H3C WX5800 Series, WX2800 Series, WA6500 Series, WA7200 Series, WA7300 Series, WA7500 Series, WA7600 Series and WX3800 Series Wireless Controllers and Access Points

Security Target Lite

Version: 3.4

Date: 2026-06-05

H3C

Document history

Version	Date	Comment	Author
0.1	2024-08-19	Initial version	H3C
0.2	2024-09-11	Updated Protection Profile and Common Criteria versions	Digital Cubes
0.3	2025-01-22	Updated FCS_TLSC_EXT.1 FCS_DTLSC_EXT.1	Digital Cubes
0.4	2025-03-03	Updated to comply with CC:2022 Transition Policy	Digital Cubes
0.5	2025-04-15	Updated TSS	H3C
0.6	2025-05-15	Updated 9.2	H3C
0.7	2025-05-21	Updated FIA_X509_EXT.1.1/ITT and 1.4.1	H3C
0.8	2025-06-09	Updated according to comments	H3C
0.9	2025-06-19	Updated FCS_DTLSC_EXT.1.9 and FCS_TLSC_EXT.1.9	H3C
1.0	2025-06-27	Updated according to comments	H3C
1.1	2025-07-03	Updated according to comments	H3C
1.2	2025-07-11	Modified section 8.5	H3C
1.3	2025-08-06	Updated according to comments	H3C
1.4	2025-08-22	Updated according to comments	H3C
1.5	2025-08-22	Modified section 1.2	H3C
1.6	2025-09-02	Updated according to comments	H3C
1.7	2025-09-03	Updated according to comments	H3C
1.8	2025-09-17	Updated according to comments	H3C
1.9	2025-09-30	Updated according to comments	H3C
2.0	2025-10-14	Modified section 1.4.1& 8.2	H3C
2.1	2025-11-06	Modified section 2.1	H3C
2.2	2025-11-26	Update FW version information	H3C
2.3	2025-12-01	Correct the error	H3C
2.4	2026-02-04	Update SFRs information	H3C
2.5	2026-02-10	Correct the error	H3C
2.6	2026-02-23	Correct the error	H3C
2.7	2026-02-24	Correct the error	H3C
2.8	2026-03-24	Supplement and improve information	H3C
2.9	2026-03-26	Correct the error & add SFR FIA_PSK_EXT.1	H3C
3.0	2026-04-16	Correct the error	H3C
3.1	2026-04-22	Correct the error	H3C
3.2	2026-04-24	Correct the error	H3C
3.3	2026-05-06	Correct the error	H3C
3.4	2026-06-05	Correct the error	H3C

Contents

1 Security Target Introduction

The ST describes what is evaluated, including the exact security properties of the TOE in a manner that the potential consumer can rely on.

1.1 Security Target Reference

Title	H3C WX5800 Series, WX2800 Series, WA6500 Series, WA7200 Series, WA7300 Series, WA7500 Series, WA7600 Series and WX3800 Series Wireless Controllers and Access Points Security Target
Version	See Document History
Date	See Document History
Author	New H3C Technologies Co., Ltd

Table 1 Security Target reference

1.2 TOE Reference

TOE Developer	New H3C Technologies Co., Ltd
TOE Name	H3C Wireless Controllers and Access Points
TOE Version	TOE hardware: H3C WX5800 Series, WX2800 Series, WX3800 Series Wireless Controllers and WA6500 Series, WA7200 Series, WA7300 Series, WA7500 Series, WA7600 Series Access Points TOE firmware: H3C Comware Software, Version 7.1.064, Release 5484P23; H3C Comware Software, Version 7.1.064, Release 5817P33; H3C Comware Software, Version 9.1.061, ESS 1404P23; H3C Comware Software, Version 7.1.064, Release 2617P33;

Table 2 TOE reference

1.3 TOE Overview

The TOE combines Wireless Access Controllers and Access Points developed by H3C to create a Wireless LAN Access System TOE. The TOE provide secure wireless access to a wired and wireless network and will hereafter be referred to as the TOE throughout this document

A typical Wireless LAN access system is showed in figure 1:

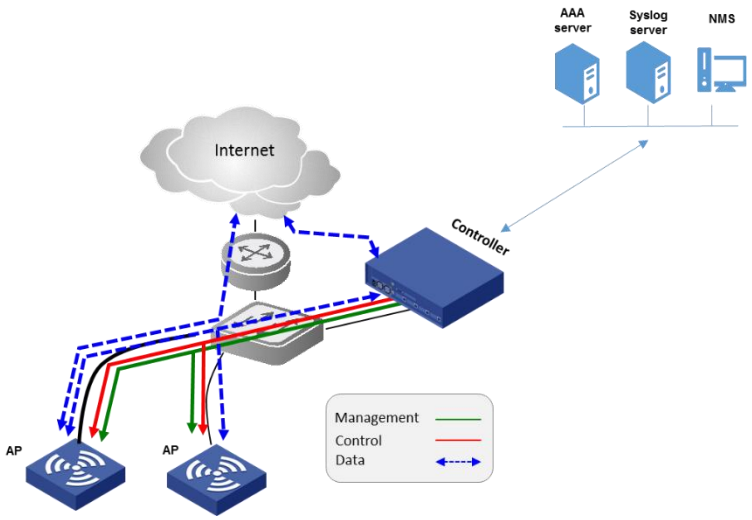


Figure 1 TOE usage scenario.

The wireless Access Controllers (ACs) are wireless switch appliances that provide a wide range of security services and features including wireless network mobility, security, centralized management, auditing, authentication, and remote access. The access point (AP) appliances service wlan clients.

1.3.1 TOE Type

The TOE is a distributed network device consisting in a one wireless Access Controller (AC) and minimum one Access Point (AP) from Table 4.

1.3.2 TOE Usage and Major Security Features

Each TOE appliance runs Comware software and offers wireless access of network traffic. The AP is connected to the AC via wired Ethernet Local Area Network (LAN) over an IP network or wired directly to the AC. The management and control tunnel between AP and AC is protected using DTLS and TLS. The TOE appliance can also be the destination of network traffic, where it provides interfaces for its own management.

The TOE may be accessed and managed through a PC or terminal in the environment which can be remote from or directly connected to the TOE.

The TOE can be configured to forward its audit records to an external audit server in the network environment, and this audit server is connected to the TOE through an IPsec tunnel. The TOE can also be configured to work with a Network Time Server (NTP Server).

TOE supports authentication server connection through IPsec tunnel. SSH clients on PCs can also connect to TOE through encrypted channels. The Figure 1 and Figure 2 shows the TOE depicted in its intended environment.

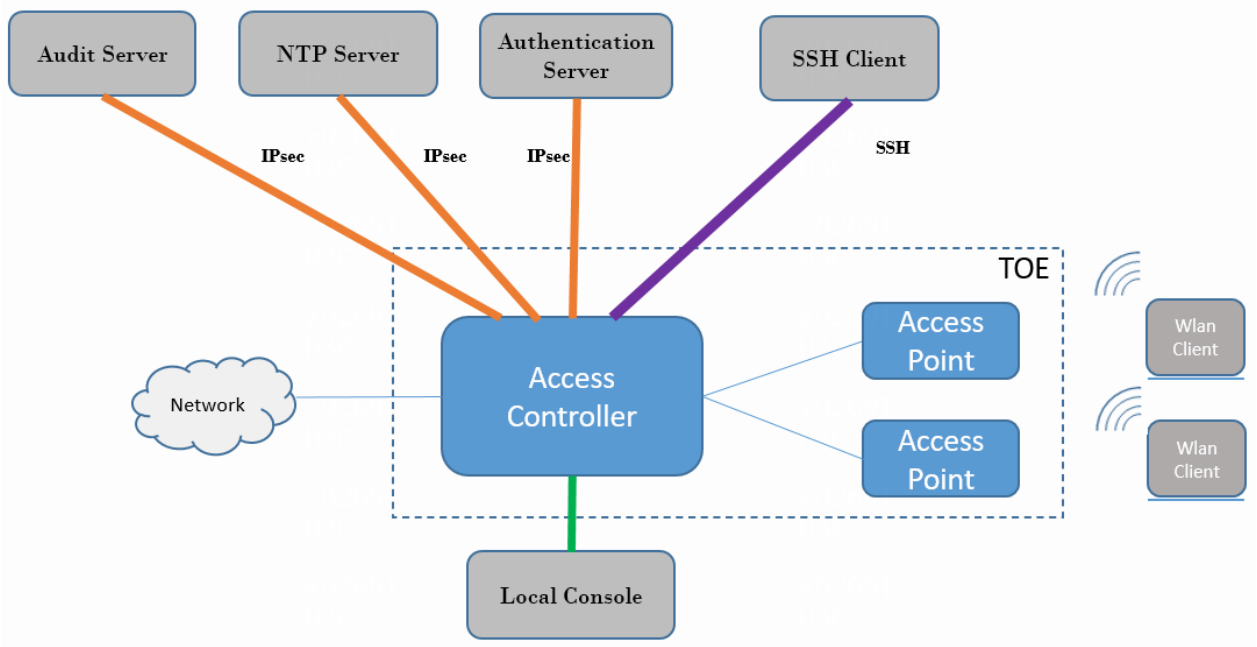


Figure 2 TOE usage scenario.

The hardware of the TOE is composed of one Access Controller, a physical network device that supports modules that serve to offer a wide range of network ports varying in number, form factor (copper or fiber), and performance; and at least one Access Point, a physical network device which provides the connection point between wlan client hosts and the wired network. The software of the TOE executes entirely within the TOE hardware.

The TOE can be configured to rely on and utilize a number of other components in its operational environment.

- Audit server – to receive audit records when the TOE is configured to deliver them to an external server.
- Authentication server – The TOE can be configured to utilize external authentication servers.
- NTP server –to keep the local hardware-based real-time clock synchronized with other network devices.
- SSH Client –SSH remote connection can access TOE.
- Local Console -- The TOE supports CLI access and as such an administrator would need a terminal emulator to utilize those administrative interfaces
- WLAN Client -- Wlan Clients are Wireless terminal devices, such as smartphones, can visit the internet via a TOE

The TOE provides the following functionality:

- Security audit
- Cryptographic support
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels.
- Communication

1.3.3 Non-TOE Hardware/Software/Firmware

Component	Required	Scope	Description
Audit Server	Mandatory	No	This includes any audit server to which the TOE would transmit audit records messages.
SSH Client	Mandatory	No	This includes any device with an SSH client installed that is used to establish a protected channel with the TOE
Local console	Mandatory	No	This includes any Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
Authentication Server	Optional	No	AAA (Authentication Authorization Accounting), implemented in accordance with related RFC, provides authentication, authorization and accounting functionalities.
NTP Server	Optional	No	The Network Time Protocol (NTP) is an application layer protocol in the TCP/IP protocol suite. NTP synchronizes the time among a set of distributed time servers and clients.
WLAN Client	Optional	No	Wlan Clients are Wireless terminal devices, such as smartphones, can visit the internet via a TOE. Wlan Client and TOE establishes an encrypted IEEE 802.11 link that encrypted IEEE 802.11 link that protects wireless data in transit from disclosure and modification.

Table 3 Components of the environment

1.4 TOE Description

1.4.1 Physical Scope

The TOE includes a total of 3 different AC series and 5 AP series:

Family	Type	Product Series	Models	Firmware
Comware V7	Access Controller	WX5800 Series	WX5860X	H3C Comware Software, Version 7.1.064, Release 5484P23
		WX2800 Series	WX2880X, WX2860X, WX2812X-PWR	H3C Comware Software, Version 7.1.064, Release 5817P33
	Access Point	WA6500 Series	WA6520, WA6526, WA6526E, WA6520H	H3C Comware Software, Version 7.1.064, Release 2617P33
		WA7200 Series	WA7220-HI	H3C Comware Software, Version 7.1.064, Release 2617P33
		WA7300 Series	WA7320i, WA7338-HI, WA7330X, WA7330i, WA7320XE, WA7322H-HI	H3C Comware Software, Version 7.1.064, Release 2617P33
		WA7500 Series	WA7539	H3C Comware Software, Version 7.1.064, Release 2617P33

		WA7600 Series	WA7638, WA7620CE	H3C Comware Software, Version 7.1.064, Release 2617P33
Comware V9	Access Controller	WX3800 Series	WX3840X, WX3820X	H3C Comware Software, Version 9.1.061, ESS 1404P23

Table 4 TOE models in scope

All V7 Wireless Controllers (WX5860X, WX2880X, WX2860X, WX2812X-PWR) run the same Comware Version 7.1. software. The difference between Wireless Controllers under the same software version is the physical port type, number of the physical port, manageable number of APs, manageable number of wireless users.

All V9 Wireless Controllers (WX3840X, WX3820X) run the same Comware Version 9.1 software. The difference between controllers under Version 7.1 and Version 9.1 is that, Version 9.1 has been adjusted and optimized in its internal architecture, and its features are based on modular fine-grained. Compared with Version 7.1, it supports more forms, such as containerized forms. In terms of security functions, Version 9.1 fully inherits the functional specifications of Version 7.1, so the security functions of Version 9.1 and Version 7.1 are consistent.

The APs of TOE include three types: Indoor AP (ceilings and are not physical reachable), Outdoor AP (hanging high and are not physical reachable), wall plate AP (wall mounted and physical reachable, but do not have user management interface). The AP provides the connection point between wlan client hosts and the wired network. The APs also communicate directly with the wireless controller for management purposes. The management traffic between H3C AP and H3C Wireless Access Controller is encrypted using DTLS and TLS. In the evaluated TOE configuration, it is mandatory to configure in the AC/AP the verification of the authenticity of Aps following section 7.7.6.7 of the Preparative and Operative Procedures [AGD_PREOPE].

All H3C APs run the same Comware Version 7.1 software. The difference between AP models under the same software version is the radio properties, MIMO properties, the physical port type, number of physical ports. H3C AP do not have user interface used for administration or configuration of the AP component. All administration and configuration of the H3C AP component occurs through the H3C Access Controller component. The evaluated configuration of the TOE needs to be performed under FIPS mode. Therefore, the TOE must be manually switched to FIPS mode prior to evaluation.

TOE Delivery

The delivery of the TOE to the customer is performed by an authorized courier service.

TOE firmware can be obtained from the H3C official website or by contacting H3C engineers. Software is delivered in .ipe file.

The Installation Guides, Configuration Guides, and Command References can be obtained from the H3C official website. If the content of the documents is revised, the version number on the H3C official website will be updated. Alternatively, you can contact the H3C engineers for the latest versions. The security administrator need to use documents with version numbers no lower than those listed in this security target.

Installation Guides are in PDF format. Configuration Guides and Command References are chm format.

Models	Item	Name	Version
WX5860X	Installation Guides	H3C WX5860X Access Controllers Installation Guide	6W105
	Command References	H3C WX5800X Series Access Controllers Command References	6W101
	Configuration Guides	H3C WX5800X Series Access Controllers Configuration Guides	6W101
WX2880X, WX2860X, WX2812X-PWR	Installation Guides	H3C WX2880X Access Controllers Installation Guide H3C WX2860X Access Controllers Installation Guide H3C WX2812X-PWR Access Controllers Installation Guide	6W101 6W101 5W103
	Command References	H3C WX2800X&WSG1800X Command References	6W101
	Configuration Guides	H3C WX2800X&WSG1800X Configuration Guides	6W101
WA6520	Installation Guides	H3C WA6520 Access Point Installation Guide	5W101
WA6526, WA6526E	Installation Guides	H3C Wi-Fi6 Indoor Access Points Installation Guide	6W104
WA6520H	Installation Guides	H3C WA6520H Access Point Installation Guide	5W100
WA7322H-HI	Installation Guides	H3C WA7322H-HI Access Point Installation Guide	AW100
WA7220-HI, WA7330i, WA7338-HI, WA7320i, WA7539, WA7638	Installation Guides	H3C Wi-Fi7 Indoor Access Points Installation Guide	5W109
WA7320XE	Installation Guides	H3C WA7320XE Access Point Installation Guide	5W100
WA7330X	Installation Guides	H3C WA7330X Access Point Installation Guide	5W101
WA7620CE	Installation Guides	H3C WA7620CE Access Point Installation Guide	6W105

WX3840X, WX3820X	Installation Guides	H3C WX3840X Access Controllers Installation Guide H3C WX3820X Access Controllers Installation Guide	6W105 6W105
	Command References	H3C WX3800X Series Access Controllers Command References	6W101
	Configuration Guides	H3C WX3800X Series Access Controllers Configuration Guides	6W101
[AGD_PREOPE]	Guidance Document	H3C Wlan Series Preparative and Operative Procedures	2.7

Table 5 TOE deliverables

1.4.2 Logical Scope

This section outlines the logical boundaries of the security functionality of the TOE.

1.4.2.1 Security audit

The TOE is designed to be able to generate logs for a wide range of security relevant events.

The TOE can be configured to store the logs locally so they can be accessed by an administrator and to send the logs to a designated external Audit server to mitigate the possibility of losing audit records when available space becomes exhausted on the TOE.

Locally stored audit records can be reviewed and managed by an administrator.

1.4.2.2 Cryptographic support

The TOE includes a cryptographic module that provides random bit generation, key management, encryption/decryption, digital signature, secure hashing and key-hashing features in support of higher level cryptographic protocols including IPsec, SSH, TLS/DTLS to provide a trusted path for remote administration.

1.4.2.3 Identification and authentication

The TOE requires users (i.e., administrators) to be successfully identified and authenticated before they can access any security management functions available in the TOE. The TOE offers both a locally connected console as well as network accessible interfaces (e.g., SSH,) for interactive administrator sessions.

The TOE supports the local definition of users with usernames and roles that can be authenticated with passwords or Public-Key. The TOE has policies to force the passwords to meet security requirements and can prevent brute-forcing it. The TOE supports roles to control permissions for administrators (i.e., network-admin and security- auditor are authorized administrators). Additionally, TOE can configure IPSEC connected RADIUS servers for authentication services to support e.g., centralized user management.

1.4.2.4 Security management

The TOE provides Command Line (CLI) commands to access the wide range of security management functions. Security management are limited to administrators only after they have provided acceptable user identification and authentication data to the TOE.

1.4.2.5 Protection of the TSF

The TOE protects the pre-shared keys, symmetric keys, and private keys from reading them by an unauthorized entity.

The TOE stores the users or administrator passwords in non-plaintext form preventing them from reading.

The TOE verifies the packet before their installation and uses the digital signature.

The TOE performs self-tests on its power on to ensure its correct behaviour.

