

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

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurations](#)

[Déclarez le serveur de RAYON sur WLC](#)

[Créez le SSID](#)

[Déclarez le WLC sur ISE](#)

[Créez un nouvel utilisateur sur ISE](#)

[Créez la règle d'authentification](#)

[Créez le profil d'autorisation](#)

[Créez la règle d'autorisation](#)

[Configuration de périphérique d'extrémité](#)

[Vérifiez](#)

[Procédure d'authentification sur WLC](#)

[Procédure d'authentification sur ISE](#)

Introduction

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

Conditions préalables

Cisco recommande d'avoir une connaissance de base de :

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

Conditions requises

[Composants utilisés](#)

WLC v8.3.102.0

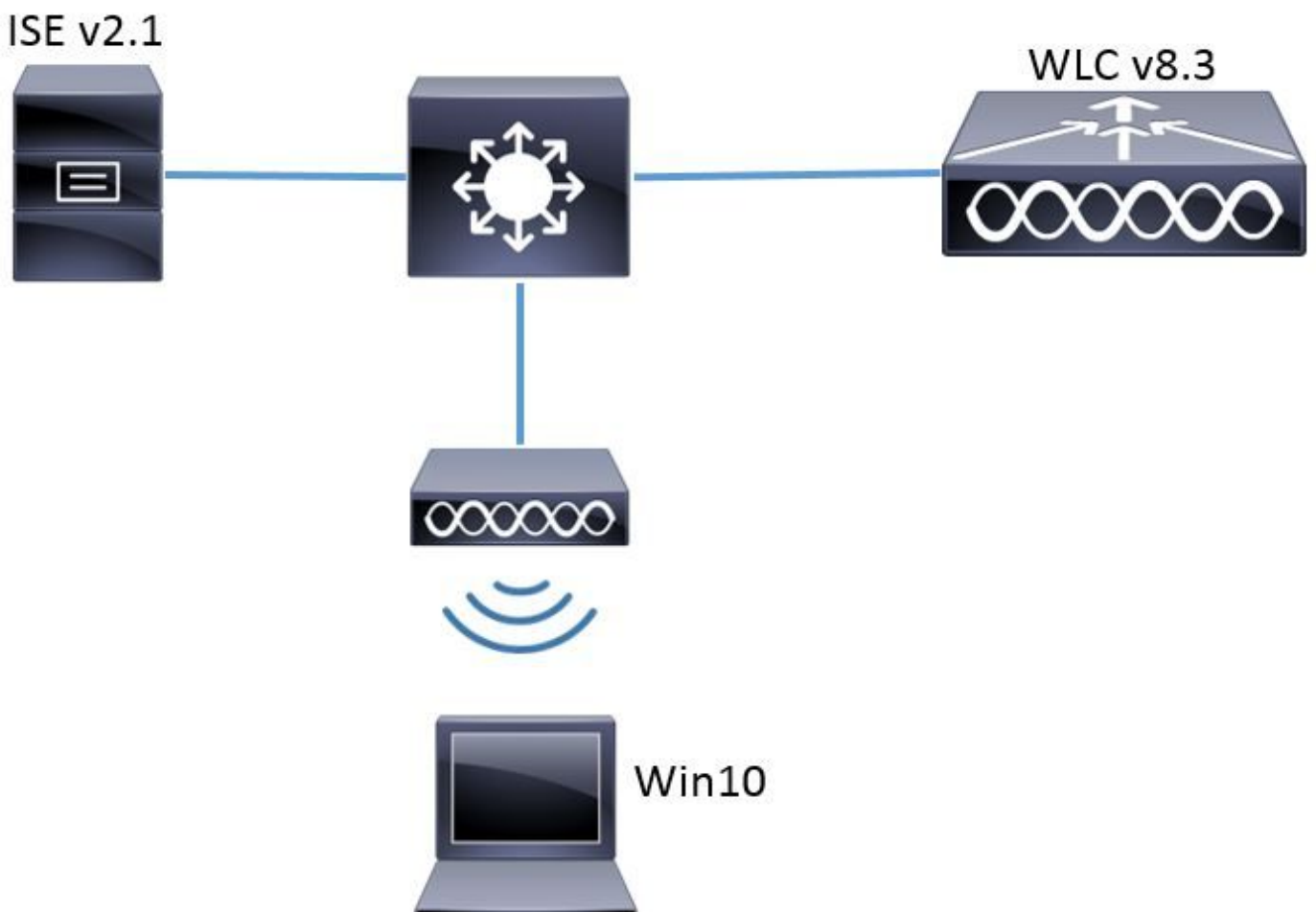
ISE v2.1

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



Configurations

Les étapes générales sont :

