

Configuration du maillage sur les contrôleurs LAN sans fil Catalyst 9800

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Étude de cas 1 : mode pont](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérifier](#)

[Dépannage](#)

[Étude de cas 2 : Flex + Bridge](#)

[Configurer](#)

[Vérifier](#)

[Dépannage](#)

Introduction

Ce document décrit un exemple de configuration de base sur la façon de joindre un point d'accès maillé au contrôleur LAN sans fil (WLC) Catalyst 9800

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Modèle de configuration Catalyst Wireless 9800
- Configuration des LAP
- Contrôle et fourniture de points d'accès sans fil (CAPWAP)
- Configuration d'un serveur DHCP externe
- Configuration des commutateurs Cisco

Composants utilisés

Cet exemple utilise un point d'accès léger (1572AP et 1542) qui peut être configuré en tant que point d'accès racine (RAP) ou point d'accès maillé (MAP) pour se connecter au WLC Catalyst 9800. La procédure est identique pour les points d'accès 1542 ou 1562. Le RAP est connecté au WLC Catalyst 9800 via un commutateur Cisco Catalyst.

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

- C9800-CL v16.12.1
- Commutateur de couche 2 Cisco
- Points d'accès extérieurs légers de la gamme Cisco Aironet 1572 pour la section Bridge
- Cisco Aironet 1542 pour la section Flex+Bridge

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

Étude de cas 1 : mode pont

Diagramme du réseau

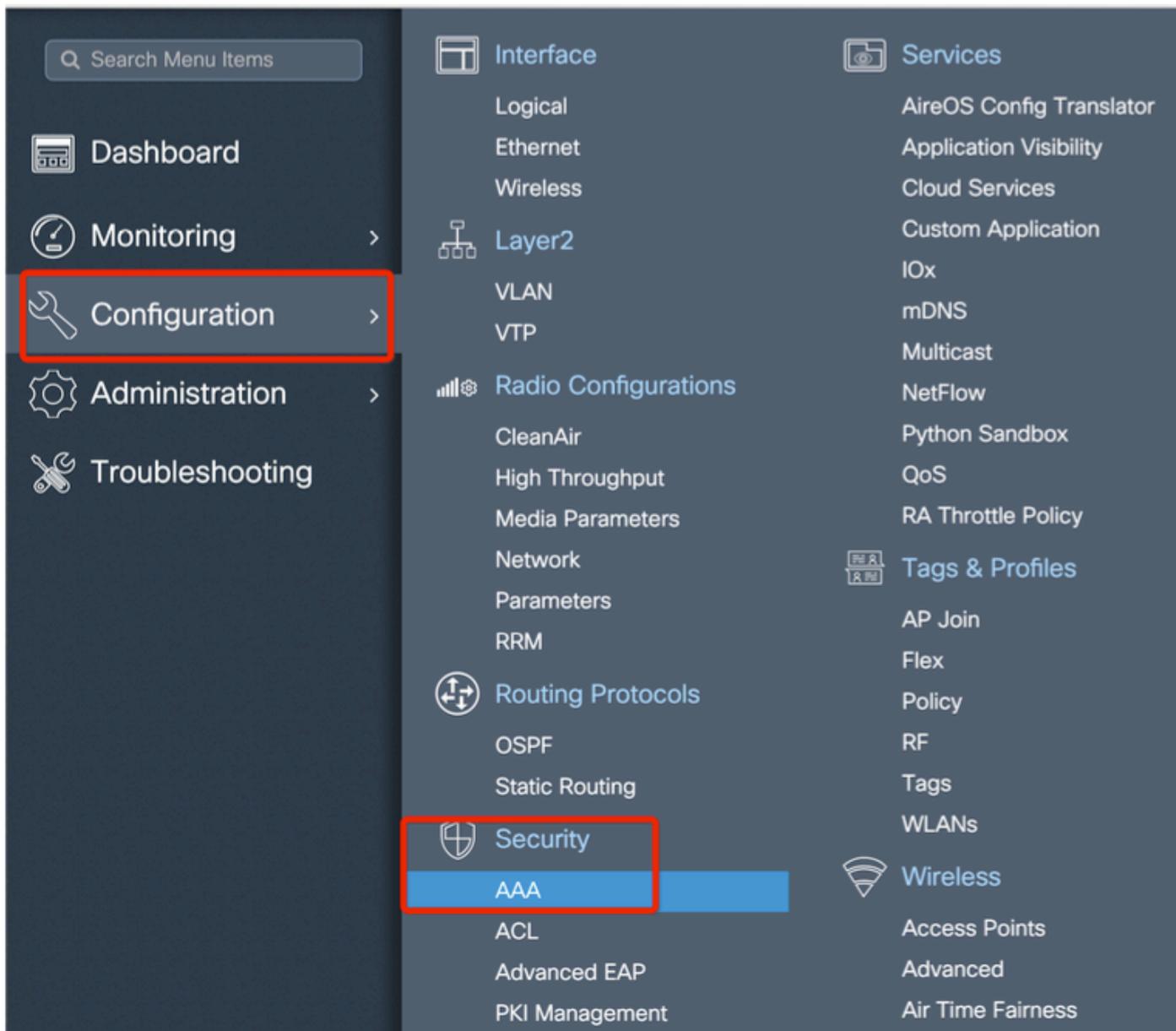
Configurations

Un point d'accès maillé doit être authentifié pour qu'il rejoigne le contrôleur 9800. Cette étude de cas considère que vous joignez l'AP en mode local d'abord au WLC, puis le convertissez en mode maillé Bridge (alias).

Pour éviter l'attribution de profils de jointure AP, utilisez cet exemple mais configurez la méthode de téléchargement d'informations d'identification d'autorisation aaa par défaut de sorte que tout AP maillé soit autorisé à joindre le contrôleur.

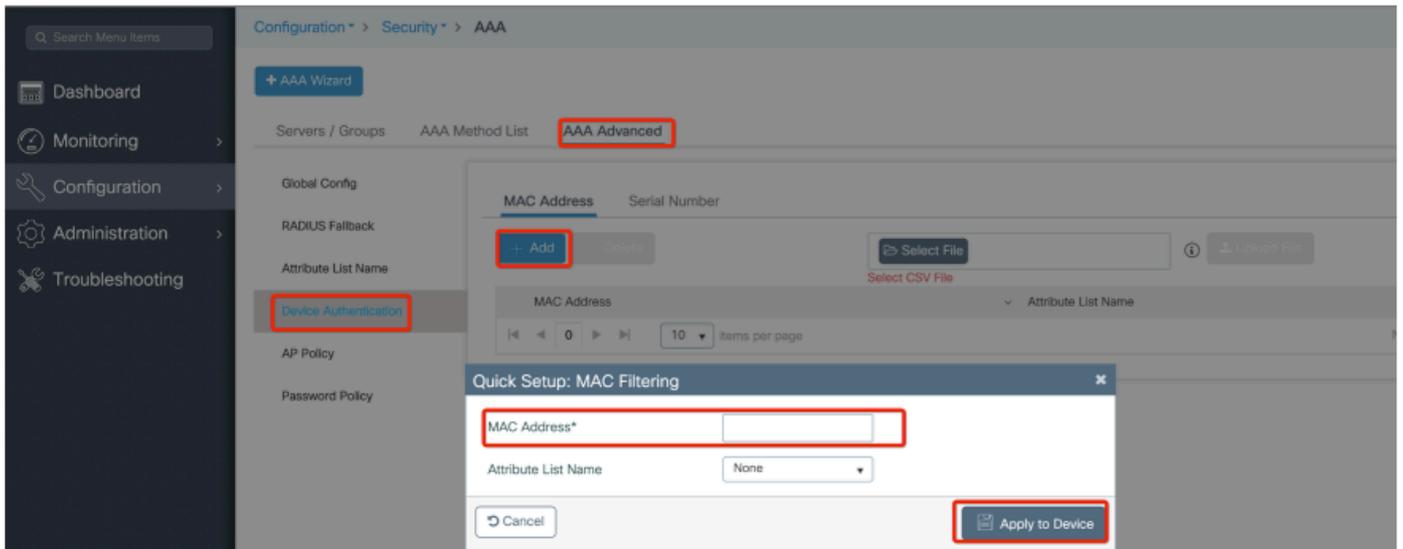
Étape 1 : configurez les adresses MAC RAP/MAP sous Device Authentication.

