Configurer PEAP et EAP-FAST avec ACS 5.2 et WLC

Table des matières

Introduction

Ce document explique comment configurer le contrôleur LAN sans fil (WLC) pour l'authentification EAP (Extensible Authentication Protocol) en utilisant un serveur RADIUS externe tel que le serveur de contrôle d'accès (ACS) 5.2.

Conditions préalables

Exigences

Assurez-vous que vous remplissez les conditions suivantes avant d'essayer cette configuration :

- Avoir une connaissance de base du WLC et des points d'accès légers (LAP)
- Avoir une connaissance fonctionnelle du serveur AAA
- Connaître parfaitement les réseaux sans fil et les problèmes de sécurité sans fil

Composants utilisés

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

- WLC Cisco 5508 exécutant la version de microprogramme 7.0.220.0
- LAP de la gamme Cisco 3502
- Supplicant natif Microsoft Windows 7 avec pilote Intel 6300-N version 14.3
- Cisco Secure ACS exécutant la version 5.2
- Commutateur de la série Cisco 3560

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. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

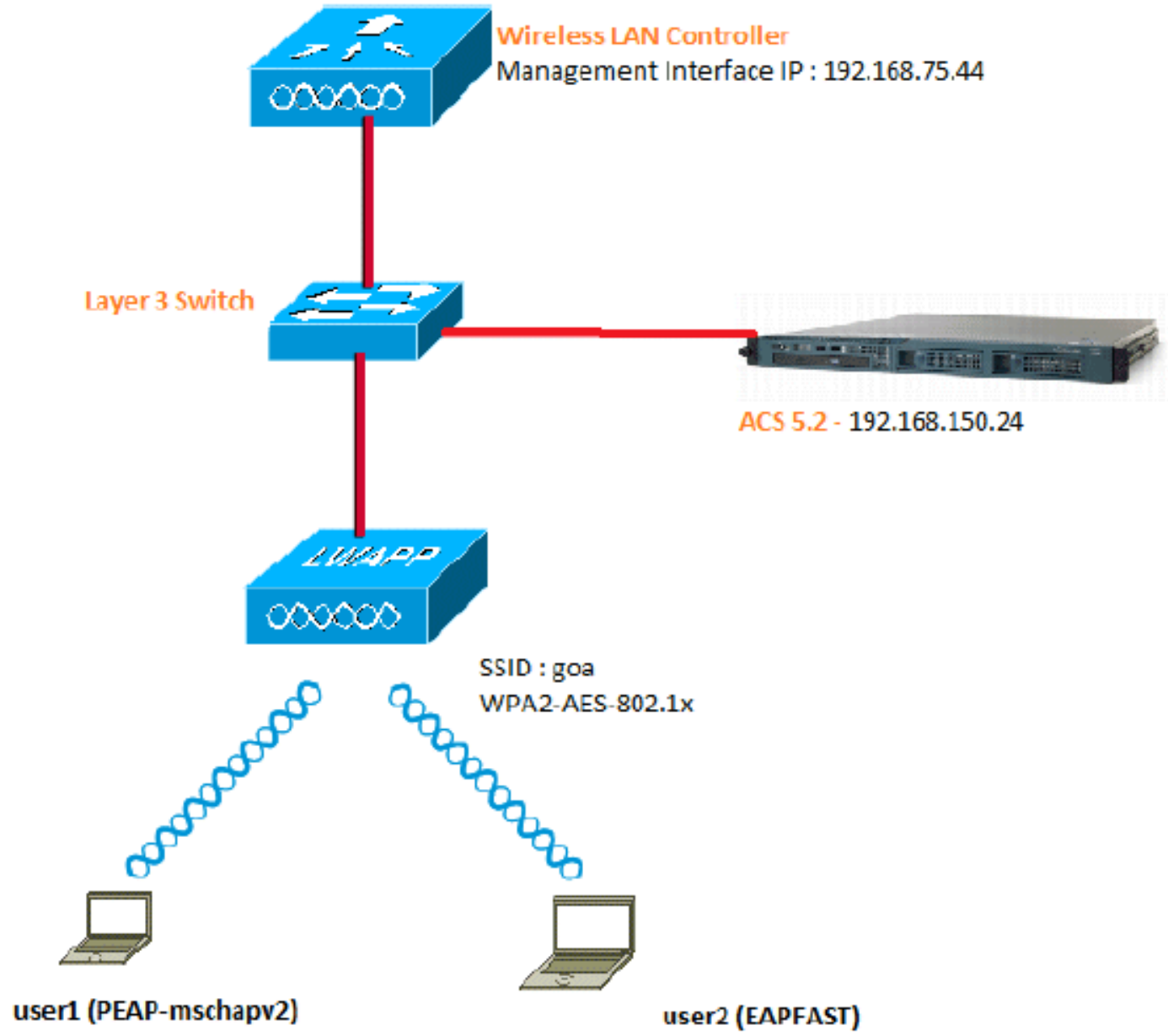
Configurer

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



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

- L'adresse IP du serveur ACS (RADIUS) est 192.168.150.24.
- L'adresse d'interface de gestion et de gestionnaire AP du WLC est 192.168.75.44.
- L'adresse des serveurs DHCP est 192.168.150.25.
- Le VLAN 253 est utilisé tout au long de cette configuration. Les deux utilisateurs se connectent au même SSID « goa ». Cependant, user1 est configuré pour s'authentifier à l'aide de PEAP-MSCHAPv2 et user2 à l'aide de EAP-FAST.
- Les utilisateurs seront affectés au VLAN 253 :VLAN 253 : 192.168.153.x/24. Passerelle : 192.168.153.1VLAN 75 : 192.168.75.x/24. Passerelle : 192.168.75.1

Hypothèses

- Les commutateurs sont configurés pour tous les VLAN de couche 3.
- Une étendue DHCP est attribuée au serveur DHCP.
- La connectivité de couche 3 existe entre tous les périphériques du réseau.
- Le LAP est déjà joint au WLC.
- Chaque VLAN possède le masque /24.

- Un certificat auto-signé est installé sur ACS 5.2.

Configuration Steps

Cette configuration est divisée en trois étapes de haut niveau :

1. Configurez le serveur RADIUS.
2. Configurer le WLC.
3. Configurer l'utilitaire client sans fil

Configuration du serveur RADIUS

La configuration du serveur RADIUS se divise en quatre étapes :

1. Configurer les ressources réseau
2. Configurer les utilisateurs.
3. Définir des éléments de stratégie.
4. Appliquer des stratégies d'accès

ACS 5.x est un système de contrôle d'accès basé sur des politiques. En d'autres termes, ACS 5.x utilise un modèle de stratégie basé sur des règles au lieu du modèle basé sur des groupes utilisé dans les versions 4.x.

Le modèle de politique basé sur des règles ACS 5.x offre un contrôle d'accès plus puissant et plus flexible que l'ancienne approche basée sur des groupes.

Dans l'ancien modèle basé sur les groupes, un groupe définit une stratégie car il contient et lie trois types d'informations :

- Informations d'identité : ces informations peuvent être basées sur l'appartenance à des groupes AD ou LDAP ou sur une affectation statique pour les utilisateurs ACS internes.
- Autres restrictions ou conditions : restrictions temporelles, restrictions de périphérique, etc.
- Autorisations : VLAN ou niveaux de privilège Cisco IOS®.

Le modèle de stratégie ACS 5.x est basé sur des règles de la forme suivante :

- Si la condition se produit

Par exemple, nous utilisons les informations décrites pour le modèle basé sur les groupes :

- Si identity-condition, restriction-condition puis authorization-profile.

Par conséquent, cela nous donne la flexibilité de limiter dans quelles conditions l'utilisateur est autorisé à accéder au réseau ainsi que le niveau d'autorisation autorisé lorsque des conditions spécifiques sont remplies.

Configuration des ressources réseau

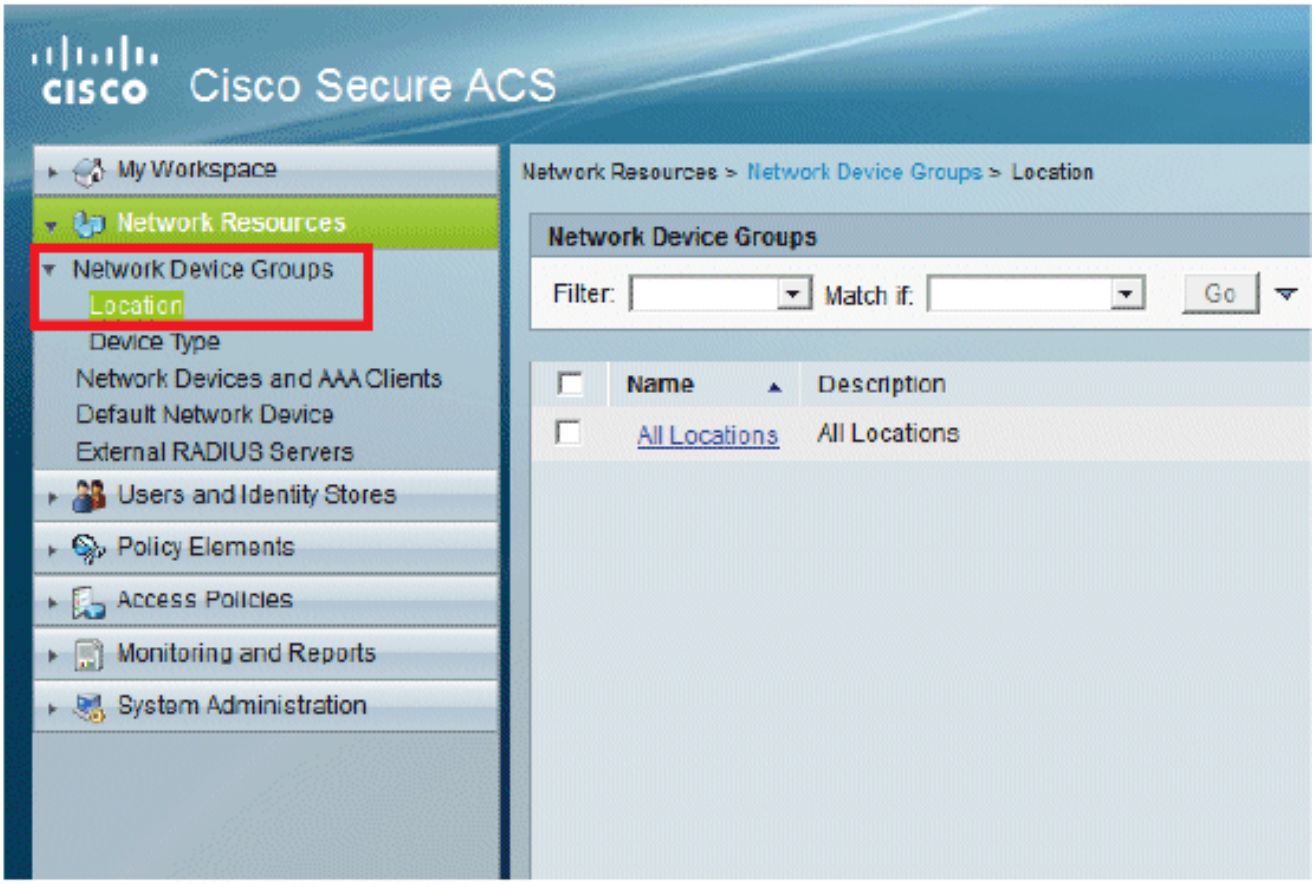
Dans cette section, nous configurons le client AAA pour le WLC sur le serveur RADIUS.

Cette procédure explique comment ajouter le WLC comme client AAA sur le serveur RADIUS de sorte que le WLC puisse passer les informations d'identification des utilisateurs au serveur

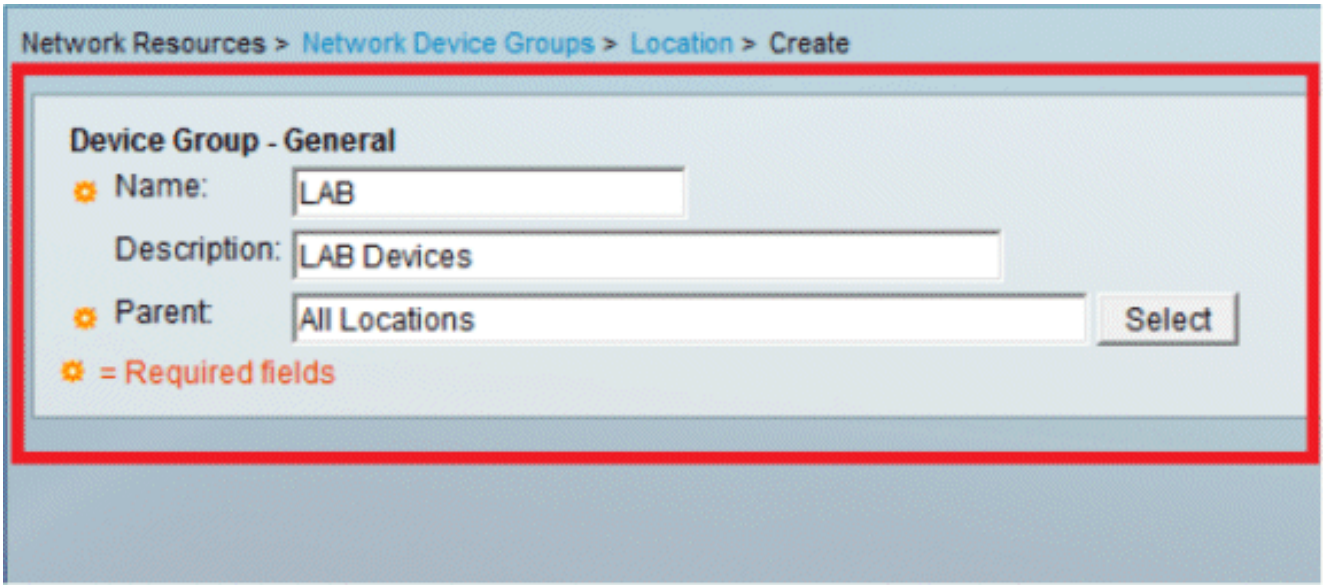
RADIUS.

Procédez comme suit :

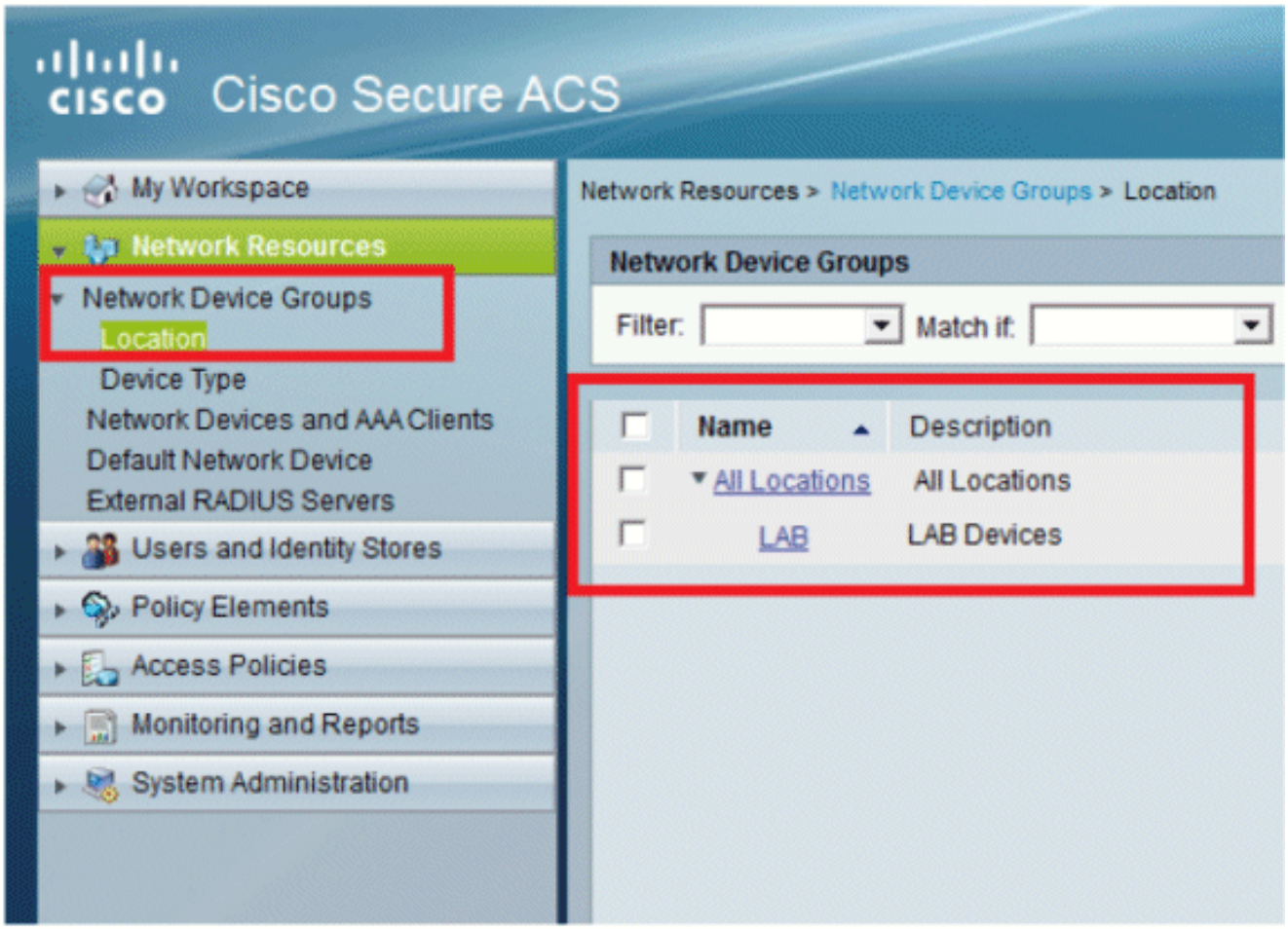
1. Dans l'interface graphique utilisateur d'ACS, accédez à **Network Resources > Network Device Groups > Location**, et cliquez sur **Create** (en bas de la page
).



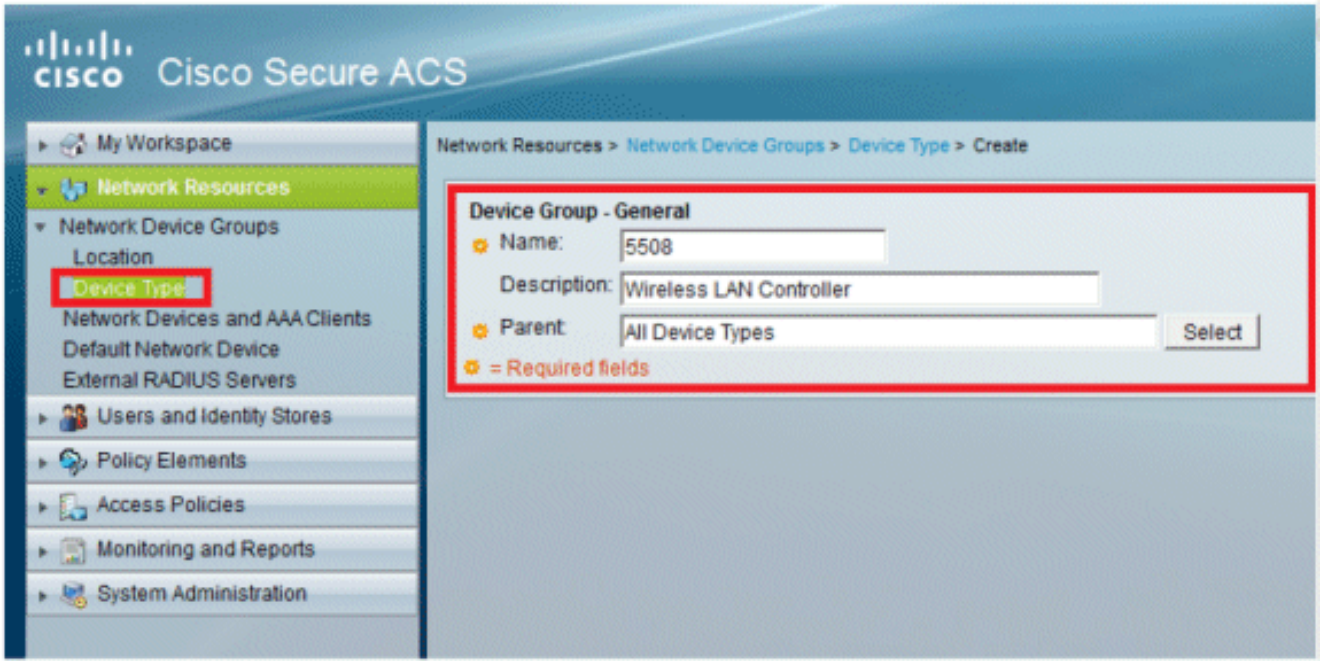
2. Ajoutez les champs requis, puis cliquez sur **Submit**.



