NETSCOUT™

Sightline and Threat Mitigation System v9.7

Security Target

Version 1.9

May 2024

Document prepared by

Lightship Security

www.lightshipsec.com

Document History

Version	Date	Author	Description
1.0	31 Jan 2023	M Baldock	Published to 1.0
1.1	02 Mar 2023	M Baldock	Consistency fixes
1.2	13 Jun 2023	M Baldock	Addressing OR04
1.3	14 Jul 2023	M Baldock	Addressing OR05
1.4	31 Oct 2023	M Baldock	Addressing OR06
1.5	17 Jan 2024	M Baldock	Addressing OR09
1.6	31 Jan 2024	M Baldock	Addressing OR08
1.7	19 Apr 2024	M Baldock	Addressing OR10
1.8	07 May 2024	M Baldock	Addressing OR11
1.9	13 May 2024	M Baldock	Correcting identifiers

Table of Contents

List of Tables

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the NETSCOUT Sightline and Threat Mitigation System v9.7 Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

2 NETSCOUT Sightline and Threat Mitigation System (TMS) is a distributed TOE. Sightline provides comprehensive network visibility and reporting capabilities to detect and understand availability threats and improve traffic engineering and service performance. TMS surgically removes DDoS attack traffic from the network without disrupting key network services.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	NETSCOUT Sightline and Threat Mitigation System v9.7 Build: 9.7.0.1
Security Target	NETSCOUT Sightline and Threat Mitigation System v9.7 Security Target, v1.9

1.3 Conformance Claims

3 This ST supports the following conformance claims:

a) CC version 3.1 revision 5

b) CC Part 2 extended

c) CC Part 3 conformant

d) collaborative Protection Profile for Network Devices, v2.2e (referenced within as NDcPP)

e) NIAP Technical Decisions per Table 2

Table 2: NIAP Technical Decisions

TD #	Name
TD0527	Updates to Certificate Revocation Testing (FIA_X509_EXT.1)
TD0528	NIT Technical Decision for Missing EAs for FCS_NTP_EXT.1.4
TD0536	NIT Technical Decision for Update Verification Inconsistency
TD0537	NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3
TD0546	NIT Technical Decision for DTLS - clarification of Application Note 63
TD0547	NIT Technical Decision for Clarification on developer disclosure of AVA_VAN

TD #	Name
TD0555	NIT Technical Decision for RFC Reference incorrect in TLSS Test
TD0556	NIT Technical Decision for RFC 5077 question
TD0563	NiT Technical Decision for Clarification of audit date information
TD0564	NiT Technical Decision for Vulnerability Analysis Search Criteria
TD0569	NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7
TD0570	NiT Technical Decision for Clarification about FIA_AFL.1
TD0571	NiT Technical Decision for Guidance on how to handle FIA_AFL.1
TD0572	NiT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers
TD0580	NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e
TD0581	NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3
TD0591	NIT Technical Decision for Virtual TOEs and hypervisors
TD0592	NIT Technical Decision for Local Storage of Audit Records
TD0631	NIT Technical Decision for Clarification of public key authentication for SSH Server
TD0632	NIT Technical Decision for Consistency with Time Data for vNDs
TD0635	NIT Technical Decision for TLS Server and Key Agreement Parameters
TD0636	NIT Technical Decision for Clarification of Public Key User Authentication for SSH
TD0638	NIT Technical Decision for Key Pair Generation for Authentication
TD0639	NIT Technical Decision for Clarification for NTP MAC Keys
TD0670	NIT Technical Decision for Mutual and Non-Mutual Auth TLSC Testing
TD0738	NIT Technical Decision for Link to Allowed-With List
TD0790	NIT Technical Decision: Clarification Required for testing IPv6
TD0792	NIT Technical Decision: FIA_PMG_EXT.1 - TSS EA not in line with SFR
TD0800	Updated NIT Technical Decision for IPsec IKE/SA Lifetimes Tolerance

1.4 Terminology

Table 3: Terminology

Term	Definition
CC	Common Criteria
EAL	Evaluation Assurance Level
NDcPP	collaborative Protection Profile for Network Devices
PP	Protection Profile
TMS	Threat Mitigation System
TOE	Target of Evaluation
TSF	TOE Security Functionality

2 TOE Description

2.1 Type

4 The TOE is a distributed network device that provides network visibility and threat mitigation.

2.2 Usage

5 The TOE is deployed within a network that provides connectivity to the monitored services. The Sightline GUI provides the primary means of management for both Sightline and TMS. The TOE interfaces within the scope of evaluation are shown in Figure 1.

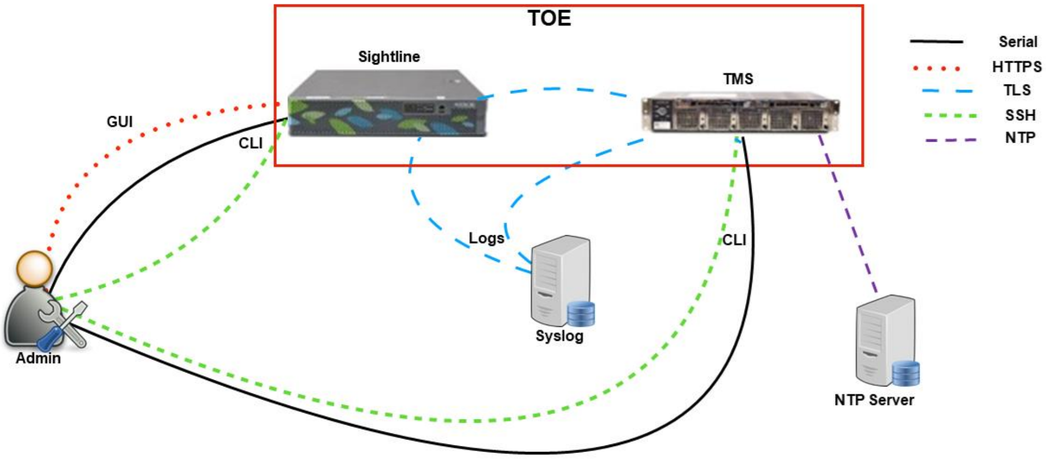

Figure 1: TOE interfaces

6 The TOE interfaces are as follows:

a) **Sightline CLI.** Administrative CLI via direct serial connection and SSH.

b) **Sightline GUI.** Administrative web GUI via HTTPS.

c) **Sightline connection with TMS.** Bi-directional TLS connections between Sightline and TMS.

d) **TMS CLI.** Administrative CLI via direct serial connection and SSH.

e) **Logs.** Sightline and TMS forwarding of logs to a remote syslog server via TLS.

2.3 Security Functions / Logical Scope

7 The TOE provides the following security functions:

a) **Protected Communications.** The TOE protects the integrity and confidentiality of communications as noted in section 2.2above.

b) **Secure Administration.** The TOE enables secure management of its security functions, including:

i) Administrator authentication with passwords

ii) Configurable password policies

iii) Role Based Access Control

iv) Access banners

v) Management of critical security functions and data

vi) Protection of cryptographic keys and passwords

c) **Trusted Update.** The TOE ensures the authenticity and integrity of software updates through digital signatures.

d) **System Monitoring.** The TOE generates logs of security relevant events. The TOE stores logs locally and is capable of sending log events to a remote audit server.

e) **Self-Test.** The TOE performs a suite of self-tests to ensure the correct operation and enforcement of its security functions.

f) **Cryptographic Operations.** The TOE implements a cryptographic module. Relevant Cryptographic Algorithm Validation Program (CAVP) certificates are shown in Table 4.

