Corelight Sensors with BroLin v28 Security Target

Version 0.6
12/20/24

Prepared for:

Corelight, Inc.

548 Market St, PMB 77799
San Francisco, CA 94104-5401

Prepared By:

Gossamer Laboratories

www.gossamersec.com

LIST OF TABLES

LIST OF FIGURES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is Corelight Sensors with BroLin v28 provided by Corelight, Inc. The TOE is being evaluated as a network device.

The Security Target contains the following additional sections:

- Conformance Claims (Section 2)
- Security Objectives (Section 3)
- Extended Components Definition (Section 4)
- Security Requirements (Section 5)
- TOE Summary Specification (Section 6)

Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
  - Iteration: allows a component to be used more than once with varying operations. In this ST, iteration may be indicated by a parenthetical number placed at the end of the component. For example FDP_ACC.1(1) and FDP_ACC.1(2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement. Alternatively, a usually descriptive textual extension may be added after a slash (/) character to identify a specific iteration. For example, iterations of a requirement such as FCS_COP.1 might be identified as FCS_COP.1/HASH and FCS_COP.1/CRYPT.
  - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
  - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
  - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.1 Security Target Reference

ST Title – Corelight Sensors with BroLin v28 Security Target

ST Version – Version 0.6

ST Date – 12/20/24

1.2 TOE Reference

TOE Identification – Corelight, Inc. Corelight Sensors with BroLin v28

TOE Developer – Corelight, Inc.

Evaluation Sponsor – Corelight, Inc.

1.3 TOE Overview

The Target of Evaluation (TOE) is Corelight's Sensors.

Simple to deploy and integrate with existing analysis tools, the Corelight Sensor Appliances transform high-volume network traffic into high-fidelity data for incident response, intrusion detection, forensics and more. The Sensor parses dozens of network protocols and generates rich, actionable data streams designed for security professionals. The TOE includes the hardware models listed below.

1.4 TOE Description

The TOE is a network device which is composed of hardware and software that offers a scalable solution to the end users. It satisfies all the criteria to meet the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP22e]. The TOE operating system is BroLin v28. The TOE boundary is the hardware appliance, which comprises hardware and software components.

1.4.1 TOE Architecture

The TOE includes several models as shown below:

Model	CPU	Form Factor	Monitoring Interface	Management Interface	Power
AP 200	Intel Xeon Scalable Silver 4110 Skylake-SP	1U half-depth rackmount	Four 1G SFP interfaces	One 10/100/1000 copper Ethernet port	120/240 VAC 50/60 Hz single PSUs.
AP 520	Intel Xeon Scalable Gold 5317 Sunny Cove/Icelake-SP	1U rackmount	Four 1G SFP interfaces	One 10/100/1000 copper Ethernet port	120/240 VAC 50/60 Hz single PSUs.
AP 1001	Intel Xeon Scalable Silver 4116 Skylake-SP	1U rackmount	Four 1G/10G SFP/SFP+ interfaces	One 10/100/1000 copper ethernet port and up to 2 10G Ethernet ports	120/240 VAC 50/60 Hz redundant dual PSUs.
AP 1100	Intel Xeon Scalable Silver 4314 Sunny Cove/Icelake-SP	1U rackmount	Four 1G/10G SFP/SFP+ interfaces	2 1G Ethernet ports and 4 10G Ethernet ports	120/240 VAC 50/60 Hz redundant dual PSUs.
AP 1200	AMD EPYC 9254 Genoa/Zen 4	1U rackmount	Four 1G/10G SFP/SFP+ interfaces	2 1G Ethernet ports and 4 10/25G Ethernet ports	120/240 VAC 50/60 Hz redundant dual PSUs.
AP 3000	Intel Xeon Scalable Gold 6238 Skylake/Cascade Lake-SP	1U rackmount	Four 1G/10G SFP/SFP+ interfaces OR 10G QSF28 OR two 40G QSFP28 OR eight 10G QSFP28 interfaces	2 1G Ethernet ports and 4 10G Ethernet ports	120/240 VAC 50/60 Hz redundant dual PSUs.
AP 3100	Intel Xeon Scalable Gold 5318Y Sunny Cove/Icelake-SP	1U rackmount	Four 1G/10G SFP/SFP+ interfaces OR 10G QSF28 OR two 40G QSFP28 OR eight 10G QSFP28 interfaces	2 1G Ethernet ports and 4 10G Ethernet ports	120/240 VAC 50/60 Hz redundant dual PSUs.

Model	CPU	Form Factor	Monitoring Interface	Management Interface	Power
AP 3200	AMD EPYC 9534 Genoa/Zen4	1U rackmount	Four 1G/10G SFP/SFP+ interfaces OR 10G QSF28 OR two 40G QSFP28 OR eight 10G QSFP28 interfaces	2 1G Ethernet ports and 4 10/25G Ethernet ports	120/240 VAC 50/60 Hz redundant dual PSUs.
AP 5000	AMD EPYC 7742 Rome/Zen2	1U rackmount	Two QSFP28 bays, capable of supporting eight 10G OR two 40G 8 OR two 100G interfaces in a powerful, specialized NIC.	One 10/100/1000 copper ethernet port and up to 4 10G ethernet ports	120/240 VAC 50/60 Hz redundant dual PSUs.
AP 5002	AMD EPYC 7713 Milan/Zen3	1U rackmount	2 x QSFP56 bays capable of supporting eight 10G, two 40G or two 100G interfaces.	One 10/100/1000 copper ethernet port and up to 4 10G ethernet ports	120/240 VAC 50/60 Hz redundant dual PSUs.
AP 5200	AMD EPYC 9754 Bergamo/Zen 4c	1U rackmount	2 x QSFP56 bays capable of supporting eight 10G, two 40G or two 100G interfaces.	2 1G Ethernet ports and 4 10/25G Ethernet ports	120/240 VAC 50/60 Hz redundant dual PSUs.

Table 1 TOE Appliance Models

The TOE operates within a network environment as diagrammed below.

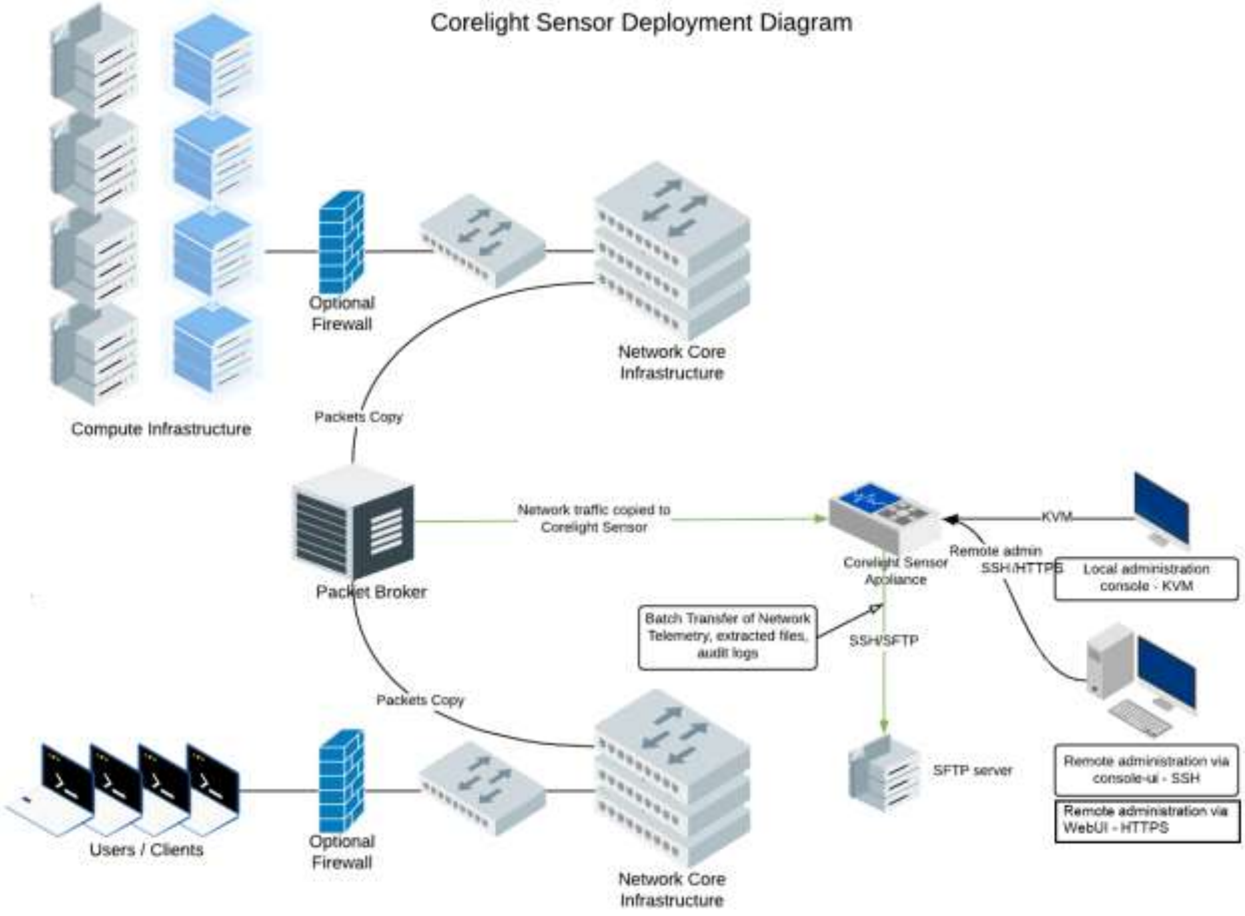
Corelight Sensor Deployment Diagram
Compute Infrastructure
Optional Firewall
Network Core Infrastructure
Packets Copy
Packet Broker
Network traffic copied to Corelight Sensor
Corelight Sensor Appliance
KVM
Remote admin SSH/HTTPS
Local administration console - KVM
Batch Transfer of Network Telemetry, extracted files, audit logs
SSH/SFTP
Packets Copy
SFTP server
Remote administration via console-ui - SSH
Remote administration via WebUI - HTTPS
Users / Clients
Optional Firewall
Network Core Infrastructure

