Ciena SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms

CC Guidance Supplement

Version: 1.3
Date: 11 March 2024

Prepared By:
Intertek Acumen Security, LLC
2400 Research Blvd
Rockville, MD 20850

Revision History

Version	Date	Change
0.1	April 03, 2023	Initial Version
0.2	2023	Second Version
0.3	July 26, 2023	Third Version
0.4	Nov 10, 2023	Fourth version
1.0	February 7, 2024	Made mods
1.1	March 05, 2024	Addressing ECR comments
1.2	March 08, 2024	Minor update
1.3	March 11, 2024	Addressing ECR comments

List of Tables

1 Introduction

This document provides supporting evidence of an evaluation of a specific Target of Evaluation (TOE), Ciena SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms. 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 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms. The TOE is comprised of both software and hardware. The hardware is comprised of the following model series: 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171 and 8180. The software is comprised of the SAOS 10.7.1.

1.1 AUDIENCE

This document is intended for users, such as network technicians and system administrators, who will install the 5162 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 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms CC Guidance Supplement*
AGD[2]	*3948/513x/5144/516x/5170/811x Routers and Platforms, Security SAOS 10.7.1*
AGD[3]	*5162 Router, Installation*
AGD[4]	D-NFVI Software, *D-NFVI Installation, D-NFVI 10.7.1*

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 the Ciena SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms. 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 10.7.1 operating system executed on the 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms.

The TOE implements the general functionality of a router/switch consistent with the collaborative Protection Profile for Network Devices v2.2E. 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). TLS and Hypertext Transfer Protocol Security (HTTPS) may also be used for secure file transfer to and from the outside of the TOE.

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 10.7.1 software executed on the 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms summarized in Table 3. 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 10.7.1 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	100G	Power Options
3926	6	4x1.5GHz ARM Cortex A53	--	AC, DC

Models/Platform	1G/10G SFP+	Processors	100G	Power Options
3928	4	4x1.5 GHz ARM Cortex A53	--	AC, DC
3948	4	4x1.5 GHz ARM Cortex A53	--	AC, DC
5144	8	4x2GHz ARM Cortex A72	--	AC, DC
5164	32x[1G/10G/25G]	4x2GHz ARM Cortex A72	4x [100G/ 200G]	AC, DC
5162	40	Intel XEON D1527, 4CORE	2	AC, DC
5170	4x 25G/10G/1G and 36x 10G/1G	Intel XEON D1527, 4CORE	4xQSFP28	AC, DC
8180	--	Intel XEON D1527, 4CORE	32xQSFP28 FRU module options: 1xWLAi FRU and 4x100G CFP2-DCO	AC, DC
5171	4x 25G/10G/1G and 36x 10G/1G	Intel XEON D1539, 8CORE	FRU module options: 2x QSFP28, 1x QSFP28 + 1x 100G CFP2-DCO, 2x 100G CFP2-DCO, 1x200G CFP2-DCO	AC, DC
Large NFV compute server (FRU)	--	Intel XEON D1548, 8CORE	--	--

2.5 The Evaluated Configuration

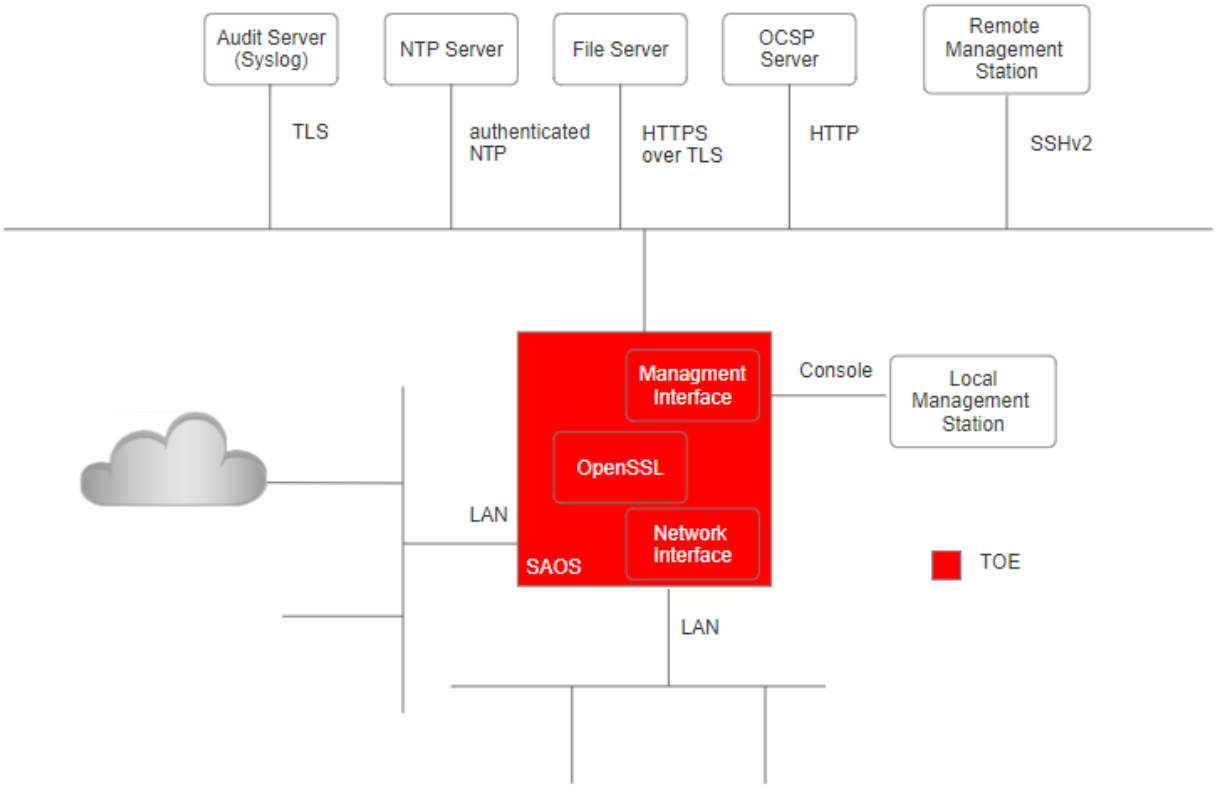
The TOE is the complete network appliance, or a Large NFV Compute Server comprised of TOE software, TOE hardware and TOE security guidance:

- TOE software is Ciena SAOS 10.7.1,
- TOE hardware is 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms, and
- The TOE security guidance is the *Ciena SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms 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 and File 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	The audit server supports syslog messages over TLS to receive the audit files from the TOE. The audit data is stored in the remote audit server for redundancy purposes.

Component	Purpose/Description
NTP server	An external NTP Server for synchronizing the TOE time with. NTP time stamps are protected from tampering using SHA-1 for authentication.
File Server	Remote file server for storing user files and updating the TOE. Communication with the File Server is with HTTPS over TLS.
OCSP Server	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	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.
- MACsec functionality is not evaluated and 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 manoeuvring 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 8 Selectable Parts

Part number	Description	Notes
170-5162-900	5162, (2) 100 GbE QSFP28, (40) 10/1 GbE SFP+, SYNC, (2) SLOTS AC OR DC	Chassis
170-0002-900	DC power distribution unit	Power units can be AC or DC, however, the combination of AC and DC units in the same chassis is not supported.
170-0093-900	AC power supply 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
170-0112-900		Switzerland
170-0113-900		Europe
170-0114-900		North America
170-0115-900		United Kingdom
170-0116-900		Universal
	SFP and SFP+ optic modules	
	Faceplate cabling	Cat-5E STP and cabling to match SFP and SFP+ connectors.

Table 9 Optional and Replacement Parts

Part number	Description	Notes
192-0004-900	Spare fan unit	

Part number	Description	Notes
170-0157-900	Rack ears for mounting in a 4-post, 19-inch rack.	The chassis ships with a four-post, 19-inch rack mount kit. All kits include mounting brackets, cable management brackets, and screws.
170-0356-900	Rack ears for mounting in a 4-post, 21-inch ETSI rack	
170-0192-900	Rack ears for mid-mounting in a 2-post, 19-inch rack	
170-0193-900	Rack ears for flush-mounting in a 2-post, 19-inch rack	
170-0194-900	Rack ears for mid-mounting in a 2-post, 23-inch rack	
170-0195-900	Rack ears for flush-mounting in a two-post, 23-inch rack in a front-mount installation.	

Overview

The following items are shipped:

- 5162 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[3] the *5162 Platform Installation* guide for hardware installation for all models except the D-NFVIs. For those models, follow AGD[4] for 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 RNG 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 13 - Cable required to connect to console port

System	Console port	Cable
3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms	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 14 - 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 15 - Baud rate by system

System	Baud rate
3926, 3928	9600 bps

System	Baud rate
3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms	115200 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
toprosecution!!!
   SAOS. The next generation in switching software.
```

4.1.2 Console Administration USB-C

Requirements

The following table lists the connection requirements for the USB-C console port.

Table 16 - Connection requirements for the USB-C console port

System	Console port	Cable
3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms	USB-C	The console port supports USBC to USB-C and USB-C to USBA type cables up to 13 feet (4 meters) in length and is based on the USB2.0 protocol. The USB console port can be connected directly to USB-based Terminal Servers or to a USB port on a Laptop/PC (a specific USB driver on the PC may be required).

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 the 3926, 3928, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms.

Table 17- Terminal settings

Terminal setting	Value
Serial line	COM port
Port	115200 bps for 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms
	9600 bps for 3926, 3928
Connection type	serial

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

Table 18 - Baud rate by system

System Baud	rate
3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms	115200 bps
3926, 3928	9600 bps

Steps

1. Plug the USB-C end of the cable into the CONSOLE port.
2. Connect a PC running terminal emulation software.
   The PC detects the cable and automatically installs any required drivers.
3. Open the Device Manager on your PC and under the Ports (COM & LPT) section, determine the COM port used to connect to the system.
4. At the prompt, configure the connected terminal.
5. When the login prompt is displayed, press **Enter** and enter the default username and password.
6. Access the configuration CLI: enter `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.
```

4.1.3 Root Username and Password

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 19 - Parameter for setting the system hostname

Parameter	Valid values	Description
hostname>	string	The system hostname is a string of up to 63 characters.

