ArcSight Logger 7.3.0.8511.8 Security Target

Date: *February 10, 2026*
Version: *0.11*
Prepared By: *Dawn Adams*
Prepared For: *OpenText*
275 Frank Tompa Drive
Waterloo ON N2L 0A1
Canada

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), ArcSight Logger 7.3.0.8511.8. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

1. Introduction:

This section identifies the Security Target (ST), Target of Evaluation (TOE), Security Target organization, document conventions, and terminology. It also includes an overview of the evaluated product.

This section introduces the Target of Evaluation (TOE) and provides the Security Target (ST) and TOE identification, the TOE overview and TOE Description.

The ST contains the following additional sections:

- Conformance Claims (Section 2)— claims of conformance to CC2022.
- Security Problem Definition (Section 3)—describes the threats and assumptions that define the security problem to be addressed by the TOE and its environment
- Security Objectives (Section 4)—describes the security objectives for the TOE and its operational
- environment necessary to counter the threats and satisfy the assumptions that define the security problem
- Extended Requirements – (Section 5) – specifies whether any SFRs or SARs are extended
- IT Security Requirements (Section 6)—specifies the security functional requirements (SFRs) and security assurance requirements (SARs) to be met by the TOE
- TOE Summary Specification (Section 7)—describes the security functions of the TOE and how they satisfy the SFRs

1.1. Security Target Reference:

ST Title	ArcSight Logger 7.3.0.8511.8 Security Target
ST Revision	0.11
ST Publication Date	February 10, 2026
Author	Dawn Adams

1.2. TOE Reference:

TOE Reference	ArcSight Logger 7.3.0.8511.8

1.3. Document Organization:

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats

SECTION	TITLE	DESCRIPTION
5	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 1 – ST Organization and Section Descriptions

1.4. Document Terminology:

The following table describes the acronyms used in this document:

TERM	DEFINITION
AD	Active Directory
CC	Common Criteria version CC2022
DB	Database
EAL	Evaluation Assurance Level
EOE	Events Originating External to the TOE
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
HTTPS	Secure Hyper Text Transfer Protocol
ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
OSP	Organizational Security Policy
SAR	Security Assurance Requirements
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
VPN	Virtual Private Network

Table 2 – Acronyms Used in Security Target

1.5. Document Conventions

Security Functional Requirements CC2022 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 is identified with a number in parentheses following the base component identifier. For example, iterations of FCS_COP.1 are identified in a manner similar to FCS_COP.1(1) (for the component) and FCS_COP.1.1(1) (for the elements).

Assignment—allows the specification of an identified parameter. Assignments are indicated using text enclosed by brackets (e.g., [assignment]).

Selection—allows the specification of one or more elements from a list. Selections are indicated using italics and are enclosed by brackets (e.g., [*selection*]).

Refinement—allows the addition or removal of details. Refinements are indicated using bold, for additions, and strike-through, for deletions.

1.6. TOE Overview:

The TOE is the ArcSight Logger 7.3.0.8511.8 from OpenText. The TOE is a software only TOE. Logger is a data collection and storage engine that unifies log data collection, storage, and security data management in a scalable, high-performance software or appliance solution. It provides capabilities to collect machine data from any source (such as logs, clickstreams, sensors, stream network traffic, security devices, web servers, custom applications, social media, and cloud services) and to monitor and search that data for security intelligence.

ArcSight Logger is a log management solution designed to handle high event throughput, support data analysis, and provide efficient long-term storage. Logger receives and stores events, supports search, retrieval, and reporting, and can optionally forward selected events (e.g., to ArcSight ESM).

Logger receives structured data in the form of normalized Common Event Format (CEF) events and unstructured data, such as syslog events. The file-type receivers configured on Logger only parse event time from an event. Although Logger is message-agnostic, it can do more with CEF. Logger provides a browser-based GUI that enables Logger users to access the following functional capabilities:

- Manage IDS data (event) storage
- Manage receivers for collecting IDS data (events) from SmartConnectors, syslog over UDP or TCP, and text files
- Search and review collected IDS data
- Manage alerts
- Manage reports
- Manage IDS data (event) archiving
- Manage Logger users

Logger also provides a Web Services Application Programming Interface (API) that exposes Logger functions as Web services. This enables Logger functionality to be integrated into other ArcSight products and third-party applications.

Capabilities provided by the Web Services API include executing searches on stored Logger events, running Logger reports, and feeding Logger reports back to the third-party application. The Web Services API supports both SOAP-based and REST-based Web services.

Logger is available in two form factors—an appliance and software. The appliance-based solution is a hardened, dedicated, enterprise-class system that is optimized for extremely high

event throughput, efficient long-term storage, and rapid data analysis. The software-based solution is similar in feature and functionality to the appliance-based solution, enabling the end customer to install ArcSight Logger on a supported platform of the customer's choice.

Multiple Loggers can work together to scale up to support extremely high event volume with search queries distributed across all Loggers.

The links between the console and Logger are protected by TLS cryptography supplied by the environment

Connectors and the Console are considered to be Trusted IT products.

1.6.1. ArcSight SmartConnectors

ArcSight SmartConnectors collect and process events generated by devices throughout an enterprise. The devices are considered part of the environment in which the TOE operates. Devices can be routers, e-mail logs, anti-virus products, firewalls, Intrusion Detection Systems, access control servers, VPN systems, anti-DoS appliances, operating system logs, and other sources where information of security threats are detected and reported.

SmartConnectors are specifically developed to work with network and security products using multiple techniques, including simple log forwarding and parsing, direct installation on native devices, SNMP, and syslog.

The following specific SmartConnectors were tested as part of the evaluated configuration:
• Syslog NG Daemon—can collect syslog records from Syslog NG Daemon, an open source implementation of the syslog protocol for UNIX and UNIX-like systems that extends the original syslogd model and adds such features as support for the IETF Standard (RFC 5424) syslog header and TLS for secure communication

• Microsoft Windows Event Log – Native (WINC)—collects Windows Event Log events.

