

# Configuration de FlexConnect avec authentification sur le WLC Catalyst 9800

## Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Diagramme du réseau](#)

## Introduction

Ce document décrit comment configurer FlexConnect avec l'authentification centrale ou locale sur le contrôleur LAN sans fil Catalyst 9800.

## Conditions préalables

## Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Modèle de configuration Catalyst Wireless 9800
- FlexConnect
- 802.1x

## Composants utilisés

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

- C980-CL, Cisco IOS-XE® 17.3.4

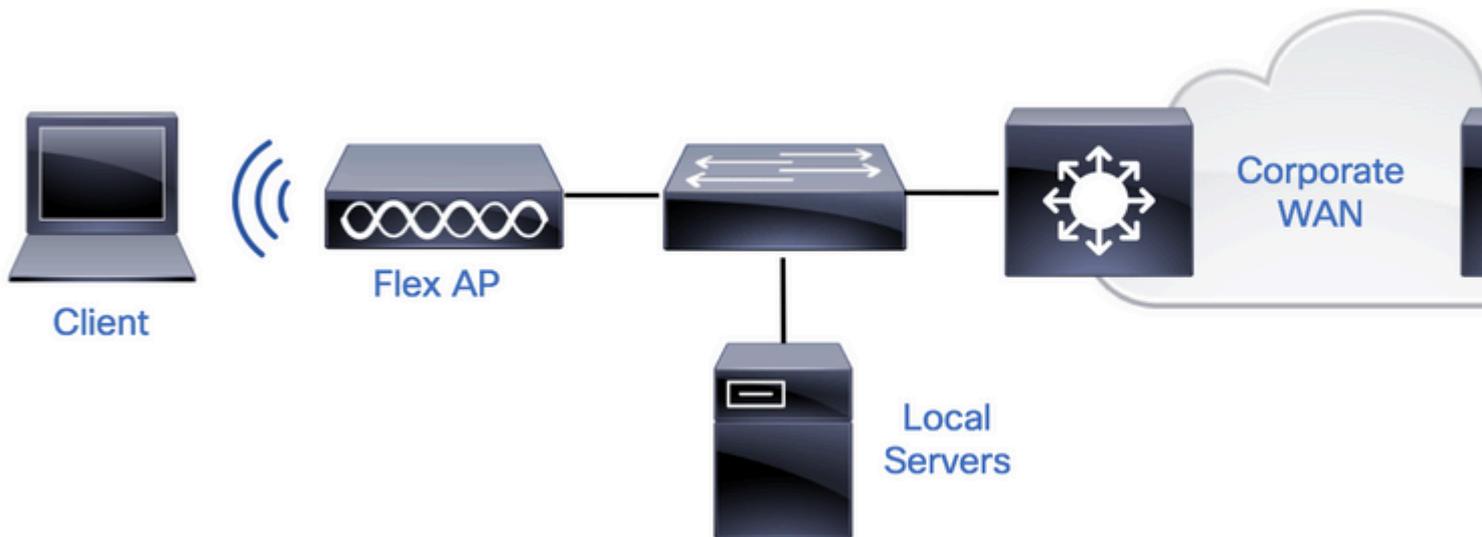
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

FlexConnect est une solution sans fil pour le déploiement de bureaux distants. Il vous permet de configurer des points d'accès (AP) dans des emplacements distants à partir du bureau de l'entreprise via une liaison WAN (Wide Area Network) sans devoir déployer un contrôleur dans chaque emplacement. Les points d'accès FlexConnect peuvent commuter le trafic de données client localement et effectuer l'authentification client localement lorsque la connexion au contrôleur est perdue. En mode connecté, les points d'accès FlexConnect peuvent également effectuer une authentification locale.

## Configurer

## Diagramme du réseau



## Configurations

### Configuration AAA sur les WLC 9800

Étape 1 : déclaration du serveur RADIUS **Dans l'interface GUI**, accédez à Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add et entrez les informations du serveur RADIUS.

The screenshot shows the Cisco WLC GUI configuration page for AAA. The breadcrumb trail is Configuration > Security > AAA. The 'Servers / Groups' tab is selected, and the 'RADIUS' sub-tab is active. The 'Servers' sub-tab is also visible. A table with columns 'Name', 'Address', and 'Auth Port' is partially visible at the bottom.

Assurez-vous que la prise en charge de CoA est activée si vous prévoyez d'utiliser tout type de sécurité qui nécessite CoA à l'avenir.