Steps

1 Access configuration mode:

```
conf
```

2 Set the system hostname:

```
system config hostname <hostname>
```

Example

The following example sets the system hostname to system2.

```
config
system config hostname system2
```

4.1.4 BOOT VERIFICATION

- If required, retrieve and installs 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.

```
CGSI5162> 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 and ecdsa-sha2-nistp256. 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 public-key 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 message authentication, 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, ecdh-sha2-nistp384, ecdh-sha2-nistp521 key exchange methods. We need to enable the same on TOE (Section 5.2.6).
- The TOE implements Time-based as well as traffic based rekey. For traffic-based TOE does rekey for administrative configured value same is the case for time-based rekey also. 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 24 Parameters for configuring the remote management interface.

Parameters	Valid values	Description
name	remote	Specifies the remote interface.
role	management	Specifies the role of the

Parameters	Valid values	Description
		interface.
admin-status	true | false	Allows the remote interface to be administratively shut down (disabled).
mtu_size	64..9216 Default: 1526	Specifies the maximum transmission unit (MTU) size.
type	ip | ettp | lag | system | loopback	For an L3 interface select ip or loopback Note: The evaluated configu joan
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 <name> oc-if:config role management mtu
<mtu> admin-status true type ip
```

3 Specify the forwarding domain for the underlay binding.

```
oc-if:interfaces interface <name> oc-if:config underlaybinding fd
<fd_name>
```

4 Assign an IP address and set the prefix length.

```
oc-if:interfaces interface <name> <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 oc-if:config role management mtu
1500 adminstatus
```

true type ip

```
oc-if:interfaces interface remote oc-if: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 22 - 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 23 - 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. Enable SSH public key authentication.

```
system ssh-server config public-key-authentication <public-key-
authentication>
```

Example

The following example enables SSH public key authentication.

```
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 5: Parameter for configuring the PKA Algorithms

Parameter	Valid Values	Description
pka-algoritm	ssh-rsa | ecdsa-sha2-nistp256	Specifies the pka algorithms. ***Note***: the evaluated configuration requires this parameter to be the

		values listed in the Valid Values column.

Steps

1. Enable SSH public key authentication.

```
system ssh-server config pka-algorithm <pka-algorithm>
```

Example

The following command enables SSH public key authentication:

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

5.2.4 CONFIGURE ENCRYPTION ALGORITHMS

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

Table 6: 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. Configure encryption algorithms.

```
system ssh-server config encryption-algorithm <encrption-algorithm>
```

Example

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

```
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 7: 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. 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.

```
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 8: 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. 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 time in seconds after which the session key can be renegotiated.

Table 9: 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 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.

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

5.2.8 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 10: Rekey Limit Parameters

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. 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.

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

5.3 SSH 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. 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.

- `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 and the file server using TLS. The evaluated configuration requires the operational environment to provide a file server that supports HTTPS over TLS communication. Configuration of a syslog server is optional. To enable communication with the file 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 11: 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 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 RFC5246, TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288, TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,	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.

Parameters	Valid Values	Description
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289	
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. Specify the name of the TLS profile:
   - `hello-params tls-profiles tls-profile <name>`
2. Set the minimum TLS version for the profile named syslog-tls:
   - `hello-params syslog-tls tls-versions tls-version tls-1.2`
3. Set the TLS cipher suites for the profile named syslog-tls:

```
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
```

4. Set the elliptic curves for the profile named syslog-tls:

```
hello-params syslog-tls elliptic-curves elliptic-curve secp256r1
secp384r1 secp521r1
```

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 on receipt of the Server's certificate

(Syslog Server and File 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 12: Peer Authentication Profile Parameters

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

Steps

1. Specify the name of the peer authentication profile:
   ```
   pkix peer-auth-profiles peer-auth-profile <peer-auth-profile-name>
   ```
2. 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
   ```
3. 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-cert-expiry false
   ```

Example

The following example creates a peer authentication profile named baseConf.

```
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-cert-expiry
false
```

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 13: TLS Service Profile Parameters

Parameters	Valid values	Description
tls-profile-name	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. 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. This can be left to null because mutual authentication is not supported by the evaluated configuration.

Steps

1. Identify the TLS Profile
   `tls-service-profiles <tls-service-profile-name> tls-profile-name <tls-profile>`
2. Identify the peer authentication profile.
   `tls-service-profiles <tls-service-profile-name> tls-peer-auth-profile-name <peer-auth-profile>`
3. 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.

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

6.2 X.509 CERTIFICATES

The TOE uses X.509 certificates for communication with the syslog server and the file 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:
    - Server certificates presented for TLS must have the Server Authentication purpose (id-kp 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 (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.
    - The TOE will only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

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 or File Server) and when they are loaded onto the TOE. 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. If the connection fails, the Administrator should check the physical connections and reenable the OCSP client with the following command: `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. 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 that 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-fileuri
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.**

Steps

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.**

Steps

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

```
pkix-certificates-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-certificates-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:**

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

The following example enables check-fingerprint for a peer authentication

profile named baseConf.

```
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) |
+---------------------+-----------------------------------+
```

- **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 | disabled |
| NONCE State | enabled |
| Default OCSP Responder URL | - |
+------------------------------+-----------------------------------+
```

- **Add entries to ip-host-list:**

```
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.

```
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
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-profilename 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 TOE supports secure communication of the TOE with an OCSP Server over an HTTPS connection using TLS v1.2 implementation. In this scenario, the TOE acts as an HTTP client communicating with the servers in the Operational Environment. The HTTP protocol complies with RFC 2818. The request/response nature of these messages results in OCSP servers being termed OCSP responders.

The TOE communications 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.**

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

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

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

- **Modify the OCSP state.**

```
hello-params <profile-name> ocsp-state <state>
```

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

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

- **Modify the nonce state.**

```
hello-params <profile-name> nonce-state <state>
```

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

```
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

- **Add entries to ip-host-list:**

```
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.

```
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
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-profilename check-ip-
host true
```

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 or to update the time from an NTP server(s). 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.

Note: If NTP is enabled on the system, you cannot set the system time with this procedure.

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 |
+--------------+------------------------+
```

7.2 NTP Server Configuration

The TOE supports the use of the NTP version 4 (NTP v4) to synchronize the time and date of the TOE with an NTP server(s). The TOE communicates with NTP servers using UDP. The TOE validates the integrity of the time source received from NTP servers using SHA1 as the message digest algorithm. The NTP server is an optional server in the operational environment. However, setting the clock is required for the evaluated configuration.

The Ciena devices support a maximum of 10 NTP servers. However, the evaluated configuration the number of NTP servers tested were up to three. This is not a configurable parameter and must be defined in your company's network plan and followed by your network administrators. By default, the NTP client is enabled in a polling mode.

- By default, the TOE does not allow timestamp updates from broadcast and multicast addresses.
- By default, the NTP version is v4.

7.2.1 Creating an Association among the System Software, NTP Client, and the NTP Server

To configure the NTP client, the administrator creates an association among the system software, the NTP client, and the NTP server to ensure that accurate time is available.

Steps

1. Create the NTP association:
   ```
   system ntp associations remote-ntp-server server-entry <IP address>
   admin-state enabled
   ```

7.2.2 Enabling the NTP Client

1. Enable the NTP client:
   ```
   system ntp admin-state enabled
   ```

7.2.3 Configure an NTP Server

1. Configure an association with the NTP server:
   ```
   system ntp associations remote-ntp-server server-entry <IP address>
   auth-key-id <integer>
   ```
2. Configure message digest algorithm along with message digest string for integrity of time source:
   ```
   system ntp authentication auth-entry <auth-key-id integer> auth-key-
   type <sha1>
   system ntp authentication auth-entry <auth-key-id integer> auth-key-enc
   <message digest string>
   ```
   Note: the Ciena device supports both SHA1 and MD5 as the message digest algorithm however, the evaluated configuration only supports SHA1.
3. Enable NTP message digest authentication:
   ```
   system ntp authentication auth-admin-state enabled
   ```

To configure multiple NTP servers, repeat the steps above with different IP addresses.

Example

The following examples shows the output from creating an association among the system software, the NTP client, and the NTP server.

```
config
➢ system ntp associations remote-ntp-server server-entry 192.0.2.0 admin-
  state
  enabled
➢ system ntp associations remote-ntp-server server-entry 192.0.2.0 auth-key-
  id 7
➢ system ntp admin-state enabled
➢ system ntp authentication auth-entry 7 auth-key-type sha1
➢ system ntp authentication auth-entry 7 auth-key-enc
  64b0bfe07a34ab4daf9ab87fda50021e77176151
➢ system ntp authentication auth-admin-state enabled
exit
```

The following example shows a successful association.