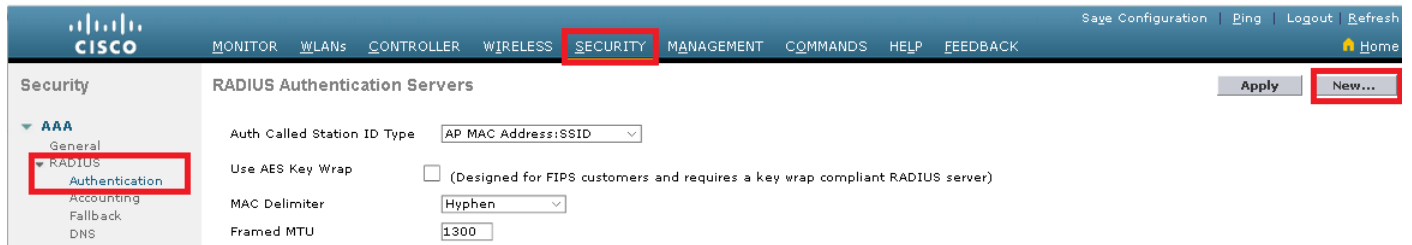
1. Déclarez le serveur de RAYON (ISE dans cet exemple) sur WLC et vice versa pour permettre la transmission les uns avec les autres
2. Créez le SSID (identifiant d'ensemble de services) dans le WLC
3. Créez la règle d'authentification sur ISE
4. Créez le profil d'autorisation sur ISE
5. Créez la règle 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**.



Étape 2. Remplissez informations du serveur de RAYON.

RADIUS Authentication Servers > New

Server Index (Priority)	2
Server IP Address(Ipv4/Ipv6)	a.b.c.d
Shared Secret Format	ASCII
Shared Secret	••••••••
Confirm Shared Secret	••••••••
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for CoA	Disabled
Server Timeout	10 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
Management Retransmit Timeout	2 seconds
IPSec	<input type="checkbox"/> Enable

CLI :

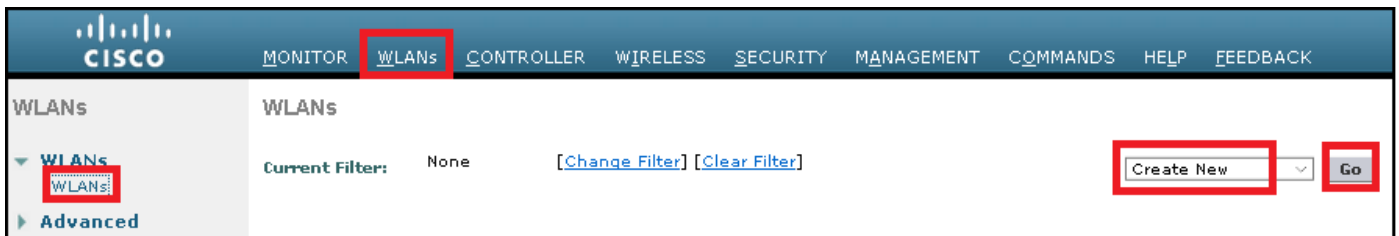
```
> config radius auth add <index> <a.b.c.d> 1812 ascii <shared-key>> config radius auth disable <index>> config radius auth retransmit-timeout <index> <timeout-seconds>> config radius auth enable <index>
```

<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**.



Étape 2. Choisissez un nom pour le SSID et le profil, puis cliquez sur Apply.

