Configure 802.1x - PEAP with FreeRadius and WLC 8.3

Contents

Introduction

This documents explains how to set up a WLAN (Wireless Local Area Network) with 802.1x security and PEAP (Protected Extensible Authentication Protocol) as EAP (Extensible Authentication Protocol). FreeRADIUS is used as the external Remote Authentication Dial-In User Service (RADIUS) server.

Prerequisites

Cisco recommends that you have basic knowledge of Linux, Vim editor and AireOS Wireless LAN Controllers (WLCs).

> **Note**: This document is intended to give the readers an example on the configuration required on a freeRADIUS server for PEAP-MS-CHAPv2 authentication. The freeRADIUS server configuration presented in this document has been tested in the lab and found to work as expected. The Cisco Technical Assistance Center (TAC) does not support freeRADIUS server configuration.

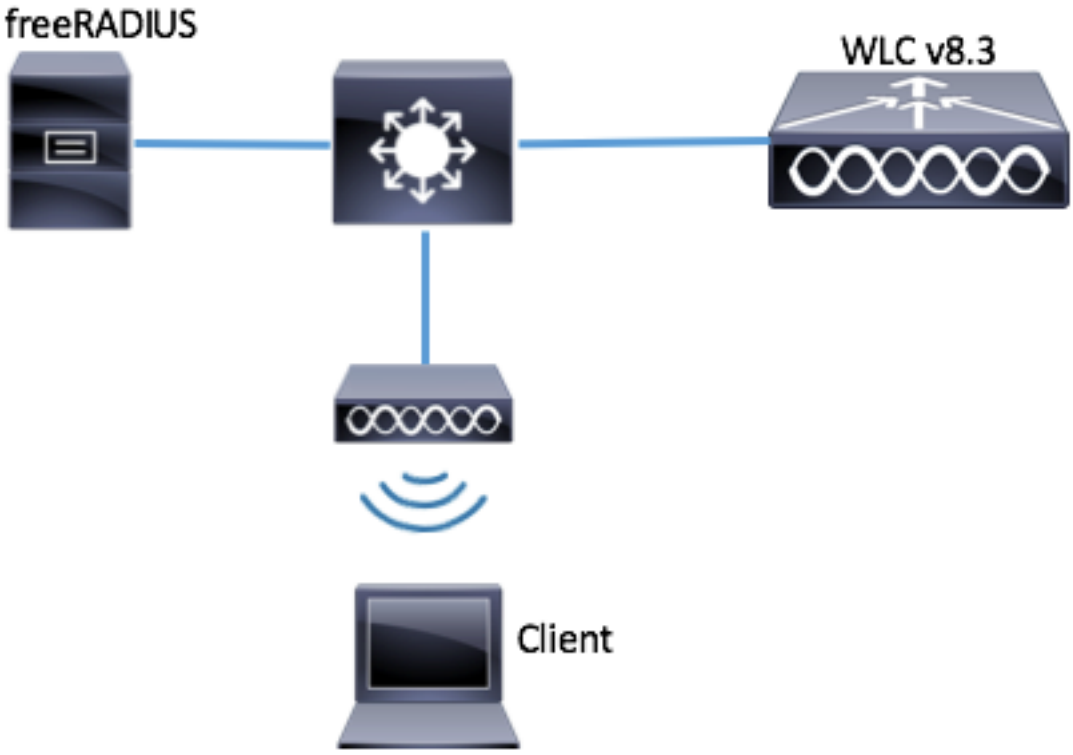
Components Used

- CentOS7 or Red Hat Enterprise Linux 7 (RHEL7) (Recommended 1 GB RAM and at least 20 GB HDD)
- 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.

Network Diagram



Configuration

Install httpd Server and MariaDB

Step 1. Run these commands to install httpd server and 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
```

Step 2. Start and enable httpd (Apache) and MariaDB server.

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

Step 3. Configure initial MariaDB settings to secure it.

```
[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!
```

Step 4. Configure Database for freeRADIUS (use same password configured in Step 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
```

Install PHP 7 on CentOS 7

Step 1. Run these commands to install PHP 7 on 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
```

Install FreeRADIUS

Step 1. Run this command to install FreeRADIUS.

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

Step 2. Make *radius.service*start after *mariadb.service.*

Run this command:

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

Add a line in **`[Unit]`** section**:**

```
After=mariadb.service
```

[Unit] section must look like this:

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

Step 3. Start and enable freeradius to start at boot up.

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

Step 4. Enable firewalld for security.

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

Step 5. Add permanent rules to default zone to allow http,https and radius services.

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

Step 6. Reload firewalld for changes to take effect.

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

Configure FreeRADIUS

In order to configure FreeRADIUS to use MariaDB, follow these steps.

Step 1. Import the RADIUSdatabase scheme to populate RADIUS database.

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

Step 2. Create a soft link for SQL under */etc/raddb/mods-enabled*

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

Step 3. Configure SQL module */raddb/mods-available/sql* and change the database connection parameters to suite your environment.

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

SQL section must look similar to below.

