National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12

Report Number: CCEVS-VR-VID11456-2025
Dated: April 10, 2025
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

Sheldon Durrant
Randy Heimann
Lisa Mitchell
Linda Morrison
Lori Sarem
Chris Thorpe
The MITRE Corporation

Common Criteria Testing Laboratory

Sean Bennett
Greg McLearn
Joon Sim
Kevin Steiner
Lightship Security USA, Inc.

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Cisco catalyst 9800 Series Wireless Controllers and Access Points 17.12 provided by Cisco Systems, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

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.

The evaluation was performed by the Lightship Ottawa laboratory, an affiliate of the Lightship Security USA Common Criteria Laboratory (CCTL) in Baltimore, MD, United States of America, and was completed in April 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Lightship Security (LS). The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the *PP-Configuration for Network Devices and Wireless Local Area Network Access Systems, 2022-04-21*, Version 1.0, (CFG_ND_WLAN-AS_V1.0) which includes the Base PP: *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 (NDcPP22e) with the *PP-Module for Wireless Local Area Network (WLAN) Access* System, Version 1.0, 31 March 2022 (WLANAS10).

The Target of Evaluation (TOE) is the Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12.

The Target of Evaluation (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). 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 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, 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 of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, 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 technical information included in this report was obtained from the *Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 Security Target*, Version 1.2, April 6, 2025 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) 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 Validated Products 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 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	Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 (Specific models identified in Section 8)
Protection Profile	*PP-Configuration for Network Devices and Wireless Local Area Network Access Systems, 2022-04-21,* Version 1.0, (CFG_ND_WLAN-AS_V1.0) which includes the Base PP: *collaborative Protection Profile for Network* Devices, Version 2.2e, 23 March 2020 (NDcPP22e) with the *PP-Module for Wireless Local Area Network (WLAN) Access System*, Version 1.0, 31 March 2022 (WLANAS10)
ST	*Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 Security Target*, Version 1.2, April 6, 2025
Evaluation Technical Report	*Evaluation Technical Report for Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12*, Version 1.2, April 2025
CC Version	*Common Criteria for Information Technology Security Evaluation*, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor and Developer	Cisco Systems, Inc.

Item	Identifier
Common Criteria Testing Lab (CCTL)	Lightship Security USA, Inc. 3600 O'Donnell St., Suite 2 Baltimore, MD 21224
CCEVS Validators	The MITRE Corporation

3 Architectural Information

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

The Cisco Catalyst 9800 Series combines Wireless LAN Controllers and Access Points to create a WLAN Access System TOE. For wireless clients, the TOE provides secure over-the-air access to an organization's network. For administrators, the TOE provides central management and administration of the wireless infrastructure within an organization.

3.1 TOE Description

The Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 Target of Evaluation (TOE) provides wireless clients access to resources on an organization's network.

The TOE is comprised of two distinct components:

1. The Access Point (AP) operates at the edge of an organization's network. The AP contains 2.4, 5, and 6 GHz wireless radios and implements functions from the IEEE 802.11 standard to communicate over-the-air directly to wireless client radios. This communication includes advertising its presence (known as beacons), responding to requests for available networks (probes), performing 802.11 authentication, association, encryption/decryption, and session management.
2. The Wireless LAN Controller (WLC) is responsible for ensuring wireless clients are authenticated and keys are derived in accordance to the IEEE 802.11 standard.

The TOE uses IEEE 802.1X to ensure Supplicants are authenticated prior to allowing wireless client traffic onto the organization's wired network. Encryption keys for wireless sessions are derived using AES-CCMP for encryption and message integrity with cryptographic key size of 128 bits in accordance with the IEEE 802.11-2020 standard. AES-CCMP-128 bit encryption as specified in 802.11-2020 is more commonly known by its Wi-Fi Alliance certification name, WPA3-Enterprise.

Additionally, the TOE derives wireless encryption keys using AES-CCMP with cryptographic key size of 256 bits and AES-GCMP, with cryptographic key size of 128 and 256 bits in accordance with the IEEE 802.11ax-2021 specification.

