

Comprendre FlexConnect sur le contrôleur sans fil Catalyst 9800

Table des matières

[Introduction](#)

[Informations générales](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Diagramme du réseau](#)

[Configurations](#)

[Créer/modifier un profil WLAN](#)

[Créer/modifier un profil de stratégie](#)

[Créer/modifier une balise de stratégie](#)

[Créer/modifier un profil flexible](#)

[Créer/modifier une balise de site](#)

[Affectation de balise de stratégie au point d'accès](#)

[Attribution de balise de stratégie par AP](#)

[Attribution de balise de stratégie pour plusieurs points d'accès](#)

[ACL Flexconnect](#)

[WLAN à commutation centrale](#)

[WLAN commuté localement](#)

[Vérifier si la liste de contrôle d'accès est appliquée](#)

[Vérification](#)

[Configuration des VLAN/interfaces](#)

[Configuration d'un réseau local sans fil \(WLAN\)](#)

[Configuration de point d'accès](#)

[Configuration des balises](#)

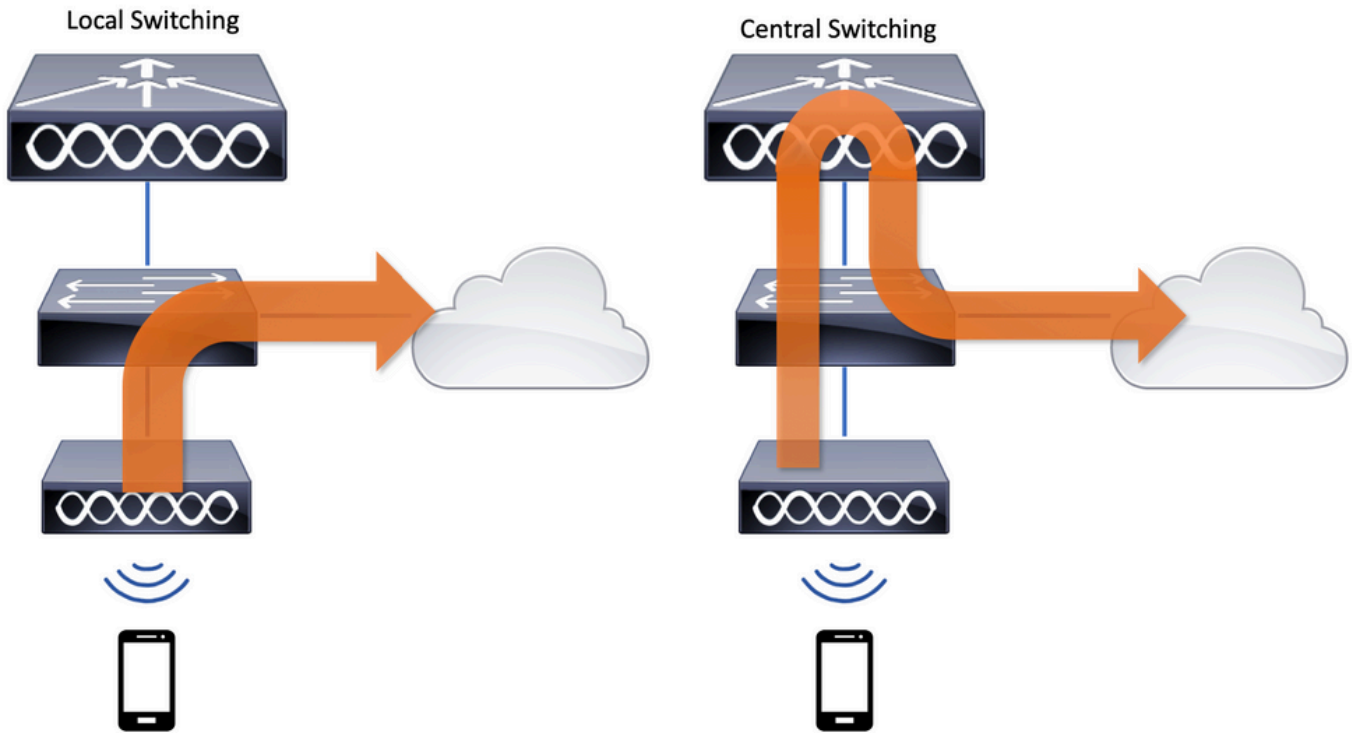
[Configuration du profil](#)

Introduction

Ce document décrit la fonctionnalité FlexConnect et sa configuration générale sur les contrôleurs sans fil 9800.

Informations générales

FlexConnect fait référence à la capacité d'un point d'accès (AP) à déterminer si le trafic provenant des clients sans fil est placé directement sur le réseau au niveau du point d'accès (commutation locale) ou si le trafic est centralisé vers le contrôleur 9800 (commutation centrale).



Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

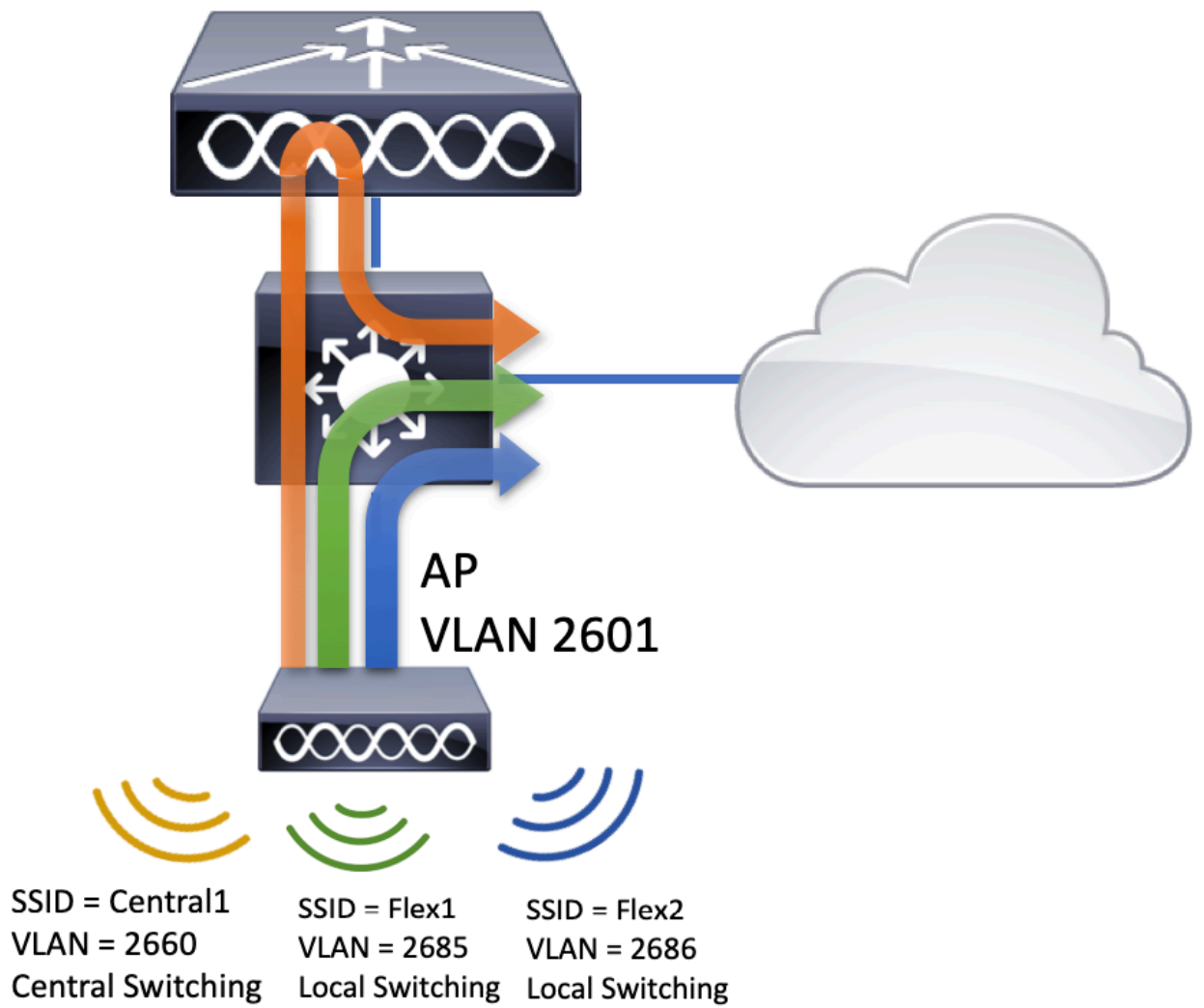
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Contrôleurs sans fil Cisco Catalyst 9800 avec Cisco IOS®-XE Gibraltar v17.3.x

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.