```
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”
```

Step 4. Change group right of */etc/raddb/mods-enabled/sql* to radiusd.

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

Configure WLC as AAA client on FreeRADIUS

Step 1. Edit */etc/raddb/clients.conf* in order to set shared key for WLC.

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

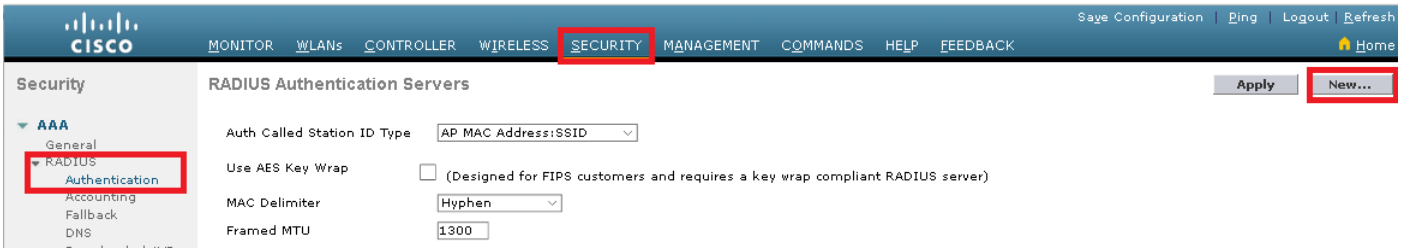
Step 2. At the bottom add your controller ip address and the shared key.

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

Configure FreeRADIUS as RADIUS server on WLC

GUI:

Step 1. Open the GUI of the WLC and navigate to **SECURITY > RADIUS > Authentication > New.**



Step 2. Fill the RADIUS server information.

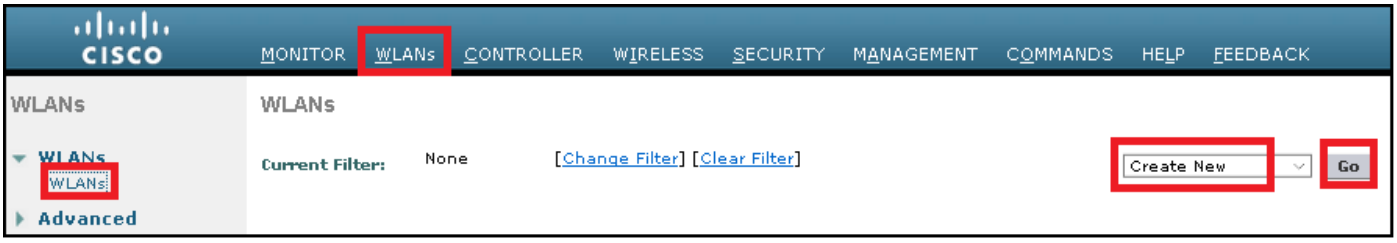
CLI:

```
> 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>
```

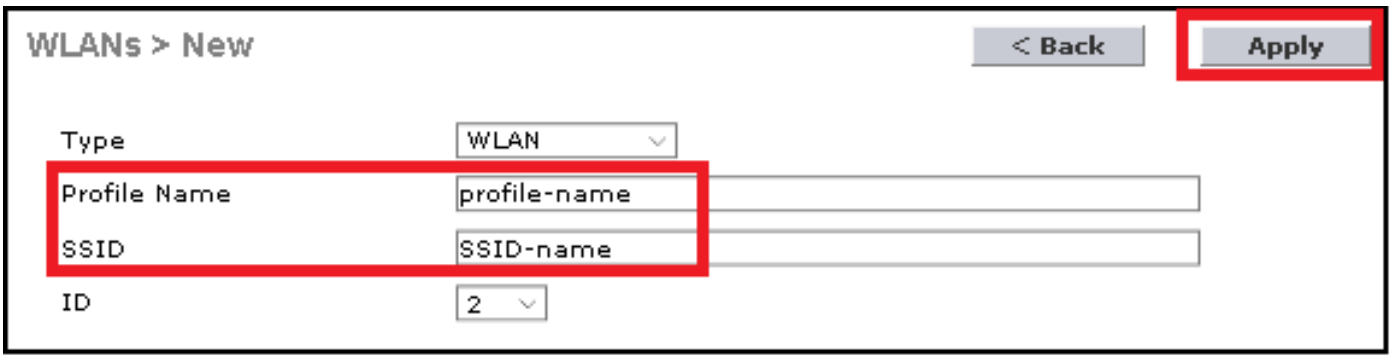
Configure a WLAN

GUI:

Step 1. Open the GUI of the WLC and navigate to **WLANs > Create New > Go.**



Step 2. Choose a name for the SSID and profile, then click **Apply.**



CLI:

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

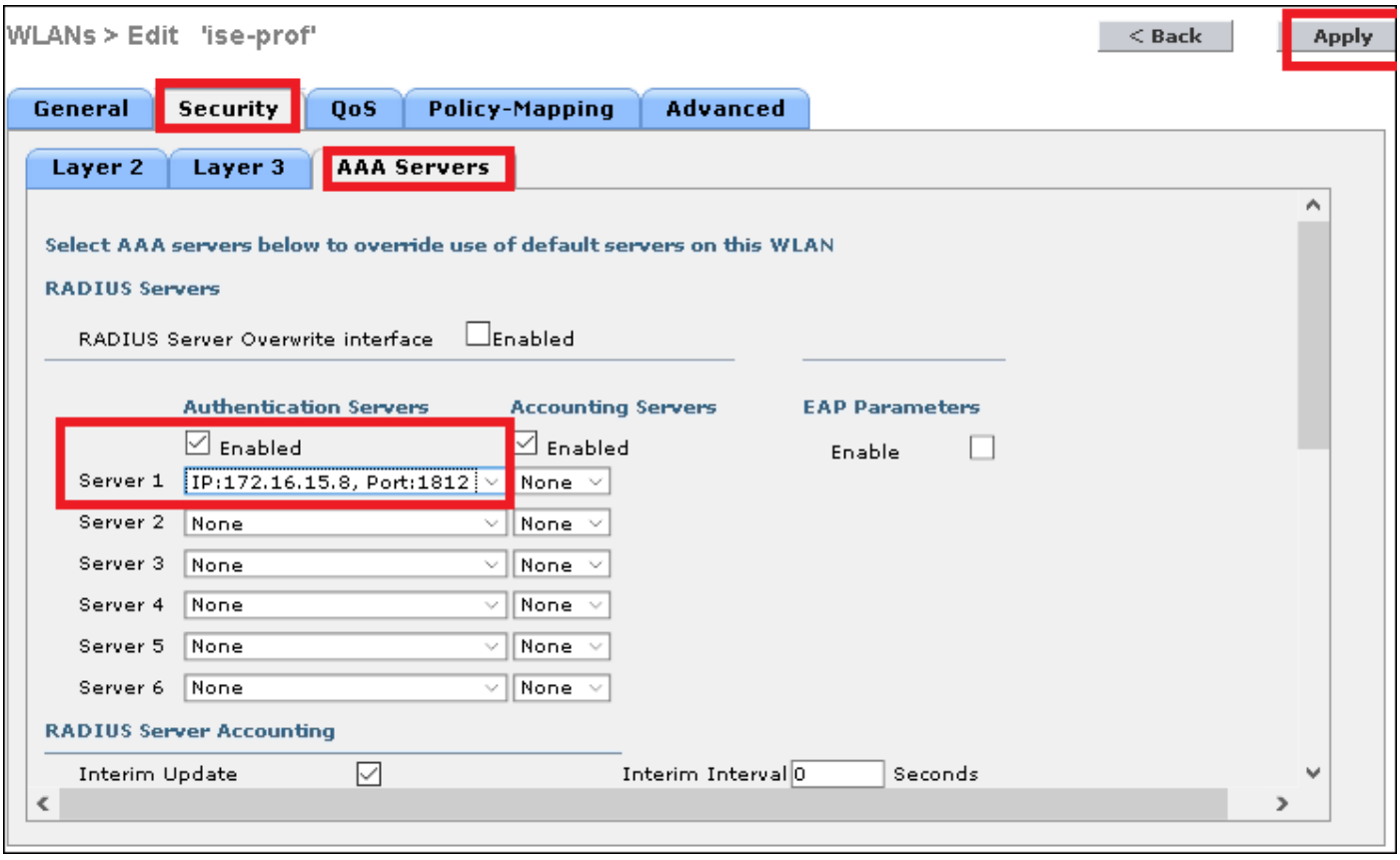
Step 3. Assign the RADIUS server to the WLAN.

CLI:

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

GUI:

Navigate to **Security > AAA Servers** and choose the desired RADIUS server, then hit **Apply.**

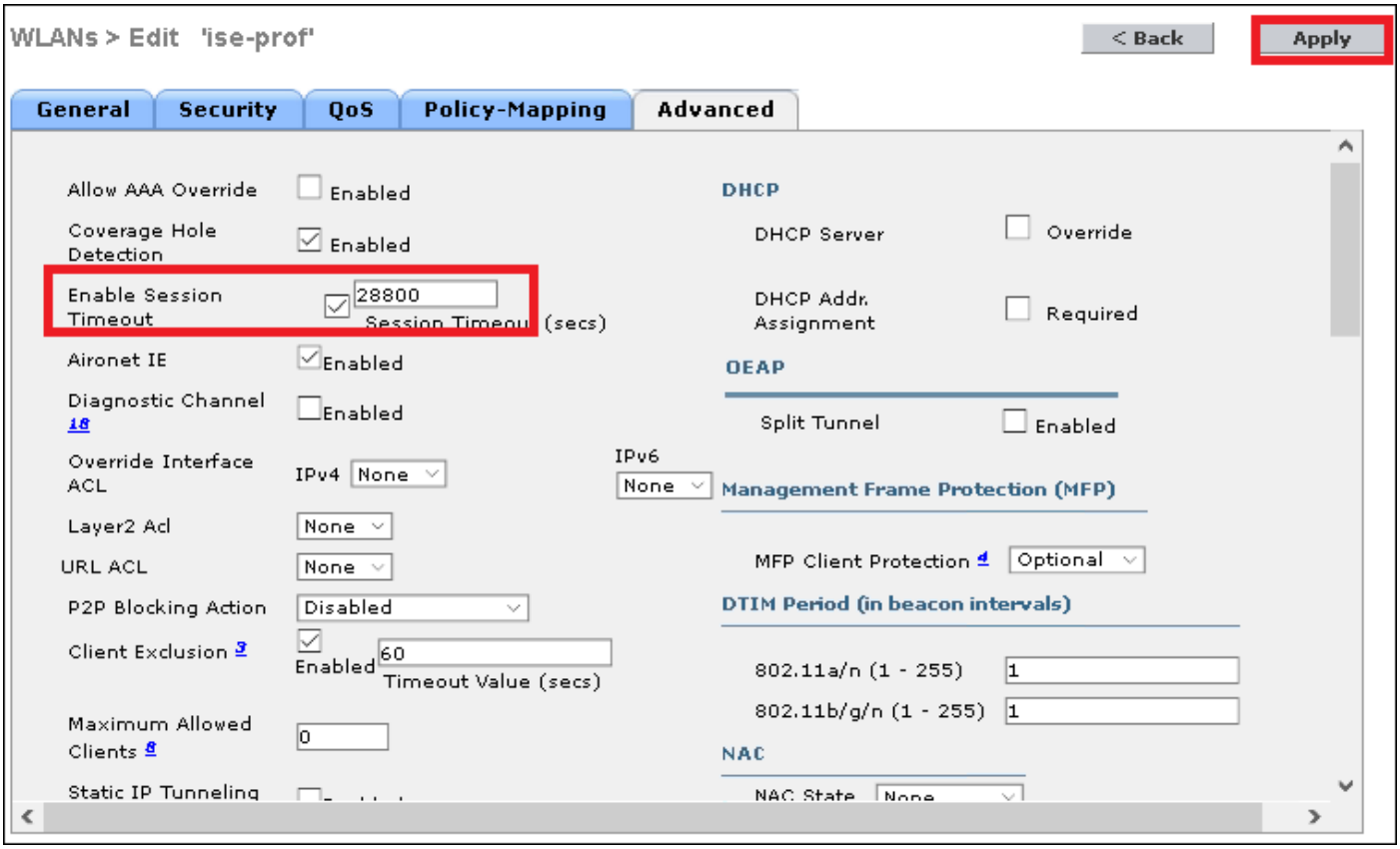


Step 4. Optionally increase the session timeout

CLI:

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

GUI:

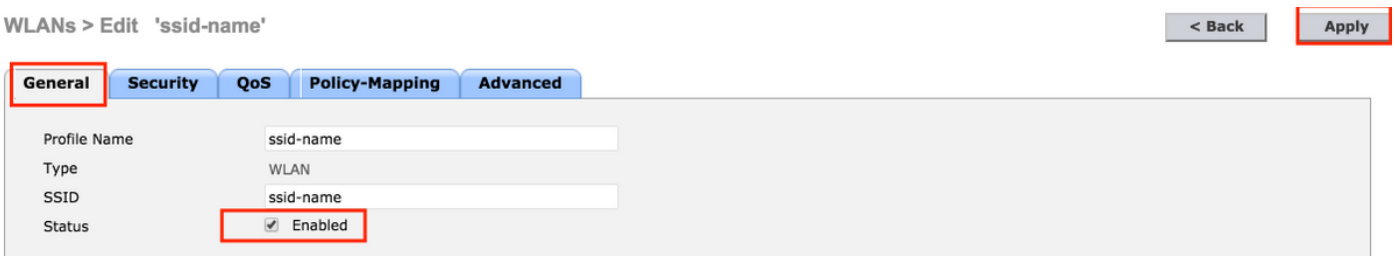


Step 5. Enable the WLAN

CLI:

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

GUI:



Add users to freeRADIUS database

By default clients use PEAP protocols, however freeRadius support other methods (not covered in this guide).

Step 1. Edit the file */etc/raddb/users*.

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

Step 2. At the bottom of the file append the users information. In this example *user1* is the username and *Cisco123* the password.

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

Step 3. Restart FreeRadius.

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

Certificates on freeRADIUS

FreeRADIUS comes with a default CA (Certification Authoritiy) certificate and a device certificate which are stored in the path */etc/raddb/certs.* The name of these certificates are *ca.pem* and *server.pem*. *server.pem* is the certificate that clients will receive while they go through the authentication process. If you need to assign a different certificate for EAP authentication you can simply delete them and save the new ones in the same path with that exact same name.

End device configuration

Configure a laptop Windows machine to connect to an SSID with 802.1x Authentication and PEAP/MS-CHAP (Microsoft version of the Challenge-Handshake Authentication Protocol) version 2.

To create the WLAN profile on the windows machine there are two options:

1. Install the self-signed certificate on the machine to validate and trust freeRADIUS server in order to complete the authentication
2. Bypass the validation of the RADIUS server and trust any RADIUS server used to perform the authentication (not recommended, as it can become a security issue). The configuration for these options are explained on End device configuration - Create the WLAN Profile - Step xx.

End device configuration - Import freeRADIUS certificate

If you use the default certificates installed on freeRADIUS, follow these steps in order to import the EAP certificate from the freeRADIUS server into the end device.

Step 1. Get the cert from FreeRadius:

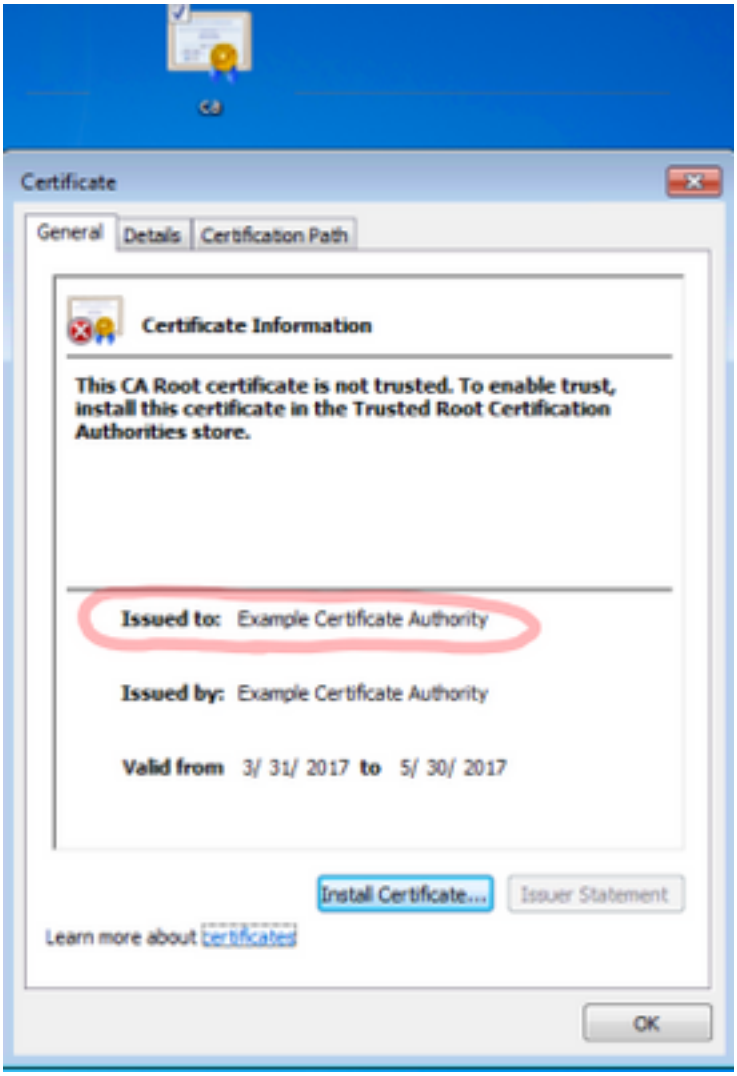
```
[root@tac-mxwireless ~]# cat /etc/raddb/certs/ca.pem

