

# Catalyst 9800でのWLANアンカーモビリティ機能の設定

## 内容

---

### [はじめに](#)

### [前提条件](#)

#### [要件](#)

#### [使用するコンポーネント](#)

### [設定](#)

#### [9800 WLC間の外部/アンカーシナリオ](#)

##### [ネットワークダイアグラム：2台のCatalyst 9800 WLC](#)

##### [9800アンカーを使用した9800 Foreignの設定](#)

#### [外部9800 WLC：アンカーAireOS](#)

##### [Catalyst 9800 Foreign - AireOSアンカーネットワーク図](#)

##### [AireOSアンカーを使用した9800 Foreignの設定](#)

#### [外部AireOS：アンカー9800 WLC](#)

##### [AireOS Foreignと9800アンカーネットワーク図](#)

##### [AireOSアンカーを使用した9800 Foreignの設定](#)

### [検証](#)

#### [9800 WLCでの確認](#)

#### [AireOS WLCでの確認](#)

### [トラブルシューティング](#)

#### [条件付きデバッグとラジオアクティブトレース](#)

#### [AireOS WLCの確認](#)

---

## はじめに

このドキュメントでは、Catalyst 9800ワイヤレスコントローラを使用した外部/アンカーシナリオでワイヤレスローカルエリアネットワーク(WLAN)を設定する方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- ワイヤレスコントローラへのコマンドラインインターフェイス(CLI)またはグラフィックユーザーインターフェイス(GUI)アクセス
- Cisco Wireless LAN Controller(WLC)でのモビリティ
- 9800ワイヤレスコントローラ
- AireOS WLC

## 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- AireOS WLCバージョン8.8 MR2(Inter Release Controller Mobility(IRCM)の特別な8.5イメージも使用可能)
- 9800 WLC v16.10以降
- 9800 WLC設定モデル