1.4.2.6 TOE access

The TOE can be configured to display advisory banners when user's login and will enforce an administrator-defined inactivity timeout value after which an inactive session will be terminated, allowing also the capability of self-terminate its session for the administrator.

1.4.2.7 Trusted path/channels.

The TOE uses IPsec to provide an encrypted channel between itself and third-party trusted IT entities in the operating environment including external audit server, external authentication server and NTP server.

The TOE secures remote communication with administrators by implementing SSHv2 for CLI access. the integrity and disclosure protection are ensured via the secure protocol.

Wlan Clients establish an encrypted IEEE 802.11 link with TOE that protects wireless data in transit from disclosure and modification.

1.4.2.8 Communication

The Security Administrator can manage, enable and disable the communication between the different parts of the TOE (Access Controller and Access Points). The communication between these parts is protected with DTLS and TLS.

2 Conformance claims

2.1 CC Conformance Claim

This Security Target claims conformance to the Common Criteria (CC) Version 3.1, Revision 5, dated: April 2017. The TOE and ST are CC Part 2 extended and CC Part 3 conformant.

The methodology used in the evaluation is [CEM] [PP_ND3.0e_SD] [PPSSH][EPWLAN_SD]:

Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 5, CCMB-2017-04-004[CEM]

Evaluation Activities for Network Device cPP Version: 3.0e Date: 06-December-2023 [PP_ND3.0e_SD]

Functional Package for Secure Shell (SSH) Version: 1.0 2021-05-13[PPSSH]

Supporting Document Mandatory Technical Document, PP-Module for Wireless Local Area Network (WLAN) Access System Version: 1.0 2022-03-31[EPWLAN_SD]

2.2 PP Conformance

The TOE claims exact conformance to:

- Collaborative Protection Profile for Network Devices v3.0e, 06-12-2023 [PP-ND].
- Functional Package for Secure Shell (SSH) v1.0, 2021-05-13 [PPSSH]
- PP-Module for Wireless Local Area Network (WLAN) Access System Version: 1.0， 2022-03-31[EPWLAN].

2.3 Conformance Rationale

The ST conforms to the [PP-ND]/[PPSSH]/[EPWLAN]. the security problem definition, security objectives, and security requirements have been drawn from the PP.

3 Security Problem Definition

The Security Problem Definition is taken from the Security Problem Definition (composed of organizational policies, threat statements, and assumption) described in the Network Devices PP [PP-ND] and PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0 (MOD_WLAN_AS_V1.0) [EPWLAN]

3.1 Threats

The threats for the Network Device are grouped according to functional areas of the device in the sections below.

3.1.1 T.UNAUTHORIZED_ADMINSTRATOR_ACCESS

Threat agents may attempt to gain Administrator access to the Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.

SFR Rationale:

- The Administrator role is defined in FMT_SMR.2 and the relevant administration capabilities are defined in FMT_SMF.1 and FMT_MTD.1/CoreData
- The actions allowed before authentication of an Administrator are constrained by FIA_UIA_EXT.1, and include the advisory notice and consent warning message displayed according to FTA_TAB.1
- The requirement for the Administrator authentication process is described in FIA_UIA_EXT.1.
- Locking of Administrator sessions is ensured by FTA_SSL_EXT.1 (for local sessions), FTA_SSL.3 (for remote sessions), and FTA_SSL.4 (for all interactive sessions)
- The secure channel used for remote Administrator connections is specified in FTP_TRP.1/Admin
- (Malicious actions carried out from an Administrator session are separately addressed by T.UNDETECTED_ACTIVITY)
- If the TOE provides remote administration using a password-based authentication mechanism, FIA_AFL.1 provides actions on reaching a threshold number of consecutive password failures.

3.1.2 T.WEAK_CRYPTOGRAPHY

Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.

SFR Rationale:

- Requirements for key generation and key distribution are set in FCS_CKM.1 and FCS_CKM.2 respectively
- Requirements for use of cryptographic schemes are set in FCS_COP.1/DataEncryption, FCS_COP.1/SigGen, FCS_COP.1/Hash, and FCS_COP.1/KeyedHash
- Requirements for random bit generation to support key generation and secure protocols (see SFRs resulting from T.UNTRUSTED_COMMUNICATION_CHANNELS) are set in FCS_RBG_EXT.1.
- Management of cryptographic functions is specified in FMT_SMF.1

3.1.3 T.UNTRUSTED_COMMUNICATION_CHANNELS

Threat agents may attempt to target Network Devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the Network Device itself.

SFR Rationale:

- The general use of secure protocols for identified communication channels is described at the top level in FTP_ITC.1, FTP_ITC.1/Client and FTP_TRP.1/Admin; for distributed TOEs the requirements for inter-component communications are addressed by the requirements in FPT_ITT.1
- Requirements for the use of secure communication protocols are set for allowed protocols in FCS_DTLSC_EXT.1, FCS_DTLSS_EXT.1, FCS_IPSEC_EXT.1, FCS_TLSC_EXT.1, FCS_TLSS_EXT.1
- Requirements for the use of secure communication protocols implemented by the packages specified in Section 2.2 may be found in the respective package's document. FCS_SSHS_EXT.1, FCS_SSH_EXT.1.
- Optional and selection-based requirements for use of public key certificates to support secure protocols are defined in FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3

3.1.4 T.WEAK_AUTHENTICATION_ENDPOINTS

Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints, e.g., a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.

SFR Rationale:

- The use of appropriate secure protocols to provide authentication of endpoints (as in the SFRs addressing T.UNTRUSTED_COMMUNICATION_CHANNELS) are ensured by the requirements in FTP_ITC.1 and FTP_TRP.1/Admin; for distributed TOEs the authentication requirements for endpoints in intercomponent communications are addressed by the requirements in FPT_ITT.1
- Additional possible special cases of secure authentication during registration of distributed TOE components are addressed by FCO_CPC_EXT.1.

3.1.5 T.UPDATE_COMPROMISE

Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. No validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.

SFR Rationale:

- Requirements for protection of updates are set in FPT_TUD_EXT.1
- Requirements for management of updates are defined in FMT_SMF.1 and (for manual updates) in FMT_MOF.1/ManualUpdate

3.1.6 *T.UNDETECTED_ACTIVITY*

Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.

SFR Rationale:

- Requirements for basic auditing capabilities are specified in FAU_GEN.1 and FAU_GEN.2, with timestamps

provided according to FPT_STM_EXT.1 and if applicable, protection of NTP channels in FCS_NTP_EXT.1
- Requirements for protecting audit records stored on the TOE are specified in FAU_STG.1.
- Requirements for secure storage and transmission of local audit records to an external IT entity via a secure channel are specified in FAU_STG_EXT.1.
- If (optionally) configuration of the audit functionality is provided by the TOE then this is specified in FMT_SMF.1 and confining this functionality to Security Administrators is required by FMT_MOF.1/Functions.

3.1.7 T.SECURITY_FUNCTIONALITY_COMPROMISE

Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker. Threat agents may also be able to take advantage of weak administrative passwords to gain privileged access to the device.
SFR Rationale:

- Protection of secret/private keys against compromise is specified in FPT_SKP_EXT.1
- Secure destruction of keys is specified in FCS_CKM.4.
- Management of keys is specified in FMT_SMF.1 and confining this functionality to Security Administrators is required by FMT_MTD.1/CryptoKeys.
- If optional local administration using a password-based authentication mechanism is provided by the TOE, FIA_UAU.7 provides protection of the password entry by providing only obscured feedback at the local console.
- If the TOE provides password-based authentication mechanisms, requirements for password lengths and available characters are set in FIA_PMG_EXT.1 Requirements for secure storage of passwords are set in FPT_APW_EXT.1.
- FIA_PSK_EXT.1 supports the objective by requiring the TSF to protect the confidentiality and integrity of configured pre-shared keys, preventing their unauthorized access or modification.

3.1.8 T.SECURITY_FUNCTIONALITY_FAILURE

An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.
SFR Rationale:

- Requirements for running self-test(s) are defined in FPT_TST_EXT.1

3.1.9 T.NETWORK_DISCLOSURE

Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to conduct unauthorized activities. If malicious external devices are able to communicate with devices on the protected network, or if devices on the protected network can establish communications with those external devices (e.g., as a result of non-existent or insufficient WLAN data encryption that exposes the WLAN data in transit to rogue elements), then those internal devices may be susceptible to the unauthorized disclosure of information.
SFR Rationale:
The threat T.NETWORK_DISCLOSURE is countered by O.AUTHENTICATION as proper authentication of external entities ensures that network data is not disclosed to an unauthorized subject.

- FCO_CPC_EXT.1 supports the objective by requiring the TSF to implement a mechanism that authenticates its distributed components to each other.
- FIA_8021X_EXT.1 supports the objective by requiring the TSF to act as the authenticator for 802.1X authentication.
- FIA_UAU.6 supports the objective by requiring the TSF to re-authenticate a security administrator under certain circumstances.
- FTA_TSE.1 supports the objective by requiring the TSF to deny the establishment of a wireless client session for reasons unrelated to the correctness of an authentication credential.

The threat T.NETWORK_DISCLOSURE is countered by O.CRYPTOGRAPHIC_FUNCTIONS as implementation of

cryptographic functions ensures that network data is not subject to unauthorized disclosure in transit.

- FCS_COP.1/DataEncryption supports the objective by requiring the TSF to implement AES in the modes needed to support its other functions.
- FCS_CKM.1/WPA supports the objective by requiring the TSF to generate symmetric keys used for WPA2.
- FCS_CKM.2/GTK supports the objective by requiring the TSF to distribute group temporal keys used for IEEE 802.11.
- FCS_CKM.2/PMK supports the objective by requiring the TSF to distribute pairwise master keys used for IEEE 802.11.

3.1.10 T.NETWORK_ACCESS

Devices located outside the protected network may seek to exercise services located on the protected network that are intended to be only accessed from inside the protected network or only accessed by entities using an authenticated path into the protected network.

SFR Rationale:

The threat T.NETWORK_ACCESS is countered by O.AUTHENTICATION as proper authentication methods ensure that subjects outside the protected network cannot access data inside the protected network until the TSF has authenticated them.

- FCO_CPC_EXT.1 supports the objective by requiring the TSF to implement a mechanism that authenticates its distributed components to each other.
- FIA_8021X_EXT.1 supports the objective by requiring the TSF to act as the authenticator for 802.1X authentication.
- FIA_UAU.6 supports the objective by requiring the TSF to re-authenticate a security administrator under certain circumstances.
- FTA_TSE.1 supports the objective by requiring the TSF to deny the establishment of a wireless client session for reasons unrelated to the correctness of an authentication credential.

The threat T.NETWORK_DISCLOSURE is countered by O.TOE_ADMINISTRATION as the TOE's administration function does not permit execution of management functions that originate from wireless clients outside the protected network.

- FMT_SMR_EXT.1 supports the objective by requiring the TSF to prevent any administrative actions that originate from the 'external' network.
- FMT_SMF.1/AccessSystem supports the objective by defining management functionality that is specific to WLAN AS devices.

3.1.11 T.TSF_FAILURE

Security mechanisms of the TOE generally build up from a primitive set of mechanisms (e.g., memory management, privileged modes of process execution) to more complex sets of mechanisms. Failure of the primitive mechanisms could lead to a compromise in more complex mechanisms, resulting in a compromise of the TOE Security Functionality (TSF).

SFR Rationale:

The threat T.TSF_FAILURE is countered by O.FAIL_SECURE as the TOE responds to self-test failures that are significant enough to show a potential compromise of the TSF by making the TSF unavailable until the failure state has been cleared.

- FPT_TST_EXT.1 supports the objective by requiring the TSF to perform self-tests that may aid in the detection of a TSF failure.
- FPT_FLS.1 supports the objective by requiring the TSF to preserve a secure state in the event of a self-test failure.

The threat T.TSF_FAILURE is countered by O.SYSTEM_MONITORING as the TOE generates audit records of unauthorized usage, communications outages, incorrect degraded ability to enforce its intended security functionality so that issues can be diagnosed and resolved appropriately.

- FAU_GEN.1/WLAN supports the objective by requiring the TSF to generate audit records for security-relevant WLAN behavior.
- FAU_GEN_EXT.1, FAU_STG_EXT.4, FAU_STG_EXT.5 supports the objective by requiring the TSF to generate

appropriate security-relevant auditable events on each of its distributed components.

- FAU_STG_EXT.1 supports the objective by defining how distributed TOE components store their generated audit records.

3.1.12 T.DATA_INTEGRITY

Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to modify the data without authorization. If known malicious external devices are able to communicate with devices on the protected network or if devices on the protected network can establish communications with those external devices then the data contained within the communications may be susceptible to a loss of integrity.

SFR Rationale:

The threat T.DATA_INTEGRITY is countered by O.CRYPTOGRAPHIC_FUNCTIONS as the TOE uses cryptographic functionality to enforce the integrity of protected data in transit.

- FCS_COP.1/DataEncryption supports the objective by requiring the TSF to implement AES in the modes needed to support its other functions.
- FCS_CKM.1/WPA supports the objective by requiring the TSF to generate symmetric keys used for WPA2.
- FCS_CKM.2/GTK supports the objective by requiring the TSF to distribute group temporal keys used for IEEE 802.11.
- FCS_CKM.2/PMK supports the objective by requiring the TSF to distribute pairwise master keys used for IEEE 802.11.

3.1.13 T.REPLAY_ATTACK

If an unauthorized individual successfully gains access to the system, the adversary may have the opportunity to conduct a "replay" attack. This method of attack allows the individual to capture packets traversing throughout the wireless network and send the packets at a later time, possibly unknown by the intended receiver.

SFR Rationale:

The threat T.REPLAY_ATTACK is countered by O.AUTHENTICATION as the TOE's use of authentication mechanisms prevent replay attacks because the source of the attack will not have the proper authentication data for the TSF to process the replayed traffic.

- FCO_CPC_EXT.1 supports the objective by requiring the TSF to implement a mechanism that authenticates its distributed components to each other.
- FIA_8021X_EXT.1 supports the objective by requiring the TSF to act as the authenticator for 802.1X authentication.
- FIA_UAU.6 supports the objective by requiring the TSF to re-authenticate a security administrator under certain circumstances.
- FTA_TSE.1 supports the objective by requiring the TSF to deny the establishment of a wireless client session for reasons unrelated to the correctness of an authentication credential.

The threat T.REPLAY_ATTACK is countered by O.CRYPTOGRAPHIC_FUNCTIONS as the TOE's use of cryptographic functionality prevents impersonation attempts that use replayed traffic.

- FCS_COP.1/DataEncryption supports the objective by requiring the TSF to implement AES in the modes needed to support its other functions.
- FCS_CKM.1/WPA supports the objective by requiring the TSF to generate symmetric keys used for WPA2.
- FCS_CKM.2/GTK supports the objective by requiring the TSF to distribute group temporal keys used for IEEE 802.11.

  FCS_CKM.2/PMK supports the objective by requiring the TSF to distribute pairwise master keys used for IEEE 802.11.

3.2 Assumptions

This section describes the assumptions made in identification of the threats and security requirements for Network Devices. The Network Device is not expected to provide assurance in any of these areas, and as a

result, requirements are not included to mitigate the threats associated.

3.2.1 A.PHYSICAL_PROTECTION

The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device

3.2.2 A.LIMITED_FUNCTIONALITY

The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general-purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).

3.2.3 A.NO_THRU_TRAFFIC_PROTECTION

A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).

3.2.4 A.TRUSTED_ADMINISTRATOR

The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) fully validate any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store as a trust anchor prior to use.

3.2.5 A.REGULAR_UPDATES

The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

3.2.6 A.ADMIN_CREDENTIALS_SECURE

The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.

3.2.7 A.COMPONENTS_RUNNING (applies to distributed TOEs only)

For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.

3.2.8 3.2.8. A.RESIDUAL_INFORMATION

The Administrator must ensure that there is no unauthorized access possible for sensitive residual information

(e.g., cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

3.2.9 A.CONNECTIONS

It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE's security policies will be enforced on all applicable network traffic flowing among the attached networks.

3.3 Organizational Security Policy

3.3.1 P.ACCESS_BANNER

The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which Administrators consent by accessing the TOE.

SFR Rationale:

- An advisory notice and consent warning message is required to be displayed by FTA_TAB.1

4 Security Objectives

4.1 Security Objectives for the TOE

4.1.1 O.CRYPTOGRAPHIC_FUNCTIONS

The TOE will provide means to encrypt and decrypt data to maintain confidentiality and allow for detection of modification of TSF data that is transmitted outside the TOE.

4.1.2 O.AUTHENTICATION

The TOE will provide a means to authenticate the user to ensure they are communicating with an authorized external IT entity.

4.1.3 O.FAIL_SECURE

Upon a self-test failure, the TOE will shut down to ensure that data cannot be passed without adhering to the TOE's security policies.

4.1.4 O.SYSTEM_MONITORING

The TOE will provide a means to audit events specific to WLAN functionality and security.

4.1.5 O.TOE_ADMINISTRATION

The TOE will provide the functions necessary to address failed authentication attempts by a remote administrator.

4.2 Security Objectives for the Operational Environment

The Security Objectives for the Operational Environment are taken from the Security Objectives for the Operational Environment described in Section 5.1 of the Network Devices PP [PP-ND], extended with the ones defined in section 4.2 of PP-Module for Wireless Local Area Network (WLAN) AccessSystem, Version 1.0 (MOD_WLAN_AS_V1.0).

4.2.1 OE.PHYSICAL

Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

4.2.2 OE.NO_GENERAL_PURPOSE

There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

4.2.3 OE.NO_THRU_TRAFFIC_PROTECTION

The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.

4.2.4 OE.TRUSTED_ADMIN

Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner.
For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE’s trust store in case such certificate can no longer be trusted.

4.2.5 OE.UPDATES

The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

4.2.6 OE.ADMIN_CREDENTIALS_SECURE

The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.

4.2.7 OE.COMPONENTS_RUNNING (applies to distributed TOEs only)

For distributed TOEs, the Security Administrator ensures that the availability of every TOE component is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. The Security Administrator also ensures that it is checked as appropriate for every TOE component that the audit functionality is running properly.

4.2.8 OE.RESIDUAL_INFORMATION

The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g., cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

4.2.9 OE.CONNECTIONS

TOE administrators will ensure that the TOE is installed in a manner that will allow the TOE to effectively enforce its policies on the network traffic of monitored networks.

5 Extended Component Definition

Extended Component Definition has been taken from the Network Devices PP [PP-ND] with the modifications provided by the Functional package [PPSSH] and PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0 (MOD_WLAN_AS_V1.0) [EPWLAN].