Table 4: CAVP Certificates

Algorithm Capability	Certificate
AES-CBC, AES-CTR, AES-GCM	C2144
SHA-1 / SHA2-256 / SHA2-384 / SHA2-512	
HMAC SHA1 / SHA256 / SHA384 / SHA512	
ECDSA KeyGen / SigGen / SigVer	
RSA SigGen / SigVer	
DSA KeyGen / SigGen / SigVer	
Counter DRBG, Hash DRBG, HMAC DRGB	
KAS-FFC-SSC Sp800-56Ar3	A1882

2.4 Physical Scope

8 The physical boundary of the TOE includes all software and hardware shown in Table 5. The TOE is delivered via commercial courier.

Table 5: TOE models

Component	Model	CPU	Software	Differences	CAVP Coverage
Sightline	SP-7000	Intel Xeon E5-2648L v3 (Haswell)	ArbOS 7.3 & SP 9.7.0.1	Network interfaces	C2144 A1882
	SP-7500	Intel Xeon Gold 5218T (Cascade Lake)			
TMS	TMS-2600	Intel Xeon E5-2608L v3 (Haswell)	ArbOS 7.3 & TMS 9.7.0.1	Throughput speeds Network interfaces Storage capacity	
	TMS-2800	Intel Xeon E5-2648L v3 (Haswell)			
	TMS-8100	Intel Xeon Silver 4210T (Cascade Lake)			

2.4.1 Guidance Documents

9 The TOE includes the following guidance documents (PDF):

a) NETSCOUT Sightline and Threat Mitigation System v9.7 Common Criteria Guide, v1.5

b) NETSCOUT Sightline and Threat Mitigation System User Guide Version 9.7.0.0

c) Software Threat Mitigation System Installation on Hardware Guide Version 9.6.0.0

d) Sightline Virtual Machine Installation Guide Version 9.7.0.0

10 Registered users download the guidance documents from NETSCOUT’s web portal. https://www.netscout.com/support-services

2.4.2 Non-TOE Components

11 The TOE operates with the following components in the environment:

a) **Syslog Server.** The TOE sends audit events to a remote syslog server.

b) **NTP Server.** The TOE makes use of an NTP server to set time.

c) **OCSP Responder.** The TOE makes use of an OCSP Responder to verify the revocation status of X.509 certificates.

2.4.3 Functions not included in the TOE Evaluation

12 The scope of evaluated security functions is limited to those identified at 2.3.

13 Functions not included in scope are the REST API. The RES API is disabled when no API tokens are generated, rendering the endpoints unusable. By default the TOE contains no API tokens and no action is required by the administrator.

3 Security Problem Definition

14 The Security Problem Definition is reproduced from section 4 of the NDcPP.

3.1 Threats

Table 6: Threats

Identifier	Description
T.UNAUTHORIZED_ ADMINISTRATOR_ ACCESS	Threat agents may attempt to gain Administrator access to the Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_ CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_ COMMUNICATION_ CHANNELS	Threat agents may attempt to target Network Devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the Network Device itself.
T.WEAK_ AUTHENTICATION_ ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.
T.UPDATE_ COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and

Identifier	Description
	the Administrator would have no knowledge that the device has been compromised.
T.SECURITY_ FUNCTIONALITY_ COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
T.PASSWORD_ CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other Network Devices.
T.SECURITY_ FUNCTIONALITY_ FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

3.2 Assumptions

Table 7: Assumptions

Identifier	Description
A.PHYSICAL_ PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.LIMITED_ FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality). In the case of vNDs, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of the distributed TOE run inside more than one virtual machine (VM) on a single VS. There are no other guest VMs on the physical platform providing non-Network Device functionality.

Identifier	Description
A.NO_THRU_ TRAFFIC_ PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the NDcPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
A.TRUSTED_ ADMINISTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_ UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_ CREDENTIALS_ SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.RESIDUAL_ INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
A.COMPONENTS_ RUNNING	For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.

3.3 Organizational Security Policies

Table 8: Organizational Security Policies

Identifier	Description
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

4 Security Objectives

15 The security objectives are reproduced from section 5 of the NDcPP.

Table 9: Security Objectives for the Operational Environment

Identifier	Description
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
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.
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.TRUSTED_ADMIN	Security 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.
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.COMPONENTS_ RUNNING	For distributed TOEs, the Security Administrator ensures that the availability of every TOE component is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. The Security Administrator also ensures that it is checked as appropriate for every TOE component that the audit functionality is running properly

Identifier	Description
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.

5 Security Requirements

5.1 Conventions

16 This document uses the following font conventions to identify the operations defined by the CC:

a) **Assignment.** Indicated with italicized text.

b) **Refinement.** Indicated with bold text and strikethroughs.

c) **Selection.** Indicated with underlined text.

d) **Assignment within a Selection:** Indicated with italicized and underlined text.

e) **Iteration.** Indicated by adding a string starting with "/" (e.g. "FCS_COP.1/Hash").

17 **Note:** Operations performed within the Security Target are denoted within brackets []. Operations shown without brackets are reproduced from the NDcPP.

5.2 Extended Components Definition

18 The Extended Components are defined in Appendix C of the NDcPP.

Table 10: Extended Components

Requirement	Title	Applicable TDs
FAU_GEN_EXT.1	Security Audit Data Generation for Distributed TOE	N/A
FAU_STG_EXT.1	Protected Audit Event Storage	N/A
FAU_STG_EXT.4	Protected Local Audit Event Storage for Distributed TOEs	N/A
FCO_CPC_EXT.1	Component Registration Channel Definition	N/A
FCS_HTTPS_EXT.1	HTTPS Protocol	N/A
FCS_RBG_EXT.1	Random Bit Generation	N/A
FCS_NTP_EXT.1	NTP Protocol	TD0639
FCS_SSHS_EXT.1	SSH Server Protocol	TD0631
FCS_TLSC_EXT.1	TLS Client Protocol Without Mutual Authentication	TD0670, TD0790
FCS_TLSS_EXT.1	TLS Server Protocol Without Mutual Authentication	TD0555, TD0556, TD0569, TD0635
FIA_PMG_EXT.1	Password Management	TD0571, TD0792

Requirement	Title	Applicable TDs
FIA_UIA_EXT.1	User Identification and Authentication	N/A
FIA_UAU_EXT.2	Password-based Authentication Mechanism	N/A
FIA_X509_EXT.1/Rev	X.509 Certificate Validation	TD0527
FIA_X509_EXT.1/ITT	X.509 Certificate Validation	TD0527
FIA_X509_EXT.2	X.509 Certification Authentication	TD0537
FIA_X509_EXT.3	X.509 Certificate Requests	N/A
FPT_SKP_EXT.1	Protection of TSF Data (for reading of all symmetric keys)	TD0639
FPT_APW_EXT.1	Protection of Administrator Passwords	N/A
FPT_TST_EXT.1	TSF Testing	N/A
FPT_TUD_EXT.1	Trusted Update	N/A
FPT_STM_EXT.1	Reliable Time Stamps	TD0639
FTA_SSL_EXT.1	TSF-initiated Session Locking	N/A

5.3 Functional Requirements

19 Table 11 provides a summary of the SFRs and identifies which distributed TOE component implements the SFR.

Table 11: Summary of SFRs

Requirement	Title	Allocation
FAU_GEN.1	Audit Data Generation	All
FAU_GEN_EXT.1	Security Audit Data Generation for Distributed TOE	All
FAU_GEN.2	User Identity Association	All
FAU_STG_EXT.1	Protected Audit Event Storage	All
FAU_STG_EXT.4	Protected Local Audit Event Storage for Distributed TOEs	All
FCO_CPC_EXT.1	Component Registration Channel Definition	All

