Namusoft Co., Ltd.

FilingBox MEGA2 v2

Security Target v1.5

The Security Target related to the certified TOE.

This Security Target is written in Korean and translated from Korean into English.

Revision history

Version	Date	Changes	Author
1.0	2023-11-30	Initial document	Namusoft Co., Ltd.
1.1	2023-12-13	TOE physical scope modification	Namusoft Co., Ltd.
1.2	2024-01-30	Observation report EOR-01 reflection	Namusoft Co., Ltd.
1.3	2024-02-23	Cryptographic support SFR update	Namusoft Co., Ltd.
1.4	2024-02-26	TOE and 3rd party version update	Namusoft Co., Ltd.
1.5	2024-03-21	Evaluation facility review reflection	Namusoft Co., Ltd.

Table of contents

1 ST introduction

1.1 ST reference

Title	FilingBox MEGA2 v2 Security Target
Version	v1.5
Date	2024-03-21
Author	Namusoft Co., Ltd.
CC version	v3.1 R5
Evaluation Assurance Level	EAL1

1.2 TOE reference

TOE	FilingBox MEGA2 v2
Version	v2.6.0
Components	FilingBox MEGA2 v2 Server v2.2.0 (FilingBox MEGA2_v2_Server_v2.2.0.tgz)
	FilingBox MEGA2 v2 Windows Client v2.2.0 (FilingBox MEGA2_v2_Windows_Client_v2.2.0.exe)
	FilingBox MEGA2 v2 Linux Client v2.2.0 (FilingBox MEGA2_v2_Linux_Client_v2.2.0.tgz)
Documentation	FilingBox MEGA2 v2 Server User Manual v1.3 (FilingBox MEGA2 v2 Server User Manual v1.3.pdf)
	FilingBox MEGA2 v2 Client User Manual v1.3 (FilingBox MEGA2 v2 Client User Manual v1.3.pdf)
	FilingBox MEGA2 v2 Server Installation Manual v1.4 (FilingBox MEGA2 v2 Server Installation Manual v1.4.pdf)
	FilingBox MEGA2 v2 Client Installation Manual v1.4 (FilingBox MEGA2 v2 Client Installation Manual v1.4.pdf)
Developer	Namusoft Co., Ltd.

1.3 TOE overview

The TOE is a storage protection software that allows only authorized applications to normally access files within the storage protected by the TOE, while restricting other applications from normally reading, modifying, or deleting file data in that storage.

When it is desired to prevent loss and theft of data for files created and used by a specific application, the data is stored in the TOE's storage connected to network storage. Then, only the

authorized application is allowed to access the data of those files, thereby preventing data loss and theft by unauthorized applications.

The TOE stores the names, paths, and hash values of the executable files of the applications it intends to allow. When an application requests access to file data, the TOE verifies the access by comparing the name, path, and hash value of the executable file making the request.

The applications that are supported by the TOE for access control to file data include the following.

Client	FilingBox MEGA2 v2 Windows Client	FilingBox MEGA2 v2 Linux Client
Supported applications	- MS Word 2013 - MS Excel 2013 - MS PowerPoint 2013 - Notepad 10	- Bash-based cli • /usr/bin/mkdir • /usr/bin/rm • /usr/bin/cp • /usr/bin/cat • /usr/bin/vi

The TOE components consist of FilingBox MEGA2 v2 Server, FilingBox MEGA2 v2 Windows Client, and FilingBox MEGA2 v2 Linux Client. The main security features of the FilingBox MEGA2 v2 Server are to record and manage audit data for major auditable events to operate the TOE securely, cryptographic support features such as cryptographic key management and cryptographic operations for encryption of users and TSF data, user data protection features that control access to file data, identification and authentication features that handle authorized administrator identification and authentication, and continuous authentication failures, security management features for defining security functions and roles, TSF protection features that include protection of TSF data being transferred between TOE components, protection of TSF data stored in storage controlled by the TSF, TSF self-test and integrity verification, and TOE access features that manage connection sessions of authorized administrators.

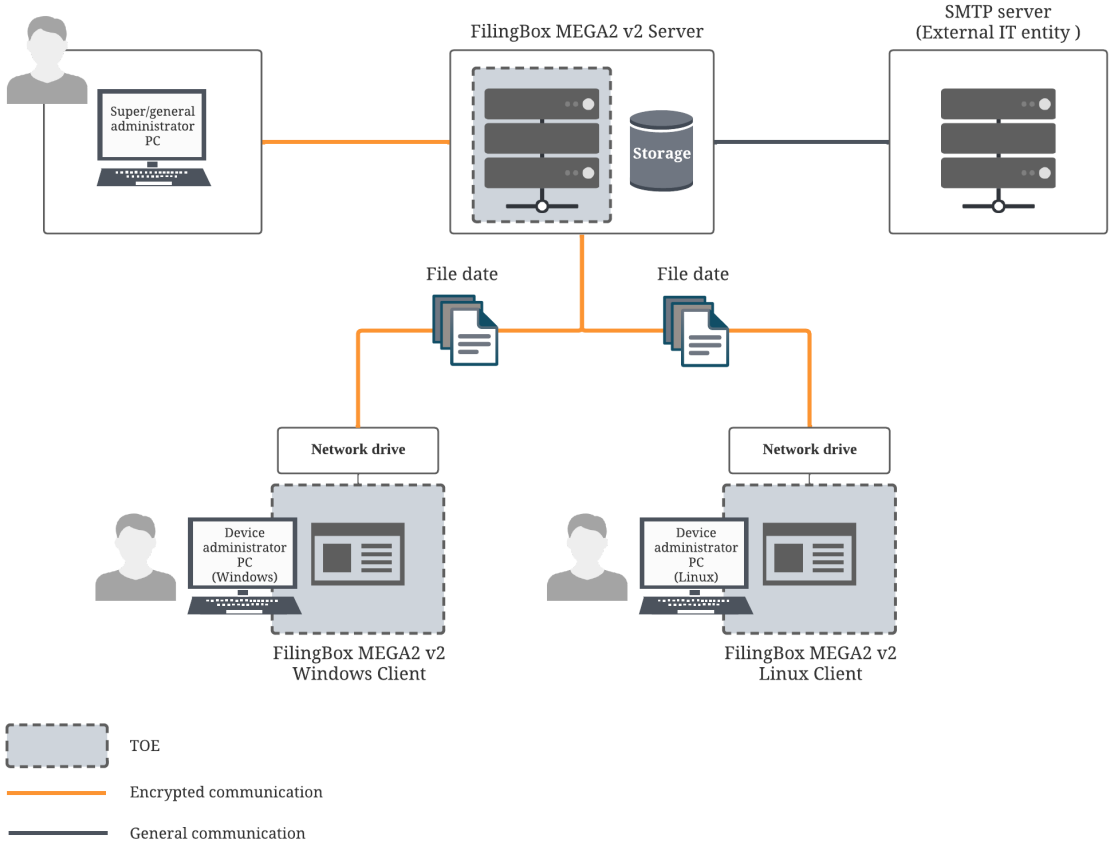
Among the TOE components, the main security features of the FilingBox MEGA2 v2 Linux Client and FilingBox MEGA2 v2 Windows Client include a security audit feature that transmits audit data to the FilingBox MEGA2 v2 Server when an auditable event occurs within those components, cryptographic support features for encryption used in communication protection with the FilingBox MEGA2 v2 Server, identification and authentication features that request user identification and authentication, security management features that manage allowed applications, and TSF protection features that include TSF self-test and integrity verification.

1.3.1 Non-TOE and TOE operational environment

The illustration below [Figure 1-1] shows the environment in which the TOE operates. The TOE is comprised of the FilingBox MEGA2 v2 Server, and the FilingBox MEGA2 v2 Windows Client and FilingBox MEGA2 v2 Linux Client, which are installed on PCs based on Windows and Linux, respectively.