Extended SFRs:
PP-ND&EPWLAN: FAU_GEN_EXT.1: Security Audit Generation
PP-ND&EPWLAN: FAU_STG_EXT.1: Protected Audit Event Storage
PP-ND&EPWLAN: FAU_STG_EXT.4: Protected Local Audit Event Storage for Distributed TOEs
PP-ND: FAU_STG_EXT.5 Protected Remote Audit Event Storage for Distributed TOEs
PP-ND&EPWLAN: FCO_CPC_EXT.1 Component Registration Channel Definition
PP-ND: FCS_IPSEC_EXT.1: IPsec Protocol
PP-ND: FCS_NTP_EXT.1: NTP Protocol
PPSSH: FCS_SSHS_EXT.1: SSH Server Protocol
PPSSH: FCS_SSH_EXT.1: SSH Protocol
PP-ND: FCS_DTLSC_EXT.1: DTLS Client Protocol Without Mutual Authentication
PP-ND: FCS_DTLSS_EXT.1: DTLS Server Protocol Without Mutual Authentication
PP-ND: FCS_TLSC_EXT.1: TLS Client Protocol Without Mutual Authentication
PP-ND: FCS_TLSS_EXT.1: TLS Server Protocol Without Mutual Authentication
PP-ND&EPWLAN: FCS_RBG_EXT.1: Random Bit Generation
EPWLAN: FIA_8021X_EXT.1: 802.1X Port Access Entity (Authenticator) Authentication
EPWLAN: FIA_PSK_EXT.1: Pre-Shared Key Composition
PP-ND: FIA_PMG_EXT.1: Password Management
PP-ND: FIA_UIA_EXT.1: User Identification and Authentication
PP-ND: FIA_X509_EXT.1/Rev: X.509 Certificate Validation
PP-ND: FIA_X509_EXT.1/ITT X.509 Certificate Validation
PP-ND: FIA_X509_EXT.2: X.509 Certificate Authentication
PP-ND: FIA_X509_EXT.3: X.509 Certificate Requests
PP-ND: FCO_CPC_EXT.1 Component Registration Channel Definition
EPWLAN: FMT_SMR_EXT.1: No Administration from Client
PP-ND: FPT_APW_EXT.1: Protection of Administrator Passwords
PP-ND: FPT_SKP_EXT.1: Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
PP-ND: FPT_STM_EXT.1: Reliable Time Stamps
PP-ND& EPWLAN: FPT_TST_EXT.1: TSF testing
PP-ND: FPT_TUD_EXT.1: Trusted update
PP-ND: FTA_SSL_EXT.1: TSF-initiated Session Locking

6 Security Functional Requirements

The conventions used in descriptions of the SFRs are as follows::

- Unaltered SFRs are given by their extended component definition (ECD);
- Refinement made in the PP, EP or ST: the refinement text is indicated with **bold text** and ~~strikethroughs~~;
- Selection wholly or partially completed in the PP, EP or ST: the selection values are indicated with underlined text

  e.g., '[selection: *disclosure, modification, loss of use*]' in an ECD might become 'disclosure' (completion) or '[selection: disclosure, modification]' (partial completion) in the ST;

- Assignment wholly or partially completed in the PP, EP or ST: indicated with *italicized text*;
- Assignment completed within a selection in the PP, EP or ST: the completed assignment text is indicated with *italicized and underlined text*

  e.g., '[selection: *change_default, query, modify, delete, [assignment: other operations]*]' in an ECD might become 'change default, select tag' (completion of both selection and assignment) or '[selection: change default, *select tag*, *select value*]' (partial completion of selection, and completion of assignment) in the ST;

- Iteration: indicated by adding a string starting with '/' (e.g., 'FCS_COP.1/Hash').

All the application notes defined in the PP [PP-ND] have been considered when writing this document. Please refer to the PP [PP-ND] for specific details.

6.1 Security Audit (FAU)

6.1.1 Security Audit Data generation (FAU_GEN)

6.1.1.1 FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shut-down of the audit functions;
b) All auditable events for the not specified level of audit; and
c) All administrative actions comprising:
- *Administrative login and logout (name of Administrator account shall be logged if individual accounts are required for Administrators).*
- *Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).*
- *Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).*
- *[selection: Resetting passwords (name of related user account shall be logged)].*
- [selection: no other actions];

*d) Specifically defined auditable events listed in **Table** .*

FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:
a. Date and time of the event, type of event, subject identity (~~if applicable~~), and the outcome (success or failure) of the event; and
b. For each audit event type, based on the auditable event definitions of the functional components included in the cPP/ST, information specified in column three of Table 6.

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_GEN.1/WLAN	None	None
FAU_GEN_EXT.1	None	None
FAU_STG_EXT.4	None	None
FAU_STG_EXT.5	None	None
FAU_STG_EXT.1	Configuration of local audit settings.	Identity of account making changes to the audit configuration.
FAU_STG.1	None.	None.
FCS_CKM.1	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.
FCS_CKM.1/WPA	None.	None.
FCS_COP.1/DataEncryption	None	None
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_RBG_EXT.1	None.	None.
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).
FIA_PMG_EXT.1	None.	None.
FIA_PSK EXT.1	None.	None.
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MTD.1/CoreData	None.	None.
FMT_SMF.1	All management activities of TSF data.	None.
FMT_SMR.2	None.	None.
FMT_MTD.1/CryptoKeys	None.	None.

FPT_ITT.1	• Initiation of the trusted channel. • Termination of the trusted channel. • Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_TST_EXT.1	Execution of this set of TSF-self tests. Detected integrity violations.	•None. •The TSF code file that caused the integrity violation.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None.
FPT_STM_EXT.1	Discontinuous changes to time – either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FTA_SSL_EXT.1 (if "terminate the session" is selected)	The termination of a local session by the session locking mechanism.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.
FTP_ITC.1	• Initiation of the trusted channel. • Termination of the trusted channel. • Failure of the trusted channel functions. • Failed attempts to establish a trusted channel (including IEEE 802.11) • Detection of modification of channel data	• None • None • Reason for failure • Identification of the initiator and target of channel • None
FTP_ITC.1/Client	None.	None.
FTP_TRP.1/Admin	• Initiation of the trusted path. • Termination of the trusted path. • Failure of the trusted path functions.	•None •None •Reason for failure
FMT_MOF.1/Functions	None.	None.
FCO_CPC_EXT.1	• Enabling communications between a pair of components. • Disabling communications between a pair of components.	Identities of the endpoint pairs enabled or disabled.
FCS_IPSEC_EXT.1	•Failure to establish an IPsec SA •Protocol failures. •Establishment/Termination of an IPsec SA.	•Reason for failure •Reason for failure Non-TOE endpoint of connection •Non-TOE endpoint of connection.
FCS_NTP_EXT.1	• Configuration of a new time server • Removal of configured time server	Identity if new/removed time server
FCS_SSH_EXT.1	Failure to establish an SSH session	Reason for failure
FCS_SSHS_EXT.1	None	None

FCS_TLSC_EXT.1	Failure to establish a TLS Session	Reason for failure
FCS_TLSS_EXT.1	Failure to establish a TLS Session	Reason for failure
FCS_DTLSC_EXT.1	Failure to establish a DTLS session	Reason for failure
FCS_DTLSS_EXT.1	Failure to establish a DTLS session	Reason for failure
	Detected replay attacks	Identity (e.g., source IP address) of the source of the replay attack
FIA_X509_EXT.1/Rev	• Unsuccessful attempt to validate a certificate • Any addition, replacement or removal of trust anchors in the TOE's trust store	• Reason for failure of certificate validation • Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store
FIA_X509_EXT.1/ITT	• Unsuccessful attempt to validate a certificate • Any addition, replacement or removal of trust anchors in the TOE's trust store	• Reason for failure of certificate validation • Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store
FIA_X509_EXT.2	None	None
FIA_X509_EXT.3	None	None
FCS_CKM.1/WPA	None.	None.
FCS_CKM.2/GTK	None.	None.
FCS_CKM.2/PMK	None.	None.
FIA_8021X_EXT.1	Attempts to access the 802.1X controlled port prior to successful completion of the authentication exchange.	Provided client identity (e.g., Media Access Control [Media Access Control (MAC)] address).
	Failed authentication attempt.	Provided client identity (e.g., MAC address).
FIA_UAU.6	Attempts to re-authenticate.	Origin of the attempt (e.g., IP address).
FMT_SMF.1/AccessSystem	None	None
FMT_SMR_EXT.1	None	None
FPT_FLS.1	Failure of the TSF.	Indication that the TSF has failed with the type of failure that occurred.
FTA_TSE.1	Failure of the TSF.	Indication that the TSF has failed with the type of failure that occurred.

Table 6 Security Functional Requirements and Auditable Events

6.1.1.2 FAU_GEN.2 User identity association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.2 Security Audit Event Storage (FAU_STG.1 & Extended –FAU_STG_EXT)

6.1.2.1 FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to prevent unauthorised modifications to the stored audit records in the audit trail.

6.1.2.2 FAU_STG_EXT.1 Protected Audit Event Storage

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1.

FAU_STG_EXT.1.2 The TSF shall be able to store generated audit data on the TOE itself. In addition [selection:

- The TOE shall be a distributed TOE that stores audit data on the following TOE components: [assignment: Access Controller].

FAU_STG_EXT.1.3 The TSF shall maintain a [selection: log file, buffer] of audit records in the event that an interruption of communication with the remote audit server occurs.

FAU_STG_EXT.1.4 The TSF shall be able to store [selection: persistent] audit records locally with a minimum storage size of [assignment: *1 Megabyte (MB)*].

FAU_STG_EXT.1.5 The TSF shall [selection: overwrite previous audit records according to the following rule: [assignment*: oldest audit record is overwritten] , [assignment: no other action]*] when the local storage space for audit data is full.

FAU_STG_EXT.1.6 The TSF shall provide the following mechanisms for administrative access to locally stored audit records [selection: manual export, ability to view locally] .

6.2 Cryptographic Support (FCS)

6.2.1 Cryptographic Key Management (FCS_CKM)

6.2.1.1 FCS_CKM.1 Cryptographic Key Generation (Refinement)

FCS_CKM.1.1 The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm: [selection:

- RSA schemes using cryptographic key sizes of [assignment: 3072 bits or greater] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;
- ECC schemes using 'NIST curves' [selection: P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4;
- FFC Schemes using 'safe-prime' groups that meet the following: "NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [RFC 3526]

] ~~and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].~~

6.2.1.2 FCS_CKM.2 Cryptographic Key Establishment (Refinement)

FCS_CKM.2.1 The TSF shall **perform** cryptographic **key establishment** in accordance with a specified cryptographic key **establishment** method: [selection:

- Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";
- FFC Schemes using "safe-prime" groups that meet the following: 'NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [selection: RFC 3526].

] ~~that meets the following: [assignment: list of standards].~~

6.2.1.3 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method.

- For plaintext keys in volatile storage, the destruction shall be executed by a [selection: single overwrite consisting of [selection: zeroes, a new value of the key]];
- • For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that [selection:
    - logically addresses the storage location of the key and performs a [selection: single-pass] overwrite consisting of [selection: zeroes, a new value of the key]];

that meets the following: No Standard.

6.2.2 Cryptographic Operation (FCS_COP.1)

6.2.2.1 FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)

FCS_COP.1.1/SigGen The TSF shall perform cryptographic *signature services (generation and verification)* in accordance with a specified cryptographic algorithm [selection:

- RSA Digital Signature Algorithm
- Elliptic Curve Digital Signature Algorithm

]

and cryptographic key sizes [

- For RSA: modulus **3072** bits or greater,
- For ECDSA: 256 bits or greater

]

that meet the following: [selection*:*

- For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes

RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,

- For ECDSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" [selection: P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4

].

6.2.2.2 FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)

FCS_COP.1.1/Hash	The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm [selection: SHA-256, SHA-384, SHA-512] ~~and cryptographic key sizes [assignment: cryptographic key sizes]~~ and **message digest sizes [selection: 256, 384, 512] bits** that meet the following: *ISO/IEC 10118-3:2004*.

6.2.2.3 FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)

FCS_COP.1.1/KeyedHash	The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm [selection: HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, implicit] and cryptographic key sizes [*assignment:256, 384, 512*] **and message digest sizes [selection: 256, 384, 512] bits** that meet the following: ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2".

6.2.3 Random Bit Generation (Extended – FCS_RBG_EXT)

6.2.3.1 FCS_RBG_EXT.1 Random Bit Generation (RBG)

FCS_RBG_EXT.1.1	The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [selection: CTR_DRBG (AES)].
FCS_RBG_EXT.1.2	The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [selection: [assignment: 1] software-based noise source] with a minimum of [selection: 256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

6.3 Identification and Authentication (FIA)

6.3.1 Authentication Failure Management (FIA_AFL)

6.3.1.1 FIA_AFL.1 Authentication Failure Management (Refinement)

FIA_AFL.1.1	The TSF shall detect when an Administrator configurable positive integer within [assignment: *2-10*] unsuccessful authentication

attempts occur related to *Administrators attempting to authenticate remotely using a password*.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall [selection: prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until [assignment: *unlock*] is taken by an Administrator].

6.3.2 Password Management (Extended – FIA_PMG_EXT)

6.3.2.1 FIA_PMG_EXT.1 Password Management

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [selection: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", [assignment: "'", "+", ",", "-", ".", "/", ":", ";", "<", "=", ">", "[", "\", "]", "_", "`", "{", "}", "|", "'", " ", *and* "~"]];

b) Minimum password length shall be configurable to between [*assignment: 15*] and [assignment: 32] characters.

6.3.3 Pre-Shared Key Composition (Extended – FIA_PSK_EXT)

6.3.3.1 FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition

FIA_PSK_EXT.1.1 The TSF shall be able to use pre-shared keys for [**selection**: IPsec, WPA3-SAE, IEEE 802.11 WPA2-PSK, [*assignment*: *None*]].

FIA_PSK_EXT.1.2 The TSF shall be able to accept text-based pre-shared keys that:

- are 22 characters and [**selection**: IPsec, WPA3-SAE, IEEE 802.11 WPA2-PSK] protocol is [assign: IPsec: *lengths from 15 to 128 characters*; WPA3-SAE/IEEE 802.11 WPA2-PSK: *lengths from 8 to 63 characters*].
- are composed of any combination of upper and lower case letters, numbers,and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")").

FIA_PSK_EXT.1.3 The TSF shall be able to [accept] bit-based pre-shared keys.

6.3.4 User Identification and Authentication (Extended – FIA_UIA_EXT)

6.3.4.1 FIA_UIA_EXT.1 User Identification and Authentication

FIA_UIA_EXT.1.1 The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- [selection: [assignment:*ICMP echo]*].

FIA_UIA_EXT.1.2 The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.

FIA_UIA_EXT.1.3 The TSF shall provide the following remote authentication mechanisms [selection: SSH password, SSH public key] and local authentication mechanisms [selection: password-based].

FIA_UIA_EXT.1.4 The TSF shall authenticate any administrative user's claimed identity according to each authentication mechanism specified in FIA_UIA_EXT.1.3.

6.3.5 User authentication (FIA_UAU) (Extended – FIA_UAU_EX

6.3.5.1 FIA_UAU.7 Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only *obscured feedback* to the **administrative** user while the authentication is in progress **at the local console**.

6.4 Security Management (FMT)

6.4.1 Specification of Management Functions (FMT_SMF)

6.4.1.1 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- *Ability to administer the TOE remotely;*
- *Ability to configure the access banner;*
- *Ability to configure the remote session inactivity time before session termination;*
- *Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates;*
- *[selection:*

- Ability to configure audit behaviour (e.g., changes to storage locations for audit; changes to behaviour when local audit storage space is full);
- Ability to modify the behaviour of the transmission of audit data to an external IT entity;
- Ability to configure local audit behaviour (e.g., changes to storage locations for audit; changes to behaviour when local audit storage space is full, changes to local audit storage size);
- Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1;
- Ability to manage the cryptographic keys;
- Ability to configure the cryptographic functionality;
- Ability to configure thresholds for SSH rekeying;
- Ability to configure the lifetime for IPsec SAs;
- Ability to configure the list of supported (D)TLS ciphers;
- Ability to configure the interaction between TOE components;
- Ability to re-enable an Administrator account;
- Ability to set the time which is used for time-stamps;
- Ability to configure NTP;
- Ability to configure the reference identifier for the peer;
- Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;
- Ability to administer the TOE locally.
- Ability to configure the local session inactivity time before session termination or locking
- Ability to configure the authentication failure parameters for FIA_AFL.1;
- Ability to manage the trusted public keys database;
- No other capabilities.*]*.

6.4.2 Security management roles (FMT_SMR)

6.4.2.1 FMT_SMR.2 Restrictions on security roles

FMT_SMR.2.1 The TSF shall maintain the roles:
- *Security Administrator.*

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions
- *The Security Administrator role shall be able to administer the TOE remotely* are satisfied.

6.5 Protection of the TSF (FPT)

6.5.1 Protection of TSF Data (Extended – FPT_SKP_EXT)

6.5.1.1 FPT_SKP_EXT.1 Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

6.5.2 Protection of Administrator Passwords (Extended – FPT_APW_EXT)

6.5.2.1 FPT_APW_EXT.1 Protection of Administrator Passwords

FPT_APW_EXT.1.1 The TSF shall store administrative passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext administrative passwords.

6.5.3 Trusted Update (FPT_TUD_EXT)

6.5.3.1 FPT_TUD_EXT.1 Trusted Update

FPT_TUD_EXT.1.1 The TSF shall provide [assignment: *Security Administrators*] the ability to query the currently executing version of the TOE firmware/software and [selection: the most recently installed version of the TOE firmware/software].

FPT_TUD_EXT.1.2 The TSF shall provide [assignment: *Security Administrators*] the ability to manually initiate updates to TOE firmware/software and [selection: no other update mechanism].

FPT_TUD_EXT.1.3 The TSF shall provide means to authenticate firmware/software updates to the TOE using a [selection: digital signature] prior to installing those updates.

6.5.4 Time stamps (Extended – FPT_STM_EXT)

6.5.4.1 FPT_STM_EXT.1 Reliable Time Stamps

FPT_STM_EXT.1.1 The TSF shall be able to provide reliable time stamps for its own use.

FPT_STM_EXT.1.2 The TSF shall [selection: allow the Security Administrator to set the time, synchronise time with an NTP server].

