配置802.1x — 使用FreeRadius和WLC 8.3的PEAP

目錄

簡介

本檔案介紹如何將具有802.1x安全性和受保護的可擴充驗證通訊協定(PEAP)的無線區域網路(WLAN)設定為可擴充驗證通訊協定(EAP)。 FreeRADIUS用作外部遠端驗證撥入使用者服務(RADIUS)伺服器。

必要條件

需求

思科建議您瞭解以下主題的基本知識：

- Linux
- Vim編輯器
- AireOS無線LAN控制器(WLC)

註：本文檔旨在為讀者提供有關freeRADIUS伺服器上進行PEAP-MS-CHAPv2身份驗證所需

的配置的示例。本文中介紹的freeRADIUS伺服器配置已在實驗室中經過測試，發現可按預期工作。思科技術援助中心(TAC)不支援freeRADIUS伺服器配置。

採用元件

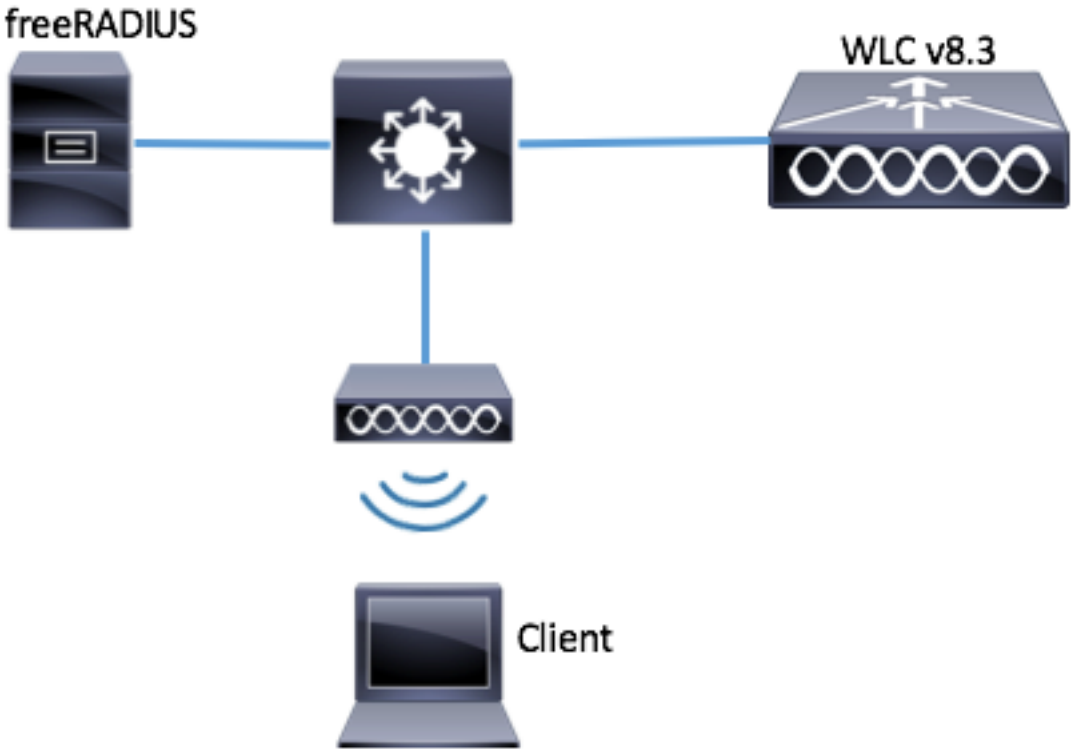
本文中的資訊係根據以下軟體和硬體版本：

- CentOS7或Red Hat Enterprise Linux 7(RHEL7)（建議使用1 GB記憶體和至少20 GB硬碟）
- WLC 5508 v8.3
- MariaDB(MySQL)
- FreeRADIUS
- 7菲律賓比索

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

網路圖表



安裝httpd伺服器和MariaDB

步驟1.運行這些命令以安裝httpd伺服器和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
```

步驟2.啟動並啟用httpd(Apache)和MariaDB伺服器。

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

步驟3.配置初始MariaDB設定以保護它。

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

附註：運行此指令碼的所有部分。建議在生產中使用所有MariaDB伺服器。仔細閱讀每一步。

```
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!
```

步驟4.為freeRADIUS配置資料庫（使用步驟3中配置的相同密碼）。

```
[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上安裝PHP 7

步驟1.運行這些命令以在CentOS7上安裝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
```

安裝FreeRADIUS

步驟1.運行此命令以安裝FreeRADIUS。

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

步驟2.使**radius.service** 在**mariadb.service**之後啟動。

運行此命令：

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

在[**Unit**]一行:

```
After=mariadb.service
```

[Unit]部分必須如下所示：

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

步驟3.啟動並啟用freeradius以在啟動時啟動。

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

步驟4.啟用firewalld以確保安全。

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

步驟5.將永久規則新增到預設區域以允許http、https和radius服務。

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

步驟6.重新載入防火牆以使更改生效。

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

FreeRADIUS

若要將FreeRADIUS設定為使用MariaDB，請執行以下步驟。

步驟1.匯入RADIUS資料庫方案以填充RADIUS資料庫。

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

步驟2.在**/etc**/raddb/mods-enabled下為結構化查詢**語言(SQL)建立軟連結**。

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

步驟3.配置SQL模組/raddb/mods-available/sql並更改資料庫連線引數以套件環境。

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

SQL節必須與以下內容類似。

```
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"
```

步驟4.將/etc/raddb/mods-enabled/sql的組許可權更改為radiusd。

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

WLC在FreeRADIUS上作為驗證、授權和記帳(AAA)使用者端

步驟1。編輯/etc/raddb/clients.conf，設定WLC的共用金鑰。

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

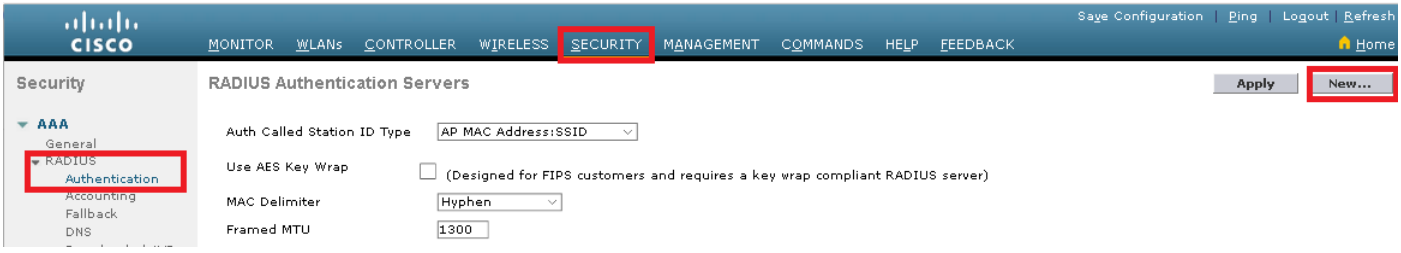
步驟2.在底部，新增控制器IP地址和共用金鑰。

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

在WLC上將FreeRADIUS作為RADIUS伺服器

GUI:

步驟1。開啟WLC的GUI，然後導覽至SECURITY > RADIUS > Authentication > New，如下圖所示。



步驟2.填寫RADIUS伺服器資訊，如圖所示。

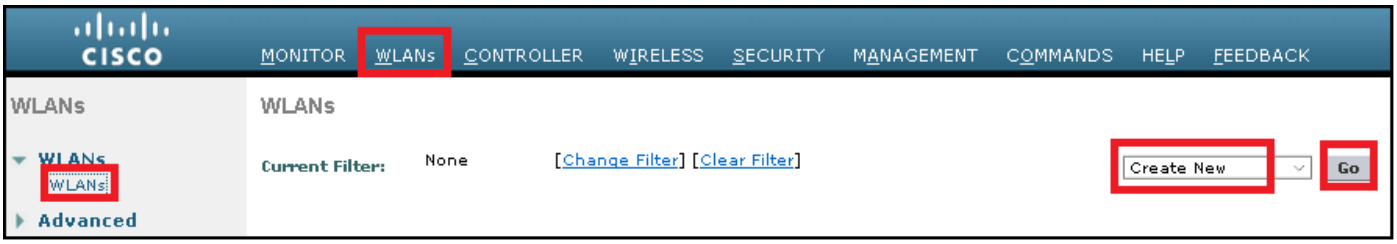
CLI:

```
> 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>
```

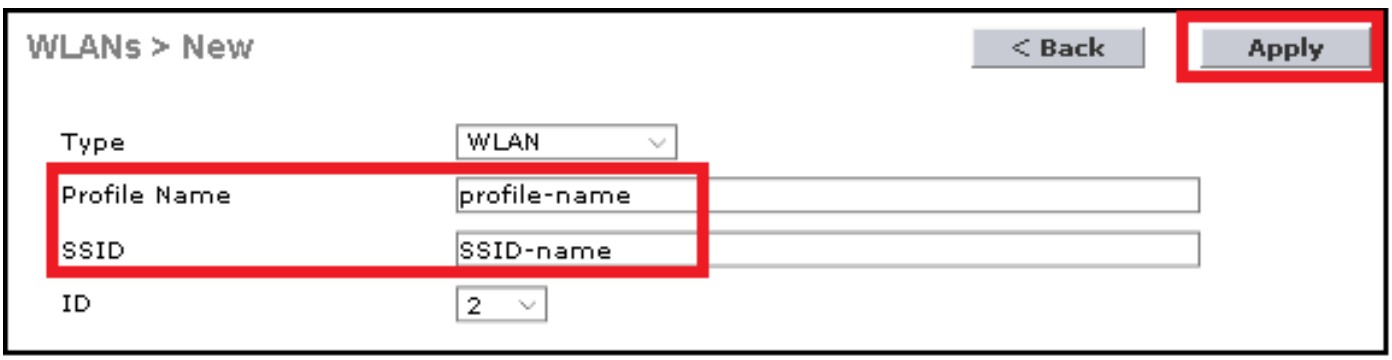
WLAN

GUI:

步驟1。開啟WLC的GUI，然後導覽至**WLANs > Create New >** Goas，如下圖所示。



步驟2.選擇服務集標識符(SSID)和配置文件的名稱，然後按一下Applyas（如圖所示）。



CLI:

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

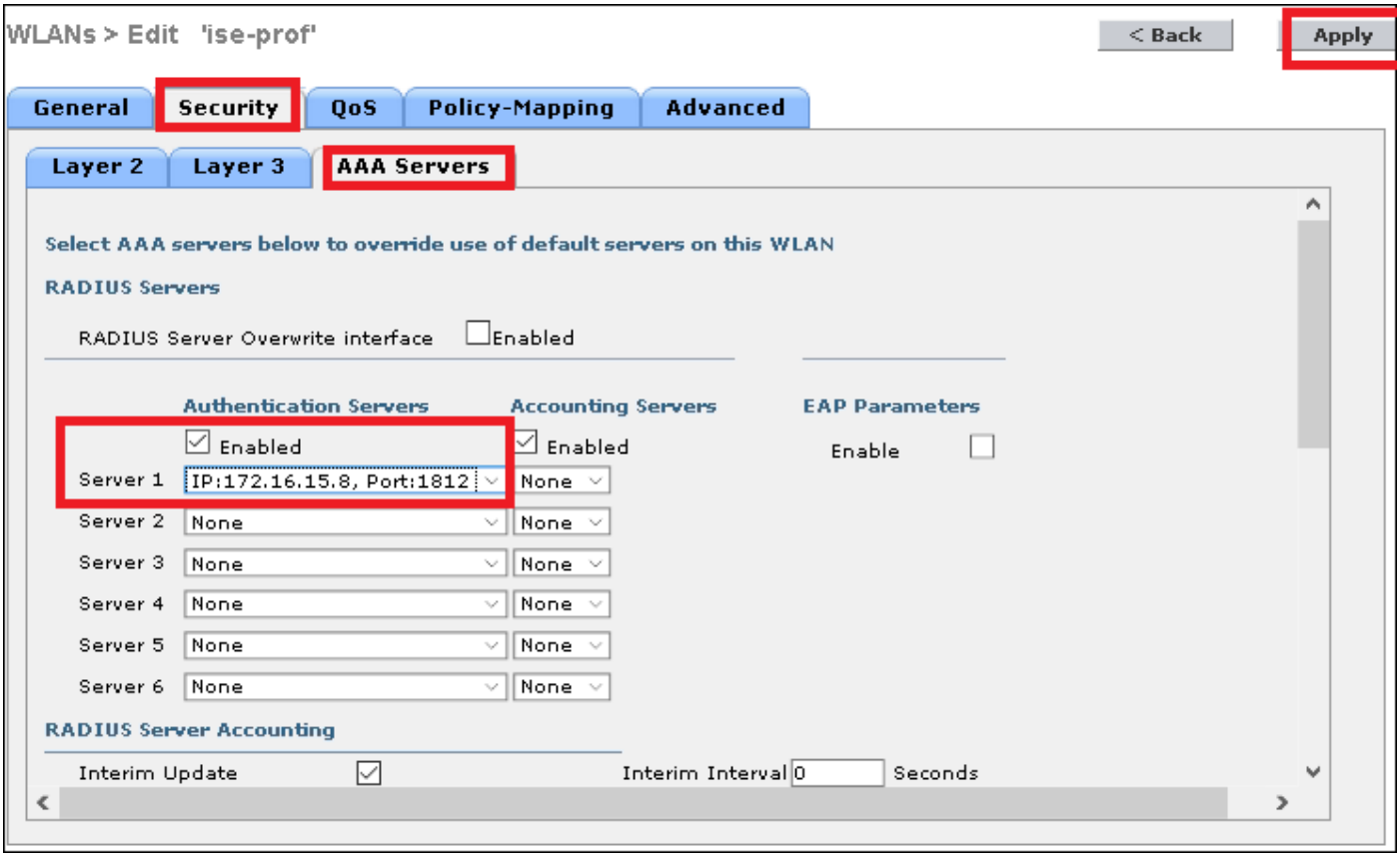
步驟3.將RADIUS伺服器分配給WLAN。

CLI:

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

GUI:

導覽至**Security > AAA Servers**，然後選擇所需的RADIUS伺服器，然後按一下**Apply**，如下圖所示。



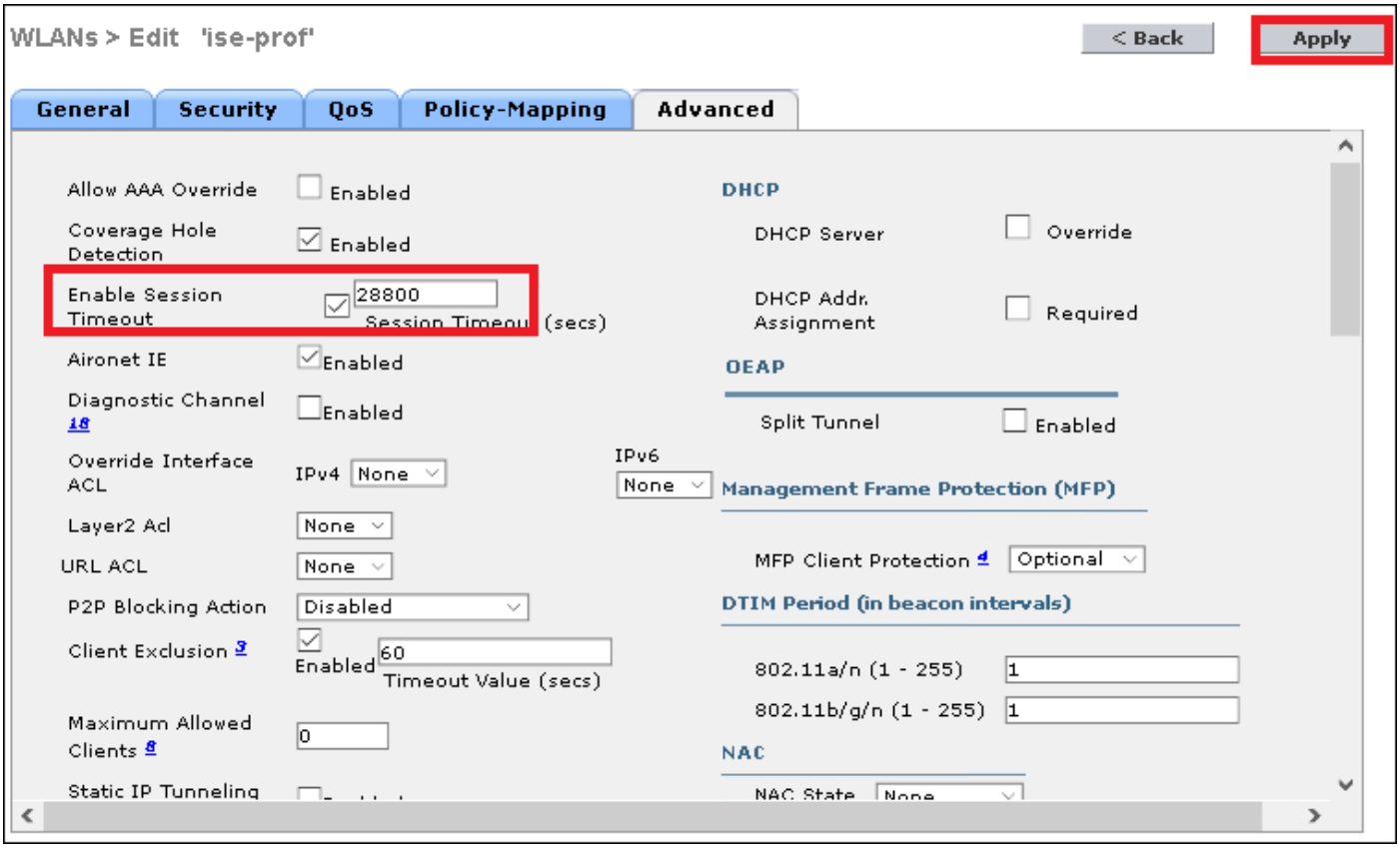
步驟4.（可選）增加會話時間。

CLI:

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

GUI:

導覽至**Advanced > Enable Session Timeout >**按一下**Apply**，如下圖所示。



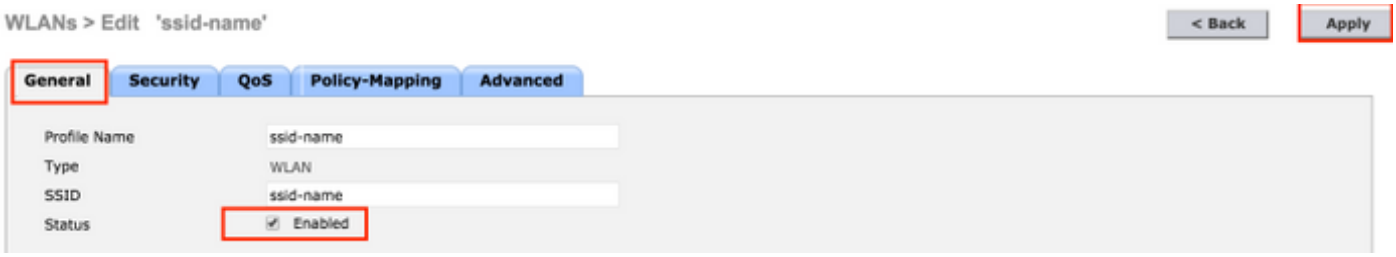
步驟5.啟用WLAN。

CLI:

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

GUI:

導覽至**General > Status > Tick Enabled > Click** Apply，如下圖所示。



將使用者新增到freeRADIUS資料庫

預設情況下，客戶端使用PEAP協定，但freeRadius支援其他方法（本指南未涉及）。