CLI :

```
> config wlan create <id> <profile-name> <ssid-name>
```

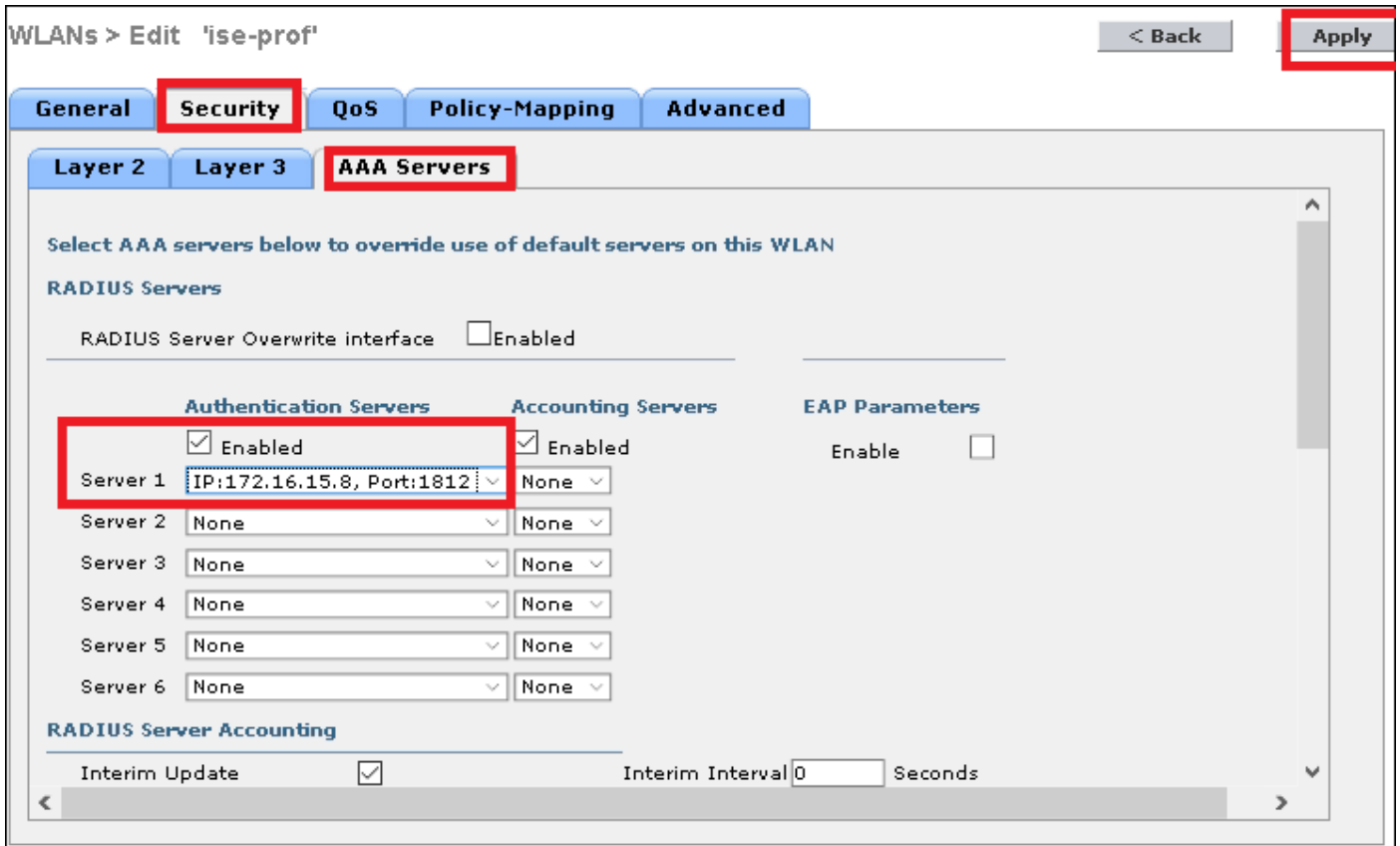
Étape 3. Affectez le serveur de RAYON au WLAN.

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.



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

CLI :

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

GUI :

