Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Points with AWOS 5.0 Security Target

Document Version: 1.9
Date: September 23, 2026

2400 Research Blvd
Suite 395
Rockville, MD 20850

Revision History

Version	Date	Changes
Version 1.0	September 11, 2025	Initial Release
Version 1.1	November 10, 2025	Updates based on vendor feedback
Version 1.2	December 26 2025	Updates based on internal review
Version 1.3	January 5, 2026	Minor update
Version 1.4	March 31, 2026	Update based on internal review
Version 1.5	May 29, 2026	Update based on vendor feedback
Version 1.6	June 16, 2026	For Check-in ECRs.
Version 1.7	July 02, 2026	Minor Update
Version 1.8	August 19, 2026	For Check-out ECRs
Version 1.9	September 23, 2026	For 2nd round Check-out ECRs

Contents

1. Introduction 5
1.1 Security Target and TOE Reference 5
1.2 TOE Overview 5
1.3 TOE Description 12
1.3.1 Physical Boundaries 13
1.3.2 Security Functions Provided by the TOE 14
1.3.3 TOE Documentation 16
1.4 TOE Environment 17
1.5 Product Functionality not Included in the Scope of the Evaluation 17
2. Conformance Claims 18
2.1 CC Conformance Claims 18
2.2 Protection Profile Conformance 18
2.3 Conformance Rationale 18
2.3.1 Technical Decisions 18
3. Security Problem Definition 20
3.1 Threats 20
3.2 Assumptions 22
3.3 Organizational Security Policies 24
4. Security Objectives 25
4.1 Security Objectives for the TOE 25
4.2 Security Objectives for the Operational Environment 25
5. Security Requirements 27
5.1 Conventions 28
5.2 Security Functional Requirements 28
5.2.1 Security Audit (FAU) 29

5.2.1.5 Cryptographic Support (FCS) 33
5.2.2 Identification and Authentication (FIA) 38
5.2.3 Security Management (FMT) 40
5.2.4 Protection of the TSF (FPT) 42
5.2.5 TOE Access (FTA) 43
5.2.6 Trusted Path/Channels (FTP) 44
5.3 TOE SFR Dependencies Rationale for SFRs 45
5.4 Security Assurance Requirements 46
5.5 Assurance Measures 47
6. TOE Summary Specification 49
6.1 TOE Summary Specification SFR Description 49
6.1.1 Security Audit (FAU) 49
6.1.2 Cryptographic Support (FCS) 50
6.1.3 Identification and Authentication (FIA) 55
6.1.4 Security Management (FMT) 57
6.1.5 Protection of the TSF (FPT) 59
6.1.6 TOE Access (FTA) 60
6.1.7 Trusted Path/Channels (FTP) 61
6.2 CAVP Algorithm Certificate Details 62
6.3 Cryptographic Key Destruction 64
7. Acronym Table 65

1. INTRODUCTION

The Security Target (ST) serves as the basis for the Common Criteria (CC) evaluation and identifies the Target of Evaluation (TOE), the scope of the evaluation, and the assumptions made throughout. This document will also describe the intended operational environment of the TOE, and the functional and assurance requirements that the TOE meets.

1.1 SECURITY TARGET AND TOE REFERENCE

This section provides the information needed to identify and control the TOE and the ST.

Table 1 – TOE/ST Identification

Category	Identifier
ST Title	Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Points with AWOS 5.0 Security Target
ST Version	1.9
ST Date	September 23, 2026
ST Author	Intertek Acumen Security
TOE Identifier	Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Points with AWOS 5.0
TOE Version	5.0
TOE Developer	ALE USA Inc.
Key Words	Network Device, Access Point, WLAN

1.2 TOE OVERVIEW

The TOE is the Alcatel-Lucent Enterprise (ALE) OmniAccess Stellar Wireless Access Points (WAPs) running AWOS 5.0, in the standalone mode. It is classified as a Network Device. This classification aligns with the Collaborative Protection Profile for Network Devices, as the TOE serves as a critical network component that connects wireless clients to the wired infrastructure, enforces access control, and provides essential security functions. The TOE fulfills the Network Device infrastructure role by providing the network interface that enables secure authenticated WLAN access, which is a fundamental use case covered by the NDcPP. These devices are designed to deliver secure, high-performance wireless connectivity for enterprise environments, with both models implementing the latest Wi-Fi 7 (IEEE 802.11be) standard to meet the demands of modern mobility and the growing number of IoT devices. The TOE provides secure connectivity with remote audit servers, supports administrator identification and authentication prior to management access, enforces session termination after inactivity, and verifies the integrity of firmware updates before installation.

- **AP 1501**

The Alcatel-Lucent OmniAccess® Stellar AP1501 delivers an accessible entry point into Wi-Fi 7, combining next-generation wireless performance with the cost efficiency enterprises expect. The OmniAccess Stellar AP1501

makes Wi-Fi 7 performance affordable for everyday connectivity. Built for mid-density and distributed environments such as branch offices, retail locations and small campuses, it delivers the high bandwidth, low latency and reliability required by next-generation mobility and connected services. With Alcatel- Lucent Enterprise's proven enterprise wireless architecture, the OmniAccess Stellar AP1501 enables organizations to modernize their wireless networks with confidence, efficiency, and long-term value.

The OmniAccess Stellar AP1501 is powered by three radios serving Wi-Fi clients. The OmniAccess Stellar AP1501 supports a maximum aggregate data rate of 9.328 Gbps (688 Mbps in 2.4GHz, 2.882 Gbps in 5GHz, 5.76 Gbps in 6GHz). As part of the optimized design, the OmniAccess Stellar AP1501 uses a Multigigabit Ethernet interface capable of 2.5 Gbps, suited for those spaces with a mid-density of wireless clients, but with intensive bandwidth needs.

The OmniAccess Stellar AP1501 supports 802.11be features, including MLO, OFDMA, DL MU-MIMO, UL MUMIMO, 4096-QAM modulation and more. These features make tomorrow's diverse digital workspaces highly reliable and efficient.

The OmniAccess Stellar AP1501 features enhanced WLAN technology with RF Radio Dynamic Adjustment, a distributed control Wi-Fi architecture, secure network admission control (NAC) with Unified Access and built-in application intelligence and analytics (Layer 7). This makes it ideal for enterprises of all sizes that demand. Simple, secure and scalable wireless solutions.

- **AP 1511**

The Alcatel-Lucent OmniAccess® Stellar AP1511 premium entry Wi-Fi 7 Access Point (AP) provides high-efficiency, high-performance 802.11be aggregate data rates up to 9.328 Gbps across the 2.4/5/6GHz band. Wi-Fi 7 technology supports a higher density of clients, delivers more capacity for bandwidth-hungry and latency-sensitive applications and provides a dependable, secure network for Internet of Things (IoT) devices. The OmniAccess Stellar WLAN portfolio brings unparalleled experience in connectivity, coverage and performance for the modern, IoT-connected enterprise.

The Wi-Fi 7 OmniAccess Stellar AP1511 is designed to accommodate the dense and high-capacity needs of next-generation mobility and IoT-enabled networks. The access point is powered with three radios serving Wi-Fi clients and an integrated Bluetooth/Zigbee radio, enabling the growing needs of enterprise IoT connectivity for powering location and building automation services. The OmniAccess Stellar AP1511 series supports a maximum aggregate data rate of 9.328 Gbps (688 Mbps in 2.4GHz, 2.882 Gbps in 5GHz, 5.76 Gbps in 6GHz). The access point provides 1 x 5GE Power over Ethernet (PoE) uplink.

The OmniAccess Stellar AP1511 supports 802.11be features, which include Multi-Link Operation (MLO), Orthogonal Frequency Division Multiplexing (OFDMA), Downlink Multi-User Multiple Input, Multiple Output (DL MU-MIMO), Uplink Multi-User Multiple Input, Multiple Output (UL MU-MIMO), 4096 Quadrature Amplitude Modulation mode (4096-QAM) and more, making tomorrow's diverse digital workspaces highly reliable and efficient.

The OmniAccess Stellar AP1511 features enhanced WLAN technology with RF Radio Dynamic Adjustment, a distributed control Wi-Fi architecture, secure network admission control with Unified Access and built-in application intelligence and analytics, making it ideal for enterprises of all sizes that demand a simple, secure and scalable wireless solution.

- **AP 1521**

The Alcatel-Lucent OmniAccess® Stellar AP1521 Wi-Fi 7 Access Point (AP) provides high-efficiency, high-performance 802.11be aggregate data rates up to 12.2 Gbps across the 6GHz, 5GHz and 2.4GHz band. Wi-Fi 7 technology supports a higher density of clients, delivers more capacity for bandwidth-hungry and latency-sensitive applications, and provides a dependable secure network for Internet of Things (IoT) devices while increasing their battery powered lifespan.

The OmniAccess Stellar WLAN portfolio brings unparalleled experience in connectivity, coverage, and performance for the modern, IoT-connected enterprise.

The Wi-Fi 7 premium OmniAccess Stellar AP1521 is designed to accommodate the very dense and high-capacity needs of next-generation mobility and IoT-enabled networks. The access point is powered with five built-in radios, three radios 2.4GHz/5GHz/6GHz serving high-density Wi-Fi clients, one full band radio dedicated to scanning for improved network security and Wi-Fi quality and an integrated Bluetooth/Zigbee radio, enabling the growing needs of enterprise IoT connectivity for powering location and building automation services. The OmniAccess Stellar AP1521 series supports a maximum aggregate data rate of 12.2 Gbps (688 Mbps in 2.4GHz, 5.76 Gbps in 5GHz, 5.76 Gbps in 6GHz). The access point provides one 10GE Power over Ethernet (PoE) uplink and one GE uplink/ downlink.

The OmniAccess Stellar AP1521 supports 802.11be features, which include Multi-Link Operation (MLO), Orthogonal Frequency Division Multiplexing (OFDMA), Downlink Multi-User Multiple Input, Multiple Output (DL MU-MIMO), Uplink Multi-User Multiple Input, Multiple Output (UL MU-MIMO), 4096 Quadrature Amplitude Modulation mode (4096-QAM) and more, making tomorrow's diverse digital workspaces highly reliable and efficient.

The OmniAccess Stellar AP1521 features enhanced WLAN technology with RF Radio Dynamic Adjustment, a distributed control Wi-Fi architecture, secure network admission control with Unified Access and built-in application intelligence and analytics, making it ideal for enterprises of all sizes that demand a simple, secure and scalable wireless solution.

- **AP 1541/42**

The OmniAccess® Stellar AP1540 series is Alcatel-Lucent Enterprise's ultra-high-performance Wi-Fi 7 access point, designed to meet the requirements of high-density enterprise environments where reliability, security and scalability are essential. This high-range series features a powerful five-radio architecture, ultra-high aggregate throughput and flexible dual 10-gigabit uplinks with AP 1541 AP 1542 an optional optical link to ensure predictable low-latency connectivity, seamless scalability and resilient operations, laying a future-proof foundation for high-density users, immersive applications and intelligent buildings.

The OmniAccess Stellar AP1540 series comprises two products:

AP1541, which has integrated omnidirectional antennas and is suitable for standard enterprise use, such as lecture halls, large classrooms, conference rooms, hotel common areas.

AP1542, which has 8 connectors for external antennas, perfectly suited to specific targeted coverage needs and specific spaces such as high ceilings in arenas, long corridors, or warehouses.

Both access points are powered with five built-in radios, three radios 6GHz 4x4:4, 5GHz 4x4:4 and 2.4GHz 4x4:4 serving high-density Wi-Fi clients, one full band radio dedicated to scanning for improved network security and Wi-Fi quality and an integrated Bluetooth/Zigbee radio enabling the growing needs of enterprise IoT connectivity for powering location and building automation services. The OmniAccess Stellar AP1540 series

supports a maximum aggregate data rate of 18.67 Gbps (1376.5 Mbps in 2.4GHz, 5.76 Gbps in 5GHz, 11.5 Gbps in 6GHz). Each access point provides one dual functionality port 10GE with Power over Ethernet (PoE) power or SFP/SFP+ uplink and one 10GE port uplink/downlink with PoE power.

The OmniAccess Stellar AP1540 series supports 802.11be features, which include Multi-Link Operation (MLO), Orthogonal Frequency Division Multiplexing (OFDMA), Downlink Multi-User Multiple Input, Multiple Output (DL MU-MIMO), Uplink Multi-User Multiple Input, Multiple Output (UL MU-MIMO), 4096 Quadrature Amplitude Modulation mode (4096-QAM) and more, making tomorrows diverse digital workspaces highly reliable and efficient.

The OmniAccess Stellar AP1540 series features enhanced WLAN technology with RF Radio Dynamic Adjustment, a distributed control Wi-Fi architecture, secure network admission control with Unified Access and built-in

application intelligence and analytics, making it ideal for enterprises of all sizes that demand a simple, secure, and scalable wireless solution.

- **AP 1561**

The Alcatel-Lucent OmniAccess® Stellar outdoor AP1561 Wi-Fi 7 Access Point (AP) provides high-efficiency, high-performance 802.11be aggregate data rates up to 9.328 Gbps across the 6GHz, 5 GHz and 2.4GHz bands for outdoor or rugged environments.

Wi-Fi 7 technology supports a higher density of clients, delivers more capacity for bandwidth-hungry and latency-sensitive applications and provides a dependable, secure network for Internet of Things (IoT) devices while increasing their battery-powered lifespan. The OmniAccess Stellar WLAN portfolio brings unparalleled experience in connectivity, coverage, and performance for the modern, IoT- connected enterprise, in all environments.

The outdoor Wi-Fi 7 AP1561 access points are ready for 6 GHz operations, supporting Automated Frequency Coordination (AFC). As in some RF domains, the use of the 6GHz band in outdoor locations is not permitted, the 6GHz radio is software configurable to operate in 6GHz or 5GHz.

