Certification Report

H3C Wireless Controllers and Access Points

version:
TOE hardware: H3C WX5800 Series, WX2800 Series, WSG1800 Series, WX3800 Series Wireless Controllers and WA6500 Series, WA7200 Series, WA7300 Series, WA7500 Series, WA7600 Series, CPE Series Access Points
TOE firmware: H3C Comware Software, Version 7.1, H3C Comware Software, Version 9.1

Sponsor and developer:	***New H3C Technologies Co Ltd*** **NO 466 CHANGHE ROAD** **HANGZHOU, Zhejiang 310052** **China**
Evaluation facility:	***Keysight Technologies Netherlands Riscure B.V.*** **Delftechpark 49** **2628 XJ Delft** **The Netherlands**
Report number:	**NSCIB-CC-2500009-01-CR**
Report version:	**1**
Project number:	NSCIB-**2500009-01**
Author(s):	**Wim Ton**
Date:	**23 October 2025**
Number of pages:	**13**
Number of appendices:	**0**

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TrustCB B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TrustCB B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TrustCB B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TrustCB B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Recognition of the Certificate

Presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the H3C Wireless Controllers and Access Points. The developer of the H3C Wireless Controllers and Access Points is New H3C Technologies Co Ltd located in Hangzou, China and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE combines Wireless Access Controllers and Access Points to create a Wireless LAN Access System. The TOE provides secure wireless access to a wired and wireless network. The Wireless Access Controller is used to manage the Access Points over a secure connection. The TOE is a distributed network device consisting of one wireless Access Controller (AC) and at least one Access Point (AP) The Wireless Access Controller can connect to external NTP and Syslog servers over a secure connection, or these functions can be performed with the TOE`s local interfaces.

The TOE has been evaluated by Keysight Technologies Netherlands Riscure B.V located in Delft, The Netherlands. The evaluation was completed on 23 October 2025 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the H3C Wireless Controllers and Access Points, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the H3C Wireless Controllers and Access Points are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL2 augmented (EAL2+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.2 (Flaw remediation).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation 2022 R 1 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation 2022, R1 *[CC]* (Parts 1,2,3,4,and 5).

TrustCB B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the H3C Wireless Controllers and Access Points from New H3C Technologies Co Ltd located in Hangzou, China.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	Wireless controller	WX5800
		WX2800
		WX3800
		WGS1800
	Access point	WA6500
		WA7200
		WA7300
		WA7500
		WA7600
Software	H3C Comware	7.1.064 Release 2617P50
		7.1.064 Release 5817P50
		9.1.061 ESS 1404P50

To ensure secure usage a set of guidance documents is provided, together with the H3C Wireless Controllers and Access Points. For details, see section 2.5 “Documentation” of this report and Table 5 in the *[ST].*

2.2 Security Policy

Security audit

Security relevant events are stored on the TOE, and a copy can be sent regularly to an external Syslog server

Cryptographic support

AES

RSA and ECDSA signatures

RSA and ECDH key management

HMAC keyed hash

Key generation for the above algorithms

SHA-2 hashing

Deterministic Random Bit Generator

X509 certificate support

Security management

Role based access control

Identification and authentication

Time from a built-in clock or from an external NTP server

Protection of the TSF

Secure software updates

Self-tests of the software integrity and the cryptographic functionality.

Protected key storage

Trusted path/channels and secure communication.

The TOE uses IPsec to secure the connections to the NTP and to the Syslog server

The TOE uses (D)TLS to secure the connection between controller and access point

The TOE's controller uses SSH to secure the connection to the external management console

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

2.3.2 Clarification of scope

The evaluated configuration is: "FIPS mode" on, and no external authentication server.

Both manual time setting and NTP synchronisation are evaluated. Manual time setting is a prerequisite for the secure connections as the time is needed for certificate validation.

The optional Syslog server is part of the evaluated configuration.

2.4 Architectural Information

The TOE provides wireless access to a network.

The AP (Access Point) is connected to the AC (Access Controller) via an IP wired Ethernet network or wired directly to the AC.

The management and control traffic between AP and AC is protected using DTLS and TLS.

For its management, the TOE can be accessed via a network (protected with SSH) of locally via a serial connection.