Other SmartConnectors may be deployed in an evaluated configuration, but no conclusions should be drawn regarding the efficacy of their event collection functionality.

The TOE uses the NTP protocol to communicate with the NTP Server.

The TOE uses HTTPS/TLS to communicate with Users (Administrators, TOE Users, End point users. The TOE also uses HTTPS/TLS to communicate with TOE Elements. The TOE supports TLS v1.2. The operational environment must also support TLS v1.2 in order to interoperate with the TOE.

1.7. TOE Description:

1.7.1. Overview:

The TOE consists of the following components:
ArcSight Logger 7.3.0.8511.8

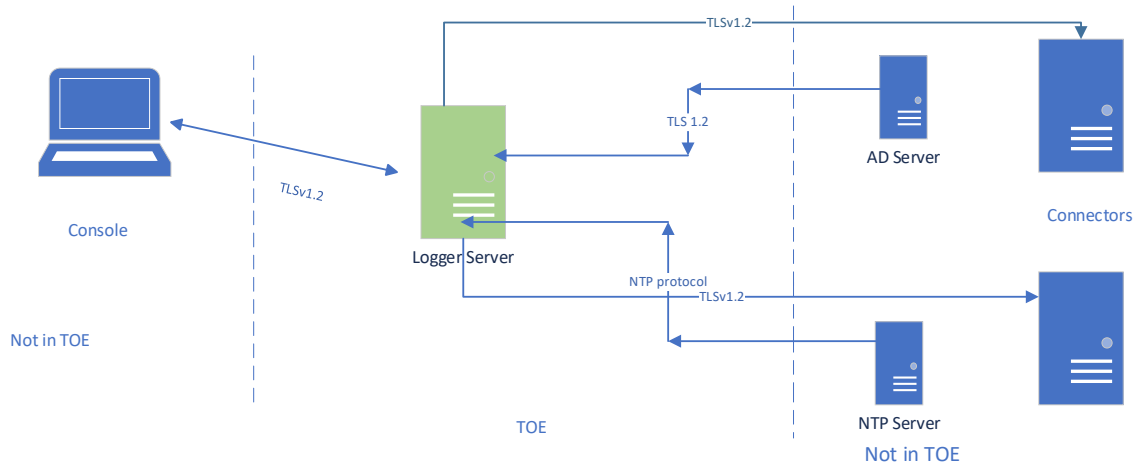


Figure 1 - Logger Evaluated Configuration

1.7.2. TOE Component:

The TOE component is:

Component	Environment (OS)
ArcSight Logger 7.3.0.8511.8	RHEL 8.8

Table 3 – TOE

The configuration requirements for the operational environment to support the TOE are listed in the table below.

1.7.3. Software Supplied by the IT Environment:

The TOE requires the following software components in order to be evaluated:

Supplied by the Environment	Environment Requirements
SmartConnector for Windows 25.1.1	Windows Server 2022
SmartConnector for Linux 25.1.1	RHEL 9.2
Browser	Firefox, Edge, Chrome

Supplied by the Environment	Environment Requirements
NTP Server	Chrony (RHEL 9 default) – Version chrony-4.6.1-1.el9.x86_64
AD Server	Windows Server 2019 Standard running LDAP version 3

Table 4 – Environment Software

1.7.4. TOE Usage:

Logger is a log management solution that is optimized for extremely high event throughput, efficient long-term storage, and rapid data analysis. Logger receives and stores events; supports search, retrieval, and reporting; and can optionally forward selected events. Logger compresses raw data, but can always retrieve unmodified data on demand for forensics-quality litigation data.

Logger is available in **Appliance** and **Software** form factors, however the TOE is a software only TOE. The appliance-based solution is a hardened, dedicated, enterprise-class system. The software-based solution is similar in feature and functionality to the appliance-based solution, however, the software solution enables you to install ArcSight Logger on a supported platform of the owner's choice. The software version is available as a VMware virtual machine.

1.7.5. Physical Boundary:

COMPONENT	VERSION NUMBER
ArcSight Logger	7.3.0.8511.8

Table 5 – Physical Boundary

1.7.6. Logical Boundary:

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following table:

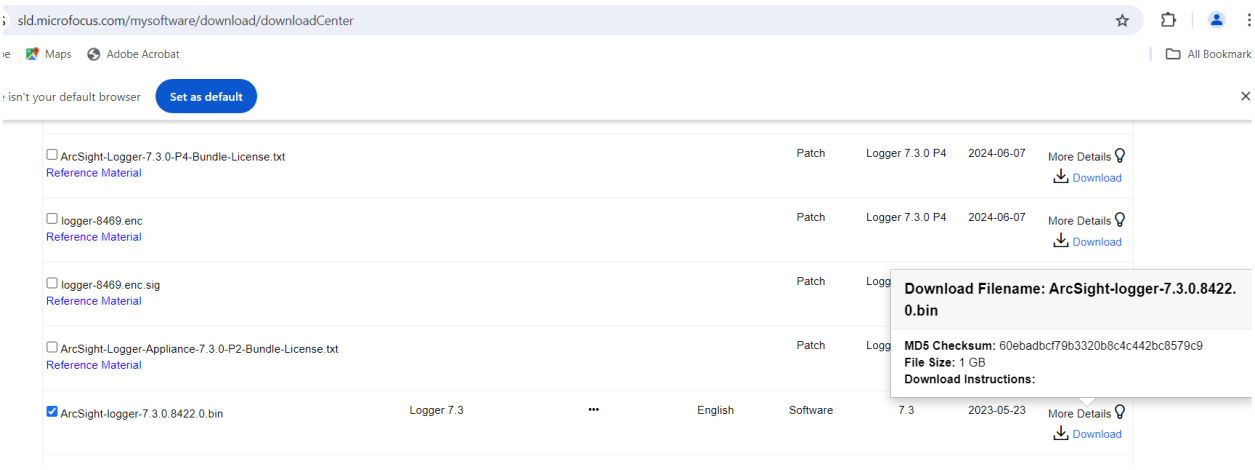
TSF	DESCRIPTION
Security Audit	Logger is able to generate and store audit records of security-relevant events. The stored audit records are protected from unauthorized modification and deletion. Audit records generated by Logger can be viewed only by users in the Logger System Admin or Logger Read Only System Admin roles. Logger provides the authorized roles with capabilities to review the generated audit records, including capabilities for selecting audit records based on date and time range and, optionally, subject identity and outcome, and ordering the selected records based on date and time, the subject associated with the audit event, and the type of audit event.
Cryptographic Support	Cryptography for TLS connections is supplied by the operational environment. Communications between the TOE and trusted IT entities are protected by TLS v1.2 provided by the environment (Bouncy Castle). Communications between the console and Logger are protected by TLS supplied by the environment (Voltage Cryptographic Module)

