802.1x de la configuración - PEAP con FreeRadius y el WLC 8.3

Contenido

Introducción

Esto documenta explica cómo configurar una red inalámbrica (WLAN) (Wireless Local Area Network) con la Seguridad y PEAP (protocolo extensible authentication protegido) del 802.1x como EAP (protocolo extensible authentication). FreeRADIUS se utiliza como el servidor externo del Remote Authentication Dial-In User Service (RADIUS).

Prerrequisitos

Cisco recomienda que usted tiene conocimiento básico del editor y de los reguladores del Wireless LAN de AireOS (WLCs) de Linux, del Vim.

> Nota: Este documento se piensa para dar a los lectores un ejemplo en la configuración requerida en un servidor del freeRADIUS para la autenticación PEAP-MS-CHAPv2. La Configuración del servidor del freeRADIUS presentada en este documento se ha probado en el laboratorio y se ha encontrado para trabajar como se esperaba. El Centro de Asistencia Técnica de Cisco (TAC) no soporta la Configuración del servidor del freeRADIUS.

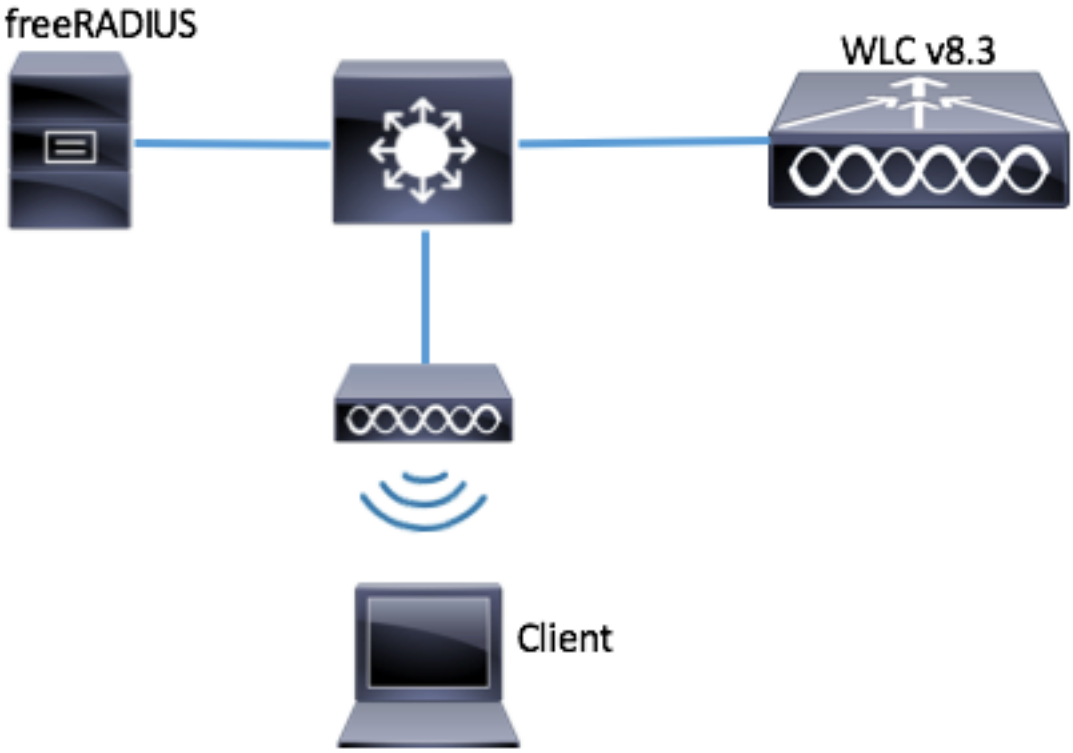
Componentes Utilizados

- CentOS7 o Red Hat Enterprise Linux 7 (RHEL7) (RAM recomendado 1 GB y por lo menos 20 HDD GB)
- WLC 5508 v8.3
- MariaDB (MySQL)
- FreeRADIUS

- PHP 7

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Diagrama de la red



Configuración

Instale el servidor y MariaDB httpd

Paso 1. Funcione con estos comandos de instalar el servidor y 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
```

Paso 2. Encienda y habilite httpd (Apache) y el servidor 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
```

Paso 3. Configuraciones iniciales de MariaDB de la configuración para asegurarlo.

```
[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!

Paso 4. Base de datos de la configuración para el freeRADIUS (utilice la misma contraseña configurada en el paso 3).

```
[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!
```

Instale PHP 7 en CentOS 7

Paso 1. Funcione con estos comandos de instalar PHP 7 en CentOS7.

```
[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!
```

Instale FreeRADIUS

Paso 1. Funcione con este comando de instalar FreeRADIUS.

```
[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!
```

Paso 2. Haga *radius.servicestart* después de mariadb.service*.*

Funcione con este comando:

```
[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!
```

Agregue una línea en la sección del **[Unit]**:

```
[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!

la sección del [Unit] debe parecer esto:

```
[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!
```

Paso 3. Comience y permita al freeradius para comenzar en el inicio para arriba.

```
[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!

Paso 4. Firewalld del permiso para la Seguridad.

```
[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!
```

Paso 5. Agregue las reglas permanentes a la zona predeterminada para permitir el HTTP, el https y los servicios RADIUS.

```
[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!
```

Paso 6. Firewalld de la recarga para que cambios tomen el efecto.

```
[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!
```

Configuración FreeRADIUS

Para configurar FreeRADIUS para utilizar MariaDB, siga los siguientes pasos.

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

```
[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!
```

Paso 2. Establezca las relaciones suaves para el SQL bajo */etc/raddb/mods-enabled*

```
[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!

Paso 3. Configure el módulo */raddb/mods-available/sql* SQL y cambie los parámetros de la Conexión de base de datos a la habitación su entorno.

```
[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!
```

La sección SQL debe parecer similar a abajo.

```
[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!
```

Paso 4. Cambie la derecha de grupo de */etc/raddb/mods-enabled/sql al* radiusd.

```
[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!
```

Configure el WLC como cliente AAA en FreeRADIUS

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

```
[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!
```

Paso 2. En la parte inferior agregue su IP Address del regulador y la clave compartida.

