

# Configuration et intégration des points d'accès sur un commutateur EWC non-SDA (C9800-SW)

## Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérifier](#)

[Dépannage](#)

[Débogage conditionnel et traçage Radio Active](#)

[Exemple d'une jointure AP réussie](#)

## Introduction

Ce document décrit le processus d'intégration et de provisionnement d'un point d'accès (AP) avec un contrôleur sans fil intégré sur un commutateur Catalyst 9000 (Catalyst 9K) (EWC-Switch) dans des déploiements non SDA (il n'y a pas de Cisco DNA Center en cours d'utilisation).

## Conditions préalables

### Exigences

Vous devez remplir les conditions suivantes :

- Installez le sous-package sans fil sur le commutateur Catalyst 9K qui jouera le rôle de contrôleur LAN sans fil (WLC).
- Assurez-vous que l'interface de bouclage est configurée pour être configurée en tant qu'interface de gestion sans fil (WMI).
- Assurez-vous que l'accès à l'interface graphique du commutateur Catalyst 9K est activé, car la configuration via l'interface graphique est recommandée.

**Remarque** : le commutateur EWC-Switch sur les déploiements non SDA est uniquement pris en charge dans les versions 17.3.X.

## Composants utilisés

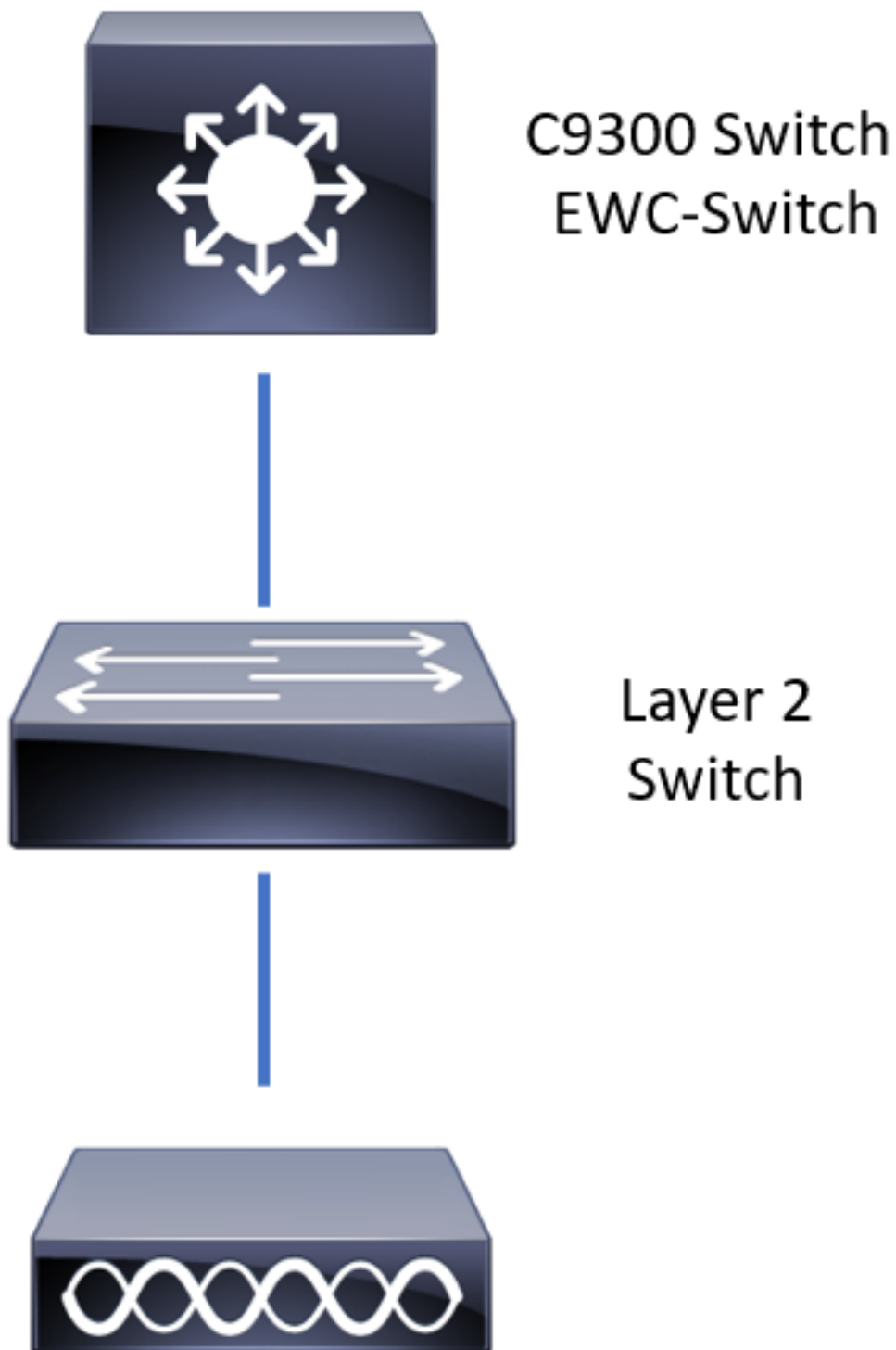
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Commutateur C9300-24P, Cisco IOS® XE Version 17.3.4
- Sous-package sans fil pour la version 17.3.4
- POINT D'ACCÈS C9120-AX

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

### Diagramme du réseau



Les points d'accès peuvent être connectés directement au commutateur EWC, mais ce n'est pas obligatoire. Il est recommandé d'utiliser un commutateur d'accès pour brancher des points d'accès afin de permettre un basculement haute disponibilité (HA) en cas de panne du commutateur EWC actif.

