

# Configurer la liste d'autorisation AP du contrôleur sans fil Catalyst 9800

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurations](#)

[Liste d'autorisation MAC AP - Local](#)

[Liste d'autorisation MAC AP - Serveur RADIUS externe](#)

[Configuration WLC 9800](#)

[Configuration ISE](#)

[Configurer ISE pour authentifier les adresses MAC en tant que terminaux](#)

[Configurer ISE pour authentifier l'adresse MAC comme nom d'utilisateur/mot de passe](#)

[Stratégie d'autorisation pour authentifier les AP](#)

[Vérifier](#)

[Dépannage](#)

[Références](#)

---

## Introduction

Ce document décrit comment configurer la stratégie d'authentification du point d'accès (AP) du contrôleur LAN sans fil Catalyst 9800.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- 9800 WLC
- Accès aux contrôleurs sans fil via l'interface de ligne de commande (CLI)

### Composants utilisés

Cisco recommande les versions matérielles et logicielles suivantes :

- WLC 9800 v17.3

- AP 1810 W
- AP 1700
- Identity Service Engine (ISE) v2.2

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.

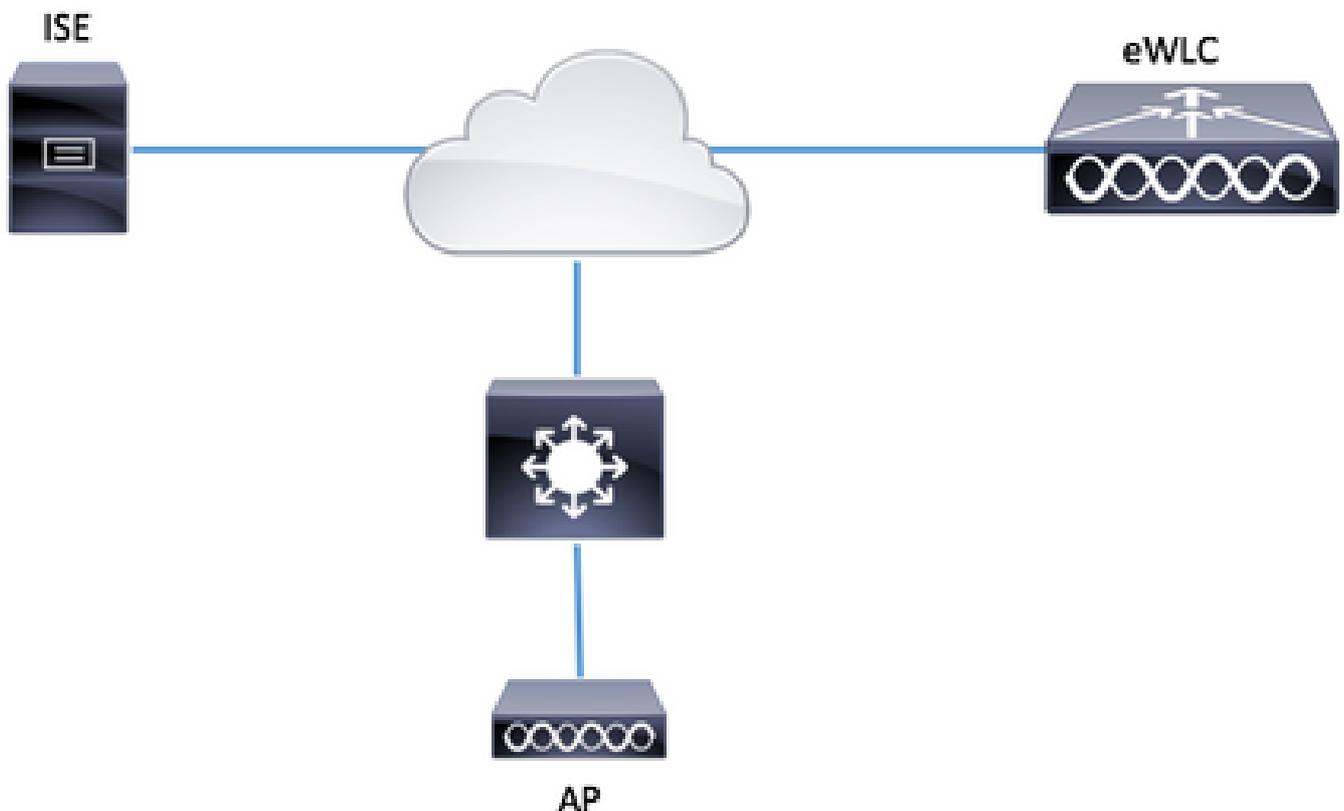
## Informations générales

Pour autoriser un point d'accès, l'adresse MAC Ethernet du point d'accès doit être autorisée sur la base de données locale avec le contrôleur LAN sans fil 9800 ou sur un serveur RADIUS (Remote Authentication Dial-In User Service) externe.

