Configurez le 802.1x - PEAP avec FreeRadius et WLC 8.3

Contenu

Introduction

Ceci documente explique comment installer un WLAN (réseau local sans fil) avec la Sécurité de 802.1x et le PEAP (Protected Extensible Authentication Protocol) comme EAP (Extensible Authentication Protocol). FreeRADIUS est utilisé en tant que serveur externe de Service RADIUS (Remote Authentication Dial-In User Service).

Conditions préalables

Cisco recommande que vous ayez la connaissance de base de l'éditeur de Linux, de score et des contrôleurs LAN Sans fil d'AireOS (WLCs).

> Remarque: Ce document est destiné pour donner aux lecteurs un exemple sur la configuration exigée sur un serveur de freeRADIUS pour l'authentification PEAP-MS-CHAPv2. La configuration du serveur de freeRADIUS présentée dans ce document a été testée dans le laboratoire et avérée pour fonctionner comme prévue. Le centre d'assistance technique Cisco (TAC) ne prend en charge pas la configuration du serveur de freeRADIUS.

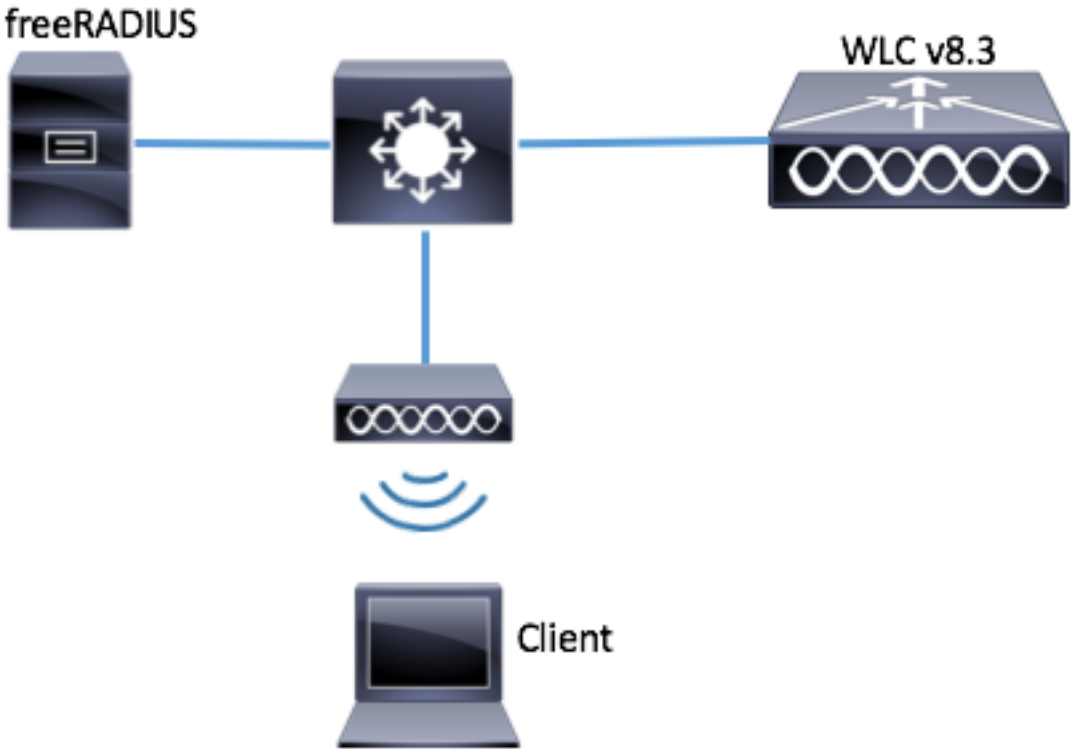
Composants utilisés

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

- PHP 7

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

Diagramme du réseau



Configuration

Installez le serveur et le MariaDB httpd

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

```
[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. Mettez en marche et activez httpd (Apache) et serveur de 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 configurations initiales de MariaDB pour la sécuriser.

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

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB SERVERS IN PRODUCTION USE!
PLEASE READ EACH STEP CAREFULLY! 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 le freeRADIUS (utilisez le même mot de passe configuré dans 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
```

Installez PHP 7 sur CentOS 7

Étape 1. Exécutez ces commandes d'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
```

Installez FreeRADIUS

Étape 1. Exécutez cette commande d'installer FreeRADIUS.

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

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

Exécutez cette commande :

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

Ajoutez une ligne dans **[la** section d'**unité]** :

```
After=mariadb.service
```

[La section d'unité] doit ressembler à ceci :

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

Étape 3. Commencez et permettez au freeradius de commencer à l'amorce.

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

Étape 4. Firewalld d'enable pour la Sécurité.

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

Étape 5. Ajoutez les règles permanentes de transférer la zone pour permettre le HTTP, les https et les services 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. Firewalld de recharge pour que les modifications les prennent effet.

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

Configurez FreeRADIUS

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

Étape 1. Importez le schéma de RADIUSdatabase de remplir base de données de RAYON.

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

Étape 2. Créez un lien mou pour le 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 */raddb/mods-available/sql* SQL et changez les paramètres de Connexion de la base de données à la suite votre environnement.

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

La section SQL doit sembler semblable à ci-dessous.

```
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. Juste de groupe de modification de */etc/raddb/mods-enabled/sql au* radiusd.

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

Configurez WLC comme client d'AAA sur FreeRADIUS

Étape 1. Éditez */etc/raddb/clients.conf* afin de placer la clé partagée pour WLC.

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

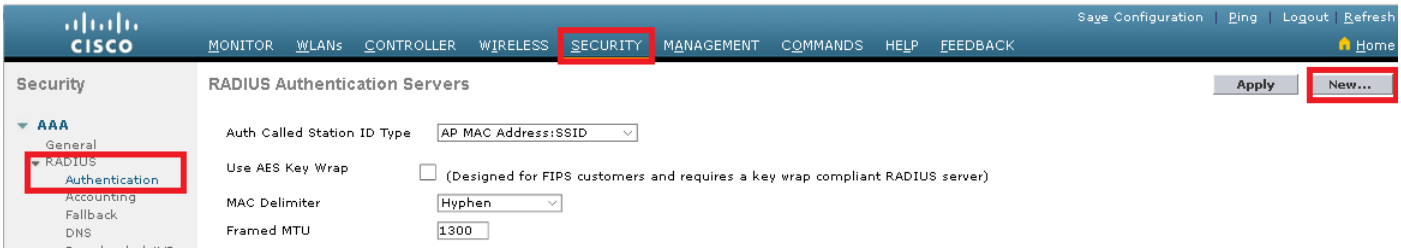
Étape 2. Au bas ajoutez votre IP address de contrôleur et la clé partagée.

```
client<WLC-ip-address> { secret = <shared-key> shortname = <WLC-name> }
```

