Assurance Activities Report
for a Target of Evaluation

Ciena 8700 Packetwave Platform with SAOS 8.5

Security Target (Version 1.0)

Assurance Activities Report (AAR)
Version 1.0

6/8/2017

Evaluated by:

Booz | Allen | Hamilton

Booz Allen Hamilton Common Criteria Test Laboratory
NIAP Lab # 200423
304 Sentinel Drive, Suite 100
Annapolis Junction, MD 20701

Prepared for:
National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

The Developer of the TOE:
Ciena Corporation,
7035 Ridge Road,
Hanover, MD 21076 USA

The Author of the Security Target:
Booz Allen Hamilton,
304 Sentinel Drive,
Annapolis Junction, MD 20701 USA

The TOE Evaluation was sponsored by:
Ciena Corporation,
7035 Ridge Road,
Hanover, MD 21076 USA

Evaluation Personnel:
Christopher Gugel, CC Technical Director
David Cornwell
Justin Fisher
Bradley Isbell
Christopher Rakaczky

Applicable Common Criteria Version

Common Criteria for Information Technology Security Evaluation, September 2012 Version 3.1 Revision 4

Common Evaluation Methodology Version

Common Criteria for Information Technology Security Evaluation, Evaluation Methodology, September 2012 Version 3.1 Revision 4

Table of Contents

1 Purpose

The purpose of this document is to serve as a non-proprietary attestation that this evaluation has satisfied all of the TSS, AGD, and ATE Assurance Activities required by the Protection Profile to which the TOE claims exact conformance.

2 TOE Summary Specification Assurance Activities

The evaluation team completed the testing of the Security Target (ST) 'Ciena 8700 Packetwave Platform with SAOS 8.5 Security Target' and confirmed that the TOE Summary Specification (TSS) contains all Assurance Activities as specified by the 'Evaluation Activities for Network Device cPP Version 1.0' and has addressed all relevant NIAP Technical Decisions. The evaluators were able to individually examine each SFR's TSS statements and determine that they comprised sufficient information to address each SFR claimed by the TOE as well as meet the expectations of the NDcPP Assurance Activities.

Through the evaluation of ASE_TSS.1-1, described in the ETR, the evaluators were able to determine that each individual SFR was discussed in sufficient detail in the TSS to describe the SFR being met by the TSF in general. However, in some cases the Assurance Activities that are specified in the claimed source material instruct the evaluator to examine the TSS for a description of specific behavior to ensure that each SFR is described to an appropriate level of detail. The following is a list of each SFR, the TSS Assurance Activities specified for the SFR, and how the TSS meets the Assurance Activities. Additionally, each SFR is accompanied by the source material (NDcPP) that defines where the most up-to-date TSS Assurance Activity was defined.

Note that the Supporting Documents list some assurance activities by SFR component due to the large number of assurance activities that are associated with those SFRs. Where this was done, the evaluators have included the specific components that have relevant assurance activities associated with them. Those components that have no TSS assurance activities have been omitted (e.g. FCS_SSHS_EXT.1.1).

FAU_GEN.1 – This SFR does not contain any NDcPP TSS Assurance Activities.

FAU_GEN.2 – This SFR does not contain any NDcPP TSS Assurance Activities.

FAU_STG.1 – The Assurance Activity requires the TSS to describe the amount of audit data that are stored locally and how these records are protected against unauthorized modification or deletion. Section 8.1.3 of the ST identifies the amount of data that is stored for each log type and identifies the Super role as the only role that has authorization to delete audit data.

FAU_STG_EXT.1 – The NDcPP TSS Assurance Activities require the TSS to describe:
(1) the means by which audit data is transferred externally
(2) how the trusted channel is provided for this operation
(3) how much audit data is stored locally
(4) what happens in the event that local audit storage is exhausted
(5) how audit records are protected from unauthorized access
(6) consistency with the behavior described in FAU_STG_EXT.2 (conditional, only if FAU_STG_EXT.2 is claimed)
(7) what happens when the storage space for audit data is full
(8) when the option 'overwrite previous audit record' is selected this description should include
an outline of the rule for overwriting audit data.
(9) if 'other actions' are chosen such as sending the new audit data to an external IT entity, then the related behaviour of the TOE shall also be detailed in the TSS

This has all been described within the information mapped to FAU_STG_EXT.1 in Section 8.1.4 of the ST.
(1) Audit data is transmitted to an external audit server via secure syslog or SFTP, depending on the type of log data

(2) Remote audit data transmission is secured using TLS or SSH, depending on the log type
(3) When the current log file reaches its allowed maximum size, it is closed and renamed sequentially. The minimum and maximum number of records for each log file type is:

- Security Log: up to 4 historical files with up to 5,000 entries per file
- Event Log: up to 4 historical files with up to 10,000 entries per file
- Command Log: up to 5 historical files with up to 2,500 entries per file

(4) Log rotation is employed such that when audit storage is exhausted for a particular type, the oldest log file of that type is deleted if the maximum number of log files for that type already exist.
(5) Audit records are protected from unauthorized access by only granting users with the Super role modify/delete privileges to the audit data. Users with the Admin and Limited roles can view each of the log types (security, event and command).
(6) This is not applicable because FAU_STG_EXT.2 is not claimed.
(7) When audit storage is full, the oldest log file of that type is deleted.
(8) When the current log file reaches its allowed maximum size, it is closed, renamed and a new log file is opened.
(9) This is not applicable because ‘other actions’ is not selected.

FCS_CKM.1 – The Assurance Activity requires the TSS to identify the key sizes and usage of each scheme supported by the TOE. The TSS states in section 8.2.1 that the RSA is supported with a key size of 2048 bits. The TSS also states that Elliptic Curve Diffie-Hellman (ECDH) is supported with key sizes of 256, 384 and 521 bits. The TSS states that ECDH is used in SSH and TLS and RSA is used in TLS. The corresponding CAVP certificates for FIPS 186-4 key generation are #2445 (RSA) and #1092 (ECDSA).

FCS_CKM.2 – The Assurance Activity requires the TSS to verify that supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1. The TOE claims RSA and Elliptic Curve Diffie-Hellman (ECDH) key establishment schemes, which is consistent with the claims made in FCS_CKM.1.1. ECDH schemes are conformant to SP 800-56A and RSA scheme is conformant to SP 800-56B. This is documented in section 8.2.2 of the ST. The corresponding CAVP KAS ECC certificate is #120. Note that RSA conformance to SP 800-56B is vendor affirmed as per the NIAP Policy Letter #5 CAVP mapping guidance.

FCS_CKM.4 – The Assurance Activity requires the TSS to list the plaintext key material stored on the TOE, its origin, and its storage location. The NDcPP also requires the TSS to document, for each type of key material, when it is destroyed and how the destruction is performed for each memory type. The TSS includes a table that contains the relevant information in section 8.2.3. All keys are overwritten with zeros with a read verify operation.

FCS_COP.1(1) – This SFR does not contain any NDcPP TSS Assurance Activities.

FCS_COP.1(2) – This SFR does not contain any NDcPP TSS Assurance Activities.

FCS_COP.1(3) – The Assurance Activity requires the TSS to describe the association of the hash function with any other TSF cryptographic functions. Section 8.2.6 of the ST states that SHA-1, SHA-256, SHA-384 and SHA-512 are used by the TOE. The following details which hash functions are used for which method:

- SHA-1, SHA-256, and SHA-512 for SSH data integrity
- SHA-256 for software integrity
- SHA-1, SHA-256, and SHA-384 for TLS
- SHA-512 for password hashing

SHA has CAVP certificate #3682.

FCS_COP.1(4) – The Assurance Activity requires the TSS to describe the key length, hash function, block size, and output MAC length used by the HMAC function. Section 8.2.7 of the TSS specifies that HMAC-SHA-1, HMAC-SHA-256, and HMAC-SHA-512 are used by the TSF and that all possible key and block lengths are supported. The supported MAC sizes are:
HMAC-SHA-1: 10, 12, 16, 20 bytes

HMAC-SHA_256: 16, 24, 32 bytes
HMAC-SHA-512: 32, 40, 48, 56, 64 bytes
HMAC has CAVP certificate #2967.

FCS_RBG_EXT.1 – This SFR does not contain any NDcPP TSS Assurance Activities.

FCS_SSHC_EXT.1.2 – The Assurance Activity requires the TSF to describe the public key algorithms that are acceptable for SSH authentication that this list conforms to FCS_SSHC_EXT.1.5, and that password-based methods are allowed. The TSS indicates in section 8.2.9 that both password and public key authentication are supported by the TOE, and that both RSA and ECDSA are supported which is conformant to FCS_SSHC_EXT.1.5.

FCS_SSHC_EXT.1.3 – The Assurance Activity requires the TSF to describe how "large packets" are detected and handled. The TSS states in section 8.2.9 that all large packets in an SSH connection are detected and if they are larger than 32,768 bytes they are dropped.

FCS_SSHC_EXT.1.4 – The Assurance Activity requires the TSF to describe any optional characteristics of the SSH transport implementation and the encryption algorithms that are used for the transport implementation such that they are consistent with the SFR definition. The TSS indicates in section 8.2.9 that the TOE supports AES in both CBC and GCM modes and with both 128 and 256 bit key sizes for its encryption algorithms which is consistent with the SFR definition.

FCS_SSHC_EXT.1.5 – The Assurance Activity requires the TSF to describe the SSH transport implementation, ensuring that optional characteristics are specified and that the public key algorithms that are supported are specified as well. The NDcPP also requires that the TSF describe public key algorithms which are consistent with the SFR definition. Section 8.2.9 of the TSS indicates that for public key algorithm the TOE uses ssh-rsa, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, which is consistent with the SFR definition.

FCS_SSHC_EXT.1.6 – The Assurance Activity requires the TSF to list the supported data integrity algorithms consistent with the SFR definition. The SFR and TSS (section 8.2.9) both specify that hmac-sha1, hmac-sha1-96, hmac-sha2-256, and hmac-sha2-512 are the supported integrity algorithms which is consistent with the SFR definition.

FCS_SSHC_EXT.1.7 – The Assurance Activity requires the TSF to list the supported key exchange algorithms consistent with the SFR definition. Section 8.2.9 of the TSS that ecdh-sha2-nistp256 is the only key exchange method used by the SSH client implementation, consistent with the SFR.

FCS_SSHC_EXT.1.8 – As per NIAP TD0167, the Assurance Activity for this SFR requires the TSF to describe that both packet-based and time-based rekey thresholds can be applied. The TSS states that both types of rekey thresholds are supported and provides the ranges of acceptable values for each.

FCS_SSHC_EXT.1.9 – This SFR does not contain any NDcPP TSS Assurance Activities.

FCS_SSHS_EXT.1.1 – This SFR does not contain any NDcPP TSS Assurance Activities.

FCS_SSHS_EXT.1.2 – The Assurance Activity requires the TSF to describe the public key algorithms that are acceptable for SSH authentication that this list conforms to FCS_SSHS_EXT.1.5, and that password-based methods are allowed. The TSS indicates in section 8.2.9 that both password and public key authentication are supported by the TOE, and that both RSA and ECDSA are supported which is conformant to FCS_SSHS_EXT.1.5.

FCS_SSHS_EXT.1.3 – The Assurance Activity requires the TSF to describe how "large packets" are detected and handled. The TSS states in section 8.2.9 that all large packets in an SSH connection are detected and if they are larger than 32,768 bytes they are dropped.

FCS_SSHS_EXT.1.4 – The Assurance Activity requires the TSF to describe any optional characteristics of the SSH transport implementation and the encryption algorithms that are used for the transport implementation such that they are consistent with the SFR definition. The TSS indicates in section 8.2.9 that the TOE supports AES in both CBC and GCM modes and with both 128 and 256 bit key sizes for its encryption algorithms which is consistent with the SFR definition.

FCS_SSHS_EXT.1.5 – The Assurance Activity requires the TSF to describe the SSH transport implementation, ensuring that optional characteristics are specified and that the public key algorithms that are supported are specified as well. The NDcPP also requires that the TSF describe public key algorithms which are consistent with the SFR definition. Section 8.2.9 of the TSS indicates that for public key algorithm the TOE uses ssh-rsa, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, which is consistent with the SFR definition.

FCS_SSHS_EXT.1.6 – The Assurance Activity requires the TSF to list the supported data integrity algorithms consistent with the SFR definition. The SFR and TSS (section 8.2.9) both specify that hmac-sha1, hmac-sha2-256, and hmac-sha2-512 are the supported integrity algorithms which is consistent with the SFR definition.

FCS_SSHS_EXT.1.7 – The Assurance Activity requires the TSF to list the supported key exchange algorithms consistent with the SFR definition. Section 8.2.9 of the TSS states that the SSH server implementation supports any of ecdh-sha2-nistp256, ecdh-sha2-nistp384, and ecdh-sha2-nistp521 for its methods of key exchange which is consistent with the SFR definition.

FCS_TLSC_EXT.2.1 – The Assurance Activity requires the TSF describe the implementation of TLS to ensure that the ciphersuites that are supported are specified and are consistent with the SFR definition. Section 8.2.10 of the TSS lists the fourteen ciphersuites that are supported by the TOE's TLS client implementation, consistent with the SFR. The TSS also indicates that both TLS 1.1 and 1.2 are supported.

FCS_TLSC_EXT.2.2 – The Assurance Activity requires the TSF describe the client's method of establishing all reference identifiers from the administrator/application-configured reference identifier in addition to the types of reference identifiers that are supported. TSF is also required to describe whether IP address and wildcards are supported as well as whether or not certificate pinning is supported or used by the TOE and the manner in which this is accomplished. Section 8.2.10 of the TSS states that the TOE can use CN or SAN for the reference identifier, and that the SAN can be DNS name or IP address. The ST also indicates that wild cards in the hostname are supported and certificate pinning is not supported.

FCS_TLSC_EXT.2.3 – This SFR does not contain any NDcPP TSS Assurance Activities.

FCS_TLSC_EXT.2.4 – The Assurance Activity requires the TSF describe the Supported Elliptic Curves Extension and whether the required behavior is performed by default or may be configured. The TSS states that the Elliptic Curves Extension is supported by NIST curves secp256r1, secp384r1 and secp521r1 and that this is configured.

FCS_TLSC_EXT.2.5 – The Assurance Activity requires the TSF describe use of client-side certificates for TLS mutual authentication. Section 8.2.10 of the TSS indicates that the TSF uses X.509v3 certificates for the syslog server and RADIUS server communications, and that mutual authentication is supported for each.

FIA_PMG_EXT.1 – This SFR does not contain any NDcPP TSS Assurance Activities.

FIA_UIA_EXT.1 – The Assurance Activity requires the TSF to describe the authentication methods supported by the TOE along with the credentials and protocols used. Section 8.3.4 of the ST states that both remote and local access are supported. Local access is granted via the serial CLI, and remote access is granted via the CLI using SSH. Both username and password are supported for each method, and the credentials can be defined either locally on the TOE or remotely on a RADIUS server. Remote SSH access also supports SSH public key authentication.

FIA_UAU_EXT.2 – This SFR does not contain any NDcPP TSS Assurance Activities.

FIA_UAU.7 – This SFR does not contain any NDcPP TSS Assurance Activities.

FIA_X509_EXT.1 – The Assurance Activity requires the TSF describe where the check for valid certificates takes place as well as the certificate path validation algorithm. Section 8.3.5 of the ST states that certificates are checked for validity in several cases: signed software updates, mutual authentication with the remote syslog server or RADIUS server. The TSS also states that if OCSP cannot authenticate a certificate, the certificate will be rejected. The TSS also describes certificate validity checking and path validation in a manner that is consistent with the SFR, notably specifying that OCSP is used to obtain the certificate revocation status. Additionally, NIAP TD0117 requires the TSS to state when validity and revocation checking is performed. The ST indicates that certificates are checked during authentication for TLS and, depending on the ciphersuites used, for SSH.

FIA_X509_EXT.2 – The Assurance Activity requires the TSS to describe how the TOE chooses which certificates to use and any necessary conditions in the administrative guidance for configuring the operational environment so that the TOE can use these certificates. Also, that the TOE behavior is described when a connection cannot be established during the validity check of a certificate used in establishing a trusted channel. The TSS states that TOE chooses which certificate to use based upon the basicConstraints extension, the CA flag and the value of the extendedKeyUsage field. Also, the TSS states that if OCSP cannot authenticate a certificate the certificate will be rejected.

