

# Configurer OEAP et RLAN sur le WLC Catalyst 9800

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Diagramme du réseau](#)

[AP Se joindre derrière la NAT](#)

[Configuration](#)

[Vérification](#)

[Connectez-vous à OEAP et configurez le SSID personnel](#)

[Configurer RLAN sur le WLC 9800](#)

[Dépannage](#)

## Introduction

Ce document explique comment configurer le point d'accès Cisco OfficeExtend (OEAP) et le réseau local distant (RLAN) sur le WLC 9800.

Un point d'accès Cisco OfficeExtend (OEAP) fournit des communications sécurisées d'un contrôleur à un point d'accès Cisco sur un site distant, étendant de manière transparente le WLAN d'entreprise via Internet à la résidence d'un employé. L'expérience d'un utilisateur au bureau à domicile est exactement la même que celle du bureau de l'entreprise. Le chiffrement DTLS (Datagram Transport Layer Security) entre un point d'accès et le contrôleur garantit que toutes les communications ont le niveau de sécurité le plus élevé.

Un réseau local distant (RLAN) est utilisé pour authentifier les clients filaires 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 des clients filaires est traité comme trafic client sans fil. Le RLAN dans le point d'accès (AP) envoie la demande d'authentification pour authentifier le client filaire. L'authentification des clients filaires dans RLAN est similaire au client sans fil authentifié central.

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

## Components Used

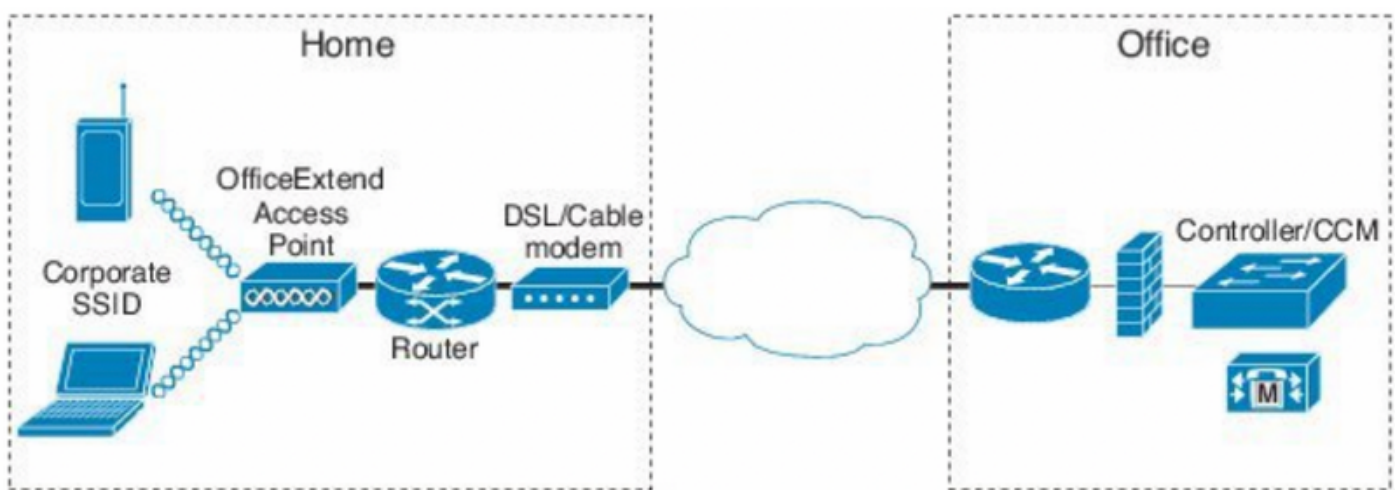
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- WLC Catalyst 9800 version 17.02.01
- Points d'accès de la gamme 1815/1810

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.

