National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report

Alcatel-Lucent Enterprise OmniSwitch series 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.6.R11

Report Number: CCEVS-VR-11069-2021

Dated: April 30, 2021

Version: 1.0

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell

John W Butterworth

Jean E Petty

MITRE Corporation

Farid Almed

John Hopkins University

Common Criteria Testing Laboratory

Trang Huynh

King Ables

Randy Baker

Elliot Keen

atsec information security corporation, Austin, TX

Table of Contents

1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Alcatel-Lucent Enterprise OmniSwitch series 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.6.R11 provided by ALE USA Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Common Criteria Testing Laboratory (CCTL) atsec information security corporation in Austin, TX, United States of America, and was completed in April, 2021. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CCTL, atsec information security corporation. The evaluation determined that the product is both Common Criteria (CC) Part 2 Extended and Part 3 Conformant, and meets the assurance requirements given in:

- collaborative Protection Profile for Network Devices, Version 2.1, September 24, 2018, [CPP_ND_v2.1]

The TOE is the Alcatel-Lucent Enterprise OmniSwitch series 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.6.9.R11 executing on the following hardware platform configurations:

Family / Series	Main Processor
OmniSwitch 6465 (OS6465)	ARM Cortex-A9
OmniSwitch 6560 (OS6560	ARM Cortex-A9
OmniSwitch 6860 (OS6860)	ARM Cortex-A9
OmniSwitch 6865 (OS6865	ARM Cortex-A9
OmniSwitch 6900 (OS6900)	NXP MPC857
	NXP QorIQP2040
	Intel Atom C2538
OmniSwitch9900 (OS9900)	Intel Atom C2518

The TOE identified in this Validation Report has been evaluated at a NIAP approved CCTL using the "Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5)" (CEM) for conformance to the "Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5)" (CC) and the Assurance Activities (AA) of the aforementioned Protection Profile. This Validation Report 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 (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, reviewed testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all the functional requirements and assurance requirements stated in the Security Target (ST). 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 evaluation technical report are consistent with the evidence produced.

The CCTL atsec information security corporation evaluation team concluded that the CC requirements specified by:

- collaborative Protection Profile for Network Devices, Version 2.1, September 24, 2018.

have been met.

The technical information included in this report was obtained from Alcatel-Lucent Enterprise OmniSwitch series 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.6.R11 Security Target (ST) Version 3.1 and analysis performed by the Validation Team.

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) using the Common Evaluation Methodology (CEM) for Evaluation Assurance in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology 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.

The following table provides information needed to completely identify the product, including the following.

- 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 results of the evaluation
- The Protection Profile (PP) to which the product is conformant
- The organizations and individuals participating in the evaluation

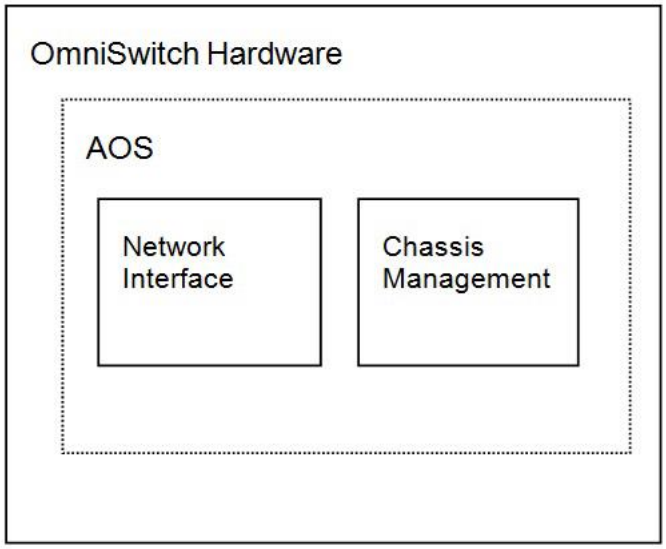
Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	The TOE is Alcatel-Lucent Enterprise OmniSwitch series 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.6.9.R11 executing on the following hardware platforms: • OmniSwitch 6465 (OS6465) (ARM Cortex-A9) • OmniSwitch 6560 (OS6560) (ARM Cortex-A9) • OmniSwitch 6860 (OS6860) (ARM Cortex-A9) • OmniSwitch 6865 (OS6865) (ARM Cortex-A9) • OmniSwitch 6900 (OS6900) (NXP MPC8572, NXP QorIQ P2040, Intel Atom C2538) • OmniSwitch 9900 (OS9900) (Intel Atom C2518)
PP	• collaborative Protection Profile for Network Devices, Version 2.1, September 24, 2018.
ST	Alcatel-Lucent Enterprise OmniSwitch series 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.6.R11 Security Target, Version 3.1, dated 2021-04-26
ETR	Evaluation Technical Report for a Target of Evaluation Alcatel-Lucent Enterprise OmniSwitch with AOS 8.6.R11 Alcatel-Lucent Enterprise OmniSwitch Alcatel-Lucent Enterprise OmniSwitch series 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.6.R11 Security Target, Version 3.1, as of 2021-04-29 Collaborative Protection Profile for Network Devices. Version 2.1 as of 24-September-2018; exact conformance. ETR Version 1.1 - RELEASED as of 2021-04-29
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	ALE USA Inc.
Developer	ALE USA Inc.
CCTL	atsec information security corporation, Austin, TX
CCEVS Validators	Paul Bicknell, John W Butterworth, Jean E Petty (MITRE Corporation) Farid Almed (John Hopkins University)