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

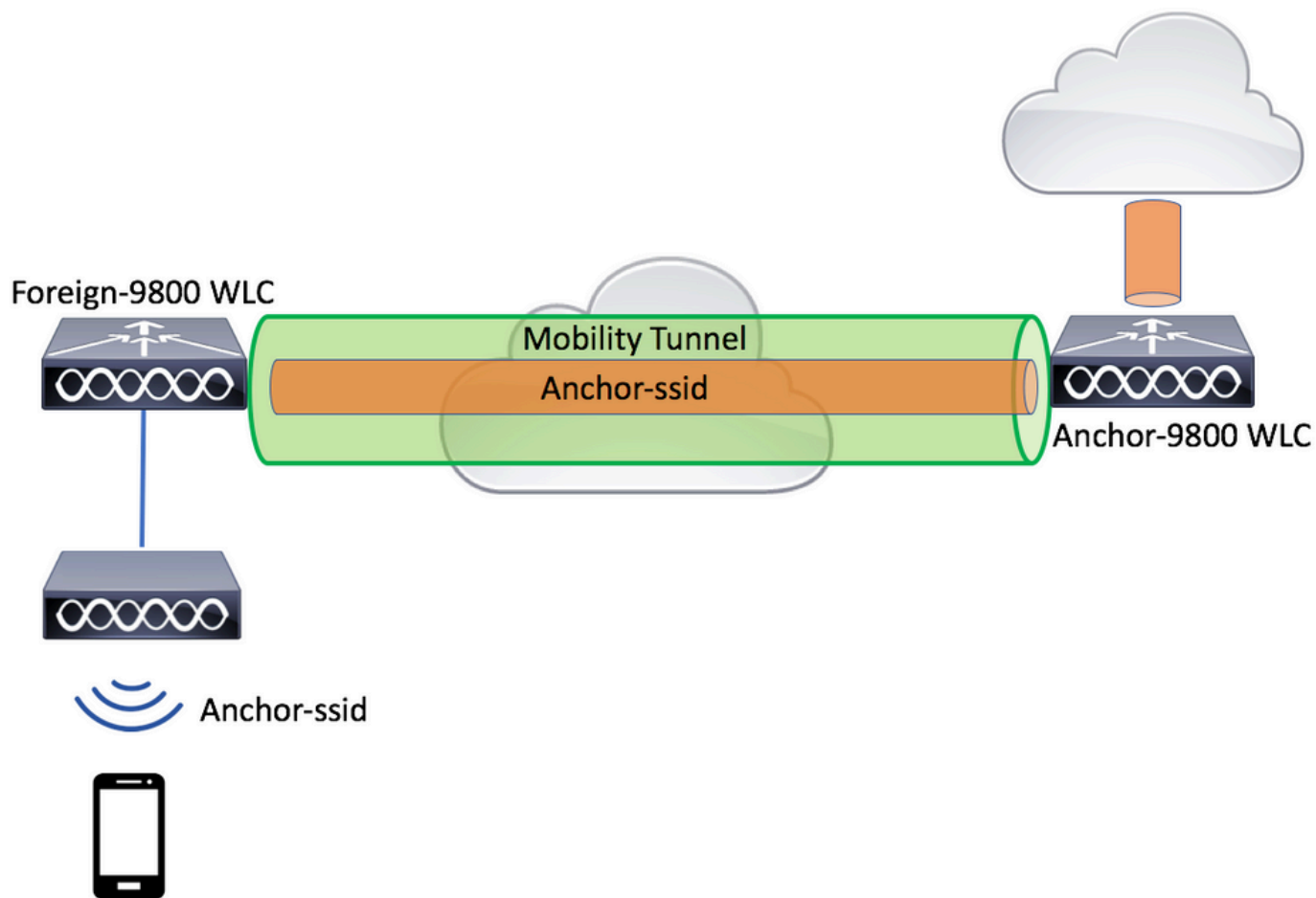
## 設定

これは通常、クライアントが異なるコントローラや物理的な場所から来ている場合でも、クライアントからのすべてのトラフィックを1つのL3出力点に終端するために、ゲストアクセスシナリオで使用される機能です。モビリティトンネルは、トラフィックがネットワークを通過する際にトラフィックを隔離するメカニズムを提供します。

### 9800 WLC間の外部/アンカーシナリオ

このシナリオでは、使用されている2台のCatalyst 9800を図示します。


ネットワークダイアグラム：2台のCatalyst 9800 WLC



モビリティゲストシナリオでは、次の2つの主要なコントローラロールがあります。

- 外部コントローラ：このWLCはレイヤ2またはワイヤレス側を所有します。アクセスポイントが接続されている。アンカーされたWLANのすべてのクライアントトラフィックは、モビリティトンネルにカプセル化され、アンカーに送信されます。これはローカルには終了しません。
- アンカーコントローラ：これはレイヤ3の出力点です。外部コントローラからモビリティトンネルを受信し、クライアントトラフィックをカプセル化解除するか、または終了して出口(VLAN)に入れます。これは、クライアントがネットワーク内で認識されるポイントです。つまり、アンカー名です。

外部WLC上のアクセスポイントはWLAN SSIDをブロードキャストし、WLANプロファイルと適切なポリシープロファイルをリンクするポリシータグが割り当てられています。ワイヤレスクライアントがこのSSIDに接続すると、外部コントローラはクライアント情報の一部としてSSID名とポリシープロファイルの両方をアンカーWLCに送信します。アンカーWLCは、SSID名とポリシープロファイル名に一致する自身の設定を受信時に確認します。アンカーWLCは、一致するエントリを見つけると、それに対応する設定と出力点をワイヤレスクライアントに適用します。したがって、WLANとポリシープロファイルの名前と設定は、ポリシープロファイルの下のVLANを除き、外部9800 WLCとアンカー9800 WLCの両方で一致する必要があります。

 注:WLANプロファイルとポリシープロファイルの名前は、9800アンカーWLCと9800外部WLCの両方で一致できます。

## 9800アンカーを使用した9800 Foreignの設定

ステップ 1： 外部9800 WLCとアンカー9800 WLCの間にモビリティトンネルを構築します。


このドキュメントの「[Catalyst 9800でのモビリティポロジの設定](#)」を参照してください。

ステップ 2： 両方の9800 WLCで目的のSSIDを作成します。

サポートされるセキュリティ方式：

- 開く
- MACフィルタ
- PSK
- Dot1x
- ローカル/外部Web認証(LWA)
- 中央Web認証(CWA)