The super administrator and general administrator perform identification and authentication through the administrator web UI using a web browser from a PC assigned with an allowed IP address, after which they conduct security management. The device administrator sets the application policy that allows access to the data of the files to be protected on PCs where the FilingBox MEGA2 v2 Windows Client and FilingBox MEGA2 v2 Linux Client are installed.

Only through allowed applications can the data of the files to be protected be stored and accessed in the storage managed by the FilingBox MEGA2 v2 Server.



[Figure 1-1] TOE operational environment

1.3.2 Non-TOE hardware/software required by the TOE.

The minimum software and hardware specifications required for the operation of the TOE are as shown in [Table 1-1] below.

FilingBox MEGA2 v2 Server	CPU	Intel(R) Core(TM) i5-13400 CPU @ 2.50 GHz or above
	RAM	16 GB or more
	SSD	At least 10 GB of space required for TOE installation
	NIC	100/1000 Mbps X 1 Port or above
	OS	Rocky Linux 8.8 64-bit (Kernel 4.18.0-477.10.1)
	S/W	MariaDB 10.11.5
		Tomcat 9.0.85
		OpenJDK 1.8.0_382
		NGINX 1.24.0
FilingBox MEGA2 v2 Windows Client	CPU	Intel(R) Core(TM) i5-7600 CPU @ 3.5 GHz or above
	RAM	8 GB or more
	SSD	At least 10 GB of space required for TOE installation
	NIC	100/1000 Mbps X 1 Port or above
	OS	Windows Server 2016 64-bit Version 1607, OS Build 14393.693
FilingBox MEGA2 v2 Linux Client	CPU	Intel(R) Core(TM) i5-13400 CPU @ 2.50 GHz or above
	RAM	16 GB or more
	SSD	At least 10 GB of space required for TOE installation
	NIC	100/1000 Mbps X 1 Port or above
	OS	Rocky Linux 8.8 64-bit (Kernel 4.18.0-477.10.1)

[Table 1-1] Minimum software/hardware specifications required for TOE operation

Web browser specifications for super/general administrators to perform security management: Chrome 120.0 (64bit)

The external IT entity required for the operation of the TOE are as shown in [Table 1-2] below.

SMTP server	Sends alert emails to authorized administrators when a potential security breach is detected.

[Table 1-2] External IT entity required for TOE operation

1.4 TOE description

1.4.1 Physical scope of the TOE

The TOE package is distributed in the form as shown in [Table 1-3] for the physical scope.

TOE	FilingBox MEGA2 v2		
Version	v2.6.0		
Category	Name and Filename	Type	Distribution Form
TOE components	FilingBox MEGA2 v2 Server v2.2.0 (FilingBox MEGA2_v2_Server_v2.2.0.tgz)	S/W	CD
	FilingBox MEGA2 v2 Windows Client v2.2.0 (FilingBox MEGA2_v2_Windows_Client_v2.2.0.exe)		
	FilingBox MEGA2 v2 Linux Client v2.2.0 (FilingBox MEGA2_v2_Linux_Client_v2.2.0.tgz)		
Documentation	FilingBox MEGA2 v2 Server User Manual v1.3 (FilingBox MEGA2 v2 Server User Manual v1.3.pdf)	PDF	
	FilingBox MEGA2 v2 Client User Manual v1.3 (FilingBox MEGA2 v2 Client User Manual v1.3.pdf)		
	FilingBox MEGA2 v2 Server Installation Manual v1.4 (FilingBox MEGA2 v2 Server Installation Manual v1.4.pdf)		
	FilingBox MEGA2 v2 Client Installation Manual v1.4 (FilingBox MEGA2 v2 Client Installation Manual v1.4.pdf)		

[Table 1-3] TOE physical scope

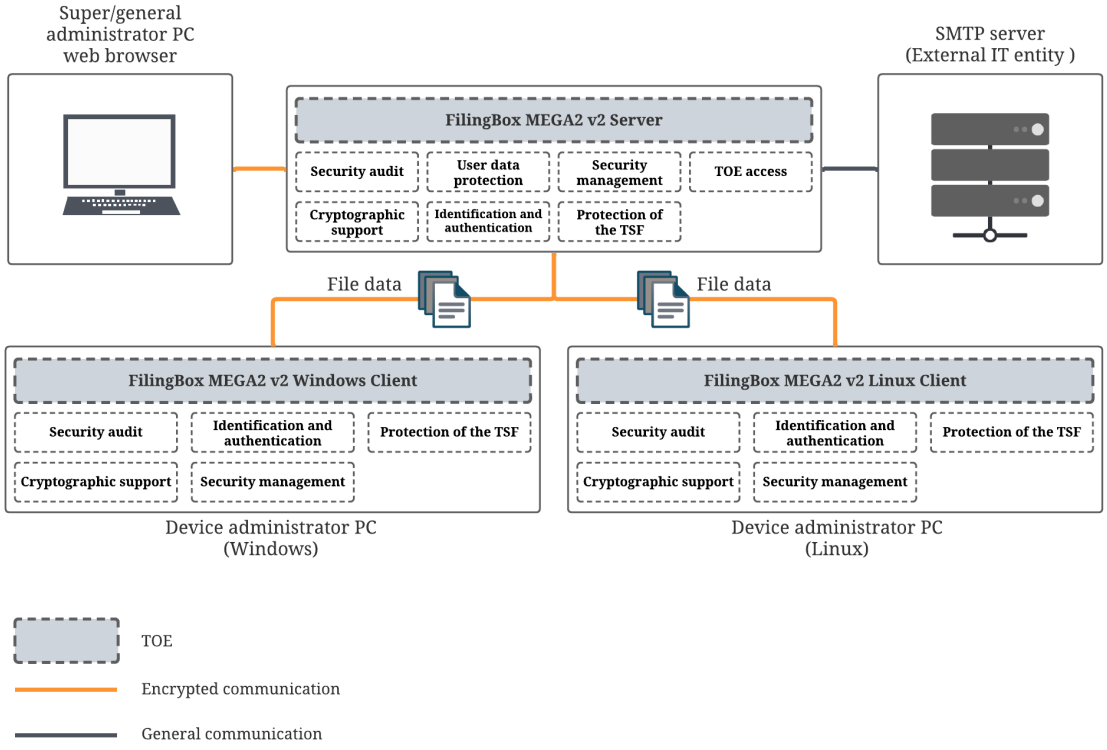
The 3rd party software included in the TOE is as follows in [Table 1-4].

FilingBox MEGA2 v2 Server	OpenSSL 3.0.13	TSF data encryption, communication channel encryption
FilingBox MEGA2 v2 Windows Client	Microsoft Visual C++ 2015-2022 Redistributable (x64) 14.38	Library for running Windows programs
	Callback File System 6.1	File system control library
	OpenSSL 3.0.13	Communication channel encryption
FilingBox MEGA2 v2 Linux Client	lsof 4.93.2	Changes the process ID value that requested file I/O to the actual application's name and path information
	Fuse 2.9.7	Supports file I/O events occurring in the kernel
	OpenSSL 3.0.13	Communication channel encryption

[Table 1-4] 3rd party software required for TOE operation

1.4.2 Logical scope of the TOE

The illustration below [Figure 1-2] shows the logical scope of the TOE.



[Figure 1-2] TOE logical scope

Main features of FilingBox MEGA2 v2 Server

[Security audit]

FilingBox MEGA2 v2 Server sends alert emails to administrators when a potential security violation occurs. Potential violations include administrator authentication failures, self-test result failures, integrity breaches, and predictions of audit data loss. An audit record containing basic information (date/time, type, result, etc.) is created whenever an auditable event occurs, including network drive connections/disconnections, server logins/logouts, etc. The audit events also include the subjects that caused them. Authorized administrators can access and read all audit data, presented in a user-friendly format. Audit data can be searched based on type, code, event name, event description, and date. Except for the event description, items such as type, code, and event name can be sorted alphabetically, and dates can be sorted chronologically in ascending or descending order. Alert emails

are sent to administrators when audit storage usage exceeds 70%, 80%, and 90%, and when audit storage is 100% full, the oldest audit records are overwritten, and alert emails are sent.

