

Configurer l'authentification Web locale avec l'authentification locale

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Carte de paramètres](#)

[Base de données pour authentification](#)

[Configurer](#)

[Authentification Web locale avec authentification locale sur la CLI](#)

[ListesMéthodePourAuthentificationLocale](#)

[Cartes de paramètres](#)

[Paramètres de sécurité WLAN](#)

[Créer un profil de stratégie](#)

[Créer une balise de stratégie](#)

[Attribuer une balise de stratégie à un point d'accès](#)

[Créer un nom d'utilisateur invité](#)

[Authentification Web locale avec authentification locale via WebUI](#)

[Vérifier](#)

[Authentification Web locale sur la commutation locale FlexConnect](#)

[Vérifier](#)

[Dépannage](#)

Introduction

Ce document décrit comment configurer l'authentification Web locale avec l'authentification locale sur un contrôleur LAN sans fil (WLC) 9800.

Conditions préalables

Cisco recommande que vous ayez connaissance du modèle de configuration WLC 9800.

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Gamme Cisco WLC 9800
- Connaissance complète de l'authentification Web.

Composants utilisés

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

- 9800-CL WLC Cisco IOS® XE version 17.12.5
- Point d'accès Cisco C917AXI.

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

Informations générales

L'authentification Web locale (LWA) est une méthode d'authentification de réseau local sans fil (WLAN) qui peut être configurée sur le WLC. Lorsqu'un utilisateur sélectionne le WLAN dans la liste des réseaux disponibles, il est redirigé vers un portail Web. Dans ce portail, selon la configuration, l'utilisateur peut être invité à entrer un nom d'utilisateur et un mot de passe, à accepter une politique d'utilisation acceptable (AUP) ou une combinaison des deux actions pour finaliser sa connexion.

Pour plus d'informations sur les quatre types de pages d'authentification Web présentés pendant le processus de connexion, référez-vous au guide [Configurer l'authentification Web locale](#) et passez en revue les options disponibles pour le type d'authentification Web. Vous pouvez également consulter le guide [Configurer l'authentification Web locale avec l'authentification externe](#) sous la section Types d'authentification.

Carte de paramètres

Parameter Map est un élément de configuration essentiel sur un WLC qui active l'authentification Web. Il se compose d'un ensemble de paramètres qui régissent diverses facettes du processus d'authentification Web, y compris le type d'authentification, les URL de redirection, les paramètres ajoutés, les délais d'attente et les pages Web personnalisées. Pour activer et gérer l'authentification Web pour un SSID particulier, cette carte doit être liée au profil WLAN.

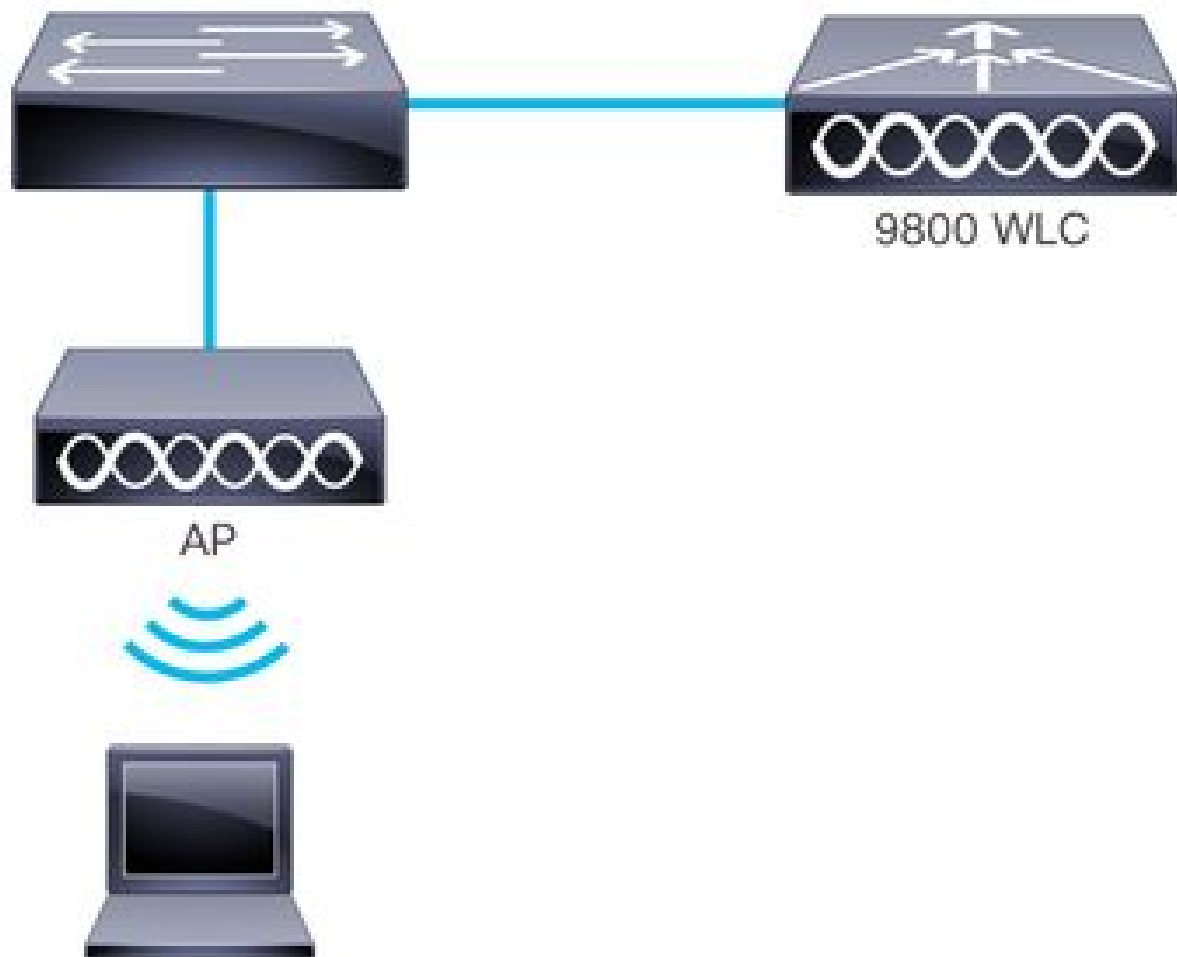
Le contrôleur de réseau local sans fil est fourni avec une carte de paramètres globale par défaut, mais les administrateurs ont la possibilité de créer des cartes de paramètres personnalisées pour personnaliser le comportement d'authentification Web en fonction des besoins spécifiques.