Requirement	Title	Allocation
FCS_CKM.1	Cryptographic Key Generation	All
FCS_CKM.2	Cryptographic Key Establishment	All
FCS_CKM.4	Cryptographic Key Destruction	All
FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)	All
FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)	All
FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)	All
FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)	All
FCS_HTTPS_EXT.1	HTTPS Protocol	Sightline
FCS_RBG_EXT.1	Random Bit Generation	All
FCS_NTP_EXT.1	NTP Protocol	TMS
FCS_SSHS_EXT.1	SSH Server Protocol	All
FCS_TLSC_EXT.1	TLS Client Protocol Without Mutual Authentication	All
FCS_TLSS_EXT.1	TLS Server Protocol Without Mutual Authentication	All
FIA_AFL.1	Authentication Failure Management	All
FIA_PMG_EXT.1	Password Management	All
FIA_UIA_EXT.1	User Identification and Authentication	All
FIA_UAU_EXT.2	Password-based Authentication Mechanism	All
FIA_UAU.7	Protected Authentication Feedback	All
FIA_X509_EXT.1/Rev	X.509 Certificate Validation	All
FIA_X509_EXT.1/ITT	X.509 Certificate Validation	All
FIA_X509_EXT.2	X.509 Certificate Authentication	All
FIA_X509_EXT.3	X.509 Certificate Requests	All

Requirement	Title	Allocation
FMT_MOF.1/ManualUpdate	Management of Security Functions Behaviour	All
FMT_MOF.1/Services	Management of Security Functions Behaviour	All
FMT_MTD.1/CoreData	Management of TSF Data	All
FMT_MTD.1/CryptoKeys	Management of TSF Data	All
FMT_SMF.1	Specification of Management Functions	All
FMT_SMR.2	Restrictions on Security Roles	All
FPT_APW_EXT.1	Protection of Administrator Passwords	All
FPT_ITT.1	Basic internal TSF data transfer protection	All
FPT_SKP_EXT.1	Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)	All
FPT_TST_EXT.1	TSF Testing	All
FPT_TUD_EXT.1	Trusted Update	All
FPT_STM_EXT.1	Reliable Time Stamps	All
FTA_SSL_EXT.1	TSF-initiated Session Locking	All
FTA_SSL.3	TSF-initiated Termination	All
FTA_SSL.4	User-initiated Termination	All
FTA_TAB.1	Default TOE Access Banners	All
FTP_ITC.1	Inter-TSF trusted channel	All
FTP_TRP.1/Admin	Trusted Path	All

5.3.1 Security Audit (FAU)

FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

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

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~~ Table 12**.*

Table 12: Audit Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG_EXT.1	None.	None.
FAU_STG_EXT.4	None.	None.
FCO_CPC_EXT.1	• Enabling communications between a pair of components. • Disabling communications between a pair of components.	Identities of the endpoint pairs enabled or disabled.
FCS_CKM.1	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.
FCS_COP.1/DataEncryption	None.	None.
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.

Requirement	Auditable Events	Additional Audit Record Contents
FCS_RBG_EXT.1	None.	None.
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address)
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of identification and authentication mechanism	Origin of the attempt (e.g., IP address)
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address)
FIA_UAU.7	None.	None.
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MTD.1/CoreData	None.	None.
FMT_SMF.1	All management activities of TSF data.	None.
FMT_SMR.2	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None.
FPT_STM_EXT.1	Discontinuous changes to time – either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FTA_SSL_EXT.1 (if “lock session” is selected)	Any attempts at unlocking of an interactive session	None.
FTA_SSL_EXT.1 (if “terminate the session” is selected)	The termination of a local session by the session locking mechanism	None.

Requirement	Auditable Events	Additional Audit Record Contents
FTA_SSL.3	The termination of a remote session by the session locking mechanism	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.
FTP_ITC.1	• Initiation of the trusted channel. • Termination of the trusted channel. • Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FTP_TRP.1/Admin	• Initiation of the trusted path. • Termination of the trusted path. • Failure of the trusted path functions.	None.
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate Any addition, replacement or removal of trust anchors in the TOE's trust store	Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store
FIA_X509_EXT.1/ITT	Unsuccessful attempt to validate a certificate Any addition, replacement or removal of trust anchors in the TOE's trust store	Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store
FIA_X509_EXT.2	None	None
FIA_X509_EXT.3	None	None

Requirement	Auditable Events	Additional Audit Record Contents
FPT_ITT.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.
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Reason for failure
FCS_NTP_EXT.1	• Configuration of a new time server • Removal of configured time server	Identity if new/removed time server
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure
FCS_TLSC_EXT.1	Failure to establish a TLS Session	Reason for failure
FCS_TLSS_EXT.1	Failure to establish a TLS Session	Reason for failure
FMT_MOF.1/Services	None	None
FMT_MTD.1/CryptoKeys	None	None

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~~ Table 12***.

FAU_GEN_EXT.1 Security Audit Data Generation

FAU_GEN_EXT.1.1 The TSF shall be able to generate audit records for each TOE component. The audit records generated by the TSF of each TOE component shall include the subset of security relevant audit events which can occur on the TOE component.

FAU_GEN.2 User Identity Association

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.

FAU_STG_EXT.1 Protected Audit Event Storage

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.

FAU_STG_EXT.1.2 The TSF shall be able to store generated audit data on the TOE itself. In addition [

- The TOE shall be a distributed TOE that stores audit data on the following TOE components: *Sightline and TMS*

]

FAU_STG_EXT.1.3 The TSF shall [overwrite previous audit records according to the following rule: [*overwrite oldest record first*], [*no other action*]] when the local storage space for audit data is full.

FAU_STG_EXT.4 Protected Local Audit Event Storage for Distributed TOEs

FAU_STG_EXT.4.1 The TSF of each TOE component which stores security audit data locally shall perform the following actions when the local storage space for audit data is full: [

Sightline: [overwrite previous audit records according to the following rule: [overwrite oldest record first]],

TMS: [overwrite previous audit records according to the following rule: [overwrite oldest record first]]

].

5.3.2 Communication (FCO)

FCO_CPC_EXT.1 Component Registration Channel Definition

FCO_CPC_EXT.1.1 The TSF shall require a Security Administrator to enable communications between any pair of TOE components before such communication can take place.

FCO_CPC_EXT.1.2 The TSF shall implement a registration process in which components establish and use a communications channel that uses [

- No channel]

for at least *TSF data*.

FCO_CPC_EXT.1.3 The TSF shall enable a Security Administrator to disable communications between any pair of TOE components.

5.3.3 Cryptographic Support (FCS)

FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm: [

- 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 7919]

]~~and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards]~~.

FCS_CKM.2 Cryptographic Key Establishment

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”;
- 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 7919];

] ~~that meets the following: [assignment: list of standards].~~

Application note: This SFR was changed by TD0580 and TD0581.

Application note: The TOE supports RSA-based key establishment only under TLS Client connections and SSH public key authentication, where key generation is not present.

FCS_CKM.4 Cryptographic Key Destruction

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 [*
    - *instructs a part of the TSF to destroy the abstraction that represents the key*

] that meets the following: *No Standard*.

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

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].

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

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, 4096*],
- Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [*256, 384, 521*],

] 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]

FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)

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 cryptographic key sizes [assignment: cryptographic key sizes]~~ and **message digest sizes [160, 256, 384, 512] bits** that meet the following: *ISO/IEC 10118-3:2004*.

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

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-512] and cryptographic key sizes *[160,* *256, 512]* **and message digest sizes [160, 256, 512] bits** that meet the following: *ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”*.

FCS_RBG_EXT.1 Random Bit Generation

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)].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [[*one*] platform-based noise source] with a minimum of [256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

FCS_HTTPS_EXT.1 HTTPS Protocol

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS.

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.