-----BEGIN CERTIFICATE-----
MIIE4TCCA8mgAwIBAgIJAKLmHn4eZLjBMA0GCSqGSIb3DQEBBQUAMIGTMQswCQYD
VQQGEwJGUjEPMA0GA1UECBMGUmFkaXVzMRIwEAYDVQQHEwlTb21ld2hlcmUxFTAT
BgNVBAoTDEV4YW1wbGUgSW5jLjEgMB4GCSqGSIb3DQEJARYRYWRtaW5AZXhhbXBs
ZS5jb20xJjAkBgNVBAMTHUV4YW1wbGUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4X
DTE3MDMzMTExMTIxNloXDTE3MDUzMDExMTIxNlowgZMxCzAJBgNVBAYTAkZSMQ8w
DQYDVQQIEwZSYWRpdXMxEjAQBgNVBAcTCVNvbWV3aGVyZTEVMBMGA1UEChMMRXhh
bXBsZSBJbmMuMSAwHgYJKoZIhvcNAQkBFhFhZG1pbkBleGFtcGxlLmNvbTEmMCQG
A1UEAxMdRXhhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQC0vJ53NN7J9vhpKhcB3B0OXLpeQFWjqolQOB9F
/8Lh2Hax2rzb9wxOi1MOyXR+kN22H7RNwUHET8VdyGUsA4OdZWuyzI8sKi5H42GU
Eu6GDw1YJvhHn4rVC36OZU/Nbaxj0eR8ZG0JGse4ftQKLfckkvCOS5QGn4X1elRS
```

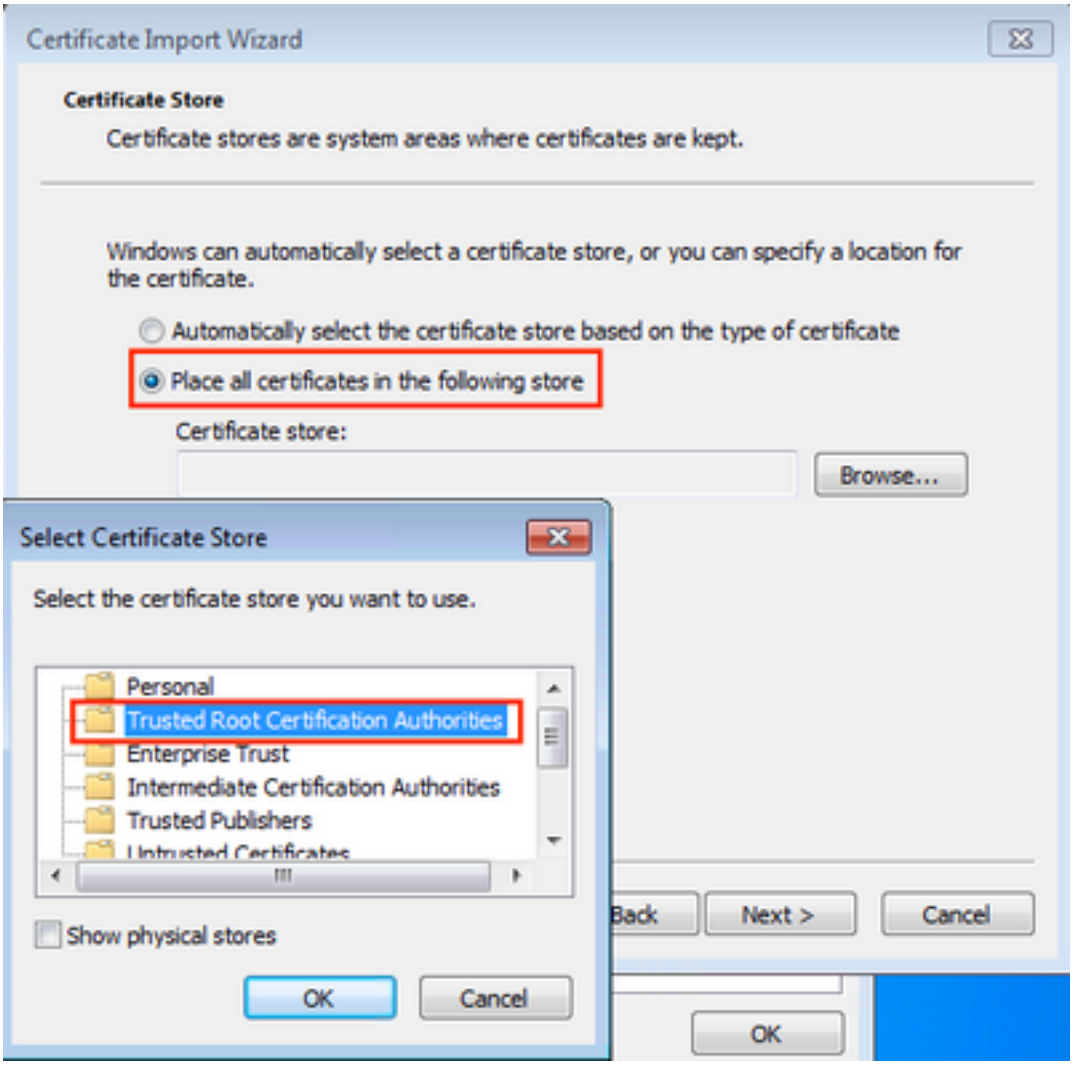
```
oFe27HRF+pTDHd+nzbaDvhYWvFoe6iA27Od7AY/sDuo/tiIJWGdm9ocPz3+0IiFC
ay6dtG55YQOHxKaswH7/HJkLsKWhS4YmXLgJXCeeJqooqr+TEwyCDEaFaiX835Jp
gwNNZ7X5US0FcjuuOtpJJ3hfQ8K6uXjEWPOkDE0DAnqp4/n9AgMBAAGjggE0MIIB
MDAdBgNVHQ4EFgQUysFNRZKpAlcFCEgwdOPVGV0waLEwgcgGA1UdIwSBwDCBvYAU
ysFNRZKpAlcFCEgwdOPVGV0waLGhgZmkgZYwgZMxCzAJBgNVBAYTAkZSMQ8wDQYD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