The WLC is responsible for all management of the APs. Once an AP has registered with the WLC, an internal channel is formed for the purposes of centralized management and configuration of the APs. No local administration is available directly on the APs. The internal channel also protects the distribution of IEEE keys between the WLC and AP.

For connections to the Syslog audit server, the WLC authenticates those devices with X.509v3 certificates and protects communication channels with the IPsec protocol. For RADIUS, the WLC protects communication to the RADIUS authentication server with RADsec. Secure remote administration is protected with HTTPS and SSH which is implemented with authentication failure handling.

3.2 TOE Evaluated Platforms

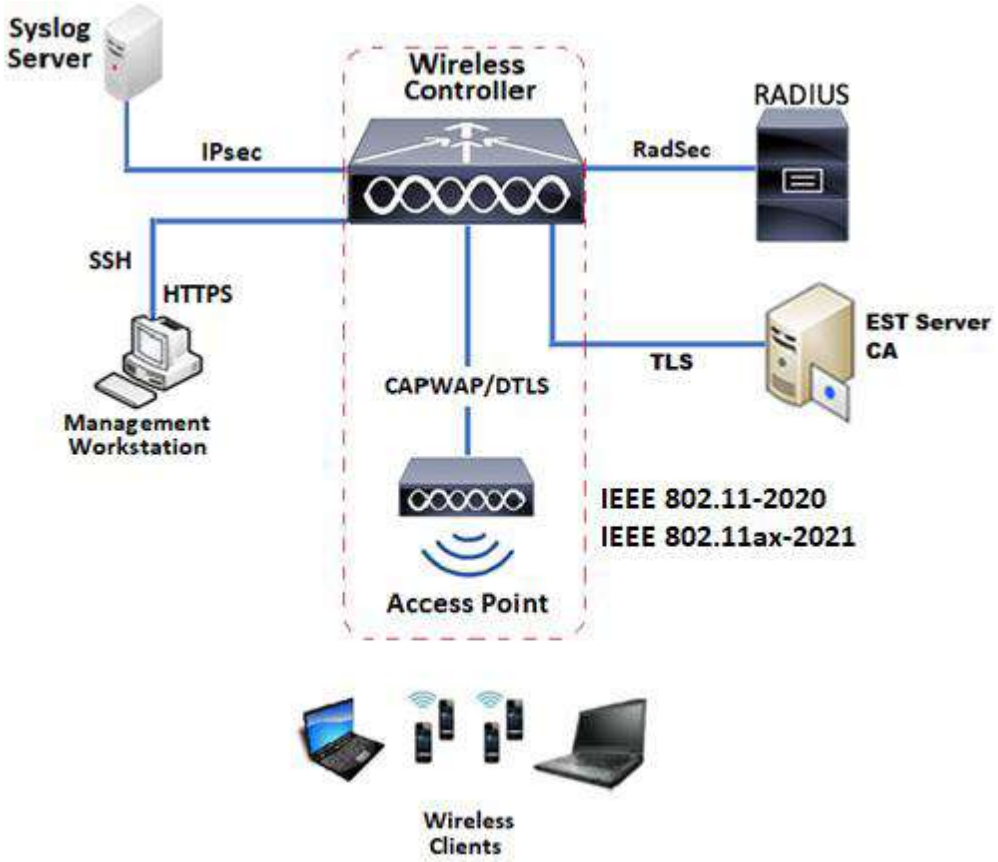
Detail regarding the evaluated configuration is provided in Section 8 below.

3.3 TOE Architecture

The Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 TOE is distributed. Deployment of the TOE in its evaluated configuration consists of one Wireless LAN Controller (WLC) model and at least one Access Point (AP). Extra instances of a WLC or AP TOE component are permitted in the evaluated configuration. The evaluated configuration of Cisco Catalyst 9800-CL (vSphere) follows vND evaluated configuration Case 1 in [NDcPP] where a virtual Network Device (vND) runs inside a virtual machine (VM) on purpose-built hardware.

