

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

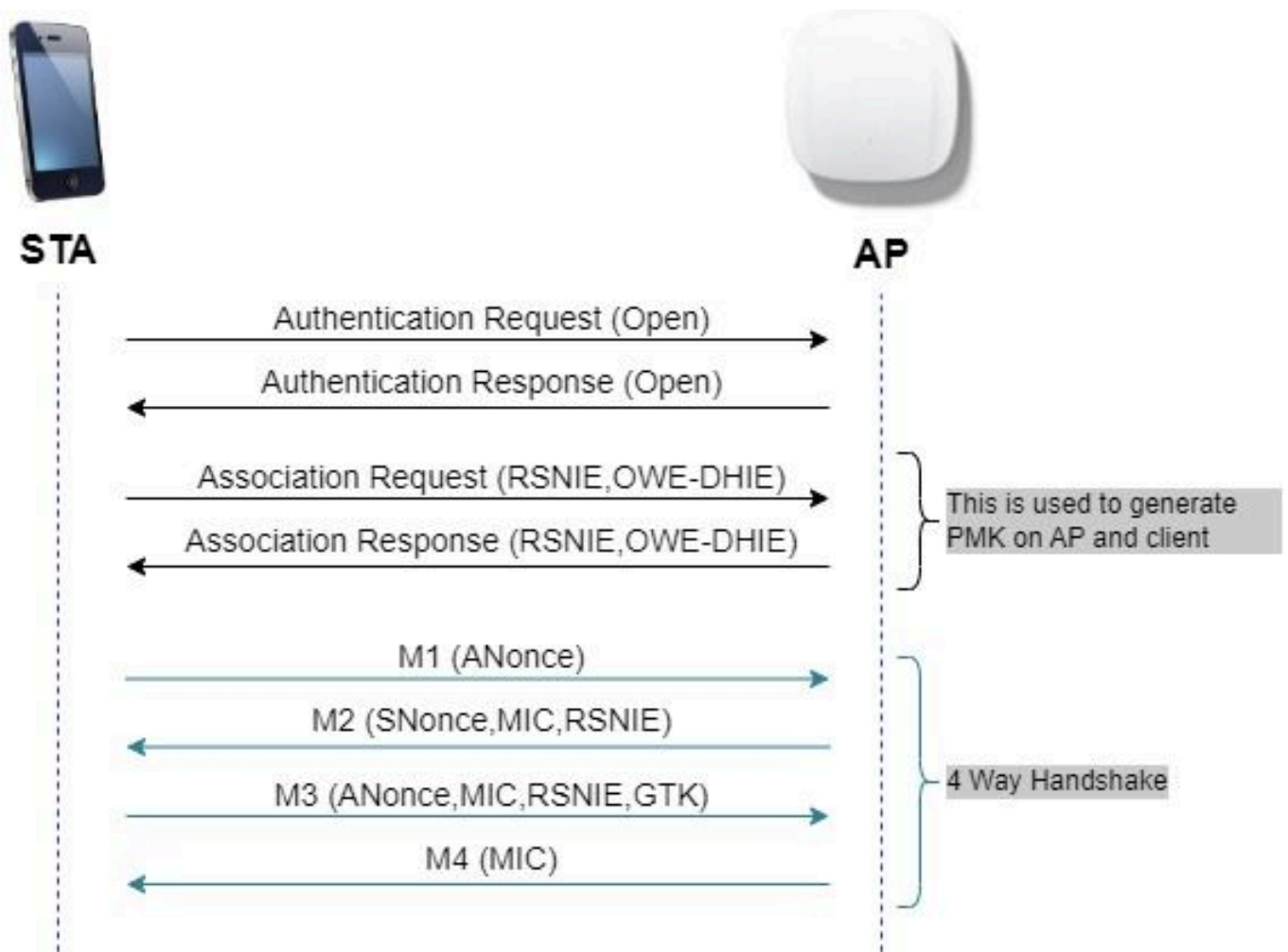
SAE	<input type="checkbox"/>	FT + SAE	<input checked="" type="checkbox"/>
OWE	<input type="checkbox"/>	FT + 802.1x	<input type="checkbox"/>
802.1x- SHA256	<input type="checkbox"/>		
Anti Clogging Threshold*		<input type="text" value="1500"/>	
Max Retries*		<input type="text" value="5"/>	
Retransmit Timeout*		<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](https://www.rfc-editor.org/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).

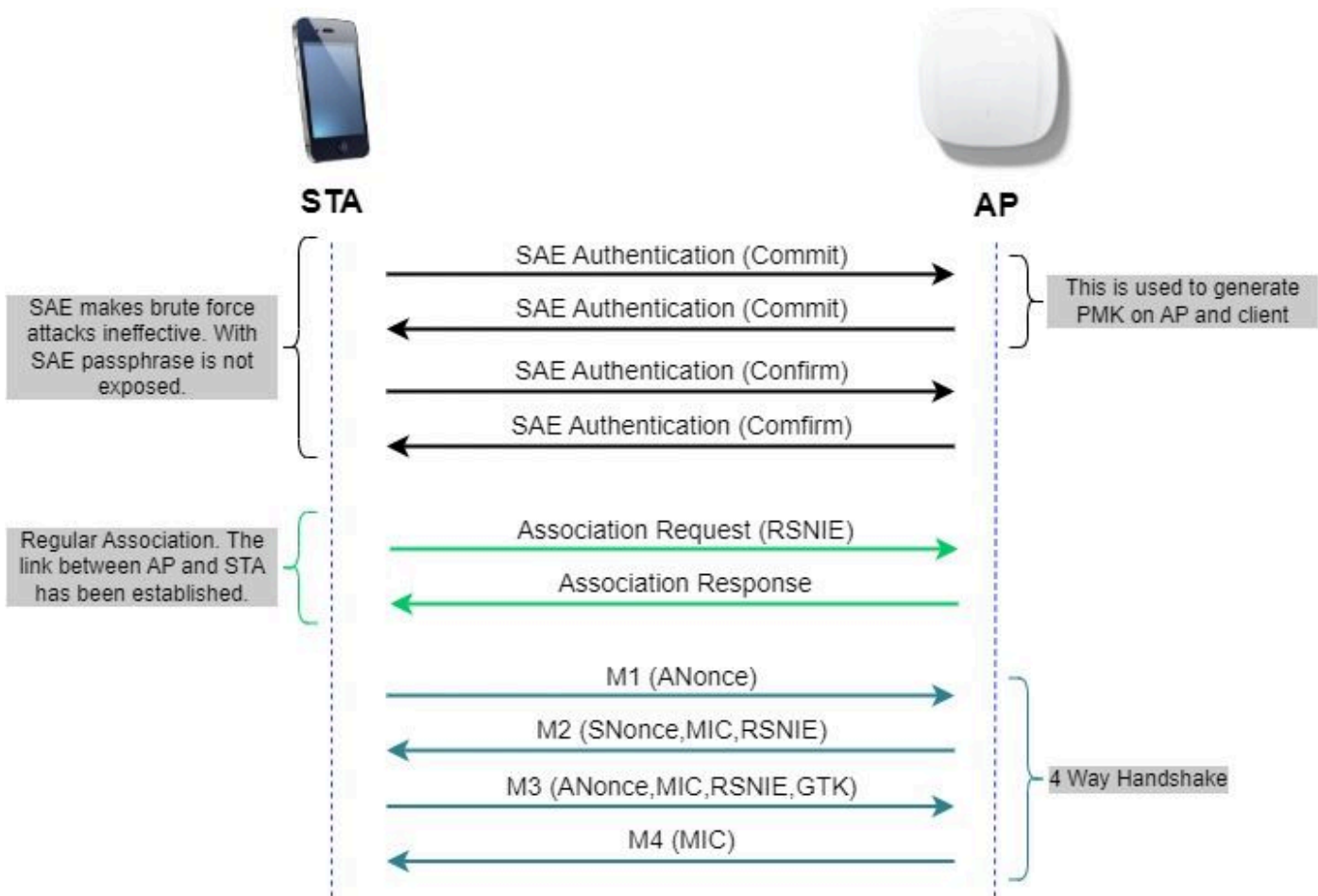
SAE with H2E is mandatory for WPA3 and Wi-Fi 6E.

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:

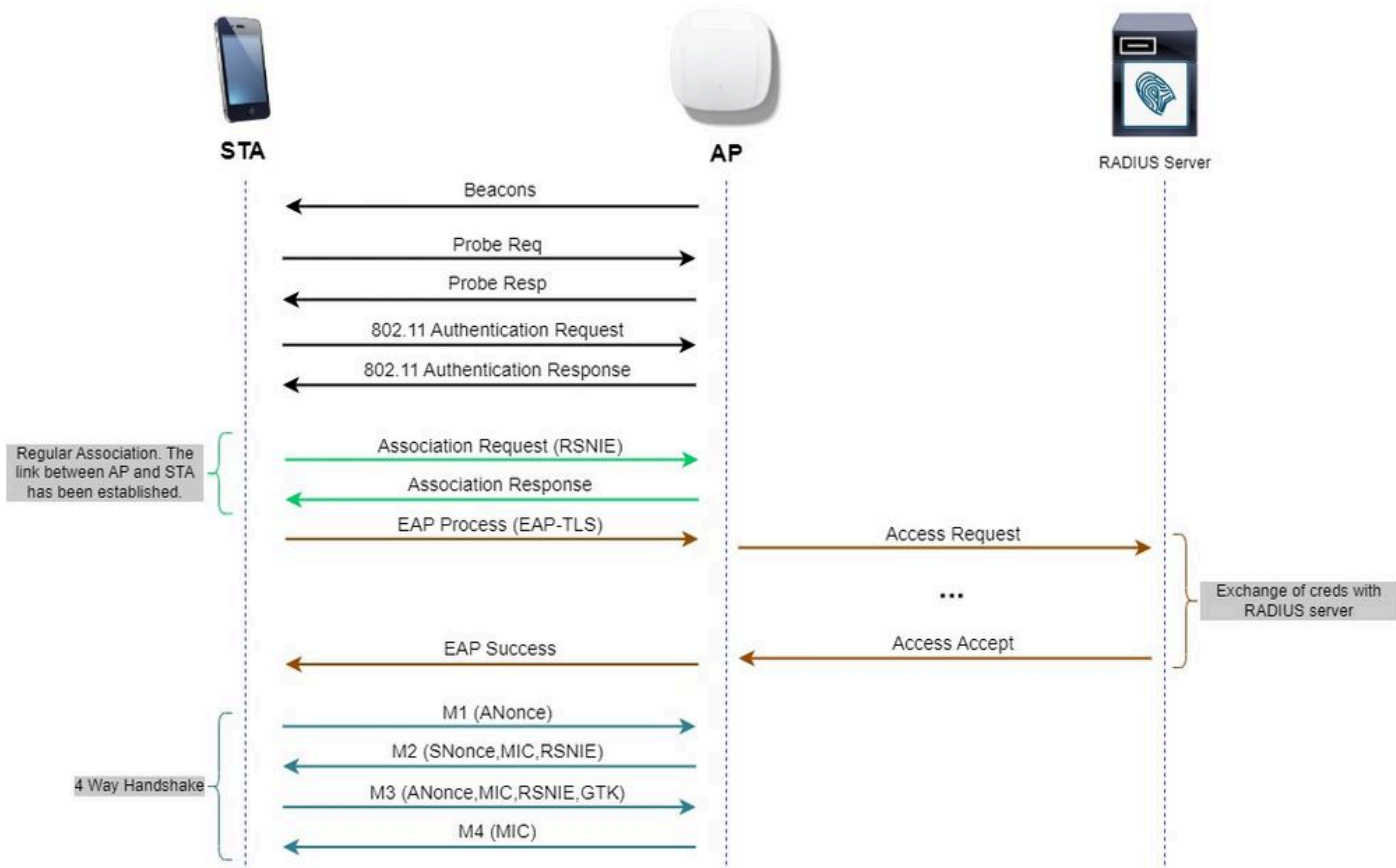
- Derivation of a secret intermediary element (PT) from the password. This can be performed offline when the password is initially configured on the device for each supported group.
- Derivation of the PWE from the stored PT. This depends on the negotiated group and MAC addresses of peers. This is performed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



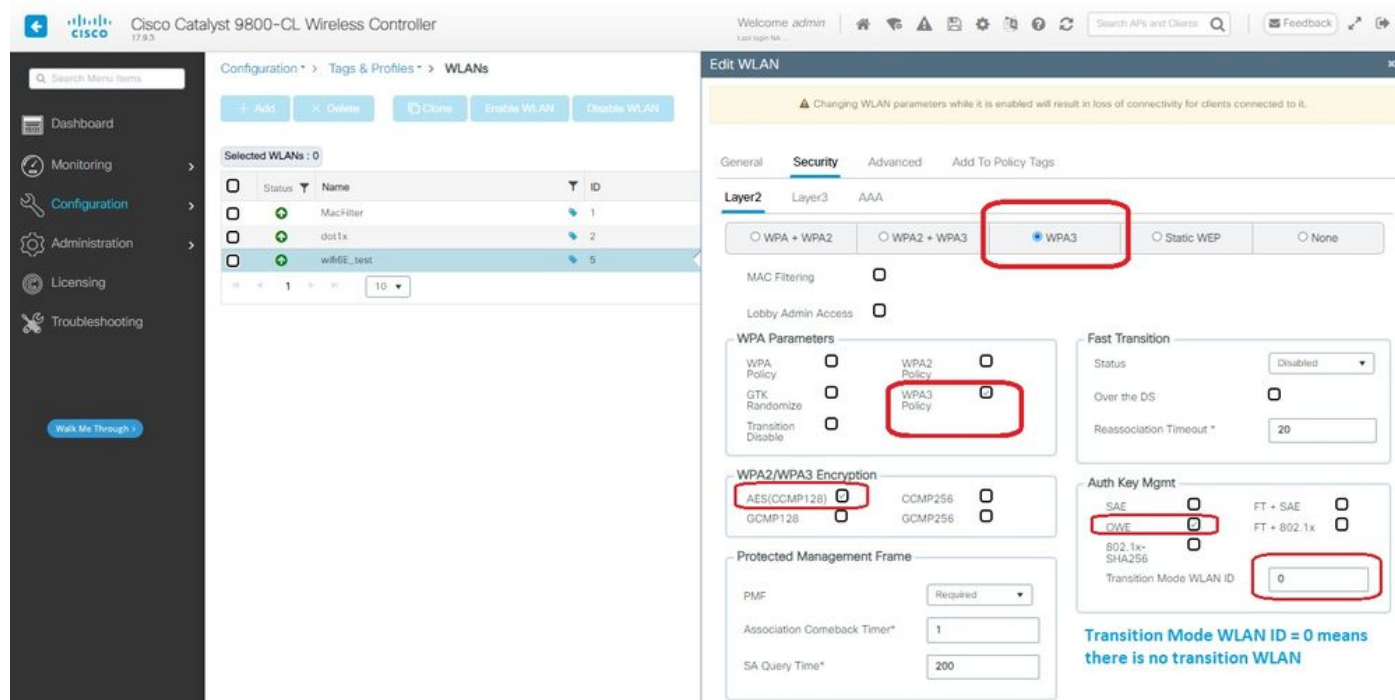
GET IT ON



: 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.

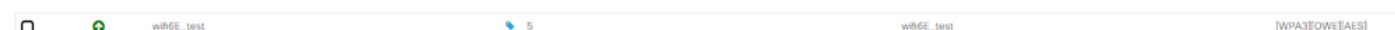
WPA3 - AES(CCMP128) + OWE

This is the WLAN Security configuration:



OWE Security Settings

View on WLC GUI of the WLAN Security settings:



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.