WLANs > Edit 'ise-prof' < Back Apply

General Security QoS Policy-Mapping Advanced

Allow AAA Override	<input type="checkbox"/> Enabled	DHCP	
Coverage Hole Detection	<input checked="" type="checkbox"/> Enabled	DHCP Server	<input type="checkbox"/> Override
Enable Session Timeout	<input checked="" type="checkbox"/> <input type="text" value="28800"/> Session Timeout (secs)	DHCP Addr. Assignment	<input type="checkbox"/> Required
Aironet IE	<input checked="" type="checkbox"/> Enabled	OEAP	
Diagnostic Channel	<input type="checkbox"/> Enabled	Split Tunnel	<input type="checkbox"/> Enabled
Override Interface ACL	IPv4 <input type="text" value="None"/> IPv6 <input type="text" value="None"/>	Management Frame Protection (MFP)	
Layer2 Ad	<input type="text" value="None"/>	MFP Client Protection	<input type="text" value="Optional"/>
URL ACL	<input type="text" value="None"/>	DTIM Period (in beacon intervals)	
P2P Blocking Action	<input type="text" value="Disabled"/>	802.11a/n (1 - 255)	<input type="text" value="1"/>
Client Exclusion	<input checked="" type="checkbox"/> Enabled <input type="text" value="60"/> Timeout Value (secs)	802.11b/g/n (1 - 255)	<input type="text" value="1"/>
Maximum Allowed Clients	<input type="text" value="0"/>	NAC	
Static IP Tunneling	<input type="checkbox"/> ...	NAC State	<input type="text" value="None"/>

Étape 5. Activez le WLAN

CLI :

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

GUI :

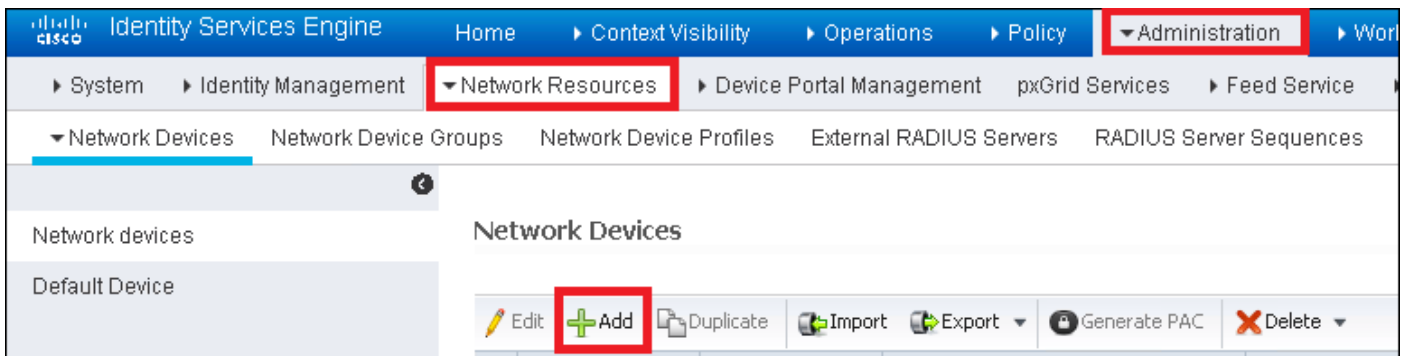
WLANs > Edit 'ise-prof' < Back Apply

General Security QoS Policy-Mapping Advanced

Profile Name	<input type="text" value="ise-prof"/>
Type	WLAN
SSID	<input type="text" value="ise-ssid"/>
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	<input type="text" value="All"/>
Interface/Interface Group(G)	<input type="text" value="management"/>
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
NAS-ID	<input type="text" value="none"/>

Déclarez le WLC sur ISE

Étape 1. Ouvrez la console ISE et naviguez vers la **gestion > les ressources de réseau > les périphériques de réseau > ajoutent.**



Étape 2. Remplissez informations

Sur option il peut être spécifié un nom modèle, 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.

Network Devices

* Name

Description

* IP Address: /

* Device Profile

Model Name

Software Version

* Network Device Group

Device Type

Location

WLCs

Enable Authentication Settings

Protocol **RADIUS**

* Shared Secret

Enable KeyWrap

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL

CoA Port

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

[ISE - Groupes de périphériques réseau](#)

Créez un nouvel utilisateur sur ISE

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

The screenshot displays the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', and 'Policy'. The left sidebar shows 'System', 'Identity Management', 'Network Resources', and 'Device Portal Management'. The main content area is titled 'Network Access Users' and features a toolbar with 'Edit', 'Add', 'Change Status', 'Import', and 'Export' buttons. Below the toolbar is a table with columns for 'Status', 'Name', and 'Description', which is currently showing a 'Loading...' message. The right-hand navigation menu is expanded, showing 'Administration' and 'Identities' highlighted with red boxes. The 'Users' link in the left sidebar is also highlighted with a red box.

