

配置802.1x -与FreeRadius和WLC 8.3的PEAP

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[安装httpd服务器和MariaDB](#)

[在CentOS 7的安装PHP 7](#)

[安装FreeRADIUS](#)

[FreeRADIUS](#)

[WLC作为FreeRADIUS的验证、授权和统计\(AAA\)客户端](#)

[FreeRADIUS作为在WLC的RADIUS服务器](#)

[WLAN](#)

[添加用户到freeRADIUS数据库](#)

[在freeRADIUS的证书](#)

[终端设备配置](#)

[导入FreeRADIUS证书](#)

[创建WLAN配置文件](#)

[验证](#)

[在WLC的认证过程](#)

[故障排除](#)

简介

本文描述如何设置一个无线局域网(WLAN)以802.1x安全和Protected Extensible Authentication Protocol (PEAP)作为可扩展的认证协议(EAP)。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

要求

Cisco 建议您具有以下主题的基础知识：

- Linux
- 精力编辑器
- AireOS无线局域网控制器(WLCs)

Note: 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

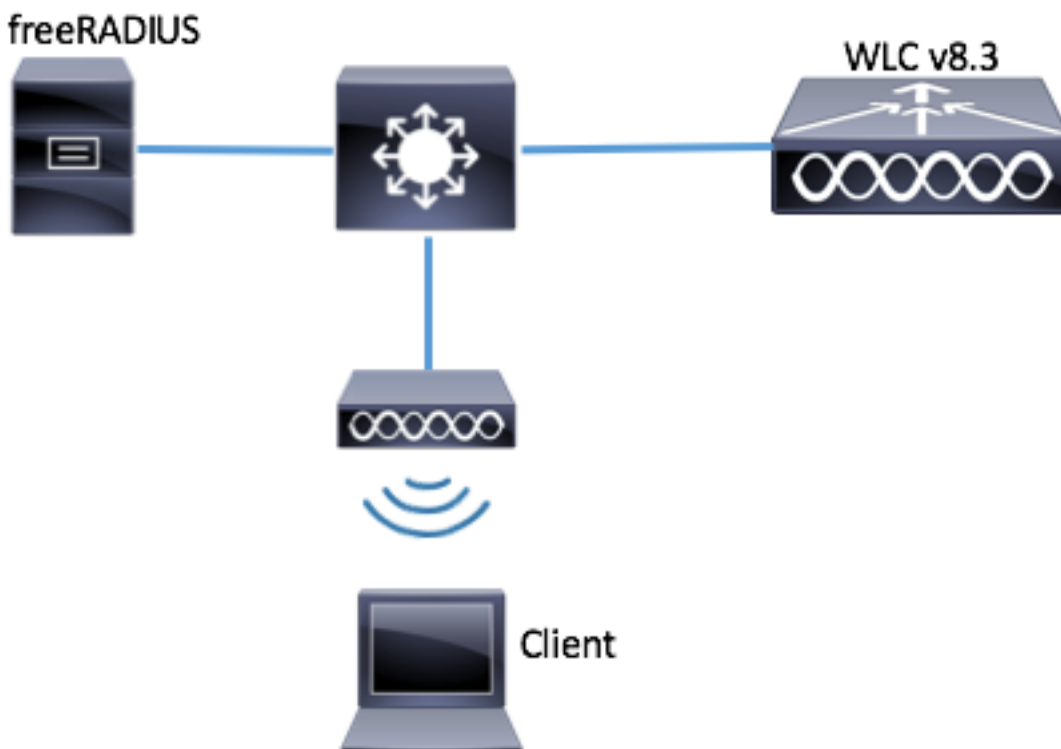
本文档中的信息基于以下软件和硬件版本：

- 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。

配置

网络图



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:管理此脚本的所有部分。为在制作使用的所有MariaDB服务器推荐。仔细阅读每个步骤。

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

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_secure_installation
```

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 ~]#mysql_secure_installation
```

安装FreeRADIUS

步骤1.运行此命令安装FreeRADIUS。

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

第二步：在mariadb.service以后做radius.service开始。

运行此指令：

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

添加在[Unit]部分的一条线路：

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

[Unit]部分必须如下所示：

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

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

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

步骤4.安全的Enable (event) firewalld。

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

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 ~]#mysql_secure_installation
```

步骤6.更改的重新加载firewalld能生效。

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

FreeRADIUS

为了配置FreeRADIUS使用MariaDB，请遵从这些步骤。

步骤1.导入RADIUS数据库方案填充RADIUS数据库。

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

步骤2.创建结构化查询语言(SQL)的一条软链在/etc/raddb/mods-enabled下。

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

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 ~]#mysql_secure_installation
```