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:

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...
 IEEE 802.11 Association Request, Flags:C
 Fixed parameters (4 bytes)
 Tagged parameters (190 bytes)
 Tag: SSID parameter set: "wifid_test"
 Tag: Supported Rates (8): 9, 12(0), 18, 24(0), 36, 48, 54, [Mbit/sec]
 Tag: Power Capability (8): 0, 0, 0, 0, 0, 0, 0, 0
 Tag: RSN Information (48)
 Tag Length: 24
 RSN Version: 1
 Group Cipher Suite: 00:0fac (IEEE 802.11) AES (CCM)
 Pairwise Cipher Suite List: 00:0fac (IEEE 802.11) AES (CCM)
 Auth Key Management (AKM) Suite Count: 1
 Auth Key Management (AKM) Suite: 00:0fac (IEEE 802.11) Opportunistic Wireless Encryption
 Auth Key Management (AKM) Suite: 00:0fac (IEEE 802.11) Opportunistic Wireless Encryption
 RSN Capabilities: 00000000
 RSN PPE-Auth capabilities: Transmitter does not support pre-authentication
 RSN No Pairwise capabilities: Transmitter can support WEP default key a simultaneously with Pairwise
 RSN No Pairwise capabilities: Transmitter can support WEP default key a simultaneously with Pairwise
 RSN DTSA Replay Counter capabilities: 16 replay counters per PTKSA/TKSA/TKA/SA (8x3)
 RSN DTSA Replay Counter capabilities: 16 replay counters per PTKSA/TKSA/TKA/SA (8x3)
 Management Frame Protection Required: True
 Management Frame Protection Capable: True
 Joint Multi-Band SNA: False
 Peerkey Enabled: False
 Extended Key ID for Individually Addressed Frames: Not supported
 PTKID Count: 0
 PTKID List:
 Group Management Cipher Suite: 00:0fac (IEEE 802.11) ESP (128)
 Supported Operating Classes
 Tag: Vendor Specific: microsoft corp. 1 000000: Information Element
 Tag: Vendor Specific: Intel Wireless Network Group
 Ext Tag: OWE Diffie-Hellman Parameter
 Tag Number: Element ID Extension (255)
 Ext Tag Length: 34
 Ext Tag Number: OWE Diffie-Hellman Parameter (32)
 Group: 254-bit random ECP group (19)
 Public Key: 849cf39923254c0bc137940877f2e0950acdf266af50b7f43018496
 Tag: HE Capabilities
 Ext Tag: HE 4 GHz Band Capabilities

Frame 15: 278 bytes on wire (2224 bits), 278 bytes captured (2224 bits) on interface 10vnic1/vpp...
 IEEE 802.11 Association Response, Flags:C
 Fixed parameters (4 bytes)
 Tagged parameters (179 bytes)
 Tag: RSN Information (48)
 Tag Length: 24
 RSN Version: 1
 Group Cipher Suite: 00:0fac (IEEE 802.11) AES (CCM)
 Pairwise Cipher Suite List: 00:0fac (IEEE 802.11) AES (CCM)
 Auth Key Management (AKM) Suite Count: 1
 Auth Key Management (AKM) Suite: 00:0fac (IEEE 802.11) Opportunistic Wireless Encryption
 Auth Key Management (AKM) Suite: 00:0fac (IEEE 802.11) Opportunistic Wireless Encryption
 RSN Capabilities: 00000000
 RSN PPE-Auth capabilities: Transmitter does not support pre-authentication
 RSN No Pairwise capabilities: Transmitter can support WEP default key a simultaneously with Pairwise
 RSN No Pairwise capabilities: Transmitter can support WEP default key a simultaneously with Pairwise
 RSN DTSA Replay Counter capabilities: 4 replay counters per PTKSA/TKSA/TKA/SA (8x2)
 RSN DTSA Replay Counter capabilities: 4 replay counters per PTKSA/TKSA/TKA/SA (8x2)
 Management Frame Protection Required: True
 Management Frame Protection Capable: True
 Joint Multi-Band SNA: False
 Peerkey Enabled: False
 Extended Key ID for Individually Addressed Frames: Not supported
 PTKID Count: 0
 PTKID List:
 Group Management Cipher Suite: 00:0fac (IEEE 802.11) ESP (128)
 Vendor Specific: microsoft corp. 1 000000: Parameter Element
 Tag: Vendor Specific: Intel Wireless Network Group
 Ext Tag: OWE Diffie-Hellman Parameter
 Tag Number: Element ID Extension (255)
 Ext Tag Length: 34
 Ext Tag Number: OWE Diffie-Hellman Parameter (32)
 Group: 254-bit random ECP group (19)
 Public Key: 6dcfe3a31a191943a3e3b34f3739ffcc3e3b2c9d70b23d0e945a58
 Tag: HE Capabilities

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
Capicm Timeout	ccsmn

NetGear A8000

Connection OTA with focus on the RSN information from client:

Packet capture analysis screenshot showing network traffic details. The main table lists packets with columns: No., Time, Delta, Source, Destination, Protocol, Length, Channel, Signal, and Info. The info column contains detailed protocol data such as IEEE 802.11 Association Request, Authentication, and Action frames. A detailed view of a specific IEEE 802.11 frame is shown on the right, including fields like SSID, Pairwise Cipher Suite List, and Authentication Key Management.

Client details in WLC:

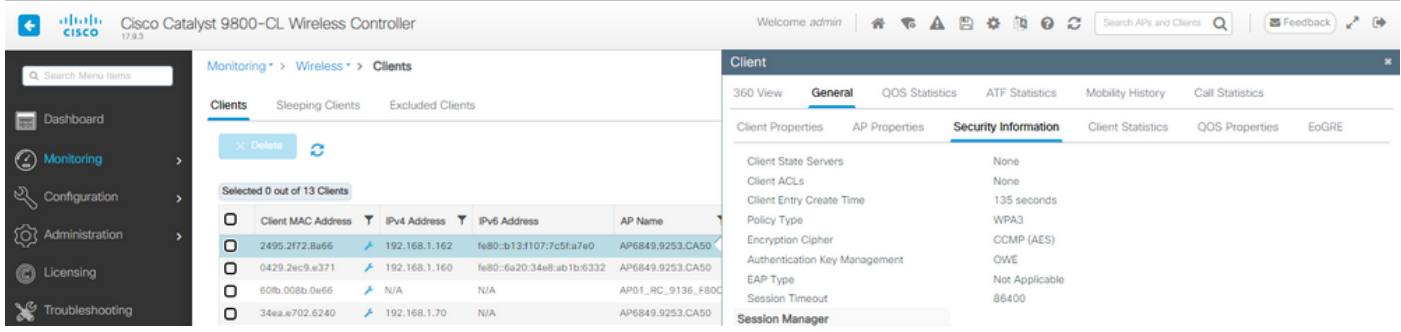
The screenshot displays the Cisco Catalyst 9800-CL Wireless Controller interface. On the left is a navigation menu with options like Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main area shows 'Monitoring > Wireless > Clients'. A table lists 11 clients, with the selected client being 9418.6548.7095. To the right, a 'Client' tab provides details for this client, including Client Properties (Client State Servers, Client ACLs), AP Properties (Policy Type, Authentication Key Management), Security Information (Encryption Cipher: CCMP (AES)), Client Statistics, and QoS Properties.

Pixel 6a

Connection OTA with focus on the RSN information from client:

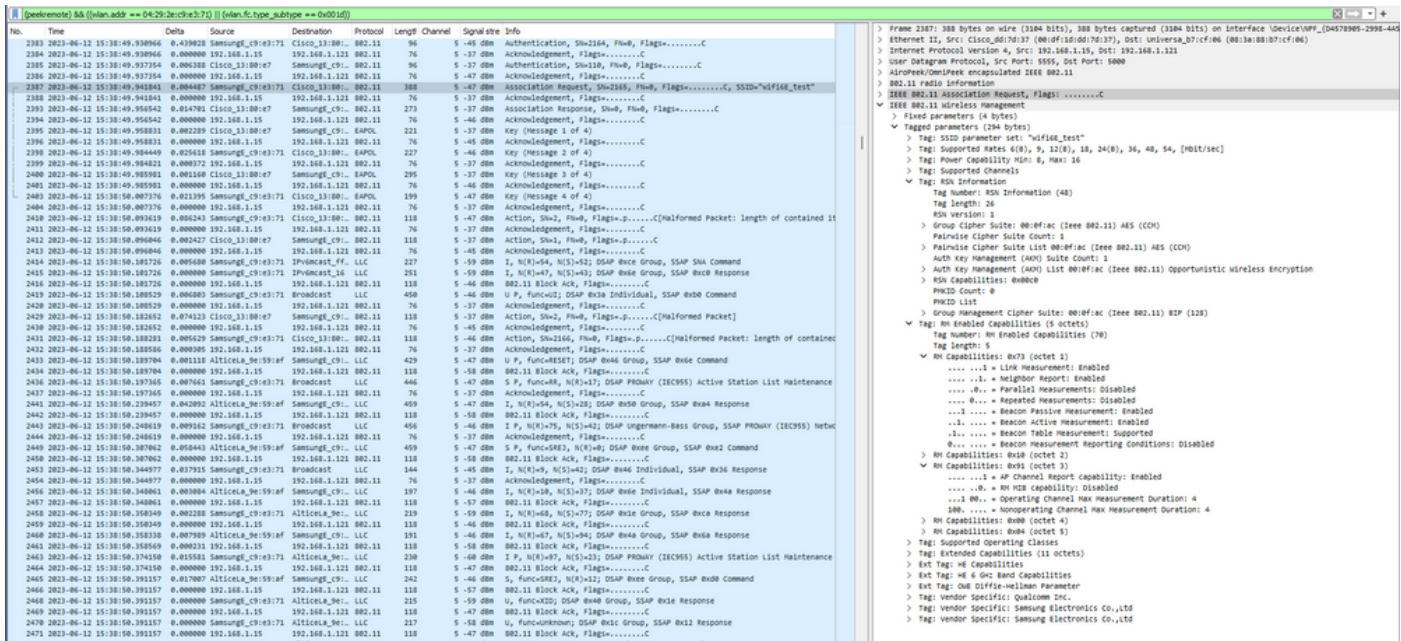
Another packet capture analysis screenshot, similar to the first one, but focusing on RSN information. It shows a list of packets and a detailed view of a frame containing RSN capabilities and other IEEE 802.11 protocol details. The RSN capabilities section lists supported cipher suites and key management methods.

Client details in WLC:

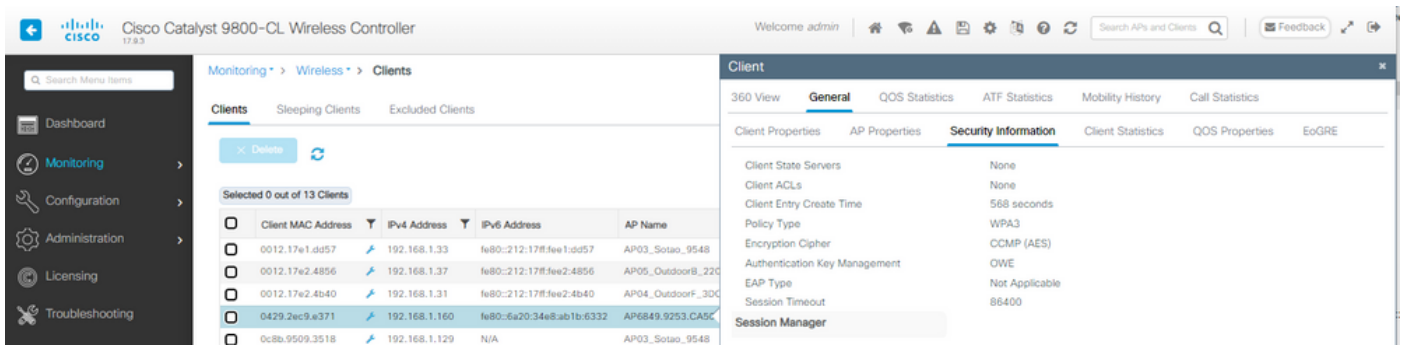


Samsung S23

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

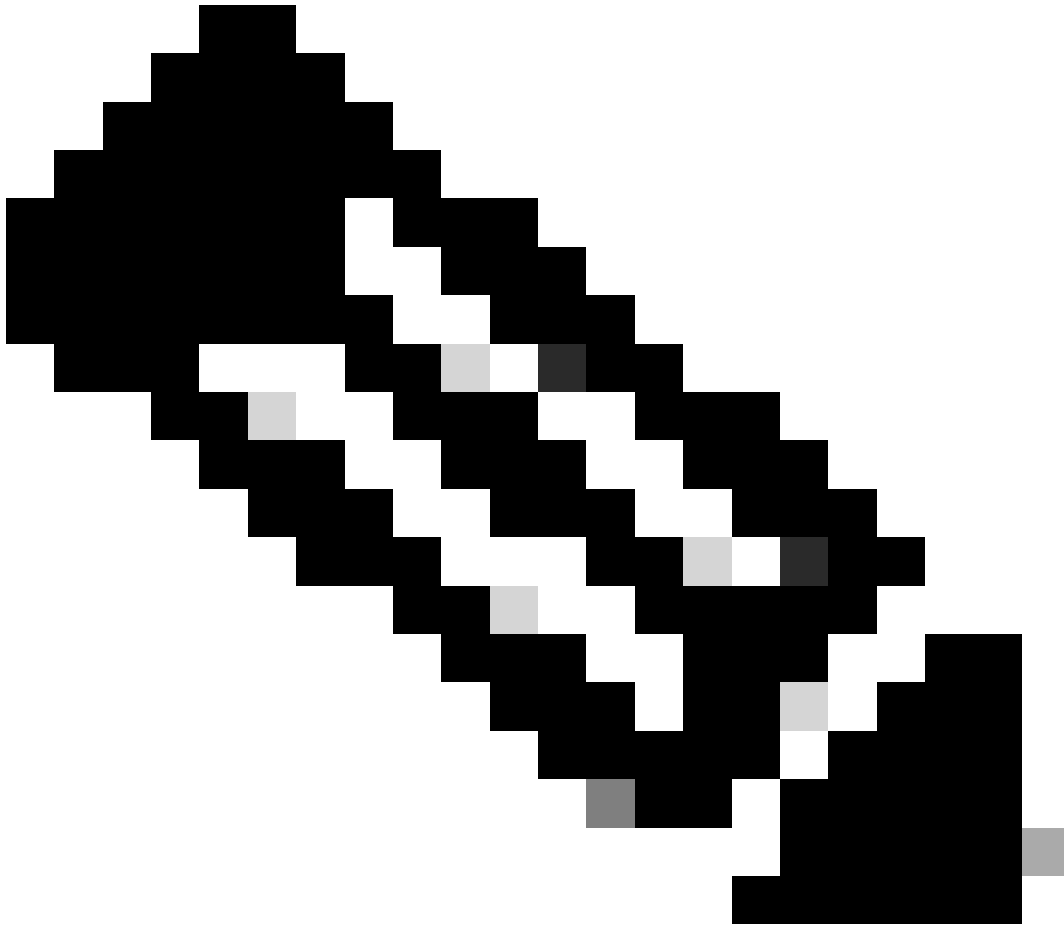
Auth Key Mgmt

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

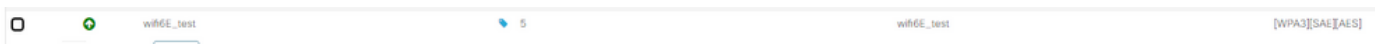
PMF
Association Comeback Timer*
SA Query Time*

