

Configure and Verify Wi-Fi 6E WLAN Layer 2 Security

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Wi-Fi 6E Security](#)

[WPA3](#)

[Level Set: WPA3 Modes](#)

[Cisco Catalyst Wi-Fi 6E APs](#)

[Clients Supported Security Settings](#)

[Configure](#)

[Network Diagram](#)

[Configurations](#)

[Base Configuration](#)

[Verify](#)

[Security Verification](#)

[WPA3 - AES\(CCMP128\) + OWE](#)

[WPA3 - AES\(CCMP128\) + OWE with Transition Mode](#)

[WPA3-Personal - AES\(CCMP128\) + SAE](#)

[WPA3-Personal - AES\(CCMP128\) + SAE + FT](#)

[WPA3-Enterprise + AES\(CCMP128\) + 802.1x-SHA256 + FT](#)

[WPA3-Enterprise + GCMP128 cipher + SUITEB-1X](#)

[WPA3-Enterprise + GCMP256 cipher + SUITEB192-1X](#)

[Security Conclusions](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

This document describes how to configure Wi-Fi 6E WLAN Layer 2 security and what to expect on different clients.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Wireless Lan Controllers (WLC) 9800
- Cisco Access Points (APs) that support Wi-Fi 6E.

- IEEE Standard 802.11ax.
- Tools: Wireshark v4.0.6

Components Used

The information in this document is based on these software and hardware versions:

- WLC 9800-CL with IOS® XE 17.9.3.
- APs C9136, CW9162, CW9164 and CW9166.
- Wi-Fi 6E Clients:
 - Lenovo X1 Carbon Gen11 with Intel AX211 Wi-Fi 6 and 6E Adapter with driver version 22.200.2(1).
 - Netgear A8000 Wi-Fi 6 and 6E Adapter with driver v1(0.0.108);
 - Mobile Phone Pixel 6a with Android 13;
 - Mobile Phone Samsung S23 with Android 13.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The key thing to know is that Wi-Fi 6E is not an entirely new standard, but an extension. At its base, Wi-Fi 6E is an extension of the Wi-Fi 6 (802.11ax) wireless standard into the 6-GHz radio-frequency band.

Wi-Fi 6E builds on Wi-Fi 6, which is the latest generation of the Wi-Fi standard, but only Wi-Fi 6E devices and applications can operate in the 6-GHz band.

Wi-Fi 6E Security

Wi-Fi 6E uplevels security with Wi-Fi Protected Access 3 (WPA3) and Opportunistic Wireless Encryption (OWE) and there is no backward compatibility with Open and WPA2 security.

WPA3 and Enhanced Open Security are now mandatory for Wi-Fi 6E certification and Wi-Fi 6E also requires Protected Management Frame (PMF) in both AP and Clients.

When configuring a 6GHz SSID there are certain security requirements that must be met:

- WPA3 L2 security with OWE, SAE or 802.1x-SHA256
- Protected Management Frame Enabled;
- Any other L2 security method is not allowed, that is, no mixed mode possible.

WPA3

WPA3 is designed to improve Wi-Fi security by enabling better authentication over WPA2, providing expanded cryptographic strength and increasing the resiliency of critical networks.

Key features of WPA3 include:

- **Protected Management Frame (PMF)** protects unicast and broadcast management frames and encrypts unicast management frames. This means wireless intrusion detection and wireless intrusion prevention systems now have fewer brute-force ways to enforce client policies.
- **Simultaneous Authentication of Equals (SAE)** enables password-based authentication and a key

agreement mechanism. This protects against brute-force attacks.

- **Transition mode** is a mixed mode that enables the use of WPA2 to connect clients that do not support WPA3.

WPA3 is about continuous security development and conformance as well as interoperability.

There is no Information Element that designates WPA3 (same as WPA2). WPA3 is defined by AKM/Cipher Suite/PMF combinations.

On the 9800 WLAN configuration, you have 4 different WPA3 encryption algorithms you can use.

They are based on Galois/Counter Mode Protocol (GCMP) and Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP): AES (CCMP128), CCMP256, GCMP128 and GCMP256:

WPA2/WPA3 Encryption

AES(CCMP128)	<input checked="" type="checkbox"/>	CCMP256	<input type="checkbox"/>
GCMP128	<input type="checkbox"/>	GCMP256	<input type="checkbox"/>

WPA2/3 Encryption options

PMF

PMF is activated on a WLAN when you enable PMF.

By default, 802.11 management frames are unauthenticated and hence not protected against spoofing. Infrastructure Management Protection Frame (MFP) and 802.11w protected management frames (PMF) provide protection against such attacks.

Protected Management Frame


PMF	Required ▼
Association Comeback Timer*	1
SA Query Time*	200

PMF Options

Authentication Key Management

These are the AKM options available in the 17.9.x version:

Auth Key Mgmt

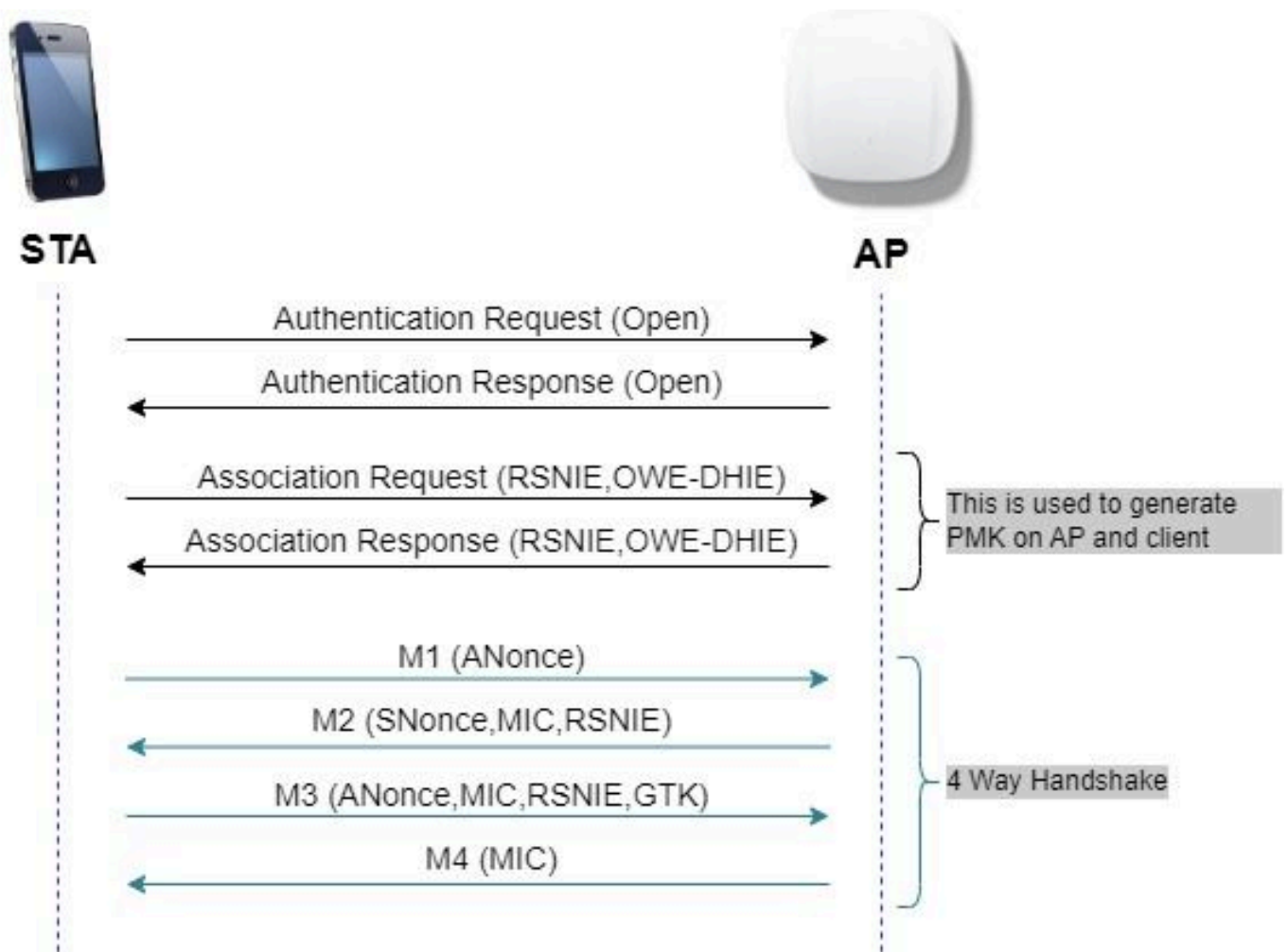
SAE	<input type="checkbox"/>	FT + SAE	<input checked="" type="checkbox"/>
OWE	<input type="checkbox"/>	FT + 802.1x	<input type="checkbox"/>
802.1x- SHA256	<input type="checkbox"/>		
Anti Clogging Threshold*		<input type="text" value="1500"/>	
Max Retries*		<input type="text" value="5"/>	
Retransmit Timeout*		<input type="text" value="400"/>	
PSK Format		<input type="text" value="ASCII"/>	▼
PSK Type		<input type="text" value="Unencrypted"/>	▼
Pre-Shared Key*		<input type="text" value="....."/>	
SAE Password Element 		<input type="text" value="Both H2E and HnP"/>	▼

AKM Options

OWE

Opportunistic Wireless Encryption (OWE) is an extension to IEEE 802.11 that provides encryption of the wireless medium ([IETF RFC 8110](#)). The purpose of OWE based authentication is avoid open unsecured wireless connectivity between the AP's and clients. The OWE uses the Diffie-Hellman algorithms based

Cryptography to setup the wireless encryption. With OWE, the client and AP perform a Diffie-Hellman key exchange during the access procedure and use the resulting pairwise master key (PMK) secret with the 4-way handshake. The use of OWE enhances wireless network security for deployments where Open or shared PSK based networks are deployed.



OWE frame exchange

SAE

WPA3 use a new authentication and key management mechanism called Simultaneous Authentication of Equals. This mechanism is further enhanced through the use of SAE Hash-to-Element (H2E).

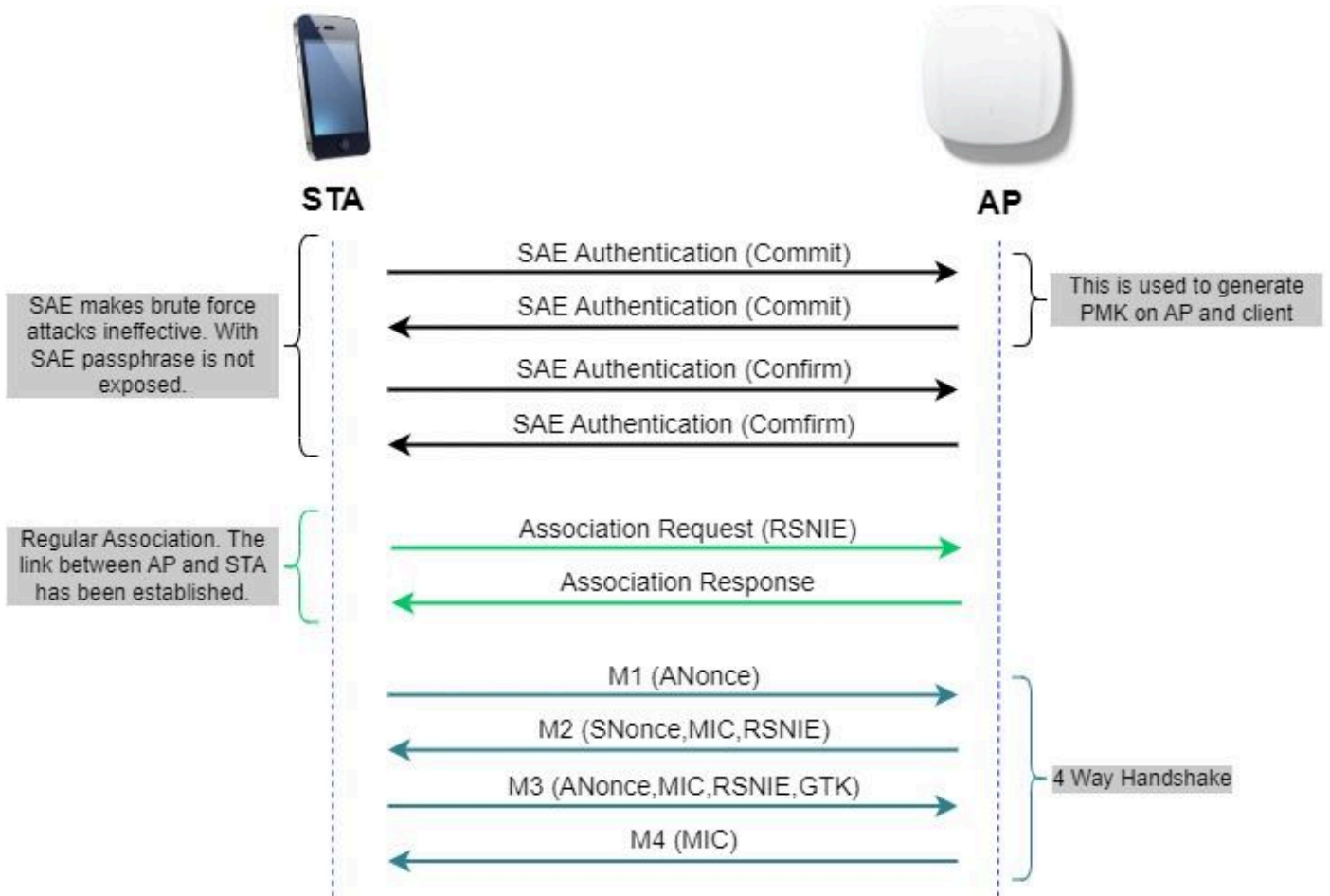
SAE with H2E is mandatory for WPA3 and Wi-Fi 6E.