Figure 1: TOE and TOE Operational Environment

An administrator uses an SSHv2 client or a web browser (each running on the administrator's workstation) to administer the TOE. The TOE does not have distributed components. Instead, the TOE implements all functionality within each model (physical appliance). Because the TOE independently satisfies all SFRs in the cPP without the Management Component, the NDcPP22e prescribes that the TOE be certified (by itself) according to the cPP and without the Management Component. "Figure 4: Non-distributed TOE use case" in the NDcPP22e depicts the TOE and its dedicated provisioning applications.

As a result, the TOE boundary includes only the TOE itself. The SSHv2 client and web browser (running on the administrator's workstation) as well as the remote SFTP audit server lie in the TOE's Operational Environment.

1.4.1.1 Physical Boundaries

The TOE boundary is the hardware appliance which consists of hardware and software components. It is deployed in an environment which contains the various IT components as depicted in the Figure above.

The TOE is shipped with the software pre-installed on it. Software updates are available for download from Corelight.

1.4.1.2 Logical Boundaries

This section summarizes the security functions provided by the Sensors:

- Security audit
- Cryptographic support

- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

1.4.1.2.1 Security audit

The TOE generates audit events for all start-up and shut-down functions, and all auditable events as specified in **Table 4**. Audit events are also generated for management actions specified in FAU_GEN.1. The TOE can store audit events locally and export them to an external audit server (via SFTP using SSH v2). Each audit record contains the date and time of event, type of event, subject identity, and the relevant data of the event.

1.4.1.2.2 Cryptographic support

The TOE provides cryptographic support for the secure administration access and audit export via SSH, for secure administration access via SFTP (FTP over SSH v2). Secure administration may also be performed using HTTPS/TLS (remote WebUI). The operating system is BroLin v28 which is based upon Linux Kernel version 5.4. The TOE leverages the SafeLogic's OpenSSL 3.0 and FIPS provider module for its cryptographic functionality. Functions include Key generation, key establishment, key distribution, key destruction, and cryptographic operations.

1.4.1.2.3 Identification and authentication

The TOE provides authentication services for administrative users to connect to the TOE's secure CLI administrator interface and to its WebUI. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE supports SSH password-based authentication and public key-based authentication. The TOE's WebUI and local console support password-based authentication. The TOE's SSHv2 interface supports authentication of administrative clients using SSH public keys.

1.4.1.2.4 Security management

TOE administrators manage the security functions of the TOE through both an SSH CLI and through the TOE's HTTPS/TLS WebUI. The TOE also provides the ability to configure the session activity timeout of an administrator and to configure the TOE's access banner.

1.4.1.2.5 Protection of the TSF

The TOE protects all passwords, pre-shared keys, symmetric keys and private keys from unauthorized disclosure. Passwords are stored on the file system in encrypted format. Passwords are stored as SHA-512 salted hash value as per standard Linux approach. The TOE executes self-tests during initial start-up to ensure correct operation and enforcement of its security functions. An administrator can install software updates to the TOE. The TOE internally maintains the date and time.

1.4.1.2.6 TOE access

Prior to establishing an administration session with the TOE, a banner is displayed to the user. The banner messaging is customizable. The TOE will terminate an interactive session after 60 minutes of session inactivity. A user can terminate their local CLI session and remote CLI session by entering exit at the prompt.

1.4.1.2.7 Trusted path/channels

The TOE supports SSH v2 for secure communication to the following IT entities: Audit server via SFTP. The TOE supports SSH v2 (remote CLI) and HTTPS/TLS (remote WebUI) for secure remote administration.

1.4.2 TOE Documentation

Corelight Sensor AP 200, AP 520, AP 1001, AP 1100, AP 1200, AP 3000, AP 3100, AP 3200, AP 5000, AP 5002 & AP 5200 Common Criteria Guidance document, v0.2, December 20, 2024 (Admin Guide)

2. Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
  - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 5, April 2017.
  - Part 3 Conformant
- Package Claims:
  - 'collaborative Protection Profile for Network Devices', Version 2.2e, 23 March 2020 (NDcPP22e)

Package	Technical Decision	Applied	Notes
CPP_ND_V2.2E	TD0800 - Updated NIT Technical Decision for IPsec IKE/SA Lifetimes Tolerance	No	IPsec not claimed
CPP_ND_V2.2E	TD0792 - NIT Technical Decision: FIA_PMG_EXT.1 - TSS EA not in line with SFR	Yes	
CPP_ND_V2.2E	TD0790 - NIT Technical Decision: Clarification Required for testing IPv6	No	DTLSC and TLSC not claimed
CPP_ND_V2.2E	TD0738 - NIT Technical Decision for Link to Allowed-With List	Yes	
CPP_ND_V2.2E	TD0670 - NIT Technical Decision for Mutual and Non-Mutual Auth TLSC Testing	No	TLSC not claimed
CPP_ND_V2.2E	TD0639 - NIT Technical Decision for Clarification for NTP MAC Keys	No	NTP not claimed
CPP_ND_V2.2E	TD0638 - NIT Technical Decision for Key Pair Generation for Authentication	Yes	
CPP_ND_V2.2E	TD0636 - NIT Technical Decision for Clarification of Public Key User Authentication for SSH	Yes	
CPP_ND_V2.2E	TD0635 - NIT Technical Decision for TLS Server and Key Agreement Parameters	Yes	
CPP_ND_V2.2E	TD0632 - NIT Technical Decision for Consistency with Time Data for vNDs	Yes	
CPP_ND_V2.2E	TD0631 - NIT Technical Decision for Clarification of public key authentication for SSH Server	Yes	
CPP_ND_V2.2E	TD0592 - NIT Technical Decision for Local Storage of Audit Records	Yes	
CPP_ND_V2.2E	TD0591 - NIT Technical Decision for Virtual TOEs and hypervisors	No	TOE is a pND, not vND.
CPP_ND_V2.2E	TD0581 - NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3	Yes	
CPP_ND_V2.2E	TD0580 - NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e	Yes	
CPP_ND_V2.2E	TD0572 - NiT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers	Yes	
CPP_ND_V2.2E	TD0571 - NiT Technical Decision for Guidance on how to handle FIA_AFL.1	Yes	
CPP_ND_V2.2E	TD0570 - NiT Technical Decision for Clarification about FIA_AFL.1	Yes	

Package	Technical Decision	Applied	Notes
CPP_ND_V2.2E	TD0569 - NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7	Yes	
CPP_ND_V2.2E	TD0564 - NiT Technical Decision for Vulnerability Analysis Search Criteria	Yes	
CPP_ND_V2.2E	TD0563 - NiT Technical Decision for Clarification of audit date information	Yes	
CPP_ND_V2.2E	TD0556 - NIT Technical Decision for RFC 5077 question	Yes	
CPP_ND_V2.2E	TD0555 - NIT Technical Decision for RFC Reference incorrect in TLSS Test	Yes	
CPP_ND_V2.2E	TD0547 - NIT Technical Decision for Clarification on developer disclosure of AVA_VAN	Yes	
CPP_ND_V2.2E	TD0546 - NIT Technical Decision for DTLS - clarification of Application Note 63	No	DTLS not claimed
CPP_ND_V2.2E	TD0537 - NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3	No	TLSC not claimed
CPP_ND_V2.2E	TD0536 - NIT Technical Decision for Update Verification Inconsistency	Yes	
CPP_ND_V2.2E	TD0528 - NIT Technical Decision for Missing EAs for FCS_NTP_EXT.1.4	No	NTP not claimed
CPP_ND_V2.2E	TD0527 - Updates to Certificate Revocation Testing (FIA_X509_EXT.1)	No	FIA_X509_EXT.1 is not claimed

Table 2 NIAP Technical Decisions

2.1 Conformance Rationale

The ST conforms to the NDcPP22e. As explained previously, the security problem definition, security objectives, and security requirements have been drawn from the PP.

3. Security Objectives

The Security Problem Definition may be found in the NDcPP22e and this section reproduces only the corresponding Security Objectives for operational environment for reader convenience. The NDcPP22e offers additional information about the identified security objectives, but that has not been reproduced here and the NDcPP22e should be consulted if there is interest in that material.

In general, the NDcPP22e has defined Security Objectives appropriate for network devices and as such are applicable to the Corelight Sensors TOE.

3.1 Security Objectives for the Operational Environment

OE.ADMIN_CREDENTIALS_SECURE The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.