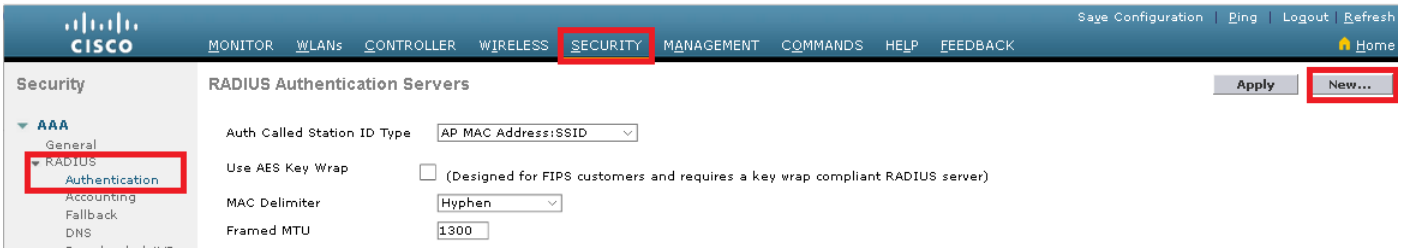
```
[root@tac-mxwireless ~]#mysql_secure_installation

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!
```

Configure FreeRADIUS como servidor de RADIUS en el WLC

GUI:

Paso 1. Abra el GUI del WLC y navegue a la **SEGURIDAD > al RADIUS > a la autenticación > nuevo.**



Paso 2. Llene la información del servidor de RADIUS.

CLI:

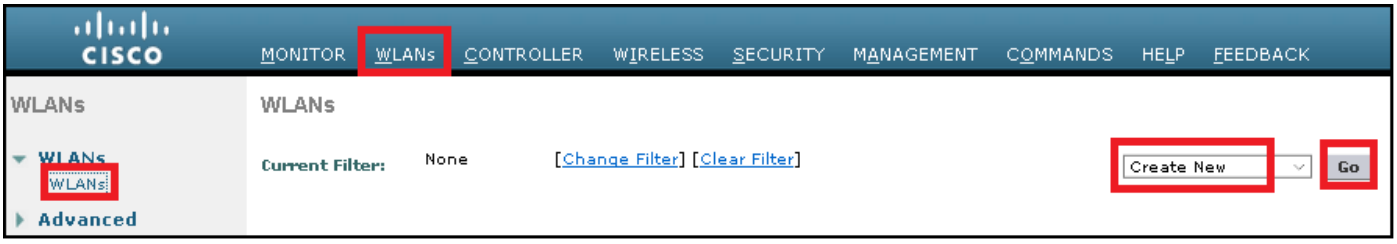
```
[root@tac-mxwireless ~]#mysql_secure_installation

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!
```

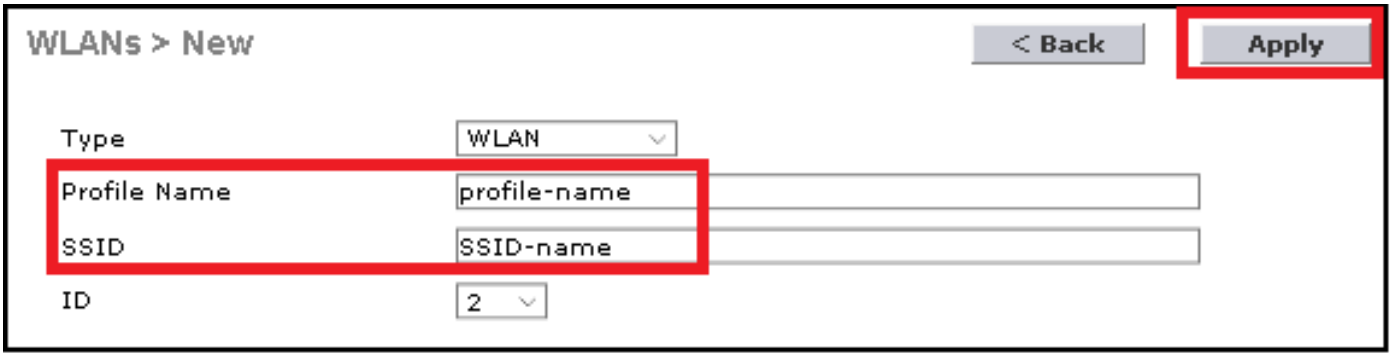
Configure una red inalámbrica (WLAN)

GUI:

Paso 1. Abra el GUI del WLC y navegue a los **WLAN > crean nuevo > van.**



Paso 2. Elija un nombre para el SSID y el perfil, después haga clic **se aplican.**