---

 注：両方の9800 WLCに同じ種類の設定を行う必要があります。そうしないと、アンカーが機能しません。

---

ステップ 3： 外部9800 WLCにログインし、ポリシープロファイルでアンカー9800 WLCのIPアドレスを定義します。

に移動し Configuration > Tags & Profiles > Policy > + Add ます。

### 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"/>	

タブでMobility、アンカー9800 WLCのIPアドレスを選択します。

**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	Anchor IP      Anchor Priority
<div style="border: 1px solid #ccc; padding: 5px; display: flex; align-items: center;"> <span>172.16.0.5</span> <span style="margin-left: 20px;">→</span> </div>	<div style="border: 1px solid #ccc; padding: 5px; display: flex; align-items: center;"> <div style="border: 2px solid red; padding: 2px;"> <span>10.88.173.49</span> </div> <div style="margin-left: 20px;"> <input type="text" value="Tertiary ..."/> <span style="margin-left: 10px;">←</span> </div> </div>

ステップ 4 : このWLANにサービスを提供する外部コントローラに関連付けられたAPに割り当てられたポリシータグ内のWLANに、ポリシープロファイルをリンクします。

に移動して新しいConfiguration > Tags & Profiles > Tags ファイルを作成するか、既存のファイルを使用します。

**Edit Policy Tag** ✕

Name\*

Description

**+ Add**

WLAN Profile  Policy Profile

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

**Map WLAN and Policy**

WLAN Profile\*  Policy Profile\*

変更をポリシー Update & Apply to Device タグに適用することを選択していることを確認します。

**Edit Policy Tag** ✕

Name\*

Description

**+ Add**

WLAN Profile  Policy Profile

anchor-ssid anchor-policy

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

ステップ 5 ( オプション ) : ポリシータグをAPに割り当てるか、すでにAPにポリシータグがあることを確認します。

に移動し Configuration > Wireless > Access Points > AP name > General ます。

✕
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	<input type="text" value="PT1"/>		
Site	<input type="text" value="ST1"/>		
RF	<input 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

注:選択後にAPタグを変更するとUpdate & Apply to Device、APはトンネルCAPWAPを再起動するため、9800 WLCとの関連付けが失われ、回復します。

CLI から、

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-ssid policy anchor-policy
# exit