## Edit AAA Radius Server

|  |   |
|--|---|
| Name*  | <input type="text" value="AmmlSE"/>               |
| Server Address*  | <input type="text" value="10.48.76.30"/>          |
| PAC Key  | <input type="checkbox"/>                          |
| Key Type   | <input type="text" value="Hidden"/>               |
| Key*  | <input type="text" value="●●●●●●●●●●●●●●●●●●●●"/> |
| Confirm Key*   | <input type="text" value="●●●●●●●●●●●●●●●●●●●●"/> |
| Auth Port  | <input type="text" value="1812"/>                 |
| Acct Port  | <input type="text" value="1813"/>                 |
| Server Timeout (seconds)   | <input type="text" value="5"/>                    |
| Retry Count  | <input type="text" value="3"/>                    |
| Support for CoA  | <input checked="" type="checkbox"/> ENABLED       |

 Cancel

**Remarque :** Remarque : Radius CoA n'est pas pris en charge dans le déploiement d'authentification locale Flex Connect. .

Étape 2. Ajoutez le serveur RADIUS à un groupe RADIUS. **Dans l'interface graphique :** accédez à Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add.

Search Menu Items

- Dashboard
- Monitoring >
- Configuration >
- Administration >
- Licensing

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups    AAA Method List    AAA Advanced

+ Add    × Delete

RADIUS

TACACS+

Servers    **Server Groups**

| Name | Server 1 | Server 2 |
|------|----------|----------|
|------|----------|----------|

## Edit AAA Radius Server Group

|                          |        |
|--------------------------|--------|
| Name*                    | AmmlSE |
| Group Type               | RADIUS |
| MAC-Delimiter            | none   |
| MAC-Filtering            | none   |
| Dead-Time (mins)         | 2      |
| Source Interface VLAN ID | 76     |

### Available Servers

^

v



### Assigned Servers

AmmlSE

^

v



Cancel

Update & Apply to

Étape 3. Créez une liste de méthodes d'authentification. **Dans l'interface graphique :** Naviguez jusqu'à Configuration > Security > AAA > AAA Method List > Authentication > + Add

Q Search Menu Items

- Dashboard
- Monitoring >
- Configuration >
- Administration >

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups

AAA Method List

AAA /

Authentication

+ Add

Authorization

| Name |
|------|
|------|

## Quick Setup: AAA Authentication

Method List Name\*

AmmISE

Type\*

dot1x

Group Type

group

Fallback to local

Available Server Groups

radius  
ldap  
tacacs+



Assigned Server Groups

AmmISE

Cancel

Up

**À partir de CLI :**

```
# config t
# aaa new-model

# radius server <radius-server-name>
# address ipv4 <radius-server-ip> auth-port 1812 acct-port 1813
```

```
# timeout 300
# retransmit 3
# key <shared-key>
# exit

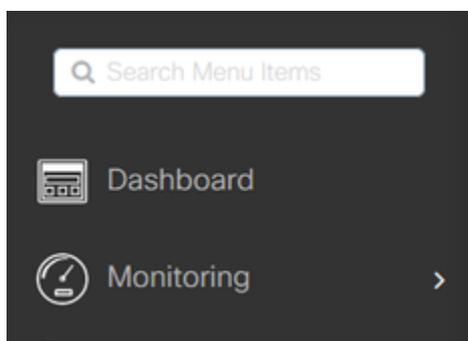
# aaa group server radius <radius-grp-name>
# server name <radius-server-name>
# exit

# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>

# aaa authentication dot1x <dot1x-list-name> group <radius-grp-name>
```

## Configuration dâ€™un réseau local sans fil (WLAN)

Étape 1. À partir de l'interface graphique : accédez à Configuration > Wireless > WLANs et cliquez sur +Add pour créer un nouveau WLAN, puis entrez les informations WLAN. Cliquez ensuite sur Apply to Device.



Configuration > Tags & Profiles > WLANs



Number of WLANs selected : 0

| <input type="checkbox"/> | Status ▾ | Name | ID |
|--------------------------|----------|------|----|
|--------------------------|----------|------|----|

## Add WLAN

General

Security

Advanced

Profile Name\*

802.1x-WLAN

Radio Policy

All

SSID\*

802.1x

Broadcast SSID

ENABLED

WLAN ID\*

1

Status

ENABLED



 Cancel

Étape 2. **À partir de l'interface utilisateur graphique** : accédez à l'onglet Security (Sécurité) pour configurer le mode de sécurité Layer2/Layer3 tant que la méthode de cryptage et la liste d'authentification au cas où la norme 802.1x serait utilisée. Cliquez ensuite sur Update & Apply to Device.

⚠ 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

Layer 2 Security Mode

MAC Filtering

### Protected Management Frame

PMF

### WPA Parameters

WPA Policy

WPA2 Policy

GTK Randomize

OSEN Policy

WPA2 Encryption  AES(CCMP128)

CCMP256

GCMP128

GCMP256

Auth Key Mgmt  802.1x

PSK

CCKM

FT + 802.1x

FT + PSK

...

