配置802.1x -与FreeRadius和WLC 8.3的PEAP

目录

简介

本文解释如何设置一WLAN (无线局域网)与802.1x安全和PEAP (已保护可扩展的认证协议)作为EAP (可扩展的认证协议)。FreeRADIUS使用作为外部远程验证拨入用户服务(RADIUS)服务器。

先决条件

思科建议您有基础知识Linux，精力编辑器和AireOS无线局域网控制器(WLCs)。

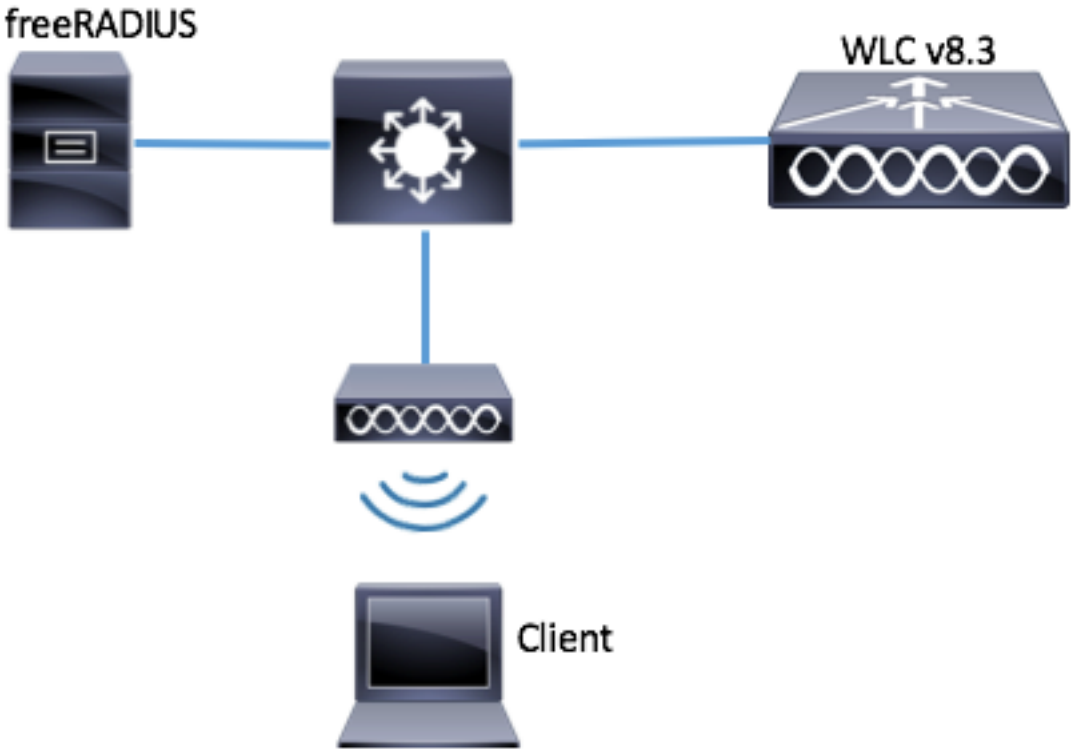
> **注意**： 本文打算提供读者在PEAP-MS-CHAPv2验证的一个freeRADIUS服务器要求的配置的一示例。在本文提交的freeRADIUS服务器配置在实验室里测试了并且被发现工作正如所料。Cisco技术支持中心(TAC)不支持freeRADIUS服务器配置。

使用的组件

- CentOS7或Red帽子恩特普赖斯Linux 7 (RHEL7) (推荐的1 GB RAM和至少20 GB HDD)
- WLC 5508个v8.3
- MariaDB (MySQL)
- FreeRADIUS
- PHP 7

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

网络图



配置

安装httpd服务器和MariaDB

步骤1.运行这些命令安装httpd服务器和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
```

步骤2.启动并且启用httpd (Apache)和MariaDB服务器。

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

步骤3.配置最初的MariaDB设置获取它。

```
[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!
```

步骤4.配置freeRADIUS的数据库(请使用配置的同样密码在步骤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
```

安装在CentOS 7的PHP 7

步骤1.运行这些命令安装在CentOS7的PHP 7。

```
[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
```

安装FreeRADIUS

步骤1.运行此命令安装FreeRADIUS。

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

第二步：在mariadb.service以后做*radius.servicestart*。

运行此指令：

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

添加在**[Unit]**部分的一条线路：

```
After=mariadb.service
```

[Unit]部分必须如下所示:

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

步骤3.开始的启动和enable (event) freeradius在启动。

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

步骤4.安全的Enable (event) firewalld。

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

步骤5.增加永久性规则到默认区域允许http、https和RADIUS服务。

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

步骤6.更改的重新加载firewalld能生效。

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

配置FreeRADIUS

为了配置FreeRADIUS使用MariaDB，请遵从这些步骤。

步骤1.导入RADIUSdatabase方案填充RADIUS数据库。

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

步骤2.创建SQL的一条软链在*/etc/raddb/mods-enabled*下

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

步骤3.配置SQL模块*/raddb/mods-available/sql*并且更改数据库连接参数到套件您的环境。

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

SQL部分一定看起来类似于下面。

```
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"
```

步骤4.崔凡吉莱*/etc/raddb/mods-enabled/sql*组对radiusd的。

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

配置WLC作为FreeRADIUS的AAA客户端

步骤1.编辑*/etc/raddb/clients.conf*为了设置WLC的共享密钥。

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

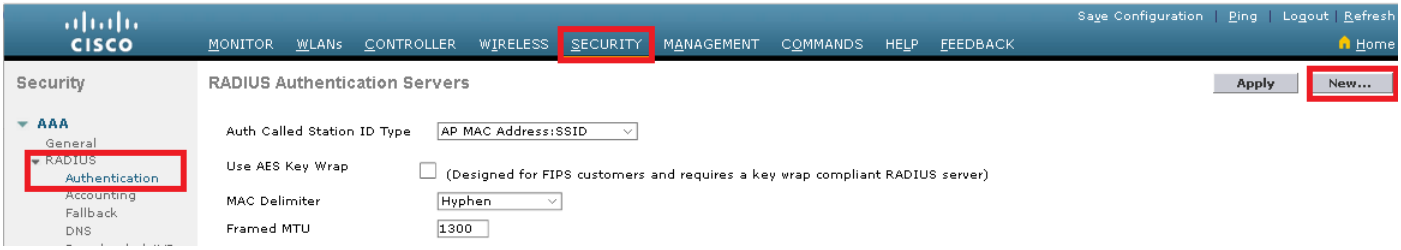
第二步：在底部请添加您的控制器IP地址和共享密钥。

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

配置FreeRADIUS作为在WLC的RADIUS服务器

GUI ：

步骤1.打开WLC的GUI并且导航对**SECURITY>RADIUS >验证>New。**



步骤2.填装RADIUS服务器信息。

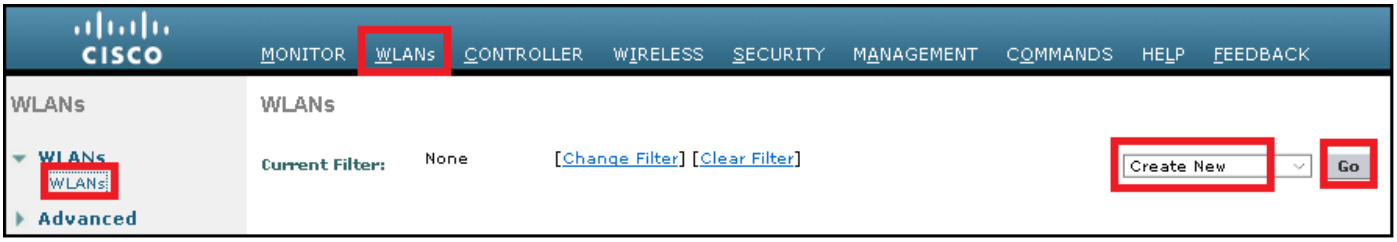
CLI ：

```
> 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>
```