3. Architectural Information

Note that the following architectural description is based on the description presented in the ST.

The Target of Evaluation (TOE) is a network switch comprised of hardware and firmware. The firmware is named Alcatel-Lucent Operating System (AOS) which is the single purpose operating system that operates the management functions of all of the Alcatel-Lucent Enterprise OmniSwitch switches. The evaluation covers AOS 8.6.9.R11, based on the Linux version 3.10.104 operating system.

The diagram is a high-level illustration of the TOE.



TOE Evaluated Configuration

The evaluation covers the following hardware configurations running AOS 8.6.9.R11 as detailed in Table 1, below.

Table 1: Hardware configurations

TOE Family / Series	Hardware Model Numbers	Processor
OmniSwitch 6465	OS6465-P6	ARM Cortex-A9
	OS6465-P12	
	OS6465-P28	
	OS6465T-P12	
	OS6465T-12	
OmniSwitch 6560	OS6560-P24Z8	ARM Cortex-A9
	OS6560-P24Z24	
	OS6560-P48Z16	
	OS6560-24Z8	
	OS6560-24Z24	
	OS6560-24X4	
	OS6560-P24X4	
	OS6560-48X4	
	OS6560-P48X4	
	OS6560-X10	
OmniSwitch 6860	OS6860-24	ARM Cortex-A9
	OS6860-P24	
	OS6860-48	
	OS6860-P48	
	OS6860E-24	
	OS6860E-P24	
	OS6860E-48	
	OS6860E-P48	
	OS6860E-U28	
	OS6860E-P24Z8	
OmniSwitch 6865	OS6865-P16X	ARM Cortex-A9
	OS6865-U12X	
	OS6865-U28X	
OmniSwitch 6900	OS6900-X20	NXP MPC8572
	OS6900-X40	
	OS6900-T20	NXP QorIQ P2040
	OS6900-T40	
	OS6900-X72	
	OS6900-Q32	

	OS6900-V72	Intel Atom C2538
	OS6900-C32	
OmniSwitch 9900[1]	OmniSwitch 9907 Chassis	Not applicable
	OS9907-CFM Not applicable	OS9907-CFM Not applicable
	OS99-CMM Intel Atom C2518	OS99-CMM Intel Atom C2518
	OS99-XNI-48 Intel Atom C2338	OS99-XNI-48 Intel Atom C2338
	OS99-XNI-U48	
	OS99-GNI-48	
	OS99-GNI-P48	
	OS99-CNI-U8	
	OS99-XNI-P24Z8	
	OS99-XNI-P48Z16	
	OS99-XNI-U12Q	
	OS99-XNI-U24	
	OS99-XNI-U48	
	OS99-XNI-UP24Q2	

Physical Scope of the TOE

The TOE is a Network Device which consists of a hardware platform and its system firmware.

The TOE is located between the external and the internal network of an organization in order to perform Layer-2 switching, Layer-3 routing, and traffic filtering of flowing IP packets.
The TOE provides secured communication channels between itself and other trusted IT entities using TLS and SSH. Via the established network connection, the TOE can communicate with an SSHv2 client, SFTP server, or SNMP Management Station, allowing administrative control of the TOE.