TSF	DESCRIPTION
Identification and Authentication	The TOE maintains accounts of the authorized users of the system. The user account includes the following attributes associated with the user: user identity; authentication data; authorizations (groups or roles); and e-mail address information. The TOE supports both passwords and certificates for authentication and users can be configured for password-only, certificate-only, or password and certificate-based authentication. The TOE requires users to provide unique identification and authentication data before any administrative access to the TOE via the Logger GUI is granted.
Security Management	Logger provides authorized Logger users with a GUI that can be used to configure and manage Logger security functions and TSF data, depending on the security management roles assigned to the user. Logger supports the following security management roles: Logger System Admin; Logger Read Only System Admin; Logger Rights; Logger Search; and Logger Reports.
Protection of the TSF	The NTP Server supplies the TOE with a reliable timestamp.
TOE Access	The TOE enforces a limit on the number of simultaneous active sessions for each user account. The maximum number is configurable by an administrator and has a default value of 15. The TOE will terminate interactive sessions after a period of inactivity configurable by an administrator. The TOE also allows user-initiated termination of the user's own interactive session by explicitly logging off. The TOE displays a banner message on the user login page. The content of the message can be configured by an administrator.
Trusted Path / Channels	The TOE provides a trusted channel to communicate securely with external destinations. The trusted channel is implemented using HTTPS (i.e., HTTP over TLS). The TOE provides a trusted path for TOE administrators to communicate with the TOE. The trusted path is implemented using HTTPS for access to the Logger GUI. Administrators initiate the trusted path by establishing an HTTPS connection (using a supported web browser). The trusted path is used for initial authentication and all subsequent administrative actions. The use of HTTPS ensures all communication over the trusted path is protected from disclosure and modification.

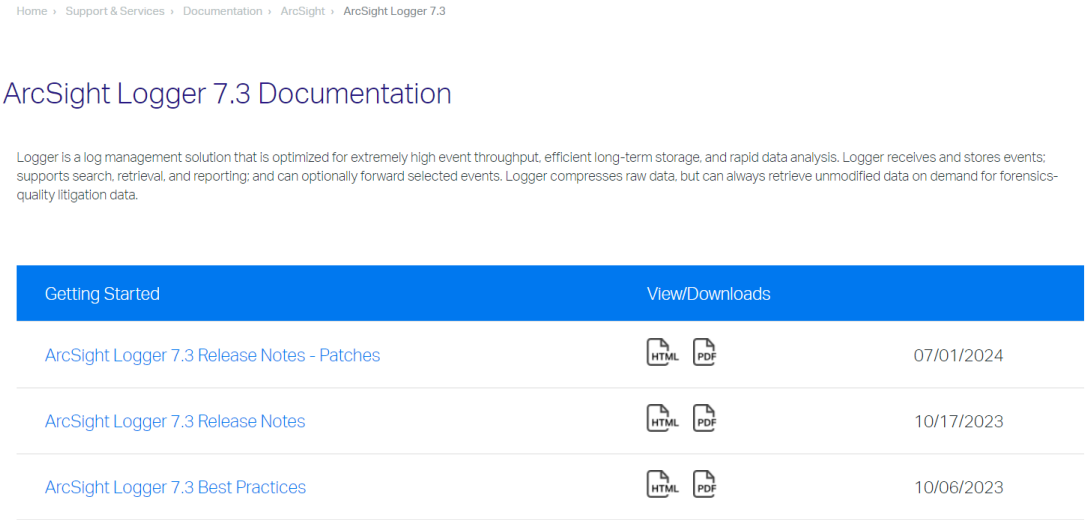
Table 6 – Logical Boundary Descriptions

1.7.7. TOE Delivery:

The TOE software is provided to customers via secure download from the download portal (https://sld.microfocus.com/mysoftware/index). The TOE software is available on this website. Once downloaded, the files can be expanded to perform the installation.



Documentation can be found at [ArcSight Logger 7.3 - Documentation | Micro Focus]



The documentation is available on the web in either html or pdf formats.

1.7.8. TOE Guidance:

The TOE includes the following guidance documentation:

Micro Focus Security ArcSight Logger, Software Version: 7.3, Installation and Configuration Guide

Micro Focus Security ArcSight Logger, Software Version: 7.3, Administrator's Guide

Additional TOE operational guidance and installation procedures will be provided in the TOE Operational Guidance and Installation Procedures (AGD-IGS.1).

Although OpenText is moving to a new nomenclature for its products, Logger will remain as version 7.3.0.8511.8 and will not be moved to the new nomenclature.

1.7.9. Supported Functionality Excluded from the Evaluated Configuration:

- Hadoop functionality

2. Conformance Claims:

2.1. CC Conformance Claim:

The TOE is conformant to Common Criteria Version CC:2022 Revision 1 November 2022.

The CC standard documents are:
Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Part 1: Introduction and general model
Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Part 2: Security functional components
Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Part 3: Security assurance components
Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Part 4: Framework for the specification of evaluation methods and activities Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Part 5: Pre-defined packages of security requirements

The TOE is conformant to: CC Part2 (conformant) and CC Part3 (conformant).

2.2. PP Claim:

The TOE does not claim conformance to any registered Protection Profile.

2.3. Package Claim

The TOE claims conformance to the EAL2 assurance package defined in Part 3 of the Common Criteria Version CC:2022 Revision 1 (November 2022). The TOE does not claim conformance to any functional package. The TOE EAL2 assurance package is augmented with ALC_FLR.3.