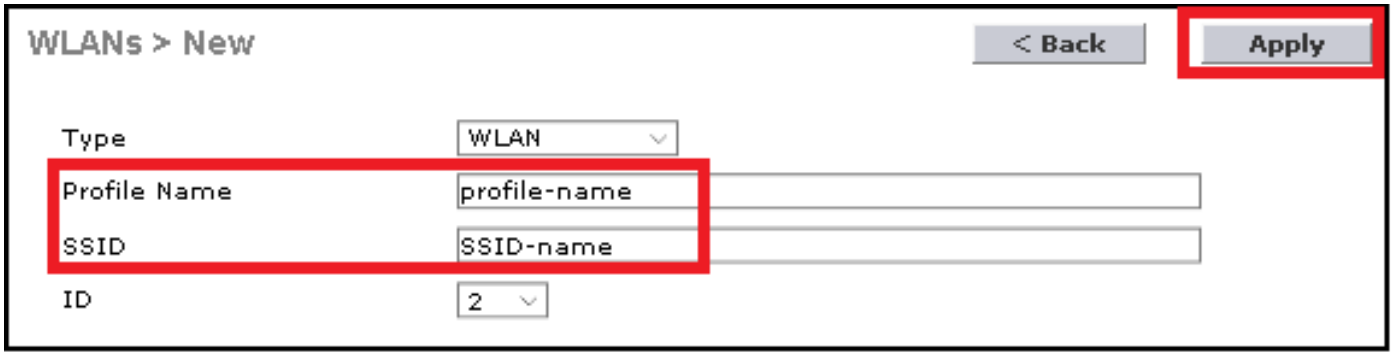
配置WLAN

GUI ：

步骤1.打开WLC的GUI并且导航对**WLAN >创建新>去。**



步骤2.选择一名称对于SSID和配置文件，然后单击**应用。**



CLI ：

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

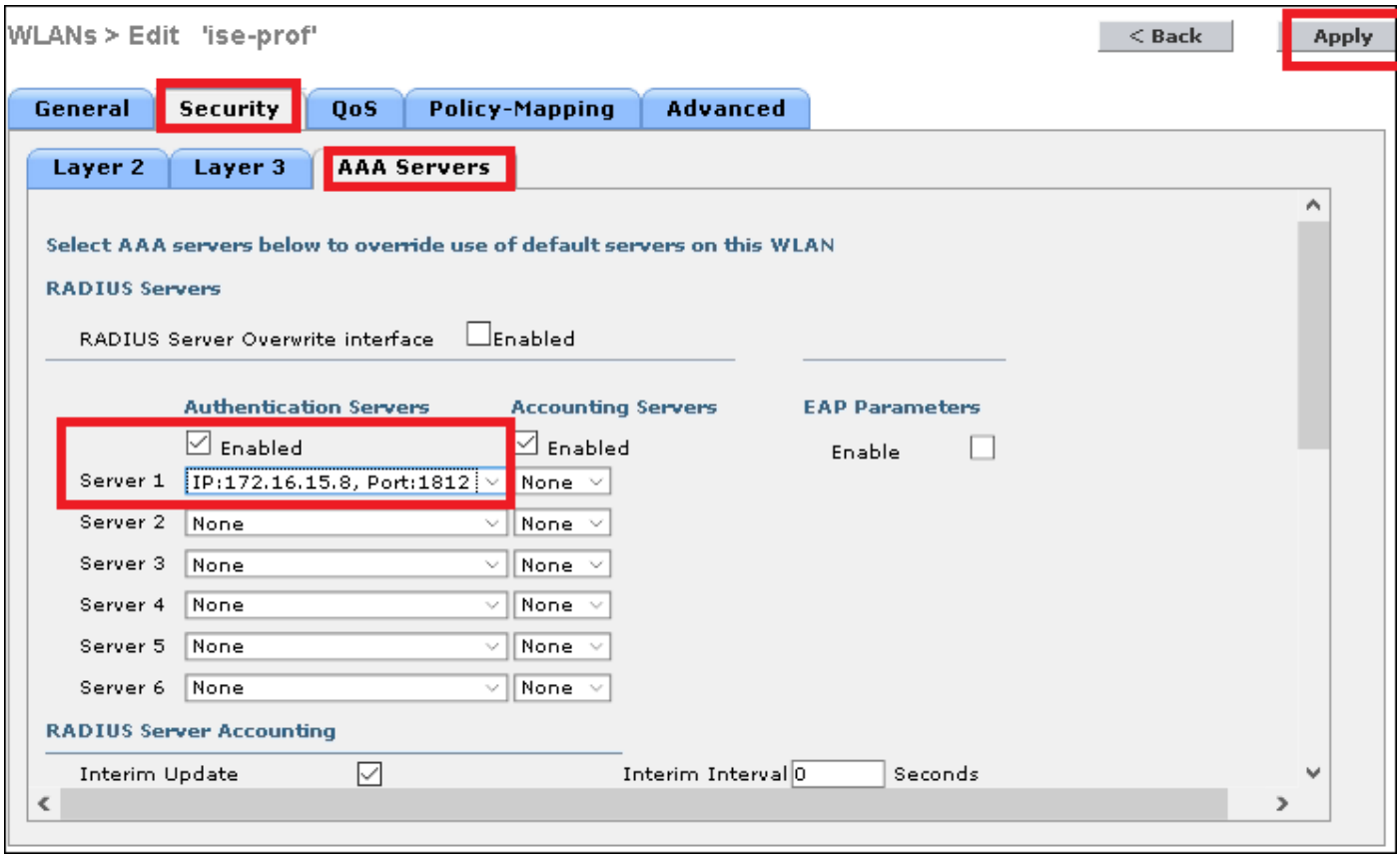
步骤3.分配RADIUS服务器到WLAN。

CLI ：

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

GUI ：

导航到**安全>AAA服务器**并且选择希望的RADIUS服务器，然后命中数**应用。**

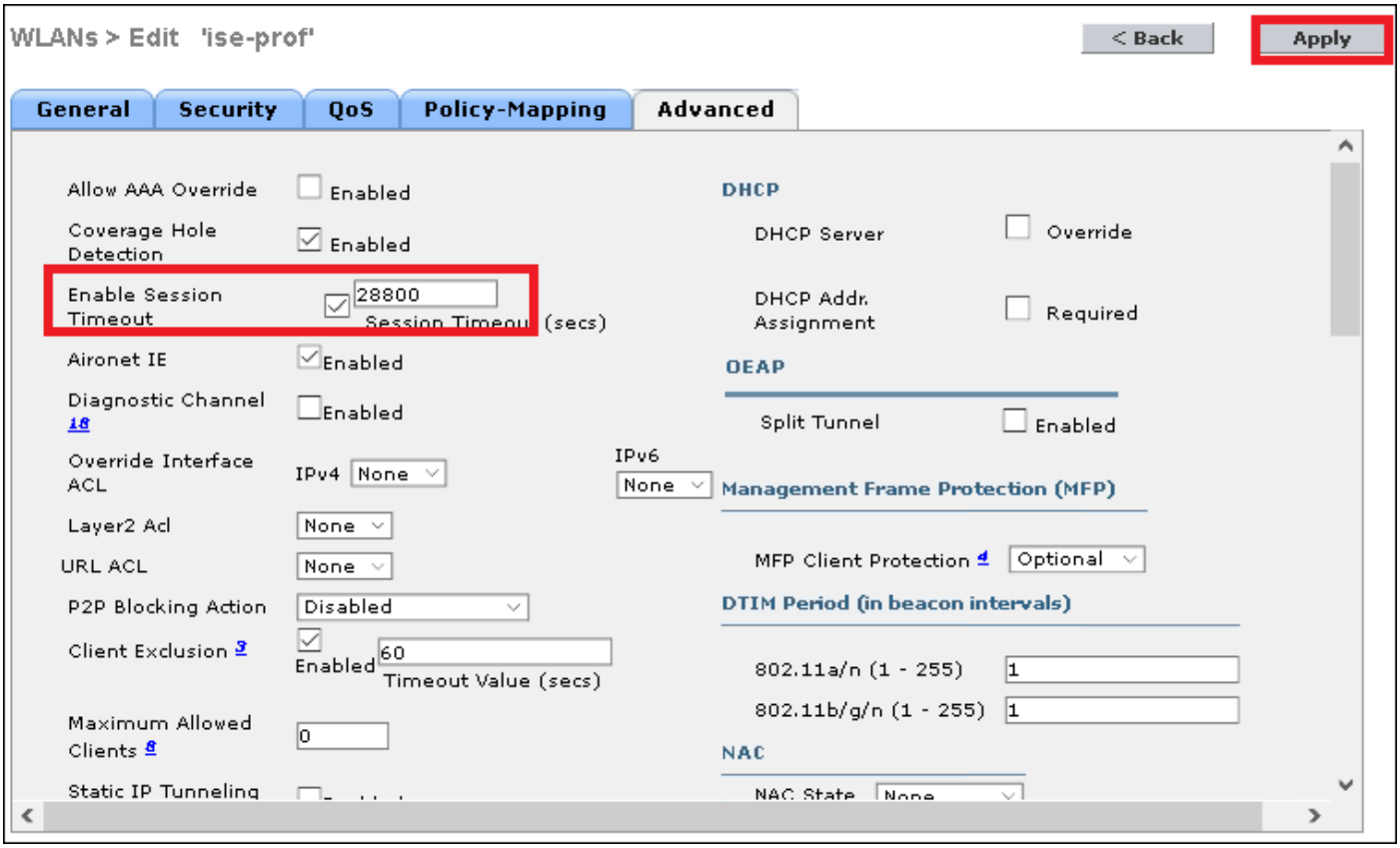


步骤4.随意地请增加会话超时

CLI ：

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

GUI ：

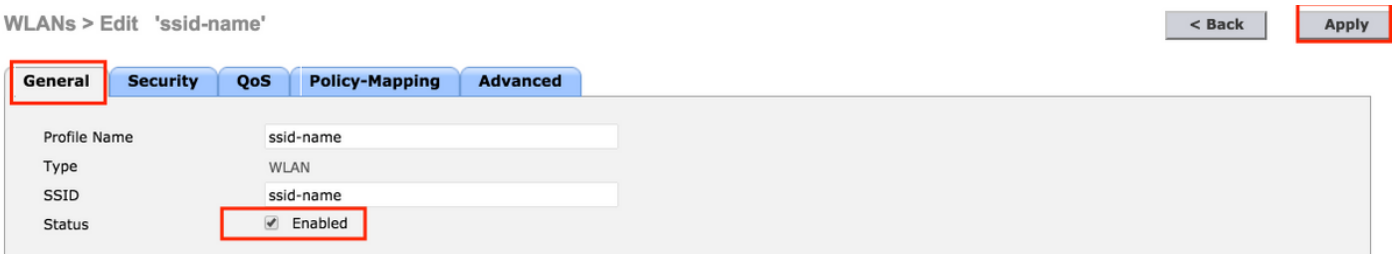


步骤5.启用WLAN

CLI ：

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

GUI ：



添加用户到freeRADIUS数据库

默认情况下客户端使用PEAP协议，然而freeRadius支持其他方法(没报道在此指南)。

步骤1.编辑文件*/etc/raddb/users*。

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

