

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 :

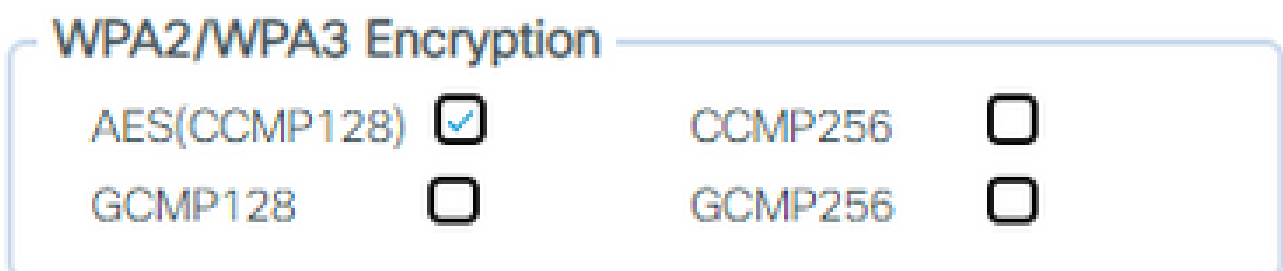
- La trame de gestion protégée (PMF) protège les trames de gestion de monodiffusion et de diffusion et chiffre les trames de gestion de monodiffusion. Cela signifie que les systèmes de détection et de prévention des intrusions sans fil disposent désormais de moins de moyens de force brute pour appliquer 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*

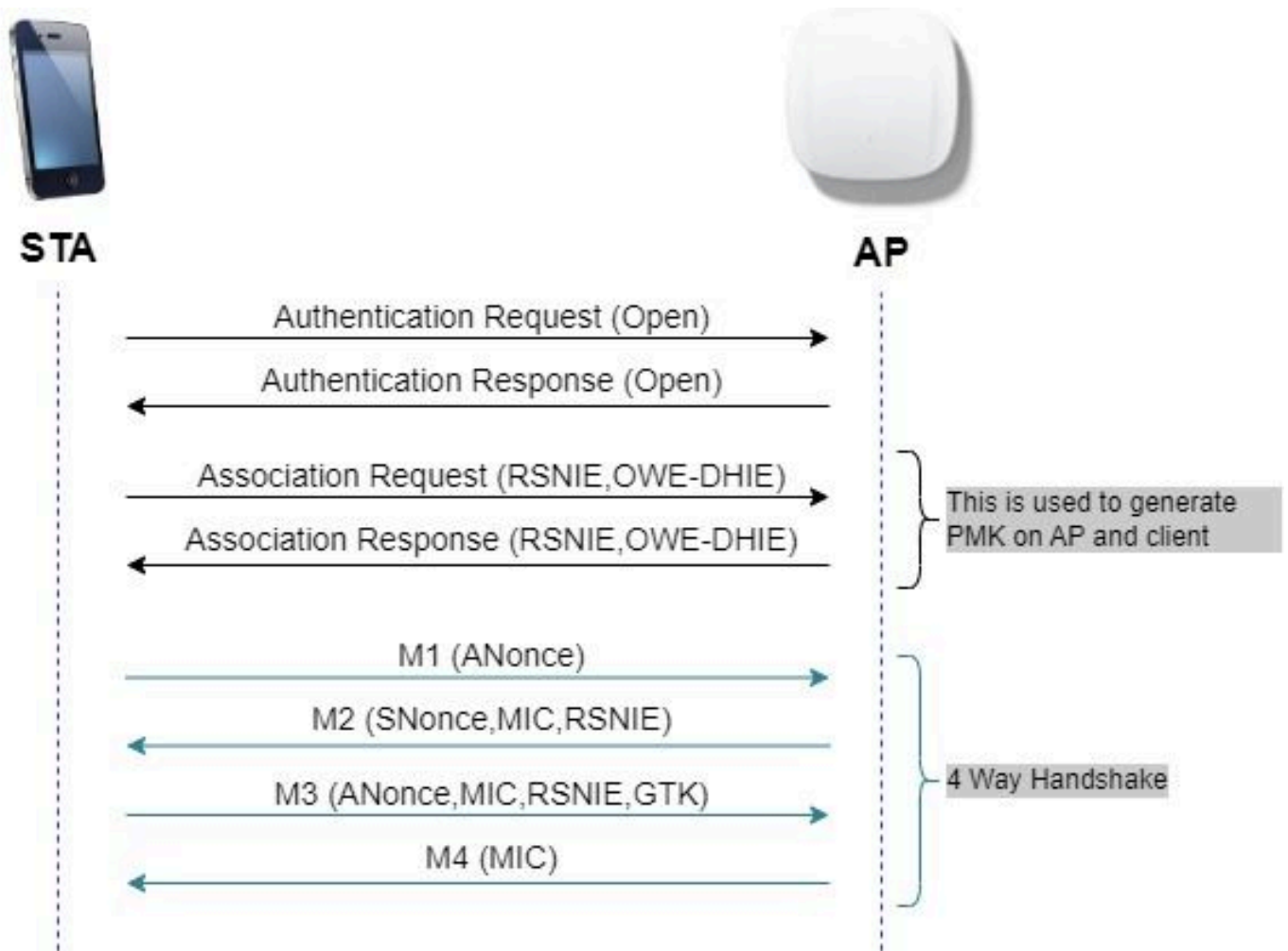
SAE Password Element ⓘ

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.

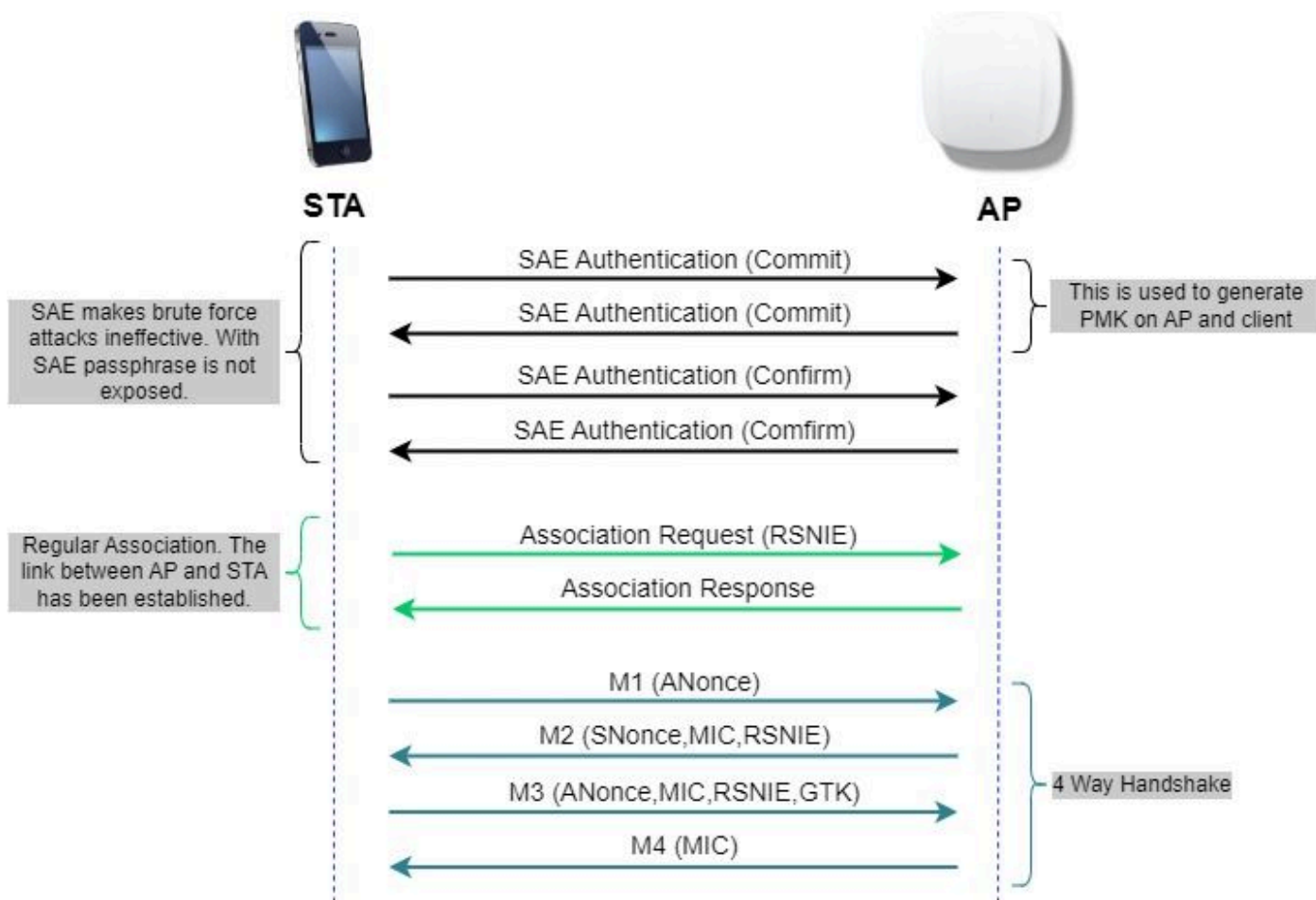
SAE utilise une cryptographie à logarithme discret pour effectuer un échange efficace d'une manière qui effectue une authentification mutuelle à l'aide d'un mot de passe qui est probablement résistant à une attaque de dictionnaire hors ligne.

