

# Configurer l'autorisation de point d'accès dans un réseau sans fil unifié

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Autorisation AP légère](#)

[Configuration](#)

[Configuration à l'aide de la liste d'autorisation interne sur le WLC](#)

[Vérification](#)

[Autorisation AP sur un serveur AAA](#)

[Configurer Cisco ISE pour autoriser les points d'accès](#)

[Configurer un nouveau profil de périphérique où MAB ne nécessite pas d'attribut de type de port NAS](#)

[Configurer le WLC en tant que client AAA sur Cisco ISE](#)

[Ajoutez l'adresse MAC AP à la base de données des terminaux sur Cisco ISE](#)

[Ajouter l'adresse MAC AP à la base de données utilisateur sur Cisco ISE \(facultatif\)](#)

[Définir un ensemble de stratégies](#)

[Vérification](#)

[Dépannage](#)

## Introduction

Ce document décrit comment configurer le WLC pour autoriser le point d'accès (AP) basé sur l'adresse MAC des AP.

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base sur la configuration d'un moteur Cisco Identity Services Engine (ISE)
- Connaissance de la configuration des points d'accès Cisco et des WLC Cisco
- Connaissance des solutions Cisco Unified Wireless Security

## Components Used

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

- WLC exécutant le logiciel AireOS 8.8.11.0 Points d'accès Wave1 : 1700/2700/3700 et 3500 (les versions 1600/2600/3600 sont toujours prises en charge, mais la prise en charge d'AireOS prend fin avec la version 8.5.x) Points d'accès Wave2 : 1800/2800/3800/4800, 1540 et 1560 version ISE 2.3.0.298

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.

## Autorisation AP légère

Pendant le processus d'enregistrement des AP, les AP et les WLC s'authentifient mutuellement à l'aide de certificats X.509. Les certificats X.509 sont gravés dans la mémoire flash protégée sur l'AP et le WLC en usine par Cisco.

Sur le point d'accès, les certificats installés en usine sont appelés certificats installés en fabrication (MIC). Tous les points d'accès Cisco fabriqués après le 18 juillet 2005 sont dotés de MIC.

Outre cette authentification mutuelle qui se produit pendant le processus d'enregistrement, les WLC peuvent également restreindre les AP qui s'enregistrent auprès d'eux en fonction de l'adresse MAC de l'AP.

L'absence d'un mot de passe fort avec l'utilisation de l'adresse MAC AP n'est pas un problème parce que le contrôleur utilise MIC pour authentifier l'AP avant d'autoriser l'AP via le serveur RADIUS. L'utilisation de MIC fournit une authentification forte.

L'autorisation AP peut être effectuée de deux manières :

- Utilisation de la liste d'autorisation interne sur le WLC
- Utilisation de la base de données d'adresses MAC sur un serveur AAA

Les comportements des points d'accès diffèrent en fonction du certificat utilisé :

- AP avec SSC : le WLC utilise uniquement la liste d'autorisation interne et ne transmet pas de requête à un serveur RADIUS pour ces AP
- AP avec MIC : le WLC peut utiliser la liste d'autorisation interne configurée sur le WLC ou utiliser un serveur RADIUS pour autoriser les AP

Ce document traite de l'autorisation AP avec l'utilisation de la liste d'autorisation interne et du serveur AAA.

## Configuration

### Configuration à l'aide de la liste d'autorisation interne sur le WLC

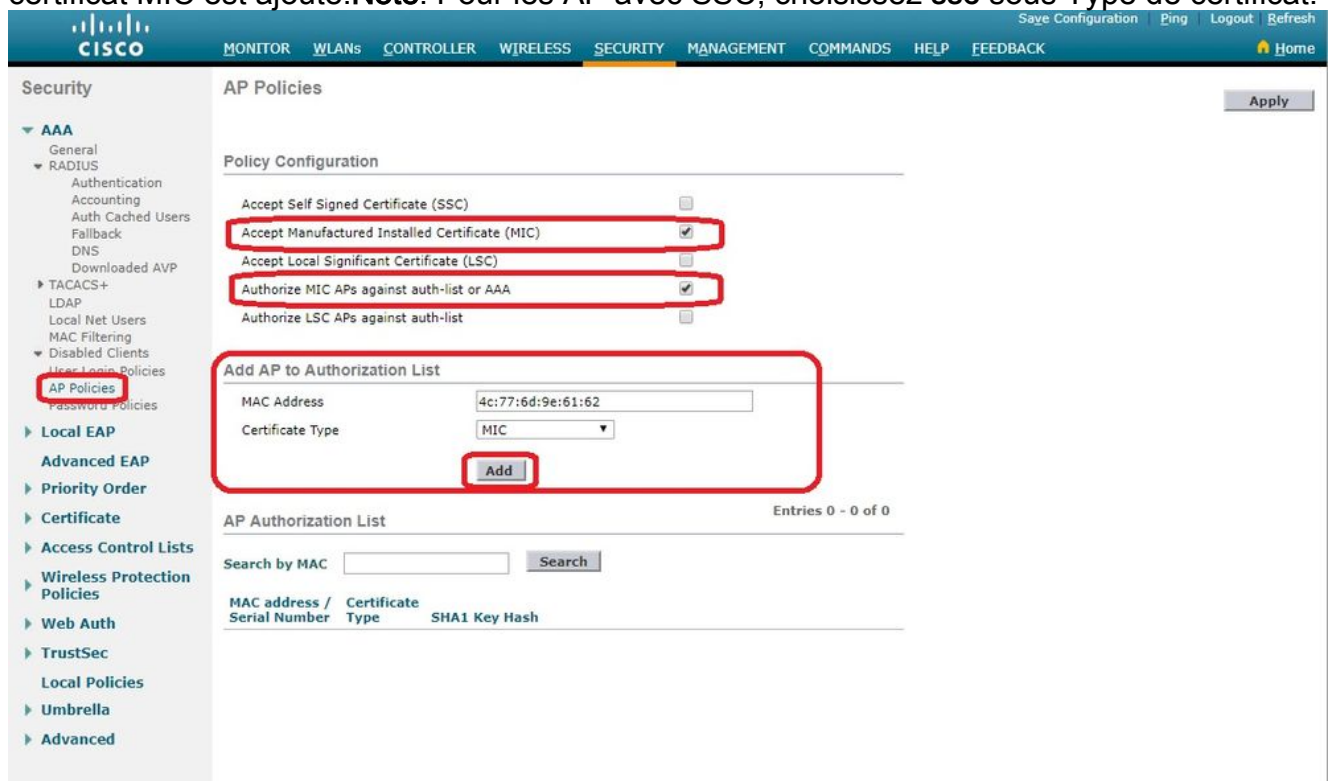
Sur le WLC, utilisez la liste d'autorisation AP pour restreindre les AP en fonction de leur adresse MAC. La liste des autorisations AP est disponible sous **Security > AP Policies** dans la GUI du WLC.

Cet exemple montre comment ajouter l'AP avec l'adresse MAC 4c:77:6d:9e:61:62.

1. Dans l'interface graphique du contrôleur WLC, cliquez sur **Security > AP Policies** et la page AP Policies s'affiche.
2. Cliquez sur le bouton **Add** sur le côté droit de l'écran.



3. Sous **Add AP to Authorization List**, entrez la commande **AP MAC** (et non l'adresse MAC radio AP). Choisissez ensuite le type de certificat et cliquez sur **Add**. Dans cet exemple, un AP avec un certificat MIC est ajouté. **Note:** Pour les AP avec SSC, choisissez **ssc** sous Type de certificat.



Le point d'accès est ajouté à la liste d'autorisation des points d'accès et est répertorié **SOUS AP Authorization List**.