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:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
2	2023-06-12 17:12:24.456138	0.00000	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
3	2023-06-12 17:12:24.479646	0.02356	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
5	2023-06-12 17:12:24.491121	0.02045	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
6	2023-06-12 17:12:24.731672	0.25091	Cisco_13:180e7	Broadcast	802.11	508	53	-37	DBM
7	2023-06-12 17:12:24.772306	0.04054	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
18	2023-06-12 17:12:24.792541	0.02045	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
11	2023-06-12 17:12:24.773881	0.02045	Cisco_13:180e7	Broadcast	802.11	463	53	-37	DBM
10	2023-06-12 17:12:24.773881	0.02045	Cisco_13:180e7	Broadcast	802.11	463	53	-37	DBM
15	2023-06-12 17:12:24.834577	0.05875	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
16	2023-06-12 17:12:24.858909	0.02045	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
17	2023-06-12 17:12:24.878478	0.02045	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
18	2023-06-12 17:12:24.895829	0.02039	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
19	2023-06-12 17:12:24.910558	0.02073	Cisco_13:180e7	Broadcast	802.11	508	53	-36	DBM
20	2023-06-12 17:12:24.937923	0.02185	Cisco_13:180e7	Broadcast	802.11	463	53	-37	DBM
21	2023-06-12 17:12:24.960625	0.03170	Cisco_13:180e7	Broadcast	802.11	463	53	-37	DBM
22	2023-06-12 17:12:24.998372	0.02874	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
23	2023-06-12 17:12:25.018111	0.02049	Cisco_13:180e7	Broadcast	802.11	508	53	-37	DBM
24	2023-06-12 17:12:25.039348	0.02037	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
25	2023-06-12 17:12:25.059812	0.02044	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
26	2023-06-12 17:12:25.080060	0.02058	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
27	2023-06-12 17:12:25.100864	0.02044	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
28	2023-06-12 17:12:25.121559	0.02075	Cisco_13:180e7	Broadcast	802.11	508	53	-36	DBM
29	2023-06-12 17:12:25.141878	0.02019	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
30	2023-06-12 17:12:25.162724	0.02186	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
35	2023-06-12 17:12:25.182664	0.01998	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
37	2023-06-12 17:12:25.203981	0.02047	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
38	2023-06-12 17:12:25.223702	0.02021	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
39	2023-06-12 17:12:25.244347	0.02045	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
40	2023-06-12 17:12:25.264534	0.02037	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
41	2023-06-12 17:12:25.284928	0.02046	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
42	2023-06-12 17:12:25.305513	0.02049	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
43	2023-06-12 17:12:25.326072	0.02059	Cisco_13:180e7	Broadcast	802.11	508	53	-36	DBM
44	2023-06-12 17:12:25.346892	0.02049	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
46	2023-06-12 17:12:25.367931	0.02031	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
47	2023-06-12 17:12:25.387562	0.02049	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
48	2023-06-12 17:12:25.407928	0.02049	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
49	2023-06-12 17:12:25.428554	0.02004	Cisco_13:180e7	Broadcast	802.11	508	53	-37	DBM
50	2023-06-12 17:12:25.449209	0.02045	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
51	2023-06-12 17:12:25.469798	0.02045	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
52	2023-06-12 17:12:25.490390	0.02045	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
53	2023-06-12 17:12:25.510833	0.02044	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
54	2023-06-12 17:12:25.531279	0.02045	Cisco_13:180e7	Broadcast	802.11	508	53	-36	DBM
55	2023-06-12 17:12:25.551206	0.02033	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
56	2023-06-12 17:12:25.571762	0.02092	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
57	2023-06-12 17:12:25.592320	0.02033	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
58	2023-06-12 17:12:25.612779	0.02000	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
59	2023-06-12 17:12:25.633372	0.02097	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
60	2023-06-12 17:12:25.653836	0.02044	Cisco_13:180e7	Broadcast	802.11	463	53	-37	DBM
61	2023-06-12 17:12:25.674388	0.02042	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
62	2023-06-12 17:12:25.694858	0.02030	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
63	2023-06-12 17:12:25.715367	0.02049	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM
64	2023-06-12 17:12:25.735819	0.02162	Cisco_13:180e7	Broadcast	802.11	463	53	-37	DBM
67	2023-06-12 17:12:25.756292	0.01973	Cisco_13:180e7	Broadcast	802.11	463	53	-36	DBM

WPA3 SAE 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
2235	2023-06-12 17:13:00.326338	0.00000	IntelCltor_9e:58f0e7	Broadcast	802.11	168	53	-48	DBM
2237	2023-06-12 17:13:00.328333	0.00204	IntelCltor_9e:58f0e7	Broadcast	802.11	168	53	-50	DBM
2242	2023-06-12 17:13:01.974933	0.644256	IntelCltor_9e:58f0e7	Broadcast	802.11	168	53	-45	DBM
2244	2023-06-12 17:13:01.977134	0.00214	IntelCltor_9e:58f0e7	Broadcast	802.11	168	53	-47	DBM
2422	2023-06-12 17:14:00.536729	58.55995	IntelCltor_9e:58f0e7	Broadcast	802.11	168	53	-50	DBM
9478	2023-06-12 17:14:29.581729	0.00000	IntelCltor_9e:58f0e7	Broadcast	802.11	168	53	-53	DBM
8007	2023-06-12 17:14:29.693397	29.162628	IntelCltor_9e:58f0e7	Broadcast	802.11	168	53	-45	DBM
8009	2023-06-12 17:14:29.707173	0.00216	IntelCltor_9e:58f0e7	Broadcast	802.11	168	53	-49	DBM
8217	2023-06-12 17:14:31.266534	1.564041	IntelCltor_9e:58f0e7	Broadcast	802.11	168	53	-48	DBM
8219	2023-06-12 17:14:31.268557	0.00203	IntelCltor_9e:58f0e7	Broadcast	802.11	168	53	-50	DBM
121	2023-06-12 17:15:17.081792	46.812326	IntelCltor_9e:58f0e7	Broadcast	802.11	168	53	-44	DBM
123	2023-06-12 17:15:17.084121	0.002319	IntelCltor_9e:58f0e7	Broadcast	802.11	168	53	-47	DBM
124	2023-06-12 17:15:18.183758	1.752349	IntelCltor_9e:58f0e7	Broadcast	802.11	168	53	-47	DBM
126	2023-06-12 17:15:18.184800	0.00248	IntelCltor_9e:58f0e7	Broadcast	802.11	168	53	-49	DBM
128	2023-06-12 17:15:18.584949	1.740939	IntelCltor_9e:58f0e7	Broadcast	802.11	168	53	-44	DBM
128	2023-06-12 17:15:20.587671	0.002722	IntelCltor_9e:58f0e7	Broadcast	802.11	168	53	-47	DBM
132	2023-06-12 17:15:32.193639	11.959559	IntelCltor_9e:58f0e7	Broadcast	802.11	168	53	-46	DBM
132	2023-06-12 17:15:32.260809	0.007339	IntelCltor_9e:58f0e7	Broadcast	Cisco_13:180e7	168	53	-36	DBM
132	2023-06-12 17:15:32.260809	0.00000	192.168.1.15	192.168.1.121	802.11	76	53	-47	DBM
132	2023-06-12 17:15:32.262711	0.004802	Cisco_13:180e7	IntelCltor_9e:58f0e7	802.11	194	53	-37	DBM
132	2023-06-12 17:15:32.262711	0.00000	192.168.1.15	192.168.1.121	802.11	76	53	-48	DBM
132	2023-06-12 17:15:32.262727	0.002866	IntelCltor_9e:58f0e7	Cisco_13:180e7	802.11	138	53	-46	DBM
132	2023-06-12 17:15:32.269464	0.003164	192.168.1.15	192.168.1.121	802.11	76	53	-37	DBM
132	2023-06-12 17:15:32.272528	0.001887	Cisco_13:180e7	IntelCltor_9e:58f0e7	802.11	138	53	-37	DBM
132	2023-06-12 17:15:32.272528	0.00000	192.168.1.15	192.168.1.121	802.11	76	53	-48	DBM
132	2023-06-12 17:15:32.273376	0.001848	IntelCltor_9e:58f0e7	Cisco_13:180e7	802.11	250	53	-49	DBM
132	2023-06-12 17:15:32.277987	0.000953	192.168.1.15	192.168.1.121	802.11	76	53	-39	DBM
132	2023-06-12 17:15:32.287395	0.011287	IntelCltor_9e:58f0e7	Cisco_13:180e7	802.11	144	53	-36	DBM
132	2023-06-12 17:15:32.285164	0.00000	IntelCltor_9e:58f0e7	Broadcast	LLC	114	53	-36	DBM
132	2023-06-12 17:15:32.286444	0.001208	Cisco_13:180e7	IntelCltor_9e:58f0e7	802.11	262	53	-36	DBM
132	2023-06-12 17:15:32.286444	0.00000	192.168.1.15	192.168.1.121	802.11	76	53	-46	DBM
132	2023-06-12 17:15:32.287797	0.001355	192.168.1.15	192.168.1.121	802.11	82	53	-36	DBM
132	2023-06-12 17:15:32.287998	0.000993	Cisco_13:180e7	IntelCltor_9e:58f0e7	APPO	221	53	-36	DBM
132	2023-06-12 17:15:32.287998	0.00000	192.168.1.15	192.168.1.121	802.11	76	53	-48	DBM
132	2023-06-12 17:15:32.290707	0.002717	IntelCltor_9e:58f0e7	Cisco_13:180e7	APPO	230	53	-42	DBM
132	2023-06-12 17:15:32.291046	0.000339	192.168.1.15	192.168.1.121	802.11	76	53	-36	DBM
132	2023-06-12 17:15:32.292135	0.002889	192.168.1.15	192.168.1.121	802.11	82	53	-36	DBM
132	2023-06-12 17:15:32.292548	0.000433							

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 339 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 000000000000FACB09B2189
 Acct Session ID 0x00000000
 Auth Method Status List
 Method SAE

Local Policies

NetGear A8000

Connection OTA with focus on the RSN information from client:

Frame 757: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on Interface 'Device\NPF_{04578995-2998-4466}...

Ethernet II, Src: Cisco_02:7d:37 (08:0f:3d:0d:7e:37), Dst: univers_07:cfc:06 (08:0a:88:07:cfc:06)

Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.121

User Datagram Protocol, Src Port: 5555, Dst Port: 5000

802.11 Radio Information

IEEE 802.11 Association Request, Flags:

IEEE 802.11 Wireless Management

- Fixed parameters (4 bytes)
- Tagged parameters (112 bytes)
 - Tag: SSID parameter set: "wifi6_test"
 - Tag: Supported Rates (0), 9, 12(6), 18, 24(6), 36, 48, 54, [Mbit/sec]
 - Ext Tag: HE Capabilities
 - Ext Tag: HE 4 GHz Band Capabilities
 - Tag: Vendor Specific: Hink Technology, Corp.
 - Tag: Vendor Specific: Microsoft Corp.: WPA/WPA2: Information Element
- Tag: RSN Information
 - Tag Number: RSN Information (48)
 - Tag Length: 22
 - RSN Version: 1
 - Group Cipher Suite: 0x00000000 (IEEE 802.11 AES (CCM))
 - Pairwise Cipher Suite Count: 1
 - Pairwise Cipher Suite List 0x00000000 (IEEE 802.11 AES (CCM))
 - Auth Key Management (AKM) Suite Count: 1
 - Auth Key Management (AKM) List 0x00000000 (IEEE 802.11 AES (CCM))
 - RSN Capabilities: 0x0000
 - PMKID Count: 0
 - PMKID List
 - Tag: RSN extension (1 octet)
 - Tag Number: RSN extension (244)
 - Tag Length: 1
 - RSN: 0x20 (octet 1)
 - 0000 = RSN Length: 0
 - ...0 = Protected TSP Operations Support: 0
 - ..1.... = SAE used to element: 1
 - 00..... = Reserved: 0
 - Tag: HE Enabled Capabilities (5 octets)

Client details in WLC:

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 24 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 000000000000FAB0A160F3
 Acct Session ID 0x00000000
 Auth Method Status List
 Method SAE

Pixel 6a

Connection OTA with focus on the RSN information from client:

The image shows a Wireshark capture of IEEE 802.11 frames. The left pane displays a list of packets, including Probe Requests, Authentication, Association Request, and Action frames. The right pane shows the details of a selected frame, detailing the IEEE 802.11 radio information, fixed parameters, and management parameters such as the Authentication Algorithm (Simultaneous Authentication of Equals (SAE)), SAE Message Type (Commit (1)), and SAE Group ID.

Client details in WLC:

The screenshot displays the Cisco Catalyst 9800-CL Wireless Controller GUI. The 'Clients' tab is active, showing a list of clients. The selected client is a Samsung S23 with MAC address 2495.2172.8a66 and IP address 192.168.1.162. The right pane shows the 'Client' details, including Client Properties, AP Properties, Security Information, Client Statistics, and QoS Properties. The Security Information section shows the Client State Servers, Client ACLs, Client Entry Create Time, Policy Type (WPA3), Encryption Cipher (CCMP (AES)), Authentication Key Management (SAE), EAP Type (Not Applicable), and Session Timeout (86400).

Samsung S23

Connection OTA with focus on the RSN information from client:

The image shows a Wireshark capture of IEEE 802.11 frames for a Samsung S23. The left pane displays a list of packets, including Authentication, Association Request, and Action frames. The right pane shows the details of a selected frame, detailing the IEEE 802.11 radio information, fixed parameters, and management parameters such as the Authentication Algorithm (Simultaneous Authentication of Equals (SAE)), SAE Message Type (Commit (1)), and SAE Group ID.