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.

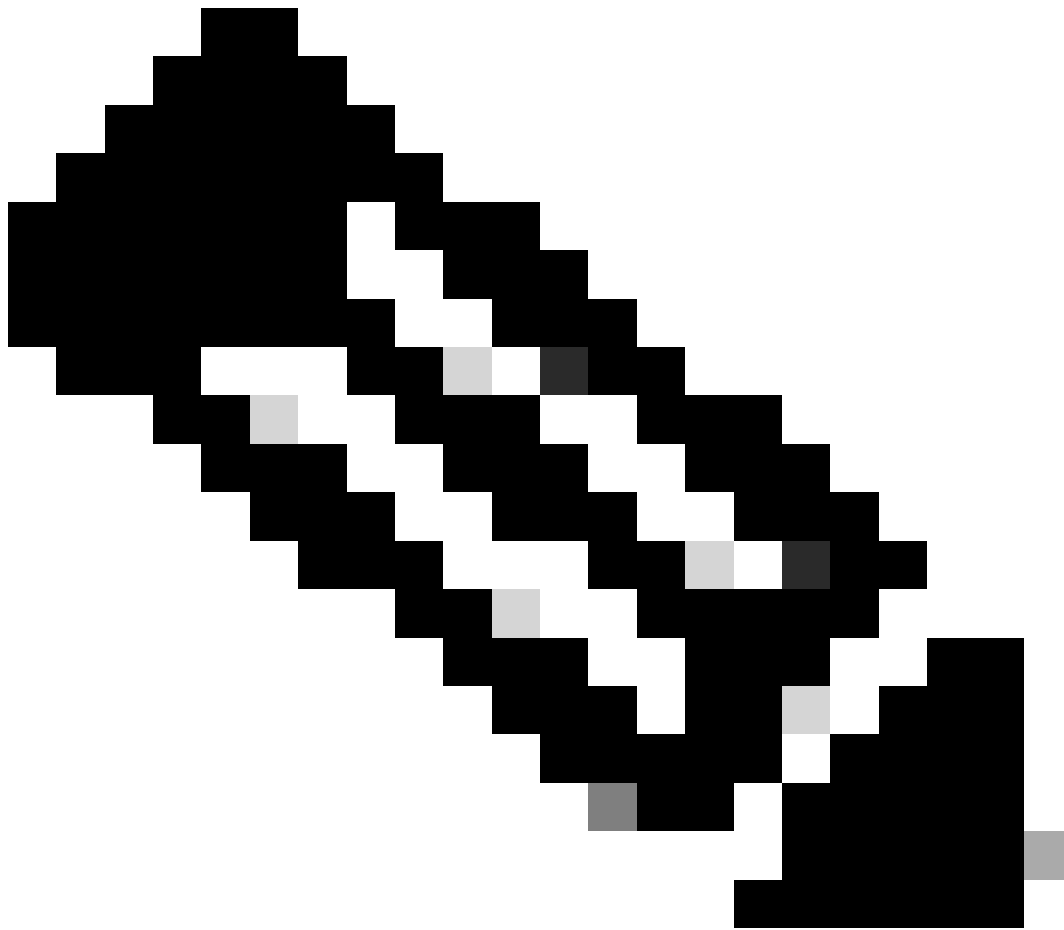
Lorsqu'une station (STA) qui prend en charge H2E lance SAE avec un point d'accès, elle vérifie si le point d'accès prend en charge H2E. Si oui, le point d'accès utilise H2E pour dériver le PWE en utilisant une valeur de code d'état nouvellement définie dans le message SAE Commit.

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.

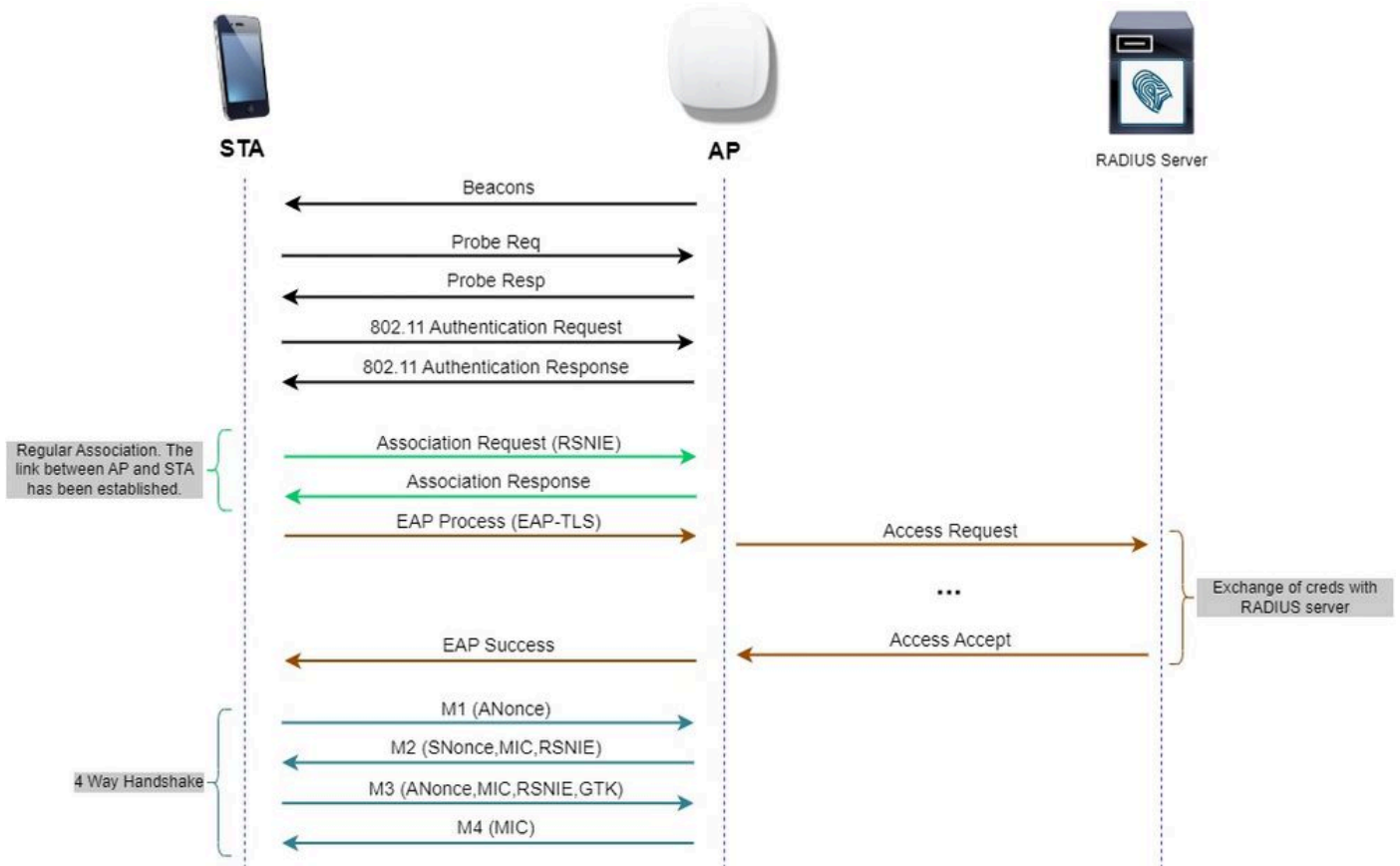
- Dérivation du PWE à partir du PT stocké. Cela dépend du groupe négocié et des adresses MAC des homologues. Cette opération est effectuée en temps réel lors de l'échange SAE.
-



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

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



WiFi



- 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, showing a 6 GHz band. The right-hand panel, 'Edit RF Profile', shows the configuration for the 802.11ax standard. It includes sections for 'General', 'RRM', and 'Advanced'. The '6 GHz Discovery Frames' section has radio buttons for 'None', 'Broadcast Probe Response' (selected), and 'FILS Discovery'. The 'Broadcast Probe Response Interval (msec)*' is set to 20. The 'Multi BSSID Profile' is set to 'MBSSIDprofile_test'. The 'Spatial Reuse' section has a 'DISABLED' button. The 'OBSS PD' section has a 'DISABLED' button. The 'Non-SRG OBSS PD Max Threshold (dBm)*' is set to -62. The 'SRG OBSS PD' section has a 'DISABLED' button. The 'SRG OBSS PD Min Threshold (dBm)*' is set to -82. The 'SRG OBSS PD Max Threshold (dBm)*' is set to -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 :

