National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme


# Validation Report for

# Alcatel-Lucent Enterprise OmniSwitch series 6360, 6465, 6465T, 6560, 6570, 6860N, 6865, 6870, 6900, 9900 with AOS 8.10

| | |
|---|---|
| Report Number: | CCEVS-VR-VID11627-2026 |
| Dated: | February 25, 2026 |
| Version: | 1.0 |

**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 Meade, MD 20755-6982**

# Acknowledgements

**Validation Team**

Swapna Katikaneni

Marybeth Panock

Patrick Mallett, Ph. D.

*The Aerospace Corporation*

**Common Criteria Testing Laboratory**

Joachim Vandersmissen

James Reid

Parker Collier

*atsec information security corporation*

Austin, TX

# Table of Contents

# List of Tables

# 1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Alcatel-Lucent Enterprise OmniSwitch series 6360, 6465, 6465T, 6560, 6570, 6860N, 6865, 6870, 6900, 9900 with AOS 8.10 (the Target of Evaluation, or 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 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 in 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 evaluated and tested and any restrictions on the evaluated configuration. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST. 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.

The evaluation was performed by atsec Common Criteria Testing Laboratory (CCTL) in Austin, TX, USA, and was completed in February 2026. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report written by atsec. The evaluation determined that the TOE is Common Criteria Part 2 Extended and Common Criteria Part 3 Conformant and meets the assurance requirements of the *Protection Profiles* and *Functional Packages* identified in Table 1.

# 2 Identification

The Common Criteria Evaluation and Validation Scheme (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, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria (CC) and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, 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 IT products can contract with a CCTL and pay a fee for their product's security evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List (PCL).

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

- The TOE—the fully qualified identifier of the product as evaluated
- The ST—the unique identification of the document describing the security features, claims, and assurances of the product
- The conformance result of the evaluation
- The *PPs/PP-Modules/Packages* to which the product is conformant
- The organizations and individuals participating in the evaluation.

**Table 1: Evaluation Identifiers**

| Item | Identifier |
|---|---|
| **Validation Scheme** | U.S. NIAP CCEVS |

| | |
|---|---|
| **TOE** | Alcatel-Lucent Enterprise OmniSwitch series 6360, 6465, 6465T, 6560, 6570, 6860N, 6865, 6870, 6900, 9900 with AOS 8.10 |
| **Security Target** | Alcatel-Lucent Enterprise OmniSwitch series 6360, 6465, 6465T, 6560, 6570, 6860N, 6865, 6870, 6900, 9900 with AOS 8.10 Security Target, Version 1.2, 2026-01-15 |
| **Sponsor & Developer** | ALE USA Inc. |
| **Completion Date** | February 2026 |
| **CC Version** | Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017 |
| **CEM Version** | Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017 |
| **PP** | • collaborative Protection Profile for Network Devices, Version 3.0e, 2023-12-06<br>• Functional Package for Secure Shell (SSH), Version 1.0, 2021-05-13 |
| **Conformance Result** | PP Compliant, CC Part 2 extended, CC Part 3 conformant |
| **CCTL** | atsec information security corporation<br>4516 Seton Center Parkway Suite 250<br>Austin, TX 78759 |
| **Validation Personnel** | Swapna Katikaneni, Marybeth Panock, Patrick Mallett |
| **Evaluation Personnel** | Joachim Vandersmissen, James Reid, Parker Collier |

# 3 TOE Architecture

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

The TOE is Alcatel-Lucent Enterprise OmniSwitch family of network switches. All the switches in the OmniSwitch family use the same secure level code, support Deep Packet Inspection (DPI) and Shortest Path Bridging (SPB), and provide wire-rate switching and routing capacity.

The TOE includes hardware and software components listed in Table 2 in Section 8.1.

The software running all the platforms below is Alcatel-Lucent Operating System (AOS), which is the single purpose operating system supporting device management and network management.

# 4 Environmental Strengths

The TOE provides the following security functions as described in the ST.

## 4.1 Security Audit

The TOE generates audit records for security-related events. The audit records contain time stamps and other information about the events, which are helpful to the administrator in investigating the issues related to the configuration and operation of the TOE.

The TOE writes audit records to a set of circular log files stored in the flash memory for permanent storage. The TOE can be configured to transfer the audit data to an external syslog server in real-time using the TLS protocol.