# ap aaaa.bbbb.dddd
# site-tag PT1
# exit

```

手順 6 : アンカー9800 WLCにログインし、アンカーポリシープロファイルを作成します。外部9800 WLCで使用したのと同じ名前であることを確認します。

に移動し Configuration > Tags & Profiles > Policy > + Add ます。

**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

Central Authentication


Central DHCP


Central Association

Flex NAT/PAT

タ MobilityExport Anchor ブに移動して有効にします。これにより、9800 WLCに対して、このポリシープロファイルを使用するすべてのWLANのアンカー9800 WLCであることが指示されます。外部9800 WLCがアンカー9800 WLCにクライアントを送信すると、クライアントが割り当てられてい

るWLANとポリシープロファイルについて通知するため、アンカー9800 WLCは使用するローカルポリシープロファイルを認識します。

 注：モビリティピアの設定とアンカーのエクスポートを同時に行うことはできません。これは無効な設定シナリオです。

 注：アクセスポイントがあるコントローラのWLANプロファイルに関連付けられているポリシープロファイルに対しては、エクスポートアンカー設定を使用しないでください。これにより、SSIDがブロードキャストされなくなります。そのため、このポリシーはアンカー機能専用にする必要があります。

### 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
 172.16.0.5 →	Anchors not assigned	
 10.88.173.49 →		

CLI から、

Anchor 9800 WLC

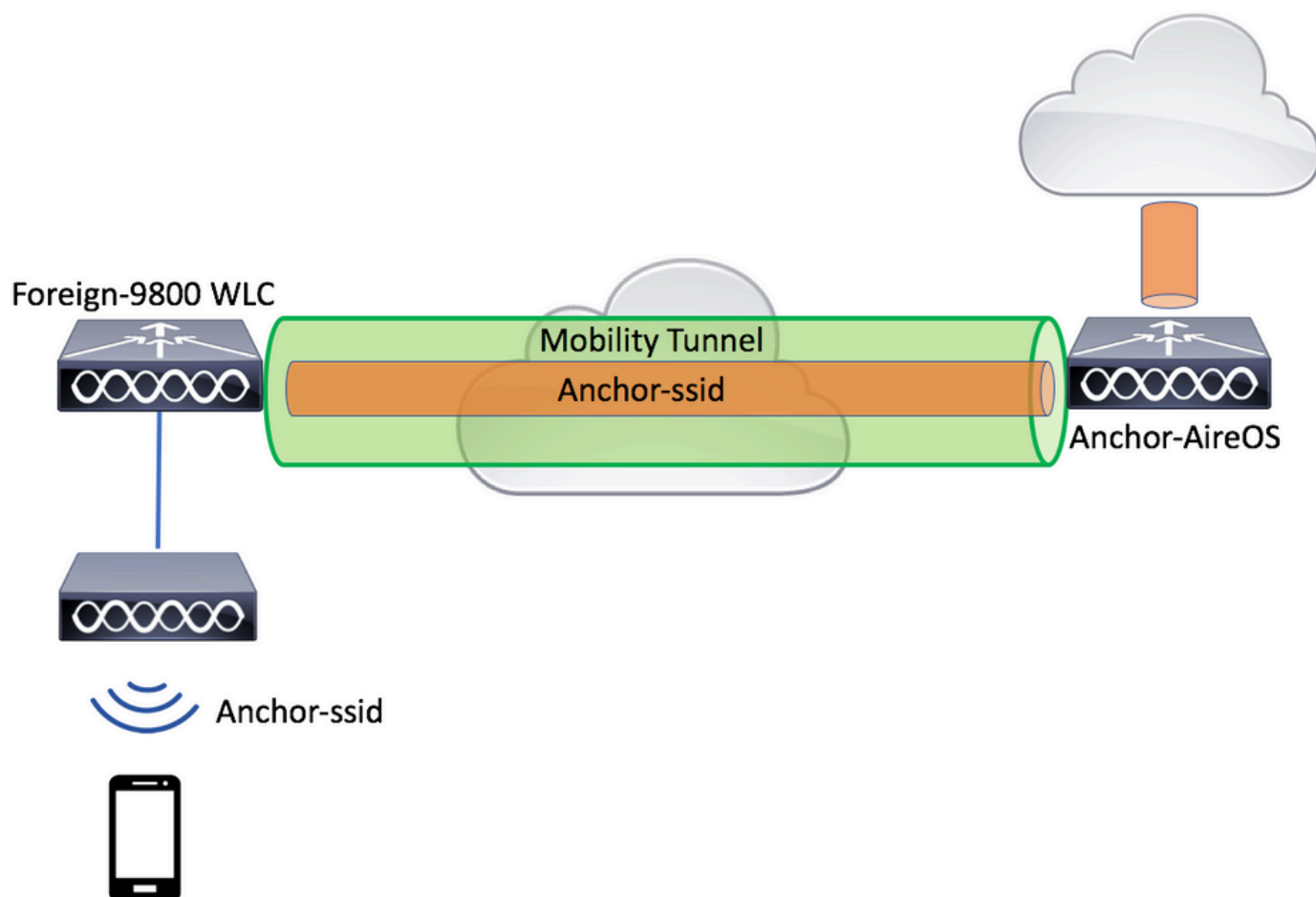
```
# config t
# wireless profile policy <anchor-policy>
# mobility anchor
# vlan <VLAN-id_VLAN-name>
# no shutdown
```

# exit

## 外部9800 WLC : アンカーAireOS

この設定は、Catalyst 9800 WLCを外部として使用し、AireOS Unified WLCをアンカーとして使用するシナリオを示しています。

Catalyst 9800 Foreign - AireOSアンカーネットワーク図



### AireOSアンカーを使用した9800 Foreignの設定

ステップ 1 : 外部9800 WLCとアンカーAireOS WLCの間にモビリティトンネルを構築します。


詳細については、[Catalyst 9800でのモビリティポロジの設定](#)

ステップ 2 : 両方のWLCで必要なWLANを作成します。

サポートされるセキュリティ方式 :

- 開く
- MACフィルタ
- PSK

- Dot1x
- ローカル/外部Web認証(LWA)
- 中央Web認証(CWA)

 注:AireOS WLCと9800 WLCの両方に同じ種類の設定が必要です。同じ種類でないとアンカーは機能しません。

ステップ 3 : 9800 WLC ( 外部として機能 ) にログインし、アンカーポリシープロファイルを作成します。

に移動します 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.

<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Name* <input style="width: 90%;" type="text" value="anchor-policy"/></div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Description <input style="width: 90%;" type="text" value="Enter Description"/></div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Status <span style="float: right; background-color: #27ae60; color: white; padding: 2px 5px; font-weight: bold;">ENABLED</span></div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Passive Client <input type="checkbox"/> DISABLED</div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Encrypted Traffic Analytics <input type="checkbox"/> DISABLED</div> <div style="background-color: #f0f0f0; padding: 5px; margin-bottom: 5px;">CTS Policy</div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Inline Tagging <input type="checkbox"/></div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">SGACL Enforcement <input type="checkbox"/></div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Default SGT <input style="width: 80%;" type="text" value="2-65519"/></div>	<div style="background-color: #f0f0f0; padding: 5px; margin-bottom: 5px;">WLAN Switching Policy</div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Central Switching <input checked="" type="checkbox"/></div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Central Authentication <input checked="" type="checkbox"/></div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Central DHCP <input checked="" type="checkbox"/></div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Central Association <input checked="" type="checkbox"/></div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Flex NAT/PAT <input type="checkbox"/></div>