4. Sous **Policy Configuration**, cochez la case correspondant à **Authorize MIC APs against auth-list or AAA**. Lorsque ce paramètre est sélectionné, le WLC vérifie d'abord la liste d'autorisation locale. Si l'adresse MAC AP n'est pas présente, il vérifie le serveur RADIUS.

The screenshot shows the Cisco Security configuration interface. The left sidebar has 'AP Policies' selected. The main content area shows the 'AP Policies' configuration. Under 'Policy Configuration', the option 'Authorize MIC APs against auth-list or AAA' is checked and highlighted with a red box. Below this, the 'AP Authorization List' is displayed as a table with 5 entries, all of type 'MIC'. The 'Apply' button is also highlighted with a red box.

MAC address / Serial Number	Certificate Type	SHA1 Key Hash
4c:77:6d:9e:61:62	MIC	
70:d3:79:26:39:68	MIC	
88:f0:31:7e:e0:38	MIC	
f4:db:e6:43:c4:b2	MIC	
fc:5b:39:e7:2b:30	MIC	

## Vérification

Afin de vérifier cette configuration, vous devez connecter l'AP avec l'adresse MAC **4c:77:6d:9e:61:62** au réseau et à la surveillance. Utilisez `debug capwap events/errors enable` et `debug aaa all enable` pour effectuer cette opération.

Ce résultat montre les débogages quand l'adresse MAC AP n'est pas présente dans la liste d'autorisation AP :

**Note:** Certaines lignes du résultat ont été déplacées vers la deuxième ligne en raison de contraintes d'espace.

```
(Cisco Controller) >debug capwap events enable
(Cisco Controller) >debug capwap errors enable
(Cisco Controller) >debug aaa all enable
```

```
*spamApTask4: Feb 27 10:15:25.592: 70:69:5a:51:4e:c0 Join Request from 192.168.79.151:5256
```

```
*spamApTask4: Feb 27 10:15:25.592: 70:69:5a:51:4e:c0 Unable to get Ap mode in Join request
```

```
*spamApTask4: Feb 27 10:15:25.592: 70:69:5a:51:4e:c0 Allocate database entry for AP
192.168.79.151:5256, already allocated index 277
```

```
*spamApTask4: Feb 27 10:15:25.592: 70:69:5a:51:4e:c0 AP Allocate request at index 277 (reserved)
```

```
*spamApTask4: Feb 27 10:15:25.593: 24:7e:12:19:41:ef Deleting AP entry 192.168.79.151:5256 from
temporary database.
```

```
*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 AP group received default-group is found in
ap group configured in wlc.
```

```
*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Dropping request or response packet to AP
:192.168.79.151 (5256) by Controller: 10.48.71.20 (5246), message Capwap_wtp_event_response,
state Capwap_no_state
```

\*spamApTask4: Feb 27 10:15:25.593: **70:69:5a:51:4e:c0 In AAA state 'Idle' for AP 70:69:5a:51:4e:c0**

\*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Join Request failed!

\*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 State machine handler: Failed to process msg type = 3 state = 0 from 192.168.79.151:5256

\*aaaQueueReader: Feb 27 10:15:25.593: **Unable to find requested user entry for 4c776d9e6162**

\*aaaQueueReader: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Normal Response code for AAA Authentication : -9

\*aaaQueueReader: Feb 27 10:15:25.593: ReProcessAuthentication previous proto 8, next proto 40000001

\*aaaQueueReader: Feb 27 10:15:25.593: AuthenticationRequest: 0x7f01b4083638

\*aaaQueueReader: Feb 27 10:15:25.593: Callback.....0xd6cef02166

\*aaaQueueReader: Feb 27 10:15:25.593: protocolType.....0x40000001

\*aaaQueueReader: Feb 27 10:15:25.593: proxyState.....70:69:5A:51:4E:C0-00:00

\*aaaQueueReader: Feb 27 10:15:25.593: Packet contains 9 AVPs:

\*aaaQueueReader: Feb 27 10:15:25.593: AVP[01] User-Name.....4c776d9e6162 (12 bytes)

\*aaaQueueReader: Feb 27 10:15:25.593: AVP[02] Called-Station-Id.....70-69-5a-51-4e-c0 (17 bytes)

\*aaaQueueReader: Feb 27 10:15:25.593: AVP[03] Calling-Station-Id.....4c-77-6d-9e-61-62 (17 bytes)

\*aaaQueueReader: Feb 27 10:15:25.593: AVP[04] Nas-Port.....0x00000001 (1) (4 bytes)

\*aaaQueueReader: Feb 27 10:15:25.593: AVP[05] Nas-Ip-Address.....0x0a304714 (170936084) (4 bytes)

\*aaaQueueReader: Feb 27 10:15:25.593: AVP[06] NAS-Identifier.....0x6e6f (28271) (2 bytes)

\*aaaQueueReader: Feb 27 10:15:25.593: AVP[07] User-Password.....[...]

\*aaaQueueReader: Feb 27 10:15:25.593: AVP[08] Service-Type.....0x0000000a (10) (4 bytes)

\*aaaQueueReader: Feb 27 10:15:25.593: AVP[09] Message-Authenticator.....DATA (16 bytes)

\*aaaQueueReader: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Error Response code for AAA Authentication : -7

\*aaaQueueReader: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Returning AAA Error 'No Server' (-7) for mobile 70:69:5a:51:4e:c0 serverIdx 0

\*aaaQueueReader: Feb 27 10:15:25.593: AuthorizationResponse: 0x7f017adf5770

\*aaaQueueReader: Feb 27 10:15:25.593: RadiusIndexSet(0), Index(0)

\*aaaQueueReader: Feb 27 10:15:25.593: resultCode.....-7

\*aaaQueueReader: Feb 27 10:15:25.593: protocolUsed.....0xffffffff

\*aaaQueueReader: Feb 27 10:15:25.593: proxyState.....70:69:5A:51:4E:C0-00:00

```

*aaaQueueReader: Feb 27 10:15:25.593: Packet contains 0 AVPs:
*aaaQueueReader: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 User entry not found in the Local FileDB for the client.
*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Join Version: = 134770432
*spamApTask0: Feb 27 10:15:25.593: 00:00:00:00:00:00 apType = 54 apModel: AIR-AP4800-E-K
*spamApTask0: Feb 27 10:15:25.593: 00:00:00:00:00:00 apType: Ox36 bundleApImageVer: 8.8.111.0
*spamApTask0: Feb 27 10:15:25.593: 00:00:00:00:00:00 version:8 release:8 maint:111 build:0
*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Join resp: CAPWAP Maximum Msg element len = 79
*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Join Failure Response sent to 0.0.0.0:5256
*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Radius Authentication failed. Closing dtls Connection.
*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Disconnecting DTLS Capwap-Ctrl session 0xd6f0724fd8 for AP (192.168.79.151/5256). Notify(true)
*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 CAPWAP State: Dtls tear down
*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 acDtlsPlumbControlPlaneKeys: lrad:192.168.79.151(5256) mwar:10.48.71.20(5246)
*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 DTLS keys for Control Plane deleted successfully for AP 192.168.79.151
*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 DTLS connection closed event receivedserver (10.48.71.20/5246) client (192.168.79.151/5256)
*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Entry exists for AP (192.168.79.151/5256)
*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 AP Delete request
*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 AP Delete request
*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Unable to find AP 70:69:5a:51:4e:c0
*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 No AP entry exist in temporary database for 192.168.79.151:5256

```

Cette sortie montre les débogages quand l'adresse MAC LAP est ajoutée à la liste d'autorisation AP :

**Note:** Certaines lignes du résultat ont été déplacées vers la deuxième ligne en raison de contraintes d'espace.

```

(Cisco Controller) >debug capwap events enable
(Cisco Controller) >debug capwap errors enable
(Cisco Controller) >debug aaa all enable

```

```

*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 Join Request from 192.168.79.151:5256
*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 using already alloced index 274
*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 Unable to get Ap mode in Join request
*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 Allocate database entry for AP 192.168.79.151:5256, already allocated index 274
*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 AP Allocate request at index 274 (reserved)
*spamApTask4: Feb 27 09:50:25.393: 24:7e:12:19:41:ef Deleting AP entry 192.168.79.151:5256 from temporary database.
*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 AP group received default-group is found in ap group configured in wlc.