Cette fonctionnalité garantit que seuls les points d'accès autorisés peuvent rejoindre un contrôleur LAN sans fil Catalyst 9800. Ce document ne couvre pas le cas de points d'accès maillés (série 1500) qui nécessitent une entrée de filtre MAC pour joindre le contrôleur, mais ne tracent pas le flux d'autorisation typique des points d'accès (voir références).

## Configurer

### Diagramme du réseau



### Configurations

## Liste d'autorisation MAC AP - Local

Les adresses MAC des points d'accès autorisés sont stockées localement dans le WLC 9800.

Étape 1. Créez une liste de méthodes de téléchargement des informations d'identification d'autorisation locale.

Accédez à Configuration > Security > AAA > AAA Method List > Authorization > + Add.

The screenshot shows the Cisco WLC configuration interface. On the left is a navigation menu with 'Configuration' highlighted. The main area is titled 'Authentication Authorization and Accounting'. Under 'AAA Method List', the 'Authorization' tab is selected. A '+ Add' button is highlighted in red. Below it is a table with two entries:

Name	Type
<input type="checkbox"/> default	network
<input type="checkbox"/> AuthZ-Netw-ISE	network

The screenshot shows the 'Quick Setup: AAA Authorization' dialog box. The fields are filled as follows:

- Method List Name\*: AP-auth
- Type\*: credential-download
- Group Type: local

Below these fields are two lists: 'Available Server Groups' (radius, ldap, tacacs+, ISE-KCG-grp, ISE-grp-name) and 'Assigned Server Groups' (empty). Navigation arrows (> and <) are between the lists. At the bottom are 'Cancel' and 'Save & Apply to Device' buttons.

Étape 2. Activez l'autorisation MAC AP.

Accédez à Configuration > Security > AAA > AAA Advanced > AP Policy. Activez Authorize APs against MAC et sélectionnez la liste de méthodes d'autorisation créée à l'étape 1.

+ AAA Wizard

AAA Method List Servers / Groups **AAA Advanced**

RADIUS Fallback

Attribute List Name

AP Authentication

**AP Policy**

Password Policy

Authorize APs against MAC  ENABLED

Authorize APs against Serial Number  DISABLED

Authorization Method List AP-auth

Apply to Device

Étape 3. Ajoutez l'adresse MAC Ethernet AP.

Accédez à Configuration > Security > AAA > AAA Advanced > Device Authentication > MAC Address > + Add.

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List **AAA Advanced**

Global Config

RADIUS Fallback

Attribute List Name

**Device Authentication**

AP Policy

Password Policy

AAA Interface

MAC Address Serial Number

+ Add × Delete

MAC Address

0 10 items per page

Quick Setup: MAC Filtering

MAC Address\* 00:B0:E1:8C:49:E8

Attribute List Name None

Cancel Save & Apply to Device

---

 Remarque : l'adresse MAC Ethernet AP doit être dans l'un de ces formats lorsqu'elle est entrée dans l'interface utilisateur Web (xx : xx : xx : xx : xx : xx (ou) xxxx.xxxx.xxxx (ou) xx-xx-xx-xx-xx) dans la version 16.12. Dans la version 17.3, ils doivent être au format xxxxxxxxxxxx sans séparateur. Le format de l'interface de ligne de commande est toujours xxxxxxxxxxxx, quelle que soit la version (dans la version 16.12, l'interface utilisateur Web supprime les séparateurs dans la configuration). L'ID de bogue Cisco [CSCv43870](#) permet l'utilisation de n'importe quel format dans l'interface de ligne de commande ou l'interface utilisateur Web dans les versions ultérieures.

---

CLI :

```
# config t
# aaa new-model
# aaa authorization credential-download <AP-auth> local

# ap auth-list authorize-mac
# ap auth-list method-list <AP-auth>

# username <aaaabbbbcccc> mac
```

Liste d'autorisation MAC AP - Serveur RADIUS externe

Configuration WLC 9800

Les adresses MAC des points d'accès autorisés sont stockées sur un serveur RADIUS externe, dans cet exemple ISE.

Sur ISE, vous pouvez enregistrer l'adresse MAC des points d'accès en tant que noms d'utilisateur/mot de passe ou en tant que terminaux. Au cours de ces étapes, vous êtes invité à choisir l'une ou l'autre des méthodes.

IUG:

Étape 1. Déclarez le serveur RADIUS.

Accédez à Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add et entrez les informations du serveur RADIUS.

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*	<input type="text" value="ISE-kcg"/>	Clear PAC Key	<input type="checkbox"/>
IPv4/IPv6 Server Address*	<input type="text" value="172.16.0.11"/>	Set New PAC Key	<input type="checkbox"/>
Shared Secret*	<input type="password" value="....."/>		
Confirm Shared Secret*	<input type="password" value="....."/>		
Auth Port	<input type="text" value="1812"/>		
Acct Port	<input type="text" value="1813"/>		
Server Timeout (seconds)	<input type="text" value="1-1000"/>		
Retry Count	<input type="text" value="0-100"/>		
Support for CoA	<input checked="" type="checkbox"/> ENABLED		

↶ Cancel

📄 Save & Apply to Device

Étape 2. Ajoutez le serveur RADIUS à un groupe RADIUS.

