Remplacement WLAN + VLAN 802.1x avec Mobility Express (ME) 8.2 et ISE 2.1

Contenu

Introduction

Ce document décrit comment configurer un WLAN (Wireless Local Area Network) avec la sécurité d'entreprise Wi-Fi Protected Access 2 (WPA2) avec un contrôleur Mobility Express et un serveur RADIUS (Remote Authentication Dial-In User Service) externe. Identity Service Engine (ISE) est utilisé comme exemple de serveurs RADIUS externes.

Le protocole EAP (Extensible Authentication Protocol) utilisé dans ce guide est le protocole PEAP (Protected Extensible Authentication Protocol). En outre, le client est affecté à un VLAN spécifique (autre que celui affecté au WLAN par défaut).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Components Used

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

ME v8.2

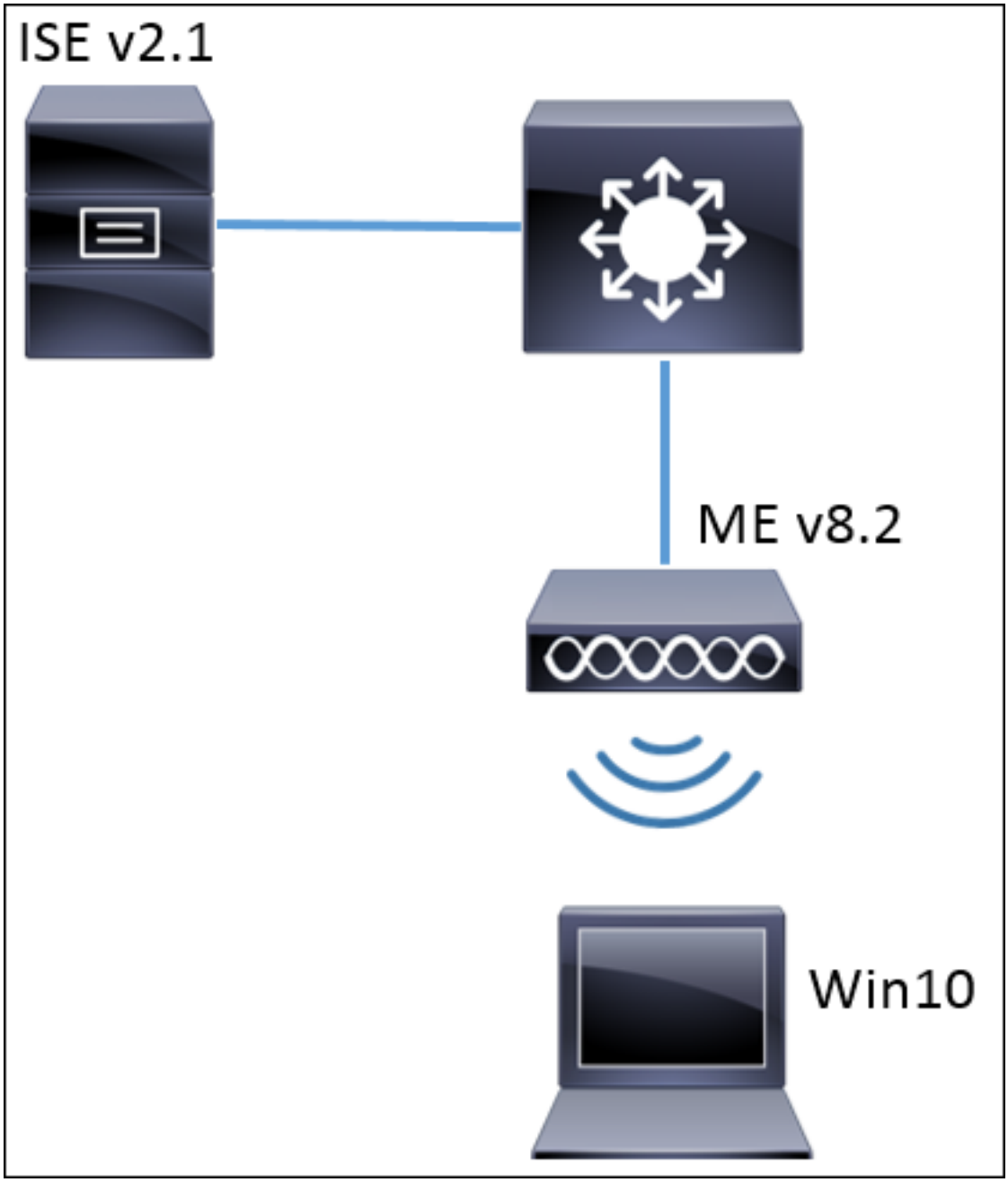
ISE v2.1

Ordinateur portable Windows 10

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.

Configuration

Diagramme du réseau



Configurations

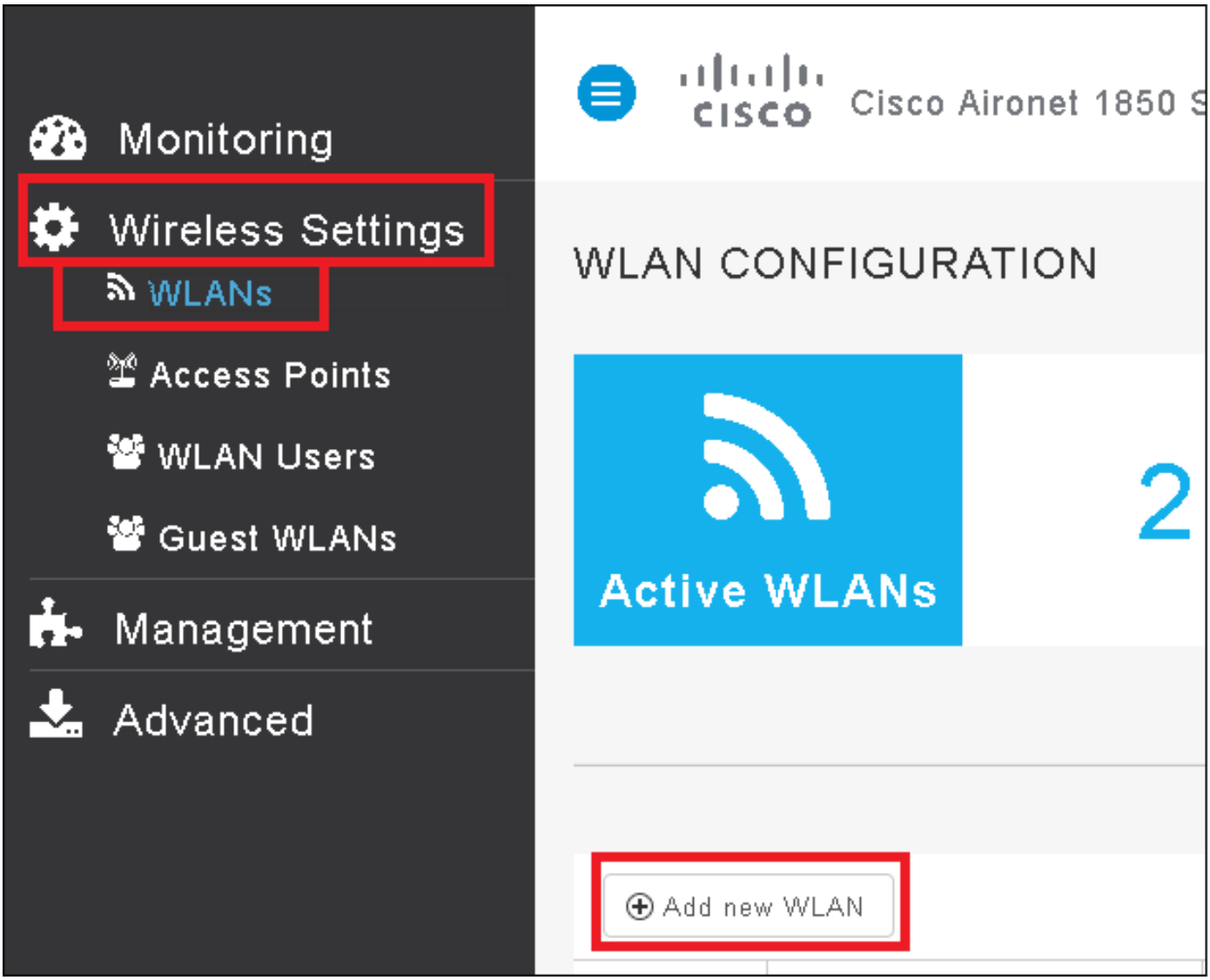
Les étapes générales sont les suivantes :

1. Créez le Service Set Identifier (SSID) dans le ME et déclarez le serveur RADIUS (ISE dans cet exemple) sur ME
2. Déclarer ME sur le serveur RADIUS (ISE)
3. Créer la règle d'authentification sur ISE
4. Créer une règle d'autorisation sur ISE
5. Configurer le point de terminaison

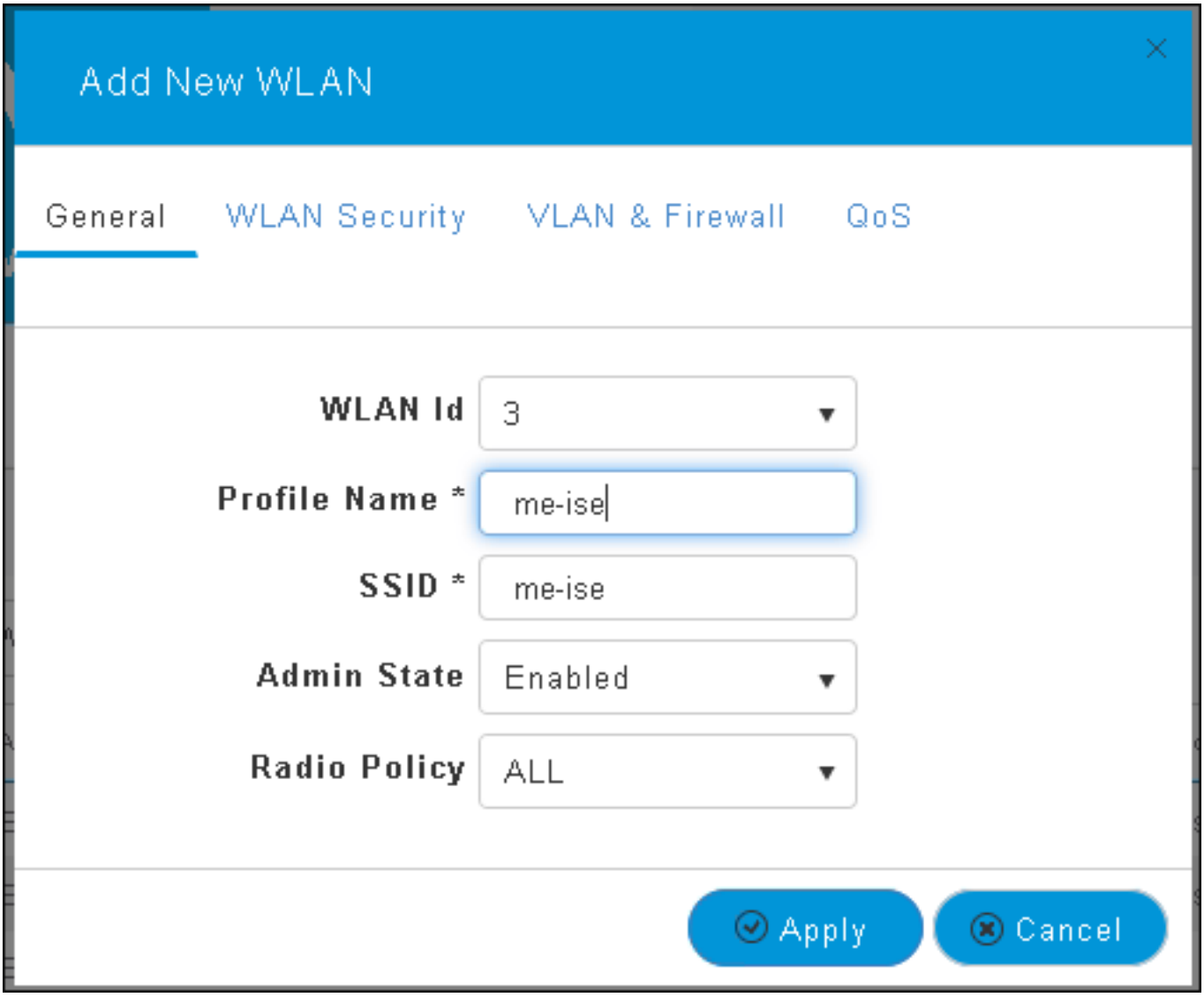
Configuration sur ME

Pour permettre la communication entre le serveur RADIUS et ME, il est nécessaire d'enregistrer le serveur RADIUS sur ME et vice versa. Cette étape montre comment enregistrer le serveur RADIUS sur ME.

Étape 1. Ouvrez l'interface utilisateur graphique de ME et accédez à **Wireless Settings > WLANs > Add new WLAN.**

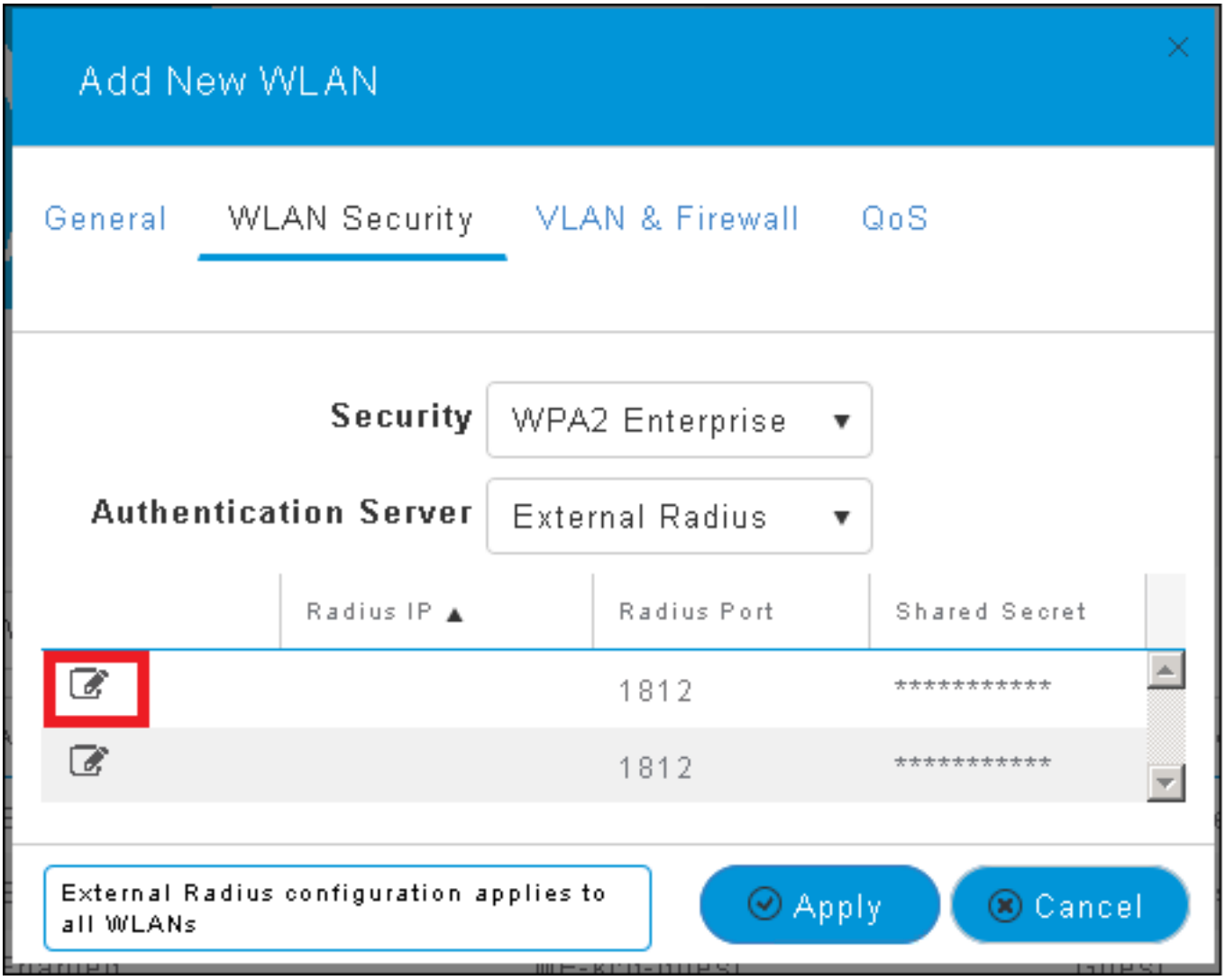


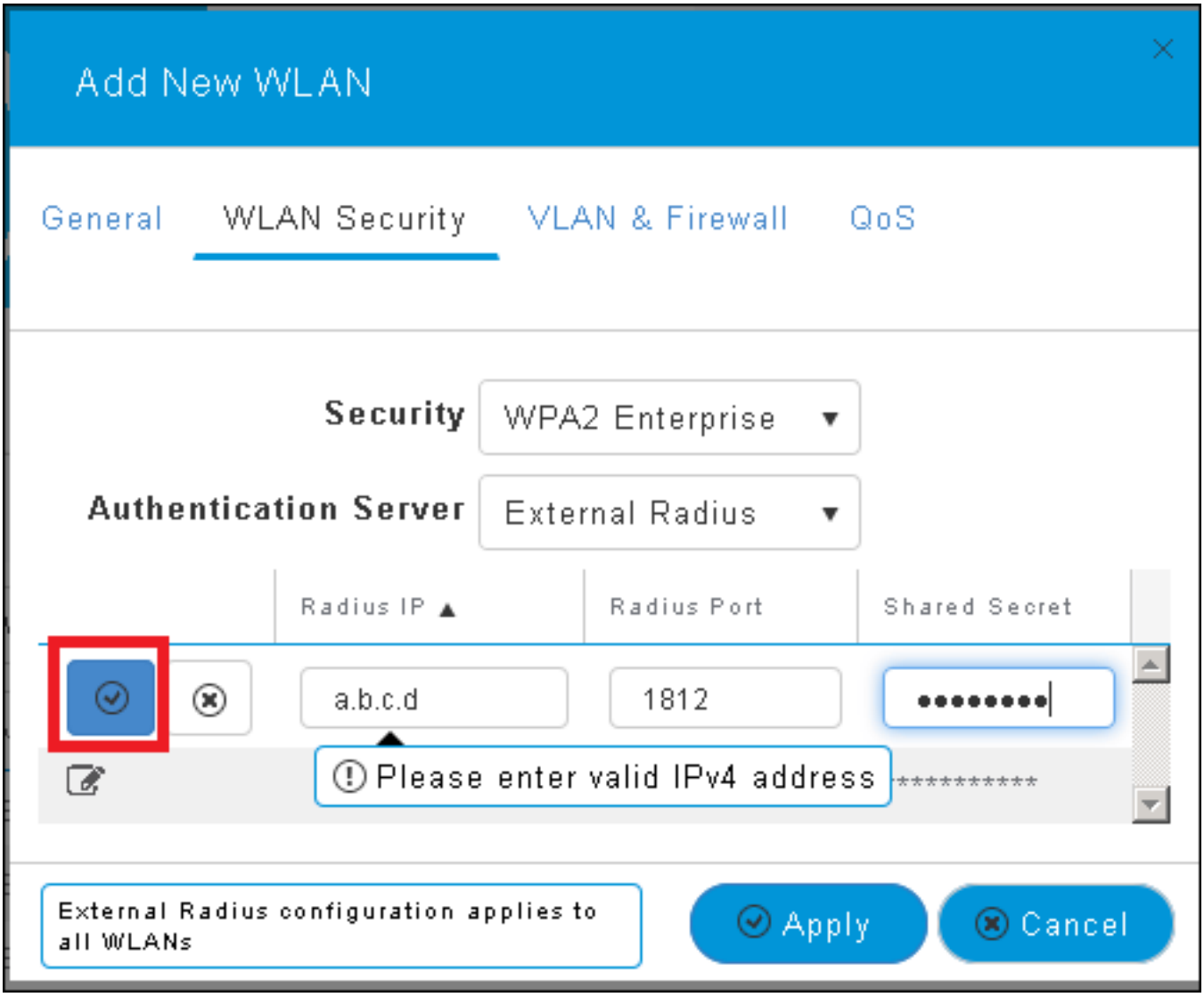
Étape 2. Sélectionnez un nom pour le WLAN.