## Configuration

### Diagramme du réseau



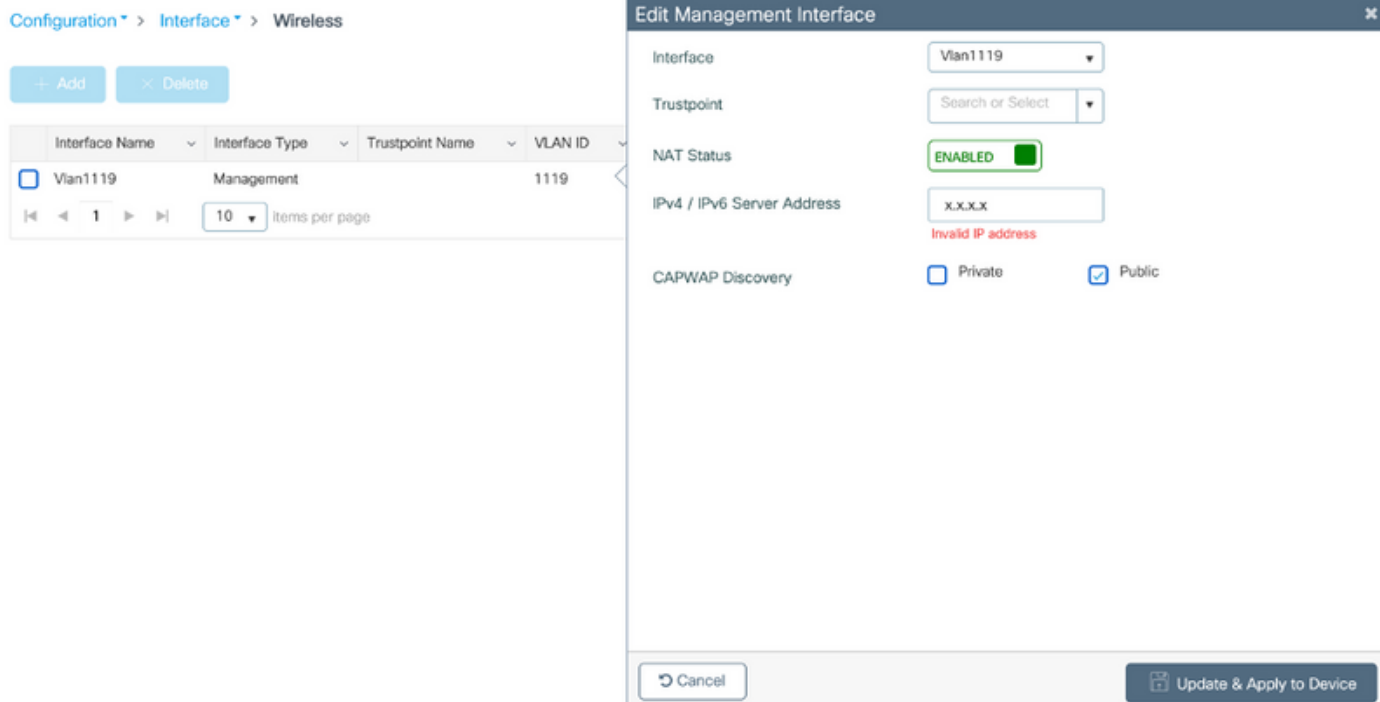
## AP Se joindre derrière la NAT

Dans les codes 16.12.x, vous devez configurer l'adresse IP NAT à partir de l'interface de ligne de commande. Aucune option d'interface utilisateur graphique n'est disponible. Vous pouvez également sélectionner la détection CAPWAP via une adresse IP publique ou privée.

```
(config)#wireless management interface vlan 1114 nat public-ip x.x.x.x
(config-nat-interface)#capwap-discovery ?
  private  Include private IP in CAPWAP Discovery Response

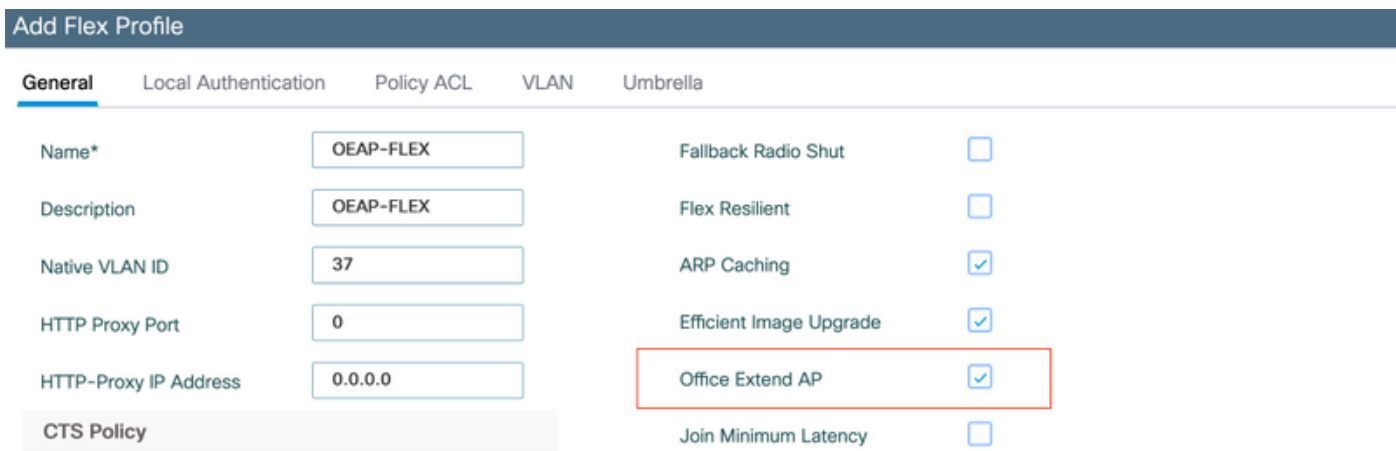
  public   Include public IP in CAPWAP Discovery Response
```

