

# Configuration de la fonction WLAN Anchor Mobility sur Catalyst 9800

## Table des matières

---

### [Introduction](#)

### [Conditions préalables](#)

#### [Exigences](#)

#### [Composants utilisés](#)

### [Configurer](#)

#### [Scénario étranger/d'ancrage entre 9800 WLC](#)

##### [Schéma du réseau : deux WLC Catalyst 9800](#)

##### [Configuration d'un 9800 étranger avec un ancrage 9800](#)

#### [WLC 9800 étranger - Ancre AireOS](#)

##### [Catalyst 9800 étranger - Schéma de réseau d'ancrage AireOS](#)

##### [Configuration du 9800 Foreign avec l'ancrage AireOS](#)

#### [AireOS étranger - WLC Anchor 9800](#)

##### [Diagramme du réseau d'ancrage AireOS Foreign avec 9800](#)

##### [Configuration d'un périphérique étranger 9800 avec une ancre AireOS](#)

### [Vérification](#)

#### [Vérification sur le WLC 9800](#)

#### [Vérification sur le WLC AireOS](#)

### [Dépannage](#)

#### [Débogage conditionnel et traçage Radio Active](#)

#### [Vérification du WLC AireOS](#)

---

## Introduction

Ce document décrit comment configurer un réseau local sans fil (WLAN) sur un scénario étranger/ancre avec des contrôleurs sans fil Catalyst 9800.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès aux contrôleurs sans fil via l'interface de ligne de commande ou l'interface utilisateur graphique
- Mobilité sur les contrôleurs LAN sans fil (WLC) Cisco
- Contrôleurs sans fil 9800
- WLC AireOS

## Composants utilisés

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

- AireOS WLC version 8.8 MR2 (vous pouvez également utiliser des images spéciales 8.5 d'Inter Release Controller Mobility (IRCM))
- 9800 WLC v16.10 ou ultérieure
- Modèle de configuration WLC 9800

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.

