Ref: APPM-ST-0.5

SECUREKi APPM Security Target

DOCUMENT VERSION	**0.5**
DOCUMENT DATE	**02 OCT 2017**

DF2-09-03A (Unit No.2), Level 9, Persoft Tower, Persiaran Tropicana,
Tropicana Golf & Country Resort, 47410 Petaling Jaya, Selangor Darul Ehsan
Email: sales@secureki.com
Tel: (603) 76520 099
Fax: (603) 76520 099
Website: http://www.secureki.com/

Prepared by:

ACROSS VERTICALS

DOCUMENT REVISION HISTORY

Version No.	Published Date	Description of changes
0.1	20 January 2017	Initial release
0.2	12 May 2017	Updated based on EOR001
0.3	04 August 2017	Update based on evaluator's feedback
0.4	28 September 2017	TOE Architecture added
0.5	02 October 2017	Update Section 1.5.3, 1.6 and 7.2

TABLE OF CONTENTS

1 Security Target Introduction

1.1 Security Target Reference

Security Target Title:	SECUREKi APPM Security Target
Security Target Version:	0.5
TOE Software Identification:	Automated Privilege Password Management v4.0.01
Evaluation Assurance Level:	EAL2

Table 1: ST Reference

1.2 TOE Reference

TOE Name & Version	TOE NAME:	TOE VERSION:
	Automated Privilege Password Management	v4.0.01
TOE Initial:	APPM	

Table 2: TOE Reference

1.3 Terminology and Acronyms

APPM	Automated Privilege Password Management
CC	Common Criteria
EAL	Evaluation Assurance Level
NTP	Network Time Protocol
OSP	Organizational Security Policy
OTP	One Time Password
PP	Protection Profile
SAR	Security Assurance Requirements
SFR	Security Functional Requirements
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification

1.4 Product Overview

APPM is an appliance based password management solution that manage access credentials (e.g. username and password) for connected system as such servers, network appliance and relevant IT components through trusted connecting networks. Thus allowing users to centralized manage access control accounts to these IT entities as well as ensuring policy security enforcement applied to all these IT entities that relevant to update those access credentials.

The APPM provides integrated appliance that combines between hardware and software.

a) APPM Appliance; and
b) APPM Web GUI.

All of these components is part of the scope of TOE except for the hardware appliance, underlying operating system and relevant supporting components (such as, Database and etc.), in which, functioning based on integration all together in its operational environment that shall be described in the TOE Guidance documentations. Note that, all hardware and software stated in Section 1.4.3 is not part of the TOE, and known as supporting components to the TOE operational environment.

Moreover, the details elaboration of APPM components as stated below:

a) APPM Appliance.
   The APPM Appliance, which is the first element of the TOE, is the security administration console to set up the user authorization parameters, defining the user's authentication mode as well as the workstation and risk policy. The following describes the features of APPM SMC:
   - Centralized administration of logon ID's.
   - Centralized policy configuration.
   - Centralized collection of logging of events.

   TOE Administrator (Super User)/s is applicable to work with different types of roles, responsibilities, access privileges and access rights based on their job descriptions. Such example, there will be a TOE Administrator (Super User) with less accessibility into the TOE plus with limited access privileges into the TOE modules or functions.
b) APPM Web GUI:
   APPM Web GUI provides a password request with the necessary setup environment for the user password management operations, including the administrator policy settings. APPM configuration is access through the Web GUI without any client installation, and configure password policy setting and user management through the APPM Web GUI (Using Web Browser).

Furthermore, with the new enhancement made on to the existing APPM, which is to include APPM Agent, allowing user to access the TOE through alternative method rather using the conventional method through web browser authentication and identification process. This is only for information and not include inside the TOE scope evaluation.

1.5 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

1.5.1 Usage and Major Security Features of the TOE

Automated Privileged Password Management (APPM for short) is the product developed by SECUREKi Sdn. Bhd. It is a solution to manage the issuance of One Time Password access credentials and permissions on Unix servers, Linux servers, Windows servers, network devices and other relevant applications for the assigned/registered privileged accounts in these stated components.

APPM enables enterprise to authorise users through the integrated workflow and manage the passwords automatically. By implementing the APPM solution, enterprise able to enforce password associated security compliance. In addition, it shall improve the security of password protection by removing the hard-coded password stored in the script. Furthermore, by having a 3rd backup mechanism through secured USB, provides fast recovery, and prevent a password loss from any system failure.

In traditional implementations, clients or customers will need to have different access credentials (e.g. usernames and password) to different products or systems and the management of these separate application accesses can be an administrative burden. This also can lead to unnecessary exposure to security leakages if accesses to different systems that are linked or integrated are not implemented according to a consistent policy.

With the multiple options or permutations available in the above implementation, the APPM enables the organization to manage the overall security through a single framework that enables the defining and assignment or implementation based on these following security functions in one system:

a) Security Audit;
b) User Data Protection;
c) Authentication and Identification; and
d) Security Management;

Additionally, with the new enhancement made into the APPM, APPM enforce the privilege and shared account password management and access control on heterogeneous IT infrastructure via periodically and automated changing password, with user access the one-time password through the authorized and approval workflow.

1.5.2 TOE Type

APPM is password management software that manage access credentials (e.g. username and password) for connected system as such servers, network appliance and relevant IT components through trusted connecting networks.

1.5.3 Non-TOE Software, Hardware and Firmware

Below is the list of non-TOE requirements:

Requirements	Descriptions	Version & Specifications
Hardware and Software Requirements (APPM 1000 series model and APPM1016S2GE Model)		
Hardware	Dimension (HxWxD)	1U Rackmount 1.7(43mm) x 16.8(426mm) x14(356mm)
	Power Supply	600W 80PLUS Platinum
	CPU	1 x Intel Xeon Quad-Core E3-1231v3 3.40Ghz processor
	RAM	16GB
	HDD	2 X 1TB RAID-1
	Backup USB	16GB
	Environment	Small < 1000 devices
Software	Operating System	OpenSUSE Linux 13.42
	Database	ORACLE XE 11.2
Minimum Client Hardware and Software Requirement		
Hardware	Desktop	Intel (R) Pentium (R) M Processor 1.60 GHz, 220 MHz, 2.00 GB of RAM
	Mouse/Pointing Device	Any pointing device with at least 2 buttons
	Component/Connected system managed by TOE	Any 3rd party components (i.e Cisco Router 3600 2 is being used as sample of components in evaluation)
Software	Operating System	Windows XP Service Pack 2, Windows Vista, Windows 7

Requirements	Descriptions	Version & Specifications
	Web Browsers	Internet Explorer [v9.0], Mozilla Firefox [v44.0] and Google Chrome [v 48.0.2564]
	Monitor Resolution	SVGA – Compatible display (256 or more colours recommended) with resolution of at least 1024 x 768 pixels
	Virtual Machine to host Component/Connected system managed by TOE	Any virtualization software
	Application Documentation	Adobe Acrobat Reader (4.0 or higher) to read online PDF files.

