

27 JULY 2026

Document Version 1.0



CRYPTOSEAL SERVER VERSION 1.1 SECURITY TARGET



For more information visit us at
www.zetvest.com

Document management

Document identification

Document title	CryptoSeal Server Version 1.1 Security Target
Document version	1.0
Document date	27-JULY-2026
Release Authority	Zetvest Sdn bhd

Document history

Version	Date	Description
0.1	05-FEB-2026	Initial Released
0.2	16-FEB-2026	Update Section 1.5, Section 5 and Section 6
0.3	20-APR-2026	Update Section 1 through Section 6 to address comments from the evaluator and the certification body
0.4	22-JUNE-2026	Update Section 1 through Section 6 to address comments from the evaluator and the certification body
1.0	27-JULY-2026	Update Section 1 and Section 6 Final Released

Table of Contents

1	Security Target introduction	5
1.1	ST Reference.....	5
1.2	TOE Reference	5
1.3	Document Organization	5
1.4	Defined Terms	6
1.5	TOE Overview	7
1.5.1	<i>TOE Usage and Major Security Functions</i>	<i>7</i>
1.5.2	<i>TOE Type</i>	<i>8</i>
1.5.3	<i>Supporting Hardware, Software and/or Firmware</i>	<i>8</i>
1.6	TOE Description	9
1.6.1	<i>Physical Scope of the TOE</i>	<i>9</i>
1.6.2	<i>Logical Scope of the TOE</i>	<i>10</i>
2	Conformance Claim	12
3	Security Problem Definition.....	13
3.1	Overview	13
3.2	Threats.....	13
3.3	Organisational Security Policies.....	13
3.4	Assumptions	14
4	Security Objectives.....	15
4.1	Overview	15
4.2	Security Objectives for the TOE.....	15
4.3	Security Objectives for the Environment	15
4.4	Security Objectives Rationale	16
4.4.1	<i>TOE Security Objectives Rationale</i>	<i>16</i>
4.4.2	<i>Environment Security Objectives Rationale</i>	<i>17</i>
5	Security Requirements	19
5.1	Overview	19
5.2	Security Functional Requirements	19
5.2.1	<i>Overview</i>	<i>19</i>
5.2.2	<i>FAU_GEN.1 Audit data generation</i>	<i>21</i>
5.2.3	<i>FAU_SAR.1 Audit review</i>	<i>21</i>
5.2.4	<i>FDP_ACC.1 Subset access control.....</i>	<i>22</i>
5.2.5	<i>FDP_ACF.1 Security attribute-based access control.....</i>	<i>31</i>
5.2.6	<i>FIA_ATD.1 User attribute definition.....</i>	<i>31</i>

CryptoSeal Server Version 1.1 Security Target

5.2.7	<i>FIA_SOS.1 Verification of secrets</i>	<i>32</i>
5.2.8	<i>FIA_UAU.2 User authentication before any action</i>	<i>32</i>
5.2.9	<i>FIA_UAU.6 Re-authenticating</i>	<i>32</i>
5.2.10	<i>FIA_UID.2 User identification before any action</i>	<i>32</i>
5.2.11	<i>FMT_MSA.1 Management of security attributes.....</i>	<i>33</i>
5.2.12	<i>FMT_MSA.3 Static attribute initialization.....</i>	<i>33</i>
5.2.13	<i>FMT_MTD.1 Management of TSF Data</i>	<i>33</i>
5.2.14	<i>FMT_SMF.1 Specification of Management Functions.....</i>	<i>34</i>
5.2.15	<i>FMT_SMR.1 Security roles</i>	<i>34</i>
5.2.16	<i>FTP_TRP.1 Trusted path.....</i>	<i>34</i>
5.3	TOE Security Assurance Requirements	34
5.4	Security Requirements Rationale	36
5.4.1	Dependency Rationale	36
5.4.2	Mapping of SFRs to Security Objectives for the TOE	37
6	TOE Summary Specification (ASE_TSS.1).....	39
6.1	Overview	39
6.2	Security Audit	39
6.3	Identification and Authentication	40
6.4	Security Management	40
6.5	Secure Communication	49

1 Security Target introduction

1.1 ST Reference

ST Title	CryptoSeal Server Version 1.1 Security Target
ST Version	1.0
ST Date	27-JULY-2026

1.2 TOE Reference

TOE Title	CryptoSeal Server
TOE Version	Version 1.1

1.3 Document Organization

This document is organized into the following major sections:

- Section 1 provides the introductory material for the ST as well as the TOE description (ASE_INT.1).
- Section 2 provides the conformance claims for the evaluation (ASE_CCL.1).
- Section 3 provides the definition of the security problem that the TOE has been designed to address (ASE_SPD.1).
- Section 4 defines the security objectives for the TOE and the environment (ASE_OBJ.2).
- Section 5 contains the security functional and assurance requirements derived from the Common Criteria, Part 2 and 3 respectively, which are in turn satisfied by the TOE and the development lifecycle (ASE_REQ.2).
- Section 6 provides a summary of the TOE specification, identifying the IT security functions provided by the TOE (ASE_TSS.1).

1.4 Defined Terms

The following table defines all subjects, objects, operations, security attributes, external entities and other key terms that are used within the statements of security functional and assurance requirements. It also describes the acronym used in this documentation.