---	--

↶ Cancel

💾 Save & Apply to Device

タMobilityブに移動し、アンカーAireOS WLCを選択します。9800 WLCは、このポリシープロファイルに関連付けられたSSIDのトラフィックを、選択されたアンカーに転送します。

**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: 1px solid red; padding: 2px;">  10.88.173.105      Tertiary ... <span style="float: right;">←</span> </div>

ステップ 4 : このWLANにサービスを提供する外部コントローラに関連付けられたAPに割り当てられたポリシータグ内のWLANに、ポリシープロファイルをリンクします。

に移動して新しいConfiguration > Tags & Profiles > Tags ファイルを作成するか、既存のファイルを使用します。

**Edit Policy Tag** ✕

Name\*

Description

**+ Add**

---

WLAN Profile  Policy Profile

◀ ◀ 0 ▶ ▶  items per page No items to display

**Map WLAN and Policy**

WLAN Profile\*   Policy Profile\*

変更をポリシー Update & Apply to Device タグに適用することを選択していることを確認します。

**Edit Policy Tag** ✕

Name\*

Description

**+ Add**

---

WLAN Profile  Policy Profile

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

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

---

ステップ 5 ( オプション ) : サイトを AP に割り当てるか、サイトにすでにサイトがあることを確認します。

に移動し Configuration > Wireless > Access Points > AP name > General ます。

Edit AP
✕

---

General
Interfaces
High Availability
Inventory
Advanced

<p>AP Name* <input type="text" value="karlcisn-AP-30"/></p> <p>Location* <input type="text" value="default-location"/></p> <p>Base Radio MAC <input type="text" value="000a.ad00.1f00"/></p> <p>Ethernet MAC <input type="text" value="000a.ad00.1ff0"/></p> <p>Admin Status <input style="border: 1px solid #ccc; width: 100%;" type="text" value="Enabled"/></p> <p>AP Mode <input style="border: 1px solid #ccc; width: 100%;" type="text" value="Local"/></p> <p>Operation Status <input type="text" value="Registered"/></p> <p>Fabric Status <input type="text" value="Disabled"/></p>	<p>Primary Software Version <input type="text" value="8.5.97.110"/></p> <p>Predownloaded Status <input type="text" value="N/A"/></p> <p>Predownloaded Version <input type="text" value="N/A"/></p> <p>Next Retry Time <input type="text" value="N/A"/></p> <p>Boot Version <input type="text" value="8.5.97.110"/></p> <p>IOS Version <input type="text" value=""/></p> <p>Mini IOS Version <input type="text" value="0.51.0.3"/></p>	<div style="background-color: #f0f0f0; padding: 5px; margin-bottom: 10px;">IP Config</div> <p>CAPWAP Preferred Mode <input type="text" value="Not Configured"/></p> <p>Static IPv4 Address <input type="text" value="11.11.0.39"/></p> <p>Static IP (IPv4/IPv6) <input checked="" type="checkbox"/></p> <p>Static IP (IPv4/IPv6) <input type="text" value="11.11.0.39"/></p> <p>Netmask <input type="text" value="255.255.0.0"/></p> <p>Gateway (IPv4/IPv6) <input type="text" value="11.11.0.1"/></p> <p>DNS IP Address (IPv4/IPv6) <input type="text" value="0.0.0.0"/></p> <p>Domain Name <input type="text" value="Cisco"/></p>
--	---	---

Tags

Policy

Site

RF

Time Statistics

Up Time

↶ Cancel

+ Update & Apply to Device

注：選択後にAPタグを変更するとUpdate & Apply to Device、APはトンネルCAPWAPを再起動するため、9800 WLCとの関連付けが失われ、回復します。

CLI から、