   L'écran suivant s'affiche
   :

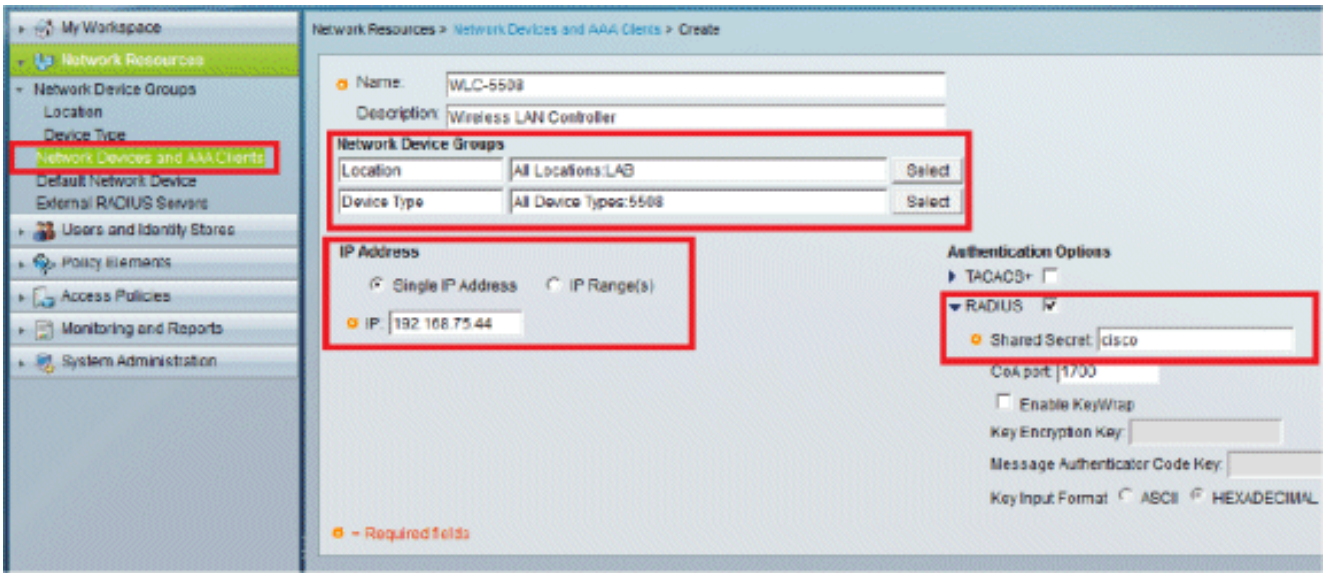


3. Cliquez sur **Device Type > Create**.

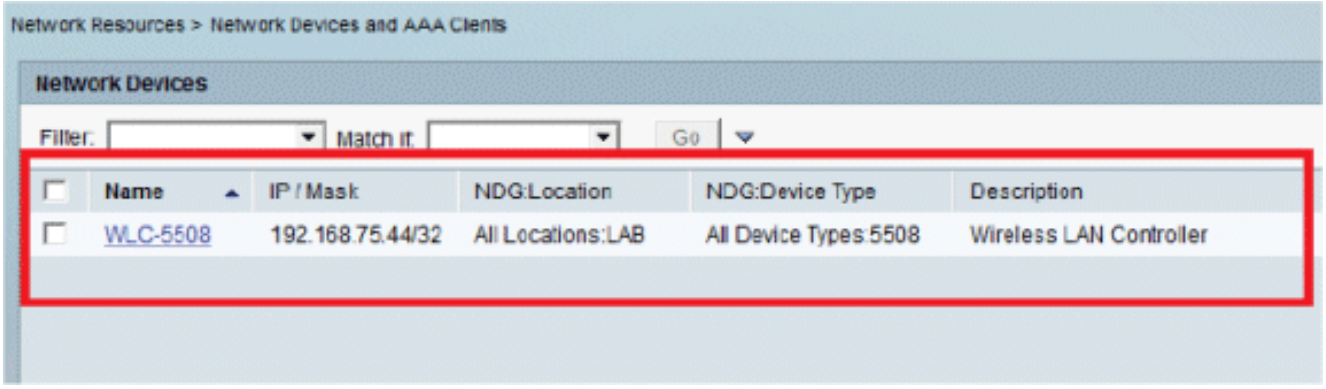


4. Cliquez sur Submit. L'écran suivant s'affiche :

5. Accédez à **Ressources réseau > Périphériques réseau et clients AAA**.
6. Cliquez sur **Create**, et remplissez les détails comme indiqué ici
:



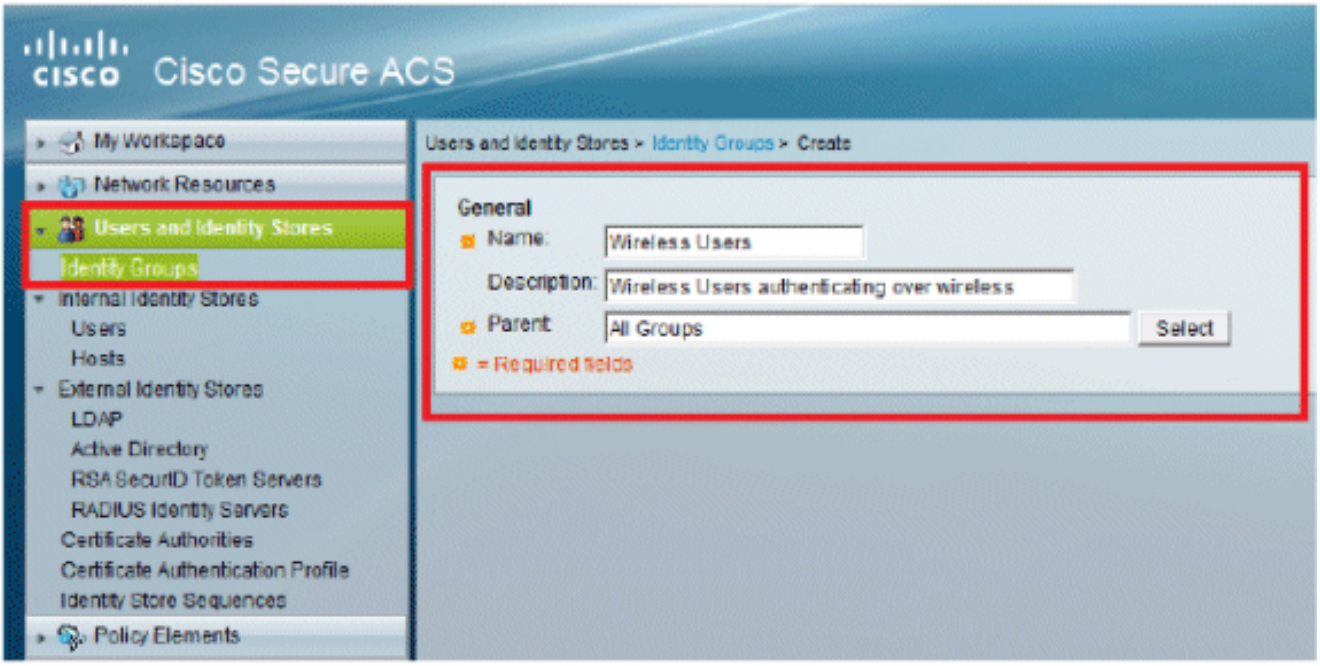
7. Cliquez sur Submit. L'écran suivant s'affiche
:



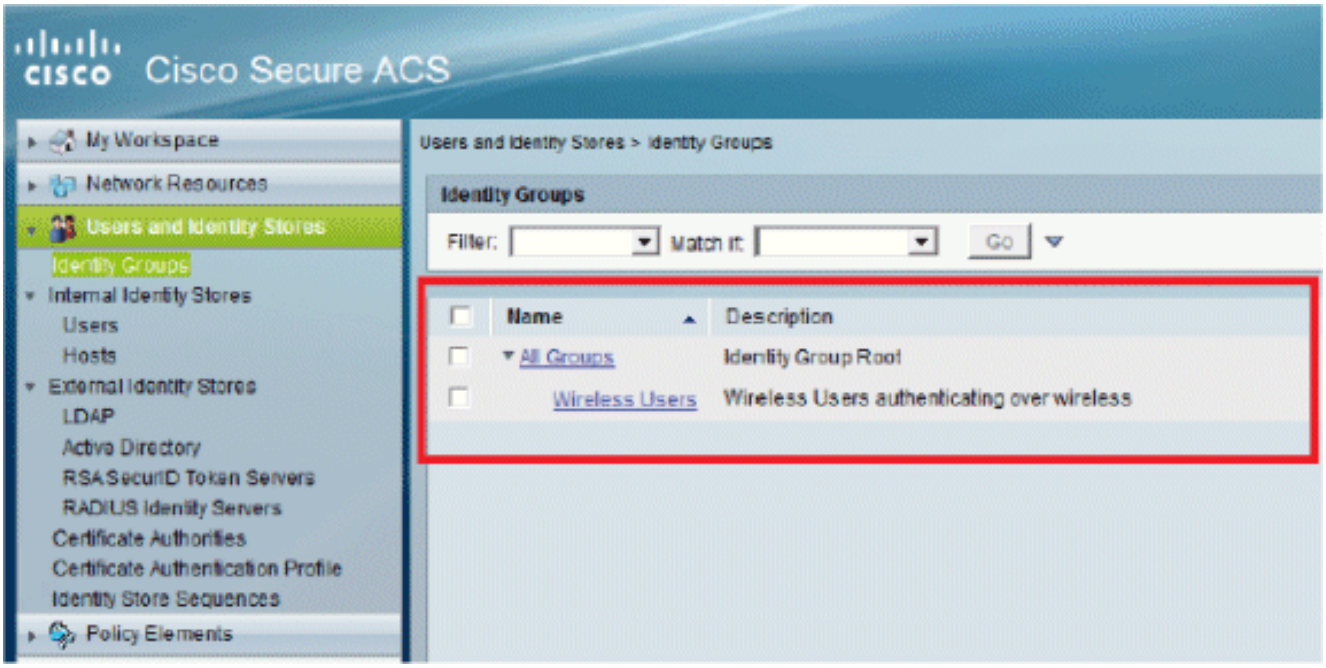
Configurer des utilisateurs

Dans cette section, nous allons créer des utilisateurs locaux sur ACS. Les deux utilisateurs (user1 et user2) sont affectés dans le groupe appelé « Utilisateurs sans fil ».

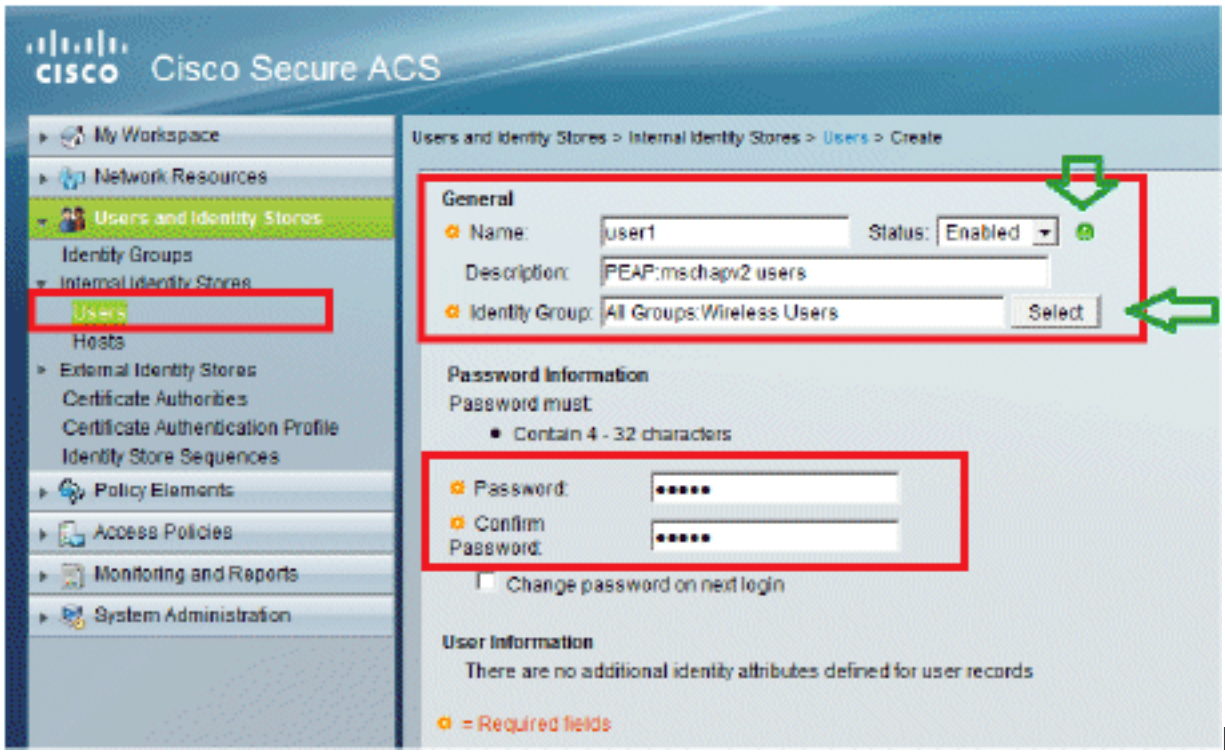
1. Accédez à **Utilisateurs et magasins d'identités > Groupes d'identités > Créer**.



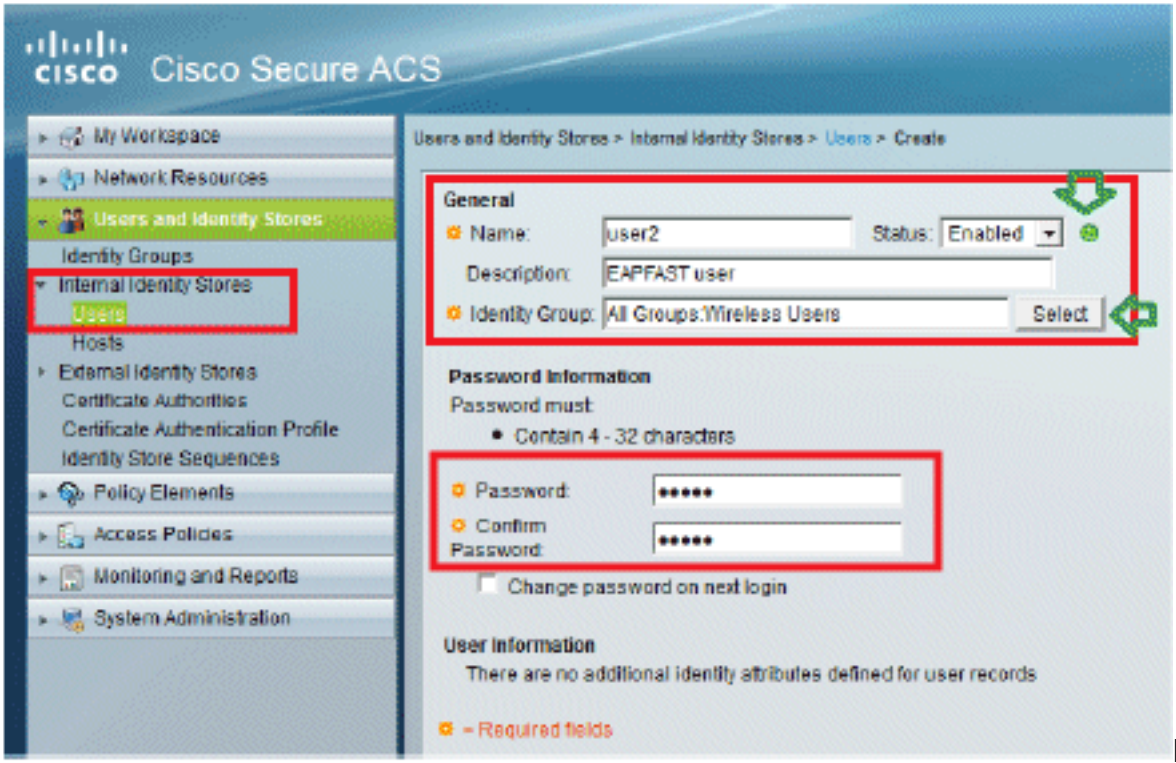
2. Une fois que vous avez cliqué sur **Submit**, la page ressemblera à ceci :



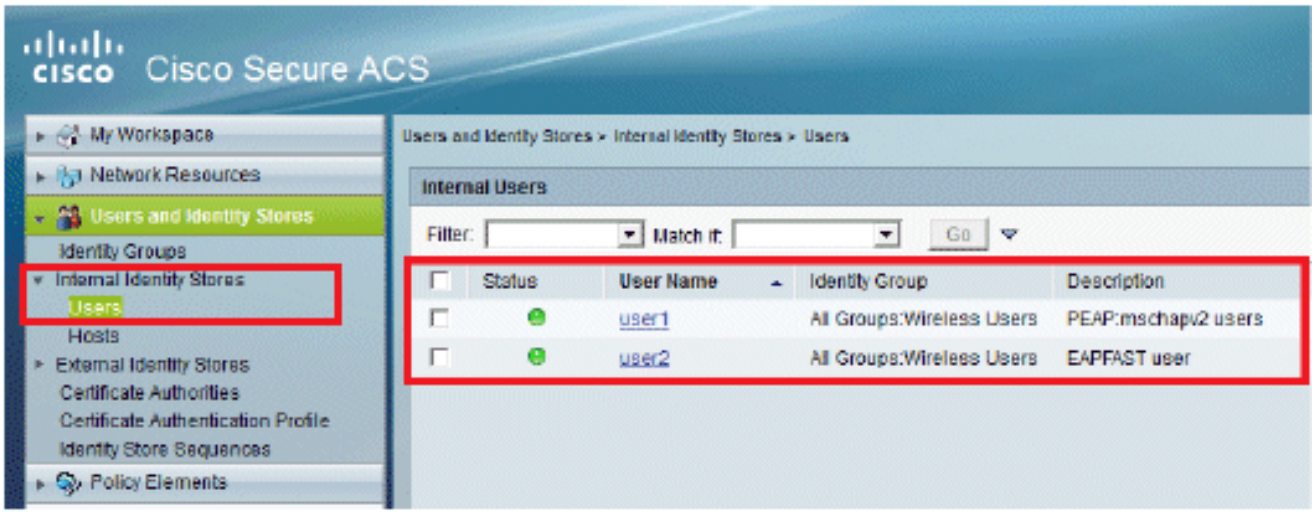
3. Créez les utilisateurs **user1** et **user2**, et attribuez-les au groupe « Utilisateurs sans fil ».Cliquez sur **Utilisateurs et magasins d'identités > Groupes d'identités > Utilisateurs > Créer**.



De même, créez user2.

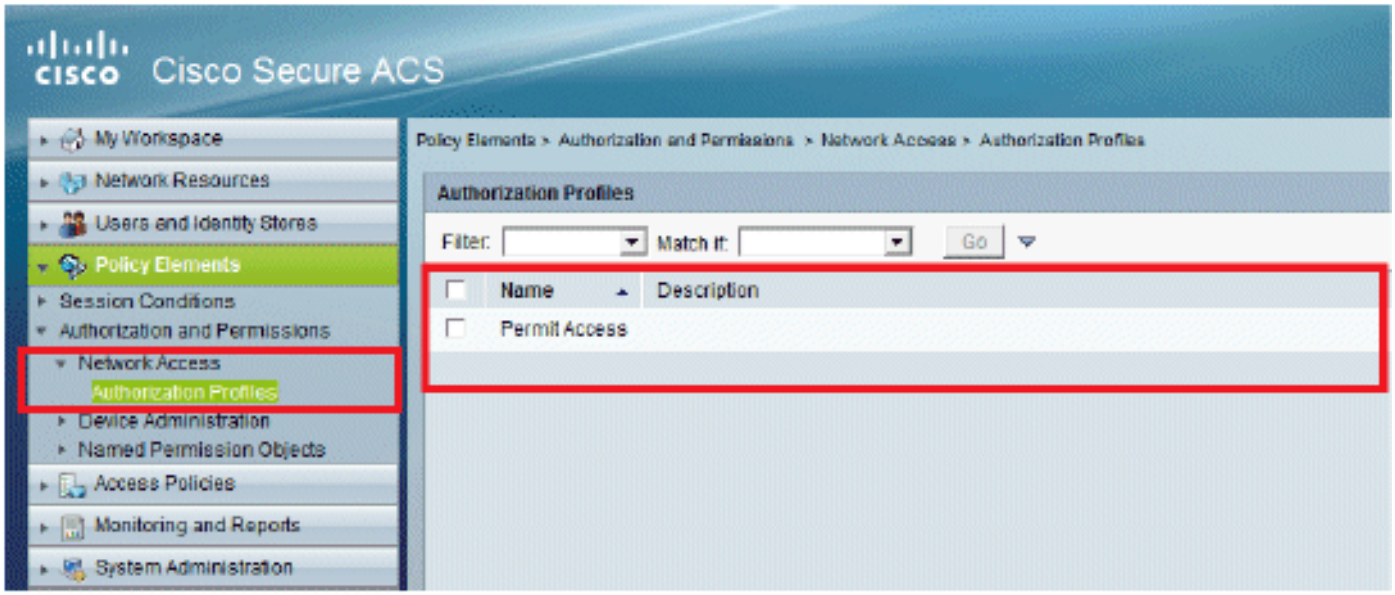


L'écran se présente comme suit :



Définir des éléments de stratégie

Vérifiez que **Permit Access** est défini.

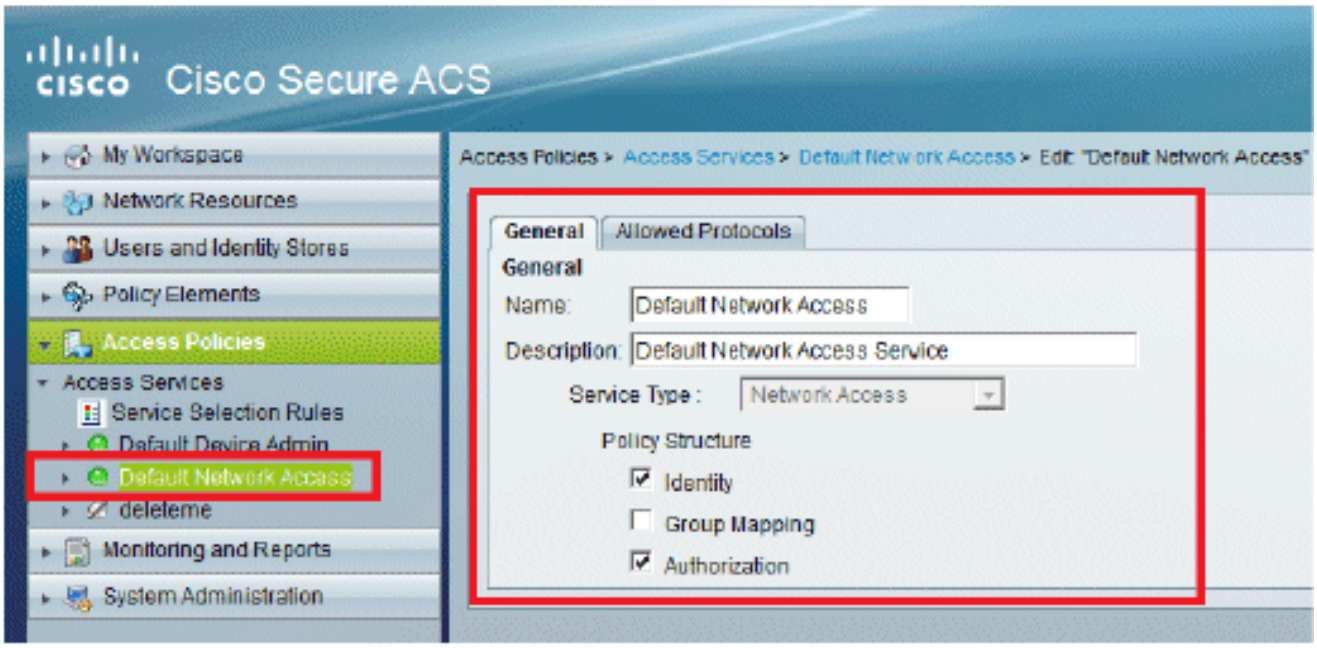


Appliquer les stratégies d'accès

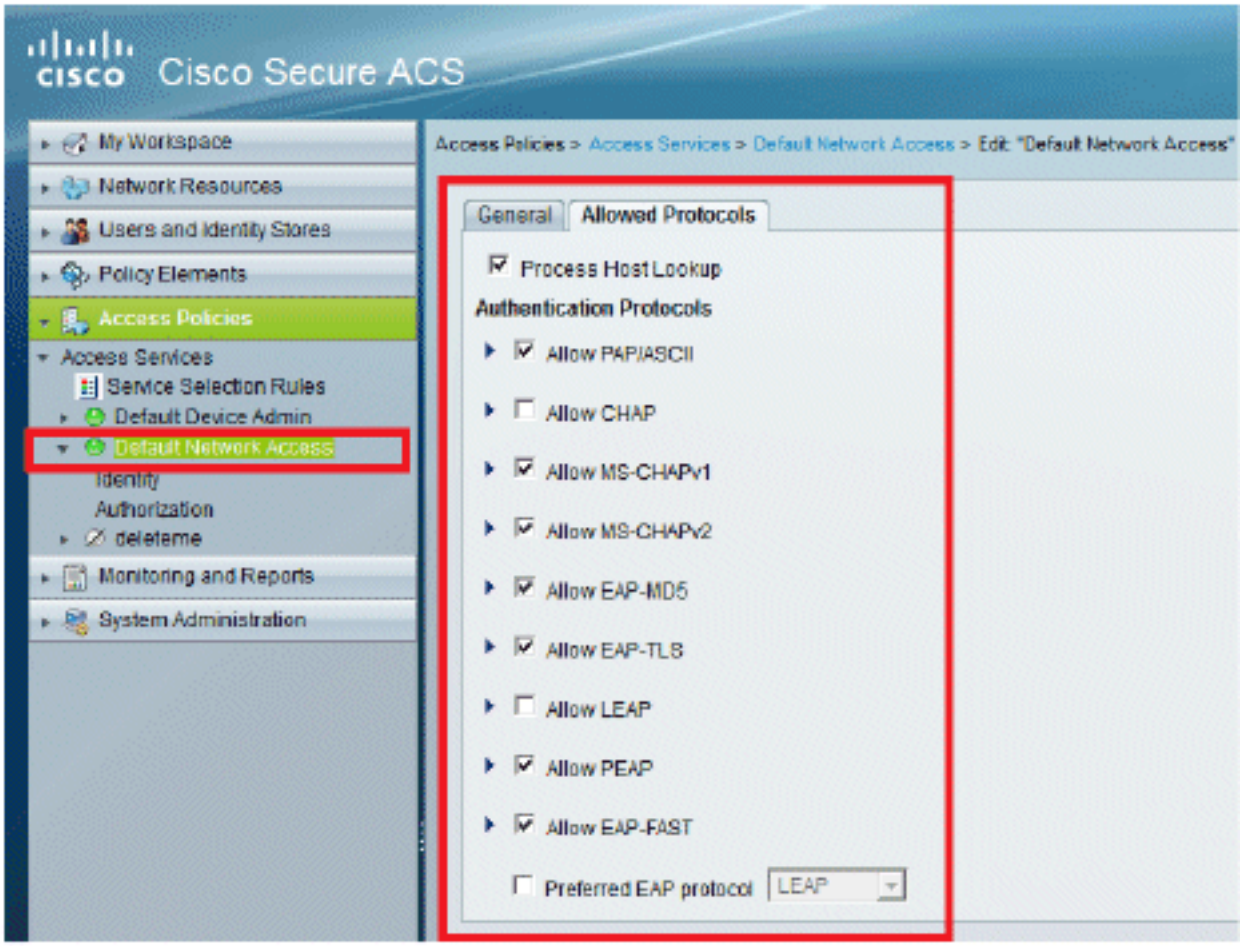
Dans cette section, nous allons sélectionner les méthodes d'authentification à utiliser et la manière dont les règles doivent être configurées. Nous allons créer des règles basées sur les étapes précédentes.