FCS_NTP_EXT.1 NTP Protocol

FCS_NTP_EXT.1.1 The TSF shall use only the following NTP version(s) [NTP v4 (RFC 5905)].

FCS_NTP_EXT.1.2 The TSF shall update its system time using [

- Authentication using [SHA1]as the message digest algorithm(s);

].

FCS_NTP_EXT.1.3 The TSF shall not update NTP timestamp from broadcast and/or multicast addresses.

FCS_NTP_EXT.1.4 The TSF shall support configuration of at least three (3) NTP time sources in the Operational Environment.

FCS_SSHS_EXT.1 SSH Server Protocol

FCS_SSHS_EXT.1.1 The TSF shall implement the SSH protocol that complies with: RFC(s) 4251, 4252, 4253, 4254, [4344, 5656, 6668, 8268, 8308 section 3.1, 8332].

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].

Application note: This SFR was changed by TD0631.

FCS_SSHS_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [*256 kilo*]bytes in an SSH transport connection are dropped.

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, aes128-gcm@openssh.com, aes256-gcm@openssh.com].

FCS_SSHS_EXT.1.5 The TSF shall ensure that the SSH public-key based authentication implementation uses [ssh-rsa, 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.

Application note: The TOE supports RSA and ECDSA for user public key authentication and ECDSA for server host keys.

FCS_SSHS_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses [hmac-sha1, hmac-sha2-256, hmac-sha2-512] as its MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHS_EXT.1.7 The TSF shall ensure that [diffie-hellman-group14-sha1, ecdh-sha2-nistp256] and [diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, ecdh-sha2-nistp384, ecdh-sha2-nistp521] are the only allowed key exchange methods used for the SSH protocol.

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.

FCS_TLSC_EXT.1 TLS Client Protocol without Mutual Authentication

FCS_TLSC_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_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492

- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_DHE_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_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289

]and no other ciphersuites.

FCS_TLSC_EXT.1.2 The TSF shall verify that the presented identifier matches [the reference identifier per RFC 6125 section 6, IPv4 address in CN or SAN and no other attribute types].

FCS_TLSC_EXT.1.3 When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also [

- Not implement any administrator override mechanism].

FCS_TLSC_EXT.1.4 The TSF shall [present the Supported Elliptic Curves/Supported Groups Extension with the following curves/groups: [secp256r1, secp384r1, secp521r1] and no other curves] in the Client Hello.

FCS_TLSS_EXT.1 TLS Server Protocol Without Mutual Authentication

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_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

] and no other ciphersuites.

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].

FCS_TLSS_EXT.1.3 The TSF shall perform key establishment for TLS using [ECDHE curves [secp256r1] and no other curves]].

FCS_TLSS_EXT.1.4 The TSF shall support [session resumption based on session IDs according to RFC 4346 (TLS1.1) or RFC 5246 (TLS1.2), session resumption based on session tickets according to RFC 5077].

5.3.4 Identification and Authentication (FIA)

FIA_AFL.1 Authentication Failure Management

FIA_AFL.1.1 The TSF shall detect when an Administrator configurable positive integer within [*1-10*] unsuccessful authentication attempts occur related to *Administrators attempting to authenticate remotely using a password*.

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 [*account unlocked via local console*] is taken by an Administrator;].

FIA_PMG_EXT.1 Password Management

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 [*7*] and [*72*] *characters.*

FIA_UIA_EXT.1 User Identification and Authentication

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]]

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.

FIA_UAU_EXT.2 Password-based Authentication Mechanism

FIA_UAU_EXT.2.1 The TSF shall provide a local [password-based] authentication mechanism to perform local administrative user authentication.

FIA_UAU.7 Protected Authentication Feedback

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**.

FIA_X509_EXT.1/Rev X.509 Certificate Validation

FIA_X509_EXT.1.1/Rev The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation supporting a minimum path length of three certificates.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [the Online Certificate Status Protocol (OCSP) as specified in RFC 6960].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
    - Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
    - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
    - Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
    - OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

FIA_X509_EXT.1.2/Rev The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

FIA_X509_EXT.1/ITT X.509 Certificate Validation

FIA_X509_EXT.1.1/ITT The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation supporting a minimum path length of two certificates.
- The certificate path must terminate with a trusted CA certificate.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [no revocation method]
- The TSF shall validate the extendedKeyUsage field according to the following rules:
    - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
    - Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
    - OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

FIA_X509_EXT.1.2/ITT The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [TLS], and [no additional uses].

FIA_X509_EXT.2.2 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [not accept the certificate].

FIA_X509_EXT.3 X.509 Certificate Requests

FIA_X509_EXT.3.1 The TSF shall generate a Certificate 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]

FIA_X509_EXT.3.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

5.3.5 Security Management (FMT)

FMT_MOF.1/ManualUpdate Management of security functions Behaviour

FMT_MOF.1.1/ManualUpdate The TSF shall restrict the ability to enable the functions *to perform manual updates* to *Security Administrators*.

FMT_MOF.1/Services Management of Security Functions Behaviour

FMT_MOF.1.1/Services The TSF shall restrict the ability to **start and stop** ~~the functions~~ **services** to Security Administrators.

FMT_MTD.1/CoreData Management of TSF Data

FMT_MTD.1.1/CoreData The TSF shall restrict the ability to *manage* the *TSF data to Security Administrators*.

FMT_MTD.1/CryptoKeys Management of TSF data

FMT_MTD.1.1/CryptoKeys The TSF shall restrict the ability to *manage* the *cryptographic keys to Security Administrators*.

FMT_SMF.1 Specification of Management Functions

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 start and stop services;
    - Ability to manage the cryptographic keys;
    - Ability to configure the interaction between TOE components;
    - Ability to re-enable an Administrator account;
    - Ability to set the time which is used for time-stamps;
    - Ability to configure NTP;
    - Ability to import X.509v3 certificates to the TOE's trust store;
    - Ability to manage the trusted public keys database;]

FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- *Security Administrator*.

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

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.

5.3.6 Protection of the TSF (FPT)

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

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

FPT_APW_EXT.1 Protection of Administrator Passwords

FPT_APW_EXT.1.1 The TSF shall store administrative passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext administrative passwords.

FPT_TST_EXT.1 TSF testing

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: [

- *BIOS tests*
- *Boot loader image verification*
- *Cryptographic module tests*].

FPT_TUD_EXT.1 Trusted update

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].

FPT_TUD_EXT.1.2 The TSF shall provide *Security Administrators* the ability to manually initiate updates to TOE firmware/software and [no other update mechanism].

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.

FPT_STM_EXT.1 Reliable Time Stamps

FPT_STM_EXT.1.1 The TSF shall be able to provide reliable time stamps for its own use.

FPT_STM_EXT.1.2 The TSF shall [allow the Security Administrator to set the time, synchronise time with an NTP server].

FPT_ITT.1 Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1 The TSF shall protect TSF data from [disclosure and detect its modification] when it is transmitted between separate parts of the TOE through the use of [TLS, HTTPS].

5.3.7 TOE Access (FTA)

FTA_SSL_EXT.1 TSF-initiated Session Locking

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [

- terminate the session]

after a Security Administrator-specified time period of inactivity.

FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1 The TSF shall terminate **a remote** interactive session after a *Security Administrator-configurable time interval of session inactivity*.

FTA_SSL.4 User-initiated Termination

FTA_SSL.4.1 Refinement: The TSF shall allow **Administrator**-initiated termination of the **Administrator's** own interactive session.

FTA_TAB.1 Default TOE Access Banners

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.

5.3.8 Trusted path/channels (FTP)

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall **be capable of using [TLS] 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**.

FTP_ITC.1.2 The TSF shall permit **the TSF or the authorized IT entities** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*audit server*].