```

```
*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 Dropping request or response packet to AP
:192.168.79.151 (5256) by Controller: 10.48.71.20 (5246), message Capwap_wtp_event_response,
state Capwap_no_state

*spamApTask4: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Message type Capwap_wtp_event_response is
not allowed to send in state Capwap_no_state for AP 192.168.79.151

*spamApTask4: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 In AAA state 'Idle' for AP
70:69:5a:51:4e:c0
*spamApTask4: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Join Request failed!

*aaaQueueReader: Feb 27 09:50:25.394: User 4c776d9e6162 authenticated
*aaaQueueReader: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Normal Response code for AAA
Authentication : 0
*aaaQueueReader: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Returning AAA Success for mobile
70:69:5a:51:4e:c0
*aaaQueueReader: Feb 27 09:50:25.394: AuthorizationResponse: 0x7f0288a66408

*aaaQueueReader: Feb 27 09:50:25.394: structureSize.....194
*aaaQueueReader: Feb 27 09:50:25.394: resultCode.....0
*aaaQueueReader: Feb 27 09:50:25.394:
proxyState.....70:69:5A:51:4E:C0-00:00
*aaaQueueReader: Feb 27 09:50:25.394: Packet contains 2 AVPs:
*aaaQueueReader: Feb 27 09:50:25.394: AVP[01] Service-
Type.....0x00000065 (101) (4 bytes)
*aaaQueueReader: Feb 27 09:50:25.394: AVP[02] Airespace / WLAN-
Identifier.....0x00000000 (0) (4 bytes)
*aaaQueueReader: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 User authentication Success with File DB
on WLAN ID :0
*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Join Version: = 134770432
*spamApTask0: Feb 27 09:50:25.394: 00:00:00:00:00:00 apType = 54 apModel: AIR-AP4800-E-K
*spamApTask0: Feb 27 09:50:25.394: 00:00:00:00:00:00 apType: 0x36 bundleApImageVer: 8.8.111.0
*spamApTask0: Feb 27 09:50:25.394: 00:00:00:00:00:00 version:8 release:8 maint:111 build:0
*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Join resp: CAPWAP Maximum Msg element len =
79
*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Join Response sent to 0.0.0.0:5256
*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 CAPWAP State: Join
*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 capwap_ac_platform.c:2095 - Operation State
0 ==> 4
*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Capwap State Change Event (Reg) from
capwap_ac_platform.c 2136
*apfReceiveTask: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Register LWAPP event for AP
70:69:5a:51:4e:c0 slot 0
```

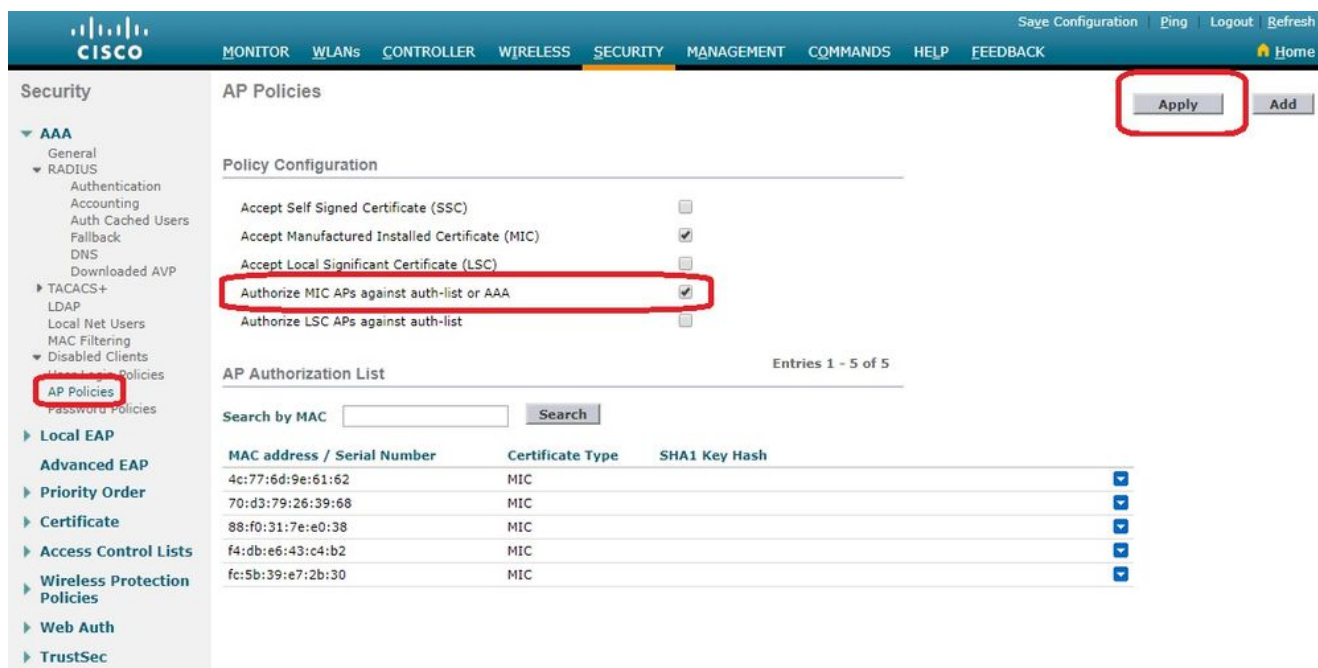
## Autorisation AP sur un serveur AAA

Vous pouvez également configurer des WLC pour utiliser des serveurs RADIUS pour autoriser

des AP utilisant des MIC. Le WLC utilise une adresse MAC AP comme nom d'utilisateur et mot de passe lors de l'envoi des informations à un serveur RADIUS. Par exemple, si l'adresse MAC du point d'accès est 4c:77:6d:9e:61:62, le nom d'utilisateur et le mot de passe utilisés par le contrôleur pour autoriser le point d'accès sont cette adresse MAC en utilisant le délimiteur défini.

Cet exemple montre comment configurer les WLC pour autoriser les AP à l'aide de Cisco ISE.

1. Dans l'interface graphique du contrôleur WLC, cliquez sur **Security > AP Policies**. La page AP Policies apparaît.
2. Sous Policy Configuration, cochez la case correspondant à **Authorize MIC APs against auth-list or AAA**. Lorsque vous choisissez ce paramètre, le WLC vérifie d'abord la liste d'autorisation locale. Si l'adresse MAC AP n'est pas présente, il vérifie le serveur RADIUS.



