

# Konfiguration und Überprüfung der Layer-2-Sicherheit des Wi-Fi 6E-WLAN

## Inhalt

---

### [Einleitung](#)

### [Voraussetzungen](#)

#### [Anforderungen](#)

#### [Verwendete Komponenten](#)

### [Hintergrundinformationen](#)

#### [Wi-Fi 6E-Sicherheit](#)

##### [WPA3](#)

##### [Stufensatz: WPA3-Modi](#)

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

##### [Von Clients unterstützte Sicherheitseinstellungen](#)

### [Konfigurieren](#)

#### [Netzwerkdiagramm](#)

#### [Konfigurationen](#)

##### [Basiskonfiguration](#)

### [Überprüfung](#)

#### [Sicherheitsüberprüfung](#)

##### [WPA3 - AES \(CCPM128\) + SCHULDENSTÜCK](#)

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

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

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

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

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

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

##### [Sicherheitsschlussfolgerungen](#)

### [Fehlerbehebung](#)

### [Zugehörige Informationen](#)

---

## Einleitung

In diesem Dokument wird beschrieben, wie Sie die Layer-2-Sicherheit des Wi-Fi 6E-WLAN konfigurieren und was Sie von verschiedenen Clients erwarten können.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Wireless LAN Controller (WLC) 9800
- Cisco Access Points (APs), die Wi-Fi 6E unterstützen.
- IEEE-Standard 802.11ax
- Tools: Wireshark v4.0.6

## Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- WLC 9800-CL mit IOS® XE 17.9.3
- APs: C9136, CW9162, CW9164 und CW9166.
- Wi-Fi 6E-Clients:
  - Lenovo X1 Carbon Gen11 mit Intel AX211 Wi-Fi 6 und 6E Adapter mit Treiberversion 22.200.2(1).
  - Netgear A8000 Wi-Fi 6 und 6E Adapter mit Treiber v1(0.0.108)
  - Mobiltelefon Pixel 6a mit Android 13;
  - Handy Samsung S23 mit Android 13.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Hintergrundinformationen

Das Wichtigste ist, dass Wi-Fi 6E kein völlig neuer Standard ist, sondern eine Erweiterung. Als Basis dient Wi-Fi 6E als Erweiterung des Wireless-Standards Wi-Fi 6 (802.11ax) in das 6-GHz-Frequenzband.

Wi-Fi 6E basiert auf Wi-Fi 6, der neuesten Generation des Wi-Fi-Standards, aber nur Wi-Fi 6E-Geräte und -Anwendungen können im 6-GHz-Band betrieben werden.

### Wi-Fi 6E-Sicherheit

Wi-Fi 6E erhöht die Sicherheit mit Wi-Fi Protected Access 3 (WPA3) und Opportunistic Wireless Encryption (OWE), und es gibt keine Abwärtskompatibilität mit Open- und WPA2-Sicherheit.

WPA3 und Enhanced Open Security sind jetzt für die Wi-Fi 6E-Zertifizierung obligatorisch, und für Wi-Fi 6E ist auch Protected Management Frame (PMF) sowohl auf dem Access Point als auch auf den Clients erforderlich.

Bei der Konfiguration einer 6-GHz-SSID müssen bestimmte Sicherheitsanforderungen erfüllt werden:

- WPA3 L2-Sicherheit mit OWE, SAE oder 802.1x-SHA256
- Geschützter Management-Frame aktiviert;

- Andere L2-Sicherheitsmethoden sind nicht zulässig, d. h., es ist kein gemischter Modus möglich.

## WPA3

WPA3 wurde entwickelt, um die Wi-Fi-Sicherheit zu verbessern, indem eine bessere Authentifizierung über WPA2 ermöglicht wird, wodurch die kryptografische Stärke erweitert und die Ausfallsicherheit kritischer Netzwerke erhöht wird.

WPA3 zeichnet sich durch folgende Hauptfunktionen aus:

- Protected Management Frame (PMF) schützt Unicast- und Broadcast-Management-Frames und verschlüsselt Unicast-Management-Frames. Wireless Intrusion Detection- und Wireless Intrusion Prevention-Systeme bieten daher weniger Möglichkeiten zur Brute-Force-Durchsetzung von Client-Richtlinien.
- Simultaneous Authentication of Equals (SAE) ermöglicht eine kennwortbasierte Authentifizierung und einen Key Agreement-Mechanismus. Dies schützt vor Brute-Force-Angriffen.
- Der Übergangsmodus ist ein gemischter Modus, der die Verwendung von WPA2 ermöglicht, um Clients zu verbinden, die WPA3 nicht unterstützen.

Bei WPA3 geht es um kontinuierliche Sicherheitsentwicklung, Konformität und Interoperabilität. Es gibt kein Informationselement, das WPA3 (identisch mit WPA2) bezeichnet. WPA3 wird durch AKM/Cipher Suite/PMF-Kombinationen definiert.

Für die WLAN-Konfiguration des 9800 stehen vier verschiedene WPA3-Verschlüsselungsalgorithmen zur Verfügung.

Sie basieren auf Galois/Counter Mode Protocol (GCMP) und Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP): AES (CCMP128), CCMP256, GCMP128 und GCMP256:

### WPA2/WPA3 Encryption

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

WPA2/3-Verschlüsselungsoptionen

## PMF

PMF wird in einem WLAN aktiviert, wenn Sie PMF aktivieren.

Standardmäßig sind 802.11-Management-Frames nicht authentifiziert und daher nicht vor

Spoofing geschützt. Infrastructure Management Protection Frame (MFP) und 802.11w Protected Management Frames (PMF) bieten Schutz vor solchen Angriffen.

### Protected Management Frame

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

PMF-Optionen

Verwaltung von Authentifizierungsschlüsseln

Folgende AKM-Optionen sind in der Version 17.9.x verfügbar:



## 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\*

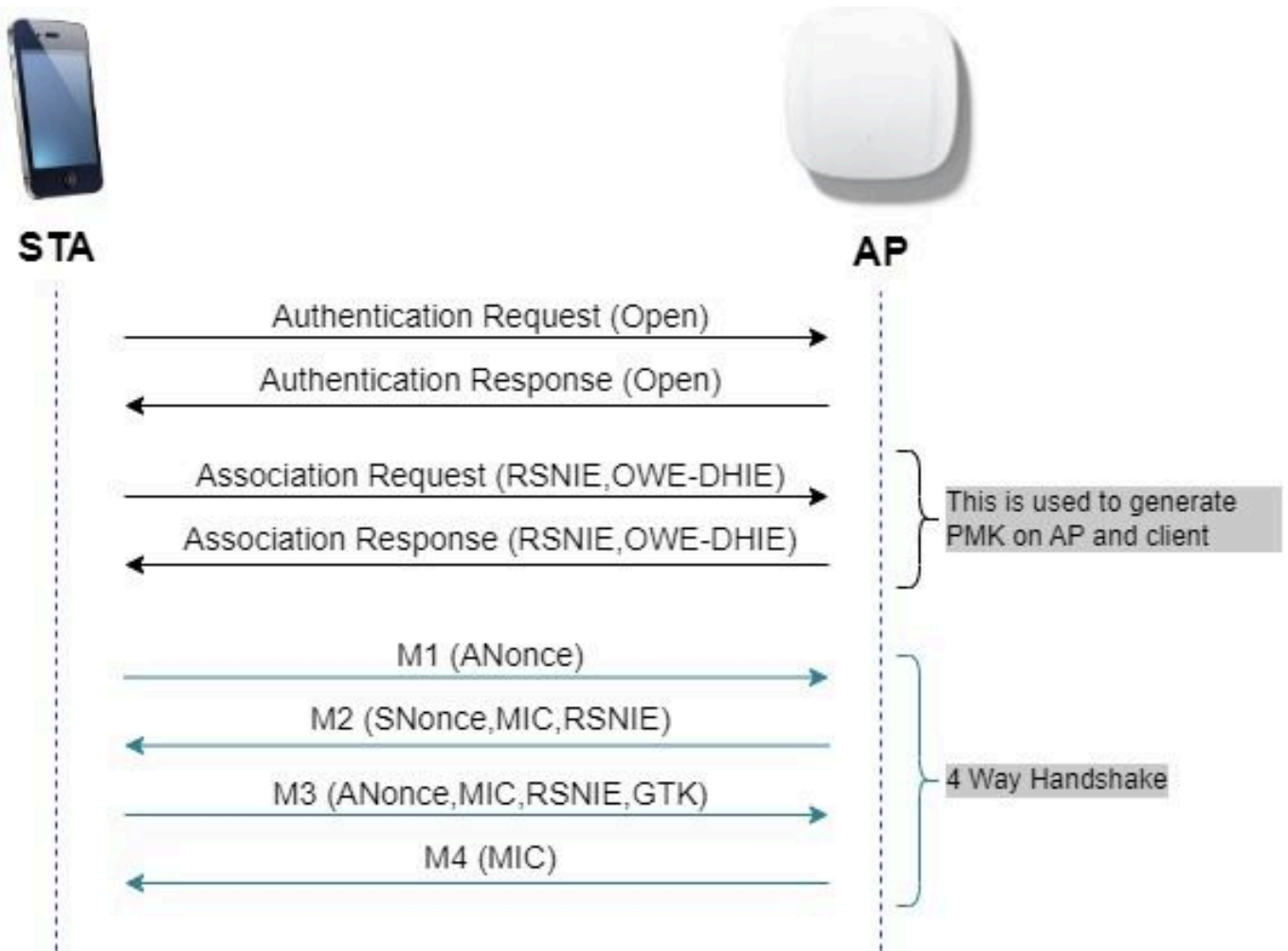
SAE Password Element ⓘ

AKM-Optionen

SCHULD

Opportunistic Wireless Encryption (OWE) ist eine Erweiterung von IEEE 802.11 für die Verschlüsselung des Wireless-Mediums ([IETF RFC 8110](#)). Der Zweck der OWE-basierten Authentifizierung besteht in der Vermeidung offener, ungesicherter Wireless-Verbindungen zwischen den APs und Clients. Der OWE verwendet die auf dem Diffie-Hellman-Algorithmus basierende Verschlüsselung, um die Wireless-Verschlüsselung einzurichten. Mit OWE führen der Client und AP während des Zugriffsvorgangs einen Diffie-Hellman-Schlüsselaustausch durch und

verwenden den resultierenden paarweisen Master Key (PMK)-Schlüssel mit dem 4-Wege-Handshake. Die Verwendung von OWE erhöht die Sicherheit von Wireless-Netzwerken in Bereitstellungen, in denen offene oder gemeinsam genutzte PSK-basierte Netzwerke bereitgestellt werden.



OWE-Frame-Austausch

## SAE

WPA3 verwendet einen neuen Authentifizierungs- und Schlüsselverwaltungsmechanismus, der als Simultane Authentifizierung von Equals bezeichnet wird. Dieser Mechanismus wird durch den Einsatz von SAE Hash-to-Element (H2E) weiter verbessert.

SAE mit H2E ist für WPA3 und Wi-Fi 6E obligatorisch.

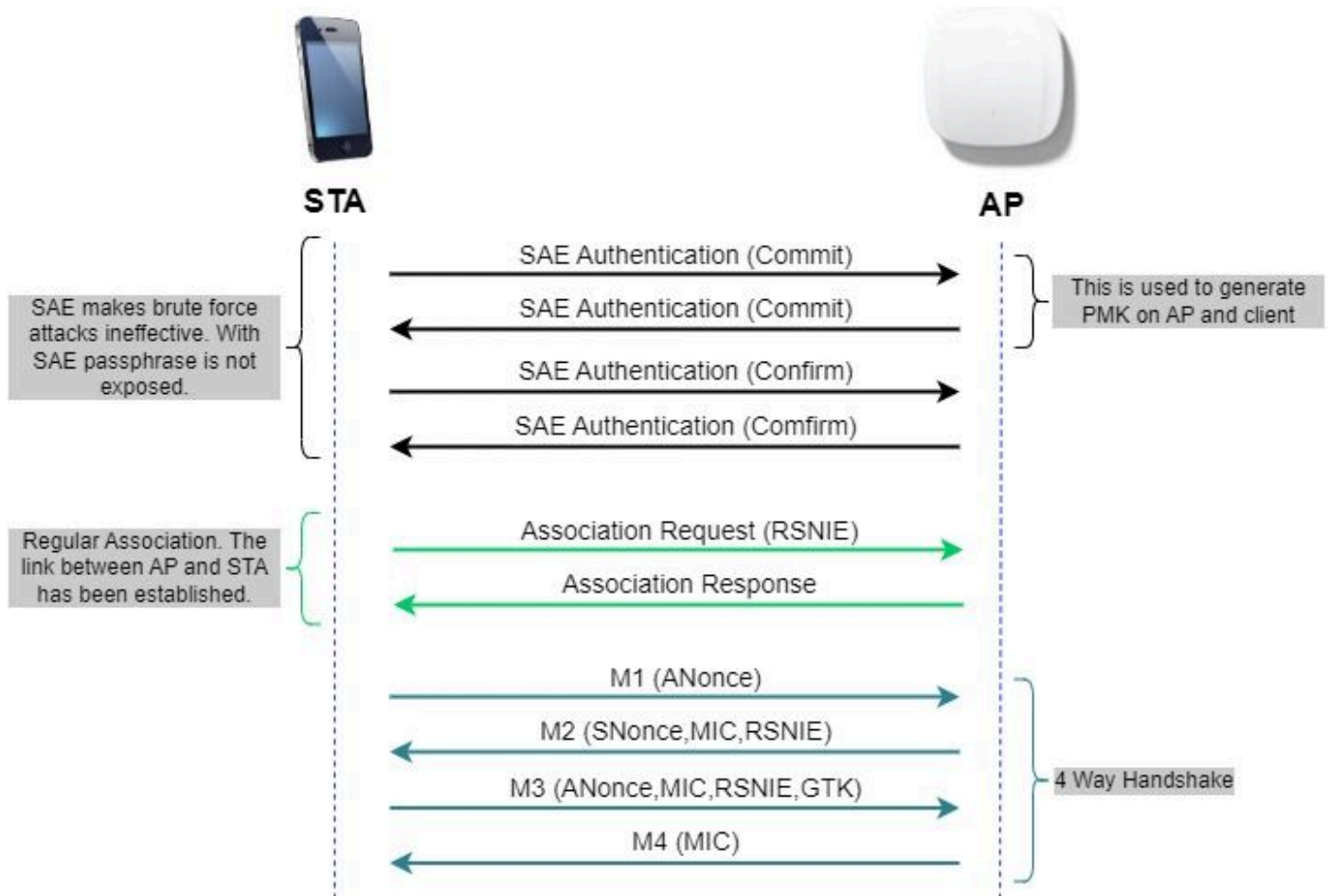
SAE verwendet eine diskrete Logarithmuskryptographie, um einen effizienten Austausch auf eine Weise durchzuführen, die eine gegenseitige Authentifizierung mit einem Passwort ermöglicht, das wahrscheinlich gegen einen Offline-Wörterbuchangriff resistent ist.

Bei einem Angriff auf ein Offline-Wörterbuch versucht ein Angreifer, ein Netzwerkkennwort zu ermitteln, indem er mögliche Kennwörter ohne weitere Netzwerkinteraktion ausprobiert.

Wenn der Client eine Verbindung mit dem Access Point herstellt, führt er einen SAE-Austausch durch. Bei Erfolg erstellen sie jeweils einen kryptographisch starken Schlüssel, von dem der

Sitzungsschlüssel abgeleitet wird. Grundsätzlich geht ein Client und Access Point in Phasen des Commit und dann bestätigen.

Sobald eine Vereinbarung besteht, können der Client und der Access Point bei jeder Generierung eines Sitzungsschlüssels in den Bestätigungsstatus wechseln. Die Methode verwendet die Weiterleitungsgeheimnis, bei der ein Eindringling einen einzelnen Schlüssel knacken könnte, aber nicht alle anderen Schlüssel.



SAE Frame Exchange

### Hash-to-Element (H2E)

Hash-to-Element (H2E) ist eine neue PWE-Methode (SAE Password Element). Bei diesem Verfahren wird die im SAE-Protokoll verwendete geheime PWE aus einem Passwort generiert.

Wenn eine Station (STA), die H2E unterstützt, SAE mit einem AP initiiert, prüft sie, ob AP H2E unterstützt. Wenn ja, leitet der AP die PWE über H2E mithilfe eines neu definierten Statuscodewerts in der SAE-Commit-Nachricht ab.

