

# Mesh auf Catalyst 9800 Wireless LAN Controllern konfigurieren

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Anwenderbericht 1: Bridge-Modus](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Anwenderbericht 2: Flex + Bridge](#)

[Konfigurieren](#)

[Überprüfung](#)

[Fehlerbehebung](#)

## Einleitung

In diesem Dokument wird ein einfaches Konfigurationsbeispiel zum Verbinden eines Mesh-Access Points (AP) mit dem Catalyst 9800 Wireless LAN Controller (WLC) beschrieben.

## Voraussetzungen

### Anforderungen

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

- Catalyst Wireless 9800-Konfigurationsmodell
- Konfiguration von LAPs
- Steuerung und Bereitstellung von Wireless Access Points (CAPWAP)
- Konfiguration eines externen DHCP-Servers
- Konfiguration der Cisco Switches

### Verwendete Komponenten

In diesem Beispiel wird ein Lightweight Access Point (1572AP und 1542) verwendet, der entweder als Root AP (RAP) oder Mesh AP (MAP) für den Anschluss an den Catalyst 9800 WLC konfiguriert werden kann. Die Vorgehensweise ist für Access Points der Serie 1542 oder 1562 identisch. Der RAP ist über einen Cisco Catalyst Switch mit dem Catalyst 9800 WLC verbunden.

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

- C9800-CL v16.12.1
- Cisco Layer-2-Switch
- Cisco Aironet Lightweight Outdoor Access Points der Serie 1572 für den Bridge-Bereich

- Cisco Aironet 1542 für den Bereich Flex+Bridge

**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**

### **Anwenderbericht 1: Bridge-Modus**

#### **Netzwerkdiagramm**

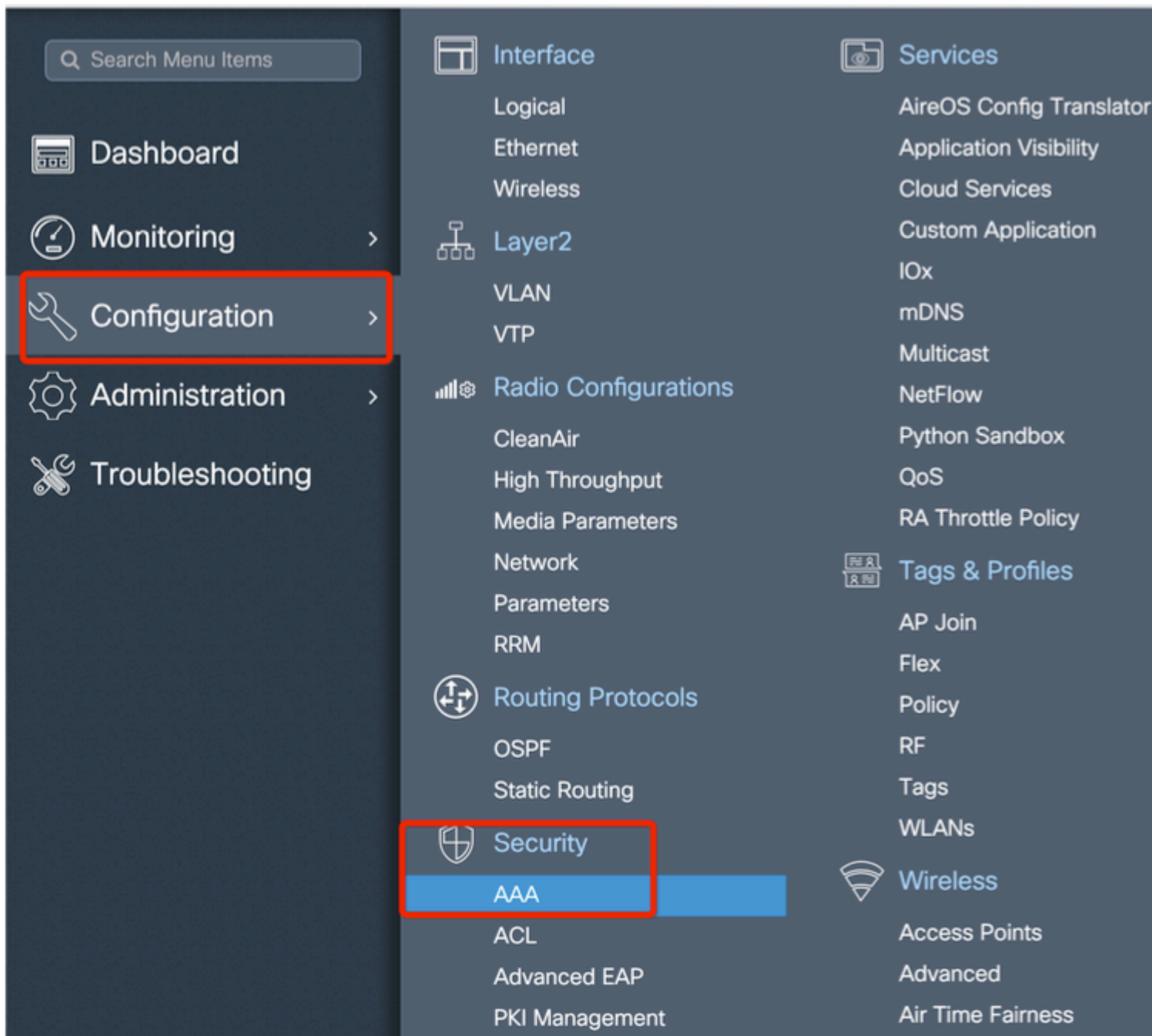
#### **Konfigurationen**

Ein Mesh-AP muss authentifiziert werden, damit er dem 9800-Controller beitreten kann. In dieser Fallstudie wird berücksichtigt, dass Sie den Access Point im lokalen Modus zuerst dem WLC beitreten und ihn dann in den Bridge (alias) Mesh-Modus umwandeln.

Um die Zuweisung von AP-Join-Profilen zu vermeiden, verwenden Sie dieses Beispiel, konfigurieren Sie jedoch die standardmäßige AAA-Methode zum Herunterladen von Autorisierungsanmeldeinformationen, sodass alle Mesh-APs dem Controller beitreten können.

**Schritt 1:** Konfigurieren Sie die RAP-/MAP-MAC-Adressen unter Device Authentication (Geräteauthentifizierung).

Gehen Sie zu **Configuration > AAA > AAA Advanced > Device Authentication** .