Table 1 - Defined terms

Terms	Descriptions
Authentication Data	It is information used to verify the claimed identity of a user.
AES-256	AES-256 stands for Advanced Encryption Standard with a 256-bit key, a symmetric encryption algorithm developed by the U.S. National Institute of Standards and Technology (NIST).
HTTPS	Hypertext Transfer Protocol Secure
OS	Operating System
RAM	Random Access Memory
TSF data	Data created by and for the TOE, which might affect the operation of the TOE.
TOE	Target of Evaluation
User data	Data created by and for the TOE user, which does not affect the operation of the TSF.
TOE Users	TOE users which are Super Admin, System Admin, User Admin, License Admin, Reporting Admin and End User. TOE users may sometimes be referred to as the Authorized TOE User throughout the document. Refer to Table 17 for detailed roles.

1.5 TOE Overview

1.5.1 TOE Usage and Major Security Functions

The Target of Evaluation (TOE) is CryptoSeal Server Version 1.1, developed by Zetvest Sdn. Bhd. The TOE is a server-based centralized management system deployed within an organization's information technology infrastructure. It provides administrative functions for managing organizational structures, user identities, device registration records, and license information within the operational environment. Refer to Section 1.6.1 for further details on the physical scope of the TOE.

The TOE is deployed on a physical or virtual server and includes a web-based portal through which TOE users perform the TOE operations as stated in Table 17. The TOE enables centralized control and administration of system entities and management data, supporting consistent configuration and oversight across TOE users and devices.

Below are the primary features of the TOE:

- Web-Based Portal – Provides a browser-accessible web portal for TOE users to perform management and configuration activities.
- Organization Management – Provides functionality to create, modify, and manage organizational entities within the system.
- License Management – Enables management of license information and subscription details.
- User Management – Supports creation, modification, and maintenance of user accounts.
- Group Management – Provides functionality to define and manage user groups and associated role assignments.
- Device Management – Enables registration and management of device records within the system.

The following table highlights the range of security functions implemented by the TOE.

Table 2 - Security functions

Security function	Description
Identification and authentication	The TOE requires that each TOE user is successfully identified and authenticated before any interaction with protected resources is permitted.
Security Management	The TOE provides functions that allow management of the TOE and its security functions. The TOE restricts access to the management functions based on the role of the user.

Security function	Description
Security Audit	The TOE generates audit records for security events
Secure Communication	The TOE able to protect the user data and transaction from disclosure and modification by using HTTPS (TLS v1.2 and TLS v1.3).

1.5.2 TOE Type

The TOE is a server-based centralized management system deployed on a physical or virtual server that provides a web-based portal for TOE users to administer organizational structures, user identities, device registration records, and license information within an organization's IT environment. The TOE provides security functionality such as Secure Communication, Security Audit, Identification and Authentication and Security Management. The TOE can be categorised as *Other Devices and Systems* in accordance with the categories identified in the Common Criteria Portal (www.commoncriteriaportal.org).

1.5.3 Supporting Hardware, Software and/or Firmware

The underlying hardware and software that is used to support the TOE are:

Table 3 - Minimum security requirements

Minimum System Requirements	
Hardware and OS requirements for the server	
Processor	Intel Core i7-10700K 8 cores / 16 threads x86 & 64 architecture
Operating System	Ubuntu Server 24.04 Red Hat Enterprise Linux 9
Memory (RAM)	32GB
Storage	1 TB SSD
Desktop (TOE User)	
Web Browser	Chrome 148 Safari 26 Firefox 150 Microsoft Edge 148
Desktop System Requirement	Windows 11

1.6 TOE Description

1.6.1 Physical Scope of the TOE

A typical implementation of the TOE can be found in Figure 1 below, which identifies the various components of the TOE architecture.

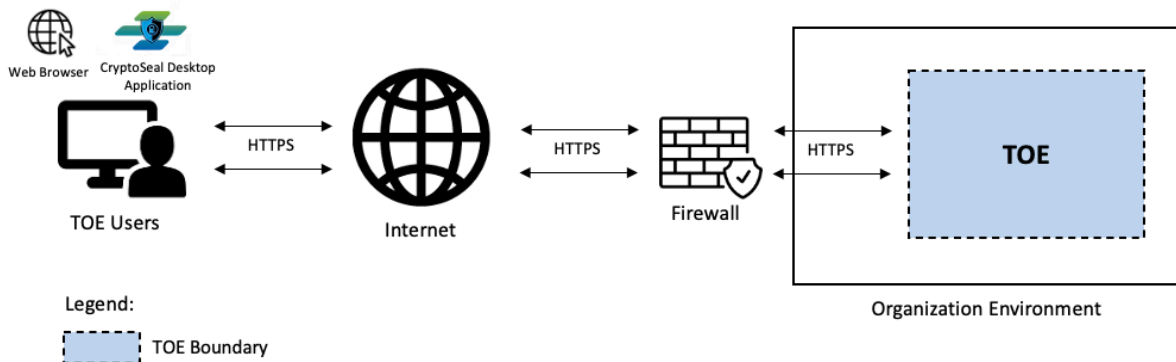


Figure 1 – TOE

The TOE is part of the CryptoSeal technology suite, which consists of CryptoSeal Server Version 1.1 (the TOE) and the CryptoSeal Desktop Application. In an enterprise deployment, the TOE resides within the organization's controlled environment, such as an on-premises data center or private cloud infrastructure. The CryptoSeal Desktop Application is outside the scope of evaluation.

- a) **Web Browser:** The TOE provides a web-based portal that allows TOE users to perform operations stated in Table 13 using a standard web browser stated in Section 1.5.3. The TOE users are created and managed within the TOE. Credentials generated and maintained by the TOE are used by those users to authenticate when accessing the CryptoSeal Desktop Application. The TOE also manages license information, including licenses that authorize the use of the CryptoSeal Desktop Application, and maintains device registration records for devices permitted to access the CryptoSeal Desktop Application.
- b) **CryptoSeal Desktop Application:** CryptoSeal desktop application is a desktop-based cryptographic application that enables application users to perform encryption and decryption on files and directories using AES-256, Threefish and Chacha20 algorithm. The application allows application users to encrypt and decrypt single files, multiple files, or entire directories.

