

Configuration du réseau local distant (RLAN) sur le point d'accès Catalyst 9124

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Fond](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configuration AAA](#)

[Configuration RLAN](#)

[Commutation locale FlexConnect RLAN](#)

[Vérifier](#)

[Commutation centrale](#)

[Commutation locale Flex-Connect](#)

Introduction

Ce document décrit comment configurer le réseau local distant (RLAN) sur le modèle AP Catalyst 9124 en utilisant le modèle WLC 9800.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- 9800 WLC
- Accès par interface de ligne de commande (CLI) aux contrôleurs sans fil et aux points d'accès.

Composants utilisés

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

- WLC Catalyst 9800-L version 17.09.05
- AP de la gamme C9124

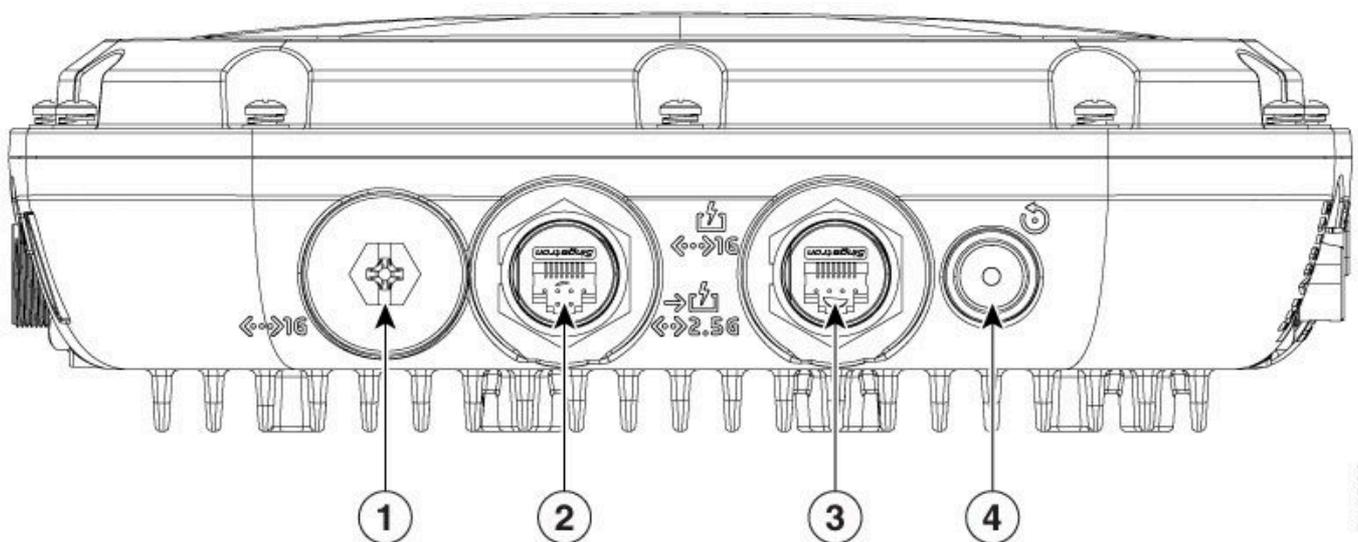
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Fond

Un réseau local distant (RLAN) est utilisé pour authentifier les clients câblés à l'aide du contrôleur. Une fois que le client filaire a réussi à joindre le contrôleur, les ports LAN commutent le trafic entre les modes de commutation central ou local. Le trafic provenant des clients filaires est traité comme du trafic client sans fil. Le RLAN du point d'accès (AP) envoie la demande d'authentification pour authentifier le client filaire. L'authentification des clients filaires dans un réseau local sans fil est similaire à celle du client sans fil authentifié central.

Pour plus d'informations sur le RLAN, consultez le [Guide de configuration du logiciel du contrôleur sans fil de la gamme Cisco Catalyst 9800](#).

RLAN est pris en charge dans les points d'accès qui ont plus d'un port Ethernet et le modèle AP 9124 contient 2 ports Ethernet nommés GigabitEthernet0 et LAN1, étiquetés respectivement comme 2 et 3 dans l'image :



9124 ports Ethernet

Pour plus d'informations sur le matériel, consultez le [Guide d'installation matérielle des points d'accès extérieurs de la gamme Cisco Catalyst 9124AX](#).

Configurer

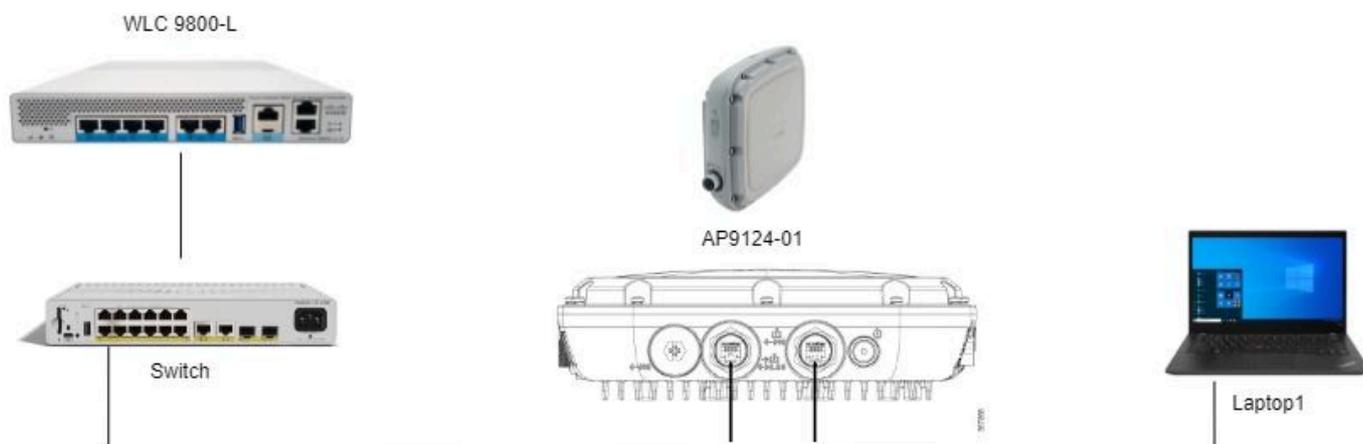
Ce document suppose que l'AP est déjà joint au WLC.

