Configure 802.1x - PEAP con FreeRadius y WLC 8.3

Contenido

Introducción

Este documento describe cómo configurar una red de área local inalámbrica (WLAN) con seguridad 802.1x y protocolo de autenticación extensible protegido (PEAP) como protocolo de autenticación extensible (EAP). FreeRADIUS se utiliza como servidor RADIUS (servicio de usuario de acceso telefónico de autenticación remota externa).

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos básicos sobre estos temas:

- Linux
- editor Vim
- Controladores LAN inalámbricos (WLC) AireOS

Nota: Este documento está diseñado para dar a los lectores un ejemplo sobre la configuración requerida en un servidor FreeRADIUS para la autenticación PEAP-MS-CHAPv2. La configuración del servidor freeRADIUS que se presenta en este documento se ha probado en el laboratorio y se ha encontrado que funciona según lo esperado. El centro de asistencia técnica Cisco Technical Assistance Center (TAC) no admite la configuración del servidor RADIUS libre.

Componentes Utilizados

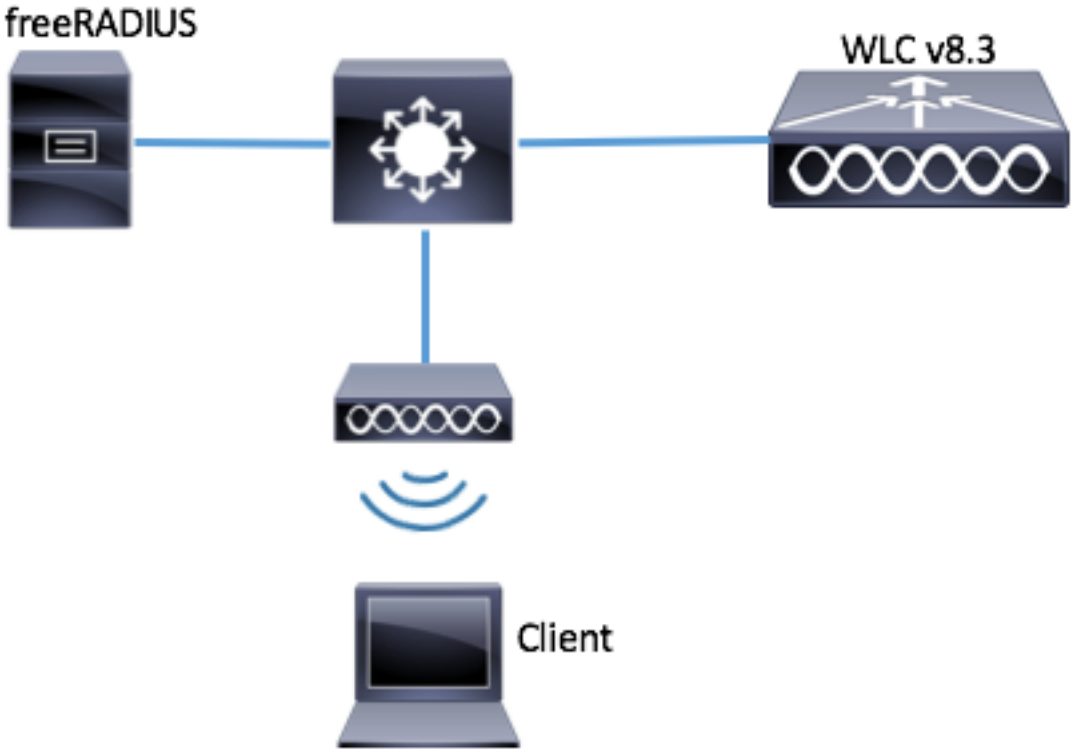
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- CentOS7 o Red Hat Enterprise Linux 7 (RHEL7) (RAM recomendada de 1 GB y HDD de al menos 20 GB)
- 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.

Configurar

Diagrama de la red



Instalar el servidor httpd y MariaDB

Paso 1. Ejecute estos comandos para instalar el servidor httpd y 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
```

Paso 2. Inicie y active httpd (Apache) y el servidor 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
```

Paso 3. Configure la configuración inicial de MariaDB para protegerla.

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

> **Nota:** Ejecute todas las partes de este script. Se recomienda para todos los servidores MariaDB en uso de producción. Lea atentamente cada paso.

```
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!
```

Paso 4. Configure la base de datos para freeRADIUS (utilice la misma contraseña configurada en el paso 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
```

Instalación de PHP 7 en CentOS 7

Paso 1. Ejecute estos comandos para instalar PHP 7 en 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
```

Instalar FreeRADIUS

Paso 1. Ejecute este comando para instalar FreeRADIUS.

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

Paso 2. Haga que **radius.service** comience después de **mariadb.service**.

Ejecute este comando:

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

Agregue una línea en la sección **[Unidad]:**

```
After=mariadb.service
```

La sección [Unit] debe tener el siguiente aspecto:

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

Paso 3. Inicie y active freeradius para que se inicie al arrancar.

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

Paso 4. Habilite el firewall para la seguridad.

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

Paso 5. Agregue reglas permanentes a la zona predeterminada para permitir los servicios http, https y radius.

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

Paso 6. Recarga el firewall para que los cambios surtan efecto.

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

FreeRADIUS

Para configurar FreeRADIUS para utilizar MariaDB, siga estos pasos.

Paso 1. Importe el esquema de base de datos RADIUS para rellenar la base de datos RADIUS.

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

Paso 2. Cree un enlace programable para lenguaje de consulta estructurado (SQL) en **/etc/raddb/mods-enabled**.

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

Paso 3. Configure el módulo SQL /raddb/mods-available/sql y cambie los parámetros de conexión de la base de datos para ajustar su entorno.

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

La sección SQL debe tener un aspecto similar a este.

```
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”
```

Paso 4. Cambie el derecho de grupo de **/etc/raddb/mods-enabled/sql** a radiusd.

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

WLC como Cliente de Autenticación, Autorización y Contabilización (AAA) en FreeRADIUS

Paso 1. Edite **/etc/raddb/clients.conf** para establecer la clave compartida para el WLC.

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

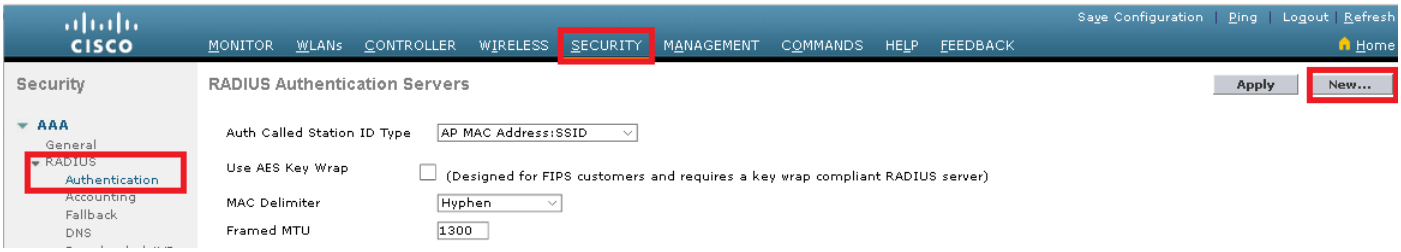
Paso 2. En la parte inferior, agregue la dirección ip del controlador y la clave compartida.

