K'INFOSEC

AITHER v1.0

Security Target v1.5

Korea Information Security System Co., Ltd.

www.kinfosec.co.kr

< Revision History>

Version	Author	Date	Description
v1.0	Su-Hwan Park	2014-11-04	Initial Version
v1.1	Su-Hwan Park	2014-12-03	Physical and logical scope edited
v1.2	Su-Hwan Park	2015-02-03	Edited based on EOR-<Revision 1>
v1.3	Su-Hwan Park	2015-03-17	1. TOE operation environment figure edited 2. TSF self-test subject of FPT.TST.1 edited 3. Minor changes
v1.4	Su-Hwan Park	2015-04-17	1. Firmware version edited 2. OS and essential software Minimum specification edited 3. Physical scope version edited 4. Minor changes
v1.5	Su-Hwan Park	2015-05-21	1. Physical scope's S/W(AITHER S/W) edited

< Table of Contents >

1 Security Target Introduction

This security target specification is prepared by Korea Information Security System Co., Ltd. This specification defines the security function requirements of AITHER v1.0, a wireless AP, and assurance requirements that ensure this securely.

This security target specification includes.

- Chapter 1 explains security target specification, TOE reference and TOE overview.
- Chapter 2 explains standards of protection profile and package.
- Chapter 3 explains security problems in TOE and TOE environment by defining threats, organizational security policy and assumption.
- Chapter 4 explains security target for TOE and TOE environment.
- Chapter 5 explains expanded components created by the security target specification creator.
- Chapter 6 explains security function requirements and assurance requirements that satisfy security target.
- Chapter 7 explains summarized specification of TOE.

1.1 ST Reference

Security target requirement reference is summarized in [Table 1-1].

[Table 1-1] ST Reference

Classification	Description
Title	AITHER v1.0 Security Target
ST Version	v1.5
Publication date	2015. 05. 21
Author	Korea Information Security System Co., Ltd. R&D Center
CC Version	CC v3.1 r4
Evaluation assurance Level	EAL2
Major key words	AP, Access Point, Wireless, WLAN

1.2 TOE Reference

TOE reference is summarized in [Table 1-2].

[Table 1-2] TOE Reference

Classification	Description
TOE Title	AITHER
TOE Version	1.0
TOE Hardware	AITHER AP-1000
TOE Firmware	AITHER v1.0.003
TOE Release date	2015. 04. 17
TOE Developer	Korea Information Security System Co., Ltd. R&D Center

1.3 TOE Overview

This section describes usage of TOE and major security functions and identifies TOE types and non-TOE requirements for hardware, software and firmware.

1.3.1 Usage and major security features of the TOE

TOE is a wireless AP that connects wireless devices to a wired network by configuring secure WLAN, and provides security functions such as Rogue AP/Station detection and unauthorized network connection prevention:

- **Security audit**
  - TOE provides audit log creation and query execution functions to the subject that require audit.

- **Cryptographic support**
  - TOE provides cryptographic functions to protect user data between TOE and wireless user and TSF data between TOE and administrator PC.

- **User data protection**
  - TOE provides threat detection and prevention functions by configuring secure WLAN and by monitoring wireless network traffic.

- **Identification and authentication**
  - TOE provides authorization and authentication functions to control administrator who accesses the management UI and wireless devices connected to WLAN.

- **Security Management**

  - TOE provides functions for system configuration, security policy planning and security function management, wireless intrusion detection and prevention sensor (WIDPS), etc.

- **TSF protection**

  - TOE provides self-test function for TOE itself.

- **TOE access**

  - TOE provides functions that constraint duplicated sessions for an administrator account and ceases the authenticated session after the defined idle time.

- **Trusted path/channels**

  - TOE provides secure paths and channels for data transmission between TOE and wireless users as well as TOE and an administrator PC.

1.3.2 TOE types

TOE is a wireless AP that connects wireless devices to a wired network by configuring secure WLAN, and provides security functions such as Rogue AP/Station detection and unauthorized network connection prevention.

1.3.3 Non-TOE (hardware/software/firmware) required for TOE

Non-TOE (hardware/software/firmware) required for TOE is identified as follows:

- **Administrator PC**

  - Administrator PC is required for security management for TOE and the following summarizes software installed on an administrative PC:

[Table 1-3] Hardware specification and essential software for administrator PC

Classification		Minimum specification
Hardware	CPU	Intel Pentium4 2.0GHz or above
	RAM	1 GB or above
	HDD	100 GB or above
	NIC	10/100 Mb/s Ethernet or above
	Wireless LAN	IEEE 802.11a/b/g/n or above
OS		Microsoft Windows 7 Professional SP1 (32bit/64bit)

Essential Software	Internet Explorer 10 (32bit/64bit) or Chrome SSH v2 accessible terminal program

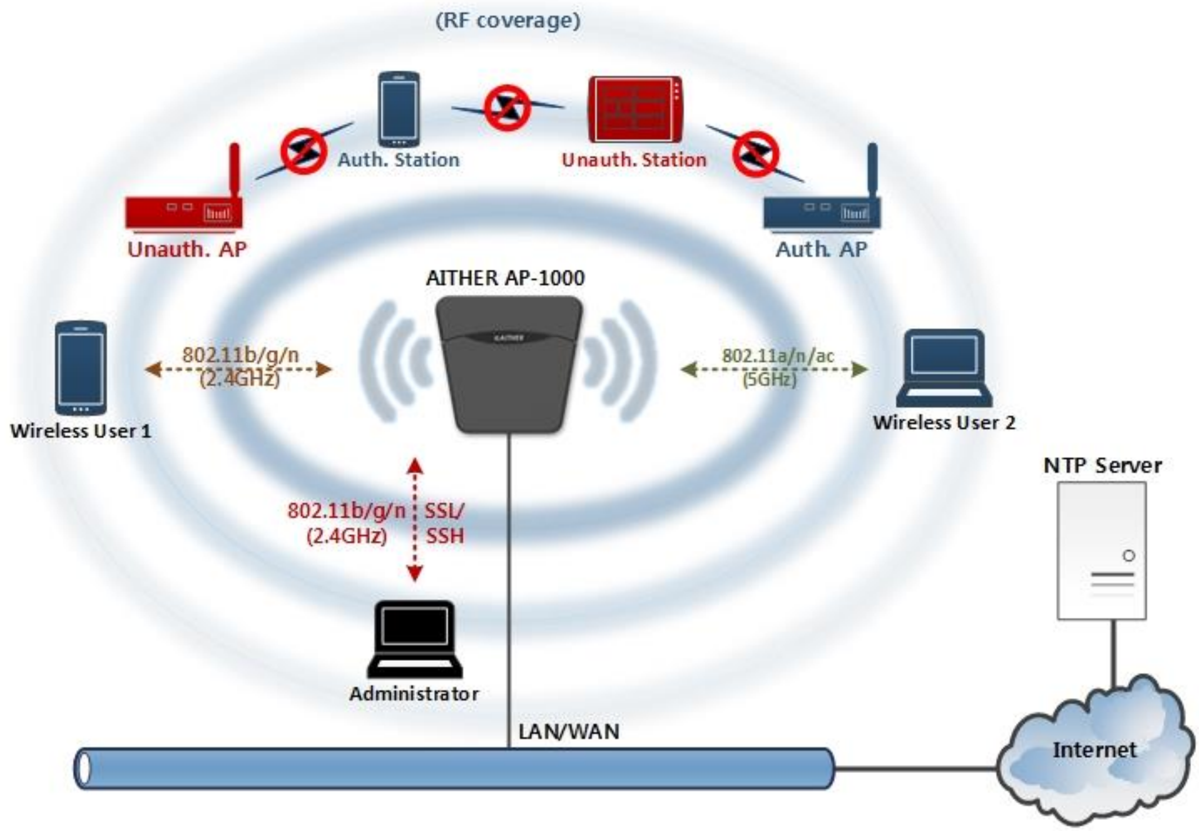
- **NTP Server**

  - NTP server is used to provide a reliable time stamp, and a public NTP server is used for this purpose.

1.4 TOE Description

This section explains environment of TOE and physical and logical scope. Physical scope includes TOE hardware, firmware, manual, and logical scope includes logical function of TOE.

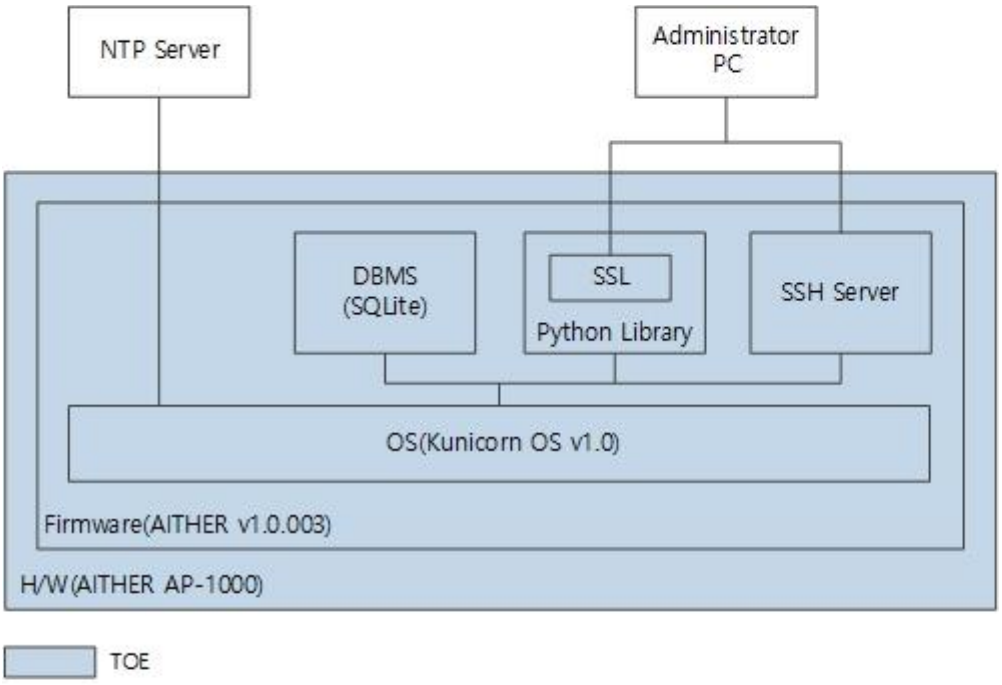
1.4.1 TOE Operation Environment



[Figure 1-1] TOE Operation environment

[Figure 1-1] illustrates a stand-alone TOE operation environment. TOE is connected to a wired network via LAN or WAN. TOE constructs WLAN using 802.11a/b/g/n/ac wireless network standard and provides secure WLAN. In order to secure a WLAN, TOE performs identification and authentication when wireless users try to connect to it. The administrator sets security policies for wireless networks by connecting to a management UI through secure SSL & SSH communication, and conducts security management operations for wireless network and audit log management. TOE provides detection and prevention of security threats of unauthorized APs and unauthorized stations within RF coverage.

1.4.2 TOE physical scope



[Figure 1-2] TOE physical scope

TOE is provided as a firmware on hardware and is an appliance product that automatically starts once electric power is on.

TOE consists of the following components.

- OS (Kunicorn OS v1.0)
  - This component is a Linux based customized operating system. It connects a wired network and wireless network via router functions and supports AP and wireless traffic data collection functions and performs authentication and authorization, security management, security audit.

- DBMS (SQLite)

- This component is storage for audit logs and use SQLite.

- Python Library

  - This component is a library for the web server based management UI and use Python.

- SSL

  - This component supports HTTPS based secure web server and use the default setting of Python Library.

- SSH Server

  - This component provides management console to the administrator and use Dropbear server.

The following summaries TOE hardware, which takes a role of starting and running embedded firmware:

- H/W (AITHER AP-1000)

  This is TOE hardware, and detailed specifications for each component are summarized in [Table 1-4].

[Table 1-4] TOE Hardware Detailed Specifications

Classification	Hardware(H/W) specification
CPU	Intel N2600 x 1ea.
Chipset	Intel NM10 x 1ea.
RAM	2GByte x 1ea.
ROM	NAND Flash 8Gbyte x 1ea.
Ethernet Port	10/100/1000 Base-T x 1ea.
Wireless Interface	Qualcomm 802.11a/b/g/n x 3ea. Qualcomm 802.11ac x 1ea.
PoE	802.3AF Type Watt/Port : 15.4W
Power Input	DC 12V Min : 1A, Max : 4A

TOE hardware is provided as all-in-one package in a box and components that come with this are summarized in [Table 1-5].