SQL部分一定看起来类似于此。

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

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

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

WLC作为FreeRADIUS的验证、授权和统计(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 ~]#mysql_secure_installation
```

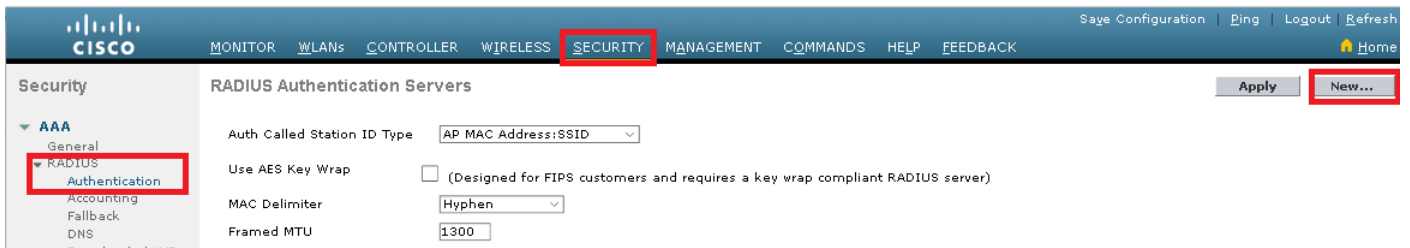
第二步：在底部，请添加您的控制器IP地址和共享密钥。

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

FreeRADIUS作为在WLC的RADIUS服务器

GUI：

步骤1.如镜像所显示，打开WLC的GUI并且导航对**SECURITY>RADIUS >验证>New**。



步骤2.如镜像所显示，填装RADIUS服务器信息。



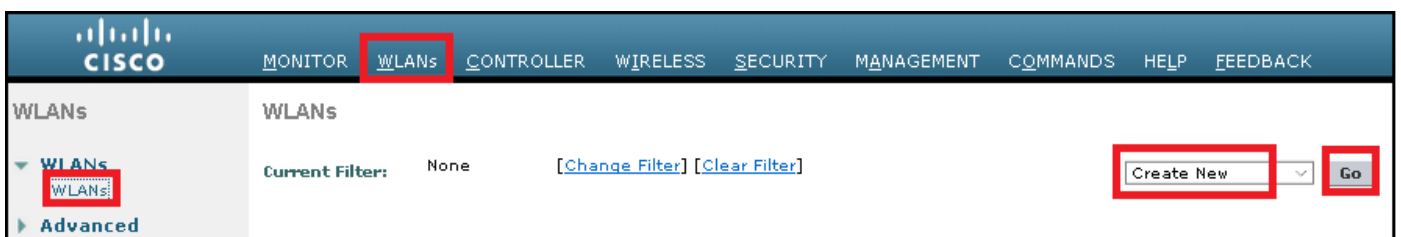
CLI :

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

WLAN

GUI :

步骤1.打开WLC的GUI并且导航对WLAN >创建新>在镜像显示的戈阿。



步骤2.选择一名称对于服务集标识(SSID)和配置文件，然后点击在镜像显示的Applyas。

WLANs > New [< Back](#) [Apply](#)

Type WLAN ▾

Profile Name profile-name

SSID SSID-name

ID 2 ▾

CLI :

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

步骤3.分配RADIUS服务器到WLAN。

CLI :

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

GUI :

如镜像所显示，导航到**安全>AAA服务器**并且选择希望的RADIUS服务器，然后单击**应用**。

WLANs > Edit 'ise-prof' [< Back](#) [Apply](#)

General **Security** **QoS** **Policy-Mapping** **Advanced**

Layer 2 **Layer 3** **AAA Servers**

Select AAA servers below to override use of default servers on this WLAN

RADIUS Servers

RADIUS Server Overwrite interface Enabled

	Authentication Servers	Accounting Servers	EAP Parameters
Server 1	<input checked="" type="checkbox"/> Enabled IP:172.16.15.8, Port:1812 ▾	<input checked="" type="checkbox"/> Enabled None ▾	Enable <input type="checkbox"/>
Server 2	None ▾	None ▾	
Server 3	None ▾	None ▾	
Server 4	None ▾	None ▾	
Server 5	None ▾	None ▾	
Server 6	None ▾	None ▾	

RADIUS Server Accounting

Interim Update Interim Interval Seconds

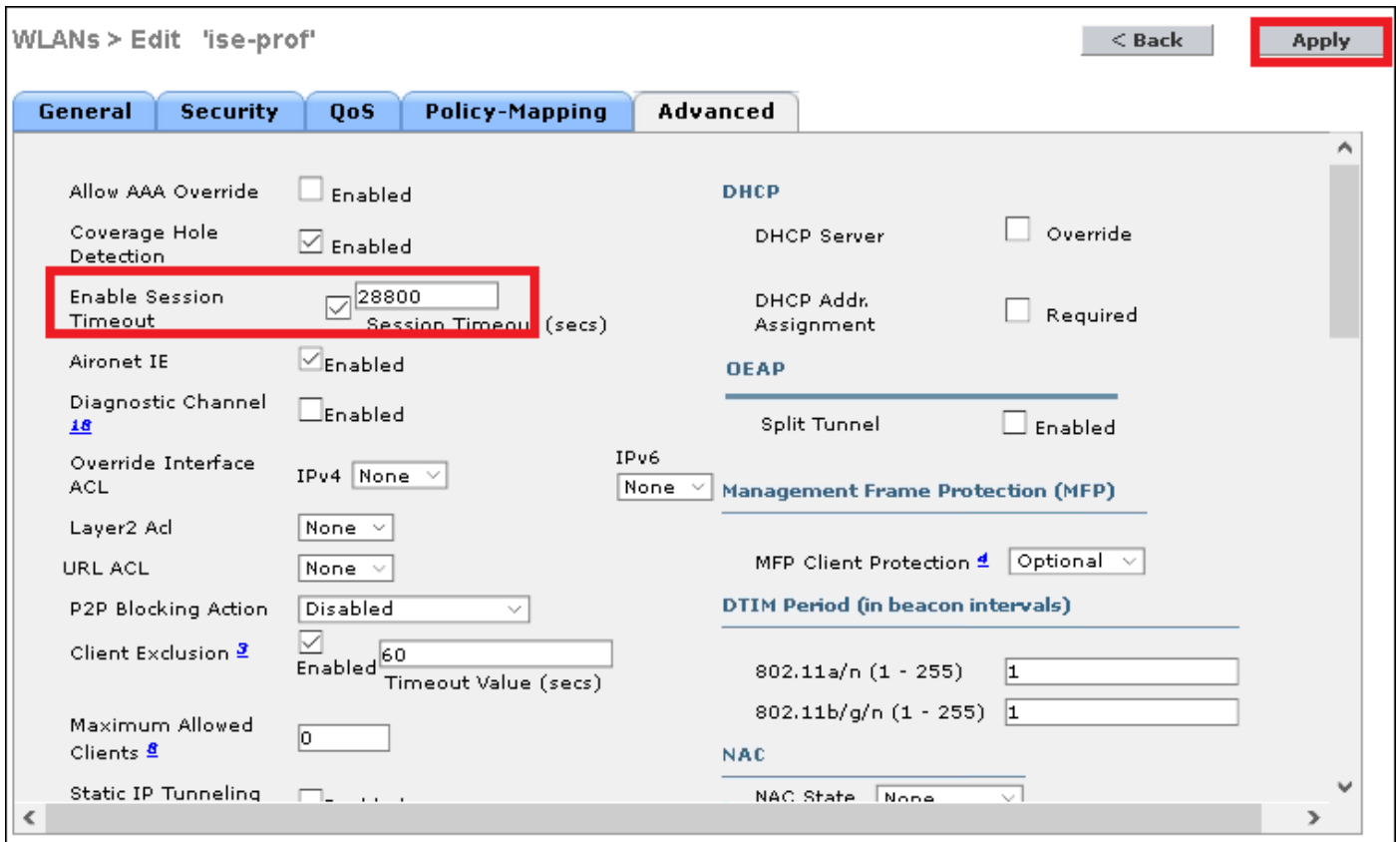
步骤4.随意地请增加会话时间。

CLI :

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

GUI :

如镜像所显示，导航对先进的>enable会话超时>单击应用。



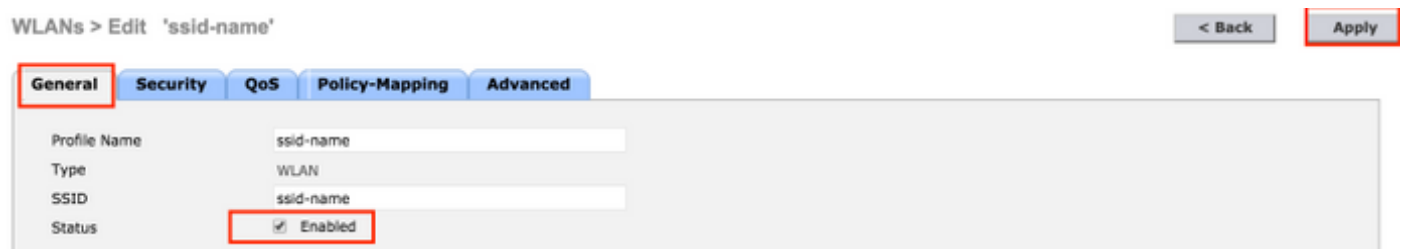
步骤5.启用WLAN。

CLI :

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

GUI :

如镜像所显示，导航对常规>启用的状态>瞬间>单击应用。



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 ~]#mysql_secure_installation
```

