Configurer l'affectation de VLAN dynamique avec des WLC basés sur la carte de groupe ISE vers Active Directory

Table des matières

Introduction

Ce document décrit le concept d'affectation dynamique de VLAN.

Conditions préalables

Le document décrit comment configurer le contrôleur LAN sans fil (WLC) et le serveur ISE (Identity Services Engine) afin d'attribuer dynamiquement des clients LAN sans fil (WLAN) dans un VLAN spécifique.

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base des contrôleurs LAN sans fil (WLC) et des points d'accès légers (LAP)
- Connaissance fonctionnelle d'un serveur d'authentification, d'autorisation et de comptabilité (AAA) tel qu'un ISE

- Avoir une connaissance complète des réseaux sans fil et des problèmes liés à la sécurité sans fil
- Connaissance fonctionnelle et configurable de l’attribution dynamique de VLAN
- Compréhension de base des services Microsoft Windows AD, ainsi que des concepts de contrôleur de domaine et DNS
- Connaissance de base du protocole CAPWAP (Control And Provisioning of Access Point Protocol)

Composants utilisés

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

- WLC de la gamme Cisco 5520 qui exécute la version de microprogramme 8.8.11.0
- AP de la gamme Cisco 4800
- Demandeur Windows natif et NAM Anyconnect
- Cisco Secure ISE version 2.3.0.298
- Microsoft Windows 2016 Server configuré comme contrôleur de domaine
- Commutateur de la gamme Cisco 3560-CX qui exécute la version 15.2(4)E1

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Affectation de VLAN dynamique avec le serveur RADIUS

Dans la plupart des systèmes WLAN, chaque WLAN a une stratégie statique qui s'applique à tous les clients associés à un SSID (Service Set Identifier), ou WLAN dans la terminologie du contrôleur. Bien que puissante, cette méthode a des limitations parce qu'elle exige que les clients soient associés à des SSID différents afin d'hériter de QoS et de stratégies de sécurité différentes.

La solution WLAN de Cisco résout cette limitation en prenant en charge la mise en réseau des identités. Cela permet au réseau d'annoncer un SSID unique, mais permet à des utilisateurs spécifiques d'hériter de différentes qualités de service, attributs VLAN et/ou stratégies de sécurité en fonction des informations d'identification de l'utilisateur.

L'affectation de VLAN dynamique est une fonction qui place un utilisateur sans fil dans un VLAN spécifique en fonction des informations fournies par l'utilisateur. Cette tâche d'affectation d'utilisateurs à un VLAN spécifique est gérée par un serveur d'authentification RADIUS, tel que Cisco ISE. Ceci peut être utilisé, par exemple, afin de permettre à l'hôte sans fil de rester sur le même VLAN lorsqu'il se déplace au sein d'un réseau de campus.

Le serveur Cisco ISE authentifie les utilisateurs sans fil par rapport à l'une des bases de données possibles, qui inclut sa base de données interne. Exemple :

- Base de données interne
- Active Directory
- Protocole LDAP (Generic Lightweight Directory Access Protocol)
- Bases de données relationnelles compatibles ODBC (Open Database Connectivity)
- Serveurs à jetons SecurID Rivest, Shamir et Adelman (RSA)
- Serveurs de jetons compatibles RADIUS

Les protocoles d'authentification Cisco ISE et les sources d'identité externes prises en charge répertorient les différents protocoles d'authentification pris en charge par les bases de données internes et externes ISE.

Ce document se concentre sur l'authentification des utilisateurs sans fil qui utilisent la base de données externe Windows Active Directory.

Après une authentification réussie, ISE récupère les informations de groupe de cet utilisateur dans la base de données Windows et associe l'utilisateur au profil d'autorisation correspondant.

Lorsqu'un client tente de s'associer à un LAP enregistré auprès d'un contrôleur, le LAP transmet les informations d'identification de l'utilisateur au WLC à l'aide de la méthode EAP respective.

WLC envoie ces informations d'identification à ISE avec l'utilisation du protocole RADIUS (encapsulation de l'EAP) et ISE transmet les informations d'identification des utilisateurs à AD pour validation avec l'aide du protocole KERBEROS.

AD valide les informations d'identification de l'utilisateur et, après authentification réussie, informe l'ISE.

Une fois l'authentification réussie, le serveur ISE transmet certains attributs IETF (Internet Engineering Task Force) au WLC. Ces attributs RADIUS déterminent l'ID de VLAN qui doit être attribué au client sans fil. Le SSID (WLAN, en termes de WLC) du client n'importe pas parce que l'utilisateur est toujours affecté à cet ID de VLAN prédéterminé.

Les attributs d'utilisateur RADIUS utilisés pour l'affectation de l'ID de VLAN sont :

- IETF 64 (type de tunnel)—Définissez cette valeur sur VLAN

- IETF 65 (Tunnel Medium Type)—Définissez cette valeur sur 802
- IETF 81 (ID de groupe privé de tunnel)—Définissez cette valeur sur ID de VLAN

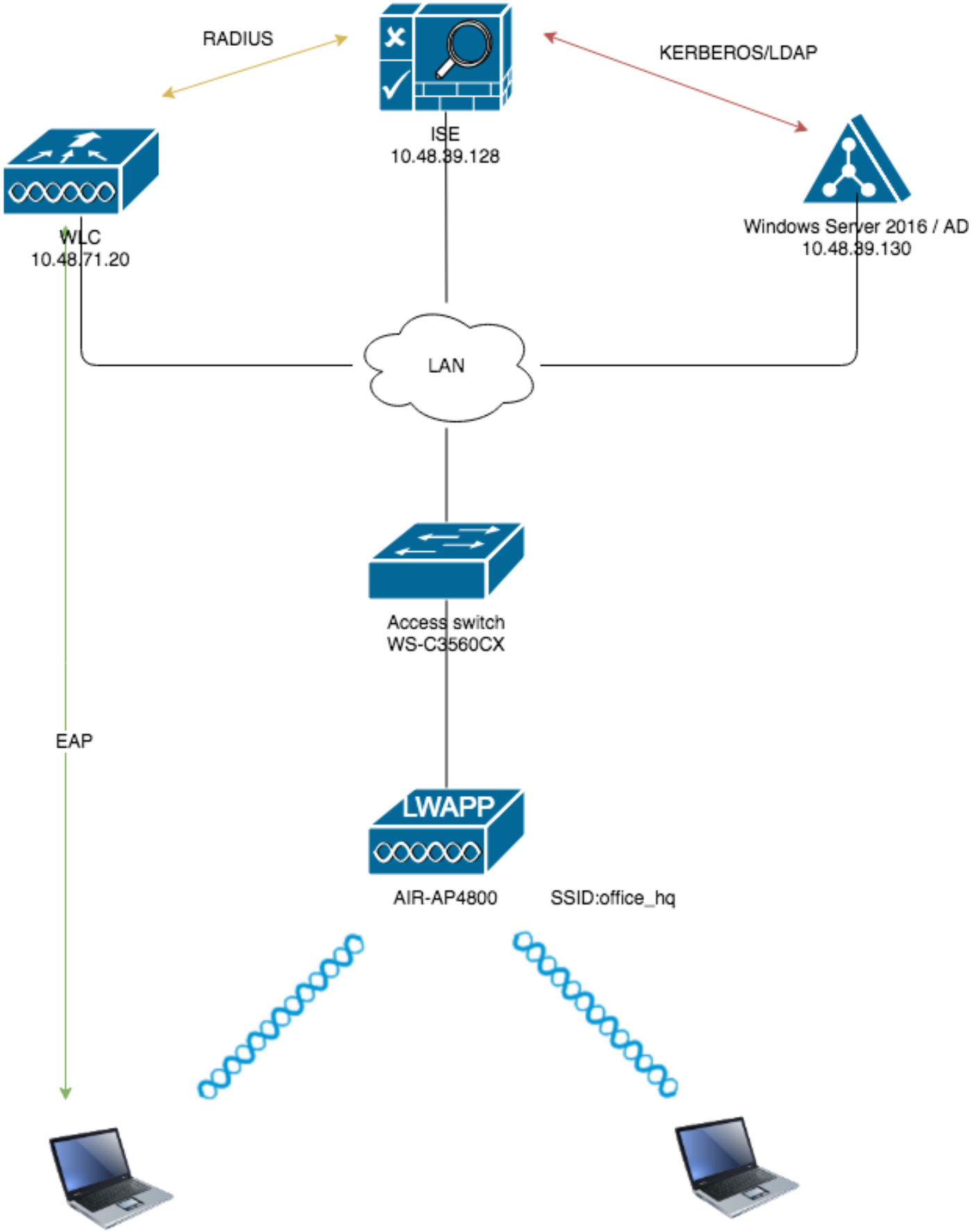
L'ID de VLAN est de 12 bits et prend une valeur comprise entre 1 et 4094 inclus. Étant donné que l'ID de groupe privé de tunnel est de type chaîne, comme défini dans RFC2868 pour une utilisation avec IEEE 802.1X, la valeur entière de l'ID de VLAN est codée sous la forme d'une chaîne. Quand ces attributs de tunnel sont envoyés, il est nécessaire de renseigner la zone Tag.

Comme indiqué dans la RFC 2868, section 3.1 : le champ Tag a une longueur d'un octet et est destiné à fournir un moyen de regrouper des attributs dans le même paquet qui font référence au même tunnel. Les valeurs valides pour cette zone sont comprises entre 0x01 et 0x1F, inclus. Si la zone Tag est inutilisée, elle doit avoir pour valeur zéro (0x00). Référez-vous à RFC 2868 pour plus d'informations sur tous les attributs RADIUS.

Configurer

Cette section fournit les informations nécessaires à la configuration des fonctions décrites dans le document.

Diagramme du réseau

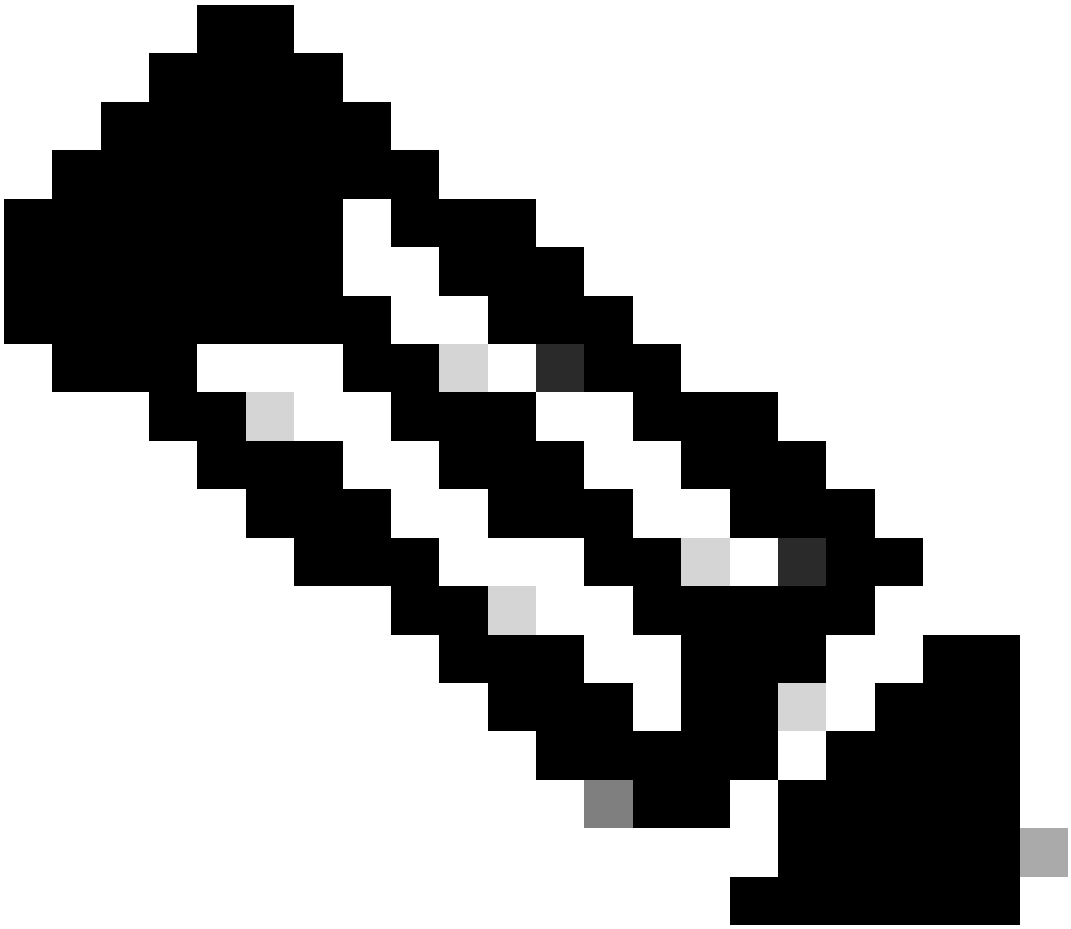


Configurations

Voici les détails de configuration des composants utilisés dans ce diagramme :

