配置802.1x - PEAP，带FreeRadius和WLC 8.3

目录

简介

本文档介绍如何将具有802.1x安全和受保护的可扩展身份验证协议(PEAP)作为可扩展身份验证协议(EAP)的无线局域网(WLAN)设置。 FreeRADIUS用作外部远程身份验证拨入用户服务(RADIUS)服务器。

先决条件

要求

Cisco 建议您具有以下主题的基础知识：

- Linux
- Vim编辑器
- AireOS无线LAN控制器(WLC)

注意：本文档旨在向读者举例说明在freeRADIUS服务器上进行PEAP-MS-CHAPv2身份验证所需的配置。本文档中介绍的freeRADIUS服务器配置已在实验中测试，并发现其可以按预期工作。思科技术支持中心(TAC)不支持免费RADIUS服务器配置。

使用的组件

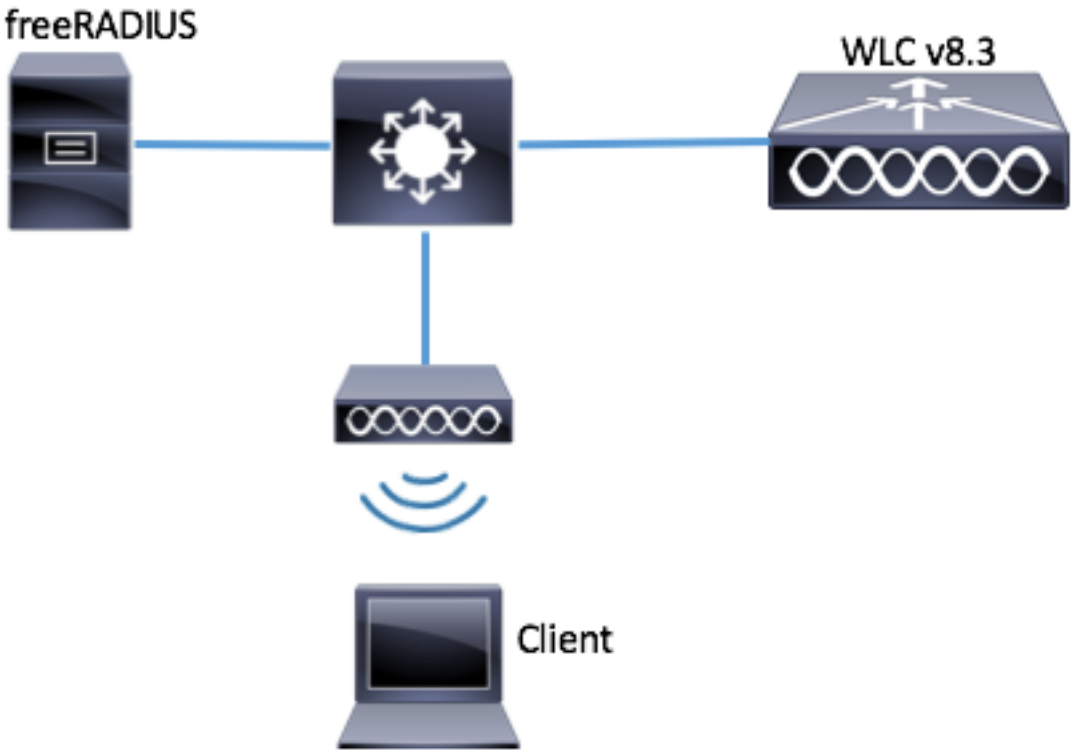
本文档中的信息基于以下软件和硬件版本：

- CentOS7或Red Hat Enterprise Linux 7(RHEL7)（建议1 GB内存和至少20 GB硬盘）
- WLC 5508 v8.3
- MariaDB(MySQL)
- FreeRADIUS
- 7菲律宾比索

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。

配置

网络图



安装httpd服务器和MariaDB

步骤1.运行这些命令以安装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.配置初始MariaDB设置以保护它。

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

注意：运行此脚本的所有部分。建议将其用于生产使用中的所有MariaDB服务器。仔细阅读每一步。

```
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.为freeRADIUS配置数据库（使用步骤3中配置的相同密码）。

```
[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
```

在CentOS 7上安装PHP 7

步骤1.运行这些命令以在CentOS7上安装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.运行此命令以安装FreeRADIUS。

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

步骤2.在mariadb.service之后启动radius.service。

运行此指令：

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

在[Unit]部一行:

```
After=mariadb.service
```

[单元]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.启动并启用freeradius以启动。

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

步骤4.启用防火墙以确保安全。

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

步骤5.向默认区域添加永久规则以允许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.重新加载防火墙以使更改生效。

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

FreeRADIUS

要配置FreeRADIUS以使用MariaDB，请执行以下步骤。

步骤1.导入RADIUS数据库方案以填充RADIUS数据库。

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

步骤2.在/etc/raddb/mods-enabled下为结构化查询语言(SQL)创建软链接。

```
[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，并更改数据库连接参数以套用您的环境。

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

SQL部分必须类似于此。

```
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.将/etc/raddb/**mods-enabled/sql的组权限更改为**radiusd。

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

WLC作为FreeRADIUS上的身份验证、授权和记帐(AAA)客户端

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

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

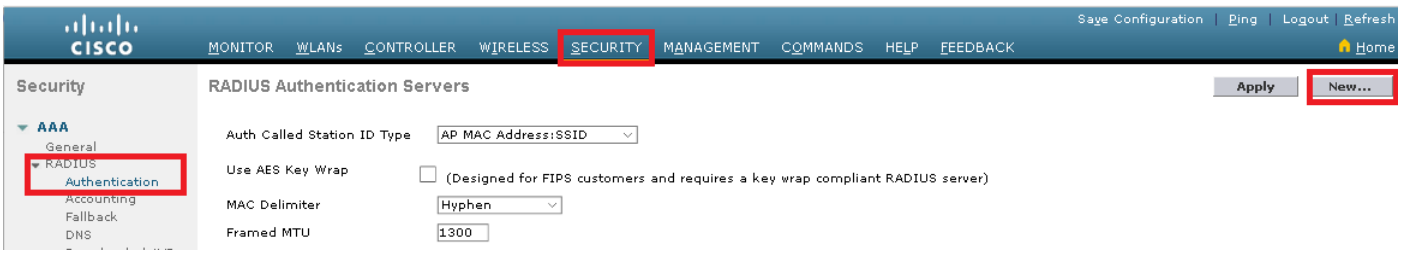
步骤2.在底部添加控制器IP地址和共享密钥。

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

在WLC上将FreeRADIUS用作RADIUS服务器

GUI:

步骤1.打开WLC的GUI并导航至**SECURITY > RADIUS > Authentication > New**，如图所示。



步骤2.填写RADIUS服务器信息，如图所示。

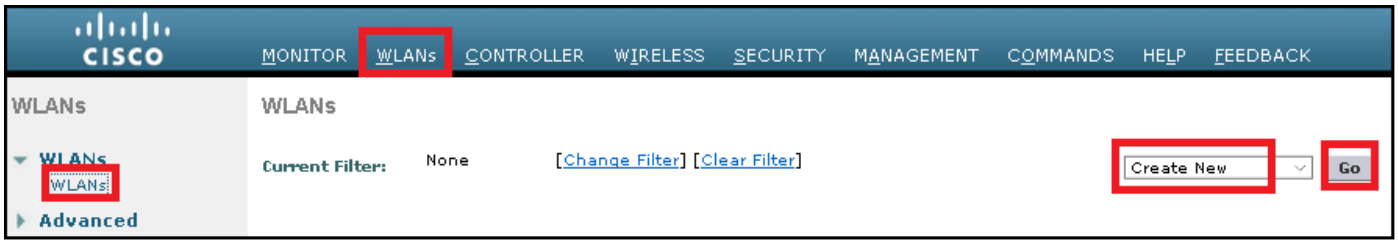
CLI：