Base de données pour authentification

Si le mappage de paramètres est configuré pour utiliser un nom d'utilisateur et un mot de passe, vous devez définir les informations d'identification d'authentification, qui sont stockées localement sur le WLC. Lorsque vous créez un compte d'utilisateur invité via l'interface utilisateur graphique, vous pouvez définir le nombre maximal de connexions simultanées autorisées par compte d'invité. Les valeurs valides sont comprises entre 0 et 64, où 0 indique qu'un nombre illimité de connexions simultanées est autorisé pour cet utilisateur invité.

LWA est principalement destiné aux petits déploiements. Il prend en charge l'intégration avec d'autres méthodes d'authentification, vous pouvez vérifier la [Combinaison d'authentifications prise en charge pour un client](#) pour plus d'informations.

L'image représente une topologie générique de LWA :



Topologie générique de LWA avec authentification locale

Périphériques de la topologie réseau de LWA :

- Client/Demandeur : initie une requête de connexion au WLAN, puis aux serveurs DHCP et DNS, et répond aux communications du WLC.
- Point d'accès : connecté à un commutateur, il diffuse le WLAN invité et fournit une connectivité sans fil aux périphériques invités. Elle autorise le trafic DHCP et DNS avant que l'utilisateur invité ne termine l'authentification en entrant des informations d'identification valides, en acceptant une AUP ou une combinaison des deux actions.
- WLC/Authenticator : Gère les points d'accès et les périphériques clients. Le WLC héberge l'URL de redirection et applique la liste de contrôle d'accès (ACL) qui régit le trafic et sa

création par défaut lors de la configuration du mappage de paramètre. Il intercepte les requêtes HTTP des utilisateurs invités et les redirige vers un portail Web (page de connexion) où les utilisateurs doivent s'authentifier. Le WLC capture les informations d'identification de l'utilisateur, authentifie les invités et vérifie la validité des informations d'identification dans la base de données locale.