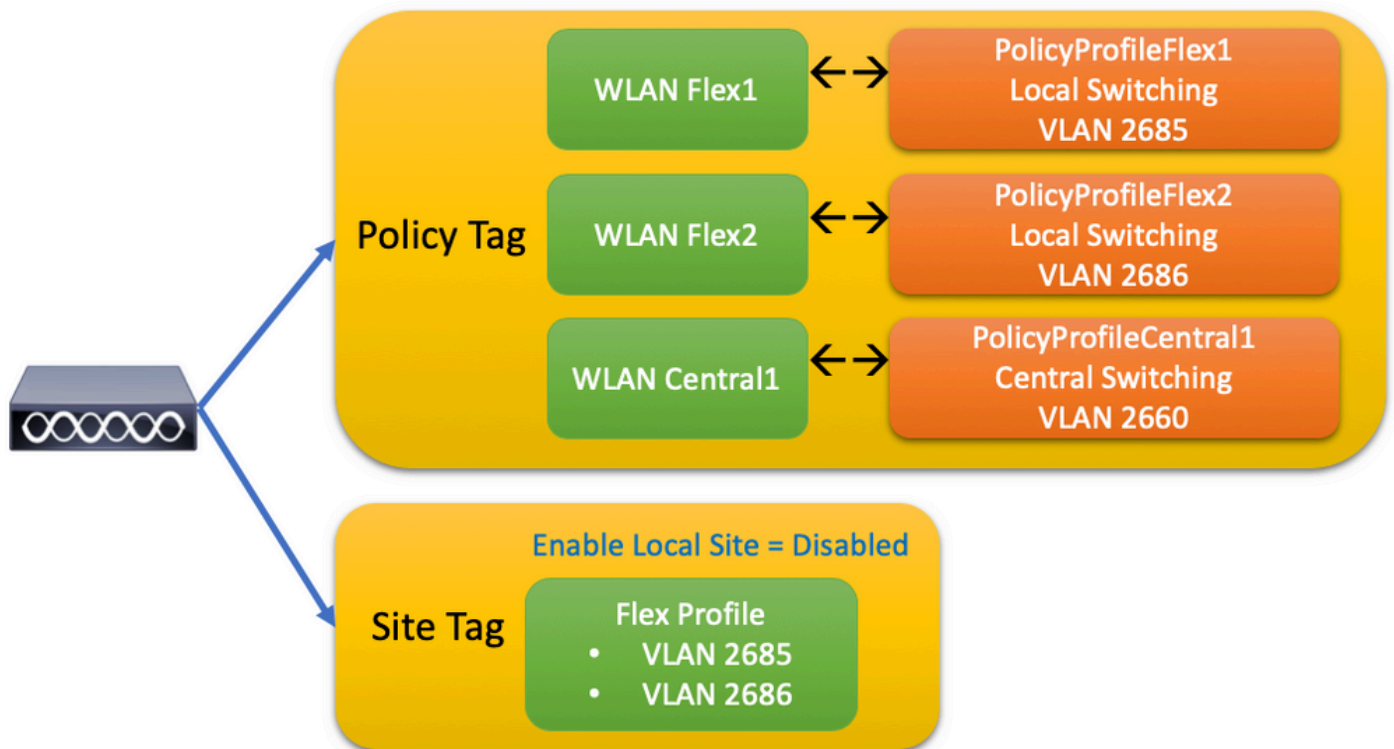
Diagramme du réseau

Le présent document se fonde sur la topologie suivante :



Configurations

Voici le schéma visuel de la configuration qui est nécessaire pour accomplir le scénario de ce document :



Pour configurer un SSID (Local Switching Service Set Identifier) FlexConnect, voici les étapes générales à suivre :

1. Créer/modifier un profil WLAN
2. Créer/modifier un profil de stratégie
3. Créer/modifier une balise de stratégie
4. Créer/modifier un profil flexible
5. Créer/modifier une balise de site
6. Affectation de balise de stratégie au point d'accès

Ces sections expliquent comment configurer chacun d'eux, étape par étape.

Créer/modifier un profil WLAN

Vous pouvez utiliser ce guide pour créer les trois SSID suivants :

[Créez votre SSID](#)

Search Menu Items

- Dashboard
- Monitoring >
- Configuration >
- Administration >

WIRELESS NETWORKS

Number of WLANs selected : 0

<input type="checkbox"/>	Name	ID	SSID
<input type="checkbox"/>	Flex1	2	Flex1
<input type="checkbox"/>	Flex2	3	Flex2
<input type="checkbox"/>	Central1	4	Central1

Créer/modifier un profil de stratégie

Étape 1. Accédez à Configuration > Tags & Profiles > Policy. Sélectionnez le nom d'un nom qui existe déjà ou cliquez sur + Ajouter pour en ajouter un nouveau.