```
> config radius auth add <index> <radius-ip-address> 1812 ascii <shared-key>
> config radius auth disable <index>
> config radius auth retransmit-timeout <index> <timeout-seconds>
> config radius auth enable <index>
```

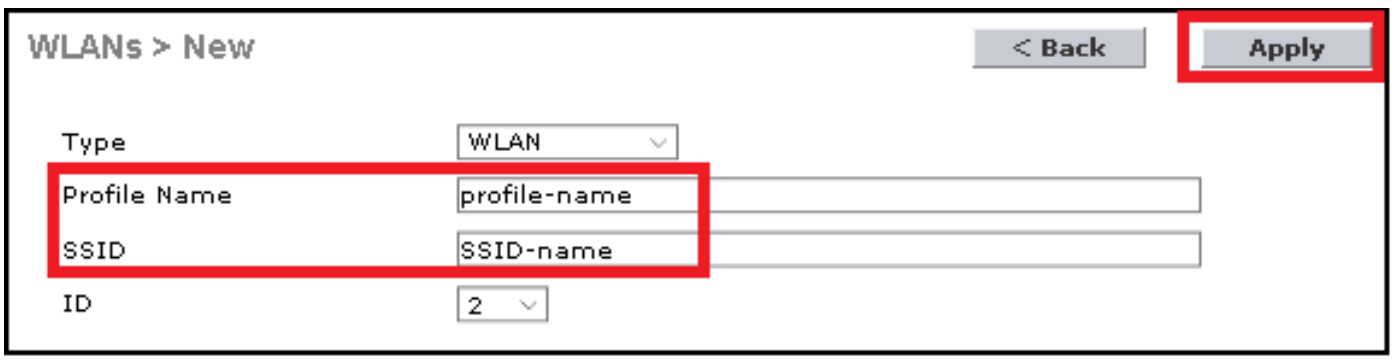
WLAN

GUI:

步骤1.打开WLC的GUI并导航至WLANs **> Create New > Goas(**如图所示)。



步骤2.为服务集标识符(SSID)和配置文件选择名称，然后单击应用，如图所示。



CLI：

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

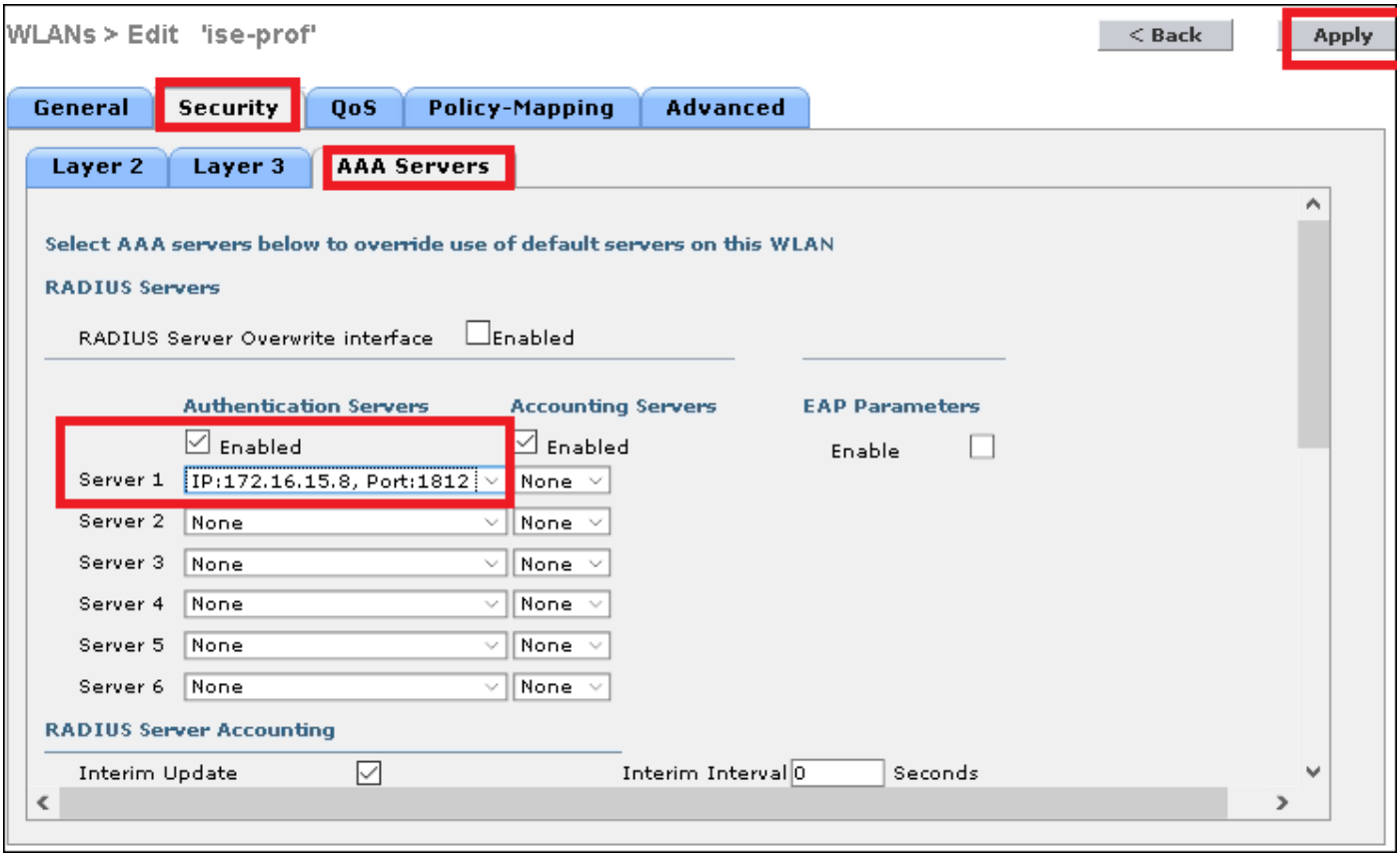
步骤3.将RADIUS服务器分配给WLAN。

CLI：

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

GUI:

导航至**Security > AAA Servers**并选择所需的RADIUS服务器，然后单击**Apply**，如图所示。



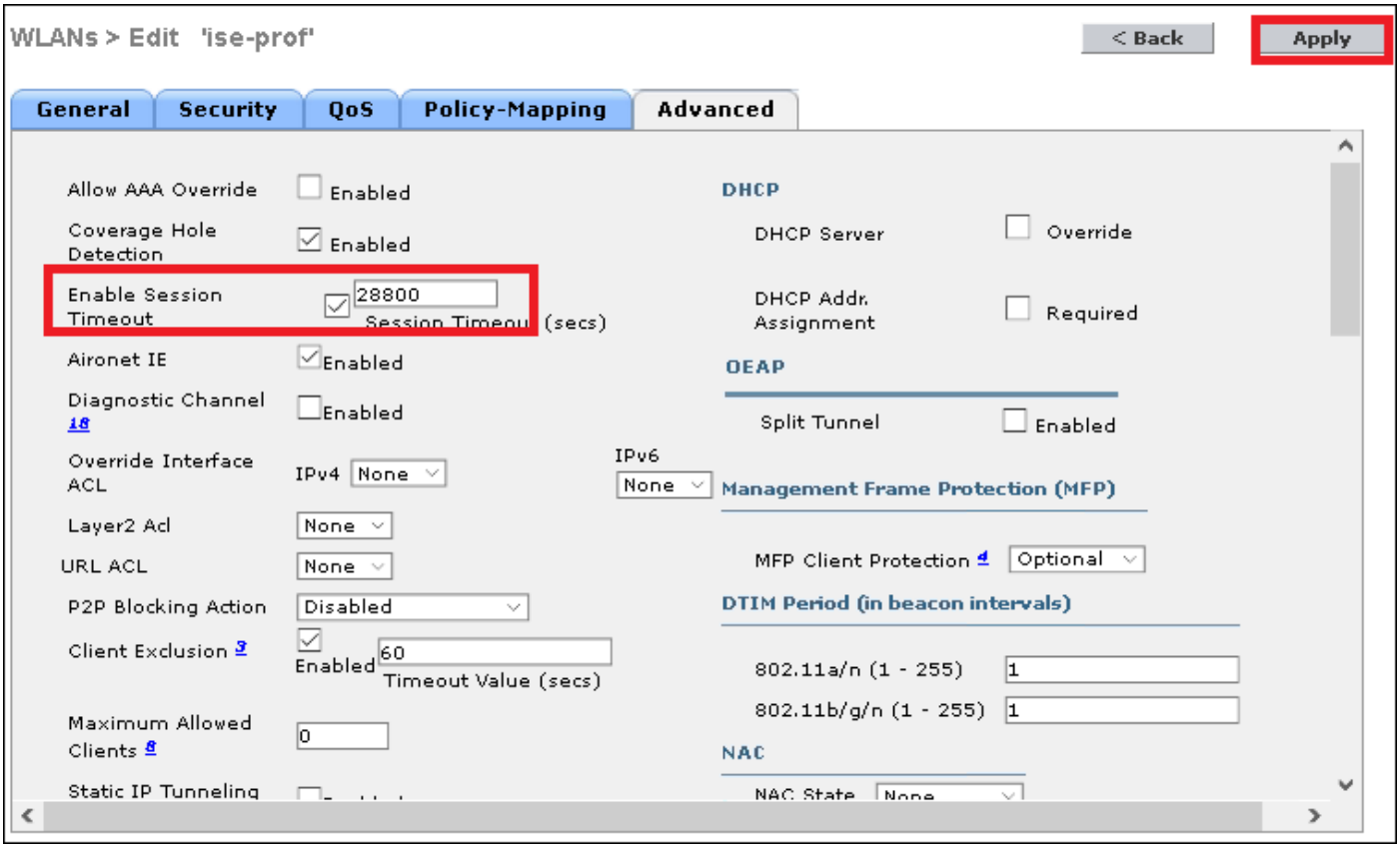
步骤4.或者增加会话时间。

CLI：

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

GUI:

导航至“**高级**”>“**启用会话超时**”>单击“**应**用”，如图所示。



步骤5.启用WLAN。

CLI：

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

GUI:

导航至“**常规**”>“**状态**”>“**启用刻度**”>单击“**应**用”，如图所示。

将用户添加到freeRADIUS数据库