[Cryptographic support]
The DEK (Data Encryption Key) generated by the FilingBox MEGA2 v2 Server uses the HASH_DRBG algorithm, and the KEK (Key Encryption Key) is generated using the PBKDF2-HMAC-SHA256 algorithm. AES_128_CBC algorithm is used for encrypting/decrypting cryptographic keys, stored configuration values in DBMS, private key passwords, SMTP passwords, and DBMS connection information. SHA256 algorithm is used for administrator password encryption and integrity verification. Communication between FilingBox MEGA2 v2 Server and FilingBox MEGA2 v2 Windows/Linux Client is protected using Open SSL based on TLS1.2. Cryptographic keys generated or used by the TOE are securely destroyed by overwriting them with zeros in memory.

[User data protection]
Applications allowed to access data in files within the storage protected by the FilingBox MEGA2 v2 Server are registered through the FilingBox MEGA2 v2 Windows Client and FilingBox MEGA2 v2 Linux Client, with access paths and read-only/read-write permissions. Only permitted applications can access and read/write the data of files in the storage protected by the FilingBox MEGA v2 Server.

[Identification and authentication]
FilingBox MEGA2 v2 Server enforces a rule for administrator password creation, combining lowercase letters, uppercase letters, numbers, and special characters ($!@%*#?&) to create passwords between 10 and 20 characters long. After 5 consecutive authentication failures, login is blocked for 5 minutes, which can be lifted by an authorized super administrator or automatically after 5 minutes. All security features require administrator identification and authentication. During authentication, substitute characters (●) are displayed instead of the actual password, and feedback for failed authentication attempts only provides the result of the failure. A random value is utilized in order to prevent the reuse of authentication data.

[Security management]
FilingBox MEGA2 v2 Server provides initial setup for setting up the first administrator's ID and password at the first connection. It offers authorized administrators security management features such as granting administrator privileges, setting administrator passwords, unlocking administrator logins, ending existing administrator sessions, setting access IP for the administrator web UI, and querying permitted applications. Administrators can be set with different levels of access: super administrator access to all menus (devices, administrators, audit logs, and settings), general administrator access to devices and audit logs (excluding the administrators and settings), and device

administrator managing permitted applications through FilingBox MEGA2 v2 Windows Client and FilingBox MEGA2 v2 Linux Client.

[Protection of the TSF]
FilingBox MEGA2 v2 Server encrypts communication channels, cryptographic keys, administrator passwords, configuration values, and SMTP account passwords to ensure their protection. Self-tests and integrity verifications are conducted to confirm correct operation. Self-tests are performed at startup and periodically during regular operation, while integrity verifications occur at startup, periodically during normal operation, and upon authorized administrator request.

[TOE access]
FilingBox MEGA2 v2 Server limits the number of concurrent sessions for administrators with the same or hierarchical roles to a maximum of one. If an administrator is inactive for 10 minutes, their session is automatically terminated. Administrators can only connect from registered IP addresses.

Main features of FilingBox MEGA2 v2 Windows Client and FilingBox MEGA2 v2 Linux Client

[Security audit]

FilingBox MEGA2 v2 Windows Client and FilingBox MEGA2 v2 Linux Client create an audit record containing the date/time, type, and result of the event whenever an auditable event occurs and transmit it to the FilingBox MEGA2 v2 Server. These events include network drive connections/disconnections, registration/deletion of allowed applications, etc.

[Cryptographic support]

Integrity verification for FilingBox MEGA2 v2 Windows Client and FilingBox MEGA2 v2 Linux Client uses the SHA256 algorithm, and data communicated with the FilingBox MEGA2 v2 Server is protected based on TLS1.2.

[Identification and authentication]

During the authentication process, FilingBox MEGA2 v2 Windows Client and FilingBox MEGA2 v2 Linux Client display substitute characters (●) instead of passwords and provide only the result of the failed authentication attempts. When setting a device administrator's password, a combination of lowercase letters, uppercase letters, numbers, and special characters ($!@%*#?&) is enforced, creating a password between 9 and 20 characters long. After 5 consecutive authentication failures, login is blocked for 5 minutes, which can be lifted by an authorized super administrator or automatically after 5 minutes. A random value is utilized in order to prevent the reuse of authentication data.

[Security management]

FilingBox MEGA2 v2 Windows Client and FilingBox MEGA2 v2 Linux Client provide device administrators with application management functions.

[Protection of the TSF]

FilingBox MEGA2 v2 Windows Client and FilingBox MEGA2 v2 Linux Client protect the communication channel with the FilingBox MEGA2 v2 Server through encryption. Self-tests and integrity verifications are conducted to confirm correct operation, performed at startup, periodically during normal operation, and upon authorized administrator request.

1.5 Conventions

The notation, formatting and conventions used in this ST are consistent with the Common Criteria for Information Technology Security Evaluation.

The CC allows several operations to be performed for functional requirements: iteration, assignment, selection and refinement. Each operation is used in this ST.

Iteration

Iteration is used when a component is repeated with varying operations. The result of iteration is marked with an iteration number in parenthesis following the component identifier, i.e., denoted as (iteration No.).

Assignment

This is used to assign specific values to unspecified parameters (e.g., password length). The result of assignment is indicated in square brackets like [assignment_value].

Selection

This is used to select one or more options provided by the CC in stating a requirement. The result of selection is shown as *underlined and italicized*.

Refinement

This is used to add details and thus further restrict a requirement. The result of refinement is shown in **bold text**.

1.6 Terms and definitions

Assignment

The specification of an identified parameter in a component (of the CC) or requirement

Authorized Administrator

Authorized user to securely operate and manage the TOE

Class

Set of CC families that share a common focus

Component

Smallest selectable set of elements on which requirements may be based

Dependency

Relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package

Element

Indivisible statement of a security need

Encryption

The act that converting the plaintext into the ciphertext using the encryption key

Evaluation Assurance Level (EAL)

Set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package

External Entity

An entity (person or IT system) outside the TOE that interacts or may interact with the TOE

Family

Set of components that share a similar goal but differ in emphasis or rigo

Identity

Representation uniquely identifying entities (e.g., user, process or disk) within the context of the TOE

Iteration

Use of the same component to express two or more distinct requirements

Operation (on a component of the CC)

Modification or repetition of a component. Allowed operations on components are assignment, iteration, refinement and selection

Operation (on a subject)

Specific type of action performed by a subject on an object

Protection Profile (PP)

Implementation-independent statement of security needs for a TOE type

Refinement

Addition of details to a component

Role

Predefined set of rules on permissible interactions between a user and the TOE

Security Target (ST)

Implementation-dependent statement of security needs for a specific identified TOE

Selection

Specification of one or more items from a list in a component

Subject

Active entity in the TOE that performs operations on objects

Target of Evaluation (TOE)

Set of software, firmware and/or hardware possibly accompanied by guidance

TOE Security Functionality (TSF)

Combined functionality of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs

TSF Data

Data for the operation of the TOE upon which the enforcement of the SFR relies

1.7 ST organization

1) Chapter 1 introduces to the ST, providing ST references and the TOE overview.

2) Chapter 2 provides the conformance claims to the CC and package; and describes the claim's conformance rationale.

3) Chapter 3 describes the security objectives for the operational environment.

4) Chapter 4 defines the extended components for this ST.

5) Chapter 5 describes the security functional and assurance requirements.

6) Chapter 6 describes how the security functional requirements are implemented within the TOE.

2 Conformance claims

2.1 CC conformance claim

This ST conforms to the following CC.