Dans les codes 17.x, accédez à **Configuration > Interface > Wireless** puis cliquez sur **Wireless Management Interface**, pour configurer le type NAT IP et CAPWAP-discovery à partir de l'interface utilisateur graphique.



## Configuration

1. Afin de créer un profil Flex, activez **Office Extend AP** et accédez à **Configuration > Tags & Profiles > Flex**.



2. Afin de créer une balise de site et de mapper un profil flexible, accédez à **Configuration > Tags & Profiles > Tags**.

## Add Site Tag

Name\*

Home-Office

Description

Enter Description

AP Join Profile

default-ap-profile

Flex Profile

OEAP-FLEX

Control Plane Name

Enable Local Site

Cancel

3. Naviguez pour marquer le point d'accès 1815 avec l'étiquette de site créée par **Configuration > Wireless Setup > Advanced > Tag APs**.

## Tag APs



### Tags

Policy

default-policy-tag

Site

Home-Office

RF

default-rf-tag

*Changing AP Tag(s) will cause associated AP(s) to reconnect*

Cancel



Apply to Device

# Vérification

Une fois que le point d'accès 1815 rerejoint le WLC, vérifiez cette sortie :

```
vk-9800-1#show ap name AP1815 config general
```

```
Cisco AP Name      : AP1815
```

```
=====
```

Cisco AP Identifier	: 002c.c8de.3460
Country Code	: Multiple Countries : IN,US
Regulatory Domain Allowed by Country	: 802.11bg:-A 802.11a:-ABDN
AP Country Code	: US - United States
<b>Site Tag Name</b>	<b>: Home-Office</b>
RF Tag Name	: default-rf-tag
Policy Tag Name	: default-policy-tag
AP join Profile	: default-ap-profile
<b>Flex Profile</b>	<b>: OEAP-FLEX</b>
Administrative State	: Enabled
Operation State	: Registered
AP Mode	: FlexConnect
AP VLAN tagging state	: Disabled
AP VLAN tag	: 0
CAPWAP Preferred mode	: IPv4
CAPWAP UDP-Lite	: Not Configured
AP Submode	: Not Configured
<b>Office Extend Mode</b>	<b>: Enabled</b>
Dhcp Server	: Disabled
Remote AP Debug	: Disabled

```
vk-9800-1#show ap link-encryption
```

	<b>Encryption</b>	Dnstream	Upstream	Last
AP Name	<b>State</b>	Count	Count	Update
-----				
N2	Disabled	0	0	06/08/20 00:47:33

when you enable the OfficeExtend mode for an access point DTLS data encryption is enabled automatically.

```
AP1815#show capwap client config
```

```
AdminState           : ADMIN_ENABLED(1)
Name                  : AP1815
Location              : default location
Primary controller name : vk-9800-1
ssh status            : Enabled
ApMode                : FlexConnect
ApSubMode             : Not Configured
Link-Encryption      : Enabled
OfficeExtend AP     : Enabled
Discovery Timer       : 10
Heartbeat Timer       : 30
Syslog server         : 255.255.255.255
Syslog Facility       : 0
Syslog level          : informational
```