默认情况下，客户端使用PEAP协议，但freeRadius支持其他方法（本指南未介绍）。

步骤1.编辑文件/etc/raddb/users。

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

步骤2.在文件底部附加用户信息。在本示例中，user1是用户名和Cisco123的密码。

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

步骤3.重新启动FreeRadius。

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

freeRADIUS上的证书

FreeRADIUS附带默认证书颁发机构(CA)证书和存储在路径/etc/raddb/certs中的设备证书。这些证书的名称是ca.pem和server.pem。server.pem是客户端在完成身份验证过程时收到的证书。如果需要为EAP身份验证分配不同的证书，只需删除它们，并将新证书保存到同一路径中，其名称与此完全相同。

终端设备配置

配置笔记本电脑Windows计算机，以使用802.1x身份验证和PEAP/MS-CHAP(质询握手身份验证协议的Microsoft版本)版本2连接到SSID。

要在Windows计算机上创建WLAN配置文件，有两个选项：

1. 在计算机上安装自签名证书以验证和信任freeRADIUS服务器以完成身份验证
2. 绕过RADIUS服务器的验证并信任用于执行身份验证的任何RADIUS服务器（不推荐，因为它可能会成为安全问题）。 这些选项的配置在终端设备配置 — 创建WLAN配置文件中进行说明。

导入FreeRADIUS证书

如果使用在freeRADIUS上安装的默认证书，请按照以下步骤将EAP证书从freeRADIUS服务器导入终端设备。

步骤1.从FreeRadius获取证书：

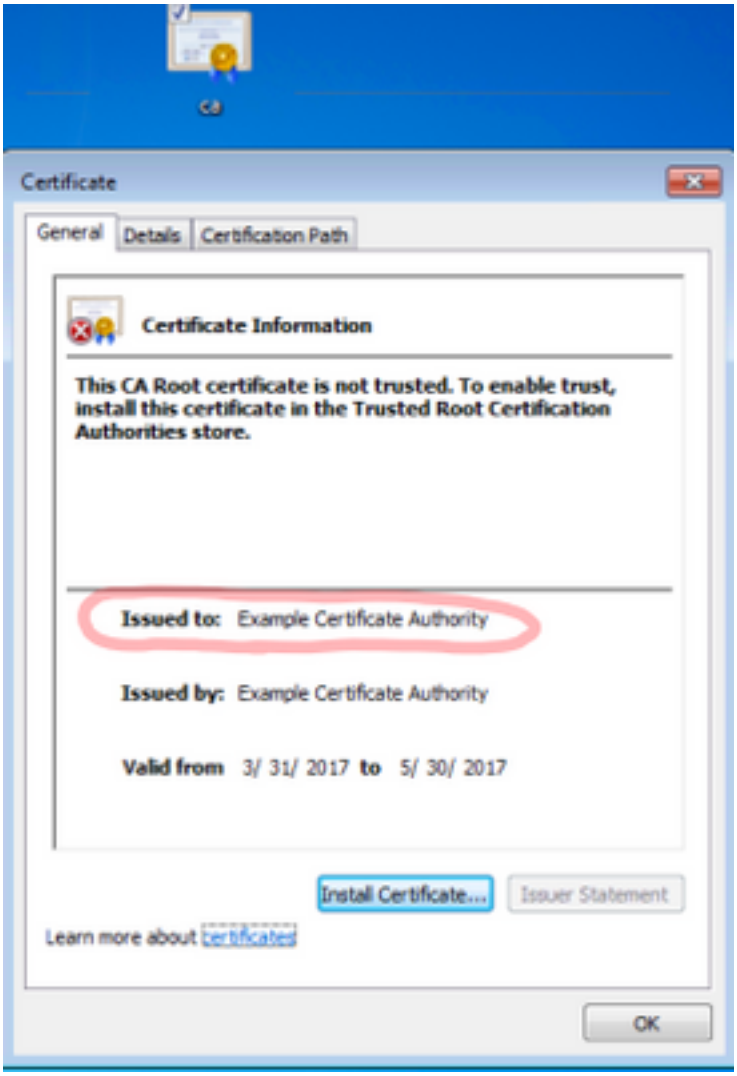
```
[root@tac-mxwireless ~]# cat /etc/raddb/certs/ca.pem