CLI:

```
[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!
```

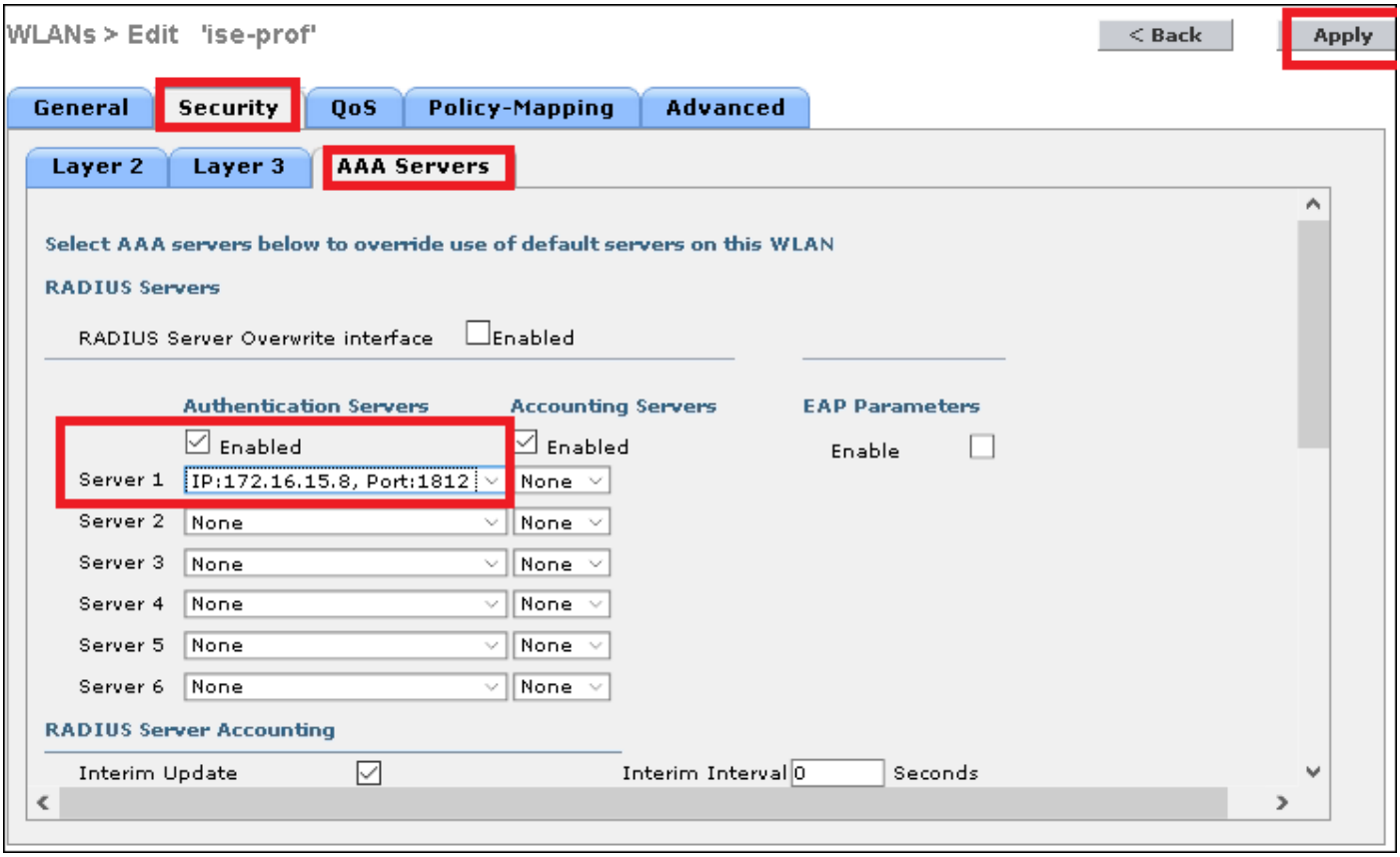
Paso 3. Asigne al servidor de RADIUS a la red inalámbrica (WLAN).

CLI:

```
[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!
```

GUI:

Navegue a los **servidores de la Seguridad >AAA** y elija al servidor de RADIUS deseado, después el golpe **se aplica.**

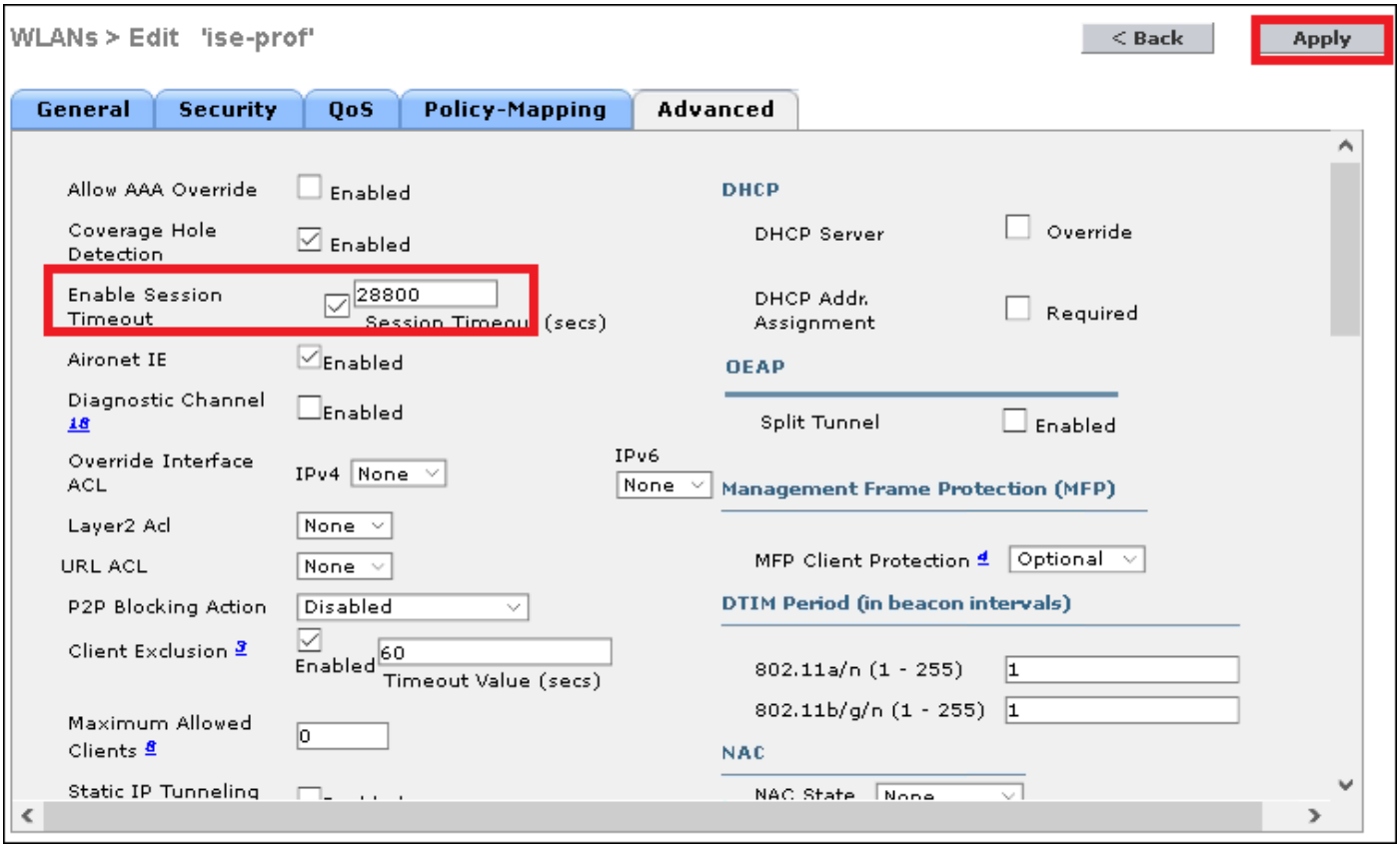


Paso 4. Aumente opcionalmente el tiempo de espera de la sesión

CLI:

```
[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!
```

GUI:

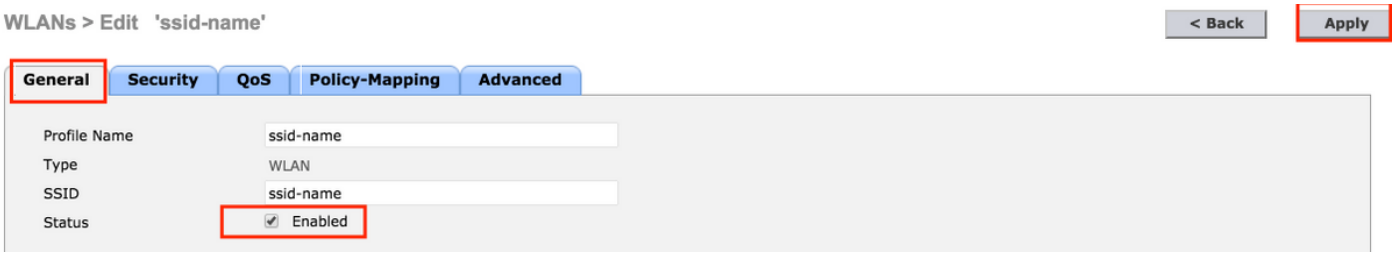


Paso 5. Habilite la red inalámbrica (WLAN)

CLI:

```
[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!
```

GUI:



Agregue a los usuarios a la base de datos del freeRADIUS

Por abandono los clientes utilizan los protocolos PEAP, no obstante soporte del freeRadius otros métodos (no cubiertos en esta guía).

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

```
[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!
```

Paso 2. En la parte inferior del archivo añada la información de usuarios al final del fichero. En este ejemplo el *user1* es el nombre de usuario y *cisco123 la* contraseña.

```
[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!
```

Paso 3. Reinicio FreeRadius.

```
[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!
```

Certificados en el freeRADIUS

FreeRADIUS viene con un certificado predeterminado de CA (certificación Authoritiy) y un certificado del dispositivo que se salven en la trayectoria */etc/raddb/certs.* El nombre de estos Certificados es *ca.pem y* server.pem *server.pemis el certificado* que los clientes recibirán mientras que pasan con el proceso de autenticación. Si usted necesita asignar un diverso certificado para la autenticación EAP usted puede borrarlos simplemente y salvar los nuevos en la misma trayectoria con ese exacto el mismo nombre.

Configuración de dispositivo extremo

Configure una máquina de Windows de la laptop para conectar con un SSID con la autenticación del 802.1x y la versión 2 PEAP/MS-CHAP (versión de Microsoft del protocolo challenge-handshake authentication).

Para crear el perfil de la red inalámbrica (WLAN) en la máquina de las ventanas allí sea dos opciones:

1. Instale el certificado autofirmado en la máquina para validar y para confiar en el servidor del freeRADIUS para completar la autenticación
2. Desvíe la validación del servidor de RADIUS y confíe en a cualquier servidor de RADIUS usado para realizar la autenticación (no recomendada, como puede convertirse en un problema de seguridad). La configuración para estas opciones se explica en la configuración de dispositivo extremo - cree el perfil de la red inalámbrica (WLAN) - el paso xx.

Configuración de dispositivo extremo - Certificado del freeRADIUS de la importación

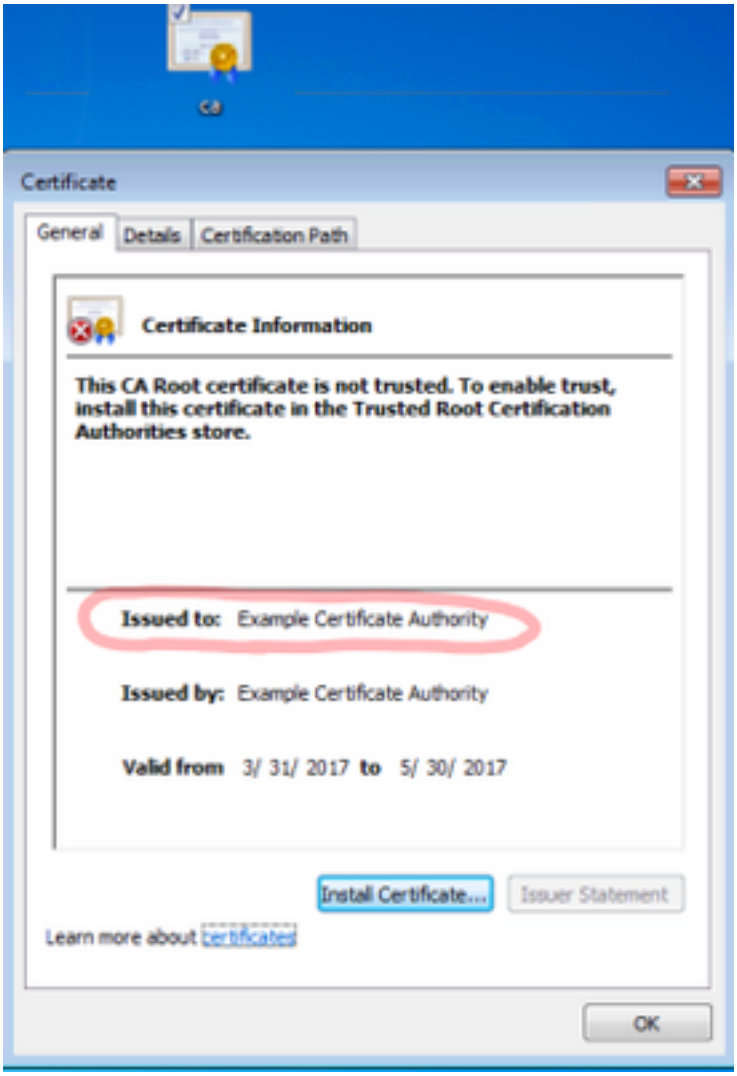
Si usted utiliza los Certificados predeterminados instalados en el freeRADIUS, siga los siguientes pasos para importar el certificado EAP del servidor del freeRADIUS en el dispositivo extremo.