Un-evaluated Functionality

The following functions were not evaluated and are therefore not included in the secure configuration of the mobile devices.

- **Virtual Chassis Mode**

  This feature allows a group of switches to operate as a single bridge and router. In the evaluation, the TOE must always operate in Standalone mode.

[1] This model uses Network Interface (NI) cards that include an Intel Atom C2338 processor, but does not execute any cryptographic functionality claimed in the Security Target.

- **Captive Portal**

  This feature allows web-based authentication of end users.

- **Terminal Access Controller Access-Control System Plus (TACACS+)**

  Authentication using an external TACACS+ server is not allowed in the evaluated configuration.

- **Port Mobility Rules**

  Port mobility allows dynamic VLAN port assignment based on VLAN rules that are applied to port traffic.

- **FTP access to the TOE**

  FTP traffic is not secured so the FTP service must be disabled for security reasons.

- **Telnet access to the TOE**

  Telnet traffic is not secured so the Telnet service must be disabled for security reasons.

- **Webview**

  This web-based interface used for management must be disabled.

- **SNMP**

  SNMP versions 1 and 2 must be disabled in the CC evaluated configuration. Only SNMP version 3 using TSM is allowed (i.e., protected by a secure channel using the TLS protocol).

- **HTTP**

  HTTP and HTTPs must be disabled in the CC evaluated configuration.

- **Cryptographic algorithms**

  The MD5 algorithm cannot be used.

- **NTP**

  The use of NTP to synchronize the time with an external time source must be disabled in the CC evaluated configuration.

- **IPsec**

  IPsec must be disabled in the CC evaluated configuration.

4. Security Policy

This section summaries the security functionality of the TOE including the following.

1. Audit

2. Identification and authentication
3. Security management
4. Cryptographic support
5. Protection of the TSF (TOE Security Functionality)
6. Trusted path/channels
7. TOE access

Audit

The TOE generates audit records. The audit records can be displayed on the serial console as they are generated in a scrolling format.

The TOE writes audit records to a set of circular files stored in the systems flash memory for permanent storage. These entries are tagged with the AOS application ID of the TOE subsystem that triggers the audit records to be generated. The TOE also provides the ability to send the audit records to an external syslog server using a secure channel.

The TOE provides to security administrators the ability to modify the maximum size allowed for the audit files. Once the files are full the oldest entries are overwritten.

Identification and Authentication

The TOE requires identification and authentication of administrators of the TOE prior to access any of the management functionality in all possible scenarios, which are as follows:

- TOE administrators accessing (either locally or remotely) the Command Line Interface (CLI) via a serial console or a Secure Shell (SSH) session.
- TOE administrators accessing TOE storage using SFTP via an SSH session.
- A SNMP Management Station accessing the TOE through the SNMP management interface.

The TOE displays to the administrator a configurable banner before the administrator successfully logs onto the TOE (either serial console, SSH, or SFTP). The TOE also provides the ability to lock the administrator after a configurable number of unsuccessful attempts and terminate the logon session after a configurable period of inactivity.

The TOE provides administrator configurable password settings to enforce password complexity when a password is created or modified.

The TOE provides support to support Identification and Authentication mechanisms:

- Identification and Authentication made by the TOE using credentials stored in the local file system;

- Identification and Authentication made by the TOE using credentials stored in a Lightweight Directory Access Protocol (LDAP) server, which is part of the operational environment; or
- Identification and Authentication made by an external authentication server, which is part of the operational environment.

The only external authentication server supported by the TOE for administrator authentication in the evaluated configuration is Remote Authentication Dial In User Service (RADIUS).

Communications with RADIUS servers, LDAP servers and SNMP Management stations are protected
with the Transport Layer Security (TLS) protocol. Communication with SSH and SFTP clients are protected with the Secure Shell (SSH) protocol.

Security Management

The TOE provides a Command-Line Interface (CLI) for security management. TOE administrators connect to the TOE via either a serial console or a remote session using Secure Shell (SSHv2). In either case, administrators are required to identify and authenticate against the TOE before getting access to the CLI.

The TOE provides an SNMPv3 management interface for security management functionality. An SNMP Management Station authenticates to the TOE and can send request commands to get and set configuration information.

The TOE also provides a Flash file system used for storing configuration files/directories. TOE administrators connect to the TOE via the Secure File Transfer Protocol (SFTP), providing their credentials to identify and authenticate against the TOE before any action.