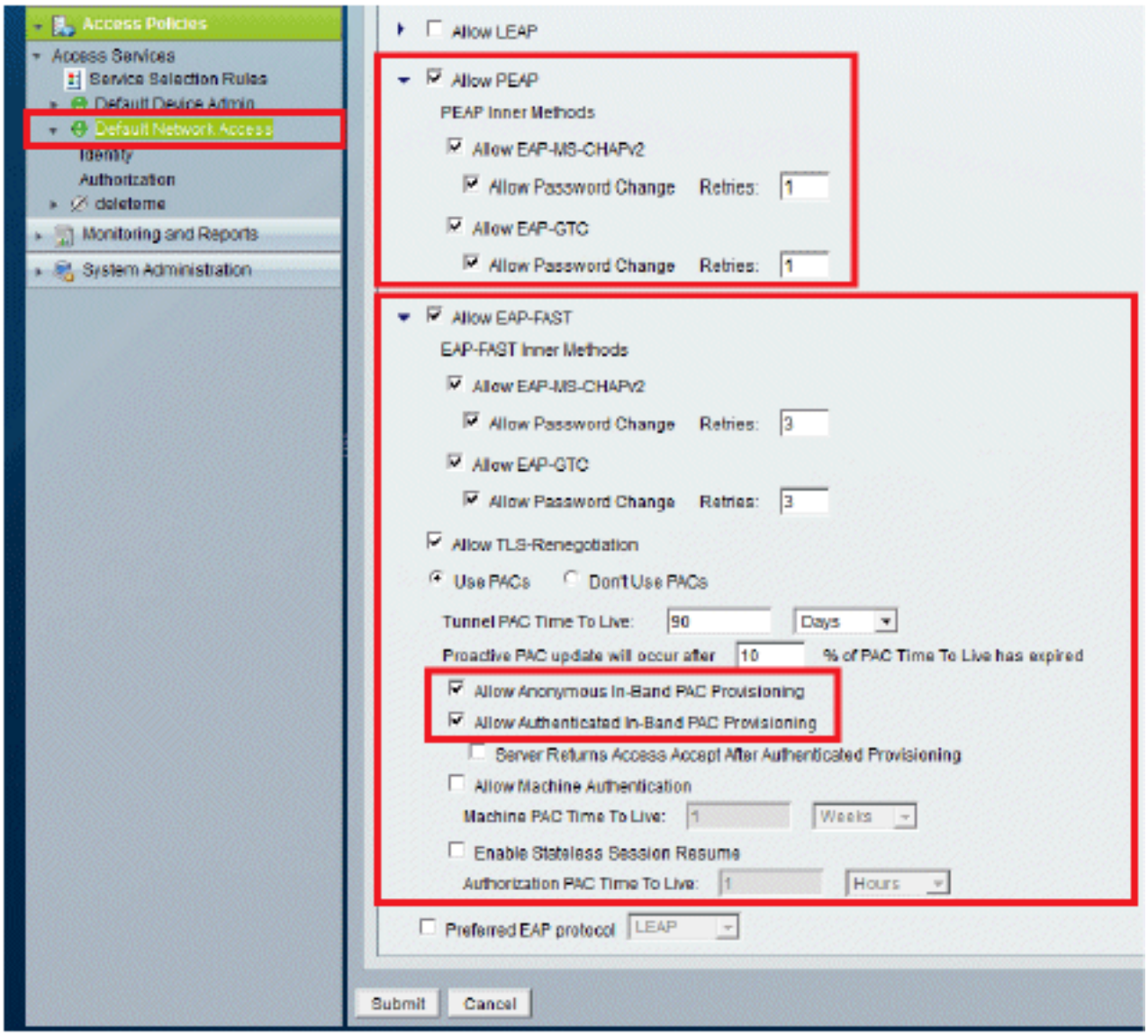
Procédez comme suit :

1. Accédez à **Politiques d'accès > Services d'accès > Accès réseau par défaut > Modifier : "Accès réseau par défaut"**.

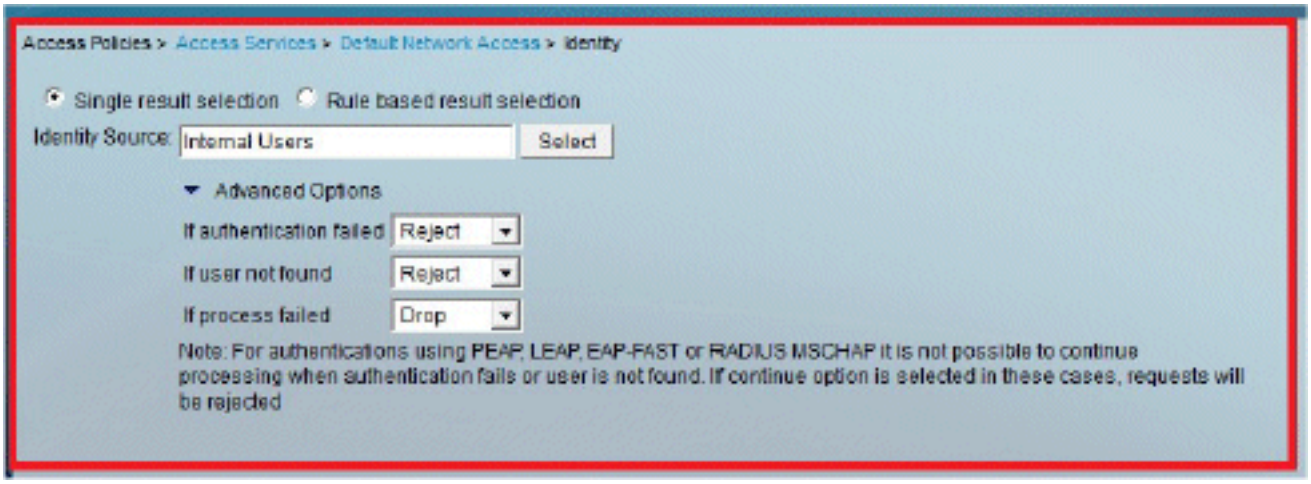


2. Sélectionnez la méthode EAP que vous souhaitez que les clients sans fil authentifient. Dans cet exemple, nous utilisons **PEAP- MSCHAPv2** et **EAP-FAST**.



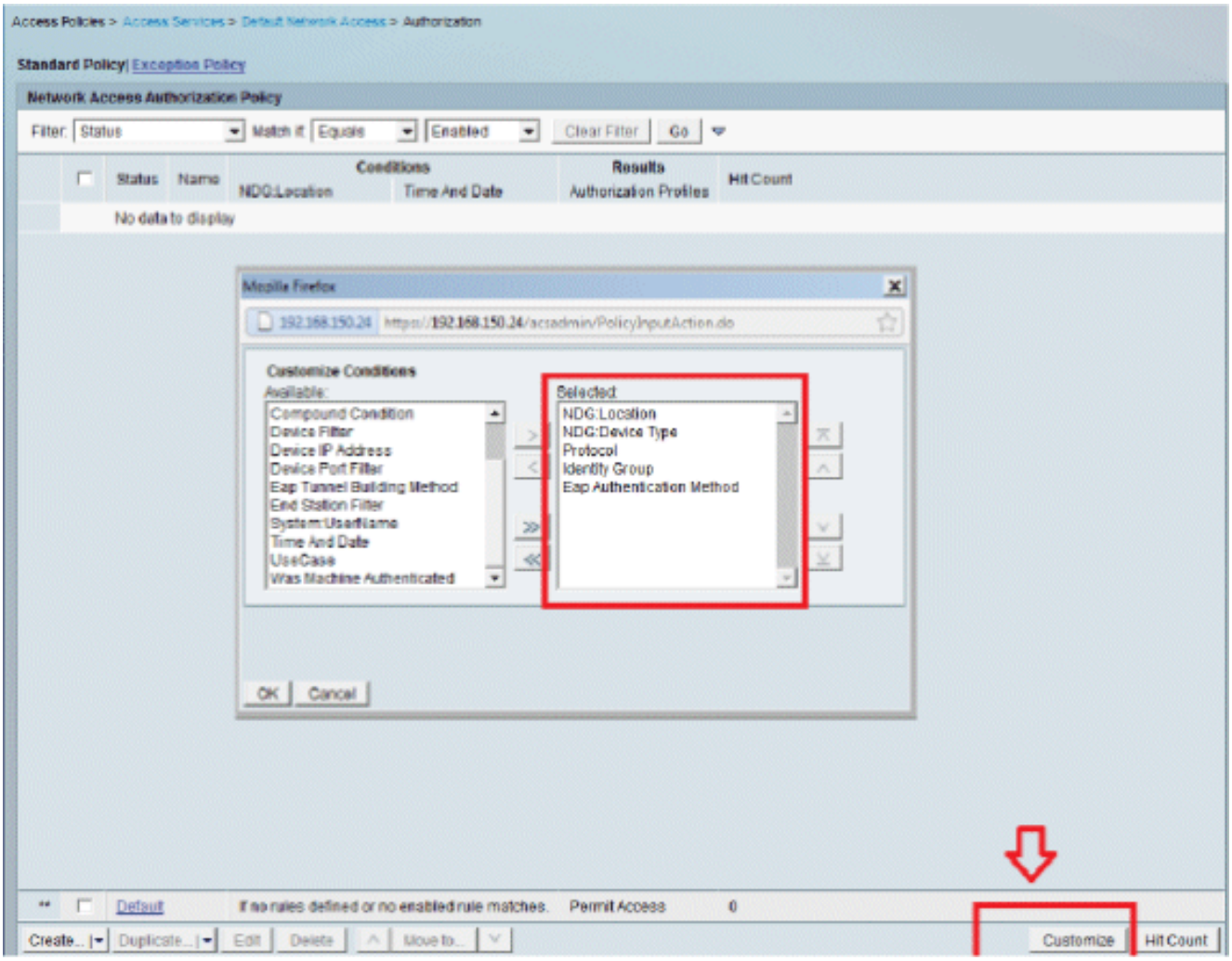


3. Cliquez sur Submit.
4. Vérifiez le groupe d'identités que vous avez sélectionné. Dans cet exemple, nous utilisons **Internal Users**, que nous avons créé sur ACS. **Enregistrez** les modifications.

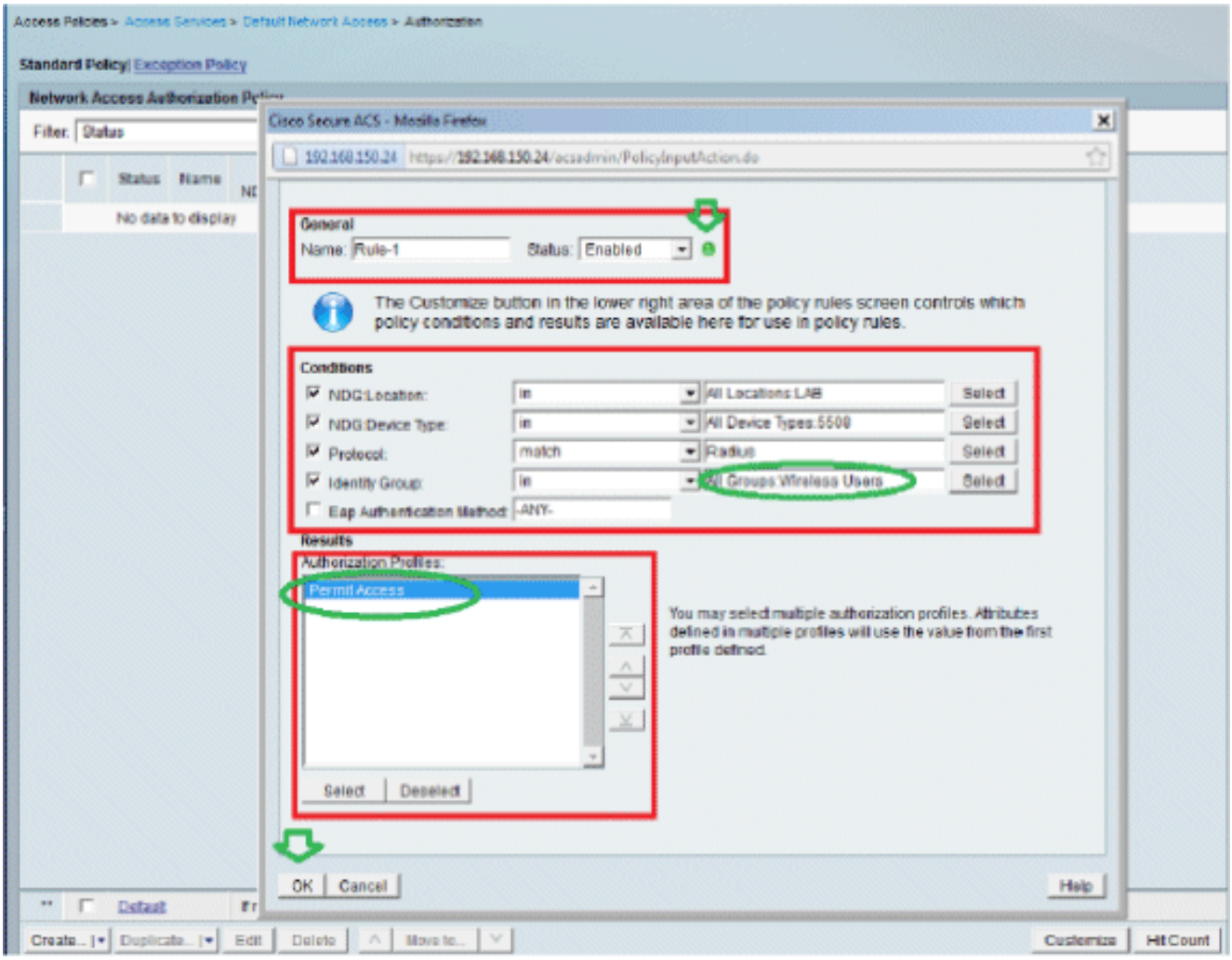


5. Afin de vérifier le profil d'autorisation, allez à **Politiques d'accès > Services d'accès > Accès réseau par défaut > Autorisation**.Vous pouvez personnaliser dans quelles conditions vous autorisez l'accès utilisateur au réseau et quel profil d'autorisation (attributs) vous passerez une fois authentifié. Cette granularité est uniquement disponible dans ACS 5.x. Dans cet exemple, nous avons sélectionné Emplacement, **Type de périphérique**, **Protocole**, **Groupe**

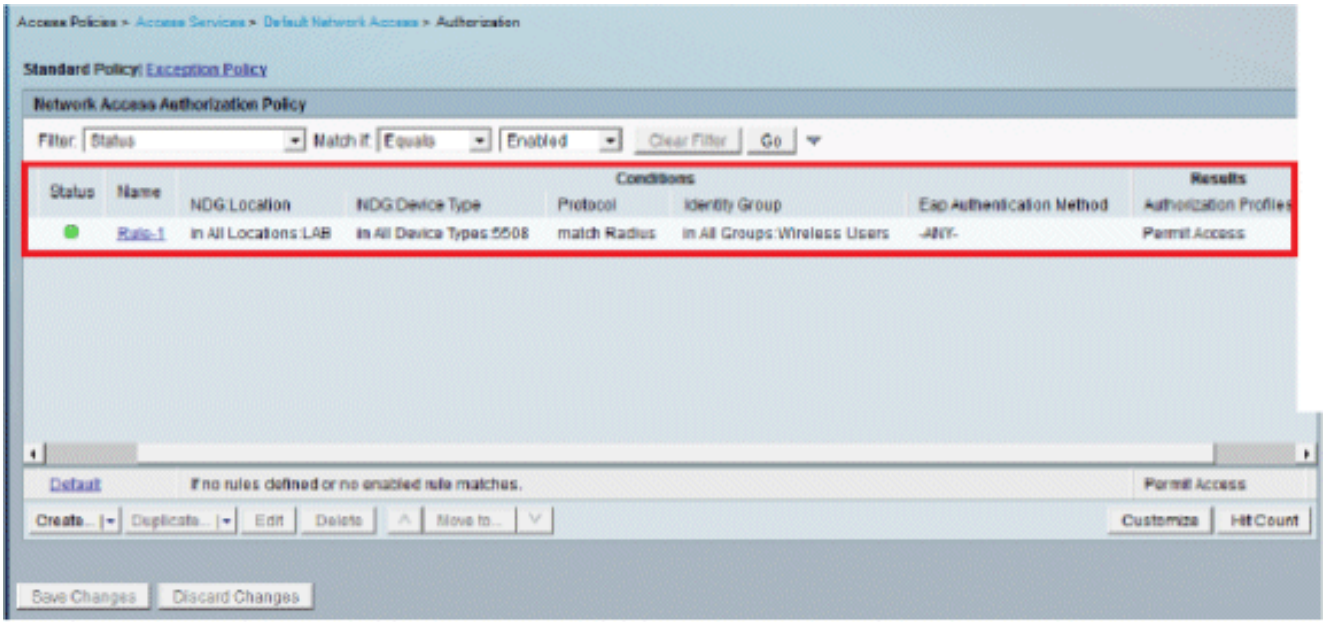
d'identités et **Méthode d'authentification EAP**.



6. Cliquez sur **OK**, puis sur **Save Changes**.
7. L'étape suivante consiste à créer une règle. Si aucune règle n'est définie, l'accès du client est autorisé sans aucune condition.Cliquez sur **Create > Rule-1**. Cette règle s'applique aux utilisateurs du groupe « Utilisateurs sans fil
   ».

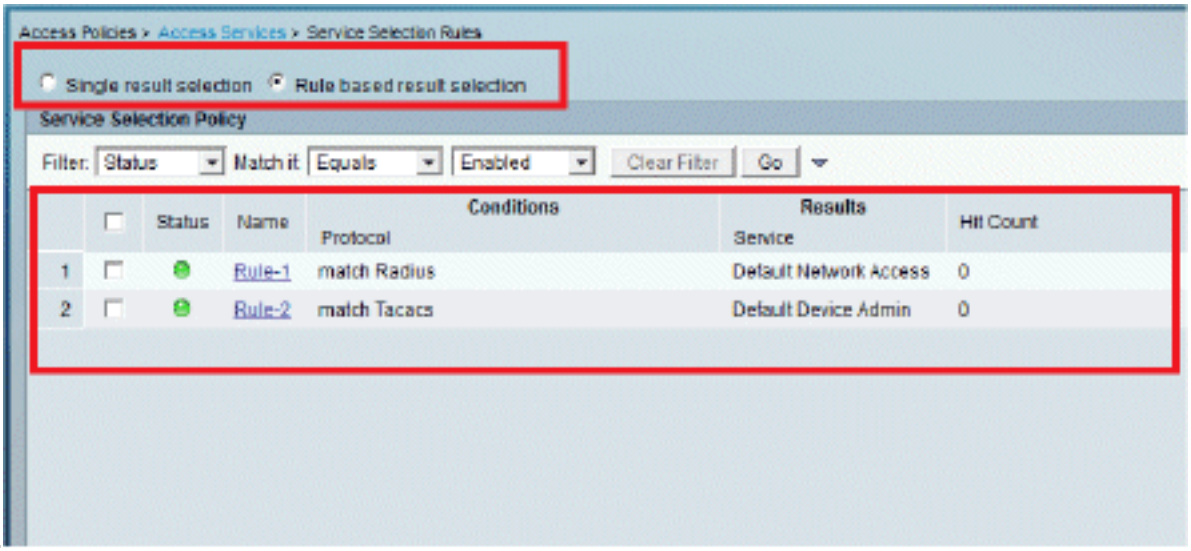


8. Enregistrez les modifications. L'écran se présente comme suit
:



Si vous souhaitez que les utilisateurs ne répondant pas aux conditions soient refusés, modifiez la règle par défaut pour dire « refuser l'accès ».

9. Nous allons maintenant définir les **règles de sélection des services**. Utilisez cette page afin de configurer une stratégie simple ou basée sur des règles pour déterminer quel service appliquer aux demandes entrantes. Dans cet exemple, une stratégie basée sur des règles est

utilisée. 