Paso 1. Consiga el CERT de FreeRadius:

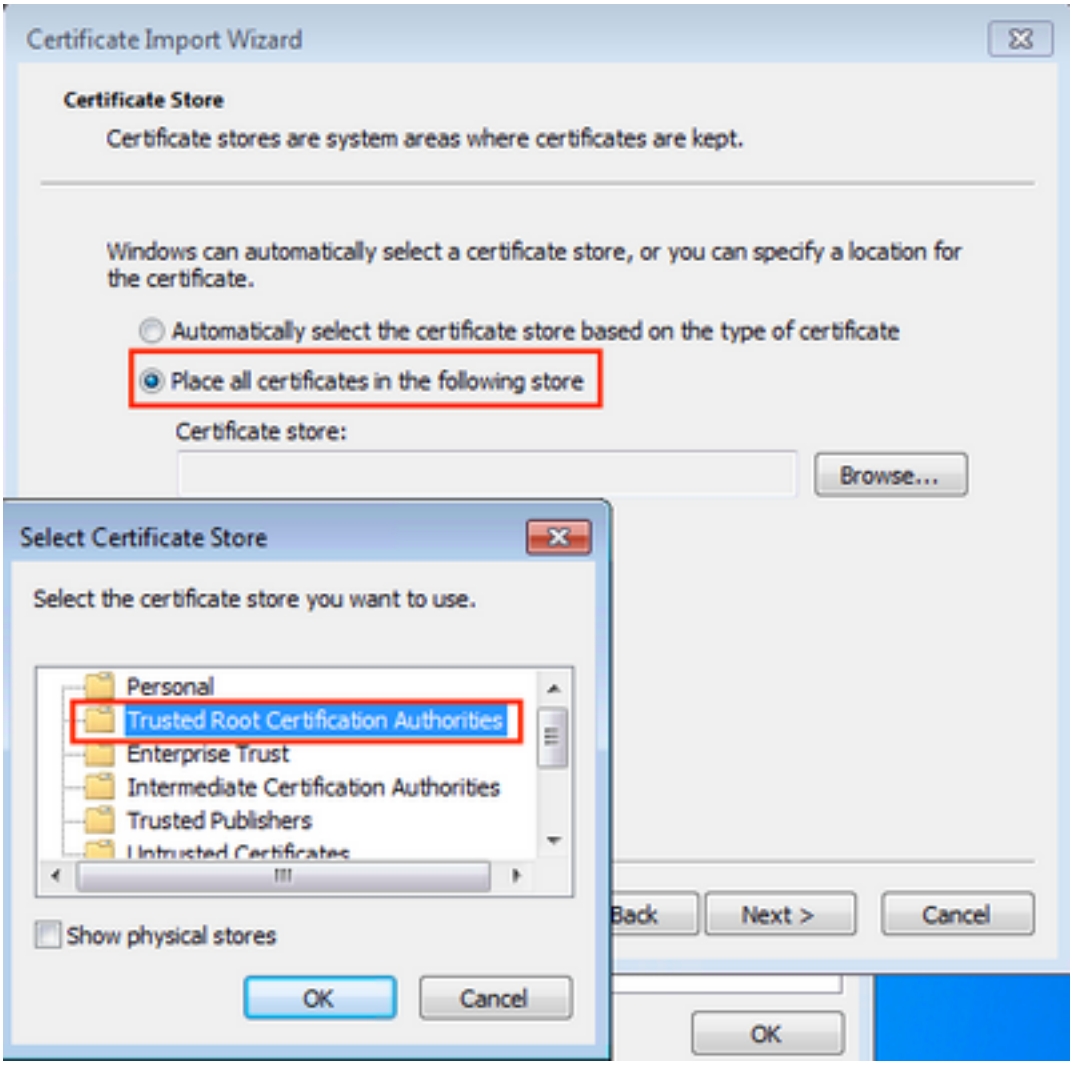
```
[root@tac-mxwireless ~]#mysql_secure_installation

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!
```

Paso 2. La copia y pega la salida del paso anterior en un archivo de texto y cambia la extensión a .crt

Paso 3. El tecleo doble el archivo y selecto **instala el certificado...**

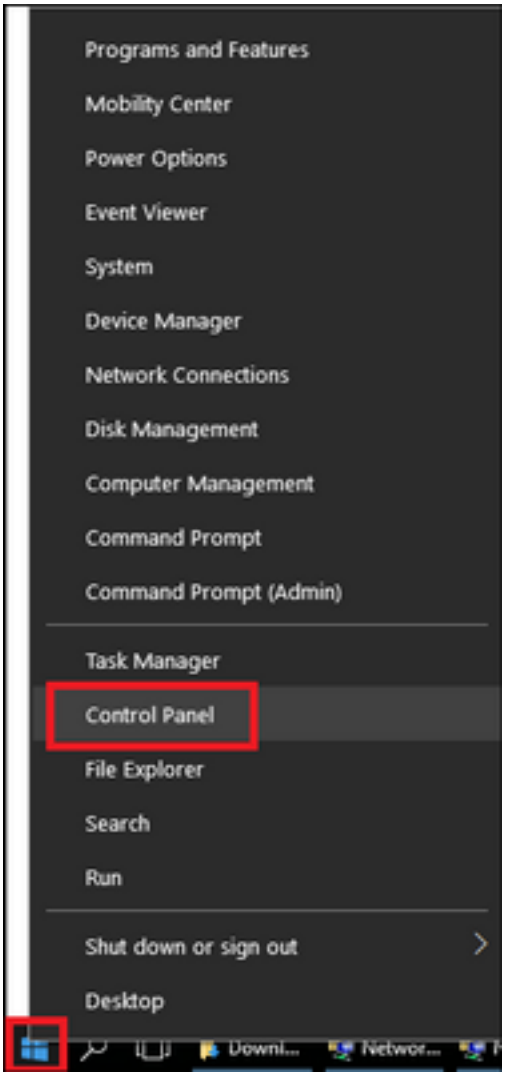


Paso 4. Instale el certificado en el almacén de los **Trusted Root Certification Authority**.