步驟1.編輯文件**/etc/raddb/users**。

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

步驟2.在檔案的底部新增使用者資訊。在本例中，**user1**是使用者名稱，**Cisco123**是密碼。

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

步驟3.重新啟動FreeRadius。

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

freeRADIUS上的憑證

FreeRADIUS附帶預設證書頒發機構(CA)證書和裝置證書，這些證書儲存在路徑/etc/raddb/certs中。這些證書的名稱為ca.pem和server.pem。server.pem是使用者端進行驗證過程中收到的憑證。如果您需要為EAP身份驗證分配不同的證書，只需刪除這些證書並將新證書儲存在同一路徑中，並且使用完全相同的名稱。

終端裝置配置

配置筆記型電腦Windows電腦，以使用802.1x身份驗證和PEAP/MS-CHAP（Microsoft版本的質詢— 握手身份驗證協定）版本2連線到SSID。

要在Windows電腦上建立WLAN配置檔案，有兩種選擇：

1. 在電腦上安裝自簽名證書以驗證和信任freeRADIUS伺服器以完成身份驗證
2. 繞過RADIUS伺服器的驗證，並信任任何用於執行驗證的RADIUS伺服器（不建議，因為這可能成為安全問題）。 這些選項的配置將在終端裝置配置 — 建立WLAN配置檔案中說明。

匯入FreeRADIUS證書

如果您使用安裝在freeRADIUS上的預設證書，請按照以下步驟操作，將EAP證書從freeRADIUS伺服器匯入到終端裝置。

步驟1.從FreeRadius取得憑證：

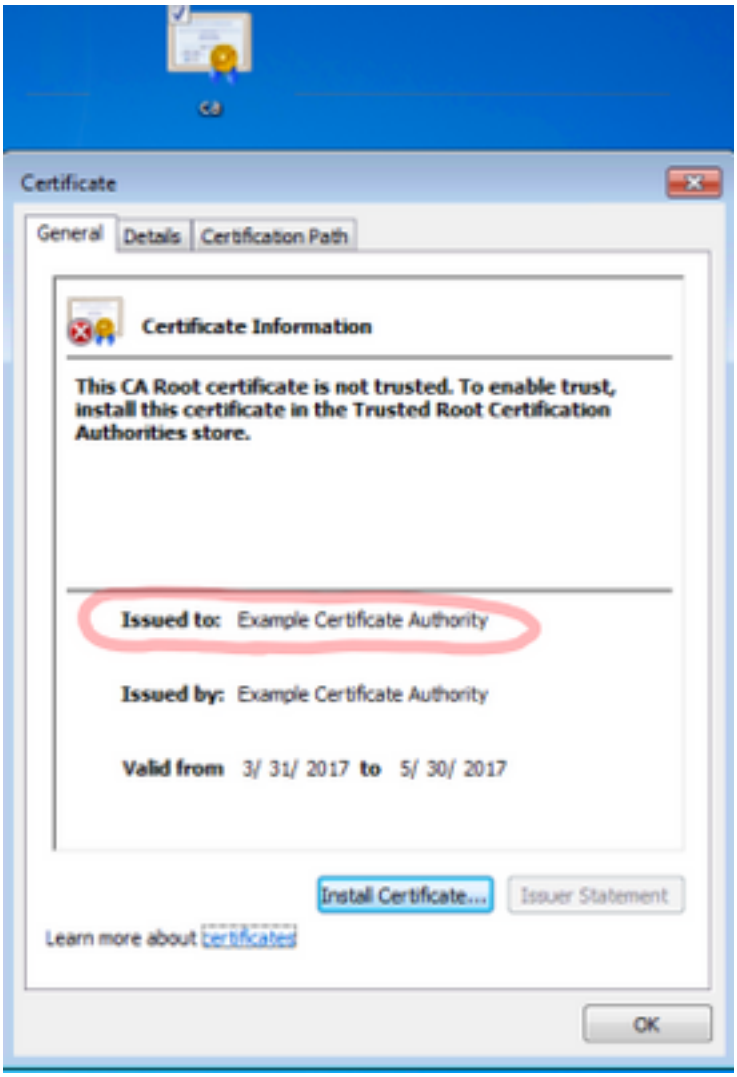
```
[root@tac-mxwireless ~]# cat /etc/raddb/certs/ca.pem