SAE employs a discrete logarithm cryptography to perform an efficient exchange in a way that performs mutual authentication using a password that is probably resistant to an offline dictionary attack.

An offline dictionary attack is where an adversary attempts to determine a network password by trying possible passwords without further network interaction.

When the client connects to the access point, they perform an SAE exchange. If successful, they create each a cryptographically strong key, from which the session key is derived. Basically a client and access point goes into phases of commit and then confirm.

Once there is a commitment, the client and access point can then go into the confirm states each time there is a session key to be generated. The method uses forward secrecy, where an intruder could crack a single key, but not all of the other keys.



SAE frame exchange

Hash-to-Element (H2E)

Hash-to-Element (H2E) is a new SAE Password Element (PWE) method. In this method, the secret PWE used in the SAE protocol is generated from a password.

When a station (STA) that supports H2E initiates SAE with an AP, it checks whether AP supports H2E. If yes, the AP uses the H2E to derive the PWE by using a newly defined Status Code value in the SAE Commit message.

If STA uses Hunting-and-Pecking (HnP), the entire SAE exchange remains unchanged.

While using the H2E, the PWE derivation is divided into these components:

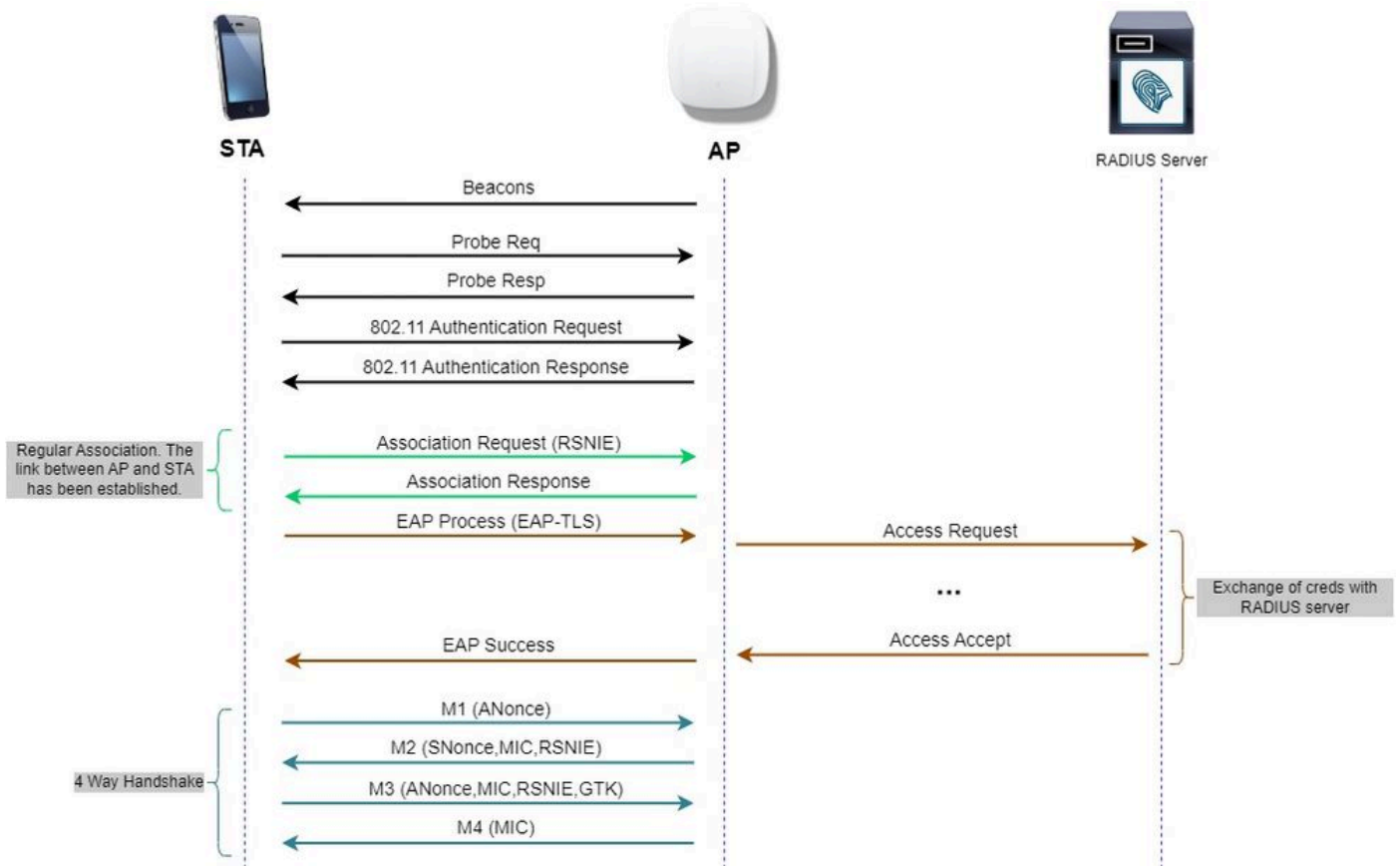
- Derivation of a secret intermediary element (PT) from the password. This can be performed offline when the password is initially configured on the device for each supported group.
- Derivation of the PWE from the stored PT. This depends on the negotiated group and MAC addresses of peers. This is performed in real-time during the SAE exchange.



Note: 6-GHz supports only Hash-to-Element SAE PWE method.

WPA-Enterprise aka 802.1x

WPA3-Enterprise is the most secure version of WPA3 and uses a username plus password combination with 802.1X for user authentication with a RADIUS server. By default, WPA3 uses 128-bit encryption, but it also introduces an optionally configurable 192-bit cryptographic strength encryption, which gives additional protection to any network transmitting sensitive data.



WPA3 Enterprise diagram flow

Level Set: WPA3 Modes





- WPA3-Personal
 - WPA3-Personal only mode
 - PMF Required
 - WPA3-Personal Transition mode
 - Configuration rules: On an AP, whenever WPA2-Personal is enabled, the WPA3-Personal Transition mode must also be enabled by default, unless explicitly overridden by the administrator to operate in WPA2-Personal only mode
- WPA3-Enterprise
 - WPA3-Enterprise only mode
 - PMF shall be negotiated for all WPA3 connections
 - WPA3-Enterprise Transition mode
 - PMF shall be negotiated for a WPA3 connection
 - PMF optional for a WPA2 connection
 - WPA3-Enterprise suite-B “192-bit” mode aligned with Commercial National Security Algorithm (CNSA)
 - More than just for the federal government
 - Consistent cryptographic cipher suites to avoid misconfiguration
 - Addition of GCMP & ECCP for crypto and better hash functions (SHA384)
 - PMF Required
 - WPA3 192-bit security shall be exclusive for EAP-TLS, which shall require certificates on both the supplicant and RADIUS server.

- To use WPA3 192-bit enterprise, the RADIUS servers must use one of the permitted EAP ciphers:

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

To know more about detailed information about WPA3 implementation in Cisco WLANs, including client security compatibility matrix, please feel free to check the [WPA3 Deployment Guide](#).

Cisco Catalyst Wi-Fi 6E APs

Ideal for Small to Medium-sized deployments	Best In Class, Flexibility		Mission Critical, Performance
 <p>CW9162</p> <ul style="list-style-type: none"> • 2x2 + 2x2 + 2x2 • 2.5 Gbps mGig • Power Options: PoE, DC Power • IoT ready + Bluetooth 5.x • Partial iCAP • USB - 4.5 W <p><small>Available with IOS-XE 17.9.2</small></p>	 <p>CW9164</p> <ul style="list-style-type: none"> • 2x2, 4x4, 4x4 • 2.5 Gbps mGig • Power Options: PoE, DC Power • IoT Ready + Bluetooth 5.x • Partial iCAP • USB- 4.5 W 	 <p>CW9166</p> <ul style="list-style-type: none"> • 4x4 + 4x4 + 4x4 (XOR 5/6) • 5 Gbps mGig • Power Options: PoE, DC Power • IoT ready + Bluetooth 5.x • Environmental Sensor • Full Packet Capture (iCAP) • Zero-Wait DFS* • USB - 4.5W 	 <p>C9136</p> <ul style="list-style-type: none"> • 4x4, 8x8, 4x4 (or) 4x4, 4x4+4x4, 4x4 • Dual 5 Gbps mGig, active fail over • PoE Redundancy • IoT ready • Bluetooth 5.x • Environmental Sensor • Full Packet Capture (iCAP) • Zero-Wait DFS* • USB - 9W <p><small>*Available in Future</small></p>
Full radio capability (6 GHz @ LPI) on single 30W PoE+			
Dedicated Radio for CleanAir Pro	Same Bracket, Industrial Design	AP Power Optimization	USB

Wi-Fi 6E Access Points

Clients Supported Security Settings

You can find which product support WPA3-Enterprise using WiFi Alliance webpage [product finder](#).

On windows devices you can verify what are the security settings supported by the adapter using the command "netsh wlan show drivers".

Here you can see the output of Intel AX211:

```

C:\Users\tantunes>netsh wlan show drivers

Interface name: Wi-Fi

Driver                : Intel(R) Wi-Fi 6E AX211 160MHz
Vendor                : Intel Corporation
Provider              : Intel
Date                  : 3/9/2023
Version               : 22.200.2.1
INF file               : oem151.inf
Type                  : Native Wi-Fi Driver
Radio types supported : 802.11b 802.11g 802.11n 802.11a 802.11ac 802.11ax
FIPS 140-2 mode supported : Yes
802.11w Management Frame Protection supported : Yes
Hosted network supported : No
Authentication and cipher supported in infrastructure mode:
    Open                None
    Open                WEP-40bit
    Open                WEP-104bit
    Open                WEP
    WPA-Enterprise      TKIP
    WPA-Enterprise      CCMP
    WPA-Personal        TKIP
    WPA-Personal        CCMP
    WPA2-Enterprise     TKIP
    WPA2-Enterprise     CCMP
    WPA2-Personal       TKIP
    WPA2-Personal       CCMP
    Open                Vendor defined
    WPA3-Personal       CCMP
    Vendor defined      Vendor defined
    WPA3-Enterprise     192 Bits GCMP-256
    OWE                 CCMP
    WPA3-Enterprise     CCMP
    WPA3-Enterprise     TKIP

Number of supported bands : 3
    2.4 GHz [ 0 MHz - 0 MHz]
    5 GHz  [ 0 MHz - 0 MHz]
    6 GHz  [ 0 MHz - 0 MHz]

IHV service present    : Yes
IHV adapter OUI        : [00 00 00], type: [00]
IHV extensibility DLL path: C:\WINDOWS\System32\DriverStore\FileRepository\netwtw6e.inf_amd64_eda979fbdede064\IntelIHVRouter12.dll

```

Windows output of _netsh wlan show driver_ for client AX211

Netgear A8000:

Interface name: A8000_NETGEAR

```
Driver : NETGEAR A8000 WiFi 6 & 6E Adapter
Vendor : NETGEAR Inc.
Provider : MediaTek, Inc.
Date : 11/25/2022
Version : 1.0.0.108
INF file : oem9.inf
Type : Native Wi-Fi Driver
Radio types supported : 802.11b 802.11a 802.11g 802.11n 802.11ac 802.11ax
FIPS 140-2 mode supported : Yes
802.11w Management Frame Protection supported : Yes
Hosted network supported : No
Authentication and cipher supported in infrastructure mode:
      Open          None
      Open          WEP-40bit
      Open          WEP-104bit
      Open          WEP
      WPA-Enterprise TKIP
      WPA-Enterprise CCMP
      WPA3-Personal  CCMP
      OWE            CCMP
      WPA-Personal  TKIP
      WPA-Personal  CCMP
      WPA2-Enterprise TKIP
      WPA2-Enterprise CCMP
      WPA2-Personal  TKIP
      WPA2-Personal  CCMP
Number of supported bands : 3
      2.4 GHz [ 0 MHz - 0 MHz]
      5 GHz   [ 0 MHz - 0 MHz]
      6 GHz   [ 0 MHz - 0 MHz]
IHV service present : Yes
IHV adapter OUI : [00 00 00], type: [00]
IHV extensibility DLL path: C:\WINDOWS\system32\mtknhvux.dll
IHV UI extensibility CLSID: {00000000-0000-0000-0000-000000000000}
IHV diagnostics CLSID : {00000000-0000-0000-0000-000000000000}
Wireless Display Supported: Yes (Graphics Driver: Yes, Wi-Fi Driver: Yes)
```

Windows output of `_netsh wlan show driver_` for client Netgear A8000s

Android Pixel 6a:



None

Enhanced Open

WEP

WPA/WPA2-Personal

WPA3-Personal

WPA/WPA2-Enterprise

WPA3-Enterprise

WPA3-Enterprise 192-bit



CIF



: Even though there are no clients supporting GCMP128 cipher + SUITEB-1X as of writing this document, it was tested to observe it being broadcasted and check the RSN info in the beacons.

