

Konfigurieren der Mobilitätsfunktion von WLAN Anchor auf dem Catalyst 9800

Inhalt

- [Einleitung](#)
- [Voraussetzungen](#)
- [Anforderungen](#)
- [Verwendete Komponenten](#)
- [Konfigurieren](#)
- [Auslands-/Ankerszenario zwischen 9800 WLCs](#)
- [Netzwerkdiagramm: Zwei Catalyst 9800 WLCs](#)
- [Konfigurieren eines 9800-Fremdkörpers mit einem 9800-Anker](#)
- [Foreign 9800 WLC - Anchor AireOS](#)
- [Catalyst 9800 \(Ausland\) - AireOS Anchor-Netzwerkdiagramm](#)
- [Konfigurieren des 9800 Foreign mit AireOS Anchor](#)
- [Foreign AirOS - Anchor 9800 WLC](#)
- [AireOS - Netzwerkdiagramm für den 9800 Anchor - Foreign](#)
- [Konfigurieren eines 9800 Foreign-Controllers mit einem AireOS-Anker](#)
- [Verifizierung](#)
- [Überprüfen Sie den 9800 WLC.](#)
- [Überprüfen auf dem AireOS WLC](#)
- [Fehlerbehebung](#)
- [Bedingtes Debugging und Radio Active Tracing](#)
- [Überprüfen des AireOS WLC](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie ein Wireless Local Area Network (WLAN) mit Catalyst 9800 Wireless Controllern in einem Fremd-/Ankerszenario konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Zugriff auf die Wireless Controller über eine Kommandozeile oder eine grafische Benutzeroberfläche
- Mobilität mit Cisco Wireless LAN Controllern (WLCs)
- Wireless Controller 9800
- AireOS-WLCs

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- AireOS WLC Version 8.8 MR2 (Sie können auch Inter Release Controller Mobility (IRCM) spezielle 8.5 Images verwenden)
- 9800 WLC v16.10 oder spätere Version