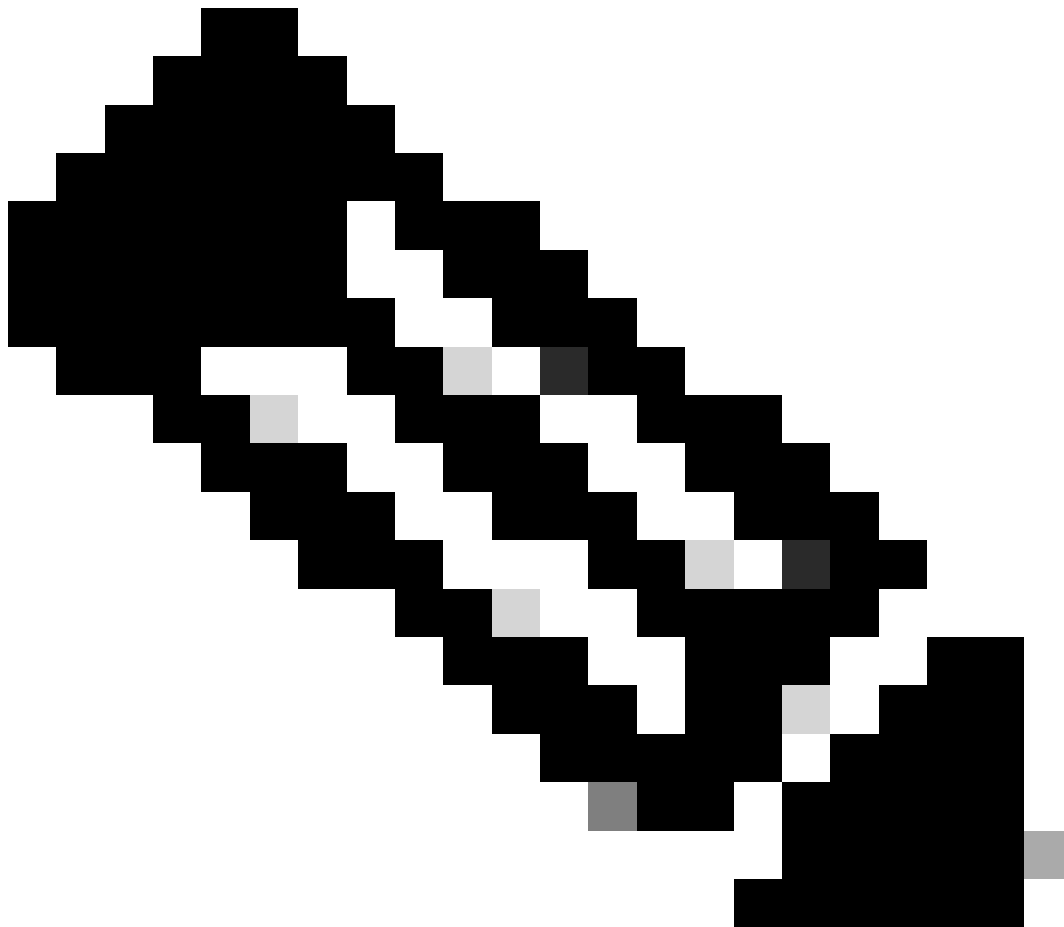
- Serveur d'authentification : dans ce scénario, le WLC fonctionne comme serveur d'authentification. Il valide les informations d'identification des utilisateurs invités et accorde ou refuse l'accès au réseau en conséquence.

Configurer

Authentification Web locale avec authentification locale sur la CLI

Listes de méthodes pour l'authentification locale

```
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
```