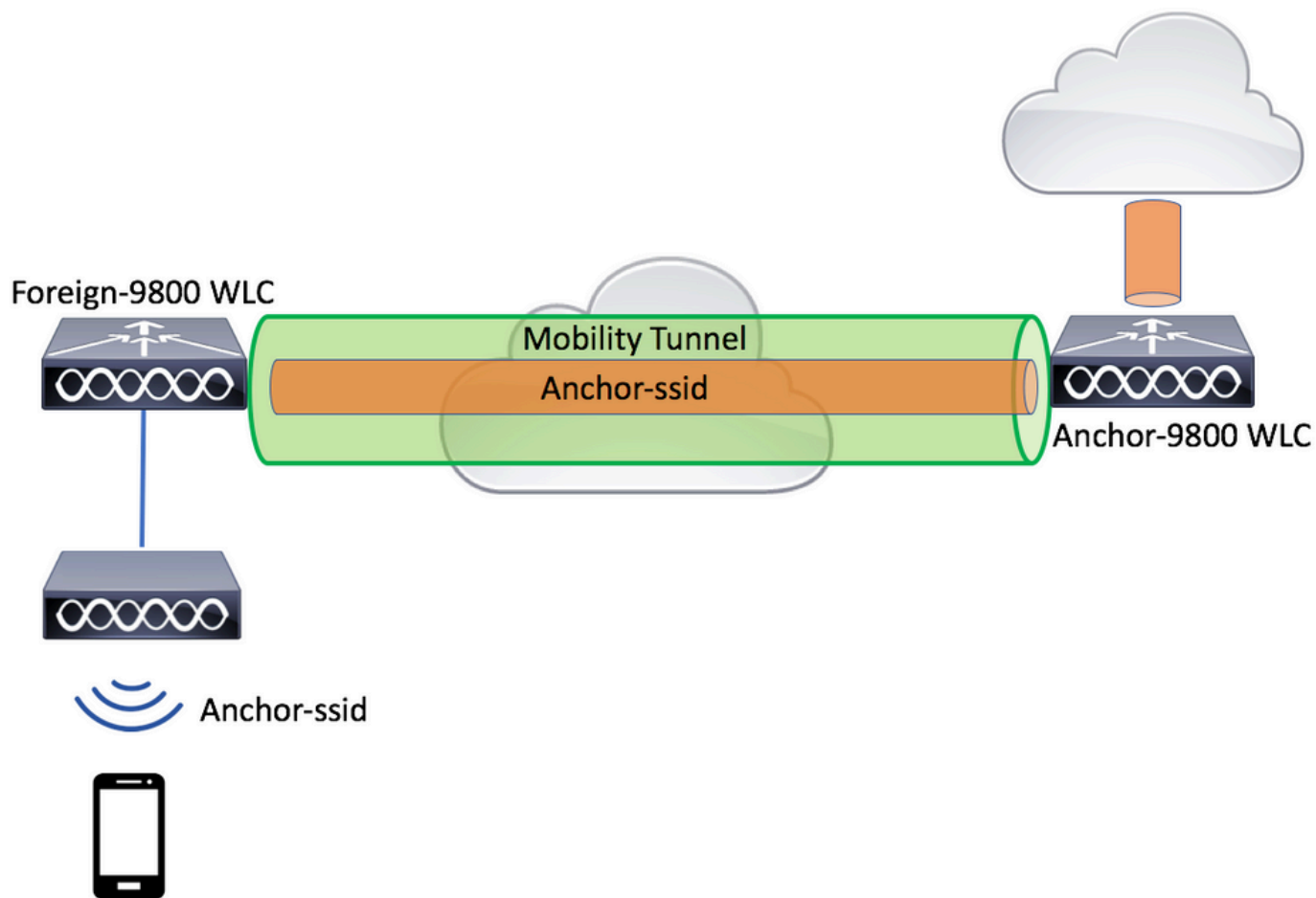
## Configurer

Il s'agit d'une fonctionnalité normalement utilisée pour les scénarios d'accès invité, pour terminer tout le trafic des clients dans un point de sortie C3 unique, même si les clients proviennent de contrôleurs et d'emplacements physiques différents. Le tunnel de mobilité fournit un mécanisme permettant de maintenir le trafic isolé lorsqu'il traverse le réseau.

### Scénario étranger/d'ancrage entre 9800 WLC

Ce scénario décrit les deux Catalyst 9800 utilisés.

Schéma du réseau : deux WLC Catalyst 9800




Pour les scénarios d'invité de mobilité, il existe deux rôles principaux de contrôleur :

- Contrôleur étranger : ce WLC possède la couche 2 ou le côté sans fil. Des points d'accès y sont connectés. Tout le trafic client pour les WLAN ancrés est encapsulé dans le tunnel de mobilité pour être envoyé à l'ancre. Il n'existe pas localement.
- Contrôleur d'ancrage : il s'agit du point de sortie de couche 3. Il reçoit les tunnels de mobilité des contrôleurs étrangers et décapsule ou termine le trafic client dans le point de sortie (VLAN). Il s'agit du point où les clients sont visibles sur le réseau, et donc du nom de l'ancre.

Les points d'accès sur le WLC étranger diffusent les SSID WLAN et ont une balise de stratégie attribuée qui lie le profil WLAN au profil de stratégie approprié. Lorsqu'un client sans fil se connecte à ce SSID, le contrôleur étranger envoie à la fois le nom SSID et le profil de stratégie dans le cadre des informations du client au WLC d'ancrage. À réception, le WLC d'ancrage vérifie sa propre configuration pour correspondre au nom SSID ainsi qu'au nom du profil de stratégie. Une fois que le WLC d'ancrage trouve une correspondance, il applique la configuration qui lui correspond et un point de sortie au client sans fil. Par conséquent, il est obligatoire que les noms et configurations du WLAN et du profil de stratégie correspondent sur le WLC 9800 étranger et le WLC d'ancrage 9800, à l'exception du VLAN sous le profil de stratégie.

---

 Remarque : les noms de profil WLAN et de profil de stratégie peuvent correspondre sur les WLC étrangers 9800 Anchor et 9800.

---

Configuration d'un 9800 étranger avec un ancrage 9800

Étape 1. Construisez un tunnel de mobilité entre le WLC étranger 9800 et le WLC Anchor 9800.


Vous pouvez vous référer à ce document : [Configuration des topologies de mobilité sur Catalyst 9800](#)

Étape 2. Créez le SSID souhaité sur les deux WLC 9800.

Méthodes de sécurité prises en charge :

- Open (ouvert)
- filtre MAC
- PSK
- Point1x
- Authentification Web locale/externe (LWA)
- Authentification Web centralisée (CWA)

---

 Remarque : les deux WLC 9800 doivent avoir le même type de configuration, sinon l'ancrage ne fonctionne pas.

---

Étape 3. Connectez-vous au WLC 9800 étranger et définissez l'adresse IP du WLC 9800 d'ancrage sous le profil de stratégie.

Accédez à Configuration > Tags & Profiles > Policy > + Add.

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

Dans l'Mobility onglet, choisissez l'adresse IP du WLC d'ancrage 9800.

### Add Policy Profile

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

**Mobility Anchors**

Export Anchor

Static IP Mobility  DISABLED

*Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.*

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (1)	Selected (1)
Anchor IP 172.16.0.5 →	Anchor IP    Anchor Priority 10.88.173.49    Tertiary ... ←

Cancel    Save & Apply to Device

Étape 4. Liez le profil de stratégie au WLAN à l'intérieur de la balise de stratégie attribuée aux points d'accès associés au contrôleur étranger qui dessert ce WLAN.

Accédez à Configuration > Tags & Profiles > Tags et créez-en un nouveau ou utilisez celui qui existe déjà.

### Edit Policy Tag

Name\*    PT1

Description    Enter Description

**+ Add**    x Delete

WLAN Profile    Policy Profile

0    10 items per page    No items to display

**Map WLAN and Policy**

WLAN Profile\*    anchor-ssid    Policy Profile\*    anchor-policy

x    ✓

Assurez-vous Update & Apply to Device d'appliquer les modifications à la balise de stratégie.

### Edit Policy Tag ✕

Name\*

Description

	WLAN Profile	Policy Profile
<input type="checkbox"/>	anchor-ssid	anchor-policy

◀ ◁ 1 ▷ ▶ ▶▶  items per page 1 - 1 of 1 items

Étape 5 (facultative). Attribuez la balise de stratégie à un point d'accès ou vérifiez qu'elle existe déjà.

