Configuration de 802.1x - PEAP avec FreeRadius et WLC 8.3

Contenu

Introduction

Ce document décrit comment configurer un réseau local sans fil (WLAN) avec la sécurité 802.1x et le protocole PEAP (Protected Extensible Authentication Protocol) en tant que protocole EAP (Extensible Authentication Protocol). FreeRADIUS est utilisé comme serveur RADIUS (Remote Authentication Dial-In User Service) externe.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Linux
- Éditeur Vim
- Contrôleurs LAN sans fil AireOS (WLC)

Remarque : ce document est destiné à donner aux lecteurs un exemple de configuration requise sur un serveur FreeRADIUS pour l'authentification PEAP-MS-CHAPv2. La configuration du serveur FreeRADIUS présentée dans ce document a été testée dans les travaux pratiques et a fonctionné comme prévu. Le centre d'assistance technique Cisco (TAC) ne prend pas en charge la configuration du serveur RADIUS gratuit.

Components Used

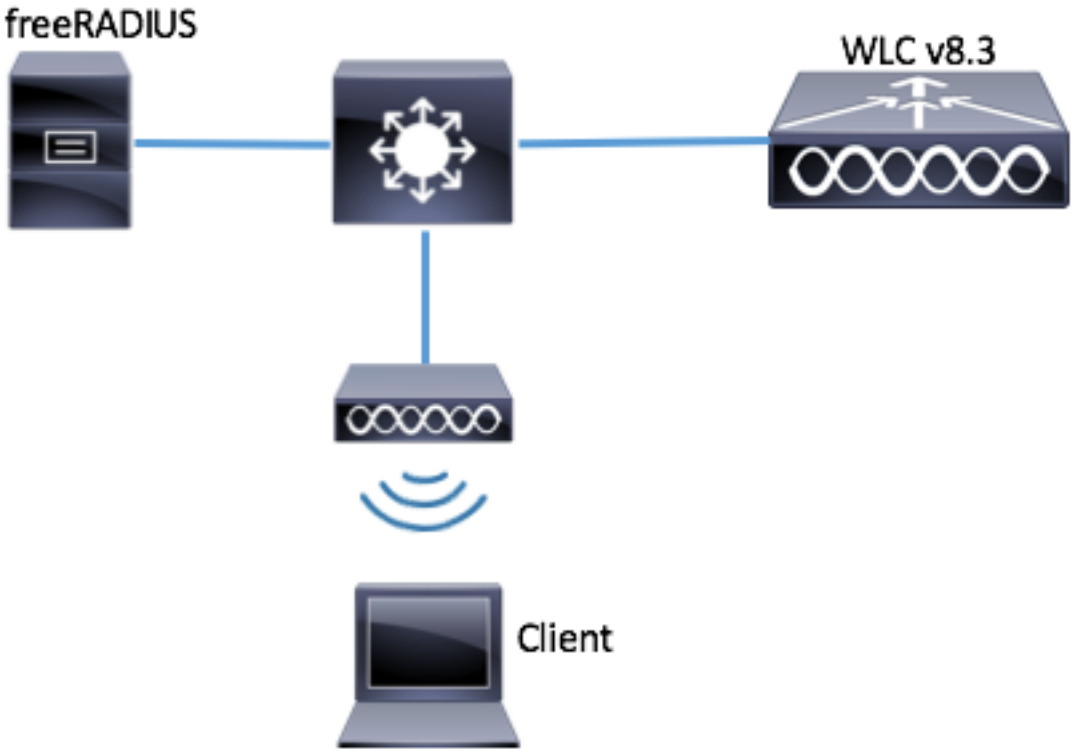
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- CentOS7 ou Red Hat Enterprise Linux 7 (RHEL7) (1 Go de RAM recommandé et au moins 20 Go de disque dur)
- WLC 5508 v8.3
- MariaDB (MySQL)
- FreeRADIUS
- PHP 7

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



Installer httpd Server et MariaDB

Étape 1. Exécutez ces commandes pour installer le serveur httpd et MariaDB.

```
[root@tac-mxwireless ~]# yum -y update
[root@tac-mxwireless ~]# yum -y groupinstall "Development Tools"
[root@tac-mxwireless ~]# yum -y install httpd httpd-devel mariadb-server mariadb
```

Étape 2. Démarrez et activez httpd (Apache) et le serveur MariaDB.

```
[root@tac-mxwireless ~]# systemctl enable httpd
[root@tac-mxwireless ~]# systemctl start httpd
[root@tac-mxwireless ~]# systemctl start mariadb
[root@tac-mxwireless ~]# systemctl enable mariadb
```

Étape 3. Configurez les paramètres MariaDB initiaux pour le sécuriser.

```
[root@tac-mxwireless ~]#mysql_secure_installation
```

> **Note**: Exécutez toutes les parties de ce script. Il est recommandé pour tous les serveurs MariaDB en production. Lisez attentivement chaque étape.

```
In order to log into MariaDB to secure it, we'll need the current
 password for the root user. If you've just installed MariaDB, and
 you haven't set the root password yet, the password will be blank,
 so you should just press enter here.

Enter current password for root (enter for none):
 OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB
 root user without the proper authorisation.

Set root password? [Y/n] Y New password: Re-enter new password: Password updated successfully!
Reloading privilege tables.. ... Success! By default, a MariaDB installation has an anonymous
user, allowing anyone to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation go a bit smoother. You
should remove them before moving into a production environment. Remove anonymous users? [Y/n] y
... Success! Normally, root should only be allowed to connect from 'localhost'. This ensures
that someone cannot guess at the root password from the network. Disallow root login remotely?
[Y/n] y ... Success! By default, MariaDB comes with a database named 'test' that anyone can
access. This is also intended only for testing, and should be removed before moving into a
production environment. Remove test database and access to it? [Y/n] y - Dropping test
database... ... Success! - Removing privileges on test database... ... Success! Reloading the
privilege tables will ensure that all changes made so far will take effect immediately. Reload
privilege tables now? [Y/n] y ... Success! Cleaning up... All done! If you've completed all of
the above steps, your MariaDB installation should now be secure. Thanks for using MariaDB!
```

Étape 4. Configurez la base de données pour freeRADIUS (utilisez le même mot de passe configuré à l'étape 3).

```
[root@tac-mxwireless ~]# mysql -u root -p -e "CREATE DATABASE radius"
[root@tac-mxwireless ~]# mysql -u root -p -e "show databases"
[root@tac-mxwireless ~]# mysql -u root -p
MariaDB [(none)]> GRANT ALL ON radius.* TO radius@localhost IDENTIFIED BY "radiuspassword";
MariaDB [(none)]> FLUSH PRIVILEGES; MariaDB [(none)]> \q
Bye
```

Installer PHP 7 sur CentOS 7

Étape 1. Exécutez ces commandes pour installer PHP 7 sur CentOS7.

```
[root@tac-mxwireless ~]# cd ~
[root@tac-mxwireless ~]# curl 'https://setup.ius.io/' -o setup-ius.sh
[root@tac-mxwireless ~]# sudo bash setup-ius.sh
[root@tac-mxwireless ~]# sudo yum remove php-cli mod_php php-common
[root@tac-mxwireless ~]# sudo yum -y install mod_php70u php70u-cli php70u-mysqlnd php70u-devel
php70u-gd php70u-mcrypt php70u-mbstring php70u-xml php70u-pear
[root@tac-mxwireless ~]# sudo apachectl restart
```

Installer FreeRADIUS

Étape 1. Exécutez cette commande pour installer FreeRADIUS.

```
[root@tac-mxwireless ~]# yum -y install freeradius freeradius-utils freeradius-mysql freeradius-
sqlite
```

Étape 2. Faites **radius.service** démarrer après **mariadb.service**.

