Configurar o 802.1x - PEAP com FreeRadius e WLC 8.3

Índice

Introdução

Isto documenta descreve como estabelecer um Wireless Local Area Network (WLAN) com Segurança do 802.1x e protocolo extensible authentication protegido (PEAP) como o Extensible Authentication Protocol (EAP). FreeRADIUS é usado como o server externo do Remote Authentication Dial-In User Service (RADIUS).

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento básico destes assuntos:

- Linux
- Editor do Vim
- Controladores do Wireless LAN de AireOS (WLC)

Note: Este documento é pretendido dar aos leitores um exemplo na configuração exigida em um server do freeRADIUS para a autenticação PEAP-MS-CHAPv2. A configuração do servidor do freeRADIUS apresentada neste documento foi testada no laboratório e encontrada para trabalhar como esperado. O centro de assistência técnica da Cisco (TAC) não apoia a configuração do servidor do freeRADIUS.

Componentes Utilizados

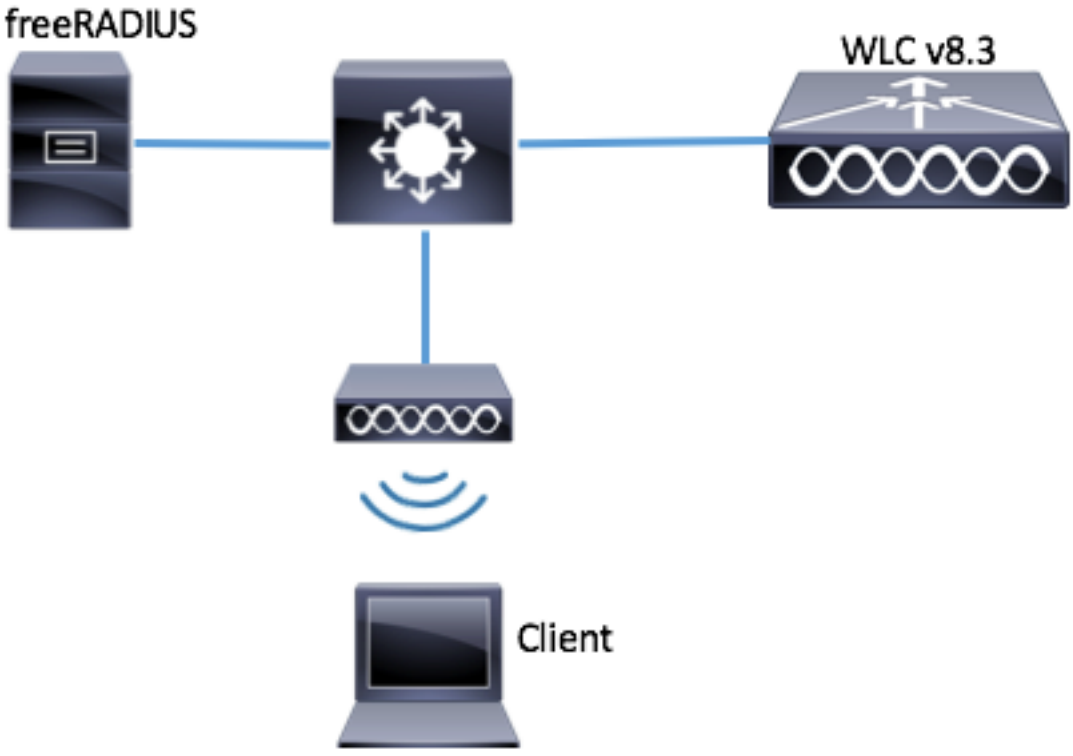
As informações neste documento são baseadas nestas versões de software e hardware:

- CentOS7 ou Red Hat Enterprise Linux 7 (RHEL7) (recomendado 1 GB RAM e pelo menos 20 GB HDD)
- WLC 5508 v8.3
- MariaDB (MySQL)
- FreeRADIUS
- PHP 7

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Diagrama de Rede



Instale o server e o MariaDB httpd

Etapa 1. Execute estes comandos instalar o server e o 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
```

Etapa 2. Ligue e permita httpd (Apache) e server 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
```

Etapa 3. Configurar ajustes iniciais de MariaDB para fixá-la.

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

> **Note**: Execute todas as partes deste script. Recomenda-se para todos os server de MariaDB no uso da produção. Leia cada etapa com cuidado.

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

Etapa 4. Configurar o base de dados para o freeRADIUS (use a mesma senha configurada em etapa 3).

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

Instale PHP 7 em CentOS 7

Etapa 1. Execute estes comandos instalar PHP 7 em CentOS7.

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

Instale FreeRADIUS

Etapa 1. Execute este comando instalar FreeRADIUS.

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

Etapa 2. Faça o **começo radius.service** após mariadb.service**.**

Execute este comando:

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

Adicionar uma linha na seção do **`[Unit]`:**

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

a seção do [Unit] deve olhar como esta:

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

Etapa 3. Comece e permita o freeradius começar acima na bota.

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

Etapa 4. Permita o firewalld para a Segurança.

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

Etapa 5. Adicionar regras permanentes à zona padrão para permitir o HTTP, os https e os serviços de raio.

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

Etapa 6. Firewalld do Reload para que as mudanças tomem o efeito.

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

FreeRADIUS

A fim configurar FreeRADIUS para usar MariaDB, siga estas etapas.

Etapa 1. Importe o esquema do base de dados RADIUS para povoar o base de dados RADIUS.

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

Etapa 2. Crie um link macio para a língua de consulta estruturada (SQL) sob **/etc/raddb/mods-enabled**.

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

Etapa 3. Configurar o módulo /raddb/mods-available/sql SQL e mude os parâmetros da Conexão ao base de dados à série seu ambiente.

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

A seção SQL deve olhar similar a esta.

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

Etapa 4. Mude o direito de grupo de **/etc/raddb/mods-enabled/sql ao** radiusd.

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

WLC como o cliente do Authentication, Authorization, and Accounting (AAA) em FreeRADIUS

Etapa 1. Edite **/etc/raddb/clients.conf** a fim ajustar a chave compartilhada para o WLC.

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

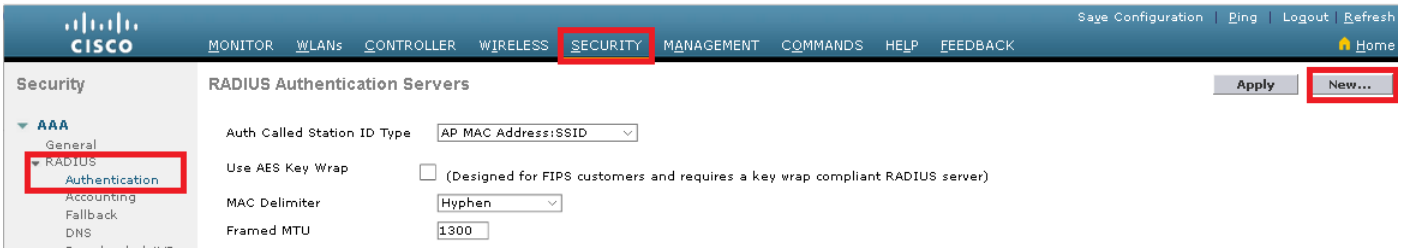
Etapa 2. Na parte inferior, adicionar seu endereço IP de Um ou Mais Servidores Cisco ICM NT do controlador e a chave compartilhada.

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

FreeRADIUS como o servidor Radius no WLC

GUI:

Etapa 1. Abra o GUI do WLC e navegue à **SEGURANÇA > ao RAIO > à autenticação > novo** segundo as indicações da imagem.



Etapa 2. Encha a informação do servidor Radius segundo as indicações da imagem.