WPA3 - AES(CCPM128) + OWE

This is the WLAN Security configuration:

The screenshot displays the Cisco Catalyst 9800-CL Wireless Controller GUI. On the left, a navigation sidebar includes Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main area shows the 'WLANs' configuration page with a table of WLANs: MacFilter (ID 1), dot1x (ID 2), and wifi6e_test (ID 5). The 'Edit WLAN' window for 'wifi6e_test' is open, showing the 'Security' tab. Under 'Layer2', 'WPA3' is selected. In the 'WPA Parameters' section, 'WPA3 Policy' is checked. Under 'WPA2/WPA3 Encryption', 'AES(CCMP128)' is checked. In the 'Auth Key Mgmt' section, 'OWE' is checked, and 'Transition Mode WLAN ID' is set to 0. A blue note at the bottom right states: 'Transition Mode WLAN ID = 0 means there is no transition WLAN'.

OWE Security Settings

View on WLC GUI of the WLAN Security settings:

This screenshot shows a close-up of the WLC GUI for the 'wifi6e_test' WLAN. The security settings are displayed as follows: WPA2/WPA3 Encryption: AES(CCMP128) [checked], CCMP256 [unchecked], GCMP128 [unchecked], GCMP256 [unchecked]. Auth Key Mgmt: SAE [unchecked], OWE [checked], FT + SAE [unchecked], FT + 802.1x [unchecked]. Transition Mode WLAN ID: 0.

WLAN Security settings on WLC GUI

Here we can observe Wi-Fi 6E clients connection process:

Intel AX211

Here we show the complete connection process of client Intel AX211.

OWE Discovery

Here you can see the beacons OTA. The AP advertises support for OWE using AKM suite selector for OWE under RSN information element.

You can see AKM suite type value 18 (00-0F-AC:18) that indicates OWE support.

Frame 151: 355 bytes on wire (2840 bits), 355 bytes captured (2840 bits) on interface 'Device\NPF_{04572965-2998-4456-8C33-C4316A3486} ...'

IEEE 802.11 wireless management

- Fixed parameters (12 bytes)
- Tagged parameters (263 bytes)
 - Tag: SSID parameter set: "wifi4test"
 - Tag: Supported rates (4(0), 5, 10(0), 18, 24(0), 36, 48, 54, [MST/sec])
 - Tag: Traffic Indication Map (TID) OTS = 4, Status
 - Tag: Country information: Country code na, environment global operating classes
 - Tag: Power Constraint 4
 - Tag: TX Power Envelope
 - Tag: TX Power Envelope
 - Tag: TX Power Envelope
 - Tag: Multiple SSID Configuration
 - Tag: HE Capabilities
 - Tag: HE Operation
- RSN Capabilities: 0x0000
 - RSN Version: 1
 - Group Cipher Suite: 00:0fac (See 802.11) AES (CCM)
 - Auth Key Management (AKM) List: 00:0fac (See 802.11) Opportunistic Wireless Encryption
 - Auth Key Management (AKM) Suites: 00:0fac (See 802.11) Opportunistic Wireless Encryption
 - Auth Key Management (AKM) OUI: 00:00:00 (See 802.11)
 - Auth Key Management (AKM) Type: Opportunistic Wireless Encryption (18)
 - RSN Capabilities: 0x0000
 - RSN Pre-auth capabilities: Transmitter does not support pre-authentication
 - RSN No Pairwise capabilities: Transmitter can support WP default key & simultaneously with Pairwise
 - RSN PTKSA Replay Counter capabilities: 4 replay counters per PTKSA/TKSA/TAckeySA (8x2)
 - Management frame Protection Required: True
 - Management frame Protection Capabilities: 4 replay counters per PTKSA/TKSA/TAckeySA (8x2)
 - Join Multi-SSID SSID: False
 - Peerkey Enabled: False
 - Extended Key ID for Individually Addressed Frames: Not supported
- PMKID List: 0
- Group Management Cipher Suite: 00:0fac (See 802.11) BIP (128)
- Group Key Element: 00:0fac (See 802.11) CCX Version 1
- Tag: HE Embedded Capabilities (18 octets)
- Tag: TX Power Envelope
- Tag: TX Power Envelope
- Tag: TX Power Envelope
- Tag: Multiple SSID Configuration
- Tag: HE Capabilities
- Tag: HE Operation

OWE beacon frame

If you look at RSN capabilities field, you can see AP is advertising both Management Frame Protection (MFP) capabilities and MFP required bit set to 1.

OWE Association

You can see the UPR sent in broadcast mode and then the association itself.

The OWE starts with the OPEN authentication request and response:

Frame 8: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface 'Device\NPF_{04572965-2998-4456-8C33-C4316A3486} ...'

IEEE 802.11 Authentication, Flags:C

- Fixed parameters (6 bytes)
- Authentication Algorithm: Open System (0)
- Authentication SEQ: 0x0000
- Status code: Successful (0x0000)

Frame 11: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface 'Device\NPF_{04572965-2998-4456-8C33-C4316A3486} ...'

IEEE 802.11 Authentication, Flags:C

- Fixed parameters (6 bytes)
- Authentication Algorithm: Open System (0)
- Authentication SEQ: 0x0002
- Status code: Successful (0x0000)

Then, a client that wants to do OWE must indicate OWE AKM in the RSN IE of Association Request frame and include Diffie Helman (DH) parameter element:

Frame 11: 284 bytes on wire (2272 bits), 284 bytes captured (2272 bits) on interface 10vnic1/vpp_04578966-2998-4456-8C33-C431664343

Frame 12: 278 bytes on wire (2208 bits), 278 bytes captured (2208 bits) on interface 10vnic1/vpp_04578966-2998-4456-8C33-C431664343

Frame 8: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface 10vnic1/vpp_04578966-2998-4456-8C33-C431664343

Frame 10: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface 10vnic1/vpp_04578966-2998-4456-8C33-C431664343

OWE Association response

After the association response we can see the 4-way handshake and client moves to connected state.

Here you can see the client details on the WLC GUI:

Client Properties: AP Properties, Security Information, Client Statistics, QOS Properties, EoGRE

Client State Servers	None
Client ACLs	None
Client Entry Create Time	43 seconds
Policy Type	WPA3
Encryption Cipher	CCMP (AES)
Authentication Key Management	OWE
EAP Type	Not Applicable
Capabilities Timeout	30min

NetGear A8000

Connection OTA with focus on the RSN information from client:

Samsung S23

Connection OTA with focus on the RSN information from client:

Client details in WLC:

WPA3 - AES(CCMP128) + OWE with Transition Mode

Detailed configuration and troubleshooting of OWE Transition Mode available in this document: [Configure Enhanced Open SSID with Transition Mode - OWE.](#)

WPA3-Personal - AES(CCMP128) + SAE

WLAN Security configuration:

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

Layer2 Layer3 AAA

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP None

MAC Filtering

Lobby Admin Access

WPA Parameters

WPA Policy WPA2 Policy
GTK Randomize WPA3 Policy
Transition Disable

Fast Transition

Status

Over the DS

Reassociation Timeout *

WPA2/WPA3 Encryption

AES(CCMP128) CCMP256
GCMP128 GCMP256

Auth Key Mgmt

SAE FT - SAE
OWE FT - 802.1x
802.1x-SHA256

Anti Clogging Threshold*

Max Retries*

Retransmit Timeout*

PSK Format

PSK Type

Pre-Shared Key*

SAE Password Element ⓘ

Protected Management Frame

PMF

Association Comeback Timer*

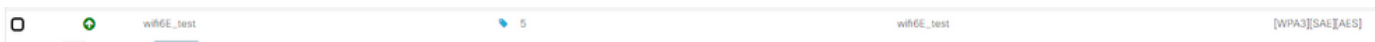
SA Query Time*

WPA3 SAE Configuration



Note: Keep in mind that Hunting and Pecking is not allowed with 6 GHz radio policy. When you configure a 6GHz only WLAN, you must select H2E SAE Password Element.

View on WLC GUI of the WLAN Security settings:



Verification of beacons OTA:

NetGear A8000

Connection OTA with focus on the RSN information from client:

Client details in WLC:

Pixel 6a

Connection OTA with focus on the RSN information from client:

Cisco Catalyst 9800-CL Wireless Controller

Welcome admin

Search APs and Clients

Feedback

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Delete

Selected 0 out of 12 Clients

	Client MAC Address	IPv4 Address	IPv6 Address	AP Name
<input type="checkbox"/>	0012.17e1.dd57	192.168.1.33	fe80::212:17ff:fee1:dd57	AP03_Sotao_9548
<input type="checkbox"/>	0012.17e2.4856	192.168.1.37	fe80::212:17ff:fee2:4856	AP05_OutdoorB_220
<input type="checkbox"/>	0012.17e2.4b40	192.168.1.31	fe80::212:17ff:fee2:4b40	AP04_OutdoorF_300
<input type="checkbox"/>	0429.2ec9.e371	192.168.1.160	fe80::6a20:34e8:ab1b:6332	AP6849.9253.CA50
<input type="checkbox"/>	0c8b.9509.3518	192.168.1.129	N/A	AP03_Sotao_9548
<input type="checkbox"/>	34ea.e702.6240	192.168.1.70	N/A	AP6849.9253.CA50
<input type="checkbox"/>	60fb.008b.0e66	N/A	N/A	AP01_RC_9136_F80
<input type="checkbox"/>	84d8.1b0f.294f	192.168.1.91	N/A	AP03_Sotao_9548
<input type="checkbox"/>	9669.5a28.a115	192.168.1.138	fe80::9469:5aff:fe28:a115	AP02_Suite_1084
<input type="checkbox"/>	a810.87bb.b833	192.168.1.94	fe80::aa10:87ff:febb:b833	AP03_Sotao_9548

Client

360 View General QoS Statistics ATF Statistics Mobility History Call Statistics

Client Properties AP Properties Security Information Client Statistics QoS Properties EoGRE

Client State Servers None
 Client ACLs None
 Client Entry Create Time 78 seconds
 Policy Type WPA3
 Encryption Cipher CCMP (AES)
 Authentication Key Management SAE
 EAP Type Not Applicable
 Session Timeout 86400

Session Manager

Point of Attachment capwap_90000010
 IF ID 0x90000010
 Authorized TRUE
 Common Session ID 000000000000FB1B0A58F78
 Acct Session ID 0x00000000
 Auth Method Status List
 Method SAE

WPA3-Personal - AES(CCMP128) + SAE + FT

WLAN Security configuration:

Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

Layer2 Layer3 AAA

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP None

MAC Filtering

Lobby Admin Access

WPA Parameters

WPA Policy WPA2 Policy
 GTK Randomize WPA3 Policy
 Transition Disable

Fast Transition

Status
 Over the DS
 Reassociation Timeout *

WPA2/WPA3 Encryption

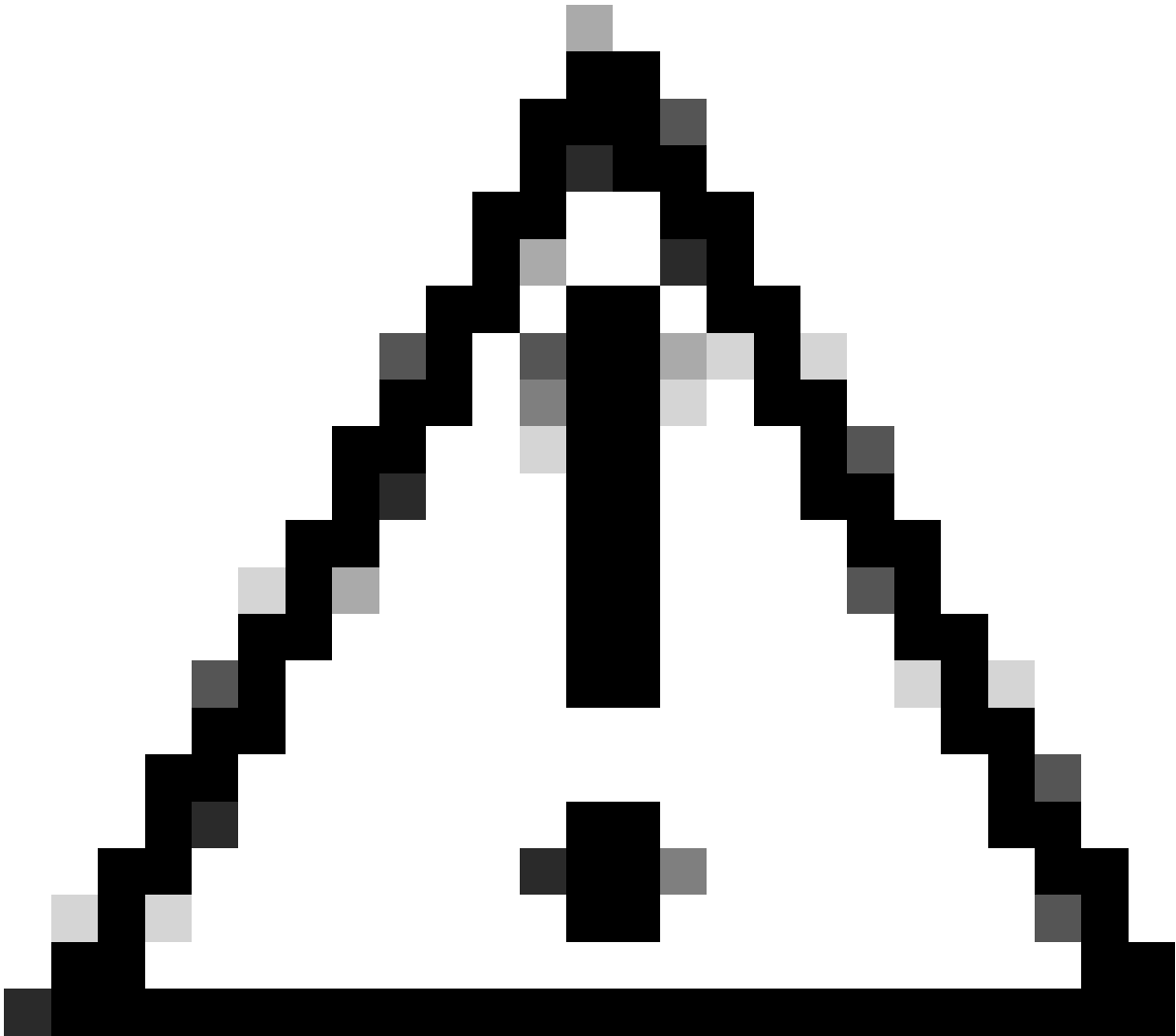
AES(OCMP128) CCMP256
 GCMP128 GCMP256

Auth Key Mgmt

SAE FT + SAE
 OWE FT + 802.1x
 802.1x-SHA256
 Anti Clogging Threshold*
 Max Retries*
 Retransmit Timeout*
 PSK Format
 PSK Type
 Pre-Shared Key*
 SAE Password Element

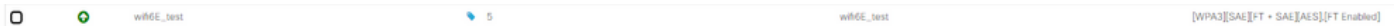
Protected Management Frame

PMF
 Association Comeback Timer*
 SA Query Time*



Caution: In the Authentication Key Management, the WLC allows to select FT+SAE without SAE enabled, however it was observed the clients were not able to connect. Always enable both check boxes SAE and FT+SAE if you want to use SAE with Fast Transition.

View on WLC GUI of the WLAN Security settings:



Verification of beacons OTA:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
1	2023-06-12 18:34:49.355337	0.000000	Cisco_13:180:e0	Eurocast	802.11	588	5	-36 dBm	Beacon frame, SWS=27, FwB, Flags=.....C, B=100, SSID="wifi6e"
2	2023-06-12 18:34:49.427544	0.102287	Cisco_13:180:e0	Eurocast	802.11	588	5	-36 dBm	Beacon frame, SWS=27, FwB, Flags=.....C, B=100, SSID="wifi6e"
3	2023-06-12 18:34:49.508567	0.182323	Cisco_13:180:e0	Eurocast	802.11	588	5	-37 dBm	Beacon frame, SWS=23, FwB, Flags=.....C, B=100, SSID="wifi6e"
4	2023-06-12 18:34:49.629332	0.182465	Cisco_13:180:e0	Eurocast	802.11	588	5	-37 dBm	Beacon frame, SWS=27, FwB, Flags=.....C, B=100, SSID="wifi6e"
5	2023-06-12 18:34:49.791804	0.096872	Netgear_48:78:95	Cisco_13:180:e0	802.11	360	5	-49 dBm	Probe Request, SWS=8, FwB, Flags=.....C, SSID="wifi6e_test"
6	2023-06-12 18:34:49.791804	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-37 dBm	Acknowledgment, Flags=.....C
7	2023-06-12 18:34:49.791804	0.000000	192.168.1.15	192.168.1.121	802.11	360	5	-49 dBm	Probe Request, SWS=1, FwB, Flags=.....C, SSID="wifi6e_test"
8	2023-06-12 18:34:49.791804	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-37 dBm	Acknowledgment, Flags=.....C
9	2023-06-12 18:34:49.794933	0.003066	Cisco_13:180:e0	Eurocast	802.11	588	5	-37 dBm	Beacon frame, SWS=23, FwB, Flags=.....C, B=100, SSID="wifi6e"
10	2023-06-12 18:34:49.818282	0.015789	Netgear_48:78:95	Cisco_13:180:e0	802.11	360	5	-49 dBm	Probe Request, SWS=1, FwB, Flags=.....C, SSID="wifi6e_test"
11	2023-06-12 18:34:49.818282	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-37 dBm	Acknowledgment, Flags=.....C
12	2023-06-12 18:34:49.874951	0.000000	Cisco_13:180:e0	Eurocast	802.11	194	5	-49 dBm	Authentication, SWS, FwB, Flags=.....C
13	2023-06-12 18:34:49.874951	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-37 dBm	Acknowledgment, Flags=.....C
14	2023-06-12 18:34:49.896563	0.021612	Cisco_13:180:e0	Netgear_48:78:95	802.11	194	5	-37 dBm	Authentication, SWS=24, FwB, Flags=.....C
15	2023-06-12 18:34:49.896563	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-49 dBm	Acknowledgment, Flags=.....C
16	2023-06-12 18:34:49.904966	0.000000	Cisco_13:180:e0	Eurocast	802.11	588	5	-37 dBm	Beacon frame, SWS=27, FwB, Flags=.....C, B=100, SSID="wifi6e"
17	2023-06-12 18:34:49.904966	0.000000	Netgear_48:78:95	Cisco_13:180:e0	802.11	130	5	-49 dBm	Authentication, SWS=5, FwB, Flags=.....C
18	2023-06-12 18:34:49.904966	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-37 dBm	Acknowledgment, Flags=.....C
19	2023-06-12 18:34:49.904966	0.000000	Netgear_48:78:95	Netgear_48:78:95	802.11	130	5	-37 dBm	Authentication, SWS=7, FwB, Flags=.....C
20	2023-06-12 18:34:49.904966	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-48 dBm	Acknowledgment, Flags=.....C
21	2023-06-12 18:34:49.904966	0.000000	Netgear_48:78:95	Cisco_13:180:e0	802.11	216	5	-49 dBm	Association Request, SWS, FwB, Flags=.....C, SSID="wifi6e_test"
22	2023-06-12 18:34:49.904966	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
23	2023-06-12 18:34:49.91474	0.005188	Cisco_13:180:e0	Netgear_48:78:95	802.11	262	5	-36 dBm	Association Response, SWS, FwB, Flags=.....C
24	2023-06-12 18:34:49.91474	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-49 dBm	Acknowledgment, Flags=.....C
25	2023-06-12 18:34:49.917179	0.000245	Netgear_48:78:95	Eurocast	LLC	114	5	-37 dBm	LS, func:unknown; DSAP 0x02 Individual, SSAP 0x02 Command
26	2023-06-12 18:34:49.917179	0.000000	Netgear_48:78:95	Eurocast	LLC	114	5	-36 dBm	LS, func:unknown; DSAP 0x02 Individual, SSAP 0x02 Response
27	2023-06-12 18:34:49.922346	0.010267	Cisco_13:180:e0	Eurocast	802.11	226	5	-49 dBm	Key Message 1 of 4
28	2023-06-12 18:34:49.922346	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-49 dBm	Acknowledgment, Flags=.....C
29	2023-06-12 18:34:49.999581	0.077235	Cisco_13:180:e0	Eurocast	802.11	588	5	-36 dBm	Beacon frame, SWS=27, FwB, Flags=.....C, B=100, SSID="wifi6e"
30	2023-06-12 18:34:50.104510	0.104029	Cisco_13:180:e0	Eurocast	802.11	588	5	-36 dBm	Beacon frame, SWS=27, FwB, Flags=.....C, B=100, SSID="wifi6e"
31	2023-06-12 18:34:50.204600	0.007824	Cisco_13:180:e0	Eurocast	802.11	588	5	-37 dBm	Beacon frame, SWS=23, FwB, Flags=.....C, B=100, SSID="wifi6e"
32	2023-06-12 18:34:50.211615	0.007815	Netgear_48:78:95	Cisco_13:180:e0	EAPOL	226	5	-55 dBm	Key Message 2 of 4
33	2023-06-12 18:34:50.211615	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-42 dBm	Acknowledgment, Flags=.....C
34	2023-06-12 18:34:50.213376	0.001761	Netgear_48:78:95	Eurocast	EAPOL	296	5	-42 dBm	Key Message 3 of 4
35	2023-06-12 18:34:50.213376	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-58 dBm	Acknowledgment, Flags=.....C
36	2023-06-12 18:34:50.214354	0.000978	Netgear_48:78:95	Cisco_13:180:e0	EAPOL	199	5	-56 dBm	Key Message 4 of 4
37	2023-06-12 18:34:50.213376	0.001924	Netgear_48:78:95	Eurocast	EAPOL	296	5	-42 dBm	Key Message 3 of 4
38	2023-06-12 18:34:50.220721	0.006367	192.168.1.15	192.168.1.121	802.11	76	5	-42 dBm	Acknowledgment, Flags=.....C
39	2023-06-12 18:34:50.224049	0.003128	192.168.1.15	192.168.1.121	802.11	119	5	-44 dBm	Trigger Buffer Status Report Poll (BSRP), Flags=.....C
40	2023-06-12 18:34:50.224049	0.000000	Netgear_48:78:95	Netgear_48:78:95	LLC	222	5	-44 dBm	LS, func:unknown; DSAP 0x02 Group, SSAP 0x02 Response
41	2023-06-12 18:34:50.224049	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-54 dBm	Acknowledgment, Flags=.....C

WPA3 SAE + FT Beacons

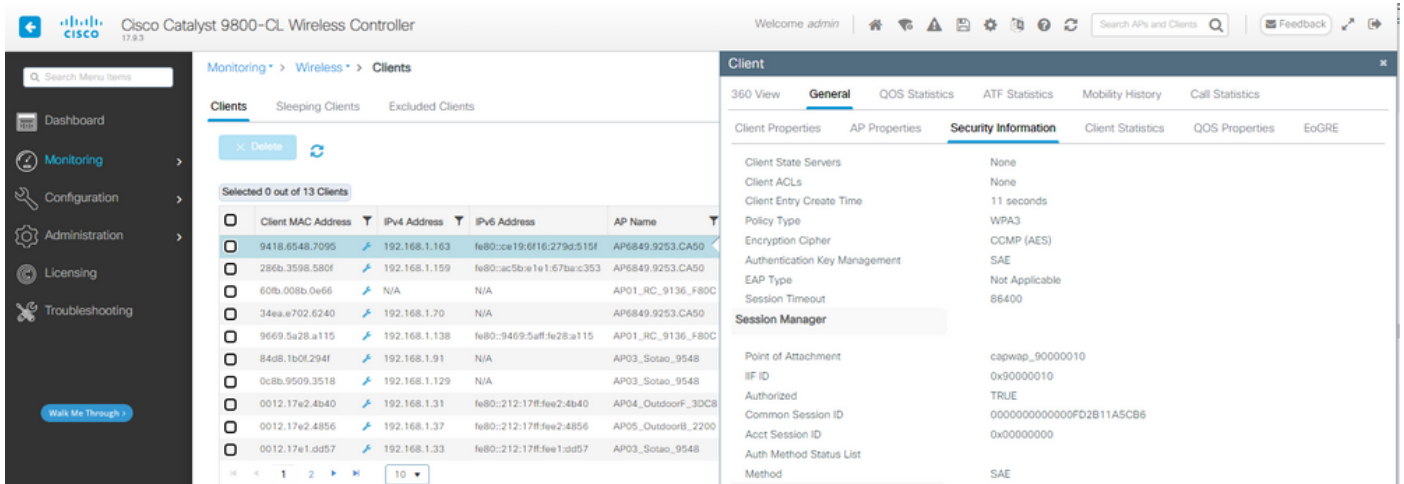
Here we can observe Wi-Fi 6E clients associating:

Intel AX211

Connection OTA with focus on the RSN information from client:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
1813	2023-06-12 18:51:51.249793	0.017337	IntelCorp_98:58:0f	Cisco_13:180:e0	802.11	194	5	-42 dBm	Authentication, SWS=8, FwB, Flags=.....C
1814	2023-06-12 18:51:51.249793	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1815	2023-06-12 18:51:51.254827	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-42 dBm	Acknowledgment, Flags=.....C
1816	2023-06-12 18:51:51.259394	0.002567	IntelCorp_98:58:0f	Cisco_13:180:e0	802.11	130	5	-45 dBm	Authentication, SWS=1, FwB, Flags=.....C
1817	2023-06-12 18:51:51.263979	0.004585	Cisco_13:180:e0	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1818	2023-06-12 18:51:51.263979	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-42 dBm	Acknowledgment, Flags=.....C
1819	2023-06-12 18:51:51.263979	0.000000	IntelCorp_98:58:0f	Cisco_13:180:e0	802.11	250	5	-46 dBm	Association Request, SWS=7, FwB, Flags=.....C, SSID="wifi6e_test"
1820	2023-06-12 18:51:51.267951	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1821	2023-06-12 18:51:51.271442	0.018463	IntelCorp_98:58:0f	Eurocast	LLC	114	5	-36 dBm	I, N(K)=8, N(C)=43; DSAP 0x02 Group, SSAP 0x02 Response
1822	2023-06-12 18:51:51.271442	0.000000	IntelCorp_98:58:0f	Eurocast	LLC	114	5	-36 dBm	I, N(K)=7, N(C)=32; DSAP 0x02 Group, SSAP 0x02 Response
1823	2023-06-12 18:51:51.277402	0.003240	Cisco_13:180:e0	Netgear_48:78:95	802.11	262	5	-36 dBm	Association Response, SWS, FwB, Flags=.....C
1824	2023-06-12 18:51:51.277402	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-43 dBm	Acknowledgment, Flags=.....C
1825	2023-06-12 18:51:51.282107	0.000785	Cisco_13:180:e0	Eurocast	802.11	517	5	-36 dBm	Beacon frame, SWS=27, FwB, Flags=.....C, B=100, SSID="wifi6e_test_02"
1826	2023-06-12 18:51:51.312349	0.025242	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1827	2023-06-12 18:51:51.316180	0.004849	192.168.1.15	192.168.1.121	802.11	76	5	-52 dBm	Clear-to-send, Flags=.....C
1828	2023-06-12 18:51:51.331425	0.017227	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1829	2023-06-12 18:51:51.338460	0.005835	Cisco_13:180:e0	Eurocast	802.11	517	5	-37 dBm	Beacon frame, SWS=26, FwB, Flags=.....C, B=100, SSID="wifi6e_test_02"
1830	2023-06-12 18:51:51.338460	0.001348	192.168.1.15	192.168.1.121	802.11	76	5	-53 dBm	Clear-to-send, Flags=.....C
1831	2023-06-12 18:51:51.339743	0.001135	192.168.1.121	802.11	82	5	-38 dBm	Request-to-send, Flags=.....C	
1832	2023-06-12 18:51:51.339892	0.000839	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C	
1833	2023-06-12 18:51:51.339912	0.000000	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C	
1834	2023-06-12 18:51:51.408524	0.000712	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1835	2023-06-12 18:51:51.408574	0.000060	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1836	2023-06-12 18:51:51.408574	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1837	2023-06-12 18:51:51.408574	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1838	2023-06-12 18:51:51.408574	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1839	2023-06-12 18:51:51.408574	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1840	2023-06-12 18:51:51.408574	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1841	2023-06-12 18:51:51.408574	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1842	2023-06-12 18:51:51.408574	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1843	2023-06-12 18:51:51.408574	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1844	2023-06-12 18:51:51.408574	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1845	2023-06-12 18:51:51.408574	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1846	2023-06-12 18:51:51.408574	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1847	2023-06-12 18:51:51.412651	0.000431	Cisco_13:180:e0	Eurocast	802.11	383	5	-37 dBm	Key Message 3 of 4
1848	2023-06-12 18:51:51.412651	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-48 dBm	Acknowledgment, Flags=.....C
1849	2023-06-12 18:51:51.412651	0.000000	Netgear_48:78:95	Cisco_13:180:e0	EAPOL	199	5	-51 dBm	Key Message 4 of 4

Roaming event where you can see the PMKID:



Pixel 6a

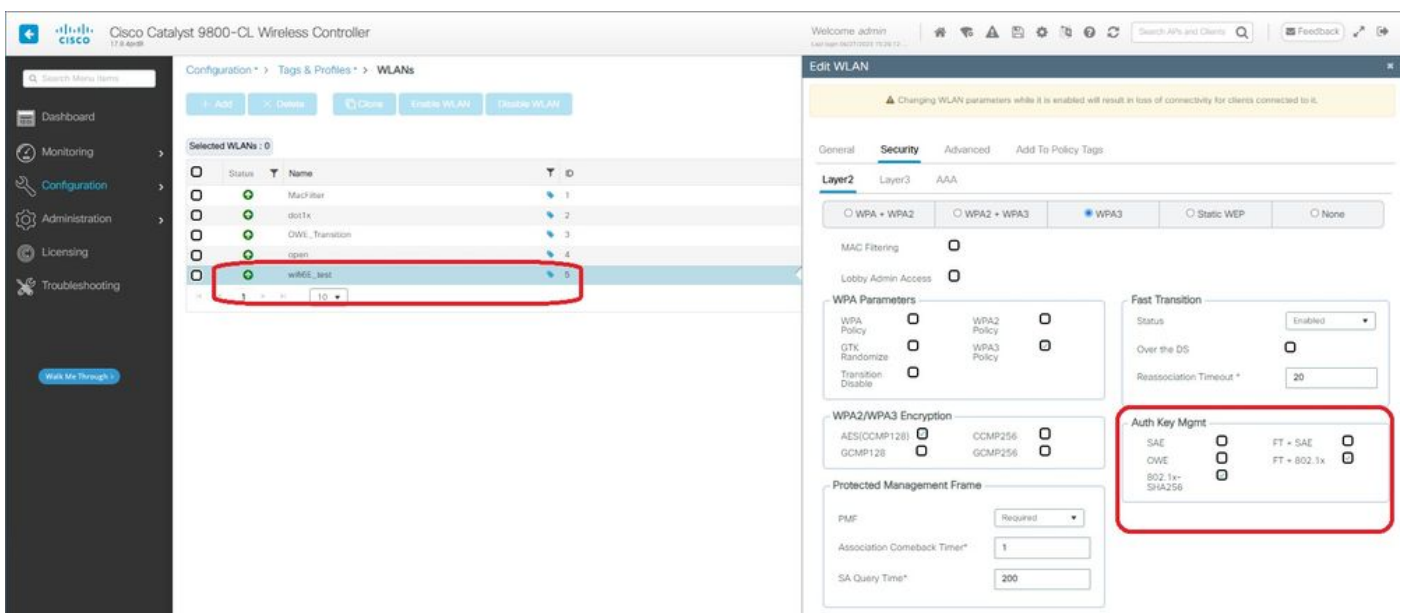
Device was not able to roam when FT is enabled.

Samsung S23

Device was not able to roam when FT is enabled.

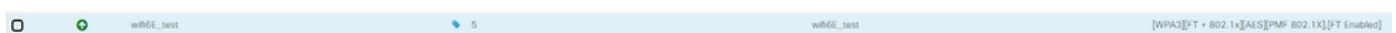
WPA3-Enterprise + AES(CCMP128) + 802.1x-SHA256 + FT

WLAN Security configuration:



WPA3 Enterprise 802.1x-SHA256 + FT WLAN Security Configuration

View on WLC GUI of the WLAN Security settings:



Here we can see the ISE Live logs showing the authentications coming from each device:

association frame followed by a complete EAP exchange because the client details were deleted from the AP/WLC.

This is basically the same frame exchange as in a new Association process. Here you can see the frame exchange:

The image shows a Wireshark packet capture of a WPA3 Enterprise 802.1x + FT Ax211 connection. The capture is divided into several sections:

- Probing and authentication frames:** This section shows the initial probe requests and responses, including authentication frames. A red box highlights the 'Authentication Request' frame.
- Regular Association:** This section shows the regular association process, including the 'Request to send' and 'Clear to send' frames. A green box highlights the 'Request to send' frame.
- EAP Exchange:** This section shows the EAP exchange, including the 'EAP-Request' and 'EAP-Response' frames. A red box highlights the 'EAP-Response' frame, which contains the PMKID used for FT.
- 4 Way Handshake:** This section shows the 4-way handshake, including the 'Key Message 1 of 4' and 'Key Message 2 of 4' frames. A blue box highlights the 'Key Message 1 of 4' frame.

WPA3 Enterprise 802.1x + FT Ax211 Connection flow

Client details in WLC:

The screenshot shows the Cisco WLC Client configuration page. The 'Client' tab is selected, and the 'Security Information' section is expanded. The client details are as follows:

- Client MAC Address:** 286b.3598.580f
- IPv4 Address:** 192.168.1.159
- IPv6 Address:** 2001:8a0:fb01:1:c00:c07a:1190:8069:7398
- AP Name:** AP9136_5C F524
- SSID:** wlan1
- Re-Authentication Timeout:** 1800 sec (Remaining time: 462 sec)
- Client State Servers:** None
- Client ACLs:** None
- Client Entry Create Time:** 1338 seconds
- Policy Type:** WPA3
- Encryption Cipher:** CCMP (AES)
- Authentication Key Management:** FT-802.1x
- EAP Type:** PEAP
- Session Timeout:** 1800