Lobby Admin Access

Fast Transition

Over the DS

Reassociation Timeout

### MPSK Configuration

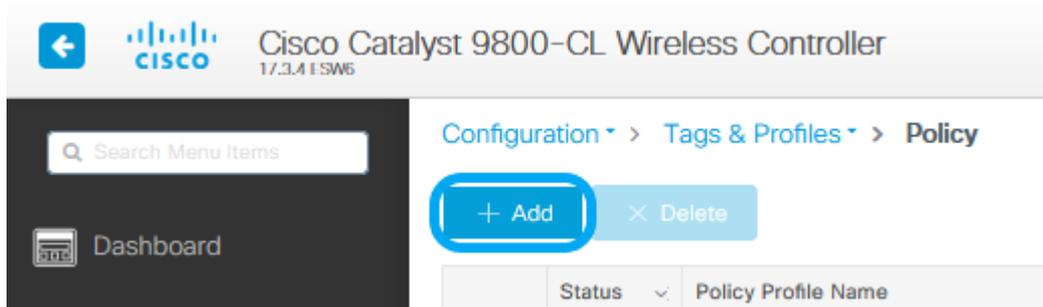
MPSK

Cancel

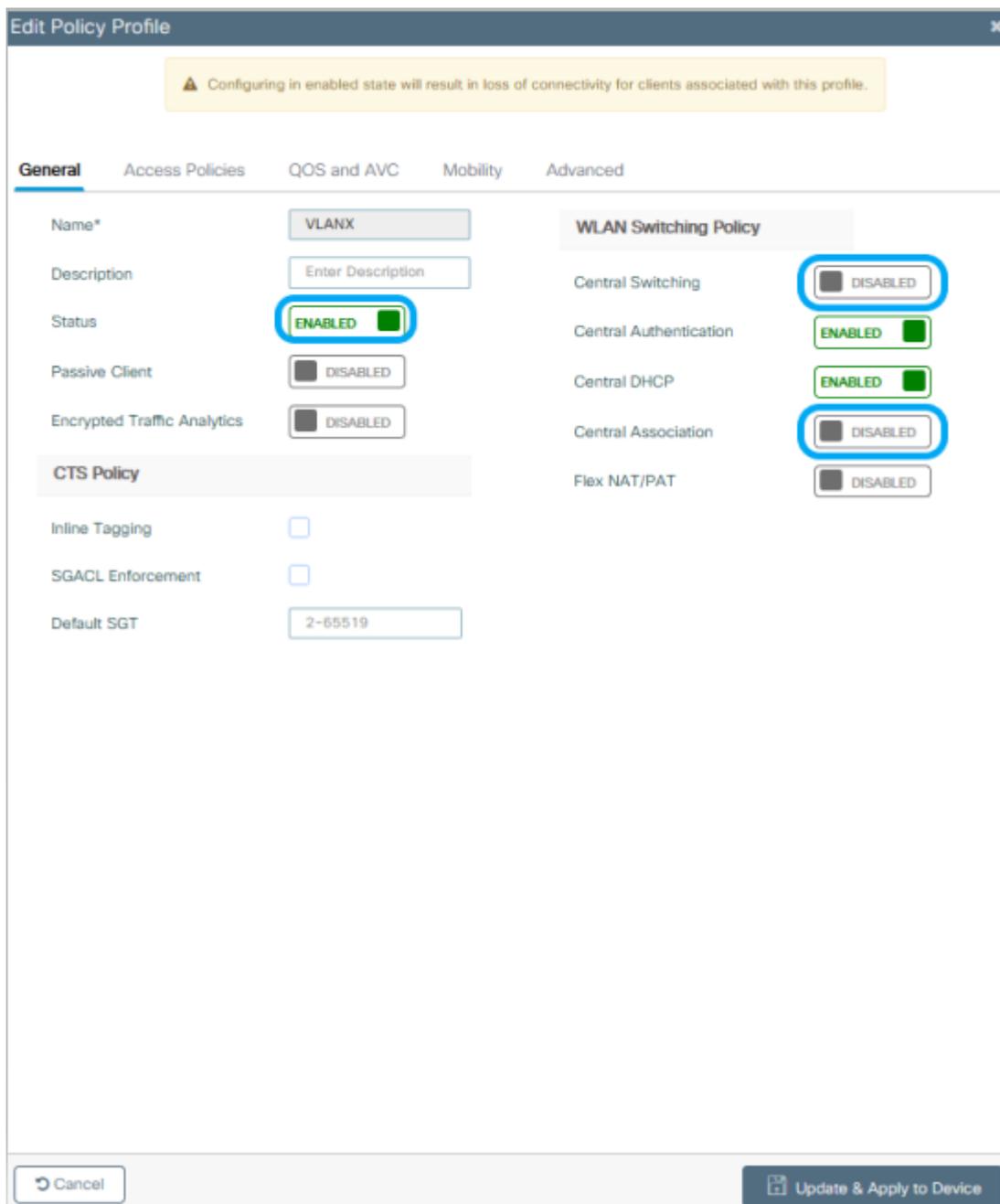
Update & Apply to Device

## Configuration du profil des politiques

Étape 1. **Dans l'interface graphique** : accédez à Configuration > Tags & Profiles > Policy et cliquez sur +Add pour créer un profil de stratégie.