If any issues occur, the TOE users can communicate via a phone call, email or meet face-to-face with the developer to resolve the issue via contact information provided below:

- Zetvest Sdn Bhd (Developer)

Unit 208, Block B, Phileo Damansara 2, Jalan 16/11, 46350 Petaling Jaya, Selangor, Malaysia

Website: <https://www.zetvest.com/>

Email: teams@zetvest.com

Phone No: +6 03 – 7660 8008

The TOE includes the following guidance documentation; CryptoSeal Server Version 1.1 Manual PDF documentation

1.6.2 Logical Scope of the TOE

The logical boundary of the TOE is summarized below.

- a) **Identification & Authentication.** TOE users are required to be identified and authenticated before any information flows are permitted. At the login page, TOE users need to enter a valid email and password in order to access the TOE. Passwords must be at least 8 characters long and include at least one uppercase letter, one lowercase letter, one number, and one special character (@\$!%*?&_). The TOE checks the credentials presented by the user against the authentication information stored in the database.
- b) **Security Management.** The TOE contains various management functions to ensure efficient and secure management of the TOE. The TOE restricts access to the management functions based on the role of the user. The TOE defines six (6) user roles which are Super Admin, System Admin, License Admin, User Admin, Reporting Admin and End User each with specific responsibilities. Refer to Table 13 for detailed functions.
- c) **Security Audit.** The TOE generates audit records for security events. Super Admin and System Admin can view and export audit logs such as:
 - Access Log
 - Failed Log
 - User Activity
 - Desktop Activity
 - System Log

Reporting Admin can view and export audit logs such as:

- Access Log
- Failed Log
- User Activity

CryptoSeal Server Version 1.1 Security Target

- System Log
- d) **Secure Communication.** The TOE can protect the user data and transactions from disclosure and modification by using HTTPS (TLS v1.2 and TLS v1.3)

2 Conformance Claim

This ST and the TOE it describes are conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, CC:2022 Revision 1, November 2022.
 - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, CC:2022 Revision 1, November 2022.
 - Part 3 Conformant
- Common Criteria for Information Technology Security Evaluation Part 5: Pre-defined packages of security requirements, CC:2022 Revision 1, November 2022.

This ST and the TOE it describes are conformant to the following package:

- EAL2

3 Security Problem Definition

3.1 Overview

This section describes the nature of the security problem that the TOE is designed to address. The security problem is described through:

- a) a series of **threats** that the TOE has been designed to mitigate,
- b) specific **assumptions** about the security aspects of the environment (both IT related and non-IT related elements) in which the TOE will operate, and
- c) any relevant **organisational security policies** statements that are made in terms of rules or guidelines that must be followed by the TOE and/or the operational environment.

3.2 Threats

The TOE addresses the following threats:

Table 4 - Threats

Identifier	Threat statement
T.COMINT	An unauthorised user may attempt to disclose or modify data transmitted between distributed TOE components, thereby compromising the confidentiality of the communication
T.DISCLOSURE	An unauthorised user may attempt to compromise the integrity of the protected resource on the TOE
T.IMPERSON	An attacker may gain unauthorised access to information or resources by impersonating an authorised user of the TOE.
T.PASSWORD	An unauthorized user may take advantage of weak administrative passwords to gain privileged access to the TOE functions.
T.NOMGMT	An unauthorized person modifies management data that they are not authorised to access resulting in a loss of integrity of the data that the TOE uses to enforce the security functions.

3.3 Organisational Security Policies

No organisational security policies have been defined regarding the use of the TOE.

3.4 Assumptions

The following specific conditions are assumed to exist in an environment where the TOE is employed.

Table 5 - Assumptions

Identifier	Assumption statement
A.NOEVIL	It is assumed that the person who manages the TOE is not hostile and is competent.
A.AUTHORISE	It is assumed that the TOE can only be accessed by authorized TOE users.
A.TIMESTAMP	It is assumed that the operational environment is capable of providing reliable timestamps for the TOE
A.UPDATE	It is assumed that the developer will regularly apply security patches and updates to the TOE and the underlying platform.
A.FIREWALL	It is assumed that the firewall should be able to provide gateway filtering; only allowing HTTP and HTTPS inbound connection traffic to pass through to TOE.

4 Security Objectives

4.1 Overview

The security objectives are a concise statement of the intended response to the security problem defined in Section 3. They are security objectives for the TOE to address and additional objectives that provide specific direction for the intended environment in which the TOE is to operate.

4.2 Security Objectives for the TOE

Table 6 - Security Objectives for the TOE

Identifier	Objective statements
O.AUTHENTICATE	The TOE must ensure that all TOE users are authenticated before they access a protected resource or functions.
O.TOECOM	The TOE must protect the confidentiality of its dialogue between distributed components from disclosure and modification
O.PASSWORD	The TOE must ensure that the TOE user password has at least 8 characters long and include at least one uppercase letter, one lowercase letter, one number, and one special character (@\$!%?&_)
O.LOGGING	The TOE shall log security-relevant actions and allow only TOE User to view them
O.MANAGE	The TOE must allow authorized TOE users to effectively manage the TOE, while ensuring that appropriate controls are maintained over those functions.

