National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme



TM

Validation Report

for the

Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Points with AWOS 5.0, Version 1.0

Report Number: CCEVS-VR- VID11710-2026

Dated: 28/09/2026

Version: 0.3

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort George G. Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Swapna Katikaneni

Marybeth Panock

Dale Schroeder

Common Criteria Testing Laboratory

Saniya Shaikh

Yogesh Pawar

Intertek Acumen Security

Table of Contents

1 Executive Summary 4

2 Identification 5

3 Architectural Information 6

3.1 TOE Description 13
3.1.1 Physical Boundaries 14

4 Security Policy 16

5 Assumptions, Threats & Clarification of Scope 18

5.1 Assumptions 18
5.2 Threats 19
5.3 Clarification of Scope 22

6 Documentation 23

7 TOE Evaluated Configuration 24

7.1 Evaluated Configuration 24
7.2 Excluded Functionality 24

8 IT Product Testing 25

8.1 Developer Testing 25
8.2 Evaluation Team Independent Testing 25

9 Results of the Evaluation 26

9.1 Evaluation of Security Target 26
9.2 Evaluation of Development Documentation 26
9.3 Evaluation of Guidance Documents 27
9.4 Evaluation of Life Cycle Support Activities 27
9.5 Evaluation of Test Documentation and the Test Activity 27
9.6 Vulnerability Assessment Activity 27
9.7 Summary of Evaluation Results 29

10 Validator Comments & Recommendations 30

11 Annexes 31

12 Security Target 32

13 Glossary 33

14 Bibliography 34

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Points with AWOS 5.0 Series Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in August 2026. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the collaborative Protection Profile for Network Device, Version 3.0e (CPP_ND_V3.0E) and PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0 (MOD_WLAN_AS_V1.0).

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the Protection Profile (PP). This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the ST. Based on these findings, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations.

Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against PPs containing Assurance Activities, which are interpretations of Common Evaluation Methodology (CEM) work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile(s) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Points with AWOS 5.0
Protection Profile	Collaborative Protection Profile for Network Device, Version 3.0e (CPP_ND_V3.0E) and PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0 (MOD_WLAN_AS_V1.0)
Security Target	Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Points with AWOS 5.0, Security Target, v1.9, 23 September 2026
Evaluation Technical Report	Evaluation Technical Report for Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Points with AWOS 5.0, v0.4., 23 September 2026
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	ALE USA Inc.
Developer	ALE USA Inc.
Common Criteria Testing Lab (CCTL)	Intertek Acumen Security
CCEVS Validators	Swapna Katikaneni Marybeth Panock Dale Schroeder

3 Architectural Information

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 802.11be 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 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:

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.

3.1 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.

3.1.1 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.