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

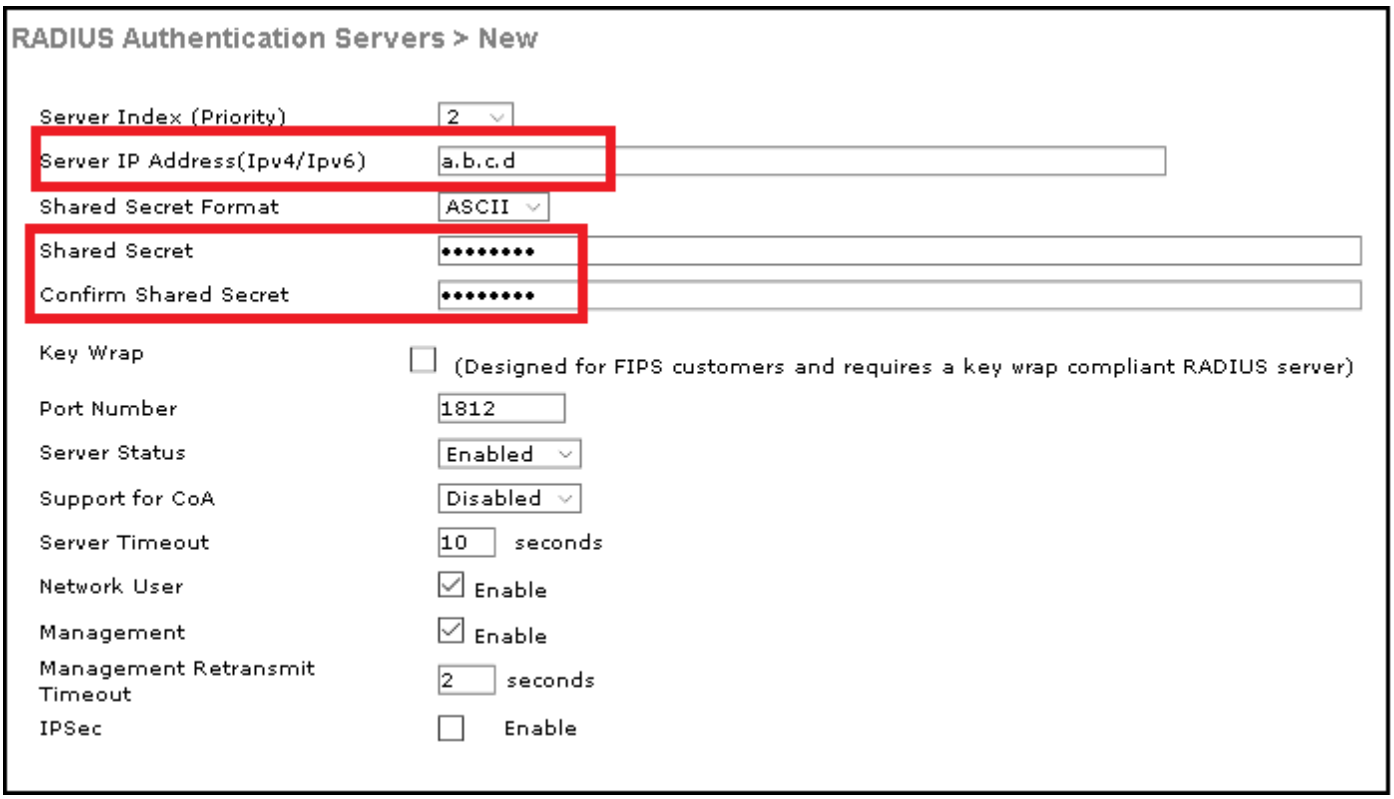
FreeRADIUS como servidor RADIUS en WLC

GUI:

Paso 1. Abra la GUI del WLC y navegue hasta **SECURITY > RADIUS > Authentication > New** como se muestra en la imagen.



Paso 2. Complete la información del servidor RADIUS como se muestra en la imagen.



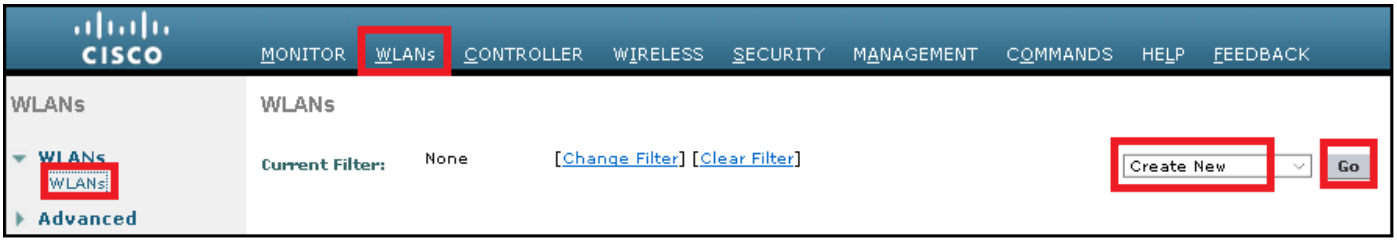
CLI:

```
> 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>
```

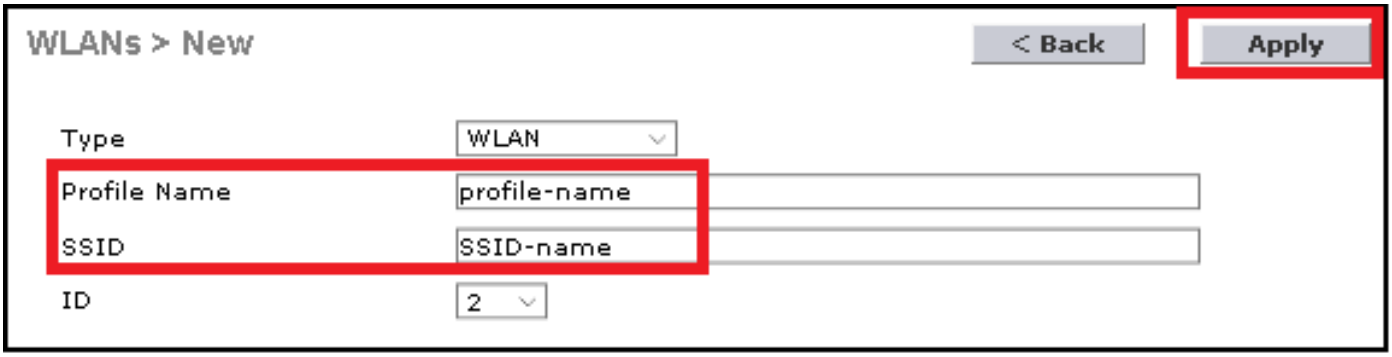
WLAN

GUI:

Paso 1. Abra la GUI del WLC y navegue hasta **WLANs > Create New >** Goas mostradas en la imagen.



Paso 2. Elija un nombre para el identificador de conjunto de servicios (SSID) y el perfil y, a continuación, haga clic en Aplicaciones mostradas en la imagen.



CLI:

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

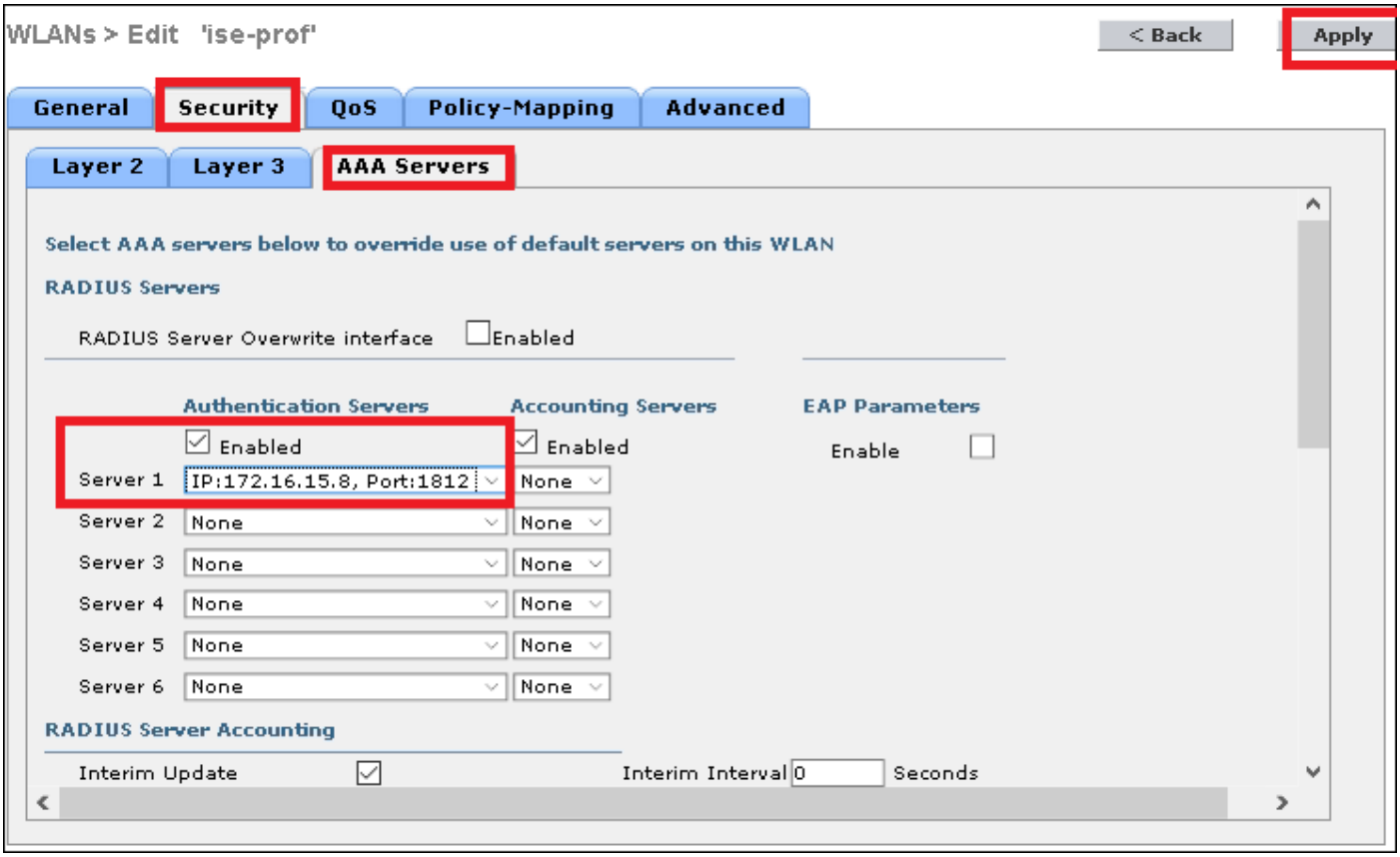
Paso 3. Asigne el servidor RADIUS a la WLAN.

