Configuration de l'authentification 802.1X avec PEAP, ISE 2.1 et WLC 8.3

Table des matières

Introduction

Ce document décrit comment configurer un réseau local sans fil (WLAN) avec la sécurité 802.1x et le remplacement du réseau local virtuel (VLAN).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- 802.1x
- PEAP (Protected Extensible Authentication Protocol)
- 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
- Identity Service Engine (ISE) v2.1
- Ordinateur portable Windows 10

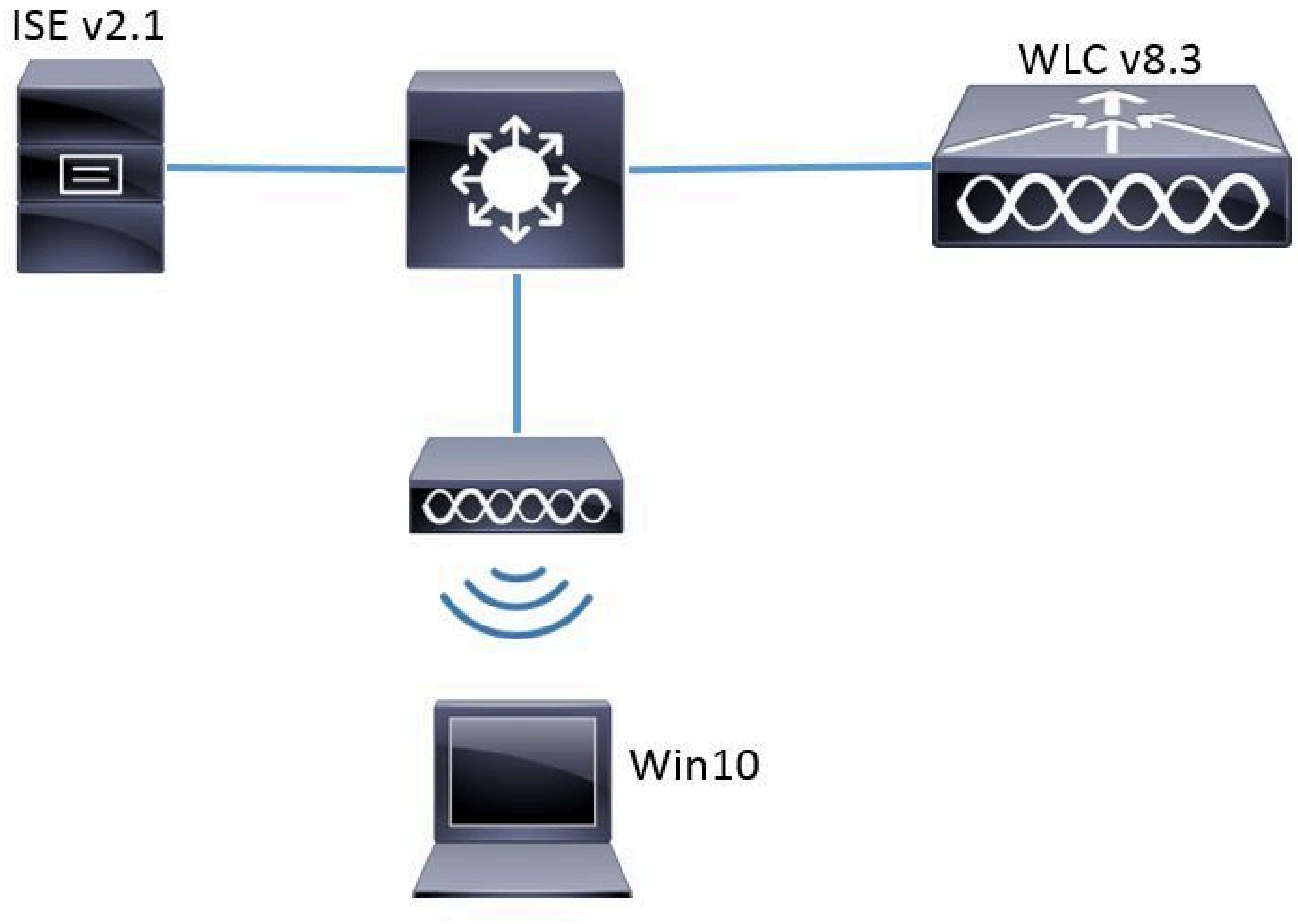
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Lorsque vous configurez un WLAN avec la sécurité 802.1x et un VLAN, vous pouvez le remplacer par le protocole EAP (Protected Extensible Authentication Protocol).

Configurer

Diagramme du réseau



Configuration

Les étapes générales sont les suivantes :

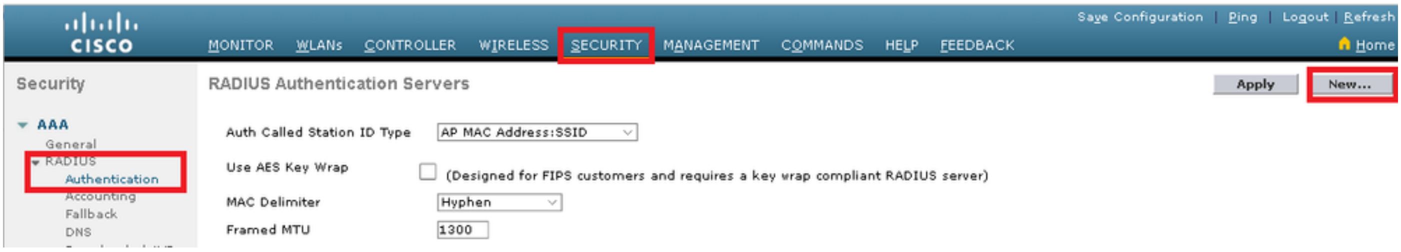
1. Déclarez le serveur RADIUS sur le WLC et vice versa pour permettre la communication entre eux.
2. Créez le SSID (Service Set Identifier) dans le WLC.
3. Créez la règle d'authentification sur ISE.
4. Créez le profil d'autorisation sur ISE.
5. Créez la règle d'autorisation sur ISE.
6. Configurez le terminal.

Déclarer le serveur RADIUS sur WLC

Afin de permettre la communication entre le serveur RADIUS et le WLC, vous devez enregistrer le serveur RADIUS sur le WLC et vice versa.

IUG:

Étape 1. Ouvrez l'interface graphique utilisateur du WLC et naviguez vers SECURITY > RADIUS > Authentication > New comme indiqué dans l'image.



RADIUS Authentication Servers

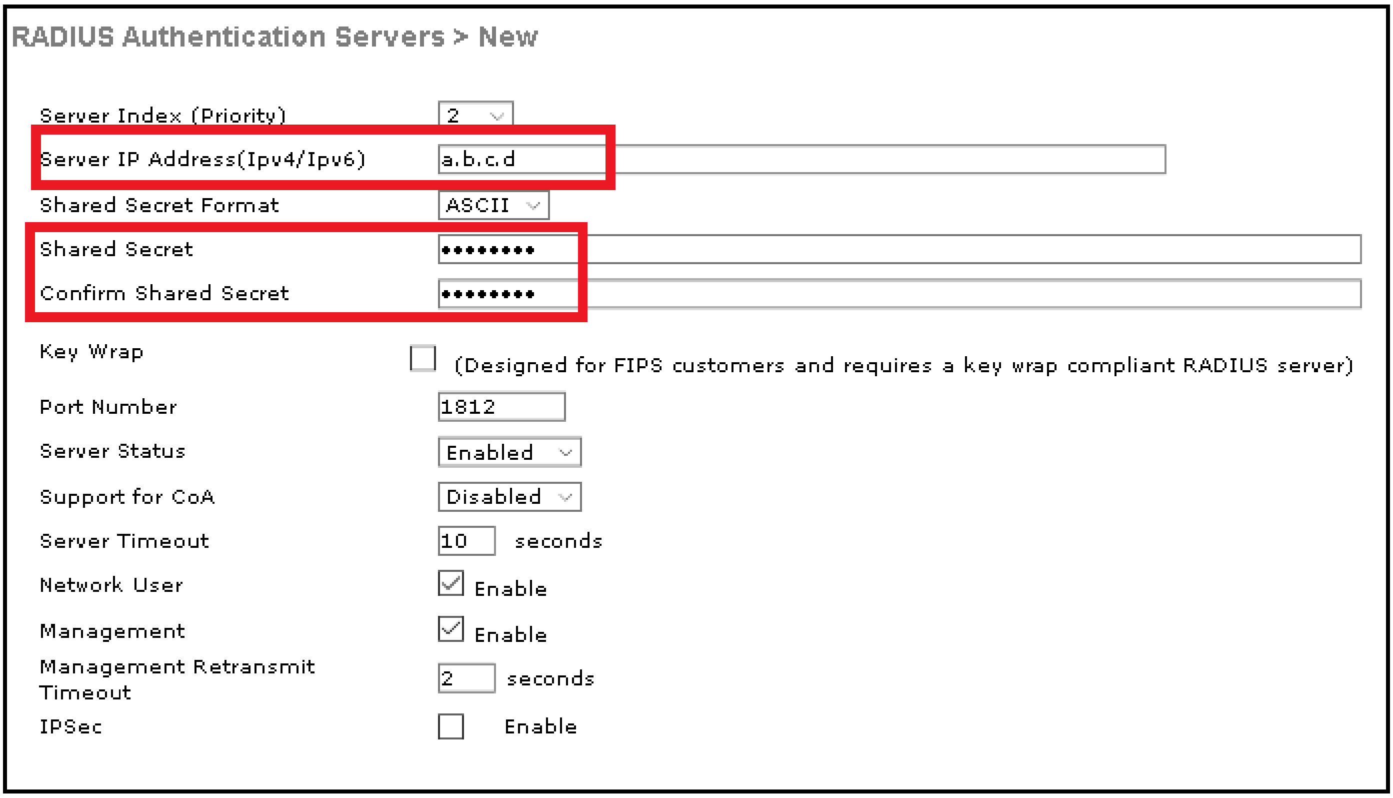
Auth Called Station ID Type: AP MAC Address:SSID

Use AES Key Wrap ☐ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter: Hyphen

Framed MTU: 1300

Étape 2. Entrez les informations du serveur RADIUS comme indiqué dans l'image.



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	□ (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	☑ Enable
Management	☑ Enable
Management Retransmit Timeout	2 seconds
IPSec	□ Enable

CLI :

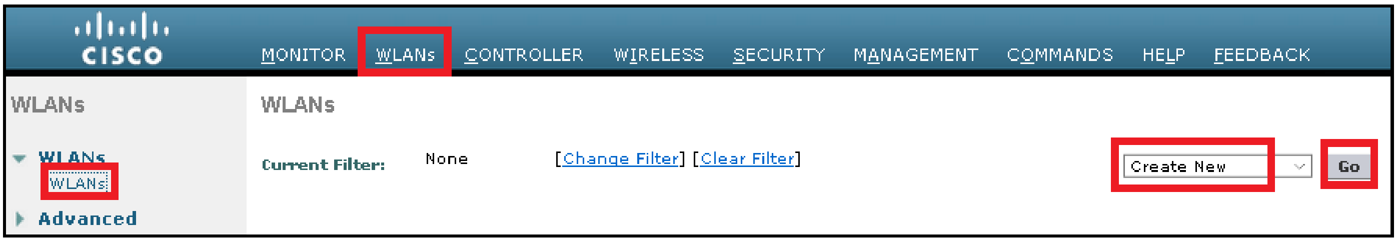
```
> config radius auth add <index> <a.b.c.d> 1812 ascii <shared-key>
> config radius auth disable <index>
> config radius auth retransmit-timeout <index> <timeout-seconds>
> config radius auth enable <index>
```

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

Créer un SSID

IUG:

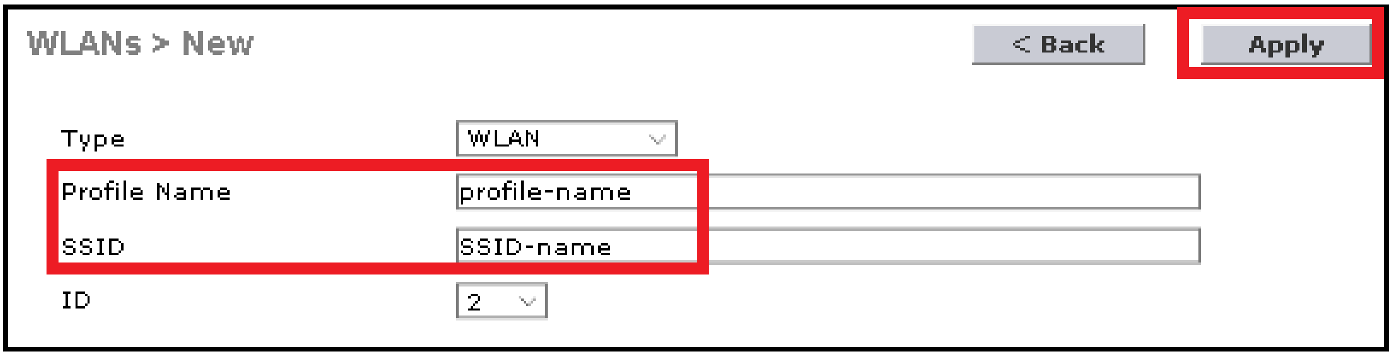
Étape 1. Ouvrez l'interface graphique utilisateur du WLC et naviguez jusqu'à WLANs > Create New > Go comme indiqué dans l'image.



WLANs

Current Filter: None

Étape 2. Choisissez un nom pour le SSID et le profil, puis cliquez sur Apply comme indiqué dans l'image.



Type WLAN

Profile Name profile-name

SSID SSID-name

ID 2

CLI :

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

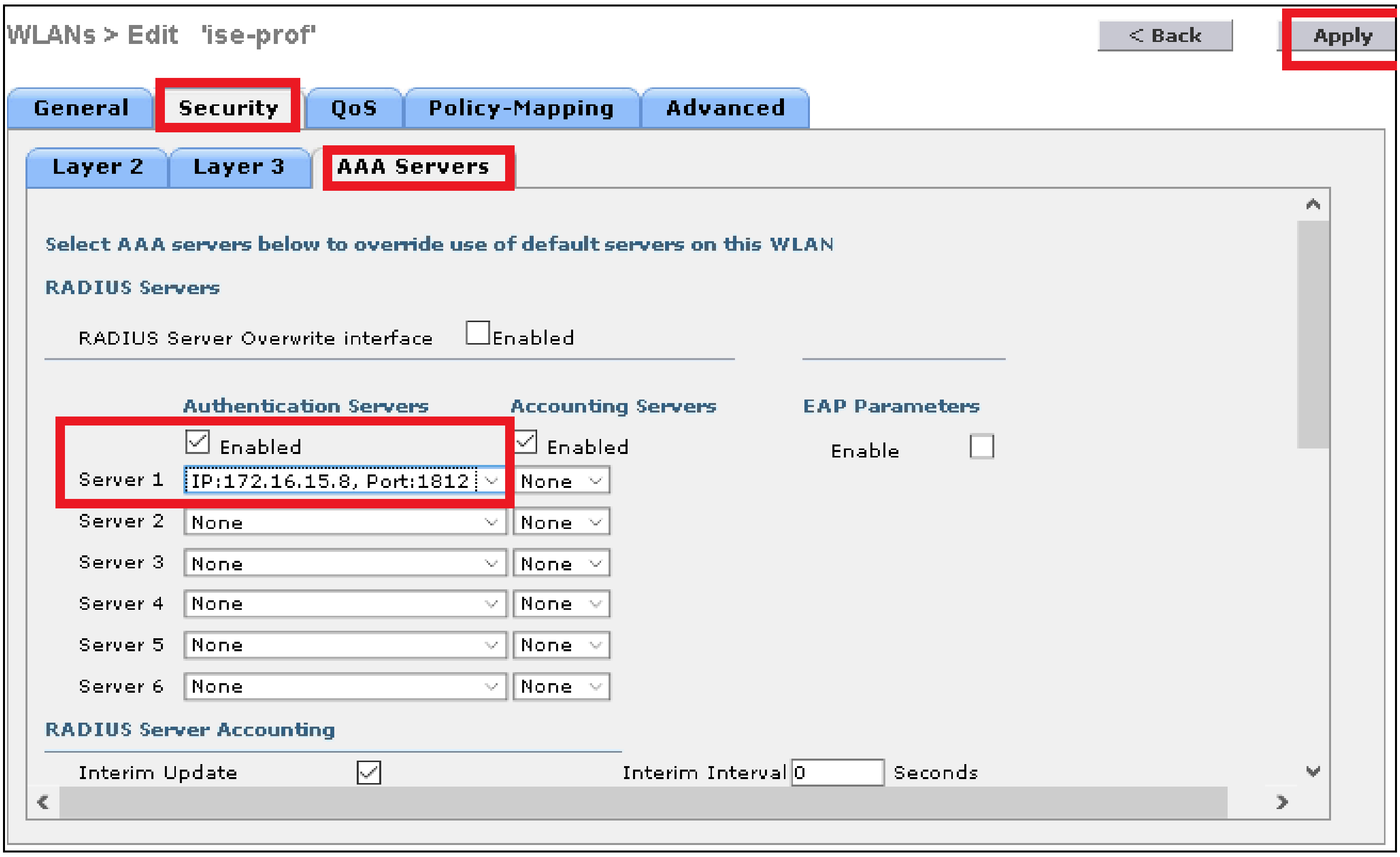
Étape 3. Attribuez le serveur RADIUS au WLAN.

