

# Configuration et vérification de la sécurité de la couche 2 du WLAN Wi-Fi 6E

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Sécurité Wi-Fi 6E](#)

[WPA3](#)

[Jeu de niveaux : modes WPA3](#)

[Points d'accès Cisco Catalyst Wi-Fi 6E](#)

[Paramètres de sécurité pris en charge](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configuration de base](#)

[Vérifier](#)

[Vérification de sécurité](#)

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

[WPA3 - AES \(CCPM128\) + OWE avec mode de transition](#)

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

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

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

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

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

[Conclusions sur la sécurité](#)

[Dépannage](#)

[Informations connexes](#)

---

## Introduction

Ce document décrit comment configurer la sécurité de la couche 2 du WLAN Wi-Fi 6E et ce à quoi s'attendre sur différents clients.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Contrôleurs LAN sans fil Cisco (WLC) 9800
- Points d'accès Cisco prenant en charge le Wi-Fi 6E.
- Norme IEEE 802.11ax.
- Outils : Wireshark v4.0.6

## Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- WLC 9800-CL avec IOS® XE 17.9.3.
- AP C9136, CW9162, CW9164 et CW9166.
- Clients Wi-Fi 6E :
  - Carte Lenovo X1 Carbon Gen11 avec Intel AX211 Wi-Fi 6 et 6E avec pilote version 22.200.2(1).
  - Adaptateur Wi-Fi 6 et 6E Netgear A8000 avec pilote v1(0.0.108);
  - Téléphone portable Pixel 6a avec Android 13 ;
  - Téléphone portable Samsung S23 avec Android 13.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

Il est important de savoir que le Wi-Fi 6E n'est pas une norme entièrement nouvelle, mais une extension. À sa base, le Wi-Fi 6E est une extension de la norme sans fil Wi-Fi 6 (802.11ax) dans la bande de radiofréquences de 6 GHz.

Le Wi-Fi 6E repose sur le Wi-Fi 6, qui est la dernière génération de la norme Wi-Fi, mais seuls les périphériques et applications Wi-Fi 6E peuvent fonctionner dans la bande 6 GHz.

### Sécurité Wi-Fi 6E

Le Wi-Fi 6E renforce la sécurité grâce à la norme Wi-Fi Protected Access 3 (WPA3) et au cryptage sans fil opportuniste (OWE) et il n'y a pas de rétrocompatibilité avec la sécurité Open et WPA2.

WPA3 et Enhanced Open Security sont désormais obligatoires pour la certification Wi-Fi 6E et Wi-Fi 6E nécessite également la technologie Protected Management Frame (PMF) dans les points d'accès et les clients.

Lors de la configuration d'un SSID 6 GHz, certaines exigences de sécurité doivent être respectées :

- Sécurité WPA3 L2 avec OWE, SAE ou 802.1x-SHA256
- trame de gestion protégée activée ;

- Toute autre méthode de sécurité de couche 2 n'est pas autorisée, c'est-à-dire qu'aucun mode mixte n'est possible.

## WPA3

WPA3 est conçu pour améliorer la sécurité Wi-Fi en permettant une meilleure authentification sur WPA2, en fournissant une puissance cryptographique étendue et en augmentant la résilience des réseaux critiques.

Fonctionnalités clés du WPA3 :

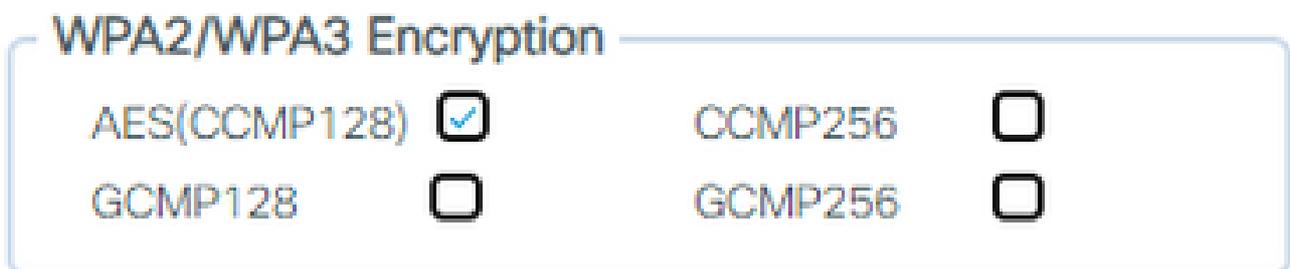
- La trame de gestion protégée (PMF) protège les trames de gestion de monodiffusion et de diffusion et chiffre les trames de gestion de monodiffusion. Cela signifie que les systèmes de détection et de prévention des intrusions sans fil disposent désormais de moins de moyens de force brute pour appliquer les stratégies client.
- L'authentification simultanée d'égal à égal (SAE) permet l'authentification par mot de passe et un mécanisme d'accord de clé. Cela permet de se protéger contre les attaques en force.
- Le mode de transition est un mode mixte qui permet d'utiliser WPA2 pour connecter des clients qui ne prennent pas en charge WPA3.

Le WPA3 concerne le développement continu de la sécurité et de la conformité, ainsi que l'interopérabilité.

Aucun élément d'information ne désigne WPA3 (comme WPA2). WPA3 est défini par les combinaisons AKM/Cipher Suite/PMF.

Dans la configuration WLAN du 9800, vous pouvez utiliser 4 algorithmes de cryptage WPA3 différents.

Ils sont basés sur les protocoles Galois/Counter Mode Protocol (GCMP) et Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) : AES (CCMP128), CCMP256, GCMP128 et GCMP256 :



The image shows a configuration window titled "WPA2/WPA3 Encryption". It contains four options, each with a checkbox:

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

Options de cryptage WPA2/3

## PMF

PMF est activé sur un WLAN lorsque vous activez PMF.

Par défaut, les trames de gestion 802.11 ne sont pas authentifiées et ne sont donc pas protégées

contre l'usurpation. Infrastructure Management Protection Frame (MFP) et 802.11w protected management frames (PMF) assurent une protection contre de telles attaques.

## Protected Management Frame

PMF

Required

Association Comeback Timer\*

1

SA Query Time\*

200

Options PMF

Gestion des clés d'authentification

Voici les options AKM disponibles dans la version 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\*

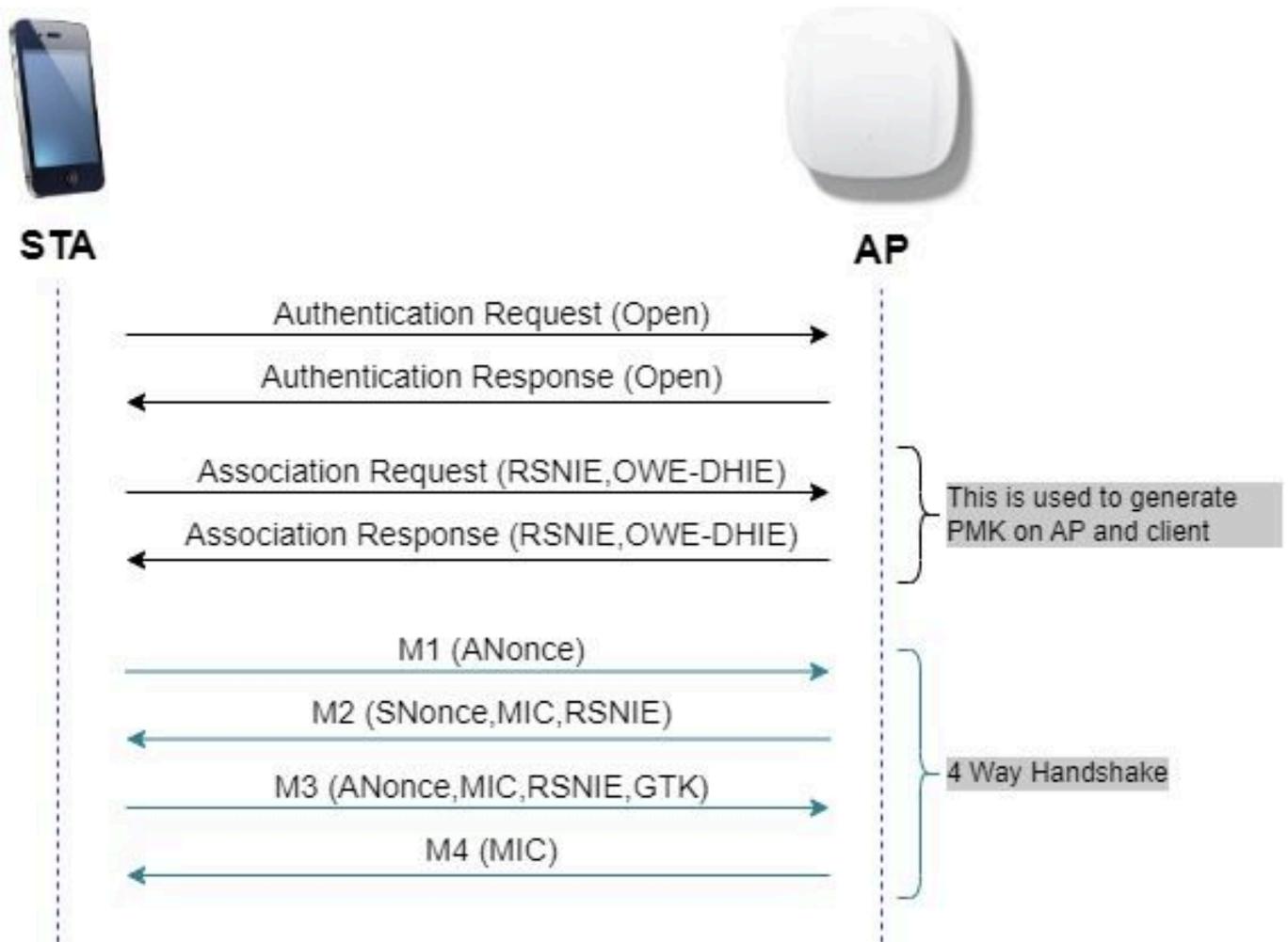
SAE Password Element ⓘ

Options AKM

### DEVOIR

Opportunistic Wireless Encryption (OWE) est une extension de la norme IEEE 802.11 qui assure le cryptage du support sans fil ([IETF RFC 8110](#)). L'objectif de l'authentification basée sur OWE est d'éviter une connectivité sans fil ouverte et non sécurisée entre les points d'accès et les clients. L'OWE utilise le cryptage basé sur les algorithmes Diffie-Hellman pour configurer le cryptage sans fil. Avec OWE, le client et le point d'accès effectuent un échange de clés Diffie-Hellman au cours de la procédure d'accès et utilisent le secret PMK (Pairwise Master Key) résultant avec la

connexion en 4 étapes. L'utilisation d'OWE améliore la sécurité du réseau sans fil pour les déploiements où des réseaux basés sur une clé prépartagée ouverte ou partagée sont déployés.



échange de trames OWE

## SAE

WPA3 utilise un nouveau mécanisme d'authentification et de gestion des clés appelé Authentification simultanée d'égal à égal. Ce mécanisme est encore amélioré grâce à l'utilisation de SAE Hash-to-Element (H2E).

SAE avec H2E est obligatoire pour WPA3 et Wi-Fi 6E.

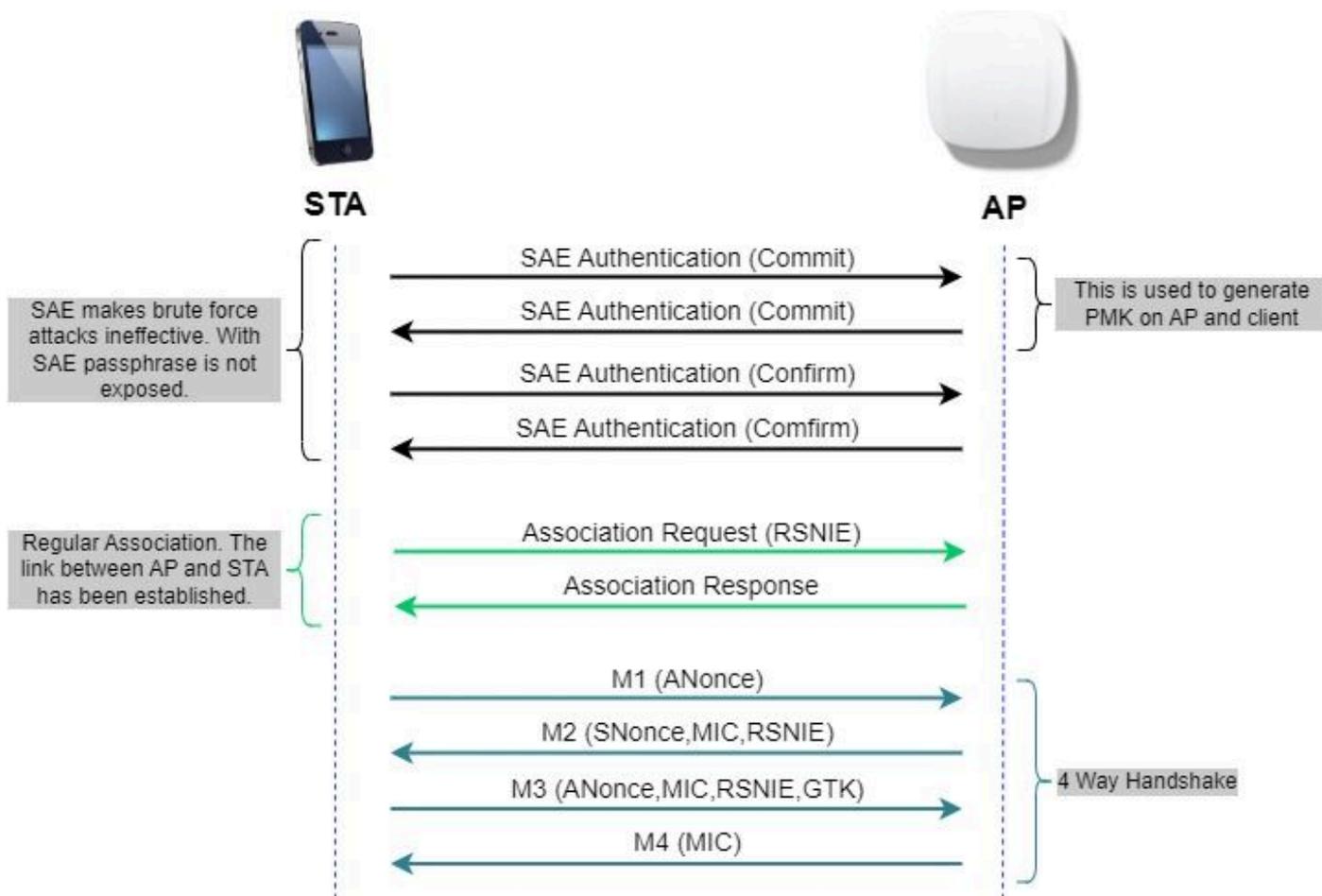
SAE utilise une cryptographie à logarithme discret pour effectuer un échange efficace d'une manière qui effectue une authentification mutuelle à l'aide d'un mot de passe qui est probablement résistant à une attaque de dictionnaire hors ligne.

Une attaque par dictionnaire hors connexion est une attaque par laquelle un pirate tente de déterminer un mot de passe réseau en essayant des mots de passe possibles sans autre interaction réseau.

Lorsque le client se connecte au point d'accès, il effectue un échange SAE. En cas de succès, ils créent chacun une clé cryptographiquement forte, à partir de laquelle la clé de session est dérivée. Fondamentalement, un client et un point d'accès passent en phases de validation, puis

de confirmation.