The AP is powered by a 5GE Multigig Ethernet uplink port, allowing to connect existing LAN Access OmniSwitch layers without investing in upgrading the access layer. AP1561 features Wi-Fi 7 serving radios and is optimized to work with IEEE 802.3at, thereby protecting existing investments in the network access layer.

The OmniAccess Stellar AP1561 is IP67 rated for harsh environments, including exposure to high and low temperatures, direct sunlight, persistent moisture and precipitation and industrial-grade surge protection.

The OmniAccess Stellar AP1561 supports 802.11be features, which include Multi-Link Operation (MLO), Orthogonal Frequency Division Multiplexing (OFDMA), Downlink Multi-User Multiple Input, Multiple Output (DL MU-MIMO), Uplink Multi-User Multiple Input, Multiple Output (UL MU-MIMO), 4096 Quadrature Amplitude Modulation mode (4096-QAM) and more, making the diverse digital workspaces highly reliable and efficient.

The OmniAccess Stellar AP1561 features enhanced WLAN technology with RF Radio Dynamic Adjustment, a distributed control Wi-Fi architecture, secure network admission control with Unified Access and built-in application intelligence and analytics, making it ideal for enterprises of all sizes that demand a simple, secure, and scalable wireless solution.

- **AP 1571/72**

The Alcatel-Lucent OmniAccess® Stellar outdoor AP1570 Wi-Fi 7 Access Point (AP) family provides high-efficiency, high-performance 802.1 be aggregate data rates up to 9.328 Gbps across the 6GHz, 5 GHz and 2.4GHz bands for outdoor or rugged environments.

Wi-Fi 7 technology supports a higher density of clients, delivers more capacity for bandwidth-hungry and latency-sensitive applications, and provides a dependable, secure network for Internet of Things (IoT) devices while increasing their battery-powered lifespan. The OmniAccess Stellar WLAN portfolio brings unparalleled experience in connectivity, coverage, and performance for the modern, IoT-connected enterprise, in all environments.

The Wi-Fi 7 high-performance and rugged OmniAccess Stellar AP1570 family is designed to meet the demanding and high-capacity needs of next-generation mobility and IoT-enabled, rugged or outdoor networks. The AP is powered with five built-in radios: three 2.4GHz/5GHz/6GHz radios serving high-density Wi-Fi clients, one full band radio dedicated to scanning for improved network security and Wi-Fi quality, and an integrated Bluetooth/Zigbee radio enabling the growing needs of enterprise IoT connectivity to power location and building automation services. The OmniAccess Stellar AP1570 series supports a maximum aggregate data rate of 9.328 Gbps (688 Mbps in 2.4GHz, 2.882 Gbps in 5GHz, 5.76 Gbps in 6GHz).

The outdoor Wi-Fi 7 AP1570 access points are ready for 6 GHz operations, supporting Automated Frequency Coordination (AFC). As in some RF domains, the use of the 6GHz band in outdoor locations is not permitted, the 6GHz radio is software configurable, to operate in 6GHz or 5GHz.

The AP is powered by a 10GE Multigig Ethernet uplink combo port. This combo port supports either 10GE multi-gigabit with an RJ45 interface or an SFP/SFP+ optical interface, allowing the AP1570 series model to be connected to the network via optical fiber (active or passive) for long-distance backhaul. AP1570 offers an additional uplink/downlink Gigabit Ethernet interface for wired IoT device endpoints, accommodating various deployment options in demanding outdoor environments.

The OmniAccess Stellar AP1570 series is IP67 rated for harsh outdoor environments, including exposure to high and low temperatures, direct sunlight, persistent moisture and precipitation and industrial-grade surge protection.

The AP1570 series includes two products:

AP1571, which features integrated omnidirectional antennas and

AP1572, which has N-Type female connectors for external antennas with integrated 6KA lightning protection.

All 8 APs utilize the same AWOS 5.0 software source; the only hardware differences are processor type and design, which affect the specific binary image deployed to each model. Security functionality and feature sets remain consistent across both models, such as chip vendor-supplied Linux kernel, device drivers, and OmniAccess Stellar Cryptographic Engine underpin the platform support for each family.

The scope of this evaluation includes standalone access point mode and does not encompass clustered or controller-managed deployments. The TOE Hardware boundaries cover:

Alcatel-Lucent Enterprise OmniAccess Stellar Hardware Platforms

Table 2 – Alcatel-Lucent Enterprise OmniAccess Stellar Hardware Platforms

Model	Processor	Network Options

AP1501	Quad-core Cortex-A53 Arm	Radio: Supports 802.11be Tri Radio, Tri Band: 2.4GHz 2x2 + 5GHz 2x2 + 6GHz 2x2 • 6GHz: 2x2:2 up to 5.76 Gbps wireless data rate • 5GHz: 2x2:2 up to 2.882 Gbps wireless data rate • 2.4GHz: 2x2:2 up to 688 Mbps wireless data rate Ethernet: 1x multi-gigabit 100M/1G/2.5G/5G/10G IEEE 802.3bz compliant autosensing (RJ-45) uplink port Eth0 Other interfaces: 1x USB 2.0 Type C (5V, 500mA) 1x USB Type C console
AP1511	Quad-core Cortex-A53 Arm	Radio: Supports 802.11be Tri Radio, Tri Band: 2.4GHz 2x2 + 5GHz 2x2 + 6GHz 2x2 • 6GHz: 2x2:2 up to 5.76 Gbps wireless data rate • 5GHz: 2x2:2 up to 2.882 Gbps wireless data rate • 2.4GHz: 2x2:2 up to 688 Mbps wireless data rate Ethernet: 1x multi-gigabit 100M/1G/2.5G/5G IEEE 802.3bz compliant autosensing (RJ-45) uplink port Eth0 Other interfaces: 1x USB 2.0 Type C (5V, 500mA) 1x USB Type C console
AP1521	Quad-core Cortex-A53 Arm	Radio: Supports 802.11be Tri Radio, Tri Band: 2.4GHz 2x2 + 5GHz 4x4 + 6GHz 2x2 • 6GHz: 2x2:2 up to 5.76 Gbps wireless data rate • 5GHz: 4x4:4 up to 5.76 Gbps wireless data rate • 2.4GHz: 2x2:2 up to 688 Mbps wireless data rate

		Ethernet: 1x multi-gigabit 100M/1G/2.5G/5G/10G IEEE 802.3bz compliant autosensing (RJ-45) uplink port Eth0 Other interfaces: 1x USB 2.0 Type C (5V, 500mA) 1x USB Type C console
AP1541/42	Quad-core Cortex-A73 Arm	Radio: Supports 802.11be Tri Radio, Tri Band: 2.4GHz 2x2 + 5GHz 4x4 + 6GHz 2x2 • 6GHz: 4x4:4 up to 11.52 Gbps wireless data rate • 5GHz: 4x4:4 up to 5.76 Gbps wireless data rate • 2.4GHz: 4x4:4 up to 1.376 Mbps wireless data rate Ethernet: 1x multi-gigabit 100M/1G/2.5G/5G/10G IEEE 802.3bz compliant autosensing (RJ-45) uplink port Eth0 1x10GE RJ45 port - Eth1 802.3bt compliant (uplink/downlink port) Other interfaces: 1x USB 2.0 Type C (5V, 500mA) 1x USB Type C console
AP1561	Quad-core Cortex-A53 Arm	Radio: Supports 802.11be Tri Radio, Tri Band: 2.4GHz 2x2 + 5GHz 2x2 + 6GHz 2x2 • 6GHz: 2x2:2 up to 5.76 Gbps wireless data rate • 5GHz: 2x2:2 up to 5.76 Gbps wireless data rate • 2.4GHz: 2x2:2 up to 688 Mbps wireless data rate Ethernet: 1x multi-gigabit 100M/1G/2.5G/5G/10G IEEE 802.3bz compliant autosensing (RJ-45) uplink port Eth0

		Other interfaces: 1x USB 2.0 Type C (5V, 500mA) 1x USB Type C console
AP1571/72	Quad-core Cortex-A53 Arm	Radio: Supports 802.11be Tri Radio, Tri Band: 2.4GHz 2x2 + 5GHz 2x2 + 6GHz 2x2 • 6GHz: 2x2:2 up to 5.76 Gbps wireless data rate • 5GHz: 2x2:2 up to 2.882 Gbps wireless data rate • 2.4GHz: 2x2:2 up to 688 Mbps wireless data rate Ethernet: 1x 10-gigabit 100M/1G/2.5G/5G/10G IEEE 802.3bz compliant autosensing (RJ-45) uplink port Eth0 Power over Ethernet (PoE) 802.3bt compliant. IEEE 802.3az Energy-Efficient Ethernet (EEE). 1 x 1GE uplink/downlink port, PSE 802.3at. Other interfaces: 1x USB 2.0 Type C (5V, 500mA) 1x USB Type C console

Software: AWOS 5.0 collaborative Protection Profile for Network Devices Certified (This is the NDcPP build for AWOS 5.0).

Each model provides unified, secure enterprise WLAN access using a common AWOS 5.0 base. Hardware differences are abstracted from the TOE's functional architecture, as only the binary image (compiled for the respective CPU/hardware) differs while security features and management remain equivalent.

1.3 TOE DESCRIPTION

The TOE is the Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Points, which provide the connection point between wireless clients and the wired enterprise network. These devices operate on tri-band radio frequencies including 2.4 GHz, 5 GHz, and 6 GHz, implementing the latest IEEE 802.11be (Wi-Fi 7) standard for over-the-air communication with wireless clients. This communication encompasses device discovery, probe request responses, client authentication, association, encryption/decryption, and session management.

The TOE supports advanced Wi-Fi 7 features such as Multi-Link Operation (MLO), Orthogonal Frequency Division Multiple Access (OFDMA), Multi-User MIMO (both uplink and downlink), and 4096-QAM modulation, enabling enhanced throughput, reduced latency, and high client density support.

Similar to its predecessor product line, the TOE can operate in standalone mode; mesh or controller-based cluster modes are excluded from this evaluation. Authorized wireless clients receive secure access to the wired network via encrypted wireless communication, leveraging WPA3 and WPA2 security protocols with AES-CCMP encryption aligned with IEEE 802.11i security standards.

Client authentication is performed either through IEEE 802.1X authentication with an external RADIUS server employing Extensible Authentication Protocol (EAP) or via a pre-shared key (PSK) configured on both the TOE and client devices. Upon successful 802.11i 4-way handshake completion, clients associate securely with the TOE, ensuring confidentiality and integrity of wireless sessions.

The TOE provides an internal web-based user interface (Web UI) serving remote management functions over secure TLS/HTTPS connections. While the Web UI server authenticates itself to the client through TLS certificates, administrative user authentication occurs post-connection via password-based methods. A local serial console interface supports troubleshooting but is not intended for management tasks.

Centralized management of the OmniAccess Stellar APs is supported via the Alcatel-Lucent OmniVista 2500 on-premises Network Management System or OmniVista Cirrus cloud platform; however, such management solutions are outside this evaluation's scope.

1.3.1 PHYSICAL BOUNDARIES

The physical boundary of the TOE is defined as the Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Point running the Alcatel Wireless Operating System (AWOS) version 5.0. Various hardware models of the TOE are described in Section 1.2. These access points constitute the complete hardware and software components of the TOE.

The TOE executes on proprietary hardware that includes a processor, memory, storage, and network interfaces. It provides IEEE 802.11 wireless connectivity to client devices and wired interfaces to connect to the broader enterprise network. The TOE enforces security policies and provides protected management access through HTTPS.

The TOE relies on its operating environment to interact with external IT entities such as a RADIUS authentication server, a syslog server, and enterprise resources. Wireless clients connect to the TOE via IEEE 802.11-2016 using WPA3 Enterprise and WPA2 Enterprise with CCMP-256, while administrators connect through a secure HTTPS channel for management functions.

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

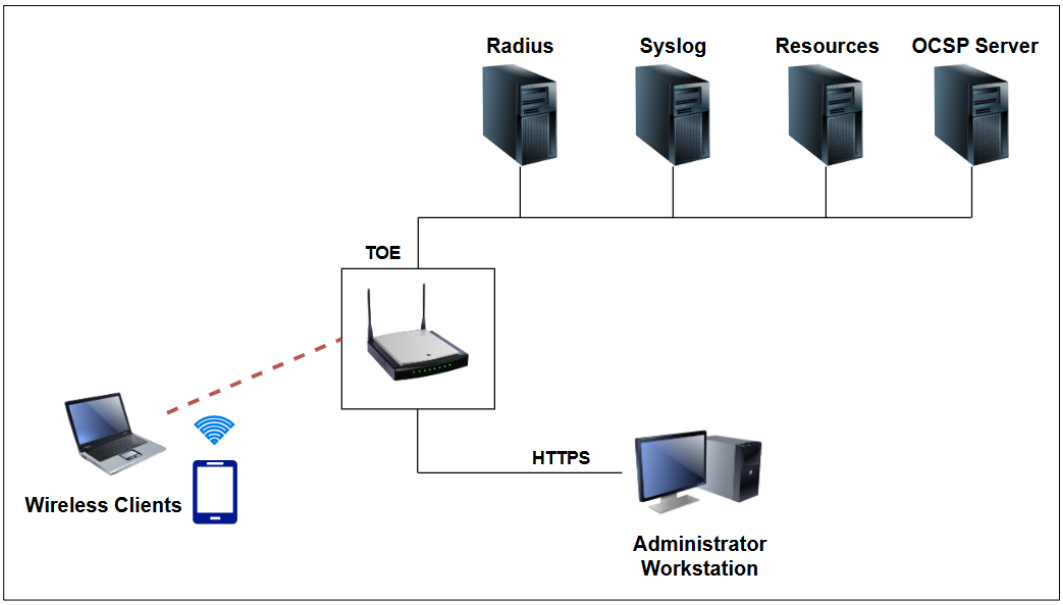


Figure 1 – TOE Boundaries

This figure depicts the Alcatel-Lucent OmniAccess Stellar Access Points as the secure bridge between wireless clients and the enterprise wired network. It illustrates wireless client authentication processes, including 802.1X authentication via an external RADIUS server, and secure wireless session establishment. The figure also highlights the secure management channel between the TOE and the administrator workstation using TLS/HTTPS, emphasizing protection of administrative operations.