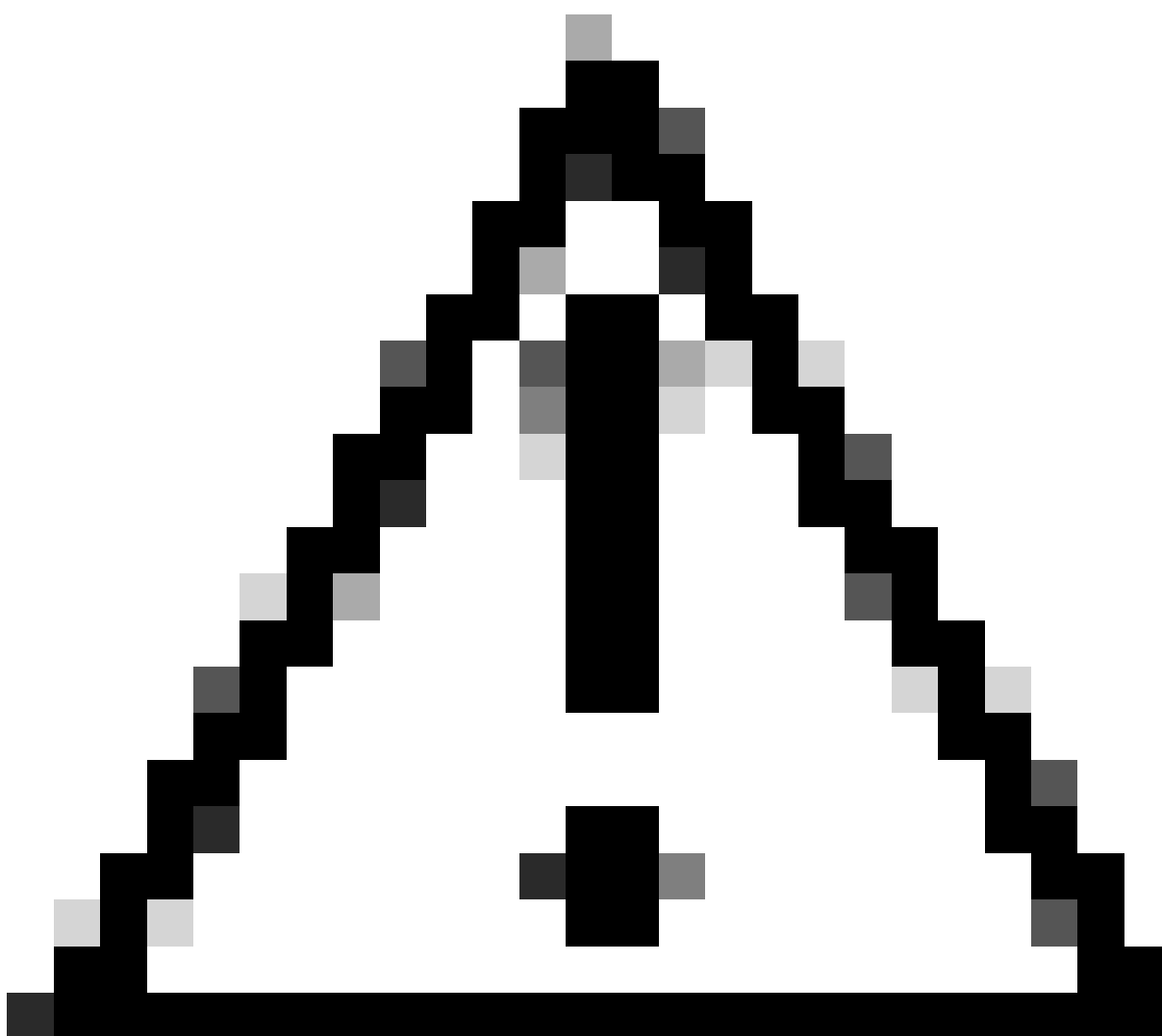
Remarque : Pour que la Liste de méthodes de connexion locale fonctionne, assurez-vous que la configuration aaa authorization network default local existe sur le WLC. Cela est nécessaire car le WLC autorise l'utilisateur à accéder au réseau.

Cartes de paramètres

```
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
```



Mise en garde : L'adresse IP virtuelle doit être une adresse non routable proposée dans la RFC 5737. Par défaut, l'adresse IP 192.0.2.1 est définie. Pour plus d'informations sur l'adresse IP virtuelle, consultez les [Méthodes Recommandées pour la configuration de la gamme Cisco Catalyst 9800](#). Sur AireOs, l'adresse IP utilisée était la plupart du temps 1.1.1.1. Cette méthode n'est plus recommandée car elle est devenue une adresse IP publique.

La possibilité de créer plusieurs mappages de paramètres permet des flux personnalisés : des pages Web personnalisées et des paramètres de présentation spécifiques pour chaque réseau local sans fil. La carte de paramètres globale détermine le point de confiance et donc le certificat

que le WLC présente au client sur le portail de redirection. En outre, il contrôle les types de trafic client interceptés, tels que HTTP/HTTPS pour le portail de redirection, la résolution de domaine ou de nom d'hôte pour l'adresse IP virtuelle. Cette séparation permet au mappage global de gérer les paramètres généraux tels que la présentation de certificats et l'interception du trafic, tandis que les mappages de paramètres définis par l'utilisateur fournissent une expérience granulaire par WLAN.

Paramètres de sécurité WLAN

```
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
```

Créer un profil de stratégie

```
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
```

