Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Points Security Target for EAL2

Version:	**1.0**
Part Number:	**015675-00**
Status:	**Released**
Last Update:	**2021-10-06**

Trademarks

atsec® is a trademark of atsec information security corporation in the United States, other countries, or both.

OmniAccess® is a trademark used by ALE USA Inc.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Legal Notices

This document is provided AS IS with no express or implied warranties. Use the information in this document at your own risk.

Revision History

Revision	**Date**	**Author(s)**	**Changes to Previous Revision**
1.0	2021-10-06	Yi Cheng	First release.

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Security Target Identification

Title: Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Points Security Target for EAL2

Version: 1.0

Part Number: 015675-00

Status: Released

Date: 2021-10-06

Sponsor: ALE USA Inc.

Developer: ALE USA Inc.

Keywords: ALE USA Inc., ALE, Alcatel-Lucent Enterprise, OmniAccess Stellar, wireless access point, AP, AWOS, OmniAccess Stellar AP1201, AP1220, AP1230, AP1251, AP1320, AP1360

1.2 TOE Identification

The TOE is Alcatel-Lucent OmniAccess Stellar AP series AP1201, AP1201H/HL/L, AP1220, AP1230, AP1251, AP1320 and AP1360 with AWOS 4.0.1 (build number 504) firmware.

1.3 TOE Type

The TOE type is Wireless Local Area Network (WLAN) access points.

1.4 TOE Overview

The Target of Evaluation (TOE) is WLAN access points (APs) comprised of hardware, firmware and guidance documentation.

The firmware is AWOS 4.0.1 (build number 504). The access points run on Linux operating system.

The TOE hardware consists of the following models:

AP Model Name	AP Model Name Marketing Description	Regional Variant	Rev
OAW-AP1201	OmniAccess Stellar AP1201	OAW-AP1201-RW	D01
		OAW-AP1201-US	A03
		OAW-AP1201-ME	A01
		OAW-AP1201H-RW	F01

OAW-AP1201H OAW-AP1201HL OAW-AP1201L	OmniAccess Stellar AP1201H, OmniAccess Stellar AP1201HL, OmniAccess Stellar AP1201L	OAW-AP1201H-US	B01
		OAW-AP1201H-ME	B01
		OAW-AP1201HL-RW	A
		OAW-AP1201L-RW	A
OAW-AP1221, OAW-AP1222	OmniAccess Stellar AP1221, OmniAccess Stellar AP1222	OAW-AP1221-RW	E
		OAW-AP1221-US	B
		OAW-AP1221-ME	B01
		OAW-AP1222-RW	E
		OAW-AP1222-US	B
		OAW-AP1222-ME	B01
OAW-AP1231, OAW-AP1232	OmniAccess Stellar AP1231, OmniAccess Stellar AP1232	OAW-AP1231-RW	B01
		OAW-AP1231-US	B04
		OAW-AP1232-RW	B01
		OAW-AP1232-US	B03
OAW-AP1251	OmniAccess Stellar AP1251	OAW-AP1251-RW	E
		OAW-AP1251-US	C
		OAW-AP1251-ME	B
OAW-AP1321, OAW-AP1322	OmniAccess Stellar AP1321, OmniAccess Stellar AP1322	OAW-AP1321-RW	A
		OAW-AP1321-US	A
		OAW-AP1321-ME	A
		OAW-AP1322-RW	A
		OAW-AP1322-US	A
		OAW-AP1322-ME	A
OAW-AP1361, OAW-AP1361D OAW-AP1362	OmniAccess Stellar AP1361, OmniAccess Stellar AP1361D, OmniAccess Stellar AP1362	OAW-AP1361-RW	A
		OAW-AP1361-US	A
		OAW-AP1361-ME	A
		OAW-AP1361D-RW	A
		OAW-AP1361D-US	A
		OAW-AP1361D-ME	A
		OAW-AP1362-RW	A
		OAW-AP1362-US	A
		OAW-AP1362-ME	A

Table 1: TOE Identification

The table below shows the chipset, CPU and Linux kernel used by the TOE:

AP Models	Chipset (Qualcomm)	CPU (integrated in main chip)	Linux Kernel
OAW-AP1201	IPQ4018	Quad-core ARM Cortex-A7 at 600 MHz	3.14.77-ARM

AP Models	Chipset (Qualcomm)	CPU (integrated in main chip)	Linux Kernel
OAW-AP1201H, OAW-AP1201HL, OAW-AP1201L	QCA9563 + QCA9886	MIPS 74Kc at 775Mhz	3.14.77-MIPS
OAW-AP1221, OAW-AP1222	IPQ4029 + QCA9994	Quad-core ARM Cortex-A7 at 717MHz	3.14.77-ARM
OAW-AP1231, OAW-AP1232	IPQ8065 + QCA9994	Dual-core SMP Krait CPU (ARMv7-compliant) at 1.7GHz	3.14.77-ARM
OAW-AP1251	IPQ4029	Quad-core ARM Cortex-A7 at 717MHz	3.14.77-ARM
OAW-AP1321, OAW-AP1322	IPQ8071A	Quad ARM Cortex A53s, 1.0GHz	4.4.60-ARM
OAW-AP1361, OAW-AP1361D, OAW-AP1362	IPQ8071A	Quad ARM Cortex A53s, 1.0GHz	4.4.60-ARM

Table 2: TOE Hardware Configurations

The Access Points included in the TOE vary by the provided data rate, antenna support and physical interfaces (see Table 2 for details). However, the differences do not affect the security functionality claimed by the TOE.

1.4.1 Intended method of use

The TOE is used to securely connect wireless clients to a wired network. It enforces Wi-Fi Protected Access 2 (WPA2) to authenticate wireless clients and to protect the confidentiality and integrity of wireless traffic.

The TOE is intended to operate in a secure enterprise environment that protects the TOE from unauthorized physical access. Appropriate security policy and security procedure guidance must be in place to govern operational management of the TOE within its operational environment.

The TOE is not intended for use as a general-purpose computer and only executes the services needed to perform its intended function.

1.4.2 Major security features

The TOE provides the following security functions:

- Security audit

- Cryptographic support for WPA2, IEEE 802.1X, TLS, and secure storage of passwords and keys
- Identification and authentication of administrators and wireless clients
- Security management
    - Management of cryptographic keys
    - Configuration of login banner, authentication failure parameters, session timeout, etc.
    - Manual update of TOE firmware
    - Start and stop WLAN service
- Protection of the TSF including firmware, sensitive data and system time
- TOE access control based on inactivity time and time/day
- Trusted path/channels for remote administration and wireless communication

1.4.3 Required non-TOE hardware / software / firmware

The TOE requires the following hardware, software and firmware in the operational environment:

- Wireless clients: wireless client hosts connecting to the wired network via the TOE
- RADIUS authentication server: an external server for authenticating wireless clients
- Local console: connected directly to the TOE via the serial console port and intended for troubleshooting
- Administrator workstation with a web browser: used by the administrator for remote TOE administration over TLS/HTTPS trusted path
- Syslog server: the TOE relies upon the external Syslog server for storage of audit records.

1.5 TOE Description

1.5.1 Architecture

The TOE provides the connection point between wireless clients and the wired network. It operates on the 2.4 and 5 GHz radio frequencies (RFs) and implements the IEEE 802.11 standard to communicate over-the-air with wireless clients. This communication includes advertising its presence, responding to probe requests from wireless clients, performing authentication, association, encryption/decryption, and session management.

The APs can also communicate among themselves (mesh mode) but the AP to AP communication is not in the scope of this evaluation.

Once installed as trusted nodes on the wired infrastructure, the APs provide authorized wireless clients secure over-the-air access to the wired network. The encrypted IEEE 802.11 link protects wireless traffic from unauthorized disclosure and/or modification.

The TOE supports Wi-Fi Protected Access 2 (WPA2), which is the Wi-Fi Alliance interoperable specification based on the IEEE 802.11i security standard. There are two ways to authenticate wireless clients prior to connecting them to the wired network. The first is 802.1X which requires an external RADIUS authentication server. The RADIUS server authenticates wireless clients using the Extensible Authentication Protocol (EAP) and communicates the authentication result and, if success, key material to the TOE. The second way to authenticate wireless clients is to use a pre-shared key (PSK) that is known to the TOE and the clients.

After successful completion of the 802.11i 4-way handshake, the wireless clients are associated to the TOE. The wireless sessions are protected using AES-CCMP for encryption and message integrity with cryptographic key size of 128 bits in accordance with the IEEE 802.11-2016 standard.

The figure below shows the TOE and its operational environment. The trusted path between the TOE and Administrator Workstation is TLS/HTTPS.

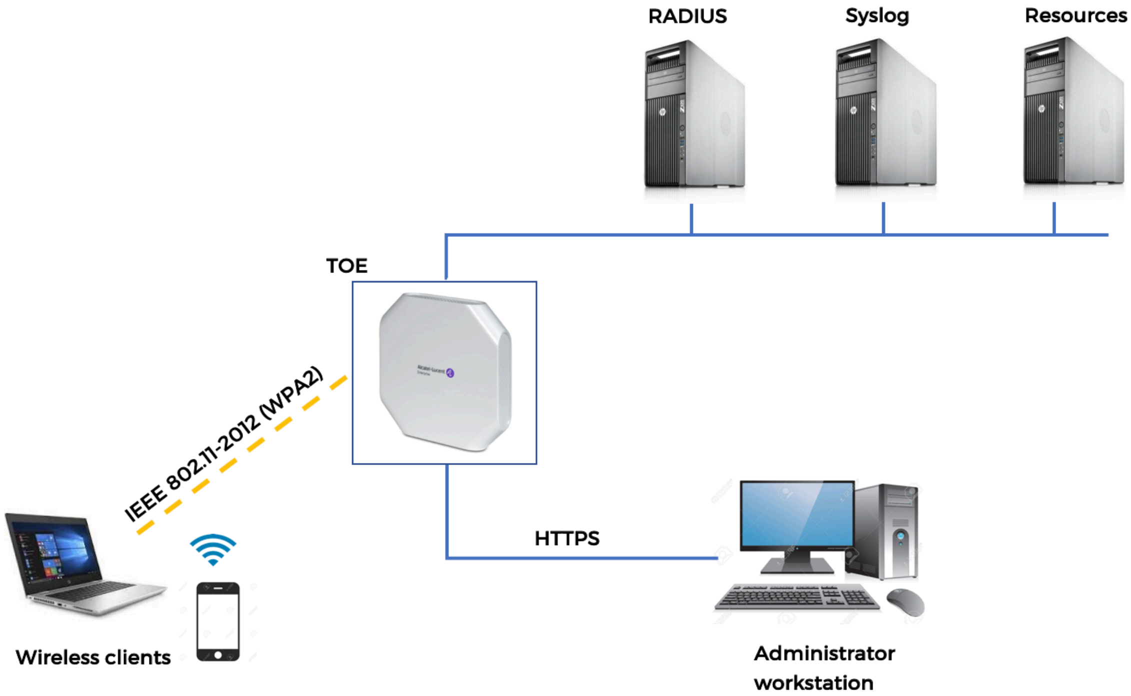


Figure 1: TOE and Environment

The TOE provides a Web based user interface (Web UI) for remote management of the TOE. The TOE runs an internal web server and uses TLS/HTTPS to secure the management traffic. The web server inside the TOE does not authenticate the client during TLS handshake. Only the server is authenticated with its certificate. After the HTTPS connection is established, administrative users authenticate themselves to the TOE using passwords.

A local console can be connected to the TOE via a serial cable. It is intended for troubleshooting and shall not be used to perform any management functions on the TOE.

Alcatel-Lucent OmniAccess Stellar APs can be centrally managed by using Alcatel-Lucent OmniVista 2500 on premise network management system or Alcatel-Lucent OmniVista Cirrus cloud platform. This central management is out of the scope of this evaluation.

1.5.2 TOE boundaries

1.5.2.1 Physical

The TOE encompasses the entire device, including both the hardware and firmware. The TOE hardware platforms (chipset and CPU) are described in Table 1.

Table 2 below specifies the firmware, physical interfaces and features of the different TOE models.

AP Models	Firmware	Description
OAW-AP1201	AWOS 4.0.1	The efficient 802.11ac AP1201 access point supports a maximum concurrent data rate of 1.2 Gb/s (867 Mb/s in 5 GHz and 400 Mb/s in 2.4 GHz), 80 MHz channels (VHT80), multi-user MIMO (MU-MIMO) and two spatial streams (2SS) per radio. Antenna: Built-in 2×2:2 @ 2.4 GHz, 2x2:2 @ 5 GHz, BLE antenna. Interfaces: • 1× 10/100/1000Base-T autosensing (RJ-45) port, Power over Ethernet (PoE) • 1x Bluetooth Low Energy (BLE) 5.0 radio, integrated antenna. Hardware ready for Zigbee. • 1× management console port (RJ-45) • Reset button: Factory reset • DC48V power jack • Kensington security slot
OAW-AP1201H, OAW-AP1201HL, OAW-AP1201L	AWOS 4.0.1	The efficient 802.11ac AP1201H access point supports a maximum concurrent data rate of 1.2 Gb/s (867 Mb/s in 5 GHz and 300 Mb/s in 2.4 GHz), MU-MIMO and two spatial streams (2SS). Antenna: Built-in 2×2:2 @ 2.4 GHz, 2x2:2 @ 5 GHz.

AP Models	Firmware	Description
		Interfaces: • Uplink: 1× 10/100/1000Base-T autosensing (RJ-45) port, Power over Ethernet (PoE) • Downlink: o AP1201H: 1× 10/100/1000Base-T autosensing (RJ-45) port, Power over Ethernet (PoE-PSE) 802.3af compliant; 2× 10/100/1000Base-T autosensing (RJ-45) port o AP1201HL: 3× 10/100/1000Base-T autosensing (RJ-45) port • AP1201H and AP1201HL: Passive Pass through one pair, back and bottom • AP1201H and AP1201HL: 1× USB 2.0 (Type A) • AP1201L: 1× management console port (RJ-45) • Reset button: Factory reset • DC48V power jack
OAW-AP1221, OAW-AP1222	AWOS 4.0.1	The high performance 802.11ac AP1220 series supports a maximum concurrent data rate of 2.1 Gb/s (1733 Mb/s in 5 GHz and 400 Mb/s in 2.4 GHz), 160 MHz channels (VHT160*), multi-user MIMO (MU-MIMO) and four spatial streams (4SS). Antenna: • AP1221: Built-in 2×2:2 @ 2.4 GHz, 4x4:4 @ 5 GHz • AP1222: External 2×2:2 @ 2.4 GHz, 4x4:4 @ 5 GHz • Optional external antenna (sold separately) Interfaces: • 1x 10/100/1000Base-T autosensing (RJ-45) port, Power over Ethernet (PoE) • 1x USB 2.0 (Type A connector) • 1x management console port (RJ-45) • Reset button: Factory reset • DC48V power jack • Kensington security slot • AP1222: 4x RP-SMA antenna connectors