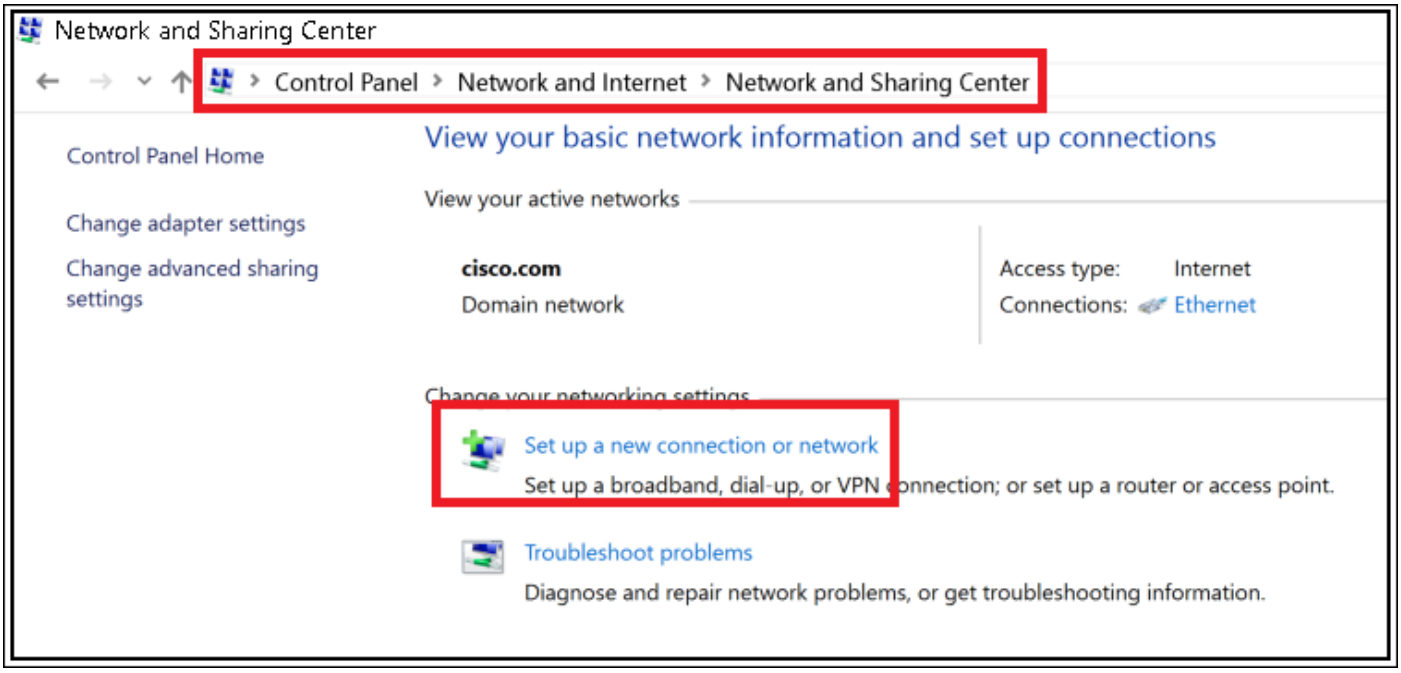


Configuración de dispositivo extremo - Cree el perfil de la red inalámbrica (WLAN)

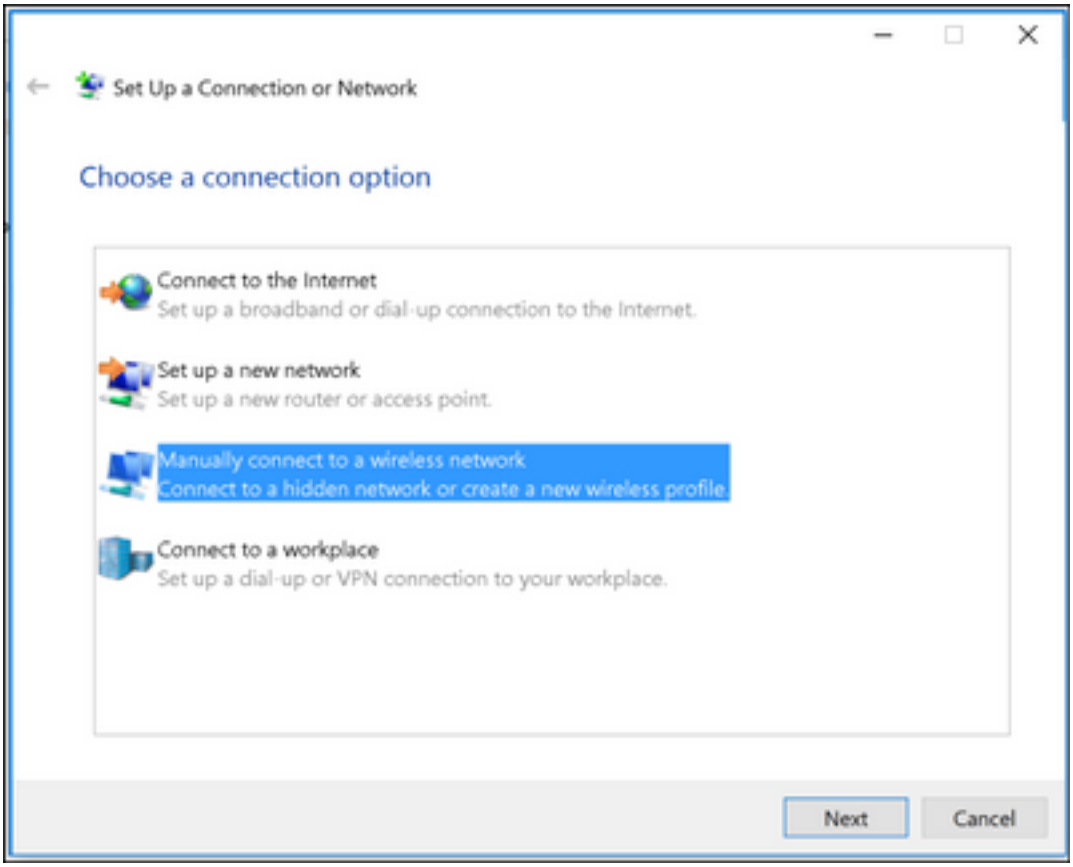
Paso 1. Click derecho en el icono del comienzo y el **panel de control** selecto.



