

# Configurer l'authentification Web centrale (CWA) sur le WLC Catalyst 9800 et ISE

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configuration AAA sur un contrôleur WLC 9800](#)

[Configuration d'un réseau local sans fil \(WLAN\)](#)

[Configuration du profil des politiques](#)

[Configuration des balises des politiques](#)

[Affectation des balises des politiques](#)

[Configuration d'une liste de contrôle d'accès de redirection](#)

[Activer la redirection pour HTTP ou HTTPS](#)

[Configuration ISE](#)

[Ajouter un contrôleur WLC 9800 à ISE](#)

[Créer un nouvel utilisateur sur ISE](#)

[Créer un profil d'autorisation](#)

[Configurer une règle d'authentification](#)

[Configurer les règles d'autorisation](#)

[Points d'accès de commutation locale Flexconnect UNIQUEMENT](#)

[Certificats](#)

[Vérifier](#)

[Dépannage](#)

[Liste de vérification](#)

[Prise en charge des ports de service pour RADIUS](#)

[Collecter les débogages](#)

[Exemples](#)

---

## Introduction

Ce document décrit comment configurer un LAN sans fil CWA sur un WLC et ISE Catalyst 9800.

## Conditions préalables

### Exigences

Cisco recommande que vous connaissiez la configuration des contrôleurs LAN sans fil (WLC) 9800.

## Composants utilisés

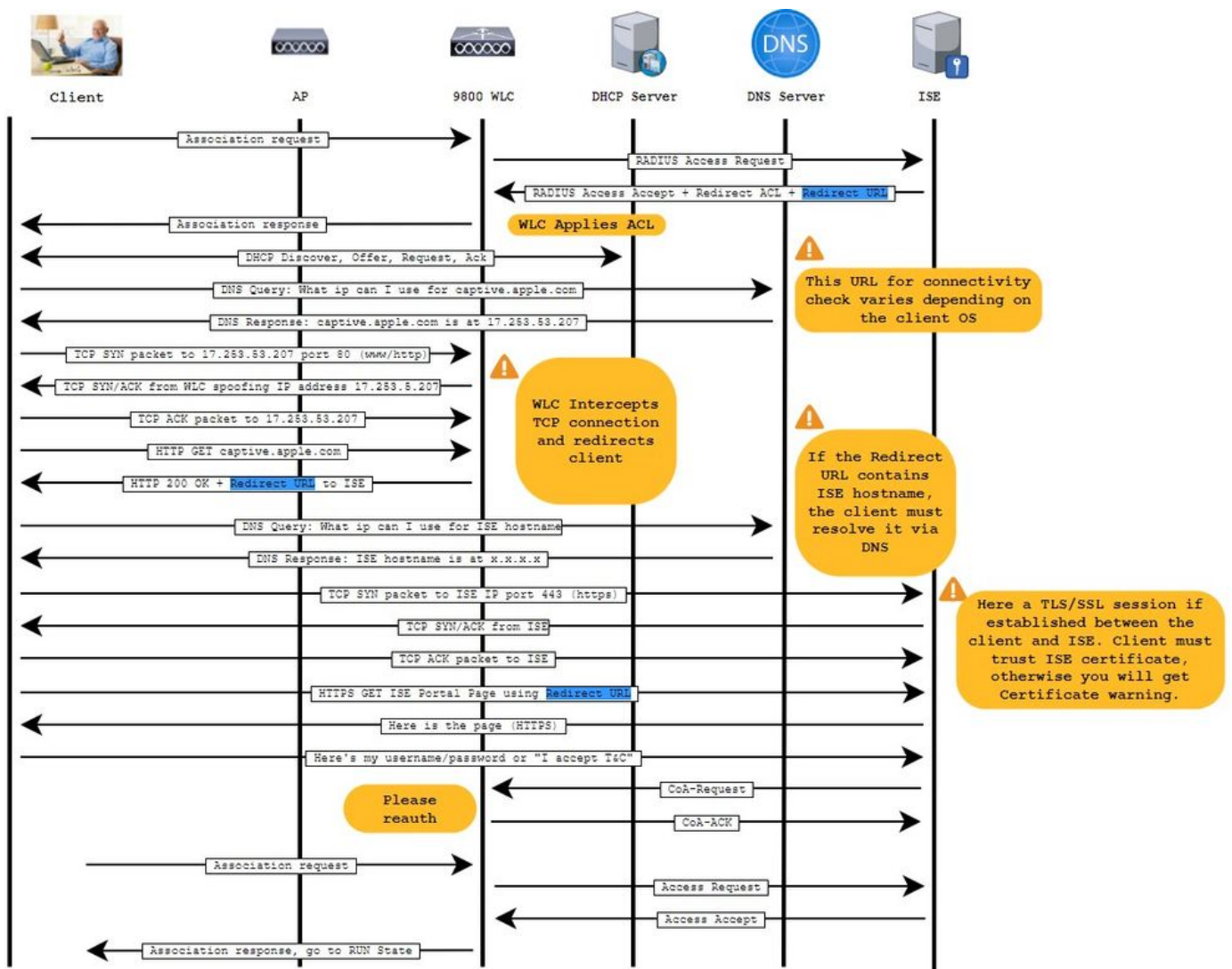
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- 9800 WLC Cisco IOS® XE Gibraltar v17.6.x
- Identity Service Engine (ISE) v3.0

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.

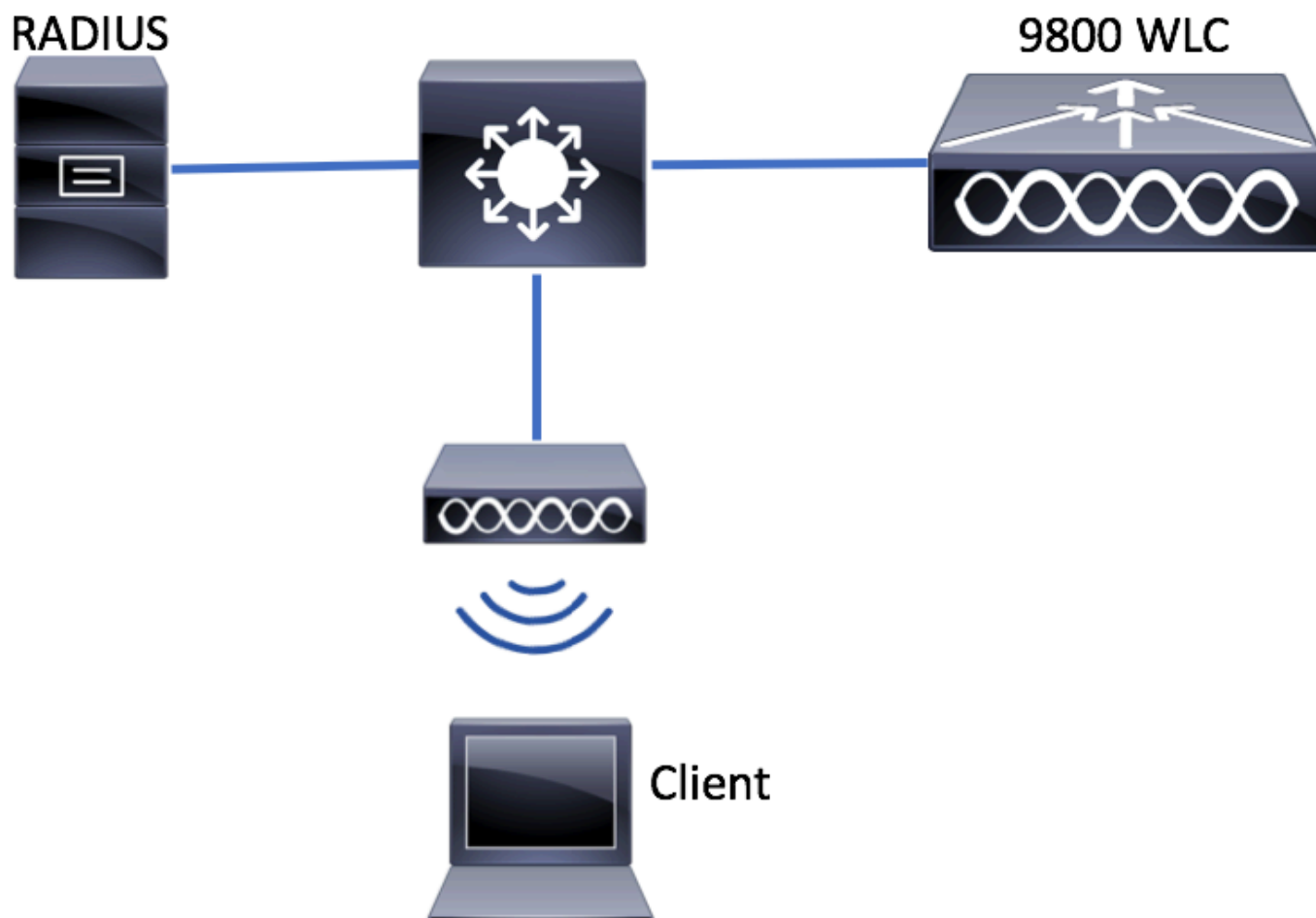
## Informations générales

Le processus CWA est présenté ici où vous pouvez voir le processus CWA d'un appareil Apple comme un exemple :



# Configurer

## Diagramme du réseau



## Configuration AAA sur un contrôleur WLC 9800

Étape 1. Ajoutez le serveur ISE à la configuration du WLC 9800.

Accédez aux informations du serveur RADIUS [Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add](#) et saisissez-les, comme indiqué dans les images.

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups    AAA Method List    AAA Advanced

+ Add    × Delete

RADIUS

TACACS+

LDAP

Servers    Server Groups

Name	Address
0	

10 items per page

Assurez-vous que la fonction Support for CoA est activée si vous prévoyez utiliser l'authentification Web centralisée (ou tout type de sécurité nécessitant CoA) à l'avenir.