FTP_TRP.1 /Admin Trusted Path

FTP_TRP.1.1/Admin The TSF shall **be capable of using [SSH, 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**.

FTP_TRP.1.2 /Admin The TSF shall permit remote **Administrators** to initiate communication via the trusted path.

FTP_TRP.1.3 /Admin The TSF shall require the use of the trusted path for initial *Administrator authentication and all remote administration actions*.

5.4 Assurance Requirements

20 The TOE security assurance requirements are summarized in Table 13.

Table 13: Assurance Requirements

Assurance Class	Components	Description
Security Target Evaluation	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.1	Security Objectives for the operational environment
	ASE_REQ.1	Stated Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Development	ADV_FSP.1	Basic Functional Specification
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative User Guidance
Life Cycle Support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM Coverage
Tests	ATE_IND.1	Independent Testing - conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability Analysis

21 In accordance with section 7.1 of the NDcPP, the following refinement is made to ASE:

a) **ASE_TSS.1.1C Refinement:** The TOE summary specification shall describe how the TOE meets each SFR. **In the case of entropy analysis, the TSS is used in conjunction with required supplementary information on Entropy.**

6 TOE Summary Specification

22 The following describes how the TOE fulfils each SFR included in section 5.3.

6.1 Security Audit

6.1.1 FAU_GEN.1

23 The TOE generates the audit records specified at FAU_GEN.1 containing the following fields:

a) Date/Time

b) Type of event

c) Message (including user if applicable and indication of success or failure)

24 The following information is logged as a result of the Security Administrator generating/importing or deleting cryptographic keys:

a) Cryptographic key name

b) Storage location

c) Function performed.

25 **Table 14** identifies the TOE components that generate the auditable events defined in FAU_GEN.1.1.

Table 14: Audit Events

Requirement	Auditable Events	TOE Component
FAU_GEN.1	Start-up and shutdown of the audit functions	All
	Administrative login and logout (Name of user account shall be logged if individual user accounts are required for Administrators)	All
	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)	All
	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)	All
	Resetting passwords (name of related user account shall be logged)	All

Requirement	Auditable Events	TOE Component
FCO_CPC_EXT.1	Enabling communications between a pair of components. Disabling communications between a pair of components. (Identities of the endpoints pairs enabled or disabled.)	All
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Sightline
FCS_NTP_EXT.1	Configuration of a new time server Removal of configured time server	TMS
FCS_SSHS_EXT.1	Failure to establish an SSH session	All
FCS_TLSC_EXT.1	Failure to establish a TLS Session	All
FCS_TLSS_EXT.1	Failure to establish a TLS Session	All
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	All
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	All
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	All
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate Any addition, replacement or removal of trust anchors in the TOE's trust store	All
FIA_X509_EXT.1/ITT	Unsuccessful attempt to validate a certificate Any addition, replacement or removal of trust anchors in the TOE's trust store	All
FIA_X509_EXT.2	X.509 Certificate Authentication	All
FIA_X509_EXT.3	X.509 Certificate Requests	All
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update	All
FMT_MOF.1/Services	Starting or stopping of services	All
FMT_SMF.1	All management activities of TSF data.	All

Requirement	Auditable Events	TOE Component
FPT_ITT.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	All
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	All
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)	All
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	All
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	All
FTA_SSL.4	The termination of an interactive session.	All
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	All
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	All

6.1.2 FAU_GEN_EXT.1

26 The TOE can generate audit records for each TOE component. The audit records generated by each TOE component include the subset of security relevant audit events which can occur on that component.

6.1.3 FAU_GEN.2

27 The TOE includes the user identity in audit events resulting from actions of identified users.

6.1.4 FAU_STG_EXT.1

28 The audit records are securely sent to a remote audit server in the operational environment using TLS. This prevents the audit records from unauthorized viewing and modification during transmission. Both TOE components transmit audit data to the remote audit server in real time using TLS.

29 The TOE logs all events related to startup/shutdown, external communications, user authentication, and user management (user creation/deletion, password changes, role changes) and administrative commands in the audit log.

30 The TOE is a distributed TOE with both components storing audit data locally. Local audit data is rotated daily. The local audit record will be rotated if it exceeds at minimum 1M, otherwise it will carry into the next day. The TOE maintains at most 7 days of records and will overwrite audit records starting with the oldest audit record.

31 Only authorized administrators may view audit records and no capability to modify the audit records is provided.

6.1.5 FAU_STG_EXT.4

32 Each TOE component stores audit data locally. Each component when local audit storage is full, will overwrite the oldest audit records first.

6.2 Communication

6.2.1 FCO_CPC_EXT.1

33 Registration of the TOE's components is performed manually by the Security Administrator and does not implement a registration channel.

34 To disable communication between the components, the Security Administrator can delete the TMS appliance entry using the Web GUI and clear the Sightline appliance entry via SSH or Local CLI.

35 The minimum configuration is the deployment of a Sightline and one TMS. Multiple TMS devices can be deployed and maintain their own separate communication channels with the Sightline and external IT entities that comply with FPT_ITT.1 and FTP_ITC.1. The TMS devices do not communicate with each other.

6.3 Cryptographic Support

6.3.1 FCS_CKM.1

36 The TOE supports key generation for the following asymmetric schemes:

a) **ECC P-256/P-384/P-521.** Used in TLS and SSH authentication and key exchange.

b) **FFC Safe Primes.** Used in SSH key exchange.

6.3.2 FCS_CKM.2

37 The TOE supports the following key establishment schemes:

a) **RSA schemes.** Used in SSH and TLS key exchange.

b) **ECC schemes.** Used in SSH and TLS key exchange. TOE is both sender and receiver.

c) **FFC schemes using safe primes.** Used in SSH key exchange. TOE is both sender and receiver. The following Diffie Helman groups are supported:

    i) Group 14 per RFC 3526 section 3

    ii) Group 16 per RFC 3526 section 5

    iii) Group 18 per RFC 3526 section 7

38 Table 15 below identifies the scheme being used by each service.

Table 15: Key Agreement Mapping

Scheme	SFR	Service
RSA	FCS_TLSC_EXT.1	TMS ITT TLS Client
ECC	FCS_SSHS_EXT.1	CLI / Administration
	FCS_TLSS_EXT.1	Sightline Web GUI / Sightline ITT Server
		TMS TLS Server
	FCS_TLSC_EXT.1	Sightline ITT TLS Client
		TMS ITT TLS Client
	FCS_TLSC_EXT.1	Sightline Audit Server
	FCS_TLSC_EXT.1	TMS Audit Server
FFC Safe Primes	FCS_SSHS_EXT.1	CLI / Administration
	FCS_TLSC_EXT.1	TMS TLS Client

6.3.3 FCS_CKM.4

39 Table 18 shows the origin, storage location and destruction details for cryptographic keys. Unless otherwise stated, the keys are generated by the TOE.

6.3.4 FCS_COP.1/DataEncryption

40 The TOE provides symmetric encryption and decryption capabilities using 128 and 256 bit AES in CBC, CTR and GCM mode. AES is implemented in TLS and SSH.

41 The relevant NIST CAVP certificate numbers are listed Table 4.

6.3.5 FCS_COP.1/SigGen

42 The TOE provides cryptographic signature generation and verification services using:

a) RSA Signature Algorithm with key size of 2048 and greater,

b) ECDSA with key size of 256, 384 and 521

43 The RSA signature verification services are used in the SSH protocol, TLS Client protocol and TOE firmware integrity checks.