WPA3 Enterprise 802.1x + FT Client details

This client was also tested using FT over the DS and was able to roam using 802.11r:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
3028	16.491589	0.182241	Cisco_5d:58:18	Broadcast	802.11	364	69	-36 dbm	Beacon Frame, SSID=wifitest, Flags=.....C, B1=180, SSID=wifitest
3029	16.504273	0.120808	Cisco_5d:58:18	Broadcast	802.11	364	69	-36 dbm	Beacon Frame, SSID=wifitest, Flags=.....C, B1=180, SSID=wifitest
3030	16.544794	0.450521	IntelCor_98:18:0f	Broadcast	802.11	368	69	-45 dbm	Probe Request, SSID=wifitest, Flags=.....C, SSID=wifitest (R)
3031	16.544794	0.000000	Cisco_5d:58:18	Broadcast	802.11	322	69	-38 dbm	Probe Response, SSID=wifitest, Flags=.....C, B1=180, SSID=wifitest
3079	16.695429	0.651635	Cisco_5d:58:18	Broadcast	802.11	364	69	-38 dbm	Beacon Frame, SSID=wifitest, Flags=.....C, B1=180, SSID=wifitest
3080	16.702450	0.000000	IntelCor_98:18:0f	Cisco_5d:58:18	802.11	218	69	-46 dbm	Authentication, SSID=wifitest, Flags=.....C
3081	16.701542	0.000007	192.168.1.15	192.168.1.121	802.11	76	69	-39 dbm	Acknowledgment, Flags=.....C
3082	16.706278	0.004736	Cisco_5d:58:18:0f	IntelCor_98:18:0f	802.11	247	69	-38 dbm	Authentication, SSID=wifitest, Flags=.....C
3083	16.706278	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-39 dbm	Acknowledgment, Flags=.....C
3084	16.706278	0.000000	Cisco_5d:58:18:0f	IntelCor_98:18:0f	802.11	372	69	-48 dbm	Association Request, SSID=wifitest, Flags=.....C, SSID=wifitest
3085	16.706278	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-38 dbm	Acknowledgment, Flags=.....C
3086	16.718126	0.000020	Cisco_5d:58:18:0f	IntelCor_98:18:0f	802.11	413	69	-39 dbm	Association Response, SSID=wifitest, Flags=.....C
3088	16.731216	0.000000	192.168.1.121	192.168.1.121	802.11	76	69	-41 dbm	Acknowledgment, Flags=.....C
3092	16.727450	0.000000	IntelCor_98:18:0f	Cisco_5d:58:18:0f	802.11	223	69	-59 dbm	I P, N(0)=18, N(5)=002: SSAP SNAP Group, SSAP Bnd Response
3092	16.727457	0.000008	192.168.1.15	192.168.1.121	802.11	76	69	-47 dbm	Acknowledgment, Flags=.....C
3095	16.740833	0.613376	IntelCor_98:18:0f	Broadcast	LLC	525	69	-59 dbm	U P, func=Unknown; SSAP Bnd Individual, SSAP Bnd Command
3096	16.740833	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-48 dbm	Acknowledgment, Flags=.....C
3099	16.742984	0.000071	IntelCor_98:18:0f	IntelCor_98:18:0f	LLC	183	69	-50 dbm	I P, N(0)=18, N(5)=002: SSAP SNAP Group, SSAP Bnd Command
3100	16.742984	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-53 dbm	Acknowledgment, Flags=.....C
3101	16.742984	0.000000	Cisco_5d:58:18:0f	IntelCor_98:18:0f	LLC	183	69	-50 dbm	I, N(0)=18, N(5)=002: SSAP SNAP Individual, SSAP Bnd Command
3102	16.742984	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-53 dbm	Acknowledgment, Flags=.....C
3106	16.740833	0.012521	IntelCor_98:18:0f	IPVencast_4f:70:c5:1b	LLC	223	69	-59 dbm	I P, N(0)=18, N(5)=002: SSAP Bnd Individual, SSAP Bnd Response
3107	16.740833	0.000124	192.168.1.15	192.168.1.121	802.11	76	69	-48 dbm	Acknowledgment, Flags=.....C
3109	16.772475	0.003842	Cisco_5d:58:18:0f	IntelCor_98:18:0f	802.11	118	69	-40 dbm	Action, S(0)=1, F(0)=0: SSAP SNAP Group, SSAP Bnd Command
3110	16.772475	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-52 dbm	Acknowledgment, Flags=.....C
3113	16.771242	0.000000	IntelCor_98:18:0f	LLC	179	69	-59 dbm	I P, N(0)=18, N(5)=002: SSAP SNAP Group, SSAP Bnd Command	
3114	16.771242	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-48 dbm	Acknowledgment, Flags=.....C
3115	16.773436	0.000024	IntelCor_98:18:0f	Cisco_5d:58:18:0f	802.11	118	69	-48 dbm	Action, S(0)=1, F(0)=0: SSAP SNAP Group, SSAP Bnd Command
3116	16.773436	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-41 dbm	Acknowledgment, Flags=.....C
3120	16.771242	0.000000	IntelCor_98:18:0f	LLC	179	69	-49 dbm	U, func=Unknown; SSAP Bnd Group, SSAP Bnd Command	
3122	16.770545	0.001433	Cisco_5d:58:18:0f	IntelCor_98:18:0f	802.11	118	69	-48 dbm	Action, S(0)=1, F(0)=0: SSAP SNAP Group, SSAP Bnd Command
3123	16.770545	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-52 dbm	Acknowledgment, Flags=.....C
3124	16.770545	0.001854	IntelCor_98:18:0f	Cisco_5d:58:18:0f	802.11	118	69	-48 dbm	Action, S(0)=1, F(0)=0: SSAP SNAP Group, SSAP Bnd Command
3125	16.770545	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-48 dbm	Acknowledgment, Flags=.....C
3128	16.781409	0.003058	Atitocor_98:18:0f	IntelCor_98:18:0f	LLC	197	69	-49 dbm	U P, func=Unknown; SSAP Bnd Individual, SSAP Bnd Command
3132	16.781409	0.000000	IntelCor_98:18:0f	Atitocor_98:18:0f	LLC	222	69	-58 dbm	U, func=Unknown; SSAP Bnd Group, SSAP Bnd Command
3133	16.781409	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-47 dbm	Acknowledgment, Flags=.....C
3136	16.790815	0.000000	IntelCor_98:18:0f	IntelCor_98:18:0f	LLC	202	69	-58 dbm	I P, N(0)=18, N(5)=002: SSAP SNAP Group, SSAP Bnd Command
3137	16.790815	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-47 dbm	Acknowledgment, Flags=.....C
3140	16.793447	0.002599	IntelCor_98:18:0f	IntelCor_98:18:0f	LLC	525	69	-58 dbm	I, N(0)=18, N(5)=002: SSAP SNAP Extended LLC Group, SSAP Netframe
3141	16.793447	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-47 dbm	Acknowledgment, Flags=.....C
3144	16.791774	0.000027	IntelCor_98:18:0f	Broadcast	LLC	179	69	-58 dbm	S, func=002: SSAP Bnd Individual, SSAP Bnd Response
3145	16.793447	0.000075	192.168.1.15	192.168.1.121	802.11	76	69	-48 dbm	Acknowledgment, Flags=.....C
3149	16.794563	0.000714	IntelCor_98:18:0f	IPVencast_4f:70:c5:1b	LLC	183	69	-58 dbm	I P, N(0)=18, N(5)=002: SSAP SNAP Group, SSAP Bnd Response
3150	16.794563	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-48 dbm	Acknowledgment, Flags=.....C
3154	16.794563	0.000000	IntelCor_98:18:0f	IPVencast_4f:70:c5:1b	LLC	202	69	-58 dbm	I P, func=002: SSAP Bnd Group, SSAP Bnd Response
3155	16.794900	0.000004	192.168.1.15	192.168.1.121	802.11	76	69	-48 dbm	Acknowledgment, Flags=.....C
3158	16.795624	0.000624	IntelCor_98:18:0f	IPVencast_4f:70:c5:1b	LLC	215	69	-58 dbm	U P, func=Unknown; SSAP MAL SSAP Individual, SSAP Bayesian View
3210	16.790599	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-48 dbm	Acknowledgment, Flags=.....C
3240	16.790599	0.000000	IntelCor_98:18:0f	IPVencast_4f:70:c5:1b	LLC	215	69	-58 dbm	S, func=002: SSAP Bnd Group, SSAP Bnd Response
3242	16.795852	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-48 dbm	Acknowledgment, Flags=.....C

AX211 roaming with FT over DS

We can also see the FT roaming events:

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Selected 0 out of 1 Clients

Client MAC Address	IPv4 Address	IPv6 Address	AP Name	SSID	WLAN ID	Client Type
286b.3598.580f	192.168.1.159	N/A	AP01_RC_9136_F80C	wifitest	5	WLAN

Client

360 View General QOS Statistics ATF Statistics **Mobility History** Call Statistics

Recent association history:

AP Name	BSSID	AP Type	Assoc Time	Instance	Mobility Role	Run Latency (ms)	Roam Type
AP01_RC_9136_F80C	00d1.1dd4.a018	3	08/04/2023 14:24:27	0	Local	15	802.11R
AP136_SC_F524	00d1.1dd4.7d38	3	08/04/2023 14:22:59	0	Local	6	802.11R

WPA3 Enterprise with FT

And client ra trace from wlc:

```

Logging display requested on 2023/08/04 14:27:55 (GMT) for hostname: [wlc-9800-01], Model: [C9800-CL-WS], Version: [17.0.0.0], SW: [S9158H1805], MD_SW: [S9158H1805]
2023/08/04 14:22:59.31030237 [wlc_m_0-0] (1): [client-orch-wm] (15210): (note): MAC: 286b.3598.580f Re-Association received. BSSID 00d1.1dd4.7d38, WLAN wifitest, Slot 3 AP 00d1.1dd4.7d38, AP136_SC_F524, old BSSID 00d1.1dd4.a018
2023/08/04 14:22:59.31030237 [wlc_m_0-0] (1): [dot11] (15210): (note): MAC: 286b.3598.580f Association success. AID 33, Roaming = True, WGB = False, llc = True, llw = True Fast Roam = True
2023/08/04 14:22:59.31030237 [wlc_m_0-0] (1): [client-orch-wm] (15210): (note): MAC: 286b.3598.580f Delete mobile payload sent for BSSID: 00d1.1dd4.a018 WTP mac: 00d1.1dd4.a018 slot 3
2023/08/04 14:22:59.31030237 [wlc_m_0-0] (1): [client-auth] (15210): (note): MAC: 286b.3598.580f Client state transition: S_CO_JOIN --> S_CO_L1_AUTH_IN_PROGRESS
2023/08/04 14:22:59.31030237 [wlc_m_0-0] (1): [client-auth] (15210): (note): MAC: 286b.3598.580f ADD MOBILE sent. Client state flags: 0x71 BSSID: MAC: 00d1.1dd4.7d38 capwap IFF: 0x00000000, Add mobiles sent: 1
2023/08/04 14:22:59.31030237 [wlc_m_0-0] (1): [client-orch-wm] (15210): (note): MAC: 286b.3598.580f Mobility Successful. Roam Type None, Sub Roam Type HS_SUB_ROAM_TYPE_INTRA_INSTANCE, Previous BSSID MAC: 00d1.1dd4.a018 Client IFF: 0x00000000, Client Role: Local Psk: 0x00000000 Psk: 0x0
2023/08/04 14:22:59.31030237 [wlc_m_0-0] (1): [client-auth] (15210): (note): MAC: 286b.3598.580f ADD MOBILE sent. Client state flags: 0x76 BSSID: MAC: 00d1.1dd4.7d38 capwap IFF: 0x00000000, Add mobiles sent: 1
2023/08/04 14:22:59.31030237 [wlc_m_0-0] (1): [client-orch-wm] (15210): (note): MAC: 286b.3598.580f Client state transition: S_CO_MOBILITY_DISCOVERY_IN_PROGRESS --> S_CO_DEATH_PLUMB_IN_PROGRESS
2023/08/04 14:22:59.31030237 [wlc_m_0-0] (1): [client-orch-wm] (15210): (note): MAC: 286b.3598.580f Client state transition: S_CO_DEATH_PLUMB_IN_PROGRESS --> S_CO_L1_LEARN_IN_PROGRESS
2023/08/04 14:22:59.31030237 [wlc_m_0-0] (1): [client-orch-wm] (15210): (note): MAC: 286b.3598.580f Client state transition: S_CO_L1_LEARN_IN_PROGRESS --> S_CO_JOIN
2023/08/04 14:24:27.91859521 [wlc_m_0-0] (1): [client-orch-wm] (15210): (note): MAC: 286b.3598.580f Re-Association received. BSSID 00d1.1dd4.a018, WLAN wifitest, Slot 3 AP 00d1.1dd4.a018, AP01_RC_9136_F80C, old BSSID 00d1.1dd4.7d38
2023/08/04 14:24:27.91859521 [wlc_m_0-0] (1): [dot11] (15210): (note): MAC: 286b.3598.580f Association success. AID 33, Roaming = True, WGB = False, llc = True, llw = True Fast Roam = True
2023/08/04 14:24:27.91859521 [wlc_m_0-0] (1): [client-orch-wm] (15210): (note): MAC: 286b.3598.580f Delete mobile payload sent for BSSID: 00d1.1dd4.7d38 WTP mac: 00d1.1dd4.7d38 slot 3
2023/08/04 14:24:27.91859521 [wlc_m_0-0] (1): [client-auth] (15210): (note): MAC: 286b.3598.580f Client state transition: S_CO_JOIN --> S_CO_L1_AUTH_IN_PROGRESS
2023/08/04 14:24:27.91859521 [wlc_m_0-0] (1): [client-auth] (15210): (note): MAC: 286b.3598.580f ADD MOBILE sent. Client state flags: 0x71 BSSID: MAC: 00d1.1dd4.a018 capwap IFF: 0x00000000, Add mobiles sent: 1
2023/08/04 14:24:27.91859521 [wlc_m_0-0] (1): [client-orch-wm] (15210): (note): MAC: 286b.3598.580f Client state transition: S_CO_L1_AUTH_IN_PROGRESS --> S_CO_MOBILITY_DISCOVERY_IN_PROGRESS
2023/08/04 14:24:27.91859521 [wlc_m_0-0] (1): [client-orch-wm] (15210): (note): MAC: 286b.3598.580f Mobility Successful. Roam Type None, Sub Roam Type HS_SUB_ROAM_TYPE_INTRA_INSTANCE, Previous BSSID MAC: 00d1.1dd4.7d38 Client IFF: 0x00000000, Client Role: Local Psk: 0x00000000 Psk: 0x0
2023/08/04 14:24:27.91859521 [wlc_m_0-0] (1): [client-auth] (15210): (note): MAC: 286b.3598.580f ADD MOBILE sent. Client state flags: 0x76 BSSID: MAC: 00d1.1dd4.a018 capwap IFF: 0x00000000, Add mobiles sent: 1
2023/08/04 14:24:27.91859521 [wlc_m_0-0] (1): [client-orch-wm] (15210): (note): MAC: 286b.3598.580f Client state transition: S_CO_MOBILITY_DISCOVERY_IN_PROGRESS --> S_CO_DEATH_PLUMB_IN_PROGRESS
2023/08/04 14:24:27.91859521 [wlc_m_0-0] (1): [client-orch-wm] (15210): (note): MAC: 286b.3598.580f Client state transition: S_CO_DEATH_PLUMB_IN_PROGRESS --> S_CO_L1_LEARN_IN_PROGRESS
2023/08/04 14:24:27.91859521 [wlc_m_0-0] (1): [client-orch-wm] (15210): (note): MAC: 286b.3598.580f Client state transition: S_CO_L1_LEARN_IN_PROGRESS --> S_CO_JOIN

```

NetGear A8000

WPA3-Enterprise is not supported on this client.