Accédez à Configuration > AAA > AAA Advanced > Device Authentication .



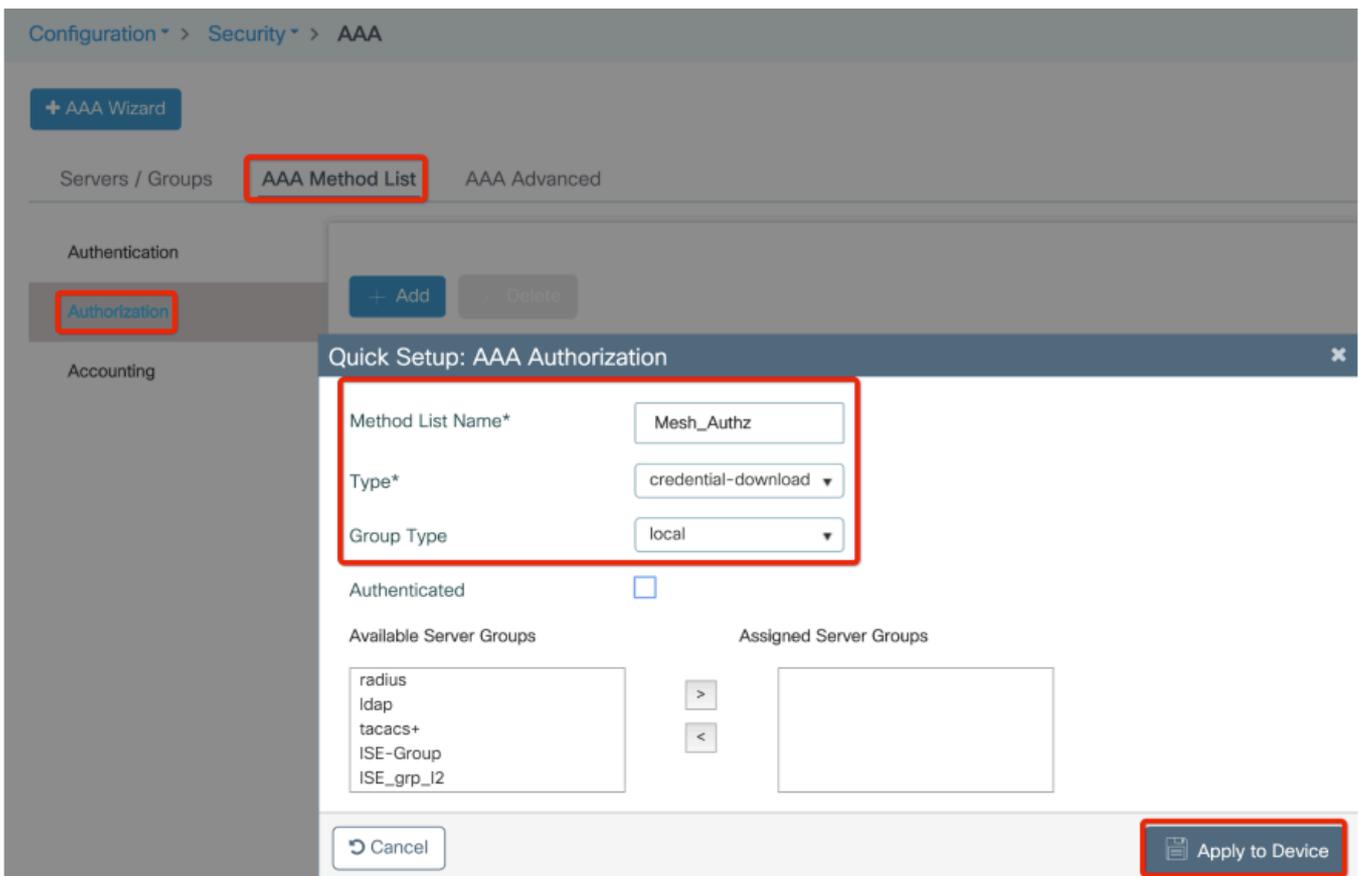
Ajoutez l'adresse MAC Ethernet de base des points d'accès maillés, sans caractères spéciaux, sans point (.) ni point (:)

 Important : à partir de la version 17.3.1, iSi des délimiteurs d'adresse MAC tels que '!', ': ' ou '-' sont ajoutés, l'AP ne peut pas se joindre. Il y a actuellement 2 améliorations ouvertes pour ceci : [ID de bogue Cisco CSCvv43870](#) et ID de bogue Cisco [CSCvr07920](#). À l'avenir, le 9800 accepte tous les formats d'adresse MAC.



Étape 2 : Configurez la liste des méthodes d'authentification et d'autorisation.

Accédez à Configuration > Security > AAA > AAA Method list > Authentication et créez la liste de méthodes d'authentification et la liste de méthodes d'autorisation.



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

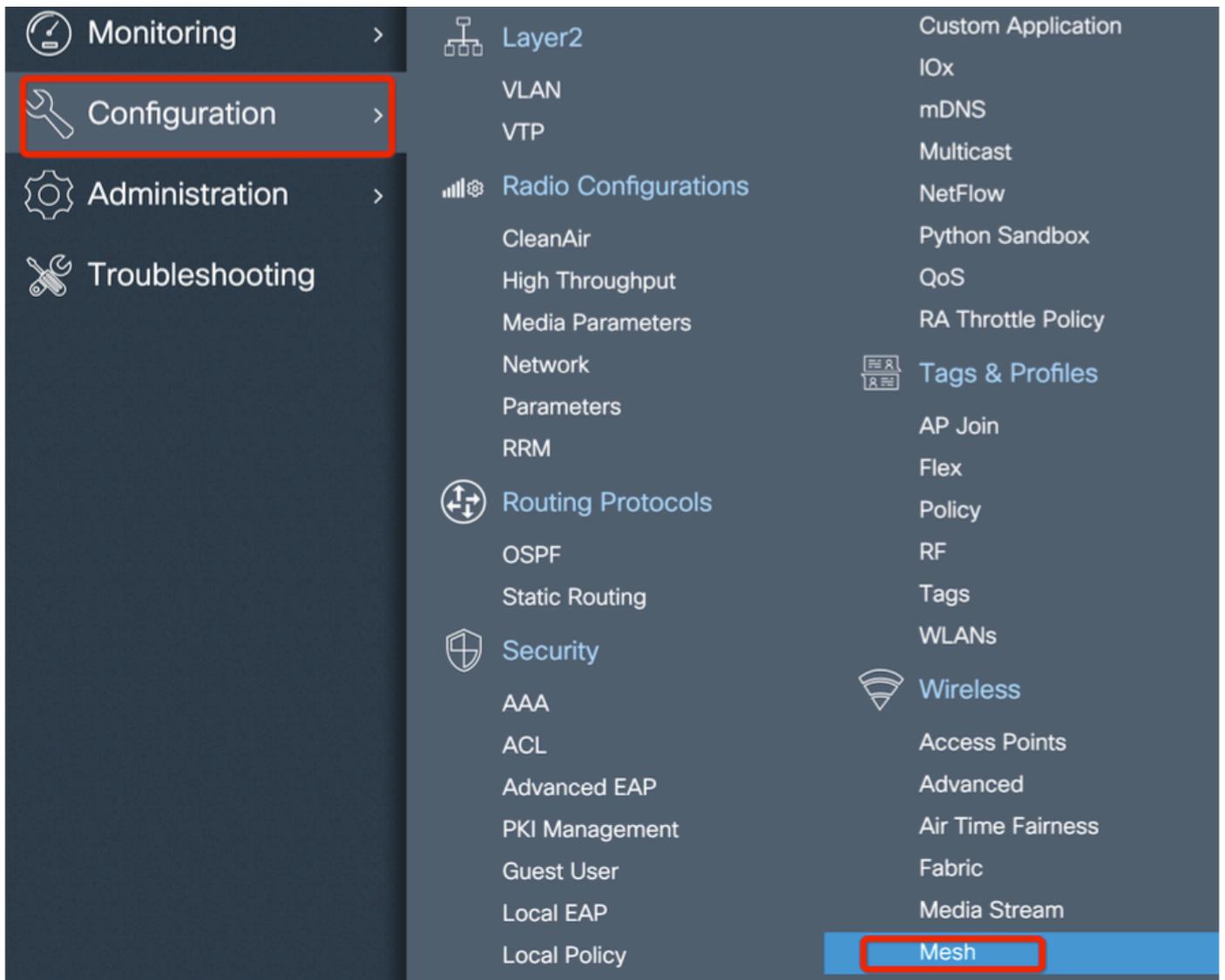
radius
ldap
tacacs+
ISE-Group
ISE_grp_I2

>
<

Cancel Apply to Device

Étape 3 : Configurez les paramètres de maillage global.

