

Configuration des points d'accès maillés pour le pontage de données local en mode Flex et Bridge

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Diagramme du réseau](#)

[Ajouter un point d'accès à la base de données locale du contrôleur](#)

[Liste de méthodes AAA pour l'authentification](#)

[Liste de méthodes AAA pour autorisation](#)

[Profil de maillage](#)

[Profil de jointure AP](#)

[Profil Flex](#)

[Profil de stratégie](#)

[Balise WLAN](#)

[Balise de stratégie](#)

[Balise de site](#)

[Configuration des points d'accès](#)

[Configuration du port de commutateur](#)

[Vérifier](#)

Introduction

Ce document décrit la configuration des MAP en mode Flex et Bridge pour le pontage de données client local, en contournant le RAP.

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 des commutateurs Cisco

Composants utilisés

Cet exemple utilise des points d'accès légers (modèles 9124AP), qui peuvent être configurés en tant que point d'accès racine (RAP) ou point d'accès maillé (MAP) pour s'intégrer de manière transparente au contrôleur LAN sans fil (WLC) Catalyst 9800.

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

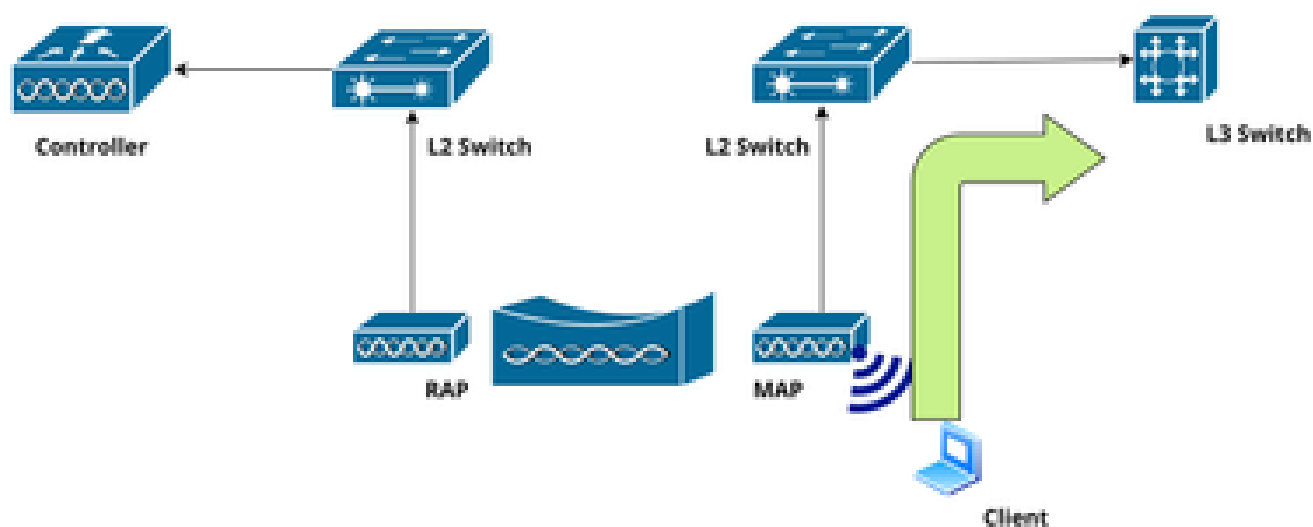
- C9800-L v17.12.5
- Commutateur Cisco Catalyst 3850
- Point d'accès Cisco Catalyst 9124AX