4.3 Security Objectives for the Environment

Table 7 - Security Objectives for the Environment

Identifier	Objective statements
OE.ADMIN	The developer of the TOE must ensure that the TOE users who manage the TOE are not hostile and competent.
OE.AUTHDATA	Those responsible for the TOE must ensure that access credentials such as passwords are protected by the users
OE.UPDATE	The developer shall ensure that the TOE and the underlying platform are regularly updated with appropriate security patches and fixes.

OE.FIREWALL	The firewall will implement network filtering; only allowing HTTP and HTTPS inbound connection traffic to pass through to Web server.
OE.TIMESTAMP	The operational environment shall provide reliable timestamps for the TOE.

4.4 Security Objectives Rationale

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

Table 8 - Security objectives traced back to assumptions and threats

Objectives \ Threats/ Assumptions	T.COMINT	T.DISCLOSURE	T.IMPERSON	T.PASSWORD	T.NOMGMT	A.AUTHORISE	A.NOEVIL	A.FIREWALL	A.UPDATE	A.TIMESTAMP
O.AUTHENTICATE		✓	✓							
O.TOECOM	✓									
O.PASSWORD				✓						
O.LOGGING			✓							
O.MANAGE					✓					
OE.ADMIN							✓			
OE.AUTHDATA						✓				
OE.UPDATE									✓	
OE.FIREWALL								✓		
OE.TIMESTAMP										✓

4.4.1 TOE Security Objectives Rationale

The following table demonstrates that all security objectives for the TOE are trace back to the threats in the security problem definition.

Table 9 - TOE security objectives rationale

Threats	Rationale
T.COMINT	The security objective below counters T.COMINT: • O.TOECOM ensures that the TOE protect the confidentiality of communications between distributed TOE components
T.DISCLOSURE	The security objective below counters T.DISCLOSURE: • O.AUTHENTICATE ensures that all TOE users are authenticated before they access a protected resources or functions
T.IMPERSON	The security objective below counters T.IMPERSON: • O.AUTHENTICATE ensures the likelihood of a successful impersonation is reduced by the identification and authentication measures (email and passwords) • O.LOGGING ensures that all security-relevant action such as unauthorised login is logged and allow only TOE User to view them
T.PASSWORD	The security objective below counters T.PASSWORD: • O.PASSWORD ensures that all TOE users adhere with the acceptable password policy (at least 8 characters long and include at least one uppercase letter, one lowercase letter, one number, and one special character (@\$!%?&_)) to avoid from unauthorised user taking advantage of weak password and gain unauthorised access to the TOE functions.
T.NOMGMT	The security objective below counters: • O.MANAGE ensures that the TOE provides the tools necessary for the authorized TOE users to manage the security-related functions and that those tools are usable only by users with appropriate authorizations.

4.4.2 Environment Security Objectives Rationale

The following table demonstrates that all security objectives for the operational environment are trace back to assumptions in the security problem definition.

Table 10 - Environment Security Objectives Rationale

Assumptions	Objective	Rationale
A.NOEVIL	OE.ADMIN	This objective ensures that those responsible for managing the TOE are competent and trustworthy individuals.

CryptoSeal Server Version 1.1 Security Target

Assumptions	Objective	Rationale
A.AUTHORISE	OE.AUTHDATA	This objective ensures that only authorised TOE user able to access the TOE and access credentials such as passwords are protected by that user
A.TIMESTAMP	OE.TIMESTAMP	This objective ensures that reliable timestamps are provided by the operational environment to support the TOE's time-related functions such as event recording and auditing
A.UPDATE	OE.UPDATE	The objective ensures that the TOE and its underlying platform will be regularly updated with appropriate security patches and fixes by the developer
A.FIREWALL	OE.FIREWALL	The objective ensures that the firewall provides network filtering at the gateway through configuration of HTTPS and HTTP defined by the organization.

5 Security Requirements

5.1 Overview

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from Common Criteria Part 2 (Ref. Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, November 2022, CC:2022, Revision 1). Following are the approved operations and the document conventions used within this ST to depict their application:

- **Assignment.** The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows [assignment].
- **Selection.** The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [*selection*].
- **Refinement.** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions~~.
- **Iteration.** The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows FDP_1FF.1a and FDP_1FF.1b.

5.2 Security Functional Requirements

5.2.1 Overview

The security functional requirements are expressed using the notation stated in Section 5.1 above and are itemised in the table below.

Table 11 - Security functional requirements

Identifier	Title
Security Audit	
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
User Data Protection	
FDP_ACC.1	Subset access control

CryptoSeal Server Version 1.1 Security Target

Identifier	Title
Security Audit	
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FDP_ACF.1	Security attribute-based access control
Identification and Authentication	
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.2	User authentication before any action
FIA_UAU.6	Re-authenticating
FIA_UID.2	User identification before any action
Security Management	
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
Trusted Path	
FTP_TRP.1	Trusted Path

5.2.2 FAU_GEN.1 Audit data generation

Hierarchical to:	No other components.
FAU_GEN.1.1	The TSF shall be able to generate an audit data 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) [Specifically defined auditable events listed in the Notes section below].
FAU_GEN.1.2	The TSF shall record within the audit data at least the following information: a) Date and time of the auditable event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; b) For each auditable event type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package or ST, [none].
Dependencies:	FPT_STM.1 Reliable time stamps
Notes:	Auditable events within the TOE: • Access Log • Failed Log • User Activity • Desktop Activity • System Log

5.2.3 FAU_SAR.1 Audit review

Hierarchical to:	No other components.
FAU_SAR.1.1	The TSF shall provide [Super Admin, System Admin and Reporting Admin] with the capability to read and export [audit information stated in Table 12] from the audit data.
FAU_SAR.1.2	The TSF shall provide the audit data in a manner suitable for the user to interpret the information.
Dependencies:	FAU_GEN.1 Audit data generation

Notes:	Table 12 - Audit Information	
	Roles	Audit Information
	Super Admin	• Access Log • Failed Log • User Activity • Desktop Activity • System Log Note: The Super Admin is able to access the audit information for all organization
	System Admin	• Access Log • Failed Log • User Activity • Desktop Activity • System Log Note: The System Admin is able to access only the audit information for the assigned organization.
	Reporting Admin	• Access Log • Failed Log • User Activity • System Log Note: The Reporting Admin is able to access only the audit information for the assigned organization.