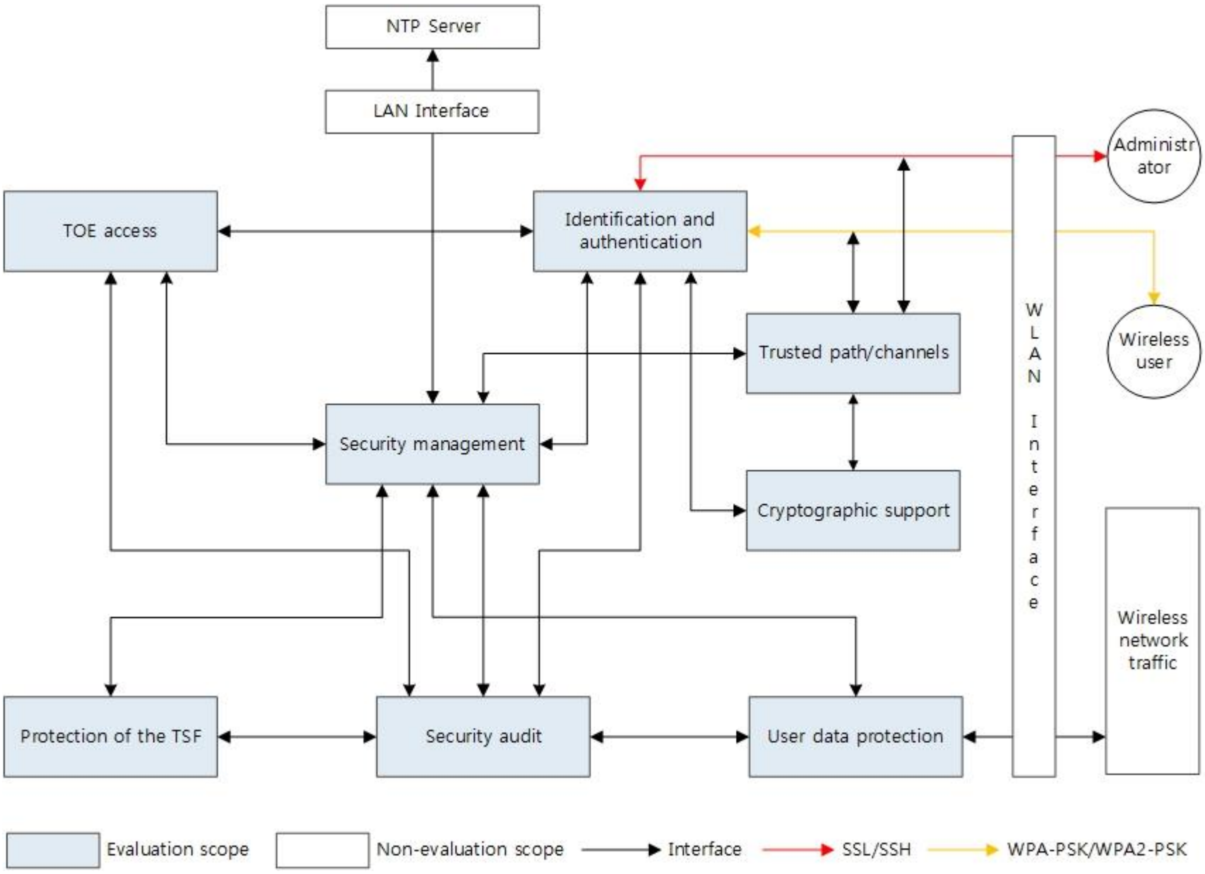
[Table 1-5] TOE Components

Classification	Type	Quantity	Notes

Products	Hardware	AITHER AP-1000	1ea.	Main hardware
	Firmware	AITHER v1.0.003	1ea.	Accompanied with hardware
Parts	Network cable	LAN cable	1ea.	
	Power cable	AC/DC Adapter(12V) and power cable	1ea.	
Manual	AITHER v1.0 User Operation Manual v1.2		1ea.	An individual manual CD (User Manual)
	AITHER v1.0 Preparation Process Manual v1.2		1ea.	
Warrant Document	Product component description and warranty document		1ea.	License description

1.4.3 TOE logical scope

The following illustrates logical scope of TOE:



[Figure 1-3] TOE logical scope

(1) Identification and authentication

TOE performs identification and authentication in order to ensure access by an authorized administrator and wireless users.

TOE provides administrator connection path through WLAN Interface (802.11b/g/n) 2.4GHz band and the administrator access using SSL or SSH. The administrator operates security functions of the security management through SSL and operates limited functions - wired network setting change, system time setting, management CLI password change, management UI password expiration date setting, and CLI log query via CLI through SSH.

During the administrator identification and authentication process, the administrator should provide ID and password. If identification and authentication failure occur more than the defined number, management procedures, such as authentication function lock for the defined time (e.g. 5 minutes), is carried out by TOE.

Wireless users connect to TOE via WLAN Interface and their communication path is securely protected by WPA-PSK/WPA2-PSK. The following wireless network standard protocol is used to support communication between TOE and wireless users:

- 2.4GHz band IEEE 802.11b/g/n
- 5GHz band IEEE 802.11a/n/ac

TKIP and CCMP (AES) used for communication encryption between TOE and wireless users and between TOE and an administrator are supported by cryptographic support and the identification and authentication results of the wireless users and administrator are stored as audit logs. The administrator conduct security audit using the created audit logs.

(2) TOE access

Since there is concurrent session limit for the administrator account used for accessing management UI of TOE, only one session is allowed to connect to the management UI and to keep its connection. For the session connected to the management UI, TOE provides an idle session management function that ceases the session if the defined idle time passes. TOE also restricts the access from an unauthorized IP by registering authorized IP.

(3) Trusted path/channels

TOE provides secure path for transmitting data between TOE and wireless users and administrator connected to WLAN of TOE and the trusted path is protected by encryption proposed by cryptographic support.

(4) Cryptographic support

TOE uses encryption key in order to support secure communication of the user data transmitting between TOE and the wireless users connected to WLAN of TOE and performs creation, distribution and destruction according to specified encryption creation algorithm, encryption distribution methods and encryption destruction methods. TOE also supports secure communication between TOE and the administrative PC connected to WLAN.

The following encryption methods are used for user data encryption:

- TKIP(Temporal Key Integrity Protocol)
- CCMP(AES)

(5) TSF protection

In order to ensure accurate operation of TOE, TOE periodically identifies abnormal stops of TSF execution process through process monitoring program during the normal operation. If abnormal stops occur, TOE restarts them.

When it starts or when the authorized administrator requests, TOE performs integrity check for TSF execution file and WLAN configuration file. If any non-integrity files are found during the integrity check at starting, TOE restores the damaged file with the original backup file.

TOE records audit logs when restoration for abnormal process stops is conducted or when damaged file is identified during the integrity check. The administrator performs security audit with the audit logs created.

(6) Security management

Using the security management, the authorized administrator performs a security audit and TSF protection, and blocks the administrator session access of the unauthorized IP address by setting IP address that allows administrator access.

TOE synchronizes between the external remote network time protocol (NTP) server's time and the local system time.

In addition, TOE detects and prevents security threat of wireless network traffics within RF coverage by setting WIDPS policy and executing it. These security management performed by Python based management UI after connecting to TOE through 802.11 wireless 2.4GHz band, and communication path is protected by SSL. In addition, if administration UI have problem, CLI mode, which is protected by SSH, can be used to check basic information. CLI mode supports following functions:

Wired network setting, system time setting, management UI password expiration date setting, CLI log management UI password expiration date setting, and CLI log query

(7) Security audit

The authorized administrator can inspect the following audit logs through "Security Audit":

- Logs for TSF protection integrity check results (Integrity damaged file)
- Administrator session restriction logs based on IPs that are allowed to access TOE
- Identification and authentication result logs of administrator and wireless users
- Wireless network traffic threat logs of the user data protection
- Administrator behavior logs of security management

In addition, the Security Audit sends security alarms to the management UI when security alarms incidents detected in the audit logs from user data protection and the security audit prevents audit log loss caused by audit log storage shortage or full.

(8) User data protection

TOE analyzes after collecting all wireless network traffic within RF coverage. Based on analysis results, TOE provides manual or auto disconnection function, which detects security threats in real time by the defined wireless intrusion detection and prevention policy. [Table 1-6] summarizes the defined threats and responses provided by TOE.

[Table 1-6] Defined Threats and Responses Provided by TOE

Threat	Response
Rogue AP	Detect and alter the unauthorized AP installation
Rogue Station	Detect and alert the unauthorized wireless device
Mis-configured AP	Detect and alert AP that does not apply encryption and that use low level security configuration
Client Mis-association	Detect and disconnect threats that outpour internal data out of internal security control scope through connecting to an external unauthorized AP by the authorized user.
Unauthorized Association	Detect and disconnect threats that connects to the internal authorized AP by the unauthorized user.
Ad-hoc Connection	Detect and disconnect threats that can configure an ad-hoc network with the internal authorized device by the unauthorized user.
AP MAC Spoofing	Detect and alert attacks conducted by spoofing MAC addresses.
Honeypot AP	Detect and alert attacks by an unauthorized AP disguised as an authorized AP.

1.5 Writing Rule

The notation, formatting and conventions used in the security target specification follows the Common Criteria for Information Technology Security Evaluation. Common Criteria allows selection, assignment, refinement and iteration operations that can be executed in the security functional requirements.

Iteration

Used when the same components are repeatedly used in various operations. The repeated operations outputs are displayed as a specific number of times enclosed within brackets (Number of times repeated) after the component identifier.

Selection

Used when select one elements in component from several alternative. Select operation outputs are displayed in *underline and italics*.

Refinement

Used to limit requirements by adding details in the requirements. Refine operation outputs are displayed in **bold**.

Assignment

Used to allocate specified values to unclaimed parameters. Assignment operation outputs are deployed with angle brackets. Example: [Assignment value]

1.6 Conventions

According to the terms used in this security target specification, if any term is the same as the common criteria, it follows the common criteria.

Object

Object is a main target of the subject's operation and the passive entity that include or receive information.

Iteration

Use the same component to express one or more different requirements.

Security attribute

Subject, user (including external IT products), object, information, and session and/or resource characteristic that used to define SFR. These values are used to execute SFR.

ST: Security Target

Implementation dependent security requirement specification appropriate for a specific TOE.

Selection

Specify one or more items from the described list in a component.

Identity

Unique expression that identifies the authorized user, which can be his/her real name, abbreviation, or alias name.

Element

Undividable minimum unit of security requirement.

Role

Set of defined rules that define allowable interactions between the user and TOE.

Operation (on a component of the CC)

Modification and repetition of components. Operations allowed for components are assignment, repetition, refinement and selection.

Operation (on an object)

Specific behavior that the subject performs to the object.

Threat Agent

Entity that can do activities making harms to the asset.

External entity

All external secure or unsecure IT products (or systems) interact (or can interact) with TOE.

Authorized Administrator

An authorized user that securely operates and manages TOE according to SFR (Security Functional Requirements)

Authentication Data

Data used to verify a user's identity.

Assets

Entity that TOE's owner is given the value.

Refinement

Specify a component by adding details.

Organizational security policies

A set of security rules, procedures, practices and guidelines that are given/will be given to the current operating environment by actual or virtual organization.

Dependency

Relationship between component, where if a dependent component includes protection profile, security target specification, and package of the dependent component, the requirements based on the dependent component should be included in protection profile, security target specification, and package.

Subject

Active entity in TOE that performs operation to the object.

Component

A set of elements. Smallest selection unit used to form the basis of requirements.

Class

A set of common evaluation criteria family that has same security target.

TOE: Target of Evaluation

A collection of software, firmware and/or hardware that accompanies available document.

EAL: Evaluation Assurance Level

Warranty family consists of three set of assurance requirements that have assurance level defined by common evaluation criteria.

Family

A collection of components that have similar purpose but have different emphasis or rigorousness.

Assignment

Specify the identified parameters in detail within component and requirement of common evaluation criteria

TSF: TOE Security Functionality

A collection set of hardware, software, firmware of TOE that contribute to accurate execution of SFR (Security Functional Requirements)

TSF Data

Data created by TOE and for TOE, which impact on TOE operations.

SSL (Secure Socket Layer)

Netscape developed for security such as e-commerce. Later it was standardized as TLS (Transport

Layer Security). In particular, since SSL is a network layer encryption method, it can be used in HTTP as well as in NNTP, FTP, etc. Basically it ensures authentication, encryption, and integrity.

WIDPS (Wireless Intrusion Detection & Prevention Sensor)
A sensor (or function) that detects and blocks intrusion threats by continually monitoring wireless network traffic.

IEEE 802.11
Computer wireless network technology for local area called Wireless LAN or Wi-Fi. It is developed by the 11th working group of IEEE LAN/MAN standard committee (IEEE 802).

AP (Access Point)
Wired-Wireless connection bridge device that performs transfer frames from one wireless device to another device.

Station
A device equipped with IEEE base WNIC (Wireless Network Interface card), which performs operations of physical layer and MAC layer operations based on IEEE 802.11 standard.

Authorized AP
An AP registered in the whitelist of TOE by the administrator

Authorized Station
A station registered in the whitelist of TOE by the administrator

Unauthorized AP
An AP not registered in the whitelist of TOE

Unauthorized Station
A station not registered in the whitelist of TOE

SSID (Service Set Identifier)
A connection identifier between wireless device and AP that are used by the service provider to differentiate various basic service sets in the wireless LAN.

Rogue AP
An AP, installed without permission by the administrator, can cause a security threat that induces malicious internal network intrusion by the insider or by the outsider.

Honeypot AP

An AP that discloses user information such as user IDs and passwords by stealing the SSID of the attack target AP and by pretending that you are connected to a normal AP.

WPA (Wi-Fi Protected Access)

Wireless LAN encryption technology that uses TKIP (Temporal Key Integrity Protocol), which uses RC4 stream encryption that improves the WEP vulnerabilities specified in the IEEE 802.11i standard.

WPA2 (Wi-Fi Protected Access 2)

Wireless LAN encryption technology that uses CCMP (CCM Mode Protocol), which uses AES encryption method specified in IEEE 802.11i standard.

Ad-hoc Network

A network that communicates each other between devices without fixed wired network.

WLAN: Wireless Local Area Network

A wireless local area network constructed by TOE

Wireless User

Station connected to a WLAN provided by TOE

RF Coverage (Radio Frequency Coverage)

Distance capable of wireless communication between TOE and other AP or wireless device. TOE can search for all wireless network traffic within the RF coverage

PBKDF2 (Password-Based Key Derivation Function 2)

A one-way hash function algorithm approved by NIST (National Institute of Standards and Technology, American Institute of Standards and Technology) and used to generate an encrypted digest of the user password

PSK (Pre-Shared Key)

AP and wireless user share specific string as password and use it for authentication.