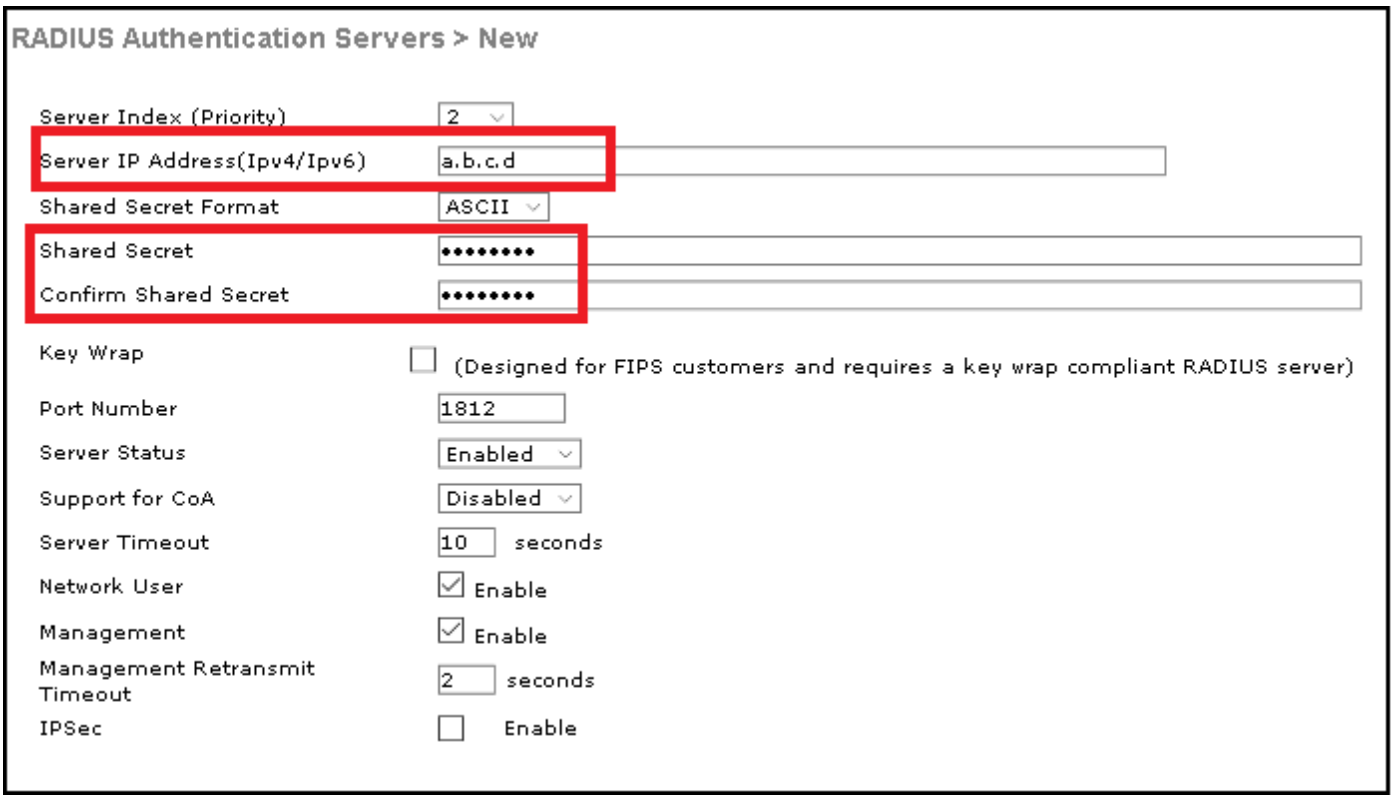
Configurez FreeRADIUS comme serveur de RAYON sur WLC

GUI :

Étape 1. Ouvrez le GUI du WLC et naviguez vers le **Security > Radius > Authentication > nouveau.**



Étape 2. Remplissez informations du serveur de RAYON.



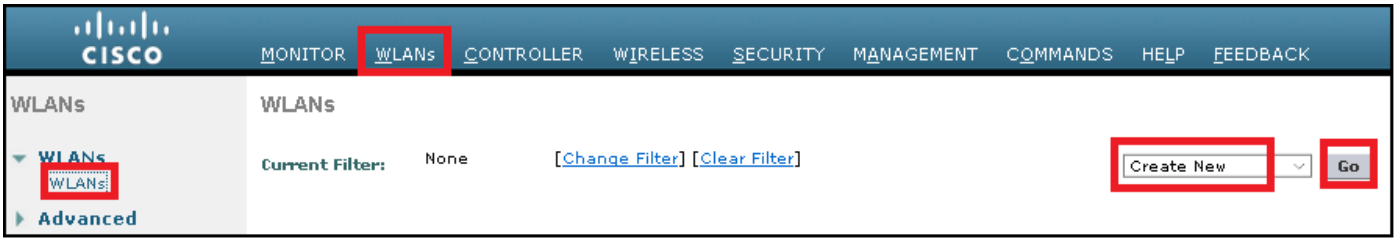
CLI :

```
> 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>
```

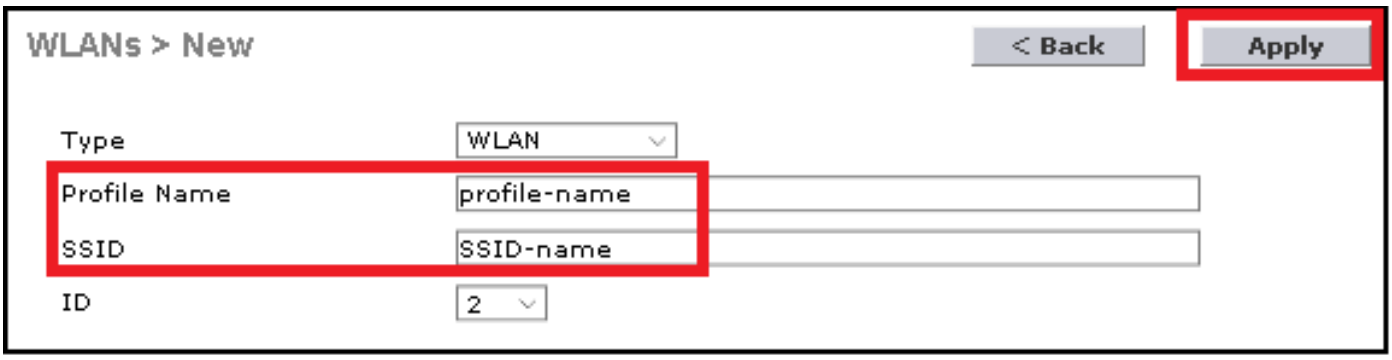
Configurez un WLAN

GUI :