CLI :

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

IUG:

Accédez à Security > AAA Servers et choisissez le serveur RADIUS souhaité, puis appuyez sur Apply comme indiqué dans l'image.



WLANs > Edit 'ise-prof'

Select AAA servers below to override use of default servers on this WLAN

RADIUS Servers

RADIUS Server Overwrite interface □Enabled

	Authentication Servers	Accounting Servers	EAP Parameters
	☑ Enabled	☑ Enabled	Enable □
Server 1	IP:172.16.15.8, Port:1812	None	
Server 2	None	None	
Server 3	None	None	
Server 4	None	None	
Server 5	None	None	
Server 6	None	None	

RADIUS Server Accounting

Interim Update ☑ Interim Interval 0 Seconds

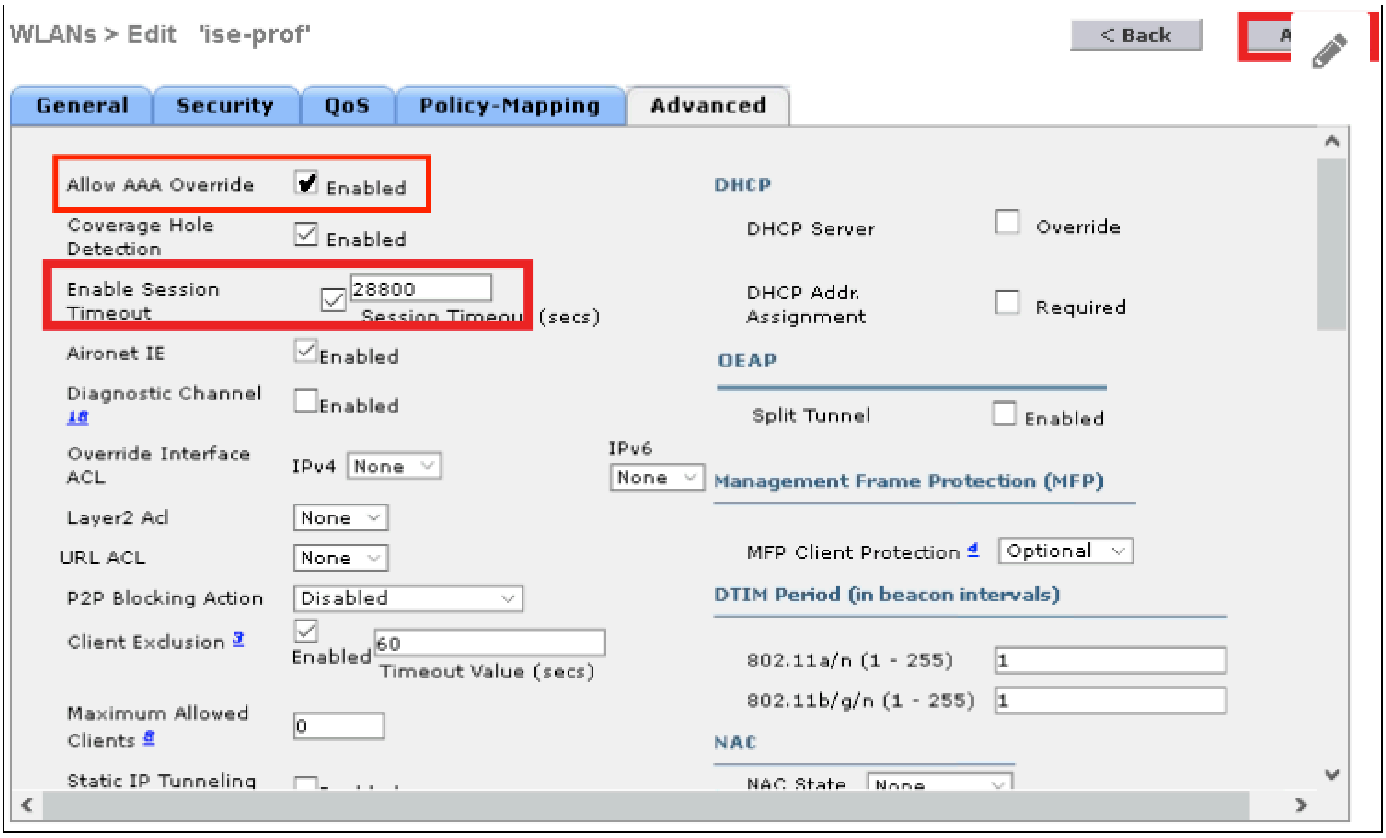
Étape 4. Activez Allow AAA Override et augmentez éventuellement le délai d'expiration de la session

CLI :

```
> config wlan aaa-override enable <wlan-id>
> config wlan session-timeout <wlan-id> <session-timeout-seconds>
```

IUG:

Accédez à WLANs > WLAN ID > Advanced et activez Allow AAA Override. Le cas échéant, spécifiez le délai d'expiration de la session comme indiqué dans l'image.



Allow AAA Override ☑ Enabled

Coverage Hole Detection ☑ Enabled

Enable Session Timeout ☑ 28800 Session Timeou (secs)

Aironet IE ☑ Enabled

Diagnostic Channel 18 □ Enabled

Override Interface ACL IPv4 None IPv6 None

Layer2 Acl None

URL ACL None

P2P Blocking Action Disabled

Client Exclusion 3 ☑ Enabled 60 Timeout Value (secs)

Maximum Allowed Clients 8 0

Static IP Tunneling □

DHCP

DHCP Server □ Override

DHCP Addr. Assignment □ Required

OEAP

Split Tunnel □ Enabled

Management Frame Protection (MFP)

MFP Client Protection 4 Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1

802.11b/g/n (1 - 255) 1

NAC

NAC State None

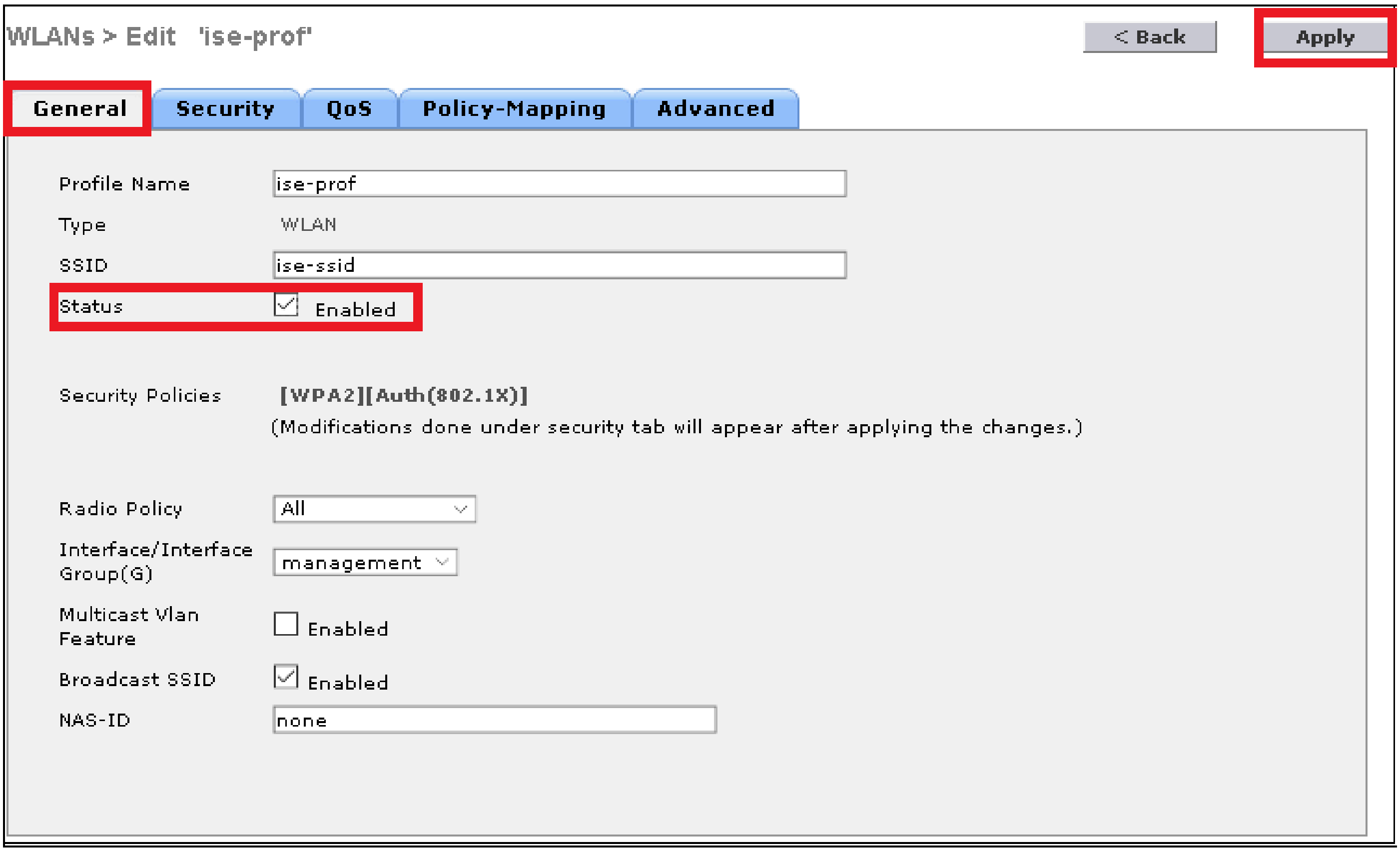
Étape 5. Activez le WLAN.

CLI :

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

IUG:

Accédez à WLANs > WLAN ID > General et activez le SSID comme indiqué dans l'image.



WLANs > Edit 'ise-prof'

< Back | Apply

General | Security | QoS | Policy-Mapping | Advanced

Profile Name: ise-prof

Type: WLAN

SSID: ise-ssid

Status: ☑ Enabled

Security Policies: [WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)

Radio Policy: All

Interface/Interface Group(G): management

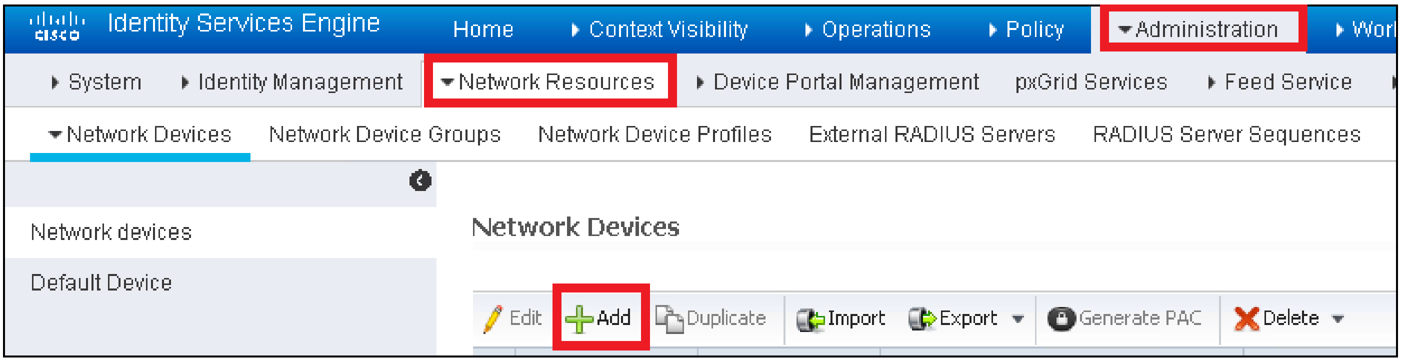
Multicast Vlan Feature: □ Enabled

Broadcast SSID: ☑ Enabled

NAS-ID: none

Déclarer WLC sur ISE

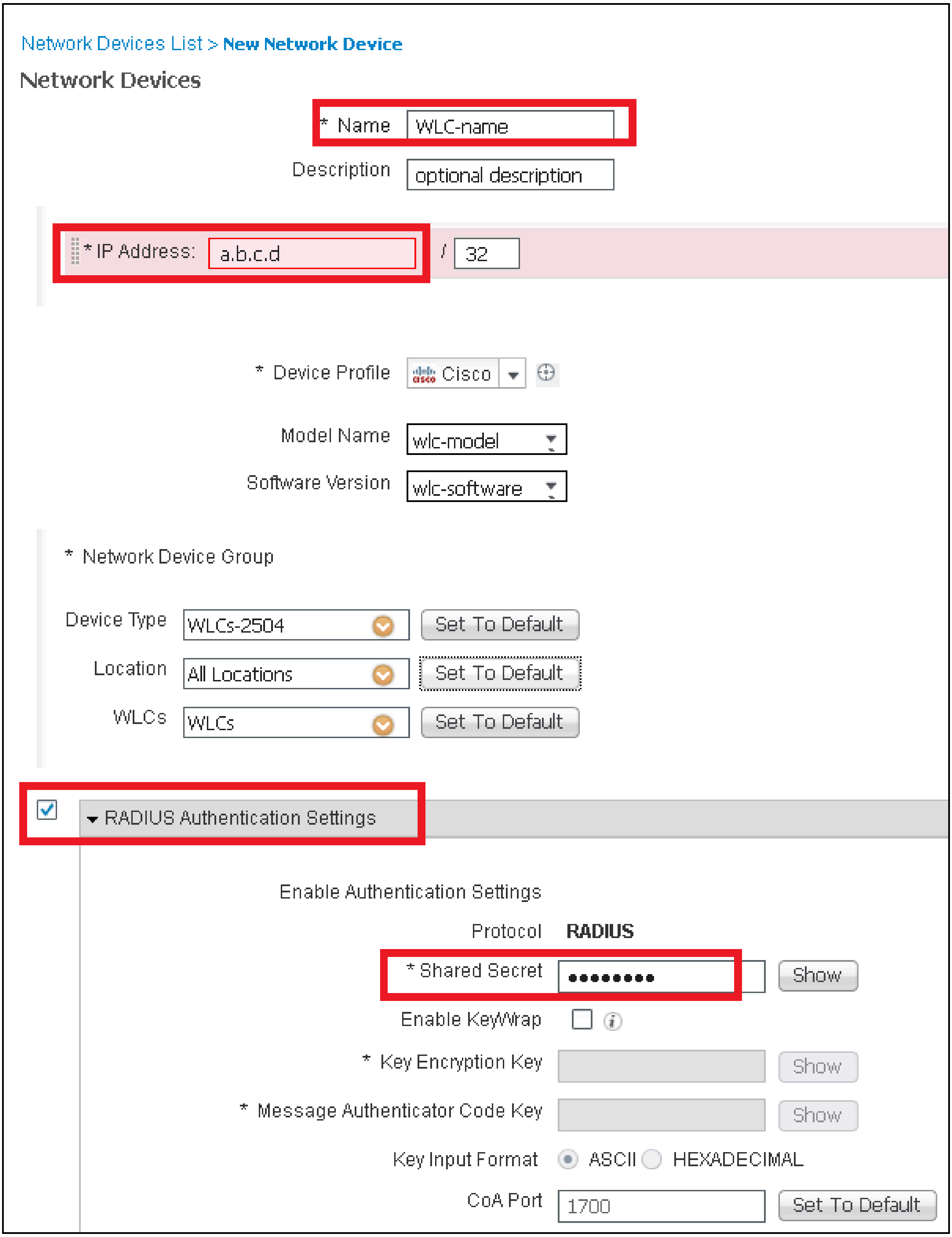
Étape 1. Ouvrez la console ISE et accédez à Administration > Network Resources > Network Devices > Add comme indiqué dans l'image.