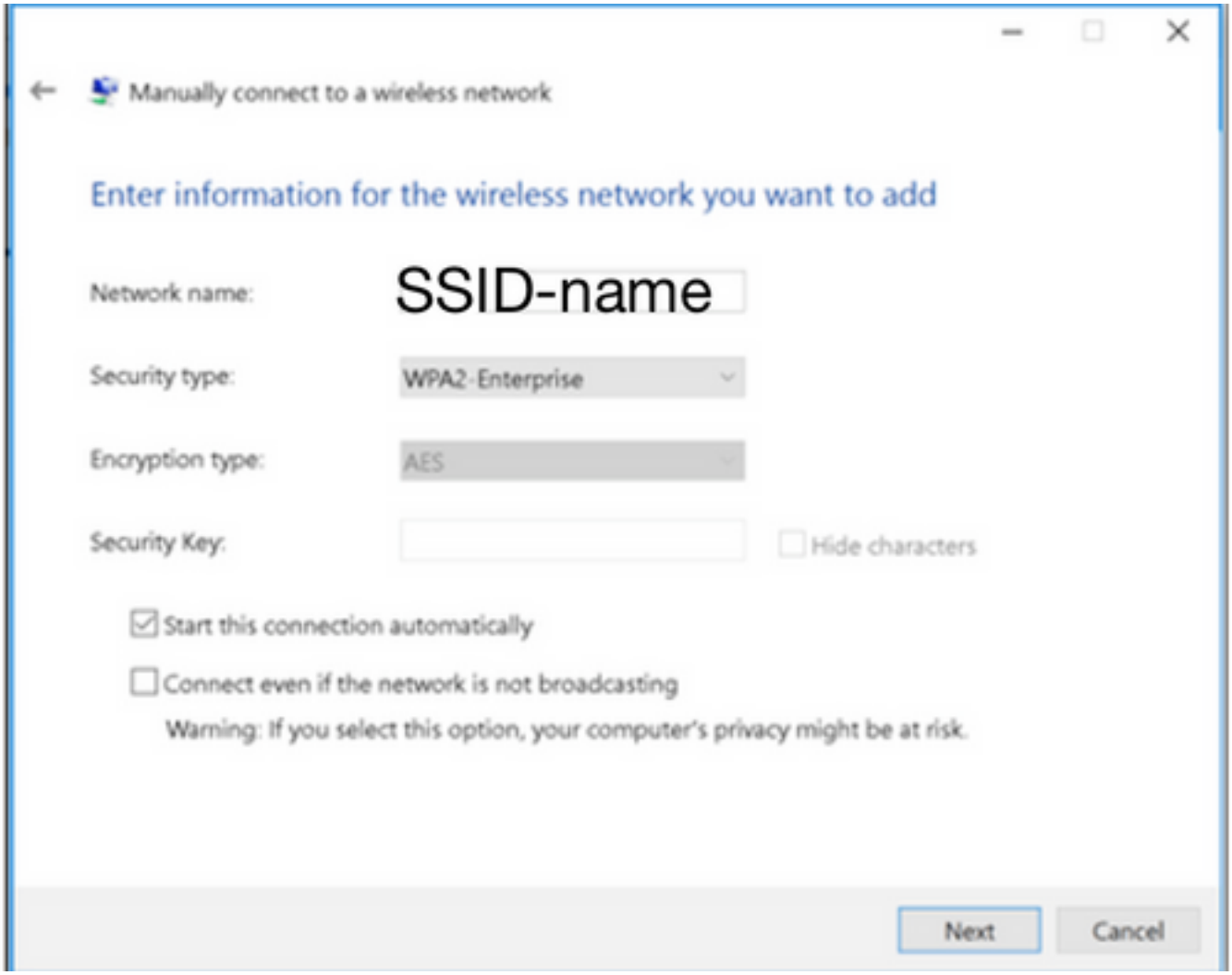
Paso 2. Navegue a la **red y al Internet**, eso navega a la **red y centro de la distribución** y hace clic en después **configura una nueva conexión o una red.**



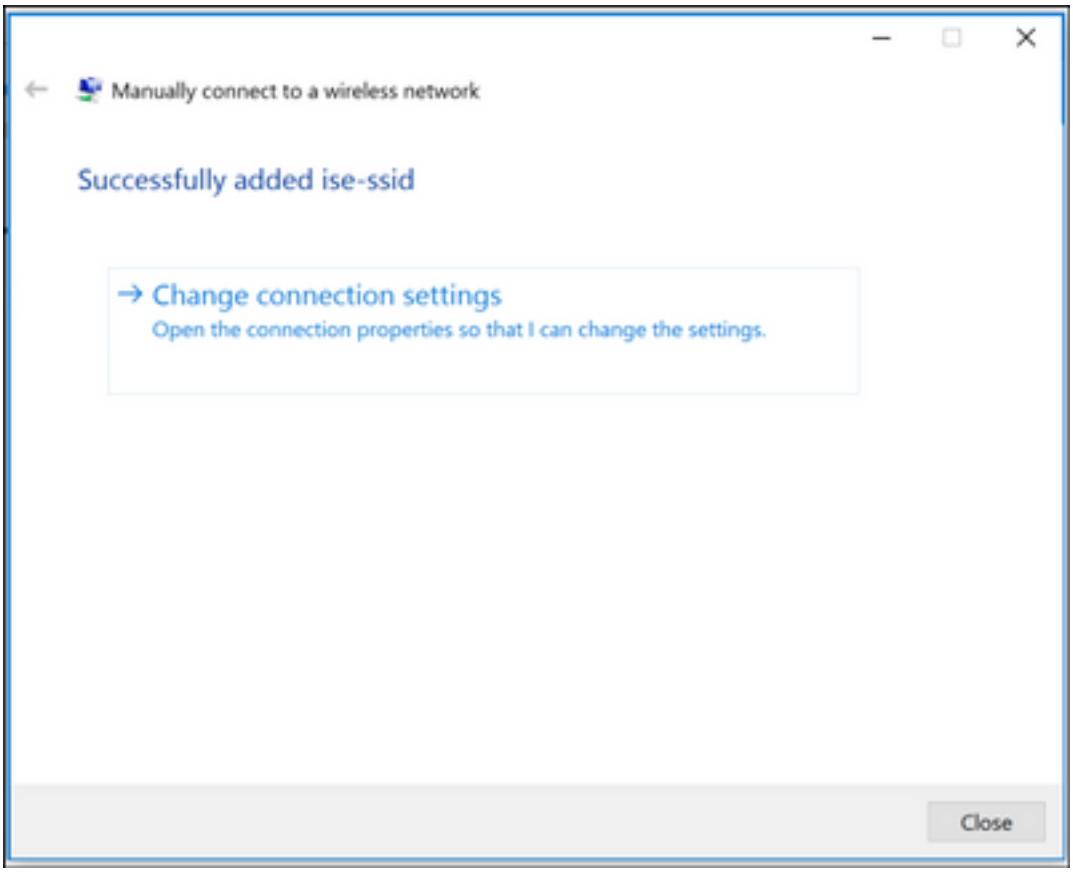
Paso 3. Seleccione **conectan manualmente con una red inalámbrica** y hacen clic **después.**