Si vous avez besoin d'aide sur la jonction AP 9124 à WLC, veuillez lire ce guide : [Configure Mesh on Catalyst 9800 Wireless LAN Controllers](#).

Le point d'accès prend en charge le RLAN en mode local et en mode flexible. Si vous avez besoin que le trafic RLAN soit commuté localement, le mode AP doit être Flex et configurer le profil RLAN en conséquence.

Remarque : si vous définissez AP en mode Flex+Bridge, l'AP consigne un message comme : "RLAN_CFG: enable_LAN_port Cannot enable LAN[0]: ClickPort 66: Feature not supported on Mesh".

Diagramme du réseau



Topologie

Configurations

Configuration AAA

1. Dans ce document, la méthode de sécurité pour le RLAN est le filtrage MAC, par conséquent vous devez configurer AAA à l'avance. Vous pouvez avoir les adresses MAC dans un serveur AAA distant ou localement sur le WLC.

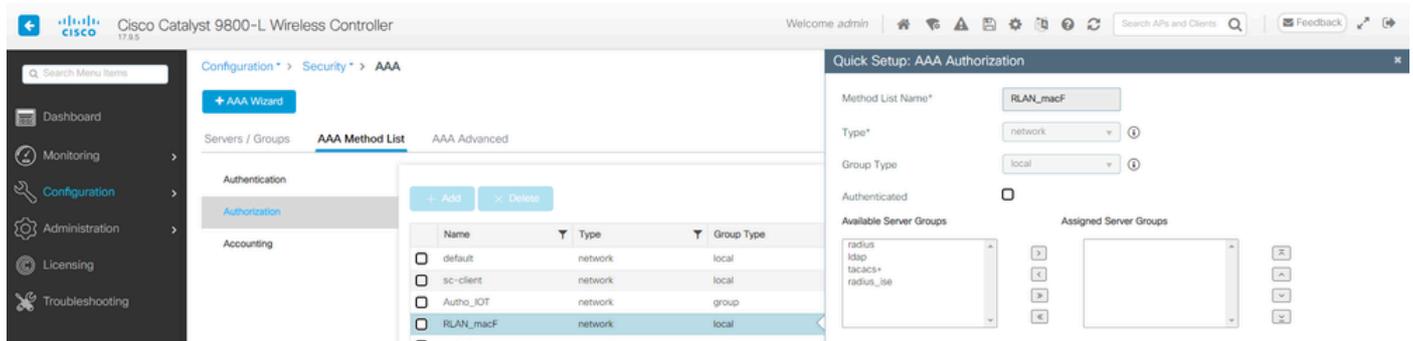
Ici, la base de données WLC locale est utilisée. Ajoutez l'adresse MAC du client sans séparateur, qui est censé se connecter au RLAN à la liste Device Authentication :

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The main page is titled "Configuration > Security > AAA" and is in the "AAA Advanced" section. A "Quick Setup: MAC Filtering" dialog box is open, showing the following fields:

- MAC Address*: f8e43bee53af
- Attribute List Name: None
- Description: RLAN Client
- WLAN Profile Name: Select a value

Buttons for "Cancel" and "Apply to Device" are visible at the bottom of the dialog box.

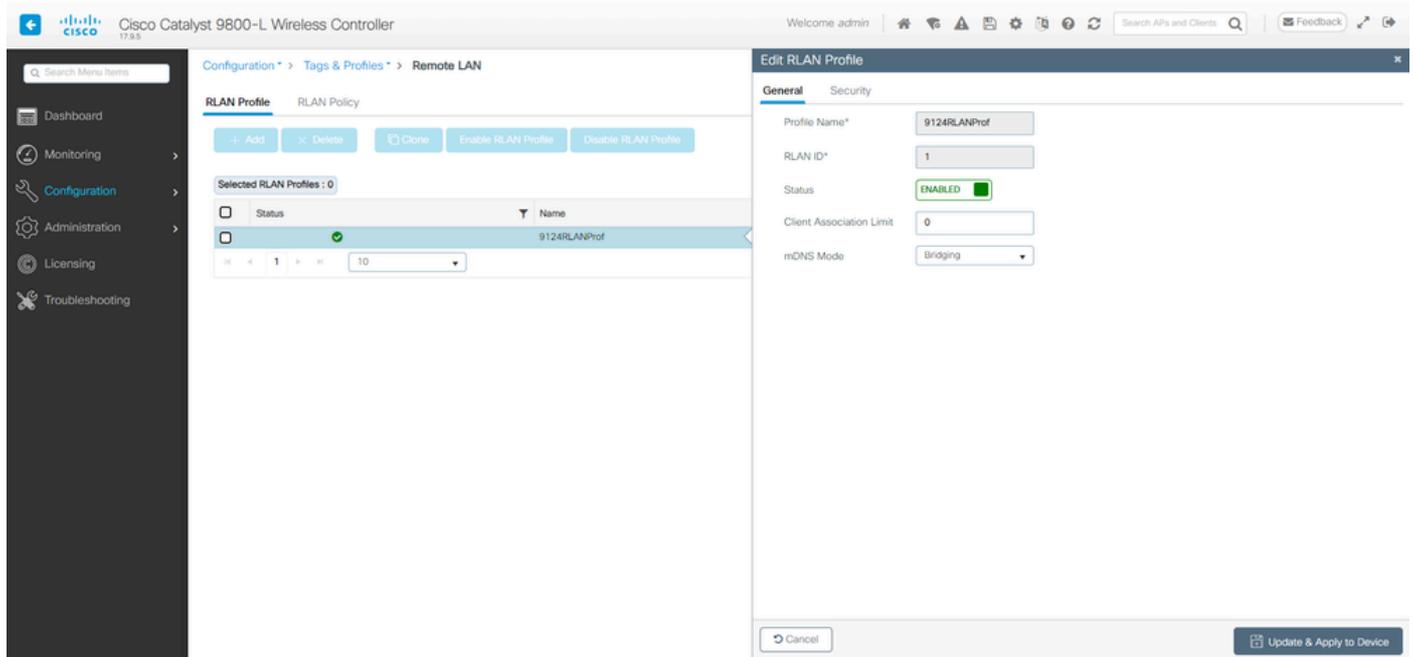
2. Configurez la méthode Authorization pour utiliser la base de données locale. Nommé ici RLAN_macF :