6.6 TOE Access (FTA)

6.6.1 TSF-initiated Session Locking (Extended – FTA_SSL_EXT)

6.6.1.1 FTA_SSL_EXT.1 TSF-initiated Session Locking

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [selection: terminate the session] after a Security Administrator-specified time period of inactivity.

6.6.2 Session Locking and Termination (FTA_SSL)

6.6.2.1 FTA_SSL.3 TSF-initiated Termination (Refinement)

FTA_SSL.3.1 The TSF shall terminate **a remote** interactive session after a *Security Administrator-configurable time interval of session inactivity*.

6.6.2.2 FTA_SSL.4 User-initiated Termination (Refinement)

FTA_SSL.4.1 The TSF shall allow ~~user~~ **Administrator-**initiated termination of the ~~user's~~ **Administrator's** own interactive session.

6.6.3 TOE Access Banners (FTA_TAB)

6.6.3.1 FTA_TAB.1 Default TOE Access Banners (Refinement)

FTA_TAB.1.1 Before establishing ~~a~~ an administrative user session the TSF shall display a Security Administrator-specified advisory notice and consent warning message regarding ~~unauthorised~~ use of the TOE.

6.7 Trusted Path/Channels (FTP)

6.7.1 Trusted Channel (FTP_ITC)

6.7.1.1 FTP_ITC.1 Inter-TSF Trusted Channel (Refinement)

[EPWLAN]FTP_ITC.1.1 The TSF shall be capable of using **IEEE 802.1X, [selection: IPsec], and [selection: no other protocol] to** provide a trusted communication channel between itself and **authorized IT entities** supporting the following capabilities**: 802.1X authentication server,** audit server**, [selection:** authentication server **, [assignment:** *NTP server*]] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

[EPWLAN]FTP_ITC.1.2 The TSF shall permit the TSF or the authorized IT entities to initiate

communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*assignment: audit service, authentication service, 802.1x authentication service and NTP service*].

6.7.2 Trusted Path (FTP_TRP)

6.7.2.1 FTP_TRP.1/Admin Trusted Path (Refinement)

FTP_TRP.1.1/Admin The TSF shall **be capable of using [selection: SSH] to** provide a communication path between itself and **authorized** remote **Administrators** ~~users~~ that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure **and provides detection of modification of the channel data**.

FTP_TRP.1.2/Admin The TSF shall permit remote **Administrators** ~~users~~ to initiate communication via the trusted path.

FTP_TRP.1.3/Admin The TSF shall require the use of the trusted path for *initial Administrator authentication and all remote administration actions*.

6.8 Selection-Based Requirements

6.8.1 Cryptographic Support (FCS)

6.8.1.1 FCS_IPSEC_EXT.1 IPsec Protocol

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC 4301.

FCS_IPSEC_EXT.1.2 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched and discards it.

FCS_IPSEC_EXT.1.3 The TSF shall implement [selection: tunnel mode, transport mode].

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms [selection: AES-GCM-128 (RFC 4106), AES-GCM-192 (RFC 4106), AES-GCM-256 (RFC 4106)] together with a Secure Hash Algorithm (SHA)-based HMAC [selection: *no HMAC algorithm*].

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [selection:

- IKEv2 as defined in RFC 7296 and [selection: with mandatory support for NAT traversal as specified in RFC 7296, section 2.23)], and [selection: RFC 4868 for hash functions]

].

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [selection: IKEv2] protocol uses the cryptographic algorithms [selection: AES-GCM-128, AES-GCM-192, AES-GCM-256 (specified in RFC 5282)]

FCS_IPSEC_EXT.1.7 The TSF shall ensure that [selection:

- IKEv2 SA lifetimes can be configured by a Security Administrator based on [selection: length of time, where the time values can be configured within [assignment: *1-24*] hours

].

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [selection:

- IKEv2 Child SA lifetimes can be configured by a Security Administrator based on
  [selection:
  - number of bytes;
  - length of time, where the time values can be configured within [assignment: *1-8*] hours;

]

FCS_IPSEC_EXT.1.9 The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange ("x" in g^x mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least [assignment: *256 (for DH Group 19), 256 (for DH Group 24), 384 (for DH Group 20)*] bits.

FCS_IPSEC_EXT.1.10 The TSF shall generate nonces used in [selection: IKEv2] exchanges of length [selection: at least 128 bits in size and at least half the output size of the negotiated pseudorandom function (PRF) hash].

FCS_IPSEC_EXT.1.11 The TSF shall ensure that IKE protocols implement DH Group(s) [selection:

- [selection: 19 (256-bit Random ECP), 20 (384-bit Random ECP), 24 (2048-bit MODP with 256-bit POS)] according to RFC 5114.

].

FCS_IPSEC_EXT.1.12 The TSF shall be able to ensure that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [selection: IKEv2 IKE_SA] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [selection: IKEv2 CHILD_SA] connection.

FCS_IPSEC_EXT.1.13 The TSF shall ensure that all IKE protocols perform peer authentication using [selection: RSA, ECDSA] that use X.509v3 certificates that conform to RFC 4945 and [selection: Pre-shared Keys].

FCS_IPSEC_EXT.1.14 The TSF shall only establish a trusted channel if the presented identifier in the received certificate matches the configured reference identifier, where the presented and reference identifiers are of the following fields and types: [selection: SAN: IP address, SAN: Fully Qualified Domain Name (FQDN) and [selection: no other reference identifier type].

6.8.1.2 FCS_NTP_EXT.1 NTP Protocol

FCS_NTP_EXT.1.1 The TSF shall use only the following NTP version(s) [selection: NTP v3 (RFC 1305), NTP v4 (RFC 5905)].

FCS_NTP_EXT.1.2 The TSF shall update its system time using [selection:

- Authentication using [selection: SHA256, SHA384, SHA512] as the message digest algorithm(s);
- [selection: IPsec] to provide trusted communication between itself and an NTP time source.

].

FCS_NTP_EXT.1.3 The TSF shall not update NTP timestamp from broadcast and/or multicast addresses.

FCS_NTP_EXT.1.4 The TSF shall support configuration of at least three (3) NTP time sources in the Operational Environment.

6.8.1.3 FCS_SSH_EXT.1 SSH Protocol

FCS_SSH_EXT.1.1 The TOE shall implement SSH acting as a [**selection:** server] in accordance with that complies with RFCs 4251, 4252, 4253, 4254, [**selection:** 4256, 4344, 5647, 5656, 6668] and [no other standard].

FCS_SSH_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods: [**selection:**

- "password" (RFC 4252),
- publickey (RFC 4252): [**selection:**
  - ecdsa-sha2-nistp256 (RFC 5656),
  - ecdsa-sha2-nistp384 (RFC 5656),
  ]

] and no other methods.

FCS_SSH_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [**assignment:** *256k*] bytes in an SSH transport connection are dropped.

FCS_SSH_EXT.1.4 The TSF shall protect data in transit from unauthorised disclosure using the following mechanisms: [**selection:**

- AEAD_AES_128_GCM (RFC 5647),
- AEAD_AES_256_GCM (RFC 5647),
- aes128-gcm@openssh.com (RFC 5647),
- aes256-gcm@openssh.com (RFC 5647)

] and no other mechanisms.

FCS_SSH_EXT.1.5 The TSF shall protect data in transit from modification, deletion, and insertion using: [**selection:**

- AEAD_AES_128_GCM (RFC 5647),
- AEAD_AES_256_GCM (RFC 5647),
- Implicit

] and no other mechanisms.

FCS_SSH_EXT.1.6 The TSF shall establish a shared secret with its peer using: [**selection:**

- ecdh-sha2-nistp256 (RFC 5656),
- ecdh-sha2-nistp384 (RFC 5656)

] and no other mechanism.

FCS_SSH_EXT.1.7 The TSF shall use SSH KDF as defined in [**selection:**

- RFC 5656 (Section 4)

] to derive the following cryptographic keys from a shared secret: session keys.

FCS_SSH_EXT.1.8 The TSF shall ensure that [**selection:**

- A rekey of the session keys,

] occurs when any of the following thresholds are met:

- One hour connection time
- No more than one gigabyte of transmitted data, or
- No more than one gigabyte of received data.

6.8.1.4 FCS_SSHS_EXT.1 SSH Protocol – Server

FCS_SSHS_EXT.1.1 The TSF shall authenticate itself to its peer (SSH Client) using: [**selection:**

- ecdsa-sha2-nistp256 (RFC 5656),
- ecdsa-sha2-nistp384 (RFC 5656),

].

6.8.1.5 FCS_DTLSC_EXT.1 DTLS Client Protocol Without Mutual Authentication

FCS_DTLSC_EXT.1.1 The TSF shall implement [selection: DTLS 1.2 (RFC 6347)] supporting the following ciphersuites: [selection:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

].

FCS_DTLSC_EXT.1.2 The TSF shall verify that the presented identifier matches [selection: the identifier per RFC 5280 Appendix A using [selection: id-at-title] and no other attribute types].

FCS_DTLSC_EXT.1.3 The TSF shall not establish a trusted channel if the server certificate is invalid. [selection: without any administrator override mechanism].

FCS_DTLSC_EXT.1.4 The TSF shall [selection: present the Supported Groups Extension with the following curves/groups: [selection: secp256r1, secp384r1, secp521r1] and no other curves/groups] in the Client Hello.

FCS_DTLSC_EXT.1.5 The TSF shall [selection: present the signature_algorithms extension with support for the following algorithms: [selection:

- rsa_pkcs1 with sha256 (0x0401)
- rsa_pkcs1 with sha384 (0x0501)
- rsa_pkcs1 with sha512 (0x0601)
- ecdsa_secp256r1 with sha256 (0x0403)
- ecdsa_secp384r1 with sha384 (0x0503)
- ecdsa_secp521r1 with sha512 (0x0603)
- rsa_pss_rsae with sha256 (0x0804)
- rsa_pss_rsae with sha384 (0x0805)
- rsa_pss_rsae with sha512 (0x0806)] and no other signature_Schemes

].

FCS_DTLSC_EXT.1.6 The TSF [selection: does not provide] the ability to configure the list of supported ciphersuites as defined in FCS_DTLSC_EXT.1.1.

FCS_DTLSC_EXT.1.7 The TSF shall prohibit the use of the following extensions:

- Early data extension

- Post-handshake client authentication according to RFC 9147, Section 5.8.4.

FCS_DTLSC_EXT.1.8 The TSF shall [selection: not use PSKs].

FCS_DTLSC_EXT.1.9 The TSF shall [selection: reject [selection: DTLS 1.2, DTLS 1.3] renegotiation attempts].

FCS_DTLSC_EXT.1.10 The TSF shall [selection: terminate the DTLS session] if a message received contains an invalid MAC.

FCS_DTLSC_EXT.1.11 The TSF shall detect and silently discard replayed messages for:

- DTLS records previously received;
- DTLS records too old to fit in the sliding window.

6.8.1.6 FCS_DTLSS_EXT.1 DTLS Server Protocol Without Mutual Authentication

FCS_DTLSS_EXT.1.1 The TSF shall implement [selection: DTLS 1.2 (RFC 6347)] and reject all other DTLS versions. The DTLS implementation will support the following ciphersuites: [selection:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

] and no other ciphersuites.

FCS_DTLSS_EXT.1.2 The TSF shall not proceed with a connection handshake attempt if the DTLS server cannot successfully validate the cookie returned by the DTLS Client.

FCS_DTLSS_EXT.1.3 The TSF shall authenticate itself using X.509 certificate(s) using [selection: *RSA with key size [selection: 3072, 4096] bits; ECDSA over NIST curves [selection: secp256r1, secp384r1, secp521r1] and no other curves*].

FCS_DTLSS_EXT.1.4 The TSF shall perform key exchange using [selection:

- EC Diffie-Hellman key agreement over NIST curves [selection: secp256r1, secp384r1, secp521r1] and no other curves].

].

FCS_DTLSS_EXT.1.5 The TSF shall [selection: silently discard the record] if a message received contains an invalid MAC.

FCS_DTLSS_EXT.1.6 The TSF shall detect and silently discard replayed messages for:

- DTLS records previously received.
- DTLS records too old to fit in the sliding window.

FCS_DTLSS_EXT.1.7 The TSF shall support [selection: no session resumption or session tickets].

FCS_DTLSS_EXT.1.8 The TSF [selection: *provides*] the ability to configure the list of supported ciphersuites as defined in FCS_DTLSS_EXT.1.1.

FCS_DTLSS_EXT.1.9 The TSF shall prohibit the use of the following extensions:

- Early data extension

FCS_DTLSS_EXT.1.10 The TSF shall [selection: *not use PSKs*].

FCS_DTLSS_EXT.1.11 The TSF shall [selection: reject [selection: DTLS 1.2, DTLS 1.3]

renegotiation attempts].

6.8.1.7 FCS_TLSC_EXT.1 TLS Client Protocol Without Mutual Authentication

FCS_TLSC_EXT.1.1 The TSF shall implement [selection: TLS 1.2 (RFC 5246)] supporting the following ciphersuites::

[selection:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

] and no other ciphersuites.

FCS_TLSC_EXT.1.2 The TSF shall verify that the presented identifier matches [selection: the identifier per RFC 5280 Appendix A using [selection: id-at-title] and no other attribute types].

FCS_TLSC_EXT.1.3 The TSF shall not establish a trusted channel if the server certificate is invalid [selection: without any administrator override mechanism].

FCS_TLSC_EXT.1.4 The TSF shall [selection: present the Supported Groups Extension with the following curves/groups: [selection: secp256r1, secp384r1, secp521r1] and no other curves/groups] in the Client Hello.

FCS_TLSC_EXT.1.5 The TSF shall [selection:

- Present the signature_algorithms extension with support for the following algorithms: [selection:
  - rsa_pkcs1 with sha256(0x0401),
  - rsa_pkcs1with sha384(0x0501),
  - rsa_pkcs1 with sha512(0x0601),
  - ecdsa_secp256r1 with sha256(0x0403),
  - ecdsa_secp384r1 with sha384(0x0503),
  - ecdsa_secp521r1 with sha512(0x0603),
  - rsa_pss_rsae with sha256(0x0804),
  - rsa_pss_rsae with sha384(0x0805),
  - rsa_pss_rsae with sha512(0x0806),] and no other algorithms;]

FCS_TLSC_EXT.1.6 The TSF [selection: does not provide] the ability to configure the list of supported ciphersuites as defined in FCS_TLSC_EXT.1.1.

FCS_TLSC_EXT.1.7 The TSF shall prohibit the use of the following extensions:

- Early data extension
- Post-handshake client authentication according to RFC 8446, Section 4.2.6.

FCS_TLSC_EXT.1.8 The TSF shall [selection: not use PSKs].

FCS_TLSC_EXT.1.9 The TSF shall [selection: reject [selection: TLS 1.2, TLS 1.3] renegotiation attempts].

6.8.1.8 FCS_TLSS_EXT.1 TLS Server Protocol Without Mutual Authentication

FCS_TLSS_EXT.1.1 The TSF shall implement [selection: TLS 1.2 (RFC 5246)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

[selection:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

] and no other ciphersuites.

FCS_TLSS_EXT.1.2 The TSF shall authenticate itself using X.509 certificate(s) using [selection: RSA with key size [selection: 3072, 4096] bits; ECDSA over NIST curves [selection: secp256r1, secp384r1, secp521r1] and no other curves].

FCS_TLSS_EXT.1.3 The TSF shall perform key exchange using: [selection:

- EC Diffie-Hellman key agreement over NIST curves [selection: secp256r1, secp384r1, secp521r1] and no other curves;

]

FCS_TLSS_EXT.1.4 The TSF shall support [selection: no session resumption].

FCS_TLSS_EXT.1.5 The TSF [selection: *provides*] the ability to configure the list of supported ciphersuites as defined in FCS_TLSS_EXT.1.1.

FCS_TLSS_EXT.1.6 The TSF shall prohibit the use of the following extensions:

- Early data extension.

FCS_TLSS_EXT.1.7 The TSF shall [selection: *not use PSKs*].

FCS_TLSS_EXT.1.8 The TSF shall [selection: reject [selection: TLS 1.2, TLS 1.3] renegotiation attempt*s*].

6.8.2 Identification and Authentication (FIA)

6.8.2.1 FIA_X509_EXT.1/Rev X.509 Certificate Validation

FIA_X509_EXT.1.1/Rev The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation **supporting a minimum path length of three certificates**.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [selection: a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3, Certificate Revocation List (CRL) as specified in RFC 5759 Section 5].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - *Certificates used for trusted updates and executable code integrity verification shall have*

the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.

- *Server certificates presented for DTLS/TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.*
- *Client certificates presented for DTLS/TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.*
- *OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.*

FIA_X509_EXT.1.2/Rev The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

6.8.2.2 FIA_X509_EXT.1/ITT X.509 Certificate Validation

FIA_X509_EXT.1.1/ITT The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation **supporting a minimum path length of two certificates**.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [selection: a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3, Certificate Revocation List (CRL) as specified in RFC 5759 Section 5].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - *Server certificates presented for DTLS/TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.*
  - *Client certificates presented for DTLS/TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.*
  - *OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.*

FIA_X509_EXT.1.2/ITT The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

6.8.2.3 FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [selection: DTLS, IPsec, TLS] and [selection: no additional uses].

FIA_X509_EXT.2.2 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [selection: not accept the certificate].

6.8.2.4 FIA_X509_EXT.3 X.509 Certificate Requests

FIA_X509_EXT.3.1 The TSF shall generate a Certificate Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [selection: Common Name, Organization, Organizational Unit, Country].

FIA_X509_EXT.3.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

6.8.3 Communication (FCO)

6.8.3.1 FCO_CPC_EXT.1 Component Registration Channel Definition

FCO_CPC_EXT.1.1 The TSF shall require a Security Administrator to enable communications between any pair of TOE components before such communication can take place.

FCO_CPC_EXT.1.2 The TSF shall implement a registration process in which components establish and use a communications channel that uses [selection: A channel that meets the secure channel requirements in [selection: FPT_ITT.1] for at least *TSF data*.

FCO_CPC_EXT.1.3 The TSF shall enable a Security Administrator to disable communications between any pair of TOE components.

6.8.4 Security Management (FMT)

6.8.4.1 FMT_MOF.1/Functions Management of Security Functions Behaviour

FMT_MOF.1.1/Functions	The TSF shall restrict the ability to [selection: modify the behaviour of] the functions [selection: transmission of audit data to an external IT entity] to Security Administrators.

6.8.4.2 FMT_MOF.1/ManualUpdate Management of Security Functions Behaviour

FMT_MOF.1.1/ ManualUpdate	The TSF shall restrict the ability to enable the functions *to perform manual updates to Security Administrators*.