Étape 2. Ajoutez le nom et décochez la case Commutation centrale. Avec cette configuration, le contrôleur gère l'authentification client et le point d'accès FlexConnect commute localement les paquets de données client.



**Remarque :** l'association et la commutation doivent toujours être appariées, si la commutation centrale est désactivée, l'association centrale doit également être désactivée sur tous les profils de stratégie lorsque des points d'accès Flexconnect sont utilisés.

Étape 3. **Dans l'interface utilisateur graphique :** accédez à l'onglet Access Policies pour attribuer le VLAN auquel les clients

sans fil peuvent être attribués lorsqu'ils se connectent à ce WLAN par défaut.

Vous pouvez sélectionner un nom de VLAN dans la liste déroulante ou, comme pratique recommandée, saisir manuellement un ID de VLAN.

### Edit Policy Profile ✕

 Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

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

|                                       |   |   |
|---------------------------------------|---|---|
| RADIUS Profiling                      | <input type="checkbox"/>                          | <b>WLAN ACL</b>   |
| HTTP TLV Caching                      | <input type="checkbox"/>                          | IPv4 ACL <input type="text" value="Search or Select"/> ▼  |
| DHCP TLV Caching                      | <input type="checkbox"/>                          | IPv6 ACL <input type="text" value="Search or Select"/> ▼  |
| <b>WLAN Local Profiling</b>           |   | <b>URL Filters</b>  |
| Global State of Device Classification | Disabled ⓘ  | Pre Auth <input type="text" value="Search or Select"/> ▼  |
| Local Subscriber Policy Name          | <input type="text" value="Search or Select"/> ▼   | Post Auth <input type="text" value="Search or Select"/> ▼ |
| <b>VLAN</b>                           |   |   |
| VLAN/VLAN Group                       | <input type="text" value="76"/> ▼                 |   |
| Multicast VLAN                        | <input type="text" value="Enter Multicast VLAN"/> |   |

Étape 4. À partir de l'interface graphique : accédez à l'onglet Advanced pour configurer les délais d'expiration WLAN, DHCP, WLAN Flex Policy et la politique AAA en cas d'utilisation. Cliquez ensuite sur Update & Apply to Device.

✕
Edit Policy Profile

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

General
Access Policies
QOS and AVC
Mobility
Advanced

### WLAN Timeout

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Guest LAN Session Timeout

### DHCP

IPv4 DHCP Required

DHCP Server IP Address

Show more >>>

### AAA Policy

Allow AAA Override

NAC State

Policy Name  ✕

Accounting List  ⓘ

Fabric Profile

mDNS Service Policy  Clear

Hotspot Server

### User Defined (Private) Network

Status

Drop Unicast

### Umbrella

Umbrella Parameter Map  Clear

Flex DHCP Option for DNS ENABLED

DNS Traffic Redirect IGNORE

### WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

### Air Time Fairness Policies

2.4 GHz Policy

5 GHz Policy

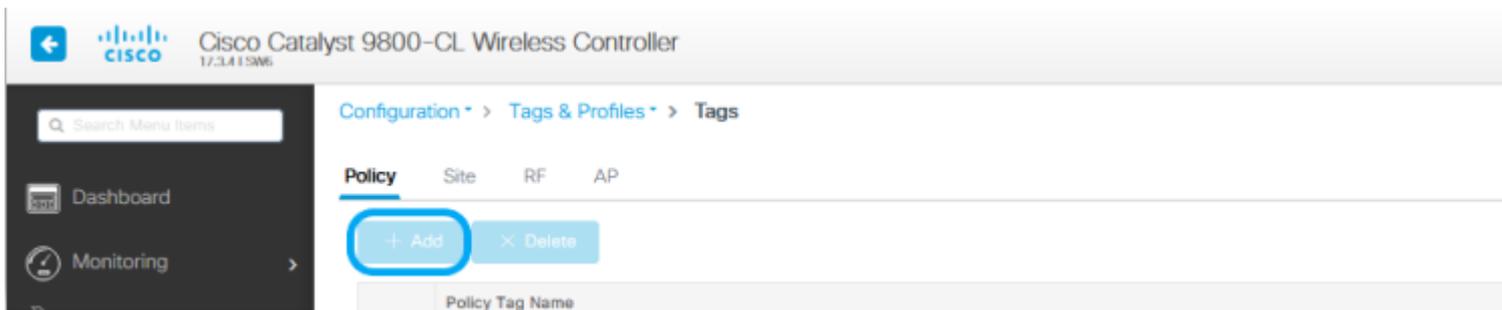
### EoGRE Tunnel Profiles

↶ Cancel

↶
Update & Apply to Device

## Configuration des balises des politiques

Étape 1. Dans l'interface graphique : accédez à Configuration > Tags & Profiles > Tags > Policy > +Add.



Étape 2. Attribuez un nom et mappez le profil de stratégie et le profil WLAN créés avant.