## Configurations

**Étape 1.** Configurez le code de pays pour les emplacements géographiques où les points d'accès seront déployés. Ceci est obligatoire afin de permettre aux AP de s'enregistrer et de garantir la conformité avec les directives du domaine réglementaire pour le pays dans lequel ils sont

déployés. Dans l'interface graphique utilisateur, accédez à **Configuration > Wireless > Access Points** et cliquez sur l'onglet **Country**. Choisissez tous les **codes de pays** applicables pour correspondre aux domaines réglementaires des points d'accès.

**Remarque** : dans les versions 17.3.1 à 17.3.3, l'interface utilisateur graphique du commutateur EWC répertorie les codes de pays, mais n'applique aucune sélection tant qu'un code de pays n'a pas été ajouté via l'interface de ligne de commande (CLI), comme indiqué dans l>ID de bogue Cisco [CSCvw20478](#). Une fois qu'un code de pays est configuré, vous pouvez en ajouter d'autres via l'interface utilisateur graphique.

Configuration > Wireless > Access Points

> All Access Points

> 5 GHz Radios

> 2.4 GHz Radios

> Dual-Band Radios

▼ Country

[Click here](#) for list of access point models and protocols supported per country and regulatory domain.

Selected Country MX, US

Apply

Regulatory Domain

802.11a/n/ac: [ Indoor: -ABN, Outdoor: -ABN ]

802.11b/g/n: [ Indoor: -A, Outdoor: -ABN ]

Search

	Country Code	Name
<input type="checkbox"/>	MX	Mexico
<input type="checkbox"/>	MO	Macau
<input type="checkbox"/>	MT	Malta
<input checked="" type="checkbox"/>	MX	Mexico
<input type="checkbox"/>	MY	Malaysia
<input type="checkbox"/>	NG	Nigeria
<input type="checkbox"/>	NL	Netherlands
<input type="checkbox"/>	NO	Norway

Configuration CLI (17.3.1 à 17.3.3) :

```
9300-1#configure terminal
9300-1(config)#ap dot11 5ghz shutdown
Disabling the 802.11a network may strand mesh APs.
Are you sure you want to continue? (y/n)[y]: y
9300-1(config)#ap dot11 24ghz shutdown
Disabling the 802.11b network may strand mesh APs.
Are you sure you want to continue? (y/n)[y]: y
9300-1(config)#wireless country MX
9300-1(config)#no ap dot11 5ghz shutdown
9300-1(config)#no ap dot11 24ghz shutdown
```

**Étape 2.** Activez la fonctionnalité de contrôleur sans fil et configurez le VLAN dans lequel les AP résideront. Accédez à **Configuration > Embedded Wireless Setup**, faites glisser **Embedded Wireless Setup** vers Enabled et sous **Location Configuration**, cliquez sur **+ Add**.

Configuration > Embedded Wireless Setup

Embedded Wireless Setup  DISABLED [Apply](#)

Location Configuration

[+ Add](#)

No locations available

Lorsque la fonction de configuration sans fil intégrée est activée, ces commandes sont transmises à l'interface de ligne de commande. Ces interfaces de ligne de commande activent le fabric lisp sur le commutateur Catalyst 9K, de sorte qu'il servira de noeud de plan de contrôle/serveur de mappage, de contrôleur sans fil avec bouclage en tant que WMI et WLC pour le mappage de plan de contrôle afin de permettre aux points d'accès et aux clients d'être intégrés.

```
9300-1(config)#router lisp
9300-1(config-router-lisp)# locator-table default
9300-1(config-router-lisp)# locator-set rloc_ewlc
9300-1(config-router-lisp-locator-set)# IPv4-interface Loopback0
9300-1(config-router-lisp-locator-set)# auto-discover-rlocs
9300-1(config-router-lisp-locator-set)# exit-locator-set
9300-1(config-router-lisp)# locator-set WLC
9300-1(config-router-lisp-locator-set)#
```

```
9300-1(config-router-lisp-locator-set)# exit-locator-set
9300-1(config-router-lisp)# service ipv4
9300-1(config-lisp-srv-ipv4)# encapsulation vxlan
9300-1(config-lisp-srv-ipv4)# itr map-resolver
```

```
9300-1(config-lisp-srv-ipv4)# etr map-server
```

```
9300-1(config-lisp-srv-ipv4)# etr map-server
```

```
9300-1(config-lisp-srv-ipv4)# etr
9300-1(config-lisp-srv-ipv4)# sgt
9300-1(config-lisp-srv-ipv4)# no map-cache away-eids send-map-request
9300-1(config-lisp-srv-ipv4)# proxy-etr
9300-1(config-lisp-srv-ipv4)# proxy-itr
```

```
9300-1(config-lisp-srv-ipv4)# map-server
9300-1(config-lisp-srv-ipv4)# map-resolver
9300-1(config-lisp-srv-ipv4)# exit-service-ipv4
9300-1(config-router-lisp)# service ethernet
9300-1(config-lisp-srv-eth)# itr map-resolver
```

```
9300-1(config-lisp-srv-eth)# itr
9300-1(config-lisp-srv-eth)# etr map-server
```

```
9300-1(config-lisp-srv-eth)# etr map-server
```

```
9300-1(config-lisp-srv-eth)# etr
9300-1(config-lisp-srv-eth)# map-server
9300-1(config-lisp-srv-eth)# map-resolver
9300-1(config-lisp-srv-eth)# exit-service-ethernet
9300-1(config-router-lisp)# ipv4 source-locator Loopback0
9300-1(config-router-lisp)# map-server session passive-open WLC
9300-1(config-router-lisp)# exit
```

```
9300-1(config)# interface LISP0
9300-1(config-if)# exit
```

```
9300-1(config)# router lisp
9300-1(config-router-lisp)# site site_uci
9300-1(config-router-lisp-site)# description map-server configured from Wireless LAN Controller
9300-1(config-router-lisp-site)# authentication-key
```

```
9300-1(config-router-lisp-site)# exit-site
9300-1(config-router-lisp)# exit-router-lisp
```

```
9300-1(config)# ip dhcp relay information option
9300-1(config)# wireless fabric
9300-1(config)# wireless management interface Loopback0
9300-1(config-mgmt-interface)# exit
```

```
9300-1(config)# wireless fabric control-plane default-control-plane
9300-1(config-wireless-cp)# ip address
```

```
9300-1(config-wireless-cp)# exit
```