-----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
```

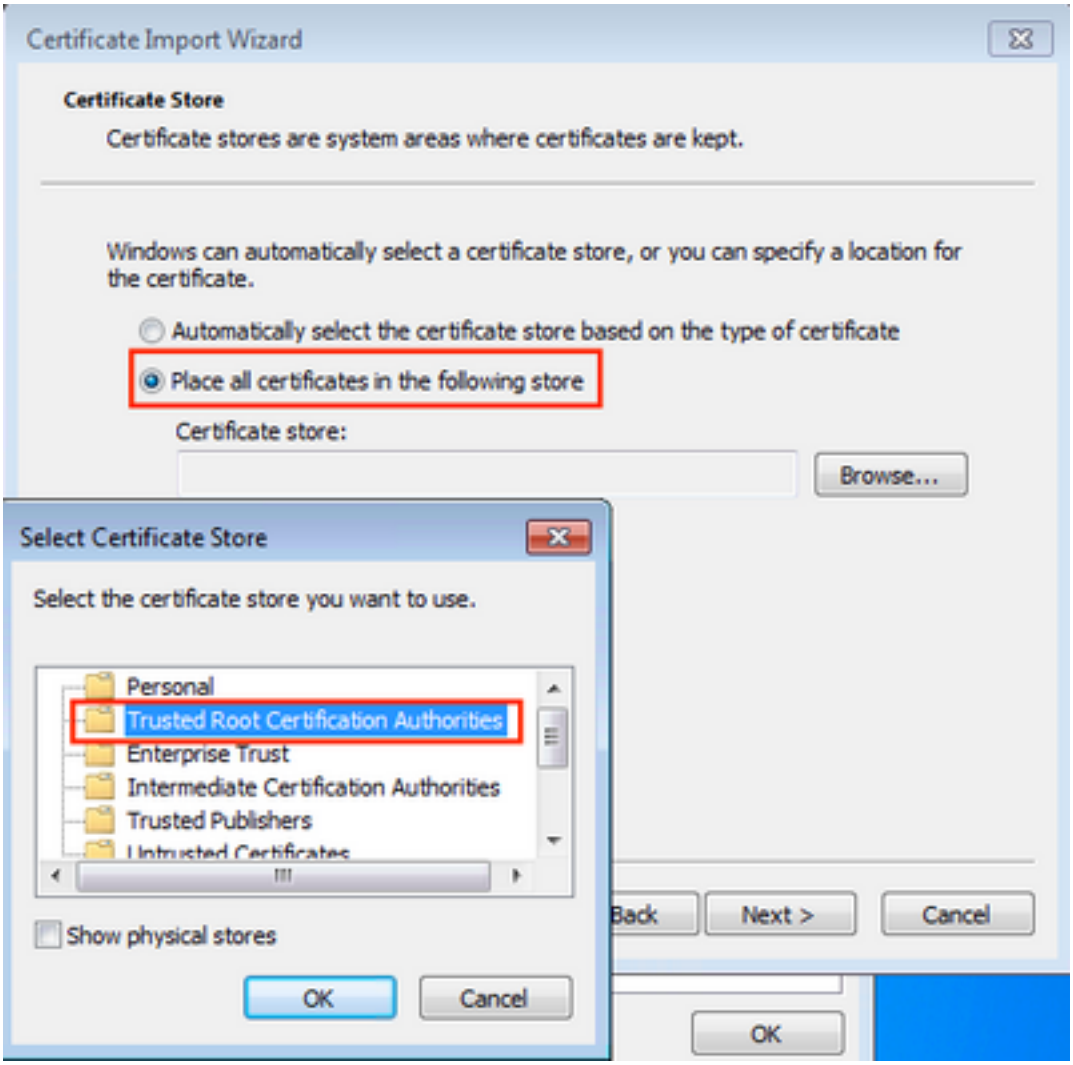
```
b20vZXhhbXBsZV9jYS5jcmwwDQYJKoZIhvcNAQEFBQADggEBACsPR2jiOFXnTsK4
1wnrrMylZZb12gDuqK+zKELox2mzlDMMK83tBsL8yjkv70KeZn821IzfTrTfvhzV
mjX6HgaWfYyMjYYYSw/iEu2JsAtQdpvC3di10nGwVPHlzbozPdov8cZtCb21ynfY
Z6cNjx8+aYQIcsRIyqA1IXMOBwIXo141TOmoODdgfX95lpoLwgktRLkvl7Y7owsz
ChYDO++H7Iewsxx5pQfm56dA2cNrlTwWtMvViKyX7GlpwlbBOxgkLiFJ5+GFbfLh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