Étape 2. Saisissez les valeurs.

Il peut éventuellement s'agir d'un nom de modèle, d'une version de logiciel, d'une description et d'une affectation de groupes de périphériques réseau en fonction des types de périphériques, de l'emplacement ou des WLC.

a.b.c.d correspond à l'interface WLC qui envoie l'authentification demandée. Par défaut, il s'agit de l'interface de gestion telle qu'illustrée dans l'image.



Network Devices List > **New Network Device**

Network Devices

* Name: WLC-name

Description: optional description

* IP Address: a.b.c.d / 32

* Device Profile: Cisco

Model Name: wlc-model

Software Version: wlc-software

* Network Device Group

Device Type: WLCs-2504 — Set To Default

Location: All Locations — Set To Default

WLCs: WLCs — Set To Default

☑ RADIUS Authentication Settings

Enable Authentication Settings

Protocol: **RADIUS**

* Shared Secret: ●●●●●●●●● — Show

Enable KeyWrap: □

* Key Encryption Key: — Show

* Message Authenticator Code Key: — Show

Key Input Format: ● ASCII ○ HEXADECIMAL

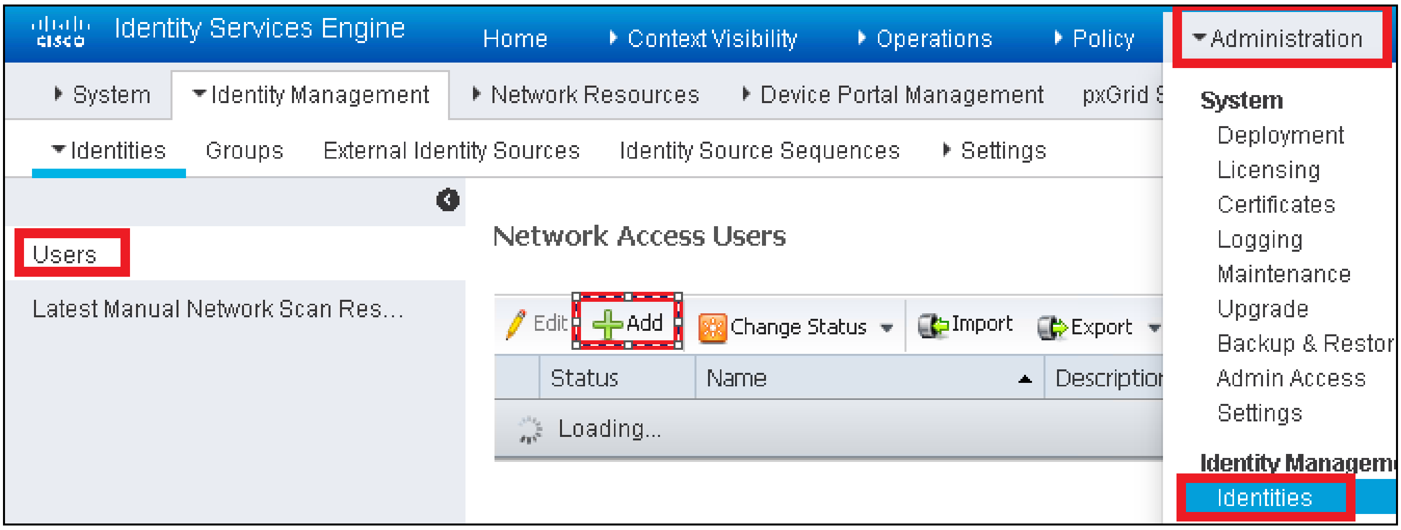
CoA Port: 1700 — Set To Default

Pour plus d'informations sur les groupes de périphériques réseau :

ISE – Groupes d’appareils réseau

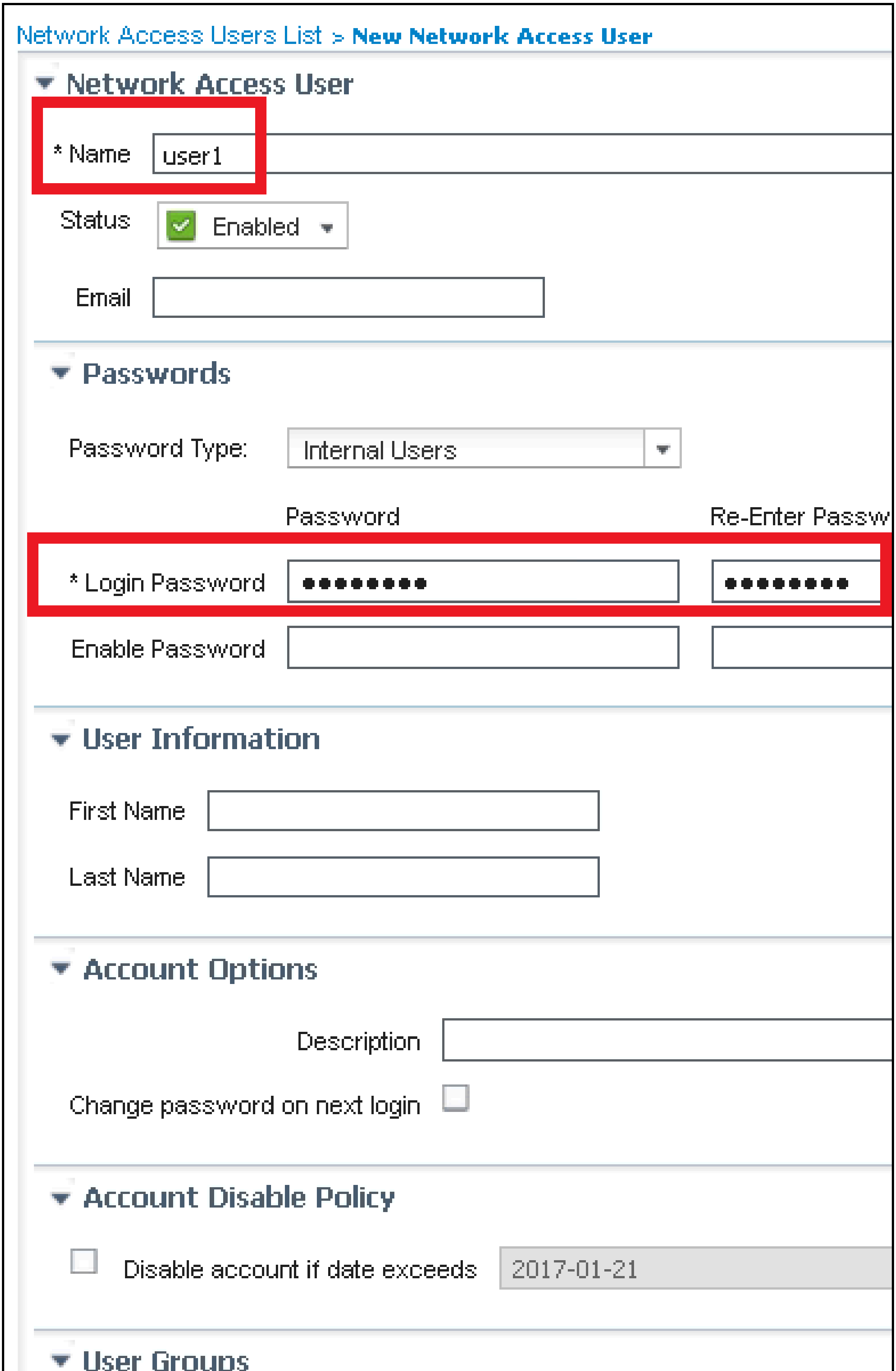
Créer un nouvel utilisateur sur ISE

Étape 1. Allez à Administration > Identity Management > Identities > Users > Add (gestion > gestion des identités > identités > utilisateurs > ajouter) en suivant les indications de l’image.



Étape 2. Entrez l’information.

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



Network Access Users List > **New Network Access User**

Network Access User

* Name user1

Status ☑ Enabled

Email

Passwords

Password Type: Internal Users

	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 2017-01-21

User Groups

2. Ignorez la validation du serveur RADIUS et faites confiance à tout serveur RADIUS utilisé pour effectuer l'authentification (non recommandé, car il peut devenir un problème de sécurité).

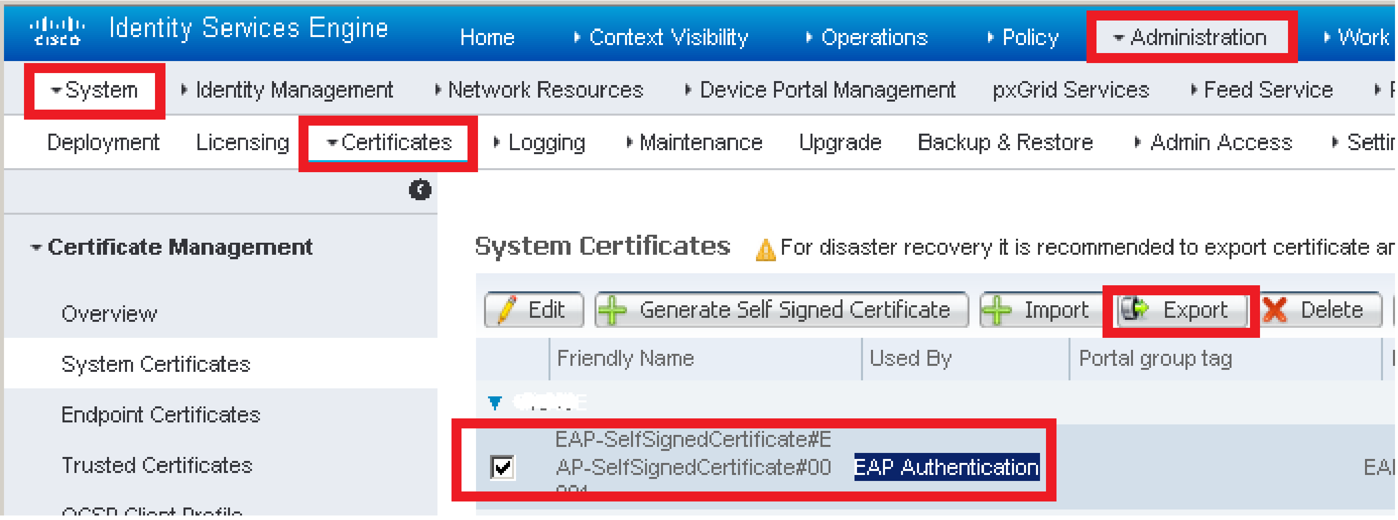
La configuration de ces options est expliquée dans Configuration du périphérique final - Créer le profil WLAN - Étape 7.

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

Étape 1. Exporter le certificat auto-signé.

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

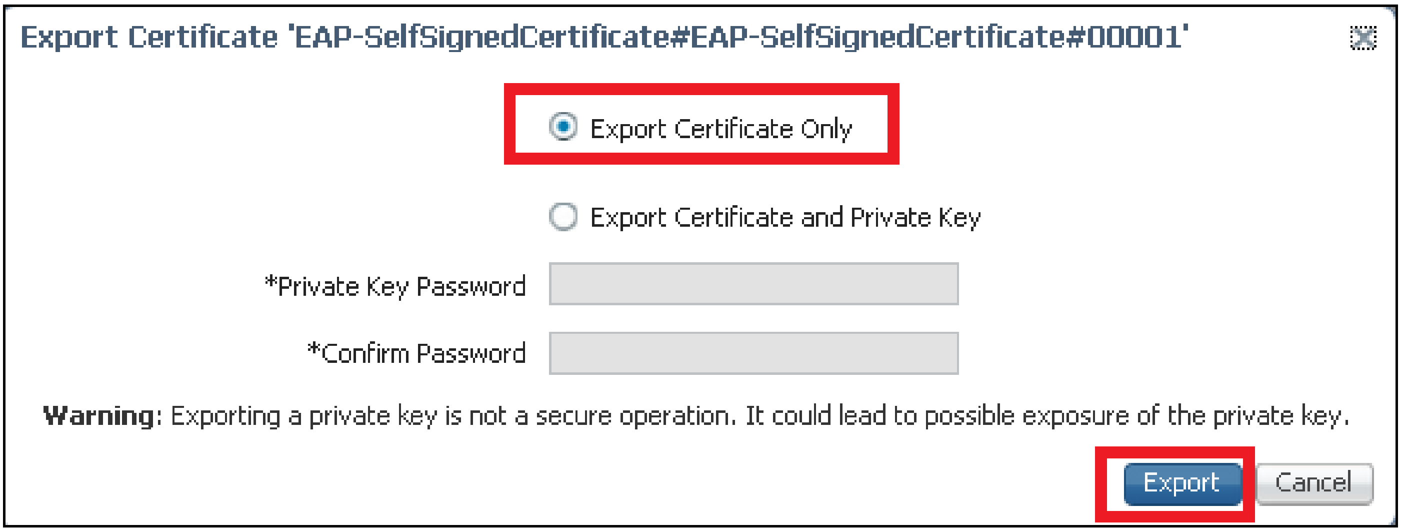
Choisissez ensuite le certificat utilisé pour l'authentification EAP et cliquez sur Export comme indiqué dans l'image.



System Certificates ⚠ For disaster recovery it is recommended to export certificate ar

	Friendly Name	Used By	Portal group tag
▼ [redacted]			
☑	EAP-SelfSignedCertificate#EAP-SelfSignedCertificate#00001	EAP Authentication	EAI

Enregistrez le certificat à l'emplacement requis. Ce certificat doit être installé sur l'ordinateur Windows comme illustré dans l'image.