Exécutez cette commande :

```
[root@tac-mxwireless ~]# vim /etc/systemd/system/multi-user.target.wants/radiusd.service
```

Ajouter une ligne dans la section **[Unité]** :

```
After=mariadb.service
```

[Unité] doit ressembler à ceci :

```
[Unit] Description=FreeRADIUS high performance RADIUS server. After=syslog.target network.target
After=mariadb.service
```

Étape 3. Démarrez et activez freeradius pour démarrer au démarrage.

```
[root@tac-mxwireless ~]# systemctl start radiusd.service
[root@tac-mxwireless ~]# systemctl enable radiusd.service
```

Étape 4. Activez le pare-feu pour la sécurité.

```
[root@tac-mxwireless ~]# systemctl enable firewalld
[root@tac-mxwireless ~]# systemctl start firewalld
[root@tac-mxwireless ~]# systemctl status firewalld
```

Étape 5. Ajoutez des règles permanentes à la zone par défaut pour autoriser les services http, https et radius.

```
[root@tac-mxwireless ~]# firewall-cmd --get-services | egrep 'http|https|radius'
[root@tac-mxwireless ~]# firewall-cmd --add-service={http,https,radius} --permanent success
```

Étape 6. Rechargez le pare-feu pour que les modifications prennent effet.

```
[root@tac-mxwireless ~]# firewall-cmd --reload
```

FreeRADIUS

Afin de configurer FreeRADIUS pour utiliser MariaDB, suivez ces étapes.

Étape 1. Importez le schéma de base de données RADIUS pour remplir la base de données RADIUS.

```
[root@tac-mxwireless ~]# mysql -u root -p radius < /etc/raddb/mods-
config/sql/main/mysql/schema.sql
```

Étape 2. Créez un lien logiciel pour Structured Query Language (SQL) sous **/etc/raddb/mods-enabled**.

```
[root@tac-mxwireless ~]# ln -s /etc/raddb/mods-available/sql /etc/raddb/mods-enabled/
```

Étape 3. Configurez le module SQL /raddb/mods-available/sql et modifiez les paramètres de connexion à la base de données pour qu'ils correspondent à votre environnement.

```
[root@tac-mxwireless ~]# vim /etc/raddb/mods-available/sql
```

La section SQL doit être similaire à ceci.

```
sql {


driver = "rlm_sql_mysql"
dialect = "mysql"

# Connection info:

server = "localhost"

 port = 3306
login = "radius"
password = "radpass" # Database table configuration for everything except Oracle radius_db =
"radius" } # Set to ‘yes’ to read radius clients from the database (‘nas’ table) # Clients will
ONLY be read on server startup. read_clients = yes # Table to keep radius client info
client_table = “nas”
```

Étape 4. Modifiez le droit du groupe de **/etc/raddb/mods-enabled/sql** en radiusd.

```
[root@tac-mxwireless ~]# chgrp -h radiusd /etc/raddb/mods-enabled/sql
```

WLC en tant que client AAA (Authentication, Authorization, and Accounting) sur FreeRADIUS

Étape 1. Modifiez **/etc/raddb/clients.conf** afin de définir la clé partagée pour le WLC.

```
[root@tac-mxwireless ~]# vim /etc/raddb/clients.conf
```

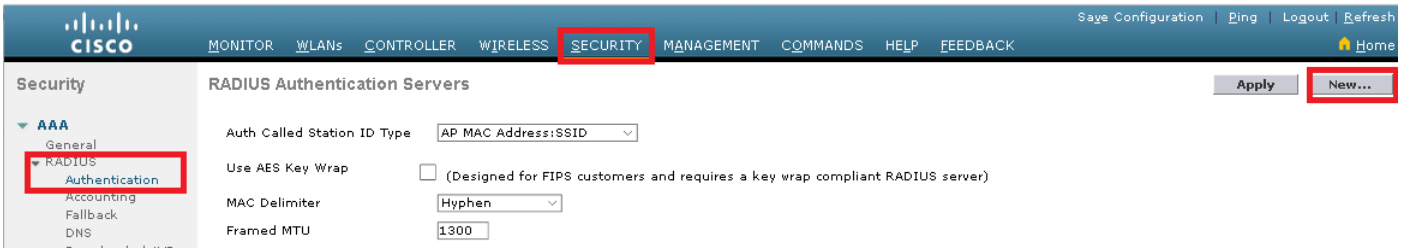
Étape 2. En bas, ajoutez l'adresse IP du contrôleur et la clé partagée.

```
client{ secret = shortname = }
```

FreeRADIUS en tant que serveur RADIUS sur WLC

IUG:

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



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

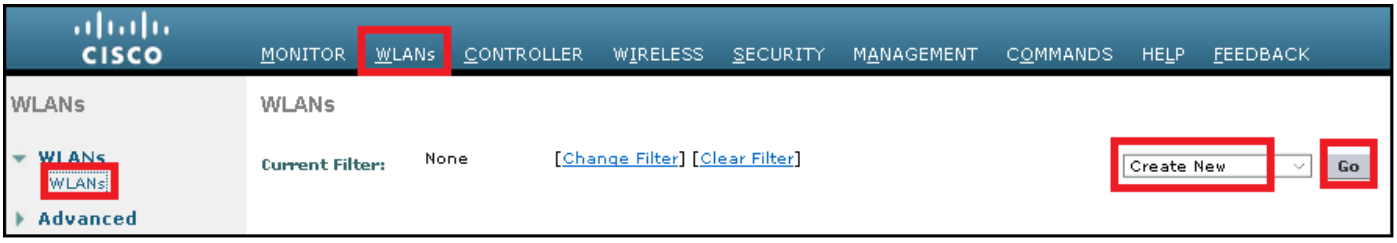
CLI :

```
> config radius auth add <index> <radius-ip-address> 1812 ascii <shared-key>
> config radius auth disable <index>
> config radius auth retransmit-timeout <index> <timeout-seconds>
> config radius auth enable <index>
```

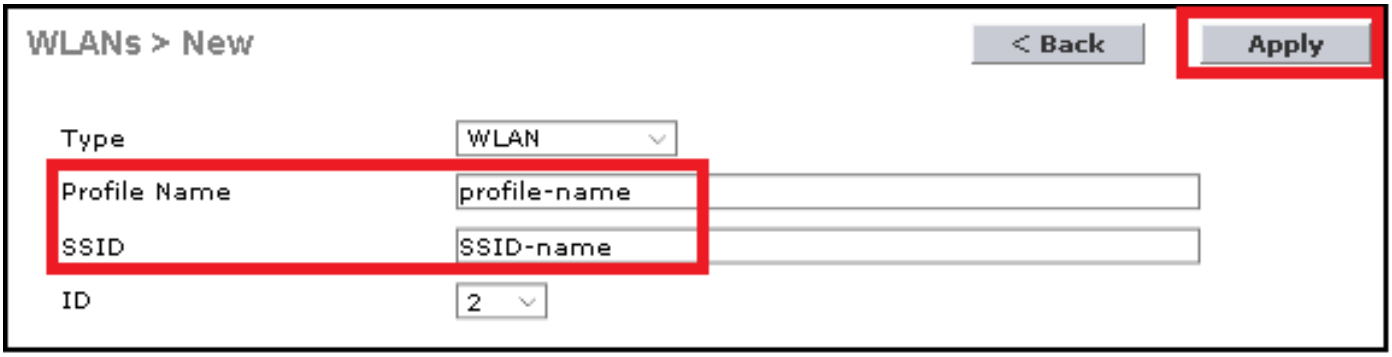
WLAN

IUG:

Étape 1. Ouvrez l'interface utilisateur graphique du WLC et accédez à **WLANs > Create New >** Goas présenté dans l'image.



Étape 2. Choisissez un nom pour l'identificateur SSID (Service Set Identifier) et le profil, puis cliquez sur Applyas comme indiqué dans l'image.