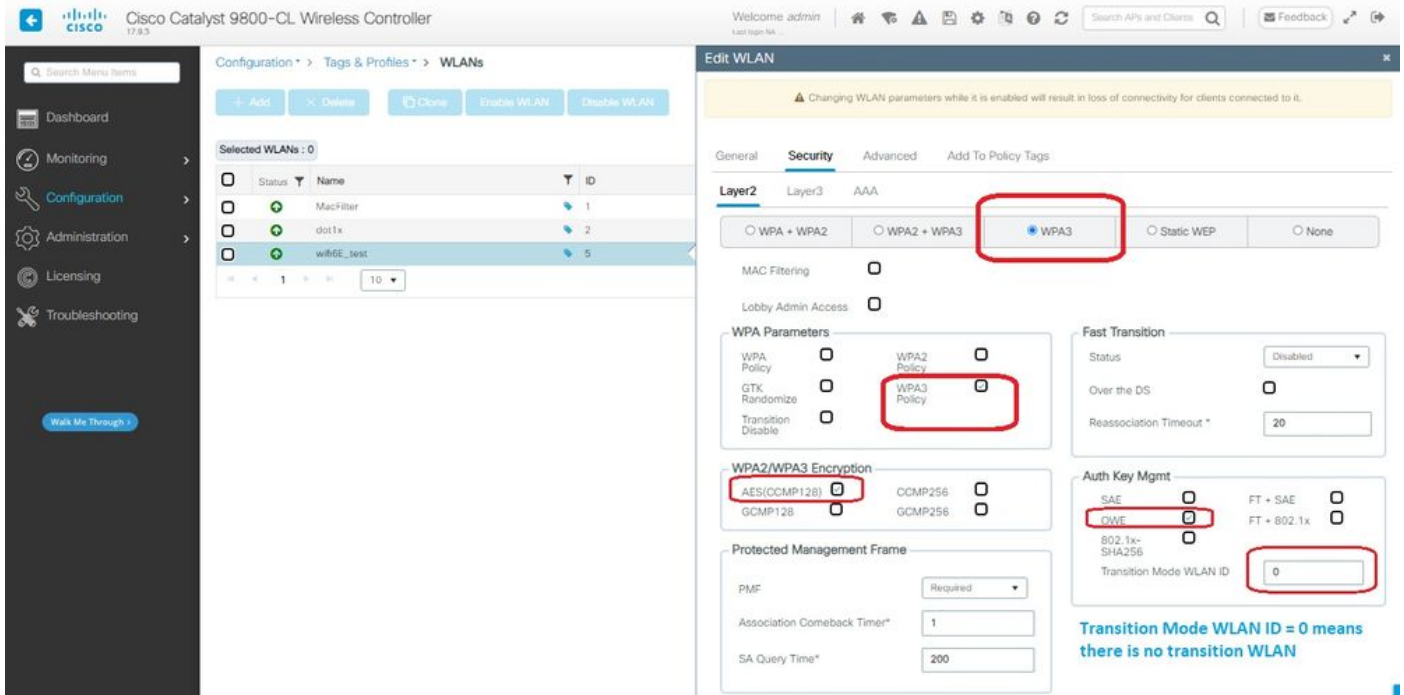
- WPA3- AES(CCMP128) + OWE
 - Mode de transition OWE
- WPA3 personnel
 - AES(CCMP128) + SAE
- WPA3-Entreprise
 - AES(CCMP128) + 802.1x-SHA256
 - AES(CCMP128) + 802.1x-SHA256 + FT
 - Chiffrement GCMP128 + SUITEB-1X
 - Chiffrement GCMP256 + SUITEB192-1X



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.

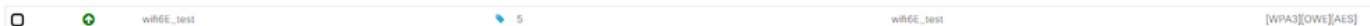
WPA3 - AES (CCPM128) + OWE

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

Session Manager

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_04578955-2398-445

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

IEEE 802.11 Wireless Management

- Fixed parameters (4 bytes)
- Tagged parameters (234 bytes)
 - Tag: SSID parameter set: "wifi168_test"
 - Tag: Supported rates (6), 9, 18(0), 24(0), 36, 48, 54, [Mbit/sec]
 - Tag: Power capability min, 9, max: 36
 - Tag: Supported Channels
 - Tag: RSN Information (48)
 - Tag length: 26
 - RSN Version: 1
 - Group Cipher Suite: 00f1fac (See 802.11 AES (CCM))
 - Pairwise Cipher Suite List: 00f1fac (See 802.11 AES (CCM))
 - Auth Key Management (AKM) Suite Count: 1
 - Auth Key Management (AKM) List: 00f1fac (See 802.11) Opportunistic Wireless Encryption
 - RSN Capabilities: 0x0000
 - PMKID Count: 0
 - PMKID List
 - Group Management Cipher Suite: 00f1fac (See 802.11) GMP (128)
 - Tag: M Enabled Capabilities (5 octets)
 - Tag Number: M Enabled Capabilities (20)
 - Tag length: 5
 - M Capabilities: 0x1 (octet 1)
 - ... 1.1 = Link Measurement: Enabled
 - ... 1.2 = Neighbor Report: Enabled
 - ... 1.3 = Parallel Measurements: Disabled
 - ... 1.4 = Reported Measurements: Disabled
 - ... 1.5 = Beacon Passive Measurement: Enabled
 - ... 1.6 = Beacon Active Measurement: Enabled
 - ... 1.7 = Beacon Traffic Measurement: Supported
 - ... 1.8 = Beacon Measurement Reporting Conditions: Disabled
 - M Capabilities: 0x0e (octet 2)
 - ... 1.1 = AP Channel Report capability: Enabled
 - ... 1.2 = M MHA capability: Disabled
 - ... 1.3 = Operating Channel Max Measurement Duration: 4
 - ... 1.4 = Nonoperating Channel Max Measurement Duration: 4
 - M Capabilities: 0x0e (octet 4)
 - M Capabilities: 0x0e (octet 5)
 - Tag: Supported Operating Classes
 - Tag: Extended Capabilities (11 octets)
 - Ext Tag: HE Capabilities
 - Ext Tag: HE 6 GHz Band Capabilities
 - Ext Tag: OWE Diffie-Hellman Parameter
 - Tag: Vendor Specific: Qualcomm Inc.
 - Tag: Vendor Specific: Samsung Electronics Co., Ltd
 - Tag: Vendor Specific: Samsung Electronics Co., Ltd

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

Session Manager

WPA3 - AES (CCPM128) + 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"/>		

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*

Fast Transition

Status

Over the DS

Reassociation Timeout*

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	Extra Info
5	2023-06-12 17:12:24.459118	0.00000	0.00000 Cisco, 13:80:0E	0.00000 Cisco, 13:80:0E	Broadcast	002.11	402	-3.36 dBm	Probe Response, Shw713, Fwub, Flags.....C, B1=800, SSID="WiFi6_Test_02", SSID	<pre> Frame 6: 508 bytes on wire (4064 bits), 508 bytes captured (4064 bits) on interface Vdevicetap_04578995-2998-4464-4 Ethernet II, Src: Cisco_00:07:0A:70:10:37, Dst: Univers_01:00:0C:00:00:00 (08:00:0C:00:00:00) Internet Protocol version 4, Src: 192.168.1.11, Dst: 192.168.1.11 User Datagram Protocol, Src Port: 5555, Dst Port: 5000 Airrotek/OnMPeek encapsulated IEEE 802.11 IEEE 802.11 radio information IEEE 802.11 Beacon frame, Flags:</pre>
6	2023-06-12 17:12:24.731872	0.00293	0.00293 Cisco, 13:80:0E	0.00000 Cisco, 13:80:0E	Broadcast	002.11	508	-3.37 dBm	Beacon frame, Shw728, Fwub, Flags.....C, B1=800, SSID="WiFi6_Test_02", SSID	<pre> Airrotek/OnMPeek encapsulated IEEE 802.11 IEEE 802.11 wireless management Fixed parameters (10 bytes) Tagged parameters (406 bytes) Tag: SSI parameter set "WiFi6_Test_02" Tag: Supported rates (S, S, I, R): 18, 24, 36, 48, 54, [Mbit/sec] Tag: Traffic Indication Map (TIM): OTSDF 2 of 3 Bitmap Tag: Country information: Country code no, Environment global operating classes Tag: Power Constraint 0 Tag: TPC Report Transm Power: 17, LNK Margin: 0 Tag: RSN information Tag number: RSN information (48) RSN Version: 1 Group Cipher Suite: 000f:ac (IEEE 802.11) AES (CCM) Pairwise Cipher Suite Count: 1 Pairwise Cipher Suite: 000f:ac (IEEE 802.11) AES (CCM) Auth Key Management (AKM) Suite Count: 1 Auth Key Management (AKM) Suite: 000f:ac (IEEE 802.11) SAE (SHA256) RSN Capabilities: 000000 PMKID Count: 0 PMKID List Group Management Cipher Suite: 000f:ac (IEEE 802.11) GCM (128) Tag: QSS Load Element 0001:cc (Cisco version) Tag: Multiple SSID Tag: AM Enabled Capabilities (5 octets) Tag: Extended Capabilities (11 octets) Tag: TX Power Envelope Tag: TX Power Envelope Ext Tag: Multiple BSSID Configuration Ext Tag: HE Capabilities Ext Tag: HE Operation Ext Tag: Spatial Reuse Parameter Set Ext Tag: MU-EDCA Parameter Set Ext Tag: HE EHT Band Capabilities Ext Tag: HE EHT Band Capabilities Tag: RSN extension (1 octet) Tag Number: RSN extension (244) RSN: 0x20 (oct 1) 0000 = RSN Length: 0 0 = Protected TWT Operations Support: 0 SAE Mesh to Element: 1 Tag: Vendor Specific: Atheros Communications, Inc.: Unknown Tag: Vendor Specific: Microsoft Corp.: WPA/WPA2: Parameter Element Tag: Vendor Specific: Cisco Systems, Inc.: Airontet Unknown (44) Tag: Vendor Specific: Cisco Systems, Inc.: Airontet Unknown (11) (11) Tag: Vendor Specific: Cisco Systems, Inc.: Airontet Cisco IWF Disabled Tag: Vendor Specific: Cisco Systems, Inc.: Airontet CCM version = 5</pre>