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。

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

步骤3.重新启动FreeRadius。

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

在freeRADIUS的证书

FreeRADIUS附有存储在路径/etc/raddb/certs的默认证明Authority (CA)证书和设备证书。这些证书名称是ca.pem和server.pem server.pem是客户端接收的证书，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。

为了创建在那里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。

导入FreeRADIUS证书

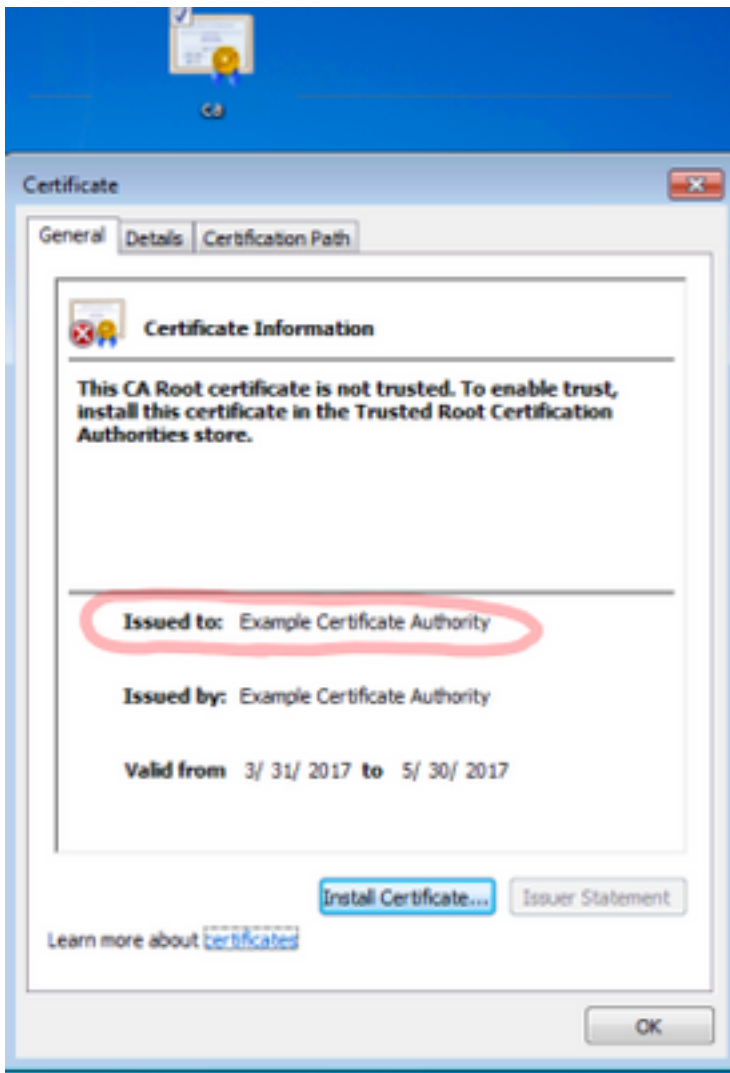
如果在使用在freeRADIUS安装的默认证书，请遵从这些步骤为了导入从freeRADIUS服务器的EAP证书到终端设备。

步骤1.从FreeRadius获得cert：

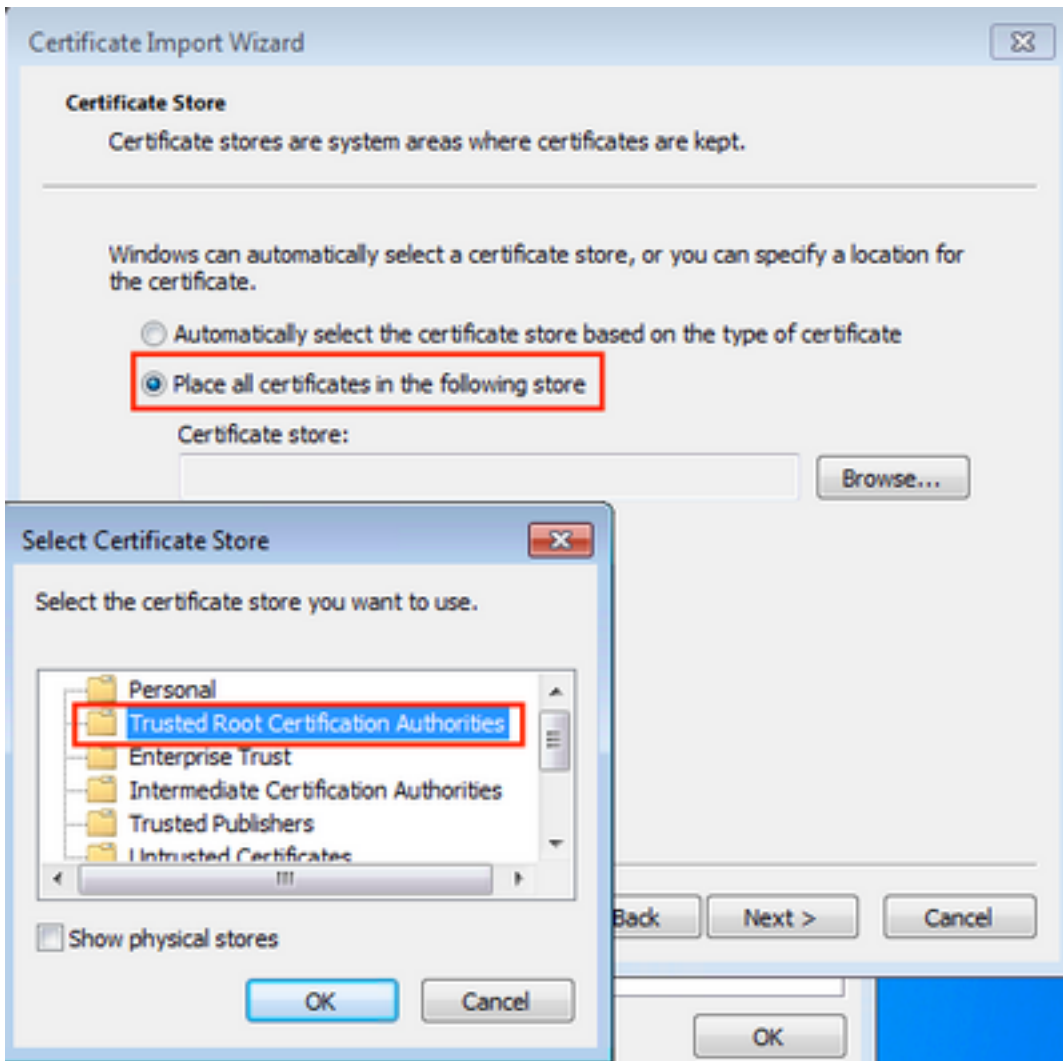
```
[root@tac-mxwireless ~]#mysql_secure_installation
```

