Configurez l'authentification de 802.1x avec le PEAP, l'ISE 2.1 et le WLC 8.3

Contenu

Introduction

Ceci documente décrit comment installer un réseau local sans fil (WLAN) avec la Sécurité de 802.1x et le dépassement virtuel du réseau local (VLAN) avec le Protected Extensible Authentication Protocol (PEAP) comme Protocole EAP (Extensible Authentication Protocol).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- 802.1x
- PEAP
- Autorité de certification (CA)
- Certificats

Composants utilisés

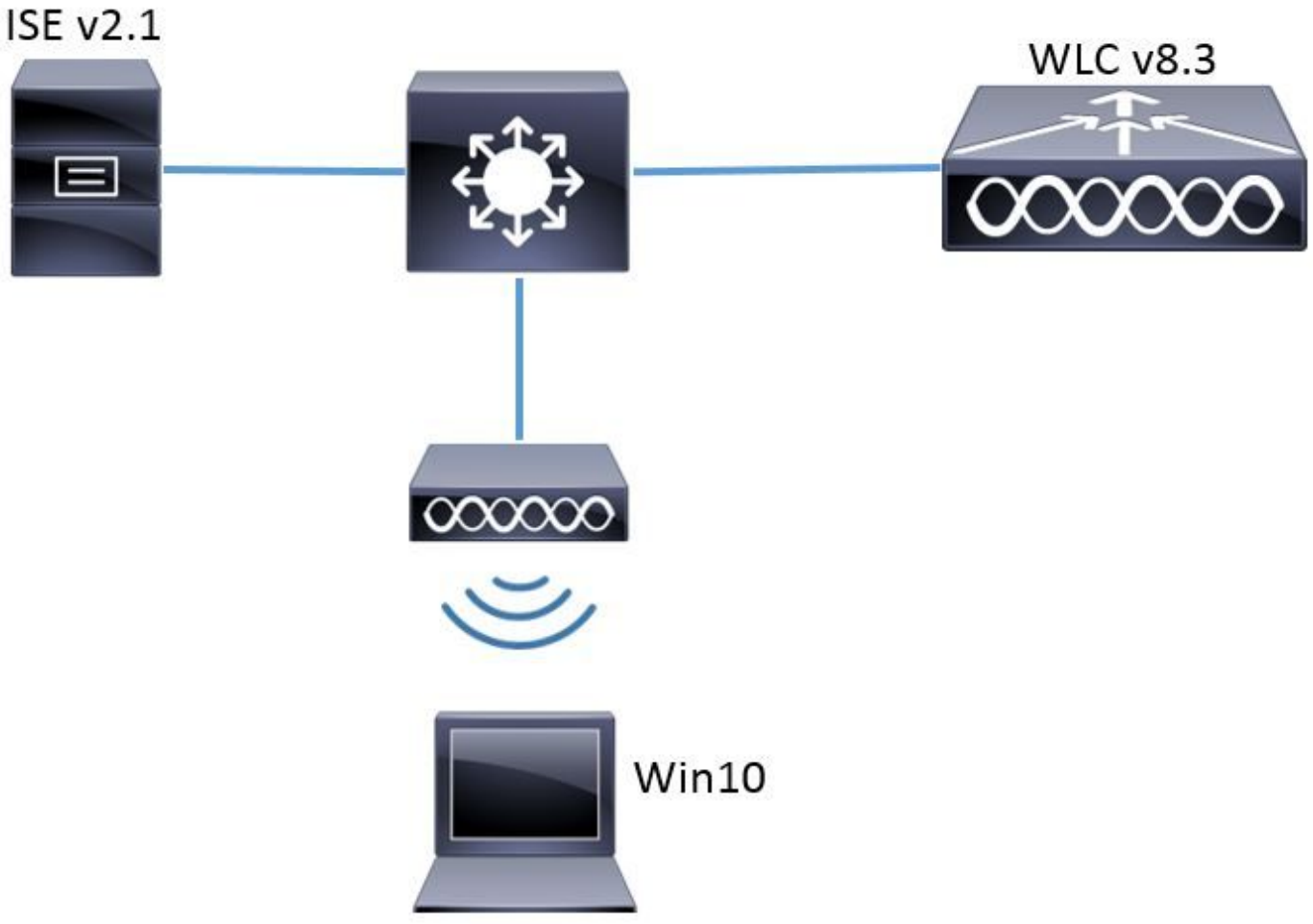
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- WLC v8.3.102.0
- Engine de gestion d'identité (ISE) v2.1
- Ordinateur portable de Windows 10

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

Diagramme du réseau



Configuration

Les étapes générales sont :

1. Déclarez le serveur de RAYON sur WLC et vice versa pour permettre la transmission les uns avec les autres.

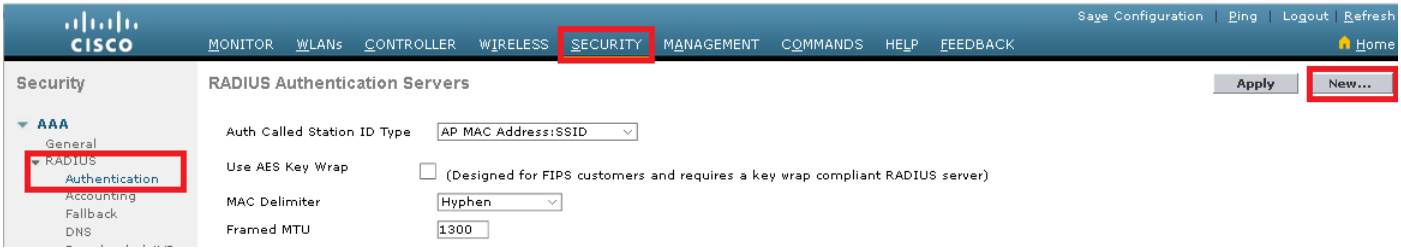
2. Créez l'Identifiant SSID (Service Set Identifier) dans le WLC.
3. Créez la règle d'authentification sur ISE.
4. Créez le profil d'autorisation sur ISE.
5. Créez la règle d'autorisation sur ISE.
6. Configurez le point final.

Déclarez le serveur de RAYON sur WLC

Afin de permettre la transmission entre le serveur de RAYON et le WLC, il est nécessaire pour enregistrer le serveur de RAYON sur WLC et vice versa.

