

Wi-Fi 6E WLAN Layer 2-beveiliging configureren en controleren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Wi-Fi 6E security](#)

[WPA3](#)

[Niveau ingesteld: WPA3-modi](#)

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

[Door clients ondersteunde beveiligingsinstellingen](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Basisconfiguratie](#)

[Verifiëren](#)

[Beveiligingsverificatie](#)

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

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

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

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

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

[WPA3-Enterprise + GCMP128-algoritme + SUBITB-1X](#)

[WPA3-Enterprise + GCMP256-algoritme + SITEB192-1X](#)

[conclusies inzake beveiliging](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u Wi-Fi 6E WLAN Layer 2-beveiliging kunt configureren en wat u op verschillende clients kunt verwachten.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco draadloze LAN-controllers (WLC) 9800
- Cisco Access points (AP's) die Wi-Fi 6E ondersteunen.
- IEEE-standaard 802.11ax.
- Tools: Wireshark v4.0.6

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- WLC 9800-CL met IOS® XE 17.9.3
- AP9136, CW9162, CW9164 en CW9166.
- Wi-Fi 6E-clients:
 - Lenovo X1 Carbon Gen11 met Intel AX211 Wi-Fi 6 en 6E adapter met driver versie 22.200.2(1).
 - Netgear A8000 Wi-Fi 6- en 6E-adapter met stuurprogramma v1(0.0.108);
 - Mobiele telefoon Pixel 6a met Android 13;
 - Mobiele telefoon Samsung S23 met Android 13.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Het belangrijkste om te weten is dat Wi-Fi 6E geen geheel nieuwe standaard is, maar een uitbreiding. Op de basis is Wi-Fi 6E een uitbreiding van de Wi-Fi 6 (802.11ax) draadloze standaard in de 6-GHz radiofrequentieband.

Wi-Fi 6E bouwt voort op Wi-Fi 6, de nieuwste generatie van de Wi-Fi standaard, maar alleen Wi-Fi 6E apparaten en toepassingen kunnen werken in de 6-GHz band.

Wi-Fi 6E security

Wi-Fi 6E verhoogt de beveiliging met Wi-Fi Protected Access 3 (WPA3) en Opportunistische Draadloze Encryptie (OWE) en er is geen achterwaartse compatibiliteit met Open en WPA2-beveiliging.

WPA3 en Enhanced Open Security zijn nu verplicht voor Wi-Fi 6E-certificering en Wi-Fi 6E vereist ook Protected Management Frame (PMF) in zowel AP als Clients.

Bij het configureren van een 6GHz SSID zijn er bepaalde beveiligingsvereisten waaraan moet worden voldaan:

- WPA3 L2-beveiliging met WAE, SAE of 802.1x-SHA256
- Beschermd beheerframe ingeschakeld;
- Een andere L2-beveiligingsmethode is niet toegestaan, dat wil zeggen geen gemengde

modus mogelijk.

WPA3

WPA3 is ontworpen om de Wi-Fi-beveiliging te verbeteren door betere verificatie via WPA2 mogelijk te maken, en uitgebreide cryptografische kracht te bieden en de veerkracht van kritieke netwerken te vergroten.

De belangrijkste kenmerken van WPA3 zijn:

- Protected Management Frame (PMF) beschermt unicast- en broadcast-beheerframes en versleutelt unicast-beheerframes. Dit betekent dat draadloze inbraakdetectie en draadloze inbraakpreventiesysteem-sneeuw minder brute-kracht manieren hebben om clientbeleid af te dwingen.
- Gelijktijdige verificatie van equals (SAE) maakt wachtwoordgebaseerde verificatie en een sleutelovereenkomstmechanisme mogelijk. Dit beschermt tegen grof geweld aanvallen.
- Overgangsmodus is een gemengde modus die het gebruik van WPA2 mogelijk maakt om clients te verbinden die geen WPA3 ondersteunen.

WPA3 gaat over continue security ontwikkeling en conformantie en interoperabiliteit.

Er is geen informatie-element dat WPA3 aanwijst (hetzelfde als WPA2). WPA3 is gedefinieerd door AKM/Cypher Suite/PMF combinaties.

Op de 9800 WLAN-configuratie hebt u vier verschillende WPA3-coderingsalgoritmen die u kunt gebruiken.

Ze zijn gebaseerd op het Galois/Counter Mode Protocol (GCMP) en de Counter Mode met Cycle Block Chaining Message Authenticatie Protocol (CCMP): AES (CCMP128), CCMP256, GCMP128 en GCMP256:

WPA2/WPA3 Encryption

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

WAP2/3-versleutelingsopties

PMF

PMF wordt geactiveerd op een WLAN wanneer u PMF inschakelt.

Standaard zijn 802.11-beheerframes niet geverifieerd en dus niet beschermd tegen spoofing. Infrastructure Management Protection Frame (MFP) en 802.11w protected management frames (PMF) bieden bescherming tegen dergelijke aanvallen.

Protected Management Frame

PMF

Required



Association Comeback Timer*

1

SA Query Time*

200

PMF-opties

Beheer van verificatiesleutels

Dit zijn de AKM-opties die beschikbaar zijn in de 17.9.x-versie:

Auth Key Mgmt

SAE FT + SAE

OWE FT + 802.1x

802.1x-
SHA256

Anti Clogging Threshold*

Max Retries*

Retransmit Timeout*

PSK Format

PSK Type

Pre-Shared Key*

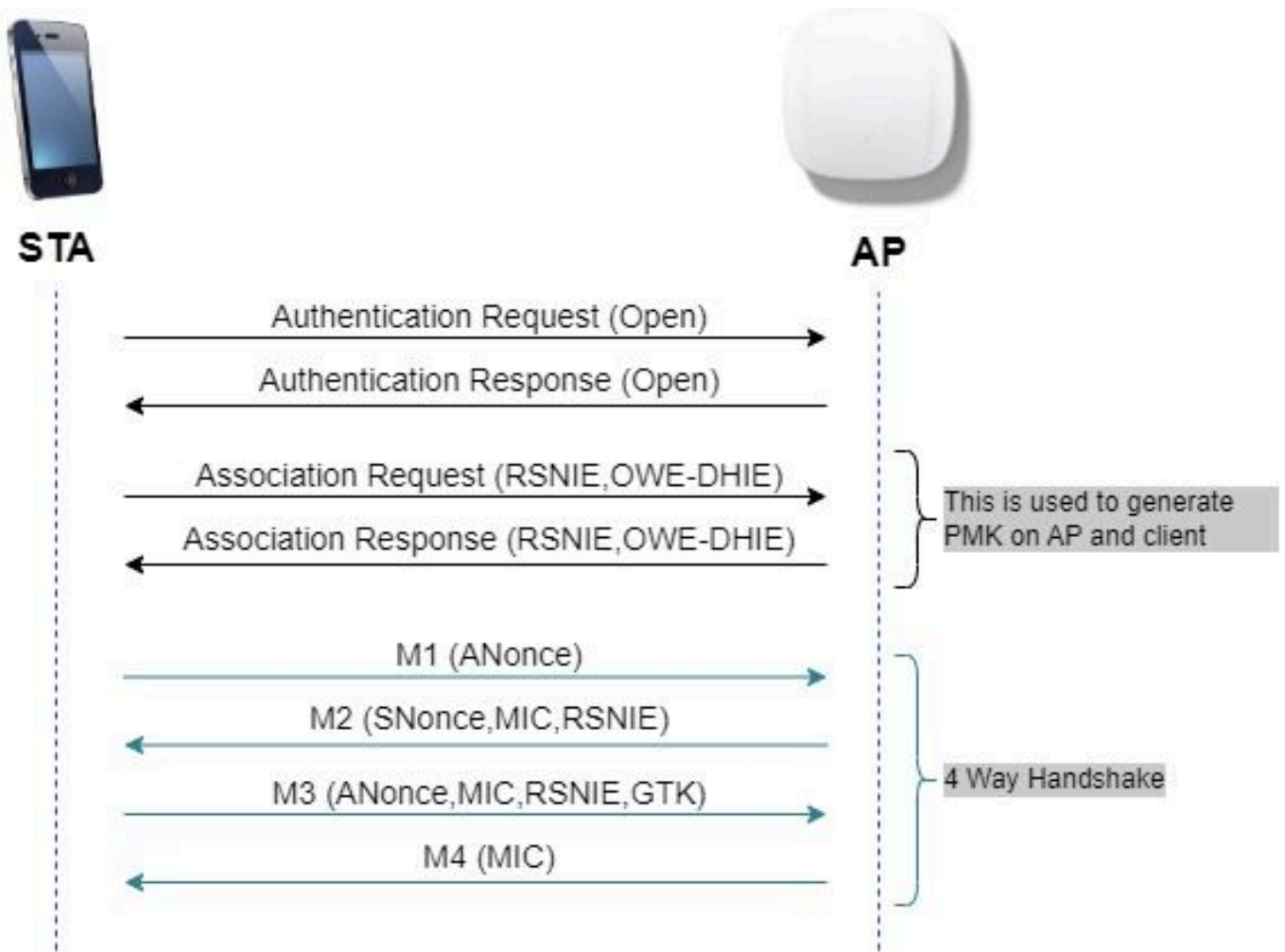
SAE Password Element ⓘ

AKM-opties

VERSCHULDIGD

Opportunistische draadloze encryptie (OWE) is een uitbreiding van IEEE 802.11 die codering van het draadloze medium biedt ([IETF RFC 8110](#)). Het doel van op OWE gebaseerde verificatie is het vermijden van open onbeveiligde draadloze connectiviteit tussen de AP's en clients. De OWE gebruikt de Diffie-Hellman algoritmen op basis van Cryptografie om de draadloze codering in te stellen. Met OWE voeren de client en AP tijdens de toegangsprocedure een Diffie-Hellman sleuteluitwisseling uit en gebruiken de resulterende paarsgewijze hoofdsleutel (PMK) geheim met

de 4-voudige handdruk. Het gebruik van OWE verbetert de draadloze netwerkbeveiliging voor implementaties waar op Open of gedeelde PSK gebaseerde netwerken worden geïmplementeerd.



OWE frame exchange

SAE

WPA3 maakt gebruik van een nieuw authenticatie- en sleutelbeheermechanisme genaamd Gelijktijdige verificatie van Gelijken. Dit mechanisme wordt verder versterkt door het gebruik van SAE Hash-to-Element (H2E).

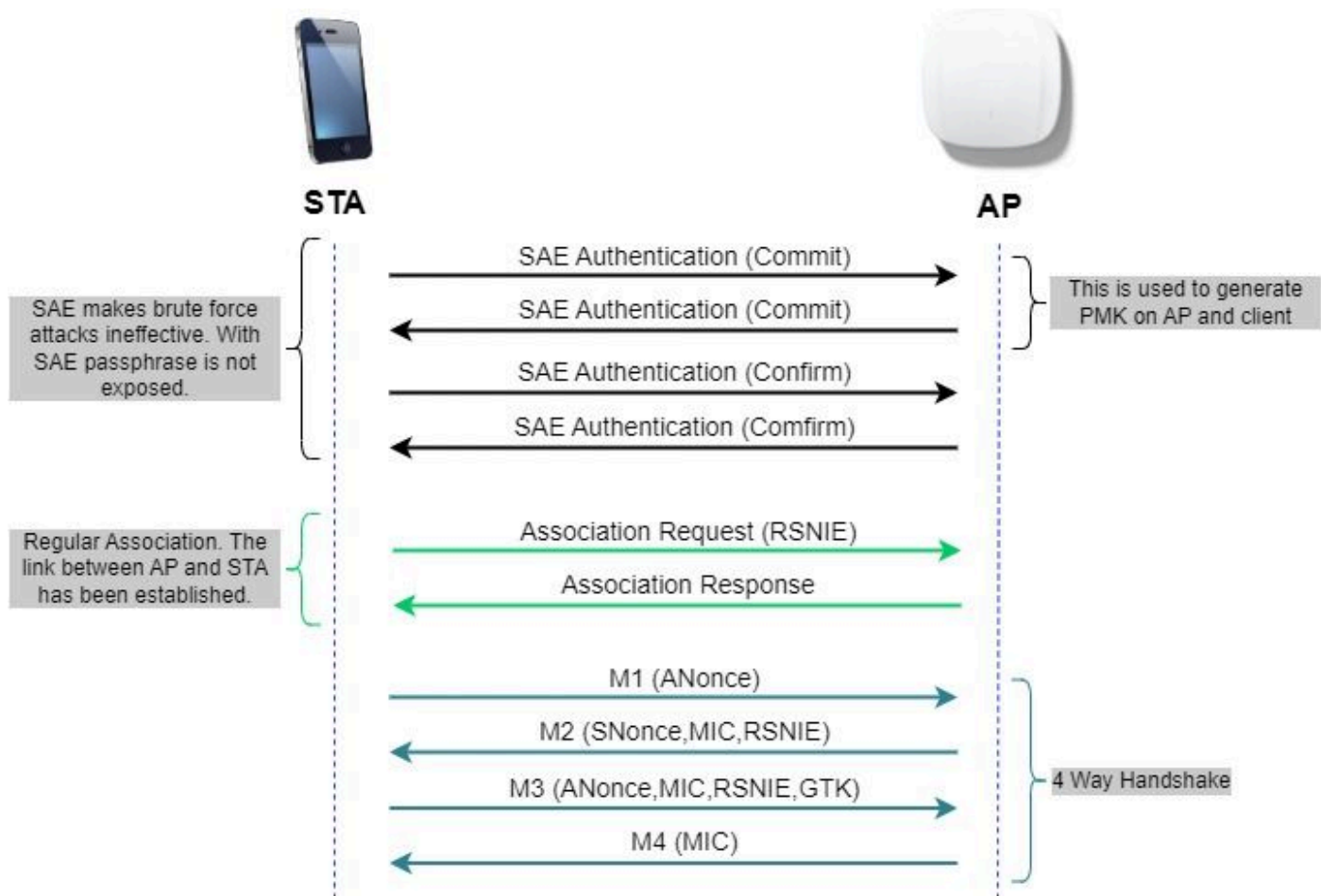
SAE met H2E is verplicht voor WPA3 en Wi-Fi 6E.