AP Models	Firmware	Description
OAW-AP1231, OAW-AP1232	AWOS 4.0.1	The high performance 802.11ac AP1230 series supports a maximum concurrent data rate of 4.266 Gb/s (dual 1733 Mb/s in 5 GHz and 800 Mb/s in 2.4 GHz), dual uplinks with 2.5 GbE and 1 GbE, 160 MHz channels (VHT160*), multi- user MIMO (MU-MIMO) and four spatial streams (4SS). Antenna: • AP1231: Built-in 4×4:4 @ 2.4 GHz, dual 4x4:4 @ 5 GHz • AP1232: External 4×4:4 @ 2.4 GHz, dual 4x4:4 @ 5 GHz 8 RP-SMA connectors for external dual band antennas. • Optional external antenna (sold separately) Interfaces: • 1x 100/1000/2500Base-T autosensing (RJ-45) port, Power over Ethernet (PoE) • 1x 10/100/1000Base-T autosensing (RJ-45) port, Power over Ethernet (PoE) • 1x Bluetooth Low Energy (BLE) radio, integrated antenna • 1x USB 2.0 (Type A connector) • 1x management console port (RJ-45) • Reset button: Factory reset • DC48V power jack • Kensington security slot • AP1232: 8x RP-SMA antenna connectors
OAW-AP1251	AWOS 4.0.1	The high performance and rugged AP1251 supports the IP67 standard for harsh outdoor environments, such as exposure to high and low temperatures, persistent moisture and precipitation, and electrical interfaces include industrial strength surge protection. The AP1251 supports a maximum concurrent data rate of 1.267 Gb/s (867 Mb/s in 5 GHz and 400 Mb/s in 2.4 GHz), and dual Gigabit Ethernet links, integrated omni-directional antennas, the AP1251 is ideal for medium density outdoor environments. Antenna: Built-in 2×2:2 @ 2.4 GHz, 2x2:2 @ 5 GHz. Interfaces:

AP Models	Firmware	Description
		• 1× 10/100/1000Base-T autosensing (RJ-45) port, Power over Ethernet (PoE) • 1× 10/100/1000Base-T autosensing (RJ-45) port • 1x management console port (Micro-USB) • Reset button: Factory reset
OAW-AP1321, OAW-AP1322	AWOS 4.0.1	The OmniAccess Stellar AP1320 series supports a maximum aggregate data rate of˜3Gbps (2.4Gbps in 5 GHz and 573Mbps in GHz). To support this higher capacity the access point is powered by a Multigig Ethernet uplink. Antenna: • AP1321: 2×2:2 @ 2.4 GHz, 4x4:4 @ 5 GHz • AP1322: 2×2:2 @ 2.4 GHz, 4x4:4 @ 5 GHz Interfaces: • 1x 10BASE-Te/100BASE-TX/1000BASE-T/2500BASE-T IEEE 802.3 compliant autosensing (RJ-45) port, ENET0, Power over Ethernet (PoE) 802.3at compliant • 1x 10/100/1000 BASE-T IEEE 802.3 compliant auto-sensing (RJ-45) port, ENET1, Power over Ethernet (PoE) 802.3at compliant • 1x BLE/ZigBee radio • 1x USB 2.0 Type A (5V, 500mA) • 1x management console port (RJ-45) • Reset button: Factory reset • DC48V power jack • AP1322: 4x RP-SMA female external antenna connectors
OAW-AP1361, OAW-AP1361D, OAW-AP1362	AWOS 4.0.1	The OmniAccess Stellar AP1320 series supports a maximum aggregate data rate of˜3Gbps (2.4Gbps in 5 GHz and 573Mbps in GHz). To support this higher capacity the access point is powered by a Multigig Ethernet uplink. Antenna: • AP1361: 2×2:2 @ 2.4 GHz, 4x4:4 @ 5 GHz • AP1361D: 2×2:2 @ 2.4 GHz, 4x4:4 @ 5 GHz • AP1362: 2×2:2 @ 2.4 GHz, 4x4:4 @ 5 GHz Interfaces:

AP Models	Firmware	Description
		• 1x 10/100/1000/2500 Mbps IEEE 802.3 compliant autosensing (RJ-45) uplink port, ENET0, Power over Ethernet (PoE) 802.3at/bt compliant • 1x 10/100/1000 Mbps IEEE 802.3 compliant auto-sensing (RJ-45) downlink port, ENET1, PoE output up to 802.1at power dependent on input PoE • 1x SFP port • 1x BLE/ZigBee radio • 1x USB 2.0 Type C • 1x management console port (Micro-USB) • Reset button: Factory reset • AP1362: 6x N-type external antenna connectors, integrated 6KA lightning protection, not require additional lighting arrester

Table 3: TOE Models and Descriptions

TOE Guidance

The following documentation comprises the TOE guidance and is available on the Alcatel-Lucent Enterprise Service and Support website:

- OmniAccess Stellar AP User Guide [APGUIDE]

- Common Criteria Evaluated Configuration Guide for Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Points [CCECG]

Delivery of the TOE

Alcatel-Lucent Enterprise orders for the Common Criteria evaluated TOE are delivered using reputable couriers for shipping. Hardware is packaged in electrostatic discharge (ESD) bags and sealed with an ESD warning label. It is then boxed in the factory using tape.

The evaluated firmware must be loaded by the customer after receiving the hardware in order to insure correct configuration. The firmware on the shipped OmniAccess Stellar AP is not guaranteed to be the same version as evaluated. The evaluated firmware can be obtained from the Alcatel-Lucent Enterprise Business Portal (https://businessportal2.alcatel-lucent.com). The TOE guidance can be downloaded from the same portal. In order to access the Business Portal, the user must have a support contract in place.

1.5.2.2 Logical

This section summarizes the security functions provided by the TOE.

Security audit

The TOE generates audit records. Each security relevant audit event has the date, timestamp, event description, subject identity and outcome. The audit records can be viewed on the serial console or within the Web UI.

The TOE writes audit records to a fixed segment in the memory. Once the segment becomes full the oldest records are overwritten. When the AP reboots, the audit records in the memory get lost. But the TOE provides the ability to send audit records to an external Syslog server. In that case, the operational environment must ensure that the communication between the TOE and the Syslog server is secure.

Cryptographic support

The TOE requires cryptography for supporting the establishment of secure channels using IEEE 802.11-2016 (WPA2), IEEE 802.1X and TLS/HTTPS.

The cryptographic functions provided by the TOE include random number and key generation, key establishment, key distribution, key destruction, AES encryption/decryption, signature generation, and secure hash.

The WPA2-related cryptographic operations are implemented by the Wi-Fi chips from Qualcomm. The other cryptographic functions are provided by the OpenSSL software package, which is bundled in the TOE.

Two of the Qualcomm chips listed in Table 1 are certified by Wi-Fi Alliance: IPQ4018 (Certification ID WFA67129) and IPQ8065 (WFA63130).

Identification and authentication

The TOE requires identification and authentication of administrators of the TOE prior to access any of the management functions. Re-authentication is required when the administrator changes his/her password.

For the Web UI, the TOE displays a configurable access banner and enforces a local password-based authentication of administrative user. Passwords are obscured when being displayed during any attempted login. The TOE also provides the ability to lock the user account after a configurable number of unsuccessful login attempts, and terminate the user session after a configurable period of inactivity.

The TOE authenticates wireless clients using either pre-shared key (PSK) or IEEE 802.1X. There are three components for 802.1X as follows:

- *The Supplicant*: this is the device residing in the TOE operational environment that supports the 802.1X protocol. The wireless client acts as the supplicant.
- *The Authenticator Port Access Entity (PAE)*: this entity requires authentication from the supplicant before allowing access. The TOE acts as the Authenticator PAE.
- *The Authentication Server*: this component resides in the TOE operational environment and provides the authentication service and verifies credentials (username, password, challenge, certificate, etc.) of the supplicant.

The operational environment ensures that the communication between the TOE and the RADIUS server is secure.

Figure 2 shows a depiction of IEEE 802.1X wireless client authentication provided by the TOE.

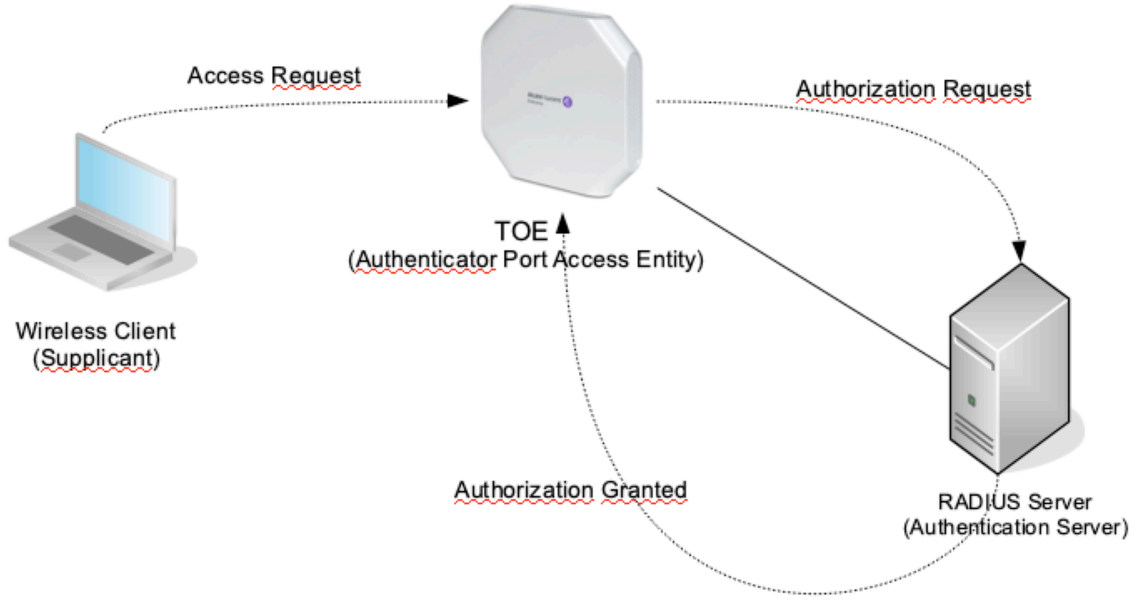


Figure 2: IEEE 802.1X Authentication

Security management

The TOE provides a secure remote interface (Web UI) for security management.

An authorized administrator has the ability to modify, edit, and delete security parameters such as user credential and cryptographic keys. The administrator can also configure the login banner that contains an advisory notice and consent warning message, the number of failed authentication attempts before account lockout and the lockout period, the inactivity timer before session termination, as well as manually update the TOE firmware.

The TOE provides a Security Administrator role and only the Security Administrator can perform the above security management functions.

Protection of the TSF

The TOE protects itself by requiring administrators to identify and authenticate themselves prior to performing any actions. The TOE stores sensitive data including cryptographic keys and credentials in non-plaintext form, and thus prevents users from reading the key values and passwords.

For manual updates of the TOE firmware, the administrator downloads the new version of TOE firmware from the Alcatel-Lucent Enterprise Business Portal using HTTPS. The administrator verifies the integrity of the downloaded firmware by calculating a hash of the downloaded file and comparing it to the hash value published on the portal. If the integrity verification succeeds the administrator uploads the firmware to the TOE.

The firmware image also contains a MD5 checksum. The TOE uses this MD5 checksum to make sure that the firmware is not damaged before installing it.

The TOE also provides a reliable date and time that is used for audit record timestamps, denial of session establishment of wireless clients based on time, and interactive session timeout.

TOE Access

The TOE monitors remote user sessions for inactivity and terminates the session when a threshold time period is reached. Once a session has been terminated the TOE requires the user to re-authenticate.

The TOE is capable of denying session establishment of wireless clients based on time, day and WLAN SSID.

The TOE also displays an administrator specified advisory notice and consent warning message prior to initiating identification and authentication for each administrative user.

Trusted path/channels

The TOE provides the following secure channels to ensure the integrity and confidentiality of the information exchanged between the TOE and external IT entities in the operational environment:

- TLS/HTTPS is used to protect communication with administrator workstation.
- WPA2 is used to protect communication with wireless clients.

1.5.2.3 Evaluated configuration

The following items need to be adhered to in the evaluated configuration:

- Versions 1.1 and 1.2 of the TLS protocol are the only versions allowed in the evaluated configuration. Usage of other protocol versions usually supported in SSL and TLS (SSLv1.0, SSLv2.0, SSLv3.0 or TLSv1.0) are prohibited.
- The console interface shall not be used to perform any management functions on the TOE.
- FTP/TFTP access to the AP must be disabled for security reasons.
- Secure Shell (SSH) is used only for diagnostics and must be disabled in the CC evaluated configuration.
- The use of NTP to synchronize the time with an external time source must be disabled in the CC evaluated configuration.
- The use of captive portal for guest WLAN access must be disabled in the CC evaluated configuration.

2 CC Conformance Claim

This Security Target is CC Part 2 extended and CC Part 3 conformant, with a claimed Evaluation Assurance Level of EAL2, augmented by ALC_FLR.1.

This Security Target does not claim conformance to any Protection Profile.

Common Criteria [CC] version 3.1 revision 5 is the basis for this conformance claim.

3 Security Problem Definition

The collaborative Protection Profile for Network Devices [NDcPPv2.1] defines the baseline security requirements for network infrastructure devices in general. The NDcPP Extended Package Wireless Local Area Network (WLAN) Access systems [WLANASEPv1.0] extends the NDcPP baseline with additional security requirements specific to WLAN access system network infrastructure devices.

Since the TOE is a WLAN access point, most of the security problems identified by NDcPPv2.1 and WLANASEPv1.0 are applicable to the TOE. Although this ST does not claim conformance to NDcPPv2.1 or WLANASEPv1.0, it reuses the applicable threats, assumptions and organizational security policies defined by these two specifications.

3.1 Threat Environment

This section describes the threat model for the TOE and identifies the individual threats that are assumed to exist in the TOE environment.

The **assets** to be protected by the TOE are as follows.

- Communications with the TOE: for administering the TOE (administration traffic), for sending and receiving wireless data packets to wireless clients.
- The current version of the TOE and trusted updates to its firmware.
- TSF data stored by the TOE (e.g. user credentials, cryptographic keys).

The **threat agents** having an interest in accessing or manipulating the assets can be categorized as either:

- Unauthorized individuals ("attackers") which are unknown to the TOE and its runtime environment.
- Authorized users of the TOE (i.e., administrators) who try to manipulate data that they are not authorized to access.

TOE administrators, including administrators of the TOE environment, are assumed to be trustworthy, trained and to follow the instructions provided to them with respect to the secure configuration and operation of the systems under their responsibility. Hence, only inadvertent attempts to manipulate the safe operation of the TOE are expected from this community.

3.1.1 Threats countered by the TOE

T.UNAUTHORIZED_ADMINISTRATOR_ACCESS

Threat agents may attempt to gain Administrator access to the network device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.

T.WEAK_CRYPTOGRAPHY

Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.

T.UNTRUSTED_COMMUNICATION_CHANNELS

Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.

T.WEAK_AUTHENTICATION_ENDPOINTS

Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints - e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.

T.UPDATE_COMPROMISE

Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.

T.UNDETECTED_ACTIVITY

Threat agents may attempt to access, change, and/or modify the security functionality of the network device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.

T.SECURITY_FUNCTIONALITY_COMPROMISE

Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.

T.PASSWORD_CRACKING

Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic and may allow them to take advantage of any trust relationships with other network devices.

T. NETWORK_DISCLOSURE

Sensitive information on a protected network might be disclosed resulting from ingress- or egress-based actions.

T. NETWORK_ACCESS

Unauthorized access may be achieved to services on a protected network from outside that network.

T. DATA_INTEGRITY

A malicious party attempts to change the data being sent - resulting in loss of integrity.

T. REPLAY_ATTACK

If malicious or external IT entities are able to gain access to the network, they may have the ability to capture information traversing throughout the network and send them on to the intended receiver.

3.2 Assumptions

3.2.1 Intended usage of the TOE

A.LIMITED_FUNCTIONALITY

The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).

A.NO_THRU_TRAFFIC_PROTECTION

A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered.

A.PRESHARED_KEY

For pre-shared key based authentication of wireless clients, it is assumed that the pre-shared key is provided only to trusted users.

3.2.2 Environment of use of the TOE

3.2.2.1 Physical

A.PHYSICAL_PROTECTION

The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains.

3.2.2.2 Personnel

A.TRUSTED_ADMINISTRATOR

The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.