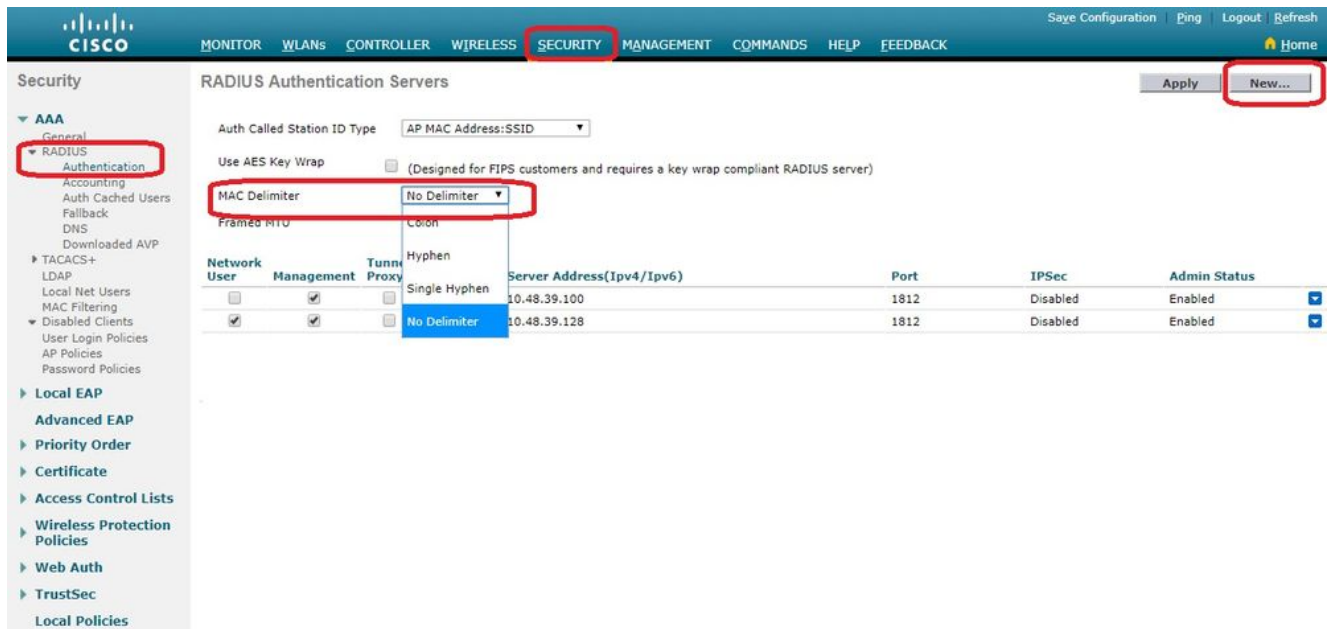
The screenshot shows the Cisco WLC GUI with the following details:

- Navigation: Security > AP Policies
- Policy Configuration:
  - Accept Self Signed Certificate (SSC):
  - Accept Manufactured Installed Certificate (MIC):
  - Accept Local Significant Certificate (LSC):
  - Authorize MIC APs against auth-list or AAA:  (highlighted with a red box)
  - Authorize LSC APs against auth-list:
- AP Authorization List (Entries 1 - 5 of 5):

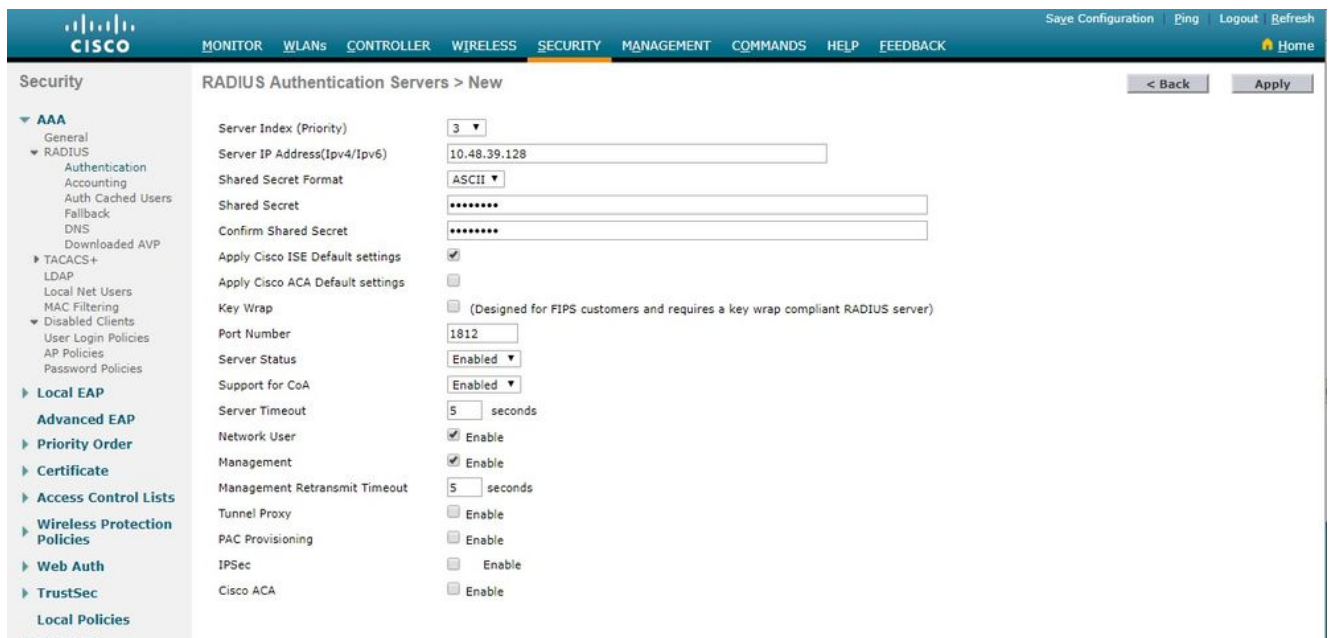
MAC address / Serial Number	Certificate Type	SHA1 Key Hash
4c:77:6d:9e:61:62	MIC	
70:d3:79:26:39:68	MIC	
88:f0:31:7e:e0:38	MIC	
f4:db:e6:43:c4:b2	MIC	
fc:5b:39:e7:2b:30	MIC	

3. Naviguez jusqu'à **Security > RADIUS Authentication** de l'interface graphique du contrôleur pour afficher **RADIUS Authentication Servers** s'affiche. Dans cette page vous pouvez définir le **Délimiteur MAC**. Le WLC obtient l'adresse MAC AP et l'envoie au serveur Radius en utilisant le délimiteur défini ici. Ceci est important afin que le nom d'utilisateur corresponde à ce qui est configuré dans le serveur Radius. Dans cet exemple, le **No Delimiter** est utilisé pour que le nom d'utilisateur soit 4c776d9e6162.





4. Cliquez ensuite sur **New** afin de définir un serveur RADIUS.



5. Définissez les paramètres du serveur RADIUS sur le **RADIUS Authentication Servers > New** s'affiche. Ces paramètres incluent le **RADIUS Server IP Address**, **Shared Secret**, **Port Number**, et **Server Status**. Lorsque vous avez terminé, cliquez sur **Apply**. Cet exemple utilise Cisco ISE comme serveur RADIUS avec l'adresse IP 10.48.39.128.

## Configurer Cisco ISE pour autoriser les points d'accès

Pour permettre à Cisco ISE d'autoriser des points d'accès, vous devez effectuer les étapes suivantes :

1. Configurez le WLC en tant que client AAA sur Cisco ISE.
2. Ajoutez les adresses MAC AP à la base de données sur Cisco ISE.

Cependant, vous pouvez ajouter l'adresse MAC AP en tant que terminaux (la meilleure façon) ou en tant qu'utilisateurs (dont les mots de passe sont également l'adresse MAC), mais cela vous oblige à diminuer les exigences des stratégies de sécurité par mot de passe.

Étant donné que le WLC n'envoie pas l'attribut NAS-Port-Type qui est une condition requise sur ISE pour correspondre au flux de travail d'authentification d'adresse Mac (MAB), vous devez modifier ceci.