Étape 3. Spécifiez la configuration de sécurité sous l'onglet **Sécurité WLAN**.

Choisissez **WPA2 Enterprise**, pour le serveur d'authentification choisissez **RADIUS externe**. Cliquez sur l'option edit pour ajouter l'adresse IP de RADIUS et sélectionner une clé **Shared Secret**.


Add New WLAN
General
WLAN Security
VLAN & Firewall
QoS
Security
WPA2 Enterprise
Authentication Server
External Radius
Radius IP
Radius Port
Shared Secret
1812
****
1812
****
External Radius configuration applies to all WLANs
Apply
Cancel

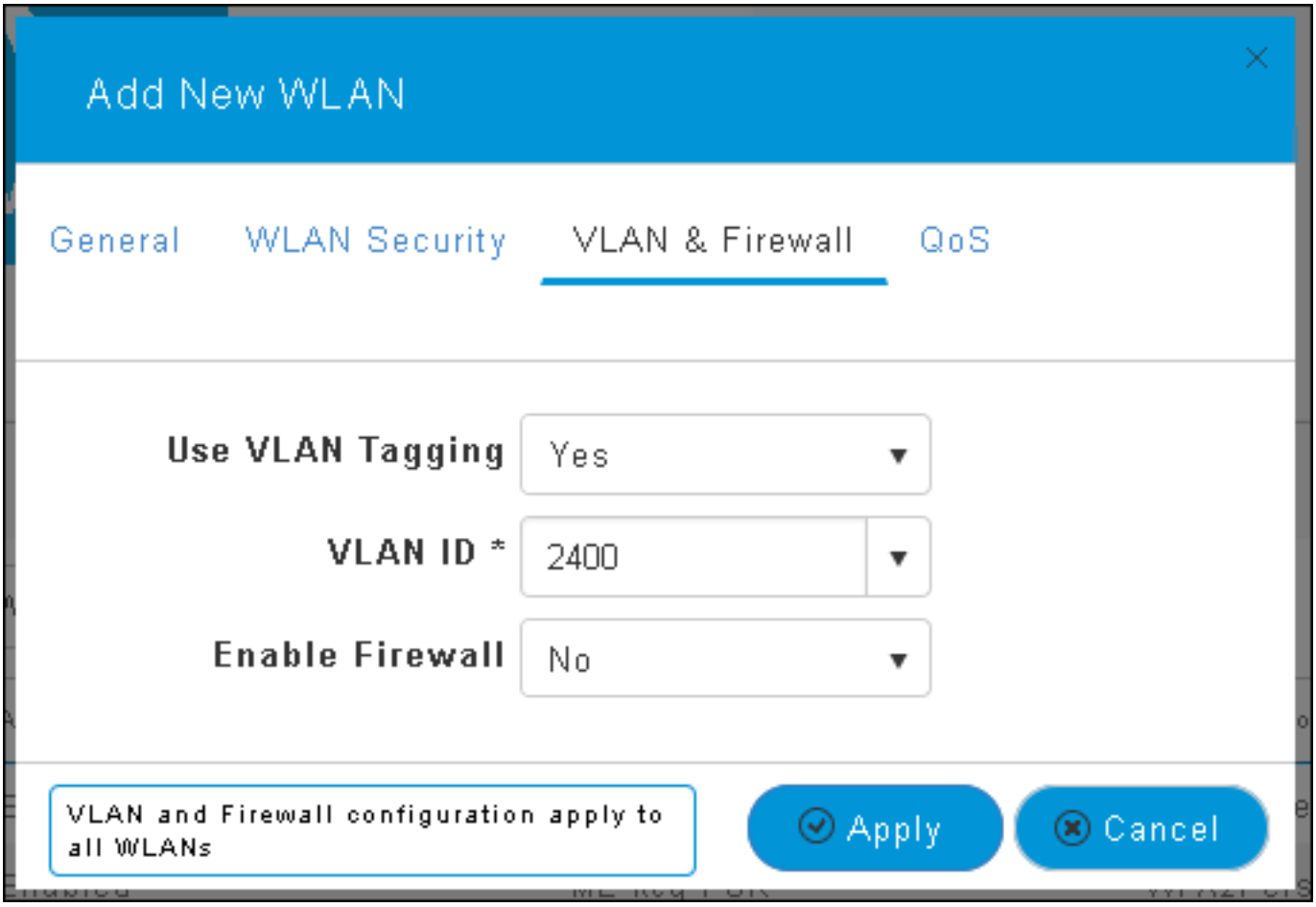


<a.b.c.d> correspond au serveur RADIUS.

Étape 4. Attribuez un VLAN au SSID.

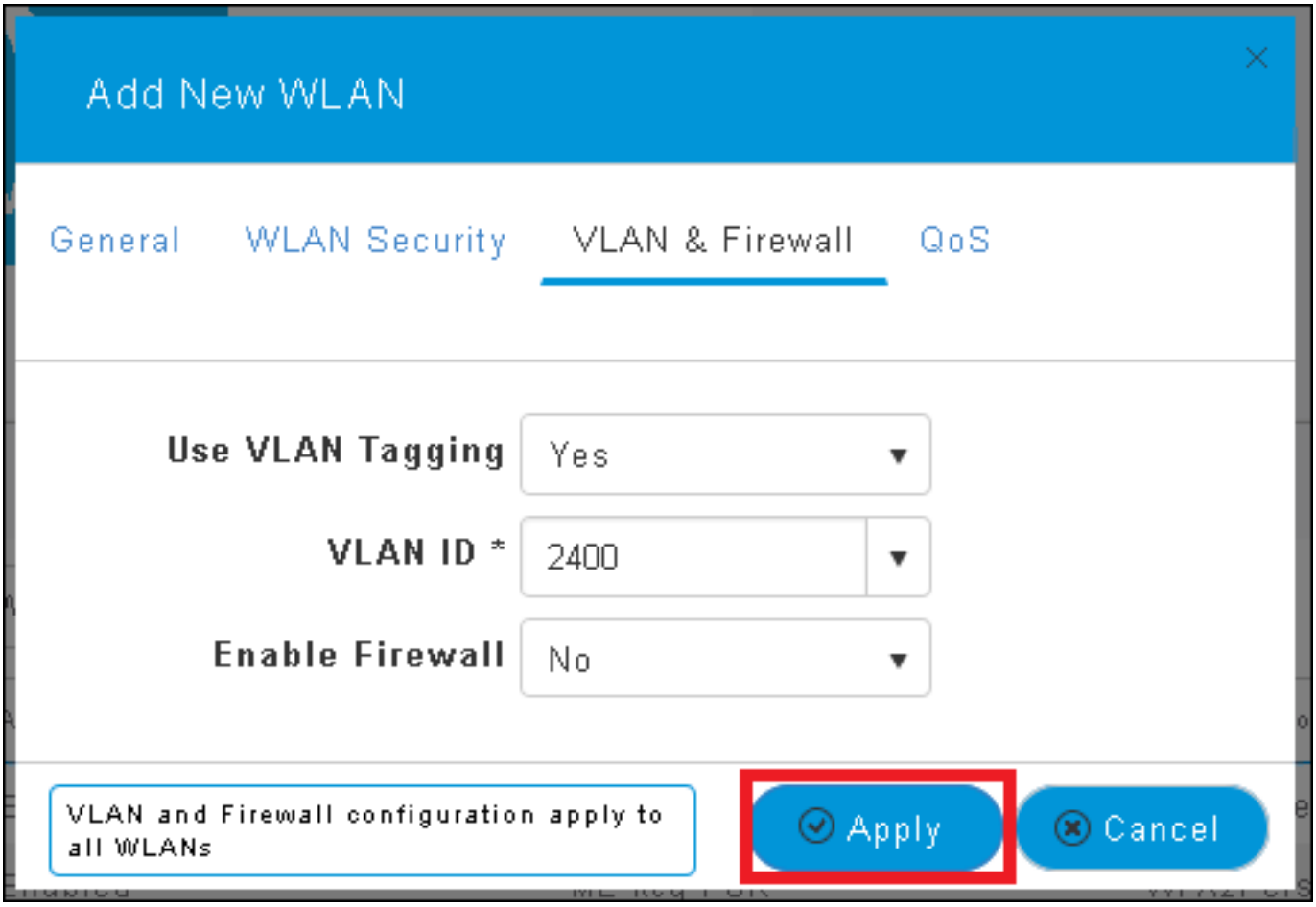
Si le SSID doit être attribué au VLAN du point d'accès, cette étape peut être ignorée.

Afin d'affecter les utilisateurs de ce SSID à un VLAN spécifique (autre que le VLAN du point d'accès), activez **Utiliser le marquage VLAN** et affectez l'**ID de VLAN** souhaité.



Note: Si l'étiquetage VLAN est utilisé, assurez-vous que le port de commutateur auquel le point d'accès est connecté est configuré comme port trunk et que le VLAN AP est configuré comme port natif.

Étape 5. Cliquez sur **Apply** pour terminer la configuration.



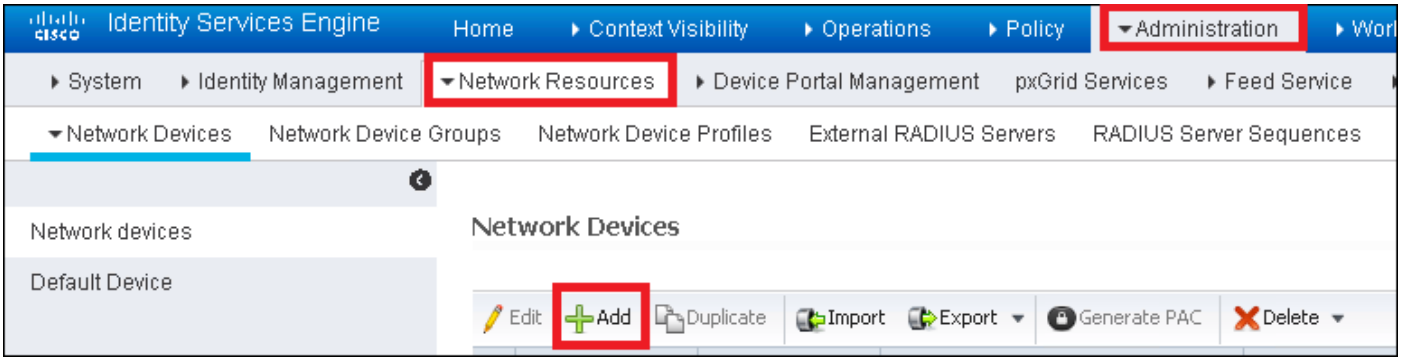
Étape 6. Facultatif, configurez le WLAN pour accepter la substitution VLAN.

Activez AAA override sur le WLAN et ajoutez les VLAN nécessaires. Pour ce faire, vous devez ouvrir une session CLI à l'interface de gestion ME et émettre ces commandes :

```
>config wlan disable <wlan-id>
>config wlan aaa-override enable <wlan-id>
>config wlan enable <wlan-id>
>config flexconnect group default-flexgroup vlan add <vlan-id>
```

Déclarer ME sur ISE

Étape 1. Ouvrez la console ISE et accédez à **Administration > Network Resources > Network Devices > Add.**

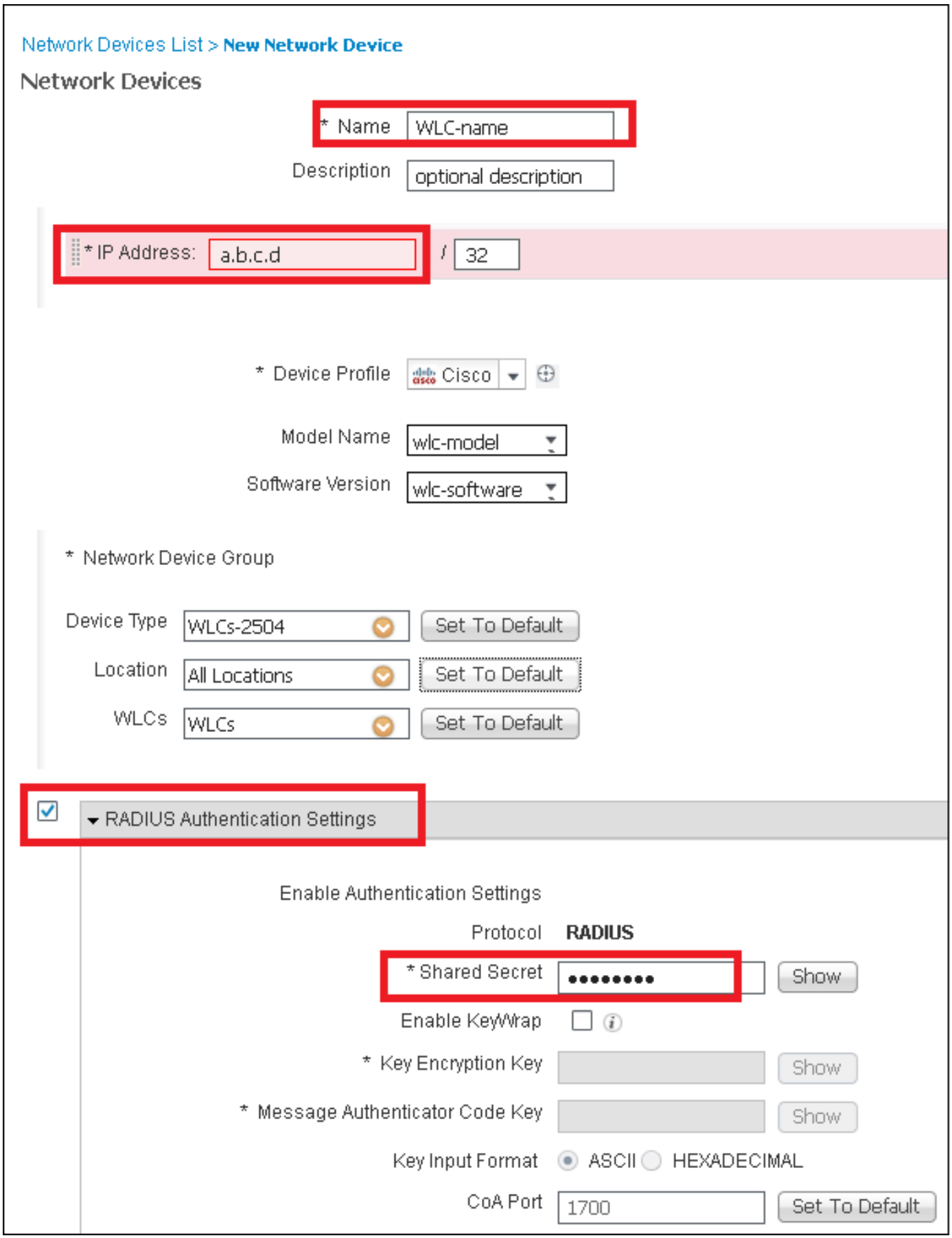


Étape 2. Entrez l'information.

Vous pouvez éventuellement spécifier un nom de modèle, une version de logiciel, une description

et affecter des groupes de périphériques réseau en fonction des types de périphériques, de l'emplacement ou des WLC.

a.b.c.d correspond à l'adresse IP du ME.