A.REGULAR_UPDATES

The network device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

A.ADMIN_CREDENTIALS_SECURE

The Administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.

A.RESIDUAL_INFORMATION

The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

3.2.2.3 Connectivity

A.SERVICES_RELIABLE

When the TOE uses the network services RADIUS and Syslog in the Operational Environment, these services provide reliable information and responses to the TOE. In addition, it is assumed that the Operational Environment protects the communication between the network service and the TOE from loss of confidentiality and integrity, either by physical or logical means.

A.CONNECTIONS

It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

3.3 Organizational Security Policies

P.ACCESS_BANNER

The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

4 Security Objectives

The collaborative Protection Profile for Network Devices [NDcPPv2.1] defines the baseline security requirements for network infrastructure devices in general. The NDcPP Extended Package Wireless Local Area Network (WLAN) Access systems [WLANASEPv1.0] extends the NDcPP baseline with additional security requirements specific to WLAN access system network infrastructure devices.

Since the TOE is a WLAN access point, most of the security objectives defined by NDcPPv2.1 and WLANASEPv1.0 are applicable to the TOE. Although this ST does not claim conformance to NDcPPv2.1 or WLANASEPv1.0, it reuses the applicable security objectives defined by these two specifications.

4.1 Objectives for the TOE

O.ADMIN_ACCESS

The TOE must ensure that only identified and authenticated users gain access to administrative functions and protected resources.

O.ADMIN_SESSION

The TOE must protect interactive administrator's sessions by allowing the termination of sessions by an administrator, and forcing the termination of a session after a specified period of inactivity.

O.CRYPTOGRAPHY

The TOE must use standardized cryptographic algorithms, which must provide sufficient strength through the use of appropriate key sizes and modes. Key generation algorithms must use a standardized Deterministic Random Bit Generator (DRBG) seeded with an amount of entropy equal or greater of the strength of the cryptographic keys generated.

O.COMMUNICATION_CHANNELS

The TOE must protect critical network traffic from disclosure and modification using standardized secure tunneling protocols. These protocols must use strong cryptographic algorithms and authentication methods for each endpoint. Critical network traffic includes transfer of TSF data to and from the TOE, and administrators performing security management activities.

O.TRUSTED_UPDATES

The TOE must verify the authenticity of software or firmware updates before being installed through one or more authentication methods using strong cryptographic algorithms.

O.AUDIT

The TOE must record security relevant actions of users on the TOE. The information recorded in these security events must be in sufficient detail to help an administrator of the TOE detect attempted security violations or potential misconfiguration of the TOE security features.

O.TSF_DATA_PROTECTION

The TOE must protect the network device software, firmware, and TSF data (administrator credentials, credentials used for secure channels, etc.) from unauthorized disclosure and modification.

O.PASSWORD_PROTECTION

The TOE must provide means to protect against password disclosure and cracking.

O.ACCESS_BANNER

The TSF must display an initial banner before users log into the TOE. The initial banner must contain restrictions of use, legal agreements, or any other appropriate information to which users make consent by accessing the TOE.

O.CRYPTOGRAPHIC_FUNCTIONS

The TOE will provide means to encrypt and decrypt data as a means to maintain confidentiality and allow for detection and modification of TSF data that is transmitted outside of the TOE.

O. AUTHENTICATION

The TOE will provide a means to authenticate the user to ensure they are communicating with an authorized external IT entity.

O. SYSTEM_MONITORING

The TOE will provide a means to audit events specific to WLAN functionality and security.

O. TOE_ADMINISTRATION

The TOE will provide the functions necessary to address failed authentication attempts by a remote administrator.

4.2 Objectives for the Operational Environment

OE.PHYSICAL

Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

OE.NO_GENERAL_PURPOSE

There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

OE.NO_ THRU_TRAFFIC_PROTECTION

The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.

OE.PRESHARED_KEY

For pre-shared key based authentication of wireless clients, the pre-shared key is provided only to trusted users.

OE.TRUSTED_ADMIN

Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner.

OE.UPDATES

The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

OE.ADMIN_CREDENTIALS_SECURE

The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.

OE.RESIDUAL_INFORMATION

The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

OE.SERVICES_RELIABLE

When the TOE uses the network services RADIUS and Syslog in the Operational Environment, these services shall provide reliable information and responses to the TOE. In addition, communication between the network service and the TOE must be protected from loss of integrity, either by physical or logical means, by the Operational Environment.

OE.STRONG_PASSWORD

The Security Administrator ensures that strong passwords are used for accessing the TOE.

OE.CONNECTIONS

TOE administrators will ensure that the TOE is installed in a manner that will allow the TOE to effectively enforce its policies on network traffic flowing among attached networks.

4.3 Security Objectives Rationale

4.3.1 Coverage

The following table provides a mapping of TOE objectives to threats and policies, showing that each objective counters or enforces at least one threat or policy, respectively.

Objective	Threats / OSPs
O.ADMIN_ACCESS	T.UNAUTHORIZED_ADMINISTRATOR_ACCESS
O.ADMIN_SESSION	T.UNAUTHORIZED_ADMINISTRATOR_ACCESS
O.CRYPTOGRAPHY	T.WEAK_CRYPTOGRAPHY

Objective	Threats / OSPs
O.COMMUNICATION_CHANNELS	T.UNTRUSTED_COMMUNICATION_CHANNELS T.WEAK_AUTHENTICATION_ENDPOINTS
O.TRUSTED_UPDATES	T.UPDATE_COMPROMISE
O.AUDIT	T.UNDETECTED_ACTIVITY
O.TSF_DATA_PROTECTION	T.SECURITY_FUNCTIONALITY_COMPROMISE
O.PASSWORD_PROTECTION	T.PASSWORD_CRACKING
O.ACCESS_BANNER	P.ACCESS_BANNER
O.CRYPTOGRAPHIC_FUNCTIONS	T.NETWORK_DISCLOSURE T.DATA_INTEGRITY T.REPLAY_ATTACK
O.AUTHENTICATION	T.NETWORK_DISCLOSURE T.NETWORK_ACCESS T.REPLAY_ATTACK
O.SYSTEM_MONITORING	T.UNDETECTED_ACTIVITY
O.TOE_ADMINISTRATION	T.NETWORK_ACCESS

Table 4: Mapping of security objectives to threats and policies

The following table provides a mapping of the objectives for the Operational Environment to assumptions, threats and policies, showing that each objective holds, counters or enforces at least one assumption, threat or policy, respectively.

Objective	Assumptions / Threats / OSPs
OE.PHYSICAL	A.PHYSICAL_PROTECTION
OE.NO_GENERAL_PURPOSE	A.LIMITED_FUNCTIONALITY
OE.NO_THRU_TRAFFIC_PROTECTION	A.NO_THRU_TRAFFIC_PROTECTION
OE.PRESHARED_KEY	A.PRESHARED_KEY, T.UNTRUSTED_COMMUNICATION_CHANNELS, T.WEAK_AUTHENTICATION_ENDPOINTS

Objective	Assumptions / Threats / OSPs
OE.TRUSTED_ADMIN	A.TRUSTED_ADMINISTRATOR
OE.UPDATES	A.REGULAR_UPDATES
OE.ADMIN_CREDENTIALS_SECURE	A.ADMIN_CREDENTIALS_SECURE
OE.RESIDUAL_INFORMATION	A.RESIDUAL_INFORMATION
OE.SERVICES_RELIABLE	A.SERVICES_RELIABLE
OE.STRONG_PASSWORD	T.PASSWORD_CRACKING
OE.CONNECTIONS	A.CONNECTIONS

Table 5: Mapping of security objectives for the Operational Environment to assumptions, threats and policies

4.3.2 Sufficiency

The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat, when achieved, actually contributes to the removal, diminishing or mitigation of that threat.

Threat	Rationale for security objectives
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	The threat of gaining administrator access to the network device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session , or performing man-in-the-middle attacks is countered by O.ADMIN_ACCESS and O.ADMIN_SESSION.
T.WEAK_CRYPTOGRAPHY	The threat of exploiting weak cryptographic algorithms or performing a cryptographic exhaust against the key space, because of poorly chosen encryption algorithms, modes, or key sizes is countered by O.CRYPTOGRAPHY.

Threat	Rationale for security objectives
T.UNTRUSTED_COMMUNICATION_CHANNELS	The threat of losing confidentiality and integrity of the critical network traffic, and potentially a compromise of the network device itself because of not using standardized secure tunneling protocols is countered by O.COMMUNICATION_CHANNELS. The threat of losing confidentiality due to misuse of pre-shared key is countered by OE.PRESHARED_KEY.
T.WEAK_AUTHENTICATION_ENDPOINTS	The threat of having critical network traffic exposed because of using protocols that use weak methods to authenticate the endpoints is countered by O.COMMUNICATION_CHANNELS. In addition, OE.PRESHARED_KEY ensures that the pre-shared key is provided only to trusted users.
T.UPDATE_COMPROMISE	The threat of using a compromised update of the software or firmware tampered by an attacker is countered by O.TRUSTED_UPDATES.
T.UNDETECTED_ACTIVITY	The threat of access, change, and/or modify the security functionality of the network device without administrator awareness is countered by O.AUDIT and O.SYSTEM_MONITORING.
T.SECURITY_FUNCTIONALITY_COMPROMISE	The threat of compromising credentials and device data enabling continued access to the network device and its critical data is countered by O.TSF_DATA_PROTECTION.
T.PASSWORD_CRACKING	The threat of gaining administrative access to the device by password cracking is countered by O.PASSWORD_PROTECTION and OE.STRONG_PASSWORD.

Threat	Rationale for security objectives
T.NETWORK_DISCLOSURE	The threat of sensitive information being disclosed on the WLAN is countered by O.AUTHENTICATION which ensures that only authorized wireless clients gain access to the network and by O.CRYPTOGRAPHIC_FUNCTIONS which ensures that WLAN traffic is encrypted.
T.NETWORK_ACCESS	The threat of gaining unauthorized access to services via the WLAN is countered by O.AUTHENTICATION which ensures that only authorized wireless clients can connect to the network. In addition, O.TOE_ADMINISTRATION ensures that failed authentication attempts by a remote administrator are handled properly.
T.DATA_INTEGRITY	The threat of WLAN traffic being modified is countered by O.CRYPTOGRAPHIC_FUNCTIONS which ensures that the wireless data packets are integrity protected.
T.REPLAY_ATTACK	The threat of WLAN traffic being replayed is countered by O.AUTHENTICATION which ensures that only authorized wireless clients gain access to the network and by O.CRYPTOGRAPHIC_FUNCTIONS which ensures that replayed data packets will be detected.

Table 6: Sufficiency of objectives countering threats

The following rationale provides justification that the security objectives for the environment are suitable to cover each individual assumption, that each security objective for the environment that traces back to an assumption about the environment of use of the TOE, when achieved, actually contributes to the environment achieving consistency with the assumption, and that if all security objectives for the environment that trace back to an assumption are achieved, the intended usage is supported.

Assumption	**Rationale for security objectives**
A.LIMITED_FUNCTIONALITY	The assumption: - The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose applications (unrelated to networking functionality). Is upheld by: - OE.NO_GENERAL_PURPOSE: There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
A.NO_THRU_TRAFFIC_PROTECTION	The assumption: - A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered. Is upheld by: - OE.NO_THRU_TRAFFIC_PROTECTION: The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
A.PRESHARED_KEY	The assumption:

Assumption	Rationale for security objectives
	• For pre-shared key based authentication of wireless clients, it is assumed that the pre-shared key is provided only to trusted users. is upheld by: • OE.PRESHARED_KEY: For pre-shared key based authentication of wireless clients, the pre-shared key is provided only to trusted users.
A.PHYSICAL_PROTECTION	The assumption: • The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device’s physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. is upheld by: • OE.PHYSICAL: Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
A.TRUSTED_ADMINISTRATOR	The assumption: • The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device.

Assumption	Rationale for security objectives
	is upheld by: • OE.TRUSTED_ADMIN: TOE Administrators are trusted to follow and apply all guidance documentation in a trusted manner.
A.REGULAR_UPDATES	The assumption: • The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities. is upheld by: • OE.UPDATES: The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The assumption: • The Administrator’s credentials (private key) used to access the network device are protected by the platform on which they reside. is upheld by: • OE.ADMIN_CREDENTIALS_SECURE: The administrator’s credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
A.RESIDUAL_INFORMATION	The assumption: • The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the

Assumption	Rationale for security objectives
	equipment is discarded or removed from its operational environment. is upheld by: • OE.RESIDUAL_INFORMATION: The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
A.SERVICES_RELIABLE	The assumption: • When the TOE uses the network services RADIUS and Syslog in the Operational Environment, these services provide reliable information and responses to the TOE. In addition, it is assumed that the Operational Environment protects the communication between the network service and the TOE from loss of confidentiality and integrity, either by physical or logical means. is upheld by: • OE.SERVICES_RELIABLE: The network services RADIUS and Syslog provided in the Operational Environment and used by the TOE must be reliable. In addition, communication between the TOE and the network service must be protected by the Operational Environment.
A.CONNECTIONS	The assumption: • It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks. is upheld by:

Assumption	Rationale for security objectives
	- OE.CONNECTIONS: TOE administrators will ensure that the TOE is installed in a manner that will allow the TOE to effectively enforce its policies on network traffic flowing among attached networks.

Table 7: Sufficiency of objectives holding assumptions

The following rationale provides justification that the security objectives are suitable to cover each individual organizational security policy (OSP), that each security objective that traces back to an OSP, when achieved, actually contributes to the implementation of the OSP, and that if all security objectives that trace back to an OSP are achieved, the OSP is implemented.

OSP	Rationale for security objectives
P.ACCESS_BANNER	The organizational security policy that requires an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE is enforced by O.ACCESS_BANNER.

Table 8: Sufficiency of objectives enforcing Organizational Security Policies

5 Extended Components Definition

This Security Target does not define its own extended components. It uses the following extended components defined in the collaborative Protection Profile for Network Devices, version 2.1 ([NDcPPv2.1]):

- FCS_HTTPS_EXT.1 Extended: HTTPS Protocol
- FCS_RBG_EXT.1 Extended: Random bit generation
- FCS_TLSS_EXT.1 Extended: TLS Server Protocol
- FIA_UIA_EXT.1 Extended: Identification and authentication
- FIA_UAU_EXT.2 Extended: Password-based authentication mechanism
- FPT_SKP_EXT.1 Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
- FPT_APW_EXT.1 Protection of Administrator Passwords
- FPT_TUD_EXT.1 Trusted Update
- FPT_STM_EXT.1 Reliable Time Stamps

This Security Target also uses the following extended components defined in the Network Device Collaborative Protection Profile (NDcPP) Extended Package Wireless Local Area Network (WLAN) Access Systems, version 1.0 ([WLANASEPv1.0]):

- FIA_8021X_EXT.1 Extended: 802.1X Port Access Entity (Authenticator) Authentication
- FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition

Please note that applicable technical decisions for the Network Devices Protection Profile and the WLAN Access Systems Extended Package have been applied.

For completeness of the ST, the extended components definitions are repeated below.

5.1 Cryptographic Support (FCS)

5.1.1 FCS_HTTPS_EXT - HTTPS Protocol

Family Behaviour

Components in this family define the requirements for protecting remote management sessions between the TOE and a Security Administrator. This family describes how HTTPS will be implemented. This is a new family defined for the FCS Class.

Component levelling

FCS_HTTPS_EXT.1 HTTPS requires that HTTPS be implemented according to RFC 2818 and supports TLS.

Management: FCS_HTTPS_EXT.1

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

a) There are no management activities foreseen.

Audit: FCS_HTTPS_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) There are no auditable events foreseen.