3.4 Physical Boundaries

The TOE physical boundary is the WLC and AP components as denoted by hashed red lines in the figure below.



The WLC can be administered interactively using a local console connection (CLI), or remotely over HTTPS (GUI) or SSH (CLI). Once the APs have registered with a Controller and 'joined' to form the TOE, the APs are entirely managed via the WLC. The TOE does not permit direct local administration of the APs thus fulfilling distributed TOE use case 1 in section 3.1 of [NDcPP].

The operational environment of the TOE will include at least one RADIUS server for authentication of wireless clients. The RADIUS Authentication Server and wireless client (Supplicant) must authenticate each other with EAP-TLS which requires use of X.509 certificates provided by the CA server. The operational environment requires a CA server to provide the TOE, Authentication Server, and Wireless clients with valid X.509 certificates. The environment will also include an audit (syslog) server and a Management Workstation.

The TOE supports two modes of operation, Local mode and Flex Connect mode. In Local mode, the Access Point processes layer 2 wireless frames which are tunneled to the Controller over an internal channel protected with DTLS. In Local mode the WLC is the single point of ingress and egress for both management (TSF data) and user data traffic. When user data traffic reaches the WLC, it is mapped to a corresponding interface (VLAN) or interface group (VLAN pool) defined as part of the WLAN configuration settings on the WLC.

Flex Connect mode is similar to Local mode in that the AP handles functions from the 802.11 specification. The difference with Flex Connect is it allows an option for user data to be distributed at the egress (wired) port of the AP as IEEE 802.3 Ethernet traffic. This mode allows authenticated wireless clients access to resources local to the AP which is particularly useful in small remote and branch offices across WAN links where only a handful of access points are needed. In Flex Connect mode, the WLC is the point of ingress and egress for management traffic (TSF data) only.

Regardless of either mode it may operate in, the AP is always centrally managed by the WLC and management traffic (TSF data) is secured in an internal channel protected with DTLS. Wireless clients are authenticated by a centralized authentication server when the TOE operates in either Local or Flex Connect mode.

4 Security Policy

This section summarizes the security functionality of the TOE:

1. Security audit
2. Communication
3. Cryptographic support
4. Identification and authentication
5. Security management
6. Protection of the TSF
7. TOE access
8. Trusted path/channels

4.1 Security audit

Auditing allows Security Administrators to discover intentional and unintentional issues with the TOE's configuration and/or operation. Auditing of administrative activities provides information that may be used to hasten corrective action should the system be configured incorrectly. Security audit data can also provide an indication of failure of critical portions of the TOE (e.g. a communication channel failure or anomalous activity (e.g. establishment of an administrative session at a suspicious time, repeated failures to establish sessions or authenticate to the TOE) of a suspicious nature.

The TOE provides extensive capabilities to generate audit data targeted at detecting such activity. The TOE generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. The AP transmits its audit messages to the WLC where they are stored along with the WLC's own audit messages in a circular audit trail configurable by the Security Administrator. All audit logs are transmitted to an external audit server over a trusted channel protected with IPsec.

4.2 Communication

The TOE provides a secure internal channel, under control of the Security Administrator, for Access Points to register and join the WLC to form a distributed TOE.

4.3 Cryptographic support

The TOE provides cryptographic functions in order to implement HTTPS, DTLS, SSH, IPsec, WPA2, and IEEE 802.11ax-2021 protocols. The cryptographic algorithm implementation has been validated for CAVP conformance. This includes key generation and random bit generation, key establishment methods, key destruction, and the various types of cryptographic operations to provide AES encryption/decryption, signature verification, hash generation, and keyed hash generation. All cryptography is implemented using the IOS Common Cryptographic Module (IC2M) Rel5a and CiscoSSL FOM 7.3 cryptographic modules. IC2M Rel5a applies to the WLC and CiscoSSL FOM 7.3 applies to the WLC and the AP. SSH and IPsec protocols are implemented using the IOS Common Cryptographic Module (IC2M) and TLS and DTLS protocols are implemented using the CiscoSSL FOM cryptographic modules. Refer to Table 22 in the ST for identification of the relevant CAVP certificates.