**Note:** Vous pouvez activer ou désactiver le chiffrement de données DTLS pour un point d'accès spécifique ou pour tous les points d'accès à l'aide de la commande `ap link-encryption`

```
vk-9800-1(config)#ap profile default-ap-profile
```

```
vk-9800-1(config-ap-profile)#no link-encryption
```

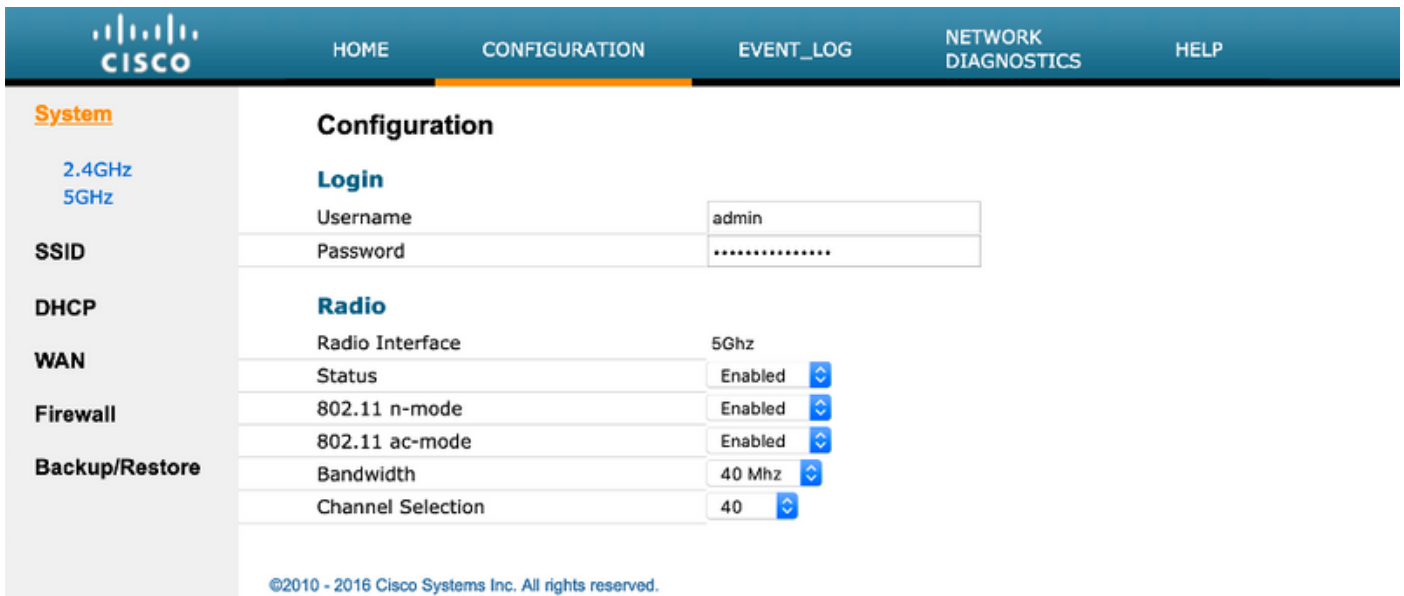
Disabling link-encryption globally will reboot the APs with link-encryption.

```
Are you sure you want to continue? (y/n) [y]:y
```