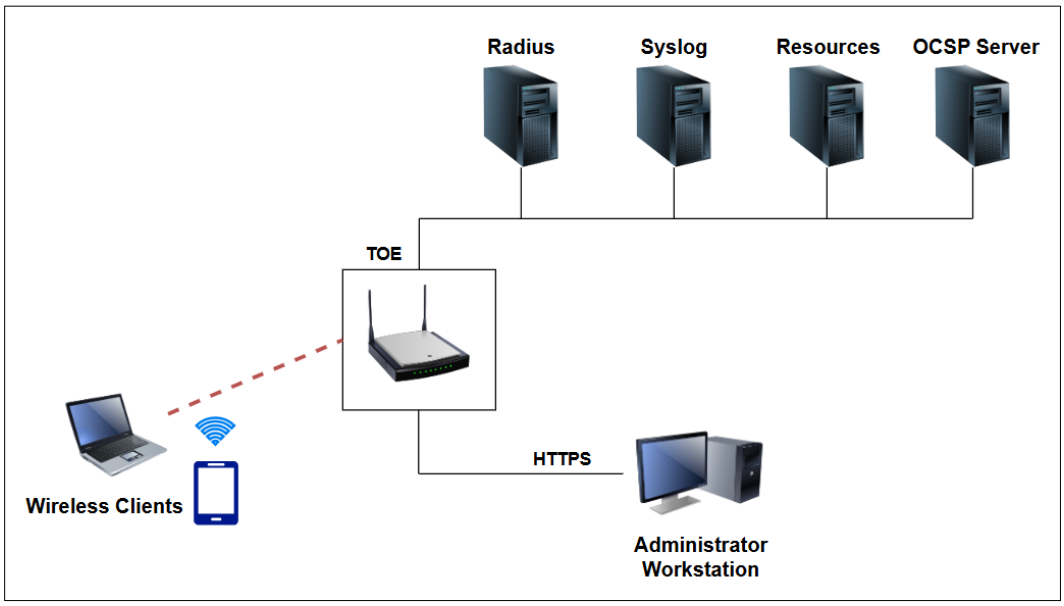


Figure 1 – TOE Boundaries

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.

4 Security Policy

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.

4.1 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.

4.2 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.

4.3 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.

4.4 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.

4.5 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.

4.6 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.

4.7 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 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.

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 1 – 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 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

ID	Assumption
	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, 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

5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

Table 2 – 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

ID	Threat
	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.
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

ID	Threat
	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 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

ID	Threat
	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.

5.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the collaborative Protection Profile for Network Device, Version 3.0e (CPP_ND_V3.0E) and PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0 (MOD_WLAN_AS_V1.0)
- Consistent with the expectations of the PP, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Points with AWOS 5.0, Security Target, v1.9, 23 September 2026
- Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Points with AWOS 5.0 Common Criteria Configuration Guide, v1.4, 22 September 2026

The documentation listed above is the only documentation that should be trusted to install, administer, or use the TOE in its evaluated configuration. Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the device as evaluated. To use the product in the evaluated configuration, the product must be configured as specified in the guidance documentation listed above.

Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

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).

7.2 Excluded Functionality

As noted in Security Target Section 1.3 TOE Description, 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.

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.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in ETR for Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Points with AWOS 5.0, which is not publicly available. The AAR provides an overview of testing and the prescribed assurance activities.

8.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the vendor-provided guidance documentation and ran the tests specified in the collaborative Protection Profile for Network Device, Version 3.0e (CPP_ND_V3.0E) and PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0 (MOD_WLAN_AS_V1.0). The Independent Testing activity is documented in the AAR Section 4 ‘Test Bed Descriptions’. Subsection 4.1 describes the Test Bed, Subsection 4.2 identifies the ‘Configuration Information’ identifying the software and test tools used, and Subsection 4.3 specifies the ‘Test Time and Location’. The AAR is publicly available and test bed descriptions are not duplicated here.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the ETR. The reader of this document can assume that all activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 Rev.5 and CEM version 3.1 Rev.5. The evaluation determined the TOE Name to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in the claimed PP.

9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Points with AWOS 5.0 that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the collaborative Protection Profile for Network Device, Version 3.0e (CPP_ND_V3.0E) and PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0 (MOD_WLAN_AS_V1.0).

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of Development Documentation

The evaluation team applied each EAL 1 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Network Device, Version 3.0e (CPP_ND_V3.0E) and PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0 (MOD_WLAN_AS_V1.0) related to the examination of the information contained in the TOE Summary Specification.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each EAL 1 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Network Device, Version 3.0e (CPP_ND_V3.0E) and PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0 (MOD_WLAN_AS_V1.0) related to the examination of the information contained in the operational guidance documents.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each EAL 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the collaborative Protection Profile for Network Device, Version 3.0e (CPP_ND_V3.0E) and PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0 (MOD_WLAN_AS_V1.0) and recorded the results in a Test Report, summarized in the ETR and AAR.

The validator reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the collaborative Protection Profile for Network Device, Version 3.0e (CPP_ND_V3.0E) and PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0 (MOD_WLAN_AS_V1.0), and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any open vulnerabilities applicable to the TOE. The vulnerability search was performed on 09/22/2026.