5.2.4 FDP_ACC.1 Subset access control

Hierarchical to:	No other components.	
FDP_ACC.1.1	The TSF shall enforce the [access control SFP] on [objects listed in the Table 13].	
Dependencies:	FDP_ACF.1 Security attribute-based access control	
Notes:	Table 13 - Subject, Object and Operations for FDP_ACC.1	
	Subject	Object
	Operation	
Super Admin (Super Admin is able to access and perform	Login	Login
	Home	View the summary of (all organization): • License Expiration

CryptoSeal Server Version 1.1 Security Target

	operation for all organization)		• Active Users • Active Groups • Registered Devices • Latest Users • Activity Timeline
		Company	• View organization list • View inactive organization list • Register new company • Show organization details • Edit organization details • Deactivate organization
		License	License List (all organization): • View license list • View expired license list • Register new license • Edit license details • Remove license Pending Approval: • View license extension information • Export pending approval list (Excel)
		Extension	• View license extension list • View pending extension approval
		User	• View user master list • View inactive user list • Import user • Register new user • View user master details • Edit user details
		Group	Group List: • View group list • View inactive group list • Register new group

CryptoSeal Server Version 1.1 Security Target

			• View group details • Edit group • Manage users • Deactivate group • Export group list (Excel) Group Invitation: • View group invitation list • Accept/Decline group invitation • Export group invitation list (Excel)
		Device	• View device list • View activity timeline • View device blacklist audit log • View device information • Edit device details • Remove device • Blacklist device • Export device list
		Reporting	Access Log: • View access log report • Export access log report (Excel) Failed Log: • View failed access log User Activity: • View user activity report • Export user activity report (Excel) Desktop Activity: • View desktop activity report • Export desktop activity report (Excel) System Logs:

CryptoSeal Server Version 1.1 Security Target

			• View system logs • Export system logs (Excel) • Export system logs (Raw Log)
		Logout	Logout
	System Admin (System Admin is able to access and perform operation only for the assigned organization)	Login	Login
		Home	View the summary of: • License Expiration • Active Users • Active Groups • Registered Devices • Latest Users • Activity Timeline
		About Us	View About Us
		FAQs	View Frequently Asked Questions (FAQS)
		License	License List: • View license list • View expired license list • Edit license details • Remove license Pending Approval: • View license extension information • Export pending approval list (Excel)
		Extension	• View license extension list
		User	• View user master list • View inactive user list • Import user • Register new user • View user master details • Edit user details

CryptoSeal Server Version 1.1 Security Target

		Group	Group List: • View group list • View inactive group list • Register new group • View group details • Edit group • Manage users • Deactivate group • Export group list (Excel) Group Invitation: • View group invitation list • Accept/Decline group invitation • Export group invitation list (Excel)
		Device	• View device list • View activity timeline • View device blacklist audit log • View device information • Edit device details • Remove device • Blacklist device • Export device list
		Content	View/Edit content
		Reporting	Access Log: • View access log report • Export access log report (Excel) Failed Log: • View failed access log User Activity: • View user activity report • Export user activity report (Excel)

CryptoSeal Server Version 1.1 Security Target

			Desktop Activity: • View desktop activity report • Export desktop activity report (Excel) System Logs: • View system logs • Export system logs (Excel) • Export system logs (Raw Log)
		Logout	Logout
	User Admin (User Admin is able to access and perform operation only for the assigned organization)	Login	Login
		Home	View the summary of: • Active Users • Active Groups • Registered Devices
		About Us	View About Us
		FAQs	View Frequently Asked Questions (FAQS)
		User (assigned organization)	• View user master list • View inactive user list • Import user • Register new user • View user master details • Edit user details
		Group (assigned organization)	Group List: • View group list • View inactive group list • Register new group • View group details • Edit group • Manage users • Deactivate group • Export group list (Excel)

CryptoSeal Server Version 1.1 Security Target

			Group Invitation: View group invitation list
		Device (assigned organization):	- View device list - View activity timeline - View device information - Edit device details - Remove device - Export device list
		Logout	Logout
	License Admin (License Admin is able to access and perform operation only for the assigned organization)	Login	Login
		Home	View the summary of : - License Expiration - Active Groups - Registered Devices
		About Us	View About Us
		FAQS	View Frequently Asked Questions (FAQS)
		License	License List: - View license list - View expired license list - Edit license details - Remove license Pending Approval: - View license extension information - Export pending approval list (Excel)
		Extension	View license extension list
		Group	Group List: - View group list - View group details