Accédez à Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add.

Pour qu'ISE authentifie l'adresse MAC AP en tant que noms d'utilisateur, laissez MAC-Filtering comme none.

## Create AAA Radius Server Group



Name\*

ISE-grp-name

Group Type

RADIUS

MAC-Delimiter

none

MAC-Filtering

none

Dead-Time (mins)

1-1440

Available Servers



Assigned Servers

ISE-iccg

Cancel

Save & Apply to Device

Pour qu'ISE authentifie l'adresse MAC du point d'accès en tant que terminaux, remplacez MAC-Filtering par MAC.

### Create AAA Radius Server Group

Name\*

Group Type

MAC-Delimiter

**MAC-Filtering**

Dead-Time (mins)

Available Servers Assigned Servers

ISE-KCG

Étape 3. Créez une liste de méthodes de téléchargement des informations d'identification d'autorisation.

Accédez à Configuration > Security > AAA > AAA Method List > Authorization > + Add.

Search Menu Items

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

### Authentication Authorization and Accounting

[+ AAA Wizard](#)

**AAA Method List** Servers / Groups AAA Advanced

General

Authentication

**Authorization**

Accounting

	Name	Type
<input type="checkbox"/>	default	network
<input type="checkbox"/>	AuthZ-Netw-ISE	network

**Quick Setup: AAA Authorization** ✕

Method List Name\*

Type\*

Group Type

Fallback to local

Available Server Groups

radius  
 ldap  
 tacacs+  
 ISE-KCG-grp

Assigned Server Groups

ISE-grp-name

Étape 4. Activez l'autorisation MAC AP.

Accédez à Configuration > Security > AAA > AAA Advanced > AP Policy. Activez Authorize APs against MAC et sélectionnez la liste de méthodes d'autorisation créée à l'étape 3.

Authentication Authorization and Accounting

+ AAA Wizard

AAA Method List  
 Servers / Groups  
AAA Advanced

RADIUS Fallback

Attribute List Name

AP Authentication

AP Policy

Password Policy

Authorize APs against MAC ENABLED ■

Authorize APs against Serial Number DISABLED

Authorization Method List

CLI :

```

# config t
# aaa new-model

# radius server <radius-server-name>
# address ipv4 <radius-server-ip> auth-port 1812 acct-port 1813
# timeout 300
# retransmit 3
# key <shared-key>
# exit
  
```

```
# aaa group server radius <radius-grp-name>
# server name <radius-server-name>
# exit

# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>

# aaa authorization credential-download <AP-auth> group <radius-grp-name>
# ap auth-list authorize-mac
# ap auth-list method-list <AP-ISE-auth>
```

## Configuration ISE

Étape 1. Pour ajouter un WLC 9800 à ISE :

### [Déclarer le WLC 9800 sur ISE](#)

Choisissez de configurer l'adresse MAC de l'AP en fonction de l'authentification avec les étapes requises :