SAE maakt gebruik van een discrete logaritme cryptografie om een efficiënte uitwisseling uit te voeren op een manier die wederzijdse authenticatie uitvoert met behulp van een wachtwoord dat waarschijnlijk bestand is tegen een offline woordenboekaanval.

Een offline woordenboekaanval is waarbij een tegenstander probeert een netwerkwachtwoord te bepalen door mogelijke wachtwoorden te proberen zonder verdere netwerkinteractie.

Wanneer de client verbinding maakt met het toegangspunt, wordt een SAE-uitwisseling uitgevoerd. Indien succesvol, maken ze elk een cryptografisch sterke sleutel, waaruit de sessiesleutel is afgeleid. In principe gaat een client en access point naar de fasen van commit en vervolgens bevestig.

Zodra er een toezegging is, kunnen de client en het access point vervolgens naar de bevestigende staten gaan telkens als er een sessiesleutel moet worden gegenereerd. De methode gebruikt voorwaartse geheimhouding, waarbij een indringer één enkele sleutel kon kraken, maar niet alle andere sleutels.



SAE frame exchange

Hash-to-element (H2E)

Hash-to-Element (H2E) is een nieuwe SAE Password Element (PWE) methode. Bij deze methode wordt de geheime PWE die in het SAE-protocol wordt gebruikt, gegenereerd met een wachtwoord.

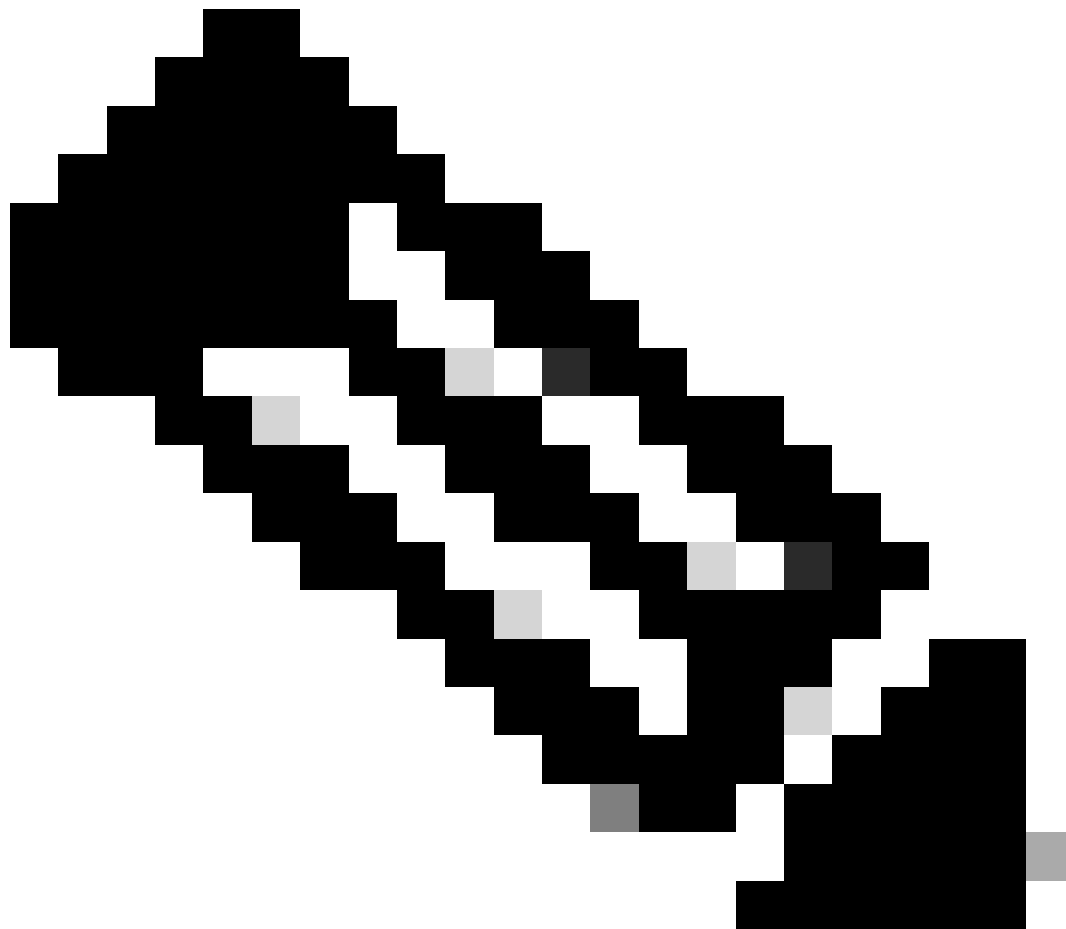
Wanneer een station (STA) dat H2E ondersteunt een SAE start met een AP, controleert het of AP H2E ondersteunt. Zo ja, gebruikt het toegangspunt de H2E om de PWE af te leiden met behulp van een nieuw gedefinieerde statuscodewaarde in het SAE Commit-bericht.

Als STA Hunting-and-Pecking (HnP) gebruikt, blijft de gehele SAE-uitwisseling ongewijzigd.

Bij gebruik van H2E wordt de PWE-afleiding onderverdeeld in de volgende componenten:

- Afleiding van een geheim tussenliggend element (PT) uit het wachtwoord. Dit kan offline worden uitgevoerd wanneer het wachtwoord in eerste instantie op het apparaat voor elke ondersteunde groep is ingesteld.
- Afleiding van de PWE uit de opgeslagen PT. Dit is afhankelijk van de onderhandelde groep

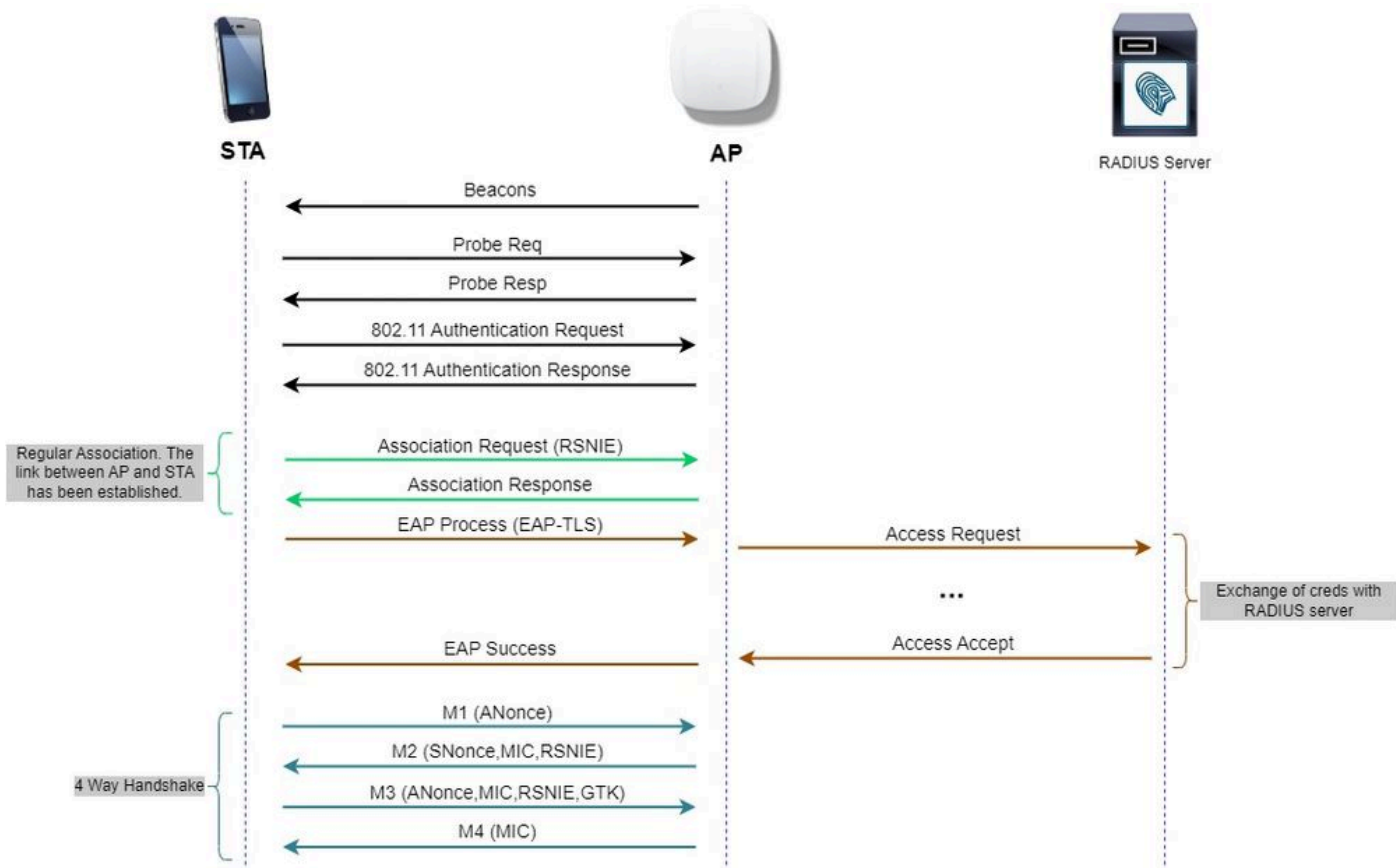
en MAC-adressen van peers. Dit wordt in real-time uitgevoerd tijdens de SAE-uitwisseling.



Opmerking: 6 GHz ondersteunt alleen Hash-to-Element SAE PWE-methode.

WPA-Enterprise ook bekend als 802.1x

WPA3-Enterprise is de veiligste versie van WPA3 en gebruikt een gebruikersnaam plus wachtwoordcombinatie met 802.1X voor gebruikersverificatie met een RADIUS-server. Standaard maakt WPA3 gebruik van 128-bits codering, maar wordt ook een optioneel configureerbare 192-bits codering van cryptografische sterkte geïntroduceerd, die extra bescherming biedt aan elk netwerk dat gevoelige gegevens doorgeeft.



Stroom WPA3-ondernemingsdiagram

Niveau ingesteld: WPA3-modi





- WPA3-Personal
 - alleen WPA3-Personal-modus
 - PMF vereist
 - WPA3-Personal-overgangsmodus
 - Configuratieregels: op een AP, wanneer WPA2-Personal is ingeschakeld, moet de WPA3-Personal Transition-modus ook standaard worden ingeschakeld, tenzij deze expliciet door de beheerder wordt overschreven om alleen in de WPA2-Personal-modus te werken
- WPA3-Enterprise
 - WPA3-Enterprise alleen-modus
 - PMF wordt voor alle WPA3-verbindingen onderhandeld
 - WPA3-Enterprise Transition Mode
 - PMF wordt overeengekomen voor een WPA3-verbinding
 - PMF optioneel voor een WPA2-verbinding
 - WPA3-Enterprise suite-B "192-bits" modus afgestemd op commercial-algoritme voor nationale beveiliging (CNSA)
 - Meer dan alleen voor de federale overheid
 - Consistente cryptografische algoritme suites om misconfiguratie te voorkomen
 - Toevoeging van GCMP & ECCP voor crypto en betere hashfuncties (SHA384)

- PMF vereist
- De WPA3 192-bit beveiliging is exclusief voor EAP-TLS, waarvoor certificaten op zowel de aanvrager als de RADIUS-server vereist zijn.
- Om WPA3 192-bit enterprise te gebruiken, moeten de RADIUS-servers een van de toegestane EAP-algoritmen gebruiken:

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Als u meer wilt weten over gedetailleerde informatie over de implementatie van WPA3 in Cisco WLAN's, inclusief de compatibiliteitsmatrix voor clientbeveiliging, kunt u de [implementatiegids voor WPA3](#) raadplegen.

Cisco Catalyst Wi-Fi 6E access points

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

Wi-Fi 6E access points

Door clients ondersteunde beveiligingsinstellingen

U kunt vinden welk product WPA3-Enterprise ondersteunen met behulp van WiFi Alliance webpagina [productzoeker](#).

Op Windows-apparaten kunt u controleren wat de beveiligingsinstellingen zijn die door de adapter worden ondersteund met de opdracht "netsh WLAN show drivers".