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	Extra Info
2235	2023-06-12 17:13:00.328183	0.00000	192.168.1.121	192.168.1.121	IPsec	168	121	-4.07 dBm	Probe Request, Shw389, Fwub, Flags.....C, SSID="Widocard (Broadcast)	<pre> Frame 1235: 194 bytes on wire (1552 bits), 194 bytes captured (1552 bits) on interface Vdevicetap_04578995-2998-4464-4 Ethernet II, Src: Cisco_00:07:0A:70:10:37, Dst: Univers_01:00:0C:00:00:00 (08:00:0C:00:00:00) Internet Protocol version 4, Src: 192.168.1.121, Dst: 192.168.1.121 User Datagram Protocol, Src Port: 5555, Dst Port: 5000 Airrotek/OnMPeek encapsulated IEEE 802.11 IEEE 802.11 authentication, Flags:</pre>
130	2023-06-12 17:13:32.260609	0.00778	192.168.1.121	192.168.1.121	IPsec	194	121	-4.45 dBm	Authentication, Shw9, Fwub, Flags.....C	<pre> Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (3) Authentication SAE: 0x0001 Status code: SAE authentication success SAE Message Type: Commit (1) Group ID: 254-01 random ECP Group (19) Scalar: c0b385c9e79701cafc0b9a57c4c7998d01d481a188d8b245312 Finite Field Element: 58c775a9b76d629b212ec725ed6a622a855267866a8eac6d31c70994.</pre>

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 the selected frame being an IEEE 802.11 Association Request. The packet details pane on the right shows the structure of the RSN (Robust Security Network) information, including the RSN Version, Group Cipher Suite, Pairwise Cipher Suite List, Auth Key Management, and RSN Capabilities. The RSN Capabilities field is expanded to show supported operations and reserved bits.