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.如镜像所显示，双击文件并且选择**安装证书...**。

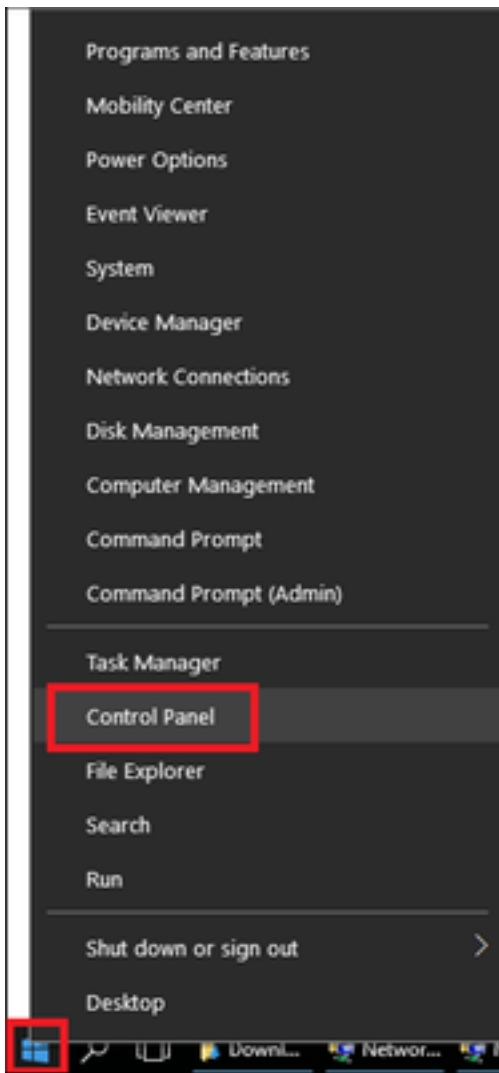


步骤4.如镜像所显示，安装证书到可靠的根证书颁发机构存储。

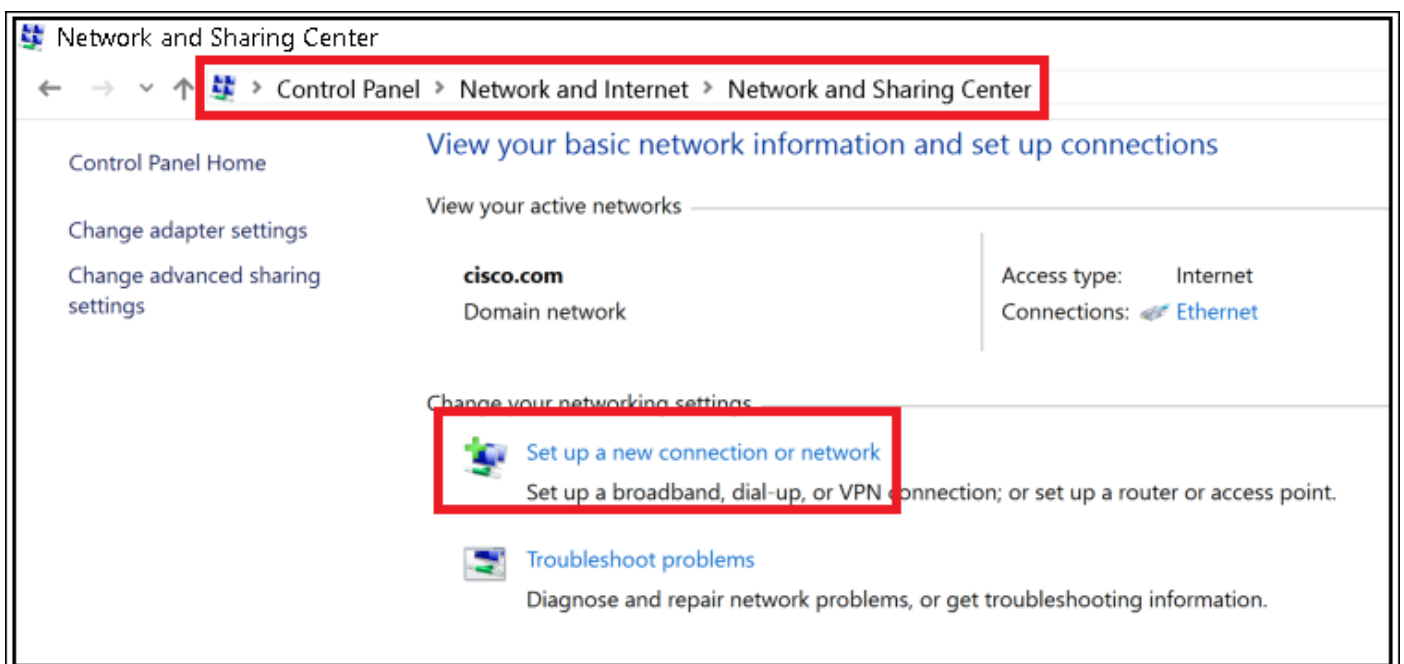