## Configurer un nouveau profil de périphérique où MAB ne nécessite pas d'attribut de type de port NAS

Naviguez jusqu'à **Administration > Network device profile** et créez un nouveau profil de périphérique. Activez RADIUS et définissez le flux MAB filaire pour exiger service-type=Call-check, comme illustré dans l'image. Vous pouvez copier d'autres paramètres du profil Cisco classique, mais l'idée est de ne pas exiger l'attribut « Nas-port-type » pour un flux de travail MAB filaire.

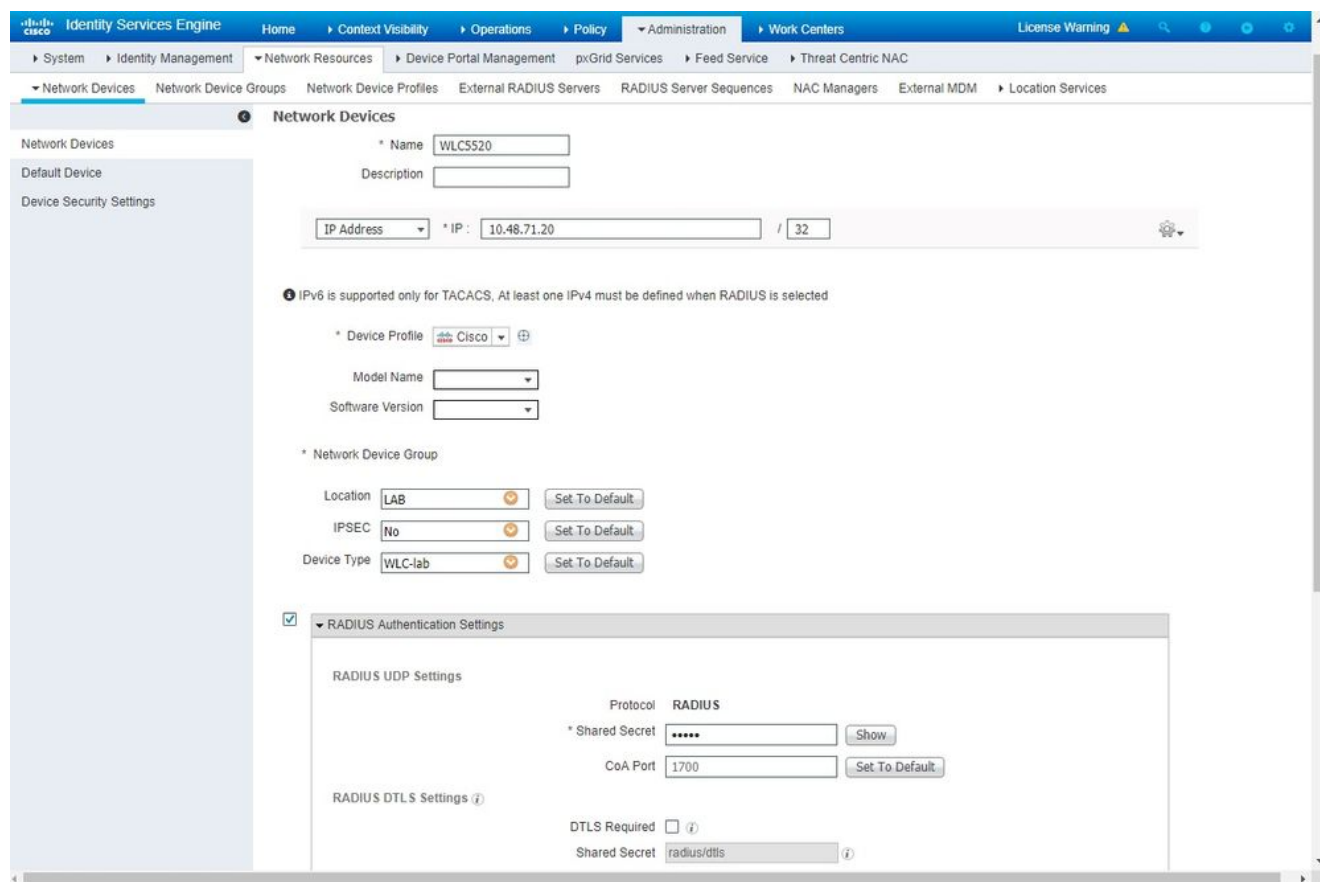
The screenshot shows the Cisco ISE Administration interface for configuring a Network Device Profile. The breadcrumb navigation is Administration > Network Resources. The main menu includes Network Devices, Network Device Groups, Network Device Profiles (selected), and External RADIUS Servers. The profile configuration form is as follows:

- Name:** Ciscotemp
- Description:** (Empty text area)
- Icon:** Cisco logo with buttons for "Change icon..." and "Set To Default".
- Vendor:** Cisco
- Supported Protocols:**
  - RADIUS:
  - TACACS+:
  - TrustSec:
- RADIUS Dictionaries:** (Empty list)
- Templates:** Expand All / Collapse All
- Authentication/Authorization:** (Collapsed)
- Flow Type Conditions:**
  - Wired MAB detected if the following condition(s) are met :
    - Radius:Service-Type = Call Check

## Configurer le WLC en tant que client AAA sur Cisco ISE

1. Aller à **Administration > Network Resources > Network Devices > Add**. La page New Network Device s'affiche.
2. Sur cette page, définissez le WLC Name, Interface de

gestion IP Address et Radius Authentications Settings genre Shared Secret. Si vous prévoyez d'entrer les adresses MAC AP en tant que points d'extrémité, assurez-vous d'utiliser le profil de périphérique personnalisé configuré précédemment plutôt que le profil Cisco par défaut !



The screenshot displays the Cisco Identity Services Engine (ISE) configuration interface for a Network Device. The main configuration area includes the following fields and options:

- Name:** WLC5520
- Description:** [Empty]
- IP Address:** 10.48.71.20 / 32
- Device Profile:** Cisco
- Model Name:** [Empty]
- Software Version:** [Empty]
- Network Device Group:**
  - Location:** LAB
  - IPSEC:** No
  - Device Type:** WLC-lab
- RADIUS Authentication Settings:**
  - Protocol:** RADIUS
  - Shared Secret:** [Redacted]
  - CoA Port:** 1700
  - DTLS Required:** [Unchecked]
  - Shared Secret:** radius/dtls

3. Cliquer Submit.

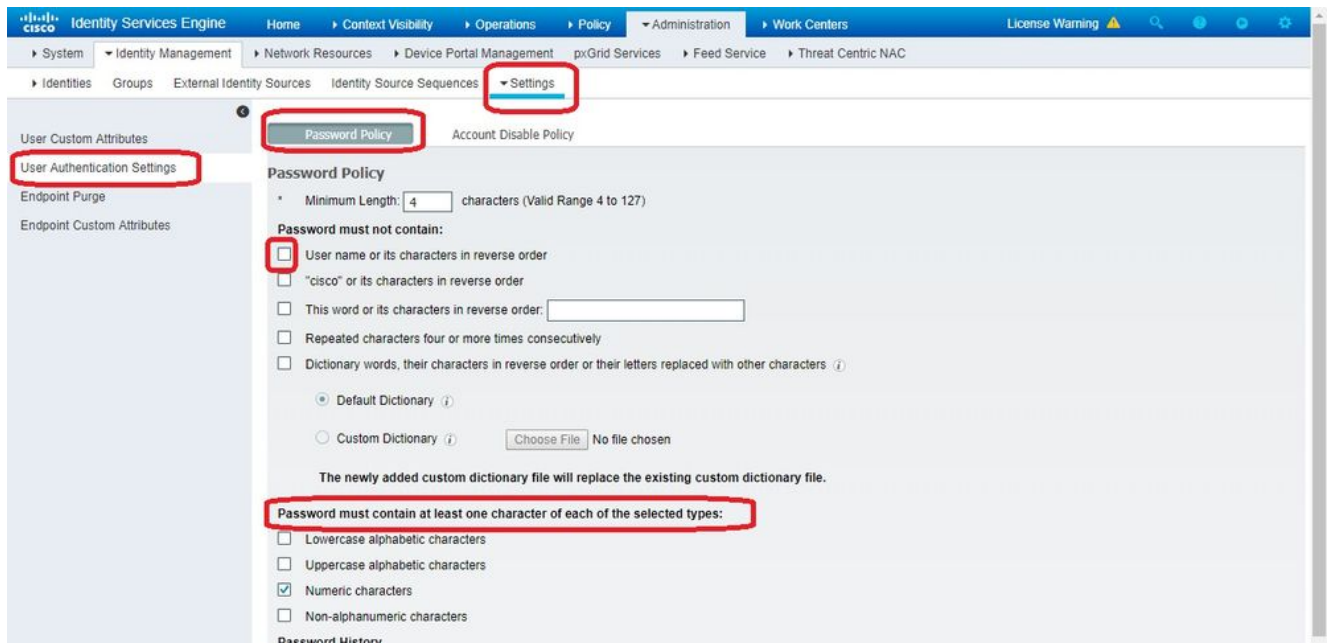
## Ajoutez l'adresse MAC AP à la base de données des terminaux sur Cisco ISE

