

# Configurazione e verifica della sicurezza Wi-Fi 6E WLAN Layer 2

## Sommario

---

### [Introduzione](#)

### [Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

### [Premesse](#)

[Sicurezza Wi-Fi 6E](#)

[WPA3](#)

[Set di livelli: modalità WPA3](#)

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

[Impostazioni di protezione supportate dai client](#)

### [Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Configurazione di base](#)

### [Verifica](#)

[Verifica della sicurezza](#)

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

[WPA3 - AES\(CCMP128\) + OWE con modalità di transizione](#)

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

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

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

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

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

[Conclusioni sulla sicurezza](#)

### [Risoluzione dei problemi](#)

### [Informazioni correlate](#)

---

## Introduzione

Questo documento descrive come configurare la sicurezza Wi-Fi 6E WLAN Layer 2 e cosa aspettarsi sui diversi client.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Wireless Lan Controller (WLC) 9800
- Cisco Access Point (AP) che supportano Wi-Fi 6E.
- Standard IEEE 802.11ax
- Strumenti: Wireshark v4.0.6

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- WLC 9800-CL con IOS® XE 17.9.3.
- AP C9136, CW9162, CW9164 e CW9166.
- Client Wi-Fi 6E:
  - Lenovo X1 Carbon Gen11 con scheda di rete Intel AX211 Wi-Fi 6 e 6E con driver versione 22.200.2(1).
  - Scheda Netgear A8000 Wi-Fi 6 e 6E con driver v1(0.0.108);
  - Pixel 6a per cellulare con Android 13;
  - Cellulare Samsung S23 con Android 13.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

La cosa fondamentale da sapere è che Wi-Fi 6E non è uno standard completamente nuovo, ma un'estensione. Alla sua base, Wi-Fi 6E è un'estensione dello standard wireless Wi-Fi 6 (802.11ax) nella banda di radiofrequenza a 6 GHz.

Wi-Fi 6E è basato su Wi-Fi 6, l'ultima generazione dello standard Wi-Fi, ma solo i dispositivi e le applicazioni Wi-Fi 6E possono funzionare nella banda a 6 GHz.

## Sicurezza Wi-Fi 6E

Wi-Fi 6E aumenta la sicurezza con Wi-Fi Protected Access 3 (WPA3) e Opportunistic Wireless Encryption (OWE) e non c'è compatibilità con le versioni precedenti della sicurezza Open e WPA2.

WPA3 e Enhanced Open Security sono ora obbligatori per la certificazione Wi-Fi 6E e Wi-Fi 6E richiede anche Protected Management Frame (PMF) sia nell'access point che nei client.

Quando si configura un SSID da 6 GHz, è necessario soddisfare alcuni requisiti di sicurezza:

- Protezione WPA3 L2 con OWE, SAE o 802.1x-SHA256
- Frame di gestione protetto abilitato;
- Qualsiasi altro metodo di sicurezza L2 non è consentito, ovvero non è possibile utilizzare

una modalità mista.

## WPA3

WPA3 è progettato per migliorare la sicurezza Wi-Fi consentendo una migliore autenticazione su WPA2, fornendo una maggiore forza di crittografia e aumentando la resilienza delle reti critiche.

Le caratteristiche principali di WPA3 includono:

- PMF (Protected Management Frame) protegge i frame di gestione unicast e broadcast e crittografa i frame di gestione unicast. Ciò significa che il rilevamento wireless delle intrusioni e i sistemi di prevenzione delle intrusioni wireless hanno meno modi bruti di applicare le policy dei client.
- L'autenticazione simultanea di Equals (SAE) consente l'autenticazione basata su password e un meccanismo di accordo chiave. Questo protegge dagli attacchi di forza bruta.
- La modalità di transizione è una modalità mista che consente l'utilizzo di WPA2 per la connessione di client che non supportano WPA3.

WPA3 è incentrato sullo sviluppo continuo della sicurezza, sulla conformità e sull'interoperabilità. Nessun elemento di informazione designa WPA3 (uguale a WPA2). WPA3 è definito dalle combinazioni AKM/Cipher Suite/PMF.

Nella configurazione WLAN 9800, sono disponibili 4 diversi algoritmi di crittografia WPA3.

Essi sono basati su GCMP (Galois/Counter Mode Protocol) e Counter Mode con Cipher Block Chaining Message Authentication Code Protocol (CCMP): AES (CCMP128), CCMP256, GCMP128 e GCMP256:

**WPA2/WPA3 Encryption**

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

Opzioni crittografia WPA2/3

## PMF

PMF viene attivato su una WLAN quando si abilita PMF.

Per impostazione predefinita, i frame di gestione 802.11 non sono autenticati e pertanto non sono protetti dallo spoofing. Infrastructure Management Protection Frame (MFP) e 802.11w protected management frame (PMF) offrono protezione da tali attacchi.

## Protected Management Frame

PMF

Required



Association Comeback Timer\*

1

SA Query Time\*

200

Opzioni PMF

Gestione delle chiavi di autenticazione

Queste sono le opzioni AKM disponibili nella versione 17.9.x:



## 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\*

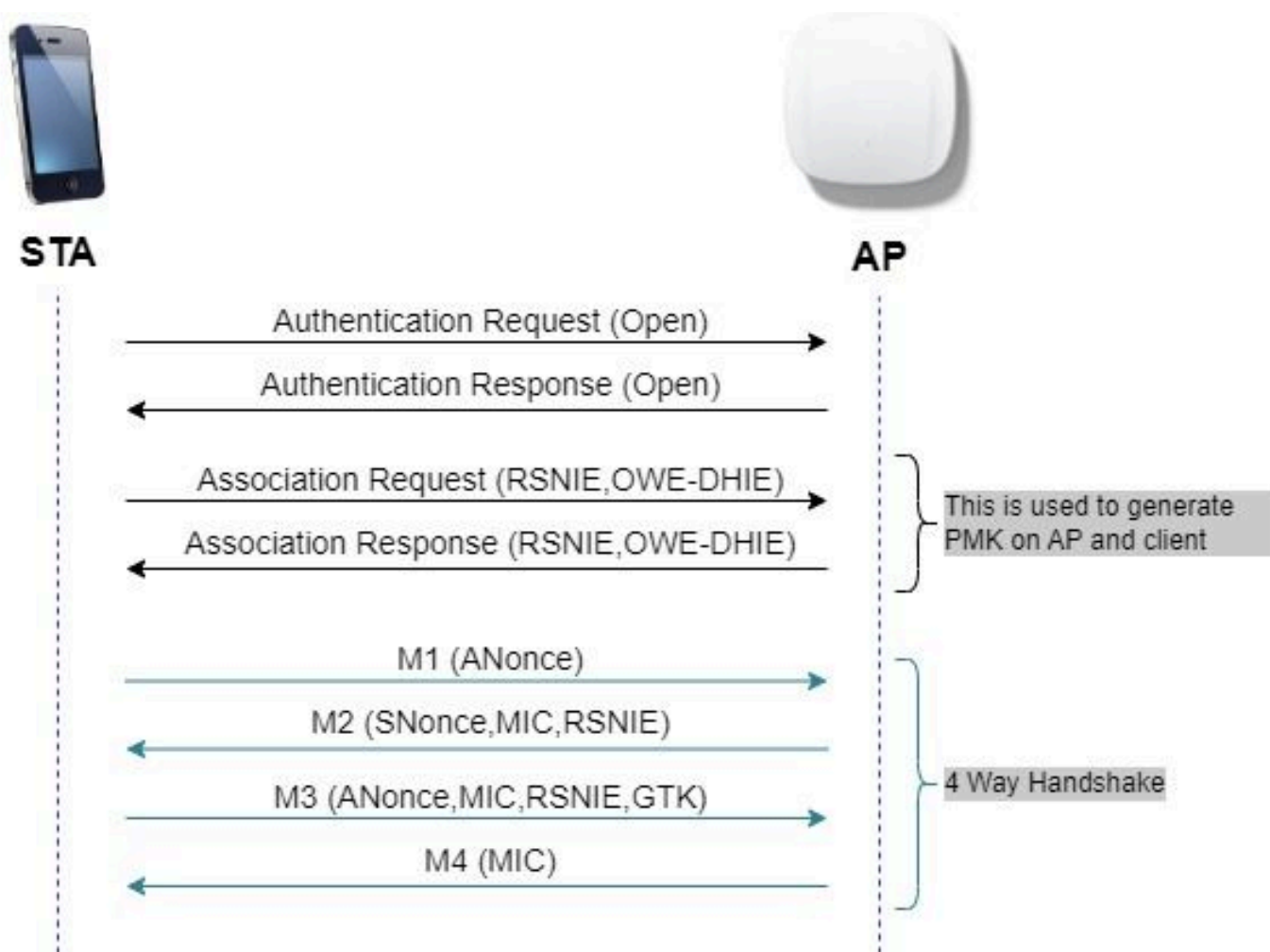
SAE Password Element ⓘ

Opzioni AKM

DOVERE

Opportunistic Wireless Encryption (OWE) è un'estensione di IEEE 802.11 che fornisce la crittografia del supporto wireless ([IETF RFC 8110](#)). Lo scopo dell'autenticazione basata su OWE è evitare la connettività wireless aperta non protetta tra l'access point e i client. L'OWE utilizza la crittografia basata sugli algoritmi Diffie-Hellman per impostare la crittografia wireless. Con OWE, il client e l'access point eseguono uno scambio di chiavi Diffie-Hellman durante la procedura di accesso e utilizzano il segreto PMK (pairwise master key) risultante con l'handshake a 4 vie.

L'utilizzo di OWE migliora la sicurezza delle reti wireless per le installazioni in cui vengono installate reti aperte o condivise basate su PSK.



scambio frame OWE

## SAE

WPA3 utilizza un nuovo meccanismo di autenticazione e gestione delle chiavi denominato Autenticazione simultanea di Equals. Questo meccanismo è ulteriormente migliorato attraverso l'uso di SAE Hash-to-Element (H2E).

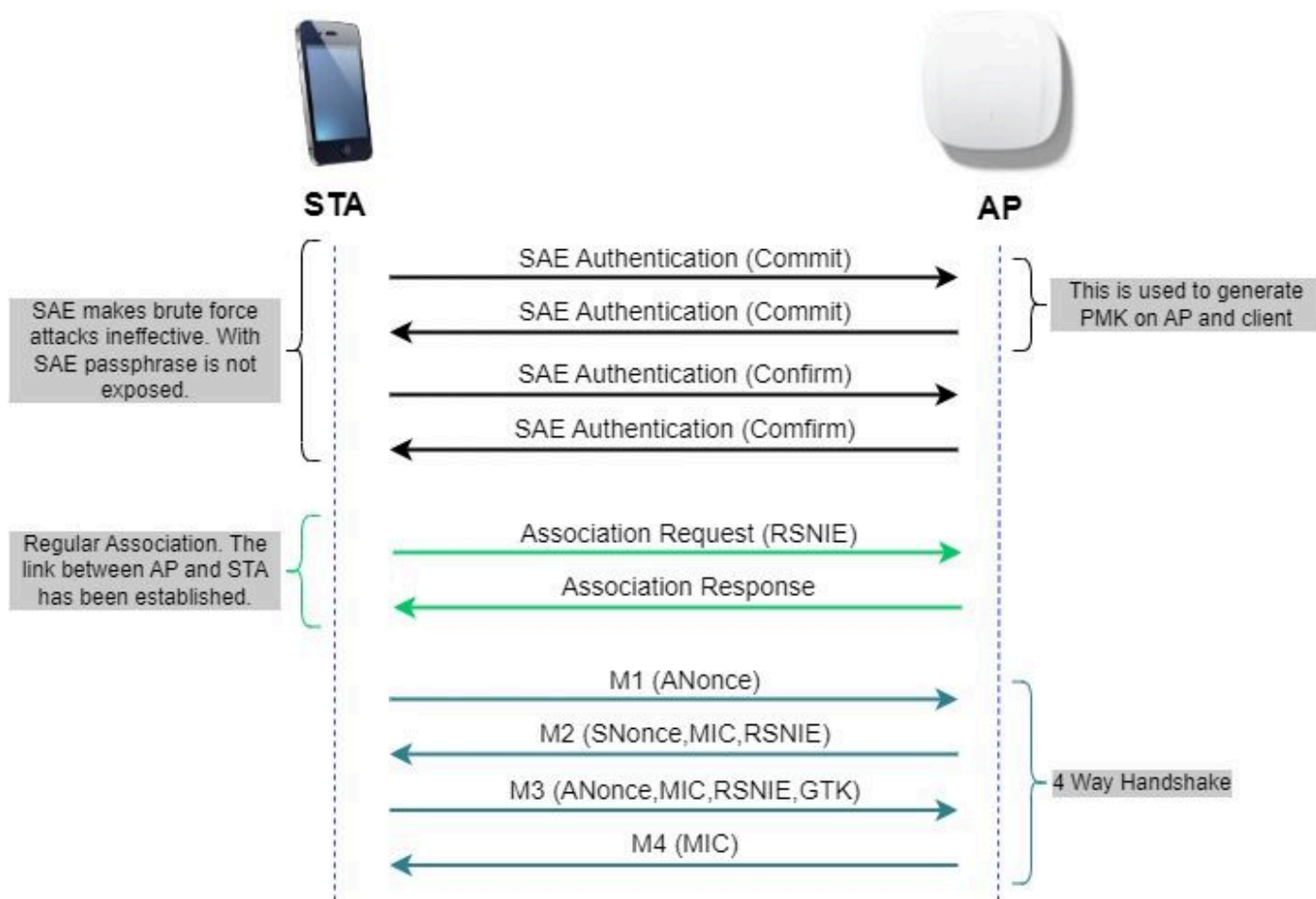
SAE con H2E è obbligatorio per WPA3 e Wi-Fi 6E.

SAE utilizza una crittografia logaritmica discreta per eseguire uno scambio efficiente in modo tale da eseguire l'autenticazione reciproca utilizzando una password che è probabilmente resistente a un attacco del dizionario offline.

Un attacco di dizionario offline è un attacco in cui un avversario tenta di determinare una password di rete provando possibili password senza ulteriori interazioni di rete.