Accédez à Configuration > Wireless > Access Points > AP name > General.

✕
Edit AP

---

General
Interfaces
High Availability
Inventory
Advanced

AP Name*	<input type="text" value="karlcisn-AP-30"/>	Primary Software Version	8.5.97.110
Location*	<input type="text" value="default-location"/>	Predownloaded Status	N/A
Base Radio MAC	000a.ad00.1f00	Predownloaded Version	N/A
Ethernet MAC	000a.ad00.1ff0	Next Retry Time	N/A
Admin Status	<input style="width: 100%;" type="text" value="Enabled"/>	Boot Version	8.5.97.110
AP Mode	<input style="width: 100%;" type="text" value="Local"/>	IOS Version	
Operation Status	Registered	Mini IOS Version	0.51.0.3
Fabric Status	Disabled		

**Tags**

Policy	<input style="width: 100%;" type="text" value="PT1"/>
Site	<input style="width: 100%;" type="text" value="ST1"/>
RF	<input style="width: 100%;" type="text" value="RT1"/>

**IP Config**

CAPWAP Preferred Mode	Not Configured
Static IPv4 Address	11.11.0.39
Static IP (IPv4/IPv6)	<input checked="" type="checkbox"/>
Static IP (IPv4/IPv6)	<input type="text" value="11.11.0.39"/>
Netmask	<input type="text" value="255.255.0.0"/>
Gateway (IPv4/IPv6)	<input type="text" value="11.11.0.1"/>
DNS IP Address (IPv4/IPv6)	<input type="text" value="0.0.0.0"/>
Domain Name	<input type="text" value="Cisco"/>

**Time Statistics**

Up Time	3 days 0 hrs 34 mins 26 secs
---------	------------------------------

↶ Cancel

📄 Update & Apply to Device

**Remarque** : Sachez que si vous effectuez une modification dans la balise AP après avoir choisi Update & Apply to Device, l'AP redémarre son tunnel CAPWAP, donc il perd l'association avec le WLC 9800 et le récupère.

À partir de la CLI :

Foreign 9800 WLC



```
# config t # wireless profile policy anchor-policy # mobility anchor 10.88.173.105 priority 3 # no shutdown # exit # wireless tag policy PT1 # wlan anchor-
```

Étape 6. Connectez-vous au WLC d'ancrage 9800 et créez le profil de stratégie d'ancrage. Assurez-vous qu'il porte exactement le même nom que celui que vous avez utilisé sur les WLC 9800 étrangers.

Accédez à Configuration > Tags & Profiles > Policy > + Add.

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

Accédez à l'Mobility onglet et activez Export Anchor. Ceci indique au WLC 9800 qu'il est le WLC 9800 d'ancrage pour tout WLAN qui utilise ce profil de stratégie. Lorsque le WLC 9800 étranger envoie les clients au WLC 9800 d'ancrage, il informe sur le WLAN et le profil de stratégie auxquels le client est affecté, de sorte que le WLC 9800 d'ancrage sait quel profil de stratégie local utiliser.

**Remarque** : vous ne devez pas configurer des homologues de mobilité et exporter l'ancre en même temps. Ce scénario de configuration n'est pas valide.

**Remarque** : vous ne devez pas utiliser le paramètre d'ancrage d'exportation pour un profil de stratégie lié à un profil WLAN sur un contrôleur avec des points d'accès. Cela empêche la diffusion du SSID, cette stratégie doit donc être utilisée exclusivement pour la fonctionnalité d'ancrage.

**Add Policy Profile** ✕

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

---

**Mobility Anchors**

**Export Anchor**

Static IP Mobility  DISABLED

*Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.*

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (2)	Selected (0)	
Anchor IP	Anchor IP	Anchor Priority
<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">  172.16.0.5 <span style="float: right;">→</span> </div> <div style="border: 1px solid #ccc; padding: 2px;">  10.88.173.49 <span style="float: right;">→</span> </div>	Anchors not assigned	