2 Conformance Claims

2.1 Common Criteria and Protection Profile, Security function requirements package Conformance

Common criteria, protection profile, assurance requirements, security requirements that security target specification and TOE should conform is summarized in [Table 2-1].

[Table 2-1] Standards that Security Target Specification and TOE Conform

Classification	Conformance
Common Criteria	Common Criteria for Information Technology Security Evaluation Version 3.1 Revision4 - Common Criteria for Information Technology Security Evaluation, Part 1 (CCMB-2012-09-001) - Common Criteria for Information Technology Security Evaluation, Part 2 (CCMB-2012-09-002) - Common Criteria for Information Technology Security Evaluation, Part 3 (CCMB-2012-09-003)
Common Criteria Part 1	Conformance
Common Criteria Part 2	Conformance
Protection Profile	Conformance
Security function requirements package	EAL2 Conformance

2.2 Protection Profile Conformance

This Security Target does not conform to the requirements of other Protection Profiles.

3 Security Problem Definition

This section defines TOE and threats that should be managed by TOE environment, as well as organizational security policy and assumption.

3.1 Property

Property that are protected by TOE are

- TOE
- User data transmitted via wireless LAN function provided by TOE
- Wired and wireless network managed by TOE
- TSF data managed by TOE

3.2 Threats

The threat agents are IT entities and users that illegally access TOE and the basic assets protected by TOE or that inflict harm to TOE anomaly. The threat agent has basic level expertise, resource and motivation.

T.Disguising as administrator
The threat agent may gain access to the product by disguising as an authorized administrator.

T.Recording failure
The threat agent can make do not record security-related incidents by exhausting the storage capacity.

T.Internal information leakage
An authorized terminal can leak the internal information via external unauthorized terminal connection through connecting the unauthorized external AP or using Ad-hoc method.

T.Unauthorized network access
Threat agents can access TOE or TOE managed wired and wireless network with unauthorized method through attack such as Rogue AP, internal policy violating AP, Honeypot AP, Ad-hoc access and MAC address modification.

T.Continious authentication trials
The threat agent can acquire authorized administrative privilege by continuous authentication

trials.

T.Reuse attack

The threat agent can access TOE by reusing administrator's authentication data.

T.Damage to the stored data

The threat agent can expose, change, or delete TSF data stored in TOE in an unauthorized manner.

T.Damage to transmission data

The threat agent can expose or change data transmitted between TOE and wireless user and between TOE and administrative PC in unauthorized way.

3.3 Organizational Security Polices

This section describes rules or specified organizational security policy that TOE and TOE environment should follow.

P.Audit

In order to trace the responsibility to the security-related events, all security related incidents should be recorded and maintained and the recorded data must be reviewed.

P.Security maintenance

When the internal network averment has been changed by changing network configuration, increasing or decreasing of hosts, and increasing or decreasing of service, the same level of security level as before by reflecting the changed environment and policy to TOE operational policy.

P.Secure management

TOE should be managed in a secure manner using the security functions provided by TOE.

3.4 Assumption

This section describes assumptions of the TOE environment from physical, personal, connectivity and other aspects.

A.Trusted administrator

An authorized administrator of the TOE is not malicious, well trained about the TOE management functions and carries out his/her duties accurately in accordance with the administrator guidelines.

A.Trusted external server

Assure the reliability and stability for external NTP Server that interacts with TOE.

A.Secure key management

Assure secure management of WLAN key in wireless terminal that connects to TOE WLAN.

4 Security objectives

This security target specification defines security objectives by classifying them to the security objectives for TOE and the security objectives for operations. The security objectives for TOE aim to the security objectives directly handled by TOE, and the security objectives for operation environment aim to support technical/procedural means, so that TOE accurately provides security functionality.

4.1 TOE Security objectives

The following explains the security objectives directly managed by TOE.

O.Audit

TOE shall record and maintain security-related events to trace responsibilities of all security-related behavior, should provide a means to review the recorded data. In addition, when the audit trail storage is full state shall provide a corresponding function.

O.Management

TOE shall provide management means that an authorized administrator of the TOE can efficiently manage the TOE in a secure manner, and shall provide a means to keep the TSF data up to date.

O.Identification and authentication

TOE shall provide management means that an authorized administrator of the TOE can efficiently manage the TOE in a secure manner, and shall provide a means to keep the TSF data up to date.

O.Stored data protection

TOE unauthorized disclosure of TSF data stored in the TOE, the change should be protected from deletion.

O.Transmission data protection

TOE shall be protected from the TOE and the TOE and the wireless user and the administrator exposed or unauthorized changes to the way data are transmitted between the PC.

O.Intrusion detection & prevention

TOE analyzes the traffic information collected by the wireless network intrusion detection (threat) for the wireless network managed by the TOE, and to block according to the security policy.

4.2 Security objectives for the TOE operation environment

The following are security objectives handled by technical/procedural means supported by the operating environment for the TOE provides security functions correctly.

OE.Audit review

The stored record should be reviewed periodically by using the audit function provided by TOE.

OE.Security maintenance

When the internal network environment has been changed by the network configuration changes, increase and decrease of host and increase and decrease of services, the same level of security as before should be maintained by reflecting the changed environment and security policy to the TOE operational policy immediately.

OE.Secure management

TOE should be managed securely by using the security functions provided by the TOE.

OE.Trusted administrator

An authorized administrator of the TOE is not malicious, well trained about the TOE management functions and carries out his/her duties accurately in accordance with the administrator guidelines.

OE.Trusted external server

Assure the reliability and stability for external NTP Server that interacts with TOE and provide reliable timestamps for TOE.

OE.Secure key management

The wireless devices connected to the TOE WLAN should manage WLAN authentication key securely.

4.3 Theoretic Rationale of Security Objectives

Theoretic rationale of security objectives proves that the specified security objectives are appropriate, are sufficient to manage security problem, and are essential rather than excessive.

The rationale of security objectives demonstrates the following:

- Each threat, organizational security policies and assumptions will be addressed by at least one security objective.

- Each security objective addresses at least one threat, organizational security policy, assumptions.

[Table 4-1] Security Problem Definition and Security Objective

Security objectives Security problem definition	TOE Security objectives						Security objectives for the TOE operation environment					
	O.Audit	O.Management	O.Identification and authentication	O.Stored data protection	O.Transmission data protection	O.Intrusion detection & prevention	OE.Audit review	OE.Security maintenance	OE.Secure management	OE.Trusted administrator	OE.Trusted external server	OE.Secure key management
T.Disguising as administrator			X									
T.Recording failure	X											
T.Internal information leakage						X						
T.Unauthorized network access						X						
T.Continious authentication trials			X									
T.Reuse attack			X									
T.Damage to the stored data			X	X								
T.Damage to transmission data					X							
P.Audit	X						X					
P.Security maintenance								X				
P.Secure management		X							X			
A.Trusted administrator										X		
A.Trusted external server											X	
A.Secure key management												X

4.3.1 Rationale for Security Objective for TOE

O.Audit

The security objectives of TOE are to record the security-related audit events to trace responsibilities of the TOE security-related events, ensure to provide means for secure maintenance and review for the record audit events, and ensure to detect the identity of the attacker through audit record in case continuous authentication attempts. Therefore, the security objectives is necessary to respond to T.Recording failure and to P.Audit organizational security policy.

O.Management

The security objectives of TOE are to ensure to provide management means to the authorized administrator manage TOE in a normal and safe. Therefore, the security objectives are required to carry out P.Secure management of organizational security policy.

O.Identification and authentication

The security objectives of TOE ensure TOE to uniquely identify and authenticate the administrator and the wireless user. In addition, they lessen disguise and saved data damage threat by providing counter action if the failed administrator authentication attempts occur continuously and by ensuring ensure access to TOE by the authorized administrator and the wireless users. Therefore, the security objectives are required in responded to the following threats: T.Disguising administrator, T.Continuous authentication trials, T.Reuse attack, and T.Damage to the stored data.

O.Secure stored data

The security objectives of TOE ensure to protect stored TSF data in TOE from unauthorized exposure, modification and deletion. Therefore, the security objectives of TOE are required to counter the threat of T.Damage to the stored data.

O.Secure transmission data

The security objectives of TOE ensure to protect from unauthorized exposure and modification of the transmission data between TOE and the wireless user and to securely protect the transmission data between TOE and the administrator PC. Therefore, the security objectives are required to counter the threat of T.Damage to transmission data.

O.Intrusion detection and prevention

The security objectives of TOE ensure to detect and prevent intrusion into internal wireless network. Therefore, the security objectives are required to counter the threats of T.Internal information leakage and T.Unauthorized network access.

4.3.2 Rationale for Security Objective for TOE Environment

OE.Audit review

The security objectives for the operational environment ensure to review recorded data periodically and to maintain recorded data securely by using audit functions provided by TOE in order to trace responsibility for the security related to activities. Therefore, the security objectives are required to carry out organizational security policy of P.Audit.

OE.Security maintenance

The security objectives for the operational environment ensure the same level of security by reflecting the changed environment and security policy to TOE operation policy immediately when the internal network environment is changed by the change of internal network configuration, increase and decrease of host, and increase and decrease of service. Therefore, the security objectives are required to carry out organizational security policy of P.Security maintenance.

OE.Secure management

The security objectives for the operational environment ensure secure configuration, management and use of the security functions provided by TOE by the authorized administrator. Therefore, the security objectives are required to carry out organizational security policy of P.Secure Management.

OE.Trusted administrator

The security objectives for the operational environment ensure trustiness of the authorized administrator of TOE. Therefore, the security objectives are required to carry out organizational security policy of A.Trusted administrator.

OE.Trusted external server

The security objectives for the operational environment ensure trustiness of NTP Server that provides time stamp. Therefore, the security objectives are required to carry out organizational security policy of A. Trusted External Server.

OE.Secure key management

The security objectives for the operational environment ensure secure management of WLAN authorization key in the wireless device connected to WLAN of TOE. Therefore, the security objectives are required to carry out organizational security policy of P.Secure key management.

5 Extended components definition

This Security Target does not include components that are extended in the Common Criteria for Information Technology Security Evaluation part 2 and part 3.

6 Security requirements

This section describes the security function requirements and the security assurance requirements to be satisfied by the TOE.

This ST defines all subjects, objects, operations, security attributes, and external entities etc. which are used in security requirements as follows.

a) Subject, Object, Operation, security attribute

[Table 6-1] Define of subject, object, related security attribute, operation

SFR	Subject	Security attribute of subject	Object (Information)	Security attribute of object	Operation
FAU_ARP.1	TOE	-	potential security violation events	Potential violation analysis rule	Security alarms
FAU_GEN.1	TOE	-	Auditable events	Date and time of the event, type of event, subject identity, the outcome of the event	Audit data generation
FAU_GEN.2	TOE	-	Auditable events	Auditable events, subject identity	Association of events and identity
FAU_SAA.1	TOE	-	Audit records	Security threat on more than the set security level	Potential violation analysis
FAU_SAR.1	Authorized administrator	ID, Security information, IP address	Audit records	-	Read
FAU_SAR.2	TOE	-	Audit records	-	Read prohibition
FAU_STG.1	TOE	-	Audit trail storage	-	Prevention of deletion and modification

FAU_STG.3	TOE	-	Audit trail storage	The use of the third partition's capacity on the ROM exceeds 90%	Occurrence of alert window
FAU_STG.4	TOE	-	Audit trail storage	The space less than 1%	Ignore audited events, Occurrence of alert window
FCS_CKM.1(1)	TOE	-	Cryptographic key	-	Generation
FCS_CKM.1(2)	TOE	-	Cryptographic key	-	Generation
FCS_CKM.1(3)	TOE	-	Cryptographic key		Generation
FCS_CKM.2(1)	TOE	-	Cryptographic key	-	Distribution
FCS_CKM.2(2)	TOE	-	Cryptographic key	-	Distribution
FCS_CKM.2(3)	TOE	-	Cryptographic key	-	Distribution
FCS_CKM.4(1)	TOE	-	Cryptographic key	-	Destruction
FCS_CKM.4(2)	TOE	-	Cryptographic key	-	Destruction
FCS_CKM.4(3)	TOE	-	Cryptographic key	-	Destruction
FCS_COP.1(1)	TOE	-	Sending/receiving data	Administrator data	Encryption, Decryption
FCS_COP.1(2)	TOE	-	Sending/receiving data	Administrator data	Encryption, Decryption
FCS_COP.1(3)	TOE	-	Sending/receiving data	Administrator data, wireless user data	Encryption, Decryption
FDP_IFC.1	TOE	-	External entity(AP)		Allow an information flow, Disconnection an information flow
	TOE	-	External		Allow an

			entity(Station)		information flow, Disconnection an information flow
FDP_IFF.1	TOE	-	External entity(AP)		Detection, warning, disconnection
	TOE	-	External entity(Station)		Detection, warning, disconnection
FIA_AFL.1	TOE	-	Identification and authentication	Number of authentication attempts	Authentication locking
FIA_ATD.1	TOE	-	User attribute	ID, Confidential information, Connection allowed IP address	Maintain the list of security attributes
FIA_SOS.1	TOE	-	Confidential information	Password quality metric	Quality metric verification
FIA_UAU.2(1)	TOE	-	Administrator attribute	Confidential information	Perform an authentication
FIA_UAU.2(2)	TOE	-	External entity(Station) attribute	Confidential information	Perform an authentication
FIA_UAU.7	TOE	-	Administrator, Wireless User	Confidential information	Protected authentication feedback
FIA_UID.2(1)	TOE	-	Administrator attribute	ID, IP address	Perform an identification
FIA_UID.2(2)	TOE	-	External entity(Station) attribute		Perform an identification
FIA_USB.1	TOE	-	Administrator attribute, subject attribute	Password, Connection allowed IP address	User-subject binding, log record
FMT_MOF.1	Authorized	ID, Confidential	Time synchronizatio	NTP Server hostname	Determine the behavior of,

	administrator	information, IP address	n		disable, enable
			Administrator information setting	Password, Connection allowed IP address	Determine the behavior of
			Integrity check	-	Determine the behavior of, disable, enable
			WLAN Authentication and cryptographic rule setting	Authentication rule, cryptographic rule	Determine the behavior of, disable, enable, modify
			WIDPS security function		Determine the behavior of, disable, enable
FMT_MSA.1	Authorized administrator	ID, Confidential information, IP address	[WIDPS] Policy	Security level, action	Change_default, modify
			[WIDPS] Wireless security policy	Channel-2.4GHz, Channel-5GHz, authentication, cryptographic	Modify
			[WIDPS] Whitelist		Query, modify delete, generation
FMT_MSA.3	Authorized administrator	ID, Confidential information, IP address	[WIDPS] Policy	Security level, action	Default values initialization
FMT_MTD.1	Authorized administrator	ID, Confidential information, IP address	Administrator password	-	modify
			Connection allowed IP	-	modify delete, generation
			Audit data	-	Query
			WLAN cryptographic	-	Query, modify delete, generation