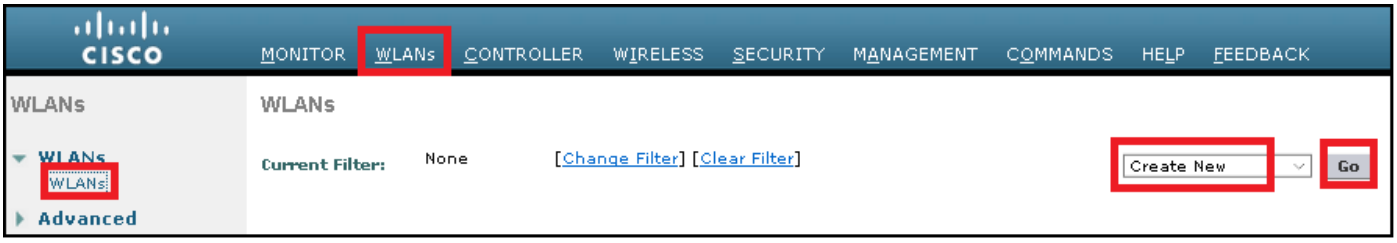
CLI:

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

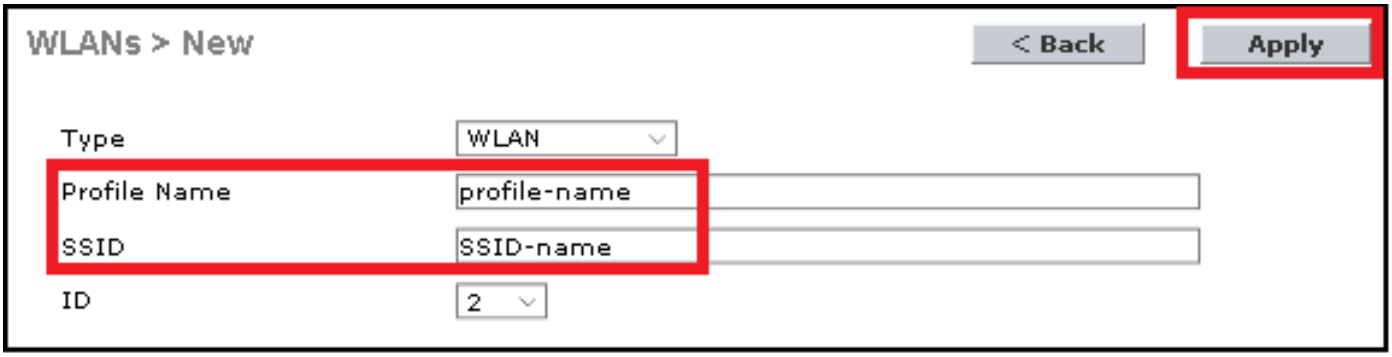
WLAN

GUI:

Etapa 1. Abra o GUI do WLC e navegue a **WLAN > criam novo > Goas** mostrado na imagem.



Etapa 2. Escolha um nome para o Service Set Identifier (SSID) e o perfil, a seguir clique **Applyas** mostrado na imagem.



CLI:

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

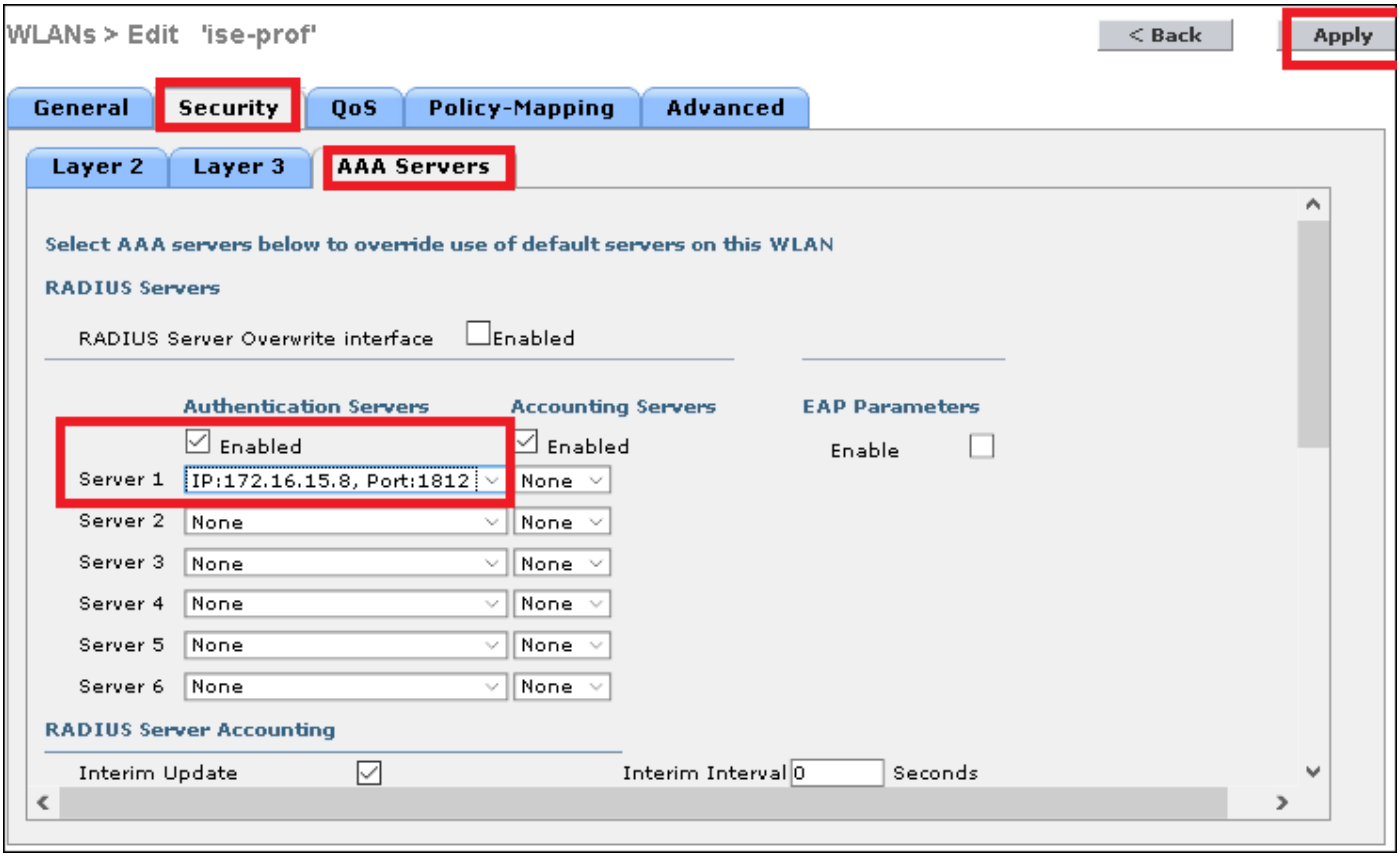
Etapa 3. Atribua o servidor Radius ao WLAN.

CLI:

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

GUI:

Navegue à **Segurança > aos servidores AAA** e escolha o servidor Radius desejado, a seguir clique-o **aplicam-se** segundo as indicações da imagem.