## Edit Policy Tag

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

Name\*

Policy

Description

Enter Description

### WLAN-POLICY Maps: 1

+ Add

× Delete

| WLAN Profile                         | Policy Profile |
|--------------------------------------|----------------|
| <input type="checkbox"/> 802.1x-WLAN | VLANX          |

10 items per page 1 - 1 of 1 items

### Map WLAN and Policy

WLAN Profile\*

802.1x-WLAN

Policy Profile\*

VLANX

×

✓

### > RLAN-POLICY Maps: 0

Cancel

Update & Apply to Device

## Configuration du profil flexible

Étape 1. **Dans l'interface graphique** : accédez à Configuration > Tags & Profiles > Flex et cliquez sur +Add pour en créer un nouveau.

Search Menu Items

Dashboard

Monitoring >

Configuration > Tags & Profiles > Flex

+ Add | X Delete

|                          | Flex Profile Name |
|--------------------------|-------------------|
| <input type="checkbox"/> | SaI_Flex          |

## Edit Flex Profile

### General

Local Authentication

Policy ACL

VLAN

Umbrella

Name\*

Description

Native VLAN ID

HTTP Proxy Port

HTTP-Proxy IP Address

### CTS Policy

Inline Tagging

SGACL Enforcement

CTS Profile Name  ▼

Fallback Radio Shut

Flex Resilient

ARP Caching

Efficient Image Upgrade

OfficeExtend AP

Join Minimum Latency

IP Overlap

mDNS Flex Profile  ▼

**Remarque :** l'ID de VLAN natif fait référence au VLAN utilisé par les AP qui peuvent obtenir ce profil flexible attribué, et il doit s'agir du même ID de VLAN configuré comme natif sur le port de commutateur où les AP sont connectés.

Étape 2. Sous l'onglet VLAN, ajoutez les VLAN nécessaires, ceux affectés par défaut au WLAN via un profil de stratégie, ou ceux poussés par un serveur RADIUS. Cliquez ensuite sur Update & Apply to Device.

## Edit Flex Profile

General Local Authentication Policy ACL **VLAN** Umbrella

+ Add

× Delete

| VLAN Name           | ID | ACL Name |
|---------------------|----|----------|
| No items to display |    |          |

VLAN Name\*

VLAN76

VLAN Id\*

76

ACL Name

Select ACL

✓ Save

↶ Cancel

↶ Cancel

↶ Update

**Remarque** : pour Policy Profile, lorsque vous sélectionnez le VLAN par défaut affecté au SSID. Si vous utilisez un nom de VLAN à cette étape, assurez-vous que vous utilisez le même nom de VLAN dans la configuration Flex Profile, sinon les clients ne pourront pas se connecter au WLAN.

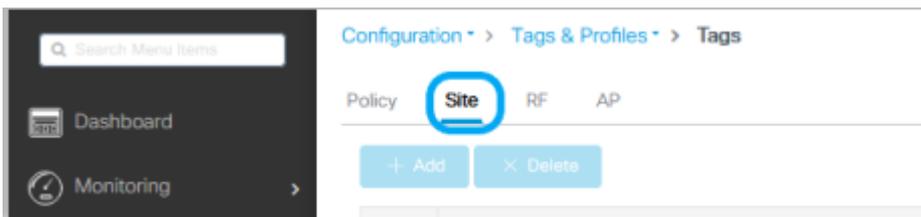
---

**Remarque** : pour configurer une liste de contrôle d'accès pour flexConnect avec remplacement AAA, configurez-la uniquement sur « Policy ACL ». Si une liste de contrôle d'accès est attribuée à un VLAN spécifique, ajoutez ACL on lorsque vous ajoutez le VLAN, puis ajoutez l'ACL sur « Policy ACL ».

---

## Configuration des balises de site

Étape 1. **Dans l'interface GUI**, accédez à Configuration > Tags & Profiles > Tags > Site et cliquez sur +Add pour créer une nouvelle balise de site. Décochez la case Enable Local Site pour permettre aux points d'accès de commuter le trafic de données client localement, et ajoutez le profil flexible créé précédemment.

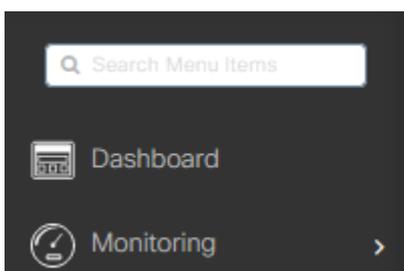


## Edit Site Tag ✕

|                           |   |
|---------------------------|---|
| Name*                     | <input type="text" value="Flex_Site"/>          |
| Description               | <input type="text" value="Flex_Site"/>          |
| AP Join Profile           | <input type="text" value="default-ap-profile"/> |
| Flex Profile              | <input type="text" value="Flex-Pro"/>           |
| Fabric Control Plane Name | <input type="text"/>                            |
| Enable Local Site         | <input type="checkbox"/>                        |

**Remarque :** l'option Activer le site local étant désactivée, les points d'accès auxquels cette balise de site est attribuée peuvent être configurés en mode FlexConnect.