步驟2.將上一步的輸出複製並貼上到文本檔案中，並將副檔名更改為.crt

步驟3.按兩下該檔案並選擇**Install Certificate...** 如下圖所示。

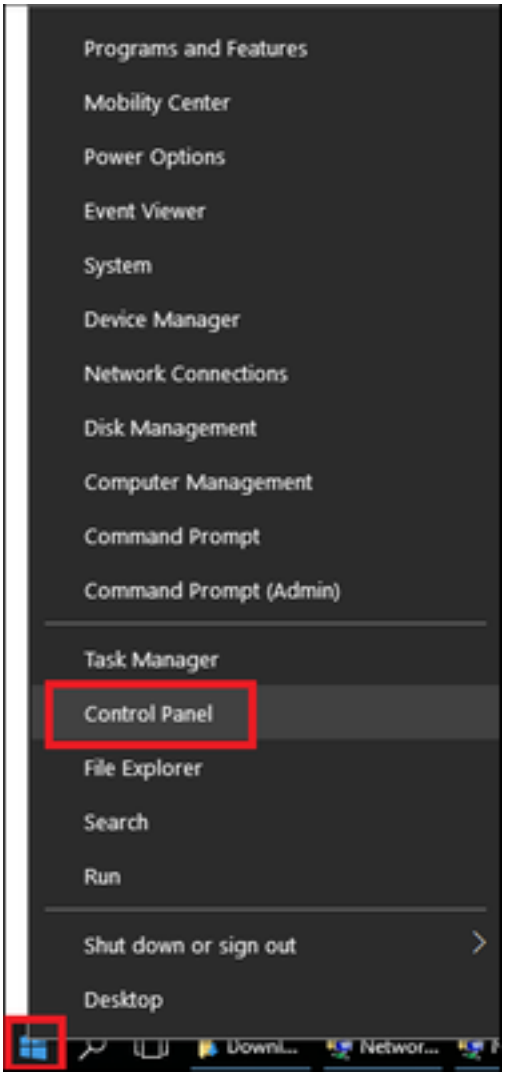


步驟4.將憑證安裝到**受信任的根憑證授權單位**儲存區，如下圖所示。

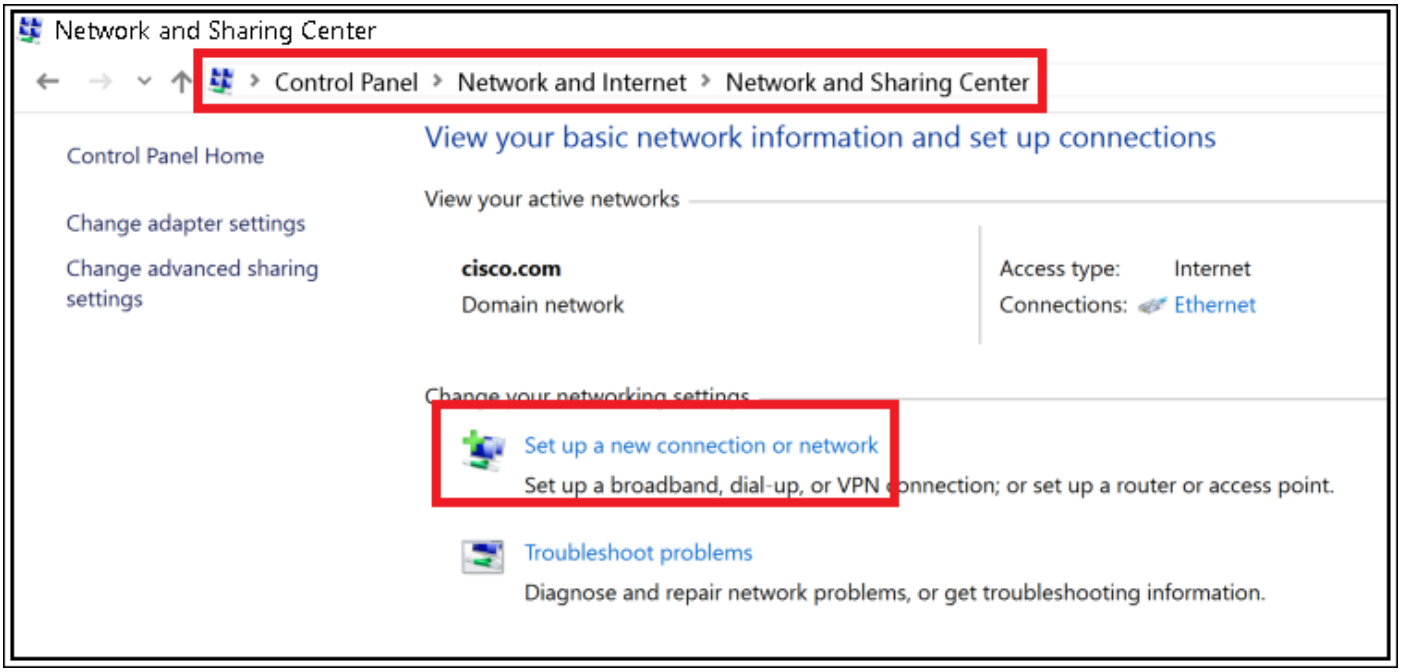


建立WLAN設定檔

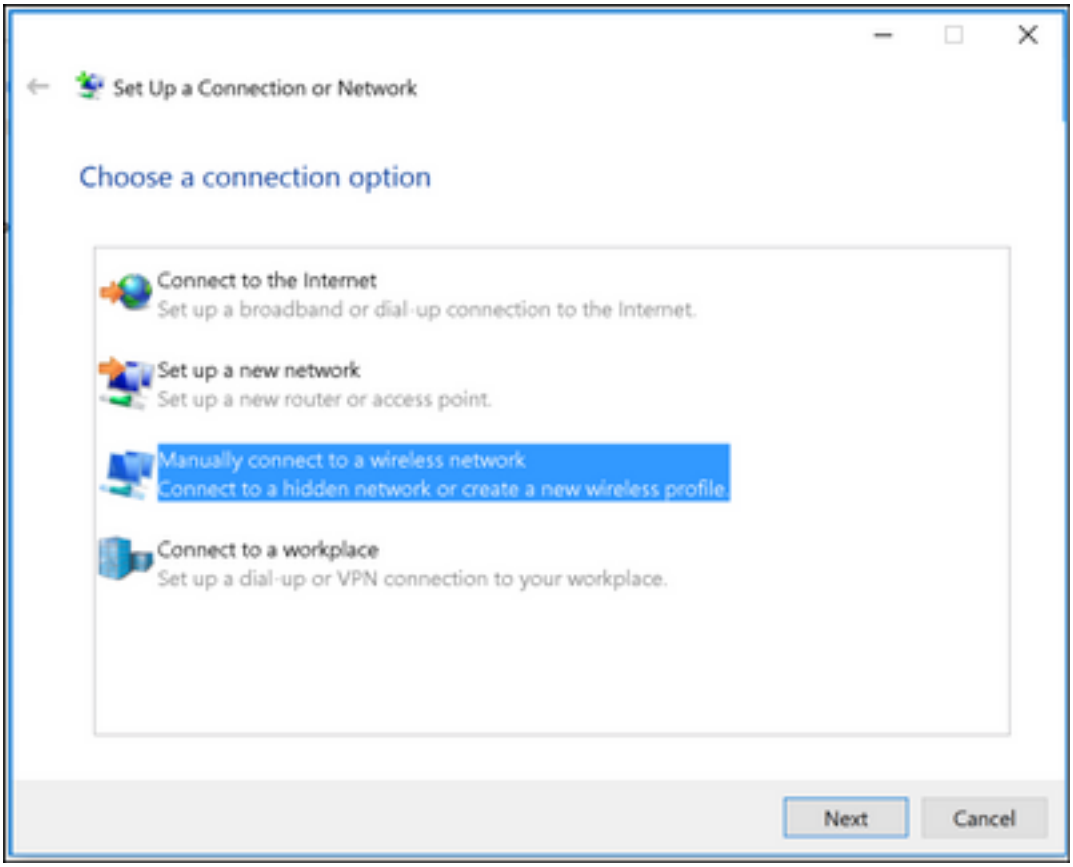
步驟1。按一下右鍵「Start（開始）」圖示並選擇**「Control panel」**，如下圖所示。



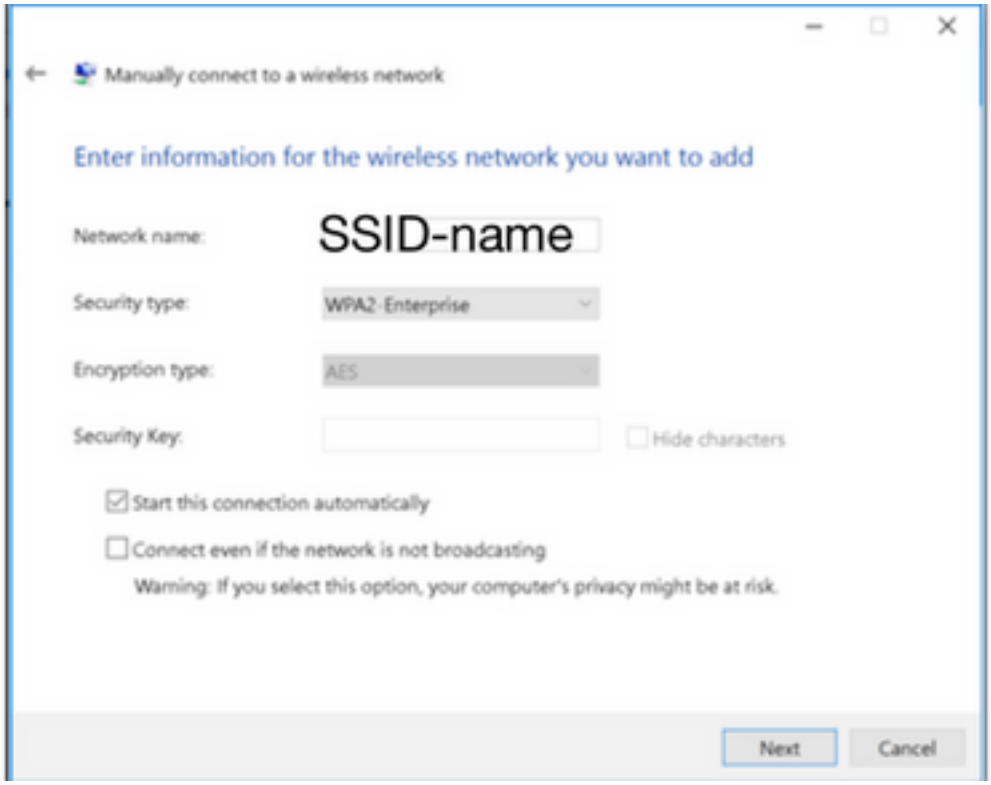
步驟2.導覽至**Network and Internet > Network and Sharing Center>**按一下Set up a new connection or network，如下圖所示。