2.4. Conformance Rationale

No Protection Profile conformance rationale is necessary for this evaluation since this Security Target does not claim conformance to a Protection Profile.

EAL2+ was chosen because it is based upon good commercial development practices with thorough functional testing. EAL2+ provides the developers and users a moderate level of independently assured security in conventional commercial TOEs. The threat of malicious attacks is not greater than low, the security environment provides physical protection, and the TOE itself offers a very limited interface, offering essentially no opportunity for an attacker to subvert the security policies without physical access.

The product was augmented to comply with ALC_FLR.3 in order to document and address requirements for remediation and reporting of faults that may be discovered in the product after release. The TOE invokes the Environment cryptography to establish TLS1.2 channels for secure communications.

3. Security Problem Definition

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required
- Any organizational security policy statements or rules with which the TOE must comply
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.1. Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all threats is unsophisticated.

The TOE addresses the following threats:

THREAT	DESCRIPTION
T.NO_AUTH	An unauthorized user may gain access to the TOE and alter the TOE configuration.
T.NO_PRIV	An authorized user of the TOE exceeds their assigned security privileges resulting in unauthorized modification of the TOE configuration and/or data.
T.UNATTENDED_SESSION	An unauthorized user gains access to the TOE via an unattended authorized user session.
T.SENSDATA	An unauthorized user may be able to view sensitive data passed between the TOE and its remote users, and between the TOE and external web servers, and exploit this data to gain unauthorized privileges on the TOE.

Table 7 – Threats Addressed by the TOE

3.2. Organizational Security Policies (OSPs)

There are no OSPs for this TOE.

3.3. Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The following specific conditions are assumed to exist in an environment where the TOE is employed.

ASSUMPTION	DESCRIPTION
A.PROTECT	The TOE software critical to security policy enforcement will be protected from unauthorized physical modification. TSF data shall be protected from disclosure.
A.HTTPS	Web browsers used to access the TOE shall support HTTPS using TLS. Communications between the TOE and trusted IT products are

ASSUMPTION	DESCRIPTION
A.PLATFORM	The underlying operating system of each TOE software component will protect the component and its configuration from unauthorized access.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	Administrators of the TOE are well-trained and non-hostile.
A.TIMESOURCE	The TOE has a trusted source for system time via NTP server

Table 8 – Assumptions

4. Security Objectives

4.1. Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.AUDIT	The TOE shall collect data from all TOE activities including changes to permissions, privileges, roles, rules, and provisioning of access. The TOE provides a method of reviewing audit logs,
O.DATA	The TOE shall collect audit data from Administrators, and Users, and user activity employing the TOE with accurate timestamps. The collected data is critical to the analysis and tracking of user events in the environment which might indicate security issues.
O.PRIVILEGE	The TOE must protect stored credentials from disclosure.
O.SEC_ACCESS	The TOE shall ensure that only Administrators and authorized applications are granted access to security functions, configuration, and associated data. This prevents unauthorized users from performing actions that may disable the TOE and result in undetected security events and issues.

Table 9 – TOE Security Objectives

4.2. Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.ENV_PROTECT	The TOE operating environment shall provide mechanisms to isolate the TOE Security Functions (TSF) and assure that TSF components cannot be tampered with or bypassed.
OE.COM_PROTECT	The TOE must make use of operating environment cryptographic functions for the protection of sensitive data in transit. The TOE must ensure the confidentiality of data passed between itself and trusted IT products.
OE.HTTPS	Web browsers and web servers used to access the TOE shall support HTTPS using TLS.
OE.PERSONNEL	Authorized Logger administrators are non-hostile and follow all Logger administrator guidance and must ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives. Any Logger administrator, user or operator of the TOE must be trusted to not disclose their authentication credentials. Authorized Logger administrators are also required to manage and administer the TOE in a secure manner. Authorized Logger administrators must be competent and security aware personnel in accordance with the administrator documentation.
OE.PHYSEC	The facility surrounding the processing platform in which the TOE resides must provide a controlled means of access into the facility.
OE.TIME	The TOE operating environment shall provide an accurate timestamp (via reliable NTP server).

Table 10 – Operational Environment Security Objectives

4.3. Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies.

OBJECTIVES / ASSUMPTIONS / THREATS / POLICIES	O.AUDIT	O.PRIVILEGE	O.DATA	O.SEC_ACCESS	OE.COM_PROTECT	OE.ENV_PROTECT	OE.HTTPS	OE.PERSONNEL	OE.PHYSEC	OE.TIME
A.PROTECT						✓			✓	
A.HTTPS							✓			
A.PLATFORM									✓	
A.MANAGE								✓		
A.NOEVIL								✓		
A.TIMESOURCE										✓
T.NO_AUTH	✓		✓	✓		✓		✓	✓	
T.NO_PRIV	✓	✓		✓						
T.SENSDATA				✓	✓					
T_UNATTENDED_SESSION				✓						

Table 11 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

4.3.1. Mapping of Objectives:

ASSUMPTION / THREAT / POLICY	RATIONALE
A.PROTECT	This assumption is addressed by • OE.ENV_PROTECT which ensures the facility surrounding the TOE data must provide physical and logical controlled access. • OE.PHYSEC, which ensures that the facility surrounding the processing platform in which the TOE resides provides a controlled means of access into the facility.
A.HTTPS	This assumption is addressed by • OE.HTTPS which ensures that Web browsers and web servers used to access the TOE shall support HTTPS using TLS.
A.MANAGE	This assumption is addressed by OE.PERSONNEL, which ensures that the TOE is managed and administered in a secure manner by a competent and security aware personnel in accordance with the administrator documentation. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner
A.NOEVIL	This assumption is addressed by OE.PERSONNEL, which ensures that the Authorized administrators are non-hostile and follow all administrator guidance.
A.PLATFORM	This assumption is addressed by OE.PHYSEC which ensures the TOE is physically protected.
A.TIMESOURCE	This assumption is addressed by OE.TIME, which ensures the provision of an accurate time source.