**Étape 3.** Dans la fenêtre contextuelle générée après l'étape 2, dans l'onglet **General**, entrez le nom de l'**emplacement et les détails d'intégration de l'AP** comme le VLAN et le masque de sous-réseau. Par défaut, le champ VLAN est pré-rempli avec 2045. Un ID de VLAN différent est autorisé, mais l'ID de VLAN doit être compris entre 2045 et 4094 et doit être indépendant du trafic client (aucun client filaire ou sans fil n'est autorisé à utiliser ce VLAN). Une fois les détails terminés, cliquez sur **Apply**

Configuration > Embedded Wireless Setup

Location Configuration

← Back

General Wireless Networks AP Provisioning

Location Name*	EWC-Location	AP Onboarding	
Description	Enter Description	VLAN*	2674
Client Density	Low Typical High	IP Address*	172.16.80.1
		Subnet Mask*	255.255.255.0
		DHCP Server*	172.16.80.1

Apply

Ceci crée le VLAN pour les AP, une SVI pour ce VLAN AP (passerelle par défaut pour les AP), l'emplacement AP, les balises Policy et RF, et les identificateurs de réseau virtuel (VNID) L2 et L3. Il s'agit des commandes affichées dans l'interface de ligne de commande à la suite de l'étape 3.

```
9300-1(config)# interface LISP0.4097
9300-1(config-subif)# router lisp
9300-1(config-router-lisp)# locator-set rloc_ewlc
9300-1(config-router-lisp-locator-set)# exit-locator-set
9300-1(config-router-lisp)# instance-id 4097
9300-1(config-lisp-inst)# remote-rloc-probe on-route-change
9300-1(config-lisp-inst)# dynamic-eid APONBOARDING_0_2674_4097_8188
9300-1(config-lisp-inst-dyn-eid)# database-mapping 172.16.80.0/24 locator-set rloc_ewlc
9300-1(config-lisp-inst-dyn-eid)# exit-dynamic-eid
9300-1(config-lisp-inst)# service ipv4
9300-1(config-lisp-inst-srv-ipv4)# eid-table default
9300-1(config-lisp-inst-srv-ipv4)# map-cache 172.16.80.0/24 map-request
9300-1(config-lisp-inst-srv-ipv4)# route-export site-registrations
9300-1(config-lisp-inst-srv-ipv4)# distance site-registrations 250
9300-1(config-lisp-inst-srv-ipv4)# map-cache site-registration
9300-1(config-lisp-inst-srv-ipv4)# exit-service-ipv4
9300-1(config-lisp-inst)# exit-instance-id
9300-1(config-router-lisp)# instance-id 8188
9300-1(config-lisp-inst)# remote-rloc-probe on-route-change
9300-1(config-lisp-inst)# service ethernet
```

```

9300-1(config-lisp-inst-srv-eth)# eid-table vlan 2674
9300-1(config-lisp-inst-srv-eth)# database-mapping mac locator-set rloc_ewlc
9300-1(config-lisp-inst-srv-eth)# exit-service-ethernet
9300-1(config-lisp-inst)# exit-instance-id
9300-1(config-router-lisp)# site site_uci
9300-1(config-router-lisp-site)# eid-record instance-id 4097 172.16.80.0/24 accept-more-
specifics
9300-1(config-router-lisp-site)# eid-record instance-id 8188 any-mac
9300-1(config-router-lisp-site)# exit-site
9300-1(config-router-lisp)# exit

9300-1(config)# vlan 2674
9300-1(config-vlan)# name AP_VLAN2674
9300-1(config-vlan)# exit

9300-1(config)# interface Vlan2674
9300-1(config-if)# description APONBOARDING_0_2674_4097_8188
9300-1(config-if)# mac-address 0000.0C9F.FAD1
9300-1(config-if)# ip address 172.16.80.1 255.255.255.0
9300-1(config-if)# ip helper-address 172.16.80.1
9300-1(config-if)# no ip redirects
9300-1(config-if)# ip route-cache same-interface
9300-1(config-if)# no lisp mobility liveness test
9300-1(config-if)# ip directed-broadcast
9300-1(config-if)# lisp mobility APONBOARDING_0_2674_4097_8188
9300-1(config-if)#exit

9300-1(config)# wireless fabric name APONBOARDING_0_2674_4097_8188 12-vnid 8188 13-vnid 4097 ip
172.16.80.0 255.255.255.

```

**Étape 4.** Configurez le commutateur Catalyst 9K pour qu'il agisse également en tant que serveur DHCP pour le VLAN AP et créez les pools DHCP correspondants. Accédez à **Administration > DHCP Pools** et cliquez sur **+ Add**. Définissez un nom de pool et des paramètres réseau, assurez-vous que la passerelle par défaut est définie sur l'adresse IP SVI ; sinon, les points d'accès rejoignent partiellement le contrôleur.