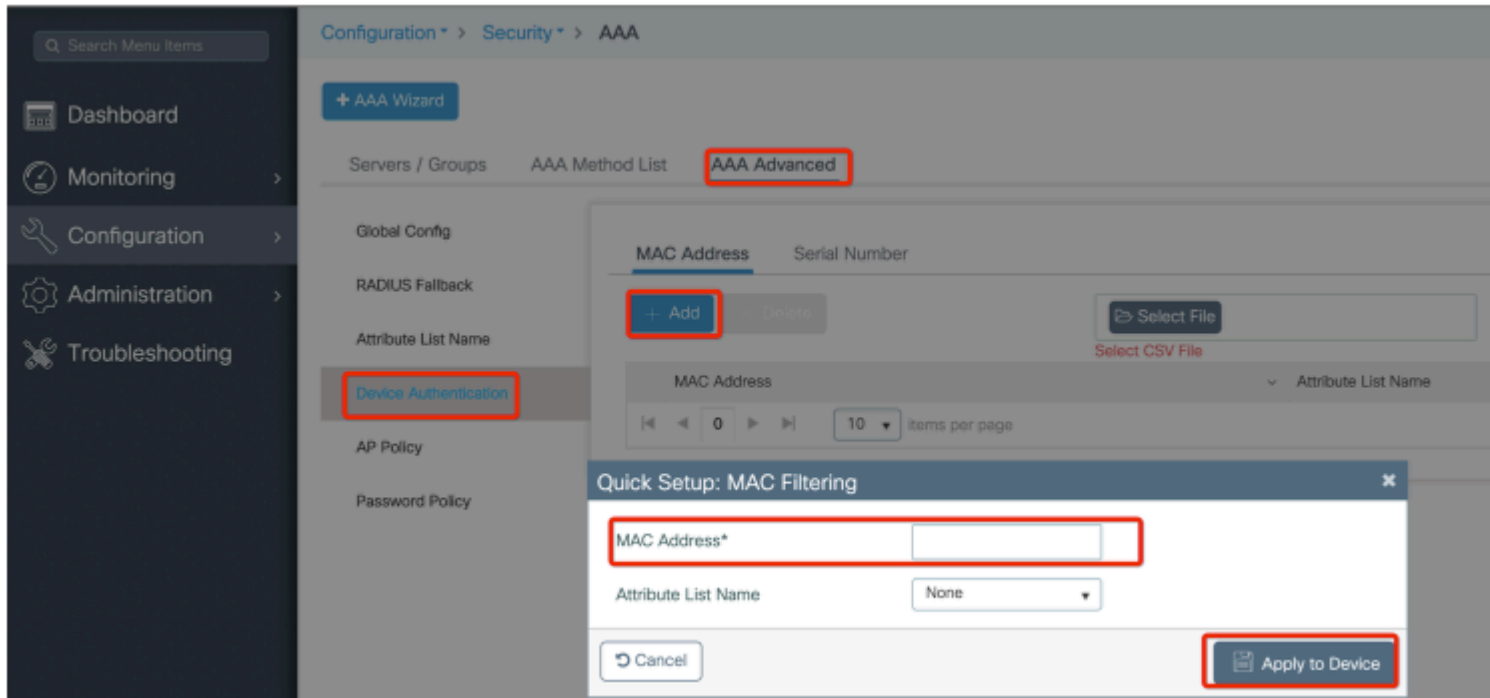


Fügen Sie die Base Ethernet-MAC-Adresse der Mesh Access Points hinzu, und fügen Sie sie ohne Sonderzeichen, ohne '.' oder ':' hinzu.

---

**Wichtig:** Ab Version 17.3.1 Wenn MAC-Adresstrennzeichen wie '.', ':' oder '-' hinzugefügt werden, kann der AP nicht beitreten. Derzeit sind zwei Erweiterungen in diesem Zusammenhang möglich: die [Cisco Bug-ID CSCvv43870](#) und die Cisco Bug-ID [CSCvr07920](#). In Zukunft werden alle MAC-Adressformate von 9800 akzeptiert.

---



**Schritt 2:** Konfigurieren Sie die Liste der Authentifizierungs- und Autorisierungsmethoden.

Gehen Sie zu **Configuration > Security > AAA > AAA Method list > Authentication**, und erstellen Sie die Liste mit Authentifizierungsmethoden und Autorisierungsmethoden.

+ AAA Wizard

Servers / Groups

AAA Method List

AAA Advanced

Authentication

Authorization

Accounting

+ Add

Delete

### Quick Setup: AAA Authorization

Method List Name\*

Mesh\_Authz

Type\*

credential-download

Group Type

local

Authenticated

Available Server Groups

radius  
ldap  
tacacs+  
ISE-Group  
ISE\_grp\_I2

Assigned Server Groups

>

<

Cancel

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups **AAA Method List** AAA Advanced

**Authentication**

Authorization

Accounting

+ Add Delete

Quick Setup: AAA Authentication

Method List Name\* Mesh\_Authentication

Type\* dot1x

Group Type local

Available Server Groups Assigned Server Groups

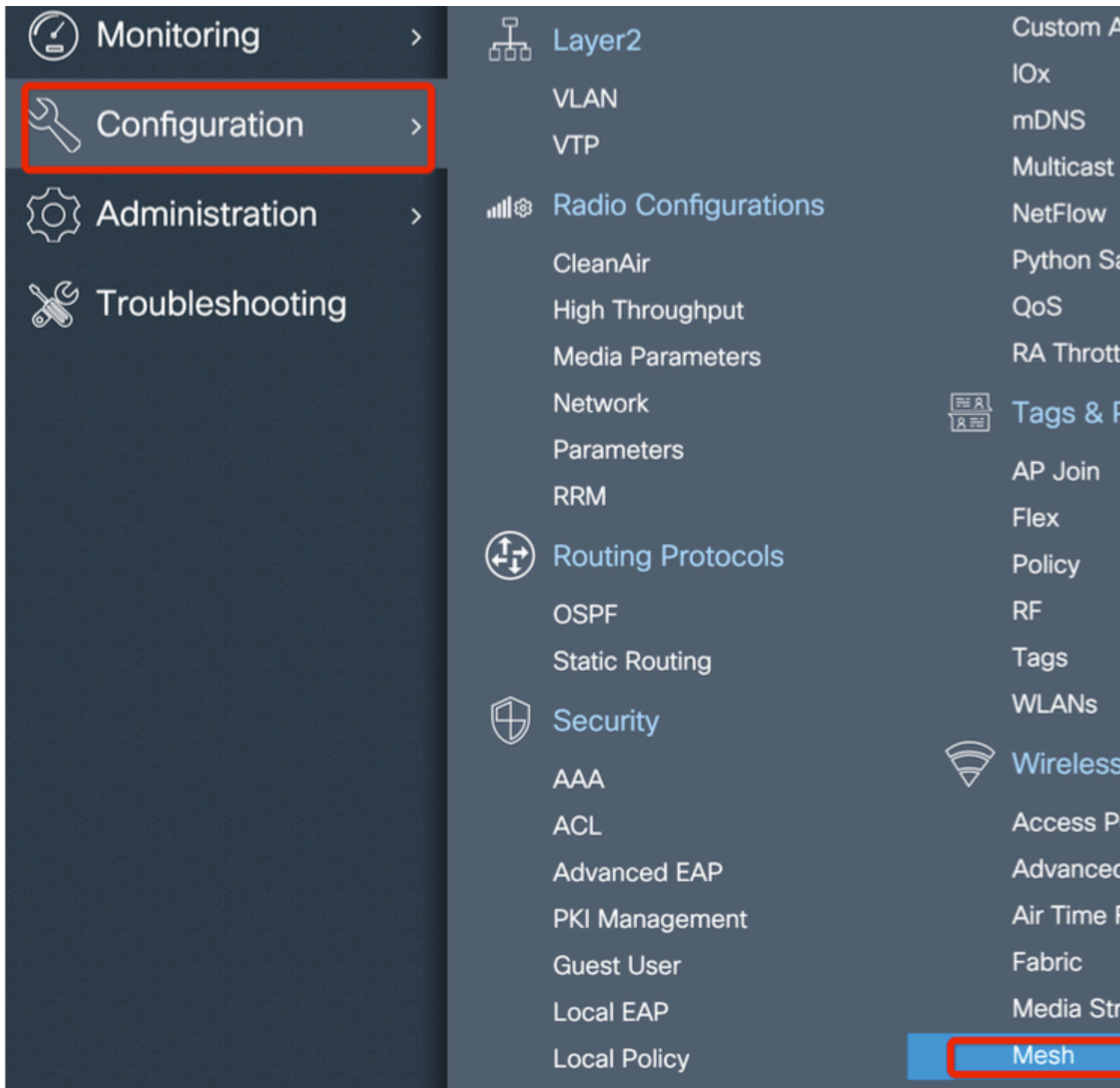
radius  
ldap  
tacacs+  
ISE-Group  
ISE\_grp\_I2

>  
<

Cancel

### Schritt 3: Konfigurieren der globalen Mesh-Parameter

Gehen Sie zu **Konfiguration > Mesh > Globale** Parameter. Zunächst können diese Werte auf die Standardwerte zurückgesetzt werden.