```
show ntp client
```

```
+-------- NTP CLIENT STATE -------+
| Name | Value |
+----------------------+----------+
| Admin State | enabled |
| Mode | polling |
| Polling Min Interval | 16 |
| Polling Max Interval | 16 |
| Auth Admin State | disabled |
| Synchronized | True |
| Delay | 0.124 |
| Offset | -2.213 |
| Jitter | 5.919 |
| Drift (PPM) | 0.0 |
+----------------------+----------+


+---------- NTP CONFIGURED SERVERS ---------+
| Address | Auth Key ID | Admin State |
+---------------+-------------+-------------+
| 192.0.2.0 |    7      | enabled |
+---------------+-------------+-------------+
+------------------------ NTP OPER SERVERS --------------------------
---+
| Address | Auth | Server | Server Condition | Auth State| Offset |
| |Key ID | State | | | |
+---------------+-------+--------+------------------+-----------+-----
---+
| 192.0.2.0 | 7 | reach | syspeer | none | -2.213 |
+---------------+-------+--------+------------------+-----------+-----
---+
```

To configure multiple NTP Servers, repeat the process and substitute new values.

8 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.

8.1 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 the table below). 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 Non-TOE 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 12 below.
As noted above, the information includes at least all of the required information. Example audit events are included in Table 12 below. The auditable events that result from administrative actions are included in Table 12 and are designated with ‘Administrative Actions’ within the Auditable Events column.

8.2 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:

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

The following example shows how to enable configuration logging:

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

8.3 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@CGSI5162.ui:/mnt/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@CGSI5162.ui:/mnt/central-logger$
```

8.4 Set Logging Size

To check the logging file and it's archived file when the latest file is full and overwrite with newest log file.

```
diag@CGSI5162.ui:/mnt/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@CGSI5162.ui:/mnt/central-logger$
```

8.4.1 Viewing Log Events

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

```
CGSI5162> log view events
```

8.4.2 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.

```
CGSI5162> log clear events
Successfully cleared events logs
CGSI5162>
```

8.5 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.

Enable logging.
```
syslog log-actions remote-syslog-tls admin-state <enable/disable>
```

Identify the IP address of the syslog server.
```
Config syslog log-actions remote-syslog-tls destination <ip address or DNS>
```

Assign a TLS Profile to the connection.
```
syslog log-actions remote-syslog-tls tls-service-profile "profile name"
```

Set TLS timeout.
```
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 document.

8.6 CONFIGURING LOG LEVEL

Table 14: 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. 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.
```
syslog log-action remote-syslog-tls destination 10.1.5.200 severity alert critical debug emergency error info notice warning
```

8.7 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.
   - `syslog log-actions remote-syslog-tls timeout 6`
   - `syslog log-actions remote-syslog-tls tls-service-profile "profile name"`

8.7.1 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.

```
CGSI5162> config
```

1.

```
username@CGSI5162# tls-service-profiles "tls service profile name"
```

2. Identify the peer authentication profile:

```
username@CGSI5162# tls-service-profiles syslog-tls-service tls-certificate-name "tls certificate name"
```

3.

```
username@CGSI5162# tls-service-profiles syslog-tls-service tls-peer-
auth-profile-name "tls peer auth profile"
```

4.

```
username@CGSI5162# tls-service-profiles syslog-tls-service tls-
profile-name "tls service profile name"

diag@CGSI5162# pkix peer-auth-profiles peer-auth-profile "peer auth
profile name"
diag@CGSI3926# pkix peer-auth-profiles peer-auth-profile Peer check-
ip-host true
diag@CGSI3926# pkix peer-auth-profiles peer-auth-profile Peer ip-host-
list "ip address"
```

Check the TLS configuration by following command and output

```
CGSI5162> 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          |
| IP/Host List       | 10.1.5.207     |
| Fingerprint List   | -              |
+--------------------+----------------+
```

9 Configuring Communication to the File Server

The TOE communicates with the File Server using HTTPS over TLS. To perform a file transfer of a new TOE from the File Server perform the following command:

- `software install url <url> tls-service-profile <tls-service-profile name>`

Where:

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

`<tls-service-profile name>` = the name of the TLS Service Profile. The TLS Service profile points to the TLS Profile which defines the minimum TOE version, the cipher suites, and elliptic curves supported by the TOE and points to the Peer Authentication Profile which defines if the Server's certificate should be validated and if true, how the certificate should be validated. Refer to Section 6 for instructions of how to configure the TLS connection to the File Server in the evaluated configuration.

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. The TLS Service Profile's name is syslog-tls-service.

```
CGSI5162>
CGSI5162> software install url https://10.1.5.208/saos-10-07-01-0289-RS12.yml tls-service-profile syslog-tls-service
```

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 by making available to the user 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 **banner motd** 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 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.
```

To create a banner of text “This is a banner” use the command.

Steps

1. Set the system welcome-banner:

```
system config motd-banner <banner-text>
```

Example
The following example sets the system welcome-banner:

```
system config motd-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 25 - 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 user name 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 and composed of any combination of upper and lower case letters, numbers, and the following special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", "+", ",", "-", ".", "/", ":", ";", "<", "=", ">", "[", "\", "_", "`", 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. Configure the minimum length of the password:
   `system aaa authentication password-policy config minlength <integer>`
2. Configure the minimum number of lower-case characters:
   `system aaa authentication password-policy config minlowercase-chars <integer>`
3. Configure the minimum number of numeric characters:
   `system aaa authentication password-policy config minnumeric-chars <integer>`
4. Configure the minimum number of special characters:
   `system aaa authentication password-policy config minspecial-chars <integer>`
5. Configure the minimum number of upper-case characters:
   `system aaa authentication password-policy config minuppercase-chars <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.

```
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. 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 15: 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.
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. Verify the newly created account by display the accounts in the system.
   ```
   show aaa users
   ```
4. 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.

Parameters	Valid values	Description
group	super, admin, limited	Specifies the group that the user will be part of.
user-name	String	Specifies the user name being add.

Steps

1. 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.

```
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. 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.

2. 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.

```
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 various FPGA devices access and sanity,
- Check of PCI bus and devices response,
- Crypto KAT/self-test
- Integrity self-tests.

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 27 - 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.

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-10-00-00-0131-packages.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.

12.1 Updating the TOE

The TOE can be updated from the File Server using HTTPS over TLS. The TOE verifies the update using signature verification. If the signature validation is successful, the TOE will be immediately applied. If the signature validation fails, an error message will be displayed.

Steps:

- `software install url <url> tls-service-profile <tls-service-profile name>`

Where:

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

`<tls-service-profile name> =` the name of the TLS Service Profile. The TLS Service profile points to the TLS Profile which defines the minimum TLS version, cipher suites and elliptic curves supported by the TOE and points to the Peer Authentication Profile which defines if the Server's certificate should be validated and if true, how the certificate should be validated. Refer to Section 6 for instructions of how to configure the TLS connection to the File Server in the evaluated configuration.

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. The TLS Service Profile's name is syslog-tls-service.

```
CGSI5162>
CGSI5162> 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 using HTTPS over TLS, the TOE image is validated with a SHA-256 digital signature. The TOE will display messages to the workstation indicating the success and or failure of the signature verification.

12.2.1 Successful Upload Signature Verification

The following shows an example of successful installation.

Example

1. Upgrade the TOE by accessing the image from the file server using HTTPS over TLS.

```
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.

```
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, indicating a successful signature validation.

```
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, and if the signature validation is successful, there is no other administrative action required. The TOE will automatically install and activate the new image.

12.2.2 Unsuccessful Upload Signature Verification

The following shows an example of an unsuccessful installation. The installation failed because the signature verification failed.

Example

1. Upgrade the TOE by accessing the image from the file server using HTTPS over TLS.

```
CGSI3926>
CGSI3926>
CGSI3926> software install url https://10.1.5.210/saos-10-07-01-0289-MRS12.yml tls-service-profile service-tls
Error: Could not read /mnt/config/docker/ciena/installed/saos-10-07-01-0289-MRS12.yml, removed
CGSI3926>
CGSI3926>
CGSI3926>
```

If an upgrade fails, go to the following website to report the error: https//www.ciena.com.

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 28 - 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 • Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators) • Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed) • Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference	None	**Start-up and shut-down of audit functions:** The audit function starts up and shuts down with the TOE. **Shut-down of audit function:** INFO 2024-03-08 14:42:28.724880 cn-node-evtbroker System(chassis): Restart alert; Restart-reason: Manual Restart, Restart-type: Power Cycle **Start-up of audit function:** INFO 2024-03-08 14:45:38.004850 cn-node-evtbroker Health_Monitoring_Manager(chassis): CPU-Utilization HealthState (Normal) CRIT 2024-03-08 14:45:44.692623 cn-node-evtbroker Health Monitoring Event: Id:03.00.00.00 Severity:Critical Status:Clear Msg:Heartbeat client has resumed data path connectivity Data:Message: Number of state transitions (1) INFO 2024-03-08 14:49:00.704094 cn-node-evtbroker cold-kick-event • **Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators)** **Administrative login:** INFO 2022-04-07 10:39:39.682209 cn-node-evtbroker Identity(chassis): Incoming connection from 10.1.5.209 : 58784 INFO 2022-04-07 10:39:39.693204 cn-node-evtbroker Identity(chassis): User

	shall be logged) • Resetting passwords (name of related user account shall be logged)		successfully logged in from IP 10.1.5.209 user name 'diag' **Administrative logout:** INFO 2022-04-11 08:49:58.530812 cn-node-evtbroker Identity(chassis): User logged out from IP 10.1.5.209 user name 'diag' INFO 2022-04-11 08:49:58.772028 cn-node-evtbroker Identity(chassis) sshd Session '10.1.5.209:58828' for User 'diag' authentication-method Local logged out • **Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed)** **Ability to administer the TOE locally and remotely.** **Local Console:** **Failed login attempt:** INFO 2022-04-07 10:21:35.715577 cn-node-evtbroker Identity(chassis): Login failure event alert for diag from Local:ttyPS0 CGSI3926> log view security INFO 2022-04-07 10:21:23.363613 login pam_unix(login:session): session closed for user diag INFO 2022-04-07 10:21:31.629584 login pam_succeed_if(login:auth): requirement "tty =~ /dev/tty*" was met by user "diag" NOTIF 2022-04-07 10:21:35.521857 login pam_unix(login:auth): authentication failure; logname=diag uid=0 euid=0 tty=/dev/ttyPS0 ruser= rhost= user=diag NOTIF 2022-04-07 10:21:38.290404 login FAILED LOGIN (1) on '/dev/ttyPS0' FOR 'diag', Authentication failure. **Successful login attempt:** CGSI3926> log view events