Configurer le WLC

Cette configuration requiert les étapes suivantes :

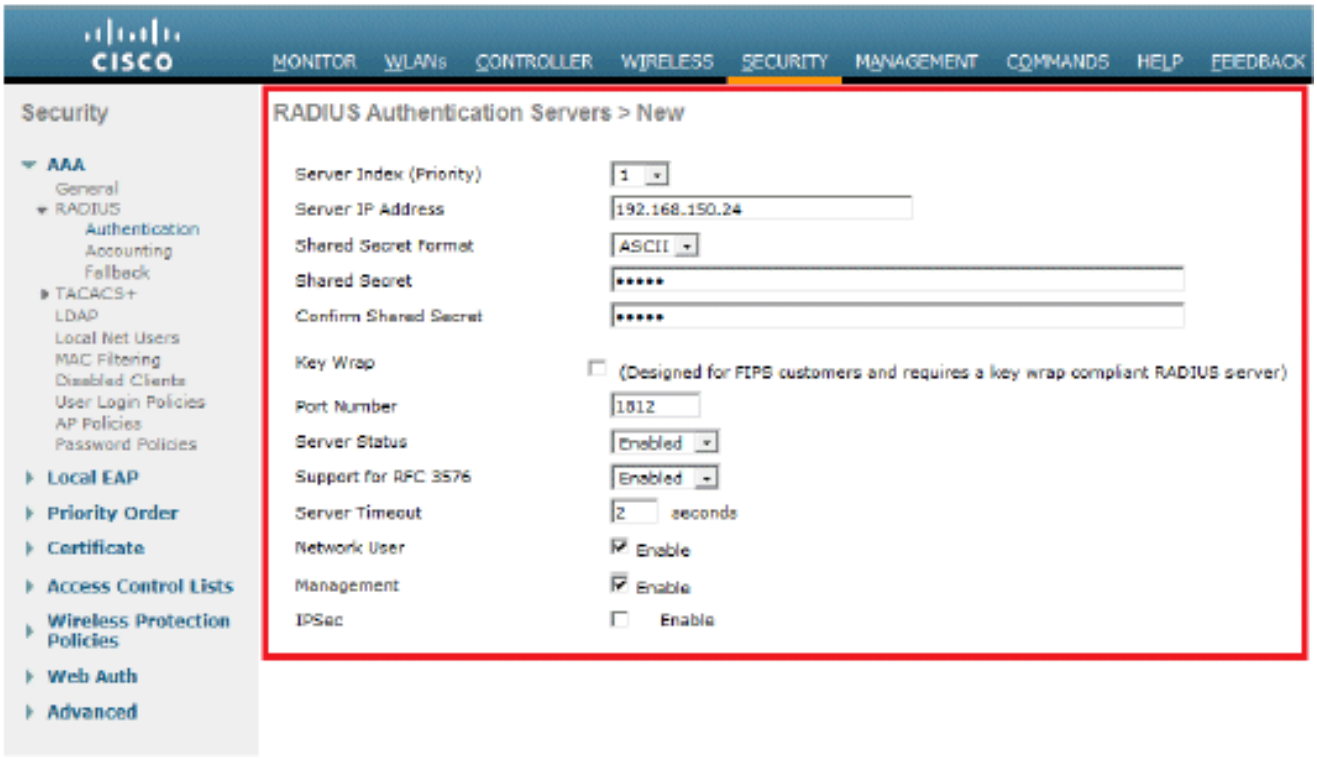
1. Configurez le WLC avec les détails du serveur d'authentification.
2. Configurez les interfaces dynamiques (VLAN).
3. Configurez les WLAN (SSID).

Configurer le WLC avec les détails du serveur d'authentification

Il est nécessaire de configurer le WLC pour qu'il puisse communiquer avec le serveur RADIUS afin d'authentifier les clients, et aussi pour toute autre transaction.

Procédez comme suit :

1. Dans l'interface graphique du contrôleur, cliquez sur **Security**.
2. Entrez l'adresse IP du serveur RADIUS et la clé Shared Secret utilisée entre le serveur RADIUS et le WLC.Cette clé secrète partagée doit être identique à celle configurée sur le serveur
   RADIUS.

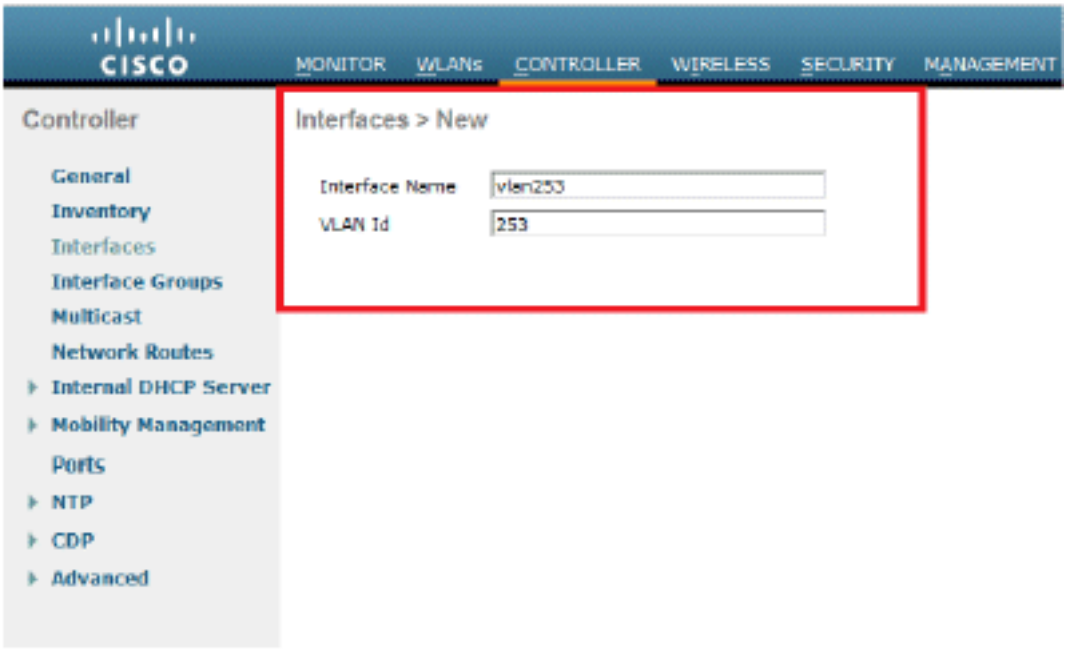


Configurer les interfaces dynamiques (VLAN)

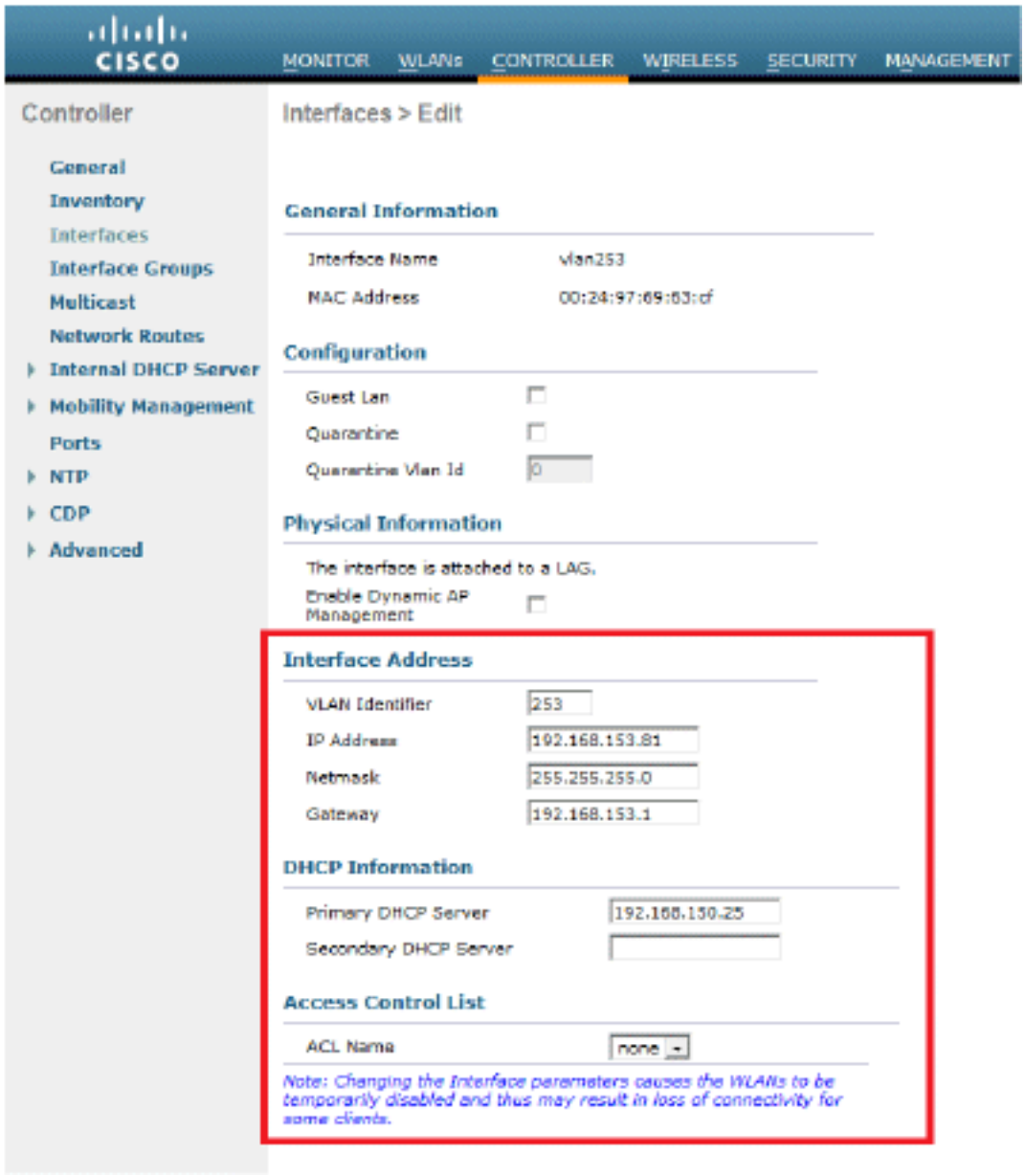
Cette procédure décrit comment configurer des interfaces dynamiques sur le WLC.

Procédez comme suit :

1. L'interface dynamique est configurée à partir de l'interface graphique du contrôleur, dans la fenêtre **Controller >**

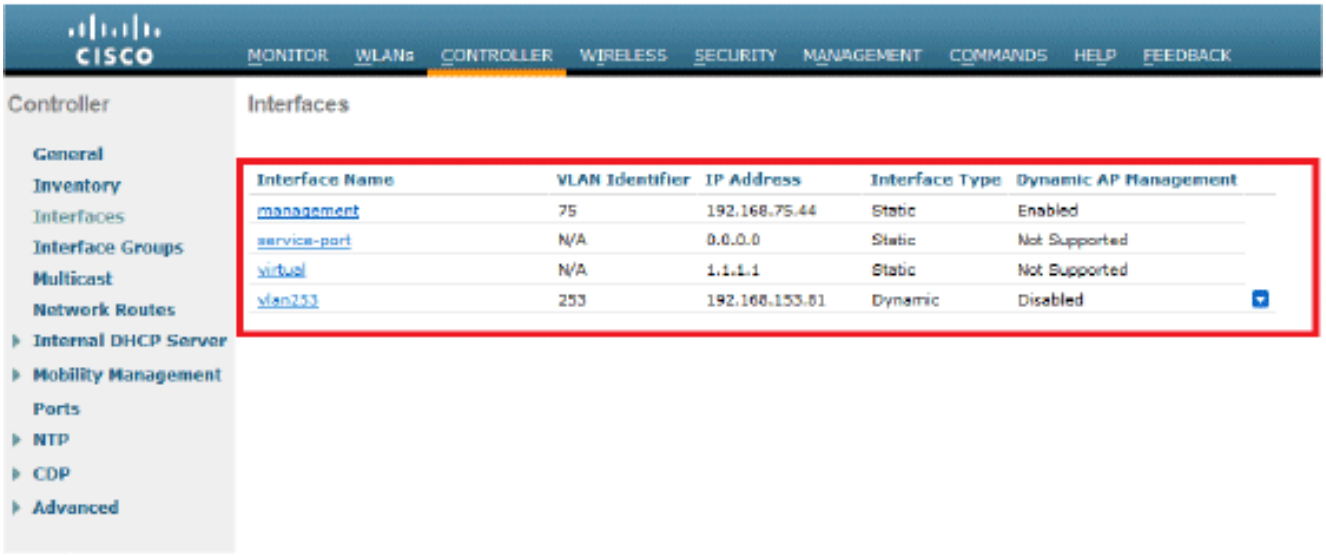


Interfaces.
2. Cliquez sur **Apply**.Cela vous mène à la fenêtre Edit de cette interface dynamique (VLAN 253 ici).
3. Entrez l'adresse IP et la passerelle par défaut de cette interface



dynamique.

4. Cliquez sur **Apply**.
5. Les interfaces configurées ressembleront à ceci :

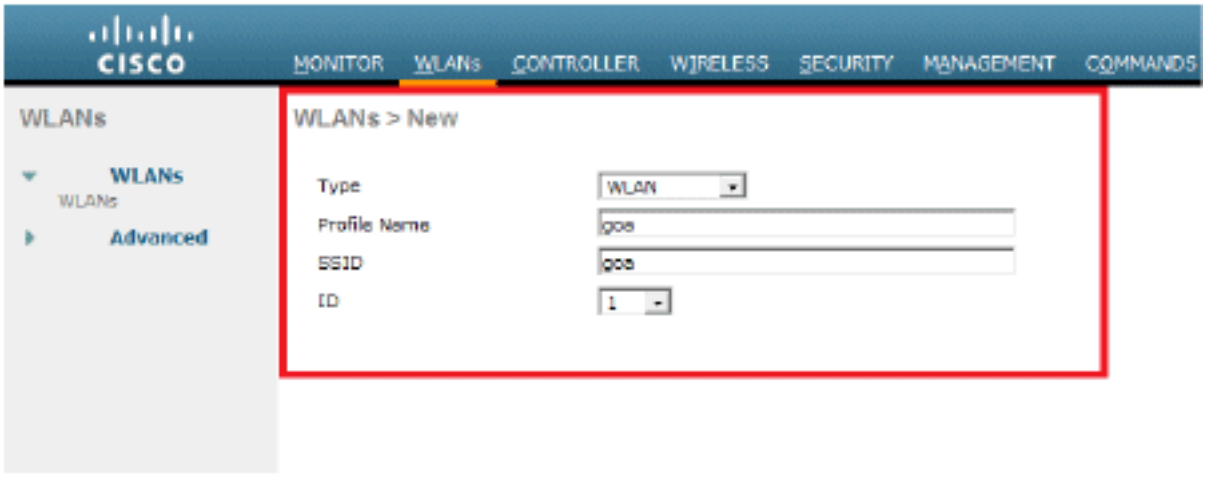


Configurer les WLAN (SSID)

Cette procédure explique comment configurer les WLAN dans le WLC.

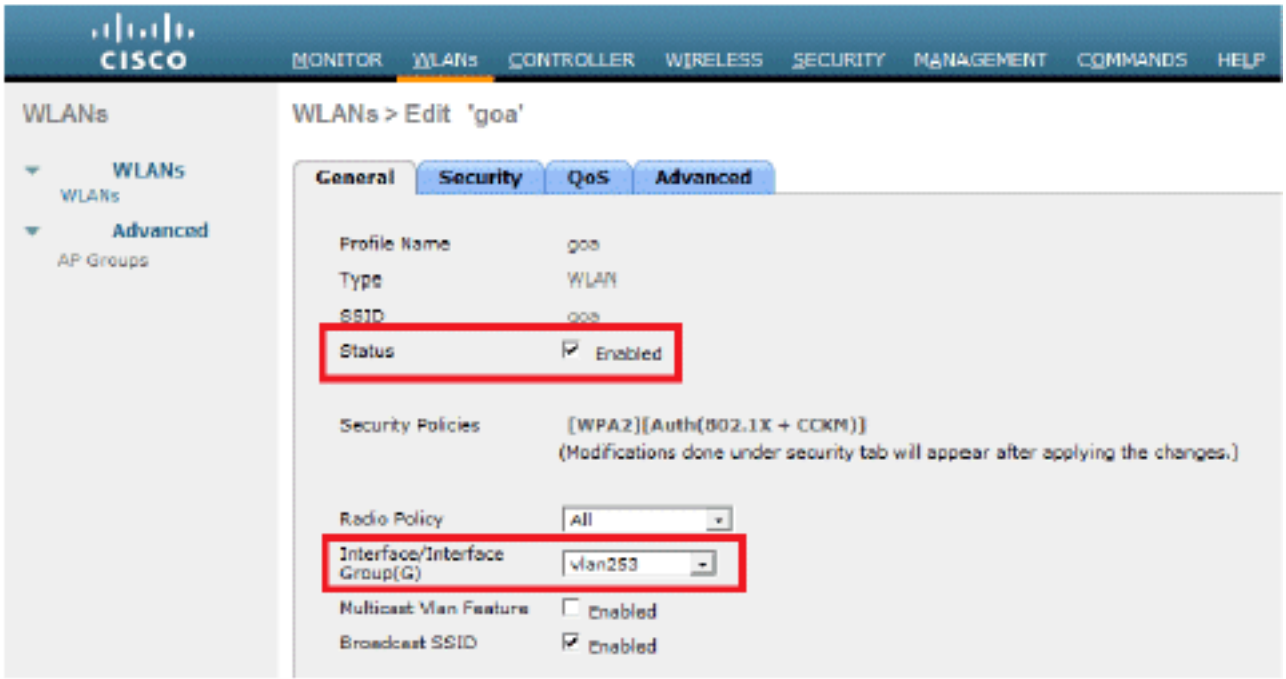
Procédez comme suit :

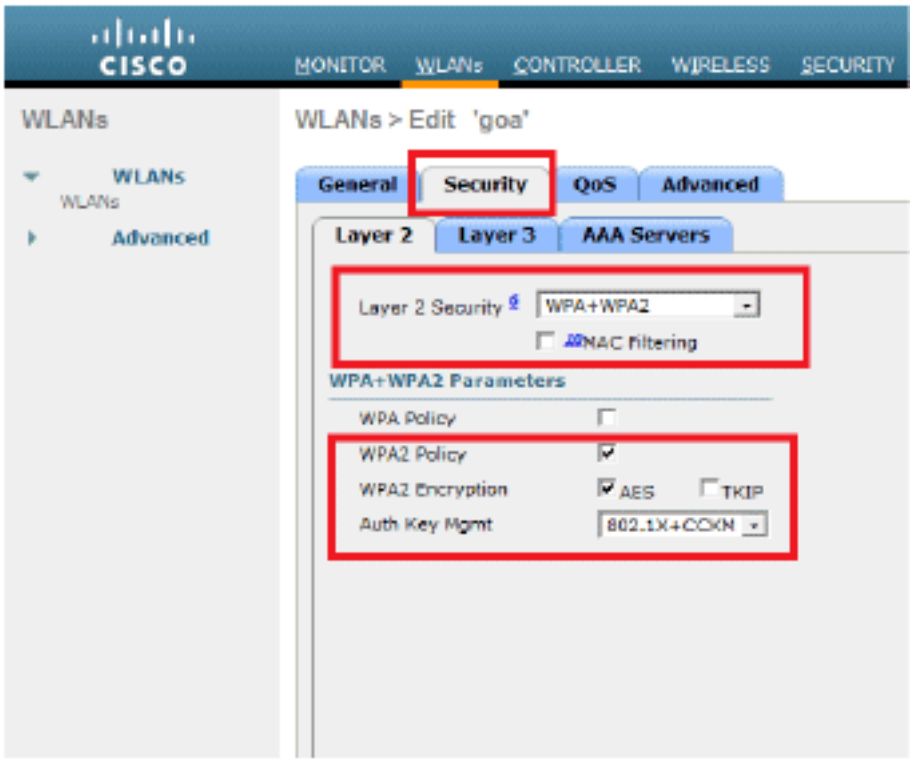
1. Dans l'interface graphique du contrôleur, allez à **WLANs > Create New** afin de créer un nouveau WLAN. La fenêtre New WLANs est affichée.
2. Entrez l'ID de WLAN et le SSID du WLAN.Vous pouvez entrer n'importe quel nom comme SSID WLAN. Cet exemple utilise **goa** comme SSID

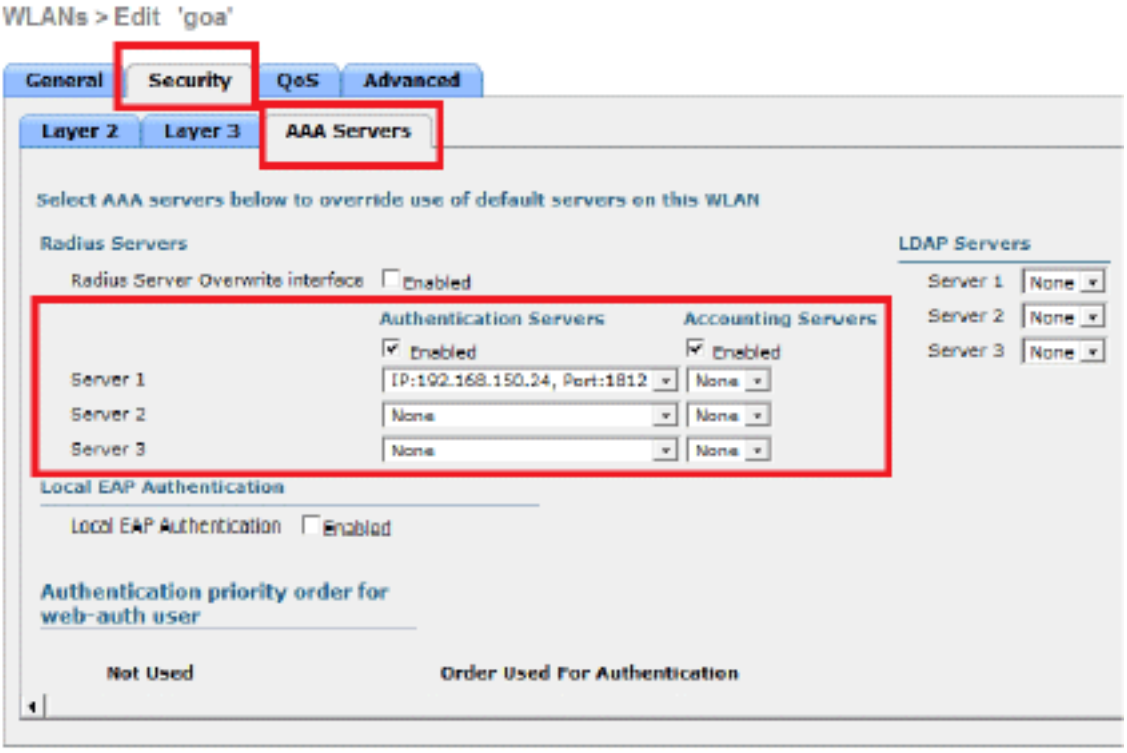


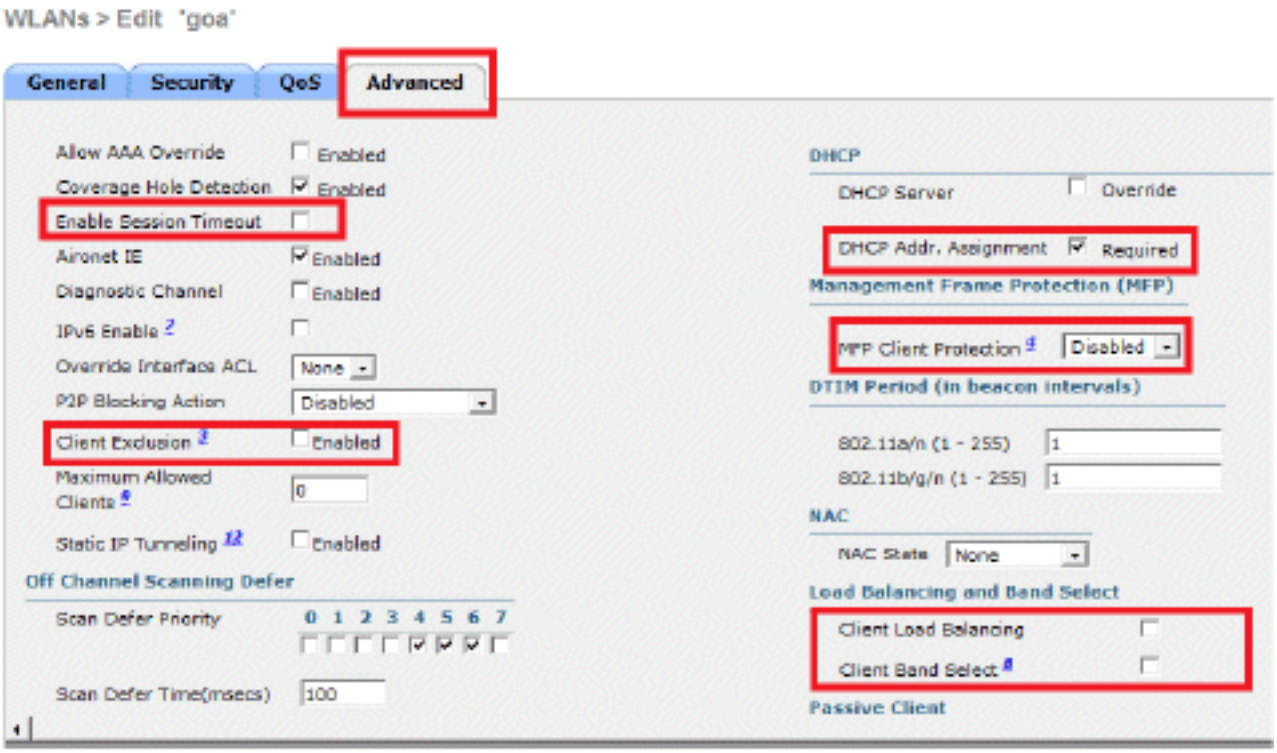
WLAN.