Hier ziet u de uitvoer van de Intel AX211:

```
C:\Users\tantunes>netsh wlan show drivers
```

```
Interface name: Wi-Fi
```

```
Driver           : Intel(R) Wi-Fi 6E AX211 160MHz
Vendor          : Intel Corporation
Provider       : Intel
Date           : 3/9/2023
Version        : 22.200.2.1
INF file       : oem151.inf
Type           : Native Wi-Fi Driver
Radio types supported : 802.11b 802.11g 802.11n 802.11a 802.11ac 802.11ax
FIPS 140-2 mode supported : Yes
802.11w Management Frame Protection supported : Yes
Hosted network supported : No
Authentication and cipher supported in infrastructure mode:
    Open          None
    Open          WEP-40bit
    Open          WEP-104bit
    Open          WEP
    WPA-Enterprise TKIP
    WPA-Enterprise CCMP
    WPA-Personal  TKIP
    WPA-Personal  CCMP
    WPA2-Enterprise TKIP
    WPA2-Enterprise CCMP
    WPA2-Personal  TKIP
    WPA2-Personal  CCMP
    Open          Vendor defined
    WPA3-Personal  CCMP
    Vendor defined Vendor defined
    WPA3-Enterprise 192 Bits GCMP-256
    OWE             CCMP
    WPA3-Enterprise CCMP
    WPA3-Enterprise TKIP
Number of supported bands : 3
    2.4 GHz [ 0 MHz - 0 MHz]
    5 GHz  [ 0 MHz - 0 MHz]
    6 GHz  [ 0 MHz - 0 MHz]
IHV service present : Yes
IHV adapter OUI    : [00 00 00], type: [00]
IHV extensibility DLL path: C:\WINDOWS\System32\DriverStore\FileRepository\netwtw6e.inf_amd64_eda979fbdede064\IntelIHVRouter12.dll
```

Windows-uitvoer van _netsh WLAN show driver_ voor client AX211

Netgear A8000:

Interface name: A8000_NETGEAR

```
Driver : NETGEAR A8000 WiFi 6 & 6E Adapter
Vendor : NETGEAR Inc.
Provider : MediaTek, Inc.
Date : 11/25/2022
Version : 1.0.0.108
INF file : oem9.inf
Type : Native Wi-Fi Driver
Radio types supported : 802.11b 802.11a 802.11g 802.11n 802.11ac 802.11ax
FIPS 140-2 mode supported : Yes
802.11w Management Frame Protection supported : Yes
Hosted network supported : No
Authentication and cipher supported in infrastructure mode:
      Open          None
      Open          WEP-40bit
      Open          WEP-104bit
      Open          WEP
      WPA-Enterprise TKIP
      WPA-Enterprise CCMP
      WPA3-Personal  CCMP
      OWE            CCMP
      WPA-Personal  TKIP
      WPA-Personal  CCMP
      WPA2-Enterprise TKIP
      WPA2-Enterprise CCMP
      WPA2-Personal  TKIP
      WPA2-Personal  CCMP
Number of supported bands : 3
      2.4 GHz [ 0 MHz - 0 MHz]
      5 GHz   [ 0 MHz - 0 MHz]
      6 GHz   [ 0 MHz - 0 MHz]
IHV service present : Yes
IHV adapter OUI : [00 00 00], type: [00]
IHV extensibility DLL path: C:\WINDOWS\system32\mtknhvux.dll
IHV UI extensibility CLSID: {00000000-0000-0000-0000-000000000000}
IHV diagnostics CLSID : {00000000-0000-0000-0000-000000000000}
Wireless Display Supported: Yes (Graphics Driver: Yes, Wi-Fi Driver: Yes)
```

Windows-uitvoer van `_netsh wlan show driver_` voor client Netgear A8000s

Android Pixel 6a:



None

Enhanced Open

WEP

WPA/WPA2-Personal

WPA3-Personal

WPA/WPA2-Enterprise

WPA3-Enterprise

WPA3-Enterprise 192-bit



CIF



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

Basisconfiguratie

WLAN is geconfigureerd met 6GHz alleen radio beleid en UPR (Broadcast Probe Response) detectiemethode:

Edit WLAN ⌵

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

General

Security

Advanced

Add To Policy Tags

Profile Name*	<input type="text" value="wifi_test"/>	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> Radio Policy ⓘ <div style="text-align: right; font-size: small; color: #4f81bd;">Show slot configuration</div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> 6 GHz Status ENABLED <input checked="" type="checkbox"/> <div style="font-size: x-small; margin-top: 5px;"> ✔ WPA2 Disabled ✔ WPA3 Enabled ✔ Dot11ax Enabled </div> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> 5 GHz Status DISABLED <input type="checkbox"/> </div> <div style="border: 1px solid #ccc; padding: 5px;"> 2.4 GHz Status DISABLED <input type="checkbox"/> 802.11b/g Policy 802.11b/g ▾ </div> </div>
SSID*	<input type="text" value="wifi_test"/>	
WLAN ID*	<input type="text" value="5"/>	
Status	ENABLED <input checked="" type="checkbox"/>	
Broadcast SSID	ENABLED <input checked="" type="checkbox"/>	

WLAN-basisconfiguratie

6 GHz RF-profielconfiguratie

Verifiëren

Beveiligingsverificatie

In deze sectie wordt het gepresenteerd de configuratie van de beveiliging en de associatiefase van de client met behulp van deze WPA3-protocolcombinaties:

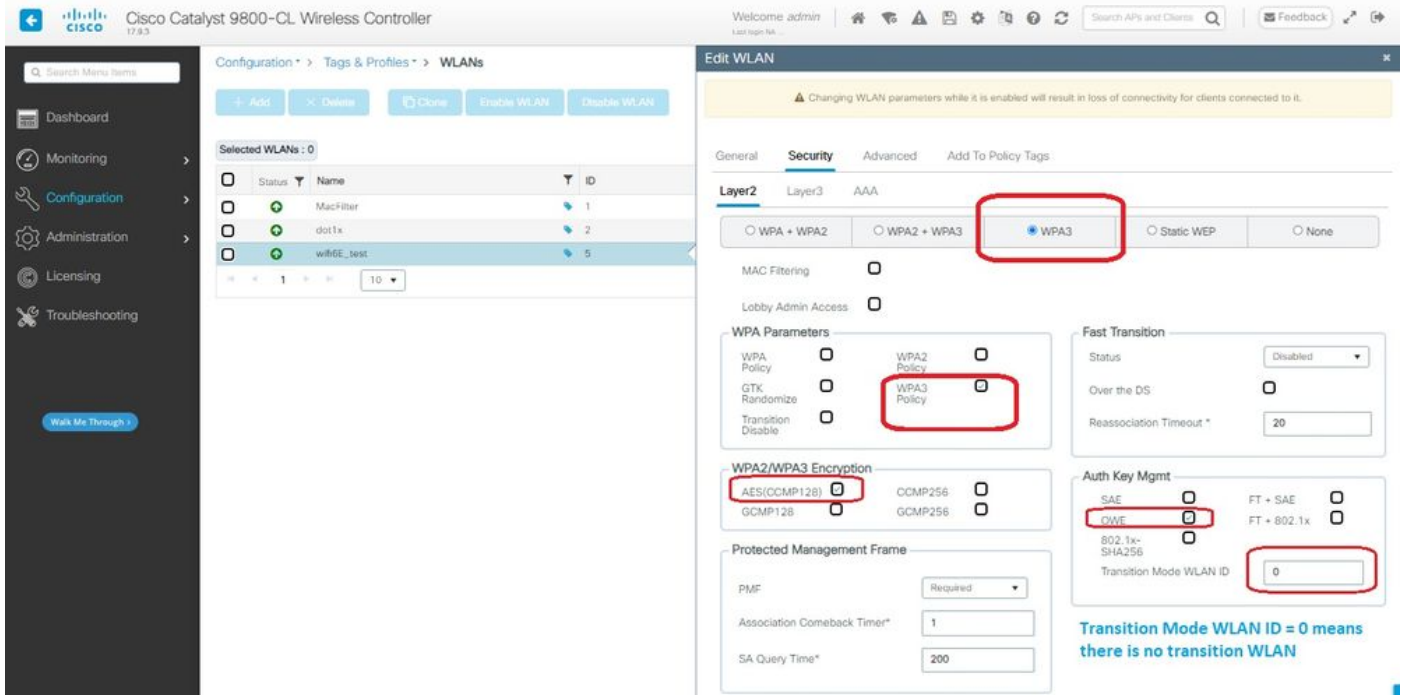
- WPA3- AES(CCMP128) + OWE
 - OWE-overgangsmodus
- WPA3-Personal
 - AES(CCMP128) + SAE
- WPA3-Enterprise
 - AES(CCMP128) + 802.1x-SHA256
 - AES(CCMP128) + 802.1x-SHA256 + FT
 - GCMP128-algoritme + SITEB-1X
 - GCMP256-algoritme + SITEB192-1X



Opmerking: Hoewel er vanaf het schrijven van dit document geen clients zijn die het GCMP128-algoritme + SUITEB-1X ondersteunen, is getest om te zien dat het wordt uitgezonden en de RSN-informatie in de bakens te controleren.

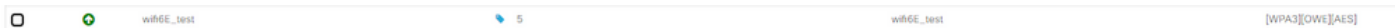
WPA3 - AES(CCPM128) + OWE

Dit is de WLAN-beveiligingsconfiguratie:



Beveiligingsinstellingen van het type OWE

Bekijk op WLC GUI van de WLAN security instellingen:



WLAN-beveiligingsinstellingen op WLC GUI

Hier kunnen we het Wi-Fi 6E-clientverbindingproces waarnemen:

Intel AX211 switch

Hier tonen we het volledige verbindingproces van de client Intel AX211.

OWE-detectie

Hier zie je de bakens OTA. De AP adverteert ondersteuning voor OWE met behulp van AKM suite selector voor OWE onder RSN informatie element.

Je ziet AKM suite type value 18 (00-0F-AC:18) dat aangeeft OWE ondersteuning.

OWE beacon frame

Als u kijkt naar het veld RSN-functies, ziet u dat AP adverteert met zowel MFP-functies (Management Frame Protection) als MFP Required bit set to 1.

OWE-associatie

U kunt de JPR zien die in de uitzendingmodus wordt verstuurd en vervolgens de associatie zelf.

De OWE begint met het Open authenticatieverzoek en antwoord:

Vervolgens moet een client die OWE wil doen OWE AKM aangeven in het RSN IE of Association request frame en Diffie Helman (DH) parameter element opnemen:

The image shows a Wireshark packet capture of an IEEE 802.11 Association Request (Frame 11) and its corresponding Association Response (Frame 12). The interface is 'lovice/wifi0' on IP 192.168.1.121. The frames are captured on the wireless interface. The Association Request frame contains several key management and security-related fields, including:

- Auth Key Management (AKM) Suite:** 00:0f:ac (IEEE 802.11) Opportunistic Wireless Encryption
- Auth Key Management (AKM) OUI:** 00:0f:ac (IEEE 802.11)
- RSN Capabilities:** 000000
- RSN PRe-Auth capabilities:** Transmitter does not support pre-authentication
- RSN No Pairwise capabilities:** Transmitter can support WEP default key a simultaneously with Pairwise
- RSN GTKSA Replay Counter capabilities:** 16 replay counters per GTKSA/GTKSA/STakeysA (8x3)
- Management Frame Protection Required:** True
- Management Frame Protection Capable:** True
- Joint Multi-band RSN:** False
- Peerkey Enabled:** False
- Extended Key ID for Individually Addressed Frames:** Not supported
- PKID Count:** 0

The Association Response frame (Frame 12) includes the following fields:

- Group Management Cipher Suite:** 00:0f:ac (IEEE 802.11) EAP (128)
- Supported Operating Classes:** 1
- Tag: Vendor Specific:** microsoft corp.: wpa/wpa: Parameter Element
- Ext Tag: OWE Diffie-Hellman Parameter:** Element ID Extension (255)
- Ext Tag Length:** 34
- Ext Tag Number:** OWE Diffie-Hellman Parameter (32)
- Group:** 256-bit random ECP group (19)
- Public Key:** 849cf39923254c0c6137940877f2e09505acd7266af6e0f743018496
- Ext Tag: HE Capabilities**
- Ext Tag: HE 4 GHz Band Capabilities**

This image shows the continuation of the Wireshark capture, focusing on the Authentication and Key Management phases. Key frames include:

- Authentication (Frame 8):** Successful authentication from the client to the AP.
- Key Management (Frame 10):** Exchange of key information, including the AKM suite and RSN capabilities.
- Key Management (Frame 11):** Further key management details, including the OUI and RSN capabilities.
- Key Management (Frame 12):** Response to the key management request, including the group management cipher suite and supported operating classes.

Antwoord van OWE Association

Na de associatiereactie kunnen we de 4-voudige handdruk en client-bewegingen naar verbonden staat zien.