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. The Security Information tab is active, displaying the same client details as in the first screenshot, 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 17:37:02.739033	0.000000	Google_7218a:66	Cisco_31180:	Broadcast	802.11	343	-42 dBm	Probe Request, S/W:2096, P/W:0, Flags:.....C, SSID:"wifi6_test"
1243	2023-06-12 17:37:02.855631	0.121238	Google_7218a:66	Cisco_31180:	Authentication	802.11	194	-42 dBm	Authentication, S/W:2097, P/W:0, Flags:.....C
1244	2023-06-12 17:37:02.855631	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags:.....C	
1246	2023-06-12 17:37:02.859394	0.007353	Cisco_31180:e7	Google_7218a:66	802.11	194	-37 dBm	Authentication, S/W:14, P/W:0, Flags:.....C	
1247	2023-06-12 17:37:02.859394	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags:.....C	
1248	2023-06-12 17:37:02.868831	0.009447	Google_7218a:66	Cisco_31180:	802.11	198	-41 dBm	Authentication, S/W:2096, P/W:0, Flags:.....C	
1249	2023-06-12 17:37:02.868831	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags:.....C	
1252	2023-06-12 17:37:02.904326	0.035495	Cisco_31180:e7	Google_7218a:66	802.11	198	-37 dBm	Authentication, S/W:14, P/W:0, Flags:.....C	
1253	2023-06-12 17:37:02.904326	0.000000	192.168.1.15	192.168.1.121	802.11	76	-41 dBm	Acknowledgment, Flags:.....C	
1255	2023-06-12 17:37:02.929933	0.016467	Google_7218a:66	Cisco_31180:	802.11	262	-41 dBm	Association Request, S/W:2099, P/W:0, Flags:.....C, SSID:"wifi6_test"	
1256	2023-06-12 17:37:02.929933	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags:.....C	
1259	2023-06-12 17:37:02.930808	0.000937	Google_7218a:66	Cisco_31180:	802.11	76	-37 dBm	I, P, N(1)>N(1); SSAP Basic Individual, SSAP Basic Command	
1261	2023-06-12 17:37:02.934129	0.003737	Cisco_31180:e7	Google_7218a:66	802.11	262	-37 dBm	Association Response, S/W:0, P/W:0, Flags:.....C	
1262	2023-06-12 17:37:02.934129	0.000000	192.168.1.15	192.168.1.121	802.11	76	-41 dBm	Acknowledgment, Flags:.....C	
1263	2023-06-12 17:37:02.934129	0.000000	Google_7218a:66	Broadcast	LLC	134	-37 dBm	S, P, Func=ity, N(1)>N(2); SSAP Basic Group, SSAP Basic Response	
1265	2023-06-12 17:37:02.943892	0.009663	Cisco_31180:e7	Google_7218a:66	EAPOL	223	-37 dBm	Key (message 1 of 4)	
1266	2023-06-12 17:37:02.943892	0.000000	192.168.1.15	192.168.1.121	802.11	76	-41 dBm	Acknowledgment, Flags:.....C	
1273	2023-06-12 17:37:02.992247	0.051155	Google_7218a:66	Cisco_31180:	EAPOL	238	-51 dBm	Key (message 2 of 4)	
1274	2023-06-12 17:37:02.992247	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags:.....C	
1275	2023-06-12 17:37:02.995369	0.003122	Cisco_31180:e7	Google_7218a:66	EAPOL	295	-37 dBm	Key (message 3 of 4)	
1276	2023-06-12 17:37:02.995369	0.000000	192.168.1.15	192.168.1.121	802.11	76	-51 dBm	Acknowledgment, Flags:.....C	
1278	2023-06-12 17:37:03.000159	0.004790	Google_7218a:66	Cisco_31180:	EAPOL	199	-48 dBm	Key (message 4 of 4)	
1279	2023-06-12 17:37:03.000159	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags:.....C	
1281	2023-06-12 17:37:03.021799	0.021231	192.168.1.15	192.168.1.121	802.11	76	-46 dBm	Acknowledgment, Flags:.....C	
1282	2023-06-12 17:37:03.025924	0.002534	Google_7218a:66	Cisco_31180:	802.11	122	-49 dBm	Action, S/W:180, P/W:0, Flags:.....C (Malformed Packet)	
1283	2023-06-12 17:37:03.025924	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags:.....C	
1284	2023-06-12 17:37:03.040493	0.017809	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags:.....C	
1286	2023-06-12 17:37:03.046766	0.007753	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags:.....C	
1290	2023-06-12 17:37:03.078167	0.027481	Cisco_31180:e7	Google_7218a:66	802.11	124	-37 dBm	Action, S/W:1, P/W:0, Flags:.....C	
1291	2023-06-12 17:37:03.078167	0.000000	192.168.1.15	192.168.1.121	802.11	76	-49 dBm	Acknowledgment, Flags:.....C	
1297	2023-06-12 17:37:03.166223	0.088956	Google_7218a:66	Cisco_31180:	802.11	115	-48 dBm	Action, S/W:180, P/W:0, Flags:.....C	
1298	2023-06-12 17:37:03.166223	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags:.....C	
1299	2023-06-12 17:37:03.166229	0.000076	Google_7218a:66	IPV6cast_vf, LLC	227	-37 dBm	U, P, Func=ID; SSAP Basic Group, SSAP Basic Command		
1300	2023-06-12 17:37:03.166229	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags:.....C	
1302	2023-06-12 17:37:03.167999	0.001780	Google_7218a:66	Cisco_31180:	802.11	115	-37 dBm	Action, S/W:1, P/W:0, Flags:.....C (Malformed Packet)	
1303	2023-06-12 17:37:03.167999	0.000000	192.168.1.15	192.168.1.121	802.11	76	-49 dBm	Acknowledgment, Flags:.....C	
1304	2023-06-12 17:37:03.168236	0.000000	192.168.1.15	192.168.1.121	802.11	82	-49 dBm	802.11 Block Ack Req, Flags:.....C	
1305	2023-06-12 17:37:03.168236	0.000000	192.168.1.15	192.168.1.121	802.11	94	-37 dBm	802.11 Block Ack, Flags:.....C	
1306	2023-06-12 17:37:03.168543	0.000477	Google_7218a:66	IPV6cast_vf, LLC	186	-38 dBm	I, P, N(1)>N(1); SSAP Basic Individual, SSAP Basic Response		
1307	2023-06-12 17:37:03.177442	0.000000	192.168.1.15	192.168.1.121	802.11	82	-49 dBm	Request-to-send, Flags:.....C	
1308	2023-06-12 17:37:03.177442	0.000000	192.168.1.15	192.168.1.121	802.11	76	-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); SSAP 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: 192.168.1.15, Dst: 192.168.1.121
> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
> AiroPeek/MiniPeek encapsulated IEEE 802.11
> IEEE 802.11 radio information
> IEEE 802.11 Authentication, Flags: .....C
  > fixed parameters (4 bytes)
  > Tagged parameters (168 bytes)
    > Tag: SSID parameter Set: "wifi6_test"
    > Tag: Supported rates (0), 9, 12.0, 18, 24.0, 36, 48, 54, [Mbit/sec]
    > Tag: Extended Supported Rates Set: hash to element only, [Mbit/sec]
    > Tag: Power Capability Min: -7, Max: 19
    > Tag: Supported Channels
  > Tag: SSN Information
    > Tag Number: SSN Information (48)
    > Tag Length: 26
    > RSN Version: 1
    > Group Cipher Suite: 00:fac (See IEEE 802.11) AES (CCM)
    > Pairwise Cipher Suite Count: 1
    > Pairwise Cipher Suite List: 00:fac (See IEEE 802.11) AES (CCM)
    > Auth Key Management (AKM) Suite Count: 1
    > Auth Key Management (AKM) List: 00:fac (See IEEE 802.11) SAE (SHA256)
    > RSN Capabilities: 00000
    > PMKID Count: 0
    > PMKID List
    > Group Management Cipher Suite: 00:fac (See IEEE 802.11) BIP (128)
  > Tag: WMM enabled capabilities (5 octets)
  > Tag: Supported Operating Classes
  > Tag: Extended Capabilities (18 octets)
  > Ext Tag: HE Capabilities
  > Tag: RSN extension (1 octet)
  > Tag Number: RSN extension (244)
  > Tag Length: 1
  > RSN: 0000 (octet 1)
    > ..... 0000 = RSN length: 0
    > ..... 0000 = Protected TWT Operation Support: 0
    > ..... 0000 = Reserved: 000
    > ..... 0000 = SAE hash to element: 1
  > Ext Tag: HE 4 oct Band Capabilities
  > Tag: Vendor Specific: Broadcom
  > Tag: Vendor Specific: Microsoft Corp.: WPA/WPAE: Information Element
  
```

Détails du client dans le WLC :

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The main area displays a list of clients under the 'Monitoring > Wireless > Clients' section. One client is selected, and its details are shown in a sidebar on the right.

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

The detailed view on the right shows the following information for the selected client:

- Client State Servers:** None
- Client ACLs:** None
- Client Entry Create Time:** 83 seconds
- Policy Type:** WPA3
- Encryption Cipher:** CCMP (AES)
- Authentication Key Management:** SAE
- EAP Type:** Not Applicable
- Session Timeout:** 86400
- Session Manager:**
 - Point of Attachment: capwap_90000010
 - IF ID: 0x90000010
 - Authorized: TRUE
 - Common Session ID: 000000000000FB50AED363
 - Acct Session ID: 0x00000000
 - Auth Method Status List: SAE
 - Method: SAE

Samsung S23

Connexion OTA avec accent sur les informations RSN du client :

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
773	2023-06-12 17:26:55.727215	0.000000	Samsung_C9:8371	Cisco_31180:	Broadcast	802.11	194	-45 dBm	Authentication, S/W:2176, P/W:0, Flags:.....C
774	2023-06-12 17:26:55.727215	0.000000	192.168.1.15	192.168.1.121	802.11	76	-38 dBm	Acknowledgment, Flags:.....C	
775	2023-06-12 17:26:55.734513	0.000038	Cisco_31180:e7	Samsung_C9:8371	802.11	194	-37 dBm	Authentication, S/W:2176, P/W:0, Flags:.....C	
776	2023-06-12 17:26:55.734513	0.000000	192.168.1.15	192.168.1.121	802.11	76	-45 dBm	Acknowledgment, Flags:.....C	
777	2023-06-12 17:26:55.742809	0.000036	Samsung_C9:8371	Cisco_31180:	802.11	198	-43 dBm	Authentication, S/W:2177, P/W:0, Flags:.....C	
778	2023-06-12 17:26:55.742809	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags:.....C	
780	2023-06-12 17:26:55.743197	0.000228	Cisco_31180:e7	Samsung_C9:8371	802.11	198	-36 dBm	Authentication, S/W:2177, P/W:0, Flags:.....C	
781	2023-06-12 17:26:55.743197	0.000000	192.168.1.15	192.168.1.121	802.11	76	-43 dBm	Acknowledgment, Flags:.....C	
782	2023-06-12 17:26:55.748041	0.004544	Samsung_C9:8371	Cisco_31180:	802.11	354	-45 dBm	Association Request, S/W:2178, P/W:0, Flags:.....C, SSID:"wifi6_test"	
783	2023-06-12 17:26:55.748041	0.000000	192.168.1.15	192.168.1.121	802.11	76	-36 dBm	Acknowledgment, Flags:.....C	
787	2023-06-12 17:26:55.758131	0.010275	Samsung_C9:8371	Broadcast	LLC	114	-37 dBm	I, N(1)>N(1); SSAP 130 Network Layer (unofficial) Group, SSAP Banyan View	
788	2023-06-12 17:26:55.758131	0.000000	Samsung_C9:8371	Broadcast	LLC	114	-36 dBm	S, P, Func=ty, N(1)>N(4); SSAP HP GetPrinter Individual, SSAP MS Response	
789	2023-06-12 17:26:55.763192	0.002476	Cisco_31180:e7	Samsung_C9:8371	802.11	236	-36 dBm	Association Response, S/W:0, P/W:0, Flags:.....C	
790	2023-06-12 17:26:55.763192	0.000000	192.168.1.15	192.168.1.121	802.11	76	-44 dBm	Acknowledgment, Flags:.....C	
792	2023-06-12 17:26:55.762296	0.001184	Cisco_31180:e7	Samsung_C9:8371	EAPOL	223	-36 dBm	Key (message 1 of 4)	
793	2023-06-12 17:26:55.762296	0.000000	192.168.1.15	192.168.1.121	802.11	76	-44 dBm	Acknowledgment, Flags:.....C	
795	2023-06-12 17:26:55.791219	0.028283	Samsung_C9:8371	Cisco_31180:	EAPOL	238	-43 dBm	Key (message 2 of 4)	
796	2023-06-12 17:26:55.791219	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags:.....C	
797	2023-06-12 17:26:55.793800	0.001781	Cisco_31180:e7	Samsung_C9:8371	EAPOL	295	-37 dBm	Key (message 3 of 4)	
798	2023-06-12 17:26:55.793800	0.000000	192.168.1.15	192.168.1.121	802.11	76	-44 dBm	Acknowledgment, Flags:.....C	
799	2023-06-12 17:26:55.798403	0.005483	Samsung_C9:8371	Cisco_31180:	EAPOL	199	-44 dBm	Key (message 4 of 4)	

Détails du client dans le WLC :

Cisco Catalyst 9800-CL Wireless Controller 17.9.3

Welcome admin

Search APs and Clients

Feedback

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Delete

Selected 0 out of 12 Clients

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

Client

360 View General QoS Statistics ATF Statistics Mobility History Call Statistics

Client Properties AP Properties Security Information Client Statistics QoS Properties EoGRE

Client State Servers None

Client ACLs None

Client Entry Create Time 78 seconds

Policy Type WPA3

Encryption Cipher CCMP (AES)

Authentication Key Management SAE

EAP Type Not Applicable

Session Timeout 86400

Session Manager

Point of Attachment capwap_90000010

IF ID 0x90000010

Authorized TRUE

Common Session ID 000000000000FB1B0A58F78

Acct Session ID 0x00000000

Auth Method Status List

Method SAE

WPA3 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

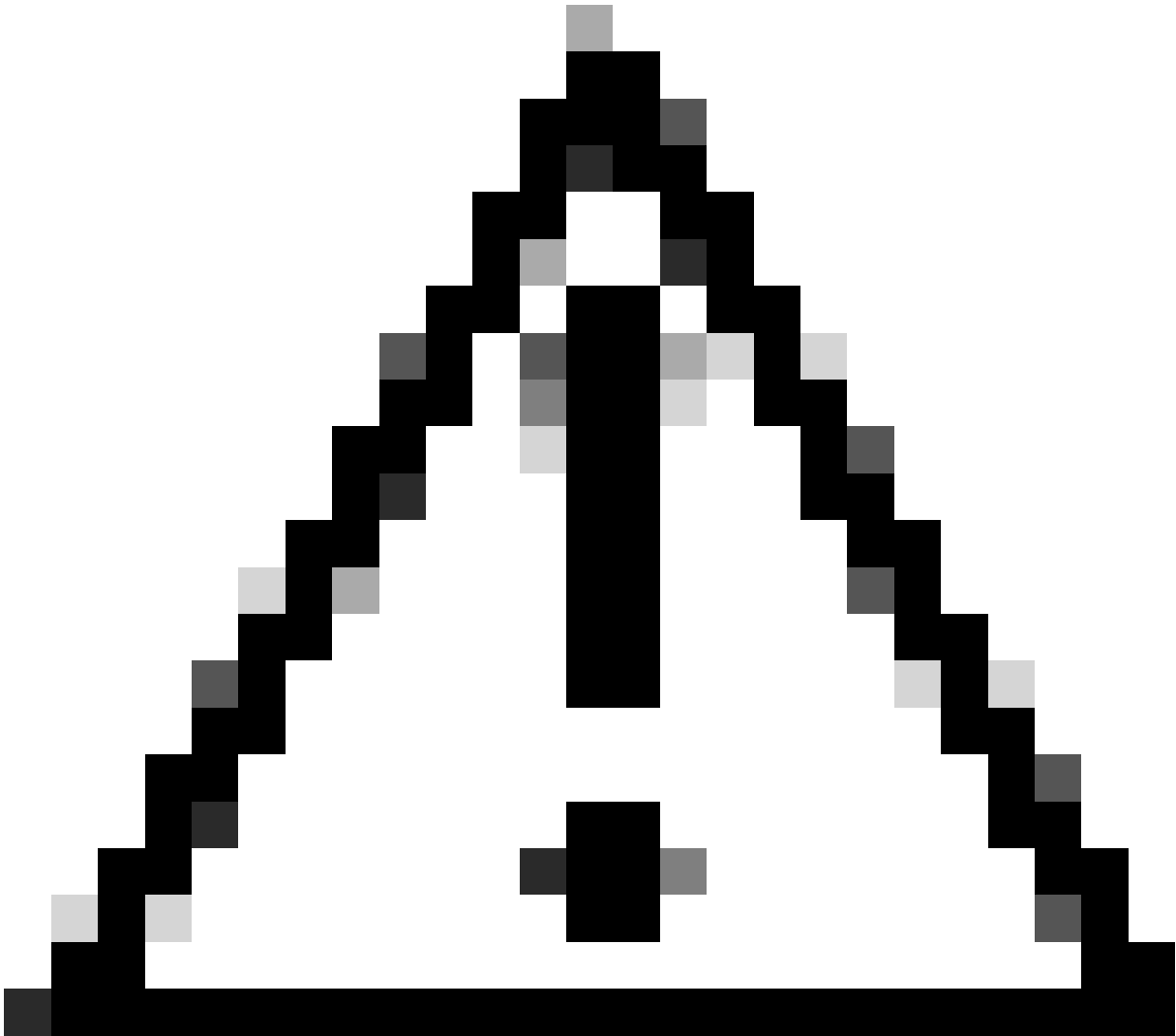
AES(OCMP128) CCMP256
 GCMP128 GCMP256

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 ⓘ ▾

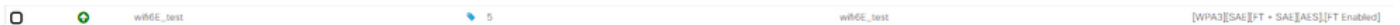
Protected Management Frame

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 :



Vérification des balises OTA :

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
1	2023-06-12 18:34:49.285337	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="wifi6e_test"
2	2023-06-12 18:34:49.427544	0.182287	Cisco_13:180:e7	Eurocast	802.11	588	5	-36 dBm	Beacon frame, S/W=27, F/W=, Flags=.....C, B=100, SSID="wifi6e_test"
3	2023-06-12 18:34:49.558567	0.182287	Cisco_13:180:e7	Eurocast	802.11	588	5	-37 dBm	Beacon frame, S/W=27, F/W=, Flags=.....C, B=100, SSID="wifi6e_test"
4	2023-06-12 18:34:49.623332	0.182465	Cisco_13:180:e7	Eurocast	802.11	588	5	-37 dBm	Beacon frame, S/W=27, F/W=, Flags=.....C, B=100, SSID="wifi6e_test"
5	2023-06-12 18:34:49.791804	0.099872	Netgear_48:78:95	Cisco_13:180:e7	802.11	360	5	-49 dBm	Probe Request, S/W=8, F/W=, Flags=.....C, SSID="wifi6e_test"
6	2023-06-12 18:34:49.791804	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-37 dBm	Acknowledgment, Flags=.....C
7	2023-06-12 18:34:49.791356	0.000152	Netgear_48:78:95	Cisco_13:180:e7	802.11	360	5	-49 dBm	Probe Request, S/W=1, F/W=, Flags=.....C, SSID="wifi6e_test"
8	2023-06-12 18:34:49.791427	0.000071	192.168.1.15	192.168.1.121	802.11	76	5	-37 dBm	Acknowledgment, Flags=.....C