			INFO 2022-04-07 10:39:39.342553 cn-node-evtbroker Identity(chassis): Login success event alert for diag from 10.1.5.209:58784 INFO 2022-04-07 10:39:39.682209 cn-node-evtbroker Identity(chassis): Incoming connection from 10.1.5.209 : 58784 INFO 2022-04-07 10:39:39.693204 cn-node-evtbroker Identity(chassis): User successfully logged in from IP 10.1.5.209 user name 'diag'. **SSH:** **Failed login attempt:** INFO 2022-04-07 10:36:16.926551 sshd pam_succeed_if(sshd:auth): requirement "tty =~ /dev/tty*" not met by user "diag" NOTIF 2022-04-07 10:36:16.960806 sshd pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh:58782 ruser= rhost=10.1.5.209 user=diag INFO 2022-04-07 10:36:19.404714 sshd Failed password for diag from 10.1.5.209 port 58782 ssh2 INFO 2022-04-07 10:36:24.406870 sshd pam_succeed_if(sshd:auth): requirement "tty =~ /dev/tty*" not met by user "diag" INFO 2022-04-07 10:36:26.324536 sshd Failed password for diag from 10.1.5.209 port 58782 ssh2 **Successful login attempt:** INFO 2022-04-07 10:39:39.693204 cn-node-evtbroker Identity(chassis): User successfully logged in from IP 10.1.5.209 user name 'dia INFO 2022-04-07 10:39:38.712940 sshd pam_succeed_if(sshd:auth): requirement "tty =~ /dev/tty*" not met by user "diag" INFO 2022-04-07 10:39:39.659076 sshd Accepted password for diag from 10.1.5.209 port 58784 ssh2 INFO 2022-04-07 10:39:39.686167 sshd pam_unix(sshd:session): session opened for user diag by (uid=0)

			Ability to configure the access banner. CGSI3926> log view events NOTIF 2022-04-11 10:06:20.618900 cn-node-evtbroker Netconf(chassis): Session ID: 58; Username: diag; Client IP: 192.168.254.45; 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 and SSH session termination** CGSI3926> log view events NOTIF 2022-04-21 06:17:30.754755 cn-node-evtbroker Netconf(chassis): Session ID: 68; Username: diag; Client IP: 192.168.254.45; Target XPath: /oc-sys:system/oc-sys:ssh-server/oc-sys:config/oc-sys:timeout; Edit Operation: create NOTIF 2022-04-11 09:17:49.919692 cn-node-evtbroker Netconf(chassis): Session ID: 55; Username: diag; Client IP: 127.0.0.1; 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 [signature] capability prior to installing those updates.** INFO 2024-01-17 17:08:59.265626 xgrade-ng Operation requested: {'operation': 'install', 'options': {'manifest_url': 'https://10.1.5.210/saos-10-07-01-0289-RS12.yml', 'verify_signature': True, 'defer_activation': False, 'ca_directory': '/mnt/config/pkix/cert///hashed/', 'tls_config_file': '/mnt/config/pkix/secure/system/systemTls.cfg', 'passphrase': 'test', 'manifest_hash_algorithm': 'sha-256'}} INFO 2024-01-17 17:09:11.455520 xgrade-ng Unscheduling pending operations: {'scheduler_state': [{'operation': 'activate', 'options': {'manifest_url': 'https://10.1.5.210/saos-10-07-01-0289-

			RS12.yml', 'verify_signature': True, 'defer_activation': False, 'ca_directory': '/mnt/config/pkix/cert///hashed/', 'tls_config_file': '/mnt/config/pkix/secure/system/systemTls.cfg', 'passphrase': 'test', 'manifest_hash_algorithm': 'sha-256'}, 'package_name': 'saos-10-07-01-0289-RS12', 'retries': 0}, {'operation': 'install', 'options': {'manifest_url': 'https://10.1.5.210/saos-10-07-01-0289-RS12.yml', 'verify_signature': True, 'defer_activation': False, 'ca_directory': '/mnt/config/pkix/cert///hashed/', 'tls_config_file': '/mnt/config/pkix/secure/system/systemTls.cfg', 'passphrase': 'test', 'manifest_hash_algorithm': 'sha-256'}, 'package_name': 'saos-10-07-01-0289-RS12', 'retries': 0}]} ERROR 2024-01-17 17:09:11.466465 xgrade-ng Invalid signing certificate: https://10.1.5.210/software-signing-cert.pem ERROR 2024-01-17 17:09:11.477016 cn-node-shwm xgrade operation failed: {"status": "error", "message": "Install failure", "code": 503, "data": {"software_state": "idle", "latest_log": "installing evernight-generic-arm-aarch64-01-07-01-0283-upgrade.sh on standby bank", "state_timeout": 0, "error_string": "Invalid signing certificate: https://10.1.5.210/software-signing-cert.pem"}} **Ability to configure the authentication failure parameters for FIA_AFL.1** NOTIF 2023-04-18 11:28:47.262741 cn-node-evtbroker Netconf(chassis): Session ID: 132; Username: diag; Client IP: 192.168.228.50; Target XPath: /oc-sys:system/oc-sys:aaa/oc-sys:authentication/ciena-oc-aaa:lockout-policy; Edit Operation: create.

			Ability to modify the behaviour of the transmission of audit data to an external IT entity. NOTIF 2022-09-19 10:44:14.647039 cn-node-evtbroker Netconf(chassis): Session ID: 16; Username: diag; Client IP: 192.168.254.108; 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.** INFO 2024-01-11 13:54:59.733594 cn-node-evtbroker Identity(chassis): User Pubkey diag.pub is successfully changed by diag from 10.1.5.209 EMERG 2024-01-19 12:19:13.090235 netconfd-pro User Pubkey diag.pub is successfully deleted by diag from 192.168.254.140 **Ability to configure the cryptographic functionality.** INFO 2024-01-11 13:54:59.733594 cn-node-evtbroker Identity(chassis): User Pubkey diag.pub is successfully changed by diag from 10.1.5.209 **Ability to set the time which is used for time stamps.** INFO 2022-04-18 09:15:00.144967 cn-node-evtbroker System(chassis): Clock change alert; configured-value: 2022-04-18T09:15:00Z. **Ability to configure thresholds for SSH rekeying** NOTIF 2022-08-25 12:02:51.610315 cn-node-evtbroker Netconf(chassis): Session ID: 40; Username: diag; Client IP: 192.168.254.99; 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. NOTIF 2022-09-16 11:09:00.810353 cn-node-evtbroker Netconf(chassis): Session ID: 118; Username: diag; Client IP: 192.168.254.108; Target XPath: /syslog:syslog/syslog:log-actions/ciena-syslog-tls:remote-syslog-tls/ciena-syslog-tls:destination[ciena-syslog-tls:address="10.1.5.210"]; Edit Operation: create. **Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors.** INFO 2023-04-19 12:50:45.010281 cn-node-evtbroker User 'diag' successfully installed X.509 CA certificate with name ROOTCA2. Result: success **Ability to import X.509v3 certificates to the TOE's trust store.** INFO 2023-04-19 12:50:45.010281 cn-node-evtbroker User 'diag' successfully installed X.509 CA certificate with name ROOTCA2. Result: success. **Ability to manage the trusted public keys database.** INFO 2023-04-19 12:50:45.010281 cn-node-evtbroker User 'diag' successfully installed X.509 CA certificate with name ROOTCA2. Result: success INFO 2023-04-19 12:51:01.420262 cn-node-evtbroker User 'diag' successfully uninstalled X.509 CA certificate with name ROOTCA2. Result: success **Ability to configure NTP.** CGSI3926> log view events NOTIF 2024-03-29 07:29:30.848414 cn-node-evtbroker Netconf(chassis): Session ID: 11; Username: diag; Client IP: 192.168.254.140; Target XPath: /oc-

			sys:system/ciena-ntp:ntp/ciena-ntp:admin-state; Edit Operation: merge NOTIF 2024-03-29 07:30:24.400034 cn-node-evtbroker Netconf(chassis): Session ID: 11; Username: diag; Client IP: 192.168.254.140; Target XPath: /oc-sys:system/ciena-ntp:ntp/ciena-ntp:associations/ciena-ntp:remote-ntp-server/ciena-ntp:server-entry[ciena-ntp:address="10.1.5.209"]; Edit Operation: create • **Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).** INFO 2024-01-11 13:54:59.733594 cn-node-evtbroker Identity(chassis): User Pubkey diag.pub is successfully changed by diag from 10.1.5.209 EMERG 2024-01-19 12:19:13.090235 netconfd-pro User Pubkey diag.pub is successfully deleted by diag from 192.168.254.140 • **Resetting passwords.** NOTIF 2024-01-30 10:46:13.417987 cn-node-evtbroker Netconf(chassis): Session ID: 64; Username: diag; Client IP: 192.168.228.34; Target XPath: /oc-sys:system/oc-sys:aaa/oc-sys:authentication/oc-sys:users/oc-sys:user[oc-sys:username="test"]/oc-sys:config/ciena-oc-sys:password; Edit Operation: create
FAU_GEN.2	None	None	