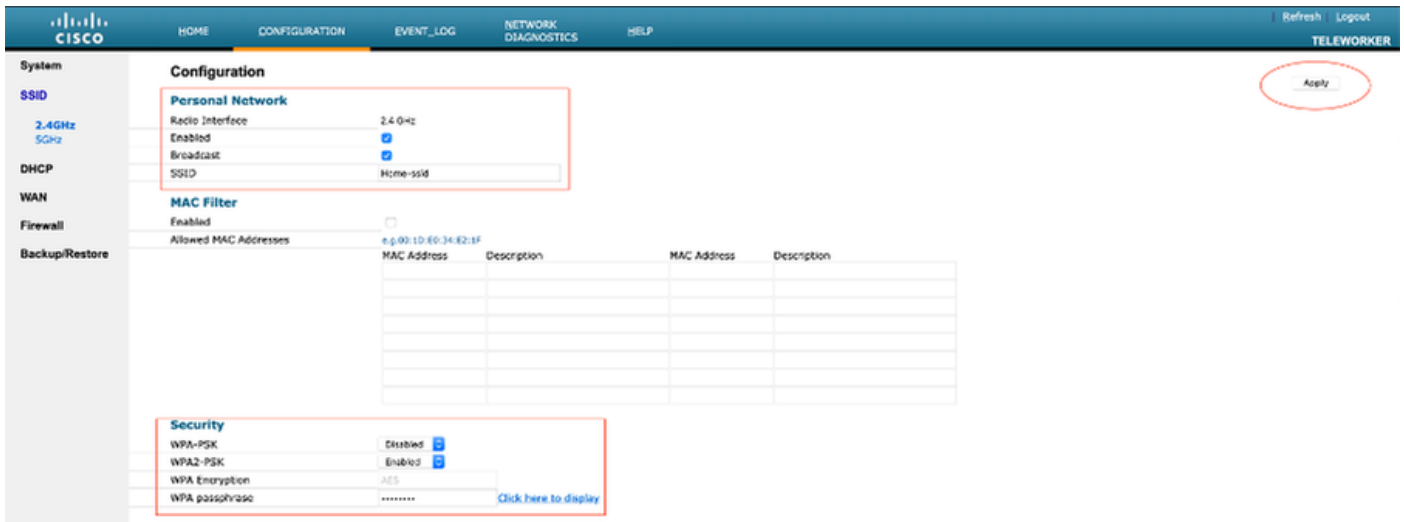
## Connectez-vous à OEAP et configurez le SSID personnel

1. Vous pouvez accéder à l'interface Web de l'OEAP avec son adresse IP. Les informations d'identification par défaut pour se connecter sont **admin** et **admin**.

2. Il est recommandé de modifier les informations d'identification par défaut pour des raisons de sécurité.



3. Accédez à **Configuration**> **SSID**> **2,4 GHz/5 GHz** pour configurer le SSID personnel.



4. Activez l'interface radio.

5. Entrez le SSID et activez la diffusion

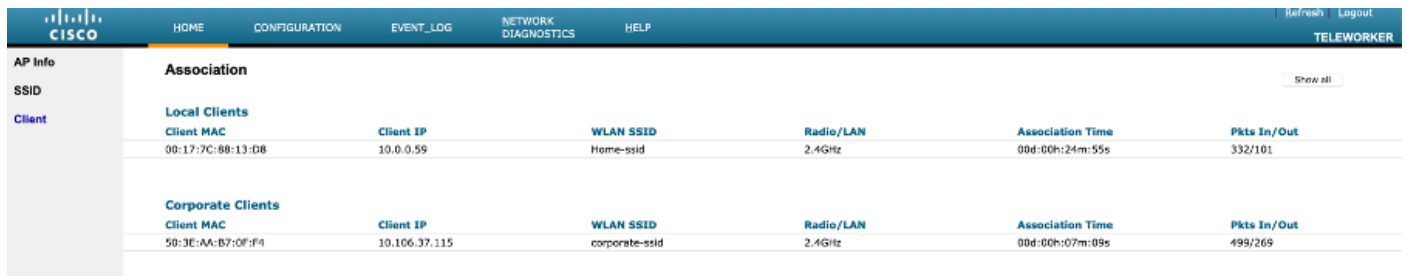
6. Pour le chiffrement, choisissez **WPA-PSK** ou **WPA2-PSK** et saisissez la phrase de passe du type de sécurité correspondant.

7. Cliquez sur Apply pour que les paramètres prennent effet.

8. Les clients qui se connectent au SSID personnel obtiennent par défaut l'adresse IP du réseau 10.0.0.1/24.

9. Les utilisateurs domestiques peuvent utiliser le même point d'accès pour se connecter à leur domicile et que le trafic n'est pas transmis via le tunnel DTLS.

10. Afin de vérifier les associations de clients sur le PAEO, accédez à **Accueil > Client**. Vous pouvez voir les clients locaux et les clients d'entreprise associés au PAEO.