- L'adresse IP du serveur ISE (RADIUS) est 10.48.39.128.
- L'adresse d'interface de gestion et de gestionnaire AP du WLC est 10.48.71.20.
- Le serveur DHCP réside sur le réseau local et est configuré pour les pools de clients respectifs ; il n'est pas représenté sur le schéma.
- Les VLAN1477 et VLAN1478 sont utilisés tout au long de cette configuration. Les utilisateurs du service Marketing sont configurés pour être placés dans le VLAN1477 et les utilisateurs du service RH sont configurés pour être placés dans le VLAN1478 par le serveur RADIUS Lorsque les deux utilisateurs se connectent au même SSID : office_hq.

  VLAN1477 : 192.168.77.0/24. Passerelle : 192.168.77.1 VLAN148 : 192.168.78.0/24. Passerelle : 192.168.78.1
- Ce document utilise 802.1x avec PEAP-mschapv2 comme mécanisme de sécurité.



Remarque : Cisco recommande d'utiliser des méthodes d'authentification avancées, telles que l'authentification EAP-FAST et EAP-TLS, afin de sécuriser le WLAN.

Les hypothèses suivantes sont faites avant d'effectuer cette configuration :

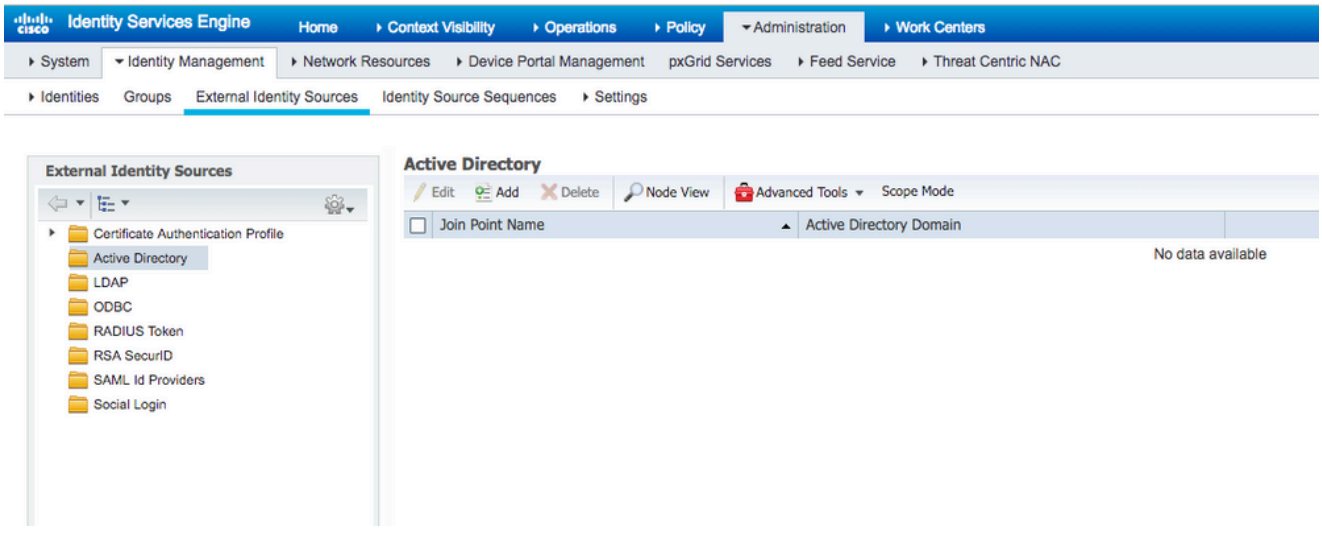
- Le LAP est déjà enregistré auprès du WLC
- Une étendue DHCP est attribuée au serveur DHCP
- La connectivité de couche 3 existe entre tous les périphériques du réseau
- Le document traite de la configuration requise du côté sans fil et suppose que le réseau câblé est en place
- Les utilisateurs et les groupes respectifs sont configurés sur Active Directory

Afin d'effectuer l'affectation de VLAN dynamique avec des WLC basés sur le mappage de groupe ISE à AD, ces étapes doivent être effectuées :

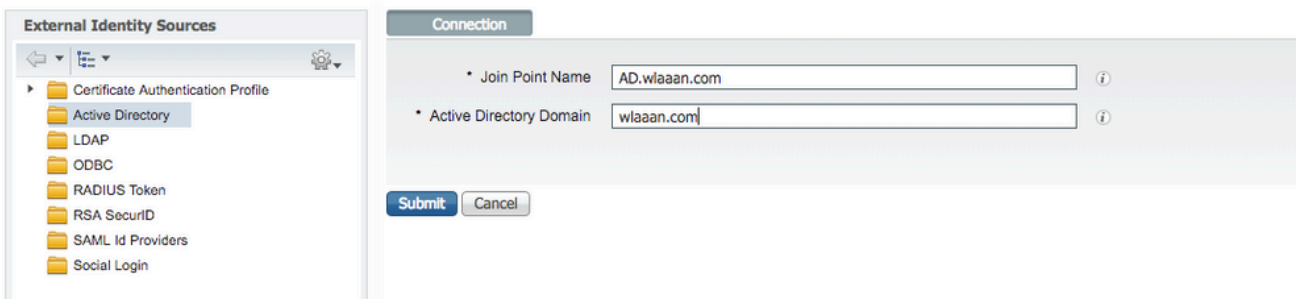
1. Intégration et configuration ISE à AD des politiques d'authentification et d'autorisation pour les utilisateurs sur ISE.
2. Configuration WLC afin de prendre en charge l'authentification dot1x et le remplacement AAA pour SSID 'office_hq'.
3. Configuration du demandeur du client final.

Intégration et configuration ISE à AD des stratégies d'authentification et d'autorisation pour les utilisateurs sur ISE

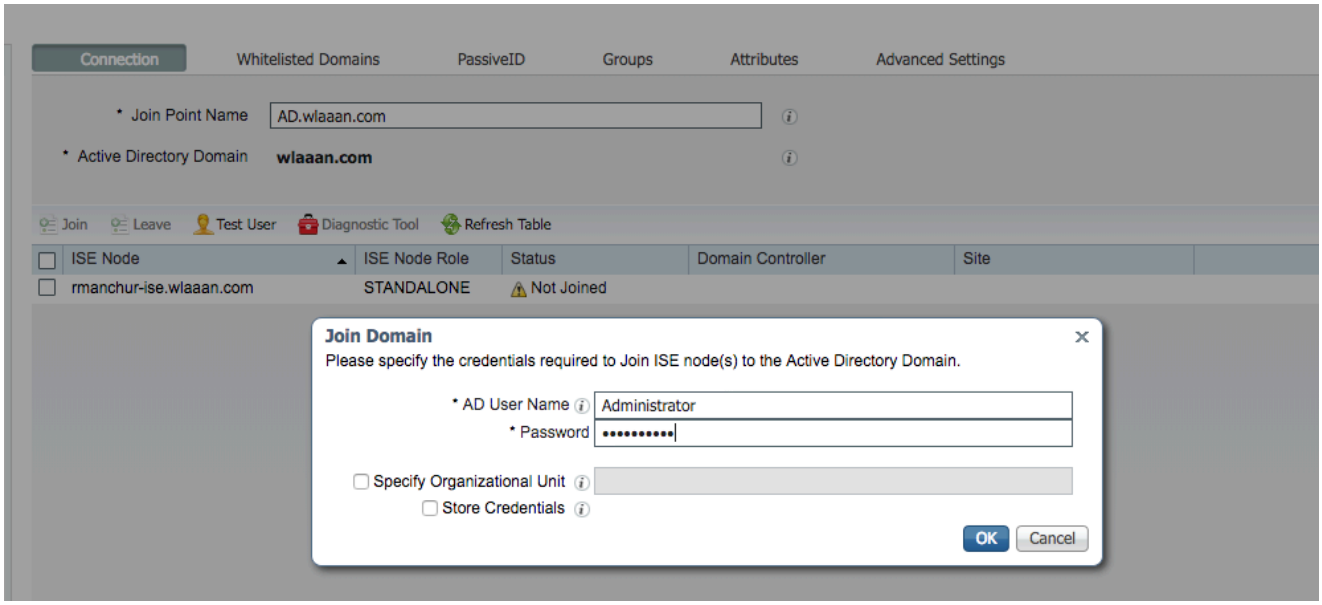
1. Connectez-vous à l'interface utilisateur Web ISE à l'aide d'un compte admin.
2. Accédez àAdministration > Identity management > External Identity Sources > Active directory.



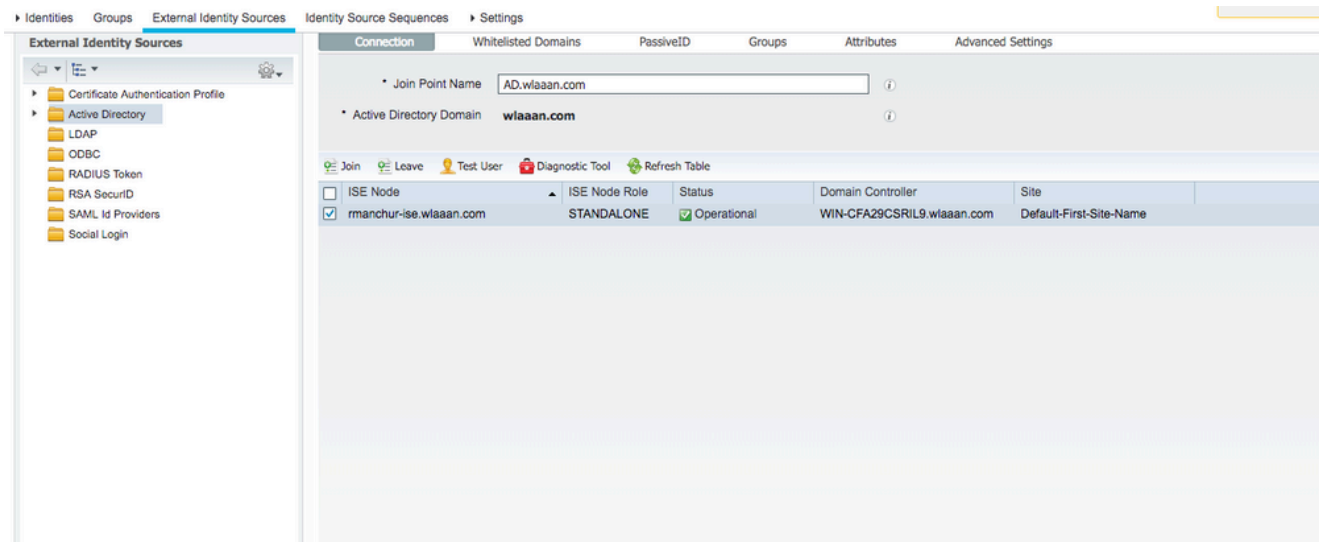
3. Cliquez sur Ajouter et entrez le nom de domaine et le nom du magasin d'identités à partir des paramètres de nom du point de jonction Active Directory. Dans l'exemple, ISE est enregistré dans le domainewlaaan.comet le point de jointure est spécifié commeAD.wlaaan.comun nom significatif localement pour ISE.