CLI :

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

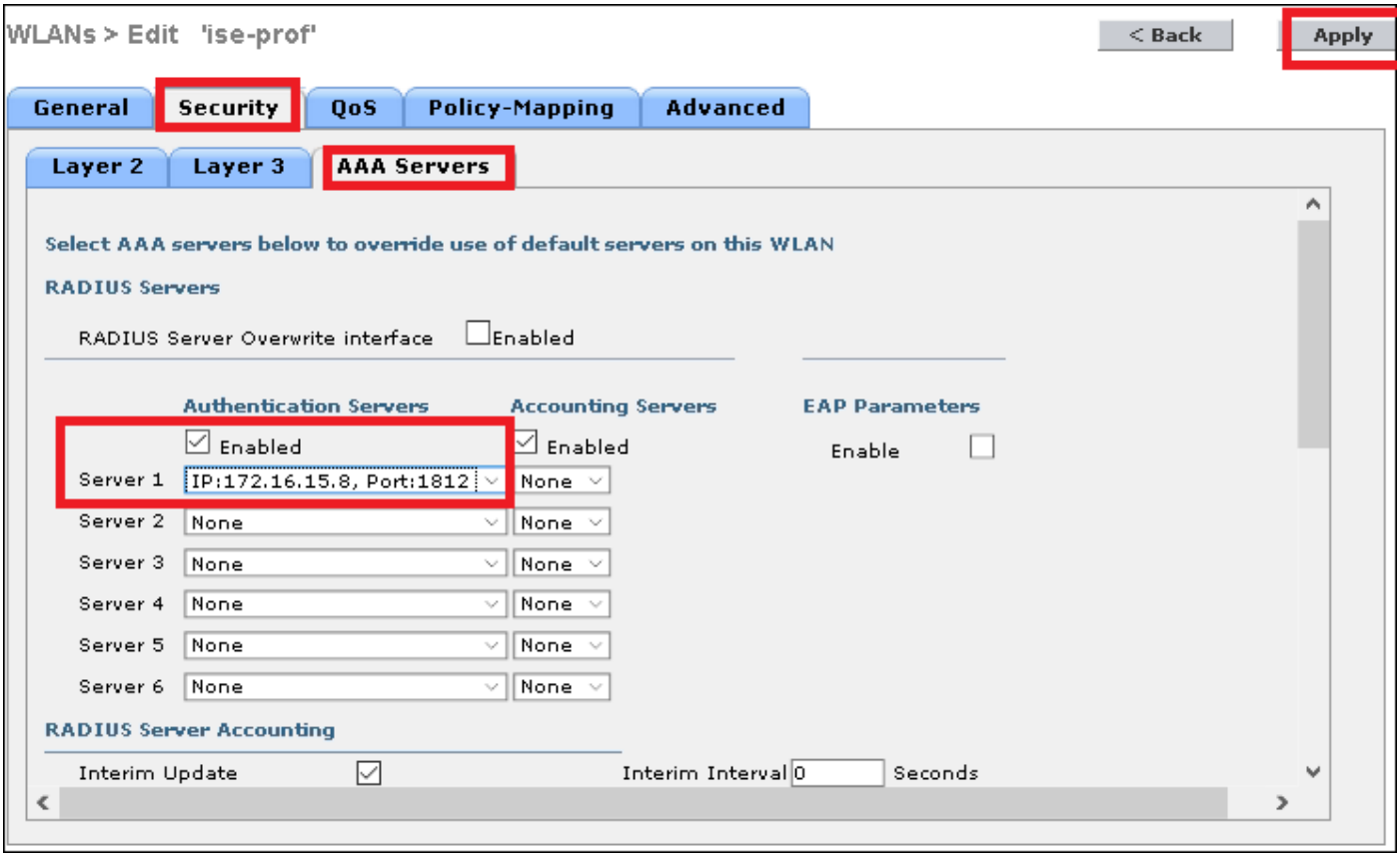
Étape 3. Attribuez le serveur RADIUS au WLAN.

CLI :

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

IUG:

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



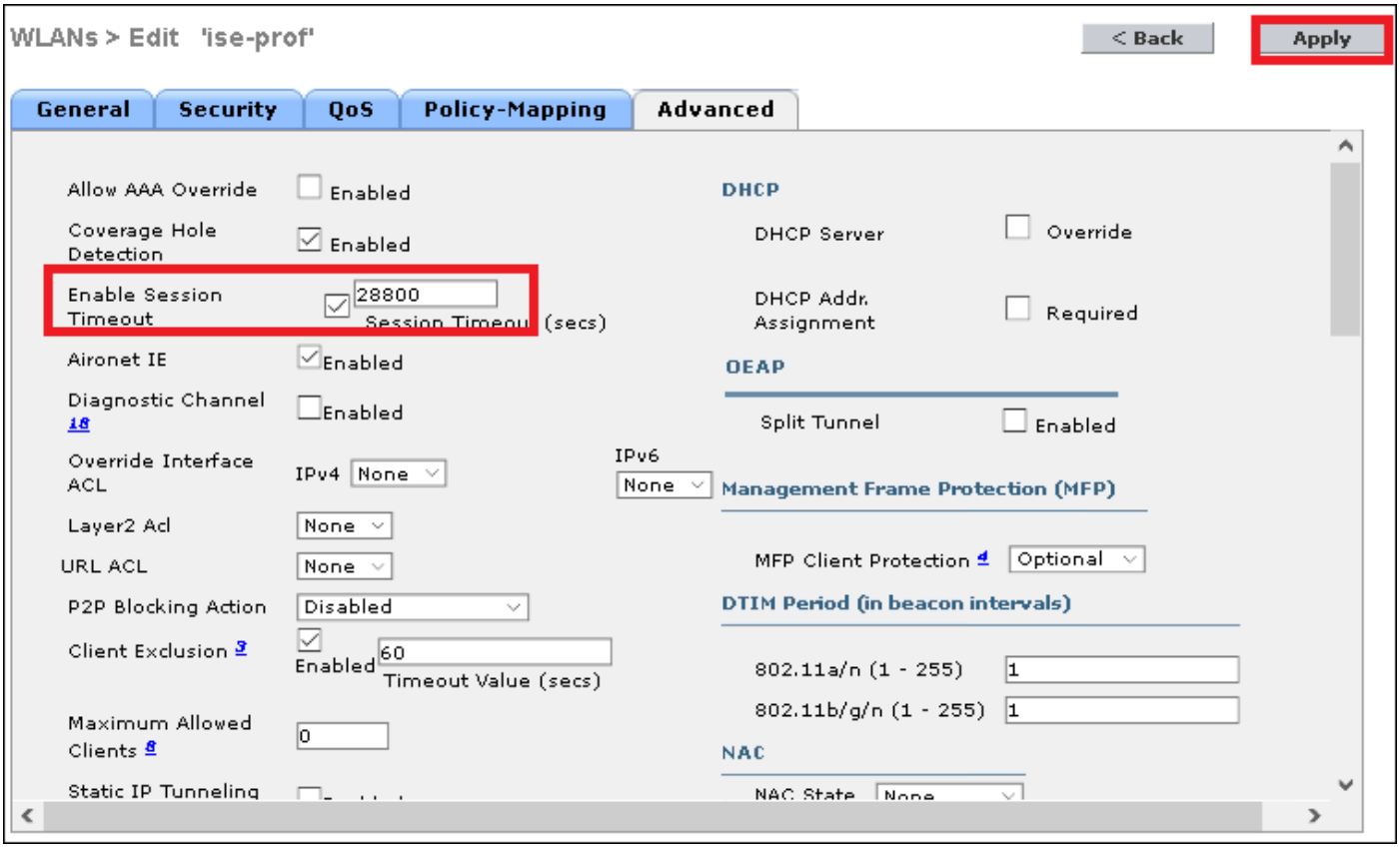
Étape 4. Augmentez éventuellement la durée de la session.

CLI :

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

IUG:

Accédez à **Avancé > Activer le délai d'attente de session >** cliquez sur **Appliquer** comme indiqué dans l'image.



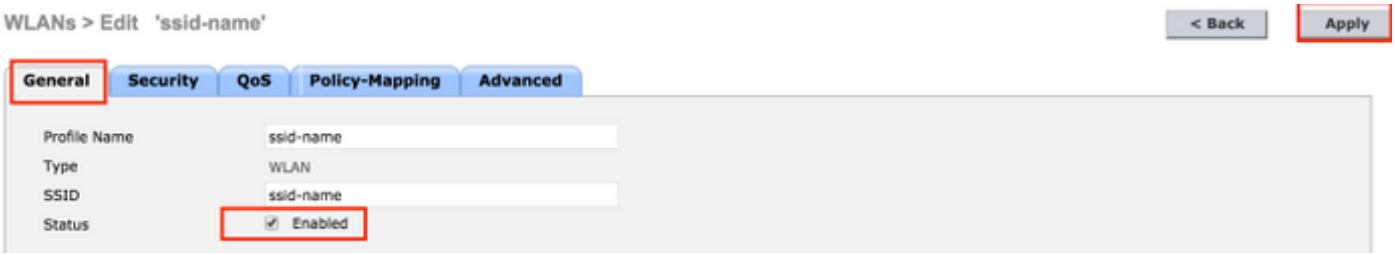
Étape 5. Activez le WLAN.

CLI :

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

IUG:

Naviguez jusqu'à **Général > Statut > Cliquez sur Activé > Cliquez sur Appliquer** comme indiqué dans l'image.



Ajouter des utilisateurs à la base de données FreeRADIUS

Par défaut, les clients utilisent des protocoles PEAP, mais freeRadius prend en charge d'autres méthodes (non couvertes dans ce guide).