Créer une balise de stratégie

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

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

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

Attribuer une balise de stratégie à un point d'accès

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

```
>
```

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

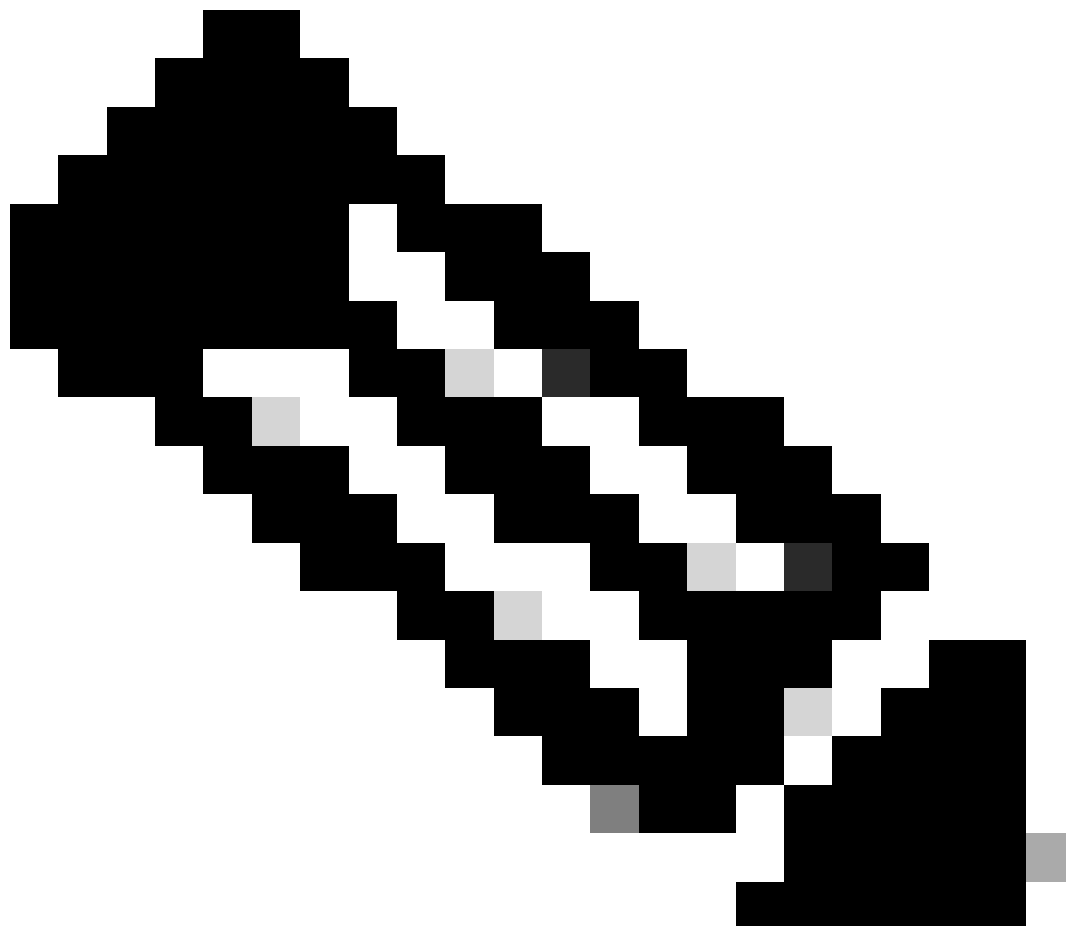
```
9800WLC(config-ap-tag)#end
```

Créer un nom d'utilisateur invité

```
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
```

Remarque : Lorsque vous définissez la durée de vie de l'utilisateur invité, si l'année est définie sur 1, vous ne pouvez pas spécifier les paramètres suivants, à savoir mois, jours, heures et minutes, car la durée de vie maximale est 1 an.

Authentification Web locale avec authentification locale via WebUI

Listes de méthodes pour l'authentification locale

Accédez à Configuration > Security > AAA > AAA Method List > Authentication > Add pour créer la liste de méthodes ultérieurement à utiliser dans la configuration WLAN.