Une fois l'engagement pris, le client et le point d'accès peuvent passer à l'état de confirmation chaque fois qu'une clé de session doit être générée. La méthode utilise le secret de transmission, où un intrus pourrait craquer une seule clé, mais pas toutes les autres clés.



échange de trames SAE

## Hachage d'élément (H2E)

Hash-to-Element (H2E) est une nouvelle méthode SAE Password Element (PWE). Dans ce procédé, le PWE secret utilisé dans le protocole SAE est généré à partir d'un mot de passe.

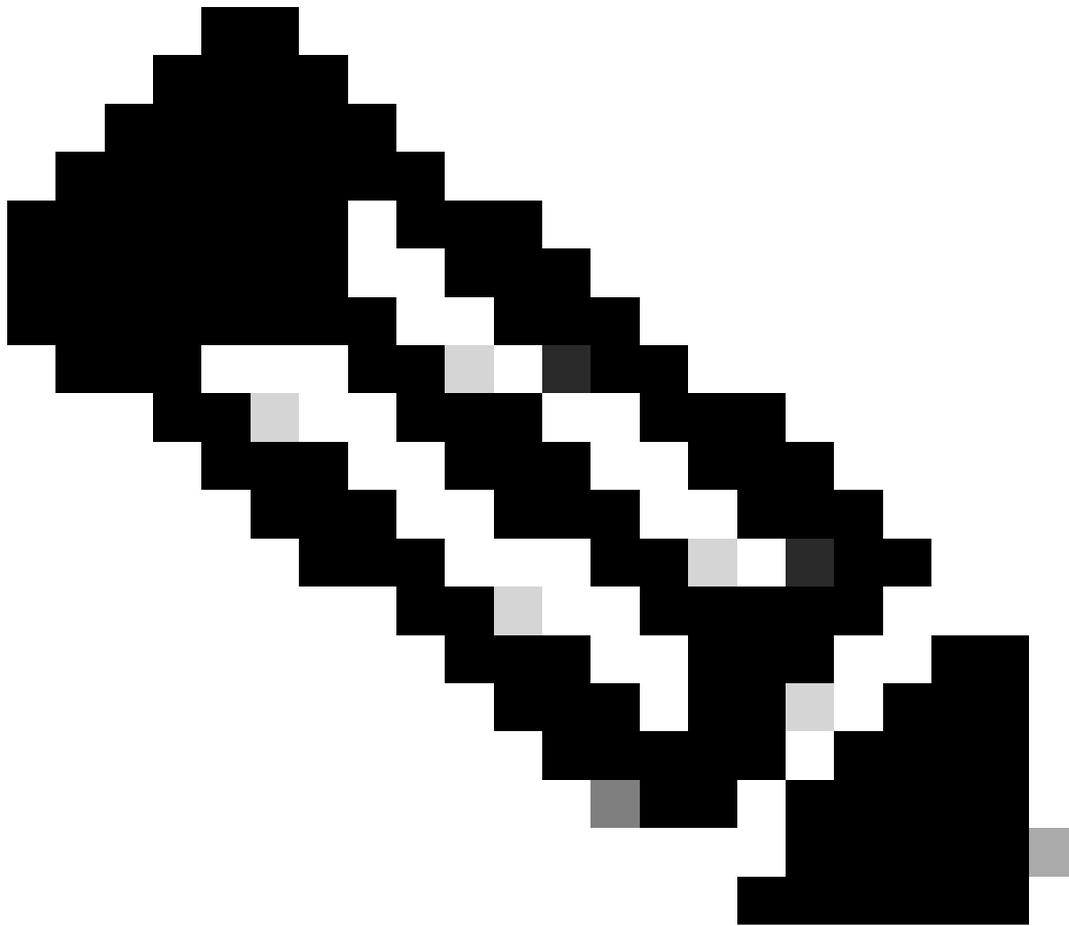
Lorsqu'une station (STA) qui prend en charge H2E lance SAE avec un point d'accès, elle vérifie si le point d'accès prend en charge H2E. Si oui, le point d'accès utilise H2E pour dériver le PWE en utilisant une valeur de code d'état nouvellement définie dans le message SAE Commit.

Si STA utilise le protocole HnP (Hunting-and-Pecking), l'ensemble de l'échange SAE reste inchangé.

Lors de l'utilisation de H2E, la dérivation PWE est divisée en ces composants :

- Dérivation d'un élément intermédiaire secret (PT) du mot de passe. Cette opération peut être effectuée hors connexion lorsque le mot de passe est initialement configuré sur le périphérique pour chaque groupe pris en charge.

- Dérivation du PWE à partir du PT stocké. Cela dépend du groupe négocié et des adresses MAC des homologues. Cette opération est effectuée en temps réel lors de l'échange SAE.
- 

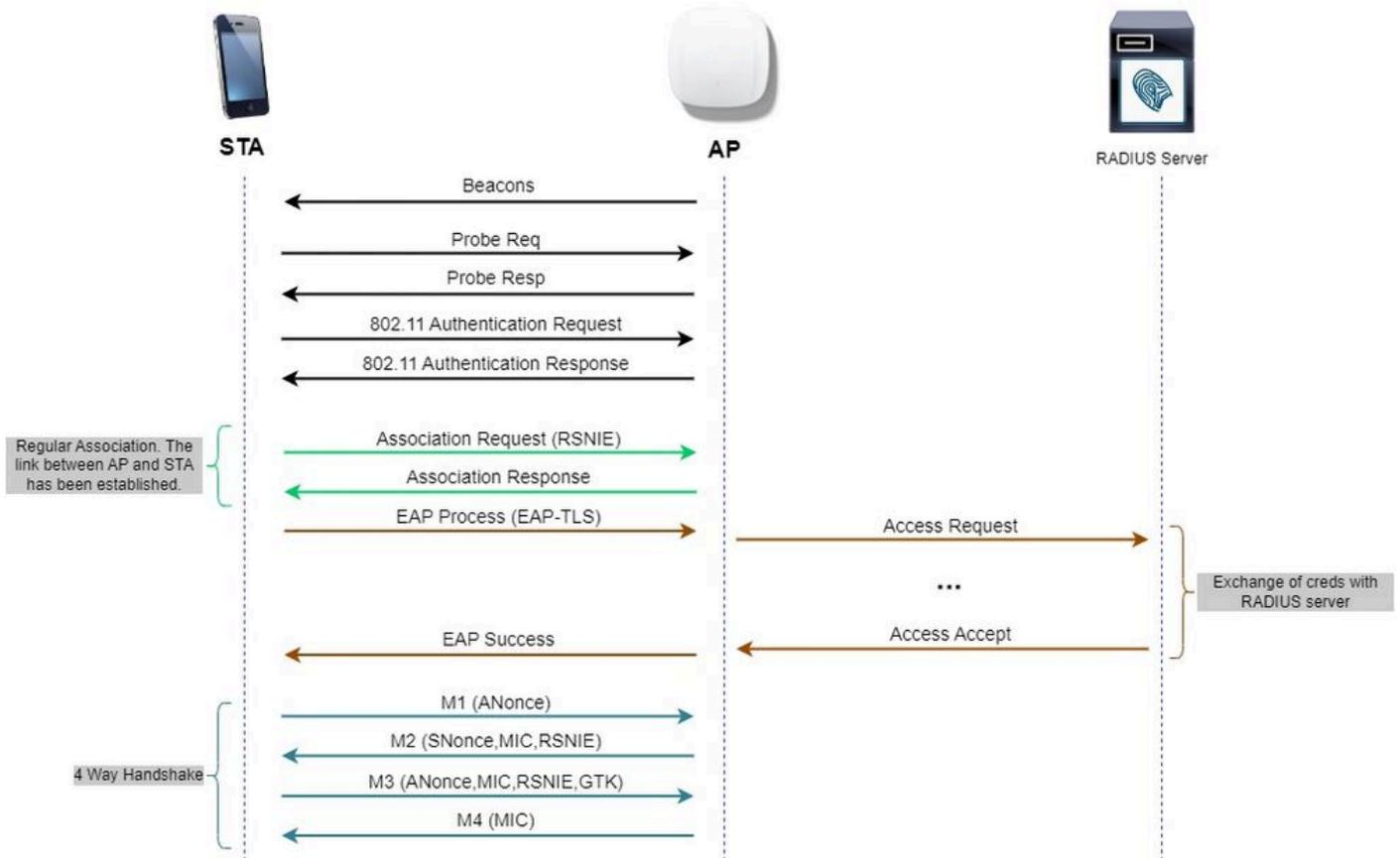


Remarque : 6 GHz prend uniquement en charge la méthode PWE SAE Hash-to-Element.

---

#### WPA-Enterprise alias 802.1x

WPA3-Enterprise est la version la plus sécurisée de WPA3 et utilise une combinaison nom d'utilisateur/mot de passe avec 802.1X pour l'authentification des utilisateurs avec un serveur RADIUS. Par défaut, le WPA3 utilise un cryptage 128 bits, mais il introduit également un cryptage de puissance cryptographique 192 bits éventuellement configurable, qui offre une protection supplémentaire à tout réseau transmettant des données sensibles.



Flux du diagramme WPA3 Enterprise

## Jeu de niveaux : modes WPA3

- WPA3 personnel
  - WPA3-Personal only mode
    - PMF requis
  - WPA3-Mode de transition personnel
    - Règles de configuration : sur un point d'accès, chaque fois que le mode WPA2 personnel est activé, le mode de transition WPA3 personnel doit également être activé par défaut, sauf si l'administrateur le remplace explicitement pour fonctionner en mode WPA2 personnel uniquement
- WPA3-Entreprise
  - WPA3 - mode entreprise uniquement
    - Le PMF doit être négocié pour toutes les connexions WPA3
  - WPA3-Mode transition entreprise
    - Le PMF doit être négocié pour une connexion WPA3
    - PMF en option pour une connexion WPA2
  - Mode WPA3-Entreprise suite-B « 192 bits » aligné sur l'algorithme CNSA (Commercial National Security Algorithm)
    - Plus que pour le seul gouvernement fédéral
    - Des suites de chiffrement cryptographiques cohérentes pour éviter toute erreur de configuration

- Ajout de GCMP et ECCP pour les fonctions de chiffrement et de hachage (SHA384)
- PMF requis
- La sécurité WPA3 192 bits doit être exclusive pour EAP-TLS, qui doit exiger des certificats à la fois sur le demandeur et sur le serveur RADIUS.
- Pour utiliser WPA3 Enterprise 192 bits, les serveurs RADIUS doivent utiliser l'un des chiffrements EAP autorisés :

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

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

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

Pour en savoir plus sur les informations détaillées sur la mise en oeuvre de WPA3 dans les WLAN Cisco, y compris la matrice de compatibilité de sécurité client, n'hésitez pas à consulter le [Guide de déploiement de WPA3](#).

## Points d'accès Cisco Catalyst Wi-Fi 6E

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>
<p><b>Full radio capability (6 GHz @ LPI) on single 30W PoE+</b></p>			
Dedicated Radio for CleanAir Pro	Same Bracket, Industrial Design	AP Power Optimization	USB

## Points d'accès Wi-Fi 6E

### Paramètres de sécurité pris en charge

Vous pouvez trouver quel produit prend en charge WPA3-Enterprise à l'aide de la page Web WiFi Alliance [product finder](#).

Sur les périphériques Windows, vous pouvez vérifier quels sont les paramètres de sécurité pris en charge par la carte à l'aide de la commande "netsh wlan show drivers".

Vous pouvez voir ici la sortie de l'AX211 Intel :

```
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
```