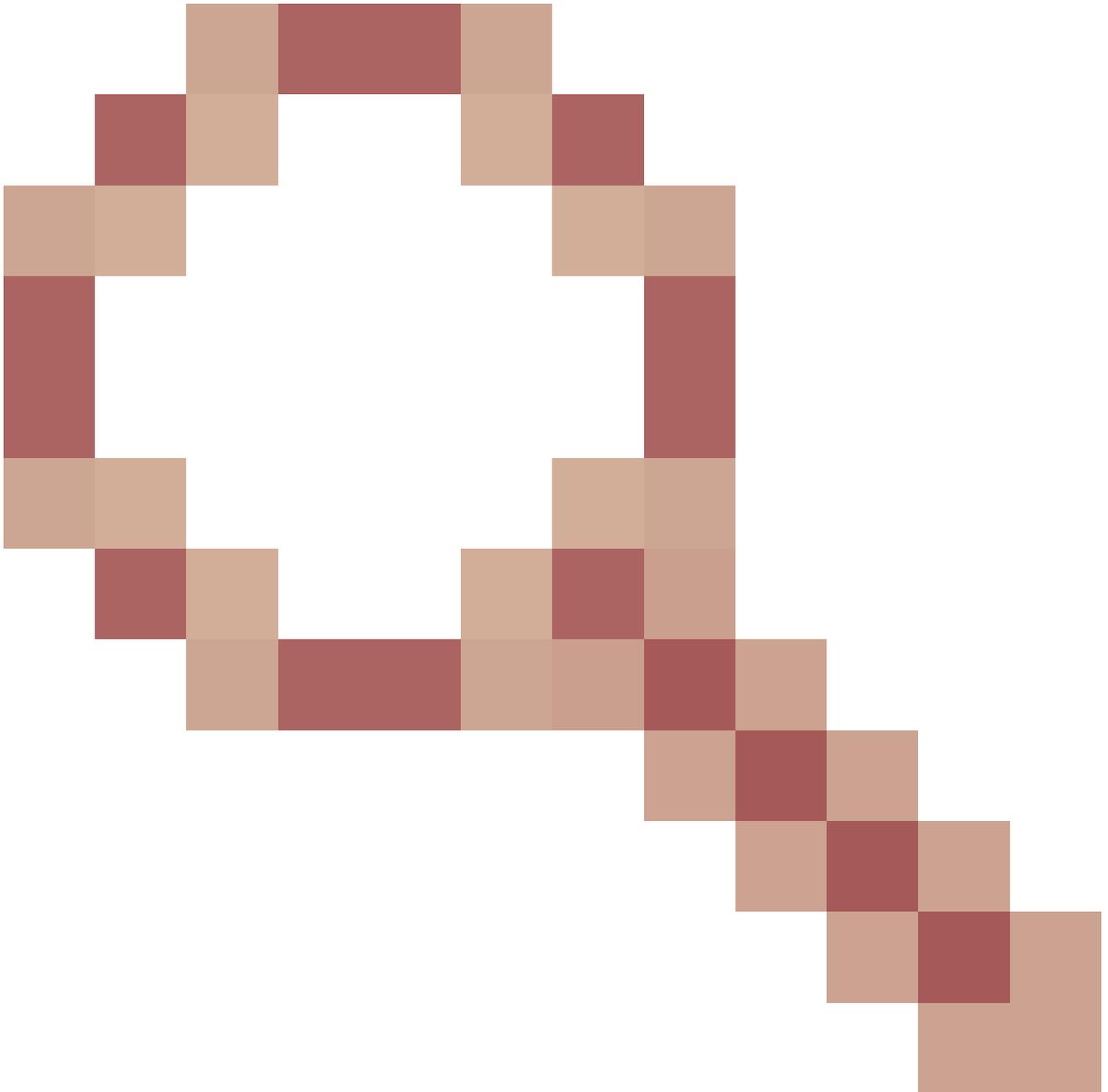
### [Configurez USE pour authentifier l'adresse MAC en tant que terminaux](#)

### [Configurer ISE pour authentifier l'adresse MAC comme nom d'utilisateur/mot de passe](#)

Configurer ISE pour authentifier les adresses MAC en tant que terminaux

Étape 2. (Facultatif) Créez un groupe d'identité pour les points d'accès.

Comme le 9800 n'envoie pas l'attribut NAS-port-Type avec l'autorisation AP (bogue Cisco [IDCSCvy74904](#)).



ISE ne reconnaît pas une autorisation AP comme un workflow MAB. Par conséquent, il n'est pas possible d'authentifier un AP si l'adresse MAC de l'AP est placée dans la liste des points d'extrémité, sauf si vous modifiez les flux de travail MAB pour ne pas exiger l'attribut NAS-PORT-type sur ISE.

Accédez à Administrator > Network device profile et créez un nouveau profil de périphérique. Activez RADIUS et ajoutez service-type=call-check pour Wired MAB. Vous pouvez copier le reste du profil Cisco d'origine. L'idée est d'avoir aucune condition de type de port nas pour le MAB filaire.

\* Name  

Description

Icon



[Change icon...](#)

[Set To Default](#)



Vendor  

### Supported Protocols

- RADIUS
- TACACS+
- TrustSec

RADIUS Dictionaries

### Templates

[Expand All](#) / [Collapse All](#)

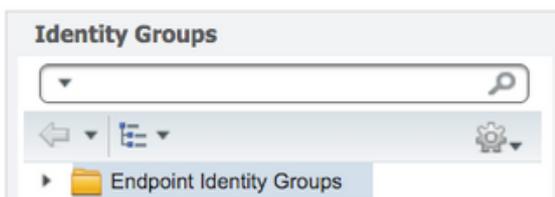
#### Authentication/Authorization

#### Flow Type Conditions

Wired MAB detected if the following condition(s) are met :

Retournez à l'entrée de périphérique réseau pour le 9800 et définissez son profil sur le profil de périphérique nouvellement créé.

Accédez à Administration > Identity Management > Groups > Endpoint Identity Groups > + Add.



### Endpoint Identity Groups

Edit    **Add**   Delete

Name	Description
------	-------------

Choisissez un nom et cliquez sur Submit.

Endpoint Identity Group List > **New Endpoint Group**

## Endpoint Identity Group

\* Name

Description

Parent Group

Étape 3. Ajoutez l'adresse MAC Ethernet AP à son groupe d'identité de point d'extrémité.

Accédez à Work Centers > Network Access > Identities > Endpoints > +.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The navigation path is: Work Centers > Network Access > Identities > Endpoints. The 'Endpoints' section is active, showing a bar chart titled 'INACTIVE ENDPOINTS' with a value of 1. The x-axis is labeled 'Last Activity Date' and shows a date of 8/27. The y-axis ranges from 0 to 1. To the right, there is a section for 'AUTHENTICATED' endpoints, showing 'disconnected: [1009]'. At the bottom, there is a table with columns for 'MAC Address', 'Status', 'IPv4 Address', and 'Username'. A red box highlights the '+' icon in the table's toolbar, indicating the option to add a new endpoint.