Étape 1. Ouvrez le GUI du WLC et naviguez vers des **WLAN > créent nouveau > vont.**



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



CLI :

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

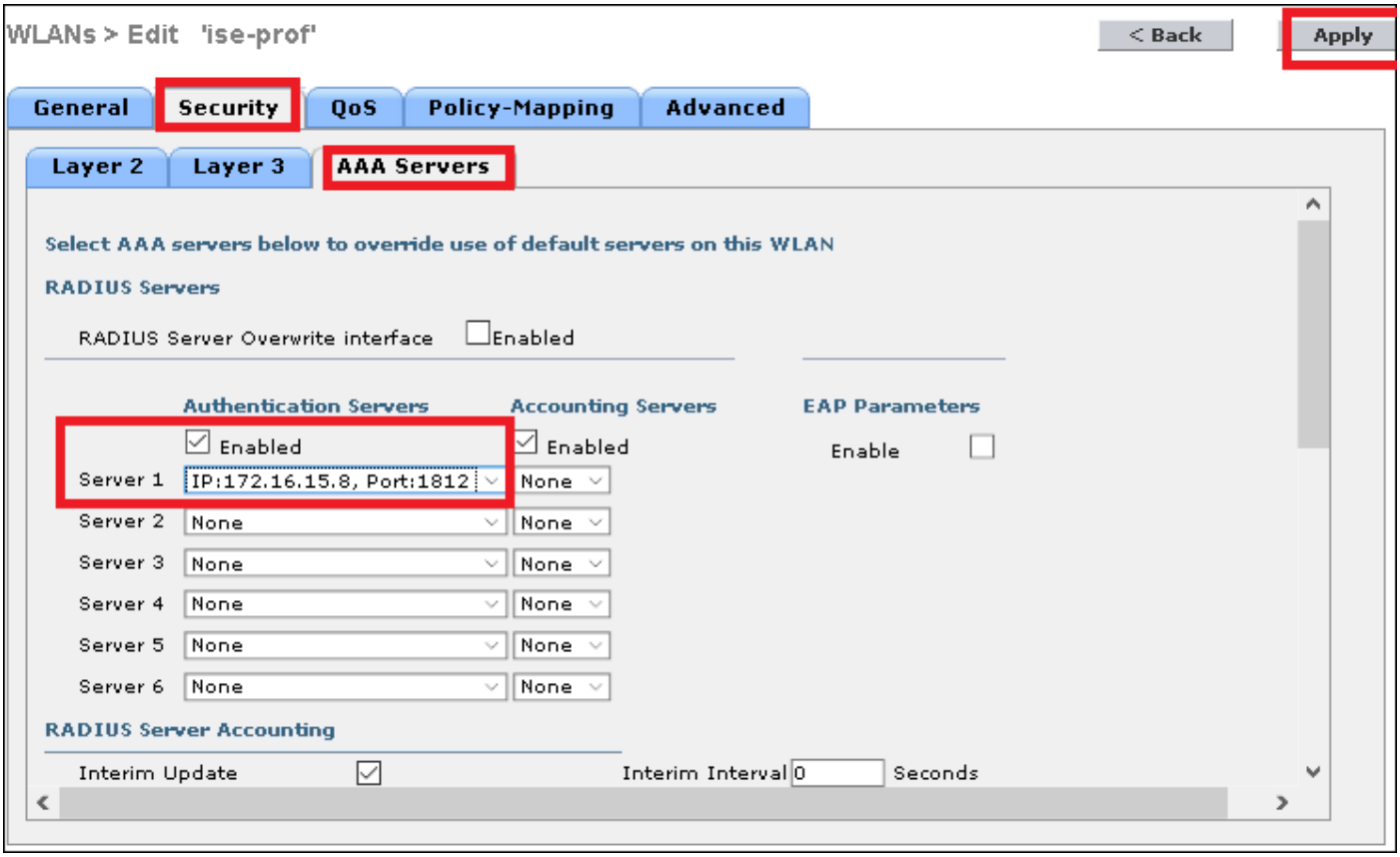
Étape 3. Affectez le serveur de RAYON au WLAN.

CLI :

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

GUI :