Étape 1. Modifiez le fichier **/etc/raddb/users**.

```
[root@tac-mxwireless ~]# nano /etc/raddb/users
```

Étape 2. Au bas du fichier, ajoutez les informations sur les utilisateurs. Dans cet exemple, **user1**

est le nom d'utilisateur et **Cisco123** le mot de passe.

```
user1        Cleartext-Password := <Cisco123>
```

Étape 3. Redémarrez FreeRadius.

```
[root@tac-mxwireless ~]# systemctl restart radiusd.service
```

Certificats sur freeRADIUS

FreeRADIUS est fourni avec un certificat d'autorité de certification (CA) par défaut et un certificat de périphérique qui sont stockés dans le chemin /etc/raddb/certs. Le nom de ces certificats est ca.pem et server.pem. server.pem est le certificat que les clients reçoivent lorsqu'ils passent par le processus d'authentification. Si vous devez attribuer un autre certificat pour l'authentification EAP, vous pouvez simplement les supprimer et enregistrer les nouveaux dans le même chemin avec ce même nom exact.

Configuration du périphérique final

Configurez un ordinateur portable Windows pour qu'il se connecte à un SSID avec l'authentification 802.1x et PEAP/MS-CHAP (version Microsoft du protocole d'authentification à échanges confirmés) version 2.

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 RADIUS libre afin de terminer l'authentification
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 sur la configuration du périphérique final - Créer le profil WLAN.

Importer un certificat FreeRADIUS

Si vous utilisez les certificats par défaut installés sur freeRADIUS, suivez ces étapes afin d'importer le certificat EAP du serveur freeRADIUS dans le périphérique final.

Étape 1. Obtenez le certificat de FreeRadius :

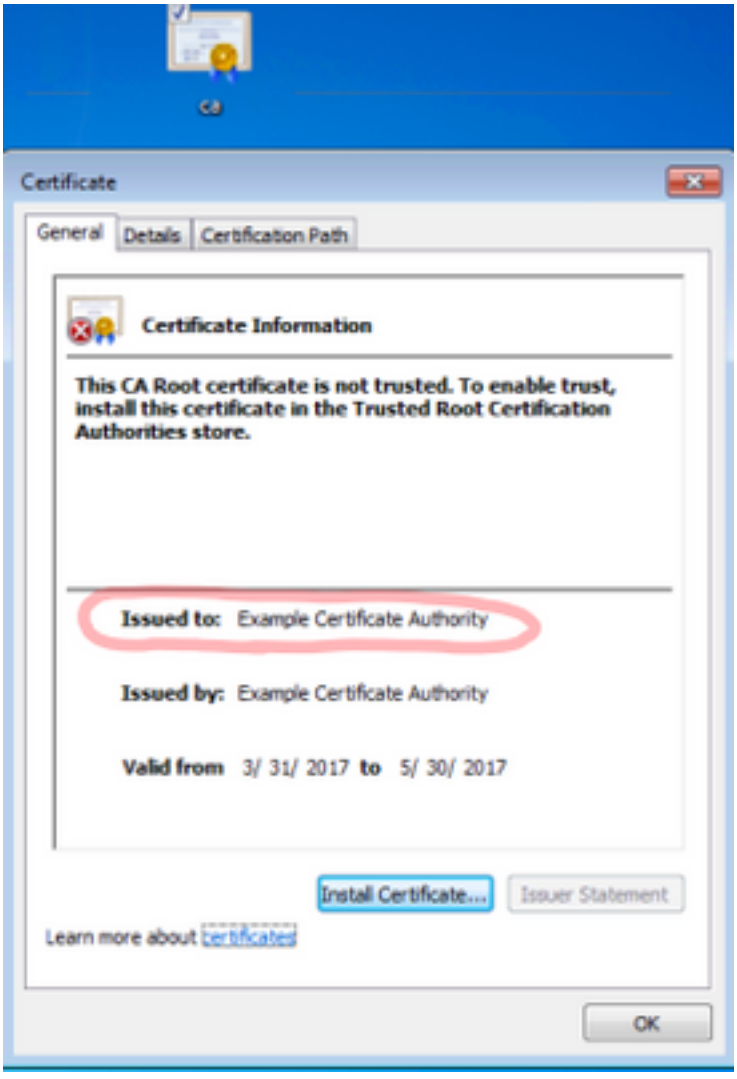
```
[root@tac-mxwireless ~]# cat /etc/raddb/certs/ca.pem

-----BEGIN CERTIFICATE-----
MIIE4TCCA8mgAwIBAgIJAKLmHn4eZLjBMA0GCSqGSIb3DQEBBQUAMIGTMQswCQYD
VQQGEwJGUjEPMA0GA1UECBMGUmFkaXVzMRIwEAYDVQQHEwlTb211ld2hlcmUxFTAT
BgNVBAoTDEV4YW1wbGUgSW5jLjEgMB4GCSqGSIb3DQEJARYRYWRtaW5AZXhhbXBs
ZS5jb20xJjAkBgNVBAMTHUV4YW1wbGUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4X
DTE3MDMzMTExMTIxNloXDTE3MDUzMDExMTIxNlowgZMxCzAJBgNVBAYTAkZSMQ8w
DQYDVQQIEwZSYWRpdXMxEjAQBgNVBAcTCVNvbWV3aGVyZTEVMBMGA1UEChMMRXhh
bXBsZSBJbmMuMSAwHgYJKoZIhvcNAQkBFhFhZG1pbkBleGFtcGxlLmNvbTEmMCQG
A1UEAxMdRXhhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwggEiMA0GCSqGSIb3
```