Add Policy Profile ✕

General

Access Policies

QOS and AVC

Mobility

Advanced

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

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 ENABLED

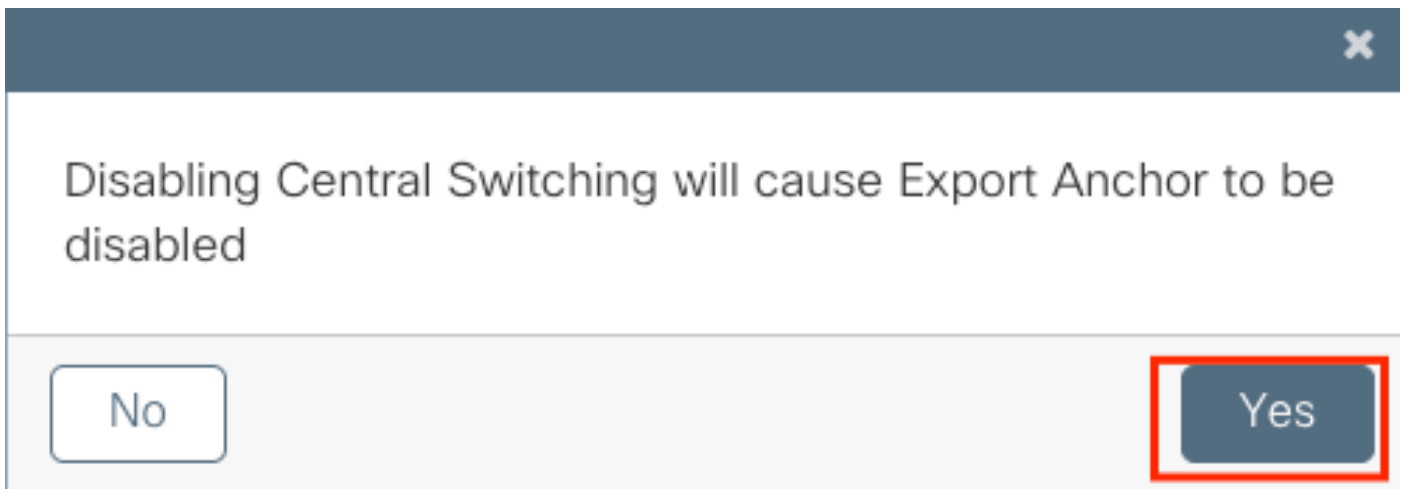
Central DHCP DISABLED

Central Association DISABLED

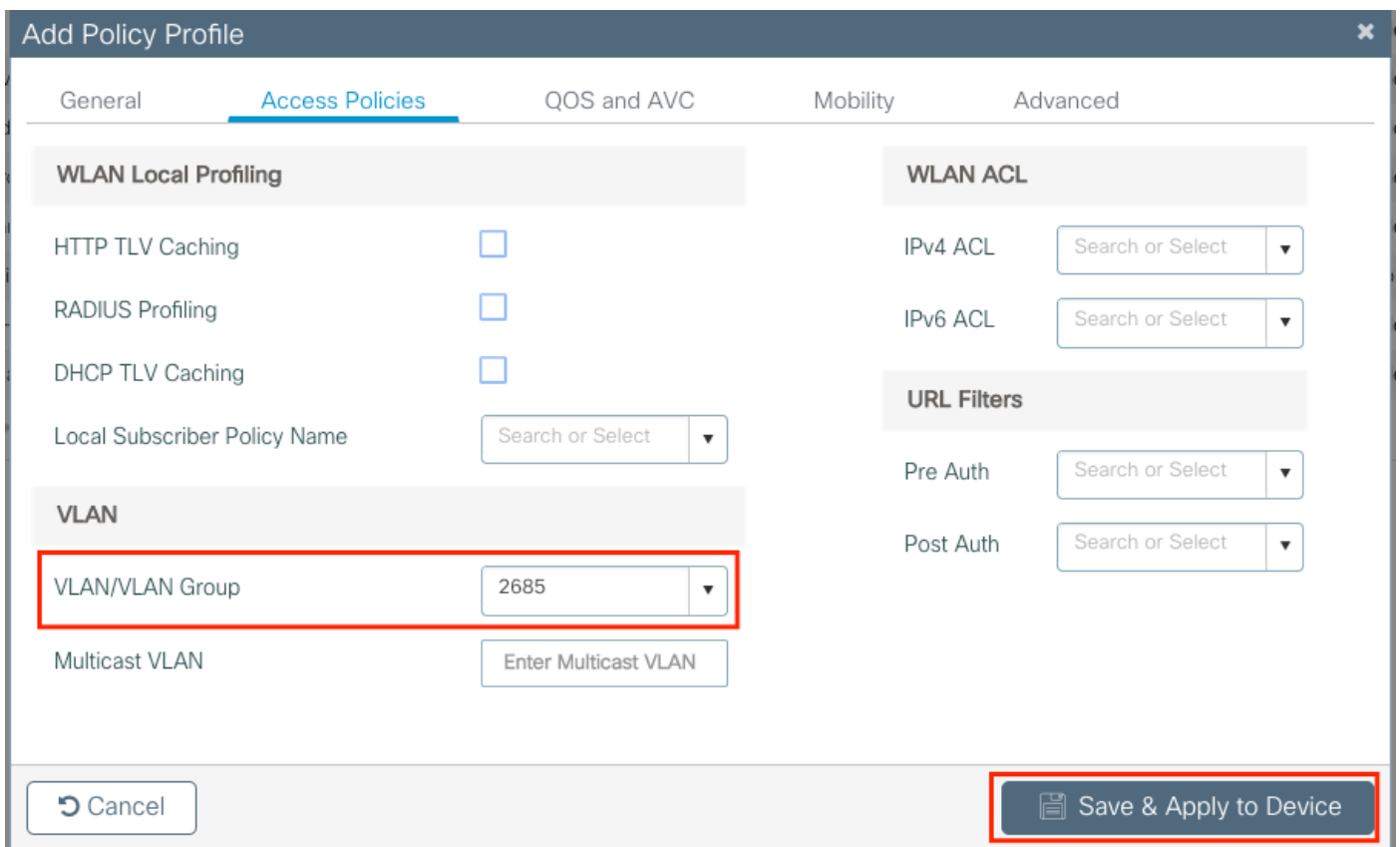
Flex NAT/PAT DISABLED

↶ Cancel

Lorsque vous désactivez Central Switching ce message d'avertissement s'affiche, cliquez sur Yes et poursuivez la configuration.



Étape 2. Accédez à l'Access Policies onglet et tapez le VLAN (Vous ne le voyez pas dans la liste déroulante parce que ce VLAN n'existe pas sur le WLC 9800). Après cela, cliquez sur Save & Apply to Device.



Étape 3. Répétez la même procédure pour PolicyProfileFlex2.

Add Policy Profile ✕

General Access Policies QOS and AVC Mobility Advanced

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

<p>Name* <input type="text" value="PolicyProfileFlex2"/></p> <p>Description <input type="text" value="Enter Description"/></p> <p>Status ENABLED <input checked="" type="checkbox"/></p> <p>Passive Client DISABLED <input type="checkbox"/></p> <p>Encrypted Traffic Analytics DISABLED <input type="checkbox"/></p> <p>CTS Policy</p> <p>Inline Tagging <input type="checkbox"/></p> <p>SGACL Enforcement <input type="checkbox"/></p> <p>Default SGT <input type="text" value="2-65519"/></p>	<p>WLAN Switching Policy</p> <p>Central Switching DISABLED <input type="checkbox"/></p> <p>Central Authentication ENABLED <input checked="" type="checkbox"/></p> <p>Central DHCP DISABLED <input type="checkbox"/></p> <p>Central Association DISABLED <input type="checkbox"/></p> <p>Flex NAT/PAT DISABLED <input type="checkbox"/></p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


Add Policy Profile ✕

General Access Policies QOS and AVC Mobility Advanced

<p>WLAN Local Profiling</p> <p>HTTP TLV Caching <input type="checkbox"/></p> <p>RADIUS Profiling <input type="checkbox"/></p> <p>DHCP TLV Caching <input type="checkbox"/></p> <p>Local Subscriber Policy Name <input type="text" value="Search or Select"/></p> <p>VLAN</p> <p>VLAN/VLAN Group <input type="text" value="2686"/></p> <p>Multicast VLAN <input type="text" value="Enter Multicast VLAN"/></p>	<p>WLAN ACL</p> <p>IPv4 ACL <input type="text" value="Search or Select"/></p> <p>IPv6 ACL <input type="text" value="Search or Select"/></p> <p>URL Filters</p> <p>Pre Auth <input type="text" value="Search or Select"/></p> <p>Post Auth <input type="text" value="Search or Select"/></p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Étape 4. Pour le SSID à commutation centrale, assurez-vous que son VLAN nécessaire existe sur

le WLC 9800 et sinon, créez-le.