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

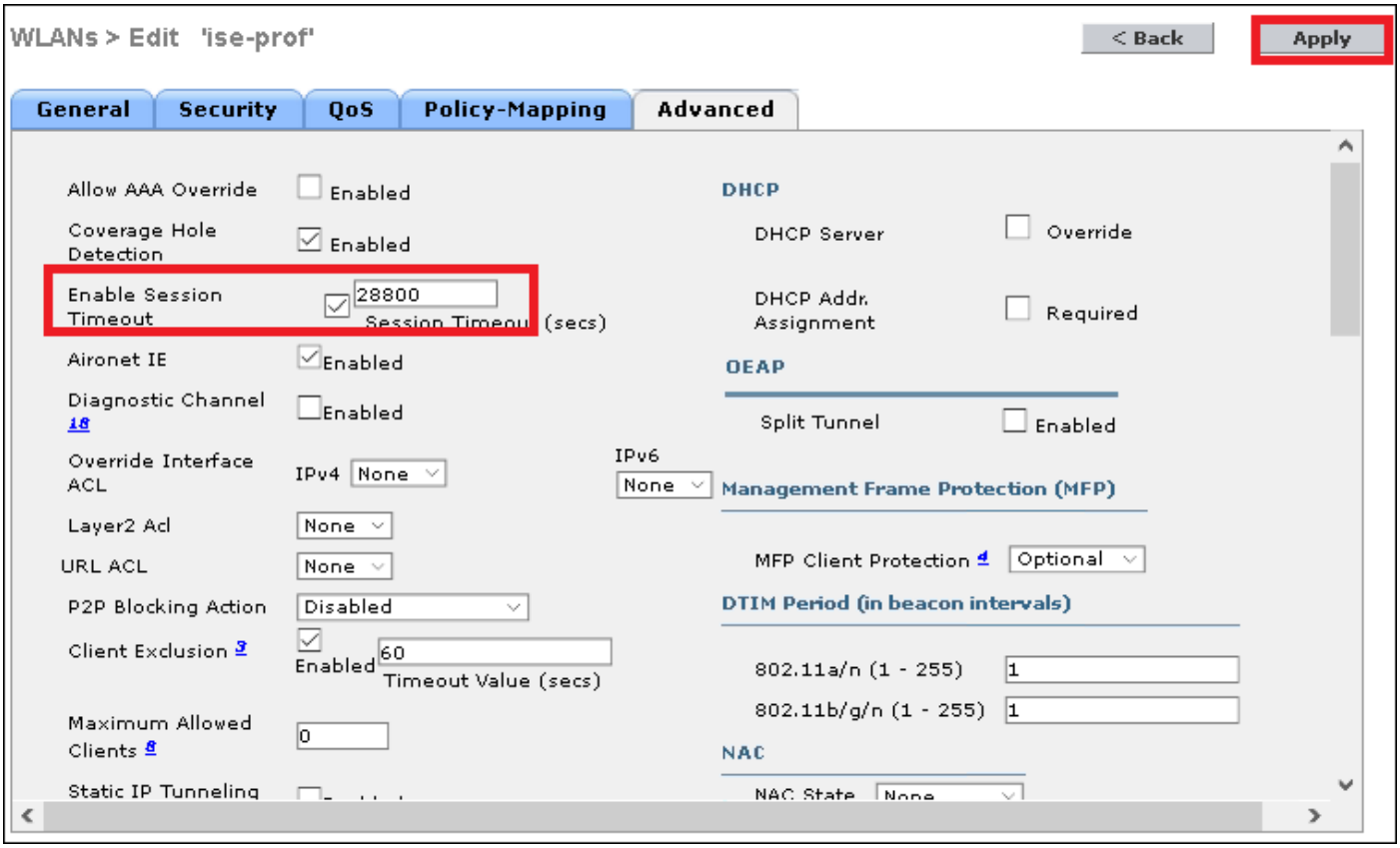


Étape 4. Augmentez sur option le délai d'attente de session

CLI :

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

GUI :

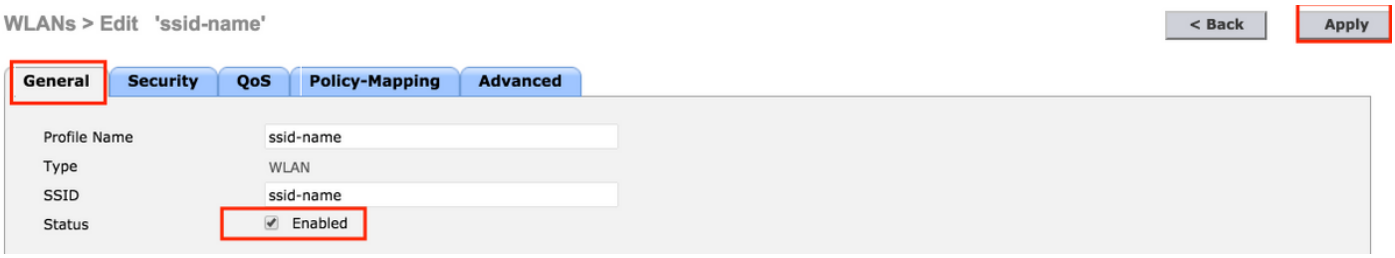


Étape 5. Activez le WLAN

CLI :

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

GUI :



Ajoutez les utilisateurs à la base de données de freeRADIUS

Par les clients par défaut utilisez les protocoles PEAP, toutefois support de freeRadius d'autres méthodes (non couvertes de ce guide).

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

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

Étape 2. Au bas du fichier ajoutez les informations d'utilisateurs. Dans cet exemple *user1* est le nom d'utilisateur et le *Cisco123 le* mot de passe.

```
user1         Cleartext-Password := "Cisco123"
```

Étape 3. Reprise FreeRadius.

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

Certificats sur le freeRADIUS

FreeRADIUS est livré avec un certificat du par défaut CA (certification Authoritiy) et un certificat de périphérique qui sont enregistrés dans le chemin */etc/raddb/certs.* Le nom de ces Certificats sont *ca.pem et* server.pem *server.pemis le certificat* que les clients recevront tandis qu'ils passent par la procédure d'authentification. Si vous devez assigner un certificat différent pour l'authentification EAP vous pouvez simplement les supprimer et sauvegarder les neufs dans le même chemin avec ce précis le même nom.

Configuration de périphérique d'extrémité

Configurez un ordinateur de Windows d'ordinateur portable pour se connecter à un SSID avec l'authentification de 802.1x et la version 2 PEAP/MS-CHAP (version de Microsoft de l'authentification Protocol à échanges confirmés).

Pour créer le profil WLAN sur l'ordinateur de fenêtres là soyez deux options :

1. Installez le certificat auto-signé sur l'ordinateur pour valider et faire confiance au serveur de freeRADIUS afin de se terminer l'authentification
2. Sautez la validation du serveur de RAYON et faites confiance à n'importe quel serveur de RAYON utilisé pour exécuter l'authentification (non recommandée, comme ce peut devenir un problème de sécurité). La configuration pour ces options sont expliquées sur la configuration de périphérique d'extrémité - créez le profil WLAN - étape xx.

Configuration de périphérique d'extrémité - Certificat de freeRADIUS d'importation

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

Étape 1. Obtenez le CERT de FreeRadius :

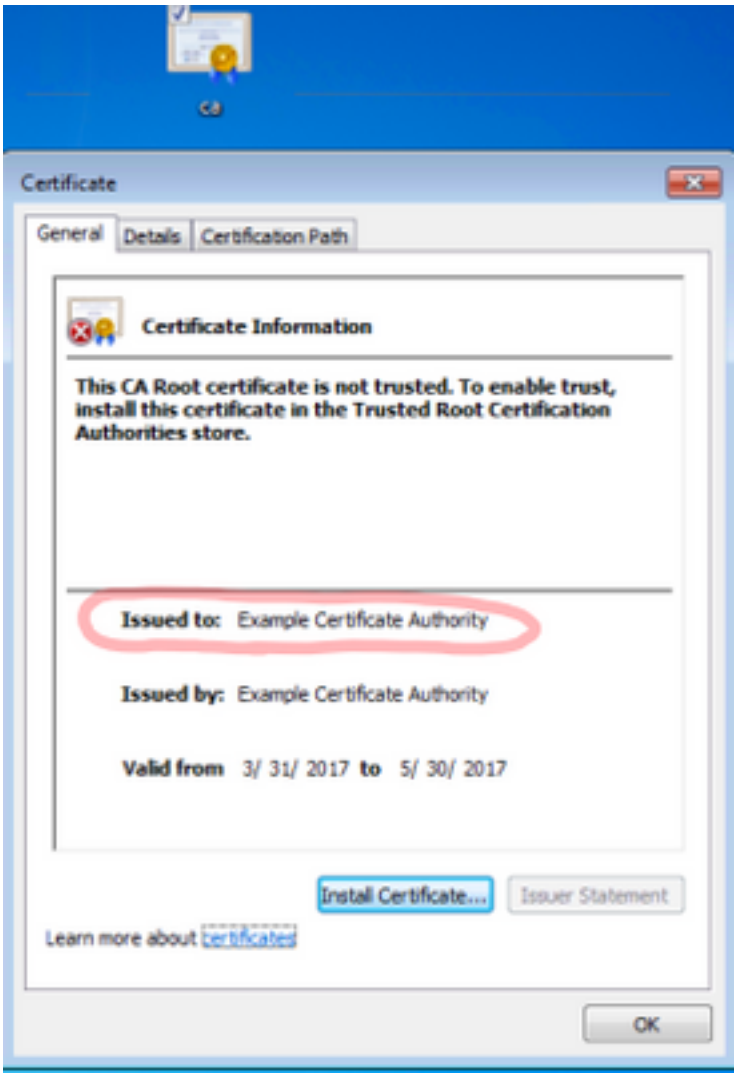
```
[root@tac-mxwireless ~]# cat /etc/raddb/certs/ca.pem

-----BEGIN CERTIFICATE-----
MIIE4TCCA8mgAwIBAgIJAKLmHn4eZLjBMA0GCSqGSIb3DQEBBQUAMIGTMQswCQYD
VQQGEwJGUjEPMA0GA1UECBMGUmFkaXVzMRIwEAYDVQQHEwlTb21ld2hlcmUxFTAT
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
```