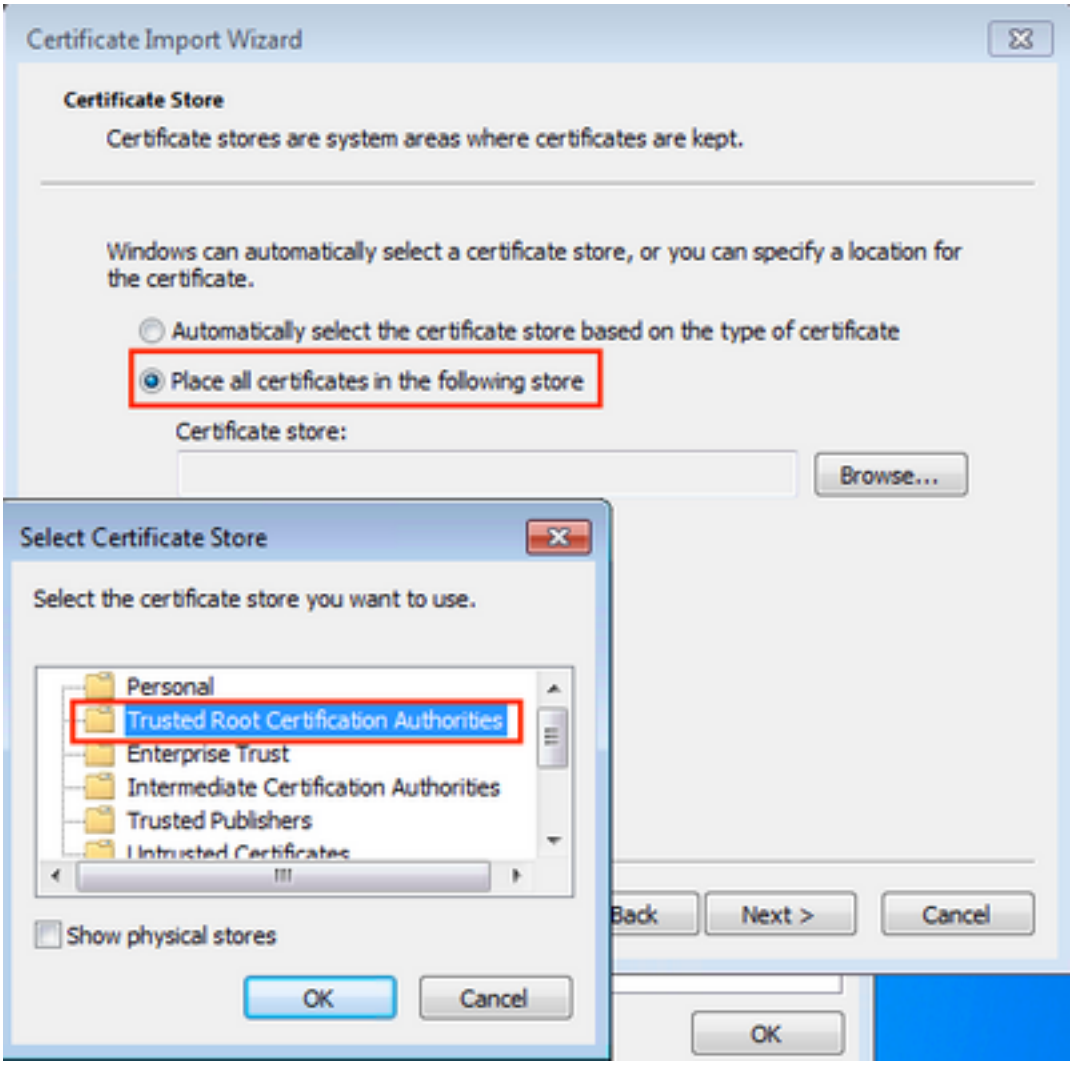
```
DQEBAQUAA4IBDwAwggEKAoIBAQC0vJ53NN7J9vhpKhcB3B0OXLpeQFWjqolQOB9F
/8Lh2Hax2rzb9wxOi1MOyXR+kN22H7RNwUHET8VdyGUsA4OdZWuyzI8sKi5H42GU
Eu6GDw1YJvhHn4rVC36OZU/Nbaxj0eR8ZG0JGse4ftQKLfckkvCOS5QGn4X1elRS
oFe27HRF+pTDHd+nzbaDvhYWvFoe6iA27Od7AY/sDuo/tiIJWGdm9ocPz3+0IiFC
ay6dtG55YQOHxKaswH7/HJkLsKWhS4YmXLgJXCeeJqooqr+TEwyCDEaFaiX835Jp
gwNNZ7X5US0FcjuuOtpJJ3hfQ8K6uXjEWPOkDE0DAnqp4/n9AgMBAAGjggE0MIIB
MDAdBgNVHQ4EFgQUysFNRZKpAlcFCEgwdOPVGV0waLEwgcgGA1UdIwSBwDCBvYAU
ysFNRZKpAlcFCEgwdOPVGV0waLGhgZmkgZYwgZMxCzAJBgNVBAYTAkZSMQ8wDQYD
VQQIEwZSYWRpdXMxEjAQBgNVBAcTCVNvbWV3aGVyZTEVMBMGA1UEChMMRXhhbXBs
ZSBJbmMuMSAwHgYJKoZIhvcNAQkBFhFhZG1pbkBleGFtcGxlLmNvbTEmMCQGA1UE
AxMdRXhhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHmCCQCi5h5+HmS4wTAMBgNV
HRMEBTADAQH/MDYGA1UdHwQvMC0wK6ApoCeGJWh0dHA6Ly93d3cuZXhhbXBsZS5j
b20vZXhhbXBsZV9jYS5jcmwwDQYJKoZIhvcNAQEFBQADggEBACsPR2jiOFXnTsK4
1wnrrMylZZb12gDuqK+zKELox2mzlDMMK83tBsL8yjkv70KeZn821IzfTrTfvhzV
mjX6HgaWfYyMjYYYSw/iEu2JsAtQdpvC3di10nGwVPHlzbozPdov8cZtCb21ynfY
Z6cNjx8+aYQIcsRIyqA1IXMOBwIXo141TOmoODdgfX95lpoLwgktRLkvl7Y7owsz
ChYDO++H7Iewsxx5pQfm56dA2cNrlTwWtMvViKyX7GlpwlbBOxgkLiFJ5+GFbfLh
a0HBHZWhTKvffbr62mkbfjCUfJU4T3xgY9zFwiwT+BetCJgAGy8CT/qmnO+NJERO
RUvDhfE=
-----END CERTIFICATE-----
```

Étape 2. Copier et coller la sortie de l'étape précédente dans un fichier texte et modifier l'extension en .crt

Étape 3. Double-cliquez sur le fichier et sélectionnez **Installer le certificat...** comme le montre l'image.

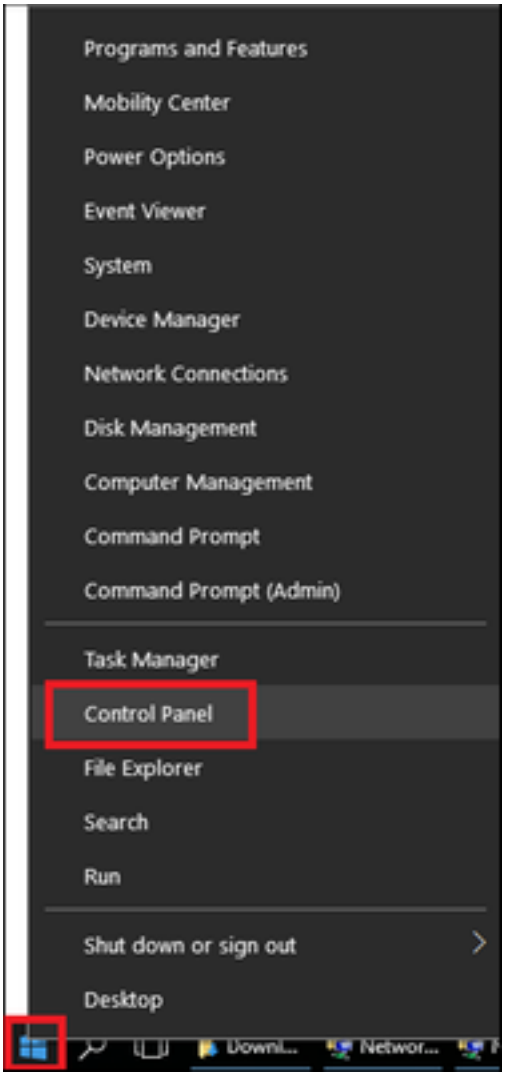


Étape 4. Installez le certificat dans le magasin **Autorités de certification racine de confiance** comme indiqué sur l'image.