Step 2. Copy and paste the output of the previous step into a text file and change extension to .crt

Step 3. Double click the file and select **Install Certificate...**

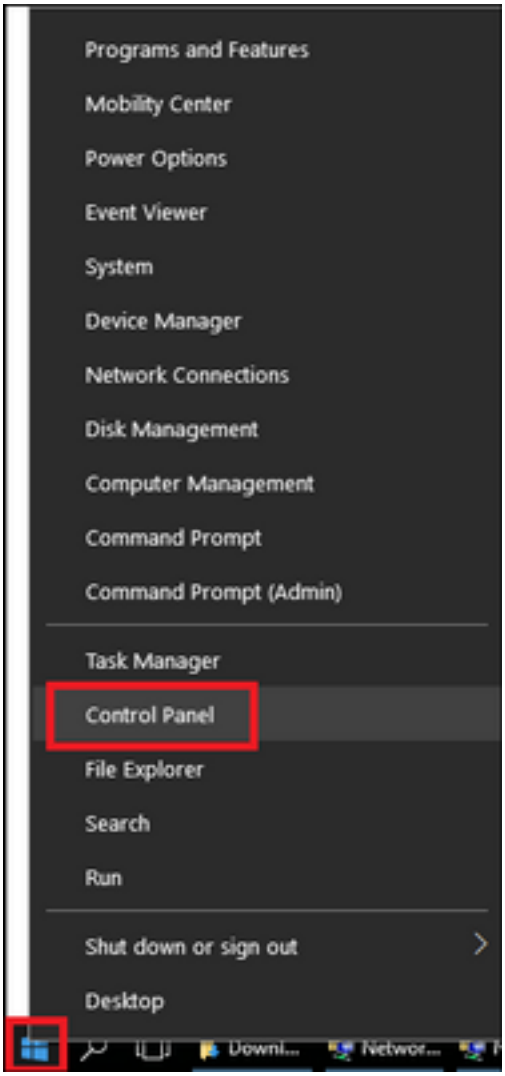


Step 4. Install the certificate into the **Trusted Root Certification Authorities** store.