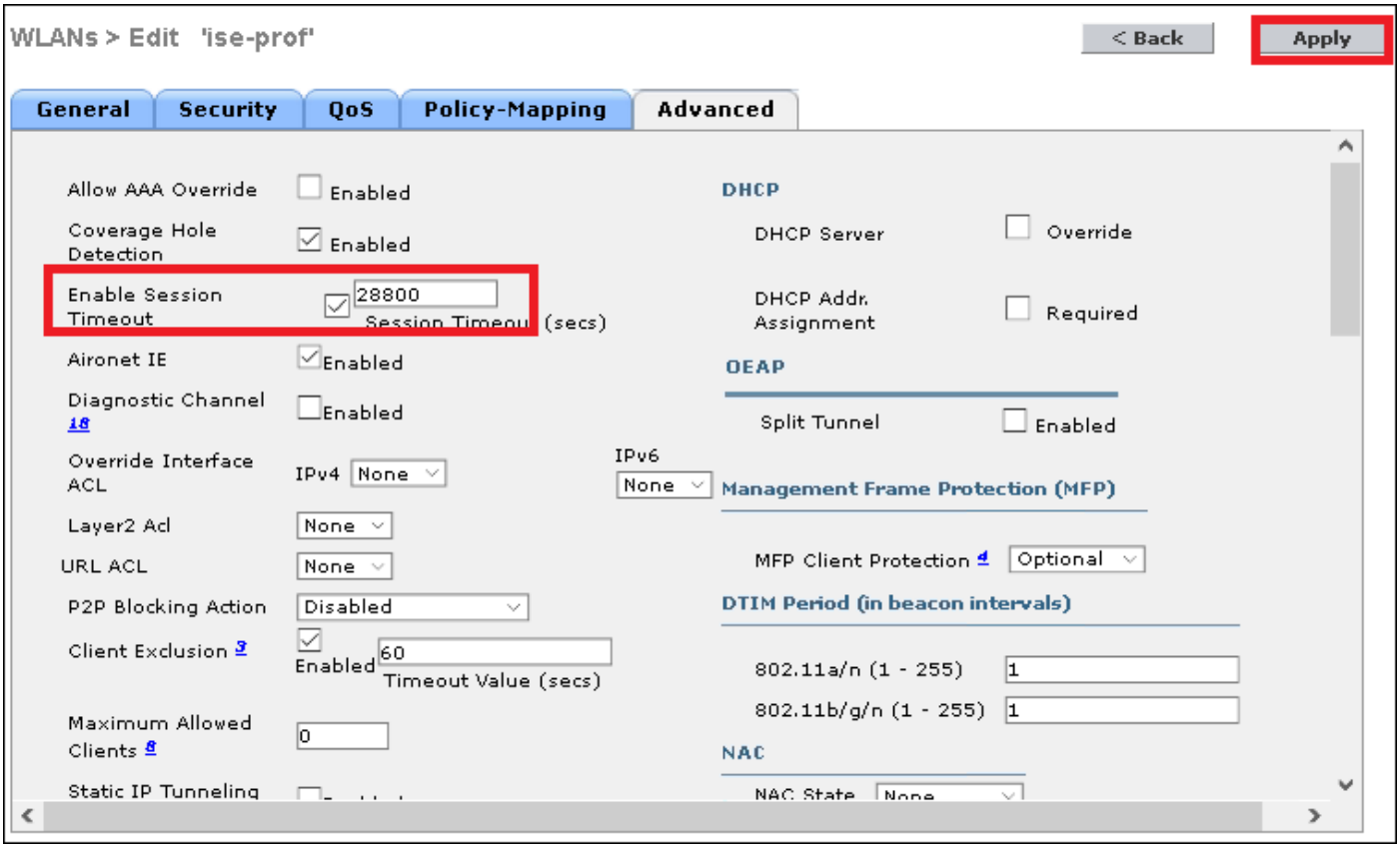
Etapa 4. Aumente opcionalmente o tempo de sessão.

CLI:

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

GUI:

Navegue a **avançado > permitem o timeout de sessão > o** clique **aplicam-se** segundo as indicações da imagem.



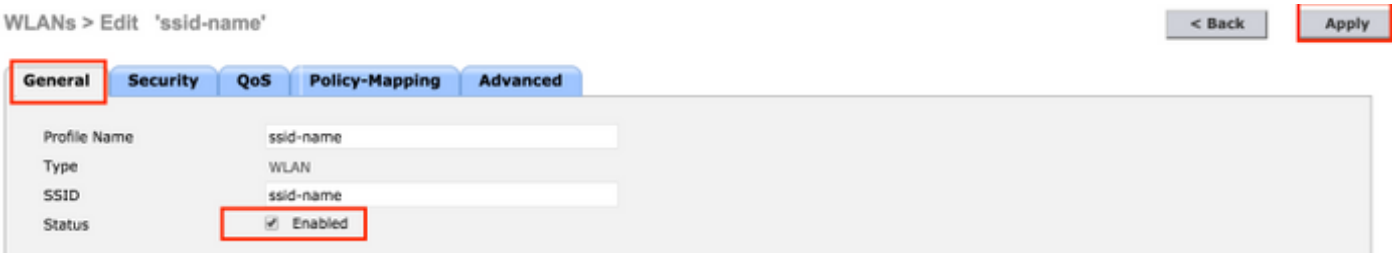
Etapa 5. Permita o WLAN.

CLI:

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

GUI:

Navegue ao **general > ao estado > ao tiquetaque permitido > clique aplicam-se** segundo as indicações da imagem.



Adicionar usuários ao base de dados do freeRADIUS

Àrevelia os clientes usam protocolos PEAP, porém apoio do freeRadius outros métodos (não cobertos neste guia).

Etapa 1. Edite o arquivo **/etc/raddb/users**.

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

Etapa 2. Na parte inferior do arquivo adicione a informação de usuários. Neste exemplo, o

usuário1 é o username e cisco123 a senha.

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

Etapa 3. Reinício FreeRadius.

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

Certificados no freeRADIUS

FreeRADIUS vem com um certificado de Authoritiy da certificação do padrão (CA) e um certificado do dispositivo que sejam armazenados no trajeto /etc/raddb/certs. O nome destes Certificados é ca.pem e server.pem server.pem é o certificado que os clientes recebem quando examinarem o processo de autenticação. Se você precisa de atribuir um certificado diferente para a autenticação de EAP você pode simplesmente suprimir d e salvar os novos no mesmo trajeto com esse exato o mesmo nome.

Configuração de dispositivo final

Configurar uma máquina de Windows do portátil para conectar a um SSID com a autenticação do 802.1x e a versão 2 PEAP/MS-CHAP (versão de Microsoft do protocolo challenge-handshake authentication).

A fim criar o perfil WLAN na máquina dos indicadores lá seja duas opções:

1. Instale o certificado auto-assinado na máquina para validar e confiar o server do freeRADIUS a fim terminar a autenticação
2. Contorneie a validação do servidor Radius e confie todo o servidor Radius usado para executar a autenticação (não recomendada, como pode se transformar uma questão de segurança). A configuração para estas opções é explicada na configuração de dispositivo final - crie o perfil WLAN.