FIA_X509_EXT.3 – The Assurance Activity requires the TSS to describe the device-specific information used in certificate requests if the corresponding selection is made in FIA_X509_EXT.3.1. Since this selection was not made in the ST, no additional information is required.

FMT_MOF.1(1)/Audit – This SFR does not contain any NDcPP TSS Assurance Activities.

FMT_MOF.1(1)/TrustedUpdate – This SFR does not contain any NDcPP TSS Assurance Activities.

FMT_MTD.1 – The Assurance Activity requires the TSS to identify all administrator functions that are accessible through an interface prior to administrator log-in are identified, and how the ability to manipulate TSF data is disallowed for non-administrative users via these interfaces. Section 8.4.5 states that the only function that can be performed by the TOE prior to administrator authentication is the display of the warning banner. The TSS also describes the different administrative roles that can be assumed.

FMT_MTD.1/AdminAct – This SFR does not contain any NDcPP TSS Assurance Activities.

FMT_SMF.1 – This SFR does not contain any NDcPP TSS Assurance Activities.

FMT_SMR.2 – This SFR does not contain any NDcPP TSS Assurance Activities.

FPT_SKP_EXT.1 – The Assurance Activity requires the TSS to detail how pre-shared keys, symmetric keys, and private keys are stored such that they're unable to be viewed. The TSS is also required to detail which values are not stored in plaintext and they these values are protected/obscured. Section 8.5.2 of the ST states that the TOE does not provide a mechanism to view pre-shared keys, symmetric keys and private keys. Public key data that is stored on the TOE can be viewed by an authorized administrator with Admin or Super roles. Key data that is resident in volatile memory cannot be accessed by administrators.

FPT_APW_EXT.1 – The Assurance Activity requires the TSS to detail all of the authentication data that is subject to this requirement and the method used to obscure the password plaintext data. The TSS is also required to assert that passwords are stored in such a way that there is no interface designed for the purpose of viewing this data. Section 8.5.1 indicates that password data is hashed using SHA-512 and it is this value that is stored by the TOE. The optional capability to provide an encrypted the password is provided via the "secret" command when creating or editing the user's password.

FPT_TST_EXT.1 – The Assurance Activity requires the TSS to detail the self-tests that are run by the TSF on start-up; this description should include an outline of what the tests are doing and makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly. Section 8.5.4 of the ST lists software integrity, cryptographic module integrity, and hardware integrity as the power-on self tests that are performed. All self-tests result in an automatic reboot of the TOE upon failure. These tests and their response to failures is sufficient to ensure that the TSF behaves as described in the ST because it would detect any unauthorized modifications to the TOE, failures or tampering of the hardware (which could be an attempt to compromise its storage or take the TOE out of the range of operating conditions specified for its entropy source), and any cryptographic failures that could result in the establishment of insecure trusted channels.

FPT_TUD_EXT.1 – The Assurance Activity requires the TSS to specify how updates are obtained, verified, and rejected in the event of a failure. Section 8.5.5 of the TSS specifies that an authorized administrator can view software/firmware version information. Software updates are retrieved from an SFTP update server. The validation process is performed automatically when the update attempt is initiated; if successful, the update proceeds without administrator intervention. In the event of a failure, the update is aborted and the invalid update is automatically erased from storage (administrators do not have direct access to the file system). Additionally, since the TOE provides a delayed activation ability for software/firmware updates NIAP TD0154 requires the ST to state how the delayed activation occurs. The TSS indicates that the newly-installed update will take effect following a reboot of the TOE.

FPT_STM.1 – The Assurance Activity requires the TSS to list each security function that makes use of time and a description of how time is maintained and considered to be reliable. Section 8.5.3 states that the TOE maintains its own. The TSS also specifies that the TSF uses the clock for timestamp of audit records, X.509 certificate validation (for expired/not-yet-valid certificates), administrator session inactivity, and RADIUS timeout.

FTA_SSL_EXT.1 – This SFR does not contain any NDcPP TSS Assurance Activities.

FTA_SSL.3 – This SFR does not contain any NDcPP TSS Assurance Activities.

FTA_SSL.4 – This SFR does not contain any NDcPP TSS Assurance Activities.

FTA_TAB.1 – The Assurance Activity requires the TSS to detail each method of access (local and remote) available to the administrator. Section 8.6.4 states that local CLI and remote CLI are the two ways of logging in to the TOE and that both display configurable access banners pre-authentication.

FTP_ITC.1 – The Assurance Activity requires the TSS to describe that, for all communications with authorized IT entities, each mechanism is identified in terms of the allowed protocols, and that these protocols are consistent with the SFR. Section 8.7.1 of the ST states that The TOE uses SSH (SFTP) for the transfer of software updates and security/event/command log data and TLS for RADIUS server communications and remote transmission of syslog records.

FTP_TRP.1 – The Assurance Activity requires the TSS to describe the methods of remote TOE administration and how these communications are protected, such that they are consistent with the protocols defined elsewhere in the ST. Section 8.7.2 of the TSS indicates that SSH conformant to FCS_SSHS_EXT.1 is the only method used to secure remote administration, which is always performed using the remote CLI.

3 Operational Guidance Assurance Activities

The evaluation team completed the testing of the Operational Guidance, which includes the review of the "*Ciena 8700 Packetwave Platform with SAOS 8.5 Supplemental Administrative Guidance"* (AGD) document, and confirmed that the Operational Guidance contains all Assurance Activities as specified by the 'collaborative Protection Profile for Network Devices Version 1.0' (NDcPP). The evaluators reviewed the NDcPP to identify the security functionality that must be discussed for the operational guidance. This is prescribed by the Assurance Activities for each SFR and the AGD SARs. The evaluators have listed below each of the SFRs defined in the NDcPP that have been claimed by the TOE (some SFRs are conditional or optional) as well as the AGD SAR, along with a discussion of where in the operational guidance the associated Assurance Activities material can be found. The AGD includes references to other guidance documents that must be used to properly install, configure, and operate the TOE in its evaluated configuration. The AGD and its references to other Ciena 8700 Packetwave Platform guidance documents were reviewed to assess the Operational Guidance Assurance Activities. The AGD contains references to these documents in Chapter 4 and these references can also be found below:

If an SFR is not listed, one of the following conditions applies:

- There is no Assurance Activity for the SFR.
- The Assurance Activity for the SFR specifically indicates that it is simultaneously satisfied by completing a different Assurance Activity (a testing Assurance Activity for the same SFR, a testing Assurance Activity for a different SFR, or a guidance Assurance Activity for another SFR).
- The Assurance Activity for the SFR does not specify any actions to review the operational guidance.

FAU_GEN.1 –
"The evaluator shall check the guidance documentation and ensure that it lists all of the auditable events and provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field. The evaluator shall check to make sure that every audit event type mandated by the cPP is described and that the description of the fields contains the information required in FAU_GEN1.2, and the additional information specified in the table of audit events."

The evaluator observed that section 8 of the supplemental AGD lists the auditable events that are relevant to the TSF, the different locations in which those events are recorded (syslog, security log, command log, event log), and sample audit records for those events. The evaluators also observed that for events that have multiple potential causes (e.g. failure to establish an SSH session), the supplemental AGD includes examples of different types of causes (e.g. no cipher match, no MAC match, no host key type match, no key exchange method match).

"The evaluator shall also make a determination of the administrative actions that are relevant in the context of the cPP. The evaluator shall examine the guidance documentation and make a determination of which administrative commands, including subcommands, scripts, and configuration files, are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the cPP. The evaluator shall document the methodology or approach taken while determining which actions in the administrative guide are security relevant with respect to the cPP. The evaluator may perform this activity as part of the activities associated with ensuring that the corresponding guidance documentation satisfies the requirements related to it."

The evaluators reviewed the supplemental AGD and observed that it contains a number of commands for managing the TSF, organized by configuration or management activity. The evaluators examined the ST to determine the functional behavior performed by the TOE and considered what management functionality would need to be present in order to administer that behavior. The evaluators observed that the auditable events defined in FAU_GEN.1 provided general coverage of this functionality but observed that the list of auditable events in the AGD also added password reset for management of user authentication data. The evaluators also observed that the sample data for 'all management activities of the TSF' includes enabling and configuring the system inactivity timer (FTA_SSL_EXT.1, FTA_SSL.3), configuration of banner text (FTA_TAB.1), and installation of X.509 certificates for SSH (FIA_UIA_EXT.1).

FAU_GEN.2 – This SFR does not contain any NDcPP AGD Assurance Activities.

FAU_STG.1 – *"The evaluator shall examine the guidance documentation to determine that it describes any configuration required for protection of the locally stored audit data against unauthorized modification or deletion."*

The evaluators observed that section 6.1 of the supplemental AGD states that by default, only the Super role has permission to delete stored audit data.

FAU_STG_EXT.1 –
"The evaluator shall also examine the guidance documentation to ensure it describes how to establish the trusted channel to the audit server, as well as describe any requirements on the audit server (particular audit server protocol, version of the protocol required, etc.), as well as configuration of the TOE needed to communicate with the audit server."

The evaluators observed that the TOE has two interfaces for remote audit storage: SFTP (SSH) and syslog (over TLS). The evaluators identified section 6.3 in the supplemental AGD as describing how to set up the SFTP client and a periodic transfer of audit data to it, including the stipulation that there is no specific version of SFTP that is required for the server in order to use this. Section 6.6 identifies the specific SSH algorithms that must be used in order to transmit this data in accordance with the evaluated configuration. For syslog, section 6.4 describes how to set up syslog while section 6.7 stipulates that TLS version 1.1 or higher must be used and specifies the ciphersuites and elliptic curves that are required for this to be used in accordance with the evaluated configuration.

"The evaluator shall also examine the guidance documentation to determine that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. For example, when an audit event is generated, is it simultaneously sent to the external server and the local store, or is the local store used as a buffer and "cleared" periodically by sending the data to the audit server."

The evaluators identified that section 6.1 of the AGD states that security, event, and command log data are persistently stored on the TOE and that section 6.3 states that the audit data transferred is a duplicate of the local copy. This means that a communications outage with the SFTP server will not result in a loss of audit data because the entire locally-stored audit trail is transmitted each time the TOE communicates with that server. The evaluators also observed that section 6.4 describes the behavior of the syslog interface and states that syslog audit data can be lost in the event of a communicates outage because syslog is a streaming interface.

"The evaluator shall also ensure that the guidance documentation describes all possible configuration options for FAU_STG_EXT.1.3 and the resulting behaviour of the TOE for each possible configuration. The description of possible configuration options and resulting behaviour shall correspond to those described in the TSS"

The evaluators observed that section 6.1 of the supplemental AGD describes the behavior of the TOE when local audit storage space is exhausted (non-configurable log rotation, fixed maximum number of entries per log file) in a manner that is consistent with the ST.

FCS_CKM.1
"The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected key generation scheme(s) and key size(s) for all uses defined in this PP."

Section 6.5 of the supplemental AGD describes how to enable FIPS mode for the TOE. Sections 6.6 and 6.7 further instruct the administrator to limit the SSH and TLS connection details to those algorithms defined in the ST. This ensures that the key generation is performed in an appropriate manner.

FCS_CKM.2
"The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected key establishment scheme(s)."

Sections 6.6 and 6.7 of the supplemental AGD list the SSH key exchange methods and TLS ciphersuites that must be used in the evaluated configuration. These sections also provide guidance on how to specify these.

FCS_CKM.4 – This SFR does not contain any NDcPP AGD Assurance Activities.

FCS_COP.1(1) – This SFR does not contain any NDcPP AGD Assurance Activities.

FCS_COP.1(2) – This SFR does not contain any NDcPP AGD Assurance Activities.

FCS_COP.1(3)
"The evaluator checks the AGD documents to determine that any configuration that is required to configure the required hash sizes is present"

Sections 6.6 and 6.7 of the supplemental AGD list the SSH integrity algorithms and TLS ciphersuites that must be used in the evaluated configuration. These sections also provide guidance on how to specify these.

FCS_COP.1(4) – This SFR does not contain any NDcPP AGD Assurance Activities.

FCS_RBG_EXT.1 – This SFR does not contain any NDcPP AGD Assurance Activities.

FCS_SSHC_EXT.1.4
"The evaluator shall also check the guidance documentation to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements)."

Section 6.6 of the supplemental AGD lists the encryption algorithms required for SSH in the evaluated configuration and provides sample syntax for how to configure this.

FCS_SSHC_EXT.1.5
"The evaluator shall also check the guidance documentation to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements)."

Section 6.6 of the supplemental AGD lists the public key authentication methods supported for SSH in the evaluated configuration and provides sample syntax for how to configure this.

FCS_SSHC_EXT.1.6
"*The evaluator shall also check the guidance documentation to ensure that it contains instructions to the administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE (specifically, that the "none" MAC algorithm is not allowed)."*

Section 6.6 of the supplemental AGD lists the data integrity algorithms supported for SSH in the evaluated configuration and provides sample syntax for how to configure this.

FCS_SSHC_EXT.1.7
"The evaluator shall also check the guidance documentation to ensure that it contains instructions to the administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections with the TOE."

Section 6.6 of the supplemental AGD lists the key exchange methods supported for SSH in the evaluated configuration and provides sample syntax for how to configure this.

FCS_SSHS_EXT.1.4

"The evaluator shall also check the guidance documentation to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements)."

Section 6.6 of the supplemental AGD lists the encryption algorithms required for SSH in the evaluated configuration and provides sample syntax for how to configure this.

FCS_SSHS_EXT.1.5
"The evaluator shall also check the guidance documentation to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements)."

Section 6.6 of the supplemental AGD lists the public key authentication methods supported for SSH in the evaluated configuration and provides sample syntax for how to configure this.

FCS_SSHS_EXT.1.6
"*The evaluator shall also check the guidance documentation to ensure that it contains instructions to the administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE (specifically, that the "none" MAC algorithm is not allowed)."*

Section 6.6 of the supplemental AGD lists the data integrity algorithms supported for SSH in the evaluated configuration and provides sample syntax for how to configure this.

FCS_SSHS_EXT.1.7
"The evaluator shall also check the guidance documentation to ensure that it contains instructions to the administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections with the TOE."

Section 6.6 of the supplemental AGD lists the key exchange methods supported for SSH in the evaluated configuration and provides sample syntax for how to configure this.

FCS_TLSC_EXT.2.1
"The evaluator shall also check the guidance documentation to ensure that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS."

Section 6.7 of the supplemental AGD provides instructions for configuring TLS and includes the list of supported TLS versions and ciphersuites that must be used in the evaluated configuration.

FCS_TLSC_EXT.2.2
"The evaluator shall verify that the AGD guidance includes instructions for setting the reference identifier to be used for the purposes of certificate validation in TLS"

Section 6.7 of the supplemental AGD cites materials in the existing vendor guidance on how to set reference identifiers used for TLS certificate validation.

FCS_TLSC_EXT.2.4
"If the TSS indicates that the Supported Elliptic Curves Extension must be configured to meet the requirement, the evaluator shall verify that AGD guidance includes configuration of the Supported Elliptic Curves Extension"

Section 6.7 of the supplemental AGD provides instructions for configuring TLS and includes the list of supported elliptic curves that must be used in the evaluated configuration.

FCS_TLSC_EXT.2.5
"The evaluator shall verify that the AGD guidance required per FIA_X509_EXT.2.1 includes instructions for configuring the client-side certificates for TLS mutual authentication"

Sections 6.4 (syslog) and 6.9 (RADIUS) of the supplemental AGD provide guidance on how to set up TLS mutual authentication for the two TOE interfaces that use this protocol.

FIA_PMG_EXT.1 –
"The evaluator shall examine the guidance documentation to determine that it provides guidance to security administrators on the composition of strong passwords, and that it provides instructions on setting the minimum password length."

Section 7.4 of the supplemental AGD lists the supported character sets for passwords and provides general guidance on the composition of strong passwords. It also species 15 as the floor for minimum password length and identifies the administrative command used to enforce this.

FIA_UAU.7 – This SFR does not contain any NDcPP AGD Assurance Activities.