FAU_STG_EXT.1	Protected Audit Event Storage	Able to send data to audit server in encrypted format not in plaintext format	**Protected Audit Event Storage.** CGSI3926> log view events NOTIF 2022-09-16 11:09:00.810353 cn-node-evtbroker Netconf(chassis): Session ID: 118; Username: diag; Client IP: 192.168.254.108; Target XPath: /syslog:syslog/syslog:log-actions/ciena-syslog-tls:remote-syslog-tls/ciena-syslog-tls:destination[ciena-syslog-tls:address="10.1.5.210"]; Edit Operation: create INFO 2022-09-16 11:09:00.948294 cn-node-evtbroker SYSLOGTLS begining connection. Client: :: Server: 10.1.5.210:6514 INFO 2022-09-16 11:14:32.162859 cn-node-evtbroker Identity(chassis): ssh_set_newkeys: rekeying in for 192.168.254.108 port 4418, input 31752 bytes 1882 blocks, output 94416 bytes 0 blocks INFO 2022-09-16 11:16:28.612313 cn-node-evtbroker Identity(chassis): Login success event alert for diag from 10.1.5.210:38202 INFO 2022-09-16 11:16:28.705768 cn-node-evtbroker SYSLOGTLS begining connection. Client: :: Server: 10.1.5.210:6514 INFO 2022-09-16 11:16:28.713530 cn-node-evtbroker TLS Client Session Module : evtbroker, Message Type : Start, Date : 2022-09-16, Time: 11:16:28.618420, Session Key : 169.254.160.9:45251_10.1.5.210:6514 , Source IP : 169.254.160.9:45251 , Destination IP: 10.1.5.210:6514 INFO 2022-09-16 11:16:28.721145 cn-node-evtbroker SYSLOGTLS X.509 certificate verified /C=US/O=Acumen/OU=CC/CN=Cienavmiii.acumensec.local Client: 169.254.160.9 Server: 10.1.5.210:6514 INFO 2022-09-16 11:16:28.727197 cn-node-evtbroker SYSLOGTLS connection established. Client: 169.254.160.9 Server: 10.1.5.210:6514

			INFO 2022-09-16 11:16:28.825451 cn-node-evtbroker Identity(chassis): Incoming connection from 10.1.5.210 : 38202 INFO 2022-09-16 11:16:28.832420 cn-node-evtbroker Identity(chassis): User successfully logged in from IP 10.1.5.210 user name 'diag'
FCS_CKM.1	None	None	
FCS_CKM.2	None	None	
FCS_CKM.4	None	None	
FCS_COP.1/Data Encryption	None	None	
FCS_COP.1/SigGen	None	None	
FCS_COP.1/Hash	None	None	
FCS_COP.1/Keyed Hash	None	None	
FCS_HTTPS_EXT.1	Failure to Establish a HTTPS session	Reason For failure	**Failure to establish a HTTPS session.** INFO 2022-06-13 07:38:36.996303 cn-node-evtbroker TLS Client Session Module : evtbroker, Message Type : Start, Date : 2022-06-13, Time: 07:38:36.990064, Session Key : 169.254.160.9:51567_10.1.5.207:6514 , Source IP : 169.254.160.9:51567 , Destination IP: 10.1.5.207:6514 INFO 2022-06-13 07:38:36.998808 cn-node-evtbroker SYSLOGTLS Error: src: '169.254.160.9' dst: '10.1.5.207' Error: 'TLS error during handshake : sslv3 alert handshake failure Certificate: CLIENT.acumensec.local' EMERG 2023-12-15 09:08:34.183283 cn-node-evtbroker SYSLOGTLS begining connection. Client: :: Server: 10.1.5.209:6514 NOTIF 2023-12-15 09:08:34.185406 cn-node-evtbroker TLS Session Client Start sessionkey = 169.254.160.9:58133_10.1.5.209:6514 |

			Source_IP_Port = 169.254.160.9:58133 | Destination_IP_Port = 10.1.5.209:6514 & EMERG 2023-12-15 09:08:34.293735 cn-node-evtbroker SYSLOGTLS Error: src: '169.254.160.9' dst: '10.1.5.209' Error: 'TLS error during handshake : digest check failed Certificate: 10.1.5.209 10.1.5.51'
FCS_NTP_EXT.1	Configuration Of a new time server Removal of Configured Time server	Identity if New/ removed time server	**Configuration of a new time server.** CGSI3926> log view events NOTIF 2024-03-29 07:29:30.848414 cn-node-evtbroker Netconf(chassis): Session ID: 11; Username: diag; Client IP: 192.168.254.140; Target XPath: /oc-sys:system/ciena-ntp:ntp/ciena-ntp:admin-state; Edit Operation: merge NOTIF 2024-03-29 07:30:24.400034 cn-node-evtbroker Netconf(chassis): Session ID: 11; Username: diag; Client IP: 192.168.254.140; Target XPath: /oc-sys:system/ciena-ntp:ntp/ciena-ntp:associations/ciena-ntp:remote-ntp-server/ciena-ntp:server-entry[ciena-ntp:address="10.1.5.209"];Edit Operation: create INFO 2023-11-16 11:44:16.384578 cn-node-evtbroker Alarm_Manager(chassis): Alarm type:ntp-out-of-sync qualifier: being CLEARED for resource:/ ciena-ntp:sync-status-change-notification with severity:Warning at time:2023-11-16T11:44:16.375534205Z **Removal of Configured Time server.** NOTIF 2022-04-21 08:30:04.219053 cn-node-evtbroker Netconf(chassis): Session ID: 71; Username: diag; Client IP: 192.168.254.45; Target XPath: /oc-sys:system/ciena-ntp:ntp/ciena-ntp:associations/ciena-ntp:remote-ntp-server/ciena-ntp:server-entry[ciena-ntp:address="10.1.5.210"]; Edit Operation: create

			INFO 2022-04-21 08:30:07.572658 cn-node-evtbroker Alarm_Manager(chassis): Alarm type:ntp-out-of-sync qualifier: being SET for resource:/ciena-ntp:sync-status-change-notification with severity:Warning at time:2022-04-21T08:30:07.558905751Z INFO 2022-04-21 08:30:12.521441 cn-node-evtbroker Alarm_Manager(chassis): Alarm type:ntp-out-of-sync qualifier: being CLEARED for resource:/ciena-ntp:sync-status-change-notification with severity:Warning at time:2022-04-21T08:30:12.516787713Z NOTIF 2022-04-21 08:30:26.679447 cn-node-evtbroker Netconf(chassis): Session ID: 71; Username: diag; Client IP: 192.168.254.45; Target XPath: /oc-sys:system/ciena-ntp:ntp/ciena-ntp:associations/ciena-ntp:remote-ntp-server/ciena-ntp:server-entry[ciena-ntp:address="10.1.5.208"]; Edit Operation: create INFO 2022-04-21 08:30:27.645806 cn-node-evtbroker Alarm_Manager(chassis): Alarm type:ntp-out-of-sync qualifier: being SET for resource:/ciena-ntp:sync-status-change-notification with severity:Warning at time:2022-04-21T08:30:27.617301399Z INFO 2022-04-21 08:30:37.536978 cn-node-evtbroker Alarm_Manager(chassis): Alarm type:ntp-out-of-sync qualifier: being CLEARED for resource:/ciena-ntp:sync-status-change-notification with severity:Warning at time:2022-04-21T08:30:37.523444063Z
FCS_RBG_EXT.1	None	None	NA
FCS_SSHS_EXT.1	Failure to Establish an SSH session	Reason For failure	**Failure to establish an SSH session:** CGSI3926> log view events INFO 2022-05-05 12:24:17.626347 cn-node-evtbroker Identity(chassis): Login failure event alert for ciena from 10.1.5.209:58868 WARN 2022-05-05 12:24:20.305971 cn-node-evtbroker Identity(chassis): Authentication failure for user 'ciena' from IP 10.1.5.209

			INFO 2022-05-05 12:24:26.836712 cn-node-evtbroker Identity(chassis): Login failure event alert for ciena from 10.1.5.209:58868 WARN 2022-05-05 12:24:28.416982 cn-node-evtbroker Identity(chassis): Authentication failure for user 'ciena' from IP 10.1.5.209 INFO 2022-05-05 12:24:33.218918 cn-node-evtbroker Identity(chassis): Login failure event alert for ciena from 10.1.5.209:58868 WARN 2022-05-05 12:24:35.075562 cn-node-evtbroker Identity(chassis): Authentication failure for user 'ciena' from IP 10.1.5.209 CGSI3926> log view security INFO 2022-05-05 12:16:24.673560 useradd new user: name=ciena, UID=2002, GID=2000, home=/home/ciena, shell=/usr/local/bin/valcli, from=none INFO 2022-05-05 12:24:13.993526 sshd rekey out after 4294967296 blocks [preauth] INFO 2022-05-05 12:24:14.001418 sshd rekey in after 4294967296 blocks [preauth] NOTIF 2022-05-05 12:24:17.405346 sshd pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh:58868 ruser= rhost=10.1.5.209 user=ciena INFO 2022-05-05 12:24:20.299523 sshd Failed password for ciena from 10.1.5.209 port 58868 ssh2 INFO 2022-05-05 12:24:28.411227 sshd Failed password for ciena from 10.1.5.209 port 58868 ssh2 INFO 2022-05-05 12:24:35.069715 sshd Failed password for ciena from 10.1.5.209 port 58868 ssh2 INFO 2022-05-05 12:24:35.125860 sshd Connection closed by authenticating user ciena 10.1.5.209 port 58868 [preauth] NOTIF 2022-05-05 12:24:35.127876 sshd PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh:58868 ruser= rhost=10.1.5.209 user =ciena
FCS_TLSC_EXT.1	Failure to	Reason	**Failure to establish a TLS Session**