Create DHCP Pool
✕

Basic     Advanced

DHCP Pool Name\*  (1-236 Characters)

IP Type

Network\*

Subnet Mask\*

Starting ip\*

Ending ip\*

Reserved Only  DISABLED

Lease\*

(0-365 days)
 (0-23 hours)
 (0-59 minutes)

↶ Cancel

📄 Apply to Device



Create DHCP Pool Basic  Advanced

Enable DNS Proxy

Default Router(s)  +

DNS Server(s)  +

IP Address	Remove
172.16.80.1	×
No items to display	

NetBios Name Server(s)  +

Domain

IP Address	Remove
No items to display	

DHCP Options List

Cancel Apply to Device

### Configuration CLI :

```
9300-1#configure terminal
9300-1(config)#ip dhcp excluded-address 172.16.80.0 172.16.80.9
9300-1(config)#ip dhcp pool
```

```
9300-1(dhcp-config)#network 172.16.80.0 255.255.255.0
9300-1(dhcp-config)#default-router 172.16.80.1
```

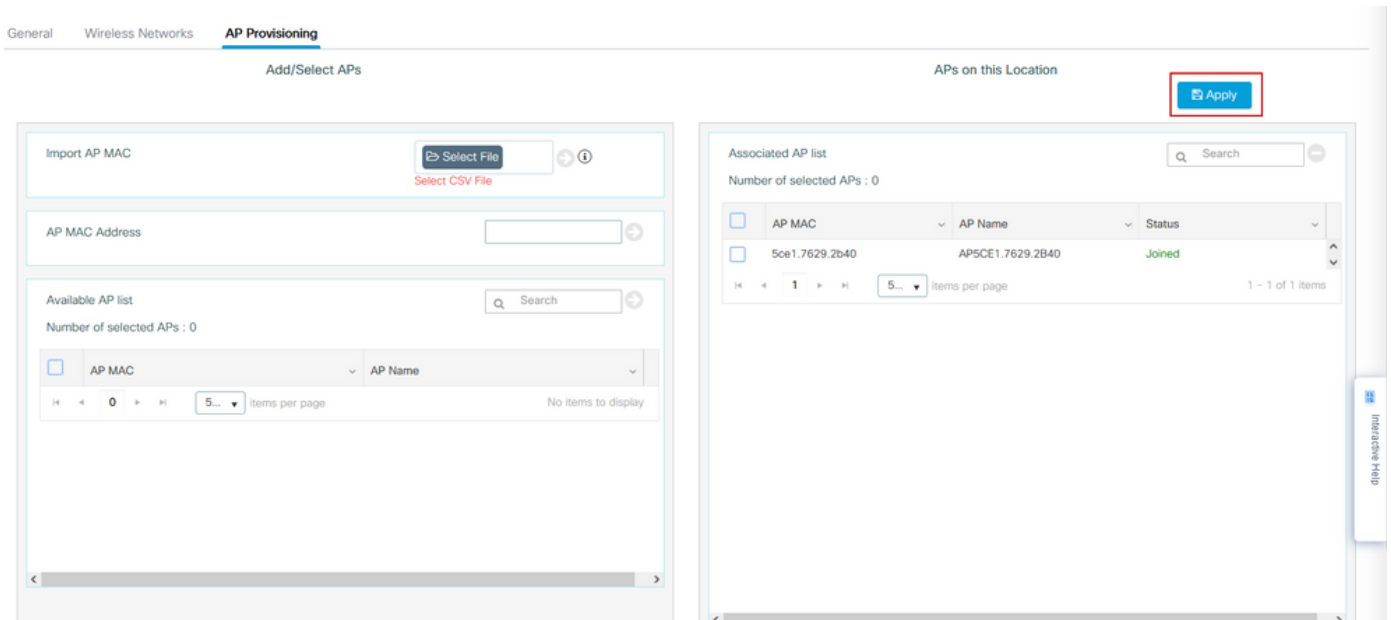
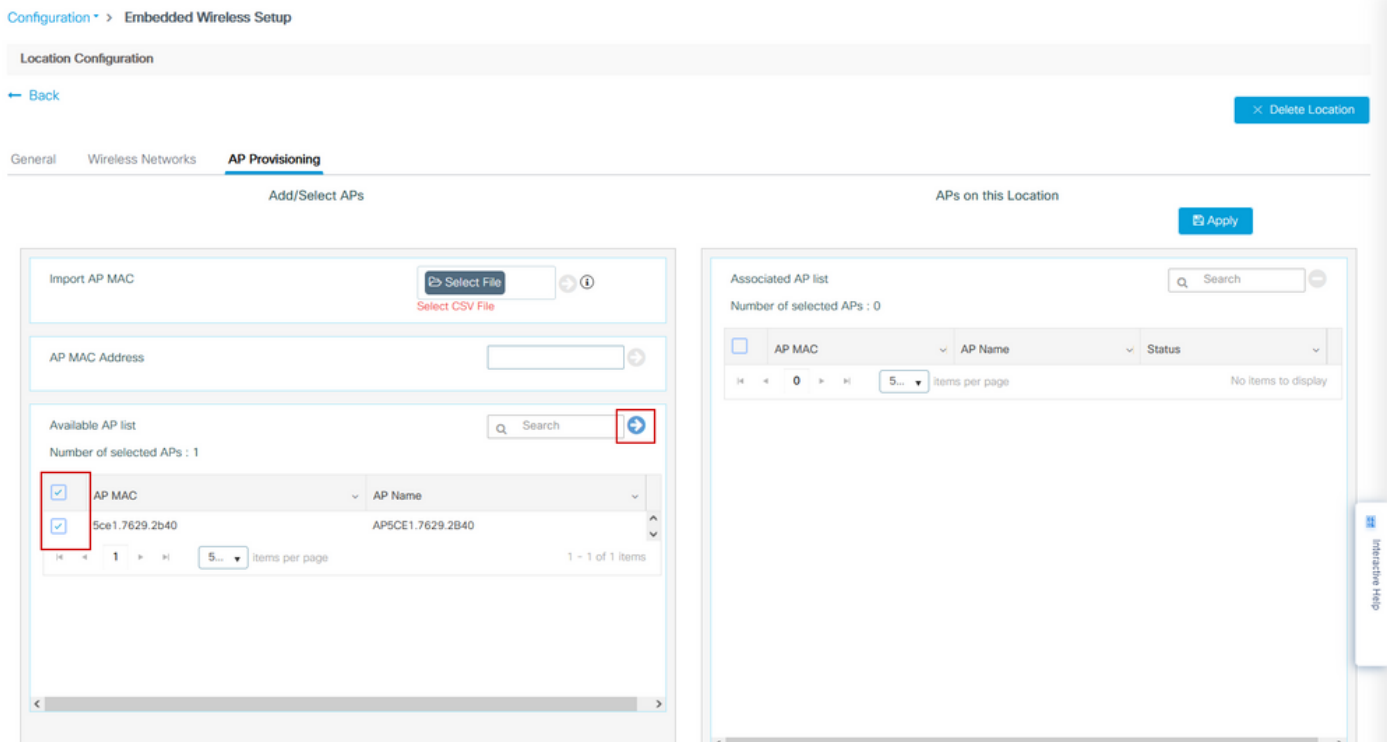
**Étape 5.** Configurez switchport en mode d'accès et attribuez-le au VLAN précédemment défini.

```
3850-1(config)#interface
```

```
3850-1(config-if)#switchport mode access
3850-1(config-if)#switchport access vlan
```