```
# config t
```

```
# wireless profile policy anchor-policy
# mobility anchor 10.88.173.105 priority 3
# no shutdown
# exit
```

```
# wireless tag policy PT1
# wlan anchor-ssid policy anchor-policy
# exit
```

```
# ap aaaa.bbbb.dddd
# site-tag PT1
# exit
```

手順 6 : AireOS WLCをアンカーとして設定します。

AireOSにログインし、に移動しWLANs > WLANs ます。WLAN行の右端にある矢印を選択して、ドロップダウンメニューに移動し、を選択しMobility Anchors ます。

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)]

ローカルアンカーとして設定します。



## Mobility Anchors

WLAN SSID anchor-ssid

Switch IP Address (Anchor)

Mobility Anchor Create

Switch IP Address (Anchor)

local

Priority <sup>1</sup>

3

### Foot Notes

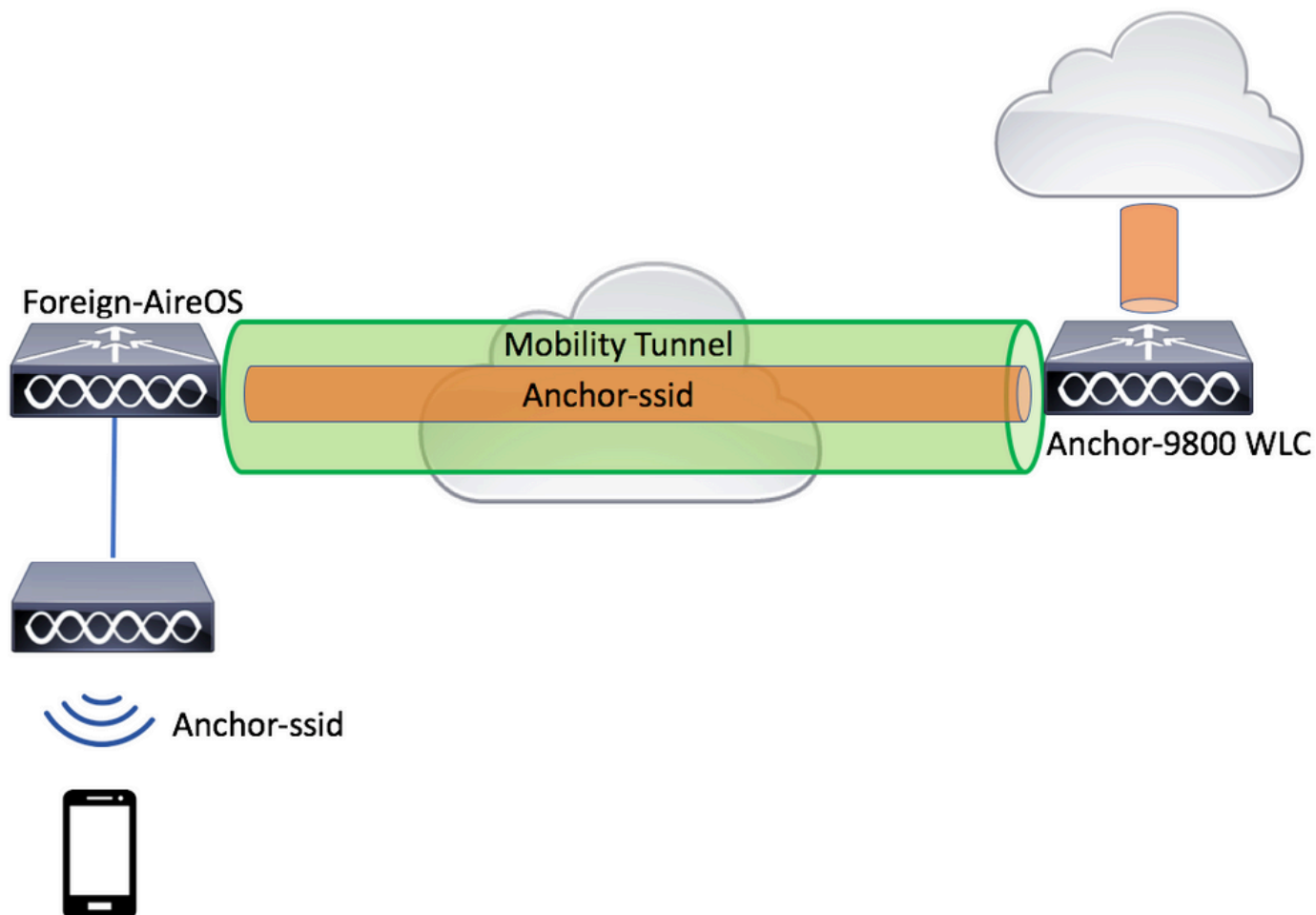
1. Priority number, 1=Highest priority and 3=Lowest priority(default).

CLI から、

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

外部AireOS : アンカー9800 WLC

AireOS Foreignと9800アンカーネットワーク図



## AireOSアンカーを使用した9800 Foreignの設定

ステップ 1： 外部9800 WLCとアンカーAireOS WLCの間にモビリティトンネルを構築します。


このドキュメントの「[Catalyst 9800でのモビリティポロジの設定](#)」を参照してください。

ステップ 2： 両方のWLCで目的のSSIDを作成します。

サポートされるセキュリティ方式：

- 開く
- MACフィルタ
- PSK
- Dot1x
- ローカル/外部Web認証(LWA)
- 中央Web認証(CWA)

---

 注:AireOS WLCと9800 WLCの両方に同じ種類の設定が必要です。同じ種類でないとアンカーは機能しません。

---

ステップ 3： ( アンカーとして機能する ) 9800 WLCにログインし、アンカーポリシープロファイルを作成します。

に移動します Configuration > Tags & Profiles > Policy > + Add。9800のポリシープロファイルの名前がAireOS WLCのプロファイル名と正確に同じであることを確認します。同じ名前でないとは機能しません。