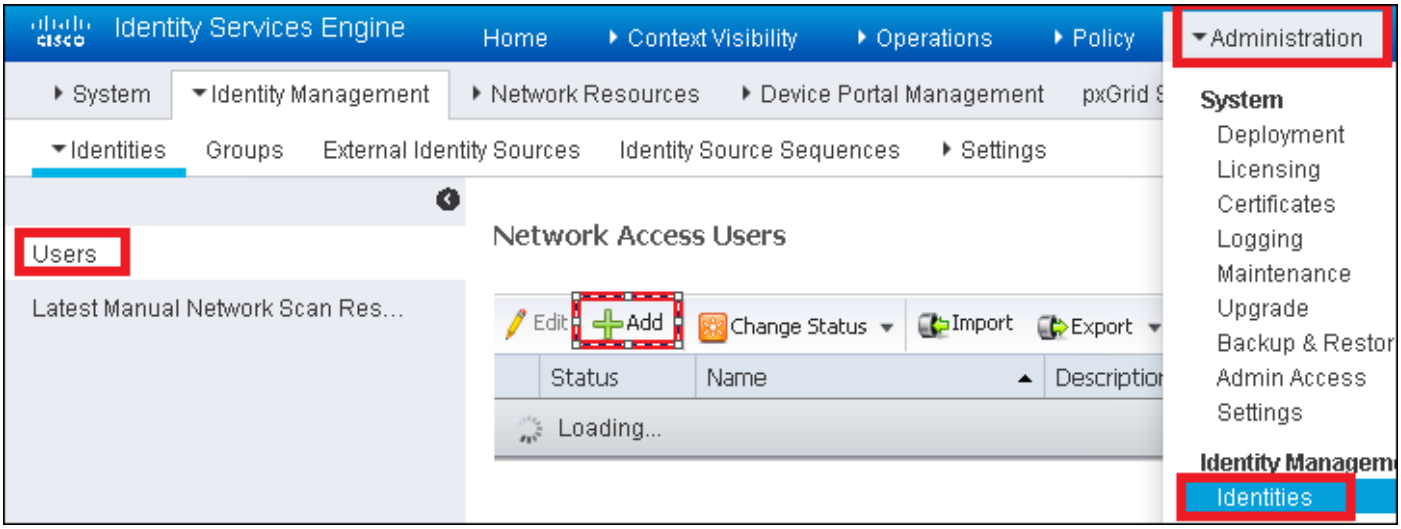


Pour plus d'informations sur les groupes de périphériques réseau, consultez ce lien :

[ISE - Groupes de périphériques réseau]

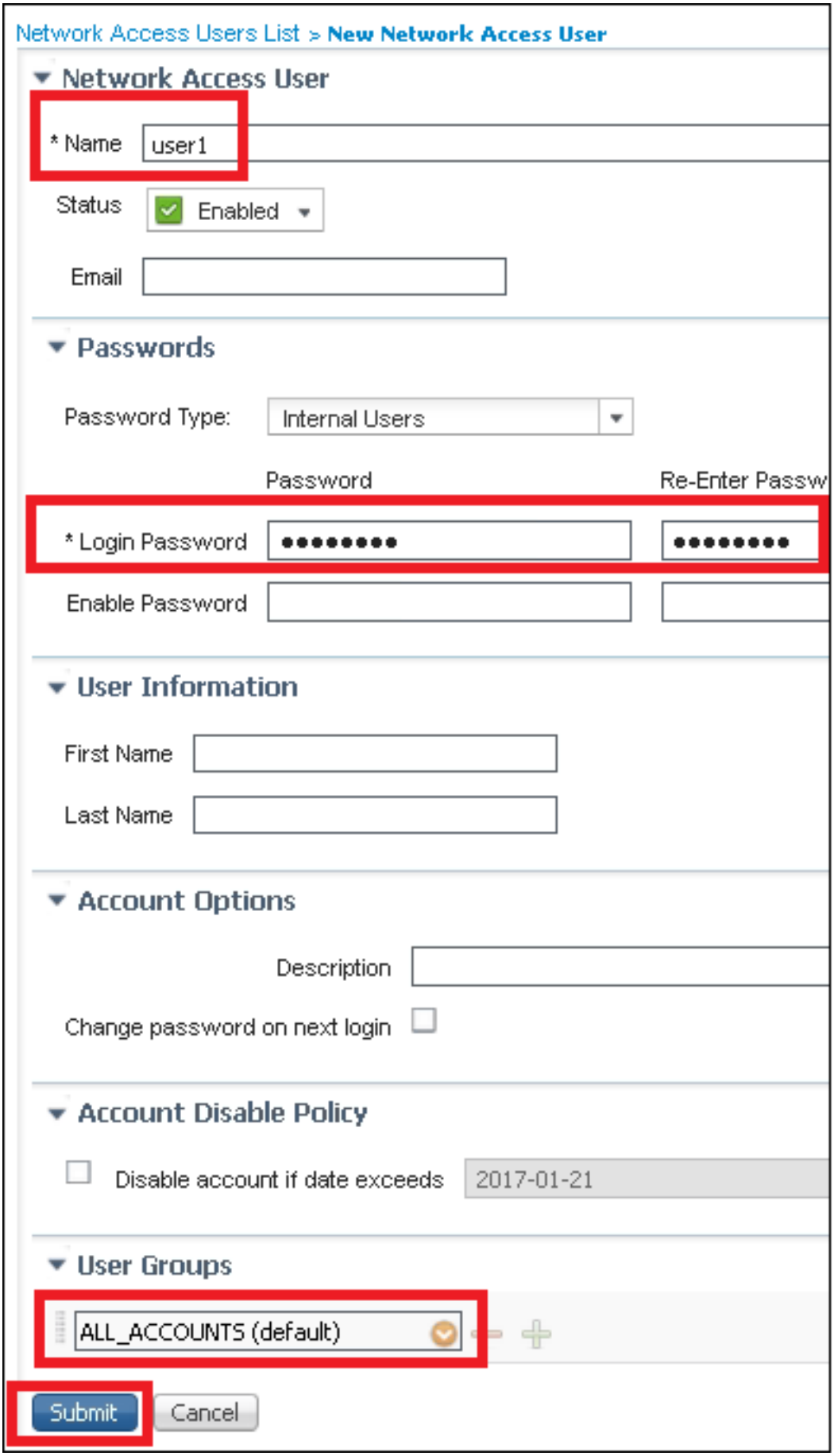
Créer un nouvel utilisateur sur ISE

Étape 1. Accéder à **Administration > Identity Management > Identities > Users > Add.**



Étape 2. Entrez l'information.

Dans cet exemple, cet utilisateur appartient à un groupe appelé ALL_ACCOUNTS, mais il peut être ajusté selon les besoins.

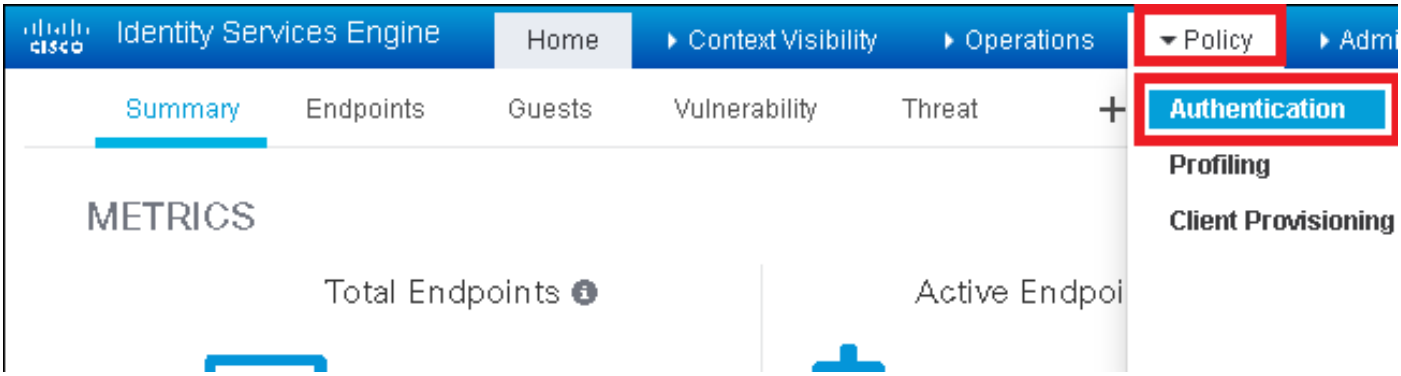


Créer la règle d'authentification

Les règles d'authentification sont utilisées pour vérifier si les informations d'identification des utilisateurs sont correctes (vérifier si l'utilisateur est vraiment celui qu'il dit être) et limiter les

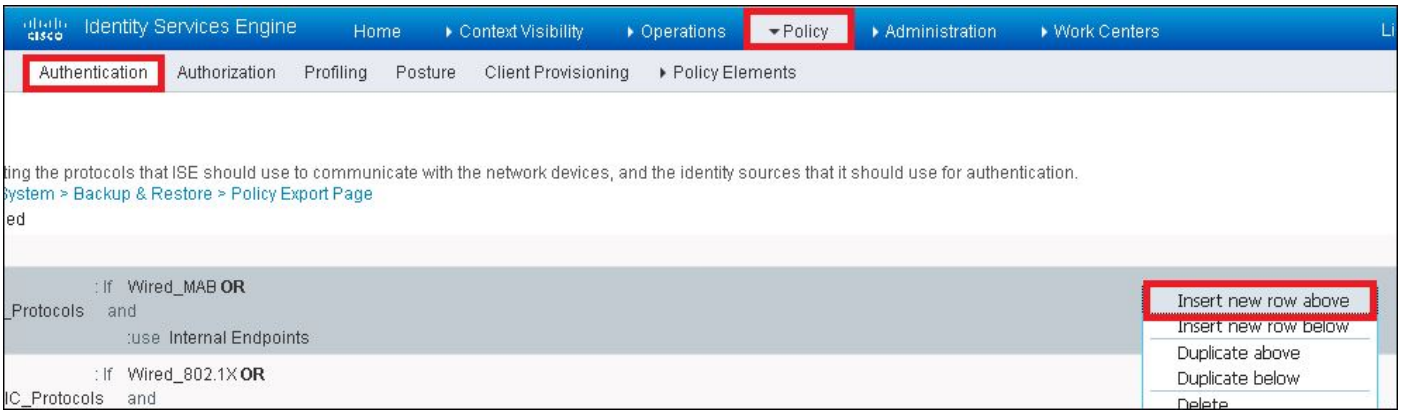
méthodes d'authentification autorisées par lui.

Étape 1. Naviguer à **Policy > Authentication**.



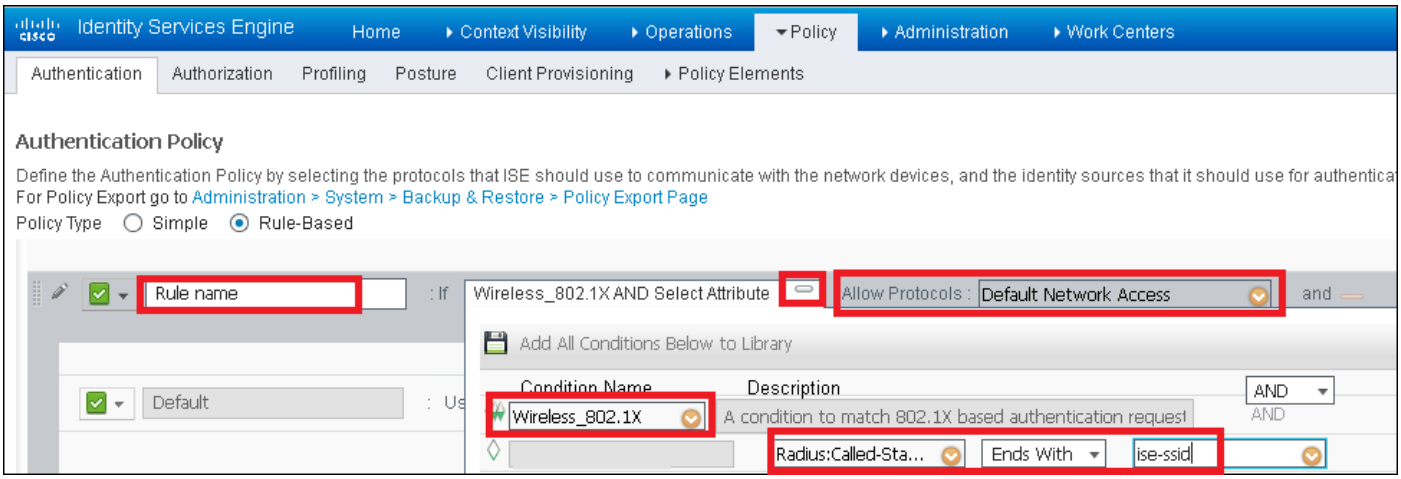
Étape 2. Insérer une nouvelle règle d'authentification.

Pour ce faire, accédez à **Stratégie > Authentification > Insérer une nouvelle ligne au-dessus/au-dessous.**

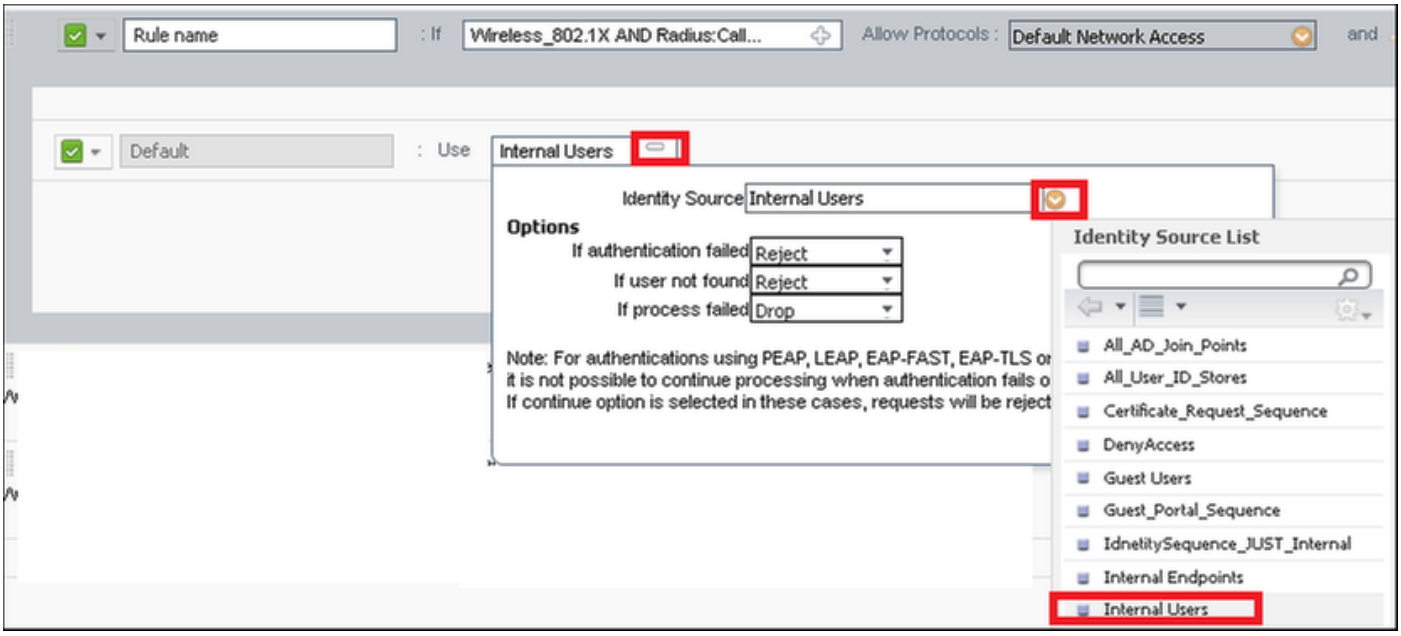


Étape 3. Saisissez les informations nécessaires

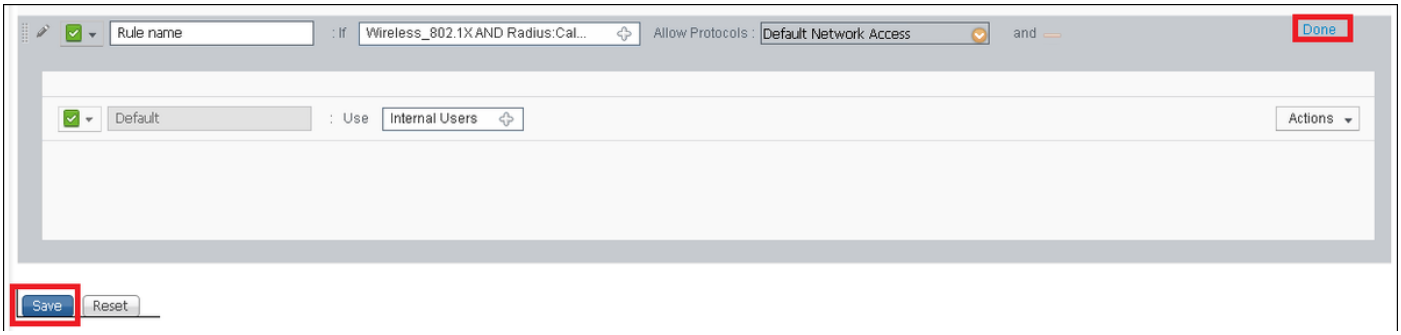
Cet exemple de règle d'authentification autorise tous les protocoles répertoriés dans la liste **Accès réseau par défaut**, ceci s'applique à la demande d'authentification pour les clients sans fil 802.1x et avec Called-Station-ID et se termine par *ise-ssid*.