Sortie Windows de \_netsh wlan show driver\_ pour le 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)
```

Sortie Windows de `_netsh wlan show driver_` pour le 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 + chiffrement AES + AKM 802.1x-SHA256 (FT)
- WPA3 + chiffrement AES + AKM OWE
- WPA3 + chiffrement AES + AKM SAE (FT)
- Chiffrement WPA3 + CCMP256 + SUITEB192-1X AKM
- Chiffrement WPA3 + GCMP128 + SUITEB-1X AKM
- Chiffrement WPA3 + GCMP256 + SUITEB192-1X AKM

## Configuration de base

Le WLAN a été configuré avec une méthode de détection de stratégie radio et de réponse de sondage de diffusion (UPR) 6 GHz uniquement :

**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

Configuration de 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 'Radio' section with a table of RF profiles. The table has columns for 'State', 'RF Profile Name', and 'Band'. The 'default-rf-profile-6ghz' profile is highlighted, indicating a 6 GHz band. Other profiles include 'Low\_Client\_Density\_rf\_5gh', 'High\_Client\_Density\_rf\_5gh', 'Low\_Client\_Density\_rf\_24gh', 'High\_Client\_Density\_rf\_24gh', 'Typical\_Client\_Density\_rf\_5gh', and 'Typical\_Client\_Density\_rf\_24gh'. The right-hand panel, 'Edit RF Profile', shows the configuration for the 802.11ax standard. It includes sections for 'General', 'RRM', and 'Advanced'. Key settings include '6 GHz Discovery Frames' (Broadcast Probe Response), 'Broadcast Probe Response Interval (msec)\*' (20), 'Multi BSSID Profile' (MBSSIDprofile\_test), and 'Spatial Reuse' (DISABLED). Other settings include 'OBSS PD' (DISABLED), 'Non-SRG OBSS PD Max Threshold (dBm)\*' (-62), 'SRG OBSS PD' (DISABLED), 'SRG OBSS PD Min Threshold (dBm)\*' (-82), and 'SRG OBSS PD Max Threshold (dBm)\*' (-62).

Configuration du profil RF 6 GHz

## Vérier

### Vérification de sécurité

Dans cette section, la configuration de la sécurité et la phase d'association du client sont présentées à l'aide des combinaisons de protocoles WPA3 suivantes :

- WPA3- AES(CCMP128) + OWE
  - Mode de transition OWE
- WPA3 personnel
  - AES(CCMP128) + SAE
- WPA3-Entreprise
  - AES(CCMP128) + 802.1x-SHA256
  - AES(CCMP128) + 802.1x-SHA256 + FT
  - Chiffrement GCMP128 + SUITEB-1X
  - Chiffrement GCMP256 + SUITEB192-1X

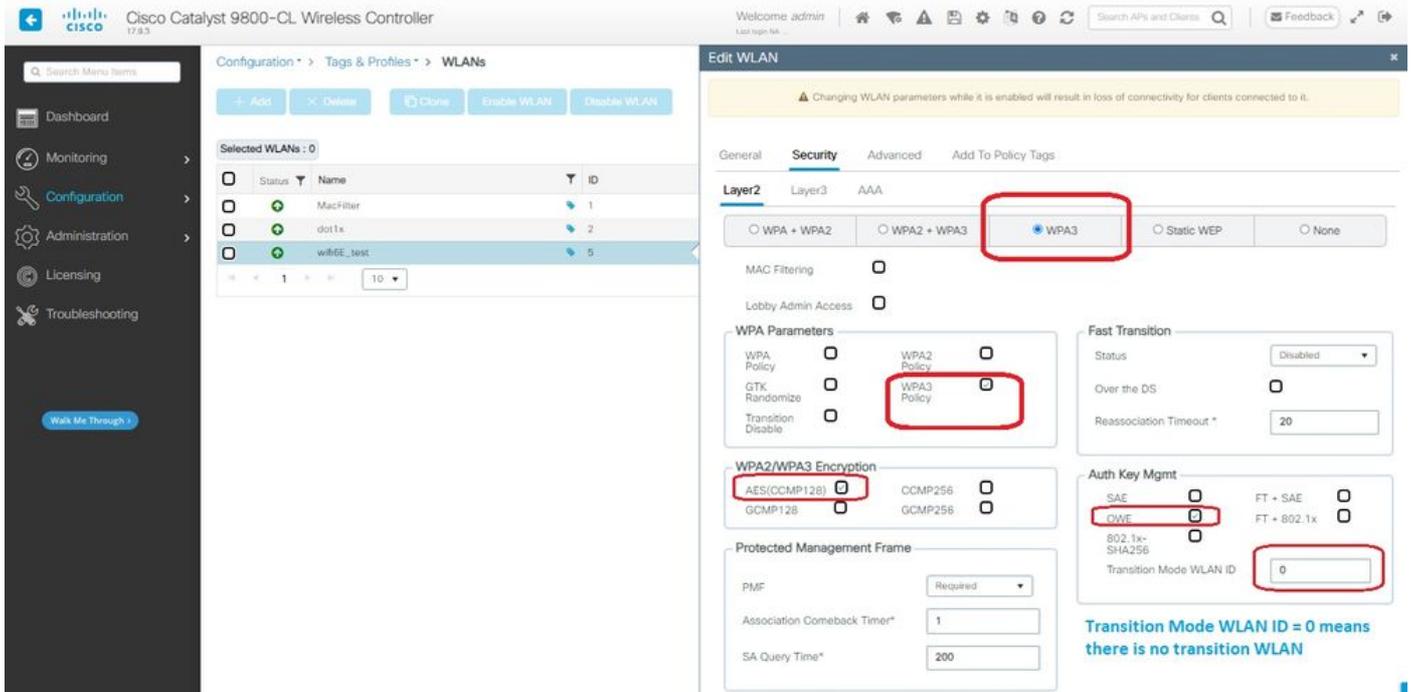


Remarque : bien qu'aucun client ne prenne en charge le chiffrement GCMP128 + SUITEB-1X au moment de la rédaction de ce document, il a été testé pour observer sa diffusion et vérifier les informations RSN dans les balises.

---

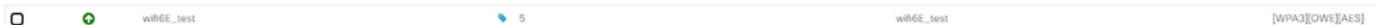
WPA3 - AES (CCPM128) + OWE

Voici la configuration de la sécurité WLAN :



Paramètres de sécurité OWE

Affichage sur l'interface graphique utilisateur WLC des paramètres de sécurité WLAN :



Paramètres de sécurité WLAN sur l'interface graphique WLC

Ici, nous pouvons observer le processus de connexion des clients Wi-Fi 6E :

Intel AX211

Nous présentons ici le processus de connexion complet du client Intel AX211.

Détection OWE

Ici vous pouvez voir les balises OTA. Le point d'accès annonce la prise en charge d'OWE en utilisant le sélecteur de suite AKM pour OWE sous l'élément d'information RSN.

Vous pouvez voir la valeur 18 (00-0F-AC:18) du type de suite AKM qui indique la prise en charge OWE.

trame de balise OWE

Si vous regardez le champ de capacités RSN, vous pouvez voir que l'AP annonce à la fois les capacités de protection de trame de gestion (MFP) et le bit requis MFP défini sur 1.

## Association OWE

Vous pouvez voir l'UPR envoyé en mode de diffusion, puis l'association elle-même.

Le message OWE commence par la requête et la réponse d'authentification OPEN :

Ensuite, un client qui veut faire OWE doit indiquer OWE AKM dans l'IE RSN de la trame de demande d'association et inclure l'élément de paramètre Diffie Helman (DH) :





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: 135 seconds  
 Policy Type: WPA3  
 Encryption Cipher: CCMP (AES)  
 Authentication Key Management: OWE  
 EAP Type: Not Applicable  
 Session Timeout: 86400

## Samsung S23

## Connexion OTA avec accent sur les informations RSN du client :

Frame 2387: 388 bytes on wire (3184 bits), 388 bytes captured (3184 bits) on interface DeviceVNF\_04578985-2398-445

Ethernet II, Src: Cisco\_00:10:00:00:00:00, 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: 5555, Dst Port: 5000

IEEE 802.11 Association Request, Flags: .....C  
 Tag Number: RSN Information (48)  
 Tag length: 26  
 RSN Version: 1  
 Group Cipher Suite: 00ff:fac (See 802.11 AES (CCM))  
 Pairwise Cipher Suite List: 00ff:fac (See 802.11 AES (CCM))  
 Auth Key Management (AKM) Suite Count: 1  
 AKM Suite List: 000e:1 (See 802.11) Opportunistic wireless encryption  
 RSN Capabilities: 0x0000  
 PMKID Count: 0  
 PMKID List: []  
 Group Management Cipher Suite: 00ff:fac (See 802.11) GMP (128)  
 Tag: 0x enabled Capabilities (5 octets)  
 Tag Number: 0x enabled Capabilities (20)  
 Tag length: 5  
 RSN Capabilities: 0x01 (octet 1)  
 .... 1.. = Link Measurement: Enabled  
 .... 1.. = Neighbor Report: Enabled  
 .... 0.. = Parallel Measurements: Disabled  
 .... 0.. = Reported Measurements: Disabled  
 .... 1.. = Beacon Passive Measurement: Enabled  
 .... 1.. = Beacon Active Measurement: Enabled  
 .... 0.. = Beacon Traffic Measurement: Supported  
 .... 0.. = Beacon Measurement Reporting Conditions: Disabled  
 RSN Capabilities: 0x02 (octet 2)  
 .... 1.. = AP Channel report capability: Enabled  
 .... 0.. = MHA capability: Disabled  
 .... 0.. = Operating Channel Max Measurement Duration: 4  
 100... = Nonoperating Channel Max Measurement Duration: 4  
 RSN Capabilities: 0x03 (octet 3)  
 .... 0.. = MHA capability: Disabled  
 .... 0.. = Operating Channel Max Measurement Duration: 4  
 100... = Nonoperating Channel Max Measurement Duration: 4  
 RSN Capabilities: 0x04 (octet 4)  
 .... 0.. = MHA capability: Disabled  
 .... 0.. = Operating Channel Max Measurement Duration: 4  
 100... = Nonoperating Channel Max Measurement Duration: 4  
 RSN Capabilities: 0x05 (octet 5)  
 .... 0.. = MHA capability: Disabled  
 .... 0.. = Operating Channel Max Measurement Duration: 4  
 100... = Nonoperating Channel Max Measurement Duration: 4  
 RSN Capabilities: 0x06 (octet 6)  
 .... 0.. = MHA capability: Disabled  
 .... 0.. = Operating Channel Max Measurement Duration: 4  
 100... = Nonoperating Channel Max Measurement Duration: 4  
 RSN Capabilities: 0x07 (octet 7)  
 .... 0.. = MHA capability: Disabled  
 .... 0.. = Operating Channel Max Measurement Duration: 4  
 100... = Nonoperating Channel Max Measurement Duration: 4  
 RSN Capabilities: 0x08 (octet 8)  
 .... 0.. = MHA capability: Disabled  
 .... 0.. = Operating Channel Max Measurement Duration: 4  
 100... = Nonoperating Channel Max Measurement Duration: 4  
 RSN Capabilities: 0x09 (octet 9)  
 .... 0.. = MHA capability: Disabled  
 .... 0.. = Operating Channel Max Measurement Duration: 4  
 100... = Nonoperating Channel Max Measurement Duration: 4  
 RSN Capabilities: 0x0a (octet 10)  
 .... 0.. = MHA capability: Disabled  
 .... 0.. = Operating Channel Max Measurement Duration: 4  
 100... = Nonoperating Channel Max Measurement Duration: 4  
 RSN Capabilities: 0x0b (octet 11)  
 .... 0.. = MHA capability: Disabled  
 .... 0.. = Operating Channel Max Measurement Duration: 4  
 100... = Nonoperating Channel Max Measurement Duration: 4  
 RSN Capabilities: 0x0c (octet 12)  
 .... 0.. = MHA capability: Disabled  
 .... 0.. = Operating Channel Max Measurement Duration: 4  
 100... = Nonoperating Channel Max Measurement Duration: 4  
 RSN Capabilities: 0x0d (octet 13)  
 .... 0.. = MHA capability: Disabled  
 .... 0.. = Operating Channel Max Measurement Duration: 4  
 100... = Nonoperating Channel Max Measurement Duration: 4  
 RSN Capabilities: 0x0e (octet 14)  
 .... 0.. = MHA capability: Disabled  
 .... 0.. = Operating Channel Max Measurement Duration: 4  
 100... = Nonoperating Channel Max Measurement Duration: 4  
 RSN Capabilities: 0x0f (octet 15)  
 .... 0.. = MHA capability: Disabled  
 .... 0.. = Operating Channel Max Measurement Duration: 4  
 100... = Nonoperating Channel Max Measurement Duration: 4

## Détails du client dans le 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: 568 seconds  
 Policy Type: WPA3  
 Encryption Cipher: CCMP (AES)  
 Authentication Key Management: OWE  
 EAP Type: Not Applicable  
 Session Timeout: 86400

## WPA3 - AES (CCMP128) + OWE avec mode de transition

La configuration détaillée et le dépannage du mode de transition OWE sont disponibles dans ce document : [Configure Enhanced Open SSID with Transition Mode - OWE.](#)

## WPA3 personnel - AES(CCMP128) + SAE

## Configuration de la sécurité 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"/>		

#### Fast Transition

Status

Over the DS

Reassociation Timeout \*

#### WPA2/WPA3 Encryption

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

#### Protected Management Frame

PMF

Association Comeback Timer\*

SA Query Time\*

#### Auth Key Mgmt

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

Anti Clogging Threshold\*

Max Retries\*

Retransmit Timeout\*

PSK Format

PSK Type

Pre-Shared Key\*

SAE Password Element ⓘ

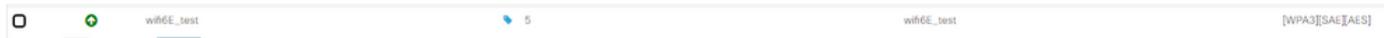
Configuration WPA3 SAE



Remarque : n'oubliez pas que la chasse et le prélèvement ne sont pas autorisés avec la politique radio 6 GHz. Lorsque vous configurez un WLAN 6 GHz uniquement, vous devez sélectionner H2E SAE Password Element.

---

Affichage sur l'interface graphique utilisateur WLC des paramètres de sécurité WLAN :



Vérification des balises OTA :

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
2	2023-06-12 17:12:24.459118	0.00000	Cisco_13:180e0f	Broadcast	802.11	463	5.36 dBm	Probe Response, Shw737, FwB, Flags:.....C, B1=800, SSID="wifi6_test_02", SS	<ul style="list-style-type: none"> <li>Frame 6: 508 bytes on wire (4064 bits), 508 bytes captured (4064 bits) on interface Vdevoice\NPF_{04578995-2998-4464-4}</li> <li>Ethernet II, Src: Cisco_0d70137 (08:00:0d:0d:70137), Dst: Universe_b7fc1f6e (08:1a:8b:b7:cf:6e)</li> <li>Internet Protocol version 4, Src: 192.168.1.11, Dst: 192.168.1.11</li> <li>User Datagram Protocol, Src Port: 5555, Dst Port: 5000</li> <li>Airframe/OnMFrame encapsulated IEEE 802.11</li> <li>IEEE 802.11 radio information</li> <li>IEEE 802.11 Beacon frame, Flags:.....C</li> <li>IEEE 802.11 wireless management</li> <li>Fixed parameters (406 bytes) <ul style="list-style-type: none"> <li>Tag: SSI parameter set "wifi6_test_02"</li> <li>Tag: Supported rates (3), 5, 11M; 18, 24M; 36, 48, 54, [Mbit/sec]</li> <li>Tag: Traffic Indication Map (TIM): OFDM 2 of 3 Bitmap</li> <li>Tag: Country Information: Country code is, Environment global operating classes</li> <li>Tag: Power Constraint: 0</li> <li>Tag: TPC Report Transm Power: 17, Link Margin: 0</li> <li>Tag: RSN Information <ul style="list-style-type: none"> <li>Tag number: RSN Information (48)</li> <li>Tag length: 36</li> <li>RSN version: 1</li> <li>Group Cipher Suite: 00f0ac (IEEE 802.11) AES (CCM)</li> <li>Pairwise Cipher Suite Count: 1</li> <li>Pairwise Cipher Suite 1: 00f0ac (IEEE 802.11) AES (CCM)</li> <li>Auth key Management (AKM) Suite Count: 1</li> <li>Auth key Management (AKM) Suite 1: 00f0ac (IEEE 802.11) SAE (SHA256)</li> <li>RSN Capabilities: 00000</li> <li>PMKID Count: 0</li> <li>PMKID List</li> <li>Group Management Cipher Suite: 00f0ac (IEEE 802.11) ESP (128)</li> <li>Tag: QSS Load Element 0001cc ECA version</li> <li>Tag: Multiple BSSID</li> <li>Tag: M Enabled Capabilities (5 octets)</li> <li>Tag: Extended Capabilities (11 octets)</li> <li>Tag length: 1</li> <li>Tag: TX Power Envelope</li> <li>Ext Tag: Multiple BSSID Configuration</li> <li>Ext Tag: HE Capabilities</li> <li>Ext Tag: HE Operation</li> <li>Ext Tag: Spatial Reuse Parameter Set</li> <li>Ext Tag: MU-EDCA Parameter Set</li> <li>Ext Tag: HE DSS Band Capabilities</li> <li>Tag: RSN extension (1 octet)</li> <li>Tag number: RSN extension (244)</li> <li>RSN: 0x20 (oct 1) <ul style="list-style-type: none"> <li>..... 0000 = RSN Length: 0</li> <li>..... 0 = Protected but Operations Support: 0</li> <li>..... SAE mesh to element: 1</li> <li>..... = Reserved 00</li> </ul> </li> </ul> </li> </ul> </li> </ul>

Balises SAE WPA3

Ici, nous pouvons observer les clients Wi-Fi 6E associés :

Intel AX211

Connexion OTA avec accent sur les informations RSN du client :

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
2235	2023-06-12 17:15:00.328310	0.00000	IntelCor_9e158f0f	Broadcast	802.11	168	5.47 dBm	Probe Request, Shw389, FwB, Flags:.....C, SSID=Wildcard (Broadcast)	<ul style="list-style-type: none"> <li>Frame 1225: 194 bytes on wire (1552 bits), 194 bytes captured (1552 bits) on interface Vdevoice\NPF_{04578995-2998-4464-4}</li> <li>Ethernet II, Src: Cisco_0d70137 (08:00:0d:0d:70137), Dst: Universe_b7fc1f6e (08:1a:8b:b7:cf:6e)</li> <li>Internet Protocol version 4, Src: 192.168.1.11, Dst: 192.168.1.11</li> <li>User Datagram Protocol, Src Port: 5555, Dst Port: 5000</li> <li>Airframe/OnMFrame encapsulated IEEE 802.11</li> <li>IEEE 802.11 radio information</li> <li>IEEE 802.11 authentication, Flags:.....C</li> <li>IEEE 802.11 wireless management</li> <li>Fixed parameters (184 bytes) <ul style="list-style-type: none"> <li>Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (3)</li> <li>Authentication SAE: 00001</li> <li>Status code: SAE authentication uses direct hashing, instead of looping, to obtain the PMK (00000)</li> <li>SAE message type: Commit (1)</li> <li>Group ID: 254-01 random ECP group (19)</li> <li>Scalar: dc0385ace797f2acaf608a67c4c4779a0d104818a1c18580e425312</li> <li>Finite Field Element: 58c775a0786249b0212ec7275ed66d2a285726786a48eac6d012f70934.</li> </ul> </li> </ul>

Détails du client dans le WLC :

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. On the left is a navigation menu with options like Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main area is titled 'Monitoring > Wireless > Clients'. It displays a table of clients with columns for Client MAC Address, IPv4 Address, IPv6 Address, and AP Name. One client is selected and highlighted in blue. To the right, a detailed view of the selected client is shown, including tabs for Client Properties, AP Properties, Security Information, Client Statistics, QoS Properties, and EoGRE. 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, IF ID, Authorized status, Common Session ID, Acct Session ID, Auth Method Status List, and Local Policies.

## NetGear A8000

Connexion OTA avec accent sur les informations RSN du client :

The screenshot shows a Wireshark packet capture of IEEE 802.11 wireless management frames. The packet list pane on the left shows several frames, with frame 797 selected. The packet details pane on the right shows the structure of the selected frame, including IEEE 802.11 Wireless Management, Fixed Parameters, Tagged Parameters, and RSN Information. The RSN Information section is expanded, showing details like RSN Version, Group Cipher Suite, Pairwise Cipher Suite List, Auth Key Management, and RSN Capabilities.

## Détails du client dans le WLC :

This screenshot is similar to the first one, showing the Cisco Catalyst 9800-CL Wireless Controller interface. The client list table is visible, and the detailed view of the selected client is shown on the right. The Security Information tab is active, displaying details for the selected client, including 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, IF ID, Authorized status, Common Session ID, Acct Session ID, Auth Method Status List, and Local Policies.

## Pixel 6a

Connexion OTA avec accent sur les informations RSN du 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_31180:16	Broadcast	802.11	343	-42 dBm	Probe Request, S/W=99, P/W=0, Flags=.....C, SSID="wifi6_test"
1243	2023-06-12 17:37:02.855631	0.117298	Google_7218a:66	Cisco_31180:16	Authentication	802.11	194	-42 dBm	Authentication, S/W=997, P/W=0, Flags=.....C
1244	2023-06-12 17:37:02.855631	0.000000	192.168.1.121	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
1246	2023-06-12 17:37:02.859394	0.007353	Cisco_31180:16	Google_7218a:66	Authentication	802.11	194	-37 dBm	Authentication, S/W=1, P/W=0, Flags=.....C
1247	2023-06-12 17:37:02.859394	0.000000	192.168.1.121	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_31180:16	Authentication	802.11	194	-41 dBm	Authentication, S/W=998, P/W=0, Flags=.....C
1249	2023-06-12 17:37:02.868831	0.000000	192.168.1.121	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
1250	2023-06-12 17:37:02.904326	0.035495	Cisco_31180:16	Google_7218a:66	Authentication	802.11	194	-37 dBm	Authentication, S/W=1, P/W=0, Flags=.....C
1253	2023-06-12 17:37:02.904326	0.000000	192.168.1.121	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_31180:16	Association Request	802.11	262	-41 dBm	Association Request, S/W=999, P/W=0, Flags=.....C, SSID="wifi6_test"
1256	2023-06-12 17:37:02.929933	0.000000	192.168.1.121	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_31180:16	Authentication	802.11	194	-37 dBm	I, P, N(=1), N(=1); DSAP Basic Individual, SSAP Basic Command
1261	2023-06-12 17:37:02.934129	0.003739	Cisco_31180:16	Google_7218a:66	Association Response	802.11	262	-37 dBm	Association Response, S/W=0, P/W=0, Flags=.....C
1262	2023-06-12 17:37:02.934129	0.000000	192.168.1.121	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=0x, N(=0); DSAP Basic Group, SSAP Basic Response	
1265	2023-06-12 17:37:02.943892	0.009663	Cisco_31180:16	Google_7218a:66	EAPOL	223	-37 dBm	Key (message 1 of 4)	
1266	2023-06-12 17:37:02.943892	0.000000	192.168.1.121	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_31180:16	EAPOL	238	-51 dBm	Key (message 2 of 4)	
1274	2023-06-12 17:37:02.992247	0.000000	192.168.1.121	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
1275	2023-06-12 17:37:02.995369	0.003122	Cisco_31180:16	Google_7218a:66	EAPOL	295	-37 dBm	Key (message 3 of 4)	
1276	2023-06-12 17:37:02.995369	0.000000	192.168.1.121	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_31180:16	EAPOL	199	-48 dBm	Key (message 4 of 4)	
1279	2023-06-12 17:37:03.000159	0.000000	192.168.1.121	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
1281	2023-06-12 17:37:03.021799	0.021231	192.168.1.121	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_31180:16	Action	802.11	122	-49 dBm	Action, S/W=180, P/W=0, Flags=.....C (Malformed Packet)
1283	2023-06-12 17:37:03.025924	0.000000	192.168.1.121	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
1284	2023-06-12 17:37:03.040303	0.017809	192.168.1.121	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
1286	2023-06-12 17:37:03.040303	0.007753	192.168.1.121	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
1290	2023-06-12 17:37:03.078167	0.027481	Cisco_31180:16	Google_7218a:66	Action	802.11	124	-37 dBm	Action, S/W=1, P/W=0, Flags=.....C
1291	2023-06-12 17:37:03.078167	0.000000	192.168.1.121	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_31180:16	Action	802.11	115	-48 dBm	Action, S/W=180, P/W=0, Flags=.....C
1298	2023-06-12 17:37:03.166223	0.000000	192.168.1.121	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	IPV6cast_vf, LLC	227	-37 dBm	U, P, Func=0x, N(=0); DSAP Basic Group, SSAP Basic Command		
1300	2023-06-12 17:37:03.166229	0.000000	192.168.1.121	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
1302	2023-06-12 17:37:03.167999	0.001780	Google_7218a:66	Google_7218a:66	Action	802.11	115	-37 dBm	Action, S/W=1, P/W=0, Flags=.....C (Malformed Packet)
1303	2023-06-12 17:37:03.167999	0.000000	192.168.1.121	192.168.1.121	802.11	76	-49 dBm	Acknowledgment, Flags=.....C	
1304	2023-06-12 17:37:03.167999	0.000000	192.168.1.121	192.168.1.121	802.11	82	-49 dBm	802.11 Block Ack Req, Flags=.....C	
1305	2023-06-12 17:37:03.168136	0.000180	192.168.1.121	192.168.1.121	802.11	94	-37 dBm	802.11 Block Ack, Flags=.....C	
1306	2023-06-12 17:37:03.168543	0.000477	Google_7218a:66	IPV6cast_vf, LLC	186	-38 dBm	I, P, N(=1), N(=1); DSAP Basic Individual, SSAP Basic Response		
1307	2023-06-12 17:37:03.177442	0.000899	192.168.1.121	192.168.1.121	802.11	82	-46 dBm	Request-to-send, Flags=.....C	
1308	2023-06-12 17:37:03.177442	0.000000	192.168.1.121	192.168.1.121	802.11	76	-36 dBm	Clear-to-send, Flags=.....C	
1309	2023-06-12 17:37:03.177515	0.000073	Google_7218a:66	IPV6cast_vf, LLC	271	-56 dBm	I, N(=1), N(=1); DSAP Basic Group, SSAP Basic Response		