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

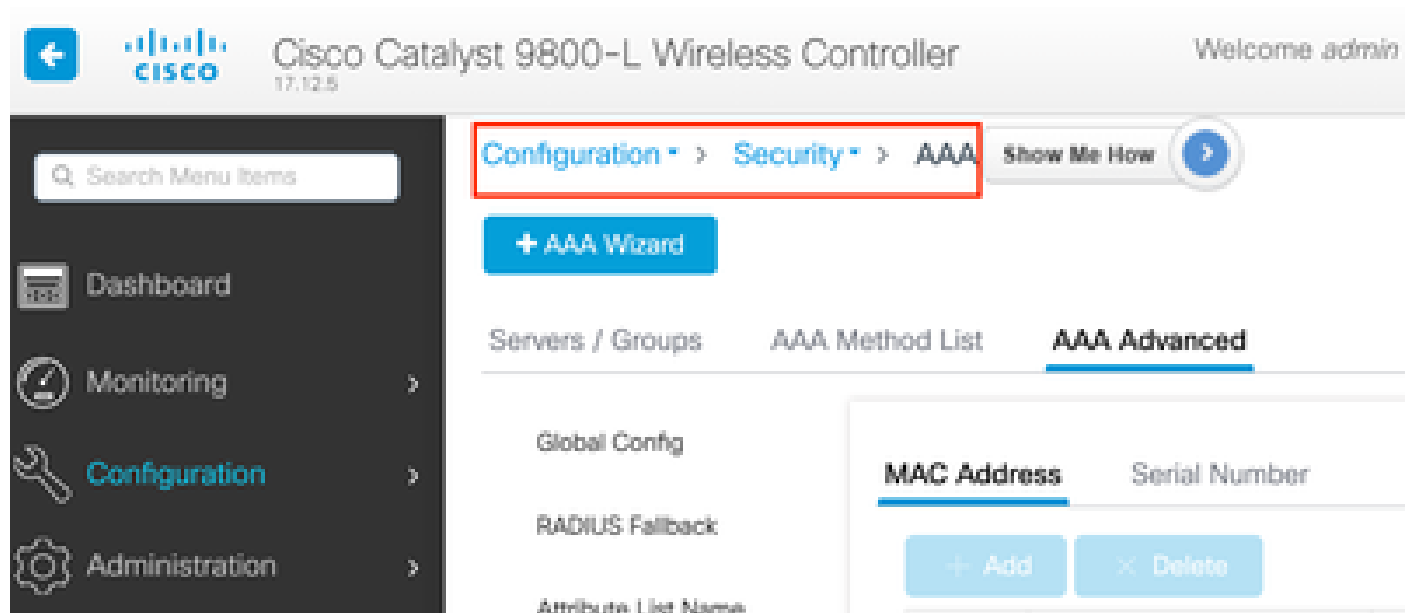
Cette section décrit la configuration des points d'accès maillés (MAP) fonctionnant en mode Maillage + Pont, ce qui permet de ponter directement les données des clients locaux vers le commutateur de liaison ascendante, en contournant le point d'accès racine (RAP).

Diagramme du réseau

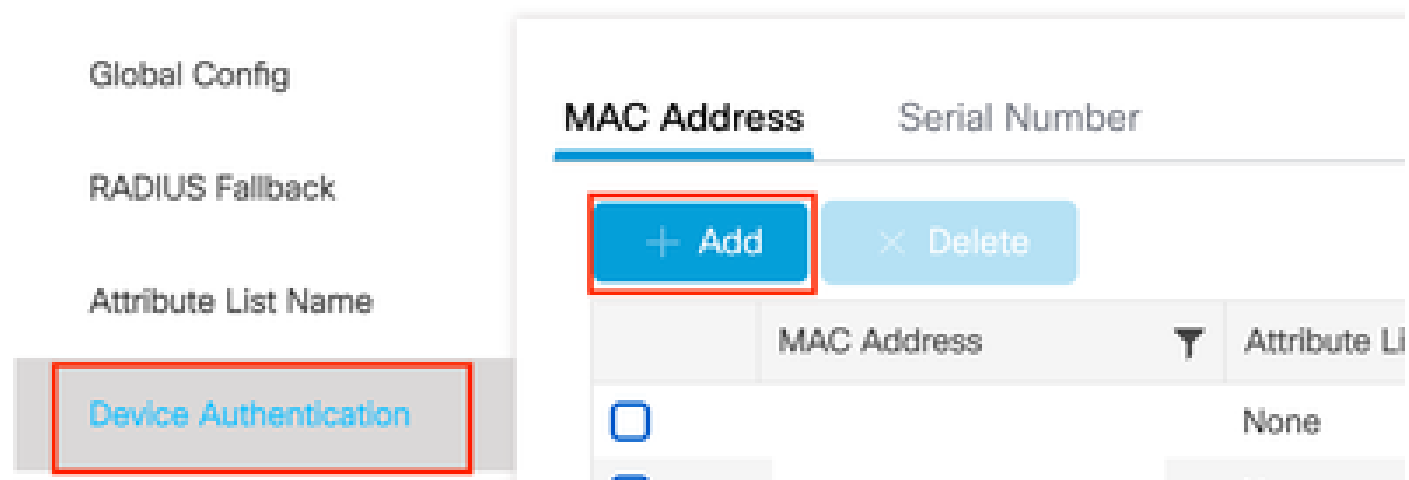


Ajouter un point d'accès à la base de données locale du contrôleur

Étape 1 : Accédez à Configuration > Security > AAA > AAA Advanced.



Étape 2. Sélectionnez Authentification du périphérique et sélectionnez Ajouter.



Étape 3. Entrez l'adresse MAC Ethernet de base du point d'accès pour joindre le WLC. Laissez le champ Nom de la liste d'attributs vide et sélectionnez Appliquer au périphérique.

MAC Address*	3a5f1c8e729b
Attribute List Name	None
Description	
WLAN Profile Name	Select a value

Liste de méthodes AAA pour l'authentification

Étape 1 : Accédez à Configuration > Security > AAA > AAA Method List > Authentication et sélectionnez Add.