ASSUMPTION / THREAT / POLICY	RATIONALE
T.NO_AUTH	This threat is countered by the following: • O.AUDIT, which ensures that all TOE transactions and attempted transactions are auditable and • O.SEC_ACCESS, which ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications and • OE.ENV_PROTECT, which ensures that TSF components cannot be tampered with or bypassed and • OE.PERSONNEL, which ensures that the TOE is managed and administered in a secure manner by competent and security aware personnel in accordance with the administrator documentation. As well as that any administrator, user, or operator of the TOE must be trusted to not disclose their authentication credentials. • OE.PHYSEC, which ensures that the facility surrounding the processing platform in which the TOE resides provides a controlled means of access into the facility
T.NO_PRIV	This threat is countered by • O.AUDIT which ensures that all TOE transactions and attempted transactions are auditable • O.PRIVILEGE, which ensures that the TOE protects stored credentials from disclosure • O.SEC_ACCESS, which ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications.
T.SENSDATA	This threat is countered by: • OE.COM_PROTECT – which ensures the use of cryptographic functions provided by the operating environment to protect sensitive data in transit and • O.SEC_ACCESS which ensures that theTOE allows access to the security functions, configuration, and associated data only by authorized users and applications.
T.UNATTENDED_SESSION	This threat is countered by: • O.SEC_ACCESS which ensures that if a session is idle for an administrator-specified duration of time, the TOE terminates the session. This ensures only authorized users have access to the TOE.

Table 12 – Mapping of Threats, Policies, and Assumptions to Objectives

5. Extended Components Definition

There are no extended components for this TOE.

6. Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST.

6.1. Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, which are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
FAU: Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit Review
	FAU_SAR.2	Restricted Audit review
	FAU_SAR.3	Selectable Audit Review
	FAU_STG.1	Audit Data Storage Location
FCS: Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.6	Timing and Event of Cryptographic Key Destruction
	FCS_RBG.1	Random Bit Generator
	FCS_RBG.2	Random Bit Generation (External Seeding)
	FPT_FLS.1	Failure With Preservation of Secure State
	FPT_TST.1	TSF-Self-Testing
	FCS_COP.1	Cryptographic Operation
FIA: Identification and Authentication	FIA_AFL.1	Authentication Failure Handling
	FIA_ATD.1	User Attribute Definition
	FIA_SOS.1	Verification of Secrets
	FIA_UAU.2	User Authentication before Any Action
	FIA_UAU.5	Multiple Authentication Mechanism
	FIA_UID.2	User Identification before Any Action
FMT: Security Management	FMT_MOF.1	Management of security function behaviour
	FMT_MTD.1(1) FMT_MTD.1(2) FMT_MTD.1(3) FMT_MTD.1(4) FMT_MTD.1(5) FMT_MTD.1(6)	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
Protection of the TSF	FPT_STM.1	Reliable Timestamps are provided
TOE Access	FTA_SSL.3	TSF-initiated termination
	FTA_SSL.4	User-initiated termination
Trusted Path/Channel	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted Path

Table 13 – TOE Security Functional Requirements

6.2. Security Audit (FAU)

6.2.1. 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 system;

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

c) [The following Auditable events:
All use of the user identification mechanism
All use of the user authentication mechanism
Reaching the threshold for unsuccessful authentication attempts and actions taken by the TOE, including restoration to normal state (e.g. account unlocking)
Modifications to the TOE behaviour
Modifications to the values of TOE data
Termination of an inactive session by the TSF
Termination of an inactive session by a user
].

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 PP/ST, [no other audit relevant information].

6.2.2. FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide [Logger System Admin, Logger Read Only System Admin] with the capability to read [all Logger-generated audit information] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.2.3. FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.2.4. FAU_SAR.3 Selectable Audit Review

FAU_SAR.3 The TSF shall provide the ability to apply [selection and ordering] of audit data based on [the following criteria:
• Selection based on date and time range and, optionally, subject identity and outcome
• Ordering based on date and time, subject identity, or type of event].

6.2.5. FAU_STG.1 Audit Data Storage Location

FAU_STG.1.1 The TSF shall be able to store generated audit data on the [*TOE itself].*

6.3. Cryptographic Support (FCS)

6.3.1. FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [see table] and specified cryptographic key sizes [see table] that meet the following: [assignment: list of standards].

[

Key Generation Algorithm	Key Size	Standard	CAVP Certificate
RSA	2048	FIPS 186-4	1985, C2204
ECDSA	Curves: P-224, P-256, P-384, P-521	FIPS 186-4	846, C2204
AES GCM mode	128, 256 bits	FIPS 197	3895, C2204
SHA	256, 384	FIPS 180-4	3211, C2204

].

Application Note: Logger relies on cryptography supplied by the environment.

Application Note: This SFR corresponds to the correct invocation by the TOE, but not the implementation of cryptographic functionality.

6.3.2. FCS_CKM.3 Cryptographic Key Access

FCS_CKM.3.1 The TSF shall perform [assignment: *type of cryptographic key access*] in accordance with a specified cryptographic key access method [assignment: *cryptographic key access method*] that meets the following: [assignment: *list of standards*].

Application Note: The TOE does not have key access. This is not applicable.

6.3.3. FCS_CKM.6 Timing and Event of Cryptographic Key Destruction

FCS_CKM.6.1 The TSF shall destroy [RSA, ECDSA, AES, SHS] when [no longer needed].

FCS_CKM.6.2 The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method [overwrite that meets the following: [no standard].

6.3.4. FCS_RBG.1 Random bit generation (RBG)

FCS_RBG.1.1 The TSF shall perform deterministic random bit generation services using [Counter DRBG, Hash DRBG] in accordance with [NIST SP800-90Ar1] after initialization with a seed.

FCS_RBG.1.2 The TSF shall use a [selection: *TSF noise source* [dev urandom] for initialized seeding.