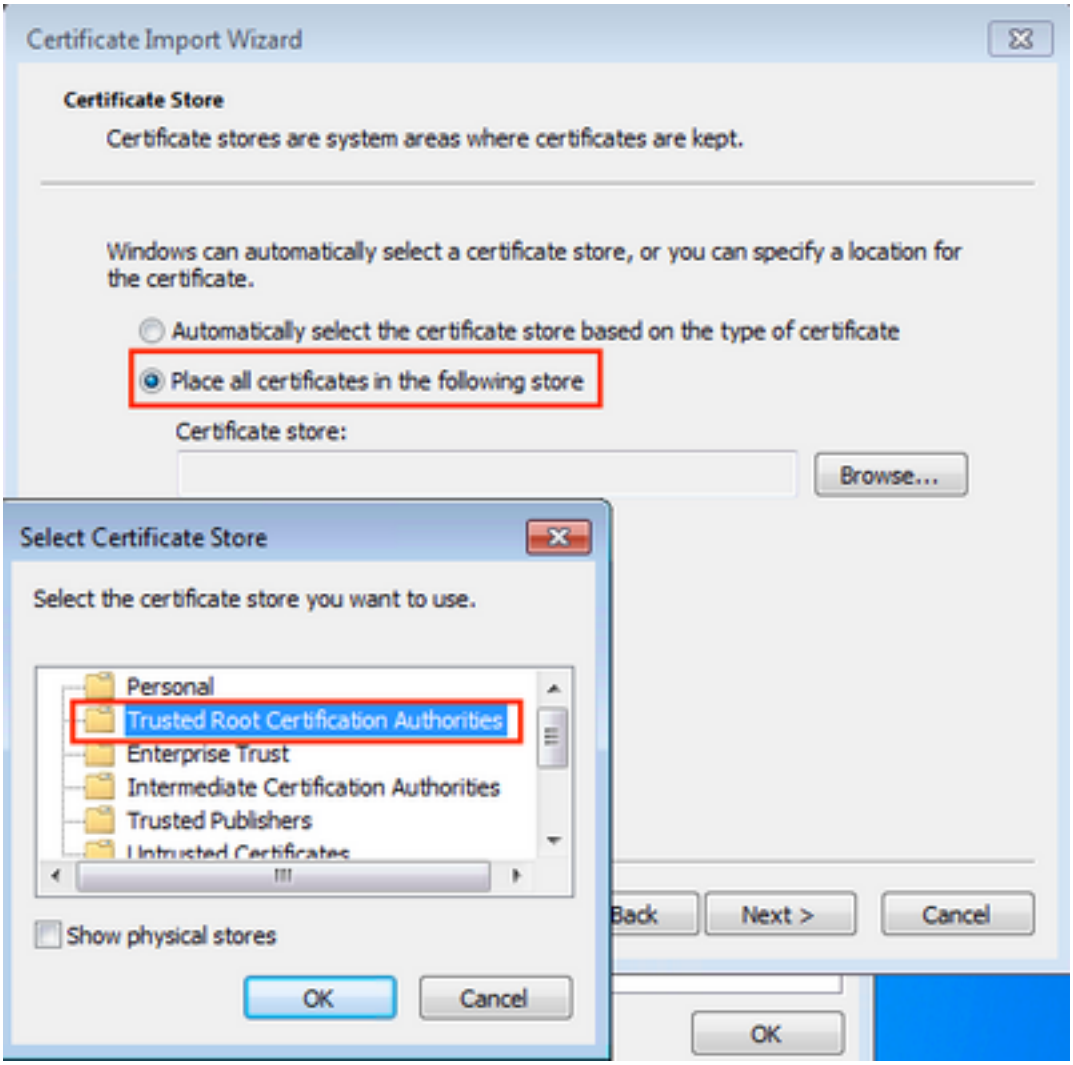
```
b20vZXhhbXBsZV9jYS5jcmwwDQYJKoZIhvcNAQEFBQADggEBACsPR2jiOFXnTsK4
1wnrrMylZZb12gDuqK+zKELox2mzlDMMK83tBsL8yjkv70KeZn821IzfTrTfvhzV
mjX6HgaWfYyMjYYYSw/iEu2JsAtQdpvC3di10nGwVPHlzbozPdov8cZtCb21ynfY
Z6cNjx8+aYQIcsRIyqA1IXMOBwIXo141TOmoODdgfX95lpoLwgktRLkvl7Y7owsz
ChYDO++H7Iewsxx5pQfm56dA2cNrlTwWtMvViKyX7GlpwlbBOxgkLiFJ5+GFbfLh
a0HBHZWhTKvffbr62mkbfjCUfJU4T3xgY9zFwiwT+BetCJgAGy8CT/qmnO+NJERO
RUvDhfE=
-----END CERTIFICATE-----
```

Étape 2. Copiez et collez la sortie de l'étape précédente dans un fichier texte et changez l'extension à .crt