第二步：在文件的底部请添附用户信息。在本例中*user1*是用户名和*Cisco123*密码。

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

步骤3.重新启动FreeRadius。

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

在freeRADIUS的证书

FreeRADIUS附有在路径*/etc/raddb/certs*存储的默认CA (证明Authoritiy)证书和设备证书。 这些证书名称是*ca.pem和*server.pem *server.pemis*客户端将接收的*证书*，当他们通过认证过程时。如果需要分配EAP验证的一不同的身份验证您能删除他们，并且保存新的在有那的同一个路径请苛求同样名称。

终端设备配置

配置笔记本电脑Windows机器连接到与802.1x验证和PEAP/MS-CHAP (质询握手验证协议的Microsoft版本)版本2的一SSID。

要创建在那里Windows机器的WLAN配置文件请是两个选项：

1. 安装在计算机的自签名证书验证和委托freeRADIUS服务器为了完成验证
2. 绕过RADIUS服务器的验证并且委托用于的所有RADIUS服务器执行验证(没推荐，能变为安全问题)。这些选项的配置在终端设备配置解释-请创建WLAN配置文件-步骤xx。

终端设备配置-导入freeRADIUS证书

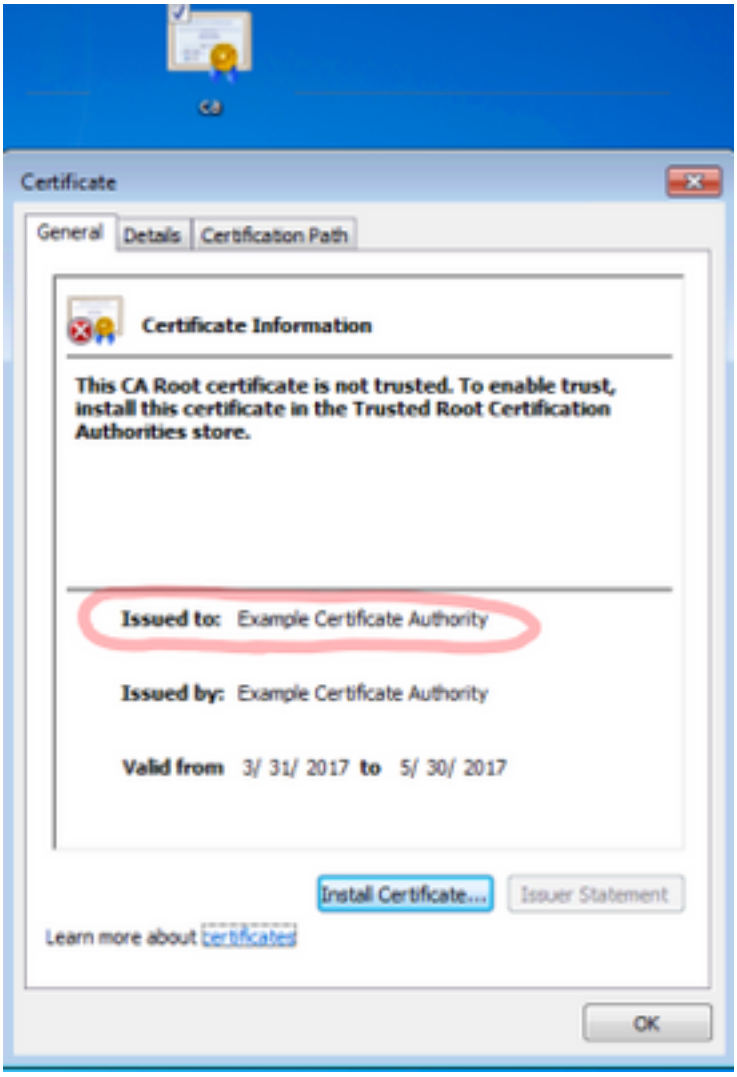
如果使用在freeRADIUS安装的默认证书，请遵从这些步骤为了导入从freeRADIUS服务器的EAP证书到终端设备。