**Schritt 4:** Erstellen Sie ein neues Mesh-Profil unter **Konfiguration > Mesh > Profil > +Hinzufügen**

Global Config **Profiles**

**+ Add** Delete

Number of Profiles : 1

### Add Mesh Profile

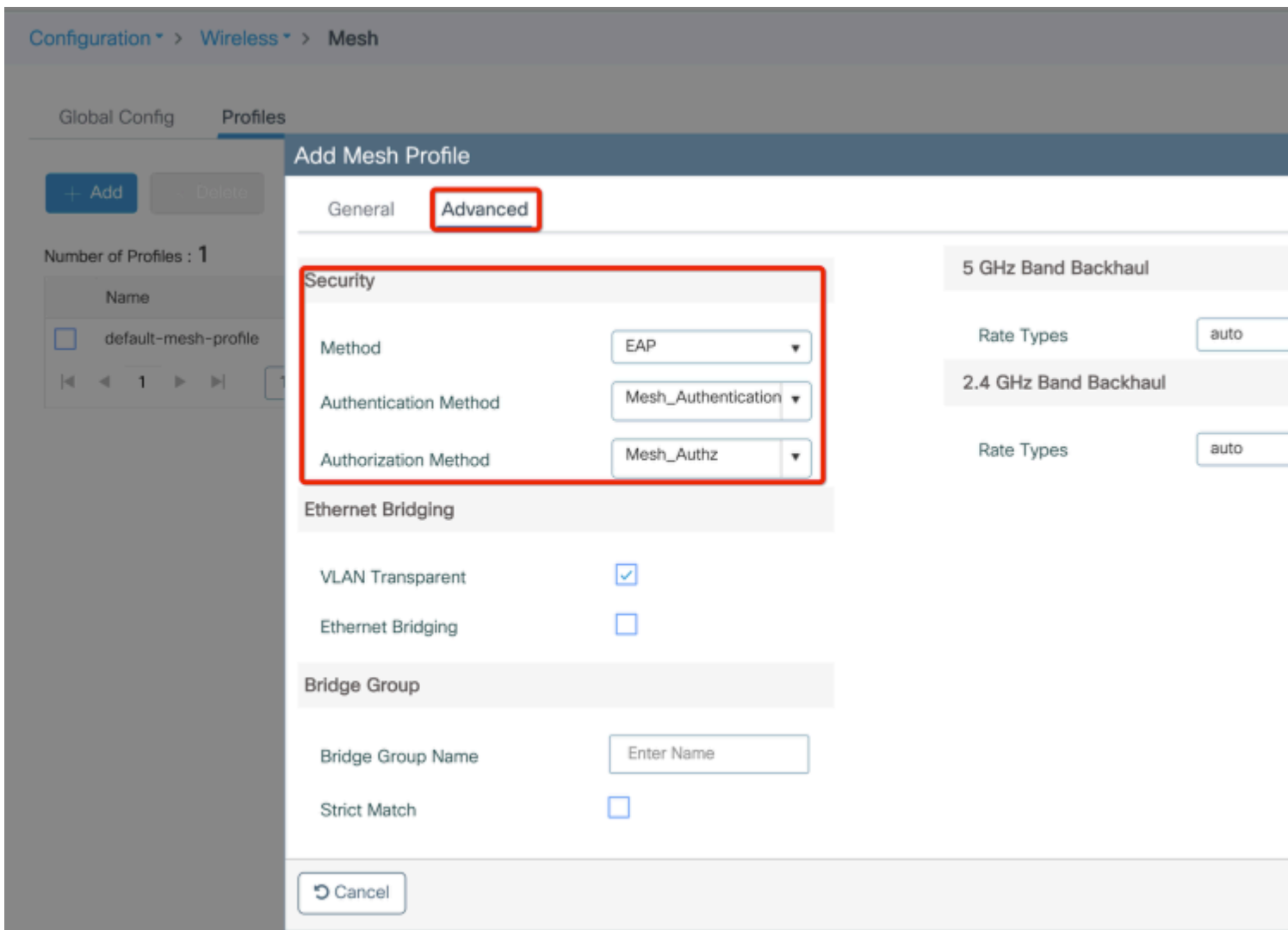
**General** Advanced

Name*	<input type="text" value="Mesh_Profile"/>	Backhaul amsdu	<input checked="" type="checkbox"/>
Description	<input type="text" value="Enter Description"/>	Backhaul Client Access	<input type="checkbox"/>
Range (Root AP to Mesh AP)	<input type="text" value="12000"/>	Battery State for an AP	<input checked="" type="checkbox"/>
Multicast Mode	<input type="text" value="In-Out"/>	Full sector DFS status	<input checked="" type="checkbox"/>
IDS (Rogue/Signature Detection)	<input type="checkbox"/>		
Convergence Method	<input type="text" value="Standard"/>		
Background Scanning	<input type="checkbox"/>		
Channel Change Notification	<input type="checkbox"/>		
LSC	<input type="checkbox"/>		

Klicken Sie auf das erstellte Mesh-Profil, um die allgemeinen und erweiterten Einstellungen für das Mesh-Profil zu bearbeiten.


Wie im Diagramm gezeigt, müssen wir das zuvor erstellte Authentifizierungs- und Autorisierungsprofil dem Mesh-Profil zuordnen.







**Schritt 5:** Erstellen eines neuen Zugangsprofils für den Access Point Gehen Sie zu **Konfigurieren > Tags und Profile: AP Join**.


Search Menu Items

 Dashboard

 Monitoring >

 Configuration >

 Administration >

 Troubleshooting

 Interface

Logical  
Ethernet  
Wireless

 Layer2

VLAN  
VTP

 Radio Configurations

CleanAir  
High Throughput  
Media Parameters

Network  
Parameters  
RRM

 Routing Protocols

OSPF  
Static Routing

 Security

AAA  
ACL

 Services

AireOS C  
Applicatio  
Cloud Se  
Custom A  
IOx  
mDNS  
Multicast  
NetFlow  
Python S  
QoS  
RA Throt

 Tags & Profiles

AP Join  
Flex  
Policy  
RF  
Tags  
WLANs

 Wireless

Access P

Configuration > Tags & Profiles > AP Join

+ Add    - Delete

AP Join Profile Name	Description
<input type="checkbox"/> default-ap-profile	default ap profile

### Add AP Join Profile

General    Client    CAPWAP    AP    Management    Rogue AP    ICap

Name\*    Mesh\_AP\_Join\_Profile

Description    Enter Description

LED State   

LAG Mode   

NTP Server    0.0.0.0

Cancel

Wenden Sie das zuvor konfigurierte Mesh-Profil an, und konfigurieren Sie die AP-EAP-Authentifizierung:

AP Join Profile Name	Description
<input type="checkbox"/> default-ap-profile	default ap profile