Méthode d'autorisation AAA

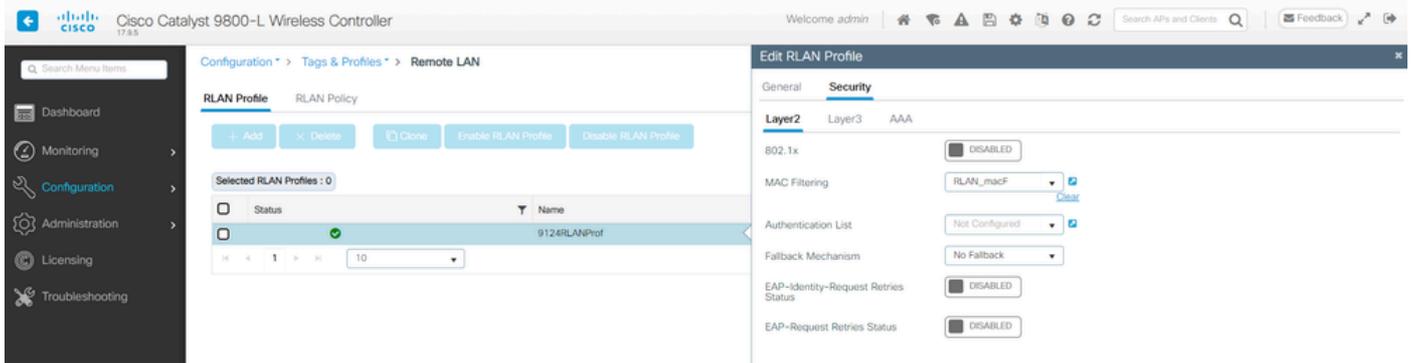
Configuration RLAN

1. Afin de créer un profil RLAN, accédez à Configuration > Wireless > Remote LAN et entrez un nom de profil et un ID RLAN pour le profil RLANP, comme indiqué dans cette image.



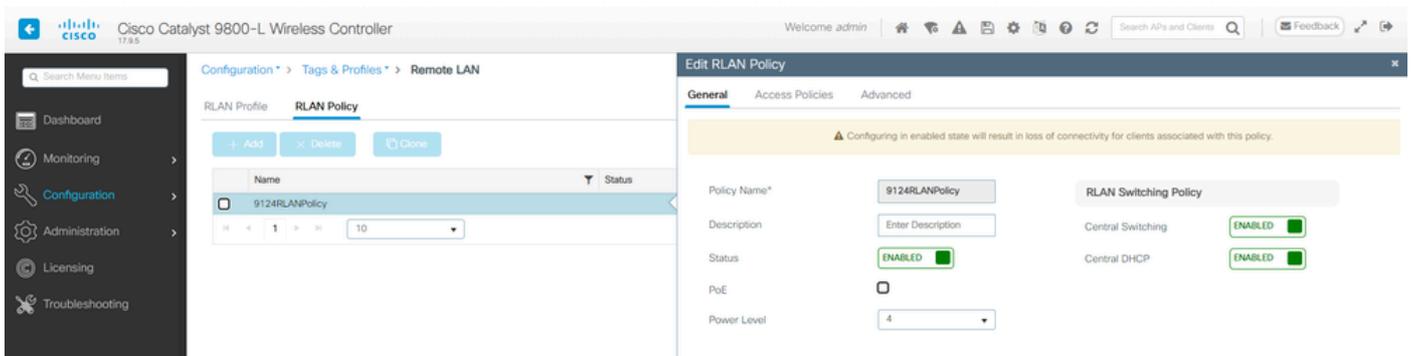
Profil RLAN Général

2. Accédez à Sécurité. Dans cet exemple, la méthode de sécurité utilisée est le filtrage MAC. Accédez à Layer 2, laissez 802.1x à Disabled et sélectionnez la méthode d'autorisation pour le filtrage MAC, comme illustré dans cette image.



