8c:6d:40: MACSEC-6-MKA_REPLAY_DETECTED: MKA Replay Detected for CA: gss-connection, Timestamp: 1541805
FPT_SKP_EXT.1	None	None	
FPT_STM_EXT.1	Discontinuous changes to time.	The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address)	**Discontinuous changes to time – Administrator actuated:** CC-3926-905-MACSEC> log view events INFO 2024-08-14 12:20:44.781874 cn-node-evtbroker Identity(chassis): Incoming connection from 172.16.16.254 : 44058 INFO 2024-08-14 12:20:44.941627 cn-node-evtbroker Identity(chassis): Login success event alert for admin from 172.16.16.254:44058 INFO 2024-08-14 12:21:14.290813 cn-node-evtbroker Identity(chassis): User successfully

			logged in from IP 172.16.16.254 user name 'admin' INFO 2024-08-14 12:21:14.297656 cn-node-evtbroker System(chassis): Clock change alert; configured-value: 2024-08-14T12:25:30Z
FPT_TST_EXT.1	None	None	
FPT_TUD_EXT.1	Initiation of update, result of the update attempt (success or failure).	None	**Success:** CC-3926-905-MACSEC> log view troubleshoot INFO 2024-09-03 17:46:46.300356 xgrade-ng Operation requested: {'operation': 'install', 'options': {'manifest_url': 'http://172.16.16.254/saos-10-09-01-0220-packages/saos-10-09-01-0220.yml', 'defer_activation': False, 'manifest_hash_algorithm': 'sha-256'}} INFO 2024-09-03 18:02:40.804259 xgrade-ng finished operation: {'operation': 'install', 'options': {'manifest_url': 'http://172.16.16.254/saos-10-09-01-0220-packages/saos-10-09-01-0220.yml', 'defer_activation': False, 'manifest_hash_algorithm': 'sha-256', 'RTSC_required': None}, 'package_name': 'saos-10-09-01-0220', 'retries': 0, 'operation_timeout': 1555, 'latest_log': 'installing /mnt/config/image/evernight-generic-arm-aarch64-01-09-01-0220-upgrade.sh on standby bank'} **Failure:** Not applicable as the hash validation of the image is performed off box by an administrator.
FPT_TUD_EXT.2	Failure of update.	Reason for failure (including identifier of invalid certificate)	Refer to audits for FTP_TUD_EXT.1.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None	**Termination of SSH session:** NFV-FRU> log view events INFO 2024-01-08 16:24:12.789039 cn-node-evtbroker Identity(chassis): Login success event alert for admin from 172.16.16.254:35374 INFO 2024-01-08 16:24:12.815717 cn-node-evtbroker Identity(chassis): Incoming connection from 172.16.16.254 : 35374 INFO 2024-01-08 16:24:12.818503 cn-node-evtbroker Identity(chassis): User successfully logged in from IP 172.16.16.254 user name 'admin' INFO 2024-01-08 16:27:50.704834 cn-node-evtbroker Identity(chassis) sshd Session '172.16.16.254:35374' for User 'admin' authentication-method Local logged out due to inactvity
FTA_SSL.4	The termination of an interactive session.	None	**Local Console:** CC-3926-905-MACSEC> log view events