OE.NO_GENERAL_PURPOSE There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE. Note: For vNDs the TOE includes only the contents of its own VM, and does not include other VMs or the VS.

OE.NO_THRU_TRAFFIC_PROTECTION The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.

OE.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

OE.RESIDUAL_INFORMATION The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.

OE.TRUSTED_ADMIN TOE Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality.
For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.

OE.UPDATES The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

4. Extended Components Definition

All of the extended requirements in this ST have been drawn from the NDcPP22e. The NDcPP22e defines the following extended requirements and since they are not redefined in this ST the NDcPP22e should be consulted for more information in regard to those CC extensions.

Extended SFRs:

- NDcPP22e:FAU_STG_EXT.1: Protected Audit Event Storage
- NDcPP22e:FCS_HTTPS_EXT.1: HTTPS Protocol
- NDcPP22e:FCS_RBG_EXT.1: Random Bit Generation
- NDcPP22e:FCS_SSHC_EXT.1: SSH Client Protocol - per TD0636
- NDcPP22e:FCS_SSHS_EXT.1: SSH Server Protocol - per TD0631
- NDcPP22e:FCS_TLSS_EXT.1: TLS Server Protocol Without Mutual Authentication - per TD0635
- NDcPP22e:FIA_PMG_EXT.1: Password Management - per TD0792
- NDcPP22e:FIA_UAU_EXT.2: Password-based Authentication Mechanism
- NDcPP22e:FIA_UIA_EXT.1: User Identification and Authentication
- NDcPP22e:FIA_X509_EXT.3: X.509 Certificate Requests
- NDcPP22e:FPT_APW_EXT.1: Protection of Administrator Passwords
- NDcPP22e:FPT_SKP_EXT.1: Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
- NDcPP22e:FPT_STM_EXT.1: Reliable Time Stamps - per TD0632
- NDcPP22e:FPT_TST_EXT.1: TSF testing
- NDcPP22e:FPT_TUD_EXT.1: Trusted update
- NDcPP22e:FTA_SSL_EXT.1: TSF-initiated Session Locking

5. Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the NDcPP22e. The refinements and operations already performed in the NDcPP22e are not identified (e.g., highlighted) here, rather the requirements have been copied from the NDcPP22e and any residual operations have been completed herein. Of particular note, the NDcPP22e made a number of refinements and completed some of the SFR operations defined in the Common Criteria (CC) and that PP should be consulted to identify those changes if necessary.

The SARs are also drawn from the NDcPP22e. The NDcPP22e should be consulted for the assurance activity definitions.

5.1 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by Corelight Sensors TOE.

Requirement Class	Requirement Component
FAU: Security audit	NDcPP22e:FAU_GEN.1: Audit Data Generation
	NDcPP22e:FAU_GEN.2: User identity association
	NDcPP22e:FAU_STG_EXT.1: Protected Audit Event Storage
FCS: Cryptographic support	NDcPP22e:FCS_CKM.1: Cryptographic Key Generation
	NDcPP22e:FCS_CKM.2: Cryptographic Key Establishment
	NDcPP22e:FCS_CKM.4: Cryptographic Key Destruction
	NDcPP22e:FCS_COP.1/DataEncryption: Cryptographic Operation (AES Data Encryption/Decryption)
	NDcPP22e:FCS_COP.1/Hash: Cryptographic Operation (Hash Algorithm)
	NDcPP22e:FCS_COP.1/KeyedHash: Cryptographic Operation (Keyed Hash Algorithm)
	NDcPP22e:FCS_COP.1/SigGen: Cryptographic Operation (Signature Generation and Verification)
	NDcPP22e:FCS_HTTPS_EXT.1: HTTPS Protocol
	NDcPP22e:FCS_RBG_EXT.1: Random Bit Generation
	NDcPP22e:FCS_SSHC_EXT.1: SSH Client Protocol - per TD0636
	NDcPP22e:FCS_SSHS_EXT.1: SSH Server Protocol - per TD0631
	NDcPP22e:FCS_TLSS_EXT.1: TLS Server Protocol Without Mutual Authentication - per TD0635
FIA: Identification and authentication	NDcPP22e:FIA_AFL.1: Authentication Failure Management
	NDcPP22e:FIA_PMG_EXT.1: Password Management - per TD0792
	NDcPP22e:FIA_UAU.7: Protected Authentication Feedback
	NDcPP22e:FIA_UAU_EXT.2: Password-based Authentication Mechanism
	NDcPP22e:FIA_UIA_EXT.1: User Identification and Authentication
	NDcPP22e:FIA_X509_EXT.3: X.509 Certificate Requests
FMT: Security management	NDcPP22e:FMT_MOF.1/AutoUpdate: Management of Security Functions Behaviour
	NDcPP22e:FMT_MOF.1/Functions: Management of Security Functions Behaviour
	NDcPP22e:FMT_MOF.1/ManualUpdate: Management of security functions behaviour
	NDcPP22e:FMT_MTD.1/CoreData: Management of TSF Data
	NDcPP22e:FMT_MTD.1/CryptoKeys: Management of TSF Data
	NDcPP22e:FMT_SMF.1: Specification of Management Functions - per TD0631
	NDcPP22e:FMT_SMR.2: Restrictions on Security Roles
FPT: Protection of the TSF	NDcPP22e:FPT_APW_EXT.1: Protection of Administrator Passwords
	NDcPP22e:FPT_SKP_EXT.1: Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)

Requirement Class	Requirement Component
	NDcPP22e:FPT_STM_EXT.1: Reliable Time Stamps - per TD0632
	NDcPP22e:FPT_TST_EXT.1: TSF testing
	NDcPP22e:FPT_TUD_EXT.1: Trusted update
FTA: TOE access	NDcPP22e:FTA_SSL.3: TSF-initiated Termination
	NDcPP22e:FTA_SSL.4: User-initiated Termination
	NDcPP22e:FTA_SSL_EXT.1: TSF-initiated Session Locking
	NDcPP22e:FTA_TAB.1: Default TOE Access Banners
FTP: Trusted path/channels	NDcPP22e:FTP_ITC.1: Inter-TSF trusted channel - per TD0639
	NDcPP22e:FTP_TRP.1/Admin: Trusted Path - per TD0639

Table 3 TOE Security Functional Components

5.1.1 Security audit (FAU)

5.1.1.1 Audit Data Generation (NDcPP22e:FAU_GEN.1)

NDcPP22e:FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shut-down of the audit functions;

b) All auditable events for the not specified level of audit; and

c) All administrative actions comprising:

- Administrative login and logout (name of user account shall be logged if individual user accounts are required for administrators).

- Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).

- Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).

- Resetting passwords (name of related user account shall be logged).

- [***no other actions***];

d) Specifically defined auditable events listed in Table 2.

NDcPP22e:FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the cPP/ST, information specified in column three of Table 2.

Requirement	Audit Event	Additional Contents
NDcPP22e:FAU_GEN.1		
NDcPP22e:FAU_GEN.2		
NDcPP22e:FAU_STG.1		
NDcPP22e:FAU_STG_EXT.1		
NDcPP22e:FCS_CKM.1		
NDcPP22e:FCS_CKM.2		
NDcPP22e:FCS_CKM.4		
NDcPP22e:FCS_COP.1/DataEncryption		
NDcPP22e:FCS_COP.1/Hash		
NDcPP22e:FCS_COP.1/KeyedHash		
NDcPP22e:FCS_COP.1/SigGen		
NDcPP22e:FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Reason for failure.
NDcPP22e:FCS_RBG_EXT.1		
NDcPP22e:FCS_SSHC_EXT.1	Failure to establish an SSH session.	Reason for failure.
NDcPP22e:FCS_SSHS_EXT.1	Failure to establish an SSH session.	Reason for failure.

Requirement	Audit Event	Additional Contents
NDcPP22e:FCS_TLSS_EXT.1	Failure to establish a TLS Session.	Reason for failure.
NDcPP22e:FIA_AFL.1	Unsuccessful login attempt limit is met or exceeded.	Origin of the attempt (e.g., IP address).
NDcPP22e:FIA_PMG_EXT.1		
NDcPP22e:FIA_UAU.7		
NDcPP22e:FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
NDcPP22e:FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
NDcPP22e:FIA_X509_EXT.3		
NDcPP22e:FMT_MOF.1/AutoUpdate		
NDcPP22e:FMT_MOF.1/Functions		
NDcPP22e:FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update.	
NDcPP22e:FMT_MTD.1/CoreData		
NDcPP22e:FMT_MTD.1/CryptoKeys		
NDcPP22e:FMT_SMF.1	All management activities of TSF data.	
NDcPP22e:FMT_SMR.2		
NDcPP22e:FPT_APW_EXT.1		
NDcPP22e:FPT_SKP_EXT.1		
NDcPP22e:FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
NDcPP22e:FPT_TST_EXT.1		
NDcPP22e:FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure).	
NDcPP22e:FTA_SSL.3	The termination of a remote session by the session locking mechanism.	
NDcPP22e:FTA_SSL.4	The termination of an interactive session.	
NDcPP22e:FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	
NDcPP22e:FTA_TAB.1		
NDcPP22e:FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
NDcPP22e:FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	

Table 4 Audit Table

5.1.1.2 User identity association (NDcPP22e:FAU_GEN.2)

NDcPP22e:FAU_GEN.2.1

For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.1.1.3 Protected Audit Event Storage (NDcPP22e:FAU_STG_EXT.1)

NDcPP22e:FAU_STG_EXT.1.1

The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1.