Sécurité RLAN

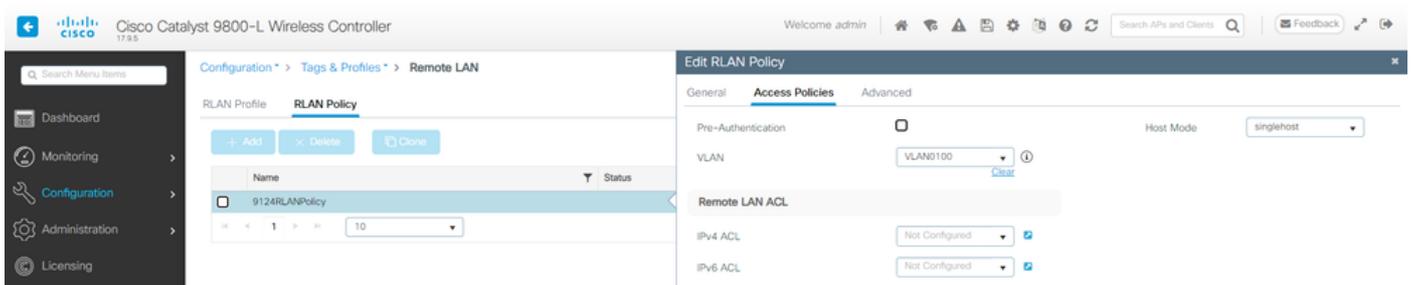
3. Créez la stratégie RLAN. Accédez à Configuration > Wireless > Remote LAN et sur la page Remote LAN, cliquez sur l'onglet RLAN Policy, comme illustré dans cette image.



Politique RLAN

Dans cette configuration, tout le trafic est commuté de manière centrale au niveau du WLC.

4. Accédez à Access Policies et configurez le VLAN et le mode hôte, puis appliquez les paramètres.



Politiques d'accès aux politiques RLAN

5. Créez un PolicyTag et mappez le profil RLAN à la politique RLAN. Accédez à Configuration > Tags & Profiles > Tags.

Edit Policy Tag

Name*

Description

WLAN-POLICY Maps: 0

WLAN Profile	Policy Profile
No items to display	

WLAN-POLICY Maps: 1

Port ID	RLAN Profile	RLAN Policy Profile
<input type="checkbox"/> 1	9124RLANProf	9124RLANPolicy

Map RLAN and Policy

RLAN Profile*

RLAN Policy Profile*

Balise de stratégie

6. Nous devons appliquer la balise de stratégie au point d'accès et activer le port LAN. Accédez à Configuration > Wireless > Access Points et cliquez sur le point d'accès.

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller interface. The main navigation pane on the left includes Dashboard, Monitoring, Configuration, Administration, and Licensing. The main content area is titled 'All Access Points' and shows a table with one AP: AP9124_01, model C9124AXI-B, 2 slots, up time 0 days 1 hrs 26 mins 30 secs, and IP address 192.168.100.1. The 'Edit AP' window is open, showing the 'General' tab. The 'Tags' section is expanded, showing a list of tags with '9124RLANPolTag' selected. Other fields include AP Name (AP9124_01), Location (WGB_LAB_Test), Base Radio MAC (4ca6.4d23.a0e0), and Ethernet MAC (3c57.31c5.ac2c).

Balise de stratégie sur la configuration AP

Appliquez le paramètre et l'AP rejoint à nouveau le WLC. Cliquez sur le point d'accès, puis sélectionnez Interfaces et activez le port LAN dans les paramètres de port LAN.

Edit AP

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

Ethernet Interfaces

Interface	Operation Status	Speed	Rx Packets	Tx Packets	Discarded Packets
GigabitEthernet0		1000 Mbps	22065	12905	0
GigabitEthernet1		Auto	0	0	0
LAN1		Auto	11682	156	0

1 - 3 of 3 items

Radio Interfaces

Slot No	Interface	Band	Admin Status	Operation Status	Spectrum Admin Status	Spectrum Operation Status	Regulatory Domain
0	802.11ax - 2.4 GHz	All	Enabled		Enabled		-A
1	802.11ax - 5 GHz	All	Enabled		Enabled		-B

1 - 2 of 2 items

Power Over Ethernet Settings

Power Type/Mode: PoE/Medium Power (25.5 W)

PoE Pre-Standard Switch: Disabled

PoE Power Injector MAC Address: Disabled

LAN Port Settings

Port ID	Status	VLAN ID	PoE	Power Level	RLAN
LAN1	<input checked="" type="checkbox"/>	100	<input type="checkbox"/>	NA	

1 - 1 of 1 items

Paramètres du port LAN1 AP

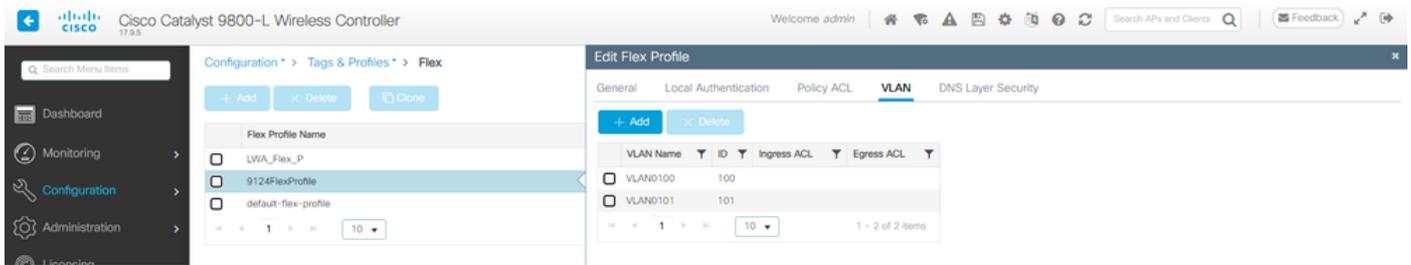
Appliquez les paramètres et vérifiez l'état. Assurez-vous que le RLAN est vert.

Commutation locale FlexConnect RLAN

Si vous avez besoin que le trafic RLAN soit commuté localement, le mode AP doit être Flex et configurer le profil RLAN en conséquence.