Client details in WLC:

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:fe1:dd57	AP03_Sotao_9548
<input type="checkbox"/>	0012.1762.4856	192.168.1.37	fe80::212:17ff:fe2:4856	AP05_OutdoorB_220
<input type="checkbox"/>	0012.17e2.4b40	192.168.1.31	fe80::212:17ff:fe2:4b40	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

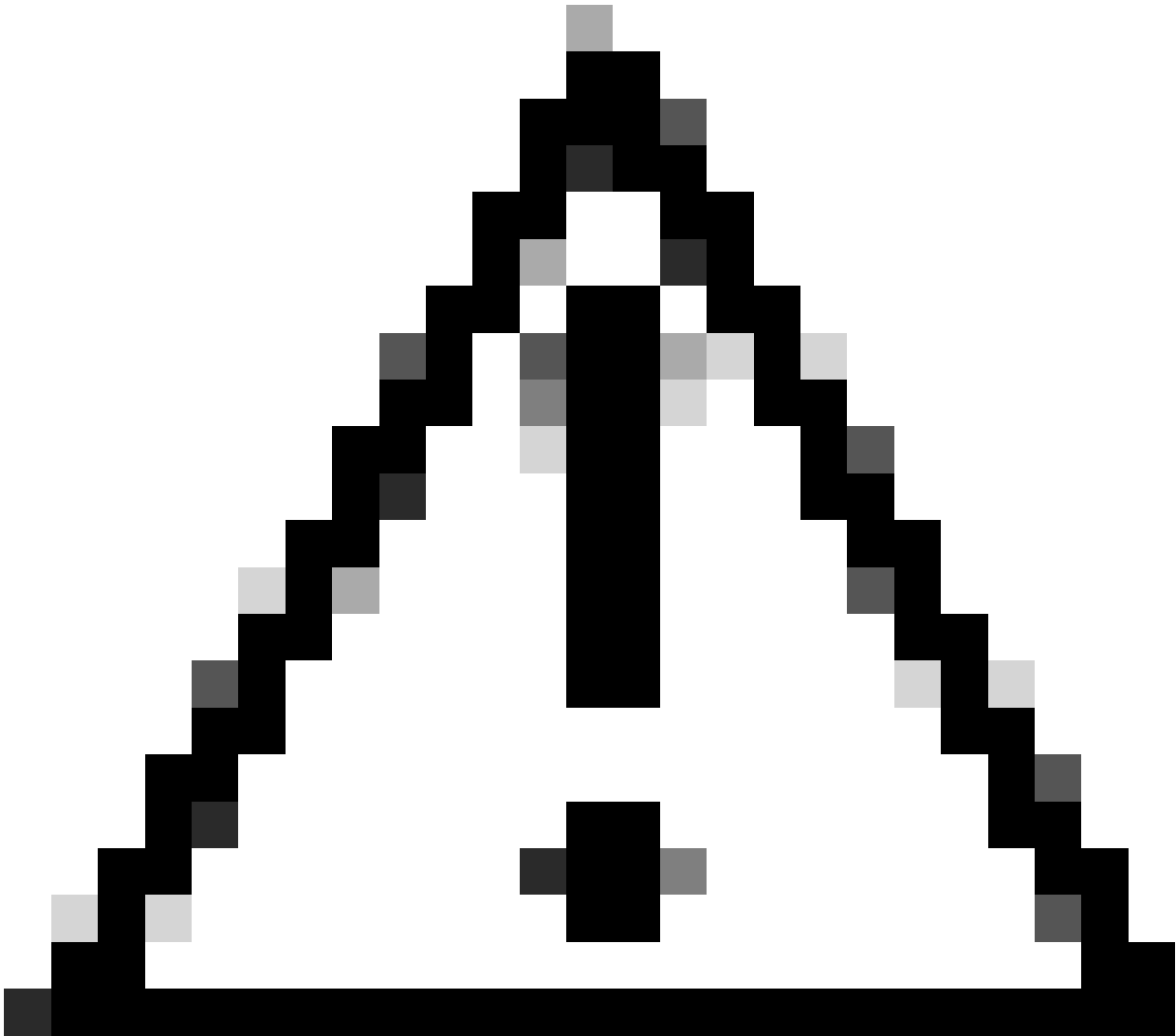
Auth Key Mgmt

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

Protected Management Frame

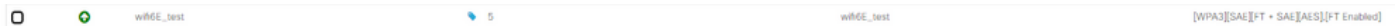
PMF ▾
 Association Comeback Timer*
 SA Query Time*

Anti Clogging Threshold*
 Max Retries*
 Retransmit Timeout*
 PSK Format ▾
 PSK Type ▾
 Pre-Shared Key*
 SAE Password Element ⓘ ▾



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 rate Info
1 2023-06-12 10:34:49.265337 0.000000 Cisco_13:180:e4 Broadcast 802.11 588 5 -36 dBm Beacon frame, SWS227, Flow, Flags:.....C, B1=100, SSID="wifi6e"
2 2023-06-12 10:34:49.427544 0.162267 Cisco_13:180:e4 Broadcast 802.11 588 5 -36 dBm Beacon frame, SWS27, Flow, Flags:.....C, B1=100, SSID="wifi6e"
3 2023-06-12 10:34:49.528357 0.102123 Cisco_13:180:e4 Broadcast 802.11 588 5 -37 dBm Beacon frame, SWS23, Flow, Flags:.....C, B1=100, SSID="wifi6e"
4 2023-06-12 10:34:49.629332 0.102465 Cisco_13:180:e4 Broadcast 802.11 588 5 -37 dBm Beacon frame, SWS27, Flow, Flags:.....C, B1=100, SSID="wifi6e"
5 2023-06-12 10:34:49.791084 0.169672 Hetgear_48:708:95 Cisco_13:180:e4 360 5 -49 dBm Probe Request, SWS28, Flow, Flags:.....C, SSID="wifi6e_test"
6 2023-06-12 10:34:49.791304 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -37 dBm Acknowledgment, Flags:.....C
7 2023-06-12 10:34:49.791527 0.000352 Hetgear_48:708:95 Cisco_13:180:e4 360 5 -49 dBm Probe Request, SWS1, Flow, Flags:.....C, SSID="wifi6e_test"
8 2023-06-12 10:34:49.791547 0.000071 192.168.1.15 192.168.1.121 802.11 76 5 -37 dBm Acknowledgment, Flags:.....C
9 2023-06-12 10:34:49.794933 0.003966 Cisco_13:180:e4 Broadcast 802.11 588 5 -37 dBm Beacon frame, SWS22, Flow, Flags:.....C, B1=100, SSID="wifi6e"
10 2023-06-12 10:34:49.818282 0.015789 Hetgear_48:708:95 Cisco_13:180:e4 360 5 -49 dBm Probe Request, SWS1, Flow, Flags:.....C, SSID="wifi6e_test"
11 2023-06-12 10:34:49.818382 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -37 dBm Acknowledgment, Flags:.....C
12 2023-06-12 10:34:49.829653 0.000000 Cisco_13:180:e4 Broadcast 802.11 194 5 -49 dBm Authentication, SWS, Flow, Flags:.....C
13 2023-06-12 10:34:49.874951 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -37 dBm Acknowledgment, Flags:.....C
14 2023-06-12 10:34:49.896563 0.021812 Hetgear_48:708:95 Broadcast 802.11 194 5 -37 dBm Authentication, SWS46, Flow, Flags:.....C
15 2023-06-12 10:34:49.896563 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -49 dBm Acknowledgment, Flags:.....C
16 2023-06-12 10:34:49.904966 0.000043 Cisco_13:180:e4 Broadcast 802.11 588 5 -37 dBm Beacon frame, SWS47, Flow, Flags:.....C, B1=100, SSID="wifi6e"
17 2023-06-12 10:34:49.904966 0.000000 Hetgear_48:708:95 Cisco_13:180:e4 360 5 -49 dBm Authentication, SWS5, Flow, Flags:.....C
18 2023-06-12 10:34:49.904966 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -37 dBm Acknowledgment, Flags:.....C
19 2023-06-12 10:34:49.904966 0.000000 Hetgear_48:708:95 Broadcast 802.11 130 5 -37 dBm Authentication, SWS47, Flow, Flags:.....C
20 2023-06-12 10:34:49.904966 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -48 dBm Acknowledgment, Flags:.....C
21 2023-06-12 10:34:49.904966 0.000000 Hetgear_48:708:95 Cisco_13:180:e4 360 5 -49 dBm Association Request, SWS4, Flow, Flags:.....C, SSID="wifi6e_test"
22 2023-06-12 10:34:49.904966 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -36 dBm Acknowledgment, Flags:.....C
23 2023-06-12 10:34:49.91474 0.000580 Hetgear_48:708:95 Broadcast 802.11 262 5 -36 dBm Association Response, SWS4, Flow, Flags:.....C
24 2023-06-12 10:34:49.91474 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -49 dBm Acknowledgment, Flags:.....C
25 2023-06-12 10:34:49.917179 0.000245 Hetgear_48:708:95 Broadcast LLC 114 5 -37 dBm v, func=unknown; DSAP 0x12 Individual, SSAP 0x02 Command
26 2023-06-12 10:34:49.917179 0.000000 Hetgear_48:708:95 Broadcast LLC 114 5 -36 dBm v, func=unknown; DSAP 0x12 Individual, SSAP 0x02 Response
27 2023-06-12 10:34:49.922246 0.000000 Hetgear_48:708:95 Broadcast LLC 221 5 -36 dBm Key (Message 1 of 4)
28 2023-06-12 10:34:49.922246 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -49 dBm Acknowledgment, Flags:.....C
29 2023-06-12 10:34:49.999581 0.077235 Cisco_13:180:e4 Broadcast 802.11 588 5 -36 dBm Beacon frame, SWS27, Flow, Flags:.....C, B1=100, SSID="wifi6e"
30 2023-06-12 10:34:50.104510 0.104929 Cisco_13:180:e4 Broadcast 802.11 588 5 -36 dBm Beacon frame, SWS27, Flow, Flags:.....C, B1=100, SSID="wifi6e"
31 2023-06-12 10:34:50.204060 0.000789 Hetgear_48:708:95 Broadcast 802.11 262 5 -36 dBm Association Response, SWS4, Flow, Flags:.....C, B1=100, SSID="wifi6e"
32 2023-06-12 10:34:50.211615 0.007915 Hetgear_48:708:95 Cisco_13:180:e4 360 5 -48 dBm Key (Message 2 of 4)
33 2023-06-12 10:34:50.211615 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -42 dBm Acknowledgment, Flags:.....C
34 2023-06-12 10:34:50.213376 0.002194 Hetgear_48:708:95 Broadcast LLC 226 5 -49 dBm Key (Message 3 of 4)
35 2023-06-12 10:34:50.213376 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -48 dBm Acknowledgment, Flags:.....C
36 2023-06-12 10:34:50.214354 0.000978 Hetgear_48:708:95 Cisco_13:180:e4 360 5 -49 dBm Key (Message 4 of 4)
37 2023-06-12 10:34:50.214354 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -42 dBm Acknowledgment, Flags:.....C
38 2023-06-12 10:34:50.228072 0.000367 192.168.1.15 192.168.1.121 802.11 76 5 -42 dBm Acknowledgment, Flags:.....C
39 2023-06-12 10:34:50.228089 0.000328 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 10:34:50.228089 0.000000 IntelCoL_30:159:df IntelCoL_30:159:df Broadcast 802.11 LLC 221 5 -44 dBm v, func=unknown; DSAP 0x00 Group, SSAP 0x00 Response
41 2023-06-12 10:34:50.228089 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -44 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 rate Info
1813 2023-06-12 18:51:51.249793 0.017337 IntelCoL_30:159:df Cisco_13:180:e4 360 5 -42 dBm Authentication, SWS4, Flow, 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 IntelCoL_30:159:df Cisco_13:180:e4 360 5 -48 dBm Authentication, SWS1, Flow, Flags:.....C
1817 2023-06-12 18:51:51.261579 0.004285 Cisco_13:180:e4 Broadcast 802.11 130 5 -36 dBm Authentication, SWS46, Flow, Flags:.....C
1818 2023-06-12 18:51:51.263679 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -42 dBm Acknowledgment, Flags:.....C
1819 2023-06-12 18:51:51.263679 0.000000 IntelCoL_30:159:df Cisco_13:180:e4 360 5 -48 dBm Association Request, SWS4, Flow, Flags:.....C, SSID="wifi6e_test"
1820 2023-06-12 18:51:51.265919 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -36 dBm Acknowledgment, Flags:.....C
1826 2023-06-12 18:51:51.274142 0.018463 IntelCoL_30:159:df Broadcast LLC 114 5 -36 dBm I, N(1)=0, N(5)=3; DSAP 0x00 Group, SSAP 0x00 Response
1827 2023-06-12 18:51:51.274142 0.000000 IntelCoL_30:159:df Broadcast LLC 114 5 -36 dBm I, N(1)=7, N(5)=32; DSAP 0x00 Group, SSAP 0x00 Spawning Tree 0x00 Response
1828 2023-06-12 18:51:51.277482 0.003240 Cisco_13:180:e4 IntelCoL_30:159:df 262 5 -36 dBm Association Response, SWS4, Flow, Flags:.....C
1829 2023-06-12 18:51:51.277482 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -43 dBm Acknowledgment, Flags:.....C
1830 2023-06-12 18:51:51.286187 0.008785 Cisco_13:180:e4 Broadcast 802.11 517 5 -36 dBm Beacon frame, SWS376, Flow, Flags:.....C, B1=100, SSID="wifi6e_test_02"
1834 2023-06-12 18:51:51.321249 0.025242 192.168.1.15 192.168.1.121 802.11 76 5 -36 dBm Acknowledgment, Flags:.....C
1835 2023-06-12 18:51:51.341810 0.004849 192.168.1.15 192.168.1.121 802.11 76 5 -52 dBm Clear-to-send, Flags:.....C
1837 2023-06-12 18:51:51.331825 0.017227 192.168.1.15 192.168.1.121 802.11 76 5 -36 dBm Acknowledgment, Flags:.....C
1841 2023-06-12 18:51:51.388460 0.058935 Cisco_13:180:e4 Broadcast 802.11 517 5 -37 dBm Beacon frame, SWS376, Flow, Flags:.....C, B1=100, SSID="wifi6e_test_02"
1842 2023-06-12 18:51:51.389880 0.001348 192.168.1.15 192.168.1.121 802.11 76 5 -53 dBm Clear-to-send, Flags:.....C
1844 2023-06-12 18:51:51.397943 0.008115 192.168.1.15 192.168.1.121 802.11 82 5 -36 dBm Request-to-send, Flags:.....C
1845 2023-06-12 18:51:51.398982 0.000839 192.168.1.15 192.168.1.121 802.11 82 5 -36 dBm Request-to-send, Flags:.....C
1846 2023-06-12 18:51:51.399181 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 18:51:51.408524 0.000712 192.168.1.15 192.168.1.121 802.11 82 5 -36 dBm Request-to-send, Flags:.....C
1848 2023-06-12 18:51:51.408193 0.000667 192.168.1.15 192.168.1.121 802.11 82 5 -36 dBm Request-to-send, Flags:.....C
1849 2023-06-12 18:51:51.408295 0.000844 192.168.1.15 192.168.1.121 802.11 82 5 -36 dBm Request-to-send, Flags:.....C
1850 2023-06-12 18:51:51.408261 0.000582 192.168.1.15 192.168.1.121 802.11 82 5 -36 dBm Request-to-send, Flags:.....C
1851 2023-06-12 18:51:51.408153 0.000636 192.168.1.15 192.168.1.121 802.11 82 5 -36 dBm Request-to-send, Flags:.....C
1852 2023-06-12 18:51:51.408374 0.001212 192.168.1.15 192.168.1.121 802.11 82 5 -36 dBm Request-to-send, Flags:.....C
1853 2023-06-12 18:51:51.408306 0.000732 192.168.1.15 192.168.1.121 802.11 82 5 -36 dBm Request-to-send, Flags:.....C
1854 2023-06-12 18:51:51.408877 0.000971 192.168.1.15 192.168.1.121 802.11 82 5 -36 dBm Request-to-send, Flags:.....C
1855 2023-06-12 18:51:51.408657 0.000740 192.168.1.15 192.168.1.121 802.11 82 5 -36 dBm Request-to-send, Flags:.....C
1856 2023-06-12 18:51:51.408681 0.000844 192.168.1.15 192.168.1.121 802.11 76 5 -36 dBm Acknowledgment, Flags:.....C
1857 2023-06-12 18:51:51.407244 0.000663 192.168.1.15 192.168.1.121 802.11 82 5 -48 dBm Request-to-send, Flags:.....C
1859 2023-06-12 18:51:51.407527 0.000253 Cisco_13:180:e4 IntelCoL_30:159:df Broadcast 802.11 EAPOL 221 5 -36 dBm Key (Message 1 of 4)
1862 2023-06-12 18:51:51.439712 0.001815 IntelCoL_30:159:df Cisco_13:180:e4 360 5 -52 dBm Key (Message 2 of 4)
1863 2023-06-12 18:51:51.439712 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -37 dBm Acknowledgment, Flags:.....C
1864 2023-06-12 18:51:51.432220 0.001580 192.168.1.15 192.168.1.121 802.11 82 5 -37 dBm Request-to-send, Flags:.....C
1866 2023-06-12 18:51:51.432651 0.000431 Cisco_13:180:e4 IntelCoL_30:159:df Broadcast 802.11 EAPOL 303 5 -37 dBm Key (Message 3 of 4)
1867 2023-06-12 18:51:51.432651 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -48 dBm Acknowledgment, Flags:.....C
1868 2023-06-12 18:51:51.432651 0.000000 IntelCoL_30:159:df Cisco_13:180:e4 Broadcast 802.11 EAPOL 199 5 -53 dBm Key (Message 4 of 4)
1869 2023-06-12 18:51:51.432651 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -37 dBm Acknowledgment, Flags:.....C
```

Roaming event where you can see the PMKID:

```

[Packet#0] 88 ( wlan_addr == 280b.3598.580f ) | ( wlan_ft_type_subtype == 0x001d ) or ( wlan_ft_type_subtype == 0x0018 )
No. Time Delta Source Destination Protocol Length Channel Signal strength Info
226 2023-06-12 18:53:11.488635 0.000229 Intercor_98180e0f Intercor_981... LLC 325 5 -75 dBm S, func=8, N(0)=0; DSAP Null LSAP Individual, SSAP Null LSAP Command
227 2023-06-12 18:53:11.488812 0.000230 Intercor_98180e0f Intercor_981... LLC 325 5 -75 dBm S, func=8, N(0)=0; DSAP Null LSAP Individual, SSAP Null LSAP Command
228 2023-06-12 18:53:11.489318 0.000229 Intercor_98180e0f Intercor_981... LLC 245 5 -75 dBm S, func=8, N(0)=0; DSAP Null LSAP Individual, SSAP Null LSAP Command
229 2023-06-12 18:53:11.489318 0.000000 Intercor_98180e0f Intercor_981... LLC 325 5 -49 dBm S, func=8, N(0)=0; DSAP Null LSAP Individual, SSAP Null LSAP Command
230 2023-06-12 18:53:11.489319 0.000049 Intercor_98180e0f Intercor_981... LLC 325 5 -74 dBm S, func=8, N(0)=0; DSAP Null LSAP Individual, SSAP Null LSAP Command
231 2023-06-12 18:53:11.489364 0.000183 Intercor_98180e0f Intercor_981... LLC 325 5 -74 dBm S, func=8, N(0)=0; DSAP Null LSAP Individual, SSAP Null LSAP Command
232 2023-06-12 18:53:11.489584 0.000042 Intercor_98180e0f Intercor_981... LLC 325 5 -74 dBm S, func=8, N(0)=0; DSAP Null LSAP Individual, SSAP Null LSAP Command
233 2023-06-12 18:53:11.489639 0.000035 Intercor_98180e0f Intercor_981... LLC 325 5 -74 dBm S, func=8, N(0)=0; DSAP Null LSAP Individual, SSAP Null LSAP Command
234 2023-06-12 18:53:11.491397 0.000000 Intercor_98180e0f Intercor_981... LLC 245 5 -74 dBm S, func=8, N(0)=0; DSAP Null LSAP Individual, SSAP Null LSAP Command
235 2023-06-12 18:53:11.491363 0.000282 Intercor_98180e0f Intercor_981... LLC 325 5 -74 dBm S, func=8, N(0)=0; DSAP Null LSAP Individual, SSAP Null LSAP Command
236 2023-06-12 18:53:11.491397 0.000034 Intercor_98180e0f Intercor_981... LLC 325 5 -77 dBm S, func=8, N(0)=0; DSAP Null LSAP Individual, SSAP Null LSAP Command
237 2023-06-12 18:53:11.491397 0.000000 Intercor_98180e0f Intercor_981... LLC 325 5 -76 dBm S, func=8, N(0)=0; DSAP Null LSAP Individual, SSAP Null LSAP Command
238 2023-06-12 18:53:11.491242 0.000045 Intercor_98180e0f Intercor_981... LLC 325 5 -77 dBm S, func=8, N(0)=0; DSAP Null LSAP Individual, SSAP Null LSAP Command
239 2023-06-12 18:53:11.491253 0.000011 Intercor_98180e0f Intercor_981... LLC 325 5 -77 dBm S, func=8, N(0)=0; DSAP Null LSAP Individual, SSAP Null LSAP Command
240 2023-06-12 18:53:11.508532 0.000009 192.168.1.15 192.168.1.121 802.11 76 5 -36 dBm Acknowledgment, Flags.....C
241 2023-06-12 18:53:11.513546 0.000034 Cisco_13180e0f Intercor_981... LLC 245 5 -77 dBm S, func=8, N(0)=0; DSAP Null LSAP Individual, SSAP Null LSAP Command
242 2023-06-12 18:53:11.513546 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -42 dBm Acknowledgment, Flags.....C
243 2023-06-12 18:53:11.514786 0.000000 192.168.1.15 192.168.1.121 802.11 272 5 -46 dBm Reassociation Request, SMO, P, H, W, Flags.....C, SSID="WiFiE_test"
244 2023-06-12 18:53:11.514787 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -36 dBm Acknowledgment, Flags.....C
245 2023-06-12 18:53:11.527665 0.013487 Cisco_13180e0f Intercor_981... LLC 262 5 -36 dBm Reassociation Response, SMO, P, H, W, Flags.....C
246 2023-06-12 18:53:11.527665 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -42 dBm Acknowledgment, Flags.....C
247 2023-06-12 18:53:11.528485 0.000744 Broadcast Intercor_98180e0f Broadcast LLC 114 5 -36 dBm I, P, N(0)=4, N(1)=2; DSAP Null Group, SSAP Null Response
248 2023-06-12 18:53:11.528485 0.000040 Intercor_98180e0f Broadcast LLC 114 5 -36 dBm I, N(0)=7, N(1)=2; DSAP Null Individual, SSAP Null Command
249 2023-06-12 18:53:11.530430 0.001935 192.168.1.15 192.168.1.121 802.11 82 5 -36 dBm Request-to-send, Flags.....C
250 2023-06-12 18:53:11.530430 0.000000 Cisco_13180e0f Intercor_981... LLC 221 5 -36 dBm Key (Message 2 of 4)
251 2023-06-12 18:53:11.530430 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -47 dBm Acknowledgment, Flags.....C
252 2023-06-12 18:53:11.531348 0.002130 Intercor_98180e0f Cisco_13180e0f EAPOL 246 5 -47 dBm Key (Message 2 of 4)
253 2023-06-12 18:53:11.531348 0.000000 192.168.1.15 192.168.1.121 802.11 82 5 -36 dBm Acknowledgment, Flags.....C
254 2023-06-12 18:53:11.534769 0.001601 192.168.1.15 192.168.1.121 802.11 82 5 -36 dBm Request-to-send, Flags.....C
255 2023-06-12 18:53:11.535972 0.000080 Cisco_13180e0f Intercor_981... EAPOL 389 5 -36 dBm Key (Message 3 of 4)
256 2023-06-12 18:53:11.535972 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -36 dBm Acknowledgment, Flags.....C
257 2023-06-12 18:53:11.535997 0.000035 Intercor_98180e0f Cisco_13180e0f EAPOL 199 5 -78 dBm I, P, N(0)=4, N(1)=2; DSAP Null Group, SSAP Null Response
258 2023-06-12 18:53:11.535997 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -36 dBm Acknowledgment, Flags.....C
259 2023-06-12 18:53:11.545286 0.000000 CiscoCom_531c1850 Intercor_981... LLC 187 5 -46 dBm I, N(0)=16, N(1)=2; DSAP Null LSAP Group, SSAP Null Command
260 2023-06-12 18:53:11.545286 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -72 dBm Acknowledgment, Flags.....C
261 2023-06-12 18:53:11.545286 0.000000 192.168.1.15 192.168.1.121 802.11 82 5 -72 dBm Request-to-send, Flags.....C
262 2023-06-12 18:53:11.556775 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -36 dBm Clear-to-send, Flags.....C
263 2023-06-12 18:53:11.556775 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -36 dBm Clear-to-send, Flags.....C
264 2023-06-12 18:53:11.556775 0.000282 Intercor_98180e0f Broadcast LLC 515 5 -75 dBm I, P, N(0)=7, N(1)=2; DSAP Null Individual, SSAP Null Command
265 2023-06-12 18:53:11.556777 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -36 dBm Acknowledgment, Flags.....C

```

WPA3 SAE + FT Reassociation Request

Client details in WLC:

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The 'Clients' tab is active, displaying a list of clients. The selected client is 280b.3598.580f, which is associated with the AP 98649.9253.CA50. The client's IP address is 192.168.1.159 and its IPv6 address is fe80::ca2b:e1e1:67ba:c353. The client's state is 'Sleeping'.

NetGear A8000

Connection OTA with focus on the RSN information from client. Initial connection:

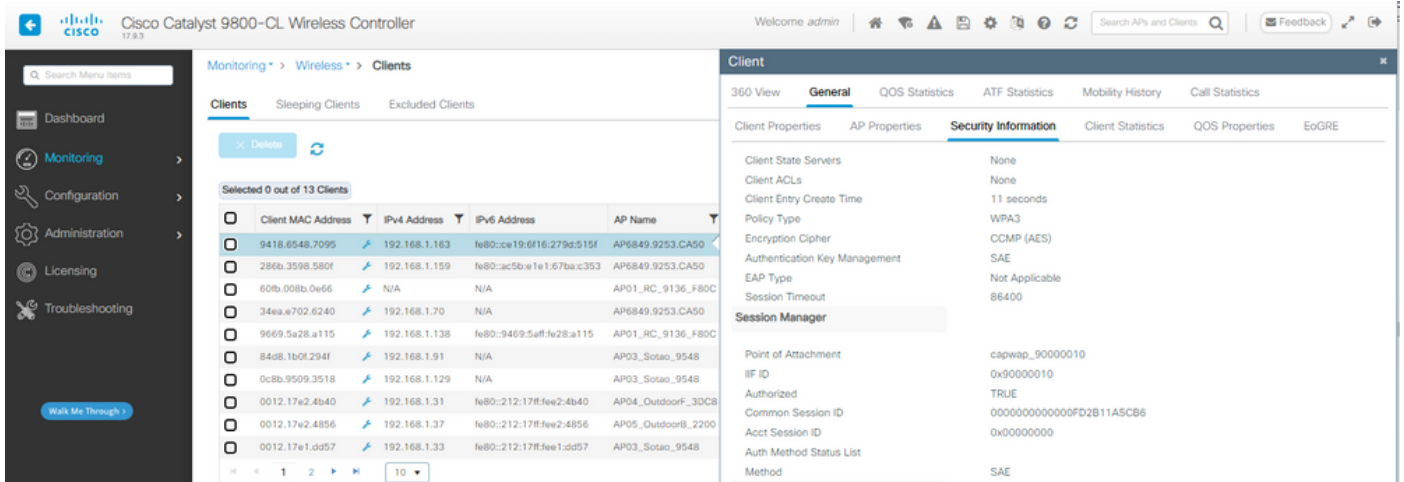
```