FCS_HTTPS_EXT.1 HTTPS Protocol

Hierarchical to: No other components

Dependencies: [FCS_TLSC_EXT.1 TLS Client Protocol, or
FCS_TLSS_EXT.1 TLS Server Protocol]

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement the HTTPS protocol using TLS.

FCS_HTTPS_EXT.1.3 If a peer certificate is presented, the TSF shall [selection: *not establish the connection, request authorization to establish the connection, [assignment: other action]*] if the peer certificate is deemed invalid.

5.1.2 FCS_RBG_EXT - Random Bit Generation

Family Behaviour

Components in this family address the requirements for random bit/number generation. This is a new family defined for the FCS class.

Component levelling

FCS_RBG_EXT.1 Random Bit Generation requires random bit generation to be performed in accordance with selected standards and seeded by an entropy source.

Management: FCS_RBG_EXT.1

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

a) There are no management activities foreseen

Audit: FCS_RBG_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: failure of the randomization process

FCS_RBG_EXT.1 Random Bit Generation

Hierarchical to: No other components

Dependencies: No other components

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [selection*: Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)*].

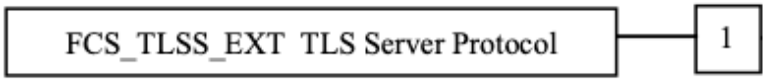
FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [selection: *[assignment: number of software-based sources] software-based noise source, [assignment: number of hardware-based sources] hardware- based noise source*] with a minimum of [selection: *128 bits, 192 bits, 256 bits*] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

5.1.3 FCS_TLSS_EXT - TLS Server Protocol

Family Behaviour

The component in this family addresses the ability for a server to use TLS to protect data between a client and the server using the TLS protocol.

Component levelling



FCS_TLSS_EXT.1 TLS Server requires that the server side of TLS be implemented as specified.

Management: FCS_TLSS_EXT.1

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

a) There are no management activities foreseen.

Audit: FCS_TLSS_EXT.1

The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:

a) Failure of TLS session establishment
b) TLS session establishment
c) TLS session termination

FCS_TLSS_EXT.1 TLS Server Protocol

Hierarchical to: No other components

Dependencies: FCS_CKM.1 Cryptographic KeyGeneration
FCS_CKM.2 Cryptographic KeyEstablishment
FCS_COP.1/DataEncryption Cryptographic operation (AES Data encryption/decryption)
FCS_COP.1/SigGen Cryptographic operation (Signature Generation and Verification)
FCS_COP.1/Hash Cryptographic operation (HashAlgorithm)
FCS_COP.1/KeyedHash Cryptographic operation (Keyed Hash Algorithm)
FCS_RBG_EXT.1 Random Bit Generation

FCS_TLSS_EXT.1.1 The TSF shall implement [selection: *TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)*] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

● [assignment: *list of optional ciphersuites and reference to RFC in which each is defined*].

FCS_TLSS_EXT.1.2 The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and [selection: *TLS 1.1, TLS 1.2, none*].

FCS_TLSS_EXT.1.3 The TSF shall [selection: *perform RSA key establishment with key size [selection: 2048 bits, 3072 bits, 4096 bits]; generate EC Diffie-Hellman parameters over NIST curves [selection: secp256r1, secp384r1, secp521r1] and no other curves; generate Diffie-Hellman parameters of size [selection: 2048 bits, 3072 bits]*].

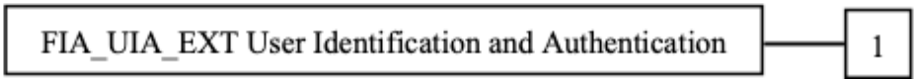
5.2 Identification and Authenticaton (FIA)

5.2.1 FIA_UIA_EXT - User Identification and Authentication

Family Behaviour

The TSF allows certain specified actions before the non-TOE entity goes through the identification and authentication process.

Component levelling



FIA_UIA_EXT.1 User Identification and Authentication requires Administrators (including remote Administrators) to be identified and authenticated by the TOE, providing assurance for that end of the communication path. It also ensures that every user is identified and authenticated before the TOE performs any mediated functions

Management: FIA_UIA_EXT.1

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

a) Ability to configure the list of TOE services available before an entity is identified and authenticated

Audit: FIA_UIA_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) All use of the identification and authentication mechanism
b) Provided user identity, origin of the attempt (e.g. IP address)

FIA_UIA_EXT.1 User Identification and Authentication

Hierarchical to: No other components

Dependencies: FTA_TAB.1 Default TOE Access Banners

FIA_UIA_EXT.1.1 The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- [selection: *no other actions, automated generation of cryptographic keys, [assignment: list of services, actions performed by the TSF in response to non-TOE requests]*].

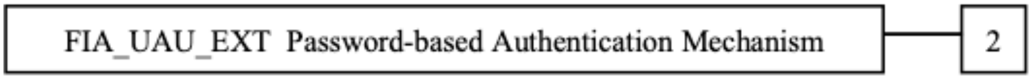
FIA_UIA_EXT.1.2 The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.

5.2.2 FIA_UAU_EXT - User authentication

Family Behaviour

Provides for a locally based administrative user authentication mechanism

Component levelling



FIA_UAU_EXT.2 The password-based authentication mechanism provides administrative users a locally based authentication mechanism.

Management: FIA_UAU_EXT.2

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

a) None

Audit: FIA_UAU_EXT.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: All use of the authentication mechanism

FIA_UAU_EXT.2 Password-based Authentication Mechanism

Hierarchical to: No other components

Dependencies: No other components

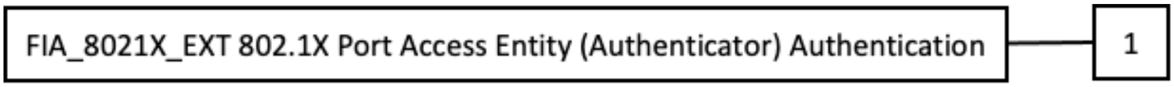
FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism, [selection: *[assignment: other authentication mechanism(s)], no other authentication mechanism*] to perform local administrative user authentication.

5.2.3 FIA_8021X_EXT - 802.1X Port Access Entity (Authenticator) Authentication

Family Behaviour

Components in this family describe requirements for implementation of 802.1X port-based network access control.

Component Leveling


FIA_8021X_EXT 802.1X Port Access Entity (Authenticator) Authentication
1

FIA_8021X_EXT.1, 802.1X Port Access Entity (Authenticator) Authentication, requires the TSF to securely implement IEEE 802.1X as an authenticator.

Management: FIA_8021X_EXT.1

No specific management functions are identified.

Audit: FIA_8021X_EXT.1

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

- Attempts to access the 802.1X controlled port prior to succesul completion of the authentication exchange.

FIA_8021X_EXT.1 802.1X Port Access Entity (Authenticator) Authentication

Hierarchical to: No other components

Dependencies: No other components

FIA_8021X_EXT.1.1 The TSF shall conform to IEEE Standard 802.1X for a Port Access Entity (PAE) in the "Authenticator" role.

FIA_8021X_EXT.1.2 The TSF shall support communications to a RADIUS authentication server conforming to RFCs 2865 and 3579.

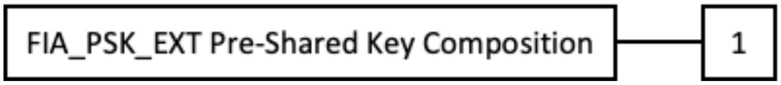
FIA_8021X_EXT.1.3 The TSF shall ensure that no access to its 802.1X controlled port is given to the wireless client prior to successful completion of this authentication exchange.

5.2.4 FIA_PSK_EXT - Pre-Shared Key Composition

Family Behaviour

Components in this family describe requirements for the creation and composition of pre-shared keys used to establish trusted communications channels.

Component Leveling



FIA_PSK_EXT.1, Pre-Shared Key Composition, requires the TSF to support pre-shared keys that meet various characteristics for specific communications usage.

Management: FIA_PSK_EXT.1

No specific management functions are identified.

Audit: FIA_PSK_EXT.1

There are no auditable events foreseen.

FIA_PSK_EXT.1 Pre-Shared Key Composition

Hierarchical to: No other components.

Dependencies to: FCS_RBG_EXT.1 Random Bit Generation

FIA_PSK_EXT.1.1 The TSF shall be able to use pre-shared keys for [selection: *RADIUS over* TLS *(RadSec)*, IPsec, *IEEE 802.11 WPA2-PSK*, *[assignment: other protocols that use pre-shared keys]*].

FIA_PSK_EXT.1.2 The TSF shall be able to accept text-based pre-shared keys that:

- are 22 characters and [selection: *[assignment: other supported lengths]*, *no other lengths*];
- are composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”).

FIA_PSK_EXT.1.3 The TSF shall be able to [selection: *accept*, *generate using the random bit generator specified in FCS_RBG_EXT.1*] bit-based pre-shared keys.

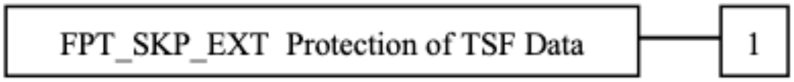
5.3 Protection of the TSF (FPT)

5.3.1 FPT_SKP_EXT - Protection of TSF Data

Family Behaviour

Components in this family address the requirements for managing and protecting TSF data, such as cryptographic keys. This is a new family modelled after the FPT_PTD Class.

Component levelling



FPT_SKP_EXT.1 Protection of TSF Data (for reading all symmetric keys), requires preventing symmetric keys from being read by any user or subject. It is the only component of this family.

Management: FPT_SKP_EXT.1

The following actions could be considered for the management functions in FMT: a) There are no management activities foreseen.

Audit: FPT_SKP_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) There are no auditable events foreseen.

FPT_SKP_EXT.1 Protection of TSF Data (for reading of all symmetric keys)

Hierarchical to: No other components

Dependencies: No other components

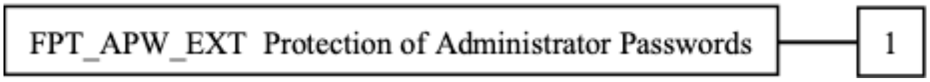
FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

5.3.2 FPT_APW_EXT - Protection of Administrator Passwords

Family Behaviour

Components in this family ensure that the TSF will protect plaintext credential data such as passwords from unauthorized disclosure.

Component levelling



FPT_APW_EXT.1 Protection of Administrator passwords requires that the TSF prevent plaintext credential data from being read by any user or subject.

Management: FPT_APW_EXT.1

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

a) No management functions.

Audit: FPT_APW_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) No audit necessary.

FPT_APW_EXT.1 Protection of Administrator Passwords

Hierarchical to: No other components

Dependencies: No other components

FPT_APW_EXT.1.1 The TSF shall store passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext passwords.

5.3.3 FPT_TUD_EXT - Trusted Update

Family Behaviour

Components in this family address the requirements for updating the TOE firmware and/or software.

Component levelling

FPT_TUD_EXT.1 Trusted Update requires management tools be provided to update the TOE firmware and software, including the ability to verify the updates prior to installation.

FPT_TUD_EXT.2 Trusted update based on certificates applies when using certificates as part of trusted update and requires that the update does not install if a certificate is invalid.

Management: FPT_TUD_EXT.1

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

a) Ability to update the TOE and to verify the updates
b) Ability to update the TOE and to verify the updates using the digital signature capability (FCS_COP.1/SigGen) and [selection: *no other functions, [assignment: other cryptographic functions (or other functions) used to support the update capability]*]
c) Ability to update the TOE, and to verify the updates using [selection: *digital signature, published hash, no other mechanism*] capability prior to installing those updates

Audit: FPT_TUD_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

Initiation of the update process.

Any failure to verify the integrity of the update

FPT_TUD_EXT.1 Trusted Update

Hierarchical to: No other components

Dependencies: FCS_COP.1/SigGen Cryptographic operation (for Cryptographic Signature and Verification), or FCS_COP.1/Hash Cryptographic operation (for cryptographic hashing)

FPT_TUD_EXT.1.1 The TSF shall provide [assignment: *Administrators*] the ability to query the currently executing version of the TOE firmware/software and [selection: *the most recently installed version of the TOE firmware/software; no other TOE firmware/software version*].

FPT_TUD_EXT.1.2 The TSF shall provide [assignment: *Administrators*] the ability to manually initiate updates to TOE firmware/software and [selection: *support automatic checking for updates, support automatic updates, no other update mechanism*].

FPT_TUD_EXT.1.3 The TSF shall provide means to authenticate firmware/software updates to the TOE using a [selection: *digital signature mechanism, published hash*] prior to installing those updates.

5.3.4 FPT_STM_EXT - Reliable Time Stamps

Family Behaviour

Components in this family extend FPT_STM requirements by describing the source of time used in timestamps.

Component levelling

FPT_STM_EXT.1 Reliable Time Stamps is hierarchic to FPT_STM.1: it requires that the TSF provide reliable time stamps for TSF and identifies the source of the time used in those timestamps.

Management: FPT_STM_EXT.1

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

a) Management of the time
b) Administrator setting of the time.

Audit: FPT_STM_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Discontinuous changes to the time.

FPT_STM_EXT.1 Reliable Time Stamps

Hierarchical to: No other components

Dependencies: No other components

FPT_STM_EXT.1.1 The TSF shall be able to provide reliable time stamps for its own use.

FPT_STM_EXT.1.2 The TSF shall [selection: *allow the Security Administrator to set the time, synchronise time with an NTP server*].

6 Security Requirements

6.1 TOE Security Functional Requirements

The Security Functional Requirements (SFRs) have been defined based on components included in CC Part 2, the collaborative Protection Profile for Network Devices Version 2.1 ([NDcPPv2.1]), and NDcPP Extended Package Wireless Local Area Network (WLAN) Access Systems ([WLANASEPv1.0]).

Notice that this ST does not claim conformance to the Network Devices Protection Profile and the WLAN Access Systems Extended Package; instead this ST reuses all the applicable extended components defined in Appendix C of [NDcPPv2.1] and in [WLANASEPv1.0]. In addition, applicable SFRs defined in Chapter 6, Appendix A and Appendix B of [NDcPPv2.1] and in Chapter 4 of [WLANASEPv1.0] are also considered. Please also note that applicable technical decisions for the Network Devices Protection Profile and the WLAN Access Systems Extended Package have been applied. However, this ST assumes that the SFRs are defined in CC Part 2, therefore all assignment, selection, refinement and iteration operations used in the Protection Profile and the Extended Package are repeated here to meet CC Part 2 extended conformance.

The following table shows the SFRs for the TOE, and the operations performed on the components according to CC part 1: iteration (Iter.), refinement (Ref.), assignment (Ass.) and selection (Sel.).