Configuration > Security > AAA

Servers / Groups

AAA Method List

AAA Advanced

Authentication

Authorization

Étape 2 : Define Method List Name. Sélectionnez dot1x dans la liste déroulante Type* et local pour le type de groupe. Sélectionnez Apply to Device pour enregistrer la configuration.

Method List Name*	MESH		
Type*	dot1x		
Group Type	local		
Available Server Groups	Assigned Server Groups		
radius ldap tacacs+ HTTSGROUP ISE_DD_Group ISE_HA Test	> < > <		+ + + +

Cancel

Update & Apply to Device

Liste de méthodes AAA pour autorisation

Étape 1 : Accédez à Configuration > Security > AAA > AAA Method List > Authorization et sélectionnez Add.

+ AAA Wizard

Servers / Groups

AAA Method List

AAA Advanced

Authentication

Authorization

Accounting

+ Add

× Delete

	Name		Type
	default		EXEC

Étape 2 : Définissez le nom de la liste de méthodes, sélectionnez téléchargements d'informations d'identification dans la liste déroulante Type* et local pour le type de groupe. Cliquez sur Apply to Device.

Method List Name*	MESH-Authorization
Type*	credential-downlo... ⓘ
Group Type	local ⓘ
Authenticated	☐
Available Server Groups	Assigned Server Groups
radius ldap tacacs+ HTTSGROUP ISE_DD_Group ISE_HA Trust	> < > <
Cancel Update & Apply to Device	

Profil de maillage

Étape 1 : Accédez à Configuration > Wireless > Mesh > Profiles et sélectionnez Add.

[Configuration ▾](#) > [Wireless ▾](#) > [Mesh](#)

Global Config

Profiles

+ Add

× Delete

Étape 2 : Dans l'onglet Général, définissez un nom et une description (facultatif) pour le profil de maillage.

General

Advanced

Name*

MESH-Profile

Description

Enter Description

Range (Root AP to Mesh AP)

12000

Multicast Mode

In-Out ▼

IDS (Rogue/Signature Detection)

☐

Étape 3 : Dans l'onglet Avancé, définissez le champ Méthode sur EAP, puis sélectionnez les profils d'autorisation et d'authentification précédemment créés dans les menus déroulants. Enfin, activez la case à cocher Ethernet Bridging et sélectionnez Update and apply.

General

Advanced

Security

Method

EAP

Authentication Method

MESH

Authorization Method

MESH-Authorizati...

Ethernet Bridging

VLAN Transparent

☐

Ethernet Bridging

☒

Profil de jointure AP

Étape 1 : Accédez à Configuration > Tag & Profiles > AP Join > Profile, cliquez sur Add.

Configuration > **Tags & Profiles** > **AP Join**

+ Add

× Delete

📄 Clone

AP Join Profile Name

Étape 2 : Définissez le nom et la description du profil (facultatif).

General

Client

CAPWAP

AP

Management

S

Name*

Mesh-AP-Join

Description

Enter Description

Country Code

IN



Time Zone



Not Configured



Use-Controller



Delta from WLC

Étape 3 : Accédez à l'onglet AP, sélectionnez le profil de maillage dans la liste déroulante Mesh Profile Name, définissez EAP-FAST pour le type EAP et CAPWAP DTLS pour le type d'autorisation AP, puis cliquez sur Apply to Device.

Edit AP Join Profile

General

Client

CAPWAP

AP

Management

Security

ICap

QoS

Geolocation

General

Power Management

Hyperlocation

AP Statistics

Power Over Ethernet

Switch Flag

Power Injector State

Power Injector Type

Injector Switch MAC

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

Cancel

Update & Apply to Device

Profil Flex

Étape 1 : Configuration > Tags & Profiles > Flex, puis cliquez sur Add.

Configuration > Tags & Profiles > Flex

+ Add

× Delete

Clone

Étape 2 : Définissez un nom pour le profil Flex.

General

Local Authentication

Policy ACL

VLAN

DNS Layer Security

Name*

Mesh-Flex

Fallback Radio Shut

Description

Enter Description

Flex Resilient

Étape 3 : Accédez à l'onglet vlan et configurez le nom et l'ID de VLAN pour le pontage local du trafic client sans fil, cliquez sur Save.

General

Local Authentication

Policy ACL

VLAN

DNS Layer Security

+ Add

< Delete

VLAN Name

T

ID

T

Ingress ACL

T

Egress ACL

T

= 0 =

10

No items to display

VLAN Name*

Bridge-VLAN

VLAN ID*

100

ACL

☒ Unidirectional☐ Bidirectional

Ingress ACL

Select ACL

?

Egress ACL

Select ACL

?

✓ Save

Cancel

Cancel

Update & Apply to Device

Profil de stratégie

Étape 1 : Accédez à Configuration > Tags & Profiles > Policy et cliquez sur Add.