No. Time Delta Source Destination Protocol Length Channel Signal strength BSSID Info
1 18:54:49.385337 0.000000 Cisco_13180e0f Broadcast 802.11 508 5 -36 dBm 38:93:37:13:80a7 Beacon frame, SMO, P, H, W, Flags.....C, B1=S0M, SSID="WiFiE_test_R0", SSID="W
2 18:54:49.487544 0.000287 Cisco_13180e0f Broadcast 802.11 508 5 -36 dBm 38:93:37:13:80a7 Beacon frame, SMO, P, H, W, Flags.....C, B1=S0M, SSID="WiFiE_test_R0", SSID="W
3 18:54:49.588867 0.000212 Cisco_13180e0f Broadcast 802.11 508 5 -37 dBm 38:93:37:13:80a7 Beacon frame, SMO, P, H, W, Flags.....C, B1=S0M, SSID="WiFiE_test_R0", SSID="W
4 18:54:49.692532 0.000260 Cisco_13180e0f Broadcast 802.11 508 5 -37 dBm 38:93:37:13:80a7 Beacon frame, SMO, P, H, W, Flags.....C, B1=S0M, SSID="WiFiE_test_R0", SSID="W
5 18:54:49.793884 0.000072 Netgear_48170c95 Cisco_13180e0f 802.11 360 5 -49 dBm 38:93:37:13:80a7 Probe Request, SMO, P, H, W, Flags.....C, SSID="WiFiE_test"
6 18:54:49.793884 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -37 dBm 38:93:37:13:80a7 Acknowledgment, Flags.....C
7 18:54:49.793884 0.000032 Netgear_48170c95 Cisco_13180e0f 802.11 360 5 -49 dBm 38:93:37:13:80a7 Probe Request, SMO, P, H, W, Flags.....C, SSID="WiFiE_test"
8 18:54:49.793884 0.000072 192.168.1.15 192.168.1.121 802.11 76 5 -37 dBm 38:93:37:13:80a7 Acknowledgment, Flags.....C
9 18:54:49.793884 0.000000 Cisco_13180e0f Broadcast 802.11 508 5 -37 dBm 38:93:37:13:80a7 Beacon frame, SMO, P, H, W, Flags.....C, B1=S0M, SSID="WiFiE_test_R0", SSID="W
10 18:54:49.892062 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -37 dBm 38:93:37:13:80a7 Acknowledgment, Flags.....C
11 18:54:49.892062 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -37 dBm 38:93:37:13:80a7 Acknowledgment, Flags.....C
12 18:54:49.892062 0.000000 Netgear_48170c95 Cisco_13180e0f 802.11 194 5 -49 dBm 38:93:37:13:80a7 Authentication, SMO, P, H, W, Flags.....C
13 18:54:49.892062 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -37 dBm 38:93:37:13:80a7 Acknowledgment, Flags.....C
14 18:54:49.892062 0.000000 Netgear_48170c95 Cisco_13180e0f 802.11 384 5 -37 dBm 38:93:37:13:80a7 Authentication, SMO, P, H, W, Flags.....C
15 18:54:49.892062 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -37 dBm 38:93:37:13:80a7 Acknowledgment, Flags.....C
16 18:54:49.892062 0.000000 Cisco_13180e0f Broadcast 802.11 508 5 -37 dBm 38:93:37:13:80a7 Beacon frame, SMO, P, H, W, Flags.....C, B1=S0M, SSID="WiFiE_test_R0", SSID="W
17 18:54:49.892062 0.000000 Netgear_48170c95 Cisco_13180e0f 802.11 130 5 -37 dBm 38:93:37:13:80a7 Authentication, SMO, P, H, W, Flags.....C
18 18:54:49.892062 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -48 dBm 38:93:37:13:80a7 Acknowledgment, Flags.....C
19 18:54:49.892062 0.000000 Netgear_48170c95 Cisco_13180e0f 802.11 254 5 -49 dBm 38:93:37:13:80a7 Association Request, SMO, P, H, W, Flags.....C, SSID="WiFiE_test"
20 18:54:49.892062 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -36 dBm 38:93:37:13:80a7 Acknowledgment, Flags.....C
21 18:54:49.912474 0.000000 Netgear_48170c95 Broadcast LLC 124 5 -36 dBm 38:93:37:13:80a7 Association Response, SMO, P, H, W, Flags.....C
22 18:54:49.912474 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -49 dBm 38:93:37:13:80a7 Acknowledgment, Flags.....C
23 18:54:49.912474 0.000000 Netgear_48170c95 Broadcast LLC 124 5 -36 dBm 38:93:37:13:80a7 Key (Message 2 of 4)
24 18:54:49.912474 0.000000 Cisco_13180e0f Broadcast 802.11 226 5 -36 dBm 38:93:37:13:80a7 Key (Message 2 of 4)
25 18:54:49.912474 0.000000 Netgear_48170c95 EAPOL 226 5 -36 dBm 38:93:37:13:80a7 Key (Message 2 of 4)
26 18:54:49.912474 0.000000 Cisco_13180e0f Broadcast 802.11 508 5 -36 dBm 38:93:37:13:80a7 Beacon frame, SMO, P, H, W, Flags.....C, B1=S0M, SSID="WiFiE_test_R0", SSID="W
27 18:54:49.912474 0.000000 Netgear_48170c95 Broadcast LLC 124 5 -36 dBm 38:93:37:13:80a7 Key (Message 2 of 4)
28 18:54:49.912474 0.000000 Cisco_13180e0f Broadcast 802.11 508 5 -36 dBm 38:93:37:13:80a7 Beacon frame, SMO, P, H, W, Flags.....C, B1=S0M, SSID="WiFiE_test_R0", SSID="W
29 18:54:49.912474 0.000000 Netgear_48170c95 EAPOL 226 5 -36 dBm 38:93:37:13:80a7 Key (Message 2 of 4)
30 18:54:49.912474 0.000000 Cisco_13180e0f Broadcast 802.11 508 5 -36 dBm 38:93:37:13:80a7 Beacon frame, SMO, P, H, W, Flags.....C, B1=S0M, SSID="WiFiE_test_R0", SSID="W
31 18:54:49.912474 0.000000 Netgear_48170c95 EAPOL 226 5 -36 dBm 38:93:37:13:80a7 Key (Message 2 of 4)
32 18:54:49.912474 0.000000 Netgear_48170c95 EAPOL 226 5 -36 dBm 38:93:37:13:80a7 Key (Message 2 of 4)
33 18:54:49.912474 0.000000 Netgear_48170c95 EAPOL 226 5 -36 dBm 38:93:37:13:80a7 Key (Message 2 of 4)
34 18:54:49.912474 0.000000 Netgear_48170c95 EAPOL 226 5 -36 dBm 38:93:37:13:80a7 Key (Message 2 of 4)
35 18:54:49.912474 0.000000 Netgear_48170c95 EAPOL 226 5 -36 dBm 38:93:37:13:80a7 Key (Message 2 of 4)
36 18:54:49.912474 0.000000 Netgear_48170c95 EAPOL 199 5 -36 dBm 38:93:37:13:80a7 Key (Message 2 of 4)
37 18:54:49.912474 0.000000 Netgear_48170c95 EAPOL 226 5 -36 dBm 38:93:37:13:80a7 Key (Message 2 of 4)
38 18:54:49.912474 0.000000 Netgear_48170c95 EAPOL 226 5 -36 dBm 38:93:37:13:80a7 Key (Message 2 of 4)
39 18:54:49.912474 0.000000 Netgear_48170c95 EAPOL 226 5 -36 dBm 38:93:37:13:80a7 Key (Message 2 of 4)
40 18:54:49.912474 0.000000 Netgear_48170c95 EAPOL 226 5 -36 dBm 38:93:37:13:80a7 Key (Message 2 of 4)
41 18:54:49.912474 0.000000 Netgear_48170c95 EAPOL 226 5 -36 dBm 38:93:37:13:80a7 Key (Message 2 of 4)
42 18:54:49.912474 0.000000 Netgear_48170c95 EAPOL 226 5 -36 dBm 38:93:37:13:80a7 Key (Message 2 of 4)
43 18:54:49.912474 0.000000 Netgear_48170c95 EAPOL 226 5 -36 dBm 38:93:37:13:80a7 Key (Message 2 of 4)
44 18:54:49.912474 0.000000 Netgear_48170c95 EAPOL 226 5 -36 dBm 38:93:37:13:80a7 Key (Message 2 of 4)
45 18:54:49.912474 0.000000 Netgear_48170c95 EAPOL 226 5 -36 dBm 38:93:37:13:80a7 Key (Message 2 of 4)

```

SSSS

Client details in WLC:



Pixel 6a

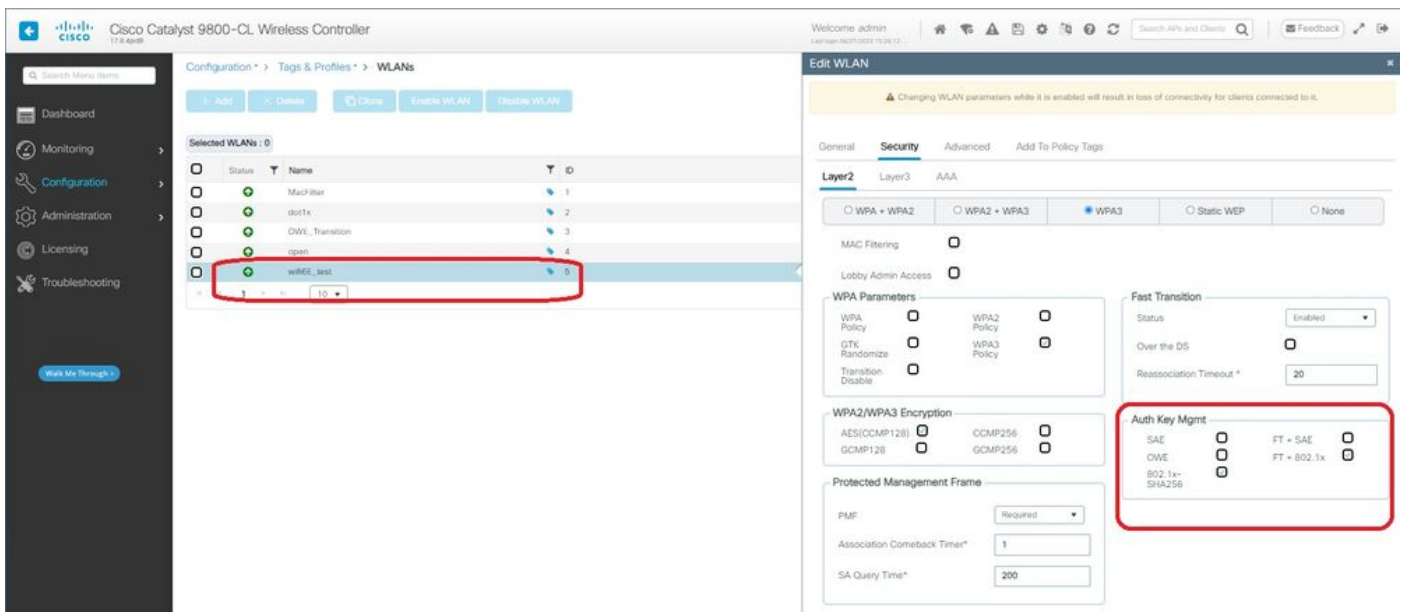
Device was not able to roam when FT is enabled.

Samsung S23

Device was not able to roam when FT is enabled.

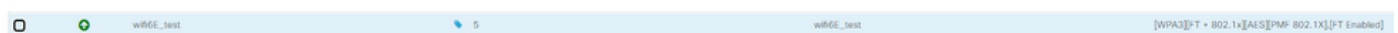
WPA3-Enterprise + AES(CCMP128) + 802.1x-SHA256 + FT

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:** Frames 104-110 showing probe requests and responses.
- Regular Association:** Frames 111-114 showing association request and response.
- EAP Exchange:** Frames 115-120 showing EAP messages, including a Protected EAP (PEAP) message and a PMKID List. A red box highlights the PMKID used for FT.
- 4 Way Handshake:** Frames 121-124 showing the four-way handshake messages.

WPA3 Enterprise 802.1x + FT Ax211 Connection flow

Client details in WLC:

The screenshot shows the Cisco WLC GUI with the following client details:

Client MAC Address	IPv4 Address	IPv6 Address	AP Name	SSID
286b.3598.580f	192.168.1.159	2001:8a0:fb01:1:c00:c07a:1190:8069:7398	AP9136_5C F524	wifiE

The right-hand pane shows the 'Security Information' tab with the following details:

- 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_05:58:08	Broadcast	802.11	364	69	-36	Beacon frame, Src: 05:58:08, FwB, Flags:.....C, B1=100, SSID=wifitest
3029	16.504273	0.120808	Cisco_05:58:08	Broadcast	802.11	364	69	-36	Beacon frame, Src: 05:58:08, FwB, Flags:.....C, B1=100, SSID=wifitest
3030	16.544794	0.450521	IntelCor_98:58:0F	Broadcast	802.11	328	69	-45	Probe Request, Src: 98:58:0F, FwB, Flags:.....C, SSID=wifitest
3031	16.544794	0.000000	Cisco_05:58:08	Broadcast	802.11	368	69	-38	Probe Response, Src: 05:58:08, FwB, Flags:.....C, B1=100, SSID=wifitest
3079	16.695429	0.151635	Cisco_05:58:08	Broadcast	802.11	364	69	-38	Beacon frame, Src: 05:58:08, FwB, Flags:.....C, B1=100, SSID=wifitest
3080	16.702455	0.005262	IntelCor_98:58:0F	Cisco_05:58:08	802.11	215	69	-46	Authentication, Src: 98:58:0F, FwB, Flags:.....C
3081	16.701542	0.000887	IntelCor_98:58:0F	IntelCor_98:58:0F	802.11	76	69	-39	Authentication, Src: 98:58:0F, FwB, Flags:.....C
3082	16.706278	0.004736	Cisco_05:58:08	IntelCor_98:58:0F	802.11	247	69	-38	Authentication, Src: 05:58:08, FwB, Flags:.....C
3083	16.706278	0.000000	IntelCor_98:58:0F	IntelCor_98:58:0F	802.11	76	69	-39	Authentication, Src: 98:58:0F, FwB, Flags:.....C
3084	16.706278	0.000000	IntelCor_98:58:0F	Cisco_05:58:08	802.11	372	69	-48	Association Request, Src: 98:58:0F, FwB, Flags:.....C, SSID=wifitest
3085	16.706278	0.000000	IntelCor_98:58:0F	IntelCor_98:58:0F	802.11	76	69	-38	Association Response, Src: 05:58:08, FwB, Flags:.....C
3086	16.718126	0.000262	Cisco_05:58:08	IntelCor_98:58:0F	802.11	413	69	-39	Association Response, Src: 05:58:08, FwB, Flags:.....C
3088	16.731216	0.000000	IntelCor_98:58:0F	IntelCor_98:58:0F	802.11	76	69	-41	Acknowledgment, Flags:.....C
3092	16.727450	0.000000	IntelCor_98:58:0F	IntelCor_98:58:0F	802.11	223	69	-59	I P, N(1)=15, N(2)=102; DSAP SNAP Group, SSAP Bnd Response
3092	16.727457	0.000188	IntelCor_98:58:0F	IntelCor_98:58:0F	802.11	76	69	-47	Acknowledgment, Flags:.....C
3095	16.748833	0.013376	IntelCor_98:58:0F	Broadcast	LLC	525	69	-59	U P, func=Unknown; DSAP Bnd Individual, SSAP Bnd Command
3095	16.748833	0.000000	IntelCor_98:58:0F	IntelCor_98:58:0F	802.11	76	69	-48	Action, Src: 98:58:0F, FwB, Flags:.....C
3099	16.742984	0.000000	IntelCor_98:58:0F	IntelCor_98:58:0F	802.11	183	69	-50	I P, N(1)=15, N(2)=102; DSAP SNAP Group, SSAP Bnd Command
3100	16.742984	0.000000	IntelCor_98:58:0F	IntelCor_98:58:0F	802.11	76	69	-53	Acknowledgment, Flags:.....C
3101	16.742984	0.000000	IntelCor_98:58:0F	IntelCor_98:58:0F	802.11	183	69	-50	I P, N(1)=15, N(2)=102; DSAP SNAP Group, SSAP Bnd Command
3102	16.742984	0.000000	IntelCor_98:58:0F	IntelCor_98:58:0F	802.11	76	69	-53	Acknowledgment, Flags:.....C
3106	16.748949	0.012522	IntelCor_98:58:0F	IPVencast_05:58:0F	LLC	223	69	-59	I P, N(1)=15, N(2)=102; DSAP Bnd Individual, SSAP Bnd Response
3107	16.748933	0.000124	IntelCor_98:58:0F	IntelCor_98:58:0F	802.11	76	69	-48	Acknowledgment, Flags:.....C
3109	16.774275	0.003842	Cisco_05:58:08	IntelCor_98:58:0F	802.11	118	69	-40	Action, Src: 05:58:08, FwB, Flags:.....C
3110	16.774275	0.000000	IntelCor_98:58:0F	IntelCor_98:58:0F	802.11	76	69	-52	Action, Src: 05:58:08, FwB, Flags:.....C
3113	16.773242	0.000000	IntelCor_98:58:0F	Broadcast	LLC	179	69	-59	I P, N(1)=15, N(2)=102; DSAP SNAP Group, SSAP 150 Network Layer
3114	16.773242	0.000000	IntelCor_98:58:0F	IntelCor_98:58:0F	802.11	76	69	-48	Acknowledgment, Flags:.....C
3115	16.773436	0.000262	IntelCor_98:58:0F	Cisco_05:58:08	802.11	118	69	-48	Action, Src: 05:58:08, FwB, Flags:.....C [Malformed Packet]
3116	16.773436	0.000000	IntelCor_98:58:0F	IntelCor_98:58:0F	802.11	76	69	-41	Acknowledgment, Flags:.....C
3120	16.779121	0.000000	IntelCor_98:58:0F	IntelCor_98:58:0F	802.11	223	69	-49	U, func=Unknown; DSAP Bnd Group, SSAP Bnd Command
3122	16.779545	0.001433	Cisco_05:58:08	IntelCor_98:58:0F	802.11	118	69	-47	Action, Src: 05:58:08, FwB, Flags:.....C
3123	16.779545	0.000000	IntelCor_98:58:0F	IntelCor_98:58:0F	802.11	76	69	-52	Action, Src: 05:58:08, FwB, Flags:.....C
3124	16.779599	0.000154	IntelCor_98:58:0F	IntelCor_98:58:0F	802.11	118	69	-48	Action, Src: 05:58:08, FwB, Flags:.....C [Malformed Packet: length
3125	16.779599	0.000000	IntelCor_98:58:0F	IntelCor_98:58:0F	802.11	76	69	-48	Acknowledgment, Flags:.....C
3128	16.781489	0.000000	IntelCor_98:58:0F	IntelCor_98:58:0F	LLC	197	69	-49	U P, func=Unknown; DSAP Bnd Individual, SSAP Bnd Command
3132	16.781489	0.000000	IntelCor_98:58:0F	IntelCor_98:58:0F	LLC	222	69	-58	U, func=Unknown; DSAP Bnd Group, SSAP Bnd Command
3133	16.781489	0.000000	IntelCor_98:58:0F	IntelCor_98:58:0F	802.11	76	69	-47	Acknowledgment, Flags:.....C
3134	16.790825	0.000000	IntelCor_98:58:0F	IntelCor_98:58:0F	802.11	223	69	-48	I P, N(1)=15, N(2)=102; DSAP Bnd Group, SSAP 150 Network Layer
3137	16.790815	0.000000	IntelCor_98:58:0F	IntelCor_98:58:0F	802.11	76	69	-47	Acknowledgment, Flags:.....C
3140	16.793447	0.002599	IntelCor_98:58:0F	Broadcast	LLC	525	69	-58	I, N(1)=8, N(2)=22; DSAP HP Extended LLC Group, SSAP NetWare
3141	16.793447	0.000000	IntelCor_98:58:0F	IntelCor_98:58:0F	802.11	76	69	-47	Acknowledgment, Flags:.....C
3144	16.791774	0.000000	IntelCor_98:58:0F	Broadcast	LLC	179	69	-58	U, func=Unknown; DSAP Bnd Individual, SSAP Bnd Response
3145	16.793849	0.000000	IntelCor_98:58:0F	IntelCor_98:58:0F	802.11	76	69	-48	Acknowledgment, Flags:.....C
3149	16.794563	0.000714	IntelCor_98:58:0F	IPVencast_05:58:0F	LLC	183	69	-58	I P, N(1)=15, N(2)=102; DSAP Bnd Group, SSAP Bnd Response
3150	16.794563	0.000000	IntelCor_98:58:0F	IntelCor_98:58:0F	802.11	76	69	-48	Acknowledgment, Flags:.....C
3154	16.794928	0.000000	IntelCor_98:58:0F	IPVencast_05:58:0F	LLC	202	69	-58	I P, N(1)=15, N(2)=102; DSAP Bnd Group, SSAP Bnd Response
3155	16.794909	0.000000	IntelCor_98:58:0F	IntelCor_98:58:0F	802.11	76	69	-48	Acknowledgment, Flags:.....C
3158	16.795624	0.000624	IntelCor_98:58:0F	IPVencast_05:58:0F	LLC	215	69	-58	U P, func=Unknown; DSAP MAL LSAP Individual, SSAP Banyan View
3230	16.795959	0.000000	IntelCor_98:58:0F	IntelCor_98:58:0F	802.11	76	69	-48	Acknowledgment, Flags:.....C
3240	16.795985	0.000000	IntelCor_98:58:0F	IPVencast_05:58:0F	LLC	215	69	-58	U, func=Unknown; DSAP Bnd Group, SSAP Bnd Response
3242	16.795852	0.000000	IntelCor_98:58:0F	IntelCor_98:58:0F	802.11	76	69	-48	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	wifetest	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: [wlc0-9800-01], Model: [C9800-CL-93], Version: [17.0.0.0], SW: [S9158H1805], MD_SW: [S9158H1805]
2023/08/04 14:22:59.31503237 [wlc_m_0-0] (1) | [client-orch-wm] (15210): (note) MAC: 286b.3598.580f Re-Association received. BSSID 00d1.1dd4.7d38, WLAN wifetest, Slot 3 AP 00d1.1dd4.7d38, AP136_SC_F524, old BSSID 00d1.1dd4.a018
2023/08/04 14:22:59.31504120 [wlc_m_0-0] (1) | [dot11] (15210): (note) MAC: 286b.3598.580f Association success. AID 33, Roaming = TRUE, WGB = False, l1r = True, l1w = True Fast Roam = TRUE
2023/08/04 14:22:59.3164693183 [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 14:22:59.317320574 [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 14:22:59.321042987 [wlc_m_0-0] (1) | [client-orch-wm] (15210): (note) MAC: 286b.3598.580f Mobility discovery triggered. Client mode: Local
2023/08/04 14:22:59.321046390 [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 Op: 0x0
2023/08/04 14:22:59.32113992 [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 14:22:59.32125052 [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 14:22:59.321466400 [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_AUTH_IN_PROGRESS
2023/08/04 14:24:27.518955521 [wlc_m_0-0] (1) | [client-orch-wm] (15210): (note) MAC: 286b.3598.580f Re-Association received. BSSID 00d1.1dd4.a018, WLAN wifetest, Slot 3 AP 00d1.1dd4.a018, AP01_RC_9136_F80C, old BSSID 00d1.1dd4.7d38
2023/08/04 14:24:27.519397444 [wlc_m_0-0] (1) | [dot11] (15210): (note) MAC: 286b.3598.580f Association success. AID 33, Roaming = TRUE, WGB = False, l1r = True, l1w = True Fast Roam = TRUE
2023/08/04 14:24:27.521929223 [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 14:24:27.522774647 [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_L2_AUTH_IN_PROGRESS
2023/08/04 14:24:27.528409164 [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 14:24:27.531501971 [wlc_m_0-0] (1) | [client-orch-wm] (15210): (note) MAC: 286b.3598.580f Mobility discovery triggered. Client mode: Local
2023/08/04 14:24:27.531511962 [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 14:24:27.531649992 [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 Op: 0x0
2023/08/04 14:24:27.531841935 [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 14:24:27.531913122 [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 14:24:27.533100190 [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 14:24:27.533811101 [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_DONE