Quando il client si connette al punto di accesso, esegue uno scambio SAE. Se l'operazione ha esito positivo, verrà creata una chiave sicura dal punto di vista crittografico, da cui deriva la chiave di sessione. Fondamentalmente, un client e un punto di accesso vanno in fasi di commit e poi di conferma.

Una volta raggiunto un impegno, il client e il punto di accesso possono passare agli stati di conferma ogni volta che viene generata una chiave di sessione. Il metodo utilizza la segretezza in avanti, in cui un intruso potrebbe decifrare una singola chiave, ma non tutte le altre.



Scambio di frame SAE

## Hash-to-Element (H2E)

Hash-to-Element (H2E) è un nuovo metodo SAE Password Element (PWE). In questo metodo, il PWE segreto utilizzato nel protocollo SAE viene generato da una password.

Quando una stazione (STA) che supporta H2E avvia SAE con un punto di accesso, controlla se quest'ultimo supporta H2E. In caso affermativo, l'access point utilizza H2E per derivare il PWE utilizzando un valore del codice di stato appena definito nel messaggio di commit SAE.

Se STA utilizza Hunting-and-Pecking (HnP), l'intero scambio SAE rimane invariato.

Durante l'utilizzo di H2E, la derivazione PWE è suddivisa in questi componenti:

- Derivazione di un elemento intermedio segreto (PT) dalla password. Questa operazione può essere eseguita non in linea quando la password è inizialmente configurata sul dispositivo per ciascun gruppo supportato.
- Derivazione del PWE dal PT memorizzato. Ciò dipende dal gruppo negoziato e dagli indirizzi MAC dei peer. Questa operazione viene eseguita in tempo reale durante lo scambio SAE.

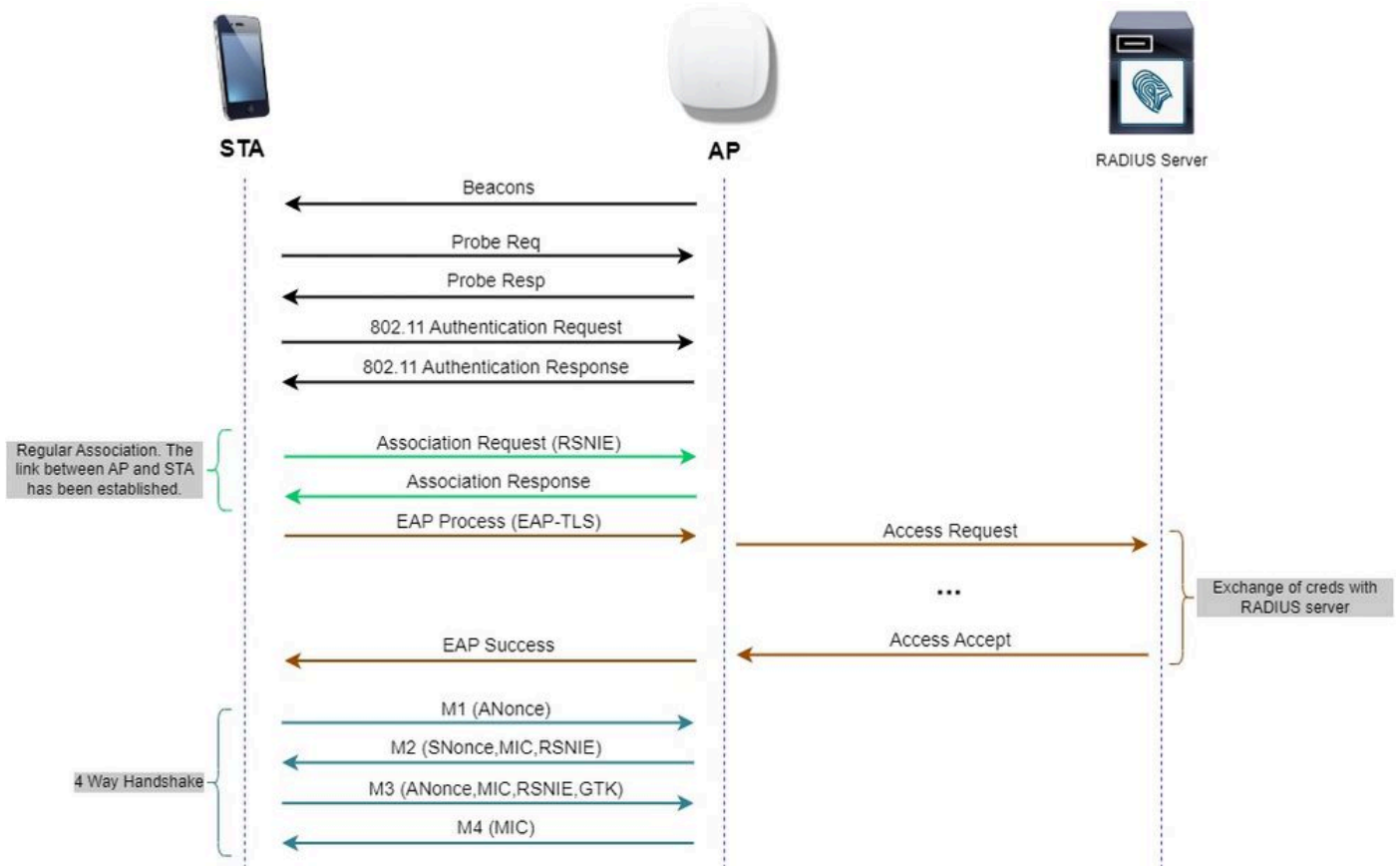


Nota: 6-GHz supporta solo il metodo Hash-to-Element SAE PWE.

---

## WPA-Enterprise aka 802.1x

WPA3-Enterprise è la versione più sicura di WPA3 e utilizza una combinazione di nome utente e password con 802.1X per l'autenticazione utente con un server RADIUS. Per impostazione predefinita, WPA3 utilizza la crittografia a 128 bit, ma introduce anche una crittografia a 192 bit configurabile facoltativamente, che offre una protezione aggiuntiva per qualsiasi rete che trasmette dati sensibili.



Flusso diagramma WPA3 Enterprise

## Set di livelli: modalità WPA3

- WPA3-Personale
  - Modalità WPA3-Personale
    - PMF necessario
  - WPA3-Modalità transizione personale
    - Regole di configurazione: in un punto di accesso, ogni volta che è abilitata la modalità WPA2-Personale, anche la modalità di transizione WPA3-Personale deve essere abilitata per impostazione predefinita, a meno che non venga esplicitamente ignorata dall'amministratore per l'utilizzo della modalità solo WPA2-Personale
- WPA3-Enterprise
  - Modalità solo WPA3-Enterprise
    - PMF viene negoziato per tutte le connessioni WPA3
  - Modalità di transizione WPA3-Enterprise
    - PMF è negoziato per una connessione WPA3
    - PMF opzionale per una connessione WPA2
  - Modalità WPA3-Enterprise suite-B "192-bit" allineata con Commercial National Security Algorithm (CNSA)
    - Non solo per il governo federale
    - Suite di cifratura crittografica coerenti per evitare configurazioni errate

- Aggiunta di GCMP ed ECCP per funzioni di crittografia e hash migliori (SHA384)
- PMF necessario
- La sicurezza WPA3 a 192 bit è esclusiva per EAP-TLS, che richiede certificati sia sul richiedente che sul server RADIUS.
- Per utilizzare WPA3 a 192 bit Enterprise, i server RADIUS devono utilizzare una delle cifrature EAP consentite:





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

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

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

Per ulteriori informazioni sull'implementazione di WPA3 nelle WLAN Cisco, inclusa la matrice di compatibilità per la sicurezza dei client, consultare la [Guida all'implementazione di WPA3](#).

## Cisco Catalyst Wi-Fi 6E AP

Ideal for Small to Medium-sized deployments	Best In Class, Flexibility		Mission Critical, Performance
 <p><b>CW9162</b></p> <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> <p><small>Available with IOS-XE 17.9.2</small></p>	 <p><b>CW9164</b></p> <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>	 <p><b>CW9166</b></p> <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>	 <p><b>C9136</b></p> <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> <p><small>*Available in Future</small></p>
Full radio capability (6 GHz @ LPI) on single 30W PoE+			
Dedicated Radio for CleanAir Pro	Same Bracket, Industrial Design	AP Power Optimization	USB

Access Point Wi-Fi 6E

### Impostazioni di protezione supportate dai client

È possibile trovare quale prodotto supporta WPA3-Enterprise utilizzando la pagina Web WiFi Alliance [product finder](#).

Sui dispositivi Windows è possibile verificare quali sono le impostazioni di sicurezza supportate dalla scheda di rete usando il comando "netsh wlan show drivers".

Qui è possibile vedere l'output di 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
```

Output Windows di \_netsh wlan show driver\_ per il 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)
```

Output Windows di \_netsh wlan show driver\_ per il 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 + cifratura AES + 802.1x-SHA256 (FT) AKM
- WPA3 + cifratura AES + OWE AKM
- WPA3 + cifratura AES + SAE (FT) AKM
- WPA3 + CCMP256 cifratura + SUITEB192-1X AKM
- CIFRATURA WPA3 + GCMP128 + SUITEB-1X AKM
- CIFRATURA WPA3 + GCMP256 + SUITEB192-1X AKM

## Configurazione di base

La WLAN è stata configurata solo con il criterio radio da 6 GHz e il metodo di rilevamento UPR (Broadcast Probe Response):

**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\*

SSID\*

WLAN ID\*

Status  **ENABLED**

Broadcast SSID  **ENABLED**

**Radio Policy** ⓘ

[Show slot configuration](#)

**6 GHz**

Status  **ENABLED**

- WPA2 Disabled
- WPA3 Enabled
- Dot11ax Enabled

**5 GHz**

Status  **DISABLED**

**2.4 GHz**

Status  **DISABLED**

802.11b/g Policy

Configurazione base WLAN

The screenshot displays the Cisco Catalyst 9800-CL Wireless Controller configuration page. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is titled 'Configuration > Tags & Profiles > RF/Radio'. It features a table of RF profiles with columns for State, RF Profile Name, and Band. The 'default-rf-profile-6ghz' profile is highlighted, indicating a 6 GHz band. The right-hand panel, 'Edit RF Profile', shows configuration options for the 802.11ax standard, including '6 GHz Discovery Frames' (set to Broadcast Probe Response), 'Broadcast Probe Response Interval (msec)\*' (set to 20), 'Multi BSSID Profile' (set to MBSSIDprofile\_test), and 'Spatial Reuse' settings (OBSS PD, Non-SRG OBSS PD Max Threshold, SRG OBSS PD, SRG OBSS PD Min Threshold, and SRG OBSS PD Max Threshold, all set to -62 dBm).

Configurazione profilo RF da 6 GHz

## Verifica

### Verifica della sicurezza

In questa sezione viene presentata la fase di configurazione della protezione e di associazione dei client utilizzando le seguenti combinazioni di protocolli WPA3:

- WPA3- AES(CCMP128) + OWE
  - Modalità di transizione OWE
- WPA3-Personale
  - AES (CCMP128) + SAE
- WPA3-Enterprise
  - AES (CCMP128) + 802.1x-SHA256
  - AES (CCMP128) + 802.1x-SHA256 + FT
  - CIFRATURA GCMP128 + SUITE-B-1X
  - CIFRATURA GCMP256 + SUITE B192-1X

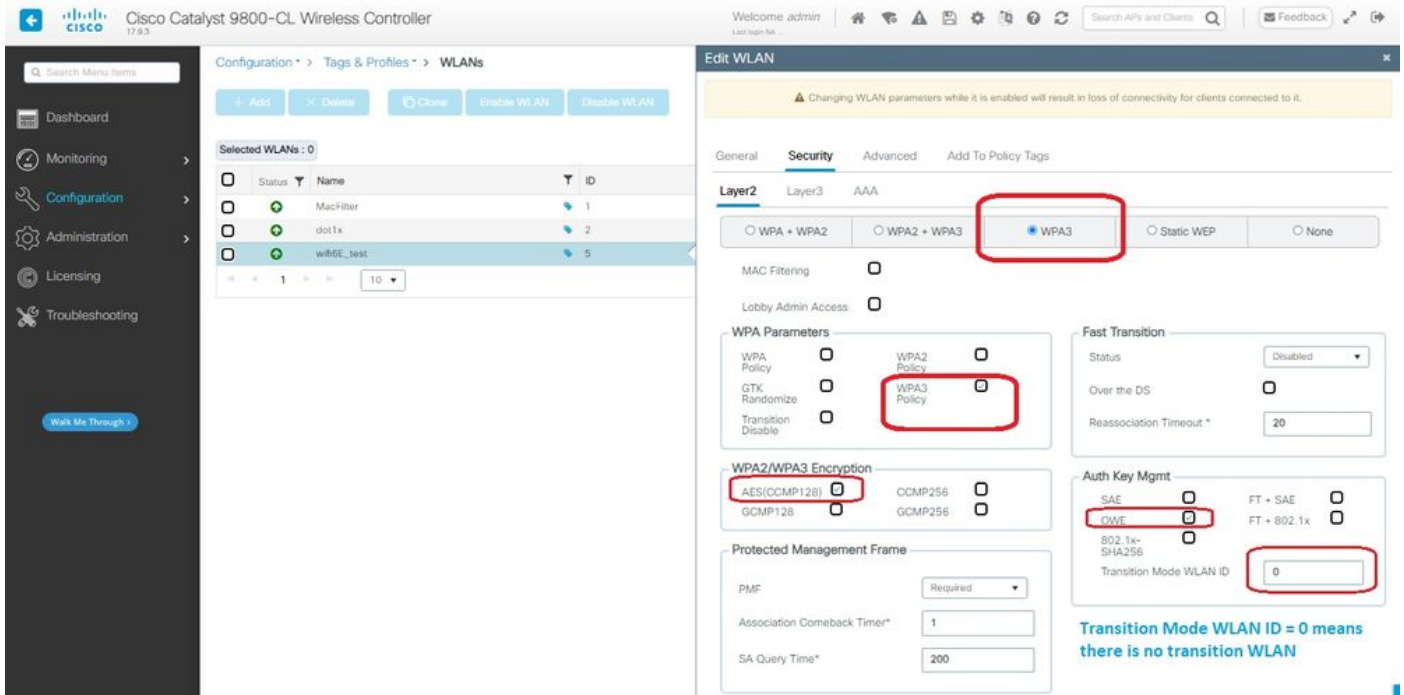


Nota: anche se non ci sono client che supportano la cifratura GCMP128 + SUITEB-1X al momento della scrittura di questo documento, è stato testato per osservarlo mentre veniva trasmesso e controllare le informazioni RSN nei beacon.