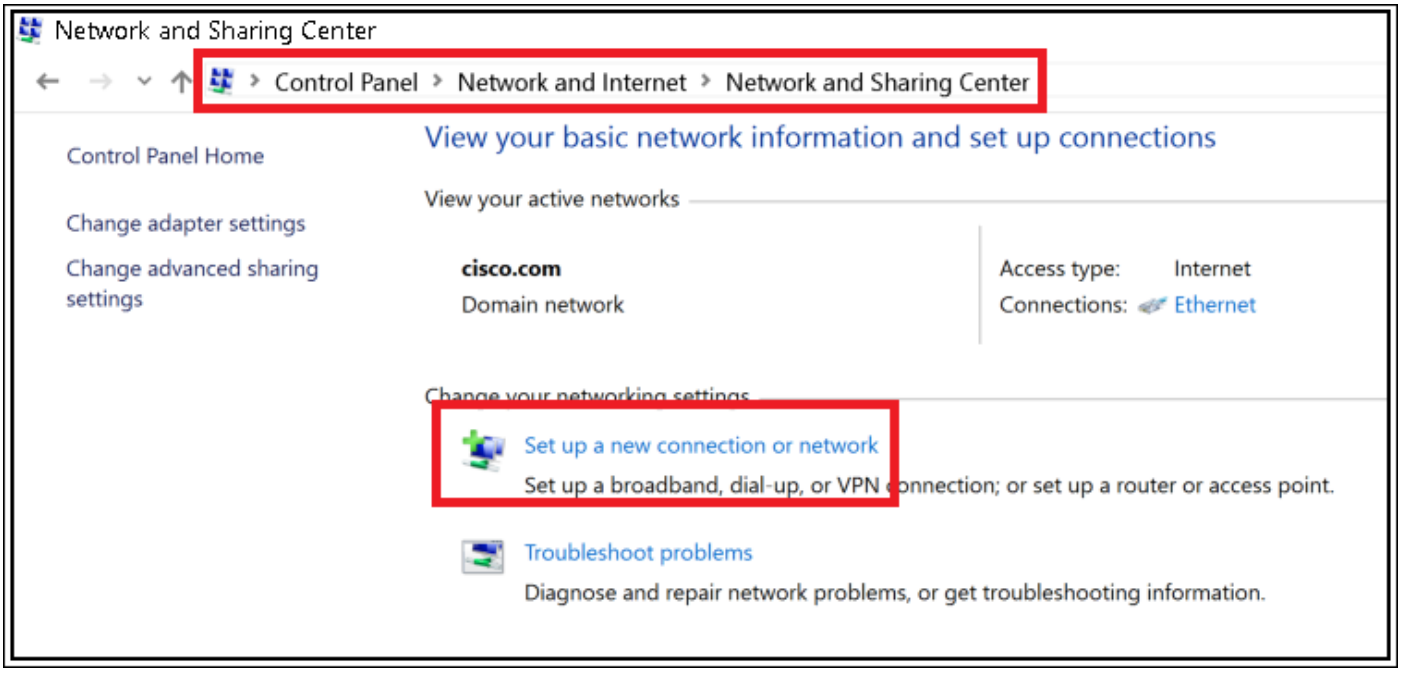


End device configuration - Create the WLAN Profile

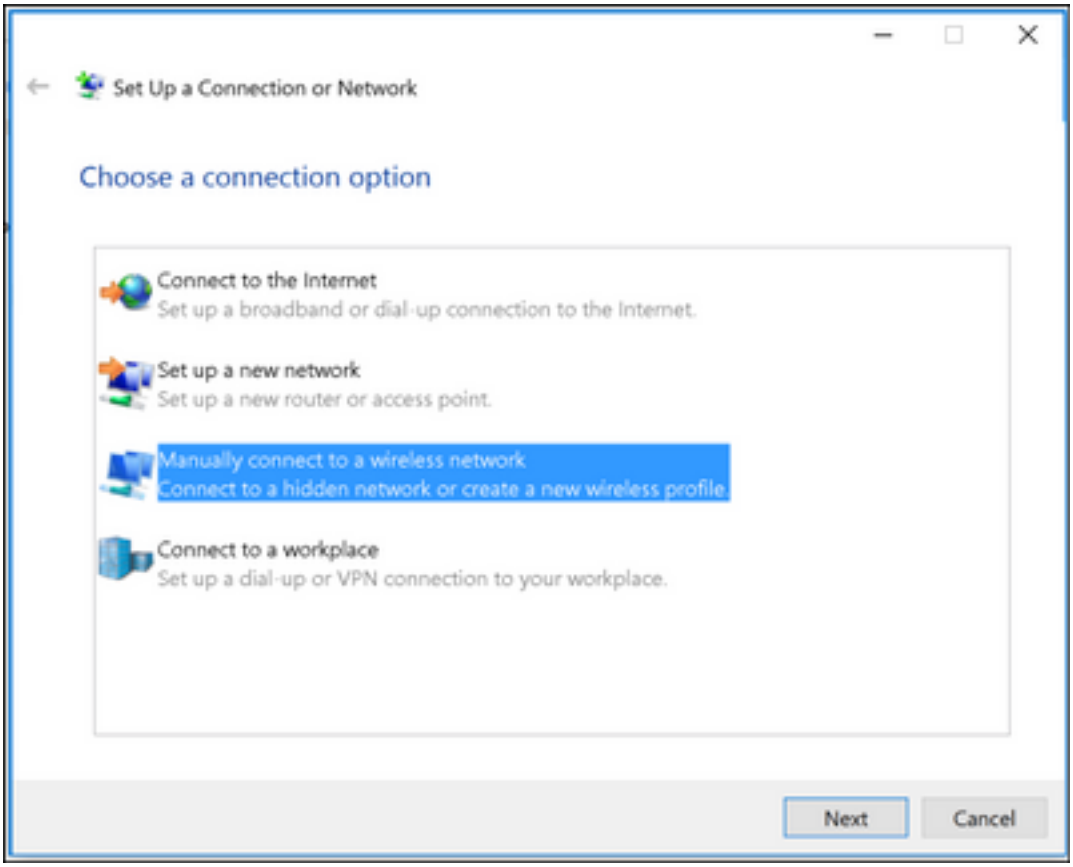
Step 1. Right click on Start icon and select **Control panel**.