Accédez à Configuration> Maillage> Paramètres globaux. Au départ, nous pouvons conserver ces valeurs par défaut.



Étape 4 : Créez un nouveau profil de maillage sous Configuration > Mesh > Profile > +Add

Global Config **Profiles**

+ Add Delete

Number of Profiles : 1

Add Mesh Profile

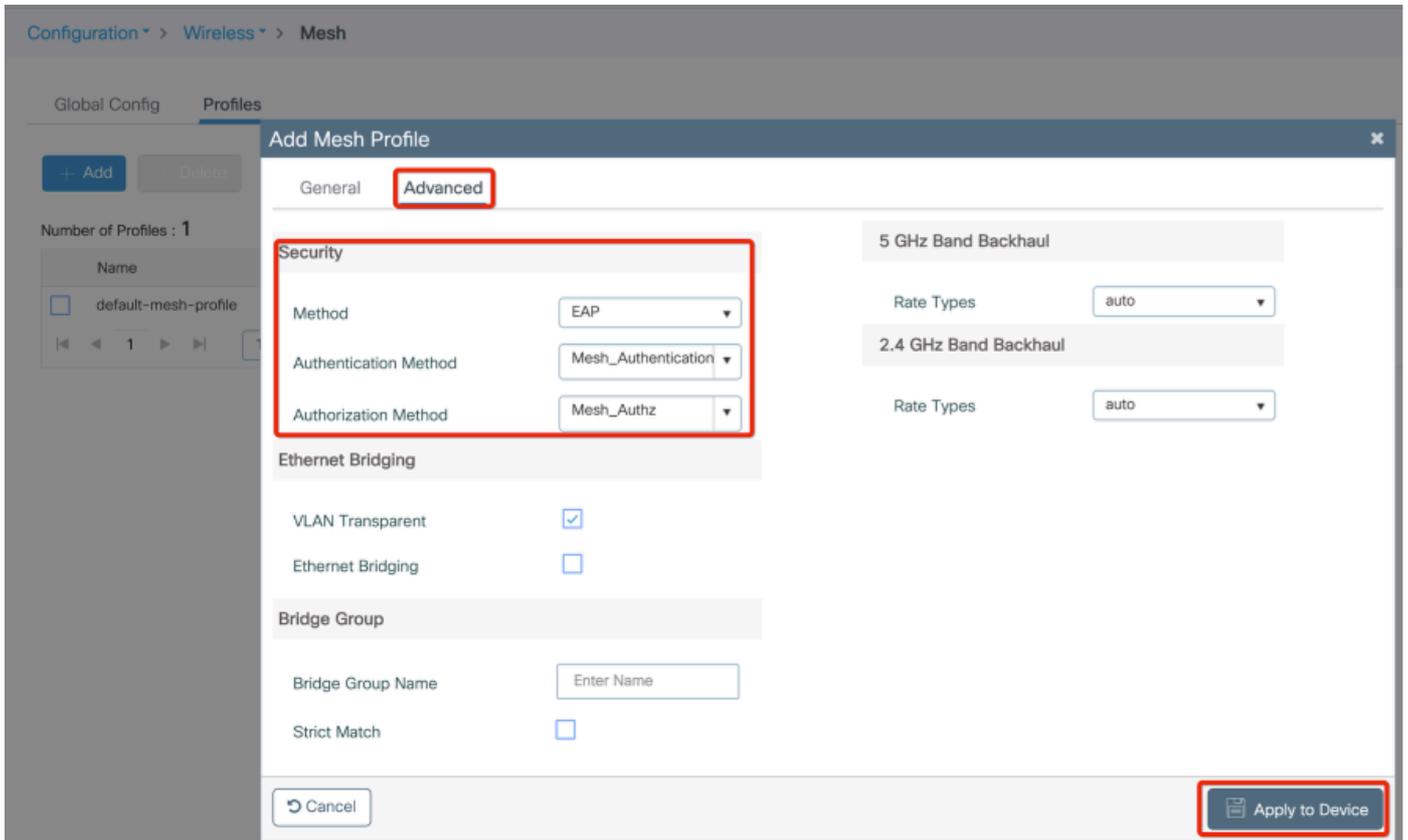
General Advanced

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

Cancel **Apply to Device**

Cliquez sur le profil de maillage créé pour modifier les paramètres généraux et avancés du profil.

Dans le schéma, comme illustré, nous devons mapper le profil d'authentification et d'autorisation créé avant le profil Mesh



Étape 5 : Créez un nouveau profil de jointure AP. Allez à Configurer > Balises et profils : 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 Config Translator

Application Visibility

Cloud Services

Custom Application

IOx

mDNS

Multicast

NetFlow

Python Sandbox

QoS

RA Throttle Policy

Tags & Profiles

AP Join

Flex

Policy

RF

Tags

WLANs

Wireless

Access Points

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 Apply to Device

Appliquez le profil de maillage précédemment configuré et configurez l'authentification AP EAP :