CryptoSeal Server Version 1.1 Security Target

			• Export group list (Excel) Group Invitation: • View group invitation list • Accept/Decline group invitation • Export group invitation list (Excel)
		Device	• View device list • View activity timeline • View device information • Edit device details • Remove device • Export device list
		Logout	Logout
	Reporting Admin (Reporting Admin is able to access and perform operation only for the assigned organization)	Login	Login
		Home	View the summary of: • Active Groups • Registered Devices
		About Us	View About Us
		Group	Group List: • View group list • View group details • Export group list (Excel) Group Invitation: • View group invitation list • Accept/Decline group invitation • Export group invitation list (Excel)
		Device	• View device list • View activity timeline • View device information • Edit device details • Remove device

CryptoSeal Server Version 1.1 Security Target

			Export device list
		Reporting	Access Log: - View access log report - Export access log report (Excel) Failed Log: - View failed access log User Activity: - View user activity report - Export user activity report (Excel) - Add remark System Logs: - View system logs - Export system logs (Excel) - Export system logs (Raw Log)
		Logout	Logout
	End User (End User is able to access and perform operation only for the assigned organization)	Login	Login
		Home	View the summary of (assigned organization): - Active Groups - Registered Devices
		FAQS	View Frequently Asked Questions (FAQS)
		Group	Group List: - View group list - View group details - Export group list (Excel) Group Invitation: - View group invitation list - Accept/Decline group invitation

CryptoSeal Server Version 1.1 Security Target

			• Export group invitation list (Excel)
		Device	• View device list • View activity timeline • View device information • Edit device details • Remove device • Export device list
		Logout	Logout

5.2.5 FDP_ACF.1 Security attribute-based access control

Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the [access control SFP] to objects based on the following: [as listed in the Table 1].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [a) If the TOE user is successfully authenticated accordingly, then access is granted based on privilege allocated; b) If the TOE user is not authenticated successfully, therefore, access permission is denied]
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [none].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [none].
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
Notes:	None.

5.2.6 FIA_ATD.1 User attribute definition

Hierarchical to:	No other components
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [

	a. Email, b. Password].
Dependencies:	No dependencies
Notes:	None.

5.2.7 FIA_SOS.1 Verification of secrets

Hierarchical to:	No other components.
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet [a minimum length of 8-characters, contain at least one uppercase letter, one lowercase letter, one number, and one special character (@\$!%*?&_)]
Dependencies:	No dependencies
Notes:	None.

5.2.8 FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication
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.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

5.2.9 FIA_UAU.6 Re-authenticating

Hierarchical to:	No other components.
FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions [no user interaction has been detected over 15 minutes] .
Dependencies:	No dependencies
Notes:	None.

5.2.10 FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any TSF-mediated actions on behalf of that user.

Dependencies:	No dependencies.
Notes:	None.

5.2.11 FMT_MSA.1 Management of security attributes

Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the [access control SFP] to restrict the ability to [change_default, modify, delete [none]] the security attributes [all organization information] to [Super Admin].
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.12 FMT_MSA.3 Static attribute initialization

Hierarchical to:	No other components
FMT_MSA.3.1	The TSF shall enforce the [access control SFP] to provide [restrictive] default values for security attributes that are used to enforce the SFP
FMT_MSA.3.2	The TSF shall allow the [none] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Notes:	None.

5.2.13 FMT_MTD.1 Management of TSF Data

Hierarchical to:	No other components
FMT_MTD.1.1	The TSF shall restrict the ability to [modify] the [Super Admin Password] to [Super Admin].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.14 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [all management functions stated in Table 13]
Dependencies:	No dependencies.
Notes:	None.

5.2.15 FMT_SMR.1 Security roles

Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles [Super Admin, System Admin, License Admin, User Admin, Reporting Admin, End User]
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

5.2.16 FTP_TRP.1 Trusted path

Hierarchical to:	No other components.
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 or 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 [initial user authentication, [and all further communication after authentication]] .
Dependencies:	No dependencies
Notes:	None.

5.3 TOE Security Assurance Requirements

The assurance package for the evaluation of the TOE is Evaluation Assurance Level 2 (EAL2). EAL2 requires evidence relating to the design information and test results, but does not demand more effort on the part of the developer than is consistent with good commercial practice.

EAL2 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation and a basic description on the architecture of the TOE, to understand the security behaviours. The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided). EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

The TOE has a low to moderate level of assurance in enforcing its security functions when instantiated in its intended environment, which imposes no restrictions on assumed activity on applicable networks. EAL2 is sufficient to demonstrate that the TOE is resistant to attackers with a Basic attack potential.

Below are the assurance class and assurance components for EAL2:

Table 14 - Assurance Components

Assurance class	Assurance components
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: Life cycle support	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_CMC.2 Use of the CM system
	ALC_DEL.1 Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification

Assurance class	Assurance components
ATE: Tests	ATE_IND.2 Independent testing - sample
	ATE_FUN.1 Functional testing
	ATE_COV.1 Evidence of coverage
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

5.4 Security Requirements Rationale

5.4.1 Dependency Rationale

The table below demonstrates the mutual supportiveness of the SFRs for the TOE by demonstrating how the SFR dependencies are fulfilled by the TOE and by justifying those dependencies that are not fulfilled.

The SARs relevant to the TOE constitute an evaluation assurance level of EAL2, as defined in the Common Criteria and include no extensions or augmentations. Therefore, as a complete evaluation assurance level, they are a mutually supportive set and require no further justification.