### 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-ssid"/>	<b>WLAN Switching Policy</b>	
Description	<input type="text" value="Enter Description"/>	Central Switching	<input checked="" type="checkbox"/>
Status	<input checked="" type="checkbox"/> ENABLED	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"/>		

MobilityExport Anchor プに移動して有効にします。これにより、9800 WLCに対して、このポリシープロファイルを使用するすべてのWLANのアンカー9800 WLCであることが指示されます。外部 AireOS WLCがクライアントをアンカー9800 WLCに送信すると、クライアントが割り当てられているWLAN名について通知するため、アンカー9800 WLCは、使用するローカルWLAN設定を認識し、この名前を使用してどのローカルポリシープロファイルを使用するかを認識します。

### 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
 172.16.0.5 →	Anchors not assigned	
 10.88.173.49 →		

 注：外部コントローラからのトラフィックを受信するためだけに、このポリシープロファイルを使用するようにしてください。

CLI から、

Anchor 9800 WLC

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

ステップ 4：AireOS WLCを外部として設定します。

AireOSにログインし、WLANs > WLANs.Navigateに移動してWLAN行の最後にある矢印に移動し、Mobility Anchorsを選択します。

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

9800 WLCをこのSSIDのアンカーとして設定します。

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 3

Foot Notes

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

CLI から、

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

## 検証

これらのコマンドを使用して、外部/アンカーSSIDを使用するワイヤレスクライアントの設定と状態を確認できます。

### 9800 WLCでの確認