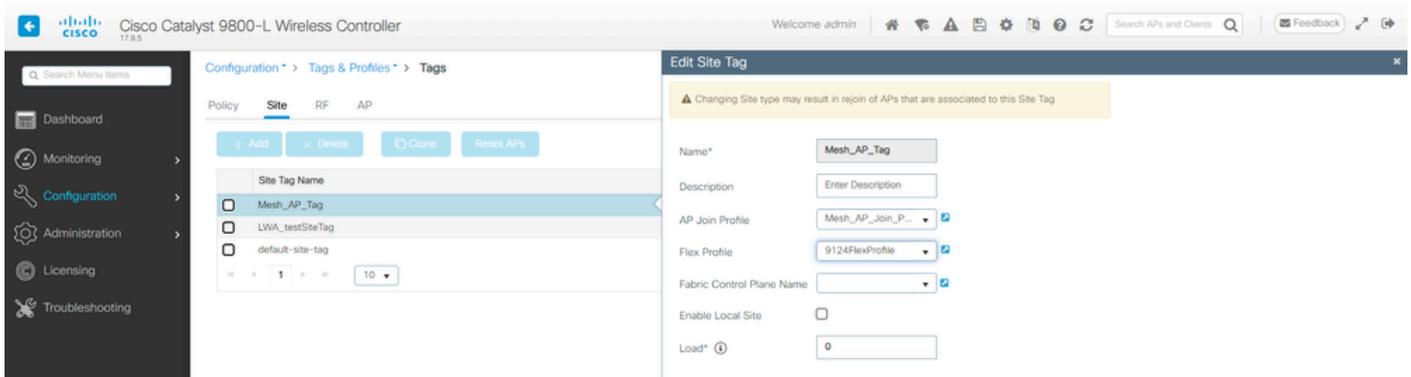
Remarque : si vous définissez AP comme mode Flex+Bridge, l'AP enregistre un message comme : "RLAN_CFG: enable_LAN_port Cannot enable LAN[0]: ClickPort 66: Feature not supported on Mesh".

1. Commencez par la configuration Flex Profile à appliquer à la balise de site. Assurez-vous de configurer le bon VLAN natif et poussez le bon VLAN client vers le point d'accès Flex.



Configuration du profil flexible

2. Pour passer le point d'accès 9124 en mode FlexConnect, vous devez désactiver l'option "Enable Local Site" dans la configuration Site Tag. Ensuite, l'option permettant de sélectionner le profil flexible apparaît. Sélectionnez le profil flexible configuré précédemment :



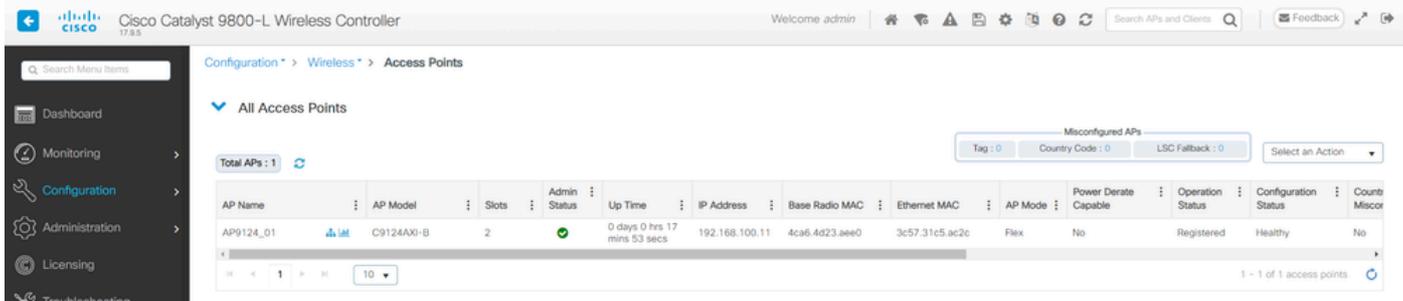
Balise de site Désactiver le site local

Une fois que vous avez cliqué sur Update and Apply to Device, la console AP enregistre :

```
[*08/29/2024 08:25:13.2976] Previous AP mode is 0, change to 2
[*08/29/2024 08:25:13.3213] DOT11_CFG[0] Radio Mode is changed from Local to FlexConnect
[*08/29/2024 08:25:13.3219] DOT11_DRV[0]: Stop Radio0 - Begin
[*08/29/2024 08:25:13.3237] wlan: [0:I:CMN_MLME] mlme_ext_vap_down: VAP (mon0) is down
[*08/29/2024 08:25:13.3262] DOT11_DRV[0]: Stop Radio0 - End
[*08/29/2024 08:25:13.3263] DOT11_CFG[0]: Starting radio 0
[*08/29/2024 08:25:13.3268] DOT11_DRV[0]: Start Radio0 - Begin
[*08/29/2024 08:25:13.3434] DOT11_DRV[0]: Start Radio0 - End
[*08/29/2024 08:25:13.3522] wlan: [0:I:CMN_MLME] mlme_ext_vap_up: VAP (mon0) is up
[*08/29/2024 08:25:13.3756] DOT11_CFG[1] Radio Mode is changed from Local to FlexConnect
[*08/29/2024 08:25:13.3920] DOT11_DRV[1]: Stop Radiol - Begin
[*08/29/2024 08:25:13.3940] wlan: [0:I:CMN_MLME] mlme_ext_vap_down: VAP (mon1) is down
[*08/29/2024 08:25:13.3963] DOT11_DRV[1]: Stop Radiol - End
[*08/29/2024 08:25:13.3964] DOT11_CFG[1]: Starting radio 1
[*08/29/2024 08:25:13.3969] DOT11_DRV[1]: Start Radiol - Begin
[*08/29/2024 08:25:13.3980] DOT11_DRV[1]: Start Radiol - End
[*08/29/2024 08:25:13.4143] wlan: [0:I:CMN_MLME] mlme_ext_vap_up: VAP (mon1) is up
```