CC identification

Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model, Version 3.1, Revision 5 (CCMB-2017-04-001, April, 2017)

Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components, Version 3.1, Revision 5 (CCMB-2017-04-002, April, 2017)

Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components, Version 3.1, Revision 5 (CCMB-2017-04-003, April, 2017)

Conformance claim

Part 2 Security Functional Components extended: FCS_RGB.1, FMT_PWD.1, and FPT_PST.1

Part 3 Security Assurance Components: Conformant

2.2 PP Conformance claim

There is no PP that this ST complies with.

2.3 Package conformance claim

This ST claims conformance to assurance package EAL1.

2.4 Conformance claim rationale

Since this ST does not claim conformance to other PPs, it is not necessary to describe the conformance claim rationale.

3 Security objectives

3.1 Security objectives for the operational environment

The followings are the security objectives handled by technical and procedural method supported from operational environment in order to provide the TOE security functionality accurately.

Definition	Description
OE.PHYSICAL_CONTROL	The place where the management server among the TOE components are installed and operated shall be equipped with access control and protection facilities so that only authorized administrator can access.
OE.TRUSTED_ADMIN	The authorized administrator of the TOE shall be non-malicious users, have appropriately trained for the TOE management functions and accurately fulfill the duties in accordance with administrator guidances.
OE.OPERATION_SYSTEM_REINFORCEMENT	The authorized administrator of the TOE shall ensure the reliability and security of the operating system by performing the reinforcement on the latest vulnerabilities of the operating system in which the TOE is installed and operated.
OE.TIMESTAMP	The TOE shall accurately record security-related events using reliable timestamps provided by the TOE operational environment.
OE.TRUSTED_EXTERNAL_SERVER	The SMTP and OS interacting with the TOE shall ensure safe and trusted operations.
OE.LOG_BACKUP	The authorized administrator shall periodically checks a spare space of audit data storage in case of the audit data loss, and carries out the audit data backup (external log server or separate storage device, etc.) to prevent audit data loss.
OE.DBMS	Audit data shall be stored in a DBMS that operates in a physically secure environment.
OE.ADMIN_ACCESS	The communication between the administrator PC's web browser and the web server, which is the operational environment of the management server, shall ensure the confidentiality and integrity of the transmitted data.

4 Extended components definition

4.1 Cryptographic support

4.1.1 Random bit generation

Family Behaviour

This family defines requirements for the TSF to provide the capability that generates random bits required for TOE cryptographic operation.

Component levelling

FCS_RBG.1 random bit generation, requires TSF to provide the capability that generates random bits required for TOE cryptographic operation.

Management: FCS_RBG.1

There are no management activities foreseen.

Audit: FCS_RBG.1

There are no auditable events foreseen.

FCS_RBG.1 Random bit generation

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RBG.1.1 The TSF shall generate random bits required to generate a cryptographic key using the specified random bit generator that meets the following [assignment: *list of standards*].

4.2 Security Management

4.2.1 ID and password

Family Behaviour

This family defines the capability that is required to control ID and password management used in the TOE, and set or modify ID and/or password by authorized users.

Component levelling

FMT_PWD.1 ID and password management, requires that the TSF provides the management function of ID and password.

Management: FMT_PWD.1

The following actions could be considered for the management functions in FMT:

a) Management of ID and password configuration rules.

Audit: FMT_PWD.1

The following actions are recommended to record if FAU_GEN Security audit data generation is included in the ST:

a) Minimal: All changes of the password.

FMT_PWD.1 Management of ID and password

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_PWD.1.1 The TSF shall restrict the ability to manage the password of [assignment: *list of functions*] to [assignment: *the authorized identified roles*].

1. [assignment: *password combination rules and/or length*]
2. [assignment: *other management such as management of special characters unusable for password, etc.*]

FMT_PWD.1.2 The TSF shall restrict the ability to manage the ID of [assignment: *list of functions*] to [assignment: *the authorized identified roles*].

1. [assignment: *ID combination rules and/or length*]
2. [assignment: *other management such as management of special characters unusable for ID, etc.*]

FMT_PWD.1.3 The TSF shall provide the capability for [selection, choose one of: *setting ID and password when installing, setting password when installing, changing the ID and password when the authorized administrator accesses for the first time, changing the password when the authorized administrator accesses for the first time*].

4.3 Protection of the TSF

4.3.1 Protection of stored TSF data

Family Behaviour

This family defines rules to protect TSF data stored within containers controlled by the TSF from the unauthorized modification or disclosure.

Component levelling

FPT_PST.1 Basic protection of stored TSF data requires the protection of TSF data stored in containers controlled by the TSF.

Management: FPT_PST.1

There are no management activities foreseen.

Audit: FPT_PST.1

There are no auditable events foreseen.

FPT_PST.1 Basic protection of stored TSF data

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PST.1.1 The TSF shall protect [assignment: *TSF data*] stored in containers controlled by the TSF from the unauthorized [selection: *disclosure, modification*].

5 Security requirements

The security requirements specify security functional requirements and assurance requirements that must be satisfied by the TOE.

5.1 Security functional requirements

The security functional requirements included in this ST are derived from CC Part 2 and Chapter 4 Extended Components Definition.

Security functional class	Security functional component	
FAU	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
FCS	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
	FCS_RBG.1 (Extended)	Random bit generation
FDB	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
FIA	FIA_AFL.1	Authentication failure handling
	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
FMT	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_PWD.1 (Extended)	Management of ID and password
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
FPT	FPT_ITT.1	Basic internal transfer protection
	FPT_PST.1 (Extended)	Basic protection of stored TSF data
	FPT_TST.1	TSF testing

FTA	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions
	FTA_SSL.3	TSF-initiated termination
	FTA_TSE.1	TOE session establishment

[Table 5-1] Security functional requirements

5.1.1 Security audit

FAU_ARP.1 Security alarms

Hierarchical to: No other components.
Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall take [sending alert emails to the registered administrator's email address] upon detection of a potential security violation.

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps

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

a) Start-up and shutdown of the audit functions;
b) All auditable events for the [*not specified*] level of audit; and
c) [Auditable events in [Table 5-2]]

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 (if applicable), 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 ST, [Other audit relevant information in [Table 5-2]].

Security functional component	Auditable event	Other audit relevant information
FAU_ARP.1	Actions taken due to potential security violations	
FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms,	

	Automated responses performed by the tool	
FAU_STG.3	Actions taken due to exceeding of a threshold	
FAU_STG.4	Actions taken due to the audit storage failure	
FDP_ACF.1	Successful requests to perform an operation on an object covered by the SFP	Identity information of object
FIA_AFL.1	the reaching of the threshold for the unsuccessful authentication attempts and the actions taken and the subsequent, if appropriate, restoration to the normal state	
FIA_UAU.2	All use of the authentication mechanism	
FIA_UAU.4	Attempts to reuse authentication data	
FIA_UID.2	All use of the user identification mechanism, including the user identity provided.	
FMT_MOF.1	All modifications in the behaviour of the functions in the TSF	
FMT_MSA.1	All modifications of the values of security attributes	
FMT_MSA.3	Modifications of the default setting of permissive or restrictive rules, All modifications of the initial values of security attributes	
FMT_MTD.1	All modifications to the values of TSF data.	Modified TSF data
FMT_PWD.1	All changes of the password	
FMT_SMF.1	Use of the management functions	
FMT_SMR.1	Modifications to the group of users that are part of a role	
FPT_TST.1	Execution of the TSF self tests and the results of the tests	Modified TSF data or execution code in case of integrity violation
FTA_MCS.2	Rejection of a new session based on the limitation of multiple concurrent sessions	
FTA_SSL.3	Termination of an interactive session by the session locking mechanism.	
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism.	

[Table 5-2] Auditable events

FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [authentication failures (FIA_UAU.2) among auditable events, self-test result failures (FPT_TST.1) among auditable events, integrity violations, and the sending of alert emails due to FAU_STG.3 and FAU_STG.4] known to indicate a potential security violation;
b) [none]

FAU_SAR.1 Audit review

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [the following authorised administrator] with the capability to read [all the audit data] from the audit records.