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

Client Statistics Reporting Interval

5 GHz (sec)

2.4 GHz (sec)

Extended Module

Enable

AP EAP Auth Configuration

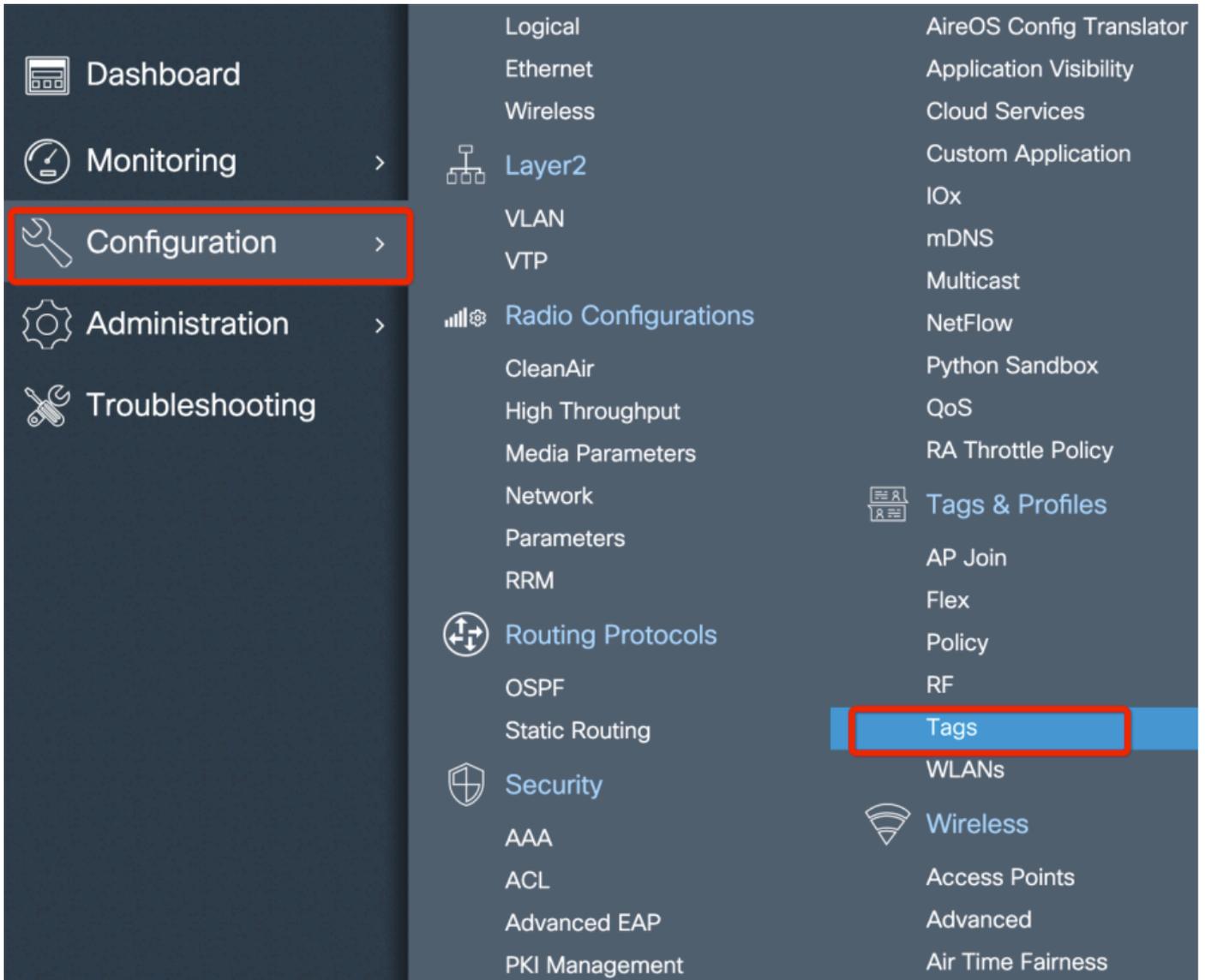
EAP Type

AP Authorization Type

Mesh

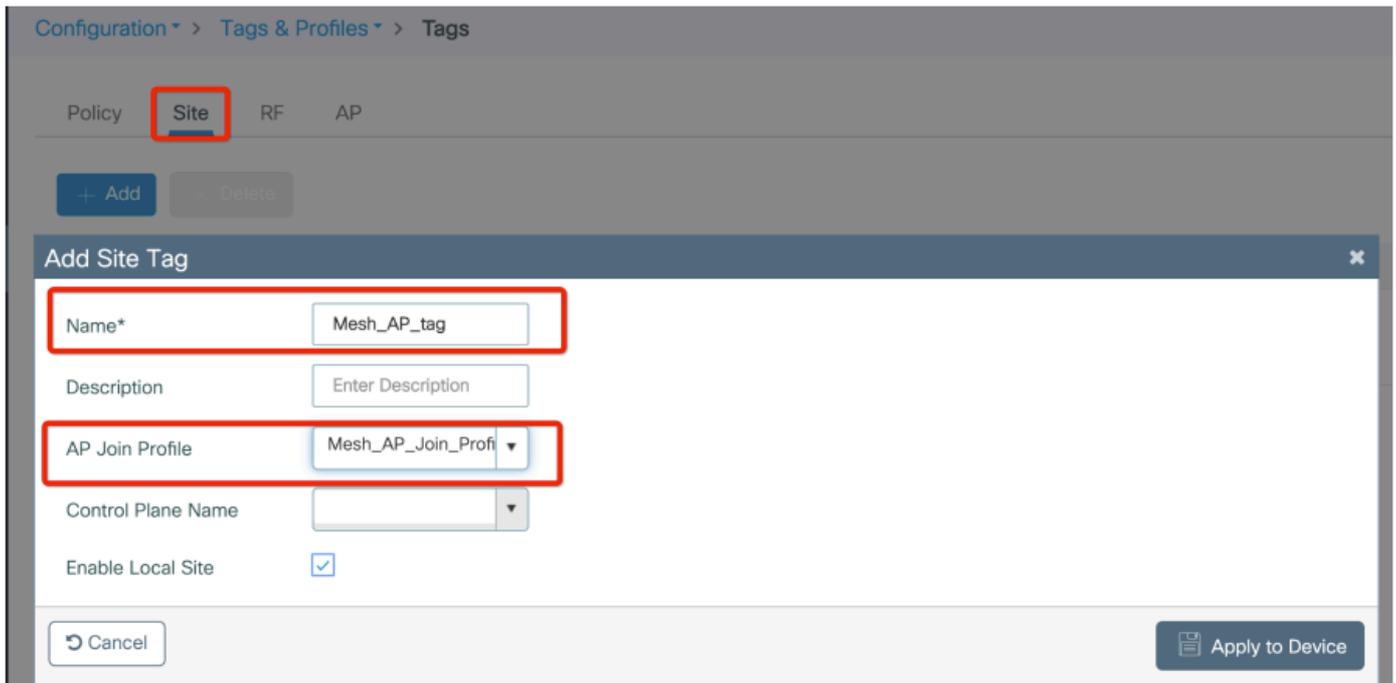
Profile Name [Clear](#)

Étape 6 : Créez une balise d'emplacement de maillage comme illustré.



configuration Cliquez sur l'étiquette d'emplacement de maillage créée à l'étape 6 pour la configurer.

Accédez à l'onglet Site et appliquez-lui le profil de jonction d'AP maillé précédemment configuré :



Étape 7. Convertissez le point d'accès en mode Pont.

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

10 items per page

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

Edit AP

General Interfaces High Availability Inventory Mesh Advanced Support Bundle

General		Version	
AP Name*	AP2C33-110E-6B66	Primary Software Version	17.3.0.17
Location*	default location	Predownloaded Status	N/A
Base Radio MAC	7070.8bb4.9200	Predownloaded Version	N/A
Ethernet MAC	2c33.110e.6b66	Next Retry Time	N/A
Admin Status	ENABLED	Boot Version	1.1.2.4
AP Mode	Bridge	IOS Version	17.3.0.17
Operation Status	Monitor	Mini IOS Version	0.0.0.0
Fabric Status	Sensor	IP Config	
LED State	Sniffer	CAPWAP Preferred Mode IPv4	
	Bridge		
	Clear		

via l'interface de ligne de commande, vous pouvez utiliser cette commande sur l'AP :

```
capwap ap mode bridge
```

Le point d'accès redémarre et se reconnecte en mode pont.

Étape 8. Vous pouvez maintenant définir le rôle du point d'accès : soit le point d'accès racine, soit le point d'accès maillé.

Le point d'accès racine est celui avec une connexion câblée au WLC tandis que le point d'accès maillé joint le WLC via sa radio qui essaie de se connecter à un point d'accès racine.

Un point d'accès maillé peut joindre le WLC via son interface câblée une fois qu'il n'a pas réussi à trouver un point d'accès racine via sa radio, à des fins de provisionnement.