## 4.2 Cryptographic Support

The TOE implements cryptography supporting the following functionalities:

- Establishment of secure network connections using the SSH and TLS protocols
- Validation of X.509 certificates
- Storage of user passwords
- Digital signature verification of TOE software updates

The TOE provides cryptographic support using the OpenSSL library version 3.0.13, which is bundled in the TOE. The TOE also includes a software-based, SP800-90B compliant Entropy Source seeding DRBGs with full entropy.

## 4.3 Identification and Authentication

Administrators can access the TOE through either the local console port or a remote SSH client. The TOE authenticates administrators before granting access to management functions. For local administrative sessions, authentication is performed using passwords. For remote sessions, administrators are authenticated via SSH passwords or SSH public keys. The TOE also supports validation of X.509 certificates for authenticating external IT entities.

## 4.4 Security Management

The TOE provides a Command-Line Interface (CLI) to the administrators for managing the configurable aspects of the TOE. The TOE provides a range of management functions, which are restricted to administrators with the appropriate privileges.

## 4.5 Protection of the TSF

The TOE includes protective features to maintain the integrity and reliability of its security functions.

- The TOE uses filesystem access control to protect sensitive data such as cryptographic keys and credentials.
- The TOE employs digital signatures to ensure trusted updates to the TOE software.
- The TOE performs self-tests to verify the correct operation of cryptographic services and the overall integrity of TOE software.
- The TOE provides a reliable system date and time, which is used for audit record time stamps, SSH rekeying, certificate validation, account lockout, and administrative session termination.

## 4.6 TOE Access

The TOE can be configured to display a login banner when an administrator establishes an interactive session (both local and remote). The TOE terminates interactive sessions after an administrator-defined period of inactivity. The TOE allows administrators to terminate their own administrative sessions.

## 4.7 Trusted Path/Channel

The TOE includes the OpenSSL library version 3.0.13 and OpenSSH package version 9.8. The TOE implements the TLS protocol version 1.2 (TLS v1.2) and the SSH protocol version 2 (SSHv2) using OpenSSL and OpenSSH, respectively.

- The TOE uses the TLS protocol to secure communications with the external audit server.
- The TOE uses the SSH protocol to protect administrative sessions from the administrator's workstation to the TOE.

# 5 Assumptions and Clarification of Scope

## 5.1 Assumptions

The ST references the *PPs, PP-Modules,* and *Packages* to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed *PPs, PP-Modules,* and *Packages*, as listed in Table 1.

## 5.2 Clarification of Scope

As with any evaluation, this evaluation shows only that the evaluated configuration meets the security claims made, with a certain level of assurance, achieved through performance by the evaluation team of the evaluation activities specified by the *PPs*, *PP-Modules*, and *Packages* specified in Table 1.

- This evaluation covers only the specific software distribution and version identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in Alcatel-Lucent Enterprise OmniSwitch series 6360, 6465, 6465T, 6560, 6570, 6860N, 6865, 6870, 6900, 9900 with AOS 8.10 Security Target, Version 1.2, 2026-01-15 ([ST]). Any additional security related functional capabilities included in the product were not covered by this evaluation. In particular, the functionality mentioned in Section 8.2 of this document is excluded from the scope of the evaluation.
- This evaluation did not specifically search for, nor attempt to exploit, 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 TOE must be installed, configured, and managed as described in the documentation referenced in Section 6 of this VR.

# 6 Documentation

The vendor provides guidance documents describing the installation process for Alcatel-Lucent Enterprise OmniSwitch series 6360, 6465, 6465T, 6560, 6570, 6860N, 6865, 6870, 6900, 9900 with AOS 8.10, as well as guidance for subsequent administration and use of the applicable security features.

The following guidance documentation was examined during the evaluation:

- Alcatel-Lucent Enterprise Preparation and Operation of Common Criteria Evaluated OmniSwitch Products (NDcPP) AOS Release 8.10, January 2026

To use the TOE in the evaluated configuration, the product must be configured as specified in the guidance documentation listed above. Consumers are encouraged to download this documentation from the NIAP website. Only the guidance documentation listed above and the specified sections of the other documents referenced by that

guide should be trusted for the installation, administration, and use of the TOE in its evaluated configuration. Any other documentation (e.g., published on the vendor's website) was not covered by the evaluation and therefore should not be relied upon to configure or operate the TOE as evaluated.