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

Group Type

local

Available Server Groups

radius

ldap

tacacs+

AAA-group

>

<

>>

<<

Assigned Server Groups

^

^

v

v

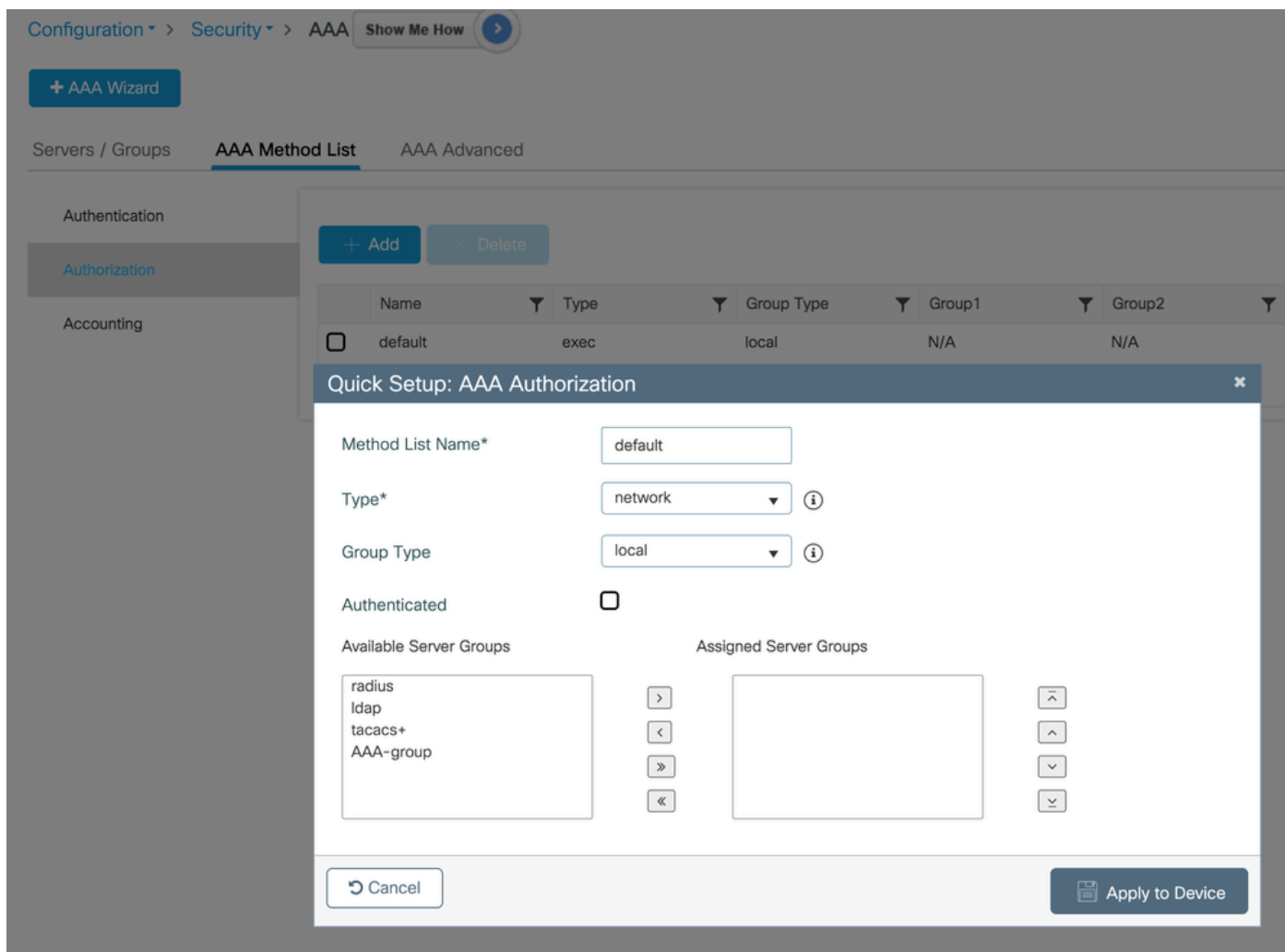
Cancel

Apply to Device

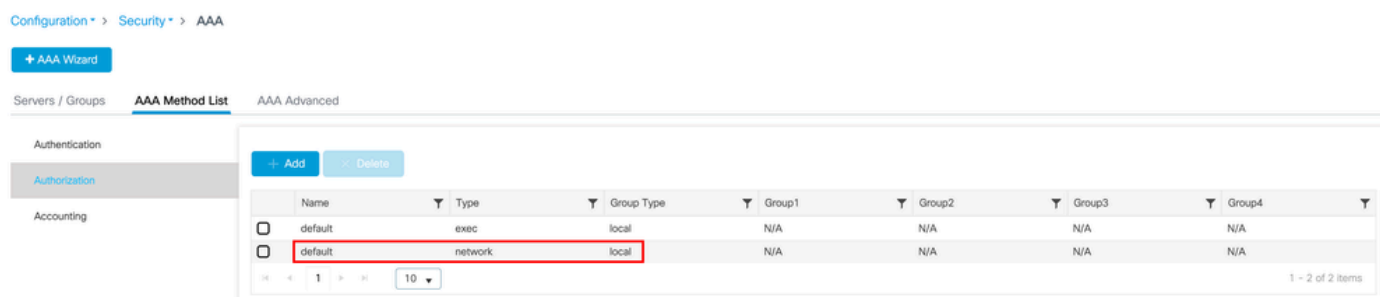
Après avoir cliqué sur Apply to Device, confirmez la création de la liste de méthodes AAA :

Assurez-vous qu'il existe une liste de méthodes d'autorisation locale, car c'est une condition requise pour que la liste de méthodes de connexion locale créée fonctionne.

Configuration > Security > AAA > AAA Method List > Authorization > Add



Après avoir cliqué sur Apply to Device, confirmez la création de la liste de méthodes AAA :



Cartes de paramètres

Modifier la carte de paramètres globale dans Configuration > Security > Web Auth

Configuration > Security > Web Auth

[Add](#) [Delete](#)

Selected Rows: 0

Parameter Map Name
☐ global

10 items per page

General

Advanced

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

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

Sélectionnez le type d'authentification Web à utiliser, Virtual IP et le point de confiance que le WLC présente sur le portail Web. Dans ce cas, le certificat auto-signé est sélectionné et est susceptible d'entraîner une clause de non-responsabilité du type « votre connexion n'est pas un réseau privé::ERR_CERT_AUTHORITY_INVALID », car il s'agit d'un certificat significatif localement (LSC) et il n'est pas signé par une autorité de certification reconnaissable sur Internet. Pour modifier ce paramètre, utilisez un certificat signé par un tiers. Les détails sont illustrés sur [Générer et télécharger des certificats CSR sur les WLC Catalyst 9800](#) ou il y a une option vidéo qui explique le téléchargement et la création de Trustpoint [Renouveler des certificats pour WebAuth & WebAdmin sur le WLC Cisco 9800 | Configuration du contrôleur LAN sans fil sécurisé](#).