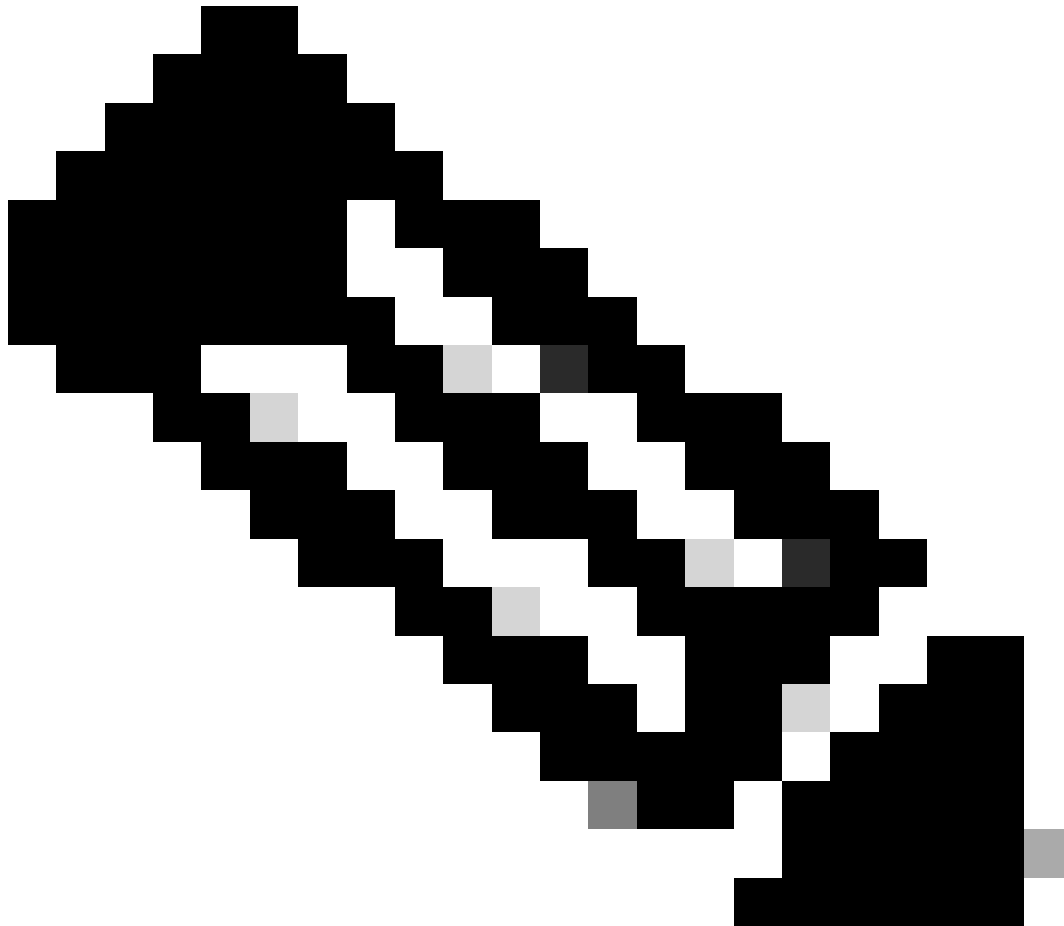
Wenn STA Hunting-and-Pecking (HnP) verwendet, bleibt der gesamte SAE-Austausch unverändert.

Bei Verwendung von H2E wird die PWE-Ableitung in folgende Komponenten unterteilt:

- Ableitung eines Secret Intermediary Elements (PT) aus dem Passwort. Dies kann offline

durchgeführt werden, wenn das Kennwort für jede unterstützte Gruppe auf dem Gerät konfiguriert wurde.

- Ableitung des PWE aus dem gespeicherten PT. Dies hängt von der ausgehandelten Gruppe und den MAC-Adressen der Peers ab. Dies erfolgt in Echtzeit während des SAE-Austauschs.

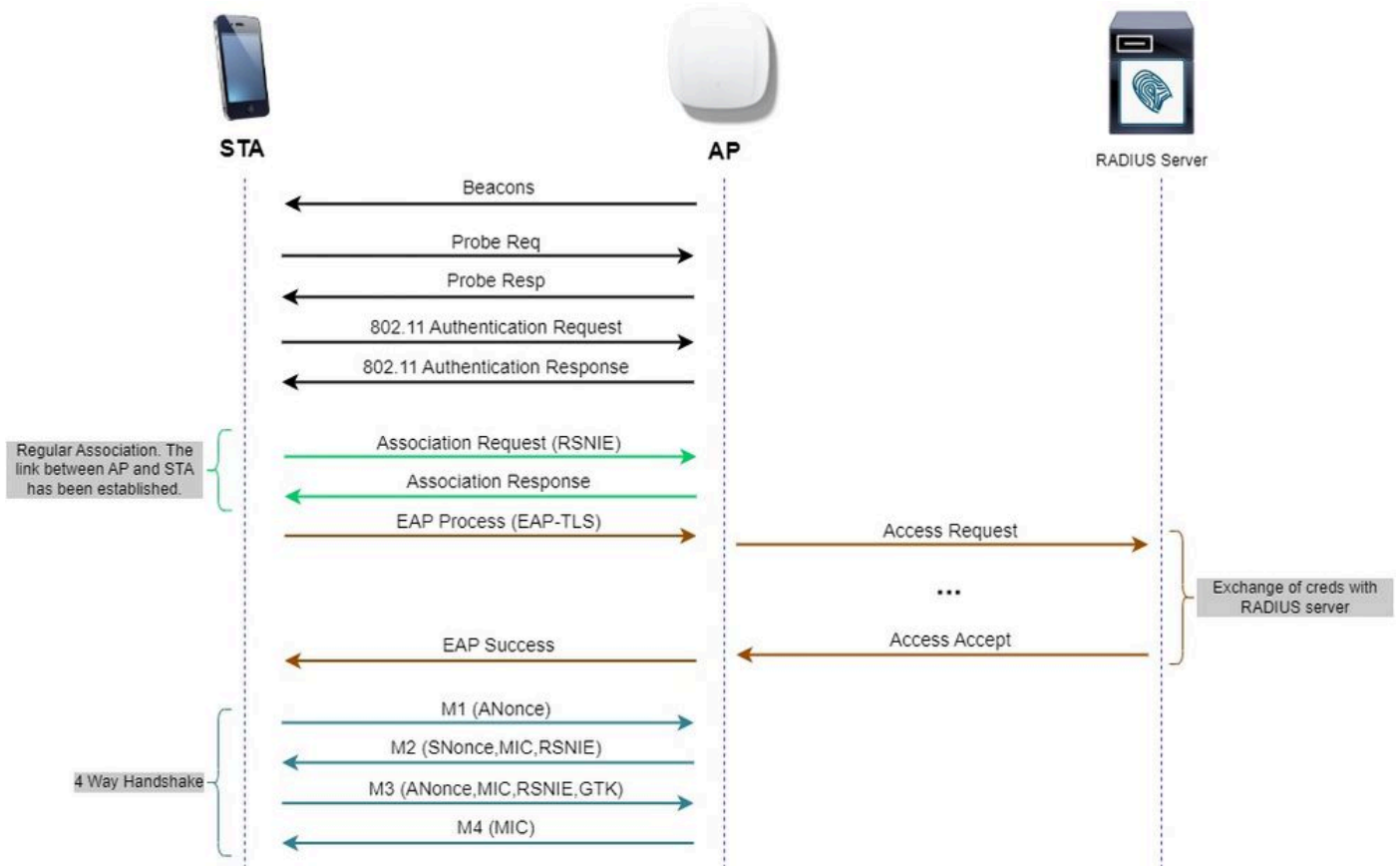


Hinweis: 6 GHz unterstützt nur die Hash-to-Element SAE PWE-Methode.

---

## WPA-Enterprise (802.1x)

WPA3-Enterprise ist die sicherste Version von WPA3 und verwendet eine Kombination aus Benutzername und Kennwort mit 802.1X für die Benutzerauthentifizierung mit einem RADIUS-Server. Standardmäßig verwendet WPA3 eine 128-Bit-Verschlüsselung, führt jedoch auch eine optional konfigurierbare Verschlüsselungsstärke-Verschlüsselung mit 192 Bit ein, die ein Netzwerk, das sensible Daten überträgt, zusätzlich schützt.



WPA3-Enterprise-Diagramm

## Stufensatz: WPA3-Modi

- WPA3-Personal
  - Nur WPA3-Personal-Modus
    - PMF erforderlich
  - WPA3-Personal-Übergangsmodus
    - Konfigurationsregeln: Wenn WPA2-Personal auf einem WAP aktiviert ist, muss standardmäßig auch der WPA3-Personal-Übergangsmodus aktiviert sein, es sei denn, der Administrator hat dies explizit überschrieben, um nur im WPA2-Personal-Modus zu arbeiten.
- WPA3-Enterprise
  - WPA3 - Nur Enterprise-Modus
    - Die PMF wird für alle WPA3-Verbindungen ausgehandelt.
  - WPA3-Enterprise-Übergangsmodus
    - Die PMF wird für eine WPA3-Verbindung ausgehandelt.
    - PMF optional für eine WPA2-Verbindung
  - WPA3-Enterprise Suite-B "192-Bit"-Modus abgestimmt auf Commercial National Security Algorithm (CNSA)
    - Mehr als nur für die Bundesregierung
    - Konsistente Verschlüsselung zur Vermeidung von Fehlkonfigurationen
    - Ergänzung von GCMP und ECCP für Crypto- und bessere Hash-Funktionen

(SHA384)

- PMF erforderlich
- Die WPA3-192-Bit-Sicherheit gilt ausschließlich für EAP-TLS, für das Zertifikate sowohl auf dem Supplicant als auch auf dem RADIUS-Server erforderlich sind.
- Um WPA3 192-Bit Enterprise verwenden zu können, müssen die RADIUS-Server eine der zulässigen EAP-Verschlüsselungen verwenden:





TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384

TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

Weitere Informationen zur WPA3-Implementierung in Cisco WLANs, einschließlich der Kompatibilitätstabelle für die Client-Sicherheit, finden Sie im [WPA3-Bereitstellungsfaden](#).

## Cisco Catalyst Wi-Fi 6E APs

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

## Von Clients unterstützte Sicherheitseinstellungen

Welche Produkte WPA3-Enterprise unterstützen, erfahren Sie auf der WiFi Alliance [Produktsuche](#).

Auf Windows-Geräten können Sie mithilfe des Befehls "netsh wlan show drivers" überprüfen, welche Sicherheitseinstellungen vom Adapter unterstützt werden.

Hier sehen Sie die Ausgabe der 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-Ausgabe von `_netsh wlan show driver_` für 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-Ausgabe von `_netsh wlan show driver_` für Client Netgear A8000s

Android-Pixel 6a:





None

Enhanced Open

WEP

WPA/WPA2-Personal

WPA3-Personal

WPA/WPA2-Enterprise

WPA3-Enterprise

WPA3-Enterprise 192-bit



CIF



- WPA3- + AES-Verschlüsselung + 802.1x-SHA256 (FT) AKM
- WPA3 + AES-Verschlüsselung + OWE AKM
- WPA3 + AES-Verschlüsselung + SAE (FT) AKM
- WPA3 + CCMP256-Chiffre + SUITEB192-1X AKM
- WPA3 + GCMP128-Chiffre + SUITEB-1X AKM
- WPA3 + GCMP256-Chiffre + SUITEB192-1X AKM

## Basiskonfiguration

Das WLAN wurde mit der Ermittlungsmethode "Nur Funkrichtlinie 6 GHz" und "UPR (Broadcast Probe Response)" konfiguriert:

**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

---

Profile Name*	<input type="text" value="wifi_test"/>	<b>Radio Policy</b> ⓘ
SSID*	<input type="text" value="wifi_test"/>	<a href="#">Show slot configuration</a>
WLAN ID*	<input type="text" value="5"/>	
Status	<input checked="" type="checkbox"/> <b>ENABLED</b>	<b>6 GHz</b> Status <input checked="" type="checkbox"/> <b>ENABLED</b> <input checked="" type="checkbox"/> WPA2 Disabled <input checked="" type="checkbox"/> WPA3 Enabled <input checked="" type="checkbox"/> Dot11ax Enabled
Broadcast SSID	<input checked="" type="checkbox"/> <b>ENABLED</b>	<b>5 GHz</b> Status <input type="checkbox"/> <b>DISABLED</b>
		<b>2.4 GHz</b> Status <input type="checkbox"/> <b>DISABLED</b> 802.11b/g Policy <input type="text" value="802.11b/g"/>

WLAN-Basiskonfiguration

Configuration > Tags & Profiles > RF/Radio

RF Radio

State	RF Profile Name	Band
<input type="checkbox"/>	default-rf-profile-6ghz	6 GHz
<input type="checkbox"/>	Low_Client_Density_rf_5gh	5 GHz
<input type="checkbox"/>	High_Client_Density_rf_5gh	5 GHz
<input type="checkbox"/>	Low_Client_Density_rf_24gh	2.4 GHz
<input type="checkbox"/>	High_Client_Density_rf_24gh	2.4 GHz
<input type="checkbox"/>	Typical_Client_Density_rf_5gh	5 GHz
<input type="checkbox"/>	Typical_Client_Density_rf_24gh	2.4 GHz

10

Edit RF Profile

General 802.11 RRM Advanced 802.11ax

6 GHz Discovery Frames  None  Broadcast Probe Response  FILS Discovery

Broadcast Probe Response Interval (msec)\*

Multi BSSID Profile

Spatial Reuse

OBSS PD

Non-SRG OBSS PD Max Threshold (dBm)\*

SRG OBSS PD

SRG OBSS PD Min Threshold (dBm)\*

SRG OBSS PD Max Threshold (dBm)\*

Konfiguration des 6-GHz-RF-Profiles

## Überprüfung

### Sicherheitsüberprüfung

In diesem Abschnitt wird die Phase der Sicherheitskonfiguration und der Client-Zuordnung mithilfe der folgenden WPA3-Protokollkombinationen erläutert:

- WPA3- AES(CCMP128) + SCHULDENSTÜCK
  - OWE-Übergangsmodus
- WPA3-Personal
  - AES (CCMP128) + SAE
- WPA3-Enterprise
  - AES (CCMP128) + 802.1x-SHA256
  - AES (CCMP128) + 802.1x-SHA256 + FT
  - GCMP128-Chiffre + SUITEB-1X
  - GCMP256-Chiffre + SUITEB192-1X

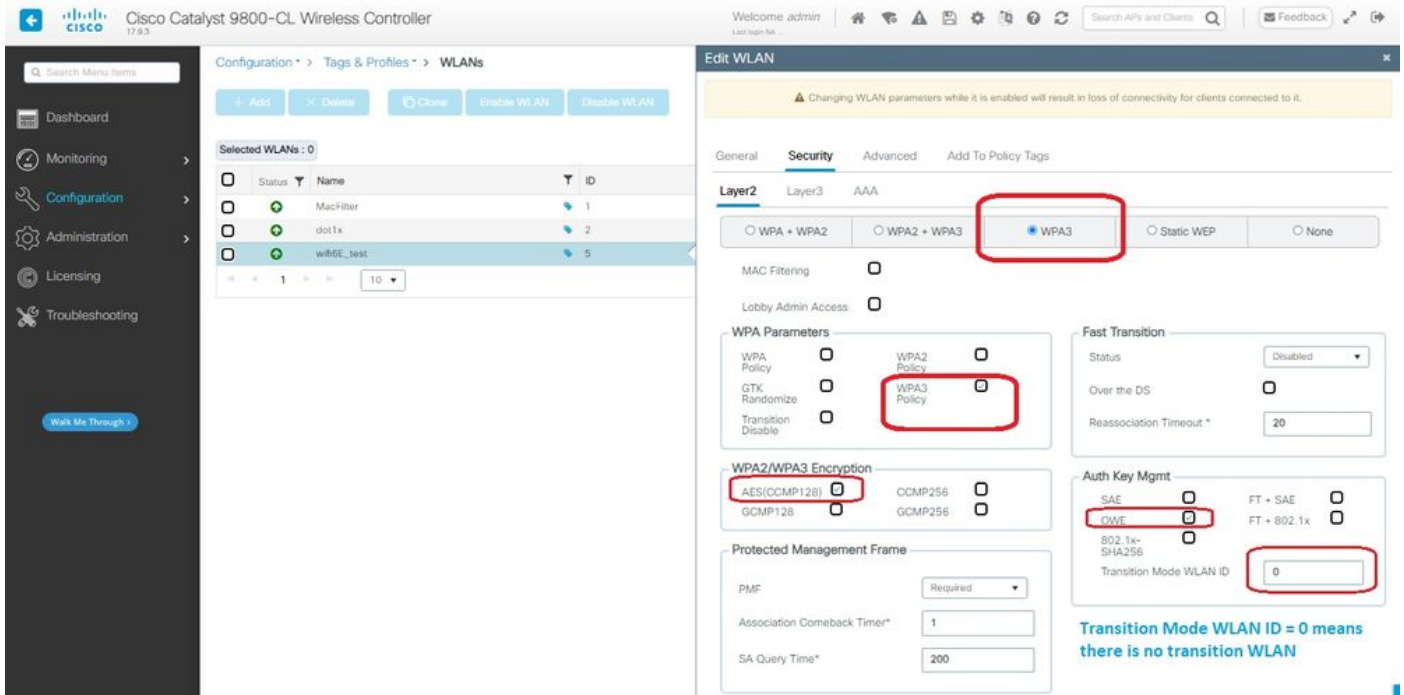


Hinweis: Obwohl es keine Clients gibt, die GCMP128 cipher + SUITEB-1X unterstützen, als sie dieses Dokument geschrieben haben, wurde es getestet, um zu beobachten, dass es gesendet wird, und die RSN-Informationen in den Beacons zu überprüfen.

---

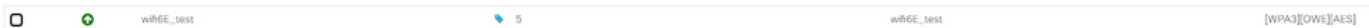
WPA3 - AES (CCPM128) + SCHULDENSTÜCK

Dies ist die WLAN-Sicherheitskonfiguration:



OWE-Sicherheitseinstellungen

Auf der WLC-GUI der WLAN-Sicherheitseinstellungen anzeigen:



WLAN-Sicherheitseinstellungen auf der WLC-GUI

Hier können wir den Verbindungsvorgang der Wi-Fi 6E Clients beobachten:

Intel AX211

Hier zeigen wir den vollständigen Verbindungsvorgang des Intel AX211-Clients.