Naviguez jusqu'à **Administration > Identity Management > Identities** et ajoutez les adresses MAC à la base de données des terminaux.

## Ajouter l'adresse MAC AP à la base de données utilisateur sur Cisco ISE (facultatif)

Si vous ne souhaitez pas modifier le profil MAB câblé et que vous choisissez de placer l'adresse MAC AP en tant qu'utilisateur, vous devez diminuer les exigences de la stratégie de mot de passe.

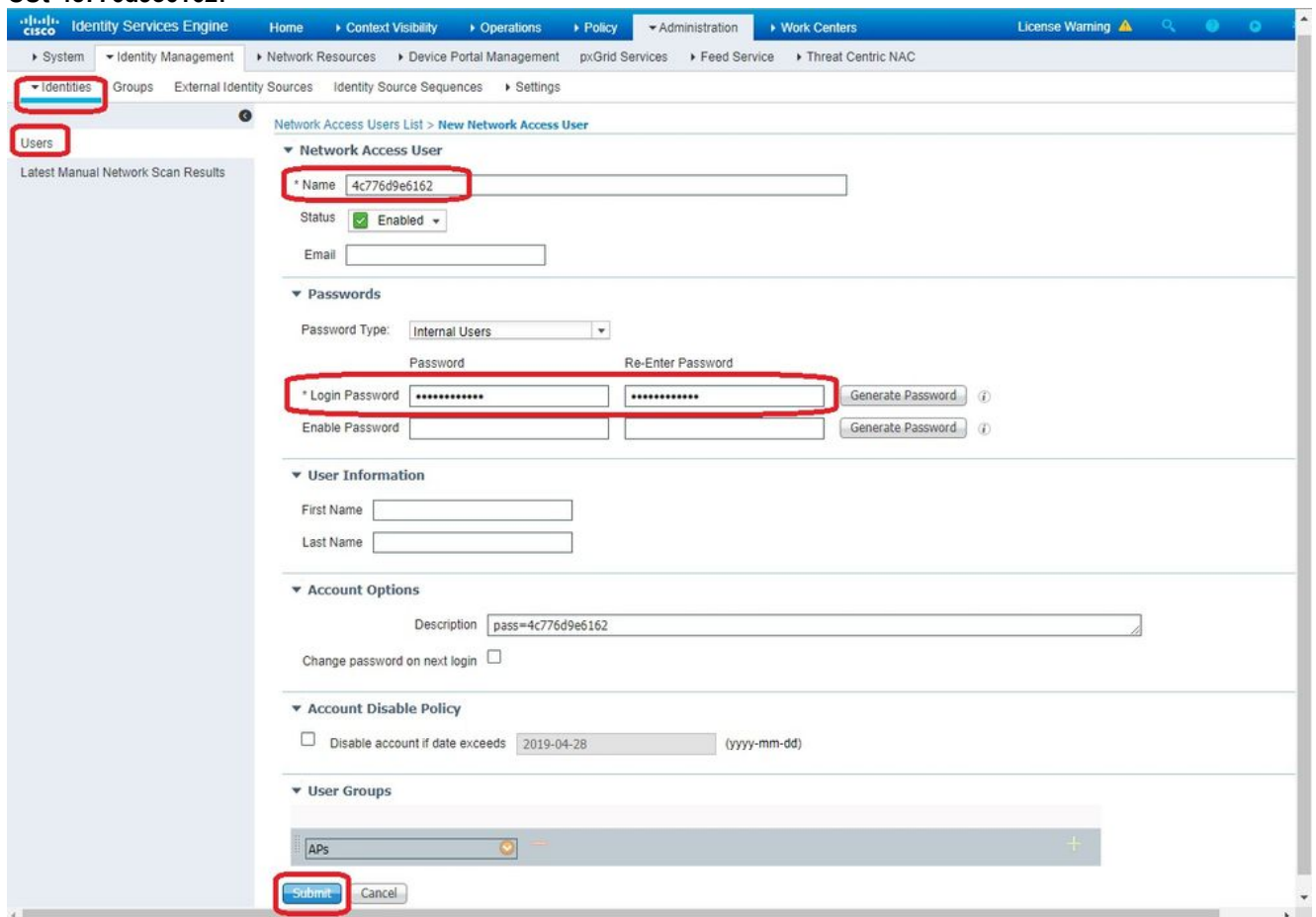
1. Naviguez jusqu'à **Administration > Identity Management**. Ici, nous devons nous assurer que la politique de mot de passe permet l'utilisation du nom d'utilisateur comme mot de passe et la politique doit également permettre l'utilisation des caractères d'adresse MAC sans avoir besoin de différents types de caractères. Naviguez jusqu'à **Settings > User Authentication Settings > Password Policy**:



2. Accédez ensuite à **Identities > Users** et cliquez sur **Add**. Lorsque la page **User Setup** apparaît, définissez le nom d'utilisateur et le mot de passe pour ce point d'accès comme indiqué.

**Astuce :** Utilisez **Description** pour entrer le mot de passe afin de pouvoir savoir facilement ce qui a été défini comme mot de passe.

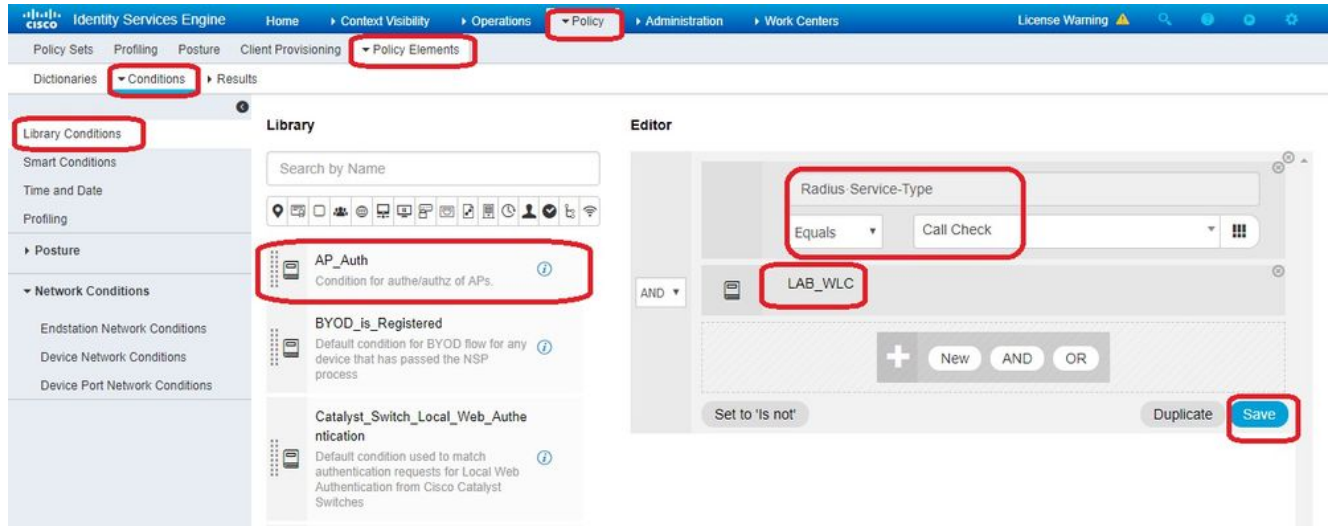
Le mot de passe doit également être l'adresse MAC AP. Dans cet exemple, il est **4c776d9e6162**.