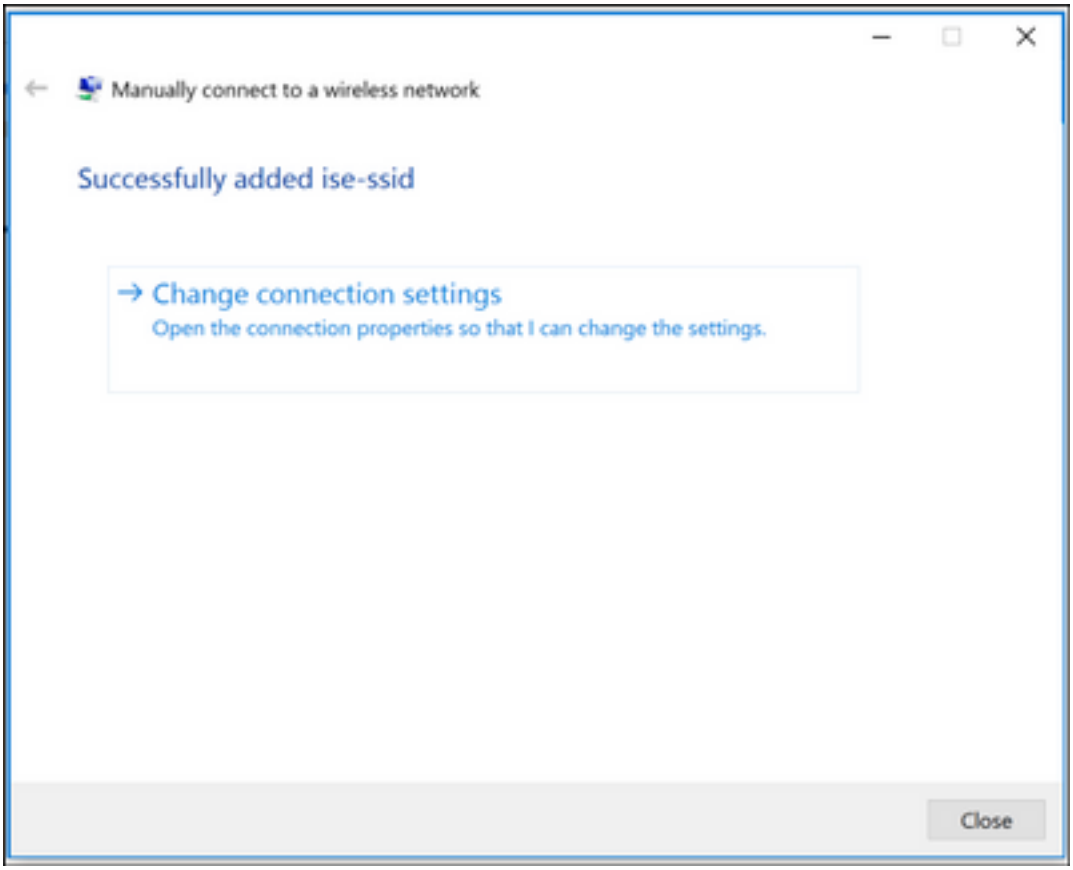
步驟3.選擇**手動連線到無線網路**，然後單擊Nextas（如圖所示）。



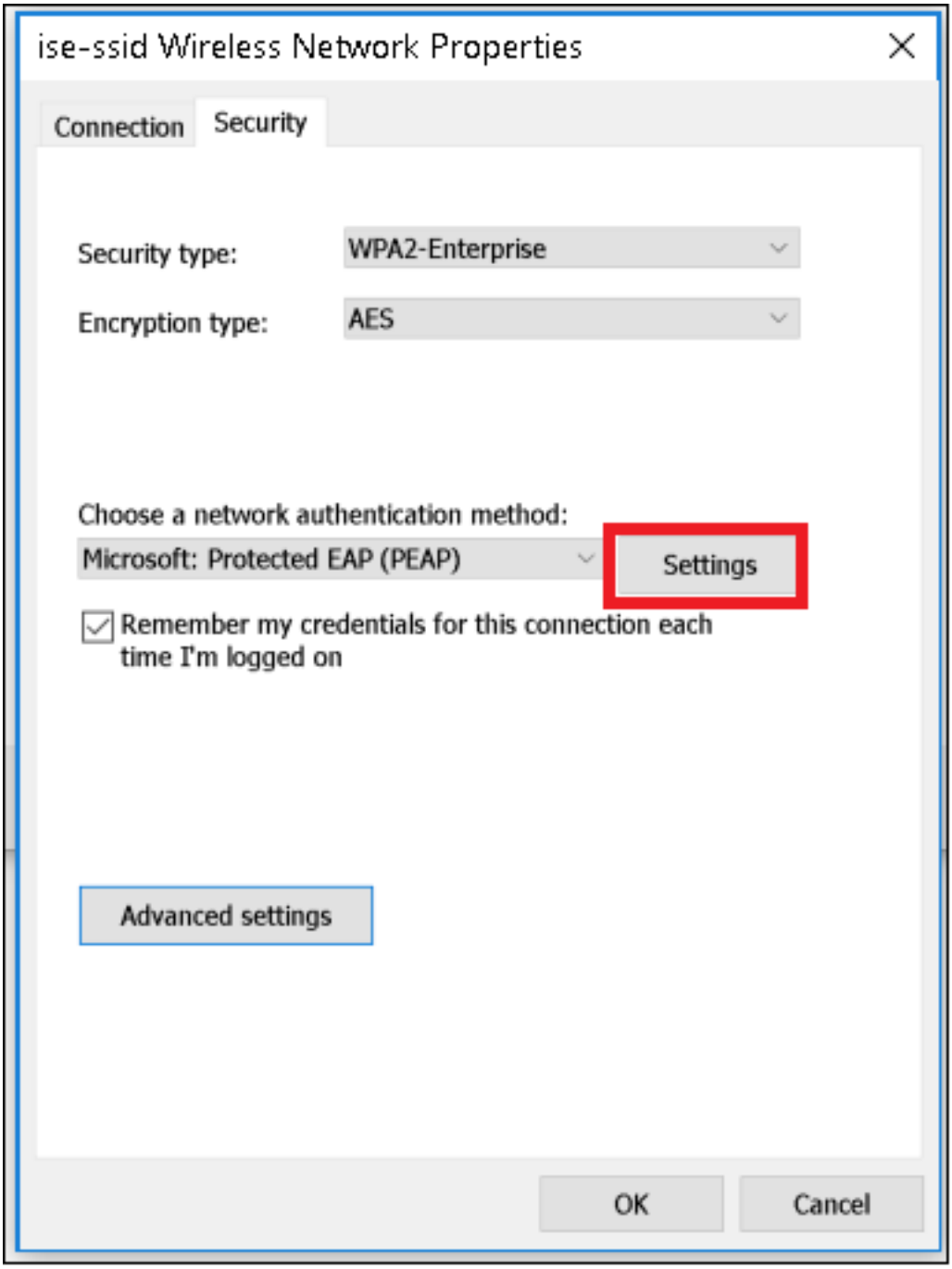
步驟4.輸入SSID名稱和安全型別WPA2-Enterprise的資訊，然後按一下**Next**（如圖所示）。



