FreeRadius と WLC 8.3 を使用した 802.1x - PEAP の設定

目次

概要

これは記述します Extensible Authentication Protocol（EAP）として 802.1X セキュリティの Wireless Local Area Network（WLAN）および Protected Extensible Authentication Protocol（PEAP）を設定する方法を文書化します。 FreeRADIUS は外部 Remote Authentication Dial-In User Service（RADIUS）サーバとして使用されます。

前提条件

要件

Cisco では、次の項目について基本的な知識があることを推奨しています。

- Linux
- Vim エディタ
- AireOS ワイヤレス LAN コントローラ（WLCs）

注: この資料が読者に PEAP-MS-CHAPv2 認証に freeRADIUS サーバで必要な設定の例を与えるように意図されています。 この資料で表記される freeRADIUS サーバコンフィギュレーションはラボでテストされ、予想通り機能するためにありました。 Cisco Technical Assistance Center（TAC）は freeRADIUS サーバコンフィギュレーションをサポートしません。

使用するコンポーネント

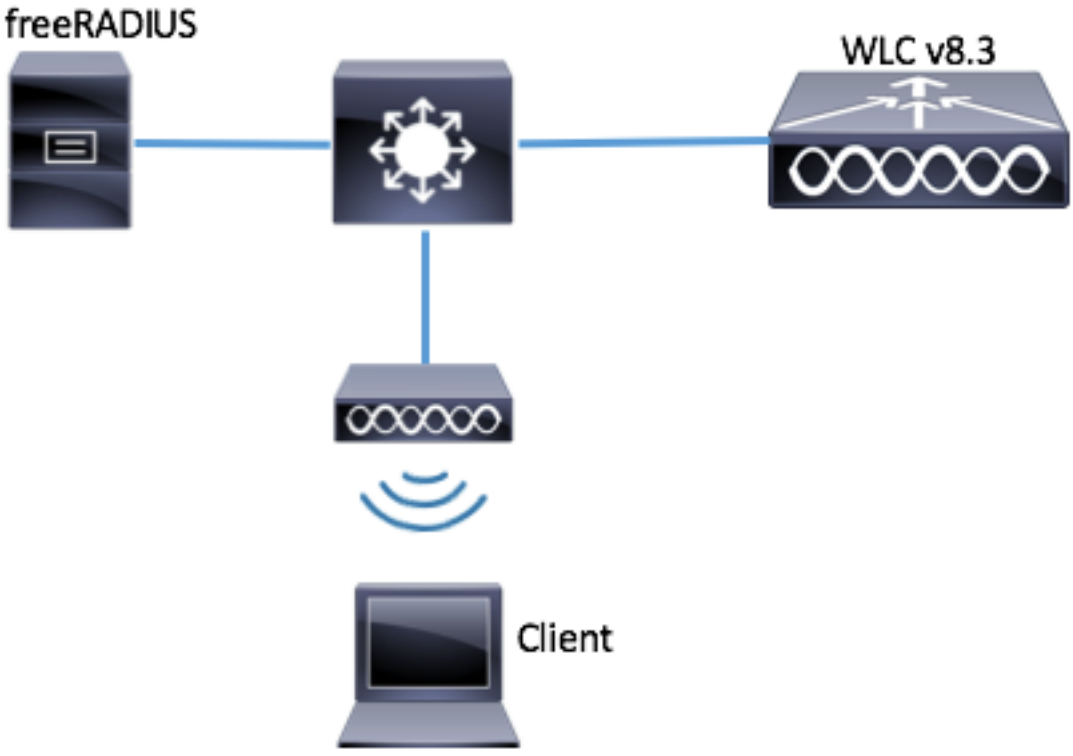
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- CentOS7 か Red Hat Enterprise Linux 7（（1 GB RAM および少なくとも 20 GB HDD 推奨される）RHEL7）
- WLC 5508 v8.3
- MariaDB（MySQL）
- FreeRADIUS
- PHP 7

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

設定

ネットワーク図



httpd サーバおよび MariaDB をインストールして下さい

ステップ 1. httpd サーバおよび MariaDB をインストールするこれらのコマンドを実行して下さい

。

```
[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
```

ステップ 2. httpd （ Apache ）および MariaDB サーバを開始し、イネーブルに設定して下さい。

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

ステップ 3.それを保護するために MariaDB 最初の設定を設定して下さい。

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

注: このスクリプトのすべての一部を経営して下さい。 本番使用中の MariaDB すべてのサーバのために推奨します。 各ステップを熟読して下さい。

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

ステップ 4. freeRADIUS のためのデータベースを設定して下さい（ 3 ）設定されるステップで同じパスワードを使用して下さい。

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

CentOS 7 で PHP 7 をインストールして下さい

ステップ 1. CentOS7 で PHP 7 をインストールするこれらのコマンドを実行して下さい。

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

FreeRADIUS をインストールして下さい

ステップ 1. FreeRADIUS をインストールするこのコマンドを実行して下さい。

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

呼び出します。 mariadb.service の後で **radius.service 開始を**して下さい。

次のコマンドを実行します。

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

[]セクションの行を追加して下さい:

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

[ユニット]セクションはこのようになる必要があります:

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

ステップ 3. freeradius を起動します始め、で開始しことを可能にして下さい。

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

ステップ 4.セキュリティ用のイネーブル firewalld。

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

ステップ 5. http、https および RADIUSサービスを許可するデフォルトのゾーンに常置ルールを追加して下さい。

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

ステップ 6.実施される変更のためのリロード firewalld。

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

FreeRADIUS

FreeRADIUS を MariaDB を使用するために設定するために次の手順に従って下さい。

ステップ 1. RADIUS データベースを読み込む RADIUS データベース方式をインポートして下さい。

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

ステップ 2. **/etc/raddb/mods-enabled** の下で構造化照会言語 （ SQL ）のためのソフト リンクを作成して下さい。

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

ステップ 3. SQL モジュール /raddb/mods-available/sql を設定し、スイートにデータベース接続パラメータを環境変更して下さい。

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

SQL セクションはこれに類似したに検知 する必要があります。

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

ステップ 4. radiusd に **/etc/raddb/mods-enabled/sql** の集団権を変更して下さい。

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

FreeRADIUS の認証、許可、アカウンティング（ AAA ） クライアントとして WLC

ステップ 1. WLC のための共有鍵を設定するために **/etc/raddb/clients.conf** を編集して下さい。

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

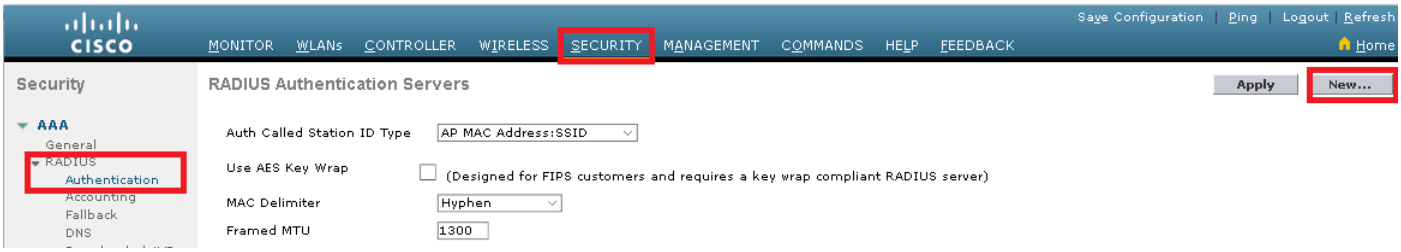
呼び出します。 下部ので、コントローラ IP アドレスおよび共有鍵を追加して下さい。