Table 3: None-TOE Software and Hardware

1.6 TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

1.6.1 Physical Scope of the TOE

The following figure illustrates the operations of TOE. Figure 1 illustrates one of example of TOE deployment in the client side.

APPM are applicable to be deployed in different operational environment that may have more components or fewer components as stated in Figure 1, shall be noted as not part of the scope of TOE. If such deployment is being performed, developer shall not be blame or taking any responsibility if the deployment produced vulnerabilities and flaw. Any deployment of the APPM shall be advice by developer in making sure that the APPM are properly deployed in its secure operational environment.

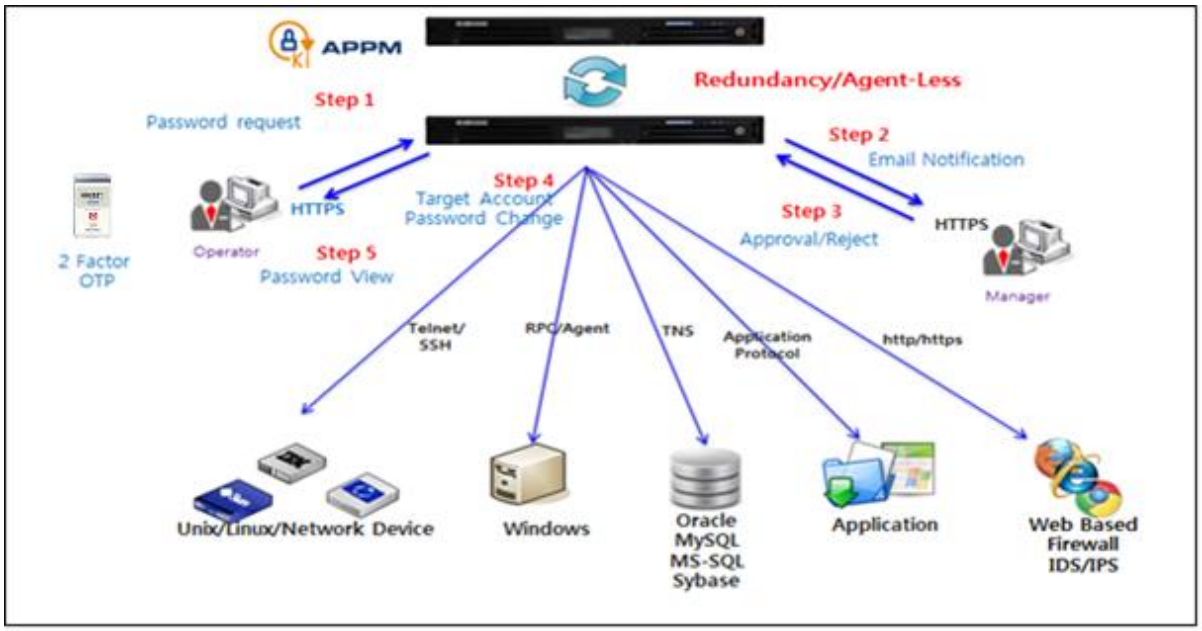

Figure 1: TOE Physical Scope

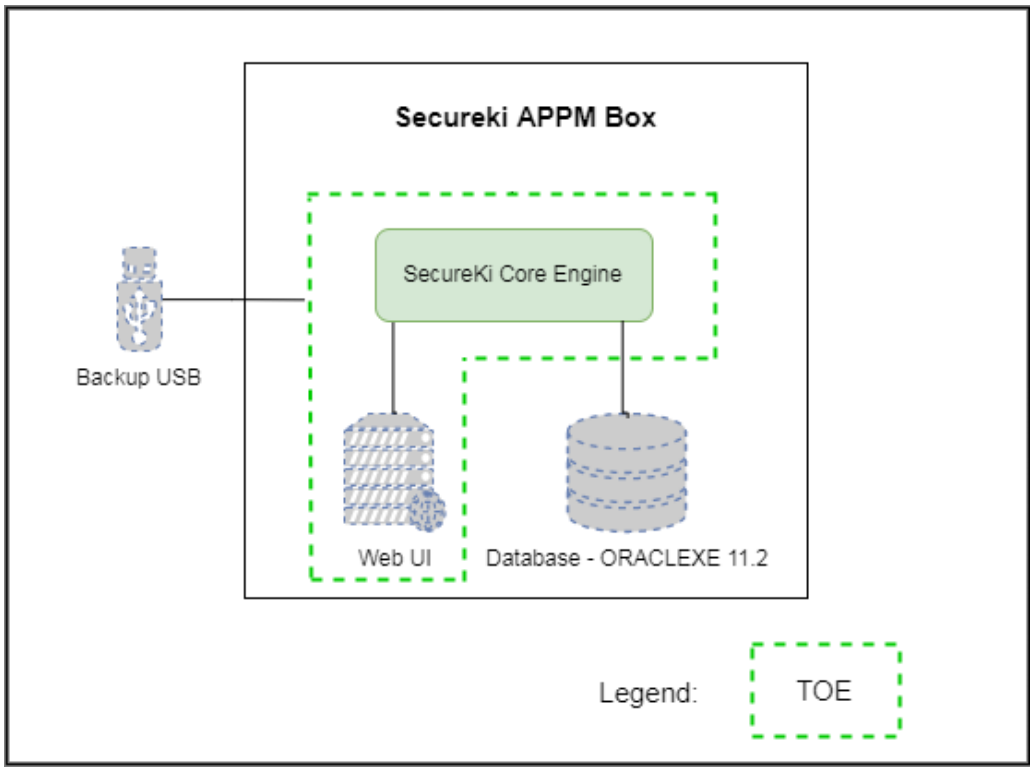

Figure 2 - APPM High-level Architecture Diagram

Figure 2 shows the APPM High-level Architecture. SecureKi Core Engine in this figure consists of:

- Security Audit subsystem
- Identification and Authentication subsystem
- User Data Protection subsystem

- Security Management subsystem

Details of the subsystem can be referred to Section 1.6.2 Logical Scope of the TOE.