Importe o certificado de FreeRADIUS

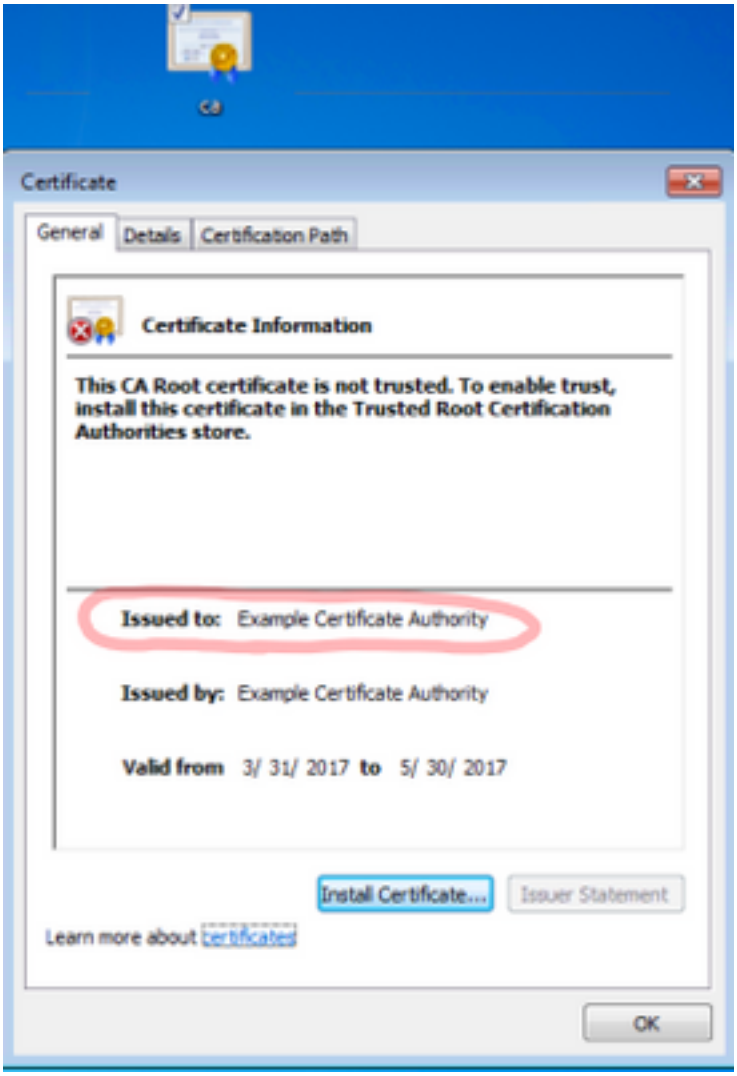
Se você usa os Certificados do padrão instalados no freeRADIUS, siga estas etapas a fim importar o certificado EAP do server do freeRADIUS no dispositivo final.

Etapa 1. Obtenha o CERT de FreeRadius:

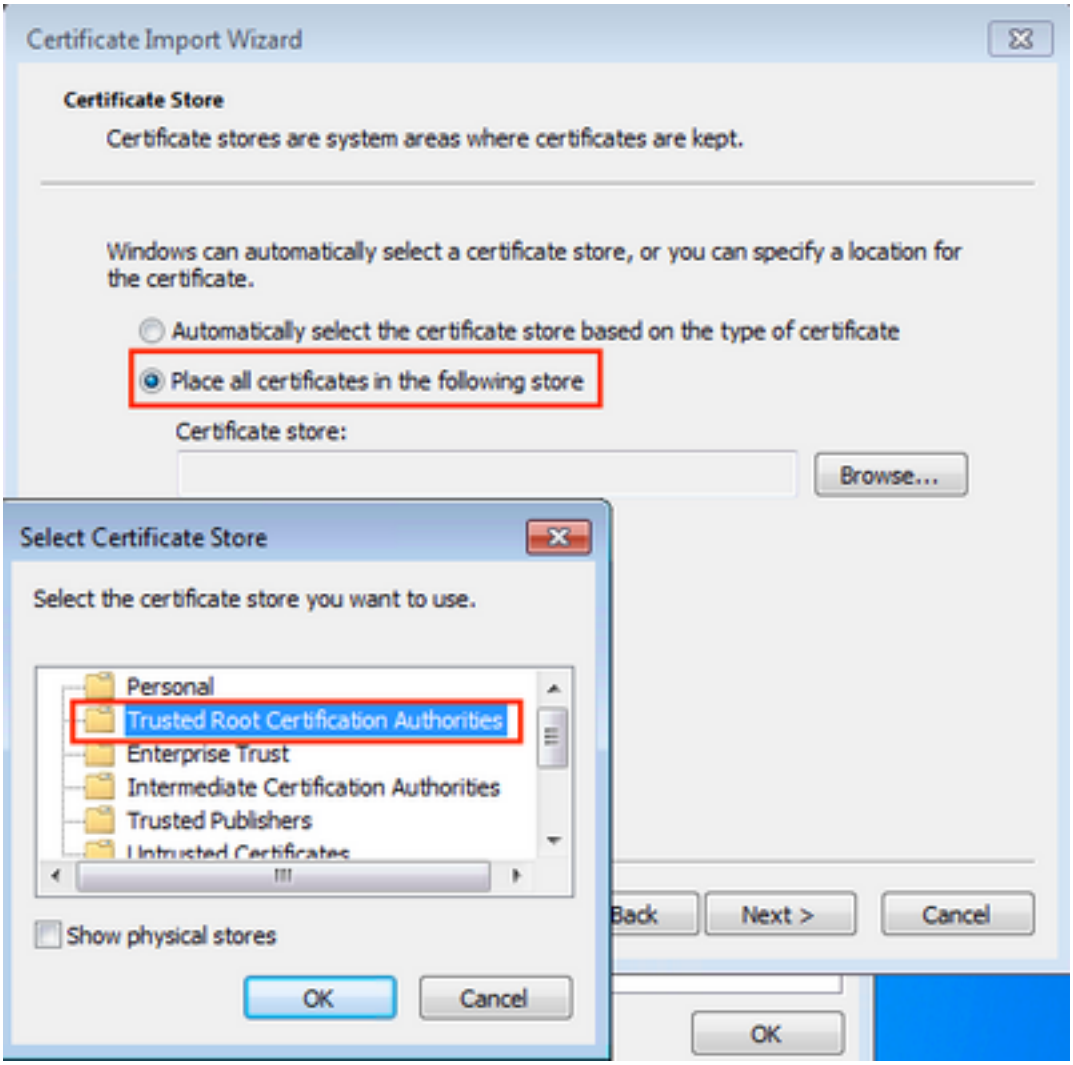
```
[root@tac-mxwireless ~]#mysql_secure_installation
```

Etapa 2. A cópia e cola a saída da etapa precedente em um arquivo de texto e muda a extensão a .crt

Etapa 3. Fazer duplo clique o arquivo e seleto instale o certificado… segundo as indicações da imagem.

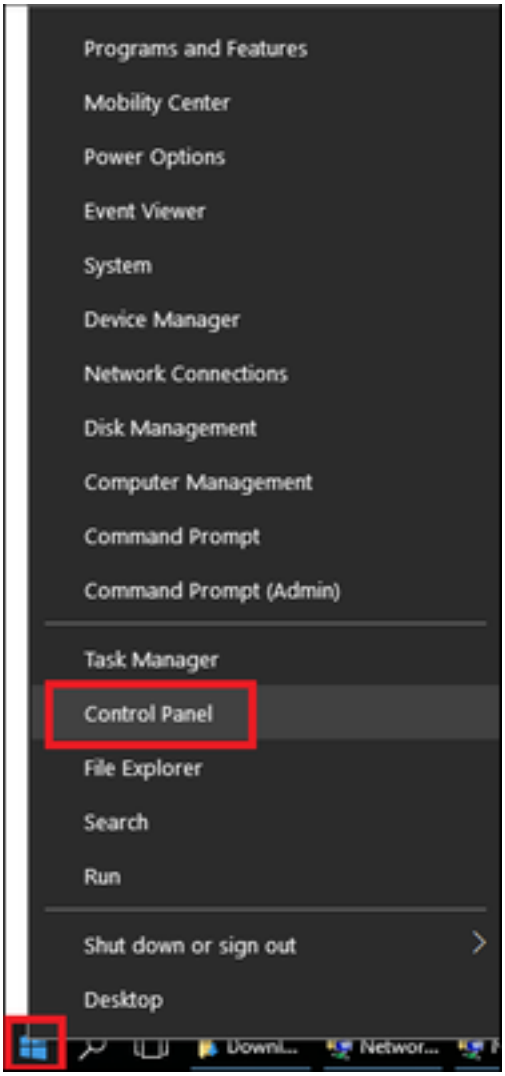


Etapa 4. Instale o certificado na loja das **Autoridades de certificação de raiz confiável** segundo as indicações da imagem.