CLI:

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

GUI:

Navegue hasta **Seguridad > Servidores AAA** y elija el servidor RADIUS deseado, luego haga clic en **Aplicar** como se muestra en la imagen.



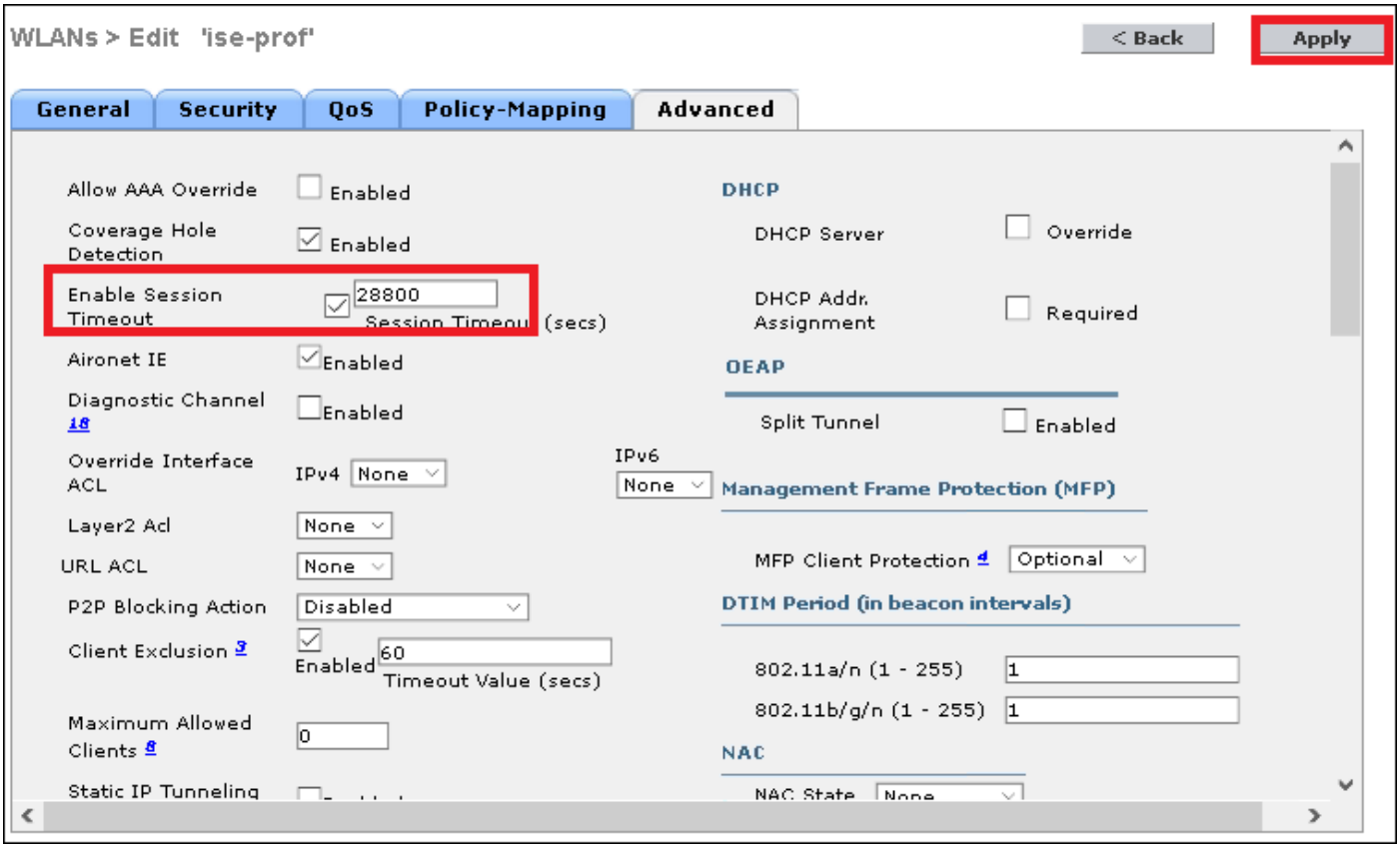
Paso 4. Opcionalmente, aumente el tiempo de sesión.

CLI:

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

GUI:

Navegue hasta **Avanzado > Activar Tiempo de Espera de Sesión >** haga clic en **Aplicar** como se muestra en la imagen.



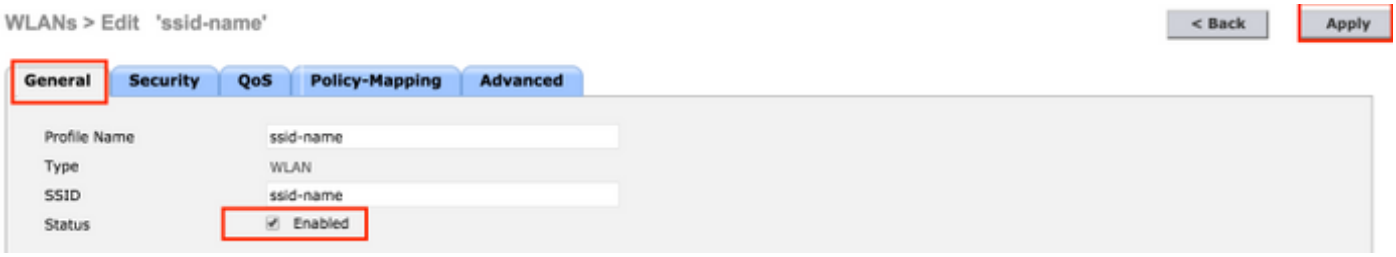
Paso 5. Habilite la WLAN.

CLI:

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

GUI:

Vaya a **General > Status > Tick Enabled > Click Apply** como se muestra en la imagen.



Agregar usuarios a base de datos de RADIUS libre

De forma predeterminada, los clientes utilizan protocolos PEAP, sin embargo freeRadius admite otros métodos (no incluidos en esta guía).

Paso 1. Edite el archivo **/etc/raddb/users**.

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

Paso 2. En la parte inferior del archivo, añada la información de los usuarios. En este ejemplo, **user1** es el nombre de usuario y **Cisco123** la contraseña.

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

Paso 3. Reinicie FreeRadius.

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

Certificados en freeRADIUS

FreeRADIUS incluye un certificado predeterminado de la Autoridad de certificación (CA) y un certificado de dispositivo que se almacenan en la ruta /etc/raddb/certs. El nombre de estos certificados es ca.pem y server.pem. server.pem es el certificado que los clientes reciben mientras pasan por el proceso de autenticación. Si necesita asignar un certificado diferente para la autenticación EAP, simplemente puede eliminarlos y guardar los nuevos en la misma ruta con el mismo nombre exacto.