# 7 IT Product Testing

A non-proprietary description of the tests performed, and their results is provided in Section 2.3.5 of the Assurance Activity Report ([AAR]).

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to the *PPs*, *PP-Modules*, and *Packages* listed in Table 1.

## 7.1 Developer Testing

No evidence of developer testing is required by the assurance activities for this TOE.

## 7.2 Evaluation Team Testing

The evaluation team established a test configuration comprising Alcatel-Lucent Enterprise OmniSwitch series 6360, 6465, 6465T, 6560, 6570, 6860N, 6865, 6870, 6900, 9900 with AOS 8.10 running on platform listed in Table 2 in Section 8.1. Section 2.3.5 of the Assurance Activity Report ([AAR]) provides a detailed description of the test configuration the CCTL used to test the TOE, including a description of the test environment and a list of tools used.

The evaluation team devised a Test Plan based on the Test Activities specified in the above *PP* and *Functional Package*. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

Independent testing took place at the atsec CCTL facility in Austin, TX, between November 2025 and January 2026.

The evaluators received the TOE in the form that customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements were fulfilled.

# 8 TOE Evaluated Configuration

## 8.1 Evaluated Configuration

The TOE is the device chassis encompassing the hardware and software. The TOE software is AOS software, which executes on the hardware platforms listed in the following table when configured in accordance with the documentation specified in Section 6.

**Table 2: TOE Hardware Platforms**

| Model | Switch Processor | Application Processor Series | Software Image | Network Interface |
|---|---|---|---|---|
| OmniSwitch 6360 | Marvell 98DX236S | Arm ARMv7-A Cortex-A | Nosa.img | Marvell AlleyCat 3 |
| | Marvell 98DX233S | | | |

| Model | Switch Processor | Application Processor Series | Software Image | Network Interface |
|---|---|---|---|---|
| OmniSwitch 6465 | Marvell 98DX3233 | Arm ARMv7-A Cortex-A | Nos.img | Marvell AlleyCat 3 |
| OmniSwitch 6465T | Marvell 98DX3233 | Arm ARMv7-A Cortex-A | Nos.img | Marvell AlleyCat 3 |
| OmniSwitch 6560 | Marvell 88F6820 | Arm ARMv7-A Cortex-A | Nos.img | Marvell AlleyCat 3 |
| OmniSwitch 6570 | Marvell 98DX3501 | Arm ARMv8.2-A Cortex-A | Wos.img | Marvell AlleyCat 5 |
| | Marvell 98DX3510 | | | |
| OmniSwitch 6860N | Intel Atom C3338 | Intel Goldmont Atom | Uosn.img | Broadcom Trident3 |
| | Intel Atom C3558 | | | |
| OmniSwitch 6865 | Broadcom BCM56342 | Arm ARMv7-A Cortex-A | Uos.img | Broadcom Helix4 |
| OmniSwitch 6870 | Intel Atom C3338 | Intel Goldmont Atom | Kos.img | Marvell Prestera DX |
| | Intel Atom C3558 | | | |
| OmniSwitch 6900 | Intel Atom C3558 | Intel Goldmont Atom | Yos.img | Broadcom Trident3 |
| | Intel Xeon D1518 | Intel Broadwell Xeon | | |
| OmniSwitch 9900 | Intel Atom C2518 | Intel Silvermont Atom | Mos.img | Marvell Prestera DX |
| | Intel Atom C3558 | Intel Goldmont Atom | | |

## 8.2 Excluded Functionality

The following features interfere with the TOE security functionality claims and must be either disabled or not configured for use in the evaluated configuration.

- File Transfer Protocol (FTP) access to the TOE
- Telnet access to the TOE
- Webview access to the TOE
- Hypertext Transfer Protocol (HTTP)
- Simple Network Management Protocol (SNMP)
- Lightweight Directory Access Protocol (LDAP) for external authentication
- Remote Authentication Dial-In User Service (RADIUS) for external authentication
- Network Time Protocol (NTP)
- Captive Portal
- Terminal Access Controller Access-Control System Plus (TACACS+)

- Port Mobility Rules

# 9 Results of the Evaluation

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the proprietary Evaluation Technical Report for Alcatel-Lucent Enterprise OmniSwitch series 6360, 6465, 6465T, 6560, 6570, 6860N, 6865, 6870, 6900, 9900 with AOS 8.10 ([*ETR*]). The reader of this VR can assume that all assurance activities and work units received passing verdicts.