Étape 2. Remplissez informations

Dans cet exemple cet utilisateur appartient à un groupe appelé l'ALL_ACCOUNTS mais il peut être ajusté comme nécessaire.

▼ **Network Access User**

* Name

Status Enabled ▼

Email

▼ **Passwords**

Password Type: ▼

Password

Re-Enter Passw

* Login Password

Enable Password

▼ **User Information**

First Name

Last Name

▼ **Account Options**

Description

Change password on next login

▼ **Account Disable Policy**

Disable account if date exceeds

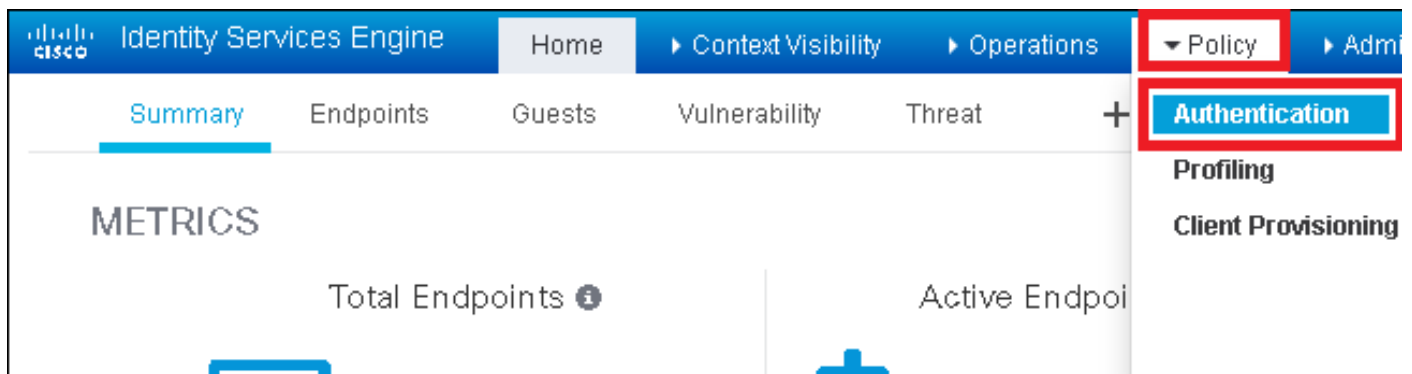
▼ **User Groups**

Créez la règle d'authentification

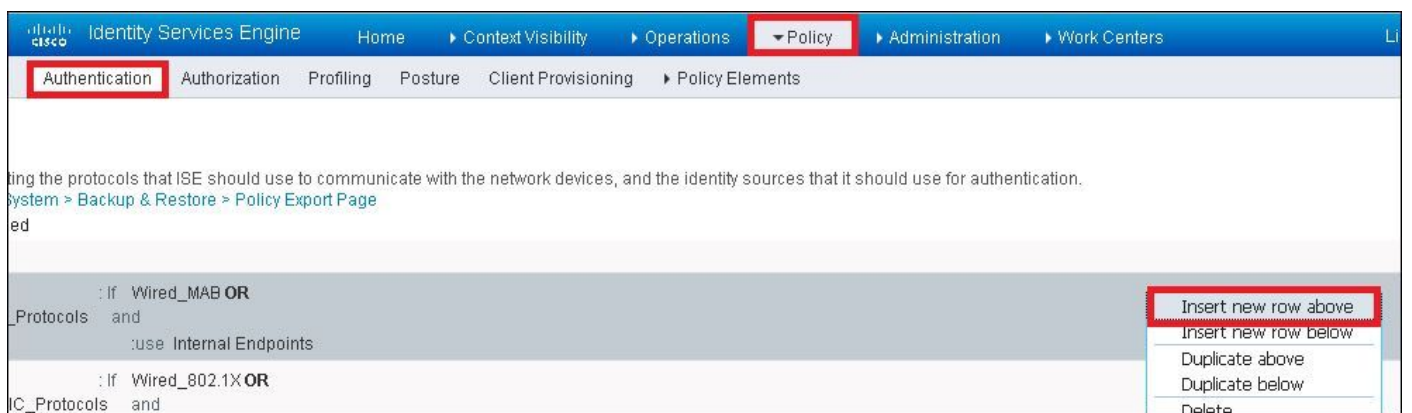
Des règles d'authentification sont utilisées de vérifier si les qualifications des utilisateurs sont juste (vérifiez si l'utilisateur est vraiment qui il indique qu'il est) et limiter les méthodes

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

Étape 1. Naviguez vers la **stratégie > l'authentification**.