FIA_UAU_EXT.2 – This SFR does not contain any NDcPP AGD Assurance Activities.

FIA_UIA_EXT.1
"The evaluator shall examine the guidance documentation to determine that any necessary preparatory steps (e.g., establishing credential material such as pre- shared keys, tunnels, certificates, etc.) to logging in are described."

Section 6.2 of the supplemental AGD describes the preparatory steps for enabling SSH authentication through the various methods that are supported by the TOE. If RADIUS is desired as a user authentication method, section 6.9 of the supplemental AGD describes how to configure it.

For each supported the login method, the evaluator shall ensure the guidance documentation provides clear instructions for successfully logging on.

Section 7.1 of the supplemental AGD provides instructions and documentation reference to how to authenticate to the CLI locally and remotely.

If configuration is necessary to ensure the services provided before login are limited, the evaluator shall determine that the guidance documentation provides sufficient instruction on limiting the allowed services."

This is N/A because no services are provided prior to login other than display of the warning banner.

FIA_X509_EXT.1 – This SFR does not contain any NDcPP AGD Assurance Activities.

FIA_X509_EXT.2 – This SFR does not contain any NDcPP AGD Assurance Activities.

FIA_X509_EXT.3
"The evaluator shall check to ensure that the guidance documentation contains instructions on requesting certificates from a CA, including generation of a Certificate Request Message. If the ST author selects "Common Name", "Organization", "Organizational Unit", or "Country", the evaluator shall ensure that this guidance includes instructions for establishing these fields before creating the certificate request message"

Sections 6.2, 6.4, and 6.9 of the supplemental AGD include the generation of a Certificate Request Message as part of establishing communications that use X.509. Section 6.9 in particular demonstrates the establishment of various Distinguished Name elements prior to the generation of the CSR.

FMT_MOF.1(1)/Audit – This SFR does not contain any NDcPP AGD Assurance Activities.

FMT_MOF.1/Locspace – This SFR does not contain any NDcPP AGD Assurance Activities.

FMT_MOF.1(1)/TrustedUpdate – This SFR does not contain any NDcPP AGD Assurance Activities.

FMT_MTD.1
"The evaluator shall review the guidance documentation to determine that each of the TSF-data-manipulating functions implemented in response to the requirements of the cPP is identified, and that configuration information is provided to ensure that only administrators have access to the functions."

The entirety of the supplemental AGD identifies the TSF-data-manipulating functions that are available to administrators. Section 7.1 provides information about the three administrative roles of the TOE as well as a summary of the privileges available to them. The list privileges assigned to each role is not configurable. According to section 2, the supplemental AGD is designed to be read by an administrator who is already familiar with the Ciena 8700 product. It is therefore reasonable to expect that the reader is familiar with the general administration of the product and that the supplemental AGD simply narrows the reader's focus to the functionality described in the ST.

FMT_MTD.1/AdminAct – This SFR does not contain any NDcPP AGD Assurance Activities.

FMT_SMF.1 – This SFR does not contain any NDcPP AGD Assurance Activities.

FMT_SMR.2
"The evaluator shall review the guidance documentation to ensure that it contains instructions for administering the TOE both locally and remotely, including any configuration that needs to be performed on the client for remote administration."

Section 7.1 of the supplemental AGD describes the ability of the TOE to be administered both locally and remotely. Section 6.2 of the supplemental AGD describes how configuration of the SSH interface for the enabling of remote administration is performed, and section 6.6 describes the specific SSH cryptographic parameters that must be configured in order for this interface to be used in accordance with its evaluated configuration.

FPT_APW_EXT.1 – This SFR does not contain any NDcPP AGD Assurance Activities.

FPT_SKP_EXT.1 – This SFR does not contain any NDcPP AGD Assurance Activities.

FPT_STM.1 – This SFR does not contain any NDcPP AGD Assurance Activities.

FPT_TST_EXT.1
"The evaluator shall also ensure that the guidance documentation describes the possible errors that may result from such tests, and actions the administrator should take in response; these possible errors shall correspond to those described in the TSS."

Section 9 of the supplemental AGD indicates that there is no error state that results from a failed self-test and that any self-test failure will prompt a reboot of the TOE. The administrator is advised that the device may need to be factory reset or re-imaged as a remediation strategy for any recurring error condition.

FPT_TUD_EXT.1
"The evaluator shall verify that the guidance documentation describes how the verification of the authenticity of the update is performed (digital signature verification or verification of published hash). The description shall include the procedures for successful and unsuccessful verification. The description shall correspond to the description in the TSS."

Section 7.8 of the supplemental AGD indicates that signature verification is performed automatically when a software upgrade command is run on an image update. Successful verification will result in the installation proceeding. The update then takes effect when the TOE is rebooted following a successful install. In the event that the signature verification fails, the update process will automatically abort and the invalid image will be discarded without administrator intervention.

FTA_SSL_EXT.1, **FTA_SSL.3**, **FTA_SSL.4 –** There is no specific assurance activity. However, the assurance activity for testing requires the tester to follow the operational guidance to configure the system inactivity period. Section 7.6 of the AGD provides information on manual and automatic session termination activities.

FTA_TAB.1 – There is no specific assurance activity. However, the assurance activity for testing requires the tester to follow the operational guidance to configure the banner. Section 7.5 of the AGD provides instructions on how to configure the login banner.

FTP_ITC.1
"The evaluator shall confirm that the guidance documentation contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken."

Sections 6.3, 6.4, and 6.9 of the supplemental AGD discuss the remote trusted channels for SSH (auditing) and TLS (auditing and RADIUS). In each case, the section discusses how to set up the trusted channel for that interface and how communications outages are handled, which includes any actions that need to be taken by the administrator when this occurs.

FTP_TRP.1
"The evaluator shall confirm that the guidance documentation contains instructions for establishing the remote administrative sessions for each supported method."

Sections 6.2 and 6.6 of the supplemental AGD describe how to enable the SSH server for remote administration and how to configure the SSH connection parameters in a manner consistent with the evaluated configuration.

AGD_OPE.1
In addition to SFR-related Evaluation Activities, the following information is also required.
a) The guidance documentation shall contain instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.

Section 6.5 of the supplemental AGD indicates how to enable FIPS mode for the TOE and explicitly states that the TOE must be run in FIPS mode in order to comply with the evaluated configuration. Sections 6.6 and 6.7 provide further instructions on the configuration of the cryptographic engine by identifying the SSH and TLS connection parameters that are permitted as well as sample syntax for how to set these parameters.

b) The documentation must describe the process for verifying updates to the TOE by verifying a digital signature. The evaluator shall verify that this process includes the following steps:

> *1) Instructions for obtaining the update itself. This should include instructions for making the update accessible to the TOE (e.g., placement in a specific directory).*
> *2) Instructions for initiating the update process, as well as discerning whether the process was successful or unsuccessful. This includes generation of the hash/digital signature.*

Section 7.8 of the supplemental AGD discusses how to acquire and verify an update at a high level and also references other vendor documentation where this process is described in more detail. It is clear from this section that the administrator is expected to download an update from Ciena's support site, place it on an SFTP server that the TOE can communicate with, and initiate the retrieval and installation process using the TOE. It is also clear that the verification of the digital signature is done without administrator intervention and an update with an invalid signature is discarded.

c) The TOE will likely contain security functionality that does not fall in the scope of evaluation under this cPP. The guidance documentation shall make it clear to an administrator which security functionality is covered by the Evaluation Activities

Section 2 of the supplemental AGD discusses the intended audience for the guidance. It is clear from this section that the behavior described in the supplemental AGD (or referenced by it) is the product functionality that comprises the TSF, and that while the product provides other security functions, these are considered to be outside the scope of the TOE and the CC evaluation makes no claims regarding their effectiveness.

AGD_PRE.1

Preparative procedures must include a description of how the administrator verifies that the operational environment can fulfil its role to support the security functionality (including the requirements of the Security Objectives for the Operational Environment specified in the Security Target). The documentation should be in an informal style and should be written with sufficient detail and explanation that they can be understood and used by the target audience (which will typically include IT staff who have general IT experience but not necessarily experience with the TOE product itself).

Section 5.3 of the supplemental AGD provides high-level information as to the expectations of the TOE's Operational Environment so that the administrator has sufficient information to ensure that the environmental security objectives are met. Through the course of conducting the Evaluation Activities the evaluators observed that the supplemental AGD was written in a formal style, as was the existing vendor documentation that it cites as needed. Security concepts central to the use of the TOE such as RADIUS, TLS, and X.509 were written with the expectation that the reader is familiar with the subject matter.

Preparative procedures must be provided for every Operational Environment that the product supports as claimed in the Security Target and must adequately address all platforms claimed for the TOE in the Security Target.

The evaluators determined from a review of the ST that the TOE has two models but each model has identical software/firmware components (SAOS 8.5). The evaluators observed from conducting the Evaluation Activities for the operational guidance that the supplemental AGD includes and/or references sufficient information to describe how to manage the TSF. The evaluators also observed that the supplemental AGD references the installation guidance for the two TOE models, which discusses the physical setup requirements that are unique to each model.

The preparative procedures must include:
a) instructions to successfully install the TSF in each Operational Environment; and
b) instructions to manage the security of the TSF as a product and as a component of the larger operational environment; and
c) instructions to provide a protected administrative capability.

Section 6 of the AGD provides the initial acceptance and setup of the TOE following physical installation. As reviewed in the prior paragraph, several sections of the AGD describe the instructions to install and configure the TOE and the Operational Environment products to communicate. Additionally, through the review of the Operational Guidance Assurance Activities for each SFR, the evaluation team determined that the AGD provides instructions on managing the TOE itself as related to the SFRs, managing the TOE and preparing the Operational Environment products to communicate, and include descriptions to protect the administration of the TOE through TOE functions. Finally, Section 5.3 of the AGD lists the assumptions of the TOE's Operational Environment as defined by the NDcPP (which correspond 1:1 with the security objectives for the Operational Environment). Each assumption is accompanied by a brief summary of what the administrator expected to ensure as part of verifying that the security objectives for the Operational Environment are satisfied. The actions provided are written in an easily understood style and clear regarding the requirements levied on the Operational Environment. For these reasons, the evaluation team has determined that the AGD contains the necessary instructions and information to securely operate the TOE within the Operational Environment that has been described in the ST.

4 Test Assurance Activities (Test Report)

The following sections demonstrate that all ATE Assurance Activities for the TOE have been met. This evidence has been presented in a manner that is consistent with the “Reporting for Evaluations Against NIAP-Approved Protection Profiles” guidance that has been provided by NIAP. Specific test steps and associated detailed results are not included in this report in order for it to remain non-proprietary. The test report is a summarized version of the test activities that were performed as part of creating the Evaluation Technical Report (ETR).

4.1 Platforms Tested and Composition

The evaluation team set up a test environment for the independent functional testing that allowed them to perform all test assurance activities across one TOE model and over the relevant interfaces. The evaluation team performed testing samples on both the local and remote CLIs. All testing required by the Evaluation Activities to be performed on the local CLI were tested locally; the remaining tests were performed using either the remote or local management interface. Additionally, a subset of testing was performed on the remote management CLI in an in-band configuration in order to verify that the management functionality of the TOE is equivalent regardless of whether the physical interface is a network port or the dedicated management port.

The TOE platform used for testing was the 4-slot model of the Ciena 8700. SAOS 8.5 was present on the TOE, consistent with the ST.

4.2 Omission Justification

The evaluation team set up a test environment for the independent functional testing that allowed them to perform all of the assurance activities against the 4-slot model of the Ciena 8700 Packetwave Platform over the SFR relevant interfaces. As per the Equivalency Considerations in the NDcPP Supporting Document, full re-testing of each model is not necessary because the only differences between them are scalability, which is not security-relevant. Since both the 4-slot and 10-slot model of the Ciena 8700 Packetwave Platform use the same hardware processor family/instruction set and software binary, and they have the same security-relevant physical and logical interfaces, the different models are considered to be equivalent in terms of security functionality. Based on the architectural arguments for equivalence, the Booz Allen CCTL has sufficient confidence that the security functionality is identical between each model that the 10-slot Ciena 8700 Packetwave Platform device is also expected to perform in the same manner as the tested model.

4.3 Assessment of the Ciena Test Environment

4.3.1 Physical Assessment

The Ciena site located in Hanover, MD is the physical location for the Ciena 8700 Packetwave Platform test environment. Booz Allen reviewed the physical security controls of the test environment and interviewed Ciena employees to ensure that the Ciena 8700 Packetwave Platform testing environment was secure. Booz Allen has found that Ciena Headquarters has similar access controls to Booz Allen’s CCTL. The Ciena location requires a person to be a Ciena employee to enter the building or be escorted as a visitor by a Ciena employee. The building is primarily controlled by a badge access system for employees whereas visitors must sign in and wear a temporary visitor nameplate. The laboratory where the Ciena 8700 Packetwave Platform device is installed is a secured internal room located at the facility. Thus, physical access to the Ciena 8700 Packetwave Platform device would require a person to pass through the badge access control by being a Ciena employee or a visitor being escorted by a Ciena employee as well as have access to the internal room where the servers are located. The evaluator conducted a daily inspection of the space and equipment for any signs of tampering of the space or equipment and found no such evidence of malicious tampering. Booz Allen finds that these physical access controls are satisfactory to protect the environment from unwanted physical access.

4.3.2 Logical Assessment

The functional testing can be executed remotely from the physical test environment. The only way to access the Ciena 8700 device was to connect to the local test network that the TOE resides on and that was built for Common Criteria functional testing specifically. At the end of each work day, the evaluators saved any configuration that was performed according to the AGD and shutdown the devices. At times during the testing, Ciena personnel performed changes to the configuration of the test environment. This was mainly to conduct testing on either the local console port or data plane ports. Any configuration performed by Ciena personnel during the functional testing timeframe was conducted using the AGD as guidance and under the supervision of the evaluators. Booz Allen finds these logical access controls are satisfactory to protect the environment from unauthorized logical access.

4.4 Test Cases

The evaluation team completed the functional testing activities within the vendor's test environment. The evaluation team conducted a set of testing that includes all ATE Assurance Activities as specified by the 'collaborative Protection Profile for Network Devices Version 1.0' (NDcPP) for the SFRs claimed in the Security Target. The evaluators reviewed the NDcPP to identify the security functionality that must be verified through functional testing. This is prescribed by the Assurance Activities for each SFR.

If an SFR is not listed, one of the following conditions applies:

- The Assurance Activity for the SFR specifically indicates that it is simultaneously satisfied by completing a test Assurance Activity for a different SFR.
- The Assurance Activity for the SFR does not specify any actions related to ATE activities (e.g. FPT_APW_EXT.1).

Note that some SFRs have Assurance Activities associated with them at the element level, but it may be the case that not all elements of the component will have Assurance Activities associated with them (e.g. FCS_SSH_EXT.1.1). In such cases, testing for the SFR is considered to be satisfied by completion of all Assurance Activities for each element underneath the component.

The following lists for each ATE Assurance Activity, the test objective, test instructions, test steps, and test results. Note that unless otherwise specified, the test configuration is to be in the evaluated configuration as defined by the AGD. For example, some tests require the TOE to be brought out of the evaluated configuration to temporarily disable cryptography to prove that the context of transmitted data is accurate. As part of the cleanup for each test, the TOE is returned to the evaluated configuration.

4.4.1 Security Audit

Test Case Number	001
SFR	FAU_GEN.1 and FAU_GEN.2
Test Objective	The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records for the events listed in the table of audit events and administrative actions listed above. This should include all instances of an event: for instance, if there are several different I&A mechanisms for a system, the FIA_UIA_EXT.1 events must be generated for each mechanism. The evaluator shall test that audit records are for the establishment and termination of a channel for each of the cryptographic protocols contained in the ST. If HTTPS is implemented, the test demonstrating the establishment and termination of a TLS session can be combined with the test for an HTTPS session. Logging of all activities related to trusted update should be tested in detail and with utmost diligence. When verifying the test results, the evaluator shall ensure the audit records generated during testing match the format specified in the guidance documentation, and that the fields in each audit record have the proper entries. Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly.