44 The ECDSA signature verification services are used in the SSH and TLS protocols.

45 The relevant NIST CAVP certificate numbers are listed in Table 4.

6.3.6 FCS_COP.1/Hash

46 The TOE provides cryptographic hashing services using SHA-1, SHA-256, SHA-384 and SHA-512.

47 SHA is implemented in the following parts of the TSF:

a) SSH;

b) TLS;

c) Digital signature verification as part of trusted update validation; and

d) Hashing of passwords in non-volatile storage.

48 The relevant NIST CAVP certificate numbers are listed in Table 4.

6.3.7 FCS_COP.1/KeyedHash

49 The TOE provides keyed-hashing message authentication services using HMAC-SHA-1, HMAC-SHA-256, and HMAC-SHA-512.

50 HMAC is implemented in SSH.

51 The characteristics of the HMACs used in the TOE are given in Table 16.

Table 16: HMAC Characteristics

Algorithm	Block Size	Key Size	Digest Size
HMAC-SHA-1	512 bits	160 bits	160 bits
HMAC-SHA-256	512 bits	256 bits	256 bits
HMAC-SHA-512	1024 bits	512 bits	512 bits

52 The relevant NIST CAVP certificate numbers are listed in Table 4.

6.3.8 FCS_HTTPS_EXT.1

53 The TOE implements the HTTPS protocol, using HTTP over TLS compliant with RFC 2818.

54 The TOE does not require client authentication when presented with a peer certificate.

6.3.9 FCS_NTP_EXT.1

55 The TMS component supports NTPv4 using SHA-1 authentication. The TMS component allows configuration of up to 3 NTP servers. Broadcast and multicast address NTP timestamp updates are not accepted.

6.3.10 FCS_RBG_EXT.1

56 The TOE contains a CTR_DRBG that is seeded from a CPU provided entropy source. Entropy from the noise is conditioned and used to seed the DRBG with 256 bits of full entropy.

57 Additional detail is provided the proprietary Entropy Description.

6.3.11 FCS_SSHS_EXT.1

58 Each TOE component implements SSH in compliance with RFCs 4251, 4252, 4253, 4254, 4344, 5656, 6668, 8268, 8308 section 3.1 and 8332.

59 Each TOE component supports password-based or public key authentication (ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521). In the case of public keys, the TOE authenticates the identity of the

SSH client using a local database associating authorized hosts with its corresponding public key. The TOE does not support the keyboard-interactive authentication method.

60 Each TOE component supports the use of ecdsa-sha2-nistp256 algorithms for its host keys.

61 Each TOE component examines the size of each received SSH packet. If the packet is greater than 256 KB, it is automatically dropped.

62 Each TOE component utilises AES-CTR-128, AES-CTR-256, AES-GCM-128 and AES-GCM-256 for SSH encryption.

63 Each TOE component provides data integrity for SSH connections via HMAC-SHA1, HMAC-SHA2-256 and HMAC-SHA2-512.

64 The Sightline component supports diffie-hellman-group14-sha1, ecdh-sha2-nistp256, diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, ecdh-sha2-nistp384 and ecdh-sha2-nistp521 for SSH key exchanges.

65 The TMS component supports ecdh-sha2-nistp256, diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, ecdh-sha2-nistp384 and ecdh-sha2-nistp521 for SSH key exchanges.

66 Each TOE component will re-key SSH connections after 1 hour of after an aggregate of 1 gig of data has been exchanged (whichever occurs first).

6.3.12 FCS_TLSC_EXT.1

67 The TOE implements TLS 1.2 and rejects all other TLS and SSL versions.

68 The TOE supports the following for the secure communication specified in FTP_ITC.1: Verifies the presented identifier against the reference identifier per RFC 6215. The TOE will only support a wildcard in the left-most label (e.g. *.example.com). All other usages of a wildcard will cause a failure in the connection. The TOE does not support URI, IP addresses or service name reference identifiers or pinned certificates.

69 The TOE supports the following for the secure communication specified in FPT_ITT.1: Verifies the presented IPv4 address in CN or SAN fields against the reference identifier. The TOE does not support wildcards. The TOE does not support URI, DNS or service name reference identifiers or pinned certificates.

70 The TOE presents the supported elliptic curves extension with the secp256r1, secp384r1 and secp521r1 curves. This behaviour is configured when FIPS mode is enabled on the TOE during installation activities.

71 The Sightline Syslog TLS connection supports the following ciphersuites:

a) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

b) TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

c) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

d) TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

e) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

f) TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

g) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

h) TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

72 The Sightline ITT TLS connection supports the following ciphersuites:

a) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

b) TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

c) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

d) TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

73 The TMS Syslog TLS connection supports the following ciphersuites:

a) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

b) TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

c) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

d) TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

74 The TMS ITT TLS connection supports the following ciphersuites:

a) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

b) TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

c) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

d) TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

e) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

f) TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

g) TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

h) TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

i) TLS_DHE_RSA_WITH_AES_256_CBC_SHA

j) TLS_RSA_WITH_AES_256_GCM_SHA384

k) TLS_RSA_WITH_AES_256_CBC_SHA256

l) TLS_RSA_WITH_AES_256_CBC_SHA

m) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

n) TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

o) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

p) TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

q) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

r) TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA

s) TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

t) TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

u) TLS_DHE_RSA_WITH_AES_128_CBC_SHA

v) TLS_RSA_WITH_AES_128_GCM_SHA256

w) TLS_RSA_WITH_AES_128_CBC_SHA256

x) TLS_RSA_WITH_AES_128_CBC_SHA

6.3.13 FCS_TLSS_EXT.1

75 Each TOE component implements TLS 1.2 and rejects all other TLS and SSL versions.

76 Each TOE component supports the following TLS ciphersuites:

a) TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

b) TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

77 Each TOE component supports ECDHE curve secp256r1.

78 The Sightline TOE component supports session resumption based on session ID or session tickets.

79 The TMS TOE component supports session resumption based on session tickets.

80 Session tickets adhere to the structural format provided in section 4 of RFC 5077. Session tickets are encrypted using 128-bit AES in CBC mode, which is consistent with FCS_COP.1/DataEncryption.

81 An abbreviated handshake occurs only when both client and server successfully validate resumption. If the connection is suspected to be compromised, a full handshake will occur.

6.4 Identification and Authentication

6.4.1 FIA_PMG_EXT.1

82 The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”.

83 The minimum password length is settable by the Administrator and can range from 7 to 72 characters.

6.4.2 FIA_UIA_EXT.1

84 The TOE requires all users to be successfully identified and authenticated before any administrative action can be taken. The TOE warning banner is displayed prior to authentication at all interfaces.

85 Administrative access to the TOE is facilitated through several interfaces:

a) **CLI.** Administrative CLI via direct serial connection.

b) **SSH CLI.** Administrative CLI via SSH.

c) **Web GUI**. Administrative GUI over HTTPS/TLS.

86 The TOE uses username and password authentication at the local CLI, SSH and HTTPS WebGUI. The SSH interface additionally supports public key authentication.

6.4.3 FIA_UAU_EXT.2

87 Regardless of the interface at which the administrator interacts, the TOE prompts the user for a credential. Only after the administrative user presents the correct authentication credentials will they be granted access to the TOE administrative functionality. No TOE administrative access is permitted until an administrator is successfully identified and authenticated.

88 The TOE provides a local password-based authentication mechanism.

89 The process for authentication is the same for administrative access whether administration is occurring via direct connection or remotely. At initial login, the administrative user is prompted to provide a username. After the user provides the username, the user is prompted to provide the administrative credential associated with the user account. The TOE then either grants administrative access (if the combination of username and credential is correct) or indicates that the login was unsuccessful. The TOE does not provide a reason for failure in the cases of a login failure.

6.4.4 FIA_UAU.7

90 For all authentication at the local CLI the TOE provides no feedback when the administrative password is entered so that the password is obscured.