### Create AAA Radius Server

Name\*    ISE-server

Server Address\*    [Redacted]

PAC Key   

Key Type    Clear Text

Key\*    [Redacted]

Confirm Key\*    [Redacted]

Auth Port    1812

Acct Port    1813

Server Timeout (seconds)    1-1000

Retry Count    0-100

Support for CoA     ENABLED

CoA Server Key Type    Clear Text

CoA Server Key    [Redacted]

Confirm CoA Server Key    [Redacted]

Automate Tester   

Cancel    Apply to Device

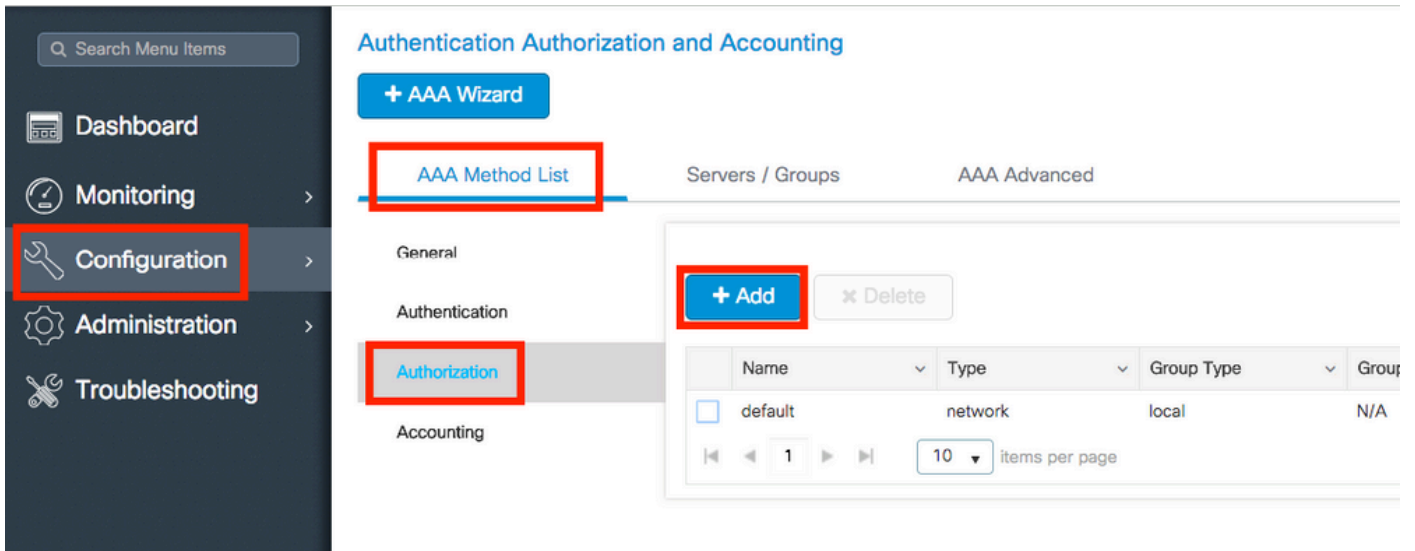


**Remarque** : sur les versions 17.4.X et ultérieures, assurez-vous de configurer également la clé du serveur CoA lorsque vous configurez le serveur RADIUS. Utilisez la même clé que le secret partagé (ils sont identiques par défaut sur ISE). L'objectif est de configurer éventuellement une clé différente pour CoA que le secret partagé si c'est ce que votre serveur RADIUS a configuré. Dans Cisco IOS XE 17.3, l'interface utilisateur Web utilisait simplement le même secret partagé que la clé CoA.

---

Étape 2. Créez une liste de méthodes d'autorisation.

Naviguez jusqu'à Configuration > Security > AAA > AAA Method List > Authorization > + Add comme indiqué dans l'image.



### Quick Setup: AAA Authorization

Method List Name\*

Type\*

Group Type

Fallback to local

Authenticated

**Available Server Groups**

**Assigned Server Groups**

Navigation buttons: >, <, >>, <<, ^, v, v

Étape 3. (Facultatif) Créez une liste de méthodes de comptabilisation, comme illustré dans l'image.

The screenshot shows the Cisco ISE configuration interface. On the left, a dark sidebar contains navigation options: Dashboard, Monitoring, Configuration (highlighted with a red box), Administration, and Troubleshooting. The main content area has a top bar with '+ AAA Wizard' and 'AAA Method List' (highlighted with a red box). Below this, there are sections for 'General', 'Authentication', and 'Authorization'. At the bottom of this section, 'Accounting' is highlighted with a red box. To the right, there is a 'Servers / Groups' section with a '+ Add' button (highlighted with a red box) and a 'Delete' button. Below the '+ Add' button is a table with a 'Name' header and a row containing a checkbox and the text 'radius'. A pagination control shows '0' items.

Quick Setup: AAA Accounting

Method List Name\*

Type\*

Available Server Groups

Assigned Server Groups

**Remarque :** CWA ne fonctionne pas si vous décidez d'équilibrer la charge (à partir de la configuration CLI de Cisco IOS XE) de vos serveurs RADIUS en raison du bogue Cisco ayant l'ID [CSCvh03827](https://cisco.com/cisco/websearch/bugsearch.html?bugid=CSCvh03827). L'utilisation d'équilibreurs de charge externes est correcte. Cependant, assurez-vous que votre équilibreur de charge fonctionne sur une base par client en utilisant l'attribut RADIUS call-station-id. L'utilisation du port source UDP n'est pas un mécanisme pris en charge pour équilibrer les requêtes RADIUS du 9800.

Étape 4. (Facultatif) Vous pouvez définir la stratégie AAA pour envoyer le nom SSID sous la forme d'un attribut Called-station-id, ce qui peut s'avérer utile si vous souhaitez tirer parti de cette condition sur ISE plus tard dans le processus.

Accédez à la stratégie AAA par défaut et modifiez-la ou créez-en une nouvelle Configuration > Security > Wireless AAA Policy.

- Dashboard
- Monitoring >
- Configuration** >
- Administration >
- Troubleshooting

Configuration > Security > **Wireless AAA Policy**

+ Add
× Delete

Policy Name
<input type="checkbox"/> default-aaa-policy

⏪ ⏩ 1 ⏪ ⏩ 10 items per page

Vous pouvez choisir SSID l'option 1. Gardez à l'esprit que même lorsque vous choisissez le SSID uniquement, l'ID de station appelé ajoute toujours l'adresse MAC AP au nom SSID.

## Edit Wireless AAA Policy

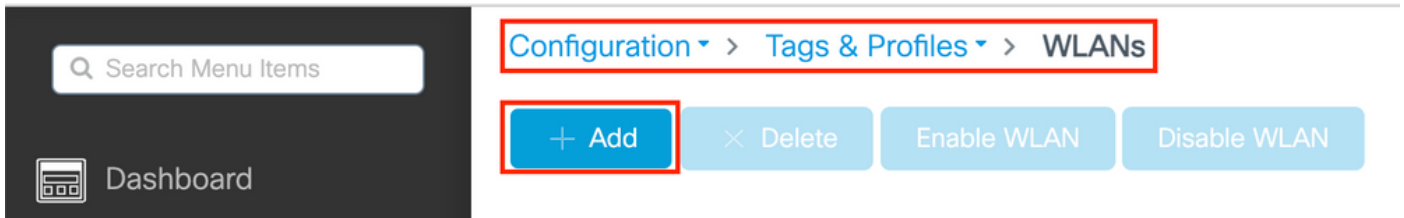
Policy Name*	<input style="width: 90%; border: 1px solid #ccc;" type="text" value="default-aaa-policy"/>
Option 1	<input style="width: 90%; border: 1px solid #ccc;" type="text" value="SSID"/>
Option 2	<input style="width: 90%; border: 1px solid #ccc;" type="text" value="Not Configured"/>
Option 3	<input style="width: 90%; border: 1px solid #ccc;" type="text" value="Not Configured"/>

Configuration d'un réseau local sans fil (WLAN)

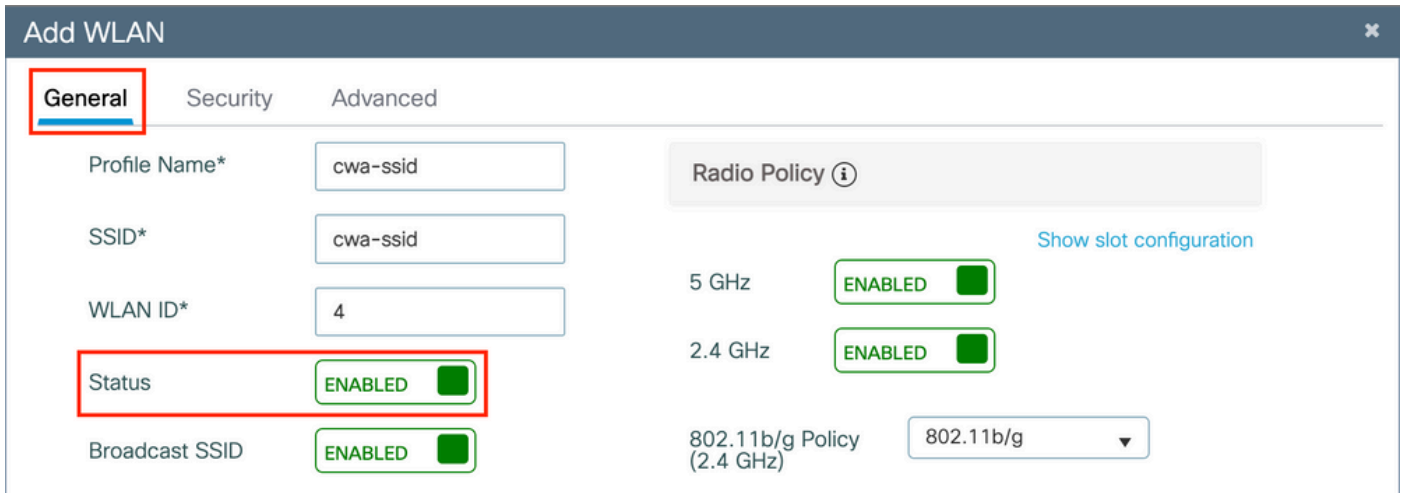
Étape 1. Créez le WLAN.

Accédez au réseau Configuration > Tags & Profiles > WLANs > + Add et configurez-le si nécessaire.

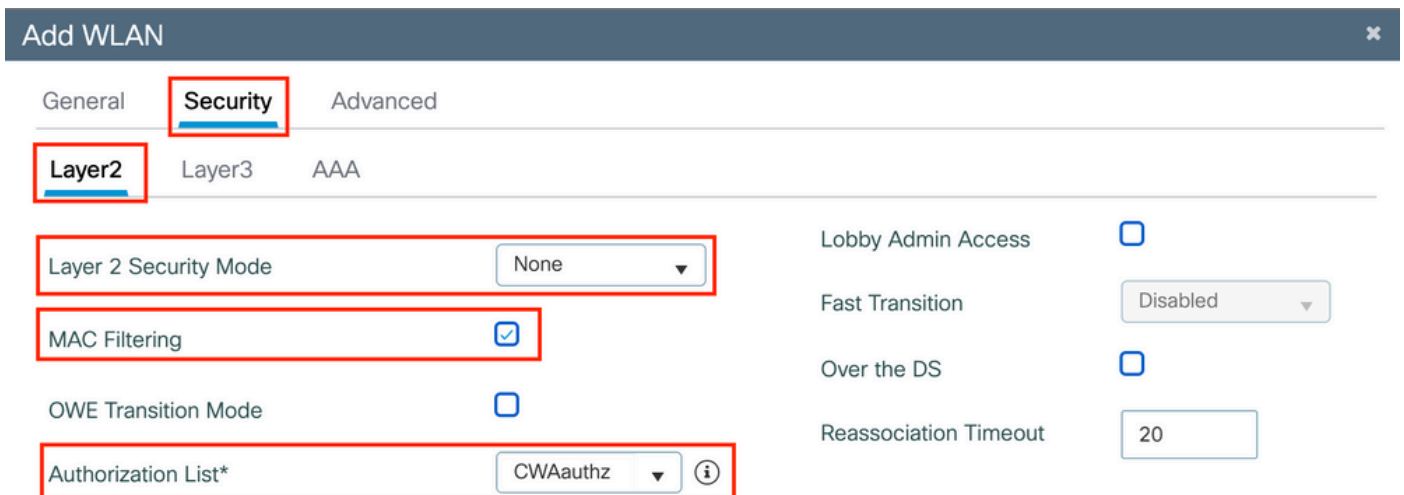




Étape 2. Saisissez les informations générales du WLAN.