Export Certificate 'EAP-SelfSignedCertificate#EAP-SelfSignedCertificate#00001'

● Export Certificate Only

○ Export Certificate and Private Key

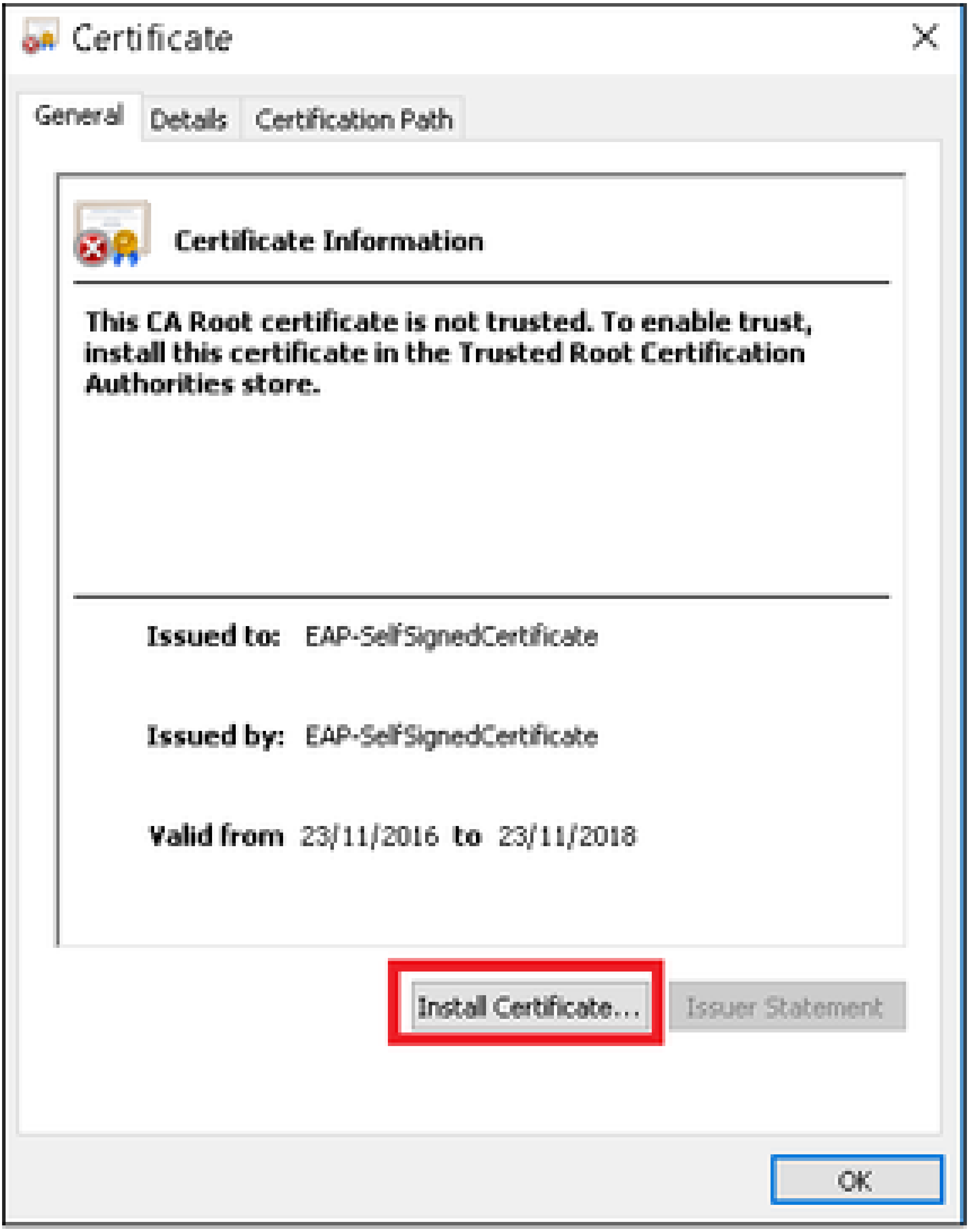
*Private Key Password

*Confirm Password

Warning: Exporting a private key is not a secure operation. It could lead to possible exposure of the private key.

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

Copiez le certificat exporté d'ISE dans la machine Windows, changez l'extension du fichier de .pem à .crt, et après cela double-cliquez afin de l'installer comme indiqué dans l'image.



Certificate Information

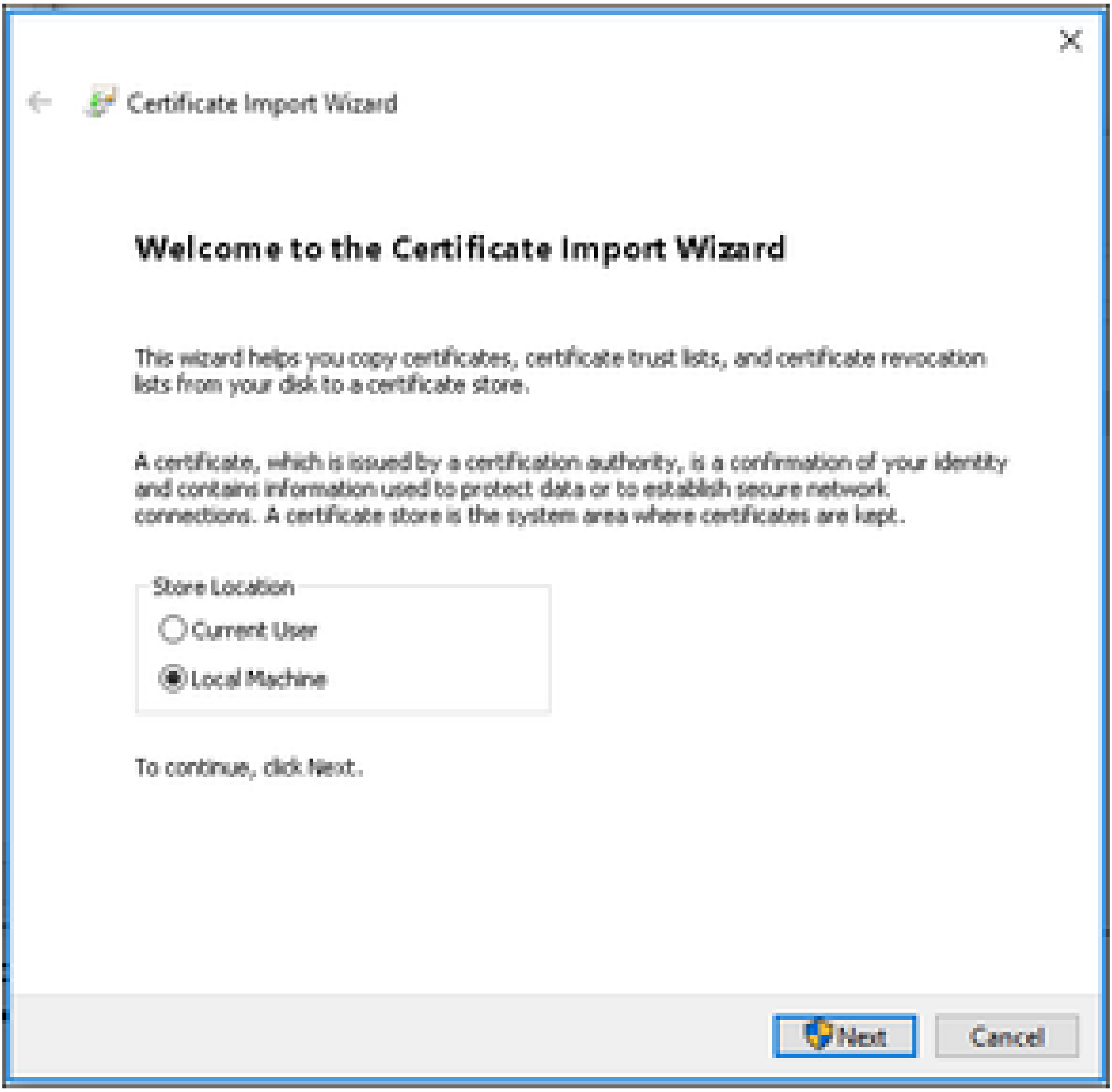
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: EAP-SelfSignedCertificate

Issued by: EAP-SelfSignedCertificate

Valid from 23/11/2016 to 23/11/2018

Étape 3. Sélectionnez l'installer dans Local Machine et cliquez sur Next comme indiqué dans l'image.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

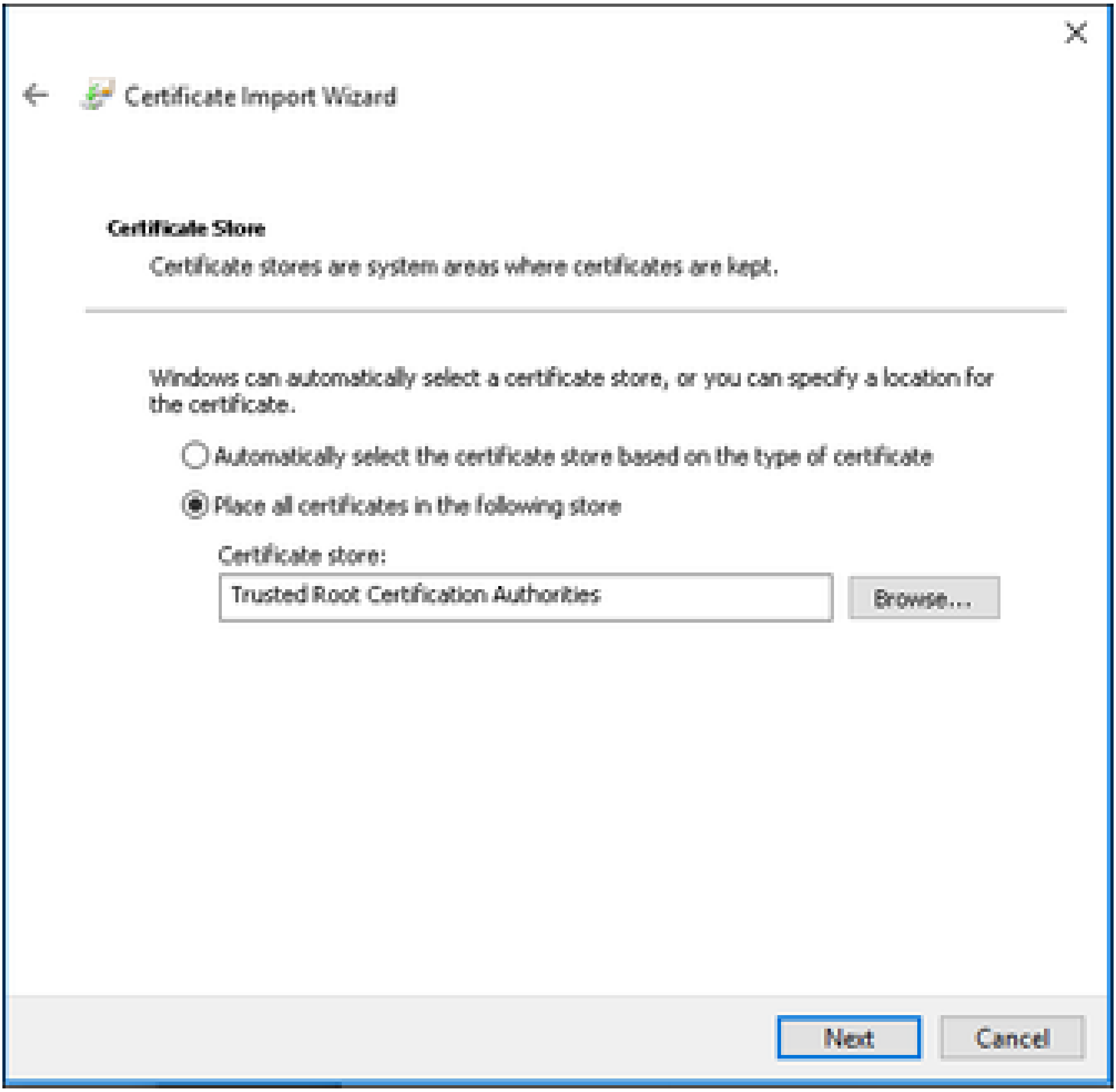
Store Location

○ Current User

● Local Machine

To continue, click Next.

Étape 4. Sélectionnez Placer tous les certificats dans ce magasin, puis recherchez et sélectionnez Autorités de certification racine de confiance. Après cela, cliquez sur Next comme indiqué dans l'image.



Certificate Store

Certificate stores are system areas where certificates are kept.

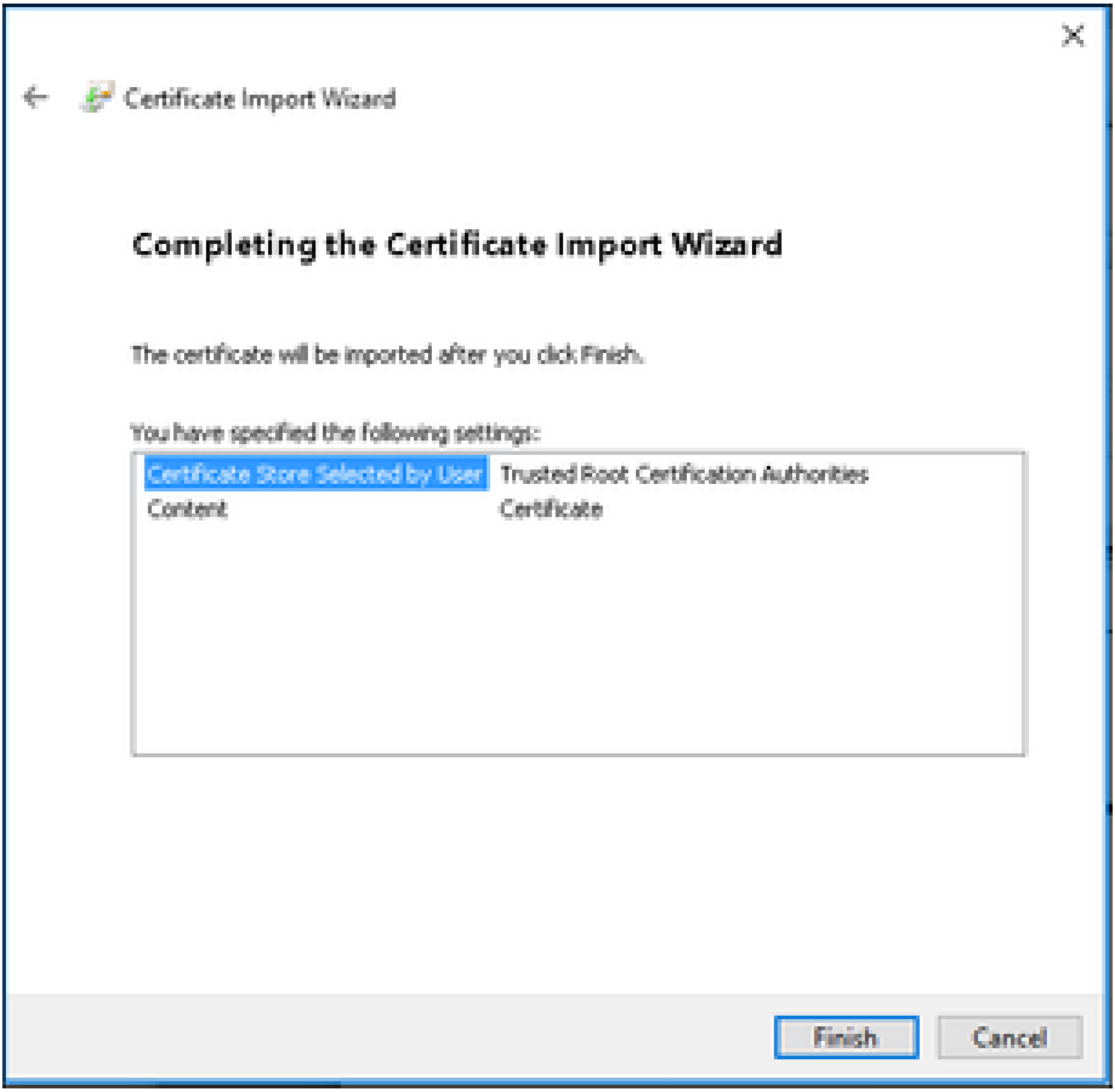
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

Étape 5. Cliquez ensuite sur Finish comme indiqué dans l'image.