### Add AP Join Profile

General Client CAPWAP **AP** Management Rogue AP ICap

**General** Hyperlocation BLE Packet Capture

**Power Over Ethernet**

Switch Flag

Power Injector State

Power Injector Type

Injector Switch MAC

Code

**AP EAP Auth Configuration**

EAP Type

AP Authorization Type

**Client Statistics Reporting Interval**

5 GHz (sec)

2.4 GHz (sec)

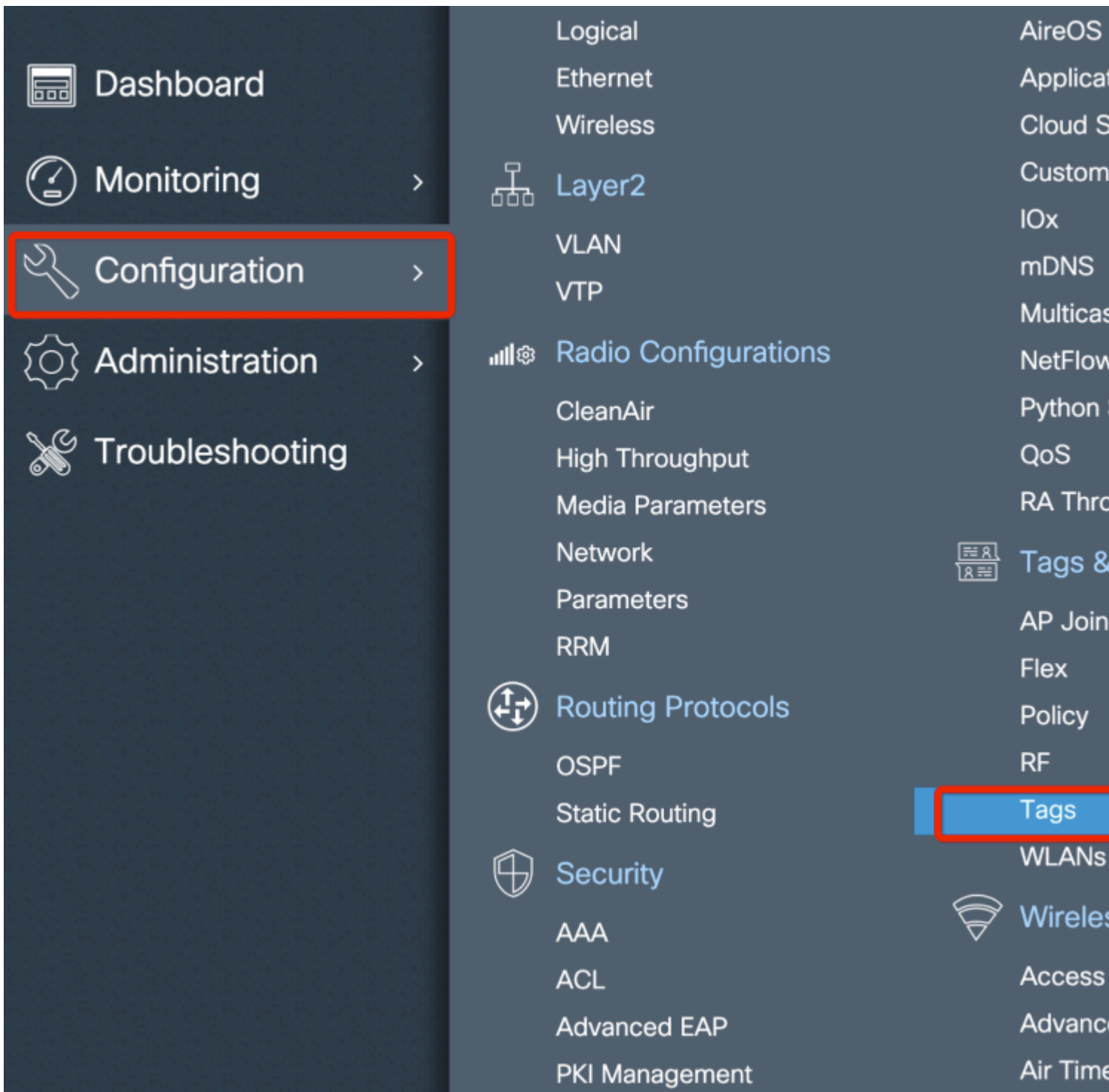
**Extended Module**

Enable

**Mesh**

Profile Name

**Schritt 6:** Erstellen Sie eine Mesh-Standort-Tag wie abgebildet.



Konfigurieren Klicken Sie auf das in Schritt 6 erstellte Mesh-Standort-TAG, um es zu konfigurieren.

Wechseln Sie zur Registerkarte "Site", und wenden Sie das zuvor konfigurierte Mesh AP-Join-Profil an:

Configuration > Tags & Profiles > Tags

Policy **Site** RF AP

+ Add - Delete

### Add Site Tag

Name\* Mesh\_AP\_tag

Description Enter Description

AP Join Profile Mesh\_AP\_Join\_Profi

Control Plane Name

Enable Local Site

Cancel

**Schritt 7.** Konvertieren Sie den AP in den Bridge-Modus.

Configuration > Wireless > Access Points

All Access Points

Number of AP(s): 1

AP Name	AP Model	Slots	Admin Status	IP Address
AP2C33-110E-6B66	AIR-AP1562E-E-K9	2	<span style="color: green;">✔</span>	109.129.49.9

1 10 items per page

- 5 GHz Radios
- 2.4 GHz Radios
- Dual-Band Radios

### Edit AP

General Interfaces High Availability Inventory

General

AP Name\* AP2C33-110E-6B66

Location\* default location

Base Radio MAC 7070.8bb4.9200

Ethernet MAC 2c33.110e.6b66

Admin Status **ENABLED**

AP Mode Bridge

Operation Status

Fabric Status

LED State

Über die CLI kann der folgende Befehl auf dem Access Point ausgeführt werden:

capwap ap mode bridge

Der Access Point wird neu gestartet und als Bridge-Modus wieder verbunden.

**Schritt 8:** Sie können jetzt die Rolle des Access Points definieren: entweder Root-Access Point oder Mesh-Access Point.

Der Root-AP ist derjenige mit einer verdrahteten Verbindung zum WLC, während der Mesh-AP über seine Funkeinheit mit dem WLC verbunden ist, die versucht, eine Verbindung zu einem Root-AP herzustellen.

Ein Mesh-AP kann dem WLC über seine verdrahtete Schnittstelle beitreten, wenn er zu Bereitstellungszwecken keinen Root-AP über seine Funkverbindung gefunden hat.

Configuration > Wireless > Access Points

All Access Points

Number of AP(s): 1

AP Name	AP Model	Slots	Admin Status	IP Address
AP2C33-110E-6B66	AIR-AP1562E-E-K9	2	✓	109.129.49.9

5 GHz Radios

2.4 GHz Radios

Dual-Band Radios

Country

LSC Provision

Edit AP

General

Interfaces

High Availability

Inventory

Mesh

General

Block Child

Daisy Chaining

Daisy Chaining strict-RAP

Preferred Parent MAC

VLAN Trunking Native

Role   
Mesh  
Root  
Mesh

Remove PSK

Backhaul

Backhaul Radio Type

Backhaul Slot ID

Rate Types

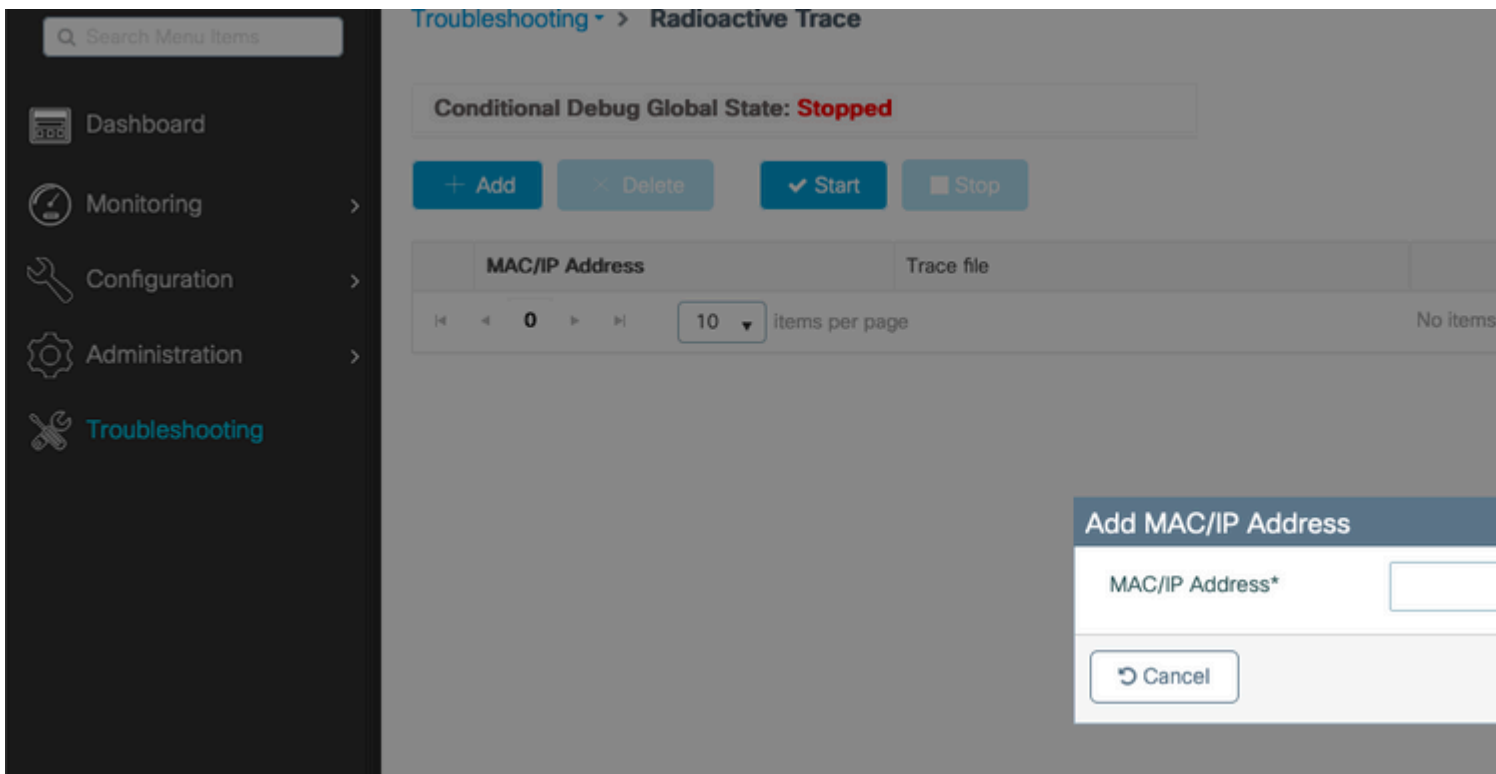
## Überprüfung

```
aaa new-model
aaa local authentication default authorization default
!
!
aaa authentication dot1x default local
```

```
aaa authentication dot1x Mesh_Authentication local
aaa authorization network default local
aaa authorization credential-download default local
aaa authorization credential-download Mesh_Authz local
username 111122223333 mac
wireless profile mesh Mesh_Profile
  method authentication Mesh_Authentication
  method authorization Mesh_Authz
wireless profile mesh default-mesh-profile
  description "default mesh profile"
wireless tag site Mesh_AP_Tag
  ap-profile Mesh_AP_Join_Profile
ap profile Mesh_AP_Join_Profile
  hyperlocation ble-beacon 0
  hyperlocation ble-beacon 1
  hyperlocation ble-beacon 2
  hyperlocation ble-beacon 3
  hyperlocation ble-beacon 4
  mesh-profile Mesh_Profile
```