Étape 3. Accédez à l'Security onglet et sélectionnez la méthode de sécurité requise. Dans ce cas, seuls 'MAC Filtering' et la liste d'autorisation AAA (que vous avez créée à l'étape 2. de la AAA Configuration section) sont nécessaires.



CLI :

```
#config t
(config)#wlan cwa-ssid 4 cwa-ssid
(config-wlan)#mac-filtering CWAauthz
(config-wlan)#no security ft adaptive
(config-wlan)#no security wpa
(config-wlan)#no security wpa wpa2
```

```
(config-wlan)#no security wpa wpa2 ciphers aes
(config-wlan)#no security wpa akm dot1x
(config-wlan)#no shutdown
```

## Configuration du profil des politiques

Dans un profil de stratégie, vous pouvez décider d'attribuer les clients à quel VLAN, entre autres paramètres (comme la liste de contrôle d'accès (ACL), la qualité de service (QoS), l'ancrage de mobilité, les minuteurs, etc.).

Vous pouvez soit utiliser votre profil de politique par défaut, soit en créer un nouveau.

IUG:

Étape 1. Créez un nouveau Policy Profile.

Accédez à Configuration > Tags & Profiles > Policy et configurez votre default-policy-profile ou créez-en un nouveau.

Policy Profile

+ Add  x Delete

Policy Profile Name	Description
<input type="checkbox"/> voice	
<input type="checkbox"/> default-policy-profile	default policy profile

1 10 items per page

Assurez-vous que le profil est activé.

## Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

### General

Access Policies

QOS and AVC

Mobility

Advanced

Name\*

Description

Status  ENABLED

Passive Client  DISABLED

Encrypted Traffic Analytics  DISABLED

#### CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

#### WLAN Switching Policy

Central Switching  ENABLED

Central Authentication  ENABLED

Central DHCP  ENABLED

Flex NAT/PAT  DISABLED

Étape 2. Sélectionnez le VLAN.

Accédez à l'Access Policies onglet et choisissez le nom du VLAN dans la liste déroulante ou tapez manuellement l'ID de VLAN. Ne configurez pas de liste de contrôle d'accès dans le profil de politique.

## Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

**Access Policies**

QOS and AVC

Mobility

Advanced

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select ▼

VLAN

VLAN/VLAN Group

VLAN1416 ▼

Multicast VLAN

Enter Multicast VLAN

WLAN ACL

IPv4 ACL

Search or Select ▼

IPv6 ACL

Search or Select ▼

URL Filters

Pre Auth

Search or Select ▼

Post Auth

Search or Select ▼

Étape 3. Configurez le profil de politique pour accepter les remplacements ISE (en cochant « Allow AAA Override ») et le changement d'autorisation (CoA) (en cochant « NAC State »). Vous pouvez également définir une méthode de gestion des comptes.

## Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

**Advanced**

### WLAN Timeout

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Guest LAN Session Timeout

### DHCP

IPv4 DHCP Required

DHCP Server IP Address

[Show more >>>](#)

### AAA Policy

Allow AAA Override

NAC State

NAC Type

Policy Name

Accounting List  ⓘ ✕

### WGB Parameters

Broadcast Tagging

WGB VLAN

### Policy Proxy Settings

ARP Proxy  DISABLED

IPv6 Proxy

Fabric Profile

Link-Local Bridging

mDNS Service Policy  [Clear](#)

Hotspot Server

### User Defined (Private) Network

Status

Drop Unicast

### DNS Layer Security

DNS Layer Security Parameter Map  [Clear](#)

Flex DHCP Option for DNS  ENABLED

Flex DNS Traffic Redirect  IGNORE

### WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

### Air Time Fairness Policies

2.4 GHz Policy

5 GHz Policy

### EoGRE Tunnel Profiles


Tunnel Profile

CLI:

```
# config # wireless profile policy <policy-profile-name> # aaa-override
# nac
# vlan <vlan-id_or_vlan-name>
# accounting-list <acct-list>
# no shutdown
```

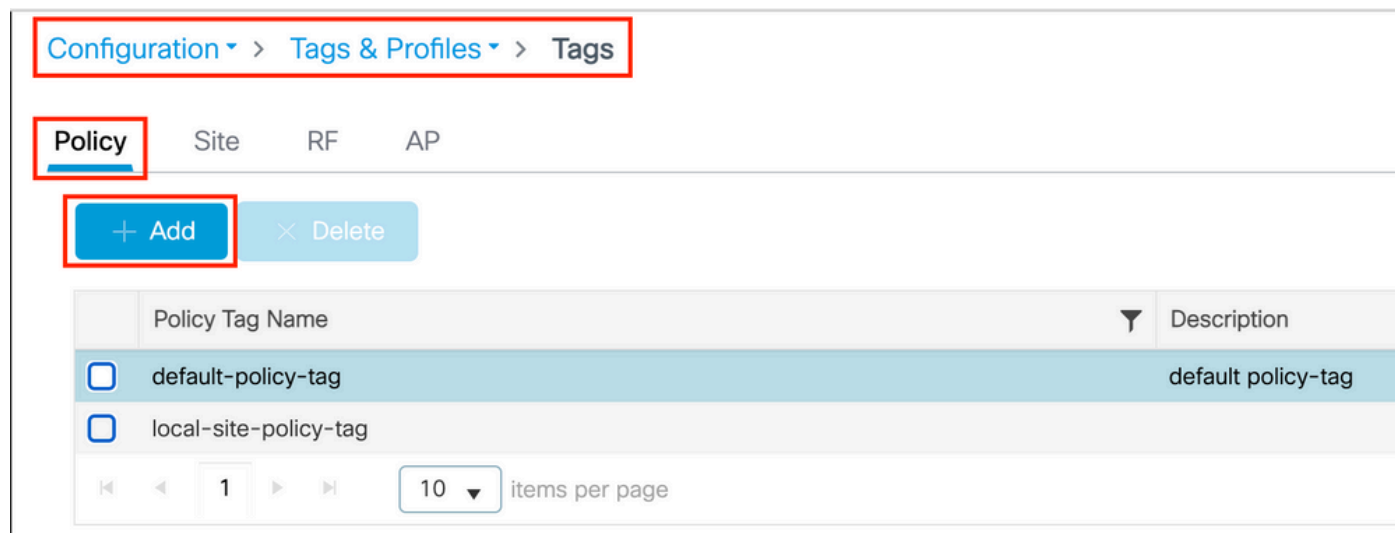
## Configuration des balises des politiques

Vous pouvez associer votre SSID à votre profil de politiques dans la balise de politiques. Vous pouvez soit créer une nouvelle balise de politiques, soit utiliser la balise de politique par défaut.

 **Remarque :** la balise default-policy mappe automatiquement tout SSID dont l'ID WLAN est compris entre 1 et 16 au profil default-policy. Il ne peut pas être modifié ou supprimé. Si vous avez un WLAN avec l'ID 17 ou ultérieur, la balise default-policy ne peut pas être utilisée.

IUG:

Naviguez jusqu'à Configuration > Tags & Profiles > Tags > Policy et ajoutez-en un nouveau si nécessaire, comme indiqué dans l'image.



The screenshot shows a web interface for configuring policy tags. The breadcrumb navigation is 'Configuration > Tags & Profiles > Tags'. Below this, there are tabs for 'Policy', 'Site', 'RF', and 'AP', with 'Policy' selected. There are two buttons: '+ Add' and '× Delete'. Below the buttons is a table with two columns: 'Policy Tag Name' and 'Description'. The table contains two entries: 'default-policy-tag' with description 'default policy-tag' and 'local-site-policy-tag'. At the bottom, there is a pagination control showing '1' of 10 items per page.

Policy Tag Name	Description
<input type="checkbox"/> default-policy-tag	default policy-tag
<input type="checkbox"/> local-site-policy-tag	

Liez votre profil de réseau WLAN au profil de politiques souhaité.

### Add Policy Tag ✕

Name\*

Description

▼ WLAN-POLICY Maps: 1

WLAN Profile	Policy Profile
<input type="checkbox"/> cwa-ssid	default-policy-profile

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

➤ RLAN-POLICY Maps: 0

CLI :

```
# config t # wireless tag policy <policy-tag-name> # wlan <profile-name> policy <policy-profile-name>
```

Affectation des balises des politiques

Affectez la balise de politiques aux points d'accès nécessaires.


IUG:

Afin d'attribuer la balise à un AP, naviguez jusqu'à Configuration > Wireless > Access Points > AP Name > General Tags, faites l'attribution nécessaire, puis cliquez sur Update & Apply to Device.

### Edit AP

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

General	Tags
AP Name*	<p>⚠ Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.</p>
Location*	
Base Radio MAC	Policy <input type="text" value="cwa-policy-tag"/>
Ethernet MAC	Site <input type="text" value="default-site-tag"/>
Admin Status <input checked="" type="checkbox"/> ENABLED	RF <input type="text" value="default-rf-tag"/>
AP Mode <input type="text" value="Local"/>	Write Tag Config to AP <input type="checkbox"/> ⓘ
Operation Status Registered	

 **Remarque** : sachez qu'après avoir modifié la balise de stratégie sur un AP, il perd son association avec le WLC 9800 et se reconnecte dans environ 1 minute.

Afin d'attribuer la même balise de stratégie à plusieurs AP, accédez à Configuration > Wireless > Wireless Setup > Advanced > Start Now.