1.3.2 SECURITY FUNCTIONS PROVIDED BY THE TOE

The TOE provides the security functions required by the Collaborative Protection Profile for Network Devices, hereafter referred to as NDcPP v3.0e or NDcPP and PP-Module for Wireless Local Area Network (WLAN) Access System Version 1.0 hereafter referred to as MOD_WLAN_AS_v1.0 or MOD_WLAN_AS.

1.3.2.1 SECURITY AUDIT

The TOE generates audit records for all security-relevant events. Each audit record includes details such as the event type, timestamp, event description, subject identity, and outcome of the event. These audit records can be viewed locally through the serial console or remotely via the Web UI over a secure HTTPS connection.

Audit data is stored in a fixed segment of the TOE's protected memory. When the allocated storage reaches capacity, the oldest records are securely overwritten to ensure continued logging. However, audit records stored in volatile memory may be lost if the device is rebooted. To mitigate potential audit data loss and support centralized monitoring, the TOE supports transmitting audit records to an external Syslog server. The operational environment is responsible for ensuring that the communication channel between the TOE and the Syslog server is secured, typically using TLS.

1.3.2.2 CRYPTOGRAPHIC SUPPORT

The TOE relies on cryptographic functionality to establish and protect secure communications, authenticate entities, and ensure the confidentiality and integrity of data in transit. Cryptographic support in the TOE is required for the establishment of secure channels over IEEE 802.11be (Wi-Fi 7), IEEE 802.1X, and TLS/HTTPS protocols, as well as for the protection of management and control plane communications.

For Wi-Fi cryptography, the TOE uses Qualcomm chip-level implementations to perform IEEE 802.11 encryption and integrity functions. All models use the Beryllium-based family of Qualcomm 802.11be Wi-Fi 7 chipsets. These chipsets implement the cryptographic functions used for WPA2 Enterprise and WPA3 Enterprise operations, including AES-CCM.

The other cryptographic services, including TLS/HTTPS, and key management, are provided by the OmniAccess Stellar Cryptographic Engine bundled within AWOS 5.0. OmniAccess Stellar Cryptographic Engine is used to support secure management communications, authentication, and logging.

1.3.2.3 IDENTIFICATION AND AUTHENTICATION

For wireless clients, the TOE supports authentication using either Pre-Shared Key (PSK) or IEEE 802.1X. In 802.1X mode, the TOE acts as the Authenticator, the client device acts as the Supplicant, and an external RADIUS server in the operational environment performs the authentication. Communication with the Authentication Server is protected using cryptographic protocols defined in IEEE 802.1X and WPA2/WPA3 standards.

1.3.2.4 SECURITY MANAGEMENT

The TOE provides secure remote management through its Web UI, accessible only to authorized administrators. The Security Administrator role is responsible for all security-relevant configuration, including management of user credentials, cryptographic keys, login banners, account lockout settings, inactivity timers, and TOE firmware updates. Only the Security Administrator can perform these management functions.

1.3.2.5 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. TOE performs Digital signature (RSA 2048bits + SHA-256) based firmware verification on manual update.
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.

1.3.2.6 TOE ACCESS

The TOE monitors remote user sessions for inactivity and terminates sessions upon reaching a configurable timeout. After termination, re-authentication is required to re-establish access.

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

Before administrative users authenticate, the TOE displays an administrator-specified advisory notice and consent warning message.

1.3.2.7 TRUSTED PATH/CHANNELS

The TOE provides secure channels to protect the integrity and confidentiality of information exchanged with external IT entities. Communication between the TOE and the administrator workstation is protected using TLS/HTTPS.

Wireless client communications are secured using WPA3 Enterprise and WPA2-Enterprise with AES-CCMP encryption as per IEEE 802.11 standards.

These trusted channels ensure that management and client data are protected against eavesdropping and tampering in the operational environment.

1.3.3 TOE DOCUMENTATION

The following documents are essential to understanding and controlling the TOE in the evaluated configuration:

- Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Points with AWOS 5.0 Common Criteria Configuration Guide v1.4

1.4 TOE ENVIRONMENT

The following environmental components are required to operate the TOE in the evaluated configuration:

Table 3 – Required Environmental Components

Components	Description
Remote Management Workstation	An administrator workstation equipped with a modern web browser is required to establish a TLS/HTTPS session with the TOE for secure remote management.
Authentication Server (RADIUS)	Provides IEEE 802.1X authentication services for wireless clients. The TOE acts as the Authenticator and relies on the RADIUS server to validate client credentials.
OCSP Server	The OCSP server supports online certificate status checking of certificates used by the TOE for TLS/HTTPS and IEEE 802.1X authentication.
Wireless Clients	Devices (e.g., laptops, mobile devices) act as supplicants in the IEEE 802.1X framework, requiring authentication before gaining access to the network.
Audit Server	External log server to which the TOE can transmit audit records over a trusted channel (e.g., TLS).

1.5 PRODUCT FUNCTIONALITY NOT INCLUDED IN THE SCOPE OF THE EVALUATION

The following product functionality is not included in the CC evaluation:

- Use of FTP/TFTP for file transfer.
- Use of SSH for management or diagnostics.
- Use of NTP for external time synchronization.
- Guest WLAN access via captive portal.
- AP-to-AP mesh communication.
- Centralized management via OmniVista 2500 or OmniVista Cirrus platforms.
- Bluetooth and Zigbee IoT functionality.

In general, any product functionality not mandated by NDcPP v3.0e or WLAN AS 1.0, or not explicitly described in Section 2.1 (Conformance Claims), is considered out of scope.

2. CONFORMANCE CLAIMS

This section identifies the TOE conformance claims, conformance rationale, and relevant Technical Decisions (TDs).

2.1 CC CONFORMANCE CLAIMS

The TOE is conformant to the following:

- Common Criteria for Information Technology Security Evaluations Part 1, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 5, April 2017 (Extended)
- Common Criteria for Information Technology Security Evaluations Part 3, Version 3.1, Revision 5, April 2017 (Conformant)

2.2 PROTECTION PROFILE CONFORMANCE

This ST claims exact conformance to the following:

- PP-Configuration for Network Device, Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS), and Wireless Local Area Network Access Systems, Version 2.0
  This PP-Configuration includes the following:
  - collaborative Protection Profile for Network Device, Version 3.0e (CPP_ND_V3.0E)
  - PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0 (MOD_WLAN_AS_V1.0)

2.3 CONFORMANCE RATIONALE

This ST provides exact conformance to the items listed in the previous section. The security problem definition, security objectives, and security requirements in this ST are all taken from the Protection Profile (PP) (CPP_ND_V3.0E) and PP-Module (MOD_WLAN_AS_V1.0), performing only the operations defined there.

2.3.1 TECHNICAL DECISIONS

All NIAP TDs issued to date and applicable to CPP_ND_V3.0E have been considered. Table 4 identifies all applicable TDs.

Table 4 – Relevant Technical Decisions

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable)
CPP_ND_V3.0E		
TD1052 NIT Technical Decision: Separation of Test Definitions for DTLSv1.2 and v1.3 (Renegotiation)	N	DTLS is not claimed.

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable)
TD1033 Sunset Dates for NDcPP Configurations	Y	
TD0990 - NIT Technical Decision: CTR_DRBG in FCS_RBG_EXT.1.2	Y	
TD0973 - IT Technical Decision: FCS_(D)TLSS_EXT.1.3 Test 2 DHE Ciphersuite Conditionality	Y	
TD0923 – NIT Technical Decision: Auditable event for FAU_STG_EXT.1 in FAU_GEN.1.2	Y	
TD0921 – NIT Technical Decision: Addition of FIPS PUB 186-5 and Correction of Assignment	Y	
TD0900 – NIT Technical Decision: Clarification to Local Administrator Access in FIA_UIA_EXT.1.3	Y	
TD0899 – NIT Technical Decision: Correction of Renegotiation Test for TLS 1.2	Y	
TD0886 – Clarification to FAU_STG_EXT.1 Test 6	Y	
TD0880 – NIT Decision: Removal of Duplicate Selection in FMT_SMF.1.1	Y	
TD0879 – NIT Decision: Correction of Chapter Headings in CPP_ND_V3.0E	Y	
TD0868 – NIT Technical Decision: Clarification of time frames in FCS_IPSEC_EXT.1.7 and FCS_IPSEC_EXT.1.8	N	IPsec is not claimed
TD0836 – NIT Technical Decision: Redundant Requirements in FPT_TST_EXT.1	Y	
MOD_WLAN_AS_V1.0		
TD0915 - Updates to FCS_CKM.1/WPA and FCS_CKM.2/GTK Tests for MOD_WLANAS	Y	
TD0903 – Correction to Auditable Event for FTA_TSE.1	Y	
TD0832 – Aligning MOD_WLAN_AS 1.0 with NDcPP 3.0E	Y	
TD0807 – Corrections for WLAN AS CC Conformance	Y	

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable)
TD0679 – Handling Standalone WLANAS TOEs with Single Interfaces	Y	
TD0651 – WLAN AS as Distributed and Non-distributed TOE	Y	

3. SECURITY PROBLEM DEFINITION

The security problem definition has been taken directly from the claimed PP and any relevant Modules specified in Section 2.2 and is reproduced here for the convenience of the reader. The security problem is described in terms of the threats that the TOE is expected to address, assumptions about the operational environment, and any Organizational Security Policies (OSPs) that the TOE is expected to enforce.

3.1 THREATS

The threats included in Table 5 are drawn directly from the PP and any Modules specified in Section 2.2.

Table 5 – Threats

ID	Threat
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 tunnelling 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.

ID	Threat
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. Threat agents may also be able to take advantage of weak administrative passwords to gain privileged access to the device.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.
T.NETWORK_DISCLOSURE	Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to conduct unauthorized activities. If malicious external devices are able to communicate with devices on the protected network, or if devices on the protected network can establish communications with those external devices (e.g., as a result of nonexistent or insufficient WLAN data encryption that exposes the WLAN data in transit to

ID	Threat
	rogue elements), then those internal devices may be susceptible to the unauthorized disclosure of information.
T.NETWORK_ACCESS	Devices located outside the protected network may seek to exercise services located on the protected network that are intended to be only accessed from inside the protected network or only accessed by entities using an authenticated path into the protected network.
T.TSF_FAILURE	Security mechanisms of the TOE generally build up from a primitive set of mechanisms (e.g., memory management, privileged modes of process execution) to more complex sets of mechanisms. Failure of the primitive mechanisms could lead to a compromise in more complex mechanisms, resulting in a compromise of the TOE Security Functionality (TSF).
T.DATA_INTEGRITY	Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to modify the data without authorization. If known malicious external devices are able to communicate with devices on the protected network or if devices on the protected network can establish communications with those external devices then the data contained within the communications may be susceptible to a loss of integrity.
T.REPLAY_ATTACK	If an unauthorized individual successfully gains access to the system, the adversary may have the opportunity to conduct a “replay” attack. This method of attack allows the individual to capture packets traversing throughout the wireless network and send the packets at a later time, possibly unknown by the intended receiver.

3.2 ASSUMPTIONS

The assumptions included in Table 6 are drawn directly from PP and any relevant Modules.

Table 6 – Assumptions

ID	Assumption
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 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. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise

ID	Assumption
	manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
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 by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
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 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. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
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,

ID	Assumption
	PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
A.CONNECTIONS	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE's security policies will be enforced on all applicable network traffic flowing among the attached networks

3.3 ORGANIZATIONAL SECURITY POLICIES

The OSPs included in Table 7 are drawn directly from the PP and any relevant Modules.

Table 7 – OSPs

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

4. SECURITY OBJECTIVES

The security objectives have been taken directly from the claimed PP and any relevant Modules and are reproduced here for the convenience of the reader.

4.1 SECURITY OBJECTIVES FOR THE TOE

The security objectives in the following table apply to the TOE.

Table 8 – Security Objectives

ID	Security Objectives
O.CRYPTOGRAPHIC_FUNCTIONS	The TOE will provide means to encrypt and decrypt data to maintain confidentiality and allow for detection of modification of TSF data that is transmitted outside 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.FAIL_SECURE	Upon a self-test failure, the TOE will shut down to ensure that data cannot be passed without adhering to the TOE's security policies.
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 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

Security objectives for the operational environment assist the TOE in correctly providing its security functionality. These objectives, which are found in the table below, track with the assumptions about the TOE operational environment.

Table 9 – Security Objectives for the Operational Environment

ID	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. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.
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.

ID	Objectives for the Operational Environment
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.
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. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.
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 the network traffic of monitored networks.

5. SECURITY REQUIREMENTS

This section identifies the Security Functional Requirements (SFRs) for the TOE. The SFRs included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revisions 5, April 2017, and all international interpretations.