6.4.5 FIA_AFL.1

91 The TOE is capable of tracking authentication failures of remote administrators.

92 When a user account has sequentially failed authentication the configured number of times the account will be locked until a Security Administrator unlock is performed.

93 The local console does not implement the lockout mechanism.

6.4.6 FIA_X509_EXT.1/Rev

94 The TOE performs certificate validation with external IT entities. The TSF ensures that the certification path is a minimum of three, the certification path terminates with a CA certificate designated as a trust anchor, all CA certificates contain a basicConstraints CA flag set to TRUE. The TSF also performs revocation status checks using OCSP. Revocation checking is performed both on leaf certificates and intermediate certificates when establishing a connection to an external IT entity (syslog server). The TSF validates the extendedKeyUsage field by verifying all certificates contain the appropriate purpose for their use.

95 Intermediate CA's that contain an extendedKeyUsage field require the Server Authentication Purpose.

6.4.7 FIA_X509_EXT.1/ITT

96 The TOE performs certificate validation with external IT entities. The TSF ensures that the certification path is a minimum of two, the certification path terminates with a CA certificate designated as a trust anchor, all CA certificates contain a basicConstrans CA flag set to TRUE. The TSF does not perform revocation status checks. The TSF validates the extendedKeyUsage field by verifying all certificates contain the appropriate purpose for their use.

6.4.8 FIA_X509_EXT.2

97 The TOE uses X.509v3 certificates to support authentication for TLS for both Syslog and ITT. Each TOE component uses a singular trust anchor for authenticating both external IT entities and the peer TOE component.

98 The TOE does not accept certificates when a connection cannot be established to determine the revocation status.

6.4.9 FIA_X509_EXT.3

99 Each TOE component is capable of generating Certificate Requests containing a Common Name, Organization, Organizational Unit and Country values.

100 The TSF only accepts Certificate Responses with the Root CA present as valid.

6.5 Security Management

6.5.1 FMT_MOF.1/ManualUpdate

101 The TOE restricts the ability to perform software updates to Security Administrators.

6.5.2 FMT_MOF.1/Services

102 The TOE restricts the ability to start and stop services to Security Administrators.

6.5.3 FMT_MTD.1/CoreData

103 Users are required to login before being provided with access to any administrative functions.

6.5.4 FMT_SMR.2

104 The TOE maintains two Security Administrator Groups:

a) **admin.** Privilege level “system_admin”. Capable of configuring all TSF data and administering all security functions.

b) **admin_disk.** Privilege level “system_admin_disk”. Capable of configuring all TSF data and administering all security functions.

105 The default Security Administrator is the **admin** user account apart of the **admin** group. This account is used to access all TOE interfaces.

106 Any additional accounts must be assigned to one of the two groups to be considered Security Administrators.

107 Management of TSF data is restricted to Security Administrators.

6.5.5 FMT_MTD.1/CryptoKeys

108 The TOE restricts the ability to manage SSH keys to Security Administrators.

6.5.6 FMT_SMF.1

109 The TOE may be managed via the CLI (console & SSH) or GUI (HTTPS). The specific management capabilities include:

Table 17: TOE Component Management Capabilities

Management Capability	TOE Components	Sightline Interfaces	TMS Interfaces
Ability to administer the TOE locally and remotely	All	CLI and GUI	CLI
Ability to configure the access banner (FTA_TAB.1)	All	CLI and GUI	CLI
Ability to configure the session inactivity time before session termination or locking (FTA_SSL_EXT.1, FTA_SSL.3)	All	CLI	CLI

Management Capability	TOE Components	Sightline Interfaces	TMS Interfaces
Ability to update the TOE and to verify the updates (FMT_MTD.1/ManualUpdate, FPT_TUD_EXT.1)	All	CLI	CLI
Ability to configure the authentication failure parameters (FIA_AFL.1)	All	CLI and GUI	CLI
Ability to start and stop services	All	CLI	CLI
Ability to manage the cryptographic keys (FMT_MTD.1/CryptoKeys, FCS_CMK.1)	All	CLI	CLI
Ability to configure the interaction between TOE components (per FCO_CPC_EXT.1)	All	GUI	CLI
Ability to re-enable an Administrator account	All	CLI	CLI
Ability to set the time which is used for time-stamps	All	CLI	CLI
Ability to configure NTP	All	CLI	CLI
Ability to import X.509v3 certificates to the TOE's trust store	All	CLI	CLI
Ability to manage the trusted public keys database	All	CLI	CLI

6.6 Protection of the TSF

6.6.1 FPT_SKP_EXT.1

110 Keys are protected as described in Table 18. In all cases, plaintext keys cannot be viewed through an interface designed specifically for that purpose.

Table 18: Keys

Key	Algorithm	Storage	Zeroization
SSH Private Keys	ECDSA	Flash - plaintext	Keys are destroyed when generating new keys by deleting the previous file and creating a new file. Initiated via CLI command by the Security Administrator.
SSH Ephemeral Keys	AES / RSA/ DH / ECDH	RAM – plaintext	OpenSSL ensures that keys (including re-keyed keys) are overwritten with zeroes when no longer required.

Key	Algorithm	Storage	Zeroization
TLS Private Keys	ECDSA	Flash – plaintext	Keys are destroyed when generating new keys by deleting the previous file and creating a new file. Initiated via CLI command by the Security Administrator.
TLS Ephemeral Keys	AES / RSA / DH / ECDH	RAM – plaintext	OpenSSL ensures that keys (including re-keyed keys) are overwritten with zeroes when no longer required.
NTP Pre-shared keys	User generated	Flash – plaintext	As NTP keys are not intended to be used for encryption of sensitive information, the level of protection is different compared to other pre-shared keys See TD0639

6.6.2 FPT_APW_EXT.1

111 Passwords are protected as describe in Table 19. In all cases plaintext passwords cannot be viewed through an interface designed specifically for that purpose.

Table 19: Passwords

Key/Password	Generation/ Algorithm	Storage
Locally stored administrator passwords	User generated	Flash - SHA-512 hash

6.6.3 FPT_TST_EXT.1

112 At startup, each TOE component undergoes the following tests:

a) Central Processing Unit (CPU) and Memory Unified Extensible Firmware Interface (UEFI) self-tests – CPU and memory are initialized by exercising a set of known answer tests and the UEFI is compared against a known checksum of the image.

b) Boot loader image verification – the boot loader compares the image of the TOE component to a known checksum of the image prior to booting.

c) OpenSSL cryptographic module self-tests

113 The TOE components rely on the standard OpenSSL functionality for FIPS Module and Integrity Tests. Each TOE component performs the following:

a) Integrity tests of the OpenSSL cryptographic module: An HMAC hash check over sections of in core data and checks the value against an expected value set when the application is compiled.

b) Cryptographic known answer tests: Each TOE component performs a variety of cryptographic checks to ensure the correctness of supported algorithms.

6.6.4 FPT_TUD_EXT.1

114 The current firmware version may be queried using any administrative interface.

115 The Security Administrator manually initiates TOE updates from the CLI. TOE update files must first be copied to the TOE via SCP.

116 TOE update files are digitally signed (RSA) and the signature is verified using a hardcoded public key prior to installation of the update. If verification fails, the update is aborted, and an error message is displayed.

6.6.5 FPT_STM_EXT.1

117 The TOE makes use of an internal clock or NTP to maintain date and time.

118 The TOE makes use of time for the following:

a) Audit record timestamps

b) Session timeouts (lockout enforcement)

c) X.509 certificate expiration

6.6.6 FPT_ITT.1

119 The TOE protects communication between the TOE components using HTTPS/TLS protocol and cipher suites. Both Sightline and TMS perform TLS Server and TLS Client connections.