Association						
<b>Local Clients</b>						
Client MAC	Client IP	WLAN SSID	Radio/LAN	Association Time	Pkts In/Out	
90:17:7C:88:13:D8	10.0.0.59	Home-ssid	2.4Ghz	00d:00h:24m:55s	332/101	
<b>Corporate Clients</b>						
Client MAC	Client IP	WLAN SSID	Radio/LAN	Association Time	Pkts In/Out	
50:3E:AA:B7:0F:F4	10.106.37.115	corporate-ssid	2.4Ghz	00d:00h:07m:09s	499/269	

To clear personal ssid from office-extend ap

```
ewlc#ap name cisco-ap clear-personalssid-config
```

clear-personalssid-config Clears the Personal SSID config on an OfficeExtend AP

## Configurer RLAN sur le WLC 9800

Un réseau local distant (RLAN) est utilisé pour authentifier les clients filaires 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 des clients filaires est traité comme trafic client sans fil. Le RLAN dans le point d'accès (AP) envoie la demande d'authentification pour authentifier le client filaire. Les

L'authentification des clients filaires dans RLAN est similaire au client sans fil authentifié central.

**Note:** Le protocole EAP local est utilisé pour l'authentification du client RLAN dans cet exemple. La configuration EAP locale doit être présente sur le WLC pour configurer les étapes ci-dessous. Il inclut des méthodes d'authentification et d'autorisation, un profil EAP local et des informations d'identification locales.

### [Exemple de configuration de l'authentification EAP locale sur le WLC Catalyst 9800](#)

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



### Add RLAN Profile

General Security

Profile Name\*

RLAN ID\*

Status **ENABLED**

Client Association Limit

mDNS Mode

2. Accédez à **Security > Layer2**, afin d'activer 802.1x pour un RLAN, définissez l'état 802.1x comme Activé, comme illustré dans cette image.

### Edit RLAN Profile

General **Security**

**Layer2** Layer3 AAA

802.1x **ENABLED**

MAC Filtering

Authentication List

3. Accédez à **Security > AAA**, définissez l'authentification EAP locale sur enabled et choisissez le nom de profil EAP requis dans la liste déroulante, comme illustré dans cette image.

## Edit RLAN Profile

General **Security**

Layer2 Layer3 **AAA**

Local EAP Authentication

ENABLED

EAP Profile Name

Local-EAP

4. Afin de créer une 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.

### Edit RLAN Policy

General **Access Policies** Advanced

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this policy.

Policy Name*	RLAN-Policy	RLAN Switching Policy
Description	Enter Description	Central Switching <input checked="" type="checkbox"/>
Status	ENABLED <input checked="" type="checkbox"/>	Central DHCP <input checked="" type="checkbox"/>
PoE	<input type="checkbox"/>	
Power Level	4 <input type="text"/>	

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

### Edit RLAN Policy

General **Access Policies** Advanced

Pre-Authentication	<input type="checkbox"/>	Host Mode	singlehost <input type="text"/>
VLAN	VLAN0039 <input type="text"/>		
Remote LAN ACL			
IPv4 ACL	Not Configured <input type="text"/>		
IPv6 ACL	Not Configured <input type="text"/>		

5. Afin de créer une balise de stratégie et de mapper le profil RLAN à la stratégie RLAN, accédez à **Configuration > Tags & Profiles > Tags**.

## Add Policy Tag



Name\*

RLAN-TAG

Description

Enter Description

WLAN-POLICY Maps: 0

RLAN-POLICY Maps: 0

+ Add

× Delete

Port ID	RLAN Profile	RLAN Policy Profile
No items to display		

### Map RLAN and Policy

Port ID\*

3

RLAN Profile\*

RLAN-TEST

RLAN Policy Profile\*

RLAN-Policy



Cancel

Apply to Device

## Add Policy Tag ✕

Name\*

Description

➤ WLAN-POLICY Maps: 0

▼ RLAN-POLICY Maps: 1

	Port ID	RLAN Profile	RLAN Policy Profile
<input type="checkbox"/>	3	RLAN-TEST	RLAN-Policy

⏪ ◀ 1 ▶ ⏩  items per page 1 - 1 of 1 items

6. Activez le port LAN et appliquez la balise Policy sur le point d'accès. Accédez à **Configuration > Wireless > Access Points** et cliquez sur le **point d'accès**.