---

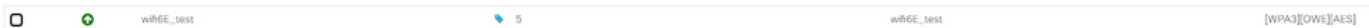
WPA3 - AES(CCPM128) + OWE

Questa è la configurazione della sicurezza WLAN:



Impostazioni di protezione OWE

Visualizzare sull'interfaccia WLC delle impostazioni di sicurezza WLAN:



Impostazioni di sicurezza WLAN sull'interfaccia utente WLC

Qui possiamo osservare il processo di connessione dei client Wi-Fi 6E:

Intel AX211

Qui viene mostrato il processo di connessione completo del client Intel AX211.

Rilevamento OWE

Qui potete vedere i beacon OTA. L'access point annuncia il supporto per OWE utilizzando il settore di suite AKM per OWE sotto l'elemento di informazioni RSN.

Il valore 18 (00-0F-AC:18) della suite AKM indica il supporto OWE.

The image shows a Wireshark capture of an IEEE 802.11 Beacon frame. The packet list pane on the left shows the frame details, and the packet bytes pane on the right shows the raw data. A red box highlights the 'Auth Key Management (AKM) Suite: Opportunistic Wireless Encryption (18)' entry in the 'Auth Key Management (AKM) Suites' field. A red arrow points to this entry.

frame beacon OWE

Se si controlla il campo delle funzionalità RSN, si osserverà che l'access point annuncia sia le funzionalità MFP (Management Frame Protection) che il bit MFP richiesto impostato su 1.

Associazione OWE

Si può vedere l'UPR inviato in modalità broadcast e quindi l'associazione stessa.

L'operazione OWE inizia con la richiesta e la risposta di autenticazione OPEN:

The image shows a Wireshark capture of the initial OWE authentication sequence. The packet list pane on the left shows the sequence of frames: Probe Request, Authentication, Association Request, and Association Response. The packet bytes pane on the right shows the raw data for the Authentication frame, which includes the Authentication Algorithm (Open System) and Status Code (Successful).

The image shows a Wireshark capture of the continuation of the OWE authentication sequence. The packet list pane on the left shows the sequence of frames: Authentication Response, Key Exchange, and Key Confirmation. The packet bytes pane on the right shows the raw data for the Authentication Response frame, which includes the Authentication Algorithm (Open System) and Status Code (Successful).

Quindi, un client che desidera eseguire OWE deve indicare OWE AKM nel frame RSN IE di Association Request e includere l'elemento parametro Diffie Helman (DH):



Frame 13: 284 bytes on wire (2272 bits), 284 bytes captured (2272 bits) on interface f0dc1e1000 (08:00:0c:00:00:00) on 08:00:0c:00:00:00

IEEE 802.11 Association Request, Flags: .....C

IEEE 802.11 Association Response, Flags: .....C

RSN Information (48)

- Tag Length: 34
- RSN Version: 1
- Group Cipher Suite: 00:0fac (IEEE 802.11) AES (CCM)
- Pairwise Cipher Suite List: 00:0fac (IEEE 802.11) AES (CCM)
- Auth Key Management (AKM) Suite Count: 1
- Auth Key Management (AKM) Suite: 00:0fac (IEEE 802.11) Opportunistic Wireless Encryption
- Auth Key Management (AKM) Suite: 00:0fac (IEEE 802.11) Opportunistic Wireless Encryption
- Auth Key Management (AKM) Suite: 00:0fac (IEEE 802.11) Opportunistic Wireless Encryption
- RSN Capabilities: 000000
- RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
- RSN No Pairwise capabilities: Transmitter can support WEP default key a simultaneously with Pairwise
- RSN GTKSA Replay Counter capabilities: 4 replay counters per GTKSA/GTKSA/STakeysA (0x1)
- RSN GTKSA Replay Counter capabilities: 4 replay counters per GTKSA/GTKSA/STakeysA (0x1)
- Management Frame Protection Required: True
- Management Frame Protection Capabilities: True
- Joint Multi-band RSN: False
- Peerkey Enabled: False
- Extended Key ID for Individually Addressed Frames: Not supported
- PKID Count: 0
- PKID List
- Group Management Cipher Suite: 00:0fac (IEEE 802.11) ESP (128)

Frame 15: 278 bytes on wire (2224 bits), 278 bytes captured (2224 bits) on interface f0dc1e1000 (08:00:0c:00:00:00) on 08:00:0c:00:00:00

IEEE 802.11 Key Management (Authenticating), Flags: .....C

IEEE 802.11 Key Management (Acknowledgment), Flags: .....C

IEEE 802.11 Key Management (Key Message 1 of 4), Flags: .....C

IEEE 802.11 Key Management (Key Message 2 of 4), Flags: .....C

IEEE 802.11 Key Management (Key Message 3 of 4), Flags: .....C

IEEE 802.11 Key Management (Key Message 4 of 4), Flags: .....C

IEEE 802.11 Key Management (Pairwise Cipher Suite List), Flags: .....C

RSN Information (48)

- Tag Length: 34
- RSN Version: 1
- Group Cipher Suite: 00:0fac (IEEE 802.11) AES (CCM)
- Pairwise Cipher Suite List: 00:0fac (IEEE 802.11) AES (CCM)
- Auth Key Management (AKM) Suite Count: 1
- Auth Key Management (AKM) Suite: 00:0fac (IEEE 802.11) Opportunistic Wireless Encryption
- Auth Key Management (AKM) Suite: 00:0fac (IEEE 802.11) Opportunistic Wireless Encryption
- Auth Key Management (AKM) Suite: 00:0fac (IEEE 802.11) Opportunistic Wireless Encryption
- RSN Capabilities: 000000
- RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
- RSN No Pairwise capabilities: Transmitter can support WEP default key a simultaneously with Pairwise
- RSN GTKSA Replay Counter capabilities: 4 replay counters per GTKSA/GTKSA/STakeysA (0x1)
- RSN GTKSA Replay Counter capabilities: 4 replay counters per GTKSA/GTKSA/STakeysA (0x1)
- Management Frame Protection Required: True
- Management Frame Protection Capabilities: True
- Joint Multi-band RSN: False
- Peerkey Enabled: False
- Extended Key ID for Individually Addressed Frames: Not supported
- PKID Count: 0
- PKID List
- Group Management Cipher Suite: 00:0fac (IEEE 802.11) ESP (128)

Risposta associazione OWE

Dopo la risposta dell'associazione è possibile vedere l'handshake a 4 vie e il client passa allo stato connesso.

Qui è possibile visualizzare i dettagli del client sull'interfaccia utente del WLC:

Client

360 View | General | QoS Statistics | ATF Statistics | Mobility History | Call Statistics

Client Properties | AP Properties | Security Information | Client Statistics | QoS Properties | EoGRE

Client State Servers	None
Client ACLs	None
Client Entry Create Time	43 seconds
Policy Type	WPA3
Encryption Cipher	CCMP (AES)
Authentication Key Management	OWE
EAP Type	Not Applicable
Session Timeout	3600s

NetGear A8000

OTA connessione con lo stato attivo sulle informazioni RSN dal client:





## Samsung S23

OTA connessione con lo stato attivo sulle informazioni RSN dal client:

## Dettagli client in WLC:

## WPA3 - AES(CCMP128) + OWE con modalità di transizione

Configurazione dettagliata e risoluzione dei problemi della modalità di transizione OWE disponibili in questo documento: [Configure Enhanced Open SSID with Transition Mode - OWE](#).

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

## Configurazione della sicurezza WLAN:

### Edit WLAN

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

General **Security** Advanced Add To Policy Tags

**Layer2** Layer3 AAA

WPA + WPA2  WPA2 + WPA3  WPA3  Static WEP  None

MAC Filtering

Lobby Admin Access

#### WPA Parameters

WPA Policy  WPA2 Policy

GTK Randomize  WPA3 Policy

Transition Disable

#### Fast Transition

Status

Over the DS

Reassociation Timeout \*

#### WPA2/WPA3 Encryption

AES(OCMP128)  OCMP256

GCMP128  GCMP256

#### Protected Management Frame

PMF

Association Comeback Timer\*

SA Query Time\*

#### Auth Key Mgmt

SAE  FT - SAE

ONE  FT - 802.1x

802.1x-SHA256

Anti Clogging Threshold\*

Max Retries\*

Retransmit Timeout\*

PSK Format

PSK Type

Pre-Shared Key\*

SAE Password Element

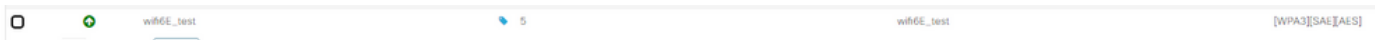
Configurazione SAE WPA3



Nota: la caccia e il prelievo non sono consentiti con policy radio a 6 GHz. Quando si configura una WLAN a 6 GHz, è necessario selezionare l'elemento H2E SAE Password.

---

Visualizzare sull'interfaccia WLC delle impostazioni di sicurezza WLAN:



Verifica dell'OTA dei beacon:





## NetGear A8000

OTA connessione con lo stato attivo sulle informazioni RSN dal client:

## Dettagli client in WLC:

## Pixel 6a

OTA connessione con lo stato attivo sulle informazioni RSN dal 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, Src=2096, Pwr=, Flags=.....C, SSID="wifi6_test"
1243	2023-06-12 17:37:02.855631	0.117200	Google_7218a:66	Cisco_31180:1	Broadcast	802.11	394	-42 dBm	Authentication, Src=2097, Pwr=, 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, Src=14, Pwr=, 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	0.009447	Google_7218a:66	Cisco_31180:1	Broadcast	802.11	139	-41 dBm	Authentication, Src=2098, Pwr=, 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, Src=14, Pwr=, 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, Src=2099, Pwr=, Flags=.....C, SSID="wifi6_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	0.000917	Google_7218a:66	Cisco_31180:1	Broadcast	802.11	144	-37 dBm	I, P, N(=), N(=); DSAP 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, Src=14, Pwr=, 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	LLC	134	-37 dBm	S, P, Func=, N(=); DSAP Basic Group, SSAP Basic Response	
1265	2023-06-12 17:37:02.943892	0.009663	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, Src=2100, Pwr=, 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 17:37:03.040493	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, Src=14, Pwr=, 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, Src=2104, Pwr=, Flags=.....C
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	IPVcast_16	LLC	227	-37 dBm	U, P, Func=, N(=); DSAP 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	0.001700	Google_7218a:66	Cisco_31180:1	Broadcast	802.11	115	-37 dBm	Action, Src=14, Pwr=, 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	0.000037	192.168.1.15	192.168.1.121	802.11	82	-49 dBm	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	Block ACK, Pwr=, Flags=.....C	
1306	2023-06-12 17:37:03.168543	0.000347	Google_7218a:66	IPVcast_16	LLC	186	-38 dBm	I, P, N(=), N(=); DSAP Basic Individual, SSAP Basic Response	
1307	2023-06-12 17:37:03.177442	0.000000	192.168.1.15	192.168.1.121	802.11	82	-49 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	-46 dBm	Clear-to-send, Flags=.....C	
1309	2023-06-12 17:37:03.177515	0.000073	Google_7218a:66	IPVcast_16	LLC	271	-56 dBm	I, N(=), N(=); DSAP Basic Group, SSAP Basic Response	

```

> Frame 1255: 262 bytes on wire (2096 bits), 262 bytes captured (2096 bits) on interface VdeviceVAP_04578905-2998-445
> Ethernet II, Src: Cisco_G0/16:17 (00:0f:1d:0d:7d:37), Dst: Univers_07:cf:06 (08:0a:8b:07:cf:06)
> Internet Protocol version 4, Src: 192.168.1.15, Dst: 192.168.1.121
> User Datagram Protocol, Src Port: 5859, Dst Port: 5800
> Airopeex/OmniPeex encapsulated IEEE 802.11
> IEEE 802.11 radio information
> IEEE 802.11 Wireless Management
  > Fixed parameters (4 bytes)
  > Tagged parameters (168 bytes)
    > Tag: SSID parameter Set: "wifi6_test"
    > Tag: Supported rates (0), 9, 12.0, 18, 24.0, 36, 48, 54, 54 (Mbit/sec)
    > Tag: Extended Supported Rates SAE mesh 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:fac (See IEEE 802.11) AES (CCM)
    > Pairwise Cipher Suite Count: 1
    > Pairwise Cipher Suite List 00:fac (See IEEE 802.11) AES (CCM)
    > Auth Key Management (AKM) Suite Count: 1
    > Auth Key Management (AKM) List 00:fac (See IEEE 802.11) SAE (SHA256)
    > RSN Capabilities: 0000e
    > PMKID Count: 0
    > PMKID List
    > Group Management Cipher Suite: 00:fac (See 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
    > RSNX: eae (octet 1)
      > ..... = RSNX length: 0
      > ... .. = Protected TWT Operations Support: 0
      > ... .. = Reserved: 000
      > ... .. = SAE mesh to element: 1
  > Ext Tag: HE 4 oct Band Capabilities
  > Tag: Vendor Specific: Broadcom
  > Tag: Vendor Specific: Microsoft Corp.: WPA/WPE: Information Element
  
```

## Dettagli client in WLC:

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The main area displays a list of clients under the 'Monitoring' tab. One client is selected, and its details are shown in a side panel.