**Étape 6.** Accédez à Configuration > Embedded Wireless Setup et choisissez le site créé à l'étape 3. Cliquez sur l'onglet AP Provisioning et dans la liste des AP disponibles, choisissez les AP qui doivent être provisionnés et cliquez sur la flèche bleue pour le changer en Associated AP list. Une fois que tous les AP d'intérêt ont été assignés à l'emplacement spécifique, cliquez sur Apply.

**Attention** : le commutateur EWC permet la création et l'affectation manuelles de balises. Cependant, cette configuration n'est pas prise en charge et la seule affectation de balises prise en charge est par affectation d'emplacement. Un seul emplacement est pris en charge sur le commutateur EWC. Tous les points d'accès doivent donc se trouver dans le même sous-réseau et être affectés au même emplacement.



Cette étape ajoute cette configuration au commutateur EWC-Switch :

```
9300-1(config)# ap location name EWC-Location
9300-1(config-ap-location)# ap-eth-mac
```

```
9300-1(config-ap-location)# tag policy EWC-Location
```

```
9300-1(config-ap-location)# tag rf EWC-Location
```

La commande **ap-eth-mac <AP mac address>** se répète pour chaque AP qui est ajouté à l'emplacement. Un seul site peut prendre en charge jusqu'à 500 points d'accès.

## Vérifier

Utilisez cette commande pour vérifier la création et l'état de VLAN pour WMI et AP Onboard.

```
9300-1#show wireless fabric summary
```

```
Fabric Status : Enabled
```

```
Control-plane:
```

```
Name IP-address Key Status
```

```
-----  
default-control-plane 172.16.0.1 ciscoeca Up
```

```
Fabric VNID Mapping:
```

```
Name L2-VNID L3-VNID IP Address Subnet Control plane name
```

```
-----  
APONBOARDING_0_2674_4097_8188 8188 4097 172.16.80.0 255.255.255.0
```

Vérifiez l'état d'enregistrement AP avec ces commandes :

```
9300-1#show wireless stats ap join summary
```

```
Number of APs: 1
```

```
Base MAC Ethernet MAC AP Name IP Address Status Last Failure Phase Last Disconnect Reason
```

```
-----  
ac4a.569c.f560 5ce1.7629.2b40 AP5CE1.7629.2B40 172.16.80.10 Joined Run Tag modified
```

```
9300-1#show fabric ap summary
```

```
Number of Fabric AP : 1
```

```
AP Name Slots AP Model Ethernet MAC Radio MAC Location Country IP Address State
```

```
-----  
AP5CE1.7629.2B40 2 9120AXI 5ce1.7629.2b40 ac4a.569c.f560 default location US 172.16.80.10  
Registered
```

Utilisez cette commande pour vérifier l'état du tunnel VxLAN avec les AP.

```
9300-1#show access-tunnel summary
```

```
Access Tunnels General Statistics:
```

```
Number of AccessTunnel Data Tunnels = 1
```

```
Name RLOC IP(Source) AP IP(Destination) VRF ID Source Port Destination Port
```

```
-----  
Ac0 172.16.0.1 172.16.80.10 0 N/A 4789
```

```
Name IfId Uptime
```

```
-----
```

```
Ac0 0x00000069 0 days, 00:20:11
```

Vérifiez l'attribution de balise AP avec cette commande. Les points d'accès doivent tous avoir les mêmes balises et afficher l'emplacement sous **Source**.

```
9300-1#show ap tag summary
```

```
Number of APs: 1
```

```
AP Name AP Mac Site Tag Name Policy Tag Name RF Tag Name Misconfigured Tag Source
```

```
-----
```

```
AP5CE1.7629.2B40 5ce1.7629.2b40 default-site-tag EWC-Location EWC-Location No Location
```

**Remarque** : dans cet exemple, 172.16.0.1 est l'adresse IP Loopback0 (qui est la gestion sans fil) et les points d'accès y accèdent. Puisqu'il s'agit d'un fabric dans une boîte, tous les composants de fabric pointent également vers ce point.

## Dépannage

### Débogage conditionnel et traçage Radio Active

Activez les débogages conditionnels et capturez la trace Radio Active (RA) pour dépanner le processus de jointure. Les traces RA fournissent des traces de niveau de débogage pour tous les processus qui interagissent avec la condition spécifiée (l'adresse MAC AP dans ce cas). Afin d'activer le débogage conditionnel, suivez ces étapes.