```

NetGear A8000

WPA3-Enterprise is not supported on this client.

Pixel 6a

Connection OTA with focus on the RSN information for client:

The image shows a Wireshark packet capture of an IEEE 802.11r roaming process. The left pane displays a list of captured frames (No., Time, Delta, Source, Destination, Protocol, Length, Channel, Signal strength, Info). The right pane shows the details of the selected frames. Key frames include:

- Frame 1205: IEEE 802.11 Authentication. The details pane shows "Authentication, Seq=4, Fw=, Flags=...".
- Frame 1206: IEEE 802.11 Key Management. The details pane shows "Auth Key Management (AKM) Suite: FT over IEEE 802.11", "Auth Key Management (AKM) type: FT over IEEE 802.11 (1)", "Management Frame Protection Capable: True", and "Per Key Enabled: false".

WPA3 Enterprise 802.1x + FT Pixel6a Association

Client details in WLC:

The screenshot shows the 'Client' configuration page on a Cisco Catalyst 9800-CL Wireless Controller. The 'Security Information' tab is active. The configuration includes:

- Re-authentication Timeout: 1800 sec (Remaining time: 267 sec)
- Client State Servers: None
- Client ACLs: None
- Client Entry Create Time: 1536 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 Pixel6a Client details

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

The screenshot shows the 'Client' configuration page with the 'Mobility History' tab selected. The 'Recent association history' table displays the following data:

AP Name	BSSID	AP Slot	Assoc. Time	Instance	Mobility Role	Run Latency (m)	Roam Type
AP01_RC_9136_F80C	00d1.10da.a018	3	07/12/2023 11:46:16	0	Local	7	802.11R
AP9136_SC_F524	00d1.10da.7d38	3	07/12/2023 11:43:48	0	Local	3161	N/A

Samsung S23

Connection OTA with focus on the RSN information from client:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
1246	8.295985	0.182133	Cisco_dfi:80:18	Broadcast	802.11	364	69	-39	dBm Beacon frame, SN=385, Fw=0, Flags=.....C, B1=100, SSID="wdf"
1247	8.401935	0.182170	Cisco_dfi:80:18	Broadcast	802.11	364	69	-40	dBm Beacon frame, SN=386, Fw=0, Flags=.....C, B1=100, SSID="wdf"
1248	8.504375	0.182420	Cisco_dfi:80:18	Broadcast	802.11	364	69	-39	dBm Beacon frame, SN=387, Fw=0, Flags=.....C, B1=100, SSID="wdf"
1249	8.606824	0.182419	Cisco_dfi:80:18	Broadcast	802.11	364	69	-40	dBm Beacon frame, SN=388, Fw=0, Flags=.....C, B1=100, SSID="wdf"
1251	8.612759	0.005945	Cisco_dfi:80:18	Broadcast	802.11	312	69	-40	dBm Probe Response, SN=459, Fw=0, Flags=.....C, B1=100, SSID="wdf"
1258	8.701133	0.096374	Cisco_dfi:80:18	Broadcast	802.11	364	69	-39	dBm Beacon frame, SN=310, Fw=0, Flags=.....C, B1=100, SSID="wdf"
1260	8.786422	0.077279	Samsung_c9:e3:71	Cisco_dfi:80:18	802.11	235	69	-48	dBm Authentication, SN=99, Fw=0, Flags=.....C
1261	8.786422	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-39	dBm Acknowledgment, Flags=.....C
1262	8.790571	0.004159	Cisco_dfi:80:18	Samsung_c9:e3:71	802.11	247	69	-39	dBm Authentication, SN=118, Fw=0, Flags=.....C
1263	8.790571	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-47	dBm Acknowledgment, Flags=.....C
1265	8.796439	0.005968	Samsung_c9:e3:71	Cisco_dfi:80:18	802.11	485	69	-48	dBm Reassociation Request, SN=100, Fw=0, Flags=.....C, SSID="wdf"
1266	8.796439	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-39	dBm Acknowledgment, Flags=.....C
1268	8.800780	0.006939	Samsung_c9:e3:71	Broadcast	LLC	114	69	-39	dBm S, Func=02, N(0)=19; DSAP 0x0a Group, SSAP 0x0a Command
1269	8.800780	0.001362	Cisco_dfi:80:18	Samsung_c9:e3:71	802.11	413	69	-39	dBm Reassociation Response, SN=0, Fw=0, Flags=.....C
1270	8.800780	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-48	dBm Acknowledgment, Flags=.....C
1271	8.807940	0.000000	Samsung_c9:e3:71	Broadcast	LLC	120	69	-39	dBm I, P, N(0)=11, N(5)=19; DSAP 0x0a Individual, SSAP 0x0a Response
1272	8.813121	0.001581	Cisco_dfi:80:18	Broadcast	802.11	364	69	-39	dBm Beacon frame, SN=311, Fw=0, Flags=.....C, B1=100, SSID="wdf"
1273	8.832754	0.012133	Cisco_Sc:F8:0c	Samsung_c9:e3:71	LLC	183	69	-40	dBm U, Func=02C; DSAP 0x0a Group, SSAP 0x0a Command
1274	8.832754	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-58	dBm Acknowledgment, Flags=.....C
1275	8.832754	0.000000	Cisco_Sc:F8:0c	Samsung_c9:e3:71	LLC	183	69	-49	dBm U, Func=unknown; DSAP Texas Instruments Group, SSAP 0x28 Response
1276	8.832817	0.000063	192.168.1.15	192.168.1.121	802.11	76	69	-58	dBm Acknowledgment, Flags=.....C
1277	8.800540	0.007723	Samsung_c9:e3:71	Broadcast	LLC	144	69	-40	dBm S, Func=02, N(0)=12; DSAP 0x0a Individual, SSAP 0x0a Response
1278	8.800540	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-40	dBm Acknowledgment, Flags=.....C
1280	8.804143	0.003063	Cisco_dfi:80:18	Samsung_c9:e3:71	802.11	118	69	-47	dBm Action, SN=1, Fw=0, Flags=p.....C
1281	8.804143	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-47	dBm Acknowledgment, Flags=.....C
1282	8.804803	0.000660	Samsung_c9:e3:71	Cisco_dfi:80:18	802.11	115	69	-47	dBm Action, SN=0, Fw=0, Flags=p.....C
1283	8.804803	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-40	dBm Acknowledgment, Flags=.....C
1284	8.806878	0.002075	Altiocel_a36:59:af	Samsung_c9:e3:71	LLC	197	69	-50	dBm I, P, N(0)=25, N(5)=40; DSAP 0x0a Individual, SSAP 0x0a Command
1286	8.913912	0.007034	Cisco_dfi:80:18	Broadcast	802.11	364	69	-41	dBm Beacon frame, SN=313, Fw=0, Flags=.....C, B1=100, SSID="wdf"
1287	8.950493	0.036381	Cisco_dfi:80:18	Broadcast	802.11	364	69	-39	dBm Acknowledgment, Flags=.....C
1322	8.975553	0.029008	192.168.1.15	192.168.1.121	802.11	76	69	-39	dBm Acknowledgment, Flags=.....C
1372	9.051519	0.040566	Cisco_dfi:80:18	Broadcast	802.11	364	69	-38	dBm Beacon frame, SN=314, Fw=0, Flags=.....C, B1=100, SSID="wdf"
1471	9.118083	0.102164	Cisco_dfi:80:18	Broadcast	802.11	364	69	-39	dBm Beacon frame, SN=315, Fw=0, Flags=.....C, B1=100, SSID="wdf"
1600	9.176834	0.058111	192.168.1.15	192.168.1.121	802.11	76	69	-40	dBm Acknowledgment, Flags=.....C
1702	9.221145	0.044131	Cisco_dfi:80:18	Broadcast	802.11	364	69	-39	dBm Beacon frame, SN=316, Fw=0, Flags=.....C, B1=100, SSID="wdf"
1933	9.124387	0.102962	Cisco_dfi:80:18	Broadcast	802.11	364	69	-39	dBm Beacon frame, SN=317, Fw=0, Flags=.....C, B1=100, SSID="wdf"
1937	9.425938	0.148312	Cisco_dfi:80:18	Broadcast	802.11	364	69	-40	dBm Beacon frame, SN=318, Fw=0, Flags=.....C, B1=100, SSID="wdf"
1939	9.528463	0.102525	Cisco_dfi:80:18	Broadcast	802.11	364	69	-38	dBm Beacon frame, SN=319, Fw=0, Flags=.....C, B1=100, SSID="wdf"
1945	9.631020	0.102557	Cisco_dfi:80:18	Broadcast	802.11	364	69	-38	dBm Beacon frame, SN=320, Fw=0, Flags=.....C, B1=100, SSID="wdf"
1946	9.731295	0.102275	Cisco_dfi:80:18	Broadcast	802.11	364	69	-39	dBm Beacon frame, SN=321, Fw=0, Flags=.....C, B1=100, SSID="wdf"
1950	9.835864	0.102569	Cisco_dfi:80:18	Broadcast	802.11	364	69	-40	dBm Beacon frame, SN=322, Fw=0, Flags=.....C, B1=100, SSID="wdf"
1951	9.925936	0.000072	Samsung_c9:e3:71	Cisco_dfi:80:18	802.11	122	69	-45	dBm Action, SN=0, Fw=0, Flags=p.....C
1952	9.925936	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-40	dBm Acknowledgment, Flags=.....C
1953	9.926093	0.000057	192.168.1.15	192.168.1.121	802.11	76	69	-40	dBm Acknowledgment, Flags=.....C
1954	9.931705	0.011002	Cisco_dfi:80:18	Broadcast	802.11	364	69	-40	dBm Beacon frame, SN=323, Fw=0, Flags=.....C, B1=100, SSID="wdf"
1955	9.942143	0.006448	192.168.1.15	192.168.1.121	802.11	76	69	-40	dBm Acknowledgment, Flags=.....C

```

> Frame 1265: 485 bytes on wire (3880 bits), 485 bytes captured (3880 bits) on interface Device\MPF_{D4578095-2}
> Ethernet II, Src: Cisco_G2:97:47 (74:11:b2:97:47), Dst: Universa_07:cf:06 (08:0a:8b:07:cf:06)
> Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.121
> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
> AiroPcap/OnixPcap encapsulated IEEE 802.11
> IEEE 802.11 radio information
> IEEE 802.11 Reassociation Request, Flags: .....C
> IEEE 802.11 Key Management
  > Fixed parameters (30 bytes)
  > Tagged parameters (185 bytes)
    > Tag: SSID parameter set: "wdf16_test"
    > Tag: Supported Rates A(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: Power Capability M(n), 8; Max: 16
    > Tag: Supported Channels
    > Tag: RM Enabled Capabilities (5 octets)
  > Tag: DSM Information
  > Tag: Mobility Domain
    > Tag Number: Mobility Domain (54)
    > Tag Length: 3
    > Mobility Domain Identifier: 0xe2f2
  > FT Capability and Policy: 0x01
    > ..... = FAST BSS Transition over DS: 0x1
    > ..... = Resource Request Protocol Capability: 0x0
    > 0x00 0x00 = Reserved: 0x00
  > Tag: Fast BSS Transition
    > Tag Number: Fast BSS Transition (55)
    > Tag Length: 96
    > MDC Control: 0x0000
    > MDC: @#124d7f4e16ad4ecf658a5a1adaca
    > Address: d514f417ab7fa005b7673e1b0d0a0822fac50fb3f492e10809b1a809ca
    > Domain: 08122a55c78aa18c4ef412424259708790fccefa12283f566d00b2c3
  > Subelement: PMK-R1 key holder Identifier (R104-ID)
    > Length: 6
    > PMK-R1 key holder Identifier (R104-ID): d68070d97ad0
  > Subelement: PMK-R0 key holder Identifier (R004-ID)
    > Length: 4
    > PMK-R0 key holder Identifier (R004-ID): 002055a2
  > Tag: Supported Operating Classes
  > Tag: Extended Capabilities (13 octets)
  > Ext Tag: Vendor-Specific: Microsoft Corp.: WPA/WPA2 Information Element
  > Ext Tag: HE Capabilities
  > Ext Tag: HE 6 GHz Band Capabilities
  > Tag: Vendor-Specific: Qualcomm Inc.
  > Tag: Vendor-Specific: Samsung Electronics Co., Ltd
  > Tag: Vendor-Specific: Samsung Electronics Co., Ltd