FMT_MTD.2	TOE	-	Administrator password	Password maintenance period	Display the password change message
FMT_SMF.1	-	-	-	-	-
FMT_SMR.1	TOE	-	Authorized administrator roles	ID, Confidential information, roles	administrator-roles association
FPT_FLS.1	TOE	-	TSF executable process	-	Re-execution
FPT_TST.1	TOE	-	WLAN setting file, TSF executable code	Self-test interval	Verification the integrity
FTA_MCS.1	TOE	-	Administrator session	Limitation on multiple concurrent sessions	Disconnection
FTA_SSL.3	TOE	-	Administrator session	Time interval of inactivity	Session termination
FTA_SSL.4(1)	Authorized administrator	ID, Confidential information, IP address	Session termination function	-	Session termination
FTA_SSL.4(2)	Wireless user	Confidential information, MAC address	Session termination function	-	Session termination
FTA_TSE.1	TOE	-	External entity(Station)	IP address	Deny of session establishment
FTP_TRP.1(1)	TOE	Administrator Identification and authentication information	Administrator	ID, Confidential information, IP address, SSL packet	Trusted path establishment

FTP_TRP.1(2)	TOE	Administrator Identification and authentication information	Administrator	ID, Confidential information, IP address, SSH packet	Trusted path establishment
FTP_TRP.1(3)	TOE	SSID, Confidential information	Wireless User	Confidential information, MAC address, WLAN 2.4GHz band	Trusted path establishment
FTP_TRP.1(4)	TOE	SSID, Confidential information	Wireless User	Confidential information, MAC address, WLAN 5GHz band	Trusted path establishment

b) External entity

[Table 6-2] Define of external entity

External entity	Description
AP (Access Point)	An Access Point (AP) is a bridge device that relay frames received from other station to another station and allows wireless devices to connect to a wired network.
Station (Wireless Client)	Station (Wireless Client) is a device that equips WNIC (Wireless Network Interface card) and works on Physical and MAC layers based on IEEE 802.11 standard.
NTP Server	NTP stands for 'Network Time Protocol' and is a protocol for synchronizing computers' system time through network. NTP server serves a role of sending time to a client which requests time through the protocol.

6.1 Security function requirements

The Security Target composes of function components in Common Criteria Part 2. Components of TOE security function requirements to satisfy TOE ST identified in section 4 are summarized as the table below.

[Table 6-3] Security function requirements

Class	Component	
Security audit (FAU)	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
Cryptographic support (FCS)	FCS_CKM.1(1)	Cryptographic key generation (SSL)
	FCS_CKM.1(2)	Cryptographic key generation (SSH)
	FCS_CKM.1(3)	Cryptographic key generation (WLAN)
	FCS_CKM.2(1)	Cryptographic key distribution (SSL)
	FCS_CKM.2(2)	Cryptographic key distribution (SSH)
	FCS_CKM.2(3)	Cryptographic key distribution (WLAN)
	FCS_CKM.4(1)	Cryptographic key destruction (SSL)
	FCS_CKM.4(2)	Cryptographic key destruction (SSH)
	FCS_CKM.4(3)	Cryptographic key destruction (WLAN)
	FCS_COP.1(1)	Cryptographic operation (SSL)
	FCS_COP.1(2)	Cryptographic operation (SSH)
	FCS_COP.1(3)	Cryptographic operation (WLAN)
User data protection (FDP)	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
Identification and authentication (FIA)	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.2(1)	User authentication before any action (Administrator)
	FIA_UAU.2(2)	User authentication before any action (Wireless User)
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2(1)	User identification before any action (Administrator)
	FIA_UID.2(2)	User identification before any action (Wireless User)
	FIA_USB.1	User-subject binding
Security management (FMT)	FMT_MOF.1	Management of security functions behavior
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data

	FMT_MTD.2	Management of limits on TSF data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_FLS.1	Failure with preservation of secure state
	FPT_TST.1	TSF testing
TOE access (FTA)	FTA_MCS.1	Basic limitation on multiple concurrent sessions
	FTA_SSL.3	TSF-initiated termination
	FTA_SSL.4(1)	User-initiated termination (Administrator)
	FTA_SSL.4(2)	User-initiated termination (Wireless user)
	FTA_TSE.1	TOE session establishment
Trusted path/channels (FTP)	FTP_TRP.1(1)	Trusted path (SSL)
	FTP_TRP.1(2)	Trusted path (SSH)
	FTP_TRP.1(3)	Trusted path (WLAN 2.4GHz)
	FTP_TRP.1(4)	Trusted path (WLAN 5GHz)

6.1.1 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 [alert a pop-up window on management UI that authorized administrator is logged in] 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 of [Table 6-4]]

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 PP/ST, [Additional audit record]

[Table 6-4] Auditable events and Additional audit record

Component	Auditable events	Additional audit record
FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms	-
FAU_SAR.1	Reading of information from the audit records	-
FDP_IFF.1	The specific security attributes used in making an information flow enforcement decision	Security Level
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions	-
FIA_SOS.1	Rejection by the TSF of any tested secret	-
FIA_UAU.2(1)	Unsuccessful use of the authentication mechanism	-
FIA_UAU.2(2)		
FIA_UID.2(1)	Unsuccessful use of the user identification mechanism, including the user identity provided	-
FIA_UID.2(2)		
FIA_USB.1	Modification of administrator password and Allowed IP address	
FMT_MOF.1	All modifications in the behavior of the functions in the TSF	-
FMT_MSA.1	All modifications of the values of security attributes	-
FMT_SMF.1	Use of the management functions	-
FPT_TST.1	Execution of the TSF self-tests and the results of the tests	Corrupt TSF data or executable code at the time of integrity violation
FTA_SSL.3	Termination of an interactive session by the session locking mechanism	-

FAU_GEN.2 **User identity association**

Hierarchical to: 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.

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 [Security Level] known to indicate a potential security violation;

b) [The security threat above the set security level]

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 [Authorized administrator] with the capability to read [assignment: list of audit information] from the audit records.

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

FAU_SAR.2 Restricted audit review

Hierarchical to: 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.

FAU_STG.1 Protected audit trail storage

Hierarchical to: 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 unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to *prevent* unauthorized modifications to the stored audit records in the audit trail.

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 [pop up an alert window about the audit storage use at management UI login] if the audit trail exceeds [90% of the third partition's capacity on the ROM].

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 *ignore audited events* and [pop up a window asking whether to delete audit data older than 1 year at management UI login, followed by an audit storage saturation alert window] if the audit trail is full.

6.1.2 Cryptographic support

FCS_CKM.1(1) Cryptographic key generation (SSL)

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 [TLS Handshake Protocol - Pseudorandom Function (PRF)] and specified cryptographic key sizes [48 byte] that meet the following: [RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2].

Application Note: The cryptographic keys (Master secret) described in this requirement are used to encrypt data transmitted between TOE and administrator's PC through SSL communication.

FCS_CKM.1(2) Cryptographic key generation (SSH)

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 [Kex algorithms - ssh-dss/ssh-rsa] and specified cryptographic key sizes [more than 1024 bit] that meet the following: [RFC 4253, The Secure Shell (SSH) Transport Layer Protocol Version 2].

Application Note: The cryptographic keys described in this requirement are used to encrypt data transmitted between TOE and administrator PC through SSH. And the Keys are generated separately.

FCS_CKM.1(3) Cryptographic key generation(WLAN)

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 [PBKDF2-SHA1] and specified cryptographic key sizes [256 bit] that meet the following: [IEEE 802.11i WPA/WPA2 PSK (Pre-Shared Key)].

Application Note: Cryptographic Key (PSK) denoted in this requirements is a Master Key (PMK, Pairwise Master Key) that provides secure communications of user data between wireless users connected to the TOE and TOE's WLAN, and this key is retrieved from WLAN password and SSID. WLAN password is set by an authorized administrator and shared with wireless users before communications. Later on, actual cryptographic key for a secure communication between an actual wireless user and TOE is retrieved from the Master key.

Application Note: The generation algorithm of cryptographic keys described in this requirement is implemented by IEEE 802.11i which is supported by TOE's OS.

FCS_CKM.2(1) Cryptographic key distribution (SSL)

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_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [TLS Handshake Protocol - Key exchange] that meets the following: [RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2].

Application Note: The cryptographic keys described in this requirement are used to encrypt data transmitted between TOE and administrator's PC through SSL; and the Keys are distributed separately.

FCS_CKM.2(2) Cryptographic key distribution (SSH)

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_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [SSH Key Exchange] that meets the following: [RFC 4253, The Secure Shell (SSH) Transport Layer Protocol Version 2].

Application Note: The cryptographic keys described in this requirement are used to encrypt data transmitted between TOE and administrator's PC through SSH; and the Keys are distributed separately.

FCS_CKM.2(3) Cryptographic key distribution (SSH)

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_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [4-Way Handshake, Group Key Handshake] that meets the following: [IEEE 802.11i WPA/WPA2 PSK (Pre-Shared Key)].

Application Note: The cryptographic keys described in this requirement are used to encrypt data transmitted between TOE and Wireless users connected to TOE's WLAN; and the Keys are distributed separately.

Application Note: The distribution method of cryptographic keys described in this requirement is implemented by IEEE 802.11i which is supported by TOE's OS.

FCS_CKM.4(1) Cryptographic key destruction (SSL)

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 [zeroization of all plaintext cryptographic keys and all other critical cryptographic security parameters] that meets the following: [FIPS PUB 140-2].

Application Note: The cryptographic keys described in this requirement saved on the TOE's ROM and the destruction of the cryptographic keys are assured when TOE and administrator's PC are disconnected.

FCS_CKM.4(2) Cryptographic key destruction (SSH)

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 [zeroization of all plaintext cryptographic keys and all other critical cryptographic security parameters] that meets the following: [FIPS PUB 140-2].

Application Note: The cryptographic keys described in this requirement saved on the TOE's ROM and the destruction of the cryptographic keys are assured when TOE and administrator's PC are disconnected.

FCS_CKM.4(3) Cryptographic key destruction (WLAN)

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 [zeroization of all plaintext cryptographic keys and all other critical cryptographic security parameters] that meets the following: [FIPS PUB 140-2].

Application Note: The cryptographic keys described in this requirement saved on the TOE's ROM and the destruction of the cryptographic keys are assured when TOE and administrator's PC are disconnected.

FCS_COP.1(1) Cryptographic operation (SSL)

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 [communication data encryption or decryption between the TOE and administrator's PC] in accordance with a specified cryptographic algorithm [AES_128_GCM] and cryptographic key sizes [128bit] that meet the following: [RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2의 TLS Record Protocol].

FCS_COP.1(2) Cryptographic operation (SSH)

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 [communication data encryption or decryption between the TOE and administrator's PC] in accordance with a specified cryptographic algorithm [AES256-CTR] and cryptographic key sizes [256bit] that meet the following: [RFC 4253, The Secure Shell (SSH) Transport Layer Protocol Version 2 - SSH data exchange].

FCS_COP.1(3) Cryptographic operation (WLAN)

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 [user data encryption or decryption between the TOE and wireless user] in accordance with a specified cryptographic algorithm [TKIP (Temporal Key Integrity CBC-MAC Protocol), CCMP (Counter Mode with CBC-MAC of the AES standard)] and cryptographic key sizes [256bit, 128bit] that meet the following: [IEEE 802.11i WPA/WPA2 PSK (Pre-Shared Key)].

Application Note: The cryptographic operation described in this requirement is implemented by IEEE 802.11i which is supported by TOE's OS.

6.1.3 User data protection

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [WIDPS policy of [Table 6-5]] on [Subject list, Information list, Operation list of [Table 6-5]].

[Table 6-5] Subject list, Information list, Operation list, WIDPS policy

Security threat	Subject list	Information list	Operation list	WIDPS policy
Rogue AP	TOE	External entity (AP)	Allow an information flow	Rogue AP detection
Rogue Station		External entity (Station)	Allow an information flow	Rogue Station detection
Mis-configured AP		External entity (AP)	Allow an information flow	Mis-configured AP detection
Client Mis-		External	Allow an	Client Mis-association

association		entity(Station)	information flow, Disconnection an information flow	detection and disconnection
		External entity (AP)		
Unauthorized Association		External entity(Station)	Allow an information flow, Disconnection an information flow	Unauthorized Association detection and disconnection
		External entity (AP)		
Ad-hoc Connection		External entity(Station)	Allow an information flow, Disconnection an information flow	Ad-hoc Connection detection and disconnection
AP MAC Spoofing		External entity (AP)	Allow an information flow	AP MAC Spoofing detection
Honeypot AP		External entity (AP)	Allow an information flow	Honeypot AP detection

FDP_IFF.1 **Simple security attributes**

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the [the WIDPS policy by security threat of the next [Table 6-7]] based on the following types of subject and information security attributes: [list of subjects and information by security threat of the next [Table 6-6], and for each, the security attributes].