In addition, the IEEE 802.11 implementation has been validated by the Wi-Fi Alliance for WPA2 certification. Refer to Table 23 in the ST for identification of the relevant Wi-Fi Alliance certificates.

4.4 Identification and authentication

The TOE facilitates authentication of wireless clients by performing the role of Authenticator in an 802.1X authentication exchange.

During the 802.1X authentication exchange, the wireless client software responsible for authentication (hereinafter referred to as a Supplicant) is relayed through the WLC. The 802.1X frames carry EAP authentication packets which are passed through to the RADIUS Authentication Server. The TOE creates a virtual port for each wireless client that is attempting access and blocks access until the RADIUS server returns an authentication success message and 802.11 wireless encryption keys are derived and installed on both the Supplicant and AP. After that point 802.11 wireless data frames from the wireless client are allowed to pass as 802.3 Ethernet frames on the network.

The TOE provides two types of authentication to provide a trusted means for Security Administrators and remote endpoints to interact with a WLAN Access System: X.509v3 certificate-based authentication for remote devices and password-based authentication for Security Administrators. Device-level authentication allows the TOE to establish a secure communication channel with remote endpoints.

Security Administrators have the ability to compose strong passwords (between 8 and 16 characters) which are stored in an obscured form. Additionally, the TOE detects and tracks successive unsuccessful remote authentication attempts and will prevent the offending account from making further attempts until a Security Administrator time period has elapsed or until the Administrator manually unblocks the account.

4.5 Security management

The TOE provides secure remote administrative interface and local interface to perform security management functions. This includes ability to configure cryptographic functionality; an access banner containing an advisory notice and consent warning message; a session inactivity timer before session termination as well as an ability to update TOE software.

The APs are managed via the WLC. Direct local administration of the APs is not supported.

The TOE provides a Security Administrator role and only the Security Administrator can perform the above security management functions. The TOE prevents attempts to perform remote administration from a wireless client.

4.6 Protection of the TSF

The TOE protects critical security data including keys and passwords against tampering by untrusted subjects. The TOE provides reliable timestamps to support monitoring local and remote interactive administrative sessions for inactivity, validating X.509 certificates (to determine if a certificate has expired), denying session establishment of wireless clients (based on time), and to support accurate audit records.

The TOE provides self-tests to ensure it is operating correctly, including the ability to detect software integrity failures. Additionally, the TOE provides an ability to perform software updates and to verify those software updates are from Cisco Systems, Inc.

4.7 TOE access

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

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

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

4.8 Trusted path/channels

The TOE provides encryption (protection from disclosure and detection of modification) for communication channels/paths between itself and remote endpoints and TOE administrators. Specifically, the TOE allows a trusted path to be established to itself from the remote authorized administrator over SSH and TLS/HTTPS. The TOE also initiates an outbound IPsec trusted channel to transmit audit messages to a remote syslog server.

In addition, the TOE provides two-way authentication of each endpoint in a cryptographically secure manner, meaning that even if there was a malicious attacker between the two endpoints, any attempt to represent themselves to either endpoint of the communications path as the other communicating party would be detected.

5 Assumptions & Clarification of Scope

Assumptions

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

- *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 (NDcPP22e)
- *PP-Module for Wireless Local Area Network (WLAN) Access System*, Version 1.0, 31 March 2022 (WLANAS10)

That information has not been reproduced here and the NDcPP22e/WLANAS10 should be consulted if there is interest in that material.