Certificate Import Wizard

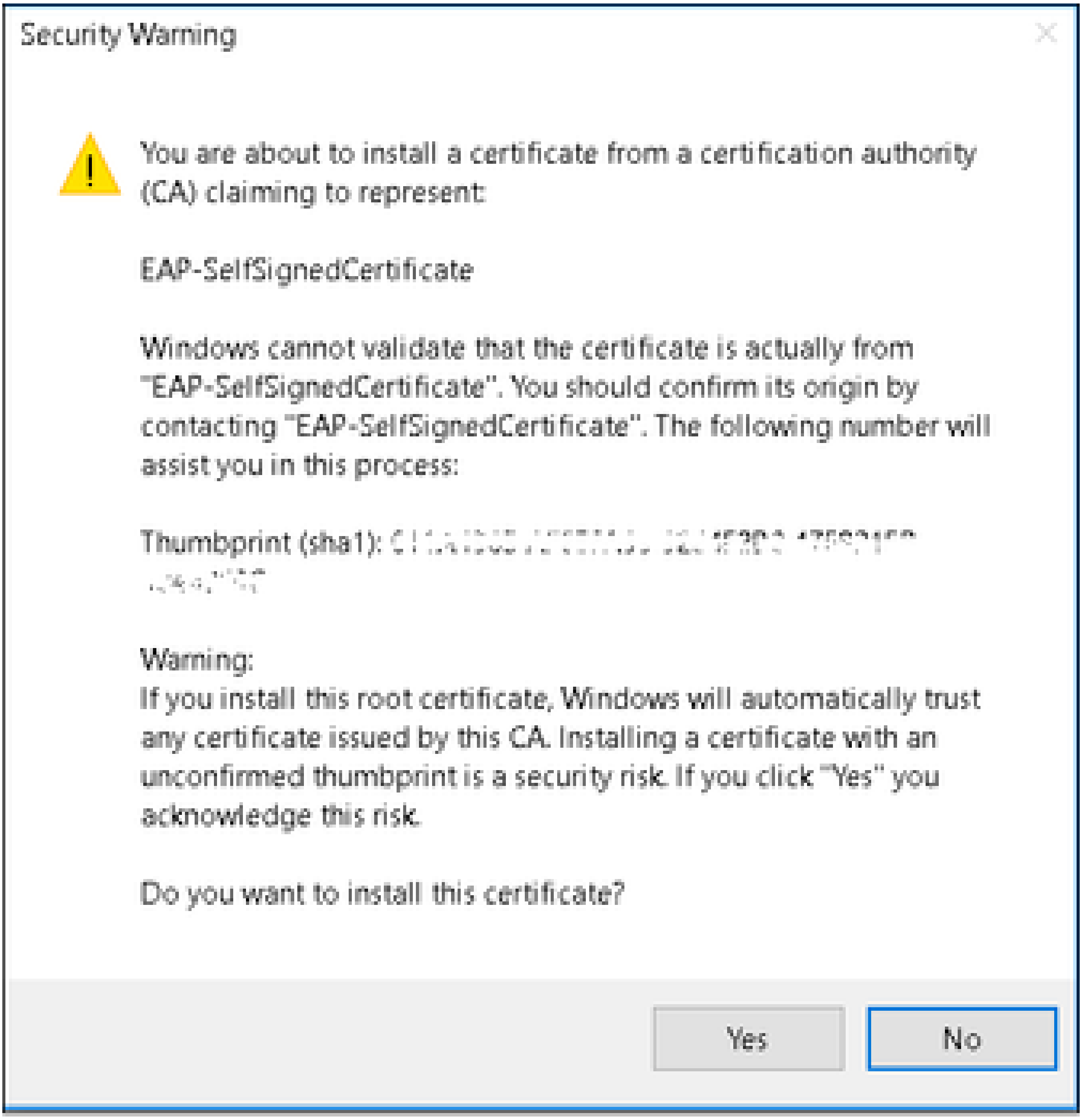
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

Étape 6. Confirmez l'installation du certificat. Cliquez sur Yes comme indiqué dans l'image.



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

EAP-SelfSignedCertificate

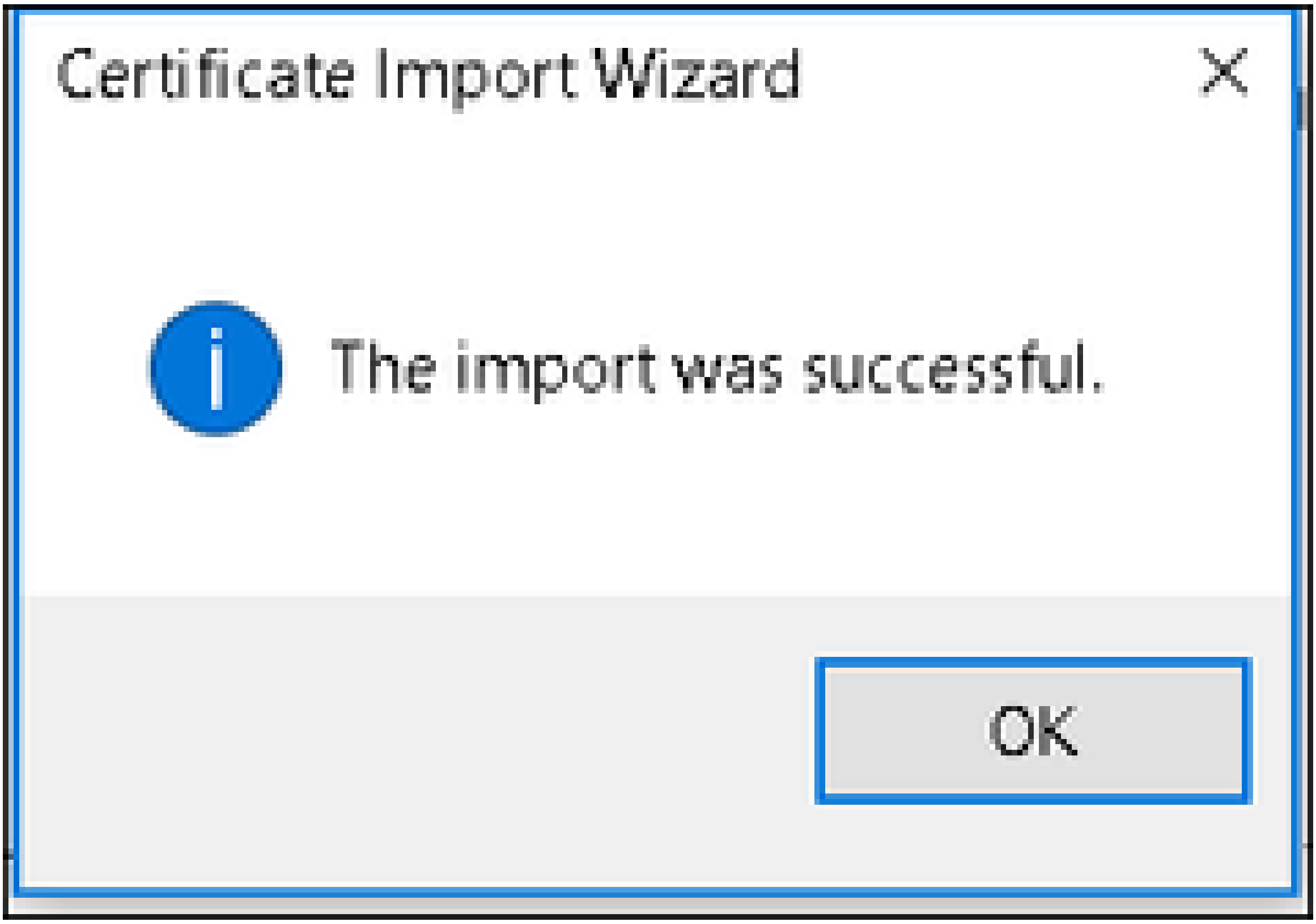
Windows cannot validate that the certificate is actually from "EAP-SelfSignedCertificate". You should confirm its origin by contacting "EAP-SelfSignedCertificate". The following number will assist you in this process:

Thumbprint (sha1): [redacted]

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Étape 7. Enfin, cliquez sur OK comme illustré dans l'image.

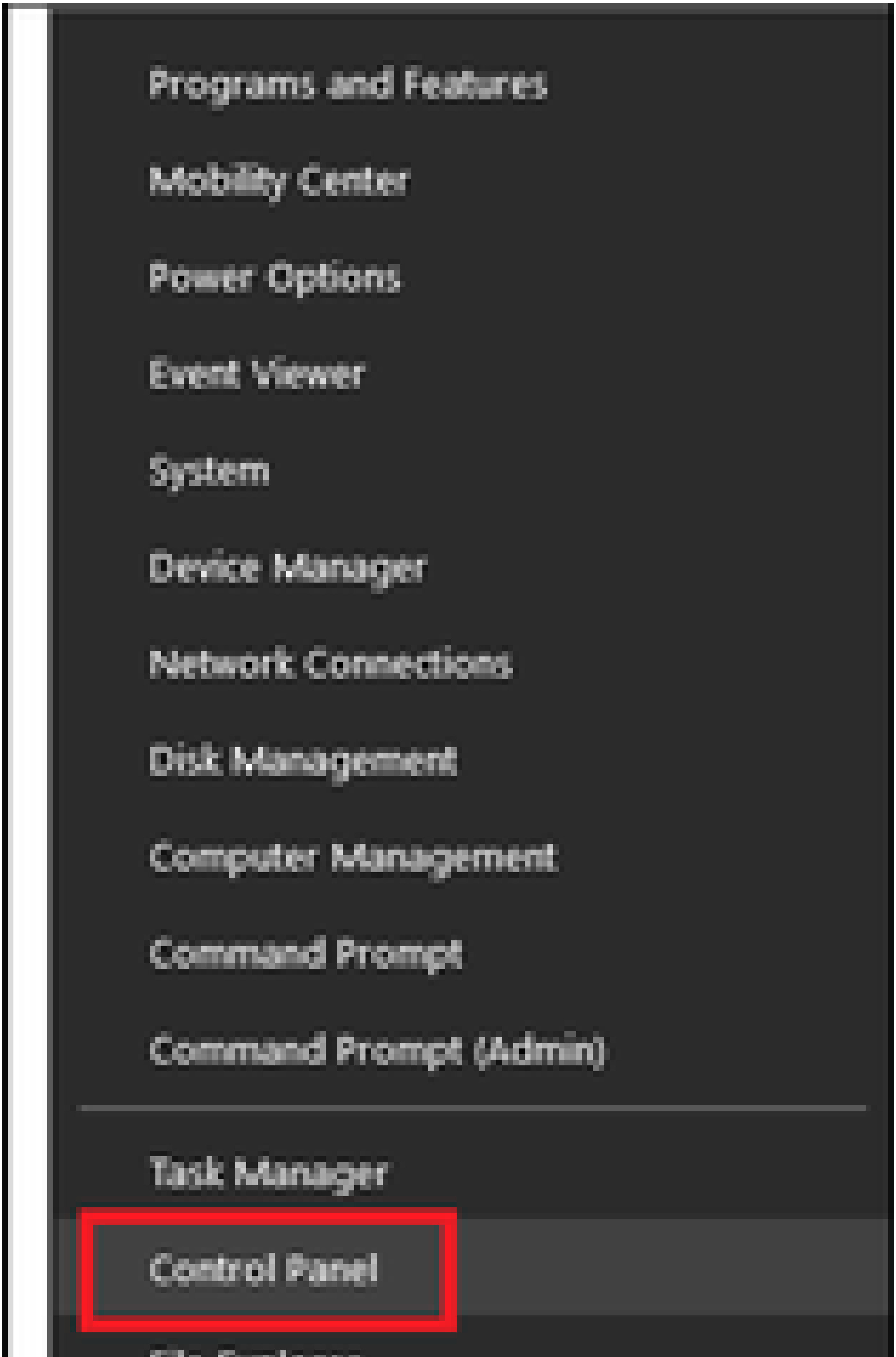


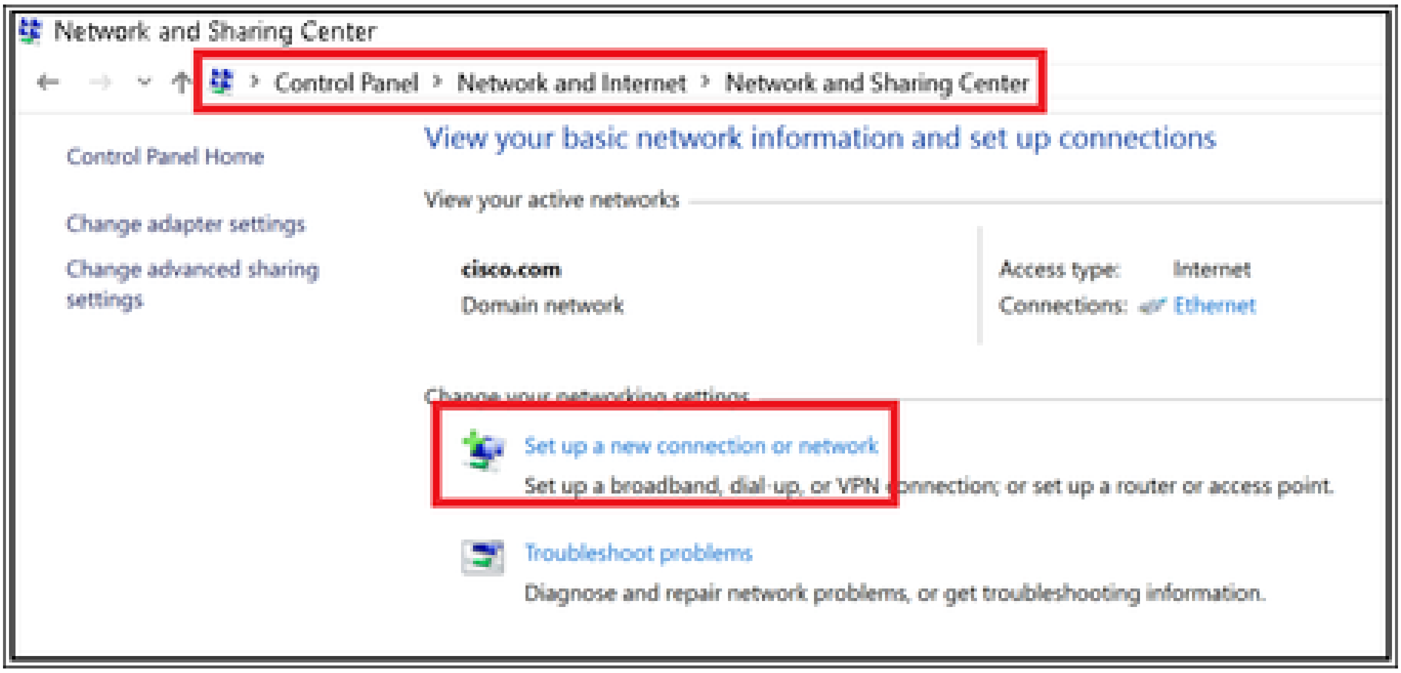
Certificate Import Wizard

The import was successful.