Configuration ▾ > Tags & Profiles ▾ > Policy

+ Add

× Delete

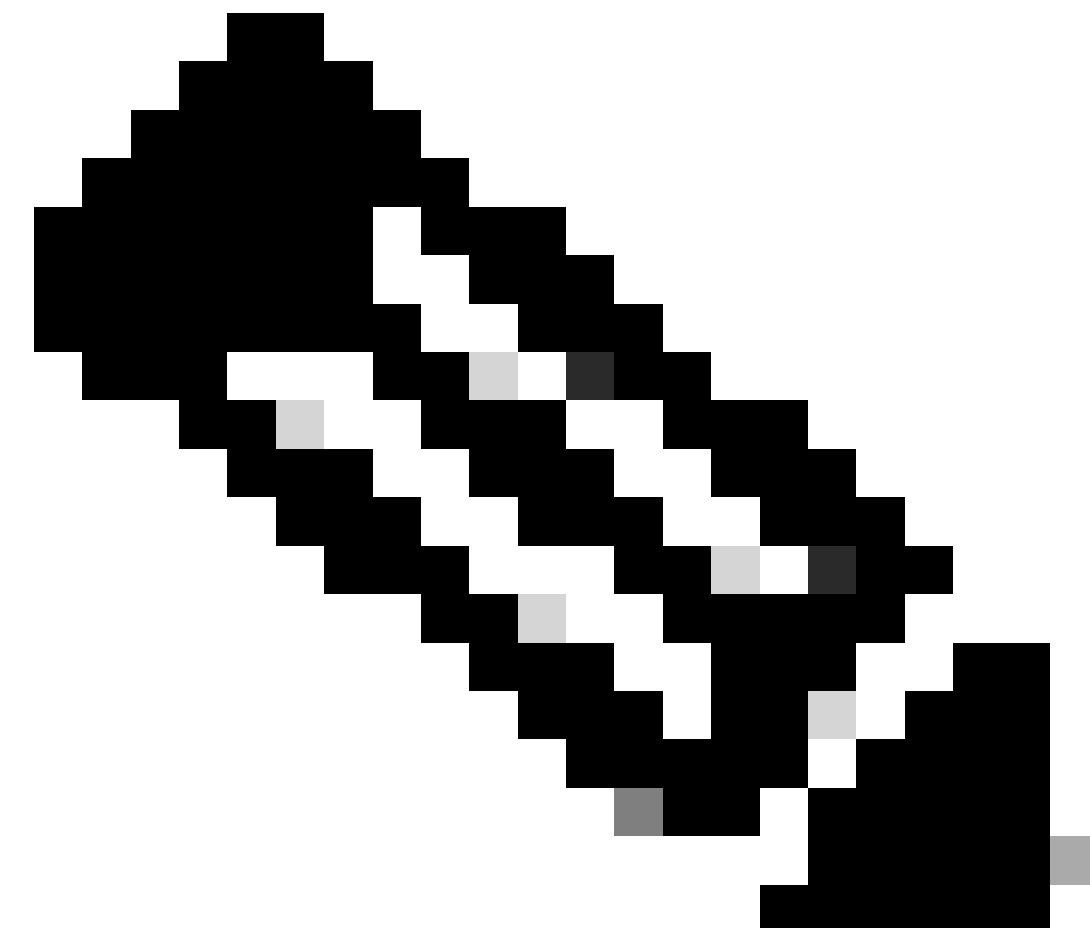
Clone

Admin
Status ▾

Associated
Policy Tags ⓘ ▾

Policy Profile Name

Étape 2 : Dans l'onglet Général, définissez le nom du profil, définissez l'état sur Activé et Désactivez la commutation centrale.



Remarque : Pour activer le pontage local du trafic client, la commutation centrale doit être désactivée. En fonction de la configuration SSID, d'autres options peuvent être activées

ou désactivées selon les besoins.

General

Access Policies

QoS and AWC

Mobility

Advanced

Name*

Bridge-Policy

Description

Enter Description

Status

ENABLED

Passive Client

DISABLED

IP MAC Binding

ENABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

Inline Tagging

☐

SGACL Enforcement

☐

Default SGT

2-65519

WLAN Switching Policy

Central Switching

DISABLED

Central Authentication

ENABLED

Central DHCP

DISABLED

Flex NAT/PAT

DISABLED

Cancel

Update & Apply to Device

Étape 3 : Configurez le VLANID spécifié sous l'onglet VLAN du AP Flex Profile, et cliquez sur Update & Apply.