Étape 3. Double-cliquer le fichier et choisi **installez le certificat…**

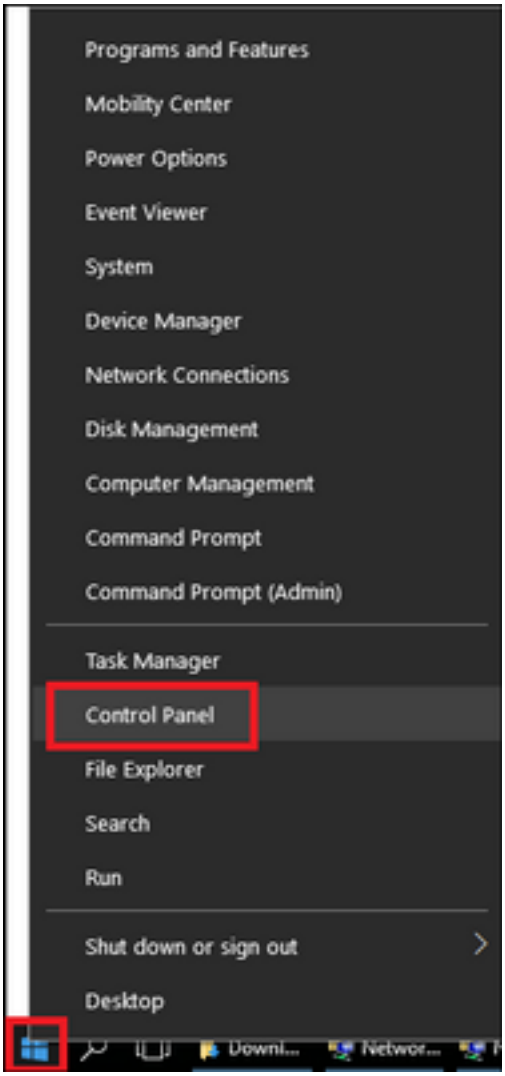


Étape 4. Installez le certificat dans la mémoire d'**Autorités de certification racine approuvée**.

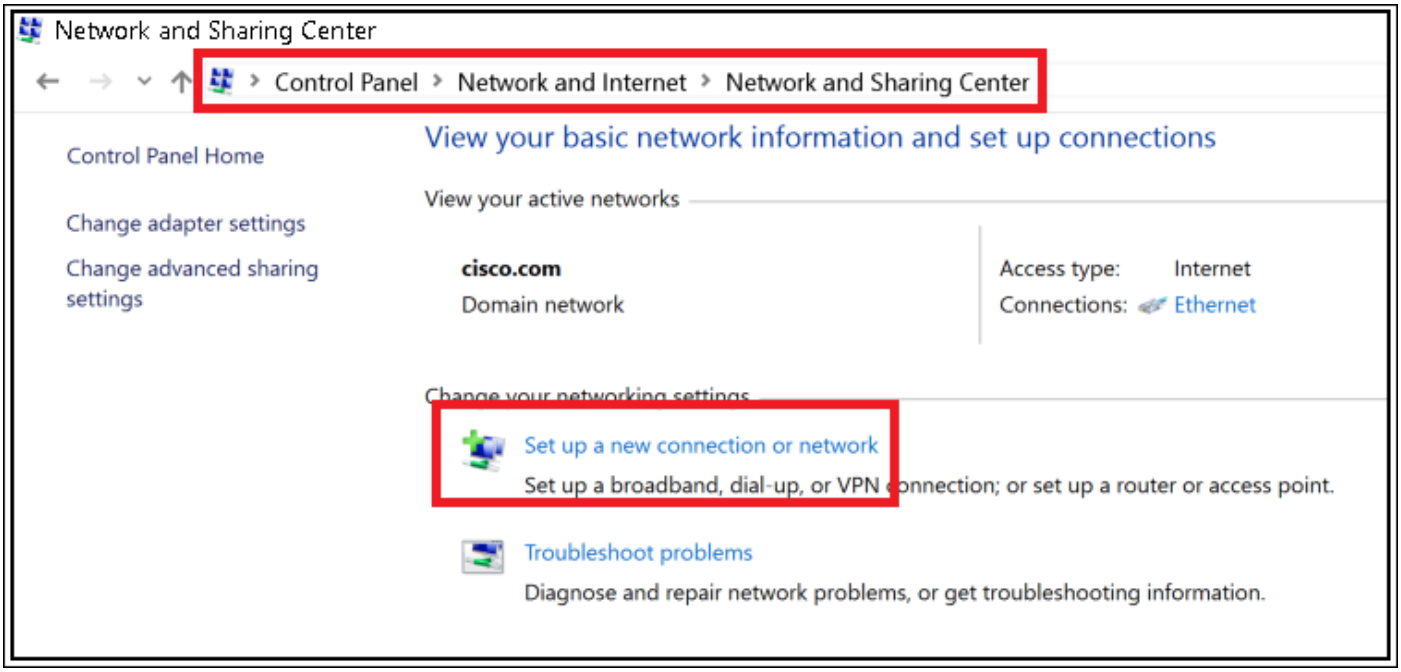


Configuration de périphérique d'extrémité - Créez le profil WLAN

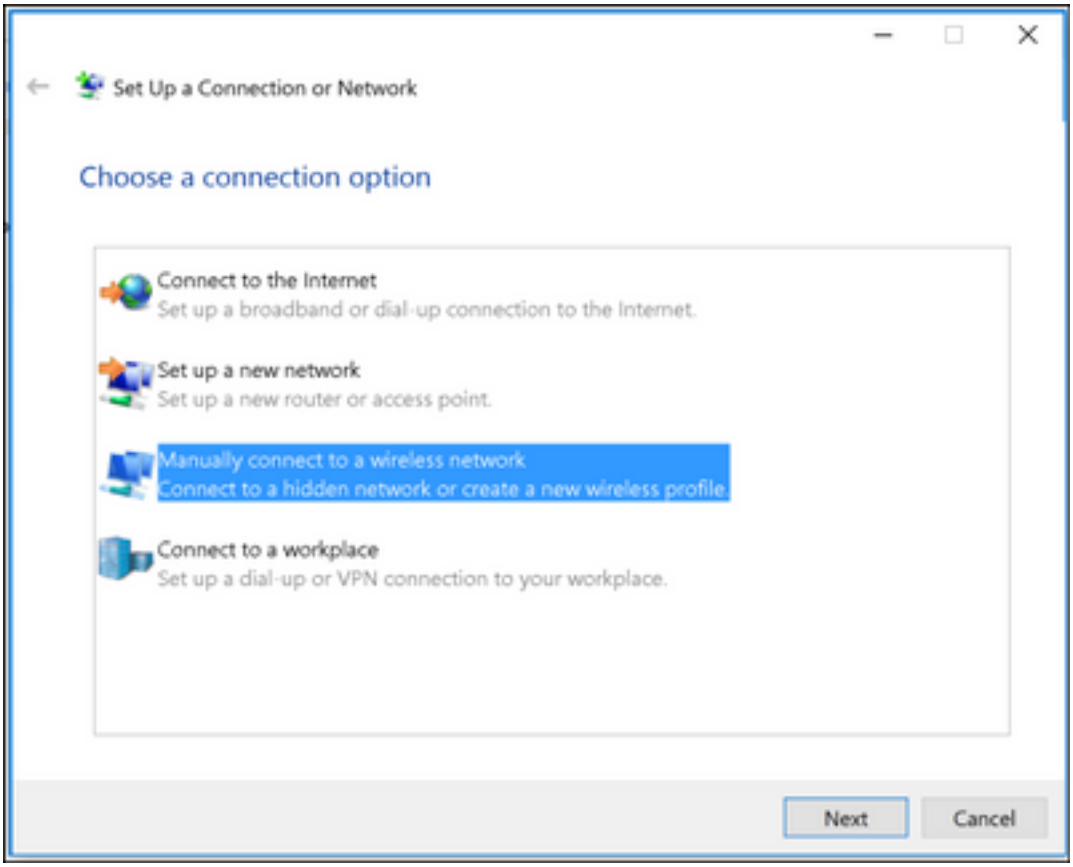
Étape 1. Clic droit sur l'icône de début et le **panneau de configuration** choisi.