The physical components of the TOE are:

- APPM software
  The TOE is installed in the APPM appliance that is delivered to the customer site.

- Guidance documents
  - SecureKi APPM Administrator's Guide (latest version)
  - SecureKi APPM Tech Training (latest version)

  The guidance documents are given to customer along with APPM appliance.

1.6.2 Logical Scope of the TOE

1.6.2.1 Security Audit

The TOE will generate audit records for selected security events in several log files and categories. Each audited events will be recorded along with date and time of event, user accounts that performed the event, event name and other event details. Audit records can be viewed by TOE Administrator (Super User) and cannot be edited. TOE Administrator (Super User) could select and filter the logs for easy viewing. TOE will create a new log file and may overwrite the old audit log records to store the audit records if the size limit is reached for a log file. Limitation of the log storage is based on the internal hard disk equipped within the TOE hardware server. Note that, TOE Administrator (Super User) shall be advice to backup all logs that is crucial to the TOE operational environment in accordance to organizational security policies in protecting the logs from any damages or tampering or loss.

The security audit function ensures that all TOE Administrator (Super User) activities pertaining to creation/update/delete of TOE Administrator (Super User), as well as the assigning TOE Administrator (Super User) roles and privilege accessibilities shall be log by audit functions. Details of audit logs and management of audit components are being explained in the Guidance documentations. Types of logs and descriptions of logs are described in details at TOE Summary Specification (TSS).

1.6.2.2 Identification and Authentication

All TOE Administrator (Super User) must have a valid username/user ID inclusive of password to access and OTP. The OTP is not part of the scope of the TOE. Accessibility mechanism to the TOE is included inside the scope of the TOE. TOE Administrator (Super User) must login to APPM to manage all the connected devices (IT entities) as well as credentials of accessing these IT entities. Thus, configurations of these IT entities required to be registered in the APPM system, plus configuration policy of managing the access credentials of the IT entities shall be defined. Whilst, each access

credentials that managed by the APPM system is been monitor through policy defined enforcement through the applied configuration made by the TOE Administrator (Super User).

In aspects of access control and session established upon authentication and identification, each TOE Administrator (Super User) are given a known configure value of idle mode, in which the value is configurable. This feature is configurable based on the policies defined by the organization security policies. If a login session has remained idle for a certain value that are been configure, such e.g. in 20 minutes, the TOE Administrator (Super User) will have to re-login to access the application again.

1.6.2.3 User Data Protection

User data and credentials including TOE Administrator (Super User) information is protected by ensuring that specific TOE Administrator (Super User) that is assigned with roles and privilege scan only access a specific web pages/portals and hence the data associated with the web pages/portal. The accessibility of the pages/portals is protected based upon the access control policy. The access control policy allows the TOE Administrator (Super User) to create username/user of the users that is assigned to access the TOE.

TOE has the capabilities of enforcing protection upon resources that the TOE protected, by implementing access control protection on authentication and identification webpage (login page) through access control policy. The TOE will check for legitimate access control credentials such as username/user ID and password/PIN before allowing such credentials to access the web applications portal protected by the TOE. TOE Administrator (Super User) could manage and configure access control policy and privilege access control, are defined to specific user account accessibility. By default, users without any access control credentials are not allowed to access the protected resources. There is also an information flow policy to control the control the information flow between the subjects and controlled information via controlled operations.

1.6.2.4 Security Management

TOE Administrator (Super User) has access to all TOE features, that applicable to be managed through web application portal hosted by TOE. TOE is able to provide accessibility of account that has access privilege, similar or limited, to “Super User” account. In which, Super User account has the full access rights, role and privileges to the TOE. TOE Administrator (Super User) could enable, disable and modify the behaviour of services controlled by TOE, user attribute values, network settings, time-of-day web access, NTP Time Server, backup and restore configurations setting and related functions of TOE.

Nonetheless, there are another 3 roles that are allows to access the TOE features, which is: Auditor, General User and Helpdesk. These roles are define with limited access to the TOE features compared to the TOE Administrator (Super User).

2 Conformance Claims

The following conformance claims are made for the TOE and ST:

CCv3.1 conformant	The ST and the TOE are Common Criteria conformant to Common Criteria version 3.1 Revision 4.
Part 2 conformant	The ST is Common Criteria Part 2 conformant.
Part 3 conformant	The ST is Common Criteria Part 3 conformant.
Package conformant	EAL 2
Protection Profile conformance	None.

3 TOE Security Problem Definition

3.1 Assumption

The assumptions are to ensure the security of the TOE and its deployed environment.

A.PHY	The TOE and its environment are physically secure.
A.ADMIN	Authorized administrators are non-hostile and follow guidance; however, they are not free from error.
A.TIMEBACK	The TOE environment will provide reliable time stamps and backup space.
A.CONN	The TOE environment will provide a secure connection between TOE and users.

Table 4: Assumptions

3.2 Threats

Assets that are protected by the TOE are sensitive data stored in the TOE and internal network including critical TOE configuration data (configuration files and others), audit records, admin credentials, TOE data and TOE security functions.

Threat agents are entities that can adversely act on the assets. The threat agents identified are an unauthorized person and an authorized administrator (a person that has been successfully authenticated and authorized as an administrator).

Threats may be addressed either by the TOE or by its intended environment.

T.ACCESSLOG	An unauthorized person successfully accesses the TOE data or security functions without being detected.

T.AUDIT	An unauthorized person or authorized user/administrator may intentionally or unintentionally delete audit records to destroy evidence of adverse events executed.
T.DEVICEAPP	An unauthorized person or unauthorized external IT entity may access device and applications in the network
T.REMOTE	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.
T.CONFIG	An unauthorized person may read and modify security TOE functions and configuration data.
T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to assess and use security functions and/or non-security functions provided by the TOE.
T.SESSION	An attacker may perform session hijacking to steal the session cookie

Table 5: Threats

3.3 Organizational Security Policies

The Organizational Security Policies (OSP) is imposed by an organization to secure the TOE and its environment.