Cryptographic Support

The TOE requires cryptography to support the following functionality.

- Establishment of secure channels using the SSHv2, TLSv1.1 and TLSv1.2 protocols.
- X.509 certificate generation and validation.
- Storage of passwords.
- Self-tests of the cryptographic algorithms.
- Verification of the integrity of the TOE firmware.

The TOE provides cryptographic support using the OpenSSL and OpenSSH software packages, which are bundled in the TOE.

Protection of the TSF

The TOE protects itself by requiring administrators to identify and authenticate themselves prior to performing any actions and by defining the access allowed by each administrator. The TOE

uses the filesystem access control to protect access to sensible data like cryptographic keys and credentials.

The TOE ensures that manual updates of the TOE firmware are done using trusted updates by verifying the integrity of the new version of the TOE firmware.

The TOE also implements self-tests to ensure the correct operation of cryptographic services.

The TOE also provides a reliable date and time that is used for audit record timestamps, certificate verification and session timing.

TOE Access

The TOE displays to the administrator a configurable banner before the administrator successfully logs onto the TOE (either serial console, SSH, or SFTP). The TOE also provides the ability to lock the administrator after a configurable number of unsuccessful attempts and terminate the logon session after a configurable period of inactivity.

Trusted Path/Channels

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

- Transport Layer Security (TLS) versions 1.1 and 1.2 are used to protect communication with authentication servers (RADIUS), LDAP servers, SNMP Management stations, and audit servers (syslog).
- Secure Shell version 2 (SSHv2) is used to protect communication with SSH and SFTP clients and servers.

5. Assumptions

The Security Problem Definition, including the assumptions, may be found in

- collaborative Protection Profile for Network Devices, Version 2.1, September 24, 2018.

That information has not been reproduced here and the respective documents should be consulted if there is interest in that material. Additionally, the Security Problem Description has been presented in the Security Target.

Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the collaborative Protection Profile for Network Devices, Version 2.1 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the product needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

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

Note: As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the Supporting Document Mandatory Technical Document Evaluation Activities for Network Device cPP, Version 2.1, September 2018.), [CPP_ND_V2.1-SD]) performed by the evaluation team.

6. Documentation

The following documentation was used as evidence for the evaluation of the TOE.

Design Documentation

None

Guidance Documentation

The following documentation was used as evidence for the evaluation.

Reference	Document Name	Location
[CCGUIDE]	Preparation and Operation of Common Criteria Evaluated OmniSwitch Products - AOS 8.6.R11	https://www.niap-ccevs.org/MMO/Product/st_vid11069-agd.pdf
[AOS8-RN]	AOS Release 8.3.1 Release Notes	
[AOS8-SM]	OmniSwitch AOS Release 8 Switch Management Guide	
[AOS8-CLI]	OmniSwitch AOS Release 8 CLI Reference Guide	
[AOS8-NC]	OmniSwitch AOS Release 8 Network Configuration Guide	
[AOS8-ARC]	OmniSwitch AOS Release 8 Advanced Routing Configuration Guide	
[AOS8-TCV]	OmniSwitch AOS Release 8 Transceivers Guide	
[AOS8-DCS]	OmniSwitch AOS Release 8 Data Center Switching Guide	
[OS6465-HWUG]	OmniSwitch 6465 Hardware Users Guide	
[OS6560-HWUG]	OmniSwitch 6560 Hardware Users Guide	

Reference	Document Name	Location
[OS6860-HWUG]	OmniSwitch 6860 Hardware Users Guide	
[OS6865-HWUG]	OmniSwitch 6865 Hardware Users Guide	
[OS6900-HWUG]	OmniSwitch 6900 Hardware Users Guide	
[OS9900-HWUG]	OmniSwitch 9900 Hardware Users Guide	

Any additional customer documentation delivered with the product or that may be available through download was not included in the scope of the evaluation and hence should not be relied upon when configuring or using the products in the evaluated configuration.

7. IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

Evaluation Team Independent Testing

The ST lists more TOE models compared to the subset of devices used for testing. The tests were performed on the TOE models listed above which were selected, by choosing one from within each device family.