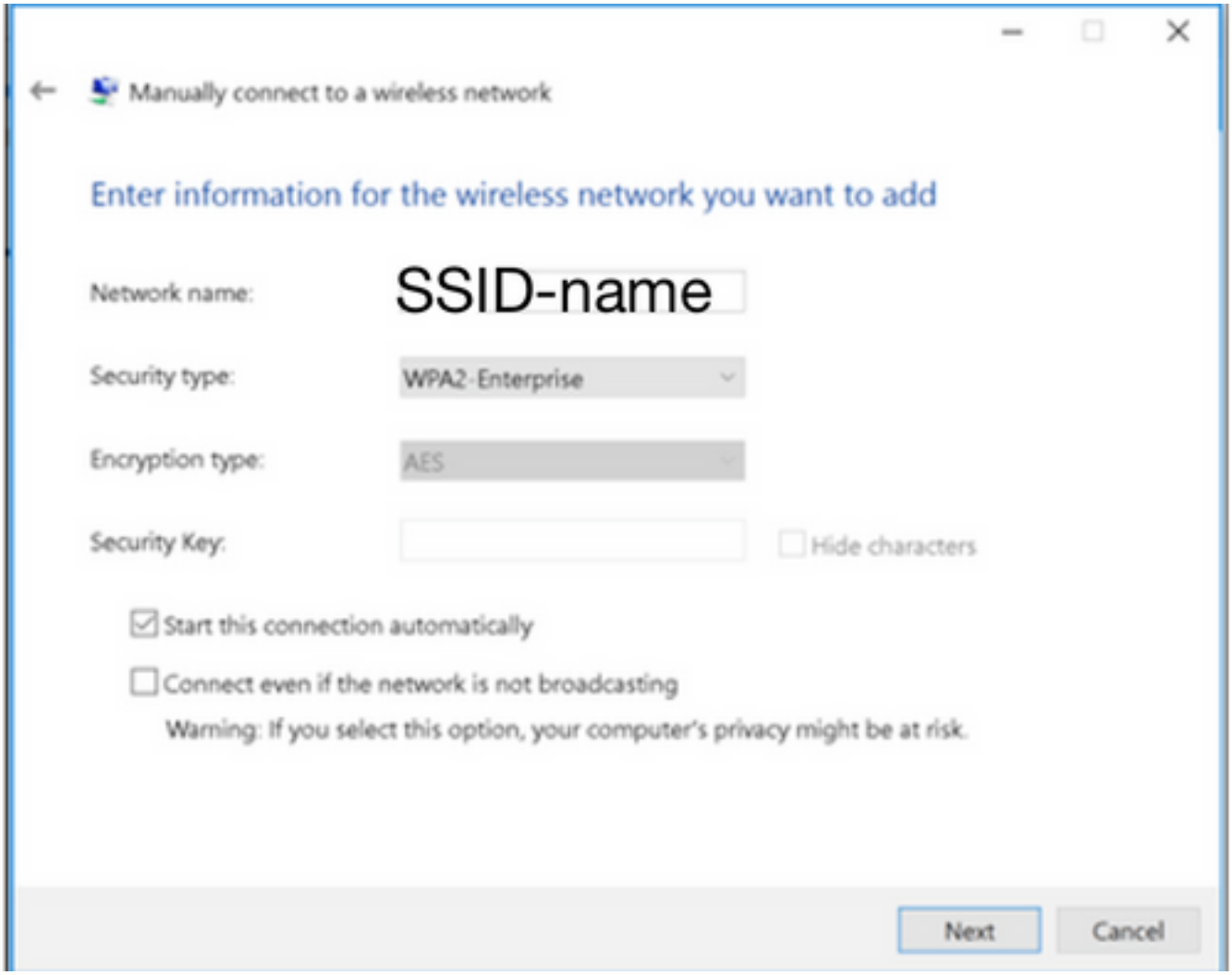
Étape 2. Naviguez vers le **réseau et l'Internet**, ensuite cela naviguent vers le **réseau et partager centraux** et cliquent sur **a en fonction installé une nouvelle connexion ou réseau.**