## Edit AP

Location*	default location	Predownloaded Status	N/A
Base Radio MAC	0042.5ab7.8f60	Predownloaded Version	N/A
Ethernet MAC	0042.5ab6.4ab0	Next Retry Time	N/A
Admin Status	ENABLED <input checked="" type="checkbox"/>	Boot Version	1.1.2.4
AP Mode	Local ▼	IOS Version	17.2.1.11
Operation Status	Registered	Mini IOS Version	0.0.0.0
Fabric Status	Disabled	<b>IP Config</b>	
LED State	<input type="checkbox"/> DISABLED	CAPWAP Preferred Mode	Not Configured
LED Brightness Level	8 ▼	DHCP IPv4 Address	10.106.39.198
<b>Tags</b>		Static IP (IPv4/IPv6)	<input type="checkbox"/>
<p>⚠ Changing Tags will cause the AP to momentarily lose association with the Controller.</p>			
Policy	RLAN-TAG  ▼	<b>Time Statistics</b>	
Site	default-site-tag ▼	Up Time	0 days 13 hrs 33 mins 40 secs
RF	default-rf-tag ▼	Controller Association Latency	20 secs

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

Edit AP

General **Interfaces** High Availability Inventory ICap Advanced

Radio Interfaces

Slot No	Interface	Band	Admin Status	Operation Status	Spectrum Admin Status	Spectrum Operation Status	Regulatory Domain
0	802.11n - 2.4 GHz	All	Enabled	↑	Disabled	↓	-A
1	802.11ac	All	Enabled	↑	Disabled	↓	-D

10 items per page 1 - 2 of 2 items

Power Over Ethernet Settings

Power Type/Mode: Power Injector/Normal Mode

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 type="checkbox"/>	0	<input type="checkbox"/>	NA	⊗
LAN2	<input type="checkbox"/>	0	NA	NA	⊗
LAN3	<input checked="" type="checkbox"/>	39	NA	NA	⊗

10 items per page 1 - 3 of 3 items

Appliquez les paramètres et vérifiez l'état.

Edit AP

General **Interfaces** High Availability Inventory ICap Advanced

Radio Interfaces

Slot No	Interface	Band	Admin Status	Operation Status	Spectrum Admin Status	Spectrum Operation Status	Regulatory Domain
0	802.11n - 2.4 GHz	All	Enabled	↑	Disabled	↓	-A
1	802.11ac	All	Enabled	↑	Disabled	↓	-D

10 items per page 1 - 2 of 2 items

Power Over Ethernet Settings

Power Type/Mode: Power Injector/Normal Mode

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 type="checkbox"/>	0	<input type="checkbox"/>	NA	⊗
LAN2	<input type="checkbox"/>	0	NA	NA	⊗
LAN3	<input checked="" type="checkbox"/>	39	NA	NA	✓

10 items per page 1 - 3 of 3 items

7. Connectez un PC au port LAN3 du point d'accès. Le PC sera authentifié via 802.1x et obtiendra une adresse IP à partir du VLAN configuré.

Accédez à **Surveillance > Sans fil > Clients** pour vérifier l'état du client.

Delete



Total Client(s) in the Network: 2

Number of Client(s) selected: 0

Client MAC Address	IPv4 Address	IPv6 Address	AP Name	SSID	WLAN ID	State	Protocol	User Name	Device Type	Role
503e.aab7.0ff4	10.106.39.227	2001::c	AP1815	corporate-ssid	3	Run	11n(2.4)		N/A	Local
b496.9126.dd6c	10.106.39.191	fe80::d8cax582:2703:f24e	AP1810	RLAN-TEST	1	Run	Ethernet	vinodh	N/A	Local

10 items per page

1 - 2 of 2 clients

## Client

360 View

General

QOS Statistics

ATF Statistics

Mobility History

Call Statistics

Client Properties

AP Properties

Security Information

Client Statistics

QOS Properties

EoGRE

## Session Manager

IIF ID	0x9000000C
Authorized	TRUE
Common Session ID	00000000000000E79E8C7A9A
Acct Session ID	0x00000000
Auth Method Status List	
Method	Dot1x
SM State	AUTHENTICATED
SM Bend State	IDLE

vk-9800-1#show wireless client summary

Number of Clients: 2

MAC Address	AP Name	Type	ID	State
-------------	---------	------	----	-------

Protocol	Method	Role
----------	--------	------

```
-----
503e.aab7.0ff4 AP1815 WLAN 3 Run
11n(2.4) None Local
b496.9126.dd6c AP1810 RLAN 1 Run
Ethernet Dot1x Local
```

Number of Excluded Clients: 0

## Dépannage

Problèmes courants:

- Seul le travail du SSID local, les SSID configurés sur le WLC ne sont pas diffusés : vérifiez si l'AP a rejoint le contrôleur correctement.
- Impossible d'accéder à l'interface utilisateur graphique OEAP : Vérifier si le point d'accès a une adresse IP et vérifier l'accessibilité ( pare-feu, liste de contrôle d'accès, etc. dans le réseau )
- Clients filaires ou sans fil commutés de manière centralisée ne pouvant pas authentifier ou obtenir l'adresse IP : Prenez les traces RA, toujours sur les traces, etc.