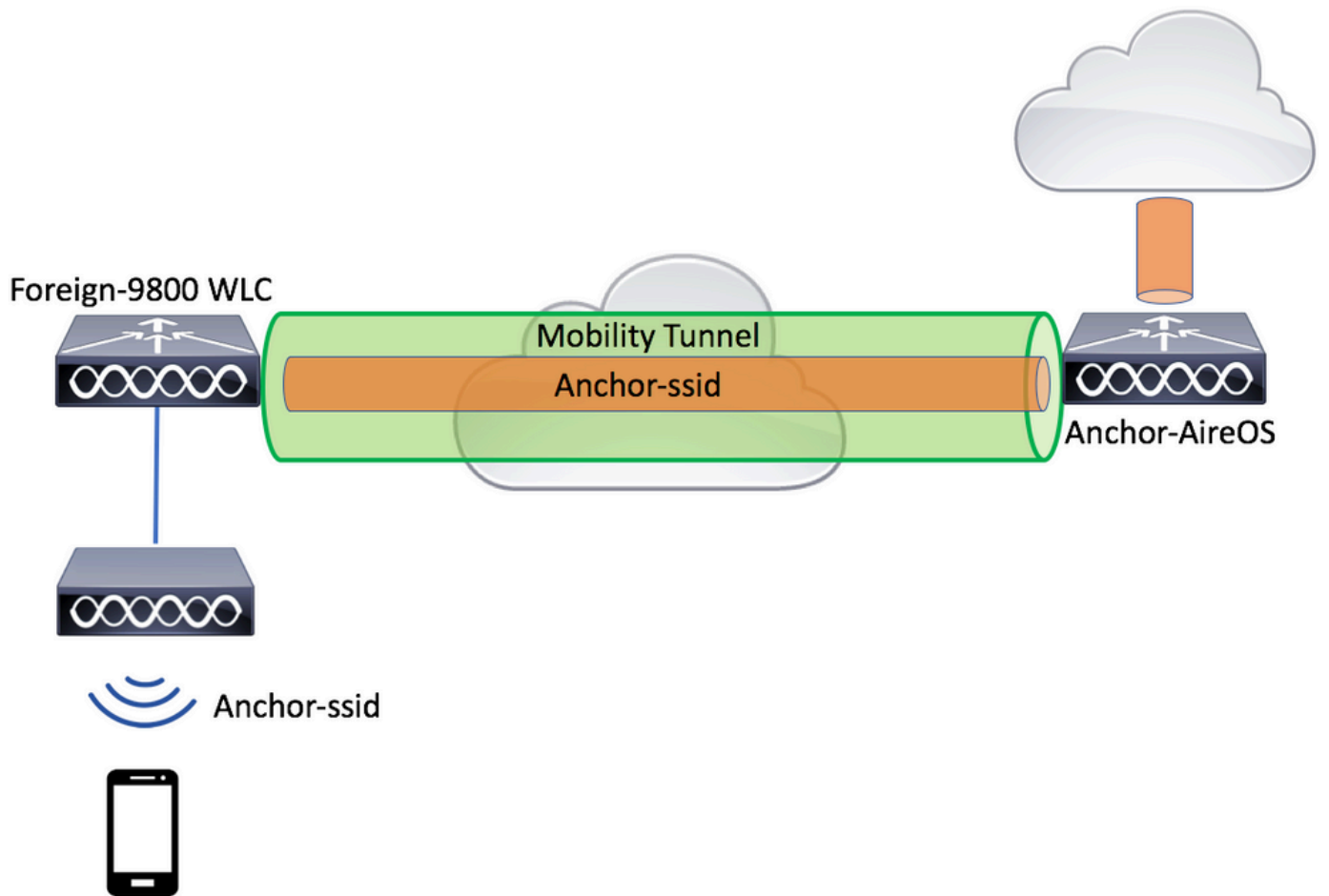
À partir de la CLI :

```
Anchor 9800 WLC # config t # wireless profile policy <anchor-policy> # mobility anchor # vlan <VLAN-id_VLAN-name> # no shutdown # exit
```

WLC 9800 étranger - Ancre AireOS

Cette configuration décrit le scénario où un WLC Catalyst 9800 est utilisé comme étranger avec un WLC unifié AireOS utilisé comme ancre.

Catalyst 9800 étranger - Schéma de réseau d'ancrage AireOS



Configuration du 9800 Foreign avec l'ancrage AireOS


Étape 1. Créez un tunnel de mobilité entre le WLC 9800 étranger et le WLC Anchor AireOS.

Reportez-vous à ce document : [Configuration des topologies de mobilité sur Catalyst 9800](#)

Étape 2. Créez les WLAN souhaités sur les deux WLC.

Méthodes de sécurité prises en charge :

- Open (ouvert)
- filtre MAC
- PSK
- Point1x
- Authentification Web locale/externe (LWA)
- Authentification Web centralisée (CWA)


 **Remarque** : le WLC AireOS et le WLC 9800 doivent avoir le même type de configuration, sinon l'ancre ne fonctionne pas.

Étape 3. Connectez-vous au WLC 9800 (qui agit en tant qu'étranger) et créez le profil de stratégie d'ancrage.

Accédez à Configuration > Tags & Profiles > Policy > + Add .

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

Accédez à l'Mobility onglet et choisissez l'ancre AireOS WLC. Le WLC 9800 transfère le trafic du SSID associé à ce profil de stratégie à l'ancre choisie.

### Add Policy Profile

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


**Mobility Anchors**

Export Anchor

Static IP Mobility  DISABLED

*Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.*

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (0)	Selected (1)
Anchor IP	Anchor IP      Anchor Priority
No anchors available	<div style="border: 2px solid red; padding: 2px;">  10.88.173.105      Tertiary ... <span style="float: right;">←</span> </div>

Étape 4. Liez le profil de stratégie au WLAN à l'intérieur de la balise de stratégie attribuée aux points d'accès associés au contrôleur étranger qui dessert ce WLAN.

Accédez à Configuration > Tags & Profiles > Tags et créez-en un nouveau ou utilisez celui qui existe déjà.

### Edit Policy Tag

Name\*

Description

WLAN Profile  Policy Profile

10 items per page    No items to display

**Map WLAN and Policy**

WLAN Profile\*  Policy Profile\*

Assurez-vous Update & Apply to Device d'appliquer les modifications à la balise de stratégie.