[Table 6-6] List of subjects and information by security threat, and for each, the security attributes

Security threat	Subject list	Security attribute of subject	Information list	Security attribute of information
Rogue AP	TOE	Whitelist (AP)	External entity (AP)	-
Rogue Station		Whitelist (Station)	External entity (Station)	-
Mis-configured AP		Whitelist (AP), wireless security policy setting	External entity (AP)	-
Client Mis-association		Whitelist (Station)	External entity (Station)	-
		Whitelist (AP)	External entity (AP)	-
Unauthorized		Whitelist (Station)	External entity	-

Association			(Station)	
		Whitelist (AP)	External entity (AP)	-
Ad-hoc Connection		Whitelist (Station)	External entity (Station)	-
AP MAC Spoofing		Whitelist (AP)	External entity (AP)	-
Honeypot AP		Whitelist (AP)	External entity (AP)	-

[Table 6-7] WIDPS policy

WIDPS policy	Description
Rogue AP detection,	When attributes that are not in the TOE's whitelist are detected from external entity (AP) sent wireless network traffic, Rogue AP detection is logged as a security event and alert pops up via management UI's popup window to the authorized administrator, if the severity of the detected security threat is higher than the one set in the event alert configuration.
Rogue Station detection,	When attributes that are not in the TOE's whitelist are detected from external entity (Station) sent wireless network traffic, Rogue Station detection is logged as a security event and alert pops up via management UI's popup window to the authorized administrator, if the severity of the detected security threat is higher than the one set in the event alert configuration.
Mis-configured AP detection,	When attributes that are in the TOE's whitelist are detected and attributes of wireless security policy match from external entity (AP) sent wireless network traffic, mis-configured AP detection is logged as a security event and alert pops up via management UI's popup window to the authorized administrator, if the severity of the detected security threat is higher than the one set in the event alert configuration.
Client Mis-association detection and disconnection	When station's attributes that are in the TOE's whitelist and AP's attributes which are not in the TOE's whitelist are detected from wireless network traffic between External entities (AP and Station), Client Mis-association detection is logged as a security event. And if auto-disconnection option is set in configuration, the disconnection command is sent to external entity (Station). Also The detection is logged as a security event and alert pops up via management UI's popup window to the authorized administrator, if the severity of the detected security threat is higher than the one set in the event alert configuration.
Unauthorized Association detection and disconnection	When station's attributes that are not in the TOE's whitelist and AP's attributes are in the TOE's whitelist are detected from wireless network traffic between External entities (AP and Station), Unauthorized Association detection is logged as a security event. And if auto-disconnection option is set in

	configuration, the disconnection command is sent to external entity (Station). Also The detection is logged as a security event and alert pops up via management UI's popup window to the authorized administrator, if the severity of the detected security threat is higher than the one set in the event alert configuration.
Ad-hoc Connection detection and disconnection	When station's attributes that are not in the TOE's whitelist are detected from wireless network traffic between ad-hoc connected External entities (Station and Station), Ad-hoc Connection detection is logged as a security event. And if auto-disconnection option is set in configuration, the disconnection command is sent to External entity (Station). Also The detection is logged as a security event and alert pops up via management UI's popup window to the authorized administrator, if the severity of the detected security threat is higher than the one set in the event alert configuration.
AP MAC Spoofing detection	When attributes that are not in the TOE's whitelist and MAC address that is in the TOE's whitelist are detected from external entity (AP) sent wireless network traffic, AP MAC spoofing detection is logged as a security event and alert pops up via management UI's popup window to the authorized administrator, if the severity of the detected security threat is higher than the one set in the event alert configuration.
Honeypot AP detection	When attributes that are in the TOE's whitelist and MAC address that is not in the TOE's whitelist are detected from external entity (AP) sent wireless network traffic, Honeypot AP detection is logged as a security event and alert pops up via management UI's popup window to the authorized administrator, if the severity of the detected security threat is higher than the one set in the event alert configuration.

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:

[

a) Attributes of external entity (AP) match attributes of TOE's whitelist.

b) Attributes of external entity (Station) matches attributes of TOE's whitelist.

c) Attributes of external entity (AP) match attributes of TOE's whitelist and attributes of connected external entity (Station) match attributes of TOE's whitelist.

d) Attributes of external entity (Station) matches attributes of TOE's whitelist and attributes of Ad-hoc connected external entity (Station) match attributes of TOE's whitelist.

e) Attributes of external entity (Station) do not matches attributes of TOE's whitelist and attributes of Ad-hoc connected external entity (Station) do not match attributes of TOE's whitelist.

]

FDP_IFF.1.3 The TSF shall enforce the [None].

FDP_IFF.1.4 The TSF shall explicitly authorize 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].

6.1.4 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 log-in].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall [Authentication locking 5minute]

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [ID, Password, Allowed IP address].

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 defined password quality metric].

[

a) Only characters of 9~20bytes are allowed: uppercase alphabet letters (26: A~Z), lowercase alphabet letters (26: a~z), Number (10: 0~9), Special characters (33: `~!@#$%^&*()-_=+₩|[{]};:'",<.>/?blank)

b) Use one letter and a combination of at least three different kinds from above

c) Prohibit using the same character more than 3 times (e.g., aaa, 111, ### etc.)

d) Prohibit using any sequential pattern of letters or numbers that exceeds three characters long (e.g., abc, 123 etc.)

e) Prohibit using the same with an ID

]

FIA_UAU.2(1) User authentication before any action (Administrator)

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

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

FIA_UAU.2(2) User authentication before any action (Wireless User)

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

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

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 ["•"] to the **administrator** while the authentication is in progress.

FIA_UID.2(1) User identification before any action (Administrator)

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

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

FIA_UID.2(2) User identification before any action (Wireless User)

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

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

FIA_USB.1 User-subject binding

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1 The TSF shall associate the following **administrator** security attributes with subjects acting on the behalf of that **administrator**: [ID].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of **administrator** security attributes with subjects acting on the behalf of **administrator**: [at the time of the successful identification and authentication, the ID has to be successful administrator account in the authentication.]

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the **administrator** security attributes associated with subjects acting on the behalf of **administrator**: [at the time of the administrator password and connection allowed IP address changes, record in the administrator log]

6.1.5 Security management

FMT_MOF.1 Management of security functions behavior

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 *determine the behavior of, disable, enable, modify the behavior of* the functions [[Table 6-8]] to [authorized administrator].

[Table 6-8] Security function list and capability

Security function list	determine the behavior of	disable	enable	modify the behavior of
Time synchronization	O	O	O	-
Administrator information(Password, Connection allowed IP) setting	O	-	-	-
Integrity check	O	O	O	-
WLAN authentication and Cryptographic method setting	O	O	O	O
WIDPS Security function	O	O	O	-

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_SMR.1 Security roles

FMT_MSA.1.1 The TSF shall enforce the [WIDPS policy] to restrict the ability to *change_default, query, modify, delete, [generation]* the security attributes [[Table 6-9]] to [authorized administrator].

[Table 6-9] Management of security attributes

Classification	Security attributes	Change_default	Query	Modify	Delete	Generation
[WIDPS] Policy	Security level	○	-	○	-	-
	Action	○	-	○	-	-
[WIDPS] Wireless security policy	Channel-2.4GHz		-	○	-	-
	Channel-5GHz		-	○	-	-
	Authentication		-	○	-	-
	Cryptographic		-	○	-	-
[WIDPS] Whitelist	attributes		○	○	○	○

FMT_MSA.3 Static attribute initialization

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 [WIDPS Policy] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [authorized administrator] to specify alternative initial values to override the default values when an object or information is created.

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 *query, modify, delete, [generation]* the [[Table 6-10] list of TSF data] to [authorized administrator].

[Table 6-10] list of TSF data

List of TSF data	Query	Modify	Delete	Generation
Administrator password	-	○	-	-
Connection allowed IP	-	○	○	○
Audit data	○	-	-	-
WLAN cryptographic	○	○	○	○

FMT_MTD.2 **Management of limits on TSF data**

Hierarchical to: No other components.

Dependencies: FMT_MTD.1 Management of TSF data
FMT_SMR.1 Security roles

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [[Table 6-11] list of TSF data] to [authorized administrator].

FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [[Table 6-11] Reaction].

[Table 6-11] Reaction of limits on TSF data

List of TSF data	Reaction
Administrator password	Once a password is set and the period of time specified by an authorized administrator has passed, a message will appear requiring to change the password.

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: [[Table 6-12]].

[Table 6-12] Management functions to be provided by the TSF

Management function	List of management functions to be provided by the TSF
Security function management	The specify item in FMT_MOF.1
Security attribute management	The specify item in FMT_MSA.1, FMT_MSA.3
TSF data management	The specify item in FMT_MTD.1, FMT_MTD

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 [authorized administrator].

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

6.1.6 TSF protection

FPT_FLS.1 **Failure with preservation of secure state**

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [The abnormal shutdown of TSF executable process].

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*, *at the request of the authorized* ***administrator*** to demonstrate the correct operation of *[TSF executable file]*.

FPT_TST.1.2 The TSF shall provide authorized **administrator** with the capability to verify the integrity of *[WLAN setting file]*.

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

6.1.7 TOE access

FTA_MCS.1 Basic limitation on multiple concurrent sessions

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FTA_MCS.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same administrator.

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of [1] sessions per **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 [time interval of authorized administrator inactivity - elapse of 10 minute].

FTA_SSL.4(1) User-initiated termination (Administrator)

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Application Note: The requirement denotes termination of the administrator's own interactive session by logout of the management UI.

FTA_SSL.4(2) User-initiated termination (Wireless user)

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

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

Application Note: The requirement denotes termination of the wireless user's own interactive session by disconnection of the TOE's WLAN.

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 session establishment based on [administrator's IP address].

6.1.8 Trusted path/channels

FTP_TRP.1(1) Trusted path (SSL)

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

FTP_TRP.1.1 The TSF shall provide a communication path between itself and *remote* **administrator** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *modification, disclosure*.

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

FTP_TRP.1.3 The TSF shall require the use of the trusted path for *[management UI access]*.

Application Note: The requirement assures protection of the communicated data between the administrator and TOE through SSL. When the administrator accesses TOE management UI, TOE defines cryptographic algorithm and private key for communicated data encryption/decryption through TLS handshake; the TOE and administrator communicate through the defined algorithm and key. The TOE allows access to the management UI through SSL Communication only.

FTP_TRP.1(2) Trusted path (SSH)

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

FTP_TRP.1.1 The TSF shall provide a communication path between itself and *remote* **administrator** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *modification, disclosure*.

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

FTP_TRP.1.3 The TSF shall require the use of the trusted path for *[management CLI access]*.

Application Note: The requirement assures protection of the communicated data between the administrator and TOE through SSL. When the administrator accesses TOE management UI, TOE defines cryptographic algorithm and private key for communicated data encryption/decryption through SSH key exchange; the TOE and administrator communicate through the defined algorithm and key. The TOE allows access to the CLI through SSH Communication only.

FTP_TRP.1(3) Trusted path (WLAN 2.4GHz)

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

FTP_TRP.1.1 The TSF shall provide a communication path between itself and *remote* **wireless users** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *modification, disclosure*.

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

FTP_TRP.1.3 The TSF shall require the use of the trusted path for *[WLAN 2.4GHz access]*.

Application Note: The requirement assures protection of the communicated data between the TOE and wireless user who connected to the WLAN 2.4GHz through WPA/WPA2. When the wireless user connects to WLAN, TOE defines cryptographic algorithm and private key for communicated data encryption/decryption through 4-way handshake; the TOE and wireless user communicate through the defined algorithm and key. The TOE allows access to the WLAN through WPA/WPA2 only.

FTP_TRP.1(4) Trusted path (WLAN 5GHz)

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

FTP_TRP.1.1 The TSF shall provide a communication path between itself and *remote* **wireless users** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *modification, disclosure*.

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

FTP_TRP.1.3 The TSF shall require the use of the trusted path for *[WLAN 5GHz access]*.

Application Note: The requirement assures protection of the communicated data between the TOE and wireless user who connected to the WLAN 5GHz through WPA/WPA2. When the wireless user connects to WLAN, TOE defines cryptographic algorithm and private key for communicated data encryption/decryption through 4-way handshake; the TOE and wireless user communicate through the defined algorithm and key. The TOE allows access to the WLAN through WPA/WPA2 only.

6.2 TOE Security Assurance Requirements

Security assurance components, as defined in Common Criteria for Information Technology Security Evaluation part 3, are the basis for the security assurance requirements expressed in this Security Target. The evaluation assurance level is EAL2. Security assurance components are summarized in [Table 6-13].

[Table 6-13] Security Assurance Requirements

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

6.2.1 Development

ADV_ARC.1 Security architecture description

Dependencies: ADV_FSP.1 Basic functional specification
ADV_TDS.1 Basic design

Developer action elements:

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

Content and presentation elements:

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialization process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

Evaluator action elements:

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

ADV_FSP.2 Security-enforcing functional specification

Dependencies: ADV_TDS.1 Basic design

Developer action elements:

ADV_FSP.2.1D The developer shall provide a functional specification.

ADV_FSP.2.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:

ADV_FSP.2.1C The functional specification shall completely represent the TSF.

ADV_FSP.2.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5C For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

ADV_FSP.2.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

ADV_FSP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

ADV_TDS.1 Basic design

Dependencies: ADV_FSP.2 Security-enforcing functional specification

Developer action elements:

ADV_TDS.1.1D The developer shall provide the design of the TOE.