Test Instructions	Execute this test per the test steps.
Test Steps	1. Turn on the audit functionality on the TOE. Audit records are generated in the security, event and commands logs. These are sent to a remote server using SFTP. Syslog logs are sent to the syslog server using TLS: command-log enable logging enable destination flash system security log enable event-id 0x1B000A syslog enable 2. Perform actions related to the SFRs listed in Table 9 – Auditable Events from the Security Target such that an audit record is generated for that particular action. Repeat events until finished. [Note: These audit records have been generated during the course of the testing] 3. Verify which audit logs go into the syslog server or the security, command or event logs 4. To view the security, command and event logs run the following commands: command-log show tail <#lines> logging view destination flash tail <#lines> keyword <string> system security log show tail <#lines> 5. View the syslog records on the syslog server: vi /var/logs/test.log 6. Save a copy of each audit record generated for each event. 7. Run the following commands to disable logging: command-log disable logging disable destination flash system security log disable event-id 0x1B000A syslog disable
Test Results	Pass
Execution Method	Manual

Test Case Number	002
SFR	FAU_STG.1
Test Objective	The evaluator shall perform the following tests: a) Test 1: The evaluator shall access the audit trail as an unauthorized administrator and attempt to modify and delete the audit records. The evaluator shall verify that these attempts fail.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Log in as a limited user and attempt to modify and delete audit records. 2. These attempts will fail. 3. Run the following commands to attempt to clear all the logs:

	system security log clear command-log clear logging clear 4. Log in as the admin user and attempt to modify and delete audit records. 5. These attempts will fail: 6. Run the following commands to attempt to clear all the logs: system security log clear command-log clear logging clear
Test Results	Pass
Execution Method	Manual

Test Case Number	003
SFR	FAU_STG.1
Test Objective	The evaluator shall perform the following tests: b) Test 2: The evaluator shall access the audit trail as an authorized administrator and attempt to delete the audit records. The evaluator shall verify that these attempts succeed. The evaluator shall verify that only the records authorized for deletion are deleted.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Login as the super user. 2. Review the audit logs. 3. Run the following commands: system security log clear command-log clear logging clear 4. Verify the information reviewed in step 2 has been deleted. 5. Save off audit records of these successful deletion attempts.
Test Results	Pass
Execution Method	Manual

Test Case Number	004
SFR	FAU_STG_EXT.1
Test Objective	Testing of the trusted channel mechanism for audit will be performed as specified in the associated assurance activities for the particular trusted channel mechanism. The evaluator shall perform the following additional test for this requirement: Test 1: The evaluator shall establish a session between the TOE and the audit server according to the configuration guidance provided. The evaluator shall then examine the traffic that passes between the audit server and the TOE during several activities of the evaluator’s choice designed to generate audit data to be transferred to the audit server. The evaluator shall observe that these data are not able to be viewed in the clear during this transfer, and that they are successfully received by the audit server. The evaluator shall record the particular software (name, version) used on the audit server during testing.

	The evaluator shall perform operations that generate audit data and verify that this data is stored locally. The evaluator shall perform operations that generate audit data until the local storage space is exceeded and verifies that the TOE complies with the behaviour defined in FAU_STG_EXT.1.3. Depending on the configuration this means that the evaluator has to check the content of the audit data when the audit data is just filled to the maximum and then verifies that a) The audit data remains unchanged with every new auditable event that should be tracked but that the audit data is recorded again after the local storage for audit data is cleared (for the option 'drop new audit data' in FAU_STG_EXT.1.3). b) The existing audit data is overwritten with every new auditable event that should be tracked according to the specified rule (for the option 'overwrite previous audit records' in FAU_STG_EXT.1.3) c) The TOE behaves as specified (for the option 'other action' in FAU_STG_EXT.1.3).
Test Instructions	Execute this test per the test steps.
Test Steps	1. Start Wireshark packet capture between the TOE and the syslog server. 2. Perform some tasks that cause audit records to be created 3. Stop and save the packet capture. 4. Verify from the packet capture that the audit data was sent encrypted using TLS. 5. Record the software version number of the syslog server 6. Start the Wireshark packet capture between the TOE and the SFTP audit server 7. Perform some tasks that cause audit records to be created 8. Transfer the audit records from the TOE to the audit server using SFTP. 9. Stop the Wireshark packet capture 10. Examine the packets to verify they were sent encrypted 11. Take a screen shot of the encrypted packets 12. Verify the audit records reside on the audit server 13. Take a screen shot 14. Save off the software version number of the audit serve 15. Save off audit records of the events
Test Results	Pass
Execution Method	Manual

Test Case Number	005
SFR	FAU_STG_EXT.1
Test Objective	Testing of the trusted channel mechanism for audit will be performed as specified in the associated assurance activities for the particular trusted channel mechanism. The evaluator shall perform the following additional test for this requirement: The evaluator shall perform operations that generate audit data and verify that this data is stored locally. The evaluator shall perform operations that generate audit data until the local storage space is exceeded and verifies that the TOE complies with the behaviour defined in FAU_STG_EXT.1.3. Depending on the configuration this means that the evaluator has to check the content of the audit data when the audit data is just filled to the maximum and then verifies that a) The existing audit data is overwritten with every new auditable event that should be tracked according to the specified rule (for the option 'overwrite

	previous audit records' in FAU_STG_EXT.1.3) b) The existing audit data is overwritten with every new auditable event that should be tracked according to the specified rule (for the option 'overwrite previous audit records' in FAU_STG_EXT.1.3) c) The TOE behaves as specified (for the option 'other action' in FAU_STG_EXT.1.3).
Test Instructions	Execute this test per the test steps.
Test Steps	Test the Security Log File 1. Clear the Security Log file. 2. Run a script so that 26,000 events are recorded in the Security Log. 3. Verify that 4 Security Log history files are created each holding 5000 records and one current Security Log file is created containing the remainder of the records. 4. Record the number of events in each security log file. 5. Clear the Event log file and Command log file. 6. Run a script 41,000 times which runs a command which gets recorded in both the Command log and Event Log. 7. Verify that 3 Event Log history files are created each holding 10,000 records and 1 current Event Log file is created containing the remainder of the records. 8. Record the number of events in each Event Log. 9. Verify that 4 Command Log history files are created each holding 2500 records and 1 current Command Log file is created holding the remainder of the records.
Test Results	Pass
Execution Method	Manual

4.4.2 Cryptographic Security

Test cases for FCS_CKM.1, FCS_CKM.2, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), and FCS_RBG_EXT.1 are not included within this section. This is because the ATE Assurance Activities have been satisfied by the vendor having the TOE's algorithms assessed under Cryptographic Algorithm Validation Program (CAVP). As part of CAVP validation the TOE's cryptographic algorithms went through CAVS testing which directly maps to these SFRs' ATE Assurance Activities. Refer to the results of the CAVP validation for the certificates listed within the Security Target.

Test Case Number	006
SFR	FCS_SSHC_EXT.1
Test Objective	Test 1: The evaluator shall, for each public key algorithm supported, show that the TOE supports the use of that public key algorithm to authenticate a user connection to an SSH server. Any configuration activities required to support this test shall be performed according to instructions in the guidance documentation.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Start a packet capture of the connection between the TOE and the SFTP-server using Wireshark 2. Get a file from the SFTP server using the SFTP-user by running the command on the TOE: system xftp getfile remote-filename <filename> sftp-server <ip address> local-filename <filename> login-id <SFTP-user> 3. This will transfer the file without password authentication. It will use public key authentication.

	4. Stop and save the packet capture 5. Capture the audit records 6. Repeat steps 1-5 using ECDSA256 7. Repeat steps 1-5 using ECDSA384
Test Results	Pass
Execution Method	Manual

Test Case Number	007
SFR	FCS_SSHC_EXT.1
Test Objective	Test 2: Using the guidance documentation, the evaluator shall configure the TOE to perform password-based authentication to an SSH server, and demonstrate that a user can be successfully authenticated by the TOE to an SSH server using a password as an authenticator.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Open Wireshark 2. Get a file from the SFTP server by running the following command on the TOE: system xftp getfile remote-filename <filename> local-filename <filename> sftp-server <ip address> login-id <user> echoless-password 3. Stop Wireshark and save the packet capture 4. Take a screenshot showing the successful password based authentication of the TOE client to the SFTP server 5. Capture all audit records
Test Results	Pass
Execution Method	Manual

Test Case Number	008
SFR	FCS_SSHC_EXT.1
Test Objective	Test 3: The evaluator shall demonstrate that if the TOE receives a packet larger than that specified in this component, that packet is dropped.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Authenticate to the TOE via the CLI. 2. Execute the following command to initiate a connection to the SSH server created during Setup: ssh client connect ip 10.41.71.102 user ciena 3. Execute the command to generate a large amount of SSH traffic. 4. Examine the logs on the SSH server for the following statement: “Bypass setting len based on remote_maxpacket” and “Read error from remote host 10.41.71.101 port <port>: Connection reset by peer” 5. Examine the logs on the TOE for the termination of the SSH session.
Test Results	Pass
Execution Method	Manual

Test Case Number	009
SFR	FCS_SSHC_EXT.1
Test Objective	Test 1: The evaluator shall establish a SSH connection using each of the encryption algorithms specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test. Test 2: The evaluator shall configure an SSH server to only allow an encryption algorithm that is not included in the ST selection. The evaluator shall attempt to establish an SSH connection from the TOE to the SSH server and observe that the connection is rejected.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Start a packet capture of the connection between the TOE client and the SFTP server using Wireshark 2. Configure the TOE SSH Client to only use AES-CBC-128 as the encryption algorithm 3. Get a file from the SFTP server by running the following command on the TOE: system xftp getfile remote-filename <filename> local-filename <filename> sftp-server <ip address> login-id <user> echoless-password 4. Stop Wireshark 5. Find the algorithm exchange packet and take a screenshot showing the successful negotiation using AES-CBC-128. 6. Save the audit record of the successful connection. 7. Repeat steps 1-6 using AES-CBC-256 the connection will be successful 8. Repeat steps 1,2,3,4 except configure the SFTP server to only use 3DES-CBC. Configure the TOE to only use AES-CBC-256. This time the connection will be unsuccessful. Take a screen shot showing the unsuccessful negotiation and save the packet capture. 9. Save the audit record showing the unsuccessful login attempt
Test Results	Pass
Execution Method	Manual

Test Case Number	010
SFR	FCS_SSHC_EXT.1
Test Objective	Test 1: The evaluator shall establish a SSH connection using each of the public key algorithms specified by the requirement to authenticate the TOE to an SSH client. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test. Test 2: The evaluator shall configure an SSH client to only allow the ssh-dsa public key algorithm and no other public key algorithms. The evaluator shall attempt to establish an SSH connection from the SSH client to the TOE and observe that the connection is rejected.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Remove the host key from the hosts key file by running the command ssh client remove ip <ip address of server> 2. Configure the TOE SSH Client to only use ssh-rsa as its public key algorithm. 3. Open Wireshark to capture packets between the TOE and the SFTP server

	4. Get a file from the SFTP Server by running the following command on the TOE: system xftp getfile remote-filename <filename> local-filename <filename> sftp-server <ip address> login-id <user> auth-interactive 5. Stop the packet capture and take a screen shot showing ssh-rsa was successfully used as the public-key algorithm. 6. Save the packet capture and audit record of the connection 7. Repeat steps 1-5 with ecdsa-sha2-nistp256 8. Repeat steps 1-5 with ecdsa-sha2-nistp384 9. Repeat steps 1-5 with x509v3-ecdsa-sha2-nistp256 10. Repeat steps 1-5 with x509v3-ecdsa-sha2-nistp384 11. Repeat steps 1-4 with ssh-dsa except configure the SFTP server to offer only this algorithm. The connection will fail.
Test Results	Pass
Execution Method	Manual

Test Case Number	011
SFR	FCS_SSHC_EXT.1
Test Objective	Test 1: The evaluator shall establish a SSH connection using each of the integrity algorithms specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test. Test 2: The evaluator shall configure an SSH client to only allow the “none” MAC algorithm. The evaluator shall attempt to connect from the SSH client to the TOE and observe that the attempt fails. Test 3: The evaluator shall configure an SSH client to only allow the hmacmd5 MAC algorithm. The evaluator shall attempt to connect from the SSH client to the TOE and observe that the attempt fails.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Configure the TOE SSH Client to use hmac-sha1 as the integrity algorithm 2. Start a packet capture of the connection between the TOE client and the SFTP server 3. Get a file from the SFTP server system xftp getfile remote-filename <filename> local-filename <filename> sftp-server <ip address> login-id <user> echoless-password 4. Stop and save the packet capture 5. Find the algorithm exchange packet and take a screen shot showing the successful negotiation using hmac-sha-1 6. Save the audit record and packet capture corresponding to the successful connection 7. Repeat steps 1-6 using hmac-sha2-256 will be successful 8. Repeat steps 1-6 using hmac-sha2-512 will be successful 9. Repeat steps 1-6 using hmacmd5 except configure the SFTP server to only use this algorithm. The connection will fail.
Test Results	Pass
Execution Method	Manual

Test Case Number	012
SFR	FCS_SSHC_EXT.1
Test Objective	Test 1: The evaluator shall configure an SSH server to permit all allowed key exchange methods. The evaluator shall attempt to connect from the TOE to the

	SSH server using each allowed key exchange method, and observe that each attempt succeeds.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Configure the SFTP Server to only use diffie-hellman-group1-sha1 2. Configure the TOE SSH Client to only use ecdh-sha2-nistp256. 3. Start the Wireshark packet capture between the TOE client and the SFTP server 4. Get a file from the SFTP server by running this command on the TOE: system xftp getfile remote-filename <filename> local-filename <filename> sftp-server <ip address> login-id <user> echoless-password 5. Stop and save the packet capture 6. This test will be unsuccessful. 7. Take a screenshot of the failed negotiation packet 8. Save the audit record corresponding to the unsuccessful attempt 9. Configure the TOE SSH Client to only use ecdh-sha2-nistp256 10. Start the Wireshark packet capture between the TOE client and the SFTP server 11. Get a file from the SFTP Server by running the following command on the TOE: system xftp getfile remote-filename <filename> local-filename <filename> sftp-server <ip address> login-id <user> echoless-password 12. Stop and save the packet capture 13. Take a screenshot of the successful algorithm exchange packet 14. Save the audit record corresponding to the successful transfer
Test Results	Pass
Execution Method	Manual

Test Case Number	013
SFR	FCS_SSHC_EXT.1
Test Objective	The evaluator shall configure the TOE to create a log entry when a rekey occurs. The evaluator shall connect to the TOE with an SSH client and cause 2^28 packets to be transmitted from the client to the TOE, and subsequently review the audit log to ensure that a rekey occurred.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Configure the SFTP server to cause a re-key after 500 MB of data by setting the rekey-limit in bytes value to 500MB ssh server set rekey-limit 500M 2. Start Wireshark between the TOE and the SFTP server 3. Download a large file that is more than 500M from the sftp server onto the TOE system xftp getfile remote-filename <filename> local-filename <filename> sftp-server <ip-address> login-id <user> auth-interactive 4. Stop the packet capture 5. Examine the audit logs to verify the rekey occurred before 500M of data was transferred system security log show tail 20 6. Configure SSH client and server to cause a rekey after 20 seconds: ssh server set rekey-timeout 1m 7. Start Wireshark between the TOE and the SFTP server 8. Download a large file from the SFTP server system xftp getfile remote-filename <filename> local-filename <filename> sftp-server <ip-address> login-id <user> auth-interactive

	9. Wait for one minute 10. Stop the packet capture 11. Examine the system log system security log show tail 20 12. Note the re-key occurs under encrypted data and will not show in the captured data. It will show in the audit logs as having occurred.
Test Results	Pass
Execution Method	Manual