-----BEGIN CERTIFICATE-----
MIIE4TCCA8mgAwIBAgIJAKLmHn4eZLjBMA0GCSqGSIb3DQEBBQUAMIGTMQswCQYD
VQQGEwJGUjEPMA0GA1UECBMGUmFkaXVzMRIwEAYDVQQHEwlTb211ld2hlcmUxFTAT
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
```

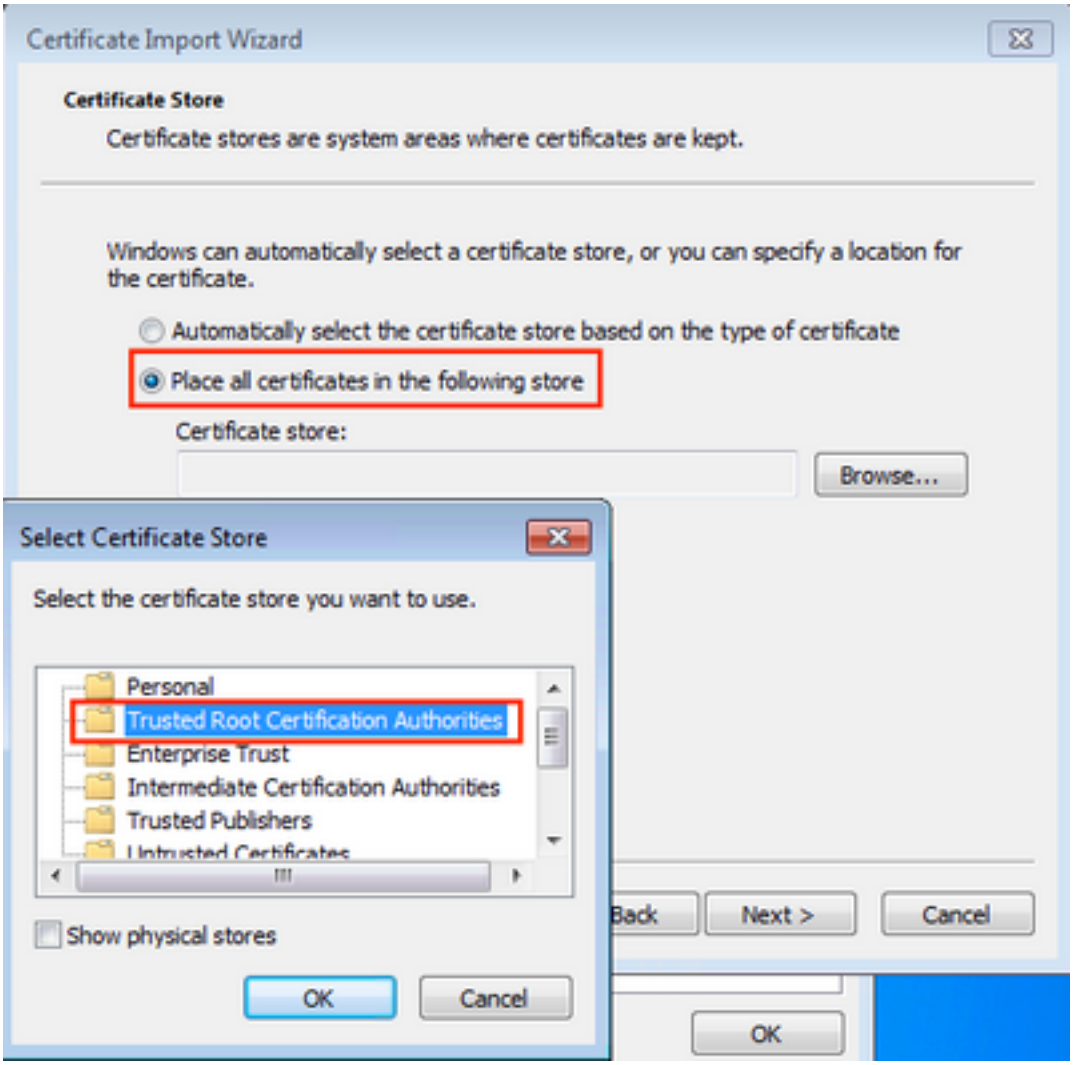
```
HRMEBTADAQH/MDYGA1UdHwQvMC0wK6ApoCeGJWh0dHA6Ly93d3cuZXhhbXBsZS5j
b20vZXhhbXBsZV9jYS5jcmwwDQYJKoZIhvcNAQEFBQADggEBACsPR2jiOFXnTsK4
1wnrrMylZZb12gDuqK+zKELox2mzlDMMK83tBsL8yjkv70KeZn821IzfTrTfvhzV
mjX6HgaWfYyMjYYYSw/iEu2JsAtQdpvC3di10nGwVPHlzbozPdov8cZtCb21ynfY