Pixel 6a

Connection OTA with focus on the RSN information from client:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
878	1.408897	0.263322	Cisco_08:00:18:18	Broadcast	802.11	428	69	-37	dmn
879	1.408907	0.123770	Cisco_08:00:18:18	Broadcast	802.11	204	69	-37	dmn
880	1.408916	0.000405	Cisco_08:00:18:18	Broadcast	802.11	428	69	-37	dmn
882	1.408978	0.000716	Cisco_08:00:18:18	Broadcast	802.11	374	69	-37	dmn
928	1.407576	0.114498	Cisco_08:00:18:18	Broadcast	802.11	428	69	-37	dmn
932	1.407589	0.000231	Google_72:8a:96	Cisco_08:00:18:18	802.11	308	69	-37	dmn
932	1.407589	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-37	dmn
923	1.407951	0.003842	Cisco_08:00:18:18	Google_72:8a:96	802.11	108	69	-37	dmn
924	1.407951	0.000000	192.168.1.122	192.168.1.122	802.11	76	69	-37	dmn
925	1.408282	0.000000	Google_72:8a:96	192.168.1.122	802.11	214	69	-37	dmn
926	1.408281	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-37	dmn
930	1.408251	0.023970	Cisco_08:00:18:18	Google_72:8a:96	802.11	313	69	-37	dmn
931	1.408251	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-37	dmn
932	1.408267	0.000620	Google_72:8a:96	Google_72:8a:96	802.11	309	69	-37	dmn
933	1.408268	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-37	dmn
939	1.407377	0.017007	Google_72:8a:96	Cisco_08:00:18:18	802.11	117	69	-37	dmn
940	1.407377	0.000000	192.168.1.122	192.168.1.122	802.11	76	69	-37	dmn
942	1.408424	0.001207	Cisco_08:00:18:18	Google_72:8a:96	802.11	110	69	-37	dmn
943	1.408424	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-37	dmn
945	1.408096	0.000672	Cisco_08:00:18:18	Broadcast	802.11	428	69	-37	dmn
946	1.408484	0.000180	Google_72:8a:96	Google_72:8a:96	802.11	124	69	-37	dmn
949	1.408424	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-37	dmn
950	1.408424	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-37	dmn
956	1.408429	0.015081	Cisco_08:00:18:18	Google_72:8a:96	802.11	1116	69	-37	dmn
957	1.408429	0.000000	192.168.1.122	192.168.1.122	802.11	76	69	-37	dmn
958	1.408429	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-37	dmn
959	1.408429	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-37	dmn
960	1.408174	0.000000	Google_72:8a:96	Google_72:8a:96	802.11	382	69	-37	dmn
961	1.408174	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-37	dmn
963	1.408273	0.000000	Google_72:8a:96	Google_72:8a:96	802.11	236	69	-37	dmn
964	1.408273	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-37	dmn
965	1.408290	0.004337	Cisco_08:00:18:18	Google_72:8a:96	802.11	161	69	-37	dmn
966	1.408290	0.000000	192.168.1.122	192.168.1.122	802.11	76	69	-37	dmn
968	1.408289	0.004229	Google_72:8a:96	Cisco_08:00:18:18	802.11	241	69	-40	dmn
969	1.408289	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-37	dmn
971	1.408178	0.003960	Cisco_08:00:18:18	Google_72:8a:96	802.11	144	69	-37	dmn
972	1.408178	0.000000	192.168.1.122	192.168.1.122	802.11	76	69	-37	dmn
973	1.408178	0.004190	Google_72:8a:96	Cisco_08:00:18:18	802.11	132	69	-37	dmn
974	1.408178	0.000078	192.168.1.15	192.168.1.122	802.11	76	69	-37	dmn
976	1.408196	0.003200	Google_72:8a:96	Google_72:8a:96	802.11	171	69	-37	dmn
977	1.408196	0.000000	192.168.1.122	192.168.1.122	802.11	76	69	-37	dmn
978	1.408522	0.004817	Google_72:8a:96	Cisco_08:00:18:18	802.11	206	69	-37	dmn
979	1.408522	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-37	dmn
984	1.408494	0.010072	Cisco_08:00:18:18	Google_72:8a:96	802.11	100	69	-37	dmn
985	1.408494	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-37	dmn
986	1.408687	0.002125	Google_72:8a:96	Cisco_08:00:18:18	802.11	145	69	-40	dmn
987	1.408687	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-37	dmn
988	1.407058	0.003771	Cisco_08:00:18:18	Broadcast	802.11	428	69	-37	dmn
989	1.407058	0.000000	Cisco_08:00:18:18	Google_72:8a:96	802.11	143	69	-37	dmn
990	1.407058	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-37	dmn
992	1.407128	0.006470	Google_72:8a:96	Cisco_08:00:18:18	802.11	120	69	-38	dmn
993	1.407128	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-37	dmn
996	1.500005	0.000291	Cisco_08:00:18:18	Google_72:8a:96	802.11	368	69	-37	dmn
997	1.500005	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-37	dmn
998	1.500005	0.000000	Cisco_08:00:18:18	Google_72:8a:96	802.11	223	69	-37	dmn
999	1.500005	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-37	dmn
1000	1.502525	0.000290	Google_72:8a:96	Cisco_08:00:18:18	802.11	368	69	-37	dmn
1001	1.502525	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-37	dmn
1004	1.502677	0.003422	Cisco_08:00:18:18	Google_72:8a:96	802.11	423	69	-37	dmn
1005	1.502677	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-37	dmn
1006	1.502886	0.000200	Google_72:8a:96	Cisco_08:00:18:18	802.11	199	69	-37	dmn
1007	1.502886	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-37	dmn

```

Frame 925: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits) on interface DeviceWPF_04578005-2998-4006-8C31-C3A13
> Ethernet II, Src: Cisco_08:00:18:18:18:18, Dst: Intelersa_01:1f:0e (08:1a:00:01:f1:0e)
> Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.122
> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
> AiroWep/Wep/Wep encapsulated IEEE 802.11
> IEEE 802.11 radio information
> IEEE 802.11 Association Request, Flags: .....C
> IEEE 802.11 W/Security Management
> Fixed parameters (4 bytes)
  Tagged parameters (167 bytes)
  > Tag: SSID parameter set: "wifi6_test"
  > Tag: Supported Rates (6R): 9, 12(0), 18, 24(0), 36, 48, 54, [Mbit/sec]
  > Tag: Power Capability Mtr: -, Max: 29
  > Tag: Supported Channels
  > Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag Length: 26
    RSN Version: 1
    > Group Cipher Suite: 00:0f:ac (See IEEE 802.11) AES (CCM)
    Pairwise Cipher Suite Count: 1
    > Pairwise Cipher Suite List: 00:0f:ac (See IEEE 802.11) AES (CCM)
    Auth Key Management (AKM) Suite Count: 1
    > Auth Key Management (AKM) List: 00:0f:ac (See IEEE 802.11) FT over IEEE 802.1X
    > Auth Key Management (AKM) Suite: 00:0f:ac (See IEEE 802.11) FT over IEEE 802.1X
    Auth Key Management (AKM) type: FT over IEEE 802.1X (1)
  > RSN Capabilities: 00:00
    .....0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
    .....0 = RSN No Pairwise capabilities: Transmitter can support MP default key @ simultaneously wdt
    .....0 = RSN PTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/TKkeySA (0x0)
    .....00 = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/TKkeySA (0x0)
    .....1 = Management Frame Protection Required: True
    .....1 = Management Frame Protection Capable: True
    .....0 = 32bit M211-band RSN: False
    .....0 = Perkey Enabled: False
    ..... = Extended key ID for Individually Addressed Frames: Not supported
  PMKID Count: 0
  PMKID List
  > Group Management Cipher Suite: 00:0f:ac (See IEEE 802.11) BIP (128)
  > Tag: W/Enabled Capabilities (5 octets)
  > Tag: Mobility domain
  > Tag: Supported Operating Classes
  > Tag: Extended Capabilities (20 octets)
  > Ext Tag: HE Capabilities
  > Ext Tag: HE 4-0 Band Capabilities
  > Tag: Vendor Specific: Broadcom
    Tag Number: Vendor Specific (221)
    Tag Length: 10
    OUI: 00:18:18 (Broadcom)
    Vendor Specific OUI Type: 2
    Vendor Specific Data: 000000000000
  > Tag: Vendor Specific: Microsoft Corp.: WPVAP: Information Element
  
```

WPA3 Enterprise 802.1x + FT Pixel6a Association

Client details in WLC:

WPA3 Enterprise 802.1x + FT Pixel6a Client details

Focus on the roam type Over the Air where we can see the roam type 802.11R:

Samsung S23

Connection OTA with focus on the RSN information from client:

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

Layer2 Layer3 AAA

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP None

MAC Filtering

Lobby Admin Access

WPA Parameters

WPA Policy	<input type="checkbox"/>	WPA2 Policy	<input type="checkbox"/>
GTK Randomize	<input type="checkbox"/>	WPA3 Policy	<input checked="" type="checkbox"/>
Transition Disable	<input type="checkbox"/>		

Fast Transition

Status

Over the DS

Reassociation Timeout *

WPA2/WPA3 Encryption

AES(CCMP128)	<input type="checkbox"/>	CCMP256	<input type="checkbox"/>
GCMP128	<input checked="" type="checkbox"/>	GCMP256	<input type="checkbox"/>

Auth Key Mgmt

SUITEB-1X

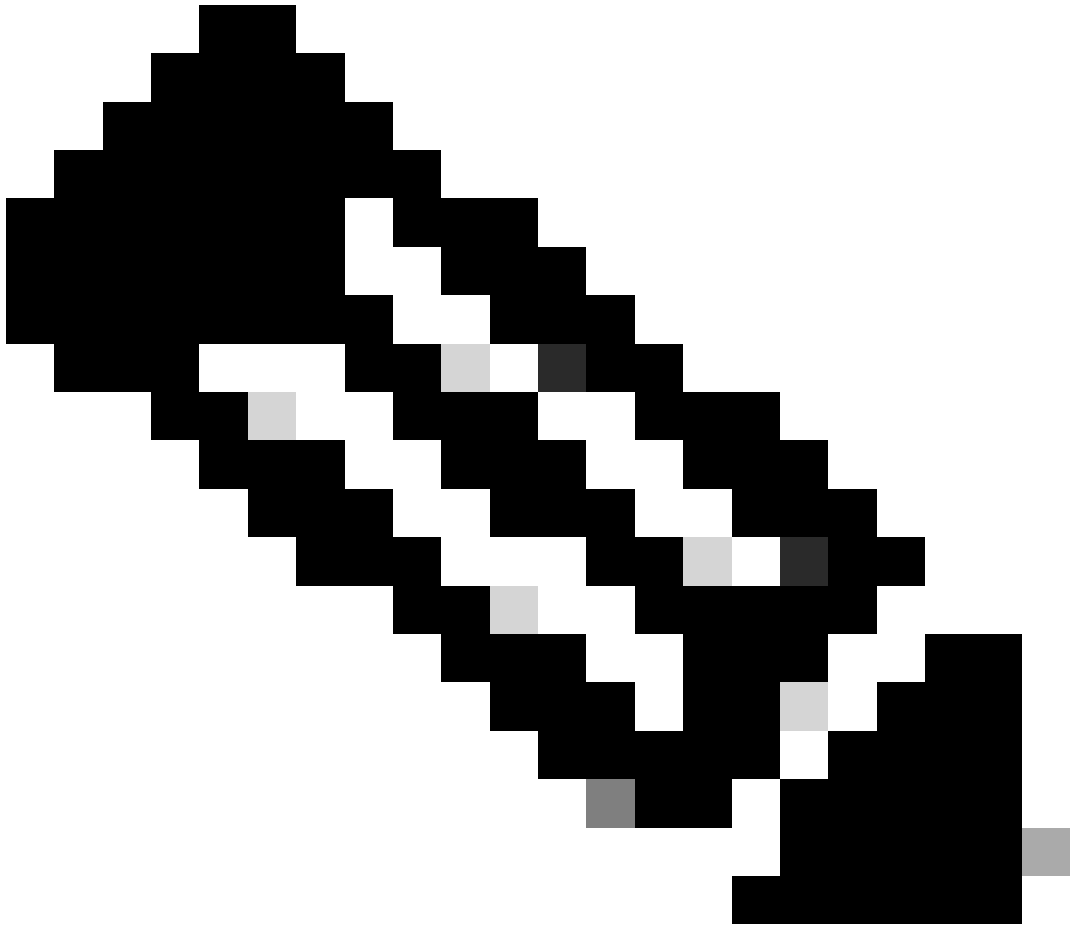
Protected Management Frame

PMF

Association Comeback Timer*

SA Query Time*

WPA3 Enterprise SuiteB-1X Security Configuration



Note: FT is not supported in SUITEB-1X

View on WLC GUI of the WLAN Security settings:



Verification of beacons OTA:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	str	Info
37376	59.189776	0.820482	Cisco_05:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2802, Fw=0, Flags=.....C, B=100, SSID=...		> frame 37326: 355 bytes on wire (2840 bits), 355 bytes captured (2840 bits) on interface \Device\NPF_{04576965-2998-4456-8C13-C4}
37385	59.190516	0.820508	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2803, Fw=0, Flags=.....C, B=100, SSID=...		> Ethernet II, Src: Cisco_02:00:07 (74:11:32:02:07:47), Dst: Unknown_07:c7:06 (08:00:00:07:c7:06)
37396	59.191709	0.820481	Cisco_05:00:18	Broadcast	802.11	355	69 -17 dbm	Beacon frame, SW=2804, Fw=0, Flags=.....C, B=100, SSID=...		> Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.121
37414	59.192161	0.820462	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2805, Fw=0, Flags=.....C, B=100, SSID=...		> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
37424	59.192713	0.820472	Cisco_05:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2806, Fw=0, Flags=.....C, B=100, SSID=...		> AlohaPdu/OnStream encapsulated IEEE 802.11
37437	59.192758	0.820457	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2807, Fw=0, Flags=.....C, B=100, SSID=...		> IEEE 802.11 Beacon frame, Flags:C
37447	59.192792	0.820442	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2808, Fw=0, Flags=.....C, B=100, SSID=...		> IEEE 802.11 Wireless Management
37459	59.193154	0.820522	Cisco_05:00:18	Broadcast	802.11	355	69 -38 dbm	Beacon frame, SW=2809, Fw=0, Flags=.....C, B=100, SSID=...		> Fixed parameters (12 bytes)
37470	59.193629	0.820399	Cisco_05:00:18	Broadcast	802.11	312	69 -39 dbm	Probe Response, SW=2809, Fw=0, Flags=.....C, B=100, SSID=...		> Tagged parameters (213 bytes)
37480	59.194345	0.820465	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2811, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: SSID parameter set: "WiFiTest"
37489	59.195487	0.821342	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2812, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: Supported Rates (6B), 9, 12(6), 18, 24(6), 36, 48, 54, [Mbit/sec]
37499	59.195516	0.821929	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2813, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: Traffic Indication Map (TIM): OPM # of 1 bitmap
37520	59.195888	0.820347	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2815, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: Country Information: Country Code not, Environment Global operating classes
37532	59.195726	0.821156	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2816, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: Power Constraint: 6
37539	59.197089	0.821751	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2817, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: TX Report Transmit Power: 36, L100 Operate: 0
37552	59.197468	0.820499	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2818, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: RSN Information
37565	59.197993	0.820545	Cisco_05:00:18	Broadcast	802.11	355	69 -17 dbm	Beacon frame, SW=2819, Fw=0, Flags=.....C, B=100, SSID=...		> Tag Number: RSN Information (64)
37574	59.198423	0.820438	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2820, Fw=0, Flags=.....C, B=100, SSID=...		> Tag Length: 26
37585	59.198865	0.820542	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2821, Fw=0, Flags=.....C, B=100, SSID=...		> RSN Version: 1
37596	59.199429	0.820476	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2822, Fw=0, Flags=.....C, B=100, SSID=...		> Group Cipher Suite: 00000000 (IEEE 802.11) GCM (128)
37606	59.199949	0.820595	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2823, Fw=0, Flags=.....C, B=100, SSID=...		> Pairwise Cipher Suite Count: 1
37626	59.202621	0.820481	Cisco_05:00:18	Broadcast	802.11	355	69 -38 dbm	Beacon frame, SW=2824, Fw=0, Flags=.....C, B=100, SSID=...		> Pairwise Cipher Suite List 00000000 (IEEE 802.11) GCM (128)
37641	59.204984	0.820561	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2825, Fw=0, Flags=.....C, B=100, SSID=...		> Auth Key Management (AKM) Suite Count: 1
37652	59.206137	0.820351	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2826, Fw=0, Flags=.....C, B=100, SSID=...		> Auth Key Management (AKM) List 00000000 (IEEE 802.11) WPA (TKIP+SuiteB)
37668	59.207467	0.820592	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2827, Fw=0, Flags=.....C, B=100, SSID=...		> Auth Key Management (AKM) Suite List 00000000 (IEEE 802.11) WPA (TKIP+SuiteB)
37686	59.212867	0.820460	Cisco_05:00:18	Broadcast	802.11	355	69 -38 dbm	Beacon frame, SW=2829, Fw=0, Flags=.....C, B=100, SSID=...		> Auth Key Management (AKM) Type: WPA (TKIP+SuiteB) (11)
37704	59.213477	0.820450	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2830, Fw=0, Flags=.....C, B=100, SSID=...		> RSN Capabilities: 0x0000
37719	59.215721	0.820424	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2831, Fw=0, Flags=.....C, B=100, SSID=...		> PMKID Count: 0
37739	59.218459	0.820628	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2832, Fw=0, Flags=.....C, B=100, SSID=...		> PMKID List
37758	59.220659	0.820180	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2833, Fw=0, Flags=.....C, B=100, SSID=...		> Group Management Cipher Suite: 00000000 (IEEE 802.11) GCM (128)
37749	59.223208	0.820495	Cisco_05:00:18	Broadcast	802.11	355	69 -38 dbm	Beacon frame, SW=2834, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: QoS User Element: IEEE 802.11 version
37775	59.226521	0.820392	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2835, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: W/ Enabled Capabilities (5 octets)
37792	59.226621	0.820508	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2836, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: Extended Capabilities (11 octets)
37809	59.227802	0.821581	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2837, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: Tx Power Envelope
37814	59.228540	0.820490	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2841, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: Tx Power Envelope
37857	59.230900	0.820550	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2842, Fw=0, Flags=.....C, B=100, SSID=...		> Ext Tag: Multiple BSSID Configuration
37864	08.013602	0.820460	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2843, Fw=0, Flags=.....C, B=100, SSID=...		> Ext Tag: HE Capabilities
37868	08.013932	0.820508	Cisco_05:00:18	Broadcast	802.11	355	69 -38 dbm	Beacon frame, SW=2844, Fw=0, Flags=.....C, B=100, SSID=...		> Ext Tag: HE Operation
37881	08.014049	0.820297	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2845, Fw=0, Flags=.....C, B=100, SSID=...		> Ext Tag: Spatial Reuse Parameter Set
37887	08.014787	0.820568	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2846, Fw=0, Flags=.....C, B=100, SSID=...		> Ext Tag: HE 4 GHz Band Capabilities
37897	08.015006	0.820839	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2847, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: Vendor Specific: Atheros Communications, Inc.: Unknown
37908	08.015976	0.820888	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2848, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: Vendor Specific: Microsoft Corp.: WPAHE: Parameter Element
37917	08.112414	0.820438	Cisco_05:00:18	Broadcast	802.11	355	69 -17 dbm	Beacon frame, SW=2849, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: Vendor Specific: Cisco Systems, Inc.: Airont Client MFP Disabled
37928	08.113087	0.820613	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2850, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: Vendor Specific: Cisco Systems, Inc.: Airont CCK version = 5
37936	08.173114	0.820267	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2851, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: Vendor Specific: Cisco Systems, Inc.: Airont Unknown (64)
37943	08.193778	0.820464	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2852, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: Vendor Specific: Cisco Systems, Inc.: Airont Unknown (11) (11)
37949	08.114389	0.820593	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2853, Fw=0, Flags=.....C, B=100, SSID=...		
37961	08.114873	0.820594	Cisco_05:00:18	Broadcast	802.11	355	69 -17 dbm	Beacon frame, SW=2854, Fw=0, Flags=.....C, B=100, SSID=...		

WPA3 Enterprise SuiteB-1X Beacon

None of the tested clients were able to connect to the WLAN using SuiteB-1X confirming that none supports this security method.

WPA3-Enterprise + GCMP256 cipher + SUITEB192-1X

WLAN Security configuration:

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

Layer2 Layer3 AAA

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP None

MAC Filtering

Lobby Admin Access

WPA Parameters

WPA Policy WPA2 Policy
GTK Randomize WPA3 Policy
Transition Disable

Fast Transition

Status
Over the DS
Reassociation Timeout *

WPA2/WPA3 Encryption

AES(CCMP128) CCMP256
GCMP128 GCMP256

Auth Key Mgmt

SUITEB192-1X

Protected Management Frame

PMF
Association Comeback Timer*
SA Query Time*

WPA3 Enterprise SUITEB192-1x security settings



Note: FT is not supported with GCMP256+SUITEB192-1X.

WLAN on WLC GUI WLANs list:



WLAN used for tests

Verification of beacons OTA:

This was a client side issue that is being worked on and as soon its resolved, this document shall be updated.

Security Conclusions

After all the previous tests, this is the resultant conclusions:

Protocol	Encryption	AKM	AKM Cipher	EAP Method	FT-OverTA	FT-OverDS	Intel AX211	Samsung/Google Android	Net A80
OWE	AES-CCMP128	OWE	NA.	NA.	NA	NA	Supported	Supported	Sup
SAE	AES-CCMP128	SAE (H2E Only)	SHA256	NA.	Supported	Supported	Supported: H2E Only and FT-oTA	Supported: H2E Only. FT Failed. FT-oDS Failed.	Sup H2E and oTA FT- Fail
Enterprise	AES-CCMP128	802.1x-SHA256	SHA256	PEAP/FAST/TLS	Supported	Supported	Supported: SHA256 and FT-oTA/oDS Not-Supported: EAP-FAST	Supported: SHA256 and FT-oTA, FT-oDS (S23) Not-Supported: EAP-FAST, FT-oDS (Pixel6a)	Sup SHA and oTA Not Sup EAP FAST FT-
Enterprise	GCMP128	SuiteB-1x	SHA256-SuiteB	PEAP/FAST/TLS	Not Supported	Not Supported	Not Supported	Not Supported	Not Sup
Enterprise	GCMP256	SuiteB-192	SHA384-SuiteB	TLS	Not Supported	Not Supported	NA/TBD	NA/TBD	Not Sup

Troubleshoot

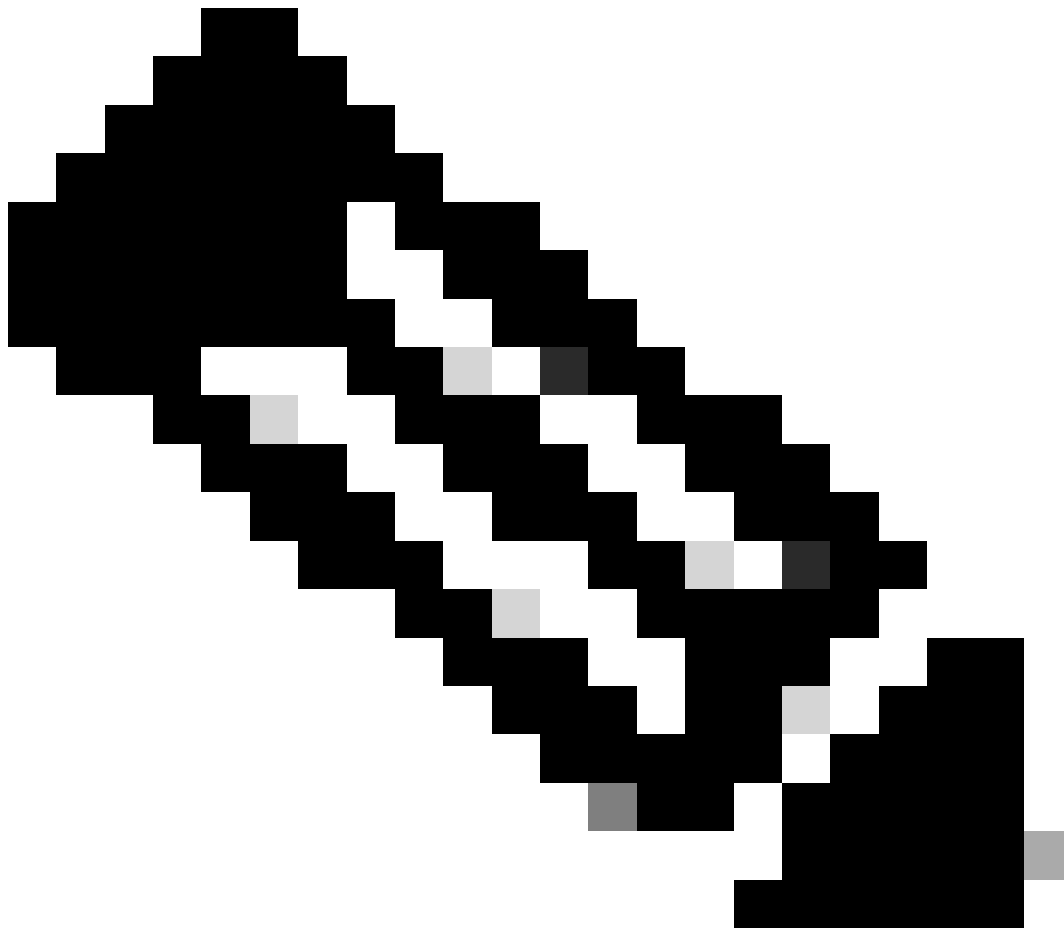
The troubleshooting used in this document was based on the online document:

[Troubleshoot COS APs](#)

The general guideline for troubleshooting is to collect RA trace in debug mode from the WLC using the client mac address making sure that the client is connecting using the device mac and not a randomized mac address.

For Over the Air troubleshooting, the recommendation is to use AP in sniffer mode capturing the traffic on

the channel of the client serving AP.



Note: Refer to [Important Information on Debug Commands](#) before you use **debug** commands.

Related Information

[What is Wi-Fi 6E?](#)

[What Is Wi-Fi 6 vs. Wi-Fi 6E?](#)

[Wi-Fi 6E At-a-Glance](#)

[Wi-Fi 6E: The Next Great Chapter in Wi-Fi White Paper](#)

[Cisco Live - Architecting Next Generation Wireless Network with Catalyst Wi-Fi 6E Access Points](#)

[Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide 17.9.x](#)

[WPA3 Deployment Guide](#)