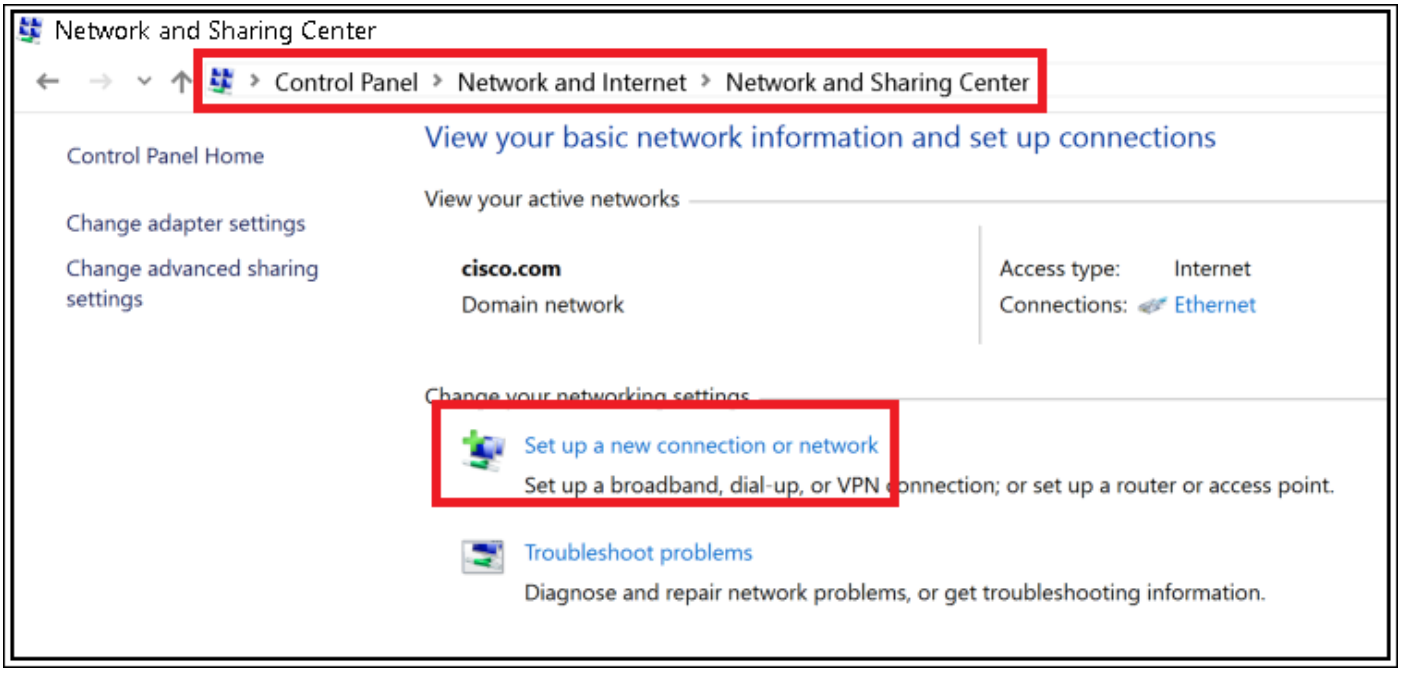


Crie o perfil WLAN

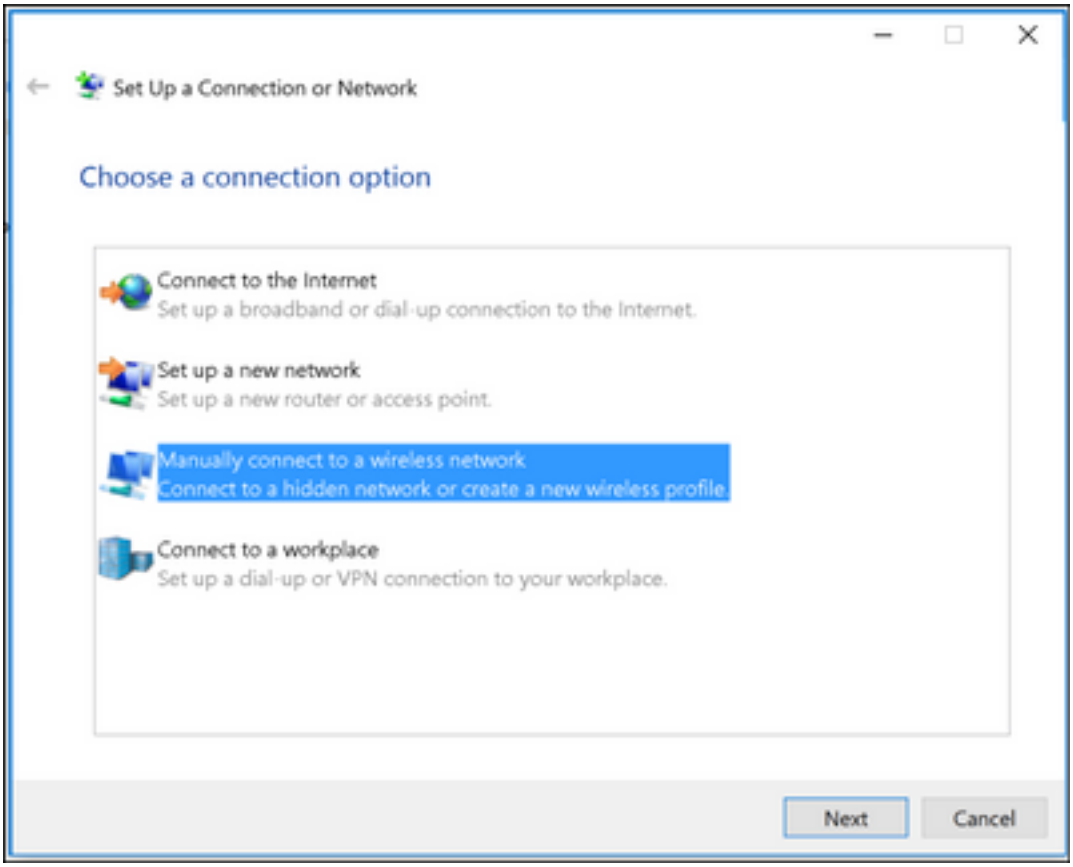
Etapa 1. Clicar com o botão direito no ícone do começo e selecione o **Control Panel** segundo as indicações da imagem.