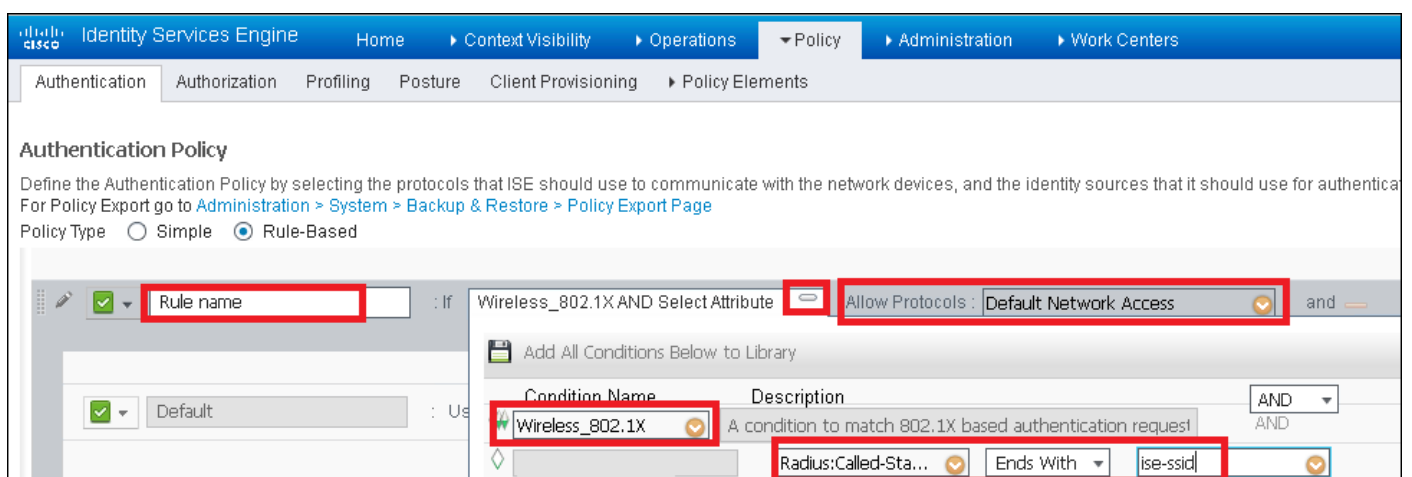


Étape 2. Insérez une nouvelle règle d'authentification.