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 for the selected client (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
- 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

OTA connessione con lo stato attivo sulle informazioni RSN dal client:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
773	2023-06-12 17:26:55.727215	0.000000	Samsung_C9:8371	Cisco_31180:1	Broadcast	802.11	194	-45 dBm	Authentication, Src=2176, Pwr=, 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_C9:8371	802.11	194	-37 dBm	Authentication, Src=2176, Pwr=, 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_C9:8371	Cisco_31180:1	Broadcast	802.11	139	-43 dBm	Authentication, Src=2177, Pwr=, 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	0.000228	Cisco_31180:1	Samsung_C9:8371	802.11	139	-36 dBm	Authentication, Src=2177, Pwr=, 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 17:26:55.748094	0.004544	Samsung_C9:8371	Cisco_31180:1	Broadcast	802.11	354	-45 dBm	Association Request, Src=2178, Pwr=, Flags=.....C, SSID="wifi6_test"
783	2023-06-12 17:26:55.748094	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_C9:8371	Broadcast	LLC	114	-37 dBm	I, N(=), N(=); DSAP ISO Network Layer (unofficial) Group, SSAP Banyan VME	
788	2023-06-12 17:26:55.758131	0.000000	Samsung_C9:8371	Broadcast	LLC	114	-36 dBm	S, P, Func=, N(=); DSAP HP Getdirect Printer Individual, SSAP MS Response	
789	2023-06-12 17:26:55.763192	0.002876	Cisco_31180:1	Samsung_C9:8371	802.11	236	-36 dBm	Association Response, Src=14, Pwr=, 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_C9:8371	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	0.028283	Samsung_C9:8371	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_C9:8371	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_C9:8371	Cisco_31180:1	EAPOL	199	-44 dBm	Key (message 4 of 4)	

## Dettagli client in WLC:

Cisco Catalyst 9800-CL Wireless Controller

Welcome admin

Search APs and Clients

Feedback

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Delete

Selected 0 out of 12 Clients

	Client MAC Address	IPv4 Address	IPv6 Address	AP Name
<input type="checkbox"/>	0012.17e1.dd57	192.168.1.33	fe80::212:17ff:fe1:dd57	AP03_Sotao_9548
<input type="checkbox"/>	0012.17e2.4856	192.168.1.37	fe80::212:17ff:fe2:4856	AP05_OutdoorB_220
<input type="checkbox"/>	0012.17e2.4b40	192.168.1.31	fe80::212:17ff:fe2:4b40	AP04_OutdoorF_300
<input type="checkbox"/>	0429.2ec9.e371	192.168.1.160	fe80::6a20:34e8:ab1b:6332	AP6849.9253.CA50
<input type="checkbox"/>	0c8b.9509.3518	192.168.1.129	N/A	AP03_Sotao_9548
<input type="checkbox"/>	34ea.e702.6240	192.168.1.70	N/A	AP6849.9253.CA50
<input type="checkbox"/>	60fb.008b.0e66	N/A	N/A	APD1_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  
 IIF ID 0x90000010  
 Authorized TRUE  
 Common Session ID 000000000000FB1B0A58F78  
 Acct Session ID 0x00000000  
 Auth Method Status List  
 Method SAE

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

Configurazione della sicurezza WLAN:

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

General **Security** Advanced Add To Policy Tags

**Layer2** Layer3 AAA

WPA + WPA2
  WPA2 + WPA3
  WPA3
  Static WEP
  None

MAC Filtering

Lobby Admin Access

WPA Parameters

WPA Policy 
 WPA2 Policy   
 GTK Randomize 
 WPA3 Policy   
 Transition Disable

Fast Transition

Status    
 Over the DS   
 Reassociation Timeout \*

WPA2/WPA3 Encryption

AES(OCMP128) 
 OCMP256   
 GCMP128 
 GCMP256

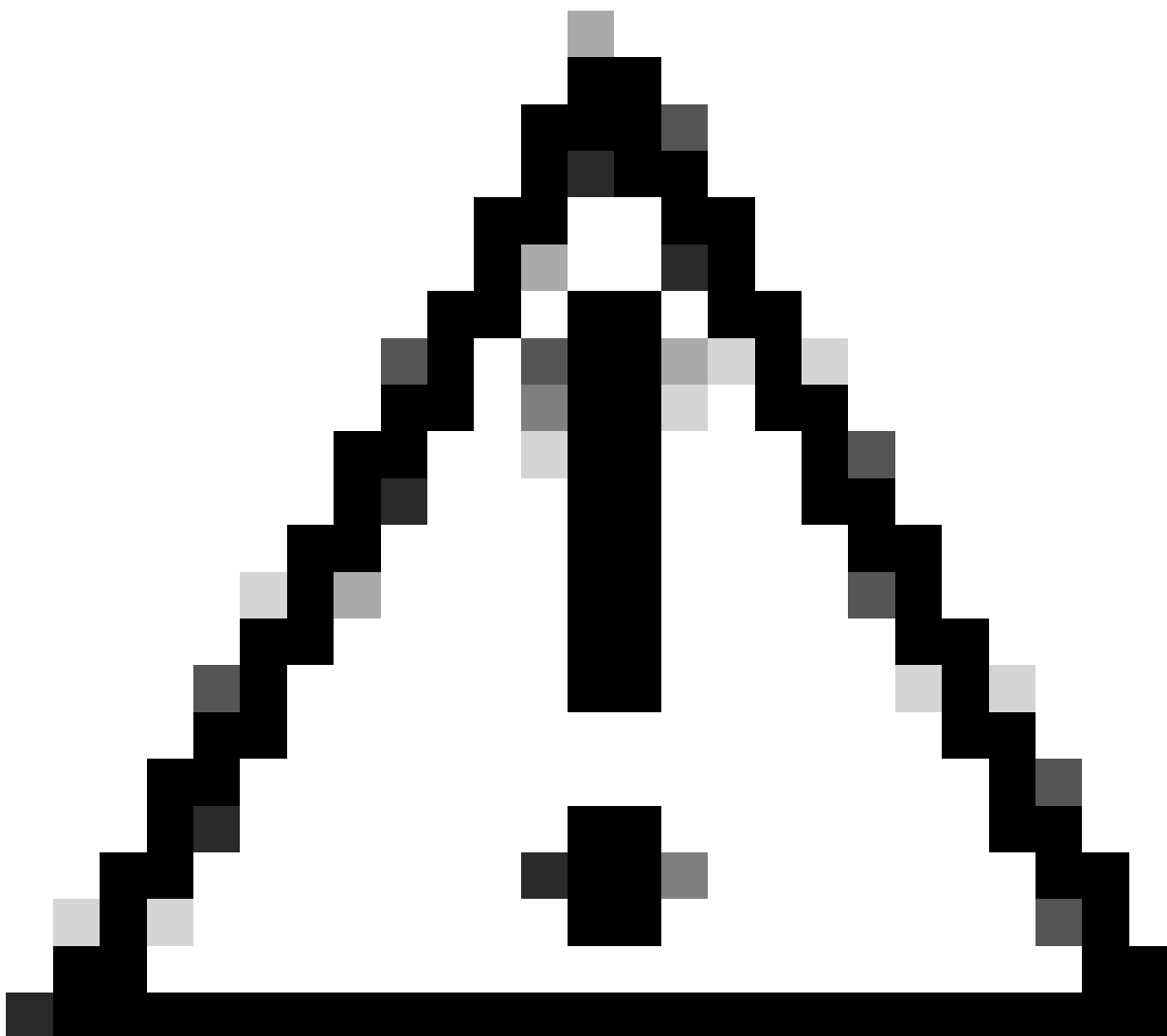
Auth Key Mgmt

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\*

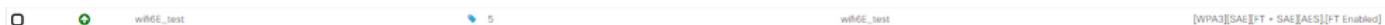




Attenzione: nella gestione delle chiavi di autenticazione, il WLC consente di selezionare FT+SAE senza abilitare SAE, tuttavia è stato osservato che i client non sono stati in grado di connettersi. Per utilizzare SAE con Transizione rapida, attivare sempre entrambe le caselle di controllo SAE e FT+SAE.

---

Visualizzare sull'interfaccia WLC delle impostazioni di sicurezza WLAN:



Verifica dell'OTA dei beacon:

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=27, F/W=, Flags=.....C, B=100, SSID="wifi6_test"
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, B=100, SSID="wifi6_test"
3	2023-06-12 18:34:49.50957	0.102287	Cisco_13:180:e7	Eurocast	802.11	588	5	-37 dBm	Beacon frame, S/W=27, F/W=, Flags=.....C, B=100, SSID="wifi6_test"
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, B=100, SSID="wifi6_test"
5	2023-06-12 18:34:49.79180	0.099672	Hetger_48:70:35	Cisco_13:180:e7	802.11	360	5	-49 dBm	Probe Request, S/W=8, F/W=, Flags=.....C, SSID="wifi6_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=1, F/W=, Flags=.....C, SSID="wifi6_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=27, F/W=, Flags=.....C, B=100, SSID="wifi6_test"
10	2023-06-12 18:34:49.81282	0.015789	Hetger_48:70:35	Cisco_13:180:e7	802.11	360	5	-49 dBm	Probe Request, S/W=1, F/W=, Flags=.....C, SSID="wifi6_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	0.060459	Hetger_48:70:35	Cisco_13:180:e7	802.11	194	5	-49 dBm	Authentication, S/W=, 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	0.021812	Cisco_13:180:e7	Hetger_48:70:35	802.11	194	5	-37 dBm	Authentication, S/W=54, 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, B=100, SSID="wifi6_test"
17	2023-06-12 18:34:49.90496	0.000000	Hetger_48:70:35	Cisco_13:180:e7	802.11	130	5	-49 dBm	Authentication, S/W=, F/W=, Flags=.....C
18	2023-06-12 18:34:49.90496	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-37 dBm	Acknowledgment, Flags=.....C
19	2023-06-12 18:34:49.90496	0.000000	Cisco_13:180:e7	Hetger_48:70:35	802.11	130	5	-37 dBm	Authentication, S/W=7, F/W=, Flags=.....C
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	Hetger_48:70:35	Cisco_13:180:e7	802.11	216	5	-49 dBm	Association Request, S/W=, F/W=, Flags=.....C, SSID="wifi6_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	Hetger_48:70:35	802.11	262	5	-36 dBm	Association Response, S/W=, 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	Hetger_48:70:35	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	Hetger_48:70:35	Eurocast	LLC	114	5	-36 dBm	U, func(unknown): DSAP 0x7a Individual, SSAP 0x0a Response
27	2023-06-12 18:34:49.92236	0.001827	Hetger_48:70:35	Hetger_48:70:35	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, B=100, SSID="wifi6_test"
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, B=100, SSID="wifi6_test"
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=27, F/W=, Flags=.....C, B=100, SSID="wifi6_test"
32	2023-06-12 18:34:50.21161	0.007815	Hetger_48:70:35	Cisco_13:180:e7	802.11	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	192.168.1.15	192.168.1.121	802.11	76	5	-48 dBm	Acknowledgment, Flags=.....C
35	2023-06-12 18:34:50.21376	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-48 dBm	Acknowledgment, Flags=.....C
36	2023-06-12 18:34:50.21454	0.000978	Hetger_48:70:35	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 18:34:50.21454	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-42 dBm	Acknowledgment, Flags=.....C
39	2023-06-12 18:34:50.22049	0.006328	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 18:34:50.22049	0.000000	192.168.1.15	192.168.1.121	802.11	221	5	-44 dBm	U, func(unknown): DSAP 0x0b Group, SSAP 0x0d Response
41	2023-06-12 18:34:50.22049	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-54 dBm	Acknowledgment, Flags=.....C

SAE WPA3 + beacon FT

Qui possiamo osservare i client Wi-Fi 6E che associano:

Intel AX211

OTA connessione con lo stato attivo sulle informazioni RSN dal client:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
1811	2023-06-12 18:51:39.24979	0.017137	IntelCor_98:58:f8	Cisco_13:180:e7	802.11	194	5	-42 dBm	Authentication, S/W=, 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	0.007834	Cisco_13:180:e7	IntelCor_98:58:f8	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	0.005567	IntelCor_98:58:f8	Cisco_13:180:e7	802.11	130	5	-48 dBm	Authentication, S/W=, 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	0.004225	Cisco_13:180:e7	IntelCor_98:58:f8	802.11	130	5	-36 dBm	Authentication, S/W=50, 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	IntelCor_98:58:f8	Cisco_13:180:e7	802.11	250	5	-46 dBm	Association Request, S/W=, F/W=, Flags=.....C, SSID="wifi6_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	IntelCor_98:58:f8	Broadcast	LLC	114	5	-36 dBm	I, H(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 18:51:39.28187	0.003705	Cisco_13:180:e7	Broadcast	802.11	517	5	-36 dBm	Beacon frame, S/W=71, F/W=, Flags=.....C, B=100, SSID="wifi6_test_02"
1825	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
1826	2023-06-12 18:51:39.28187	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-52 dBm	Clear-to-send, Flags=.....C
1827	2023-06-12 18:51:39.332425	0.017227	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1828	2023-06-12 18:51:39.331349	0.055835	Cisco_13:180:e7	Broadcast	802.11	517	5	-37 dBm	Beacon frame, S/W=76, F/W=, Flags=.....C, B=100, SSID="wifi6_test_02"
1829	2023-06-12 18:51:39.331349	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-53 dBm	Clear-to-send, Flags=.....C
1830	2023-06-12 18:51:39.339308	0.001348	192.168.1.15	192.168.1.121	802.11	82	5	-38 dBm	Request-to-send, Flags=.....C
1831	2023-06-12 18:51:39.339308	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-38 dBm	Request-to-send, Flags=.....C
1832	2023-06-12 18:51:39.339308	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1833	2023-06-12 18:51:39.339308	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1834	2023-06-12 18:51:39.339308	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1835	2023-06-12 18:51:39.339308	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1836	2023-06-12 18:51:39.339308	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1837	2023-06-12 18:51:39.339308	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 18:51:39.339308	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 18:51:39.339308	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 18:51:39.339308	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 18:51:39.339308	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 18:51:39.339308	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 18:51:39.339308	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 18:51:39.339308	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 18:51:39.339308	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 18:51:39.339308	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 18:51:39.339308	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 18:51:39.339308	0.000000	192.168.1.15	192.1					

```

(pcapmeta) [d] (vlan_addr == 200.2558.5807) || (vlan_fc_type_subtype == 0x0016) || (vlan_fc_type_subtype == 0x0008)
No. Time Delta Source Destination Protocol Length Channel Signal strength Info
226 2023-06-12 18:53:11.488353 0.000229 Interior_98:58:0F Interior_98:.. LLC 325 5 -75 dBm S, func=8, N(0):0; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
227 2023-06-12 18:53:11.488353 0.000229 Interior_98:58:0F Interior_98:.. LLC 325 5 -75 dBm S, func=9, N(0):0; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
228 2023-06-12 18:53:11.489318 0.000000 Interior_98:58:0F Interior_98:.. LLC 325 5 -49 dBm S, func=8, N(0):0; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
229 2023-06-12 18:53:11.489318 0.000000 Interior_98:58:0F Interior_98:.. LLC 325 5 -74 dBm S, func=9, N(0):0; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
230 2023-06-12 18:53:11.491642 0.000483 Interior_98:58:0F Interior_98:.. LLC 325 5 -74 dBm S, func=8, N(0):0; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
231 2023-06-12 18:53:11.491642 0.000484 Interior_98:58:0F Interior_98:.. LLC 325 5 -74 dBm S, func=9, N(0):0; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
232 2023-06-12 18:53:11.491639 0.000435 Interior_98:58:0F Interior_98:.. LLC 325 5 -74 dBm S, func=8, N(0):0; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
233 2023-06-12 18:53:11.491639 0.000435 Interior_98:58:0F Interior_98:.. LLC 325 5 -74 dBm S, func=9, N(0):0; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
234 2023-06-12 18:53:11.491377 0.000000 Interior_98:58:0F Interior_98:.. LLC 325 5 -80 dBm S, func=8, N(0):0; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
235 2023-06-12 18:53:11.491377 0.000000 Interior_98:58:0F Interior_98:.. LLC 325 5 -76 dBm S, func=9, N(0):0; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
236 2023-06-12 18:53:11.491242 0.000045 Interior_98:58:0F Interior_98:.. LLC 325 5 -77 dBm S, func=8, N(0):0; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
237 2023-06-12 18:53:11.491242 0.000045 Interior_98:58:0F Interior_98:.. LLC 325 5 -77 dBm S, func=9, N(0):0; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
238 2023-06-12 18:53:11.491242 0.000045 Interior_98:58:0F Interior_98:.. LLC 325 5 -77 dBm S, func=8, N(0):0; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
239 2023-06-12 18:53:11.491242 0.000045 Interior_98:58:0F Interior_98:.. LLC 325 5 -77 dBm S, func=9, N(0):0; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
240 2023-06-12 18:53:11.513546 0.000434 Cisco_13:18:07 Interior_98:.. LLC 325 5 -77 dBm S, func=8, N(0):0; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
241 2023-06-12 18:53:11.513546 0.000434 Cisco_13:18:07 Interior_98:.. LLC 325 5 -77 dBm S, func=9, N(0):0; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
242 2023-06-12 18:53:11.513546 0.000000 192.168.1.15 192.168.1.121 802.11 96 5 -36 dBm Authentication, ShwA, Phw, Flags.....C
243 2023-06-12 18:53:11.513546 0.000000 192.168.1.15 192.168.1.121 802.11 96 5 -36 dBm Acknowledgment, Flags.....C
244 2023-06-12 18:53:11.513546 0.000000 192.168.1.15 192.168.1.121 802.11 272 5 -46 dBm Reassociation Request, ShwA, Phw, Flags.....C, SSID="WiFi6_test"
245 2023-06-12 18:53:11.513546 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -36 dBm Acknowledgment, Flags.....C
246 2023-06-12 18:53:11.527645 0.011847 Cisco_13:18:07 Interior_98:.. LLC 325 5 -36 dBm Reassociation Response, ShwA, Phw, Flags.....C
247 2023-06-12 18:53:11.527645 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -42 dBm Acknowledgment, Flags.....C
248 2023-06-12 18:53:11.528445 0.000749 Broadcast L2 114 5 -36 dBm I P, N(0):4, N(1):2; DSAP MMS Group, SSAP MMS Command
249 2023-06-12 18:53:11.528445 0.000040 Interior_98:58:0F Broadcast L2 114 5 -36 dBm Request-to-send, Flags.....C
250 2023-06-12 18:53:11.528445 0.000040 Interior_98:58:0F Broadcast L2 114 5 -36 dBm Key (Message 1 of 4)
251 2023-06-12 18:53:11.528445 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -47 dBm Acknowledgment, Flags.....C
252 2023-06-12 18:53:11.531348 0.000238 Interior_98:58:0F EAPOL 246 5 -47 dBm Key (Message 2 of 4)
253 2023-06-12 18:53:11.531348 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -36 dBm Acknowledgment, Flags.....C
254 2023-06-12 18:53:11.531348 0.000000 192.168.1.15 192.168.1.121 802.11 82 5 -36 dBm Request-to-send, Flags.....C
255 2023-06-12 18:53:11.531348 0.000000 192.168.1.15 192.168.1.121 802.11 82 5 -36 dBm Key (Message 3 of 4)
256 2023-06-12 18:53:11.531348 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -36 dBm Acknowledgment, Flags.....C
257 2023-06-12 18:53:11.531348 0.000000 192.168.1.15 192.168.1.121 802.11 82 5 -46 dBm Request-to-send, Flags.....C, R1=000, SSID="WiFi6_test_02"
258 2023-06-12 18:53:11.531348 0.000000 192.168.1.15 192.168.1.121 802.11 82 5 -46 dBm Request-to-send, Flags.....C
259 2023-06-12 18:53:11.531348 0.000000 CiscoCom_53:c1:c9 Interior_98:.. LLC 187 5 -42 dBm I, N(0):8, N(1):2; DSAP NULL LSAP Group, SSAP WMS Command
260 2023-06-12 18:53:11.531348 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -72 dBm Acknowledgment, Flags.....C
261 2023-06-12 18:53:11.531348 0.000000 192.168.1.15 192.168.1.121 802.11 82 5 -72 dBm Request-to-send, Flags.....C
262 2023-06-12 18:53:11.531348 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -36 dBm Clear-to-send, Flags.....C
263 2023-06-12 18:53:11.531348 0.000000 Interior_98:58:0F Broadcast L2 515 5 -75 dBm I P, N(0):7, N(1):7; DSAP WMS Individual, SSAP WMS Command
264 2023-06-12 18:53:11.531348 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -36 dBm Acknowledgment, Flags.....C

```

### SAE WPA3 + richiesta di riassociazione FT

### Dettagli client in WLC:

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The 'Clients' tab is active, displaying a list of 12 clients. The selected client is '286b.3598.580f' with IP address '192.168.1.159' and AP name 'AP01\_RC\_9136\_F80C'. The detailed view on the right shows the following information:

- Client Properties:** Client State Servers: None; Client ACLs: None; Client Entry Create Time: 380 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; IIF ID: 0x90000010; Authorized: TRUE; Common Session ID: 0000000000000FC9B0F311A6; Act Session ID: 0x00000000; Auth Method Status List: SAE.

### NetGear A8000

### OTA connessione con lo stato attivo sulle informazioni RSN dal client. Connessione iniziale:

```

No. Time Delta Source Destination Protocol Length Channel Signal strength BSS ID Info
1 18:54:49.385337 0.000000 Cisco_13:18:07 Broadcast 802.11 508 5 -36 dBm 38:53:17:13:8047 Beacon frame, ShwA2, Phw, Flags.....C, R1=000, SSID="WiFi6_test_02", SSID="Wif
2 18:54:49.487544 0.102267 Cisco_13:18:07 Broadcast 802.11 508 5 -36 dBm 38:53:17:13:8047 Beacon frame, ShwA2, Phw, Flags.....C, R1=000, SSID="WiFi6_test_02", SSID="Wif
3 18:54:49.589807 0.102212 Cisco_13:18:07 Broadcast 802.11 508 5 -37 dBm 38:53:17:13:8047 Beacon frame, ShwA2, Phw, Flags.....C, R1=000, SSID="WiFi6_test_02", SSID="Wif
4 18:54:49.692032 0.102166 Cisco_13:18:07 Broadcast 802.11 508 5 -37 dBm 38:53:17:13:8047 Beacon frame, ShwA2, Phw, Flags.....C, R1=000, SSID="WiFi6_test_02", SSID="Wif
5 18:54:49.794284 0.000000 Netgear_48:78:95 Cisco_13:18:07 802.11 368 5 -49 dBm 38:53:17:13:8047 Probe Request, ShwA, Phw, Flags.....C, SSID="WiFi6_test"
6 18:54:49.794284 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -37 dBm Acknowledgment, Flags.....C
7 18:54:49.795246 0.000052 Netgear_48:78:95 Cisco_13:18:07 802.11 368 5 -49 dBm 38:53:17:13:8047 Probe Request, ShwA, Phw, Flags.....C, SSID="WiFi6_test"
8 18:54:49.795246 0.000071 192.168.1.15 192.168.1.121 802.11 76 5 -37 dBm Acknowledgment, Flags.....C
9 18:54:49.796949 0.000056 Cisco_13:18:07 Broadcast 802.11 384 5 -49 dBm 38:53:17:13:8047 Beacon frame, ShwA2, Phw, Flags.....C, R1=000, SSID="WiFi6_test_02", SSID="Wif
10 18:54:49.892682 0.051789 Netgear_48:78:95 Cisco_13:18:07 802.11 368 5 -49 dBm 38:53:17:13:8047 Probe Request, ShwA, Phw, Flags.....C, SSID="WiFi6_test"
11 18:54:49.892682 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -37 dBm Acknowledgment, Flags.....C
12 18:54:49.892682 0.000000 192.168.1.15 192.168.1.121 802.11 246 5 -49 dBm Authentication, ShwA, Phw, Flags.....C
13 18:54:49.892682 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -49 dBm Acknowledgment, Flags.....C
14 18:54:49.892682 0.021232 Cisco_13:18:07 Netgear_48:78:95 802.11 394 5 -37 dBm 38:53:17:13:8047 Authentication, ShwA6, Phw, Flags.....C
15 18:54:49.892682 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -49 dBm Acknowledgment, Flags.....C
16 18:54:49.892682 0.000000 Cisco_13:18:07 Broadcast 802.11 384 5 -37 dBm 38:53:17:13:8047 Beacon frame, ShwA2, Phw, Flags.....C, R1=000, SSID="WiFi6_test_02", SSID="Wif
17 18:54:49.892682 0.000000 Netgear_48:78:95 Cisco_13:18:07 802.11 368 5 -49 dBm 38:53:17:13:8047 Beacon frame, ShwA2, Phw, Flags.....C, R1=000, SSID="WiFi6_test_02", SSID="Wif
18 18:54:49.892682 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -37 dBm Acknowledgment, Flags.....C
19 18:54:49.892682 0.000000 Netgear_48:78:95 Cisco_13:18:07 802.11 368 5 -49 dBm 38:53:17:13:8047 Authentication, ShwA, Phw, Flags.....C
20 18:54:49.892682 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -49 dBm Acknowledgment, Flags.....C
21 18:54:49.892682 0.000000 Netgear_48:78:95 Cisco_13:18:07 802.11 246 5 -49 dBm 38:53:17:13:8047 Association Request, ShwA, Phw, Flags.....C, SSID="WiFi6_test"
22 18:54:49.892682 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -36 dBm Acknowledgment, Flags.....C
23 18:54:49.892682 0.000000 Cisco_13:18:07 Netgear_48:78:95 802.11 262 5 -36 dBm 38:53:17:13:8047 Association Response, ShwA, Phw, Flags.....C
24 18:54:49.921474 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -49 dBm 38:53:17:13:8047 I, func=8; DSAP MMS Individual, SSAP MMS Command
25 18:54:49.921474 0.000045 Netgear_48:78:95 Broadcast L2 114 5 -37 dBm 38:53:17:13:8047 U, func=8; DSAP MMS Individual, SSAP MMS Command
26 18:54:49.921474 0.000000 Netgear_48:78:95 Broadcast L2 114 5 -36 dBm 38:53:17:13:8047 U, func=9; DSAP MMS Individual, SSAP MMS Command
27 18:54:49.922046 0.000000 Cisco_13:18:07 Netgear_48:78:95 EAPOL 221 5 -36 dBm 38:53:17:13:8047 Key (Message 1 of 4)
28 18:54:49.922046 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -49 dBm Acknowledgment, Flags.....C
29 18:54:49.922046 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -49 dBm Acknowledgment, Flags.....C
30 18:54:49.922046 0.000000 Netgear_48:78:95 Cisco_13:18:07 802.11 394 5 -36 dBm 38:53:17:13:8047 Beacon frame, ShwA2, Phw, Flags.....C, R1=000, SSID="WiFi6_test_02", SSID="Wif
31 18:54:49.922046 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -36 dBm Acknowledgment, Flags.....C
32 18:54:49.922046 0.000000 Netgear_48:78:95 Cisco_13:18:07 802.11 368 5 -37 dBm 38:53:17:13:8047 Beacon frame, ShwA2, Phw, Flags.....C, R1=000, SSID="WiFi6_test_02", SSID="Wif
33 18:54:49.922046 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -49 dBm Acknowledgment, Flags.....C
34 18:54:49.922046 0.001761 Cisco_13:18:07 Netgear_48:78:95 EAPOL 205 5 -36 dBm 38:53:17:13:8047 Key (Message 1 of 4)
35 18:54:49.922046 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -49 dBm Acknowledgment, Flags.....C
36 18:54:49.922046 0.000000 Netgear_48:78:95 Cisco_13:18:07 802.11 394 5 -36 dBm 38:53:17:13:8047 Beacon frame, ShwA2, Phw, Flags.....C, R1=000, SSID="WiFi6_test_02", SSID="Wif
37 18:54:49.922046 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -42 dBm Acknowledgment, Flags.....C
38 18:54:49.922046 0.000000 192.168.1.15 192.168.1.121 802.11 82 5 -42 dBm Request-to-send, Flags.....C
39 18:54:49.922046 0.001528 Netgear_48:78:95 Netgear_48:78:95 802.11 119 5 -48 dBm Trigger Buffer Status Report PDU (BSRP), Flags.....C
40 18:54:49.922046 0.000000 192.168.1.15 192.168.1.121 802.11 231 5 -44 dBm 38:53:17:13:8047 U, func=9; DSAP MMS Group, SSAP MMS Response
41 18:54:49.922046 0.000000 192.168.1.15 192.168.1.121 802.11 76 5 -44 dBm Acknowledgment, Flags.....C

```



## Dettagli client 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 the first one selected. The selected client's details are shown in a 'Client' panel on the right, including 'General', 'QoS Statistics', 'ATF Statistics', 'Mobility History', and 'Call Statistics' tabs. 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

Impossibile eseguire il roaming del dispositivo quando FT è abilitato.

## Samsung S23

Impossibile eseguire il roaming del dispositivo quando FT è abilitato.