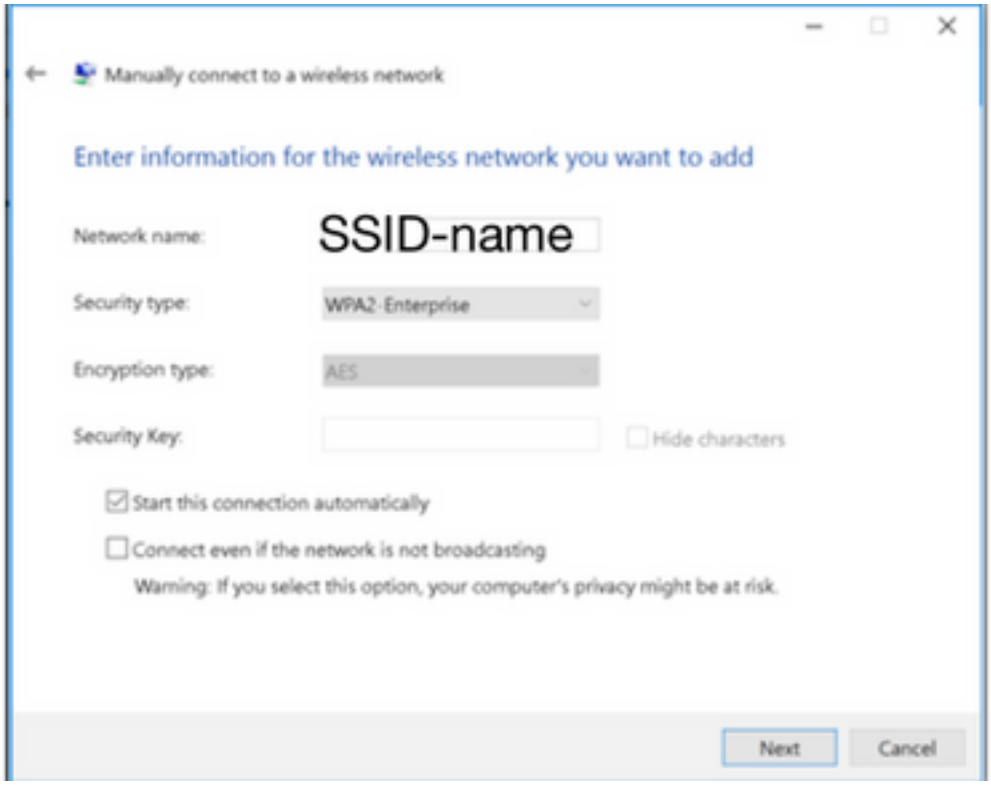
Etapa 2. Navegue à **rede e o Internet > a rede e o centro > o clique da partilha estabelecem uma nova conexão ou uma rede** segundo as indicações da imagem.



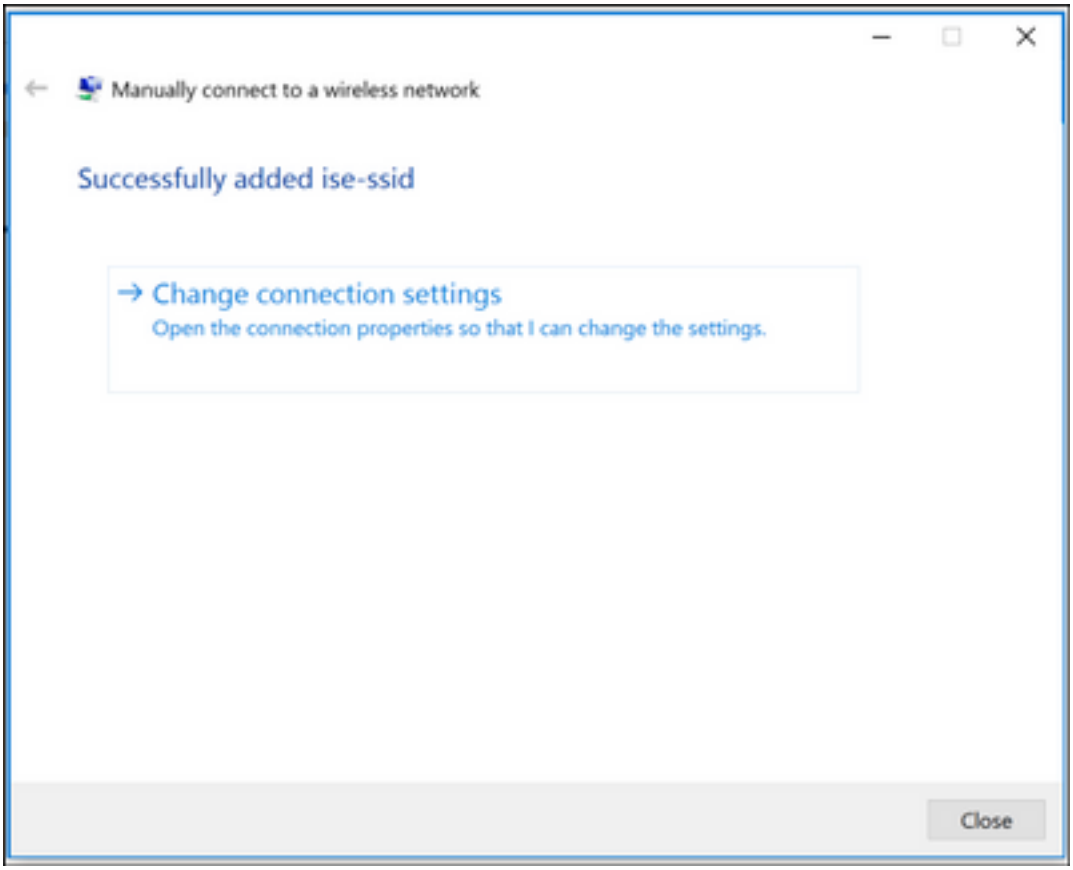
Etapa 3. Selecione **conectam manualmente a uma rede Wireless** e clicam **Nextas** mostrado na imagem.



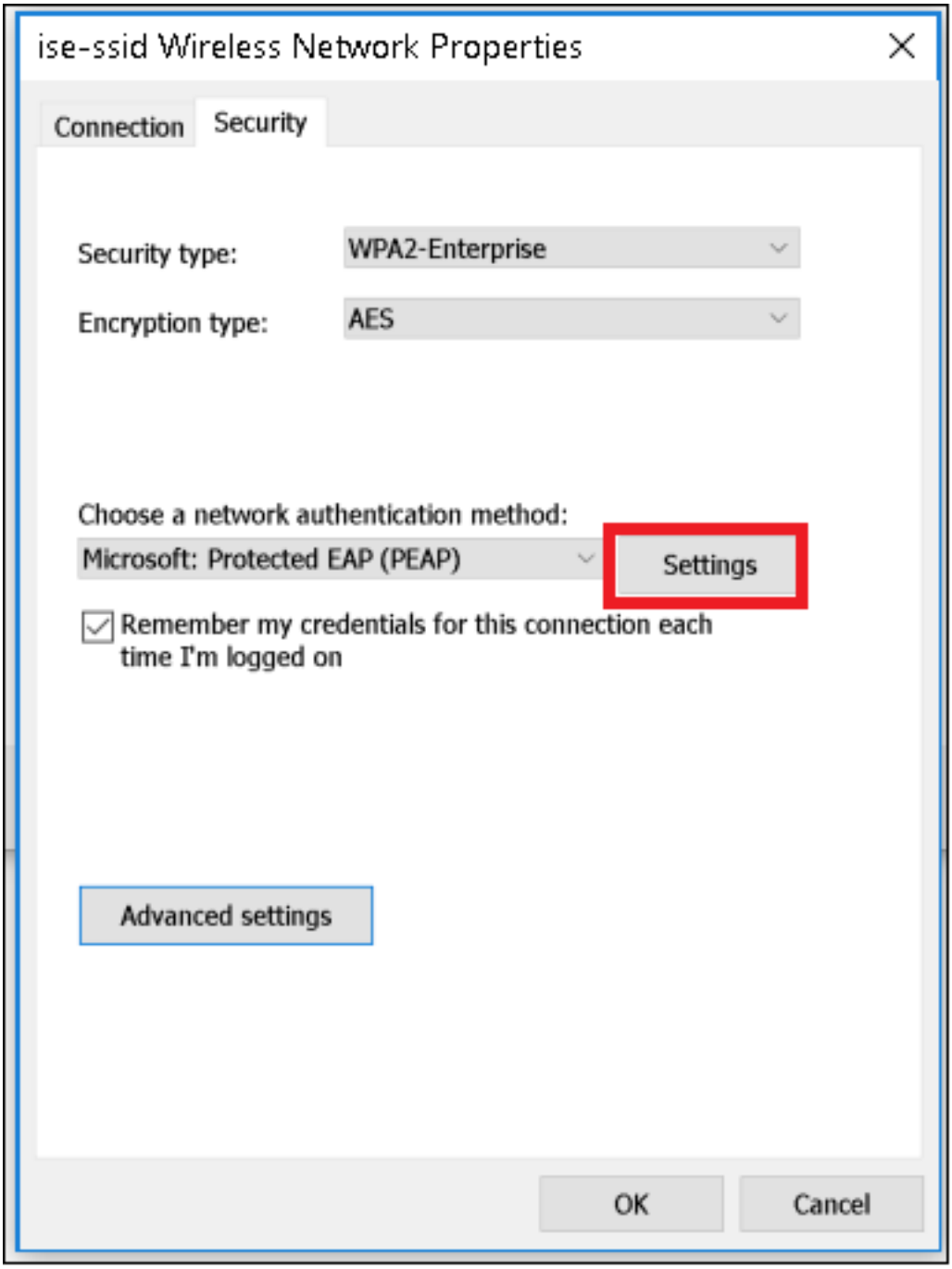
Etapa 4. Incorpore a informação com o nome do tipo WPA2-Enterprise SSID e de Segurança e clique-a **em seguida** segundo as indicações da imagem.