- Konfigurationsmodell des 9800 WLC

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

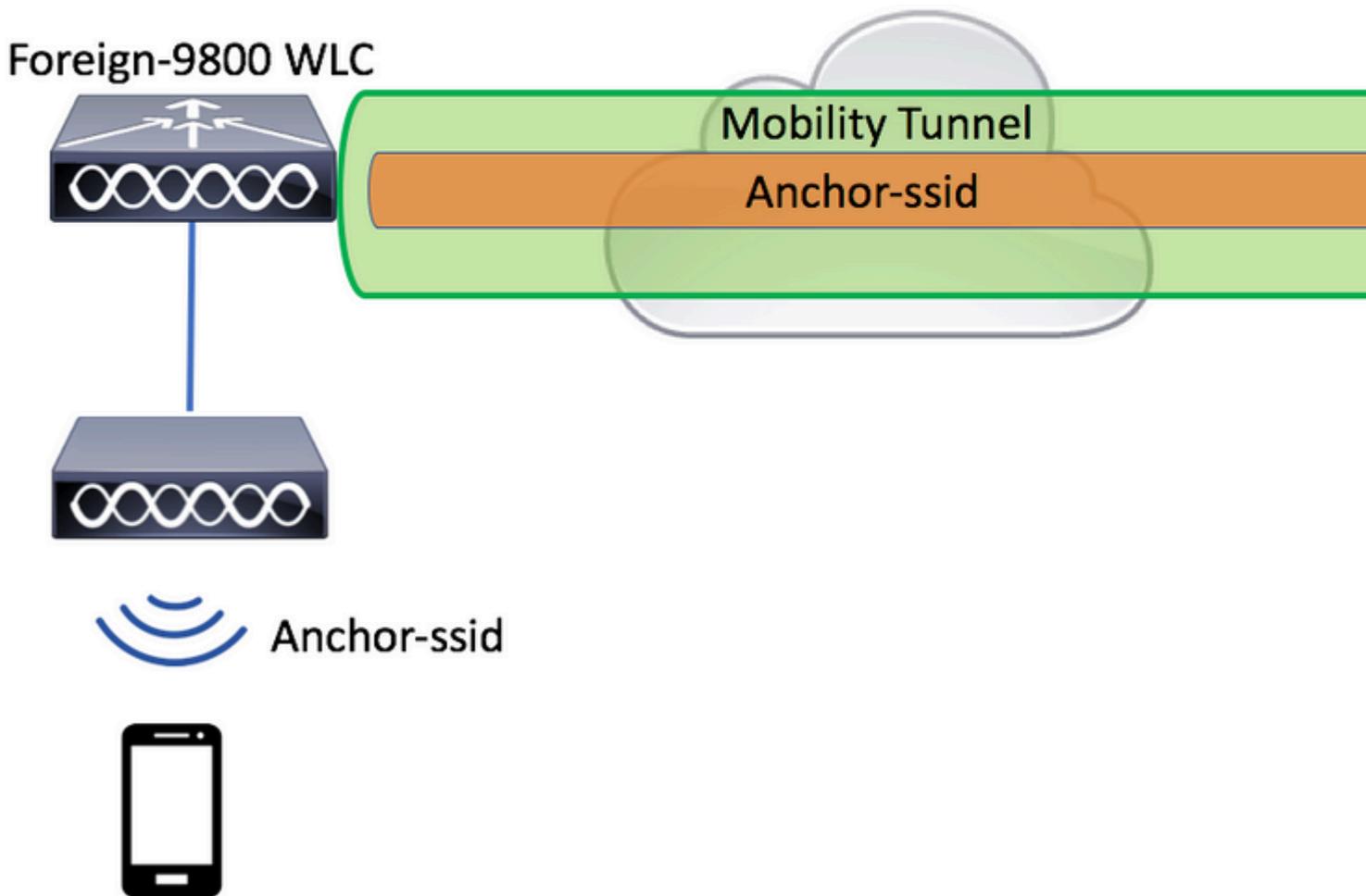
Konfigurieren

Dies ist eine Funktion, die normalerweise für Gastzugriffsszenarien verwendet wird, um den gesamten Datenverkehr von Clients an einem einzigen L3-Ausgangspunkt zu terminieren, selbst wenn die Clients von verschiedenen Controllern und physischen Standorten stammen. Der Mobility-Tunnel isoliert den Datenverkehr im Netzwerk.

Auslands-/Ankerszenario zwischen 9800 WLCs

Dieses Szenario zeigt die beiden verwendeten Catalyst Switches der Serie 9800.

Netzwerkdiagramm: Zwei Catalyst 9800 WLCs



In Szenarien mit Mobilitätsgästen gibt es zwei Hauptcontrollerrollen:

- Foreign Controller: Dieser WLC besitzt Layer 2 oder die Wireless-Seite. Es ist mit Access Points verbunden. Der gesamte Client-Datenverkehr für die verankerten WLANs wird in den Mobility Tunnel gekapselt und an den Anker gesendet. Es wird nicht lokal beendet.
- Anker-Controller: Dies ist der Ausgangspunkt für Layer 3. Es empfängt die Mobility-Tunnel von den ausländischen Controllern und entkapselt oder terminiert den Client-Datenverkehr an den Ausgangspunkt (VLAN). Dies ist der Punkt, an dem die Clients im Netzwerk sichtbar sind, also der Ankernamen.

Die Access Points auf dem ausländischen WLC übertragen die WLAN-SSIDs und verfügen über ein zugewiesenes Richtlinien-Tag, das das WLAN-Profil mit dem entsprechenden Richtlinienprofil verknüpft. Wenn ein Wireless-Client eine Verbindung mit dieser SSID herstellt, sendet der ausländische Controller beide, den SSID-Namen und das Richtlinienprofil, als Teil der Client-Informationen an den Anker-WLC. Nach Eingang überprüft der Anker-WLC seine eigene Konfiguration auf Übereinstimmung mit dem SSID-Namen und dem Richtlinienprofilnamen. Sobald der Anker-WLC eine Übereinstimmung gefunden hat,

wendet er die entsprechende Konfiguration und einen Ausgangspunkt auf den Wireless-Client an. Aus diesem Grund ist es erforderlich, dass die Namen und Konfigurationen der WLAN- und Richtlinienprofile auf dem ausländischen 9800 WLC und dem verankerten 9800 WLC übereinstimmen, mit Ausnahme des VLAN unter dem Richtlinienprofil.

Hinweis: Die Namen der WLAN-Profile und Richtlinienprofile können auf dem 9800 Anchor und dem 9800 Foreign WLC übereinstimmen.

Konfigurieren eines 9800-Fremdkörpers mit einem 9800-Anker

Schritt 1: Bau eines Mobilitätstunnels zwischen dem Foreign 9800 WLC und dem Anchor 9800 WLC.

Sie können sich auf dieses Dokument beziehen: [Konfigurieren von Mobilitätstopologien auf Catalyst 9800](#)

Schritt 2: Erstellen Sie die gewünschte SSID auf beiden 9800 WLCs.