GUI :

Étape 1. Ouvrez le GUI du WLC et naviguez vers le **Security > Radius > Authentication > nouveau** suivant les indications de l'image.



Étape 2. Écrivez les informations du serveur de RAYON suivant les indications de l'image.

CLI :

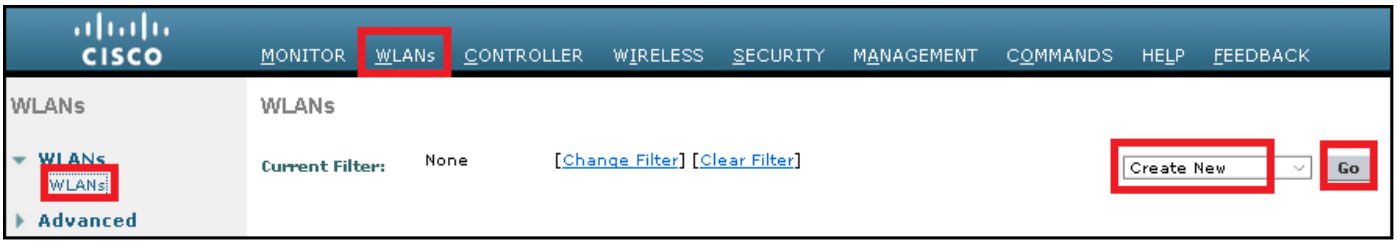
```
> config radius auth add <index> <a.b.c.d> 1812 ascii <shared-key>
> config radius auth disable <index>
> config radius auth retransmit-timeout <index> <timeout-seconds>
```

```
> config radius auth enable <index>
```
<a.b.c.d> correspond au serveur de RAYON.

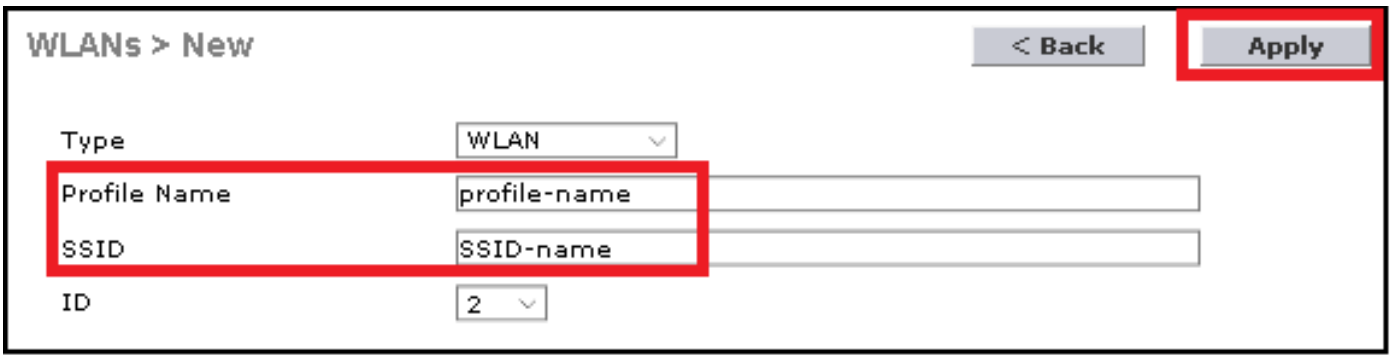
Créez le SSID

GUI :

Étape 1. Ouvrez le GUI du WLC et naviguez vers des **WLAN > créent nouveau > vont** suivant les indications de l'image.



Étape 2. Choisissez un nom pour le SSID et le profil, puis cliquez sur Apply **suivant les indications de l'image.**



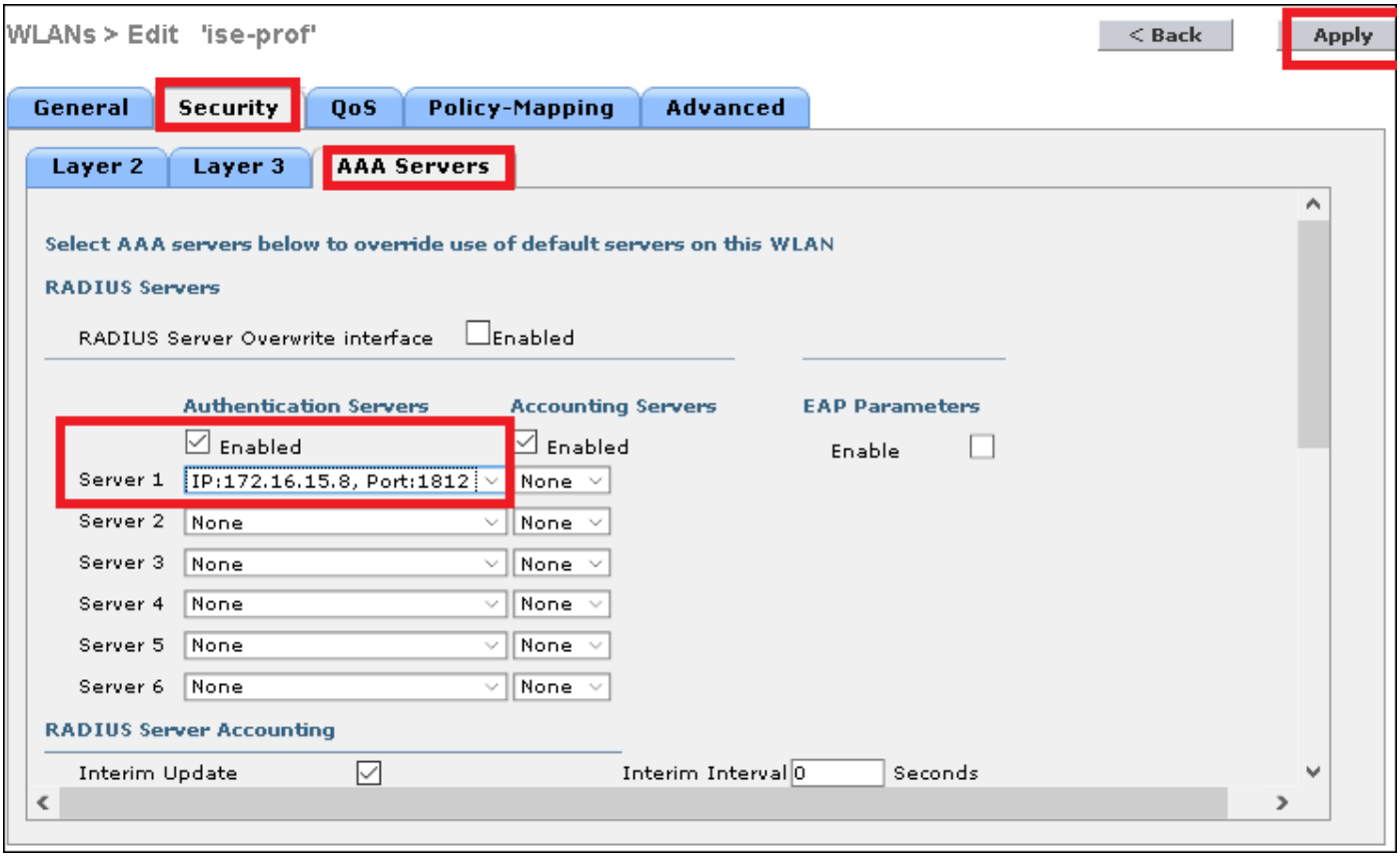
CLI :

```
> config wlan create <id> <profile-name> <ssid-name>
```
Étape 3. Affectez le serveur de RAYON au WLAN.