En outre, choisissez la source d'identité pour les clients qui correspondent à cette règle d'authentification, dans cet exemple, elle est utilisée par *les utilisateurs internes*



Une fois terminé, cliquez sur **Terminé** et **Enregistrer**



Pour plus d'informations sur les stratégies d'autorisation des protocoles, consultez ce lien :

[Service de protocoles autorisés]

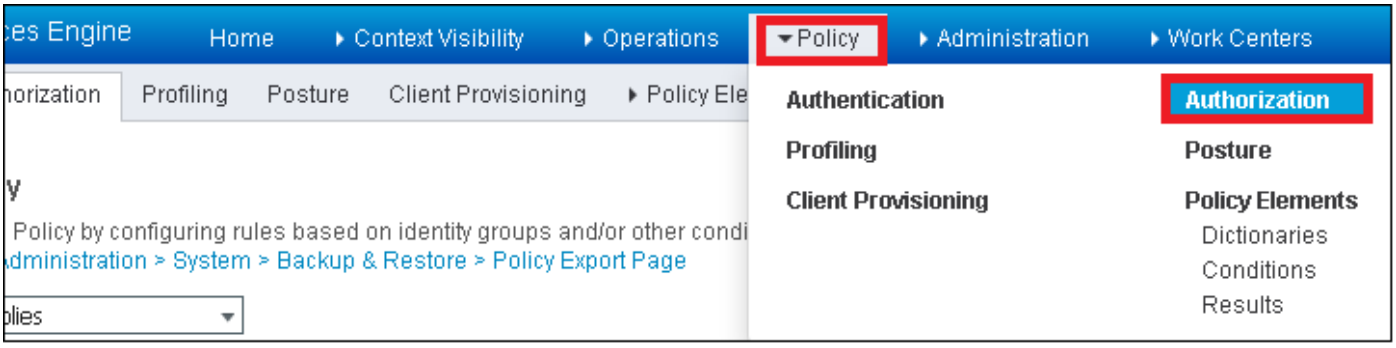
Pour plus d'informations sur les sources d'identité, consultez ce lien :

[Créer un groupe d'identités utilisateur]

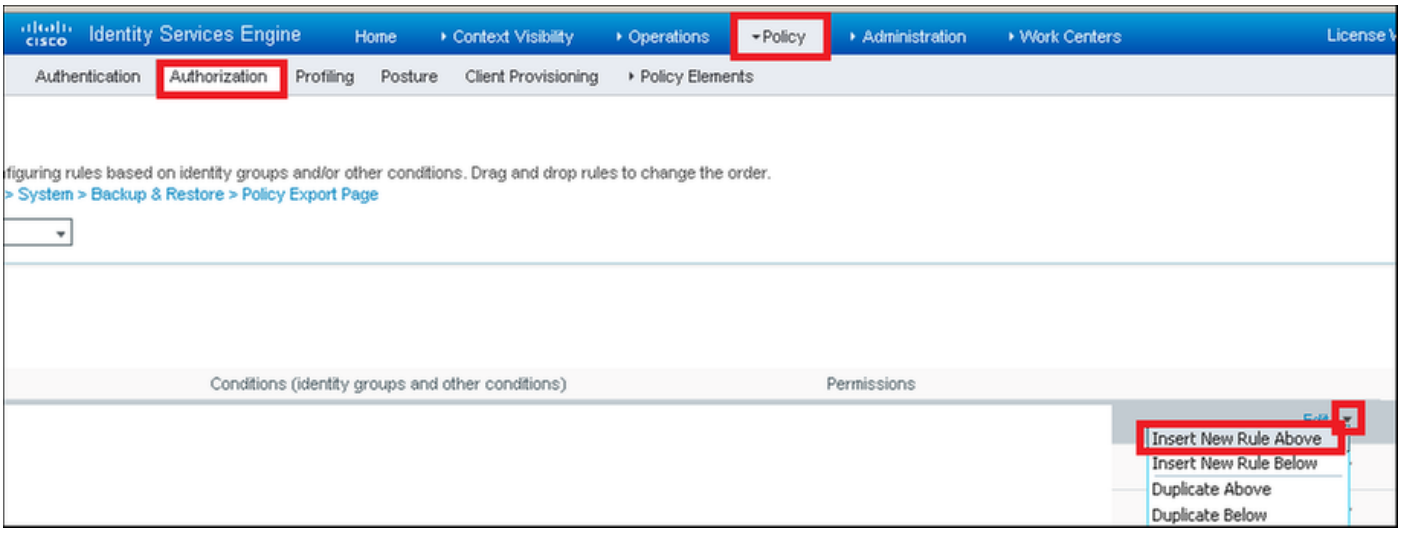
Créer la règle d'autorisation

La règle d'autorisation est celle qui est chargée de déterminer si le client est autorisé à rejoindre le réseau ou non

Étape 1. Accédez à **Stratégie > Autorisation.**

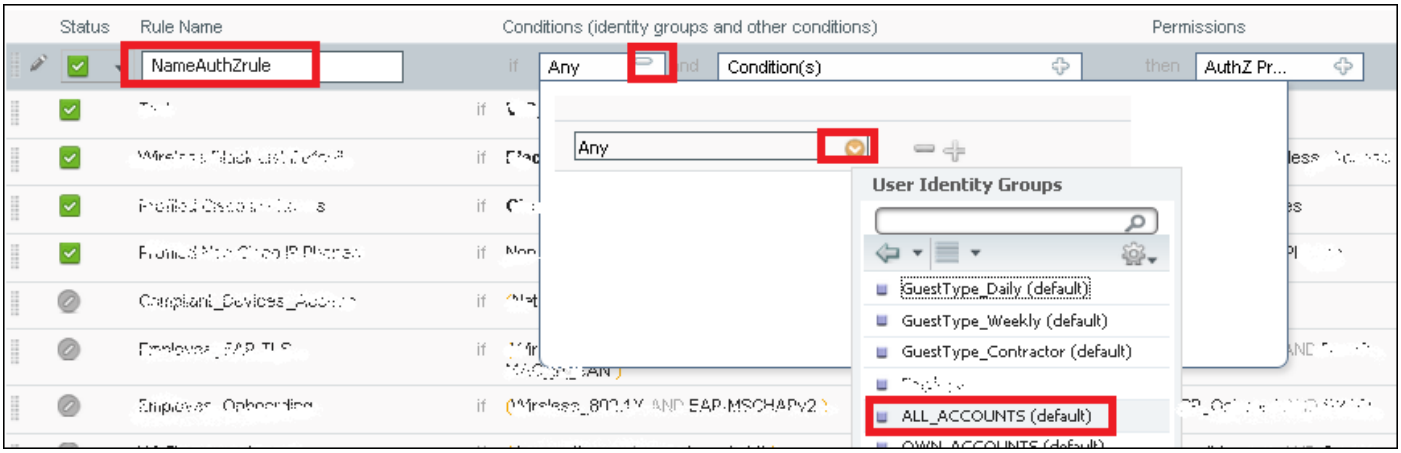


Étape 2. Insérer une nouvelle règle. Accédez à **Stratégie > Autorisation > Insérer une nouvelle règle au-dessus/au-dessous.**

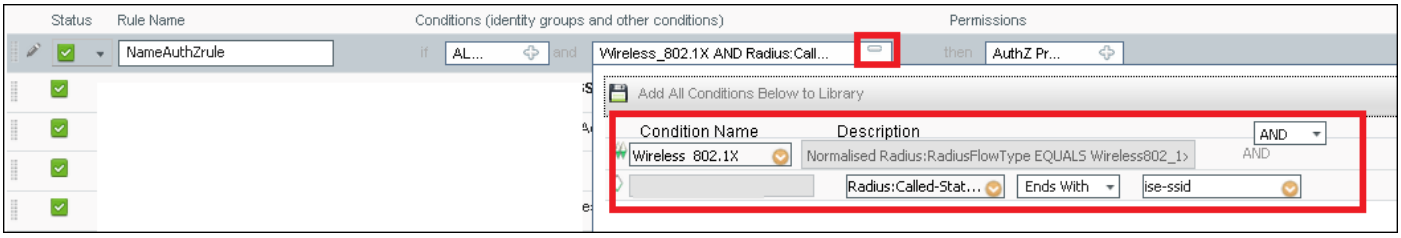


Étape 3. Entrez l'information.

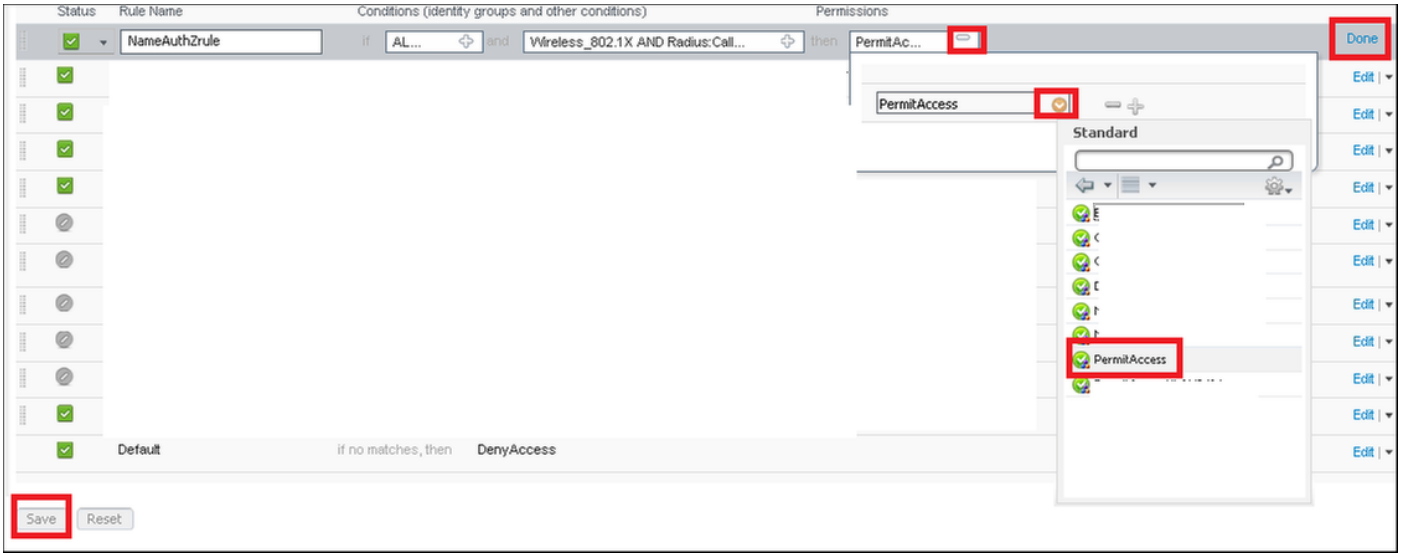
Choisissez d'abord un nom pour la règle et les groupes d'identité où l'utilisateur est stocké. Dans cet exemple, l'utilisateur est stocké dans le groupe *ALL_ACCOUNTS.*



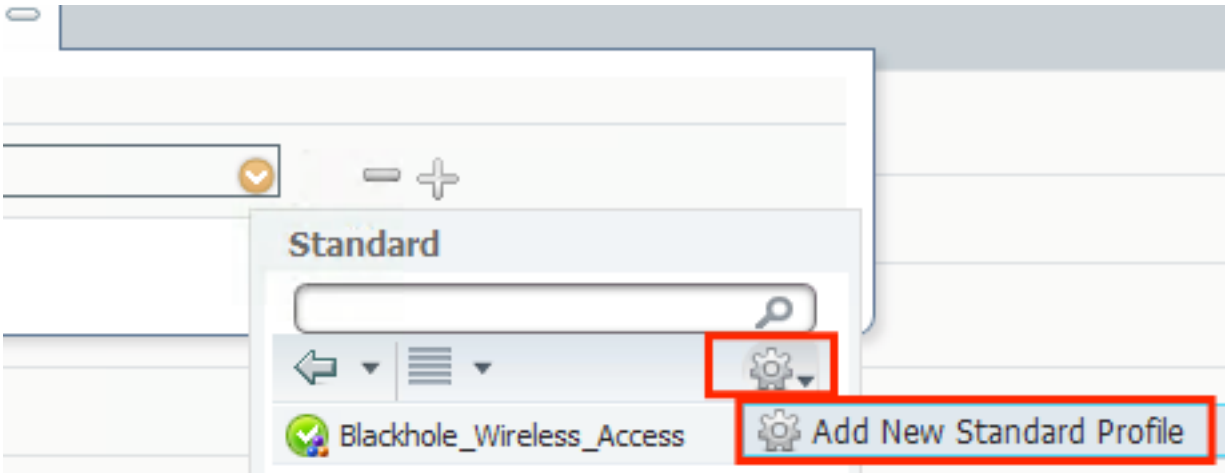
Après cela, choisissez d'autres conditions qui font que le processus d'autorisation tombe dans cette règle. Dans cet exemple, le processus d'autorisation atteint cette règle s'il utilise la norme 802.1x Wireless et s'il est appelé ID de station se termine par *ise-ssid.*



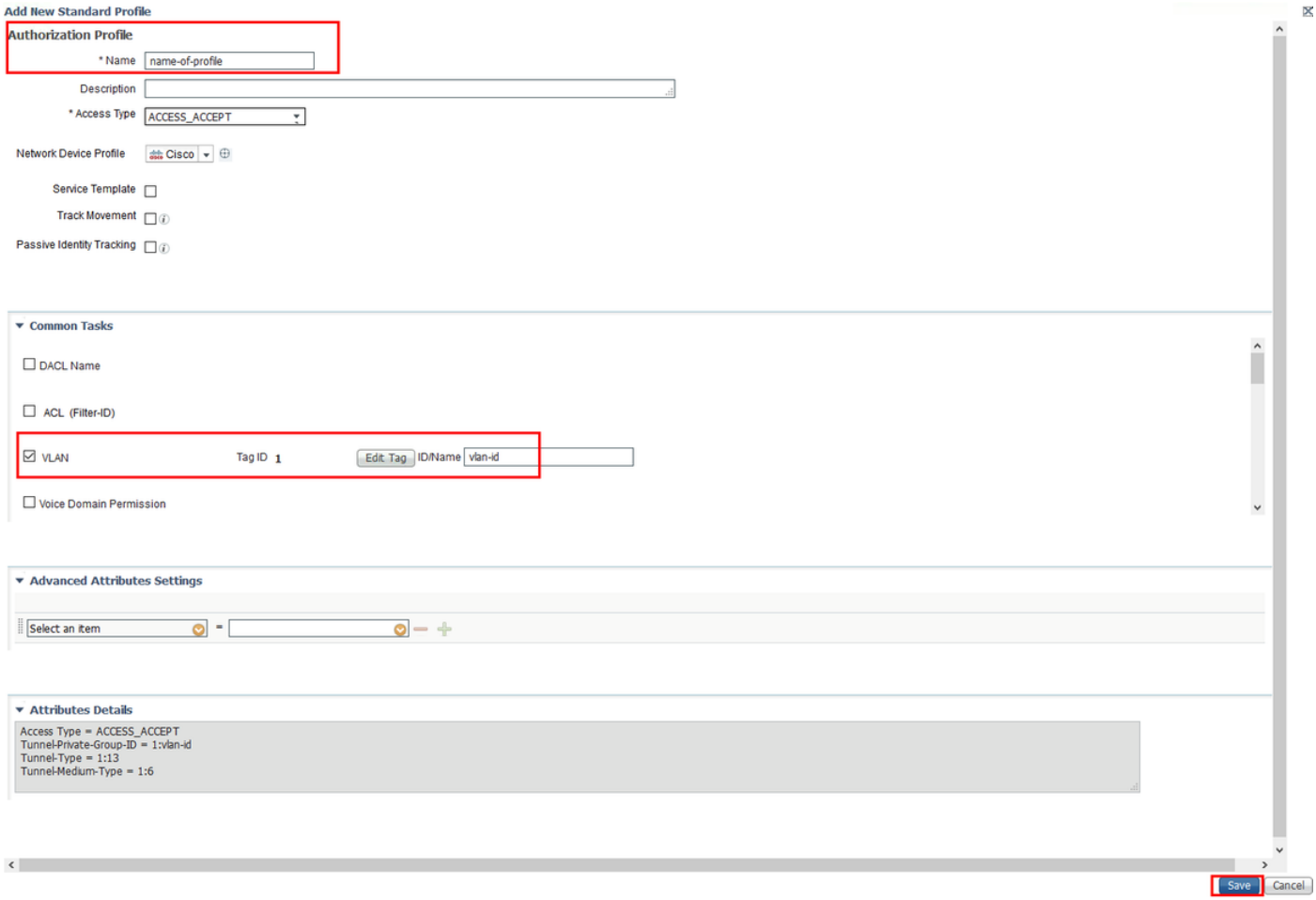
Enfin, choisissez le profil d'autorisation qui permet aux clients de rejoindre le réseau, cliquez sur **Terminé** et **Enregistrer.**



Le cas échéant, créez un nouveau profil d'autorisation qui attribuera le client sans fil à un autre VLAN :



Entrez l’information:



Configuration du périphérique final

Configurez un ordinateur portable Windows 10 pour vous connecter à un SSID avec authentification 802.1x à l'aide de PEAP/MS-CHAPv2 (version Microsoft du protocole d'authentification à échanges confirmés version 2).

Dans cet exemple de configuration, ISE utilise son certificat auto-signé pour effectuer l'authentification.

Pour créer le profil WLAN sur la machine Windows, deux options sont disponibles :

1. Installer le certificat auto-signé sur l'ordinateur pour valider et approuver le serveur ISE pour terminer l'authentification
2. Ignorer la validation du serveur RADIUS et faire confiance à tout serveur RADIUS utilisé pour effectuer l'authentification (non recommandé, car il peut devenir un problème de sécurité)

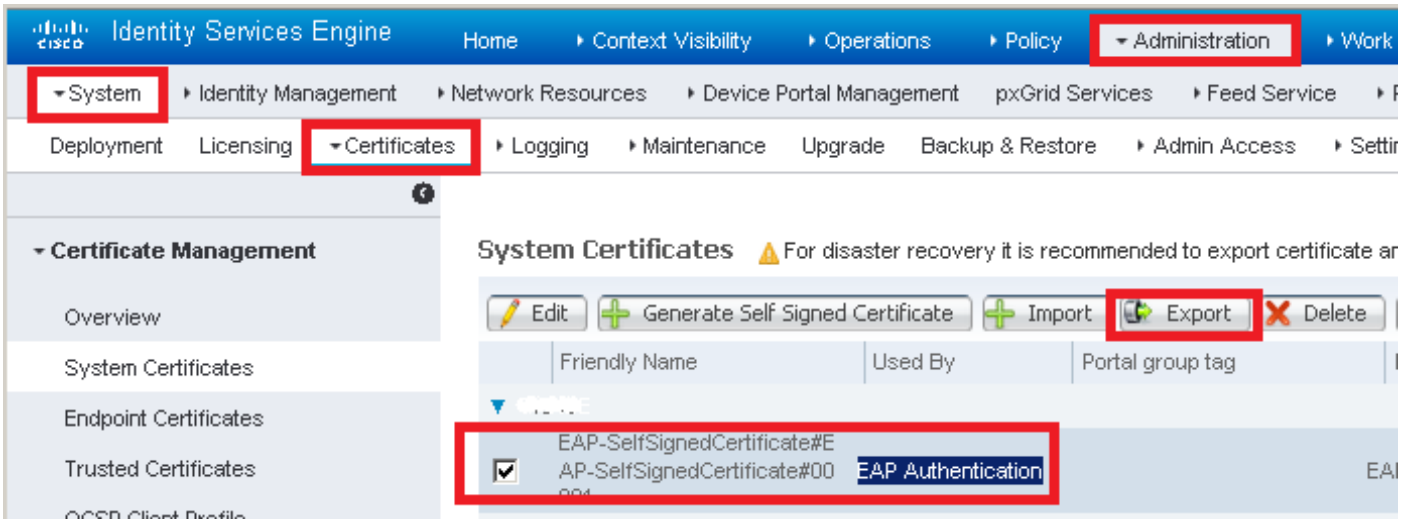
La configuration de ces options est expliquée sur la configuration du périphérique final - Créer le profil WLAN - Étape 7.