创建WLAN配置文件

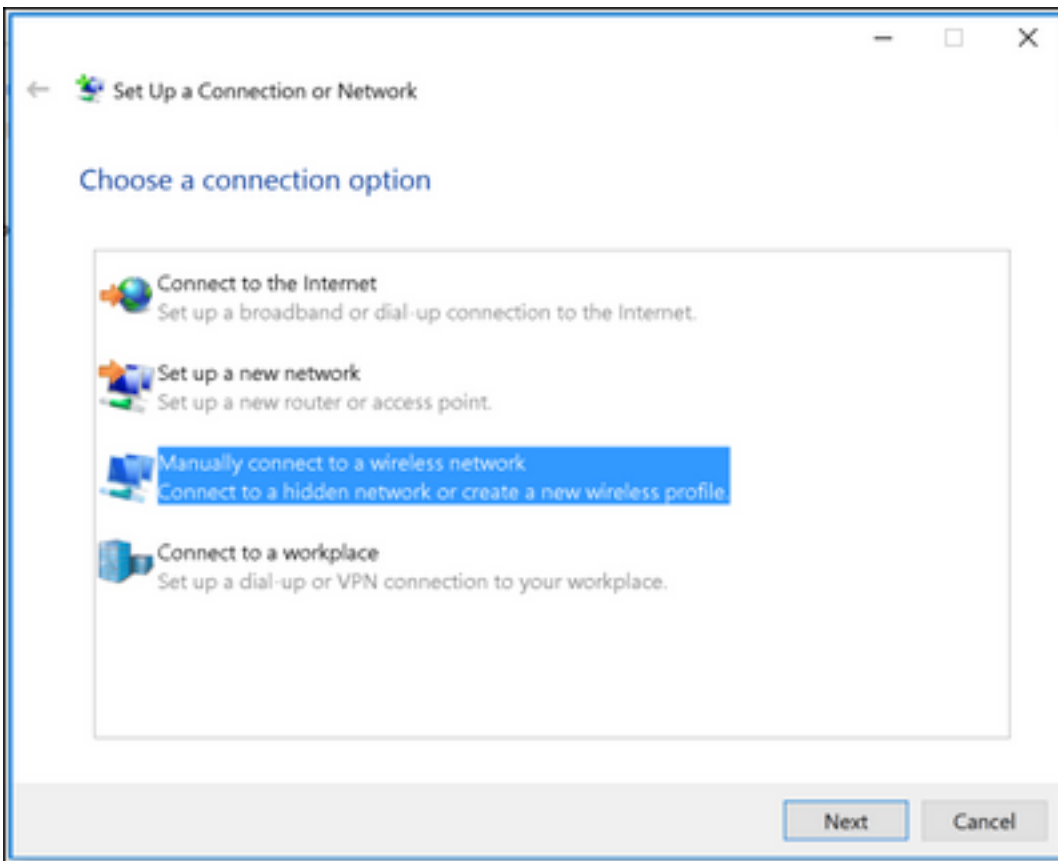
步骤1.如镜像所显示，用鼠标右键单击在Start图标并且选择**控制面板**。



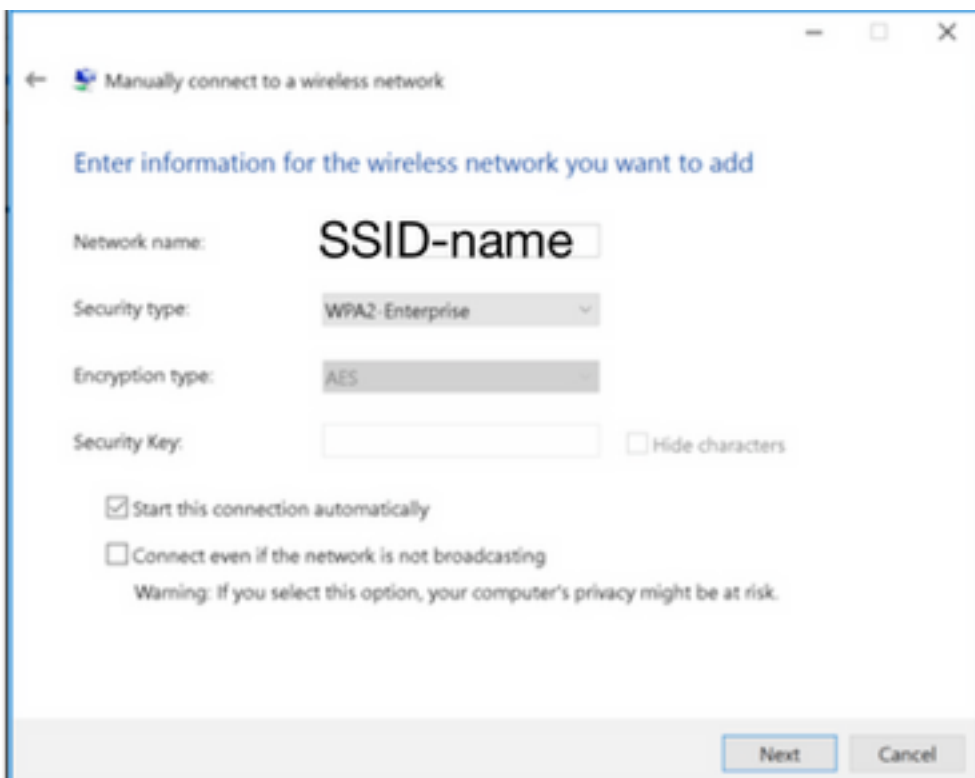
步骤2.导航对网络如镜像所显示，并且互联网>网络和共享中心>单击建立了新连接或网络。