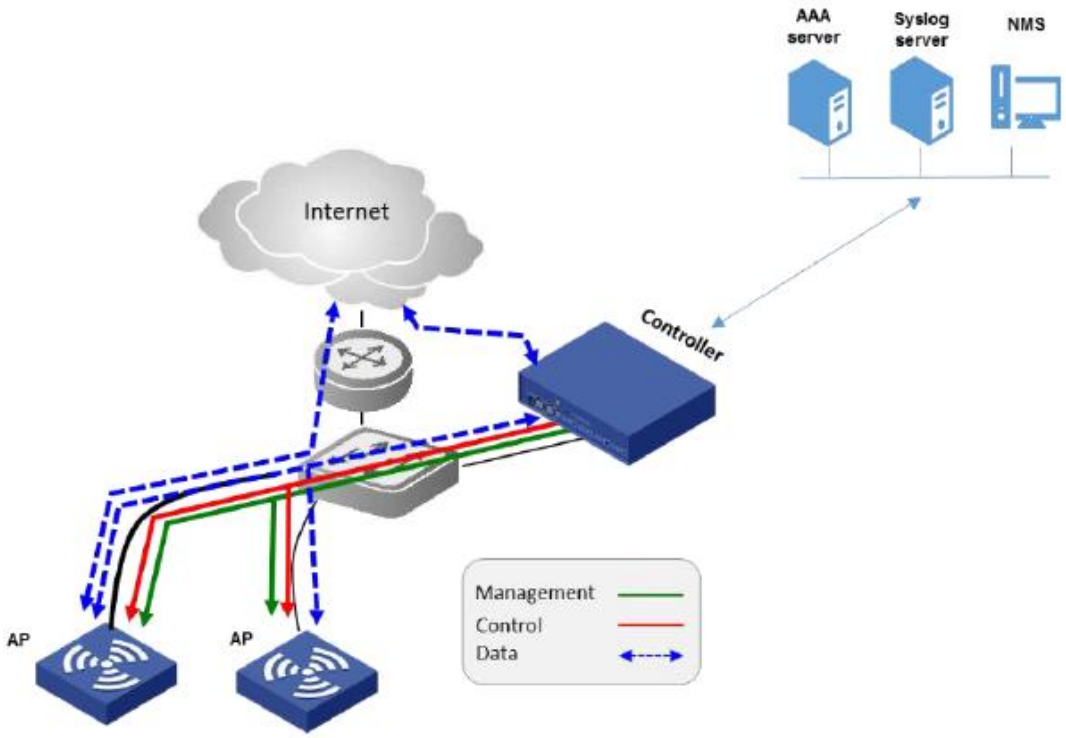

Figure 1 TOE usage

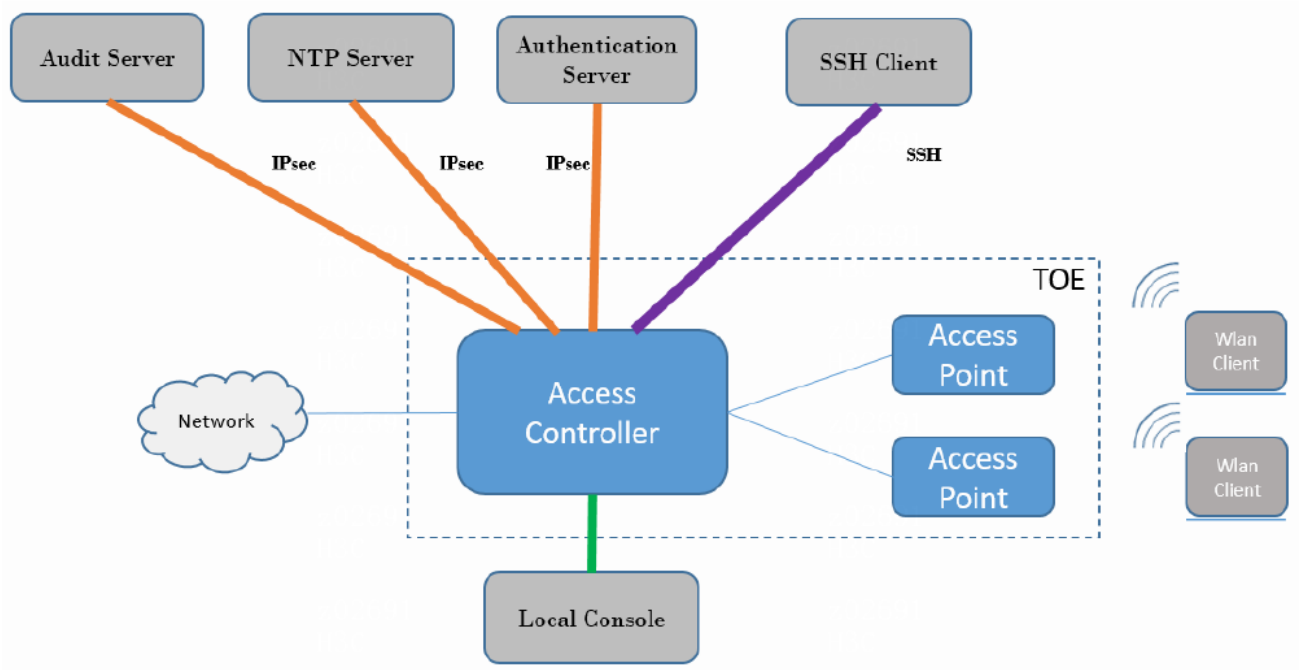

Figure 2 The TOE with external components

The security relevant hardware for the TOE variants is the same, the differences are in the processor speed, memory, and the network interfaces (which are out of scope).

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
Access Controllers Installation Guide	See table 5 in the [ST], as every device in 2.1 has its own set of manuals.
Access Controllers Command References	
Access Controllers Configuration Guides	
Wireless Integrated Services Gateway Installation Guide	
H3C Access Controllers System Log Messages Reference(E80xx_R56xx)-6W101-book.pdf	6W101
H3C Wireless Products Troubleshooting Guide-6W101-book.pdf	6W101
Preparative and Operative Procedures	2.9

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer has elaborated exhaustive test campaign covering different parts of the TOE and their functionalities. These testing efforts have given the evaluator enough assurance that the TOE behaves as desired. Due to this reason, the approach of the independent tests was as following:

The evaluator has conducted 16 witnessing sessions performing a representative coverage of the different TOE subcomponents. The tests were executed on 2 software versions, 9.1.061 ESS 1404P50 and 7.1.064 Release 5817P50.

The evaluator has conducted extra tests to confirm that the NTP and the Syslog server can only communicate with the TOE over a secure connection.

2.6.2 Independent penetration testing

Besides a port scan, the evaluator has tested the SSH interface for command injection and the CLI interface with fuzzing.

The total test effort expended by the evaluators was 2.4 weeks. During that test campaign, 0% of the total time was spent on Perturbation attacks, 0% on side-channel testing, and 100% on logical tests.

