

Lokale webverificatie configureren met externe verificatie

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[parameterkaart](#)

[Database voor verificatie](#)

[Configureren](#)

[Lokale webverificatie met lokale verificatie op de CLI](#)

[MethodListsforLocalAuthentication](#)

[Parameterkaarten](#)

[WLAN-beveiligingsparameters](#)

[Een beleidsprofiel maken](#)

[Een beleidstag maken](#)

[Een beleidstag aan een toegangspunt toewijzen](#)

[Gastgebruikersnaam maken](#)

[Lokale webverificatie met lokale verificatie via WebUI](#)

[Verifiëren](#)

[Lokale webverificatie voor lokale FlexConnect-switching](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

In dit document wordt beschreven hoe u lokale webverificatie configureert met lokale verificatie op een 9800 Wireless LAN-controller (WLC).

Voorwaarden

Cisco raadt u aan kennis te hebben van het 9800 WLC-configuratiemodel.

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco WLC 9800-serie.
- Uitgebreide kennis van webauthenticatie.

Gebruikte componenten

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

- 9800-CL WLC Cisco IOS® XE versie 17.12.5
- Cisco Access Point C9117AXI.

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

Local Web Authentication (LWA) is een verificatiemethode voor Wireless Local Area Network (WLAN) die kan worden geconfigureerd op de WLC. Wanneer een gebruiker het WLAN selecteert in de lijst met beschikbare netwerken, wordt deze doorgestuurd naar een webportaal. In dit portaal kan de gebruiker, afhankelijk van de configuratie, worden gevraagd om een gebruikersnaam en wachtwoord in te voeren, een Acceptable Use Policy (AUP) te accepteren of een combinatie van beide acties om hun verbinding te voltooien.

Raadpleeg de handleiding [Lokale webverificatie configureren](#) voor informatie over de vier typen webpagina's die tijdens het aanmeldingsproces worden weergegeven en bekijk de beschikbare opties voor het type webverificatie. U kunt ook de handleiding [Lokale webverificatie configureren met externe verificatie](#) raadplegen in het gedeelte Typen verificatie.

parameterkaart

Parameter Map is een essentieel configuratie-element op een WLC dat webverificatie mogelijk maakt. Het bestaat uit een reeks instellingen die verschillende facetten van het webverificatieproces regelen, waaronder het verificatietype, omleidings-URL's, toegevoegde parameters, time-outs en aangepaste webpagina's. Als u webgebaseerde verificatie voor een bepaalde SSID wilt activeren en beheren, moet deze kaart zijn gekoppeld aan het WLAN-profiel.

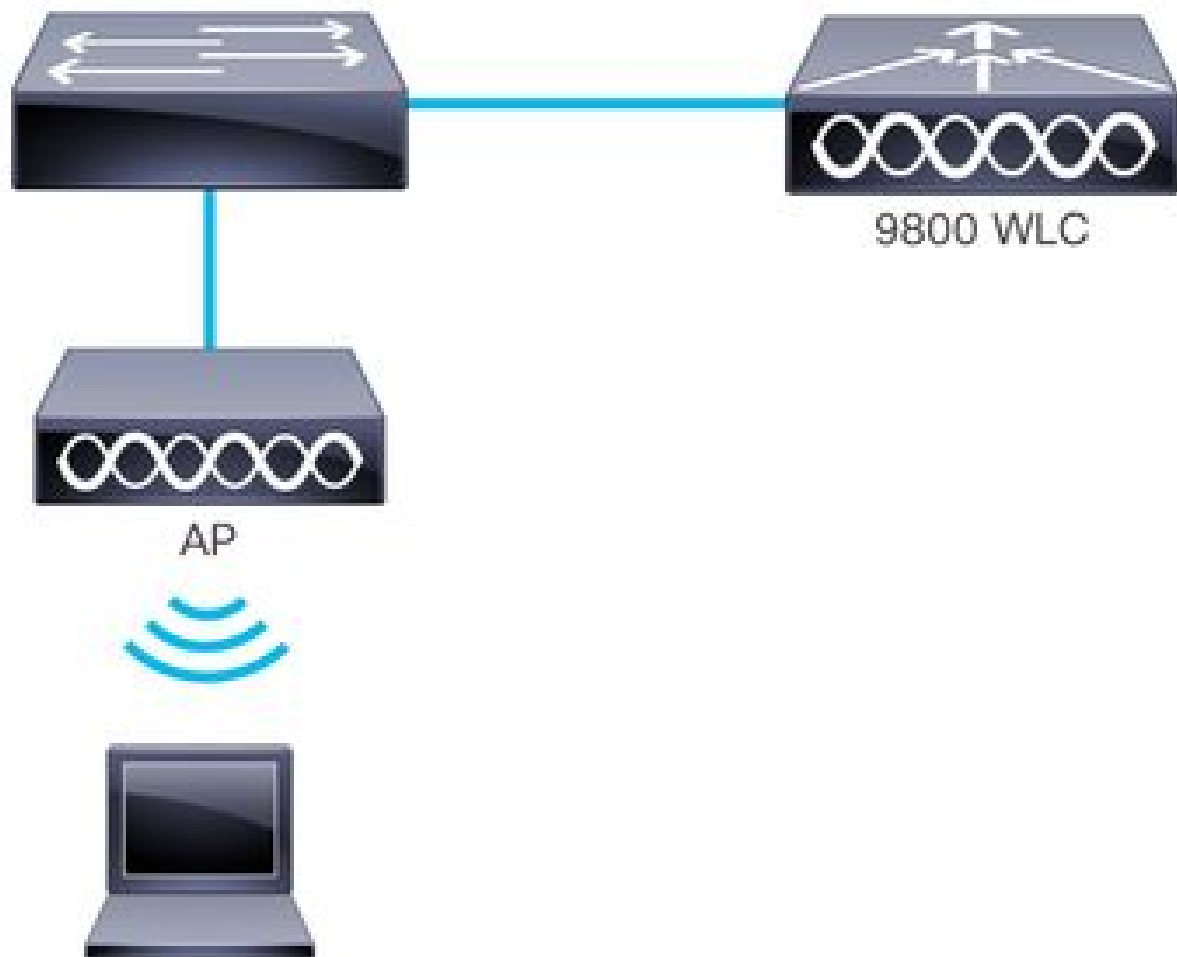
De draadloze LAN-controller wordt geleverd met een standaard globale parametertoewijzing, maar beheerders hebben de optie om aangepaste parametertoewijzingen te maken om het webverificatiegedrag aan te passen aan specifieke behoeften.

Database voor verificatie

Als de parametertoewijzing is geconfigureerd om een gebruikersnaam en wachtwoord te gebruiken, moet u de verificatiereferenties definiëren die lokaal op de WLC worden opgeslagen. Wanneer u een gastgebruikersaccount aanmaakt via de GUI, kunt u het maximum aantal gelijktijdige aanmeldingen instellen dat per gastaccount is toegestaan. Geldige waarden variëren van 0 tot 64, waarbij 0 aangeeft dat onbeperkte gelijktijdige aanmeldingen zijn toegestaan voor die gast.

LWA is voornamelijk bedoeld voor kleine implementaties. Het ondersteunt integratie met andere verificatiemethoden. U kunt de [ondersteunde combinatie van verificaties voor een client](#) controleren voor meer informatie.