```
# 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>
```

### AireOS WLCでの確認

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

## トラブルシューティング

WLC 9800 では、ALWAYS-ON トレース機能を利用できます。これにより、クライアント接続に関連するすべてのエラー、警告、通知レベルのメッセージが常にログに記録され、インシデントまたは障害状態が発生した後でそのイベントを表示できます。



注：生成されるログの量に応じて、数時間から数日に戻ることができます。

---

9800 WLCがデフォルトで収集したトレースを表示するには、SSH/Telnet経由で9800 WLCに接続し、次の手順を参照します。（セッションは必ずテキストファイルに記録してください）

ステップ 1：コントローラの現在時刻を確認して、問題が発生した時刻までのログを追跡できるようにします。

```
# show clock
```

ステップ 2 : システム設定に従って、コントローラバッファまたは外部syslogからsyslogを収集します。これにより、システムの健全性とエラー (ある場合) をすばやく確認できます。

```
# show logging
```

ステップ 3 : 特定のMACアドレスまたはIPアドレスのAlways-on Notice Level(AIP)トレースを収集します。モビリティトンネルの問題が疑われる場合、またはワイヤレスクライアントのMACアドレスによって、リモートモビリティピアはこれをフィルタリングできます。

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

ステップ 4 : セッションで内容を表示するか、ファイルを外部 TFTP サーバーにコピーできます。

```
# more bootflash:always-on-<FILENAME.txt>
```

```
or
```

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

## 条件付きデバッグとラジオアクティブトレース

常時接続トレースで、調査中の問題のトリガーを判別するのに十分な情報が得られない場合は、条件付きデバッグを有効にしてRadio Active(RA)トレースをキャプチャできます。これにより、指定された条件 (この場合はクライアントMACアドレス) と対話するすべてのプロセスにデバッグレベルのトレースが提供されます。条件付きデバッグを有効にするには、次の手順を参照してください。

ステップ 5 : 有効なデバッグ条件がないことを確認します。


```
# clear platform condition all
```

手順 6：監視するワイヤレスクライアントのMACアドレスのデバッグ条件を有効にします。


次のコマンドは、指定された MAC アドレスの 30 分間 ( 1800 秒 ) のモニターを開始します。必要に応じて、この時間を最大 2085978494 秒まで増やすことができます。

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

---

 注:複数のクライアントを同時にモニタするには、MACアドレスごとにdebug wireless mac <aaaa.bbbb.cccc>コマンドを実行します。

---

 注:すべての内容は後で表示できるように内部でバッファされるため、ターミナルセッションのクライアントアクティビティの出力は表示されません。

---

手順 7：監視する問題または動作を再現します。

ステップ 8：デフォルトまたは設定されたモニタ時間がアップする前に問題が再現した場合は、デバッグを停止します。

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

モニタ時間が経過するか、ワイヤレスのデバッグが停止すると、9800 WLCは次の名前のローカルファイルを生成します。 ra\_trace\_MAC\_aaaabbbbcccc\_HHMMSS.XXX\_timezone\_DayWeek\_Month\_Day\_year.log

ステップ 9：MAC アドレスアクティビティのファイルを収集します。 RAトレースを外部サーバにコピーするか.log、出力を画面に直接表示できます。

RAトレースファイルの名前を確認します。



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

ファイルを外部サーバーにコピーします。

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


内容を表示します。

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

ステップ 10：根本原因がまだ明らかでない場合は、デバッグレベルのログのより詳細なビューである内部ログを収集します。ログはすでにコントローラメモリに書き込まれているため、クライアントを再度デバッグする必要はありません。ログの詳細ビューを表示するだけで済みます。

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

---

 注：このコマンド出力は、すべてのプロセスのすべてのログレベルのトレースを返し、非常に大量です。これらのトレースの解析をCisco TACに依頼してください。

---

を外部サーバにコピーするか `ra-internal-FILENAME.txt`、出力を画面に直接表示できます。

ファイルを外部サーバーにコピーします。

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


内容を表示します。

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

ステップ 11デバッグ条件を削除します。

```
# clear platform condition all
```

---

 注：トラブルシューティングセッションの後は、必ずデバッグ条件を削除してください。

---

## AireOS WLCの確認

このコマンドを実行して、AireOS WLC上のワイヤレスクライアントのアクティビティを監視できます。

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

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。