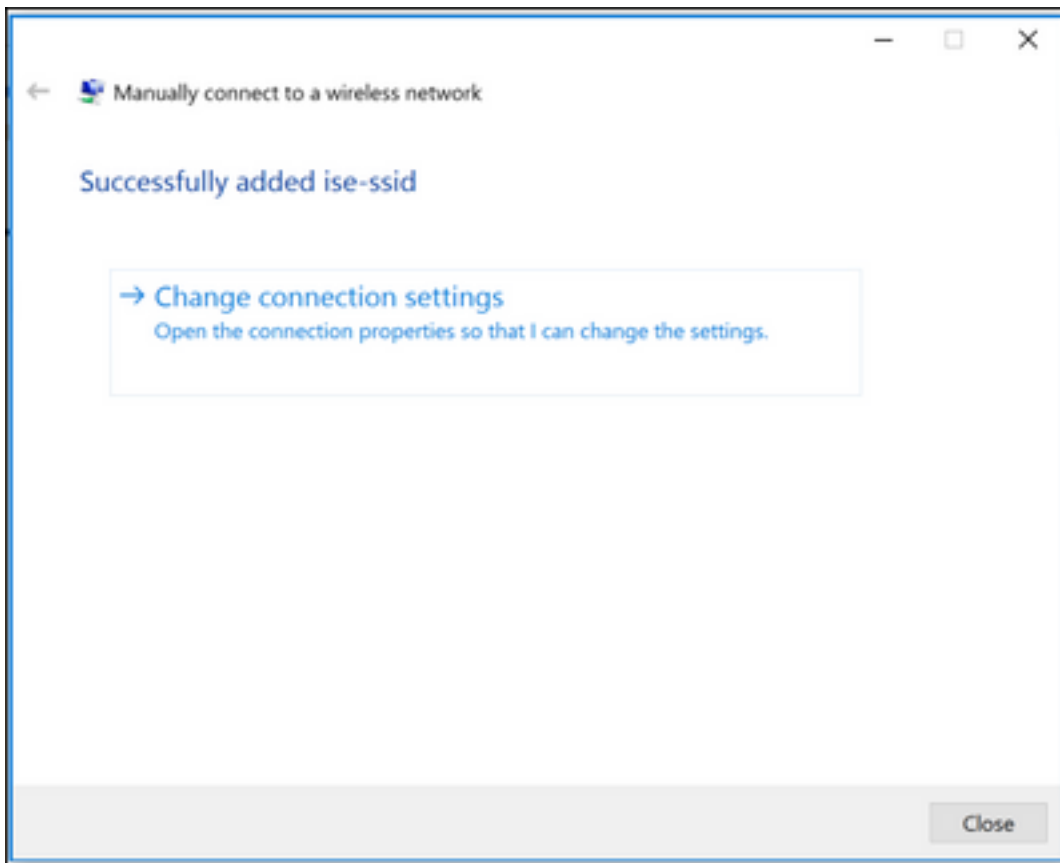
步骤3.选择手工连接对无线网络并且点击在镜像显示的Nextas。



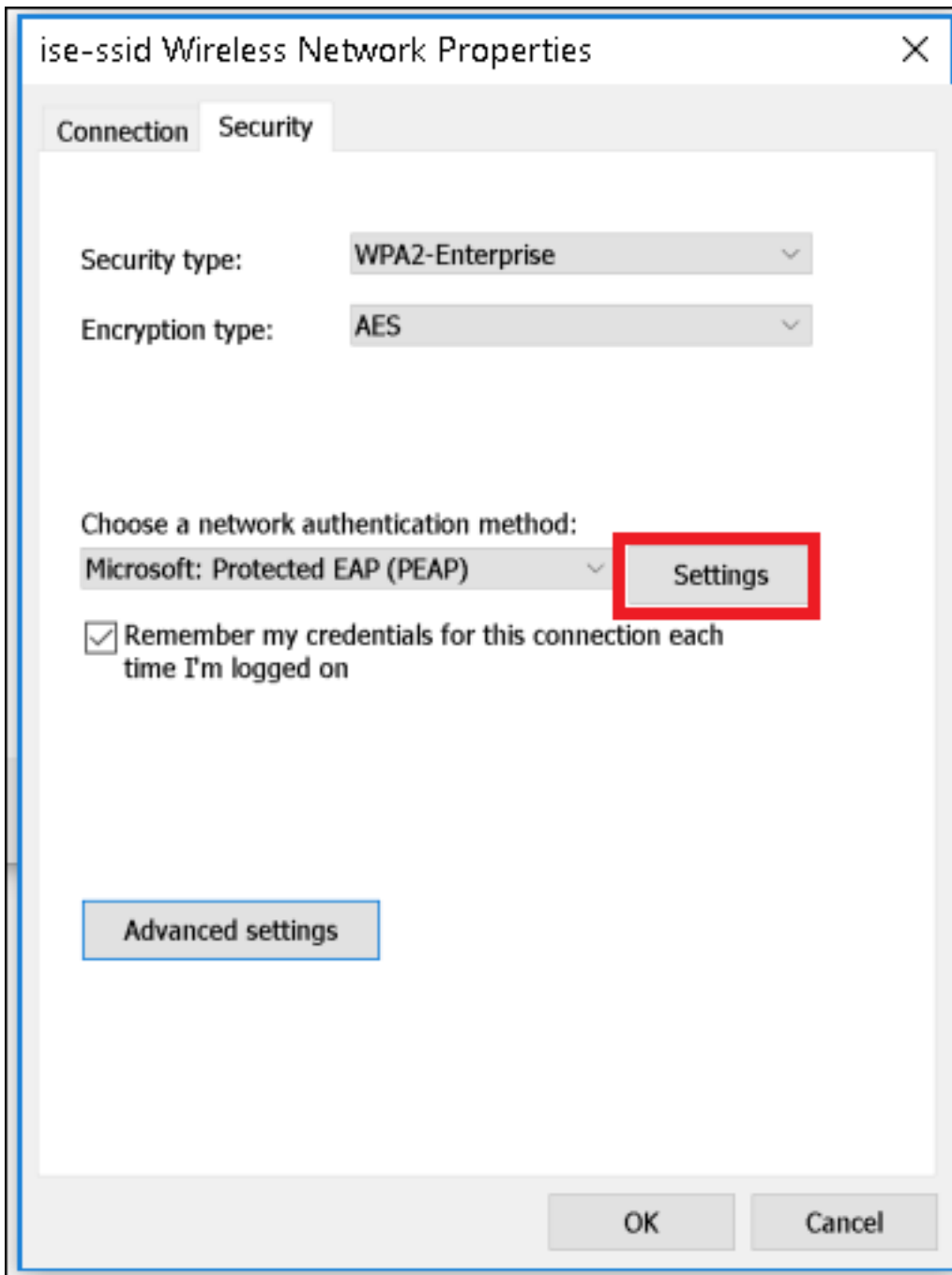
步骤4.如镜像所显示，输入与SSID和安全类型WPA2-Enterprise的名称的信息并且其次单击。