Configuración del dispositivo final

Configure un equipo portátil Windows para conectarse a un SSID con autenticación 802.1x y PEAP/MS-CHAP (versión de Microsoft del Protocolo de autenticación por desafío mutuo) versión 2.

Para crear el perfil WLAN en el equipo de Windows hay dos opciones:

1. Instale el certificado autofirmado en el equipo para validar y confiar en el servidor freeRADIUS para completar la autenticación
2. Omita la validación del servidor RADIUS y confíe en cualquier servidor RADIUS utilizado para realizar la autenticación (no recomendado, ya que puede convertirse en un problema de seguridad). La configuración de estas opciones se explica en End device configuration - Create the WLAN Profile (Configuración del dispositivo final - Crear el perfil WLAN).

Importar certificado FreeRADIUS

Si utiliza los certificados predeterminados instalados en freeRADIUS, siga estos pasos para importar el certificado EAP del servidor freeRADIUS al dispositivo final.

Paso 1. Obtenga el certificado de FreeRadius:

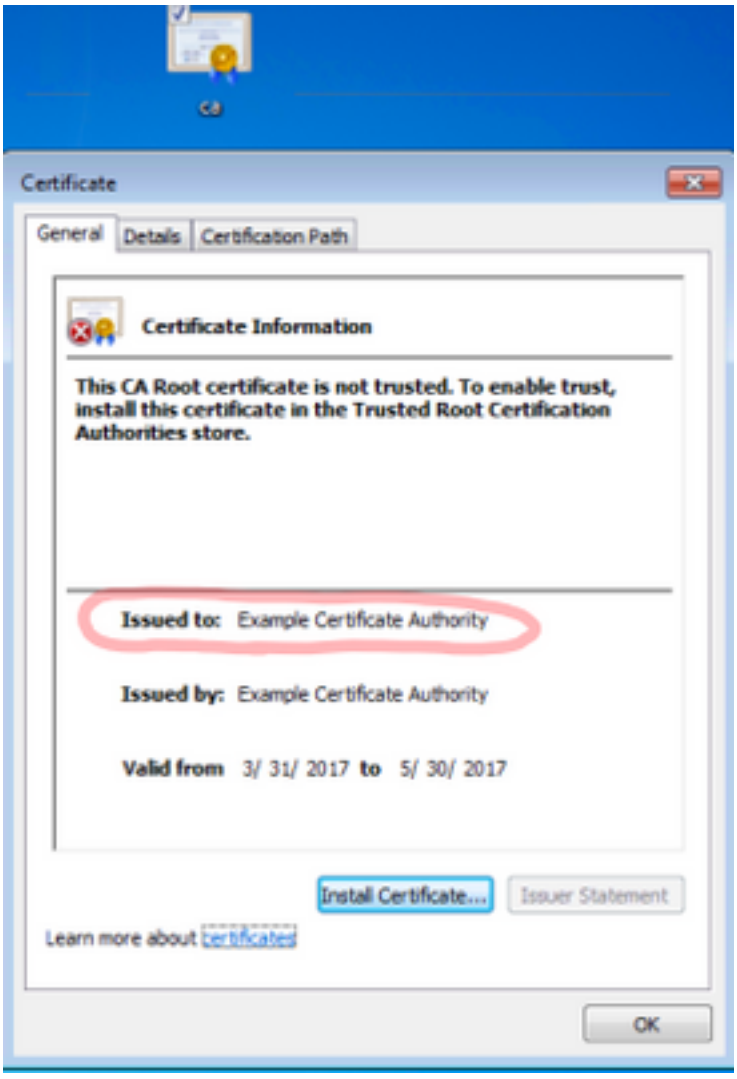
```
[root@tac-mxwireless ~]# cat /etc/raddb/certs/ca.pem

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

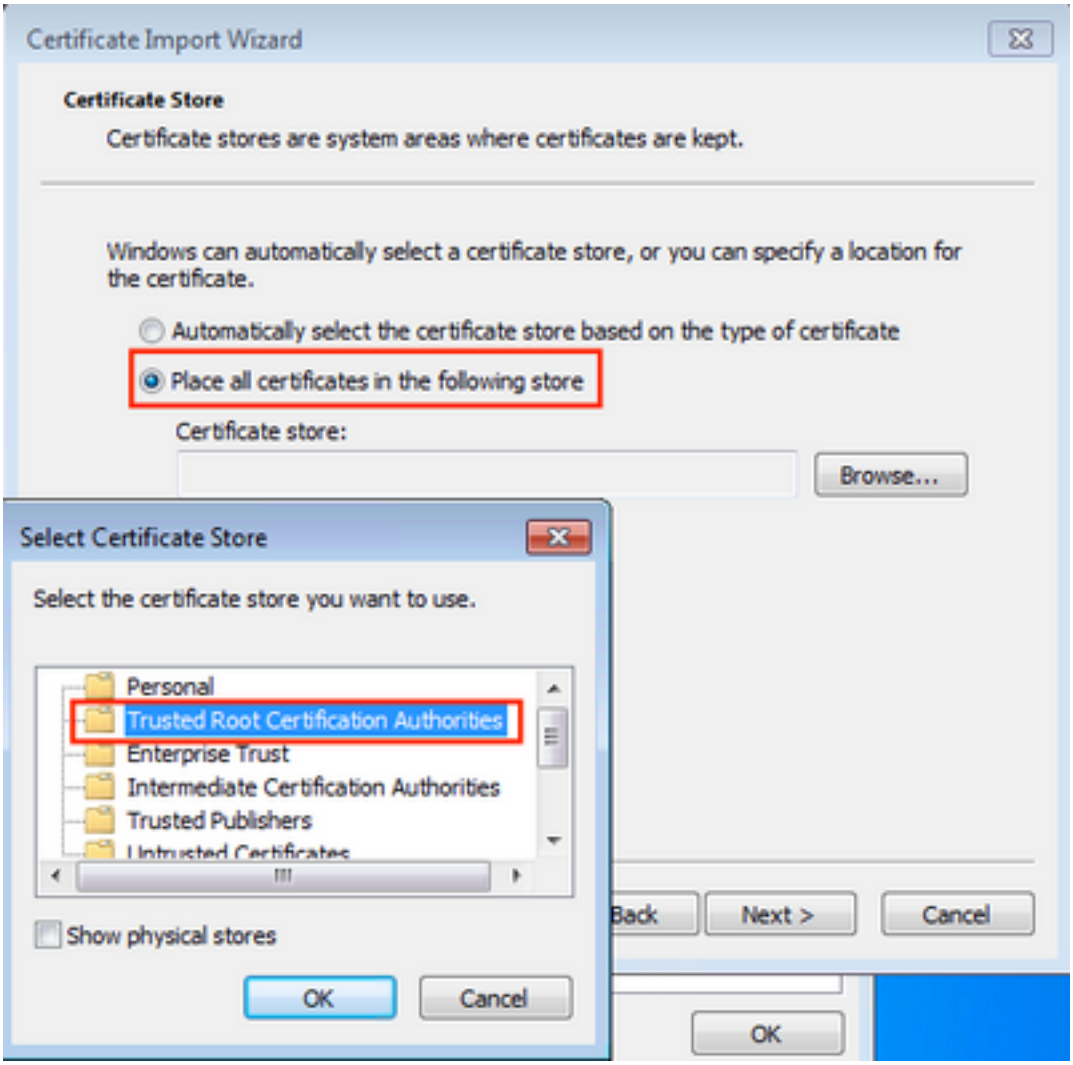
```
Eu6GDw1YJvhHn4rVC36OZU/Nbaxj0eR8ZG0JGse4ftQKLfckkvCOS5QGn4X1elRS
oFe27HRF+pTDHd+nzbaDvhYWvFoe6iA27Od7AY/sDuo/tiIJWGdm9ocPz3+0IiFC
ay6dtG55YQOHxKaswH7/HJkLsKWhS4YmXLgJXCeeJqooqr+TEwyCDEaFaiX835Jp
gwNNZ7X5US0FcjuuOtpJJ3hfQ8K6uXjEWPOkDE0DAnqp4/n9AgMBAAGjggE0MIIB
MDAdBgNVHQ4EFgQUysFNRZKpAlcFCEgwdOPVGV0waLEwgcgGA1UdIwSBwDCBvYAU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

Paso 2. Copie y pegue el resultado del paso anterior en un archivo de texto y cambie la extensión a .crt

Paso 3. Haga doble clic en el archivo y seleccione **Instalar certificado...** como se muestra en la imagen.