P.ROLE	Only authorized persons assigned by the organization have access to the TOE.
P.PASSWORD	Authorized administrator shall use password with combination of special character, number and alphabet with minimum lengths of 12 to make it hard to guess.

Table 6: Organizational Security Policy

4 Security Objectives

Security objectives are formed to address the security problem definition defined in earlier section. The security implementation in TOE and its environment will meet these objectives.

4.1 Security Objectives for the TOE

The security objectives for the TOE as following:

O.ACCESSLOG	TOE shall record a readable log of security events.
O.AUDIT	TOE shall prevent an unauthorized person or authorized administrator to modify or deletes audit records of security events executed. The TOE shall ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.
O.DEVICEAPP	TOE shall provide control for user to access the device and applications in the network
O.CONFIG	TOE shall prevent unauthorized person to access TOE functions and configuration data.
O.NOAUTH	TOE shall protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functionality.
O.SESSION	TOE shall perform session timeout control to avoid session hijacking

Table 7: Security Objectives for the TOE

4.2 Security Objectives for the Operational Environment

The security objectives for the TOE operational environment as following:

OE.PHY	The TOE and its environment shall be physically secure.

OE.ADMIN	Authorized administrators shall be non-hostile and follow guidance; however, they are not free from error.
OE.TIMEBACK	The TOE environment shall provide reliable time stamps and backup space.
OE.CONN	Authorized administrators shall access the TOE using a secure connection provided by the environment to prevent eavesdropping.

Table 8: Security Objectives for the Operational Environment

5 Extended Components

This section defines the extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs) applicable for the TOE.

5.1 Extended Security Functional Requirement (SFR)

There are no extended SFR components defined for this evaluation.

5.2 Extended Security Assurance Requirement (SAR)

There are no extended SAR components defined for this evaluation.

6 TOE Security Requirements

This section provides the security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC, extended requirements, and an Evaluation Assurance Level (EAL) that contains assurance components from Part 3 of the CC.

6.1 Conventions

Part 2 of the Common Criteria defines an approved set of operations that may be applied to the statement of security functional requirements. Following are the operations and the document conventions as 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 an acronym at the end of the component identifier as follows: FCS_COP.1 (SWP).

6.2 Security Functional Requirements (SFR)

This section contains the security functional requirements (SFRs) for the TOE. The summary of SFRs is listed in following table.

Component	Component Name
Class FAU : Security Audit	
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User identity association
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FAU_STG.1	Protected audit trail storage
Class FDP : User Data Protection	
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
Class FIA : Identification and Authentication	
FIA_ATD.1	User attributes definition
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FIA_USB.1	User-subject binding
Class FMT : Security Management	
FMT_MOF.1	Management of security functions behaviour

FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation

Table 9: Security Functional Requirements List

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical 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) **[**

a) Authentication success or failure

b) Password request

c) Password approval/reject

d) User info modification

e) Configuration modification

].

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 definition

of the functional components included in the PP/ST, [**None**].

Application notes	Note that this SFR did not require to define the FPT_STM.1 statement as dependencies due to the timestamp are rely based on the underlying operating system. Furthermore, the start-up and shutdown of the audit function are not applicable and only can be turn off (not disable temporary) if the TOE are being turn off/power off.

FAU_GEN.2 User identity association

Hierarchical	No other components
Dependencies	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification
FAU_GEN.2.1	For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.
Application notes	None

FAU_SAR.1 Audit review

Hierarchical	No other components
Dependencies	FAU_GEN.1 Audit data generation
FAU_SAR.1.1	The TSF shall provide [**TOE Administrator (Super User)**] with the capability to read [**all audit logs trail data**] from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
Application notes	None.

FAU_SAR.2 Restricted audit review

Hierarchical	No other components
Dependencies	FAU_SAR.1 Audit review

FAU_SAR.2.1	The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.
Application notes	None

FAU_STG.1 Protected audit trail storage

Hierarchical	No other components
Dependencies	FAU_GEN.1 Audit data generation
FAU_STG.1.1	The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.1.2	The TSF shall be able to [***prevent***] unauthorised modifications to the stored audit records in the audit trail.
Application notes	None.

6.2.2 Class FDP: User Data Protection

FDP_ACC.1 Subset access control

Hierarchical	No other components
Dependencies	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1	The TSF shall enforce the [**access control policy**] on [**Table 10**].

Objects	Operations	Subjects
Main Module	View only	TOE Administrator (Super User).
Access Module	View only	TOE Administrator (Super User).
Main, Password, Approval, Policy, System (SYS MGMT) Management,	Enable to create, delete, view and edit accounts created in TOE, related to credentials and	TOE Administrator (Super User).

Report, Audit Log and Setup modules	roles/privileges. For Audit Log module, subject can only perform view and filter of audit records.	
SYS MGMT (Person) Module	View and edit user account	Helpdesk
Password (Password management) Module	View and edit user password	General User
Approval (Approval/Reject and Approval Request Status) Module	Request access to account device	General User
Audit & Report Module	Enable to viewing logs and filter of all activities performed by TOE. The logs will have details on all activities.	TOE Administrator (Super User) and Auditor.
SYS MGMT module	Centralized management module for the TOE in accessing other components of the TOE modules and managing data among the TOE operations.	TOE Administrator (Super User).
Policy module	Create, delete, enable and disable management of other types of data	TOE Administrator (Super User).

	accessibility related to TOE operations. Able to manage timeout session on the TOE.	

Table 10: Subject, Object and Operations for FDP_ACC.1

Application notes None

FDP_ACF.1 Security attribute based access control

Hierarchical 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 [**access control policy**] to objects based on the following: [**TOE Administrator (Super User)/s, users and groups that are associated with subject as stated in Table 4**].

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 TOE Administrator (Super User)/Auditor/General User/Helpdesk is successfully authenticated according to access privilege assigned, then access are granted based on privilege allocated for that users; and**

b) **If user attempt are not successful, therefore, access permission is denied**].

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**].

Application notes None.

FDP_IFC.1 Subset Information Flow Control

Hierarchical No other components

Dependencies FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the **[information flow control policy**] on[**Table 11**].