Start

## Tags & Profiles



WLAN Profile



Policy Profile



Policy Tag



AP Join Profile



Flex Profile



Site Tag



RF Profile



RF Tag



## Apply



Tag APs



Start Now →

Done

Configuration > Wireless Setup > Advanced

Show Me How

+ Tag APs

Number of APs: 2  
Selected Number of APs: 2

<input checked="" type="checkbox"/>	AP Name	AP Model	AP MAC	Serial Number	AP Mode	Admin Status	Operation Status	Policy Tag	Site Tag	RF Tag
<input checked="" type="checkbox"/>	[blurred]	AIR-AP1815I-E-K9	[blurred]	[blurred]	Flex	Disabled	Registered	local-site-policy-tag	flex-site-tag	defa rf-ta
<input checked="" type="checkbox"/>	[blurred]	AIR-AP1815I-E-K9	[blurred]	[blurred]	Local	Enabled	Registered	default-policy-tag	default-site-tag	defa rf-ta

10 items per page 1 - 2 of 2 items

Choisissez la balise souhaitée et cliquez sur Save & Apply to Device comme indiqué dans l'image.

## Tag APs

Tags

Policy

Site

RF

*Changing AP Tag(s) will cause associated AP(s) to rejoin and disrupt connected client(s)*

CLI :

```
# config t # ap <ethernet-mac-addr> # policy-tag <policy-tag-name> # end
```

## Configuration d'une liste de contrôle d'accès de redirection

Étape 1. Accédez à Configuration > Security > ACL > + Add afin de créer une nouvelle liste de contrôle d'accès.

Choisissez un nom pour la liste de contrôle d'accès, faites-la IPv4 Extended taper et ajoutez chaque règle sous forme de séquence, comme illustré dans l'image.

Add ACL Setup
✕

ACL Name\*

ACL Type

**Rules**

Sequence\*

Source Type

Destination Type

Protocol

Log

Action

Host Name\*  ! This field is mandatory

DSCP

+ Add
✕ Delete

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
No items to display										

Cancel
Apply to Device

Vous devez refuser le trafic vers vos nœuds PSN ISE, refuser le DNS et autoriser tout le reste. Cette liste de contrôle d'accès de redirection n'est pas une liste de contrôle d'accès de sécurité, mais une liste de contrôle d'accès ponctuelle qui définit le trafic acheminé vers le processeur (en cas d'autorisation) pour un traitement ultérieur (comme la redirection) et le trafic restant sur le plan de données (en cas de refus) et qui évite la redirection.

La liste de contrôle d'accès doit ressembler à ceci (remplacez 10.48.39.28 par votre adresse IP ISE dans cet exemple) :

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
<input type="checkbox"/> 10	deny	any		10.48.39.28		ip			None	Disabled
<input type="checkbox"/> 20	deny	10.48.39.28		any		ip			None	Disabled
<input type="checkbox"/> 30	deny	any		any		udp		eq domain	None	Disabled
<input type="checkbox"/> 40	deny	any		any		udp	eq domain		None	Disabled
<input type="checkbox"/> 50	permit	any		any		tcp		eq www	None	Disabled

**Remarque :** pour la liste de contrôle d'accès de redirection, considérez l'deny action comme une redirection de refus (et non comme un trafic de refus) et l'permit action comme une redirection d'autorisation. Le WLC examine uniquement le trafic qu'il peut rediriger (ports 80 et 443 par défaut).

CLI :

```
ip access-list extended REDIRECT
deny ip any host <ISE-IP>
deny ip host<ISE-IP> any
deny udp any any eq domain
deny udp any eq domain any
permit tcp any any eq 80
```



**Remarque** : si vous terminez la liste de contrôle d'accès avec une `permit ip any any` autorisation axée sur le port 80, le WLC redirige également HTTPS, ce qui est souvent indésirable car il doit fournir son propre certificat et crée toujours une violation de certificat. Il s'agit de l'exception à l'instruction précédente qui dit que vous n'avez pas besoin d'un certificat sur le WLC dans le cas de CWA : vous en avez besoin si vous avez l'interception HTTPS activée, mais elle n'est jamais considérée comme valide de toute façon.

---

Vous pouvez améliorer la liste de contrôle d'accès en refusant uniquement le port invité 8443 au serveur ISE.

Activer la redirection pour HTTP ou HTTPS

La configuration du portail d'administration Web est liée à la configuration du portail d'authentification Web et doit écouter sur le port 80 afin de rediriger. Par conséquent, HTTP doit être activé pour que la redirection fonctionne correctement. Vous pouvez choisir de l'activer globalement (avec l'utilisation de la commande `ip http server`) ou vous pouvez activer HTTP pour le module d'authentification Web uniquement (avec l'utilisation de la commande `webauth-http-enable` sous la carte de paramètre).



**Remarque** : la redirection du trafic HTTP se produit à l'intérieur de CAPWAP, même dans le cas de la commutation locale FlexConnect. Puisque c'est le WLC qui fait le travail d'interception, le point d'accès envoie les paquets HTTP(S) à l'intérieur du tunnel CAPWAP et reçoit la redirection du WLC dans CAPWAP

---

Si vous voulez être redirigé lorsque vous essayez d'accéder à une URL HTTPS, ajoutez alors la commande `intercept-https-enable` sous le mappage de paramètre mais notez qu'il ne s'agit pas d'une configuration optimale, qu'elle a un impact sur le CPU du WLC et génère quand même des erreurs de certificat :

```
<#root>
```

```
parameter-map type webauth global
```

type webauth

intercept-https-enable

trustpoint xxxxx

Vous pouvez également le faire via l'interface graphique avec l'option 'Web Auth intercept HTTPS' cochée dans la carte de paramètres (Configuration > Security > Web Auth).

The screenshot displays the 'Edit Web Auth Parameter' configuration page. On the left, a navigation sidebar includes 'Dashboard', 'Monitoring', 'Configuration', 'Administration', 'Licensing', and 'Troubleshooting'. The main content area is titled 'Configuration > Security > Web Auth' and features a table of parameter maps. The 'global' map is selected, and its details are shown in the right-hand panel. The 'Web Auth intercept HTTPS' checkbox is checked and highlighted with a red box. Other parameters include 'Maximum HTTP connections' (100), 'Init-State Timeout(secs)' (120), 'Type' (webauth), 'Virtual IPv4 Address', 'Trustpoint' (--- Select ---), 'Virtual IPv6 Address' (X::X::X::X), and 'Captive Bypass Portal' (unchecked).

Parameter Map Name
<input type="checkbox"/> global

Edit Web Auth Parameter	
Maximum HTTP connections	100
Init-State Timeout(secs)	120
Type	webauth
Virtual IPv4 Address	
Trustpoint	--- Select ---
Virtual IPv6 Address	X::X::X::X
Web Auth intercept HTTPS	<input checked="" type="checkbox"/>
Captive Bypass Portal	<input type="checkbox"/>



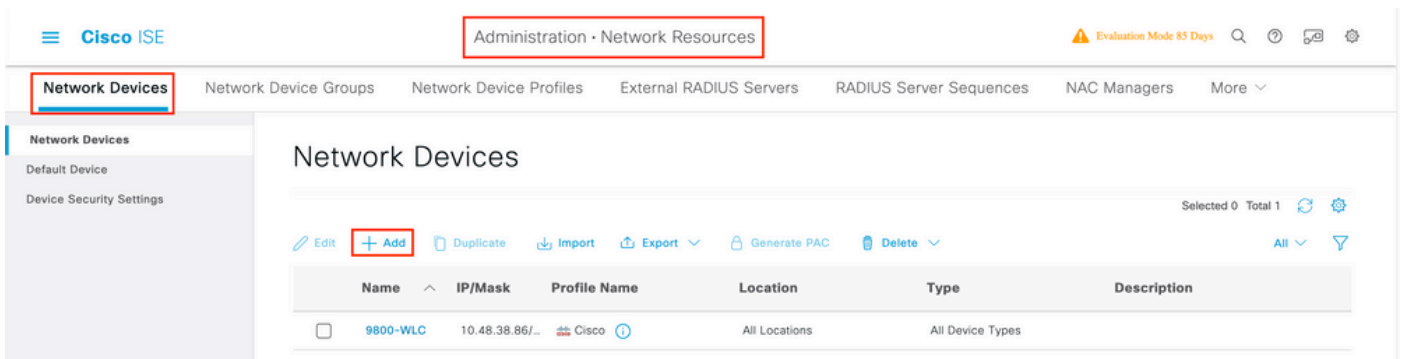
**Remarque** : par défaut, les navigateurs utilisent un site Web HTTP pour lancer le processus de redirection. Si la redirection HTTPS est nécessaire, l'interception de l'authentification Web HTTPS doit être vérifiée. Toutefois, cette configuration n'est pas recommandée car elle augmente l'utilisation du processeur.

---

## Configuration ISE

Ajouter un contrôleur WLC 9800 à ISE

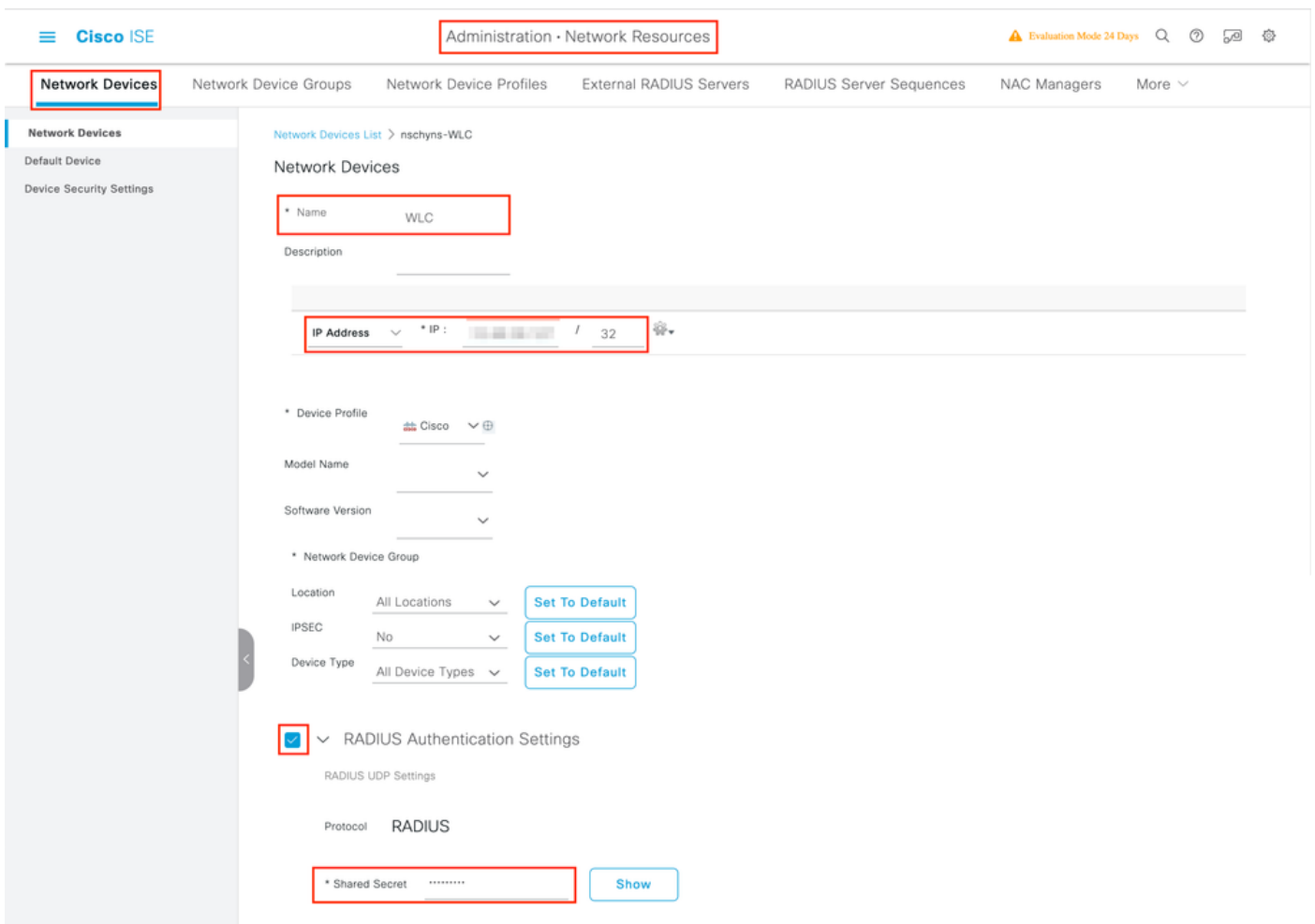
Étape 1. Ouvrez la console ISE et accédez Administration > Network Resources > Network Devices > Add à comme indiqué dans l'image.