OWE-Analyse

Hier sehen Sie die Beacons OTA. Der Access Point kündigt mithilfe des Selektors der AKM-Suite für OWE unter dem RSN-Informationselement die Unterstützung für OWE an.

Sie können den Wert 18 (00-0F-AC:18) für den Typ der AKM-Suite sehen, der auf die OWE-Unterstützung hinweist.

Wireshark capture showing IEEE 802.11 Beacon frames. The packet details pane highlights the RSN Information field, which includes RSN Capabilities, Group Cipher Suite, and Authentication Algorithms.

### OWE-Bakenrahmen

Wenn Sie sich das Feld "RSN-Funktionen" ansehen, sehen Sie, dass der Access Point sowohl MFP-Funktionen (Management Frame Protection) als auch das erforderliche MFP-Bit (1) ankündigt.

### OWE-Verbind

Sie können den UPB im Broadcast-Modus und dann die Zuordnung selbst sehen.

Das OWE beginnt mit der OPEN-Authentifizierungsanfrage und -antwort:

Wireshark capture showing the initial OWE authentication process. The packet details pane shows the Authentication frame details, including the Authentication Algorithm (Open System) and successful status.

Wireshark capture showing the continuation of the OWE authentication process. The packet details pane shows the Action frame details, including the Action Set (Sh-26) and successful status.

Anschließend muss ein Client, der OWE durchführen möchte, OWE AKM im RSN IE des Association Request-Frames angeben und das Diffie Helman (DH)-Parametererelement einschließen:









## Samsung S23

## Verbindung OTA mit Fokus auf RSN-Informationen vom Client:

## Client-Details in WLC:

## WPA3 - AES(CCMP128) + OWE mit Übergangsmodus

Ausführliche Informationen zur Konfiguration und Fehlerbehebung des OWE-Übergangsmodus finden Sie in diesem Dokument: [Konfigurieren der erweiterten offenen SSID mit dem Übergangsmodus - OWE.](#)

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

## WLAN-Sicherheitskonfiguration:

### 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(OCMP128)	<input type="checkbox"/>	OCMP256	<input type="checkbox"/>
GCMP128	<input type="checkbox"/>	GCMP256	<input type="checkbox"/>

#### Protected Management Frame

PMF

Association Comeback Timer\*

SA Query Time\*

#### Auth Key Mgmt

SAE	<input checked="" type="checkbox"/>	FT - SAE	<input type="checkbox"/>
ONE	<input type="checkbox"/>	FT - 802.1x	<input type="checkbox"/>
802.1x-SHA256	<input type="checkbox"/>		

Anti Clogging Threshold\*

Max Retries\*

Retransmit Timeout\*

PSK Format

PSK Type

Pre-Shared Key\*

SAE Password Element

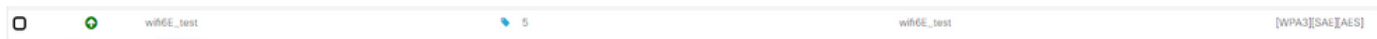
WPA3 SAE-Konfiguration



Hinweis: Beachten Sie, dass Hunting und Pecking gemäß der 6-GHz-Funkrichtlinie nicht zulässig sind. Wenn Sie ein reines 6-GHz-WLAN konfigurieren, müssen Sie H2E SAE Password Element auswählen.

---

Auf der WLC-GUI der WLAN-Sicherheitseinstellungen anzeigen:



Verifizierung von Beacons OTA:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
2023-06-12 17:12:24.459118	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Frame 6: 508 bytes on wire (4064 bits), 508 bytes captured (4064 bits) on interface Vdeice\NPF_{04578995-2998-4464-4}	
2023-06-12 17:12:24.478646	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Ethernet II, Src: Cisco_00:10:00:00:00:00, Dst: Universal_Broadcast(00:00:00:00:00:00)	
2023-06-12 17:12:24.491121	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Internet Protocol version 4, Src: 192.168.1.13, Dst: 192.168.1.1	
2023-06-12 17:12:24.511872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	User Datagram Protocol, Src Port: 5000, Dst Port: 5000	
2023-06-12 17:12:24.531872	0.00000	Cisco,13:80:0E	Broadcast	002:11	508	-13.7 dBm	Beacon frame, S/W78, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SSID	AirPortKey/OnMfiKey encapsulated IEEE 802.11	
2023-06-12 17:12:24.551872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	IEEE 802.11 radio information	
2023-06-12 17:12:24.571872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	IEEE 802.11 Beacon frame, Flags:.....C	
2023-06-12 17:12:24.591872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	IEEE 802.11 wireless management	
2023-06-12 17:12:24.611872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Fixed parameters (406 bytes)	
2023-06-12 17:12:24.631872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Tag: SSI parameter set "WiFi6_Test_02"	
2023-06-12 17:12:24.651872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Tag: Supported rates (3), 5, 11M; 18, 24M; 36, 48, 54, 72Mbit/sec	
2023-06-12 17:12:24.671872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Tag: Traffic Indication Map (TIM): OFDM 2 of 3 bitmap	
2023-06-12 17:12:24.691872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Tag: Country Information: Country code is, Environment global operating classes	
2023-06-12 17:12:24.711872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Tag: Power Constraints: 0	
2023-06-12 17:12:24.731872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Tag: TPC Report Transm Power: 17, Link Margin: 0	
2023-06-12 17:12:24.751872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Tag: RSN Information	
2023-06-12 17:12:24.771872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Tag number: RSN Information (48)	
2023-06-12 17:12:24.791872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Tag length: 36	
2023-06-12 17:12:24.811872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	RSN version: 1	
2023-06-12 17:12:24.831872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Group Cipher Suite: 000fac (IEEE 802.11 AES (CCM))	
2023-06-12 17:12:24.851872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Pairwise Cipher Suite Count: 1	
2023-06-12 17:12:24.871872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Pairwise Cipher Suite: 000fac (IEEE 802.11 AES (CCM))	
2023-06-12 17:12:24.891872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Auth Key Management (AKM) Suite Count: 1	
2023-06-12 17:12:24.911872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Auth Key Management (AKM) Suite: 000fac (IEEE 802.11 SAE (SHA256))	
2023-06-12 17:12:24.931872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	RSN Capabilities: 000000	
2023-06-12 17:12:24.951872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	PMKID Count: 0	
2023-06-12 17:12:24.971872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	PMKID List	
2023-06-12 17:12:24.991872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Group Management Cipher Suite: 000fac (IEEE 802.11 GSP (128))	
2023-06-12 17:12:25.011872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Tag: QSS Load Element 000fac (CCM version)	
2023-06-12 17:12:25.031872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Tag: Multiple BSSID	
2023-06-12 17:12:25.051872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Tag: M Enabled Capabilities (5 octets)	
2023-06-12 17:12:25.071872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Tag: Extended Capabilities (11 octets)	
2023-06-12 17:12:25.091872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Tag: TX Power Envelope	
2023-06-12 17:12:25.111872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Ext Tag: Multiple BSSID Configuration	
2023-06-12 17:12:25.131872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Ext Tag: HE Capabilities	
2023-06-12 17:12:25.151872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Ext Tag: HE Operation	
2023-06-12 17:12:25.171872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Ext Tag: Spatial Reuse Parameter Set	
2023-06-12 17:12:25.191872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Ext Tag: MU-EDCA Parameter Set	
2023-06-12 17:12:25.211872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Ext Tag: HE DSS Band Capabilities	
2023-06-12 17:12:25.231872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Tag: RSN extension (1 octet)	
2023-06-12 17:12:25.251872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Tag Number: RSN extension (244)	
2023-06-12 17:12:25.271872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	RSN: 0x20 (octet 1)	
2023-06-12 17:12:25.291872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	..... 0000 = RSN Length: 0	
2023-06-12 17:12:25.311872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	..... 0 = Protected but Operations Support: 0	
2023-06-12 17:12:25.331872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	..... 0000 = SAE Mesh to Element: 1	
2023-06-12 17:12:25.351872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	..... 0000 = Reserved 00	
2023-06-12 17:12:25.371872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Tag: Vendor Specific: Atheros Communications, Inc.: Unknown	
2023-06-12 17:12:25.391872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Tag: Vendor Specific: Microsoft Corp.: WPA/WPA2: Parameter Element	
2023-06-12 17:12:25.411872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Tag: Vendor Specific: Cisco Systems, Inc.: Airont Unknown (44)	
2023-06-12 17:12:25.431872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Tag: Vendor Specific: Cisco Systems, Inc.: Airont Unknown (11) (11)	
2023-06-12 17:12:25.451872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Tag: Vendor Specific: Cisco Systems, Inc.: Airont IEEE Disabled	
2023-06-12 17:12:25.471872	0.00000	Cisco,13:80:0E	Broadcast	002:11	463	-13.6 dBm	Probe Response, S/W73, F/W0, Flags:.....C, B1=00, SSID="WiFi6_Test_02", SS	Tag: Vendor Specific: Cisco Systems, Inc.: Airont CCM version = 5	

## WPA3 SAE-Beacons

Hier können wir beobachten, wie Wi-Fi 6E-Clients sich verbinden:

## Intel AX211

Verbindung OTA mit Fokus auf RSN-Informationen vom Client:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
2235	2023-06-12 17:15:00.328330	0.00000	IntelCor_9E:18:50:09	Broadcast	002:11	168	-4.07 dBm	Probe Request, S/W309, F/W0, Flags:.....C, SSID=Wildcard (Broadcast)	Frame 1225: 194 bytes on wire (1552 bits), 194 bytes captured (1552 bits) on interface Vdeice\NPF_{04578995-2998-4464-4}
2237	2023-06-12 17:15:00.328335	0.00000	IntelCor_9E:18:50:09	Broadcast	002:11	168	-4.07 dBm	Probe Request, S/W309, F/W0, Flags:.....C, SSID=Wildcard (Broadcast)	Ethernet II, Src: Cisco_00:10:00:00:00:00, Dst: Universal_Broadcast(00:00:00:00:00:00)
2342	2023-06-12 17:15:00.974931	0.00000	IntelCor_9E:18:50:09	Broadcast	002:11	168	-4.07 dBm	Probe Request, S/W309, F/W0, Flags:.....C, SSID=Wildcard (Broadcast)	Internet Protocol version 4, Src: 192.168.1.13, Dst: 192.168.1.13
2344	2023-06-12 17:15:00.977134	0.00000	IntelCor_9E:18:50:09	Broadcast	002:11	168	-4.07 dBm	Probe Request, S/W309, F/W0, Flags:.....C, SSID=Wildcard (Broadcast)	User Datagram Protocol, Src Port: 5000, Dst Port: 5000
5474	2023-06-12 17:15:00.536729	0.00000	IntelCor_9E:18:50:09	Broadcast	002:11	168	-4.07 dBm	Probe Request, S/W309, F/W0, Flags:.....C, SSID=Wildcard (Broadcast)	AirPortKey/OnMfiKey encapsulated IEEE 802.11
5478	2023-06-12 17:15:00.536729	0.00000	IntelCor_9E:18:50:09	Broadcast	002:11	168	-4.07 dBm	Probe Request, S/W309, F/W0, Flags:.....C, SSID=Wildcard (Broadcast)	IEEE 802.11 radio information
8087	2023-06-12 17:15:00.490857	0.00000	IntelCor_9E:18:50:09	Broadcast	002:11	168	-4.07 dBm	Probe Request, S/W309, F/W0, Flags:.....C, SSID=Wildcard (Broadcast)	IEEE 802.11 Beacon frame, Flags:.....C
8089	2023-06-12 17:15:00.492713	0.00000	IntelCor_9E:18:50:09	Broadcast	002:11	168	-4.07 dBm	Probe Request, S/W309, F/W0, Flags:.....C, SSID=Wildcard (Broadcast)	IEEE 802.11 wireless management
8227	2023-06-12 17:15:00.264316	0.00000	IntelCor_9E:18:50:09	Broadcast	002:11	168	-4.07 dBm	Probe Request, S/W309, F/W0, Flags:.....C, SSID=Wildcard (Broadcast)	Fixed parameters (184 bytes)
8229	2023-06-12 17:15:00.266567	0.00000	IntelCor_9E:18:50:09	Broadcast	002:11	168	-4.07 dBm	Probe Request, S/W309, F/W0, Flags:.....C, SSID=Wildcard (Broadcast)	Tag: SSI parameter set "WiFi6_Test_02"
121	2023-06-12 17:15:01.083192	0.00000	IntelCor_9E:18:50:09	Broadcast	002:11	168	-4.07 dBm	Probe Request, S/W309, F/W0, Flags:.....C, SSID=Wildcard (Broadcast)	Tag: Supported rates (3), 5, 11M; 18, 24M; 36, 48, 54, 72Mbit/sec
122	2023-06-12 17:15:01.084321	0.00000	IntelCor_9E:18:50:09	Broadcast	002:11	168	-4.07 dBm	Probe Request, S/W309, F/W0, Flags:.....C, SSID=Wildcard (Broadcast)	Tag: Traffic Indication Map (TIM): OFDM 2 of 3 bitmap
124	2023-06-12 17:15:01.084800	0.00000	IntelCor_9E:18:50:09	Broadcast	002:11	168	-4.07 dBm	Probe Request, S/W309, F/W0, Flags:.....C, SSID=Wildcard (Broadcast)	Tag: Country Information: Country code is, Environment global operating classes
125	2023-06-12 17:15:01.084949	0.00000	IntelCor_9E:18:50:09	Broadcast	002:11	168	-4.07 dBm	Probe Request, S/W309, F/W0, Flags:.....C, SSID=Wildcard (Broadcast)	Tag: Power Constraints: 0
126	2023-06-12 17:15:01.085099	0.00000	IntelCor_9E:18:50:09	Broadcast	002:11	168	-4.07 dBm	Probe Request, S/W309, F/W0, Flags:.....C, SSID=Wildcard (Broadcast)	Tag: TPC Report Transm Power: 17, Link Margin: 0
132	2023-06-12 17:15:01.193430	0.00000	IntelCor_9E:18:50:09	Broadcast	002:11	168	-4.07 dBm	Probe Request, S/W309, F/W0, Flags:.....C, SSID=Wildcard (Broadcast)	Tag: RSN Information
133	2023-06-12 17:15:01.206809	0.00000	IntelCor_9E:18:50:09	Broadcast	002:11	168	-4.07 dBm	Probe Request, S/W309, F/W0, Flags:.....C, SSID=Wildcard (Broadcast)	Tag number: RSN Information (48)
134	2023-06-12 17:15:01.221121	0.00000	IntelCor_9E:18:50:09	Broadcast	002:11	168	-4.07 dBm</		



Cisco Catalyst 9800-CL Wireless Controller

Welcome admin

Search APs and Clients

Feedback

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Selected 0 out of 12 Clients

Client MAC Address	IPv4 Address	IPv6 Address	AP Name
0012.17e1.d5d7	192.168.1.33	fe80::212:17ff:fee1:d5d7	AP03_Sotao_9548
0012.17e2.4856	192.168.1.37	fe80::212:17ff:fee2:4856	AP05_OutdoorB_2200
0012.17e2.4b40	192.168.1.31	fe80::212:17ff:fee2:4b40	AP04_OutdoorF_3DC0
0c8b.9509.3518	192.168.1.129	N/A	AP03_Sotao_9548
286b.3598.580f	192.168.1.159	fe80::ac5b:e1e1:67bac:353	AP6849.9253.CA50
34ea.e702.6240	192.168.1.70	N/A	AP6849.9253.CA50
60fb.008b.0e66	N/A	N/A	AP01_RC_9136_F80C
84d8.1b0f.294f	192.168.1.91	N/A	AP03_Sotao_9548
9669.5a28.a115	192.168.1.138	fe80::9469:5aff:fe28:a115	AP02_Suite_1084
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: 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