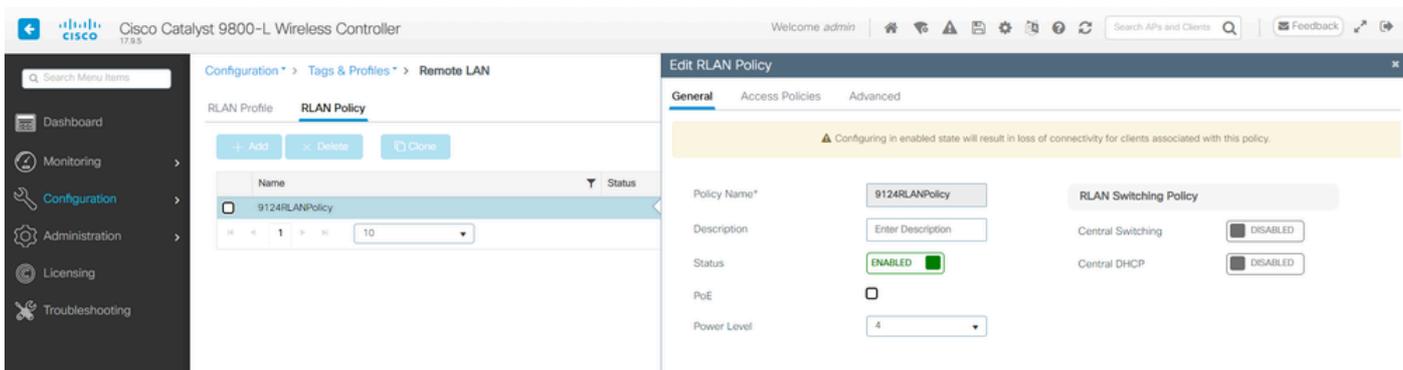
Changement du mode AP Local en Flex

Et l'AP affiche maintenant Flex comme AP Mode :



Remarque : lorsque nous déplaçons l'AP du mode local au mode flexible, l'AP ne se recharge PAS, mais lorsque nous passons du mode flexible au mode local, l'AP se recharge.

3. Accédez à Configuration > Tags & Profiles > Remote LAN > RLAN Policy et modifiez la stratégie de commutation RLAN pour la commutation locale. Désactiver la commutation centrale et le DHCP central :



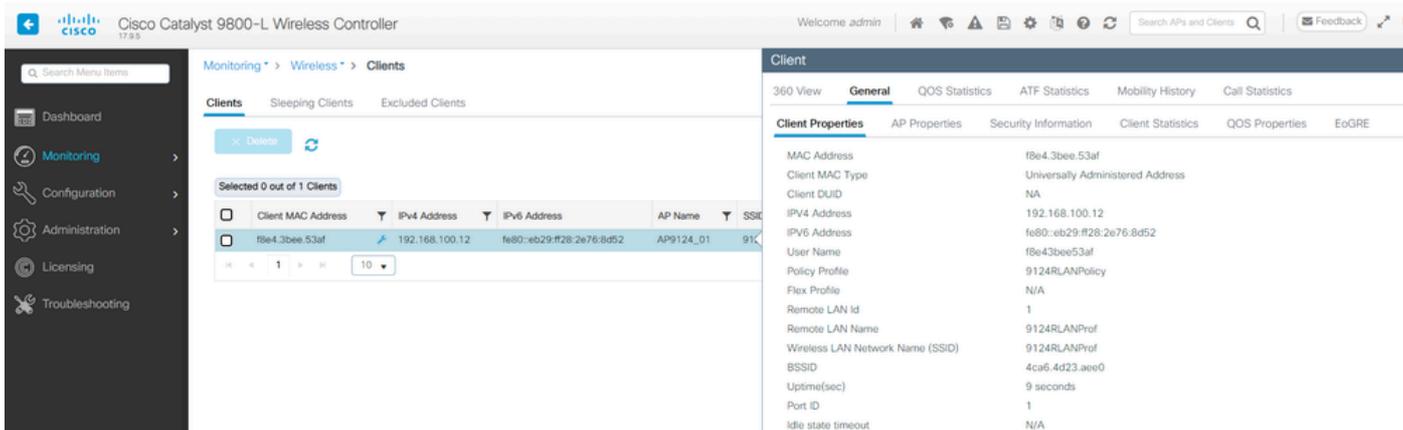
Stratégie RLAN Commutation locale

Vérifier

Commutation centrale

Connectez un PC au port LAN1 du point d'accès. Le PC s'authentifie via MAB et obtient une adresse IP du VLAN configuré.

Accédez à Monitoring > Wireless > Clients pour vérifier l'état du client.