Unterstützte Sicherheitsmethoden:

- Offen
- MAC-Filter
- PSK
- Punkt 1x
- Lokale/externe Webauthifizierung (LWA)
- Zentrale Webauthifizierung (CWA)

Hinweis: Beide 9800 WLCs müssen die gleiche Konfiguration haben, da die Auslösung aus diesem Grund nicht funktioniert.

Schritt 3: Melden Sie sich beim ausländischen 9800 WLC an, und definieren Sie im Richtlinienprofil die Anker-IP-Adresse des 9800 WLC.

Navigieren Sie zu `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

Description

Enter Description

Status

ENABLED

Passive Client

DISABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

2-65519

WLAN Switching Policy

Central Switching

Central Authentication

Central DHCP

Central Association

Flex NAT/PAT

 Cancel

 Save

Auf dem **Mobility** die IP-Adresse des Anker 9800 WLC aus.

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)

Anchor IP

 172.16.0.5	→
---	---

Selected (1)

Anchor IP

Anchor Priority

 10.88.173.49	Tertiary ...
---	--------------

Cancel

Save &

Schritt 4: Verknüpfen Sie das Richtlinienprofil mit dem WLAN innerhalb der Richtlinien-Tag-Nummer, die den APs zugewiesen ist, die dem ausländischen Controller zugeordnet sind, der dieses WLAN bedient.

Navigieren Sie zu [Configuration > Tags & Profiles > Tags](#) und entweder eine neue erstellen oder die vorhandene verwenden.

Edit Policy Tag

Name*

Description

+ Add

WLAN Profile	Policy Profile
<input type="button" value="x"/> <input type="button" value="✓"/>	

Map WLAN and Policy

WLAN Profile* Policy Profile*

Auswahl **Update & Apply to Device** , um die Änderungen auf das Policy Tag anzuwenden.

Edit Policy Tag

Name*

Description

+ Add

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

Schritt 5 (optional). Weisen Sie die Policy Tag-Nummer einem Access Point zu, oder stellen Sie sicher, dass dieser bereits vorhanden ist.

Navigieren Sie zu Configuration > Wireless > Access Points > AP name > General.

Edit AP

General

Interfaces

High Availability

Inventory

Advanced

AP Name*	<input type="text" value="karlcisn-AP-30"/>
Location*	<input type="text" value="default-location"/>
Base Radio MAC	000a.ad00.1f00
Ethernet MAC	000a.ad00.1ff0
Admin Status	<input type="text" value="Enabled"/>
AP Mode	<input type="text" value="Local"/>
Operation Status	Registered
Fabric Status	Disabled

Tags

Policy	<input type="text" value="PT1"/>
Site	<input type="text" value="ST1"/>
RF	<input type="text" value="RT1"/>

Primary Software Version	8.5.97.110
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A
Boot Version	8.5.97.110
IOS Version	
Mini IOS Version	0.51.0.3

IP Config

CAPWAP Preferred Mode	Not Configured
Static IPv4 Address	<input type="text" value="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 mins 26
---------	------------------

 Cancel

 Update &

Anmerkung: Beachten Sie, dass, wenn Sie eine Änderung am AP-Tag vornehmen, nachdem Sie `Update & Apply to Device` wird der Tunnel CAPWAP neu gestartet, sodass die Verbindung zum 9800 WLC unterbrochen wird und dieser dann wiederhergestellt wird.

Über die 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-ssid policy anchor-policy
# exit
```

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

Schritt 6: Melden Sie sich beim Anker 9800 WLC an, und erstellen Sie das Anker-Richtlinienprofil. Vergewissern Sie sich, dass der Name exakt dem entspricht, den Sie für die ausländischen 9800-WLCs verwendet haben.

Navigieren Sie zu `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"/>	WLAN Switching Policy
Description	<input type="text" value="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"/>
CTS Policy		Flex NAT/PAT <input type="checkbox"/>
Inline Tagging	<input type="checkbox"/>	
SGACL Enforcement	<input type="checkbox"/>	
Default SGT	<input type="text" value="2-65519"/>	

Navigieren Sie zu **Mobility** Registerkarte und aktivieren **Export Anchor**. Dadurch wird der 9800 WLC angewiesen, dass er der Anker-WLC für alle WLANs ist, die dieses Richtlinienprofil verwenden. Wenn der ausländische 9800-WLC die Clients an den Anker-9800-WLC sendet, informiert er über das WLAN und das Richtlinienprofil, dem der Client zugewiesen ist, sodass der Anker-9800-WLC weiß, welches lokale Richtlinienprofil verwendet werden soll.

Hinweis: Sie dürfen nicht gleichzeitig Mobilitäts-Peers und den Exportanker konfigurieren. Dies ist ein ungültiges Konfigurationsszenario.

Hinweis: Sie dürfen die Einstellung "Anker exportieren" nicht für Richtlinienprofile verwenden, die mit einem WLAN-Profil auf einem Controller mit Access Points verknüpft sind. Dadurch wird verhindert, dass die SSID übertragen wird. Daher muss diese Richtlinie ausschließlich für die Ankerfunktion verwendet werden.

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 →		

Über die CLI:

```
Anchor 9800 WLC

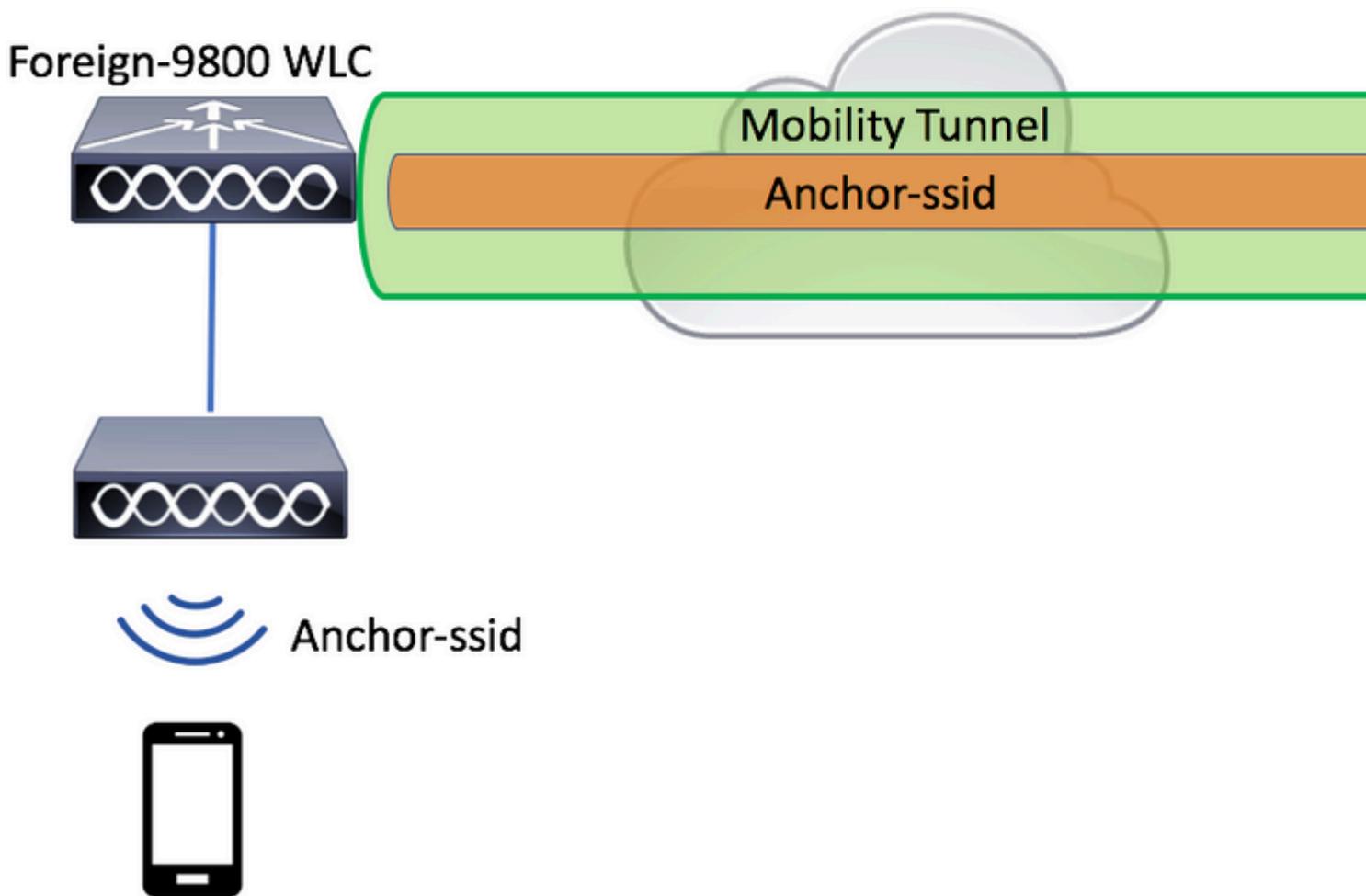
# config t
# wireless profile policy <anchor-policy>
# mobility anchor
# vlan <VLAN-id_VLAN-name>
# no shutdown
# exit
```

Foreign 9800 WLC - Anchor AireOS

In dieser Konfiguration wird das Szenario dargestellt, in dem ein Catalyst 9800 WLC als Foreign (Ausland)

und ein AireOS Unified WLC als Anker verwendet werden.

Catalyst 9800 (Ausland) - AireOS Anchor-Netzwerkdiagramm



Konfigurieren des 9800 Foreign mit AireOS Anchor

Schritt 1: Bau eines Mobilitätstunnels zwischen dem Foreign 9800 WLC und dem Anchor AireOS WLC.

Weitere Informationen finden Sie in diesem Dokument: [Konfigurieren von Mobilitätstopologien auf Catalyst 9800](#)

Schritt 2: Erstellen Sie die gewünschten WLANs auf beiden WLCs.

Unterstützte Sicherheitsmethoden:

- Offen
- MAC-Filter
- PSK
- Punkt 1x
- Lokale/externe Webauthentifizierung (LWA)
- Zentrale Webauthentifizierung (CWA)

Hinweis: Sowohl der AireOS WLC als auch der 9800 WLC müssen gleich konfiguriert sein, andernfalls funktioniert die Verankerung nicht.

Schritt 3: Melden Sie sich beim 9800 WLC (der als ausländischer Benutzer agiert) an, und erstellen Sie das Ankerrichtlinienprofil.

Navigieren Sie zu 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

Description

Enter Description

Status

ENABLED



Passive Client



DISABLED

Encrypted Traffic Analytics



DISABLED

CTS Policy

Inline Tagging



SGACL Enforcement



Default SGT

2-65519

WLAN Switching Policy

Central Switching



Central Authentication



Central DHCP



Central Association



Flex NAT/PAT



↶ Cancel

📄 Save &

Navigieren Sie zu **Mobility** und wählen Sie den Anker AireOS WLC. Der 9800 WLC leitet den Datenverkehr der mit diesem Richtlinienprofil verknüpften SSID an den ausgewählten Anker weiter.

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	 10.88.173.105 Tertiary ... ▼

Schritt 4: Verknüpfen Sie das Richtlinienprofil mit dem WLAN innerhalb der Richtlinien-Tag-Nummer, die den APs zugewiesen ist, die dem ausländischen Controller zugeordnet sind, der dieses WLAN bedient.

Navigieren Sie zu **Configuration > Tags & Profiles > Tags** und entweder eine neue erstellen oder die vorhandene verwenden.

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*

Auswahl Update & Apply to Device , um die Änderungen auf das Policy Tag anzuwenden.

Edit Policy Tag

Name*

Description

+ Add