NDcPP22e:FAU_STG_EXT.1.2

The TSF shall be able to store generated audit data on the TOE itself. In addition [***The TOE shall consist of a single standalone component that stores audit data locally,***]

NDcPP22e:FAU_STG_EXT.1.3

The TSF shall [***overwrite previous audit records according to the following rule: [oldest audit events being replaced with new ones]***] when the local storage space for audit data is full.

5.1.2 Cryptographic support (FCS)

5.1.2.1 Cryptographic Key Generation (NDcPP22e:FCS_CKM.1)

NDcPP22e:FCS_CKM.1.1

The TSF shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm: [
- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.3,
- ECC schemes using 'NIST curves' [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.4,
- FFC Schemes using 'safe-prime' groups that meet the following: 'NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography' and [RFC 3526]].

5.1.2.2 Cryptographic Key Establishment (NDcPP22e:FCS_CKM.2)

NDcPP22e:FCS_CKM.2.1

The TSF shall perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [
- RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, 'Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1,
- Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, 'Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography' (TD0581 applied),
- FFC Schemes using 'safe-prime' groups that meet the following: 'NIST Special Publication 800-56A Revision 3, 'Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography' and [groups listed in RFC 3526] (TD0580 applied)].

5.1.2.3 Cryptographic Key Destruction (NDcPP22e:FCS_CKM.4)

NDcPP22e:FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method
- For plaintext keys in volatile storage, the destruction shall be executed by a [***single overwrite consisting of [zeroes]***];

- For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that [***logically addresses the storage location of the key and performs a [single] overwrite consisting of [zeroes]***]

that meets the following: No Standard.

5.1.2.4 Cryptographic Operation (AES Data Encryption/Decryption) (NDcPP22e:FCS_COP.1/DataEncryption)

NDcPP22e:FCS_COP.1.1/DataEncryption

The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in [***CBC, CTR, GCM***] mode and cryptographic key sizes [***128 bits, 256 bits***] that meet the following: AES as specified in ISO 18033-3, [***CBC as specified in ISO 10116, CTR as specified in ISO 10116, GCM as specified in ISO 19772***].

5.1.2.5 Cryptographic Operation (Hash Algorithm) (NDcPP22e:FCS_COP.1/Hash)

NDcPP22e:FCS_COP.1.1/Hash

The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [***SHA-1, SHA-256, SHA-384, SHA-512***] and message digest sizes [***160, 256, 384, 512***] bits that meet the following: ISO/IEC 10118-3:2004.

5.1.2.6 Cryptographic Operation (Keyed Hash Algorithm) (NDcPP22e:FCS_COP.1/KeyedHash)

NDcPP22e:FCS_COP.1.1/KeyedHash

The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm [***HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512***] and cryptographic key sizes [**160, 256, 384, 512 (in bits) used in HMAC**] and message digest sizes [***160, 256, 384, 512***] bits that meet the following: ISO/IEC 9797-2:2011, Section 7 'MAC Algorithm 2'.

5.1.2.7 Cryptographic Operation (Signature Generation and Verification) (NDcPP22e:FCS_COP.1/SigGen)

NDcPP22e:FCS_COP.1.1/SigGen

The TSF shall perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm [***- RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [2048, 3072], - Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [256 bits]***]

that meet the following:

[***- For RSA schemes: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3, - For ECDSA schemes: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Section 6 and Appendix D, Implementing 'NIST curves' [P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4***].

5.1.2.8 HTTPS Protocol (NDcPP22e:FCS_HTTPS_EXT.1)

NDcPP22e:FCS_HTTPS_EXT.1.1

The TSF shall implement the HTTPS protocol that complies with RFC 2818.

NDcPP22e:FCS_HTTPS_EXT.1.2

The TSF shall implement HTTPS using TLS.

NDcPP22e:FCS_HTTPS_EXT.1.3

If a peer certificate is presented, the TSF shall [***not require client authentication***] if the peer certificate is deemed invalid.

5.1.2.9 Random Bit Generation (NDcPP22e:FCS_RBG_EXT.1)

NDcPP22e:FCS_RBG_EXT.1.1

The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [***CTR_DRBG (AES)***].

NDcPP22e:FCS_RBG_EXT.1.2

The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [***[1] software-based noise source***] with a minimum of [***256 bits***] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011Table C.1 'Security Strength Table for Hash Functions', of the keys and hashes that it will generate.

5.1.2.10 SSH Client Protocol - per TD0636 (NDcPP22e:FCS_SSHC_EXT.1)

NDcPP22e:FCS_SSHC_EXT.1.1

The TSF shall implement the SSH protocol that complies with RFC(s) 4251, 4252, 4253, 4254, [***4256, 4344, 5647, 5656, 6668, 8268, 8308 section 3.1, 8332***].

NDcPP22e:FCS_SSHC_EXT.1.2

The TSF shall ensure that the SSH protocol implementation supports the following user authentication methods as described in RFC 4252: public key-based, [***no other method***].

NDcPP22e:FCS_SSHC_EXT.1.3

The TSF shall ensure that, as described in RFC 4253, packets greater than [**262144**] bytes in an SSH transport connection are dropped.

NDcPP22e:FCS_SSHC_EXT.1.4

The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [***aes128-cbc, aes256-cbc, aes128-ctr, aes256-ctr***].

NDcPP22e:FCS_SSHC_EXT.1.5

The TSF shall ensure that the SSH public-key based authentication implementation uses [***rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521***] as its public key algorithm(s) and rejects all other public key algorithms.

NDcPP22e:FCS_SSHC_EXT.1.6

The TSF shall ensure that the SSH transport implementation uses [***hmac-sha2-256, hmac-sha2-512***] as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

NDcPP22e:FCS_SSHC_EXT.1.7

The TSF shall ensure that [***diffie-hellman-group14-sha1, ecdh-sha2-nistp256***] and [***no other methods***] are the only allowed key exchange methods used for the SSH protocol.

NDcPP22e:FCS_SSHC_EXT.1.8

The TSF shall ensure that within SSH connections, the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed.

NDcPP22e:FCS_SSHC_EXT.1.9

The TSF shall ensure that the SSH client authenticates the identity of the SSH server using a local database associating each host name with its corresponding public key and [***no other methods***] as described in RFC 4251 section 4.1.

5.1.2.11 SSH Server Protocol - per TD0631 (NDcPP22e:FCS_SSHS_EXT.1)

NDcPP22e:FCS_SSHS_EXT.1.1

The TSF shall implement the SSH protocol that complies with: RFC(s) 4251, 4252, 4253, 4254, [***4256, 4344, 5647, 5656, 6668, 8268, 8308 section 3.1, 8332***].

NDcPP22e:FCS_SSHS_EXT.1.2

The TSF shall ensure that the SSH protocol implementation supports the following user authentication methods as described in RFC 4252: public key-based, [***password-based***]. (TD0631 applied)

NDcPP22e:FCS_SSHS_EXT.1.3

The TSF shall ensure that, as described in RFC 4253, packets greater than [**262144**] bytes in an SSH transport connection are dropped.

NDcPP22e:FCS_SSHS_EXT.1.4

The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [***aes128-ctr, aes256-ctr***].

NDcPP22e:FCS_SSHS_EXT.1.5

The TSF shall ensure that the SSH public-key based authentication implementation uses [***rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256***] as its public key algorithm(s) and rejects all other public key algorithms.

NDcPP22e:FCS_SSHS_EXT.1.6

The TSF shall ensure that the SSH transport implementation uses [***hmac-sha2-256, hmac-sha2-512***] as its MAC algorithm(s) and rejects all other MAC algorithm(s).

NDcPP22e:FCS_SSHS_EXT.1.7

The TSF shall ensure that [***ecdh-sha2-nistp256***] and [***diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, ecdh-sha2-nistp384, ecdh-sha2-nistp521***] are the only allowed key exchange methods used for the SSH protocol.

NDcPP22e:FCS_SSHS_EXT.1.8

The TSF shall ensure that within SSH connections, the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed.

5.1.2.12 TLS Server Protocol Without Mutual Authentication - per TD0635 (NDcPP22e:FCS_TLSS_EXT.1)

NDcPP22e:FCS_TLSS_EXT.1.1

The TSF shall implement [***TLS 1.2 (RFC 5246)***] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:
[***TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492,***
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492,
TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,
TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289]
and no other ciphersuites.

NDcPP22e:FCS_TLSS_EXT.1.2

The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and [***TLS 1.1***].

NDcPP22e:FCS_TLSS_EXT.1.3

The TSF shall perform key establishment for TLS using [***RSA with key size [2048 bits, 3072 bits, 4096 bits], ECDHE curves [secp256r1, secp384r1, secp521r1] and no other curves***]].

NDcPP22e:FCS_TLSS_EXT.1.4

The TSF shall support [***session resumption based on session tickets according to RFC 5077***].

5.1.3 Identification and authentication (FIA)

5.1.3.1 Authentication Failure Management (NDcPP22e:FIA_AFL.1)

NDcPP22e:FIA_AFL.1.1

The TSF shall detect when an Administrator configurable positive integer within [**3-15**] unsuccessful authentication attempts occur related to Administrators attempting to authenticate remotely using a password.