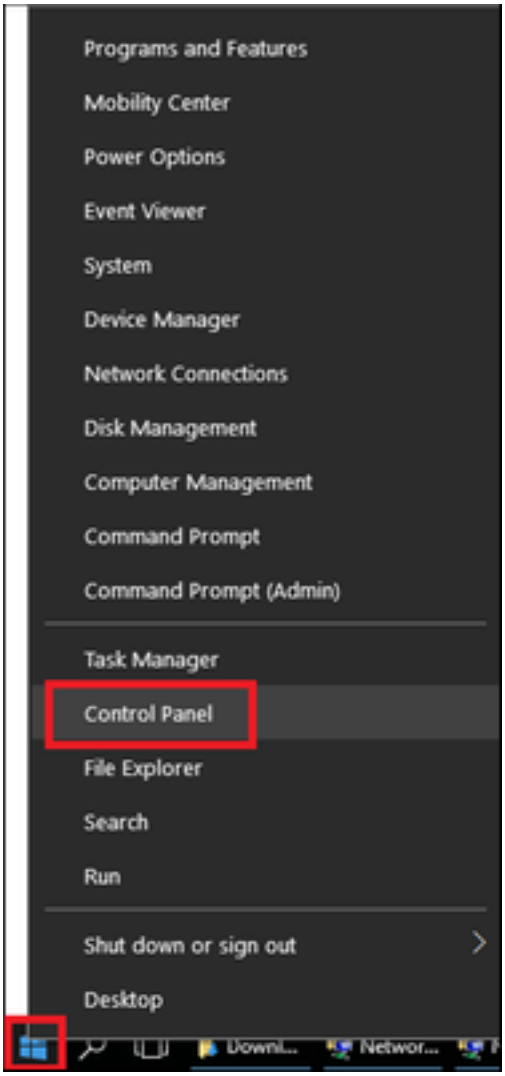


Paso 4. Instale el certificado en el almacén **Autoridades de certificación raíz de confianza** como se muestra en la imagen.

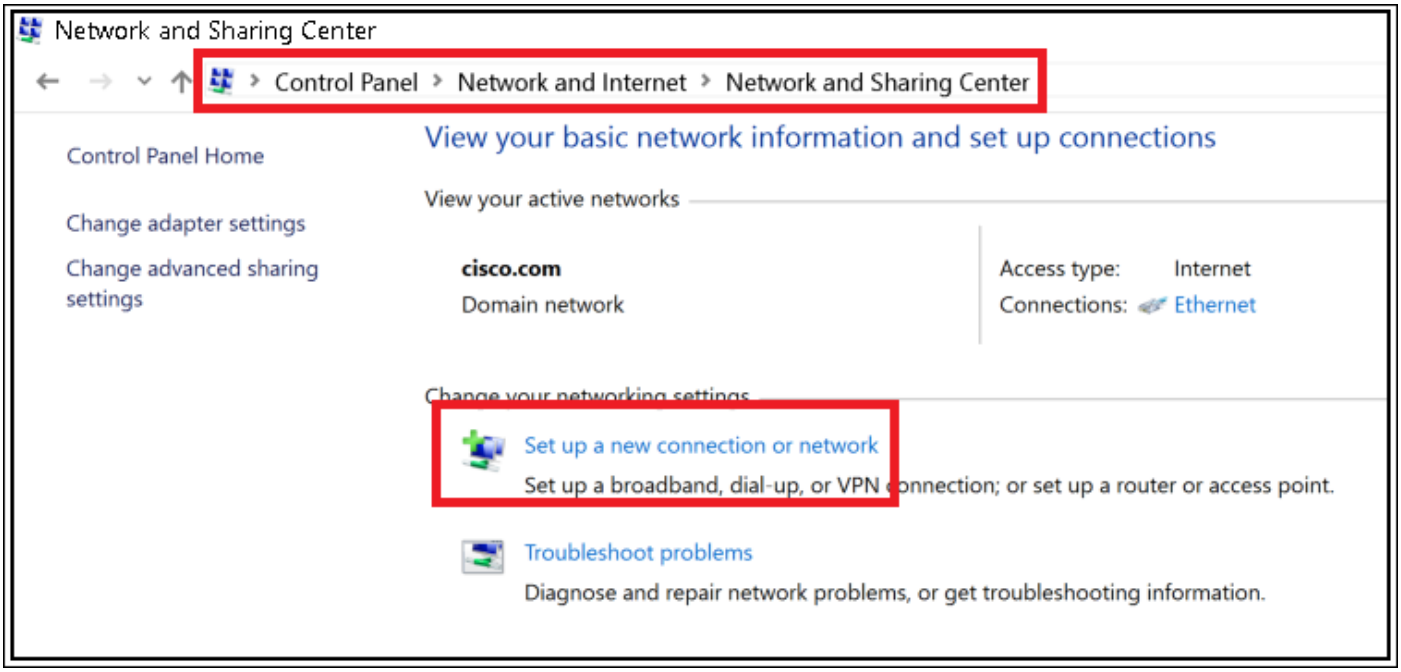


Crear perfil WLAN

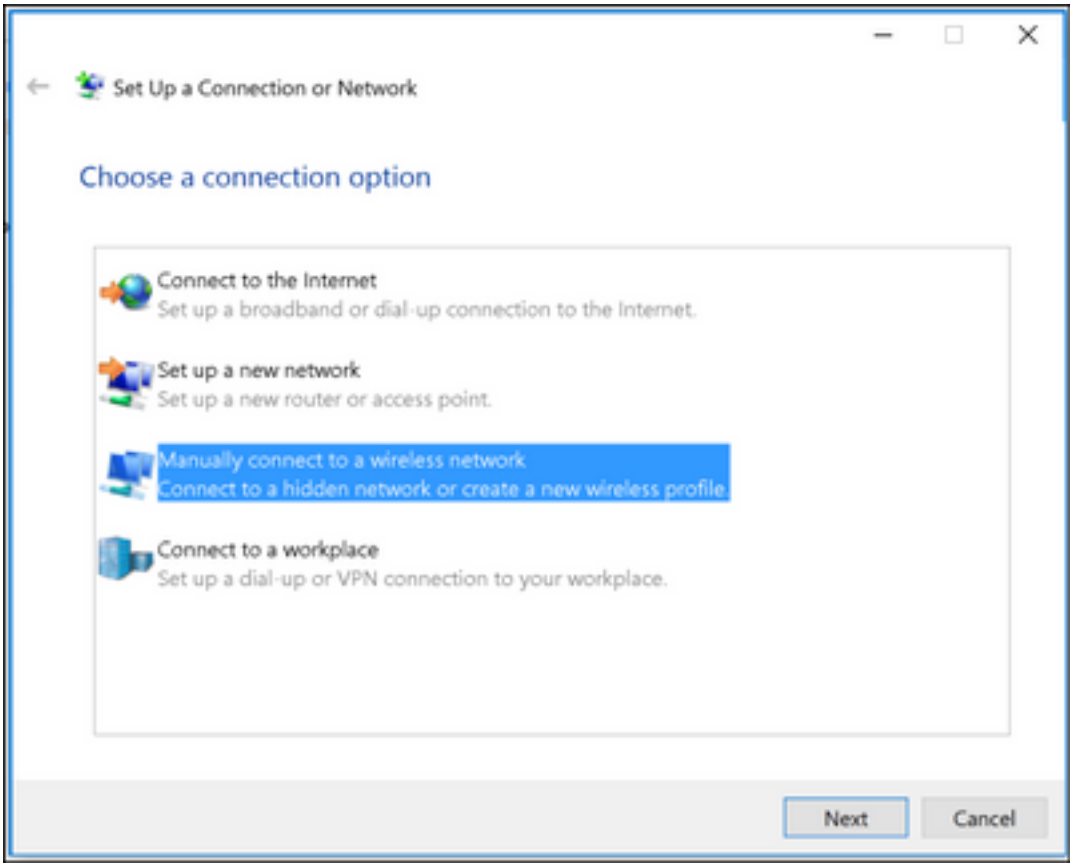
Paso 1. Haga clic con el botón derecho del ratón en el icono Inicio y seleccione **Panel de control** como se muestra en la imagen.