4. Une fenêtre contextuelle s'ouvre une foisSubmitque vous avez appuyé sur le bouton pour vous demander si vous souhaitez vous connecter immédiatement à ISE et à AD. Appuyez surYeset fournissez des informations d'identification d'utilisateur Active Directory avec des droits d'administration pour ajouter un nouvel hôte au domaine.



5. Après ce point, vous devez avoir ISE correctement enregistré auprès d'AD.



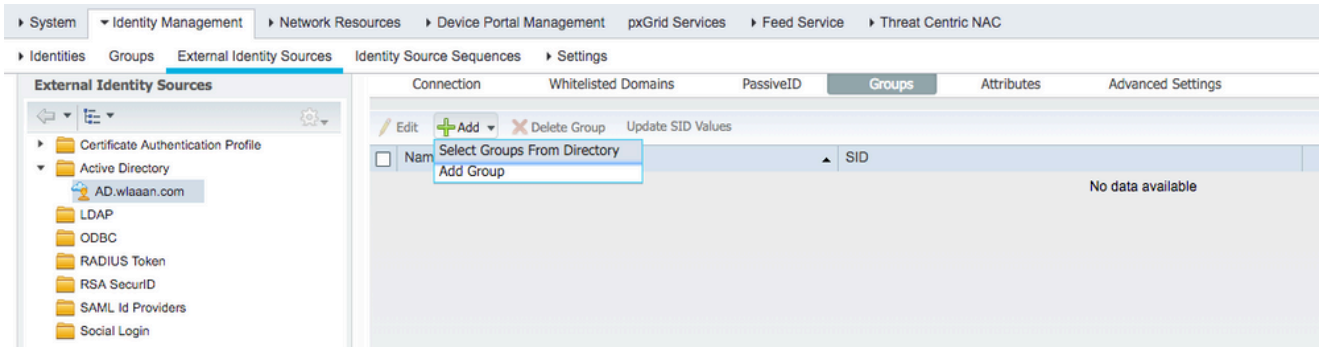
En cas de problème avec le processus d'enregistrement, vous pouvez utiliser l'Diagnostic Tool

afin d'exécuter les tests requis pour la connectivité AD.

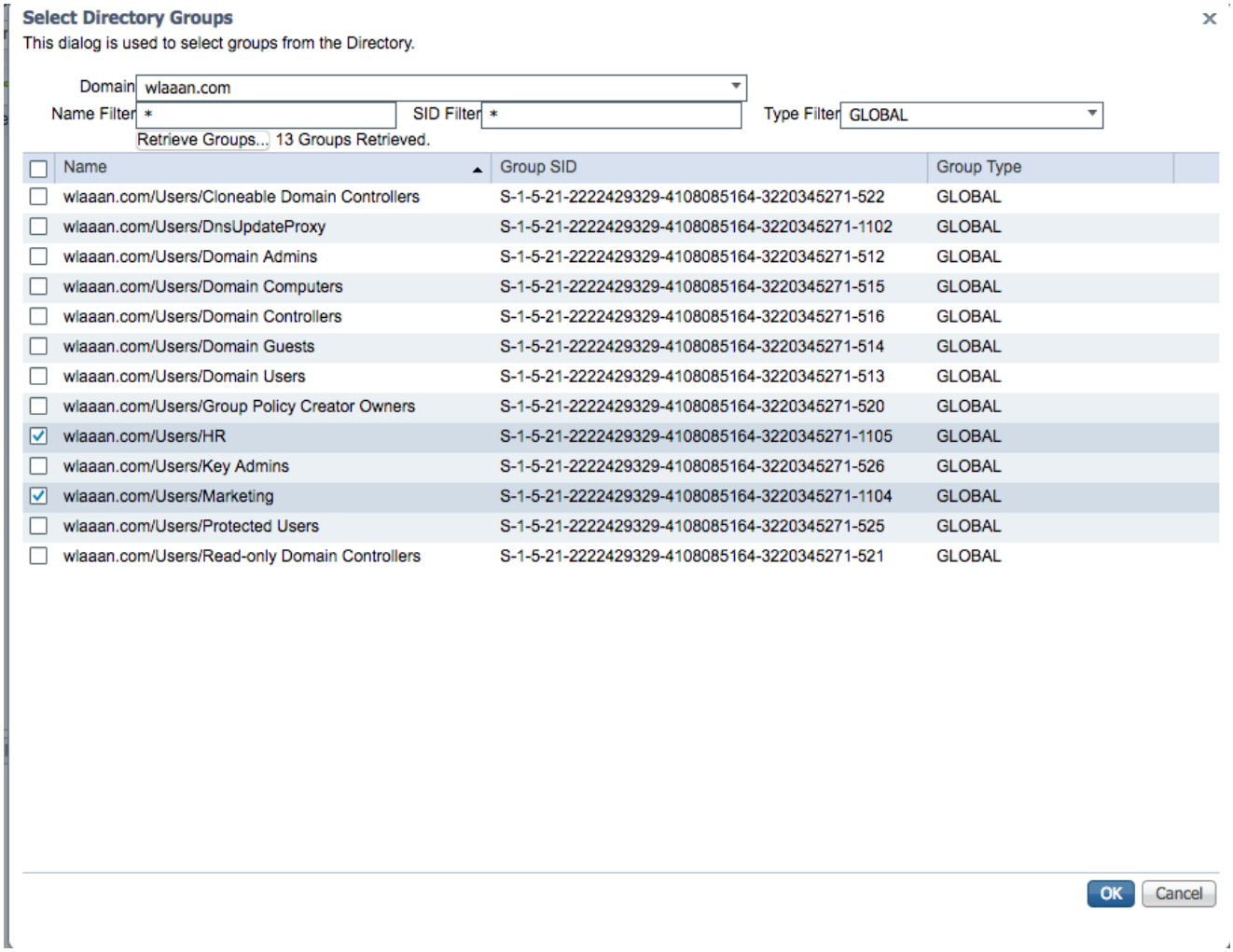
6. Vous devez récupérer les groupes pour les répertoires actifs qui sont utilisés afin d'attribuer des profils d'autorisation respectifs. Accédez àAdministration > Identity management > External Identity Sources > Active directory >

   > Groups

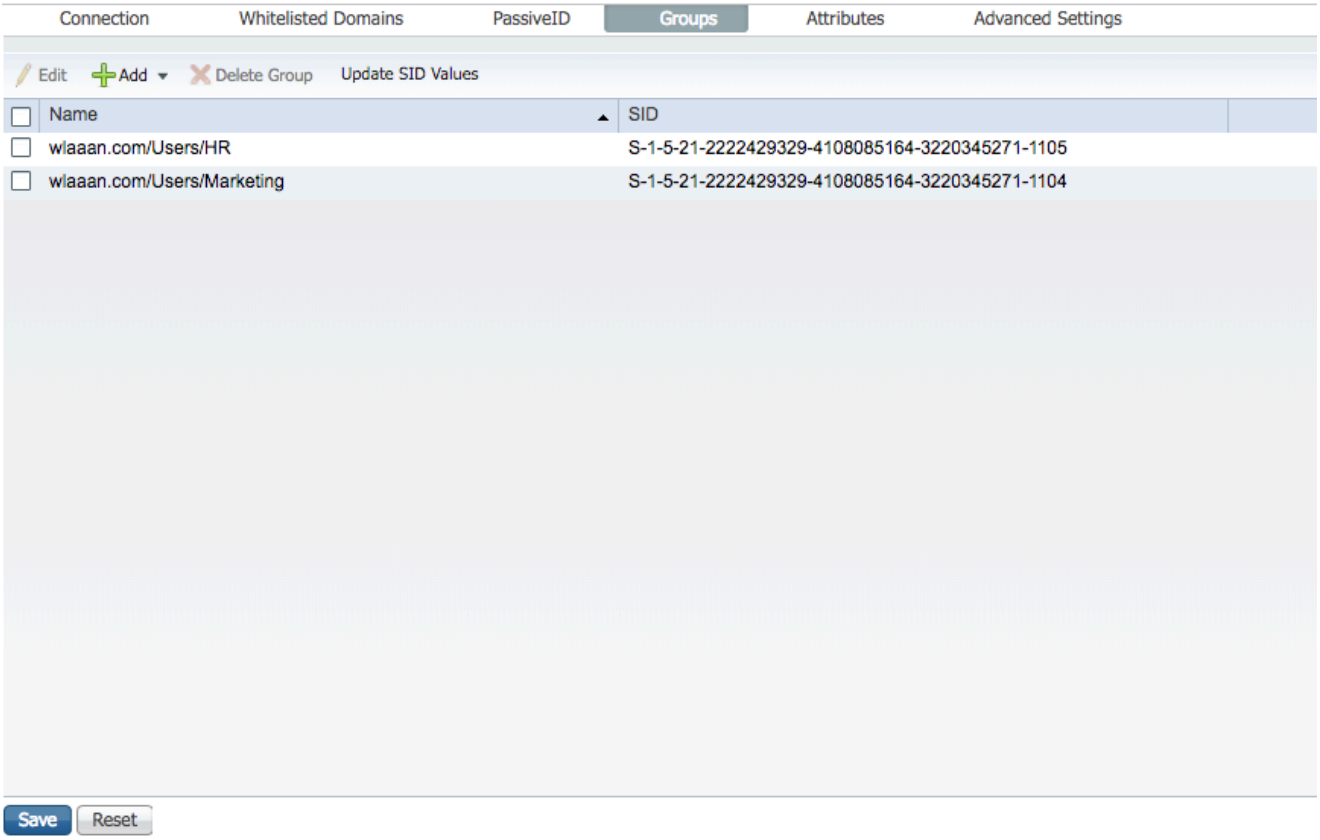
   , puis cliquez surAddet choisissezSelect Groups from Active Directory.