CLI :

```
> config wlan radius_server auth add <wlan-id> <radius-index>
```
GUI :

Naviguez vers le **Security > AAA Servers** et choisissez le serveur désiré de RAYON, puis le hit **s'appliquent** suivant les indications de l'image.



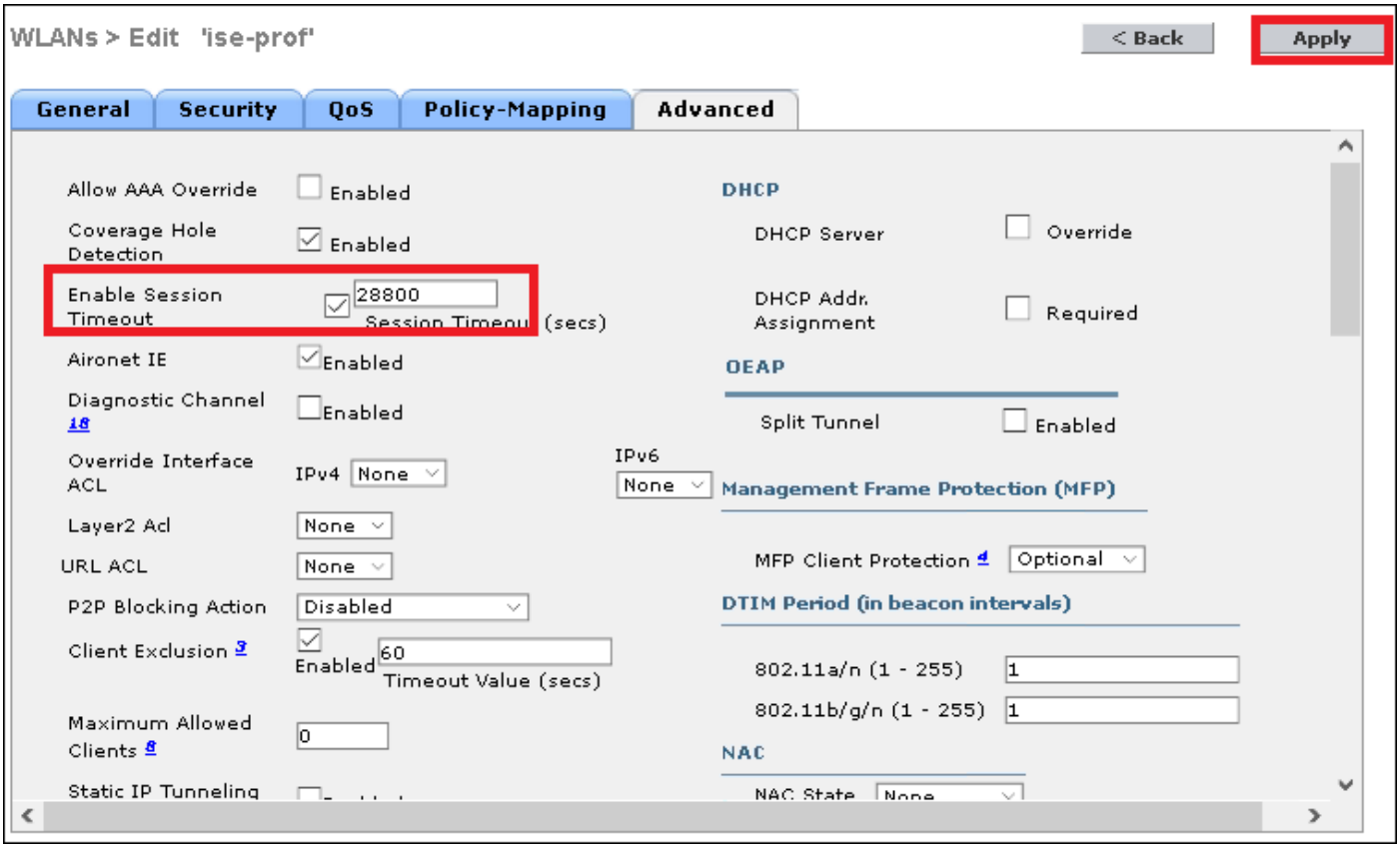
Étape 4. Augmentez sur option le délai d'attente de session

CLI :

```
> config wlan session-timeout <wlan-id> <session-timeout-seconds>
```

GUI :

Naviguez vers des **WLAN > ID de WLAN > a avancé** et spécifie la Session Timeout suivant les indications de l'image.