6.8.4.3 FMT_MTD.1/CoreData Management of TSF Data

FMT_MTD.1.1/ CoreData	The TSF shall restrict the ability to manage the *TSF data to Security Administrators*.

6.8.4.4 FMT_MTD.1/CryptoKeys Management of TSF Data

FMT_MTD.1.1/CryptoKeys	The TSF shall restrict the ability to *manage* the *cryptographic keys* to *Security Administrators.*

6.8.5 Protection of the TSF (FPT)

6.8.5.1 FPT_ITT.1 Basic internal TSF data transfer protection (Refinement)

FPT_ITT.1.1 The TSF shall protect TSF data from disclosure and **detect its modification** when it is transmitted between separate parts of the TOE **through the use of [selection: TLS, DTLS]**.

6.9 Extended Package Requirements

6.9.1 Security Audit (FAU)

6.9.1.1 FAU_GEN_EXT.1 Security Audit Generation

FAU_GEN_EXT.1.1 The TSF shall be able to generate audit records for each TOE component. The audit records generated by the TSF of each TOE component shall include the subset of security relevant audit events which can occur on the TOE component.

6.9.1.2 FAU_STG_EXT.4 Protected Local Audit Event Storage for Distributed TOEs

FAU_STG_EXT.4.1 The TSF of each TOE component which stores security audit data locally shall perform the following actions when the local storage space for audit data is full: [assignment: *access controller and for each component its action chosen according to the following*: [selection: overwrite previous audit records according to the following rule: [assignment: *oldest audit record is overwritten*],]].

6.9.1.3 FAU_STG_EXT.5 Protected Remote Audit Event Storage for Distributed TOEs

FAU_STG_EXT.5.1 Each TOE component which does not store security audit data locally shall be able to buffer security audit data locally until it has been transferred to another TOE component that stores or forwards it. All transfer of audit records between TOE components shall use a protected channel according to [selection: FPT_ITT.1].

6.9.2 Cryptographic Support (FCS)

6.9.2.1 Cryptographic Operation (AES Data Encryption/Decryption)

FCS_COP.1.1/DataEncryption

The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm Advanced Encryption Standard

(AES) used in ~~**Cipher Block Chaining (CBC),**~~ **CCM mode Protocol (CCMP),** and [**selection**: Galois-Counter Mode (GCM), **GCMP**] **modes** and cryptographic key sizes **256 bits(IPsec, TLS, DTLS and SSH) and** [**selection**: 128 bits**(IPsec, TLS,DTLS, wifi,and SSH)**, 192 bits**(IPsec and wifi)**] that meet the following: AES as specified in ISO 18033-3~~**, CBC as specified in ISO 10116,**~~ **CCMP as specified in NIST SP 800-38C and IEEE 802.11-2020,** [**selection**: GCM as specified in ISO 19772, **GCMP as specified in NIST SP 800-38D and IEEE 802.11ax-2021**].

6.9.3 Protection of the TSF (FPT)

6.9.3.1 FPT_TST_EXT.1 TSF Testing

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests **during initial start-up (on power on) and [selection**: at the request of the authorized user] to demonstrate the correct operation of the TSF: **integrity verification of stored TSF executable code when it is loaded for execution through the use of the TSF-provided cryptographic service specified in FCS_COP.1/SigGen, [selection: [assignment:AES,SHA,HMAC,RSA,ECDSA and DRBG]**.

[PP-ND]FPT_TST_EXT.1.2 The TSF shall respond to [selection: [assignment: *Cryptographic algorithm power-on self-test failure]*] by [selection: rebooting]

6.9.4 Security Audit (FAU)

6.9.4.1 FAU_GEN.1/WLAN Audit Data Generation

FAU_GEN.1.1/WLAN The TSF shall be able to generate an audit record of the following auditable events:

a. Start-up and shutdown of the audit functions;

b. All auditable events for the [not specified] level of audit; and

c. [Auditable events listed in the Auditable Events table (Table 7)

d. Failure of wireless sensor communication]

Requirement	**Auditable Events**	**Additional Audit Record Contents**
FCS_CKM.1/WPA	None.	None.
FCS_CKM.2/GTK	None.	None.

FCS_CKM.2/PMK	None.	None.
FIA_8021X_EXT.1	Attempts to access the 802.1X controlled port prior to successful completion of the authentication exchange.	Provided client identity (e.g., Media Access Control [Media Access Control (MAC)] address).
	Failed authentication attempt.	Provided client identity (e.g., MAC address).
FIA_PSK_EXT.1 (selectionbased)	None.	None.
FIA_UAU.6	Attempts to re-authenticate.	Origin of the attempt (e.g., IP address).
FMT_SMF.1/AccessSystem	None.	None.
FMT_SMR_EXT.1	None.	None.
FPT_FLS.1	Failure of the TSF.	Indication that the TSF has failed with the type of failure that occurred.
FPT_TST_EXT.1	Execution of TSF self-test.	None.
	Detected integrity violations.	The TSF code file that caused the integrity violation.
FTA_TSE.1	Failure of the TSF.	Indication that the TSF has failed with the type of failure that occurred.
FTP_ITC.1	Failed attempts to establish a trusted channel (including IEEE 802.11).	Identification of the initiator and target of channel.
	Detection of modification of channel data.	None.

Table 7: Auditable Events

6.9.5 Cryptographic Support (FCS)

6.9.5.1 FCS_CKM.1/WPA Cryptographic Key Generation (Symmetric Keys for WPA2 Connections)

FCS_CKM.1.1/WPA The TSF shall generate **symmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm [PRF-384 and [**selection**: PRF-704] and specified cryptographic key sizes [256 bits and [**selection**: 128 bits]] **using a Random Bit Generator as specified in FCS_RBG_EXT.1** that meet the following: [IEEE 802.11-2020 and [**selection**: IEEE 802.11ax-2021].

6.9.5.2 FCS_CKM.2/GTK Cryptographic Key Distribution (GTK)

FCS_CKM.2.1/GTK	The TSF shall distribute **GTK** in accordance with a specified cryptographic key distribution method: [**selection**: AES Key Wrap with Padding in an EAPOL-Key frame] that meets the following: [NIST SP 800-38F, IEEE 802.11-2020 for the packet format and timing considerations] **and does not expose the cryptographic keys**.

6.9.5.3 FCS_CKM.2/PMK Cryptographic Key Distribution (PMK)

FCS_CKM.2.1/PMK	The TSF shall **receive the 802.11 PMK** in accordance with a specified cryptographic key distribution method: [from 802.1X Authorization Server] that meets the following: [IEEE 802.11-2020] **and does not expose the cryptographic keys**.

6.9.6 Identification and Authentication

6.9.6.1 FIA_8021X_EXT.1 802.1X Port Access Entity (Authenticator) Authentication

FIA_8021X_EXT.1.1	The TSF shall conform to IEEE Standard 802.1X for a Port Access Entity (PAE) in the "Authenticator" role.
FIA_8021X_EXT.1.2	The TSF shall support communications to a RADIUS authentication server conforming to RFCs 2865 and 3579.
FIA_8021X_EXT.1.3	The TSF shall ensure that no access to its 802.1X controlled port is given to the wireless client prior to successful completion of this authentication exchange.

6.9.6.2 FIA_UAU.6 Re-Authenticating

FIA_UAU.6.1	The TSF shall re-authenticate the **administrative** user under the conditions [when the user changes their password, [**selection**: following TSF-initiated session locking].

6.9.7 Security Management (FMT)

6.9.7.1 FMT_SMF.1/AccessSystem Specification of Management Functions (WLAN Access Systems)

FMT_SMF.1.1/AccessSystem The TSF shall be capable of performing the following management functions:

- Configure the security policy for each wireless network, including:
  - Security type
  - Authentication protocol
  - Client credentials to be used for authentication
  - Service Set Identifier (SSID)
  - If the SSID is broadcasted
  - Frequency band set to [**selection**: 2.4 GHz, 5 GHz,6 GHz]
  - Transmit power level

6.9.7.2 FMT_SMR_EXT.1 No Administration from Client

FMT_SMR_EXT.1.1 The TSF shall ensure that the ability to administer remotely the TOE from a wireless client shall be disabled by default.

6.9.8 Protection of the TSF (FPT)

6.9.8.1 FPT_FLS.1 Failure with Preservation of Secure State

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [failure of the self-tests].

6.9.9 TOE Access (FTA)

6.9.9.1 FTA_TSE.1 TOE Session Establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment **of a wireless client session** based on [TOE interface, time, day, [selection*: [assignment: no other attributes]*]].

6.9.10 Trusted Path/Channels (FTP)

6.9.10.1 FTP_ITC.1/Client Inter-TSF Trusted Channel (WLAN Client Communications)

FTP_ITC.1.1/Client The TSF shall be capable of using WPA3-Enterprise, WPA2-Enterprise and [**selection**: WPA3-SAE, WPA2-PSK] as defined by IEEE 802.11-2020 to provide a trusted communication channel between itself and WLAN clients that is logically distinct from other

	communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.
FTP_ITC.1.2/Client	The TSF shall permit the authorized IT entities to initiate communication via the trusted channel.
FTP_ITC.1.3/Client	The TSF shall initiate communication via the trusted channel for [no services].

7 Security Assurance Requirements

The description of the SARs is an exact copy of the Network Devices PP [PP-ND] Section 7.

8 TOE Summary Specification

8.1 Security audit

FAU_GEN.1, FAU_GEN.2, FAU_GEN_EXT.1, FAU_GEN.1/WLAN:

The TOE is designed to be able to generate log records for a wide range of security relevant and other events as they occur. The events that can cause an audit record to be logged include starting and stopping the audit function as well as all of the events identified in Table .

1)Administrative login and logout (including the name of the user account).

2)Enabling and disabling communications between a pair of components.

3)Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).

4)Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference is logged).

5)Resetting passwords (name of related user account is logged).

6)Attempts to initiate a TOE update.

7)Modification of the behavior of the transmission of audit data to an external IT entity.

APs generate audit records for the security relevant audit events which occur on that device and send these to the AC via the CAPWAP tunnel.

In general, the logged audit records identify the date and time, the nature or type of the triggering event, an indication of whether the event succeeded, failed or had some other outcome, and the identity of the agent (e.g., user) responsible for the event. The logged audit records also include event-specific content that includes at least all of the content required in Table .

FAU_STG.1:

The internal log can be accessed only by a user with the network-admin, network-operator,security-audit role , who can review, or archive stored audit records using available CLI commands specifically designed for the management of the internal LOG.only network-admin and security-audit user can delete log. The functions available to review audit records allow the audit records to be sorted in forward or reverse order according to date/time and to be searched using regular expressions.AP's audit log send to AC through capwap tunnel.

FAU_STG_EXT.1:

The TOE includes an internal log implementation that can be used to store and review audit records locally. The TOE can be configured to send generated audit records to an external Audit server in to mitigate the possibility of losing audit records.

Audit records generated by the AP are sent to the AC, where they are stored and then forwarded to the remote audit server. If the connection between the AP and the controller is lost, logs will continue to be stored on the AP. Once the connection is restored, the AP can automatically send the logs to the AC. Logs are not persistently stored after an AP restart.

The TOE uses IPsec to protect the communication channel with the remote audit server and DTLS to protect the communication channel between the AC and the AP. If an external audit server is enabled, all audit logs are written simultaneously (in real-time) to both the local audit log on the AC and the audit server. The local audit log and the logs sent to the remote server are the same.

For audit records stored locally on the AC, the minimum logs size is 1MB. The local AC log storage uses a new-over-oldest method, so when available space is exhausted, the audit logs will be overwritten.

FAU_STG_EXT.4, FAU_STG_EXT.5: AP buffers audit records for transmission to AC for storage. If the buffer is full, the oldest audit records will be overwritten. The transmission of audit records to the AC is conducted over a DTLS-protected channel, according to FPT_ITT.1.

FMT_MOF.1.1/Functions: The security administrator can configure and modify the local audit log to be sent to the audit server using the "info-center loghost" command.

8.2 Cryptographic support

The TOE includes a crypto-module providing supporting cryptographic functions.

FCS_CKM.1 For asymmetric key pairs used for authentication, the TOE can generate RSA (3072, and 4096 bits) and ECDSA (P-256, P-384, and P-521) pair-wise keys. Additionally, the administrator can load and remove user SSH public keys that the TOE will use to authenticate SSH clients.

FCS_CKM.2 Key Exchange Mechanism, The TOE supports generating temporary ECDH and DH key pairs for TLS/DTLS, IPsec, and SSHv2 for use in the key exchange process.

TLS/DTLS key exchange: The TOE uses the temporary Elliptic Curve Diffie-Hellman (ECDH) key agreement protocol, supporting the following curves: secp256r1 (P-256), secp384r1 (P-384), secp521r1 (P-521)

IPsec key exchange: In IKEv2, the TOE uses temporary ECDH keys (supporting group 19 [NIST P-256], group 20 [NIST P-384]) and DH keys (group 24).

SSHv2 key exchange: TOE uses a mutually agreed key exchange algorithm (supporting ecdh-sha2-nistp256, ecdh-sha2-nistp384) during the SSH login process to generate a temporary key pair, which is used to produce the subsequent shared key. All key exchanges use temporary keys to provide forward secrecy.

Scheme	SFR	Service
DH	FCS_IPSEC_EXT.1	Protect the transmission of audit logs, authentication messages, and NTP messages.
ECDH	FCS_IPSEC_EXT.1	Protect the transmission of audit logs, authentication messages, and NTP messages.
ECDH	FCS_SSH_EXT.1	SSH Remote administration
ECDH	FCS_SSHS_EXT.1	SSH Remote administration

ECDH	FCS_DTLSC_EXT.1	AP communicates with AC
ECDH	FCS_DTLS_EXT.1	AP communicates with AC
ECDH	FCS_TLSC_EXT.1	AP communicates with AC
ECDH	FCS_TLSS_EXT.1	AP communicates with AC

FCS_COP.1/DataEncryption: The TOE encryption algorithm supports the GCM mode of AES as available ciphers, and all with key size 128, 192, and 256-bit. which are implemented in the TLS, DTLS, SSH and IPsec protocols. Wireless use AES (CCMP and GCMP) algorithms, with encryption key lengths of 128 bits and 192bits.

Since NDcPP 3.0e no longer requires the implementation of FCS_IPSEC_EXT.1 CBC, Therefore, this SFR does not select CBC.

FCS_COP.1/Hash: The TOE performs SHA-256, SHA-384, and SHA-512 cryptographic hashing services in accordance with ISO/IEC 10118-3:2004. The SHA hash algorithm is used as part of HMAC, but is also used as part of RSA and ECDSA digital signature creation and verification.

FCS_COP.1/KeyedHash: The TOE HMAC algorithms supports the HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512.

Algorithm	Block Size	Key Size	Digest Size
HMAC-SHA256	512 bits	256 bits	256 bits
HMAC-SHA384	1024 bits	384 bits	384 bits
HMAC-SHA512	1024 bits	512 bits	512 bits

FCS_COP.1/SigGen: The TOE supports both RSA(modulus **3072** bits or greater) and ECDSA(p-256,P-384,p-521) signing and verification. The TOE verifies RSA signatures on firmware updates and supports RSA and ECDSA authentication during TLS/DTLS, SSH and IPsec.

FCS_RBG_EXT.1: The TOE Component implements a random bit generator (RBG) based on the AES-256 block cipher, in accordance with ISO/IEC 18031:2011. This DRBG is seeded with a software entropy source that provides with a minimum of [256 bits of entropy to the DRBG. The noise sources includes the following:

- Compute timing jitter (CPU instruction-level latency)
- Memory bus contention (cache miss timing deviation)
- Interrupt event entropy (hardware interrupt response time variation)

FCS_NTP_EXT.1: The TOE provides the ability to synchronize its time with a NTP server using NTP v3 and v4. The time data is protected by SHA256, SHA384, and SHA512. The TOE updates its system time using IPsec to provide trusted communication between itself and an NTP time source.

FCS_SSH_EXT.1.1

The TOE supports SSHv2 interactive command-line secure administrator sessions. The TOE implements the SSHv2 protocol, compliant to the following RFCs: 4251, 4252, 4253, 4254, 4256, 4344, 5647, 5656, 6187, 6668.

FCS_SSH_EXT.1.2

The TOE supports public key-based, X.509 certificate-based, and password-based authentication. The TOE allows use of the ecdsa-sha2-nistp256, ecdsa-sha2-nistp384 algorithms for public key authentication and X.509 certificate-based authentication. The TOE establishes a user identity when an SSH client presents a valid public key, a valid X.509 certificate, or correct password.

FCS_SSH_EXT.1.3

The TOE continuously receives data from the network, with a buffer threshold of 256KB. It uses a "cumulative calculation + forced discard" processing strategy. When the amount of unprocessed data exceeds 256KB due to insufficient processing capacity or other reasons, the protection mechanism is triggered, and subsequent incoming network packets will be actively discarded until the backlog is processed below the threshold, at which point the system will resume receiving.

FCS_SSH_EXT.1.4

The TOE supports AEAD_AES_128_GCM, AEAD_AES_256_GCM, aes128-gcm@openssh.com and aes256-gcm@openssh.com for both encryption and data integrity.

FCS_SSH_EXT.1.5

The TOE protect data in transit from modification, deletion, and insertion using AEAD_AES_128_GCM (RFC 5647), AEAD_AES_256_GCM (RFC 5647), Implicit.

FCS_SSH_EXT.1.6

The TOE uses ecdh-sha2-nistp256/384 for SSHv2 key exchange.

FCS_SSH_EXT.1.7

The TOE use SSH KDF as defined in RFC 5656 (Section 4) to derive the following cryptographic keys from a shared secret: session keys.

FCS_SSH_EXT.1.8

Rekeying based on time, with a range of 30 to 60 minutes, configured by the user.

Rekeying based on data traffic, with a range of 512 to 1024 MB, configured by the user.

FCS_IPSEC_EXT.1.1

The TOE includes an implementation of IPsec/IKEv2 in accordance with RFC 2407, 2408, 2409, 3526, 3602, 4106, 4109, 4301, 4303, 4868, 4945, 5114, 5996.

The process described for IPsec packet processing applies to both initial packets (before an SA is established) and packets that are already part of an established SA, with the following distinctions:

Before the IPsec connection establishment is successful, if packets matching the IPsec policy, they will be directly discarded and not cached. Once the SA is established, subsequent packets matching the IPsec policy are processed using the relevant SA parameters (encryption, authentication) and flow through the IPsec tunnel.