Hier kunt u de klantgegevens zien op de WLC GUI:

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller GUI. The 'Clients' page is active, displaying a list of clients. The client with MAC address 286b.3598.580f is selected. The details pane on the right shows the following information:

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

NetGear A800

OTA-verbinding met focus op RSN-informatie van client:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
930	2023-06-12 14:03:07.117065	0.000000	netgear_48:78195	broadcast	802.11	166	5	-51 dBm	Probe Request, Ss=1538, Fw=0, Flags=.....C, SSID="billzar"
931	2023-06-12 14:03:07.117790	0.000021	netgear_48:78195	broadcast	802.11	166	5	-51 dBm	Probe Request, Ss=1531, Fw=0, Flags=.....C, SSID="billzar"
932	2023-06-12 14:03:07.118792	0.000021	netgear_48:78195	broadcast	802.11	166	5	-51 dBm	Probe Request, Ss=1532, Fw=0, Flags=.....C, SSID="billzar"
933	2023-06-12 14:03:07.119655	0.000021	netgear_48:78195	broadcast	802.11	166	5	-51 dBm	Probe Request, Ss=1531, Fw=0, Flags=.....C, SSID="billzar"
1013	2023-06-12 14:03:08.455478	1.165423	netgear_48:78195	Cisco_31:08:	802.11	368	5	-51 dBm	Association Request, Ss=0696, Fw=0, Flags=.....C, SSID="wifi6_test"
1014	2023-06-12 14:03:08.455478	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1015	2023-06-12 14:03:08.455488	0.000070	netgear_48:78195	Cisco_31:08:	802.11	368	5	-52 dBm	Probe Request, Ss=2, Fw=0, Flags=.....C, SSID="wifi6_test"
1016	2023-06-12 14:03:08.455959	0.000041	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1019	2023-06-12 14:03:08.504575	0.011566	netgear_48:78195	Cisco_31:08:	802.11	368	5	-41 dBm	Probe Request, Ss=2, Fw=0, Flags=.....C, SSID="wifi6_test"
1020	2023-06-12 14:03:08.504575	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1024	2023-06-12 14:03:08.718083	0.213580	netgear_48:78195	Cisco_31:08:	802.11	96	5	-51 dBm	Authentication, Ss=1, Fw=0, Flags=.....C
1025	2023-06-12 14:03:08.724041	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1026	2023-06-12 14:03:08.724041	0.000330	Cisco_31:08:	netgear_48:7	802.11	96	5	-36 dBm	Authentication, Ss=0x6, Fw=0, Flags=.....C
1027	2023-06-12 14:03:08.724041	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1029	2023-06-12 14:03:08.728154	0.000373	netgear_48:78195	Cisco_31:08:	802.11	258	5	-55 dBm	Association Request, Ss=0x6, Fw=0, Flags=.....C, SSID="wifi6_test"
1030	2023-06-12 14:03:08.728154	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1044	2023-06-12 14:03:08.736159	0.000285	netgear_48:78195	broadcast	LLC	124	5	-36 dBm	U, P, FuncUnknown, DSAP 0x0C Group, SSAP Remote Program Load Response
1045	2023-06-12 14:03:08.736159	0.000000	Cisco_31:08:	netgear_48:7	802.11	259	5	-36 dBm	Association Response, Ss=0x6, Fw=0, Flags=.....C
1046	2023-06-12 14:03:08.739159	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1047	2023-06-12 14:03:08.739159	0.000000	netgear_48:78195	broadcast	LLC	124	5	-36 dBm	I, P, N(0x08, N(5)) DSAP 0x0C Group, SSAP 0x0C
1049	2023-06-12 14:03:08.742159	0.000000	Cisco_31:08:	netgear_48:7	802.11	221	5	-36 dBm	Key (Message 1 of 4)
1050	2023-06-12 14:03:08.743159	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1051	2023-06-12 14:03:08.743159	0.000000	netgear_48:78195	Cisco_31:08:	802.11	223	5	-51 dBm	Key (Message 2 of 4)
1052	2023-06-12 14:03:08.743159	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1053	2023-06-12 14:03:08.751342	0.000000	Cisco_31:08:	netgear_48:7	802.11	235	5	-36 dBm	Key (Message 1 of 4)
1054	2023-06-12 14:03:08.751342	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1055	2023-06-12 14:03:08.751342	0.000000	netgear_48:78195	Cisco_31:08:	802.11	199	5	-55 dBm	Key (Message 4 of 4)
1056	2023-06-12 14:03:08.751342	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-43 dBm	Acknowledgment, Flags=.....C
1057	2023-06-12 14:03:08.757481	0.000139	Cisco_31:08:	netgear_48:7	802.11	187	5	-42 dBm	I, P, N(0x08, N(5)) DSAP 0x0C Individual, SSAP 0x0C Command
1058	2023-06-12 14:03:08.757481	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-55 dBm	Acknowledgment, Flags=.....C
1059	2023-06-12 14:03:08.757481	0.000000	192.168.1.15	192.168.1.121	802.11	119	5	-43 dBm	Trigger Buffer Status Report Poll (BSRP), Flags=.....C
1060	2023-06-12 14:03:08.758468	0.001187	192.168.1.15	192.168.1.121	802.11	119	5	-43 dBm	Trigger Buffer Status Report Poll (BSRP), Flags=.....C
1061	2023-06-12 14:03:08.808063	0.001495	netgear_48:78195	PfVmcncr_36	LLC	127	5	-41 dBm	I, N(0x08, N(5)) DSAP 0x0C (IC955) Active Station List Maintenance
1062	2023-06-12 14:03:08.808063	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-43 dBm	Acknowledgment, Flags=.....C
1063	2023-06-12 14:03:08.811342	0.000000	192.168.1.15	192.168.1.121	802.11	119	5	-42 dBm	Trigger Buffer Status Report Poll (BSRP), Flags=.....C
1064	2023-06-12 14:03:08.828063	0.000000	netgear_48:78195	PfVmcncr_36	LLC	127	5	-38 dBm	I, N(0x08, N(5)) DSAP 0x0C Group, SSAP 0x0C Command
1065	2023-06-12 14:03:08.828063	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-43 dBm	Acknowledgment, Flags=.....C
1110	2023-06-12 14:03:08.892420	0.000000	netgear_48:78195	broadcast	LLC	444	5	-36 dBm	U, P, Func0x08, DSAP 0x0C Group, SSAP 0x0C Command
1111	2023-06-12 14:03:08.892420	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-42 dBm	Acknowledgment, Flags=.....C
1112	2023-06-12 14:03:08.892420	0.000000	192.168.1.15	192.168.1.121	802.11	195	5	-37 dBm	I, N(0x10, N(5)) DSAP 0x0C Group, SSAP 0x0C Response
1113	2023-06-12 14:03:08.898255	0.001576	netgear_48:78195	broadcast	LLC	442	5	-36 dBm	I, P, N(0x10, N(5)) DSAP 0x0C Individual, SSAP 0x0C Response
1143	2023-06-12 14:03:08.917921	0.027996	netgear_48:78195	PfVmcncr_36	LLC	265	5	-41 dBm	U, P, FuncUnknown, DSAP 0x0C Individual, SSAP 0x0C Response
1144	2023-06-12 14:03:08.917921	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-41 dBm	Acknowledgment, Flags=.....C
1145	2023-06-12 14:03:08.917921	0.000000	192.168.1.15	192.168.1.121	802.11	208	5	-37 dBm	I, N(0x08, N(5)) DSAP 0x0C BSA 85-511 Manufacturing Message Service Ind
1146	2023-06-12 14:03:08.921977	0.004056	Cisco_31:08:	netgear_48:7	802.11	118	5	-36 dBm	Action, Ss=0, Fw=0, Flags=.....C
1149	2023-06-12 14:03:08.921977	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-51 dBm	Acknowledgment, Flags=.....C

Klantgegevens in WLC:

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The 'Clients' tab is active, displaying a list of clients. The selected client is 9418.6548.7095, with IP address 192.168.1.163 and AP name AP6849.9253.CA50. The client details pane on the right shows security information, including Client State Servers (None), Client ACLs (None), Client Entry Create Time (25 seconds), Policy Type (WPA3), Encryption Cipher (CCMP (AES)), Authentication Key Management (OWE), EAP Type (Not Applicable), and Session Timeout (86400).

Pixel 6a

OTA-verbinding met focus op RSN-informatie van client:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
584	2023-06-12 15:53:27.558985	1.165952	google_72:8a:66	netgear_48:78195	Cisco_31:08:	108	5	-47 dBm	Authentication, Ss=1097, Fw=0, Flags=.....C, SSID="wifi6_test"
585	2023-06-12 15:53:27.693928	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
587	2023-06-12 15:53:27.726589	0.001841	Cisco_31:08:	google_72:8a:66	802.11	108	5	-36 dBm	Authentication, Ss=1097, Fw=0, Flags=.....C
588	2023-06-12 15:53:27.726589	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-48 dBm	Acknowledgment, Flags=.....C
589	2023-06-12 15:53:27.726589	0.000000	google_72:8a:66	Cisco_31:08:	802.11	293	5	-46 dBm	Association Request, Ss=0696, Fw=0, Flags=.....C, SSID="wifi6_test"
590	2023-06-12 15:53:27.726589	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-46 dBm	Acknowledgment, Flags=.....C
594	2023-06-12 15:53:27.791916	0.001818	Cisco_31:08:	google_72:8a:66	802.11	299	5	-36 dBm	Association Response, Ss=0x6, Fw=0, Flags=.....C
595	2023-06-12 15:53:27.791916	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-45 dBm	Acknowledgment, Flags=.....C
600	2023-06-12 15:53:27.794140	0.002232	Cisco_31:08:	google_72:8a:66	802.11	221	5	-36 dBm	Key (Message 1 of 4)
601	2023-06-12 15:53:27.794140	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-46 dBm	Acknowledgment, Flags=.....C
604	2023-06-12 15:53:27.832152	0.007884	google_72:8a:66	Cisco_31:08:	802.11	227	5	-46 dBm	Key (Message 2 of 4)
605	2023-06-12 15:53:27.832152	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
607	2023-06-12 15:53:27.834424	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-46 dBm	Acknowledgment, Flags=.....C
609	2023-06-12 15:53:27.840723	0.000239	google_72:8a:66	Cisco_31:08:	802.11	199	5	-46 dBm	Key (Message 4 of 4)
610	2023-06-12 15:53:27.840723	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-37 dBm	Acknowledgment, Flags=.....C
611	2023-06-12 15:53:27.868914	0.020191	Cisco_31:08:	google_72:8a:66	802.11	187	5	-46 dBm	I, P, N(0x08, N(5)) DSAP 0x0C Group, SSAP 0x0C Command
612	2023-06-12 15:53:27.868914	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-53 dBm	Acknowledgment, Flags=.....C
613	2023-06-12 15:53:27.868914	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-37 dBm	Acknowledgment, Flags=.....C
614	2023-06-12 15:53:27.864096	0.001192	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
615	2023-06-12 15:53:27.879567	0.011561	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
617	2023-06-12 15:53:27.882181	0.000614	192.168.1.15	192.168.1.121	802.11	76	5	-45 dBm	Acknowledgment, Flags=.....C
618	2023-06-12 15:53:27.884515	0.002852	google_72:8a:66	Cisco_31:08:	802.11	122	5	-36 dBm	Action, Ss=1097, Fw=0, Flags=.....C
619	2023-06-12 15:53:27.884515	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-46 dBm	Acknowledgment, Flags=.....C
621	2023-06-12 15:53:27.933021	0.000318	Cisco_31:08:	google_72:8a:66	802.11	124	5	-37 dBm	Action, Ss=0, Fw=0, Flags=.....C [Malformed Packet]
624	2023-06-12 15:53:27.919191	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-47 dBm	Acknowledgment, Flags=.....C
629	2023-06-12 15:53:28.018096	0.005295	google_72:8a:66	Cisco_31:08:	802.11	115	5	-48 dBm	Action, Ss=1097, Fw=0, Flags=.....C
630	2023-06-12 15:53:28.018096	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
631	2023-06-12 15:53:28.018096	0.000000	google_72:8a:66	Cisco_31:08:	802.11	227	5	-55 dBm	I, N(0x10, N(5)) DSAP 0x0C Individual, SSAP 0x0C Command
632	2023-06-12 15:53:28.018096	0.000014	192.168.1.15	192.168.1.121	802.11	76	5	-46 dBm	Acknowledgment, Flags=.....C
634	2023-06-12 15:53:28.020947	0.002803	Cisco_31:08:	google_72:8a:66	802.11	115	5	-37 dBm	Action, Ss=2, Fw=0, Flags=.....C
635	2023-06-12 15:53:28.020947	0.000000	192.168.1.15	192.168.1.121	8				

Samsung S23

OTA-verbinding met focus op RSN-informatie van client:

Klantgegevens in WLC:

WPA3 - AES(CCPM128) + OWE met overgangsmodus

Gedetailleerde configuratie en probleemoplossing van de OWE Transition Mode beschikbaar in dit document: [Configure Enhanced Open SSID with Transition Mode - OWE](#).

WPA3-Personal - AES(CCMP128) + SAE

WLAN-beveiligingsconfiguratie:

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

Configuratie WPA3 SAE



Opmerking: Houd er rekening mee dat jagen en pecken niet is toegestaan met 6 GHz radiobeleid. Wanneer u een 6GHz alleen WLAN configureert, moet u H2E SAE-wachtwoordelement selecteren.