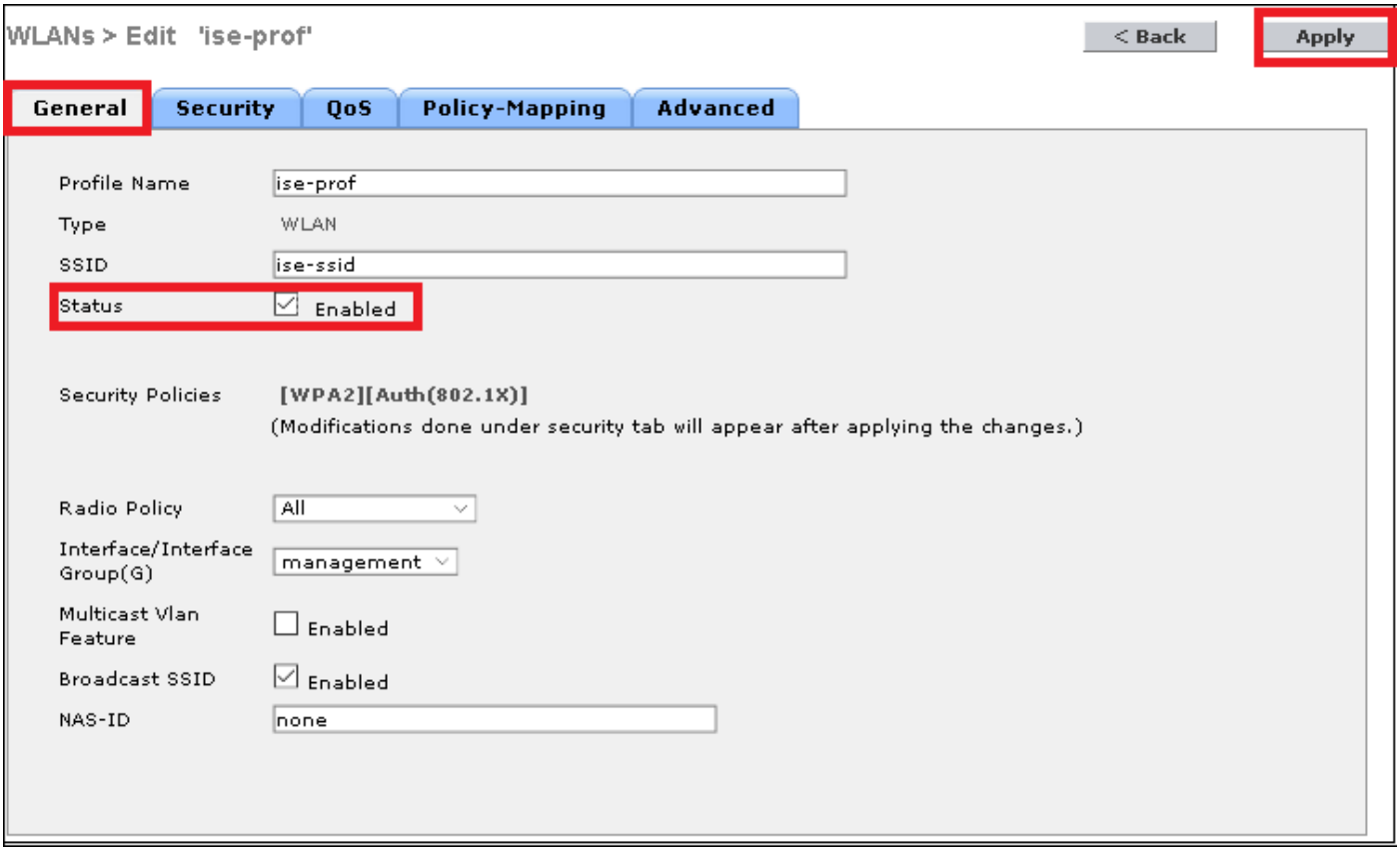
Étape 5. Activez le WLAN.

CLI :

```
> config wlan enable <wlan-id>
```

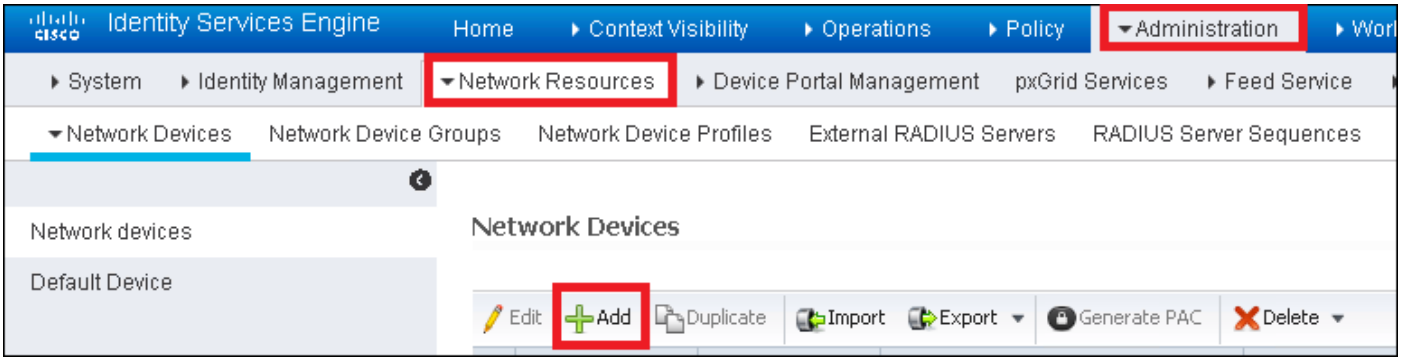
GUI :

Naviguez vers des **WLAN > ID de WLAN > général** et activez le SSID suivant les indications de l'image.