ADV_TDS.1.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements:

ADV_TDS.1.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.1.2C The design shall identify all subsystems of the TSF.

ADV_TDS.1.3C The design shall describe the behavior of each SFR-supporting or SFR-non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.

ADV_TDS.1.4C The design shall summarize the SFR-enforcing behavior of the SFR-enforcing subsystems.

ADV_TDS.1.5C The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

ADV_TDS.1.6C The mapping shall demonstrate that all TSFIs trace to the behavior described in the TOE design that they invoke.

Evaluator action elements:

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

ADV_TDS.1.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

6.2.2 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 should 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.

6.2.3 Life-cycle Support

ALC_CMC.2 Use of a CM system

Dependencies: ALC_CMS.1 TOE CM coverage

Developer action elements:

ALC_CMC.2.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.2.2D The developer shall provide the CM documentation.

ALC_CMC.2.3D The developer shall use a CM system.

Content and presentation elements:

ALC_CMC.2.1C The TOE shall be labelled with its unique reference.

ALC_CMC.2.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.2.3C The CM system shall uniquely identify all configuration items.

Evaluator action elements:

ALC_CMC.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_CMS.2 Parts of the TOE CM coverage

Dependencies: No dependencies.

Developer action elements:

ALC_CMS.2.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.2.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.

ALC_CMS.2.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.2.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements:

ALC_CMS.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DEL.1 Delivery procedures

Dependencies: No dependencies.

Developer action elements:

ALC_DEL.1.1D The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation elements:

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

Evaluator action elements:

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

6.2.4 Security Target

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 identify the TOE.

ASE_INT.1.4C The TOE overview shall summarize 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_INT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_INT.1.2E 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_SPD.1 Security problem definition

Dependencies: No dependencies.

Developer action elements:

ASE_SPD.1.1D The developer shall provide a security problem definition.

Content and presentation elements:

ASE_SPD.1.1C The security problem definition shall describe the threats.

ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

ASE_SPD.1.3C The security problem definition shall describe the OSPs.

ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

Evaluator action elements:

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

ASE_OBJ.2 **Security objectives**

Dependencies: ASE_SPD.1 Security problem definition

Developer action elements:

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.

ASE_OBJ.2.2D The developer shall provide a security objectives rationale.

Content and presentation elements:

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

Evaluator action elements:

ASE_OBJ.2.1E 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.2 Derived security requirements

Dependencies: ASE_OBJ.2 Security objectives
ASE_ECD.1 Extended components definition

Developer action elements:

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a security requirements rationale.

Content and presentation elements:

ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.2.2C 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.2.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.4C All operations shall be performed correctly.

ASE_REQ.2.5C ach dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.2.9C The statement of security requirements shall be internally consistent.

Evaluator action elements:

ASE_REQ.2.1E 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.

6.2.5 Tests

ATE_COV.1 **Evidence of coverage**

Dependencies: ADV_FSP.2 Security-enforcing functional specification
ATE_FUN.1 Functional testing

Developer action elements:

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation elements:

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

Evaluator action elements:

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

ATE_FUN.1 **Functional testing**

Dependencies: ATE_COV.1 Evidence of coverage

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

Evaluator action elements:

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

ATE_IND.2 Independent testing - sample

Dependencies: ADV_FSP.2 Security-enforcing functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures
ATE_COV.1 Evidence of coverage
ATE_FUN.1 Functional testing

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

6.2.6 Vulnerability assessment

AVA_VAN.2 Vulnerability analysis

Dependencies: ADV_ARC.1 Security architecture description
ADV_FSP.1 Security-enforcing functional specification
ADV_TDS.1 Basic design
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

Developer action elements:

AVA_VAN.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.2.1C The TOE shall be suitable for testing.

Evaluator action elements:

AVA_VAN.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.2.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3E The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4E 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.

6.3 Rationale for Security Requirements

This chapter will demonstrate that the security requirements of the ST meet the security objectives and appropriately control the security issues.

6.3.1 Rationale of security function requirements

The supporting rationale of security functional requirements demonstrate the following facts.

- Each TOE security objective traces back to at least one TOE security functional requirement.
- Each TOE security functional requirement addresses at least one TOE security objective.

[Table 6-14] Security objectives and security function requirements response

Security objectives Security functional requirements	O.Audit	O.Management	O.Identification and authentication	O.Stored data protection	O.Transmission data protection	O.Intrusion Detection & Prevention
FAU_ARP.1	X					X
FAU_GEN.1	X					
FAU_GEN.2	X					
FAU_SAA.1	X					
FAU_SAR.1	X					
FAU_SAR.2	X		X			
FAU_STG.1	X					
FAU_STG.3	X					
FAU_STG.4	X					
FCS_CKM.1(1)					X	
FCS_CKM.1(2)					X	
FCS_CKM.1(3)					X	
FCS_CKM.2(1)					X	
FCS_CKM.2(2)					X	
FCS_CKM.2(3)					X	
FCS_CKM.4(1)					X	
FCS_CKM.4(2)					X	
FCS_CKM.4(3)					X	
FCS_COP.1(1)					X	
FCS_COP.1(2)					X	
FCS_COP.1(3)					X	
FDP_IFC.1						X
FDP_IFF.1						X
FIA_AFL.1			X			
FIA_ATD.1	X		X			
FIA_SOS.1			X			
FIA_UAU.2(1)			X			

FIA_UAU.2(2)			X			
FIA_UAU.7			X			
FIA_UID.2(1)			X			
FIA_UID.2(2)			X			
FIA_USB.1			X			
FMT_MOF.1		X				
FMT_MSA.1		X				
FMT_MSA.3		X				
FMT_MTD.1		X				
FMT_MTD.2		X				
FMT_SMF.1		X				
FMT_SMR.1		X				
FPT_FLS.1		X				
FPT_TST.1		X		X		
FTA_MCS.1		X	X			
FTA_SSL.3		X	X			
FTA_SSL.4(1)		X	X			
FTA_SSL.4(2)			X			
FTA_TSE.1		X	X			
FTP_TRP.1(1)			X		X	
FTP_TRP.1(2)			X		X	
FTP_TRP.1(3)			X		X	
FTP_TRP.1(4)			X		X	

FAU_ARP.1 Security alarms

As this component ensures the capability of performing appropriate countermeasures in case of detecting potential security violations, it satisfies the TOE security objectives O.Audit, O.Intrusion detection and prevention.

FAU_GEN.1 Audit data generation

As this component ensures the capability of defining auditable events and creating audit records, it satisfies the TOE security objectives O.Audit.

FAU_GEN.2 User identity association

As this component ensures the capability of relating user's identity and auditable events, it satisfies the TOE security objectives O.Audit.

FAU_SAA.1 Potential violation analysis

As this component ensures the capability of inspecting audited events to point out security violations, it satisfies the TOE security objectives O.Audit.

FAU_SAR.1 Audit review

As this component ensures the authorized log administrator to review audit records, it satisfies the TOE security objectives O.Audit.

FAU_SAR.2 Restricted audit review

As this component ensures the capability of prohibiting all users – not including authorized administrators - from reading audit records, it satisfies the TOE security objectives O.Audit, O.Identification and authentication.

FAU_STG.1 Protected audit trail storage

As this component ensures the capability of protecting audit trails from unauthorized changes and deletions, it satisfies TOE security objectives O.Audit.

FAU_STG.3 Action in case of possible audit data loss

As this component ensures the capability of performing countermeasures when the audit trail exceeds the pre-defined threshold, it satisfies TOE security objectives O.Audit.

FAU_STG.4 Prevention of audit data loss

As this component ensures the capability of performing countermeasure when the audit trail exceeds the pre-defined threshold, it satisfies the TOE security objectives O.Audit.

FCS_CKM.1(1) Cryptographic key generation (SSL)

As this component ensures the capability of creating cryptographic keys in accordance with the specified cryptographic key algorithm and cryptographic key length, and protecting transmitted data based on the created cryptographic keys, it satisfies the TOE security objectives O.Transmission data protection.

FCS_CKM.1(2) Cryptographic key generation(SSH)

As this component ensures the capability of creating cryptographic keys in accordance with the specified cryptographic key algorithm and cryptographic key length, and protecting transmitted data based on the created cryptographic keys, it satisfies the TOE security objectives O.Transmission data protection.

FCS_CKM.1(3) Cryptographic key generation (WLAN)

As this component ensures the capability of creating cryptographic keys in accordance with the specified cryptographic key algorithm and cryptographic key length, and protecting transmitted data based on the created cryptographic keys, it satisfies the TOE security objectives O.Transmission data protection.

FCS_CKM.2(1) Cryptographic key distribution (SSL)

As this component ensures the capability of distributing cryptographic keys in accordance with the specified cryptographic key distribution method, and protecting transmitted data based on the distributed cryptographic keys, it satisfies the TOE security objectives O.Transmission data protection.

FCS_CKM.2(2) Cryptographic key distribution (SSH)

As this component ensures the capability of distributing cryptographic keys in accordance with the specified cryptographic key distribution method, and protecting transmitted data based on the distributed cryptographic keys, it satisfies the TOE security objectives O.Transmission data protection.

FCS_CKM.2(3) Cryptographic key distribution (WLAN)

As this component ensures the capability of distributing cryptographic keys in accordance with the specified cryptographic key distribution method, and protecting transmitted data based on the distributed cryptographic keys, it satisfies the TOE security objectives O.Transmission data protection.

FCS_CKM.4(1) Cryptographic key destruction (SSL)

As this component ensures the capability of destroying cryptographic keys used for transmitted data encryption/decryption in accordance with the specified cryptographic key destruction method, it satisfies the TOE security objectives O.Transmission data protection.

FCS_CKM.4(2) Cryptographic key destruction (SSH)

As this component ensures the capability of destroying cryptographic keys used for transmitted data encryption/decryption in accordance with the specified cryptographic key destruction method, it satisfies the TOE security objectives O.Transmission data protection.

FCS_CKM.4(3) Cryptographic key destruction (WLAN)

As this component ensures the capability of destroying cryptographic keys used for transmitted data encryption/decryption in accordance with the specified cryptographic key destruction method, it satisfies the TOE security objectives O.Transmission data protection.

FCS_COP.1(1) Cryptographic operation (SSL)

As this component ensures the capability of encrypting or decrypting communicated data between the TOE and administrator PC by performing cryptographic operation in accordance with the specified cryptographic algorithm and cryptographic key length, it satisfies the TOE security objectives O.Transmission data protection.

FCS_COP.1(2) Cryptographic operation (SSH)

As this component ensures the capability of encrypting or decrypting communicated data between the TOE and administrator PC by performing cryptographic operation in accordance with the specified cryptographic algorithm and cryptographic key length, it satisfies the TOE security objectives O.Transmission data protection.

FCS_COP.1(3) Cryptographic operation (WLAN)

As this component ensures the capability of encrypting or decrypting communicated data between the TOE and administrator PC by performing cryptographic operation in accordance with the specified cryptographic algorithm and cryptographic key length, it satisfies the TOE security objectives O.Transmission data protection.

FDP_IFC.1 Subset information flow control

As this component ensures the capability of detecting and preventing wireless threats managed by the TOE in accordance with the WIDPS security policies of the TOE, it satisfies the TOE security objectives O.Intrusion Detection & Prevention.

FDP_IFF.1 Simple security attributes

As this component ensures the capability of detecting and preventing wireless threats managed by the TOE in accordance with the attributes of the WIDPS security policies of the TOE, it satisfies the TOE security objectives O.Intrusion Detection & Prevention.

FIA_AFL.1 Authentication failure handling

As this component defines the number of allowed failed login attempts and ensures the capability of performing countermeasure when the failed login attempts reach or exceed the limit, it satisfies the TOE security objectives O.Identification and authentication.

FIA_ATD.1 User attribute definition

As this component ensures the capability of managing administrator's security attributes list, it satisfies the TOE security objectives O.Identification and authentication.

FIA_SOS.1 Verification of secrets

As this component ensures the capability of verifying check if the password meets the defined acceptance criteria, it satisfies the TOE security objectives O.Identification and authentication.

FIA_UAU.2(1) User authentication before any action (Administrator)

As this component ensures the capability of authenticating authorized administrator successfully, it satisfies the TOE security objectives O.Identification and authentication.

FIA_UAU.2(2) User authentication before any action (Wireless User)

As this component ensures the capability of authenticating wireless users successfully, it satisfies the TOE security objectives O.Identification and authentication.

FIA_UAU.7 Protected authentication feedback

As this component ensures the capability of authenticating administrator, it satisfies the TOE security objectives O.Identification and authentication.

FIA_UID.2(1) User identification before any action (Administrator)

As this component ensures the capability of identifying administrator, it satisfies the TOE security objectives O.Identification and authentication.

FIA_UID.2(2) User identification before any action (Wireless User)

As this component ensures the capability of identifying wireless user, it satisfies the TOE security objectives O.Identification and authentication.

FIA_USB.1 User-subject binding

As this component ensures the capability of binding authorized administrator and active subject, it satisfies the TOE security objectives O.Identification and authentication.

FMT_MOF.1 Management of security functions behavior

As this component ensures the capability of managing security functions by an authorized administrator, it satisfies the TOE security objectives O.Management.

FMT_MSA.1 Management of security attributes

As this component ensures the capability of managing security attributes by an authorized administrator, it satisfies the TOE security objectives O.Management.

FMT_MSA.3 Static attribute initialization

As this component ensures the capability of initializing security attributes by an authorized administrator, it satisfies the TOE security objectives O.Management.

FMT_MTD.1 Management of TSF data

As this component ensures the capability of managing TSF data and identification/authentication data by an authorized administrator, it satisfies the TOE security objectives O.Management.