3. Cliquez sur **Apply** afin d'accéder à la fenêtre Edit de l'objectif WLAN.




MONITOR
WLANs
CONTROLLER
WIRELESS
SECURITY
WLANs
WLANs > Edit 'goa'
WLANs
WLANs
Advanced
General
Security
QoS
Advanced
Layer 2
Layer 3
AAA Servers
Layer 2 Security
WPA+WPA2
MAC Filtering
WPA+WPA2 Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption
AES
TKIP
Auth Key Mgmt
802.1X+CCKM


WLANs > Edit 'goa'
General
Security
QoS
Advanced
Layer 2
Layer 3
AAA Servers
Select AAA servers below to override use of default servers on this WLAN
Radius Servers
Radius Server Overwrite interface
Enabled
Authentication Servers
Accounting Servers
Enabled
Enabled
Server 1
IP:192.168.150.24, Port:1812
None
Server 2
None
None
Server 3
None
None
LDAP Servers
Server 1
None
Server 2
None
Server 3
None
Local EAP Authentication
Local EAP Authentication
Enabled
Authentication priority order for web-auth user
Not Used
Order Used For Authentication



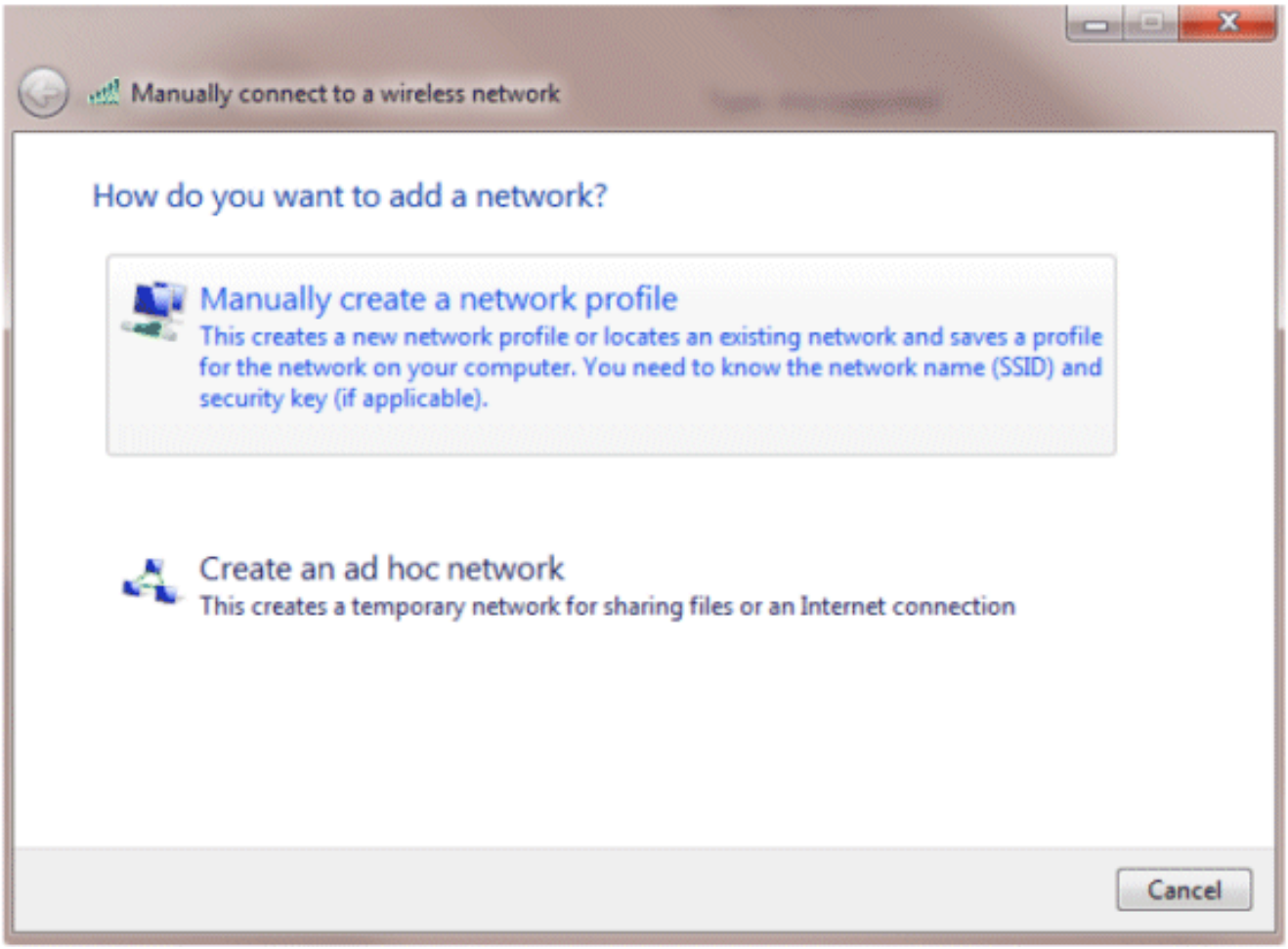
Configuration de l'utilitaire client sans fil

PEAP-MSCHAPv2 (utilisateur1)

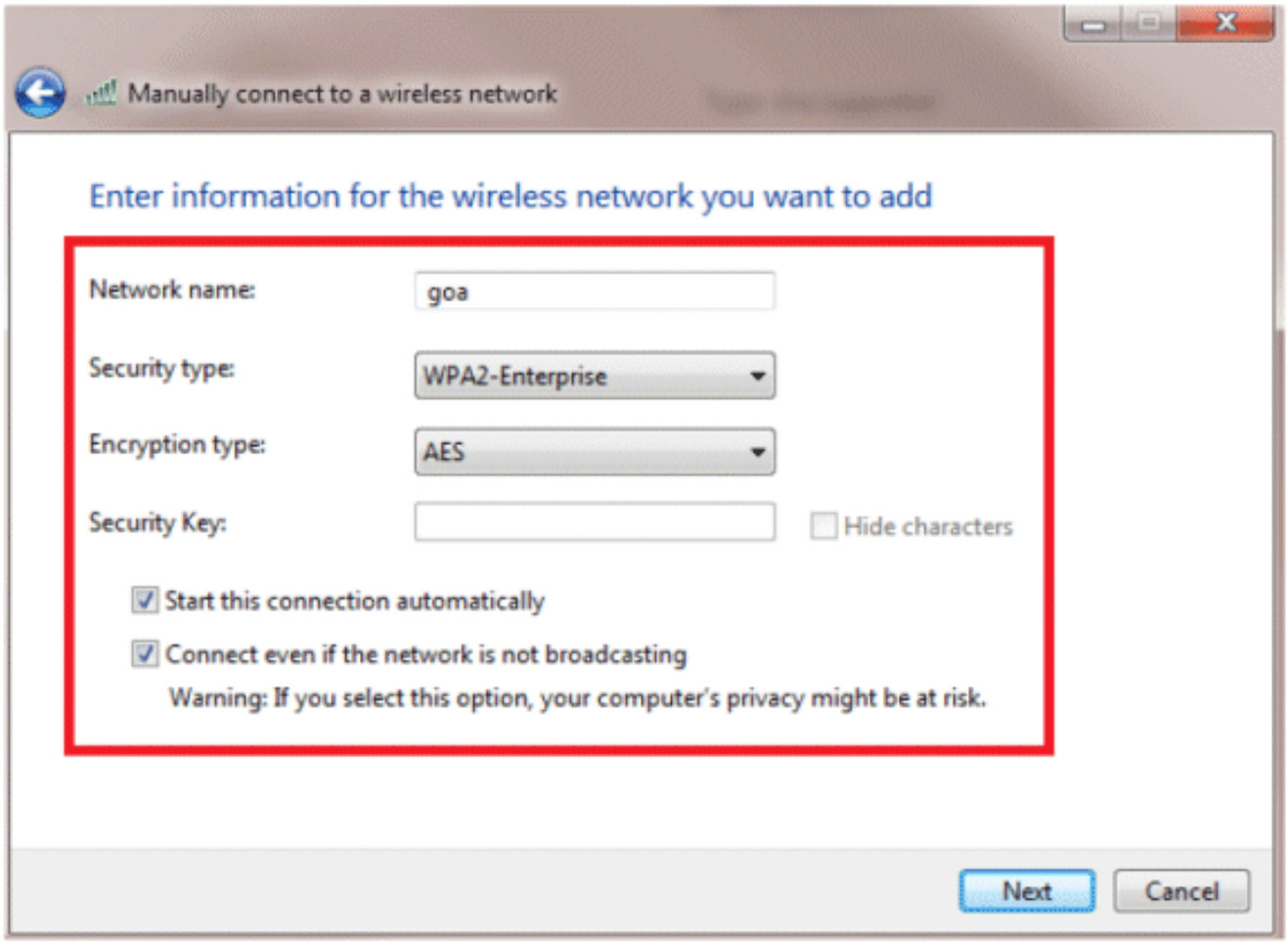
Dans notre client test, nous utilisons Windows 7 Native supplicant avec une carte Intel 6300-N exécutant la version 14.3 du pilote. Il est recommandé de tester à l'aide des pilotes les plus récents des fournisseurs.

Complétez ces étapes afin de créer un profil dans Windows Zero Config (WZC) :

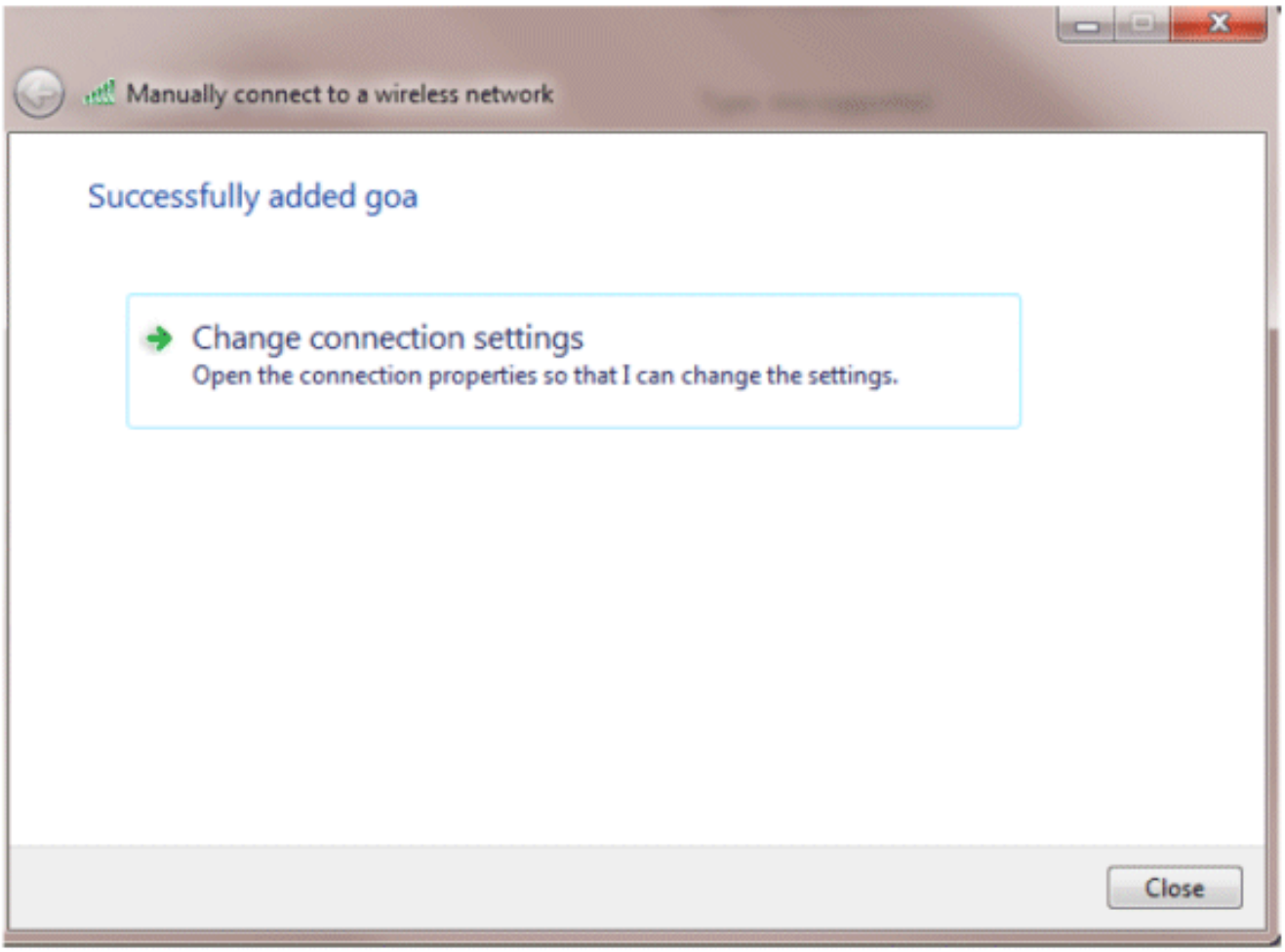
1. Accédez à **Panneau de configuration > Réseau et Internet > Gérer les réseaux sans fil**.
2. Cliquez sur l'onglet **Ajouter**.
3. Cliquez sur **Manually create a network profile**.



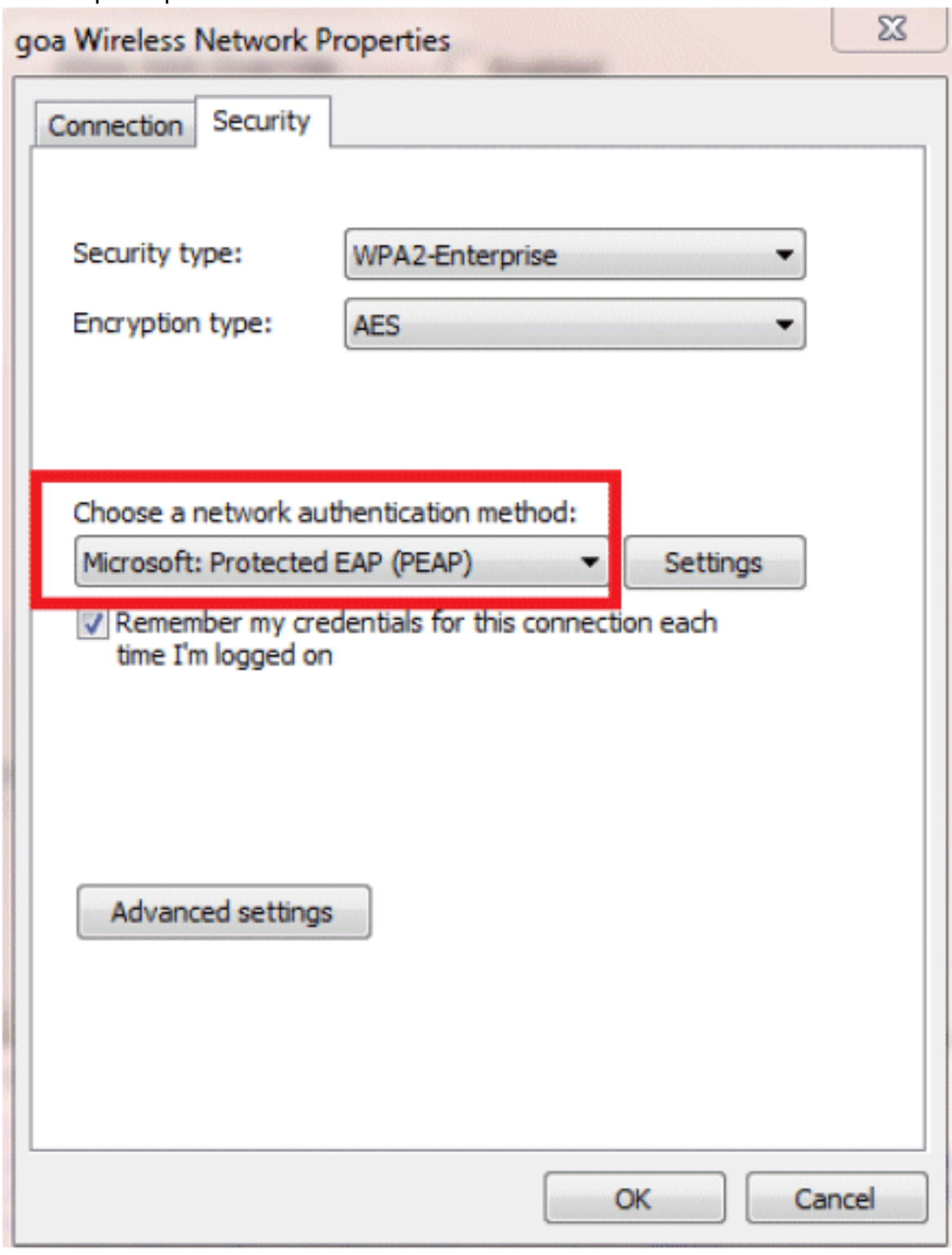
4. Ajoutez les détails tels que configurés sur le WLC.**Remarque :** le SSID est sensible à la casse.
5. Cliquez sur **Next**
   (Suivant).