Clarification of scope

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP22e/WLANAS10 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 devices 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 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 assurance activities specified in the collaborative Protection Profile for Network Devices and the Wireless LAN Module and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide, additional customer documentation for the specific Wireless LAN models was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.
- 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 functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP22e/WLANAS10 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following documents were available with the TOE for evaluation:

- *Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 CC Configuration Guide*, Version 0.9, April 6, 2025

Any additional customer documentation provided with the product, or that is available online, was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating 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 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary *Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 NDcPPv2.2E + MOD_WLAN_ASv1.0 Detailed Test Report*, Version 1.2, April 9, 2025 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

7.1 Developer Testing

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

7.2 Evaluation Team Independent Testing

The evaluation team conducted independent testing from November 2024 through April 2025. Testing was performed in the Lightship Ottawa (Canada) facility that has been accredited by the Standards Council of Canada. The TOE and test setup were physically and logically protected from unauthorized access, and the TOE was configured according to vendor installation instructions and as identified in the Security Target.

Testing within the Lightship lab in Canada was pre-approved by NIAP. The Lightship lab in Ottawa, Canada is an ISO-17025 accredited facility. It has access control to all areas containing systems under test and only authorized personnel are permitted access to the test space.

The evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the NDcPP22e/WLANAS10 including the tests associated with optional requirements. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here.

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The TOE components are Wireless LAN Controllers and Access Points and each is composed of hardware and software. When components are joined, the TOE forms a Wireless LAN Access System.

The TOE is comprised of the following models:

Hardware Configuration	Software Version
9166 Series Wi-Fi 6/6E AP 9164I Series Wi-Fi 6/6E AP 9162I Series Wi-Fi 6/6E AP 9136I Series AP 9130AX Series Wi-Fi 6/6E AP 9124AX Series AP IW9167 Heavy Duty AP	IOS-XE 17.12.04 (embedded in WLC)
9800-80 WLC	C9800-80: IOS-XE 17.12.04
9800-40 WLC	C9800-40: IOS-XE 17.12.04
9800-L WLC	C9800-L: IOS-XE 17.12.04
9800-CL WLC running on ESXi 6.7 on the Unified Computing System (UCS) USCS-C220-M5, UCSC-C240-M5, UCSC-C480-M5	C9800-CL: IOS-XE 17.12.04

8.2 Excluded Functionality

The following functionality is excluded from the evaluation.

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 and CC mode of operation	The TOE includes FIPS and CC modes of operation. The FIPS modes allows the TOE to use only approved cryptography and CC mode removes the ability to use non-PFS ciphersuites for DTLS. FIPS and CC modes of operation must be enabled in order for the TOE to be operating in its evaluated configuration.
WPA and WPA2 with TKIP encryption	Only WPA2/3-Enterprise along with 802.1X with AES encryption will meet the requirements of the PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0 (MOD_WLAN_AS_V1.0).
Cisco Catalyst 9800-CL for public cloud	The Cisco Catalyst 9800-CL for public cloud is an Infrastructure-as-a-Service (IaaS) solution available on the Amazon Web Services (AWS) and Google Cloud Platform (GCP) Marketplace. The Cisco Catalyst

Excluded Functionality	Exclusion Rationale
	9800-CL for public cloud solution is excluded from the evaluation.
Cisco CleanAir	Cisco CleanAir is a spectrum intelligence solution designed to proactively manage the challenges of a shared wireless spectrum.

Additionally, the TOE includes a number of functions where there are no Security Functional Requirements that apply from the collaborative Protection Profile for Network Devices v2.2e or the PP-Module for Wireless Local Area Network (WLAN) Access System Version 1.0. The excluded functionality does not affect the TOE's conformance to the claimed Protection Profiles.

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. The reader of this document can assume that all assurance 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 Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e/WLANAS10.

9.1 Evaluation of the Security Target (ASE)

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 Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

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 that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each 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 Security Target and Guidance documents. Additionally, the evaluation team performed the assurance activities specified in the NDcPP22e/WLANAS10 related to the examination of the information contained in the TSS.

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 that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each 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. All of the 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 that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

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

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 that the conclusion reached by the evaluation team was justified.