 Remarque : dans les points d'accès FlexConnect avec des WLAN commutés localement, le trafic est commuté au niveau du point d'accès et les requêtes DHCP du client vont directement dans le réseau câblé par l'interface du point d'accès. L'AP n'a pas d'interface SVI dans le sous-réseau client, il n'est donc pas en mesure d'effectuer le proxy DHCP ; et par conséquent, la configuration du relais DHCP (adresse IP du serveur DHCP), dans l'onglet Policy Profile > Advanced, n'a aucune signification pour les WLAN commutés localement. Dans ces scénarios, le port de commutation doit autoriser le VLAN client, puis, si le serveur DHCP se trouve dans un autre VLAN, configurer l'assistant IP dans l'interface SVI/passarelle par défaut du client afin qu'il sache où envoyer la requête DHCP du client.

[Déclarer les VLAN clients](#)

Étape 5. Créez un profil de stratégie pour le SSID central.

Accédez à Configuration > Tags & Profiles > Policy. Sélectionnez le nom d'un nom qui existe déjà ou cliquez sur + Add pour en ajouter un nouveau.

Add Policy Profile ✕

General Access Policies QOS and AVC Mobility Advanced

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

Name*	<input type="text" value="PolicyProfileCentral1"/>	WLAN Switching Policy
Description	<input type="text" value="Enter Description"/>	<input checked="" type="checkbox"/> Central Switching
Status	<input checked="" type="checkbox"/> ENABLED	<input checked="" type="checkbox"/> Central Authentication
Passive Client	<input type="checkbox"/> DISABLED	<input checked="" type="checkbox"/> Central DHCP
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED	<input checked="" type="checkbox"/> Central Association
CTS Policy		<input type="checkbox"/> Flex NAT/PAT
Inline Tagging	<input type="checkbox"/>	
SGACL Enforcement	<input type="checkbox"/>	
Default SGT	<input type="text" value="2-65519"/>	

Add Policy Profile

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

WLAN Local Profiling

HTTP TLV Caching

RADIUS Profiling

DHCP TLV Caching

Local Subscriber Policy Name

VLAN

VLAN/VLAN Group

Multicast VLAN

WLAN ACL

IPv4 ACL

IPv6 ACL

URL Filters

Pre Auth

Post Auth

Par conséquent, il existe trois profils de stratégie.

	Policy Profile Name	Description
<input type="checkbox"/>	PolicyProfileFlex1	
<input type="checkbox"/>	PolicyProfileFlex2	
<input type="checkbox"/>	PolicyProfileCentral1	

1 10 items per page

CLI :

```
# config t
# vlan 2660
# exit

# wireless profile policy PolicyProfileFlex1
# no central switching
# vlan 2685
# no shutdown
# exit

# wireless profile policy PolicyProfileFlex2
# no central switching
```

```
# vlan 2686
# no shutdown
# exit

# wireless profile policy PolicyProfileCentral1
# vlan VLAN2660
# no shutdown
# end
```

Créer/modifier une balise de stratégie

La balise de stratégie est l'élément qui vous permet de spécifier quel SSID est lié à quel profil de stratégie.

Étape 1. Accédez à [Configuration > Tags & Profiles > Tags > Policy](#). Sélectionnez le nom d'un nom qui existe déjà ou cliquez sur **+ Add** pour en ajouter un nouveau.

	Policy Tag Name
<input type="checkbox"/>	PT1
<input type="checkbox"/>	PT2
<input type="checkbox"/>	PT3
<input type="checkbox"/>	PolTag1
<input type="checkbox"/>	new-policy

Étape 2. Dans la balise de stratégie, cliquez sur **+Add**, dans la liste déroulante, sélectionnez le **WLAN Profile** nom à ajouter à la balise de stratégie et **Policy Profile** auquel vous souhaitez la lier. Ensuite, cliquez sur la coche.

Add Policy Tag ✕

Name*

Description

WLAN Profile Policy Profile

◀ ◁ 0 ▷ ▶ 10 items per page No items to display

Add Policy Tag ✕

Name*

Description

WLAN Profile Policy Profile

◀ ◁ 0 ▷ ▶ 10 items per page No items to display

Map WLAN and Policy

WLAN Profile*

Policy Profile*

Répétez l' pour les trois SSID, puis cliquez sur Save & Apply to Device.

Add Policy Tag
✕

Name*

Description

+ Add
✕ Delete

	WLAN Profile	Policy Profile
<input type="checkbox"/>	Flex1	PolicyProfileFlex1
<input type="checkbox"/>	Flex2	PolicyProfileFlex2
<input type="checkbox"/>	Central1	PolicyProfileCentral1