	Establish an TLS session	For failure	**FCS_TLSC_EXT.1.1 Test #4a** CGSI3926> log view events INFO 2023-12-15 07:53:33.872960 cn-node-evtbroker SYSLOGTLS begining connection. Client: :: Server: 10.1.5.209:6514 INFO 2023-12-15 07:53:33.922769 cn-node-evtbroker TLS Client Session Module : evtbroker, Message Type : Start, Date : 2023-12-15, Time: 07:53:33.841915, Session Key : 169.254.160.9:51693_10.1.5.209:6514 , Source IP : 169.254.160.9:51693 , Destination IP: 10.1.5.209:6514 INFO 2023-12-15 07:53:33.930526 cn-node-evtbroker SYSLOGTLS Error: src: '169.254.160.9' dst: '10.1.5.209' Error: 'TLS error during handshake : unknown cipher returned Certificate: 10.1.5.209 10.1.5.51' INFO 2023-12-15 07:53:33.937007 cn-node-evtbroker TLS Client Session Module : evtbroker, Message Type : Ended, Date : 2023-12-15, Time: 07:53:33.850251, Session Key : 169.254.160.9:51693_10.1.5.209:6514 , Reason : Normal CGSI3926> CGSI3926> log view security EMERG 2023-12-15 07:53:33.839827 cn-node-evtbroker SYSLOGTLS begining connection. Client: :: Server: 10.1.5.209:6514 NOTIF 2023-12-15 07:53:33.841915 cn-node-evtbroker TLS Session Client Start sessionkey = 169.254.160.9:51693_10.1.5.209:6514 | Source_IP_Port = 169.254.160.9:51693 | Destination_IP_Port = 10.1.5.209:6514 & EMERG 2023-12-15 07:53:33.848524 cn-node-evtbroker SYSLOGTLS Error: src: '169.254.160.9' dst: '10.1.5.209' Error: 'TLS error during handshake : unknown cipher returned Certificate: 10.1.5.209 10.1.5.51' NOTIF 2023-12-15 07:53:33.850251 cn-node-evtbroker TLS Session Client Ended sessionkey = 169.254.160.9:51693_10.1.5.209:6514 | Reason = Normal &

FIA_AFL.1	Unsuccessful Login attempts limit is met or exceeded	Origin of the attempt (e.g., IP address)	**Unsuccessful login attempts limit is met or exceeded.** INFO 2022-04-06 13:27:26.602293 cn-node-evtbroker Identity(chassis): Login failure event alert for test from 10.1.5.209:58776 WARN 2022-04-06 13:27:29.239211 cn-node-evtbroker Identity(chassis): Authentication failure for user 'test' from IP 10.1.5.209 INFO 2022-04-06 13:30:17.078281 cn-node-evtbroker Maximum authentication retry reached for user test as per lockout policy
FIA_PMG_EXT.1	None	None	NA
FIA_UIA_EXT.1	All use of Identification And Authentication mechanism	Origin of the attempt (e.g., IP address)	**Identification and Authentication mechanism.** **<u>Local Successful Login</u>** CGSI3926> log view events INFO 2022-04-07 10:28:04.934050 cn-node-evtbroker Identity(chassis): Login success event alert for diag from Local:ttyPS0 CGSI3926> log view security INFO 2022-04-07 10:27:56.680551 login pam_succeed_if(login:auth): requirement “tty =~ /dev/tty*” was met by user “diag” INFO 2022-04-07 10:28:05.066628 login pam_unix(login:session): session opened for user diag by diag(uid=0) **<u>Local Unsuccessful Login</u>** CGSI3926> log view events INFO 2022-04-07 10:21:35.715577 cn-node-evtbroker Identity(chassis): Login failure event alert for diag from Local:ttyPS0 CGSI3926> log view security INFO 2022-04-07 10:21:23.363613 login pam_unix(login:session): session closed for user diag INFO 2022-04-07 10:21:31.629584 login pam_succeed_if(login:auth):

			requirement "tty =~ /dev/tty*" was met by user "diag" NOTIF 2022-04-07 10:21:35.521857 login pam_unix(login:auth): authentication failure; logname=diag uid=0 euid=0 tty=/dev/ttyPS0 ruser= rhost= user=diag NOTIF 2022-04-07 10:21:38.290404 login FAILED LOGIN (1) on '/dev/ttyPS0' FOR 'diag', Authentication failure **Remote Successful Password-Based Login** CGSI3926> log view events INFO 2022-04-07 10:39:39.342553 cn-node-evtbroker Identity(chassis): Login success event alert for diag from 10.1.5.209:58784 INFO 2022-04-07 10:39:39.682209 cn-node-evtbroker Identity(chassis): Incoming connection from 10.1.5.209 : 58784 INFO 2022-04-07 10:39:39.693204 cn-node-evtbroker Identity(chassis): User successfully logged in from IP 10.1.5.209 user name 'diag' **Remote Unsuccessful Password-Based Login** CGSI3926> log view events INFO 2022-04-07 10:36:17.156206 cn-node-evtbroker Identity(chassis): Login failure event alert for diag from 10.1.5.209:58782 WARN 2022-04-07 10:36:19.411202 cn-node-evtbroker Identity(chassis): Authentication failure for user 'diag' from IP 10.1.5.209 INFO 2022-04-07 10:36:24.625033 cn-node-evtbroker Identity(chassis): Login failure event alert for diag from 10.1.5.209:58782 WARN 2022-04-07 10:36:26.331769 cn-node-

			evtbroker Identity(chassis): Authentication failure for user 'diag' from IP 10.1.5.209
FAU_UAU_EXT.2	All use of identification and authentication mechanism	Origin of the attempt (e.g., IP address)	**Identification and Authentication mechanism.** **Local Successful Login** CGSI3926> log view events INFO 2022-04-07 10:28:04.934050 cn-node- evtbroker Identity(chassis): Login success event alert for diag from Local:ttyPS0 CGSI3926> log view security INFO 2022-04-07 10:27:56.680551 login pam_succeed_if(login:auth): requirement “tty =~ /dev/tty*” was met by user “diag” INFO 2022-04-07 10:28:05.066628 login pam_unix(login:session): session opened for user diag by diag(uid=0) **Local Unsuccessful Login** CGSI3926> log view events INFO 2022-04-07 10:21:35.715577 cn-node-evtbroker Identity(chassis): Login failure event alert for diag from Local:ttyPS0 CGSI3926> log view security INFO 2022-04-07 10:21:23.363613 login pam_unix(login:session): session closed for user diag INFO 2022-04-07 10:21:31.629584 login pam_succeed_if(login:auth): requirement "tty =~ /dev/tty*" was met by user "diag" NOTIF 2022-04-07 10:21:35.521857 login pam_unix(login:auth): authentication failure; logname=diag uid=0 euid=0 tty=/dev/ttyPS0 ruser= rhost= user=diag NOTIF 2022-04-07 10:21:38.290404 login FAILED LOGIN (1) on '/dev/ttyPS0' FOR 'diag', Authentication failure

			Remote Successful Password-Based Login CGSI3926> log view events INFO 2022-04-07 10:39:39.342553 cn-node-evtbroker Identity(chassis): Login success event alert for diag from 10.1.5.209:58784 INFO 2022-04-07 10:39:39.682209 cn-node-evtbroker Identity(chassis): Incoming connection from 10.1.5.209 : 58784 INFO 2022-04-07 10:39:39.693204 cn-node-evtbroker Identity(chassis): User successfully logged in from IP 10.1.5.209 user name 'diag' **Remote Unsuccessful Password-Based Login** CGSI3926> log view events INFO 2022-04-07 10:36:17.156206 cn-node-evtbroker Identity(chassis): Login failure event alert for diag from 10.1.5.209:58782 WARN 2022-04-07 10:36:19.411202 cn-node-evtbroker Identity(chassis): Authentication failure for user 'diag' from IP 10.1.5.209 INFO 2022-04-07 10:36:24.625033 cn-node-evtbroker Identity(chassis): Login failure event alert for diag from 10.1.5.209:58782 WARN 2022-04-07 10:36:26.331769 cn-node-evtbroker Identity(chassis): Authentication failure for user 'diag' from IP 10.1.5.209
FIA_UAU.7	None	None	
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate	Reason For Failure of Certificate Validation	• **Unsuccessful attempt to validate a certificate.** INFO 2023-12-15 07:06:52.785016 cn-node-evtbroker SYSLOGTLS begining connection. Client: :: Server: 10.1.5.209:6514

	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	INFO 2023-12-15 07:06:52.826286 cn-node-evtbroker TLS Client Session Module : evtbroker, Message Type : Start, Date : 2023-12-15, Time: 07:06:52.707750, Session Key : 169.254.160.9:39405_10.1.5.209:6514 , Source IP : 169.254.160.9:39405 , Destination IP: 10.1.5.209:6514 INFO 2023-12-15 07:06:52.847069 cn-node-evtbroker SYSLOGTLS X.509 certificate verification fail - /C=US/O=Acumen/OU=CC/CN=10.1.5.209 Client: 169.254.160.9 Server: 10.1.5.209:6514 INFO 2023-12-15 07:06:52.869157 cn-node-evtbroker SYSLOGTLS Error: src: '169.254.160.9' dst: '10.1.5.209' Error: 'Certificate verification error : unsuitable certificate purpose Error #26 Certificate: 10.1.5.209 10.1.5.51' INFO 2023-12-15 07:06:52.890102 cn-node-evtbroker TLS Client Session Module : evtbroker, Message Type : Ended, Date : 2023-12-15, Time: 07:06:52.729233, Session Key : 169.254.160.9:39405_10.1.5.209:6514 , Reason : Normal • **Addition of certificate to trust anchors in the TOE's trust store.** INFO 2023-04-19 12:50:45.010281 cn-node-evtbroker User 'diag' successfully installed X.509 CA certificate with name ROOTCA2. Result: success • **Removal of certificate from the TOE's trust store** INFO 2023-04-19 12:51:01.420262 cn-node-evtbroker User 'diag' successfully uninstalled X.509 CA certificate with name ROOTCA2. Result: success
FIA_X509_EXT.2	None	None	
FMT_MOF.1/Functions	None	None	
FMT_MOF.1/Manual Update	Any attempt to initiate a manual update	None	• **Any attempt to initiate a manual update:** INFO 2024-01-18 09:07:59.623078 xgrade-ng Operation requested: {'operation':