6.7 TOE Access

6.7.1 FTA_SSL_EXT.1

120 The Security Administrator may configure the TOE to terminate an inactive local interactive session following a specified period of time. This is applicable to the local CLI.

6.7.2 FTA_SSL.3

121 The Security Administrator may configure the TOE to terminate an inactive remote interactive session following a specified period of time. This is applicable to the local CLI, remote CLI and Web GUI.

6.7.3 FTA_SSL.4

122 Administrative users may terminate their own sessions at any time. Session termination at the CLI / SSH CLI is initiated via the exit command. Interactive session termination at the Web GUI is initiated via the Log Out button in the top navigation bar.

6.7.4 FTA_TAB.1

123 The TOE displays an administrator configurable message to users prior to login at the local CLI, remote CLI and Web GUI.

6.8 Trusted Path/Channels

6.8.1 FTP_ITC.1

124 The TOE supports secure communication with an audit server per FCS_TLSC_EXT.1

6.8.2 FTP_TRP.1/Admin

125 The TOE provides the following trusted paths for remote administration:

a) **Remote CLI.** Administrative CLI via SSH per FCS_SSHS_EXT.1.

b) **Web GUI.** HTTPS Web interface via TLS per FCS_HTTPS_EXT.1 and FCS_TLSS_EXT.1.

7 Rationale

7.1 Conformance Claim Rationale

126 The following rationale is presented with regard to the PP conformance claims:

a) **TOE type.** As identified in section 2.1, the TOE is network device, consistent with the NDcPP.

b) **Security problem definition.** As shown in section 3, the threats, OSPs and assumptions are reproduced directly from the NDcPP.

c) **Security objectives.** As shown in section 4, the security objectives are reproduced directly from the NDcPP.

d) **Security requirements.** As shown in section 5, the security requirements are reproduced directly from the NDcPP. No additional requirements have been specified.

7.2 Security Objectives Rationale

127 All security objectives are drawn directly from the NDcPP.

7.3 Security Requirements Rationale

128 All security requirements are drawn directly from the NDcPP. Table 20 presents a mapping between threats and SFRs as presented in the NDcPP.

Table 20: NDcPP SFR Rationale

Identifier	SFR Rationale
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	• The Administrator role is defined in FMT_SMR.2 and the relevant administration capabilities are defined in FMT_SMF.1 and FMT_MTD.1/CoreData, with optional additional capabilities in FMT_MOF.1/Services and FMT_MOF.1/Functions • The actions allowed before authentication of an Administrator are constrained by FIA_UIA_EXT.1, and include the advisory notice and consent warning message displayed according to FTA_TAB.1 • The requirement for the Administrator authentication process is described in FIA_UAU_EXT.2 • Locking of Administrator sessions is ensured by FTA_SSL_EXT.1 (for local sessions), FTA_SSL.3 (for remote sessions), and FTA_SSL.4 (for all interactive sessions) • The secure channel used for remote Administrator connections is specified in FTP_TRP.1/Admin • (Malicious actions carried out from an Administrator session are separately addressed by T.UNDETECTED_ACTIVITY)

Identifier	SFR Rationale
	• (Protection of the Administrator credentials is separately addressed by T.PASSWORD_CRACKING).
T.WEAK_CRYPTOGRAPHY	• Requirements for key generation and key distribution are set in FCS_CKM.1 and FCS_CKM.2 respectively • Requirements for use of cryptographic schemes are set in FCS_COP.1/DataEncryption, FCS_COP.1/SigGen, FCS_COP.1/Hash, and FCS_COP.1/KeyedHash • Requirements for random bit generation to support key generation and secure protocols (see SFRs resulting from T.UNTRUSTED_COMMUNICATION_CHANNELS) are set in FCS_RBG_EXT.1 • Management of cryptographic functions is specified in FMT_SMF.1
T.UNTRUSTED_COMMUNICATION_CHANNELS	• The general use of secure protocols for identified communication channels is described at the top level in FTP_ITC.1 and FTP_TRP.1/Admin; for distributed TOEs the requirements for inter-component communications are addressed by the requirements in FPT_ITT.1 • Requirements for the use of secure communication protocols are set for all the allowed protocols in FCS_DTLSC_EXT.1, FCS_DTLSC_EXT.2, FCS_DTLSS_EXT.1, FCS_DTLSS_EXT.2, FCS_HTTPS_EXT.1, FCS_IPSEC_EXT.1, FCS_SSHC_EXT.1, FCS_SSHS_EXT.1, FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSS_EXT.1, FCS_TLSS_EXT.2 • Optional and selection-based requirements for use of public key certificates to support secure protocols are defined in FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3
T.WEAK_AUTHENTICATION_ENDPOINTS	• The use of appropriate secure protocols to provide authentication of endpoints (as in the SFRs addressing T.UNTRUSTED_COMMUNICATION_CHANNELS) are ensured by the requirements in FTP_ITC.1 and FTP_TRP.1/Admin; for distributed TOEs the authentication requirements for endpoints in inter-component communications are addressed by the requirements in FPT_ITT.1 • Additional possible special cases of secure authentication during registration of distributed TOE components are addressed by FCO_CPC_EXT.1 and FTP_TRP.1/Join.

Identifier	SFR Rationale
T.UPDATE_COMPROMISE	• Requirements for protection of updates are set in FPT_TUD_EXT.1 • Additional optional use of certificate-based protection of signatures can be specified using FPT_TUD_EXT.2, supported by the X.509 certificate processing requirements in FIA_X509_EXT.1, FIA_X509_EXT.2 and FIA_X509_EXT.3 • Requirements for management of updates are defined in FMT_SMF.1 and (for manual updates) in FMT_MOF.1/ManualUpdate, with optional requirements for automatic updates in FMT_MOF.1/AutoUpdate
T.UNDETECTED_ACTIVITY	• Requirements for basic auditing capabilities are specified in FAU_GEN.1 and FAU_GEN.2, with timestamps provided according to FPT_STM_EXT.1 and if applicable, protection of NTP channels in FCS_NTP_EXT.1 • Requirements for protecting audit records stored on the TOE are specified in FAU_STG.1 • Requirements for secure transmission of local audit records to an external IT entity via a secure channel are specified in FAU_STG_EXT.1 • Optional additional requirements for dealing with potential loss of locally stored audit records are specified in FAU_STG_EXT.2/LocSpace, and FAU_STG_EXT.3/LocSpace • If (optionally) configuration of the audit functionality is provided by the TOE then this is specified in FMT_SMF.1, and confining this functionality to Security Administrators is required by FMT_MOF.1/Functions.
T.SECURITY_FUNCTIONALITY_COMPROMISE	• Protection of secret/private keys against compromise is specified in FPT_SKP_EXT.1 • Secure destruction of keys is specified in FCS_CKM.4 • If (optionally) management of keys is provided by the TOE then this is specified in FMT_SMF.1, and confining this functionality to Security Administrators is required by FMT_MTD.1/CryptoKeys • (Protection of passwords is separately covered under T.PASSWORD_CRACKING)

Identifier	SFR Rationale
T.PASSWORD_CRACKING	• Requirements for password lengths and available characters are set in FIA_PMG_EXT.1 • Protection of password entry by providing only obscured feedback is specified in FIA_UAU.7 • Actions on reaching a threshold number of consecutive password failures are specified in FIA_AFL.1 • Requirements for secure storage of passwords are set in FPT_APW_EXT.1.
T.SECURITY_FUNCTIONALITY_FAILURE	• Requirements for running self-test(s) are defined in FPT_TST_EXT.1
P.ACCESS_BANNER	• An advisory notice and consent warning message is required to be displayed by FTA_TAB.1