Configuration du périphérique final - Installer le certificat auto-signé ISE

Étape 1. Exporter le certificat auto-signé à partir d'ISE.

Connectez-vous à ISE et accédez à **Administration > System > Certificates > System Certificates**.

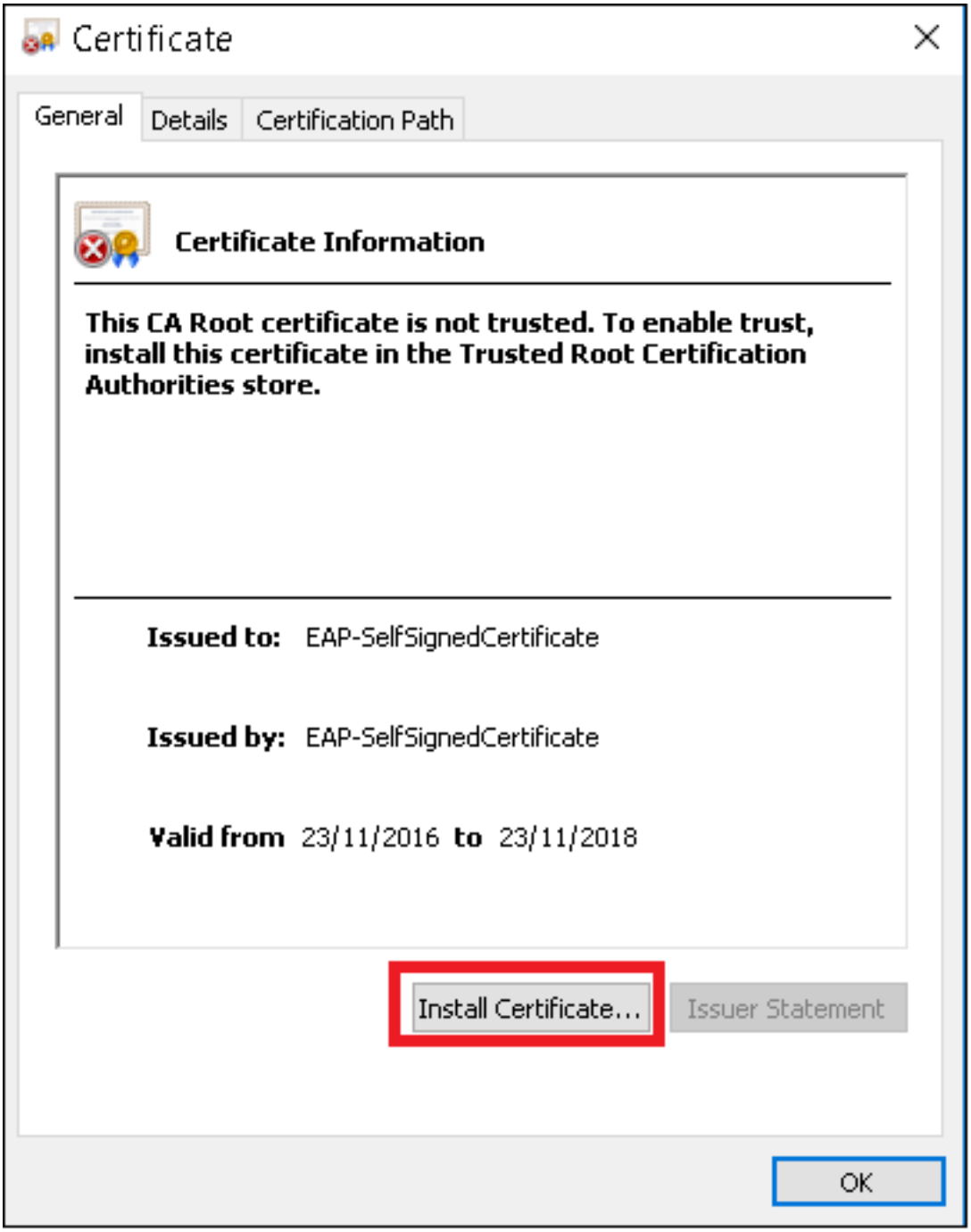
Sélectionnez ensuite le certificat utilisé pour l'**authentification EAP** et cliquez sur **Exporter.**



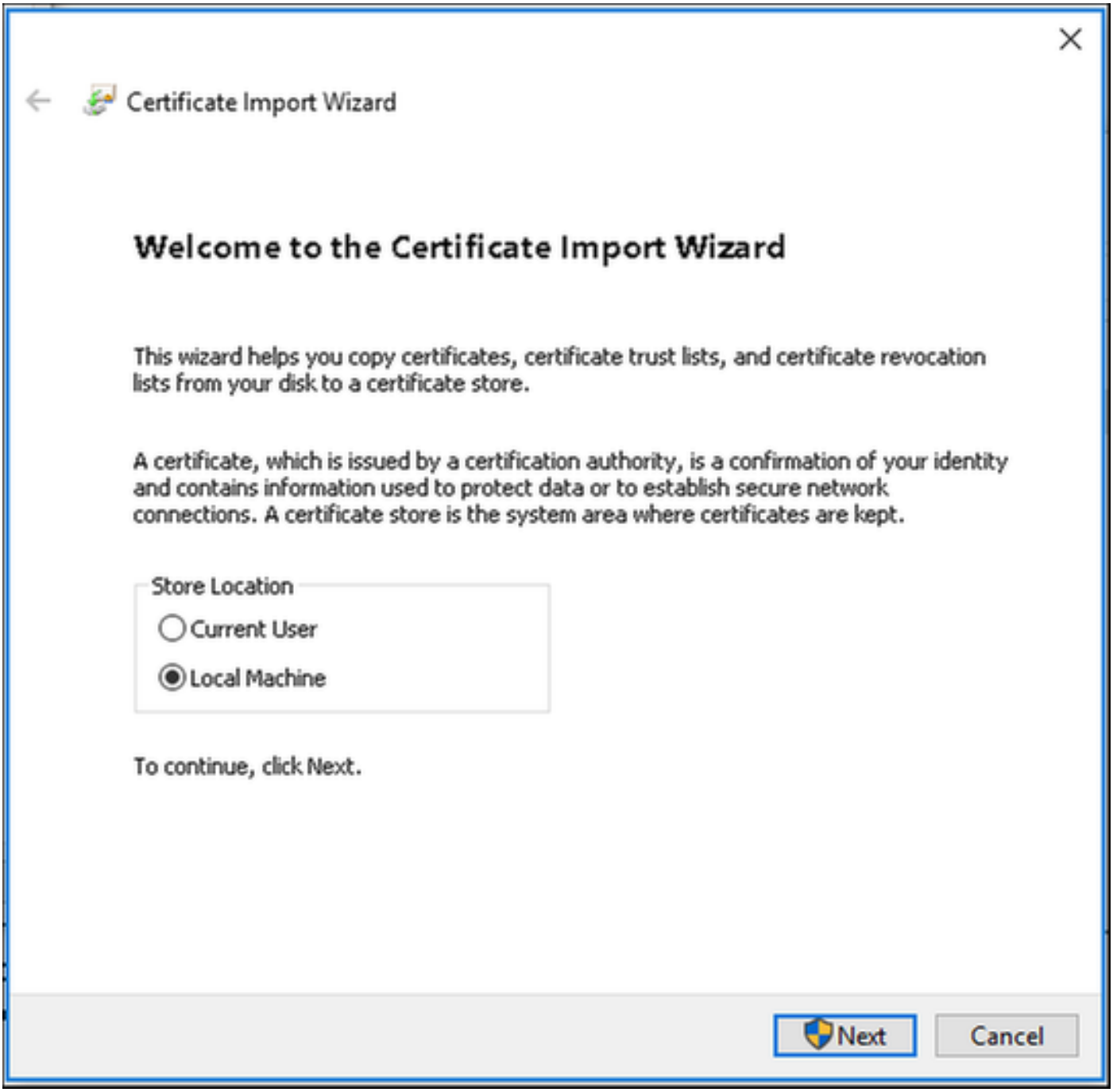
Enregistrez le certificat à l'emplacement requis. Ce certificat est installé sur l'ordinateur Windows.

Étape 2. Installez le certificat sur l'ordinateur Windows.

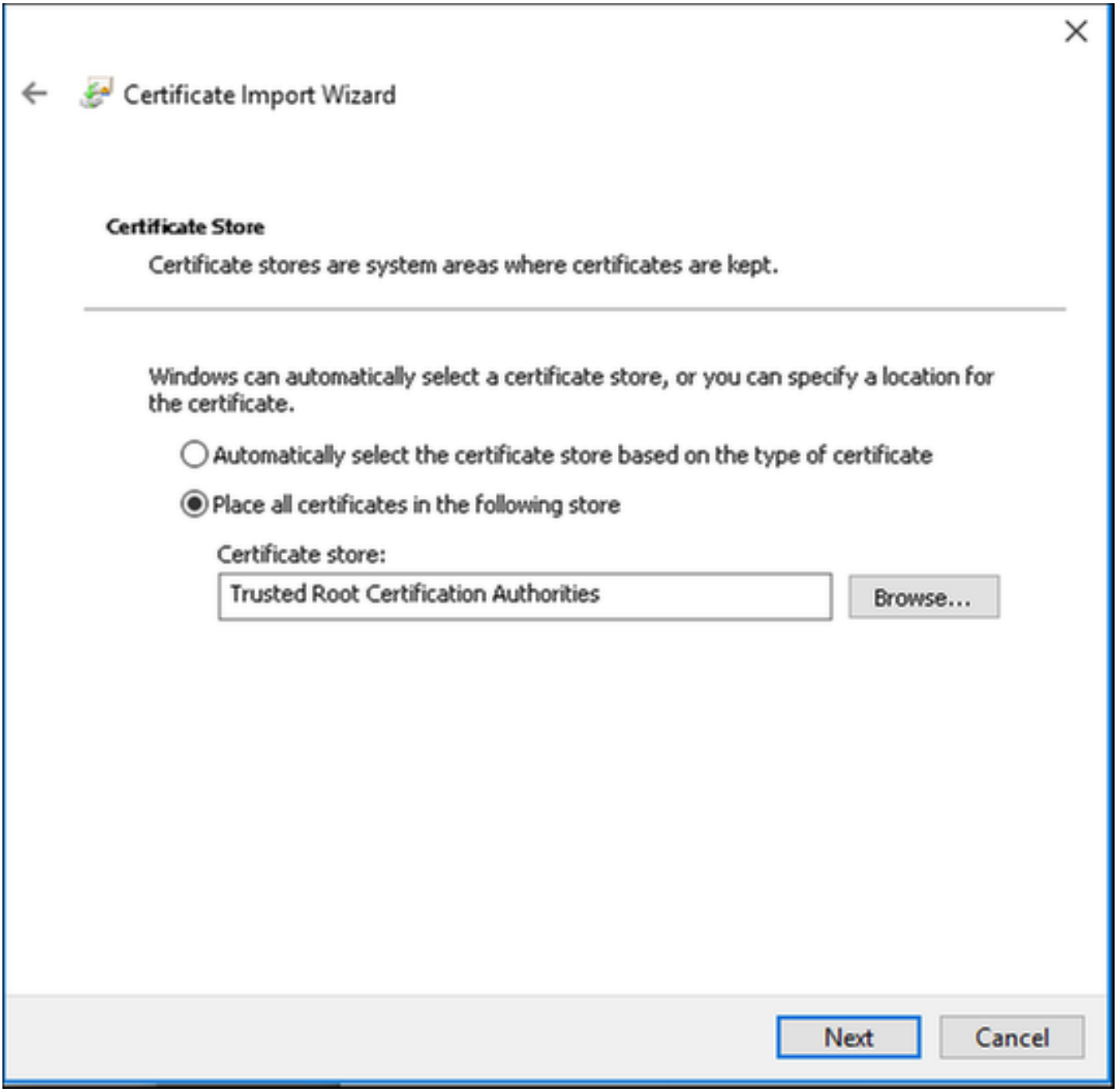
Copiez le certificat exporté avant dans l'ordinateur Windows, modifiez l'extension du fichier de .pem à .crt, après ce double-clic dessus et sélectionnez **Installer le certificat...**.



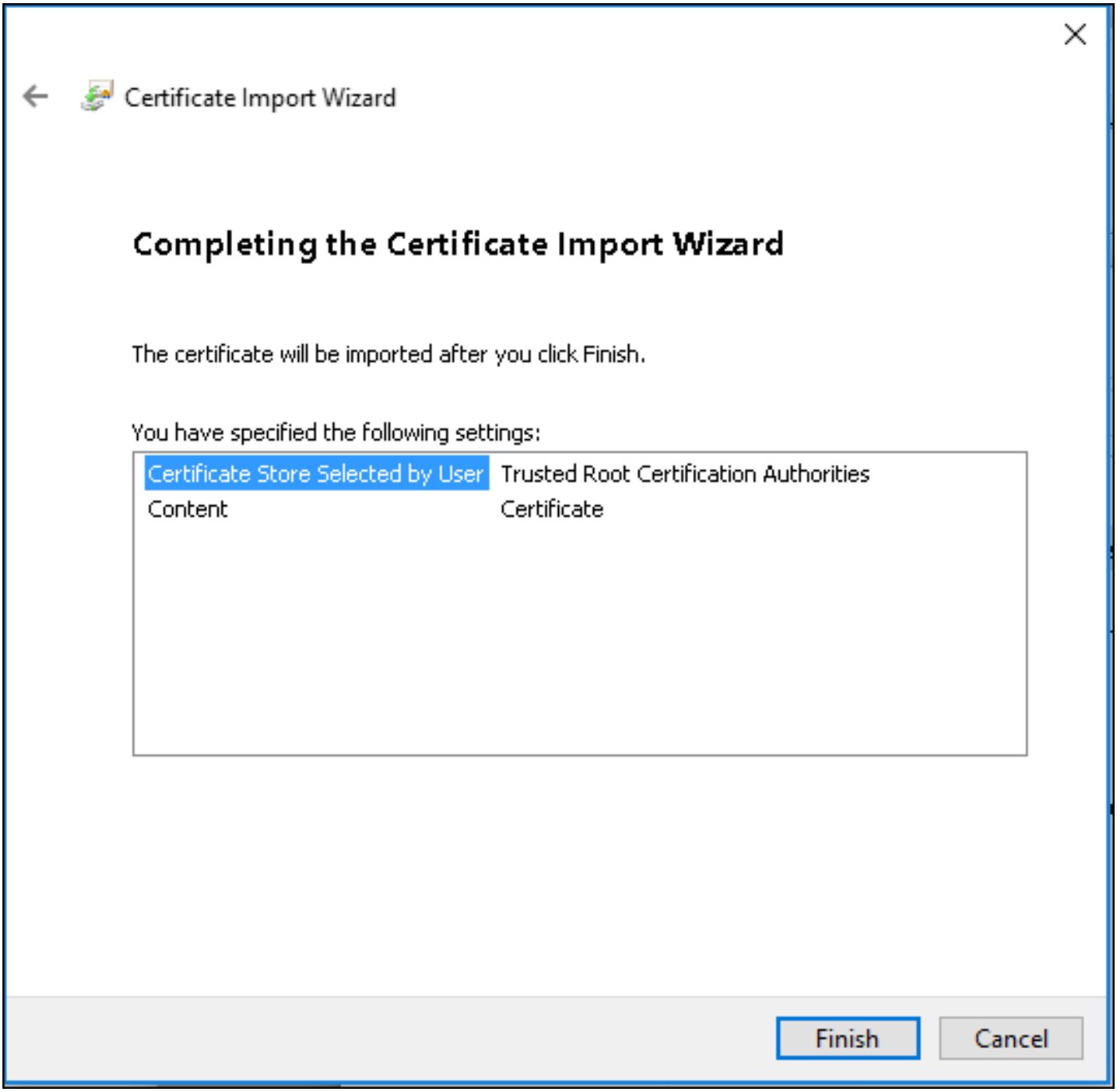
Choisissez de l'installer dans **Local Machine,** puis cliquez sur **Next (Suivant).**



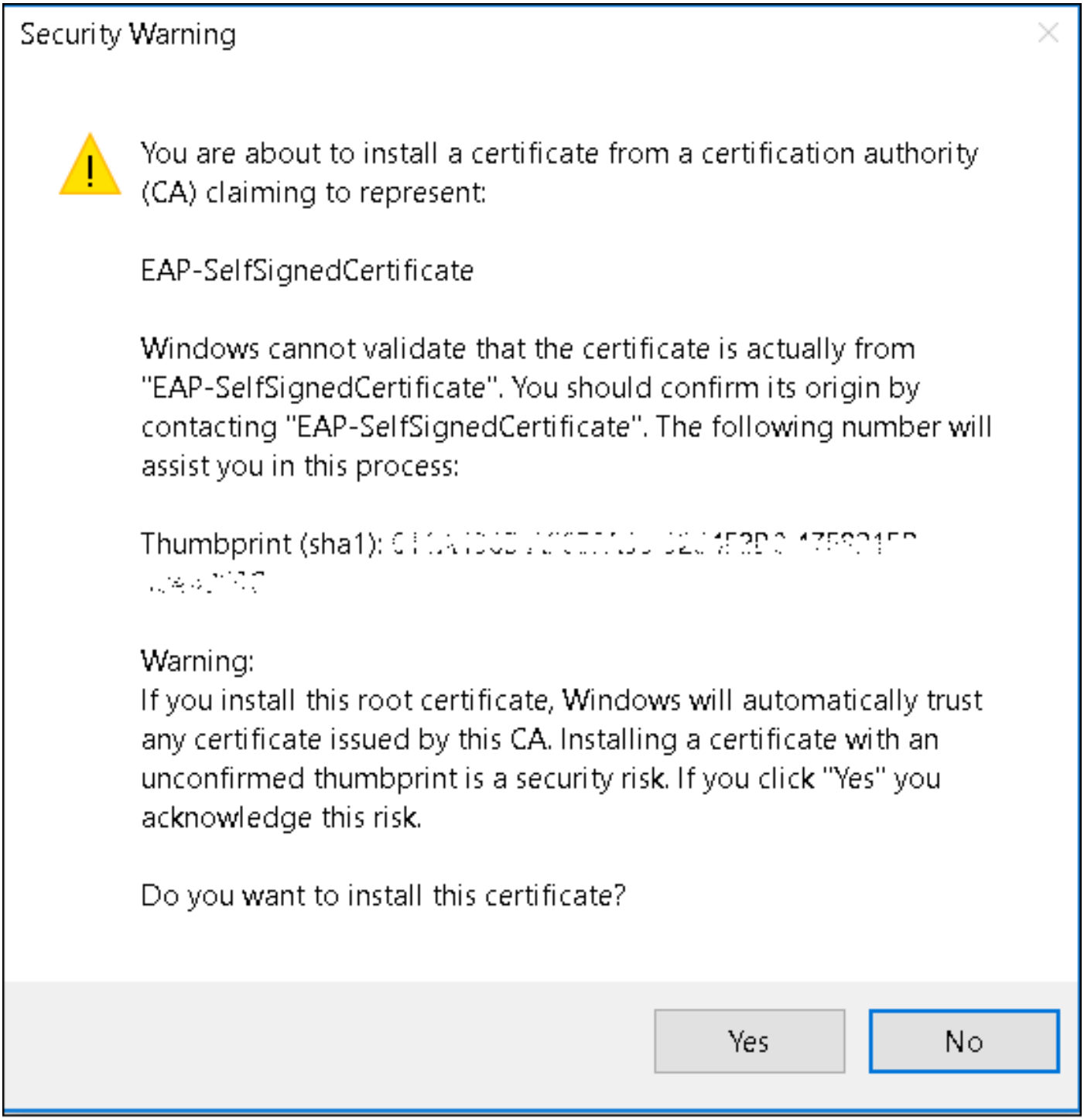
Sélectionnez **Placer tous les certificats dans le magasin suivant**, puis naviguez et choisissez **Autorités de certification racines de confiance**. Ensuite, cliquez sur **Suivant**.