General	Access Policies	QoS and AVC	Mobility	Advanced
RADIUS Profiling ☐ HTTP TLV Caching ☐ DHCP TLV Caching ☐		WLAN ACL IPv4 ACL Search or Select IPv6 ACL Search or Select		
WLAN Local Profiling Global State of Device Classification Enabled Local Subscriber Policy Name Search or Select		URL Filters Pre Auth Search or Select Post Auth Search or Select		
VLAN VLAN/VLAN Group 100 Multicast VLAN Enter Multicast VLAN				

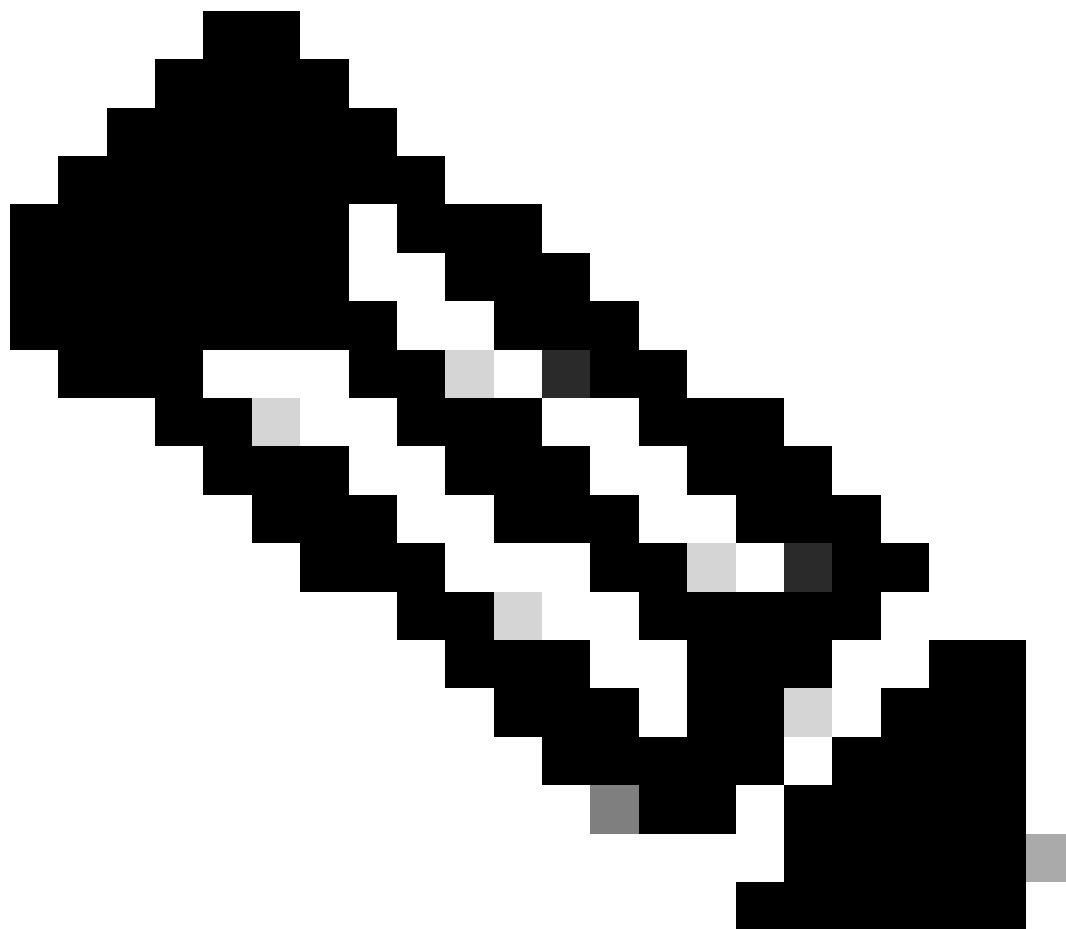
Cancel
 Update & Apply to Device

Balise WLAN

Étape 1 : Accédez à Configuration > Tags & Profiles > WLANs et sélectionnez Add.

Étape 2 : Sous l'onglet General, configurez le nom du profil, le SSID et définissez l'état sur enabled.

Étape 3 : Sélectionnez l'onglet Security, Enable WAP+WPA2 et configurez une clé pré-partagée.



Remarque : La configuration du SSID dépend entièrement de vos besoins. Dans cet exemple, un SSID basé sur PSK est configuré.