Étape 2. Configurez le périphérique réseau.

Il peut éventuellement s'agir d'un nom de modèle, d'une version de logiciel et d'une description spécifiés, et attribuer des groupes de périphériques réseau en fonction des types de périphériques, de l'emplacement ou des WLC.

L'adresse IP correspond ici à l'interface WLC qui envoie les requêtes d'authentification. Par défaut, il s'agit de l'interface de gestion, comme illustré dans l'image :

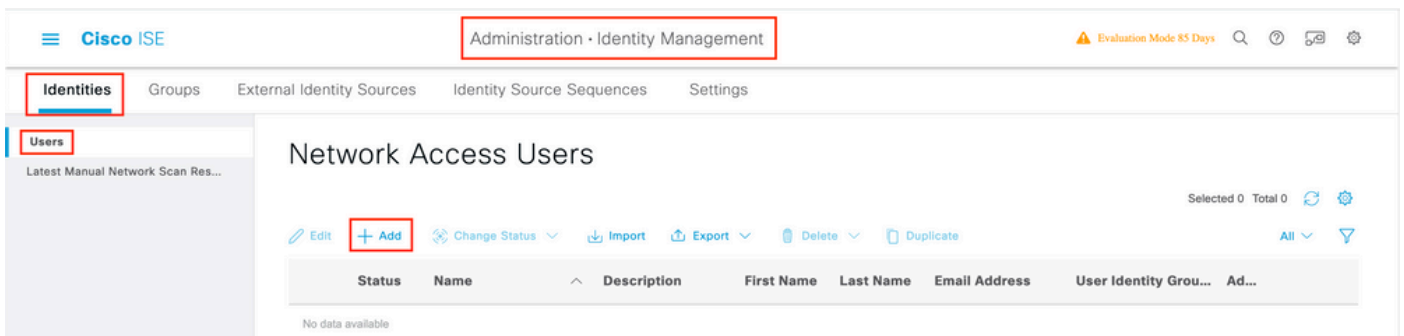


Pour plus d'informations sur les groupes de périphériques réseau, consultez le chapitre du guide d'administration d'ISE : Gestion des périphériques réseau : [ISE - Groupes de périphériques réseau](#).

Créer un nouvel utilisateur sur ISE

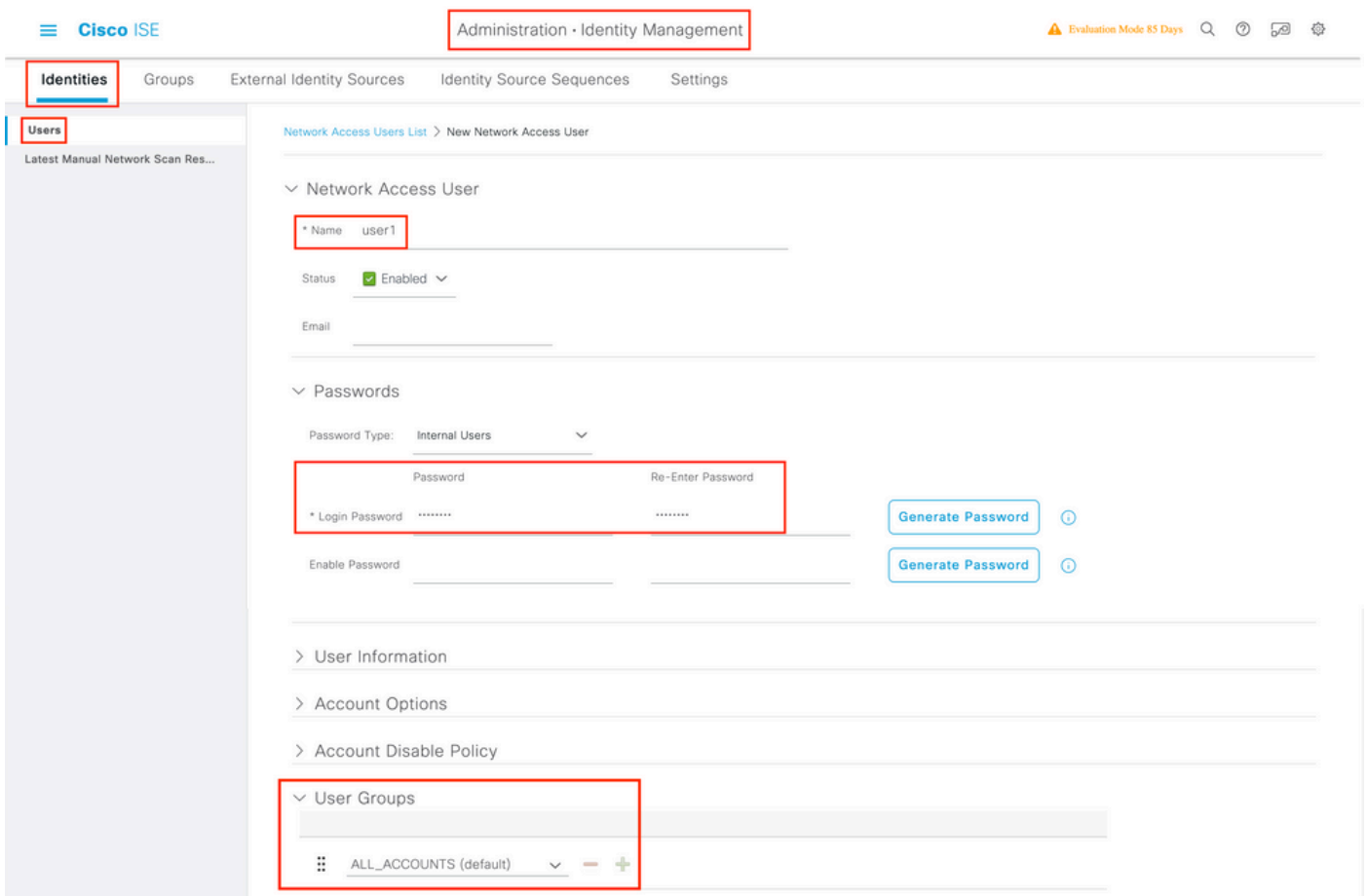


Étape 1. Naviguez jusqu'à Administration > Identity Management > Identities > Users > Add comme indiqué dans l'image.



Étape 2. Entrez l'information.

Dans cet exemple, cet utilisateur appartient à un groupe appelé ALL\_ACCOUNTS mais il peut être ajusté selon les besoins, comme le montre l'image.



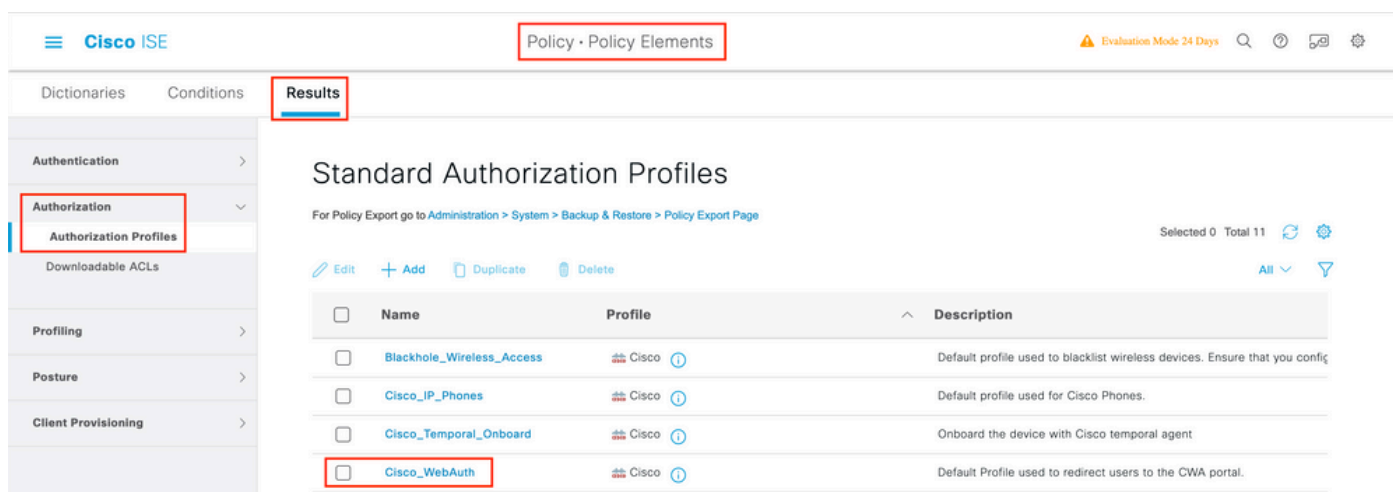
Créer un profil d'autorisation

Le profil de stratégie est le résultat attribué à un client en fonction de ses paramètres (tels que l'adresse MAC, les informations d'identification, le WLAN utilisé, etc.). Il peut attribuer des paramètres spécifiques tels que le réseau local virtuel (VLAN), les listes de contrôle d'accès (ACL), les redirections d'URL, etc.