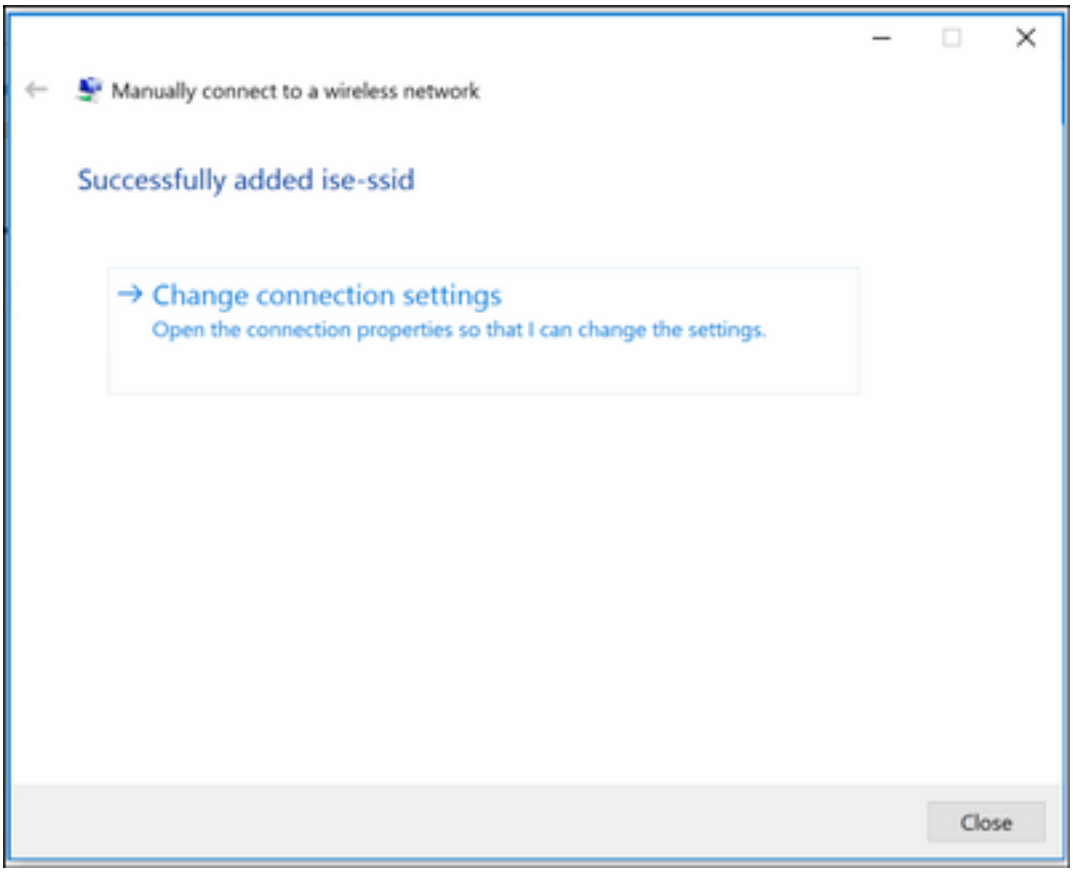
Étape 3. Sélectionnez **se connectent manuellement à un réseau Sans fil** et cliquent sur Next.



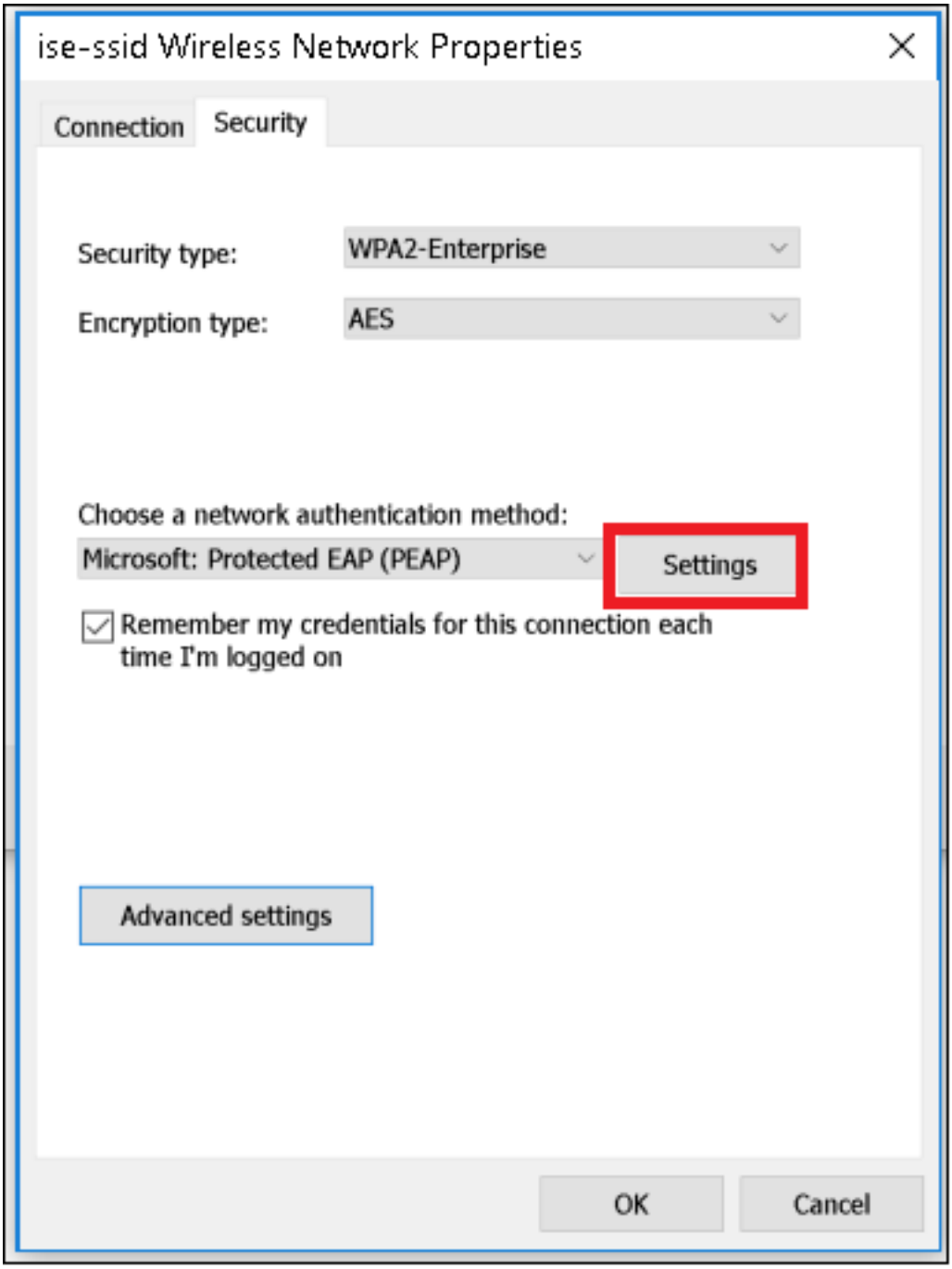
Étape 4. Écrivez les informations avec le nom du WPA2 Enterprise de type SSID et de Sécurité et cliquez sur Next.



Étape 5. Sélectionnez les **paramètres de connexion de modification** afin de personnaliser la configuration du profil WLAN.



Étape 6. Naviguez vers l'**onglet Sécurité** et cliquez sur les **configurations.**



Étape 7. Choisissez si le serveur de RAYON est validé ou pas.

Si oui, l'enable **vérifient l'identité du serveur en validant le certificat** et des **Autorités de certification racine approuvée :** la liste sélectionnent le certificat auto-signé du freeRADIUS.

Ensuite ce choisi **configure** et désactive **automatiquement l'utilisation mon nom de connexion et mot de passe de Windows…**, puis clique sur OK