Z6cNjx8+aYQIcsRIyqA1IXMOBwIXo141TOmoODdgfX95lpoLwgktRLkvl7Y7owsz
ChYDO++H7Iewsxx5pQfm56dA2cNrlTwWtMvViKyX7GlpwlbBOxgkLiFJ5+GFbfLh
a0HBHZWhTKvffbr62mkbfjCUfJU4T3xgY9zFwiwT+BetCJgAGy8CT/qmnO+NJERO
RUvDhfE=
-----END CERTIFICATE-----
```

步骤2.将上一步的输出复制并粘贴到文本文件中，并将扩展名更改为.crt

步骤3.双击该文件并选择“安**装证书……**”如图所示.

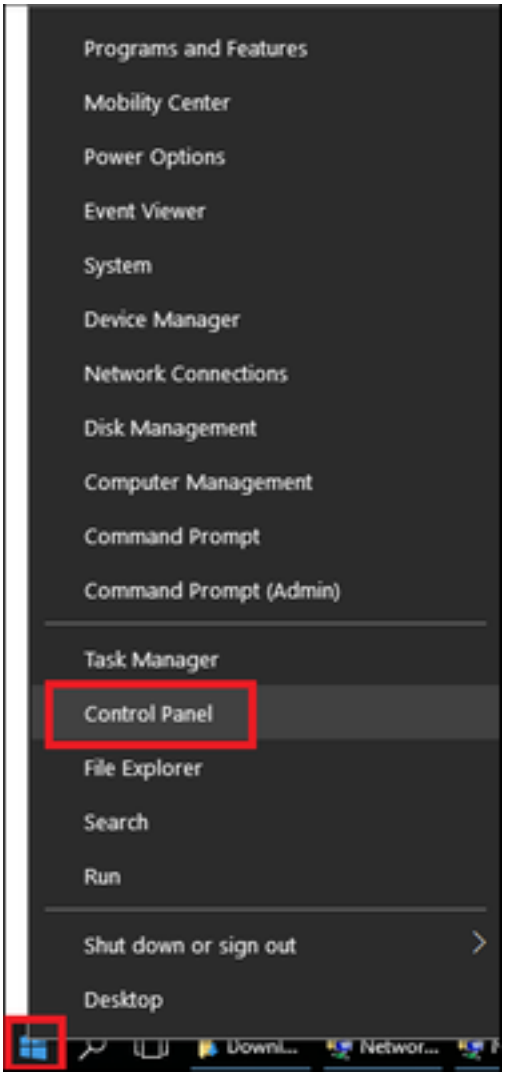


步骤4.将证书安装到受信任**根证书颁发**机构存储中，如图所示。

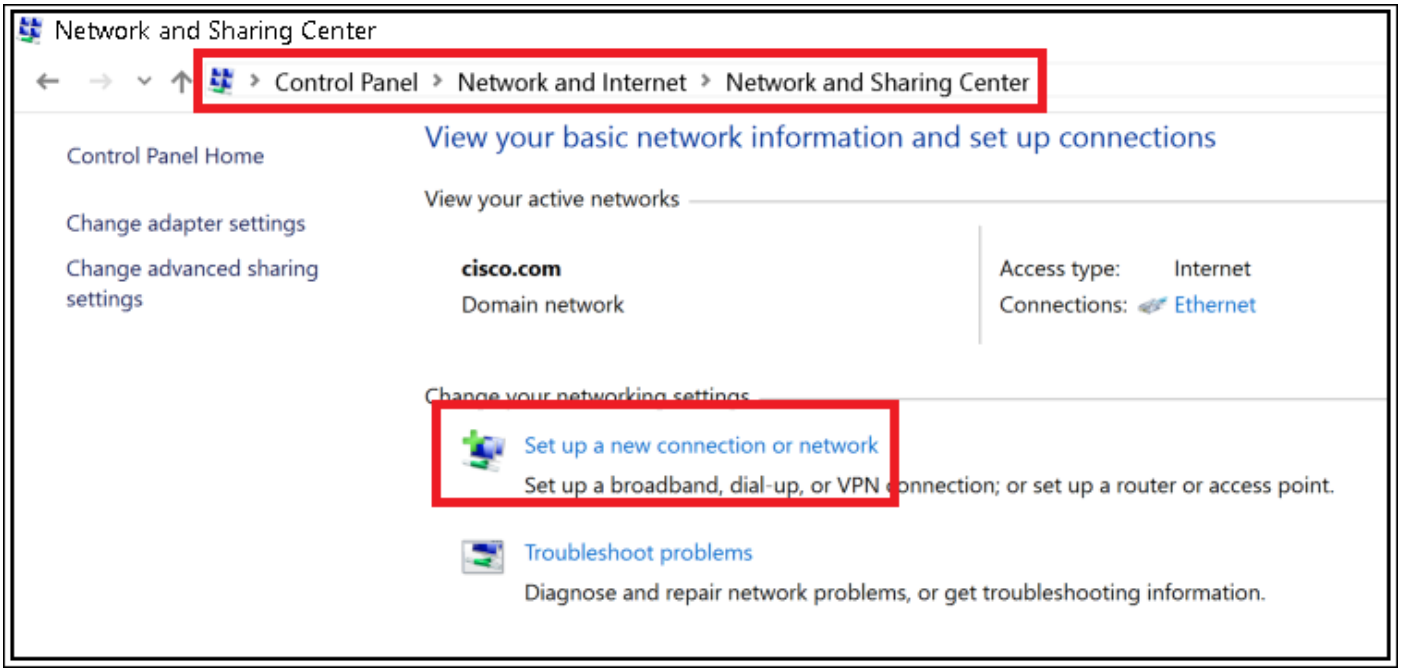


创建WLAN配置文件

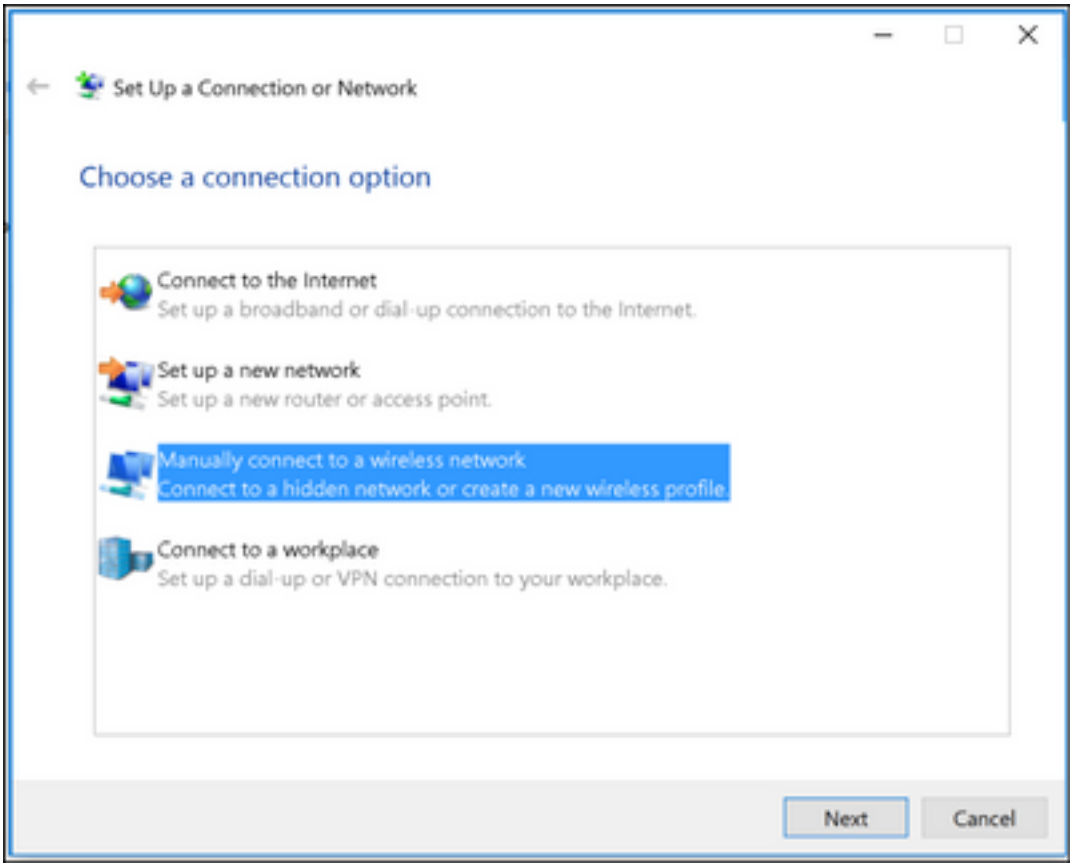
步骤1.右键单击“开始”图标，然**后选择**“控制面板”，如图所示。



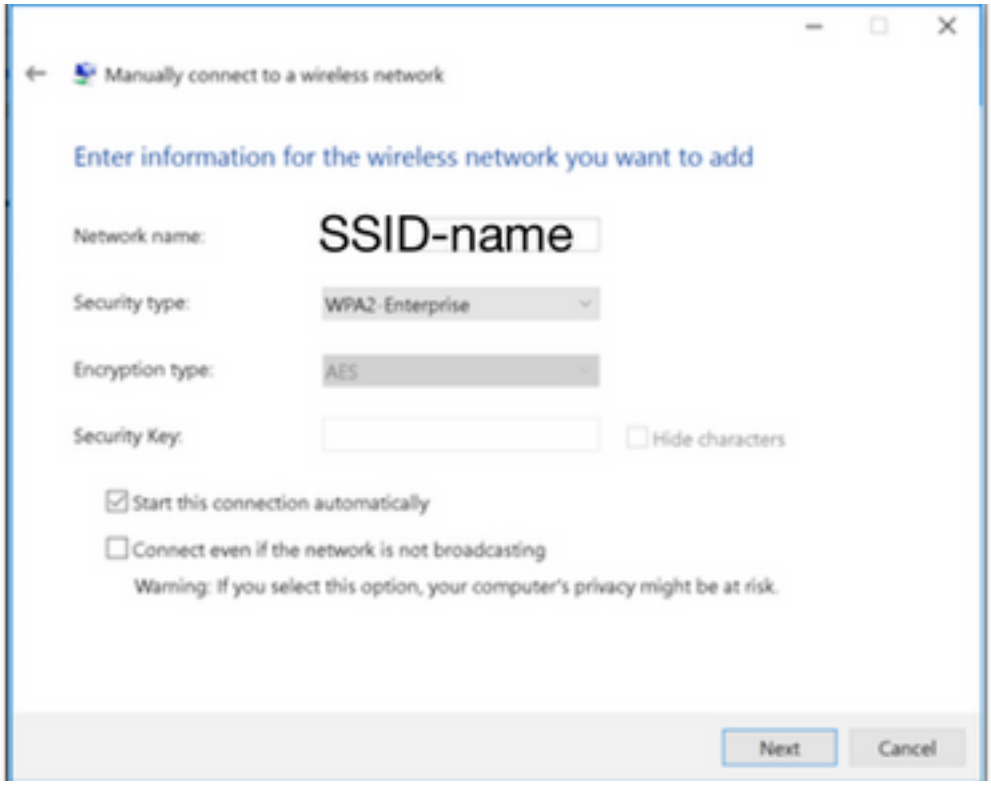