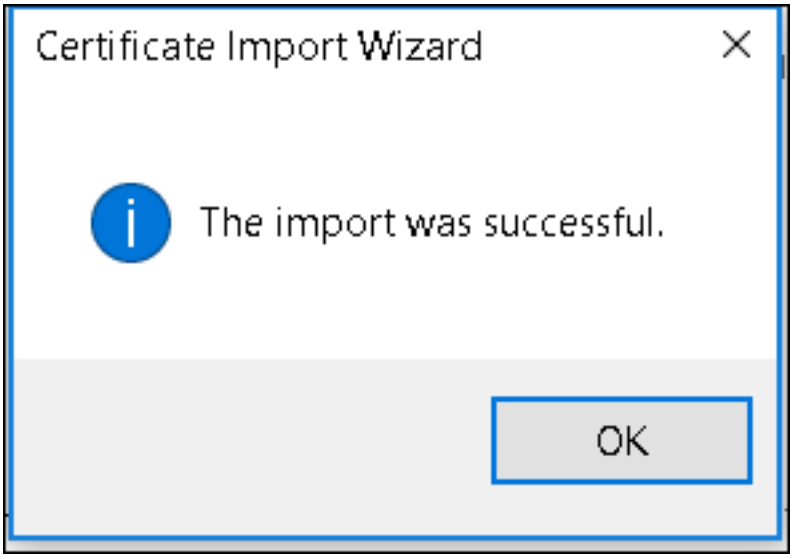
Cliquez ensuite sur **Terminer.**



Àla fin, cliquez sur **Oui** pour confirmer l'installation du certificat.

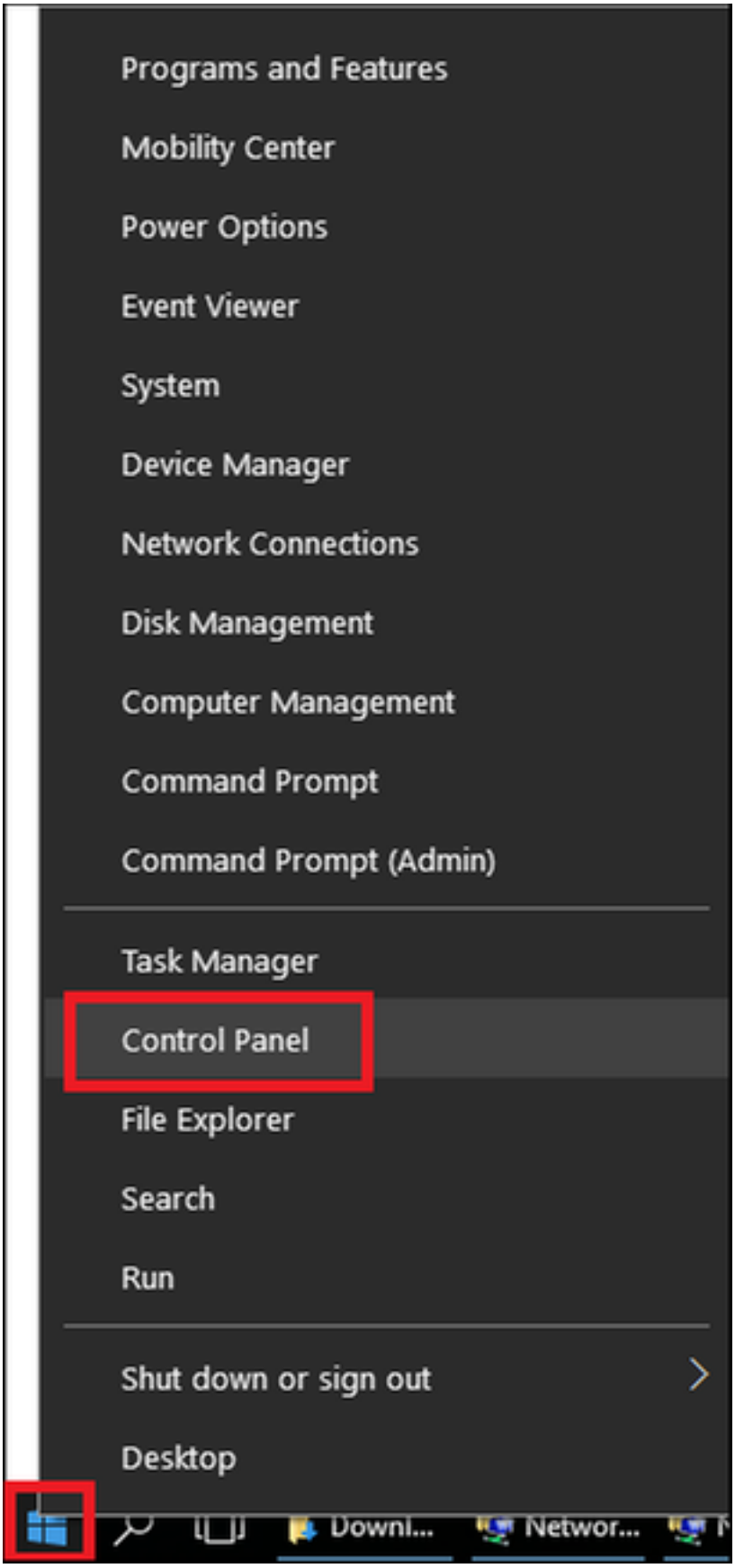


Enfin, cliquez sur **OK.**

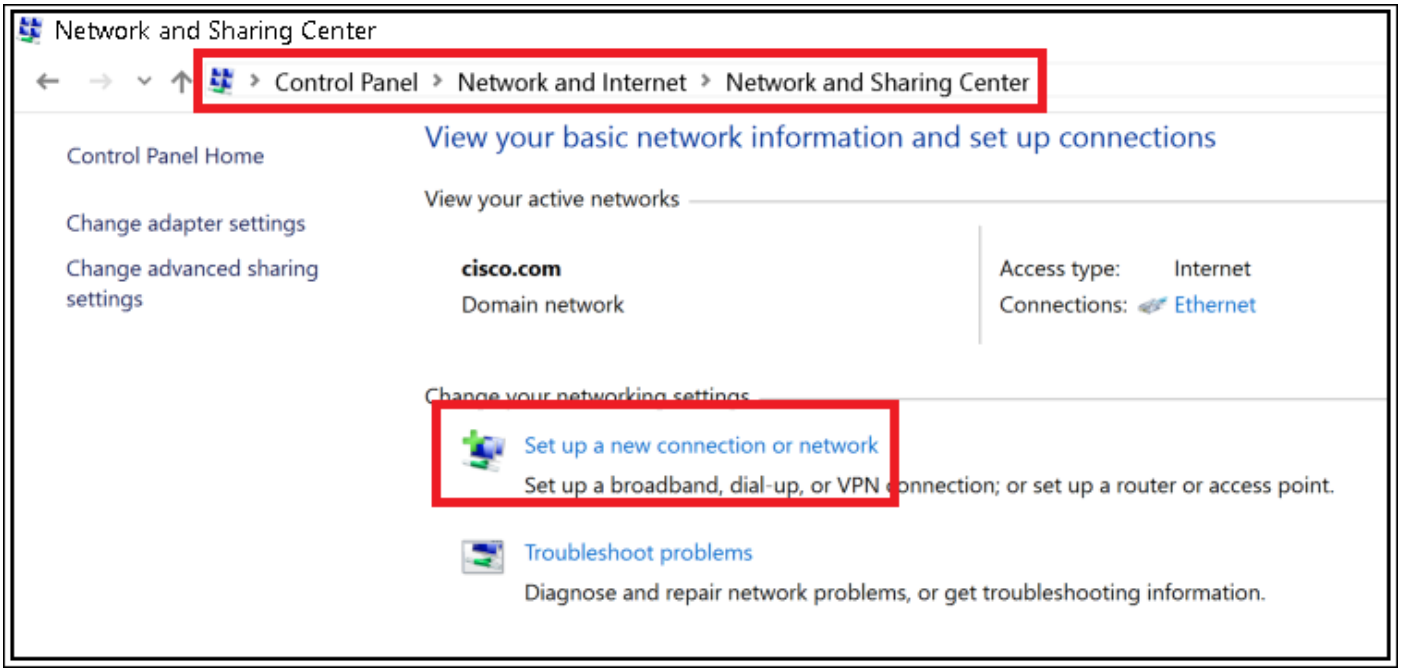


Configuration du périphérique final : création du profil WLAN

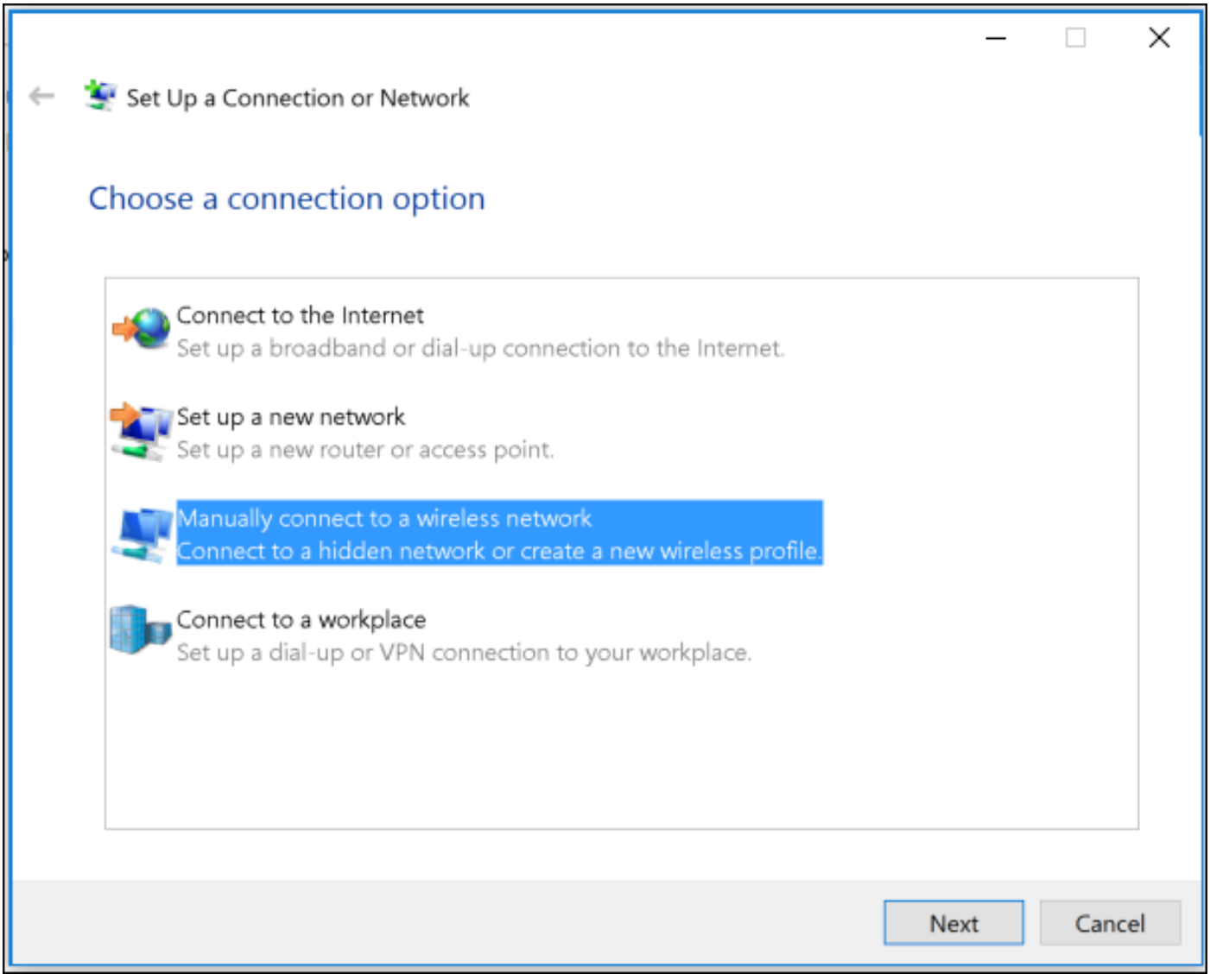
Étape 1. Cliquez avec le bouton droit sur l'icône **Démarrer** et sélectionnez **Panneau de configuration.**



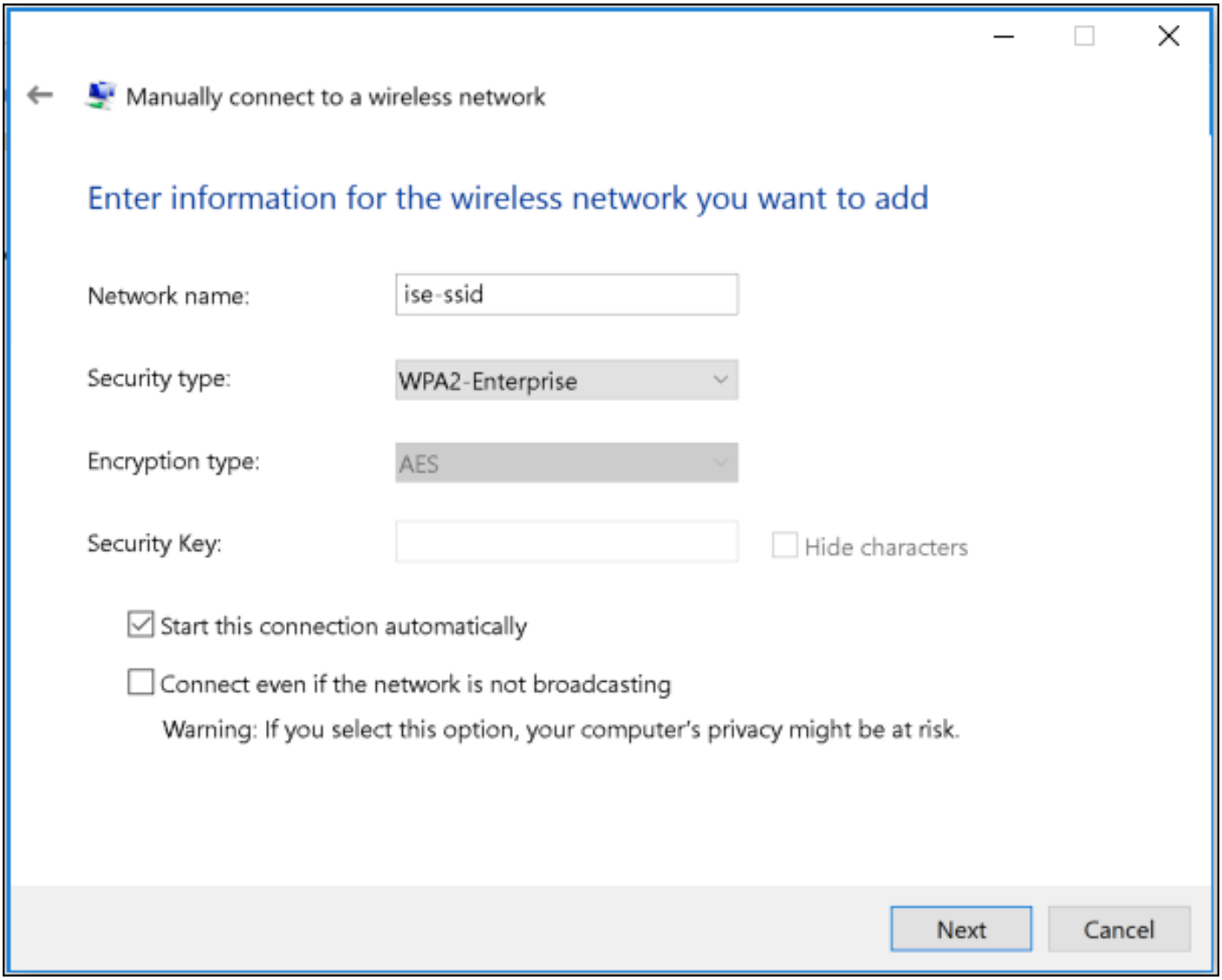
Étape 2. Accédez à **Réseau et Internet**, puis à **Centre Réseau et partage** et cliquez sur **Configurer une nouvelle connexion ou un nouveau réseau.**