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

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the NDcPP22e/WLANAS10 and recorded the results in a Test Report, summarized in the AAR.

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 that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluation team searched the following sources:

- National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search)
- MITRE CVE List (https://cve.mitre.org/cve/search_cve_list.html),
- CVE Details (https://www.cvedetails.com/vulnerability-search.php)
- CISA - Known Exploited Vulnerabilities Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog)
- Cisco Security Advisories (https://sec.cloudapps.cisco.com/security/center/publicationListing.x)
- Cisco Security Software Checker for IOS-XE 17.12.04 (https://sec.cloudapps.cisco.com/security/center/softwarechecker.x?productSelected=ios_xe&selectedMethod=A&captchaPage=true&platformCode=NA&versionNam

esSelected=17.12.04&allAdvisoriesSelectedByTree=N&advisoryType=0&iosBundleId=cisco-sa-20240925-bundle&isFewCheckBoxChecked1=false&isNoneCheckBoxsChecked1=true#~onStep3)

The searches were performed on April 6, 2025 with the following search terms:

Cisco IOS-XE 17.12
Wireless LAN Controller
Lightweight AP software 17.12
Intel Xeon Silver 4116T
Intel Xeon Broadwell D-1548
Intel Xeon Broadwell D-1563N
Intel Xeon Skylake SP
Qualcomm IPQ8076 ARMv8
Qualcomm IPQ6010 ARMv8
Qualcomm IPQ8078 ARMv8
Cisco Catalyst 9800-80 Wireless Controller
Cisco Catalyst 9800-40 Wireless Controller
Cisco Catalyst 9800-L Wireless Controller
Cisco Catalyst 9800-CL Wireless Controller
Access Points (As identified in [ST] Section 1.7)
ACT2Lite
SmartFusion2
OpenSSH
OpenResty
DNSmasq
OpenSSL
CiscoSSL
IC2M Rel5a
CiscoSSH
VMWare ESXi 6.7

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 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 testing 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 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 instructions in the *Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 CC Configuration Guide*, Version 0.9, April 6, 2025. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST, and the only evaluated functionality was that which was described by the SFRs claimed in the ST. 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. It is important to note the excluded functionality listed in Section 8.2 and follow the configuration instructions to ensure that this functionality is disabled. In addition, it is important to apply all updates and patches, particularly for ESXi 6.7 if using the 9800-CL WCL.

Evaluation activities are strictly bound by the assurance activities described in the NDcPP22e/WLANASS10 and accompanying Supporting Documents. Consumers and integrators of this TOE are advised to understand the inherent limitations of these activities and take additional measures as needed to ensure proper TOE behavior when integrated into an operational environment.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 Security Target*, Version 1.2, April 6, 2025.

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 VR:

[1] *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model,* Version 3.1, Revision 5, April 2017.

[2] *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components*, Version 3.1, Revision 5, April 2017.

[3] *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components*, Version 3.1 Revision 5, April 2017.

[4] *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 (NDcPP22e).

[5] *PP-Module for Wireless Local Area Network (WLAN) Access System),*Version 1.0, 31 March 2022 (WLANAS10).

[6] *Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 Security Target*, Version 1.2, April 6, 2025 (ST).

[7] *Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 Assurance Activity Report*, Version 1.2, April 9, 2025 (AAR).

[8] *Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 NDcPPv2.2E + MOD_WLAN_ASv1.0 Detailed Test Report*, Version 1.2, April 9, 2025 (DTR).

[9] *Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 Detailed Test Report Evidence WLC-40*, Version 1.1, April 6, 2025 (DTRE1*).*

[10] *Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 Detailed Test Report Evidence WLC-CL*, Version 1.1, April 6, 2025 (DTRE2).

[11] *Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 Evaluation Technical Report*, Version 1.2, April 2025 (ETR).

[12] *Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 Vulnerability Assessment*, Version 1.1, April 6, 2025 (VA).

[13] *Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 CC Configuration Guide*, Version 0.9, April 6, 2025 (AGD).