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

10 items per page 1 - 1 of 1 items

Schritt 5 (optional). Weisen Sie die Site einem Access Point zu, oder stellen Sie sicher, dass sie bereits vorhanden ist.

Navigieren Sie zu Configuration > Wireless > Access Points > AP name > General.

Edit AP

General

Interfaces

High Availability

Inventory

Advanced

AP Name*	<input type="text" value="karlcisn-AP-30"/>
Location*	<input type="text" value="default-location"/>
Base Radio MAC	000a.ad00.1f00
Ethernet MAC	000a.ad00.1ff0
Admin Status	<input type="text" value="Enabled"/>
AP Mode	<input type="text" value="Local"/>
Operation Status	Registered
Fabric Status	Disabled

Tags

Policy	<input type="text" value="PT1"/>
Site	<input type="text" value="ST1"/>
RF	<input type="text" value="RT1"/>

Primary Software Version	8.5.97.110
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A
Boot Version	8.5.97.110
IOS Version	
Mini IOS Version	0.51.0.3

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 mins 26
---------	------------------

 Cancel

 Update &

Hinweis: Beachten Sie, dass, wenn Sie eine Änderung am AP-Tag vornehmen, nachdem Sie `Update & Apply to Device` wird der Tunnel CAPWAP neu gestartet, sodass die Verbindung zum 9800 WLC unterbrochen wird und dieser dann wiederhergestellt wird.

Über die 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-ssid policy anchor-policy
# exit

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

Schritt 6: Konfigurieren Sie den AireOS WLC als Auslöser.

Melden Sie sich bei AireOS an, und navigieren Sie zu `WLANs > WLANs`. Klicken Sie auf den Pfeil am rechten Ende der WLAN-Zeile, um zum Dropdown-Menü zu navigieren, und wählen Sie `Mobility Anchors`.

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status
1	WLAN			Enabled
2	Remote LAN		---	Enabled
3	WLAN			Enabled
4	Remote LAN		---	Disabled
5	WLAN	anchor-ssid	anchor-ssid	Disabled

Legen Sie ihn als lokalen Anker fest.

Mobility Anchors

WLAN SSID anchor-ssid

Switch IP Address (Anchor)

Mobility Anchor Create

Switch IP Address (Anchor)

local

Priority ¹

3

Foot Notes

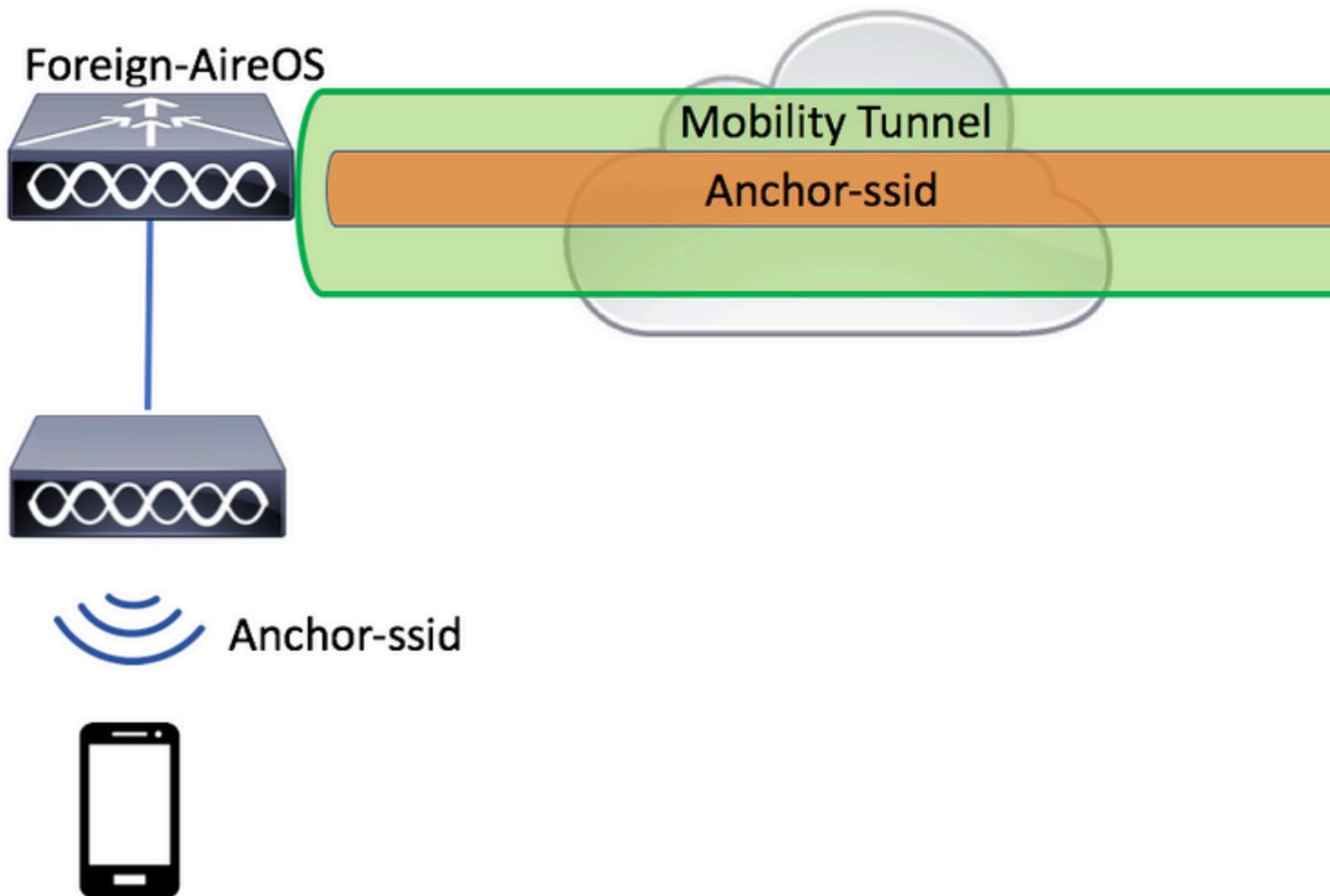
1. Priority number, 1=Highest priority and 3=Lowest priority(default).

Über die CLI:

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

Foreign AirOS - Anchor 9800 WLC

AireOS - Netzwerkdiagramm für den 9800 Anchor - Foreign