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
FAU - Security audit	FAU_GEN.1 Audit data generation		CC Part 2	No	No	Yes	Yes
	FAU_GEN.2 User identity association		CC Part 2	No	No	No	No
FCS - Cryptographic support	FCS_CKM.1 Cryptographic key generation	FCS_CKM.1	CC Part 2	Yes	Yes	Yes	No
	FCS_CKM.1(2) Cryptographic key generation (Symmetric Keys for WPA2 Connections)	FCS_CKM.1	CC Part 2	Yes	Yes	Yes	No
	FCS_CKM.2 Cryptographic Key Establishment	FCS_CKM.2	CC Part 2	Yes	Yes	Yes	No

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
	FCS_CKM.2(2) Cryptographic Key Distribution (PMK)	FCS_CKM.2	CC Part 2	Yes	Yes	Yes	No
	FCS_CKM.2(3) Cryptographic Key Distribution (GTK)	FCS_CKM.2	CC Part 2	Yes	Yes	Yes	No
	FCS_CKM.4 Cryptographic key destruction		CC Part 2	No	No	Yes	No
	FCS_COP.1/DataEncryption Cryptographic Operation (AES Data Encryption/Decryption)	FCS_COP.1	CC Part 2	Yes	No	Yes	No
	FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)	FCS_COP.1	CC Part 2	Yes	No	Yes	No
	FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)	FCS_COP.1	CC Part 2	Yes	Yes	Yes	No
	FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)	FCS_COP.1	CC Part 2	Yes	Yes	Yes	No
	FCS_RBG_EXT.1 Extended: Random bit generation		NDcPPv2.1	No	No	Yes	Yes
	FCS_HTTPS_EXT.1 Extended: HTTPS Protocol		NDcPPv2.1	No	No	No	Yes
	FCS_TLSS_EXT.1 Extended: TLS Server Protocol		NDcPPv2.1	No	No	No	Yes

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
FIA - Identification and authentication	FIA_AFL.1 Authentication Failure Management		CC Part 2	No	No	Yes	Yes
	FIA_UIA_EXT.1 User Identification and authentication		NDcPPv2.1	No	No	No	Yes
	FIA_UAU_EXT.2 Password-based Authentication Mechanism		NDcPPv2.1	No	No	No	Yes
	FIA_UAU.6 Re-authenticating		CC Part 2	No	Yes	Yes	No
	FIA_UAU.7 Protected authentication feedback		CC Part 2	No	Yes	Yes	No
	FIA_8021X_EXT.1 Extended: 802.1X Port Access Entity (Authenticator)		WLANASEPv1.0	No	No	No	No
	FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition		WLANASEPv1.0	No	No	Yes	Yes
FMT - Security management	FMT_MOF.1/ManualUpdate Management of security functions behaviour	FMT_MOF.1	CC Part 2	Yes	No	Yes	Yes
	FMT_MOF.1/Services Management of security functions behaviour	FMT_MOF.1	CC Part 2	Yes	Yes	Yes	Yes
	FMT_MTD.1/CoreData Management of TSF data	FMT_MTD.1	CC Part 2	Yes	No	Yes	Yes
	FMT_MTD.1/CryptoKeys Management of TSF data	FMT_MTD.1	CC Part 2	Yes	No	Yes	Yes

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
	FMT_SMF.1 Specification of management functions		CC Part 2	No	No	Yes	No
	FMT_SMR.2 Restrictions on security roles		CC Part 2	No	No	Yes	No
FPT - Protection of the TSF	FPT_SKP_EXT.1 Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)		NDcPPv2.1	No	No	No	No
	FPT_APW_EXT.1 Protection of Administrator Passwords		NDcPPv2.1	No	No	No	No
	FPT_TUD_EXT.1 Trusted Update		NDcPPv2.1	No	No	No	Yes
	FPT_STM_EXT.1 Reliable Time Stamps		NDcPPv2.1	No	No	No	Yes
FTA - TOE access	FTA_SSL.3 TSF-initiated Termination		CC Part 2	No	Yes	Yes	No
	FTA_SSL.4 User-initiated Termination		CC Part 2	No	Yes	No	No
	FTA_TAB.1 Default TOE Access Banners		CC Part 2	No	Yes	No	No
	FTA_TSE.1 TOE session establishment		CC Part 2	No	Yes	Yes	No
FTP - Trusted path/channels	FTP_ITC.1 Inter-TSF trusted channel		CC Part 2	No	Yes	Yes	Yes
	FTP_TRP.1/Admin Trusted Path	FTP_TRP.1	CC Part 2	Yes	Yes	Yes	Yes

Table 9: SFRs for the TOE

6.1.1 Security audit (FAU)

6.1.1.1 Audit data generation (FAU_GEN.1)

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

a) Start-up and shut-down of the audit functions;

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

c) **All administrative actions comprising:**

- **Administrative login and logout (name of user account shall be logged if individual user accounts are required for administrators).**
- **Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).**
- **Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).**
- **Resetting passwords (name of related user account shall be logged).**
- **Starting and stopping services.**

d) **Specifically defined auditable events listed in Table 9.**

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

e) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

f) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **information specified in column three of Table 9**.

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FCS_CKM.1	None.	None.
FCS_CKM.1(2)	Failure of the key generation activity.	None.
FCS_CKM.2	None.	None.
FCS_CKM.2(2)	Failure of the key distribution activity.	None.
FCS_CKM.2(3)	Failure of the key distribution activity, including failures related to wrapping the GTK.	Identifier(s) for intended recipients of wrapped key.
FCS_CKM.4	None.	None.
FCS_COP.1/DataEncryption	Failure of WPA2 Encryption or Decryption.	Cryptographic mode of operation, name/identifier of object being encrypted/decrypted, non-TOE endpoint of connection.
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_RBG_EXT.1	None.	None.
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Reason for failure.
FCS_TLSS_EXT.1	Failure to establish a TLS Session.	Reason for failure.

FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.6	Attempts to re-authenticate.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FIA_8021X_EXT.1	Attempts to access the 802.1X controlled port prior to successful completion of the authentication exchange.	Provided client identity (MAC address).
FIA_PSK_EXT.1	None.	None.
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MOF.1/Services	None.	None.
FMT_MTD.1/CoreData	None.	None.
FMT_MTD.1/CryptoKeys	None.	None.
FMT_SMF.1	All management activities of TSF data.	None.
FMT_SMR.2	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None.

FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1).	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism.	Reason for denial, origin of establishment attempt.
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel (including IEEE 802.11) functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	None.

Table 10: Security Functional Requirements and Auditable Events

6.1.1.2 User identity association (FAU_GEN.2)

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.

6.1.2 Cryptographic support (FCS)

6.1.2.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1 The TSF shall generate *asymmetric* cryptographic keys in accordance with a specified cryptographic key generation algorithm*:*

- **RSA schemes using cryptographic key sizes of 2048-bit that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)";**

- **ECC schemes using "NIST curves" P-384 that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)";**

~~and specified cryptographic key sizes~~ ~~that meet the following:~~ .

6.1.2.2 Cryptographic key generation (Symmetric Keys for WPA2 Connections) (FCS_CKM.1(2))

FCS_CKM.1.1(2) The TSF shall generate *symmetric* cryptographic keys in accordance with a specified cryptographic key generation algorithm **PRF-384 and no other** and specified cryptographic key sizes **128 bits and no other key sizes** *using a Random Bit Generator as specified in FCS_RBG_EXT.1* that meet the following: **IEEE 802.11-2016 and no other standards**.

6.1.2.3 Cryptographic Key Establishment (FCS_CKM.2)

FCS_CKM.2.1 The TSF shall ~~distribute cryptographic keys~~ *perform cryptographic key establishment* in accordance with a specified cryptographic key ~~distribution~~ *establishment* method*:*

- **Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";**

~~that meets the following:~~ .

6.1.2.4 Cryptographic key distribution (PMK) (FCS_CKM.2(2))

FCS_CKM.2.1(2) The TSF shall ~~distribute cryptographic keys~~ *receive the 802.11 Pairwise Master Key (PMK)* in accordance with a specified cryptographic key distribution method **from 802.1X Authorization Server** that meets the following: **IEEE 802.11-2016** *and does not expose the cryptographic keys*.

6.1.2.5 Cryptographic key distribution (GTK) (FCS_CKM.2(3))

FCS_CKM.2.1(3) The TSF shall distribute ~~cryptographic keys~~ *Group Temporal Key (GTK)* in accordance with a specified cryptographic key distribution method **AES Key Wrap in an EAPOL-Key frame** that meets the following: **NIST SP 800-38F, IEEE 802.11-2016 for the packet format and timing considerations** *and does not expose the cryptographic keys*.

6.1.2.6 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method

- **For plaintext keys in volatile memory, the destruction shall be executed by a single overwrite consisting of zeroes;**

that meets the following: **No Standard**.

Application Note: There are no plaintext keys stored in the non-volatile storage of the TOE.

6.1.2.7 Cryptographic Operation (AES Data Encryption/Decryption) (FCS_COP.1/DataEncryption)

FCS_COP.1.1 / DataEncryption The TSF shall perform **encryption/decryption** in accordance with a specified cryptographic algorithm **AES used in CBC, CCMP, CTR and GCM mode** and cryptographic key sizes **128 bits and 256 bits** that meet the following: **AES as specified in ISO 18033-3, CCMP as defined in NIST SP 800-38C and IEE 802.11-2016, CBC as specified in ISO 10116, CTR as specified in ISO 10116, GCM as specified in ISO 19772**.

Application Note: AES-CBC and AES-GCM with 128-bit and 256-bit key are used in TLS; AES-CCMP with 128-bit key is used in WPA2; AES-CTR is used for random number generation; and AES-CBC with 128-bit and 256-bit key are used for encryption of keys.

6.1.2.8 Cryptographic Operation (Signature Generation and Verification) (FCS_COP.1/SigGen)

FCS_COP.1.1 / SigGen The TSF shall perform **cryptographic signature services (generation and verification)** in accordance with a specified cryptographic algorithm

- **RSA Digital Signature Algorithm** and cryptographic key sizes **(modulus) 2048 bits and 3072 bits**

that meet the following:

- **For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or**

RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3.

6.1.2.9 Cryptographic Operation (Hash Algorithm) (FCS_COP.1/Hash)

FCS_COP.1.1 / Hash The TSF shall perform **cryptographic hashing services** in accordance with a specified cryptographic algorithm **MD5, SHA-256, SHA-384 and SHA3-256** ~~and cryptographic key sizes~~ *and message digest sizes* **128, 256, 384 bits** that meet the following: **RFC 1321, ISO/IEC 10118-3:2004, and FIPS PUB 202**.

Application Note: MD5 and SHA3-256 together are used for secure storage of passwords. SHA-256 and SHA-384 are used in TLS.

6.1.2.10 Cryptographic Operation (Keyed Hash Algorithm) (FCS_COP.1/KeyedHash)

FCS_COP.1.1 / KeyedHash The TSF shall perform **keyed-hash message authentication** in accordance with a specified cryptographic algorithm **HMAC-SHA-256, HMAC-SHA-384** and cryptographic key sizes **256 and 384 bits** *and message digest sizes 256, 384 bits* that meets the following: **ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"**

Application Note: Both HMAC-SHA-256 and HMAC-SHA-384 are used in TLS.

6.1.2.11 Extended: Random bit generation (FCS_RBG_EXT.1)

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using **Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)**.

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from **two hardware-based noise source** with a minimum of **256 bits** of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

Application Note: Qualcomm WiFi chip used by the TOE provides two noise sources: Received Signal Strength Indicator (RSSI) and Analog-to-Digital (ADC) register.

6.1.2.12 Extended: HTTPS Protocol (FCS_HTTPS_EXT.1)

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS.

FCS_HTTPS_EXT.1.3 If a peer certificate is presented, the TSF shall **not require client authentication** if the peer certificate is deemed invalid.

Application Note: The TOE does not authenticate the HTTPS client. Administrative users are authenticated using password after the HTTPS channel is established between the web server in the TOE and the administrative user's web browser.

6.1.2.13 Extended: TLS Server Protocol (FCS_TLSS_EXT.1)

FCS_TLSS_EXT.1.1 The TSF shall implement **TLS 1.2 ([RFC5246]), TLS 1.1 ([RFC4346])** and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

- **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in [RFC5289]**
- **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in [RFC5289]**
- **TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in [RFC5289]**
- **TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in [RFC5289]**

.

FCS_TLSS_EXT.1.2 The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and **none**.

FCS_TLSS_EXT.1.3 The TSF shall **generate EC Diffie-Hellman parameters over NIST curves secp384r1 and no other curves**.

6.1.3 Identification and authentication (FIA)

6.1.3.1 Authentication Failure Management (FIA_AFL.1)

FIA_AFL.1.1 The TSF shall detect when **an Administrator configurable positive integer within 2 and 5** unsuccessful authentication attempts occur related to **Administrators attempting to authenticate remotely using a password**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until an Administrator defined time period has elapsed**.

Application Note: This SFR applies to Web UI login.

6.1.3.2 User Identification and authentication (FIA_UIA_EXT.1)

FIA_UIA_EXT.1.1 The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- **no other actions**.

FIA_UIA_EXT.1.2 The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.

6.1.3.3 Password-based Authentication Mechanism (FIA_UAU_EXT.2)

FIA_UAU_EXT.2.1 The TSF shall provide a local **password-based** authentication mechanism to perform local administrative user authentication.

6.1.3.4 Protected authentication feedback (FIA_UAU.6)

FIA_UAU.6.1 The TSF shall re-authenticate the *administrative* user under the conditions: **when the user changes their password, no other conditions**.

6.1.3.5 Protected authentication feedback (FIA_UAU.7)

FIA_UAU.7.1 The TSF shall provide only **obscured feedback** to the *administrative* user while the authentication is in progress *at the Web UI*.

6.1.3.6 Extended: 802.1X Port Access Entity (Authenticator) (FIA_8021X_EXT.1)

FIA_8021X_EXT.1.1 The TSF shall conform to IEEE Standard 802.1X for a Port Access Entity (PAE) in the “Authenticator” role.

FIA_8021X_EXT.1.2 The TSF shall support communications to a RADIUS authentication server conforming to RFCs 2865 and 3579.

FIA_8021X_EXT.1.3 The TSF shall ensure that no access to its 802.1X controlled port is given to the wireless client prior to successful completion of this authentication exchange.

6.1.3.7 Extended: Pre-Shared Key Composition (FIA_PSK_EXT.1)

FIA_PSK_EXT.1.1 The TSF shall be able to use pre-shared keys for **IEEE 802.11 WPA2-PSK, no other protocols**.

FIA_PSK_EXT.1.2 The TSF shall be able to accept text-based pre-shared keys that:

- are 22 characters and **lengths from 8 to 63 characters**;
- composed of any combination of upper and lower case letters, numbers, and

  special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”).

FIA_PSK_EXT.1.3 The TSF shall be able to **accept** bit-based pre-shared keys.

6.1.4 Security management (FMT)

6.1.4.1 Management of security functions behaviour (FMT_MOF.1/ManualUpdate)

FMT_MOF.1.1 / ManualUpdate The TSF shall restrict the ability to **enable** the functions **to perform manual updates** to **Security Administrators**.

6.1.4.2 Management of security functions behaviour (FMT_MOF.1/Services)

FMT_MOF.1.1 / Services The TSF shall restrict the ability to **enable, disable**, *start and stop* ~~the functions~~ **services** to **Security Administrators**.

6.1.4.3 Management of TSF data (FMT_MTD.1/CoreData)

FMT_MTD.1.1 / CoreData The TSF shall restrict the ability to **manage** the **TSF data** to **Security Administrators**.

6.1.4.4 Management of TSF data (FMT_MTD.1/CryptoKeys)

FMT_MTD.1.1 / CryptoKeys The TSF shall restrict the ability to **manage** the **cryptographic keys** to **Security Administrators**.

6.1.4.5 Specification of management functions (FMT_SMF.1)

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

- **Ability to administer the TOE remotely;**
- **Ability to configure the access banner;**
- **Ability to configure the session inactivity time before session termination or locking;**

- **Ability to update the TOE, and to verify the updates using hash comparison capability prior to installing those updates;**

- **Ability to configure the authentication failure parameters for FIA_AFL.1;**

- **Ability to start and stop services;**

- **Ability to configure audit behaviour;**

- **Ability to manage the cryptographic keys;**

- **Ability to set the time which is used for time-stamps.**

6.1.4.6 Restrictions on security roles (FMT_SMR.2)

FMT_SMR.2.1 The TSF shall maintain the roles:

- **Security Administrator**.

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions

- **The Security Administrator role shall be able to administer the TOE remotely**

are satisfied.