			'install', 'options': {'manifest_url': 'https://10.1.5.210/saos-10-07-01-0289-RS12.yml', 'defer_activation': False, 'ca_directory': '/mnt/config/pkix/cert///hashed/', 'tls_config_file': '/mnt/config/pkix/secure/system/systemTls.cfg', 'passphrase': 'test', 'manifest_hash_algorithm': 'sha-256'}} INFO 2024-01-18 09:40:37.619020 xgrade-ng finished operation: {'operation': 'install', 'options': {'manifest_url': 'https://10.1.5.210/saos-10-07-01-0289-RS12.yml', 'defer_activation': False, 'ca_directory': '/mnt/config/pkix/cert///hashed/', 'tls_config_file': '/mnt/config/pkix/secure/system/systemTls.cfg', 'passphrase': 'test', 'manifest_hash_algorithm': 'sha-256', 'RTSC_required': None}, 'package_name': 'saos-10-07-01-0289-RS12', 'retries': 0, 'operation_timeout': 1375, 'latest_log': 'installing evernight-generic-arm-aarch64-01-07-01-0289-upgrade.sh on standby bank'}
FMT_MTD.1/CoreData	None	None	
FMT_MTD.1/CryptoKeys	None	None	
FMT_SMF.1	All Management activities of TSF data	None	• **Ability to administer the TOE locally and remotely.** **Local Console:** **Failed login attempt:** INFO 2022-04-07 10:21:35.715577 cn-node-evtbroker Identity(chassis): Login failure event alert for diag from Local:ttyPS0 CGSI3926> log view security INFO 2022-04-07 10:21:23.363613 login pam_unix(login:session): session closed for user diag INFO 2022-04-07 10:21:31.629584 login pam_succeed_if(login:auth): requirement "tty =~ /dev/tty*" was met by user "diag"

			NOTIF 2022-04-07 10:21:35.521857 login pam_unix(login:auth): authentication failure; logname=diag uid=0 euid=0 tty=/dev/ttyPS0 ruser= rhost= user=diag NOTIF 2022-04-07 10:21:38.290404 login FAILED LOGIN (1) on '/dev/ttyPS0' FOR 'diag', Authentication failure **Successful login attempt:** CGSI3926> log view events INFO 2022-04-07 10:39:39.342553 cn-node-evtbroker Identity(chassis): Login success event alert for diag from 10.1.5.209:58784 INFO 2022-04-07 10:39:39.682209 cn-node-evtbroker Identity(chassis): Incoming connection from 10.1.5.209 : 58784 INFO 2022-04-07 10:39:39.693204 cn-node-evtbroker Identity(chassis): User successfully logged in from IP 10.1.5.209 user name 'diag' **SSH:** **Failed login attempt:** INFO 2022-04-07 10:36:16.926551 sshd pam_succeed_if(sshd:auth): requirement "tty =~ /dev/tty*" not met by user "diag" NOTIF 2022-04-07 10:36:16.960806 sshd pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh:58782 ruser= rhost=10.1.5.209 user=diag INFO 2022-04-07 10:36:19.404714 sshd Failed password for diag from 10.1.5.209 port 58782 ssh2 INFO 2022-04-07 10:36:24.406870 sshd pam_succeed_if(sshd:auth): requirement "tty =~ /dev/tty*" not met by user "diag" INFO 2022-04-07 10:36:26.324536 sshd Failed password for diag from 10.1.5.209 port 58782 ssh2 **Successful login attempt:** INFO 2022-04-07 10:39:38.712940 sshd pam_succeed_if(sshd:auth): requirement "tty =~ /dev/tty*" not met by user "diag"

			INFO 2022-04-07 10:39:39.659076 sshd Accepted password for diag from 10.1.5.209 port 58784 ssh2 INFO 2022-04-07 10:39:39.686167 sshd pam_unix(sshd:session): session opened for user diag by (uid=0) • **Ability to configure the access banner.** CGSI3926> log view events NOTIF 2022-04-11 10:06:20.618900 cn-node-evtbroker Netconf(chassis): Session ID: 58; Username: diag; Client IP: 192.168.254.45; 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 and SSH session termination** CGSI3926> log view events NOTIF 2022-04-21 06:17:30.754755 cn-node-evtbroker Netconf(chassis): Session ID: 68; Username: diag; Client IP: 192.168.254.45; Target XPath: /oc-sys:system/oc-sys:ssh-server/oc-sys:config/oc-sys:timeout; Edit Operation: create NOTIF 2022-04-11 09:17:49.919692 cn-node-evtbroker Netconf(chassis): Session ID: 55; Username: diag; Client IP: 127.0.0.1; 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 [signature] capability prior to installing those updates.** INFO 2024-01-17 17:08:59.265626 xgrade-ng Operation requested: {'operation': 'install', 'options': {'manifest_url': 'https://10.1.5.210/saos-10-07-01-0289-RS12.yml', 'verify_signature': True,

			'defer_activation': False, 'ca_directory': '/mnt/config/pkix/cert///hashed/', 'tls_config_file': '/mnt/config/pkix/secure/system/systemTls.cfg', 'passphrase': 'test', 'manifest_hash_algorithm': 'sha-256'}} INFO 2024-01-17 17:09:11.455520 xgrade-ng Unscheduling pending operations: {'scheduler_state': [{'operation': 'activate', 'options': {'manifest_url': 'https://10.1.5.210/saos-10-07-01-0289-RS12.yml', 'verify_signature': True, 'defer_activation': False, 'ca_directory': '/mnt/config/pkix/cert///hashed/', 'tls_config_file': '/mnt/config/pkix/secure/system/systemTls.cfg', 'passphrase': 'test', 'manifest_hash_algorithm': 'sha-256'}, 'package_name': 'saos-10-07-01-0289-RS12', 'retries': 0}, {'operation': 'install', 'options': {'manifest_url': 'https://10.1.5.210/saos-10-07-01-0289-RS12.yml', 'verify_signature': True, 'defer_activation': False, 'ca_directory': '/mnt/config/pkix/cert///hashed/', 'tls_config_file': '/mnt/config/pkix/secure/system/systemTls.cfg', 'passphrase': 'test', 'manifest_hash_algorithm': 'sha-256'}, 'package_name': 'saos-10-07-01-0289-RS12', 'retries': 0}]} ERROR 2024-01-17 17:09:11.466465 xgrade-ng Invalid signing certificate: https://10.1.5.210/software-signing-cert.pem ERROR 2024-01-17 17:09:11.477016 cn-node-shwm xgrade operation failed: {"status": "error", "message": "Install failure", "code": 503, "data": {"software_state": "idle", "latest_log": "installing evernight-generic-arm-aarch64-01-07-01-0283-upgrade.sh on standby bank", "state_timeout": 0, "error_string": "Invalid signing certificate: https://10.1.5.210/software-signing-cert.pem"}}

			• **Ability to configure the authentication failure parameters for FIA_AFL.1** NOTIF 2023-04-18 11:28:47.262741 cn-node-evtbroker Netconf(chassis): Session ID: 132; Username: diag; Client IP: 192.168.228.50; Target XPath: /oc-sys:system/oc-sys:aaa/oc-sys:authentication/ciena-oc-aaa:lockout-policy; Edit Operation: create • **Ability to modify the behaviour of the transmission of audit data to an external IT entity.** NOTIF 2022-09-19 10:44:14.647039 cn-node-evtbroker Netconf(chassis): Session ID: 16; Username: diag; Client IP: 192.168.254.108; 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.** INFO 2024-01-11 13:54:59.733594 cn-node-evtbroker Identity(chassis): User Pubkey diag.pub is successfully changed by diag from 10.1.5.209 EMERG 2024-01-19 12:19:13.090235 netconfd-pro User Pubkey diag.pub is successfully deleted by diag from 192.168.254.140 • **Ability to configure thresholds for SSH rekeying.** NOTIF 2022-08-25 12:02:51.610315 cn-node-evtbroker Netconf(chassis): Session ID: 40; Username: diag; Client IP: 192.168.254.99; 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.**

			INFO 2022-04-18 09:06:43.297656 cn-node-evtbroker Identity(chassis): User successfully logged in from IP 10.1.5.209 user name 'diag' INFO 2022-04-18 09:15:00.144967 cn-node-evtbroker System(chassis): Clock change alert; configured-value: 2022-04-18T09:15:00Z • **Ability to configure NTP.** CGSI3926> log view events NOTIF 2024-03-29 07:29:30.848414 cn-node-evtbroker Netconf(chassis): Session ID: 11; Username: diag; Client IP: 192.168.254.140; Target XPath: /oc-sys:system/ciena-ntp:ntp/ciena-ntp:admin-state; Edit Operation: merge NOTIF 2024-03-29 07:30:24.400034 cn-node-evtbroker Netconf(chassis): Session ID: 11; Username: diag; Client IP: 192.168.254.140; Target XPath: /oc-sys:system/ciena-ntp:ntp/ciena-ntp:associations/ciena-ntp:remote-ntp-server/ciena-ntp:server-entry[ciena-ntp:address="10.1.5.209"]; Edit Operation: create • **Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors.** INFO 2023-04-19 12:50:45.010281 cn-node-evtbroker User 'diag' successfully installed X.509 CA certificate with name ROOTCA2. Result: success. INFO 2023-04-19 12:51:01.420262 cn-node-evtbroker User 'diag' successfully uninstalled X.509 CA certificate with name ROOTCA2. Result: success. • **Ability to manage the trusted public keys database.** INFO 2023-04-19 12:50:45.010281 cn-node-evtbroker User 'diag' successfully

			installed X.509 CA certificate with name ROOTCA2. Result: success INFO 2023-04-19 12:51:01.420262 cn-node-evtbroker User 'diag' successfully uninstalled X.509 CA certificate with name ROOTCA2. Result: success
FMT_SMR.2	None	None	
FPT_SKP_EXT.1	None	None	
FPT_APW_EXT.1	None	None	
FPT_TST_EXT.1	None	None	
FPT_STM_EXT.1	Discontinuous changes to time – either Administrator Actuated or changed via an automated process (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For Discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).	• **Discontinuous changes to time - Administrator actuated.** CGSI3926> log view events INFO 2022-04-18 09:06:42.781874 cn-node-evtbroker Identity(chassis): Login success event alert for diag from 10.1.5.209:58838 INFO 2022-04-18 09:06:43.290813 cn-node-evtbroker Identity(chassis): Incoming connection from 10.1.5.209 : 58838 INFO 2022-04-18 09:06:43.297656 cn-node-evtbroker Identity(chassis): User successfully logged in from IP 10.1.5.209 user name 'diag' INFO 2022-04-18 09:15:00.144967 cn-node-evtbroker System(chassis): Clock change alert; configured-value: 2022-04-18T09:15:00Z • **Discontinuous changes to time - changed via an automated process.** NOTIF 2022-04-18 13:41:05.742670 cn-node-evtbroker Netconf(chassis): Session ID: 65; Username: diag; Client IP: 192.168.254.45; Target XPath: /oc-sys:system/ciena-ntp:ntp/ciena-ntp:admin-state; Edit Operation: merge NOTIF 2022-04-18 13:41:38.099226 cn-node-evtbroker Netconf(chassis): Session ID: 65; Username: diag; Client IP: 192.168.254.45; Target XPath: /oc-sys:system/ciena-ntp:ntp/ciena-ntp:associations/ciena-ntp:remote-ntp-server/ciena-ntp:server-entry[ciena-ntp:address="10.1.5.209"]; Edit Operation: create