			INFO 2024-02-13 07:30:10.583569 cn-node-evtbroker Identity(chassis) login Session 'Local:ttyPS0' for User 'admin' authentication-method Local logged out CC-3926-905-MACSEC> log view security INFO 2024-02-13 07:30:10.448056 login pam_unix(login:session): session closed for user admin **Remote Session (SSH):** CC-3926-905-MACSEC> log view events INFO 2024-09-04 18:10:46.700070 cn-node-evtbroker Identity(chassis): User logged out from IP 172.16.16.254 user name 'admin' INFO 2024-09-04 18:10:46.936554 cn-node-evtbroker Identity(chassis) sshd Session '172.16.16.254:58138' for User 'admin' authentication-method Local logged out
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	None	CC-3926-905-MACSEC> log view events INFO 2024-01-08 16:23:50.706112 cn-node-evtbroker Identity(chassis) sshd Session 'Local:ttyPS0' for User 'admin' authentication-method Local logged out due to inactvity
FTA_TAB.1	None	None	
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the indicator and target of failed trusted channels establishment attempt	**Initiation of the trusted channel:** CC-3926-905-MACSEC> log view events INFO 2024-01-05 19:30:46.882138 cn-node-evtbroker TLS Client Session Module : evtbroker, Message Type : Ended, Date : 2024-01-05, Time: 19:30:46.875368, Session Key : 169.254.160.9:44439_172.16.16.254:6514 , Reason : Normal INFO 2024-01-05 19:30:46.885113 cn-node-evtbroker SYSLOGTLS X.509 certificate verified - /C=US/ST=MD/L=Catonsville/O=GSS/CN=tl45-16x.example.com Client: 169.254.160.9 Server: 172.16.16.254:6514 INFO 2024-01-05 19:30:46.886177 cn-node-evtbroker SYSLOGTLS connection established. Client: 169.254.160.9 Server: 172.16.16.254:6514 **Termination of the trusted channel:** CC-3926-905-MACSEC> log view events INFO 2024-01-05 19:30:46.898523 cn-node-evtbroker SYSLOGTLS connection closed normally. Client: 169.254.160.9 Server: 172.16.16.254:6514 **Failure of the trusted channel functions:** CC-3926-905-MACSEC> log view events INFO 2024-01-05 19:30:16.882447 cn-node-evtbroker SYSLOGTLS connection closed unexpectedly. Client: 169.254.160.9 Server: 172.16.16.254:6514
FTP_TRP.1/Admin	Initiation of the trusted path.	None	**Initiation of the trusted path:** CC-3926-905-MACSEC> log view events

	Termination of the trusted path. Failure of the trusted path functions.		INFO 2024-09-06 17:16:49.908270 cn-node-evtbroker Identity(chassis): Incoming connection from 172.16.16.254 : 57018 INFO 2024-09-06 17:17:04.342280 cn-node-evtbroker Identity(chassis): Login success event alert for admin from 172.16.16.254:57018 INFO 2024-09-06 17:17:04.471539 cn-node-evtbroker Identity(chassis): User successfully logged in from IP 172.16.16.254 user name 'admin' **Termination of the trusted path:** CC-3926-905-MACSEC> log view events INFO 2024-09-09 16:12:57.259240 cn-node-evtbroker Identity(chassis): User logged out from IP 172.16.16.254 user name 'admin' INFO 2024-09-09 16:12:57.296188 cn-node-evtbroker Identity(chassis) sshd Session '172.16.16.254:57104' for User 'admin' authentication-method Local logged out **Failure of the trusted path functions:** CC-3926-905-MACSEC> log view events INFO 2024-09-06 17:16:54.333933 cn-node-evtbroker Identity(chassis): Login failure event alert for admin from 172.16.16.254:57018 WARN 2024-09-06 17:16:56.205042 cn-node-evtbroker Identity(chassis): Authentication failure for user 'admin' from IP 172.16.16.254

14 Network Services and Protocols

The following table lists the network services/protocols available on the TOE as a client (initiated outbound) and/or server (listening for inbound connections), all of which run as system-level processes. The table indicates whether each service or protocol is allowed to be used in the certified configuration.

For more detail about each service, including whether the service is limited by firewall mode (routed or transparent), or by context (single, multiple, system), refer to the ***Command Reference*** guides listed above in this document.

Table 44: Protocols and Services

Service or Protocol	Description	Client (initiating)	Allowed	Server (terminating)	Allowed	Allowed use in the certified configuration
DHCP	Dynamic Host Configuration Protocol	Yes	Yes	Yes	Yes	Out of scope of the evaluation
DNS	Domain Name Service	Yes	Yes	No	Yes	Out of scope of the evaluation
FTP	File Transfer Protocol	Yes	Yes	No	No	Out of scope of the evaluation
HTTP	Hypertext Transfer Protocol	Yes	Yes	Yes	No	Out of scope of the evaluation
HTTPS	Hypertext Transfer Protocol Secure	Yes	No	Yes	No	Out of scope of the evaluation
ICMP	Internet Control Message Protocol	Yes	No	Yes	No	Out of scope of the evaluation
IKE	Internet Key Exchange	Yes	No	Yes	No	Out of scope of the evaluation
Kerberos	A ticket-based authentication protocol	Yes	No	No	No	Out of scope of the evaluation
LDAP	Lightweight Directory Access Protocol	Yes	No	No	n/a	Out of scope of the evaluation
LDAP-over-SSL	LDAP over Secure Sockets Layer	Yes	No	No	No	Out of scope of the evaluation
RADIUS	Remote Authentication Dial 1n User Service	Yes	No	No	No	Out of scope of the evaluation