步骤2.导航至**Network and Internet > Network and Sharing Center>单击Set a new connection or network，如图**所示。



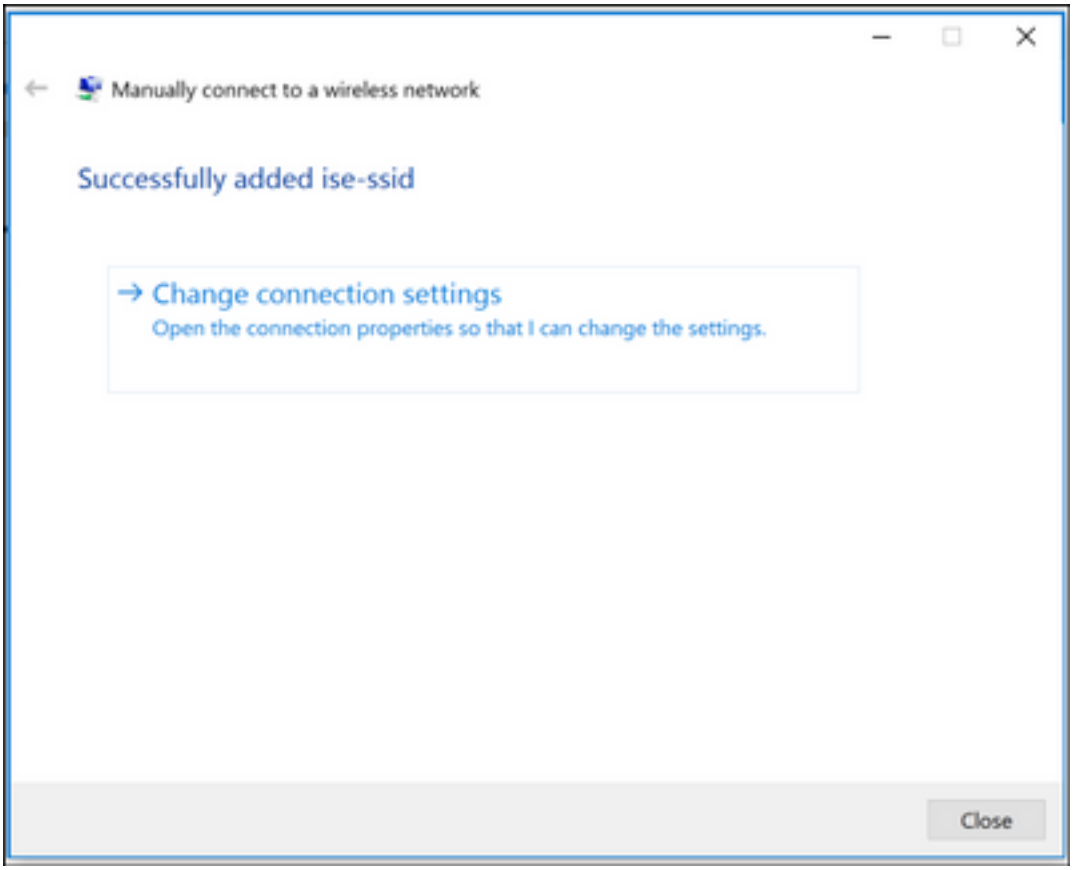
步骤3.选择“**手动连接到无线网络”，**然后单击图中所示的“下一步”。



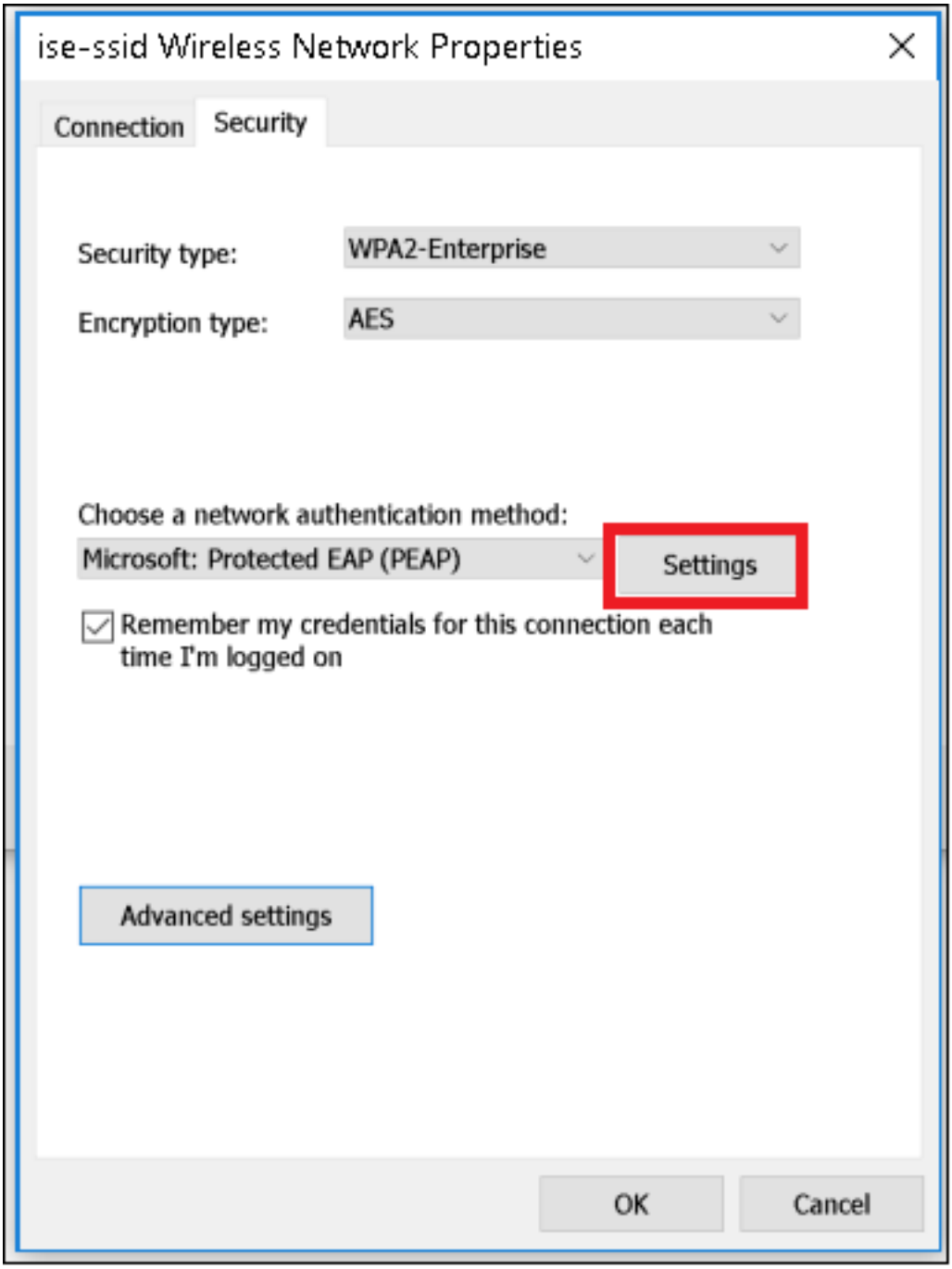
步骤4.输入名称为SSID的信息和安全类型WPA2-Enterprise，然后单击**Next**，如图所示。



步骤5.选择**更改连接**设置以自定义WLAN配置文件的配置，如图所示。



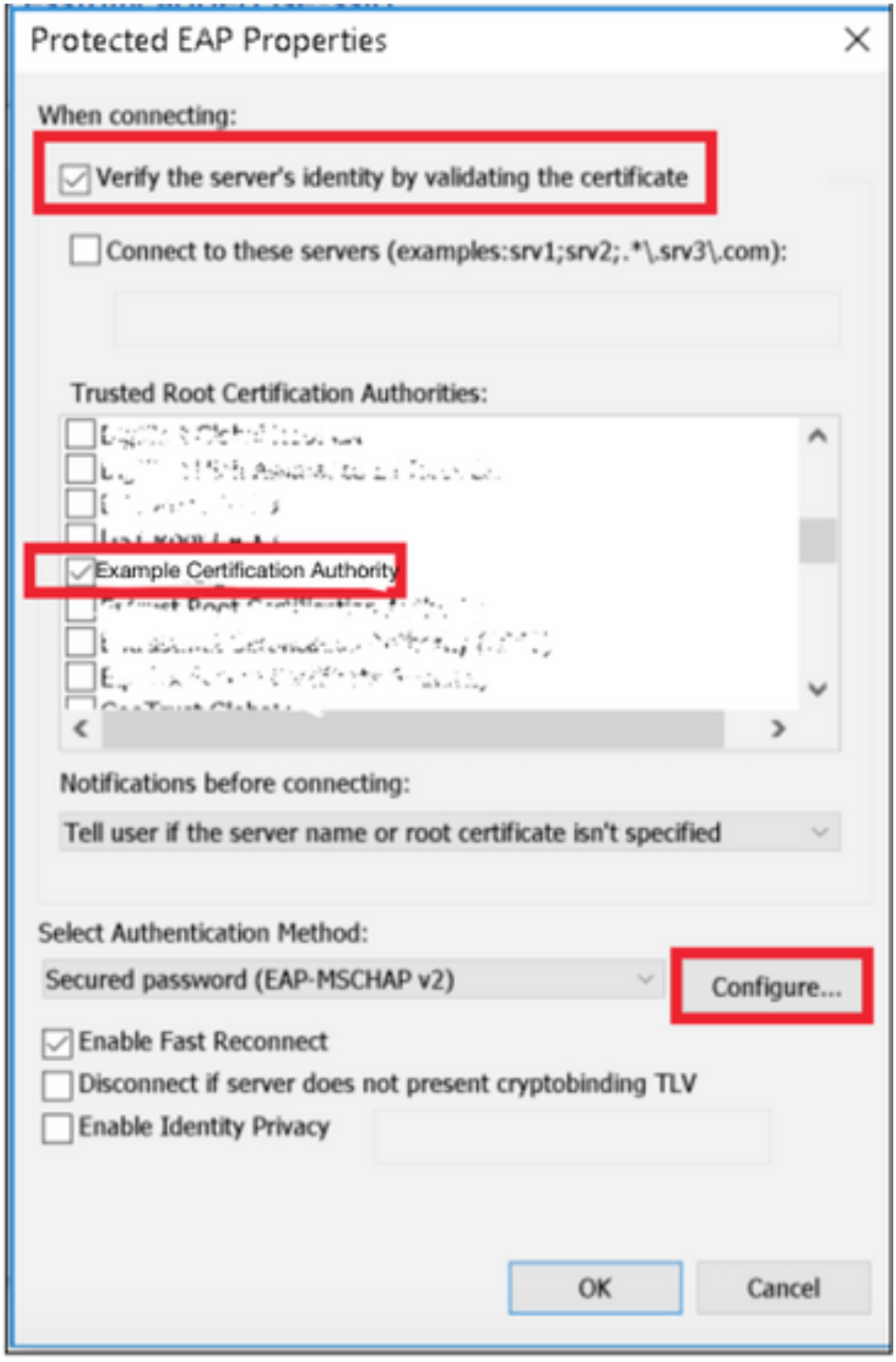
步骤6.导航至“安**全**”选项卡，然**后单**击“设置”，如图所示。

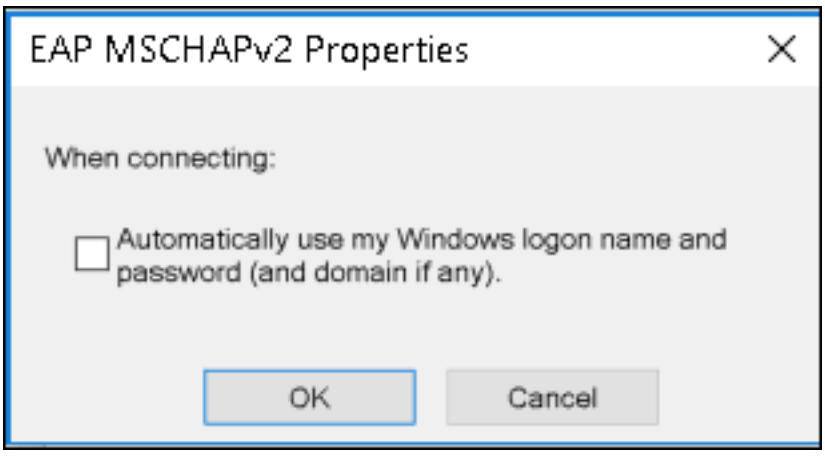


步骤7.选择是否验证RADIUS服务器。

如果是，请启用**“通过验证证书和来自受信任根证书颁发**机构验证服**务器的身份：**列表选择freeRADIUS的自签名证书。