Saisissez les informations requises.

## Add Endpoint



### General Attributes

Mac Address \*

Description

Static Assignment

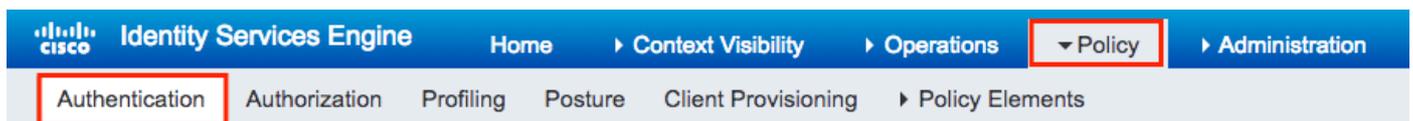
Policy Assignment

Static Group Assignment

Identity Group Assignment

Étape 4. Vérifiez le magasin d'identités utilisé sur votre règle d'authentification par défaut qui contient les points de terminaison internes.

A. Accédez à Policy > Authentication et prenez note de la banque d'identités.



### Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identifier for Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Policy Type  Simple  Rule-Based

<input checked="" type="checkbox"/>	MAB	: If Wired_MAB OR Wireless_MABAllow Protocols : Default Network Access and <input checked="" type="checkbox"/> Default :use Internal Endpoints
<input checked="" type="checkbox"/>	Dot1X	: If Wired_802.1X OR Wireless_802.1XAllow Protocols : Default Network Access and <input checked="" type="checkbox"/> Default :use All_User_ID_Stores
<input checked="" type="checkbox"/>	Default Rule (If no match)	: Allow Protocols : Default Network Access and use : All_User_ID_Stores

B. Accédez à Administration > Identity Management > Identity Source Sequences > Identity Name.

### Identity Source Sequences

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

 Edit  Add  Duplicate  Delete

<input type="checkbox"/>	Name	Description	Identity
<input type="checkbox"/>	All_User_ID_Stores	A built-in Identity Sequence to include all User Identity Stores	Preload
<input type="checkbox"/>	Certificate_Request_Sequence	A built-in Identity Sequence for Certificate Request APIs	Internal
<input type="checkbox"/>	Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal
<input type="checkbox"/>	MyDevices_Portal_Sequence	A built-in Identity Sequence for the My Devices Portal	Internal
<input type="checkbox"/>	Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Internal

C. Assurez-vous que les terminaux internes lui appartiennent. Sinon, ajoutez-les.

## Identity Source Sequence

### ▼ Identity Source Sequence

\* Name

Description

### ▼ Certificate Based Authentication

Select Certificate Authentication Profile

### ▼ Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available		Selected
<input type="text" value="Internal Endpoints"/>	<input type="button" value="&gt;"/>	<input type="text" value="Internal Users"/> <input type="text" value="All_AD_Join_Points"/> <input type="text" value="Guest Users"/>
	<input type="button" value="&lt;"/>	<input type="button" value="↑"/>
	<input type="button" value="⇒"/>	<input type="button" value="↑"/>
	<input type="button" value="⇐"/>	<input type="button" value="↓"/>
		<input type="button" value="↓"/>

### ▼ Advanced Search List Settings

If a selected identity store cannot be accessed for authentication

- Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"
- Treat as if the user was not found and proceed to the next store in the sequence

Configurer ISE pour authentifier l'adresse MAC comme nom d'utilisateur/mot de passe

Cette méthode est déconseillée car elle nécessite des stratégies de mot de passe inférieures pour autoriser le même mot de passe que le nom d'utilisateur.

Il peut toutefois s'agir d'une solution de contournement si vous ne pouvez pas modifier votre profil de périphérique réseau.

Étape 2. (Facultatif) Créez un groupe d'identité pour les points d'accès.

Accédez à Administration > Identity Management > Groups > User Identity Groups > + Add.

**Identity Groups**

Endpoint Identity Groups  
User Identity Groups

**User Identity Groups**

Edit Add Delete Import Export

Name	Description
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_

Choisissez un nom et cliquez sur Submit.

User Identity Groups > **New User Identity Group**

## Identity Group

\* Name

Description

Étape 3. Vérifiez que votre stratégie de mot de passe actuelle vous permet d'ajouter une adresse MAC comme nom d'utilisateur et mot de passe.

Accédez à Administration > Identity Management > Settings > User Authentication Settings > Password Policy et assurez-vous que ces options au moins sont désactivées :

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

> System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC

> Identities > Groups > External Identity Sources > Identity Source Sequences > Settings

User Custom Attributes

User Authentication Settings

Endpoint Purge

Endpoint Custom Attributes

Password Policy Account Disable Policy

### Password Policy

- Minimum Length: 4 characters (Valid Range 4 to 127)

**Password must not contain:**

- User name or its characters in reverse order
- "cisco" or its characters in reverse order
- This word or its characters in reverse order:
- Repeated characters four or more times consecutively
- Dictionary words, their characters in reverse order or their letters replaced with other characters ?