**Étape 1.** Assurez-vous qu'aucune condition de débogage n'est activée.

```
9300-1#clear platform condition all
```

**Étape 2.** Activez la condition de débogage pour l'adresse MAC AP que vous souhaitez surveiller.

Par défaut, la durée de surveillance est de 30 minutes (1 800 secondes). Vous pouvez augmenter le temps d'exécution des débogages jusqu'à 2085978494 secondes.

```
9300-1#debug wireless mac
```

```
9300-1#debug wireless mac
```

**Remarque** : afin de déboguer plusieurs AP, exécutez la commande debug wireless mac pour chaque adresse MAC radio et Ethernet de chaque AP. Seul le débogage MAC Ethernet affiche les transactions DTLS.

**Remarque** : le débogage C9800 fonctionne dans le modèle de stockage et de traitement. En d'autres termes, le débogage n'est pas affiché sur la session de terminal et tous les journaux sont mis en mémoire tampon en interne afin d'être affichés ultérieurement.

**Étape 3.** Rejeter AP switchport ou capwap reset AP à partir de l'interface de ligne de commande AP pour capturer la trace complète.

**Étape 4.** Arrêtez le débogage si le problème est reproduit avant la fin du temps de surveillance par défaut ou configuré.

```
9300-1#no debug wireless mac
```

```
9300-1#no debug wireless mac
```

Une fois que le temps de surveillance est écoulé ou que le débogage sans fil a été arrêté manuellement, le commutateur EWC génère un fichier local nommé :

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

**Étape 5.** Recueillir le fichier de l'activité de l'adresse MAC. Vous avez la possibilité de copier le fichier ra trace.log sur un serveur externe pour l'analyse hors connexion ou d'afficher le résultat directement sur la session du terminal. L'analyse hors connexion est préférable en raison du volume de journaux de suivi générés.

Vérifiez le nom du fichier de suivi RA.

```
9300-1#dir flash: | inc ra_trace
```

Copiez le fichier sur un serveur externe :

```
9300-1#copy flash:ra_trace_MAC_<AP_RADIO_MAC>_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log  
tftp://
```

```
ra-AP_RADIO_MAC.txt
```

```
9300-1#copy flash:ra_trace_MAC_<AP_ETHERNET_MAC>_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log  
tftp://
```

```
ra-AP_ETHERNET_MAC.txt
```

Afin d'afficher les journaux de suivi sur une session de terminal :

```
9300-1#more flash:ra_trace_MAC_<AP_RADIO_MAC>_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
9300-1#more flash:ra_trace_MAC_<AP_ETHERNET_MAC>_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

**Étape 6.** Si la cause première n'est pas évidente, collectez les journaux internes qui sont une vue plus détaillée des journaux de suivi. Vous n'avez pas besoin de déboguer à nouveau le client car la commande fournit des journaux de débogage qui ont déjà été collectés et stockés en interne.

```
9300-1#show logging profile wireless internal filter
```

```
ra-internal-<AP_RADIO_MAC>.txt
```

```
9300-1#show logging profile wireless internal filter
```

```
ra-internal-<AP_RADIO_MAC>.txt
```

**Remarque :** cette sortie de commande retourne des traces pour tous les niveaux de journalisation pour tous les processus et est assez volumineuse. Contactez le Centre d'assistance technique (TAC) pour vous aider à analyser ces traces.

```
9300-1#copy flash:ra-internal-<AP_RADIO_MAC>.txt tftp://
```

```
ra-internal-<AP_RADIO_MAC>.txt
```

```
9300-1#copy flash:ra-internal-<AP_RADIO_MAC>.txt tftp://
```

```
ra-internal-<AP_RADIO_MAC>.txt
```

Afin d'afficher les journaux de suivi sur la session de terminal :

```
9300-1#more flash:ra-internal-<AP_RADIO_MAC>.txt
```

```
9300-1#more flash:ra-internal-<AP_ETHERNET_MAC>.txt
```

**Étape 7.** Supprimez les conditions de débogage.

**Remarque :** assurez-vous de toujours supprimer les conditions de débogage après avoir résolu le problème.

## Exemple d'une jointure AP réussie

Il s'agit du résultat d'une tentative de connexion réussie du point de vue de la trace RA. Utilisez les échantillons de journal pour vérifier à quelle étape le point d'accès est bloqué.

### Requête et réponse de détection CAPWAP :

```
2021/09/30 17:49:13.823492 {wncmgrd_R0-0}{1}: [capwapac-discovery] [7353]: (note): MAC:
ac4a.569c.f560 IP:172.16.80.10[5264], Discovery Request received
2021/09/30 17:49:13.823519 {wncmgrd_R0-0}{1}: [capwapac-discovery] [7353]: (note): MAC:
ac4a.569c.f560 EWLC TAGS payload is not present in discovery request
2021/09/30 17:49:13.823793 {wncmgrd_R0-0}{1}: [ewlc-infra-evq] [7353]: (debug): instance :0
port:12289MAC: 0002.0002.ffff
2021/09/30 17:49:13.824314 {wncmgrd_R0-0}{1}: [capwapac-discovery] [7353]: (note): MAC:
ac4a.569c.f560 Public IP learnt is FALSE, public IP discovery is FALSE, private IP discovery is
TRUE.
2021/09/30 17:49:13.824414 {wncmgrd_R0-0}{1}: [capwapac-discovery] [7353]: (note): MAC:
ac4a.569c.f560 IP:172.16.80.10[5264], Discovery Response sent
```

### Connexion DTLS pour le contrôle de validité du certificat :