Table 15 - Dependency rationale

SFR	Dependency	Inclusion
FAU_GEN.1	FPT_STM.1 Reliable time stamps	FPT_STM.1 has not been included as the TOE obtains all audit timestamps from the underlying platform. This has been addressed in Section 3.4 by A.TIMESTAMP.
FAU_SAR.1	FAU_GEN.1 Audit data generation	FAU_GEN.1
FDP_ACC.1	FDP_ACF.1 Security attribute-based access control	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static Attribute initialisation	FDP_ACC.1 FMT_MSA.3
FIA_ATD.1	No dependencies	N/A
FIA_SOS.1	No dependencies	N/A
FIA_UAU.2	FIA_UID.1 Timing of identification	FIA_UID.2
FIA_UAU.6	No dependencies	N/A

CryptoSeal Server Version 1.1 Security Target

SFR	Dependency	Inclusion
FIA_UID.2	No dependencies	N/A
FMT_MSA.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 FMT_SMR.1
FMT_MTD.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 FMT_SMR.1
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.2
FTP_TRP.1	No dependencies	N/A

5.4.2 Mapping of SFRs to Security Objectives for the TOE

Table 16 - Security objectives rationale

Objective	Rationale
O.LOGGING	This objective is met by: - FAU_GEN.1 specifying which events to log - FAU_SAR.1 allowing Super Admin, System Admin, and Reporting Admin the capability to read and export audit information
O.AUTHENTICATE	This objective is met by: - FIA_UID.2 and FIA_UAU.2 specifying that TOE users must be identified and authenticated before allowing access - FIA_ATD.1 ensures user security attributes are maintained. - FMT_SMF.1 lists the security management functions that must be controlled after TOE users are identified and authenticated
O.TOECOM	This objective is met by: FTP_TRP.1 which ensures that traffic transmitted between TOE components is protected from disclosure and modification

CryptoSeal Server Version 1.1 Security Target

Objective	Rationale
O.PASSWORD	This objective is met by: FIA_SOS.1 specifying that the TOE user password has a minimum of 8 characters and include at least one uppercase letter, one lowercase letter, one number, and one special character (@\$!%?&_)
O.MANAGE	This objective is met by: - FMT_MSA.1. The requirement helps meet the objective by enforcing access control to restrict modification of security attributes (all organization information) to Super Admin. - FMT_MSA.3. The requirement helps meet the objective by restricting access to provide default values for security attributes that are used to enforce the SFP - FMT_MTD.1. The requirement helps meet the objective by restricting modification of the Super Admin Password to Super Admin only - FMT_SMF.1. The requirement helps meet the objective by performing all management functions listed in Table 17 - FMT_SMR.1. The requirement helps meet the objective by maintaining all roles (Super Admin, System Admin, License Admin, User Admin, Reporting Admin, End User) and the ability to associate users with roles.

6 TOE Summary Specification (ASE_TSS.1)

6.1 Overview

This section provides the TOE summary specification, a high-level description of how the TOE implements the claimed security functional requirements. The TOE provides the following security functions:

- Security Audit;
- Identification and Authentication;
- Security Management; and
- Secure Communication

6.2 Security Audit

The TOE will generate audit records (which contain the date and time of the event, type of event, subject identity and outcome of the transaction event) for the auditable events (**FAU_GEN.1**) such as Access Log, Failed Log, User Activity, Desktop Activity and System Log.

System Admin can view and export audit logs such as (**FAU_SAR.1**):

- Access Log
- Failed Log
- User Activity
- Desktop Activity
- System Log

Reporting Admin can view and export audit logs such as (**FAU_SAR.1**):

- Access Log
- Failed Log
- User Activity
- System Log

Timestamps for the server are generated for audit logs by utilising the underlying operating system. The TOE does not generate its own timestamps for use in audit records; these are supplied by the underlying operating system.

6.3 Identification and Authentication

The TOE implement access control and authentication measures to ensure that TOE data and functionality is not misused by unauthorised parties (**FDP_ACC.1**). All TOE users must provide authentication data to the TOE to affirm their identity and role prior to being granted access to any TOE functions or interfaces.

The TOE maintains six types of users which are Super Admin, System Admin, License Admin, User Admin, Reporting Admin and End User (**FMT_SMR.1**). These users may access the TOE via the web based portal that the platform provides. At the login page, TOE user need to enter a valid email and password in order to access the TOE (**FIA_ATD.1**). The acceptable minimum password length is 8 characters contain at least one uppercase letter, one lowercase letter, one number, and one special character (@\$!%*?&_) (**FIA_SOS.1**). TOE user must be authenticated to the TOE prior performing any TOE functions by entering a valid email and password (**FIA_ATD.1**, **FIA_UAU.2**, **FIA_UID.2**, **FDP_ACF.1**). If there is no interaction with the TOE for over 15 minutes, TOE users will be directed to the login page and need to re-authenticate (**FIA_UAU.6**)

6.4 Security Management

The TOE provides a suite of TOE functions to authorized TOE users. These functions allow the TOE to be configured in accordance with the operational environment in which it is deployed. All functions are subject to role-based access control to prevent unauthorized configuration changes. The TOE user's operation is as follows (**FMT_SMF.1**, **FMT_MTD.1**, **FMT_MSA.1** and **FMT_MSA.3**):

Table 17 - TOE User's operation

TOE User	Menu / Function	Operation
Super Admin (Super Admin is able to access and perform operation for all organization)	Login	Login
	Home	View the summary of (all organization): • License Expiration • Active Users • Active Groups • Registered Devices • Latest Users • Activity Timeline
	Company	• View organization list

CryptoSeal Server Version 1.1 Security Target

		• View inactive organization list • Register new company • Show organization details • Edit organization details • Deactivate organization
	License	License List (all organization): • View license list • View expired license list • Register new license • Edit license details • Remove license Pending Approval: • View license extension information • Export pending approval list (Excel)
	Extension	• View license extension list • View pending extension approval
	User	• View user master list • View inactive user list • Import user • Register new user • View user master details • Edit user details
	Group	Group List: • View group list • View inactive group list • Register new group • View group details • Edit group • Manage users • Deactivate group • Export group list (Excel)