6.1.5 Protection of the TSF (FPT)

6.1.5.1 Protection of TSF Data (for reading of all pre-shared, symmetric and private keys) (FPT_SKP_EXT.1)

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

6.1.5.2 Protection of Administrator Passwords (FPT_APW_EXT.1)

FPT_APW_EXT.1.1 The TSF shall store administrative passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext administrative passwords.

6.1.5.3 Trusted Update (FPT_TUD_EXT.1)

FPT_TUD_EXT.1.1 The TSF shall provide Security Administrators the ability to query the currently executing version of the TOE firmware/software and **no other TOE firmware/software version**.

FPT_TUD_EXT.1.2 The TSF shall provide Security Administrators the ability to manually initiate updates to TOE firmware/software and **no other update mechanism**.

FPT_TUD_EXT.1.3 The TSF shall provide means to authenticate firmware/software updates to the TOE using a **published hash** prior to installing those updates.

6.1.5.4 Reliable Time Stamps (FPT_STM_EXT.1)

FPT_STM_EXT.1.1 The TSF shall be able to provide reliable time stamps for its own use.

FPT_STM_EXT.1.2 The TSF shall **allow the Security Administrator to set the time**.

6.1.6 TOE access (FTA)

6.1.6.1 TSF-initiated Termination (FTA_SSL.3)

FTA_SSL.3.1 The TSF shall terminate *a remote* interactive session after a **Security Administrator-configurable time interval of session inactivity**.

6.1.6.2 User-initiated Termination (FTA_SSL.4)

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

6.1.6.3 Default TOE Access Banners (FTA_TAB.1)

FTA_TAB.1.1 Before establishing ~~a~~ *an administrative* user session, the TSF shall display ~~an~~ *a Security Administrator-specified* advisory *notice and consent* warning message regarding ~~unauthorised~~ use of the TOE.

6.1.6.4 TOE Session Establishment (FTA_TSE.1)

FTA_TSE.1.1 The TSF shall be able to deny ~~session~~ establishment *of a wireless client session* based on **TOE interface, time, day, and no other attributes**.

6.1.7 Trusted path/channels (FTP)

6.1.7.1 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1 The TSF shall *be capable of using IEEE 802.11-2016 (WPA2), IEEE 802.1X, and no other protocol to* provide a *trusted* communication channel between itself and ~~another trusted IT product~~ *authorized IT entities supporting the following capabilities: WLAN clients, and no other capabilities* that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from ~~modification or~~ disclosure *and detection of modification of the channel data*.

FTP_ITC.1.2 The TSF shall permit **the TSF, *or the authorized IT entities* ~~another trusted IT product~~** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **Wi-Fi communications**.

Application Note: OE.SERVICES_RELIABLE ensures that the communication between the TOE and 802.1X authentication server is protected by the operational environment.

6.1.7.2 Trusted Path (FTP_TRP.1/Admin)

FTP_TRP.1.1/Admin The TSF shall *be capable of using TLS, HTTPS to* provide a communication path between itself and *authorized* **remote** *Administrators* ~~users~~ that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure** *and provides detection of modification of the channel data*.

FTP_TRP.1.2/Admin The TSF shall permit **remote ~~users~~ *Administrators*** to initiate communication via the trusted path.

FTP_TRP.1.3/Admin The TSF shall require the use of the trusted path for **initial ~~user~~ *Administrator* authentication, and all remote administration actions**.

6.2 Security Functional Requirements Rationale

6.2.1 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

Security functional requirements	Objectives
FAU_GEN.1	O.AUDIT,

Security functional requirements	**Objectives**
	O.SYSTEM_MONITORING
FAU_GEN.2	O.AUDIT
FCS_CKM.1	O.CRYPTOGRAPHY
FCS_CKM.1(2)	O.CRYPTOGRAPHIC_FUNCTIONS
FCS_CKM.2	O.CRYPTOGRAPHY
FCS_CKM.2(2)	O.CRYPTOGRAPHIC_FUNCTIONS
FCS_CKM.2(3)	O.CRYPTOGRAPHIC_FUNCTIONS
FCS_CKM.4	O.CRYPTOGRAPHY
FCS_COP.1/DataEncryption	O.CRYPTOGRAPHY, O.CRYPTOGRAPHIC_FUNCTIONS
FCS_COP.1/SigGen	O.CRYPTOGRAPHY
FCS_COP.1/Hash	O.CRYPTOGRAPHY
FCS_COP.1/KeyedHash	O.CRYPTOGRAPHY
FCS_RBG_EXT.1	O.CRYPTOGRAPHY
FCS_HTTPS_EXT.1	O.COMMUNICATION_CHANNELS
FCS_TLSS_EXT.1	O.COMMUNICATION_CHANNELS
FIA_AFL.1	O.PASSWOR_PROTECTION, O.AUTHENTICATION, O.TOE_ADMINISTRATION
FIA_UIA_EXT.1	O.ADMIN_ACCESS
FIA_UAU_EXT.2	O.ADMIN_ACCESS
FIA_UAU.6	O.AUTHENTICATION

Security functional requirements	Objectives
FIA_UAU.7	O.ADMIN_ACCESS, O.PASSWORD_PROTECTION
FIA_8021X_EXT.1	O.AUTHENTICATION
FIA_PSK_EXT.1	O.CRYPTOGRAPHIC_FUNCTIONS
FMT_MOF.1/ManualUpdate	O.ADMIN_ACCESS, O.TRUSTED_UPDATES
FMT_MOF.1/Services	O.ADMIN_ACCESS
FMT_MTD.1/CoreData	O.ADMIN_ACCESS, O.TSF_DATA_PROTECTION
FMT_MTD.1/CryptoKeys	O.ADMIN_ACCESS, O.TSF_DATA_PROTECTION
FMT_SMF.1	O.ADMIN_ACCESS, O.AUDIT, O.TRUSTED_UPDATES, O.TSF_DATA_PROTECTION
FMT_SMR.2	O.ADMIN_ACCESS, O.AUDIT, O.TRUSTED_UPDATES, O.TSF_DATA_PROTECTION
FPT_SKP_EXT.1	O.TSF_DATA_PROTECTION
FPT_APW_EXT.1	O.TSF_DATA_PROTECTION, O.PASSWORD_PROTECTION
FPT_TUD_EXT.1	O.TRUSTED_UPDATES
FPT_STM_EXT.1	O.AUDIT
FTA_SSL.3	O.ADMIN_SESSION
FTA_SSL.4	O.ADMIN_SESSION
FTA_TAB.1	O.ACCESS_BANNER

Security functional requirements	Objectives
FTA_TSE.1	O.AUTHENTICATION
FTP_ITC.1	O.COMMUNICATION_CHANNELS
FTP_TRP.1/Admin	O.COMMUNICATION_CHANNELS

Table 11: Mapping of security functional requirements to security objectives

6.2.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives.

Security objectives	Rationale
O.ADMIN_ACCESS	FIA_UIA_EXT.1 defines that the display of the banner is the only action allowed prior to identification and authentication. FIA_UAU_EXT.2 defines the password-based authentication mechanism, while FIA_UAU.7 requires that password feedback be obscured during authentication. The following SFRs restrict security management functionality to security administrators: FMT_MOF.1/ManualUpdate for Trusted Updates of the TOE, FMT_MOF.1/Services for starting and stopping services, FMT_MTD.1/CryptoKeys for management of cryptographic keys, and FMT_MTD.1/CoreData for management of TSF data. FMT_SMF.1 and FMT_SMR.2 specify the security management functionality associated with this objective.
O.ADMIN_SESSION	FTA_SSL.3 addresses the termination of remote sessions after a specified period of inactivity. FTA_SSL.4 addresses the termination of the session by the administrator.

Security objectives	Rationale
O.CRYPTOGRAPHY	FCS_CKM.1 defines the required standards and key sizes for key generation, while FCS_CKM.2 defines the required standards for key distribution. FCS_COP.1/DataEncryption, FCS_COP.1/SigGen, FCS_COP.1/Hash, FCS_COP.1/KeyedHash define the cryptographic algorithms, modes, key sizes and standards. FCS_RBG_EXT.1 defines the Deterministic Random Bit Generator (DRBG) and the minimum entropy required for key generation. FCS_CKM.4 defines the mechanisms for destroying cryptographic keys.
O.COMMUNICATION_CHANNELS	FTP_ITC.1 and FTP_TRP.1 define trusted communication channels with external IT entities and remote administrators, respectively. Trusted communication channels are secured by the protocols mentioned below. Secure transport protocols are defined in FCS_HTTPS_EXT.1 and FCS_TLSS_EXT.1.
O.TRUSTED_UPDATES	FPT_TUD_EXT.1 specifies the behavior of the verification and installation of software updates by the TOE administrator. FMT_MOF.1/ManualUpdate, FMT_SMF.1 and FMT_SMR.2 specify the security management functionality associated with this objective.
O.AUDIT	FAU_GEN.1 defines the events that the TOE is required to audit. Those events are related to other security functional requirements showing which event contributes to make users accountable for their actions with respect to the requirement. FAU_GEN.2 requires that the events are associated with the identity of the user that caused the event. This association can only be established if the user is known, which is not the case for unsuccessful login attempts. FMT_SMF.1 and FMT_SMR.2 specify the security management functionality associated with this objective. FPT_STM_EXT.1 provides reliable timestamps for generating audit records.

Security objectives	Rationale
O.TSF_DATA_PROTECTION	FPT_SKP_EXT.1 addresses the protection of cryptographic key material, whereas FPT_APW_EXT.1 addresses the protection of administrator passwords. FMT_MTD.1/CoreData, FMT_MTD.1/CryptoKeys, FMT_SMF.1 and FMT_SMR.2 specify security management functionality associated with this objective and its corresponding access constraints.
O.PASSWORD_PROTECTION	FIA_AFL.1 specifies the actions on reaching a threshold number of consecutive password failures. FMT_SMF.1 and FMT_SMR.2 specify the security management functionality associated with this objective. FIA_UAU.7 requires obscured feedback when password is entered at login time. FPT_APW_EXT.1 addresses the protection of administrator passwords.
O.ACCESS_BANNER	FTA_TAB.1 addresses the display of the banner before a session is established.
O.CRYPTOGRAPHIC_FUNCTIONS	FCS_CKM.1(2) addresses the generation of wireless session keys. FCS_CKM.2(2) and FCS_CKM.2(3) address the distribution of PMK and GTK, respectively. FCS_COP.1/DataEncryption addresses the encryption and decryption of wireless data packets using AES-CCMP. FIA_PSK_EXT.1 addresses the use of pre-shared key for WPA2.
O.AUTHENTICATION	FIA_8021X_EXT.1 ensures that no access to the 802.1X controlled port is given to wireless client prior to successful completion of the 802.1X authentication exchange.

Security objectives	Rationale
	FIA_AFL.1 ensures that, after the number of failed authentication attempts reaches the defined threshold, the remote administrator is prevented from logging into the TOE until the configured lockout time has elapsed. FIA_UAU.6 ensures that the administrative user is re-authenticated when the user changes his or her password. FTA_TSE.1 ensures that the TOE is able to deny establishment of wireless client session based on TOE interface, time and day.
O.SYSTEM_MONITORING	FAU_GEN.1 defines the events that the TOE is required to audit, including those that are specific to WLAN operations.
O.TOE_ADMINISTRATION	FIA_AFL.1 addresses failed authentication attempts by a remote administrator.

Table 12: Security objectives for the TOE rationale

6.2.3 Security Requirements Dependency Analysis

The following table demonstrates the dependencies of the SFRs modeled in CC Part 2, the extended component definition in this Security Target and [NDcPPv2.1], and how the SFRs for the TOE resolve those dependencies.

Security functional requirement	Dependencies	Resolution
FAU_GEN.1	FPT_STM.1	FPT_STM_EXT.1
FAU_GEN.2	FAU_GEN.1	FAU_GEN.1
	FIA_UID.1	FIA_UIA_EXT.1
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1]	FCS_CKM.2

Security functional requirement	Dependencies	Resolution
	FCS_CKM.4	FCS_CKM.4
FCS_CKM.1(2)	[FCS_CKM.2 or FCS_COP.1]	FCS_COP.1/DataEncryption
	FCS_CKM.4	FCS_CKM.4
FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
	FCS_CKM.4	FCS_CKM.4
FCS_CKM.2(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Unresolved dependency. Satisfied by FIA_8021X_EXT.1 instead because the PMK is resulted from 802.1X authentication.
	FCS_CKM.4	FCS_CKM.4
FCS_CKM.2(3)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1(2)
	FCS_CKM.4	FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
FCS_COP.1/DataEncryption	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
	FCS_CKM.4	FCS_CKM.4
FCS_COP.1/SigGen	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1

Security functional requirement	**Dependencies**	**Resolution**
	FCS_CKM.4	FCS_CKM.4
FCS_COP.1/Hash	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Unresolved dependency because keys are not required for the hashing algorithms defined in FCS_COP.1/Hash
	FCS_CKM.4	Unresolved dependency because keys are not required for the hashing algorithms defined in FCS_COP.1/Hash
FCS_COP.1/KeyedHash	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
	FCS_CKM.4	FCS_CKM.4
FCS_RBG_EXT.1	No dependencies	
FCS_HTTPS_EXT.1	FCS_TLSC_EXT.1 or FCS_TLSS_EXT.1	FCS_TLSS_EXT.1
FCS_TLSS_EXT.1	FCS_CKM.1	FCS_CKM.1
	FCS_CKM.2	FCS_CKM.2
	FCS_COP.1/DataEncryption	FCS_COP.1/DataEncryption
	FCS_COP.1/SigGen	FCS_COP.1/SigGen
	FCS_COP.1/Hash	FCS_COP.1/Hash
	FCS_COP.1/KeyedHash	FCS_COP.1/KeyedHash

Security functional requirement	Dependencies	Resolution
	FCS_RBG_EXT.1	FCS_RBG_EXT.1
FIA_AFL.1	FIA_UAU.1	FIA_UIA_EXT.1
FIA_UIA_EXT.1	FTA_TAB.1	FTA_TAB.1
FIA_UAU_EXT.2	No dependencies	
FIA_UAU.6	No dependencies	
FIA_UAU.7	FIA_UAU.1	FIA_UIA_EXT.1
FIA_8021X_EXT.1	No dependencies	
FIA_PSK_EXT.1	No dependencies	
FMT_MOF.1/ManualUpdate	FMT_SMR.1	FMT_SMR.2
	FMT_SMF.1	FMT_SMF.1
FMT_MOF.1/Services	FMT_SMR.1	FMT_SMR.2
	FMT_SMF.1	FMT_SMF.1
FMT_MTD.1/CoreData	FMT_SMR.1	FMT_SMR.2
	FMT_SMF.1	FMT_SMF.1
FMT_MTD.1/CryptoKeys	FMT_SMR.1	FMT_SMR.2

Security functional requirement	Dependencies	Resolution
	FMT_SMF.1	FMT_SMF.1
FMT_SMF.1	No dependencies	
FMT_SMR.2	FIA_UID.1	FIA_UIA_EXT.1
FPT_SKP_EXT.1	No dependencies	
FPT_APW_EXT.1	No dependencies	
FPT_TUD_EXT.1	FCS_COP.1/SigGen or FCS_COP.1/Hash	FCS_COP.1/Hash
FPT_STM_EXT.1	No dependencies	
FTA_SSL.3	No dependencies	
FTA_SSL.4	No dependencies	
FTA_TAB.1	No dependencies	
FTA_TSE.1	No dependencies	
FTP_ITC.1	No dependencies	
FTP_TRP.1/Admin	No dependencies	

Table 13: TOE SFR dependency analysis

The security functional requirements in this Security Target do not introduce dependencies on any security assurance requirement; neither do the security assurance requirements in this Security Target introduce dependencies on any security functional requirement.