Table 10 – SFRs

Requirement	Description
FAU_GEN.1	Audit Data Generation
FAU_GEN.1/WLAN	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_STG_EXT.1	Protected Audit Event Storage
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.1/WPA	Cryptographic Key Generation (Symmetric Keys for WPA2 Connections)
FCS_CKM.2	Cryptographic Key Establishment
FCS_CKM.2/GTK	Cryptographic Key Distribution (GTK)
FCS_CKM.2/PMK	Cryptographic Key Distribution (PMK)
FCS_CKM.4	Cryptographic Key Destruction
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 (Hash Algorithm)
FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)
FCS_HTTPS_EXT.1	HTTPS Protocol
FCS_RBG_EXT.1	Random Bit Generation
FCS_TLSC_EXT.1	TLS Client Protocol
FCS_TLSC_EXT.2	TLS Client Support for Mutual Authentication
FCS_TLSS_EXT.1	TLS Server Protocol
FCS_RADSEC_EXT.1	RadSec
FIA_AFL.1	Authentication Failure Handling
FIA_PMG_EXT.1	Password Management
FIA_UIA_EXT.1	User Identification and Authentication
FIA_UAU.6	Re-Authenticating
FIA_X509_EXT.1/Rev	X.509 Certificate Validation
FIA_X509_EXT.2	X.509 Certificate Authentication
FIA_X509_EXT.3	X.509 Certificate Requests
FIA_8021X_EXT.1	802.1X Port Access Entity (Authenticator) Authentication
FMT_MOF.1/Functions	Management of Security Functions Behaviour
FMT_MOF.1.1/Service	Management of Security Functions Behaviour

Requirement	Description
FMT_MOF.1/ManualUpdate	Management of Security Functions Behaviour
FMT_MTD.1/CoreData	Management of TSF Data
FMT_MTD.1/CryptoKeys	Management of TSF Data
FMT_SMF.1	Specification of Management Functions
FMT_SMF.1/AccessSystem	Specification of Management Functions (WLAN Access Systems)
FMT_SMR_EXT.1	No Administration from Client
FMT_SMR.2	Restrictions on Security Roles
FPT_APW_EXT.1	Protection of Administrator Passwords
FPT_SKP_EXT.1	Protection of TSF Data (for reading of all symmetric keys)
FPT_STM_EXT.1	Reliable Time Stamps
FPT_TST_EXT.1	TSF Testing
FPT_TUD_EXT.1	Trusted Update
FPT_FLS.1	Failure with Preservation of Secure State
FTA_SSL.3	TSF-initiated Termination
FTA_SSL.4	User-initiated Termination
FTA_TAB.1	Default TOE Access Banner
FTA_TSE.1	TOE Session Establishment
FTP_ITC.1	Inter-TSF Trusted Channel
FTP_ITC.1/Client	Inter-TSF Trusted Channel (WLAN Client Communications)
FTP_TRP.1/Admin	Trusted Path

5.1 CONVENTIONS

The CC allows the following types of operations to be performed on the functional requirements: assignments, selections, refinements, and iterations. The following font conventions are used within this document to identify operations defined by CC:

- Assignment: Indicated with *italicized* text;
- Refinement: Indicated with **bold** text;
- Selection: Indicated with <u>underlined</u> text;
- Iteration: Indicated by appending the iteration identifier after a slash, e.g., /SigGen.
- Where operations were completed in the PP and relevant EPs/Modules/Packages, the formatting used in the PP has been retained.
- Extended SFRs are identified by the addition of “EXT” after the requirement name.

5.2 SECURITY FUNCTIONAL REQUIREMENTS

This section includes the security functional requirements for this ST.

5.2.1 SECURITY AUDIT (FAU)

5.2.1.1 FAU_GEN.1 AUDIT DATA GENERATION (CPP_ND_V3.0E)

FAU_GEN.1.1 [TD0651] [TD0923]

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) Auditable events for the not specified level of audit; and

c) *All administrative actions comprising:*

- *Administrative login and logout (name of Administrator account shall be logged if individual 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).*
- *[no other actions]*

d) Specifically defined auditable events listed in Table 11.

FAU_GEN.1.2

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the cPP/ST, *information specified in column three of Table 11.*

Table 11 – Security Functional Requirements and Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG_EXT.1	Configuration of local audit settings.	Identity of account making changes to the audit configuration.
FCS_CKM.1	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.
FCS_COP.1/DataEncryption	None.	None.
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Reason for failure
FCS_RBG_EXT.1	None.	None.
FCS_TLSC_EXT.1	Failure to establish a TLS Session	Reason for failure

Requirement	Auditable Events	Additional Audit Record Contents
FCS_TLSC_EXT.2	None	None
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_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of identification and authentication mechanisms.	Origin of the attempt (e.g., IP address).
FIA_X509_EXT.1/Rev	• Unsuccessful attempt to validate a certificate • Any addition, replacement or removal of trust anchors in the TOE's trust store	• Reason for failure of certificate validation • Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store
FIA_X509_EXT.2	None	None
FIA_X509_EXT.3	None.	None.
FMT_MOF.1/Functions	None.	None.
FMT_MOF.1.1/Service	None	None
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	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_APW_EXT.1	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_TST_EXT.1	None.	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).
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None.

Requirement	Auditable Events	Additional Audit Record Contents
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.
FTP_ITC.1	• Initiation of the trusted channel. • Termination of the trusted channel. • Failure of the trusted channel functions.	• None • None • Reason for failure
FTP_TRP.1/Admin	• Initiation of the trusted path. • Termination of the trusted path. • Failure of the trusted path functions.	• None • None • Reason for failure

5.2.1.2 FAU_GEN.1/WLAN AUDIT DATA GENERATION (MOD_WLAN_AS_V1.0)

FAU_GEN.1.1/WLAN [TD0807] [TD0903]

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

a. Start-up and shutdown of the audit functions;
b. All auditable events for the [*not specified*] level of audit; and
c. [Auditable events listed in the Auditable Events table (Table 12)
d. Failure of wireless sensor communication]

Table 12 – Security Functional Requirements and Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FCS_CKM.1/WPA	None.	None
FCS_CKM.2/GTK	None.	None
FCS_CKM.2/PMK	None.	None
FCS_RADSEC_EXT.1	None.	None
FIA_8021X_EXT.1	• Attempts to access the 802.1X controlled port prior to successful completion of the authentication exchange. • Failed authentication attempt.	• Provided client identity (e.g. Media Access Control [Media Access Control (MAC)] address). • Provided client identity (e.g. MAC address).

Requirement	Auditable Events	Additional Audit Record Contents
FIA_UAU.6	Attempts to reauthenticate.	Origin of the attempt (e.g., IP address).
FMT_SMF.1/AccessSystem	None.	None
FMT_SMR_EXT.1	None.	None
FPT_FLS.1	Failure of the TSF.	Indication that the TSF has failed with the type of failure that occurred.
FPT_TST_EXT.1	• Execution of TSF self-test. • Detected integrity violations.	• None. • The TSF code file that caused the integrity violation.
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism.	Reason for denial, origin of establishment attempt.
FTP_ITC.1	• Failed attempts to establish a trusted channel (including IEEE 802.11). • Detection of modification of channel data.	• Identification of the initiator and target of channel.

5.2.1.3 FAU_GEN.2 USER IDENTITY ASSOCIATION (CPP_ND_V3.0E)

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.

5.2.1.4 FAU_STG_EXT.1 PROTECTED AUDIT EVENT STORAGE (CPP_ND_V3.0E)

FAU_STG_EXT.1.1 [TD0651] [TD0832]

The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1.

FAU_STG_EXT.1.2 [TD0651]

The TSF shall be able to store generated audit data on the TOE itself. In addition [

- *The TOE shall consist of a single standalone component that stores audit data locally*

].

FAU_STG_EXT.1.3 [TD0651] [TD0832]
The TSF shall maintain a [*log file*] of audit records in the event that an interruption of communication with the remote audit server occurs.

FAU_STG_EXT.1.4 [TD0832]
The TSF shall be able to store [*non-persistent*] audit records locally with a minimum storage size of [*1MB*].

FAU_STG_EXT.1.5 [TD0832]
The TSF shall [*overwrite previous audit records according to the following rule: [overwrite the oldest logs]*] when the local storage space for audit data is full.

FAU_STG_EXT.1.6 [TD0832]
The TSF shall provide the following mechanisms for administrative access to locally stored audit records [*none*].

5.2.1.5CRYPTOGRAPHIC SUPPORT (FCS)

5.2.1.6 FCS_CKM.1 CRYPTOGRAPHIC KEY GENERATION (CPP_ND_V3.0E)

FCS_CKM.1.1 [TD0921]
The TSF shall generate **asymmetric** cryptographic key 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)", Appendix B.3 or FIPS PUB 186-5, "Digital Signature Standard (DSS)", A.1;*
- *ECC schemes using 'NIST curves' [P-384] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4, or FIPS PUB 186-5, "Digital Signature Standard (DSS)", Appendix A.2, or ISO/IEC 14888-3, "IT Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms", Section 6.6.;*

  ].

] ~~and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: *list of standards*].~~

5.2.1.7 FCS_CKM.1/WPA CRYPTOGRAPHIC KEY GENERATION (SYMMETRIC KEYS FOR WPA2 CONNECTIONS) (MOD_WLAN_AS_V1.0)

FCS_CKM.1.1/WPA
The TSF shall generate symmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm [*PRF-384 and [no other algorithm]*] and specified cryptographic key sizes [*256 bits and [no other key sizes]*] **using a Random Bit Generator as specified in FCS_RBG_EXT.1** that meet the following: *[IEEE 802.11-2020 and [no other standards]*].

5.2.1.8 FCS_CKM.2 CRYPTOGRAPHIC KEY ESTABLISHMENT (CPP_ND_V3.0E)

FCS_CKM.2.1
The TSF shall **perform** cryptographic **key establishment** in accordance with a specified cryptographic key **establishment** method: [

- *Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision* 3, *"Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";*

].

] ~~that meets the following: [assignment: *list of standards*].~~

5.2.1.9 FCS_CKM.2/GTK CRYPTOGRAPHIC KEY DISTRIBUTION (GTK) (MOD_WLAN_AS_V1.0)

FCS_CKM.2.1/GTK
The TSF shall distribute **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 802.11-2020 for the packet format and timing considerations*] **and does not expose the cryptographic keys.**

5.2.1.10 FCS_CKM.2/PMK CRYPTOGRAPHIC KEY DISTRIBUTION (PMK) (MOD_WLAN_AS_V1.0)

FCS_CKM.2.1/PMK
The TSF shall **receive the 802.11 PMK** in accordance with a specified cryptographic key distribution method: [*from 802.1X Authorization Server*] that meets the following: [*IEEE 802.11-2020*] **and does not expose the cryptographic keys.**

5.2.1.11 FCS_CKM.4 CRYPTOGRAPHIC KEY DESTRUCTION (CPP_ND_V3.0E)

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

- *For plaintext keys in volatile storage, the destruction shall be executed by a [single overwrite consisting of [zeroes]];*
- *For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that [*
  - logically addresses the storage location of the key and performs a [single] overwrite consisting of [zeroes];

  ]

that meets the following: *No Standard.*

5.2.1.12 FCS_COP.1/DATAENCRYPTION CRYPTOGRAPHIC OPERATIONS (AES DATA ENCRYPTION/DECRYPTION) (CPP_ND_V3.0E)

FCS_COP.1.1/DataEncryption [TD0832]
The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm Advanced Encryption Standard (AES) used in **Cipher Block Chaining (CBC), CCM mode Protocol (CCMP),** and [no other] modes and cryptographic key sizes 256 bits and [no other key sizes] that meet the following: AES as specified in ISO

18033-3, CBC as specified in ISO 10116, CCMP as specified in NIST SP 800-38C and IEEE 802.11-2020, [no other standards].

Application note: The SFR has been modified as per the MOD_WLAN_AS_V1.0.

5.2.1.13 FCS_COP.1/SIGGEN CRYPTOGRAPHIC OPERATION (SIGNATURE GENERATION AND VERIFICATION) (CPP_ND_V3.0E)

FCS_COP.1.1/SigGen [TD0921]
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 [

- *For RSA: [modulus 2048 bits],*

]
that meets the following: [

- *For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 or FIPS PUB 186-5, "Digital Signature Standard (DSS)", Section 5.4 using PKCS #1 v2.2 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,*

].

5.2.1.14 FCS_COP.1/HASH CRYPTOGRAPHIC OPERATIONS (HASH ALGORITHM) (CPP_ND_V3.0E)

FCS_COP.1.1/Hash
The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm [*SHA-1, SHA-256, SHA-384*] ~~and cryptographic key sizes~~ [~~*assignment: cryptographic key sizes*~~] and **message digest sizes [*160, 256, 384*] bits** that meet the following: *ISO/IEC 10118-3:2004*.

5.2.1.15 FCS_COP.1/KEYEDHASH CRYPTOGRAPHIC OPERATION (KEYED HASH ALGORITHM) (CPP_ND_V3.0E)

FCS_COP.1.1/KeyedHash
The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm [*HMAC-SHA-1, HMAC-SHA-384*] and cryptographic key sizes *[key size 160 (in bits) used in HMAC]* **and message digest sizes [*160, 384*] *bits*** that meet the following: *ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"*.

5.2.1.16 FCS_HTTPS_EXT.1 HTTPS PROTOCOL (CPP_ND_V3.0E)

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 ~~protocol~~ using TLS.

5.2.1.17 FCS_RBG_EXT.1 RANDOM BIT GENERATION (CPP_ND_V3.0E)

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 [SHA-384]*].

FCS_RBG_EXT.1.2 [TD0990]
The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [[1] software-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"

].

5.2.1.18 FCS_TLSC_EXT.1 TLS CLIENT PROTOCOL (CPP_ND_V3.0E)

FCS_TLSC_EXT.1.1
The TSF shall implement [*TLS 1.2 (RFC 5246)*] supporting the following ciphersuites:
[

- *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 8422*
- *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289*

] and no other ciphersuites.