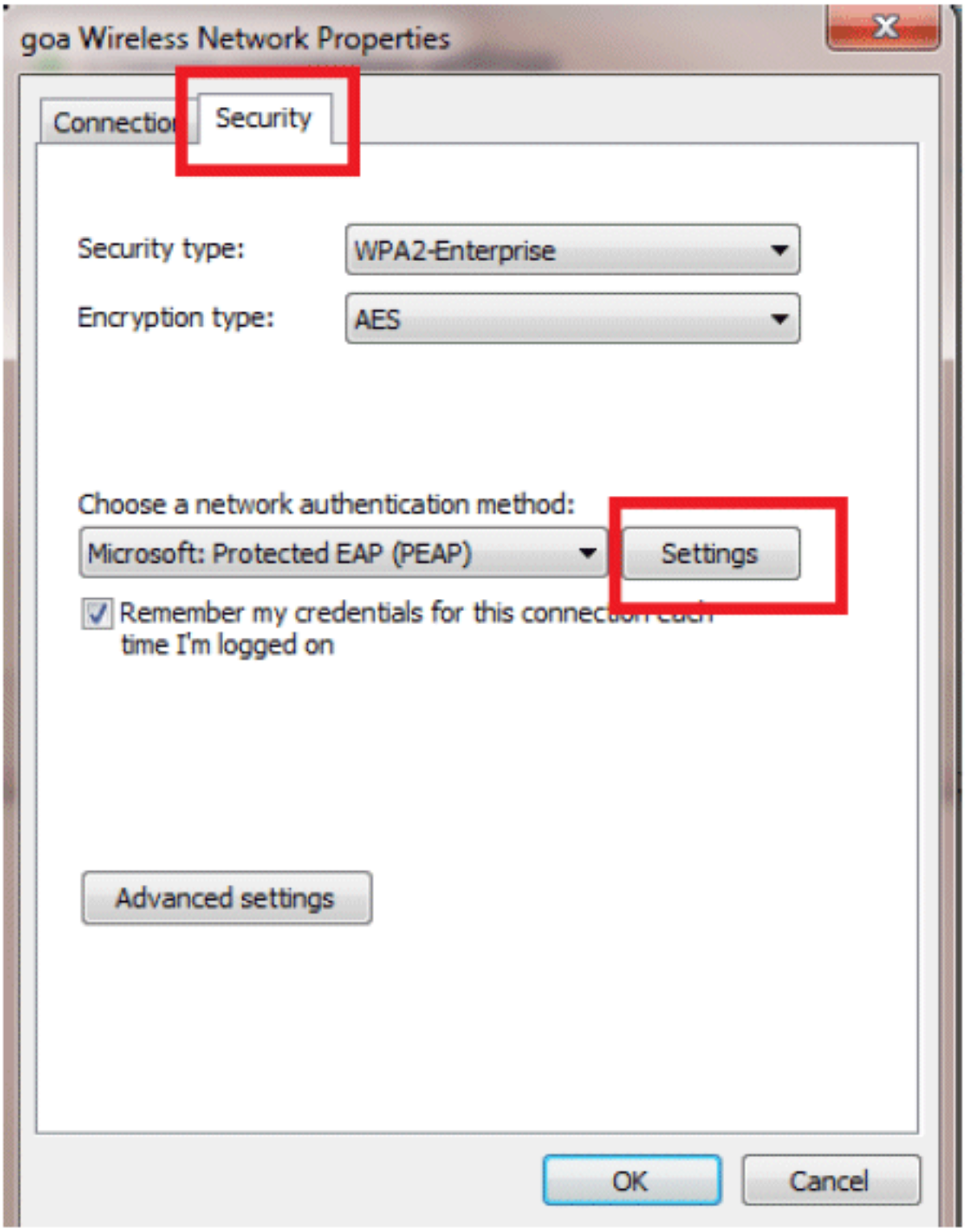


6. Cliquez sur **Change connection settings** afin de vérifier à nouveau les paramètres.

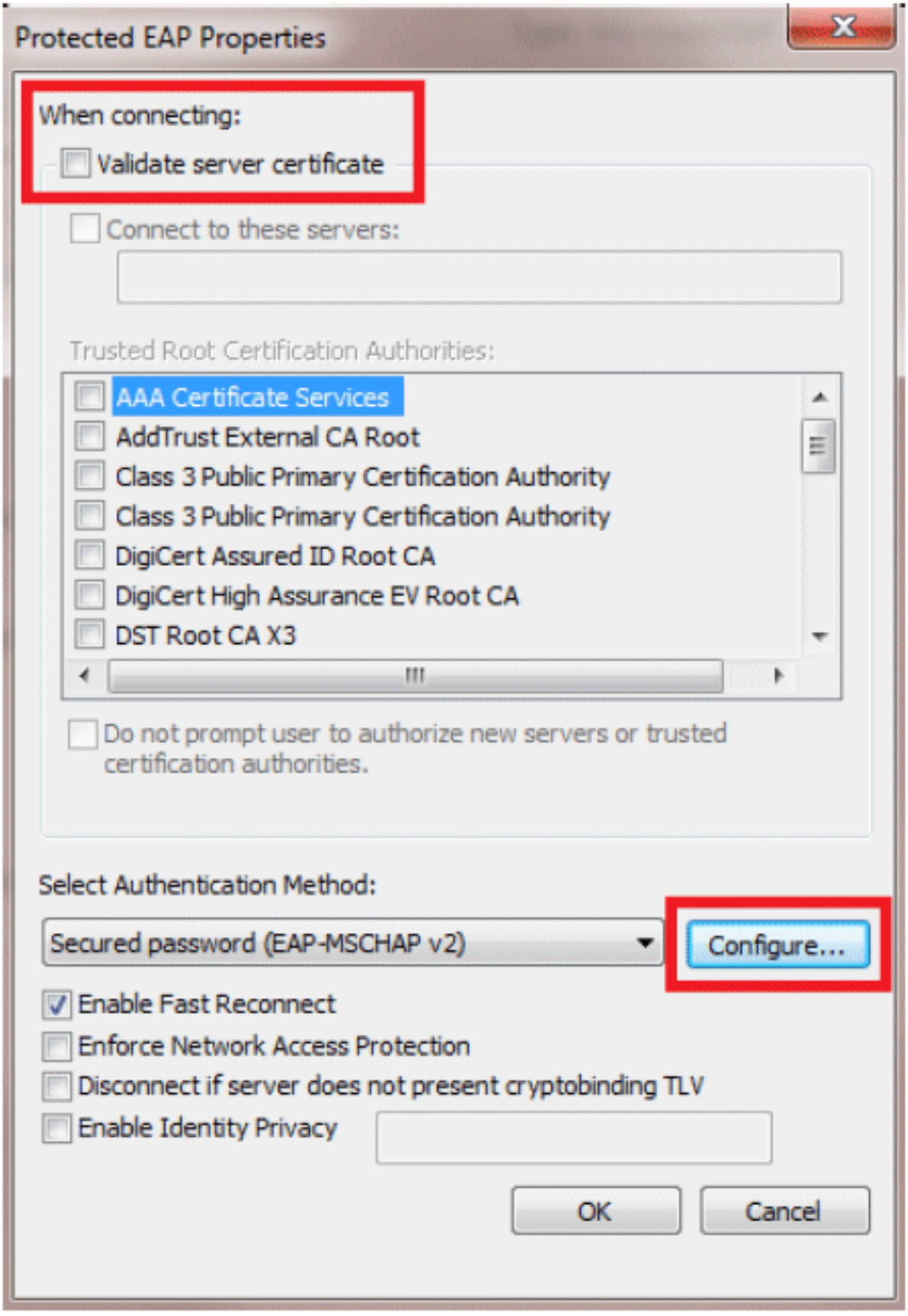


7. Assurez-vous que le protocole **PEAP est** activé.

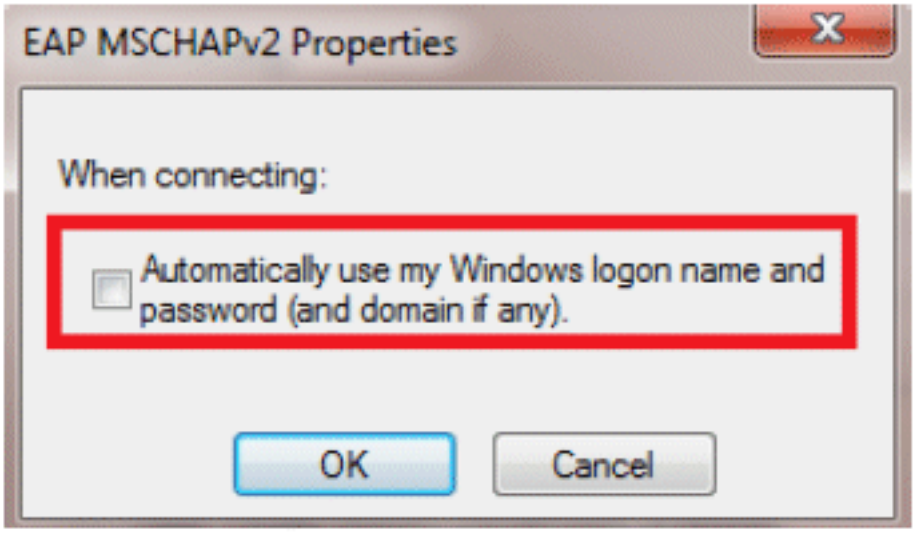




8. Dans cet exemple, nous ne validons pas le certificat du serveur. Si vous cochez cette case et que vous ne parvenez pas à vous connecter, essayez de désactiver la fonction et de la tester à
nouveau.

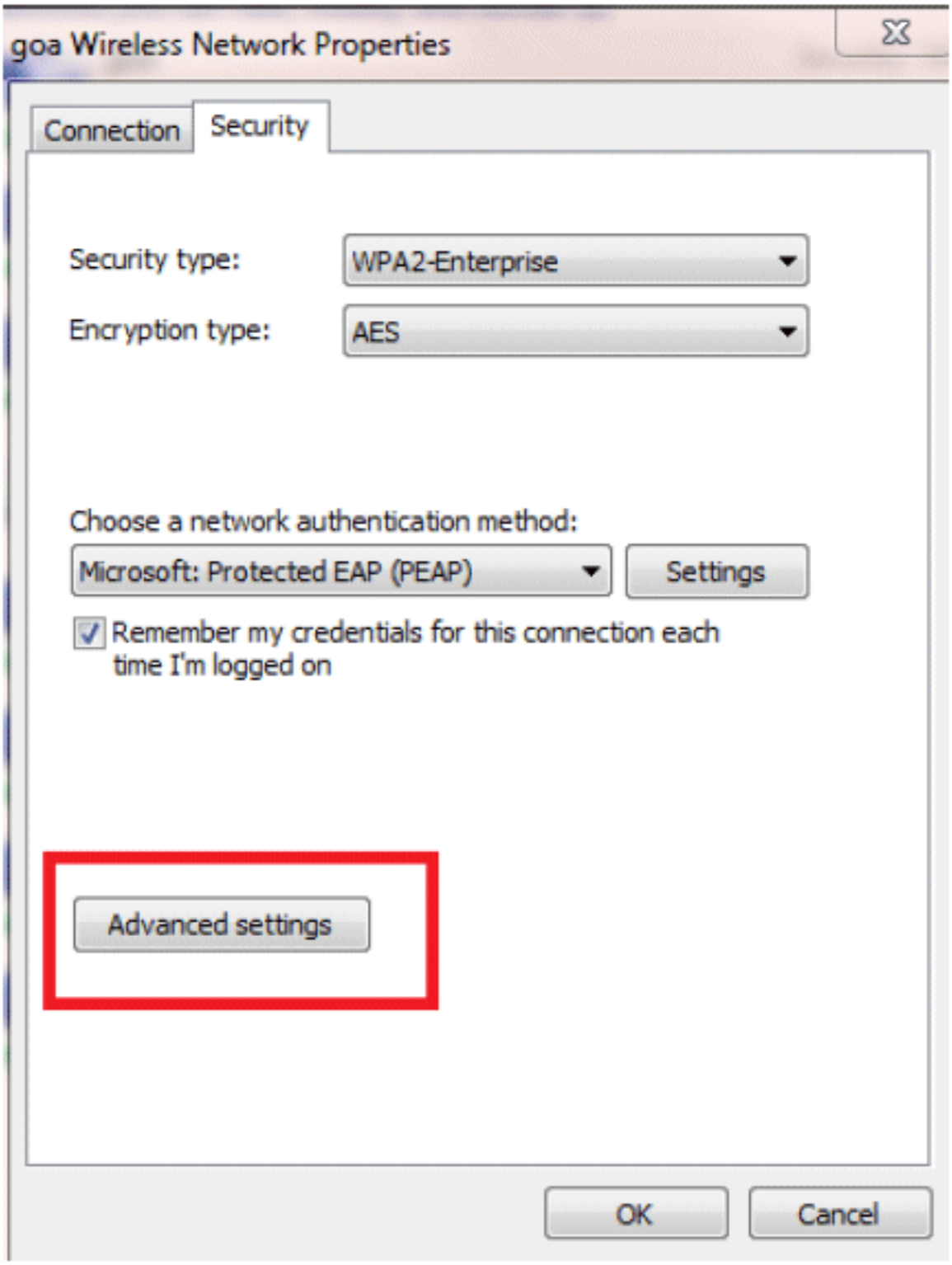


9. Vous pouvez également utiliser vos informations d'identification Windows pour vous connecter. Cependant, dans cet exemple, nous n'allons pas l'utiliser. Click

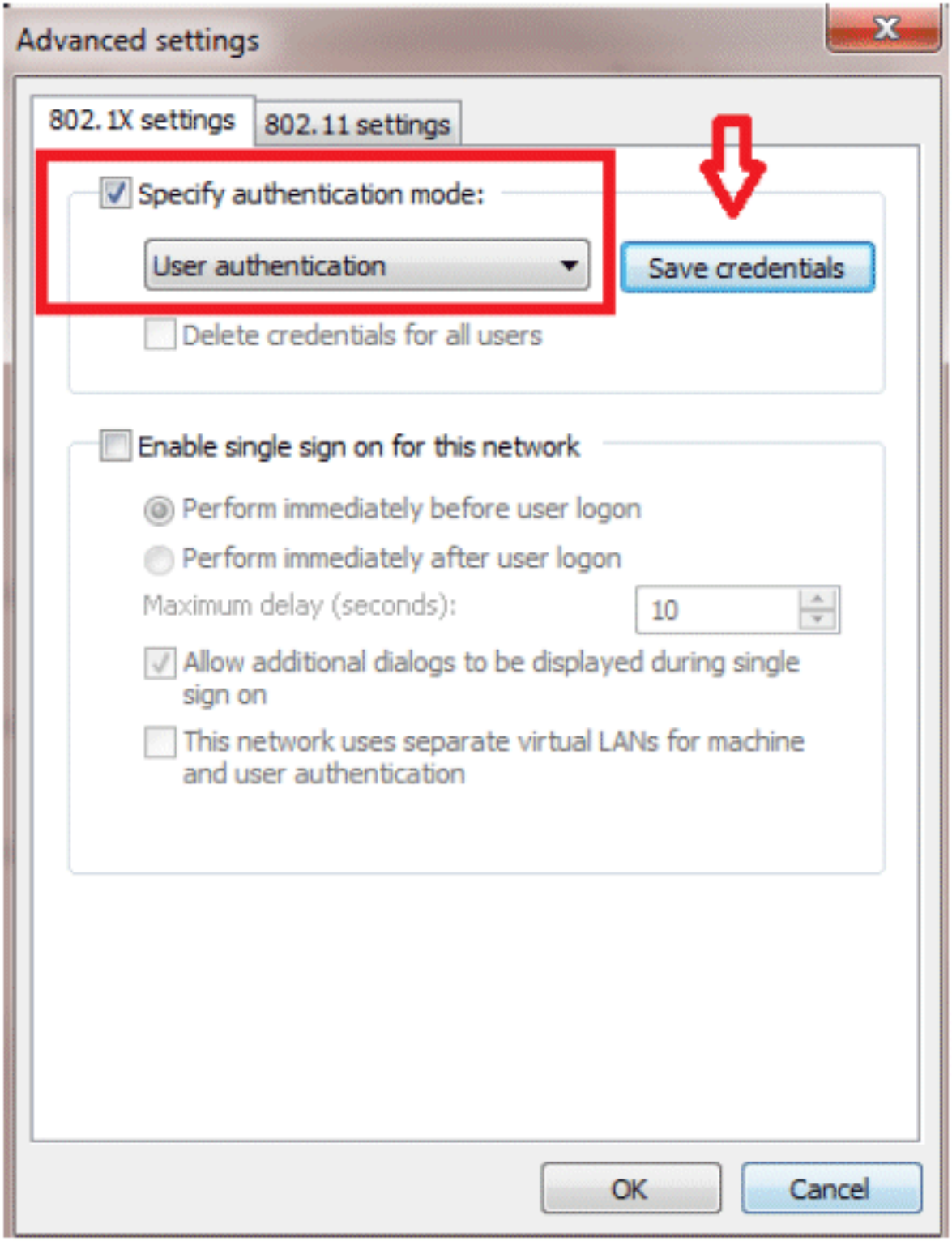


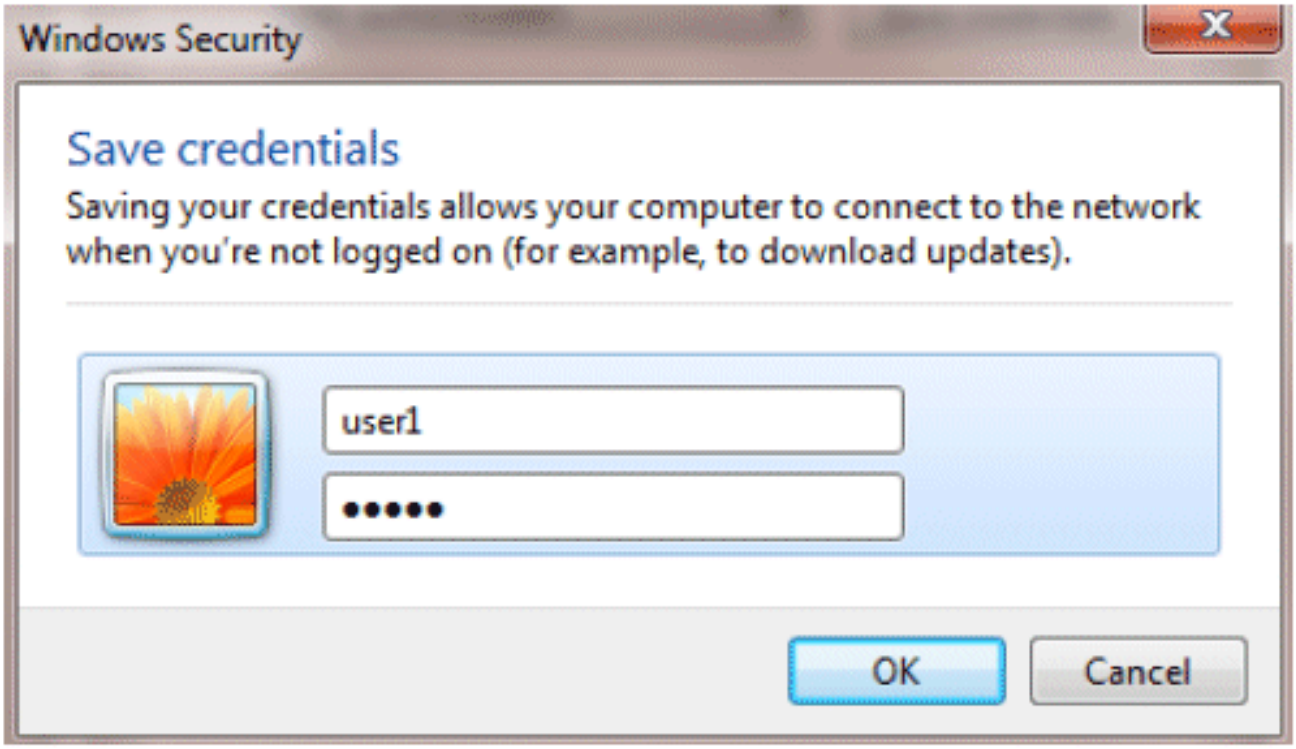
OK.

10. Cliquez sur **Advanced settings** afin de configurer le nom d'utilisateur et le mot de


goa Wireless Network Properties
Connection
Security
Security type:
WPA2-Enterprise
Encryption type:
AES
Choose a network authentication method:
Microsoft: Protected EAP (PEAP)
Settings
Remember my credentials for this connection each time I'm logged on
Advanced settings
OK
Cancel

passe.


Advanced settings
802.1X settings
802.11 settings
Specify authentication mode:
User authentication
Save credentials
Delete credentials for all users
Enable single sign on for this network
Perform immediately before user logon
Perform immediately after user logon
Maximum delay (seconds):
10
Allow additional dialogs to be displayed during single sign on
This network uses separate virtual LANs for machine and user authentication
OK
Cancel



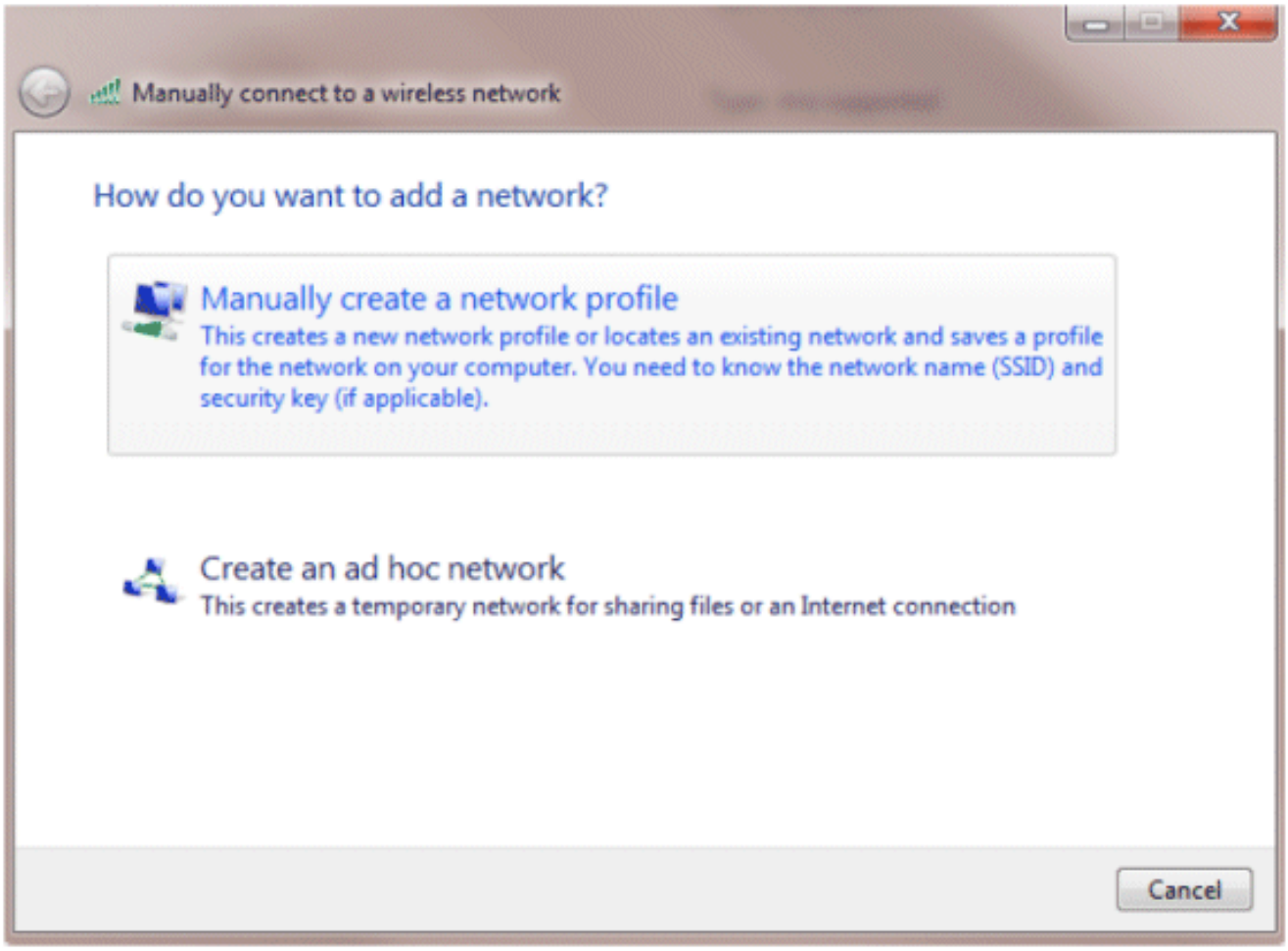
Votre utilitaire client est maintenant prêt à se connecter.

EAP-FAST (utilisateur2)

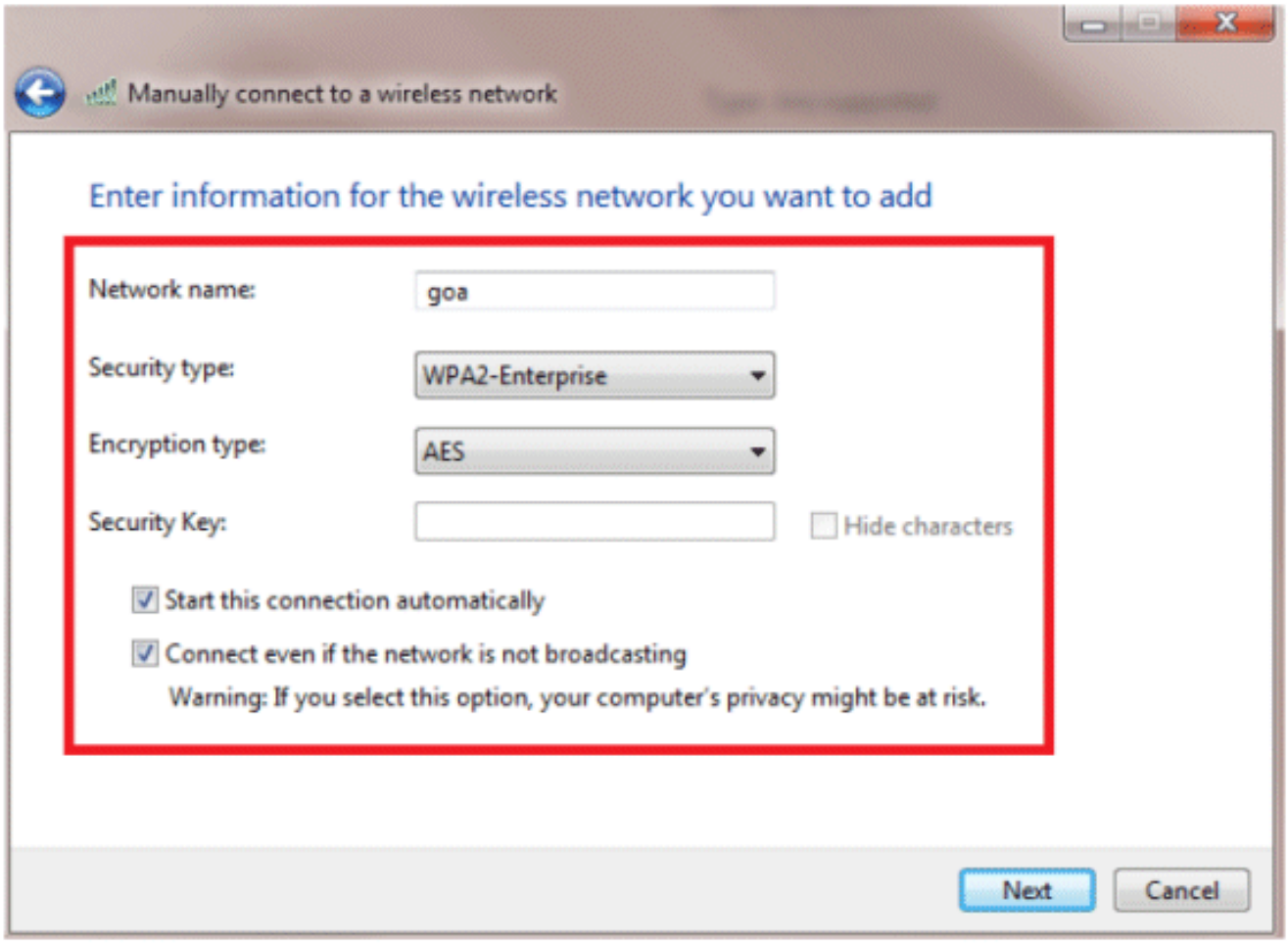
Dans notre client test, nous utilisons Windows 7 Native supplicant avec une carte Intel 6300-N exécutant la version 14.3 du pilote. Il est recommandé de tester à l'aide des pilotes les plus récents des fournisseurs.