NDcPP22e:FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been met, the TSF shall [***prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until an Administrator defined time period has elapsed***].

5.1.3.2 Password Management - per TD0792 (NDcPP22e:FIA_PMG_EXT.1)

NDcPP22e:FIA_PMG_EXT.1.1

The TSF shall provide the following password management capabilities for administrative passwords:

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [***'!', '@', '#', '$', '%', '^', '&', '*', '(', ')'***];

b) Minimum password length shall be configurable to between [**8**] and [**64**] characters.

5.1.3.3 Protected Authentication Feedback (NDcPP22e:FIA_UAU.7)

NDcPP22e:FIA_UAU.7.1

The TSF shall provide only obscured feedback to the administrative user while the authentication is in progress at the local console.

5.1.3.4 Password-based Authentication Mechanism (NDcPP22e:FIA_UAU_EXT.2)

NDcPP22e:FIA_UAU_EXT.2.1

The TSF shall provide a local [***password-based***] authentication mechanism to perform local administrative user authentication.

5.1.3.5 User Identification and Authentication (NDcPP22e:FIA_UIA_EXT.1)

NDcPP22e:FIA_UIA_EXT.1.1

The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- [***no other actions***].

NDcPP22e:FIA_UIA_EXT.1.2

The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.

5.1.3.6 X.509 Certificate Requests (NDcPP22e:FIA_X509_EXT.3)

NDcPP22e:FIA_X509_EXT.3.1

The TSF shall generate a Certification Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [***Common Name, Organization, Organizational Unit, Country***].

NDcPP22e:FIA_X509_EXT.3.2

The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

5.1.4 Security management (FMT)

5.1.4.1 Management of Security Functions Behaviour (NDcPP22e:FMT_MOF.1/AutoUpdate)

NDcPP22e:FMT_MOF.1.1/AutoUpdate

The TSF shall restrict the ability to [***enable, disable***] the functions [***automatic checking for updates, automatic update***] to Security Administrators.

5.1.4.2 Management of Security Functions Behaviour (NDcPP22e:FMT_MOF.1/Functions)

NDcPP22e:FMT_MOF.1.1/Functions

The TSF shall restrict the ability to [***determine the behaviour of, modify the behaviour of***] the functions [***transmission of audit data to an external IT entity***] to Security Administrators.

5.1.4.3 Management of security functions behaviour (NDcPP22e:FMT_MOF.1/ManualUpdate)

NDcPP22e:FMT_MOF.1.1/ManualUpdate

The TSF shall restrict the ability to enable the functions to perform manual updates to Security Administrators.

5.1.4.4 Management of TSF Data (NDcPP22e:FMT_MTD.1/CoreData)

NDcPP22e:FMT_MTD.1.1/CoreData

The TSF shall restrict the ability to manage the TSF data to Security Administrators.

5.1.4.5 Management of TSF Data (NDcPP22e:FMT_MTD.1/CryptoKeys)

NDcPP22e:FMT_MTD.1.1/CryptoKeys

The TSF shall restrict the ability to manage the cryptographic keys to Security Administrators.

5.1.4.6 Specification of Management Functions - per TD0631 (NDcPP22e:FMT_SMF.1)

NDcPP22e:FMT_SMF.1.1

The TSF shall be capable of performing the following management functions:
- Ability to administer the TOE locally and remotely;
- Ability to configure the access banner;
- Ability to configure the session inactivity time before session termination or locking;
- Ability to update the TOE, and to verify the updates using [***digital signature***] capability prior to installing those updates;
- Ability to configure the authentication failure parameters for FIA_AFL.1;
- [***Ability to configure audit behavior (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full),***
Ability to manage the cryptographic keys,
Ability to configure the cryptographic functionality,
Ability to enable or disable automatic checking for updates or automatic updates,
Ability to set the time which is used for time-stamps;
Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors,
Ability to import X509v3 certificates to the TOE's trust store,
Ability to manage the trusted public keys database].
(TD0631 applied)

5.1.4.7 Restrictions on Security Roles (NDcPP22e:FMT_SMR.2)

NDcPP22e:FMT_SMR.2.1

The TSF shall maintain the roles: - Security Administrator.

NDcPP22e:FMT_SMR.2.2

The TSF shall be able to associate users with roles.

NDcPP22e:FMT_SMR.2.3

The TSF shall ensure that the conditions
- The Security Administrator role shall be able to administer the TOE locally;
- The Security Administrator role shall be able to administer the TOE remotely

are satisfied.

5.1.5 Protection of the TSF (FPT)

5.1.5.1 Protection of Administrator Passwords (NDcPP22e:FPT_APW_EXT.1)

NDcPP22e:FPT_APW_EXT.1.1

The TSF shall store administrative passwords in non-plaintext form.

NDcPP22e:FPT_APW_EXT.1.2

The TSF shall prevent the reading of plaintext administrative passwords.

5.1.5.2 Protection of TSF Data (for reading of all pre-shared, symmetric and private keys) (NDcPP22e:FPT_SKP_EXT.1)

NDcPP22e:FPT_SKP_EXT.1.1

The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

5.1.5.3 Reliable Time Stamps - per TD0632 (NDcPP22e:FPT_STM_EXT.1)

NDcPP22e:FPT_STM_EXT.1.1

The TSF shall be able to provide reliable time stamps for its own use.

NDcPP22e:FPT_STM_EXT.1.2

The TSF shall [***allow the Security Administrator to set the time***].

5.1.5.4 TSF testing (NDcPP22e:FPT_TST_EXT.1)

NDcPP22e:FPT_TST_EXT.1.1

The TSF shall run a suite of the following self-tests [***during initial start-up (on power on)***] to demonstrate the correct operation of the TSF: [**Known Answer Tests for SHA, AES, HMAC-SHA, DRBG, ECDH, GCM, RSA, and ECDSA**].

5.1.5.5 Trusted update (NDcPP22e:FPT_TUD_EXT.1)

NDcPP22e:FPT_TUD_EXT.1.1

The TSF shall provide Security Administrators the ability to query the currently executing version of the TOE firmware/software and [***no other TOE firmware/software version***].

NDcPP22e:FPT_TUD_EXT.1.2

The TSF shall provide Security Administrators the ability to manually initiate updates to TOE firmware/software and [***support automatic checking for updates, support automatic updates***].

NDcPP22e:FPT_TUD_EXT.1.3

The TSF shall provide means to authenticate firmware/software updates to the TOE using a [***digital signature***] prior to installing those updates.

5.1.6 TOE access (FTA)

5.1.6.1 TSF-initiated Termination (NDcPP22e:FTA_SSL.3)

NDcPP22e:FTA_SSL.3.1

The TSF shall terminate a remote interactive session after a Security Administrator-configurable time interval of session inactivity.

5.1.6.2 User-initiated Termination (NDcPP22e:FTA_SSL.4)

NDcPP22e:FTA_SSL.4.1

The TSF shall allow Administrator-initiated termination of the Administrator's own interactive session.

5.1.6.3 TSF-initiated Session Locking (NDcPP22e:FTA_SSL_EXT.1)

NDcPP22e:FTA_SSL_EXT.1.1

The TSF shall, for local interactive sessions, [***terminate the session***] after a Security Administrator-specified time period of inactivity.

5.1.6.4 Default TOE Access Banners (NDcPP22e:FTA_TAB.1)

NDcPP22e:FTA_TAB.1.1

Before establishing an administrative user session the TSF shall display a Security Administrator-specified advisory notice and consent warning message regarding use of the TOE.

5.1.7 Trusted path/channels (FTP)

5.1.7.1 Inter-TSF trusted channel - per TD0639 (NDcPP22e:FTP_ITC.1)

NDcPP22e:FTP_ITC.1.1

The TSF shall be capable of using [***SSH***] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, [***[no other capabilities]***] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

NDcPP22e:FTP_ITC.1.2

The TSF shall permit the TSF or the authorized IT entities to initiate communication via the trusted channel.

NDcPP22e:FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [**audit server**].

5.1.7.2 Trusted Path - per TD0639 (NDcPP22e:FTP_TRP.1/Admin)

NDcPP22e:FTP_TRP.1.1/Admin

The TSF shall be capable of using [***SSH, TLS, HTTPS***] to provide a communication path between itself and authorized remote Administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure and provides detection of modification of the channel data.

NDcPP22e:FTP_TRP.1.2/Admin

The TSF shall permit remote Administrators to initiate communication via the trusted path.

NDcPP22e:FTP_TRP.1.3/Admin

The TSF shall require the use of the trusted path for initial Administrator authentication and all remote administration actions.

5.2 TOE Security Assurance Requirements

The SARs for the TOE are the components as specified in Part 3 of the Common Criteria. Note that the SARs have effectively been refined with the assurance activities explicitly defined in association with both the SFRs and SARs.

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1: Basic Functional Specification
AGD: Guidance documents	AGD_OPE.1: Operational User Guidance
	AGD_PRE.1: Preparative Procedures
ALC: Life-cycle support	ALC_CMC.1: Labelling of the TOE
	ALC_CMS.1: TOE CM Coverage
ATE: Tests	ATE_IND.1: Independent Testing - Conformance
AVA: Vulnerability assessment	AVA_VAN.1: Vulnerability Survey

Table 5 Assurance Components

5.2.1 Development (ADV)

5.2.1.1 Basic Functional Specification (ADV_FSP.1)

ADV_FSP.1.1d

The developer shall provide a functional specification.