Déclarez WLC sur ISE

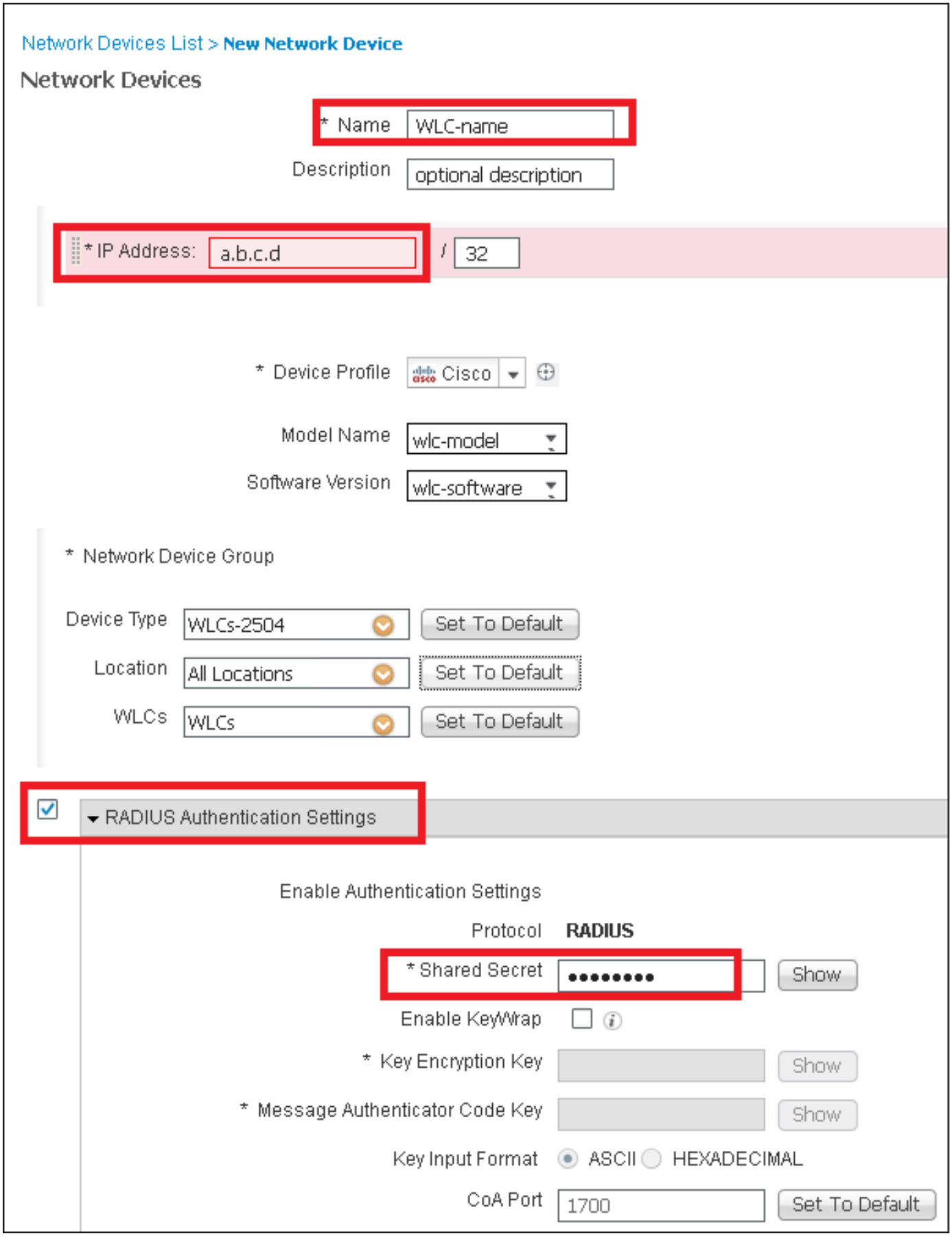
Étape 1. Ouvrez la console ISE et naviguez vers la **gestion > les ressources de réseau > les périphériques de réseau > ajoutent** suivant les indications de l'image.



Étape 2. Écrivez les valeurs.

Sur option, il peut être un nom modèle spécifié, version de logiciel, description et affecter des groupes de périphériques réseau basés sur des types de périphérique, l'emplacement ou le WLCs.

a.b.c.d correspondent à l'interface du WLC qui envoie l'authentification demandée. Par défaut c'est l'interface de gestion suivant les indications de l'image.

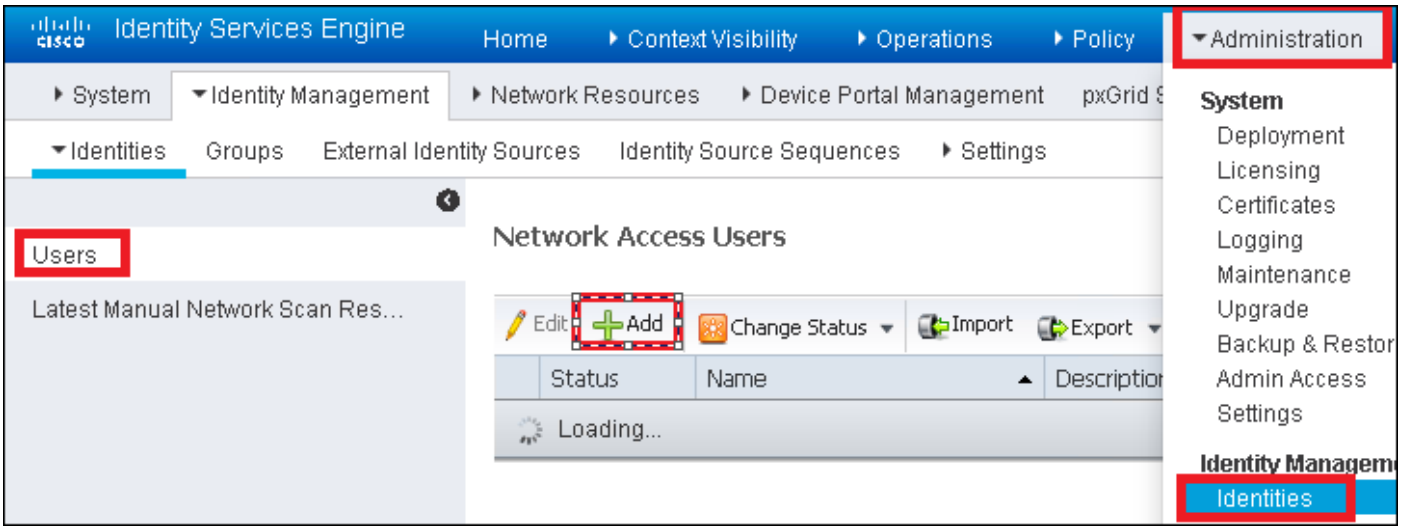


Pour plus d'informations sur des **groupes de périphériques réseau** examinez ce lien :

[ISE - Groupes de périphériques réseau]