Verbindung OTA mit Fokus auf RSN-Informationen vom Client:

```

[00:00:00] 88 (vlan_addr == 9418.6548.7095) || (vlan_fc_type_subtype == 0x001d)
No. Time Delta Source Destination Protocol Length Channel Signal Info
322 2023-06-12 17:22:13.932040 0.000000 netgear_48170:95 Broadcast 802.11 166 5 -40 dBm Probe Request, Ssn=1799, Pw=, Flags=.....C, SSID="billiard"
323 2023-06-12 17:22:13.928174 0.000014 netgear_48170:95 Broadcast 802.11 166 5 -40 dBm Probe Request, Ssn=1799, Pw=, Flags=.....C, SSID="billiard"
324 2023-06-12 17:22:13.922893 0.000019 netgear_48170:95 Broadcast 802.11 166 5 -40 dBm Probe Request, Ssn=1794, Pw=, Flags=.....C, SSID="billiard"
326 2023-06-12 17:22:13.921977 0.000084 netgear_48170:95 Broadcast 802.11 166 5 -40 dBm Probe Request, Ssn=1794, Pw=, Flags=.....C, SSID="billiard"
733 2023-06-12 17:22:13.416940 7.494063 netgear_48170:95 Cisco_131:80:.. 802.11 368 5 -49 dBm Probe Request, Ssn=, Pw=, Flags=.....C, SSID="wifi6_test"
734 2023-06-12 17:22:13.416940 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -36 dBm Acknowledgment, Flags=.....C
736 2023-06-12 17:22:13.419412 0.002472 netgear_48170:95 Cisco_131:80:.. 802.11 368 5 -49 dBm Probe Request, Ssn=, Pw=, Flags=.....C, SSID="wifi6_test"
737 2023-06-12 17:22:13.419412 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -37 dBm Acknowledgment, Flags=.....C
740 2023-06-12 17:22:13.444835 0.024223 netgear_48170:95 Cisco_131:80:.. 802.11 368 5 -49 dBm Probe Request, Ssn=, Pw=, Flags=.....C, SSID="wifi6_test"
741 2023-06-12 17:22:13.444835 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -37 dBm Acknowledgment, Flags=.....C
746 2023-06-12 17:22:13.498956 0.054211 netgear_48170:95 Cisco_131:80:.. 802.11 394 5 -50 dBm Authentication, Ssn=, Pw=, Flags=.....C
747 2023-06-12 17:22:13.498956 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -36 dBm Acknowledgment, Flags=.....C
750 2023-06-12 17:22:13.546544 0.048488 Cisco_131:80:.. netgear_4817:.. 802.11 194 5 -37 dBm Authentication, Ssn=123, Pw=, Flags=.....C
751 2023-06-12 17:22:13.546544 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -40 dBm Acknowledgment, Flags=.....C
753 2023-06-12 17:22:13.558937 0.004153 netgear_48170:95 Cisco_131:80:.. 802.11 390 5 -49 dBm Authentication, Ssn=, Pw=, Flags=.....C
754 2023-06-12 17:22:13.558937 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -37 dBm Acknowledgment, Flags=.....C
755 2023-06-12 17:22:13.553082 0.002795 Cisco_131:80:.. netgear_4817:.. 802.11 390 5 -49 dBm Authentication, Ssn=124, Pw=, Flags=.....C
756 2023-06-12 17:22:13.553082 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -49 dBm Acknowledgment, Flags=.....C
757 2023-06-12 17:22:13.557006 0.003404 netgear_48170:95 Cisco_131:80:.. 802.11 216 5 -49 dBm Association Request, Ssn=, Pw=, Flags=.....C, SSID="wifi6_test"
758 2023-06-12 17:22:13.557006 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -37 dBm Acknowledgment, Flags=.....C
760 2023-06-12 17:22:13.568065 0.001199 netgear_48170:95 Broadcast LLC 124 5 -37 dBm U, Func=Command, SSAP=8002 Group, SSAP SNAP Command
763 2023-06-12 17:22:13.567111 0.000406 Cisco_131:80:.. netgear_4817:.. 802.11 262 5 -37 dBm Association Response, Ssn=, Pw=, Flags=.....C
764 2023-06-12 17:22:13.567111 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -49 dBm Acknowledgment, Flags=.....C
765 2023-06-12 17:22:13.567108 0.000049 netgear_48170:95 Broadcast LLC 124 5 -37 dBm I P, N(0)=0, N(3)=0; SSAP=8006 Group, SSAP 8006 Response
766 2023-06-12 17:22:13.568723 0.001563 Cisco_131:80:.. netgear_4817:.. EAPOL 221 5 -37 dBm Key (Message 1 of 4)
767 2023-06-12 17:22:13.568723 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -40 dBm Acknowledgment, Flags=.....C
782 2023-06-12 17:22:13.742256 0.173333 netgear_48170:95 Cisco_131:80:.. EAPOL 226 5 -55 dBm Key (Message 2 of 4)
783 2023-06-12 17:22:13.742256 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -44 dBm Acknowledgment, Flags=.....C
785 2023-06-12 17:22:13.743972 0.001716 Cisco_131:80:.. netgear_4817:.. EAPOL 295 5 -44 dBm Key (Message 3 of 4)
786 2023-06-12 17:22:13.743972 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -50 dBm Acknowledgment, Flags=.....C
787 2023-06-12 17:22:13.744676 0.000704 netgear_48170:95 Cisco_131:80:.. EAPOL 199 5 -55 dBm Key (Message 4 of 4)
788 2023-06-12 17:22:13.744676 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -44 dBm Acknowledgment, Flags=.....C
789 2023-06-12 17:22:13.752542 0.007866 Cisco_931c:50 netgear_4817:.. LLC 187 5 -44 dBm U, Func=Command, SSAP=8006 Group, SSAP 8030 Response
790 2023-06-12 17:22:13.752542 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -55 dBm Acknowledgment, Flags=.....C
791 2023-06-12 17:22:13.754271 0.001729 192.168.1.15 192.168.1.121 802.11 119 5 -43 dBm Trigger Buffer Status Report Poll (BSRP), Flags=.....C
793 2023-06-12 17:22:13.754647 0.000376 netgear_48170:95 Broadcast LLC 144 5 -55 dBm I P, N(0)=1, N(3)=0; SSAP=8006 Group, SSAP LLC Sub-Layer Management
794 2023-06-12 17:22:13.754647 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -44 dBm Acknowledgment, Flags=.....C
  
```

## 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

Selected 0 out of 12 Clients

Client MAC Address	IPv4 Address	IPv6 Address	AP Name
0012.17e1.d5d7	192.168.1.33	fe80::212:17ff:fee1:d5d7	AP03_Sotao_9548
0012.17e2.4856	192.168.1.37	fe80::212:17ff:fee2:4856	AP05_OutdoorB_2200
0012.17e2.4b40	192.168.1.31	fe80::212:17ff:fee2:4b40	AP04_OutdoorF_3DC0
0c8b.9509.3518	192.168.1.129	N/A	AP03_Sotao_9548
34ea.e702.6240	192.168.1.70	N/A	AP6849.9253.CA50
60fb.008b.0e66	N/A	N/A	AP01_RC_9136_F80C
84d8.1b0f.294f	192.168.1.91	N/A	AP03_Sotao_9548
9418.6548.7095	192.168.1.163	fe80::c0e19:6116:279d:5151	AP6849.9253.CA50
9669.5a28.a115	192.168.1.138	fe80::9469:5aff:fe28:a115	AP02_Suite_1084
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: 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: 000000000000FAFB0A160F3  
 Acct Session ID: 0x00000000

Auth Method Status List

Method: SAE

## Pixel 6a

Verbindung OTA mit Fokus auf RSN-Informationen vom Client:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
1235	2023-06-12 17:37:02.738033	0.000000	Google_7218a-66	Cisco_31180-1	Broadcast	802.11	343	-42 dBm	Probe Request, S/W=99, P/W=0, Flags=.....C, SSID="wifid_test"
1243	2023-06-12 17:37:02.855631	0.117298	Google_7218a-66	Cisco_31180-1	Broadcast	802.11	394	-42 dBm	Authentication, S/W=997, P/W=0, Flags=.....C
1244	2023-06-12 17:37:02.855631	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
1246	2023-06-12 17:37:02.859394	0.007353	Cisco_31180-1	Google_7218a-66	802.11	194	-37 dBm	Authentication, S/W=1, P/W=0, Flags=.....C	
1247	2023-06-12 17:37:02.859394	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
1248	2023-06-12 17:37:02.868831	0.009487	Google_7218a-66	Cisco_31180-1	Broadcast	802.11	139	-41 dBm	Authentication, S/W=998, P/W=0, Flags=.....C
1249	2023-06-12 17:37:02.868831	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
1252	2023-06-12 17:37:02.904326	0.035495	Cisco_31180-1	Google_7218a-66	802.11	139	-37 dBm	Authentication, S/W=1, P/W=0, Flags=.....C	
1253	2023-06-12 17:37:02.904326	0.000000	192.168.1.15	192.168.1.121	802.11	76	-41 dBm	Acknowledgment, Flags=.....C	
1255	2023-06-12 17:37:02.929933	0.016687	Google_7218a-66	Cisco_31180-1	Broadcast	802.11	262	-41 dBm	Association Request, S/W=999, P/W=0, Flags=.....C, SSID="wifid_test"
1256	2023-06-12 17:37:02.929933	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
1259	2023-06-12 17:37:02.930808	0.000817	Google_7218a-66	Broadcast	802.11	144	-37 dBm	I P, N(1)<N(1), N(1)>: SSAP Basic Individual, SSAP Basic Command	
1261	2023-06-12 17:37:02.934129	0.003779	Cisco_31180-1	Google_7218a-66	802.11	262	-37 dBm	Association Response, S/W=0, P/W=0, Flags=.....C	
1262	2023-06-12 17:37:02.934129	0.000000	192.168.1.15	192.168.1.121	802.11	76	-41 dBm	Acknowledgment, Flags=.....C	
1263	2023-06-12 17:37:02.934129	0.000000	Google_7218a-66	Broadcast	802.11	134	-37 dBm	S P, Func=0x1, N(1)<N(1)>: SSAP Basic Group, SSAP Basic Response	
1265	2023-06-12 17:37:02.943892	0.009363	Cisco_31180-1	Google_7218a-66	EAPOL	223	-37 dBm	Key (message 1 of 4)	
1266	2023-06-12 17:37:02.943892	0.000000	192.168.1.15	192.168.1.121	802.11	76	-41 dBm	Acknowledgment, Flags=.....C	
1273	2023-06-12 17:37:02.992247	0.051155	Google_7218a-66	Cisco_31180-1	EAPOL	230	-51 dBm	Key (message 2 of 4)	
1274	2023-06-12 17:37:02.992247	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
1275	2023-06-12 17:37:02.995369	0.003122	Cisco_31180-1	Google_7218a-66	EAPOL	295	-37 dBm	Key (message 3 of 4)	
1276	2023-06-12 17:37:02.995369	0.000000	192.168.1.15	192.168.1.121	802.11	76	-51 dBm	Acknowledgment, Flags=.....C	
1278	2023-06-12 17:37:03.000159	0.004790	Google_7218a-66	Cisco_31180-1	EAPOL	199	-48 dBm	Key (message 4 of 4)	
1279	2023-06-12 17:37:03.000159	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
1281	2023-06-12 17:37:03.021709	0.021231	192.168.1.15	192.168.1.121	802.11	76	-46 dBm	Acknowledgment, Flags=.....C	
1282	2023-06-12 17:37:03.025924	0.002534	Google_7218a-66	Cisco_31180-1	Broadcast	802.11	122	-49 dBm	Action, S/W=180, P/W=0, Flags=.....C (Malformed Packet)
1283	2023-06-12 17:37:03.025924	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
1284	2023-06-12 17:37:03.040313	0.017809	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
1286	2023-06-12 17:37:03.046766	0.007753	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
1290	2023-06-12 17:37:03.078167	0.027401	Cisco_31180-1	Google_7218a-66	802.11	124	-37 dBm	Action, S/W=1, P/W=0, Flags=.....C	
1291	2023-06-12 17:37:03.078167	0.000000	192.168.1.15	192.168.1.121	802.11	76	-49 dBm	Acknowledgment, Flags=.....C	
1297	2023-06-12 17:37:03.166223	0.088956	Google_7218a-66	Cisco_31180-1	Broadcast	802.11	115	-48 dBm	Action, S/W=180, P/W=0, Flags=.....C (Malformed Packet)
1298	2023-06-12 17:37:03.166223	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
1299	2023-06-12 17:37:03.166229	0.000076	Google_7218a-66	IPVcastst_16	LLC	227	-57 dBm	U P, Func=0x2: SSAP Basic Group, SSAP Basic Command	
1300	2023-06-12 17:37:03.166229	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
1302	2023-06-12 17:37:03.167999	0.001780	Cisco_31180-1	Google_7218a-66	802.11	115	-37 dBm	Action, S/W=1, P/W=0, Flags=.....C (Malformed Packet)	
1303	2023-06-12 17:37:03.167999	0.000000	192.168.1.15	192.168.1.121	802.11	76	-49 dBm	Acknowledgment, Flags=.....C	
1304	2023-06-12 17:37:03.168236	0.000237	192.168.1.15	192.168.1.121	802.11	82	-49 dBm	802.11 Block ACK Req, Flags=.....C	
1305	2023-06-12 17:37:03.168236	0.000000	192.168.1.15	192.168.1.121	802.11	94	-37 dBm	802.11 Block ACK, Flags=.....C	
1306	2023-06-12 17:37:03.168543	0.000347	Google_7218a-66	IPVcastst_16	LLC	186	-38 dBm	I P, N(1)<N(1), N(1)>: SSAP Basic Individual, SSAP Basic Response	
1307	2023-06-12 17:37:03.177442	0.000899	192.168.1.15	192.168.1.121	802.11	82	-45 dBm	Request-to-send, Flags=.....C	
1308	2023-06-12 17:37:03.177442	0.000000	192.168.1.15	192.168.1.121	802.11	76	-38 dBm	Clear-to-send, Flags=.....C	
1309	2023-06-12 17:37:03.177515	0.000073	Google_7218a-66	IPVcastst_16	LLC	271	-56 dBm	I, N(1)<N(1), N(1)>: SSAP Basic Group, SSAP Basic Response	

```

Frame 1255: 262 bytes on wire (2096 bits), 262 bytes captured (2096 bits) on interface Vdevice\WPA_04578905-2998-445
Ethernet II, Src: Cisco_00:1b:7c:17 (00:1b:7c:17:00:17), Dst: Univers_07:cf:c6 (08:0a:8b:07:cf:c6)
Internet Protocol version 4, Src: 192.168.1.15, Dst: 192.168.1.121
User Datagram Protocol, Src Port: 5858, Dst Port: 5800
Airopeek/OMniPeek encapsulated IEEE 802.11
IEEE 802.11 radio information
IEEE 802.11 Authentication, Flags: .....C
fixed parameters (4 bytes)
Tagged parameters (168 bytes)
Tag: SSID parameter Set: "wifid_test"
Tag: Supported rates (0), 9, 12.0, 18, 24.0, 36, 48, 54, [Mbit/sec]
Tag: Extended Supported Rates SAE hash to Element Only, [Mbit/sec]
Tag: Power Capability MHI: -7, MHI: 19
Tag: Supported Channels
Tag: RSN Information
Tag Number: RSN Information (48)
Tag Length: 26
RSN Version: 1
Group Cipher Suite: 00:0fac (IEEE 802.11) AES (CCM)
Pairwise Cipher Suite Count: 1
Pairwise Cipher Suite List 00:0fac (IEEE 802.11) AES (CCM)
Auth Key Management (AKM) Suite Count: 1
Auth Key Management (AKM) List 00:0fac (IEEE 802.11) SAE (SHA256)
RSN Capabilities: 00000
PMKID Count: 0
PMKID List
Group Management Cipher Suite: 00:0fac (IEEE 802.11) BIP (128)
Tag: W enabled capabilities (5 octets)
Tag: Supported Operating Classes
Tag: Extended Capabilities (18 octets)
Ext Tag: HE Capabilities
Tag: RSN extension (1 octet)
Tag Number: RSN extension (244)
Tag Length: 1
RSN: 0000 (octet 1)
..... 0000 = RSN length: 0
..... = Protected TWT Operations Support: 0
..... = Reserved: 000
..... = SAE hash to Element: 1
..... =
Ext Tag: HE 4 oct Band Capabilities
Tag: Vendor Specific: Broadcom
Tag: Vendor Specific: Microsoft Corp.: WPA/WPE: Information Element
  
```

## Client-Details in WLC:

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The main area displays a list of clients, with one client selected. The selected client's details are shown in a sidebar on the right.