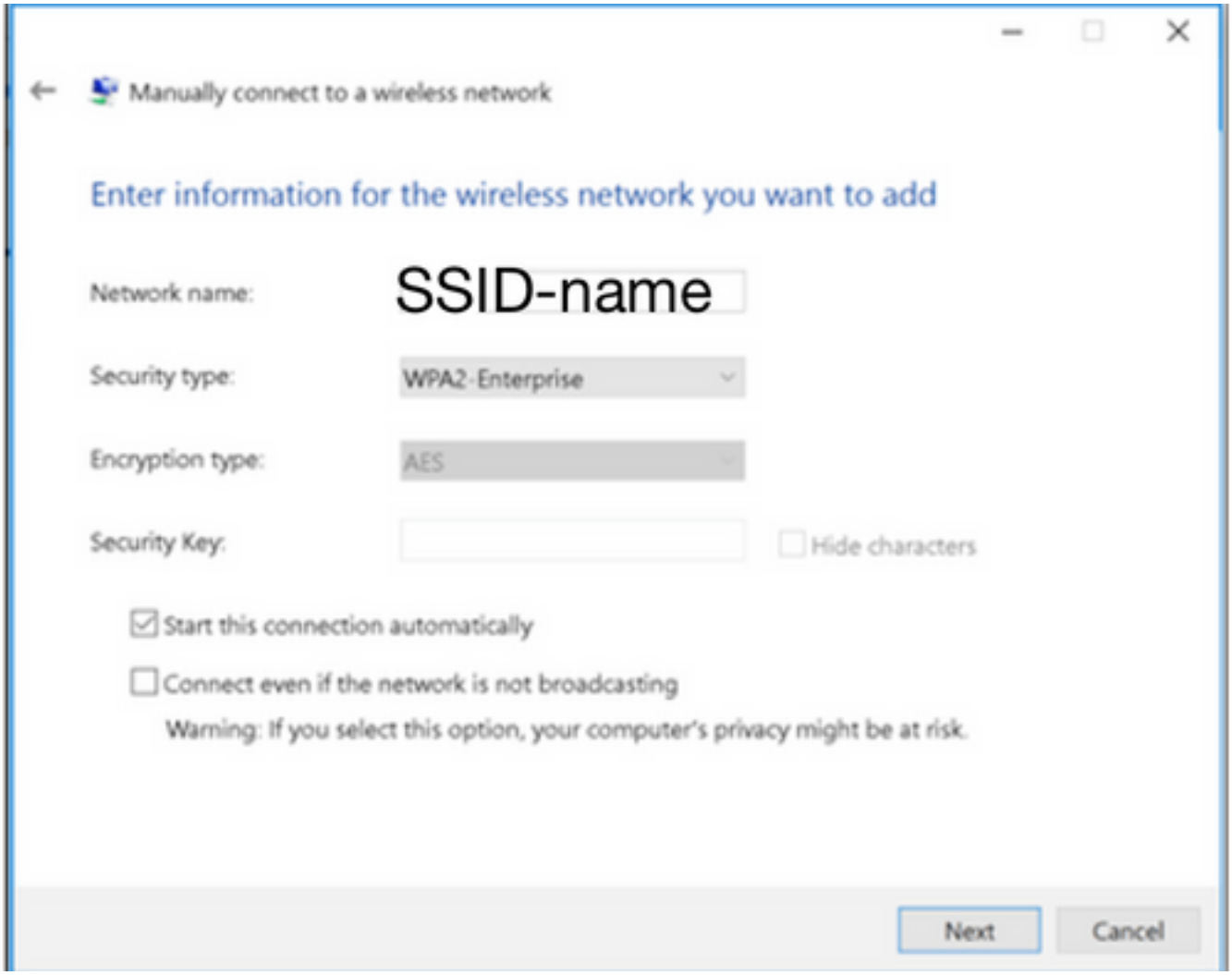
Step 2. Navigate to **Network and Internet**, after that navigate to **Network and Sharing Center** and click on **Set up a new connection or network.**