⏪ ◀ 1 ▶ ⏩
 items per page
1 - 3 of 3 items

↶ Cancel
📄 Save & Apply to Device

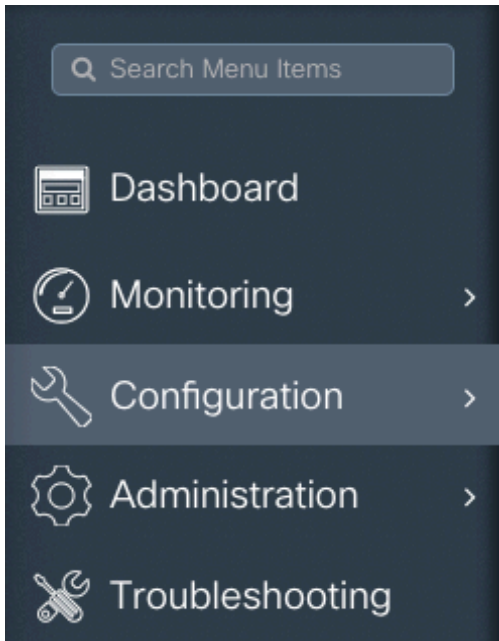
CLI :

```
# config t
# wireless tag policy PolicyTag1
# wlan Flex1 policy PolicyProfileFlex1
# wlan Flex2 policy PolicyProfileFlex2
# wlan Central1 policy PolicyProfileCentral1
# end
```

Créer/modifier un profil flexible

Dans la topologie utilisée pour ce document, notez qu'il y a deux SSID dans la commutation locale avec deux VLAN différents. À l'intérieur du profil Flex, vous spécifiez le VLAN des AP (VLAN natif) et tout autre VLAN dont le point d'accès doit avoir connaissance, dans ce cas, les VLAN utilisés par les SSID.

Étape 1. Accédez à [Configuration > Tags & Profiles > Flex](#) et créez-en un nouveau ou modifiez-en un qui existe déjà.



Flex Profile



	Flex Profile Name
<input type="checkbox"/>	new-flex-profile
<input type="checkbox"/>	default-flex-profile

Navigation controls: 1 (current page), 10 items per page

Étape 2. Définissez un nom pour le profil flexible et spécifiez le VLAN AP (ID de VLAN natif).

Add Flex Profile

General | Local Authentication | Policy ACL | VLAN

Name*	FlexProfileLab	Multicast Overridden Interface	<input type="checkbox"/>
Description	Enter Description	Fallback Radio Shut	<input type="checkbox"/>
Native VLAN ID	2601	Flex Resilient	<input type="checkbox"/>
HTTP Proxy Port	0	ARP Caching	<input type="checkbox"/>
HTTP-Proxy IP Address	0.0.0.0	Efficient Image Upgrade	<input checked="" type="checkbox"/>
CTS Policy		Office Extend AP	<input type="checkbox"/>
Inline Tagging	<input type="checkbox"/>	Join Minimum Latency	<input type="checkbox"/>
SGACL Enforcement	<input type="checkbox"/>		
CTS Profile Name	default-sxp-profile x		

Buttons: Cancel | Save & Apply to Device

Étape 3. Accédez à l'**VLAN** onglet et spécifiez le VLAN requis.

Dans ce scénario, il y a des clients sur les VLAN 2685 et 2686. Ces VLAN n'existent pas sur le WLC 9800, ajoutez-les au profil Flex afin qu'ils existent sur le point d'accès.

Add Flex Profile ✕

General Local Authentication Policy ACL VLAN

+ Add ✕ Delete

VLAN Name	ID	ACL Name
◀ ▶ 0 ▶ ▶ 10 items per page No items to display		

↶ Cancel Save & Apply to Device

VLAN Name*

VLAN Id*

ACL Name Select ACL ▼

✓ Save

↶ Cancel

Remarque : lorsque vous avez créé le profil de stratégie, si vous avez sélectionné un nom de VLAN au lieu d'un ID de VLAN, assurez-vous que le nom de VLAN ici dans le profil flexible est exactement le même.

Répétez l' pour les VLAN nécessaires.

Add Flex Profile ✕

General Local Authentication Policy ACL VLAN

+ Add ✕ Delete

VLAN Name	ID	ACL Name
<input type="checkbox"/> VLAN2685	2685	
<input type="checkbox"/> VLAN2686	2686	

◀ ▶ 1 ▶ ▶ 10 items per page
 1 - 2 of 2 items

↶ Cancel Save & Apply to Device

Notez que le VLAN utilisé pour la commutation centrale n'a pas été ajouté, car le point d'accès n'a

pas besoin d'en être conscient.

CLI :

```
# config t
# wireless profile flex FlexProfileLab
# native-vlan-id 2601
# vlan-name VLAN2685
# vlan-id 2685
# vlan-name VLAN2686
# vlan-id 2686
# end
```

Créer/modifier une balise de site

La balise de site est l'élément qui vous permet de spécifier quelle jointure AP et/ou quel profil flexible est affecté aux AP.

Étape 1. Accédez à **Configuration > Tags & Profiles > Tags > Site**. Sélectionnez le nom d'un nom qui existe déjà ou cliquez sur **+ Add** pour en ajouter un nouveau.

Site Tag Name
<input type="checkbox"/> ST1

Étape 2. À l'intérieur de la balise de site, désactivez l'**Enable Local Siteoption** (tout point d'accès qui reçoit une balise de site avec l'**Enable Local Siteoption** désactivée est converti en mode FlexConnect). Une fois la fonction désactivée, vous pouvez également sélectionner la **Flex Profile**. Après cela, cliquez sur **Save & Apply to Device**.

Add Site Tag ✕

Name*	FlexSite1
Description	Enter Description
AP Join Profile	default-ap-profile ▼
Flex Profile	FlexProfileLab ▼
Control Plane Name	▼
Enable Local Site	<input type="checkbox"/>

↶ Cancel 📄 Save & Apply to Device

CLI :

```
# config t
# wireless tag site FlexSite1
# flex-profile FlexProfileLab
# no local-site
```

Affectation de balise de stratégie au point d'accès

Vous pouvez attribuer une balise de stratégie directement à un point d'accès ou attribuer la même balise de stratégie à un groupe de points d'accès en même temps. Choisissez celui qui vous convient.