步骤1.从FreeRadius获得cert ：

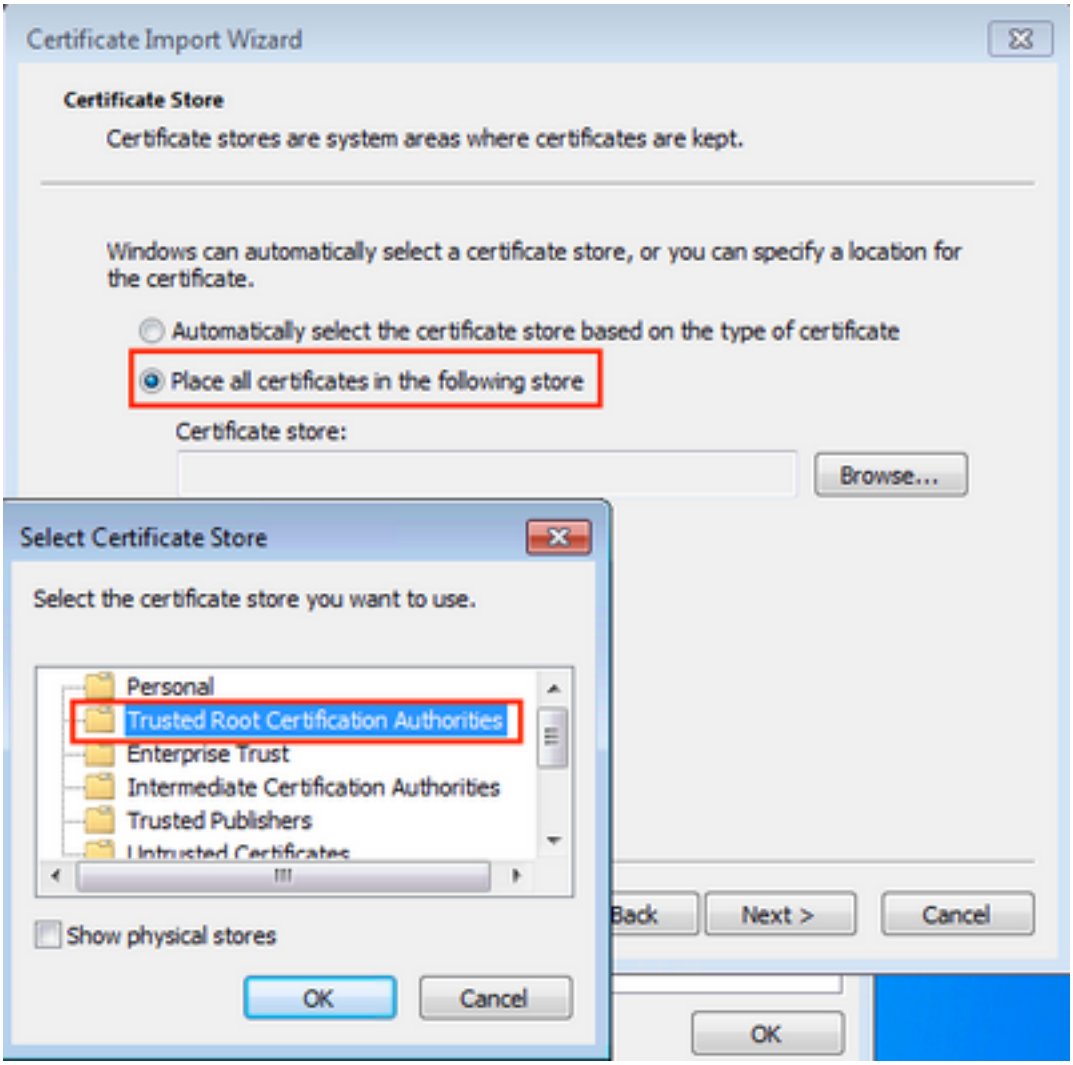
```
[root@tac-mxwireless ~]# cat /etc/raddb/certs/ca.pem

-----BEGIN CERTIFICATE-----
MIIE4TCCA8mgAwIBAgIJAKLmHn4eZLjBMA0GCSqGSIb3DQEBBQUAMIGTMQswCQYD
VQQGEwJGUjEPMA0GA1UECBMGUmFkaXVzMRIwEAYDVQQHEwlTb211d2hlcmUxFTAT
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-----
```