SNMP	Simple Network Management Protocol	Yes (snmp-trap)	No	Yes	No	Out of scope of the evaluation
SSH	Secure Shell	Yes	Yes	Yes	Yes	As described on the relevant section of this document.
SSL	Secure Sockets Layer	Yes	No	Yes	No	Use SSH instead.
TACACS+	Terminal Access Controller Access-Control System Plus	Yes	No	No	No	Out of scope of the evaluation
Telnet	A protocol used for terminal emulation	Yes	No	Yes	No	Use SSH instead.
TLS	Transport Layer Security	Yes	No	Yes	No	Out of scope of the evaluation
TFTP	Trivial File Transfer Protocol	Yes	No	No	No	Out of scope of the evaluation

15 Modes of Operation

The TOE uses X.509 certificates for communication with the syslog server. The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication of external TLS peers. There are two categories of X.509 certificates:

Access to the system can be established by means of:

- Console port. The console port is used to access the system by means of a laptop PC. The serial console port is a Serial EIA-561 (RJ-45) or USBC port. The console allows for local CLI access to the system.
- Secure Shell (SSH). SSH provides remote login for remote CLI access to the system and SFTP file transfers. SSH verifies and grants access to login requests by encrypting user ID and passwords or through public key encryption. SSH/SFTP is supported over IPv4 and IPv6.

Understanding the user interface

Configure the system and view the configuration by means of the user interface.

You can access the user interface by means of:

- Command Line Interface (CLI)
- **Software installation and upgrade**

By default, SAOS software is installed by means of Ciena's Zero Touch Provisioning (ZTP)which was not evaluated. ZTP enables rapid deployment of new systems to the network through automatic configuration. It also automates the process of upgrading software images.

For additional security, Ciena also offers:

- Secure ZTP (SZTP), which adds the ability to deploy software securely in various environments, for example, including scenarios where DHCP cannot be relied on to provide the location of the command file. SZTP provides secure provisioning by means of HTTPS or a pre-configured list of command file URLs.
- RFC-based SZTP, which follows the implementation and processes outlined in Internet Engineering Task Force (IETF) RFC-8572, Secure Zero Touch Provisioning.

Obtain licenses

Systems are licensed from the Ciena Support Portal. Systems require a base operating system (OS) license. Network operators choose additional optional OS applications. When the network operator places an order, Ciena generates licenses and makes them available on the Ciena Support Portal, and sends the activation codes by means of email.

Licenses are processed locally or by using an external license server:

- When local license processing is used, a license file must be uploaded to the system. A license file is generated using the registration ID of the system.
- When an external license server is used, one license file that contains multiple entitlements can be loaded on the license server. The license server provides these entitlements to many different license service components. One license file can be generated to license many different instances which simplifies the administration of licenses for each system.

The software license service is always started as part of the software initialization. At startup, there are no pre-installed licenses.

16 Obtaining Documentation

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Ciena Product Documentation* which also lists all new and revised Ciena technical documentation at:

Detailed information about the Ciena products:

https://www.ciena.com/products

You can access the most current Ciena documentation on the World Wide Web at:

https://www.ciena.com

16.1 Document Feedback

Ciena is committed to ensuring digital accessibility for people with disabilities. Ciena is continually improving the user experience for everyone and applying the relevant accessibility standards. Please let us know if you encounter accessibility barriers on Ciena websites by contacting webchanges@ciena.com and we will get back to you in 2-5 business days.

16.2 Obtaining Technical Assistance

Ciena provides ciena.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Ciena.com registered users, additional troubleshooting tools are available from the Support website.

Ciena.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Ciena information and resources at any time, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Ciena.

Ciena.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Ciena.com, you can find information about Ciena and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Ciena learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Ciena.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Ciena.

To access Ciena.com, go to the following website: http://www.ciena.com.