### Edit Policy Tag ✕

Name\*

Description

	WLAN Profile	Policy Profile
<input type="checkbox"/>	anchor-ssid	anchor-policy

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

Étape 5 (facultative). Attribuez le site à un point d'accès ou vérifiez qu'il l'a déjà.

Accédez à Configuration > Wireless > Access Points > AP name > General.

## Edit AP ✕

General Interfaces High Availability Inventory Advanced

AP Name*	<input type="text" value="karlcisn-AP-30"/>	Primary Software Version	8.5.97.110
Location*	<input type="text" value="default-location"/>	Predownloaded Status	N/A
Base Radio MAC	000a.ad00.1f00	Predownloaded Version	N/A
Ethernet MAC	000a.ad00.1ff0	Next Retry Time	N/A
Admin Status	<input type="text" value="Enabled"/>	Boot Version	8.5.97.110
AP Mode	<input type="text" value="Local"/>	IOS Version	
Operation Status	Registered	Mini IOS Version	0.51.0.3
Fabric Status	Disabled		

**Tags**

Policy

Site

RF

**IP Config**

CAPWAP Preferred Mode Not Configured

Static IPv4 Address 11.11.0.39

Static IP (IPv4/IPv6)

Static IP (IPv4/IPv6)

Netmask

Gateway (IPv4/IPv6)

DNS IP Address (IPv4/IPv6)

Domain Name

**Time Statistics**

Up Time 3 days 0 hrs 34 mins 26 secs

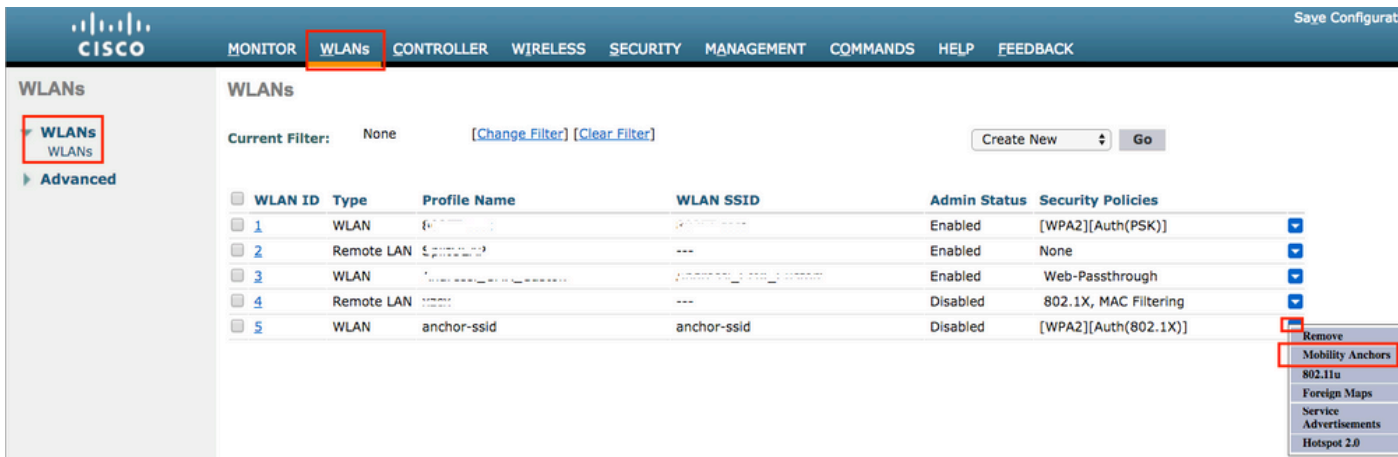
**Remarque** : sachez que si vous effectuez une modification dans la balise AP après avoir choisi, l'AP redémarre son tunnel CAPWAP, donc il perd l'association avec le WLC 9800 et le récupère Update & Apply to Device.

À partir de la CLI :