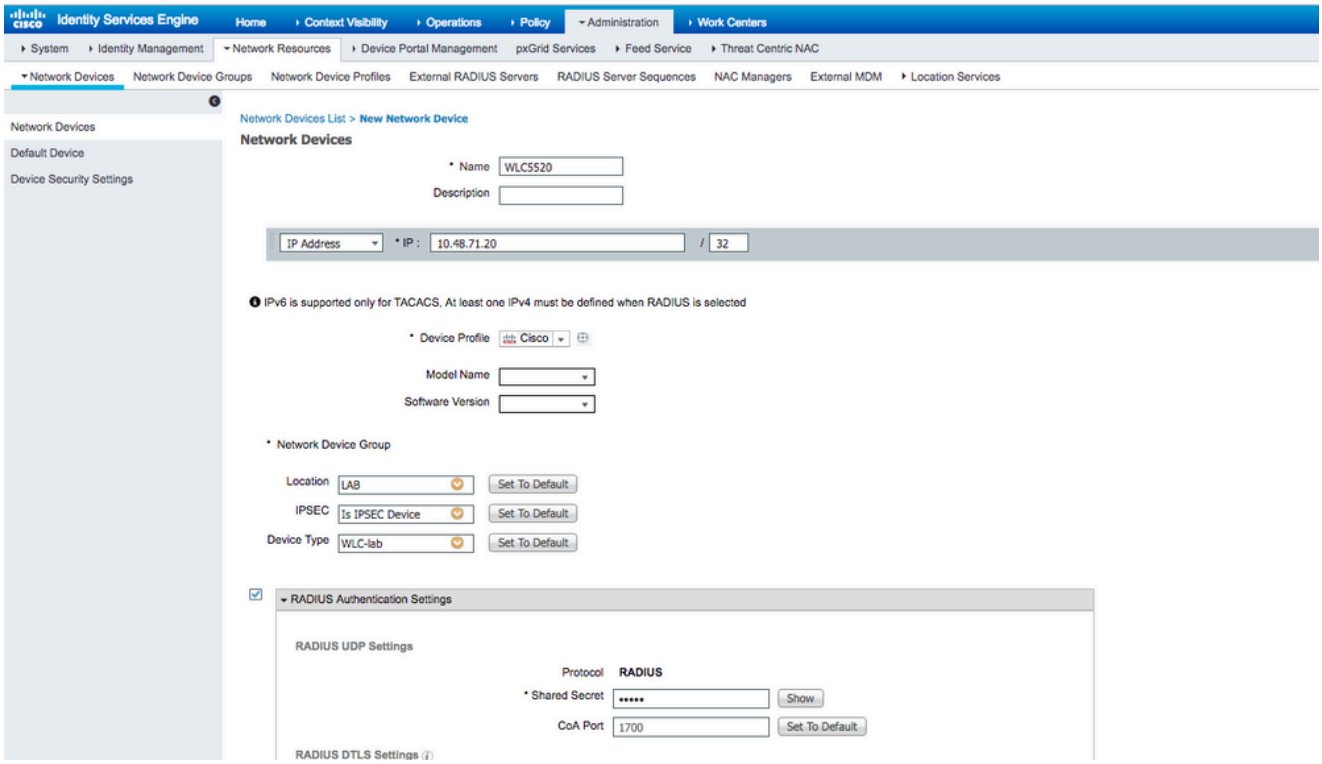
7. Une nouvelle fenêtre contextuelle s'ouvre, dans laquelle vous pouvez spécifier un filtre afin de récupérer des groupes spécifiques ou récupérer tous les groupes à partir d'Active Directory.
   Choisissez les groupes respectifs dans la liste des groupes AD et appuyez surOK.



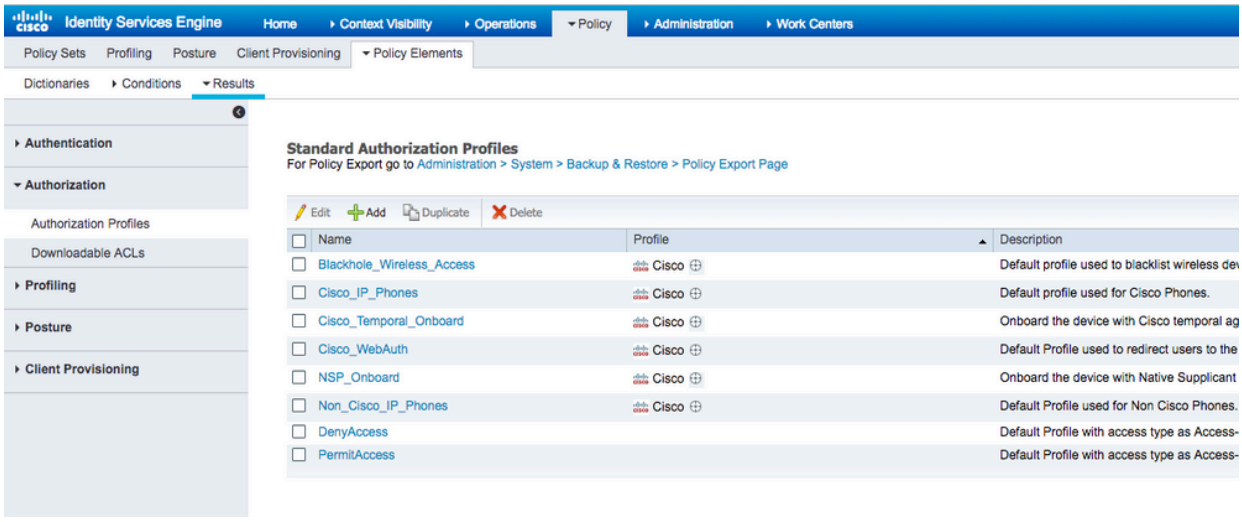
8. Les groupes respectifs sont ajoutés à ISE et peuvent être enregistrés. Appuyez surSave.



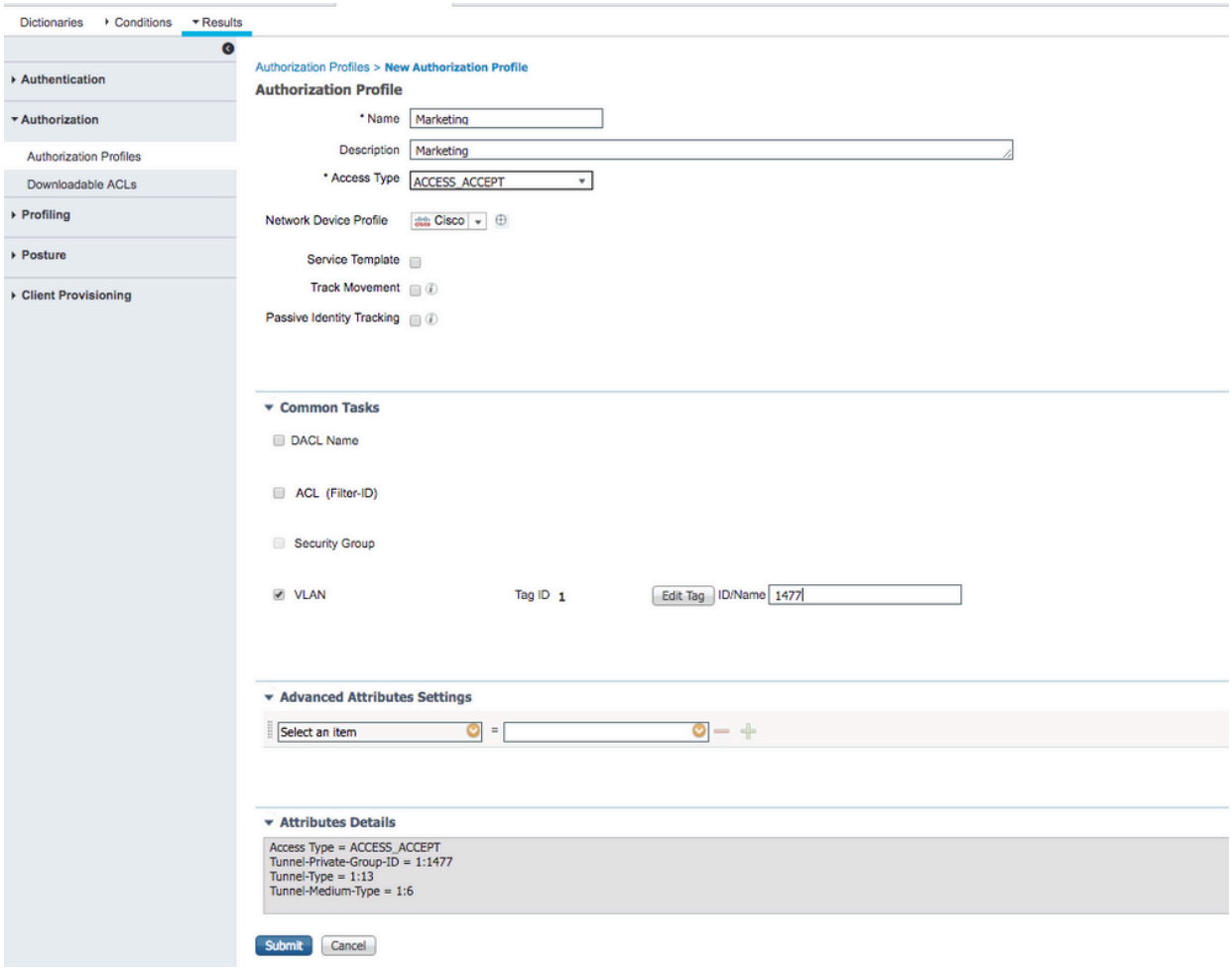
9. Ajoutez WLC à la liste des périphériques réseau ISE - accédez àAdministration > Network Resources > Network Devicesetappuyez surAdd.
   Configuration complète, en fournissant l'adresse IP de gestion WLC et le secret partagé RADIUS entre WLC et ISE.



10. Maintenant, après avoir rejoint ISE à AD et ajouté le WLC à la liste des périphériques, vous pouvez commencer la configuration des stratégies d'authentification et d'autorisation pour les utilisateurs.
    - Créez un profil d'autorisation afin d'attribuer des utilisateurs de Marketing à VLAN1477 et du groupe HR à VLAN1478.
      Accédez àPolicy > Policy Elements > Results > Authorization > Authorization profilesetcliquez sur le boutonAddafin de créer un nouveau profil.

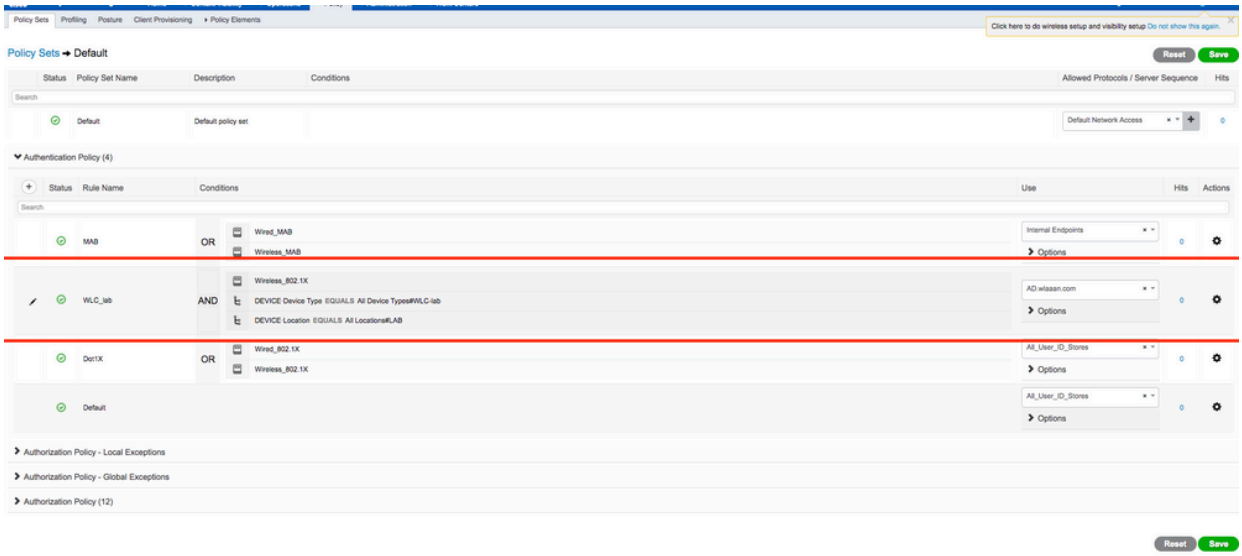


    - MarketingComplétez la configuration du profil d'autorisation avec les informations VLAN pour le groupe correspondant ; l'exemple montre les paramètres de configuration du groupe.

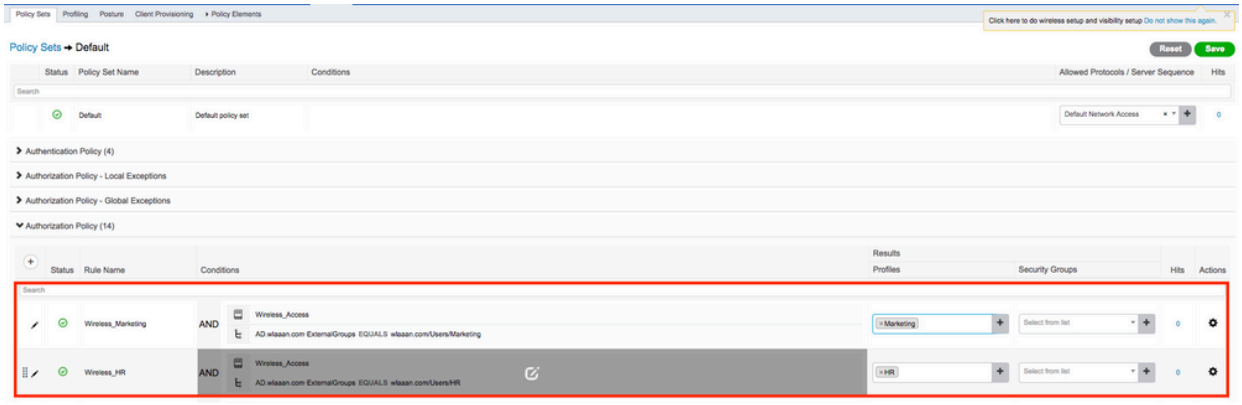


Une configuration similaire doit être effectuée pour les autres groupes et les attributs de balise VLAN respectifs doivent être configurés.