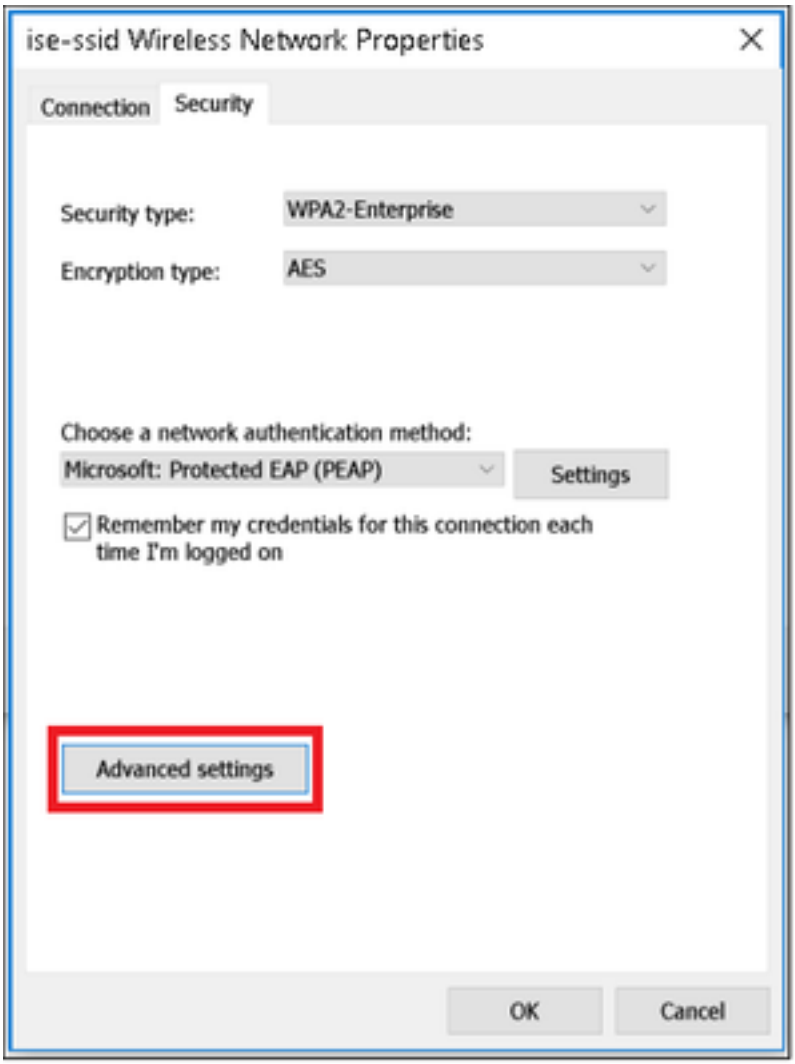
然后，选择**配置**并禁用**自动使用Windows登录名和密码……**，然后单击**确定**，如图所示。

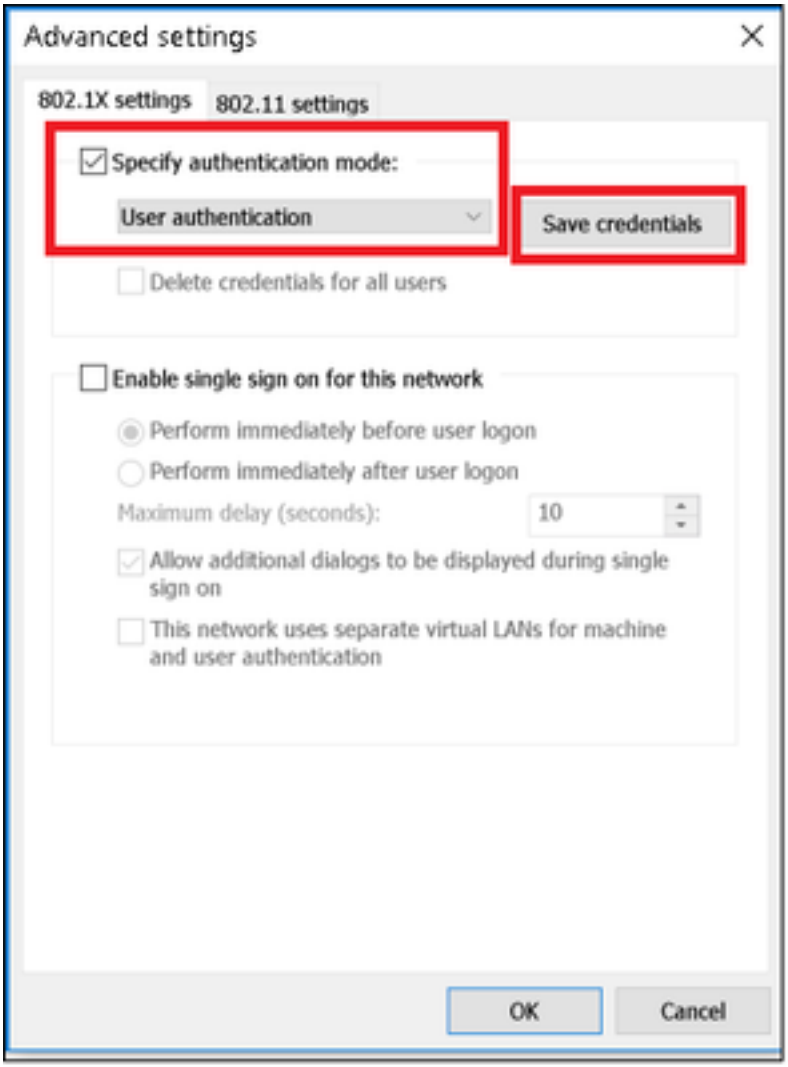

Protected EAP Properties
When connecting:
Verify the server's identity by validating the certificate
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):
Trusted Root Certification Authorities:
Example Certification Authority
Notifications before connecting:
Tell user if the server name or root certificate isn't specified
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
Configure...
Enable Fast Reconnect