General

Security

Advanced

Add To Policy Tags

Profile Name*

Bridge

R

SSID*

Bridge-SSID

WLAN ID*

6

6

St

Status

ENABLED



Broadcast SSID

ENABLED



5

St

Edit WLAN

General

Security

Advanced

Add To Policy Tags

Layer2

Layer3

AAA

☒ WPA + WPA2
 ☐ WPA2 + WPA3
 ☐ WPA3
 ☐ Static WEP
 ☐ None

MAC Filtering

☐

Lobby Admin Access

☐

WPA Parameters

WPA Policy

☐

GTK Randomize

☐

WPA2 Policy

☒

OSN Policy

☐

Fast Transition

Status

Disabled

Over the DS

☐

Reassociation Timeout *

20

WPA2 Encryption

AES(CCMP128)

☒

CCMP256

☐

GCMP128

☐

GCMP256

☐

Protected Management Frame

PMF

Disabled

Auth Key Mgmt

802.1X

☐

Easy-PSK

☐

FT + 802.1X

☐

802.1X-SHA256

☐

PSK

☒

CKM

☐

FT + PSK

☐

PSK-SHA256

☐

PSK Format

ASCII

PSK Type

AES

Pre-Shared Key*

Cancel

Update & Apply to Device

Balise de stratégie

Étape 1 : Accédez à Configuration > Tags & Profiles > Tags > Policy Tab, cliquez sur Add.

Étape 2 : Créez une balise de stratégie en définissant un nom et en associant le WLAN et le profil de stratégie.

Add Policy Tag

Name*

Mesh-Policy-Tag

Description

Enter Description

WLAN-POLICY Maps: 0

+ Add

× Delete

WLAN Profile

Policy Profile

10

No items to display

Map WLAN and Policy

WLAN Profile*

Bridge

Policy Profile*

Bridge-Policy

×

✓

> WLAN-POLICY Maps: 0

Cancel

Apply to Device

Balise de site

Étape 1 : Accédez à Configuration > Tags & Profiles > Tags > Site et cliquez sur Add.

Configuration > Tags & Profiles > Tags

Policy

Site

RF

AP

+ Add

× Delete

Clone

Étape 2 : Configurez le nom de balise, désactivez l'option Enable Local Site et associez le profil de jonction d'AP et le profil flexible.