De afbeelding vertegenwoordigt een generieke topologie van LWA:



Algemene topologie van LWA met lokale authenticatie

Apparaten in de netwerktopologie van LWA:

- Client/leverancier: initieert een verbindingsverzoek naar het WLAN, later naar de DHCP- en DNS-servers en reageert op communicatie van de WLC.
- Toegangspunt: Verbonden met een switch, zendt het het gast-WLAN uit en biedt draadloze connectiviteit met gastapparaten. Het staat DHCP- en DNS-verkeer toe voordat de gastgebruiker de verificatie voltooit door geldige referenties in te voeren, een AUP te accepteren of een combinatie van beide acties.
- WLC/Authenticator: beheert de toegangspunten en clientapparaten. De WLC host de omleidings-URL en handhaaft de Access Control List (ACL) die het verkeer regelt en de URL

die standaard wordt gemaakt bij het configureren van de parametertoewijzing. Het onderschept HTTP-verzoeken van gastgebruikers en leidt ze door naar een webportaal (aanmeldingspagina) waar gebruikers zich moeten authenticeren. De WLC legt gebruikersreferenties vast, verifieert gasten en controleert de lokale database om de geldigheid van de referenties te verifiëren.

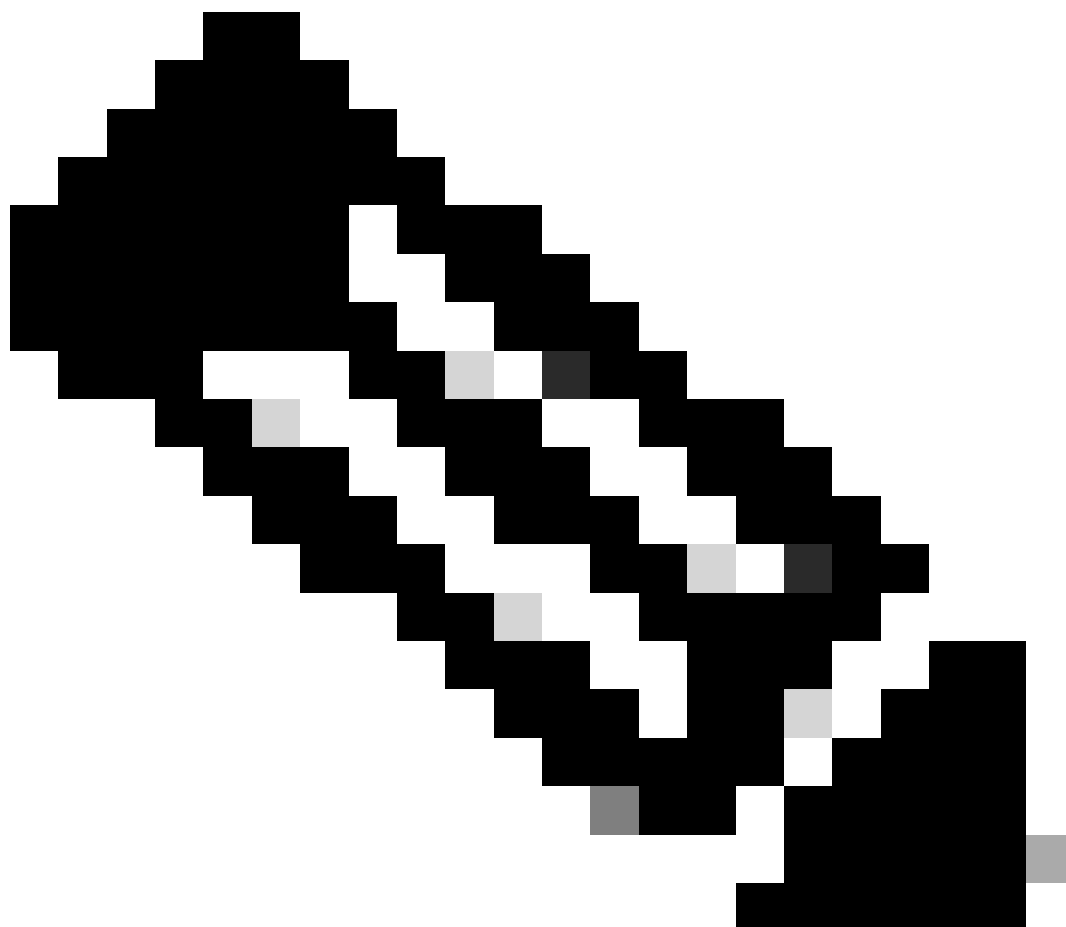
- Verificatieserver: in dit scenario fungeert de WLC als de verificatieserver. Het valideert de referenties van gastgebruikers en verleent of weigert netwerktoegang dienovereenkomstig.

Configureren

Lokale webverificatie met lokale verificatie op de CLI

Methodenlijsten voor lokale verificatie

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#aaa new-model
9800WLC(config)#aaa authentication login LWA_AUTHENTICATION local
9800WLC(config)#aaa authorization network default local
9800WLC(config)#end
```



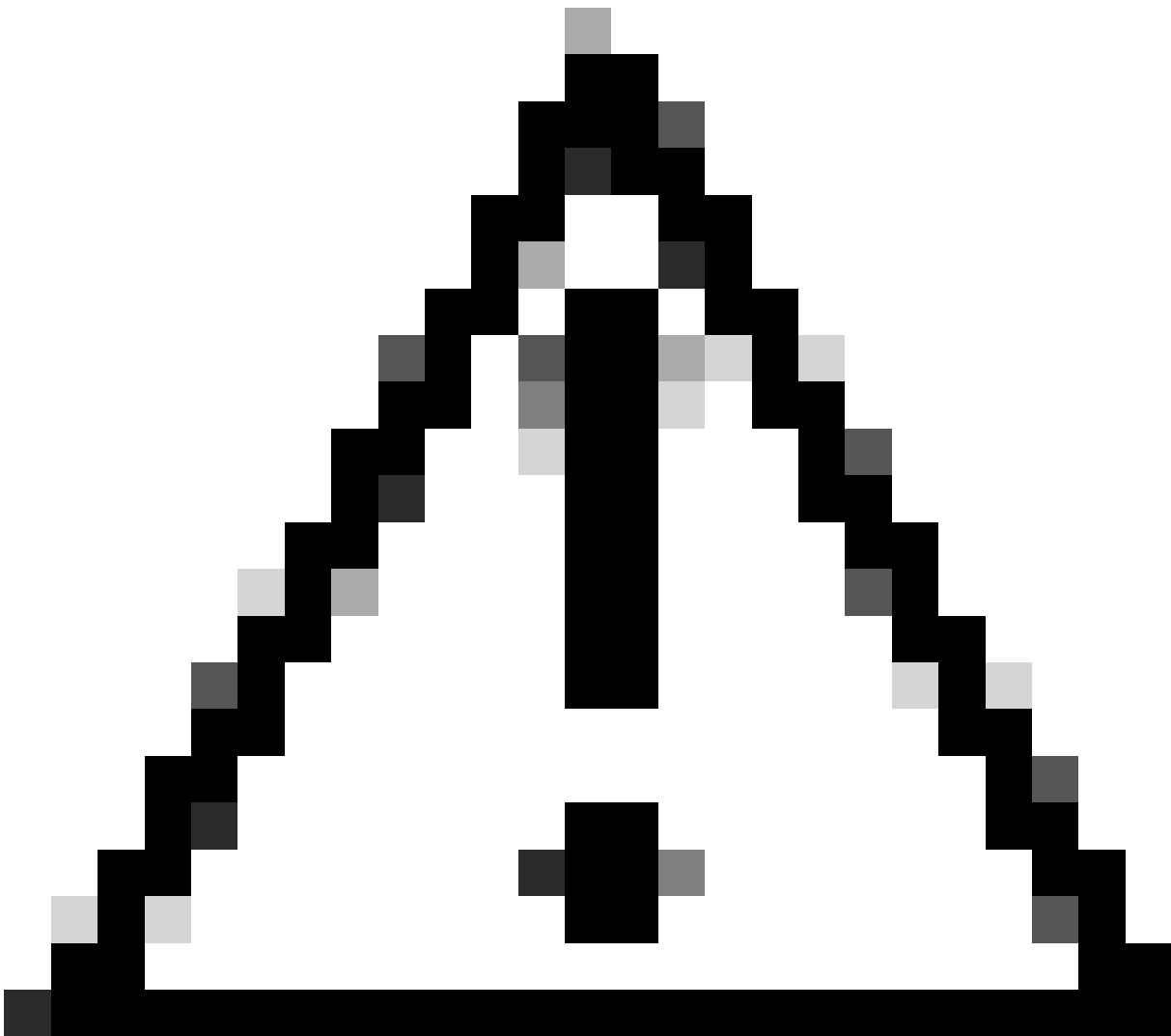
Opmerking: Zorg ervoor dat de standaard lokale netwerkautorisatie voor configuratie aaa bestaat op de WLC, zodat de lijst met lokale aanmeldingsmethoden werkt. Dit is nodig omdat de WLC de gebruiker autoriseert om het netwerk te betreden.

Parameterkaarten

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#parameter-map type webauth global
9800WLC(config-params-parameter-map)#type webauth
9800WLC(config-params-parameter-map)#virtual-ip ipv4 192.0.2.1
9800WLC(config-params-parameter-map)#trustpoint
```

```
9800WLC(config-params-parameter-map)#webauth-http-enable
```

```
9800WLC(config-params-parameter-map)#end
```