Attribution de balise de stratégie par AP

Accédez à Configuration > Wireless > Access Points > AP name > General > Tags. Dans la liste site déroulante, sélectionnez les balises souhaitées, puis cliquez sur Update & Apply to Device.

Edit AP



General

Interfaces

High Availability

Inventory

Advanced

General

AP Name*	<input type="text" value="AP1702-05"/>
Location*	<input type="text" value="karlcisn-WS"/>
Base Radio MAC	00c0.0000.0000
Ethernet MAC	00f0.0000.0000
Admin Status	<input type="button" value="Enabled"/>
AP Mode	<input type="button" value="Flex"/>
Operation Status	Registered
Fabric Status	Disabled

Tags

⚠ Changing Tags will cause the AP to momentarily lose association with the Controller.

Policy	<input type="button" value="PolicyTag1"/>
Site	<input type="button" value="FlexSite1"/>
RF	<input type="button" value="default-rf-tag"/>

Version

Primary Software Version	16.10.1.0
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A
Boot Version	15.3.0.0
IOS Version	15.3(3)JPG1S
Mini IOS Version	0.0.0.0


IP Config


CAPWAP Preferred Mode	Not Configured
DHCP IPv4 Address	172.16.1.110
Static IP (IPv4/IPv6)	<input type="checkbox"/>

Time Statistics

Up Time	6 days 20 hrs 27 mins 53 secs
Controller Association Latency	5 days 18 hrs 0 mins 30 secs

Remarque : sachez qu'après modification, la balise de stratégie sur un point d'accès perd

 son association avec les WLC 9800 et se reconnecte dans environ 1 minute.


 Remarque : si l'AP est configuré en mode Local (ou tout autre mode) et qu'il obtient une balise de site avec l'Enable Local Siteoption désactivée, l'AP redémarre et revient en mode FlexConnect.

CLI :

```
# config t
# ap <ethernet-mac-addr>
# site-tag <site-tag-name>
# end
```

Attribution de balise de stratégie pour plusieurs points d'accès

Accédez à **Configuration > Wireless Setup > Advanced > Start Now**.

Cliquez sur l'icône Tag APs:, après cela, sélectionnez la liste des AP auxquels vous voulez attribuer les balises (Vous pouvez cliquer sur la flèche pointant vers le bas à côté de AP name[ou tout autre champ] pour filtrer la liste des AP).

Number of APs: 2

Selected Number of APs: 2

The screenshot shows a table of APs with a filter dropdown menu open. The dropdown menu contains the text "Show items with value that:" followed by a selection box containing "Is equal to". Below the selection box are two buttons: "Filter" (green) and "Clear" (grey).

<input type="checkbox"/>	AP Name	AP
<input checked="" type="checkbox"/>	AP3802-karlcisn	
<input checked="" type="checkbox"/>	AP2802-01	

Filter dropdown menu content:

Show items with value that:

Is equal to

Filter Clear

Une fois que vous avez sélectionné les AP désirés, cliquez sur + Tag APs.

Advanced Wireless Setup

Back

The screenshot shows the "Advanced Wireless Setup" interface. On the left, a vertical navigation pane lists various setup steps: Start, Tags & Profiles (WLAN Profile, Policy Profile, Policy Tag, AP Join Profile, Flex Profile, Site Tag), RF Profile, RF Tag, Apply, and Tag APs. The "Tag APs" step is highlighted with a red box. On the right, a table displays the selected APs. The table has columns for AP Name, AP Model, AP MAC, AP Mode, Admin Status, Operation Status, Policy Tag, Site Tag, RF Tag, Location, Country, and Hyperlocation Method. Two APs are selected, indicated by checkmarks in the first column. Below the table, there is a pagination control showing "10 items per page" and "1 - 2 of 2 items".

+ Tag APs

Number of APs: 2
Selected Number of APs: 2

<input type="checkbox"/>	AP Name	AP Model	AP MAC	AP Mode	Admin Status	Operation Status	Policy Tag	Site Tag	RF Tag	Location	Country	Hyperlocation Method
<input checked="" type="checkbox"/>	AP3802-karlcisn	AIR-AP3802I-A-K9	0042.68c6.4120	Local	Disabled	Registered	Location-typical-density	Location-typical-density	Location-typical-density	default location	MX	Local
<input checked="" type="checkbox"/>	AP2802-01	AIR-AP2802I-B-K9	2c5a.0f40.6900	Local	Enabled	Registered	PT1	default-site-tag	default-rf-tag	CALO	US	Local

10 items per page 1 - 2 of 2 items

Sélectionnez les balises que vous souhaitez attribuer aux points d'accès et cliquez sur **Save & Apply to Device**.

Tag APs ✕


Tags


Policy ▼

Site ▼

RF ▼

Changing AP Tag(s) will cause associated AP(s) to reconnect

 Remarque : sachez qu'après avoir modifié la balise de stratégie sur un AP, il perd son association aux WLC 9800 et se reconnecte dans environ 1 minute.

 Remarque : si l'AP est configuré en mode local (ou tout autre mode) et qu'il obtient une balise de site avec l'Enable Local Site option désactivée, l'AP redémarre et revient en mode FlexConnect.

CLI :

Il n'y a pas d'option CLI pour attribuer la même balise à plusieurs AP.

ACL Flexconnect

Lorsque vous disposez d'un réseau local sans fil commuté, il convient de réfléchir à la manière d'appliquer une liste de contrôle d'accès aux clients.