ADV_FSP.1.2d

The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.1.1c

The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2c

The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3c

The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV_FSP.1.4c

The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2e

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.2 Guidance documents (AGD)

5.2.2.1 Operational User Guidance (AGD_OPE.1)

AGD_OPE.1.1d

The developer shall provide operational user guidance.

AGD_OPE.1.1c

The operational user guidance shall describe, for each user role, the user accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2c

The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3c

The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4c

The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5c

The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences, and implications for maintaining secure operation.

AGD_OPE.1.6c

The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7c

The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2.2 Preparative Procedures (AGD_PRE.1)

AGD_PRE.1.1d

The developer shall provide the TOE, including its preparative procedures.

AGD_PRE.1.1c

The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2c

The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

AGD_PRE.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2e

The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.3 Life-cycle support (ALC)

5.2.3.1 Labelling of the TOE (ALC_CMC.1)

ALC_CMC.1.1d

The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.1.1c

The TOE shall be labelled with its unique reference.

ALC_CMC.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.2 TOE CM Coverage (ALC_CMS.1)

ALC_CMS.1.1d

The developer shall provide a configuration list for the TOE.

ALC_CMS.1.1c

The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2c

The configuration list shall uniquely identify the configuration items.

ALC_CMS.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Tests (ATE)

5.2.4.1 Independent Testing - Conformance (ATE_IND.1)

ATE_IND.1.1d

The developer shall provide the TOE for testing.

ATE_IND.1.1c

The TOE shall be suitable for testing.

ATE_IND.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2e

The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.2.5 Vulnerability assessment (AVA)

5.2.5.1 Vulnerability Survey (AVA_VAN.1)

AVA_VAN.1.1d

The developer shall provide the TOE for testing.

AVA_VAN.1.1c

The TOE shall be suitable for testing.

AVA_VAN.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.1.2e

The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3e

The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6. TOE Summary Specification

This chapter describes the security functions:

- Security audit
- Cryptographic support
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

6.1 Security audit

NDcPP22e:FAU_GEN.1:

The TOE generates a comprehensive set of audit logs that identify specific TOE operations whenever an auditable event occurs. Auditable events are specified in **Table 4**. Each audit record contains the date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event.

All configuration changes are recorded with subject identity as the user request is made through the command line interface (CLI) with either local or remote connection as well as through the TOE's Web UI. Administrative tasks of generating and deleting cryptographic keys contain the necessary audit information as the key name is used to identify the key.

NDcPP22e:FAU_GEN.2:

For audit events that result from actions of identified users, the TOE can associate each auditable event with the identity of the user that caused the event.

NDcPP22e:FAU_STG_EXT.1:

The TOE can be configured to export audit events securely to an audit server using FTP within the SSH v2 protocol. The audit server in this case is the SFTP server.

The TOE is a standalone TOE that stores audit data locally. The TOE stores up to 100,000 audit records locally. When the local data is full, the oldest audit events are overwritten to allow new audit events to be created. The TOE is designed to store 100K records in the database. API queries however are limited to 7 days. Security Administrators can access the audit events and can clear the audit events. This way, audit events are protected against unauthorized access.

The TOE transmits audit data to an external audit server periodically (every two minutes) in batches. If there is an SSH connection failure, the TOE will continue to store local audit events on the TOE and will transmit any locally stored contents when connectivity to the audit server is restored.

6.2 Cryptographic support

NDcPP22e:FCS_CKM.1:

The TOE supports RSA key sizes of 2048 bits and 3072 bits, for key generation conforming to Cryptographic key generation conforming to FIPS PUB 186-4 Digital Signature Standard (DSS), Appendix B.3. The RSA keys are used in support of SSH and TLS communications.

The TOE supports Elliptical NIST curve sizes of P-256, P-384 and P-521 conforming to Cryptographic key generation conforming to FIPS PUB 186-4 Digital Signature Standard (DSS)", Appendix B.4. The Elliptic keys are used in support of ECDH key exchange for SSH and TLS. The TOE supports FFC Schemes using 'safe-prime' groups that meet the following: “NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and RFC 3526. The TOE supports DH14 and DH16(server only) key generation in support of DH key exchanges as part of SSH.

The table below identifies the algorithm certificates supported by the Corelight Cryptographic Module, Corelight Cryptographic Module KAS, and Corelight RSA Engine all version 2.1.2.

Requirements	Functions	CAVP Cert
	Cryptographic key generation	
NDcPP22e:FCS_CKM.1	RSA schemes using key sizes of 2048 and 3072	A5867
NDcPP22e:FCS_CKM.1	ECC schemes using 'NIST curves' P-256, P-384, P-521 (keyge/keyver)	A5859
NDcPP22e:FCS_CKM.1	FFC schemes using 'safe prime' group DH14 (2048), DH16 (4096)	Tested with known, good implementation
	Cryptographic key establishment	
NDcPP22e:FCS_CKM.2	RSA schemes using key sizes of 2048 and 3072	Tested with known, good implementation
NDcPP22e:FCS_CKM.2	Diffie-Hellman schemes using safe primes	Tested with known, good implementation
NDcPP22e:FCS_CKM.2	Elliptic curve-based key establishment schemes: P-256, P-384. P-521	A5862
	Encryption/Decryption	
NDcPP22e:FCS_COP.1/ DataEncryption	AES CBC, CTR, GCM (128, 256 bits)	A5859
	Cryptographic hashing	
NDcPP22e:FCS_COP.1/Hash	SHA-1/256/384/512 (digest sizes 160, 256, 384 and 512 bits)	A5859
	Keyed-hash message authentication	
NDcPP22e:FCS_COP.1/KeyedHash	HMAC-SHA-1/256/384/512 (key and output MAC size 160, 256, 384, 512)	A5859
	Cryptographic signature services	
NDcPP22e:FCS_COP.1/SigGen	RSA schemes using key sizes of 2048 and 3072 (siggen/sigver)	A5859
NDcPP22e:FCS_COP.1/SigGen	Elliptic Curve Digital Signature Algorithm (ECDSA) with an elliptical curve P-256, P-384. P-521 (siggen/sigver)	A5859
	Random bit generation	
NDcPP22e:FCS_RBG_EXT.1	CTR_DRBG (AES) with SW based noise source (256 bits)	A5859

Table 6 Cryptographic Algorithm Certificates

NDcPP22e:FCS_CKM.2:

The TOE supports Cryptographic Key Establishment using the following schemes:

- RSA key based establishment conforming to RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1. The TOE implements RSA key establishment scheme with key sizes of 2048 and 3072 bits
- Elliptical curve-based establishment conforming to NIST Special Publication 800-56A Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography.
- FFC Schemes using "safe-prime" groups that meet the following: 'NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and groups listed in RFC 3526.

The TOE uses RSA and ECC schemes during TLS and uses FFC safe primes and ECC schemes during SSH.

Scheme	SFR	Service
RSA	FCS_TLSS_EXT.1	WebUI for remote administration
ECC	FCS_SSHC_EXT.1 FCS_SSHS_EXT.1 FCS_TLSS_EXT.1	Audit log secure export CLI remove administration WebUI for remote administration
FFC/safe primes	FCS_SSHC_EXT.1 FCS_SSHS_EXT.1	Audit log secure export CLI remove administration

Table 7 TOE Key Establishment Schemes

Please refer to **Table 6 Cryptographic Algorithm Certificates** for the TOE's CAVP certificates.

NDcPP22e:FCS_CKM.4:

The TOE satisfies all requirements as specified in FCS_CKM.4 of NDcPPv2.2e for destruction of keys and CSPs and includes the following cryptographic keys

Key	Purpose	Storage (RAM/Flash)	Encrypted/ Plaintext	Destruction and when
TLS session keys	Keys exchanged for protecting the confidentiality of the remote administration session	RAM	Plaintext	Overwritten w/ zeros after use
TLS auth keys	X509 certificate used for authentication as TLS server	Flash	Plaintext	Stored persistently in the TOE's data partition, and overwritten w/ zeros upon reset to factory defaults
SSH session keys	Keys exchanged for protecting the confidentiality of the SSH sessions	RAM	Plaintext	Overwritten w/ zeros after use
SSH host keys	The host key for authentication of the TOE as an SSH server. As an SSH client, the host key of the SSH server the TOE is connecting too.	Flash	Plaintext	Stored persistently in the TOE's data partition, and overwritten w/ zeros prior to generating new ones or upon reset to factory defaults
SSH public keys	The public key for authentication as an SSH client. As an SSH server, the public key of the client authenticating to the TOE.	Flash	Plaintext	Stored persistently in the TOE's data partition, and overwritten w/ zeros prior to generating new ones or upon reset to factory defaults

Table 8 TOE Keys and Key Destruction

NDcPP22e:FCS_COP.1/DataEncryption:

The TOE supports AES encryption and decryption conforming to CBC as specified in ISO 10116, CTR as specified in ISO 10116 and GCM as specified in ISO 19772.

The AES key size supported are 128 bits and 256 bits and the AES modes supported are: CBC, CTR and GCM.

Please refer to **Table 6 Cryptographic Algorithm Certificates** for the TOE's CAVP certificates.