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

WLC の RADIUSサーバとして FreeRADIUS

GUI：

ステップ 1. WLC の GUI を開き、**セキュリティ > RADIUS > 認証**に > イメージに示すように**新しい**ナビゲート して下さい。



ステップ 2.イメージに示すように RADIUSサーバ情報を一杯にして下さい。

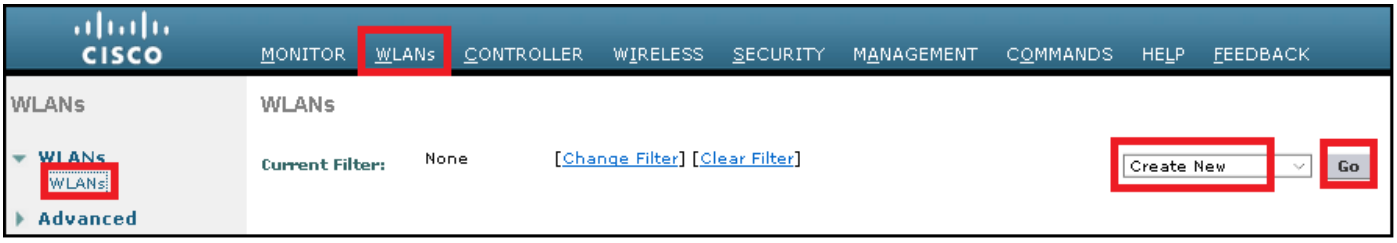
CLI：

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

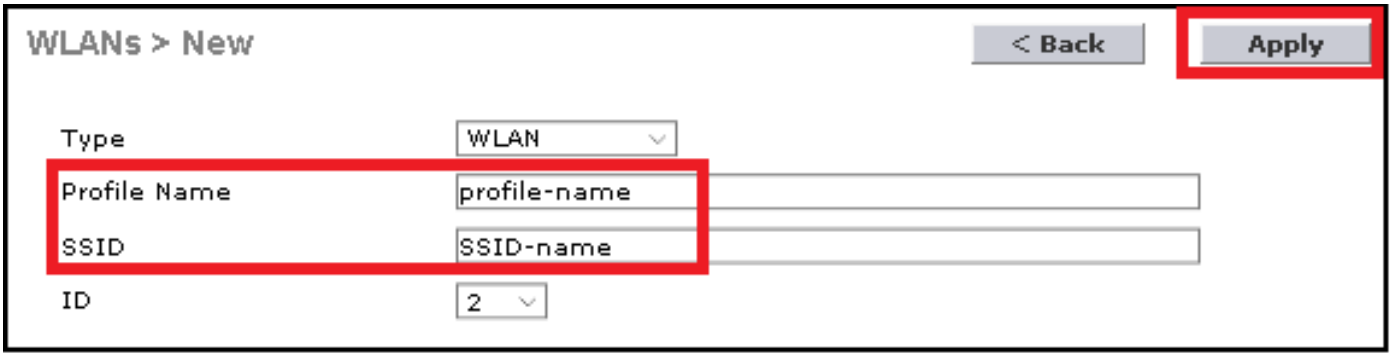
WLAN

GUI：

ステップ 1. WLC およびナビゲートの GUI をに **WLAN > 作成します新しい** > イメージで示されている **Goas** 開いて下さい。



ステップ 2. Service Set Identifier（SSID）およびプロファイルの名前を選択し、そしてイメージで示されている **Applyas をクリックして下さい。**