- Une fois les profils d'autorisation configurés, vous pouvez définir des stratégies d'authentification pour les utilisateurs sans fil. Pour ce faire, vous pouvez configurer`Custom`ou modifier le jeu de stratégies`Default`. Dans cet exemple, le jeu de stratégies par défaut est modifié. Accédez à`Policy > Policy Sets > Default`. `dot1x`Par défaut pour le type d'authentification, ISE va utiliser`All_User_ID_Stores`, bien qu'il fonctionne même avec les paramètres par défaut actuels puisque AD fait partie de la liste de sources d'identité de`All_User_ID_Stores`, cet exemple utilise une règle plus spécifique`WLC_lab`pour ce contrôleur LAB respectif et utilise AD comme seule source pour l'authentification.

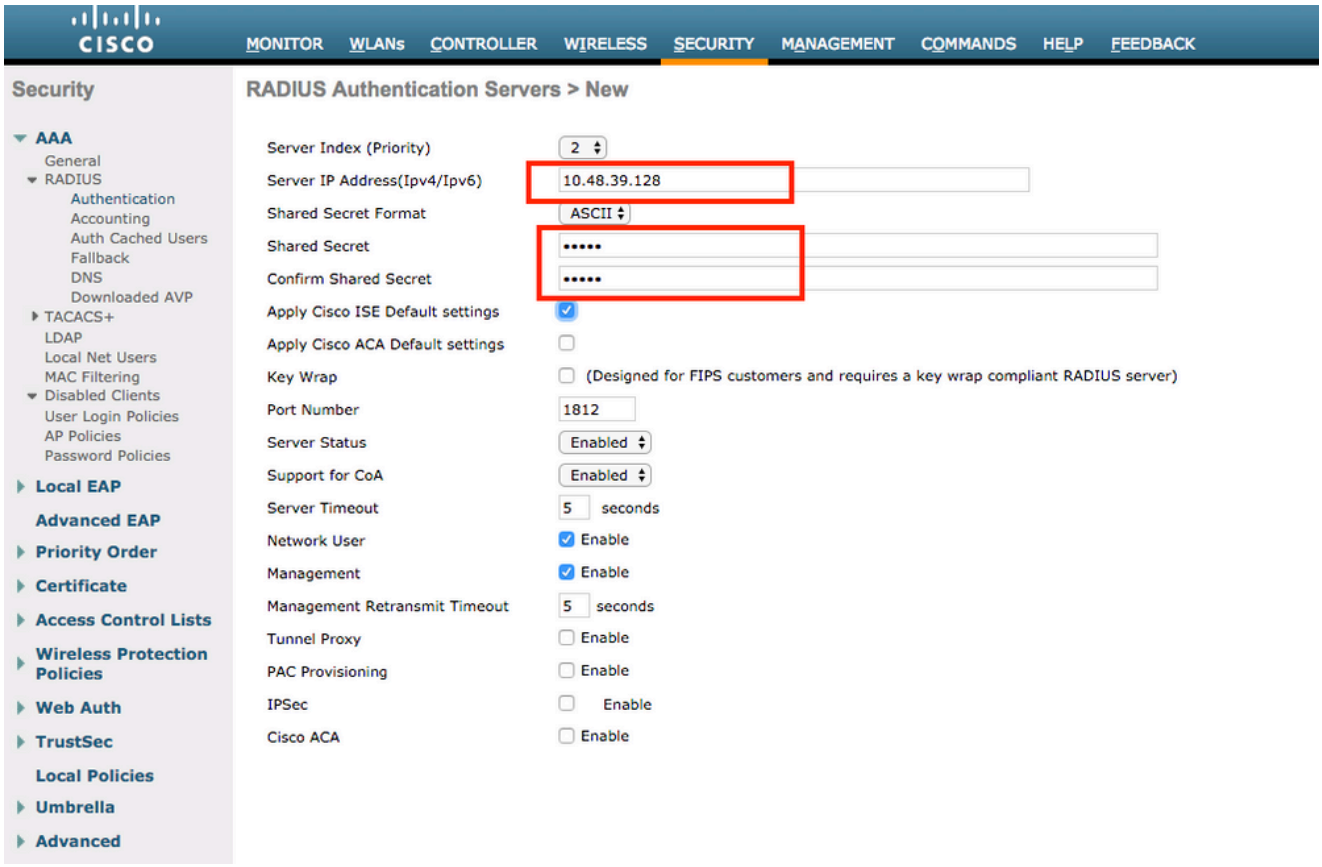


- Vous devez maintenant créer des stratégies d'autorisation pour les utilisateurs qui attribuent des profils d'autorisation respectifs en fonction de l'appartenance au groupe. Accédez à la sectionAuthorization policyet créez des stratégies afin de répondre à cette exigence.

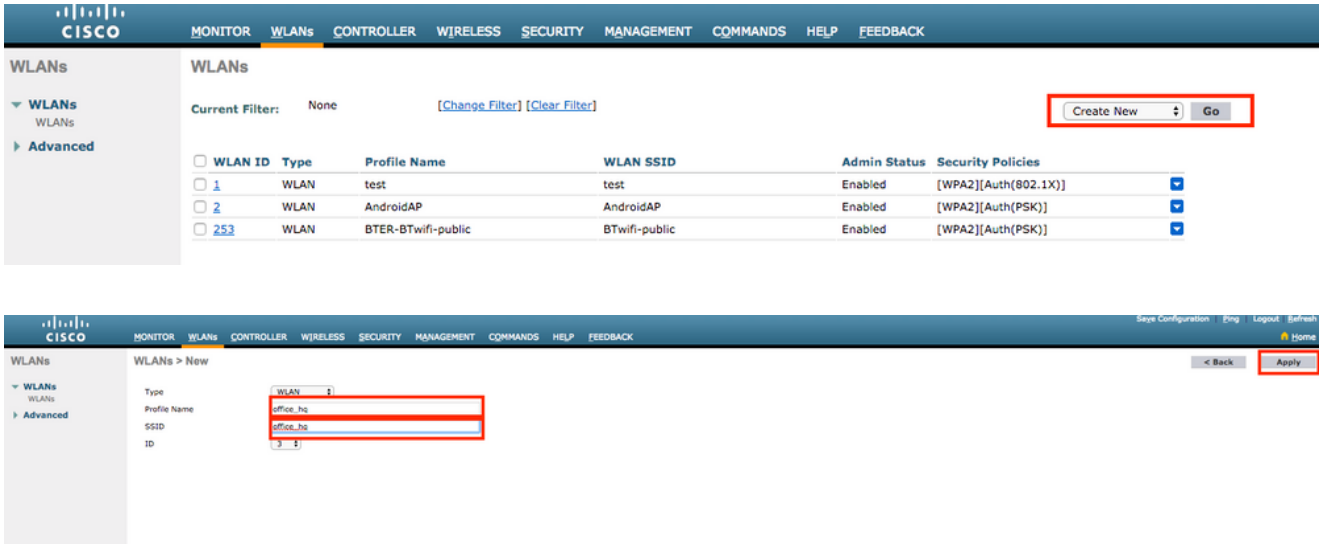


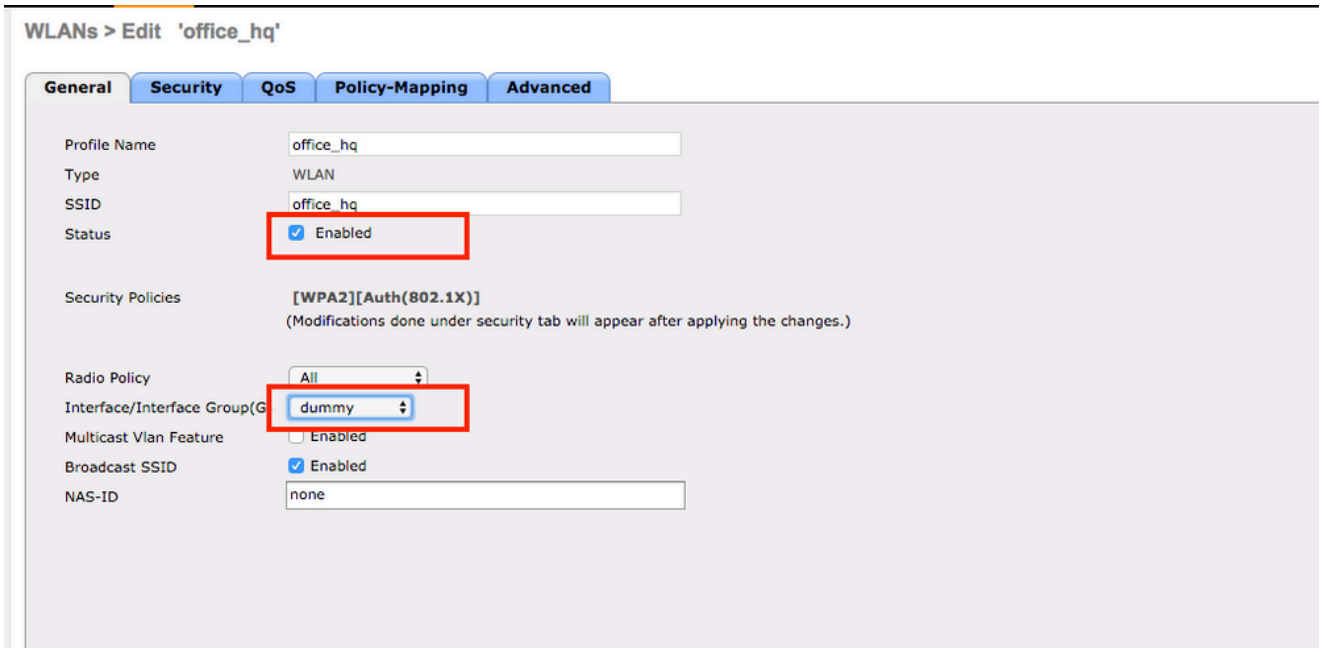
Configuration WLC pour prendre en charge l'authentification dot1x et le remplacement AAA pour le SSID 'office_hq'