步骤5.如镜像所显示，选择**崔凡吉莱连接设置**为了定制WLAN配置文件的配置。



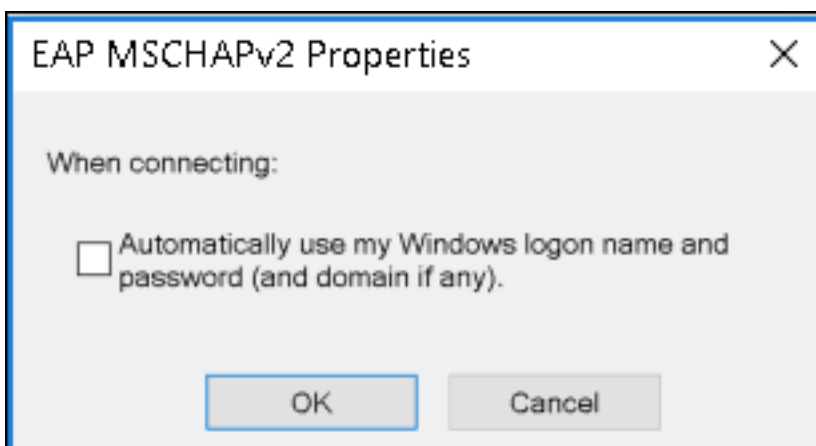
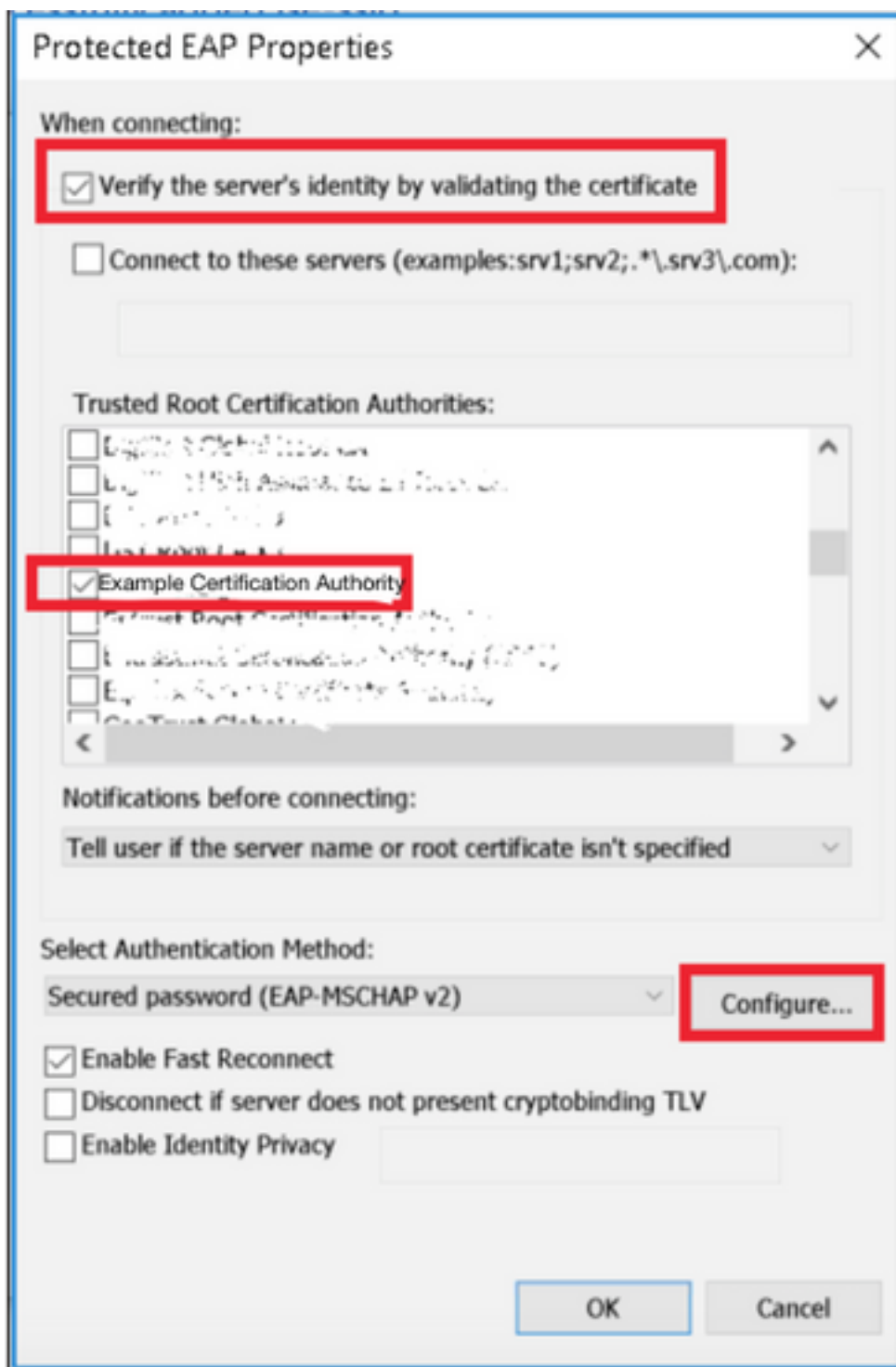
步骤6.如镜像所显示，导航对安全选项卡并且单击**设置**。



步骤7.，如果RADIUS服务器验证，请选择。

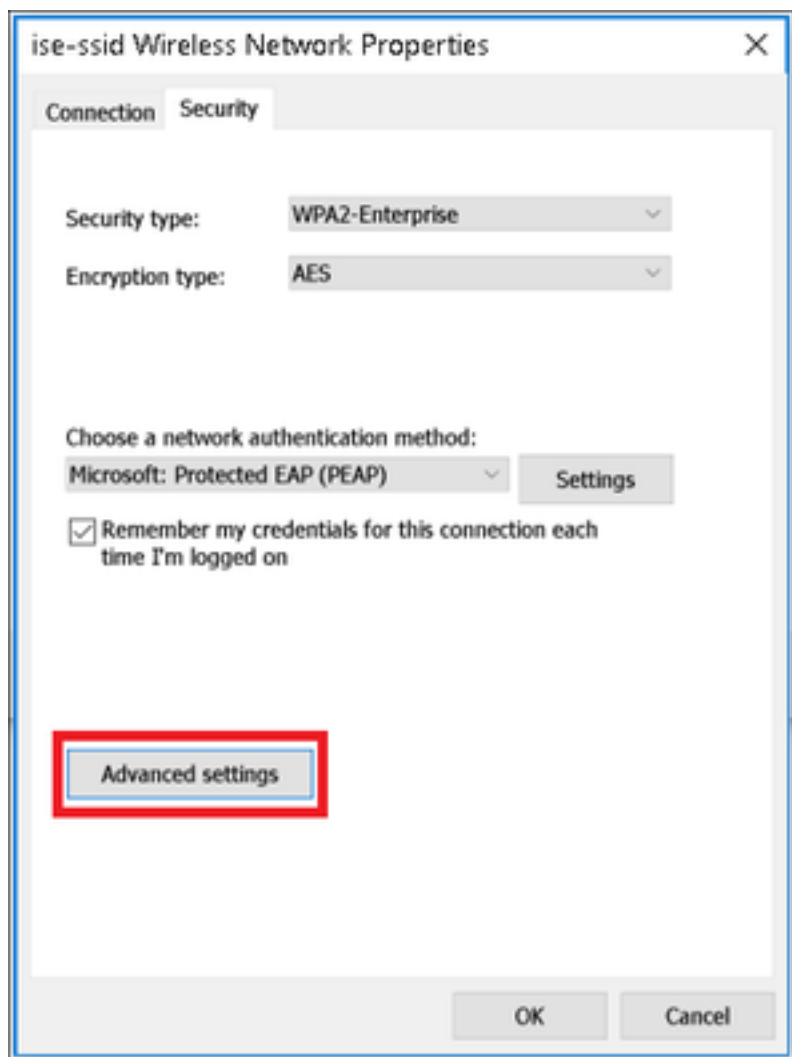
如果是，enable (event)验证服务器的标识通过验证证书和从可靠的根证书颁发机构：列出精选freeRADIUS自签名证书。