Bekijk op WLC GUI van de WLAN security instellingen:



Verificatie van de OTA van bakens:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
2	2023-06-12 17:12:24.459118	0.00000	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: Cisco_0d70137 (00:0f:1d:0d:70137), Dst: universe_b7c1cf0e (00:1a:8b:07:c1cf0e)
5	2023-06-12 17:12:24.491121	0.00045	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 192.168.1.13, Dst: 192.168.1.11
6	2023-06-12 17:12:24.731872	0.24053	Cisco_13:1801e0	Broadcast	802.11	508	5	-37 dBm	Beacon frame, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
7	2023-06-12 17:12:24.732106	0.00034	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
10	2023-06-12 17:12:24.772881	0.04045	Cisco_13:1801e0	Broadcast	802.11	463	5	-37 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
11	2023-06-12 17:12:24.773099	0.00023	Cisco_13:1801e0	Broadcast	802.11	463	5	-37 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
14	2023-06-12 17:12:24.814901	0.04045	Cisco_13:1801e0	Broadcast	802.11	508	5	-36 dBm	Beacon frame, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
15	2023-06-12 17:12:24.834577	0.02075	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
16	2023-06-12 17:12:24.855609	0.02082	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
17	2023-06-12 17:12:24.875476	0.02082	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
18	2023-06-12 17:12:24.895829	0.02093	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
19	2023-06-12 17:12:24.916558	0.02073	Cisco_13:1801e0	Broadcast	802.11	508	5	-36 dBm	Beacon frame, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
20	2023-06-12 17:12:24.937923	0.02165	Cisco_13:1801e0	Broadcast	802.11	463	5	-37 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
21	2023-06-12 17:12:24.959625	0.03172	Cisco_13:1801e0	Broadcast	802.11	463	5	-37 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
22	2023-06-12 17:12:24.980372	0.02077	Cisco_13:1801e0	Broadcast	802.11	463	5	-37 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
23	2023-06-12 17:12:25.001811	0.02089	Cisco_13:1801e0	Broadcast	802.11	508	5	-36 dBm	Beacon frame, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
24	2023-06-12 17:12:25.023948	0.02037	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
25	2023-06-12 17:12:25.045912	0.02044	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
26	2023-06-12 17:12:25.068008	0.02058	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
27	2023-06-12 17:12:25.090884	0.02044	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
28	2023-06-12 17:12:25.113159	0.02075	Cisco_13:1801e0	Broadcast	802.11	508	5	-36 dBm	Beacon frame, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
29	2023-06-12 17:12:25.134178	0.02019	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
30	2023-06-12 17:12:25.156274	0.02182	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
35	2023-06-12 17:12:25.182664	0.01990	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
37	2023-06-12 17:12:25.203881	0.02047	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
38	2023-06-12 17:12:25.225792	0.02042	Cisco_13:1801e0	Broadcast	802.11	508	5	-36 dBm	Beacon frame, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
39	2023-06-12 17:12:25.244147	0.02045	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
40	2023-06-12 17:12:25.264334	0.02037	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
41	2023-06-12 17:12:25.285513	0.02049	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
42	2023-06-12 17:12:25.306792	0.02059	Cisco_13:1801e0	Broadcast	802.11	508	5	-36 dBm	Beacon frame, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
43	2023-06-12 17:12:25.328107	0.02059	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
44	2023-06-12 17:12:25.349489	0.02059	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
45	2023-06-12 17:12:25.370972	0.02059	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
46	2023-06-12 17:12:25.392536	0.02059	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
48	2023-06-12 17:12:25.407908	0.02060	Cisco_13:1801e0	Broadcast	802.11	463	5	-37 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
49	2023-06-12 17:12:25.429354	0.02064	Cisco_13:1801e0	Broadcast	802.11	508	5	-36 dBm	Beacon frame, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
50	2023-06-12 17:12:25.450929	0.02047	Cisco_13:1801e0	Broadcast	802.11	463	5	-37 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
51	2023-06-12 17:12:25.472618	0.02045	Cisco_13:1801e0	Broadcast	802.11	508	5	-36 dBm	Beacon frame, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
52	2023-06-12 17:12:25.494300	0.02045	Cisco_13:1801e0	Broadcast	802.11	463	5	-37 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
53	2023-06-12 17:12:25.516033	0.02044	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
54	2023-06-12 17:12:25.537872	0.02062	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
55	2023-06-12 17:12:25.559829	0.02033	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
56	2023-06-12 17:12:25.581892	0.02062	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
57	2023-06-12 17:12:25.604067	0.02033	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
58	2023-06-12 17:12:25.626352	0.02037	Cisco_13:1801e0	Broadcast	802.11	508	5	-36 dBm	Beacon frame, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
59	2023-06-12 17:12:25.648748	0.02044	Cisco_13:1801e0	Broadcast	802.11	463	5	-37 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
60	2023-06-12 17:12:25.671253	0.02039	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
61	2023-06-12 17:12:25.693887	0.02040	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
62	2023-06-12 17:12:25.716622	0.02040	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
63	2023-06-12 17:12:25.739517	0.02040	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
64	2023-06-12 17:12:25.762571	0.02162	Cisco_13:1801e0	Broadcast	802.11	508	5	-37 dBm	Beacon frame, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1
67	2023-06-12 17:12:25.765892	0.00373	Cisco_13:1801e0	Broadcast	802.11	463	5	-36 dBm	Probe Response, Src: 78078, FwB, Flags:.....C, B1=80, SSID="WiFi6_Test_02", SSID Extension: 1

```

Frame 6: 508 bytes on wire (4064 bits), 508 bytes captured (4064 bits) on interface Vdeice\NPF_{04578995-2998-4464-4
Ethernet II, Src: Cisco_0d70137 (00:0f:1d:0d:70137), Dst: universe_b7c1cf0e (00:1a:8b:07:c1cf0e)
Internet Protocol version 4, Src: 192.168.1.13, Dst: 192.168.1.11
User Datagram Protocol, Src Port: 5555, Dst Port: 5000
AirOreok/OmniPeek encapsulated IEEE 802.11
IEEE 802.11 radio information
IEEE 802.11 Beacon frame, Flags:.....C
IEEE 802.11 wireless management
Fixed parameters (406 bytes)
Tag: SSI parameter set "WiFi6_Test_02"
Tag: Supported rates (3), 5, 11M; 18, 24M; 36, 48, 54, 72Mbit/sec
Tag: Traffic Indication Map (TIM): ODFI 2 of 3 Bitmap
Tag: Country Information: Country code is, Environment global operating classes
Tag: Power Constraint: 0
Tag: TPC Report Transm Power: 17, Link Margin: 0
Tag: RSN Information
Tag number: RSN Information (48)
Tag length: 36
RSN version: 1
Group Cipher Suite: 00f0ac (See 802.11) AES (CCM)
Pairwise Cipher Suite Count: 1
Pairwise Cipher Suite List: 00f0ac (See 802.11) AES (CCM)
Auth Key Management: (AOK) Suite Count: 1
Auth Key Management (AOK) List: 00f0ac (See 802.11) SAE (SHA256)
RSN Capabilities: 00000
PMKID Count: 0
PMKID List
Group Management Cipher Suite: 00f0ac (See 802.11) ESP (128)
Tag: QSS Load Element: 001e cca version
Tag: Multiple SSID
Tag: HT Extended Capabilities (11 octets)
Tag: TX Power Envelope
Tag: Extended Capabilities (11 octets)
Tag: TX Power Envelope
Ext Tag: Multiple SSID Configuration
Ext Tag: HE Capabilities
Ext Tag: HE Operation
Ext Tag: Spatial Reuse Parameter Set
Ext Tag: MU-EDCA Parameter Set
Ext Tag: HE Capabilities
Tag: RSN extension (1 octet)
Tag number: RSN extension (244)
RSN: 0x20 (protected)
... 0000 = RSN Length: 0
... 0 = Protected but Operations Support: 0
... 0000 = SAE mesh to element: 1
... 0000 = Reserved 00
Tag: Vendor Specific: Atheros Communications, Inc.: Unknown
Tag: Vendor Specific: Cisco Systems, Inc.: Airont Unknown (44)
Tag: Vendor Specific: Cisco Systems, Inc.: Airont Unknown (11) (11)
Tag: Vendor Specific: Cisco Systems, Inc.: Airont IEEE WPA Disabled
Tag: Vendor Specific: Cisco Systems, Inc.: Airont CCM version = 5

```

WPA3 SAE-bakens

Hier kunnen we Wi-Fi 6E-clients waarnemen die associëren:

Intel AX211 switch

OTA-verbinding met focus op RSN-informatie van client:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
2235	2023-06-12 17:15:00.328330	0.00000	IntelCor_98:1581e0	Broadcast	802.11	168	5	-47 dBm	Probe Request, Src: 98039, FwB, Flags:.....C, SSID=WiFi6 (Broadcast)
2237	2023-06-12 17:15:00.328335	0.00055	IntelCor_98:1581e0	Broadcast	802.11	168	5	-47 dBm	Probe Request, Src: 98039, FwB, Flags:.....C, SSID=WiFi6 (Broadcast)
2342	2023-06-12 17:15:01.974931	1.64426	IntelCor_98:1581e0	Broadcast	802.11	168	5	-49 dBm	Probe Request, Src: 98039, FwB, Flags:.....C, SSID=WiFi6 (Broadcast)
2344	2023-06-12 17:15:01.977134	0.00245	IntelCor_98:1581e0	Broadcast	802.11	168	5	-47 dBm	Probe Request, Src: 98039, FwB, Flags:.....C, SSID=WiFi6 (Broadcast)
5674	2023-06-12 17:15:00.536729	58.55995	IntelCor_98:1581e0	Broadcast	802.11	168	5	-47 dBm	Probe Request, Src: 98039, FwB, Flags:.....C, SSID=WiFi6 (Broadcast)
5878	2023-06-12 17:15:00.536729	0.00000	IntelCor_98:1581e0	Broadcast	802.11	168	5	-49 dBm	Probe Request, Src: 98039, FwB, Flags:.....C, SSID=WiFi6 (Broadcast)
8087	2023-06-12 17:15:00.490357	79.16218	IntelCor_98:1581e0	Broadcast	802.11	168	5	-46 dBm	Probe Request, Src: 98039, FwB, Flags:.....C, SSID=WiFi6 (Broadcast)
8089	2023-06-12 17:15:00.492713	0.00256	IntelCor_98:1581e0	Broadcast	802.11	168	5	-49 dBm	Probe Request, Src: 98039, FwB, Flags:.....C, SSID=WiFi6 (Broadcast)
8237	2023-06-12 17:15:01.264354	1.64441	IntelCor_98:1581e0	Broadcast	802.11	168	5	-48 dBm	Probe Request, Src: 98039, FwB, Flags:.....C, SSID=WiFi6 (Broadcast)
8239	2023-06-12 17:15:01.266557	0.00220	IntelCor_98:1581e0	Broadcast	802.11	168	5	-49 dBm	Probe Request, Src: 98039, FwB, Flags:.....C, SSID=WiFi6 (Broadcast)
123	2023-06-12 17:15:01.087192	45.81235	IntelCor_98:1581e0	Broadcast	802.11	168	5	-44 dBm	Probe Request, Src: 98039, FwB, Flags:.....C, SSID=WiFi6 (Broadcast)
123	2023-06-12 17:15:01.084321	0.002829	IntelCor_98:1581e0	Broadcast	802.11	168	5	-47 dBm	Probe Request, Src: 98039, FwB, Flags:.....C, SSID=WiFi6 (Broadcast)
124	2023-06-12 17:15:01.083758	1.75249	IntelCor_98:1581e0	Broadcast	802.11	168	5	-47 dBm	Probe Request, Src: 98039, FwB, Flags:.....C, SSID=WiFi6 (Broadcast)
124	2023-06-12 17:15:01.084008	0.00240	IntelCor_98:1581e0						

NetGear A800

OTA-verbinding met focus op RSN-informatie van client:

Klantgegevens in WLC:

Pixel 6a

OTA-verbinding met focus op RSN-informatie van client:

Cisco Catalyst 9800-CL Wireless Controller

Welcome admin

Search APs and Clients

Feedback

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Selected 0 out of 12 Clients

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

Client

360 View General QoS Statistics ATF Statistics Mobility History Call Statistics

Client Properties AP Properties Security Information Client Statistics QoS Properties EoGRE

Client State Servers None

Client ACLs None

Client Entry Create Time 78 seconds

Policy Type WPA3

Encryption Cipher CCMP (AES)

Authentication Key Management SAE

EAP Type Not Applicable

Session Timeout 86400

Session Manager

Point of Attachment capwap_90000010

IF ID 0x90000010

Authorized TRUE

Common Session ID 000000000000FB1B0A58F78

Acct Session ID 0x00000000

Auth Method Status List

Method SAE

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

WLAN-beveiligingsconfiguratie:

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

General **Security** Advanced Add To Policy Tags

Layer2 Layer3 AAA

WPA + WPA2
 WPA2 + WPA3
 WPA3
 Static WEP
 None

MAC Filtering

Lobby Admin Access

WPA Parameters

WPA Policy
 WPA2 Policy
 GTK Randomize
 WPA3 Policy
 Transition Disable

Fast Transition

Status
 Over the DS
 Reassociation Timeout *

WPA2/WPA3 Encryption

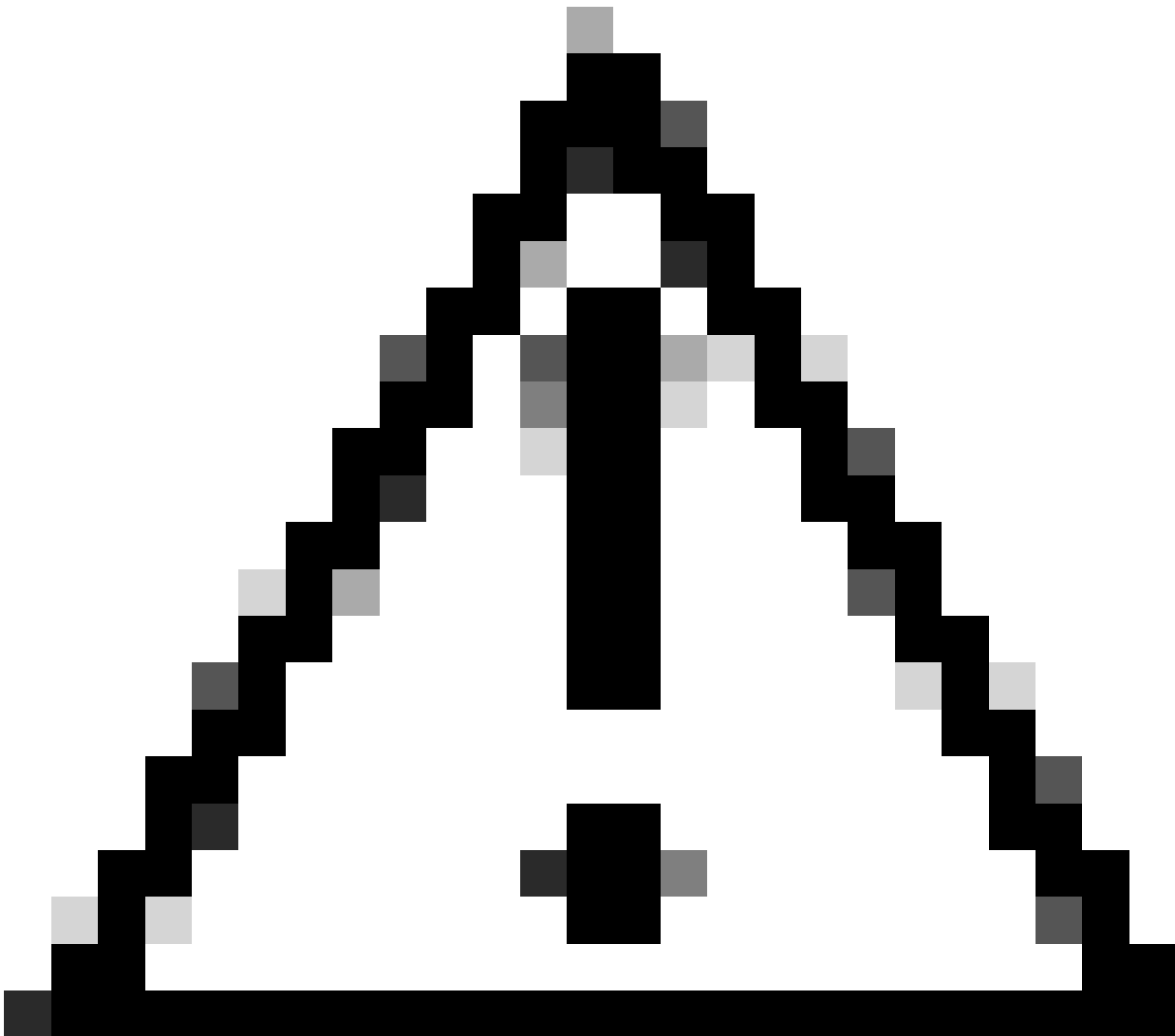
AES(OCMP128)
 OCMP256
 GCMP128
 GCMP256

Auth Key Mgmt

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

Protected Management Frame

PMF
 Association Comeback Timer*
 SA Query Time*



Waarschuwing: in het beheer van de verificatiesleutel staat de WLC toe om FT+SAE te selecteren zonder dat SAE is ingeschakeld, maar er werd geconstateerd dat de clients geen verbinding konden maken. Schakel altijd beide selectievakjes SAE en FT+SAE in als u SAE met Fast Transition wilt gebruiken.

Bekijk op WLC GUI van de WLAN security instellingen:

WiFiE_test 5 WiFiE_test [WPA3][SAE][FT + SAE][AES][FT Enabled]

Verificatie van de OTA van bakens:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
1	2023-06-12 18:34:49.35337	0.000000	Cisco_13:180:e7	Eurocast	802.11	588	5	-36 dBm	Beacon frame, S/W=22, F/W=, Flags=.....C, B=100, SSID="wifi6_test"
2	2023-06-12 18:34:49.42754	0.102287	Cisco_13:180:e7	Eurocast	802.11	588	5	-36 dBm	Beacon frame, S/W=27, F/W=, Flags=.....C, B=100, SSID="wifi6_test"
3	2023-06-12 18:34:49.50957	0.102287	Cisco_13:180:e7	Eurocast	802.11	588	5	-37 dBm	Beacon frame, S/W=23, 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, B=100, 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 18:34:49.79136	0.000012	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"
8	2023-06-12 18:34:49.79147	0.000071	192.168.1.15	192.168.1.121	802.11	76	5	-37 dBm	Acknowledgment, Flags=.....C
9	2023-06-12 18:34:49.79493	0.000066	Cisco_13:180:e7	Eurocast	802.11	588	5	-37 dBm	Beacon frame, S/W=22, 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 18:34:49.87495	0.000000	Netgear_48:78:95	Cisco_13:180:e7	802.11	194	5	-49 dBm	Authentication, S/W=, F/W=, Flags=.....C
13	2023-06-12 18:34:49.87495	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-37 dBm	Acknowledgment, Flags=.....C
14	2023-06-12 18:34:49.89653	0.021812	Cisco_13:180:e7	Netgear_48:78:95	802.11	194	5	-37 dBm	Authentication, S/W=54, F/W=, Flags=.....C
15	2023-06-12 18:34:49.89653	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-37 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	76	5	-37 dBm	Acknowledgment, Flags=.....C
19	2023-06-12 18:34:49.90496	0.000000	Netgear_48:78:95	Cisco_13:180:e7	802.11	130	5	-37 dBm	Authentication, S/W=7, F/W=, Flags=.....C
20	2023-06-12 18:34:49.90496	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-48 dBm	Acknowledgment, Flags=.....C
21	2023-06-12 18:34:49.90496	0.000000	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	Netgear_48:78:95	Cisco_13:180:e7	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	0.000045	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	0.016267	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	0.104029	Cisco_13:180:e7	Eurocast	802.11	588	5	-36 dBm	Beacon frame, S/W=27, F/W=, Flags=.....C, B=100, SSID="wifi6_test"
31	2023-06-12 18:34:50.20400	0.100000	Cisco_13:180:e7	Eurocast	802.11	588	5	-37 dBm	Beacon frame, S/W=22, F/W=, Flags=.....C, B=100, SSID="wifi6_test"
32	2023-06-12 18:34:50.21165	0.007615	Netgear_48:78:95	Cisco_13:180:e7	EAPOL	226	5	-55 dBm	Key (Message 2 of 4)
33	2023-06-12 18:34:50.21165	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-42 dBm	Acknowledgment, Flags=.....C
34	2023-06-12 18:34:50.21165	0.000000	Netgear_48:78:95	Eurocast	EAPOL	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 18:34:50.21434	0.000078	Netgear_48:78:95	Cisco_13:180:e7	EAPOL	199	5	-56 dBm	Key (Message 4 of 4)
37	2023-06-12 18:34:50.22364	0.000000	Netgear_48:78:95	Eurocast	EAPOL	221	5	-42 dBm	Key (Message 1 of 4)
38	2023-06-12 18:34:50.22364	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-42 dBm	Acknowledgment, Flags=.....C
39	2023-06-12 18:34:50.22872	0.006367	192.168.1.15	192.168.1.121	802.11	76	5	-42 dBm	Acknowledgment, Flags=.....C
40	2023-06-12 18:34:50.22849	0.000000	Netgear_48:78:95	Cisco_13:180:e7	802.11	119	5	-44 dBm	Trigger Buffer Status Report Poll (BSRP), Flags=.....C
41	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
42	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 + FT-bakens

Hier kunnen we Wi-Fi 6E-clients waarnemen die associëren:

Intel AX211 switch

OTA-verbinding met focus op RSN-informatie van client:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
1811	2023-06-12 18:51:39.24979	0.021337	IntelCor_98:53:8f	Cisco_13:180:e7	802.11	194	5	-42 dBm	Authentication, S/W=, F/W=, Flags=.....C
1812	2023-06-12 18:51:39.24979	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1813	2023-06-12 18:51:39.254827	0.007634	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	0.002465	IntelCor_98:53:8f	Cisco_13:180:e7	802.11	130	5	-46 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_98:53:8f	802.11	130	5	-36 dBm	Authentication, S/W=50, F/W=, Flags=.....C
1818	2023-06-12 18:51:39.263479	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-42 dBm	Acknowledgment, Flags=.....C
1819	2023-06-12 18:51:39.263479	0.000000	IntelCor_98:53:8f	Cisco_13:180:e7	802.11	250	5	-46 dBm	Association Request, S/W=2, 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 18:51:39.274142	0.018463	IntelCor_98:53:8f	Broadcast	LLC	114	5	-36 dBm	I, H(K)=7, H(S)=12; DSAP 0x02 Group, SSAP 0x02 Response
1827	2023-06-12 18:51:39.274142	0.000000	IntelCor_98:53:8f	Broadcast	LLC	114	5	-36 dBm	I, H(K)=7, H(S)=12; DSAP 0x02 Group, SSAP 0x02 Response
1828	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
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	0.003705	Cisco_13:180:e7	Broadcast	802.11	517	5	-36 dBm	Beacon frame, S/W=71, F/W=, Flags=.....C, B=100, SSID="wifi6_test_02"
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	0.055035	Cisco_13:180:e7	Broadcast	802.11	517	5	-37 dBm	Beacon frame, S/W=76, F/W=, Flags=.....C, B=100, SSID="wifi6_test_02"
1842	2023-06-12 18:51:39.389088	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	0.000135	192.168.1.15	192.168.1.121	802.11	82	5	-38 dBm	Request-to-send, Flags=.....C
1845	2023-06-12 18:51:39.398282	0.000139	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1846	2023-06-12 18:51:39.398812	0.000030	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	0.000067	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	0.000044	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	0.000052	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	0.000036	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	0.000071	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	0.000023	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 18:51:39.420712	0.003185	IntelCor_98:53:8f	Cisco_13:180:e7	EAPOL	230	5	-36 dBm	

Klantgegevens in WLC:

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The main panel displays a list of clients under the 'Clients' tab. The table has columns for Client MAC Address, IP4 Address, IP6 Address, and AP Name. The 'Security Information' tab is selected, showing 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, IIF ID, Authorized, Common Session ID, Acct Session ID, Auth Method Status List, and Method.

Pixel 6a

Het apparaat kon niet zwerven wanneer FT is ingeschakeld.

Samsung S23

Het apparaat kon niet zwerven wanneer FT is ingeschakeld.

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

WLAN-beveiligingsconfiguratie:

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The main panel displays the 'WLANs' configuration page. The 'wif6E_test' WLAN is selected and highlighted in red. The 'Security' tab is active, showing the following settings:

- General:** WPA3 is selected.
- WPA Parameters:** WPA3 Policy is selected.
- WPA2/WPA3 Encryption:** AES(CCMP128) and CCMP256 are selected.
- Protected Management Frame:** PMF is set to Required.
- Auth Key Mgmt:** SAE, OWE, and 802.1x-SHA256 are selected.

WPA3 Enterprise 802.1x-SHA256 + FT WLAN-beveiligingsconfiguratie

Bekijk op WLC GUI van de WLAN security instellingen:

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The main panel displays the 'WLANs' configuration page. The 'wif6E_test' WLAN is selected and highlighted in red. The 'Security' tab is active, showing the following settings:

- General:** WPA3 is selected.
- WPA Parameters:** WPA3 Policy is selected.
- WPA2/WPA3 Encryption:** AES(CCMP128) and CCMP256 are selected.
- Protected Management Frame:** PMF is set to Required.
- Auth Key Mgmt:** SAE, OWE, and 802.1x-SHA256 are selected.