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 ☐

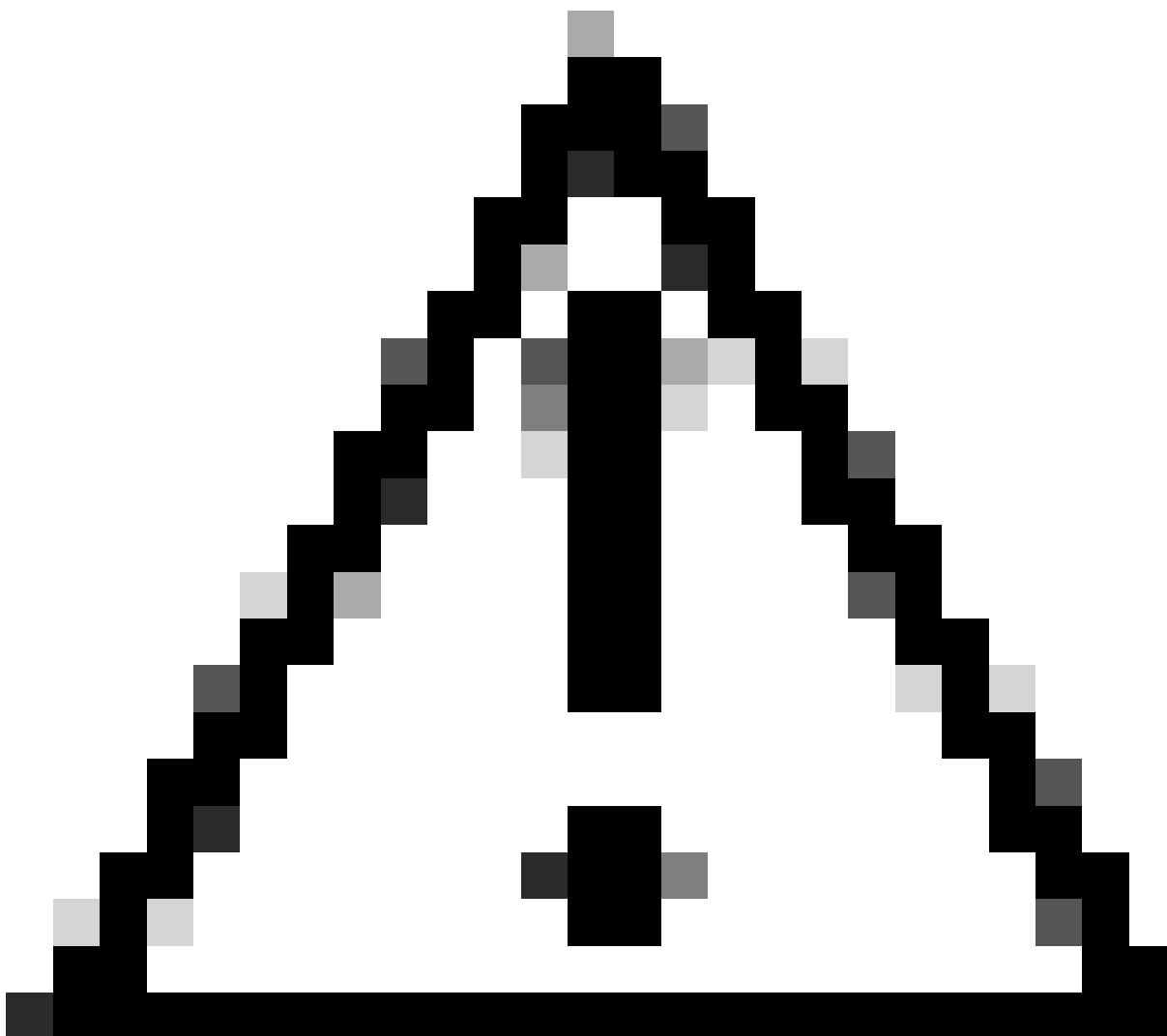
Enable HTTP server for Web Auth ☒

Disable HTTP secure server for Web Auth ☐

Banner Configuration

Banner Title

Banner Type ☒ None ☐ Banner Text ☐ Read From File



Mise en garde : Si le protocole HTTP est globalement désactivé sur le routeur 9800, assurez-vous que l'option Enable HTTP server for Web Auth (Activer le serveur HTTP pour l'authentification Web) est cochée, car Cisco a séparé la dépendance de ces processus. Les clients ou les demandeurs sont censés initier un processus de connexion HTTP et cette session est interceptée par le contrôleur pour présenter le portail Web. Pour cette raison, il n'est pas recommandé d'activer Web Auth Intercept HTTPS à moins d'une nécessité absolue, car ce paramètre n'est pas nécessaire pour la plupart des déploiements et peut augmenter l'utilisation du processeur du contrôleur, ce qui peut avoir un impact sur les performances.