Test Case Number	014
SFR	FCS_SSHC_EXT.1
Test Objective	Test 1: The evaluator shall delete all entries in the TOE's list of recognized SSH server host keys and, if selected, all entries in the TOE's list of trusted certification authorities. The evaluator shall initiate a connection from the TOE to an SSH server. The evaluator shall ensure that the TOE either rejects the connection or displays the SSH server's public key (either the key bytes themselves or a hash of the key using any allowed hash algorithm) and prompts the user to accept or deny the key before continuing the connection.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Authenticate to the TOE via the CLI. 2. Begin capturing packets using Wireshark between the TOE and the remote SSH server. 3. Perform the steps in the Setup to remove the host keys and CA certificates of the remote SSH servers. 4. Attempt to authenticate to the remote SSH server by executing the following commands: ssh client connect ip 10.41.71.100 5. Stop capturing packets between the TOE and the remote SSH server. 6. Verify that the TOE displays the SSH server's hash of its host key prior to continuing the connection. 7. Repeat Steps 2-6, except connect to the SSH server that uses X.509 certificates.
Test Results	Pass
Execution Method	Manual

Test Case Number	015
SFR	FCS_SSHC_EXT.1
Test Objective	Test 2: The evaluator shall add an entry associating a host name with a public key into the TOE's local database. The evaluator shall replace, on the corresponding SSH server, the server's host key with a different host key. The evaluator shall initiate a connection from the TOE to the SSH server using password-based authentication, shall ensure that the TOE rejects the connection, and shall ensure that the password was not transmitted to the SSH server (for example, by instrumenting the SSH server with a debugging capability to output received passwords).
Test Instructions	Execute this test per the test steps.
Test Steps	1. Start Wireshark between the TOE and the SFTP server 2. Connect to the SFTP server: 3. system xftp getfile remote-filename <filename> local-filename <filename> sftp-server <ip address> login-id <user> auth-interactive

	4. Stop the Wireshark packet capture 5. The connection will fail 6. Verify no passwords were sent to the SFTP server
Test Results	Pass
Execution Method	Manual

Test Case Number	016
SFR	FCS_SSHS_EXT.1
Test Objective	Test 1: The evaluator shall, for each public key algorithm supported, show that the TOE supports the use of that public key algorithm to authenticate a user connection. Any configuration activities required to support this test shall be performed according to instructions in the guidance documentation.
Test Instructions	Execute this test per the test steps.
Test Steps	1. On the client running Bitvise generate a new client key pair. 2. Export the public key using OpenSSH format into a file called <user>.pub 3. Place this file in the sftp server under the root directory 4. On the TOE run the command to transfer and install the key for <user> ssh server key install user <user> sftp-server <ip address> login-id <sftp user> echoless-password <cr> 5. Enter the password for the sftp user 6. Start a packet capture of the connection between the client and the TOE using Wireshark 7. On the client machine run Bitvise and connect to the TOE using the RSA algorithm for authentication. 8. Stop and save the packet capture 9. Take a screenshot of the Bitvise authentication parameters 10. Take a screenshot of the CLI connection showing the successful connection to the TOE. 11. Take a screenshot of the packet capture showing the algorithm negotiation includes RSA 12. Repeat steps 1-11 using ecdsa256
Test Results	Pass
Execution Method	Manual

Test Case Number	017
SFR	FCS_SSHS_EXT.1
Test Objective	Test 2: The evaluator shall choose one public key algorithm supported by the TOE. The evaluator shall generate a new key pair for that algorithm without configuring the TOE to recognize the public key for authentication. The evaluator shall use an SSH client to attempt to connect to the TOE with the new key pair and demonstrate that authentication fails.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Open Bitvise 2. Generate a new client public key using Bitvise (for RSA) 3. Attempt to login to the TOE using Bitvise and the public key authentication to the TOE

	4. The attempt will fail
Test Results	Pass
Execution Method	Manual

Test Case Number	018
SFR	FCS_SSHS_EXT.1
Test Objective	Test 3: Using the guidance documentation, the evaluator shall configure the TOE to accept password-based authentication, and demonstrate that a user can be successfully authenticated to the TOE over SSH using a password as an authenticator. Test 4: The evaluator shall use an SSH client, enter an incorrect password to attempt to authenticate to the TOE, and demonstrate that the authentication fails
Test Instructions	Execute this test per the test steps.
Test Steps	1. Open BitVise and login to the TOE using password based authentication. 2. Save the audit record showing a successful login via SSH 3. Take a screenshot of the Bitvise login 4. The tester will logout from the TOE and attempt to reauthenticate using an incorrect password 5. The login attempt will fail 6. An audit record will be created for the unsuccessful SSH login attempt
Test Results	Pass
Execution Method	Manual

Test Case Number	019
SFR	FCS_SSHS_EXT.1
Test Objective	The evaluator shall demonstrate that if the TOE receives a packet larger than that specified in this component, that packet is dropped.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Create a large file on the test machine. 2. Launch the modified SFTP (modified implementation of OpenSSH created during Setup) client and use to to establish a connection to the TOE. 3. Once authenticated to the TOE via SFTP, execute the following command: put largefile 4. Examine the output for the following similar text: “Remote Window Size 1834714 Remote Max Packet 32768 Length 49152 Bypass setting len based on remote_maxpacket packet_write_wait: Connection to 10.41.71.101 port 22: Broken pipe Couldn't read packet: Connection reset by peer”
Test Results	Pass
Execution Method	Manual

Test Case Number	020
SFR	FCS_SSHS_EXT.1
Test Objective	Test 1: The evaluator shall establish a SSH connection using each of the encryption algorithms specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.

	Test 2: The evaluator shall configure an SSH client to only allow an encryption algorithm that is not included in the ST selection. The evaluator shall attempt to establish an SSH connection from the SSH client to the TOE and observe that the connection is rejected.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Start a packet capture of the connection between the client and the TOE using Wireshark 2. Run Bitvise and connect to the TOE using AES-CBC-128 as the encryption algorithm 3. Run Show command to send packets between the TOE and the client 4. Stop and save the packet capture 5. Find the algorithm exchange packet and take a screenshot showing the successful negotiation using AES-CBC-128. 6. Save the audit record of the successful connection. 7. Repeat steps 1-6 using AES-CBC-256 the connection will be successful 8. Repeat steps 1, 2, 4 using 3DES-CBC. This time the connection will be unsuccessful. Take a screen shot showing the unsuccessful negotiation and save the packet capture. 9. Save the audit record showing the unsuccessful login attempt
Test Results	Pass
Execution Method	Manual

Test Case Number	021
SFR	FCS_SSHS_EXT.1
Test Objective	Test 1: The evaluator shall establish a SSH connection using each of the public key algorithms specified by the requirement to authenticate the TOE to an SSH client. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test. Test 2: The evaluator shall configure an SSH client to only allow the ssh-dsa public key algorithm and no other public key algorithms. The evaluator shall attempt to establish an SSH connection from the SSH client to the TOE and observe that the connection is rejected.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Open Wireshark to capture packets between the SSH client and the TOE. 2. Open BitVise and configure SSH to use ssh-rsa for the public-key algorithm. 3. Connect to the TOE 4. Stop the packet capture and confirm ssh-rsa was used as the public-key algorithm. 5. Save off the audit records of the successful connection 6. Repeat steps 1-5 with ecdsa-sha2-nistp256 7. Repeat steps 1-5 with ecdsa-sha2-nistp384 8. Repeat steps 1-5 with ssh-dsa 9. Open Wireshark to capture packets between the SSH client and the TOE 10. Configure the TOE SSH Server to use x509v3-ecdsa-sha2-nistp256 11. Run the following command on the SSH client: sudo /home/ciena/pkixssh-8.7/ssh ciena1@10.41.71.101 -i /home/ciena/ciena1.id -F /home/ciena/pkixssh-8.7/ssh_config 12. Stop the packet capture and confirm x509v3-ecdsa-sha2-nistp256 was

	used as the public key algorithm 13. Repeat steps 9-12 with x509v3-ecdsa-sha2-nistp384
Test Results	Pass
Execution Method	Manual

Test Case Number	021
SFR	FCS_SSHS_EXT.1
Test Objective	Test 1: The evaluator shall establish a SSH connection using each of the integrity algorithms specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test. Test 2: The evaluator shall configure an SSH client to only allow the “none” MAC algorithm. The evaluator shall attempt to connect from the SSH client to the TOE and observe that the attempt fails. Test 3: The evaluator shall configure an SSH client to only allow the hmacmd5 MAC algorithm. The evaluator shall attempt to connect from the SSH client to the TOE and observe that the attempt fails.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Start a packet capture of the connection between the client and the TOE using Wireshark 2. Run Bitvise and connect to the TOE using hmac-sha1 as the integrity algorithm 3. Run logging show command to send packets between the TOE and the Client. 4. Stop and save the packet capture 5. Find the algorithm exchange packet and take a screen shot showing the successful negotiation using hmac-sha-1 6. Save the audit record corresponding to the successful log 7. Repeat steps 1-6 using hmac-sha2-256 will be successful 8. Repeat steps 1-6 using hmac-sha2-512 will be successful 9. Repeat steps 1-6 using hmacmd5 which will fail to connect 10. Repeat steps 1-6 using none which will fail to connect
Test Results	Pass
Execution Method	Manual

Test Case Number	022
SFR	FCS_SSHS_EXT.1
Test Objective	Test 1: The evaluator shall configure an SSH client to only allow the diffiehellman-group1-sha1 key exchange. The evaluator shall attempt to connect from the SSH client to the TOE and observe that the attempt fails. Test 2: For each allowed key exchange method, the evaluator shall configure an SSH client to only allow that method for key exchange, attempt to connect from the client to the TOE, and observe that the attempt succeeds.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Start the Wireshark packet capture between the client and the TOE. 2. Run Bitvise and connect to the TOE using diffie-hellman-group14-sha1 3. Stop and save the packet capture 4. This test will be unsuccessful. 5. Take a screenshot of the Bitvise configuration screen.

	6. Take a screenshot of the failed negotiation packet 7. Save the audit record corresponding to the unsuccessful attempt 8. Start the Wireshark packet capture between the client and the TOE. 9. Run Bitvise and connect to the TOE using ecdh-sha2-nistp256 10. Run the logging show command to send packets between the TOE and the client 11. Stop and save the packet capture. 12. Take a screenshot of the Bitvise configuration 13. Take a screenshot of the successful algorithm exchange packet 14. Save the audit record corresponding to the successful login 15. Repeat steps 8-14 using ecdh-sha2-nistp384 16. Repeat steps 8-14 using ecdh-sha2-nistp521
Test Results	Pass
Execution Method	Manual

Test Case Number	023
SFR	FCS_SSHS_EXT.1
Test Objective	The evaluator shall configure the TOE to create a log entry when a rekey occurs. The evaluator shall connect to the TOE with an SSH client and cause 2^28 packets to be transmitted from the client to the TOE, and subsequently review the audit log to ensure that a rekey occurred.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Configure the TOE SSH Server to rekey before 500MB 2. Open Wireshark between the TOE and the client 3. Download a 500MB file from an SFTP client. 4. Close Wireshark 5. Examine the log file to show that a rekey occurred before the file transfer was completed 6. Note: the rekey occurs under encrypted data therefore no packet capture can show it 7. Save off any audit records 8. Configure the TOE SSH Server to rekey before 1 minute 9. Transfer a file from the SFTP client 10. Examine the Bitvise screen shot to verify that a rekey occurred before 1 minute had elapsed once the SFTP connection was made. 11. Save off any audit records
Test Results	Pass
Execution Method	Manual

Test Case Number	024
SFR	FCS_TLSC_EXT.2
Test Objective	Test 1: The evaluator shall establish a TLS connection using each of the ciphersuites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of an HTTPS session. It is sufficient to observe the successful negotiation of a ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the ciphersuite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).

Test Instructions	Execute this test per the test steps.
Test Steps	1. Configure the remote server to use the following ciphersuites: 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_ECDHE_ECDSA_WITH_AES_128_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_ SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 2. Open Wireshark and begin capturing packets between the TOE and the remote server. 3. Perform some activity on the TOE to cause a TLS connection to be established to the remote server. 4. Stop capturing packets with Wireshark between the TOE and the remote server. 5. Examine the packet capture Server Hello packet for the ciphersuite selected in Step 1. 6. Repeat Steps 1-5, except iterate through to the next ciphersuite in Step 1.
Test Results	Pass
Execution Method	Manual

Test Case Number	025
SFR	FCS_TLSC_EXT.2
Test Objective	Test 2: The evaluator shall attempt to establish the connection using a server with a server certificate that contains the Server Authentication purpose in the extendedKeyUsage field and verify that a connection is established. The evaluator will then verify that the client rejects an otherwise valid server certificate that lacks the Server Authentication purpose in the extendedKeyUsage field and a connection is not established. Ideally, the two certificates should be identical except for the extendedKeyUsage field.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Install a certificate on the server with the Server Authentication purpose in the extendedKeyUsage field. 2. Start Wireshark and begin capturing packets between the TOE and the remote server. 3. Perform some activity on the TOE that causes a TLS connection to be established to the remote server. 4. Stop capturing packets with Wireshark. 5. Verify the connection was successful and that the server certificate was accepted by the TOE. 6. Repeat Steps 1-4, except install a certificate on the server without the Server Authentication purpose (i.e. use Client Authentication purpose) 7. Verify that the TLS connection failed.
Test Results	Pass
Execution Method	Manual

Test Case Number	026

SFR	FCS_TLSC_EXT.2
Test Objective	Test 3: The evaluator shall send a server certificate in the TLS connection that the does not match the server-selected ciphersuite (for example, send a ECDSA certificate while using the TLS_RSA_WITH_AES_128_CBC_SHA ciphersuite.) The evaluator shall verify that the TOE disconnects after receiving the server's Certificate handshake message.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Install a certificate on the remote server signed using RSA. 2. Configure the server to use the TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ciphersuite. 3. Begin capturing packets with Wireshark between the TOE and the remote server. 4. Perform some activity on the TOE to cause a TLS connection to be established to the remote server. 5. Stop capturing packets with Wireshark. 6. Verify that the connection failed after the TOE receives the server's Certificate handshake message.
Test Results	Pass
Execution Method	Manual

Test Case Number	027
SFR	FCS_TLSC_EXT.2
Test Objective	Test 4: The evaluator shall configure the server to select the TLS_NULL_WITH_NULL_NULL ciphersuite and verify that the client denies the connection. Test 2 in FCS_TLSS_EXT.1.1 or FCS_TLSS_EXT.2.1 can be used as a substitute for this test.
Test Instructions	Execute this test per the test steps.
Test Steps	The client cannot be configured to use the TLS_NULL_WITH_NULL_NULL ciphersuite. The server selects which ciphersuite to use based on the Client Hello ciphersuite advertisement from the client. The only way for the server to select this ciphersuite is if the client offers it as a choice. If the client includes this ciphersuite in the Client Hello then it would be offering an insecure ciphersuite and would fail validation. If the client does not include this ciphersuite and the server is configured to accept only this ciphersuite then the server would be the one to reject the connection.
Test Results	Pass
Execution Method	Manual

Test Case Number	028
SFR	FCS_TLSC_EXT.2
Test Objective	Test 5: The evaluator perform the following modifications to the traffic: a) Change the TLS version selected by the server in the Server Hello to a non-supported TLS version (for example 1.3 represented by the two bytes 03 04) and verify that the client rejects the connection. b) Modify at least one byte in the server's nonce in the Server Hello handshake message, and verify that the client rejects the Server Key Exchange handshake message (if using a DHE or ECDHE ciphersuite) or that the server denies the client's Finished handshake message. c) Modify the server's selected ciphersuite in the Server Hello handshake message to be a ciphersuite not presented in the Client Hello handshake message. The evaluator shall verify that the client rejects the connection after receiving the Server Hello.

	d) Modify the signature block in the Server's Key Exchange handshake message, and verify that the client rejects the connection after receiving the Server Key Exchange message. e) Modify a byte in the Server Finished handshake message, and verify that the client sends a fatal alert upon receipt and does not send any application data. f) Send a garbled message from the Server after the Server has issued the ChangeCipherSpec message and verify that the client denies the connection.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Open Wireshark and begin capturing packets between the TOE and the TLS server. 2. Run the modification program on the test system. 3. Initiate a connection from the TOE to the server such that the program modifies the appropriate packet. 4. Stop capturing packets with Wireshark. 5. Confirm the expected behavior for this subtest occurred. 6. Repeat Steps 2-5 for each of the subtests in this test.
Test Results	Pass
Execution Method	Manual

Test Case Number	029
SFR	FCS_TLSC_EXT.2
Test Objective	The evaluator shall present a server certificate that does not contain an identifier in either the Subject Alternative Name (SAN) or Common Name (CN) that matches the reference identifier. The evaluator shall verify that the connection fails.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Install a certificate on the server that does not contain either the Subject Alternative Name (SAN) or Common Name (CN) that matches the reference identifier. 2. Using Wireshark, begin capturing packets between the TOE and the server. 3. Connect the TOE to the server using TLS. 4. Stop capturing packets using Wireshark. 5. Verify that the connection fails.
Test Results	Pass
Execution Method	Manual

Test Case Number	030
SFR	FCS_TLSC_EXT.2
Test Objective	The evaluator shall present a server certificate that contains a CN that matches the reference identifier, contains the SAN extension, but does not contain an identifier in the SAN that matches the reference identifier. The evaluator shall verify that the connection fails. The evaluator shall repeat this test for each supported SAN type
Test Instructions	Execute this test per the test steps.
Test Steps	1. Install a certificate on the server that contains a CN that matches the reference identifier, contains the SAN extension but does not contain an identifier in the SAN that matches the reference identifier. 2. Begin capturing packets between the TOE and the server using Wireshark. 3. Connect the TOE to the server. 4. Stop capturing packets between the TOE and the server with Wireshark. 5. Verify the connection fails.