```

> Frame 1255: 262 bytes on wire (2096 bits), 262 bytes captured (2096 bits) on interface Vdevice\MPF_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: 192.168.1.18, Dst: 192.168.1.121
> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
> Airopeex/OmniPeex encapsulated IEEE 802.11
> IEEE 802.11 radio information
> IEEE 802.11 Association Request, Flags: .....C
  > fixed parameters (4 bytes)
  > Tagged parameters (168 bytes)
    > Tag: SSID parameter Set: "wifi6_test"
    > Tag: Supported rates (0), 9, 12, 18, 24, 36, 48, 54, 60, 66, 72, 84, 96, 108, 120, 132, 144, 150, 165, 180, 195, 210, 225, 240, 255, 270, 285, 300, 315, 330, 345, 360, 375, 390, 405, 420, 435, 450, 465, 480, 495, 510, 525, 540, 555, 570, 585, 600, 615, 630, 645, 660, 675, 690, 705, 720, 735, 750, 765, 780, 795, 810, 825, 840, 855, 870, 885, 900, 915, 930, 945, 960, 975, 990, 1005, 1020, 1035, 1050, 1065, 1080, 1095, 1110, 1125, 1140, 1155, 1170, 1185, 1200, 1215, 1230, 1245, 1260, 1275, 1290, 1305, 1320, 1335, 1350, 1365, 1380, 1395, 1410, 1425, 1440, 1455, 1470, 1485, 1500, 1515, 1530, 1545, 1560, 1575, 1590, 1605, 1620, 1635, 1650, 1665, 1680, 1695, 1710, 1725, 1740, 1755, 1770, 1785, 1800, 1815, 1830, 1845, 1860, 1875, 1890, 1905, 1920, 1935, 1950, 1965, 1980, 1995, 2010, 2025, 2040, 2055, 2070, 2085, 2100, 2115, 2130, 2145, 2160, 2175, 2190, 2205, 2220, 2235, 2250, 2265, 2280, 2295, 2310, 2325, 2340, 2355, 2370, 2385, 2400, 2415, 2430, 2445, 2460, 2475, 2490, 2505, 2520, 2535, 2550, 2565, 2580, 2595, 2610, 2625, 2640, 2655, 2670, 2685, 2700, 2715, 2730, 2745, 2760, 2775, 2790, 2805, 2820, 2835, 2850, 2865, 2880, 2895, 2910, 2925, 2940, 2955, 2970, 2985, 3000, 3015, 3030, 3045, 3060, 3075, 3090, 3105, 3120, 3135, 3150, 3165, 3180, 3195, 3210, 3225, 3240, 3255, 3270, 3285, 3300, 3315, 3330, 3345, 3360, 3375, 3390, 3405, 3420, 3435, 3450, 3465, 3480, 3495, 3510, 3525, 3540, 3555, 3570, 3585, 3600, 3615, 3630, 3645, 3660, 3675, 3690, 3705, 3720, 3735, 3750, 3765, 3780, 3795, 3810, 3825, 3840, 3855, 3870, 3885, 3900, 3915, 3930, 3945, 3960, 3975, 3990, 4005, 4020, 4035, 4050, 4065, 4080, 4095, 4110, 4125, 4140, 4155, 4170, 4185, 4200, 4215, 4230, 4245, 4260, 4275, 4290, 4305, 4320, 4335, 4350, 4365, 4380, 4395, 4410, 4425, 4440, 4455, 4470, 4485, 4500, 4515, 4530, 4545, 4560, 4575, 4590, 4605, 4620, 4635, 4650, 4665, 4680, 4695, 4710, 4725, 4740, 4755, 4770, 4785, 4800, 4815, 4830, 4845, 4860, 4875, 4890, 4905, 4920, 4935, 4950, 4965, 4980, 4995, 5010, 5025, 5040, 5055, 5070, 5085, 5100, 5115, 5130, 5145, 5160, 5175, 5190, 5205, 5220, 5235, 5250, 5265, 5280, 5295, 5310, 5325, 5340, 5355, 5370, 5385, 5400, 5415, 5430, 5445, 5460, 5475, 5490, 5505, 5520, 5535, 5550, 5565, 5580, 5595, 5610, 5625, 5640, 5655, 5670, 5685, 5700, 5715, 5730, 5745, 5760, 5775, 5790, 5805, 5820, 5835, 5850, 5865, 5880, 5895, 5910, 5925, 5940, 5955, 5970, 5985, 6000, 6015, 6030, 6045, 6060, 6075, 6090, 6105, 6120, 6135, 6150, 6165, 6180, 6195, 6210, 6225, 6240, 6255, 6270, 6285, 6300, 6315, 6330, 6345, 6360, 6375, 6390, 6405, 6420, 6435, 6450, 6465, 6480, 6495, 6510, 6525, 6540, 6555, 6570, 6585, 6600, 6615, 6630, 6645, 6660, 6675, 6690, 6705, 6720, 6735, 6750, 6765, 6780, 6795, 6810, 6825, 6840, 6855, 6870, 6885, 6900, 6915, 6930, 6945, 6960, 6975, 6990, 7005, 7020, 7035, 7050, 7065, 7080, 7095, 7110, 7125, 7140, 7155, 7170, 7185, 7200, 7215, 7230, 7245, 7260, 7275, 7290, 7305, 7320, 7335, 7350, 7365, 7380, 7395, 7410, 7425, 7440, 7455, 7470, 7485, 7500, 7515, 7530, 7545, 7560, 7575, 7590, 7605, 7620, 7635, 7650, 7665, 7680, 7695, 7710, 7725, 7740, 7755, 7770, 7785, 7800, 7815, 7830, 7845, 7860, 7875, 7890, 7905, 7920, 7935, 7950, 7965, 7980, 7995, 8010, 8025, 8040, 8055, 8070, 8085, 8100, 8115, 8130, 8145, 8160, 8175, 8190, 8205, 8220, 8235, 8250, 8265, 8280, 8295, 8310, 8325, 8340, 8355, 8370, 8385, 8400, 8415, 8430, 8445, 8460, 8475, 8490, 8505, 8520, 8535, 8550, 8565, 8580, 8595, 8610, 8625, 8640, 8655, 8670, 8685, 8700, 8715, 8730, 8745, 8760, 8775, 8790, 8805, 8820, 8835, 8850, 8865, 8880, 8895, 8910, 8925, 8940, 8955, 8970, 8985, 9000, 9015, 9030, 9045, 9060, 9075, 9090, 9105, 9120, 9135, 9150, 9165, 9180, 9195, 9210, 9225, 9240, 9255, 9270, 9285, 9300, 9315, 9330, 9345, 9360, 9375, 9390, 9405, 9420, 9435, 9450, 9465, 9480, 9495, 9510, 9525, 9540, 9555, 9570, 9585, 9600, 9615, 9630, 9645, 9660, 9675, 9690, 9705, 9720, 9735, 9750, 9765, 9780, 9795, 9810, 9825, 9840, 9855, 9870, 9885, 9900, 9915, 9930, 9945, 9960, 9975, 9990, 10005, 10020, 10035, 10050, 10065, 10080, 10095, 10110, 10125, 10140, 10155, 10170, 10185, 10200, 10215, 10230, 10245, 10260, 10275, 10290, 10305, 10320, 10335, 10350, 10365, 10380, 10395, 10410, 10425, 10440, 10455, 10470, 10485, 10500, 10515, 10530, 10545, 10560, 10575, 10590, 10605, 10620, 10635, 10650, 10665, 10680, 10695, 10710, 10725, 10740, 10755, 10770, 10785, 10800, 10815, 10830, 10845, 10860, 10875, 10890, 10905, 10920, 10935, 10950, 10965, 10980, 10995, 11010, 11025, 11040, 11055, 11070, 11085, 11100, 11115, 11130, 11145, 11160, 11175, 11190, 11205, 11220, 11235, 11250, 11265, 11280, 11295, 11310, 11325, 11340, 11355, 11370, 11385, 11400, 11415, 11430, 11445, 11460, 11475, 11490, 11505, 11520, 11535, 11550, 11565, 11580, 11595, 11610, 11625, 11640, 11655, 11670, 11685, 11700, 11715, 11730, 11745, 11760, 11775, 11790, 11805, 11820, 11835, 11850, 11865, 11880, 11895, 11910, 11925, 11940, 11955, 11970, 11985, 12000, 12015, 12030, 12045, 12060, 12075, 12090, 12105, 12120, 12135, 12150, 12165, 12180, 12195, 12210, 12225, 12240, 12255, 12270, 12285, 12300, 12315, 12330, 12345, 12360, 12375, 12390, 12405, 12420, 12435, 12450, 12465, 12480, 12495, 12510, 12525, 12540, 12555, 12570, 12585, 12600, 12615, 12630, 12645, 12660, 12675, 12690, 12705, 12720, 12735, 12750, 12765, 12780, 12795, 12810, 12825, 12840, 12855, 12870, 12885, 12900, 12915, 12930, 12945, 12960, 12975, 12990, 13005, 13020, 13035, 13050, 13065, 13080, 13095, 13110, 13125, 13140, 13155, 13170, 13185, 13200, 13215, 13230, 13245, 13260, 13275, 13290, 13305, 13320, 13335, 13350, 13365, 13380, 13395, 13410, 13425, 13440, 13455, 13470, 13485, 13500, 13515, 13530, 13545, 13560, 13575, 13590, 13605, 13620, 13635, 13650, 13665, 13680, 13695, 13710, 13725, 13740, 13755, 13770, 
```

Cisco Catalyst 9800-CL Wireless Controller 17.9.3

Welcome admin

Search APs and Clients

Feedback

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Delete

Selected 0 out of 12 Clients

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

Client

360 View General QoS Statistics ATF Statistics Mobility History Call Statistics

Client Properties AP Properties Security Information Client Statistics QoS Properties EoGRE

Client State Servers None

Client ACLs None

Client Entry Create Time 78 seconds

Policy Type WPA3

Encryption Cipher CCMP (AES)

Authentication Key Management SAE

EAP Type Not Applicable

Session Timeout 86400

Session Manager

Point of Attachment capwap\_90000010

IF ID 0x90000010

Authorized TRUE

Common Session ID 000000000000FB1B0A58F78

Acct Session ID 0x00000000

Auth Method Status List

Method SAE

WPA3 personnel - AES(CCMP128) + SAE + FT

Configuration de la sécurité 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**

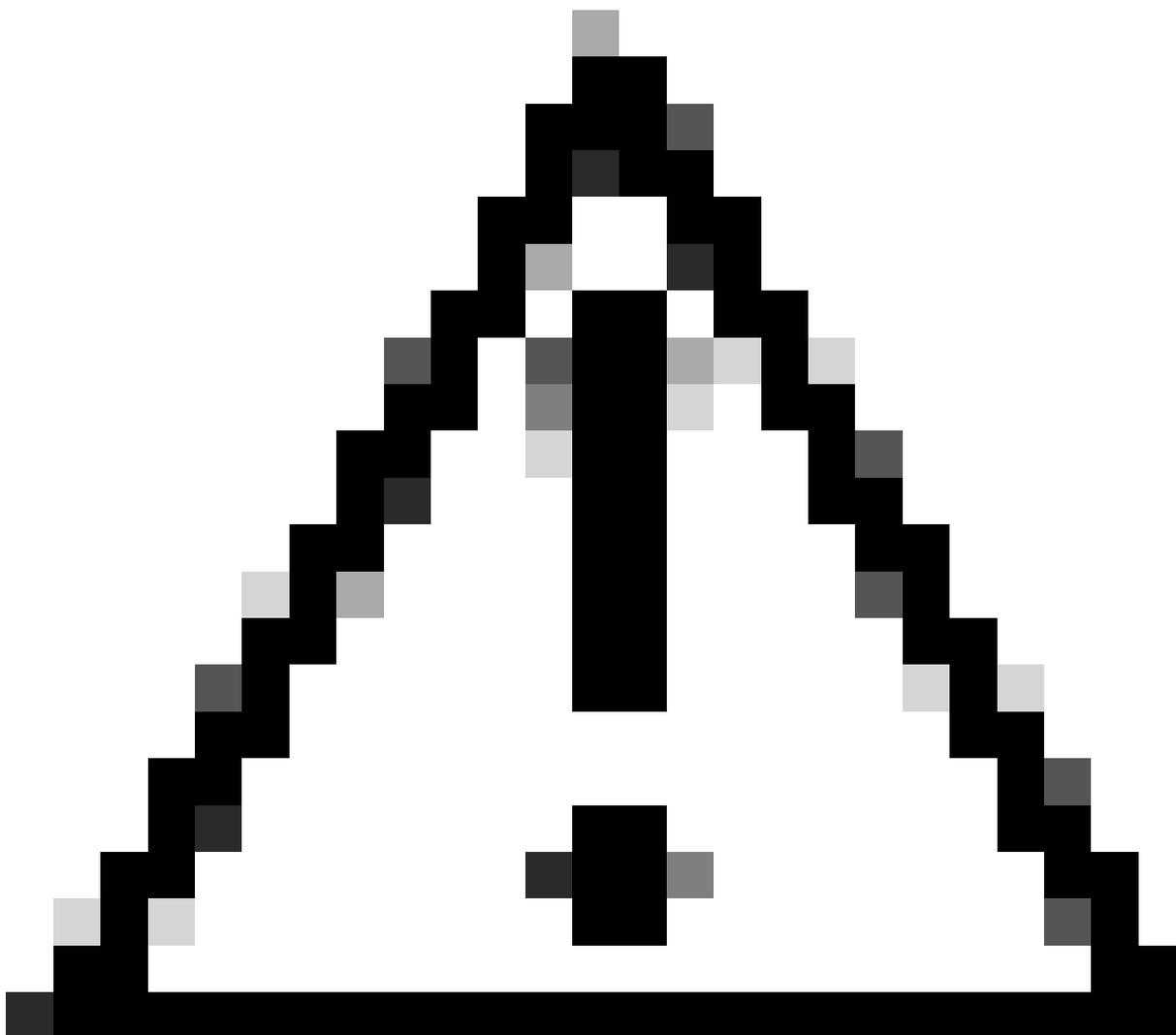
AES(OCMP128)  CCMP256   
 GCMP128  GCMP256

**Auth Key Mgmt**

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

**Protected Management Frame**

PMF    
 Association Comeback Timer\*   
 SA Query Time\*



Attention : dans la gestion des clés d'authentification, le WLC permet de sélectionner FT+SAE sans SAE activé, mais il a été observé que les clients ne pouvaient pas se connecter. Activez toujours les deux cases à cocher SAE et FT+SAE si vous souhaitez utiliser SAE avec transition rapide.

---

Affichage sur l'interface graphique utilisateur WLC des paramètres de sécurité WLAN :

A screenshot of a WLC GUI showing WLAN security parameters. The interface includes a top navigation bar with a home icon, a green status indicator, the text 'wifGE\_test', a blue status indicator, the text 'wifGE\_test', and a status indicator with the text '[WPA3][SAE][FT + SAE][AES][FT Enabled]'. The main content area is currently blank.

wifGE\_test wifGE\_test [WPA3][SAE][FT + SAE][AES][FT Enabled]

Vérification des balises OTA :

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
1	2023-06-12 18:34:49.35337	0.000000	Cisco_13:180:e7	Eurocast	802.11	588	5	-36 dBm	Beacon frame, S/W=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 18:34:49.50867	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	Netgear_48:78:95	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	Netgear_48:78:95	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	0.000000	192.168.1.15	192.168.1.121	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 18:34:49.89656	0.021812	Cisco_13:180:e7	Netgear_48:78:95	802.11	194	5	-37 dBm	Authentication, S/W=54, F/W=, Flags=.....C
15	2023-06-12 18:34:49.89656	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	Netgear_48:78:95	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	130	5	-37 dBm	Authentication, S/W=, F/W=, Flags=.....C
19	2023-06-12 18:34:49.90496	0.000000	Cisco_13:180:e7	Eurocast	802.11	588	5	-37 dBm	Beacon frame, S/W=27, F/W=, Flags=.....C, B=100, SSID="wifi6_test"
20	2023-06-12 18:34:49.90496	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-48 dBm	Acknowledgment, Flags=.....C
21	2023-06-12 18:34:49.90496	0.000000	Netgear_48:78:95	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	0.000000	Cisco_13:180:e7	Netgear_48:78:95	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	Netgear_48:78:95	Eurocast	LLC	114	5	-37 dBm	U, func:unknown; DSAP 0x02 Individual, SSAP 0x02 Command
26	2023-06-12 18:34:49.91719	0.000000	Netgear_48:78:95	Eurocast	LLC	114	5	-36 dBm	U, func:unknown; DSAP 0x02 Individual, SSAP 0x02 Response
27	2023-06-12 18:34:49.92236	0.001827	Cisco_13:180:e7	Netgear_48:78:95	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	0.104929	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	-40 dBm	Beacon frame, S/W=27, F/W=, Flags=.....C, B=100, SSID="wifi6_test"
32	2023-06-12 18:34:50.21161	0.007615	Netgear_48:78:95	Cisco_13:180:e7	EAPOL	226	5	-55 dBm	Key (Message 2 of 4)
33	2023-06-12 18:34:50.21161	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-42 dBm	Acknowledgment, Flags=.....C
34	2023-06-12 18:34:50.21161	0.000000	Netgear_48:78:95	Eurocast	LLC	296	5	-49 dBm	Key (Message 3 of 4)
35	2023-06-12 18:34:50.21376	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-58 dBm	Acknowledgment, Flags=.....C
36	2023-06-12 18:34:50.21454	0.000978	Netgear_48:78:95	Cisco_13:180:e7	EAPOL	199	5	-56 dBm	Key (Message 4 of 4)
37	2023-06-12 18:34:50.22240	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-42 dBm	Acknowledgment, Flags=.....C
38	2023-06-12 18:34:50.22722	0.006367	192.168.1.15	192.168.1.121	802.11	76	5	-42 dBm	Acknowledgment, Flags=.....C
39	2023-06-12 18:34:50.22849	0.003128	192.168.1.15	192.168.1.121	802.11	119	5	-44 dBm	Trigger Buffer Status Report Poll (BSRP), Flags=.....C
40	2023-06-12 18:34:50.22849	0.000000	Netgear_48:78:95	Eurocast	LLC	221	5	-44 dBm	U, func:unknown; DSAP 0x02 Group, SSAP 0x02 Response
41	2023-06-12 18:34:50.22849	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-54 dBm	Acknowledgment, Flags=.....C

WPA3 SAE + balises FT

Ici, nous pouvons observer les clients Wi-Fi 6E associés :

Intel AX211

Connexion OTA avec accent sur les informations RSN du client :

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
1811	2023-06-12 18:51:39.24979	0.001337	IntelCor_98:58:5f	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	-49 dBm	Acknowledgment, Flags=.....C
1813	2023-06-12 18:51:39.254827	0.007834	Cisco_13:180:e7	IntelCor_98:58:5f	802.11	194	5	-36 dBm	Authentication, S/W=59, F/W=, Flags=.....C
1814	2023-06-12 18:51:39.254827	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-42 dBm	Acknowledgment, Flags=.....C
1815	2023-06-12 18:51:39.259394	0.002167	IntelCor_98:58:5f	Cisco_13:180:e7	802.11	130	5	-40 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	0.004235	Cisco_13:180:e7	IntelCor_98:58:5f	802.11	130	5	-36 dBm	Authentication, S/W=58, 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_98:58:5f	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
1826	2023-06-12 18:51:39.271442	0.018463	IntelCor_98:58:5f	Eurocast	LLC	114	5	-36 dBm	I, H(K)=, N(S)=; DSAP 0x02 Group, SSAP 0x02 Response
1827	2023-06-12 18:51:39.271442	0.000000	IntelCor_98:58:5f	Eurocast	LLC	114	5	-36 dBm	I, H(K)=, N(S)=; DSAP 0x02 Group, SSAP 0x02 Response
1828	2023-06-12 18:51:39.277402	0.001240	Cisco_13:180:e7	IntelCor_98:58:5f	802.11	262	5	-36 dBm	Association Response, S/W=, F/W=, Flags=.....C