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

10 items per page

- 5 GHz Radios
- 2.4 GHz Radios
- Dual-Band Radios
- Country
- LSC Provision

Edit AP

General Interfaces High Availability Inventory **Mesh** Advanced Support Bundle

General

Block Child

Daisy Chaining

Daisy Chaining strict-RAP

Preferred Parent MAC: 0000.0000.0000

VLAN Trunking Native 1

Role: Mesh (dropdown menu)

Remove PSK

Backhaul

Backhaul Radio Type: 5ghz

Backhaul Slot ID: 1

Rate Types: auto

Ethernet Port Configuration

⚠ Ethernet Bridging on the associated Mesh Profile should be enabled to configure this section successfully

Port: 0

Mode: normal

Cancel Update & Apply to Device

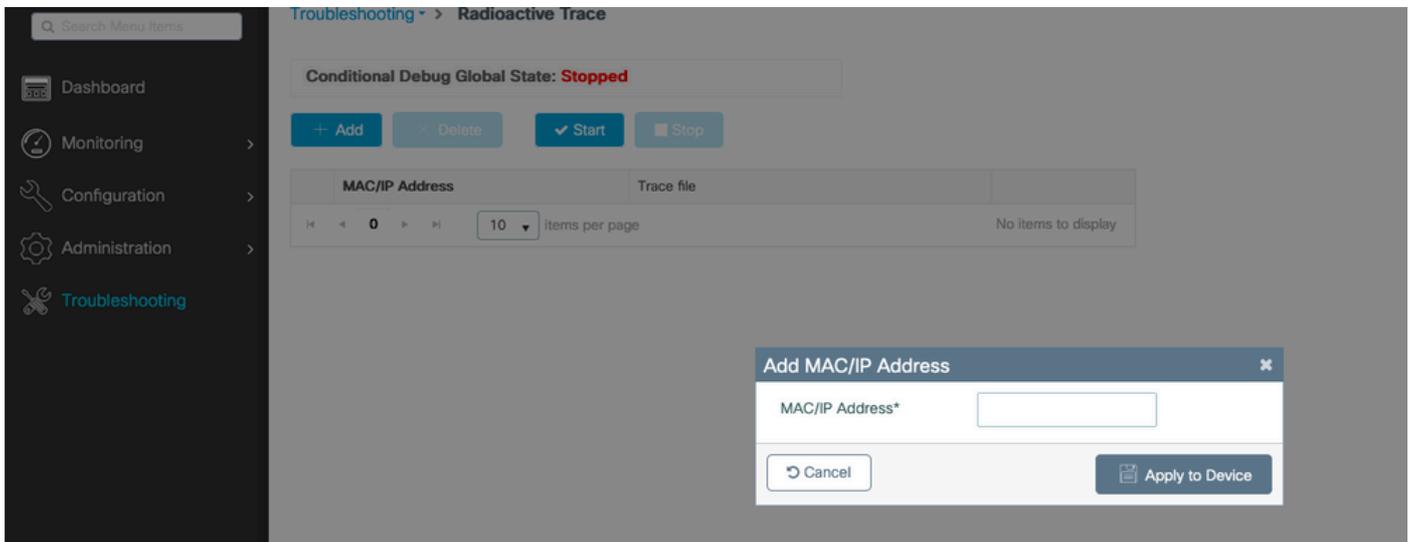
Vérifier

```

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
  
```

Dépannage

Dans la page Troubleshoot > Radioactive Trace web UI, cliquez sur add et entrez l'adresse MAC de l'AP.



Cliquez sur Start et attendez que le point d'accès essaie de joindre à nouveau le contrôleur.

Une fois terminé, cliquez sur Generate et choisissez une période pour collecter les journaux (les 10 ou 30 dernières minutes par exemple).

Cliquez sur le nom du fichier Trace pour le télécharger à partir de votre navigateur.

Voici un exemple de point d'accès non joint en raison d'un nom de méthode d'autorisation aaa incorrect qui a été défini :

```
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, appli
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess] [23388]: (info): Session-IP: 192.168.88.
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess] [23388]: (info): Session-IP: 192.168.88.
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [mesh-config] [23388]: (ERR): Failed to get ap PMK cache rec
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [mesh-config] [23388]: (ERR): Failed to get ap PMK cache rec
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [mesh-config] [23388]: (ERR): Failed to get ap PMK cache rec
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-capwap-join] [23388]: (info): 00a3.8e95.6c40 Ap auth p
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-capwap-join] [23388]: (ERR): Failed to initialize auth
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-capwap-join] [23388]: (ERR): 00a3.8e95.6c40 Auth requ
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-db] [23388]: (ERR): 00a3.8e95.6c40 Failed to get wtp r
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-db] [23388]: (ERR): 00a3.8e95.6c40 Failed to get ap ta
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess-fsm] [23388]: (ERR): Session-IP: 192.168.
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.
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [ewlc-dtls-sessmgr] [23388]: (info): Remote Host: 192.168.88.
2019/11/28 13:08:38.289 {wncmgrd_R0-0}{1}: [ewlc-infra-evq] [23038]: (debug): instance :0 port:38932MAC
```

La même chose peut être vu plus facilement dans le tableau de bord de l'interface utilisateur Web lorsque vous cliquez sur AP non joint. "Ap auth pending" est l'indice qui pointe vers l'authentification de l'AP lui-même :

The screenshot displays the 'Join Statistics' interface, which is divided into two main sections: 'General' and 'Statistics'.

General Section:

- Buttons: Clear, ClearAll
- Number of AP(s): 2
- Status filter: "Is equal to" NOT JOINED
- Table with columns: AP Name, AP Mod
- Table content:

AP Name	AP Mod
AP2CF8-9B5F-7D70	C9120A
NA	
- Items per page: 10

Statistics Section:

Category	Value	Category	Value
DTLS Session request received	1	Configuration requests received	0
Established DTLS session	1	Successful configuration responses sent	0
Unsuccessful DTLS session	0	Unsuccessful configuration request processing	0
Reason for last unsuccessful DTLS session	DTLS Handshake Success	Reason for last unsuccessful configuration attempt	NA
Time at last successful DTLS session	Mon, 17 Feb 2020 09:15:41 GMT	Time at last successful configuration attempt	NA
Time at last unsuccessful DTLS session	NA	Time at last unsuccessful configuration attempt	NA

Join phase statistics:

Join requests received	1
Successful join responses sent	0
Unsuccessful join request processing	0
Reason for last unsuccessful join attempt	Ap auth pending
Time at last successful join attempt	NA
Time at last unsuccessful join attempt	NA

Data DTLS Statistics:

DTLS Session request received	0
Established DTLS session	0
Unsuccessful DTLS session	0
Reason for last unsuccessful DTLS session	DTLS Handshake Success
Time at last successful DTLS session	NA
Time at last unsuccessful DTLS session	NA

Étude de cas 2 : Flex + Bridge

Cette section met en évidence le processus de jonction d'un AP 1542 en mode Flex+bridge avec l'authentification EAP effectuée localement sur le WLC.

Configurer

- Étape 1. Accédez à 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

MAC Address

Serial Number

+ Add

4

× Delete

MAC Address

002cc8de2b40

- Étape 2. Sélectionnez Device Authentication, puis Add
- Étape 3. Tapez l'adresse MAC Ethernet de base de l'AP à joindre au WLC, laissez le champ Attribute List Name vide, et sélectionnez Apply to Device