	6. Repeat this test for supported SAN type.
Test Results	Pass
Execution Method	Manual

Test Case Number	031
SFR	FCS_TLSC_EXT.2
Test Objective	The evaluator shall present a server certificate that contains a CN that matches the reference identifier and does not contains the SAN extension. The evaluator shall verify that the connection succeeds
Test Instructions	Execute this test per the test steps.
Test Steps	1. Install a certificate on the server that contains a CN that matches the reference identifier but does not contain the SAN extension 2. Using Wireshark, begin capturing packets between the TOE and the server. 3. Connect the TOE to the server. 4. Stop capturing packets with Wireshark. 5. Verify the connection succeeds.
Test Results	Pass
Execution Method	Manual

Test Case Number	032
SFR	FCS_TLSC_EXT.2
Test Objective	The evaluator shall present a server certificate that contains a CN that does not match the reference identifier but does contain an identifier in the SAN that matches. The evaluator shall verify that the connection succeeds.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Install a certificate on the server with a CN that does not match the reference identifier but does contain an identifier in the SAN that matches. 2. Using Wireshark, begin capturing packets between the TOE and the server. 3. Connect the TOE to the server. 4. Stop capturing packets with Wireshark. 5. Verify the connection succeeds.
Test Results	Pass
Execution Method	Manual

Test Case Number	033
SFR	FCS_TLSC_EXT.2
Test Objective	The evaluator shall perform the following wildcard tests with each supported type of reference identifier: 1) The evaluator shall present a server certificate containing a wildcard that is not in the left-most label of the presented identifier (e.g. foo.*.example.com) and verify that the connection fails. 2) The evaluator shall present a server certificate containing a wildcard in the left-most label (e.g. *.example.com). The evaluator shall configure the reference identifier with a single left-most label (e.g. foo.example.com) and verify that the connection succeeds. The evaluator shall configure the reference identifier without a left-most label as in the certificate (e.g. example.com) and verify that the connection fails. The evaluator shall configure the reference identifier with two left-most labels (e.g. bar.foo.example.com) and verify that the connection fails.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Install a certificate on the server containing a wildcard that is not in the left-most label of the presented identifier (e.g. foo.*.ciena.com) and

	specify the reference identifier of the host to be foo.cc-server-2.ciena.com. 2. Using Wireshark, begin capturing packets between the TOE and the server. 3. Connect the TOE to the server (e.g. foo.cc-server-2.ciena.com). 4. Stop capturing packets between the TOE and the server with Wireshark. 5. Verify the connection fails. 6. Install a certificate on the server containing a wildcard in the left-most label (e.g. *.ciena.com), and specify the reference identifier of the host to be with a single left-most label (e.g. cc-server-2.ciena.com). 7. Using Wireshark, begin capturing packets between the TOE and the server. 8. Connect the TOE to the server. 9. Stop capturing packets between the TOE and the server with Wireshark. 10. Verify the connection succeeds. 11. Repeat Steps 6-9, except in Step 6, configure the reference identifier of the host to ciena.com. 12. Repeat Steps 6-9, except in Step 6, configure the reference identifier of the host to cc-server-2.foo.ciena.com. 13. Repeat Steps 1-5, except in Step 1, install a certificate containing a wildcard in the left-most label immediate preceding the public suffix (e.g. *.com) and specify the reference identifier of the host to be with a single left-most label (e.g. ciena.com) 14. Repeat Step 13, except specify the reference identifier of the host to be with two left-most labels (e.g. foo.ciena.com).
Test Results	Pass
Execution Method	Manual

Test Case Number	034
SFR	FCS_TLSC_EXT.2
Test Objective	[conditional] If URI or Service name reference identifiers are supported, the evaluator shall configure the DNS name and the service identifier. The evaluator shall present a server certificate containing the correct DNS name and service identifier in the URIName or SRVName fields of the SAN and verify that the connection succeeds. The evaluator shall repeat this test with the wrong service identifier (but correct DNS name) and verify that the connection fails.
Test Instructions	Execute this test per the test steps.
Test Steps	URI or Service name reference identifiers are not supported; therefore, this test does not apply.
Test Results	Pass
Execution Method	Manual

Test Case Number	035
SFR	FCS_TLSC_EXT.2
Test Objective	[conditional] If pinned certificates are supported the evaluator shall present a certificate that does not match the pinned certificate and verify that the connection fails.
Test Instructions	Execute this test per the test steps.
Test Steps	Pinned certificates are not supported; therefore, this test does not apply.
Test Results	Pass
Execution Method	Manual

Test Case Number	036
SFR	FCS_TLSC_EXT.2
Test Objective	The evaluator shall demonstrate that using a certificate without a valid certification path results in the function failing. Using the administrative guidance, the evaluator shall then load a certificate or certificates needed to validate the certificate to be used in the function, and demonstrate that the function succeeds. If the certificate is validated and a trusted channel is established, the test passes. The evaluator then shall delete one of the certificates, and show that the certificate is not validated and the trusted channel is not established.
Test Instructions	Execute this test per the test steps.

Test Steps	1. Install the certificates needed to verify the server's certificate.
	2. Open Wireshark and begin capturing packets between the TOE and the remote server.
	3. Perform some activity on the TOE that causes the TOE to establish a connection to the remote server.
	4. Stop capturing packets with Wireshark.
	5. Verify the TLS connection succeeds.
	6. Remove one of the certificates in the certificate chain.
	7. If using RADIUS, skip Steps 8-9.
	8. Disable the syslog collector on the TOE by executing the following command on the TOE:
	`syslog tls disable collector cc-server-2.ciena.com`
	9. Enable the syslog collector on the TOE by executing the following command on the TOE:
	`syslog tls enable collector cc-server-2.ciena.com`
	10. Repeat Steps 2-4.
	11. Verify that the TLS connection fails.

Test Results	Pass
Execution Method	Manual

Test Case Number	037
SFR	FCS_TLSC_EXT.2
Test Objective	The evaluator shall configure the server to perform an ECDHE key exchange in the TLS connection using a non-supported curve (for example P-192) and shall verify that the TOE disconnects after receiving the server's Key Exchange handshake message.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Configure the remote server to only use secp192k1 curve for ECDHE. 2. Open Wireshark and begin capturing packets between the TOE and the remote server. 3. Perform some activity on the TOE to cause the TOE to establish a TLS connection to the remote server. 4. Stop capturing packets with Wireshark. 5. Verify the TLS connection failed after the TOE received the server's Key Exchange handshake message.
Test Results	Pass
Execution Method	Manual

Test Case Number	038
SFR	FCS_TLSC_EXT.2
Test Objective	Configure the server to require mutual authentication and then modify a byte in a CA field in the Server's Certificate Request handshake message. The modified CA field must not be the CA used to sign the client's certificate. The evaluator shall verify the connection fails.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Open Wireshark and begin capturing packets between the TOE and the TLS server. 2. Run the modification program on the test system. 3. Initiate a connection from the TOE to the server such that the program modifies the appropriate packet. 4. Stop capturing packets with Wireshark. 5. Confirm the expected behavior for this test occurred.
Test Results	Pass
Execution Method	Manual

4.4.3 Identification and Authentication

Test Case Number	039
SFR	FIA_PMG_EXT.1
Test Objective	The evaluator shall compose passwords that either meet the requirements, or fail to meet the requirements, in some way. For each password, the evaluator shall verify that the TOE supports the password. While the evaluator is not required (nor is it feasible) to test all possible compositions of passwords, the evaluator shall ensure that all characters, rule characteristics, and a minimum length listed in the requirement are supported, and justify the subset of those characters chosen for testing.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Authenticate to the TOE via the CLI and execute the following command: user create user test2 access-level admin echoless-password 2. Enter Password: abcdefghijklmnopqrstuvwxyzA12! 3. Verify Password: abcdefghijklmnopqrstuvwxyzA12! 4. Login with the user and password abcdefghijklmnopqrstuvwxyzA12! 5. Confirm the user password is accepted 6. Repeat steps 1-5 with test3 and password BCDEFGHIJKLMNOPQRSTUVWXYZa345@ 7. Repeat steps 1-5 with test4 and password aA67890#$%^&*() 8. Repeat steps 1-5 with test5 and password abcdefghijklA1! 9. Repeat steps 1-5 with test6 and password bcdefghijklA1! 10. This time the password is rejected 11. Take screen shots of the configuration and login attempts
Test Results	Pass
Execution Method	Manual

Test Case Number	040
SFR	FIA_UAU.7
Test Objective	Test 1: The evaluator shall locally authenticate to the TOE. While making this attempt, the evaluator shall verify that at most obscured feedback is provided while entering the authentication information
Test Instructions	Execute this test per the test steps.
Test Steps	1. Login to the TOE over the local console connection via the serial port 2. Ensure the password is obscured (Not shown on the terminal)
Test Results	Pass
Execution Method	Manual

Test Case Number	041
SFR	FIA_UIA_EXT.1
Test Objective	Test 1: The evaluator shall use the guidance documentation to configure the appropriate credential supported for the login method. For that credential/login method, the evaluator shall show that providing correct I&A information results in the ability to access the system, while providing incorrect information results in denial of access
Test Instructions	Execute this test per the test steps.
Test Steps	See Tests 16 and 17 for SSH public key authentication LOCAL CONSOLE via SERIAL 1. If needed create a user using the following command 2. User create user test1 access-level admin echoless-password Enter Password: Verify Password: 3. Login in via the local console screen over the serial connection using a valid username and password 4. Take a screenshot showing the successful login attempt 5. Exit from the local console 6. Save the audit record 7. Login in via the local console using a valid username and invalid password 8. Take a screenshot showing the unsuccessful login attempt. 9. Save the audit record 10. Login in via the local console using an invalid username and invalid password 11. Take a screenshot showing the unsuccessful login attempt. 12. Save the audit record 13. Login in via the local console using an invalid username and valid password 14. Take a screenshot showing the unsuccessful login attempt. 15. Save the audit record REMOTE via SSH 16. Login via the remote SSH connection using a valid username and password 17. Take a screenshot showing the successful login attempt 18. Save the audit record 19. Exit from the CLI.

	20. Login via the remote SSH connection using a valid username and invalid password 21. Take a screenshot showing the successful login attempt 22. Save the audit record 23. Login via the remote SSH connection using an invalid username and invalid password 24. Take a screenshot showing the successful login attempt 25. Save the audit record 26. Login via the remote SSH connection using an invalid username and valid password 27. Take a screenshot showing the successful login attempt 28. Save the audit record 29. Login via the remote SSH connection using an invalid username and valid password 30. Take a screenshot showing the successful login attempt 31. Save the audit record REMOTE via SSH using RADIUS Server Authentication 32. Enable RADIUS server authentication 33. Login via the remote SSH connection using a valid username and password 34. Take a screenshot showing the successful login attempt 35. Save the audit record 36. Exit from the CLI. 37. Login via the remote SSH connection using a valid username and invalid password 38. Take a screenshot showing the successful login attempt 39. Save the audit record 40. Login via the remote SSH connection using an invalid username and invalid password 41. Take a screenshot showing the successful login attempt 42. Save the audit record 43. Login via the remote SSH connection using an invalid username and valid password 44. Take a screenshot showing the successful login attempt 45. Save the audit record 46. Login via the remote SSH connection using an invalid username and valid password 47. Take a screenshot showing the successful login attempt 48. Save the audit record
Test Results	Pass
Execution Method	Manual

Test Case Number	042
SFR	FIA_UIA_EXT.1
Test Objective	Test 2: The evaluator shall configure the services allowed (if any) according to the guidance documentation, and then determine the services available to an external remote entity. The evaluator shall determine that the list of services available is

	limited to those specified in the requirement.
Test Instructions	Execute this test per the test steps.
Test Steps	REMOTE via SSH 1. Login to the TOE and run the command: system shell banner create banner login line Warning! 2. Exit from the TOE 3. Use bitvise to login remotely using SSH and take a screenshot to show that the login banner is the only service that was run prior to login. 4. Save the audit record showing the banner configuration and login attempt 5. Use bitvise to login remotely using SSH with username=”show version” and password=”show version” 6. Save the audit record showing the banner configuration and login attempt
Test Results	Pass
Execution Method	Manual

Test Case Number	043
SFR	FIA_UIA_EXT.1
Test Objective	Test 3: For local access, the evaluator shall determine what services are available to a local administrator prior to logging in, and make sure this list is consistent with the requirement
Test Instructions	Execute this test per the test steps.
Test Steps	1. If the banner is not created, create it using the command: system shell banner create banner login line Warning 2. Login to the TOE via the local console and verify that only the banner service is available. 3. Save the audit record showing the banner configuration and login attempt 4. Login to the TOE via the local console using username=”show version” and password “show version”
Test Results	Pass
Execution Method	Manual

Test Case Number	044
SFR	FIA_X509_EXT.1
Test Objective	Test 1a: The evaluator shall load a valid chain of certificates (terminating in a trusted CA certificate) as needed to validate the certificate to be used in the function, and shall use this chain to demonstrate that the function succeeds. Test 1b: The evaluator shall then delete one of the certificates in the chain (i.e. the root CA certificate or other intermediate certificate, but not the end-entity certificate), and show that the function fails.
Test Instructions	Execute this test per the test steps.
Test Steps	**TOE as client:** **This test is performed in FCS_TLSC_EXT.2.3 - Test Case 036.**

	TOE as server: 1. On the TOE, disable all SSH public key algorithms except for x509v3-ecdsa-sha2-nistp256 2. Generate an ECDSA public key on the client system (e.g. ssh-keygen -t ecdsa -b 256) 3. Generate CSR on the client system 4. Sign client CSR on the client system 5. Generate an ID file by concatenating the ECDSA public key with the signed certificate 6. Run the command on the SSH client to connect to the TOE using the X.509 algorithm and observe the connection succeeds. 7. On the TOE run command to break the certificate chain 8. Repeat step 6 and observe that a password prompt is issued because certificate validation failed
Test Results	Pass
Execution Method	Manual

Test Case Number	045
SFR	FIA_X509_EXT.1
Test Objective	Test 2: The evaluator shall demonstrate that validating an expired certificate results in the function failing.
Test Instructions	Execute this test per the test steps.
Test Steps	[Assumption: Root CA, Intermediate01, Intermediate02 certificates are in the Trusted Certificate store.] **TOE as client:** 1. Load the expired X.509v3 Server certificate onto the environmental entity. 2. Connect the TOE to the environmental entity (the connection will fail because an expired certificate is sent from the environmental entity to the TOE). **TOE as server:** [Assumption: test 044 has already been conducted] 1. Change the date on the TOE to a time after the client certificate has expired (in the sample steps in test 044 the client certificate was configured to live for a year) using ‘system set date’ 2. Run the command on the SSH client to connect to the TOE using the X.509 algorithm and observe the certificate fails to be validated.
Test Results	Pass
Execution Method	Manual