			INFO 2022-04-18 13:41:47.528098 cn-node-evtbroker Alarm_Manager(chassis): Alarm type:ntp-out-of-sync qualifier: being CLEARED for resource:/ciena-ntp:sync-status-change-notification with severity:Warning at time:2022-04-18T13:41:47.520262802Z
FPT_TUD_EXT.1	Initiation of Update, Result of the Update attempt (success or failure)	None	**Initiation of Update – Successful.** INFO 2024-01-18 09:07:59.623078 xgrade-ng Operation requested: {'operation': 'install', 'options': {'manifest_url': 'https://10.1.5.210/saos-10-07-01-0289-RS12.yml', 'defer_activation': False, 'ca_directory': '/mnt/config/pkix/cert///hashed/', 'tls_config_file': '/mnt/config/pkix/secure/system/systemTls.cfg', 'passphrase': 'test', 'manifest_hash_algorithm': 'sha-256'}} INFO 2024-01-18 09:40:37.619020 xgrade-ng finished operation: {'operation': 'install', 'options': {'manifest_url': 'https://10.1.5.210/saos-10-07-01-0289-RS12.yml', 'defer_activation': False, 'ca_directory': '/mnt/config/pkix/cert///hashed/', 'tls_config_file': '/mnt/config/pkix/secure/system/systemTls.cfg', 'passphrase': 'test', 'manifest_hash_algorithm': 'sha-256', 'RTSC_required': None}, 'package_name': 'saos-10-07-01-0289-RS12', 'retries': 0, 'operation_timeout': 1375, 'latest_log': 'installing evernight-generic-arm-aarch64-01-07-01-0289-upgrade.sh on standby bank'} **Initiation of Update – Failure.** INFO 2024-01-17 17:08:59.265626 xgrade-ng Operation requested: {'operation': 'install', 'options': {'manifest_url': 'https://10.1.5.210/saos-10-07-01-0289-RS12.yml', 'verify_signature': True, 'defer_activation': False, 'ca_directory':

			'/mnt/config/pkix/cert///hashed/', 'tls_config_file': '/mnt/config/pkix/secure/system/systemTls.cfg', 'passphrase': 'test', 'manifest_hash_algorithm': 'sha-256'}} ERROR 2024-01-17 17:09:11.477016 cn-node-shwm xgrade operation failed: {"status": "error", "message": "Install failure", "code": 503, "data": {"software_state": "idle", "latest_log": "installing evernight-generic-arm-aarch64-01-07-01-0283-upgrade.sh on standby bank", "state_timeout": 0, "error_string": "Invalid signing certificate: https://10.1.5.210/software-signing-cert.pem"}}
FTA_SSL.3	The Termination of a remote session by the session locking mechanism	None	**Termination of a remote session by the session locking mechanism** INFO 2022-04-21 06:17:59.865286 cn-node-evtbroker Identity(chassis): Login success event alert for diag from 10.1.5.209:58848 INFO 2022-04-21 06:18:00.359450 cn-node-evtbroker Identity(chassis): Incoming connection from 10.1.5.209 : 58848 INFO 2022-04-21 06:18:00.365956 cn-node-evtbroker Identity(chassis): User successfully logged in from IP 10.1.5.209 user name 'diag' INFO 2022-04-21 06:19:52.060120 cn-node-evtbroker Identity(chassis) sshd Session '10.1.5.209:58848' for User 'diag' authentication-method Local logged out due to inactivity
FTA_SSL.4	The Termination of an interactive session	None	**Termination of an interactive session LOCAL** CGSI3926> log view events INFO 2022-04-11 08:16:40.387547 cn-node-evtbroker Identity(chassis) login Session 'Local:ttyPS0' for User 'diag' authentication-method Local logged out CGSI3926> log view security INFO 2022-04-11 08:16:40.146181 login

			pam_unix(login:session): session closed for user diag **SSH** INFO 2022-04-11 08:49:58.772028 cn-node-evtbroker Identity(chassis) sshd Session '10.1.5.209:58828' for User 'diag' authentication-method Local logged out INFO 2022-04-11 08:49:58.530812 cn-node-evtbroker Identity(chassis): User logged out from IP 10.1.5.209 user name 'diag'
FTA_SSL_EXT.1	The Termination of a local session by the session locking mechanism	None	**Termination of a local session by the session locking mechanism** INFO 2022-04-07 14:09:56.525974 cn-node-evtbroker Identity(chassis) login Session 'Local:ttyS0' for User 'diag' authentication-method Local logged out due to inactvity INFO 2022-04-07 14:09:56.528171 cn-node-evtbroker Identity(chassis) sshd Session '10.1.5.207:43114' for User 'diag' authentication-method Local logged out due to inactvity INFO 2022-04-07 14:09:56.529884 cn-node-evtbroker Identity(chassis) sshd Session '192.168.254.209:21290' for User 'diag' 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 initiator and target of failed trusted channels establishment attempt	• **Initiation of the trusted channel** INFO 2024-01-24 13:03:47.125283 cn-node-evtbroker TLS Client Session Module : evtbroker, Message Type : Start, Date : 2024-01-24, Time: 13:03:46.871666, Session Key : 169.254.160.9:50777_10.1.5.209:6514 , Source IP : 169.254.160.9:50777 , Destination IP: 10.1.5.209:6514 INFO 2024-01-24 13:03:47.137652 cn-node-evtbroker SYSLOGTLS X.509 certificate verified - /C=US/O=Acumen/OU=CC/CN=10.1.5.209 Client: 169.254.160.9 Server: 10.1.5.209:6514

			INFO 2024-01-24 13:03:47.144029 cn-node-evtbroker SYSLOGTLS connection established. Client: 169.254.160.9 Server: 10.1.5.209:6514 • **Termination of the trusted channel** INFO 2024-01-24 13:19:34.968348 cn-node-evtbroker SYSLOGTLS connection closed normally. Client: 169.254.160.9 Server: 10.1.5.209:6514 • **Failure of the trusted channel** INFO 2024-01-24 13:25:28.592837 cn-node-evtbroker SYSLOGTLS connection closed unexpectedly. Client: 169.254.160.9 Server: 10.1.5.209:6514
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	None	• **Initiation of the trusted path** INFO 2023-04-20 09:39:55.294937 cn-node-evtbroker Identity(chassis): Login success event alert for diag from 10.1.5.209:59388 INFO 2023-04-20 09:39:55.483144 cn-node-evtbroker Identity(chassis): Incoming connection from 10.1.5.209 : 59388 INFO 2023-04-20 09:39:55.489954 cn-node-evtbroker Identity(chassis): User successfully logged in from IP 10.1.5.209 user name 'diag' • **Termination of the trusted path** INFO 2023-04-20 09:39:58.546855 cn-node-evtbroker Identity(chassis): **User logged out from IP 10.1.5.209 user name 'diag'** INFO 2023-04-20 09:39:58.818041 cn-node-evtbroker Identity(chassis) sshd Session '10.1.5.209:59388' for **User 'diag' authentication-method Local logged out** • **Failure of the trusted path functions.** INFO 2023-04-20 09:39:45.252976 cn-node-evtbroker Identity(chassis): **Login**

			failure event alert for diag from 10.1.5.209:59388 WARN 2023-04-20 09:39:47.307057 cn-node-evtbroker Identity(chassis**): Authentication failure for user 'diag' from IP 10.1.5.209**

Network Services and Protocols
The table below 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 29 - 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	No restrictions.
DNS	Domain Name Service	Yes	Yes	No	Yes	No restrictions.
FTP	File Transfer Protocol	Yes	Yes	No	No	No restrictions.
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

Service or Protocol	Description	Client (initiating)	Allowed	Server (terminating)	Allowed	Allowed use in the certified configuration
LDAP-over-SSL	LDAP over Secure Sockets Layer	Yes	No	No	No	Out of scope of the evaluation.
RADIUS	Remote Authentication Dial In 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 in 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.

14 Modes of Operation

Ciena's Service Aggregation Systems and Service Aware Operating System (SAOS) software are used to cost-effectively create simple and scalable networks. Network operators can realize new levels of speed, differentiation, operational scalability, and reliability.

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.
- 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)
- web-based graphical user interface (Web GUI) on 3948, 5130, 5131, 5132, 5144, 5162, 5164, 5166, 5168, 5170, 5171, 8110, and 8112

Software installation and upgrade

By default, SAOS software is installed by means of Ciena's Zero Touch Provisioning (ZTP). 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.

15 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.

15.1 Document Feedback

Ciena is committed to ensuring digital accessibility for people with disabilities. Ciena are 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.

15.2 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