FCS_RBG.1.3 The TSF shall update the RBG state by [selection: *reseeding, uninstantiating and re-instantiating*] using a [selection: *TSF noise source* [assignment: *name of noise source*], TSF interface for seeding] in the following situations: [selection:

— on demand;

— on the condition: [module startup];

in accordance with [FIPS 140-2].

6.3.5. FCS_RBG.2 Random bit generation (external seeding)

FCS_RBG.2 The TSF shall be able to accept a minimum input of [128 bits] from a TSF interface for the purpose of seeding.

6.3.6. FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [self-test failure].

6.3.7. FPT_TST.1 TSF Self-Test

FPT_TST.1.1 The TSF shall run a suite of the following self-tests [*during initial start-up, at the request of the authorized user*] to demonstrate the correct operation of [*the TSF*]: [AES 256 Known Answer Test, RSA 2048 Pairwise Consistency Test, ECDSA Pairwise Consistency Test, SHA256 and SHA384ntested with HMAC Known Answer Test, DRBG tests].

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of [*TSF data*].

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of *[TSF*].

6.3.8. FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform [establishment of TLS v1.2 channels] in accordance with a specified cryptographic algorithm [See Table] and cryptographic key sizes [See Table] that meet the following: [See Table].

[

Algorithm	Mode (if applicable)	Key Size	Standard	CAVP Certificate #
AES	GCM	128, 256 bits	SP 800-38D	3895, C2204
RSA		2048	FIPS 186-4	1985, C2204
ECDSA		Curves: P-224, P-256, P-384, P-521	FIPS 186-4	846, C2204

Algorithm	Mode (if applicable)	Key Size	Standard	CAVP Certificate #
SHS		384, 256 bits	FIPS 180-4	3211, C2204

].

Application Note: The TOE's use of environment cryptography is being evaluated, not the cryptographic implementation.

6.4. Authentication Failure Handling (FIA)

FIA_AFL.1.1 The TSF shall detect when [3] unsuccessful authentication attempts occur related to [user login].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [disable the user account for an administrator configurable period of time].

6.4.1. FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [User Identity, Authentication Data, User Group membership and Email address].

6.4.2. FIA_SOS.1 Verification of Secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [the following constraints for all user accounts:
Minimum length of passwords
Minimum number of numeric characters
Minimum number of uppercase characters
Minimum number of lowercase characters
Minimum number of special characters].

6.4.3. FIA_UAU.2 User Authentication before Any Action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.4.4. FIA_UAU.5 Multiple Authentication Mechanisms

FIA_UAU.5.1 The TSF shall provide [passwords, digital certificates, LDAP, RADIUS] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [following rules: Users can be configured for the following authentication modes:

- o Password-based
- o Certificate-based
- o Password-based and certificate-based
- o LDAP-based

o RADIUS-based

• Users configured for "password-based and certificate-based" must satisfy the authentication requirements of both mechanisms in order to be successfully authenticated].

6.4.5. FIA_UID.2 User Identification before Any Action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.5. Security Management (FMT)

6.5.1. FMT_MOF.1 Management of Security Function Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to [*determine the behavior of*, *modify the behavior of*] the functions [The TSF requires that User Identity, Authentication Data, User Group membership and Email address].

6.5.2. FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1(1) The TSF shall restrict the ability to [*[create]* the [storage groups] to [user with both Logger System Admin and Logger Rights].

FMT_MTD.1.1(2) The TSF shall restrict the ability to [*modify*] the [retention policies] to [Logger Rights].

FMT_MTD.1.1(3) The TSF shall restrict the ability to [*modify, delete, [create]*] the [event archives, alerts, alert notifications] to [Logger Rights].

FMT_MTD.1.1(4) The TSF shall restrict the ability to [*query, [create, schedule, run, publish]*] the [reports] to [Logger Reports].

FMT_MTD.1.1(5) The TSF shall restrict the ability to [*modify*] the [time, password settings, user session attributes, password of another user] to [Logger System Admin].

FMT_MTD.1.1(6) The TSF shall restrict the ability to [*modify, delete, [create]*] the [TOE users] to [Logger System Admin].

6.5.3. FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

- Manage reports
- Manage time
- Manage TOE users
- Manage password settings

- Manage authentication function
- Manage authentication failure handling
- Manage user session attributes
- Manage user session behavior
- Reset user password]

6.5.4. FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [Logger System Admin, Logger Read Only System Admin, Logger Rights, Logger Search and Logger Reports].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.6. Protection of the TSF (FPT)

6.6.1. FPT_STM.1 Reliable time stamp

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.7. TOE Access (FTA)

6.7.1. FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after an [Administrator-configurable period of inactivity.]

6.7.2. FTA_SSL.4 User-initiated termination

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

6.8. Trusted Path / Channel (FTP)

6.8.1. FTP_ITC Inter-TSF Trusted Channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [*the TSF*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel.

6.8.2. FTP_TRP Trusted Path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured

identification of its end points and protection of the communicated data from [*modification, disclosure*].

FTP_TRP.1.2 The TSF shall permit [*remote users*] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [*remote administration*].

Note: The cryptography is provided by the environment.

6.9. Security Assurance Requirements

The assurance security requirements are summarized in the following table.

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
AGD: Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Lifecycle Support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Part of TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.3	Systematic flaw remediation
ASE: ST evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	Introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE: Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

Table 14 – Security Assurance Requirements at EAL2+

6.10. Security Assurance Requirements Rationale

The ST specifies Evaluation Assurance Level 2. EAL2 was chosen because it is based upon good commercial development practices with thorough functional testing. EAL2 provides the developers and users a moderate level of independently assured security in conventional commercial TOEs. The threat of malicious attacks is not greater than low, the security environment provides physical protection, and the TOE itself offers a very limited interface, offering essentially no opportunity for an attacker to subvert the security policies without physical access. The product was augmented to comply with ALC_FLR.3 in order to document and address requirements for remediation and reporting of faults that may be

discovered in the product after release. The TOE invokes the Environment cryptography to establish TLS1.2 channels for secure communications.