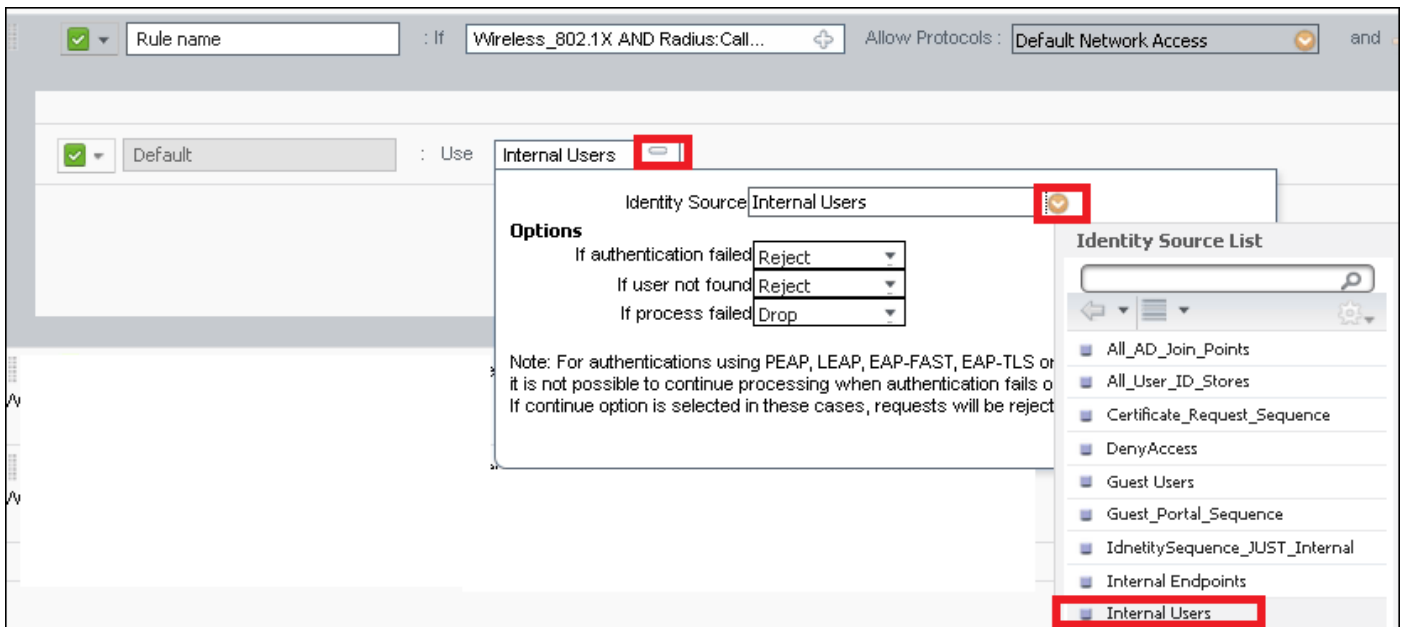


Étape 3. Écrivez les valeurs.

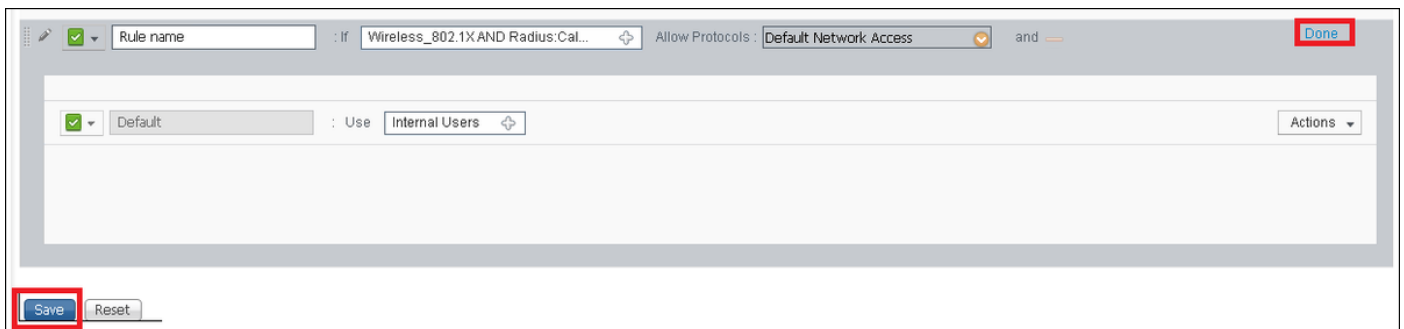
Cette règle d'authentification permet tous les protocoles répertoriés sous la liste d'**accès au réseau par défaut**, ceci s'applique à la demande d'authentification pour les clients Sans fil de 802.1x et avec l'Appeler-Station-ID et finit avec ise-SSID.



Choisissez également la source d'identité pour les clients qui apparie cette règle d'authentification, cette liste d'origine d'identité d'**utilisateurs internes d'utilisations d'exemple**



Une fois que c'est clic de finition **fait** et **sauvegarde**



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

[Service permis de protocoles](#)