Default Dictionary ?

Custom Dictionary ?  No file chosen

The newly added custom dictionary file will replace the existing custom dictionary file.

**Password must contain at least one character of each of the selected types:**

- Lowercase alphabetic characters
- Uppercase alphabetic characters
- Numeric characters
- Non-alphanumeric characters

**Password History**

- Password must be different from the previous 3 versions (Valid Range 1 to 10)
- Password change delta 3 characters (Valid Range 3 to 10)
- Cannot reuse password within 15 days (Valid Range 0 to 365)

**Password Lifetime**

Users can be required to periodically change password

- Disable user account after 60 days if password was not changed (valid range 1 to 3650)
- Display reminder 30 days prior to password expiration (valid range 1 to 3650)
- Lock/Suspend Account with Incorrect Login Attempts

- # 3 (Valid Range 3 to 20)
  - Suspend account for 15 minutes (Valid Range 15 to 1440)  Disable account

 Remarque : vous pouvez également désactiver l'option Disable user account after XX days si le mot de passe n'a pas été modifié. Comme il s'agit d'une adresse MAC, le mot de passe ne change jamais.

Étape 4. Ajoutez l'adresse MAC Ethernet AP.

Accédez à Administration > Identity Management > Identities > Users > + Add.

**CISCO Identity Services Engine** Home > Context Visibility > Operations > Policy > Administration

System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Services

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Edit Add Change Status Import Export Delete

Status	Name	Description	First N
--------	------	-------------	---------

Saisissez les informations requises.

▼ Network Access User

\* Name

Status  Enabled ▼

Email

▼ Passwords

Password Type:

Password

Re-Enter Password

\* Login Password

ⓘ

Enable Password

ⓘ

▼ User Information

First Name

Last Name

▼ Account Options

Description

Change password on next login

▼ Account Disable Policy

Disable account if date exceeds  (yyyy-mm-dd)