Let op: Virtual IP moet een niet-routeerbaar adres zijn dat wordt voorgesteld op RFC 5737. Standaard is IP 192.0.2.1 ingesteld. Meer informatie over virtueel IP-adres vindt u in de [best practices voor configuratie](#) van de [Cisco Catalyst 9800-reeks](#). Op AireOs was het IP-adres meestal 1.1.1.1. Dit wordt niet meer aanbevolen omdat het een openbaar IP is geworden.

De mogelijkheid om meerdere parameterkaarten te maken maakt aangepaste stromen mogelijk: aangepaste webpagina's en specifieke presentatieparameters voor elk WLAN. De globale parametermap bepaalt het Trustpoint en daarmee het certificaat dat de WLC aan de client op het omleidingsportaal presenteert. Daarnaast regelt het de soorten clientverkeer die worden

onderschept, zoals HTTP / HTTPS voor het omleidingsportaal, domein- of hostnaamomzetting voor het virtuele IP-adres. Door deze scheiding kan de globale kaart overkoepelende instellingen zoals certificaatpresentatie en verkeersonderschepping verwerken, terwijl door de gebruiker gedefinieerde parameterkaarten een gedetailleerde ervaring per WLAN bieden.

WLAN-beveiligingsparameters

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#wlan LWA_LA 1 "LWA LA"
9800WLC(config-wlan)#no security wpa
9800WLC(config-wlan)#no security wpa wpa2
9800WLC(config-wlan)#no security wpa wpa2 ciphers aes
9800WLC(config-wlan)#no security wpa akm dot1x
9800WLC(config-wlan)#security web-auth
9800WLC(config-wlan)#security web-auth authentication-list LWA_AUTHENTICATION
9800WLC(config-wlan)#security web-auth parameter-map global
9800WLC(config-wlan)#no shutdown
9800WLC(config-wlan)#end
```

Een beleidsprofiel maken

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#wireless profile policy
```

```
9800WLC(config-wireless-policy)#vlan
```

```
9800WLC(config-wireless-policy)#no shutdown
```

```
9800WLC(config-wireless-policy)#end
```

Een beleidstag maken

```
9800WLC>enable
9800WLC#configure terminal
```

```
9800WLC(config)#wireless tag policy
```

```
9800WLC(config-policy-tag)#wlan LWA_LA policy
```

```
9800WLC(config-policy-tag)# end
```

Een beleidstag aan een toegangspunt toewijzen

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#ap
```

```
>
```

```
9800WLC(config-ap-tag)#policy-tag POLICY_TAG
```

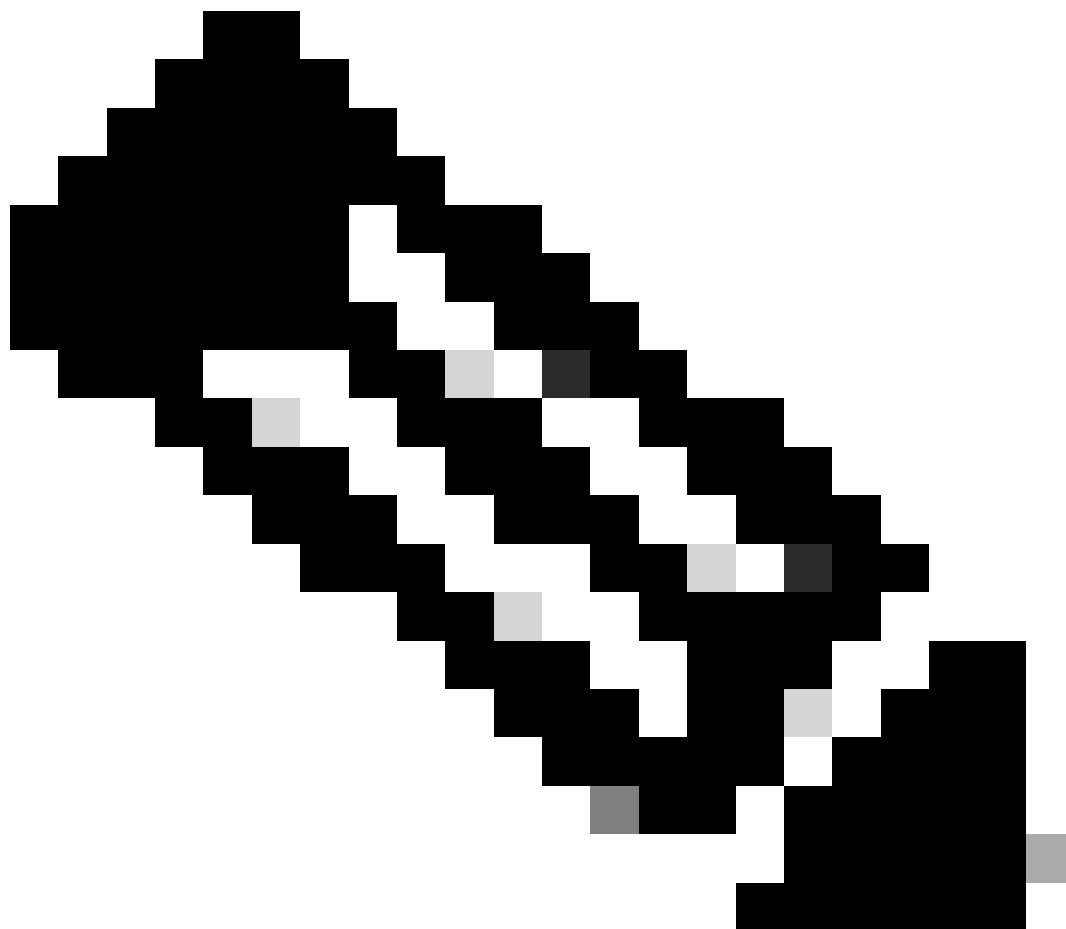
```
9800WLC(config-ap-tag)#end
```

Gastgebruikersnaam maken

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#user-name johndoe
9800WLC(config-user-name)#description Guest-User
9800WLC(config-user-name)#password 0 Cisco123
9800WLC(config-user-name)#type network-user description
```

```
guest-user lifetime year 0 month 11 day 30 hour 23
```

```
9800WLC(config-user-name)#end
```

Opmerking: Als het jaar is ingesteld op 1, kunt u bij het instellen van de levensduur voor de gastgebruiker de volgende parameters niet opgeven: maanden, dagen, uren en minuten, omdat de maximale levensduur 1 jaar is.