Détails du client

À partir de l'interface de ligne de commande AP, vous pouvez afficher le changement d'état du port et les détails du client :

```
AP9124_01#debug client F8:E4:3B:EE:53:AF
AP9124_01#debug rlan
critical Enable RLAN critical level debugging
errors Enable RLAN error level debugging
events Enable RLAN event level debugging
info Enable RLAN info level debugging
```

```
AP9124_01#show wired clients
Total wired clients: 1
mac port state local_client detect_ago associated_ago tx_pkts tx_bytes rx_pkts rx_bytes
F8:E4:3B:EE:53:AF 2 ASSOCIATED No 12 12 9 1074 337 55639
```

```
AP9124_01#debug rlan info
AP9124_01#debug rlan eve
AP9124_01#debug client F8:E4:3B:EE:53:AF
AP9124_01#[*08/29/2024 08:51:12.7861] chatter: wiredif_mapper :: WiredIfMapper - Invalid Port 2 State 1
[*08/29/2024 08:51:12.7861] chatter: Device wired2 notify state change link UP
[*08/29/2024 08:51:13.3611] RLAN_EVENT-RlanPortControl: LAN-Port[0] UP Event
[*08/29/2024 08:51:16.8306] RLAN_EVENT-RlanPortControl: LAN-Port[0] Detect client F8:E4:3B:EE:53:AF
[*08/29/2024 08:51:16.8307] RLAN_EVENT-RlanPortControl: LAN-Port[0] send_assoc for client F8:E4:3B:EE:53:AF
[*08/29/2024 08:51:16.8308] CLSM[F8:E4:3B:EE:53:AF]: US Assoc Req(0) IF 5 slot 16 port_id 0 vap_id 0 Len 52 client state UNASSOC
[*08/29/2024 08:51:16.8309] CLSM[F8:E4:3B:EE:53:AF]: client moved from UNASSOC to ASSOC
[*08/29/2024 08:51:16.8341] CLSM[F8:E4:3B:EE:53:AF]: DS Assoc Resp(10) IF 87 slot 16 vap 0 state ASSOC
[*08/29/2024 08:51:16.8372] CLSM[F8:E4:3B:EE:53:AF]: Added to ClientIPTable on wired2
[*08/29/2024 08:51:16.8375] RLAN_CFG: rlan_add_client client F8:E4:3B:EE:53:AF, port 0 vlan: 0
[*08/29/2024 08:51:16.8377] CLSM[F8:E4:3B:EE:53:AF]: Add RLAN client succeeded in vap 0
[*08/29/2024 08:51:16.8378] CLSM[F8:E4:3B:EE:53:AF]: client moved from ASSOC to FWD
[*08/29/2024 08:51:16.8379] CLSM[F8:E4:3B:EE:53:AF]: Added to WCP client table AID 0 Radio 16 Vap 0
[*08/29/2024 08:51:16.8381] CLSM[F8:E4:3B:EE:53:AF]: Decoding TLV_CLIENTCAPABILITYPAYLOAD: capbaility: 0 Apple Client: No
[*08/29/2024 08:51:18.0620] chatter: eap_from_cli: 60 | 4ca64d23 aee0f8e4 3bee53af 888e0101 00000000 00000000 00000000 00000000 00000000 0000
0000 00000000 00000000 00000000 00000000
[*08/29/2024 08:51:19.6631] chatter: ethertype_c11: 1724921479.663102627: arp who-has 169.254.233.120 tell 0.0.0.0
[*08/29/2024 08:51:20.6609] chatter: ethertype_c11: 1724921480.660846272: arp who-has 169.254.233.120 tell 0.0.0.0
[*08/29/2024 08:51:21.1727] chatter: dhcp_from_inet: 1724921481.172667939: 0.0.0.0.68 > 255.255.255.255.67: udp 309
[*08/29/2024 08:51:21.1746] chatter: dhcp_reply_nonat: 1724921481.174640751: 192.168.101.1.67 > 192.168.101.11.68: udp 308
[*08/29/2024 08:51:21.2150] chatter: ethertype_c11: 1724921481.215028303: arp who-has 192.168.101.1 tell 192.168.101.11
[*08/29/2024 08:51:21.5063] chatter: ethertype_c11: 1724921481.506300855: arp who-has 192.168.101.1 tell 192.168.101.11
[*08/29/2024 08:51:21.6544] chatter: ethertype_c11: 1724921481.654387730: arp who-has 192.168.101.11 tell 0.0.0.0
[*08/29/2024 08:51:22.6518] chatter: ethertype_c11: 1724921482.651782313: arp who-has 192.168.101.11 tell 0.0.0.0
[*08/29/2024 08:51:23.0676] chatter: eap_from_cli: 60 | 4ca64d23 aee0f8e4 3bee53af 888e0101 00000000 00000000 00000000 00000000 0000
0000 00000000 00000000 00000000 00000000
[*08/29/2024 08:51:23.6552] chatter: ethertype_c11: 1724921483.655126375: arp who-has 192.168.101.11 tell 0.0.0.0
[*08/29/2024 08:51:24.6645] chatter: ethertype_c11: 1724921484.664425489: arp who-has 192.168.101.11 tell 192.168.101.11
```