Complétez ces étapes afin de créer un profil dans WZC :

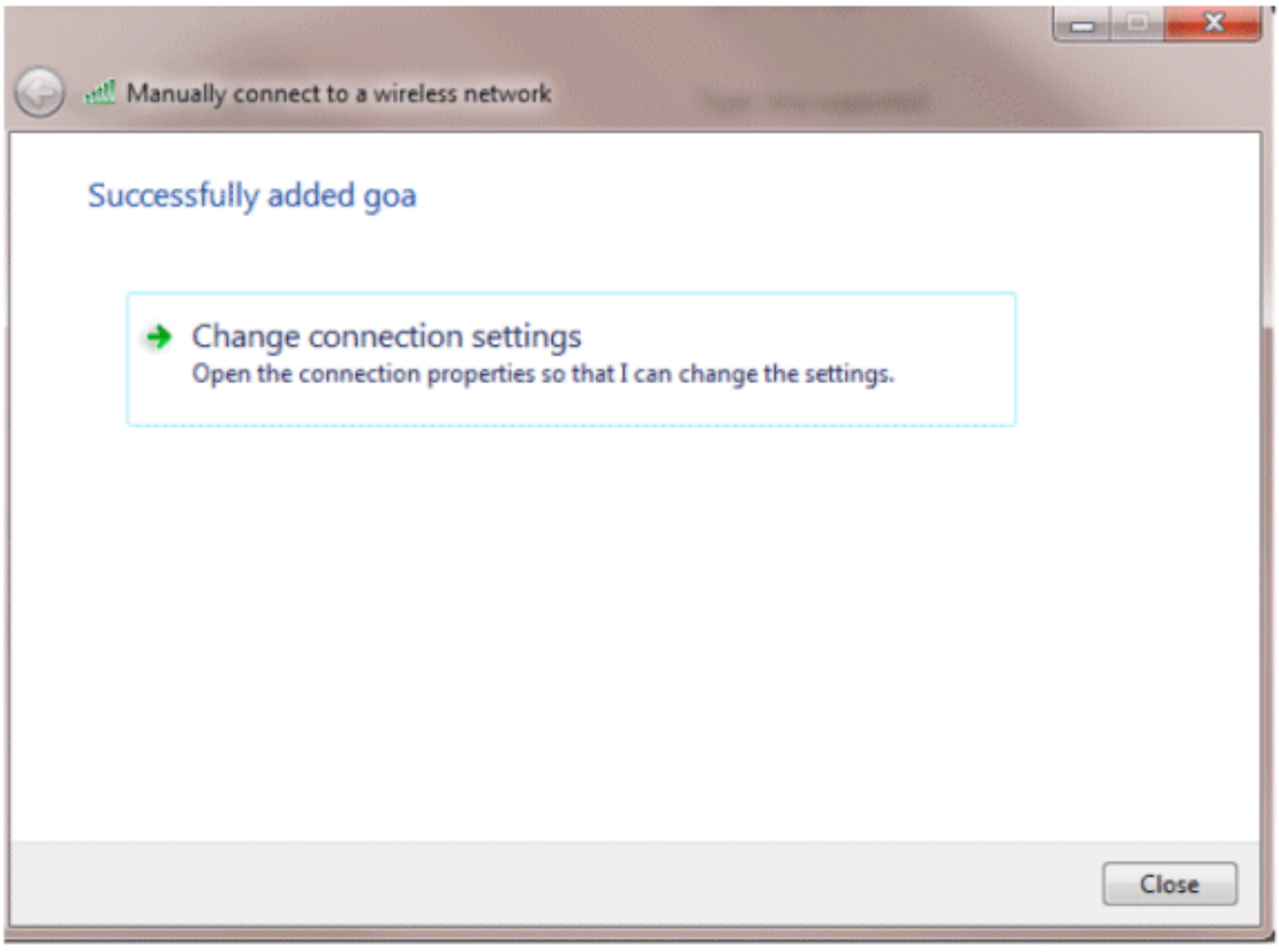
1. Accédez à **Panneau de configuration > Réseau et Internet > Gérer les réseaux sans fil**.
2. Cliquez sur l'onglet **Ajouter**.
3. Cliquez sur **Manually create a network profile**.



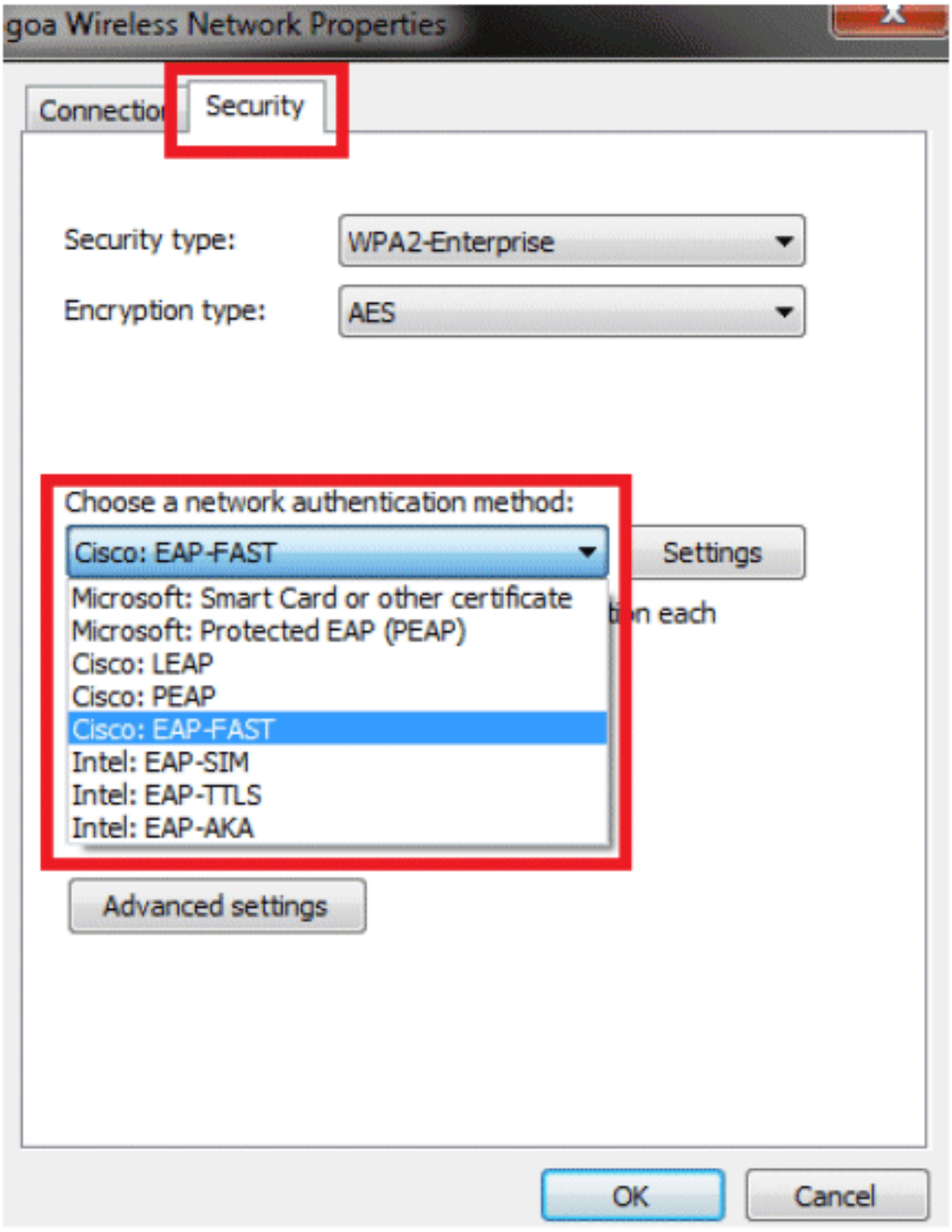
4. Ajoutez les détails tels que configurés sur le WLC.**Remarque :** le SSID est sensible à la casse.
5. Cliquez sur **Next**
   (Suivant).

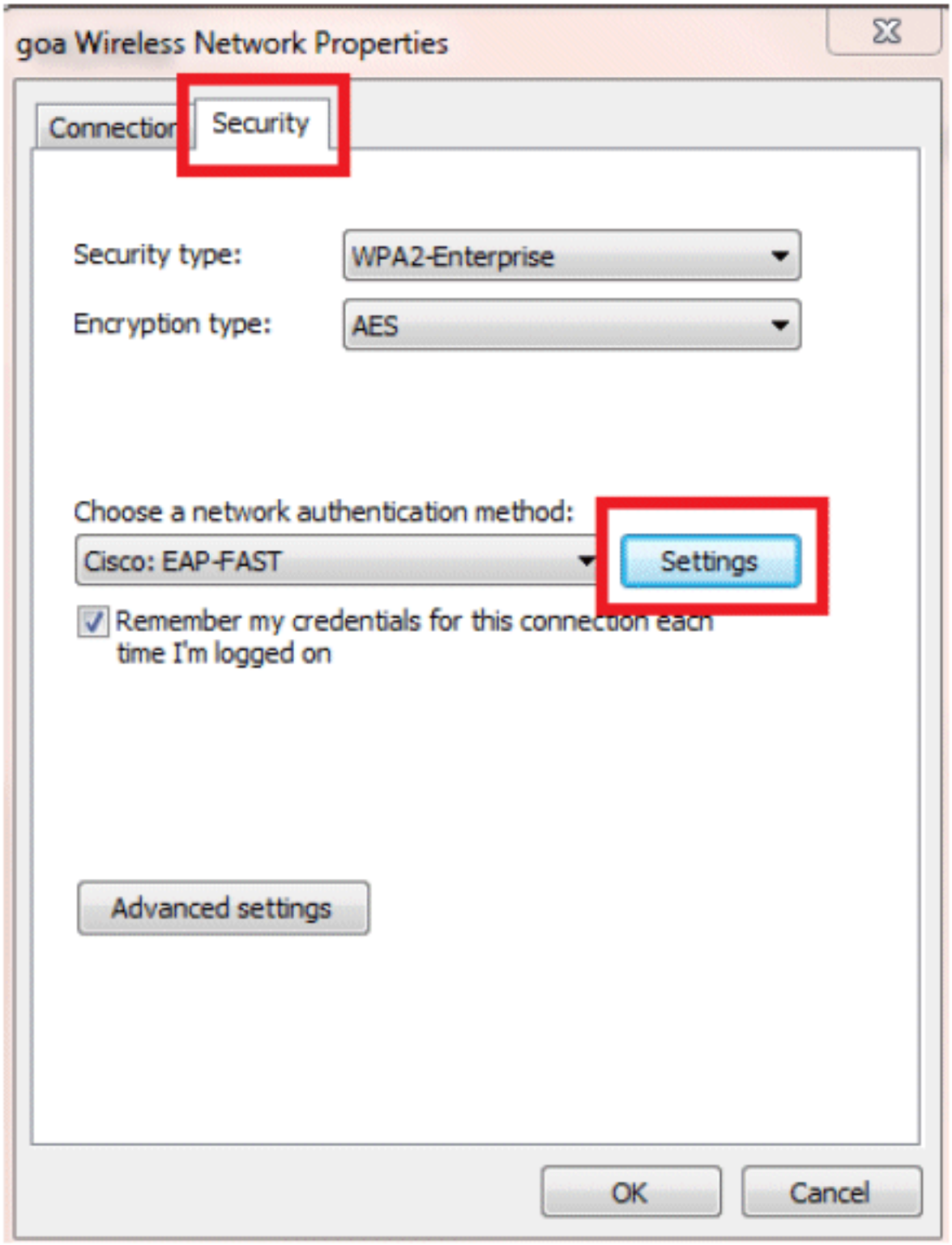


6. Cliquez sur **Change connection settings** afin de vérifier à nouveau les paramètres.

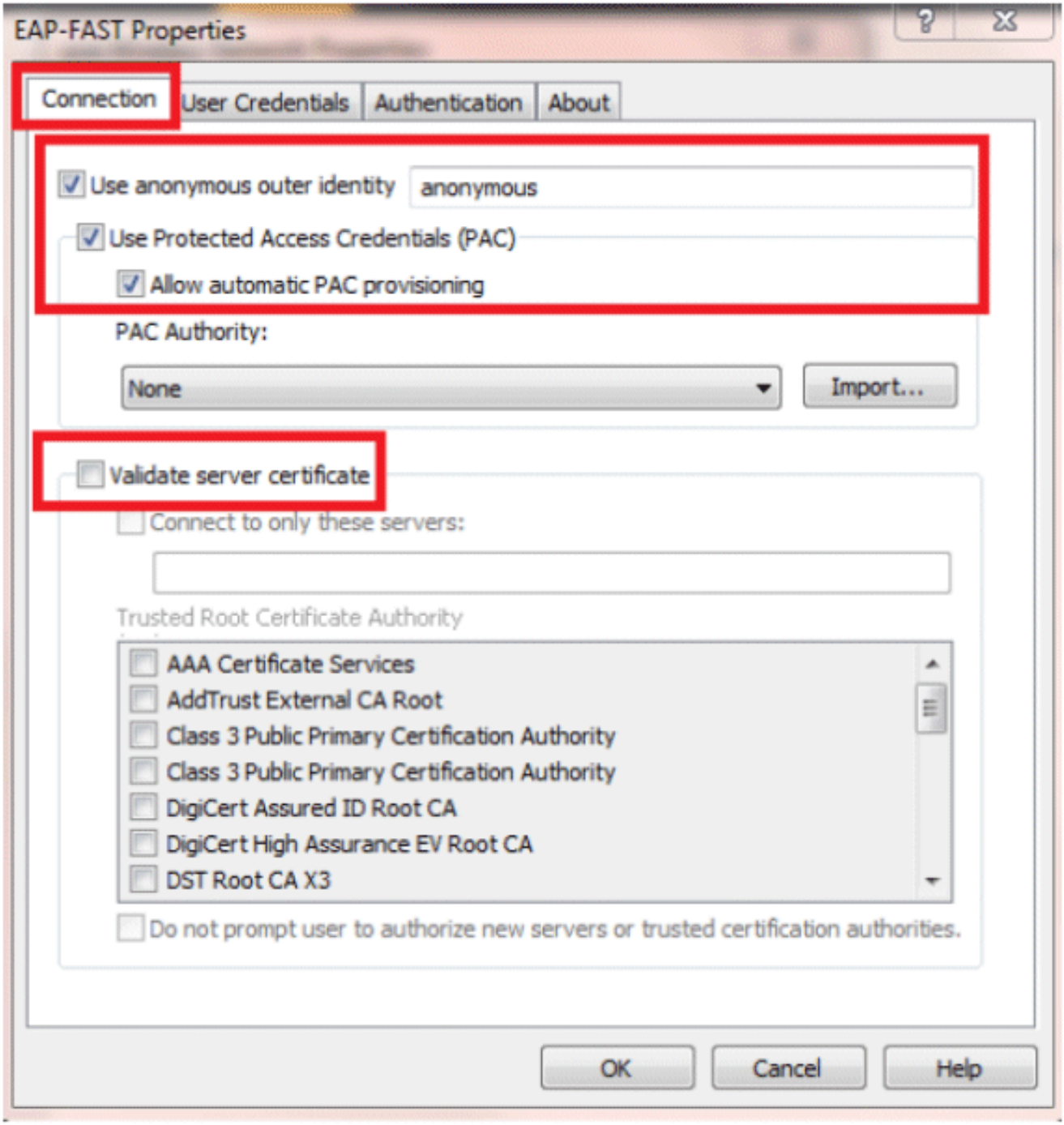


7. Assurez-vous que EAP-FAST est activé.**Remarque :** par défaut, WZC n'a pas EAP-FAST comme méthode d'authentification. Vous devez télécharger l'utilitaire auprès d'un fournisseur tiers. Dans cet exemple, puisqu'il s'agit d'une carte Intel, Intel PROSet est installé sur le système.

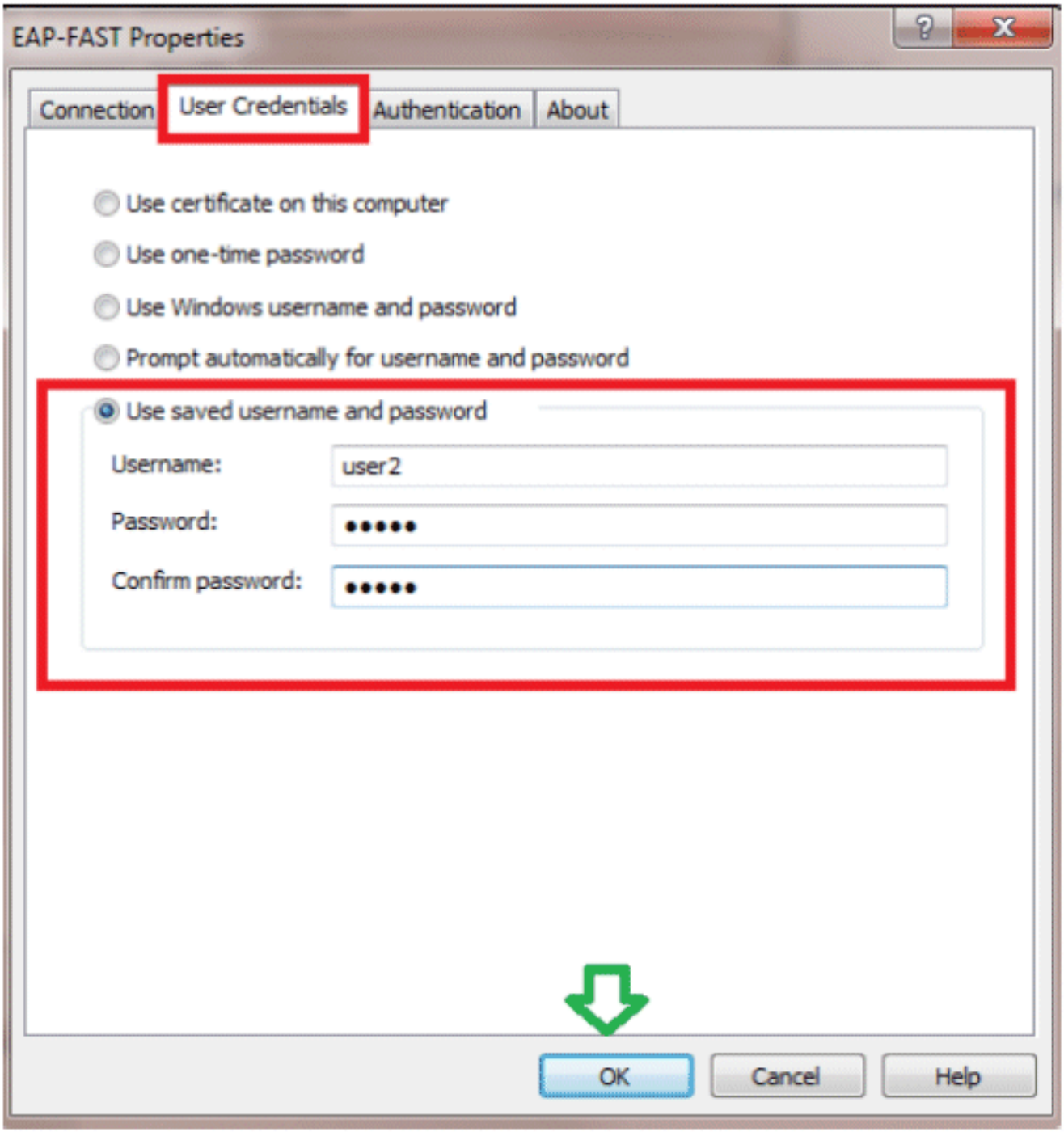




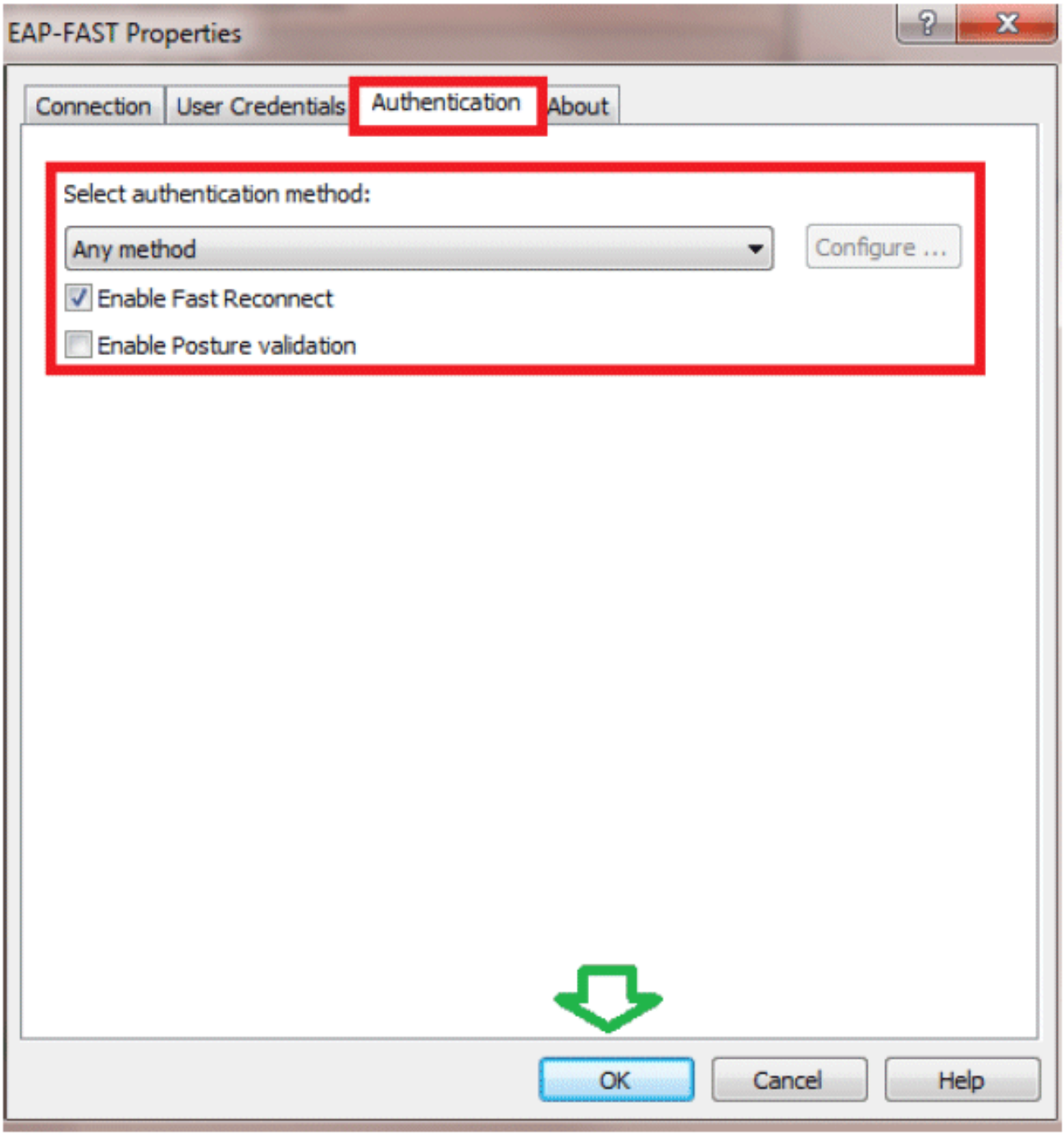
8. Activez **Allow automatic PAC provisioning** et assurez-vous que **Validate server certificate** est décoché.