Objects	Operations	Subjects	Information
Main Module	View only	TOE Administrator (Super User).	TOE and user data
Access Module	View only	TOE Administrator (Super User).	User access to account device
Main, Password, Approval, Policy, System (SYS MGMT) Management, Report, Audit Log and Setup modules	Enable to create, delete, view and edit accounts created in TOE, related to credentials and roles/privileges. For Audit Log module, subject can only perform view and filter of audit records.	TOE Administrator (Super User).	IT Entities data and credentials

SYS MGMT (Person) Module	View and edit user account	Helpdesk	IT Entities data and credentials
Password (Password management) Module	View and edit user password	General User	IT Entities data and credentials
Approval (Approval/Reject and Approval Request Status) Module	Request access to account device	General User	Approval status
Audit & Report Module	Enable to viewing logs and filter of all activities performed by TOE. The logs will have details on all activities.	TOE Administrator (Super User) and Auditor.	Audit logs
SYS MGMT module	Centralized management module for the TOE in accessing other components of the TOE modules and managing data among the TOE operations.	TOE Administrator (Super User).	Information related to TOE operations that links to all TOE modules
Policy module	Create, delete, enable and disable management of other types of data accessibility	TOE Administrator (Super User).	Information of policy enforcement applicable and enforce within TOE

	related to TOE operations. Able to manage timeout session on the TOE.		operations

Table 11: Subject, Object, Operations and Information for FDP_IFC.1

Application notes None

FDP_IFF.1 Simple Security Attributes

Hierarchical	No other components
Dependencies	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation
FDP_IFF.1.1	The TSF shall enforce the [**information flow control policy**] based on the following types of subject and information security attributes: [**refer to Table 11**].
FDP_IFF.1.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [**refer to Table 11**].
FDP_IFF.1.3	The TSF shall enforce the [**none**].
FDP_IFF.1.4	The TSF shall explicitly authorise an information flow based on the following rules: [**None**].
FDP_IFF.1.5	The TSF shall explicitly deny an information flow based on the following rules: [**None**].
Application notes	None

6.2.3 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition

Hierarchical No other components

Dependencies No dependencies

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [

a) **Username/User ID;**

b) **Password/PIN;**

c) **Group Roles**

d) **Privilege**].

]

Application notes None

FIA_UAU.2 User authentication before any action

Hierarchical FIA_UAU.1 Timing of authentication

Dependencies FIA_UID.1 Timing of identification

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.

Application notes None

FIA_UID.2 User identification before any action

Hierarchical FIA_UID.1 Timing of identification

Dependencies No dependencies.

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

Application notes None

FIA_USB.1 User-subject binding

Hierarchical	No other components.
Dependencies	FIA_ATD.1 User attribute definition
FIA_USB.1.1	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [**a) Username/User ID;** **b) Password/PIN;** **c) Group Roles/Privilege**.]
FIA_USB.1.2	The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:[**a) Identification and Authentication shall be enforced upon all the users of the TOE when accessing TOE; and** **b) All users shall access TOE according to its Group roles and Privilege given**].
FIA_USB1.3	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [**changes of configuration on the TOE only performed by TOE Administrator (Super User)**].
Application notes	The default account for TOE Administrator (Super User) is “admin” for web login and “appm” for SSH login

6.2.4 Class FMT: Security Management

FMT_MOF.1 Management of security functions behavior

Hierarchical	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 [***disable, enable and modify***] the functions [**TOE Configurations**] to [**TOE Administrator (Super User)**].
Application Note	TOE configurations is all functions that are applicable for TOE Administrator (Super User)s for modification, disable and enable relevant functions of TOE, whereby, TOE functions are list of configurations menu are editable or selectable values are made available for TOE Administrator (Super User) to perform relevant actions based on organization requirements on the operational environment of the TOE.

FMT_MTD.1 Management of TSF data

Hierarchical	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 [***[Table 11: Operations]***] the [**Table 11: Information**] to [**Table 11: Subjects**].
Application Note	None

FMT_SMF.1 Specification of Management Functions

Hierarchical	No other components
Dependencies	No dependencies.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [**refer to Table 10**].
Application Note	None

FMT_SMR.1 Security roles

Hierarchical	No other components
Dependencies	FIA_UID.1 Timing of identification
FMT_SMR.1.1	The TSF shall maintain the roles **Administrator [TOE Administrator (Super User), Auditor, General User and Helpdesk**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Application Note	By default, TOE Administrator (Super User)/s account that is newly created will have limited access to the TOE. It is up to the default administrator account to give access to specific pages in the web-based administration portal and access to core functions of TOE.

FMT_MSA.1 Management of security attributes

Hierarchical	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 [**access control policy**] to restrict the ability to [***Table 12: Ability*** **[none]**] the security attributes [**Table 12: Security Attributes**] to [**Table 12: Authorized Roles**].

Ability	Security Attributes	Authorized Roles
change_default, modify, delete, [view, filter, add]	**Username/User ID, password/PIN, Group Roles/Privilege**	**TOE Administrator (Super User)**
change_default, modify, delete, [view, filter, add]	**Username/User ID, password/PIN**	**Helpdesk**

change_default, modify	**password/PIN**	**General User**
change_default, modify	**password/PIN**	**Auditor**

Table 12: Ability to perform actions on security attributes

Application Note Details on the security attributes, kindly refer to Table 10 or Table 11.

FMT_MSA.3 Static attribute initialisation

Hierarchical 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 [**access control policy**] to provide [***permissive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**TOE Administrator (Super User), General User, Helpdesk and Auditor**] to specify alternative initial values to override the default values when an object or information is created.

Application Note None.

6.3 Security Assurance Requirements

This ST claims compliance to the assurance requirements from the CC EAL2 assurance package. This EAL was chosen based on the security problem definition and the security objectives for the TOE. The chosen assurance level is consistent with the claimed threat and environment.

The following table summarized the TOE assurance requirements drawn from CC Part 3.

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_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	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
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

Table 13: Security Assurance Requirements for EAL2

7 TOE Summary Specifications

TOE addressed the security functional requirements as following:

7.1 Security Audit

The TOE will generate audit records for selected security events in several log files and categories. The events that being audited as following:

a) Authentication success or failure

b) Password request

c) Password approval/reject

d) User info modification

e) Configuration modification

Each audited events will be recorded along with date and time of event, user accounts that performed the event, event name and other event details. The timestamp are rely based on the underlying operating system. Furthermore, the start-up and shutdown of the audit function are not applicable and only can be turn off (not disable temporary) if the TOE are being turn off/power off.