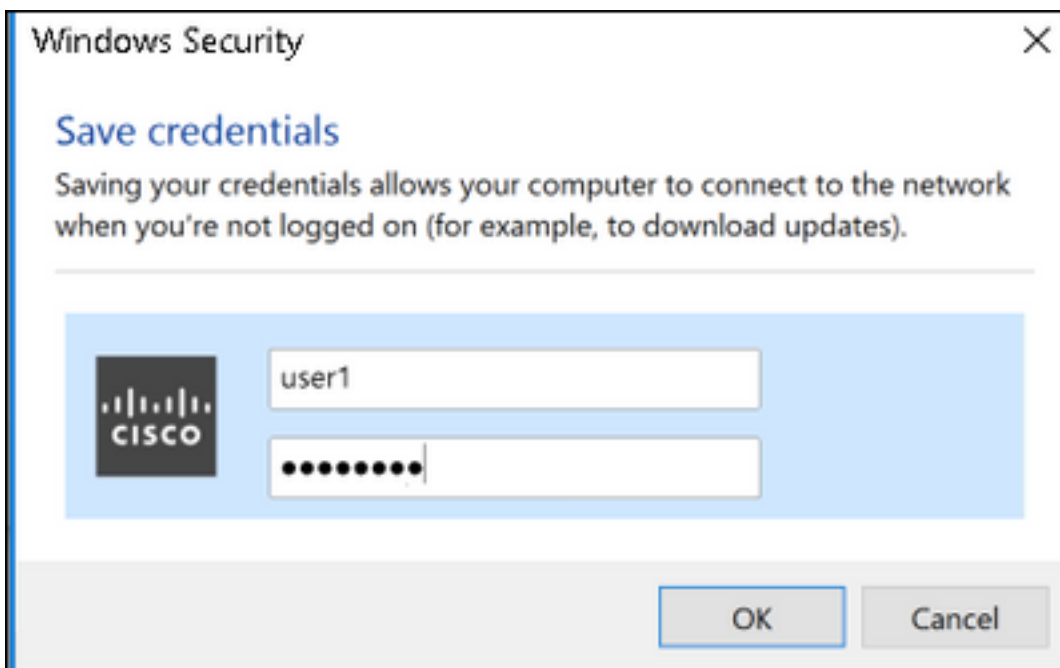
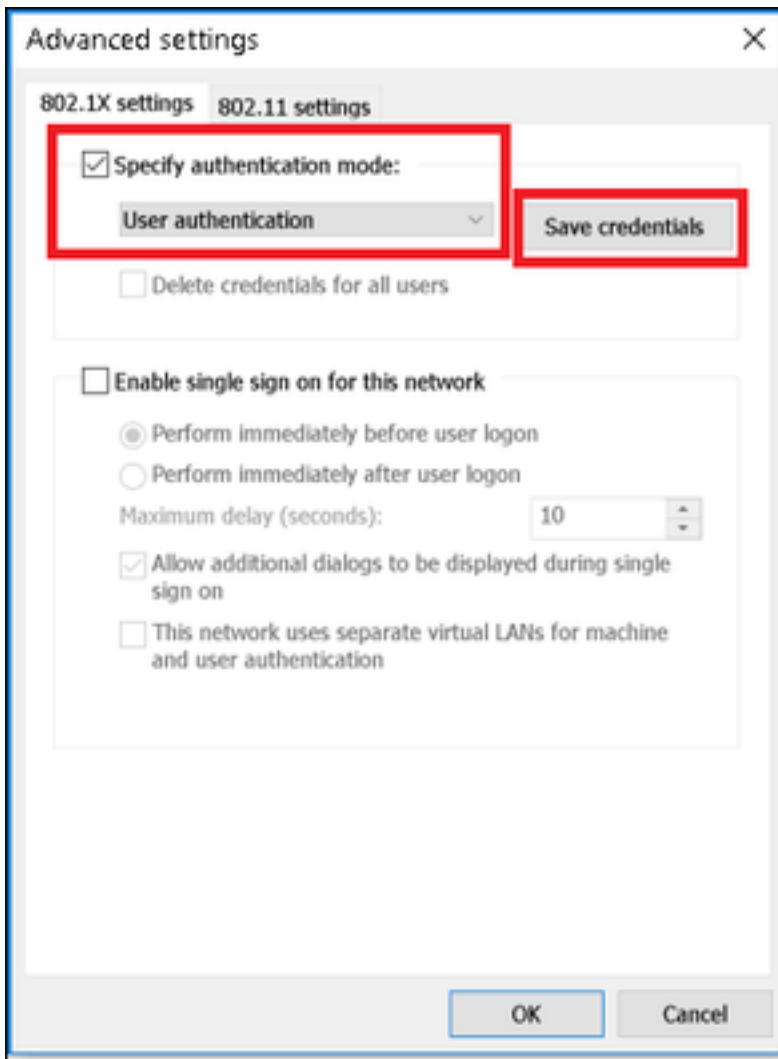
如镜像所显示，以后该请选择自动地配置并且禁用使用我的Windows登录名字和密码...，然后点击OK键。



步骤8.配置用户凭证。

如镜像所显示，一旦回到安全选项卡，请选择在freeRADIUS配置为了验证用户的**先进的设置**，指定认证模式作为**用户认证**并且保存凭证。





验证

使用本部分可确认配置能否正常运行。

在WLC的认证过程

运行下命令为了监控一个特定用户的认证过程：

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

为了使阅读的简单的方法调试客户端输出，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。