## Fehlerbehebung

Klicken Sie auf der Webseite **Troubleshoot > Radioactive Trace (Fehlerbehebung > Radioaktive Trace)** auf **Hinzufügen**, und geben Sie die MAC-Adresse des Access Points ein.



The screenshot shows the 'Radioactive Trace' interface. The sidebar on the left contains navigation links: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main area displays the 'Radioactive Trace' section with a 'Conditional Debug Global State: Stopped' indicator. Below this are buttons for '+ Add', 'Delete', 'Start', and 'Stop'. A table with columns 'MAC/IP Address' and 'Trace file' is visible, showing 0 items per page. A modal window titled 'Add MAC/IP Address' is open, featuring a text input field for 'MAC/IP Address\*' and a 'Cancel' button.

Klicken Sie auf **Start**, und warten Sie, bis der Access Point erneut versucht, dem Controller beizutreten.

Klicken Sie anschließend auf **Generate (Erstellen)**, und wählen Sie einen Zeitraum für die Protokollerfassung aus (z. B. die letzten 10 oder 30 Minuten).

Klicken Sie auf den Namen der Trace-Datei, um sie von Ihrem Browser herunterzuladen.

Das folgende Beispiel zeigt einen AP, der nicht beigetreten ist, weil ein falscher AAA-



Autorisierungsmethodenname definiert wurde:

```
2019/11/28 13:08:38.269 {wncd_x_R0-0}{1}: [capwapac-smgr-srvr] [23388]: (info): Session-IP: 192.168.88.4
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [23388]: (info): DTLS record type: 23, applic
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess] [23388]: (info): Session-IP: 192.168.88.4
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess] [23388]: (info): Session-IP: 192.168.88.4
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [mesh-config] [23388]: (ERR): Failed to get ap PMK cache rec s
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [mesh-config] [23388]: (ERR): Failed to get ap PMK cache rec s
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [mesh-config] [23388]: (ERR): Failed to get ap PMK cache rec s
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-capwap-join] [23388]: (info): 00a3.8e95.6c40 Ap auth pe
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-capwap-join] [23388]: (ERR): Failed to initialize autho
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-capwap-join] [23388]: (ERR): 00a3.8e95.6c40 Auth reques
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-db] [23388]: (ERR): 00a3.8e95.6c40 Failed to get wtp re
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-db] [23388]: (ERR): 00a3.8e95.6c40 Failed to get ap tag
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess-fsm] [23388]: (ERR): Session-IP: 192.168.8
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess-fsm] [23388]: (info): Session-IP: 192.168.
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess-fsm] [23388]: (note): Session-IP: 192.168.
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess-fsm] [23388]: (note): Session-IP: 192.168.
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [ewlc-dtls-sessmgr] [23388]: (info): Remote Host: 192.168.88.4
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [ewlc-dtls-sessmgr] [23388]: (info): Remote Host: 192.168.88.4
2019/11/28 13:08:38.289 {wncmgrd_R0-0}{1}: [ewlc-infra-evq] [23038]: (debug): instance :0 port:38932MAC.
```

Dasselbe lässt sich einfacher im Dashboard der Webbenutzeroberfläche erkennen, wenn Sie auf APs klicken, die nicht beigetreten sind. Der Hinweis "AP auth pending" deutet auf die Authentifizierung des AP selbst hin:

General **Join Statistics**

[Clear](#) [ClearAll](#)

Number of AP(s): 2

Status "Is equal to" NOT JOINED ✕

AP Name	AP Mod
<input type="checkbox"/> AP2CF8-9B5F-7D70	C9120A
<input type="checkbox"/> NA	

1 items per page

**Join Statistics**

General **Statistics**

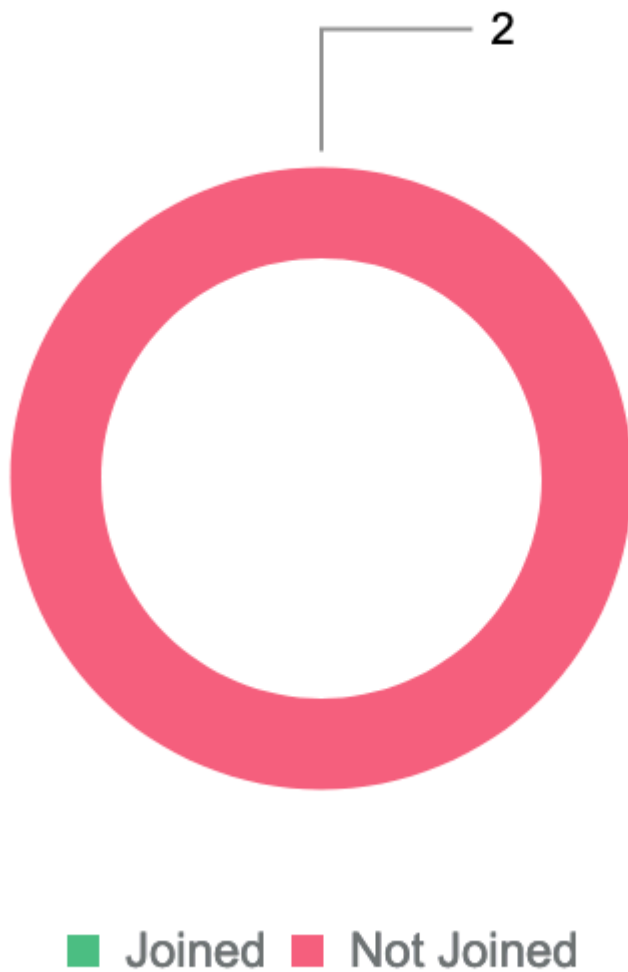
DTLS Session request received	1	Configuration
Established DTLS session	1	Successful co responses se
Unsuccessful DTLS session	0	Unsuccessful request proces
Reason for last unsuccessful DTLS session	DTLS Handshake Success	Reason for las configuration
Time at last successful DTLS session	Mon, 17 Feb 2020 09:15:41 GMT	Time at last s configuration
Time at last unsuccessful DTLS session	NA	Time at last u configuration

**Join phase statistics**

Join requests received	1	Data DTLS S
Successful join responses sent	0	DTLS Session
Unsuccessful join request processing	0	Established D
Reason for last unsuccessful join attempt	Ap auth pending	Unsuccessful
Time at last successful join attempt	NA	Reason for las DTLS session
Time at last unsuccessful join attempt	NA	Time at last s session
		Time at last u session

---

## Access Point Join Summary



---

### Anwenderbericht 2: Flex + Bridge

In diesem Abschnitt wird der Join-Prozess eines 1542 AP im Flex+Bridge-Modus mit lokaler EAP-Authentifizierung auf dem WLC beschrieben.