9	2023-06-12 18:34:49.794933	0.003066	Cisco_13:180:e7	Eurocast	802.11	588	5	-37 dBm	Beacon frame, S/W=27, F/W=, Flags=.....C, B=100, SSID="wifi6e_test"
10	2023-06-12 18:34:49.812822	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="wifi6e_test"
11	2023-06-12 18:34:49.812822	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-37 dBm	Acknowledgment, Flags=.....C
12	2023-06-12 18:34:49.874951	0.000049	Netgear_48:78:95	Cisco_13:180:e7	802.11	194	5	-49 dBm	Authentication, S/W=8, F/W=, Flags=.....C
13	2023-06-12 18:34:49.874951	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-37 dBm	Acknowledgment, Flags=.....C
14	2023-06-12 18:34:49.896563	0.021812	Cisco_13:180:e7	Netgear_48:78:95	802.11	194	5	-37 dBm	Authentication, S/W=8, F/W=, Flags=.....C
15	2023-06-12 18:34:49.896563	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-49 dBm	Acknowledgment, Flags=.....C
16	2023-06-12 18:34:49.904966	0.000043	Cisco_13:180:e7	Eurocast	802.11	588	5	-37 dBm	Beacon frame, S/W=27, F/W=, Flags=.....C, B=100, SSID="wifi6e_test"
17	2023-06-12 18:34:49.904966	0.000000	Netgear_48:78:95	Cisco_13:180:e7	802.11	130	5	-49 dBm	Authentication, S/W=8, F/W=, Flags=.....C
18	2023-06-12 18:34:49.904966	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-37 dBm	Acknowledgment, Flags=.....C
19	2023-06-12 18:34:49.904966	0.000000	Netgear_48:78:95	Netgear_48:78:95	802.11	130	5	-37 dBm	Authentication, S/W=8, F/W=, Flags=.....C
20	2023-06-12 18:34:49.904966	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-48 dBm	Acknowledgment, Flags=.....C
21	2023-06-12 18:34:49.904966	0.000000	Netgear_48:78:95	Cisco_13:180:e7	802.11	216	5	-49 dBm	Association Request, S/W=8, F/W=, Flags=.....C, SSID="wifi6e_test"
22	2023-06-12 18:34:49.904966	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
23	2023-06-12 18:34:49.911474	0.005188	Cisco_13:180:e7	Netgear_48:78:95	802.11	262	5	-36 dBm	Association Response, S/W=8, F/W=, Flags=.....C
24	2023-06-12 18:34:49.911474	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-49 dBm	Acknowledgment, Flags=.....C
25	2023-06-12 18:34:49.911719	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 18:34:49.911719	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 18:34:49.922346	0.010267	Cisco_13:180:e7	Netgear_48:78:95	EAPOL	221	5	-36 dBm	Key Message 1 of 4
28	2023-06-12 18:34:49.922346	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-49 dBm	Acknowledgment, Flags=.....C
29	2023-06-12 18:34:49.999581	0.077235	Cisco_13:180:e7	Eurocast	802.11	588	5	-36 dBm	Beacon frame, S/W=27, F/W=, Flags=.....C, B=100, SSID="wifi6e_test"
30	2023-06-12 18:34:50.104510	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="wifi6e_test"
31	2023-06-12 18:34:50.204600	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="wifi6e_test"
32	2023-06-12 18:34:50.211615	0.007815	Netgear_48:78:95	Cisco_13:180:e7	EAPOL	226	5	-55 dBm	Key Message 2 of 4
33	2023-06-12 18:34:50.211615	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-42 dBm	Acknowledgment, Flags=.....C
34	2023-06-12 18:34:50.211615	0.000000	Netgear_48:78:95	Eurocast	EAPOL	298	5	-49 dBm	Key Message 3 of 4
35	2023-06-12 18:34:50.211376	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-58 dBm	Acknowledgment, Flags=.....C
36	2023-06-12 18:34:50.214354	0.000978	Netgear_48:78:95	Cisco_13:180:e7	EAPOL	199	5	-56 dBm	Key Message 4 of 4
37	2023-06-12 18:34:50.222346	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-42 dBm	Acknowledgment, Flags=.....C
38	2023-06-12 18:34:50.222712	0.006367	192.168.1.15	192.168.1.121	802.11	76	5	-42 dBm	Acknowledgment, Flags=.....C
39	2023-06-12 18:34:50.224849	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 18:34:50.224849	0.000000	Netgear_48:78:95	Netgear_48:78:95	LLC	221	5	-44 dBm	U, func:unknown; DSAP 0x02 Group, SSAP 0x02 Response
41	2023-06-12 18:34:50.224849	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 18:51:39.249793	0.007137	IntelCor_98:53:8f	Cisco_13:180:e7	802.11	194	5	-42 dBm	Authentication, S/W=8, F/W=, Flags=.....C
1812	2023-06-12 18:51:39.249793	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_98:53:8f	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_98:53:8f	Cisco_13:180:e7	802.11	130	5	-40 dBm	Authentication, S/W=1, F/W=, Flags=.....C
1816	2023-06-12 18:51:39.259394	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1817	2023-06-12 18:51:39.261879	0.004235	Cisco_13:180:e7	IntelCor_98:53:8f	802.11	130	5	-36 dBm	Authentication, S/W=8, F/W=, Flags=.....C
1818	2023-06-12 18:51:39.261879	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-42 dBm	Acknowledgment, Flags=.....C
1819	2023-06-12 18:51:39.261879	0.000000	IntelCor_98:53:8f	Cisco_13:180:e7	802.11	250	5	-46 dBm	Association Request, S/W=8, F/W=, Flags=.....C, SSID="wifi6e_test"
1820	2023-06-12 18:51:39.261879	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_98:53:8f	Broadcast	LLC	114	5	-36 dBm	I, H(K)=, H(S)=; DSAP 0x02 Group, SSAP 0x02 Response
1827	2023-06-12 18:51:39.271442	0.000000	IntelCor_98:53:8f	Broadcast	LLC	114	5	-36 dBm	I, H(K)=, H(S)=; DSAP 0x02 Group, SSAP 0x02 Response
1828	2023-06-12 18:51:39.277402	0.001268	Cisco_13:180:e7	IntelCor_98:53:8f	802.11	262	5	-36 dBm	Association Response, S/W=8, 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 18:51:39.281817	0.003795	Cisco_13:180:e7	Broadcast	802.11	517	5	-36 dBm	Beacon frame, S/W=71, F/W=, Flags=.....C, B=100, SSID="wifi6e_test"
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 18:51:39.333425	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	Broadcast	802.11	517	5	-37 dBm	Beacon frame, S/W=76, F/W=, Flags=.....C, B=100, SSID="wifi6e_test"
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 18:51:39.399382	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 18:51:39.399382	0.000330	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 18:51:39.402835	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 18:51:39.402835	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1851	2023-06-12 18:51:39.402835	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 18:51:39.406367	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 18:51:39.406367	0.000844	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1857	2023-06-12 18:51:39.407244	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_98:53:8f	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_98:53:8f	Cisco_13:180:e7	EAPOL	230	5	-56 dBm	Key Message 2 of 4
1863	2023-06-12 18:51:39.428712	0.000000							

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 status bar at the bottom of the Cisco Catalyst 9800-CL Wireless Controller interface. It displays the WLAN name 'wif6E_test' and its ID '5'. The security configuration is shown as '[WPA3][FT + 802.1x][AES][PMF 802.1x][FT Enabled]'. The 'FT Enabled' part is highlighted in blue.

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 :

Flux de connexion WPA3 Enterprise 802.1x + FT Ax211

Détails du client dans le WLC :

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 :

Association WPA3 Enterprise 802.1x + FT Pixel6a

Détails du client dans le WLC :

Détails sur le client WPA3 Enterprise 802.1x + FT Pixel6a

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 :

AP Name	BSSID	AP Slot	Assoc Time	Instance	Mobility Role	Run Latency (ms)	Room Type
AP01_RC_9136_F80C	00d1.10d3.a018	3	07/12/2023 11:46:16	0	Local	7	802.11R
AP9136_Sc-F524	00d1.10d3.7a38	3	07/12/2023 11:43:48	0	Local	3161	N/A

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	0.182133	Cisco_d5:80:18	Broadcast	802.11	364	69 -39 dBm		Beacon frame, SN=385, FH=0, Flags=.....C, BI=100, SSID="wif
1247	8.481935	0.182170	Cisco_d5:80:18	Broadcast	802.11	364	69 -40 dBm		Beacon frame, SN=386, FH=0, Flags=.....C, BI=100, SSID="wif
1248	8.584375	0.102420	Cisco_d5:80:18	Broadcast	802.11	364	69 -39 dBm		Beacon frame, SN=387, FH=0, Flags=.....C, BI=100, SSID="wif
1249	8.686824	0.102419	Cisco_d5:80:18	Broadcast	802.11	364	69 -40 dBm		Beacon frame, SN=388, FH=0, Flags=.....C, BI=100, SSID="wif
1251	8.612759	0.089585	Cisco_d5:80:18	Broadcast	802.11	312	69 -40 dBm		Probe Response, SN=459, FH=0, Flags=.....C, BI=100, SSID="w
1258	8.701133	0.096374	Cisco_d5:80:18	Broadcast	802.11	364	69 -39 dBm		Beacon frame, SN=318, FH=0, Flags=.....C, BI=100, SSID="wif
1260	8.786432	0.077279	Samsung_c9:e3:71	Cisco_d5:80:18	802.11	235	69 -48 dBm		Authentication, SN=99, FH=0, Flags=.....C
1261	8.786432	0.000000	192.168.1.15	192.168.1.122	802.11	76	69 -39 dBm		Acknowledgment, Flags=.....C
1262	8.790571	0.004159	Cisco_d5:80:18	Samsung_c9:e3:71	802.11	247	69 -39 dBm		Authentication, SN=118, FH=0, Flags=.....C
1263	8.790571	0.000000	192.168.1.15	192.168.1.122	802.11	76	69 -47 dBm		Acknowledgment, Flags=.....C
1265	8.796439	0.005868	Samsung_c9:e3:71	Cisco_d5:80:18	802.11	485	69 -48 dBm		Association Request, SN=100, FH=0, Flags=.....C, SSID="wif
1266	8.796439	0.000000	192.168.1.15	192.168.1.122	802.11	76	69 -39 dBm		Acknowledgment, Flags=.....C
1268	8.808749	0.006939	Samsung_c9:e3:71	Broadcast	LLC	114	69 -39 dBm		S, Func=03, N(5)=19; DSAP 0x0a Group, SSAP 0x0a Command
1269	8.807940	0.001362	Cisco_d5:80:18	Samsung_c9:e3:71	802.11	413	69 -39 dBm		Association Response, SN=0, FH=0, Flags=.....C
1270	8.807940	0.000000	192.168.1.15	192.168.1.122	802.11	76	69 -48 dBm		Acknowledgment, Flags=.....C
1271	8.807940	0.000000	Samsung_c9:e3:71	Broadcast	LLC	120	69 -39 dBm		I, P, N(5)=11, N(5)=19; DSAP 0x08 Individual, SSAP 0x0a Respons
1272	8.813151	0.001581	Cisco_d5:80:18	Broadcast	802.11	364	69 -39 dBm		Beacon frame, SN=311, FH=0, Flags=.....C, BI=100, SSID="wif
1273	8.832754	0.021313	Cisco_Sc:F8:0c	Samsung_c9:e3:71	LLC	183	69 -40 dBm		U, Func=01C1; 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		Acknowledgment, Flags=.....C
1275	8.832754	0.000000	Cisco_Sc:F8:0c	Samsung_c9:e3:71	LLC	183	69 -49 dBm		U, Func=Unknown; DSAP Texas Instruments Group, SSAP 0x28 Respo
1276	8.832817	0.000063	192.168.1.15	192.168.1.122	802.11	76	69 -58 dBm		Acknowledgment, Flags=.....C
1277	8.808540	0.007723	Samsung_c9:e3:71	Broadcast	LLC	144	69 -46 dBm		S, P, Func=0E2, N(0)=32; DSAP 0x0a Individual, SSAP 0x0a Respon
1278	8.808540	0.000000	192.168.1.15	192.168.1.122	802.11	76	69 -40 dBm		Acknowledgment, Flags=.....C
1280	8.984143	0.003063	Cisco_d5:80:18	Samsung_c9:e3:71	802.11	118	69 -40 dBm		Action, SN=1, FH=0, Flags=p.....C
1281	8.984143	0.000000	192.168.1.15	192.168.1.122	802.11	76	69 -47 dBm		Acknowledgment, Flags=.....C
1282	8.984083	0.000660	Samsung_c9:e3:71	Cisco_d5:80:18	802.11	115	69 -47 dBm		Action, SN=0, FH=0, Flags=p.....C
1283	8.984083	0.000000	192.168.1.15	192.168.1.122	802.11	76	69 -40 dBm		Acknowledgment, Flags=.....C
1284	8.986878	0.002075	Altiocel_a3:59:af	Samsung_c9:e3:71	LLC	197	69 -50 dBm		I, P, N(7)=25, N(5)=48; DSAP 0x0a Individual, SSAP 0x0a Command
1286	8.913932	0.007034	Cisco_d5:80:18	Broadcast	802.11	364	69 -41 dBm		Beacon frame, SN=313, FH=0, Flags=.....C, BI=100, SSID="wif
1287	8.958493	0.036581	Cisco_d5:80:18	Broadcast	802.11	364	69 -39 dBm		Acknowledgment, Flags=.....C
1322	9.375553	0.029808	192.168.1.15	192.168.1.122	802.11	76	69 -39 dBm		Acknowledgment, Flags=.....C
1372	9.851519	0.049566	Cisco_d5:80:18	Broadcast	802.11	364	69 -38 dBm		Beacon frame, SN=314, FH=0, Flags=.....C, BI=100, SSID="wif
1471	9.181683	0.102164	Cisco_d5:80:18	Broadcast	802.11	364	69 -39 dBm		Beacon frame, SN=315, FH=0, Flags=.....C, BI=100, SSID="wif
1600	9.176834	0.058111	192.168.1.15	192.168.1.122	802.11	76	69 -40 dBm		Acknowledgment, Flags=.....C
1702	9.221145	0.044131	Cisco_d5:80:18	Broadcast	802.11	364	69 -39 dBm		Beacon frame, SN=316, FH=0, Flags=.....C, BI=100, SSID="wif
1933	9.124387	0.102962	Cisco_d5:80:18	Broadcast	802.11	364	69 -39 dBm		Beacon frame, SN=317, FH=0, Flags=.....C, BI=100, SSID="wif
1937	9.425938	0.104511	Cisco_d5:80:18	Broadcast	802.11	364	69 -40 dBm		Beacon frame, SN=318, FH=0, Flags=.....C, BI=100, SSID="wif
1939	9.528463	0.102525	Cisco_d5:80:18	Broadcast	802.11	364	69 -38 dBm		Beacon frame, SN=319, FH=0, Flags=.....C, BI=100, SSID="wif
1945	9.631020	0.102557	Cisco_d5:80:18	Broadcast	802.11	364	69 -38 dBm		Beacon frame, SN=320, FH=0, Flags=.....C, BI=100, SSID="wif
1946	9.733295	0.102275	Cisco_d5:80:18	Broadcast	802.11	364	69 -39 dBm		Beacon frame, SN=321, FH=0, Flags=.....C, BI=100, SSID="wif
1950	9.835864	0.102569	Cisco_d5:80:18	Broadcast	802.11	364	69 -40 dBm		Beacon frame, SN=322, FH=0, Flags=.....C, BI=100, SSID="wif
1951	9.825936	0.008072	Samsung_c9:e3:71	Cisco_d5:80:18	802.11	122	69 -45 dBm		Action, SN=4, FH=0, Flags=p.....C
1952	9.825936	0.000000	192.168.1.15	192.168.1.122	802.11	76	69 -40 dBm		Acknowledgment, Flags=.....C
1953	9.826893	0.000957	192.168.1.15	192.168.1.122	802.11	76	69 -40 dBm		Acknowledgment, Flags=.....C
1954	9.817895	0.013082	Cisco_d5:80:18	Broadcast	802.11	364	69 -40 dBm		Beacon frame, SN=323, FH=0, Flags=.....C, BI=100, SSID="wif
1955	9.842343	0.006448	192.168.1.15	192.168.1.122	802.11	76	69 -40 dBm		Acknowledgment, Flags=.....C