Dans le cas d'un WLAN à commutation centrale, tout le trafic est libéré au niveau du WLC, de

sorte que la liste de contrôle d'accès n'a pas besoin d'être poussée vers le point d'accès. Cependant, lorsque le trafic est commuté localement (connexion flexible - commutation locale), la liste de contrôle d'accès (définie sur le contrôleur) doit être poussée vers le point d'accès, puisque le trafic est libéré au niveau du point d'accès. Cette opération est effectuée lorsque vous ajoutez la liste de contrôle d'accès au profil flexible.

WLAN à commutation centrale

Pour appliquer une liste de contrôle d'accès aux clients connectés à un réseau local sans fil commuté de manière centralisée :

Étape 1 : appliquez la liste de contrôle d'accès au profil de stratégie. Accédez à Configuration > Tags & Profiles > Policy, sélectionnez le profil de stratégie associé au WLAN commuté de manière centrale. Dans la section "Access Policies" > "WLAN ACL", sélectionnez l'ACL que vous voulez appliquer aux clients.

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 ACL

IPv4 ACL BLOCK-WLC ▼

IPv6 ACL Search or Select ▼

Si vous configurez l'authentification Web centrale sur un WLAN à commutation centrale, vous pouvez créer une liste de contrôle d'accès de redirection sur le 9800, comme si l'AP était en mode local, puisque tout est géré de manière centrale sur le WLC dans ce cas.

WLAN commuté localement

Pour appliquer une liste de contrôle d'accès aux clients connectés à un réseau local sans fil commuté :

Étape 1 : appliquez la liste de contrôle d'accès au profil de stratégie. Accédez à Configuration > Tags & Profiles > Policy, sélectionnez le profil de stratégie associé au WLAN commuté de manière centrale. Dans la section "Access Policies" > "WLAN ACL", sélectionnez l'ACL que vous voulez appliquer aux clients.

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 ACL

IPv4 ACL BLOCK-WLC ▼

IPv6 ACL Search or Select ▼

Étape 2 : appliquez la liste de contrôle d'accès au profil flexible. Accédez à Configuration > Tags & Profiles > Flex, sélectionnez le profil flex attribué aux AP de connexion flex. Dans la section "Policy ACL", ajoutez l'ACL et cliquez sur "Save"

Edit Flex Profile

General Local Authentication **Policy ACL** VLAN DNS Layer Security

+ Add × Delete

ACL Name	Central Web Auth	URL Filter
<input type="checkbox"/> ACL_WEBAUTH_REDIRECT	Enabled	

1 10 items per page 1 - 1 of 1 items

ACL Name* BLOCK-WLC ▼

Central Web Auth

URL Filter Search or Select ▼

✓ Save Cancel

Vérifier si la liste de contrôle d'accès est appliquée

Vous pouvez vérifier si la liste de contrôle d'accès est appliquée à un client lorsque vous allez à Surveillance > Sans fil > Clients, sélectionnez le client que vous voulez vérifier. Dans la section General > Security Information, cochez dans la section «Server Policies» le nom du «Filter-ID» : il doit correspondre à la liste de contrôle d'accès appliquée.

Client	
360 View	General QOS Statistics ATF Statistics Mobility History Call Statistics
Client Properties	AP Properties Security Information Client Statistics QOS Properties EoGRE
SM State	TERMINATE
Local Policies	
Service Template	wlan_svc_local-switched-policy-profile (priority 254)
VLAN	VLAN1416
Absolute Timer	1800
Server Policies	
Output SGT	0006-00
Filter-ID	BLOCK-WLC
Resultant Policies	
Output SGT	0006-00
Filter-ID	BLOCK-WLC
VLAN Name	VLAN1416

Dans le cas des AP Flex Connect (commutation locale), vous pouvez vérifier si l'ACL est envoyée à l'AP en tapant la commande "#show ip access-lists" sur l'AP lui-même.

Vérification

Vous pouvez utiliser ces commandes pour vérifier la configuration.

Configuration des VLAN/interfaces

```
# show vlan brief
# show interfaces trunk
# show run interface <interface-id>
```

Configuration d'un réseau local sans fil (WLAN)

```
# show wlan summary
# show run wlan [wlan-name]
# show wlan { id <wlan-id> | name <wlan-name> | all }
```

Configuration de point d'accès

```
# show ap summary
# show ap tag summary
# show ap name <ap-name> tag { info | detail }
```

```
# show ap name <ap-name> tag detail
```

```
AP Name      : AP2802-01
AP Mac       : 0896.ad9d.143e
```

```
Tag Type      Tag Name
-----
Policy Tag    PT1
RF Tag        default-rf-tag
Site Tag      default-site-tag
```

```
Policy tag mapping
```

```
-----
WLAN Profile Name      Policy Name      VLAN      Cent
-----
psk-pbl-ewlc          ctrl-vl2602      VLAN0210      ENAB
```

```
Site tag mapping
```

```
-----
Flex Profile      : default-flex-profile
AP Profile        : default-ap-profile
Local-site        : Yes
```

```
RF tag mapping
```

```
-----
5ghz RF Policy    : Global Config
2.4ghz RF Policy  : Global Config
```

Configuration des balises

```
# show wireless tag { policy | rf | site } summary
# show wireless tag { policy | rf | site } detailed <tag-name>
```

Configuration du profil

```
# show wireless profile { flex | policy } summary
# show wireless profile { flex | policy } detailed <profile-name>
# show ap profile <AP-join-profile-name> detailed
```


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.