步驟5.選擇**Change connection settings**以自訂WLAN設定檔的組態，如下圖所示。



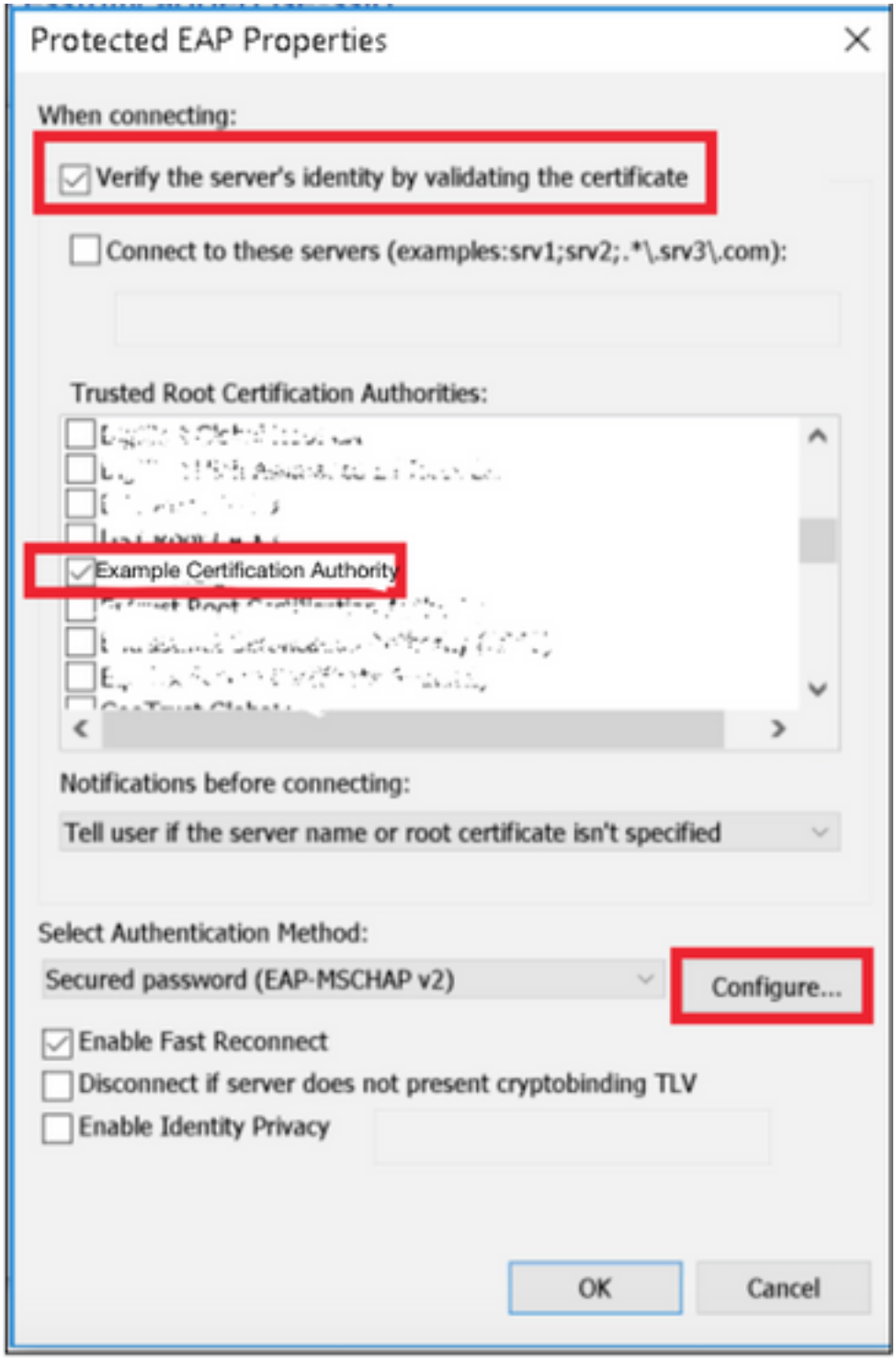
步驟6.導覽至**Security**索引標籤，然後按一下**Settings**，如下圖所示。