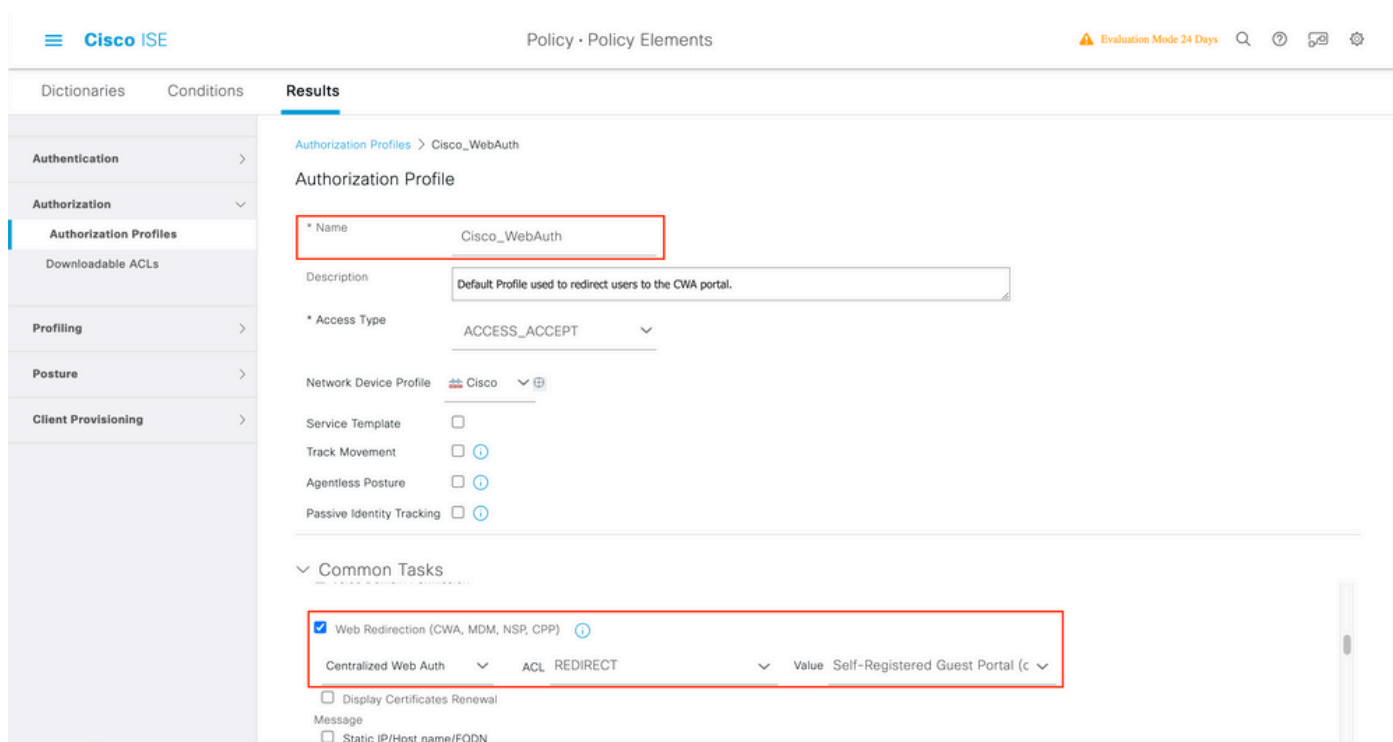
Notez que dans les versions récentes d'ISE, un résultat d'autorisation Cisco\_Webauth existe déjà. Ici, vous pouvez le modifier pour modifier le

nom de la liste de contrôle d'accès de redirection afin qu'il corresponde à ce que vous avez configuré sur le contrôleur WLC.

Étape 1. Accédez à Policy > Policy Elements > Results > Authorization > Authorization Profiles. Cliquez sur add afin de créer votre propre ou modifier le résultat par Cisco\_Webauth défaut.

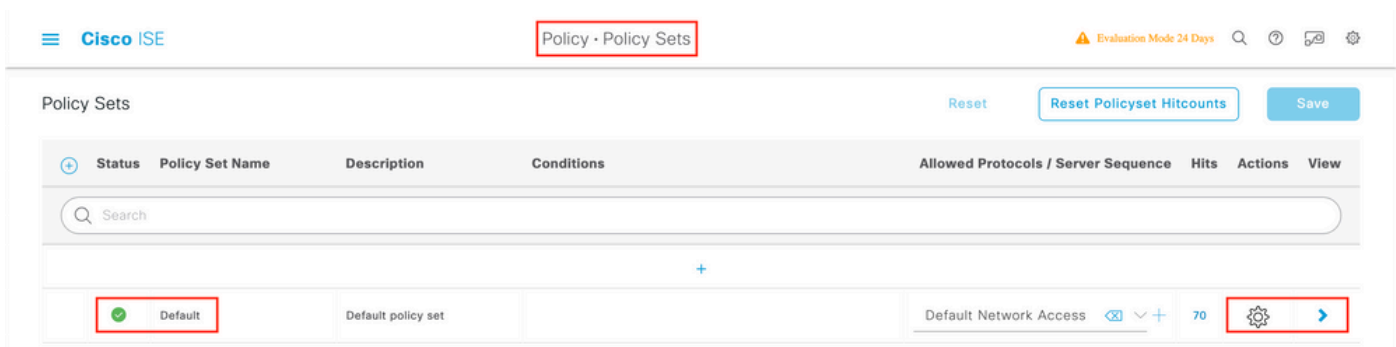


Étape 2. Entrez les informations de redirection. Assurez-vous que le nom de la liste de contrôle d'accès est le même que celui configuré sur le WLC 9800.

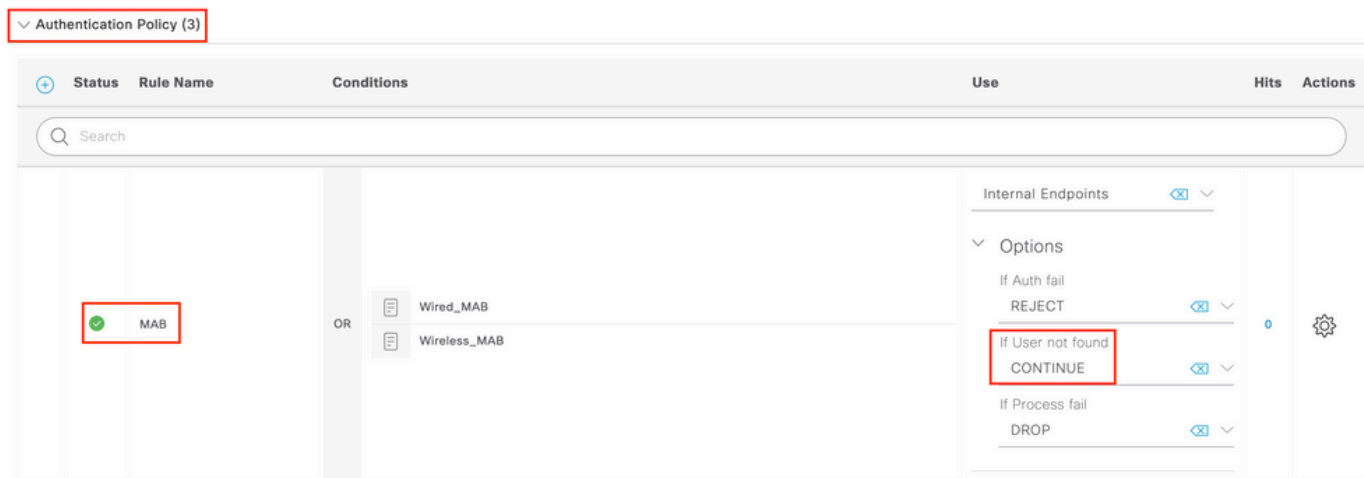


## Configurer une règle d'authentification

Étape 1. Un ensemble de stratégies définit un ensemble de règles d'authentification et d'autorisation. Pour en créer un, accédez à Policy > Policy Sets à, cliquez sur l'engrenage du premier jeu de stratégies de la liste et Insert new row choisissez ou cliquez sur la flèche bleue à droite pour choisir le jeu de stratégies par défaut.



Étape 2. Développez Authentication la stratégie. Pour la règle MAB (correspondance sur MAB filaire ou sans fil), développez Options, et choisissez l'CONTINUE option au cas où vous verriez « Si l'utilisateur est introuvable ».



Étape 3. Cliquez sur Save afin d'enregistrer les modifications.

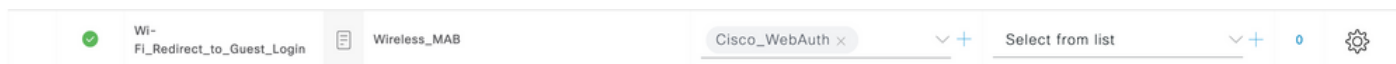
Configurer les règles d'autorisation

La règle d'autorisation est celle qui détermine quelles autorisations (quel profil d'autorisation) s'appliquent au client.

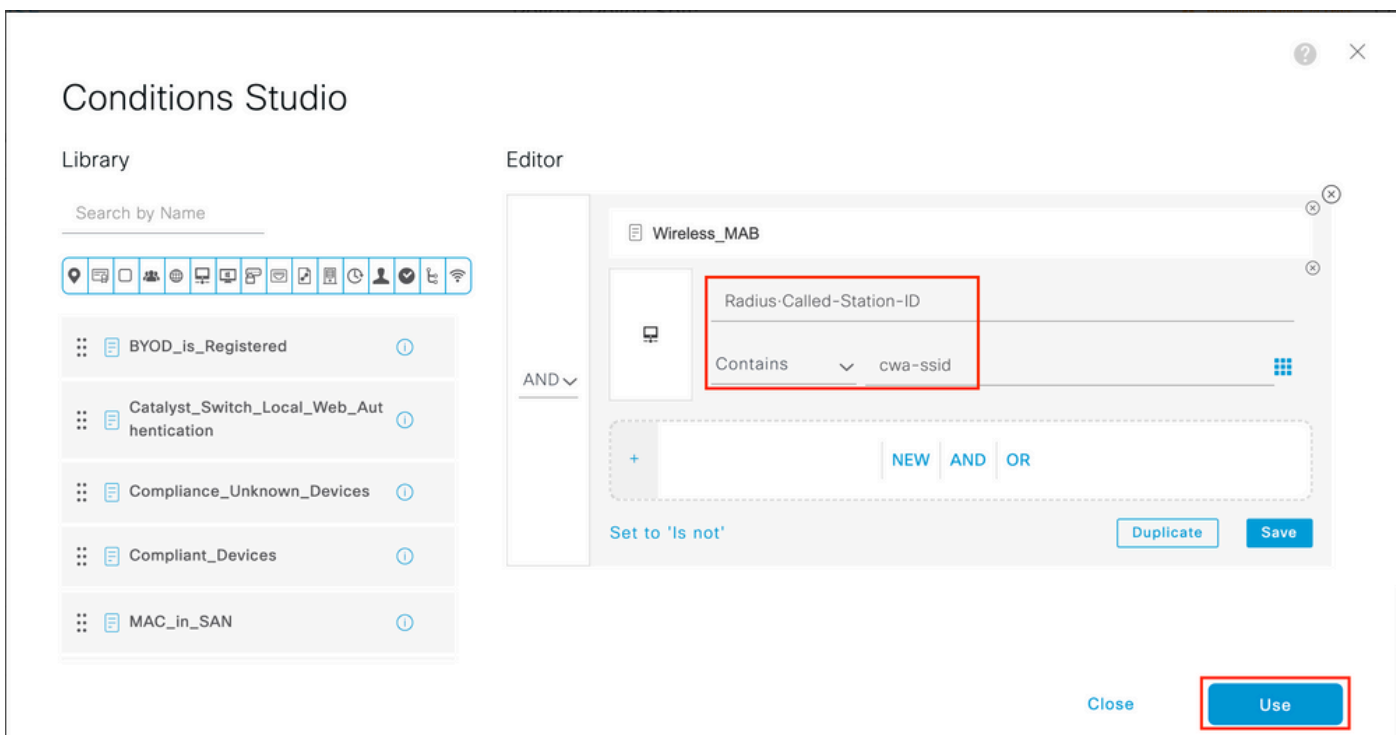
Étape 1. Sur la même page Jeu de stratégies, fermez le Authentication Policy et développez Authorziation Policy comme indiqué dans l'image.