[
a) Super adminitrator
b) General adminitrator
]

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

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.
Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [methods of selection and ordering of audit data items in [Table 5-3]] of audit data based on [the following criteria with logical relations].

Audit data items	Selection (All AND / All OR)	Ordering (Ascending / Descending)
Type	○	○
Code	○	○
Event name	○	○
Event description	○	X
Date	○	○

[Table 5-3] Methods of selection and ordering of audit data items

FAU_STG.3 Action in case of possible audit data loss

Hierarchical to: No other components.
Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall [send an alert email to the registered administrator's email address once for each threshold range] if the audit trail exceeds [70%, 80%, 90% of the allocated capacity for audit data].

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss
Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall *overwrite the oldest stored audit records* and [send an authorised administrator an alert email] if the audit trail is full.

5.1.2 Cryptographic support

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.
Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Algorithm in [Table 5-4]] and specified cryptographic key sizes [Key size in [Table 5-4]] that meet the following: [Standard in [Table 5-4]].

Standard	Algorithm	Key size	Purpose
NIST SP 800-90A Rev.1	HASH_DRBG	128 bits	Generation of DEK (Data Encryption Key)
NIST Special Publication 800-132	PBKDF2_HMAC_SHA256	256 bits	Generation of KEK (Key Encryption Key)
ISO/IEC 18033-2:2006	RSA 2048	2048 bits	Asymmetric key for authentication during TLS1.2 communication
ISO/IEC 18033-2:2006	ECDHE	520 bits	Key establishment during TLS1.2 communication

[Table 5-4] Cryptographic key generation

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [Cryptographic key destruction method in [Table 5-5]] that meets the following: [none].

Target	Cryptographic key destruction method	Destruction timing
DEK(Data Encryption Key)	Overwrite with zeros 3 times in memory	At process termination
KEK(Key Encryption Key)	Overwrite with zeros 3 times in memory	Immediately after use
Keys used during TLS1.2 communication	Overwrite with zero once in memory	At session termination

[Table 5-5] Cryptographic key destruction

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [Purpose in [Table 5-6]] in accordance with a specified cryptographic algorithm [Algorithm in [Table 5-6]] and cryptographic key sizes [Key size in [Table 5-6]] that meet the following: [Standard in [Table 5-6]].

Standard	Algorithm	Key size	Purpose
ISO/IEC 29167-10:2017	AES_128_CBC	128 bits	Encryption and decryption of DEK (Data Encryption Key)
			Encryption and decryption of private key passwords
			Encryption and decryption of DBMS access information
			Encryption and decryption of SMTP passwords
RFC 5289	AES_256_GCM	256 bits	Encryption and decryption of communication data between TOE components (TLS1.2 communication)
ISO/IEC 10118-3:2004	SHA256 + Salt	256 bits	Storage and comparison of administrator passwords
	SHA256		Integrity verification of TOE
	SHA384	384 bits	Integrity verification of communication data between TOE components

[Table 5-6] Cryptographic operations

FCS_RBG.1 Random bit generation (Extended)

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RBG.1.1 The TSF shall generate random bits required to generate a cryptographic key using the specified random bit generator that meets the following [Standard in [Table 5-7]].

Standard	Algorithm
NIST SP 800-90A Rev.1	HASH_DRBG

[Table 5-7] Random bit generation

5.1.3 User data protection

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [file data access control] on [the following subjects, objects, and their operations].

[

a) Subjects: Devices

b) Objects: File data stored and protected in the TOE

c) Operations : Reading and writing of file data

]

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [file data access control] to objects based on the following: [security attribute groups for the following subjects and objects].

[

a) Subjects: Devices

b) Subject's security attributes: Device's IP address, device's MAC address, device administrator ID, path of the executable file of the application running on the device, name of the executable file, hash value of the executable file

c) Objects: File data stored and protected in the TOE

d) Object's security attributes: path to the storage that the application can access

]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [The TSF shall enforce rules that allow an operation to be performed only if the subject's security attributes are included in the object's access-permitted security attributes, and the operation matches the object's operation security attributes.].

FDP_ACF.1.3 The TSF shall explicitly authorise 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]

5.1.4 Identification and authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [*5*] unsuccessful authentication attempts occur related to [administrator authentication].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall [perform the following actions].

[

a) Display an authentication failure message on the authentication screen and block authentication for 5 minutes.

b) The authentication block is lifted after 5 minutes or when the super administrator lifts the block.

]

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [the following permitted criteria].

[

a) Length of at least 10 characters and a maximum of 20 characters (For device administrators changing passwords on the client, a minimum of 9 characters and a maximum of 20 characters).

b) At least one uppercase letter, one lowercase letter, one digit, and one special character ($!@%*#?&).

c) Prohibition of three consecutive identical characters or numbers (For device administrators changing passwords on the client, prohibition of two consecutive identical characters or numbers).

d) Prohibition of sequential input of adjacent keyboard characters or numbers.

e) Prohibition of reusing the immediately preceding password.

]

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication
Dependencies: FIA_UID.1 Timing of identification

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

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [the following authentication mechanisms].

Category	Authentication mechanism
Super/general administrator authentication	Ensure the uniqueness of a random value per session
Device administrator authentication	Ensure the uniqueness of a random value per session

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [the following feedback] to the user while the authentication is in progress.

[
a) Substitute characters (●) for the entered password
b) Only the result of the failure without the cause when authentication fails
]

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification
Dependencies: No dependencies.

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

5.1.5 Security management

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to *manage the behaviour of* the functions [listed in [Table 5-8]] to [the administrator roles specified in [Table 5-8]].

Security function	Super administrator				General administrator				Device administrator			
	A: Determine the behaviour of, B: Disable, C: Enable, D: Modify the behaviour of											
	A	B	C	D	A	B	C	D	A	B	C	D
Device management	X	X	○	X	X	X	○	X	X	X	X	X
Administrator management	X	X	○	X	X	X	X	X	X	X	X	X
Administrator privilege granting	X	X	○	X	X	X	X	X	X	X	X	X
Administrator Password Reset	X	X	○	X	X	X	X	X	X	X	X	X
Login Unlock	X	X	○	X	X	X	X	X	X	X	X	X
Admin web UI access IP address management	X	X	○	X	X	X	X	X	X	X	X	X
SMTP server connection management	X	X	○	X	X	X	X	X	X	X	X	X
Alert email recipient address management	X	X	○	X	X	X	X	X	X	X	X	X
Client integrity verification baseline Management	X	X	○	X	X	X	X	X	X	X	X	X
Allowed application management	X	X	X	X	X	X	X	X	X	X	○	X

[Table 5-8] Abilities to manage of behaviour of security functions

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

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

FMT_MSA.1.1 The TSF shall enforce the [file data access control] to restrict the ability to *change_default, query, modify, delete* the security attributes [listed in [Table 5-9]] to [the administrator roles specified in [Table 5-9]].

Security attribute	Super administrator				General administrator				Device administrator			
	A: Change_default, B: Query, C: Modify, D: Delete											
	A	B	C	D	A	B	C	D	A	B	C	D
Device IP address	○	○	○	○	○	○	○	○	X	X	X	X
Device MAC address	○	○	○	○	○	○	○	○	X			
Device administrator ID	○	○	X	○	○	○	X	○	X	X	X	X
Application executable file path	X	○	X	X	X	○	X	X	○	○	○	○
Application executable file name	X	○	X	X	X	○	X	X	○	○	○	○
Executable file hash value	X	○	X	X	X	○	X	X	○	○	○	○
Storage path accessible by application	X	○	X	X	X	○	X	X	○	○	○	○
File data reading and writing	X	○	X	X	X	○	X	X	○	○	○	○

[Table 5-9] Abilities to change default, query, modify, delete security attributes

※ In the case of the Linux Client, the device administrator cannot query the hash value of the executable file.