Etapa 5. Selecione **configurações de conexão da mudança** a fim personalizar a configuração do perfil WLAN segundo as indicações da imagem.



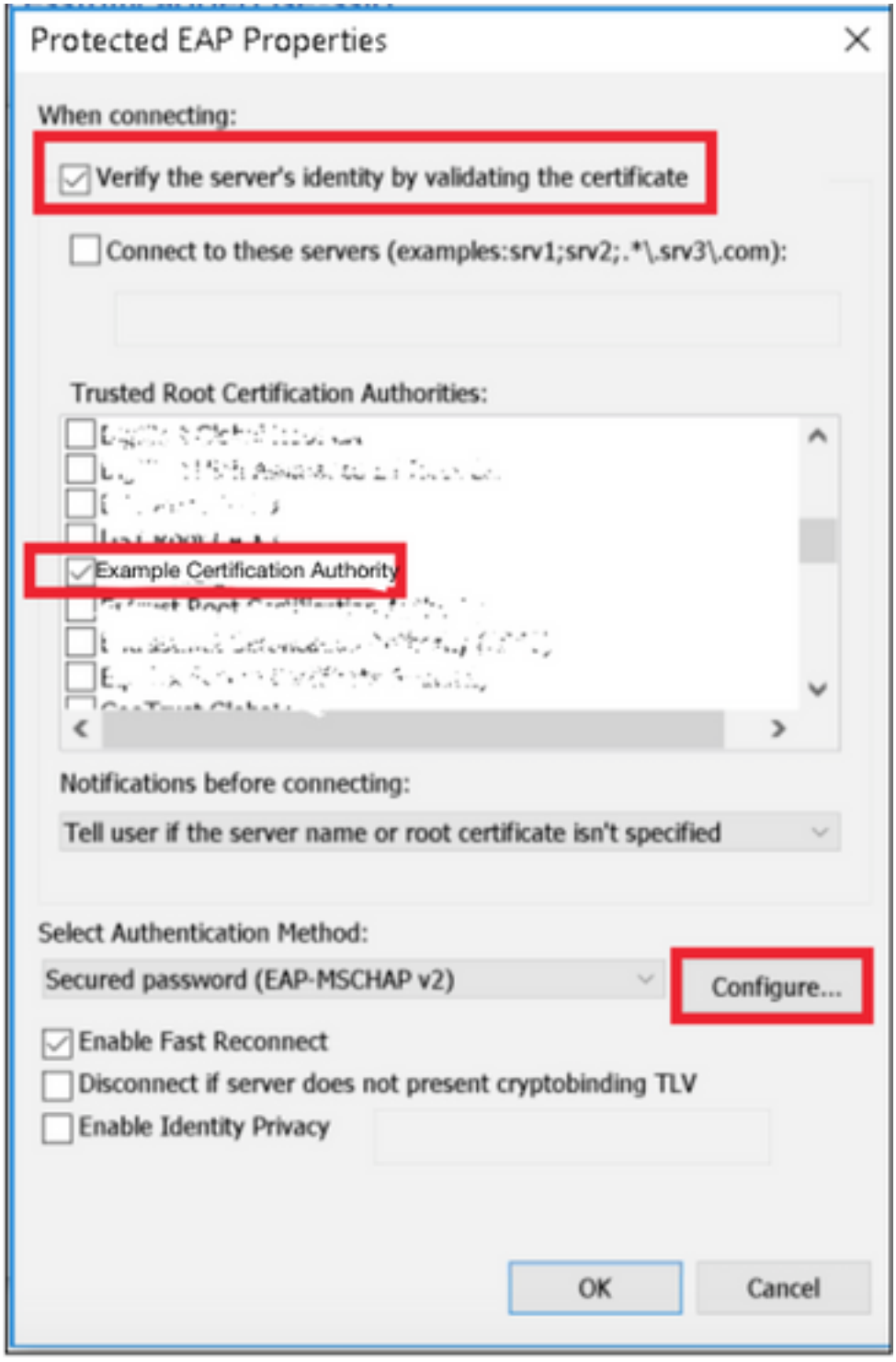
Etapa 6. Navegue à **ABA de segurança** e clique **ajustes** segundo as indicações da imagem.

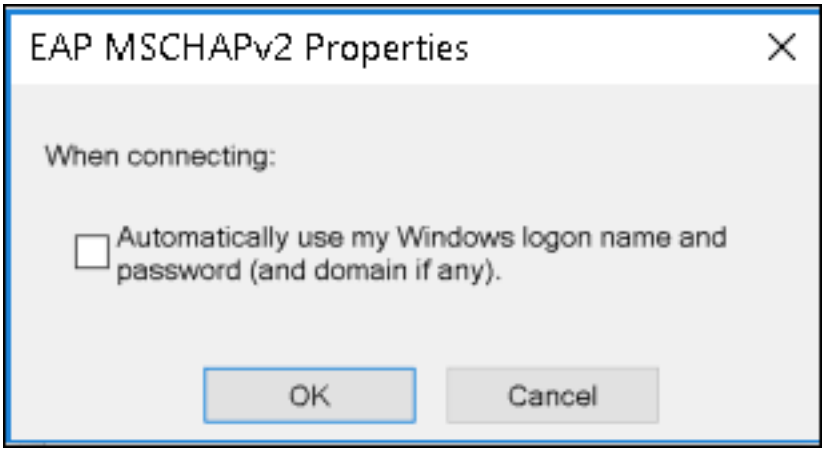


Etapa 7. Escolha se o servidor Radius é validado ou não.

Se sim, permita **verificam a identidade do server validando o certificado** e das **Autoridades de certificação de raiz confiável:** aliste seleto o certificado auto-assinado do freeRADIUS.