Quick Setup: MAC Filtering

MAC Address*

ffffffffffff

1

Attribute List Name

None

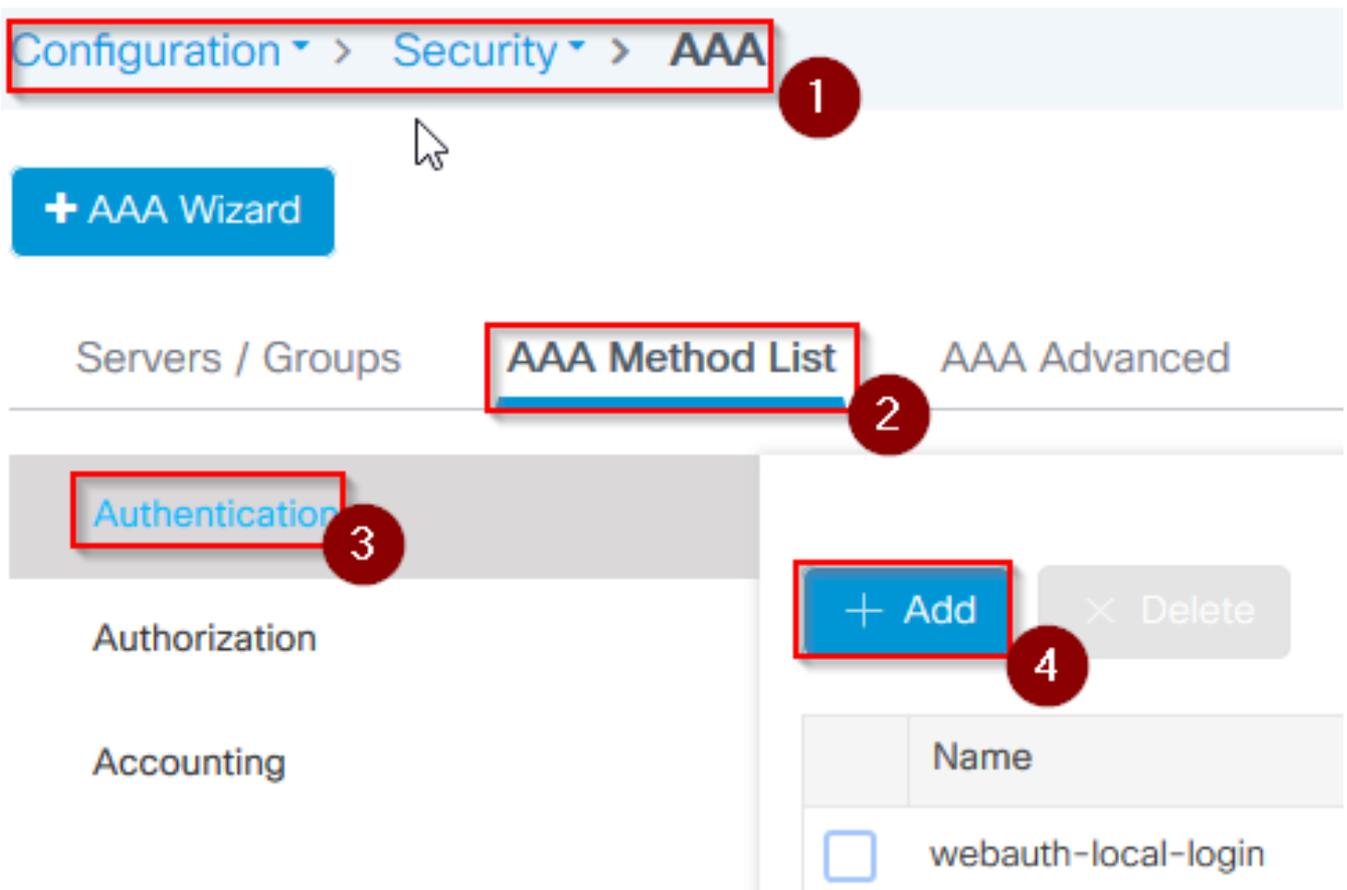
2

Cancel

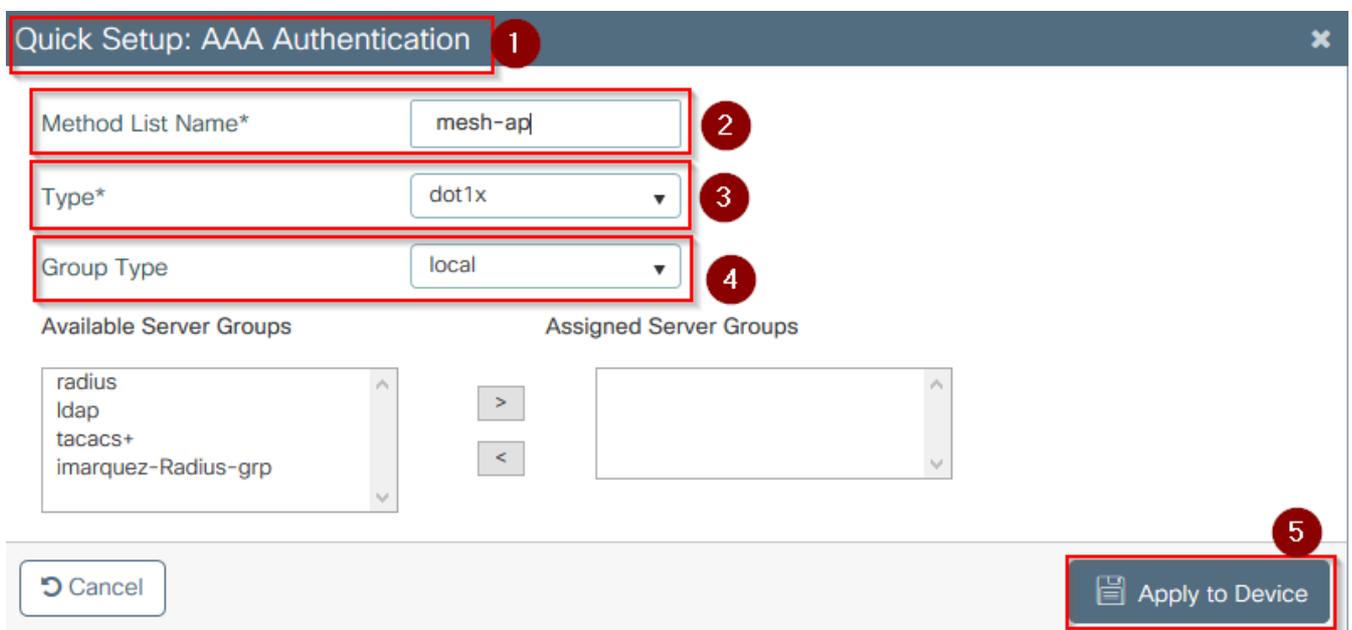
Apply to Device

3

- Étape 4. Accédez à Configuration > Security > AAA > AAA Method List > Authentication
- Étape 5. Sélectionnez Add, la fenêtre AAA Authentication s'affiche



- Étape 6. Tapez un nom dans la liste Nom de la méthode, sélectionnez 802.1x dans la liste déroulante Type* et local pour le type de groupe, puis sélectionnez Apply to Device



- Étape 6b. Si vos AP rejoignent directement en mode pont et qu'aucune balise de site et de stratégie n'a été attribuée auparavant, répétez l'étape 6, mais pour la méthode par défaut.
- Configurez une méthode d'authentification dot1x aaa qui pointe vers local (CLI `aaa authentication dot1x default local`)
- Étape 7. Accédez à Configuration > Security > AAA > AAA Method List > Autorisation

- Étape 8. Sélectionnez Add, la fenêtre AAA Authorization s'affiche

Configuration > Security > AAA 1

+ AAA Wizard

Servers / Groups AAA Method List 2 AAA Advanced

Authentication

Authorization 3

Accounting

+ Add 4 × Delete

Name
<input type="checkbox"/> default

- Étape 9. Saisissez un nom dans le champ Method List Name, sélectionnez Credential download dans la liste déroulante Type* et local pour le champ Group Type, puis sélectionnez Apply to Device