An IPsec policy set can contain multiple entries, each with a different access list (ACL). The IPsec policy entries are searched in a sequence - the TOE attempts to match the packet to the ACL specified in that entry.

The traffic matching the permit IPsec policy ACL would then flow through the IPsec tunnel and be classified as "PROTECTED".

Traffic that does not match a permit IPsec policy ACL and is also blocked by packet filter ACL on the interface would be DISCARDED.

Traffic that does not match a permit ACL in the IPsec policy, but that is not disallowed by packet filter ACLs on the interface is allowed to BYPASS the tunnel.

FCS_IPSEC_EXT.1.3

The TOE supports IPsec in transport mode and tunnel mode.

FCS_IPSEC_EXT.1.4

The IPsec AH and ESP protocol AES-GCM-128, AES-GCM-192 and AES-GCM-256 (as specified by RFC 4106) together with no HMAC algorithm.

FCS_IPSEC_EXT.1.5

The TOE implements IKE2 with support for NAT traversal as defined in RFC 7296 and RFC 4868 for hash functions (HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512).

FCS_IPSEC_EXT.1.6

The encrypted payload in the IKEv2 protocol uses the cryptographic algorithms AES-GCM-128, AES-GCM-192, AES-GCM-256 (specified in RFC 5282).

FCS_IPSEC_EXT.1.7

IKEv2 SA lifetimes can be configured by a Security Administrator based on length of time.

The IKEv2 profile view "sa duration" command is used to configure the lifetime of the IKEv2 SA. Parameter is seconds: The lifetime of the IKEv2 SA, with a value range of 1 to 24 hours.

FCS_IPSEC_EXT.1.8

IKEv2 Child SA lifetimes can be configured by a Security Administrator based on number of bytes or length of time.

In the IPsec policy view, the “sa duration” command is used to configure the lifetime of the IPsec SA. time-based seconds: specifies the time-based lifetime, with a value range of 1 to8 hours. traffic-based kilobytes: specifies the traffic-based lifetime, with a value range of 2560 to 4294967295 kilobytes.

FCS_IPSEC_EXT.1.9

The TOE generates the secret value x used in the IKEv2 Diffie-Hellman key exchange using the FIPS validated RBG specified in FCS_RBG.1 and having possible lengths of 256 bits for DH group 24, 256 bits for DH group 19, and 384 bits for DH group 20. The TOE generates nonces used in the IKEv2 exchanges of 256 bits in size. Nonces are generated using RBG meet the requirements specified in FCS_RBG1 for random bit generation.

FCS_IPSEC_EXT.1.10

The TSF generate nonces used in IKEv2 exchanges of length 256 bits.

FCS_IPSEC_EXT.1.11

During the IKE_SA_INIT exchange phase, the originator uses a "guess" method to speculate on the most likely DH group that the responder will use and sends this guess in the first message. The responder then responds based on the DH group guessed by the originator. If the originator's guess is correct, the IKE_SA_INIT exchange can be completed with just two messages. If the guess is incorrect, the responder will reply with an INVALID_KE_PAYLOAD message, specifying the DH group to be used. Following this, the originator will re-initiate the negotiation using the DH group specified by the responder. This DH guessing mechanism makes the originator's DH group configuration more flexible, allowing it to adapt to different responders. Multiple DH parameters can be configured, with their precedence decreasing in the order of configuration.

FCS_IPSEC_EXT.1.12

In the evaluation configuration of the TOE, ensure the functionality that the symmetric algorithm strength of IKEv2 CHILD_SA negotiation does not exceed the strength of the IKEv2 IKE_SA This functionality is implemented through the built-in IKE/IPsec policy check mechanism. During IKEv2 CHILD_SA negotiation, the TSF automatically compares the key length (strength) of the proposed symmetric algorithm with the strength of the IKEv2 IKE_SA used to protect the negotiation. The negotiation proceeds only when the CHILD_SA algorithm strength is less than or equal to the IKEv2 IKE_SA strength; otherwise, the TSF will reject the establishment of that IKEV2_CHILD_SA.

FCS_IPSEC_EXT.1.13

IKE protocols perform peer authentication using RSA, ECDSA that use X.509v3 certificates that conform to RFC 4945 and Pre-shared Keys. The TOE supports both RSA (modulus 3072 bits or greater) and ECDSA (p-256, P-384, p-521) signing and verification.

Pre-shared Keys: Both parties in the communication authenticate the peer's identity using a shared key. The PSK configured for IKE negotiation on both sides must be the same, otherwise authentication will fail. Whether set in plaintext or ciphertext, the PSK is stored in the configuration file in ciphertext form.

The "pre-shared-key" command in IKEv2 peer view is used to configure the pre-shared key for an IKEv2 peer.

FCS_IPSEC_EXT.1.14

The TOE will only establish a trusted IPsec channel if the presented identifier in the received certificate matches the configured reference identifier, where the presented and reference identifiers are of the following type: IP address and Fully Qualified Domain Name (FQDN) in SAN.

Certificate-based access control policies allow you to authorize access to a device based on the attributes of an authenticated client's certificate. A certificate-based access control policy is a set of access control rules (permit or deny statements), each associated with a certificate attribute group. A certificate attribute group contains multiple attribute rules, each defining a matching criterion for an attribute in the certificate issuer name, subject name, or alternative subject name field. If the corresponding attributes in a certificate meet all the attribute requirements of the attribute set associated with an access control rule, the certificate is considered to match the rule. If there are multiple rules in an access control policy, the rules are traversed in ascending order of their rule numbers. Once the certificate matches a rule, the inspection is immediately terminated and no further rules are checked.

The following conditions describe how a certificate-based access control policy verifies the validity of a certificate:

• If a certificate matches a permit statement, the certificate passes the verification.

• If a certificate matches a deny statement or does not match any statements in the policy, the certificate is regarded invalid.

• If a statement is associated with a non-existing attribute group, or the attribute group does not have attribute rules, the certificate matches the statement.

• If the certificate-based access control policy specified for a security application does not exist, all certificates in the application pass the verification.

A certificate matches an attribute group if it matches all attribute rules in the group.

FCS_DTLSC_EXT & FCS_DTLSS_EXT DTLS & FCS_TLSC_EXT & FCS_TLSS_EXT TLS: DTLS and TLS are used to protect TSF data from disclosure and detect its modification when it is transmitted between AP and AC. AP services as TLS and DTLS client and AC service as TLS and DTLS server.

FCS_DTLSC_EXT.1.1, FCS_DTLSS_EXT.1.1, FCS_TLSC_EXT.1.1, FCS_TLSS_EXT.1.1: TOE supports the following cipher suites:

ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, ECDHE_RSA_WITH_AES_128_GCM_SHA256, ECDHE_RSA_WITH_AES_256_GCM_SHA384

If TOE uses an unsupported or undefined SSL and TLS version, the AC and AP negotiation fails, and the connection cannot be established.

FCS_DTLSC_EXT.1.2: DTLS client and server confirm to DTLS 1.2 (RFC 6347). DTLS session is established only when the server certificate is valid. The AP verify the presented identifier of AC’s certificate using id-at-title.

TLS client and server confirm to TLS 1.2 (RFC 5246). TLS session is established only when the server certificate is valid. The AP verify the presented identifier of AC’s certificate using id-at-title.

TOE supports including the title field when requesting a certificate, so the server certificate issued by the CA will include the title field. When the DTLS client receives the server certificate information, it checks whether the title field in the certificate is a specific value (capwap.dtls.fips). If it is, this rule passes the check.

For example: execute command

[system] pki entity 1

[H3C-pki-entity-1] title capwap.dtls.fips

id-at-title is just one of the checks; the successful connection of AP and AC also requires multiple other checks. The security administrator must manually configure the AP template (The template contains the unique identifier serial-id or MAC address of the AP.) and set up tunnel encryption. AP checks the validity of the certificate. Refer to FCO_CPC_EXT.1.1. After all checks are passed, the AP can successfully connect to the AC.

FCS_DTLSC_EXT.1.4: The TOE supports group extensions with the following curves/groups in the Client Hello message: secp256r1, secp384r1, secp521r1, these functions are enabled by default, matching the curves/groups specified in the imported certificate. If the server uses an ECDSA certificate, we set the ECDSA certificate key curve as the curve for ECDH negotiation, with the two being the same.

The specific correspondences are as follows:

If the ECDSA certificate key is: NID_X9_62_prime256v1, the corresponding negotiated elliptic curve is set to P-256;

If the ECDSA certificate key is: NID_secp384r1, the corresponding negotiated elliptic curve is set to P-384;

If the ECDSA certificate key is: NID_secp521r1, the corresponding negotiated elliptic curve is set to P-521.

FCS_DTLSC_EXT.1.5: TOE supports the signature_algorithms expansion, which is executed by default and is not configurable.

FCS_DTLSC_EXT.1.6: The TSF does not provide the ability to configure the list of supported ciphersuites as defined in FCS_DTLSC_EXT.1.1.

FCS_DTLSC_EXT.1.10: The TOE supports terminate the DTLS session if a message received contains an invalid MAC.

FCS_DTLSC_EXT.1.11: The TOE supports detecting and discarding replayed DTLS packets, such as DTLS records that have been previously received or DTLS records that are too old and fall outside the sliding window.

Sequence Number Verification Mechanism:

- Each DTLS record contains a 16-bit sequence number.
- The sequence number increments in the order of transmission.

The receiver must detect and discard duplicate records (replay attack) or outdated records (out of window range).Sliding Window: the TOE uses a fixed-size bitmap window (default size 64) to track valid sequence numbers:

- Window Top (window_top): The highest sequence number currently received.

- Window Bitmap (window_bitmap): A 64-bit mask that marks which sequence numbers within the window have been received.

Window Range: Valid sequence numbers must satisfy window_top - 64 < seq ⩽ window_top + 1.

FCS_DTLSS_EXT.1.2: The TOE does not provide the ability to verify the client IP. The TOE generates cookies using HMAC-SHA256, with the calculation incorporating the client IP address, timestamp, and server key. Upon receiving a Client Hello message, the TOE verifies the validity of the cookie's HMAC signature.

FCS_DTLSS_EXT.1.3: The TSF shall authenticate itself using X.509 certificate(s) using:

- RSA with key size 3072, 4096 bits;

ECDSA over NIST curves secp256r1, secp384r1, secp521r1.

FCS_DTLSS_EXT.1.4: The TSF shall perform key exchange using: EC Diffie-Hellman key agreement over NIST curves secp256r1, secp384r1, secp521r1. For each connection attempt, the server key exchange message includes: 1) a NIST named curve specifying predefined EC domain parameters; 2) an ECDH public key corresponding to these parameters.

FCS_DTLSS_EXT.1.5: The TSF shall silently discard the record if a message received contains an invalid MAC.

FCS_DTLSS_EXT.1.6: The TSF shall detect and silently discard replayed messages for DTLS records previously received or DTLS records too old to fit in the sliding window.

Sequence Number Verification Mechanism:

- Each DTLS record contains a 16-bit sequence number.
- The sequence number increments in the order of transmission.
- The receiver must detect and discard duplicate records (replay attack) or outdated records (out of window range).

Sliding Window Mechanism: the TOE uses a fixed-size bitmap window (default size 64) to track valid sequence numbers:

- Window Top (window_top): The highest sequence number currently received.
- Window Bitmap (window_bitmap): A 64-bit mask that marks which sequence numbers within the window have been received.
- Window Range: Valid sequence numbers must satisfy window_top - 64 < seq ⩽ window_top + 1.

FCS_DTLSS_EXT.1.7: TOE does not support session resumption.

FCS_DTLSS_EXT.1.8: The TSF provide the ability to configure the list of supported ciphersuites as defined in FCS_DTLSS_EXT.1.1.

FCS_DTLSS_EXT.1.10: The TSF shall not use PSKs.

FCS_TLSC_EXT.1.2: TLS client and server confirm to TLS 1.2 (RFC 5246). TLS session is established only when the server certificate is valid. The AP verify the presented identifier of AC's certificate using id-at-title. The TOE does not support using IP addresses as reference identifiers in common name.

TOE supports including the title field when requesting a certificate, so the server certificate issued by the CA will include the title field. When the TLS client receives the server certificate information, it checks whether the title field in the certificate is a specific value (capwap.dtls.fips). If it is, this rule passes the check.

For example: execute command

[system] pki entity 1

[H3C-pki-entity-1] title capwap.dtls.fips

FCS_TLSC_EXT.1.4: The TOE supports group extensions with the following curves/groups in the Client Hello message: secp256r1, secp384r1, secp521r1, these functions are enabled by default, matching the curves/groups specified in the imported certificate. If the server uses an ECDSA certificate, we set the ECDSA certificate key curve as the curve for ECDH negotiation, with the two being the same. The specific correspondences are as follows:

If the ECDSA certificate key is: NID_X9_62_prime256v1, the corresponding negotiated elliptic curve is set to P-256;

If the ECDSA certificate key is: NID_secp384r1, the corresponding negotiated elliptic curve is set to P-384;

If the ECDSA certificate key is: NID_secp521r1, the corresponding negotiated elliptic curve is set to P-521.

FCS_TLSC_EXT.1.5: The TOE supports the signature_algorithms expansion, which is executed by default and is not configurable.

FCS_TLSC_EXT.1.6: The TOE does not support the configuration of ciphersuites.

FCS_TLSC_EXT.1.8: The TSF shall not use PSKs.

FCS_TLSS_EXT.1.2: The TSF shall authenticate itself using X.509 certificate(s) using:

- RSA with key size 3072, 4096 bits;
- ECDSA over NIST curves secp256r1, secp384r1, secp521r1.

FCS_TLSS_EXT.1.3: The TSF shall perform key exchange using: EC Diffie-Hellman key agreement over NIST curves secp256r1, secp384r1, secp521r1.

FCS_TLSS_EXT.1.4: TOE does not support session resumption.

FCS_TLSS_EXT.1.5: The TOE supports ciphersuites can be configured.

FCS_TLSS_EXT.1.7: The TSF shall not use PSKs.

EPWLAN: FCS_CKM.1/WPA & FCS_CKM.2/GTK & FCS_CKM.2/PMK

The TOE supports cryptographic key distribution for 802.11 PMK key reception from an 802.1X authentication server. If the WLAN client successfully authenticates using 802.1X, the RADIUS authentication server returns an Access-Accept packet and generates a Pairwise Master Key (PMK) that meets [IEEE 802.11-2012 and does not expose the cryptographic keys. The RADIUS authentication server then distributes the PMK to the Access Controller and the WLAN client. The target object (TOE) also generates a Group Master Key (GMK). The TOE provides IPsec to protect the PMK received from the RADIUS authentication server. The PMK is received by the TOE via the MS-MPPE-Recv-Key EAP attribute. If PSK authentication is used for identity verification, the PMK is generated from the PSK key, and both the client and the AC use this PMK to generate the PTK and GTK.

The Access Controller and the WLAN client execute a four-way handshake process to derive a Pairwise Transient Key (PTK) from the master key, and, if necessary, a Group Temporal Key (GTK).

The TSF implements the PRF-384 and PRF-704 key derivation algorithms according to the [IEEE 802.11-2020] and [IEEE 802.11ax-2021] standards to derive the required number of bits for generating the Pairwise Transient Key (PTK) and the Group Temporal Key (GTK).

The Access Controller securely distributes the GTK to the WLAN client using a Key Encryption Key (KEK) and distributes the PTK and GTK to the AP via an internally trusted channel protected by DTLS. The TSF use AES Key Wrap in an EAPOL-Key frame to distribute Group Temporal Key (GTK), that meets NIST SP 800-38F, IEEE 802.11-2012 for the packet format and timing considerations and does not expose the cryptographic keys. The GTK is used to protect multicast/broadcast traffic and is shared among all WLAN clients and APs. Key management defines how to generate and update the PTK and group temporary key (GTK). The PTK is used in unicast and the GTK is used in multicast and broadcast.

PTK structure: KCK | KEK | TK

EAPOL-Key Confirmation Key (KCK) is used to verify the integrity of an EAPOL-Key frame.

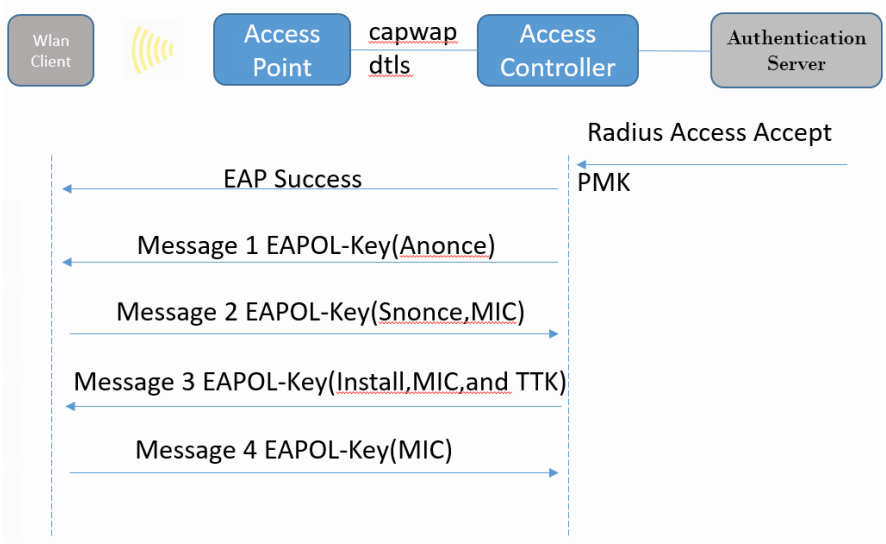
EAPOL-Key Encryption Key (KEK) is used to encrypt the key data in the EAPOL-Key frame.

Temporal Key (TK) is used to encrypt unicast packets.

The GTK includes the TK and other fields. The TK is used to encrypt multicast and broadcast packets.

EAPOL-Key packet: The IEEE 802.11i protocol uses EAPOL-Key packets during key negotiation.

RSN uses EAPOL-Key packets in the four-way handshake to negotiate the PTK and the GTK.