Étape 2. **À partir de l'interface graphique :** accédez à Configuration > Wireless > Access Points > AP name pour ajouter l'étiquette de site et l'étiquette de stratégie à un point d'accès associé. Cela peut entraîner le point d'accès à redémarrer son tunnel CAPWAP et à se joindre à nouveau au WLC 9800.



Configuration > Wireless > Access Points

▼ All Access Points

Number of AP(s): 1

Edit AP
✕

General
Interfaces
High Availability
Inventory
ICap
Advanced
Support Bundle

General

AP Name\*

Location\*

Base Radio MAC

Ethernet MAC

Admin Status ENABLED

AP Mode Local

Operation Status

Fabric Status

LED State ENABLED

LED Brightness Level

**⚠** Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.

Policy

Site Flex\_Site

RF

Write Tag Config to AP

Version

Primary Software Version

Predownload Status

Predownload Version

Next Retry Time

Boot Version

IOS Version

Mini IOS Version

IP Config

CAPWAP Preferred Mode

DHCP IPv4 Address

Static IP (IPv4/IPv6)

Time Statistics

Up Time

Controller Association Latency

↶ Cancel

↶ Update & Apply to Device

Une fois que le point d'accès se reconnecte, notez qu'il est maintenant en mode FlexConnect.

Configuration > Wireless > Access Points

▼ All Access Points

Number of AP(s): 1

| AP Name   | AP Model         | Slots | Admin Status | IP Address  | Base Radio MAC | AP Mode | Operation Status | Configuration Status | Policy Tag | Site Tag  |
|-----------|------------------|-------|--------------|-------------|----------------|---------|------------------|----------------------|------------|-----------|
| talomari1 | AIR-AP2802I-E-K9 | 2     | ✔            | 10.48.70.77 | b4de.31d7.b920 | Flex    | Registered       | Healthy              | Policy     | Flex_Site |

## Authentification locale avec serveur RADIUS externe

Étape 1. Ajoutez le point d'accès en tant que périphérique réseau au serveur RADIUS. Pour un exemple, référez-vous à [Comment utiliser Identity Service Engine \(ISE\) comme serveur RADIUS](#)

Étape 2. Créez un WLAN.

La configuration peut être la même que celle précédemment configurée.

### Add WLAN ✕

**General** Security Advanced

|               |   |                |  |
|---------------|---|----------------|--|
| Profile Name* | <input type="text" value="Local auth"/>     | Radio Policy   | <input style="border: 1px solid #ccc;" type="text" value="All"/> |
| SSID*         | <input type="text" value="Local auth"/>     | Broadcast SSID | <input checked="" type="checkbox"/> ENABLED                      |
| WLAN ID*      | <input type="text" value="9"/>              |                |  |
| Status        | <input checked="" type="checkbox"/> ENABLED |                |  |

Étape 3. Configuration du profil des politiques.

Vous pouvez soit en créer un nouveau, soit utiliser le précédemment configuré. Cette fois, décochez les cases Commutation centrale, Authentification centrale, DHCP central, et Association centrale activée.

## Add Policy Profile



⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

### General

### Access Policies

### QOS and AVC

### Mobility

### Advanced

Name\*

Description

Status  **ENABLED**

Passive Client  DISABLED

Encrypted Traffic Analytics  DISABLED

#### CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

#### WLAN Switching Policy

Central Switching  DISABLED

Central Authentication  DISABLED

Central DHCP  DISABLED

Central Association  DISABLED

Flex NAT/PAT  DISABLED

Cancel

Apply to Device

Étape 4. Configuration des balises de politiques.

Associez le WLAN configuré et le profil de stratégie créé.

Étape 5. Configuration du profil flexible.

Créez un profil flexible, accédez à l'onglet Authentification locale, configurez le groupe de serveurs Radius et cochez la case RADIUS.

## Edit Flex Profile

General **Local Authentication** Policy ACL VLAN Umbrella

Radius Server Group

AmmISE

Local Accounting Radius Server Group

Select Accounting S

Local Client Roaming

EAP Fast Profile

Select Profile

LEAP

PEAP

TLS

RADIUS

### Users

+ Add

× Delete

Select File

Select CSV File



Upload

Username

0 10 items per page

No items to display

Cancel

Update

Étape 6. Configuration des balises de site.

Configurez le profil paramétrable configuré à l'étape 5 et décochez la case Enable Local Site.

## Add Site Tag

|                           |                          |
|---------------------------|--------------------------|
| Name*                     | Local Auth               |
| Description               | Enter Description        |
| AP Join Profile           | default-ap-profile ▼     |
| Flex Profile              | Local ▼                  |
| Fabric Control Plane Name | ▼                        |
| Enable Local Site         | <input type="checkbox"/> |

Cancel

Apply to D

## Vérifier

À partir de l'interface utilisateur graphique : accédez à **Surveillance** > **Sans fil** > **Clients**, puis confirmez l'état du **Gestionnaire de stratégies** et les paramètres FlexConnect.