2.6.3 Test configuration

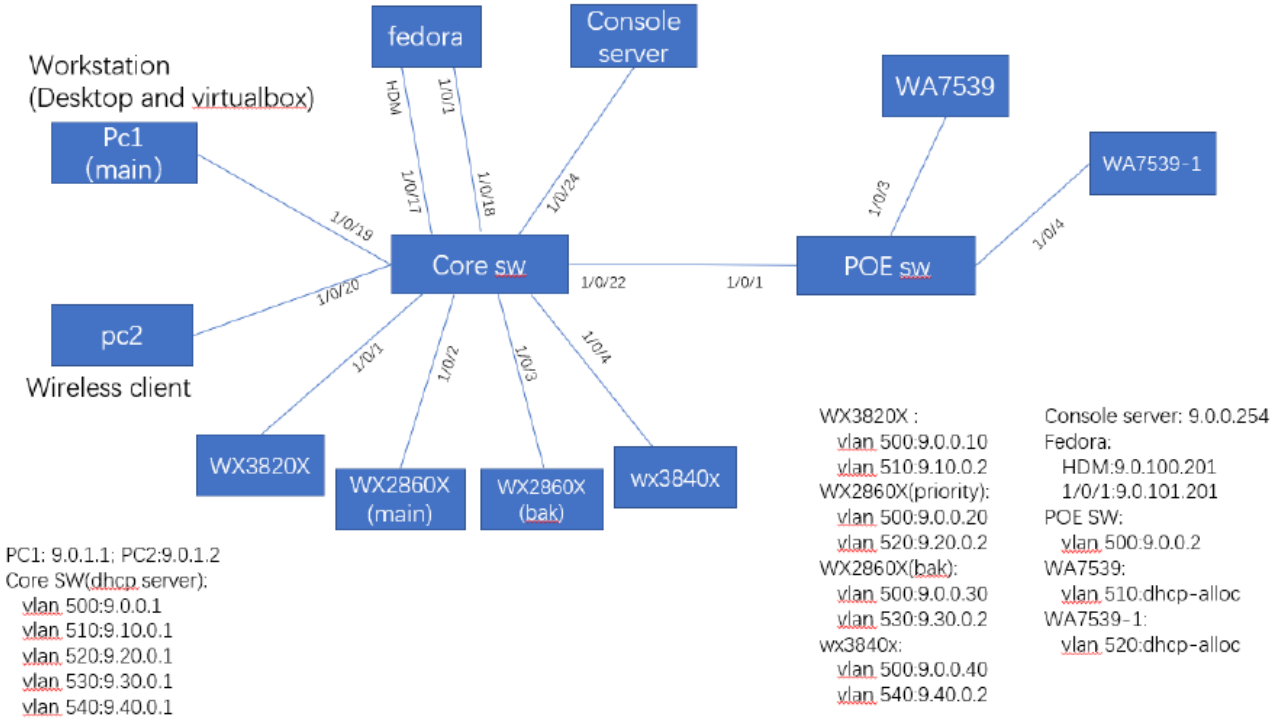

Figure 3 Test configuration

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

2.7 Reused Evaluation Results

There is no reuse of evaluation results in this certification.

No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number H3C Wireless Controllers and Access Points. The user can verify the TOE version with the commands: "display fips status", "display version" and "display wlan ap-model all".

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the H3C Wireless Controllers and Access Points, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of

EAL 2 augmented with ALC_FLR.2. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims conformance to the following functional package: Functional Package for SSH Version 1.0 [PPSSH]

The Security Target closely follows the Protection Profile *[PP]* with the WLAN module *[EPWLAN]* and configuration *[PP-CONFIG]*, but does not claim conformance to it.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 “Documentation” contains necessary information about the usage of the TOE. Certain aspects of the TOE’s security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: <**none**>, which are out of scope as there are no security claims relating to these.

3 Security Target

The H3C WX5800 Series, WX2800 Series, WSG1800 Series, WA6500 Series, WA7200 Series, WA7300 Series, WA7500Series, WA7600 Series, CPE Series, and WX3800 Series Wireless Controllers and Access Points Security Target, v4.4, 21 October 2025 *[ST]* is included here by reference.

Please note that, to satisfy the need for publication, a public version *[ST-lite]* has been created and verified according to *[ST-SAN]*.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
TOE	Target of Evaluation
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining (a block cipher mode of operation)
CLI	Command Line Interface
ECB	Electronic Code Book (a block-cipher mode of operation)
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
HMAC	Hash based Message Authentication Code
IPsec	IP security (RFC4301)
LAN	Local Area Network
MAC	Message Authentication Code
MITM	Man-in-the-Middle
NTP	Network Time Protocol
PACE	Password Authenticated Connection Establishment
PKI	Public Key Infrastructure
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TRNG	True Random Number Generator
VLAN	Virtual LAN

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation CC:2022, Parts I, II and III, R1, November 2022
[CEM]	Common Methodology for Information Technology Security Evaluation CC:2022, R1, November 2022
[ETR]	H3C WX5800 Series, WX2800 Series, WSG1800 Series, WA6500 Series, WA7200 Series, WA7300 Series, WA7500Series, WA7600 Series, CPE Series, and WX3800 Series Wireless Controllers and Access Points Evaluation Technical Report, OPP01233108D3, v1.1, 23 October 2025
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[PP]	Collaborative Protection Profile for Network Devices, v3.0e, 06 December 2023.
[PPSSH]	Functional Package for Secure Shell (SSH), v1.0, 13 May 2021.
[EPWLAN]]	PP-Module for Wireless Local Area Network (WLAN) Access System, v1.0, 31 March 2022.
[PP-CONFIG]	PP-Configuration for Network Devices and Wireless Local Area Network Access Systems, v1.0, 31 March 2024.
[ST]	H3C WX5800 Series, WX2800 Series, WSG1800 Series, WA6500 Series, WA7200 Series, WA7300 Series, WA7500Series, WA7600 Series, CPE Series, and WX3800 Series Wireless Controllers and Access Points Security Target, v4.4, 21 October 2025
[ST-lite]	H3C WX5800 Series, WX2800 Series, WSG1800 Series, WA6500 Series, WA7200 Series, WA7300 Series, WA7500Series, WA7600 Series, CPE Series, and WX3800 Series Wireless Controllers and Access Points Security Target, Version: 4.4, 22 October 2025
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)