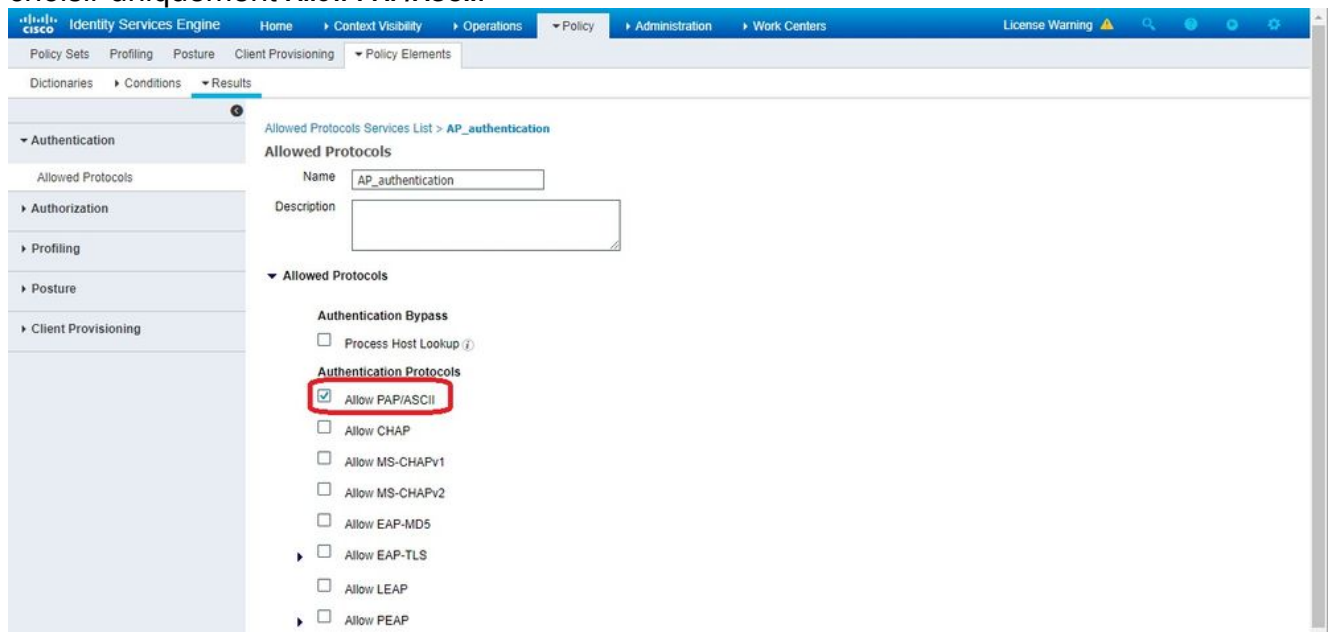
3. Cliquer **Submit**.

**Définir un ensemble de stratégies**

1. Vous devez définir un **Policy Set** pour correspondre à la demande d'authentification provenant du WLC. Vous commencez par créer une condition en navigant jusqu'à **Policy > Policy Elements > Conditionset** en créant une nouvelle condition pour correspondre à l'emplacement du WLC, dans cet exemple, 'LAB\_WLC' et **Radius:Service-Type Equals Call Check** qui est utilisé pour l'authentification Mac. Ici, la condition est nommée 'AP\_Auth'.



2. Cliquer **Save**.
3. Créez ensuite un nouveau **Allowed Protocols Service** pour l'authentification AP. Assurez-vous de choisir uniquement **Allow PAP/ASCII**:



4. Sélectionnez le service précédemment créé dans la **Allowed Protocols/Server Sequence**. Développez le **view** et **Authentication Policy > Use > Internal Users** afin qu'ISE recherche le nom d'utilisateur/mot de passe de l'AP dans la base de données interne.

The image displays two screenshots of the Cisco Identity Services Engine (ISE) configuration interface. The top screenshot shows the 'Policy Sets' overview page. A table lists policy sets, with 'Policy4APsAuth' selected. Red boxes highlight the 'AP\_Auth' condition in the 'Conditions' column and the 'AP\_authentication' protocol in the 'Allowed Protocols / Server Sequence' column. The bottom screenshot shows the detailed configuration for 'Policy4APsAuth'. It highlights the 'AP\_Auth' condition, the 'AP\_authentication' protocol, and the 'Internal Users' user group in the 'Authentication Policy' section. A 'Save' button is highlighted in the bottom right corner.

5. Cliquer **save**.

## Vérification

Afin de vérifier cette configuration, vous devez connecter le point d'accès avec l'adresse MAC 4c:77:6d:9e:61:62 au réseau et au moniteur.

Utilisez `debug capwap events/errors enable` et `debug aaa all enable` afin d'effectuer cette opération.

Comme le montrent les débogages, le WLC a transmis l'adresse MAC AP au serveur RADIUS 10.48.39.128, et le serveur a authentifié avec succès l'AP. L'AP s'enregistre alors auprès du contrôleur.

**Note:** Certaines lignes du résultat ont été déplacées vers la deuxième ligne en raison de contraintes d'espace.

```
*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Join Request from 192.168.79.151:5248
```

```
*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 using already allocated index 437
```

```
*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Unable to get Ap mode in Join request
```

```
*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Allocate database entry for AP
```

192.168.79.151:5248, already allocated index 437

\*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 AP Allocate request at index 437 (reserved)

\*spamApTask4: Feb 27 14:58:07.566: 24:7e:12:19:41:ef Deleting AP entry 192.168.79.151:5248 from temporary database.

\*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 AP group received default-group is found in ap group configured in wlc.

\*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Dropping request or response packet to AP :192.168.79.151 (5248) by Controller: 10.48.71.20 (5246), message Capwap\_wtp\_event\_response, state Capwap\_no\_state

\*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Message type Capwap\_wtp\_event\_response is not allowed to send in state Capwap\_no\_state for AP 192.168.79.151

\*spamApTask4: Feb 27 14:58:07.566: **70:69:5a:51:4e:c0 In AAA state 'Idle' for AP 70:69:5a:51:4e:c0**

\*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Join Request failed!