FMT_MTD.2 Management of limits on TSF data

As this component ensures the capability of managing TSF data by an authorized administrator, it satisfies the TOE security objectives O.Management.

FMT_SMF.1 Specification of Management Functions

As this component ensures the capability of using management functions of TSF provided data and security functions, it satisfies the TOE security objectives O.Management.

FMT_SMR.1 Security roles

As this component ensures the capability of binding a role with an administrator, it satisfies the TOE security objectives O.Management.

FPT_FLS.1 Failure with preservation of secure state

As this component ensures the capability of preserving secure state at abnormal terminations of major processes, it satisfies the TOE security objectives O.Management.

FPT_TST.1 TSF testing

As this component ensures TSF testing for accurate operation and the capability of verifying integrity of authenticated administrator's TSF data and executable codes, it satisfies the TOE security objectives O.Management, O.Stored data protection.

FTA_MCS.1 Basic limitation on multiple concurrent sessions

As this component ensures the capability of limiting multiple concurrent sessions by an identical user, it satisfies the TOE security objectives O.Management, O.Identification and authentication.

FTA_SSL.3 TSF-initiated termination

As this component ensures the capability of terminating administrator's session when administrator remains inactive for a specified time, it satisfies the TOE security objectives O.Management, O.Identification and authentication.

FTA_SSL.4(1) User-initiated termination (Administrator)

As this component ensures an administrator of the capability of terminating own interactive session, it satisfies the TOE security objectives O.Management, O.Identification and authentication.

FTA_SSL.4(2) User-initiated termination (Wireless user)

As this component ensures a wireless user of the capability of terminating own interactive session, it satisfies the TOE security objectives O.Identification and authentication.

FTA_TSE.1 TOE session establishment

As this component ensures the capability of rejecting a session establishment with the unallowed IP address based on the authorized administrator's IP address, it satisfies the TOE security objectives O.Management, O.Identification and authentication.

FTP_TRP.1(1) Trusted path (SSL)

As this component ensures the capability of providing communication path which protects communicated data between an administrator and TOE, initializing communication through trusted path by remote administrator, and enforcing use of trusted path for a management UI access, it satisfies the TOE security objectives O.Identification and authentication, O.Transmission data protection.

FTP_TRP.1(2) Trusted path (SSH)

As this component ensures the capability of providing communication path which protects communicated data between an administrator and TOE, initializing communication through trusted path by remote administrator, and enforcing use of trusted path for a management CLI access, it satisfies the TOE security objectives O.Identification and authentication, O.Transmission data protection.

FTP_TRP.1(3) Trusted path (WLAN 2.4GHz)

As this component ensures the capability of providing communication path which protects communicated data between an administrator and TOE, initializing communication through trusted path by remote administrator, and enforcing use of trusted path for a WLAN 2.4GHz connection , it satisfies the TOE security objectives O.Identification and authentication, O.Transmission data protection.

FTP_TRP.1(4) Trusted path (WLAN 5GHz)

As this component ensures the capability of providing communication path which protects communicated data between an administrator and TOE, initializing communication through trusted path by remote administrator, and enforcing use of trusted path for a WLAN 5GHz connection , it satisfies the TOE security objectives O.Identification and authentication, O.Transmission data protection.

6.3.2 Rationale of security assurance requirements

The assurance level for this Security Target is EAL2.

EAL2 is an assurance package that requires a structural test and the cooperation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 can be applied in situations when developers of users require a low to moderate level of independently assured security in the absence of availability of the complete development records. Such a situation may arise when securing existing systems, or where access to the developer may be limited.

EAL2 provides assurance with the functional and interface specification, operational user guides, testing results, a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guide evidence provided) demonstrating resistance to penetration attackers with a basic attack potential, and a basic description of the architecture of the TOE, to understand security behaviors. EAL2 also provides assurance with the evidence of the CM system and the secure distribution procedures.

6.4 Rationale for dependency

6.4.1 Dependencies of security functional requirements

Security functional requirements defined in this ST satisfies dependency as the table below and there are no components not satisfying dependency.

[Table 6-15] Dependencies of the functional components

Number	Functional component	Dependencies	Reference number
1	FAU_ARP.1	FAU_SAA.1	4
2	FAU_GEN.1	FPT_STM.1	OE.Trusted external server
3	FAU_GEN.2	FAU_GEN.1 FIA_UID.1	2 21 (FIA_UID.2)
4	FAU_SAA.1	FAU_GEN.1	2
5	FAU_SAR.1	FAU_GEN.1	2
6	FAU_SAR.2	FAU_SAR.1	5
7	FAU_STG.1	FAU_GEN.1	2
8	FAU_STG.3	FAU_STG.1	7
9	FAU_STG.4	FAU_STG.1	7
10	FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	11 or 13 12

11	FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	10 12
12	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	10
13	FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	10 12
14	FDP_IFC.1	FDP_IFF.1	15
15	FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	15 25
16	FIA_AFL.1	FIA_UAU.1	19 (FIA_UAU.2)
17	FIA_ATD.1	-	-
18	FIA_SOS.1	-	-
19	FIA_UAU.2	FIA_UID.1	21 (FIA_UID.2)
20	FIA_UAU.7	FIA_UAU.1	19 (FIA_UAU.2)
21	FIA_UID.2	-	-
22	FIA_USB.1	FIA_ATD.1	17
23	FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	28 29
24	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	14 28 29
25	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	24 29
26	FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	28 29
27	FMT_MTD.2	FMT_MTD.1 FMT_SMR.1	26 29
28	FMT_SMF.1	-	-
29	FMT_SMR.1	FIA_UID.1	21 (FIA_UID.2)
30	FPT_FLS.1	-	-
31	FPT_TST.1	-	-
32	FTA_MCS.1	FIA_UID.1	21 (FIA_UID.2)
33	FTA_SSL.3	-	-
34	FTA_SSL.4	-	-
35	FTA_TSE.1	-	-
36	FTP_TRP.1	-	-

FAU_GEN.1 dependencies on FPT_STM.1, but the dependencies of FAU_GEN.1 are satisfied with security objectives for operating environments OE.Trusted external server instead of FPT_STM.1

because security-related events are accurately recorded with the trusted timestamps provided by the TOE operating environment.

FAU_GEN.2, FIA_UAU.2, FMT_SMR.1 dependencies on FIA_UID.1, but the dependencies are satisfied with FIA_UID.2 that is hierarchical to them.

FIA_AFL.1, FIA_UAU.7 dependencies on FIA_UAU.1, but the dependencies are satisfied with FIA_UAU.2 that is hierarchical to them.

6.4.2 Dependencies of security assurance requirements

The dependencies of each assurance package provided by the Common Criteria for Information Technology Security Evaluation are already satisfied.

7 TOE Summary specification

This section describes TOE security functions, including all security functions described in the security requirements.

7.1 Security audit

Security auditing features provided by the management UI are audit log generation, audit log query, selectable audit record query, audit data loss prevention and security alarms log.

7.1.1 Security log generation

TOE generates audit logs when all audit target incidents occur, including the system startup and shutdown (audit functions start and end). Auditable events and audit log content are summarized in [Table 7-1] and the audit log is stored in physical memory and DBMS of the TOE.

[Table 7-1] Audit Log Content for Auditable events

구분	Auditable events	Audit log content
System	System start-up and shut-down	Date, IP Address, Type, Details
Security Audit	Audit Loge Query	Date, IP Address, Type, Details
Wireless Intrusion Detection and Prevention	Wireless Network traffic information	Device type, SSID, MAC address, signal, Manufacturer, Band, Channel, Security Type, Encryption method, Connected Station
	Security attributes that are used in the decision to enforce information flow	Number, Security Level, Detection/Prevention Date, Security Threat Type, MAC Address 1, MAC Address 2, Content, Behavior
Identification and authentication	Counter action when the unsuccessful authentication attempts leach the limit	Date, IP address, type, details
	Rejection of any secret information tested by TSF	Date, IP address, type, details
	Failure of Authorization mechanism use	Date, IP address, type, details
	Failure of Identification mechanism use, including the user identity provided	Date, IP address, type, details
	Interaction session close by the session locking mechanism	Date, IP address, type, details

Security management	Any modification for TSF function	Date, IP address, type, details
	Any modification for security attribute value	Date, IP address, type, details
	Administration Function Use	Date, IP address, type, details
	TSF self-test execution and test result	Date, type, details (Integrity damaged file)

Audit log content include date time of the auditable events (date), events type (category), subject identity, events results (details). In addition, additional content, such as security level and integrity damaged file are include in details.

In addition, in order to check the identity of the administrator in the administrator logs, which record the action of the authorized administrator such as audit and security management, the administrator logs record the IP address of the administrator for each log.

※ The relevant SFR : FAU_GEN.1, FAU_GEN.2

7.1.2 Audit review

Audit review functions in the administration UI is provided only to the authorized administrator and provide log query and monitoring function as summarized in [Table 7-2].

[Table 7-2] Log query and monitoring functions

Classification		Description
Log query	Administrator log	Records of the administrator behaviors in the management UI
	Integrity log	Integrity damaged file recode in case of integrity check
	Security event	Detection and prevention log for WIDPS security threat
Monitoring	System information	System name, firmware version, local time, system operation time
	Memory usage	Output current system memory usage
	Internet connection status	Output connection status when TOE connected to the internet through wired network.
	WLAN connection status	Output the number of wireless users in ratio connected by WLAN 2.4GHz, 5GHz

	WLAN network status	Output status of individual configuration and status of WLAN 2.4GHz, 5GHz
	WLAN internal IP allocation information	Output the allocated internal IP of the wireless users connected to WLAN 2.4GHz, 5GHz. Keep the information until the lease time finishes.
	WLAN user connection information	Output the current wireless user connected to WLAN 2.4GHz, 5GHz
	Detected surrounding device (Wireless network traffic information)	Output current AP and Stations detected with in RF coverage by analyzing collected wireless network traffic information.

In addition, the TOE provides the ability to query from the audit log by selecting the set, as shown in the following table.

[Table 7-3] Selectable set

Classification	Selectable set
Administrator log	IP address (subject identity), Type (event type), Date (event date)
Integrity log	Inspection date (event date), Type (event type)
Security event	MAC Address 1 (subject identity), Security Threat Name (event type), Detection/Prevention date (event date), Security Level

※ The relevant SFR : FAU_SAR.1, FAU_SAR.2

7.1.3 Security alarms

When TOE detects security threats configured in WIDPS policy, the administration UI displays a pop-up or makes alert sound according WIDPS event notification settings. Options that can be selected in WIDPS event notification settings are ‘security level’, ‘duration’, and ‘sound’.

※ The relevant SFR: FAU_ARP.1, FAU_SAA.1

7.1.4 Protected audit trail

The audit log created by TOE can be queried by the authorized administrator, but even the authorized administrator cannot delete or modify the audit log arbitrarily.

※ The relevant SFR : FAU_STG.1

7.1.5 Prevention of audit data loss

If the audit storage of TOE (third partition of the ROM) capacity exceeds the defined threshold (90%), the management UI displays "audit trail storage use alert" pop-up when the administrator login to the management UI. In addition, if the audit storage capacity is saturated, stop storing the audit log and display "audit storage saturated notification" pop-up window with an audit data deletion message asking to delete previous year's data in order to free up space. If the administrator desires, TOE frees up space by automatically deleting audit data that is of previous one year; otherwise, return to the audit log storage function is aborted. If the administrator log in to the management UI later, the "audit trail saturated alert" pop-up window will display again.

※ The relevant SFR : FAU_STG.3, FAU_STG.4

7.2 Cryptographic support

7.2.1 SSL

The TOE protects the communication data transmitted between the TOE and the administrator's PC via SSL communication by encrypting them. SSL communication is provided through an RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2 standard.

TOE and the administrator's PC generate and distribute the encryption key used for communication data via the TLS Handshake Protocol. When the TOE and the administrator's PC are disconnected, the encryption key is destructed by the destruction method (Zeroization of all plaintext cryptographic keys and all other critical cryptographic security parameters), which comply with FIPS PUB 140-2.

Communication data transmitted between the TOE and the administrator PC is securely transmitted by encrypting communication data with AES 128 GCM.

※ The relevant SFR : FCS_CKM.1(1), FCS_CKM.2(1), FCS_CKM.4(1), FCS_COP.1(1)

7.2.2 SSH

The TOE protects the communication data transmitted between the TOE and the administrator's PC via SSH communication by encrypting them. SSH communication is provided through an RFC 4253, The Secure Shell (SSH) Transport Layer Protocol Version 2 standard.

TOE and the administrator's PC generate and distribute the encryption key used for communication data via SSH Key Exchange. When the TOE and the administrator's PC are disconnected, the encryption key is destructed by the destruction method (Zeroization of all plaintext cryptographic keys and all other critical cryptographic security parameters), which comply with FIPS PUB 140-2.

Communication data transmitted between the TOE and the administrator PC is securely transmitted by encrypting communication data with AES256-CTR.

※ The relevant SFR : FCS_CKM.1(2), FCS_CKM.2(2), FCS_CKM.4(2), FCS_COP.1(2)

7.2.3 WLAN

The TOE carries out secure communication of datagram transmitted between the wireless users connected to WLAN of TOE using IEEE 802.11i standard supported by OS. The following two encryption methods are used in the communication.

- WPA-PSK (Pre-Shared Key)
- WPA2-PSK (Pre-Shared Key)

WPA-PSK and WPA2-PSK have the following three security components. WLAN of TOE and the wireless user generates the encryption key used for datagram protection via authenticating each other and after key establishment.