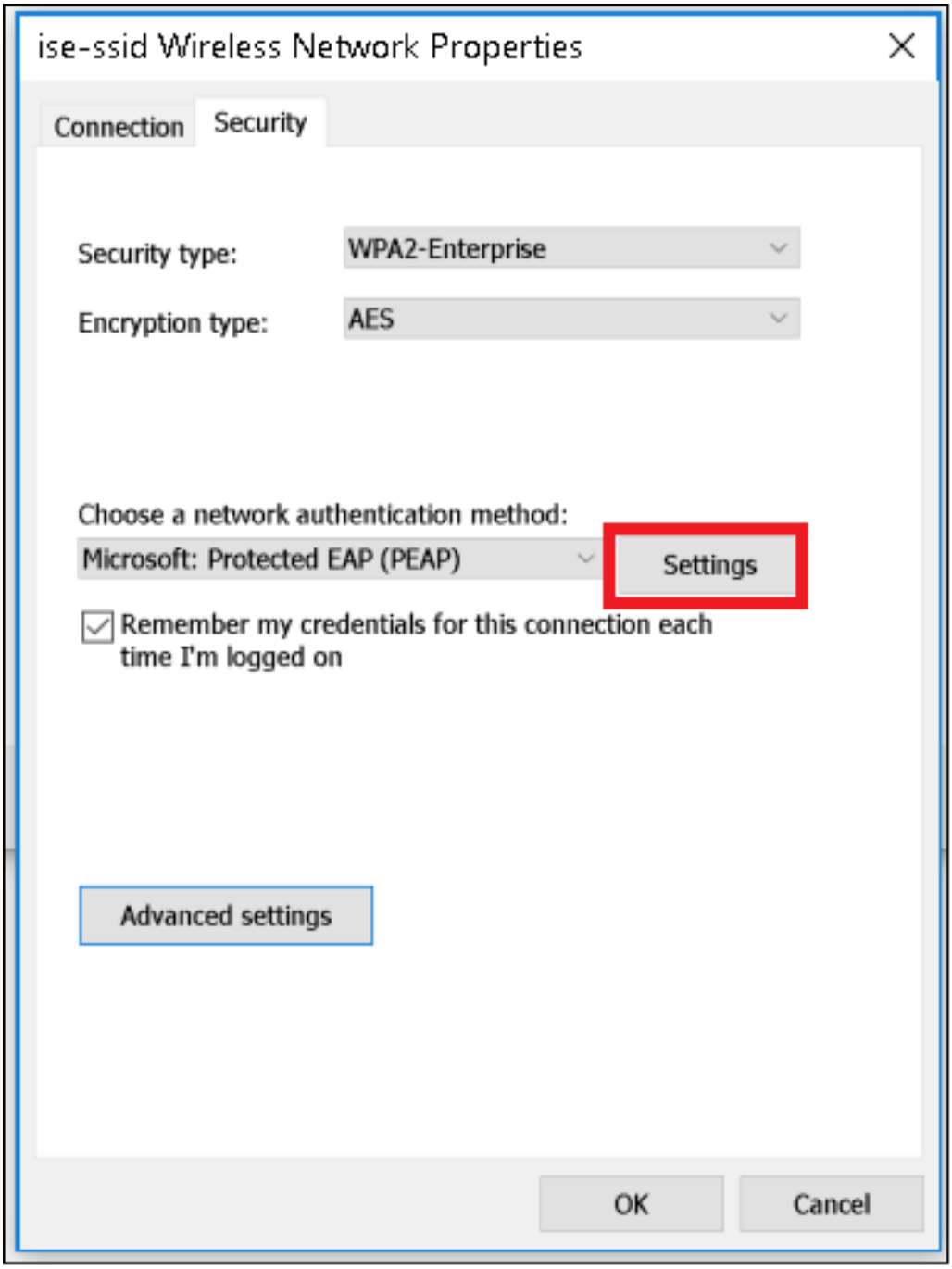
Paso 4. Ingrese la información con el nombre del tipo WPA2-Enterprise SSID y de la Seguridad y haga clic **después.**



Paso 5. Seleccione las **configuraciones de la conexión del cambio** para personalizar la configuración del perfil de la red inalámbrica (WLAN).



Paso 6. Navegue a la **ficha de seguridad** y haga clic las **configuraciones.**



Paso 7. Elija si validan al servidor de RADIUS o no.

Si sí, el permiso **verifica la identidad del servidor validando el certificado** y de los **Trusted Root Certification Authority:** la lista selecciona el certificado autofirmado de freeRADIUS.

Después esa **configuración** y neutralización selectas **utilizan automáticamente mi nombre de inicio y contraseña de Windows…**, después hacen clic la **AUTORIZACIÓN**