Edit Site Tag

Name*

Mesh-Site-Tag

Description

Enter Description

AP Join Profile

Mesh-AP-Join

Flex Profile

Mesh-Flex

Fabric Control Plane Name

Enable Local Site

☐

Load* ⓘ

0

Cancel

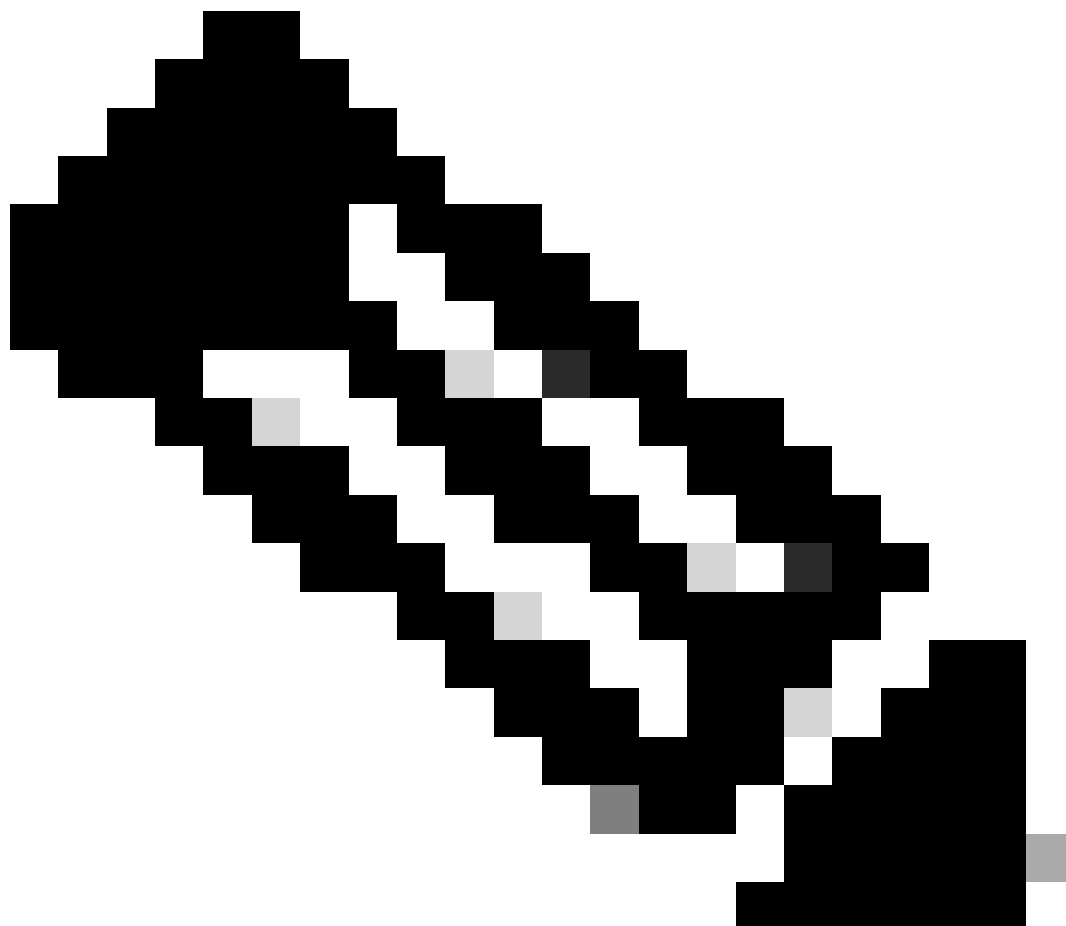
Update & Apply to Device

Configuration des points d'accès

Cette étude de cas suppose que le point d'accès (AP) est d'abord joint au contrôleur LAN sans fil (WLC) en mode local, puis est passé en mode Flex+Bridge.

Étape 1 : Accédez à Configuration > Wireless > Access Points et sélectionnez le point d'accès.

Étape 2 : Attribuez la balise de site et la balise de stratégie aux points d'accès (AP).



Remarque : Le point d'accès (AP) redémarre, établit la connexion avec le contrôleur en mode Flex+Bridge et l'onglet Maillage est disponible.

General		Tags	
AP Name*	AP34B8.8314.A204	 Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.	
Location*	default location		
Base Radio MAC	34b8.831d.05a0		
Ethernet MAC	34b8.8314.a204	Policy	Mesh-Policy-Tag 
Admin Status	ENABLED 	Site	Mesh-Site-Tag 

Étape 3 : Sous l'onglet Maillage, sélectionnez le rôle à racine

Edit AP
General
Interfaces
High Availability
Inventory
Geolocation
Mesh
Advanced
Support Bundle

General

Block Child
☐

Daisy Chaining
☐

Daisy Chaining strict-RAP
☐

Preferred Parent MAC

Role

Ethernet Port Configuration

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

Port

Mode

VLAN ID*

Étape 4 : Répétez les étapes 1 et 2 pour le point d'accès désigné pour fonctionner comme point d'accès maillé afin de le mettre en ligne en mode Flex+Bridge. Accédez à l'onglet Maillage et configurez le rôle en tant que Maillage.

Étape 5 : Le point d'accès maillé est connecté au commutateur sur le port 0, configuré en mode Trunk, avec le VLAN AP défini comme VLAN natif. Assurez-vous que les VLAN autorisés incluent le VLAN client spécifié dans le profil Flex.

Étape 6 : Cliquez sur Update and Apply.

General
Interfaces
High Availability
Inventory
Geolocation
Mesh
Advanced
Support Bundle

General

Block Child
☐

Daisy Chaining
☐

Daisy Chaining strict-RAP
☐

Preferred Parent MAC

Role

Remove PSK

Ethernet Port Configuration

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

Port

Mode

Native VLAN ID*

Allowed VLAN IDs

Configuration du port de commutateur

```
interface GigabitEthernet1/0/4
switchport trunk allowed vlan 100
switchport mode trunk
end
```

Vérifier

Association d'AP maillé à l'AP racine :

```
#show wireless mesh ap summary
AP Name AP Model BVI MAC BGN AP Role
-----
AP34B8.8314.A204 C9124AXI-ROW 34b8.8314.a204 Default Root AP
APC828.E536.D47C C9124AXI-ROW c828.e536.d47c Default Mesh AP
Number of Flex+Bridge APs : 2
Number of Flex+Bridge RAPs : 1
Number of Flex+Bridge MAPs : 1
```

```
#show wireless mesh ap tree
=====
AP Name [Hop Ctr,Link SNR,BG Name,Channel,Pref Parent,Chan Util,Clients]
=====
[Sector 1]
-----
AP34B8.8314.A204 [0, 0, Default, (36,40), 0000.0000.0000, 5%, 0]
|-APC828.E536.D47C [1, 68, Default, (36,40), 0000.0000.0000, 6%, 0]

Number of Bridge APs : 2
Number of RAPs : 1
Number of MAPs : 1
```

Association de client sur le point d'accès maillé :

```
#show flexconnect client
Flexconnect Clients:
mac radio vap aid state encr aaa-vlan aaa-acl aaa-ipv6-acl assoc auth switching key-method roam key-pro
52:95:C7:EE:B7:E5 0 0 1 FWD AES_CCM128 none none none Local Central Local Other regular No Yes No 0

#show controllers dot11Radio 0 client
mac radio vap aid state encr Maxrate Assoc Cap is_wgb_wired wgb_mac_addr
52:95:C7:EE:B7:E5 0 0 1 FWD AES_CCM128 MCS92SS HE HE false 00:00:00:00:00:00
```

```
#show flexconnect client aaa-override
Flexconnect Clients:
mac vlan qos acl ipv6-acl vlan-name avgdtids avgrtdtids bstdtids bstrtdtids avgdtus avgrtdtus bstdtus bstrtdtus
52:95:C7:EE:B7:E5 none none none none Bridge-VLAN 0 0 0 0 0 0 0 0
```