6.11. Security Requirements Rationale

6.11.1. Dependency Rationale

This ST satisfies all the security functional requirement dependencies of the Common Criteria. The table below lists each SFR to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

SFR CLAIM	DEPENDENCIES	DEPENDENCY MET	RATIONALE
FAU_GEN.1	FPT_STM.1	YES	Provided by an NTP Server in the Operational Environment
FAU_SAR.1	FAU_GEN.1	YES	
FAU_SAR.2	FAU_SAR.1	YES	
FAU_SAR.3	FAU_SAR.1	YES	
FAU_STG.1	FAU_GEN.1 TRP_ITC.1	YES	
FCS_CKM.1	FCS_CKM.3 FCS_CKM.6 FCS_COP.1 FCS_RBG.1.	YES	Provided by the environment
FCS_CKM.3	FCS_CKM.1	YES	The TOE has no access to cryptographic keys, so FCS_CKM.3 is N/A.
FCS_CKM.6	FCS_CKM.1	YES	Provided by the environment
FCS_RBG.1	FCS_RBG.1	YES	Provided by the environment
FCS_RBG.2	FCS_RBG.1	YES	Provided by the environment
FCS_COP.1	FCS_CKM.1 FCS_CKM.3	YES	Provided by the environment Note: FCS_CKM.3 is not applicable.
FIA_AFL.1	FIA_UAU.1	YES	Although FIA_ UAU.1 is not included, FIA_ UAU.2, which is hierarchical to FIA_ UAU.1 is included. This satisfies this dependency.
FIA_ATD.1	None	N/A	
FIA_SOS.1	None	N/A	
FIA_UAU.2	FIA_UID.1	YES	Although FIA_ UID.1 is not included, FIA_ UID.2, which is hierarchical to FIA_ UID.1 is included. This satisfies this dependency.
FIA_UAU.5	None	N/A	
FIA_UID.2	None	N/A	
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	YES	
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	YES	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	YES	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FPT_STM.1	None	N/A	Provided by an NTP Server in the Operational Environment

SFR CLAIM	DEPENDENCIES	DEPENDENCY MET	RATIONALE
FTA_SSL.3	FMT_SMR.1	YES	
FTA_SSL.4	None	N/A	
FTP_ITC.1	None	N/A	
FTP_TRP.1	None	N/A	

Table 15 – Dependency Rationale

6.11.2. Security Functional Mappings

The following table provides the correspondence mapping between security objectives for the TOE and the requirements that satisfy them.

OBJECTIVE / SFR	O.AUDIT	OE.COM_PROTECT	O.PRIVILEGE	O.SEC_ACCESS
FAU_GEN.1	✓			
FAU_SAR.1	✓			
FAU_SAR.2	✓			
FAU_SAR.3	✓			
FAU_STG.1	✓			✓
FCS_CKM.1		✓		
FCS_CKM.3	Not Applicable			
FCS_CKM.6		✓		
FCS_RBG.1		✓		
FCS_RBG.2		✓		
FPT_FLS.1		✓		
FPT_TST.1		✓		
FCS_COP.1		✓		
FIA_ATD.1			✓	✓
FIA_SOS.1			✓	✓
FIA_UAU.2			✓	✓
FIA_UAU.5			✓	✓
FIA_UID.2			✓	✓
FMT_MOF.1			✓	✓
FMT_MTD.1				✓
FMT_SMF.1				✓
FMT_SMR.1				✓
FPT_STM.1	✓			
FTA_SSL.3				✓
FTA_SSL.4				✓
FTP_ITC.1		✓		✓
FTP_TRP.1		✓		

Table 16 – Mapping of TOE Security Functional Requirements and Objectives

6.11.3. Sufficiency of Security Requirements

The following table presents a mapping of the rationale of TOE Security Requirements to Objectives.

Objective	RATIONALE
O.AUDIT	The objective to ensure that the TOE shall collect data from all TOE activities including changes to permissions or privileges and provisioning of access, and is met by the following security requirements: • FAU_GEN.1 define the auditing capability for events and administrative access control • FAU_SAR.1 The TOE provides a method to review the audit records. • FAU_SAR.2 The access to the audit records is restricted to those explicitly allowed to access them. • FAU_SAR.3 the audit records can be viewed selectively. • FAU_STG.1 defines where the storage of the audit data. In this case, it is on the Logger server.
OE.COM_PROTECT	This objective ensures that sensitive data in transit is protected[1]. The objective also ensures the confidentiality of data passed between itself and remote users, and between the TOE and external web servers. The cryptography is provided by the TOE environment as are the requirements for FCS_CKM.1, FCS_CKM.6, FCS_RBG.1, FCS_RBG.2, FPT_FLS.1, FPT_TST.1 and FCS_COP.1 • FPT_ITC.1 specifies that a trusted communication channel is available to authorized TOE Components. • FTP_TRP.1 specifies that the TSF provides a distinct trusted communication path to/from TOE. • FCS_CKM.1 and FCS_COP.1 specify the keys that are generated and used. • FCS_CKM.6 specifies the destruction of the keys when no longer needed. • FCS_RBG.1 specifies the random number generator that creates the keys. • FCS_RBG.2 specifies the entropy for the RBG. • FPT_FLS.1 ensures a failure to secure mode when an error occurs. • FPT_TST.1 runs self-tests to ensure correct operation. • **Note:** FCS_CKM.3 is not applicable as the TOE has no access to keys.
O.SEC_ACCESS	This objective ensures that the TOE shall ensure that only Administrators, System Users, and authorized users and applications are granted access to security functions, configuration, and associated data only by authorized users and applications. • FAU_STG.1 defines where the storage of the audit data. In this case, it is on the Logger server. • FIA_ATD.1 specifies security attributes for users of the TOE • FIA_SOS.1 specifies the password requirements • FIA_UAU.2 requires the TOE to enforce authentication of all users

[1] Note encryption is provided by the operating environment.