Authentification centrale :

| Client                          |                         |
|---------------------------------|-------------------------|
| General                         |                         |
| Client Properties               |                         |
| MAC Address                     | 484b.aa52.5937          |
| IPv4 Address                    | 172.16.76.41            |
| User Name                       | address1                |
| Policy Profile                  | VLAN2669                |
| Flex Profile                    | RemoteSite1             |
| Wireless LAN Id                 | 1                       |
| Wireless LAN Name               | eWLC_do1x               |
| BSSID                           | 38ed.18c6.932f          |
| Uptime(sec)                     | 9 seconds               |
| CCX version                     | No CCX support          |
| Power Save mode                 | OFF                     |
| Supported Rates                 | 9.0,18.0,36.0,48.0,54.0 |
| Policy Manager State            | Run                     |
| Last Policy Manager State       | IP Learn Complete       |
| Encrypted Traffic Analytics     | No                      |
| Multicast VLAN                  | 0                       |
| Access VLAN                     | 2669                    |
| Anchor VLAN                     | 0                       |
| Server IP                       | 10.88.173.94            |
| DNS Snooped IPv4 Addresses      | None                    |
| DNS Snooped IPv6 Addresses      | None                    |
| 11v DMS Capable                 | No                      |
| FlexConnect Data Switching      | Local                   |
| FlexConnect DHCP Status         | Local                   |
| FlexConnect Authentication      | Central                 |
| FlexConnect Central Association | Yes                     |

Authentification locale :

| Client                          |                |                         |                   |                 |
|---------------------------------|----------------|-------------------------|-------------------|-----------------|
| General                         | QOS Statistics | ATF Statistics          | Mobility History  | Call Statistics |
| Client Properties               | AP Properties  | Security Information    | Client Statistics | QOS Properties  |
| MAC Address                     |                | 484b.aa52.5937          |                   |                 |
| IPv4 Address                    |                | 172.16.76.41            |                   |                 |
| IPv6 Address                    |                | fe80::80be782:7c78:68f9 |                   |                 |
| User Name                       |                | addressi                |                   |                 |
| Policy Profile                  |                | VLAN2669                |                   |                 |
| Flex Profile                    |                | RemoteSite1             |                   |                 |
| Wireless LAN Id                 |                | 1                       |                   |                 |
| Wireless LAN Name               |                | eWLC_do1x               |                   |                 |
| BSSID                           |                | 38ed.18c6.932f          |                   |                 |
| Uptime(sec)                     |                | 11 seconds              |                   |                 |
| CCX version                     |                | No CCX support          |                   |                 |
| Power Save mode                 |                | OFF                     |                   |                 |
| Policy Manager State            |                | Run                     |                   |                 |
| Last Policy Manager State       |                | IP Learn Complete       |                   |                 |
| Encrypted Traffic Analytics     |                | No                      |                   |                 |
| Multicast VLAN                  |                | 0                       |                   |                 |
| Access VLAN                     |                | 2669                    |                   |                 |
| Anchor VLAN                     |                | 0                       |                   |                 |
| DNS Snooped IPv4 Addresses      |                | None                    |                   |                 |
| DNS Snooped IPv6 Addresses      |                | None                    |                   |                 |
| 11v DMS Capable                 |                | No                      |                   |                 |
| FlexConnect Data Switching      |                | Local                   |                   |                 |
| FlexConnect DHCP Status         |                | Local                   |                   |                 |
| FlexConnect Authentication      |                | Local                   |                   |                 |
| FlexConnect Central Association |                | No                      |                   |                 |

Vous pouvez utiliser ces commandes pour vérifier la configuration actuelle:

### À partir de CLI :

```
# show wlan { summary | id | name | all }
# show run wlan
# show run aaa
# show aaa servers
# show ap config general
# show ap name <ap-name> config general
# show ap tag summary
# show ap name <AP-name> tag detail
# show wlan { summary | id | name | all }
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
```

## Dépannage

Le WLC 9800 offre des fonctionnalités de suivi ALWAYS-ON. Cela garantit que tous les messages d'erreur, d'avertissement et de niveau de notification liés à la connectivité du client sont constamment consignés et que vous pouvez afficher les journaux d'un incident ou d'une défaillance après qu'il se soit produit.

---

**Remarque :** en fonction du volume de journaux générés, vous pouvez revenir en arrière de quelques heures à plusieurs jours.

---

Afin d'afficher les traces que le WLC 9800 a collectées par défaut, vous pouvez vous connecter via SSH/Telnet au WLC 9800 et passer par ces étapes (assurez-vous que vous consignez la session dans un fichier texte).