\*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 State machine handler: Failed to process msg type = 3 state = 0 from 192.168.79.151:5248

\*spamApTask4: Feb 27 14:58:07.566: 24:7e:12:19:41:ef Failed to parse CAPWAP packet from 192.168.79.151:5248

\*aaaQueueReader: Feb 27 14:58:07.566: **70:69:5a:51:4e:c0 Normal Response code for AAA Authentication : -9**

\*aaaQueueReader: Feb 27 14:58:07.566: ReProcessAuthentication previous proto 8, next proto 40000001

\*aaaQueueReader: Feb 27 14:58:07.566: AuthenticationRequest: 0x7f01b404f0f8

\*aaaQueueReader: Feb 27 14:58:07.566: Callback.....0xd6cef02166

\*aaaQueueReader: Feb 27 14:58:07.566: protocolType.....0x40000001

\*aaaQueueReader: Feb 27 14:58:07.566: proxyState.....70:69:5A:51:4E:C0-00:00

\*aaaQueueReader: Feb 27 14:58:07.566: Packet contains 9 AVPs:

\*aaaQueueReader: Feb 27 14:58:07.566: AVP[02] Called-Station-Id.....70:69:5a:51:4e:c0 (17 bytes)

\*aaaQueueReader: Feb 27 14:58:07.566: AVP[03] Calling-Station-Id.....4c:77:6d:9e:61:62 (17 bytes)

\*aaaQueueReader: Feb 27 14:58:07.566: AVP[04] Nas-Port.....0x00000001 (1) (4 bytes)

\*aaaQueueReader: Feb 27 14:58:07.566: AVP[05] Nas-Ip-Address.....0x0a304714 (170936084) (4 bytes)

\*aaaQueueReader: Feb 27 14:58:07.566: AVP[06] NAS-Identifier.....0x6e6f (28271) (2 bytes)

\*aaaQueueReader: Feb 27 14:58:07.566: AVP[08] Service-Type.....0x0000000a (10) (4 bytes)

\*aaaQueueReader: Feb 27 14:58:07.566: AVP[09] Message-Authenticator.....DATA (16 bytes)

\*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 radiusServerFallbackPassiveStateUpdate: **RADIUS server is ready 10.48.39.128 port 1812 index 1 active 1**

\*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 NAI-Realm not enabled on Wlan, radius servers will be selected as usual

\*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Found the radius server : 10.48.39.128 from the global server list

\*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Send Radius Auth Request with pktId:185 into qid:0 of server at index:1

\*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Sending the packet to v4 host 10.48.39.128:1812 of length 130

\*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 **Successful transmission of Authentication Packet (pktId 185) to 10.48.39.128:1812** from server queue 0, proxy state 70:69:5a:51:4e:c0-00:00

\*aaaQueueReader: Feb 27 14:58:07.566: 00000000: 01 b9 00 82 d9 c2 ef 27 f1 bb e4 9f a8 88 5a 6d .....'......Zm

\*aaaQueueReader: Feb 27 14:58:07.566: 00000010: 4b 38 1a a6 01 0e 34 63 37 37 36 64 39 65 36 31 K8....4c776d9e61

\*aaaQueueReader: Feb 27 14:58:07.566: 00000020: 36 32 1e 13 37 30 3a 36 39 3a 35 61 3a 35 31 3a 62..70:69:5a:51:

\*aaaQueueReader: Feb 27 14:58:07.566: 00000030: 34 65 3a 63 30 1f 13 34 63 3a 37 37 3a 36 64 3a 4e:c0..4c:77:6d:

\*aaaQueueReader: Feb 27 14:58:07.566: 00000040: 39 65 3a 36 31 3a 36 32 05 06 00 00 00 01 04 06 9e:61:62.....

\*aaaQueueReader: Feb 27 14:58:07.566: 00000050: 0a 30 47 14 20 04 6e 6f 02 12 54 46 96 61 2a 38 .0G...no..TF.a\*8

\*aaaQueueReader: Feb 27 14:58:07.566: 00000060: 5a 57 22 5b 41 c8 13 61 97 6c 06 06 00 00 00 0a ZW"[A..a.l.....

\*aaaQueueReader: Feb 27 14:58:07.566: 00000080: 15 f9 ..

\*aaaQueueReader: Feb 27 14:58:07.566: **70:69:5a:51:4e:c0 User entry not found in the Local FileDB for the client.**

\*radiusTransportThread: Feb 27 14:58:07.587: Vendor Specif Radius Attribute(code=26, avp\_len=28, vId=9)

\*radiusTransportThread: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 \*\*\* Counted VSA 150994944 AVP of length 28, code 1 atrlen 22)

\*radiusTransportThread: Feb 27 14:58:07.588: Vendor Specif Radius Attribute(code=26, avp\_len=28, vId=9)

\*radiusTransportThread: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 AVP: VendorId: 9, vendorType: 1, vendorLen: 22

\*radiusTransportThread: Feb 27 14:58:07.588: 00000000: 70 72 6f 66 69 6c 65 2d 6e 61 6d 65 3d 55 6e 6b profile-name=Unk

\*radiusTransportThread: Feb 27 14:58:07.588: 00000010: 6e 6f 77 6e nown

\*radiusTransportThread: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Processed VSA 9, type 1, raw bytes 22, copied 0 bytes

\*radiusTransportThread: Feb 27 14:58:07.588: **70:69:5a:51:4e:c0 Access-Accept received from RADIUS server 10.48.39.128** (qid:0) with port:1812, pktId:185

\*radiusTransportThread: Feb 27 14:58:07.588: RadiusIndexSet(1), Index(1)

\*radiusTransportThread: Feb 27 14:58:07.588: structureSize.....432

\*radiusTransportThread: Feb 27 14:58:07.588: protocolUsed.....0x00000001

\*radiusTransportThread: Feb 27 14:58:07.588: proxyState.....70:69:5A:51:4E:C0-00:00

\*radiusTransportThread: Feb 27 14:58:07.588: Packet contains 4 AVPs:

\*radiusTransportThread: Feb 27 14:58:07.588: **AVP[01] User-Name.....4c776d9e6162** (12 bytes)

\*radiusTransportThread: Feb 27 14:58:07.588: AVP[02] State.....ReauthSession:0a302780bNEx79SKIFosJ2ioAmIYNOiRe2iDSY3dr cFsHuYpChs (65 bytes)

\*radiusTransportThread: Feb 27 14:58:07.588: AVP[03] Class.....DATA (83 bytes)



```
*radiusTransportThread: Feb 27 14:58:07.588: AVP[04] Message-
Authenticator.....DATA (16 bytes)

*spamApTask0: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Join Version: = 134770432

*spamApTask0: Feb 27 14:58:07.588: 00:00:00:00:00:00 apType = 54 apModel: AIR-AP4800-E-K

*spamApTask0: Feb 27 14:58:07.588: 00:00:00:00:00:00 apType: Ox36 bundleApImageVer: 8.8.111.0
*spamApTask0: Feb 27 14:58:07.588: 00:00:00:00:00:00 version:8 release:8 maint:111 build:0
*spamApTask0: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Join resp: CAPWAP Maximum Msg element len =
79

*spamApTask0: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Join Response sent to 0.0.0.0:5248

*spamApTask0: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 CAPWAP State: Join
```

## Dépannage

Utilisez ces commandes pour dépanner votre configuration :

- debug capwap events enable: configure le débogage des événements LWAPP
- debug capwap packet enable— Configure le débogage de la trace de paquet LWAPP
- debug capwap errors enable— Configure le débogage des erreurs de paquets LWAPP
- debug aaa all enable: configure le débogage de tous les messages AAA

Dans ce cas, ISE signale dans le journal RADIUS en direct le nom d'utilisateur « INVALID » au moment où vous avez des AP autorisés par rapport à ISE, cela signifie que l'authentification est vérifiée par rapport à la base de données de point d'extrémité et que vous n'avez pas modifié le profil MAB câblé comme expliqué dans ce document. ISE considère qu'une authentification d'adresse MAC n'est pas valide si elle ne correspond pas au profil MAB filaire/sans fil, qui par défaut nécessite l'attribut NAS-port-type qui n'est pas envoyé par le WLC.

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.