Konfigurieren eines 9800 Foreign-Controllers mit einem AireOS-Anker

Schritt 1: Bau eines Mobilitätstunnels zwischen dem Foreign 9800 WLC und dem Anchor AireOS WLC.

Sie können sich auf dieses Dokument beziehen: [Konfigurieren von Mobilitätstopologien auf Catalyst 9800](#)

Schritt 2: Erstellen Sie die gewünschte SSID auf beiden WLCs.

Unterstützte Sicherheitsmethoden:

- Offen
- MAC-Filter
- PSK
- Punkt 1x
- Lokale/externe Webauthentifizierung (LWA)

- Zentrale Webauthentifizierung (CWA)

Hinweis: Sowohl der AireOS WLC als auch der 9800 WLC müssen gleich konfiguriert sein, andernfalls funktioniert die Verankerung nicht.

Schritt 3: Melden Sie sich beim 9800 WLC an (der als Anker fungiert), und erstellen Sie das Ankerrichtlinienprofil.

Navigieren Sie zu [Configuration > Tags & Profiles > Policy > + Add](#). Stellen Sie sicher, dass der Name des Richtlinienprofils auf dem 9800 mit dem Namen des Profils auf dem AireOS WLC übereinstimmt. Andernfalls funktioniert er nicht.

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-ssid

Description

Enter Description

Status

ENABLED



Passive Client



DISABLED

Encrypted Traffic Analytics



DISABLED

CTS Policy

Inline Tagging



SGACL Enforcement



Default SGT

2-65519

WLAN Switching Policy

Central Switching



Central Authentication



Central DHCP



Central Association



Flex NAT/PAT



Cancel



Save &

Navigieren Sie zu [Mobility Registerkarte](#) und aktivieren [Export Anchor](#). Dadurch wird der 9800 WLC angewiesen, dass er der Anker-WLC für alle WLANs ist, die dieses Richtlinienprofil verwenden. Wenn der ausländische AireOS-WLC die Clients an den Anker 9800 WLC sendet, informiert er über den WLAN-Namen, dem der Client zugewiesen ist, sodass der Anker 9800 WLC weiß, welche lokale WLAN-

Konfiguration verwendet werden soll, und er verwendet diesen Namen, um zu erfahren, welches lokale Richtlinienprofil verwendet werden soll.

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><thead><tr><th>Anchor IP</th><th></th></tr></thead><tbody><tr><td> 172.16.0.5</td><td>→</td></tr><tr><td> 10.88.173.49</td><td>→</td></tr></tbody></table>	Anchor IP		 172.16.0.5	→	 10.88.173.49	→	Anchor IP	Anchor Priority
Anchor IP								
 172.16.0.5	→							
 10.88.173.49	→							
	Anchors not assigned							

Hinweis: Verwenden Sie dieses Richtlinienprofil ausschließlich für den Empfang von Datenverkehr von ausländischen Controllern.

Über die CLI:

```
Anchor 9800 WLC

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

exit

Schritt 4: Konfigurieren Sie den AireOS WLC als Foreign.

Melden Sie sich bei AireOS an, und navigieren Sie zu WLANs > WLANs. Navigieren Sie zum Pfeil am Ende der Zeile WLAN, und wählen Sie Mobility AnchorS .

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status
1	WLAN			Enabled
2	Remote LAN		---	Enabled
3	WLAN			Enabled
4	Remote LAN		---	Disabled
5	WLAN	anchor-ssid	anchor-ssid	Disabled

Legen Sie den 9800 WLC als Referenzzeichen für diese SSID fest.

WLAN SSID anchor-ssid

Switch IP Address (Anchor) 10.88.173.105

Mobility Anchor Create

Priority 1 3

Foot Notes

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

Über die CLI:

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

Verifizierung

Mithilfe dieser Befehle können Sie die Konfiguration und den Status der Wireless-Clients mithilfe einer Foreign-/Anker-SSID überprüfen.

Überprüfen Sie den 9800 WLC.

```
# 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>
```

Überprüfen auf dem AireOS WLC

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

Fehlerbehebung

WLC 9800 bietet ALWAYS-ON-Tracing-Funktionen (immer aktiv). So wird sichergestellt, dass alle verbindungsbezogenen Fehler, Warnungen und Benachrichtigungen auf Client-Ebene ständig protokolliert werden und Sie Ereignisse für einen Vorfall oder einen Fehler anzeigen können, nachdem dieser aufgetreten ist.

Hinweis: Je nach Umfang der generierten Protokolle können Sie einige Stunden bis mehrere Tage zurückgehen.

Um die Traces anzuzeigen, die der 9800 WLC standardmäßig erfasst, können Sie sich über SSH/Telnet mit dem 9800 WLC verbinden und diese Schritte lesen. (Stellen Sie sicher, dass die Sitzung in einer Textdatei protokolliert wird.)