#### Konfigurieren

- Schritt 1: Navigieren Sie zu **Configuration > Security > AAA > AAA Advanced > Device Authentication**.

Configuration > Security > AAA (1)

+ AAA Wizard

Servers / Groups    AAA Method List    **AAA Advanced** (2)

Global Config

RADIUS Fallback

Attribute List Name

**Device Authentication** (3)

+ Add (4)    × Delete

MAC Address

002cc8de2b40

- Schritt 2: Wählen Sie **Geräteauthentifizierung** und dann **Hinzufügen aus**.
- Schritt 3: Geben Sie die Base Ethernet MAC-Adresse des AP ein, der dem WLC beitreten soll, lassen Sie das Feld **Attributlistenname** leer, und wählen Sie **Auf Gerät anwenden aus**.

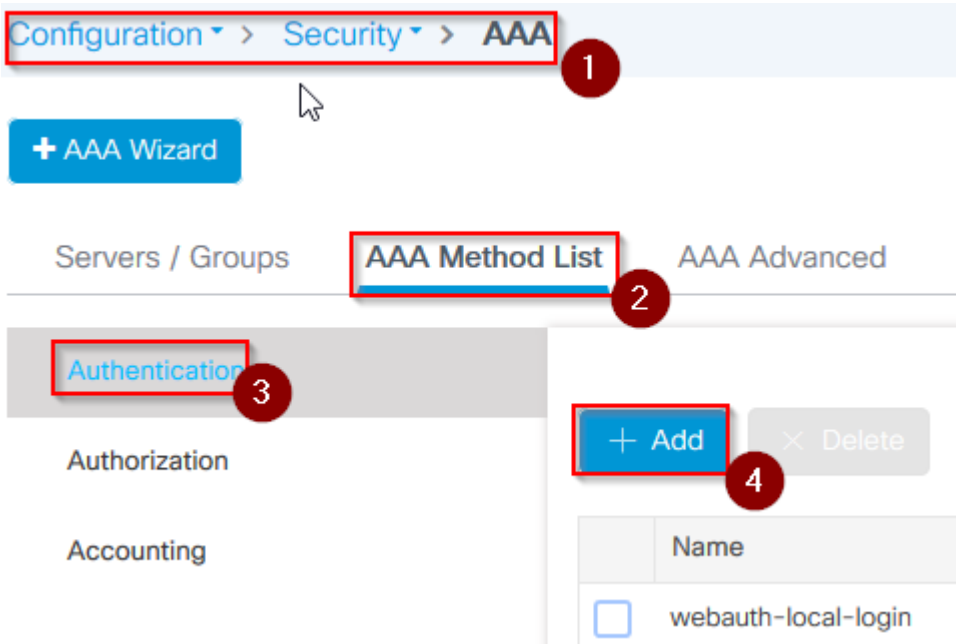
Quick Setup: MAC Filtering

MAC Address\* (1)    ffffffff

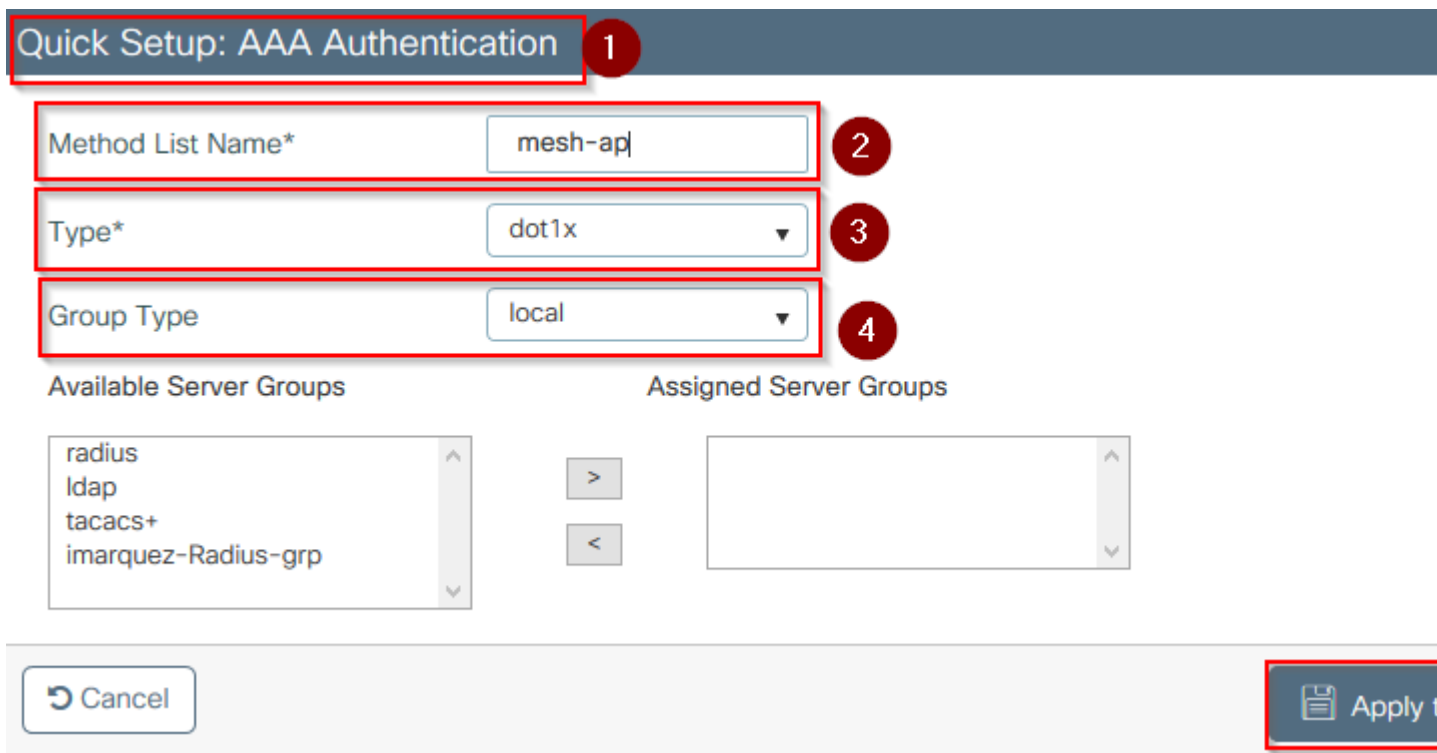
Attribute List Name (2)    None

Cancel

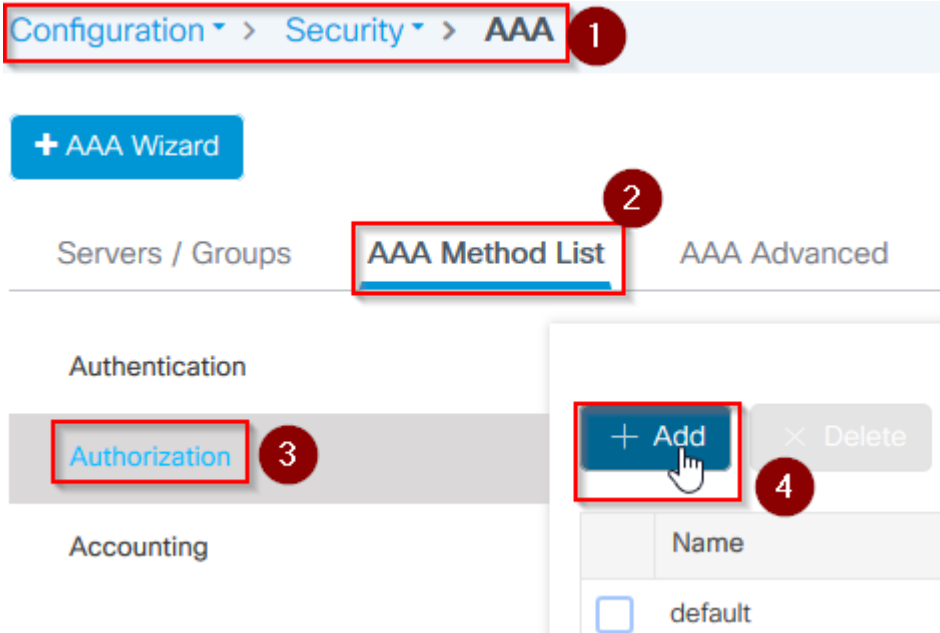
- Schritt 4: Navigieren Sie zu **Konfiguration > Sicherheit > AAA > AAA-Methodenliste > Authentifizierung**
- Schritt 5: Wählen Sie **Hinzufügen**, um das Popup-Fenster **AAA Authentication (AAA-Authentifizierung)** zu öffnen.



- Schritt 6: Geben Sie einen Namen in das Feld Methodenlistenname ein, wählen Sie 802.1x aus dem **Typ\***-Dropdown-Menü und **lokal** für den **Gruppentyp** aus, und wählen Sie schließlich die Option Auf Gerät anwenden aus.



- Schritt 6b. Falls Ihre APs direkt als Bridge-Modus beitreten und ihnen zuvor kein Standort- und Richtlinien-Tag zugewiesen wurde, wiederholen Sie Schritt 6, jedoch für die Standardmethode.
- Konfigurieren einer dot1x aaa-Authentifizierungsmethode, die auf lokal verweist (CLI aaa authentication dot1x default local)
- Schritt 7. Navigieren Sie zu **Konfiguration > Sicherheit > AAA > AAA-Methodenliste > Autorisierung**
- Schritt 8: Wählen Sie **Hinzufügen**, um das Popup-Fenster **AAA-Autorisierung** anzuzeigen.



- Schritt 9. Geben Sie einen Namen in das Feld Name der Methodenliste ein, wählen Sie im Dropdown-Menü **Type\*** die Option Credentials Download aus und **lokal** für den **Gruppentyp**, und wählen Sie schließlich die Option Auf Gerät anwenden aus.

### Quick Setup: AAA Authorization

Method List Name\*  1

Type\*  2

Group Type  3

Authenticated

Available Server Groups

Assigned Server Groups

- Schritt 9b: Wenn Ihr AP direkt im Bridge-Modus beitrifft (d. h. er tritt nicht zuerst im lokalen Modus bei), wiederholen Sie Schritt 9 für die Standardmethode zum Herunterladen von Anmeldeinformationen (CLI aaa Authorization Credential-Download default local).
- Schritt 10. Navigieren Sie zu **Konfiguration > Wireless > Mesh > Profile**.
- Schritt 11. Wählen Sie **Hinzufügen**, um das Pop-up-Fenster **Netzprofil hinzufügen** anzuzeigen.

Configuration > Wireless > Mesh

1

Global Config

Profiles

2

+ Add

× Delete

3

- Schritt 12: Legen Sie auf der Registerkarte **Allgemein** einen Namen und eine Beschreibung für das Mesh-Profil fest.

## Add Mesh Profile

General

Advanced

Name\*

mesh-profile

Description

mesh-profile

- Schritt 13: Wählen Sie auf der Registerkarte **Erweitert** die Option **EAP** für das Feld **Methode aus**.