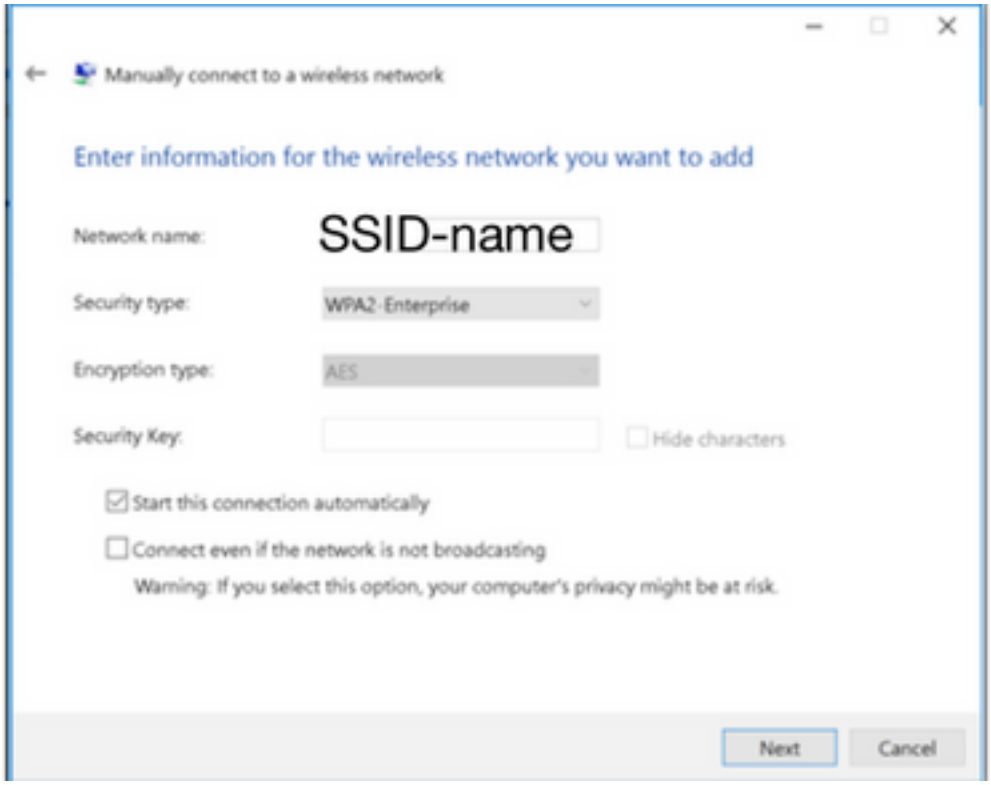
Paso 2. Navegue hasta **Red e Internet > Centro de redes y recursos compartidos> haga clic en Configurar una nueva conexión o red** como se muestra en la imagen.



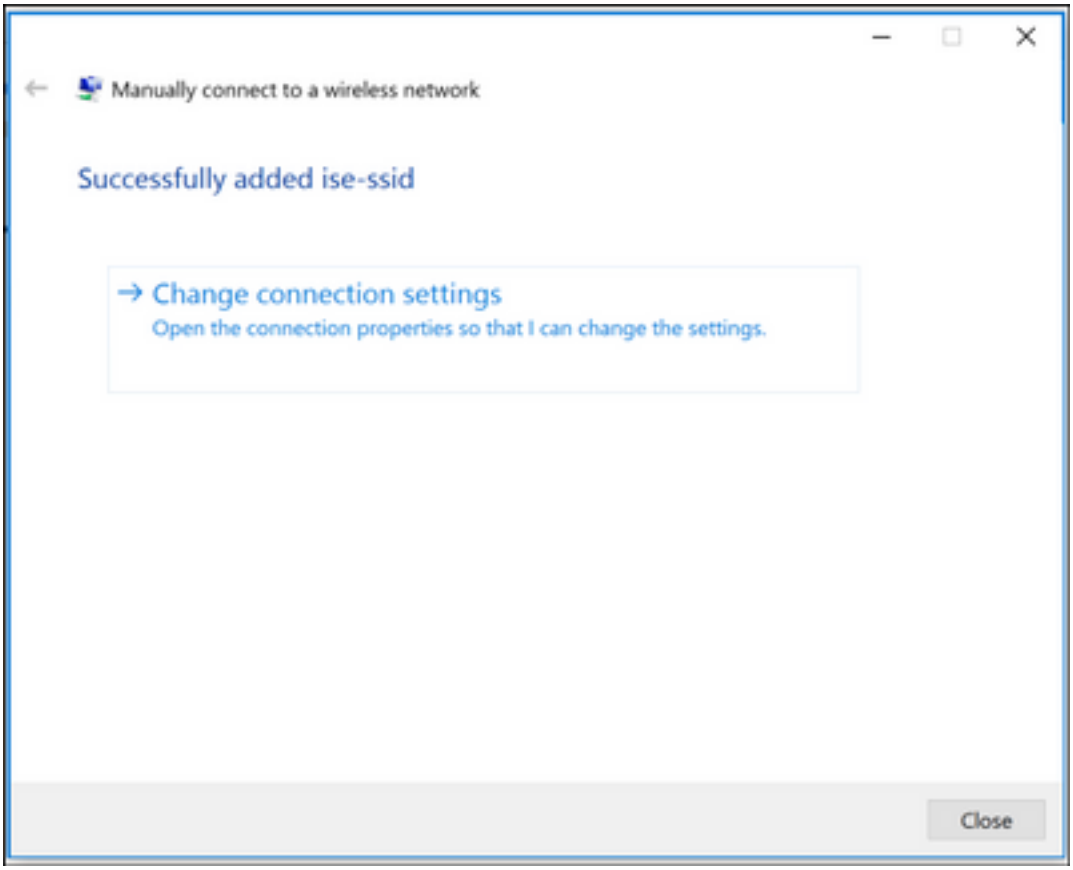
Paso 3. Seleccione **Conexión manual a una red inalámbrica** y haga clic en Nextas que se muestra en la imagen.