```
2021/09/30 17:49:23.259157 {wncd_x_R0-0}{1}: [capwapac-smgr-srvr] [7770]: (note): MAC:
ac4a.569c.f560 DTLS session create callback received.
2021/09/30 17:49:23.259393 {wncd_x_R0-0}{1}: [capwapac-smgr-sess] [7770]: (info): Session-IP:
172.16.80.10[5264] Mac: PMTU 576, effective capwap size 416
2021/09/30 17:49:23.259406 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [7770]: (debug): DTLS record type:
22, handshake
2021/09/30 17:49:23.259406 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [7770]: (info): DTLS client hello
2021/09/30 17:49:23.260931 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [7770]: (debug): DTLS record type:
22, handshake
2021/09/30 17:49:23.260931 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [7770]: (info): DTLS client hello
2021/09/30 17:49:23.267234 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [7770]: (debug): DTLS record type:
22, handshake
2021/09/30 17:49:23.267332 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [7770]: (debug): DTLS record type:
22, handshake
2021/09/30 17:49:23.267891 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [7770]: (debug): DTLS record type:
22, handshake
2021/09/30 17:49:23.270741 {wncd_x_R0-0}{1}: [ewlc-dtls-sessmgr] [7770]: (info): Remote Host:
172.16.80.10[5264] MAC: ac4a.569c.f56 Completed cert verification, status:CERT_VALIDATE_SUCCESS
2021/09/30 17:49:23.608757 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [7770]: (debug): DTLS record type:
22, handshake
2021/09/30 17:49:23.608990 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [7770]: (debug): DTLS record type:
20, change cipher-spec
2021/09/30 17:49:23.609255 {wncd_x_R0-0}{1}: [ewlc-dtls-sess] [7770]: (info): Remote Host:
172.16.80.10[5264] MAC: ac4a.569c.f56 DTLS session established
2021/09/30 17:49:23.609348 {wncd_x_R0-0}{1}: [capwapac-smgr-sess] [7770]: (info): Session-IP:
172.16.80.10[5264] Mac: PMTU 576, effective capwap size 456
2021/09/30 17:49:23.609361 {wncd_x_R0-0}{1}: [capwapac-smgr-srvr] [7770]: (info): Session-IP:
172.16.80.10[5264] Mac: DTLS session has been established for AP
2021/09/30 17:49:23.650838 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [7770]: (debug): DTLS record type:
23, application data
```

### Demande et réponse de jonction CAPWAP :

```
2021/09/30 17:49:23.650970 {wncd_x_R0-0}{1}: [capwapac-smgr-sess] [7770]: (info): Session-IP:
172.16.80.10[5264] Mac: Capwap message received, type: join_request
2021/09/30 17:49:23.650972 {wncd_x_R0-0}{1}: [capwapac-smgr-sess] [7770]: (note): MAC:
ac4a.569c.f560 Received CAPWAP join request
2021/09/30 17:49:23.652901 {wncd_x_R0-0}{1}: [rrm-client] [7770]: (ERR): ac4a.569c.f560 Failed
to override default values inradio oper for slot 1, reg domain chk status failed
2021/09/30 17:49:23.653789 {wncd_x_R0-0}{1}: [rrm-client] [7770]: (ERR): ac4a.569c.f560 Failed
to override default values inradio oper for slot 0, reg domain chk status failed
```

2021/09/30 17:49:23.653959 {wncd\_x\_R0-0}{1}: [apmgr-capwap-join] [7770]: (info): ac4a.569c.f560 Retrieved AP SW version: 17.3.4.30, for AP model: C9120AXI-B, AP image type: aplg7, site-tag: default-site-tag  
2021/09/30 17:49:23.653967 {wncd\_x\_R0-0}{1}: [apmgr-db] [7770]: (info): ac4a.569c.f560 Operation state of AP changed to: Registered  
2021/09/30 17:49:23.654039 {wncd\_x\_R0-0}{1}: [apmgr-capwap-join] [7770]: (note): MAC: ac4a.569c.f560 **Successfully processed Join request.** AP name: AP5CE1.7629.2B40, Model: C9120AXI-B, radio slots: 2, rlan slots: 0, site tag name: default-site-tag, **policy tag name: EWC-Location, rf tag name: EWC-Location**  
2021/09/30 17:49:23.654112 {wncmgrd\_R0-0}{1}: [ewlc-infra-evq] [7353]: (note): Msg type :msg->msgtype Priority:1  
2021/09/30 17:49:23.654233 {wncd\_x\_R0-0}{1}: [capwapac-smgr-srvr] [7770]: (info): MAC: ac4a.569c.f560 Join Response generated with MTU 1485. as per MTU payload, update flag: 0  
2021/09/30 17:49:23.654311 {wncd\_x\_R0-0}{1}: [capwapac-smgr-srvr] [7770]: (note): MAC: ac4a.569c.f560 **Join processing complete. AP in joined state**

## Configuration CAPWAP :

2021/09/30 17:49:23.947851 {wncd\_x\_R0-0}{1}: [apmgr-ap-global] [7770]: (info): ac4a.569c.f560 Lispagent was triggered during ap join.  
2021/09/30 17:49:23.948023 {wncd\_x\_R0-0}{1}: [capwapac-smgr-srvr] [7770]: (info): Session-IP: 172.16.80.10[5264] Mac: ac4a.569c.f560 **Config status request was processed and Config status response was sent. AP in Configuration state.**  
2021/09/30 17:49:23.948157 {wncd\_x\_R0-0}{1}: [lisp-agent-db] [7770]: (ERR): Invalid source IP address type  
2021/09/30 17:49:23.948344 {wncd\_x\_R0-0}{1}: [ewlc-infra-evq] [7770]: (note): Map request msg sent successfully for AP vnid 4097  
2021/09/30 17:49:23.949993 {wncmgrd\_R0-0}{1}: [hl-core] [7353]: (debug): Radio change on AP ac4a.569c.f560 not connected to a L1 cache entry  
2021/09/30 17:49:23.950130 {wncmgrd\_R0-0}{1}: [hl-core] [7353]: (debug): Radio change on AP ac4a.569c.f560 not connected to a L1 cache entry  
2021/09/30 17:49:24.889682 {wncd\_x\_R0-0}{1}: [ewlc-infra-evq] [7770]: (debug): DTLS record type: 23, application data  
2021/09/30 17:49:24.889807 {wncd\_x\_R0-0}{1}: [ewlc-infra-evq] [7770]: (debug): DTLS record type: 23, application data  
2021/09/30 17:49:24.889992 {wncd\_x\_R0-0}{1}: [capwapac-smgr-sess] [7770]: (info): Session-IP: 172.16.80.10[5264] Mac: ac4a.569c.f560 **Capwap message received, type: config\_status\_request**  
2021/09/30 17:49:24.890020 {wncd\_x\_R0-0}{1}: [capwapac-smgr-sess-fsm] [7770]: (info): Session-IP: 172.16.80.10[5264] Mac: ac4a.569c.f560 process config status request  
2021/09/30 17:49:24.890045 {wncd\_x\_R0-0}{1}: [capwapac-smgr-srvr] [7770]: (info): Session-IP: 172.16.80.10[5264] Mac: ac4a.569c.f560 Updating capwap path MTU: 1485 received in config status request  
2021/09/30 17:49:24.890048 {wncd\_x\_R0-0}{1}: [capwapac-smgr-sess] [7770]: (info): Session-IP: 172.16.80.10[5264] Mac: ac4a.569c.f560 PMTU 1485, effective capwap size 1368  
2021/09/30 17:49:24.890134 {wncd\_x\_R0-0}{1}: [apmgr-msgelem] [7770]: (info): ac4a.569c.f560 AP domain name is not set in config status  
2021/09/30 17:49:24.890135 {wncd\_x\_R0-0}{1}: [apmgr-msgelem] [7770]: (info): ac4a.569c.f560 AP IPv6 nameserver is not set in config status  
[...]  
2021/09/30 17:49:24.890818 {wncd\_x\_R0-0}{1}: [capwapac-smgr-srvr] [7770]: (info): Session-IP: 172.16.80.10[5264] Mac: ac4a.569c.f560 **Config status request was processed and Config status response was sent. AP in Configuration state.**  
2021/09/30 17:49:24.892967 {wncmgrd\_R0-0}{1}: [hl-core] [7353]: (debug): Radio change on AP ac4a.569c.f560 not connected to a L1 cache entry  
2021/09/30 17:49:24.892993 {wncmgrd\_R0-0}{1}: [hl-core] [7353]: (debug): Radio change on AP ac4a.569c.f560 not connected to a L1 cache entry  
2021/09/30 17:49:24.964085 {wncd\_x\_R0-0}{1}: [ewlc-infra-evq] [7770]: (debug): DTLS record type: 23, application data  
[...]  
2021/09/30 17:49:24.964384 {wncd\_x\_R0-0}{1}: [ble-d] [7770]: (debug): BLE LTX DB: Creating AP ac4a.569c.f560  
2021/09/30 17:49:24.964474 {wncd\_x\_R0-0}{1}: [ble-d] [7770]: (debug): BLE LTX DB: **Successfully created AP** ac4a.569c.f560