FCS_TLSC_EXT.1.2
The TSF shall verify that the presented identifier matches [*the reference identifier per RFC 6125 Section 6, IPv4 address in the CN or in the SAN*] *and no other attribute types*].

FCS_TLSC_EXT.1.3
The TSF shall not establish a trusted channel if the server certificate is invalid [

- *without any administrator override mechanism.*

].

FCS_TLSC_EXT.1.4
The TSF shall [*present the Supported Groups Extension with the following curves/groups: [secp384r1] and no other curves/groups*] in the Client Hello.

FCS_TLSC_EXT.1.5
The TSF shall [

- *present the signature_algorithms extension with support for the following algorithms:*
  [
  - *rsa_pkcs1with sha384(0x0501),*
  - *]* and no other algorithms;

].

FCS_TLSC_EXT.1.6

The TSF [*does not provide*] the ability to configure the list of supported ciphersuites as defined in FCS_TLSC_EXT.1.1.

FCS_TLSC_EXT.1.7
The TSF shall prohibit the use of the following extensions:

- Early data extension
- Post-handshake client authentication according to RFC 8446, Section 4.2.6.

FCS_TLSC_EXT.1.8
The TSF shall [*not use PSKs*].

FCS_TLSC_EXT.1.9
The TSF shall [*reject [TLS 1.2] renegotiation attempts*].

5.2.1.19 FCS_TLSC_EXT.2 TLS CLIENT SUPPORT FOR MUTUAL AUTHENTICATION (CPP_ND_V3.0E)

FCS_TLSC_EXT.2.1
The TSF shall support TLS communication with mutual authentication using X.509v3 certificates.

5.2.1.20 FCS_TLSS_EXT.1 TLS SERVER PROTOCOL (CPP_ND_V3.0E)

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

- *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 8422*

] and no other ciphersuites.

FCS_TLSS_EXT.1.2
The TSF shall authenticate itself using X.509 certificate(s) using [*RSA with key size [2048] bits and no other curves*].

FCS_TLSS_EXT.1.3 [TD0973]
The TSF shall perform key exchange using: [

- *EC Diffie-Hellman key agreement over NIST curves [secp384r1] and no other curves;*

].

FCS_TLSS_EXT.1.4
The TSF shall support [*no session resumption*].

FCS_TLSS_EXT.1.5
The TSF [*does not provide*] the ability to configure the list of supported ciphersuites as defined in FCS_TLSS_EXT.1.1.

FCS_TLSS_EXT.1.6
The TSF shall prohibit the use of the following extensions:

- Early data extension

FCS_TLSS_EXT.1.7
The TSF shall [*not use PSKs*].

FCS_TLSS_EXT.1.8
The TSF shall [*reject [TLS 1.2] renegotiation attempts*].

5.2.1.21 FCS_RADSEC_EXT.1 RADSEC (MOD_WLAN_AS_V1.0)

FCS_RADSEC_EXT.1.1
The TSF shall implement RADIUS over TLS as specified in RFC 6614 to communicate securely with a RADIUS server.

FCS_RADSEC_EXT.1.2
The TSF shall perform peer authentication using [*X.509v3 certificates*].

5.2.2 IDENTIFICATION AND AUTHENTICATION (FIA)

5.2.2.1 FIA_AFL.1 AUTHENTICATION FAILURE HANDLING (CPP_ND_V3.0E)

FIA_AFL.1.1
The TSF shall detect when an Administrator configurable positive integer within *[2 to 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]*.

5.2.2.2 FIA_PMG_EXT.1 PASSWORD MANAGEMENT (CPP_ND_V3.0E)

FIA_PMG_EXT.1.1
The TSF shall provide the following password management capabilities for administrative passwords:

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers and the following special characters: [*"!", "@", "#", "$", "%", "^", "&", "*", "(", ")", [no other characters]*];
b) Minimum password length shall be *configurable to between [4] and [15] characters.*

5.2.2.3 FIA_UIA_EXT.1 USER IDENTIFICATION AND AUTHENTICATION (CPP_ND_V3.0E)

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.

FIA_UIA_EXT.1.3 [TD0900]
The TSF shall provide the following remote authentication mechanisms [*Web GUI password*] and [*no other mechanism*]. The TSF shall provide the following local authentication mechanisms [*none*].

FIA_UIA_EXT.1.4
The TSF shall authenticate any administrative user's claimed identity according to each authentication mechanism specified in FIA_UIA_EXT.1.3.

5.2.2.4 FIA_UAU.6 RE-AUTHENTICATING (MOD_WLAN_AS_V1.0)

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

5.2.2.5 FIA_X509_EXT.1/REV X.509 CERTIFICATE VALIDATION (CPP_ND_V3.0E)

FIA_X509_EXT.1.1/Rev
The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation **supporting a minimum path length of three certificates**.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [*the Online Certificate Status Protocol (OCSP) as specified in RFC 6960*].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - *Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.*
  - *Server certificates presented for DTLS/TLS shall have the Server Authentication purpose(id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.*
  - *Client certificates presented for DTLS/TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsagefield.*
  - *OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose(id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.*

FIA_X509_EXT.1.2/Rev
The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

5.2.2.6 FIA_X509_EXT.2 X.509 CERTIFICATE AUTHENTICATION (CPP_ND_V3.0E)

FIA_X509_EXT.2.1
The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [*TLS*] and [*no additional uses*].

FIA_X509_EXT.2.2
When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [*accept the certificate*].

5.2.2.7 FIA_X509_EXT.3 X.509 CERTIFICATE REQUESTS (CPP_ND_V3.0E)

FIA_X509_EXT.3.1
The TSF shall generate a Certificate Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [*Common Name*].

FIA_X509_EXT.3.2
The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

5.2.2.8 FIA_8021X_EXT.1 802.1X PORT ACCESS ENTITY (AUTHENTICATOR) AUTHENTICATION (MOD_WLAN_AS_V1.0)

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.

5.2.3 SECURITY MANAGEMENT (FMT)

5.2.3.1 FMT_MOF.1/FUNCTIONS MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOUR (CPP_ND_V3.0E)

FMT_MOF.1.1/Functions
The TSF shall restrict the ability to [*determine the behaviour of*] the functions [*transmission of audit data to an external IT entity*] to *Security Administrators*.

5.2.3.2 FMT_MOF.1/MANUALUPDATE MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOR (CPP_ND_V3.0E)

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

5.2.3.3 FMT_MTD.1/COREDATA MANAGEMENT OF TSF DATA (CPP_ND_V3.0E)

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

5.2.3.4 FMT_MTD.1/CRYPTOKEYS MANAGEMENT OF TSF DATA (CPP_ND_V3.0E)

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

5.2.3.5 FMT_SMF.1 SPECIFICATION OF MANAGEMENT FUNCTIONS (CPP_ND_V3.0E)

FMT_SMF.1.1 [TD0880]
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 remote session inactivity time before session termination;*
- *Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates;*
- [
  - *Ability to manage the cryptographic keys;*
  - *Ability to set the time which is used for time-stamps;*
  - *Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;*
  - *Ability to generate Certificate Signing Request (CSR) and process CA certificate response;*

  ].

5.2.3.6 FMT_SMF.1/ACCESSSYSTEM SPECIFICATION OF MANAGEMENT FUNCTIONS (WLAN ACCESS SYSTEMS) (MOD_WLAN_AS_V1.0)

FMT_SMF.1.1/AccessSystem [TD0807]
The TSF shall be capable of performing the following management functions:
[

- *Configure the security policy for each wireless network, including:*
  - *Security type*
  - *Authentication protocol*
  - *Client credentials to be used for authentication*
  - *Service Set Identifier (SSID)*
  - *If the SSID is broadcasted*
  - *Frequency band set to [2.4 GHz, 5 GHz, 6 GHz]*
  - *Transmit power level*

]

5.2.3.7 FMT_SMR_EXT.1 NO ADMINISTRATION FROM CLIENT (MOD_WLAN_AS_V1.0)

FMT_SMR_EXT.1.1
The TSF shall ensure that the ability to administer remotely the TOE from a wireless client shall be disabled by default.

5.2.3.8 FMT_SMR.2 RESTRICTIONS ON SECURITY ROLES (CPP_ND_V3.0E)

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.

5.2.4 PROTECTION OF THE TSF (FPT)

5.2.4.1 FPT_APW_EXT.1 PROTECTION OF ADMINISTRATOR PASSWORDS (CPP_ND_V3.0E)

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.

5.2.4.2 FPT_SKP_EXT.1 PROTECTION OF TSF DATA (FOR READING OF ALL SYMMETRIC KEYS) (CPP_ND_V3.0E)

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

5.2.4.3 FPT_STM_EXT.1 RELIABLE TIME STAMPS (CPP_ND_V3.0E)

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*].

5.2.4.4 FPT_TST_EXT.1 TSF TESTING (CPP_ND_V3.0E)

FPT_TST_EXT.1.1 [TD0836, TD0832]
The TSF shall run a suite of the following self-tests:

- *During initial start-up (on power on) to verify the integrity of the TOE firmware and software;*
- *Prior to providing any cryptographic service and [at no other time] to verify correct operation of cryptographic implementation necessary to fulfil the TSF;*
- [*no other*] *self-tests* [*none*]

to demonstrate the correct operation of the TSF**: integrity verification of stored TSF executable code through the use of the TSF-provided cryptographic service specified in FCS_COP.1/SigGen**.

Application note: The SFR has been modified as per the MOD_WLAN_AS_V1.0.

FPT_TST_EXT.1.2 [TD0832]
The TSF shall respond to [*all failures*] by [*rebooting*].

5.2.4.5 FPT_TUD_EXT.1 TRUSTED UPDATE (CPP_ND_V3.0E)

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 [*digital signature*] prior to installing those updates.

5.2.4.6 FPT_FLS.1 FAILURE WITH PRESERVATION OF SECURE STATE (MOD_WLAN_AS_V1.0)

FPT_FLS.1.1
The TSF shall preserve a secure state when the following types of failures occur: [*failure of the self-tests*].

5.2.5 TOE ACCESS (FTA)

5.2.5.1 FTA_SSL.3 TSF-INITIATED TERMINATION (CPP_ND_V3.0E)

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

5.2.5.2 FTA_SSL.4 USER-INITIATED TERMINATION (CPP_ND_V3.0E)

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

5.2.5.3 FTA_TAB.1 DEFAULT TOE ACCESS BANNERS (CPP_ND_V3.0E)

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

5.2.5.4 FTA_TSE.1 TOE SESSION ESTABLISHMENT (MOD_WLAN_AS_V1.0)

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

5.2.6 TRUSTED PATH/CHANNELS (FTP)

5.2.6.1 FTP_ITC.1 INTER-TSF TRUSTED CHANNEL (CPP_ND_V3.0E)

FTP_ITC.1.1
The TSF shall be capable of using **IEEE 802.1X, [Remote Authentication Dial In User Service (RADIUS) over Transport Layer Security (TLS)]**, and [TLS] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: **802.1X authentication server**, audit server, [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 disclosure and detection of modification of the channel data.

Application note: The SFR has been modified as per the MOD_WLAN_AS_V1.0.

FTP_ITC.1.2 [TD0832]
The TSF shall permit [*the TSF*] to initiate communication via the trusted channel.

FTP_ITC.1.3
The TSF shall initiate communication via the trusted channel for [*transmission of audit data to the syslog server, requesting remote authentication*].

5.2.6.2 FTP_ITC.1/CLIENT INTER-TSF TRUSTED CHANNEL (WLAN CLIENT COMMUNICATIONS) (MOD_WLAN_AS_V1.0)

FTP_ITC.1.1/Client [TD0807]
The TSF shall **be capable of using WPA3-Enterprise, WPA2-Enterprise and [*no other mode*] as defined by IEEE 802.11-2020** to provide a **trusted** communication channel between itself and **WLAN clients** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data**.

FTP_ITC.1.2/Client
The TSF shall permit the authorized IT entities to initiate communication via the trusted channel.

FTP_ITC.1.3/Client

The TSF shall initiate communication via the trusted channel for [*no services*].

5.2.6.3 FTP_TRP.1/ADMIN TRUSTED PATH (CPP_ND_V3.0E)

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 **Administrators** ~~users~~ to initiate communication via the trusted path.

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

5.3 TOE SFR DEPENDENCIES RATIONALE FOR SFRS

The PP and any relevant Modules contain(s) all the requirements claimed in this ST. As such, the dependencies are not applicable since the PP has been approved.

Table 13 – SFR Rationale

Objective	Addressed by	Rationale
O.CRYPTOGRAPHIC_ FUNCTIONS	FCS_COP.1/DataEncryption (modified from Base-PP)	FCS_COP.1/DataEncryption supports the objective by requiring the TSF to implement AES in the modes needed to support its other functions.
	FCS_CKM.1/WPA	FCS_CKM.1/WPA supports the objective by requiring the TSF to generate symmetric keys used for WPA2.
	FCS_CKM.2/GTK	FCS_CKM.2/GTK supports the objective by requiring the TSF to distribute group temporal keys used for IEEE 802.11.
	FCS_CKM.2/PMK	FCS_CKM.2/PMK supports the objective by requiring the TSF to distribute pairwise master keys used for IEEE 802.11.
O.AUTHENTICATION	FIA_8021X_EXT.1	FIA_8021X_EXT.1 supports the objective by requiring the TSF to act as the authenticator for 802.1X authentication.
	FIA_UAU.6	FIA_UAU.6 supports the objective by requiring the TSF to re-authenticate a security administrator under certain circumstances.
	FTA_TSE.1	FTA_TSE.1 supports the objective by requiring the TSF to deny the

Objective	Addressed by	Rationale
		establishment of a wireless client session for reasons unrelated to the correctness of an authentication credential.
	FCS_RADSEC_EXT.1 (selection-based)	FCS_RADSEC_EXT.1 supports the objective by optionally requiring the TSF to implement RadSec in accordance with a defined specification.
O.FAIL_SECURE	FPT_TST_EXT.1 (modified from Base-PP)	FPT_TST_EXT.1 supports the objective by requiring the TSF to perform self-tests that may aid in the detection of a TSF failure.
	FPT_FLS.1	FPT_FLS.1 supports the objective by requiring the TSF to preserve a secure state in the event of a selftest failure.
O.SYSTEM_ MONITORING	FAU_GEN.1/WLAN	FAU_GEN.1/WLAN supports the objective by requiring the TSF to generate audit records for security-relevant WLAN behavior.
	FAU_STG_EXT.1 (modified from Base-PP)	FAU_STG_EXT.1 supports the objective by defining how distributed TOE components store their generated audit records.
O.TOE_ ADMINISTRATION	FMT_SMR_EXT.1	FMT_SMR_EXT.1 supports the objective by requiring the TSF to prevent any administrative actions that originate from the 'external' network.
	FMT_SMF.1/AccessSystem	FMT_SMF.1/AccessSystem supports the objective by defining management functionality that is specific to WLAN AS devices.