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [file data access control] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [administrator roles specified in [Table 5-10]] to specify alternative initial values to override the default values when an object or information is created.

Security attribute	Super administrator	General administrator	Device administrator
Device IP address	○	○	X
Device MAC address	○	○	X
Device administrator ID	○	○	X
Application executable file path	X	X	○
Application executable file name	X	X	○
Executable file hash value	X	X	○
Storage path accessible by application	X	X	○
File data reading and writing	X	X	○

[Table 5-10] Permissions to specify alternative initial values for security attributes

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [*manage*] the [following list of TSF data] to [the authorised administrator roles].

TSF data	Super administrator	General administrator	Device administrator
Device identification information	○	○	X
Administrator identification and authentication information	○	X	X
Administrator privileges	○	X	X
Audit logs	○	○	X
Admin web UI access IP address	○	X	X
SMTP server connection information	○	X	X
Alert email recipient address	○	X	X
Client integrity verification baseline	○	X	X
Allowed application information	○	○	○

[Table 5-11] Abilities to manage TSF data

FMT_PWD.1 Management of ID and password (Extended)

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_PWD.1.1 The TSF shall restrict the ability to manage the password of [none] to [none].

1. [none]
2. [none]

FMT_PWD.1.2 The TSF shall restrict the ability to manage the ID of [none] to [none].

1. [none]
2. [none]

FMT_PWD.1.3 The TSF shall provide the capability for *setting ID and password when installing*.

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

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

[

a) Security Function Management: As specified in FMT_MOF.1

b) Security Attribute Management: As specified in FMT_MSA.1

c) TSF Data Management: As specified in FMT_MTD.1

d) ID and Password Management: As specified in FMT_PWD.1

]

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [the following authorised identified roles].

[

a) Super administrator

b) General administrator

c) Device administrator

]

FMT_SMR.1.2 TSF shall be able to associate users and their **roles defined in FMT_SMR.1.1**.

5.1.6 Protection of the TSF

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITT.1.1 The TSF shall protect TSF data from *disclosure, modification* when it is transmitted between separate parts of the TOE.

FPT_PST.1 Basic protection of stored TSF data (Extended)

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PST.1.1 The TSF shall protect [the following TSF data] stored in containers controlled by the TSF from the unauthorized *disclosure, modification*.

[

a) Encryption key

b) TOE configuration values stored in DBMS

c) Private key password

d) SMTP password

e) Administrator passwords

f) DBMS access information

]

FPT_TST.1 TSF testing

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests *during initial start-up, periodically during normal operation* to demonstrate the correct operation of *the TSF*.

FPT_TST.1.2 The TSF shall provide **authorised administrators** with the capability to verify the integrity of *TSF data*.

FPT_TST.1.3 The TSF shall provide **authorised administrators** with the capability to verify the integrity of *TSF*.

5.1.7 TOE access

FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions

Hierarchical to: FTA_MCS.1 Basic limitation on multiple concurrent sessions
Dependencies: FIA_UID.1 Timing of identification

FTA_MCS.2.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same **super and general administrator** according to the rules [the maximum number of concurrent sessions for users with the same or hierarchical roles is limited to 1].

FTA_MCS.2.2 The TSF shall enforce, by default, a limit of [1] sessions per **super and general administrator**.

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.
Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [user inactivity period of 10 minutes for **super and general administrators**].

FTA_TSE.1 TOE session establishment

Hierarchical to: No other components.
Dependencies: No dependencies.

FTA_TSE.1.1 The TSF shall be able to deny **management access session** establishment based on [the connecting IP address].

5.2 Security assurance requirements

Assurance requirements of this ST are comprised of assurance components in CC part 3, and the evaluation assurance level is EAL1+. The following [Table 5-12] summarizes assurance components.

Security assurance class	Security assurance component	
Security Target evaluation	ASE_INT.1	ST introduction
	ASE_CCL.1	Conformance claims
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_ECD.1	Extended components definition
	ASE_REQ.1	Stated security requirements
	ASE_TSS.1	TOE summary specification
Development	ADV_FSP.1	Basic functional specification
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_IND.1	Independent testing - conformance
Vulnerability assessment	AVA_VAN.1	Vulnerability survey

[Table 5-12] Security assurance requirements

5.2.1 Security Target evaluation

ASE_INT.1 ST introduction

Dependencies

No dependencies.

Developer action elements

ASE_INT.1.1D The developer shall provide an ST introduction.

Content and presentation elements

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall uniquely identify the TOE.

ASE_INT.1.4C The TOE overview shall summarise the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

Evaluator action elements

ASE_INT1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_INT1.2E The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

ASE_CCL.1 Conformance claims

Dependencies

ASE_INT.1 ST introduction

ASE_ECD.1 Extended components definition

ASE_REQ.1 Stated security requirements

Developer action elements

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

Content and presentation elements

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

Evaluator action elements

ASE_CCL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_OBJ.1 Security objectives for the operational environment

Dependencies

No dependencies.

Developer action elements

ASE_OBJ.1.1D The developer shall provide a statement of security objectives.

Content and presentation elements

ASE_OBJ.1.1C The statement of security objectives shall describe the security objectives for the operational environment.

Evaluator action elements

ASE_OBJ.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1 Extended components definition

Dependencies

No dependencies.

Developer action elements

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

Content and presentation elements

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

Evaluator action elements

ASE_ECD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence

ASE_ECD.1.2E The evaluator shall confirm that no extended component can be clearly expressed using existing components.

ASE_REQ.1 Stated security requirements

Dependencies

ASE_ECD.1 Extended components definition

Developer action elements

ASE_REQ.1.1D The developer shall provide a statement of security requirements.

ASE_REQ.1.2D The developer shall provide a security requirements rationale.

Content and presentation elements

ASE_REQ.1.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.1.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.1.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.1.4C All operations shall be performed correctly.

ASE_REQ.1.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.1.6C The statement of security requirements shall be internally consistent.

Evaluator action elements

ASE_REQ.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1 TOE summary specification

Dependencies

ASE_INT.1 ST introduction

ASE_REQ.1 Stated security requirements

ADV_FSP.1 Basic functional specification

Developer action elements

ASE_TSS.1.1D The developer shall provide a TOE summary specification

Content and presentation elements

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

Evaluator action elements

ASE_TSS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1.2E The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

5.2.2 Development

ADV_FSP.1 Basic functional specification

Dependencies

No dependencies.

Developer action elements

ADV_FSP.1.1D The developer shall provide a functional specification.

ADV_FSP.1.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements

ADV_FSP.1.1C The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2C The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3C The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV_FSP.1.4C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification

Evaluator action elements

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.3 Guidance documents

AGD_OPE.1 Operational user guidance

Dependencies

ADV_FSP.1 Basic functional specification

Developer action elements

AGD_OPE.1.1D The developer shall provide operational user guidance.

Content and presentation elements

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that shall be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1 Preparative procedures

Dependencies

No dependencies.

Developer action elements

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Content and presentation elements

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements

AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.4 Life-cycle support

ALC_CMC.1 TOE Labelling of the TOE

Dependencies

ALC_CMS.1 TOE CM coverage

Developer action elements

ALC_CMC.11D The developer shall provide the TOE and a reference for the TOE.

Content and presentation elements

ALC_CMC.1.1C The TOE shall be labelled with its unique reference.

Evaluator action elements

ALC_CMC.1.1E The evaluator shall confirm that the information provided meet requirements for content and presentation of evidence.

ALC_CMS.1 TOE CM coverage

Dependencies

No dependencies.

Developer action elements

ALC_CMS.1.1D The developer shall provide a configuration list for the TOE

Content and presentation elements

ALC_CMS.1.1C The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2C The configuration list shall uniquely identify the configuration items.

Evaluator action elements

ALC_CMS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.5 Tests

ATE_IND.1 Independent testing - conformance

Dependencies

ADV_FSP.1 Basic functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Developer action elements

ATE_IND.1.1D The developer shall provide the TOE for testing.