Test Case Number	046
SFR	FIA_X509_EXT.1
Test Objective	Test 3: The evaluator shall test that the TOE can properly handle revoked certificates–conditional on whether CRL or OCSP is selected; if both are selected, then a test shall be performed for each method. The evaluator shall test revocation of the TOE certificate and revocation of the TOE intermediate CA certificate i.e. the intermediate CA certificate should be revoked by the root CA. The evaluator

	shall ensure that a valid certificate is used, and that the validation function succeeds. The evaluator then attempts the test with a certificate that has been revoked (for each method chosen in the selection) to ensure when the certificate is no longer valid that the validation function fails.
Test Instructions	Execute this test per the test steps.
Test Steps	[Assumption: Root CA, Intermediate01, Intermediate02 certificates are in the Trusted Certificate store.] **TOE as client:** **OCSP** 1. Load a valid server certificate onto the environmental entity. 2. Begin capturing packets using Wireshark between the TOE and the environmental entity. 3. Create a connection between the TOE and the environmental entity. (The connection will succeed.) 4. Stop capturing packets between the TOE and the environmental entity. 5. Load an OCSP revoked certificate onto the environmental entity. 6. Begin capturing packets using Wireshark between the TOE and the environmental entity. 7. Create a connection between the TOE and the environmental entity. (e.g. Disable and then enable the syslog tls client on the TOE by executing the following commands: syslog tls disable syslog tls enable (The connection will fail because the server certificate is revoked.) 8. Stop capturing packets between the TOE and the environmental entity. 9. Load a valid server certificate onto the environmental entity. 10. Load an OCSP revoked intermediate01 certificate onto the TOE by performing the steps under “Install CA Certificate” in Section 5. 11. Begin capturing packets using Wireshark between the TOE and the environmental entity. 12. Create a connection between the TOE and the environmental entity. (The connection will fail because the intermediate01 certificate is revoked.) 13. Stop capturing packets between the TOE and the environmental entity. **TOE as server:** [Assumption: test 044 has already been conducted] 1. On the OCSP server, revoke the client certificate (the one that is used as an input to the .id file) 2. Run the command on the SSH client to connect to the TOE using the X.509 algorithm and observe that certificate validation fails 3. On the OCSP server, unrevoke client certificate 4. On the OCSP server, revoke the intermediate02 certificate 5. Re-attempt step 2 and observe that certificate validation still fails
Test Results	Pass

Execution Method	Manual

Test Case Number	047
SFR	FIA_X509_EXT.1
Test Objective	Test 4: If OCSP is selected, the evaluator shall configure the OCSP server or use a man-in-the-middle tool to present a certificate that does not have the OCSP signing purpose and verify that validation of the OCSP response fails. If CRL is selected, the evaluator shall configure the CA to sign a CRL with a certificate that does not have the cRLsign key usage bit set, and verify that validation of the CRL fails
Test Instructions	Execute this test per the test steps.
Test Steps	**OCSP** **TOE as client:** 1. Load a certificate on the OCSP server containing the OCSP signing purpose. 2. Begin capturing packets using Wireshark between the TOE and the environmental entity. 3. Cause the TOE to establish a connection to the environmental entity. 4. Stop capturing packets with Wireshark between the TOE and the environmental entity. 5. Load a certificate without the OCSP signing purpose used for signing OCSP responses onto the OCSP server. 6. Repeat Steps 2-4. 7. The connection should fail because the OCSP response could not be validated. **TOE as server:** [Assumption: test 044 and the 'TOE as client' step above has already been conducted] This test is executed in the same manner as the 'TOE as client' case above. Repeat the SSH connection attempt described in test 044 while the OCSP server is configured in such a way that its responses are not considered to be valid OCSP responses.
Test Results	Pass
Execution Method	Manual

Test Case Number	048
SFR	FIA_X509_EXT.1
Test Objective	Test 5: The evaluator shall modify any byte in the first eight bytes of the certificate and demonstrate that the certificate fails to validate. (The certificate will fail to parse correctly.)
Test Instructions	Execute this test per the test steps.
Test Steps	1. Begin capturing packets between the TOE and the environmental entity. 2. Execute the modification program on the test machine. 3. Cause the TOE to initiate a connection to the environmental entity. 4. Stop capturing packets between the TOE and the environmental entity. 5. The connection will fail because the certificate will fail to validate. **TOE as server:**

	This test is not applicable when the TOE is acting as an SSH server. The test system's SSH client will fail to parse the ID file as containing a valid X.509 certificate so it will not be sent to the TOE for validation. It is not possible to modify this in transit because the certificate is not transmitted until after the SSH key establishment has occurred so any certificate exchange will be encrypted.
Test Results	Pass
Execution Method	Manual

Test Case Number	049
SFR	FIA_X509_EXT.1
Test Objective	Test 6: The evaluator shall modify any byte in the last byte of the certificate and demonstrate that the certificate fails to validate. (The signature on the certificate will not validate.)
Test Instructions	Execute this test per the test steps.
Test Steps	1. Begin capturing packets between the TOE and the environmental entity. 2. Execute the modification program on the test machine. 3. Cause the TOE to initiate a connection to the environmental entity. 4. Stop capturing packets between the TOE and the environmental entity. 5. The connection will fail because the certificate will fail to validate. **TOE as server:** [Assumption: test 044 has already been conducted] 1. Modify the ID file such that the last byte of the client PEM certificate is modified. 2. Run the command on the SSH client to connect to the TOE using the X.509 algorithm.
Test Results	Pass
Execution Method	Manual

Test Case Number	050
SFR	FIA_X509_EXT.1
Test Objective	Test 7: The evaluator shall modify any byte in the public key of the certificate and demonstrate that the certificate fails to validate. (The hash of the certificate will not validate.)
Test Instructions	Execute this test per the test steps.
Test Steps	1. Begin capturing packets between the TOE and the environmental entity. 2. Execute the modification program on the test machine. 3. Cause the TOE to initiate a connection to the environmental entity. 4. Stop capturing packets between the TOE and the environmental entity. 5. The connection will fail because the certificate will fail to validate. **TOE as server:** This test is not applicable when the TOE is acting as an SSH server. The test system's SSH client will fail to parse the ID file as containing a valid X.509 certificate so it will not be sent to the TOE for validation. It is not possible to modify this in transit because the certificate is not transmitted until after the SSH key establishment has occurred so any certificate exchange will be encrypted.
Test Results	Pass

Execution Method	Manual

Test Case Number	051
SFR	FIA_X509_EXT.1
Test Objective	Test 1: The evaluator shall construct a certificate path, such that the certificate of the CA issuing the TOE's certificate does not contain the basicConstraints extension. The validation of the certificate path fails.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Authenticate to the TOE via the CLI. 2. Attempt to load the invalid CA certificate onto the TOE. 3. The validation of the invalid CA certificate should fail.
Test Results	Pass
Execution Method	Manual

Test Case Number	052
SFR	FIA_X509_EXT.1
Test Objective	Test 2: The evaluator shall construct a certificate path, such that the certificate of the CA issuing the TOE's certificate has the cA flag in the basicConstraints extension set to FALSE. The validation of the certificate path fails.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Authenticate to the TOE via the CLI. 2. Attempt to load the invalid CA certificate onto the TOE. 3. The validation of the invalid CA certificate should fail.
Test Results	Pass
Execution Method	Manual

Test Case Number	053
SFR	FIA_X509_EXT.1
Test Objective	Test 3: The evaluator shall construct a certificate path, such that the certificate of the CA issuing the TOE's certificate has the cA flag in the basicConstraints extension set to TRUE. The validation of the certificate path succeeds
Test Instructions	Execute this test per the test steps.
Test Steps	1. Load a valid server certificate onto the server which chains to the CA certificates on the TOE. 2. Connect the TOE to the environmental entity (this connection succeeds).
Test Results	Pass
Execution Method	Manual

Test Case Number	054
SFR	FIA_X509_EXT.2
Test Objective	The evaluator shall perform the following test for each trusted channel: The evaluator shall demonstrate that using a valid certificate that requires certificate validation checking to be performed in at least some part by communicating with a non-TOE IT entity. The evaluator shall then manipulate the environment so that the TOE is unable to verify the validity of the certificate, and observe that the action selected in FIA_X509_EXT.2.2 is performed. If the selected action is

	administrator-configurable, then the evaluator shall follow the guidance documentation to determine that all supported administrator-configurable options behave in their documented manner
Test Instructions	Execute this test per the test steps.
Test Steps	1. Ensure that the OCSP server is up and running. 2. Begin capturing packets using Wireshark between the TOE and the environmental entity. 3. Perform some activity on the TOE that causes the TOE to check the validation of the certificate. 4. Stop capturing packets using Wireshark between the TOE and the environmental entity. 5. Verify that the TOE accepts the certificate. 6. Shutdown the OCSP server. 7. Repeat Steps 1-4. 8. Verify that the denies the certificate.
Test Results	Pass
Execution Method	Manual

Test Case Number	055
SFR	FIA_X509_EXT.3
Test Objective	Test 1: The evaluator shall use the guidance documentation to cause the TOE to generate a certificate request message. The evaluator shall capture the generated message and ensure that it conforms to the format specified. The evaluator shall confirm that the certificate request provides the public key and other required information, including any necessary user-input information.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Authenticate to the TOE via CLI. 2. Execute the following command to generate a CSR: radsec certificate csr generate key-type rsa2048 filename rc.cnf sftp-server 10.41.71.104 login-id ciena echoless-password 3. The TOE will generate a CSR based on the supplied config file data which contains the Common Name, Organization, Organizational Unit, and Country information.
Test Results	Pass
Execution Method	Manual

Test Case Number	056
SFR	FIA_X509_EXT.3
Test Objective	Test 2: The evaluator shall demonstrate that validating a certificate response message without a valid certification path results in the function failing. The evaluator shall then load a certificate or certificates as trusted CAs needed to validate the certificate response message, and demonstrate that the function succeeds. The evaluator shall then delete one of the certificates, and show that the function fails.
Test Instructions	Execute this test per the test steps.
Test Steps	This test is performed in conjunction with FIA_X509_EXT.1 Test 1 - Test Case 044.

Test Results	Pass
Execution Method	Manual

4.4.4 Security Management

Test Case Number	057
SFR	FMT_MOF.1/TrustedUpdate
Test Objective	The evaluator shall try to perform the update using a legitimate update image without prior authentication as security administrator (either by authentication as a user with no administrator privileges or without user authentication at all – depending on the configuration of the TOE). This test should fail. The evaluator shall try to perform the update with prior authentication as security administrator using a legitimate update image. This test should pass. This test case should be covered by the tests for FPT_TUD_EXT.1 already.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Create a user with the Limited privilege level user create user <userLimited> access-level limited password <string> 2. Logout 3. Login as userLimited 4. Try to run the software install command 5. This will fail 6. Logout 7. Login as the Admin user 8. Run the software install command 9. This will succeed
Test Results	Pass
Execution Method	Manual

Test Case Number	058
SFR	FMT_MOF.1(1)/Audit
Test Objective	The evaluator shall try to modify all parameters for configuration of the transmission protocol for transmission of audit data to an external IT entity without prior authentication as security administrator (either by authentication as a user with no administrator privileges or without user authentication at all – depending on the configuration of the TOE). This test should fail. The evaluator shall try to modify all parameters for configuration of the transmission protocol for transmission of audit data to an external IT entity with prior authentication as security administrator. The effects of the modifications should be confirmed. The evaluator does not necessarily have to test all possible values of all parameters for configuration of the transmission protocol for transmission of audit data to an external IT entity but at least one allowed value per configurable parameter.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Login as a user with Admin role 2. Attempt to configure each of the SFTP protocol parameters used to send

	audit records to the remote audit server 3. This test will fail. An Admin user does not have the right privilege level 4. Attempt to configure the TLS parameters used to send audit records to the syslog server 5. This test will fail 6. Save off the audit logs for both failed attempts 7. Logout 8. Login as a user with Super role 9. Configure each of the SFTP protocol parameters used to send audit records to the remote audit server 10. Verify that the configuration changes have been accepted 11. This test will succeed 12. Configure each of the TLS parameters used to send audit data to the syslog server 13. Verify the configuration changes have been accepted 14. This test will succeed 15. Save off the audit logs for both successful attempts
Test Results	Pass
Execution Method	Manual

Test Case Number	059
SFR	FMT_MOF.1/LocSpace
Test Objective	The evaluator shall try to perform at least one of the related actions without prior authentication as security administrator (either by authentication as a user with no administrator privileges or without user authentication at all – depending on the configuration of the TOE). These attempts should fail. The evaluator shall try to perform at least one of the related actions with prior authentication as security administrator. These attempts should succeed.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Logon as a user with Admin role 2. Perform an action that modifies the behavior of the audit functionality when the local audit storage space is full 3. Logout 4. The test will fail 5. Login as a user with Super role 6. Perform an action that modifies the behavior of the audit functionality when the local audit storage space is full 7. Logout 8. The test will succeed
Test Results	Pass
Execution Method	Manual

Test Case Number	060
SFR	FMT_MTD.1/AdminAct
Test Objective	The evaluator shall try to perform at least one of the related actions without prior authentication as security administrator (either by authentication as a user with no administrator privileges or without user authentication at all – depending on the configuration of the TOE). This test should fail. The evaluator shall try to perform at least one of the related actions with prior

	authentication as security administrator. This test should pass
Test Instructions	Execute this test per the test steps.
Test Steps	1. Login as a user with Limited role 2. Attempt to enable or disable SSH 3. This attempt will fail 4. Logout 5. Login as a user with the Admin role 6. Attempt to enable or disable SSH 7. This attempt will succeed 8. Logout 9. Save off all audit records and take screenshots
Test Results	Pass
Execution Method	Manual

Test Case Number	061
SFR	FMT_SMF.1
Test Objective	The security management functions for FMT_SMF.1 are distributed throughout the cPP and are included as part of the requirements in FTA_TAB.1, FTA_SSL.3, FTA_SSL.4, FMT_MOF.1(1)/TrustedUpdate, FMT_MOF.1(2)/TrustedUpdate (if included in the ST), FIA_X509_EXT.2.2 & FPT_TUD_EXT.2.2 (if included in the ST and if they include an administrator-configurable action), FMT_MOF.1(1)/Audit, FMT_MOF.1(2)/Audit, FMT_MOF.1.1(1)/AdminAct, FMT_MOF.1.1(2)/AdminAct and FMT_MOF.1/LocSpace (for all of these SFRs that are included in the ST), FMT_MTD, FPT_TST_EXT, and any cryptographic management functions specified in the reference standards. Compliance to these requirements satisfies compliance with FMT_SMF.1.
Test Instructions	Execute this test per the test steps.
Test Steps	This test is satisfied by testing performed throughout the evaluation.
Test Results	Pass
Execution Method	Manual

Test Case Number	062
SFR	FMT_SMR.2
Test Objective	In the course of performing the testing activities for the evaluation, the evaluator shall use all supported interfaces, although it is not necessary to repeat each test involving an administrative action with each interface. The evaluator shall ensure, however, that each supported method of administering the TOE that conforms to the requirements of this cPP be tested; for instance, if the TOE can be administered through a local hardware interface; SSH; and TLS/HTTPS; then all three methods of administration must be exercised during the evaluation team's test activities
Test Instructions	Execute this test per the test steps.
Test Steps	1. Verify that all supported methods of administering the TOE have been tested by other means.
Test Results	Pass
Execution Method	Manual

4.4.5 Protection of the TSF

Test Case Number	063
SFR	FPT_STM.1
Test Objective	Test 1: The evaluator uses the guidance documentation to set the time. The evaluator shall then use an available interface to observe that the time was set correctly.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Disable NTP (ntp delete) or verify that it is not configured or running. 2. Run the command: system show date time 3. Run the command: system set date <yy-mm-dd> time <hh:mm:ss> 4. Run the command: system show date time 5. Take screen shots and save the audit records
Test Results	Pass
Execution Method	Manual