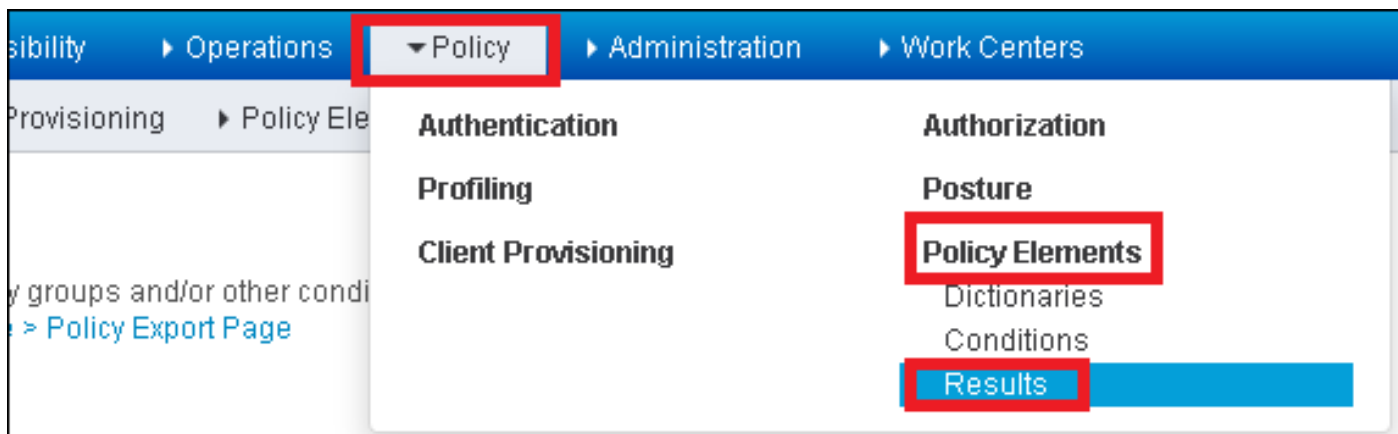
Pour plus d'informations sur l'identité les sources consultent ce lien :

[Créez un groupe d'identité de l'utilisateur](#)

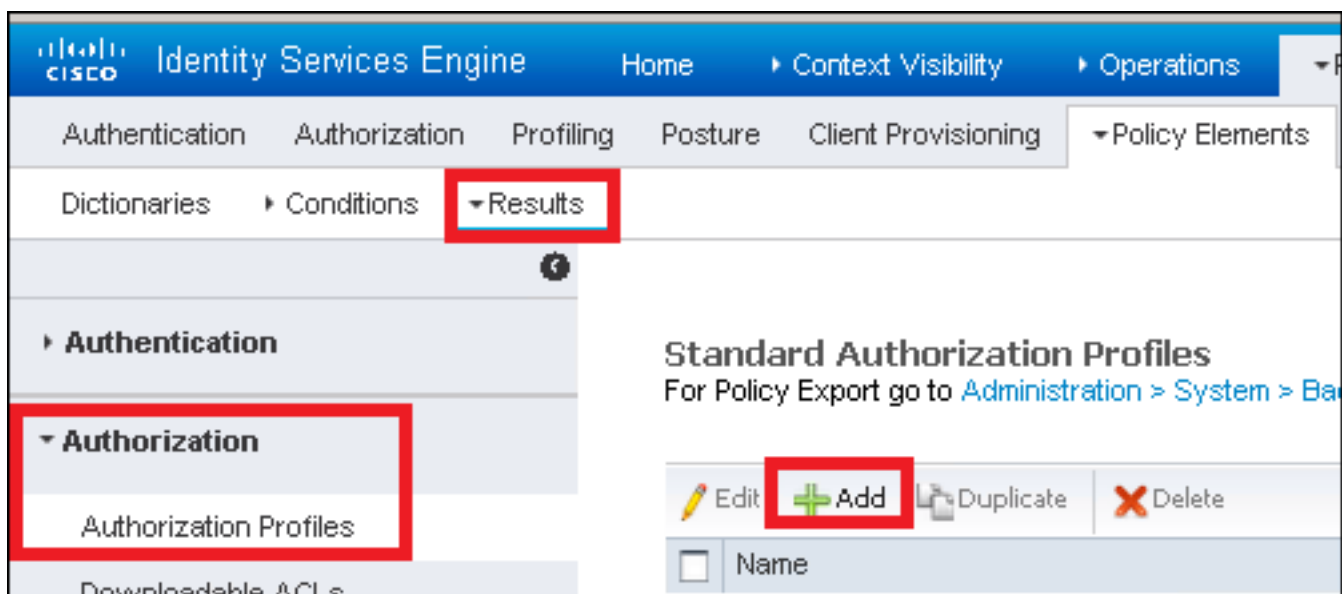
Créez le profil d'autorisation

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

Étape 1. Naviguez vers la **stratégie > les éléments > les résultats de stratégie**



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



Étape 3. Remplissez valeurs.