RSN key negotiation uses the following process:

1. The AC sends the client EAPOL-Key message 1 that contains a random value ANonce.
2. The client performs the following operations:

   a. Uses the random value SNonce, ANonce, and PMK to generate a PTK by using the KDF (key derivation function).

   b. Uses the KCK in the PTK to generate the MIC (Message integrity check).

   c. Returns EAPOL-Key message 2 that contains the SNonce and MIC.
3. The AC performs the following operations:

   a. Uses the SNonce, ANonce, and PMK to generate a PTK by using the KDF.

   b. Uses the KCK in the PTK to generate the MIC.

   c. Compares the received MIC with the local MIC.

   d. Generates a GTK with the random GMK and MAC address of the AP by using the KDF if the two MICs are the same.

   e. Returns EAPOL-Key message 3 that contains the key installation request tag, MIC, and GTK.
4. The client performs the following operations:

   a. Compares the received MIC with the local MIC.

   b. Installs the PTK and GTK if the two MICs are the same.

   c. Returns EAPOL-Key message 4 that contains the MIC.
5. The AC performs the following operations:

   a. Compares the received MIC with the local MIC.

   b. Installs the PTK and GTK if the two MICs are the same.

WLAN networks enhance WLAN security through key update mechanisms in identity authentication and key management. Key updates include PTK updates and GTK updates.

PTK Update: PTK update is a security measure for updating the encryption key of unicast datagrams. It employs a mechanism of re-performing a four-way handshake to negotiate a new PTK key, thereby enhancing security.

GTK Update: GTK update is a security measure for updating the encryption key of multicast datagrams. It uses a mechanism of re-performing a two-way multicast handshake to negotiate a new GTK key, thereby enhancing security.
The implementation of TOE was also subjected to systematic internal testing during the product development process, and regression testing was conducted according to internal policies, including packet capture to acknowledge message structure.
H3C conducts interoperability tests by connecting to H3C Wi-Fi access points using different client operating systems (include Windows, Mac OS X, Linux, Apple iOS, Android, etc.).The developer's test approach includes systematic functional testing to verify that product development meets standard requirements. Guaranteed through Wi-Fi Alliance testing and certification. Additionally, internal development policies include code review and approval processes to further ensure compliance during implementation.

8.3 Identification and authentication

The TOE is designed to require users to be identified and authenticated before they can access any of the TOE functions.

The TOE supports the local definition of users with corresponding password and role. The passwords can be composed of any combination of upper- and lower-case letters, numbers, and special characters. Minimum password length is settable by the authorized security administrator, the minimum length range is 15 to 32 and supports password of 15 to 63 characters.

The administrator can also configure the TOE to authenticate users using an external authentication server. The TOE supports RADIUS servers. A trusted channel using IPsec is established between TOE and external authentication server.

Administrators can connect to the TOE via a local console or remotely using SSHv2 Local administrators can access the TOE CLI interface via a serial console (direct) connection by using username and password. Remote administrators can access the CLI interface via an SSH protocol connection from an SSH client.

TOE provide password-based and public-key-based authentication mechanism for SSH. For public-key-based, administrator must import user public key into the configuration of TOE. The algorithm of public-key or certification public-key support ECDSA.

When logging via password, only obscured feedback is provided so the password is not visible when the user is inputting it.

The TOE provides the security administrator the ability to specify the maximum number of unsuccessful authentication attempts before administrator is locked out. While the TOE supports a range from 2-10.

When the defined number of unsuccessful authentication attempts has been met, the TOE shall prevent the offending Administrator from accessing TOE using any authentication method until unlock is taken by a Security Administrator or an Administrator defined time period has elapsed.

IPsec, TLS/DTLS support X.509 certificate authentication. The certificate chain is a sequence of certificates, from a peer certificate to the root CA certificate. Within the PKI hierarchy, all enrolled peers can validate the certificate of one another if the peers share a trusted root CA certificate or a common subordinate CA. Each CA corresponds to a trust point. When a certificate chain is received from a peer, TOE processing of a certificate chain path continues until the first trusted certificate, or trust point, is reached. TOE validate certificates in certificate chain according RFC

5280 certificate validation. The TOE also validates the revocation status of the certificate using a Certificate Revocation List (CRL) and check the basicConstraints extension and the CA flag to determine whether they are present and set to TRUE.

If the connection to determine the certificate validity cannot be established, the certificate is not accepted and the connection will not be established.
The TOE forces the administrator to re-authenticate when its password is changed.

The TOE can use pre-shared keys for IEEE 802.11 WPA2-PSK and WPA3-SAE, that support both text-based and bit-based pre-shared keys.

For IEEE 802.11 WPA2-PSK and WPA3-SAE, the text-based pre-shared key (PSK) has a length of 8 to 63 characters; for IPsec, the text-based pre-shared key (PSK) has a length of 15 to 128 characters. It can be composed of any combination of uppercase and lowercase letters, digits, and special characters (including: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")").For bit-based pre-shared keys that are 64 hexadecimal digits.

The TOE support wireless 802.1X Authentication. When a wireless client associates with TOE under an 802.1x authentication architecture, an EAP exchange takes place, followed by a four-way handshake to verify the encryption keys. The TOE acts as the authenticator, relaying information between the authentication server and supplicant. The EAP type must be consistent between the authentication server and supplicant, and is transparent to the TOE.

Before 802.1x authentication was successful, the TOE only forward EAPOL frame from or to wireless client.

The Identification and authentication function is designed to satisfy the following security functional requirements:

FIA_AFL.1: After an administrator specified (2-10) number of failed attempts, the TOE will lockout (blacklist) the offending remote administrator and log the event. The offending administrator will remain locked out until the administrator configured lock-out period has expired or administrator unlock. FIA_AFL.1 is enforced by the TOE，but is not applicable when using external authentication servers.

Administrator access via the local console is always reserved, and administrators are never locked out from accessing the console. The lockout mechanism applies to remote access according to the configured policy, does not affect local console access.

If a user fails to log in, the system adds the user account and the user's IP address to the password control blacklist. When a user fails the maximum number of consecutive attempts, login attempt limit limits the user and user account in any of the following ways:

- For VTY user, the system prohibits the user from using the user account to log in through the user's IP address. The locked user can use their own account to log in to the device only after the account is manually removed from the password control blacklist.
- Allows the user to continue using the user account. The user's IP address and user account are removed from the password control blacklist when the user uses this account to successfully log in to the device.
- Locks the user account and the user's IP address for a period of time.

The user can use the account to log in from the IP address when either of the following conditions exists:

- The locking timer expires.
- The account is manually removed from the password control blacklist before the locking timer expire.

FIA_PMG_EXT.1: The TOE authentication mechanism provides configuration for minimum password length. The following calculation is based on the following facts:

Minimum password length

You can define the minimum length of user passwords. The system rejects the setting of a password that is shorter than the configured minimum length. The minimum length range is 15 to 32.

Password composition policy

A password can be a combination of characters from the following types:

- Uppercase letters A to Z.
- Lowercase letters a to z.
- Digits 0 to 9.
- Special characters in Table 8.

Character name	Symbol	Character name	Symbol
Ampersand sign	&	Apostrophe	'
Asterisk	*	At sign	@
Back quote	`	Back slash	\
Blank space		Caret	^
Colon	:	Comma	,
Dollar sign	$	Dot	.
Equal sign	=	Exclamation point	!
Left angle bracket	<	Left brace	{
Left bracket	[	Left parenthesis	(
Minus sign	-	Percent sign	%
Plus sign	+	Pound sign	#
Quotation marks	"	Right angle bracket	>
Right brace	}	Right bracket	]
Right parenthesis	)	Semi-colon	;
Slash	/	Tilde	~
Underscore	_	Vertical bar	|

Table 8 Special Characters

Password complexity checking policy

For higher security, you can configure a password complexity checking policy to ensure that all user passwords are relatively complicated. When a user configures a password, the system checks the complexity of the password. If the password is complexity-incompliant, the configuration will fail.

Password history record

The password for the device management user is stored in a hashed ciphertext format and cannot be restored to plaintext. Therefore, when configuring a new password for the device management user: if the new password is set

in a hashed manner, it will not be compared with all recorded historical passwords and the current password; if the new password is configured in plaintext, it must be different from all recorded historical passwords and the current password. Additionally, when the user is required to enter the old password for verification, it must be checked that the new password and the user-entered old password differ by at least 4 characters, and these 4 characters must be distinct from each other; otherwise, the password change will fail.

FIA_PSK_EXT.1: The TOE supports the use of pre-shared keys to authenticate the IPsec peer between the AC and the remote syslog server. The pre-shared key is entered as characters.

For IPsec, the TOE supports a pre-shared key length of 22 characters, while also supporting lengths ranging from 15 to 128 characters and the ciphertext key is a character string of 15 to 201 characters. The character set for the pre-shared key includes uppercase and lowercase letters, digits, and 27 special characters (including: ~ ` ! @ # $ % ^ & * ( ) _ + - = { } | [ ] : ; ’ , . /), spaces are not supported. A minimum pre-shared key length of 22 is recommended. Pre-shared keys can also be entered as HEX (“bit-based”) values, the plaintext key must consist of an even number of hexadecimal digits. While also supporting lengths ranging from 30 to 256 characters and the ciphertext key is a character string of 69 to 373characters.

For WPA3-SAE and IEEE 802.11 WPA2-PSK: The key length shall be between 8 and 63 characters inclusive, and the ciphertext key is a character string of 41 to 117 characters. The character set for the pre-shared key includes uppercase and lowercase letters, digits, and 31 special characters (including: ~ ` ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : ” ; ’ < > , . /), spaces are not supported. Pre-shared keys can also be entered as HEX (“bit-based”) values, the plaintext key consists of 64 hexadecimal digits, and the ciphertext key is a character string of 117 characters. The TOE rejects keys that exceed the length declared as supported.

FIA_UIA_EXT.1: The TOE requires an administrator to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that user.

Before requiring a non-TOE entity to initiate the identity verification and authentication process, the TOE will display warning notifications and unauthorized usage consent warnings specified by the authorized administrator (FTA_TAB.1). The TOE requires the administrator to successfully identify and authenticate before accessing the management console and performing any other TSF-mediated operations on behalf of the user.

Once the TOE is operational, the administrator can access the TOE interface through the AC using the CLI (SSH). The login process is initiated by the administrator via the required interface, and the administrator receives an authentication challenge. If the administrator enters valid credentials, the authentication process will be successfully completed, and the management interface will be displayed to the administrator. Administrators cannot log in to the AP since those interfaces are disabled after initial configuration.

The TOE supports replaying ICMP echo prior to requiring the non-TOE entity to initiate the identification and authentication process.

FIA_UAU.7: TOE provides only vague feedback to administrative users when verifying identity on the local console, without echoing the entered password.

FIA_X509_EXT.1/ITT: The TOE performs X.509 certificate validation at the following points:

- When importing a certificate.

- When establishing an SSL or DTLS trusted channel, verify the peer (AP verifies AC).

The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation supporting a minimum path length of two certificates.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using CRL.
- The TSF shall validate certificates in accordance with the following rules:
  - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.

For FIA_X509_EXT.1.1/ITT, the TOE's certificate extendedKeyUsage field only requires server authentication purpose, Since the TOE only requires one-way verification (AP to AC), it does not need client authentication purpose. Certificate checks support only CRL and not OCSP.

FIA_X509_EXT.1/Rev: The TOE performs X.509 certificate validation at the following points:

- When importing a certificate.
- During IPsec peer authentication

In all scenarios, certificates are checked for several validation characteristics:

- If the certificate 'notAfter' date is in the past, then this is an expired certificate which is considered invalid;
- The certificate chain must terminate with a trusted CA certificate designated as a trust anchor;
- A trusted CA certificate is defined as any certificate loaded into the TOE trust store that has, at a minimum, a basicConstraints extension with the CA flag set to TRUE;

Certificate revocation checks are performed when certificates are submitted to the TOE and loaded into the TOE. The system will verify the complete certificate chain, including intermediate and leaf certificates. When both intermediate and leaf certificates are present, all certificates are checked. When a leaf certificate is submitted to the TOE as part of the certificate chain during the authentication process, revocation checks are performed on both the leaf certificate and the intermediate CA certificates. The TOE does not allow incomplete certificate chains; if only a leaf certificate exists without an intermediate certificate, a leaf certificate signed by an intermediate CA cannot be loaded.The TOE does not use any extendedKeyUsage rules for FIA_X509_EXT.1/Rev.

FIA_X509_EXT.1/Rev focuses only on Ipsec and does not involve code signing or web servers. Certificate checks support only CRL and not OCSP.

FIA_X509_EXT.2: The TOE uses X.509v3 certificates defined in RFC 5280 to support Ipsec or SSL authentication, which can be imported and specified.

When a connection cannot be established to determine the validity of a certificate, the certificate is not accepted. No other distinctions are made between trusted channels, and certificate validation is performed in the same manner across trusted channels.

FIA_X509_EXT.3: The TOE generates Certificate Request Messages and includes the following information: public key, common name, organization, organizational unit, country, fqdn, title. Upon receiving the CA Certificate response, the TOE will validate the chain of certificates from the Root CA.

FIA_UAU.6: The TOE requires a user to reauthenticate when a password is changed or the session is locked.

FIA_8021X_EXT.1: For 802.1X authentication, extended authentication protocol (EAP) is used to communicate between the wireless client and the TOE over the local area network (EAPOL). The TOE also establishes an Ipsec tunnel with the RADIUS authentication server. Management can be performed via an external RADIUS server that complies with RFC 2865 and RFC 3579 standards.
The TSF follows port-based network control as defined in Clause 7.1 and EAP as defined in Clause 8 and Clause 11 of [IEEE 802.1X-2010]. For Clause 8, the TOE acts only as an Authenticator. For Clause 11, the TOE supports only the first four message processes of Table 11-3—EAPOL Packet Types. These meet the wireless 802.1x authentication requirements.
H3C conducts 802.1x interoperability tests by connecting to H3C Wi-Fi access points using different client operating systems (include Windows, Mac OS X, Linux, Apple iOS, Android, etc.). The developer's test approach includes systematic functional testing to verify that product development meets standard requirements. Guaranteed through Wi-Fi Alliance testing and certification. Additionally, internal development policies include code review and approval processes to further ensure compliance during implementation.

8.4 Security management

The TOE implements a role mechanism that is used to specify the role and corresponding permissions which authenticated users possess.

The TOE maintains Security Administrators that includes privileged and semi-privileged roles.
The privileged role can access all features and resources in the system except some specific commands, and can perform all of the operations defined in FMT_SMF.1. This is privilege level 15 or Network-admin or Network Administrator.
Semi-privileges roles are any that have a subset of the privileges of the level 15.
Privilege level 0, 1 (also known as network-operator) and 9 are defined by default and are customizable, privilege 2 to 8 and 10 to 14 are undefined by default and are customizable. It exists also a pre-defined privilege level called Security-audit with rights to display and maintain security log files.
Use of the level-0 through level-14 roles, as well as the network-operator role, is not required in order to properly administer a TOE. These roles possess a subset of the permissions of the network-admin role and thus are capable of only some of the management functions available to him.
The TOE offers command-line interface providing a range of security management functions for use by Security Administrators. Among the functions available are those functions that are necessary to manage all aspects of the cryptographic functions of the TOE, those necessary to enable or disable the network services offered by the TOE, and the functions necessary to review the TOE versions, update the TOE components, and also to verify the validity of those updates.

FMT_MOF.1/ Functions: Only Security Administrators can modify the behavior of the transmission of audit data to an external audit server. A user with no administrator privileges cannot configure and enable the info-center function.

FMT_MTD.1/CoreData: Only Security Administrators can manage TSF data. There are no security functions available through any interfaces prior to administrator login. Non-administrative users (i.e., wireless users) do not have access to the TOE via the CLI, therefore, they do not have any access to the security functions of the TOE.

FMT_MOF.1.1/ ManualUpdate: Management of security functions behaviour related to manual updates is provided by FMT_MOF.1/ManualUpdate. In order to meet this SFR, The TSF restricts the ability to enable the functions to perform manual updates to Security Administrators. In addition, only security administrators have the right to create or delete users in the TOE. While changing the local user privilege level, the configured new level of the local user cannot be higher than that of the login-in user. In this way no user except administrators can change another user to be at the privilege level of administrator, and only administrators have the ability to perform manual update. Therefore, the manual update is restricted to administrators. The TOE uses groups to organize users. Security administrators must first transfer the candidate AP update onto the AC. It will be downloaded to the AP the next time the AP component connects to the AC (assuming the digital signature is valid).

FMT_SMF.1: Management of security functions behaviour related to transmission of audit data to external IT entities is provided FMT_SMF.1. The TOE meets this SFR by enforcing that:

- Only Security Administrators have right to configure audit servers where audit records are exported to.
- Only Security Administrators have the privilege to choose the trusted channel for external audit server and decide whether transmit the audit data to an external IT entity or not.
- Only Security Administrators have the privilege to modify the behaviour of TOE Security Functions (e.g., cryptographic algorithm, audit server).

The TOE also offers the following functions, which are limited to the privileged level Network Administrator:

- Restart the TOE.
- configure the access banner.
- configure the remote session inactivity time before session termination.
- update the TOE, and to verify the updates using digital signature capability prior to installing those updates.
- configure audit behaviour (e.g., changes to storage locations for audit; changes to behaviour when local audit storage space is full).
- configure local audit behaviour (e.g., changes to storage locations for audit; changes to behaviour when local audit storage space is full, changes to local audit storage size).
- configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1.
- manage the cryptographic keys.
- configure the cryptographic functionality.
- configure thresholds for SSH rekeying.
- configure the lifetime for Ipsec Sas.
- configure the list of supported (D)TLS ciphers.
- configure the interaction between TOE components.
- re-enable an Administrator account.
- set the time which is used for time-stamps.
- configure NTP.
- configure the reference identifier for the peer.
- manage the TOE's trust store and designate X509.v3 certificates as trust anchors.
- administer the TOE locally.
- configure the local session inactivity time before session termination or locking.
- configure the authentication failure parameters for FIA_AFL.1.
- manage the trusted public keys database.

All of the above functions can be performed on the AC using the CLI.
A default administrator account is configured during initial configuration where the password is set by the admin.
The interaction of TOE components can be configured via the AC per FCO_CPC_EXT.1 and as described in section 8.8.

FMT_SMR.2: The Target of Evaluation (TOE) provides an administrator role that corresponds to the security administrator role specified in the NDcPP. The administrator can use the Command Line Interface (CLI) to manage all aspects of the TOE locally or remotely.

FMT_MTD.1/CryptoKeys: The TSF shall restrict the ability to manage the cryptographic keys to Security Administrators. Only Security Administrators have the capability to modify, delete, generate, and import the cryptographic keys and certificates.

EPWLAN: FMT_SMR_EXT.1: The TOE cannot be administrated by a wireless client.