- Authentication
- Key Establishment
- Datagram Protection

TOE and the wireless users exchange the cryptographic key using IEEE 802.11i 4-Way Handshake or Group Key exchange. Key establishment process is as follows.

a) Share the WLAN password set by the authorized administrator with the wireless users in advance.
b) TOE and the wireless users generates a 256bit size of the pre-shared key (PSK, Pre-Shared Key) assigning WLAN and password (8 to 63 characters), SSID and SSID length into PBKDF2-SHA1 function. PSK becomes a master key (PMK, Pairwise Master Key).
c) TOE and the wireless users generates the one-to-one matching symmetric key (PTK, Pairwise Transient Key) using exchanged information (PMK, AP nonce (ANonce), STA nonce (SNonce), AP MAC address, STA MAC address).

Datagram between the TOE and the wireless users are safely encrypted by PTK and communicate, where the encryption algorithm used at this time is as follows:

- TKIP (Temporal Key Integrity CBC-MAC Protocol), 256bit
- CCMP (Counter Mode with CBC-MAC of the AES standard), 128bit

※ The relevant SFR : FCS_CKM.1(3), FCS_CKM.2(3), FCS_CKM.4(3), FCS_COP.1(3)

7.3 User data protection

The TOE analyze wireless network traffic after collecting them in the RF coverage. Using analysis results, TOR provides the ability to detect and disconnection security threats in real-time by defined WIDPS policies.

The TOE holds information about the authorized AP and Station via the whitelist and based on from the collected the wireless network traffic information determines whether the AP or Station is unauthorized. After comparison, once turned out to be a security threat, it is recorded as the security event and then informs the authorized administrator by generating an event alert pop-up on the management UI.

The detection detail by the WIDPS policy appears in the TOE is divided as follows:

- Detected surrounding device: (Rogue) AP list and (Rogue) Station list connected to the AP
- Security event: Detection/prevention date by security threat type, security level, MAC address, information is displayed

TOE provides disconnection method for detected security threat as follows:

- Manual disconnection : Provide connected station [disconnection] button of the detected surrounding device
- Auto disconnection : When threats are detected, immediately disconnected by policy

The security threats and their detailed process description detected by TOE are summarized in [Table 7-4]

[Table 7-4] The Security Threats and Process Details Detected by TOE

WIDPS policy	Description
Rogue AP detection,	When attributes that are not in the TOE's whitelist are detected from external entity (AP) sent wireless network traffic, Rogue AP detection is logged as a

	security event and alert pops up via management UI's popup window to the authorized administrator, if the severity of the detected security threat is higher than the one set in the event alert configuration.
Rogue Station detection,	When attributes that are not in the TOE's whitelist are detected from external entity (Station) sent wireless network traffic, Rogue Station detection is logged as a security event and alert pops up via management UI's popup window to the authorized administrator, if the severity of the detected security threat is higher than the one set in the event alert configuration.
Mis-configured AP detection,	When attributes that are in the TOE's whitelist are detected and attributes of wireless security policy match from external entity (AP) sent wireless network traffic, mis-configured AP detection is logged as a security event and alert pops up via management UI's popup window to the authorized administrator, if the severity of the detected security threat is higher than the one set in the event alert configuration.
Client Mis-association detection and disconnection	When station's attributes that are in the TOE's whitelist and AP's attributes which are not in the TOE's whitelist are detected from wireless network traffic between External entities (AP and Station), Client Mis-association detection is logged as a security event. And if auto-disconnection option is set in configuration, the disconnection command is sent to external entity (Station). Also The detection is logged as a security event and alert pops up via management UI's popup window to the authorized administrator, if the severity of the detected security threat is higher than the one set in the event alert configuration.
Unauthorized Association detection and disconnection	When station's attributes that are not in the TOE's whitelist and AP's attributes are in the TOE's whitelist are detected from wireless network traffic between External entities (AP and Station), Unauthorized Association detection is logged as a security event. And if auto-disconnection option is set in configuration, the disconnection command is sent to external entity (Station). Also The detection is logged as a security event and alert pops up via management UI's popup window to the authorized administrator, if the severity of the detected security threat is higher than the one set in the event alert configuration.
Ad-hoc Connection detection and disconnection	When station's attributes that are not in the TOE's whitelist are detected from wireless network traffic between ad-hoc connected External entities (Station and Station), Ad-hoc Connection detection is logged as a security event. And if auto-disconnection option is set in configuration, the disconnection command is sent to External entity (Station). Also The detection is logged as a security event and alert pops up via management UI's popup window to the authorized administrator, if the severity of the detected security threat is

	higher than the one set in the event alert configuration.
AP MAC Spoofing detection	When attributes that are not in the TOE's whitelist and MAC address that is in the TOE's whitelist are detected from external entity (AP) sent wireless network traffic, AP MAC spoofing detection is logged as a security event and alert pops up via management UI's popup window to the authorized administrator, if the severity of the detected security threat is higher than the one set in the event alert configuration.
Honeypot AP detection	When attributes that are in the TOE's whitelist and MAC address that is not in the TOE's whitelist are detected from external entity (AP) sent wireless network traffic, Honeypot AP detection is logged as a security event and alert pops up via management UI's popup window to the authorized administrator, if the severity of the detected security threat is higher than the one set in the event alert configuration.

All security threats detected and disconnected by TOE are logged as security events and provided to the administrator for monitoring.

※ The relevant SFR : FDP_IFC.1, FDP_IFF.1, FMT_MOF.1

7.4 Identification and authentication

TOE requires identification and authentication for the administrator and the wireless users before TSF performs its functions.

7.4.1 Administrator identification and authentication

The TOE shall provide administrator access path through the WLAN Interface (802.11b/g/n) 2.4GHz band and the administrator access is achieved by SSL or SSH. The administrator can access the management UI through SSL, performs the security functions of security management and performs limited functions (wired network settings change and time change) connected to CLI through SSH.

During the administrator login process, the administrator ID and password is required and the administrator try to connect from disallowed IP address is blocked in accordance with the allowed IP address list setup of the administrator information. Administrator ID, administrator password set in the management UI and, allowed IP address are store in DB and used as validation value during login process.

In login page, the password provided by the administrator cannot be identified for each character is replaced with a special character ("•"). In this way, the login page provides authentication feedback protection function.

If authentication failure reaches 5 times, the TOE locks identification and authentication function for 5 minutes in order to respond repeated authentication failures. Additionally, the authentication failure records are generated as audit logs to provide tracking function for failures.

When connecting to the management UI, the administrator authentication mechanism applied is as follows:

- Password rules
  - Only characters of 9~20bytes are allowed: uppercase alphabet letters (26: A~Z), lowercase alphabet letters (26: a~z), Number (10: 0~9), Special characters (33: `~!@#$%^&*()-_=+₩|[{]};:'",<.>/?blank)
  - Use one letter and a combination of at least three different kinds from above
  - Prohibit using the same character more than 3 times (e.g., aaa, 111, ### etc.)
  - Prohibit using any sequential pattern of letters or numbers that exceeds three characters long (e.g., abc, 123 etc.)
  - Prohibit using the same with an ID

TOE identifies an administrator - who performs security management or security audit on the management UI – with ID, which is one of the administrator attributes. Upon a successful login, ID is also a valid administrator account on the management UI. The administrator security attributes (administrator password and access permitted IP address) changed in the management UI by the authorized administrator are recorded as the administrator log and will allow an administrator to perform a security audit.

※ The relevant SFR : FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.2(1), FIA_UAU.7, FIA_UID.2(1), FIA_USB.1, FTP_TRP.1(1), FTP_TRP.1(2)

7.4.2 Wireless user identification and Authentication

The TOE configures WLAN with IEEE 802.11a/b/g/n/ac wireless network standard and provides the following two WLAN bands to the wireless users. The provided bands construct internal network by DHCP.

- 2.4GHz band IEEE 802.11b/g/n
- 5GHz band IEEE 802.11a/n/ac

When the wireless users connect to WLAN, the TOE requests authentication and perform authentication via a WAP-PSK/WPA2-PSK protocol that uses a pre-shared key (PSK, Pre-Shared Key).

Pre-shared key used for authentication is also used to generate an encryption key to encrypt the data stream. Encryption key uses TKIP and CCMP-AES algorithm.

※ The relevant SFR: FIA_UAU.2(2), FIA_UID.2(2), FMT_MOF.1, FTP_TRP.1(3), FTP_TRP.1(4)

7.5 Security management

TSF of the TOE provides the below security function management, security attributes management, TSF data management to the authorized administrator. The authorized administrator is the administrator who successfully login the management UI and the role for all the following security management roles.

7.5.1 System configuration

The authorized administrator performs the following system configuration security function via management UI.

[Table 7-5] System Configuration Security Function

Function	Configuration	The capacity of execution possibility
Time synchronization	- NTP client activation - NTP sever list configuration	Determine the behavior of, Disable, Enable
Administrator information	- Connection allowed IP configuration - Password change	Determine the behavior of
Integrity test	- Test execution	Determine the behavior of, Disable, Enable
WIDPS security function	- WIDPS behavior management (Stop, Start, Restart)	Determine the behavior of, Disable, Enable
Wireless configuration	- SSID configuration - SSID alarm (ON/OFF) selection - Beacon period setting - Area configuration	Determine the behavior of, Disable, Enable, Modify the behavior of

	- Mode selection - Channel selection - Authentication method selection (Open/WPA-PSK/WPA2-PSK) - Encryption selection (TKIP/CCMP(AES)) - Password setting - Channel bonding selection - Signal strength configuration	

※ The relevant SFR : FMT_MOF.1

7.5.2 WIDPS Policy Configuration

The authorized administrator performs WIDPS policy setting function via the interface provided by the management UI.

WIDPS policy performs alert settings, policy settings, whitelist management, wireless security policy settings and the type of threat that can be specified in WIDPS policy are shown in the following table.

[Table 7-6] WDIPS security threats

Security threat name	Description
Rogue AP	Unauthorized AP installed
Rogue Station	Unauthorized wireless device (Station)
Mis-configured AP	AP using a low-level security settings
Client Mis-association	Risk that an authorized internal data can leak out of the internal security control range by the authorized station connecting to an unauthorized external AP
Unauthorized Association	The risk of unauthorized connection of an unauthorized station to the authorized AP.
Ad-hoc Connection	Risk that construction of Ad-hoc network between an unauthorized station with internal authorized station
AP MAC Spoofing	A theft attacks to the MAC address of the authorized AP
Honeypot AP	The authorized AP spoofing attacks of the unauthorized AP

The authorized administrator performs event alert settings and WIDPS policy setting function, as shown in the following table. If the WIDPS security function is started by an authorized administrator, the security level of the WIDPS is set, and event alert settings as well as wireless security policies should be added as a new set. The security level and the processing of changed WIDPS policy by the authorized administrator is not initialized, but is applied to default when WIDPS security functions are restarted later.

[Table 7-7] WDIPS policy configuration function

Function	Detailed configuration	Security attribute management
Event alert setting	- Alert condition selection - Retention time selection - Sound selection	Modify
WIDPS policy	- Security threat selection - Security level selection - Processing type selection	Change_default, Modify
Wireless security policy	- Channel 2.4GHz - Channel 5GHz - Authentication - Encryption	Modify
Whitelist		

The authorized administrator registers authorized AP and/or Station by inputting attributes of a specific AP and attributes of a specific Station in the whitelist settings. The information registered in the whitelist is used to detect the security threat from collected information of the wireless network traffic.

It also provides misconfiguration type for detecting Mis-configured AP threats.

※ The relevant SFR : FMT_MSA.1, FMT_MSA.3

7.5.3 TSF data management

The TOE restricts to the following TSF data management only to the authorized administrator.

- Administrator password : Modify
- Access permit IP : Modify, Delete, generation
- Audit data: Query
- WLAN Password : Query, Modify, Delete, Generation

In addition, once a password is set and the period of time specified by an authorized administrator has passed, warns the authorized administrator by displaying a password change message on the management UI.

※ The relevant SFR: FMT_MTD.1, FMT_MTD.2

7.6 TSF protection

7.6.1 Process monitoring

If there is an abnormal termination of the TSF execution process in the operation, the TOE detects the termination and restarts the abnormally terminated process, and maintains a secure state of the TOE.

※ The relevant SFR : FPT_FLS.1

7.6.2 Self-test

In order to prove accurate operation, the TOE verifies its integrity by performing self-test during start-up and on request by the administrator from the management UI. If the TOE detects an error from the WLAN configuration files or TSF executable code in integrity verification at start-up, it provides function that execute again by restoring the normal file.

- Cryptographic algorithm used for integrity verification: SHA-256

※ The relevant SFR: FMT_MOF.1, FPT_TST.1

7.7 TOE access

The TOE provides only one session for one administrator account access to the TOE, and if there is a session, the login is restricted to the same account. In addition, the access of the administrator from the IP address not in the connection allowed IP address is restricted.

For secure session management for the authorized administrator, if the authorized session does not take any action within specified period of time (10 minutes), the TOE provides forced logout function after the time passed.

The session established between the TOE and the administrator can be closed by log out of the administrator, and the session established between the TOE and the wireless user can be closed when the wireless user disconnects himself/herself from the WLAN.

※ The relevant SFR : FTA_MCS.1, FTA_SSL.3, FTA_SSL.4(1), FTA_SSL.4(2), FTA_TSE.1

7.8 Trusted path/channels

The TOE shall allow access to the management UI and also to the management CLI only through SSL and SSH communications. SSL and SSH communication path provided is securely encrypted and protected from change and/or exposure.

The TOE also provides a communication path to wireless users by WLAN 2.4GHz and 5GHz bands, WLAN 2.4GHz and 5GHz bands provided is allowed to be accessed only through WPA / WPA2 authentication. Encrypted with TKIP or CCMP for WLAN 2.4GHz and 5GHz bands, the communication path is secured from change and/or exposure.

※ The relevant SFR : FTP_TRP.1(1), FTP_TRP.1(2), FTP_TRP.1(3), FTP_TRP.1(4)