Hier kunnen we de Live-logboeken van ISE zien met de authenticaties die van elk apparaat

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
878	1.408897	0.263322	Cisco_08:00:18:18	Broadcast	802.11	428	69-37	dbm	Beacon frame, SN=3662, PWR=, Flags=.....C, BI=100, SSID=W
880	1.408907	0.143770	Cisco_72:8a:96	Broadcast	802.11	204	69-37	dbm	Probe Request, SN=3662, PWR=, Flags=.....C, SSID=Wifi6E, S
888	1.563162	0.000405	Cisco_08:00:18:18	Broadcast	802.11	428	69-37	dbm	Beacon frame, SN=3662, PWR=, Flags=.....C, BI=100, SSID=W
892	1.564878	0.000716	Cisco_08:00:18:18	Broadcast	802.11	374	69-37	dbm	Probe Response, SN=3662, PWR=, Flags=.....C, BI=100, SSID=W
928	1.675576	0.114498	Cisco_08:00:18:18	Broadcast	802.11	428	69-37	dbm	Beacon frame, SN=3662, PWR=, Flags=.....C, BI=100, SSID=W
932	1.675989	0.000000	Cisco_08:00:18:18	Cisco_08:00:18:18	802.11	368	69-37	dbm	Authentication, SN=0111, PWR=, Flags=.....C
932	1.675989	0.000000	192.168.1.121	192.168.1.121	802.11	76	69-37	dbm	Acknowledgment, Flags=.....C
923	1.679651	0.003842	Cisco_08:00:18:18	Google_72:8a:96	802.11	108	69-37	dbm	Authentication, SN=14, PWR=, Flags=.....C
924	1.679651	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-34	dbm	Acknowledgment, Flags=.....C
925	1.682828	0.006598	Cisco_72:8a:96	Cisco_08:00:18:18	802.11	262	69-34	dbm	Association Request, SN=0002, PWR=, Flags=.....C, SSID=W
926	1.682181	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-37	dbm	Acknowledgment, Flags=.....C
930	1.792511	0.023970	Cisco_08:00:18:18	Google_72:8a:96	802.11	313	69-37	dbm	Association Request, SN=0, PWR=, Flags=.....C
931	1.792511	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-13	dbm	Acknowledgment, Flags=.....C
932	1.792629	0.006620	Google_72:8a:96	Google_72:8a:96	EAP	309	69-37	dbm	Request, Identity
933	1.792629	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-11	dbm	Acknowledgment, Flags=.....C
939	1.747377	0.017007	Google_72:8a:96	Cisco_08:00:18:18	EAP	117	69-33	dbm	Response, Identity
940	1.747377	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-37	dbm	Acknowledgment, Flags=.....C
942	1.794248	0.012047	Cisco_08:00:18:18	Google_72:8a:96	EAP	110	69-37	dbm	Request, Protected EAP (EAP-PEAP)
943	1.794248	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-11	dbm	Acknowledgment, Flags=.....C
945	1.798896	0.005672	Cisco_08:00:18:18	Broadcast	802.11	428	69-37	dbm	Beacon frame, SN=3662, PWR=, Flags=.....C, BI=100, SSID=W
946	1.794884	0.000188	Google_72:8a:96	Cisco_08:00:18:18	LIC	124	69-37	dbm	1, N(*)=0, N(S)=; SOAP Error Individual, SOAP Network Response
949	1.794517	0.018971	Google_72:8a:96	Cisco_08:00:18:18	EAP	110	69-37	dbm	Request, Protected EAP (EAP-PEAP)
950	1.794517	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-37	dbm	Acknowledgment, Flags=.....C
956	1.794529	0.015081	Cisco_08:00:18:18	Google_72:8a:96	EAP	1116	69-37	dbm	Request, Protected EAP (EAP-PEAP)
957	1.794529	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-37	dbm	Acknowledgment, Flags=.....C
958	1.797058	0.002510	Google_72:8a:96	Cisco_08:00:18:18	EAP	110	69-37	dbm	Request, Protected EAP (EAP-PEAP)
959	1.797058	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-37	dbm	Acknowledgment, Flags=.....C
960	1.801724	0.004656	Cisco_08:00:18:18	Google_72:8a:96	TLV1.2	382	69-37	dbm	Ignored Unknown Record
961	1.801724	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-39	dbm	Acknowledgment, Flags=.....C
963	1.820671	0.018709	Google_72:8a:96	Cisco_08:00:18:18	EAP	110	69-37	dbm	Client key exchange, Change Cipher Spec, Encrypted Handshake M
964	1.820671	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-37	dbm	Acknowledgment, Flags=.....C
965	1.820990	0.004317	Cisco_08:00:18:18	Google_72:8a:96	TLV1.2	161	69-37	dbm	Change Cipher Spec, Encrypted Handshake Message
966	1.820990	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-39	dbm	Acknowledgment, Flags=.....C
968	1.820920	0.004229	Google_72:8a:96	Cisco_08:00:18:18	EAP	110	69-39	dbm	Request, Protected EAP (EAP-PEAP)
969	1.820920	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-37	dbm	Acknowledgment, Flags=.....C
971	1.831178	0.003960	Cisco_08:00:18:18	Google_72:8a:96	TLV1.2	144	69-37	dbm	Application data
972	1.831178	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-39	dbm	Acknowledgment, Flags=.....C
973	1.831728	0.004169	Google_72:8a:96	Cisco_08:00:18:18	TLV1.2	132	69-39	dbm	Application data
974	1.831728	0.000078	192.168.1.15	192.168.1.121	802.11	76	69-37	dbm	Acknowledgment, Flags=.....C
976	1.840795	0.003290	Cisco_08:00:18:18	Google_72:8a:96	TLV1.2	171	69-37	dbm	Application data
977	1.840795	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-39	dbm	Acknowledgment, Flags=.....C
978	1.845522	0.004817	Google_72:8a:96	Cisco_08:00:18:18	TLV1.2	206	69-39	dbm	Application data
979	1.845522	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-37	dbm	Acknowledgment, Flags=.....C
984	1.848494	0.013072	Cisco_08:00:18:18	Google_72:8a:96	TLV1.2	190	69-37	dbm	Application data
985	1.848494	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-39	dbm	Acknowledgment, Flags=.....C
986	1.856887	0.002115	Google_72:8a:96	Cisco_08:00:18:18	TLV1.2	145	69-48	dbm	Application data
987	1.856887	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-37	dbm	Acknowledgment, Flags=.....C
988	1.870858	0.003771	Cisco_08:00:18:18	Broadcast	802.11	428	69-37	dbm	Beacon frame, SN=3662, PWR=, Flags=.....C, BI=100, SSID=W
989	1.870858	0.000000	192.168.1.15	Google_72:8a:96	TLV1.2	143	69-37	dbm	Application data
990	1.870858	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-39	dbm	Acknowledgment, Flags=.....C
992	1.877128	0.006470	Google_72:8a:96	Cisco_08:00:18:18	EAP	110	69-38	dbm	Request, Protected EAP (EAP-PEAP)
993	1.877128	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-37	dbm	Acknowledgment, Flags=.....C
996	1.920065	0.002917	Cisco_08:00:18:18	Google_72:8a:96	EAP	110	69-37	dbm	Request, Protected EAP (EAP-PEAP)
997	1.920065	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-39	dbm	Acknowledgment, Flags=.....C
998	1.920065	0.000000	Cisco_08:00:18:18	Google_72:8a:96	EAPOL	223	69-37	dbm	Key (Message 1 of 4)
999	1.920065	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-39	dbm	Acknowledgment, Flags=.....C
1000	1.920255	0.000000	Cisco_08:00:18:18	Google_72:8a:96	EAPOL	346	69-37	dbm	Key (Message 2 of 4)
1001	1.920255	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-37	dbm	Acknowledgment, Flags=.....C
1004	1.920677	0.003422	Cisco_08:00:18:18	Google_72:8a:96	EAPOL	423	69-37	dbm	Key (Message 3 of 4)
1005	1.920677	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-39	dbm	Acknowledgment, Flags=.....C
1006	1.920886	0.000000	Cisco_08:00:18:18	EAPOL	199	69-39	dbm	Key (Message 4 of 4)	
1007	1.920886	0.000000	192.168.1.15	192.168.1.121	802.11	76	69-37	dbm	Acknowledgment, Flags=.....C

```

> Frame 925: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits) on interface DeviceWPF_04578005-2998-4006-8C31-C3A13
> Ethernet II, Src: Cisco_08:00:18:18:18:18, Dst: Anderson_07:1c:96 (08:1c:96:07:1c:96)
> Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.121
> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
> AiroHw/0x1f0000 encapsulated IEEE 802.11
> IEEE 802.11 radio information
> IEEE 802.11 Association Request, Flags: .....C
> Tagged parameters (167 bytes)
> Fixed parameters (4 bytes)
> Tagged parameters (167 bytes)
  > Tag: SSID parameter set: "Wifi6E_test"
  > Tag: Supported Rates (6R), 9, 12(18), 18, 24(18), 36, 48, 54, [Mbit/sec]
  > Tag: Power Capability Mtr: 7, Max: 29
  > Tag: Supported Channels
  > Tag: RSN Information
  > Tag Number: RSN Information (48)
  > Tag Length: 28
  RSN Version: 1
  > Group Cipher Suite: 00:0f:ac (See IEEE 802.11) AES (CCM)
  Pairwise Cipher Suite Count: 1
  > Pairwise Cipher Suite List: 00:0f:ac (See IEEE 802.11) AES (CCM)
  Auth Key Management (AKM) Suite Count: 1
  > Auth Key Management (AKM) List: 00:0f:ac (See IEEE 802.11) FT over IEEE 802.1X
  > Auth Key Management (AKM) OUI: 00:0f:ac (See IEEE 802.11)
  > Auth Key Management (AKM) type: FT over IEEE 802.1X (1)
  > RSN Capabilities: 00:00
  .....0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
  .....0 = RSN No Pairwise capabilities: Transmitter can support MP default key @ simultaneously wdt
  .....0 = RSN PTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/TKkeySA (0x0)
  .....00 = 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 MIC11-band RSN: false
  .....0 = Perkey Enabled: false
  .....0 = Extended key ID for Individually Addressed Frames: Not supported
  PMSK Count: 0
  PMSK List:
  > Group Management Cipher Suite: 00:0f:ac (See IEEE 802.11) BIP (128)
  > Tag: W Enabled Capabilities (5 octets)
  > Tag: Mobility domain
  > Tag: Supported Operating Classes
  > Tag: Extended Capabilities (20 octets)
  > Ext Tag: HE Capabilities
  > Ext Tag: HE 4-0 Band Capabilities
  > Tag: Vendor Specific: Broadcom
  Tag Number: Vendor Specific (221)
  Tag Length: 10
  OUI: 00:18:18 (Broadcom)
  Vendor Specific OUI Type: 2
  Vendor Specific Data: 000000000000
  > Tag: Vendor Specific: Microsoft Corp.: WPVUE: Information Element
  
```

WPA3 Enterprise 802.1x + FT Pixel6a Association

Klantgegevens in WLC:

WPA3 Enterprise 802.1x + FT Pixel6a Clientgegevens

Stel scherp op het roamtype Over the Air waar we het roamtype 802.11R kunnen zien:

Samsung S23

OTA-verbinding met focus op RSN-informatie van client:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
1246	8.295985	0.102133	Cisco_dfi:08:18	Broadcast	802.11	364	69	-39 dBm	Beacon frame, SW=085, Fw=0, Flags=.....C, B1=100, SSID="wif
1247	8.401935	0.102170	Cisco_dfi:08:18	Broadcast	802.11	364	69	-40 dBm	Beacon frame, SW=086, Fw=0, Flags=.....C, B1=100, SSID="wif
1248	8.504375	0.102420	Cisco_dfi:08:18	Broadcast	802.11	364	69	-39 dBm	Beacon frame, SW=087, Fw=0, Flags=.....C, B1=100, SSID="wif
1249	8.606824	0.102419	Cisco_dfi:08:18	Broadcast	802.11	364	69	-40 dBm	Beacon frame, SW=088, Fw=0, Flags=.....C, B1=100, SSID="wif
1251	8.612759	0.005945	Cisco_dfi:08:18	Broadcast	802.11	312	69	-40 dBm	Probe Response, SW=089, Fw=0, Flags=.....C, B1=100, SSID="w
1258	8.701133	0.096374	Cisco_dfi:08:18	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_dfi:08:18	802.11	235	69	-48 dBm	Authentication, SW=099, Fw=0, Flags=.....C
1261	8.786422	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-39 dBm	Acknowledgement, Flags=.....C
1262	8.790571	0.004159	Cisco_dfi:08:18	Samsung_c9:e3:71	802.11	247	69	-39 dBm	Authentication, SW=118, Fw=0, Flags=.....C
1263	8.790571	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-47 dBm	Acknowledgement, Flags=.....C
1265	8.796429	0.005968	Samsung_c9:e3:71	Cisco_dfi:08:18	802.11	485	69	-48 dBm	Association Request, SW=100, Fw=0, Flags=.....C, SSID="wif
1266	8.796429	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-39 dBm	Acknowledgement, Flags=.....C
1268	8.800749	0.005639	Samsung_c9:e3:71	Broadcast	LLC	114	69	-39 dBm	S, Func=03, N(5)=17; DSAP 0x0a Group, SSAP 0x0a Command
1269	8.807940	0.003362	Cisco_dfi:08:18	Samsung_c9:e3:71	802.11	413	69	-39 dBm	Association Response, SW=0, Fw=0, Flags=.....C
1270	8.807940	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-48 dBm	Acknowledgement, Flags=.....C
1271	8.807940	0.000000	Samsung_c9:e3:71	Broadcast	LLC	120	69	-39 dBm	I P, N(1)=11, N(5)=19; DSAP 0x08 Individual, SSAP 0x0a Respon
1272	8.813121	0.003581	Cisco_dfi:08:18	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_Sci:F8:0c	Samsung_c9:e3:71	LLC	183	69	-40 dBm	U, Func=01C; DSAP 0x0a Group, SSAP 0x0a Command
1274	8.832754	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-58 dBm	Acknowledgement, Flags=.....C
1275	8.832754	0.000000	Cisco_Sci:F8:0c	Samsung_c9:e3:71	LLC	183	69	-49 dBm	U, Func=Unknown; DSAP Texas Instruments Group, SSAP 0x28 Respo
1276	8.832817	0.000063	192.168.1.15	192.168.1.121	802.11	76	69	-58 dBm	Acknowledgement, Flags=.....C
1277	8.800540	0.007723	Samsung_c9:e3:71	Broadcast	LLC	144	69	-46 dBm	S P, Func=02, N(5)=12; DSAP 0x0a Individual, SSAP 0x0a Respon
1278	8.800540	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-40 dBm	Acknowledgement, Flags=.....C
1280	8.804143	0.003083	Cisco_dfi:08:18	Samsung_c9:e3:71	802.11	118	69	-47 dBm	Action, SW=1, Fw=0, Flags=p.....C
1281	8.804143	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-47 dBm	Acknowledgement, Flags=.....C
1282	8.804803	0.000660	Samsung_c9:e3:71	Cisco_dfi:08:18	802.11	115	69	-47 dBm	Action, SW=0, Fw=0, Flags=p.....C
1283	8.804803	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-40 dBm	Acknowledgement, Flags=.....C
1284	8.806878	0.002075	Altiocel_a_36:59:af	Samsung_c9:e3:71	LLC	197	69	-50 dBm	I P, N(1)=25, N(5)=08; DSAP 0x0a Individual, SSAP 0x0a Command
1286	8.913192	0.007034	Cisco_dfi:08:18	Broadcast	802.11	364	69	-41 dBm	Beacon frame, SW=113, Fw=0, Flags=.....C, B1=100, SSID="wif
1287	8.950493	0.036381	Cisco_dfi:08:18	Broadcast	802.11	364	69	-39 dBm	Acknowledgement, Flags=.....C
1322	8.975553	0.029908	192.168.1.15	192.168.1.121	802.11	76	69	-39 dBm	Acknowledgement, Flags=.....C
1372	9.055519	0.040566	Cisco_dfi:08:18	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_dfi:08:18	Broadcast	802.11	364	69	-39 dBm	Beacon frame, SW=115, Fw=0, Flags=.....C, B1=100, SSID="wif
1600	9.176834	0.058311	192.168.1.15	192.168.1.121	802.11	76	69	-40 dBm	Acknowledgement, Flags=.....C
1702	9.221145	0.044131	Cisco_dfi:08:18	Broadcast	802.11	364	69	-39 dBm	Beacon frame, SW=116, Fw=0, Flags=.....C, B1=100, SSID="wif
1933	9.124397	0.102062	Cisco_dfi:08:18	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_dfi:08:18	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_dfi:08:18	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_dfi:08:18	Broadcast	802.11	364	69	-38 dBm	Beacon frame, SW=120, Fw=0, Flags=.....C, B1=100, SSID="wif
1946	9.731295	0.102275	Cisco_dfi:08:18	Broadcast	802.11	364	69	-39 dBm	Beacon frame, SW=121, Fw=0, Flags=.....C, B1=100, SSID="wif
1948	9.835864	0.102569	Cisco_dfi:08:18	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_dfi:08:18	802.11	122	69	-45 dBm	Action, SW=0, Fw=0, Flags=p.....C
1952	9.825936	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-40 dBm	Acknowledgement, Flags=.....C
1953	9.826083	0.000057	192.168.1.15	192.168.1.121	802.11	76	69	-40 dBm	Acknowledgement, Flags=.....C
1954	9.917895	0.011002	Cisco_dfi:08:18	Broadcast	802.11	364	69	-40 dBm	Beacon frame, SW=123, Fw=0, Flags=.....C, B1=100, SSID="wif
1955	9.942343	0.004648	192.168.1.15	192.168.1.121	802.11	76	69	-40 dBm	Acknowledgement, Flags=.....C

```

> Frame 1265: 485 bytes on wire (3880 bits), 485 bytes captured (3880 bits) on interface Device\MPF_04578095-2
> Ethernet II, Src: Cisco_G2:97:47 (74:11:b2:02:97:47), Dst: Universa_07:cf:06 (08:0a:8b:07:cf:06)
> Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.121
> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
> AiroPcap/OnixPcap encapsulated IEEE 802.11
> IEEE 802.11 radio information
> IEEE 802.11 Reassociation Request, Flags: .....C
> IEEE 802.11 Mgmt Management
> Fixed parameters (185 bytes)
> Tagged parameters (185 bytes)
> Tag: SSID parameter set: "wif166_test"
> Tag: Supported Rates A(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
> Tag: Power Capability M(n), 8, Max: 16
> Tag: Supported Channels
> Tag: RM Enabled Capabilities (5 octets)
> Tag: SSM 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: @#124d7f4e16ad4ecf658a5a5afaca
  Address: d514f817ab7fa085b7673e1b6d6a982cfae50fb7492e11089f01a809ca
  Domain: 08122a55c78aa18c4ef412424259780790fccefa12283f566d80b2bc3
  > 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) (3)
  Length: 4
  PMK-R0 key holder Identifier (R004-ID): 002055a2
> Tag: Supported Operating Classes
> Tag: Extended Capabilities (13 octets)
> Ext Tag: Vendor Specific: Microsoft Corp.: WPA/WPA2 Information Element
> Ext Tag: HE Capabilities
> Ext Tag: HE 6 GHz Band Capabilities
> Tag: Vendor Specific: Qualcomm Inc.
> Tag: Vendor Specific: Samsung Electronics Co., Ltd
> Tag: Vendor Specific: Samsung Electronics Co., Ltd

```

S23 FToDS-pakketten voor roaming

WPA3-Enterprise + GCMP128-algoritme + SUBITB-1X

WLAN-beveiligingsconfiguratie:

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*

Configuratie van WPA3 Enterprise Suite B-1X-beveiliging



Opmerking: FT wordt niet ondersteund in SUITEB-1X

Bekijk op WLC GUI van de WLAN security instellingen:

□ ● wif6E_test 5 wif6E_test [WPA3][SUITEB-1X][GCMP128]

Verificatie van de OTA van bakens:

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

General **Security** Advanced Add To Policy Tags

Layer2 Layer3 AAA

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP None

MAC Filtering

Lobby Admin Access

WPA Parameters

WPA Policy WPA2 Policy
GTK Randomize WPA3 Policy
Transition Disable

Fast Transition

Status
Over the DS
Reassociation Timeout *

WPA2/WPA3 Encryption

AES(CCMP128) CCMP256
GCMP128 GCMP256

Auth Key Mgmt

SUITEB192-1X

Protected Management Frame

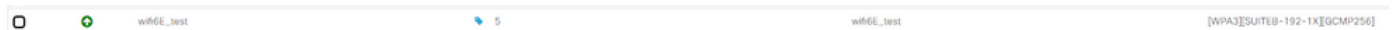
PMF
Association Comeback Timer*
SA Query Time*

WPA3 Enterprise SUITEB192-1x-beveiligingsinstellingen



Opmerking: FT wordt niet ondersteund door GCMP256+SUITEB192-1X.

WLAN's op WLC GUI WLAN-lijst:



WLAN gebruikt voor tests

Verificatie van de OTA van bakens:

Op de datum waarop dit document is geschreven, kon deze client geen verbinding maken met WPA3 Enterprise met behulp van EAP-TLS.

Dit was een kwestie aan de zijde van de cliënt waaraan wordt gewerkt en zodra het is opgelost, wordt dit document bijgewerkt.

conclusies inzake beveiliging

Na alle voorgaande tests zijn de volgende conclusies getrokken:

Protocol	Versleuteling	AKM	AKM Cipher	EAP-methode	FT-OverTA	FT-overDS
VERSCHULDIGD	AES-CCMP128 router	VERSCHULDIGD	NVT.	NVT.	NA	NA
SAE	AES-CCMP128 router	SAE (alleen H2E)	SHA256-software	NVT.	Ondersteunde producten	Ondersteund producten
Ondernemingen	AES-CCMP128 router	802.1x-SHA256-router	SHA256-software	PEAP/FAST/TLS	Ondersteunde producten	Ondersteund producten
Ondernemingen	GCMP128 router	Suite B-1x	SHA256-Suite B	PEAP/FAST/TLS	Niet ondersteund	Niet ondersteund
Ondernemingen	GCMP256 applicatie	Suite B-192	SHA384-Suite B	TLS	Niet ondersteund	Niet ondersteund

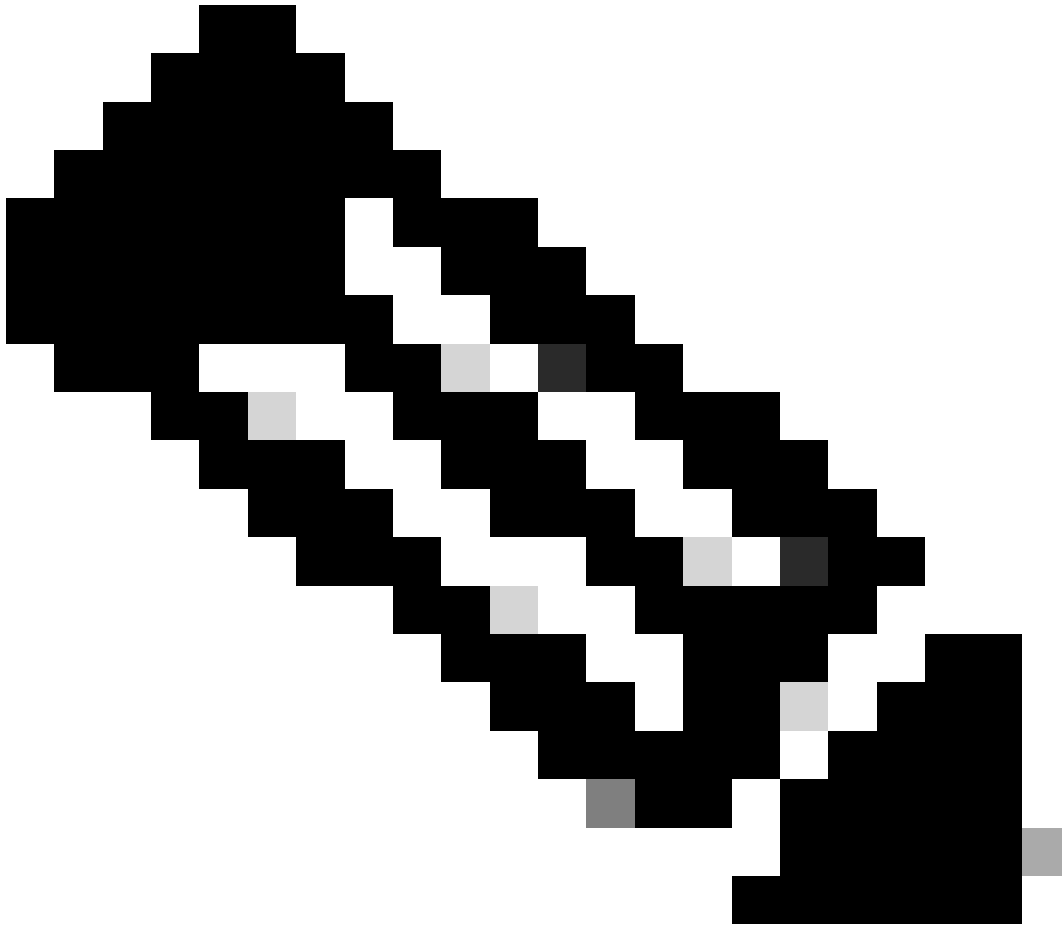
Problemen oplossen

De in dit document gebruikte probleemoplossing is gebaseerd op het online document:

[Probleemoplossing voor COS-toegangspunten](#)

De algemene richtlijn voor het oplossen van problemen is om RA-spoor in debug-modus te verzamelen van de WLC met behulp van het client mac-adres, ervoor te zorgen dat de client verbinding maakt met behulp van de apparaat mac en niet een gerandomiseerd mac-adres.

Voor de probleemoplossing via de lucht wordt aanbevolen om AP in de snuffelmodus te gebruiken om het verkeer op te nemen op het kanaal van de client die AP bedient.



Opmerking: Raadpleeg [Belangrijke informatie over debug](#) commando's voordat u debug commando's gebruikt.

Gerelateerde informatie

[Wat is Wi-Fi 6E?](#)

[Wat is Wi-Fi 6 versus Wi-Fi 6E?](#)

[Wi-Fi 6E At-a-Glance](#)

[Wi-Fi 6E: Het volgende grote hoofdstuk in Wi-Fi White Paper](#)

[Cisco Live - Architect voor draadloze netwerken van de volgende generatie met Catalyst Wi-Fi 6E access points](#)

[Software voor Cisco Catalyst 9800 Series draadloze controller, configuratiehandleiding 17.9.x](#)

[Implementatiegids voor WPA3](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.