Le trafic du point d'accès maillé (MAP) est directement ponté vers le commutateur de liaison ascendante, en contournant le point d'accès racine (RAP) :

<#root>

DHCP:

```
May 30 04:25:21 APC828.E536.D47C kernel: [*05/30/2025 04:25:21.2883] [ 62081:607119] [APC828.E536.D47C]
```

[U:C] DHCP_REQUEST : TransId 0x3bcb0a7b

```
May 30 04:25:21 APC828.E536.D47C kernel: [*05/30/2025 04:25:21.2884] chatter: dhcp_req_local_sw_nonat: 1
```

```
May 30 04:25:21 APC828.E536.D47C kernel: [*05/30/2025 04:25:21.2885] [ 62081:607245] [APC828.E536.D47C]
```

[U:C] DHCP_REQUEST : TransId 0x3bcb0a7b

```
May 30 04:25:21 APC828.E536.D47C kernel: [*05/30/2025 04:25:21.2885] chatter: dhcp_reply_nonat: 17485791
```

```
May 30 04:25:21 APC828.E536.D47C kernel: [*05/30/2025 04:25:21.2943] [ 62081:613080] [APC828.E536.D47C]
```

[D:C] DHCP_ACK : TransId 0x3bcb0a7b

```
May 30 04:25:21 APC828.E536.D47C kernel: [*05/30/2025 04:25:21.2943] [ 62081:613123] [APC828.E536.D47C]
```

[D:W] DHCP_ACK : TransId 0x3bcb0a7b

ARP:

May 30 04:31:44 APC828.E536.D47C kernel: [*05/30/2025 04:31:44.0572] [62464:537183] [APC828.E536.D47C]

[U:W] ARP_QUERY : Sender 100.0.0.2 TargIp 100.0.0.1

May 30 04:31:44 APC828.E536.D47C kernel: [*05/30/2025 04:31:44.0572] [62464:537219] [APC828.E536.D47C]

[U:C] ARP_QUERY : Sender 100.0.0.2 TargIp 100.0.0.1

May 30 04:31:44 APC828.E536.D47C kernel: [*05/30/2025 04:31:44.0573] chatter: ethertype_cl1: 1748579504

May 30 04:31:44 APC828.E536.D47C kernel: [*05/30/2025 04:31:44.0628] [62464:542842] [APC828.E536.D47C]

[D:C] ARP_REPLY : Sender 100.0.0.1 HwAddr c4:44:a0:a2:61:d1

May 30 04:31:44 APC828.E536.D47C kernel: [*05/30/2025 04:31:44.0629] chatter: fromdevs_arp_resp: arp rep

May 30 04:31:44 APC828.E536.D47C kernel: [*05/30/2025 04:31:44.0629] [62464:542971] [APC828.E536.D47C]

[D:C] ARP_REPLY : Sender 100.0.0.1 HwAddr c4:44:a0:a2:61:d1

May 30 04:31:44 APC828.E536.D47C kernel: [*05/30/2025 04:31:44.0630] [62464:543018] [APC828.E536.D47C]

[D:W] ARP_REPLY : Sender 100.0.0.1 HwAddr c4:44:a0:a2:61:d1

May 30 04:31:45 APC828.E536.D47C kernel: [*05/30/2025 04:31:45.4301] [62465:910100] [APC828.E536.D47C]

[D:A] ARP_REPLY : Sender 100.0.0.1 HwAddr c4:44:a0:a2:61:d1

ICMP:

May 30 04:32:09 APC828.E536.D47C kernel: [*05/30/2025 04:32:09.3059] [62489:785903] [APC828.E536.D47C]

[U:W] ICMP_ECHO : Id 39016 Seq 0

May 30 04:32:09 APC828.E536.D47C kernel: [*05/30/2025 04:32:09.3059] [62489:785938] [APC828.E536.D47C]

[U:C] ICMP_ECHO : Id 39016 Seq 0

May 30 04:32:09 APC828.E536.D47C kernel: [*05/30/2025 04:32:09.3104] [62489:790444] [APC828.E536.D47C]

[D:C] ICMP_ECHO_REPLY : Id 39016 Seq 0

May 30 04:32:09 APC828.E536.D47C kernel: [*05/30/2025 04:32:09.3105] [62489:790534] [APC828.E536.D47C]

[D:C] ICMP_ECHO_REPLY : Id 39016 Seq 0

May 30 04:32:09 APC828.E536.D47C kernel: [*05/30/2025 04:32:09.3105] [62489:790583] [APC828.E536.D47C]

[D:W] ICMP_ECHO_REPLY : Id 39016 Seq 0

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.