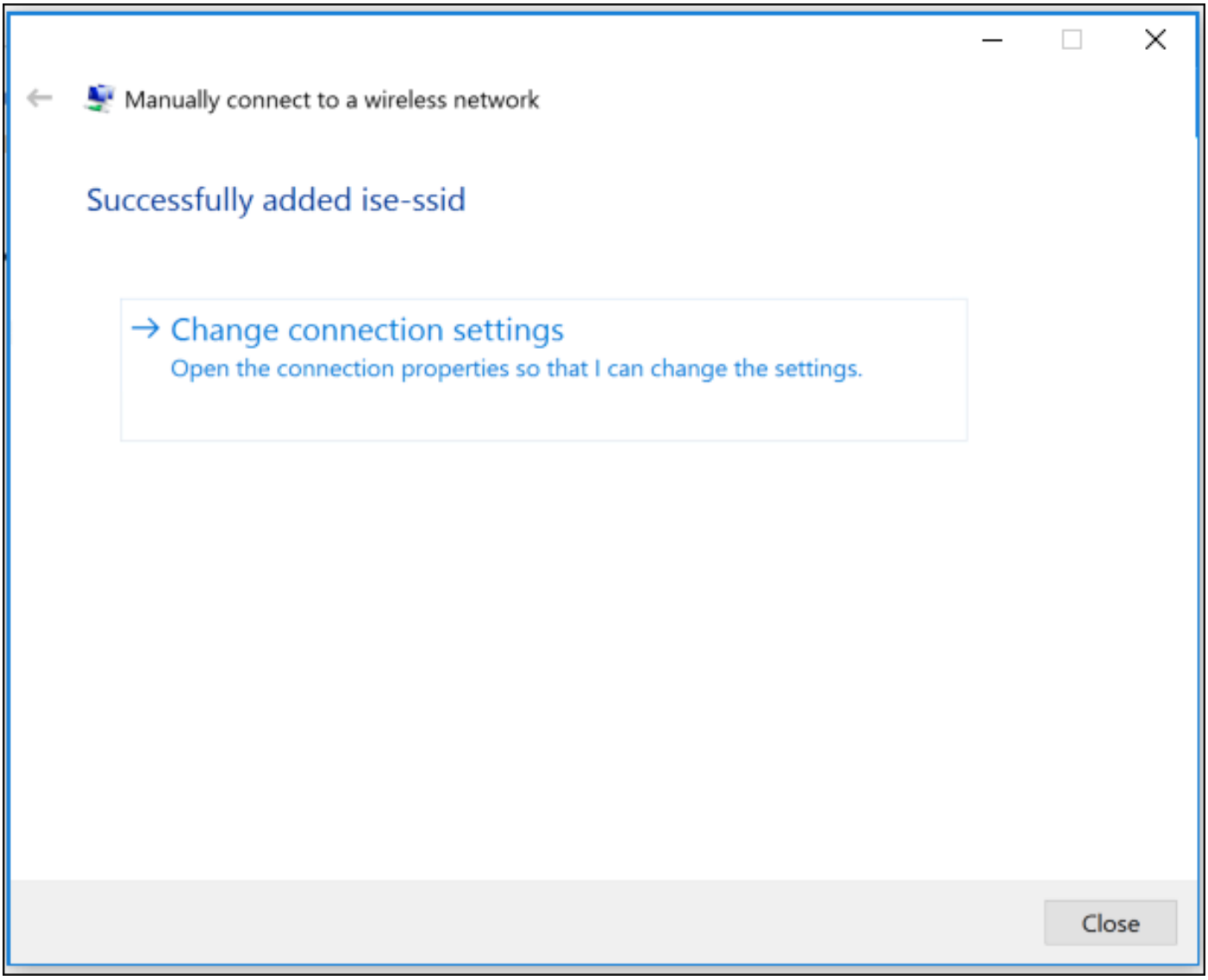
Étape 3. Sélectionnez **Connexion manuelle à un réseau sans fil** et cliquez sur **Suivant**.



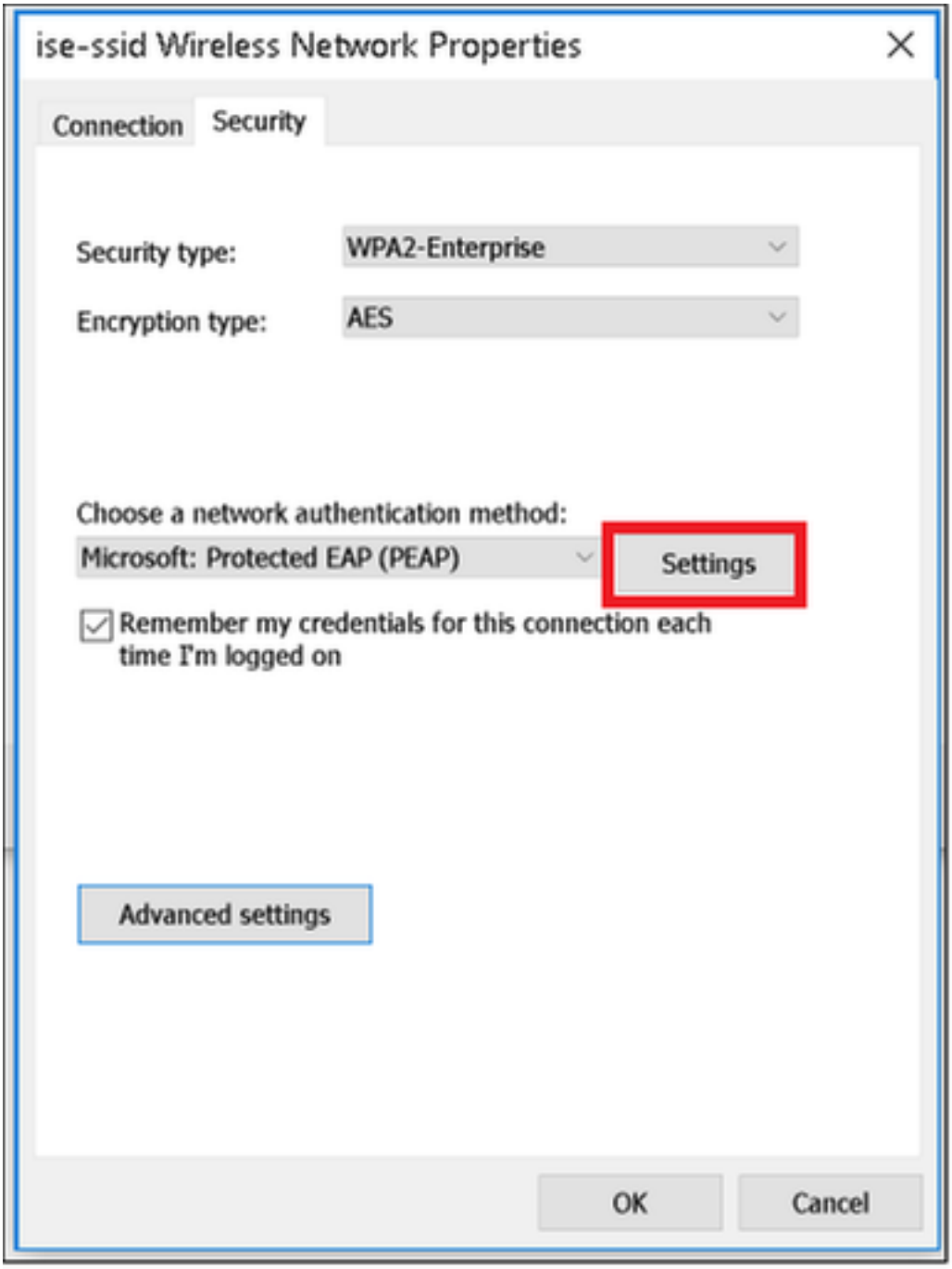
Étape 4. Entrez les informations avec le nom du SSID et du type de sécurité WPA2-Enterprise, puis cliquez sur **Next (Suivant)**.



Étape 5. Sélectionnez **Modifier les paramètres de connexion** pour personnaliser la configuration du profil WLAN.



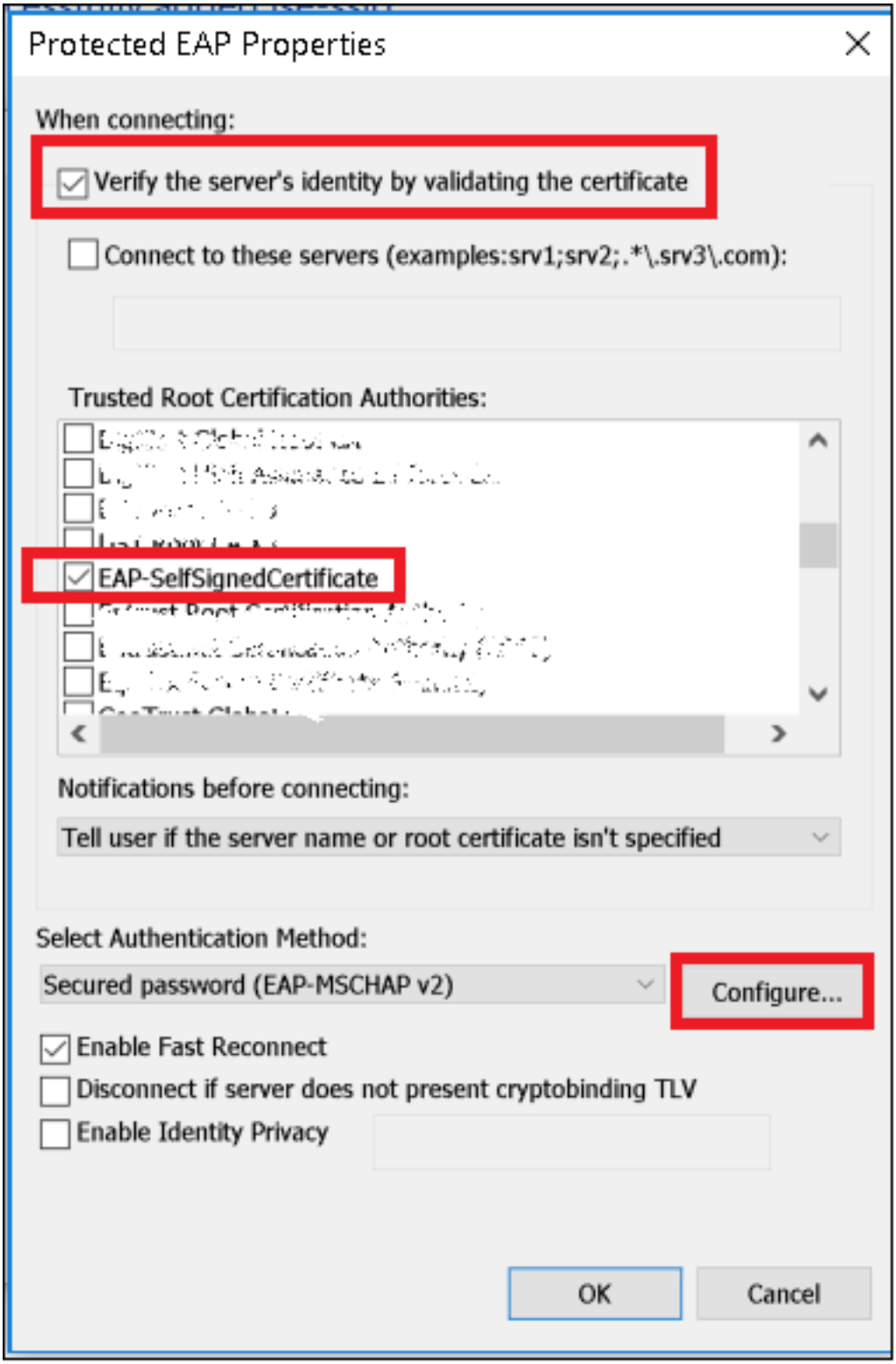
Étape 6. Accédez à l'onglet **Sécurité** et cliquez sur **Paramètres.**

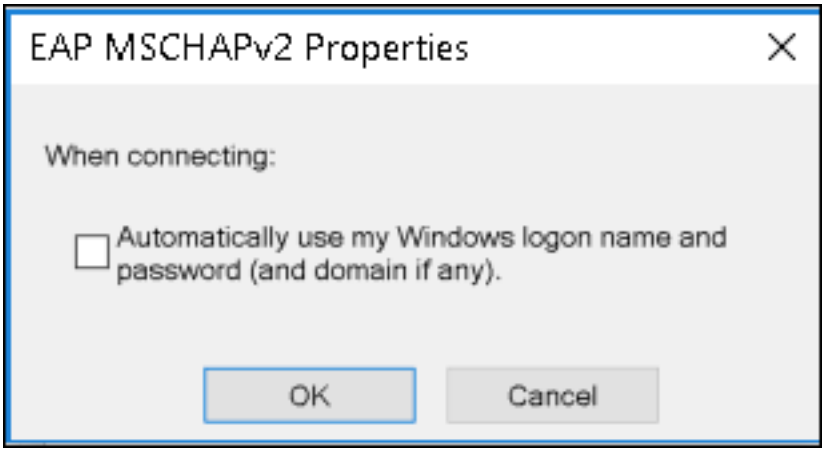


Étape 7. Choisissez si le serveur RADIUS est validé ou non.

Si oui, activez **Vérifier l'identité du serveur en validant le certificat** et à partir de **Autorités de certification racines de confiance :** sélectionnez le certificat auto-signé d'ISE.

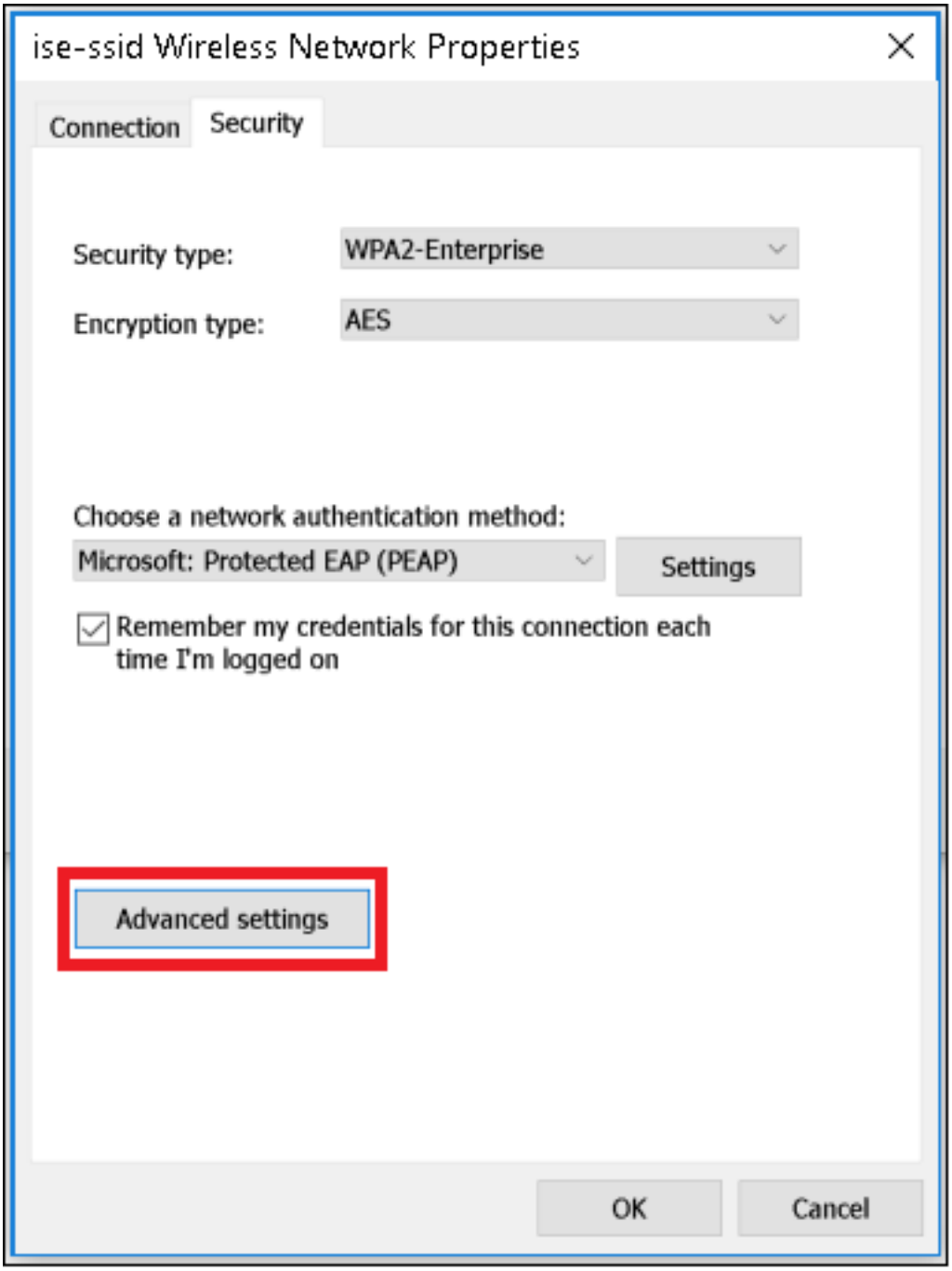
Après cela, sélectionnez **Configurer** et désactiver **Utiliser automatiquement mon nom de connexion et mon mot de passe Windows...**, puis cliquez sur **OK.**