Commutation locale Flex-Connect

```
AP9124_01#[*08/28/2024 14:16:30.7138] chatter: wiredif_mapper :: WiredIfMapper - Invalid Port 2 State 1
[*08/28/2024 14:16:30.7138] chatter: Device wired2 notify state change link UP
[*08/28/2024 14:16:30.9659] RLAN_EVENT-RlanPortControl: LAN-Port[0] UP Event
[*08/28/2024 14:16:33.2574] RLAN_EVENT-RlanPortControl: LAN-Port[0] Detect client F8:E4:3B:EE:53:AF
[*08/28/2024 14:16:33.2574] RLAN_EVENT-RlanPortControl: LAN-Port[0] send_assoc for client F8:E4:3B:EE:53:AF
[*08/28/2024 14:16:33.2576] CLSM[F8:E4:3B:EE:53:AF]: US Assoc Req(0) IF 5 slot 16 port_id 0 vap_id 0 Len 52 client state UNASSOC
[*08/28/2024 14:16:33.2576] CLSM[F8:E4:3B:EE:53:AF]: client moved from UNASSOC to ASSOC
[*08/28/2024 14:16:33.2619] CLSM[F8:E4:3B:EE:53:AF]: DS Assoc Resp(10) IF 87 slot 16 vap 0 state ASSOC
[*08/28/2024 14:16:33.2654] CLSM[F8:E4:3B:EE:53:AF]: Added to ClientIPTable on wired2
[*08/28/2024 14:16:33.2657] RLAN_CFG: rlan_add_client client F8:E4:3B:EE:53:AF, port 0 vlan: 101
[*08/28/2024 14:16:33.2659] CLSM[F8:E4:3B:EE:53:AF]: Add RLAN client succeeded in vap 0
[*08/28/2024 14:16:33.2660] CLSM[F8:E4:3B:EE:53:AF]: client moved from ASSOC to FWD
[*08/28/2024 14:16:33.2661] CLSM[F8:E4:3B:EE:53:AF]: Added to WCP client table AID 0 Radio 16 Vap 0
[*08/28/2024 14:16:33.2664] CLSM[F8:E4:3B:EE:53:AF]: ADD_CENTRAL_AUTH_INFO_MOBILE Payload
[*08/28/2024 14:16:33.2667] CLSM[F8:E4:3B:EE:53:AF]: TLV_FLEX_CENTRAL_AUTH_STA_PAYLOAD
[*08/28/2024 14:16:33.2669] CLSM[F8:E4:3B:EE:53:AF]: Decoding TLV_CLIENTCAPABILITYPAYLOAD: capbaility: 0 Apple Client: No
[*08/28/2024 14:16:35.4185] chatter: eap_from_cli: 60 | 4ca64d23 aee0f8e4 3bee53af 888e0101 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
[*08/28/2024 14:16:35.7577] chatter: dhcp_req_local_sw_nonat: 1724854595.757647899: 0.0.0.0.68 > 255.255.255.255.67: udp 345
[*08/28/2024 14:16:35.7618] chatter: dhcp_from_inet: 1724854595.761843211: 192.168.101.1.67 > 192.168.101.11.68: udp 308
[*08/28/2024 14:16:35.7619] chatter: dhcp_reply_nonat: 1724854595.761843211: 192.168.101.1.67 > 192.168.101.11.68: udp 308
[*08/28/2024 14:16:35.7834] chatter: ethertype_c11: 1724854595.783373680: arp who-has 192.168.101.1 tell 192.168.101.11
[*08/28/2024 14:16:35.7844] chatter: fromdevs_arp_resp: arp reply 192.168.101.1 is-at 64:8F:3E:D5:E5:C1
[*08/28/2024 14:16:36.0169] chatter: ethertype_c11: 1724854596.016884669: arp who-has 192.168.101.11 tell 0.0.0.0
[*08/28/2024 14:16:36.0537] chatter: fromdevs_arp_resp: arp reply 192.168.101.1 is-at 64:8F:3E:D5:E5:C1
[*08/28/2024 14:16:37.0143] chatter: ethertype_c11: 1724854597.014276961: arp who-has 169.254.233.120 tell 0.0.0.0
[*08/28/2024 14:16:38.0098] chatter: ethertype_c11: 1724854598.009745033: arp who-has 169.254.233.120 tell 0.0.0.0
[*08/28/2024 14:16:39.0159] chatter: ethertype_c11: 1724854599.015890970: arp who-has 169.254.233.120 tell 0.0.0.0
[*08/28/2024 14:16:40.4324] chatter: eap_from_cli: 60 | 4ca64d23 aee0f8e4 3bee53af 888e0101 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
[*08/28/2024 14:16:41.0055] chatter: ethertype_c11: 1724854601.005426230: arp who-has 192.168.101.11 tell 192.168.101.11
[*08/28/2024 14:16:44.5998] chatter: ethertype_c11: 1724854604.599751802: arp who-has 192.168.101.1 tell 192.168.101.11
[*08/28/2024 14:16:44.6010] chatter: fromdevs_arp_resp: arp reply 192.168.101.1 is-at 64:8F:3E:D5:E5:C1
[*08/28/2024 14:16:50.5117] chatter: ethertype_c11: 1724854610.511644351: arp who-has 192.168.101.1 (64:8F:3E:D5:E5:C1) tell 192.168.101.11
[*08/28/2024 14:16:50.5129] chatter: fromdevs_arp_resp: arp reply 192.168.101.1 is-at 64:8F:3E:D5:E5:C1
[*08/28/2024 14:16:56.0159] chatter: ethertype_c11: 1724854616.015864610: arp who-has 192.168.101.1 (64:8F:3E:D5:E5:C1) tell 192.168.101.11
[*08/28/2024 14:16:56.0181] chatter: fromdevs_arp_resp: arp reply 192.168.101.1 is-at 64:8F:3E:D5:E5:C1
[*08/28/2024 14:17:01.5107] chatter: ethertype_c11: 1724854621.510631795: arp who-has 192.168.101.1 (64:8F:3E:D5:E5:C1) tell 192.168.101.11
[*08/28/2024 14:17:01.5118] chatter: fromdevs_arp_resp: arp reply 192.168.101.1 is-at 64:8F:3E:D5:E5:C1
[*08/28/2024 14:17:07.5075] chatter: ethertype_c11: 1724854627.507420491: arp who-has 192.168.101.1 (64:8F:3E:D5:E5:C1) tell 192.168.101.11
[*08/28/2024 14:17:07.5086] chatter: fromdevs_arp_resp: arp reply 192.168.101.1 is-at 64:8F:3E:D5:E5:C1
[*08/28/2024 14:17:11.3535] chatter: ethertype_c11: 1724854631.353461218: arp who-has 192.168.101.1 tell 192.168.101.11
[*08/28/2024 14:17:11.3550] chatter: fromdevs_arp_resp: arp reply 192.168.101.1 is-at 64:8F:3E:D5:E5:C1
[*08/28/2024 14:17:16.0084] chatter: ethertype_c11: 1724854636.008371529: arp who-has 192.168.101.1 (64:8F:3E:D5:E5:C1) tell 192.168.101.11
[*08/28/2024 14:17:16.0098] chatter: fromdevs_arp_resp: arp reply 192.168.101.1 is-at 64:8F:3E:D5:E5:C1
```

Débugages pour RLAN commuté local

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.