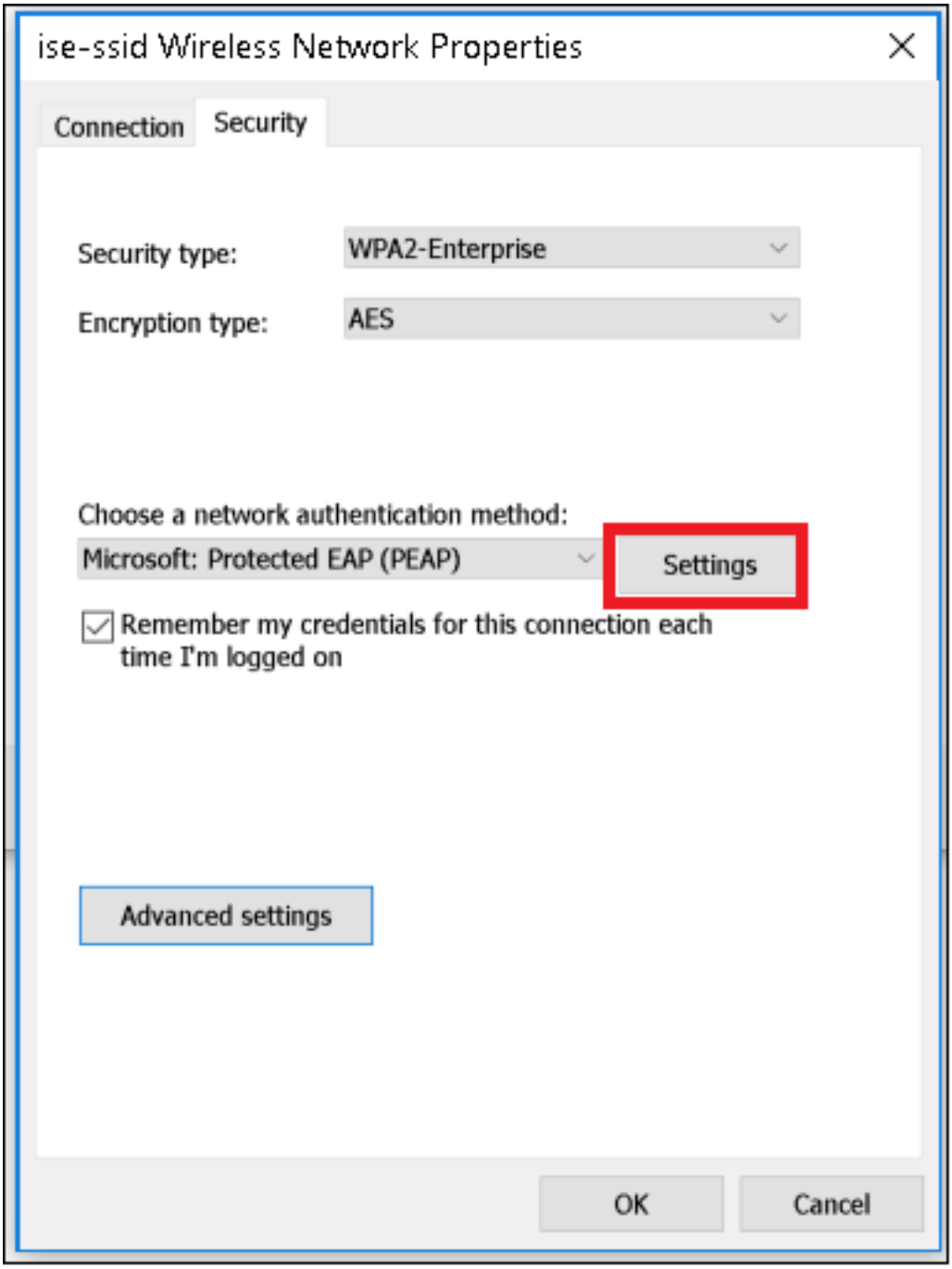
Paso 4. Introduzca la información con el nombre del SSID y el tipo de seguridad WPA2-Enterprise y haga clic en **Next** como se muestra en la imagen.



Paso 5. Seleccione **Cambiar configuración de conexión** para personalizar la configuración del perfil WLAN como se muestra en la imagen.



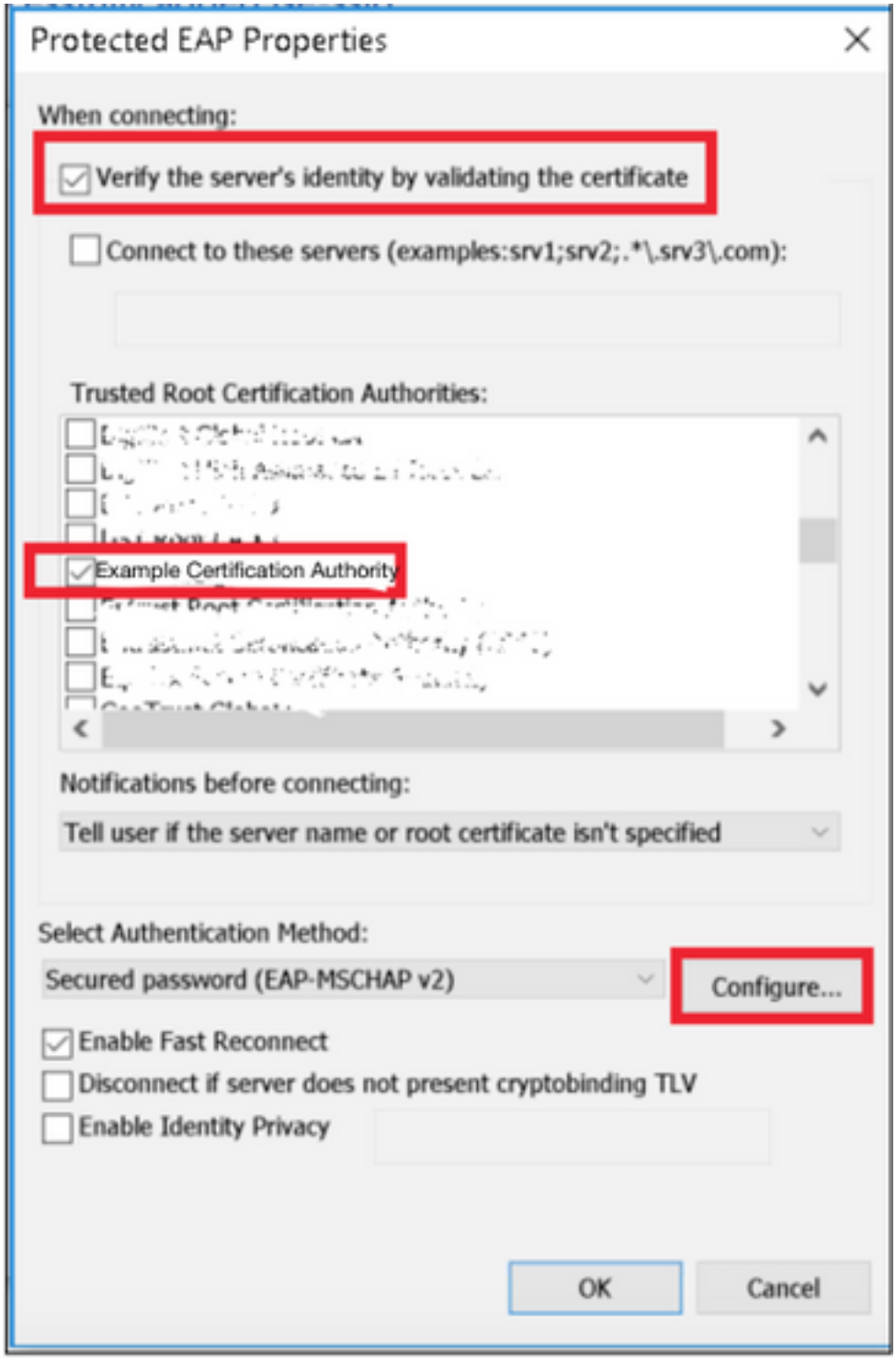
Paso 6. Vaya a la ficha **Seguridad** y haga clic en **Configuración** como se muestra en la imagen.

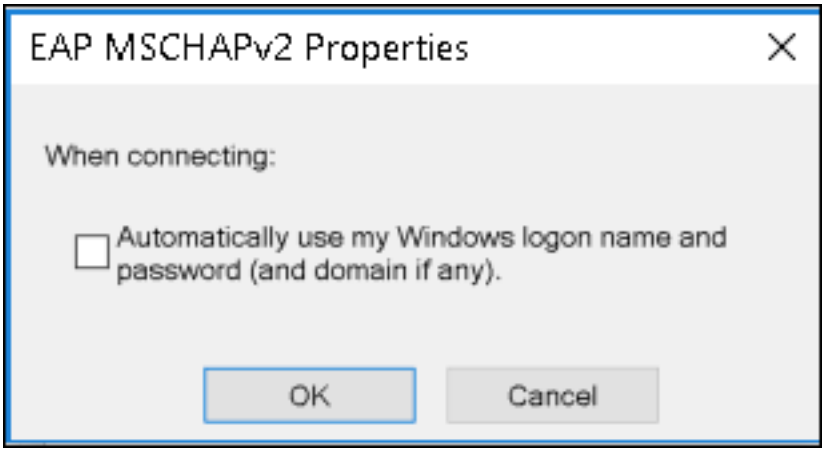


Paso 7. Elija si el servidor RADIUS está validado o no.

En caso afirmativo, habilite **Verificar la identidad del servidor validando el certificado** y de **Autoridades de certificación raíz de confianza:** list (lista) seleccione el certificado autofirmado de freeRADIUS.