Configuration du périphérique final - Création du profil WLAN

Étape 1. Cliquez avec le bouton droit sur l'icône Démarrer et sélectionnez Panneau de configuration comme illustré dans l'image.


Programs and Features
Mobility Center
Power Options
Event Viewer
System
Device Manager
Network Connections
Disk Management
Computer Management
Command Prompt
Command Prompt (Admin)
Task Manager
Control Panel


Network and Sharing Center
Control Panel › Network and Internet › Network and Sharing Center
Control Panel Home
Change adapter settings
Change advanced sharing settings

View your basic network information and set up connections

View your active networks

cisco.com
Domain network

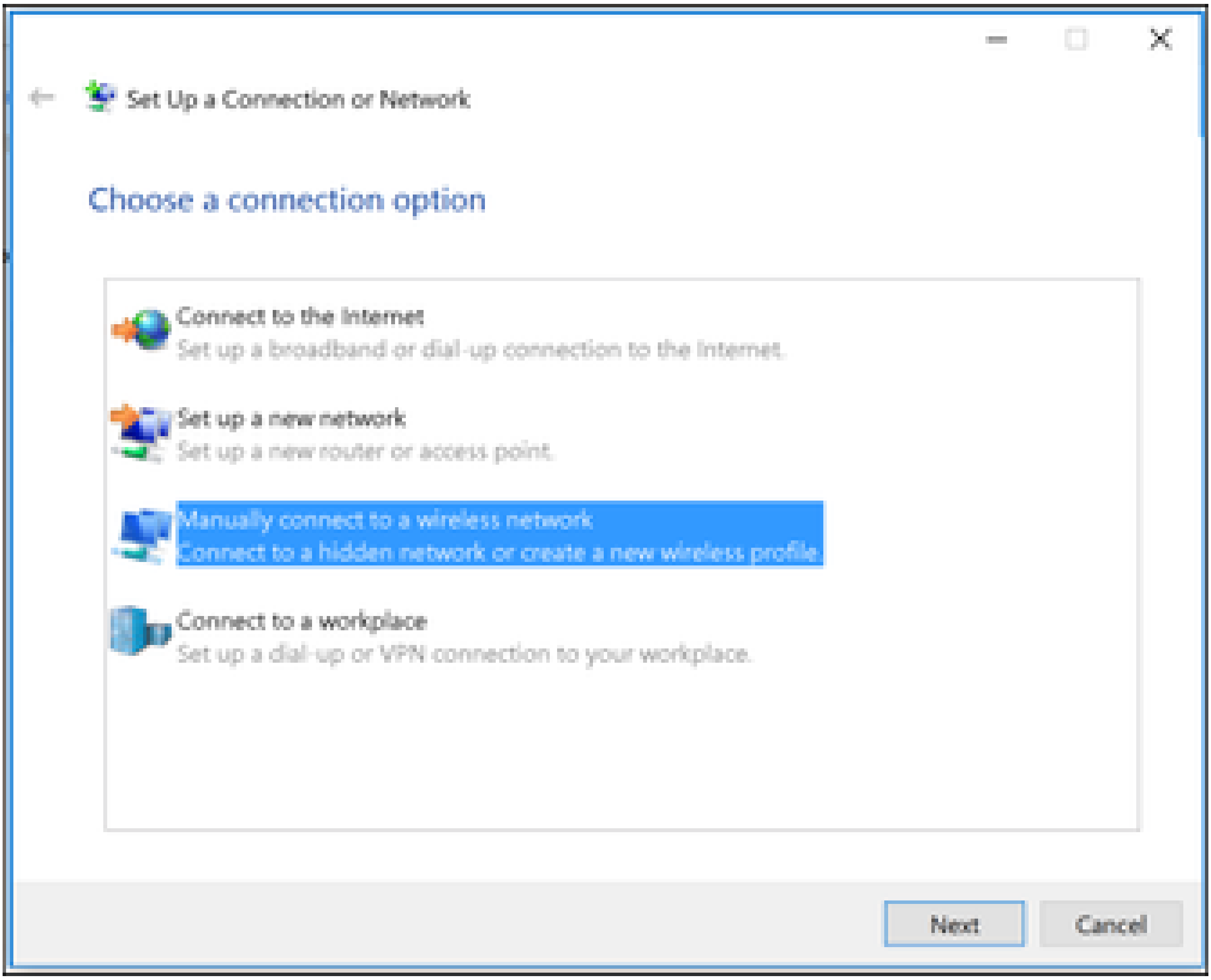
Access type: Internet
Connections: Ethernet

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

Étape 3. Sélectionnez Manually connect to a wireless network, puis cliquez sur Next, comme indiqué dans l'image.



Set Up a Connection or Network

Choose a connection option

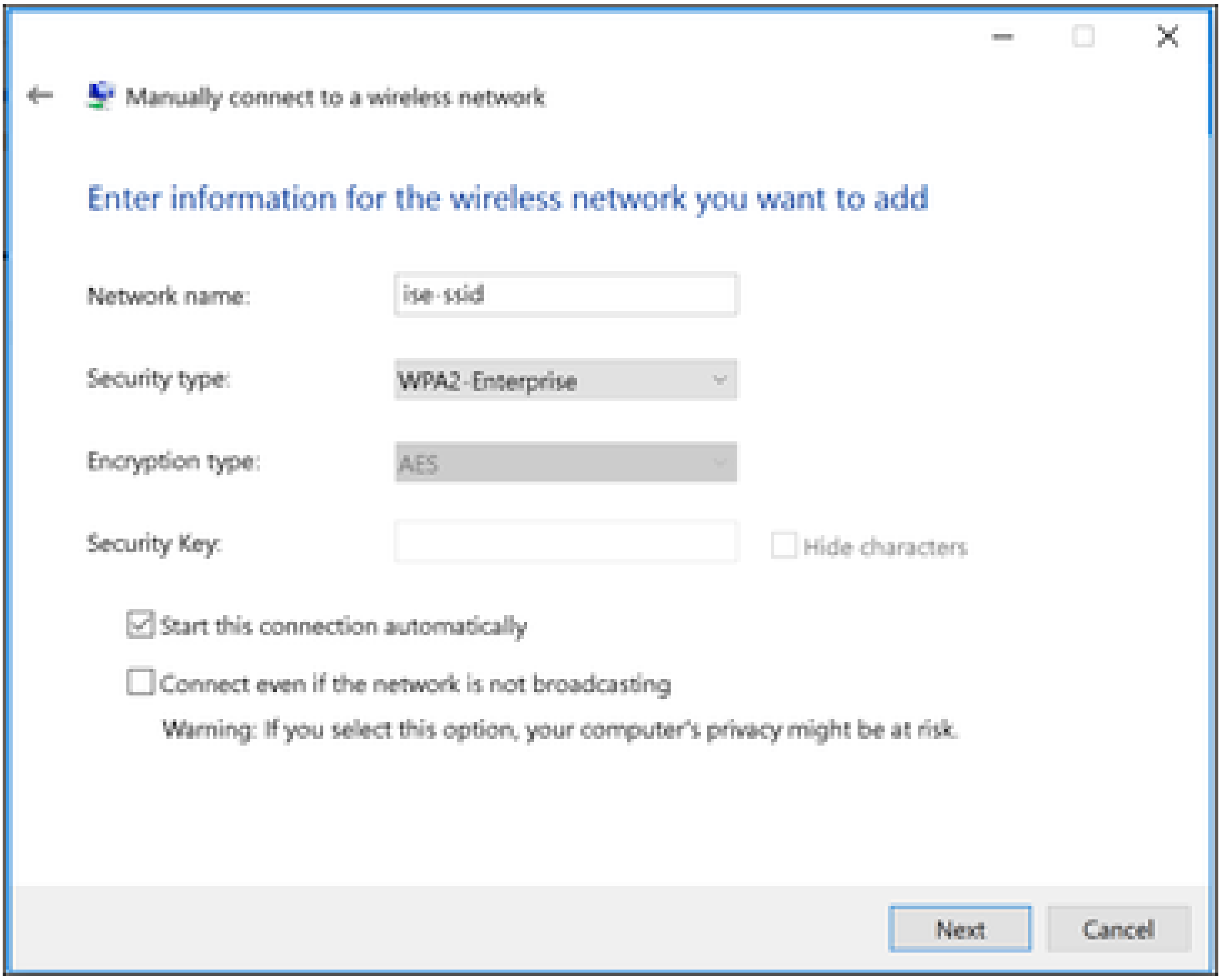
Connect to the Internet
Set up a broadband or dial-up connection to the Internet.

Set up a new network
Set up a new router or access point.

Manually connect to a wireless network
Connect to a hidden network or create a new wireless profile

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

Étape 4. Entrez les informations avec le nom du SSID et le type de sécurité WPA2-Enterprise et cliquez sur Next comme indiqué dans l'image.



Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name: ise-ssid

Security type: WPA2-Enterprise

Encryption type: AES

Security Key:

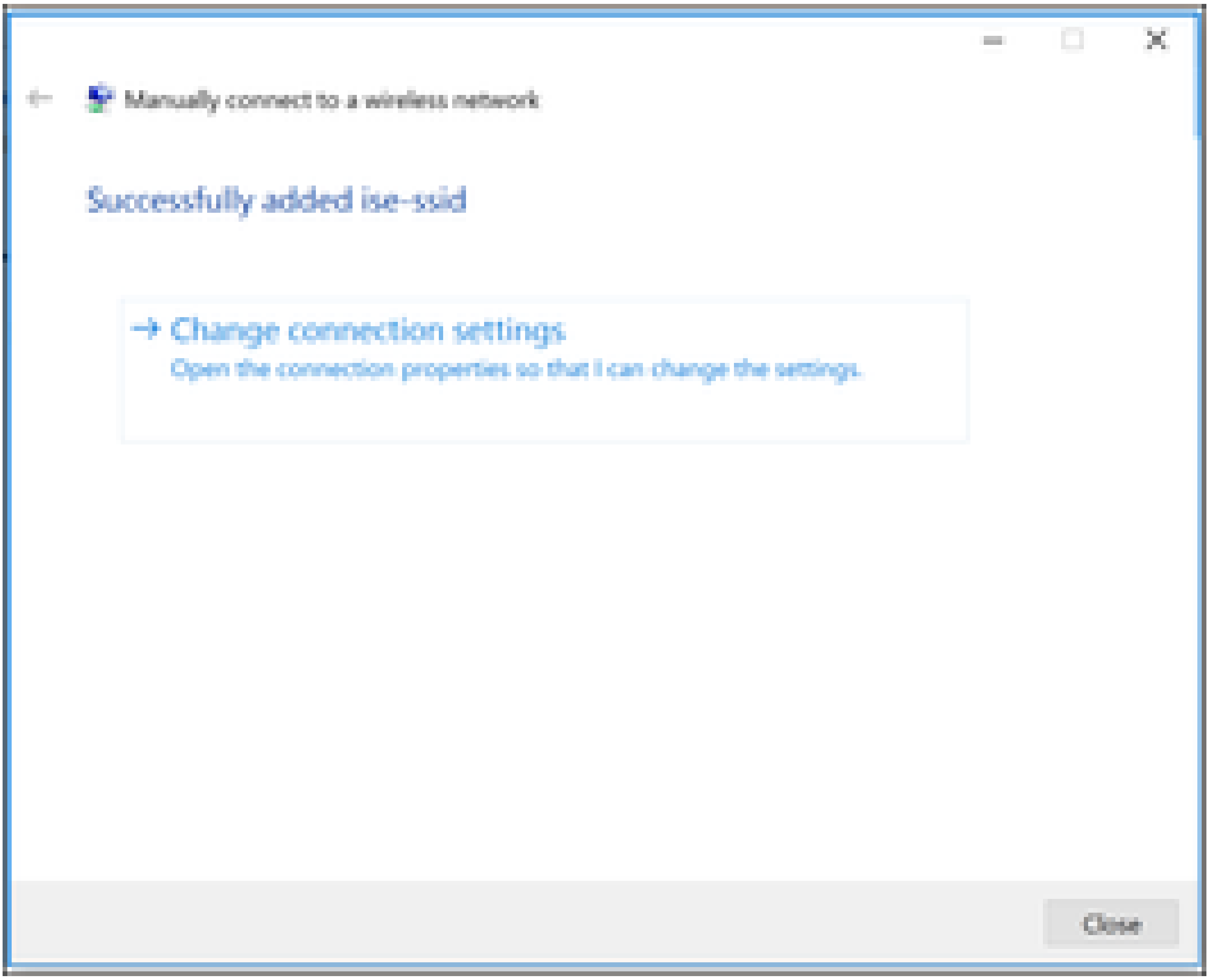
□ Hide characters

☑ Start this connection automatically

□ Connect even if the network is not broadcasting

Warning: If you select this option, your computer's privacy might be at risk.

Étape 5. Sélectionnez Change connection settings afin de personnaliser la configuration du profil WLAN comme indiqué dans l'image.

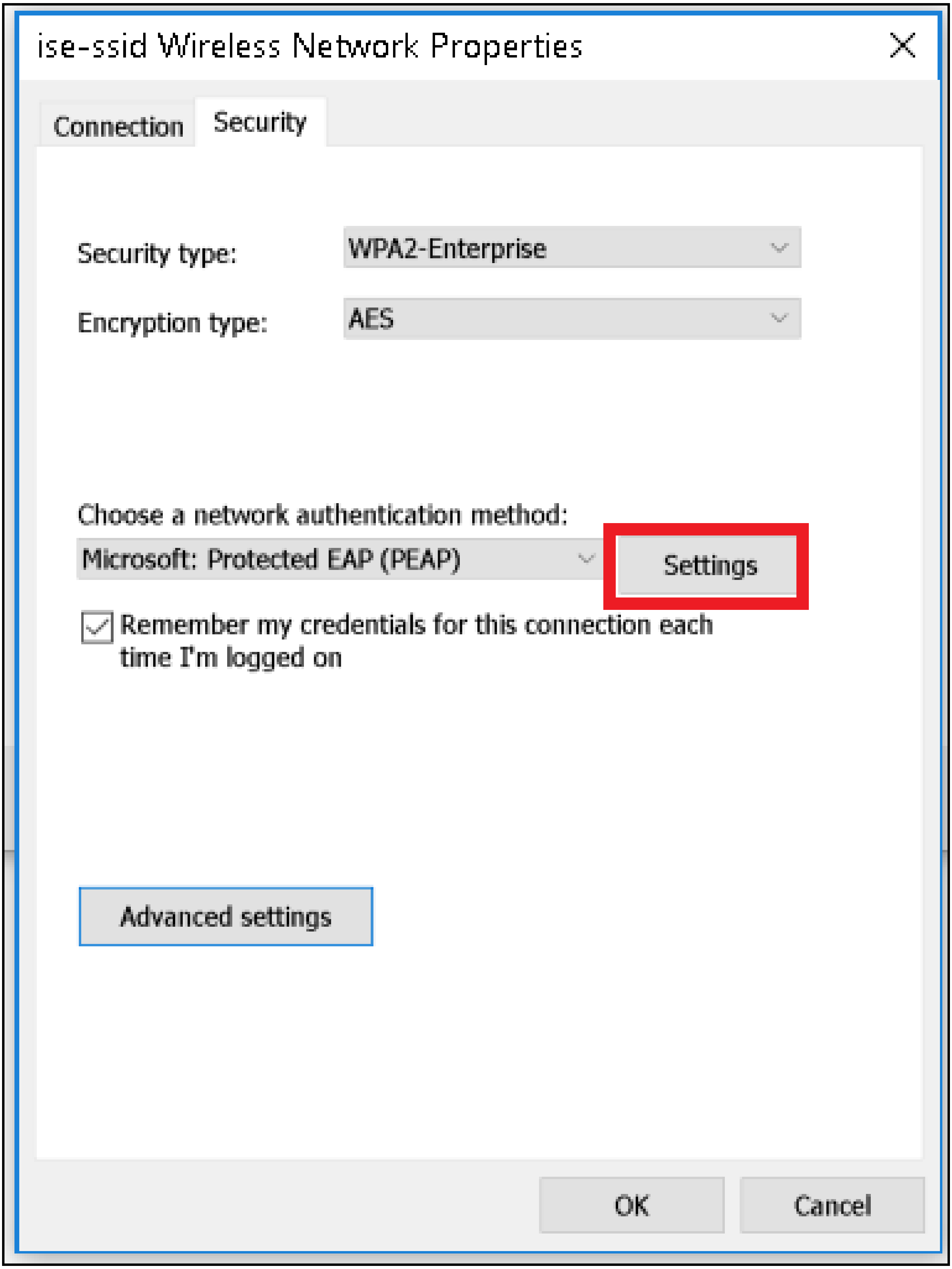


Manually connect to a wireless network

Successfully added ise-ssid

→ Change connection settings
Open the connection properties so that I can change the settings.