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

## Configurazione della sicurezza WLAN:

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface in the 'Configuration > Tags & Profiles > WLANs' section. The 'wif6E\_test' WLAN is selected and highlighted with a red box. The 'Edit WLAN' panel on the right shows the configuration for this WLAN. The 'Security' tab is active, showing 'Layer2' settings. The 'WPA Parameters' section has 'WPA3' selected. The 'WPA2/WPA3 Encryption' section has 'AES(CCMP128)' and 'GCMP128' selected. The 'Protected Management Frame' section has 'PMF' set to 'Required'. The 'Auth Key Mgmt' section has 'SAE', 'OWE', and '802.1x-SHA256' selected, and 'FT + SAE' and 'FT + 802.1x' are also visible. A red box highlights the 'Auth Key Mgmt' section.

WPA3 Enterprise 802.1x-SHA256 + Configurazione protezione FTWLAN

## Visualizzare sull'interfaccia WLC delle impostazioni di sicurezza WLAN:

The screenshot shows the bottom status bar of the Cisco Catalyst 9800-CL Wireless Controller interface. It displays the selected WLAN 'wif6E\_test' and its ID '5'. The security configuration is shown as '[WPA3][FT + 802.1x][AES][PMF 802.1x][FT Enabled]'. The status bar also includes a search icon and a 'Feedback' button.

Qui possiamo vedere i log di ISE Live che mostrano le autenticazioni provenienti da ciascun



Un comportamento interessante si verifica se si elimina manualmente il client dalla WLAN (ad esempio dalla GUI del WLC). Il client riceve un frame di disassociazione ma tenta di riconnettersi allo stesso access point e utilizza un frame di riassociazione seguito da uno scambio EAP completo perché i dettagli del client sono stati eliminati dall'access point/WLC.

Si tratta sostanzialmente dello stesso scambio di frame di un nuovo processo di associazione. Qui è possibile vedere lo scambio di frame:

Flusso di connessione WPA3 Enterprise 802.1x + FT Ax211

Dettagli client in WLC:

WPA3 Enterprise 802.1x + dettagli sul client FT

Anche questo client è stato testato utilizzando FT su DS ed è stato in grado di eseguire il roaming utilizzando 802.11r:





No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
878	1.408897	0.263322	Cisco_08:00:18	Broadcast	802.11	428	69-17	dm	Beacon frame, SN=3662, FwB, Flags=.....C, BI=100, SSID=W
880	1.409017	0.120770	Cisco_72:8a:96	Broadcast	802.11	204	69-17	dm	Probe Request, SN=3680, FwB, Flags=.....C, SSID=Wifi6E, S
882	1.409162	0.000405	Cisco_08:00:18	Broadcast	802.11	428	69-17	dm	Beacon frame, SN=3662, FwB, Flags=.....C, BI=100, SSID=W
884	1.409317	0.000716	Cisco_08:00:18	Broadcast	802.11	374	69-17	dm	Probe Response, SN=3680, FwB, Flags=.....C, BI=100, SSID=W
928	1.479576	0.114490	Cisco_08:00:18	Broadcast	802.11	428	69-17	dm	Beacon frame, SN=3662, FwB, Flags=.....C, BI=100, SSID=W
932	1.479709	0.000213	Google_72:8a:96	Cisco_08:00:18	802.11	308	69-14	dm	Authentication, SN=0111, FwB, Flags=.....C
934	1.479789	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-17	dm	Acknowledgment, Flags=.....C
936	1.479951	0.000382	Cisco_08:00:18	Broadcast	802.11	108	69-17	dm	Authentication, SN=14, FwB, Flags=.....C
938	1.479952	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-14	dm	Acknowledgment, Flags=.....C
940	1.480284	0.000508	Cisco_72:8a:96	Cisco_08:00:18	802.11	264	69-14	dm	Association Request, SN=0082, FwB, Flags=.....C, SSID=Wifi6E
942	1.480321	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-17	dm	Acknowledgment, Flags=.....C
944	1.480511	0.023970	Cisco_08:00:18	Cisco_72:8a:96	802.11	313	69-17	dm	Association Response, SN=0, FwB, Flags=.....C
946	1.480521	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-13	dm	Acknowledgment, Flags=.....C
948	1.480629	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-13	dm	Acknowledgment, Flags=.....C
950	1.480709	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-13	dm	Acknowledgment, Flags=.....C
952	1.480809	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-11	dm	Acknowledgment, Flags=.....C
954	1.481077	0.017007	Google_72:8a:96	Cisco_08:00:18	EAP	1377	69-13	dm	Response, Identity
956	1.481377	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-17	dm	Acknowledgment, Flags=.....C
958	1.481624	0.012047	Cisco_08:00:18	Cisco_72:8a:96	EAP	118	69-17	dm	Request, Protected EAP (EAP-PEAP)
960	1.481744	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-11	dm	Acknowledgment, Flags=.....C
962	1.481896	0.000672	Cisco_08:00:18	Broadcast	802.11	428	69-17	dm	Beacon frame, SN=3662, FwB, Flags=.....C, BI=100, SSID=W
964	1.481944	0.000180	Google_72:8a:96	Cisco_08:00:18	LIC	124	69-17	dm	Request, 1 N(1)=0, N(5)=1; SOAP Envs Individual, SOAP NameSpace
966	1.481957	0.000000	Cisco_08:00:18	Cisco_08:00:18	802.11	76	69-17	dm	Acknowledgment, Flags=.....C
968	1.481957	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-17	dm	Acknowledgment, Flags=.....C
970	1.481957	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-17	dm	Acknowledgment, Flags=.....C
972	1.481957	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-17	dm	Acknowledgment, Flags=.....C
974	1.481957	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-17	dm	Acknowledgment, Flags=.....C
976	1.481957	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-17	dm	Acknowledgment, Flags=.....C
978	1.481957	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-17	dm	Acknowledgment, Flags=.....C
980	1.481957	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-17	dm	Acknowledgment, Flags=.....C
982	1.481957	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-17	dm	Acknowledgment, Flags=.....C
984	1.481957	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-17	dm	Acknowledgment, Flags=.....C
986	1.481957	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-17	dm	Acknowledgment, Flags=.....C
988	1.481957	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-17	dm	Acknowledgment, Flags=.....C
990	1.481957	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-17	dm	Acknowledgment, Flags=.....C
992	1.481957	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-17	dm	Acknowledgment, Flags=.....C
994	1.481957	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-17	dm	Acknowledgment, Flags=.....C
996	1.481957	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-17	dm	Acknowledgment, Flags=.....C
998	1.481957	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-17	dm	Acknowledgment, Flags=.....C
1000	1.481957	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-17	dm	Acknowledgment, Flags=.....C
1002	1.481957	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-17	dm	Acknowledgment, Flags=.....C
1004	1.481957	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-17	dm	Acknowledgment, Flags=.....C
1006	1.481957	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-17	dm	Acknowledgment, Flags=.....C
1008	1.481957	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-17	dm	Acknowledgment, Flags=.....C
1010	1.481957	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-17	dm	Acknowledgment, Flags=.....C

```

> frame 925: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits) on interface DeviceWPF_04578005-2998-4056-8C33-C3413
> Ethernet II, Src: Cisco_02:19:747 (14:11:1b:02:19:747), Dst: Anderson_07:c9:a37e (08:1a:0b:07:c9:a37e)
> Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.121
> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
> AiroHw/0x1f0000 encapsulated IEEE 802.11
> IEEE 802.11 radio information
> IEEE 802.11 Association Request, Flags: .....C
> Tagged parameters (167 bytes)
> Fixed parameters (4 bytes)
> Tag: SSID parameter set: "Wifi6E_test"
> Tag: Supported Rates (6R), 9, 12(R), 18, 24(R), 36, 48, 54, [Mbit/sec]
> Tag: Power Capability Mtr: 7, Max: 29
> Tag: Supported Channels
> TAG: RSN Information
> Tag Number: 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) OUI: 00:0f:ac (See IEEE 802.11)
> 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
> .....0B = RSN No Pairwise capabilities: Transmitter can support MP default key @ simultaneously w/dt
> .....0B = RSN PTKSA Replay Counter capabilities: 1 replay counter per PTKSA/PTKSA/STakeySA (0x0)
> .....0B = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/PTKSA/STakeySA (0x0)
> .....1 = Management frame Protection Required: True
> .....1 = Management frame Protection Capable: True
> .....0B = 32bit MIC11-band RSN: false
> .....0B = PerKey Enabled: false
> .....0B = Extended key ID for Individually Addressed Frames: Not supported
> PTKID Count: 0
> PTKID List:
> Group Management Cipher Suite: 00:0f:ac (See IEEE 802.11) BIP (128)
> TAG: W/ Enabled Capabilities (5 octets)
> TAG: Mobility domain
> TAG: Supported Operating Classes
> TAG: Extended Capabilities (20 octets)
> Ext Tag: HE Capabilities
> Ext Tag: HE 4-0 Band Capabilities
> TAG: Vendor Specific: Broadcom
> Tag Number: Vendor Specific (221)
> Tag Length: 10
> OUI: 00:13:18 (Broadcom)
> Vendor Specific OUI Type: 2
> Vendor Specific Data: 0000000000000000
> TAG: Vendor Specific: Microsoft Corp.: WPA/WPA2 Information Element

```

WPA3 Enterprise 802.1x + associazione FT Pixel6a

Dettagli client in WLC:

Dettagli sul client WPA3 Enterprise 802.1x + FT Pixel6a

Concentrati sul tipo di roaming Over the Air dove possiamo vedere il tipo di roaming 802.11R:

Samsung S23

OTA connessione con lo stato attivo sulle informazioni RSN dal client:





No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
1246	8.295985	0.102133	Cisco_d5:80:18	Broadcast	802.11	364	69	-39 dBm	Beacon frame, SW=385, Fw=0, Flags=.....C, BI=300, SSID="wif
1247	8.401935	0.102170	Cisco_d5:80:18	Broadcast	802.11	364	69	-40 dBm	Beacon frame, SW=386, Fw=0, Flags=.....C, BI=300, SSID="wif
1248	8.504375	0.102420	Cisco_d5:80:18	Broadcast	802.11	364	69	-39 dBm	Beacon frame, SW=387, Fw=0, Flags=.....C, BI=300, SSID="wif
1249	8.606824	0.102419	Cisco_d5:80:18	Broadcast	802.11	364	69	-40 dBm	Beacon frame, SW=388, Fw=0, Flags=.....C, BI=300, SSID="wif
1251	8.612759	0.005945	Cisco_d5:80:18	Broadcast	802.11	312	69	-40 dBm	Probe Response, SW=459, Fw=0, Flags=.....C, BI=300, SSID="w
1258	8.701133	0.096374	Cisco_d5:80:18	Broadcast	802.11	364	69	-39 dBm	Beacon frame, SW=310, Fw=0, Flags=.....C, BI=300, SSID="wif
1260	8.786422	0.077279	Samsung_c9:e3:71	Cisco_d5:80:18	802.11	235	69	-48 dBm	Authentication, SW=99, Fw=0, Flags=.....C
1261	8.786422	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-39 dBm	Acknowledgement, Flags=.....C
1262	8.790571	0.004159	Cisco_d5:80:18	Samsung_c9:e3:71	802.11	247	69	-39 dBm	Authentication, SW=118, Fw=0, Flags=.....C
1263	8.790571	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-47 dBm	Acknowledgement, Flags=.....C
1265	8.796439	0.005968	Samsung_c9:e3:71	Cisco_d5:80:18	802.11	485	69	-48 dBm	Association Request, SW=300, Fw=0, Flags=.....C, SSID="wif
1266	8.796439	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-39 dBm	Acknowledgement, Flags=.....C
1268	8.800749	0.005639	Samsung_c9:e3:71	Broadcast	LLC	114	69	-39 dBm	S, Func=02, N(5)=17; DSAP 0x0a Group, SSAP 0x0a Command
1269	8.807940	0.003362	Cisco_d5:80:18	Samsung_c9:e3:71	802.11	413	69	-39 dBm	Association Response, SW=0, Fw=0, Flags=.....C
1270	8.807940	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-48 dBm	Acknowledgement, Flags=.....C
1271	8.807940	0.000000	Samsung_c9:e3:71	Broadcast	LLC	120	69	-39 dBm	I P, N(5)=11, N(5)=19; DSAP 0x08 Individual, SSAP 0x0a Respons
1272	8.813121	0.003381	Cisco_d5:80:18	Broadcast	802.11	364	69	-39 dBm	Beacon frame, SW=311, Fw=0, Flags=.....C, BI=300, SSID="wif
1273	8.832754	0.012133	Cisco_Sc:F8:0c	Samsung_c9:e3:71	LLC	183	69	-40 dBm	U, Func=01C; DSAP 0x0a Group, SSAP 0x0a Command
1274	8.832754	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-58 dBm	Acknowledgement, Flags=.....C
1275	8.832754	0.000000	Cisco_Sc:F8:0c	Samsung_c9:e3:71	LLC	183	69	-49 dBm	U, Func=unknown; DSAP Texas Instruments Group, SSAP 0x28 Respo
1276	8.832817	0.000063	192.168.1.15	192.168.1.121	802.11	76	69	-58 dBm	Acknowledgement, Flags=.....C
1277	8.800540	0.007723	Samsung_c9:e3:71	Broadcast	LLC	144	69	-46 dBm	S P, Func=02, N(5)=32; DSAP 0x0a Individual, SSAP 0x0a Respon
1278	8.800540	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-40 dBm	Acknowledgement, Flags=.....C
1280	8.804143	0.003603	Cisco_d5:80:18	Samsung_c9:e3:71	802.11	118	69	-40 dBm	Action, SW=1, Fw=0, Flags=p.....C
1281	8.804143	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-47 dBm	Acknowledgement, Flags=.....C
1282	8.804803	0.000660	Samsung_c9:e3:71	Cisco_d5:80:18	802.11	115	69	-47 dBm	Action, SW=0, Fw=0, Flags=p.....C
1283	8.804803	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-40 dBm	Acknowledgement, Flags=.....C
1284	8.806878	0.002075	Altiocel_a3e:59:af	Samsung_c9:e3:71	LLC	197	69	-50 dBm	I P, N(5)=25, N(5)=40; DSAP 0x0a Individual, SSAP 0x0a Command
1286	8.913192	0.007034	Cisco_d5:80:18	Broadcast	802.11	364	69	-41 dBm	Beacon frame, SW=311, Fw=0, Flags=.....C, BI=300, SSID="wif
1287	8.950493	0.036381	Cisco_d5:80:18	Broadcast	802.11	364	69	-39 dBm	Acknowledgement, Flags=.....C
1322	9.375553	0.029908	192.168.1.15	192.168.1.121	802.11	76	69	-39 dBm	Acknowledgement, Flags=.....C
1372	9.851619	0.040566	Cisco_d5:80:18	Broadcast	802.11	364	69	-38 dBm	Beacon frame, SW=314, Fw=0, Flags=.....C, BI=300, SSID="wif
1471	9.181683	0.102164	Cisco_d5:80:18	Broadcast	802.11	364	69	-39 dBm	Beacon frame, SW=315, Fw=0, Flags=.....C, BI=300, SSID="wif
1600	9.176834	0.058111	192.168.1.15	192.168.1.121	802.11	76	69	-40 dBm	Acknowledgement, Flags=.....C
1702	9.221145	0.044131	Cisco_d5:80:18	Broadcast	802.11	364	69	-39 dBm	Beacon frame, SW=316, Fw=0, Flags=.....C, BI=300, SSID="wif
1913	9.124397	0.102962	Cisco_d5:80:18	Broadcast	802.11	364	69	-39 dBm	Beacon frame, SW=317, Fw=0, Flags=.....C, BI=300, SSID="wif
1917	9.425938	0.103511	Cisco_d5:80:18	Broadcast	802.11	364	69	-40 dBm	Beacon frame, SW=318, Fw=0, Flags=.....C, BI=300, SSID="wif
1919	9.528463	0.102525	Cisco_d5:80:18	Broadcast	802.11	364	69	-38 dBm	Beacon frame, SW=319, Fw=0, Flags=.....C, BI=300, SSID="wif
1945	9.631020	0.102557	Cisco_d5:80:18	Broadcast	802.11	364	69	-38 dBm	Beacon frame, SW=320, Fw=0, Flags=.....C, BI=300, SSID="wif
1946	9.731295	0.102275	Cisco_d5:80:18	Broadcast	802.11	364	69	-39 dBm	Beacon frame, SW=321, Fw=0, Flags=.....C, BI=300, SSID="wif
1950	9.835864	0.102569	Cisco_d5:80:18	Broadcast	802.11	364	69	-40 dBm	Beacon frame, SW=322, Fw=0, Flags=.....C, BI=300, SSID="wif
1951	9.825936	0.000072	Samsung_c9:e3:71	Cisco_d5:80:18	802.11	122	69	-45 dBm	Action, SW=0, Fw=0, Flags=p.....C
1952	9.825936	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-40 dBm	Acknowledgement, Flags=.....C
1953	9.826083	0.000057	192.168.1.15	192.168.1.121	802.11	76	69	-40 dBm	Acknowledgement, Flags=.....C
1954	9.817895	0.013002	Cisco_d5:80:18	Broadcast	802.11	364	69	-40 dBm	Beacon frame, SW=323, Fw=0, Flags=.....C, BI=300, SSID="wif
1955	9.842143	0.006448	192.168.1.15	192.168.1.121	802.11	76	69	-40 dBm	Acknowledgement, Flags=.....C

```

> Frame 1265: 485 bytes on wire (3880 bits), 485 bytes captured (3880 bits) on interface Device\MPF_04578095-2
> Ethernet II, Src: Cisco_02:00:0c:70:47:47, Dst: Universa_07:cf:06 (08:0a:8b:07:cf:06)
> Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.121
> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
> AiroPcap/OnixPcap encapsulated IEEE 802.11
> IEEE 802.11 radio information
> IEEE 802.11 Association Request, Flags: .....C
> IEEE 802.11 Mgmt Management
> Fixed parameters (18 bytes)
> Tagged parameters (185 bytes)
> Tag: SSID parameter set: "wif06_test"
> Tag: Supported Rates (4B): 9, 12(B), 18, 24(B), 36, 48, 54, [Dbit/sec]
> Tag: Power Capability Mgmt 8, Max: 16
> Tag: Supported Channels
> Tag: RM Enabled Capabilities (5 octets)
> Tag: SBA information
> Tag: Mobility Domain
  > Tag Number: Mobility Domain (54)
  Tag Length: 3
  Mobility Domain Identifier: 0x027
  > FT Capability and Policy: 0x01
  .....0 = Fast BSS Transition over DS: 0x1
  .....0 = Resource Request Protocol Capability: 0x0
  0x00 0x00 = Reserved: 0x00
> Tag: Fast BSS Transition
  Tag Number: Fast BSS Transition (55)
  Tag Length: 96
  > MDC Control: 0x0000
  MDC: 0x01007f01e16ad0e4cf650a5a1a4ca
  Address: d514f017ab7fa005b76f75e1b0d0a0822cfa050b7492e10809b1a809ca
  Owner: 00120455c78a010c7ef012424259700790c0e9fa12283f566d00b2c3
  > Subelement: PMK-R1 key holder Identifier (R104-ID) (1)
  Length: 6
  PMK-R1 key holder Identifier (R104-ID): d68070d97ad0
  > Subelement: PMK-R0 key holder Identifier (R004-ID) (1)
  Length: 4
  PMK-R0 key holder Identifier (R004-ID): 002055a2
> Tag: Supported Operating Classes
> Tag: Extended Capabilities (13 octets)
> Ext Tag: Vendor Specific: Microsoft Corp.: WPA/WPA2 Information Element
> Ext Tag: HE Capabilities
> Ext Tag: HE 6 GHz Band Capabilities
> Tag: Vendor Specific: Qualcomm Inc.
> Tag: Vendor Specific: Samsung Electronics Co., Ltd
> Tag: Vendor Specific: Samsung Electronics Co., Ltd

```

Pacchetti FTtoDS roaming S23

### WPA3-Enterprise + cifratura GCMP128 + SUITEB-1X

Configurazione della sicurezza WLAN:

### 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"/>		

**WPA2/WPA3 Encryption**

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

**Protected Management Frame**

PMF

Association Comeback Timer\*

SA Query Time\*

**Fast Transition**

Status

Over the DS

Reassociation Timeout \*

**Auth Key Mgmt**

SUITEB-1X

WPA3 Enterprise Suite B-1X Security Configuration



Nota: FT non è supportato in SUITEB-1X

---

Visualizzare sull'interfaccia WLC delle impostazioni di sicurezza WLAN:

□  wif6E\_test  5 wif6E\_test [WPA3][SUITEB-1X][GCMP128]

Verifica dell'OTA dei beacon:



No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
37376	59.189776	0.820482	Cisco_05:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2062, 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	0.820508	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2063, Fw=0, Flags=.....C, B=100, SSID=...	> Ethernet II, Src: Cisco_02:00:07 (74:11:32:02:07:47), Dst: Unknown_07:c7:c7:0e (08:00:00:07:c7:0e)
37396	59.191709	0.820481	Cisco_05:00:18	Broadcast	802.11	355	69 -17 dbm	Beacon frame, SW=2064, Fw=0, Flags=.....C, B=100, SSID=...	> Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.121
37414	59.193261	0.820462	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2065, Fw=0, Flags=.....C, B=100, SSID=...	> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
37424	59.193713	0.820472	Cisco_05:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2066, Fw=0, Flags=.....C, B=100, SSID=...	> AlohaPdu/OnlinkPdu encapsulated IEEE 802.11
37437	59.194258	0.820457	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2067, Fw=0, Flags=.....C, B=100, SSID=...	> IEEE 802.11 radio information
37447	59.194792	0.820442	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2068, Fw=0, Flags=.....C, B=100, SSID=...	> IEEE 802.11 Beacon frame, Flags: .....C
37459	59.195334	0.820522	Cisco_05:00:18	Broadcast	802.11	355	69 -38 dbm	Beacon frame, SW=2069, Fw=0, Flags=.....C, B=100, SSID=...	> IEEE 802.11 Wireless Management
37470	59.196329	0.820399	Cisco_05:00:18	Broadcast	802.11	312	69 -39 dbm	Probe Response, SW=2070, Fw=0, Flags=.....C, B=100, SSID=...	> Fixed parameters (12 bytes)
37480	59.196445	0.820461	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2071, Fw=0, Flags=.....C, B=100, SSID=...	> Tagged parameters (213 bytes)
37489	59.197487	0.821342	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2072, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: SSID parameter set: "wifi6e_test"
37499	59.199116	0.821929	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2073, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: Supported Rates 6(B), 9, 12(6), 18, 24(6), 36, 48, 54, [Mbit/sec]
37520	59.195713	0.820817	Cisco_05:00:18	Broadcast	802.11	355	69 -17 dbm	Beacon frame, SW=2074, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: Traffic Indication Map (TIM): OPM # of 1 bitmap
37529	59.196888	0.820832	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2075, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: Country Information: Country Code na, Environment Global operating classes
37532	59.197236	0.821156	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2076, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: Power Constraint: 6
37539	59.197689	0.821751	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2077, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: TX Report Transmit Power: 36, Link Operat: 0
37552	59.197648	0.820459	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2078, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: RSN Information
37565	59.197993	0.820461	Cisco_05:00:18	Broadcast	802.11	355	69 -17 dbm	Beacon frame, SW=2079, Fw=0, Flags=.....C, B=100, SSID=...	> Tag Number: RSN Information (64)
37574	59.198423	0.820438	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2080, Fw=0, Flags=.....C, B=100, SSID=...	> Tag Length: 26
37585	59.198865	0.820542	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2081, Fw=0, Flags=.....C, B=100, SSID=...	> RSN Version: 1
37596	59.199439	0.820476	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2082, Fw=0, Flags=.....C, B=100, SSID=...	> Group Cipher Suite: 00000000 (IEEE 802.11) GCM (128)
37606	59.199949	0.820495	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2083, Fw=0, Flags=.....C, B=100, SSID=...	> Pairwise Cipher Suite Count: 1
37626	59.202621	0.820481	Cisco_05:00:18	Broadcast	802.11	355	69 -38 dbm	Beacon frame, SW=2084, Fw=0, Flags=.....C, B=100, SSID=...	> Pairwise Cipher Suite List 00000000 (IEEE 802.11) GCM (128)
37641	59.204864	0.820961	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2085, Fw=0, Flags=.....C, B=100, SSID=...	> Auth Key Management (AKM) Suite Count: 1
37652	59.206337	0.820351	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2086, Fw=0, Flags=.....C, B=100, SSID=...	> Auth Key Management (AKM) List 00000000 (IEEE 802.11) WPA (SHA256-SuiteB)
37668	59.207365	0.820792	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2087, Fw=0, Flags=.....C, B=100, SSID=...	> Auth Key Management (AKM) Suite: 00000000 (IEEE 802.11) WPA (SHA256-SuiteB)
37687	59.210487	0.820792	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2088, Fw=0, Flags=.....C, B=100, SSID=...	> Auth Key Management (AKM) Type: WPA (SHA256-SuiteB) (11)
37696	59.212867	0.820408	Cisco_05:00:18	Broadcast	802.11	355	69 -38 dbm	Beacon frame, SW=2089, Fw=0, Flags=.....C, B=100, SSID=...	> RSN Capabilities: 000000
37704	59.214477	0.820410	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2090, Fw=0, Flags=.....C, B=100, SSID=...	> PMKID Count: 0
37719	59.215721	0.820240	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2091, Fw=0, Flags=.....C, B=100, SSID=...	> PMKID List
37733	59.218459	0.820628	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2092, Fw=0, Flags=.....C, B=100, SSID=...	> Group Management Cipher Suite: 00000000 (IEEE 802.11) BIP (GCM-128)
37738	59.218659	0.820180	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2093, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: QoS Class Identifier: IEEE 802.11e version
37749	59.223208	0.820495	Cisco_05:00:18	Broadcast	802.11	355	69 -38 dbm	Beacon frame, SW=2094, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: W Enabled Capabilities (5 octets)
37775	59.240621	0.820420	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2095, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: Extended Capabilities (11 octets)
37792	59.246221	0.820508	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2096, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: Tx Power Envelope
37809	59.247802	0.821481	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2097, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: Tx Power Envelope
37814	59.247913	0.821551	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2098, Fw=0, Flags=.....C, B=100, SSID=...	> Ext Tag: Multiple BSSID Configuration
37822	59.247968	0.820347	Cisco_05:00:18	Broadcast	802.11	355	69 -38 dbm	Beacon frame, SW=2099, Fw=0, Flags=.....C, B=100, SSID=...	> Ext Tag: HE Capabilities
37833	59.248658	0.820398	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2100, Fw=0, Flags=.....C, B=100, SSID=...	> Ext Tag: HE Operation
37841	59.248848	0.820498	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2101, Fw=0, Flags=.....C, B=100, SSID=...	> Ext Tag: Spatial Reuse Parameter Set
37857	59.249898	0.820556	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2102, Fw=0, Flags=.....C, B=100, SSID=...	> Ext Tag: HE 4 GHz Band Capabilities
37864	59.251362	0.820460	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2103, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: Vendor Specific: Atheros Communications, Inc.: Unknown
37868	59.251932	0.820508	Cisco_05:00:18	Broadcast	802.11	355	69 -38 dbm	Beacon frame, SW=2104, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: Vendor Specific: Microsoft Corp.: WPA/WPA2 Parameter Element
37881	59.254849	0.820297	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2105, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: Vendor Specific: Cisco Systems, Inc.: Airont Client MFP Disabled
37887	59.254957	0.820468	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2106, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: Vendor Specific: Cisco Systems, Inc.: Airont CCK version = 5
37897	59.261896	0.820839	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2107, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: Vendor Specific: Cisco Systems, Inc.: Airont Unknown (64)
37908	59.211976	0.820888	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2108, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: Vendor Specific: Cisco Systems, Inc.: Airont Unknown (11) (11)
37927	59.124244	0.820438	Cisco_05:00:18	Broadcast	802.11	355	69 -17 dbm	Beacon frame, SW=2099, Fw=0, Flags=.....C, B=100, SSID=...	
37928	59.153887	0.820813	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2098, Fw=0, Flags=.....C, B=100, SSID=...	
37936	59.173134	0.820827	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2095, Fw=0, Flags=.....C, B=100, SSID=...	
37943	59.193778	0.820464	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2082, Fw=0, Flags=.....C, B=100, SSID=...	
37949	59.124389	0.820393	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2083, Fw=0, Flags=.....C, B=100, SSID=...	
37961	59.124873	0.820398	Cisco_05:00:18	Broadcast	802.11	355	69 -17 dbm	Beacon frame, SW=2084, Fw=0, Flags=.....C, B=100, SSID=...	