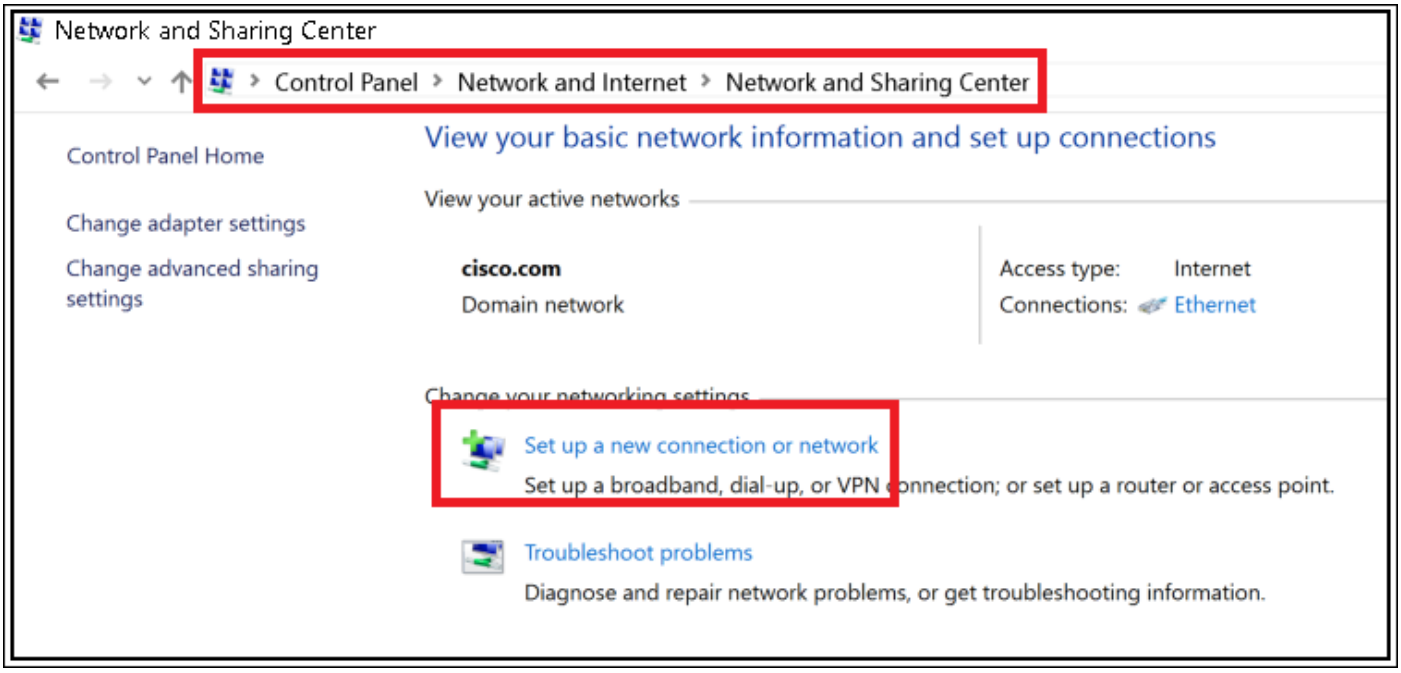


Créer un profil WLAN

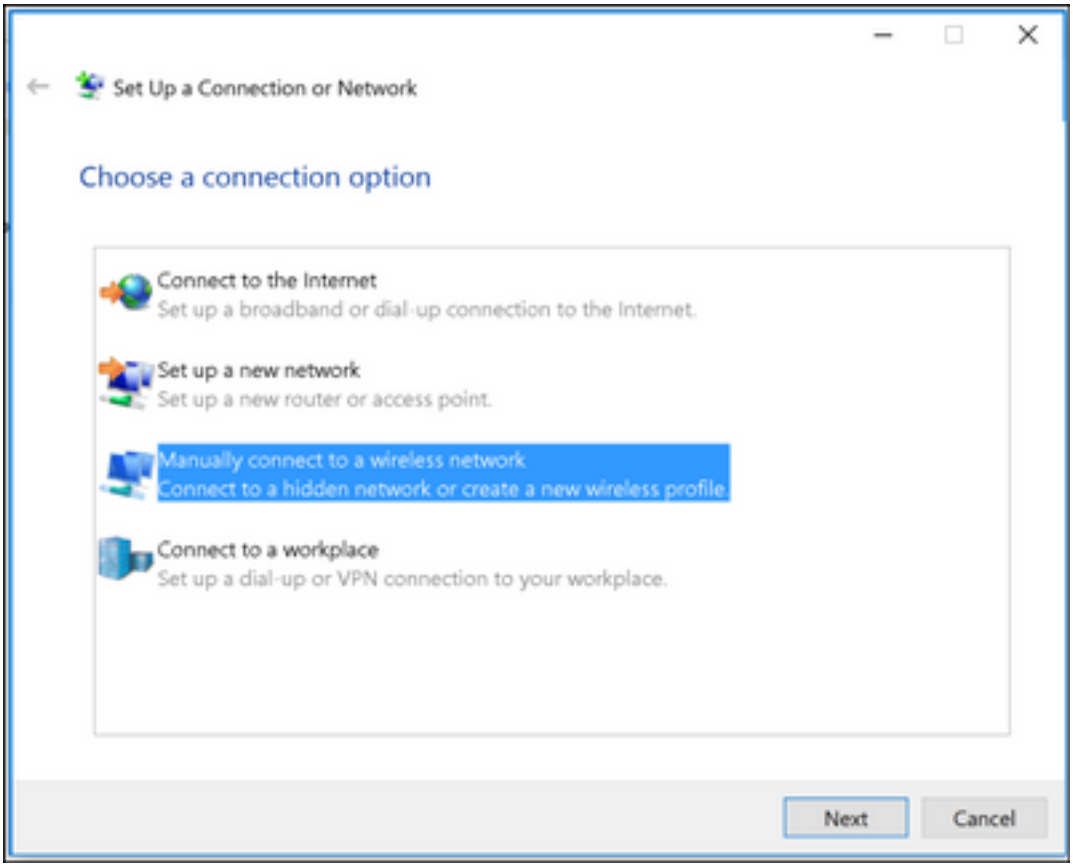
Étape 1. Cliquez avec le bouton droit sur l'icône Démarrer et sélectionnez **Panneau de configuration** comme indiqué dans l'image.



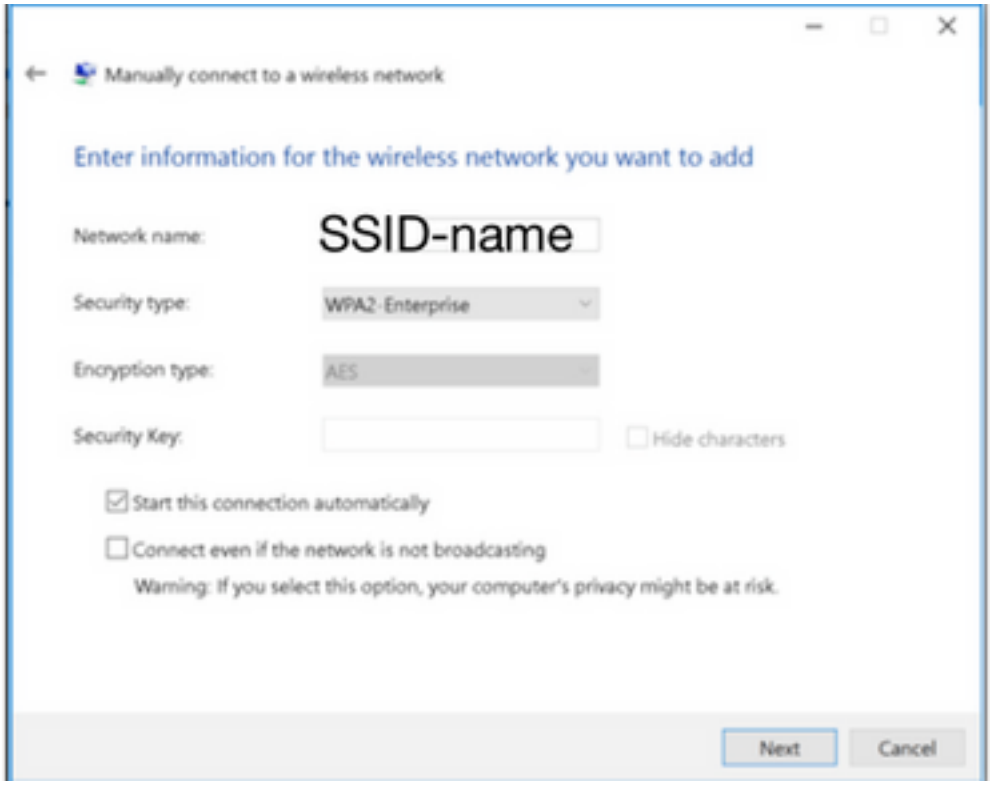
Étape 2. Accédez à **Réseau et Internet > Centre Réseau et partage> cliquez sur Configurer une nouvelle connexion ou un nouveau réseau** comme indiqué dans l'image.



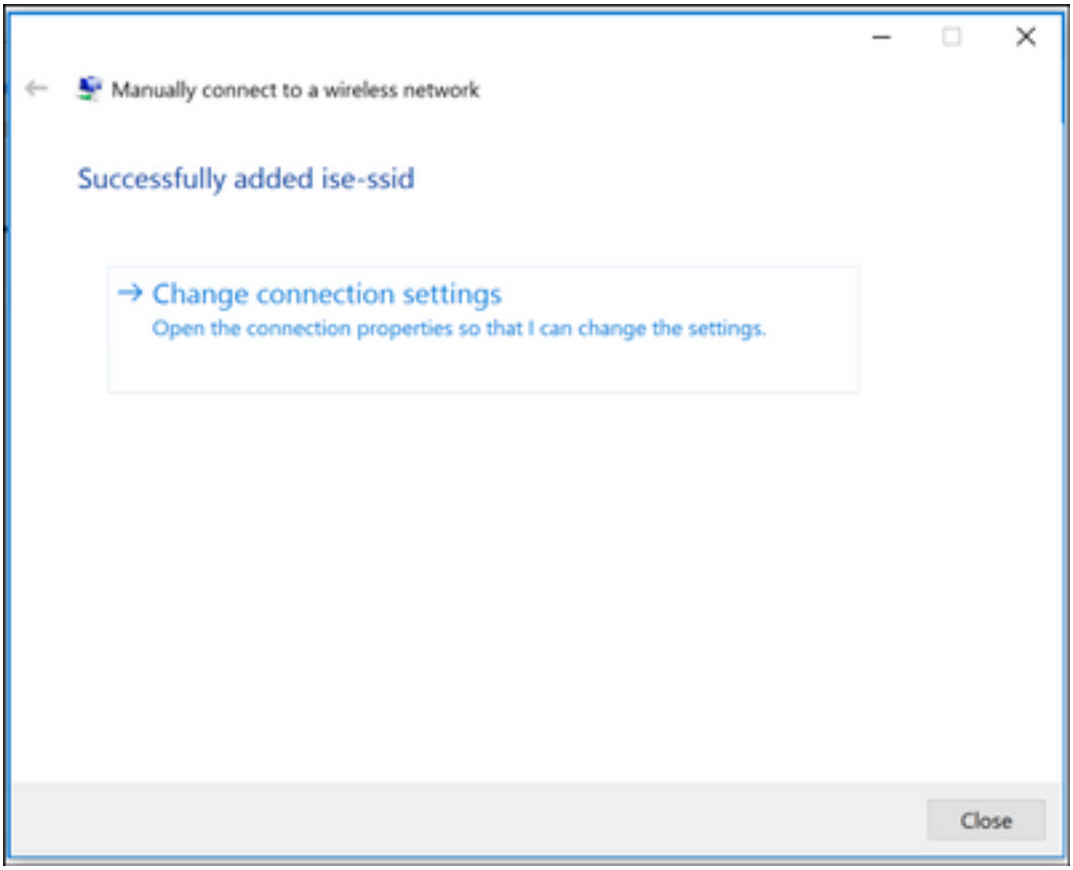
Étape 3. Sélectionnez **Connexion manuelle à un réseau sans fil** et cliquez sur Suivant comme indiqué dans l'image.