Étape 6. Accédez à l'onglet Security et cliquez sur Settings comme indiqué dans l'image.



ise-ssid Wireless Network Properties

Connection | Security

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:

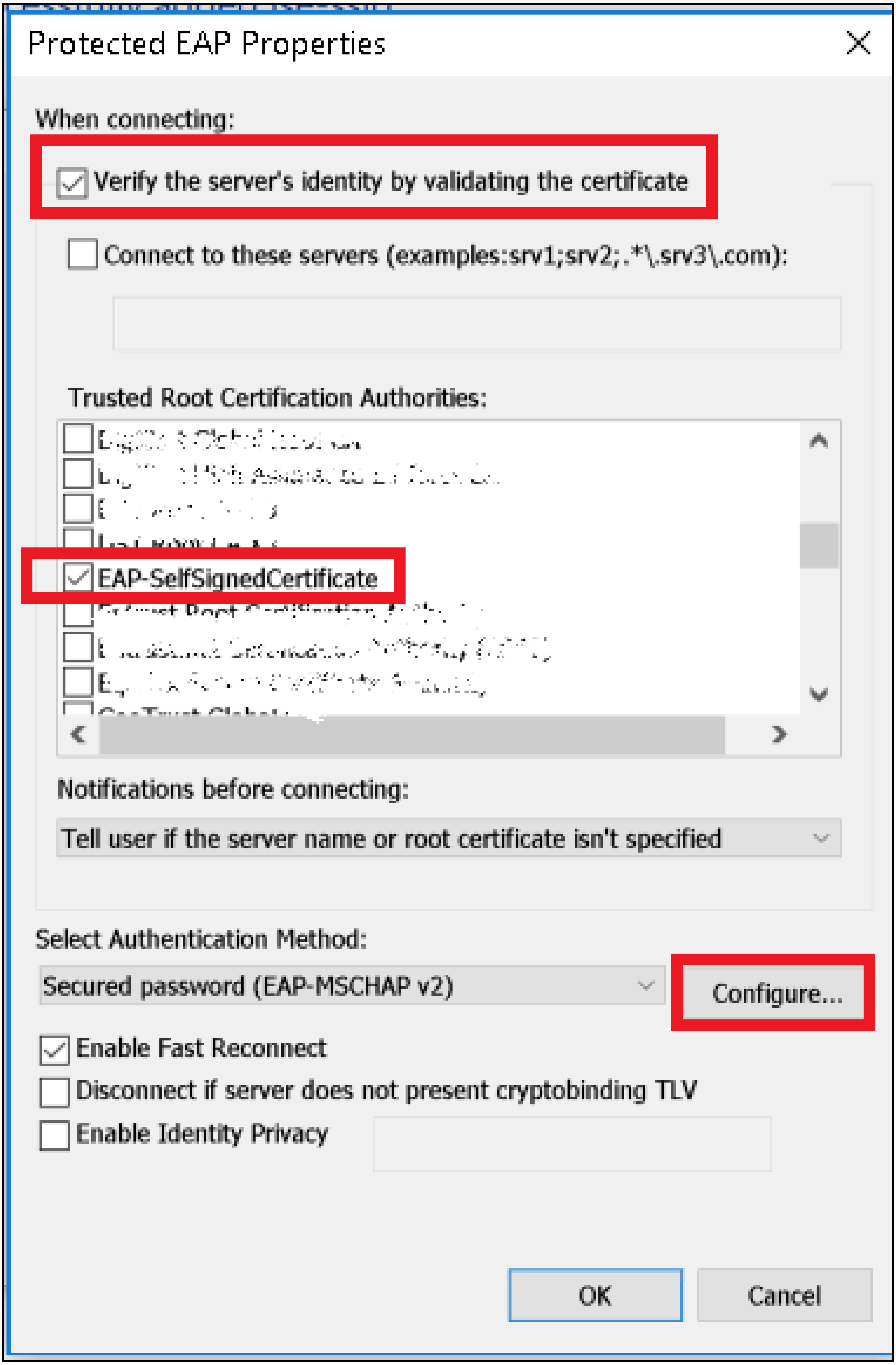
Microsoft: Protected EAP (PEAP)

☑ Remember my credentials for this connection each time I'm logged on

Étape 7. Sélectionnez cette option si le serveur RADIUS est validé ou non.

Si oui, activez Vérifier l'identité du serveur en validant le certificat et, dans Autorités de certification racine de confiance : liste, sélectionnez le certificat auto-signé d'ISE.

Après cela, sélectionnez Configure et disable Automatically use my Windows logon name and password..., puis cliquez sur OK comme indiqué dans les images.



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:

□ [redacted]
□ [redacted]
□ [redacted]
□ [redacted]
☑ EAP-SelfSignedCertificate
□ [redacted]
□ [redacted]
□ [redacted]
□ [redacted]

Notifications before connecting:

Tell user if the server name or root certificate isn't specified

Select Authentication Method:

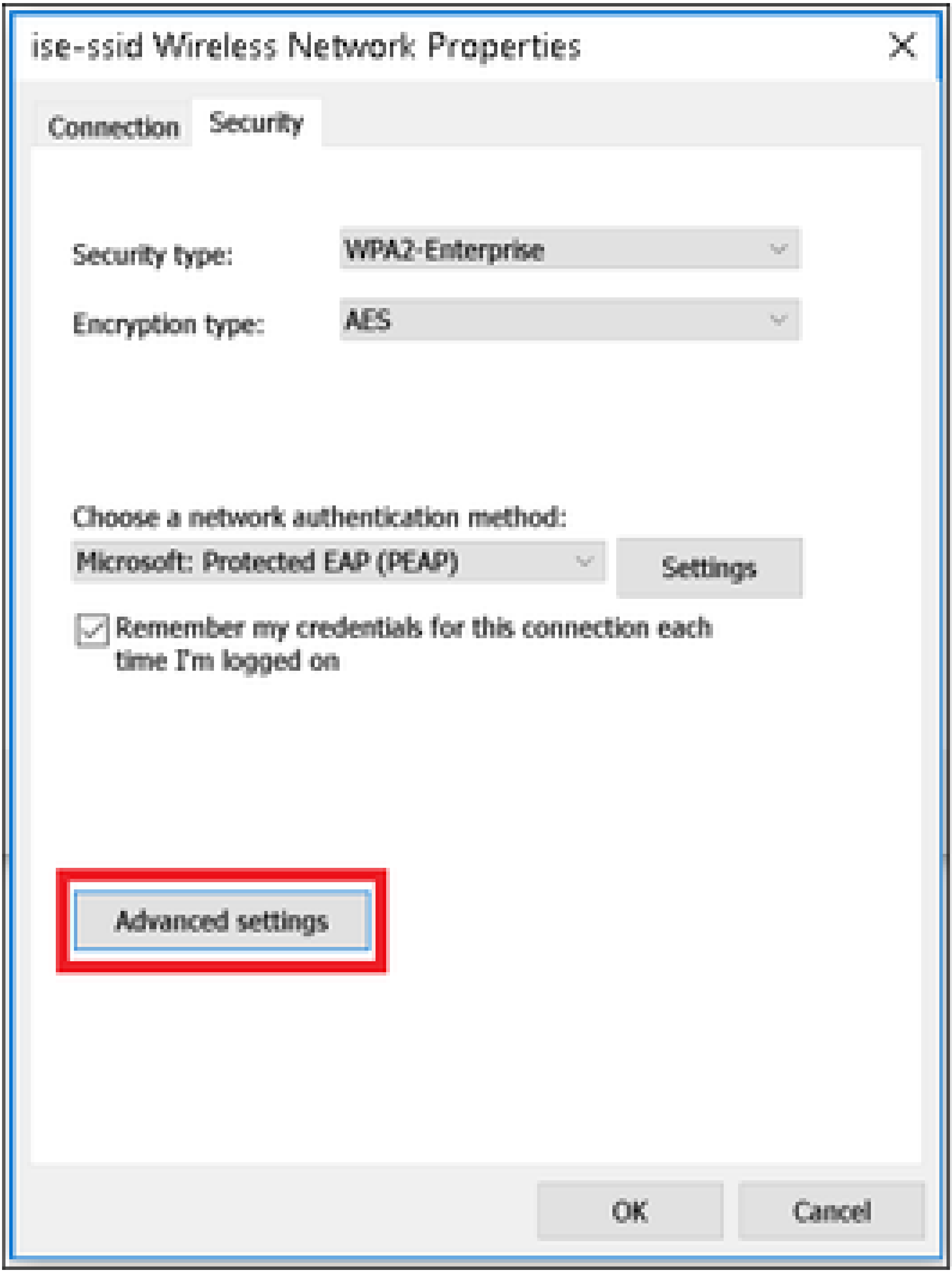
Secured password (EAP-MSCHAP v2)

☑ Enable Fast Reconnect

□ Disconnect if server does not present cryptobinding TLV

□ Enable Identity Privacy

Une fois de retour à l'onglet Security, sélectionnez Advanced settings, spécifiez authentication mode comme User authentication, et enregistrez les informations d'identification qui ont été configurées sur ISE afin d'authentifier l'utilisateur comme indiqué dans les images.

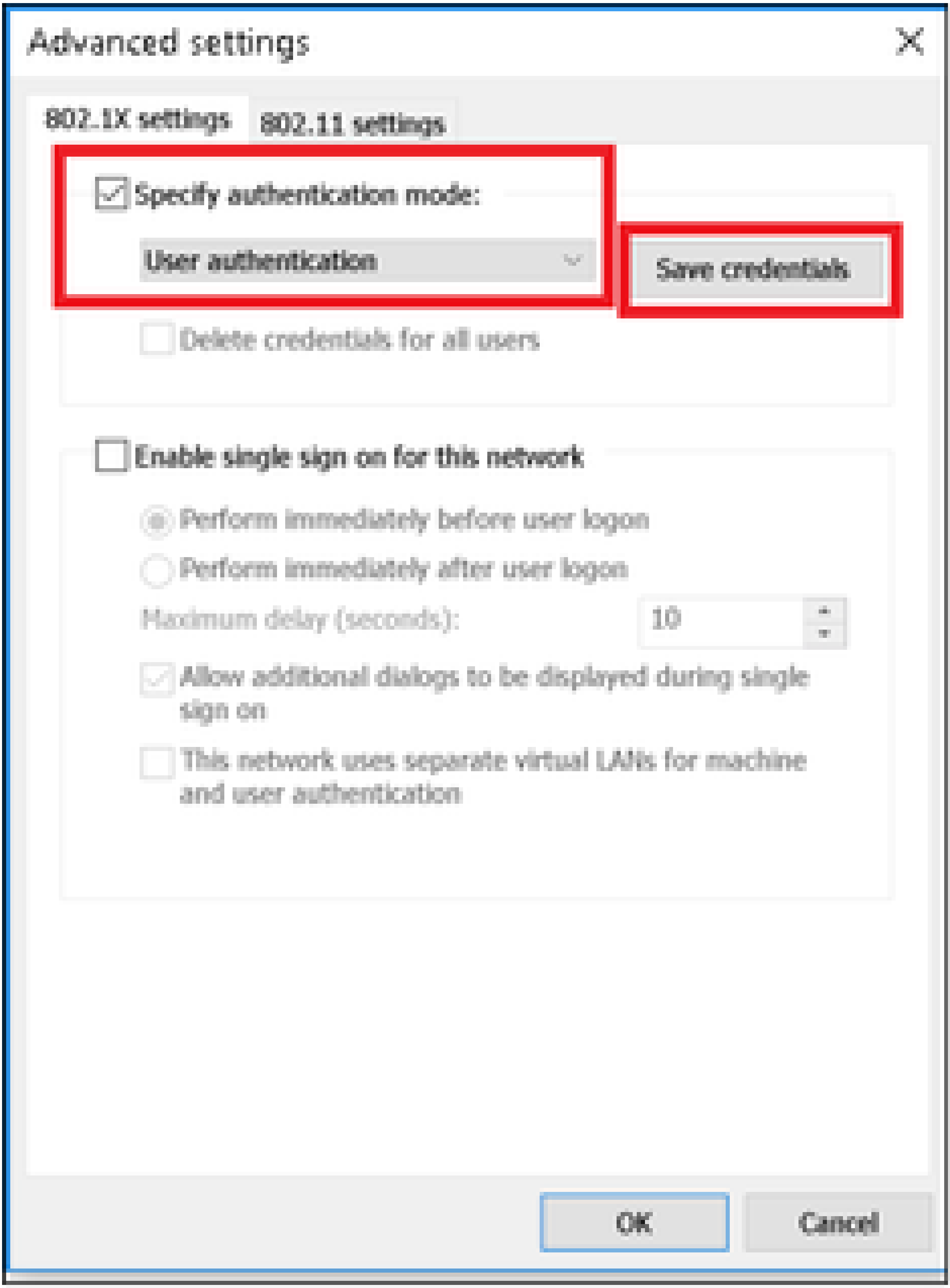


Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method: Microsoft: Protected EAP (PEAP)