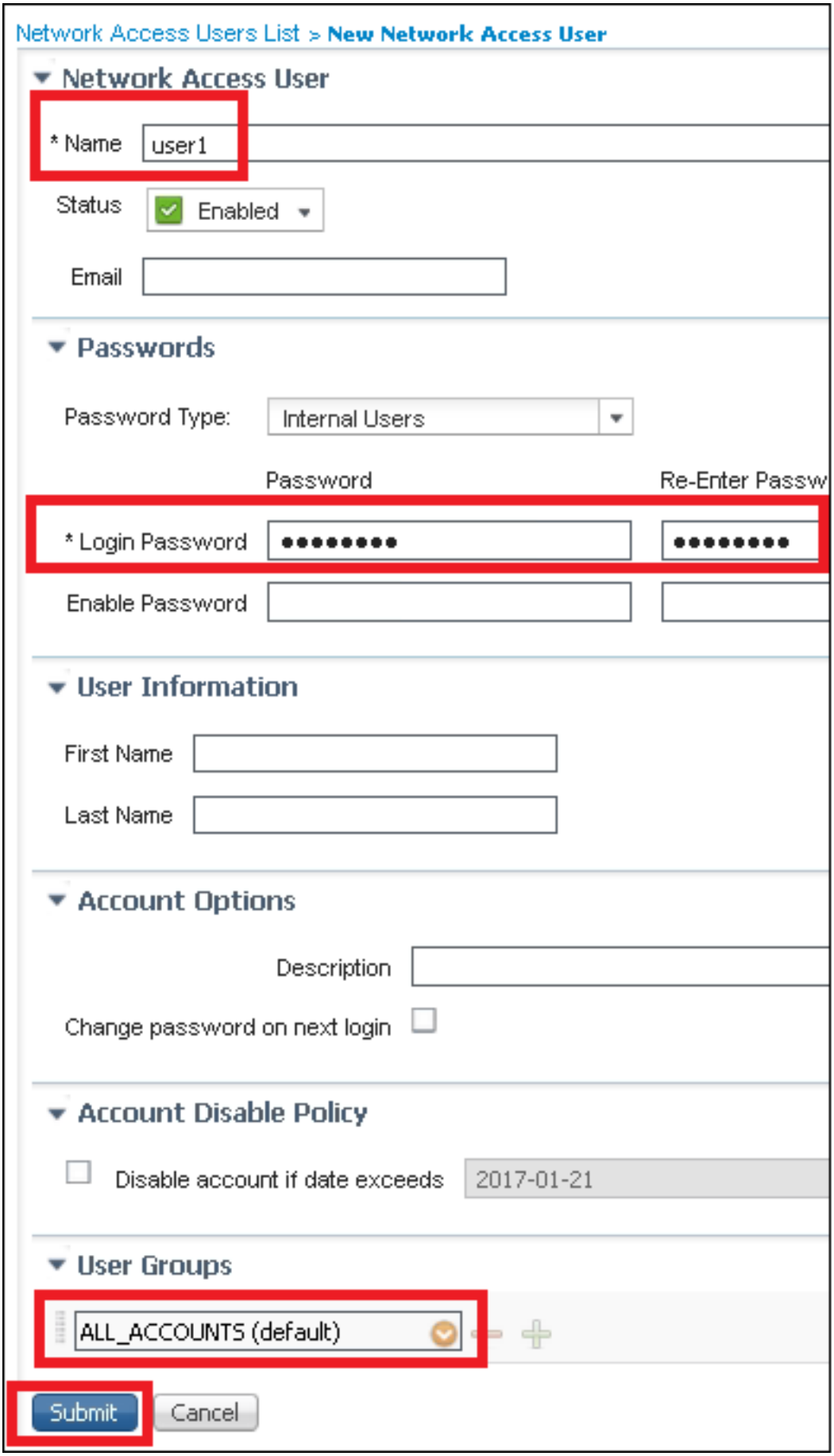
Créez le nouvel utilisateur sur ISE

Étape 1. Naviguez vers la **gestion > la Gestion de l'identité > les identités > les utilisateurs > ajoutent** suivant les indications de l'image.



Étape 2. Écrivez les informations.

Dans cet exemple, cet utilisateur appartient à un groupe appelé l'ALL_ACCOUNTS mais il peut être ajusté comme nécessaire suivant les indications de l'image.

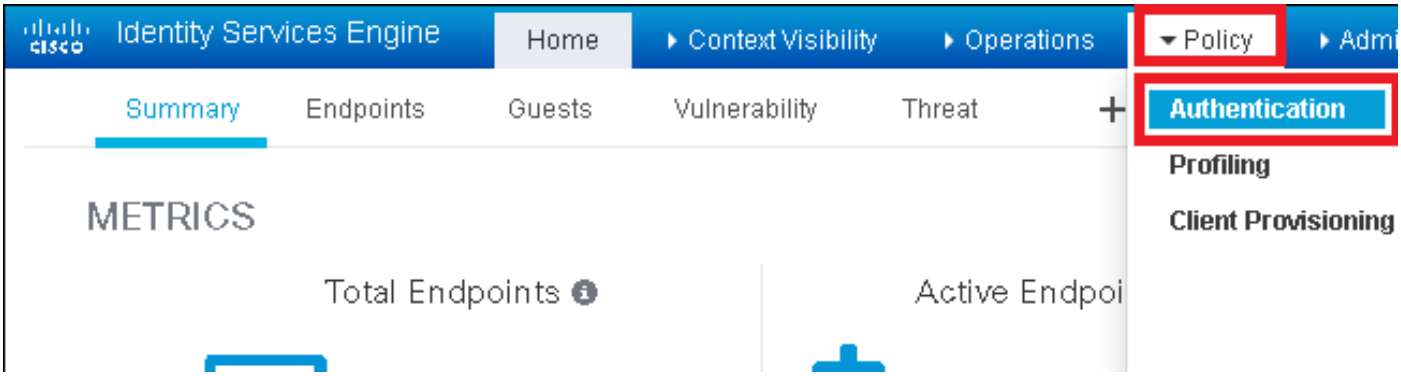


Créez la règle d'authentification

Des règles d'authentification sont utilisées de vérifier si les qualifications des utilisateurs sont juste (vérifiez si l'utilisateur est vraiment qui il indique qu'il est) et limiter les méthodes

d'authentification qui sont permises pour être utilisées par lui.