5.4 SECURITY ASSURANCE REQUIREMENTS

The TOE assurance requirements for this ST are taken directly from the PP and any relevant Modules, which is/are derived from Common Criteria Version 3.1, Revision 5. The assurance requirements are summarized in Table 14.

Table 14 – Security Assurance Requirements

Assurance Class	Assurance Components	Component Description
Security Target	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_SPD.1	Security problem definition

Assurance Class	Assurance Components	Component Description
	ASE_TSS.1	TOE summary specification
Development	ADV_FSP.1	Basic functional specification
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life Cycle Support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_IND.1	Independent testing – conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability survey

5.5 ASSURANCE MEASURES

The TOE satisfied the identified assurance requirements. This section identifies the Assurance Measures applied by ALE USA Inc. to satisfy the assurance requirements. The following table lists the details.

Table 15 – TOE Security Assurance Measures

SAR Component	How the SAR will be met
ASE_TSS.1.1C Refinement	Vendor will provide information on how the TOE meets each claimed SFR. This information has been documented in detail in the subsequent section.
ADV_FSP.1	The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes).
AGD_OPE.1	The Administrative Guide provides descriptions of the processes and procedures on how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.1	The Configuration Management (CM) documents describe how the consumer identifies the evaluated TOE. The CM documents identify the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked and how potential changes are incorporated.
ALC_CMS.1	The Configuration Management (CM) documents describe how the consumer identifies the evaluated TOE. The CM documents identify the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that

SAR Component	How the SAR will be met
	are used to control and track changes that are made to the TOE. This includes details on what changes are tracked and how potential changes are incorporated.
ATE_IND.1	Vendor will provide the TOE for testing.
AVA_VAN.1	Vendor will provide the TOE for testing. Vendor will provide a document identifying the list of software and hardware components.

6. TOE SUMMARY SPECIFICATION

6.1 TOE SUMMARY SPECIFICATION SFR DESCRIPTION

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

6.1.1 SECURITY AUDIT (FAU)

6.1.1.1 FAU_GEN.1 AUDIT DATA GENERATION (CPP_ND_V3.0E)

The local audit logging functionality is not configurable by the administrator.

The TOE generates audit records for all administrative actions related to certificates and key management. These include operations such as adding, removing, enabling, or disabling certificates.

Each audit record includes sufficient details such as the administrative user, source IP address, certificate type, and certificate name to uniquely identify the cryptographic key management operations as required by FAU_GEN.1.1c.

6.1.1.2 FAU_GEN.1/WLAN AUDIT DATA GENERATION (MOD_WLAN_AS_V1.0)

There are no TSS evaluation activities for this SFR.

6.1.1.3 FAU_GEN.2 USER IDENTITY ASSOCIATION (CPP_ND_V3.0E)

The TSS and Guidance Documentation requirements for FAU_GEN.2 are already covered by the TSS and Guidance Documentation requirements for FAU_GEN.1.

6.1.1.4 FAU_STG_EXT.1 PROTECTED AUDIT EVENT STORAGE (CPP_ND_V3.0E)

The TOE transmits audit records to an external audit server immediately after each auditable event occurs. The communication channel for this transmission is secured using TLS.

The TOE is a standalone TOE, consisting of a single component. All audit data generated by the TOE is stored locally within this component, and no distribution of audit storage across multiple components is implemented. Audit data transmission is performed in real-time only, immediately after the occurrence of each auditable event. The TOE does not support periodic or batched transmission of audit data.

The local audit logging functionality is not configurable by the administrator, the TOE writes audit records to a fixed memory segment of 1MB in size. The TOE provides no administrative access mechanisms to locally stored audit data; therefore, audit records cannot be modified or deleted by administrators or users. The TOE stores audit records locally in a dedicated memory buffer allocated for logging. These locally stored audit records are non-persistent, and the contents of the log buffer are lost when the TOE is rebooted.

The TOE does not provide any administrative mechanism for the authorized deletion of audit records. When the allocated local storage of 1MB reaches capacity, the TOE continues to accept new audit records without interruption. In this case, the TOE automatically overwrites the oldest audit records first. This overwrite rule ensures that the most recent audit data is always preserved while older records are discarded.

6.1.2 CRYPTOGRAPHIC SUPPORT (FCS)

6.1.2.1 FCS_CKM.1 CRYPTOGRAPHIC KEY GENERATION (CPP_ND_V3.0E)

The TSF supports the generation of RSA 2048-bit keys for TLS server authentication, TLS key establishment, and digital signature generation.

The TSF supports ECDSA P-384 key generation and verification for TLS ECDHE key establishment.

6.1.2.2 FCS_CKM.1/WPA CRYPTOGRAPHIC KEY GENERATION (SYMMETRIC KEYS FOR WPA2 CONNECTIONS) (MOD_WLAN_AS_V1.0)

The TOE establishes and maintains secure wireless connectivity with clients using WPA2 as defined in IEEE 802.11-2020. End-to-end encryption between the TOE and wireless clients is achieved through the 802.11i security framework.

When IEEE 802.1X authentication is used, the RADIUS server authenticates the wireless client and securely transmits the Pairwise Master Key (PMK) to the TOE. Both TOE and the wireless client then execute the 802.11i 4-way handshake to derive the Pairwise Transient Key (PTK). The key derivation function (PRF-384) uses HMAC-SHA1 with the following inputs: PMK, AP Nonce (ANonce), client Nonce (SNonce), AP MAC address, and client MAC address, producing a 384-bit PTK.

The PTK is divided into three session keys:

- Key Encryption Key (KEK) – used for encrypting the Group Temporal Key (GTK).
- Key Confirmation Key (KCK) – used to ensure the integrity of key exchange messages.
- Temporal Key (TK) – also referred to as the CCMP key, used for encrypting unicast traffic.

The TOE generates a Group Temporal Key (GTK) for securing multicast and broadcast communications. The GTK is distributed to clients in an EAPOL-Key frame using AES Key Wrap, in compliance with NIST SP 800-38F and IEEE 802.11-2020. The KEK is used to encrypt the GTK during transmission, and the client confirms receipt using the KCK.

AES-CCM provides confidentiality and integrity protection for data traffic through the combined use of AES encryption and Cipher Block Chaining Message Authentication Code (CBC-MAC). All WPA2-related keys (PMK, PTK, GTK, KEK, KCK, and TK) are securely zeroized by the TOE when they are no longer required.

The cryptographic implementation conforms to recognized standards through vendor and third-party validations. The wireless components are Wi-Fi Alliance (WFA) certified for WPA2/WPA3 Enterprise modes:

- AP1501: Certification ID: WFA138439

- AP1511: Certification ID: WFA132769
- AP1521: Certification ID: WFA132830
- AP1541: Certification ID: WFA138437
- AP1542: Certification ID: WFA138438
- AP1561: Certification ID: WFA138416
- AP1571: Certification ID: WFA138417
- AP1572: Certification ID: WFA138418

The cryptographic algorithms have also been validated under the NIST Cryptographic Algorithm Validation Program (CAVP) for AES-CCM with 256-bit keys:

- CAVP Validation No. A3239 and A7677

These certifications demonstrate compliance with the applicable cryptographic standards.

6.1.2.3 FCS_CKM.2 CRYPTOGRAPHIC KEY ESTABLISHMENT (CPP_ND_V3.0E)

The TSF performs ECDSA P-384 key establishment for TLS connections, corresponding to the ECDSA P-384 key generation and verification defined in FCS_CKM.1.1. The TOE's key establishment implementation meets the requirements of NIST Special Publication 800-56A Revision 3.

6.1.2.4 FCS_CKM.2/GTK CRYPTOGRAPHIC KEY DISTRIBUTION (GTK) (MOD_WLAN_AS_V1.0)

The TOE distributes the Group Temporal Key (GTK) to each wireless client by using the AES-KW 128-bit, Key Wrap algorithm. This process ensures that the GTK is securely encrypted with the client's unique Key Encryption Key (KEK), which is derived during the 4-way handshake, preventing key exposure. The entire process is performed within an EAPOL-Key frame and meets the NIST SP 800-38F and IEEE 802.11-2020 standards for packet format and timing.

When multiple clients connect to the TOE, the GTK is a single key used for all multicast and broadcast traffic. The TOE distributes this same GTK to each client individually. For each client, the GTK is wrapped separately using their unique KEK, ensuring that only that specific client can unwrap and access the GTK.

6.1.2.5 FCS_CKM.2/PMK CRYPTOGRAPHIC KEY DISTRIBUTION (PMK) (MOD_WLAN_AS_V1.0)

During IEEE 802.1X authentication, the TOE creates a virtual port for the wireless client and initially sets it to an "unauthorized" state, allowing only 802.1X traffic from the client. The TOE relays EAP messages between the wireless client (supplicant) and the RADIUS authentication server using RadSec. Upon successful authentication, the RADIUS server shares the Pairwise Master Key (PMK) with the wireless client and sends a copy to the TOE.

The PMK is transmitted to the TOE via the MS-MPPE-Recv-Key EAP attribute in the RADIUS Access-Accept packet. The TOE and wireless client then perform the IEEE 802.11i 4-way handshake to derive session keys and establish a secure communication channel. RadSec ensures that the PMK is protected during transfer from the RADIUS server to the TOE.

6.1.2.6 FCS_CKM.4 CRYPTOGRAPHIC KEY DESTRUCTION (CPP_ND_V3.0E)

Table 17 of the Security Target lists all relevant keys consistent with the functions carried out by the TOE, as well as their origin, storage location, situations in which keys are destroyed and key destruction method used. The TOE does not store any plaintext cryptographic keys in non-volatile memory.

The TOE protects private keys stored in non-volatile memory using an internal encryption mechanism. A small application generates a key-encrypting key (KEK) derived from the certificate type using a letter transformation algorithm. This KEK is used to encrypt or decrypt the private key before saving to or after loading from flash. The KEK itself is never stored in flash and is generated dynamically in RAM when required. Upon session termination, the KEK is zeroized and deallocated from memory.

There are no configurations that do not conform to the key destruction requirement.

6.1.2.7 FCS_COP.1/DATAENCRYPTION CRYPTOGRAPHIC OPERATIONS (AES DATA ENCRYPTION/DECRYPTION) (CPP_ND_V3.0E)

The TSF performs AES encryption and decryption using a 256-bit key in CBC mode for TLS communication as specified in ISO 10116, and in CCM (CCMP) mode for WLAN data protection as specified in NIST SP 800-38C and IEEE 802.11-2020; no other key sizes or modes are supported.

6.1.2.8 FCS_COP.1/SIGGEN CRYPTOGRAPHIC OPERATION (SIGNATURE GENERATION AND VERIFICATION) (CPP_ND_V3.0E)

The TSF supports cryptographic signature generation and verification using the RSA Digital Signature Algorithm with a 2048-bit modulus. This is implemented in accordance with FIPS PUB 186-4, Section 5.5, using PKCS #1 v2.1; FIPS PUB 186-5, Section 5.4, using RSASSA-PKCS1v1_5; and ISO/IEC 9796-2, supporting Digital Signature Scheme 2 and Digital Signature Scheme 3. No other algorithms or key sizes are supported.

6.1.2.9 FCS_COP.1/HASH CRYPTOGRAPHIC OPERATIONS (HASH ALGORITHM) (CPP_ND_V3.0E)

The TOE implements the following hash functions for its cryptographic mechanisms:

- Syslog over TLS & RadSec of TLSC: For secure logging (Syslog over TLS) and RADIUS authentication (RadSec), it uses SHA-1 and SHA-384 for key derivation and message authentication.
- Web Server of TLSS: The web server, which uses TLS to provide secure client connections, relies on SHA-1 for key exchange and message integrity.
- Signed Image Verification: To verify firmware or software image authenticity and integrity, the TOE performs signed image verification using SHA-256 to compute and compare image hashes.
- DRBG: The system's DRBG uses SHA-384 as its underlying hash function for generating cryptographic keys and nonces.

6.1.2.10 FCS_COP.1/KEYEDHASH CRYPTOGRAPHIC OPERATION (KEYED HASH ALGORITHM) (CPP_ND_V3.0E)

The TOE implements keyed-hash message authentication using the HMAC algorithm as specified in ISO/IEC 9797-2:2011, Section 7, "MAC Algorithm 2". The TOE supports the following keyed-hash functions: HMAC-SHA-1 and HMAC-SHA-384.

- For HMAC-SHA-1, the key length is 160 bits, the internal block size is 512 bits, and the output MAC length is 160 bits.
- For HMAC-SHA-384, the key length is 384 bits, the internal block size is 1024 bits, and the output MAC length is 384 bits.