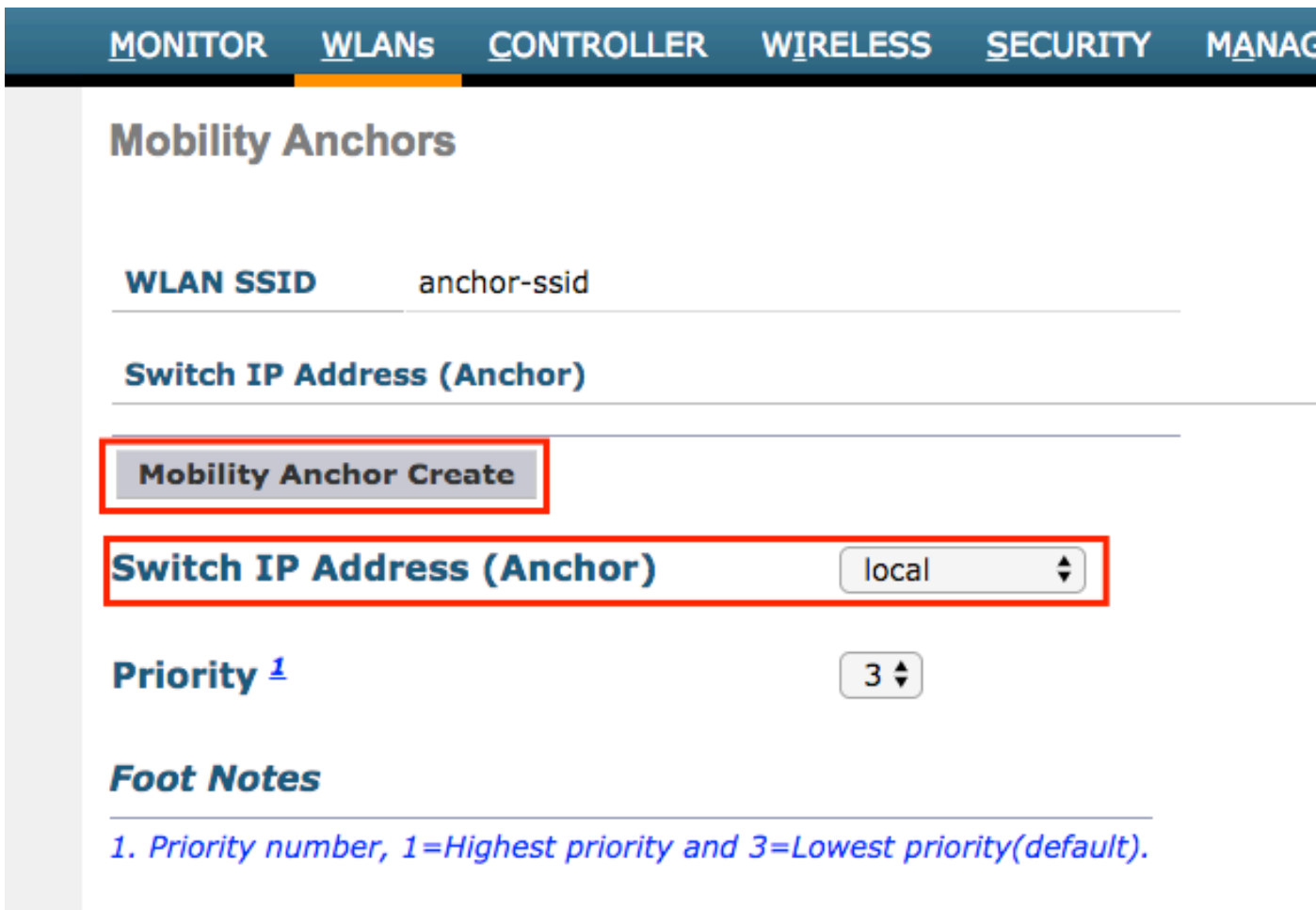
```
# config t # wireless profile policy anchor-policy # mobility anchor 10.88.173.105 priority 3 # no shutdown # exit # wireless tag policy PT1 # wlan anchor-
```

Étape 6. Configurez le WLC AireOS comme point d'ancrage.

Connectez-vous à AireOS et accédez à WLANs > WLANs. Choisissez la flèche à l'extrémité droite de la ligne WLAN afin de naviguer vers le menu déroulant et choisissez Mobility Anchors.



Définissez-le comme ancre locale.



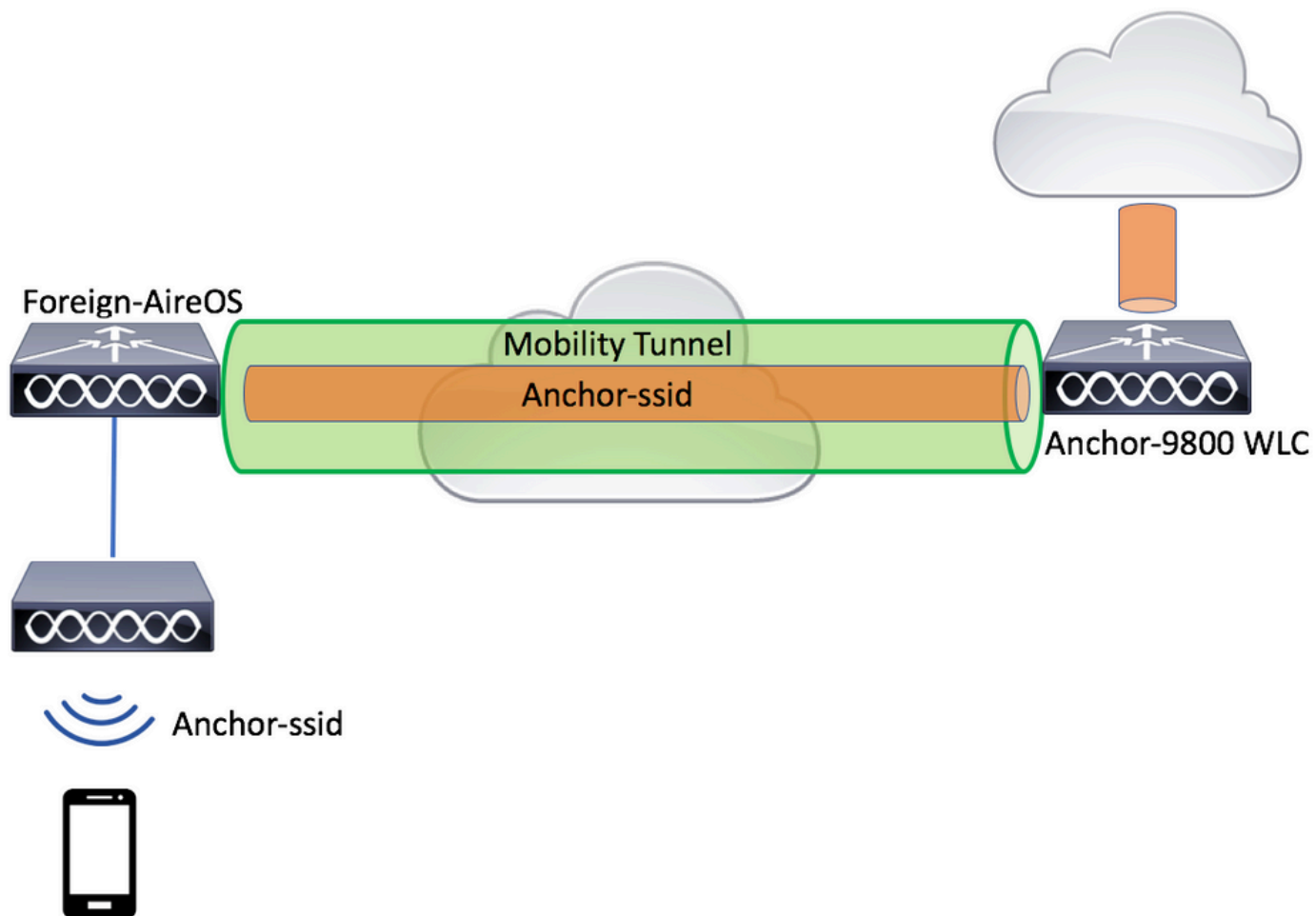
À partir de la CLI :



```
> config wlan disable <wlan-id> > config wlan mobility anchor add <wlan-id> <AireOS-WLC's-mgmt-interface> > config wlan enable <wlan-id>
```