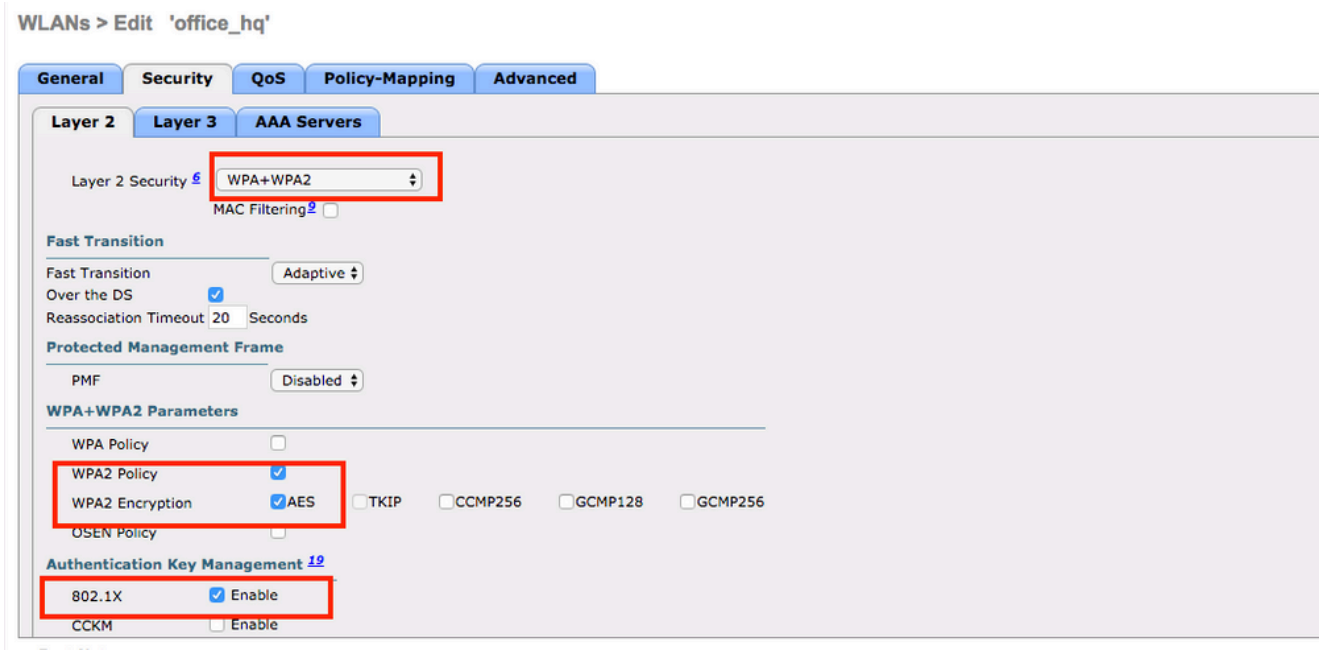
1. Configurez ISE en tant que serveur d'authentification RADIUS sur WLC. Accédez à laSecurity > AAA > RADIUS > Authenticationsection de l'interface utilisateur Web et fournissez l'adresse IP ISE et les informations secrètes partagées.

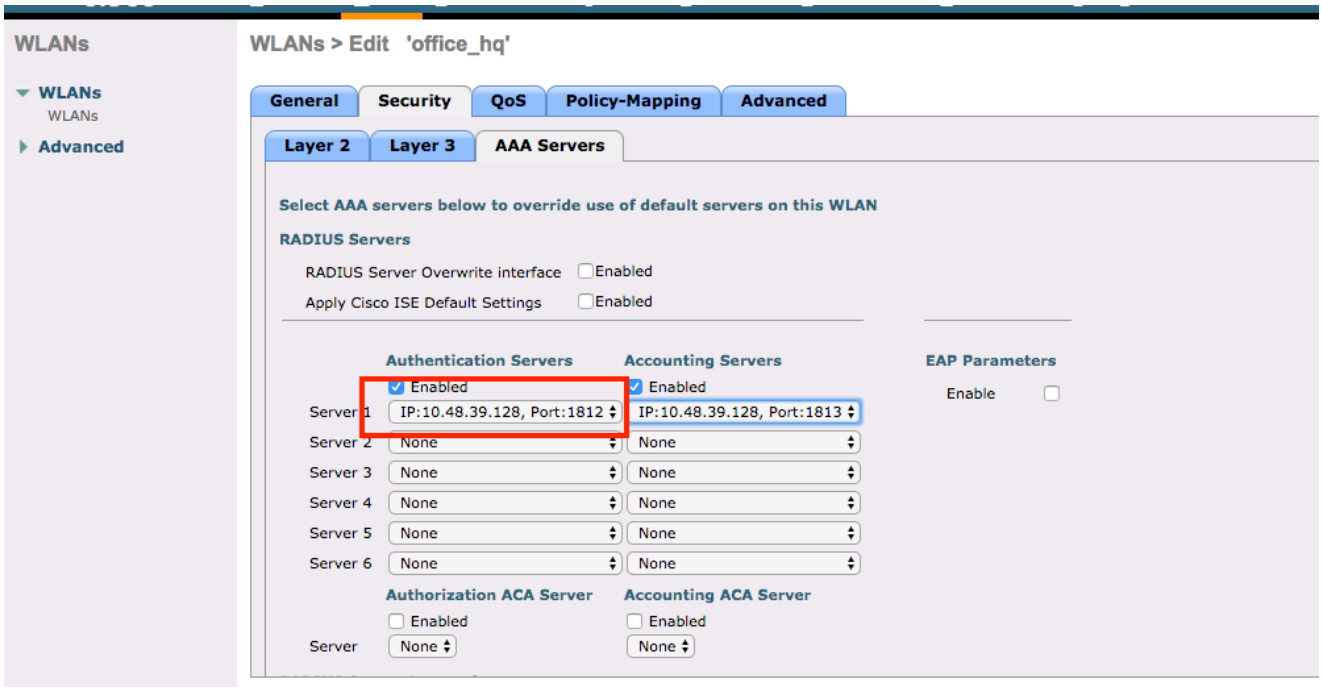


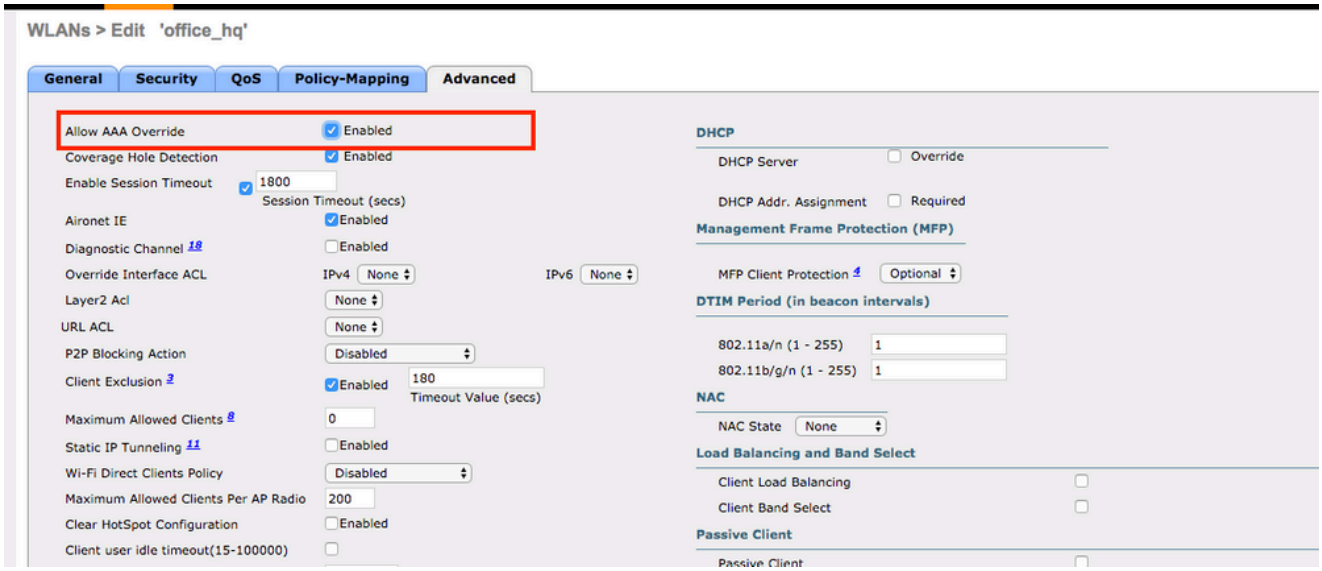
2. Configurez SSIDoffice_hqsous la sectionWLANssur le WLC ; cet exemple configure SSID avecWPA2/AES+dot1xet AAA override. L'interfaceDummyest choisie pour le WLAN puisque le VLAN approprié est attribué de toute façon via RADIUS. Cette interface fictive doit être créée sur le WLC et recevoir une adresse IP, mais l'adresse IP ne doit pas être valide et le VLAN dans lequel elle est placée ne peut pas être créé dans le commutateur de liaison ascendante de sorte que si aucun VLAN n'est attribué, le client ne peut aller nulle part.



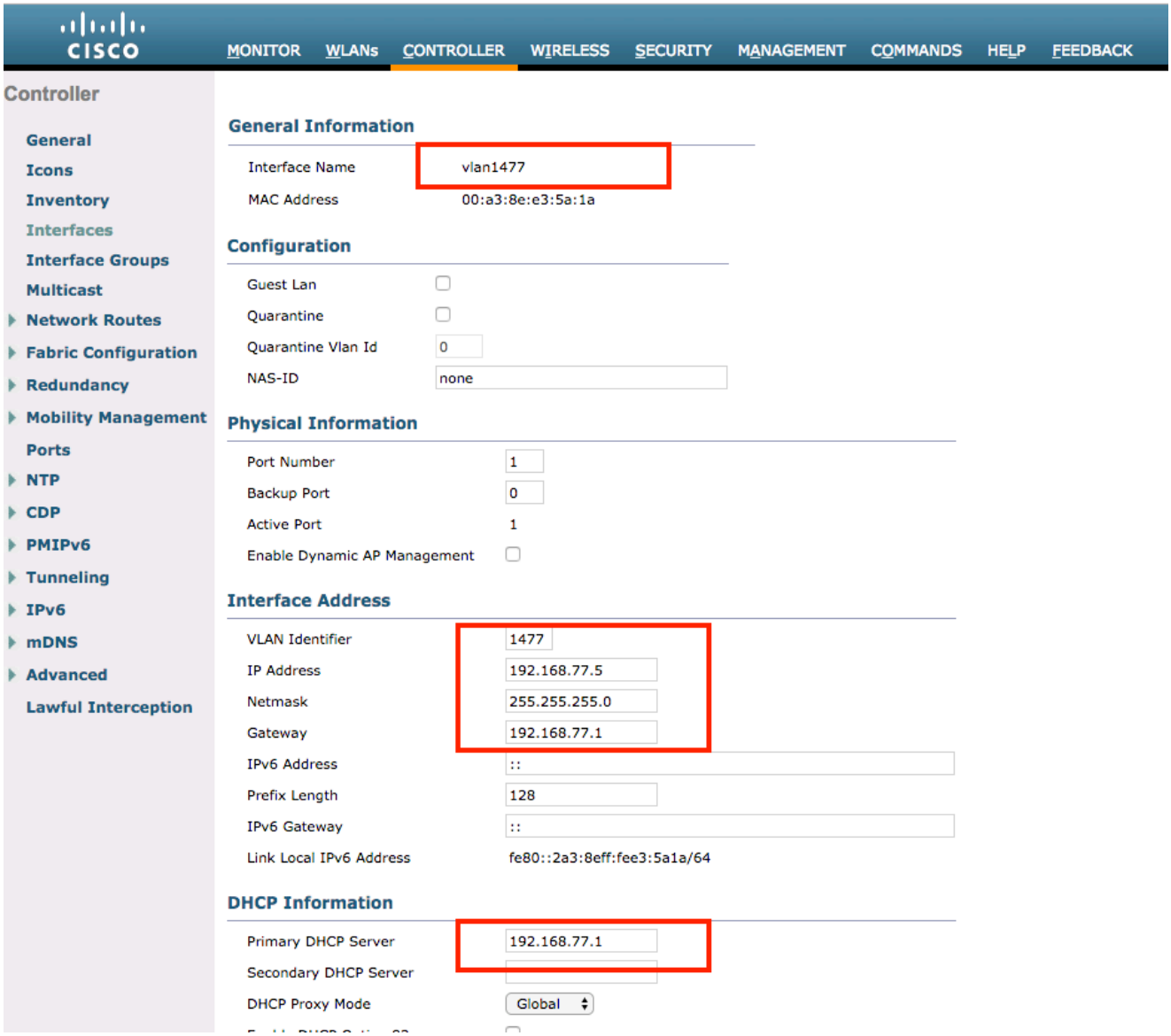

WLANs > Edit 'office_hq'
General
Security
QoS
Policy-Mapping
Advanced
Profile Name
office_hq
Type
WLAN
SSID
office_hq
Status
Enabled
Security Policies
[WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)
Radio Policy
All
Interface/Interface Group(G
dummy
Multicast Vlan Feature
Enabled
Broadcast SSID
Enabled
NAS-ID
none


WLANs > Edit 'office_hq'
General
Security
QoS
Policy-Mapping
Advanced
Layer 2
Layer 3
AAA Servers
Layer 2 Security
WPA+WPA2
MAC Filtering
Fast Transition
Fast Transition
Adaptive
Over the DS
Reassociation Timeout
20
Seconds
Protected Management Frame
PMF
Disabled
WPA+WPA2 Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption
AES
TKIP
CCMP256
GCMP128
GCMP256
OSEN Policy
Authentication Key Management
802.1X
Enable
CCKM
Enable





3. Vous devez également créer des interfaces dynamiques sur le WLC pour les VLAN utilisateur. Accédez au menuController > Interfacesde l'interface utilisateur. Le WLC ne peut honorer l'affectation de VLAN reçue via AAA que s'il a une interface dynamique dans ce VLAN.