6.1.2.11 FCS_HTTPS_EXT.1 HTTPS PROTOCOL (CPP_ND_V3.0E)

The TOE implements the HTTPS protocol in compliance with RFC 2818 to provide a secure communication channel for the administrative web interface. The implementation uses the TLS protocol, with the TOE acting as a TLS server that authenticates itself to clients using a server certificate.

6.1.2.12 FCS_RBG_EXT.1 RANDOM BIT GENERATION (CPP_ND_V3.0E)

The TOE performs all deterministic random bit generation services using a Hash_DRBG provided by the OmniAccess Stellar Cryptographic Engine. The DRBG is seeded by an entropy source from the operating system's entropy pool, which utilizes the Jitter Entropy (JENT) source. The entropy is gathered by the kernel's entropy subsystem and made available to user-space through the /dev/random interface. The entropy source is certified and validated with ESV #E330.

The JENT source collects entropy based on fine-grained variations in CPU execution time and system jitter, ensuring high-quality randomness for seeding the DRBG. The minimum entropy provided by this source is 256 bits of entropy per 256-bit block (i.e., provides full entropy), which is equal to the greatest security strength of the keys and hashes generated by the TOE.

6.1.2.13 FCS_TLSC_EXT.1 TLS CLIENT PROTOCOL (CPP_ND_V3.0E)

The TOE, acting as a TLS client, implements the TLS 1.2 protocol in compliance with RFC 5246. It is configured to support the following two ciphersuites:

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (RFC 8422)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (RFC 5289)

No other ciphersuites are supported.

The TOE establishes the server identity by verifying that the server certificate's presented identifier matches the administrator-configured reference identifier. The TOE supports reference identifiers in the form of FQDN and IPv4 addresses located in either the Common Name (CN) or the Subject Alternative Name (SAN) fields of the certificate. No other identifier types, such as wildcards or application-specific SANs, are supported.

When the TOE uses an IPv4 address as a reference identifier in the Common Name (CN) of a server certificate, it converts the text representation of the IP address into a binary representation in network byte order. The TOE

enforces the canonical IPv4 format as defined in RFC 3986 to ensure consistency in comparison with the administrator-configured reference identifier.

The TOE presents the Supported Groups Extension in the TLS Client Hello message with the group secp384r1. This behaviour is performed by default and is not configurable. Since only TLS 1.2 is supported and DHE ciphers are not claimed or used by the TOE, the TOE does not perform DHE key exchange, and no negotiation of DHE parameters is performed.

The TOE presents the signature_algorithms extension in the TLS Client Hello message. The supported algorithm is rsa_pkcs1_with_sha384 (0x0501). This behavior is the default and is not configurable; no other signature algorithms are supported or advertised by the TOE.

The TOE does not support the signature_algorithms_cert extension.

The TOE does not provide the ability to configure the list of supported ciphersuites. The ciphersuites supported by the TOE client are fixed and enforced by default.

The TOE does not use pre-shared keys (PSKs) in the evaluated configuration. No mechanism is provided for out-of-band provisioning of PSKs, ensuring that all keying material is derived through the supported TLS protocol only.

6.1.2.14 FCS_TLSC_EXT.2 TLS CLIENT SUPPORT FOR MUTUAL AUTHENTICATION (CPP_ND_V3.0E)

The TOE supports TLS communication in accordance with RFC 5280 using X.509v3 certificates. Mutual authentication using client-side X.509v3 certificates is supported only for RadSec (RADIUS over TLS) connections, where the TOE authenticates itself to the RadSec server during the TLS handshake.

6.1.2.15 FCS_TLSS_EXT.1 TLS SERVER PROTOCOL (CPP_ND_V3.0E)

The TOE implements the TLS 1.2 protocol in compliance with RFC 5246 when acting as a TLS server, rejecting all other TLS and SSL versions. The TOE supports the following ciphersuite for securing communications with TLS clients:

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (RFC 8422)

No additional ciphersuites are supported. The TSF supports TLSv1.2 for HTTPS/TLS connection. If the TSF receives a ClientHello message that requests TLSv1.1 or earlier, the TSF sends a fatal handshake_failure message and terminates the connection.

The TOE authenticates itself to TLS clients using an X.509 certificate with the RSA algorithm and a 2048-bit key size, consistent with the selected ciphersuites. Key exchange is performed using EC Diffie-Hellman (ECDHE) over the NIST curve secp384r1; no other curves or Diffie-Hellman groups are used.

The TOE does not support session resumption. The TLS server ciphersuites are pre-configured by default and cannot be modified by administrators or users. The TOE does not support TLS 1.3 in the evaluated configuration and does not use pre-shared keys (PSKs).

6.1.2.16 FCS_RADSEC_EXT.1 RADSEC (MOD_WLAN_AS_V1.0)

The TOE supports RADIUS over TLS (RADSEC) in accordance with RFC 6614 to establish secure communication between the TOE (acting as a RADIUS client) and a trusted RADIUS server. RADSEC ensures confidentiality and integrity of RADIUS messages by encapsulating them within a TLS-protected channel.

The TOE performs mutual authentication between the RADIUS client and the RADIUS server using X.509v3 certificates. During the TLS handshake, the TOE presents its client certificate to the RADIUS server and validates the server certificate against the configured trusted CA certificates in its trust store. Only when the certificate verification succeeds is the secure RADSEC channel established.

6.1.3 IDENTIFICATION AND AUTHENTICATION (FIA)

6.1.3.1 FIA_AFL.1 AUTHENTICATION FAILURE HANDLING (CPP_ND_V3.0E)

The TOE maintains a counter of consecutive failed authentication attempts for each administrator. Each failed login increments the counter, while a successful login resets it. The administrator can configure the maximum number of consecutive failed attempts to be between 2 and 5.

Once this threshold is reached, the TOE temporarily blocks the offending administrator from remote password-based access. Access is automatically restored after an administrator-defined lockout period expires, which also resets the counter.

Even when an account is blocked for remote access to the TOE, an administrator is always able to log in locally through the serial console, which is intended for debugging purposes only.

6.1.3.2 FIA_PMG_EXT.1 PASSWORD MANAGEMENT (CPP_ND_V3.0E)

The TOE enforces password management policies for administrator accounts. Administrative passwords may include any combination of uppercase and lowercase letters, numbers, and the following special characters: *"!", "@", "#", "$", "%", "^", "&", "*", "(", ")"*. The TOE also allows the Security Administrator to configure the minimum password length. The supported range for this parameter is from 4 to 15 characters.

6.1.3.3 FIA_UIA_EXT.1 USER IDENTIFICATION AND AUTHENTICATION (CPP_ND_V3.0E)

The TOE requires all administrative users to authenticate before performing any TSF-mediated actions. For remote access via the Web GUI password, the TOE verifies the provided username and password against stored credentials. A successful logon occurs when the TOE confirms that the username exists, and the password matches the stored (non-plaintext) password for that account. No local authentication mechanisms are supported. No protocol transactions other than standard HTTPS requests/responses are involved in this authentication process.

Prior to requiring administrator identification and authentication, the TOE only allows the display of the warning banner in accordance with FTA_TAB.1. No other actions are permitted before authentication. This applies to remote authentication only, as local authentication is not supported.

6.1.3.4 FIA_UAU.6 RE-AUTHENTICATING (MOD_WLAN_AS_V1.0)

There are no TSS evaluation activities for this component.

6.1.3.5 FIA_X509_EXT.1/REV X.509 CERTIFICATE VALIDATION (CPP_ND_V3.0E)

The TOE validates X.509v3 certificates for authenticating external TLS peers during the TLS handshake, in accordance with RFC 5280. The validation process adheres to the following rules:

- The TOE supports a minimum certification path length of three certificates.
- The TOE validates that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE; only such certificates are treated as CA certificates.
- The TOE validates the revocation status of all certificates in the certification path, from the leaf certificate up to the issuing intermediate CA, using the Online Certificate Status Protocol (OCSP) as specified in RFC 6960. If revocation cannot be verified due to OCSP unavailability, the certificate is not accepted, and the TLS connection is terminated.
- The TOE validates the extendedKeyUsage (EKU) field for the following purposes:
    - Server certificates: Server Authentication (id-kp 1)
    - Client certificates: Client Authentication (id-kp 2)
    - OCSP response certificates: OCSP Signing (id-kp 9)
    - Code Signing EKU: not applicable for this TOE and therefore considered trivially satisfied.

This validation ensures that revocation checking is consistently applied to all certificates in the path during TLS authentication. There is no difference in how leaf or intermediate CA certificates are treated.

6.1.3.6 FIA_X509_EXT.2 X.509 CERTIFICATE AUTHENTICATION (CPP_ND_V3.0E)

When establishing a TLS connection, the TSF uses the certificate presented by the TLS server to verify the server's identity. The TSF also presents its own certificate to the TLS server for client authentication. This certificate is provisioned and configured by the Security Administrator specifically for TLS authentication, with detailed guidance provided in the administrative documentation.

If the TOE is unable to connect to the OCSP responder to determine the validity of a certificate, the certificate will not be accepted, and the trusted channel will not be established. This behavior is consistent across all trusted channels implemented by the TOE, with no distinctions. The TOE does not permit the Security Administrator to override or configure a default action in this scenario.

6.1.3.7 FIA_X509_EXT.3 X.509 CERTIFICATE REQUESTS (CPP_ND_V3.0E)

The TOE is capable of generating a Certificate Request in accordance with RFC 2986. The request includes the TOE's private key and Common Name. No device-specific information is included in the request.

Upon receiving the Certificate Response from the Certificate Authority (CA), the TOE validates the chain of certificates from Root CA.

6.1.3.8 FIA_8021X_EXT.1 802.1X PORT ACCESS ENTITY (AUTHENTICATOR) AUTHENTICATION (MOD_WLAN_AS_V1.0)

The TOE implements IEEE 802.1X-2010 as the Authenticator to control access of wireless clients prior to granting network connectivity. The TSF strictly conforms to Clause 7.1 (Port-Based Network Access Control) and Clauses 8 and 11 (Extensible Authentication Protocol – EAP) of IEEE 802.1X-2010.

During operation, after the 802.11 association is complete, the TOE sends an EAPOL Identity Request to the Supplicant and relays the corresponding EAP Identity Response to the RADIUS Authentication Server using a RADIUS Access-Request message. The TOE supports EAP-TLS, enabling mutual authentication between the Supplicant and the RADIUS server using X.509 certificates.

Upon successful authentication, the RADIUS server returns an Access-Accept message containing the Pairwise Master Key (PMK), which is delivered to the TOE via the MS-MPPE-Recv-Key EAP attribute. The TOE protects this key transfer using RadSec (TLS) to ensure confidentiality and integrity of communication with the RADIUS server.

Conformance of the TOE's 802.1X and EAP/RADIUS implementation with RFCs 2865 and 3579 has been verified through development testing and Wi-Fi Alliance certification. The TOE is Wi-Fi Certified for 802.1X and EAP/RADIUS conformance under the WPA2/3 Enterprise certification program.

6.1.4 SECURITY MANAGEMENT (FMT)

6.1.4.1 FMT_MOF.1/FUNCTIONS MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOUR (CPP_ND_V3.0E)

The Security Administrator controls audit behavior through configurable Syslog features. They can set the Log Level (message severity), enable or disable remote log transmission to an external Syslog server, and configure secure transport via TLS, along with the destination Server IP and Port. The TOE ensures continuity of audit data by transmitting all records to the external Syslog server, mitigating the risk of data loss upon reboot.

For local audit storage, the TOE maintains a fixed 1 MB memory segment. When this limit is reached, the oldest records are automatically overwritten to accommodate new audit entries.

6.1.4.2 FMT_MOF.1/MANUALUPDATE MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOR (CPP_ND_V3.0E)

There are no specific requirements for non-distributed TOEs.

6.1.4.3 FMT_MTD.1/COREDATA MANAGEMENT OF TSF DATA (CPP_ND_V3.0E)

The TOE permits only the display of an access banner prior to successful identification and authentication. All interfaces or functionality that could allow manipulation of TSF data are inaccessible until the user successfully authenticates as a Security Administrator.

Management of the TOE's trust store, including the addition, removal, or modification of trusted X.509v3 certificates, is restricted to users with the Security Administrator role. Access to these functions requires successful authentication as a Security Administrator, ensuring that non-administrative users cannot manage the trust store.

6.1.4.4 FMT_MTD.1/CRYPTOKEYS MANAGEMENT OF TSF DATA (CPP_ND_V3.0E)

The ability to manage cryptographic keys is restricted to users with the Security Administrator role. This includes management of private keys used for TLS authentication and trusted CA certificates used for validating external certificates.

The operations a Security Administrator can perform on these keys include generating a private key to create a certificate request, importing a private key or trusted CA certificate, and deleting a private key or trusted CA certificate. Non-administrative users are not permitted to access, modify, or delete any cryptographic keys.

6.1.4.5 FMT_SMF.1 SPECIFICATION OF MANAGEMENT FUNCTIONS (CPP_ND_V3.0E)

The TOE provides the following security management functions, all of which are available through its remote administration interface (Web GUI):

Ability to administer the TOE remotely;

- Ability to configure the access banner;
- Ability to configure the remote session inactivity time before session termination;
- Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates;
- Ability to manage the cryptographic keys;
- Ability to set the time which is used for time-stamps;
- Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;
- Ability to generate Certificate Signing Request (CSR) and process CA certificate response;

The TOE does not provide a local administrative interface. All security management functions are accessible only through the remote administration interface.