AireOS étranger - WLC Anchor 9800

Diagramme du réseau d'ancrage AireOS Foreign avec 9800



Configuration d'un périphérique étranger 9800 avec une ancre AireOS

Étape 1. Créez un tunnel de mobilité entre le WLC 9800 étranger et le WLC Anchor AireOS.


Vous pouvez vous référer à ce document : [Configuration des topologies de mobilité sur Catalyst 9800](#)

Étape 2. Créez le SSID souhaité sur les deux WLC.

Méthodes de sécurité prises en charge :

- Open (ouvert)
- filtre MAC
- PSK

- Point1x
- Authentification Web locale/externe (LWA)
- Authentification Web centralisée (CWA)

 **Remarque :** le WLC AireOS et le WLC 9800 doivent avoir le même type de configuration, sinon l'ancre ne fonctionne pas.

Étape 3. Connectez-vous au WLC 9800 (qui agit comme une ancre) et créez le profil de stratégie d'ancre.

Accédez à Configuration > Tags & Profiles > Policy > + Add. Assurez-vous que le nom du profil de stratégie sur 9800 est exactement le même que le nom du profil sur le WLC AireOS, sinon, il ne fonctionne pas.

**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.

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

↶ Cancel

💾 Save & Apply to Device

Accédez à l'Mobility onglet et activez Export Anchor. Ceci indique au WLC 9800 qu'il est le WLC 9800 d'ancrage pour tout WLAN qui utilise ce profil de stratégie. Lorsque le WLC AireOS étranger envoie les clients au WLC d'ancrage 9800, il informe sur le nom WLAN auquel le client est affecté, de sorte que le WLC d'ancrage 9800 sait quelle configuration WLAN locale utiliser et il utilise également ce nom pour savoir quel profil de stratégie locale utiliser.

✕
Add Policy Profile

---

General
Access Policies
QOS and AVC
Mobility
Advanced

**Mobility Anchors**

Export Anchor

Static IP Mobility  DISABLED

*Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.*

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (2)	Selected (0)										
<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 80%;">Anchor IP</th> <th style="width: 20%;"></th> </tr> </thead> <tbody> <tr> <td> 172.16.0.5</td> <td style="text-align: right;">→</td> </tr> <tr> <td> 10.88.173.49</td> <td style="text-align: right;">→</td> </tr> </tbody> </table>	Anchor IP		172.16.0.5	→	10.88.173.49	→	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">Anchor IP</th> <th style="width: 50%;">Anchor Priority</th> </tr> </thead> <tbody> <tr> <td colspan="2" style="text-align: center; padding: 20px;">Anchors not assigned</td> </tr> </tbody> </table>	Anchor IP	Anchor Priority	Anchors not assigned	
Anchor IP											
172.16.0.5	→										
10.88.173.49	→										
Anchor IP	Anchor Priority										
Anchors not assigned											

↶ Cancel

Save & Apply to Device

**Remarque** : assurez-vous d'utiliser ce profil de stratégie exclusivement pour recevoir le trafic des contrôleurs étrangers.

À partir de la CLI :

```
Anchor 9800 WLC # config t # wireless profile policy <anchor-policy> # mobility anchor # vlan <VLAN-id_VLAN-name> # no shutdown # exit
```

Étape 4. Configurez le WLC AireOS comme étant étranger.