```
> Frame 1265: 485 bytes on wire (3880 bits), 485 bytes captured (3880 bits) on interface Device\WIFI_04578095-2
> Ethernet II, Src: Cisco_G2:97:47 (74:11:b2:97:47), Dst: Universa_07:cf:06 (08:0a:88:b7: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
> AloTpkw/OmIpkw encapsulated IEEE 802.11
> IEEE 802.11 radio information
> IEEE 802.11 Association Request, Flags: .....C
> IEEE 802.11 Mgmt Management
> Fixed parameters (10 bytes)
> Tagged parameters (185 bytes)
> Tag: SSID parameter set: "wif66_test"
> Tag: Supported Rates A(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
> Tag: Power Capability Mtn: 8, Max: 16
> Tag: Supported Channels
> Tag: RM Enabled Capabilities (5 octets)
> Tag: SM Information
> Tag: Mobility Domain
  Tag Number: Mobility Domain (54)
  Tag Length: 3
  Mobility Domain Identifier: 0x027
  FT Capability and Policy: 0x01
    .....0 = Fast BSS Transition over DS: 0x1
    .....0 = Resource Request Protocol Capability: 0x0
    0x00 0x00 = Reserved: 0x00
> Tag: Fast BSS Transition
  Tag Number: Fast BSS Transition (55)
  Tag Length: 96
  MDC Control: 0x0000
  MDC: 0xF104F7F4E16ad6ecf658a51a5aca
  Address: d514f17ab7fa085b76775e1b6d6a9822fac58fbc7492e11089f01a869ca
  Status: 0x122a455778a118c7ef6124215978079d0c9ef9a12283f566d682b2c3
  Subelement: PMK-R1 key holder Identifier (R104-ID) (1)
    Length: 6
    PMK-R1 key holder Identifier (R104-ID): d6807b097ad0
  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 (11 octets)
> Ext Tag: Vendor-Specific: Microsoft Corp.: WMM/NAI: 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"/>		