Audit records can be viewed by TOE Administrator (Super User) and cannot be edited. TOE Administrator (Super User) could select and filter the logs for easy viewing. TOE will create a new log file and may overwrite the old audit log records to store the audit records if the size limit is reached for a log file. Limitation of the log storage is based on the internal hard disk equipped within the TOE hardware server. Note that, TOE Administrator (Super User) shall be advice to backup all logs that is crucial to the TOE operational environment in accordance to organizational security policies in protecting the logs from any damages or tampering or loss.

The security audit function ensures that all TOE Administrator (Super User) activities pertaining to creation/update/delete of TOE Administrator (Super User), as well as the assigning TOE Administrator (Super User) roles and privilege accessibilities shall be log by audit functions. Details of audit logs and management of audit components are being explained in the Guidance documentations.

Relevant SFR: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_STG.1, FMT_MTD.1

7.2 Identification and Authentication

All users must have a valid username/user ID inclusive of password to access the TOE. User needs to provide their correct username/user ID and password/pin to be successfully identified and authenticated in the login page of the APPM Web GUI. Each user will have the following security attributes:

a) Username/User ID;

b) Password/PIN;

c) Group Roles/Privilege

All the security attributes will be enforced to user once user successfully identified and authenticated in the TOE. User shall access the TOE according to its Group Roles and Privilege given. The default account for TOE Administrator (Super User) is “admin” for web login and “appm” for SSH login. The default account will have default role and privilege when accessing the TOE. Only TOE Administrator (Super User) can disable, enable and modify configuration of the TOE. TOE Administrator (Super User) must login to APPM to manage all the connected devices (IT entities) as well as credentials of accessing these IT entities. Thus, configurations of these IT entities required to be registered in the APPM system, plus configuration policy of managing the access credentials of the IT entities shall be defined. Whilst, each access credentials that managed by the APPM system is been monitor through policy defined enforcement through the applied configuration made by the TOE Administrator (Super User).

In aspects of access control and session established upon authentication and identification, each TOE Administrator (Super User) are given a known configure value of idle mode, in which the value is configurable. This feature is configurable based on the policies defined by the organization security policies. If a login session has remained idle for a certain value that are been configure, such e.g. in 20 minutes, the TOE Administrator (Super User) will have to re-login to access the application again.

Relevant SFR: FIA_ATD.1, FIA_UAU.2, FIA_UID.2, FIA_USB.1, FMT_MOF.1, FDP_IFC.1

7.3 User Data Protection

User data and credentials including TOE Administrator (Super User) information is protected by ensuring that specific TOE Administrator (Super User) that is assigned with roles and privilege can only access a specific web pages/portals and hence the data associated with the web pages/portal. The accessibility of the pages/portals is protected based upon the access control policy. The access control policy allows the TOE Administrator (Super User) to create username/user of the users that is assigned to access the TOE.

TOE has the capabilities of enforcing protection upon resources that the TOE protected, by implementing access control protection on authentication and identification webpage (login page) through access control policy. The TOE will check for legitimate access control credentials such as username/user ID and password/PIN before allowing such credentials to access the web applications portal protected by the TOE. TOE Administrator (Super User) could manage and configure access control policy and privilege access control, are defined to specific user account accessibility. By default, users without any access control credentials are not allowed to access the protected resources.

The details of access control policy are as following:

Objects	Operations	Subjects
Main Module	View only	TOE Administrator (Super User).
Access Module	View only	TOE Administrator (Super User).
Main, Password, Approval, Policy, System (SYS MGMT) Management, Report, Audit Log and Setup modules	Enable to create, delete, view and edit accounts created in TOE, related to credentials and roles/privileges. For Audit Log module, subject can only perform view and filter of audit records.	TOE Administrator (Super User).
SYS MGMT (Person) Module	View and edit user account	Helpdesk
Password (Password management) Module	View and edit user password	General User
Approval (Approval/Reject and Approval Request Status) Module	Request access to account device	General User
Audit & Report Module	Enable to viewing logs and filter of all activities performed by TOE. The logs will have details on all activities.	TOE Administrator (Super User) and Auditor.
SYS MGMT module	Centralized management module for the TOE in accessing other components of the TOE modules and managing data among the TOE operations.	TOE Administrator (Super User).
Policy module	Create, delete, enable and disable management of other types of data accessibility	TOE Administrator (Super User).

Objects	Operations	Subjects
	related to TOE operations. Able to manage timeout session on the TOE.	

Information flow control policy will be enforced to control the information flow between the subjects and controlled information via controlled operations following the rules below:

Objects	Operations	Subjects	Information
Main Module	View only	TOE Administrator (Super User).	TOE and user data
Access Module	View only	TOE Administrator (Super User).	User access to account device
Main, Password, Approval, Policy, System (SYS MGMT) Management, Report, Audit Log and Setup modules	Enable to create, delete, view and edit accounts created in TOE, related to credentials and roles/privileges. For Audit Log module, subject can only perform view and filter of audit records.	TOE Administrator (Super User).	IT Entities data and credentials
SYS MGMT (Person) Module	View and edit user account	Helpdesk	IT Entities data and credentials
Password (Password management) Module	View and edit user password	General User	IT Entities data and credentials
Approval (Approval/Reject and Approval Request Status) Module	Request access to account device	General User	Approval status
Audit & Report	Enable to viewing logs	TOE Administrator	Audit logs

Objects	Operations	Subjects	Information
Module	and filter of all activities performed by TOE. The logs will have details on all activities.	(Super User) and Auditor.	
SYS MGMT module	Centralized management module for the TOE in accessing other components of the TOE modules and managing data among the TOE operations.	TOE Administrator (Super User).	Information related to TOE operations that links to all TOE modules
Policy module	Create, delete, enable and disable management of other types of data accessibility related to TOE operations. Able to manage timeout session on the TOE.	TOE Administrator (Super User).	Information of policy enforcement applicable and enforce within TOE operations

Relevant SFR: FDP_ACC.1, FDP_ACF.1, FDP_IFC.1, FDP_IFF.1

7.4 Security Management

TOE Administrator (Super User) has access to all TOE features, that applicable to be managed through web application portal hosted by TOE. TOE is able to provide accessibility of account that has access privilege, similar or limited, to “Super User” account. In which, Super User account has the full access rights, role and privileges to the TOE. TOE Administrator (Super User) could enable, disable and modify the behaviour of services controlled by TOE, user attribute values, network settings, time-of-day web access, NTP Time Server, backup and restore configurations setting and related functions of TOE. These are TOE configurations.