Client MAC Address	IPv4 Address	IPv6 Address	AP Name
2495.2f72.8a66	192.168.1.162	fe80::b13:1107:7c5fa7e0	AP6849_9253_CA50
60fb.008b.0e66	N/A	N/A	AP01_RC_9136_F80C
34ea.e702.6240	192.168.1.70	N/A	AP6849_9253_CA50
a810.87bb.b833	192.168.1.94	fe80::a10:87f:febb:b833	AP03_Sotao_9548
9669.5a28.a115	192.168.1.138	fe80::9669:5aff:fa28:a115	AP02_Sotao_1084
8408.1b01.2941	192.168.1.91	N/A	AP03_Sotao_9548
0c8b.9509.3518	192.168.1.129	N/A	AP03_Sotao_9548
0012.17e2.4b40	192.168.1.31	fe80::212:17f:fe2:4b40	AP04_Outdoor_3DC8
0012.17e2.4856	192.168.1.37	fe80::212:17f:fe2:4856	AP05_Outdoor_2200
0012.17e1.dd57	192.168.1.133	fe80::212:17f:fe1:dd57	AP03_Sotao_9548

The detailed view of the selected client (Client MAC: 2495.2f72.8a66) shows the following information:

- Client State Servers:** None
- Client ACLs:** None
- Client Entry Create Time:** 83 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: 000000000000FB58AED363
  - Acct Session ID: 0X00000000
  - Auth Method Status List: SAE
  - Method: SAE

## Samsung S23

## Verbindung OTA mit Fokus auf RSN-Informationen vom Client:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
773	2023-06-12 17:26:55.727215	0.000000	Samsung_C9-0371	Cisco_31180-1	Broadcast	802.11	194	-45 dBm	Authentication, S/W=176, P/W=0, Flags=.....C
774	2023-06-12 17:26:55.727215	0.000000	192.168.1.15	192.168.1.121	802.11	76	-38 dBm	Acknowledgment, Flags=.....C	
775	2023-06-12 17:26:55.734513	0.000038	Cisco_31180-1	Samsung_C9-0371	802.11	194	-37 dBm	Authentication, S/W=126, P/W=0, Flags=.....C	
776	2023-06-12 17:26:55.734513	0.000000	192.168.1.15	192.168.1.121	802.11	76	-45 dBm	Acknowledgment, Flags=.....C	
777	2023-06-12 17:26:55.742809	0.000316	Samsung_C9-0371	Cisco_31180-1	Broadcast	802.11	139	-43 dBm	Authentication, S/W=177, P/W=0, Flags=.....C
778	2023-06-12 17:26:55.742809	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
780	2023-06-12 17:26:55.743197	0.002123	Cisco_31180-1	Samsung_C9-0371	802.11	139	-36 dBm	Authentication, S/W=127, P/W=0, Flags=.....C	
781	2023-06-12 17:26:55.743197	0.000000	192.168.1.15	192.168.1.121	802.11	76	-43 dBm	Acknowledgment, Flags=.....C	
782	2023-06-12 17:26:55.748041	0.004544	Samsung_C9-0371	Cisco_31180-1	Broadcast	802.11	194	-45 dBm	Association Request, S/W=178, P/W=0, Flags=.....C, SSID="wifid_test"
783	2023-06-12 17:26:55.748041	0.000000	192.168.1.15	192.168.1.121	802.11	76	-36 dBm	Acknowledgment, Flags=.....C	
787	2023-06-12 17:26:55.758131	0.010275	Samsung_C9-0371	Broadcast	LLC	114	-37 dBm	I, N(1)<N(1), N(1)>: SSAP 130 Network Layer (unofficial) Group, SSAP Banyan VME	
788	2023-06-12 17:26:55.758131	0.000000	Samsung_C9-0371	Broadcast	LLC	114	-36 dBm	Association Response, S/W=0, P/W=0, Flags=.....C	
789	2023-06-12 17:26:55.763192	0.002876	Cisco_31180-1	Samsung_C9-0371	802.11	236	-36 dBm	Authentication Response, S/W=0, P/W=0, Flags=.....C	
790	2023-06-12 17:26:55.763192	0.000000	192.168.1.15	192.168.1.121	802.11	76	-44 dBm	Acknowledgment, Flags=.....C	
792	2023-06-12 17:26:55.762296	0.001184	Cisco_31180-1	Samsung_C9-0371	EAPOL	223	-36 dBm	Key (message 1 of 4)	
793	2023-06-12 17:26:55.762296	0.000000	192.168.1.15	192.168.1.121	802.11	76	-44 dBm	Acknowledgment, Flags=.....C	
795	2023-06-12 17:26:55.791219	0.028823	Samsung_C9-0371	Cisco_31180-1	EAPOL	230	-43 dBm	Key (message 2 of 4)	
796	2023-06-12 17:26:55.791219	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
797	2023-06-12 17:26:55.793800	0.001781	Cisco_31180-1	Samsung_C9-0371	EAPOL	295	-37 dBm	Key (message 3 of 4)	
798	2023-06-12 17:26:55.793800	0.000000	192.168.1.15	192.168.1.121	802.11	76	-44 dBm	Acknowledgment, Flags=.....C	
799	2023-06-12 17:26:55.798403	0.000483	Samsung_C9-0371	Cisco_31180-1	EAPOL	199	-44 dBm	Key (message 4 of 4)	

## Client-Details in WLC:

Cisco Catalyst 9800-CL Wireless Controller 17.9.3

Welcome admin

Search APs and Clients

Feedback

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Delete

Selected 0 out of 12 Clients

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

Client

360 View General QoS Statistics ATF Statistics Mobility History Call Statistics

Client Properties AP Properties Security Information Client Statistics QoS Properties EoGRE

Client State Servers None

Client ACLs None

Client Entry Create Time 78 seconds

Policy Type WPA3

Encryption Cipher CCMP (AES)

Authentication Key Management SAE

EAP Type Not Applicable

Session Timeout 86400

Session Manager

Point of Attachment capwap\_90000010

IF ID 0x90000010

Authorized TRUE

Common Session ID 000000000000FB1B0A58F78

Acct Session ID 0x00000000

Auth Method Status List

Method SAE

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

WLAN-Sicherheitskonfiguration:

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

General **Security** Advanced Add To Policy Tags

**Layer2** Layer3 AAA

WPA + WPA2  WPA2 + WPA3  WPA3  Static WEP  None

MAC Filtering

Lobby Admin Access

WPA Parameters

WPA Policy  WPA2 Policy   
 GTK Randomize  WPA3 Policy   
 Transition Disable

Fast Transition

Status  ▾  
 Over the DS   
 Reassociation Timeout \*

WPA2/WPA3 Encryption

AES(OCMP128)  CCMP256   
 GCMP128  GCMP256

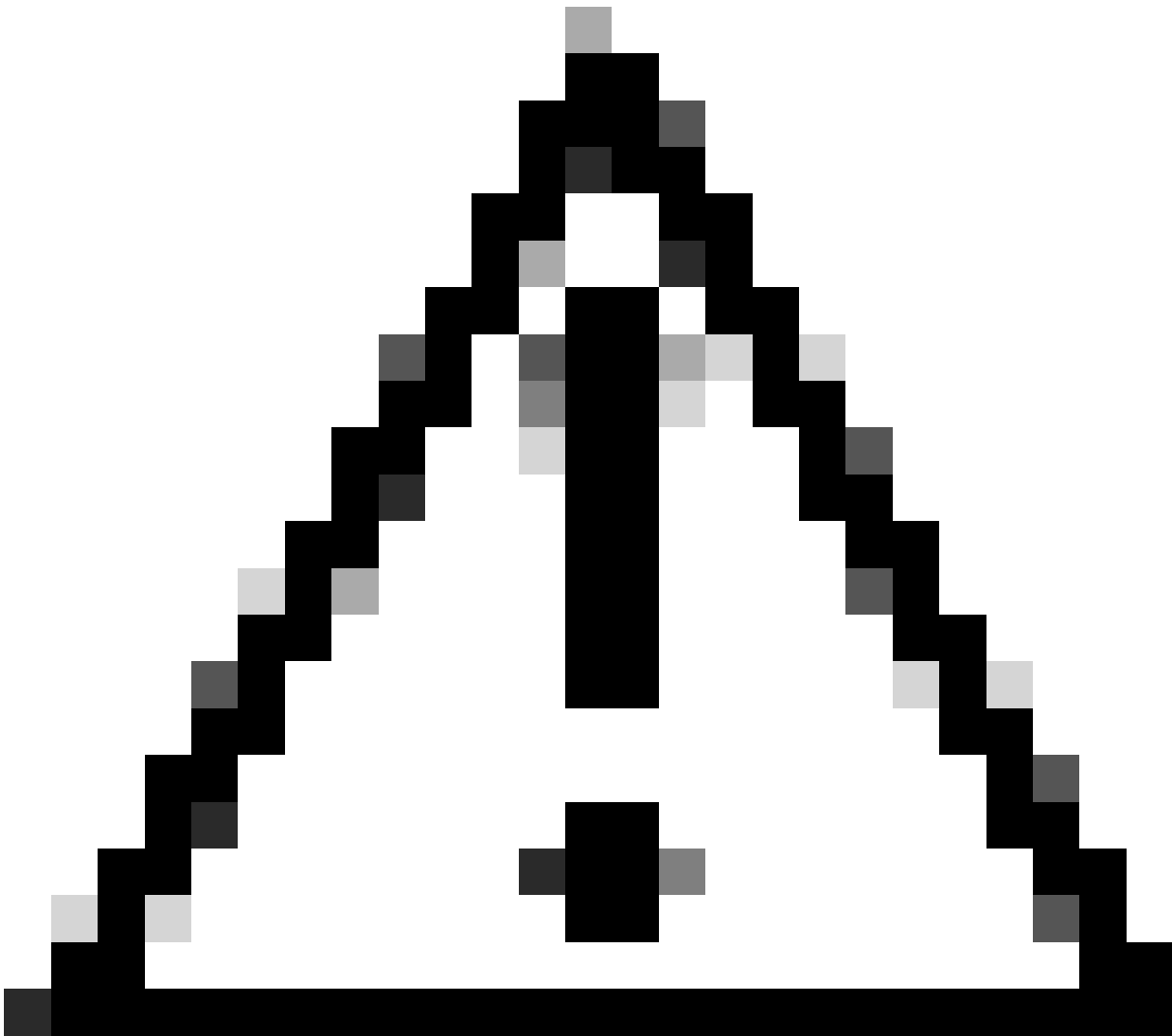
Auth Key Mgmt

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

Protected Management Frame

PMF  ▾  
 Association Comeback Timer\*   
 SA Query Time\*





Vorsicht: Bei der Verwaltung von Authentifizierungsschlüsseln kann der WLC FT+SAE auswählen, ohne dass SAE aktiviert ist. Es wurde jedoch beobachtet, dass die Clients keine Verbindung herstellen konnten. Aktivieren Sie immer beide Kontrollkästchen SAE und FT+SAE, wenn Sie SAE mit Fast Transition verwenden möchten.

---

Auf der WLC-GUI der WLAN-Sicherheitseinstellungen anzeigen:

wfGE\_test 5 wfGE\_test [WPA3][SAE][FT + SAE][AES][FT Enabled]

Verifizierung von Beacons OTA:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
1	2023-06-12 18:34:49.35337	0.000000	Cisco_13:180:e7	Eurocast	802.11	588	5	-36 dBm	Beacon frame, S/W=22, F/W=, Flags=.....C, IE=100, SSID="wifi6e"
2	2023-06-12 18:34:49.42754	0.102287	Cisco_13:180:e7	Eurocast	802.11	588	5	-36 dBm	Beacon frame, S/W=27, F/W=, Flags=.....C, IE=100, SSID="wifi6e"
3	2023-06-12 18:34:49.55857	0.102287	Cisco_13:180:e7	Eurocast	802.11	588	5	-37 dBm	Beacon frame, S/W=23, F/W=, Flags=.....C, IE=100, SSID="wifi6e"
4	2023-06-12 18:34:49.62332	0.102465	Cisco_13:180:e7	Eurocast	802.11	588	5	-37 dBm	Beacon frame, S/W=27, F/W=, Flags=.....C, IE=100, SSID="wifi6e"
5	2023-06-12 18:34:49.79180	0.099672	Netgear_48:78:35	Cisco_13:180:e7	802.11	360	5	-49 dBm	Probe Request, S/W=18, F/W=, Flags=.....C, SSID="wifi6e_test"
6	2023-06-12 18:34:49.79180	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-37 dBm	Acknowledgment, Flags=.....C
7	2023-06-12 18:34:49.79180	0.000000	192.168.1.15	192.168.1.121	802.11	360	5	-49 dBm	Probe Request, S/W=11, F/W=, Flags=.....C, SSID="wifi6e_test"
8	2023-06-12 18:34:49.79180	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-37 dBm	Acknowledgment, Flags=.....C
9	2023-06-12 18:34:49.79493	0.003066	Cisco_13:180:e7	Eurocast	802.11	588	5	-37 dBm	Beacon frame, S/W=22, F/W=, Flags=.....C, IE=100, SSID="wifi6e"
10	2023-06-12 18:34:49.81282	0.015789	Netgear_48:78:35	Cisco_13:180:e7	802.11	360	5	-49 dBm	Probe Request, S/W=11, F/W=, Flags=.....C, SSID="wifi6e_test"
11	2023-06-12 18:34:49.81282	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-37 dBm	Acknowledgment, Flags=.....C
12	2023-06-12 18:34:49.87491	0.000000	192.168.1.15	192.168.1.121	802.11	194	5	-49 dBm	Authentication, S/W=6, F/W=, Flags=.....C
13	2023-06-12 18:34:49.87491	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-37 dBm	Acknowledgment, Flags=.....C
14	2023-06-12 18:34:49.89653	0.021612	Cisco_13:180:e7	Netgear_48:78:35	802.11	194	5	-37 dBm	Authentication, S/W=6, F/W=, Flags=.....C
15	2023-06-12 18:34:49.89653	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-49 dBm	Acknowledgment, Flags=.....C
16	2023-06-12 18:34:49.90496	0.000000	Cisco_13:180:e7	Eurocast	802.11	588	5	-37 dBm	Beacon frame, S/W=27, F/W=, Flags=.....C, IE=100, SSID="wifi6e"
17	2023-06-12 18:34:49.90496	0.000000	Netgear_48:78:35	Cisco_13:180:e7	802.11	130	5	-49 dBm	Authentication, S/W=6, F/W=, Flags=.....C
18	2023-06-12 18:34:49.90496	0.000000	192.168.1.15	192.168.1.121	802.11	130	5	-37 dBm	Authentication, S/W=7, F/W=, Flags=.....C
19	2023-06-12 18:34:49.90496	0.000000	Cisco_13:180:e7	Eurocast	802.11	588	5	-37 dBm	Beacon frame, S/W=27, F/W=, Flags=.....C, IE=100, SSID="wifi6e"
20	2023-06-12 18:34:49.90496	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-48 dBm	Acknowledgment, Flags=.....C
21	2023-06-12 18:34:49.90496	0.000000	Netgear_48:78:35	Cisco_13:180:e7	802.11	216	5	-49 dBm	Association Request, S/W=6, F/W=, Flags=.....C, SSID="wifi6e_test"
22	2023-06-12 18:34:49.90496	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
23	2023-06-12 18:34:49.91474	0.005180	Cisco_13:180:e7	Netgear_48:78:35	802.11	262	5	-36 dBm	Association Response, S/W=6, F/W=, Flags=.....C
24	2023-06-12 18:34:49.91474	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-49 dBm	Acknowledgment, Flags=.....C
25	2023-06-12 18:34:49.91719	0.000245	Netgear_48:78:35	Eurocast	LLC	114	5	-37 dBm	U, func:unknown; DSAP 0x12 Individual, SSAP 0x02 Command
26	2023-06-12 18:34:49.91719	0.000000	Netgear_48:78:35	Eurocast	LLC	114	5	-36 dBm	U, func:unknown; DSAP 0x7a Individual, SSAP 0x0a Response
27	2023-06-12 18:34:49.92236	0.010267	Cisco_13:180:e7	Netgear_48:78:35	EAPOL	221	5	-36 dBm	Key (Message 1 of 4)
28	2023-06-12 18:34:49.92236	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-49 dBm	Acknowledgment, Flags=.....C
29	2023-06-12 18:34:49.99951	0.077235	Cisco_13:180:e7	Eurocast	802.11	588	5	-36 dBm	Beacon frame, S/W=27, F/W=, Flags=.....C, IE=100, SSID="wifi6e"
30	2023-06-12 18:34:50.10458	0.104029	Cisco_13:180:e7	Eurocast	802.11	588	5	-36 dBm	Beacon frame, S/W=27, F/W=, Flags=.....C, IE=100, SSID="wifi6e"
31	2023-06-12 18:34:50.20460	0.100000	Cisco_13:180:e7	Eurocast	802.11	588	5	-48 dBm	Beacon frame, S/W=22, F/W=, Flags=.....C, IE=100, SSID="wifi6e"
32	2023-06-12 18:34:50.21161	0.007615	Netgear_48:78:35	Cisco_13:180:e7	EAPOL	226	5	-55 dBm	Key (Message 2 of 4)
33	2023-06-12 18:34:50.21161	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-42 dBm	Acknowledgment, Flags=.....C
34	2023-06-12 18:34:50.21161	0.000000	Netgear_48:78:35	Eurocast	EAPOL	296	5	-48 dBm	Key (Message 3 of 4)
35	2023-06-12 18:34:50.21376	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-58 dBm	Acknowledgment, Flags=.....C
36	2023-06-12 18:34:50.21454	0.000978	Netgear_48:78:35	Cisco_13:180:e7	EAPOL	199	5	-56 dBm	Key (Message 4 of 4)
37	2023-06-12 18:34:50.21454	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-42 dBm	Acknowledgment, Flags=.....C
38	2023-06-12 18:34:50.22072	0.006367	192.168.1.15	192.168.1.121	802.11	76	5	-42 dBm	Acknowledgment, Flags=.....C
39	2023-06-12 18:34:50.22489	0.003128	192.168.1.15	192.168.1.121	802.11	119	5	-44 dBm	Trigger Buffer Status Report Poll (BSRP), Flags=.....C
40	2023-06-12 18:34:50.22489	0.000000	Netgear_48:78:35	Eurocast	LLC	221	5	-44 dBm	U, func:unknown; DSAP 0x0b Group, SSAP 0x0d Response
41	2023-06-12 18:34:50.22489	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-54 dBm	Acknowledgment, Flags=.....C

## WPA3 SAE + FT Beacons

Hier können wir beobachten, wie Wi-Fi 6E-Clients sich verbinden:

Intel AX211

Verbindung OTA mit Fokus auf RSN-Informationen vom Client:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
1811	2023-06-12 18:51:39.24979	0.017137	IntelCorp_98:58:5f	Cisco_13:180:e7	802.11	194	5	-42 dBm	Authentication, S/W=6, F/W=, Flags=.....C
1812	2023-06-12 18:51:39.24979	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1813	2023-06-12 18:51:39.254827	0.007634	Cisco_13:180:e7	IntelCorp_98:58:5f	802.11	194	5	-36 dBm	Authentication, S/W=59, F/W=, Flags=.....C
1814	2023-06-12 18:51:39.254827	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-42 dBm	Acknowledgment, Flags=.....C
1815	2023-06-12 18:51:39.259394	0.002567	IntelCorp_98:58:5f	Cisco_13:180:e7	802.11	130	5	-48 dBm	Authentication, S/W=1, F/W=, Flags=.....C
1816	2023-06-12 18:51:39.259394	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1817	2023-06-12 18:51:39.263479	0.004235	Cisco_13:180:e7	IntelCorp_98:58:5f	802.11	130	5	-36 dBm	Authentication, S/W=6, F/W=, Flags=.....C
1818	2023-06-12 18:51:39.263479	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-42 dBm	Acknowledgment, Flags=.....C
1819	2023-06-12 18:51:39.263479	0.000000	IntelCorp_98:58:5f	Cisco_13:180:e7	802.11	250	5	-46 dBm	Association Request, S/W=2, F/W=, Flags=.....C, SSID="wifi6e_test"
1820	2023-06-12 18:51:39.263479	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1821	2023-06-12 18:51:39.271442	0.018463	IntelCorp_98:58:5f	Eurocast	LLC	114	5	-36 dBm	I, W(K)M, N(S)=1; DSAP 0x0a Group, SSAP 0x0a Response
1822	2023-06-12 18:51:39.271442	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-43 dBm	Acknowledgment, Flags=.....C
1823	2023-06-12 18:51:39.277402	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-43 dBm	Acknowledgment, Flags=.....C
1824	2023-06-12 18:51:39.277402	0.001268	Cisco_13:180:e7	IntelCorp_98:58:5f	802.11	262	5	-36 dBm	Association Response, S/W=6, F/W=, Flags=.....C
1825	2023-06-12 18:51:39.277402	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-43 dBm	Acknowledgment, Flags=.....C
1826	2023-06-12 18:51:39.28187	0.004705	Cisco_13:180:e7	Eurocast	802.11	517	5	-36 dBm	Beacon frame, S/W=71, F/W=, Flags=.....C, IE=100, SSID="wifi6e_test_02"
1827	2023-06-12 18:51:39.28187	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1828	2023-06-12 18:51:39.311349	0.025242	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1829	2023-06-12 18:51:39.311349	0.004549	192.168.1.15	192.168.1.121	802.11	76	5	-52 dBm	Clear-to-send, Flags=.....C
1830	2023-06-12 18:51:39.311349	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-52 dBm	Clear-to-send, Flags=.....C
1831	2023-06-12 18:51:39.334245	0.017227	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1832	2023-06-12 18:51:39.334245	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1833	2023-06-12 18:51:39.338468	0.055035	Cisco_13:180:e7	Eurocast	802.11	517	5	-37 dBm	Beacon frame, S/W=76, F/W=, Flags=.....C, IE=100, SSID="wifi6e_test_02"
1834	2023-06-12 18:51:39.338468	0.001348	192.168.1.15	192.168.1.121	802.11	76	5	-53 dBm	Clear-to-send, Flags=.....C
1835	2023-06-12 18:51:39.338468	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-38 dBm	Request-to-send, Flags=.....C
1836	2023-06-12 18:51:39.339382	0.001839	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1837	2023-06-12 18:51:39.339382	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1838	2023-06-12 18:51:39.339382	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1839	2023-06-12 18:51:39.339382	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1840	2023-06-12 18:51:39.339382	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1841	2023-06-12 18:51:39.339382	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1842	2023-06-12 18:51:39.339382	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1843	2023-06-12 18:51:39.339382	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1844	2023-06-12 18:51:39.339382	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1845	2023-06-12 18:51:39.339382	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1846	2023-06-12 18:51:39.339382	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 18:51:39.339382	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1848	2023-06-12 18:51:39.339382	0.000000	19						





## Client-Details in WLC:

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main area is titled 'Monitoring > Wireless > Clients'. Below this, there are tabs for 'Clients', 'Sleeping Clients', and 'Excluded Clients'. A table lists 13 clients with columns for Client MAC Address, IPv4 Address, IPv6 Address, and AP Name. The first client is selected. The right pane shows the 'Client' details for this client, with tabs for 'General', 'QoS Statistics', 'ATF Statistics', 'Mobility History', and 'Call Statistics'. The 'Security Information' tab is active, showing details like Client State Servers, Client ACLs, Client Entry Create Time, Policy Type, Encryption Cipher, Authentication Key Management, EAP Type, Session Timeout, Session Manager, Point of Attachment, IIF ID, Authorized, Common Session ID, Acct Session ID, Auth Method Status List, and Method.

Pixel 6a

Das Gerät konnte kein Roaming durchführen, wenn FT aktiviert ist.

Samsung S23

Das Gerät konnte kein Roaming durchführen, wenn FT aktiviert ist.

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

WLAN-Sicherheitskonfiguration:

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main area is titled 'Configuration > Tags & Profiles > WLANs'. Below this, there are tabs for 'Add', 'Delete', 'Clone', 'Enable WLAN', and 'Disable WLAN'. A table lists 5 WLANs with columns for Status, Name, and ID. The 'wif6E\_test' WLAN is selected. The right pane shows the 'Edit WLAN' configuration for this WLAN, with tabs for 'General', 'Security', 'Advanced', and 'Add To Policy Tags'. The 'Security' tab is active, showing 'Layer2' settings. The 'Security' section includes 'WPA Parameters' (WPA3 selected), 'WPA2/WPA3 Encryption' (AES/CCMP128 and CCMP256 selected), and 'Protected Management Frame' (PMF Required). The 'Auth Key Mgmt' section is highlighted with a red box, showing 'SAE' and 'FT + SAE' selected, and 'OWE' and 'FT + 802.1x' unselected.

WPA3 Enterprise 802.1x-SHA256 + FT WLAN-Sicherheitskonfiguration

Auf der WLC-GUI der WLAN-Sicherheitseinstellungen anzeigen:

The screenshot shows the status bar at the bottom of the Cisco Catalyst 9800-CL Wireless Controller interface. It displays the WLAN name 'wif6E\_test' and the ID '5'. The security configuration is shown as '[WPA3][FT + 802.1x][AES][PMF 802.1x][FT Enabled]'. The 'FT + 802.1x' part is highlighted with a red box.

Hier sehen Sie die ISE-Live-Protokolle mit den Authentifizierungen der einzelnen Geräte:



Ein interessantes Verhalten tritt auf, wenn Sie den Client manuell aus dem WLAN löschen (z.B. aus der WLC GUI). Der Client empfängt einen Trennungs-Frame, versucht jedoch, erneut eine Verbindung mit demselben Access Point herzustellen, und verwendet einen Trennungs-Frame, gefolgt von einem vollständigen EAP-Austausch, da die Client-Details vom Access Point/WLC gelöscht wurden.

Das ist im Grunde der gleiche Rahmenaustausch wie in einem neuen Assoziationsprozess. Hier sehen Sie den Frame-Austausch:

The image shows a Wireshark packet capture of a client re-associating with an access point. The capture is divided into several sections:

- Probing and authentication frames:** Includes frames 153-161, showing Probe Request, Probe Response, Authentication Request, and Authentication Response.
- Regular Association:** Includes frames 162-170, showing Association Request, Association Response, and the start of the EAP-PEAP exchange.
- EAP Exchange:** Includes frames 171-200, showing the EAP-PEAP handshake, including the EAP-Request (Protected EAP), EAP-Response (Protected EAP), and EAP-Request (Protected EAP).
- 4 Way Handshake:** Includes frames 201-204, showing the 4-way handshake (EAP-Request (Protected EAP), EAP-Response (Protected EAP), EAP-Request (Protected EAP), and EAP-Response (Protected EAP)).

Red boxes highlight the EAP-Request (Protected EAP) frame (frame 171) and the EAP-Response (Protected EAP) frame (frame 172), with a note: "PMKID used for FT".

WPA3 Enterprise 802.1x + FT AX211-Verbindungsablauf

Client-Details in WLC:

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

- Client:** 360 View, General, QoS Statistics, ATF Statistics, Mobility History, Call Statistics
- Client Properties:** AP Properties, Security Information, Client Statistics, QoS Properties, EoGRE
- Security Information:**
  - 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

Details zum WPA3 Enterprise 802.1x + FT-Client

Dieser Client wurde auch mit FT über den DS getestet und konnte mithilfe von 802.11r Roaming durchführen:



No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
3028	16.492589	0.182243	Cisco_9818-0F	Broadcast	802.11	364	69	-36	dtm Beacon Frame, Src=9817, FwB, Flags=.....C, B1=100, SSID=WiFi
3029	16.504273	0.120828	Cisco_9818-0F	Broadcast	802.11	364	69	-36	dtm Beacon Frame, Src=9817, FwB, Flags=.....C, B1=100, SSID=WiFi
3030	16.564794	0.076523	IntelCor_9818-0F	Broadcast	802.11	368	69	-45	dtm Probe Request, Src=327, FwB, Flags=.....C, SSID=80211C (E
3031	16.564794	0.000000	Cisco_9818-0F	Broadcast	802.11	328	69	-38	dtm Probe Response, Src=400, FwB, Flags=.....C, B1=100, SSID=
3079	16.695629	0.013635	Cisco_9818-0F	Broadcast	802.11	364	69	-38	dtm Beacon Frame, Src=9816, FwB, Flags=.....C, B1=100, SSID=WiFi
3088	16.704545	0.000220	IntelCor_9818-0F	Cisco_9818-0F	802.11	235	69	-46	dtm Authentication, Src=11, FwB, Flags=.....C
3089	16.705142	0.000087	192.168.1.121	192.168.1.121	802.11	76	69	-39	dtm Acknowledgment, Flags=.....C
3092	16.706278	0.004736	192.168.1.121	192.168.1.121	802.11	247	69	-38	dtm Authentication, Src=115, FwB, Flags=.....C
3093	16.706278	0.000000	192.168.1.121	192.168.1.121	802.11	76	69	-39	dtm Acknowledgment, Flags=.....C
3098	16.708297	0.000000	192.168.1.121	192.168.1.121	802.11	372	69	-48	dtm Association Request, Src=327, FwB, Flags=.....C, SSID=WiFi
3099	16.708297	0.000000	192.168.1.121	192.168.1.121	802.11	76	69	-38	dtm Acknowledgment, Flags=.....C
3100	16.718126	0.000020	192.168.1.121	192.168.1.121	802.11	433	69	-39	dtm Association Response, Src=400, FwB, Flags=.....C
3108	16.731226	0.000000	192.168.1.121	192.168.1.121	802.11	76	69	-41	dtm Acknowledgment, Flags=.....C
3092	16.727457	0.000108	192.168.1.15	192.168.1.121	802.11	76	69	-47	dtm Acknowledgment, Flags=.....C
3095	16.748833	0.013376	IntelCor_9818-0F	Broadcast	LLC	525	69	-59	dtm U_P, func=Unknown; DSAP Bkch Individual, SSAP Bkch Command
3096	16.748833	0.000000	192.168.1.121	192.168.1.121	802.11	76	69	-48	dtm Acknowledgment, Flags=.....C
3099	16.742984	0.000071	Cisco_Sc18-0c	IntelCor_9818-0F	LLC	383	69	-50	dtm I_P, N(K)=11, N(S)=72; DSAP Upperm-Bkch Individual, SSAP B
3100	16.742984	0.000000	192.168.1.121	192.168.1.121	802.11	76	69	-53	dtm Acknowledgment, Flags=.....C
3101	16.742984	0.000000	Cisco_Sc18-0c	IntelCor_9818-0F	LLC	383	69	-50	dtm I, N(K)=16, N(S)=75; DSAP SAPP Individual, SSAP Bkch Command
3102	16.742984	0.000000	192.168.1.121	192.168.1.121	802.11	76	69	-53	dtm Acknowledgment, Flags=.....C
3106	16.769880	0.012522	IntelCor_9818-0F	IPwcastc_9818-0F	LLC	223	69	-59	dtm I_P, N(K)=16, N(S)=11; DSAP Bkch Individual, SSAP Bkch Respons
3107	16.769883	0.000124	192.168.1.15	192.168.1.121	802.11	76	69	-48	dtm Acknowledgment, Flags=.....C
3109	16.772475	0.003842	Cisco_9818-0F	IntelCor_9818-0F	802.11	118	69	-48	dtm Action, Src=1, FwB, Flags=.....C
3110	16.772475	0.000000	192.168.1.121	192.168.1.121	802.11	76	69	-52	dtm Acknowledgment, Flags=.....C
3113	16.773242	0.000000	192.168.1.121	192.168.1.121	802.11	179	69	-59	dtm I_P, N(K)=19, N(S)=13; DSAP SAPP Group, SSAP 150 Network Layer
3114	16.773242	0.000000	192.168.1.121	192.168.1.121	802.11	76	69	-48	dtm Acknowledgment, Flags=.....C
3115	16.773242	0.000204	IntelCor_9818-0F	Cisco_9818-0F	802.11	118	69	-48	dtm Action, Src=1, FwB, Flags=.....C [Malformed Packet]
3116	16.773242	0.000000	192.168.1.121	192.168.1.121	802.11	76	69	-41	dtm Acknowledgment, Flags=.....C
3120	16.779112	0.000000	192.168.1.121	192.168.1.121	802.11	118	69	-48	dtm Action, Src=1, FwB, Flags=.....C
3122	16.779545	0.001433	IntelCor_9818-0F	IntelCor_9818-0F	802.11	118	69	-48	dtm Action, Src=2, FwB, Flags=.....C
3123	16.779545	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-52	dtm Acknowledgment, Flags=.....C
3124	16.779599	0.001854	IntelCor_9818-0F	Cisco_9818-0F	802.11	118	69	-48	dtm Action, Src=3, FwB, Flags=.....C [Malformed Packet: length
3125	16.779599	0.000000	192.168.1.121	192.168.1.121	802.11	76	69	-48	dtm Acknowledgment, Flags=.....C
3128	16.781489	0.003058	AttiCor_9818-0F	IntelCor_9818-0F	LLC	197	69	-49	dtm U_P, func=Unknown; DSAP Bkch Individual, SSAP Bkch Command
3132	16.781489	0.000000	192.168.1.121	192.168.1.121	802.11	222	69	-58	dtm U, func=Unknown; DSAP Bkch Group, SSAP Bkch Command
3133	16.781489	0.000000	192.168.1.121	192.168.1.121	802.11	76	69	-47	dtm Acknowledgment, Flags=.....C
3136	16.790628	0.000000	192.168.1.121	192.168.1.121	802.11	223	69	-59	dtm I_P, N(K)=19, N(S)=13; DSAP SAPP Group, SSAP 150 Network Layer
3137	16.790615	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-47	dtm Acknowledgment, Flags=.....C
3140	16.793424	0.002599	IntelCor_9818-0F	Broadcast	LLC	525	69	-58	dtm I, N(K)=8, N(S)=22; DSAP HP Extended LLC Group, SSAP NetWare
3141	16.793477	0.000000	192.168.1.121	192.168.1.121	802.11	76	69	-47	dtm Acknowledgment, Flags=.....C
3144	16.793774	0.000027	IntelCor_9818-0F	Broadcast	LLC	179	69	-58	dtm I, func=Unknown; DSAP Bkch Individual, SSAP Bkch Respons
3145	16.793849	0.000075	192.168.1.15	192.168.1.121	802.11	76	69	-48	dtm Acknowledgment, Flags=.....C
3149	16.794563	0.000714	IntelCor_9818-0F	IPwcastc_9818-0F	LLC	383	69	-58	dtm I_P, N(K)=12, N(S)=13; DSAP Bkch Group, SSAP Bkch Respons
3150	16.794620	0.000000	192.168.1.121	192.168.1.121	802.11	76	69	-48	dtm Acknowledgment, Flags=.....C
3151	16.794628	0.000000	IntelCor_9818-0F	IPwcastc_9818-0F	LLC	383	69	-58	dtm I_P, N(K)=13, N(S)=13; DSAP Bkch Group, SSAP Bkch Respons
3155	16.794909	0.000064	192.168.1.15	192.168.1.121	802.11	76	69	-48	dtm Acknowledgment, Flags=.....C
3158	16.795624	0.000624	IntelCor_9818-0F	IPwcastc_9818-0F	LLC	235	69	-58	dtm U_P, func=Unknown; DSAP MALL LSAP Individual, SSAP Banyan View
3229	16.995959	0.000000	192.168.1.121	192.168.1.121	802.11	76	69	-48	dtm Acknowledgment, Flags=.....C
3248	16.995958	0.000000	IntelCor_9818-0F	IPwcastc_9818-0F	LLC	235	69	-58	dtm U, func=Unknown; DSAP Bkch Group, SSAP Bkch Respons
3262	16.995852	0.000007	192.168.1.15	192.168.1.121	802.11	76	69	-48	dtm Acknowledgment, Flags=.....C

### AX211-Roaming mit FT über DS

Außerdem werden die Roaming-Ereignisse der FT angezeigt:

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
2866.3598.580F	192.168.1.159	N/A	AP01_RC_9136_F80C	wifi6_test	5	WLAN

Client

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

Recent association history:

AP Name	BSSID	AP Slot	Assoc Time	Instance	Mobility Role	Run Latency (ms)	Roam Type
AP01_RC_9136_F80C	00d1.1d8d.a018	3	08/04/2023 14:24:27	0	Local	15	802.11R
AP9136_5C_F524	00d1.1d8d.7d38	3	08/04/2023 14:22:59	0	Local	6	802.11R