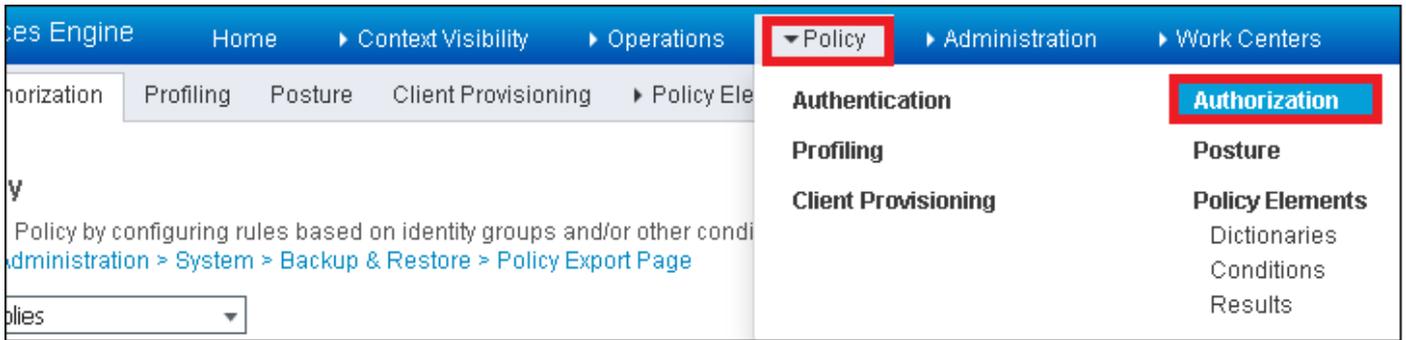
▼ User Groups

- +

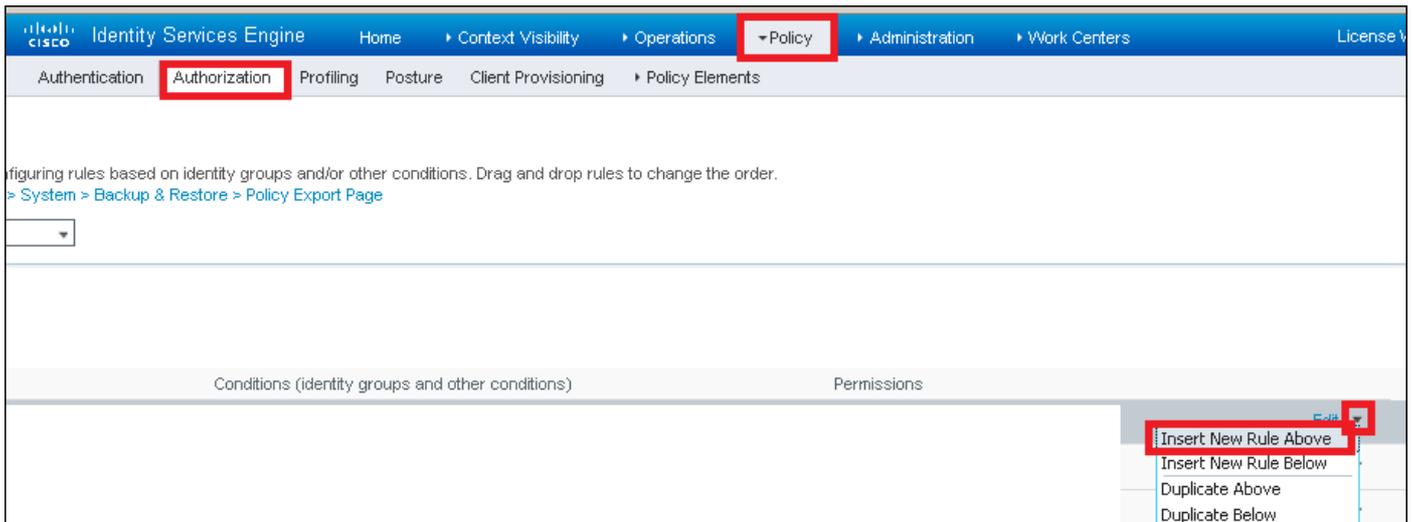
 Remarque : les champs Nom et Mot de passe de connexion doivent correspondre à l'adresse MAC Ethernet du point d'accès, tous en minuscules et sans séparateur.

Stratégie d'autorisation pour authentifier les AP

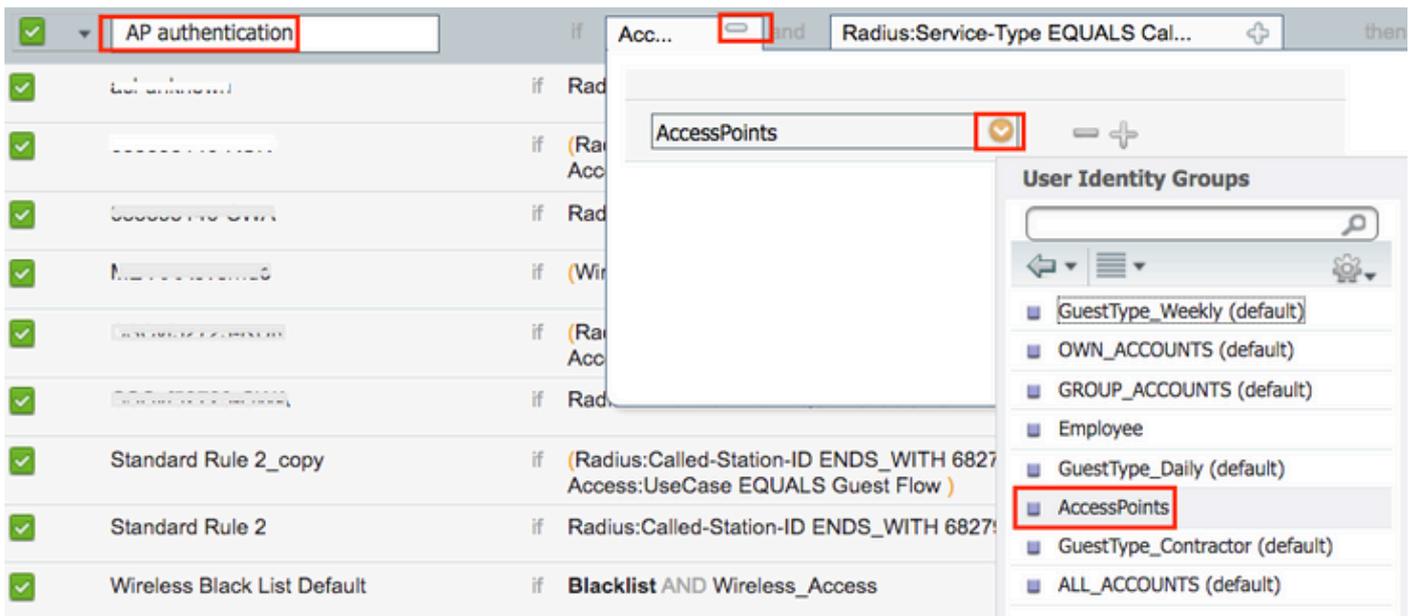
Accédez à Policy > Authorization comme indiqué dans l'image.



Insérez une nouvelle règle comme illustré dans l'image.



Commencez par sélectionner un nom pour la règle et le groupe Identité dans lequel le point d'accès est stocké (AccessPoints). Sélectionnez User Identity Groups si vous avez décidé d'authentifier l'adresse MAC en tant que nom d'utilisateur et mot de passe ou Endpoint Identity Groups si vous choisissez d'authentifier l'adresse MAC AP en tant que points d'extrémité.



Ensuite, sélectionnez d'autres conditions qui font que le processus d'autorisation est soumis à cette règle. Dans cet exemple, le processus d'autorisation atteint cette règle s'il utilise la

vérification d'appel de type service et que la demande d'authentification provient de l'adresse IP 10.88.173.52.