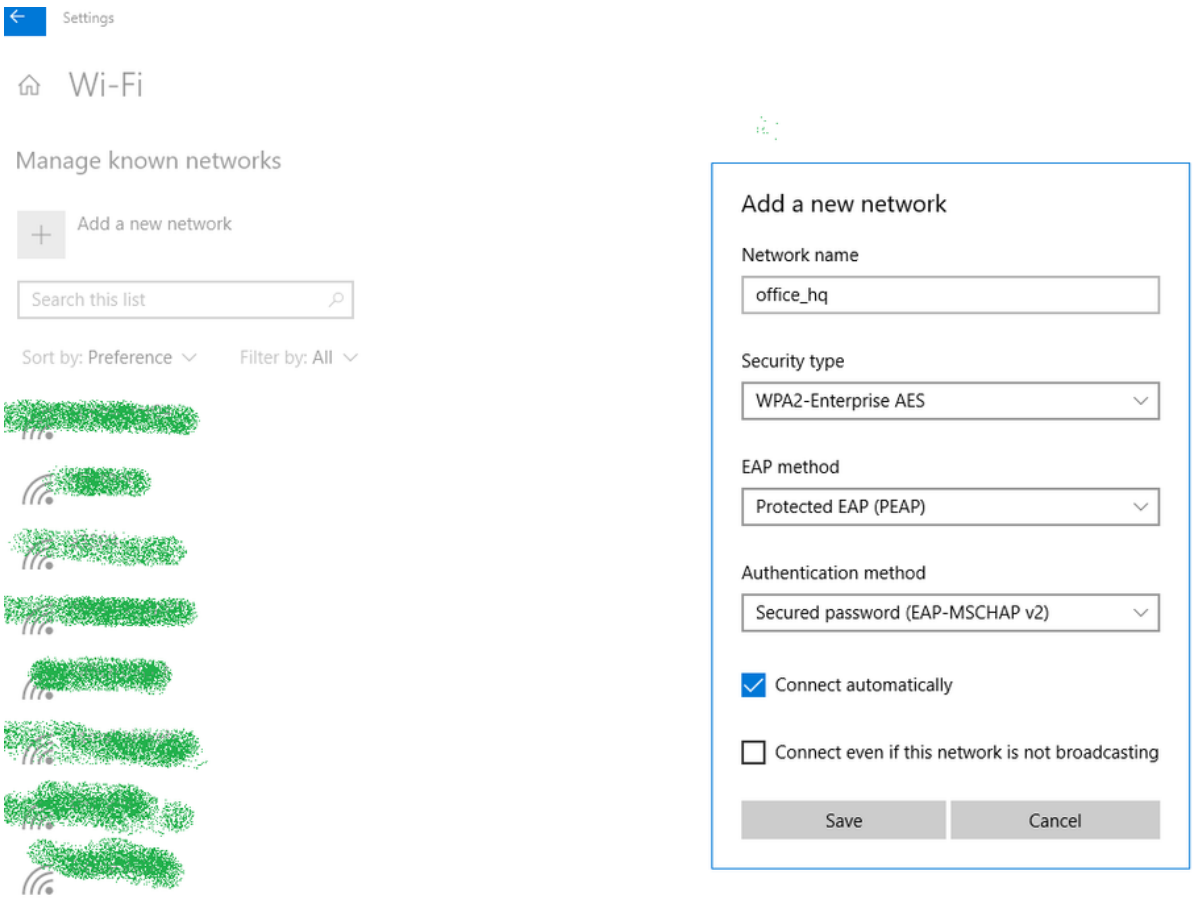
Vérifier

Utilisez le demandeur natif Windows 10 et Anyconnect NAM afin de tester les connexions.

Étant donné que vous utilisez l'authentification EAP-PEAP et qu'ISE utilise un certificat auto-signé (SSC), vous devez accepter un avertissement de certificat ou désactiver la validation de certificat. Dans un environnement d'entreprise, vous devez utiliser un certificat signé et approuvé sur ISE et vous assurer que les périphériques des utilisateurs finaux disposent du certificat racine approprié installé sous la liste Autorités de certification approuvées.

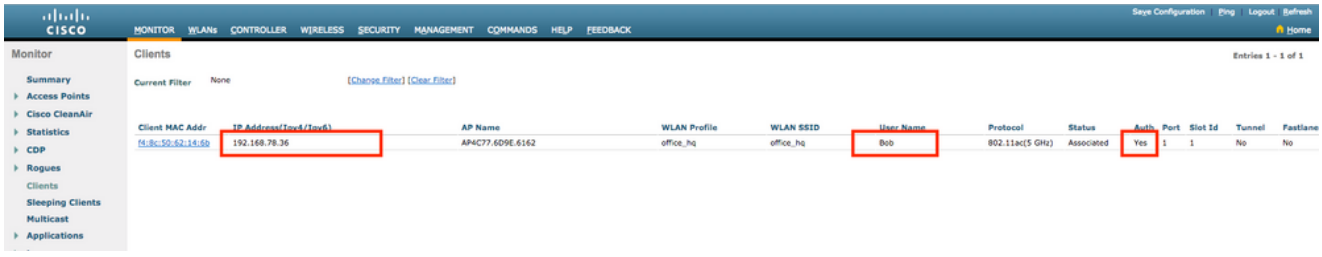
Testez la connexion avec Windows 10 et le demandeur natif :

1. OuvrezNetwork & Internet settings > Wi-Fi > Manage known networksetcréez un nouveau profil réseau en appuyant sur leAdd new networkbouton ; complétez les informations requises.



2. Vérifiez le journal d'authentification sur ISE et assurez-vous que le profil approprié est sélectionné pour l'utilisateur.

3. Vérifiez l'entrée du client sur le WLC et assurez-vous qu'il est assigné au bon VLAN et est dans l'état RUN.



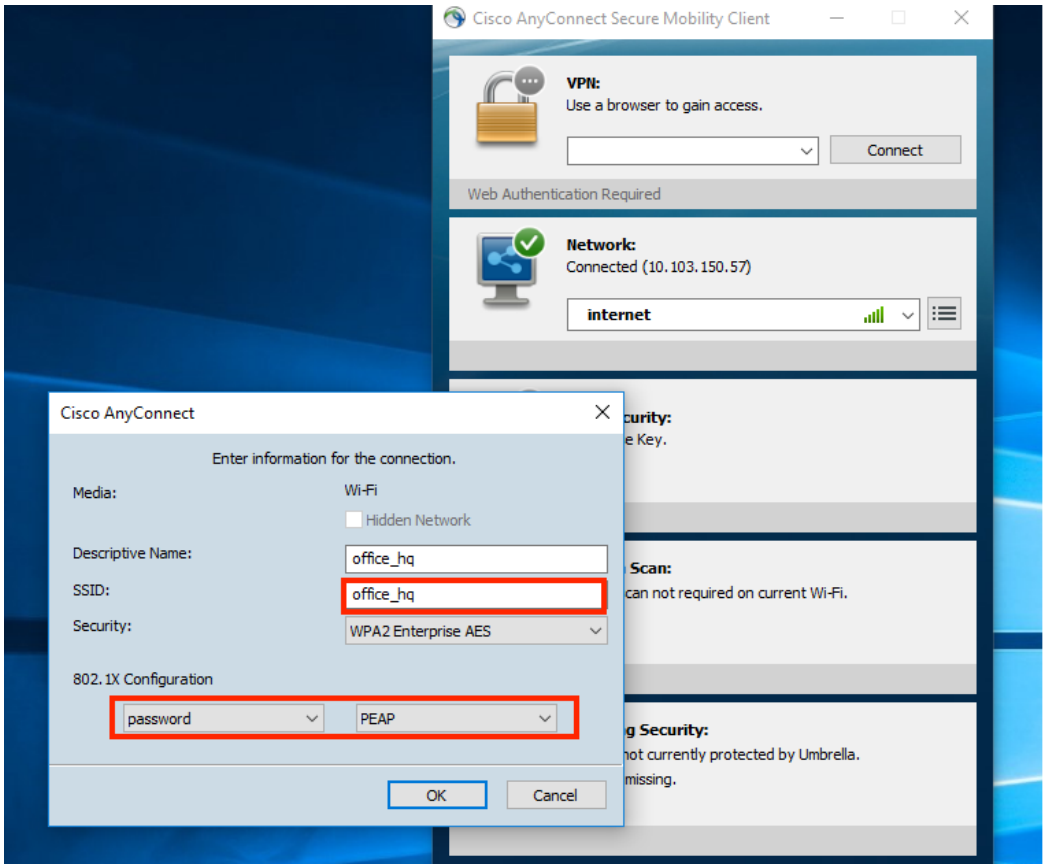
4. À partir de l'ILC WLC, l'état du client peut être vérifié avec leshow client dertails :

```
show client detail f4:8c:50:62:14:6b
Client MAC Address.............................. f4:8c:50:62:14:6b
Client Username ................................ Bob
```

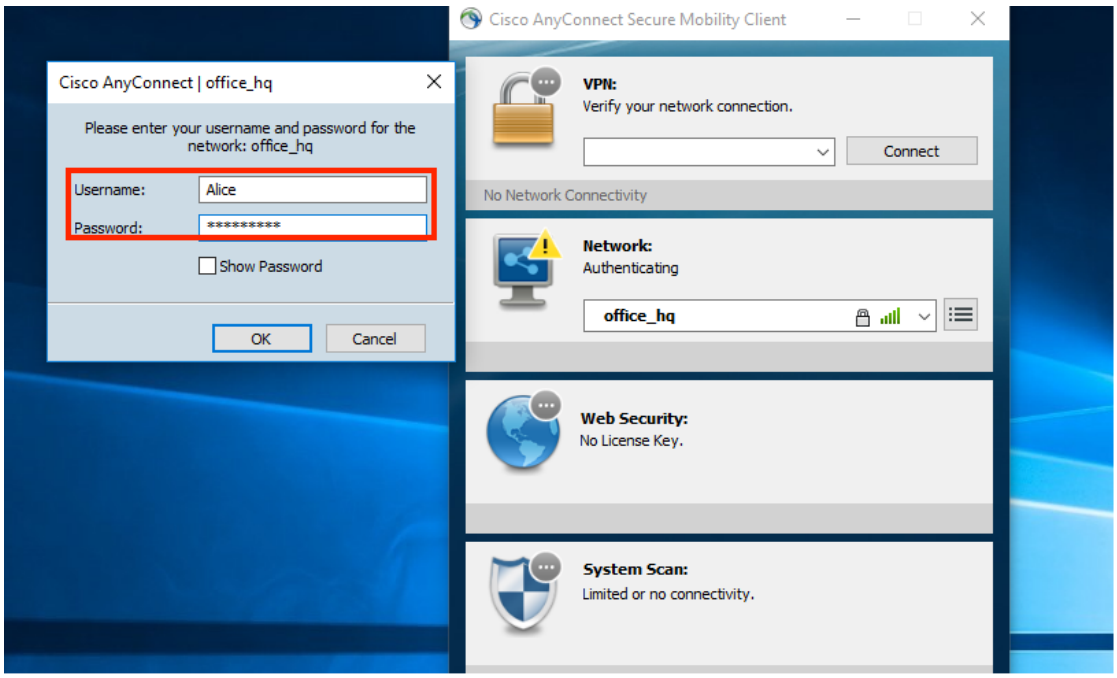
```
Client Webauth Username ..... N/A
Hostname: .....
Device Type: ..... Intel-Device
AP MAC Address..... 70:69:5a:51:4e:c0
AP Name..... AP4C77.6D9E.6162
AP radio slot Id..... 1
Client State..... Associated
User Authenticated by ..... RADIUS Server
Client User Group..... Bob
Client NAC OOB State..... Access
Wireless LAN Id..... 3
Wireless LAN Network Name (SSID)..... office_hq
Wireless LAN Profile Name..... office_hq
Hotspot (802.11u)..... Not Supported
Connected For ..... 242 secs
BSSID..... 70:69:5a:51:4e:cd
Channel..... 36
IP Address..... 192.168.78.36
Gateway Address..... 192.168.78.1
Netmask..... 255.255.255.0
...
Policy Manager State..... RUN
...
EAP Type..... PEAP
Interface..... vlan1478
VLAN..... 1478
Quarantine VLAN..... 0
Access VLAN..... 1478
```