Lokale webverificatie met lokale verificatie via WebUI

Methodenlijsten voor lokale verificatie

Navigeer naar Configuratie > Beveiliging > AAA > Methodenlijst > Authenticatie > Toevoegen om de methodenlijst later te maken voor gebruik in de WLAN-configuratie.

Configuration > Security > AAA [Show Me How](#)

[+ AAA Wizard](#)

Servers / Groups **AAA Method List** AAA Advanced

Authentication
Authorization
Accounting

[+ Add](#) [- Delete](#)

Name	Type	Group Type	Group1	Group2
☐ default	login	local	N/A	N/A

Quick Setup: AAA Authentication

Method List Name*

LWA-AUTHENTICATION

Type*

login

i

Group Type

local

i

Available Server Groups

radius
ldap
tacacs+
AAA-group

>
<
>>
<<

Assigned Server Groups

^
^
v
v

Cancel

Apply to Device

Nadat u op Toepassen op apparaat hebt geklikt, bevestigt u het maken van de AAA-methodenlijst:

Zorg ervoor dat er een lijst met lokale autorisatiemethoden is, dit is een vereiste voor de lijst met lokale aanmeldingsmethoden die is gemaakt om te werken.

Configuratie > Beveiliging > AAA > Methodenlijst AAA > Autorisatie > Toevoegen

Configuration > Security > AAA [Show Me How](#)

[+ AAA Wizard](#)

Servers / Groups **AAA Method List** AAA Advanced

Authentication

Authorization

Accounting

[+ Add](#) [- Delete](#)

Name	Type	Group Type	Group1	Group2
☐ default	exec	local	N/A	N/A

Quick Setup: AAA Authorization

Method List Name*

Type* ⓘ

Group Type ⓘ

Authenticated ☐

Available Server Groups

- radius
- ldap
- tacacs+
- AAA-group

Assigned Server Groups

[Cancel](#) [Apply to Device](#)

Nadat u op Toepassen op apparaat hebt geklikt, bevestigt u het maken van de AAA-methodenlijst:

Configuration > Security > AAA

[+ AAA Wizard](#)

Servers / Groups **AAA Method List** AAA Advanced

Authentication

Authorization

Accounting

[+ Add](#) [- Delete](#)

Name	Type	Group Type	Group1	Group2	Group3	Group4
☐ default	exec	local	N/A	N/A	N/A	N/A
☐ default	network	local	N/A	N/A	N/A	N/A

1 - 2 of 2 items

Parameterkaarten

De globale parametertoewijzing bewerken bij Configuratie > Beveiliging > Webverificatie

Configuration > Security > Web Auth

+ Add - Delete

Selected Rows: 0

Parameter Map Name
☐ global

1 10 items per page

General

Parameter-map Name: global

Maximum HTTP connections: 100

Init-State Timeout(secs): 120

Type: webauth

Captive Bypass Portal: ☐

Disable Success Window: ☐

Disable Logout Window: ☐

Disable Cisco Logo: ☐

Sleeping Client Status: ☐

Sleeping Client Timeout (minutes): 720

Advanced

Virtual IPv4 Address: 192.0.2.1

Trustpoint: TP-self-signed-...

Virtual IPv4 Hostname:

Virtual IPv6 Address: :::::::

Web Auth intercept HTTPs: ☐

Enable HTTP server for Web Auth: ☒

Disable HTTP secure server for Web Auth: ☐

Banner Configuration

Banner Title:

Banner Type: ☒ None ☐ Banner Text ☐ Read From File

Selecteer het type webverificatie dat moet worden gebruikt, Virtual IP en het Trustpoint dat de WLC op het webportaal weergeeft. In dit geval wordt het Self-Signed-certificaat geselecteerd en zal dit waarschijnlijk een disclaimer veroorzaken van het soort "uw verbinding is niet privé-net:: ERR_CERT_AUTHORITY_INVALID", omdat dit een Lokaal significant certificaat (LSC) is en niet is ondertekend door een herkenbare CA op internet. Om dit te wijzigen, gebruikt u een door derden ondertekend certificaat. Details worden weergegeven op [MVO-certificaten genereren en downloaden op Catalyst 9800 WLC's](#) of er is een video-optie die de upload- en Trustpoint-creatie uitlegt [Vernieuwingscertificaten voor WebAuth & WebAdmin op Cisco 9800 WLC | Secure Wireless LAN Controller Setup](#).

Edit Web Auth Parameter



General

Advanced

Parameter-map Name

Maximum HTTP connections

Init-State Timeout(secs)

Type

Captive Bypass Portal ☐

Disable Success Window ☐

Disable Logout Window ☐

Disable Cisco Logo ☐

Sleeping Client Status ☐

Sleeping Client Timeout (minutes)