1829	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
1830	2023-06-12 18:51:39.28187	0.003795	Cisco_13:180:e7	Eurocast	802.11	517	5	-36 dBm	Beacon frame, S/W=71, F/W=, Flags=.....C, B=100, SSID="wifi6_test_02"
1834	2023-06-12 18:51:39.311349	0.025242	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1835	2023-06-12 18:51:39.311349	0.000449	192.168.1.15	192.168.1.121	802.11	76	5	-52 dBm	Clear-to-send, Flags=.....C
1837	2023-06-12 18:51:39.332425	0.017227	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1841	2023-06-12 18:51:39.388468	0.055835	Cisco_13:180:e7	Eurocast	802.11	517	5	-37 dBm	Beacon frame, S/W=76, F/W=, Flags=.....C, B=100, SSID="wifi6_test_02"
1842	2023-06-12 18:51:39.389388	0.001348	192.168.1.15	192.168.1.121	802.11	76	5	-53 dBm	Clear-to-send, Flags=.....C
1844	2023-06-12 18:51:39.397943	0.008131	192.168.1.15	192.168.1.121	802.11	82	5	-38 dBm	Request-to-send, Flags=.....C
1845	2023-06-12 18:51:39.399282	0.001839	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1846	2023-06-12 18:51:39.399812	0.000530	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1847	2023-06-12 18:51:39.400924	0.000712	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1848	2023-06-12 18:51:39.401191	0.000667	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1849	2023-06-12 18:51:39.402035	0.000844	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1850	2023-06-12 18:51:39.402517	0.000582	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1851	2023-06-12 18:51:39.402523	0.000636	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1852	2023-06-12 18:51:39.404674	0.001321	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1853	2023-06-12 18:51:39.405196	0.000732	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1854	2023-06-12 18:51:39.405877	0.000571	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1855	2023-06-12 18:51:39.406637	0.000769	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1856	2023-06-12 18:51:39.406651	0.000044	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1857	2023-06-12 18:51:39.407244	0.000563	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1859	2023-06-12 18:51:39.407327	0.000283	Cisco_13:180:e7	IntelCor_98:58:5f	EAPOL	221	5	-52 dBm	Key (Message 1 of 4)
1860	2023-06-12 18:51:39.407327	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-48 dBm	Acknowledgment, Flags=.....C
1862	2023-06-12 18:51:39.428712	0.003185	IntelCor_98:58:5f	Cisco_13:180:e7	EAPOL	230	5	-56 dBm	Key (Message 2 of 4)
1863	2023-06-12 18:51:39.428712	0.000000	192.168.1.15	192.168.1.121	8				



## Détails du client dans le WLC :

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main area is titled 'Monitoring > Wireless > Clients'. Below this, there are tabs for 'Clients', 'Sleeping Clients', and 'Excluded Clients'. A table lists 13 clients with columns for Client MAC Address, IPv4 Address, IPv6 Address, and AP Name. The client with MAC address 9418.6548.7095 is selected. The right pane shows the 'Client' details for this client, including 'General', 'QoS Statistics', 'ATF Statistics', 'Mobility History', and 'Call Statistics'. The 'Security Information' tab is active, showing details like Client State Servers, Client ACLs, Client Entry Create Time, Policy Type, Encryption Cipher, Authentication Key Management, EAP Type, Session Timeout, Session Manager, Point of Attachment, IIF ID, Authorized status, Common Session ID, Acct Session ID, Auth Method Status List, and Method.

Pixel 6a

Le périphérique n'a pas pu se déplacer lorsque FT est activé.

Samsung S23

Le périphérique n'a pas pu se déplacer lorsque FT est activé.

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

## Configuration de la sécurité 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 right pane shows the 'Edit WLAN' configuration for 'wif6E\_test'. The 'Security' tab is active, showing 'Layer2' settings. The 'WPA' section has 'WPA3' selected. The 'WPA2/WPA3 Encryption' section has 'AES(CCMP128)' and '802.1x-SHA256' selected. The 'Auth Key Mgmt' section has 'FT + SAE' and 'FT + 802.1x' selected. The 'Protected Management Frame' section has 'PMF' set to 'Required'.

Configuration de la sécurité WPA3 Enterprise 802.1x-SHA256 + FTWLAN

## Affichage sur l'interface graphique utilisateur WLC des paramètres de sécurité WLAN :

The screenshot shows the bottom of the Cisco Catalyst 9800-CL Wireless Controller interface. It displays the WLAN configuration summary for 'wif6E\_test' with the following parameters: [WPA3][FT + 802.1x][AES][PMF 802.1x][FT Enabled].

Ici, nous pouvons voir les journaux en direct ISE montrant les authentifications provenant de



Un comportement intéressant se produit si vous supprimez manuellement le client du WLAN (à partir de l'interface graphique du WLC par exemple). Le client reçoit une trame de dissociation mais tente de se reconnecter au même AP et utilise une trame de réassociation suivie d'un échange EAP complet parce que les détails du client ont été supprimés de l'AP/WLC.

Il s'agit essentiellement du même échange de trames que dans un nouveau processus d'association. Ici vous pouvez voir l'échange de trames :

The image shows a Wireshark packet capture of a WLAN client re-associating with an AP. The capture is annotated with several sections:

- Probing and authentication frames:** Lines 179-200, showing initial probe requests and responses.
- Regular Association:** Lines 201-300, showing the association request and response.
- EAP Exchange:** Lines 301-400, showing the EAP-FT exchange, including the EAP-Request, EAP-Response, and EAP-Request/Response.
- 4 Way Handshake:** Lines 401-450, showing the final 4-way handshake for key derivation.

A detailed view of the EAP-FT frame (line 301) is shown on the right, highlighting the 'Auth Key Management (AKM) List' and 'Auth Key Management (AKM) Type: FT over IEEE 802.1X'. A red box and arrow point to the 'Auth Key Management (AKM) Type: FT over IEEE 802.1X' field, with the label 'PMKID used for FT'.

Flux de connexion WPA3 Enterprise 802.1x + FT Ax211

Détails du client dans le WLC :

The screenshot shows the Cisco WLC GUI with the 'Clients' tab selected. The 'Client Properties' section is expanded to show 'Security Information'. The 'Security Information' section shows the following details:

- Re-Authentication Timeout: 1800 sec (Remaining time: 462 sec)
- Client State Servers: None
- Client ACLs: None
- Client Entry Create Time: 1338 seconds
- Policy Type: WPA3
- Encryption Cipher: CCMP (AES)
- Authentication Key Management: FT-802.1x
- EAP Type: PEAP
- Session Timeout: 1800

Détails du client WPA3 Enterprise 802.1x + FT

Ce client a également été testé à l'aide de FT sur le DS et a pu se déplacer à l'aide de 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	dbm	Beacon frame, SN=3685, FHW, Flags=.....C, BI=100, SSID=W
879	1.409057	0.120370	Google_72:8a:96	Broadcast	802.11	204	69-17	dbm	Probe Request, SN=3685, FHW, Flags=.....C, SSID=Wifi6E, S
880	1.561362	0.000405	Cisco_08:00:18	Broadcast	802.11	428	69-17	dbm	Beacon frame, SN=3685, FHW, Flags=.....C, BI=100, SSID=W
882	1.564878	0.000716	Cisco_08:00:18	Broadcast	802.11	374	69-17	dbm	Probe Response, SN=3685, FHW, Flags=.....C, BI=100, SSID=W
928	1.675576	0.114998	Cisco_08:00:18	Broadcast	802.11	428	69-17	dbm	Beacon frame, SN=3685, FHW, Flags=.....C, BI=100, SSID=W
932	1.675989	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Request, Protected GAP (EAP-PEAP)
933	1.675989	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Acknowledgment, Flags=.....C
923	1.679651	0.003842	Cisco_08:00:18	Broadcast	802.11	108	69-17	dbm	Authentication, SN=34, FHW, Flags=.....C
924	1.679651	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-16	dbm	Acknowledgment, Flags=.....C
925	1.682824	0.000000	Google_72:8a:96	Broadcast	802.11	284	69-18	dbm	Association Request, SN=3685, FHW, Flags=.....C, SSID=W
926	1.682824	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Acknowledgment, Flags=.....C
930	1.782511	0.023970	Cisco_08:00:18	Broadcast	802.11	313	69-17	dbm	Association Response, SN=36, FHW, Flags=.....C
931	1.782511	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-13	dbm	Acknowledgment, Flags=.....C
932	1.782689	0.000620	Google_72:8a:96	EAP	119	389	69-17	dbm	Request, Identity
933	1.782689	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-11	dbm	Acknowledgment, Flags=.....C
939	1.747377	0.017007	Google_72:8a:96	EAP	117	117	69-13	dbm	Response, Identity
940	1.747377	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Acknowledgment, Flags=.....C
942	1.784248	0.012047	Cisco_08:00:18	EAP	119	119	69-17	dbm	Request, Protected GAP (EAP-PEAP)
943	1.784248	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-11	dbm	Acknowledgment, Flags=.....C
945	1.788896	0.005672	Cisco_08:00:18	Broadcast	802.11	428	69-17	dbm	Beacon frame, SN=3685, FHW, Flags=.....C, BI=100, SSID=W
946	1.788896	0.000180	Google_72:8a:96	LIC	124	124	69-17	dbm	1, N(1)=8, N(5)=7; SOAP:808 Individual, SOAP:808 Response
949	1.779457	0.018977	Google_72:8a:96	EAP	119	119	69-17	dbm	Request, Protected GAP (EAP-PEAP)
950	1.779457	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Acknowledgment, Flags=.....C
956	1.794529	0.015801	Cisco_08:00:18	EAP	1116	1116	69-17	dbm	Request, Protected GAP (EAP-PEAP)
957	1.794529	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-18	dbm	Acknowledgment, Flags=.....C
958	1.797058	0.002530	Google_72:8a:96	EAP	119	119	69-17	dbm	Response, Protected GAP (EAP-PEAP)
959	1.797058	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Acknowledgment, Flags=.....C
960	1.801724	0.004656	Cisco_08:00:18	EAP	119	119	69-17	dbm	Client key exchange, Change Cipher Spec, Encrypted Handshake M
961	1.801724	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Acknowledgment, Flags=.....C
963	1.820890	0.004337	Cisco_08:00:18	EAP	119	119	69-17	dbm	Change Cipher Spec, Encrypted Handshake Message
964	1.820890	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Acknowledgment, Flags=.....C
968	1.820890	0.004229	Google_72:8a:96	EAP	119	119	69-17	dbm	Response, Protected GAP (EAP-PEAP)
969	1.820890	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Acknowledgment, Flags=.....C
971	1.831178	0.003960	Cisco_08:00:18	EAP	119	119	69-17	dbm	Application data
972	1.831178	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-19	dbm	Acknowledgment, Flags=.....C
973	1.831728	0.004249	Cisco_08:00:18	EAP	119	119	69-17	dbm	Application data
974	1.831728	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Acknowledgment, Flags=.....C
976	1.840795	0.003290	Cisco_08:00:18	EAP	119	119	69-17	dbm	Application data
977	1.840795	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-19	dbm	Acknowledgment, Flags=.....C
978	1.845522	0.004817	Google_72:8a:96	EAP	119	119	69-17	dbm	Application data
979	1.845522	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Acknowledgment, Flags=.....C
984	1.849494	0.010872	Cisco_08:00:18	EAP	119	119	69-17	dbm	Application data
985	1.849494	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-19	dbm	Acknowledgment, Flags=.....C
986	1.866887	0.002125	Google_72:8a:96	EAP	119	119	69-17	dbm	Application data
987	1.866887	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Acknowledgment, Flags=.....C
988	1.870858	0.003771	Cisco_08:00:18	Broadcast	802.11	428	69-17	dbm	Beacon frame, SN=3687, FHW, Flags=.....C, BI=100, SSID=W
989	1.870858	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Application data
990	1.870858	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-19	dbm	Acknowledgment, Flags=.....C
992	1.877128	0.006470	Google_72:8a:96	EAP	119	119	69-18	dbm	Response, Protected GAP (EAP-PEAP)
993	1.877128	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Acknowledgment, Flags=.....C
996	1.920865	0.002917	Cisco_08:00:18	EAP	119	119	69-17	dbm	Success, Key (Message 2 of 4)
997	1.920865	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-19	dbm	Acknowledgment, Flags=.....C
998	1.920865	0.000000	Cisco_08:00:18	EAP	223	223	69-17	dbm	Key (Message 1 of 4)
999	1.920865	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-19	dbm	Acknowledgment, Flags=.....C
1000	1.920865	0.002917	Google_72:8a:96	EAP	119	119	69-18	dbm	Key (Message 2 of 4)
1001	1.920865	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Acknowledgment, Flags=.....C
1004	1.920677	0.003422	Cisco_08:00:18	EAP	423	423	69-17	dbm	Key (Message 3 of 4)
1005	1.920677	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-19	dbm	Acknowledgment, Flags=.....C
1006	1.920866	0.002099	Google_72:8a:96	EAP	119	119	69-19	dbm	Key (Message 4 of 4)
1007	1.920866	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Acknowledgment, Flags=.....C