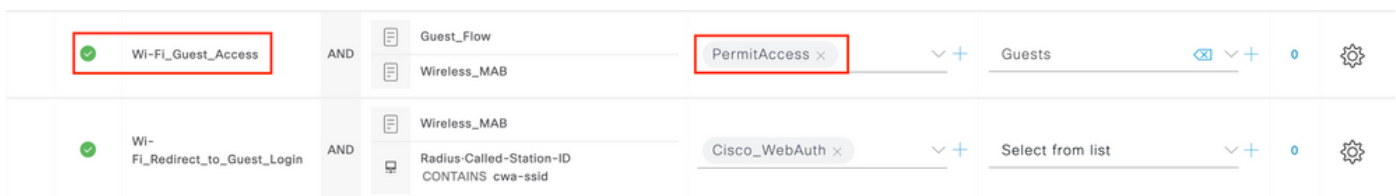
Étape 2. Les versions récentes d'ISE commencent par une règle précréée appelée Wifi\_Redirect\_to\_Guest\_Login qui correspond principalement à nos besoins. Tournez le signe gris sur la gauche vers enable.



Étape 3. Cette règle correspond uniquement à Wireless\_MAB et renvoie les attributs de redirection CWA. Maintenant, vous pouvez éventuellement ajouter une petite torsion et faire correspondre seulement le SSID spécifique. Choisissez la condition (Wireless\_MAB à partir de maintenant) pour faire apparaître Conditions Studio. Ajoutez une condition à droite et choisissez le dictionnaireRadius avec l'Called-Station-ID attribut. Faites en sorte qu'il corresponde à votre nom SSID. Validez avec le Use en bas de l'écran, comme illustré dans l'image.



Étape 4. Guest Flow Vous avez maintenant besoin d'une deuxième règle, définie avec une priorité plus élevée, qui corresponde à la condition afin de renvoyer les détails d'accès au réseau une fois que l'utilisateur s'est authentifié sur le portail. Vous pouvez utiliser la règleWifi Guest Access qui est également précréée par défaut sur les versions récentes d'ISE. Il vous suffit ensuite d'activer la règle avec une marque verte à gauche. Vous pouvez renvoyer le paramètre PermitAccess par défaut ou configurer des restrictions de liste d'accès plus précises.



Étape 5. Enregistrez les règles.

Cliquez Save au bas des règles.

Points d'accès de commutation locale Flexconnect UNIQUEMENT

Que faire si vous avez des points d'accès de commutation locaux Flexconnect et des WLAN? Les sections précédentes sont toujours valides. Cependant, vous avez besoin d'une étape supplémentaire afin de pousser l'ACL de redirection aux AP à l'avance.

Accédez à votre profil FlexConfiguration > Tags & Profiles > Flex et sélectionnez-le. Accédez ensuite à l'Policy ACLonglet.

Cliquez sur Add comme indiqué dans l'image.

The screenshot shows the 'Edit Flex Profile' interface with the 'Policy ACL' tab selected. A red box highlights the '+ Add' button. Below the button, there is a table with columns for 'ACL Name', 'Central Web Auth', and 'URL Filter'. The table shows 0 items per page and a 'No items to display' message.

Choisissez le nom de votre ACL de redirection et activez l'authentification Web centralisée. Cette case à cocher inverse automatiquement la liste de contrôle d'accès sur l'AP lui-même (car une instruction « deny » signifie « ne pas rediriger vers cette IP » sur le WLC dans Cisco IOS XE. Cependant, sur l'AP, l'instruction 'deny' signifie le contraire. Ainsi, cette case à cocher permute automatiquement toutes les autorisations et les refuse lorsqu'elle effectue la poussée vers le point d'accès. Vous pouvez le vérifier à l'aide d'uneshow ip access list commande de l'AP (CLI).

**Remarque :** dans un scénario de commutation locale Flexconnect, la liste de contrôle d'accès doit mentionner spécifiquement les instructions de retour (ce qui n'est pas nécessairement requis en mode local). Assurez-vous donc que toutes vos règles de liste de contrôle d'accès couvrent les deux modes de trafic (vers et depuis l'ISE par exemple).

N'oubliez pas de frapper Save et puis Update and apply to the device.

The screenshot shows the 'Edit Flex Profile' interface with the 'Policy ACL' tab selected. A modal dialog is open for adding a new ACL. The 'ACL Name\*' field is set to 'REDIRECT', and the 'Central Web Auth' checkbox is checked. The 'Save' button is highlighted.

## Certificats

Pour que le client fasse confiance au certificat d'authentification Web, il n'est pas nécessaire d'installer un certificat sur le WLC car le seul certificat présenté est le certificat ISE (qui doit être approuvé par le client).

Vérifier

Vous pouvez utiliser ces commandes pour vérifier la configuration actuelle.

```
<#root>
```

```
# show run wlan # show run aaa # show aaa servers # show ap config general # show ap name <ap-name> config general
# show ap tag summary
# show ap name <AP-name> tag detail
# show wlan { summary | id | nme | all }
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
```

Voici la partie pertinente de la configuration du WLC qui correspond à cet exemple :

```
<#root>
```

```
aaa new-model !
aaa authorization network CWAauthz group radius aaa accounting identity CWAacct start-stop group radius ! aaa server radius dynamic-author client <ISE
mac-filtering CWAauthz
no security ft adaptive
no security wpa
no security wpa wpa2
no security wpa wpa2 ciphers aes
no security wpa akmp dot1x
no shutdown
ip http server (or "webauth-http-enable" under the parameter map)
ip http secure-server
```

Dépannage

Liste de vérification

- Assurez-vous que le client se connecte et obtient une adresse IP valide.
- Si la redirection n'est pas automatique, ouvrez un navigateur et essayez une adresse IP aléatoire. Par exemple, 10.0.0.1. Si la redirection fonctionne, il est possible que vous ayez un problème de résolution DNS. Vérifiez que vous disposez d'un serveur DNS valide fourni via DHCP et qu'il peut résoudre les noms d'hôte.
- Assurez-vous que vous avez configuré la commande `ip http server` pour que la redirection sur HTTP fonctionne. La configuration du portail d'administration Web est liée à la configuration du portail d'authentification Web et doit être répertoriée sur le port 80 pour

pouvoir être redirigée. Vous pouvez choisir de l'activer globalement (avec l'utilisation de la commande ip http server) ou vous pouvez activer HTTP pour le module d'authentification Web uniquement (avec l'utilisation de la commande webauth-http-enable sous la carte de paramètre).

- Si vous n'êtes pas redirigé lorsque vous essayez d'accéder à une URL HTTPS et que cela est requis, vérifiez que vous avez la commande intercept-https-enable sous le mappage de paramètre :

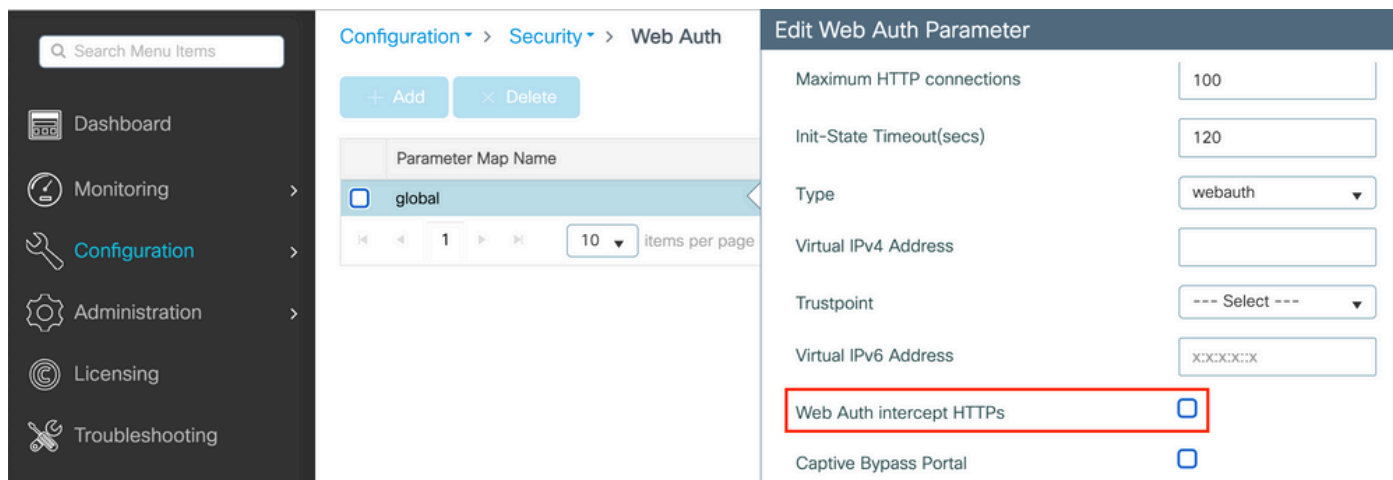
```
<#root>
```

```
parameter-map type webauth global  
type webauth
```

```
intercept-https-enable
```

```
trustpoint xxxxx
```

Vous pouvez également vérifier via l'interface graphique que l'option 'Web Auth intercept HTTPS' est cochée dans la carte des paramètres :



The screenshot shows the Cisco configuration interface. On the left is a navigation menu with options like Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main area is titled 'Configuration > Security > Web Auth'. Below this, there are '+ Add' and 'Delete' buttons, and a table with 'Parameter Map Name' and a 'global' entry. To the right, the 'Edit Web Auth Parameter' page is open, showing various settings: Maximum HTTP connections (100), Init-State Timeout(secs) (120), Type (webauth), Virtual IPv4 Address, Trustpoint (--- Select ---), Virtual IPv6 Address (xxxx:xx:xx:xx), Web Auth intercept HTTPS (checked), and Captive Bypass Portal (unchecked). The 'Web Auth intercept HTTPS' checkbox is highlighted with a red box.