Virtual IPv4 Address

Trustpoint

Virtual IPv4 Hostname

Virtual IPv6 Address

Web Auth intercept HTTPs ☐

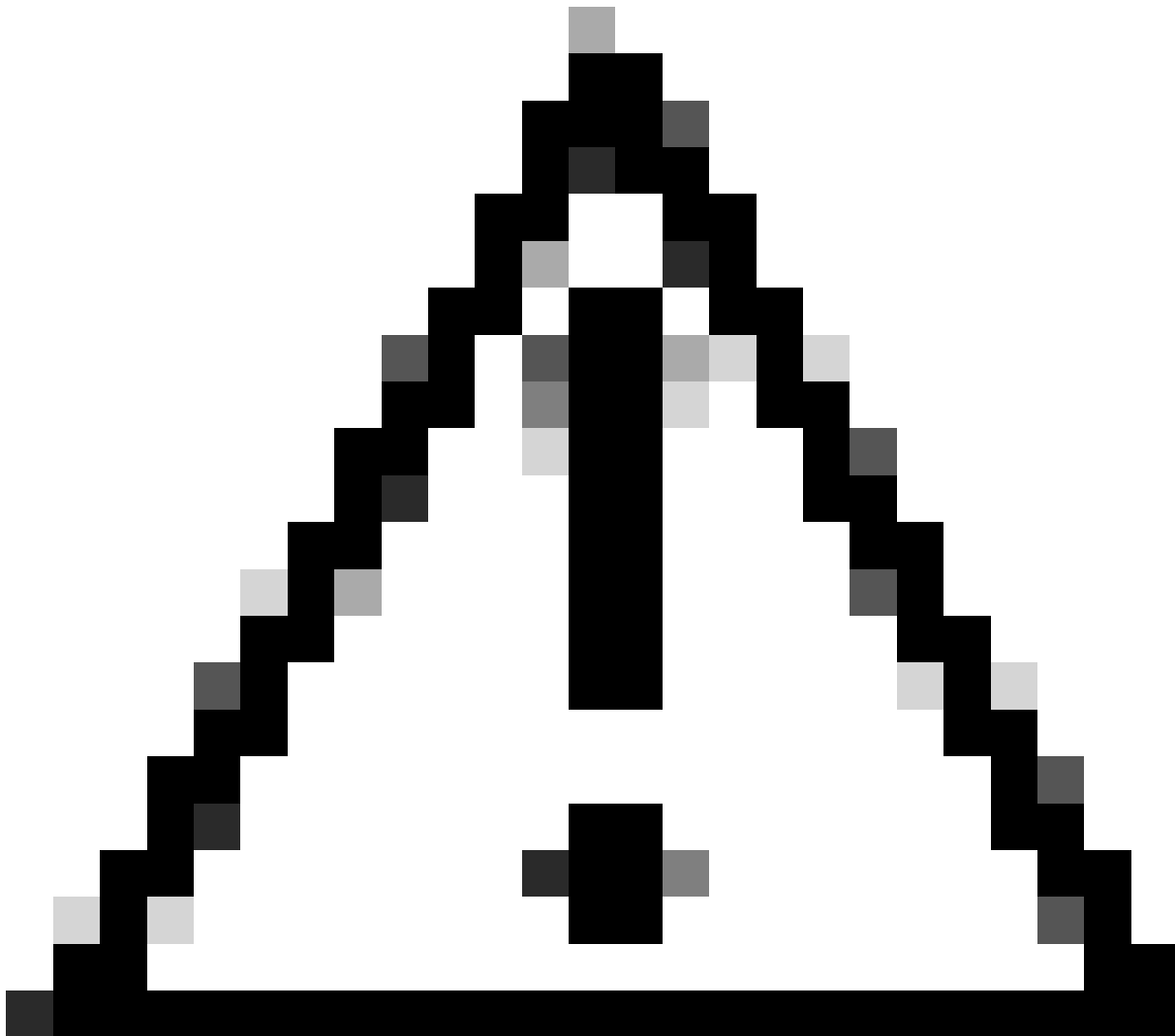
Enable HTTP server for Web Auth ☒

Disable HTTP secure server for Web Auth ☐

Banner Configuration

Banner Title

Banner Type ☒ None ☐ Banner Text ☐ Read From File



Waarschuwing: Als HTTP wereldwijd is uitgeschakeld op de 9800, moet u ervoor zorgen dat de HTTP-server inschakelen voor Web Auth is ingeschakeld, omdat Cisco de afhankelijkheid van deze processen heeft gescheiden. Van klanten of leveranciers wordt verwacht dat ze een HTTP-verbindingsproces starten en dat die sessie door de controller wordt onderschept om het webportaal te presenteren. Om die reden wordt het niet aanbevolen om Web Auth Intercept HTTPS in te schakelen tenzij absoluut vereist, omdat deze instelling voor de meeste implementaties overbodig is en het CPU-gebruik van de controller kan verhogen, wat mogelijk van invloed is op de prestaties.

WLAN-beveiligingsparameters

Navigeer naar Configuratie > Tags en profielen > WLAN's, klik op Toevoegen.

⚠ 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*

LWA_LA

SSID*

LWA LA

WLAN ID*

1

Status

ENABLED ☒

Broadcast SSID

ENABLED ☒

Radio Policy ⓘ

6 GHz

Status

ENABLED ☒☒ Slot 2/3

✖ WPA3 Enabled

✔ Dot11ax Enabled

5 GHz

Status

ENABLED ☒☒ Slot 0☒ Slot 1☒ Slot 2

2.4 GHz

Status

ENABLED ☒☒ Slot 0802.11b/g
Policy

802.11b/g ▼

Selecteer op het tabblad Beveiliging voor Layer2 Geen.

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

⚠ To review the necessary considerations for ensuring WLAN compatibility with Wi-Fi 7 security [click here](#).

☐ WPA + WPA2

☐ WPA2 + WPA3

☐ WPA3

☐ Static WEP

☒ None

MAC Filtering

☐

OWE Transition Mode

☐

Lobby Admin Access

☐

Fast Transition

Status

Adaptive Ena...

Over the DS

☐

Reassociation Timeout *

20

Selecteer op het tabblad Beveiliging voor Layer3 het vak Webbeleid de eerder geconfigureerde parametertoewijzing in het vervolgkeuzemenu en de verificatielijst.

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

Web Policy

☒

Web Auth Parameter Map

global

Authentication List

LWA_AUTHENTI...

[<< Hide](#)

On MAC Filter Failure

☐

Splash Web Redirect

DISABLED

Preauthentication ACL

IPv4

None

IPv6

None

For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device

Een beleidsprofiel maken

Als u het beleidsprofiel wilt maken dat aan het WLAN-profiel moet worden gekoppeld, gaat u naar Configuratie > Codes en profielen > Beleid.

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

LWA_CentralSW

Description

Enter Description

Status

ENABLED

Passive Client

DISABLED

IP MAC Binding

ENABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

Inline Tagging

☐

SGACL Enforcement

☐

Default SGT

2-65519

WLAN Switching Policy

Central Switching

ENABLED

Central Authentication

ENABLED

Central DHCP

ENABLED

Flex NAT/PAT

DISABLED

Selecteer op het tabblad Toegangsbeleid het VLAN van waaruit de clients/leveranciers een IP-adres aanvragen.

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General **Access Policies** QOS and AVC Mobility Advanced

RADIUS Profiling

☐

HTTP TLV Caching

☐

DHCP TLV Caching

☐

WLAN Local Profiling

Global State of Device Classification

Enabled ⓘ

Local Subscriber Policy Name

Search or Select ▼



VLAN

VLAN/VLAN Group

2622 ▼



Multicast VLAN

Enter Multicast VLAN

WLAN ACL

IPv4 ACL

Search or Select ▼



IPv6 ACL

Search or Select ▼



URL Filters ⓘ

Pre Auth

Search or Select ▼



Post Auth

Search or Select ▼



Een beleidstag maken

Voor deze configuratiehandleiding hebben we een aangepaste beleidstag gemaakt met de naam LWA.

Edit Policy Tag

⚠ Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name*

LWA

Description

LWA_LA

✓ WLAN-POLICY Maps: 1

+ Add

× Delete

WLAN Profile	Policy Profile
☐ LWA_LA	LWA_CentralSW
1 - 1 of 1 items	

WLAN en beleidsprofiel koppelen

Als u de beleidsregels voor het overschakelen vanuit het beleidsprofiel en het WLAN-netwerk wilt koppelen, gaat u naar Configuratie > Codes en profielen > WLAN's, selecteert u het WLAN-profiel en klikt u op Toevoegen aan beleidscodes.

Warning: 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**

+ Add × Delete

☐	Policy Tag	Policy Profile
☒	LWA	LWA_CentralSW

1 10 1 - 1 of 1 items

Een beleidstag aan een toegangspunt toewijzen

Als u het toegangspunt wilt labelen met de gemaakte beleidstag, gaat u naar Configuratie > Draadloos > Toegangspunten, selecteert u het toegangspunt en op het tabblad Algemeen vindt u rechts de tags die door het toegangspunt worden gebruikt.