Quick Setup: AAA Authorization

Method List Name* mesh-ap 1

Type* credential-download 2

Group Type local 3

Authenticated

Available Server Groups Assigned Server Groups

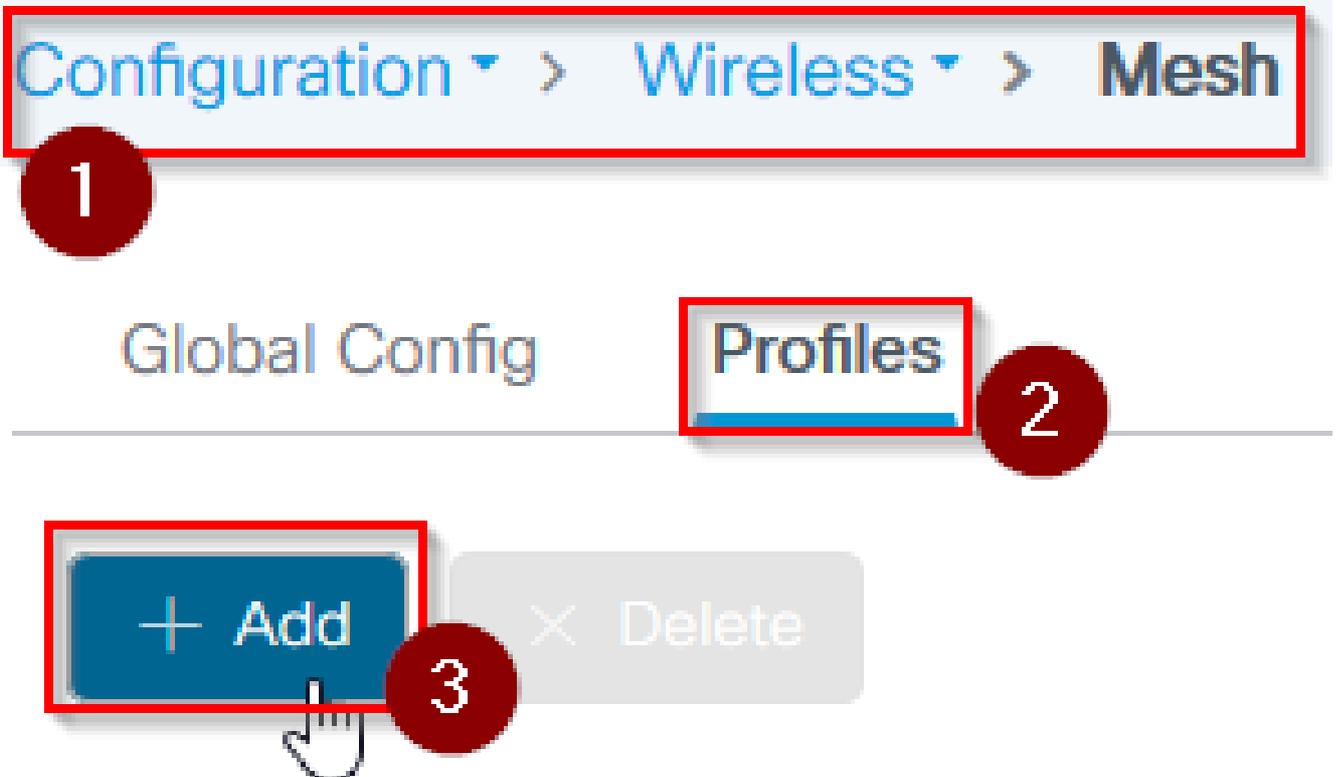
radius ldap tacacs+ imarquez-Radius-grp

Cancel Apply to Device 4

- Étape 9b. Si votre point d'accès se connecte directement en mode Bridge (c'est-à-dire qu'il

ne se connecte pas d'abord en mode local), répétez l'étape 9 pour la méthode de téléchargement des informations d'identification par défaut (CLI aaa autorisation credential-download default local)

- Étape 10. Accédez à Configuration > Wireless > Mesh > Profiles
- Étape 11. Sélectionnez Ajouter, la fenêtre contextuelle Ajouter un profil de maillage apparaît



- Étape 12. Dans l'onglet Général, définissez un nom et une description pour le profil de maillage

Add Mesh Profile

General Advanced

Name*	<input type="text" value="mesh-profile"/>
Description	<input type="text" value="mesh-profile"/>

- Étape 13. Sous l'onglet Advanced, sélectionnez EAP pour le champ Method
- Étape 14. Sélectionnez le profil d'autorisation et d'authentification défini aux étapes 6 et 9, puis sélectionnez Apply to Device (Appliquer au périphérique)

Add Mesh Profile ✕

General **Advanced** 1

Security

Method 2 EAP

Authentication Method 3 mesh-ap

Authorization Method 4 mesh-apl

Ethernet Bridging

VLAN Transparent

Ethernet Bridging

Bridge Group

Bridge Group Name

Strict Match

5 GHz Band Backhaul

Rate Types 5 auto

2.4 GHz Band Backhaul

Rate Types 5 auto

5

Cancel 5 Apply to Device

- Étape 15. Accédez à Configuration > Tag & Profiles > AP Join > Profile
- Étape 16. Sélectionnez Add, la fenêtre contextuelle AP Join Profile apparaît, définissez un nom et une description pour le profil AP Join

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"/>					

- Étape 17. Accédez à l'onglet AP et sélectionnez le profil de maillage créé à l'étape 12 dans la liste déroulante Nom du profil de maillage
- Étape 18. Assurez-vous que EAP-FAST et CAPWAP DTLS sont définis pour les champs respectivement EAP Type et AP Authorization Type
- Stéo 19. Sélectionnez Apply to Device

Add AP Join Profile ✕

General	Client	CAPWAP	AP ¹	Management	Rogue AP	ICap
General	Hyperlocation	BLE	Packet Capture			

Power Over Ethernet
Switch Flag
Power Injector State
Power Injector Type
Injector Switch MAC
Code

Client Statistics Reporting Interval
5 GHz (sec)
2.4 GHz (sec)

Extended Module
Enable

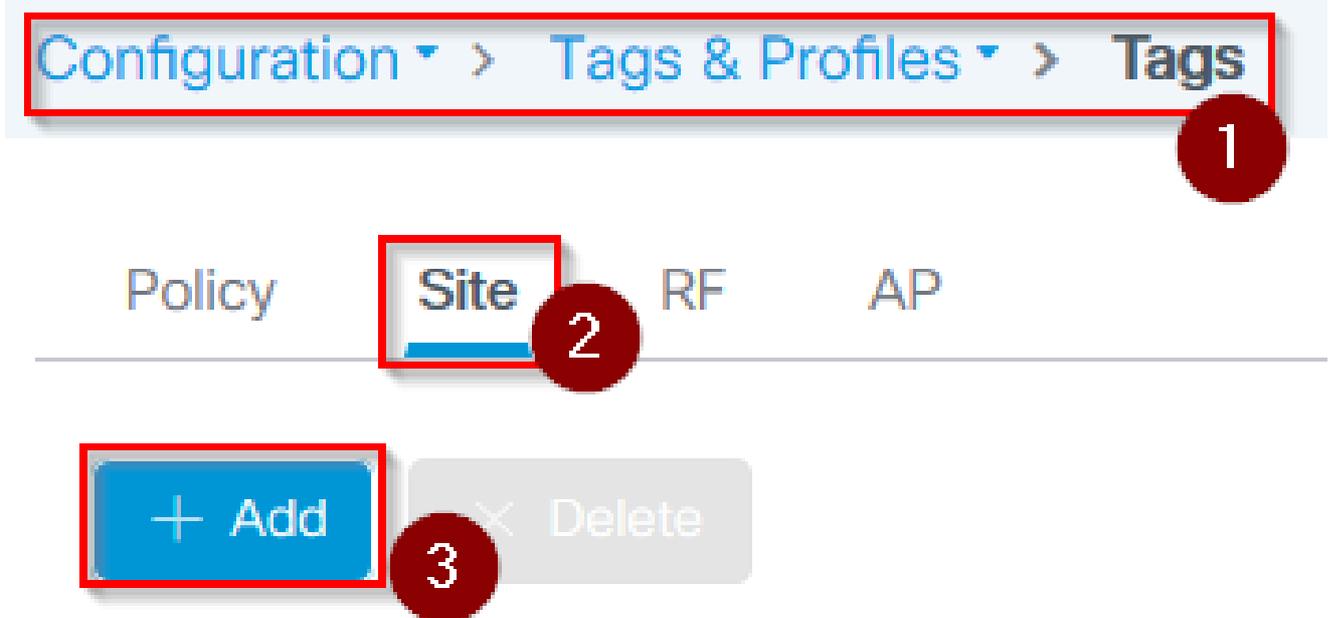
Mesh ²
Profile Name Clear

AP EAP Auth Configuration
EAP Type ³
AP Authorization Type ⁴

⁵

- Étape 20. Accédez à Configuration > Tag & Profiles > Tags > Site

- Étape 21. Sélectionnez Add, la fenêtre contextuelle Site Tag s'affiche



- Étape 22. Entrez un nom et une description pour la balise de site

The screenshot shows the 'Add Site Tag' form. The title 'Add Site Tag' is highlighted with a red box and a red circle containing the number 1. The form has three input fields: 'Name*' with the value 'mesh-ap-site', 'Description' with the value 'mesh-ap-site', and 'AP Join Profile' with the value 'mesh-ap-join-profile'. The 'AP Join Profile' field is highlighted with a red box and a red circle containing the number 2.