Nonetheless, there are another 3 roles that are allows to access the TOE features, which is: Auditor, General User and Helpdesk. These roles are define with limited access to the TOE features compared to the TOE Administrator (Super User). By default, TOE Administrator (Super User)/s account that is

newly created will have limited access to the TOE. It is up to the default administrator account to give access to specific pages in the web-based administration portal and access to core functions of TOE.

Through access control policy, the TOE shall restrict the ability to perform actions to security attributes by roles as following:

Ability	Security Attributes	Authorized Roles
change_default, modify, delete, [view, filter, add]	**Username/User ID, password/PIN, Group Roles/Privilege**	**TOE Administrator (Super User)**
change_default, modify, delete, [view, filter, add]	**Username/User ID, password/PIN**	**Helpdesk**
change_default, modify	**password/PIN**	**General User**
change_default, modify	**password/PIN**	**Auditor**

Through access control policy also, the TOE Administrator (Super User), General User, Helpdesk and Auditor are able to override the defaults values of above table.

Relevant SFR: FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, FMT_MSA.1, FMT_MSA.3

8 Rationale

8.1 Protection Profile Conformance Claim Rationale

ST does not claim conformance to any Protection Profile. Hence, there are no elements to be covered in the conformance claim rationale.

8.2 Security Objectives Rationale

This section explains how threat, assumptions and OSP are related to each other. The following tables show threat, assumptions and organizational policy being mapped to security objectives.

8.2.1 Rationale for Security Objectives Mapped to Threats

Threats	Security Objectives	Rationale
T.ACCESSLOG An unauthorized person successfully accesses the TOE data or security functions without being detected.	**O.ACCESSLOG** TOE shall record a readable log of security events.	This security objectives counter threat because any success or failure of authentication events will be recorded in a readable log of security events. Each security events will be logged along with the user identity.
T.AUDIT An unauthorized person or authorized administrator may intentionally or unintentionally delete audit records to destroy evidence of adverse events executed.	**O.AUDIT** TOE shall prevent an unauthorized person or authorized administrator to modify or deletes audit records of security events executed. The TOE shall ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	This security objective counter threat because it will prevent an unauthorized person or authorized administrator to modify or deletes audit records of security events executed. The objective also ensures the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.
T.DEVICEAPP An unauthorized person or unauthorized external IT entity may access device and applications in the network	**O.DEVICEAPP** TOE shall provide control for user to access the device and applications in the network	This security objective counters threat because TOE will mediate the information flow to the device and application in the network. TOE will allow user to access only approved device and application based on user role. Unauthorized person or

		external IT entity will not have access to the controlled device and applications.
T.REMOTE An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.	**OE.CONN** Authorized administrators shall access the TOE using a secure connection provided by the environment to prevent eavesdropping.	This security objective counters threat because the environment will provide a secure and encrypted connection to prevent unauthorized person or external IT entity sniff the data and modify it.
T.CONFIG An unauthorized person may read and modify security TOE functions and configuration data.	**O.CONFIG** TOE shall prevent unauthorized person to access TOE functions and configuration data.	This security objective counters threat because TOE will prevent unauthorized person to access TOE functions and configuration data. Only TOE authorized administrator shall have access to TOE management interface.
T.NOAUTH An unauthorized person may attempt to bypass the security of the TOE so as to assess and use security functions and/or non-security functions provided by the TOE.	**O.NOAUTH** TOE shall protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functionality.	This security objective counters threat because security events are being audited and recorded in log file. Each security event will be recorded along with date and time of event, user who execute the event, filename and other event details. The audit records cannot be modified by administrator in order to preserve its integrity. Access control shall be enforced to ensure only the permitted user role have privilege to TOE functions that is relevant to their role.
T.SESSION An attacker may perform session hijacking to steal the session cookie	**O.SESSION** TOE shall perform session timeout control to avoid session hijacking.	This security objective counters threat because TOE shall have session timeout to avoid session hijacking. The session timeout is configurable by TOE Administrator (Super Admin)

Table 14: Rationale Security Objectives Mapped to Threats

8.2.2 Rationale Security Objectives Mapped to OSP Rationale

OSP	Security Objectives	Rationale
P.ROLE Only authorized persons assigned by the organization have access to the TOE.	**O.CONFIG** TOE shall prevent unauthorized person to access TOE functions and configuration data.	This security objective counters OSP because TOE will prevent unauthorized person to access TOE functions and configuration data. Only TOE authorized user shall have access to TOE.
P.PASSWORD Authorized administrator shall use password with combination of special character, number and alphabet with minimum lengths of 12 to make it hard to guess.	**OE.ADMIN** Authorized administrators shall be non-hostile and follow guidance; however, they are not free from error.	This security objective counters OSP because authorized administrator shall be non-hostile and follow guidance on creating a good password.

Table 15: Rationale Security Objectives Mapped to OSP

8.2.3 Rationale Security Objectives Mapped to Assumptions

Assumptions	Security Objectives	Rationale
A.PHY The TOE and its environment are physically secure.	**OE.PHY** The TOE and its environment shall be physically secure.	This security objective counters assumption because the TOE and its environment shall be physically secure.
A.ADMIN Authorized administrators are non-hostile and follow guidance; however, they are not free from error.	**OE.ADMIN** Authorized administrators shall be non-hostile and follow guidance; however, they are not free from error.	This security objective counters assumption because authorized administrators shall be non-hostile and follow guidance; however, they are not free from error.
A.TIMEBACK The TOE environment will provide reliable time stamps and backup	**OE.TIMEBACK** The TOE environment shall provide reliable time stamps	This security objective counters assumption because TOE environment shall

space.	and backup space.	provide reliable time stamps and backup space.
A.CONN The TOE environment will provide a secure connection between TOE and users.	**OE.CONN** Authorized administrators shall access the TOE using a secure connection provided by the environment to prevent eavesdropping.	This security objective counters assumption because authorized administrators shall access the TOE using a secure connection provided by the environment to prevent eavesdropping.

Table 16: Rationale Security Objectives Mapped to Assumptions

8.3 Extended Security Functional Requirement Rationale

Not applicable since there is no extended Security Functional Requirement declared in ST.