CryptoSeal Server Version 1.1 Security Target

		Group Invitation: • View group invitation list • Accept/Decline group invitation • Export group invitation list (Excel)
	Device	• View device list • View activity timeline • View device blacklist audit log • View device information • Edit device details • Remove device • Blacklist device • Export device list
	Reporting	Access Log: • View access log report • Export access log report (Excel) Failed Log: • View failed access log User Activity: • View user activity report • Export user activity report (Excel) Desktop Activity: • View desktop activity report • Export desktop activity report (Excel) System Logs: • View system logs • Export system logs (Excel) • Export system logs (Raw Log)
	Logout	Logout
System Admin	Login	Login

CryptoSeal Server Version 1.1 Security Target

(System Admin is able to access and perform operation only for the assigned organization)	Home	View the summary of: • License Expiration • Active Users • Active Groups • Registered Devices • Latest Users • Activity Timeline
	About Us	View About Us
	FAQs	View Frequently Asked Questions (FAQS)
	License	License List: • View license list • View expired license list • Edit license details • Remove license Pending Approval: • View license extension information • Export pending approval list (Excel)
	Extension	• View license extension list
	User	• View user master list • View inactive user list • Import user • Register new user • View user master details • Edit user details
	Group	Group List: • View group list • View inactive group list • Register new group • View group details • Edit group

CryptoSeal Server Version 1.1 Security Target

		• Manage users • Deactivate group • Export group list (Excel) Group Invitation: • View group invitation list • Accept/Decline group invitation • Export group invitation list (Excel)
	Device	• View device list • View activity timeline • View device blacklist audit log • View device information • Edit device details • Remove device • Blacklist device • Export device list
	Content	View/Edit content
	Reporting	Access Log: • View access log report • Export access log report (Excel) Failed Log: • View failed access log User Activity: • View user activity report • Export user activity report (Excel) Desktop Activity: • View desktop activity report • Export desktop activity report (Excel) System Logs: • View system logs

CryptoSeal Server Version 1.1 Security Target

		• Export system logs (Excel) • Export system logs (Raw Log)
	Logout	Logout
User Admin (User Admin is able to access and perform operation only for the assigned organization)	Login	Login
	Home	View the summary of: • Active Users • Active Groups • Registered Devices
	About Us	View About Us
	FAQs	View Frequently Asked Questions (FAQS)
	User (assigned organization)	• View user master list • View inactive user list • Import user • Register new user • View user master details • Edit user details
	Group (assigned organization)	Group List: • View group list • View inactive group list • Register new group • View group details • Edit group • Manage users • Deactivate group • Export group list (Excel) Group Invitation: • View group invitation list
	Device (assigned organization):	• View device list • View activity timeline • View device information • Edit device details

CryptoSeal Server Version 1.1 Security Target

		• Remove device • Export device list
	Logout	Logout
License Admin (License Admin is able to access and perform operation only for the assigned organization)	Login	Login
	Home	View the summary of : • License Expiration • Active Groups • Registered Devices
	About Us	View About Us
	FAQS	View Frequently Asked Questions (FAQS)
	License	License List: • View license list • View expired license list • Edit license details • Remove license Pending Approval: • View license extension information • Export pending approval list (Excel)
	Extension	View license extension list
	Group	Group List: • View group list • View group details • Export group list (Excel) Group Invitation: • View group invitation list • Accept/Decline group invitation • Export group invitation list (Excel)
	Device	• View device list • View activity timeline

CryptoSeal Server Version 1.1 Security Target

		• View device information • Edit device details • Remove device • Export device list
	Logout	Logout
Reporting Admin (Reporting Admin is able to access and perform operation only for the assigned organization)	Login	Login
	Home	View the summary of: • Active Groups • Registered Devices
	About Us	View About Us
	Group	Group List: • View group list • View group details • Export group list (Excel) Group Invitation: • View group invitation list • Accept/Decline group invitation • Export group invitation list (Excel)
	Device	• View device list • View activity timeline • View device information • Edit device details • Remove device • Export device list
	Reporting	Access Log: • View access log report • Export access log report (Excel) Failed Log: • View failed access log

CryptoSeal Server Version 1.1 Security Target

		User Activity: • View user activity report • Export user activity report (Excel) • Add remark System Logs: • View system logs • Export system logs (Excel) • Export system logs (Raw Log)
	Logout	Logout
End User (End User is able to access and perform operation only for the assigned organization)	Login	Login
	Home	View the summary of (assigned organization): • Active Groups • Registered Devices
	FAQS	View Frequently Asked Questions (FAQS)
	Group	Group List: • View group list • View group details • Export group list (Excel) Group Invitation: • View group invitation list • Accept/Decline group invitation • Export group invitation list (Excel)
	Device	• View device list • View activity timeline • View device information • Edit device details • Remove device • Export device list
	Logout	Logout

The TOE implement access control and authentication measures to ensure that TOE data and functionality is not misused by unauthorised parties (**FDP_ACC.1** and **FDP_ACF.1**).

6.5 Secure Communication

When a TOE user accesses the TOE on their browser by typing in the URL address, the TOE will initiate a secure channel establishment with the TOE user's browser (**FTP_TRP.1**).

The TOE protects user data and transactions from disclosure and modification by using Transport Layer Security (TLS v1.2 and TLS v1.3). This secure channel ensures the confidentiality and integrity of data exchanged between the TOE and the user's browser.

--- END OF DOCUMENT ---