Content and presentation elements

ATE_IND.1.1C The TOE shall be suitable for testing.

Evaluator action elements

ATE_IND.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.2.6 Vulnerability assessment

AVA_VAN.1 Vulnerability survey

Dependencies

ADV_FSP.1 Basic functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Developer action elements

AVA_VAN.1.1D The developer shall provide the TOE for testing.

Content and presentation elements

AVA_VAN.1.1C The TOE shall be suitable for testing.

Evaluator action elements

AVA_VAN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.1.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

5.3 Security requirements rationale

5.3.1 Dependency rationale of security functional requirements

The following [Table 5-13] demonstrates the dependency relationships of the TOE's security functional components.

AU_GEN.1 has a dependency on FPT_STM.1. However, since the TOE uses reliable timestamps provided by the TOE operational environment to accurately record security-related events, the dependency of FAU_GEN.1 is satisfied by the security objective for the operational environment, OE.TIMESTAMP, instead of FPT_STM.1.

FAU_STG.3 and FAU_STG.4 depend on FAU_STG.1. But since the TOE stores audit records in a physically secure DBMS provided by the TOE operational environment, the dependencies of FAU_STG.3 and FAU_STG.4 are met by the security objective for the operational environment, OE.DBMS, instead of FAU_STG.1.

FIA_AFL.1 and FIA_UAU.7 are dependent on FIA_UAU.1. However, these dependencies are satisfied by FIA_UAU.2, which is hierarchical to FIA_UAU.1.

FIA_UAU.2, FMT_SMR.1, and FTA_MCS.2 have dependencies on FIA_UID.1. These dependencies are met by FIA_UID.2, which is hierarchical to FIA_UID.1.

No.	Security functional requirements	Dependency	Reference No.
1	FAU_ARP.1	FAU_SAA.1	4
2	FAU_GEN.1	FPT_STM.1	OE.TIMESTAMP
3	FAU_SAA.1	FAU_GEN.1	2
4	FAU_SAR.1	FAU_GEN.1	2
5	FAU_SAR.3	FAU_SAR.1	4
6	FAU_STG.3	FAU_STG.1	OE.DBMS
7	FAU_STG.4	FAU_STG.1	OE.DBMS
8	FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	10 9
9	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	8
10	FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	8 9
11	FCS_RBG.1 (Extended)	-	-
12	FDP_ACC.1	FDP_ACF.1	13
13	FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	12 22
14	FIA_AFL.1	FIA_UAU.1	16
15	FIA_SOS.1	-	-
16	FIA_UAU.2	FIA_UID.1	19
17	FIA_UAU.4	-	-
18	FIA_UAU.7	FIA_UAU.1	16
19	FIA_UID.2	-	-
20	FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	25 26
21	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	12 25 26
22	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	21 26
23	FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	25 26
24	FMT_PWD.1 (Extended)	FMT_SMF.1 FMT_SMR.1	25 26
25	FMT_SMF.1	-	-
26	FMT_SMR.1	FIA_UID.1	19
27	FPT_ITT.1	-	-
28	FPT_PST.1 (Extended)	-	-
29	FPT_TST.1	-	-

30	FTA_MCS.2	FIA_UID.1	19
31	FTA_SSL.3	-	-
32	FTA_TSE.1	-	-

[Table 5-13] Dependency of security functional requirement

5.3.2 Dependency rationale of security assurance requirements

The dependency of EAL1 assurance package provided in the CC is already satisfied, the rationale is omitted.

6 TOE summary specification

6.1 Security audit

6.1.1 Audit data generation

The TOE records audit records (date/time of the event, event type, identity of the subject, event outcome, and other audit-related information) when the following auditable events occur. When generating audit data, the identity of the user who triggered the event is included in the audit record to correlate auditable events with user identity.

Security functional component	Auditable event	Other audit relevant information
FAU_ARP.1	Actions taken due to potential security violations	
FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms, Automated responses performed by the tool	
FAU_STG.3	Actions taken due to exceeding of a threshold	
FAU_STG.4	Actions taken due to the audit storage failure	
FDP_ACF.1	Successful requests to perform an operation on an object covered by the SFP	Identity information of object
FIA_AFL.1	the reaching of the threshold for the unsuccessful authentication attempts and the actions taken and the subsequent, if appropriate, restoration to the normal state	
FIA_UAU.2	All use of the authentication mechanism	
FIA_UAU.4	Attempts to reuse authentication data	
FIA_UID.2	All use of the user identification mechanism, including the user identity provided.	
FMT_MOF.1	All modifications in the behaviour of the functions in the TSF	
FMT_MSA.1	All modifications of the values of security attributes	
FMT_MSA.3	Modifications of the default setting of permissive or restrictive rules, All modifications of the initial values of security attributes	
FMT_MTD.1	All modifications to the values of TSF data.	Modified TSF data
FMT_PWD.1	All changes of the password	
FMT_SMF.1	Use of the management functions	

FMT_SMR.1	Modifications to the group of users that are part of a role	
FPT_TST.1	Execution of the TSF self tests and the results of the tests	Modified TSF data or execution code in case of integrity violation
FTA_MCS.2	Rejection of a new session based on the limitation of multiple concurrent sessions	
FTA_SSL.3	Termination of an interactive session by the session locking mechanism.	
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism.	

Related SFR FAU_GEN.1

6.1.2 Audit review

The audit records generated by the TOE are stored in a DBMS and are only accessible by super and general administrators for review. The audit record review function allows searching with 'AND' or 'OR' conditions across all records. Additionally, it provides functionalities to sort and view the records in ascending or descending order based on type, code, event name, and date.

Related SFR FAU_SAR.1, FAU_SAR.3

6.1.3 Potential violation analysis

When the TOE detects a potential security violation among audited events, it sends an alert email to the registered administrator's email address. Potential security violations include audit events of authentication failures, self-test result failures among auditable events, integrity violations, and the sending of alert emails based on predictions and prevention of audit log loss.

Related SFR FAU_ARP.1, FAU_SAA.1

6.1.4 Prevention of audit data loss

The TOE sends an alert email to the registered email address through the admin web UI only once for each threshold range when the allocated audit record storage, set for 1,700 events, exceeds the specified thresholds of 70%, 80%, and 90%. In the case of audit record storage saturation, the TOE should overwrite the oldest audit records and send an alert email through the admin web UI to the registered email address.

Related SFR FAU_STG.3, FAU_STG.4

6.2 Cryptographic support

6.2.1 Cryptographic key management and cryptographic operation

Category	Standard	Algorithm	Key size	Purpose
Cryptographic key generation	NIST SP 800-90A Rev.1	HASH_DRBG	128 bits	Generation of DEK (Data Encryption Key)
	NIST Special Publication 800-132	PBKDF2-HMAC-SHA256	256 bits	Generation of KEK (Key Encryption Key)
	ISO/IEC 18033-2:2006	RSA 2048	2048 bits	Asymmetric key for authentication during TLS1.2 communication
	ISO/IEC 18033-2:2006	ECDHE	520 bits	Key establishment during TLS1.2 communication

Category	Standard	Algorithm	Random bit generator Ffnction	Purpose
Random bit generation	NIST SP 800-90A Rev.1	HASH_DRBG	Provided by OpenSSL	Cryptographic key generation and salt creation

Category	Standard	Algorithm	Key size	Purpose
Cryptographic operation	ISO/IEC 29167-10:2017	AES_128_CBC	128 bits	Encryption and decryption of DEK (Data Encryption Key)
				Encryption and decryption of private key passwords
				Encryption and decryption of DBMS access information
				Encryption and decryption of SMTP passwords
	RFC 5289	AES_256_GCM	256 bits	Encryption and decryption of communication data between TOE components (TLS1.2 communication)
	ISO/IEC 10118-3:2004	SHA256 + Salt	256 bits	Storage and comparison of administrator passwords
		SHA256		Integrity verification of TOE
		SHA384	384 bits	Integrity verification of communication data between TOE components

Category	Target	Cryptographic key destruction method	Destruction timing
Cryptographic key destruction	DEK(Data Encryption Key)	Overwrite with zeros 3 times in memory	At process termination
	KEK(Key Encryption Key)	Overwrite with zeros 3 times in memory	Immediately after use
	Keys used during TLS1.2 communication	Overwrite with zero once in memory	At session termination

Related SFR FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FCS_RBG.1 (Extended)

6.3 User data protection

6.3.1 File data access control

Access to read and write operations on file data is only permitted when the security attributes of the subject are included in the object's access-permitted security attributes, and the operation matches the object's operation security attributes.