6.3 Security Assurance Requirements

The security assurance requirements (SARs) for the TOE are the Evaluation Assurance Level 2 components as specified in [CC] part 3, augmented by ALC_FLR.1.

The following table shows the SARs, and the operations performed on the components according to CC part 3: iteration (Iter.), refinement (Ref.), assignment (Ass.) and selection (Sel.).

Security assurance class	**Security assurance requirement**	**Source**	**Operations**			
			Iter.	**Ref.**	**Ass.**	**Sel.**
ADV Development	ADV_ARC.1 Security architecture description	CC Part 3	No	No	No	No
	ADV_FSP.2 Security-enforcing functional specification	CC Part 3	No	No	No	No
	ADV_TDS.1 Basic design	CC Part 3	No	No	No	No
AGD Guidance documents	AGD_OPE.1 Operational user guidance	CC Part 3	No	No	No	No
	AGD_PRE.1 Preparative procedures	CC Part 3	No	No	No	No
ALC Life-cycle support	ALC_CMC.2 Use of a CM system	CC Part 3	No	No	No	No
	ALC_CMS.2 Parts of the TOE CM coverage	CC Part 3	No	No	No	No
	ALC_DEL.1 Delivery procedures	CC Part 3	No	No	No	No
	ALC_FLR.2 Flaw reporting procedures	CC Part 3	No	No	No	No
ASE Security Target evaluation	ASE_INT.1 ST introduction	CC Part 3	No	No	No	No
	ASE_CCL.1 Conformance claims	CC Part 3	No	No	No	No
	ASE_SPD.1 Security problem definition	CC Part 3	No	No	No	No
	ASE_OBJ.2 Security objectives	CC Part 3	No	No	No	No

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
	ASE_ECD.1 Extended components definition	CC Part 3	No	No	No	No
	ASE_REQ.2 Derived security requirements	CC Part 3	No	No	No	No
	ASE_TSS.1 TOE summary specification	CC Part 3	No	No	No	No
ATE Tests	ATE_COV.1 Evidence of coverage	CC Part 3	No	No	No	No
	ATE_FUN.1 Functional testing	CC Part 3	No	No	No	No
	ATE_IND.2 Independent testing - sample	CC Part 3	No	No	No	No
AVA Vulnerability assessment	AVA_VAN.2 Vulnerability analysis	CC Part 3	No	No	No	No

Table 14: SARs

6.4 Security Assurance Requirements Rationale

The chosen assurance level, EAL2, ensures the TOE to be resistant to an attacker possessing a Basic attack potential, commensurate with the threat environment that is experienced by typical consumers of the TOE. As such minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. Additionally, the product vendor has specific customer requests for the evaluation of the TOE at this assurance level. These potential customers of the product vendor have determined for their own networks that an EAL2 evaluation of the product will provide satisfactory assurance.

EAL2 is augmented with ALC_FLR.1 to assist in ensuring that discovered security flaws are tracked and are corrected by the developer and that TOE users are aware of how to report a security flaw and receive corrective fixes.

7 TOE Summary Specification

This section presents a description of how the TOE SFRs are satisfied, organized by security function:

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

7.1 Security Audit

The TOE records audit events for authentication attempts, administrative operations, as well as all of the events identified in Table 9. Each audit record contains the date and time of the event, type of event, subject identity (user, device or process) and outcome (success or failure).

The TOE writes audit records to a fixed segment in the memory. The size of this memory segment is 1M bytes, and when the limit is reached the oldest records are overwritten to accommodate new records.

When the AP reboots, the audit records stored in the memory will get lost. So the TOE transmits all the audit records to a specified, external Syslog server. The operational environment ensures that the communication between the TOE and the Syslog server is secure to protect audit data from loss of integrity or confidentiality (OE.SERVICES_RELIABLE).

An audit record is sent to the remote Syslog server immediately after the event occurs. If communication fails with the syslog server, the audit event is only recorded locally and is not resent.

7.1.1 SFR coverage

The TOE security functionality satisfies the following security functional requirements.

FAU_GEN.1

The audit functionality generates records for the auditable events specified in this SFR, including the general information required as well as the specific information required for each event.

FAU_GEN.2

The TOE ensures that each auditable event is associated with the user or entity that triggered the event, such as administrator's user name and wireless client's MAC/IP address.

7.2 Cryptographic Support

The TOE implements cryptographic protocols and algorithms using the following packages included in the TOE:

- Qualcomm Wi-Fi chips for WPA2 cryptographic algorithm support
- lighttpd v1.4.35 for HTTPS (which uses OpenSSL for TLS implementation)
- OpenSSL v1.0.2n for TLSv1.1, TLSv1.2 and cryptographic algorithm support

7.2.1 WPA2

End-to-end wireless encryption between the TOE and the wireless client is implemented using WPA2.

In case of 802.1X authentication, after the wireless client is successfully authenticated by the RADIUS server, the RADIUS server sends the Pairwise Master Key (PMK) to the TOE. The operational environment ensures that this communication is secure (OE.SERVICES_RELIABLE).

During the 802.11i 4-way handshake, both the TOE and the wireless client have derived the Pairwise Transient Key (PTK). As specified by IEEE 802.11-2016, the PMK, AP's nonce (ANonce), client's nonce (SNonce), AP's MAC address, and client's MAC address are inputs to the key derivation function PRF-384. PRF-384 is a pseudorandom function that uses HMAC-SHA-1 and outputs 384 bits.

The PTK is divided into individual session keys including the Key Encryption Key (KEK), Key Confirmation Key (KCK) and Temporal Key (TK).

A Group Temporal Key (GTK) is generated by the TOE for protecting multicast and broadcast communications. The TOE distributes this key by using AES Key Wrap in an EAPOL-Key frame that meets NIST SP 800-38F and IEEE 802.11-2016 for the packet format and timing consideration. The GTK is encrypted with the KEK to prevent key exposure during the distribution. The wireless client uses the KCK to confirm the receipt of the GTK.

The TK, also known as the CCMP key, is the 802.11i session key for unicast communications. AES-CCMP provides not only encryption but also integrity protection using the Cipher Block Chaining Message Authentication Code (CBC-MAC).

The keys used by WPA2, i.e. PMK, PTK, GTK, KEK, KCK and TK, are destroyed using zeroization when no longer needed.

7.2.1.1 SFR coverage

The TOE security functionality satisfies the following security functional requirements.

FCS_CKM.1(2)

The TOE derives the PTK using PRF-384.

FCS_CKM.2(2)

The TOE receives the PMK from the RADIUS authentication server after successful authentication of the wireless client.

FCS_CKM.2(3)

The TOE distributes the GTK by using AES Key Wrap in an EAPOL-Key frame that meets NIST SP 800-38F and IEEE 802.11-2016 for the packet format and timing consideration.

FCS_CKM.4

The TOE destroys the WPA2 keys using zeroization when they are no longer needed.

FCS_COP.1/DataEncryption

The TOE encrypts/decrypts WLAN data packets using AES_CCMP with 128-bit key.

7.2.2 OpenSSL cryptographic module

OpenSSL implements versions 1.1 and 1.2 of the Transport Layer Security (TLS) protocol and cryptographic algorithms. The following table summarizes the cryptographic algorithms implemented in OpenSSL and used by the TOE to support communication protocols, protection of TSF data and authentication.

Cryptographic Services	Cryptographic Algorithms and Key Sizes	Usage / Purpose
Key Generation	RSA 2048-bit keys	TLSv1.1 and TLSv1.2
	ECDSA P-384 ephemeral keys	TLSv1.1 and TLSv1.2
Key Establishment	Elliptic curve based, P-384 keys	TLSv1.1 and TLSv1.2
Encryption / Decryption	AES in CBC mode, 128 and 256 bit keys	TLSv1.1 and TLSv1.2 Private key protection (AES-256) WPA2 PSK protection (AES-128)
	AES in CTR mode, 128 and 256 bit keys	Random number generation
	AES in GCM mode, 128 and 256 bit keys	TLSv1.1 and TLSv1.2

Cryptographic Services	Cryptographic Algorithms and Key Sizes	Usage / Purpose
Signature Generation	RSA PKCS#1 v1.5 with SHA-256, using 2048-bit key	TLSv1.1 and TLSv1.2
Message Digest	SHA-256	Signature generation Keyed hashing
	SHA-384	Keyed Hashing
	MD5 and SHA3-256	Password storage
Keyed Hashing	HMAC-SHA-256 with 256-bit key	TLSv1.1 and TLSv1.2
	HMAC-SHA-384 with 384-bit key	
DRBG	Hash_DRBG (default), CTR_DRBG, HMAC_DRBG	Asymmetric key generation Session key generation

Table 15: Cryptographic Services and Algorithms

OpenSSL includes a Deterministic Random Bit Generator (DRBG) used for key generation and random data (e.g. shared secrets). The DRBG uses the Hash_DRBG with SHA-256 algorithm by default; if there is a failure in the instantiation, the DRBG will fall back to CTR_DRBG, and then to HMAC_DRBG.

The Qualcomm chip in the TOE provides entropy by updating /dev/random with Received Signal Strength Indicator (RSSI) and/or Analog-to-Digital (ADC) register based on the mode. There are 3 modes:

- Mode0 – Random is updated by RSSI on interrupt
- Mode1 – Random is updated by RSSI every 10ms, and if the same RSSI is read for 5 times, it is read from ADC registers and a sleep of 100 ms occurs
- Mode2 – Random is updated by ADC registers alone every 100 ms

The TOE uses Mode1.

OpenSSL maintains in RAM all critical security parameters (CSP) used by the cryptographic services (DRBG internal state, session keys, etc.) requested by the TOE. OpenSSL clears with zeroes and deallocates all the memory used by the CSP when they are no longer needed.

7.2.2.1 Transport Layer Security (TLS) protocol

The TOE implements versions 1.1 and 1.2 of the TLS protocol provided by OpenSSL. The TOE establishes a secure channel using TLS/HTTPS for communication with the web browser on the administrator workstation.

The TOE acts as a TLS server and authenticates to the client using a certificate. The TOE does not authenticate the TLS client.

The TOE only allows the establishment of a TLS secure channel using TLSv1.1 or TLSv1.2. The TOE denies any attempt by a TLS client to establish communication using the following versions of the SSL or TLS protocols: SSLv1.0, SSLv2.0, SSLv3.0 or TLSv1.0.

The TOE creates session keys following the TLS protocol specification and using the DRBG implemented in OpenSSL. The TOE destroys session keys when the session is terminated by clearing with zeroes and deallocating the RAM memory used to store the session keys.

The TOE supports the following cipher suites:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

The TOE implements the Supported Elliptic Curves Extension according to [RFC4492] with NIST curve secp384r1. There is no security management function to configure its behavior.

ECDHE key agreement parameters used for server key exchange are determined based on the selected NIST curve, as described in [RFC8422].

The following table shows the cryptographic keys involved in the TLS protocol, their location and how they are created and destroyed:

Certificate / Key	Certificate / Key Location	Purpose	Destruction
TOE server certificate (public and private keys)	Flash (private key AES-256 encrypted)	TOE authentication (TOE acting as TLS server)	As the private key is stored encrypted, no destruction is needed
Session keys (AES encryption keys and HMAC keys)	RAM	Integrity and confidentiality during session	Zeroization and deallocation when session is terminated

Table 16: Certificates and keys used by the TLS protocol

7.2.2.2 SFR coverage

The TOE security functionality satisfies the following security functional requirements.

FCS_CKM.1

The TOE generates RSA and ECDSA asymmetric cryptographic keys that are used to protect communications for TLSv1.1, TLSv1.2 and HTTPS.

FCS_CKM.2

The TOE performs key establishment based on ECDSA asymmetric cryptographic keys that are used to protect communications for TLSv1.1, TLSv1.2 and HTTPS.

FCS_CKM.4

The TOE destroys key material by overwriting it with zeroes and releasing the allocated memory only after a read-verify to ensure it was properly zeroized.

FCS_COP.1/DataEncryption

OpenSSL implements AES encryption and decryption in accordance to this SFR.

FCS_COP.1/SigGen

OpenSSL implements RSA signature generation in accordance to this SFR.

FCS_COP.1/Hash

OpenSSL implements MD5, SHA-256, SHA-384 and SHA3-256 hashing algorithms in accordance to this SFR.

FCS_COP.1/KeyedHash

OpenSSL implements HMAC keyed hashing algorithm with SHA-256 and SHA-384 in accordance to this SFR.

FCS_RBG_EXT.1

OpenSSL implements DRBG algorithms in accordance to this SFR. The TOE provides an entropy source for seeding the DRBG with a minimum of 256 bits.

FCS_HTTPS_EXT.1

The TOE provides HTTPS [RFC2818] for the Web UI. HTTPS uses TLS to securely establish the remote session.

FCS_TLSS_EXT.1

OpenSSL implements TLSv1.1 and TLSv1.2 protocols in accordance to this SFR. The TOE supports the cipher suites selected in this SFR.

7.3 Identification and Authentication

7.3.1 Identification and Authentication of TOE Administrators

The TOE requires the administrator to identify and authenticate themselves prior to accessing the TOE. The administrator logs into the TOE through the Web UI. The Web UI is accessible over HTTPS only and the authentication of administrator is determined by a username and password combination after the HTTPS connection. The authentication is performed locally on the TOE using local user database.

For web users, there are three accounts: Administrator, Viewer and GuestOperator. The Administrator account allows configuring and viewing the whole system, the Viewer account allows checking configuration and monitoring of WLAN operations, while GuestOperator only has the privilege to edit the users for captive portal (disabled in the evaluated configuration). User names and passwords are stored in /etc/cluster_config/man_user.conf in the flash and in /var/config/man_user.conf in the RAM. The passwords stored in the flash are double hashed by MD5 and SHA3-256.

If the user and password information match the authentication data stored in the TOE, authentication succeeds and the user is granted access.

The TOE provides the following user authentication failure settings:

- *Lockout threshold*: The number of failed user login attempts allowed before the user account is locked (2-5). The default lockout threshold is set to 3.

- *Lockout duration*: The length of time a user account remains locked until it is automatically unlocked. The valid range is 1 to 15 minutes. The default lockout duration is set to 1 minute.

The TOE ensures that if the number of failed user login attempts exceeds the lockout threshold, the user account is locked out for the lockout duration. The user's authentication failure counter is reset when the user successfully authenticates.

For Web UI login, the TOE does not display the password characters; instead, a dot is echoed for each character input.

7.3.1.1 SFR coverage

The TOE security functionality satisfies the following security functional requirements.

FIA_AFL.1

The TOE prevents the establishment of a remote session after a defined number of unsuccessful attempts using the password-based authentication method.

FIA_UIA_EXT.1

The TOE displays a warning banner before an administrative user attempts to login through the Web UI.

FIA_UAU_EXT.2, FIA_UAU.7

The TOE provides a local password-based mechanism to authenticate administrative users, where passwords are not shown during the identification and authentication process.

FIA_UAU.6

The TOE re-authenticates the administrator when his or her password is changed.

7.3.2 Identification and Authentication of Wireless Clients

The TOE authenticates wireless clients using the following authentication mechanisms: IEEE 802.1X authentication or PSK-based authentication.

In IEEE 802.1X authentication, the TOE creates a virtual port for the wireless client and sets it to an "unauthorized" state. In this state, only 802.1X traffic from the wireless client is allowed; other network traffic is blocked. Next, the TOE (authenticator) sends out the EAP-Request identity to the supplicant, the supplicant responds with the EAP-response packet that the TOE forwards to the RADIUS authentication server (which is part of the operational environment). More EAP messages are relayed by the TOE between the RADIUS server and the wireless client until the authentication of the wireless client completes. Successful authentication results in a secret key called Pairwise Master Key (PMK) to be shared by the RADIUS server and the wireless client.