Testez la connexion avec Windows 10 et Anyconnect NAM :

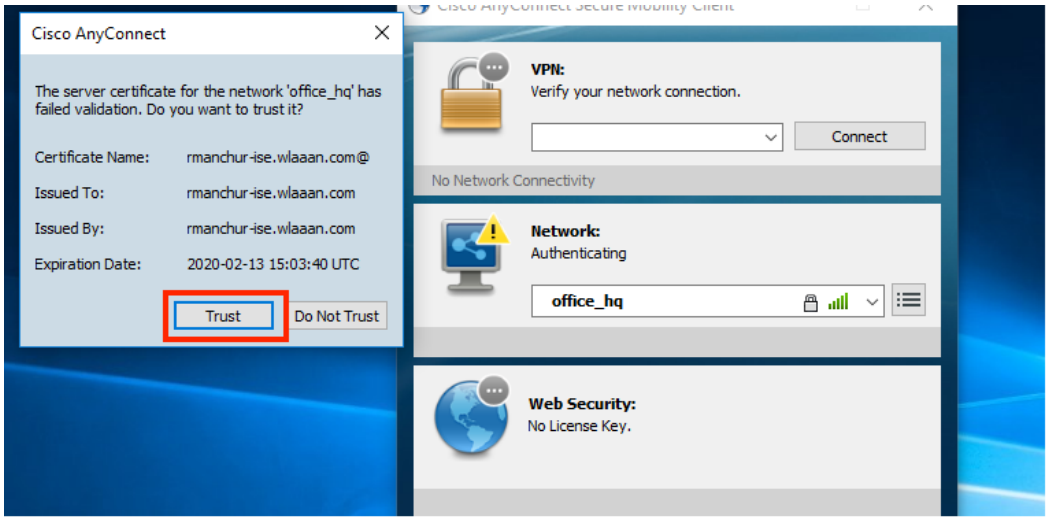
1. Choisissez le SSID dans la liste SSID disponibles et le type d'authentification EAP respectif (dans cet exemple PEAP) et le formulaire d'authentification interne.



2. Fournissez un nom d'utilisateur et un mot de passe pour l'authentification utilisateur.

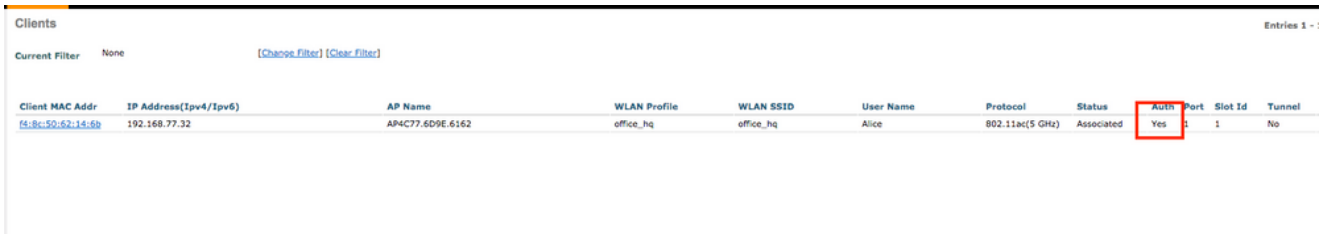


3. Étant donné qu'ISE envoie un SSC au client, vous devez choisir manuellement d'approuver le certificat (dans l'environnement de production, il est fortement recommandé d'installer le certificat approuvé sur ISE).



4. Vérifiez les journaux d'authentification sur ISE et assurez-vous que le profil d'autorisation approprié est sélectionné pour l'utilisateur.

5. Vérifiez l'entrée du client sur le WLC et assurez-vous qu'il est assigné au bon VLAN et est dans l'état RUN.



6. À partir de l'ILC WLC, l'état du client peut être vérifié avec leshow client dertails :

```
Client MAC Address.............................. f4:8c:50:62:14:6b
Client Username ................................ Alice
Client Webauth Username ........................ N/A
Hostname: ......................................
Device Type: ................................... Intel-Device
AP MAC Address.................................. 70:69:5a:51:4e:c0
AP Name......................................... AP4C77.6D9E.6162
AP radio slot Id................................ 1
```

```
Client State..................................... Associated
User Authenticated by ........................... RADIUS Server
Client User Group................................ Alice
Client NAC OOB State............................. Access
Wireless LAN Id.................................. 3
Wireless LAN Network Name (SSID)................. office_hq
Wireless LAN Profile Name........................ office_hq
Hotspot (802.11u)................................ Not Supported
Connected For ................................... 765 secs
BSSID............................................ 70:69:5a:51:4e:cd
Channel.......................................... 36
IP Address....................................... 192.168.77.32
Gateway Address.................................. 192.168.77.1
Netmask.......................................... 255.255.255.0
...
Policy Manager State............................. RUN
...
Policy Type...................................... WPA2
Authentication Key Management.................... 802.1x
Encryption Cipher................................ CCMP-128 (AES)
Protected Management Frame ...................... No
Management Frame Protection...................... No
EAP Type......................................... PEAP
Interface........................................ vlan1477
VLAN............................................. 1477
```

Dépannage

1. Utilisez la`test aaa radius username`

   `password`

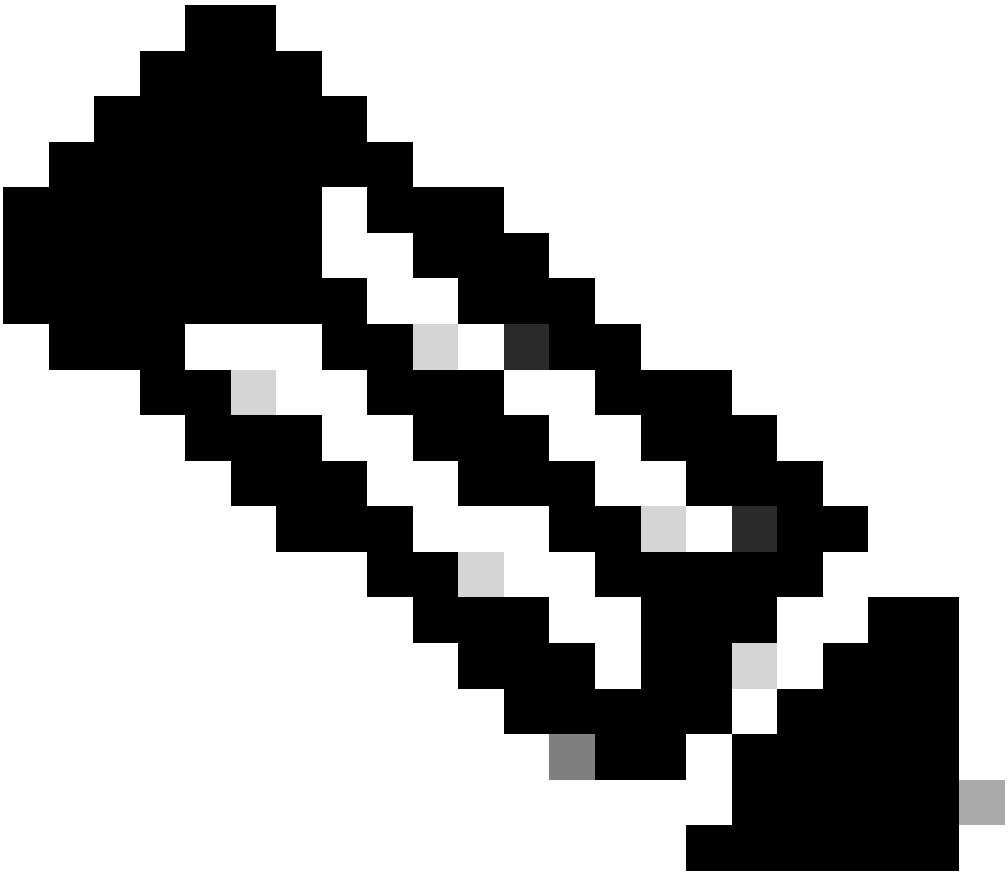
   `wlan-id`

   afin de tester la connexion RADIUS entre WLC et ISE et la`test aaa show radius`afin d'afficher les résultats.

```
test aaa radius username Alice password <removed> wlan-id 2

Radius Test Request
  Wlan-id.......................................... 2
  ApGroup Name..................................... none

  Attributes                    Values
  ----------                    ------
  User-Name                     Alice
  Called-Station-Id             00-00-00-00-00-00:AndroidAP
  Calling-Station-Id            00-11-22-33-44-55
  Nas-Port                      0x00000001 (1)
```

```
  Nas-Ip-Address                  10.48.71.20
  NAS-Identifier                  0x6e6f (28271)
  Airespace / WLAN-Identifier     0x00000002 (2)
  User-Password                   cisco!123
  Service-Type                    0x00000008 (8)
  Framed-MTU                      0x00000514 (1300)
  Nas-Port-Type                   0x00000013 (19)
  Cisco / Audit-Session-Id        1447300a0000003041d5665c
  Acct-Session-Id                 5c66d541/00:11:22:33:44:55/743


test radius auth request successfully sent. Execute 'test aaa show radius' for response

(Cisco Controller) >test aaa show radius

Radius Test Request
  Wlan-id..................................... 2
  ApGroup Name................................ none
Radius Test Response

Radius Server            Retry Status
-------------            ----- ------
10.48.39.128             1     Success

Authentication Response:
  Result Code: Success

  Attributes                      Values
  ----------                      ------
  User-Name                       Alice
  State                           ReauthSession:1447300a0000003041d5665c
  Class                           CACS:1447300a0000003041d5665c:rmanchur-ise/339603379/59
  Tunnel-Type                     0x0000000d (13)
  Tunnel-Medium-Type              0x00000006 (6)
  Tunnel-Group-Id                 0x000005c5 (1477)


(Cisco Controller) >
```

2. Utilisez la debug client
   afin de dépanner les problèmes de connectivité du client sans fil.
3. Utilisez ladebug aaa all enableafin de dépanner les problèmes d'authentification et d'autorisation sur le WLC.



Remarque : utilisez cette commande uniquement avec le`debug mac addr`afin de limiter la sortie basée sur l'adresse MAC pour laquelle le débogage est effectué.

4. Référez-vous aux journaux en direct ISE et aux journaux de session afin d'identifier les problèmes d'échecs d'authentification et les problèmes de communication AD.

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.