In addition, the security functions specified in the ST are all implemented above the hardware layer. Once a request is processed by the hardware, the security relevant decisions have been already made by the software. The hardware now only needs to enforce the functionality requested by the software. Based on this consideration, the evaluation team used the hardware information provided by the developer which lists all TOE models found in the ST and references the CPUs used by those models. All devices listed in the ST use one of the following CPUs:

- ARM Cortex-A9
- NXP MPC8572
- NXP QorIQ P2040
- Intel Atom C2538
- Intel Atom C2518

The test systems were set up according to a setup strategy that followed the evaluated configuration requirements specified in the guidance, supplemented by configurations required to perform testing.

The testing was performed by setting in addition to the TOE platforms, a a VMware EXSi system hosting two Linux virtual machines is used for testing. The two Linux VMs are used for the following purposes.

1. A server VM #1 running CentOS 8
   Hosting the following services and protocols:
   - Radius: FreeRADIUS Version 3.0.17 (TLS 1.1, 1.2)
   - LDAP: openldap version 2.4.46 (TLS 1.1, 1.2)
   - SSH: (OpenSSH_8.0p1)
   - SFTP (SSH)
   - OpenSSL: version 1.1.1c FIPS 28 May 2019
   - Syslog: syslog-ng 3.23.1 (TLS 1.1, 1.2)
2. A client VM #2 running CentOS 8

The following software tools were used during testin:

1. Wireshark Version 2.6.2
2. Tcpdump Version 4.9.3
3. Nmap Version 7.70

The test network configuration consists of the 6 TOE platforms and 2 Linux VMs hosted by the EXSi hardware platform listed above. In addition, there is a router/firewall device which protects the test network and allows access to it from the atsec internal network only. The only access to any TOE device is from one of the two Linux VMs.

8. Evaluated Configuration

The guidance documentation provides specific instructions for configuring the AOS to comply with the functions defined in the Security Target. The evaluated configuration included the TOE models listed below running AOS 8.6.9.R11:

- OmniSwitch 6465 (OS6465) with CPU ARM Cortex-A9
- OmniSwitch 6560 (OS6560) with CPU ARM Cortex-A9
- OmniSwitch 6860 (OS6860) with CPU ARM Cortex-A9
- OmniSwitch 6865 (OS6865) with CPU ARM Cortex-A9
- OmniSwitch 6900 (OS6900) with CPU NXP MPC8572
- OmniSwitch 6900 (OS6900) with CPU NXP QorlQ P2040
- OmniSwitch 6900 (OS6900) with CPU Intel Atom C2538
- OmniSwitch 9900 (OS9900) with CPU Intel Atom C2518

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 ETR.

All work units defined by CC Version 3.1 Revision 5 and CEM Version 3.1 Revision 5 and the [CPP_ND_v2.1-SD] received a pass verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements as well as assurance activities. The evaluation was conducted based upon CEM Version 3.1 Revision 5. The evaluation determined the TOE to be CC Part 2 extended and Part 3 conformant, and to meet the assurance requirements defined by the [CPP_ND_v2.1].

Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit and the assurance activity specified in the [CPP_ND_V2.1-SD]. 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 ALE product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validators 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 the [CPP_ND_V2.1-SD] and that the conclusion reached by the evaluation team was justified.

Evaluation of the Development Documentation (ADV)

The evaluation team applied each ADV CEM work unit and assurance activity specified in [CPP_ND_V2.1-SD]. The evaluation team assessed the documentation and found it adequate to aid in understanding how the TSF provides the security functions. The documentation consists of a functional specification contained in the Security Target and guidance documents.

The validators 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 the [CPP_ND_V2.1-SD] and that the conclusion reached by the evaluation team was justified.

Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit and assurance activity specified in [CPP_ND_V2.1-SD]. 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. Both the administrator and user guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validation team 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 the [CPP_ND_V2.1-SD] and that the conclusion reached by the evaluation team was justified.

Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The ALC evaluation also ensured the TOE is identified such that the consumer can identify the evaluated TOE.

The validators 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 the [CPP_ND_V2.1-SD] and that the conclusion reached by the evaluation team was justified.

Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit and assurance activity specified in the [CPP_ND_V2.1-SD]. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. The evaluation team performed devised an independent set of tests as mandated by the protection profile.

The validators 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 the [CPP_ND_V2.1-SD] and that the conclusion reached by the evaluation team was justified.

Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit and assurance activity specified in the [CPP_ND_V2.1-SD]. The vendor provided security updates to the TOE during the evaluation, therefore, while the tested version of the TOE did contain vulnerabilities, subsequent security updates, in line with the guidance provided in Scheme Policy Letter 15, fixed all known issues. The evaluation team ensured that the currently available version of the TOE does not contain known exploitable flaws or weaknesses in the TOE based upon the evaluation team's vulnerability analysis, and the evaluation team's performance of penetration tests.

The evaluators searched for publicly known vulnerabilities applicable to AOS using the following sources:

- Common Vulnerabilities and Exposures (CVE)
  https://cve.mitre.org/cve/cve.html
- Exploit Database (EDB)
  http://www.exploit-db.com/
- National Vulnerability Database (NVD)

https://nvd.nist.gov/vuln/search

- Packet Storm (PS)
  https://packetstormsecurity.com
- SecurityFocus (SF)
  http://www.securityfocus.com/vulnerabilities
- United States Computer Emergency Readiness Team (US-CERT)
  http://search.us-cert.gov/search?affiliate=us-cert
- OpenSSL website (the evaluator only searched this

The evaluator also accessed the developer's own customer support site available only to registered
customers:

- Developers site for security publications
  https://businessportal.al-enterprise.com/

using the following search terms:

- router
- switch
- IPsec
- SSHv2
- SFTP
- TLS
- 802.1Q
- IPv4
- 802.1X
- OSCP
- ICMP
- IGMP
- TCP
- UDP
- BGP
- RIPv2, RIPng
- OSPF, OSPFv3
- VRRP, VRRPv2, VRRPv3
- VLAN
- UNP
- CRL
- MAC-based authentication
- DHCP
- DHCPv6
- SNMP, SNMPv3
- syslog-ng
- PPPoE
- OmniSwitch 6465

- OmniSwitch 6560
- OmniSwitch 6860
- OmniSwitch 6865
- OmniSwitch 6900
- OmniSwitch 9900
- AOS 8.6.9.R11
- Linux 3.10.104
- OpenSSL 1.0.2u, OpenSSL-fips 2.0.16
- OpenSSH 7.7p1

The evaluator found no vulnerabilities applicable to the TOE that could be exploited by a Basic Attack Potential or that required any additional testing apart from the evaluator's normal independent testing.

The validators 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 the [CPP_ND_V2.1-SD] and that the conclusion reached by the evaluation team was justified.

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 performance of the testing defined by the [CPP_ND_V2.1-SD] and the penetration test also demonstrated the accuracy of the claims in the ST.

The validator's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM and the [CPP_ND_V2.1-SD] and correctly verified that the product meets the claims in the ST.

10. Validator Comments/Recommendations

The validators suggest that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the Security Target, and the only evaluated functionality was that which was described by the SFRs claimed in the Security Target. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained.

11. Annexes

Not applicable.

12. Security Target

Alcatel-Lucent Enterprise OmniSwitch series 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.6.R11 Security Target, Version 3.1, dated 2021-04-26

13. Glossary

The following definitions are used throughout this document.

AA	Assurance Activity
AES	Advanced Encryption Standard
ARM	Advanced RISC Machine
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory—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.
CEM	Common Criteria Evaluation Methodology
CPU	Central Processing Unit
Conformance	The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
EC	Elliptic Curve
ETR	Evaluation Technical Report
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.
HMAC	Keyed-hash Message Authentication Code
NIAP	National Information Assurance Partnership
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
PP	Protection Profile

RFC	Request For Comments
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation—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.
TLS	Transport Layer Security
TSF	TOE Security Functionality
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.
VR	Validation Report

14. Bibliography

The evaluation team used the following documents to produce this Validation Report:

- Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.
- PP-Configuration for Mobile Device Fundamentals (MDF), Mobile Device Management (MDM) Agents, and Virtual Private Network (VPN) Clients, Version 1.0, 28 February 2020.
- collaborative Protection Profile for Mobile Devices, Version 21, September 24, 2018.
- Supporting Document Mandatory Technical Document Evaluation Activities for cPP, Version 2.1. September 2018.
- Preparation and Operation of Common Criteria Evaluated OmniSwitch Products (NDcPP), AOS Release 8.6.R11, Rev April 2021.
- Alcatel-Lucent Enterprise OmniSwitch series 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.6.R11 Security Target, Version 3.1, 2021-04-26
- Assurance Activity Report, Version 1.2, 2021-04-29