```

> Frame 925: 263 bytes on wire (2088 bits), 263 bytes captured (2088 bits) on interface Wpa_04578005-2998-4056-8C31-C3A13
> Ethernet II, Src: Cisco_08:00:18:00:00:00:00, Dst: Indefina_08:00:18:00:00:00:00
> Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.122
> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
> AiroHw/0x10000000 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 (8): 9, 12(0), 18, 24(0), 36, 48, 54, [Mbit/sec]
  > Tag: Power Capability Mtr: 9, Max: 29
  > Tag: Supported Channels
  > Tag: RSN Information (48)
    Tag Length: 28
    RSN Version: 1
    > Group Cipher Suite: 00:0f:ac (See IEEE 802.11 AES (CCM))
    Pairwise Cipher Suite Count: 1
    Pairwise Cipher Suite List: 00:0f:ac (See IEEE 802.11 AES (CCM))
    Auth Key Management (AKM) Suite Count: 1
    Auth Key Management (AKM) List: 00:0f:ac (See IEEE 802.11 FT over IEEE 802.1X)
    Auth Key Management (AKM) OUI: 00:0f:ac (See IEEE 802.11)
    Auth Key Management (AKM) type: FT over IEEE 802.1X (1)
  > RSN Capabilities: 00:00
    .....0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
    .....0 = RSN No Pairwise capabilities: Transmitter can support MP default key if simultaneously with
    .....0 = RSN PTK Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/TKkeySA (0x0)
    .....0 = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/TKkeySA (0x0)
    .....1 = Management frame Protection Required: True
    .....1 = Management frame Protection Capable: True
    .....0 = 32bit PMK11-band RSN: False
    .....0 = Perkey Enabled: False
    .....0 = Extended key ID for Individually Addressed Frames: Not supported
  PMKID Count: 0
  PMKID List:
  > Group Management Cipher Suite: 00:0f:ac (See IEEE 802.11 GIP (128))
  > Tag: WPA Enabled Capabilities (5 octets)
  > Tag: Mobility domain
  > Tag: Supported Operating Classes
  > Tag: Extended Capabilities (20 octets)
  > Ext Tag: HE Capabilities
  > Ext Tag: HE 4-0ns Band Capabilities
  > Tag: Vendor Specific: Broadcom
    Tag Length: 30
    Tag Number: Vendor Specific (221)
    OUI: 00:13:00 (Broadcom)
    Vendor Specific OUI Type: 2
    Vendor Specific Data: 0000000000000000
  > Tag: Vendor Specific: Microsoft Corp.: WPAVUE: Information Element
  
```

Association WPA3 Enterprise 802.1x + FT Pixel6a

## Détails du client dans le WLC :

Détails sur le client WPA3 Enterprise 802.1x + FT Pixel6a

Concentrez-vous sur le type d'itinérance 802.11R sur les ondes, où vous pouvez voir le type d'itinérance 802.11R :

Samsung S23

Connexion OTA avec accent sur les informations RSN du 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=805, Fw=0, Flags=.....C, B1=100, SSID="wif
1247	8.401935	0.102170	Cisco_d5:80:18	Broadcast	802.11	364	69	-40 dBm	Beacon frame, SW=806, Fw=0, Flags=.....C, B1=100, SSID="wif
1248	8.504375	0.102420	Cisco_d5:80:18	Broadcast	802.11	364	69	-39 dBm	Beacon frame, SW=807, Fw=0, Flags=.....C, B1=100, SSID="wif
1249	8.606824	0.102419	Cisco_d5:80:18	Broadcast	802.11	364	69	-40 dBm	Beacon frame, SW=808, Fw=0, Flags=.....C, B1=100, SSID="wif
1251	8.612759	0.005945	Cisco_d5:80:18	Broadcast	802.11	312	69	-40 dBm	Probe Response, SW=859, Fw=0, Flags=.....C, B1=100, SSID="w
1258	8.705133	0.096374	Cisco_d5:80:18	Broadcast	802.11	364	69	-39 dBm	Beacon frame, SW=110, Fw=0, Flags=.....C, B1=100, 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	192.168.1.122	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	192.168.1.122	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=100, Fw=0, Flags=.....C, SSID="wif
1266	8.796439	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-39 dBm	Acknowledgement, Flags=.....C
1268	8.800740	0.005639	Samsung_c9:e3:71	Broadcast	LLC	114	69	-39 dBm	S, Func=03, 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	192.168.1.122	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	0.003581	Cisco_d5:80:18	Broadcast	802.11	364	69	-39 dBm	Beacon frame, SW=111, Fw=0, Flags=.....C, B1=100, SSID="wif
1273	8.832754	0.012133	Cisco_Sc:F8:0c	Samsung_c9:e3:71	LLC	183	69	-40 dBm	U, Func=01DC; DSAP 0x0a Group, SSAP 0x0a Command
1274	8.832754	0.000000	192.168.1.15	192.168.1.122	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	192.168.1.122	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)=12; DSAP 0x0a Individual, SSAP 0x0a Respon
1278	8.800540	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-40 dBm	Acknowledgement, Flags=.....C
1280	8.804143	0.003063	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	192.168.1.122	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	192.168.1.122	802.11	76	69	-40 dBm	Acknowledgement, Flags=.....C
1284	8.806878	0.002075	Altiocel_a36:59: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	8.913912	0.007034	Cisco_d5:80:18	Broadcast	802.11	364	69	-41 dBm	Beacon frame, SW=113, Fw=0, Flags=.....C, B1=100, SSID="wif
1287	8.950493	0.036581	192.168.1.15	192.168.1.122	802.11	76	69	-39 dBm	Acknowledgement, Flags=.....C
1322	9.375553	0.029908	192.168.1.15	192.168.1.122	802.11	76	69	-39 dBm	Acknowledgement, Flags=.....C
1372	9.855519	0.040566	Cisco_d5:80:18	Broadcast	802.11	364	69	-38 dBm	Beacon frame, SW=114, Fw=0, Flags=.....C, B1=100, SSID="wif
1471	9.118083	0.102164	Cisco_d5:80:18	Broadcast	802.11	364	69	-39 dBm	Beacon frame, SW=115, Fw=0, Flags=.....C, B1=100, SSID="wif
1600	9.176814	0.058111	192.168.1.15	192.168.1.122	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=116, Fw=0, Flags=.....C, B1=100, SSID="wif
1933	9.124397	0.102962	Cisco_d5:80:18	Broadcast	802.11	364	69	-39 dBm	Beacon frame, SW=117, Fw=0, Flags=.....C, B1=100, SSID="wif
1937	9.425938	0.103511	Cisco_d5:80:18	Broadcast	802.11	364	69	-40 dBm	Beacon frame, SW=118, Fw=0, Flags=.....C, B1=100, SSID="wif
1939	9.528463	0.102525	Cisco_d5:80:18	Broadcast	802.11	364	69	-38 dBm	Beacon frame, SW=119, Fw=0, Flags=.....C, B1=100, SSID="wif
1945	9.631020	0.102557	Cisco_d5:80:18	Broadcast	802.11	364	69	-38 dBm	Beacon frame, SW=120, Fw=0, Flags=.....C, B1=100, SSID="wif
1946	9.733295	0.102275	Cisco_d5:80:18	Broadcast	802.11	364	69	-39 dBm	Beacon frame, SW=121, Fw=0, Flags=.....C, B1=100, SSID="wif
1950	9.835864	0.102569	Cisco_d5:80:18	Broadcast	802.11	364	69	-40 dBm	Beacon frame, SW=122, Fw=0, Flags=.....C, B1=100, 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	192.168.1.122	802.11	76	69	-40 dBm	Acknowledgement, Flags=.....C
1953	9.826093	0.000057	192.168.1.15	192.168.1.122	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=123, Fw=0, Flags=.....C, B1=100, SSID="wif
1955	9.842143	0.006448	192.168.1.15	192.168.1.122	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: 192.168.1.122
> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
> AiroPcap/OnixPcap encapsulated IEEE 802.11
> 802.11 radio information
> IEEE 802.11 Association Request, Flags: .....C
> IEEE 802.11 Key Management
> Fixed parameters (10 bytes)
> Tagged parameters (185 bytes)
> Tag: SSID parameter set: "wif06_test"
> Tag: Supported Rates (4B): 9, 12(0), 18, 24(0), 36, 48, 54, [Mbit/sec]
> Tag: Power Capability MIMO #, Max: 16
> Tag: Supported Channels
> Tag: RM Enabled Capabilities (5 octets)
> Tag: SNA information
> Tag: Mobility Domain
  > Tag Number: Mobility Domain (54)
  Tag Length: 3
  Mobility Domain Identifier: 0xe2f2
  > 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: @#124d7f4e16ad4ecf65a0a5a0a4ca
  Address: d514f817ab7fa005b7673e1b0d0a082c2fac50b07492e10809b1a809ca
  Owner: 00122a55578aa18c4ef4124242597007905c0e9a12283f566d00b2c0
  > 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