NDcPP22e:FCS_COP.1/Hash:

The TOE supports Cryptographic hashing services conforming to ISO/IEC 10118-3:2004. The hashing algorithms are used in SSH and TLS connections for secure communications.

The following hashing algorithms are supported: SHA-1, SHA-256, SHA-384 and SHA-512.

The message digest sizes supported are: 160, 256, 384 and 512 bits.

Please refer to **Table 6 Cryptographic Algorithm Certificates** for the TOE's CAVP certificates.

NDcPP22e:FCS_COP.1/KeyedHash:

The TOE supports Keyed-hash message authentication conforming to ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2". HMAC algorithms are used in support of SSH and TLS sessions.

HMAC algorithm	Hash function	Block size	Key length	MAC length
HMAC-SHA-1	SHA-1	512-bits	160 bits	160 bits
HMAC-SHA-256	SHA-256	512 bits	256 bits	256 bits
HMAC-SHA-384	SHA-384	1024 bits	384 bits	384 bits
HMAC-SHA-512	SHA-512	1024 bits	512 bits	512 bits

Table 9 TOE Supported Keyed Hash Algorithms

Please refer to **Table 6 Cryptographic Algorithm Certificates** for the TOE's CAVP certificates.

NDcPP22e:FCS_COP.1/SigGen:

The TOE provides Cryptographic signature generation and verification in accordance with the following cryptographic algorithms:

- RSA digital signature conforming to FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3.
    - The RSA key sizes supported are: 2048 and 3072 bits.
- The TOE uses Elliptical curve digital signature algorithm conforming to FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" [P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4
    - The Elliptical curve key size supported is 256, 384, and 521 bits.

Please refer to **Table 6 Cryptographic Algorithm Certificates** for the TOE's CAVP certificates.

NDcPP22e:FCS_HTTPS_EXT.1:

The TOE adheres to RFC 2818 by acting as a server and hosting the Admin Web UI on port 443. The TOE provides a server identity certificate to connecting clients (either a self-signed certificate, or one that the admin can load or issue against a TOE generated CSR).

NDcPP22e:FCS_RBG_EXT.1:

The TOE uses CTR_DRBG conforming to ISO/IEC 18031:2011.

The CTR_DRBG is seeded by an entropy source that accumulates entropy from software-based noise source with a minimum of 256 bits of entropy. An entropy document was submitted and approved.

Please refer to **Table 6 Cryptographic Algorithm Certificates** for the TOE's CAVP certificates.

NDcPP22e:FCS_SSHC_EXT.1:

NDcPP22e:FCS_SSHC_EXT.1.1:

The TOE implements SSH protocol that complies with RFC(s) 4251, 4252, 4253, 4254, 4256, 4344, 5647, 5656, 6668, 8268, 8308 Section 3.1, and 8332.

NDcPP22e:FCS_SSHC_EXT.1.2:

The TOE supports authenticating itself to a remote endpoint with a user-based public key.

The following public key algorithms are supported: rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384 and ecdsa-sha2-nistp521.

NDcPP22e:FCS_SSHC_EXT.1.3:

The TOE accepts packet size up to 262144 bytes and meets the requirements of RFC 4253. Any packet greater than the max size will be dropped and the connection will be terminated.

NDcPP22e:FCS_SSHC_EXT.1.4:

The TOE supports the following encryption algorithms: aes128-cbc, aes256-cbc, aes128-ctr, aes256-ctr for SSH transport. There are no optional characteristics specified for FCS_SSHC_EXT.1.4. This list is identical to those claimed for FCS_SSHC_EXT.1.4.

NDcPP22e:FCS_SSHC_EXT.1.5:

The following are the public key algorithms supported: rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384 and ecdsa-sha2-nistp521. There are no optional characteristics specified for FCS_SSHC_EXT.1.5. This list is identical to those claimed for FCS_SSHC_EXT.1.5.

When configuring the SFTP channel for the audit server, the administrator defines the expected server host key.

NDcPP22e:FCS_SSHC_EXT.1.6:

The TOE supports the following data integrity MAC algorithms: hmac-sha2-256, and hmac-sha2-512. This list corresponds to the list in FCS_SSHC_EXT.1.6.

NDcPP22e:FCS_SSHC_EXT.1.7:

The TOE supports the following key exchange algorithms: diffie-hellman-group14-sha1 and ecdh-sha2-nistp256. This list corresponds to the list in FCS_SSHC_EXT.1.7.

NDcPP22e:FCS_SSHC_EXT.1.8:

The TOE is capable of rekeying. The TOE verifies the following thresholds:

- No longer than one hour
- No more than one gigabyte of transmitted data

The TOE continuously checks both conditions. When either of the conditions is met, the TOE will initiate a rekey.

NDcPP22e:FCS_SSHC_EXT.1.9:

The TOE's SSH client authenticates the identity of the SSH server using a local database associating each host name with its corresponding public key (as per RFC 4251 section 4.1).

NDcPP22e:FCS_SSHS_EXT.1:

NDcPP22e:FCS_SSHS_EXT.1.1:

The TOE implements SSH protocol that complies with RFC(s) 4251, 4252, 4253, 4254, 4256, 4344, 5647, 5656, 6668, 8268, 8308 Section 3.1, and 8332.

NDcPP22e:FCS_SSHS_EXT.1.2:

The TOE supports public key authentication and password-based authentication.

The following public key algorithms: ssh-rsa, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521.

The TOE verifies the presented public key matches the one configured for the user by the administrator.

NDcPP22e:FCS_SSHS_EXT.1.3:

The TOE accepts packet size up to 262144 bytes and meets the requirements of RFC 4253. Any packet greater than the max size will be dropped and the connection will be terminated.

NDcPP22e:FCS_SSHS_EXT.1.4:

The TOE supports the following encryption algorithms: aes128-ctr, aes256-ctr for SSH transport. There are no optional characteristics specified for FCS_SSHS_EXT.1.4. This list is identical to those claimed for FCS_SSHS_EXT.1.4.

NDcPP22e:FCS_SSHS_EXT.1.5:

The following are the public key algorithms supported: rsa-sha2-256, rsa-sha2-512, and ecdsa-sha2-nistp256. There are no optional characteristics specified for FCS_SSHS_EXT.1.5. This list is identical to those claimed for FCS_SSHS_EXT.1.5.

NDcPP22e:FCS_SSHS_EXT.1.6:

The TOE supports the following data integrity MAC algorithms: hmac-sha2-256, and hmac-sha2-512. This list corresponds to the list in FCS_SSHS_EXT.1.6.

NDcPP22e:FCS_SSHS_EXT.1.7:

The TOE supports the following key exchange algorithms: diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, ecdh-sha2-nistp256, ecdh-sha2-nistp384, and ecdh-sha2-nistp521. This list corresponds to the list in FCS_SSHS_EXT.1.7.

NDcPP22e:FCS_SSHS_EXT.1.8:

The TOE is capable of rekeying. The TOE verifies the following thresholds:

- No longer than one hour
- No more than one gigabyte of transmitted data

The TOE continuously checks both conditions. When either of the conditions is met, the TOE will initiate a rekey.

NDcPP22e:FCS_TLSS_EXT.1:

NDcPP22e:FCS_TLSS_EXT.1.1:

The TOE supports the following ciphersuites:

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492,
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492,
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289,

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289

NDcPP22e:FCS_TLSS_EXT.1.2:

The TOE's server includes a non-modifiable configuration that prohibits all TLS versions other than v1.2. If the TOE receives a TLS attempt using a version other than v1.2 the connection attempt will be rejected.

NDcPP22e:FCS_TLSS_EXT.1.3:

The TOE includes ECDHE ciphersuites and supports curves secp256r1, secp384r1, secp521r1.

NDcPP22e:FCS_TLSS_EXT.1.4:

The TOE supports session resumption based on session tickets that adhere to the format provided in section 4 RFC 5077. The session tickets are encrypted using symmetric algorithms AES used in CBC and GCM modes and key sizes of 128 and 256 bits.

6.3 Identification and authentication

NDcPP22e:FIA_AFL.1:

The TOE allows the administrator to configure the number of successive failed authentication attempts.

When a user fails to authenticate a number of times equal to the configured limit, the TOE locks the claimed user identity until the configured time is reached.

Administrators can configure unsuccessful authentication attempts range between 3 – 15 within 60 minutes. When the account is locked, the TOE does not permit any further actions until the account is accessible.

The authentication failures cannot lead to a situation where no administrator access is available since the local CLI would not be subject to lockout.

NDcPP22e:FIA_PMG_EXT.1:

The TOE provides the following password management capabilities for administrator passwords:

- Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)” ,“ ~ “,“ “.
- Minimum password lengths shall be configurable to 8 characters to maximum of 64 characters. The default minimum password length is 8 characters.

NDcPP22e:FIA_UAU.7:

Password are obscured to the users. For all authentication at the local CLI the TOE displays only "*" characters when the administrative password is entered

NDcPP22e:FIA_UAU_EXT.2:

The TOE provides a local password-based authentication mechanism to perform local administration user authentication.

NDcPP22e:FIA_UIA_EXT.1:

The TOE does not permit any actions prior to Administrators logging into the TOE. They can view the banner at the login prompt.