Prise en charge des ports de service pour RADIUS

Le contrôleur sans fil de la gamme Cisco Catalyst 9800 dispose d'un port de service appelé GigabitEthernet 0port. À partir de la version 17.6.1, RADIUS (qui inclut CoA) est pris en charge par ce port.

Si vous souhaitez utiliser le port de service pour RADIUS, vous devez disposer de la configuration suivante :

```
<#root>
```

```
aaa server radius dynamic-author  
client 10.48.39.28
```

```
vrf Mgmt-intf
```

```
server-key cisco123

interface GigabitEthernet0

vrf forwarding Mgmt-intf

ip address x.x.x.x x.x.x.x

!if using aaa group server:
aaa group server radius group-name
server name nicoISE


ip vrf forwarding Mgmt-intf

ip radius source-interface GigabitEthernet0
```

Collecter les débogages

Le contrôleur WLC 9800 offre des fonctionnalités de traçage TOUJOURS ACTIVES. Cela garantit que toutes les erreurs, avertissements et messages de niveau de notification liés à la connectivité du client sont constamment consignés et que vous pouvez afficher les journaux d'un incident ou d'une défaillance après qu'il se soit produit.

---

 **Remarque** : vous pouvez revenir en arrière de quelques heures à plusieurs jours dans les journaux, mais cela dépend du volume de journaux générés.

---

Afin d'afficher les traces que le WLC 9800 a collectées par défaut, vous pouvez vous connecter via SSH/Telnet au WLC 9800 et effectuer ces étapes (assurez-vous que vous consignez la session dans un fichier texte).

Étape 1. Vérifiez l'heure actuelle du WLC de sorte que vous puissiez suivre les journaux dans le temps de retour à quand le problème s'est produit.

```
<#root>
```

```
# show clock
```

Étape 2. Collectez les syslogs à partir de la mémoire tampon WLC ou du syslog externe comme dicté par la configuration du système. Cela permet d'avoir un aperçu rapide de l'état du système et des erreurs éventuelles.



```
<#root>
```


```
# show logging
```

Étape 3. Vérifiez si les conditions de débogage sont activées.

```
<#root>
```

```
# show debugging Cisco IOS XE Conditional Debug Configs: Conditional Debug Global State: Stop Cisco IOS XE Packet Tracing Configs: Packet Infra d
```

---

 **Remarque** : si une condition est répertoriée, cela signifie que les traces sont consignées au niveau de débogage pour tous les processus qui rencontrent les conditions activées (adresse MAC, adresse IP, etc.). Cela augmente le volume des journaux. Par conséquent, il est recommandé d'effacer toutes les conditions lorsque vous ne déboguez pas activement.

---

Étape 4. En supposant que l'adresse MAC testée n'était pas répertoriée comme condition à l'étape 3., collectez les traces de niveau de notification toujours actif pour l'adresse MAC spécifique.

```
<#root>
```

```
# show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file always-on-<FILENAME.txt>
```

Vous pouvez soit afficher le contenu de la session, soit copier le fichier sur un serveur TFTP externe.

```
<#root>
```

```
# more bootflash:always-on-<FILENAME.txt>
```

```
or
```

```
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

## Débogage conditionnel et traçage Radio Active

Si les traces toujours actives ne vous donnent pas suffisamment d'informations pour déterminer le déclencheur du problème en cours d'investigation, vous pouvez activer le débogage conditionnel et capturer la trace Radio Active (RA), qui fournit des traces au niveau du débogage pour tous les processus qui interagissent avec la condition spécifiée (l'adresse MAC du client dans ce cas). Afin d'activer le débogage conditionnel, passez à ces étapes.

Étape 5. Assurez-vous qu'aucune condition de débogage n'est activée.

```
<#root>
```

```
# clear platform condition all
```


Étape 6. Activez la condition de débogage pour l'adresse MAC du client sans fil que vous souhaitez surveiller.

Ces commandes commencent à surveiller l'adresse MAC fournie pendant 30 minutes (1 800 secondes). Vous pouvez aussi augmenter ce délai pour qu'il atteigne jusqu'à 2085978494 secondes.


```
<#root>
```

```
# debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

---

 **Remarque** : pour surveiller plusieurs clients à la fois, exécutez la commande `debug wireless mac<aaaa.bbbb.cccc>` par adresse mac.

---

 **Remarque** : vous ne voyez pas le résultat de l'activité du client sur la session du terminal, car tout est mis en mémoire tampon en interne pour être visualisé ultérieurement.

---

Étape 7». Reproduisez le problème ou le comportement que vous souhaitez surveiller.

Étape 8. Arrêtez le débogage si le problème est reproduit avant la fin du temps de surveillance par défaut ou configuré.

```
<#root>
```

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

Une fois le temps de surveillance écoulé ou le débogage sans fil arrêté, le WLC 9800 génère un fichier local avec le nom :

```
ra_trace_MAC_aaaabbbccccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Étape 9. Collectez le fichier de l'exercice d'adressage MAC. Vous pouvez copier le fichier `ra_trace .log` sur un serveur externe ou afficher le

résultat directement à l'écran.

Vérifiez le nom du fichier de suivi RA.

```
<#root>
```

```
# dir bootflash: | inc ra_trace
```

Copiez le fichier sur un serveur externe :

```
<#root>
```

```
# copy bootflash: ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.d/ra-FILENAME.txt
```

Affichez-en le contenu :

```
<#root>
```


```
# more bootflash: ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Étape 10. Si la cause première n'est toujours pas évidente, collectez les journaux internes qui sont une vue plus détaillée des journaux de niveau débogage. Vous n'avez pas besoin de déboguer à nouveau le client, car nous examinons seulement plus en détail les journaux de débogage qui ont déjà été collectés et stockés en interne.

```
<#root>
```

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file ra-internal-<FILENAME>.txt
```

---

 **Remarque** : cette sortie de commande retourne des traces pour tous les niveaux de log pour tous les processus et est assez volumineuse. Contactez le TAC Cisco pour vous aider à analyser ces traces.

---

Vous pouvez copier le fichier ra-internal-FILENAME.txt sur un serveur externe ou afficher le résultat directement à l'écran.

Copiez le fichier sur un serveur externe :

```
<#root>
```

```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```

Affichez-en le contenu :

```
<#root>
```

```
# more bootflash:ra-internal-<FILENAME>.txt
```

Étape 11. Supprimez les conditions de débogage.

```
<#root>
```

```
# clear platform condition all
```



**Remarque** : assurez-vous de toujours supprimer les conditions de débogage après une session de dépannage.

## Exemples

Si le résultat de l'authentification n'est pas ce que vous attendiez, il est important de naviguer jusqu'à la page ISEOperations > Live logs et d'obtenir les détails du résultat de l'authentification.

La raison de la panne (en cas de panne) et tous les attributs Radius reçus par ISE s'affichent.

Dans l'exemple suivant, ISE a rejeté l'authentification, car aucune règle d'autorisation n'y correspondait. En effet, vous voyez l'attribut Called-station-ID envoyé en tant que nom SSID ajouté à l'adresse MAC AP, alors que l'autorisation correspond exactement au nom SSID. Elle est corrigée avec la modification de cette règle en 'contient' au lieu de 'égal'.

Event	5400 Authentication failed
Failure Reason	15039 Rejected per authorization profile
Resolution	Authorization Profile with ACCESS_REJECT attribute was selected as a result of the matching authorization rule. Check the appropriate Authorization policy rule-results.
Root cause	Selected Authorization Profile contains ACCESS_REJECT attribute
Username	E8:36:17:1F:A1:62

```
15048 Queried PIP - Radius.NAS-Port-1-type
15048 Queried PIP - Network Access.UserName
15048 Queried PIP - IdentityGroup.Name (2 times)
15048 Queried PIP - EndPoints.LogicalProfile
15048 Queried PIP - Radius.Called-Station-ID
15048 Queried PIP - Network Access.AuthenticationStatus
15016 Selected Authorization Profile - DenyAccess
15039 Rejected per authorization profile
11003 Returned RADIUS Access-Reject
```



## Other Attributes

ConfigVersionId	140
Device Port	58209
DestinationPort	1812
RadiusPacketType	AccessRequest
Protocol	Radius
NAS-Port	71111
Framed-MTU	1485
OriginalUserName	e836171fa162
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	nicolse26/356963261/1
UseCase	Host Lookup
SelectedAuthenticationIdentityStores	Internal Endpoints
IdentityPolicyMatchedRule	MAB
AuthorizationPolicyMatchedRule	Default
EndPointMACAddress	E8-36-17-1F-A1-62
ISEPolicySetName	Default
IdentitySelectionMatchedRule	MAB
DTLSSupport	Unknown
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
RADIUS Username	E8:36:17:1F:A1:62
NAS-Identifler	cwa-ssid
Device IP Address	10.48.71.120
CPMSessionID	7847300A0000012DFC227BF1
Called-Station-ID	00-27-e3-8f-33-a0:cwa-ssid
CiscoAVPair	service-type=Call Check, audit-session-id=7847300A0000012DFC227BF1, method=mab, client-if-id=3003124185, vlan-id=1468, cisco-wlan-ssid=cwa-ssid

Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Troubleshooting

Troubleshooting > Radioactive Trace

Conditional Debug Global State: **Stopped**

+ Add Delete Start Stop

MAC/IP Address	Trace file
<input type="checkbox"/> e836.171f.a162	debugTrace_e836.171f.a162.txt <a href="#">Download</a>

10 Items per page 1 - 1 of 1 items

Generate

Dans ce cas, le problème réside dans le fait que vous avez fait une faute de frappe lorsque vous avez créé le nom de la liste de contrôle d'accès et il ne correspond pas au nom de la liste de contrôle d'accès retourné par les ISE ou le WLC se plaint qu'il n'y a pas de liste de contrôle d'accès comme celle demandée par ISE :

<#root>

2019/09/04 12:00:06.507 {wncd\_x\_R0-0}{1}: [client-auth] [24264]: (ERR): MAC: e836.171f.a162 client authz result: FAILURE 2019/09/04 12:00:06.51

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.