## Exemple de traces Always on pour le client 802.1x filaire :

[client-orch-sm] [18950]: (note): MAC: <client-mac> Association received. BSSID 00b0.e187.cfc0, old BSSID 0000.0000.0000, WLAN test\_rlan, Slot 2 AP 00b0.e187.cfc0, Ap\_1810

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S\_CO\_INIT -> S\_CO\_ASSOCIATING

[dot11-validate] [18950]: (ERR): MAC: <client-mac> Failed to dot11 determine ms physical radio type. Invalid radio type :0 of the client.

[dot11] [18950]: (ERR): MAC: <client-mac> Failed to dot11 send association response. Encoding of assoc response failed for client reason code: 14.

[dot11] [18950]: (note): MAC: <client-mac> Association success. AID 1, Roaming = False, WGB = False, llr = False, llw = False AID list: 0x1| 0x0| 0x0| 0x0

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S\_CO\_ASSOCIATING -> S\_CO\_L2\_AUTH\_IN\_PROGRESS

[client-auth] [18950]: (note): MAC: <client-mac> ADD MOBILE sent. Client state flags: 0x71 BSSID: MAC: 00b0.e187.cfc0 capwap IFID: 0x90000012

[client-auth] [18950]: (note): MAC: <client-mac> L2 Authentication initiated. method DOT1X, Policy VLAN 1119,AAA override = 0 , NAC = 0

[ewlc-infra-evq] [18950]: (note): Authentication Success. Resolved Policy bitmap:11 for client <client-mac>

[client-orch-sm] [18950]: (note): MAC: <client-mac> Mobility discovery triggered. Client mode: Local

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S\_CO\_L2\_AUTH\_IN\_PROGRESS -> S\_CO\_MOBILITY\_DISCOVERY\_IN\_PROGRESS

[mm-client] [18950]: (note): MAC: <client-mac> Mobility Successful. Roam Type None, Sub Roam Type MM\_SUB\_ROAM\_TYPE\_NONE, Previous BSSID MAC: 0000.0000.0000 Client IFID: 0xa0000003, Client Role: Local PoA: 0x90000012 PoP: 0x0

[client-auth] [18950]: (note): MAC: <client-mac> ADD MOBILE sent. Client state flags: 0x72 BSSID: MAC: 00b0.e187.cfc0 capwap IFID: 0x90000012

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S\_CO\_MOBILITY\_DISCOVERY\_IN\_PROGRESS -> S\_CO\_DPATH\_PLUMB\_IN\_PROGRESS

[dot11] [18950]: (note): MAC: <client-mac> Client datapath entry params - ssid:test\_rlan,slot\_id:2 bssid ifid: 0x0, radio\_ifid: 0x90000006, wlan\_ifid: 0xf0404001

[dpath\_svc] [18950]: (note): MAC: <client-mac> Client datapath entry created for ifid 0xa0000003

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S\_CO\_DPATH\_PLUMB\_IN\_PROGRESS -> S\_CO\_IP\_LEARN\_IN\_PROGRESS

[client-iplearn] [18950]: (note): MAC: <client-mac> Client IP learn successful. Method: DHCP IP: <Client-IP>

[apmgr-db] [18950]: (ERR): 00b0.e187.cfc0 Get ATF policy name from WLAN profile:: Failed to get wlan profile. Searched wlan profile test\_rlan

[apmgr-db] [18950]: (ERR): 00b0.e187.cfc0 Failed to get ATF policy name



[apmgr-bssid] [18950]: (ERR): 00b0.e187.cfc0 Failed to get ATF policy name from WLAN profile name: No such file or directory

[client-orch-sm] [18950]: (ERR): Failed to get client ATF policy name: No such file or directory

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition:  
S\_CO\_IP\_LEARN\_IN\_PROGRESS -> S\_CO\_RUN