The screenshot shows a configuration window with a tab titled 'Radius:Service-Type EQUALS Cal...' and a sub-tab 'then AuthZ Pr...'. Below the tabs is a button 'Add All Conditions Below to Library'. The main area contains a table of conditions:

Condition Name	Description	Operator	Value	Logic
	Radius:Service-Type	Equals	Call Check	AND
	Radius:NAS-IP-Ad...	Equals	10.88.173.52	

Enfin, sélectionnez le profil d'autorisation attribué aux clients qui ont atteint cette règle, cliquez sur Terminer et enregistrez-le comme indiqué dans l'image.

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
	AP authentication	if AccessPoints AND (Radius:Service-Type EQUALS Call Check AND Radius:NAS-IP-Address EQUALS 10.88.173.52)	then PermitAccess

Remarque : les AP qui ont déjà rejoint le contrôleur ne perdent pas leur association. Cependant, si, après l'activation de la liste d'autorisation, ils perdent la communication avec le contrôleur et tentent de se joindre à nouveau, ils passent par le processus d'authentification. Si leurs adresses MAC ne sont pas répertoriées localement ou dans le serveur RADIUS, ils ne peuvent pas rejoindre le contrôleur.

## Vérifier

Vérifiez si le WLC 9800 a activé la liste d'authentification AP.

```
<#root>
```

```
# show ap auth-list
```

```
Authorize APs against MAC : Disabled  
Authorize APs against Serial Num : Enabled  
Authorization Method List : <auth-list-name>
```

Vérifiez la configuration du rayon :

```
<#root>
```

```
#
```

```
show run aaa
```

# Dépannage

Le WLC 9800 offre des fonctionnalités de suivi ALWAYS-ON. Cela garantit que toutes les erreurs liées à la jonction AP, les messages de niveau d'avertissement et d'avertissement sont constamment consignés et que vous pouvez afficher les journaux d'un incident ou d'une condition d'échec après qu'il se soit produit.



Remarque : le volume de journaux générés varie rétroactivement de quelques heures à plusieurs jours.

---

Pour afficher les traces que le WLC 9800 a collectées par défaut, vous pouvez vous connecter via SSH/Telnet au WLC 9800 à l'aide de ces étapes. (Veillez à consigner la session dans un fichier texte).

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

```
# show clock
```

Étape 2. Collectez les syslog à partir de la mémoire tampon du contrôleur ou du syslog externe, comme dicté par la configuration système. Cela fournit un aperçu rapide de l'intégrité du système et des erreurs, le cas échéant.

```
# show logging
```

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

```
# show debugging
```

```
IOSXE Conditional Debug Configs:
```

```
Conditional Debug Global State: Stop
```

```
IOSXE Packet Trace Configs:
```

```
Packet Infra debugs:
```

```
Ip Address
```

```
Port
```

```
-----|-----
```

---

 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 augmenterait le volume de journaux. Par conséquent, il est recommandé d'effacer toutes les conditions lorsque vous ne procédez pas activement au débogage.

---

Étape 4. Supposons que l'adresse MAC testée n'était pas répertoriée comme condition. À l'étape 3, collectez les suivis de niveau de notification toujours actif pour l'adresse MAC radio spécifique.

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

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

```
# 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 de niveau de débogage pour tous les processus qui interagissent avec la condition spécifiée (adresse MAC du client dans ce cas).

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

```
# clear platform condition all
```

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

Cette commande commence 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.

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

---

 Remarque : Afin de surveiller plusieurs clients à la fois, exécutez la <aaaa.bbbb.cccc>commande de débogage sans fil mac par adresse MAC.

---

 Remarque : vous ne voyez pas le résultat de l'activité du client dans 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.

```
# 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_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Étape 9. Recueillir le fichier de l'activité de l'adresse MAC. Il est possible de copier le fichier de suivi RA .log sur un serveur externe ou d'afficher le résultat directement à l'écran.

Vérifiez le nom du fichier de suivi RA:

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

Copiez le fichier sur un serveur externe :

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.
```

Affichez-en le contenu :

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

Étape 10. Si vous ne trouvez toujours pas la cause première, collectez les journaux internes, qui peuvent vous offrir une vue plus détaillée des journaux de niveau de débogage. Vous n'avez pas besoin de déboguer à nouveau le client, car vous n'avez qu'à examiner plus en détail les journaux de débogage qui ont déjà été collectés et stockés en interne.

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

---

 Remarque : cette sortie de commande retourne des traces pour tous les niveaux de journalisation pour tous les processus et est assez volumineuse. Veuillez faire appel à Cisco TAC pour faciliter l'analyse de ces suivis.

---

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

Copiez le fichier sur un serveur externe :

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

Affichez-en le contenu :

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

Étape 11. Supprimez les conditions de débogage:

```
# clear platform condition all
```

---

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

---

## Références

[Joindre des points d'accès maillés au WLC 9800](#)

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.