Test Case Number	065
SFR	FPT_TST_EXT.1
Test Objective	Future versions of this cPP will mandate a clearly defined minimum set of self tests. But also for this version of the cPP it is expected that at least the following tests are performed: a) Verification of the integrity of the firmware and executable software of the TOE b) Verification of the correct operation of the cryptographic functions necessary to fulfill any of the SFRs. Although formal compliance is not mandated, the self tests performed should aim for a level of confidence comparable to: a) FIPS 140-2, chap. 4.9.1, Software/firmware integrity test for the verification of the integrity of the firmware and executable software. b) FIPS 140-2, chap. 4.9.1, Cryptographic algorithm test for the verification of the correct operation of cryptographic functions. Alternatively, national requirements of any CCRA member state for the security evaluation of cryptographic functions should be considered as appropriate. The evaluator shall verify that the self tests described above are either carried out during initial start-up and that the developer has justified any deviation from this (if applicable).
Test Instructions	Execute this test per the test steps.
Test Steps	1. Verify that the integrity of the firmware/software is performed at startup 2. Verification of the correct operation of the cryptographic functions during startup. This could be achieved if the TOE uses a FIPS validated cryptographic module which includes a series of KATs and conditional tests. The crypto module also does a self-check but the requirement in 1. Is that all of the software has an integrity test on it not just the crypto module.
Test Results	Pass
Execution Method	Manual

Test Case Number	066

SFR	FPT_TUD_EXT.1
Test Objective	Test 1: The evaluator performs the version verification activity to determine the current version of the product as well as the most recently installed version (should be the same version before updating). The evaluator obtains a legitimate update using procedures described in the guidance documentation and verifies that it is successfully installed on the TOE. For some TOEs loading the update onto the TOE and activation of the update are separate steps ('activation' could be performed e.g. by a distinct activation step or by rebooting the device). In that case the evaluator verifies after loading the update onto the TOE but before activation of the update that the current version of the product did not change but the most recently installed version has changed to the new product version. After the update, the evaluator performs the version verification activity again to verify the version correctly corresponds to that of the update and that current version of the product and most recently installed version match again.
Test Instructions	Execute this test per the test steps.
Test Steps	Test using the update server 1. Perform a version check prior to the update by running the following command: Software show 2. Turn on software signing mode: system security set software-signing-mode on 3. To install and activate the package after the next reboot/restart run the following command: software install package-path saos-08-05/rel_saos8700_8.5.0_ga223.tgz sftp-server 10.41.71.100 login-id ciena echoless-password 4. software forced-upgrade package rel_saos8700_8.5.0_ga223 5. Note software validation always occurs on both banks 5 minutes after boot but it can be run manually by running the software validate command 6. Note the software activate command will activate the software 7. Run the following command to show the new version is being used Software show
Test Results	Pass
Execution Method	Manual

Test Case Number	067
SFR	FPT_TUD_EXT.1
Test Objective	Test 2: The evaluator performs the version verification activity to determine the current version of the product as well as the most recently installed version (should be the same version before updating). The evaluator obtains or produces illegitimate updates as defined below, and attempts to install them on the TOE. The evaluator verifies that the TOE rejects all of the illegitimate updates. The evaluator performs this test using all of the following forms of illegitimate updates: 1) A modified version (e.g. using a hex editor) of a legitimately signed update (if digital signatures are used) or a version that does not match the published hash (if published hashes are used) 2) An image that has not been signed (if digital signatures are used) or an image without published hash (if published hashes are used) 3) An image signed with an invalid signature (e.g. by using a different key as expected for creating the signature or by manual modification of a legitimate signature) (only if digital signatures are used).

	4) The handling of version information of the most recently installed version might differ between different TOEs. Depending on the point in time when the attempted update is rejected, the most recently installed version might or might not be updated. The evaluator shall verify that the TOE handles the most recently installed version information for that case as described in the guidance documentation. After the TOE has rejected the update the evaluator shall verify, that both, current version and most recently installed version, reflect the same version information as prior to the update attempt. The evaluator shall perform the Tests 1 and 2 for all methods supported (manual updates, automatic checking for updates, automatic updates).
Test Instructions	Execute this test per the test steps.
Test Steps	1. Test using the update server 2. Perform a version check prior to attempting to install an illegitimate update and notate the version. Software show 3. Obtain an image and modify it using a Hex Editor 4. Put the modified image on the SFTP server 5. To install and activate the package after the next reboot/restart issue the software install command specifying the package-path as the path to the modified image. 6. The software installation should fail to install 7. This will test the validity of the digital signature. 8. Perform a version check after attempting to install an illegitimate update and verify that the version number did not change. Software show 9. Repeat the test steps 1-8 using an image without a digital signature 10. This will also be rejected by the system 11. Repeat the test steps 1-8 using an image where the correct digital signature has been modified 12. This will also be rejected by the system 13. For each of these 3 tests verify the version before and after the test are the same.
Test Results	Pass
Execution Method	Manual

4.4.6 TOE Access

Test Case Number	068
SFR	FTA_SSL_EXT.1
Test Objective	The evaluator follows the guidance documentation to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a local interactive session with the TOE. The evaluator then observes that the session is either locked or terminated after the configured time period. If locking was selected from the component, the evaluator then ensures that reauthentication is needed when trying to unlock the session.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Test using the local console connection over the serial port 2. Login to the TOE using the local console port

	3. Run the commands: system shell set global-inactivity-timer on system shell set global-inactivity-timeout 3 4. Exit the TOE 5. Login to the TOE again and run the show time command 6. Wait for 3 minutes 7. Take a snapshot of the screen showing the inactivity terminated the session to show that 3 minutes elapsed 8. Repeat steps 2-7 using 5 minutes and 7 minutes
Test Results	Pass
Execution Method	Manual

Test Case Number	069
SFR	FTA_SSL.3
Test Objective	The evaluator follows the guidance documentation to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a remote interactive session with the TOE. The evaluator then observes that the session is terminated after the configured time period.
Test Instructions	Execute this test per the test steps.
Test Steps	REMOTE via SSH 1. Login to the TOE from the client using Bitvise and using SSH 2. Run the command: System shell set global-inactivity-timer on system shell set global-inactivity-timeout 3 3. Exit the TOE 4. Login to the TOE again and run the show time command 5. Wait for 3 minutes 6. Take a snapshot of the screen showing the inactivity terminated the session to show that 3 minutes elapsed 7. Repeat steps 2-7 using 5 minutes and 7 minutes
Test Results	Pass
Execution Method	Manual

Test Case Number	070
SFR	FTA_SSL.4
Test Objective	The evaluator initiates an interactive local session with the TOE. The evaluator then follows the guidance documentation to exit or log off the session and observes that the session has been terminated.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Login using the local serial port connection 2. Run the exit command 3. Take a screenshot showing the user logged off
Test Results	Pass
Execution Method	Manual

Test Case Number	071
SFR	FTA_SSL.4
Test Objective	The evaluator initiates an interactive remote session with the TOE. The evaluator then follows the guidance documentation to exit or log off the session and observes that the session has been terminated.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Login to the TOE via SSH 2. Run the exit command 3. Take a snapshot showing the user logged off
Test Results	Pass
Execution Method	Manual

Test Case Number	072
SFR	FTA_TAB.1
Test Objective	The evaluator follows the guidance documentation to configure a notice and consent warning message. The evaluator shall then, for each method of access specified in the TSS, establish a session with the TOE. The evaluator shall verify that the notice and consent warning message is displayed in each instance.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Login via the local console connection via the serial port 2. Run the command: system shell banner create banner login line Warning!! 3. Run the exit command 4. Login over the local console connection via the serial port 5. Take a snapshot of the screen and verify the banner is displayed 6. Login over the Remote SSH connection and verify the banner is displayed. 7. Take a snapshot of the screen 8. Run the exit command 9. Verify Limited and Admin users cannot configure the banner but Super can.
Test Results	Pass
Execution Method	Manual

4.4.7 Trusted Path/Channels

Test Case Number	073
SFR	FTP_ITC.1
Test Objective	The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.
Test Instructions	Execute this test per the test steps.
Test Steps	Test SFTP between the TOE and the SFTP Update Server 1. Start Wireshark packet capture between the TOE and the SFTP Update Server 2. To install the package but not activate it, run the following command:

	software download package-path rel_saos8700_8.5.0_ga215.tgz destination-path rel_saos8700_8.5.0_ga215.tgz sftp-server 10.41.71.100 login-id ciena 3. Run the following command to show that the update has been pulled from the server and stored in the update bank: Software show 4. Stop the Wireshark packet capture NOTE: The SFTP server is used for the storage of audit records as well as being the update server. Testing the secure SSH communications while transferring audit records was completed while testing FAU_STG_EXT.1 (TEST002). NOTE: The syslog server is used for the storage of audit records. Testing of the secure TLS communications while transferring audit records to the syslog server was completed while testing FAU_STG_EXT.1.
Test Results	Pass
Execution Method	Manual

Test Case Number	074
SFR	FTP_ITC.1
Test Objective	For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the guidance documentation to ensure that in fact the communication channel can be initiated from the TOE
Test Instructions	Execute this test per the test steps.
Test Steps	This requirement is satisfied by the testing of FAU_STG_EXT.1 and FPT_TUD_EXT.1.
Test Results	Pass
Execution Method	Manual

Test Case Number	075
SFR	FTP_ITC.1
Test Objective	The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data are not sent in plaintext.
Test Instructions	Execute this test per the test steps.
Test Steps	This requirement is satisfied by the testing of FAU_STG_EXT.1 (Test002) and FTP_ITC.1 (Test 073)
Test Results	Pass
Execution Method	Manual

Test Case Number	076
SFR	FTP_ITC.1
Test Objective	The evaluators shall, for each protocol associated with each authorized IT entity tested during test 1, the connection is physically interrupted. The evaluator shall ensure that when physical connectivity is restored, communications are appropriately protected.

Test Instructions	Execute this test per the test steps.
Test Steps	Test SFTP between the TOE and the audit server 1. Start Wireshark packet capture between the TOE and the SFTP audit server 2. If the TOE is not configured to send logs to the SFTP audit server then configure it to do so. 3. Perform some auditable events 4. Transfer the logs to the SFTP server using: 5. While the transfer is taking place, physically disconnect the connection and reconnect it. 6. Stop and save the packet capture 7. Take a screenshot of the encrypted packets. Verify there are no packets in plaintext and the communications is protected. 8. Verify the audit data has been received on the sftp server. Take a screenshot showing the data has been received. 9. Save a copy of the audit records Test SFTP between the TOE and the SFTP Update Server 10. Run software show command 11. Start Wireshark packet capture between the TOE and the SFTP Update Server 12. To install the package but not activate it, run the software install command and specify a valid update on the SFTP server using the package-path parameter. 13. While the transfer is taking place, physically disconnect the connection and reconnect it. 14. Run the software show command to show the configuration information. 15. Stop the Wireshark packet capture and verify that no packets were sent in plaintext. 16. Test TLS between the TOE and the syslog server 17. Start Wireshark packet capture between the TOE and the syslog server 18. Perform some auditable events 19. While the transfer is taking place, physically disconnect the connection and reconnect it 20. Stop Wireshark and verify that no packets were sent in plaintext.
Test Results	Pass
Execution Method	Manual

Test Case Number	077
SFR	FTP_TRP.1
Test Objective	The evaluators shall ensure that communications using each specified (in the guidance documentation) remote administration method is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.
Test Instructions	Execute this test per the test steps.
Test Steps	This test is satisfied by testing performed in FCS_SSHS_EXT.1.

Test Results	Pass
Execution Method	Manual

Test Case Number	078
SFR	FTP_TRP.1
Test Objective	For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the guidance documentation to ensure that in fact the communication channel can be initiated from the TOE.
Test Instructions	Execute this test per the test steps.
Test Steps	This test is satisfied by testing performed in FCS_SSHS_EXT.1.
Test Results	Pass
Execution Method	Manual

Test Case Number	079
SFR	FTP_TRP.1
Test Objective	The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Start Wireshark packet capture between the TOE and the SSH client. 2. Connect to the TOE using SSH. 3. Run the following command: software show 4. Stop the packet capture 5. Search for the encrypted SSH packets between the client and the TOE in the Wireshark capture. 6. Take a screenshot to show they are encrypted. 7. Save the packet capture.
Test Results	Pass
Execution Method	Manual

Test Case Number	080
SFR	FTP_TRP.1
Test Objective	The evaluators shall ensure that, for each protocol associated with each authorized IT entity tested during test 1, the connection is physically interrupted. The evaluator shall ensure that when physical connectivity is restored, communications are appropriately protected.
Test Instructions	Execute this test per the test steps.
Test Steps	1. Start Wireshark packet capture between the TOE and the SSH client. 2. Connect to the TOE using SSH. 3. Run the following command: software show 4. While this command is running physically disconnect the connection and reconnect it. 5. Stop the packet capture. 6. Search for the encrypted SSH packets between the client and the TOE in the Wireshark capture. 7. Take a screenshot to show they are encrypted. 8. Save the packet capture.
Test Results	Pass
Execution Method	Manual

4.5 Vulnerability Testing

The evaluation team created a set of vulnerability tests to attempt to subvert the security of the TOE. These tests were created based upon the evaluation team's review of the vulnerability analysis evidence and independent research. The evaluation team conducted searches for public vulnerabilities related to the TOE. A few notable resources consulted include securityfocus.com, the cve.mitre.org, and the nvd.nist.gov.

The following keywords were used individually and as part of various permutations and combinations to search for vulnerabilities identified in the public domain:

Keyword	Description
Ciena	This is a generic term for searching for known vulnerabilities produced by the company as a whole.
Packetwave	This is a generic term for searching for known vulnerabilities for the specific product.
8700	This is a generic term for searching for known vulnerabilities for specific model of the specific product line.
SAOS	This is a generic term for searching for known vulnerabilities produced by the software operating system.
OpenSSL	A specific version was not included in the search because this version may be within a range of vulnerable operating system versions and not listed separately

Table 4-1: Vulnerability Keywords

The TOE handles a large number of network protocols. However, any vulnerability that may be present in the TOE’s implementation of these protocols will also show up in a product-specific search (e.g. “A vulnerability in the Ciena 8700 Series implementation of TFTP may allow a remote attacker to…”). Therefore, searches for the specific protocols were not performed.

Upon the completion of the vulnerability analysis research, the team had identified several generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration.

All search activities were conducted in April 2017, prior to the execution of the vulnerability testing activities.

The team tested the following areas:

- Port Scanning
  Remote access to the TOE should be limited to the standard TOE interfaces and procedures. This test enumerates network port and service information to determine if any ports were open and running services outside of the TOE standard configuration.
- CLI Privilege Escalation
  The TSF should not disclose authentication data to unprivileged users that allows a user to successfully impersonate another user who has a greater degree of privilege to manage the TOE.
- Force SSHv1
  This attack determines if the client will accept both SSHv1 and SSHv2 connections when the TOE claims to only support SSHv2
- Fuzzing – Mutated TYPE and CODE
  This test determines if the TOE is adversely affected by the handling of large number of mutated IPv4, IPv6, ICMPv4, and ICMPv6 packets.
- Fuzzing – Mutated remaining field
  This test determines if the TOE is adversely affected by the handling of large number of mutated IPv4 and IPv6 packets where the header fields are carefully mutated to represent boundary cases, significant values, and randomly chosen values.

The TOE successfully prevented any attempts of subverting its security.

5 Conclusions

The TOE was found to exhibit security functional behavior consistent with its claimed Protection Profile. The TOE's related documentation was found to adequately define the scope of the TSF and instructions for its usage in a manner that was subsequently verified through functional testing. The TOE did not exhibit any obvious vulnerabilities that would adversely affect its ability to implement its security functionality.

6 Glossary of Terms

Acronym	Definition
AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CLI	Command Line Interface
CSP	Critical Security Parameter
DHE	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
HMAC	Hashed Message Authentication Code
MCLI	Management Command Line Interface
MPLS	Multiprotocol Label Switching
NDcPP	Network Device collaborative Protection Profile
NTP	Network Time Protocol
OSI	Open Systems Interconnection
OTN	Optical Transport Network
RSA	Rivest Shamir Adelman (encryption algorithm)
SDH	Synchronous Digital Hierarchy
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SONET	Synchronous Optical Networking
SSH	Secure Shell
TL1	Transaction Language One

Table 6-1: Acronyms

Terminology	Definition
Authorized Administrator	Any user which has been assigned to a privilege level that is permitted to perform all TSF-related functions.
Role	An assigned role gives a user varying access to the management of the TOE.
Security Administrator	Synonymous with Authorized Administrator for the purposes of this evaluation.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Table 6-2: Terminology