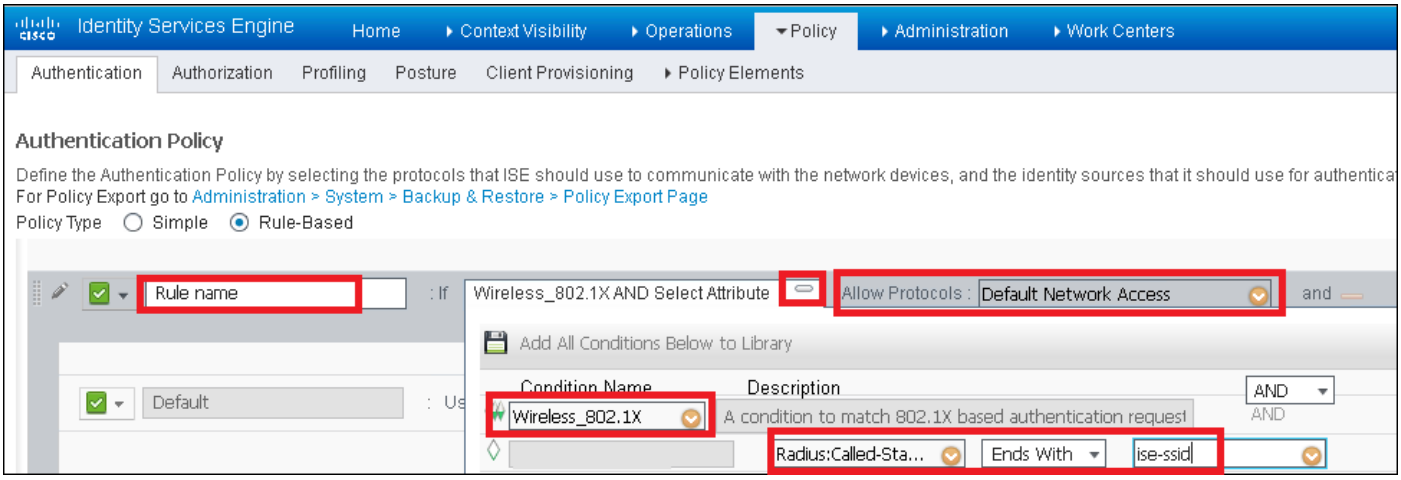
Étape 1. Naviguez vers la **stratégie > l'authentification** suivant les indications de l'image.



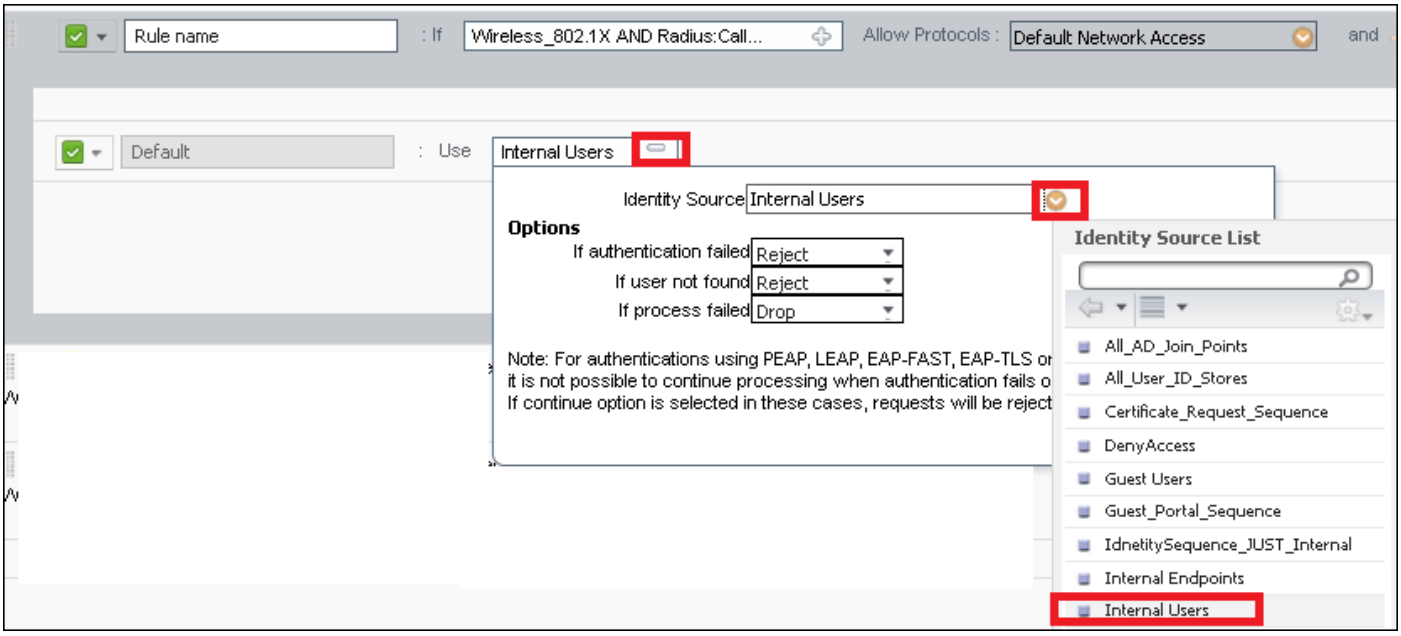
Étape 2. Insérez une nouvelle règle d'authentification suivant les indications de l'image.

Étape 3. Écrivez les valeurs.

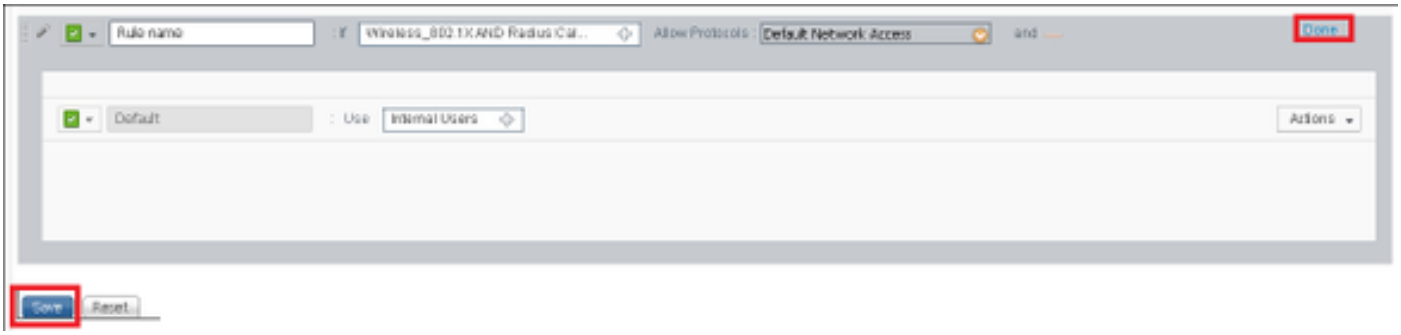
Cette règle d'authentification permet tous les protocoles répertoriés sous la liste d'**accès au réseau par défaut**, ceci s'applique à la demande d'authentification pour les clients Sans fil de 802.1x et avec l'Appeler-Station-ID et finit avec ise-**SSID** suivant les indications de l'image.