- Subject: device
- Subject's security attributes: Device's IP address, device's MAC address, device administrator ID, path of the executable file of the application running on the device, name of the executable file, hash value of the executable file
- Object: File data stored and protected in the TOE
- Object's security attributes: path to the storage that the application can access

Related SFR FDP_ACC.1, FDP_ACF.1

6.4 Identification and authentication

6.4.1 Identification and authentication

Before allowing any security function, user authentication and identification based on ID and password are performed, and failed authentication attempts are detected. When the number of failed authentication attempts reaches five, the authentication is blocked. If the super administrator does not lift the authentication block, it remains in place for five minutes.

The uniqueness of a random value per session is ensured for both super and general administrator authentication, as well as device administrator authentication, to prevent the reuse of authentication data.

During authentication, substitute characters (●) are displayed instead of the entered passwords. Only the result of the failure, excluding the cause, is provided when authentication fails.

Related SFR FIA_AFL.1, FIA_UAU.2, FIA_UAU.4, FIA_UAU.7, FIA_UID.2

6.4.2 Verification of secrets

Passwords are created according to the following rules:

- Length of at least 10 characters and a maximum of 20 characters (For device administrators changing passwords on the client, a minimum of 9 characters and a maximum of 20 characters).
- At least one uppercase letter, one lowercase letter, one digit, and one special character ($!@%*#?&).
- Prohibition of three consecutive identical characters or numbers (For device administrators changing passwords on the client, prohibition of two consecutive identical characters or numbers).
- Prohibition of sequential input of adjacent keyboard characters or numbers.
- Prohibition of reusing the immediately preceding password.

Related SFR FIA_SOS.1

6.5 Security management

6.5.1 Security management

The abilities to manage behaviour of security functions are limited for super administrators, general administrators, and device administrators as follows.

Security function	Super administrator			General administrator			Device administrator					
	A: Determine the behaviour of, B: Disable, C: Enable, D: Modify the behaviour of											
	A	B	C	A	B	C	A	B	C	A	B	C
Device management	X	X	○	X	X	X	○	X	X	X	X	X
Administrator management	X	X	○	X	X	X	X	X	X	X	X	X
Administrator privilege granting	X	X	○	X	X	X	X	X	X	X	X	X

Administrator Password Reset	X	X	○	X	X	X	X	X	X	X	X	X
Login Unlock	X	X	○	X	X	X	X	X	X	X	X	X
Admin web UI access IP address management	X	X	○	X	X	X	X	X	X	X	X	X
SMTP server connection management	X	X	○	X	X	X	X	X	X	X	X	X
Alert email recipient address management	X	X	○	X	X	X	X	X	X	X	X	X
Client integrity verification baseline Management	X	X	○	X	X	X	X	X	X	X	X	X
Allowed application management	X	X	X	X	X	X	X	X	X	X	○	X

The management abilities over TSF data are restricted as follows.

TSF data	Super administrator	General administrator	Device administrator
Device identification information	○	○	X
Administrator identification and authentication information	○	X	X
Administrator privileges	○	X	X
Audit logs	○	○	X
Admin web UI access IP address	○	X	X
SMTP server connection information	○	X	X
Alert email recipient address	○	X	X
Client integrity verification baseline	○	X	X

The abilities to change default values, query, modify, and delete security attributes for enforcing file data access control are limited as follows.

Security attribute	Super administrator				General administrator				Device administrator			
	A: Change_default, B: Query, C: Modify, D: Delete											
	A	B	C	D	A	B	C	D	A	B	C	D
Device IP address	○	○	○	○	○	○	○	○	X	X	X	X
Device MAC address	○	○	○	○	○	○	○	○	X			
Device administrator ID	○	○	X	○	○	○	X	○	X	X	X	X

Application executable file path	X	○	X	X	X	○	X	X	○	○	○	○
Application executable file name	X	○	X	X	X	○	X	X	○	○	○	○
Executable file hash value	X	○	X	X	X	○	X	X	○	○	○	○
Storage path accessible by application	X	○	X	X	X	○	X	X	○	○	○	○
File data reading and writing	X	○	X	X	X	○	X	X	○	○	○	○

※ In the case of the Linux Client, the device administrator cannot query the hash value of the executable file.

Super administrators, general administrators, and device administrators are permitted to specify alternative initial values to replace restrictive default values for the following security attributes.

Security attribute	Super administrator	General administrator	Device administrator
Device IP address	○	○	X
Device MAC address	○	○	X
Device administrator ID	○	○	X
Application executable file path	X	X	○
Application executable file name	X	X	○
Executable file hash value	X	X	○
Storage path accessible by application	X	X	○
File data reading and writing	X	X	○

During the installation process, a function is provided to set the ID and password of the super administrator when connecting from an IP address that is permitted access. Subsequently, authorized administrators are provided with role-specific management functionalities for security functions, security attributes, and TSF data.

Related SFR FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_PWD.1 (Extended), FMT_SMF.1,

6.6 Protection of the TSF

6.6.1 Protection of TSF data

When TSF data is transmitted between separated parts of the TOE, it must be protected using the TLS 1.2 protocol to prevent exposure and modification. The following cryptographic algorithms

protect encryption key, TOE configuration values stored in DBMS, private key password, SMTP password, administrator passwords, and DBMS access information from unauthorized exposure and modification.

TSF data	Standard	Algorithm	Key size
Encryption key	ISO/IEC 29167-10:2017	AES_128_CBC	128 bits
TOE configuration values stored in DBMS	ISO/IEC 29167-10:2017	AES_128_CBC	128 bits
Private key password	ISO/IEC 29167-10:2017	AES_128_CBC	128 bits
SMTP password	ISO/IEC 29167-10:2017	AES_128_CBC	128 bits
Administrator passwords	ISO/IEC 10118-3:2004	SHA256 + Salt	256 bits
DBMS access information	ISO/IEC 29167-10:2017	AES_128_CBC	128 bits

Related SFR FPT_ITT.1, FPT_PST.1 (Extended)

6.6.2 TSF testing

The TOE executes self-tests at start-up and periodically during regular operation to demonstrate the accurate operation of the TSF. Self-tests ensure that service components are functioning correctly and in the specified order. If any service is found abnormal during the self-test, all services are immediately terminated.

Additionally, the TOE provides a function to verify the integrity of TSF data and the TSF itself at start-up, periodically during normal operation, and upon requests from super and general administrators. Integrity verification is conducted through hash value comparisons of essential files such as configuration files, libraries, and executables using the following hash algorithm.

Standard	Algorithm
ISO/IEC 10118-3:2004	SHA256

Related SFR FPT_TST.1

6.7 TOE access

6.7.1 Management of sessions

After a super or general administrator logs into the admin web UI, the system must limit the maximum number of concurrent sessions when an administrator with the same or hierarchical roles successfully logs in.

Regardless of the administrator level, only one session is allowed for the admin web UI, and the maximum number of concurrent sessions for administrators with the same or hierarchical roles is limited to one. Session establishment for the admin web UI is based on the connecting IP address, and sessions are forcibly terminated after 10 minutes of inactivity for super and general administrators.

Related SFR FTA_MCS.2, FTA_SSL.3, FTA_TSE.1