```

Paquets FTODS itinérants S23

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

### Configuration de la sécurité 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

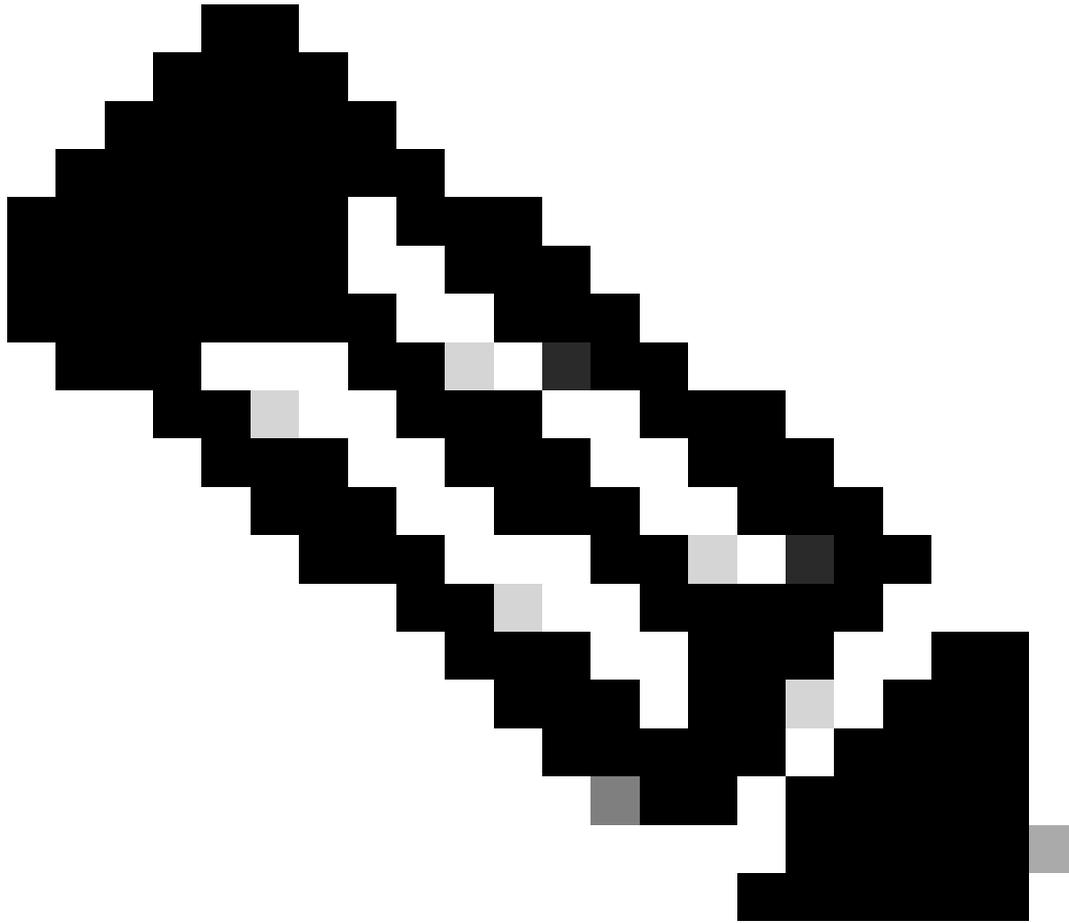
Over the DS

Reassociation Timeout \*

**Auth Key Mgmt**

SUITEB-1X

WPA3 Enterprise SuiteB-1X Configuration de la sécurité



Remarque : FT n'est pas pris en charge dans SUITEB-1X

---

Affichage sur l'interface graphique utilisateur WLC des paramètres de sécurité WLAN :

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

Vérification des balises OTA :

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
37376	59.189776	0.820482	Cisco_06:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2002, Fw=0, Flags=.....C, B=100, SSID=N	> frame 37626: 355 bytes on wire (2840 bits), 355 bytes captured (2840 bits) on interface \Device\NPF_{04576965-2998-4456-8C13-C4}
37385	59.190516	0.820498	Cisco_06:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2003, Fw=0, Flags=.....C, B=100, SSID=N	> Ethernet II, Src: Cisco_02:00:07 (74:11:32:02:07:47), Dst: Unknown_07:c7:0e (08:00:00:07:c7:0e)
37396	59.191709	0.820481	Cisco_06:00:18	Broadcast	802.11	355	69 -17 dbm	Beacon frame, SW=2004, Fw=0, Flags=.....C, B=100, SSID=N	> Internet Protocol Version 4, Src: 192.168.1.121, Dst: 192.168.1.121
37414	59.192161	0.820462	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2005, Fw=0, Flags=.....C, B=100, SSID=N	> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
37424	59.192713	0.820472	Cisco_06:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2006, Fw=0, Flags=.....C, B=100, SSID=N	> AlohaPdu/OnStream encapsulated IEEE 802.11
37437	59.192759	0.820457	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2007, Fw=0, Flags=.....C, B=100, SSID=N	> IEEE 802.11 radio information
37447	59.192792	0.820442	Cisco_06:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2008, Fw=0, Flags=.....C, B=100, SSID=N	> IEEE 802.11 Beacon frame, Flags: .....C
37459	59.193134	0.820522	Cisco_06:00:18	Broadcast	802.11	355	69 -38 dbm	Beacon frame, SW=2009, Fw=0, Flags=.....C, B=100, SSID=N	> IEEE 802.11 Wireless Management
37470	59.193629	0.820399	Cisco_06:00:18	Broadcast	802.11	312	69 -39 dbm	Probe Response, SW=2009, Fw=0, Flags=.....C, B=100, SSID=N	> Fixed parameters (12 bytes)
37480	59.194345	0.820501	Cisco_06:00:18	Broadcast	802.11	355	69 -17 dbm	Beacon frame, SW=2010, Fw=0, Flags=.....C, B=100, SSID=N	> Tagged parameters (213 bytes)
37489	59.194567	0.821342	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2012, Fw=0, Flags=.....C, B=100, SSID=N	> Tag: SSID parameter set: "wifi6_test"
37499	59.195116	0.821629	Cisco_06:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2013, Fw=0, Flags=.....C, B=100, SSID=N	> Tag: Supported Rates (6B), 9, 12(6), 18, 24(6), 36, 48, 54, [Mbit/sec]
37520	59.195713	0.820817	Cisco_06:00:18	Broadcast	802.11	355	69 -17 dbm	Beacon frame, SW=2014, Fw=0, Flags=.....C, B=100, SSID=N	> Tag: Traffic Indication Map (TIM): OPM # of 1 bitmap
37529	59.195889	0.820832	Cisco_06:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2015, Fw=0, Flags=.....C, B=100, SSID=N	> Tag: Country Information: Country Code na, Environment Global operating classes
37532	59.195726	0.821156	Cisco_06:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2016, Fw=0, Flags=.....C, B=100, SSID=N	> Tag: Power Constraint: 6
37539	59.197089	0.821751	Cisco_06:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2017, Fw=0, Flags=.....C, B=100, SSID=N	> Tag: TX Report Transmit Power: 36, Link Operat: 0
37552	59.197468	0.820499	Cisco_06:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2018, Fw=0, Flags=.....C, B=100, SSID=N	> Tag: RSN Information
37565	59.197793	0.820501	Cisco_06:00:18	Broadcast	802.11	355	69 -17 dbm	Beacon frame, SW=2019, Fw=0, Flags=.....C, B=100, SSID=N	> Tag Number: RSN Information (64)
37574	59.198423	0.820438	Cisco_06:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2020, Fw=0, Flags=.....C, B=100, SSID=N	> Tag Length: 26
37585	59.198865	0.820542	Cisco_06:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2021, Fw=0, Flags=.....C, B=100, SSID=N	> RSN Version: 1
37596	59.199439	0.820476	Cisco_06:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2022, Fw=0, Flags=.....C, B=100, SSID=N	> Group Cipher Suite: 00FF:AC (IEEE 802.11) GCM (128)
37606	59.199949	0.820995	Cisco_06:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2023, Fw=0, Flags=.....C, B=100, SSID=N	> Pairwise Cipher Suite Count: 1
37626	59.202621	0.820881	Cisco_06:00:18	Broadcast	802.11	355	69 -38 dbm	Beacon frame, SW=2024, Fw=0, Flags=.....C, B=100, SSID=N	> Pairwise Cipher Suite List 00FF:AC (IEEE 802.11) GCM (128)
37641	59.204964	0.820961	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2025, Fw=0, Flags=.....C, B=100, SSID=N	> Auth Key Management (AKM) Suite Count: 1
37652	59.206137	0.820351	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2026, Fw=0, Flags=.....C, B=100, SSID=N	> Auth Key Management (AKM) List 00FF:AC (IEEE 802.11) WPA (SHA256-Suite0)
37668	59.207165	0.820428	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2027, Fw=0, Flags=.....C, B=100, SSID=N	> Auth Key Management (AKM) SUIT: 00FF:AC (IEEE 802.11)
37687	59.207467	0.820792	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2028, Fw=0, Flags=.....C, B=100, SSID=N	> Auth Key Management (AKM) Type: WPA (SHA256-Suite0) (11)
37696	59.207867	0.820460	Cisco_06:00:18	Broadcast	802.11	355	69 -38 dbm	Beacon frame, SW=2029, Fw=0, Flags=.....C, B=100, SSID=N	> RSN Capabilities: 0x0000
37704	59.208477	0.820430	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2030, Fw=0, Flags=.....C, B=100, SSID=N	> PMKID Count: 0
37719	59.209721	0.820240	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2031, Fw=0, Flags=.....C, B=100, SSID=N	> PMKID List
37733	59.209459	0.820628	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2032, Fw=0, Flags=.....C, B=100, SSID=N	> Group Management Cipher Suite: 00FF:AC (IEEE 802.11) GCM (128)
37738	59.208659	0.820180	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2033, Fw=0, Flags=.....C, B=100, SSID=N	> Tag: QoS User Element: IEEE 802.11e version
37749	59.209208	0.820495	Cisco_06:00:18	Broadcast	802.11	355	69 -38 dbm	Beacon frame, SW=2034, Fw=0, Flags=.....C, B=100, SSID=N	> Tag: W Enabled Capabilities (5 octets)
37775	59.209521	0.820320	Cisco_06:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2035, Fw=0, Flags=.....C, B=100, SSID=N	> Tag: Extended Capabilities (11 octets)
37792	59.206121	0.820508	Cisco_06:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2036, Fw=0, Flags=.....C, B=100, SSID=N	> Tag: Tx Power Envelope
37809	59.207802	0.821581	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2037, Fw=0, Flags=.....C, B=100, SSID=N	> Tag: Tx Power Envelope
37814	59.207513	0.821511	Cisco_06:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2038, Fw=0, Flags=.....C, B=100, SSID=N	> Ext Tag: Multiple BSSID Configuration
37822	59.207960	0.820347	Cisco_06:00:18	Broadcast	802.11	355	69 -38 dbm	Beacon frame, SW=2039, Fw=0, Flags=.....C, B=100, SSID=N	> Ext Tag: HE Capabilities
37833	59.208050	0.820398	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2040, Fw=0, Flags=.....C, B=100, SSID=N	> Ext Tag: HE Operation
37841	59.208540	0.820498	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2041, Fw=0, Flags=.....C, B=100, SSID=N	> Ext Tag: Spatial Reuse Parameter Set
37857	59.209090	0.820556	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2042, Fw=0, Flags=.....C, B=100, SSID=N	> Ext Tag: HE 4 GHz Band Capabilities
37864	08.013602	0.820460	Cisco_06:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2043, Fw=0, Flags=.....C, B=100, SSID=N	> Ext Tag: HE 4 GHz Band Capabilities
37868	08.013932	0.820508	Cisco_06:00:18	Broadcast	802.11	355	69 -38 dbm	Beacon frame, SW=2044, Fw=0, Flags=.....C, B=100, SSID=N	> Tag: Vendor Specific: Atheros Communications, Inc.: Unknown
37881	08.014049	0.820297	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2045, Fw=0, Flags=.....C, B=100, SSID=N	> Tag: Vendor Specific: Microsoft Corp.: WPA/WPA2 Parameter Element
37887	08.014787	0.820568	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2046, Fw=0, Flags=.....C, B=100, SSID=N	> Tag: Vendor Specific: Cisco Systems, Inc.: Airont Client MFP Disabled
37897	08.015006	0.820839	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2047, Fw=0, Flags=.....C, B=100, SSID=N	> Tag: Vendor Specific: Cisco Systems, Inc.: Airont CCK version = 5
37908	08.112976	0.820880	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2048, Fw=0, Flags=.....C, B=100, SSID=N	> Tag: Vendor Specific: Cisco Systems, Inc.: Airont Unknown (64)
37927	08.124244	0.820438	Cisco_06:00:18	Broadcast	802.11	355	69 -17 dbm	Beacon frame, SW=2049, Fw=0, Flags=.....C, B=100, SSID=N	> Tag: Vendor Specific: Cisco Systems, Inc.: Airont Unknown (11) (11)
37928	08.133867	0.820813	Cisco_06:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2050, Fw=0, Flags=.....C, B=100, SSID=N	
37936	08.173134	0.820267	Cisco_06:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2051, Fw=0, Flags=.....C, B=100, SSID=N	
37943	08.193778	0.820464	Cisco_06:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2052, Fw=0, Flags=.....C, B=100, SSID=N	
37949	08.124369	0.820993	Cisco_06:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2053, Fw=0, Flags=.....C, B=100, SSID=N	
37961	08.124873	0.820994	Cisco_06:00:18	Broadcast	802.11	355	69 -17 dbm	Beacon frame, SW=2054, Fw=0, Flags=.....C, B=100, SSID=N	

## WPA3 Enterprise SuiteB-1X Beacon

Aucun des clients testés n'a pu se connecter au WLAN à l'aide de SuiteB-1X, ce qui confirme qu'aucun d'entre eux ne prend en charge cette méthode de sécurité.