步骤2.复制和插入上一步的输出到文本文件并且更改分机对.crt

步骤3.双击文件并且选择**安装证书...**

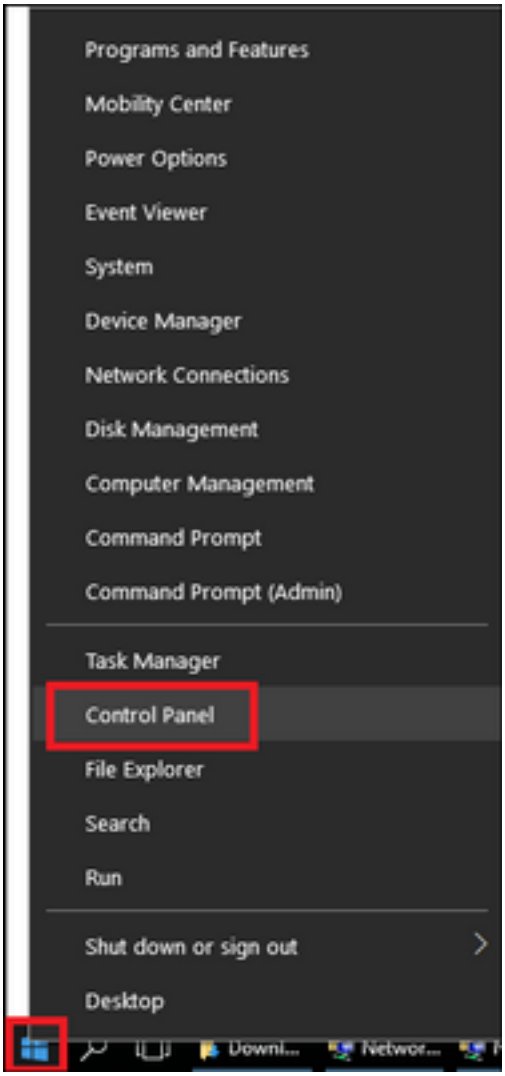


步骤4.安装证书到**可靠的根证书颁发机构**存储。

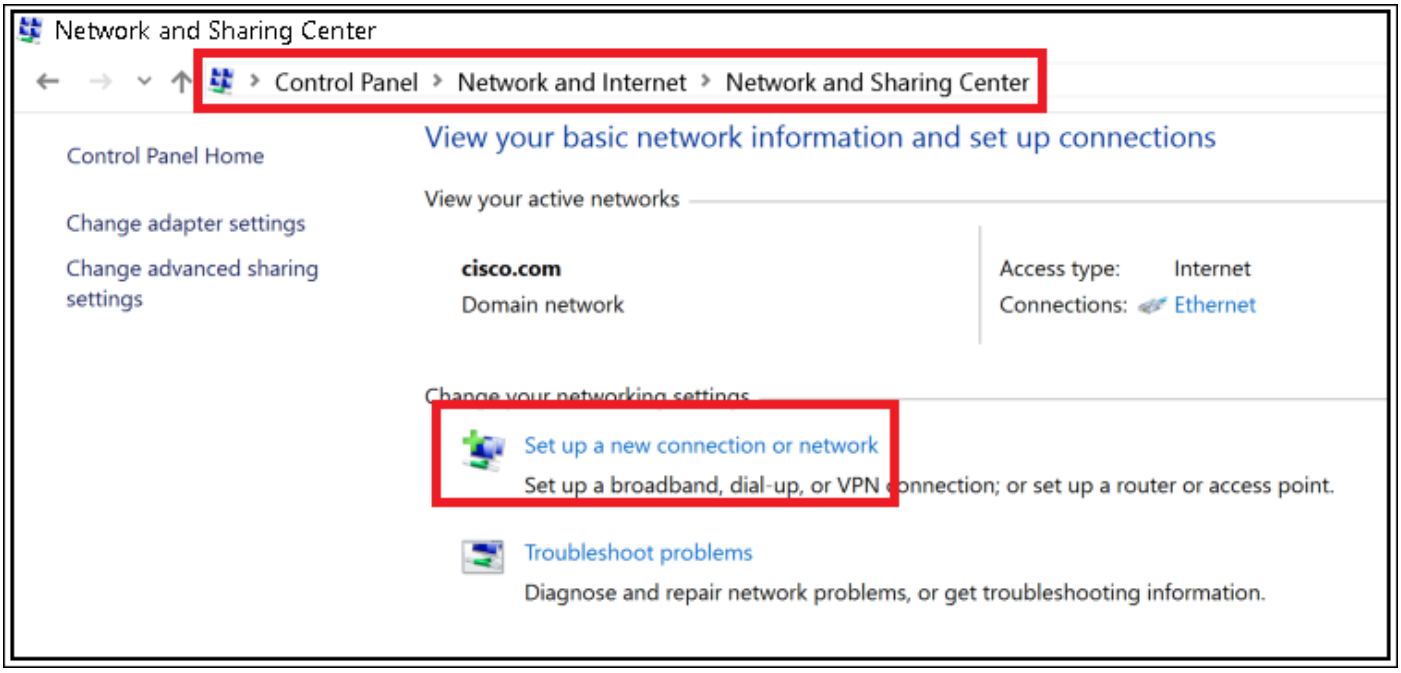


终端设备配置-创建WLAN配置文件