- Étape 23. Sélectionnez le profil de jointure AP créé à l'étape 16 dans la liste déroulante AP Join Profile
- Étape 24. Au bas de la fenêtre contextuelle Balise du site, décochez la case Enable Local Site pour activer la liste déroulante Flex Profile.
- Étape 35. Dans la liste déroulante Flex Profile, sélectionnez le profil Flex Profile que vous souhaitez utiliser pour l'AP

Add Site Tag ✕

Name*

Description

AP Join Profile

Flex Profile **2**

Control Plane Name

Enable Local Site **1**

3

- Étape 36. Connectez le point d'accès au réseau et assurez-vous qu'il est en mode local.
- Étape 37. Pour vous assurer que le point d'accès est en mode local, émettez la commande capwap ap mode local.

Le point d'accès doit avoir un moyen de trouver le contrôleur, soit la diffusion L2, DHCP Option 43, la résolution DNS ou la configuration manuelle.

- Étape 38. Le point d'accès rejoint le WLC, assurez-vous qu'il est répertorié dans la liste AP, naviguez vers Configuration > Wireless > Access Points > All Access Points

Configuration > Wireless > Access Points **1**

✓ All Access Points

Number of AP(s): 2

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

- Étape 39. Sélectionnez le point d'accès, la fenêtre contextuelle AP apparaît.
- Étape 40. Sélectionnez la balise de site créée à l'étape 22 sous Général > Balises > onglet Site dans la fenêtre contextuelle AP, sélectionnez Mettre à jour et appliquer au périphérique

Edit AP

General 1 Interfaces High Availability Inventory Mesh Advanced

General		Version	
AP Name*	[Redacted]	Primary Software Version	16.12.1.139
Location*	default location	Predownloaded Status	N/A
Base Radio MAC	[Redacted]	Predownloaded Version	N/A
Ethernet MAC	[Redacted]	Next Retry Time	N/A
Admin Status	ENABLED <input checked="" type="checkbox"/>	Boot Version	1.1.2.4
AP Mode	Flex-Bridge	IOS Version	16.12.1.139
Operation Status	Registered	Mini IOS Version	0.0.0.0
Fabric Status	Disabled	IP Config	
LED State	ENABLED <input checked="" type="checkbox"/>	CAPWAP Preferred Mode	IPv4
LED Brightness Level	8	DHCP IPv4 Address	[Redacted]
CleanAir NSI Key		Static IP (IPv4/IPv6)	<input type="checkbox"/>
Tags		Time Statistics	
Policy	imarquez-FlexLocal	Up Time	4 days 3 hrs 2 mins 6 secs
Site	Mesh-AP-Tag	Controller Association Latency	20 secs
RF	default-rf-tag		

3

Cancel Update & Apply to Device

- Étape 41. L'AP redémarre et doit joindre le WLC en mode Flex + Bridge

Notez que cette méthode joint d'abord le point d'accès en mode local (où il n'effectue pas l'authentification dot1x) pour appliquer la balise de site avec le profil maillé, puis bascule le point d'accès en mode pont.

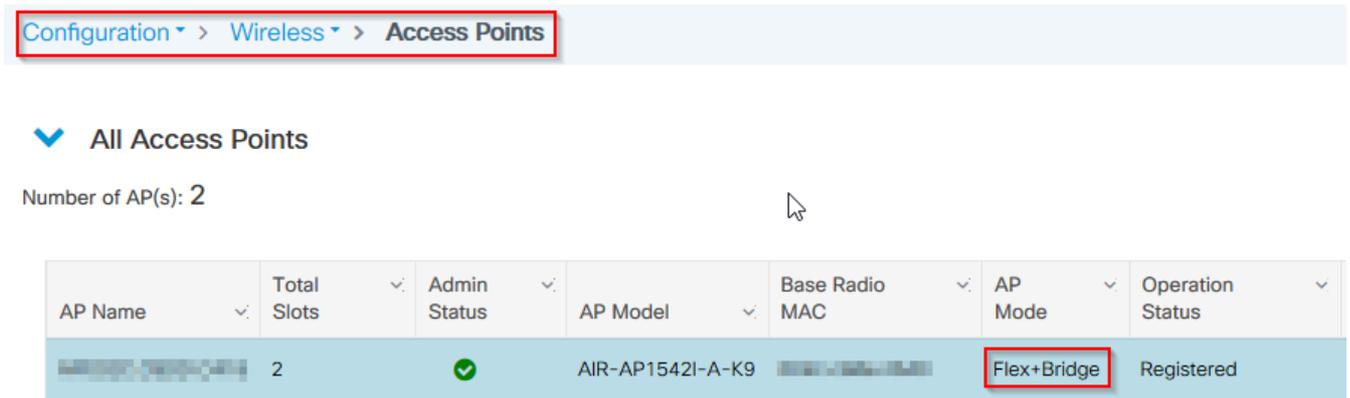
Pour joindre un AP qui est bloqué en mode Bridge (ou Flex+Bridge), configurez les méthodes par défaut (aaa authentication dot1x default local et aaa authorization cred default local).

Le point d'accès est alors capable de s'authentifier et vous pouvez assigner les balises par la suite.

Vérifier

Assurez-vous que le mode AP est affiché sous la forme Flex + Bridge, comme illustré dans cette

image.



Exécutez ces commandes à partir de l'interface de ligne de commande du WLC 9800 et recherchez l'attribut AP Mode. Il doit être répertorié comme Flex+Bridge

```
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
```

Dépannage

Assurez-vous que les commandes aaa authentication dot1x default local et aaa authorization cred default local sont présentes. Ils sont nécessaires si votre AP n'a pas été pré-joiné en mode local.

Le tableau de bord principal 9800 a un widget qui affiche les points d'accès qui ne peuvent pas se joindre. Cliquez dessus pour obtenir la liste des points d'accès qui ne parviennent pas à se connecter :



Cliquez sur le point d'accès spécifique pour voir la raison pour laquelle il n'est pas joint. Dans ce cas, nous voyons un problème d'authentification (AP auth pending) parce que la balise de site n'a pas été assignée à l'AP.

Par conséquent, le 9800 n'a pas choisi la méthode d'authentification/autorisation nommée pour authentifier le point d'accès :

Join Statistics ✕			
General		Statistics	
Control DTLS Statistics		Configuration phase statistics	
DTLS Session request received	179	Configuration requests received	173
Established DTLS session	179	Successful configuration responses sent	4
Unsuccessful DTLS session	0	Unsuccessful configuration request processing	0
Reason for last unsuccessful DTLS session	DTLS Handshake Success	Reason for last unsuccessful configuration attempt	Regulatory domain check failed
Time at last successful DTLS session	Thu, 19 Dec 2019 13:03:19 GMT	Time at last successful configuration attempt	Thu, 19 Dec 2019 12:36:10 GMT
Time at last unsuccessful DTLS session	NA	Time at last unsuccessful configuration attempt	NA
Join phase statistics		Data DTLS Statistics	
Join requests received	179	DTLS Session request received	0
Successful join responses sent	173	Established DTLS session	0
Unsuccessful join request processing	0	Unsuccessful DTLS session	0
Reason for last unsuccessful join attempt	Ap auth pending	Reason for last unsuccessful DTLS session	DTLS Handshake Success
Time at last successful join attempt	Thu, 19 Dec 2019 12:36:10 GMT	Time at last successful DTLS session	NA
Time at last unsuccessful join attempt	NA	Time at last unsuccessful DTLS session	NA

Pour un dépannage plus avancé, accédez à la page [Troubleshooting > Radioactive Trace](#) sur l'interface utilisateur Web.

Si vous entrez l'adresse MAC de l'AP, vous pouvez immédiatement générer un fichier pour obtenir les journaux toujours actifs (au niveau de notification) de l'AP qui tente de se joindre.

Cliquez sur Démarrer pour activer le débogage avancé pour cette adresse MAC. La prochaine fois que les journaux sont générés, générez les journaux, les journaux de niveau de débogage pour la jointure AP sont affichés.



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 ↓	▶ Generate

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

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.