Paramètres de sécurité WLAN

Accédez à Configuration > Tags & Profiles > WLANs, cliquez sur Add.

⚠ 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 ▼

Dans l'onglet Security, sélectionnez None pour Layer2.

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

Sous l'onglet Security, pour Layer3, cochez la case Web Policy, sélectionnez Parameter Map précédemment configuré dans le menu déroulant et la liste Authentication List.

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...

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

[<< Hide](#)

On MAC Filter Failure

☐

Splash Web Redirect

DISABLED

Preauthentication ACL

IPv4

None

IPv6

None

Créer un profil de stratégie

Afin de créer le profil de stratégie qui doit être lié au profil WLAN, naviguez à Configuration > Tags & Profiles > Policy.

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

Dans l'onglet Access Policies, sélectionnez le VLAN à partir duquel les clients/demandeurs doivent demander une adresse IP.

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 ▼ ⓘ

Créer une balise de stratégie

Pour ce guide de configuration, nous avons créé une balise de stratégie personnalisée nommée 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

Associer le WLAN et le profil de stratégie

Afin de lier les stratégies de commutation du profil de stratégie et du WLAN, accédez à Configuration > Tags & Profiles > WLANs, sélectionnez le profil WLAN, cliquez sur Add to Policy Tags.

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_CentralSW

⏪ ⏩ 1 ⏪ ⏩

10 ▾

1 - 1 of 1 items

Attribuer une balise de stratégie à un point d'accès

Afin d'étiqueter le point d'accès avec la balise de stratégie créée, naviguez à Configuration > Wireless > Access Points, sélectionnez le point d'accès et sur l'onglet General, à droite il y a les balises utilisées par le point d'accès.

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

Créer un nom d'utilisateur invité

Si vous avez sélectionné le type webauth sur la carte des paramètres, un nom d'utilisateur invité est nécessaire, pour le créer, accédez à Configuration > Security > Guest User.

La durée de vie maximale de l'utilisateur est de 1 an. Vous pouvez spécifier le contraire avec les options disponibles.

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

Selected Rows: 0

☐	User Name
☐	johndoe

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* 0
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* 1

Months* 0

Days* 0

Hours* 0

Mins* 0

Vérifier

Via GUI

Cisco Catalyst 9800-CL Wireless Controller 17.12.5

Welcome admin

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	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

Authentification Web locale sur la commutation locale FlexConnect

Dans ce scénario, le point d'accès est supposé être en mode FlexConnect. Pour qu'un point d'accès soit en mode FlexConnect, vous avez besoin d'un profil Flex associé sur SiteTag, où la case à cocher Activer le site local est désactivée. Cette balise de site utilise default-ap-join et un nom de profil paramétrable personnalisé 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

Attribuer une balise de stratégie à un point d'accès

Accédez à Configuration > Wireless > Access Points, sélectionnez le point d'accès et dans l'onglet General, à droite se trouvent les balises utilisées par le point d'accès.

Edit AP

General Interfaces High Availability Inventory Geolocation Advanced Support Bundle

General

AP Name* 9117

Location* default location

Base Radio MAC

Ethernet MAC

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)



Avertissement : La modification des balises entraîne la disjonction de l'AP du WLC.

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

Le profil de stratégie associé au WLAN est Commutation locale

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

Vérifier

```

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

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Delete

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

Dépannage

L'état « Authentification Web en attente » indique que le client est associé au point d'accès mais n'a pas encore terminé le processus d'authentification Web. Pendant cet état, le contrôleur intercepte le trafic HTTP client et le redirige vers un portail d'authentification Web pour la connexion de l'utilisateur ou l'acceptation des termes. Le client reste dans cet état jusqu'à ce que l'authentification Web soit terminée, après quoi l'état du gestionnaire de stratégies client passe à « Exécuter » et un accès réseau complet est accordé.

Afin de voir le flux de la connexion client visuellement, vérifiez le flux LWA à partir de [Configurer Local Web Authentication with External Authentication](#).

Les étapes que le client subit du point de vue du client sont décrites dans [Dépanner les problèmes courants avec LWA sur les WLC 9800](#).

- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

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

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