The RADIUS server sends a copy of the PMK to the TOE. If PSK-based authentication has been used instead of 802.1X authentication, the PMK is the same as the PSK. The TOE and the wireless client then carry out a 4-way handshake to establish a secure session:

1. The TOE generates a random number (ANonce) and sends it to the wireless client.
2. The wireless client also generates a nonce (SNonce). It derives a Pairwise Transient Key (PTK) from the PMK, ANonce, SNonce, TOE’s MAC address, and the wireless client’s MAC address. The wireless client sends SNonce together with a message integrity code (MIC) to the TOE.
3. The TOE also derives the PTK using a pseudorandom function (PRF) and verifies the received MIC. The PTK includes a Key Encryption Key (KEK). The TOE generates a Group Temporal Key (GTK) and encrypts it with the KEK. It sends the encrypted GTK, together with a new MIC, to the wireless client.
4. The wireless client is able to decrypt the GTK as it has derived its own copy of the KEK. It verifies the MIC received from the TOE and if valid sends a confirmation to the TOE.

If the 4-way handshake is successful, the TOE sets the virtual port to the "authorized" state and wireless traffic from the wireless client is allowed to pass on to the wired network.

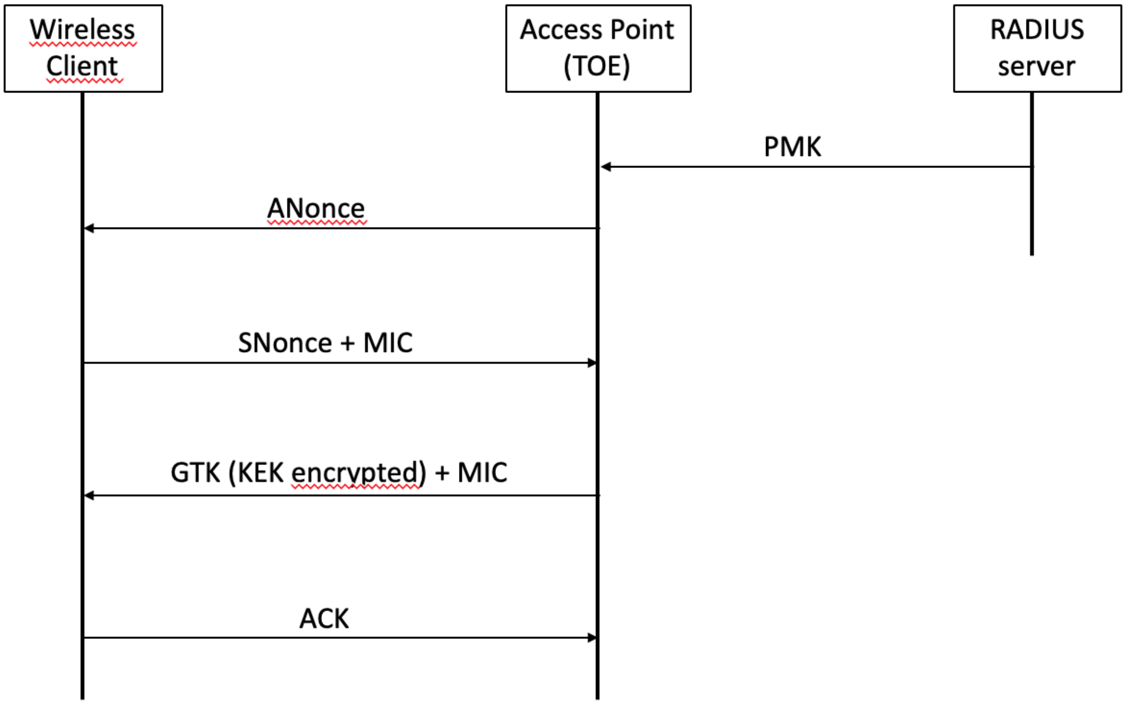


Figure 3: IEEE 802.11i 4-way Handshake

802.1X requires the use of a RADIUS server as an external authentication server, which is part of the operational environment. The operational environment ensures that the communication between the TOE and the RADIUS server is secure.

PSK for wireless client can be entered either as a string of 64 hexadecimal digits, or as a passphrase of 8 to 63 printable ASCII characters. In the latter case, the PSK used for 802.11i 4-way handshake is derived from the passphrase, together with SSID and other parameters. The passphrase/PSK is encrypted by AES-128 before being stored in the TOE.

7.3.2.1 SFR coverage

The TOE security functionality satisfies the following security functional requirements.

FIA_8021X_EXT.1

The TOE acts as 802.1X Authenticator and relays EAP packets between wireless client and the RADIUS server.

FIA_PSK_EXT.1

The TOE supports PSK for wireless client authentication. The PSK is between 8 and 63 characters and must be composed of any combination of upper and lower case letters, numbers, and special characters (that include: '!', '@', '#', '$', '%', '^', '&', '*', '(', and ')').

7.4 Security Management

The TOE provides the following management functions for use by security administrators:

- Configure the access banner for login sessions
- Configure session inactivity time before session termination
- Install TOE firmware updates with the capability of verifying the integrity of those updates
- Configure authentication failure parameters for FIA_AFL.1 (number of unsuccessful authentication attempts before account lockout and lockout period)
- Start and stop the WLAN services
- Configure audit behavior (Syslog settings)
- Manage cryptographic keys (e.g. WPA2 pre-shared key/passphrase)
- Set the date and time

The above security management functions can be performed through the Web UI. Use of each of these management functions is restricted to the Administrator. As described in section 7.3.1, Viewer and GuestOperator do not have the privilege to manage the TOE.

7.4.1 SFR coverage

The TOE security functionality satisfies the following security functional requirements.

FMT_MOF.1/ManualUpdate

The TOE restricts security administrators to perform manual updates of the TOE software.

FMT_MOF.1/Services

The TOE restricts the ability to start and stop the WLAN services to security administrators.

FMT_MTD.1/CoreData

The TOE restricts security administrators to manage TSF data.

FMT_MTD.1/CryptoKeys

The TOE restricts security administrators to manage cryptographic keys.

FMT_SMF.1

The TOE provides the security management functions specified in this SFR.

FMT_SMR.2

The TOE supports the Security Administrator role, who is the only role authorized to administer the TOE remotely.

7.5 Protection of the TSF

Passwords are stored in non-plaintext form using two hashing algorithms in sequence: MD5 and SHA3-256.

The TOE stores pre-shared keys, symmetric keys and private keys in encrypted form using AES. This prevents users, including administrators, from reading the keys.

The TOE does not provide a mechanism for automatic updates of the TOE. The administrator is responsible for downloading the new version of the TOE and the corresponding SHA-256 hash value (firmware image and hash value files) from the vendor's secure website. The administrator performs the hash verification outside the TOE. The TOE provides via the Web UI for installing and updating the TOE in a secure way:

- View the currently executing version of the TOE firmware.
- Upload new version of the TOE firmware to the TOE via the Web UI
- Verify the integrity of the uploaded image file that represents the TOE firmware against the MD5 checksum.

If the MD5 checksum is verified successfully, the new version of the TOE firmware is installed and the administrator must reboot the TOE in order to make the changes effective. If the verification fails, then the TOE image is rejected and not installed. The administrator should follow the instructions included in the TOE guidance to securely download, and install and/or update the TOE.

The TOE provides a reliable date and time for the following security functions:

- Generation of a timestamp for audit events.
- Calculation of period of inactivity of an interactive session to evaluate the termination of user sessions.

The TOE obtains the date and time from an internal system clock. This system clock can be updated by the security administrator through the Web UI.

7.5.1 SFR coverage

The TOE security functionality satisfies the following security functional requirements.

FPT_SKP_EXT.1

The TOE stores key material in encrypted form which prevents read/access from any user, including administrators.

FPT_APW_EXT.1

The TOE stores passwords in encrypted form which prevents read/access from any user, including administrators.

FPT_TUD_EXT.1

The TOE allows administrators to verify the currently executing version of the TOE firmware. It also allows manual updates of the TOE firmware, verifying its integrity using a published hash before being installed.

FPT_STM_EXT.1

The TOE has an internal system clock which is used to generate reliable timestamps for security related purposes like auditing.

7.6 TOE Access

Before a remote session is established, a banner is displayed to the user that attempts to log into the TOE. An administrator of the TOE can modify the content of this banner to display warnings or advisory notices that reflect the security policy of the organization.

The TOE monitors the time of inactivity of remote sessions. It terminates a session if no user activity is detected for the administrator configured period of time. The user must re-authenticate in order to set up a new session. The inactivity period can be configured between 5 and 60 minutes and the default is 30 minutes.

The user can terminate his or her own session at any time.

The administrator can via the Web UI enable WLAN service on a selected SSID for certain weekdays and hours only. The TOE will then deny establishment of connections from wireless clients at other time.

7.6.1 SFR coverage

The TOE security functionality satisfies the following security functional requirements.

FTA_SSL.3

The TOE terminates remote sessions after a period of inactivity.

FTA_SSL.4

An administrative user can terminate a remote session (the user's own session) at any time.

FTA_TAB.1

The TOE allows the configuration of a banner shown to the user before an interactive session is established.

FTA_TSE.1

The TOE can deny establishment of wireless client session based on time, day and WLAN SSID.

7.7 Trusted Path/Channels

The TOE uses WPA2 and 802.1X to authenticate wireless clients and set up a secure communication channel between itself and each wireless client.

The TOE also provides a trusted communication path using the HTTPS protocol for sessions remotely initiated by administrators.

The TOE has a default certificate installed for the HTTPS server. The corresponding private key is encrypted by AES-256. Both the certificate and encrypted private key are stored in the flash.

The following table summarizes the services used by the TOE and how they are protected.

Purpose	**External IT entity**	**Secure channel**
Wireless communication	Wireless client	WPA2, 802.1X
Management of the TOE	Web browser on the administrator workstation	HTTPS (TLSv1.1 or TLSv1.2)

Table 17: Trusted channels

Please refer to Section 7.2 for a summary of TLS and the associated cryptographic support measures implemented by the TOE.

7.7.1 SFR coverage

The TOE security functionality satisfies the following security functional requirements.

FTP_ITC.1

All communications between the TOE and wireless clients are protected using a secure channel via WPA2 and 802.1X protocols.

FTP_TRP.1/Admin

All communications initiated by remote administrators to the TOE are protected using a secure channel via the HTTPS (TLSv1.1 or TLSv1.2) protocol.

8 Abbreviations, Terminology and References

8.1 Abbreviations

AES

Advanced Encryption System

ALE

Alcatel-Lucent Enterprise

AP

Access Point

ARM

Advanced RISC Machine

AWOS

Alcatel-Lucent Enterprise Wireless Operation System

CBC

Cipher Block Chaining

CLI

Command Line Interface

CSP

Critical Security Parameter

DHCP

Dynamic Host Configuration Protocol

DNS

Domain Name Server

DRBG

Deterministic Random Bit Generator

DSA

Digital Signature Algorithm

EAP

Extensible Authentication Protocol

ECD

Extended Component Definition

ECDH

Elliptic Curve Diffie-Hellman

ECDHE

Elliptic Curve Diffie-Hellman Exchange

ECDSA

Elliptic Curve Digital Signature Algorithm

HMAC

Keyed-Hash Message Authentication Code

HTTPS

Hypertext Transfer Protocol Secure

IEEE

Institute of Electrical and Electronics Engineers

IP

Internet Protocol

IPv4

Internet Protocol version 4

IPv6

Internet Protocol version 6

LAN

Local Area Network

PAE

Port Access Entity

PoE

Power over Ethernet

RADIUS

Remote Authentication Dial In User Service

RSA

Rivest Shamir Adleman (cryptosystem)

SFTP

Secure File Transfer Protocol

SNMP

Simple Network Management Protocol

SSID

Service Set Identifier

TCP

Transmission Control Protocol

TFTP

Trivial File Transfer Protocol

TLS

Transport Layer Security

UDP

User Datagram Protocol

USB

Universal Serial BUS

WLAN

Wireless LAN

8.2 Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise.

Administrator

An administrative user of the TOE, authorized to control TOE settings, as opposed to end-users, associated with general network traffic.

CAVP

The NIST Cryptographic Algorithm Validation Program provides validation testing of Approved (i.e., FIPS-approved and NIST-recommended) cryptographic algorithms and their individual components.

End-user

Network traffic, non-administrative users of the TOE.

IEEE 802.1X

IEEE 802.1X is an IEEE Standard for port-based Network Access Control.

MAC Address

Media Access Control Address, also known as the hardware or adaptor address.

Power over Ethernet

Power over Ethernet (PoE) provides inline power directly from the switch's Ethernet ports. Powered Devices (PDs) such as IP phones and wireless APs can be powered directly from the switch's RJ-45 ports.

Security Administrator

The terms “Administrator” and “Security Administrator” are used interchangeably in this document.

Web UI

The web based GUI to manage the TOE.

8.3 References

APGUIDE **Alcatel-Lucent Enterprise OmniAccess Stellar AP User Guide – AWOS 4.0.1**

Version 033517-10 Rev. B

Date October 2020

CC **Common Criteria for Information Technology Security Evaluation**

Version 3.1R5

Date April 2017

Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf

Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf

Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf

CCECG **Common Criteria Evaluated Configuration Guide for Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Points**

Version 0.3

Date 2020-11-02

NDcPPv2.1 **collaborative Protection Profile for Network Devices Version 2.1**

Version 2.1

Date 2019-03-11

Location https://www.niap-ccevs.org/MMO/PP/CPP_ND_V2.1.pdf

RFC1321 **The MD5 Message-Digest Algorithm**

Author(s) R. Rivest

Date April 1992

Location http://www.ietf.org/rfc/rfc1321.txt

RFC3268 **Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)**

Author(s) P. Chown

Date 2002-06-01

Location http://www.ietf.org/rfc/rfc3268.txt

RFC4346 **The Transport Layer Security (TLS) Protocol Version 1.1**

Author(s) T. Dierks, E. Rescorla

Date 2006-04-01

Location http://www.ietf.org/rfc/rfc4346.txt

RFC4492 **Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)**

Author(s) S. Blake-Wilson, N. Bolyard, V. Gupta, C. Hawk, B. Moeller

Date 2006-05-01

Location http://www.ietf.org/rfc/rfc4492.txt

RFC5246 **The Transport Layer Security (TLS) Protocol Version 1.2**

Author(s) T. Dierks, E. Rescorla

Date 2008-08-01

Location http://www.ietf.org/rfc/rfc5246.txt

RFC5288 **AES Galois Counter Mode (GCM) Cipher Suites for TLS**

Author(s) J. Salowey, A. Choudhury, D. McGrew

Date 2008-08-01

Location http://www.ietf.org/rfc/rfc5288.txt

RFC5289 **TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)**

Author(s) E. Rescorla

Date 2008-08-01

Location http://www.ietf.org/rfc/rfc5289.txt

RFC8017 **PKCS #1: RSA Cryptography Specifications Version 2.2**

Author(s) K. Moriarty, B. Kaliski, J. Jonsson, A. Rusch

Date 2016-11-01

Location http://www.ietf.org/rfc/rfc8017.txt

RFC8422 **Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier**

Author(s) Y. Nir, S. Josefsson, M. Pegourie-Gonnard

Date 2018-08-01

Location http://www.ietf.org/rfc/rfc8422.txt

WLANASEPv1.0 **Network Device Collaborative Protection Profile (NDcPP) Extended Package Wireless Local Area Network (WLAN) Access Systems**

Version 1.0

Date	2015-05-29
Location	https://www.niap-ccevs.org/MMO/PP/pp_wlan_as_ep_v1.0.pdf