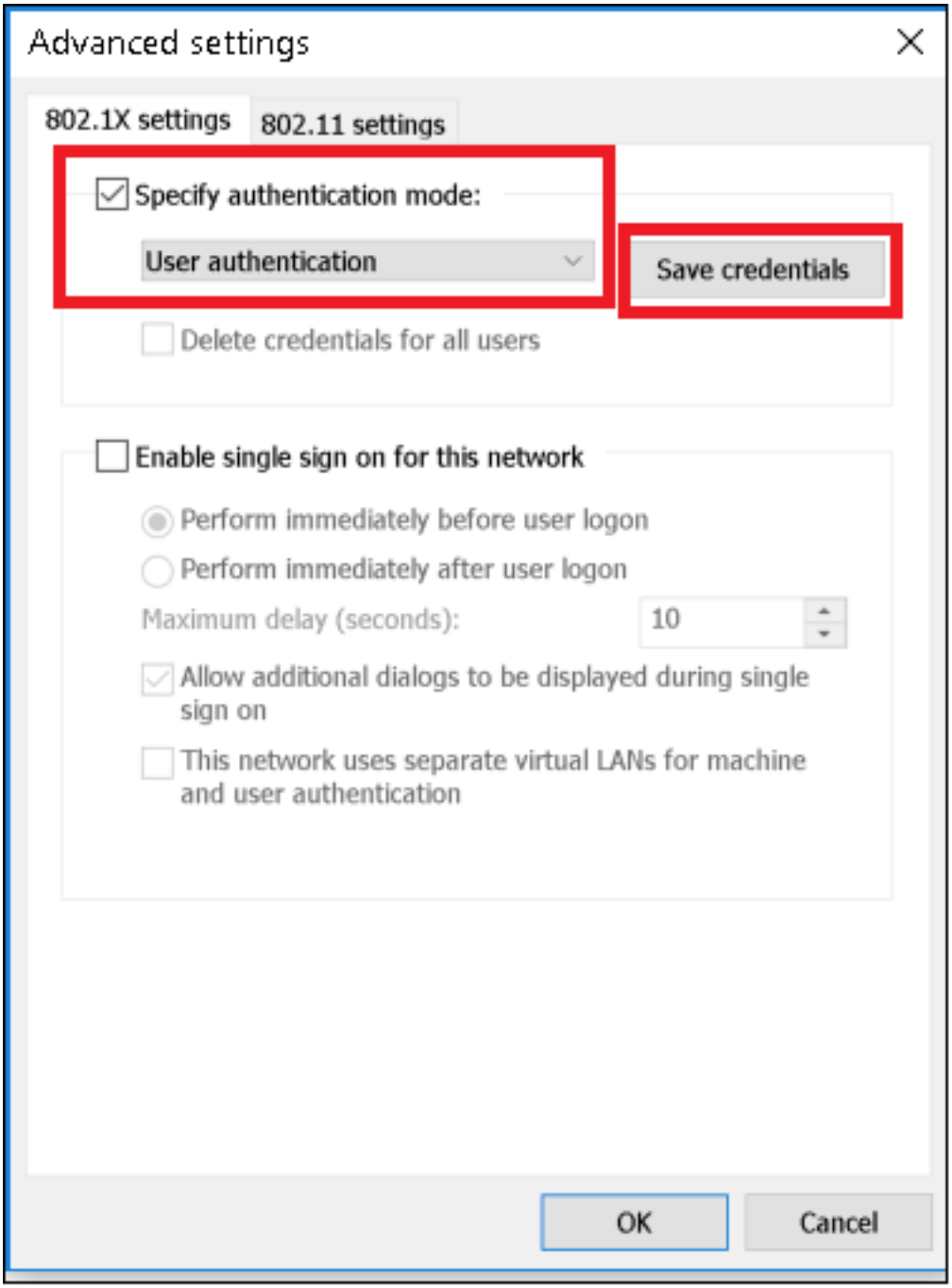

Protected EAP Properties
When connecting:
Verify the server's identity by validating the certificate
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):
Trusted Root Certification Authorities:
EAP-SelfSignedCertificate
Notifications before connecting:
Tell user if the server name or root certificate isn't specified
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
Configure...
Enable Fast Reconnect
Disconnect if server does not present cryptobinding TLV
Enable Identity Privacy
OK
Cancel

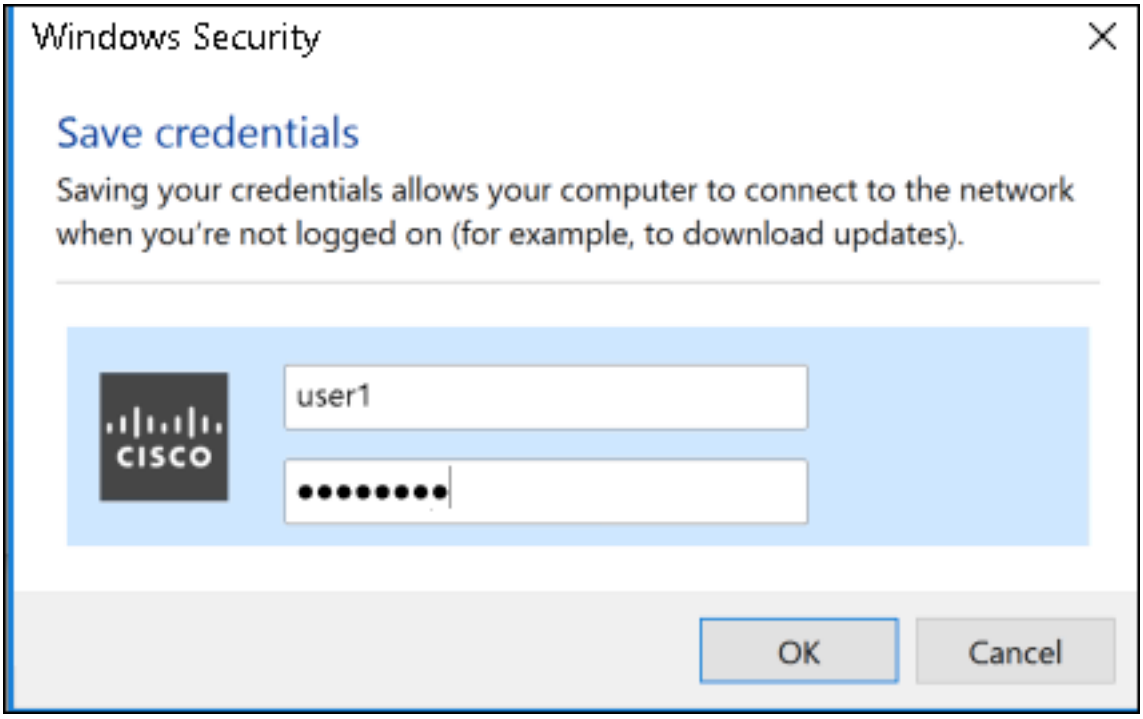

EAP MSCHAPv2 Properties
When connecting:
Automatically use my Windows logon name and password (and domain if any).
OK
Cancel

Étape 8. Configurer les informations d'identification de l'utilisateur

Une fois de retour à l'onglet **Sécurité**, sélectionnez **Paramètres avancés**, spécifiez le mode d'authentification comme **authentification utilisateur** et enregistrez les informations d'identification configurées sur ISE pour authentifier l'utilisateur.




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



Vérification

Le flux d'authentification peut être vérifié du point de vue WLC ou ISE.

Processus d'authentification sur ME

Exécutez cette commande pour surveiller le processus d'authentification d'un utilisateur spécifique :

```
> debug client <mac-add-client>
```

Exemple d'authentification réussie (certains résultats ont été omis) :

```
*apfMsConnTask_0: Nov 25 16:36:24.333: 08:74:02:77:13:45 Processing assoc-req
station:08:74:02:77:13:45 AP:38:ed:18:c6:7b:40-01 thread:669ba80
*apfMsConnTask_0: Nov 25 16:36:24.333: 08:74:02:77:13:45 Association received from mobile on
BSSID 38:ed:18:c6:7b:4d AP 1852-4
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Applying site-specific Local Bridging
override for station 08:74:02:77:13:45 - vapId 3, site 'FlexGroup', interface 'management'
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Applying Local Bridging Interface
Policy for station 08:74:02:77:13:45 - vlan 0, interface id 0, interface 'management'
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Set Clinet Non AP specific
apfMsAccessVlan = 2400
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 This apfMsAccessVlan may be changed
later from AAA after L2 Auth
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Received 802.11i 802.1X key management
suite, enabling dot1x Authentication
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 START (0) Change state to
AUTHCHECK (2) last state START (0)
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 AUTHCHECK (2) Change state to
8021X_REQD (3) last state AUTHCHECK (2)
```

*apfMsConnTask_0: Nov 25 16:36:24.335: **08:74:02:77:13:45 0.0.0.0 8021X_REQD (3) DHCP required on AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3for this client**
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 apfPemAddUser2:session timeout forstation 08:74:02:77:13:45 - Session Tout 0, apfMsTimeOut '0' and sessionTimerRunning flag is 0
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Stopping deletion of Mobile Station: (callerId: 48)
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Func: apfPemAddUser2, Ms Timeout = 0, Session Timeout = 0
*apfMsConnTask_0: Nov 25 16:36:24.335: 0**8:74:02:77:13:45 Sending assoc-resp with status 0 station:08:74:02:77:13:45 AP:38:ed:18:c6:7b:40-01 on apVapId 3**
*apfMsConnTask_0: Nov 25 16:36:24.335: **08:74:02:77:13:45 Sending Assoc Response to station on BSSID 38:ed:18:c6:7b:4d (status 0) ApVapId 3 Slot 1**
*spamApTask0: Nov 25 16:36:24.341: 08:74:02:77:13:45 Sent dot1x auth initiate message for mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 reauth_sm state transition 0 ---> 1 for mobile 08:74:02:77:13:45 at 1x_reauth_sm.c:47
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 EAP-PARAM Debug - eap-params for Wlan-Id :3 is disabled - applying Global eap timers and retries
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Disable re-auth, use PMK lifetime.
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Station 08:74:02:77:13:45 setting dot1x reauth timeout = 1800
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 dot1x - moving mobile 08:74:02:77:13:45 into Connecting state
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: **08:74:02:77:13:45 Sending EAP-Request/Identity to mobile 08:74:02:77:13:45 (EAP Id 1)**
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.401: **08:74:02:77:13:45 Received EAPOL EAPPKT from mobile 08:74:02:77:13:45**
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.401: **08:74:02:77:13:45 Received Identity Response (count=1) from mobile 08:74:02:77:13:45**
.
.
.
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: **08:74:02:77:13:45 Processing Access-Accept for mobile 08:74:02:77:13:45**
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: **08:74:02:77:13:45 Username entry (user1) created in mscb for mobile, length = 253**
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Station 08:74:02:77:13:45 setting dot1x reauth timeout = 1800
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Creating a PKC PMKID Cache entry for station 08:74:02:77:13:45 (RSN 2)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Adding BSSID 38:ed:18:c6:7b:4d to PMKID cache at index 0 for station 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: New PMKID: (16)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] 80 3a 20 8c 8f c2 4c 18 7d 4c 28 e7 7f 10 11 03
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Adding Audit session ID payload in Mobility handoff
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 0 PMK-update groupcast messages sent
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 PMK sent to mobility group
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Disabling re-auth since PMK lifetime can take care of same.
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Sending EAP-Success to mobile 08:74:02:77:13:45 (EAP Id 70)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Freeing AAACB from Dot1xCB as AAA auth is done for mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Found an cache entry for BSSID 38:ed:18:c6:7b:4d in PMKID cache at index 0 of station 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Found an cache entry for BSSID 38:ed:18:c6:7b:4d in PMKID cache at index 0 of station 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: Including PMKID in M1 (16)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] 80 3a 20 8c 8f c2 4c 18 7d 4c 28 e7 7f 10 11 03
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: M1 - Key Data: (22)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] dd 14 00 0f ac 04 80 3a 20 8c 8f c2 4c 18 7d 4c
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0016] 28 e7 7f 10 11 03

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: **08:74:02:77:13:45 Starting key exchange to mobile 08:74:02:77:13:45, data packets will be dropped**
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: **08:74:02:77:13:45 Sending EAPOL-Key Message to mobile 08:74:02:77:13:45**
state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Reusing allocated memory for EAP Pkt for retransmission to mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Entering Backend Auth Success state (id=70) for mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Received Auth Success while in Authenticating state for mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 dot1x - moving mobile 08:74:02:77:13:45 into Authenticated state
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received EAPOL-Key from mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: **08:74:02:77:13:45 Received EAPOL-key in PTK_START state (message 2) from mobile 08:74:02:77:13:45**
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Successfully computed PTK from PMK!!!
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received valid MIC in EAPOL Key Message M2!!!!!
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000000: 30 14 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00 0..............
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000010: 00 0f ac 01 0c 00 ......
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000000: 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00 00 0f ....
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000010: ac 01 0c 00 ....
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 PMK: Sending cache add
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Stopping retransmission timer for mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: **08:74:02:77:13:45 Sending EAPOL-Key Message to mobile 08:74:02:77:13:45**
state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Reusing allocated memory for EAP Pkt for retransmission to mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: **08:74:02:77:13:45 Received EAPOL-key in PTKINITNEGOTIATING state (message 4) from mobile 08:74:02:77:13:45**
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Stopping retransmission timer for mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: **08:74:02:77:13:45 0.0.0.0 8021X_REQD (3) Change state to L2AUTHCOMPLETE (4) last state 8021X_REQD (3)**
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Mobility query, PEM State: L2AUTHCOMPLETE
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building Mobile Announce :
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building Client Payload:
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Ip: 0.0.0.0
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Vlan Ip: 172.16.0.136, Vlan mask : 255.255.255.224
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Vap Security: 16384
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Virtual Ip: 192.0.2.1
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 ssid: ise-ssid
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building VlanIpPayload.
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) DHCP required on AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3for this client
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Not Using WMM Compliance code qosCap 00
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3 flex-acl-name:
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: **08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4)**
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6623, Adding TMP rule
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Adding Fast Path rule

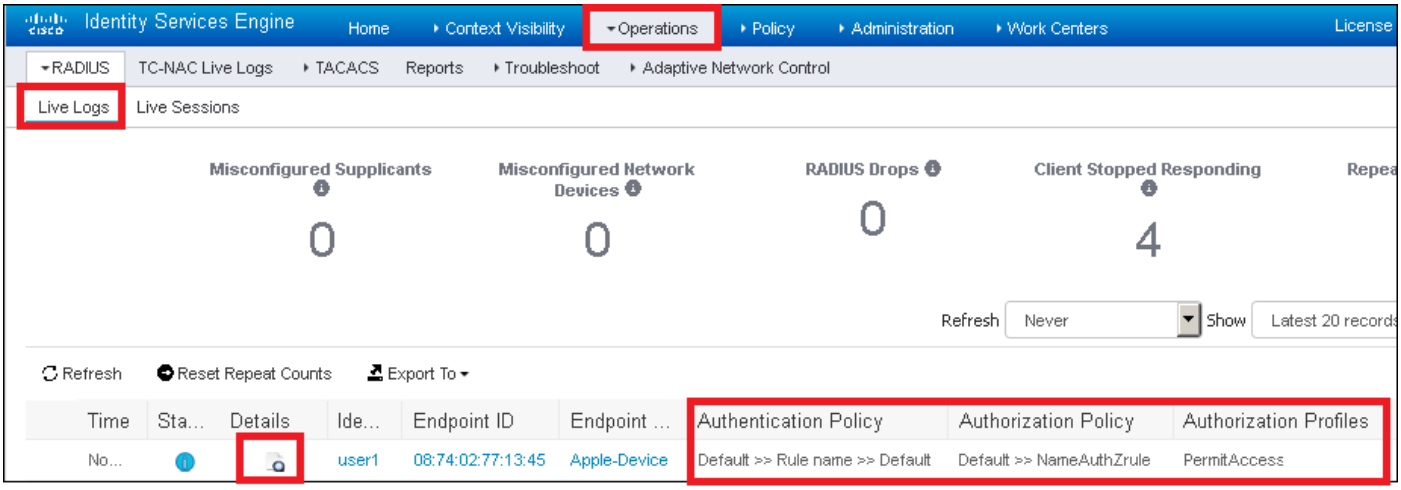
```
type = Airespace AP - Learn IP address
on AP 38:ed:18:c6:7b:40, slot 1, interface = 1, QOS = 0
IPv4 ACL ID = 255, IPv
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) mobility role
update request from Unassociated to Local
Peer = 0.0.0.0, Old Anchor = 0.0.0.0, New Anchor = 172.16.0.136
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) State Update from
Mobility-Incomplete to Mobility-Complete, mobility role=Local, client
state=APF_MS_STATE_ASSOCIATED
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) pemAdvanceState2
6261, Adding TMP rule
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Replacing Fast
Path rule
type = Airespace AP - Learn IP address
on AP 38:ed:18:c6:7b:40, slot 1, interface = 1, QOS = 0
IPv4 ACL ID = 255,
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Successfully
plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*pemReceiveTask: Nov 25 16:36:25.990: 08:74:02:77:13:45 0.0.0.0 Added NPU entry of type 9,
dtlFlags 0x0
*pemReceiveTask: Nov 25 16:36:25.990: 08:74:02:77:13:45 0.0.0.0 Added NPU entry of type 9,
dtlFlags 0x0
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 WcdbClientUpdate: IP Binding from WCDB
ip_learn_type 1, add_or_delete 1
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 IPv4 Addr: 0:0:0:0
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 In apfRegisterIpAddrOnMscb_debug:
regType=1 Invalid src IP address, 0.0.0.0 is part of reserved ip address range (caller
apf_ms.c:3593)
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 IPv4 Addr: 0:0:0:0
*apfReceiveTask: Nov 25 16:36:27.840: 08:74:02:77:13:45 WcdbClientUpdate: IP Binding from WCDB
ip_learn_type 1, add_or_delete 1
*apfReceiveTask: Nov 25 16:36:27.841: 08:74:02:77:13:45 172.16.0.16 DHCP_REQD (7) Change state
to RUN (20) last state DHCP_REQD (7)
```

Pour lire facilement les sorties du client de débogage, utilisez l'outil *Wireless debug analyseur* :

Analyseur de débogage sans fil

Processus d'authentification sur ISE

Accédez à **Operations > RADIUS > Live Logs** afin de connaître la stratégie d'authentification, la stratégie d'autorisation et le profil d'autorisation attribués à l'utilisateur.



Pour plus d'informations, cliquez sur **Détails** pour voir un processus d'authentification plus détaillé.