☑ Remember my credentials for this connection each time I'm logged on



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

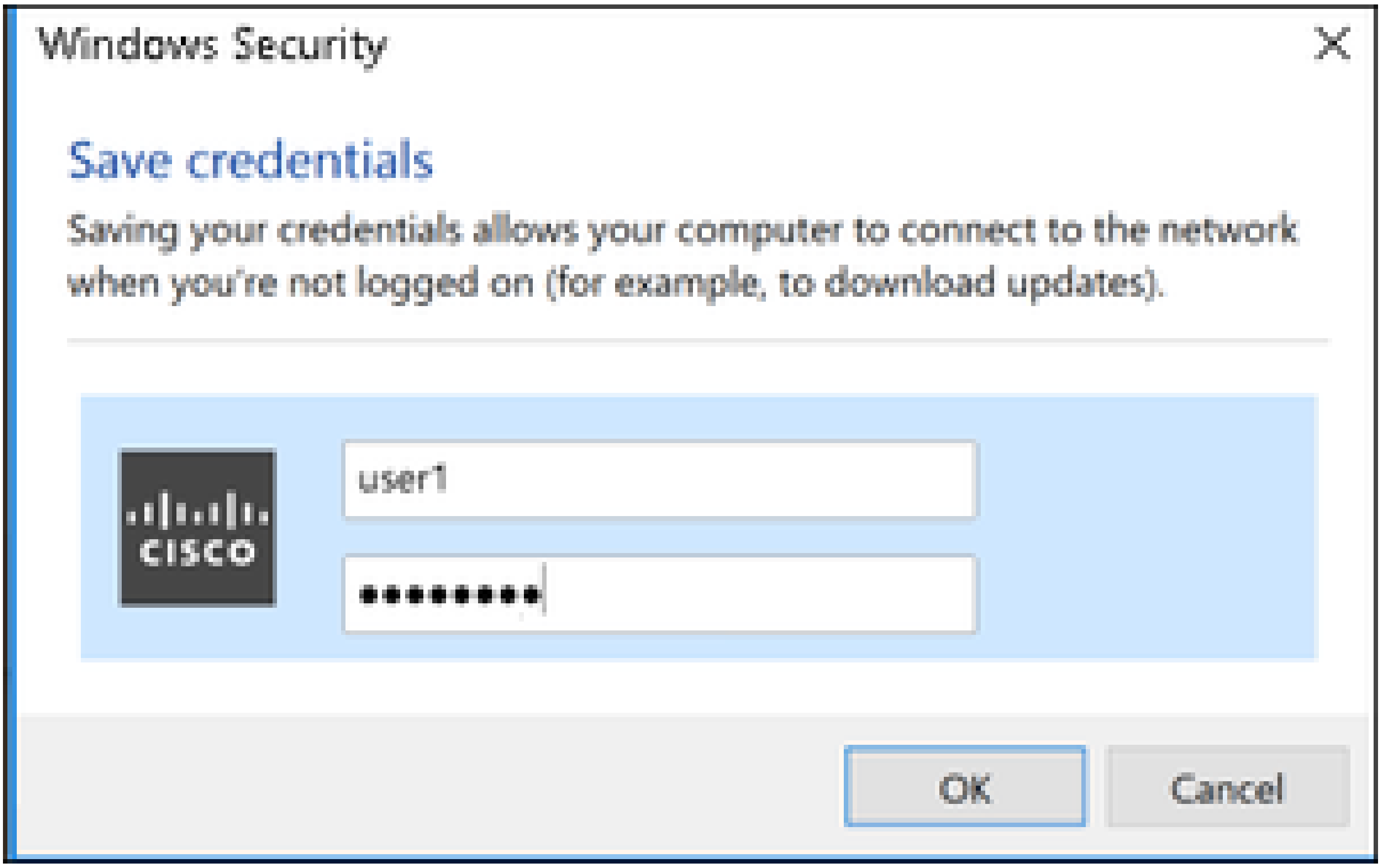
○ Perform immediately after user logon

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



Windows Security

Save credentials

Saving your credentials allows your computer to connect to the network when you're not logged on (for example, to download updates).

user1

••••••••

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

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

Processus d'authentification sur WLC

Exécutez les commandes suivantes afin de surveiller le processus d'authentification pour un utilisateur spécifique :

```
> debug client <mac-add-client>
> debug dot1x event enable
> debug dot1x aaa enable
```

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

<#root>

```
*apfMsConnTask_1: Nov 24 04:30:44.317:
```

`e4:b3:18:7c:30:58 Processing assoc-req station:e4:b3:18:7c:30:58 AP:00:c8:8b:26:2c:d0-00`

```
 thread:1a5cc288
```

```
*apfMsConnTask_1: Nov 24 04:30:44.317: e4:b3:18:7c:30:58 Reassociation received from mobile on BSSID 00
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying Interface(management) policy on Mobil
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying site-specific Local Bridging override
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying Local Bridging Interface Policy for st
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 RSN Capabilities:  60
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Marking Mobile as non-
```

e4:b3:18:7c:30:58 Received 802.11i 802.1X key management suite, enabling dot1x Authentication

```
11w Capable
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Received RSN IE with 1 PMKIDs from mobile e4:b
*apfMsConnTask_1: Nov 24 04:30:44.319: Received PMKID:  (16)
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Searching for PMKID in MSCB PMKID cache for mob
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 No valid PMKID found in the MSCB PMKID cache fo
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 0.0.0.0 START (0) Initializing policy
*apfMsConnTask_1: Nov 24 04:30:44.319:
```

e4:b3:18:7c:30:58 0.0.0.0 START (0) Change state to AUTHCHECK (2) last state START (0)

```
*apfMsConnTask_1: Nov 24 04:30:44.319:
```

e4:b3:18:7c:30:58 0.0.0.0 AUTHCHECK (2) Change state to 8021X_REQD (3) last state AUTHCHECK (2)

```
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 0.0.0.0 8021X_REQD (3) Plumbed mobile LWAPP ru
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfMsAssoStateInc
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfPemAddUser2 (apf_policy.c:437) Changing sta
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfPemAddUser2:session timeout forstation e4:b
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Stopping deletion of Mobile Station: (callerId
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Func: apfPemAddUser2, Ms Timeout = 0, Session 
*apfMsConnTask_1: Nov 24 04:30:44.320: e4:b3:18:7c:30:58 Sending Assoc Response to station on BSSID 00:
*spamApTask2: Nov 24 04:30:44.323: e4:b3:18:7c:30:58 Successful transmission of LWAPP Add-Mobile to AP 
*spamApTask2: Nov 24 04:30:44.325: e4:b3:18:7c:30:58 Received ADD_MOBILE ack - Initiating 1x to STA e4:
*spamApTask2: Nov 24 04:30:44.325: e4:b3:18:7c:30:58
```

Sent dot1x auth initiate message for mobile e4:b3:18:7c:30:58

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 reauth_sm state transition 0 ---> 1 for mob
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 EAP-PARAM Debug - eap-params for Wlan-Id :2
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Disable re-auth, use PMK lifetime.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Station e4:b3:18:7c:30:58 setting dot1x reau
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Stopping reauth timeout for e4:b3:18:7c:30:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 int
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326:
```

e4:b3:18:7c:30:58 Sending EAP-Request/Identity to mobile e4:b3:18:7c:30:58 (EAP Id 1)

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Received EAPOL EAPPKT from mobile e4:b3:18:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Received Identity Response (count=1) from m
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Resetting reauth count 1 to 0 for mobile e4
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 EAP State update from Connecting to Authent
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 int
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Entering Backend Auth Response state for mob
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Created Acct-Session-ID (58366cf4/e4:b3:18:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.386: e4:b3:18:7c:30:58 Processing Access-Challenge for mobile e4:b
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Entering Backend Auth Req state (id=215) fo
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 WARNING: updated EAP-Identifier 1 ===> 215 
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Sending EAP Request from AAA to mobile e4:b
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Allocating EAP Pkt for retransmission to mob
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Received EAPOL EAPPKT from mobile e4:b3:18:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Received EAP Response from mobile e4:b3:18:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Resetting reauth count 0 to 0 for mobile e4
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Entering Backend Auth Response state for mob
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Processing Access-Challenge for mobile e4:b
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Entering Backend Auth Req state (id=216) fo
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Sending EAP Request from AAA to mobile e4:b
```

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Reusing allocated memory for  EAP Pkt for r
.
.
.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530:

e4:b3:18:7c:30:58 Processing Access-Accept for mobile e4:b3:18:7c:30:58

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Resetting web IPv4 acl from 255 to 255
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Resetting web IPv4 Flex acl from 65535 to 6
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530:

e4:b3:18:7c:30:58 Username entry (user1) created for mobile, length = 253

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530:

e4:b3:18:7c:30:58 Found an interface name:'vlan2404' corresponds to interface name received: vlan2404

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 override for default ap group, marking intg
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Applying Interface(management) policy on Mo
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Re-applying interface policy for client
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 apfApplyWlanPolicy: Apply WLAN Policy over
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531:

e4:b3:18:7c:30:58 Inserting AAA Override struct for mobile

        MAC: e4:b3:18:7c:30:58, source 4
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Applying override policy from source Overri
*Dot1x_NW_MsgTask_0: Nov 24

04:30:44.531: e4:b3:18:7c:30:58 Found an interface name:'vlan2404' corresponds to interface name receive

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Applying Interface(vlan2404) policy on Mobi
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Re-applying interface policy for client
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Setting re-auth timeout to 0 seconds, got f
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Station e4:b3:18:7c:30:58 setting dot1x rea
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Stopping reauth timeout for e4:b3:18:7c:30:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Creating a PKC PMKID Cache entry for statio
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Resetting MSCB PMK Cache Entry 0 for statio
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Adding BSSID 00:c8:8b:26:2c:d1 to PMKID cac
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: New PMKID: (16)
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531:      [0000] cc 3a 3d 26 80 17 8b f1 2d c5 cd fd a0 8a c4 39
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 unsetting PmkIdValidatedByAp
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Updating AAA Overrides from local for stati
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Adding Audit session ID payload in Mobility
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 0 PMK-update groupcast messages sent
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 PMK sent to mobility group
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Disabling re-auth since PMK lifetime can ta
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Sending EAP-Success to mobile e4:b3:18:7c:3
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Freeing AAACB from Dot1xCB as AAA auth is d
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Found an cache entry for BSSID 00:c8:8b:26:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: Including PMKID in M1  (16)
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:      [0000] cc 3a 3d 26 80 17 8b f1 2d c5 cd fd a0 8a c4 39
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: M1 - Key Data: (22)
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:      [0000] dd 14 00 0f ac 04 cc 3a 3d 26 80 17 8b f1 2d c5
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:      [0016] cd fd a0 8a c4 39
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:

e4:b3:18:7c:30:58 Starting key exchange to mobile e4:b3:18:7c:30:58, data packets will be dropped

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:

e4:b3:18:7c:30:58 Sending EAPOL-Key Message to mobile e4:b3:18:7c:30:58

state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00
```

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Reusing allocated memory for  EAP Pkt for r
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Entering Backend Auth Success state (id=223
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Received Auth Success while in Authenticati
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 int
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 Received EAPOL-Key from mobile e4:b3:18:7c:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 Ignoring invalid EAPOL version (1) in EAPOL
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547:

e4:b3:18:7c:30:58 Received EAPOL-key in PTK_START state (message 2) from mobile

 e4:b3:18:7c:30:58
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Successfully computed PTK from PMK!!!
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Received valid MIC in EAPOL Key Message M2!
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Not Flex client. Do not distribute PMK Key 
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Stopping retransmission timer for mobile e4
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Sending EAPOL-Key Message to mobile e4:b3:1
state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Reusing allocated memory for  EAP Pkt for r
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Received EAPOL-Key from mobile e4:b3:18:7c:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Ignoring invalid EAPOL version (1) in EAPOL
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555:

e4:b3:18:7c:30:58 Received EAPOL-key in PTKINITNEGOTIATING state (message 4)

 from mobile e4:b3:18:7c:30:58
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Stopping retransmission timer for mobile e4
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Freeing EAP Retransmit Bufer for mobile e4:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMs1xStateInc
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMsPeapSimReqCntInc
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMsPeapSimReqSuccessCntInc
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555:

e4:b3:18:7c:30:58 0.0.0.0 8021X_REQD (3) Change state to L2AUTHCOMPLETE (4) last state 8021X_REQD (3)

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Mobility query, PEM State: L2AUTHCOMPLETE
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Building Mobile Announce :
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58   Building Client Payload:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     Client Ip: 0.0.0.0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     Client Vlan Ip: 172.16.0.134, Vlan mask
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     Client Vap Security: 16384
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     Virtual Ip: 10.10.10.10
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     ssid: ise-ssid
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58   Building VlanIpPayload.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Not Using WMM Compliance code qosCap 00
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile L
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556:

e4:b3:18:7c:30:58 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6677
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Adding Fast Path rule
  type = Airespace AP - Learn IP address
  on AP 00:c8:8b:26:2c:d0, slot 0, interface = 1, QOS = 0
  IPv4 ACL ID = 255, IPv
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Successfully plumbed 
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Successfully Plumbed PTK session Keysfor mo
*spamApTask2: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Successful transmission of LWAPP Add-Mobile to AP 
*pemReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) mobility role update requ
```

```
  Peer = 0.0.0.0, Old Anchor = 0.0.0.0, New Anchor = 172.16.0.3
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) State Update from Mobilit
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6315, Ad
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Replacing Fast Path rule
  IPv4 ACL ID = 255,
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...)
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...)
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobi
*pemReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 Sent an XID frame
*dtlArpTask: Nov 24 04:30:47.932: e4:b3:18:7c:30:58 Static IP client associated to interface vlan2404 w
*dtlArpTask: Nov 24 04:30:47.933: e4:b3:18:7c:30:58 apfMsRunStateInc
*dtlArpTask: Nov 24 04:30:47.933:

e4:b3:18:7c:30:58 172.16.0.151 DHCP_REQD (7) Change state to RUN (20)

 last state DHCP_REQD (7)
```

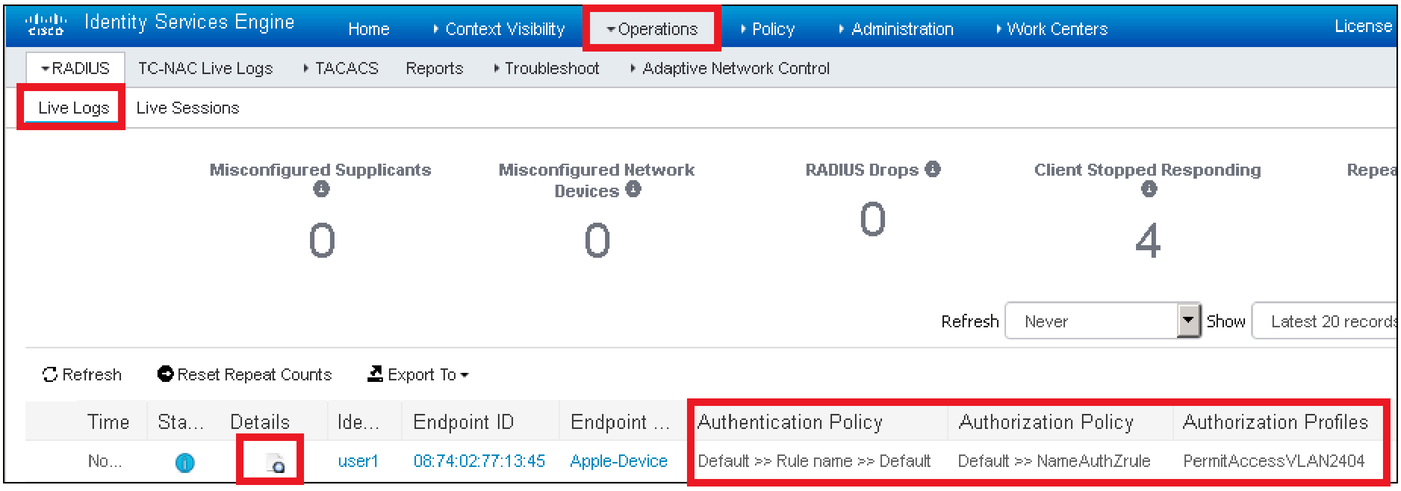
Pour lire facilement les sorties du client de débogage, utilisez l'outil d'analyse de débogage sans fil :

Outil d’analyse pour le débogage de réseaux sans fil

Processus d'authentification sur ISE

Accédez à Operations > RADIUS > Live Logs afin de voir quelle stratégie d'authentification, stratégie d'autorisation et profil d'autorisation a été attribué à l'utilisateur.

Pour plus d'informations, cliquez sur Details afin de voir un processus d'authentification plus détaillé comme montré dans l'image.



Time	Sta...	Details	Ide...	Endpoint ID	Endpoint ...	Authentication Policy	Authorization Policy	Authorization Profiles
No...	●	🔍	user1	08:74:02:77:13:45	Apple-Device	Default >> Rule name >> Default	Default >> NameAuthZrule	PermitAccessVLAN2404

Dépannage

Il n’y a actuellement aucune information spécifique disponible pour dépanner cette configuration.

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.