8.4 Extended Security Assurance Requirement Rationale

Not applicable since there is no extended Security Assurance Requirement declared in ST.

8.5 Security Functional Requirements Rationale

This section provides the rationale of using SFRs to meet the security objectives for the TOE and justify the SFRs dependencies that have been satisfied or not satisfied.

8.5.1 Rationale for SFR Mapped to Security Objectives for TOE

Security Objectives	SFRs	Rationale
O.ACCESSLOG TOE shall record a readable log of security events.	FAU_GEN.1	This SFR specify security events that are being audited and recorded in log file. Each security event will be recorded along with date and time of event, user who execute the event, filename and other event details. It traces back to this objective.
	FAU_SAR.1	This SFR specify that administrator will have the capability to view the audit trail data in log form. It traces back to this objective.
	FAU_SAR.2	This SFR specify that TOE Administrator (Super User) and Auditor users who can read access to the audit records. It traces back to this objective.

O.AUDIT TOE shall prevent an unauthorized person or authorized administrator to modify or deletes audit records of security events executed. The TOE shall ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	FAU_STG.1	This SFR specify that audit records cannot be modified or deleted by administrator or unauthorized person. It traces back to this objective.
O.CONFIG TOE shall prevent unauthorized person to access TOE functions and configuration data.	FIA_ATD.1	This SFR provide users with attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. It traces back to this objective.
	FIA_UAU.2	This SFR require each person to be successfully authenticated before being allowed to perform any actions on TOE functions and configuration data. It traces back to this objective.
	FIA_UID.2	This SFR require each person to be successfully identified before being allowed to perform any actions on TOE functions and configuration data at the TOE management interface. It traces back to this objective.
	FIA_USB.1	This SFR associate users with their security attributes in order to access TOE functions. The access given to user will be based on their roles or privilege. Changes to configurations in TOE is only allowed to TOE Administrator (Super User). It traces back to this objective.
	FMT_MOF.1	This SFR restrict the ability to enable, disable and modify TOE functions to administrator. It traces back to this objective.
	FMT_MTD.1	This SFR restrict the ability to change default value, modify, delete and add user attributes to authorized roles in TOE. It traces back to this objective.
	FMT_SMF.1	This SFR identify management functions that are available in TOE, that are managed by administrator and other roles in TOE. It traces back to this objective.

	FMT_SMR.1	This SFR identify the roles exist in TOE, which are TOE Administrator (Super Admin), Auditor, General User and Helpdesk. It traces back to this objective.
	FMT_MSA.1	This SFR restrict the ability to change default value, modify, delete, view, filter and add security attributes to roles in TOE. It traces back to this objective.
	FMT_MSA.3	This SFR enforce that only TOE Administrator (Super User), General User and Helpdesk can override the default password/pin and configurations. It traces back to this objective.
O.NOAUTH The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functionality.	FAU_GEN.1	This SFR specify security events that are being audited and recorded in log file. Each security event will be recorded along with date and time of event, user who execute the event, filename and other event details. It traces back to this objective.
	FAU_GEN.2	This SFR specify security events that are being audited and recorded in log file. Each security event will be recorded along with user who execute the event. It traces back to this objective.
	FAU_STG.1	This SFR specify that audit records cannot be modified or deleted by any user or unauthorized person. It traces back to this objective.
	FDP_ACC.1	This SFR specify that each user will have privilege to access and use TOE functions based roles. It traces back to this objective.
	FDP_ACF.1	This SFR specify that each user will have privilege to access and use TOE functions based roles. It traces back to this objective.
	FDP_IFF.1	This SFR specify TOE shall permit only information flow from authorized user to TOE. It traces back to this objective.
	FIA_UAU.2	This SFR require each person to be successfully authenticated before being allowed to perform any actions on TOE functions and configuration data. It traces back to this objective.

	FIA_UID.2	This SFR require each person to be successfully identified before being allowed to perform any actions on TOE functions and configuration data. It traces back to this objective.
O.SESSION TOE shall perform session timeout control to avoid session hijacking	FDP_ACC.1	This SFR require session timeout to be managed by TOE and the session timeout is configurable. It traces back to this objective.
	FDP_IFC.1	This SFR require session timeout to be managed by TOE and the session timeout is configurable. It traces back to this objective.

Table 17: Rationale for SFR Mapped to Security Objectives for TOE

8.5.2 SFR Dependency Rationale

The following table provides a demonstration that all SFRs dependencies included in the ST have been satisfied.

SFR	Dependency	Dependency Met?	Justification
FAU_GEN.1	FPT_STM.1	No	Timestamp are rely based on the underlying operating system.
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Yes No	FIA_UID.2 is hierarchical to FIA_UID.1. Dependency is fulfilled with FIA_UID.2.
FAU_SAR.1	FAU_GEN.1	Yes	-
FAU_SAR.2	FAU_SAR.1	Yes	
FAU_STG.1	FAU_GEN.1	Yes	-
FDP_ACC.1	FDP_ACF.1	Yes	-
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Yes	-
FDP_IFC.1	FDP_IFF.1	Yes	-
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	Yes	
FIA_ATD.1	-	-	-
FIA_UAU.2	FIA_UID.1	No	FIA_UID.2 is hierarchical to FIA_UID.1. Dependency is fulfilled with FIA_UID.2.
FIA_UID.2	FIA_UID.1	No	FIA_UID.2 is hierarchical to FIA_UID.1. Dependency is fulfilled with FIA_UID.2.
FIA_USB.1	FIA_ATD.1	Yes	-
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	Yes	-
FMT_MTD.1	FMT_SMR.1	Yes	-

	FMT_SMF.1		
FMT_SMF.1	-	-	-
FMT_SMR.1	FIA_UID.1	-	FIA_UID.2 is hierarchical to FIA_UID.1. Dependency is fulfilled with FIA_UID.2.
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes	-
FMT_MSA.3	FMT_MSA.1 FMT_SMF.1	Yes	-

Table 18: SFR Dependencies

8.6 Security Assurance Requirements Rationale

EAL2 was chosen to provide a basic assurance. The chosen assurance level is appropriate with the threats defined for the environment. At EAL2, the TOE will have undergone an independent vulnerability analysis demonstrating resistance to penetration attackers with an attack potential of basic.