9. Cliquez sur l'onglet **User Credentials**, et entrez les identifiants de l'utilisateur user2. Vous pouvez également utiliser vos informations d'identification Windows pour vous connecter. Cependant, dans cet exemple, nous n'allons pas l'utiliser.

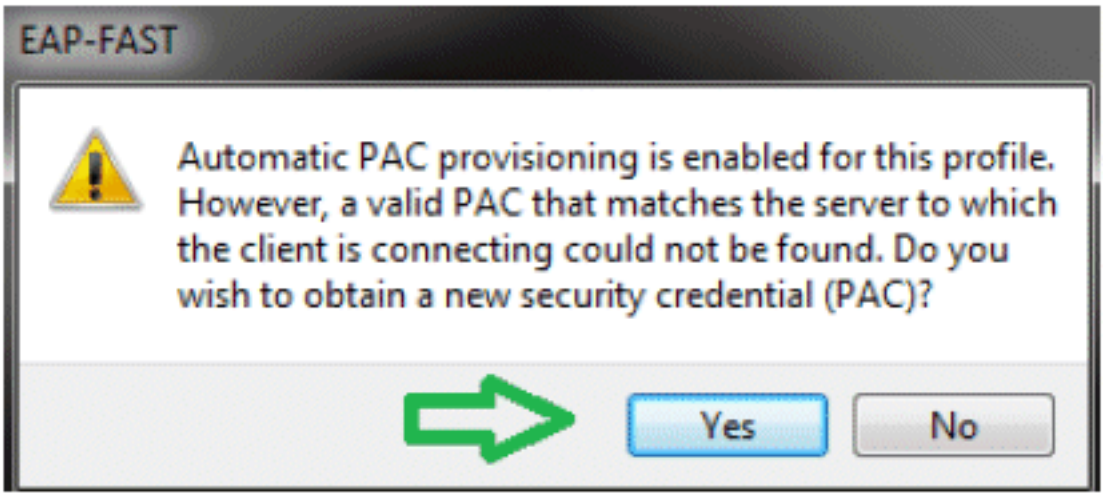

EAP-FAST Properties
Connection
User Credentials
Authentication
About
Use certificate on this computer
Use one-time password
Use Windows username and password
Prompt automatically for username and password
Use saved username and password
Username:
user2
Password:
Confirm password:
OK
Cancel
Help

10. Click OK.



Votre utilitaire Client est maintenant prêt à se connecter pour user2.

Remarque : lorsque l'utilisateur 2 tente de s'authentifier, le serveur RADIUS va envoyer un PAC. Acceptez le PAC afin de terminer l'authentification.



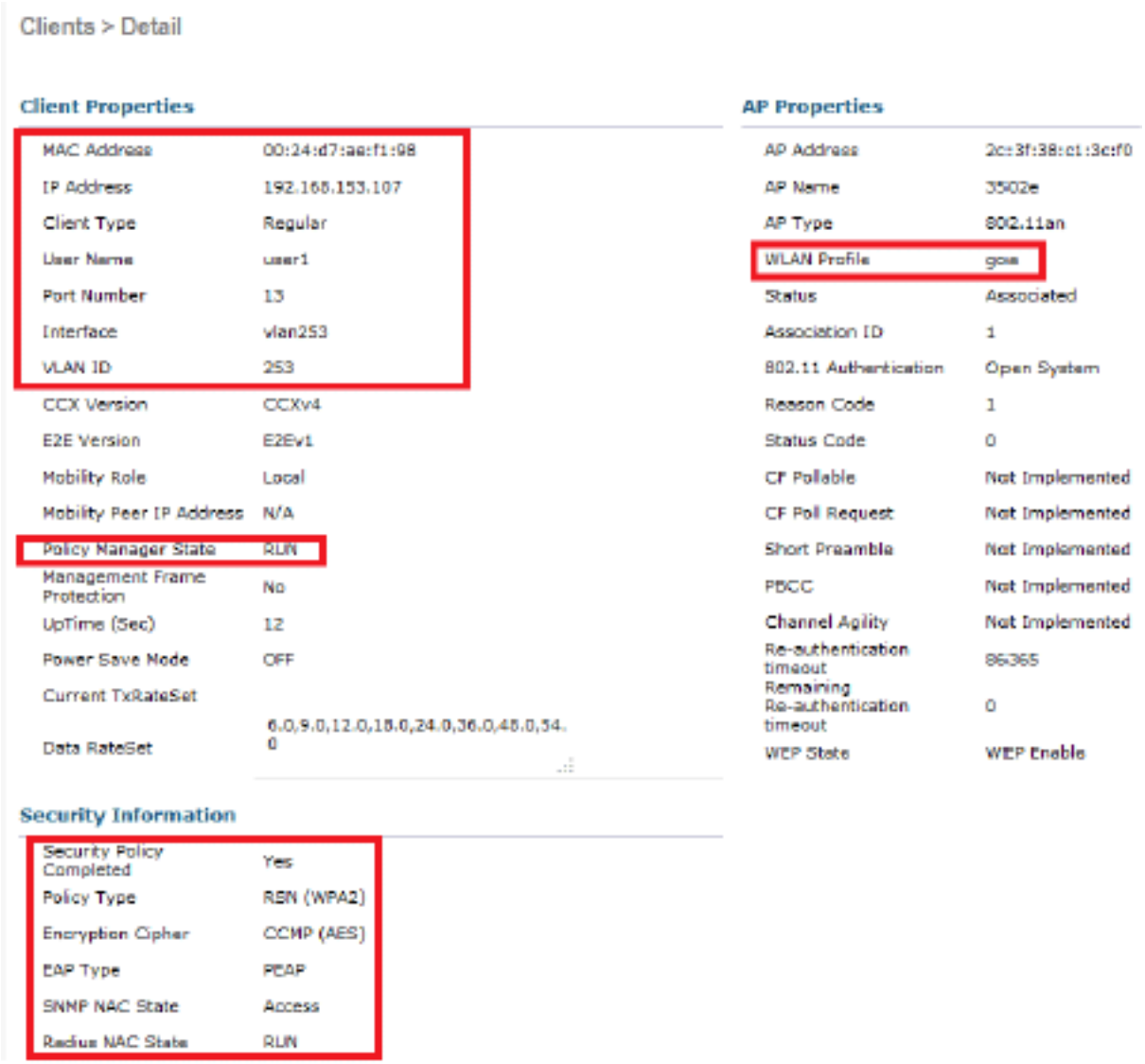
Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

Vérifier l'utilisateur 1 (PEAP-MSCHAPv2)

Dans l'interface graphique utilisateur du WLC, accédez à **Monitor > Clients**, et sélectionnez l'adresse MAC.

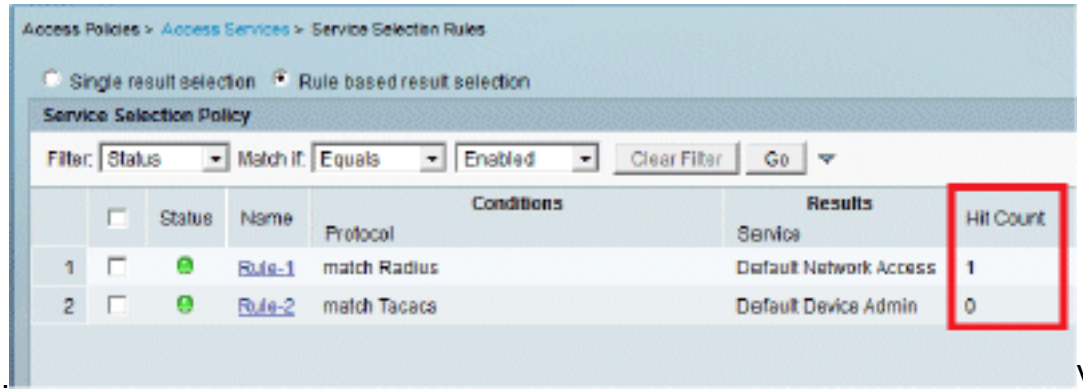


Statistiques WLC RADIUS :

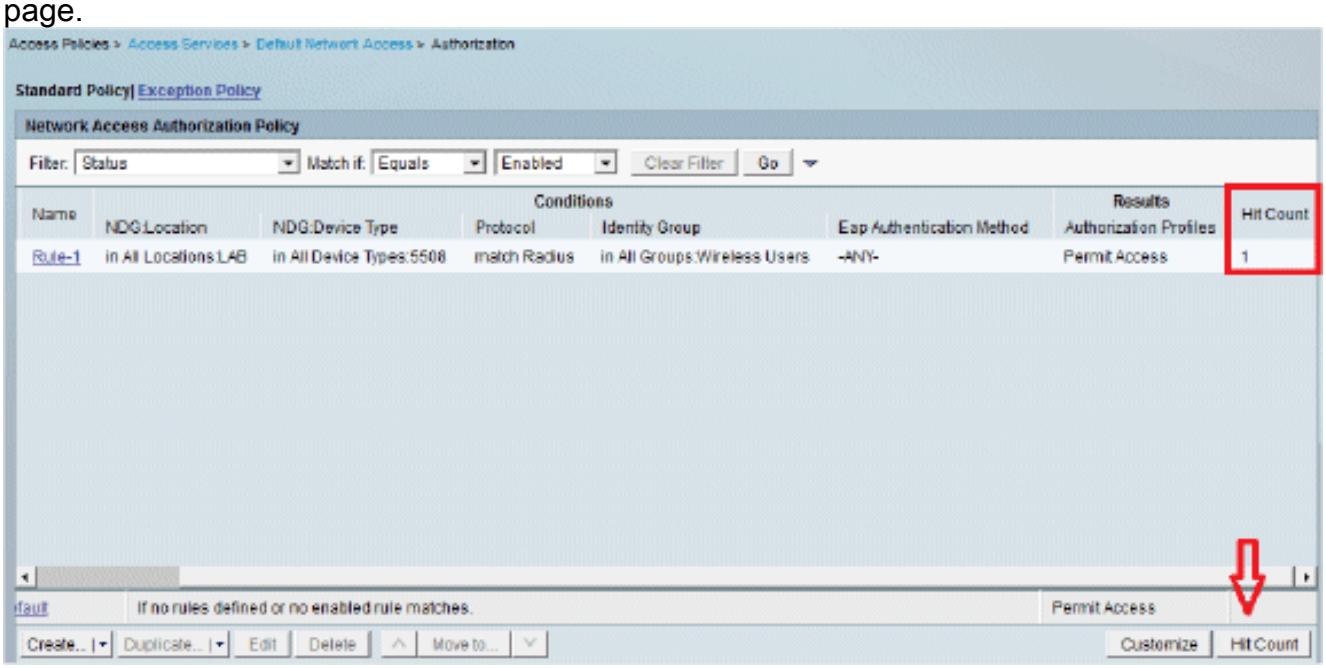
```
(Cisco Controller) >show radius auth statistics
Authentication Servers:
Server Index..................................... 1
Server Address................................... 192.168.150.24
Msg Round Trip Time.............................. 1 (msec)
First Requests................................... 8
Retry Requests................................... 0
Accept Responses................................. 1
Reject Responses................................. 0
Challenge Responses.............................. 7
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. 0
Timeout Requests................................. 0
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

Journaux ACS :

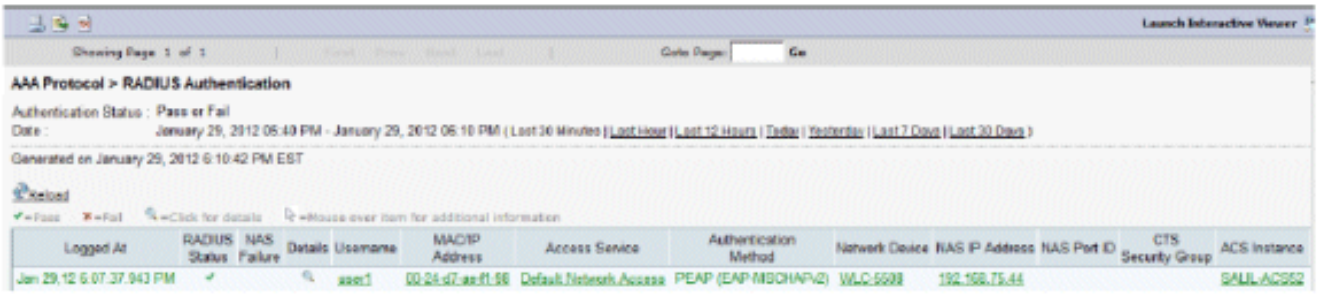
1. Complétez ces étapes afin d'afficher le nombre de succès :Si vous vérifiez les journaux dans les 15 minutes qui suivent l'authentification, assurez-vous d'actualiser le nombre

d'accès. 

Vous avez un onglet pour le **nombre de succès** au bas de la même page.



2. Cliquez sur **Surveillance et rapports** et une fenêtre contextuelle Nouveau s'affiche. Accédez à **Authentifications - Radius -Today**. Vous pouvez également cliquer sur **Details** afin de vérifier quelle règle de sélection de service a été appliquée.



Vérification de user2 (EAP-FAST)

Dans l'interface graphique utilisateur du WLC, accédez à **Monitor > Clients**, et sélectionnez l'adresse MAC.

Clients > Detail

Client Properties

MAC Address	00:24:d7:ae:f1:98
IP Address	192.168.153.111
Client Type	Regular
User Name	user2
Port Number	13
Interface	vlan253
VLAN ID	253
CCX Version	CCXv4
E2E Version	E2Ev1
Mobility Role	Local
Mobility Peer IP Address	N/A
Policy Manager State	RUN
Management Frame Protection	No
UpTime (Sec)	29
Power Save Mode	OFF
Current TxRateSet	m15
Data RateSet	6.0,9.0,12.0,18.0,24.0,36.0,48.0,54.0

AP Properties

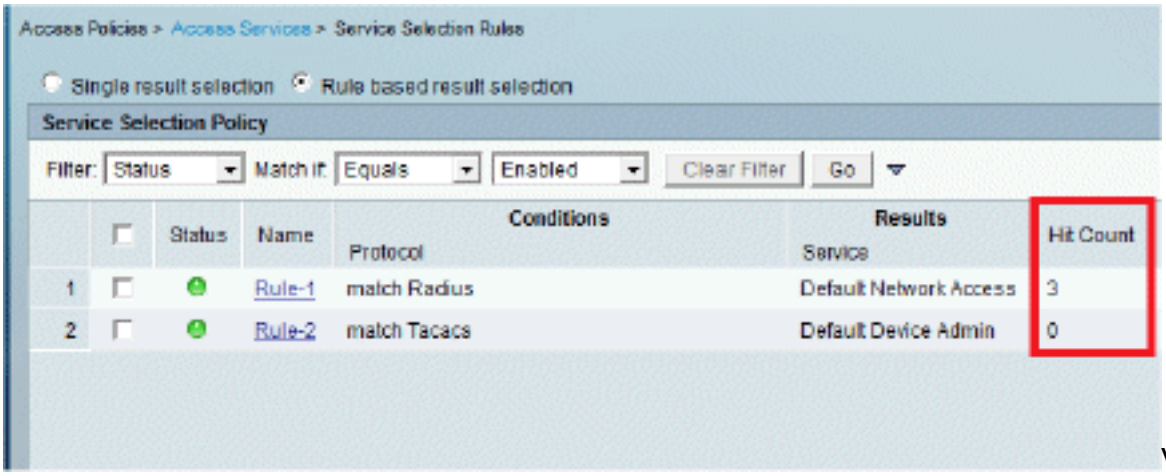
AP Address	2c:3f:38:c1:3c:f0
AP Name	3502e
AP Type	802.11an
WLAN Profile	goa
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	1
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Re-authentication timeout	86392
Remaining Re-authentication timeout	0
WEP State	WEP Enable

Security Information

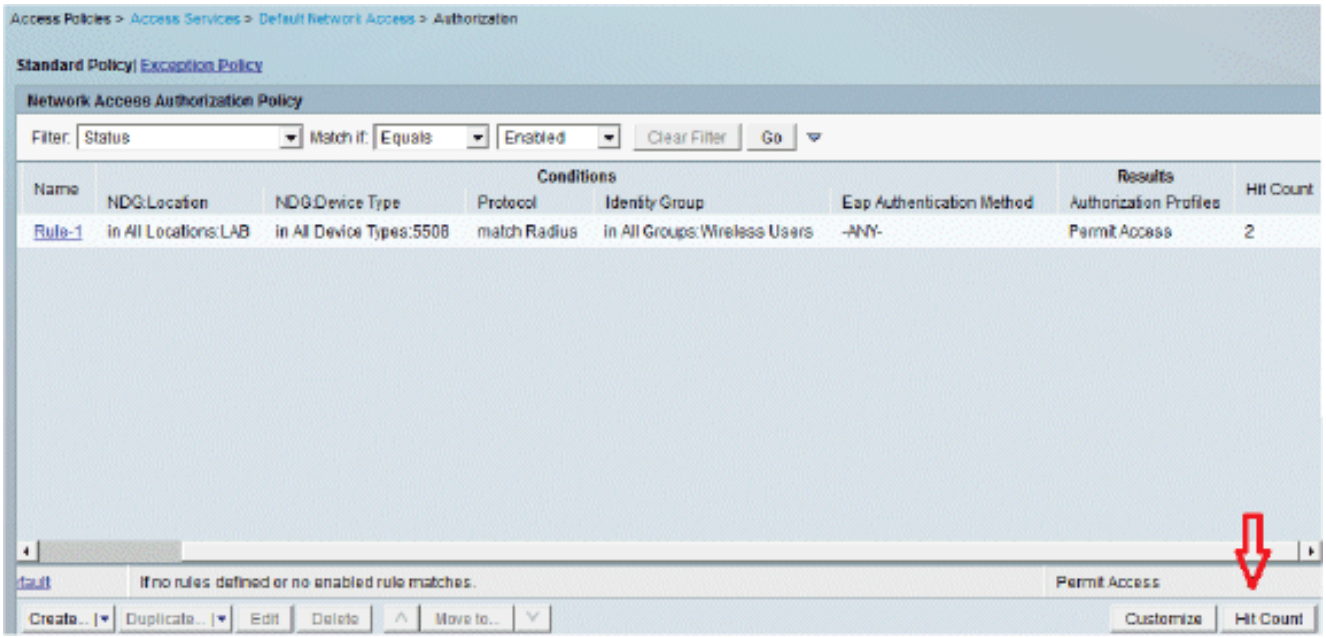
Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	EAP-FAST
SNMP NAC State	Access
Radius NAC State	RUN

Journaux ACS :

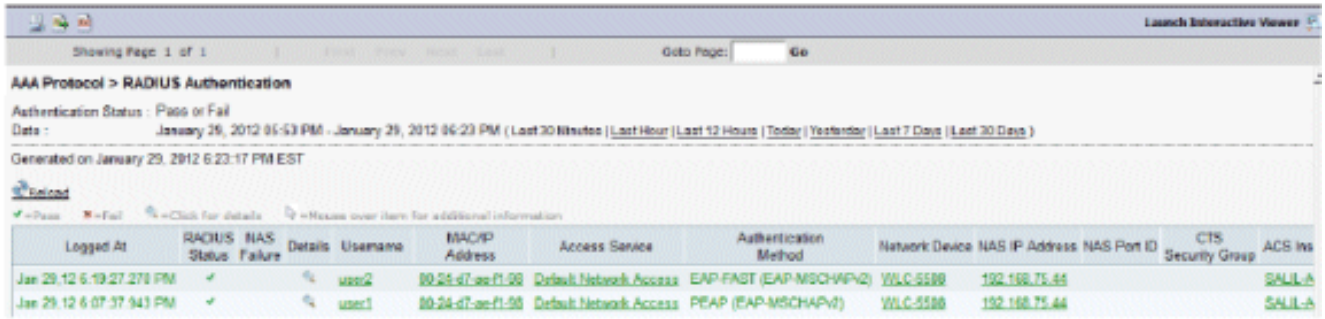
1. Complétez ces étapes afin d'afficher le nombre de succès :Si vous vérifiez les journaux dans les 15 minutes qui suivent l'authentification, assurez-vous d'actualiser le nombre d'occurrences.



Vous avez un onglet pour le **nombre de succès** au bas de la même page.



2. Cliquez sur **Surveillance et rapports** et une fenêtre contextuelle Nouveau s'affiche. Accédez à **Authentifications - Radius -Today**. Vous pouvez également cliquer sur **Details** afin de vérifier quelle règle de sélection de service a été appliquée.



Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Dépannage des commandes

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

1. Si vous rencontrez des problèmes, émettez ces commandes sur le WLC :**debug client *<mac add of the client>*debug aaa all enableshow client detail *<mac addr>*** - Vérifiez l'état du gestionnaire de stratégies.**show radius auth statistics** - Vérifiez la raison de l'échec.**debug disable-all** - Désactivez les débogages.**clear stats radius auth all** - Effacer les statistiques de rayon sur le WLC.
2. Vérifiez les journaux dans l'ACS et notez la raison de l'échec.

Informations connexes

- Assistance et documentation techniques - Cisco Systems

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.

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.