```

S23 Roaming FTODS packets

WPA3-Enterprise + GCMP128 cipher + SUITEB-1X

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	<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	Info
37376	59.189776	0.820482	Cisco_06:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2002, Fw=0, Flags=.....C, B=100, SSID=...	
37385	59.190516	0.820498	Cisco_06:00:18	Broadcast	802.11	312	69 -47 dbm	Probe Response, SW=2003, Fw=0, Flags=.....C, B=100, SSID=...	
37396	59.191709	0.820483	Cisco_06:00:18	Broadcast	802.11	355	69 -47 dbm	Beacon frame, SW=2004, Fw=0, Flags=.....C, B=100, SSID=...	
37414	59.192161	0.820462	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2005, Fw=0, Flags=.....C, B=100, SSID=...	
37424	59.192713	0.820472	Cisco_06:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2006, Fw=0, Flags=.....C, B=100, SSID=...	
37437	59.192759	0.820437	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2007, Fw=0, Flags=.....C, B=100, SSID=...	
37447	59.192792	0.820442	Cisco_06:00:18	Broadcast	802.11	312	69 -47 dbm	Probe Response, SW=2008, Fw=0, Flags=.....C, B=100, SSID=...	
37459	59.193134	0.820522	Cisco_06:00:18	Broadcast	802.11	355	69 -38 dbm	Beacon frame, SW=2009, Fw=0, Flags=.....C, B=100, SSID=...	
37470	59.193629	0.820399	Cisco_06:00:18	Broadcast	802.11	312	69 -39 dbm	Probe Response, SW=2010, Fw=0, Flags=.....C, B=100, SSID=...	
37480	59.194345	0.820463	Cisco_06:00:18	Broadcast	802.11	312	69 -47 dbm	Probe Response, SW=2011, Fw=0, Flags=.....C, B=100, SSID=...	
37489	59.194687	0.821342	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2012, Fw=0, Flags=.....C, B=100, SSID=...	
37499	59.195116	0.821929	Cisco_06:00:18	Broadcast	802.11	312	69 -37 dbm	Probe Response, SW=2013, Fw=0, Flags=.....C, B=100, SSID=...	
37520	59.195713	0.820817	Cisco_06:00:18	Broadcast	802.11	355	69 -37 dbm	Beacon frame, SW=2014, Fw=0, Flags=.....C, B=100, SSID=...	
37529	59.195889	0.820347	Cisco_06:00:18	Broadcast	802.11	312	69 -47 dbm	Probe Response, SW=2015, Fw=0, Flags=.....C, B=100, SSID=...	
37532	59.195726	0.821156	Cisco_06:00:18	Broadcast	802.11	312	69 -47 dbm	Probe Response, SW=2016, Fw=0, Flags=.....C, B=100, SSID=...	
37539	59.197089	0.821751	Cisco_06:00:18	Broadcast	802.11	312	69 -37 dbm	Probe Response, SW=2017, Fw=0, Flags=.....C, B=100, SSID=...	
37552	59.197468	0.820499	Cisco_06:00:18	Broadcast	802.11	312	69 -47 dbm	Probe Response, SW=2018, Fw=0, Flags=.....C, B=100, SSID=...	
37565	59.197993	0.820545	Cisco_06:00:18	Broadcast	802.11	355	69 -47 dbm	Beacon frame, SW=2019, Fw=0, Flags=.....C, B=100, SSID=...	
37574	59.198423	0.820438	Cisco_06:00:18	Broadcast	802.11	312	69 -47 dbm	Probe Response, SW=2020, Fw=0, Flags=.....C, B=100, SSID=...	
37585	59.198865	0.820542	Cisco_06:00:18	Broadcast	802.11	312	69 -47 dbm	Probe Response, SW=2021, Fw=0, Flags=.....C, B=100, SSID=...	
37596	59.199439	0.820476	Cisco_06:00:18	Broadcast	802.11	312	69 -47 dbm	Probe Response, SW=2022, Fw=0, Flags=.....C, B=100, SSID=...	
37616	59.199949	0.820995	Cisco_06:00:18	Broadcast	802.11	312	69 -47 dbm	Probe Response, SW=2023, Fw=0, Flags=.....C, B=100, SSID=...	
37628	59.200621	0.820481	Cisco_06:00:18	Broadcast	802.11	355	69 -38 dbm	Beacon frame, SW=2024, Fw=0, Flags=.....C, B=100, SSID=...	
37641	59.200984	0.820961	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2025, Fw=0, Flags=.....C, B=100, SSID=...	
37652	59.201317	0.820351	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2026, Fw=0, Flags=.....C, B=100, SSID=...	
37668	59.201765	0.820428	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2027, Fw=0, Flags=.....C, B=100, SSID=...	
37687	59.202467	0.820792	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2028, Fw=0, Flags=.....C, B=100, SSID=...	
37696	59.202867	0.820480	Cisco_06:00:18	Broadcast	802.11	355	69 -38 dbm	Beacon frame, SW=2029, Fw=0, Flags=.....C, B=100, SSID=...	
37704	59.203477	0.820430	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2030, Fw=0, Flags=.....C, B=100, SSID=...	
37719	59.203721	0.820241	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2031, Fw=0, Flags=.....C, B=100, SSID=...	
37719	59.204549	0.820628	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2032, Fw=0, Flags=.....C, B=100, SSID=...	
37738	59.204659	0.820120	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2033, Fw=0, Flags=.....C, B=100, SSID=...	
37749	59.205208	0.820495	Cisco_06:00:18	Broadcast	802.11	355	69 -38 dbm	Beacon frame, SW=2034, Fw=0, Flags=.....C, B=100, SSID=...	
37775	59.205621	0.820392	Cisco_06:00:18	Broadcast	802.11	312	69 -47 dbm	Probe Response, SW=2035, Fw=0, Flags=.....C, B=100, SSID=...	
37792	59.206121	0.820508	Cisco_06:00:18	Broadcast	802.11	312	69 -47 dbm	Probe Response, SW=2036, Fw=0, Flags=.....C, B=100, SSID=...	
37809	59.207002	0.821581	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2037, Fw=0, Flags=.....C, B=100, SSID=...	
37814	59.207213	0.821751	Cisco_06:00:18	Broadcast	802.11	312	69 -47 dbm	Probe Response, SW=2038, Fw=0, Flags=.....C, B=100, SSID=...	
37822	59.207660	0.820428	Cisco_06:00:18	Broadcast	802.11	355	69 -38 dbm	Beacon frame, SW=2039, Fw=0, Flags=.....C, B=100, SSID=...	
37833	59.208050	0.820398	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2040, Fw=0, Flags=.....C, B=100, SSID=...	
37841	59.208540	0.820490	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2041, Fw=0, Flags=.....C, B=100, SSID=...	
37857	59.209090	0.820590	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2042, Fw=0, Flags=.....C, B=100, SSID=...	
37864	08.013062	0.820480	Cisco_06:00:18	Broadcast	802.11	312	69 -47 dbm	Probe Response, SW=2043, Fw=0, Flags=.....C, B=100, SSID=...	
37868	08.013192	0.820508	Cisco_06:00:18	Broadcast	802.11	355	69 -38 dbm	Beacon frame, SW=2044, Fw=0, Flags=.....C, B=100, SSID=...	
37881	08.013489	0.820297	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2045, Fw=0, Flags=.....C, B=100, SSID=...	
37887	08.013787	0.820568	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2046, Fw=0, Flags=.....C, B=100, SSID=...	
37897	08.014006	0.820839	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2047, Fw=0, Flags=.....C, B=100, SSID=...	
37908	08.112976	0.820888	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2048, Fw=0, Flags=.....C, B=100, SSID=...	
37927	08.124244	0.820438	Cisco_06:00:18	Broadcast	802.11	355	69 -37 dbm	Beacon frame, SW=2049, Fw=0, Flags=.....C, B=100, SSID=...	
37928	08.125087	0.820813	Cisco_06:00:18	Broadcast	802.11	312	69 -47 dbm	Probe Response, SW=2050, Fw=0, Flags=.....C, B=100, SSID=...	
37936	08.173134	0.820267	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2051, Fw=0, Flags=.....C, B=100, SSID=...	
37943	08.193778	0.820464	Cisco_06:00:18	Broadcast	802.11	312	69 -47 dbm	Probe Response, SW=2052, Fw=0, Flags=.....C, B=100, SSID=...	
37949	08.124389	0.820593	Cisco_06:00:18	Broadcast	802.11	312	69 -47 dbm	Probe Response, SW=2053, Fw=0, Flags=.....C, B=100, SSID=...	
37961	08.124873	0.820598	Cisco_06:00:18	Broadcast	802.11	355	69 -47 dbm	Beacon frame, SW=2054, Fw=0, Flags=.....C, B=100, SSID=...	

```

> frame 37628: 355 bytes on wire (2840 bits), 355 bytes captured (2840 bits) on interface \Device\NPF_{04576965-2998-4456-8C13-C4}
> Ethernet II, Src: Cisco_02:00:07:00:18:12, Dst: Unknown_07:0c:60:00:00:00 (08:00:00:07:0c:60)
> Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.121
> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
> AlohaPdu/OnlinkPdu encapsulated IEEE 802.11
> IEEE 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: .....C
IEEE 802.11 Wireless Management
> Fixed parameters (12 bytes)
> Tagged parameters (213 bytes)
  > Tag: SSID parameter set: "wifi168_test"
  > Tag: Supported Rates (6(B), 9, 12(0), 18, 24(0), 36, 48, 54, [Mbit/sec])
  > Tag: Traffic Indication Map (TIM): OPM # of 1 bitmap
  > Tag: Country Information: Country Code not set, Environment Global operating classes
  > Tag: Power Constraint: 6
  > Tag: TX Report Transmit Power: 36, Link Operat: 0
  > Tag: RSN Information
    > Tag Number: RSN Information (64)
    > Tag Length: 36
    > RSN Version: 1
    > Group Cipher Suite: 00000000: 00000000 (IEEE 802.11) GCM (128)
    > Pairwise Cipher Suite Count: 1
    > Pairwise Cipher Suite List 00000000: 00000000 (IEEE 802.11) GCM (128)
    > Auth Key Management (AKM) Suite Count: 1
    > Auth Key Management (AKM) List 00000000: 00000000 (IEEE 802.11) WPA (SHA256-SuiteB)
    > Auth Key Management (AKM) OUI: 00000000: 00000000 (IEEE 802.11)
    > Auth Key Management (AKM) Type: WPA (SHA256-SuiteB) (11)
  > RSN Capabilities: 000000
  > PMKID Count: 0
  > PMKID List
  > Group Management Cipher Suite: 00000000: 00000000 (IEEE 802.11) BIP (GCM-128)
  > Tag: QoS Class of Service: IEEE 802.11e version
  > Tag: WMM Enabled Capabilities (5 octets)
  > Tag: Extended Capabilities (11 octets)
  > Tag: TX Power Envelope
  > Tag: TX Power Envelope
  > Ext Tag: Multiple BSSID Configuration
  > Ext Tag: HE Capabilities
  > Ext Tag: HE Operation
  > Ext Tag: Spatial Reuse Parameter Set
  > Ext Tag: HE SIFID Parameter Set
  > Ext Tag: HE 4 GHz Band Capabilities
  > Tag: Vendor Specific: Atheros Communications, Inc.: Unknown
  > Tag: Vendor Specific: Microsoft Corp.: WPA/WPA2 Parameter Element
  > Tag: Vendor Specific: Cisco Systems, Inc.: Airont Client MFP Disabled
  > Tag: Vendor Specific: Cisco Systems, Inc.: Airont CCK version = 5
  > Tag: Vendor Specific: Cisco Systems, Inc.: Airont Unknown (64)
  > Tag: Vendor Specific: Cisco Systems, Inc.: Airont Unknown (11) (11)

```

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

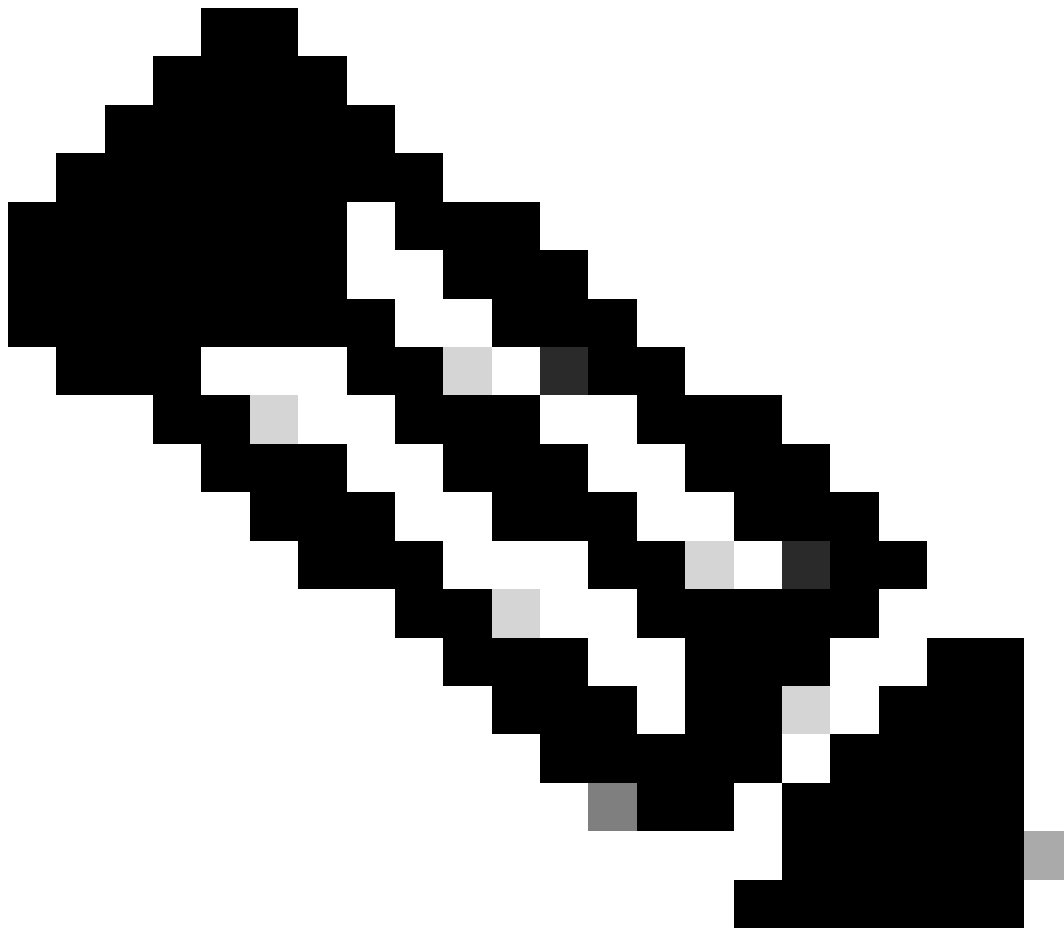
The troubleshooting used in this document was based on the online document:

[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](#)