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, revision 5 ([CCPART1], [CCPART2], [CCPART3]) and CEM version 3.1, revision 5 ([CEM]), and the specific evaluation activities specified in the *PPs*, *PP-Modules*, and *Packages* listed in Table 1.

The evaluation determined the TOE satisfies the conformance claims made in the Alcatel-Lucent Enterprise OmniSwitch series 6360, 6465, 6465T, 6560, 6570, 6860N, 6865, 6870, 6900, 9900 with AOS 8.10 Security Target ([ST]), of Part 2 extended and Part 3 conformant. The TOE satisfies the requirements specified in the *PPs*, *PP-Modules*, and *Packages* listed in Table 1.

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

## 9.1 Evaluation of the Security Target (ST) (ASE)

The evaluation team performed each TSS assurance activity and each CEM work unit from ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.1, ASE_REQ.1, ASE_SPD.1, and ASE_TSS.1. The ST evaluation ensured the ST contains an ST introduction, TOE overview, TOE description, security problem definition in terms of threats, policies and assumptions, description of security objectives for the operational environment, a statement of security requirements claimed to be met by the product that are consistent with the claimed *PPs*, *PP-Modules*, and *Packages*, and security function descriptions that satisfy the requirements.

## 9.2 Evaluation of the Development Activities (ADV)

The evaluation team performed each ADV assurance activity and applied each CEM work unit from ADV_FSP.1. The evaluation team assessed the evaluation evidence and found it adequate to meet the requirements specified in the claimed *PPs, PP-Modules*, and *Packages* for design evidence. The ADV evidence consists of the TSS descriptions provided in the ST and product guidance documentation providing descriptions of the TOE external interfaces.

## 9.3 Evaluation of the Guidance Activities (AGD)

The evaluation team performed each AGD assurance activity and applied each CEM work unit from AGD_OPE.1 and AGD_PRE.1. The evaluation team determined the adequacy of the operational user guidance in describing how to operate the TOE in accordance with the descriptions in the ST. The evaluation team followed the guidance in the TOE preparative procedures to test the installation and configuration procedures to ensure the procedures result in the evaluated configuration. The guidance documentation was assessed during the design and testing phases of the evaluation to ensure it was complete.

## 9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team performed each ALC assurance activity and applied each CEM work unit from ALC_CMC.1, ALC_CMS.1, ALC_FLR.2 to the extent possible given the evaluation evidence required by the claimed *PPs*, *PP-Modules*, and *Packages.* The evaluation team ensured the TOE is labeled with a unique identifier consistent with the

TOE identification in the evaluation evidence and also that flaw reporting procedures are sufficiently described in the evaluation evidence.

## 9.5 Evaluation of the Test Documentation and the Test Activities (ATE)

The evaluation team performed each ATE assurance activity and applied each CEM work unit from ATE_IND.1. The evaluation team ran the set of tests specified by the claimed *PPs*, *PP-Modules*, and *Packages* and recorded the results in the Test Report, summarized in section 2.3.5 of the [AAR].

## 9.6 Evaluation of the Vulnerability Assessment Activity (AVA)

The evaluation team performed each AVA assurance activity and applied each CEM work unit from AVA_VAN.1. The evaluation team performed a vulnerability analysis following the processes described in the claimed PPs, PP-Modules, and Packages. This comprised a search of public vulnerability databases.

Search terms were used during the vulnerability search:

Omniswitch

OpenSSL

OpenSSH

Intel Atom

Intel Xeon

Marvell

Broadcom

Arm cortex

zlib

The evaluator searched for publicly known vulnerabilities using the following sources:

MITRE Common Vulnerabilities and Exposures (CVE) List:o

https://cve.mitre.org/cve/

National Vulnerability Database (NVD):o

https://nvd.nist.gov/

CISA Known Exploited Vulnerabilities (KEV) Catalog:o

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

US-CERT:o

https://www.kb.cert.org/vuls/html/search

Tenable Network Security:o

https://www.tenable.com/plugins

Tipping Point Zero Day Initiative:o

https://www.zerodayinitiative.com/advisories/published/

Rapid7 Vulnerability Database:o

https://www.rapid7.com/db/?type=nexpose

OpenSSL Vulnerabilities:

https://openssl-library.org/news/vulnerabilities-3.0/

The vulnerability search was repeated on the following dates, throughout the evaluation process (last search date: 2026-02-18):