### WPA3 Enterprise Suite B-1X Beacon

Nessuno dei client testati è stato in grado di connettersi alla WLAN utilizzando SuiteB-1X, confermando che nessuno supporta questo metodo di sicurezza.

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

Configurazione della sicurezza WLAN:

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

General **Security** Advanced Add To Policy Tags

**Layer2** Layer3 AAA

WPA + WPA2  WPA2 + WPA3  WPA3  Static WEP  None

MAC Filtering

Lobby Admin Access

WPA Parameters

WPA Policy  WPA2 Policy   
GTK Randomize  WPA3 Policy   
Transition Disable

Fast Transition

Status   
Over the DS   
Reassociation Timeout \*

WPA2/WPA3 Encryption

AES(CCMP128)  CCMP256   
GCMP128  GCMP256

Auth Key Mgmt

SUITEB192-1X

Protected Management Frame

PMF   
Association Comeback Timer\*   
SA Query Time\*

WPA3 Enterprise SUITEImpostazioni di protezione B192-1x





Nota: FT non è supportato con GCMP256+SUITEB192-1X.

---

Elenco WLAN su WLC GUI WLAN:



WLAN utilizzata per i test

Verifica dell'OTA dei beacon:



No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal strength	BSS ID	Info
17760	11:51:07.067643	0.001572	192.168.1.15	192.168.1.121	Broadcast	112	6A	-39 dBm	FF:FF:FF:FF:FF:FF	Probe Request, Src: 192.168.1.15, Dest: 192.168.1.121, SSID: wif66_test
17761	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Clear-to-send, Flags:.....C	76	6A	-44 dBm	00:0F:30:00:00:18	Clear-to-send, Flags:.....C
17762	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Authentication, Seq: 1, Flags:.....C	69	6A	-44 dBm	00:0F:30:00:00:18	Authentication, Seq: 1, Flags:.....C
17763	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Acknowledgment, Flags:.....C	76	6A	-37 dBm	00:0F:30:00:00:18	Acknowledgment, Flags:.....C
17764	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Association Request, Seq: 1, Flags:.....C	96	6A	-37 dBm	00:0F:30:00:00:18	Association Request, Seq: 1, Flags:.....C
17765	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Association Response, Seq: 1, Flags:.....C	252	6A	-45 dBm	00:0F:30:00:00:18	Association Response, Seq: 1, Flags:.....C
17766	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Acknowledgment, Flags:.....C	76	6A	-37 dBm	00:0F:30:00:00:18	Acknowledgment, Flags:.....C
17767	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Request to-send, Flags:.....C	114	6A	-37 dBm	00:0F:30:00:00:18	Request to-send, Flags:.....C
17768	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Request to-send, Flags:.....C	114	6A	-37 dBm	00:0F:30:00:00:18	Request to-send, Flags:.....C
17769	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Request to-send, Flags:.....C	114	6A	-37 dBm	00:0F:30:00:00:18	Request to-send, Flags:.....C
17770	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Request to-send, Flags:.....C	114	6A	-37 dBm	00:0F:30:00:00:18	Request to-send, Flags:.....C
17771	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Request to-send, Flags:.....C	114	6A	-37 dBm	00:0F:30:00:00:18	Request to-send, Flags:.....C
17772	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Request to-send, Flags:.....C	114	6A	-37 dBm	00:0F:30:00:00:18	Request to-send, Flags:.....C
17773	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Request to-send, Flags:.....C	114	6A	-37 dBm	00:0F:30:00:00:18	Request to-send, Flags:.....C
17774	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Request to-send, Flags:.....C	114	6A	-37 dBm	00:0F:30:00:00:18	Request to-send, Flags:.....C
17775	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Request to-send, Flags:.....C	114	6A	-37 dBm	00:0F:30:00:00:18	Request to-send, Flags:.....C
17776	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Request to-send, Flags:.....C	114	6A	-37 dBm	00:0F:30:00:00:18	Request to-send, Flags:.....C
17777	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Request to-send, Flags:.....C	114	6A	-37 dBm	00:0F:30:00:00:18	Request to-send, Flags:.....C
17778	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Request to-send, Flags:.....C	114	6A	-37 dBm	00:0F:30:00:00:18	Request to-send, Flags:.....C
17779	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Request to-send, Flags:.....C	114	6A	-37 dBm	00:0F:30:00:00:18	Request to-send, Flags:.....C
17780	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Request to-send, Flags:.....C	114	6A	-37 dBm	00:0F:30:00:00:18	Request to-send, Flags:.....C
17781	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Request to-send, Flags:.....C	114	6A	-37 dBm	00:0F:30:00:00:18	Request to-send, Flags:.....C
17782	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Request to-send, Flags:.....C	114	6A	-37 dBm	00:0F:30:00:00:18	Request to-send, Flags:.....C
17783	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Request to-send, Flags:.....C	114	6A	-37 dBm	00:0F:30:00:00:18	Request to-send, Flags:.....C
17784	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Request to-send, Flags:.....C	114	6A	-37 dBm	00:0F:30:00:00:18	Request to-send, Flags:.....C
17785	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Request to-send, Flags:.....C	114	6A	-37 dBm	00:0F:30:00:00:18	Request to-send, Flags:.....C
17786	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Request to-send, Flags:.....C	114	6A	-37 dBm	00:0F:30:00:00:18	Request to-send, Flags:.....C
17787	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Request to-send, Flags:.....C	114	6A	-37 dBm	00:0F:30:00:00:18	Request to-send, Flags:.....C
17788	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Request to-send, Flags:.....C	114	6A	-37 dBm	00:0F:30:00:00:18	Request to-send, Flags:.....C
17789	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Request to-send, Flags:.....C	114	6A	-37 dBm	00:0F:30:00:00:18	Request to-send, Flags:.....C
17790	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Request to-send, Flags:.....C	114	6A	-37 dBm	00:0F:30:00:00:18	Request to-send, Flags:.....C
17791	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Request to-send, Flags:.....C	114	6A	-37 dBm	00:0F:30:00:00:18	Request to-send, Flags:.....C
17792	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Request to-send, Flags:.....C	114	6A	-37 dBm	00:0F:30:00:00:18	Request to-send, Flags:.....C
17793	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Request to-send, Flags:.....C	114	6A	-37 dBm	00:0F:30:00:00:18	Request to-send, Flags:.....C
17794	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Request to-send, Flags:.....C	114	6A	-37 dBm	00:0F:30:00:00:18	Request to-send, Flags:.....C
17795	11:51:07.067643	0.000000	192.168.1.15	192.168.1.121	Request to-send, Flags:.....C	114	6A	-37 dBm	00:0F:30:00:00:18	Request to-send, Flags:.....C

WPA3 Enterprise con associazione EAP-TLS con il client Intel AX211 e EAP-TLS Focus

### Dettagli client in WLC:

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The 'Monitoring' tab is active, and the 'Clients' section is expanded. A table lists client details for a selected client with MAC address 286b:3998:580f and IP address 192.168.1.159. The client is associated with APD1\_RC\_9136\_F80C and SSID wif66\_test. The 'Security Information' tab is selected, showing various security parameters:

- Re-Authentication Timeout: 1800 sec (Remaining time: 1172 sec)
- Client State Servers: None
- Client ACLs: None
- Client Entry Create Time: 628 seconds
- Policy Type: WPA3
- Encryption Cipher: CCMP (AES)
- Authentication Key Management: FT-802.1x
- EAP Type: EAP-TLS
- Session Timeout: 1800

The 'Session Manager' section shows the Point of Attachment as caswap\_9000000e, the IF ID as 0x9000000e, and the Common Session ID as 0f01abc0000001bc0080064.

Dettagli sul client WPA3 Enterprise con EAP-TLS

### NetGear A8000

WPA3-Enterprise non è supportato su questo client.

### Pixel 6a

Alla data di scrittura del documento, il client non è stato in grado di connettersi a WPA3 Enterprise utilizzando EAP-TLS.

Si trattava di un problema a questo cliente su cui si sta lavorando e, non appena risolto, il presente documento deve essere aggiornato.

### Samsung S23

Alla data di scrittura del documento, il client non è stato in grado di connettersi a WPA3 Enterprise utilizzando EAP-TLS.

Si trattava di un problema sul lato cliente su cui si sta lavorando e, non appena risolto, il presente documento deve essere aggiornato.

## Conclusioni sulla sicurezza

Dopo tutti i test precedenti, ne risulta quanto segue:

Protocollo	Crittografia	AKM	Cifratura AKM	Metodo EAP	FT- OverTA	FT- OverDS	Intel AX211	Samsung/C Android
DOVERE	AES- CCMP128	DOVERE	N/D.	N/D.	N/D	N/D	Supportato	Supportato
SAE	AES- CCMP128	SAE (solo H2E)	SHA256	N/D.	Supportato	Supportato	Supportati: solo H2E e FT-oTA	Supportato H2E. FT non rius FT-oDS non riuscito.
Azienda	AES- CCMP128	802.1x- SHA256	SHA256	PEAP/FAST/TLS	Supportato	Supportato	Supportati: SHA256 e FT- oTA/oDS Non supportato: EAP-FAST	Supportati: SHA256 e oTA, FT-oD (S23) Non suppor EAP-FAST oDS (Pixel6
Azienda	GCMP128	Suite B- 1x	SHA256- SuiteB	PEAP/FAST/TLS	Non supportata	Non supportata	Non supportata	Non suppor
Azienda	GCMP256	Suite B- 192	SHA384- SuiteB	TLS	Non supportata	Non supportata	ND/TBD	ND/TBD

## Risoluzione dei problemi

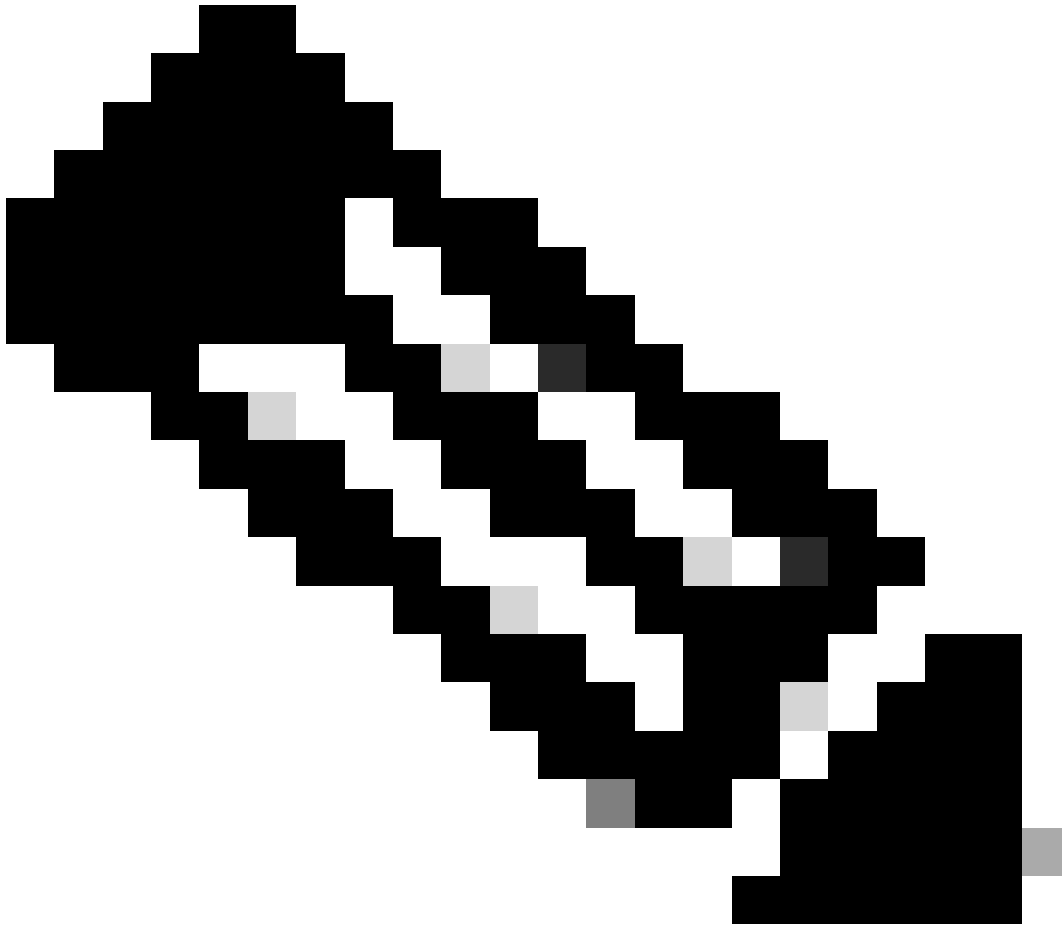
La risoluzione dei problemi utilizzata in questo documento si basa sul documento online:

## [Risoluzione dei problemi dei punti di accesso COS](#)

Per risolvere i problemi, si consiglia di raccogliere la traccia RA in modalità di debug dal WLC utilizzando l'indirizzo MAC del client, assicurandosi che il client si connetta utilizzando il mac del dispositivo e non un indirizzo mac casuale.

Per la risoluzione dei problemi di Over the Air, si consiglia di utilizzare il punto di accesso in modalità sniffer per catturare il traffico sul canale del client che serve il punto di accesso.

---



Nota: consultare le [informazioni importanti sui](#) comandi di [debug](#) prima di usare i comandi di debug.

---

## Informazioni correlate

[Cos'è Wi-Fi 6E?](#)

[Cos'è Wi-Fi 6 rispetto a Wi-Fi 6E?](#)



[Wi-Fi 6E in breve](#)

[Wi-Fi 6E: il prossimo grande capitolo nel white paper Wi-Fi](#)

[Cisco Live - Architettura di una rete wireless di nuova generazione con i punti di accesso Catalyst Wi-Fi 6E](#)

[Guida alla configurazione del software Cisco Catalyst serie 9800 Wireless Controller 17.9.x](#)

[Guida alla distribuzione di WPA3](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).