Connectez-vous à AireOS et accédez à WLANs > WLANs. Accédez à la flèche ci-dessous à la fin de la ligne WLAN et sélectionnez Mobility Anchors .

CISCO MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Saye Configurati

WLANs

WLANs  
WLANs  
Advanced

WLANs

Current Filter: None [Change Filter] [Clear Filter] Create New Go

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN			Enabled	[WPA2][Auth(PSK)]
2	Remote LAN		---	Enabled	None
3	WLAN			Enabled	Web-Passthrough
4	Remote LAN		---	Disabled	802.1X, MAC Filtering
5	WLAN	anchor-ssid	anchor-ssid	Disabled	[WPA2][Auth(802.1X)]

Remove  
Mobility Anchors  
802.11u  
Foreign Maps  
Service Advertisements  
Hotspot 2.0

Définissez le WLC 9800 comme point d'ancrage pour ce SSID.

MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT

## Mobility Anchors

**WLAN SSID** anchor-ssid

**Switch IP Address (Anchor)**

**Mobility Anchor Create**

**Switch IP Address (Anchor)** 10.88.173.105

**Priority** 1 3

**Foot Notes**

1. Priority number, 1=Highest priority and 3=Lowest priority(default).

À partir de la CLI :

```
> config wlan disable <wlan-id> > config wlan mobility anchor add <wlan-id> <9800 WLC's-mgmt-interface> > config wlan enable <wlan-id>
```

## Vérification

Vous pouvez utiliser ces commandes pour vérifier la configuration et l'état des clients sans fil à l'aide d'un SSID étranger/d'ancrage.

### Vérification sur le WLC 9800

```
# show run wlan # show wlan summary # show wireless client summary
# show wireless mobility summary
# show ap tag summary
# show ap <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>
```

### Vérification sur le WLC AireOS

```
> show client summary > show client detail <client-mac-addr> > show wlan summary > show wlan <wlan-id>
```

## Dépannage

Le contrôleur WLC 9800 offre des fonctionnalités de traçage TOUJOURS ACTIVES. Cela garantit que toutes les erreurs, avertissements et messages de niveau de notification liés à la connectivité du client sont constamment consignés et que vous pouvez afficher les événements d'un incident ou d'une condition d'échec après qu'il se soit produit.



**Remarque** : selon le volume de journaux générés, vous pouvez revenir 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 vous référer à ces étapes. (Veillez à consigner la session dans un fichier texte)

Étape 1. Vérifiez l'heure actuelle du contrôleur de sorte que vous puissiez suivre les journaux dans le temps de retour à quand le problème s'est produit.

```
# show clock
```

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

```
# show logging
```

Étape 3. Collectez les traces de niveau de notification toujours actif pour l'adresse MAC ou IP spécifique. L'homologue de mobilité à distance peut filtrer ce paramètre, si vous suspectez un problème de tunnel de mobilité, ou par adresse MAC de client sans fil.

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

Étape 4. Vous pouvez soit afficher le contenu de la session, soit copier le fichier sur un serveur TFTP externe.

```
# 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 traçage Radio Active

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 les traces Radio Active (RA), qui fournit des traces de niveau débogage pour tous les processus qui interagissent avec la condition spécifiée (adresse MAC du client dans ce cas). Afin d'activer le débogage conditionnel, référez-vous à ces étapes.

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

```
# clear platform condition all
```

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

Ces commandes commencent 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.

```
# 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.

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

Une fois le temps de surveillance écoulé ou le débogage sans fil arrêté, le WLC 9800 génère un fichier local avec le nom : ra\_trace\_MAC\_aaaabbbbcccc\_HHMMSS.XXX\_timezone\_DayWeek\_Month\_Day\_year.log

Étape 9. Recueillir le fichier de l'activité de l'adresse MAC. Vous pouvez copier le suivi RA .log sur un serveur externe ou afficher le résultat directement à l'écran.

Vérifiez le nom du fichier de suivi RA:

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

Copiez le fichier sur un serveur externe :

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.d/ra-FILENAME.txt
```


Affichez-en le contenu :

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

Étape 10. Si la cause première n'est toujours pas évidente, collectez les journaux internes qui sont une vue plus détaillée des journaux de niveau débogage. Vous n'avez pas besoin de déboguer à nouveau le client car les journaux ont déjà été écrits dans la mémoire du contrôleur et vous devez seulement remplir une vue plus détaillée d'eux.

```
# show logging profile wireless internal filter { mac | ip } { <aaa.bbb.ccc> | <a.b.c.d> } to-file ra-internal-<FILENAME>.txt
```

---

 **Remarque** : cette sortie de commande retourne des traces pour tous les niveaux de journalisation pour tous les processus et est assez volumineuse. Contactez le TAC Cisco pour vous aider à analyser ces traces.

---

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

Copiez le fichier sur un serveur externe :

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

Affichez-en le contenu :

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

Étape 11. Supprimez les conditions de débogage.



```
# clear platform condition all
```



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

---

Vérification du WLC AireOS

Vous pouvez exécuter cette commande pour surveiller l'activité d'un client sans fil sur un WLC AireOS.

```
> debug client <client-mac-add>
```

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.