CLI：

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

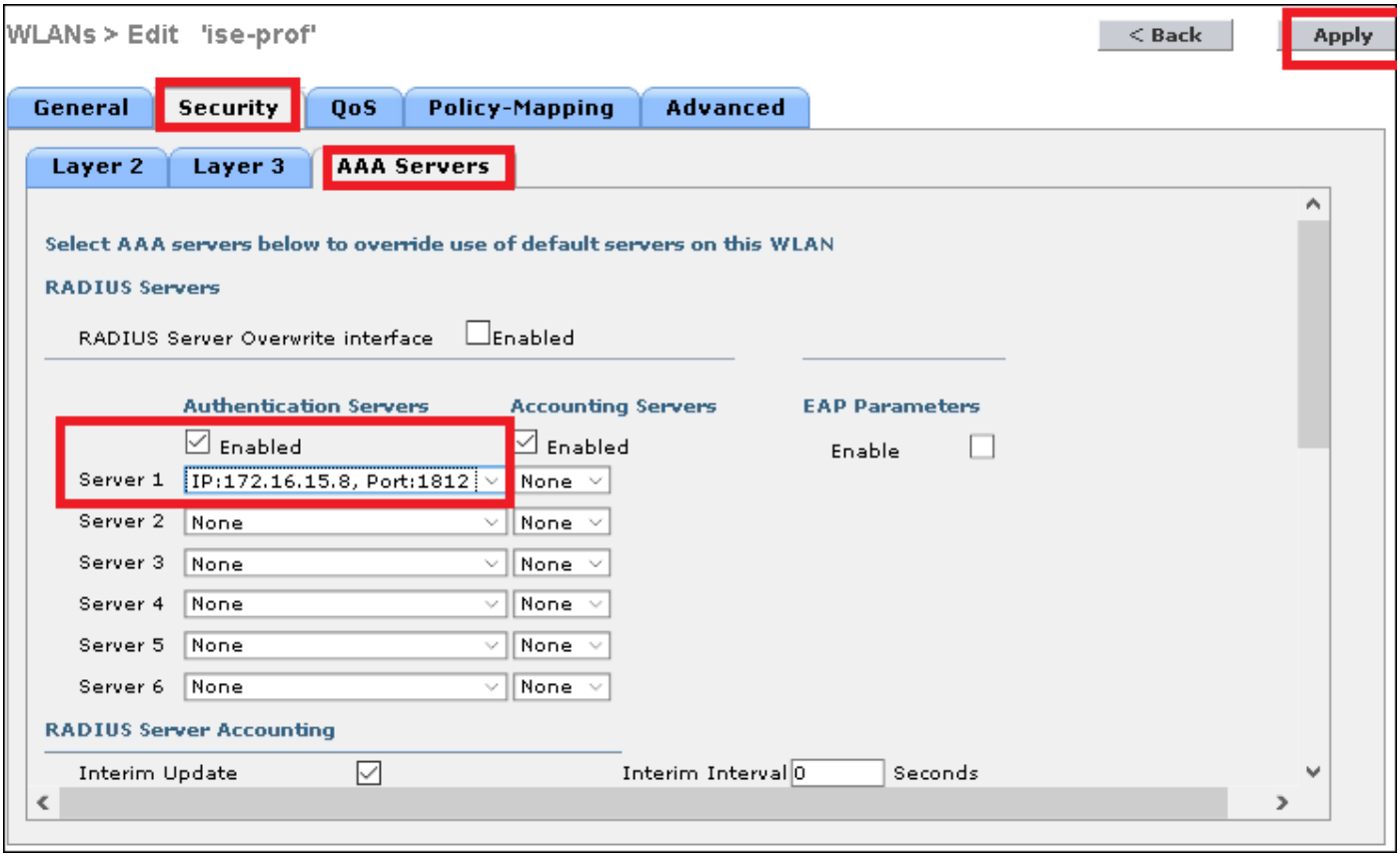
ステップ 3. WLAN に RADIUSサーバを割り当てて下さい。

CLI：

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

GUI：

セキュリティ > AAA サーバへのナビゲートはおよび望ましい RADIUSサーバを選択しましたり、そしてイメージに示すように『Apply』 をクリック します。