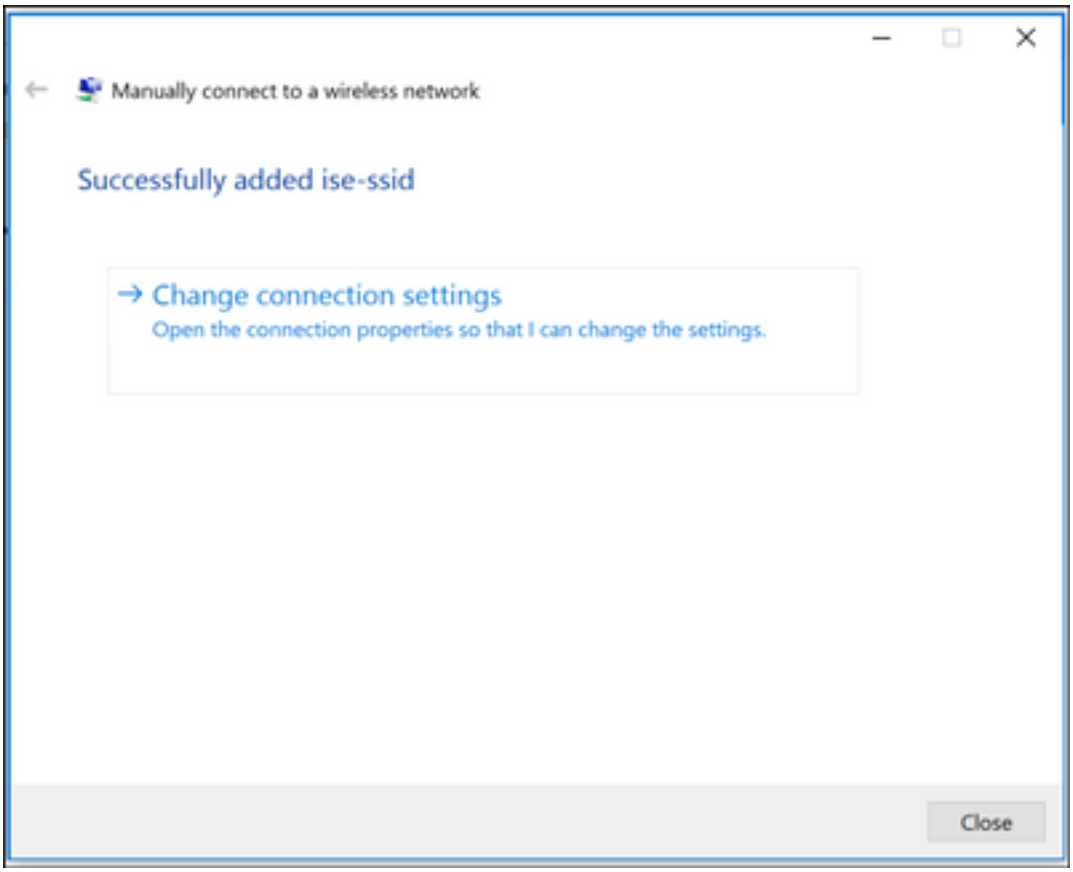
Step 3. Select **Manually connect to a wireless network** and click **Next.**



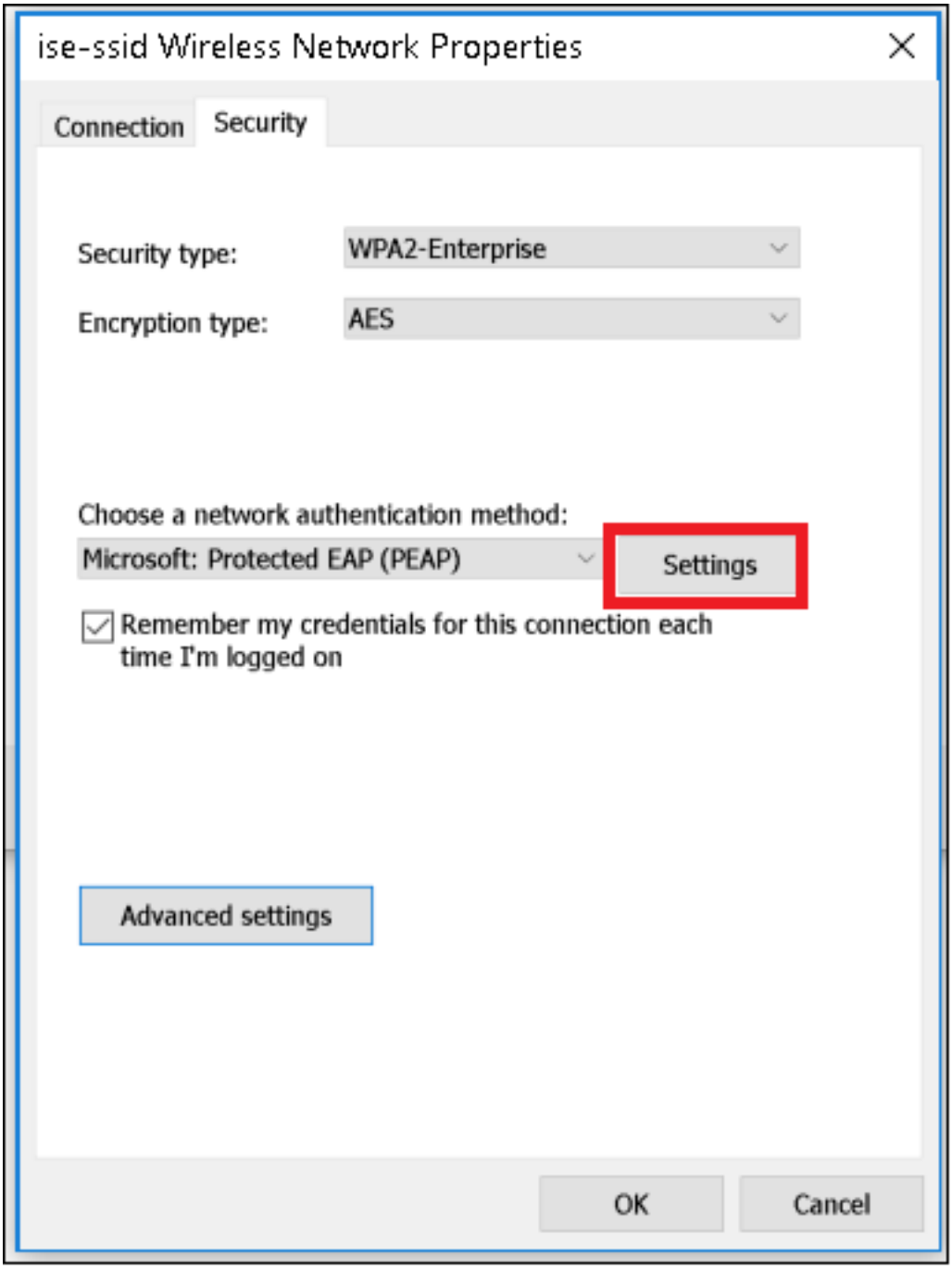
Step 4. Enter the information with the name of the SSID and security type WPA2-Enterprise and click **Next.**



Step 5. Select **Change connection settings** in order to customize the configuration of the WLAN profile.



Step 6. Navigate to **Security** tab and click **Settings.**



Step 7. Choose if RADIUS server is validated or not.

If yes, enable **Verify the server's identity by validating the certificate** and from **Trusted Root Certification Authorities:** list select the self-signed certificate of freeRADIUS.

After that select **Configure** and disable **Automatically use my Windows logon name and password...**, then click **OK**