- Schritt 14: Wählen Sie das in den Schritten 6 und 9 definierte **Autorisierungs-** und **Authentifizierungsprofil aus**, und wählen Sie **Auf Gerät anwenden aus**.

## Add Mesh Profile

General

**Advanced**

1

### Security

Method

EAP

2

Authentication Method

mesh-ap

3

Authorization Method

mesh-ap|

4

### 5 GHz Band Backhaul

Rate Types

### 2.4 GHz Band Backhaul

Rate Types

### Ethernet Bridging

VLAN Transparent

Ethernet Bridging

### Bridge Group

Bridge Group Name

Enter Name

Strict Match

Cancel

- Schritt 15: Navigieren Sie zu **Konfiguration > Tag & Profiles > AP Join > Profile**.
- Schritt 16: Wählen Sie **Hinzufügen aus**, das Popup-Fenster "AP Join Profile" wird angezeigt, legen Sie einen Namen und eine Beschreibung für das AP Join-Profil fest.

Configuration > Tags & Profiles > AP Join

1

+ Add

× Delete

2

AP Join Profile Name



## Add AP Join Profile

General	Client	CAPWAP	AP	Management	Rogue AP	ICap
Name*	<input type="text" value="mes-ap-join"/>					
Description	<input type="text" value="mesh-ap-join"/>					
LED State	<input checked="" type="checkbox"/>					
LAG Mode	<input type="checkbox"/>					
NTP Server	<input type="text" value="0.0.0.0"/>					

- Schritt 17: Navigieren Sie zur Registerkarte **AP**, und wählen Sie das in Schritt 12 erstellte **Mesh-Profil** aus dem Dropdown-Menü **Mesh Profile Name (Netzprofilname)** aus.
- Schritt 18: Stellen Sie sicher, dass **EAP-FAST**- und **CAPWAP-DTLS** für die Felder **EAP Type (EAP-Typ)** und **AP Authorization Type (AP-Autorisierungstyp)** festgelegt sind.
- Schritt 19: Wählen Sie **Auf Gerät anwenden** aus.

## Add AP Join Profile

General Client CAPWAP **AP** Management Rogue AP ICap

**General** Hyperlocation BLE Packet Capture

**Power Over Ethernet**

Switch Flag

Power Injector State

Power Injector Type Unknown ▾

Injector Switch MAC 00:00:00:00:00:00

Code

**AP EAP Auth Configuration**

EAP Type EAP-FAST ▾

AP Authorization Type CAPWAP DTLS ▾

**Client Statistics Reporting Interval**

5 GHz (sec) 90

2.4 GHz (sec) 90

**Extended Module**

Enable

**Mesh**

Profile Name mesh-p

Cancel

- Schritt 20: Navigieren Sie zu **Konfiguration** > **Tag & Profile** > **Tags** > **Site**.
- Schritt 21: Wählen Sie **Hinzufügen**, um das Popup-Fenster "Site-Tag" anzuzeigen.

Configuration ▾ > Tags & Profiles ▾ > **Tags**

Policy **Site** RF AP

+ Add Delete

- Schritt 22: Geben Sie einen Namen und eine Beschreibung für das Site-Tag ein.

**Add Site Tag** 1

Name\* mesh-ap-site

Description mesh-ap-site

AP Join Profile mesh-ap-join-profile 2

- Schritt 23: Wählen Sie das in Schritt 16 erstellte **AP-Join-Profil** aus der Dropdown-Liste **AP-Join-Profil** aus.
- Schritt 24: Deaktivieren Sie unten im Popup-Fenster "Site-Tag" das Kontrollkästchen "**Lokalen Standort aktivieren**", um das Dropdown-Menü "**Flex Profile**" zu aktivieren.
- Schritt 35: Wählen Sie im Dropdown-Menü **Flex Profile (Flex-Profil)** das **Flex Profile (Flex-Profil)** aus, das Sie für den AP verwenden möchten.