Objective	RATIONALE
	prior to configuration of the TOE • FIA_UAU.5 provides multiple methods of authenticating to the TOE • FIA_UID.2 requires the TOE to enforce identification of all users prior to configuration of the TOE • FMT_MOF.1 requires that only an administrator be allowed to make changes to authentication, authentication failure actions or session termination activities. • FMT_MTD.1 restricts the ability to perform the functions on TSF data to the Administrator. • FMT_SMF.1 and FMT_SMR.1 support the security functions relevant to the TOE and ensure the definition of an authorized administrator role. • FTA_SSL.3 requires the TSF terminate an interactive session after an administrator configured period. • FTA_SSL.4 requires the user be able to terminate their own session.
O.PRIVILEGE	This objective ensures that the TOE shall protect stored credentials from exposure. • FIA_UAU.2 requires the TOE to enforce authentication of all users prior to configuration of the TOE • FIA_ATD.1 specifies security attributes for users of the TOE • FIA_SOS.1 specifies the password requirements • FIA_UAU.5 provides multiple methods of authenticating to the TOE

Table 17 – Rationale for TOE

7. TOE Summary Specification

This section presents the Security Functions implemented by the TOE.

7.1. TOE Security Functions

The security functions performed by the TOE are as follows:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path

7.2. Security Audit

The TOE generates the following audit data:

- Start-up and shutdown of the audit functions (instantiated by start-up of the TOE)
- User login/logout, Login failures All User access and activities performed while accessing systems]

The TOE records the date, time and type of event as well as the subject identity and outcome of the event.

The TOE provides the Administrator with the capability to read all audit data generated within the TOE via the Console or via the external event sources. The Console provides a suitable means for an Administrator to interpret the information from either the audit log. The audit data is stored on the Logger server.

A.TIMESOURCE is added to the assumptions on operational environment, and OE.TIME is added to the operational environment security objectives. The time and date are provided by the operational environment. The TOE ensures that the audit trail data is stamped when recorded with a dependable date and time received from the OE (operating system). In this manner, accurate time and date is maintained on the TOE.

The Security Audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1
- FAU_SAR.1
- FAU_SAR.2
- FAU_SAR.3
- FAU_STG.1
- FPT_STM.1 (provided by the environment NTP Server)

7.3. Cryptographic Support

Logger uses the environment cryptography to establish TLS v1.2 connections for secure communications.

If Logger is the Server, as in the case of the evaluated configuration, and FIPS mode is configured, Logger avails itself of the Voltage environment Cryptography. This is not part of the TOE, but it is invoked by TOE.

The Cryptographic Support function is designed to satisfy the following security functional requirements:

- FCS_CKM.1
- FCS_CKM.6
- FCS_RBG.1
- FCS_RBG.2
- FPT_FLS.1
- FPT_TST.1
- FCS_COP.1

7.4. Identification and Authentication

The Console provides user interfaces that administrators may use to manage TOE functions. The Console provides web-based access to TOE functions through supported web browsers. The TOE enforces individual identification and authentication and provides a centralized authentication mechanism. Users must reauthenticate after changing their own password. Administrators and Users with management access must successfully authenticate themselves using a unique identifier and authenticator prior to performing any actions on the TOE. The TOE maintains authorization information that determines which TOE functions an authenticated administrator or user (of a given role) may perform.

The TOE allows several authentication mechanisms. They are:

- Password-based
- Certificate-based
- Password-based and certificate-based
- LDAP-based
- RADIUS-based

The TOE maintains the following list of security attributes belonging to individual users:

- User Identity (i.e., user name)
- Password
- Roles
- Rules

The Identification and Authentication function is designed to satisfy the following security functional requirements:

- FIA_AFL.1
- FIA_ATD.1
- FIA_SOS.1
- FIA_UAU.2
- FIA_UAU.5
- FIA_UID.2

7.5. Security Management

Security Management is provided by enforcing roles and rules. Each role consists of a series of privileges. Roles can have privileges added to or removed from them. These roles are then assigned to individuals. In addition, rules can be specified controlling where and when the privileges may be used. Note a user may only have one role at a time.

The table below describes the TOE management functions along with their SFRs.

Functional Description	SFR
Authentication, authentication failure handling, user session behavior is restricted to the Administrator role	FMT_MOF.1
Changes made to TSF data is restricted to either the Logger System Administrator role, the Logger Rights role or to both. These are administrator roles.	FMT_MTD.1
The SFF management functions are: Manage reports Manage time Manage TOE Users Manage password settings Manage authentication function Manage authentication failure handling Manage user session attributes Manage user session behaviour	FMT_SMF.1
Logger maintains the following roles: Logger System Admin, Logger Read Only System Admin, Logger Rights, Logger Search and Logger Reports.	FMT_SMR.1

Table 18– Security Management Functions and SFRs

7.6. Protection of the TSF

Reliable timestamps are provided by an NTP Server in the environment.

FPT_STM.1

7.7. TOE Access

The TOE can terminate sessions either via a pre-configured inactivity timeout or via a user-initiated timeout. The TOE can also prevent TOE users (Administrators, Users), from accessing the system outside of their authorized time.

Functional Description	SFR
The TOE provides the capability for TSF initiated termination of an interactive session after an administrator configurable period of inactivity.	FTA_SSL.3
The TOE provides the TSF with the ability to allow users to initiate termination of their interactive session.	FTA_SSL.4

Table 19 – TOE Access Functions and SFRs

7.8. Trusted Path

The Environment provides the cryptographic algorithms needed to establish a trusted path using TLS v1.2. The table below describes the TOE management functions along with their SFRs.

Functional Description	SFR
The TOE OE provides the trusted path for TOE Users, using environmentally provided cryptography for HTTPS/TLS.	FTP_TRP.1
The TOE OE provides a trusted channel between the parts of the TOE	FTP_ITC.1

Table 20 – Trusted Path/Channels Functions and SFRs

The Environment provides Bouncy Castle version 1.0.2.1 (CMVP certificate # 4616) to protect communications between Logger and the SmartConnectors and between Logger and the AD Server.

The environment provides TLS v1.2 to protect communications between the console and Logger using the environment provided Voltage Cryptographic Module v5.0 (CMVP certificate #2686). The TOE OE supports TLS v1.2.

The TOE supports the cipher suites:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384