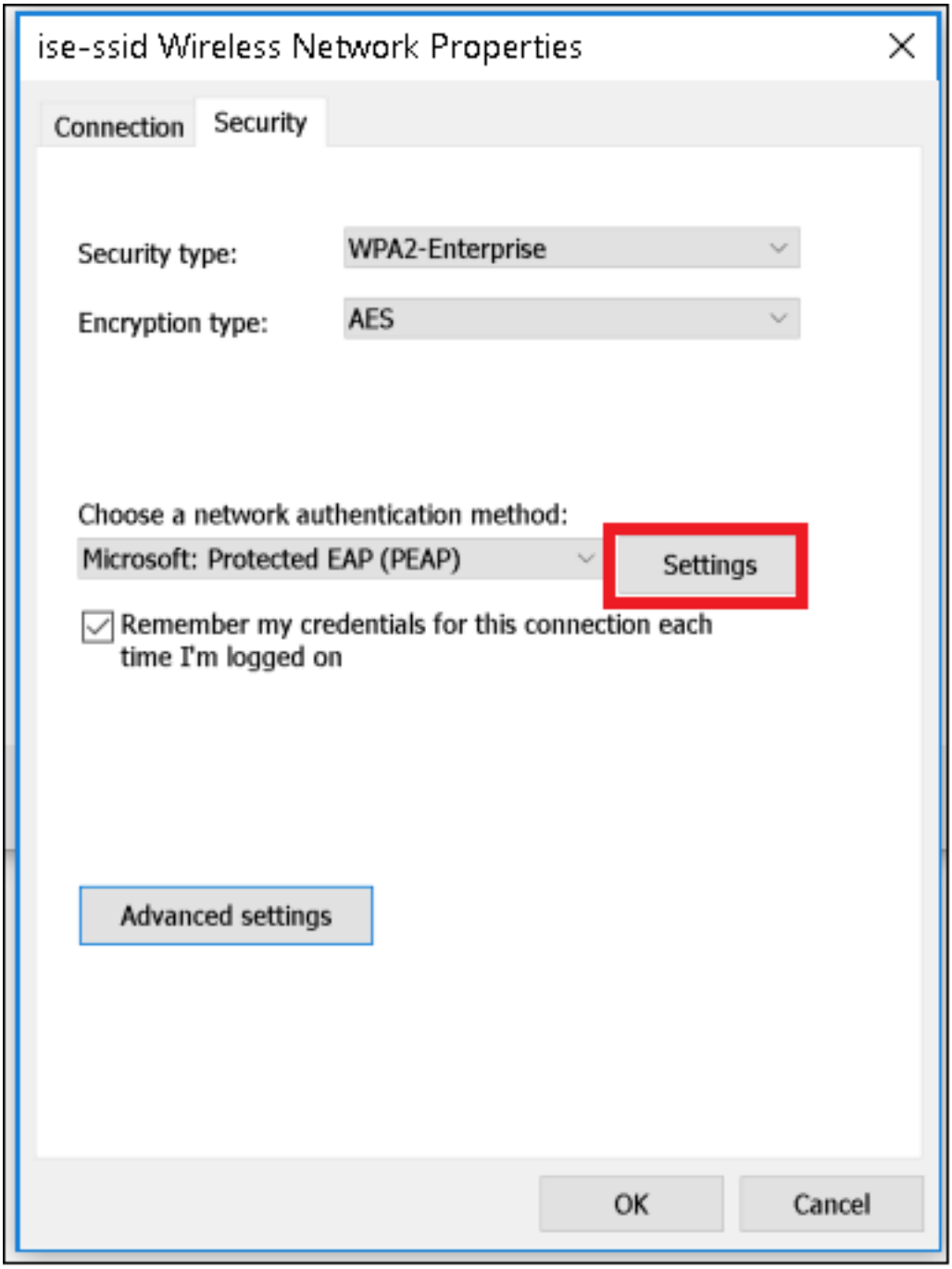
Étape 4. Entrez les informations avec le nom du SSID et du type de sécurité WPA2-Enterprise, puis cliquez sur **Suivant** comme indiqué dans l'image.



Étape 5. Sélectionnez **Modifier les paramètres de connexion** afin de personnaliser la configuration du profil WLAN comme indiqué dans l'image.



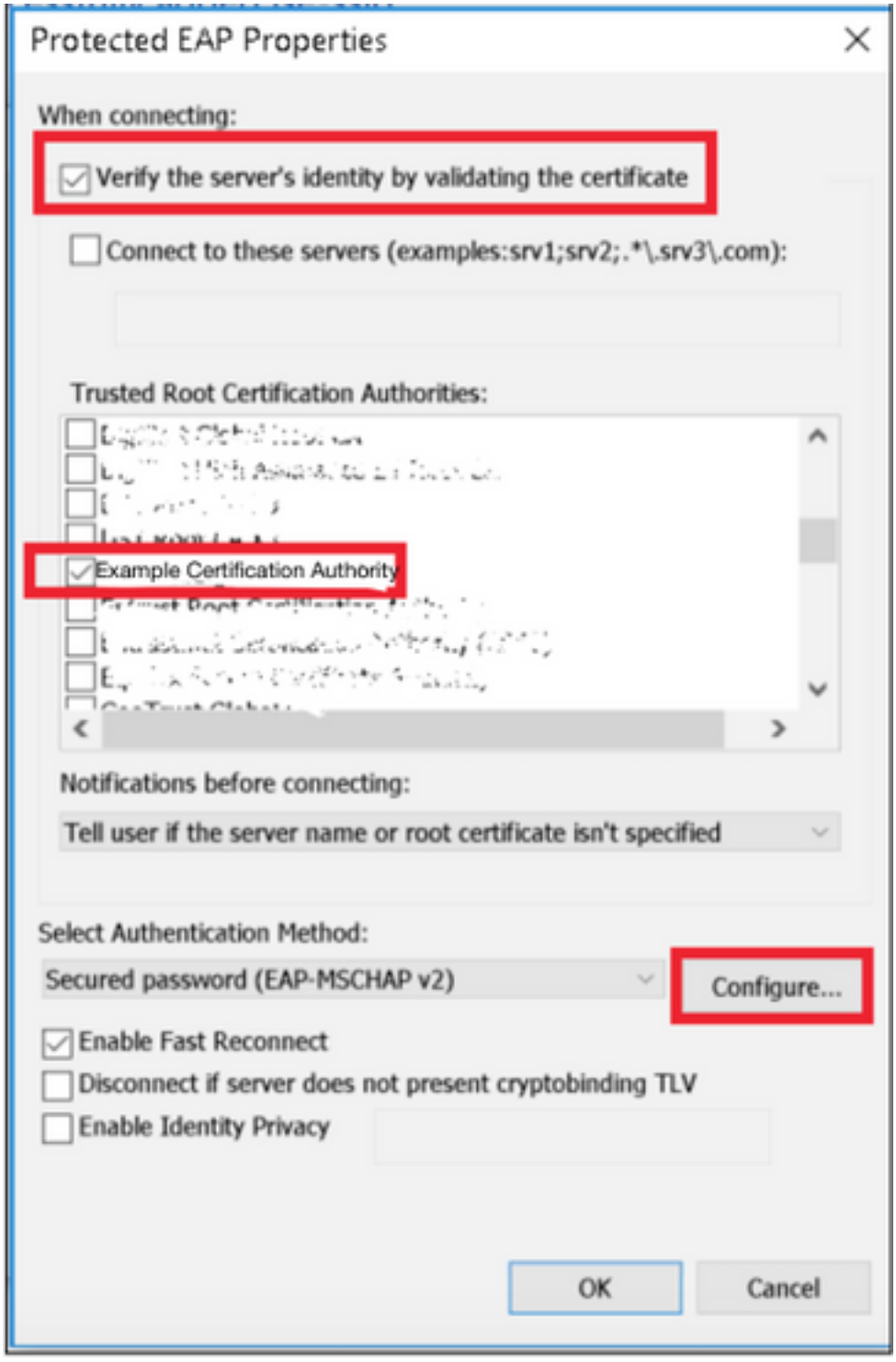
Étape 6. Accédez à l'onglet **Sécurité** et cliquez sur **Paramètres** comme indiqué dans l'image.