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

Configuration de la sécurité 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

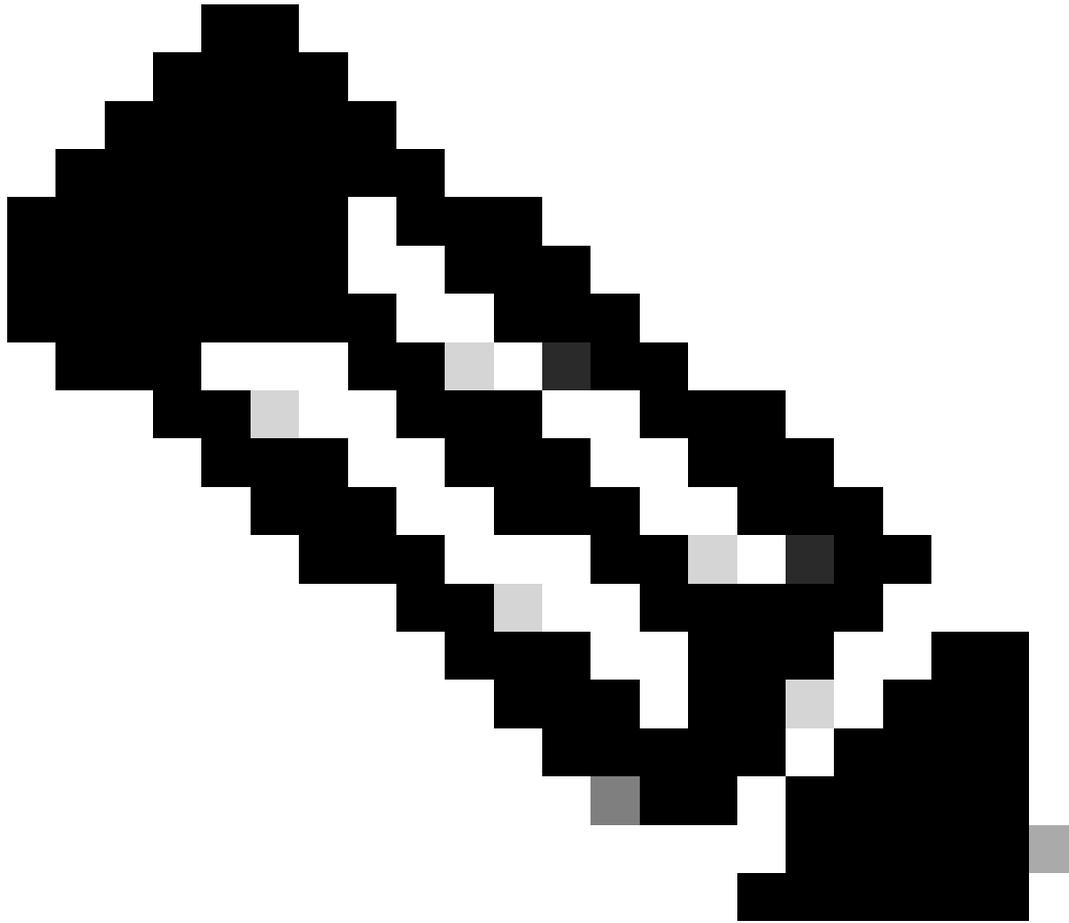
Auth Key Mgmt

SUITEB192-1X

Protected Management Frame

PMF   
Association Comeback Timer\*   
SA Query Time\*

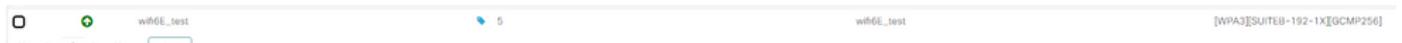
Paramètres de sécurité WPA3 Enterprise SUITEB192-1x



Remarque : FT n'est pas pris en charge avec GCMP256+SUITEB192-1X.

---

WLAN sur WLC GUI Liste des WLAN :



WLAN utilisé pour les tests

Vérification des balises OTA :

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal strength	BSS Id	Info
2	0.813335	0.000000	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
3	0.813784	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
4	0.814233	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
5	0.814682	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
6	0.815131	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
7	0.815580	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
8	0.816029	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
9	0.816478	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
10	0.816927	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
11	0.817376	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
12	0.817825	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
13	0.818274	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
14	0.818723	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
15	0.819172	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
16	0.819621	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
17	0.820070	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
18	0.820519	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
19	0.820968	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
20	0.821417	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
21	0.821866	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
22	0.822315	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
23	0.822764	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
24	0.823213	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
25	0.823662	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
26	0.824111	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
27	0.824560	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
28	0.825009	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
29	0.825458	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
30	0.825907	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
31	0.826356	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
32	0.826805	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
33	0.827254	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
34	0.827703	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
35	0.828152	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
36	0.828601	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
37	0.829050	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
38	0.829499	0.000449	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
39	0.830000	0.000501	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
40	0.830501	0.000501	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
41	0.831002	0.000501	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
42	0.831503	0.000501	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
43	0.832004	0.000501	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
44	0.832505	0.000501	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
45	0.833006	0.000501	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
46	0.833507	0.000501	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
47	0.834008	0.000501	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
48	0.834509	0.000501	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
49	0.835010	0.000501	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
50	0.835511	0.000501	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
51	0.836012	0.000501	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
52	0.836513	0.000501	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
53	0.837014	0.000501	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
54	0.837515	0.000501	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
55	0.838016	0.000501	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
56	0.838517	0.000501	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
57	0.839018	0.000501	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
58	0.839519	0.000501	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
59	0.840020	0.000501	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
60	0.840521	0.000501	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
61	0.841022	0.000501	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1
62	0.841523	0.000501	192.168.1.1	Broadcast	802.11	312	60	-48 dBm	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1	Probe Response, Src: 192.168.1.1, Dst: 192.168.1.1

```

} Frame 8: 255 bytes on wire (2040 bits), 255 bytes captured (2040 bits) on interface 'DeviceN'
} Ethernet II, Src: Cisco_C8130A2 (74:13:12:02:07:07), Dst: IntelAX210 (88:3c:2b:cf:86)
} Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.11
} User Datagram Protocol, Src Port: 5555, Dst Port: 5000
} Application/OSMpack encapsulated IEEE 802.11
} IEEE 802.11 radio information
} IEEE 802.11 Beacon frame, Flags: .....C
} IEEE 802.11 beacon management
} IEEE 802.11 beacon parameters (253 bytes)
  > Tag: SSB parameter set: "WiFiTest"
  > Tag: Supported Rates (0), S, 12.0M, 18, 24.0M, 36, 48, 54, [Mbit/sec]
  > Tag: Traffic Indication Map (TIM): 01M 0 of 3 Bitmap
  > Tag: Country Information: Country Code is, ISM:unrestricted operating classes
  > Tag: Power Constraint: 0
  > Tag: TX Report Transmit Power: 15, Link Manager: 0
} RSN Information
  > Tag: RSN Information (08)
  > Tag: Length: 26
  > RSN Version: 1
  > Group Cipher Suite: WPA2-PSK (See 802.11 GPP (256))
  > Pairwise Cipher Suite Count: 1
  > Pairwise Cipher Suite List: WPA2-PSK (See 802.11 GPP (256))
  > Auth Key Management (AKM) Suite Count: 1
  > Auth Key Management (AKM) Suite List: WPA2-PSK (See 802.11 GPP (256))
  > Auth Key Management (AKM) Suite: WPA2-PSK (See 802.11 GPP (256))
  > Auth Key Management (AKM) Suite: WPA2-PSK (See 802.11 GPP (256))
} RSN Capabilities: WPA2-PSK
  > Tag: RSN Pre-Auth capabilities: Transmitter can support pre-authentication
  > Tag: RSN No Pairwise capabilities: Transmitter can support WPA2-PSK default key if simultaneously with Pairwise key
  > Tag: RSN PSK Replay Counter capabilities: 4 replay counters per PTK/AKMP/SAK/GroupKey (0x1)
  > Tag: RSN Group Key Management capabilities: 4 replay counters per PTK/AKMP/SAK/GroupKey (0x1)
  > Tag: Management Frame Protection Request: True
  > Tag: Management Frame Protection Capable: True
  > Tag: TX Power Envelope
  > Tag: TX Power Envelope: Joint Multi-Band RSN: False
  > Tag: TX Power Envelope: Per-Channel: False
  > Tag: TX Power Envelope: Extended Key ID Per Individually Addressed Frames: Not supported
} WMM Information
  > Tag: WMM Information (08)
  > Tag: Length: 26
  > WMM Version: 1
  > Group Management Cipher Suite: WPA2-PSK (See 802.11 GPP (256))
  > Tag: QoS Control: WMM
  > Tag: WMM Capabilities: WMM
  > Tag: WMM Capabilities: WMM
  > Tag: WMM Capabilities: WMM
  > Tag:
```



À la date de rédaction de ce document, ce client n'était pas en mesure de se connecter à WPA3 Enterprise à l'aide d'EAP-TLS.

Il s'agissait d'un problème du côté du client sur lequel on travaille et, dès qu'il sera résolu, le présent document sera mis à jour.

### Conclusions sur la sécurité

Après tous les essais précédents, voici les conclusions qui en résultent :

Protocole	Chiffrement	AKM	Chiffrement AKM	Méthode EAP	FT-OverTA	FT-OverDS	Intel AX211	Samsung/Android
DEVOIR	AES-CCMP128	DEVOIR	S. O..	S. O..	S. O.	S. O.	Pris en charge	Pris en charge
SAE	AES-CCMP128	SAE (H2E uniquement)	SHA256	S. O..	Pris en charge	Pris en charge	Prise en charge : H2E uniquement et FT-oTA	Pris en charge H2E uniquement Échec de FT-oTA Échec de FT-OverDS.
Entreprise	AES-CCMP128	802.1x-SHA256	SHA256	PEAP/FAST/TLS	Pris en charge	Pris en charge	Prise en charge : SHA256 et FT-oTA/oDS Non pris en charge : EAP-FAST	Prise en charge : SHA256 et FT-oTA, FT-OverDS (S23) Non pris en charge : EAP-FAST (Pixel6a)
Entreprise	GCMP128	Suite B-1x	SHA256-SuiteB	PEAP/FAST/TLS	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge
Entreprise	GCMP256	Bureau B-192	SHA384-Suite B	TLS	Non pris en charge	Non pris en charge	NA/À déterminer	NA/À déterminer

# Dépannage

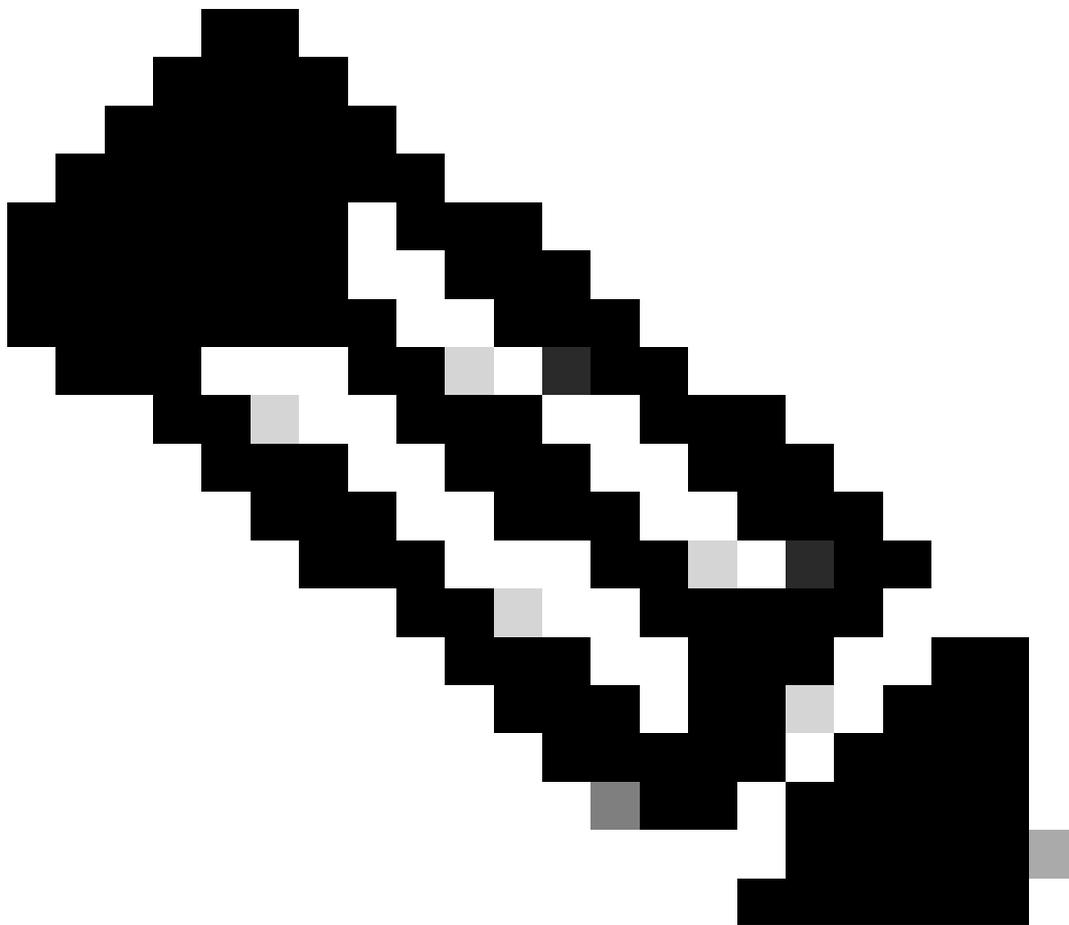
Le dépannage utilisé dans ce document est basé sur le document en ligne :

## [Dépannage des AP COS](#)

La ligne directrice générale pour le dépannage est de collecter la trace RA en mode de débogage à partir du WLC en utilisant l'adresse mac du client en s'assurant que le client se connecte en utilisant l'adresse mac du périphérique et non une adresse mac randomisée.

Pour le dépannage Over the Air, la recommandation est d'utiliser AP en mode sniffer capturant le trafic sur le canal du client desservant AP.

---



Remarque : reportez-vous à [Informations importantes sur les commandes de débogage](#) avant d'utiliser les commandes de débogage.

---

## Informations connexes

[Qu'est-ce que le Wi-Fi 6E ?](#)

[Qu'est-ce que le Wi-Fi 6 et le Wi-Fi 6E ?](#)

[Wi-Fi 6E en quelques mots](#)

[Wi-Fi 6E : le prochain grand chapitre du livre blanc sur le Wi-Fi](#)

[Cisco Live : concevoir un réseau sans fil de nouvelle génération avec des points d'accès Wi-Fi 6E Catalyst](#)

[Guide de configuration du logiciel du contrôleur sans fil Cisco Catalyst 9800 17.9.x](#)

[Guide de déploiement WPA3](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.