6.1.4.6 FMT_SMF.1/ACCESSSYSTEM SPECIFICATION OF MANAGEMENT FUNCTIONS (WLAN ACCESS SYSTEMS) (MOD_WLAN_AS_V1.0)

The TOE supports multiple wireless security types, including WPA2-Enterprise and WPA3-Enterprise, as defined in IEEE 802.11. For client authentication, the TOE uses 802.1X authentication with EAP-TLS, ensuring mutual authentication and secure key establishment. The TOE supports operation across the 2.4 GHz, 5 GHz, and 6 GHz frequency bands, depending on the regional regulatory limits. If a wireless client attempts to connect to TOE with a non-supported security type, the client's authentication attempt will fail and the connection to the WLAN is rejected.

6.1.4.7 FMT_SMR_EXT.1 NO ADMINISTRATION FROM CLIENT (MOD_WLAN_AS_V1.0)

There are no TSS evaluation activities for this component.

6.1.4.8 FMT_SMR.2 RESTRICTIONS ON SECURITY ROLES (CPP_ND_V3.0E)

The TOE maintains the Security Administrator role, which is the only role authorized to perform security management functions, including remote administration of the TOE. The TSF associates user accounts with this role and enforces that only users assigned the Security Administrator role can access administrative functions.

The TOE also supports a read-only role, which has view-only permissions for the TOE configuration and operational state.

6.1.5 PROTECTION OF THE TSF (FPT)

6.1.5.1 FPT_APW_EXT.1 PROTECTION OF ADMINISTRATOR PASSWORDS (CPP_ND_V3.0E)

The TOE protects administrative passwords by storing them in a non-plaintext form. To obscure plaintext data, the TOE applies a two-step hashing process in which the password is first hashed using MD5 and then further processed with SHA3-256. The TOE does not provide any interface that allows passwords to be viewed, ensuring they cannot be disclosed in plaintext under any circumstances.

6.1.5.2 FPT_SKP_EXT.1 PROTECTION OF TSF DATA (FOR READING OF ALL SYMMETRIC KEYS) (CPP_ND_V3.0E)

The TOE stores pre-shared keys, symmetric keys and private keys in encrypted form using AES which prevents users, including administrators, from reading the keys. This protection ensures that the keys cannot be viewed through any interface.

6.1.5.3 FPT_STM_EXT.1 RELIABLE TIME STAMPS (CPP_ND_V3.0E)

The TOE provides reliable timestamps for its security functions, including the generation of audit event timestamps, calculation of user session inactivity, and validation of certificate validity periods.

The TOE maintains time using an internal system clock, which serves as a reliable source for these functions. A Security Administrator can set or adjust this clock through the Web UI.

6.1.5.4 FPT_TST_EXT.1 TSF TESTING (CPP_ND_V3.0E)

During initial start-up, the TOE automatically performs a suite of self-tests to ensure the integrity of its firmware and correct operation of cryptographic modules.

Upon boot, the TOE verifies the integrity of the stored image by validating its digital signature using an embedded Stellar AP public key. The TOE computes a SHA-256 hash of the image and compares it with the embedded hash. If

the two hashes match, the image is authenticated; if not, the TOE halts the boot process and displays an error message indicating signature verification failure.

After successful image verification, the TOE runs Known Answer Tests (KATs) for all implemented cryptographic algorithms to confirm their correct operation:

- AES KAT: Encrypts and decrypts known values and compares results with expected ciphertext and plaintext.
- SHA-1/256/384 KAT: Generates known hashes and verifies them against expected values.
- HMAC (HMAC-SHA-1/384) KAT: Produces message authentication codes and compares them with known results.
- ECDSA Algorithm Test: Uses known public/private key pairs to sign and verify data.
- RSA Algorithm Test: Performs encryption and decryption using known keys and verifies outputs.

If any cryptographic self-test fails, the TOE displays a failure message to the local console and automatically reboots. If the firmware integrity verification fails, the TOE will not boot and requires factory repair.

These self-tests collectively ensure that the TSF operates correctly before allowing any security functionality to execute.

6.1.5.5 FPT_TUD_EXT.1 TRUSTED UPDATE (CPP_ND_V3.0E)

The TOE allows the Security Administrator to view the currently active firmware version through the Web UI. The TOE does not support automatic updates, firmware images and corresponding SHA-256 hash values are securely obtained from the vendor's secure website and verified by the administrator prior to installation. The TOE does not support delayed activation.

Firmware updates are initiated manually via the Web UI over HTTPS. During the update process, the TOE verifies the digital signature of the uploaded image using its stored public key and SHA-256. The update proceeds only if the signature verification is successful, otherwise the installation is aborted, and an audit record is generated indicating the failure reason.

6.1.5.6 FPT_FLS.1 FAILURE WITH PRESERVATION OF SECURE STATE (MOD_WLAN_AS_V1.0)

When the TOE determines that the firmware/software image being installed is invalid, the TOE rejects the image and does not install or execute it. The TOE subsequently reboots as part of the normal firmware upgrade process. Following the reboot, the previously installed valid firmware remains in place, thereby preventing the TOE from operating with the invalid firmware image and preserving the TOE's secure state. A secure state, in this context, is defined as preventing the TOE from operating with a potentially compromised firmware or software image. By immediately rebooting, the TOE returns to a known-good state, which ensures the continued protection of any key material and user data by preventing insecure operations.

6.1.6 TOE ACCESS (FTA)

6.1.6.1 FTA_SSL.3 TSF-INITIATED TERMINATION (CPP_ND_V3.0E)

The TOE monitors remote interactive sessions for inactivity. If no user activity is detected for a Security Administrator-configurable period of time, the TOE automatically terminates the session. The inactivity period can be configured between 5 and 60 minutes, with a default value of 30 minutes.

6.1.6.2 FTA_SSL.4 USER-INITIATED TERMINATION (CPP_ND_V3.0E)

The TOE enforces automatic and manual termination of administrative sessions to maintain session security. Remote administrative sessions are monitored for inactivity, and the TOE automatically terminates an idle session after the administrator-configured timeout period, which can range from 5 to 60 minutes and default of 30 minutes. Once terminated, the user must re-authenticate to establish a new session. In addition, users can manually terminate their sessions at any time.

6.1.6.3 FTA_TAB.1 DEFAULT TOE ACCESS BANNERS (CPP_ND_V3.0E)

The TOE provides a single administrative method of access through remote access via the Web GUI (HTTPS). A local administrative interface is not claimed in this evaluation.

Before a user session is established through this administrative method, the TOE displays a Security Administrator-specified advisory notice and consent warning message. The content of this message is configurable by the administrator.

6.1.6.4 FTA_TSE.1 TOE SESSION ESTABLISHMENT (MOD_WLAN_AS_V1.0)

The TOE enforces control over wireless client session establishment based on defined attributes. Session establishment is denied based on the TOE interface, time, and day, as configured by the administrator. The TOE restricts session establishment to specific SSIDs or radio interfaces and enforces time-of-day and day-of-week policies that determine when client associations are permitted. No attributes other than interface, time, and day are used by the TOE in determining whether a wireless client session is established.

6.1.7 TRUSTED PATH/CHANNELS (FTP)

6.1.7.1 FTP_ITC.1 INTER-TSF TRUSTED CHANNEL (CPP_ND_V3.0E)

The TOE establishes trusted communication channels with 802.1X authentication server, using 802.1X with RADIUS over TLS, and a syslog server, using TLS. The TOE initiates communication via these trusted channels when requesting remote authentication from a RADIUS server and when transmitting audit data to an external syslog server. All secure communications are logically distinct from other communication channels.

The TOE establishes the following trusted communication mechanisms with authorized IT entities:

- RADIUS Server (802.1X Authentication) – The TOE acts as a client during the 802.1X authentication process and communicates with the RADIUS server using RADIUS over TLS. The server endpoint is assured through certificate validation as per RFC 5280.

- Syslog Server (Audit Transmission) – The TOE acts as a client and uses TLS to transmit audit data. The server endpoint is assured through the same certificate validation measures, including chain verification, validity period checks, and revocation status checks as defined in RFC 5280.

6.1.7.2 FTP_ITC.1/CLIENT INTER-TSF TRUSTED CHANNEL (WLAN CLIENT COMMUNICATIONS) (MOD_WLAN_AS_V1.0)

This component is adequately evaluated when performing the evaluation activities for FTP_ITC.1 in the Network Device, version 3.0e base-PP.

6.1.7.3 FTP_TRP.1/ADMIN TRUSTED PATH (CPP_ND_V3.0E)

The TOE supports a single method for remote administration, which is performed through the Web GUI using HTTPS protected by TLSv1.2. This mechanism provides a trusted communication path that is logically distinct from other communication paths.

6.2 CAVP ALGORITHM CERTIFICATE DETAILS

Each of these cryptographic algorithms have been validated as identified in the table below.

Table 16 – CAVP Algorithm Certificate References

SFR	Algorithm Description	Implementation Name	CAVP Alg.	CAVP Cert #
FCS_CKM.1	RSA schemes using cryptographic key sizes of [**2048 bit**] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;	OmniAccess Stellar Cryptographic Engine	RSA KeyGen (FIPS186-4) Capabilities: Key Generation Mode: B.3.6 Properties: Modulo: 2048	A7677
	ECC schemes using 'NIST curves' [**P-384**] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4;	OmniAccess Stellar Cryptographic Engine	ECDSA KeyGen (FIPS186-4) Curve: P-384 ECDSA KeyVer (FIPS186-4) Curve: P-384	A7677
FCS_CKM.2	Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using	OmniAccess Stellar Cryptographic Engine	KAS-ECC-SSC Sp800-56Ar3 Domain Parameter Generation Methods: P-384	A7677

SFR	Algorithm Description	Implementation Name	CAVP Alg.	CAVP Cert #
	Discrete Logarithm Cryptography"			
FCS_CKM.2/GTK	GTK distribution in accordance with a specified cryptographic key distribution method using AES Key Wrap as defined in NIST SP 800-38F, and IEEE 802.11-2020 for packet format and timing considerations.	OmniAccess Stellar Cryptographic Engine	AES-KW Direction: Decrypt, Encrypt Cipher: Cipher, Inverse Key Length: 128.	A7677
FCS_COP.1/ DataEncryption	AES used in [**CBC**] mode and cryptographic key sizes [**256 bits**] CBC as specified in ISO 10116	OmniAccess Stellar Cryptographic Engine and Qualcomm Beryllium AES-256 engine – Config E	AES-CBC Direction: Decrypt, Encrypt Key Length: 256	A7677
	AES used in [**CCMP**] mode and cryptographic key sizes [**256 bits**] CCMP as specified in NIST SP 800-38C and IEEE 802.11-2020	OmniAccess Stellar Cryptographic Engine and Qualcomm Beryllium AES-256 engine – Config E	AES-CCM Key Length: 256	A7677 And A3239
FCS_COP.1/ SigGen	For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, 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	OmniAccess Stellar Cryptographic Engine	RSA SigGen (FIPS186-4) Capabilities: Signature Type: PKCS 1.5 Properties: Modulo: 2048 RSA SigVer (FIPS186-4) Capabilities: Signature Type: PKCS 1.5 Properties: Modulo: 2048	A7677
FCS_COP.1/ Hash	[**SHA-1, SHA-256, SHA-384**] and message digest sizes [**160, 256, 384**] bits, in accordance with *ISO/IEC 10118-3:2004*.	OmniAccess Stellar Cryptographic Engine	SHA-1 SHA2-256 SHA2-384 Message Length: 0-65536 Increment 8	A7677

SFR	Algorithm Description	Implementation Name	CAVP Alg.	CAVP Cert #
FCS_COP.1/ KeyedHash	**HMAC-SHA-1, HMAC-SHA-384** and cryptographic key sizes [**key size 160, 384 (in bits) used in HMAC**] and message digest sizes [**160, 384**] bits in accordance with *ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"*.	OmniAccess Stellar Cryptographic Engine	HMAC-SHA-1 MAC: 32-160 Increment 8 HMAC-SHA2-384 MAC: 32-384 Increment 8	A7677
FCS_RBG_EXT.1	**Hash_DRBG [SHA-384]** in accordance with ISO/IEC 18031:2011	OmniAccess Stellar Cryptographic Engine	Hash DRBG Prediction Resistance: Yes Supports Reseed Capabilities: Mode: SHA2-384	A7677

6.3 CRYPTOGRAPHIC KEY DESTRUCTION

The table below describes the key zeroization provided by the TOE and as referenced in FCS_CKM.4.

Table 17 – Zeroization of Keys

Keys/CSPs	Purpose	Storage Location	Method of Zeroization
Web Server Certificate (public and private keys)	Web Server (TOE acting as server) and TOE authentication	Flash (private key AES-256 encrypted)	As the private key is stored encrypted, no destruction is needed for the persistent copy.
RadSec Certificate (public and private keys)	RadSec client (acting as client) and authentication	Flash (private key AES-256 encrypted)	As the private key is stored encrypted, no destruction is needed for the persistent copy.
Private Key Encryption KEK (Key-Encrypting-Key)	Encrypt private key (before save to Flash) and decrypt (after load from Flash)	RAM (Dynamically generated upon use)	Zeroization and deallocation when session is terminated.
Session keys (encryption keys and keys)	Integrity and confidentiality during session	RAM	Zeroization and deallocation when session is terminated.
Administrator Passwords (Stored Hash)	TOE authentication (Administrator login)	Flash	Not a key; stored as a SHA3-256 hash. Overwritten/deleted upon change or factory reset.

7. ACRONYM TABLE

Acronyms should be included as an Appendix in each document.

Table 18 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CC	Common Criteria
CRL	Certificate Revocation List
DTLS	Datagram Transport Layer Security
EP	Extended Package
GUI	Graphical User Interface
IP	Internet Protocol
NDcPP	Network Device Collaborative Protection Profile
NIAP	Nation Information Assurance Partnership
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
PP	Protection Profile
RSA	Rivest, Shamir & Adleman
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TLS	Transport Layer Security
TSS	TOE Summary Specification