Disconnect if server does not present cryptobinding TLV
Enable Identity Privacy
OK
Cancel

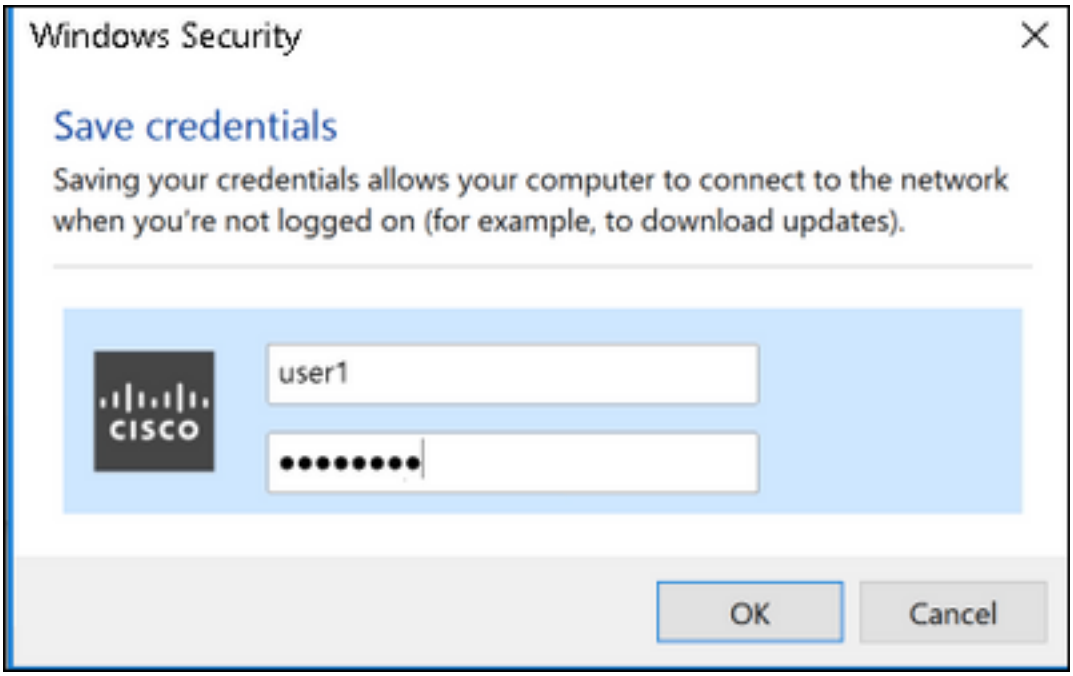

EAP MSCHAPv2 Properties
When connecting:
Automatically use my Windows logon name and password (and domain if any).
OK
Cancel

步骤8.配置用户凭证。

返回“安全”选项卡后，选择**高级设置**，将身份验证模式指定为**用户身份验证**，并保存在freeRADIUS上配置的凭据以对用户进行身份验证，如图所示。







验证

使用本部分可确认配置能否正常运行。

WLC上的身份验证过程

运行下一个命令以监控特定用户的身份验证过程：

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

要方便地读取调试客户端输出，请使用无线调试分析器工具：

[无线调试分析器]

故障排除

目前没有针对此配置的故障排除信息。