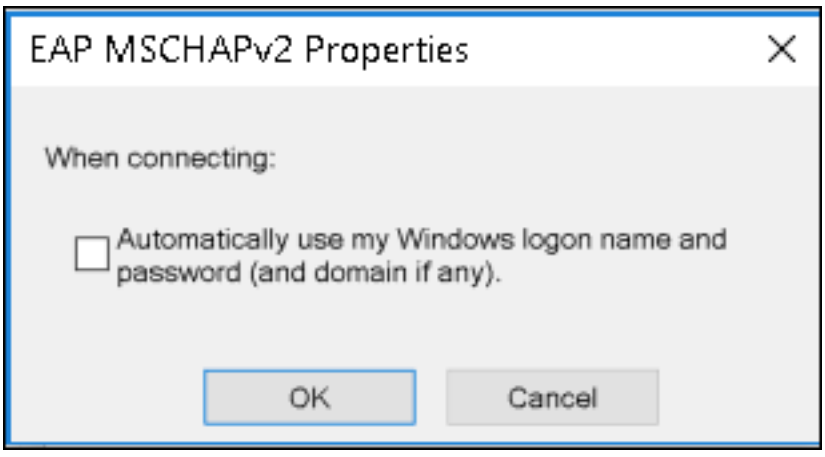


步驟7.選擇是否已驗證RADIUS伺服器。

如果是，請啟用**通過驗證證書和從受信任的根證書頒發機構**驗證服**務器的標識**：清單選擇freeRADIUS的自簽名證書。

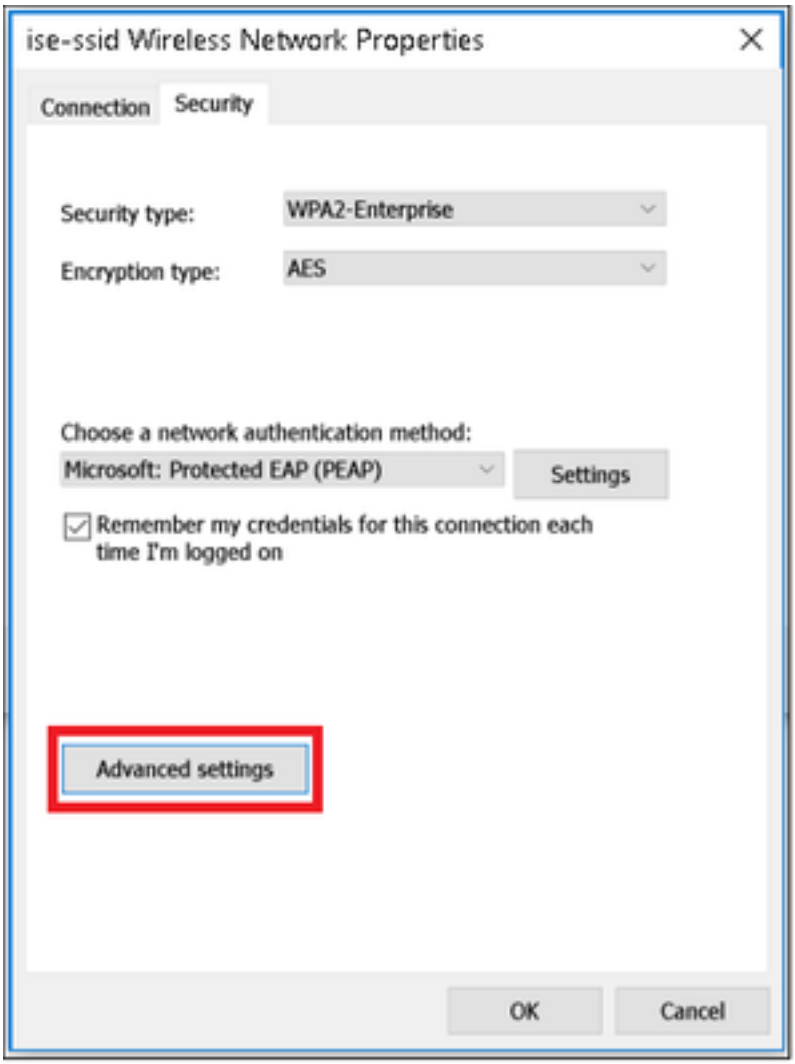
選擇**Configure**並禁用**Automatically use my Windows logon name and password...**後，按一下**OK**，如下圖所示。

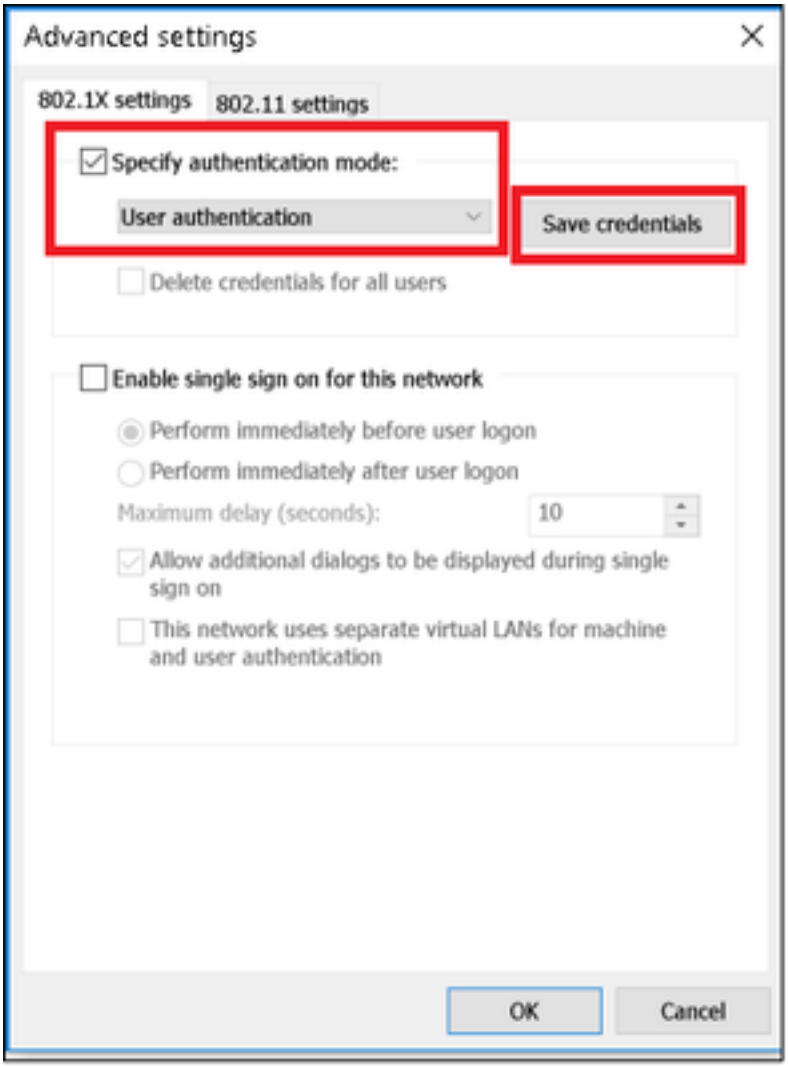

Protected EAP Properties
When connecting:
Verify the server's identity by validating the certificate
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):
Trusted Root Certification Authorities:
Example Certification Authority
Notifications before connecting:
Tell user if the server name or root 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

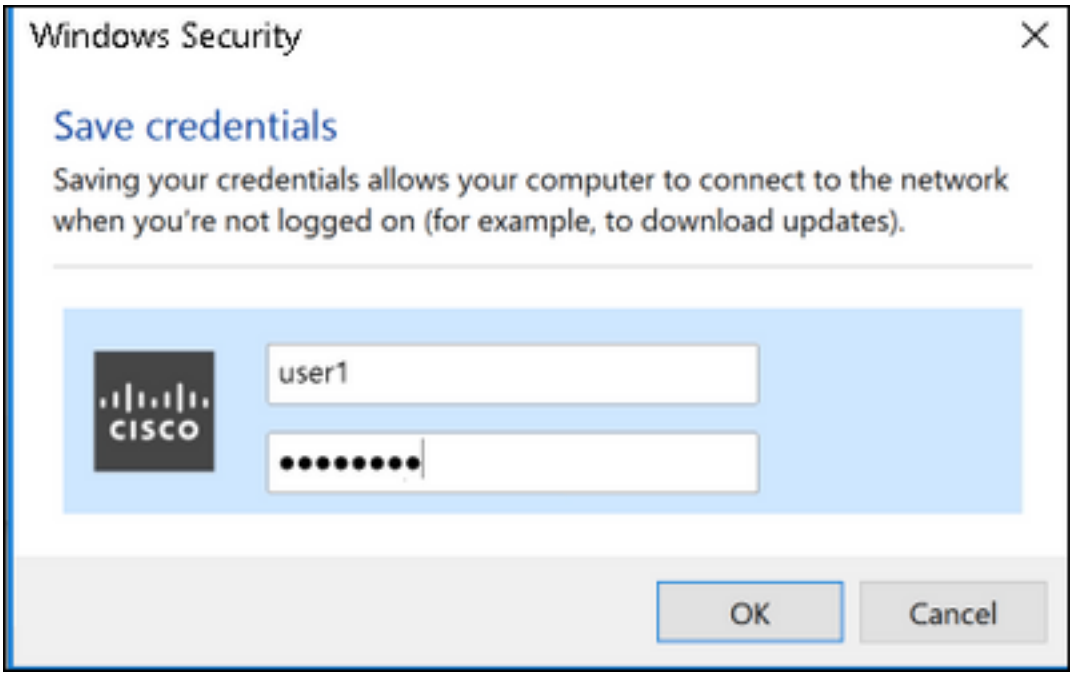

EAP MSCHAPv2 Properties
When connecting:
Automatically use my Windows logon name and password (and domain if any).
OK
Cancel

步驟8.配置使用者憑據。

回到「安全」頁籤後，選擇**Advanced settings**，將身份驗證模式指定為**User authentication**，並儲存在freeRADIUS上配置的憑據以驗證使用者，如下圖所示。







驗證

使用本節內容，確認您的組態是否正常運作。

WLC上的驗證程式

運行以下命令以監控特定使用者的身份驗證過程：

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

若要輕鬆讀取偵錯使用者端輸出，請使用無線偵錯分析器工具：

無線偵錯分析器

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。