### WPA3 Enterprise mit FT

Client-RA-Trace von wlc:

```

Logging display requested on 2023/08/04 14:27:55 (GMT) for Hostname: [wlc0-9800-01], Model: [C9500-CL-F91, Version: [17.09.03], SN: [59Y3SR1909], MD_SN: [59Y3SR1909]
2023/08/04 14:22:59.3185623 [wmlc_w_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Re-Association Received. BSSID 00d1.1d8d.7d38, WLAN wlc6_test, Slot 3 AP 00d1.1d8d.7d38, AP9136_5C_F524, old BSSID 00d1.1d8d.a018
2023/08/04 14:22:59.3185623 [wmlc_w_0-0] (1): [dot11] [15218]: (note) MAC: 286b.3598.580f Re-Association Received. BSSID 00d1.1d8d.7d38, WLAN wlc6_test, Slot 3 AP 00d1.1d8d.7d38, AP9136_5C_F524, old BSSID 00d1.1d8d.a018
2023/08/04 14:22:59.3184912 [wmlc_w_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Delete mobile payload sent for BSSID: 00d1.1d8d.a018 WTP mac: 00d1.1d8d.a018 slot id: 3
2023/08/04 14:22:59.3184912 [wmlc_w_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Client state transition: S_CO_RSN --> S_CO_L2_AUTH_IN_PROGRESS
2023/08/04 14:22:59.317320574 [wmlc_w_0-0] (1): [client-auth] [15218]: (note) MAC: 286b.3598.580f ADO Mobile sent. Client state flags: 0x71 BSSID: MAC: 00d1.1d8d.7d38 capwap IFID: 0x00000000, Add mobiles sent: 1
2023/08/04 14:22:59.321041967 [wmlc_w_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Mobility discovery triggered. Client mode: Local
2023/08/04 14:22:59.321041967 [wmlc_w_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Client state transition: S_CO_L2_AUTH_IN_PROGRESS --> S_CO_MOBILITY_DISCOVERY_IN_PROGRESS
2023/08/04 14:22:59.321041967 [wmlc_w_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Mobility Successful. Roam Type Home, Sub Roam Type HM_SUB_ROAM_TYPE_INTRA_INSTANCE, Previous BSSID MAC: 00d1.1d8d.a018 Client IFID: 0x00000000, Client Role: Local Pk: 0x00000000 Pop: 0x0
2023/08/04 14:22:59.32113992 [wmlc_w_0-0] (1): [client-auth] [15218]: (note) MAC: 286b.3598.580f ADO MOBILE sent. Client state flags: 0x76 BSSID: MAC: 00d1.1d8d.7d38 capwap IFID: 0x00000000, Add mobiles sent: 1
2023/08/04 14:22:59.32113992 [wmlc_w_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Client state transition: S_CO_MOBILITY_DISCOVERY_IN_PROGRESS --> S_CO_DEATH_PLUMB_IN_PROGRESS
2023/08/04 14:22:59.321463455 [wmlc_w_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Client state transition: S_CO_DEATH_PLUMB_IN_PROGRESS --> S_CO_IP_LEARN_IN_PROGRESS
2023/08/04 14:22:59.321463455 [wmlc_w_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Client state transition: S_CO_IP_LEARN_IN_PROGRESS --> S_CO_RSN
2023/08/04 14:24:17.918585521 [wmlc_w_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Client state transition: S_CO_L2_AUTH_IN_PROGRESS --> S_CO_IP_LEARN_IN_PROGRESS
2023/08/04 14:24:17.918585521 [wmlc_w_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Re-Association Received. BSSID 00d1.1d8d.a018, WLAN wlc6_test, Slot 3 AP 00d1.1d8d.a018, AP01_RC_9136_F80C, old BSSID 00d1.1d8d.7d38
2023/08/04 14:24:17.91897444 [wmlc_w_0-0] (1): [dot11] [15218]: (note) MAC: 286b.3598.580f Association success. AID 33, Roaming = True, WGB = False, llc = True, llw = True Fast roam = True
2023/08/04 14:24:17.91897444 [wmlc_w_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Delete mobile payload sent for BSSID: 00d1.1d8d.7d38 WTP mac: 00d1.1d8d.7d38 slot id: 3
2023/08/04 14:24:17.91897444 [wmlc_w_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Client state transition: S_CO_RSN --> S_CO_L2_AUTH_IN_PROGRESS
2023/08/04 14:24:17.91897444 [wmlc_w_0-0] (1): [client-auth] [15218]: (note) MAC: 286b.3598.580f ADO MOBILE sent. Client state flags: 0x71 BSSID: MAC: 00d1.1d8d.a018 capwap IFID: 0x00000000, Add mobiles sent: 1
2023/08/04 14:24:17.91897444 [wmlc_w_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Mobility discovery triggered. Client mode: Local
2023/08/04 14:24:17.91897444 [wmlc_w_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Client state transition: S_CO_L2_AUTH_IN_PROGRESS --> S_CO_MOBILITY_DISCOVERY_IN_PROGRESS
2023/08/04 14:24:17.91897444 [wmlc_w_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Mobility Successful. Roam Type Home, Sub Roam Type HM_SUB_ROAM_TYPE_INTRA_INSTANCE, Previous BSSID MAC: 00d1.1d8d.7d38 Client IFID: 0x00000000, Client Role: Local Pk: 0x00000000 Pop: 0x0
2023/08/04 14:24:17.91913132 [wmlc_w_0-0] (1): [client-auth] [15218]: (note) MAC: 286b.3598.580f ADO MOBILE sent. Client state flags: 0x76 BSSID: MAC: 00d1.1d8d.a018 capwap IFID: 0x00000000, Add mobiles sent: 1
2023/08/04 14:24:17.91913132 [wmlc_w_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Client state transition: S_CO_MOBILITY_DISCOVERY_IN_PROGRESS --> S_CO_DEATH_PLUMB_IN_PROGRESS
2023/08/04 14:24:17.91913132 [wmlc_w_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Client state transition: S_CO_DEATH_PLUMB_IN_PROGRESS --> S_CO_IP_LEARN_IN_PROGRESS
2023/08/04 14:24:17.91913132 [wmlc_w_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Client state transition: S_CO_IP_LEARN_IN_PROGRESS --> S_CO_RSN

```

### NetGear A8000

WPA3-Enterprise wird auf diesem Client nicht unterstützt.

Pixel 6a

Verbindung OTA mit Fokus auf RSN-Informationen vom Client:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info	
878	1.408897	0.000000	192.168.1.15	Broadcast	802.11	428	69	-17	dm Beacon frame, SN=3686, FwB, Flags=.....C, BI=100, SSID=W	
879	1.409032	0.132370	Cisco_08:00:18	Broadcast	802.11	208	69	-17	dm Probe Request, SN=3686, FwB, Flags=.....C, SSID=W, F	
880	1.409167	0.000405	Cisco_08:00:18	Broadcast	802.11	428	69	-17	dm Beacon frame, SN=3686, FwB, Flags=.....C, BI=100, SSID=W	
882	1.408778	0.000716	Cisco_08:00:18	Broadcast	802.11	374	69	-17	dm Probe Response, SN=3686, FwB, Flags=.....C, BI=100, SSID=W	
928	1.675576	0.114990	Cisco_08:00:18	Broadcast	802.11	428	69	-17	dm Beacon frame, SN=3686, FwB, Flags=.....C, BI=100, SSID=W	
932	1.675989	0.000000	192.168.1.15	Broadcast	802.11	76	69	-17	dm Acknowledgment, Flags=.....C	
933	1.675989	0.000000	192.168.1.15	Broadcast	802.11	76	69	-17	dm Acknowledgment, Flags=.....C	
923	1.679651	0.003842	Cisco_08:00:18	Broadcast	802.11	108	69	-17	dm Authentication, SN=34, FwB, Flags=.....C	
924	1.679651	0.000000	192.168.1.15	Broadcast	802.11	76	69	-17	dm Acknowledgment, Flags=.....C	
925	1.682828	0.003170	Cisco_08:00:18	Broadcast	802.11	202	69	-17	dm Association Request, SN=3686, FwB, Flags=.....C, SSID=W	
926	1.682828	0.000000	192.168.1.15	Broadcast	802.11	76	69	-17	dm Acknowledgment, Flags=.....C	
930	1.782521	0.002370	Cisco_08:00:18	Broadcast	802.11	312	69	-17	dm Association Response, SN=36, FwB, Flags=.....C	
931	1.782521	0.000000	192.168.1.15	Broadcast	802.11	76	69	-17	dm Acknowledgment, Flags=.....C	
932	1.782629	0.000620	Cisco_08:00:18	Broadcast	802.11	309	69	-17	dm Request, Identity	
933	1.782629	0.000000	192.168.1.15	Broadcast	802.11	76	69	-17	dm Acknowledgment, Flags=.....C	
939	1.747377	0.017007	Google_72:8a:96	EAP	113	69	-13	dm	Response, Identity	
940	1.747377	0.000000	192.168.1.15	Broadcast	802.11	76	69	-17	dm Acknowledgment, Flags=.....C	
942	1.78424	0.012047	Cisco_08:00:18	EAP	110	69	-17	dm	Request, Protected EAP (EAP-PEAP)	
943	1.78424	0.000000	192.168.1.15	Broadcast	802.11	76	69	-17	dm Acknowledgment, Flags=.....C	
945	1.788956	0.005672	Cisco_08:00:18	Broadcast	802.11	428	69	-17	dm Beacon frame, SN=3686, FwB, Flags=.....C, BI=100, SSID=W	
946	1.788956	0.000180	Google_72:8a:96	LLC	124	69	-17	dm	1, N(1)>0, N(5)>1; SOAP: SOAP Individual, SOAP Network Response	
949	1.794517	0.015671	Cisco_08:00:18	EAP	110	69	-17	dm	Request, Protected EAP (EAP-PEAP)	
950	1.794517	0.000000	192.168.1.15	Broadcast	802.11	76	69	-17	dm Acknowledgment, Flags=.....C	
956	1.794529	0.015801	Cisco_08:00:18	EAP	1116	69	-17	dm	Request, Protected EAP (EAP-PEAP)	
957	1.794529	0.000000	192.168.1.15	Broadcast	802.11	76	69	-17	dm Acknowledgment, Flags=.....C	
958	1.797058	0.002510	Google_72:8a:96	EAP	110	69	-17	dm	Response, Protected EAP (EAP-PEAP)	
959	1.797058	0.000000	192.168.1.15	Broadcast	802.11	76	69	-17	dm Acknowledgment, Flags=.....C	
960	1.801724	0.004656	Cisco_08:00:18	Broadcast	802.11	382	69	-17	dm Ignored Unknown Record	
961	1.801724	0.000000	192.168.1.15	Broadcast	802.11	76	69	-17	dm Acknowledgment, Flags=.....C	
963	1.820873	0.001870	Google_72:8a:96	EAP	110	69	-17	dm	Client key exchange, Change Cipher Spec, Encrypted Handshake P	
964	1.820873	0.000000	192.168.1.15	Broadcast	802.11	76	69	-17	dm Acknowledgment, Flags=.....C	
965	1.820890	0.004327	Cisco_08:00:18	EAP	1151.2	161	69	-17	dm	Change Cipher Spec, Encrypted Handshake Message
966	1.820890	0.000000	192.168.1.15	Broadcast	802.11	76	69	-17	dm Acknowledgment, Flags=.....C	
968	1.820920	0.004229	Google_72:8a:96	EAP	110	69	-17	dm	Response, Protected EAP (EAP-PEAP)	
969	1.820920	0.000000	192.168.1.15	Broadcast	802.11	76	69	-17	dm Acknowledgment, Flags=.....C	
971	1.831178	0.003900	Cisco_08:00:18	EAP	1151.2	148	69	-17	dm	Application data
972	1.831178	0.000000	192.168.1.15	Broadcast	802.11	76	69	-17	dm Acknowledgment, Flags=.....C	
973	1.831728	0.004910	Cisco_08:00:18	EAP	1151.2	152	69	-17	dm	Application data
974	1.831728	0.000000	192.168.1.15	Broadcast	802.11	76	69	-17	dm Acknowledgment, Flags=.....C	
976	1.840795	0.003200	Cisco_08:00:18	EAP	1151.2	171	69	-17	dm	Application data
977	1.840795	0.000000	192.168.1.15	Broadcast	802.11	76	69	-17	dm Acknowledgment, Flags=.....C	
978	1.845522	0.004817	Google_72:8a:96	EAP	1151.2	206	69	-17	dm	Application data
979	1.845522	0.000000	192.168.1.15	Broadcast	802.11	76	69	-17	dm Acknowledgment, Flags=.....C	
984	1.849494	0.010072	Cisco_08:00:18	EAP	1151.2	190	69	-17	dm	Application data
985	1.849494	0.000000	192.168.1.15	Broadcast	802.11	76	69	-17	dm Acknowledgment, Flags=.....C	
986	1.866887	0.002125	Google_72:8a:96	EAP	1151.2	145	69	-17	dm	Application data
987	1.866887	0.000000	192.168.1.15	Broadcast	802.11	76	69	-17	dm Acknowledgment, Flags=.....C	
988	1.870058	0.003771	Cisco_08:00:18	Broadcast	802.11	428	69	-17	dm Beacon frame, SN=3687, FwB, Flags=.....C, BI=100, SSID=W	
989	1.870058	0.000000	192.168.1.15	Broadcast	802.11	76	69	-17	dm Acknowledgment, Flags=.....C	
990	1.870058	0.000000	192.168.1.15	Broadcast	802.11	76	69	-17	dm Acknowledgment, Flags=.....C	
992	1.877128	0.006470	Google_72:8a:96	EAP	110	69	-18	dm	Response, Protected EAP (EAP-PEAP)	
993	1.877128	0.000000	192.168.1.15	Broadcast	802.11	76	69	-17	dm Acknowledgment, Flags=.....C	
996	1.920065	0.002917	Cisco_08:00:18	EAP	110	69	-17	dm	Success, Key (Message 2 of 4)	
997	1.920065	0.000000	192.168.1.15	Broadcast	802.11	76	69	-17	dm Acknowledgment, Flags=.....C	
998	1.920065	0.000000	Cisco_08:00:18	EAP	223	69	-17	dm	Key (Message 1 of 4)	
999	1.920065	0.000000	192.168.1.15	Broadcast	802.11	76	69	-17	dm Acknowledgment, Flags=.....C	
1001	1.925255	0.002917	Cisco_08:00:18	EAP	110	69	-18	dm	Success, Key (Message 2 of 4)	
1002	1.925255	0.000000	192.168.1.15	Broadcast	802.11	76	69	-17	dm Acknowledgment, Flags=.....C	
1004	1.926677	0.001422	Cisco_08:00:18	EAP	423	69	-17	dm	Key (Message 3 of 4)	
1005	1.926677	0.000000	192.168.1.15	Broadcast	802.11	76	69	-17	dm Acknowledgment, Flags=.....C	
1006	1.926886	0.002209	Cisco_08:00:18	EAP	199	69	-17	dm	Key (Message 4 of 4)	
1007	1.926886	0.000000	192.168.1.15	Broadcast	802.11	76	69	-17	dm Acknowledgment, Flags=.....C	

```

> Frame 925: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits) on interface Wpa_04578005-2998-4006-8C31-C3A13
> Ethernet II, Src: Cisco_08:00:18:00:00:00:00, Dst: Intelwpa_08:00:18:00:00:00:00
> Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.121
> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
> AiroHw/OniHw encapsulated IEEE 802.11
> IEEE 802.11 radio information
> IEEE 802.11 Association Request, Flags: .....C
> Tagged parameters (167 bytes)
> Fixed parameters (4 bytes)
> Tagged parameters (167 bytes)
> Tag: SSID parameter set: "wifi66_test"
> Tag: Supported Rates (8): 9, 12(0), 18, 24(0), 36, 48, 54, [Mbit/sec]
> Tag: Power Capability Mtr: 9, Max: 29
> Tag: Supported Channels
> Tag: RSN Information (48)
> Tag Length: 28
> RSN Version: 1
> Group Cipher Suite: 00:0f:ac (See IEEE 802.11) AES (CCM)
> Pairwise Cipher Suite Count: 1
> Pairwise Cipher Suite List: 00:0f:ac (See IEEE 802.11) AES (CCM)
> Auth Key Management (AKM) Suite Count: 1
> Auth Key Management (AKM) List: 00:0f:ac (See IEEE 802.11) FT over IEEE 802.1X
> Auth Key Management (AKM) Suite: 00:0f:ac (See IEEE 802.11) FT over IEEE 802.1X
> Auth Key Management (AKM) Type: FT over IEEE 802.1X (1)
> RSN Capabilities: 00000
> .....0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
> .....0 = RSN No Pairwise capabilities: Transmitter can support MP default key @ simultaneously wdt
> .....0 = RSN PTK Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/TKkeySA (0x0)
> .....0 = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/TKkeySA (0x0)
> .....1 = Management frame Protection Required: True
> .....1 = Management frame Protection Capable: True
> .....0 = 32bit PMK11-band RSN: False
> .....0 = Perkey Enabled: False
> .....0 = Extended key ID for Individually Addressed Frames: Not supported
PMKID Count: 0
PMKID List:
> Group Management Cipher Suite: 00:0f:ac (See IEEE 802.11) BIP (128)
> Tag: W Enabled Capabilities (5 octets)
> Tag: Mobility domain
> Tag: Supported Operating Classes
> Tag: Extended Capabilities (20 octets)
> Ext Tag: HE Capabilities
> Ext Tag: HE 4-0 Band Capabilities
> Tag: Vendor Specific: Broadcom
> Tag Length: 30
> OUI: 00:13:00 (Broadcom)
> Vendor Specific OUI Type: 2
> Vendor Specific Data: 0000000000000000
> Tag: Vendor Specific: Microsoft Corp.: WPAVUE: Information Element