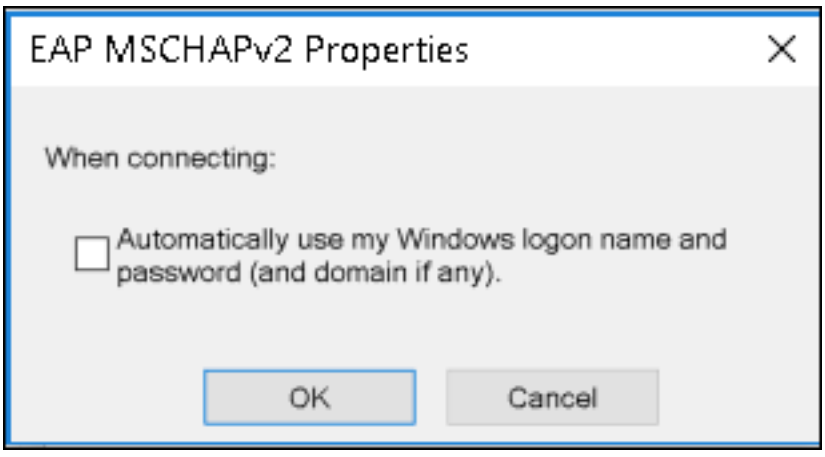


Étape 7. Choisissez si le serveur RADIUS est validé ou non.

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

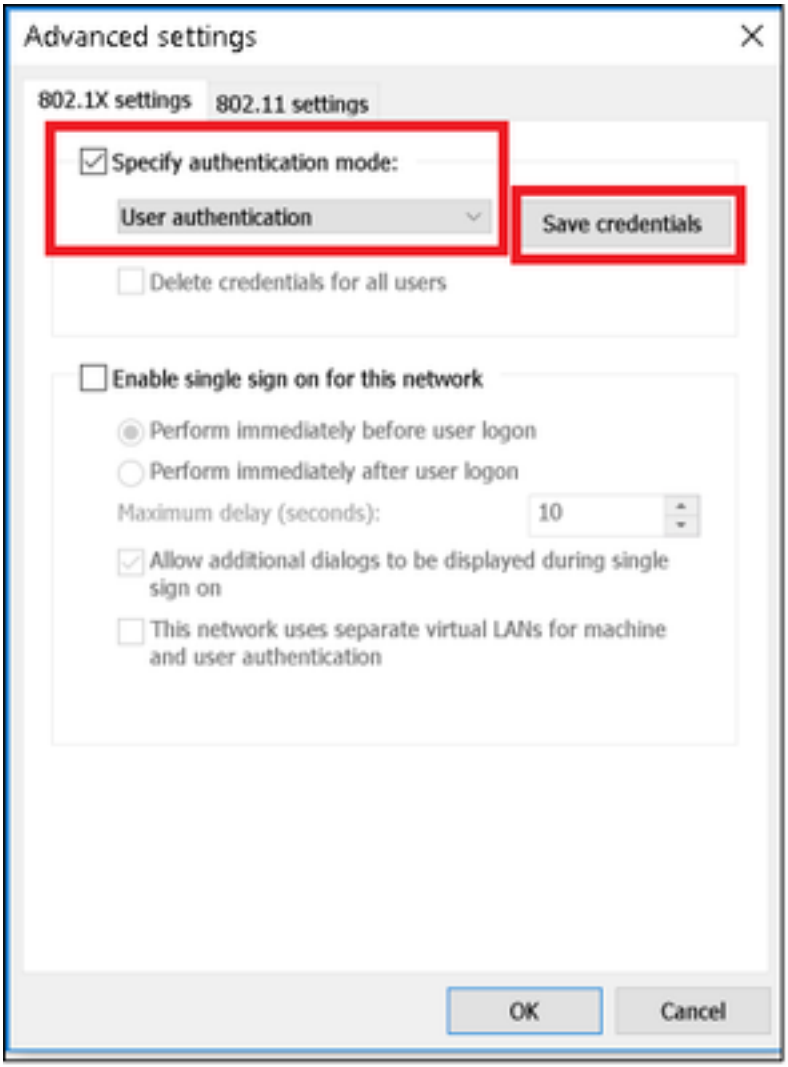
Après cela, sélectionnez **Configurer** et désactiver **Utiliser automatiquement mon nom de connexion et mon mot de passe Windows...**, puis cliquez sur **OK** comme indiqué dans les images.

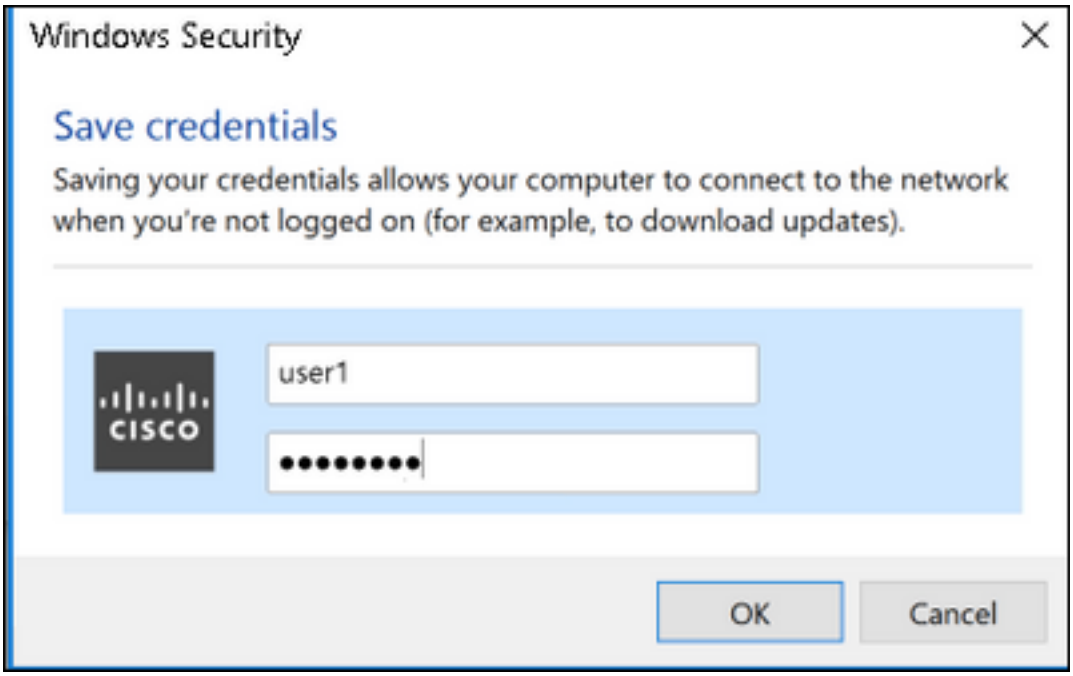




Étape 8. Configurez les informations d'identification de l'utilisateur.

Une fois de retour à l'onglet Sécurité, sélectionnez **Paramètres avancés**, spécifiez le mode d'authentification en tant qu'**authentification utilisateur** et enregistrez les informations d'identification configurées sur freeRADIUS afin d'authentifier l'utilisateur, comme indiqué dans les images.





Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

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
```

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

Analyseur de débogage sans fil

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.