EPWLAN: FMT_SMF.1/AccessSystem: Wireless security types supported include WPA3-Enterprise, WPA2-Enterprise, WPA3-SAE, and WPA2-PSK. WLAN clients can connect to the wireless network securely via 2.4 GHz, 5 GHz, or 6 GHz bands. If a client uses an unsupported security type to connect, it will fail.

8.5 Protection of the TSF

FPT_SKP_EXT.1: The TOE stores all pre-shared keys, symmetric keys, and private keys in the file system in Flash that can't be read, copy or extract by administrators; hence no interface access is available. Section 8.2 describes how the pre-shared keys, symmetric keys and private keys are stored.

FPT_APW_EXT.1: The administrator's password is encrypted using SHA-512 and stored as irreversible ciphertext data. The plaintext password of the administrator cannot be obtained externally from the device.

FPT_TST_EXT.1/ FPT_FLS.1: During start-up of the TOE, the TOE first checks the integrity of the firmware, and then runs a series of self-tests to ensure it is performing its cryptographic functions correctly. If any of these checks fails, the device will halt and require administrator intervention to successfully start-up.
The following tests are performed:

- Cryptographic Module Known Answer Tests:
  - SHA (SHA256, SHA384, SHA512)
  - HMAC (HMAC_SHA256, HMAC_SHA384, HMAC_SHA512)
  - AES (AES-128-GCM, AES-192-GCM, AES-256-GCM, AES-CCM)
  - RSA
  - ECDSA
  - RNG
- Bootloader Module
  - Firmware Integrity Test

FPT_TUD_EXT.1: Security administrators can check the version of the installed firmware through the command line and manually initiate a firmware update. There are means to authenticate those updates to the TOE using a digital signature and prior to installing them.
For AC, When the firmware version is updated

1. Use the display version command to verify the current firmware version.
2. Use the release notes for the firmware software version to evaluate the upgrade impact on your network and verify the following items:

   Software and hardware compatibility.

   Version and size of the upgrade firmware.

Compatibility of the upgrade firmware with the current and startup firmware image.

3. Use the dir command to verify that the device has sufficient storage space for the upgrade images. If the storage space is not sufficient, delete unused files by using the delete /unreserved command.

4. Use SCP or SFTP to transfer the upgrade image file to the root directory of a file system.

Use "bootloader" command to set files for next startup. At this point, the digital signature of the next boot file will be verified.

If the digital signature verification fails, the TOE will not update the startup image and you will receive a verification failure message.

If the digital signature verification success, users use "display boot-loader" to display current firmware images and next startup firmware images.

Use "reboot" command to restart the device to update the version.

For AP, use "display wlan ap-model name" command on AC to display current AP version.

The AP's version needs to be transferred to the AC's apimge directory. When the AP connects to the AC, if the versions do not match, the AP will automatically download the version from the AC. If the AP's digital signature verification fails, the AP will not write the version to the local flash. If the AP's digital signature verification succeeds, the AP will write the version from memory to the flash and then automatically restart to update the version.

The software images for the TOE are digitally signed for authenticity and integrity verification. This mechanism ensures that the firmware installed on the TOE is from a trusted source and has not been tampered with in the transfer, storage, or installation phase.

The TOE software digital signature verification for authenticity and integrity in the following situations:

- Before the TOE loads a software image during startup. If the digital signature verification fails, the TOE will not load the image and you will receive a verification failure message.
- When you specify a software image to upgrade the device from the Bootware menu. If the digital signature verification fails, the TOE will not set the image for upgrade and you will receive a verification failure message.
- Before the TOE loads a Bootware image to the Normal area of Bootware. If the digital signature verification fails, the TOE will not load the image and you will receive a verification failure message.
- When you specify a firmware image as a startup image through the boot loader. The TOE will verify the digital signature of the image before it updates the startup image list with the specified image. If the digital signature verification fails, the TOE will not update the startup image and you will receive a verification failure message.
- Before the TOE activates a feature or patch image. If the digital signature verification fails, the TOE will not activate the image and you will receive a digital signature failure message.

FPT_ STM_EXT.1: The hardware of the TOE includes a hardware-based real-time clock. The TOE's embedded OS manages the clock and exposes clock-related functions for use by the TOE. The TOE software can also be configured to utilize the NTP protocol to keep the local hardware-based real-time clock synchronized with other network devices. The communication between TOE and NTP server will be protected by Ipsec security channel. AP connects to AC and synchronizes time from AC to keep both devices' time consistent.

FPT_ITT.1: The communication between the different parts of the TOE is protected with DTLS and tls.

The Protection of the TSF function is designed to satisfy the following security functional requirements: FPT_SKP_EXT.1, FPT_APW_EXT.1, FPT_TST_EXT.1, FPT_TUD_EXT.1, FPT_STM_EXT.1, FPT_ITT.1, FPT_FLS.1.

8.6 TOE access

FTA_SSL_EXT.1/ FTA_SSL.3: The TOE can be configured by an administrator (in the Network-admin role) to set an interactive session timeout value (any integer value in minutes and also optionally in seconds, with 0 disabling the timeout – the default timeout is 10 minutes). A session that is inactive (i.e., no commands issuing from the remote client) for the defined timeout value will be terminated, both for local and for remote sessions.
The user will be required to re-enter their user id and their password so they can be re-authenticated in order to establish a new session.

FTA_SSL.4: The user also has the ability to terminate his own sessions (log out). The TOE allows users to terminate their own local and remote CLI sessions by issuing the 'quit command.

FTA_TAB.1: The TOE can be configured to display administrator-configured advisory banners that will be displayed in conjunction with user login prompts. The banner contents are configured by a user in the Network-admin role. When accessing the CLI locally via the console or remotely via SSH, this banner is displayed. The configuration information is consistent across all interfaces. It can be configured using the 'header' command in the CLI.

FTA_TSE.1: The TOE has a scheduler that allows to shut down the communication between TOE and wlan client based on time, day and specific access point.

8.7 Trusted path/channels.

FTP_TRP.1/Admin: To support secure remote administration, the TOE includes implementations of SSH. In each case, a remote host (presumably acting on behalf of an administrator) can initiate a secure remote connection for the purpose of security management. Note that only the local console is available by default and each of these remote administration services can be independently enabled by an administrator.

FTP_ITC.1: The TOE uses the Ipsec/IKEv2 protocol to establish trusted channels between the AC and the external authentication server, Audit server, 802.1x server, and NTP server. These Ipsec channels are peer-to-peer connections whereby the TOE can act as either the server or the client.
As indicated earlier, the TOE can be configured to export audit records to an external audit server. In order to protect exported audit records from disclosure or modification, the TOE can be configured to utilize an IPSEC secure channel for this purpose. This protection is initiated by the TOE whenever Audit connections are established for the purpose of exporting audit records.
Ipsec can protect RADIUS messages between AC and authentication servers, as well as 802.1x servers.
The communication with the NTP server and the authentication server is also protected by an Ipsec secure channel.
All of the secure protocols are supported by the cryptographic operations provided by the FCS requirements in this Security Target.

EPWLAN: FTP_ITC.1/Client: For wireless users operating in a Robust Security Network (RSN), WPA3-Enterprise, WPA2-Enterprise, WPA3-SAE and WPA2-PSK as defined by IEEE 802.11-2020 are used to provide a trusted channel between the TOE and WLAN clients. If the client attempts to use another security type to establish a connection, the authentication attempt will be rejected.

8.8 Communication

The communication function is designed to satisfy the following security functional requirements:
FCO_CPC_EXT.1:
After starting up with zero configurations, an AP automatically creates VLAN-interface 1 and enables the DHCP client, DHCPv6 client, and DNS features on the interface. Then it obtains its own IP address from the DHCP server and discovers Acs by using the following methods:

- Static IP address.

  If AC IP addresses have been manually configured for the AP, the AP sends a unicast discovery request to each AC IP address to discover Acs.

- DHCP options.

  The AP obtains AC Ipv4 addresses from Option 138, Option 43, and Ipv6 addresses from Option 52 sent from the DHCP server. It uses these addresses in descending order.

- DNS.

  a. The AP obtains the domain name suffix from the DHCP server.

  b. The AP adds the suffix to the host name.

  c. The DNS server translates the domain name into IP addresses.

- Broadcast.

  The AP broadcasts discovery requests to IP address 255.255.255.255 to discover Acs.

- Ipv4 multicast:

  The AP sends multicast discovery requests to Ipv4 address 224.0.1.140 to discover Acs.

- Ipv6 multicast.

  The AP sends multicast discovery requests to Ipv6 address FF0E::18C to discover Acs.

  The methods of static IP address, DHCPv4 options, broadcast/Ipv4 multicast, Ipv4 DNS, Ipv6 multicast, DHCPv6 option, and Ipv6 DNS are used in descending order.

  The AP does not stop AC discovery until it establishes a CAPWAP tunnel with one of the discovered Acs.

  The AP sends a discovery request to each AC to discover Acs.

  Upon receiving a discovery request, an AC determines whether to send a discovery response by performing the following steps:

Identifies whether the discovery request is a unicast packet.

–**Unicast packet**—The AC proceeds to step .

–**Broadcast or multicast packet**—The AC proceeds to step if it is disabled with the feature of responding only to unicast discovery requests. If this feature is enabled, the AC does not send a discovery response.

b. Identifies whether it has manual AP configuration for the AP model specified in the discovery request.

–If manual AP configuration exists, the AC sends a discovery response to the AP. The discovery response contains information about whether the AC has the manual configuration for the AP, the AP connection priority, and the AC's load status.

–If no manual AP configuration exists, the AC does not send a discovery response.

The Security Administrator must enable communications between the Remote Access Points and Controller components before any communication can take place. The security administrator must manually configure the AP template and set up tunnel encryption so that the AP can establish a connection with the AC.
The AC's factory firmware includes a default certificate, which the AP can check to establish an initial DTLS and TLS tunnel (FPT_ITT.1) with the AC. The AC and AP can also be pre-configured with ECDSA or RSA certificates. The import and configure certificate function on the AP is only temporarily enabled for this purpose, which will also enforce the AP to use the pre-configured certificate in the connection, supporting more certificate security checks (FIA_X509_EXT.1.1/ITT). After the AP establishes a channel with the AC, the configuration function on the AP will be disabled. The security administrator can disable communication between the AP and the controller by deleting the AP template from the AC.

Support for Additional TOE Component Instances
The TOE consists of one Access Controller (AC) and one or more Access Points (AP), operating together as a distributed system.

- Allowance of Additional Instances: The TOE allows additional AP instances to be added to the system in accordance with the deployment design.
- Behavioral Differences:
    - Single Component: When a single AC is deployed with a single AP, all management, authentication, and encryption functions are performed between the AC and the AP using the secure management channels defined in the ST.
    - Multiple Components: When multiple Aps are connected to the AC, the AC manages each AP independently over the secure management channel, and all Aps enforce the same security policies as defined in the AC configuration.
- Maintaining the SFRs:
    - All additional Aps run the same TOE software/firmware version as described in the ST and TSS to ensure that all SFRs are identically enforced.
    - Secure channels between the AC and each AP maintain confidentiality and integrity protection in the same manner as for a single AP.
    - The system configuration does not permit any AP or AC to operate in a manner that would disable, corrupt, or bypass the security functionality enforced by the SFRs.

Therefore, the addition of extra instances of Aps does not alter the enforcement of the SFRs, and no operational mode is available that would allow bypassing or weakening of the evaluated security functionality.

9 Rationales

9.1 Security Objectives Rationale

This rationale consists of a table mapping assumptions against security objectives. It is informative only, as it is a representation of the tracing of assumptions to objectives as defined in [PP-ND] and extended by [EP-WLAN] adopted in this ST.

9.1.1 Assumptions to Security Objectives Mapping

Objectives \ Threats and assumptions	A.PHYSICAL_PROTECTION	A.LIMITED_FUNCTIONALITY	A.NO_THRU_TRAFFIC_PROTECTION	A.TRUSTED_ADMINISTRATOR	A.REGULAR_UPDATES	A.ADMIN_CREDENTIALS_SECURE	A.COMPONENTS_RUNNING	A.RESIDUAL_INFORMATION	A.CONNECTIONS
OE.PHYSICAL	X								
OE.NO_GENERAL_PURPOSE		X							
OE.NO_THRU_TRAFFIC_PROTECTION			X						
OE.TRUSTED_ADMIN				X					
OE.UPDATES					X				
OE.ADMIN_CREDENTIALS_SECURE						X			
OE.COMPONENTS_RUNNING							X		
OE.RESIDUAL_INFORMATION								X	
OE.CONNECTIONS									X

Table 9 Threats and Assumptions to Security Objectives Mapping

9.1.2 Assumptions

9.1.2.1 A.PHYSICAL_PROTECTION

This assumption is directly upheld by OE.PHYSICAL, which requires that physical protection to the TOE is provided by the operational environment.

9.1.2.2 A.LIMITED_FUNCTIONALITY

LIMITED_FUNCTIONALITY is upheld by OE.NO_GENERAL_PURPOSE.

9.1.2.3 A.NO_THRU_TRAFFIC_PROTECTION

This assumption is directly upheld by OE.NO_THRU_TRAFFIC_PROTECTION, which requires that the TOE does not provide any protection of traffic that traverses it, but such protection is covered by other security and assurance measures in the operational environment.

9.1.2.4 A.TRUSTED_ADMINISTRATOR

This assumption is directly upheld by OE.TRUSTED_ADMIN, which requires that TOE Administrators are trusted to follow and apply all guidance documentation in a trusted manner.

9.1.2.5 A.REGULAR_UPDATES

This assumption is directly upheld by OE.UPDATES, which requires that the TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

9.1.2.6 A.ADMIN_CREDENTIALS_SECURE

This assumption is directly upheld by OE.ADMIN_CREDENTIALS_SECURE, which requires that the administrator's credentials (private key) used to access the TOE are protected on any other platform on which they reside.

9.1.2.7 A.COMPONENTS_RUNNING (applies to distributed TOEs only)

This assumption is directly upheld by OE.COMPONENTS_RUNNING , for distributed TOE, the security administrator ensures the availability of each TOE component is checked as needed.

9.1.2.8 A.RESIDUAL_INFORMATION

This assumption is directly upheld by OE.RESIDUAL_INFORMATION which requires administrators to ensure that there is no unauthorized access possible for sensitive residual information on networking equipment when the equipment is discarded or removed from its operational environment.

9.1.2.9 A.CONNECTIONS

The OE objective OE.CONNECTIONS is realized through A.CONNECTIONS.

9.2 SFRs to component of the TOE rationale

This rationale consists of a table mapping SFRs to each of the components of the TOE.

SFR	TOE Component
FAU_GEN.1	All
FAU_GEN.2	All
FAU_STG.1	Access Controller
FAU_STG_EXT.1	All
FAU_GEN_EXT.1	ALL
FAU_STG_EXT.4	Access Controller
FAU_STG_EXT.5	Access Point
FCS_CKM.1	All
FCS_CKM.2	All

FCS_CKM.4	All
FCS_COP.1/DataEncryption	All
FCS_COP.1/SigGen	All
FCS_COP.1/Hash	All
FCS_COP.1/KeyedHash	All
FCS_RBG_EXT.1	All
FIA_AFL.1	Access Controller
FIA_PMG_EXT.1	Access Controller
FIA_PSK_EXT.1	All
FIA_UIA_EXT.1	Access Controller
FIA_UAU.7	Access Controller
FMT_MOF.1/ManualUpdate	All
FMT_MTD.1/CoreData	All
FMT_SMF.1	Access Controller
FMT_SMR.2	Access Controller
FPT_SKP_EXT.1	All
FPT_APW_EXT.1	Access Controller
FPT_TST_EXT.1	All
FPT_TUD_EXT.1	All
FPT_STM_EXT.1	ALL
FMT_MOF.1/Functions	Access Controller
FTA_SSL_EXT.1	Access Controller
FTA_SSL.3	Access Controller
FTA_SSL.4	Access Controller
FTA_TAB.1	Access Controller
FTP_ITC.1	Access Controller
FTP_TRP.1/Admin	Access Controller
FCS_IPSEC_EXT.1	Access Controller
FCS_NTP_EXT.1	Access Controller
FCS_SSHS_EXT.1	Access Controller
FCS_SSH_EXT.1	Access Controller
FCS_DTLSC_EXT.1	Access Point

FCS_DTLSS_EXT.1	Access Controller
FCS_TLSC_EXT.1	Access Point
FCS_TLSS_EXT.1	Access Controller
FIA_X509_EXT.1/ITT	All
FIA_X509_EXT.1/Rev	Access Controller
FIA_X509_EXT.2	All
FIA_X509_EXT.3	Access Controller
FCO_CPC_EXT.1	ALL
FMT_MTD.1/CryptoKeys	Access Controller
FPT_ITT.1	All
FAU_GEN.1.1/WLAN	ALL
FMT_SMR_EXT.1	ALL
FTP_ITC.1/CLIENT	ALL
FCS_CKM.1/WPA	Access Controller
FCS_CKM.2/GTK	Access Controller
FCS_CKM.2/PMK	Access Controller
FIA_UAU.6	Access Controller
FMT_SMF.1/AccessSystem	Access Controller
FIA_8021X_EXT.1	Access Controller
FPT_FLS.1	All
FTA_TSE.1	ALL

9.3 Dependency Rationale

This rationale provided in [PP-ND] annex E.1 shows that all dependencies of all security requirements have been addressed.

10 Abbreviations and glossary

[CC]	Common Criteria
[EAL]	Evaluation Assurance Level
[ST]	Security Target
[TOE]	Target of Evaluation
[TSF]	TOE Security Functionality
[PP]	Protection Profile

11 References

[CC_PART1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, version 3.1, Revision 5, CCMB-2017-04-001

[CC_PART2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 5, CCMB-2017-04-002

[CC_PART3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 5, CCMB-2017-04-003

[CEM] Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 5, CCMB-2017-04-004

[PP-ND] Collaborative Protection Profile for Network Devices, v3.0e, Date: 06-December-2023

[PPSSH] Functional Package for Secure Shell (SSH), Version 1.0

[EPWLAN] PP-Module for Wireless Local Area Network (WLAN) Access System Version: 1.0 , 2022-03-31.

[PP_ND3.0e_SD] Evaluation Activities for Network Device cPP Version: 3.0e Date: 06-December-2023

[EPWLAN_SD] Supporting Document Mandatory Technical Document, PP-Module for Wireless Local Area Network (WLAN) Access System Version: 1.0 2022-03-31

[AGD_PREOPE] [WLAN][AGD][ENS]H3C Wlan Series Preparative and Operative Procedures_V2.7.docx