Administrative access to the TOE is facilitated through one of several interfaces:

- Connecting to the console port by plugging a keyboard and monitor directly into the ports on the back of the TOE
- Remotely connecting to each appliance via SSHv2
- Remotely connecting to each appliance via the TOE's TLS Web UI

For local administration, the TOE prompts the user for a username and password. When the user provides the correct username and password, this is compared to the known user database and if they match then the user is granted access. Otherwise, the user will not be granted access to the TOE. The TOE does not provide a reason for failure in the cases of a login failure.

For remote SSH administration, the TOE supports RSA and ECDSA public key authentication. If the user uses public key-based authentication and it is successful, then the user is granted access to the TOE. If the user enters invalid user credentials, they will not be granted access and will be presented the login page. Username and password are also supported. If the username and password match the expected value, the administrator will be granted access, or if the values do not match, the administrator will be denied. In the case of a failed login attempt, the account lockout counter will be incremented.

For remote TLS Web UI administration, the TOE supports a username and password. When the user provides the correct username and password, this is compared to the known user database and if they match then the user is granted access. Otherwise, the user will not be granted access to the TOE. The TOE does not provide a reason for failure in the cases of a login failure.

NDcPP22e:FIA_X509_EXT.3:

In addition to the Common Name, Organization, Organizational Unit, and Country, the TOE additionally allows an administrator to specify the State, Locality, Email, and a list of Subject Alternative Names that the TOE will include in the Certificate Signing Request (CSR) it generates.

6.4 Security management

NDcPP22e:FMT_MOF.1/AutoUpdate:

The TOE permits the administrator (either through the TOE's Web UI or through its CLI) to enable the TOE to contact Corelight's servers to automatically check for new firmware releases. Additionally, the administrator can further specify whether the TOE should automatically download and install new firmware release, as they become available. The security administrator can enable automatic updates on the TOE by toggling on the feature "Install software updates" under the configuration -> maintain screen. Once that feature is enabled, the TOE will automatically apply any software updates as they become available. If disabled, the TOE lists the available updates (without applying them) so that the security administrator can then choose which update to apply manually.

NDcPP22e:FMT_MOF.1/Functions:

The TOE allows the administrator to configure and modify transmission of the TOE's audit functionality via SFTP.

NDcPP22e:FMT_MOF.1/ManualUpdate:

Only Security Administrators can perform manual software updates.

NDcPP22e:FMT_MTD.1/CoreData:

Administrative users are required to login before being provided with access to any administrative functions. They can view the banner at the login prompt (both CLI and Web UI). The TOE restricts the ability to manage the TOE to Security Administrators. This includes handling of X509 certificates and the trust store.

The TOE maintains the following role: Security administrator (Admin). The role defined has a set of permissions that will grant them access to the TOE data.

NDcPP22e:FMT_MTD.1/CryptoKeys:

The TOE allows the administrator to generate new SSH host keys, to generate (CSR) or import the TOE's TLS server certificate (for the Web UI).

NDcPP22e:FMT_SMF.1:

The TOE provides all the capabilities necessary to securely manage the TOE. The administrative user can connect to the TOE using the CLI to perform the below functions via SSHv2, using the TOE's Web UI, or at the local console. Refer to the Guidance documentation for configuration syntax, commands, and information related to each of these functions.

The Security Administrator (admin) has the following privileges:

- Ability to administer the TOE locally and remotely;
- Ability to configure the access banner;
- Ability to configure the session inactivity time before session termination or locking;
- Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates;
- Ability to configure the authentication failure parameters for FIA_AFL.1;
- Ability to configure audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full);
- Ability to manage the cryptographic keys,
- Ability to configure the cryptographic functionality;
- Ability to enable or disable automatic checking for updates or automatic updates;
- Ability to set the time which is used for time-stamps;
- Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;
- Ability to import X509v3 certificates to the TOE's trust store,
- Ability to manage the trusted public keys database

NDcPP22e:FMT_SMR.2:

The TOE maintains the following user role: Security Administrator (Admin).The Security Administrator can manage the TOE both locally and remotely.

6.5 Protection of the TSF

NDcPP22e:FPT_APW_EXT.1:

All passwords are stored in a secure directory that is not readily accessible to administrators through any interface. The passwords are stored as SHA-512 salted hash.

NDcPP22e:FPT_SKP_EXT.1:

The TOE stores all pre-shared keys, symmetric keys and private keys in plaintext in a secure storage location that is not accessible through an interface to administrators.

Refer to the table in the **NDcPP22e:FCS_CKM.4** section for details on key storage and destruction.

NDcPP22e:FPT_STM_EXT.1:

The TOE provides reliable time stamps. The clock function is reliant on the system clock provided by the underlying hardware.

The following security functions make use of the time:

- Audit events
- Session inactivity
- Certificate validation (for validity/expiration)

NDcPP22e:FPT_TST_EXT.1:

All crypto algorithms used by the TOE go through power up self-tests (KAT) before they can be used to provide service. The TOE executes the following power-on self-tests using Known Answer Tests (in which the TOE tests the algorithm using known inputs [plaintext, keys, messages, seed, etc.] and verifies that the algorithm produces the expected/known output [signature, ciphertext, hash, random output, etc.]):

- SHA KAT
- AES KAT
- HMAC SHA KAT
- DRBG KAT
- ECDH KAT
- GCM KAT
- RSA KAT
- ECDSA KAT

When device detects a failure during one or more of the self-tests, it raises an alarm. The administrator can attempt to reboot the TOE to clear the error. If rebooting the device does not resolve the issue, then the administrator should contact their next level of support or their Corelight support group for further assistance. All power up self-tests execution is logged for both successful and unsuccessful completion.

The Software Integrity Test is run automatically on start-up, and whenever the system images are loaded. These tests are sufficient to verify that the correct version of the TOE software is running as well as that the cryptographic operations are all performing as expected.

NDcPP22e:FPT_TUD_EXT.1:

Security Administrators can query the current version of the TOE and they are able to perform manual software updates. The currently active version of the TOE can be queried by issuing the “corelight-client information get” command.

When software updates are become available, the administrator can obtain and install the updates. The TOE can alternatively automatically download new updates as described in NDcPP22e:FMT_MOF.1/AutoUpdate.

The software images are digitally signed using RSA digital signature mechanism. The TOE will use a public key in order to verify the digital signature, upon successful verification the image will be loaded onto the TOE. If the images cannot be verified, the image will not be loaded onto the TOE.

6.6 TOE access

NDcPP22e:FTA_SSL.3:

A Security Administrator can configure maximum inactivity times for administrative sessions through the TOE local CLI and remote SSH interfaces. The default inactivity time period is 60 minutes for both the CLI and SSH interfaces. The configuration of inactivity period is applied on a per interface basis. A configured inactivity period will be applied to both local and remote sessions in the same manner. When the interface has been idle for more than the configured period, the session will be terminated and will require authentication to establish a new session.

The TOE will terminate the local/SSH administrative session after a Security Administrator defined period of inactivity. The inactivity time-out for CLI can be configured by the following commands:

```
corelight-client configuration update --security.auto_logout.enable=1

corelight-client configuration update --security.auto_logout.timeout=1
```

The TOE maintains separate settings for its Web UI, which allow the Security Administrator to configure the idle user session timeout (in minutes). By default, the TOE does not enforce an inactivity time period, but once the admin enabled the auto logout, the TOE allows the admin to configure the timeout in minutes. The configuration of inactivity period is applied to all Web UI admin sessions. When the interface has been idle for more than the configured period, the TOE will automatically logout (effectively terminate) the administrator from their Web UI session and require authentication to establish a new session.

The TOE's Web UI (under "Login Behaviors") allows an administrator to "Enable auto logout for idle user sessions" and then specify the "Timeout (min)".

NDcPP22e:FTA_SSL.4:

The Security Administrator can terminate their local CLI and remote SSH sessions by typing "exit" at the prompt. Likewise, the administrator can terminate their remote Web UI session by closing their web browser or selecting "logout".

NDcPP22e:FTA_SSL_EXT.1:

See NDcPP22e:FTA_SSL.3 above

NDcPP22e:FTA_TAB.1:

Security Administrators can create a customized login banner that will be displayed at the following interfaces:

- Local CLI
- Remote CLI via SSH v2
- Remote Web UI via TLS

This banner will be displayed prior to allowing Security Administrator access through those interfaces.

The banner will be same for local CLI and SSH remote methods of access and can be configured during initial configuration. The TOE maintains a separate banner for the Web UI , which that admin can configure and update.

6.7 Trusted path/channels

NDcPP22e:FTP_ITC.1:

The TOE supports secure communication to the following IT entities: Audit server (via SFTP).The TOE protects communications between the TOE and the SFTP audit server using SFTP (FTP over the SSH v2 protocol). The TOE acts as a client in all cases. The protocols listed are consistent with those included in the requirements in the ST.

NDcPP22e:FTP_TRP.1/Admin:

The TOE supports SSH v2.0 for secure remote CLI administration and supports HTTPS/TLSS for secure remote WebUI. SSH v2.0 session is encrypted using AES encryption to protect confidentiality and uses HMACs to protect integrity of traffic.

The TOE also supports TLS for secure remote Web UI administration of the TOE. The TLS v1.2 session is also encrypted using AES to protect confidentiality and uses HMAC or GCM to protect integrity of traffic. The protocols listed are consistent with those specified in the requirement.