**Add Site Tag**

Name\* mesh-ap-site

Description mesh-ap-site

AP Join Profile mesh-ap-join-profile

Flex Profile imarquez-FlexLocal 2

Control Plane Name

Enable Local Site  1

Cancel

- Schritt 36: Verbinden Sie den Access Point mit dem Netzwerk, und stellen Sie sicher, dass sich der Access Point im lokalen Modus befindet.
- Schritt 37: Um sicherzustellen, dass sich der Access Point im lokalen Modus befindet, geben Sie den Befehl **capwap ap mode local ein**.

Der Access Point muss über eine Suchmöglichkeit für den Controller verfügen (L2-Broadcast, DHCP-Option 43, DNS-Auflösung oder manuelle Einrichtung).

- Schritt 38: Der AP wird Mitglied des WLC. Stellen Sie sicher, dass er in der AP-Liste aufgeführt ist, und navigieren Sie zu **Configuration > Wireless > Access Points > All Access Points**.

## ▼ All Access Points

Number of AP(s): 2

AP Name	Total Slots	Admin Status	AP Model	Base Radio MAC	AP Mode
[blurred]	2	✓	[blurred]	[blurred]	Flex+Bridge
[blurred]	2	✓	[blurred]	[blurred]	Local

- Schritt 39: Wählen Sie den Access Point aus, und das **AP**-Popup wird angezeigt.
- Schritt 40: Wählen Sie die in Schritt 22 erstellte **Site-Tag-Nummer** unter **Allgemein > Tags > Site-**Registerkarte im AP-Popup-Fenster aus, und wählen Sie die Option "**Auf Gerät anwenden**" aus.

## Edit AP

General

1

Interfaces

High Availability

Inventory

Mesh

Advanced

### General

AP Name\*

Location\*

Base Radio MAC

Ethernet MAC

Admin Status  ENABLED

AP Mode

Operation Status Registered

Fabric Status Disabled

LED State  ENABLED

LED Brightness Level

CleanAir [NSI Key](#)

### Tags

Policy

Site

RF

### Version

Primary Software Version 16.12.1.13

Predownloaded Status N/A

Predownloaded Version N/A

Next Retry Time N/A

Boot Version 1.1.2.4

IOS Version 16.12.1.13

Mini IOS Version 0.0.0.0

### IP Config

CAPWAP Preferred Mode IPv4

DHCP IPv4 Address

Static IP (IPv4/IPv6)

### Time Statistics

Up Time 4 da mins

Controller Association Latency 20 s

- Schritt 41: Der AP wird neu gestartet und muss den WLC im Flex + Bridge-Modus wieder verbinden.

Beachten Sie, dass diese Methode dem Access Point zuerst im lokalen Modus beitrifft (wobei keine Punkt1x-Authentifizierung erfolgt), um das Site-Tag auf das Mesh-Profil anzuwenden und dann den Access Point in den Bridge-Modus umzuschalten.

Um einem Access Point beizutreten, der im Bridge-Modus (oder Flex+Bridge) feststeckt, konfigurieren Sie Standardmethoden (**aaa authentication dot1x default local** und **aaa authentication cred default local**).

Der Access Point kann sich dann authentifizieren, und Sie können die Tags anschließend zuweisen.

## Überprüfung

Stellen Sie sicher, dass der AP-Modus "Flex + Bridge" (Flex + Bridge) angezeigt wird, wie in dieser Abbildung gezeigt.

Configuration > Wireless > Access Points

### All Access Points

Number of AP(s): 2

AP Name	Total Slots	Admin Status	AP Model	Base Radio MAC	AP Mode
	2	✓	AIR-AP1542I-A-K9		Flex+Bridge

Führen Sie diese Befehle in der WLC 9800 CLI aus, und suchen Sie nach dem Attribut **AP Mode**. Sie muss als **Flex+Bridge** aufgeführt sein.

```
aaa authorization credential-download mesh-ap local
aaa authentication dot1x mesh-ap local
wireless profile mesh default-mesh-profile
  description "default mesh profile"
wireless tag site meshsite
  ap-profile meshapjoin
  no local-site
ap profile meshapjoin
  hyperlocation ble-beacon 0
  hyperlocation ble-beacon 1
  hyperlocation ble-beacon 2
  hyperlocation ble-beacon 3
  hyperlocation ble-beacon 4
mesh-profile mesh-profile
```

## Fehlerbehebung

Stellen Sie sicher, dass die Befehle **aaa authentication dot1x default local** und **aaa authentication cred default local** vorhanden sind. Sie sind erforderlich, wenn Ihr Access Point im lokalen Modus nicht vorab verbunden wurde.

Das Haupt-Dashboard der Serie 9800 verfügt über ein Widget, über das APs angezeigt werden, die nicht beitreten können. Klicken Sie hier, um eine Liste der APs anzuzeigen, die nicht beitreten können:

General **Join Statistics**[Clear](#) [ClearAll](#)

Number of AP(s): 2

Status \*is equal to\* NOT JOINED x

	Status	Base Radio MAC	Ethernet MAC	AP Name
<input type="checkbox"/>	+	10b3.c622.5d80	2cf8.9b21.18b0	AP2CF8.9B21.18B0
<input type="checkbox"/>	+	7070.8bb4.9200	2c33.110e.6b66	AP2C33.110E.6B66

1 10 items per page

Klicken Sie auf den jeweiligen Access Point, um den Grund anzuzeigen, warum er nicht beigetreten ist. In diesem Fall tritt ein Authentifizierungsproblem auf (die AP-Authentifizierung steht aus), da das Site-Tag nicht dem AP zugewiesen wurde.

Daher hat der 9800 nicht die benannte Authentifizierungs-/Autorisierungsmethode ausgewählt, um den AP zu authentifizieren:

## Join Statistics

General

**Statistics**

### Control DTLS Statistics

DTLS Session request received	179
Established DTLS session	179
Unsuccessful DTLS session	0
Reason for last unsuccessful DTLS session	DTLS Handshake Success
Time at last successful DTLS session	Thu, 19 Dec 2019 13:03:19 GMT
Time at last unsuccessful DTLS session	NA

### Join phase statistics

Join requests received	179
Successful join responses sent	173
Unsuccessful join request processing	0
Reason for last unsuccessful join attempt	Ap auth pending
Time at last successful join attempt	Thu, 19 Dec 2019 12:36:10 GMT
Time at last unsuccessful join attempt	NA

### Configuration phase statistics

Configuration requests received
Successful configuration responses sent
Unsuccessful configuration request processing
Reason for last unsuccessful configuration attempt
Time at last successful configuration attempt
Time at last unsuccessful configuration attempt

### Data DTLS Statistics

DTLS Session request received
Established DTLS session
Unsuccessful DTLS session
Reason for last unsuccessful DTLS session
Time at last successful DTLS session
Time at last unsuccessful DTLS session

Weitere Informationen zur erweiterten Fehlerbehebung finden Sie auf der Seite **Troubleshooting > Radioactive Trace (Fehlerbehebung > Radioaktive Ablaufverfolgung)** in der Webbenutzeroberfläche.

Wenn Sie die MAC-Adresse des AP eingeben, können Sie sofort eine Datei erstellen, um die stets verfügbaren Protokolle (auf Benachrichtigungsebene) des AP abzurufen, der beitreten möchte.

Klicken Sie auf **Start**, um das erweiterte Debuggen für diese MAC-Adresse zu aktivieren. Wenn die Protokolle das nächste Mal generiert werden, werden die Protokolle generiert und Protokolle auf Debugebene für den AP-Beitritt angezeigt.





Search Menu Items



Dashboard



Monitoring



Configuration



Administration



Troubleshooting

Troubleshooting > Radioactive Trace

[← Back to Troubleshooting Menu](#)

Conditional Debug Global State: **Stopped**

+ Add

× Delete

✓ Start

■ Stop

	MAC/IP Address	Trace file
<input type="checkbox"/>	2c33.110e.6b66	debugTrace_2c33.110e.6b66.txt <a href="#">↓</a>

⏪ < 1 > ⏩ 10 items per page

## 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.