```
2021/09/30 17:49:24.964479 {wncd_x_R0-0}{1}: [ble-d] [7770]: (debug): BLE LTX DB: Setting
capability
2021/09/30 17:49:24.964479 {wncd_x_R0-0}{1}: [ble-d] [7770]: (debug): BLE LTX DB: Updating AP
ac4a.569c.f560
2021/09/30 17:49:24.964483 {wncd_x_R0-0}{1}: [ble-d] [7770]: (debug): BLE LTX DB: Successfully
updated AP ac4a.569c.f560
[...]
2021/09/30 17:49:25.000954 {wncd_x_R0-0}{1}: [apmgr-capwap-config] [7770]: (info):
ac4a.569c.f560 AP is in config ready state. Initial configuration will be pushed.
2021/09/30 17:49:25.000972 {wncd_x_R0-0}{1}: [apmgr-capwap-config] [7770]: (info):
ac4a.569c.f560 Sending FIPS vendor payload config, FIPS status 0
2021/09/30 17:49:25.000975 {wncd_x_R0-0}{1}: [apmgr-capwap-config] [7770]: (info): Preparing
FIPS config, fips status 0
2021/09/30 17:49:25.000978 {wncd_x_R0-0}{1}: [apmgr-capwap-config] [7770]: (info): Preparing
WLANCC config, wlancc status 0
2021/09/30 17:49:25.001064 {wncd_x_R0-0}{1}: [apmgr-ap-global] [7770]: (info): ac4a.569c.f560 AP
is in Local mode.
2021/09/30 17:49:25.001064 {wncd_x_R0-0}{1}: [apmgr-ap-global] [7770]: (info): ac4a.569c.f560
Mode update on AP join : AP already in Local mode which matches site configuration
2021/09/30 17:49:25.001081 {wncd_x_R0-0}{1}: [apmgr-db] [7770]: (info): ac4a.569c.f560 Tag
process ap wlan config mapping. wlans[0] associated to to AP
```

Si l'AP n'est pas en mode **Local**, alors il redémarre pour appliquer un changement de mode. Un journal similaire à celui-ci est imprimé sur la console EWC-Switch :

```
*Sep 29 20:54:07.769: %APMGR_TRACE_MESSAGE-4-WLC_CONFIG_CHECKER_WARNING: Switch 1 R0/0: wncd:
config check: The mode of AP ac4a.569c.f560 is changed from Flexconnect to Local.
*Sep 29 20:54:07.769: %APMGR_TRACE_MESSAGE-3-WLC_EXEC_MSG: Switch 1 R0/0: wncd: % Error: AP:
AP5CE1.7629.2B40 will go for a reboot due to Mode change from Flexconnect to 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.