Edit AP

General

Interfaces

High Availability

Inventory

Geolocation

Advanced

Support Bundle

General

AP Name*

9117

Location*

default location

Base Radio MAC

cc0

Ethernet MAC

c00

Admin Status

ENABLED

AP Mode

Local

Operation Status

Registered

Fabric Status

Disabled

LED Settings

LED State

ENABLED

Brightness Level

8

Flash Settings

Flash State

DISABLED

Apply

Time Statistics

Up Time

8 days 15 hrs 26 mins 48 secs

Controller Association Latency

1 sec

Tags

Policy

LWA

Site

default-site-tag

RF

default-rf-tag

Write Tag Config to AP

Version

Primary Software Version

17.12.5.41

Predownloaded Status

N/A

Predownloaded Version

N/A

Next Retry Time

N/A

Boot Version

1.1.2.4

IOS Version

17.12.5.41

Mini IOS Version

0.0.0.0

IP Config

CAPWAP Preferred Mode

IPv4

DHCP IPv4 Address

172.16.60.40

Static IP (IPv4/IPv6)

Cancel

Update & Apply to Device

Gebruikersnaam gast maken

Als u het webauth-type hebt geselecteerd op de Parameter Map, is een gastgebruikersnaam nodig om deze te maken en te navigeren naar Configuratie > Beveiliging > Gastgebruiker.

De maximale levensduur van de gebruiker is 1 jaar. U kunt anders opgeven met de beschikbare opties.

[+ Add](#) [- Delete](#)

Selected Rows: 0

☐ User Name
☐ johndoe

1 10 items per page

Edit Guest User

General

Enter User Name* johndoe

Password* 

☐ Generate password

Confirm Password

Description* Guest-User

AAA Attribute list 

No. of Simultaneous User Logins*
Enter 0 for unlimited users

Start Time 15:21:19 UTC Aug 26 2025

Expiry Time 15:21:19 UTC Aug 21 2026

Remaining Time 0 years 11 months 29 days 23 hours 34 mins 24 secs

Lifetime

Years*

Months*

Days*

Hours*

Mins*

Verifiieren

Via GUI

Cisco Catalyst 9800-CL Wireless Controller 17.12.5

Welcome admin

Monitoring > Wireless > Clients

Monitoring Sleeping Clients Excluded Clients

Selected 0 out of 1 Clients

☐	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type	Role	6E Capable
☐	9ef2.4b16.a507	172.16.74.83	fe80:9c72:4b16:fe16:a507	9117	0	LWA LA	1	WLAN	Run	11ax(2.4)	johndoe	N/A	Local	No

1 - 1 of 1 clients

Monitoring > Wireless > Clients

Clients

Sleeping Clients

Excluded Clients

Delete
Refresh

Selected 0 out of 1 Clients

	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID
☐	507	172.16.74.83	fe80::9cf2:4bff:fe16:a507	-9117	0	LWA LA

1
10

Client

360 View
General
QoS Statistics
ATF Statistics
Mobility History
Call Statistics

Client Properties

AP Properties

Security Information

Client Statistics

QoS Properties

EoGRE

MAC Address
Client MAC Type
Client DUID
IPv4 Address
IPv6 Address
User Name
Policy Profile
Flex Profile
Wireless LAN Id
WLAN Profile Name
Wireless LAN Network Name (SSID)
BSSID
Uptime(sec)
Idle state timeout
Session Timeout
Session Warning Time
Client Active State
Power Save mode
Current TxRateSet
Supported Rates
QoS Average Data Rate Upstream
QoS Realtime Average Data Rate Upstream
QoS Burst Data Rate Upstream
QoS Realtime Burst Data Rate Upstream
QoS Average Data Rate Downstream
QoS Realtime Average Data Rate Downstream
QoS Burst Data Rate Downstream
QoS Realtime Burst Data Rate Downstream
Join Time Of Client
Policy Manager State
Last Policy Manager State
Transition Disable Bitmap
User Defined (Private) Network
User Defined (Private) Network Drop
Unicast

y507
Locally Administered Address
NA
172.16.74.83
fe80::9cf2:4bff:fe16:a507
johndoe
LWA_CentralSW
N/A
1
LWA_LA
LWA LA
0cd0.f897.acc0
151 seconds
N/A
28800 sec (Remaining time: 28678 sec)
Timer not running
Active
ON
1.0
1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0
0 (kbps)
0 (kbps)
0 (kbps)
0 (kbps)
0 (kbps)
0 (kbps)
0 (kbps)
0 (kbps)
0 (kbps)
0 (kbps)
09/10/2025 21:26:11 UTC
Run
Webauth Pending
0x00
Disabled
Disabled

OK

Via CLI

```
9800WLC>enable
9800WLC#show wireless client summary
Number of Clients: 1
MAC Address      AP Name          Type ID State Protocol Method  Role
-----
9ef2.4b16.a507   xxxxx-9117 WLAN 1 Run  11ax(2.4) Web Auth Local
9800WLC#show wireless client mac-address
```

detail

- Client MAC Address : 9ef2.4b16.a507
- Client MAC Type : Locally Administered Address
- Client DUID: NA
- Client IPv4 Address : 172.16.74.83
- Client IPv6 Addresses : fe80::9cf2:4bff:fe16:a507
- Client Username : johndoe

AP MAC Address : 0cd0.f897.acc0

AP Name: xxxxx-9117

AP slot : 0

Client State : Associated

Policy Profile : LWA_CentralSW

Flex Profile : N/A

Wireless LAN Id: 1

WLAN Profile Name: LWA_LA

Wireless LAN Network Name (SSID): LWA LA

BSSID : 0cd0.f897.acc0

Connected For : 392 seconds

Protocol : 802.11ax - 2.4 GHz

Channel : 11

Client IIF-ID : 0xa0000002

Association Id : 1

Authentication Algorithm : Open System

Idle state timeout : N/A

Session Timeout : 28800 sec (Remaining time: 28455 sec)

Session Warning Time : Timer not running

Input Policy Name : None

Input Policy State : None

Input Policy Source : None

Output Policy Name : None

Output Policy State : None

Output Policy Source : None

WMM Support : Enabled

U-APSD Support : Disabled

Fastlane Support : Disabled

Client Active State : Active

Power Save : ON

Current Rate : m0 ss2

Supported Rates : 1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0

AAA QoS Rate Limit Parameters:

QoS Average Data Rate Upstream : 0 (kbps)

QoS Realtime Average Data Rate Upstream : 0 (kbps)

QoS Burst Data Rate Upstream : 0 (kbps)

QoS Realtime Burst Data Rate Upstream : 0 (kbps)

QoS Average Data Rate Downstream : 0 (kbps)

QoS Realtime Average Data Rate Downstream : 0 (kbps)

QoS Burst Data Rate Downstream : 0 (kbps)

QoS Realtime Burst Data Rate Downstream : 0 (kbps)

Mobility:

Move Count : 0

Mobility Role : Local

Mobility Roam Type : None

Mobility Complete Timestamp : 09/10/2025 21:41:11 UTC

Client Join Time:

Join Time Of Client : 09/10/2025 21:41:11 UTC

Client State Servers : None

Client ACLs : None

Policy Manager State: Run

Last Policy Manager State : Webauth Pending

Client Entry Create Time : 392 seconds

Policy Type : N/A

Encryption Cipher : None

Transition Disable Bitmap : 0x00

User Defined (Private) Network : Disabled

User Defined (Private) Network Drop Unicast : Disabled

Encrypted Traffic Analytics : No

Protected Management Frame - 802.11w : No

EAP Type : Not Applicable

VLAN Override after Webauth : No

VLAN : 2667

Multicast VLAN : 0

VRF Name : N/A

WiFi Direct Capabilities:

WiFi Direct Capable : No

Central NAT : DISABLED

Session Manager:

Point of Attachment : capwap_90400005

IIF ID : 0x90400005

Authorized : TRUE

Session timeout : 28800

Common Session ID: 044A10AC0000000F359351E3

Acct Session ID : 0x00000000

Auth Method Status List

Method : Web Auth

Webauth State : Authz

Webauth Method : Webauth

Local Policies:

Service Template : IP-Adm-V4-LOGOUT-ACL (priority 100)

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

Service Template : wlan_svc_LWA_CentralSW_local (priority 254)

VLAN : 2667

Absolute-Timer : 28800

Server Policies:

Resultant Policies:

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

VLAN Name : xxxxx

VLAN : 2667

Absolute-Timer : 28800

DNS Snooped IPv4 Addresses : None

DNS Snooped IPv6 Addresses : None

Client Capabilities

CF Pollable : Not implemented

CF Poll Request : Not implemented

Short Preamble : Not implemented

PBCC : Not implemented

Channel Agility : Not implemented

Listen Interval : 0

Fast BSS Transition Details :

Reassociation Timeout : 0

11v BSS Transition : Implemented

11v DMS Capable : No

QoS Map Capable : Yes

FlexConnect Data Switching : N/A

FlexConnect Dhcp Status : N/A

FlexConnect Authentication : N/A

Client Statistics:

Number of Bytes Received from Client : 111696

Number of Bytes Sent to Client : 62671

Number of Packets Received from Client : 529

Number of Packets Sent to Client : 268

Number of Data Retries : 136

Number of RTS Retries : 0

Number of Tx Total Dropped Packets : 1

Number of Duplicate Received Packets : 0

Number of Decrypt Failed Packets : 0

Number of Mic Failed Packets : 0

Number of Mic Missing Packets : 0

Number of Policy Errors : 0

Radio Signal Strength Indicator : -61 dBm

Signal to Noise Ratio : 4 dB

Fabric status : Disabled

Radio Measurement Enabled Capabilities

Capabilities: Link Measurement, Neighbor Report, Repeated Measurements, Passive Beacon Measurement, Act

Client Scan Report Time : Timer not running

Client Scan Reports

Assisted Roaming Neighbor List

Nearby AP Statistics:

EoGRE : Pending Classification

Max Client Protocol Capability: Wi-Fi6 (802.11ax)

WiFi to Cellular Steering : Not implemented

Cellular Capability : N/A

Advanced Scheduling Requests Details:

Apple Specific Requests(ASR) Capabilities/Statistics:

Regular ASR support: DISABLED

Lokale webverificatie voor lokale FlexConnect-switching

Voor dit scenario wordt ervan uitgegaan dat het toegangspunt zich in de FlexConnect-modus bevindt. Als een toegangspunt zich in de FlexConnect-modus bevindt, hebt u een Flex-profiel nodig dat is gekoppeld aan de SiteTag, waarbij het selectievakje Lokale site inschakelen is uitgeschakeld. Deze sitetag gebruikt de standaard-ap-join en een aangepaste flexprofielnaam Flex_LWA:

Configuration > Tags & Profiles > Tags

Policy Site RF AP

Add Delete Clone Reset APs

Site Tag Name

☐ FlexConnect
☐ default-site-tag

1 10

Edit Site Tag

Name* FlexConnect

Description Enter Description

AP Join Profile default-ap-profile

Flex Profile Flex_LWA

Fabric Control Plane Name

Enable Local Site ☐

Load* 0

Een beleidstag aan een toegangspunt toewijzen

Navigeer naar Configuratie > Draadloos > Toegangspunten, selecteer het toegangspunt en op het tabblad Algemeen staan rechts de tags die door het toegangspunt worden gebruikt.

Edit AP

General Interfaces High Availability Inventory Geolocation Advanced Support Bundle

General

AP Name* 9117

Location* default location

Base Radio MAC 000000000000

Ethernet MAC 000000000000

Admin Status ENABLED

AP Mode Local

Operation Status Registered

Fabric Status Disabled

LED Settings

LED State DISABLED

Flash Settings

Flash State DISABLED

Apply

Time Statistics

Up Time 8 days 15 hrs 51 mins 4 secs

Controller Association Latency 1 sec

Tags

Policy LWA

Site FlexConnect

RF default-rf-tag

Write Tag Config to AP

Version

Primary Software Version 17.12.5.41

Predownloaded Status N/A

Predownloaded Version N/A

Next Retry Time N/A

Boot Version 1.1.2.4

IOS Version 17.12.5.41

Mini IOS Version 0.0.0.0

IP Config

CAPWAP Preferred Mode Not Configured

DHCP IPv4 Address 172.16.60.40

Static IP (IPv4/IPv6)



Waarschuwing: als u de tags wijzigt, wordt de verbinding met de WLC verbroken.

Configuration > Wireless > Access Points

▼ All Access Points

Total APs: 1

Misconfigured APs
Tag : 0 Country Code : 0 LSC Fallback : 0 Select an Action ▼

Multiple APs can be configured at once from [Bulk AP Provisioning](#) feature

AP Name	AP Model	Slots	Admin Status	Up Time	IP Address	Base Radio MAC	Ethernet MAC	AP Mode	Power Derate Capable	Operation Status	Configuration Status	Country Code Misconfigured	LSC Fallback Misconfigure
9117	C9117AXI-A	2	✓	8 days 15 hrs 54 mins 53 secs	172.16.60.40	cc0	c00	Flex	No	Registered	Healthy	No	No

Het beleidsprofiel dat aan het WLAN is gekoppeld, is Lokale switching

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

+ Add

× Delete

Policy Tag

Policy Profile

LWA

LWA_LocalSW

1

10

1 - 1 of 1 items

Configuration > Tags & Profiles > Policy

+ Add

× Delete

🔄 Clone

Policy Profile Name "is equal to" LWA_LocalSW

Admin Status

Associated Policy Tags

Policy Profile Name

LWA_LocalSW

1

10

Edit Policy Profile

Disabling a Policy or configuring it in "Enabled" state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QoS and AVC

Mobility

Advanced

Name*

LWA_LocalSW

WLAN Switching Policy

Description

Enter Description

Central Switching

DISABLED

Status

ENABLED

Central Authentication

ENABLED

Passive Client

DISABLED

Central DHCP

ENABLED

IP MAC Binding

ENABLED

Flex NAT/PAT

DISABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

2-65519

Verifiëren

9800WLC>enable

9800WLC#show wireless client summary

Number of Clients: 1

MAC Address	AP Name	Type	ID	State	Protocol	Method	Role
-------------	---------	------	----	-------	----------	--------	------

9ef2.4b16.a507	xxxxx-9117	WLAN	1	Run	11ax(2.4)	Web Auth	Local
----------------	------------	------	---	-----	-----------	----------	-------

9800WLC#show wireless client mac-address

detail

Client MAC Address :

Client MAC Type : Locally Administered Address

Client DUID: NA

Client IPv4 Address : 172.16.74.83

Client IPv6 Addresses : fe80::9cf2:4bff:fe16:a507

Client Username : johndoe

AP MAC Address : xxxx.xxxx.xcc0

AP Name: xxxxxx-9117

AP slot : 0

Client State : Associated

Policy Profile : LWA_LocalSW

Flex Profile : Flex_LWA

Wireless LAN Id: 1

WLAN Profile Name: LWA_LA

Wireless LAN Network Name (SSID): LWA LA

BSSID : 0cd0.f897.acc0

Connected For : 315 seconds

Protocol : 802.11ax - 2.4 GHz

Channel : 6

Client IIF-ID : 0xa0000004

Association Id : 1

Authentication Algorithm : Open System

Idle state timeout : N/A

Session Timeout : 28800 sec (Remaining time: 28525 sec)