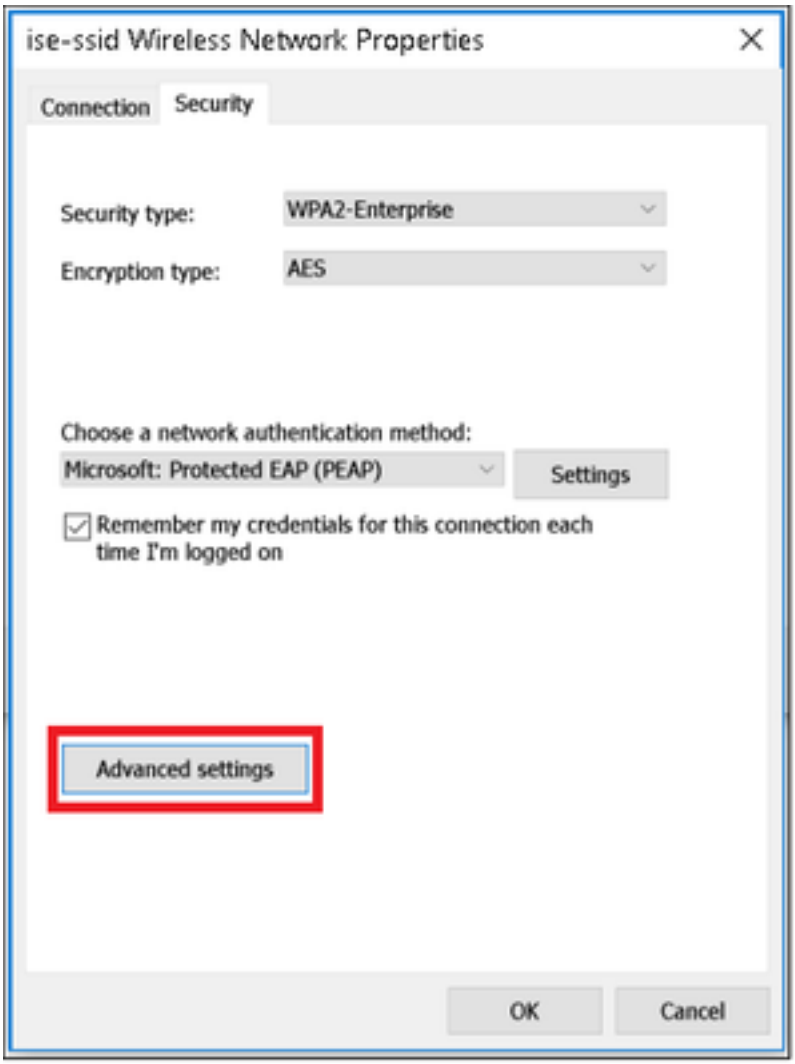
Después de seleccionar **Configure** y disable **Use automáticamente mi nombre de inicio de sesión y contraseña de Windows...**, luego haga clic en **OK** como se muestra en las imágenes.

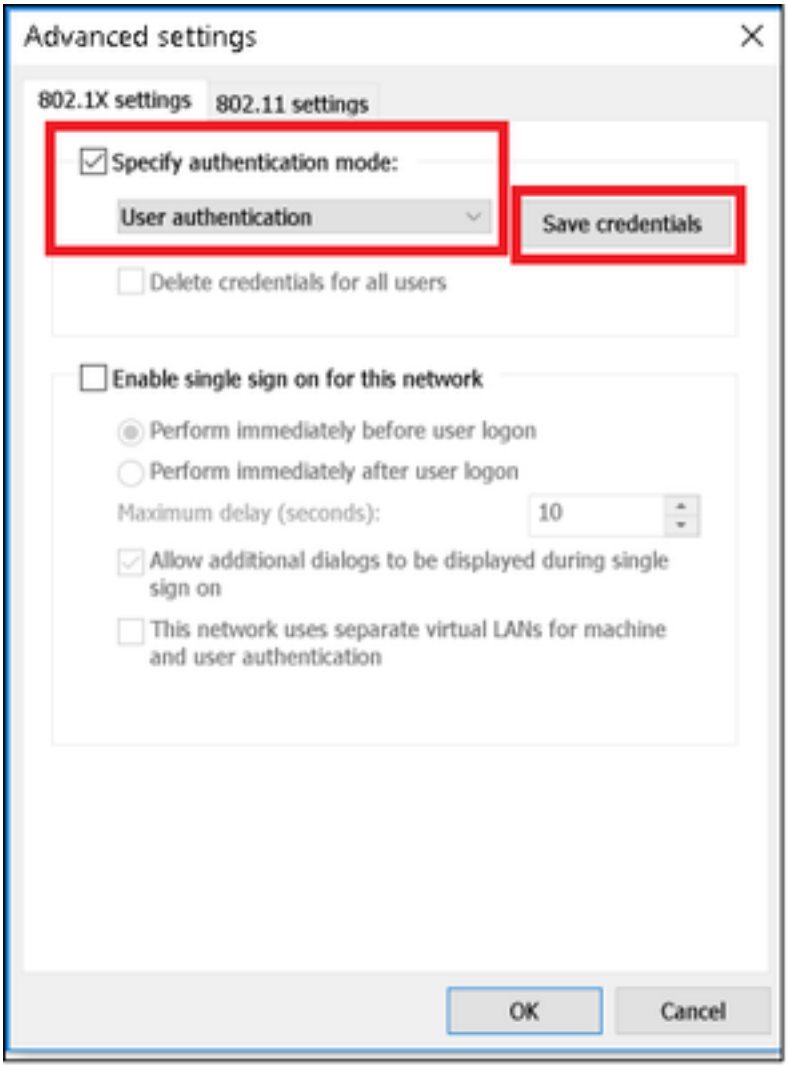


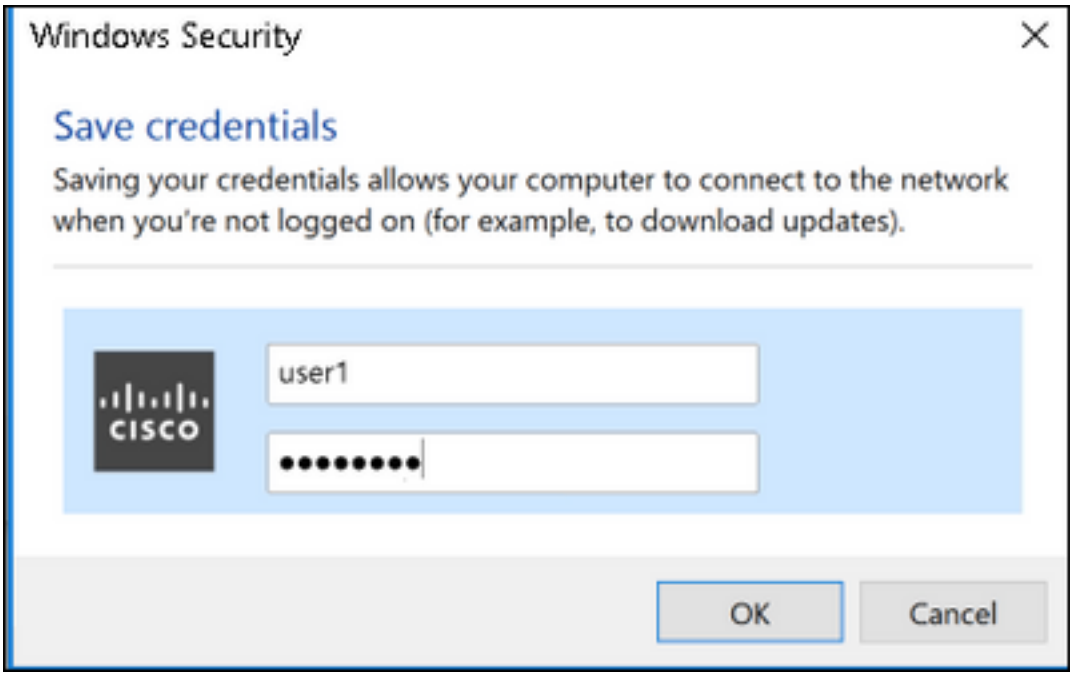


Paso 8. Configure las credenciales del usuario.

Una vez de nuevo a la ficha Security , seleccione **Advanced settings**, especifique el modo de autenticación como **User authentication** y guarde las credenciales configuradas en freeRADIUS para autenticar al usuario, como se muestra en las imágenes.







Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Proceso de autenticación en WLC

Ejecute los siguientes comandos para monitorear el proceso de autenticación para un usuario específico:

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

Para leer fácilmente los resultados de debug client, utilice la herramienta Wireless debug analyzer:

Analizador de depuración inalámbrica

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.