Fast Transition

Status

Over the DS

Reassociation Timeout *

WPA2/WPA3 Encryption

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

Auth Key Mgmt

SUITEB-1X

Protected Management Frame

PMF

Association Comeback Timer*

SA Query Time*

WPA3 Enterprise SuiteB-1X 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 :

⚠ 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 :

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-oDS.
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-oDS (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

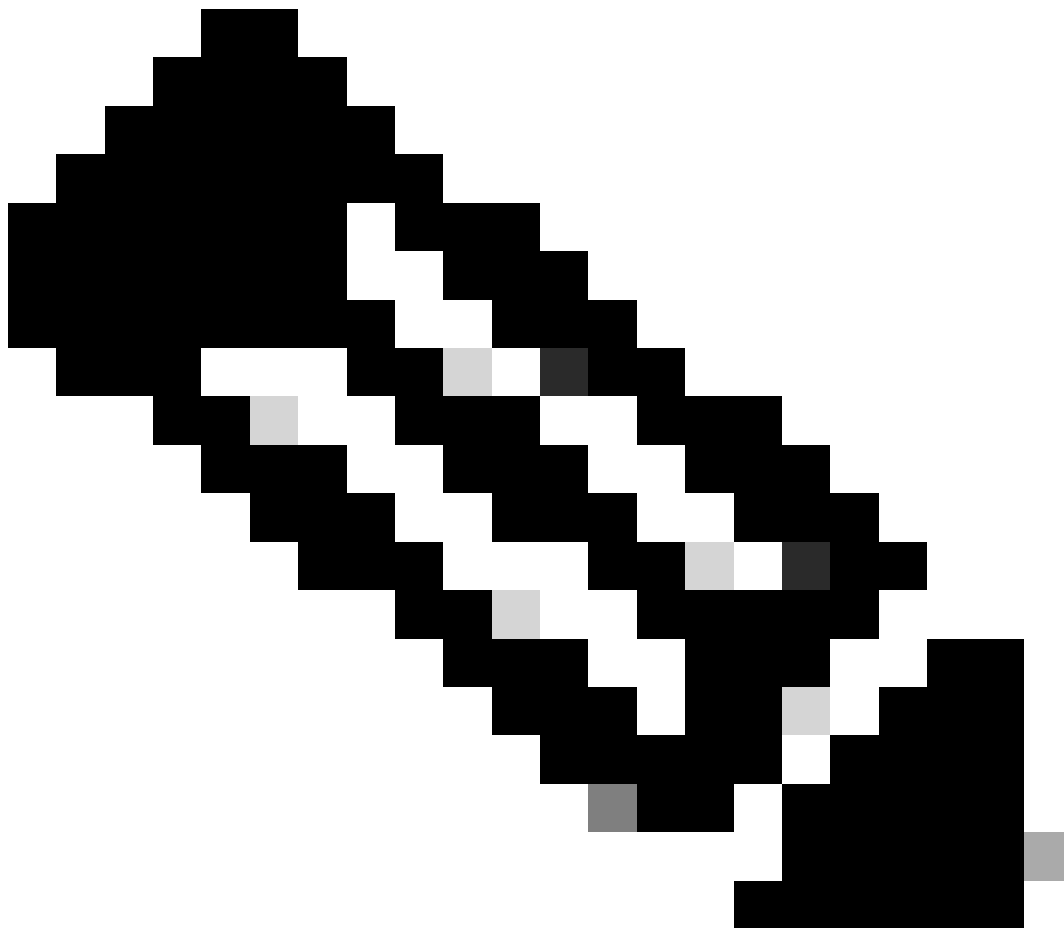
Dépannage

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.