Session Warning Time : Timer not running

Input Policy Name : None

Input Policy State : None

Input Policy Source : None

Output Policy Name : None

Output Policy State : None

Output Policy Source : None

WMM Support : Enabled

U-APSD Support : Disabled

Fastlane Support : Disabled

Client Active State : Active

Power Save : ON

Current Rate : m11 ss2

Supported Rates : 1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0

AAA QoS Rate Limit Parameters:

QoS Average Data Rate Upstream : 0 (kbps)

QoS Realtime Average Data Rate Upstream : 0 (kbps)

QoS Burst Data Rate Upstream : 0 (kbps)

QoS Realtime Burst Data Rate Upstream : 0 (kbps)

QoS Average Data Rate Downstream : 0 (kbps)

QoS Realtime Average Data Rate Downstream : 0 (kbps)

QoS Burst Data Rate Downstream : 0 (kbps)

QoS Realtime Burst Data Rate Downstream : 0 (kbps)

Mobility:

Move Count : 0

Mobility Role : Local

Mobility Roam Type : None

Mobility Complete Timestamp : 09/11/2025 17:38:26 UTC

Client Join Time:

Join Time Of Client : 09/11/2025 17:38:26 UTC

Client State Servers : None

Client ACLs : None

Policy Manager State: Run

Last Policy Manager State : Webauth Pending

Client Entry Create Time : 315 seconds

Policy Type : N/A

Encryption Cipher : None

Transition Disable Bitmap : 0x00

User Defined (Private) Network : Disabled

User Defined (Private) Network Drop Unicast : Disabled

Encrypted Traffic Analytics : No

Protected Management Frame - 802.11w : No

EAP Type : Not Applicable

VLAN Override after Webauth : No

VLAN : 2667

Multicast VLAN : 0

VRF Name : N/A

WiFi Direct Capabilities:

WiFi Direct Capable : No

Central NAT : DISABLED

Session Manager:

Point of Attachment : capwap_90400005

IIF ID : 0x90400005

Authorized : TRUE

Session timeout : 28800

Common Session ID: 044A10AC0000002A39DB6F52

Acct Session ID : 0x00000000

Auth Method Status List

Method : Web Auth

Webauth State : Authz

Webauth Method : Webauth

Local Policies:

Service Template : IP-Adm-V4-LOGOUT-ACL (priority 100)

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

Service Template : wlan_svc_LWA_LocalSW (priority 254)

VLAN : 2667

Absolute-Timer : 28800

Server Policies:

Resultant Policies:

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

VLAN Name : xxxxx

VLAN : 2667

Absolute-Timer : 28800

DNS Snooped IPv4 Addresses : None

DNS Snooped IPv6 Addresses : None

Client Capabilities

CF Pollable : Not implemented

CF Poll Request : Not implemented

Short Preamble : Not implemented

PBCC : Not implemented

Channel Agility : Not implemented

Listen Interval : 0

Fast BSS Transition Details :

Reassociation Timeout : 0

11v BSS Transition : Implemented

11v DMS Capable : No

QoS Map Capable : Yes

FlexConnect Data Switching : Local

FlexConnect Dhcp Status : Central

FlexConnect Authentication : Central

Client Statistics:

Number of Bytes Received from Client : 295564

Number of Bytes Sent to Client : 90146

Number of Packets Received from Client : 1890

Number of Packets Sent to Client : 351

Number of Data Retries : 96

Number of RTS Retries : 0

Number of Tx Total Dropped Packets : 0

Number of Duplicate Received Packets : 0

Number of Decrypt Failed Packets : 0

Number of Mic Failed Packets : 0

Number of Mic Missing Packets : 0

Number of Policy Errors : 0

Radio Signal Strength Indicator : -34 dBm

Signal to Noise Ratio : 31 dB

Fabric status : Disabled

Radio Measurement Enabled Capabilities

Capabilities: Link Measurement, Neighbor Report, Repeated Measurements, Passive Beacon Measurement, Act

Client Scan Report Time : Timer not running

Client Scan Reports

Assisted Roaming Neighbor List

Nearby AP Statistics:

EoGRE : Pending Classification

Max Client Protocol Capability: Wi-Fi6 (802.11ax)

WiFi to Cellular Steering : Not implemented

Cellular Capability : N/A

Advanced Scheduling Requests Details:

Apple Specific Requests(ASR) Capabilities/Statistics:

Regular ASR support: DISABLED

The screenshot displays the Cisco WLC interface. On the left, the 'Clients' tab is active, showing a list of clients. The 'Client Properties' window is open on the right, showing the 'General' tab. The 'Policy Profile' and 'Flex Profile' are highlighted with a red box, indicating they are set to 'LWA_LocalSW' and 'Flex_LWA' respectively.

Client Properties	Value
MAC Address	9ef2.4b16.a507
Client MAC Type	Locally Administered Address
Client DUID	NA
IPv4 Address	172.16.74.83
IPv6 Address	fe80::9cf2:4b16:fe16:a507
User Name	john.doe
Policy Profile	LWA_LocalSW
Flex Profile	Flex_LWA
Wireless LAN Id	1
WLAN Profile Name	LWA_LA
Wireless LAN Network Name (SSID)	LWA_LA
BSSID	cc0
Uptime(sec)	103 seconds
Idle state timeout	N/A
Session Timeout	28800 sec (Remaining time: 28737 sec)
Session Warning Time	Timer not running
Client Active State	Active
Power Save mode	OFF
Current TxRateSet	m11 ss2
Supported Rates	1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0
QoS Average Data Rate Upstream	0 (kbps)
QoS Realtime Average Data Rate Upstream	0 (kbps)
QoS Burst Data Rate Upstream	0 (kbps)
QoS Realtime Burst Data Rate Upstream	0 (kbps)
QoS Average Data Rate Downstream	0 (kbps)
QoS Realtime Average Data Rate Downstream	0 (kbps)
QoS Burst Data Rate Downstream	0 (kbps)
QoS Realtime Burst Data Rate Downstream	0 (kbps)
Join Time Of Client	09/11/2025 17:38:26 UTC
Policy Manager State	Run
Last Policy Manager State	Webauth Pending
Transition Disable Bitmap	0x00
User Defined (Private) Network	Disabled
User Defined (Private) Network Drop Unicast	Disabled

Problemen oplossen

De status "Web Auth Pending" geeft aan dat de client is gekoppeld aan het toegangspunt, maar dat het webverificatieproces nog niet is voltooid. Tijdens deze status onderschept de controller het HTTP-verkeer van de client en leidt het door naar een webverificatieportaal voor gebruikersaanmelding of acceptatie van voorwaarden. De client blijft in deze status totdat de webverificatie is voltooid, waarna de status van de clientbeleidsmanager wordt gewijzigd in "Uitvoeren" en volledige netwerktoegang wordt verleend.

Om de stroom van de clientverbinding visueel te bekijken, controleert u LWA Flow van [Configure Local Web Authentication with External Authentication \(Lokale webverificatie configureren met externe verificatie\)](#).

De fasen die de klant ondergaat vanuit het perspectief van de klant worden weergegeven in [Problemen oplossen met veelvoorkomende problemen met LWA op 9800 WLC's](#).

- [Technische ondersteuning en documentatie – Cisco Systems](#)

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.