2025-10-02

2025-10-14

2025-10-21

2025-10-31

2025-11-06

2025-11-14

2025-11-21

2025-12-05

2025-12-11

2025-12-18

2026-01-14

2026-02-18

All “crucial” vulnerabilities (as defined by the NIAP Policy 17 Addendum #1) were mitigated.

Finally, the evaluator examined the Type 1, Type 2, and Type 3 flaw hypotheses specified in Appendix A.1 of [CPP_ND_V3.0E-SD]. The Type 4 flaw hypotheses are not mandatory and were therefore not tested. More information, including the process of the vulnerability analysis and the result of the analysis, is provided in the proprietary Evaluation Technical Report (ETR).

## 9.7 Summary of Evaluation Results

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met, sufficient to satisfy the evaluation activities specified in the claimed *PP*. Furthermore, the evaluation team’s testing demonstrates 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 followed the procedures defined in the CEM, 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 guide in Section 6.

No versions of the TOE and software, either earlier or later are covered by the scope of this evaluation. Please note that 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. All other

functionalities provided by devices in the operational environment need to be assessed separately and no further conclusions can be drawn about their effectiveness.

The validation team recommends that the customer pay attention to the excluded functionality discussed in Section 5 and 8.2 as they all appear to be security functions likely to be used.

# 11 Security Target

The ST for this product's evaluation is Alcatel-Lucent Enterprise OmniSwitch series 6360, 6465, 6465T, 6560, 6570, 6860N, 6865, 6870, 6900, 9900 with AOS 8.10 Security Target, Version 1.2, 2026-01-15 ([ST]).

# A Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

| | |
|---|---|
| **CAVP** | Cryptographic Algorithm Validation Program |
| **CC** | Common Criteria for Information Technology Security Evaluation |
| **CCTL** | Common Criteria Testing Laboratory |
| **CEM** | Common Evaluation Methodology |
| **ETR** | Evaluation Technical Report |
| **HTTPS** | Hypertext Transfer Protocol Secure |
| **IT** | Information Technology |
| **NIAP** | National Information Assurance Partnership |
| **NIST** | National Institute of Standards and Technology |
| **PCL** | Product Compliant List |
| **PP** | Protection Profile |
| **SAR** | Security Assurance Requirement |
| **SFR** | Security Functional Requirement |
| **ST** | Security Target |
| **TOE** | Target of Evaluation |
| **TSF** | TOE Security Functions |
| **TSS** | TOE Summary Specification |
| **VR** | Validation Report |

# B Bibliography

The validation team used the following documents to produce this VR:


| | |
|---|---|
| [CCPART1] | Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017. |
| [CCPART2] | Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components, Version 3.1, Revision 5, April 2017. |
| [CCPART3] | Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security assurance requirements, Version 3.1, Revision 5, April 2017. |
| [CEM] | Common Criteria Project Sponsoring Organisations. Common Evaluation Methodology for Information Technology Security, Version 3.1, Revision 5, April 2017. |
| [ST] | Alcatel-Lucent Enterprise OmniSwitch series 6360, 6465, 6465T, 6560, 6570, 6860N, 6865, 6870, 6900, 9900 with AOS 8.10 Security Target, Version 1.2, 2026-01-15 ([ST]). |
| [CCGUIDE] | Alcatel-Lucent Enterprise Preparation and Operation of Common Criteria Evaluated OmniSwitch Products (NDcPP) AOS Release 8.10, Jan 2026 |
| [ETR] | Evaluation Technical Report Alcatel-Lucent Enterprise OmniSwitch series 6360, 6465, 6465T, 6560, 6570, 6860N, 6865, 6870, 6900, 9900 with AOS 8.10, Version 1.1, 2026-02-23 |
| [AAR] | Assurance Activity Report Alcatel-Lucent Enterprise OmniSwitch series 6360, 6465, 6465T, 6560, 6570, 6860N, 6865, 6870, 6900, 9900 with AOS 8.10, Version 1.1, 2026-02-23 |