En outre, choisissez la source d'identité pour les clients qui apparie cette règle d'authentification. Cet exemple utilise la liste d'origine d'identité d'**utilisateurs internes** suivant les indications de l'image.



Une fois que terminé, cliquez sur **fait** et **sauvegardez** suivant les indications de l'image.



Pour plus d'informations sur permettez les protocoles que les stratégies consultent ce lien :

Service permis de protocoles

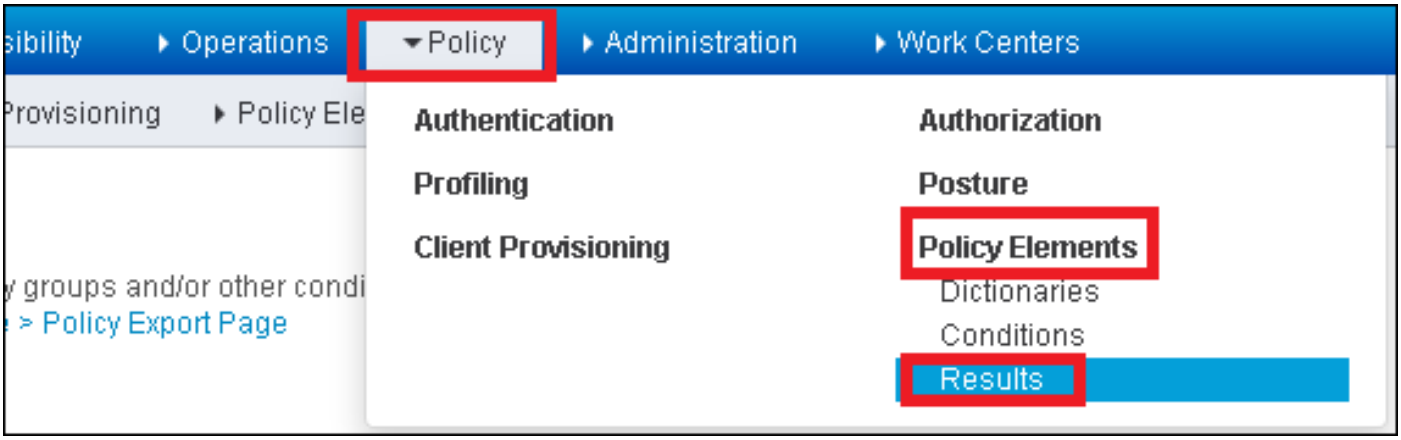
Pour plus d'informations sur l'identité les sources consultent ce lien :

Créez un groupe d'identité de l'utilisateur

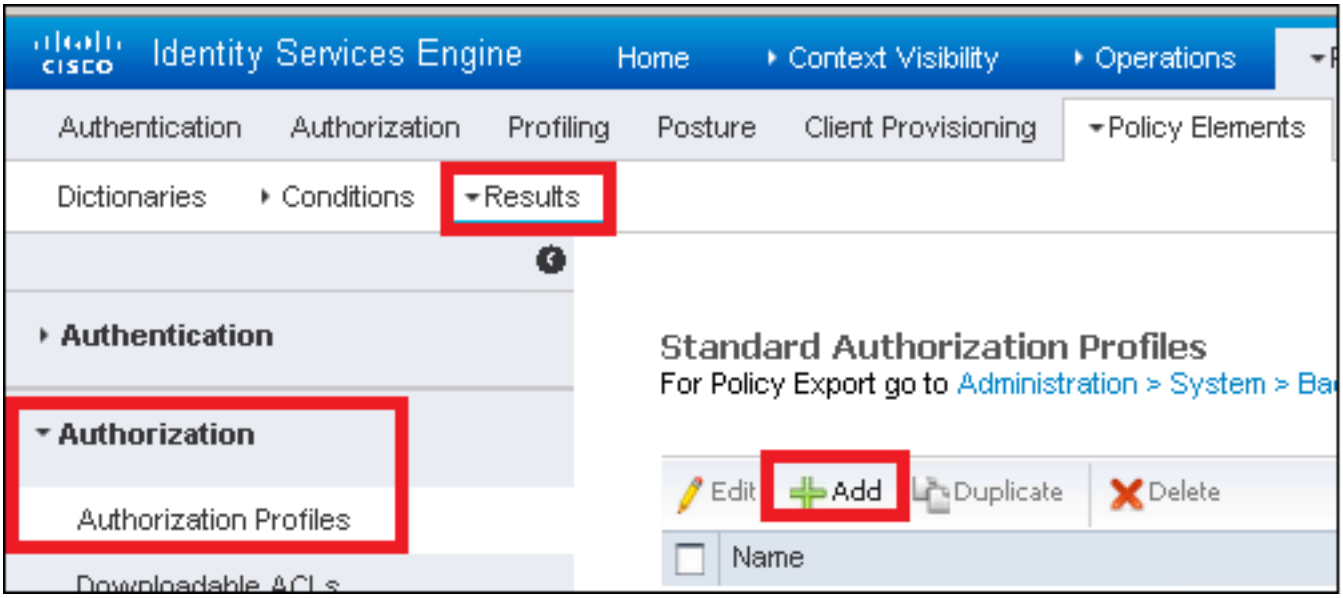
Créez le profil d'autorisation

Le profil d'autorisation détermine si le client a accès ou pas au réseau, au Listes de contrôle d'accès (ACL) de pousser, au dépassement VLAN ou à n'importe quel autre paramètre. Le profil d'autorisation affiché dans cet exemple envoie un accès reçoivent pour le client et affectent le client à VLAN 2404.

Étape 1. Naviguez vers la **stratégie > les éléments > les résultats de stratégie** suivant les indications de l'image.



Étape 2. Ajoutez un nouveau profil d'autorisation. Naviguez vers l'**autorisation > les profils d'autorisation > ajoutent** suivant les indications de l'image.



Étape 3. Écrivez les valeurs suivant les indications de l'image.