In compliance with AVA_VAN.1, the evaluator examined sources of publicly available information to identify potential vulnerabilities in the TOE. The sources of examined are as follows:

- https://nvd.nist.gov/view/vuln.search
- http://cve.mitre.org/cve
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog-print

The evaluator examined public domain vulnerability searches by performing a keyword search. The terms used for this search were based on the vendor name, product name, and key platform features leveraged by the product. As a result, the evaluator performed a search using the following keywords:

- Alcatel-Lucent Enterprise
- OmniAccess Stellar Wireless Access Points
- AWOS 5.0
- Quad-core Cortex-A53 Arm
- Quad-core Cortex-A73 Arm
- OmniAccess Stellar AP1511
- OmniAccess Stellar AP1521
- OmniAccess Stellar AP1501
- OmniAccess Stellar AP1541
- OmniAccess Stellar AP1542
- OmniAccess Stellar AP1561
- OmniAccess Stellar AP1571
- OmniAccess Stellar AP1572
- openssl 3.5.2
- jitterentropy-library 3.6.3
- busybox 1.35.0 (cpe:2.3:a:busybox:busybox:1.35.0:*:*:*:*:*:*:*)
- dropbear v2020.80 (cpe:2.3:a:dropbear_ssh_project:dropbear_ssh:2020.80:*:*:*:*:*:*:*)
- curl 8.17 (cpe:2.3:a:haxx:curl:8.17.0:*:*:*:*:*:*:*)
- hostapd 2.10
- wpa_supplicant 2.10 (cpe:2.3:a:w1.fi:wpa_supplicant:2.10:*:*:*:*:*:*:*)
- lighttpd 1.4.55
- Mosquito v1.4.14
- iptables-tools 1.8.3
- OpenVPN 2.4.11 (cpe:2.3:a:openvpn:openvpn:2.4.11:*:*:*:community:*:*:*)
- radsecproxy 1.9.2
- syslog-ng 3.38.1
- wireguard-linux 1.0.20200611
- wireguard-tools 1.0.20191226

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the collaborative Protection Profile for Network Device, Version 3.0e (CPP_ND_V3.0E) and PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0 (MOD_WLAN_AS_V1.0), and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the collaborative Protection Profile for Network Device, Version 3.0e (CPP_ND_V3.0E) and PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0 (MOD_WLAN_AS_V1.0), and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Points with AWOS 5.0 Common Criteria Configuration Guide, v1.4 document. No versions of the TOE and software, either earlier or later were evaluated.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Section 7.2 of this document, and Section 1.5 "Product Functionality Not Included in the Scope of the Evaluation" of the ST, provide the details of features that are part of the purchased product but were not included in the evaluation. These include mesh or controller-based cluster modes and the following functionality:

- 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.

All other functionality provided, including software, firmware, or hardware that was not part of the evaluated configuration needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

All other concerns and issues are adequately addressed in other parts of this document.

11 Annexes

Not applicable.

12 Security Target

Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Points with AWOS 5.0, Security Target v1.9

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
5. Collaborative Protection Profile for Network Device, Version 3.0e (CPP_ND_V3.0E).
6. PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0 (MOD_WLAN_AS_V1.0).
7. Assurance Activity Report for Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Points with AWOS 5.0, v0.8, 22 September 2026
8. Evaluation Technical Report for Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Points with AWOS 5.0, v0.4., 23 September 2026
9. Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Points with AWOS 5.0 Common Criteria Conformance Guide, v1.4., 22 September 2026
10. Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Points with AWOS 5.0 Security Target, v1.9, 23 September 2026
11. Vulnerability Assessment for Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Points with AWOS 5.0, v0.8, 23 September 2026
12. Test Plan for Alcatel-Lucent Enterprise OmniAccess Stellar Wireless Access Points with AWOS 5.0, v0.6, 24 August 2026