Étape 1. Vérifiez l'heure actuelle du contrôleur de sorte que vous puissiez suivre les journaux dans l'heure

jusqu'à quand le problème s'est produit.

### À partir de CLI :

```
# show clock
```

Étape 2. Collectez les syslogs à partir de la mémoire tampon du contrôleur ou du syslog externe, comme dicté par la configuration système. Cela permet d'obtenir un aperçu rapide de l'état du système et des erreurs éventuelles.

### À partir de CLI :

```
# show logging
```

Étape 3. Vérifiez si les conditions de débogage sont activées.

### À partir de CLI :

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Tracing Configs:

Packet Infra debugs:
```

| Ip Address | Port  |
|------------|-------|
| -----      | ----- |

---

**Remarque :** si vous trouvez une condition répertoriée, cela signifie que les traces sont enregistrées au niveau de débogage pour tous les processus qui rencontrent les conditions activées (adresse MAC, adresse IP, etc.). Cela augmenterait le volume de journaux. Par conséquent, il est recommandé d'effacer toutes les conditions lorsque le débogage n'est pas actif.

---

Étape 4. Si vous supposez que l'adresse MAC testée n'était pas répertoriée comme condition à l'étape 3, collectez les traces de niveau de notification toujours actif pour l'adresse MAC spécifique.

### À partir de CLI :

```
# show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file always-on-
```

Vous pouvez soit afficher le contenu de la session, soit copier le fichier sur un serveur TFTP externe.

### À partir de CLI :

```
# more bootflash:always-on-<FILENAME.txt>
or
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

### Débogage conditionnel et suivi actif radio

Si les traces toujours actives ne vous donnent pas suffisamment d'informations pour déterminer le déclencheur du problème en cours d'investigation, vous pouvez activer le débogage conditionnel et capturer la trace Radio Active (RA), qui peut fournir des traces de niveau de débogage pour tous les processus qui interagissent avec la condition spécifiée (adresse MAC du client dans ce cas). Afin d'activer le débogage conditionnel, passez par ces étapes.

Étape 5. Assurez-vous qu'aucune condition de débogage n'est activée.

### À partir de CLI :

```
# clear platform condition all
```

Étape 6. Activez la condition de débogage pour l'adresse MAC du client sans fil que vous souhaitez surveiller.

Cette commande commence à surveiller l'adresse MAC fournie pendant 30 minutes (1 800 secondes). Vous pouvez aussi augmenter ce délai pour qu'il atteigne jusqu'à 2085978494 secondes.

### À partir de CLI :

```
# debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

---

**Remarque :** Afin de surveiller plusieurs clients à la fois, exécutez la <aaaa.bbbb.cccc>commande de débogage sans fil mac par adresse MAC.

---

**Remarque :** vous ne voyez pas le résultat de l'activité du client sur la session du terminal, car tout est mis en mémoire tampon en interne pour être visualisé ultérieurement.

---

Étape 7. Reproduisez le problème ou le comportement que vous souhaitez surveiller.

Étape 8. Arrêtez le débogage si le problème est reproduit avant la fin du temps de surveillance par défaut ou

configuré.

### À partir de CLI :

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

Une fois que le temps de surveillance sâ€™est écoulé ou que le débogage sans fil a été arrêté, le contrôleur WLC 9800 génère un fichier local du nom de :

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Étape 9. Recueillir le fichier de l’activité de l’adresse MAC. Il est possible de copier le fichier de suivi RA .log sur un serveur externe ou d’afficher le résultat directement à l’écran.

Vérifiez le nom du fichier de suivi RA

### À partir de CLI :

```
# dir bootflash: | inc ra_trace
```

Copiez le fichier sur un serveur externe :

### À partir de CLI :

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.d
```

Affichez-en le contenu :

### À partir de CLI :

```
# more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Étape 10. Si vous ne trouvez toujours pas la cause première, collectez les journaux internes, qui peuvent vous offrir une vue plus détaillée des journaux de niveau de débogage. Vous n’avez pas besoin de déboguer à nouveau le client car vous avez examiné en détail les journaux de débogage qui ont déjà été collectés et stockés en interne.

### À partir de CLI :

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file ra
```

---

**Remarque** : cette sortie de commande retourne des traces pour tous les niveaux de journalisation pour tous les processus et est assez volumineuse. Veuillez faire appel à Cisco TAC pour faciliter l'analyse de ces suivis.

---

Vous pouvez soit copier le fichier ra-internal-FILENAME.txt sur un serveur externe, soit afficher le résultat directement à l'écran.

Copiez le fichier sur un serveur externe :

**À partir de CLI :**

```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```

Affichez-en le contenu :

**À partir de CLI :**

```
# more bootflash:ra-internal-<FILENAME>.txt
```

Étape 11. Supprimez les conditions de débogage.

**À partir de CLI :**

```
# clear platform condition all
```

---

**Remarque** : assurez-vous de toujours supprimer les conditions de débogage après une session de dépannage.

---

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.