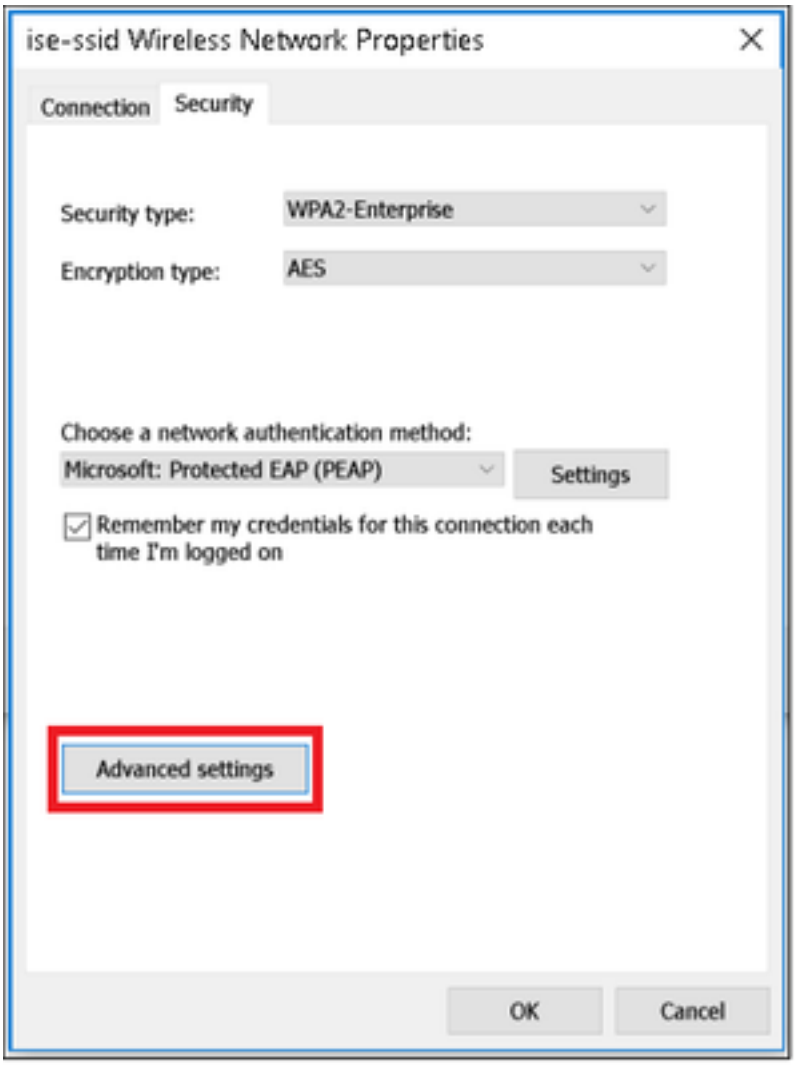
Em seguida esse seleto **configura** e desabilita **automaticamente o uso meus nome de logon e senha de Windows…**, a seguir clica a **APROVAÇÃO** segundo as indicações das imagens.

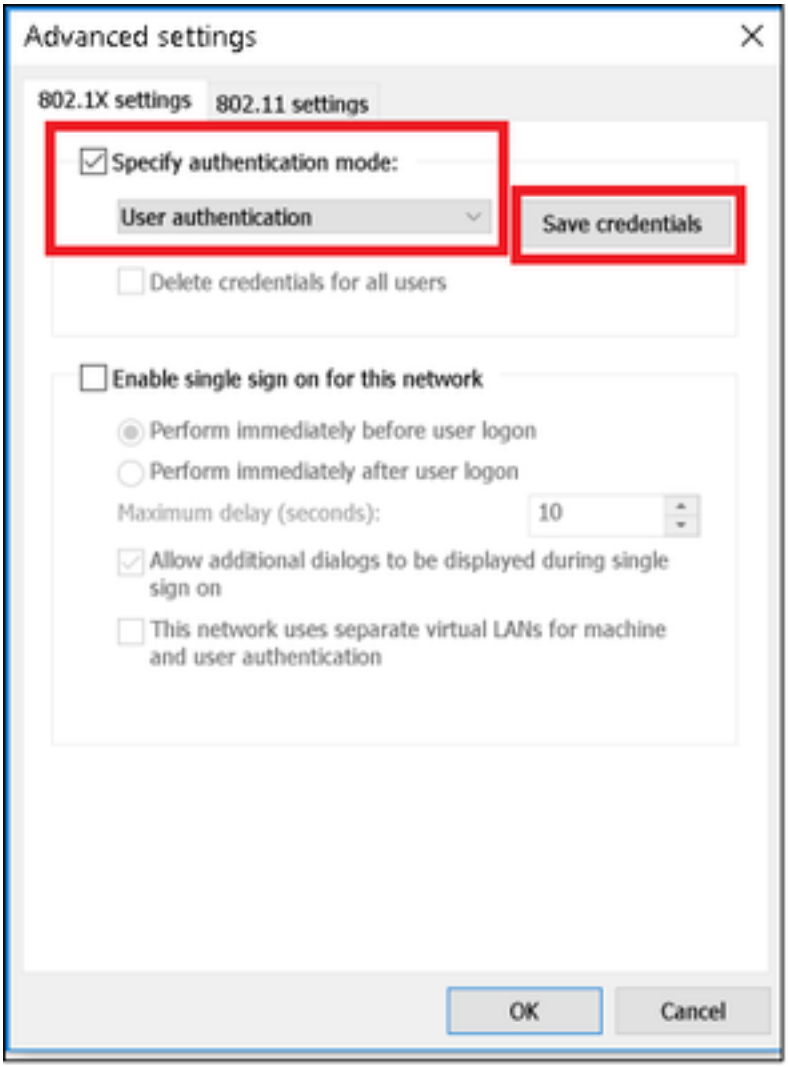


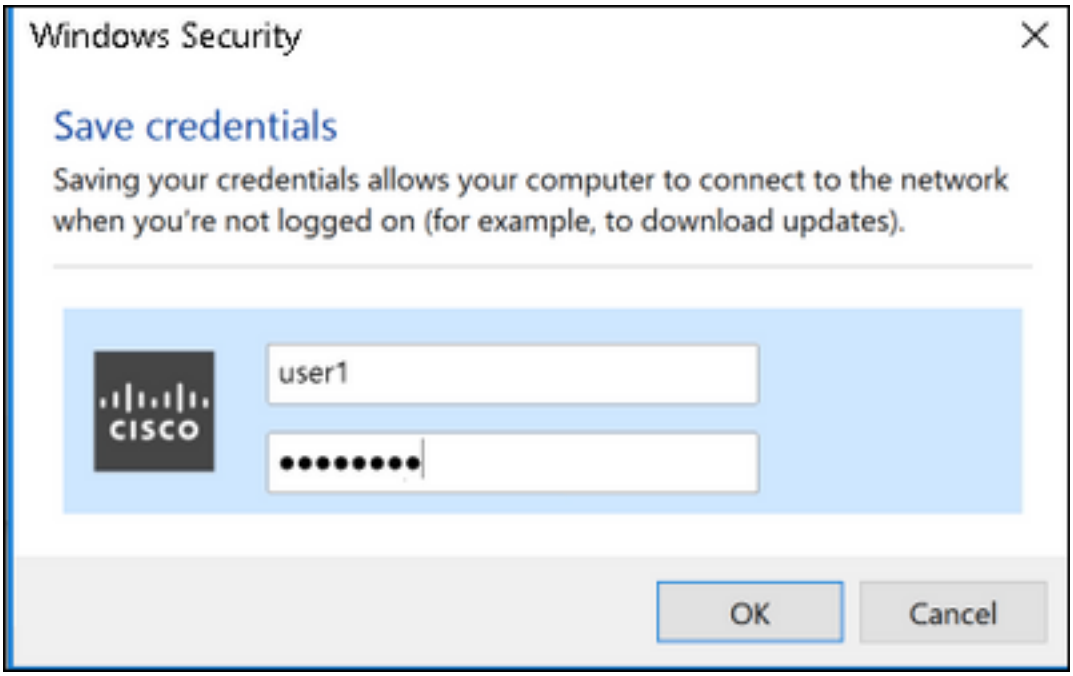


Etapa 8. Configurar as credenciais do usuário.

Uma vez de volta à ABA de segurança, selecione **ajustes avançados**, especifique o modo de autenticação como a **autenticação de usuário** e salvar as credenciais que foram configuradas no freeRADIUS a fim autenticar o usuário, segundo as indicações das imagens.







Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Processo de autenticação no WLC

Execute os comandos seguintes a fim monitorar o processo de autenticação para um usuário específico:

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

Para que uma maneira fácil leia debugar saídas do cliente, usam o Sem fio debugam a ferramenta do analisador:

O Sem fio debuga o analisador

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.