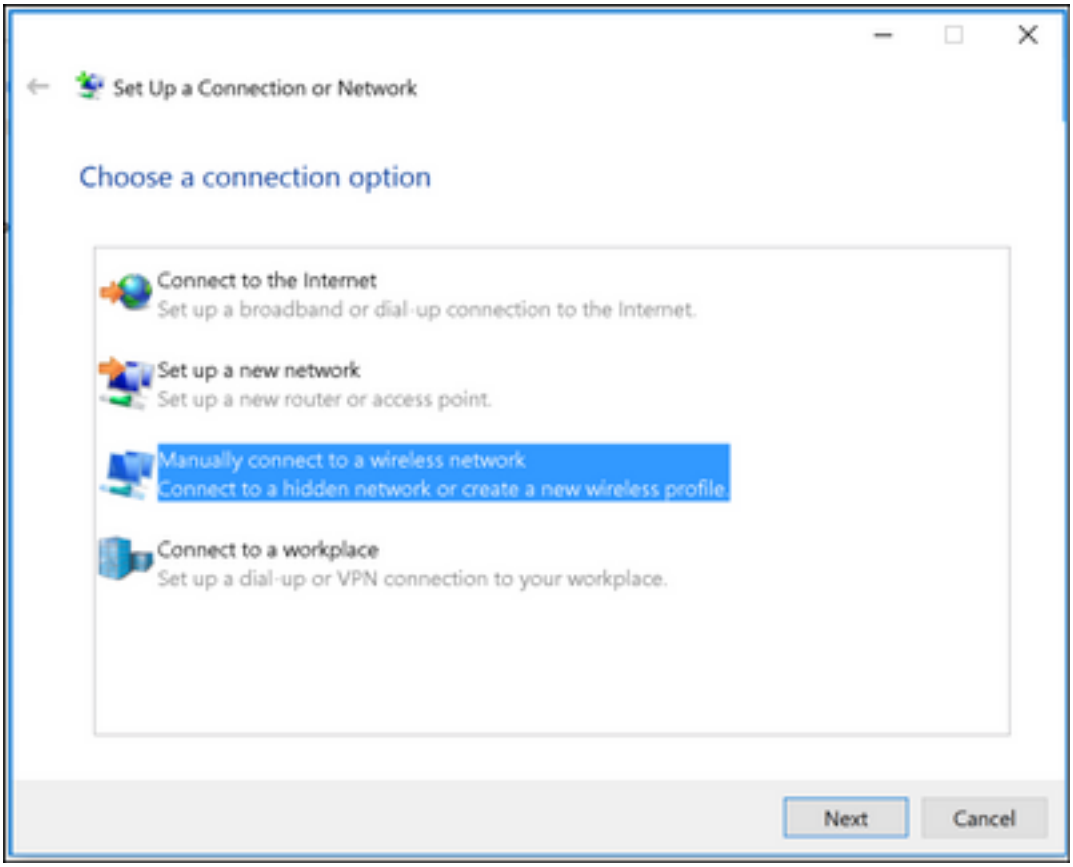
步骤1.在Start图标的右键单击和选择**控制面板**。



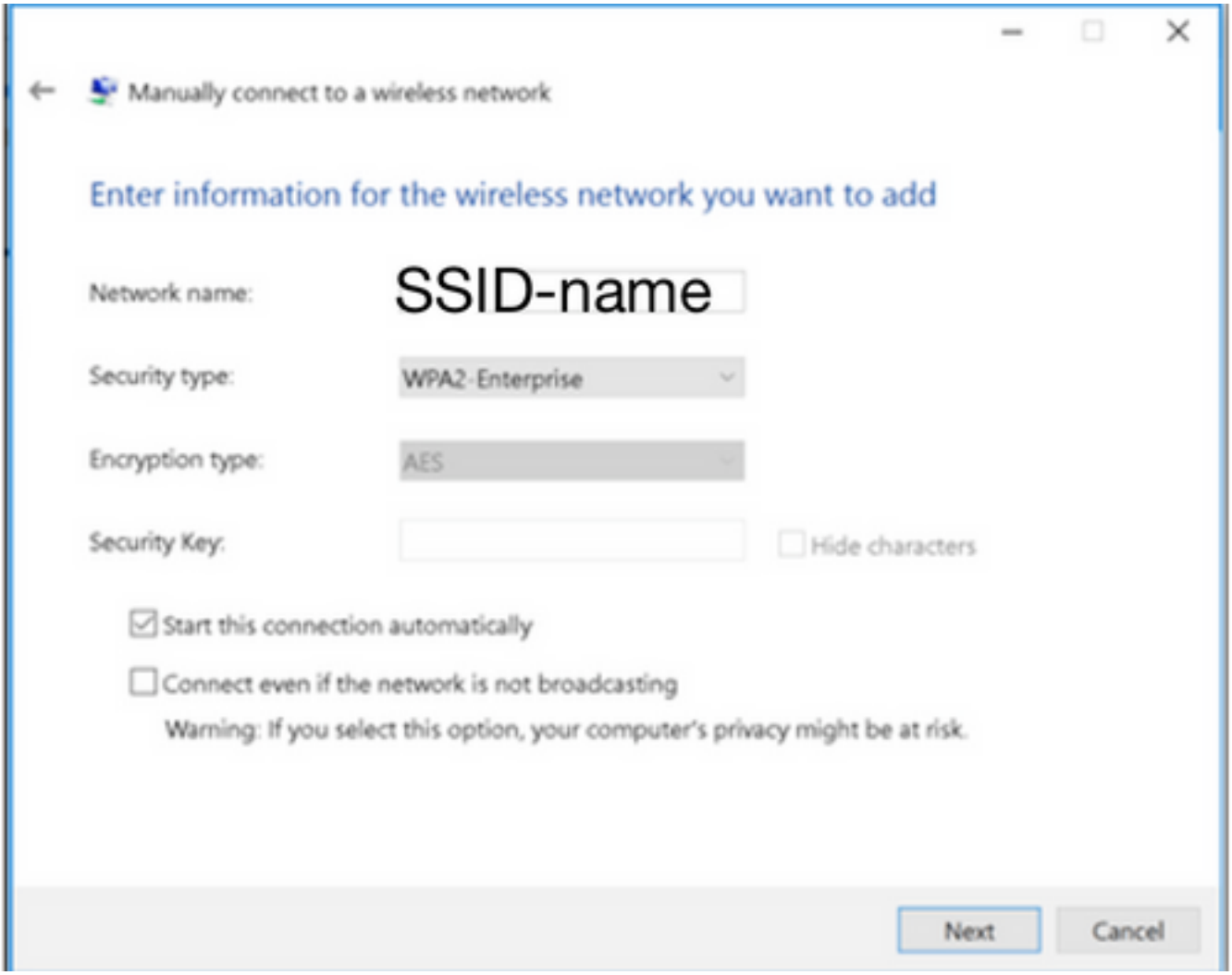
步骤2.导航到**网络和互联网**，那以后导航对**中心的网络和共享**并且单击**建立了新连接或网络。**