Schritt 1: Überprüfen Sie die aktuelle Uhrzeit des Controllers, damit Sie die Protokolle bis zum Auftreten des Problems nachverfolgen können.

```
# show clock
```

Schritt 2: Sammeln Sie Syslogs aus dem Controller-Puffer oder dem externen Syslog, je nach Systemkonfiguration. Dadurch erhalten Sie eine Kurzübersicht über den Systemzustand und etwaige Fehler.

```
# show logging
```

Schritt 3: Sammeln Sie die Traces auf permanenter Benachrichtigungsebene für die jeweilige MAC- oder IP-Adresse. Remote-Mobility-Peer kann dies filtern, wenn Sie ein Problem mit dem Mobility-Tunnel vermuten, oder nach der MAC-Adresse des Wireless-Clients.

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

Schritt 4: Sie können entweder den Inhalt der Sitzung anzeigen oder die Datei auf einen externen TFTP-Server kopieren.

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

Bedingtes Debugging und Radio Active Tracing

Wenn die stets verfügbaren Ablaufverfolgungen nicht genügend Informationen liefern, um den Auslöser für das zu untersuchende Problem zu bestimmen, können Sie bedingtes Debuggen aktivieren und Radio Active (RA)-Ablaufverfolgungen erfassen, die Ablaufverfolgungen auf Debugebene für alle Prozesse bereitstellen, die mit der angegebenen Bedingung interagieren (in diesem Fall Client-MAC-Adresse). Informationen zum Aktivieren des bedingten Debuggens finden Sie in diesen Schritten.

Schritt 5: Stellen Sie sicher, dass keine Debugbedingungen aktiviert sind.

```
# clear platform condition all
```

Schritt 6: Aktivieren Sie die Debug-Bedingung für die MAC-Adresse des Wireless-Clients, die Sie überwachen möchten.

Mit diesen Befehlen wird die angegebene MAC-Adresse 30 Minuten (1800 Sekunden) lang überwacht. Sie können diese Zeit optional auf bis zu 2085978494 Sekunden erhöhen.

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

Hinweis: Um mehr als einen Client gleichzeitig zu überwachen, führen Sie den Befehl `debug wireless mac <aaaa.bbbb.cccc>` für jede MAC-Adresse aus.

Hinweis: Die Ausgabe der Client-Aktivität wird in der Terminal-Sitzung nicht angezeigt, da alles intern gepuffert wird, um später angezeigt zu werden.

Schritt 7. Reproduzieren Sie das Problem oder Verhalten, das Sie überwachen möchten.

Schritt 8: Stoppen Sie die Debugs, wenn das Problem reproduziert wird, bevor die standardmäßige oder konfigurierte Monitoring-Zeit abgelaufen ist.

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

Wenn die Überwachungszeit abgelaufen ist oder das Wireless-Debugging beendet wurde, generiert der 9800 WLC eine lokale Datei mit dem

Namen: `ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log`

Schritt 9. Rufen Sie die Datei mit der MAC-Adressaktivität ab. Sie können die RA-Ablaufverfolgung entweder kopieren `.log` auf einen externen Server oder zeigen die Ausgabe direkt auf dem Bildschirm an.

Überprüfen Sie den Namen der RA-Tracing-Datei:

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

Datei auf externen Server kopieren:

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

Inhalt anzeigen:

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

Schritt 10. Wenn die Ursache immer noch nicht offensichtlich ist, sammeln Sie die internen Protokolle, die eine ausführlichere Ansicht der Protokolle auf Debugebene darstellen. Sie müssen den Client nicht erneut debuggen, da die Protokolle bereits im Controller-Speicher geschrieben wurden und Sie nur eine ausführlichere Ansicht dieser Protokolle erstellen müssen.

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

Hinweis: Diese Befehlsausgabe gibt Traces für alle Protokollierungsebenen für alle Prozesse zurück und ist sehr umfangreich. Wenden Sie sich an das Cisco TAC, um diese Traces zu analysieren.

Sie können die `ra-internal-FILENAME.txt` auf einen externen Server oder zeigen die Ausgabe direkt auf dem Bildschirm an.

Datei auf externen Server kopieren:

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

Inhalt anzeigen:

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

Schritt 11. Entfernen Sie die Debug-Bedingungen.

```
# clear platform condition all
```

Hinweis: Stellen Sie sicher, dass Sie die Debug-Bedingungen immer nach einer Fehlerbehebungssitzung entfernen.

Überprüfen des AireOS WLC

Mit diesem Befehl können Sie die Aktivität eines Wireless-Clients auf einem AireOS WLC überwachen.

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.