```

WPA3 Enterprise 802.1x + FT Pixel6a-Zuordnung

Client-Details in WLC:

Details zum WPA3 Enterprise 802.1x + FT Pixel6a-Client

Konzentrieren Sie sich auf den Roamingtyp Over the Air (Über das Flugzeug), wo Sie den Roamingtyp 802.11R sehen können:

Samsung S23

Verbindung OTA mit Fokus auf RSN-Informationen vom Client:







### Edit WLAN

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

General **Security** Advanced Add To Policy Tags

Layer2 Layer3 AAA

WPA + WPA2  WPA2 + WPA3  WPA3  Static WEP  None

MAC Filtering

Lobby Admin Access

**WPA Parameters**

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

**Fast Transition**

Status

Over the DS

Reassociation Timeout \*

**WPA2/WPA3 Encryption**

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

**Auth Key Mgmt**

SUITEB-1X

**Protected Management Frame**

PMF

Association Comeback Timer\*

SA Query Time\*

WPA3 Enterprise Suite B-1X - Sicherheitskonfiguration



Hinweis: FT wird in SUITEB-1X nicht unterstützt

---

Auf der WLC-GUI der WLAN-Sicherheitseinstellungen anzeigen:

□  w66E\_test  5 w66E\_test [WPA3][SUITEB-1X][GCMP128]

Verifizierung von Beacons OTA:



No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	str	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=...		> frame 37626: 355 bytes on wire (2840 bits), 355 bytes captured (2840 bits) on interface \Device\NPF_{04576965-2998-4456-8C33-C4}
37385	59.190516	0.820488	Cisco_06:00:18	Broadcast	802.11	312	69 -47 dbm	Probe Response, SW=2003, Fw=0, Flags=.....C, B=100, SSID=...		> Ethernet II, Src: Cisco_02:00:07 (74:11:32:02:07:47), Dst: Unknown_07:c7:0e (08:00:00:07:c7:0e)
37396	59.191709	0.820481	Cisco_06:00:18	Broadcast	802.11	355	69 -47 dbm	Beacon frame, SW=2004, Fw=0, Flags=.....C, B=100, SSID=...		> Internet Protocol Version 4, Src: 192.168.1.121, Dst: 192.168.1.121
37414	59.192161	0.820462	Cisco_06:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2005, Fw=0, Flags=.....C, B=100, SSID=...		> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
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=...		> AlohaPdu/OnStream encapsulated IEEE 802.11
37437	59.192258	0.820457	Cisco_06:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2007, Fw=0, Flags=.....C, B=100, SSID=...		> IEEE 802.11 radio information
37447	59.192726	0.820452	Cisco_06:00:18	Broadcast	802.11	312	69 -47 dbm	Probe Response, SW=2008, Fw=0, Flags=.....C, B=100, SSID=...		> IEEE 802.11 Beacon frame, Flags: .....C
37459	59.193154	0.820522	Cisco_06:00:18	Broadcast	802.11	355	69 -48 dbm	Beacon frame, SW=2009, Fw=0, Flags=.....C, B=100, SSID=...		> IEEE 802.11 Wireless Management
37470	59.193629	0.820399	Cisco_06:00:18	Broadcast	802.11	312	69 -49 dbm	Probe Response, SW=2010, Fw=0, Flags=.....C, B=100, SSID=...		> Fixed parameters (12 bytes)
37480	59.194345	0.820501	Cisco_06:00:18	Broadcast	802.11	312	69 -47 dbm	Probe Response, SW=2011, Fw=0, Flags=.....C, B=100, SSID=...		> Tagged parameters (213 bytes)
37489	59.195487	0.821342	Cisco_06:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2012, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: SSID parameter set: "wifi_test"
37499	59.195116	0.821629	Cisco_06:00:18	Broadcast	802.11	312	69 -47 dbm	Probe Response, SW=2013, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: Supported Rates (6B), 9, 12(0), 18, 24(0), 36, 48, 54, [Mbit/sec]
37520	59.195713	0.820817	Cisco_06:00:18	Broadcast	802.11	355	69 -47 dbm	Beacon frame, SW=2014, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: Traffic Indication Map (TIM): OPM # of 1 bitmap
37529	59.195888	0.820835	Cisco_06:00:18	Broadcast	802.11	312	69 -47 dbm	Probe Response, SW=2015, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: Country Information: Country Code na, Environment Global operating classes
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=...		> Tag: Power Constraint: 6
37539	59.197089	0.821751	Cisco_06:00:18	Broadcast	802.11	312	69 -47 dbm	Probe Response, SW=2017, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: TX Report Transmit Power: 36, L100 Operate: 0
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=...		> Tag: RSN Information
37565	59.197199	0.820501	Cisco_06:00:18	Broadcast	802.11	355	69 -47 dbm	Beacon frame, SW=2019, Fw=0, Flags=.....C, B=100, SSID=...		> Tag Number: RSN Information (64)
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=...		> Tag Length: 26
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=...		> RSN Version: 1
37596	59.199439	0.820474	Cisco_06:00:18	Broadcast	802.11	312	69 -47 dbm	Probe Response, SW=2022, Fw=0, Flags=.....C, B=100, SSID=...		> Group Cipher Suite: 00:00:00:00:00:00:00:00 (IEEE 802.11) GCM (128)
37606	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=...		> Pairwise Cipher Suite Count: 1
37626	59.202621	0.820881	Cisco_06:00:18	Broadcast	802.11	355	69 -48 dbm	Beacon frame, SW=2024, Fw=0, Flags=.....C, B=100, SSID=...		> Pairwise Cipher Suite List (IEEE 802.11) GCM (128)
37641	59.204964	0.820961	Cisco_06:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2025, Fw=0, Flags=.....C, B=100, SSID=...		> Auth Key Management (AKM) Suite Count: 1
37652	59.206137	0.820351	Cisco_06:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2026, Fw=0, Flags=.....C, B=100, SSID=...		> Auth Key Management (AKM) List (IEEE 802.11) WPA (SHA256-Suite0)
37668	59.207165	0.820428	Cisco_06:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2027, Fw=0, Flags=.....C, B=100, SSID=...		> Auth Key Management (AKM) Suite: 00:00:00:00:00:00:00:00 (IEEE 802.11) WPA (SHA256-Suite0)
37687	59.207467	0.820792	Cisco_06:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2028, Fw=0, Flags=.....C, B=100, SSID=...		> Auth Key Management (AKM) Type: WPA (SHA256-Suite0) (11)
37696	59.208267	0.820488	Cisco_06:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2029, Fw=0, Flags=.....C, B=100, SSID=...		> RSN Capabilities: 0x0000
37699	59.208267	0.820488	Cisco_06:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2030, Fw=0, Flags=.....C, B=100, SSID=...		> PMKID Count: 0
37704	59.208267	0.820488	Cisco_06:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2031, Fw=0, Flags=.....C, B=100, SSID=...		> PMKID List
37719	59.207571	0.820241	Cisco_06:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2032, Fw=0, Flags=.....C, B=100, SSID=...		> Group Management Cipher Suite: 00:00:00:00:00:00:00:00 (IEEE 802.11) GCM (128)
37738	59.208659	0.820180	Cisco_06:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2033, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: QoS User Element: IEEE80211Q version
37749	59.205208	0.820495	Cisco_06:00:18	Broadcast	802.11	355	69 -48 dbm	Beacon frame, SW=2014, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: W Enabled Capabilities (5 octets)
37775	59.205621	0.820428	Cisco_06:00:18	Broadcast	802.11	312	69 -47 dbm	Probe Response, SW=2035, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: Extended Capabilities (11 octets)
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=...		> Tag: Tx Power Envelope
37809	59.207802	0.821581	Cisco_06:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2037, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: Tx Power Envelope
37814	59.207813	0.821551	Cisco_06:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2038, Fw=0, Flags=.....C, B=100, SSID=...		> Ext Tag: Multiple BSSID Configuration
37822	59.207968	0.820847	Cisco_06:00:18	Broadcast	802.11	355	69 -48 dbm	Beacon frame, SW=2019, Fw=0, Flags=.....C, B=100, SSID=...		> Ext Tag: HE Capabilities
37833	59.204859	0.820398	Cisco_06:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2040, Fw=0, Flags=.....C, B=100, SSID=...		> Ext Tag: HE Operation
37841	59.208540	0.820498	Cisco_06:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2041, Fw=0, Flags=.....C, B=100, SSID=...		> Ext Tag: Spatial Reuse Parameter Set
37857	59.208908	0.820550	Cisco_06:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2042, Fw=0, Flags=.....C, B=100, SSID=...		> Ext Tag: HE 4 GHz Band Capabilities
37864	08.013602	0.820462	Cisco_06:00:18	Broadcast	802.11	312	69 -47 dbm	Probe Response, SW=2043, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: Vendor Specific: Atheros Communications, Inc.: Unknown
37868	08.013932	0.820508	Cisco_06:00:18	Broadcast	802.11	355	69 -48 dbm	Beacon frame, SW=2044, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: Vendor Specific: Microsoft Corp.: WPAHE: Parameter Element
37881	08.014049	0.820297	Cisco_06:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2045, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: Vendor Specific: Cisco Systems, Inc.: Airont Client MFP Disabled
37887	08.014057	0.820508	Cisco_06:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2046, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: Vendor Specific: Cisco Systems, Inc.: Airont CCK version = 5
37897	08.014084	0.820839	Cisco_06:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2047, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: Vendor Specific: Cisco Systems, Inc.: Airont Unknown (64)
37908	08.112976	0.820888	Cisco_06:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2048, Fw=0, Flags=.....C, B=100, SSID=...		> Tag: Vendor Specific: Cisco Systems, Inc.: Airont Unknown (11) (11)
37927	08.124244	0.820438	Cisco_06:00:18	Broadcast	802.11	355	69 -47 dbm	Beacon frame, SW=2049, Fw=0, Flags=.....C, B=100, SSID=...		
37928	08.153887	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	08.173124	0.820267	Cisco_06:00:18	Broadcast	802.11	312	69 -48 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	0.820993	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	0.820994	Cisco_06:00:18	Broadcast	802.11	355	69 -47 dbm	Beacon frame, SW=2054, Fw=0, Flags=.....C, B=100, SSID=...		

### WPA3 Enterprise Suite B-1X Beacon

Keiner der getesteten Clients konnte sich mit SuiteB-1X mit dem WLAN verbinden. Dies bestätigt, dass keiner dieser Clients diese Sicherheitsmethode unterstützt.

### WPA3-Enterprise + GCMP256-Chiffre + SUITEB192-1X

### WLAN-Sicherheitskonfiguration:

⚠ 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

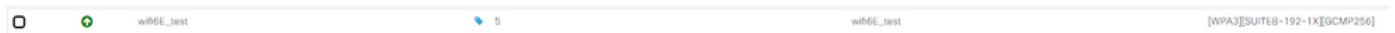
PMF   
Association Comeback Timer\*   
SA Query Time\*





Hinweis: FT wird von GCMP256+SUITEB192-1X nicht unterstützt.

Liste der WLANs auf der WLC-GUI:



WLAN für Tests

Verifizierung von Beacons OTA:





Zum Zeitpunkt der Erstellung dieses Dokuments war dieser Client nicht in der Lage, mithilfe von EAP-TLS eine Verbindung zu WPA3 Enterprise herzustellen.

Dies war ein kundenseitiges Problem, das derzeit bearbeitet wird, und sobald es gelöst ist, wird dieses Dokument aktualisiert werden.

### Sicherheitsschlussfolgerungen

Nach allen vorherigen Tests sind folgende Schlussfolgerungen zu ziehen:

Protokolle	Verschlüsselung	AKM	AKM-Verschlüsselung	EAP-Methode	FT-OverTA	FT-OVER-DS	Intel AX211
SCHULD	AES-CCMP128	SCHULD	N.	N.	NA	NA	Unterstützt
SAE	AES-CCMP128	SAE (nur H2E)	SHA 256	N.	Unterstützt	Unterstützt	Unterstützt nur H2E und FT-OverTA
Unternehmen	AES-CCMP128	802.1x-SHA256	SHA 256	PEAP/FAST/TLS	Unterstützt	Unterstützt	Unterstützt SHA256 und FT-OverTA/OverDS Nicht unterstützt EAP-Fast
Unternehmen	GMP 128	Suite B-1x	SHA256-Suite B	PEAP/FAST/TLS	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Unternehmen	GMP 256	Suite B-192	SHA384-Suite B	TLS	Nicht unterstützt	Nicht unterstützt	k. A.

## Fehlerbehebung

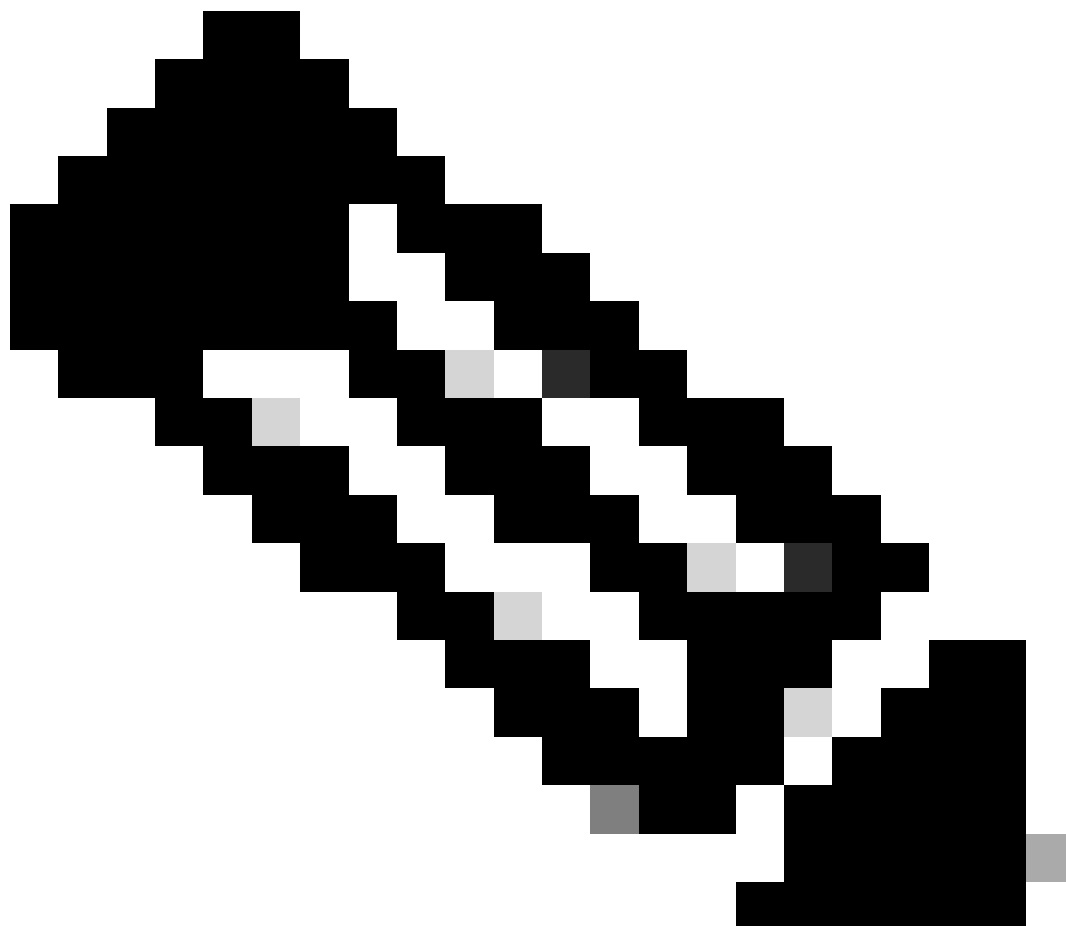
Die in diesem Dokument verwendete Fehlerbehebung basiert auf dem Online-Dokument:

[Fehlerbehebung bei COS-APs](#)

Die allgemeine Richtlinie für die Fehlerbehebung besteht darin, die RA-Ablaufverfolgung im Debugmodus vom WLC mithilfe der Client-MAC-Adresse zu erfassen. Dabei wird sichergestellt, dass der Client die Verbindung über die Geräte-MAC herstellt und keine randomisierte MAC-Adresse.

Für die Fehlerbehebung per Funk wird empfohlen, AP im Sniffer-Modus zu verwenden, um den Datenverkehr auf dem Kanal des Client-AP zu erfassen.

---



Hinweis: Lesen Sie [Wichtige Informationen zu Debug-Befehlen](#), bevor Sie Debug-Befehle verwenden.

---

## Zugehörige Informationen

[Was ist Wi-Fi 6E?](#)

[Was ist Wi-Fi 6 im Vergleich zu Wi-Fi 6E?](#)



[Wi-Fi 6E - Informationen auf einen Blick](#)

[Wi-Fi 6E: Das nächste große Kapitel im Wi-Fi-Whitepaper](#)

[Cisco Live - Architektur eines Wireless-Netzwerks der nächsten Generation mit Catalyst Wi-Fi 6E Access Points](#)

[Software-Konfigurationsleitfaden für Cisco Catalyst Wireless Controller der Serie 9800 17.9.x](#)

[WPA3-Bereitstellungsleitfaden](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.