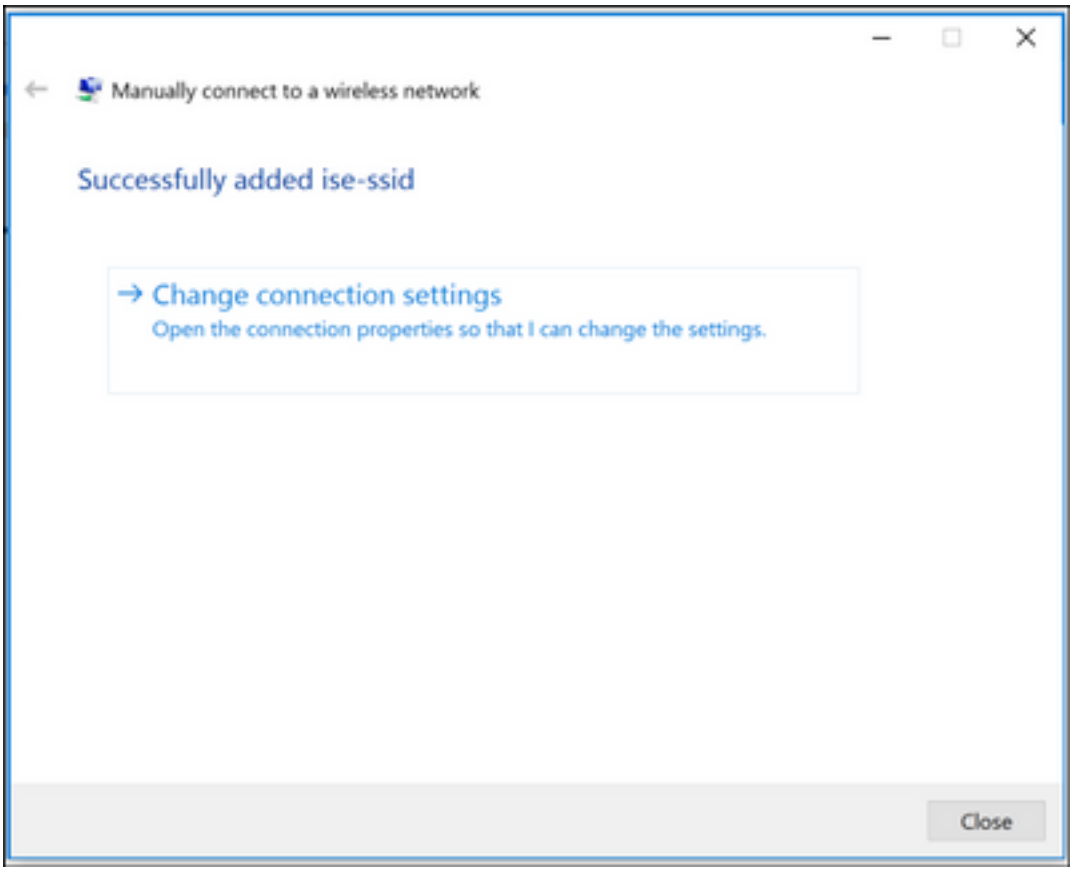
步骤3.选择**手工连接对无线网络**并且**其次**单击。



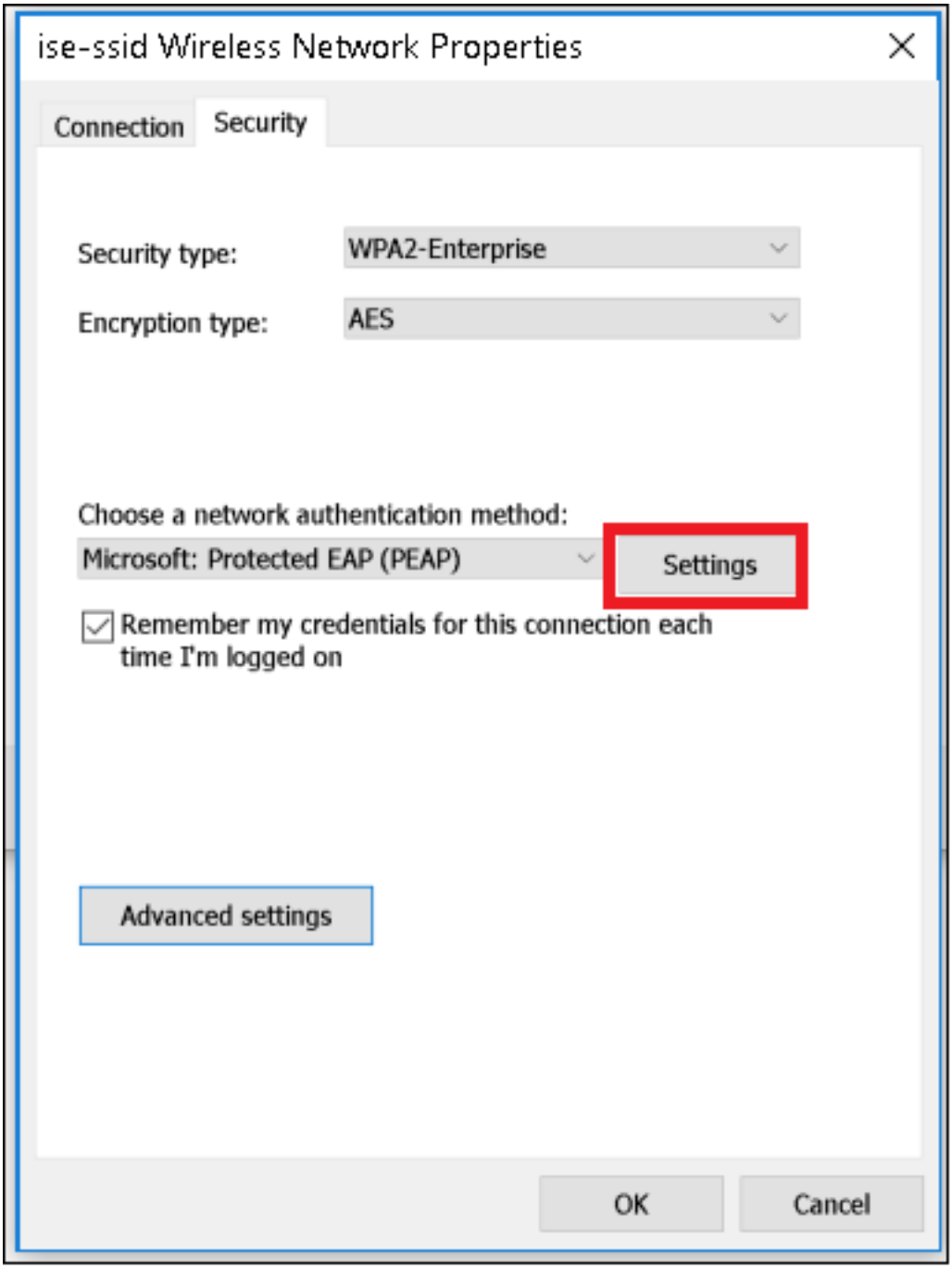
步骤4.输入与SSID和安全类型WPA2-Enterprise的名称的信息并且**其次**单击。



步骤5.选择**崔凡吉莱连接设置**为了定制WLAN配置文件的配置。



步骤6.导航对**安全选项卡**并且点击**设置。**



步骤7.，如果RADIUS服务器验证，请选择。

如果是， enable (event)**验证服务器的标识通过验证证书**和从**可靠的根证书颁发机构：**列出精选freeRADIUS自签名证书。

以后该请选择**自动地配置**并且禁用**使用我的Windows登录名字和密码...**，然后点击OK键