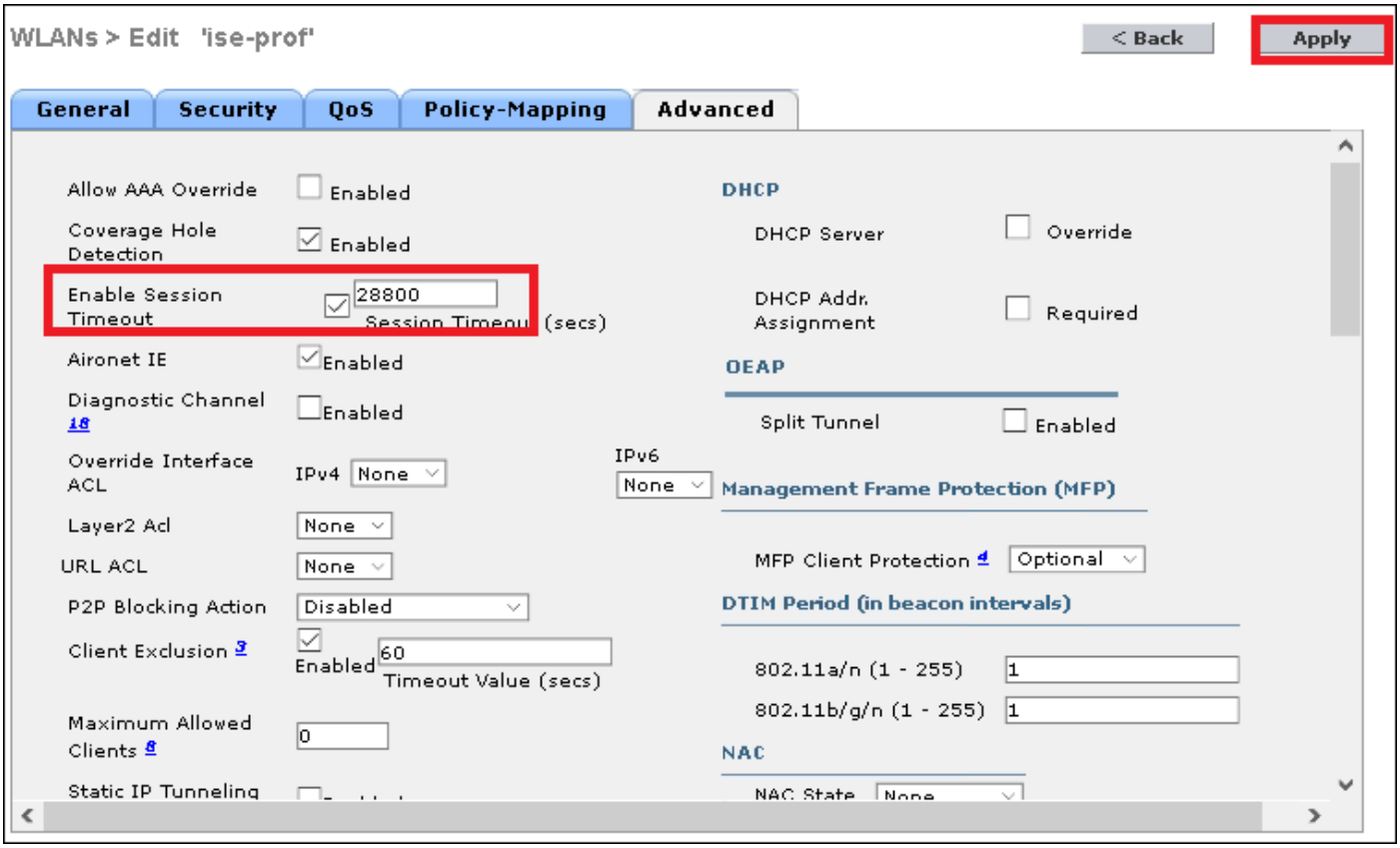
ステップ 4.任意でセッションタイムを増加して下さい。

CLI：

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

GUI：

> イネーブル セッション タイムアウトはイメージに示すように**高度に > **『Apply』 をクリックします ナビゲート します。



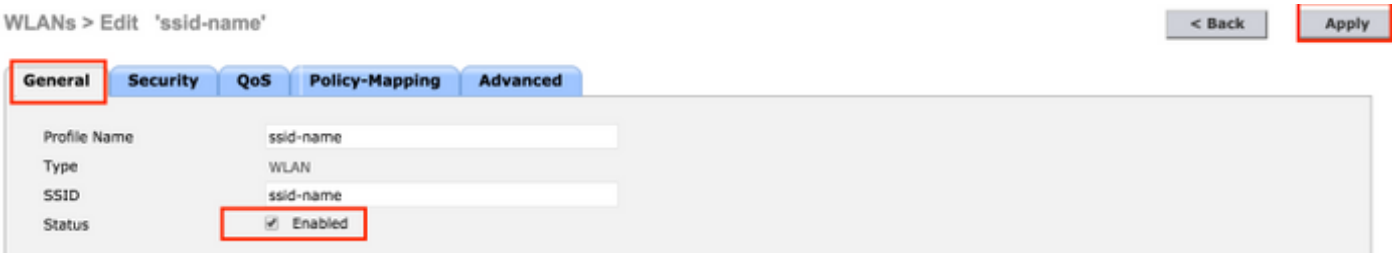
ステップ 5. WLAN を有効に して下さい。

CLI：

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

GUI：

一般 > イネーブルになっているステータス > ティックに > 『Apply』 をクリック します イメージに示すようにナビゲート して下さい。



freeRADIUS データベースにユーザを追加して下さい

デフォルトでクライアントは PEAP プロトコルを、どんなに freeRadius サポート他の方式使用します（ このガイドでカバーされない ）。

ステップ 1.ファイル **/etc/raddb/users を**編集して下さい。

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

呼び出します。 ファイル アペンドの下部のユーザー情報。 この例では、**user1 は**ユーザ名およ

び Cisco123 パスワードです。

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

ステップ 3.再起動 FreeRadius。

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

freeRADIUS の認証

FreeRADIUS はパス /etc/raddb/certs で保存されるデフォルト認証 Authoritiy（CA）認証およびデバイス認証が付いています。 これらの認証の名前は認証プロセスを通過する間、ca.pem および server.pem server.pem ですクライアントが受け取る認証です。 EAP 認証に別の認証を割り当てる必要があればそれらを単に削除でき、それの同じパスの新しいものを保存するために同じ名前を強要して下さい。

エンド デバイス設定

SSID に接続するために 802.1X 認証および PEAP/MS-CHAP（Challenge-Handshake Authentication Protocol の Microsoft バージョン）バージョン 2 でラップトップ Windows マシンを設定して下さい。

そこのウィンドウ マシンの WLAN プロファイルを作成するために 2 つのオプションでであって下さい:

1. freeRADIUS サーバを認証を完了するために検証し、信頼するようにマシンで自己署名証明書をインストールして下さい
2. それがセキュリティ上の問題になることができるように） RADIUSサーバの検証をバイパスし、認証を信頼して下さい（推奨されない、行うのに使用される RADIUSサーバを。 これらのオプションのための設定はエンド デバイス設定で説明されます- WLAN プロファイルを作成して下さい。

FreeRADIUS 認証をインポートして下さい

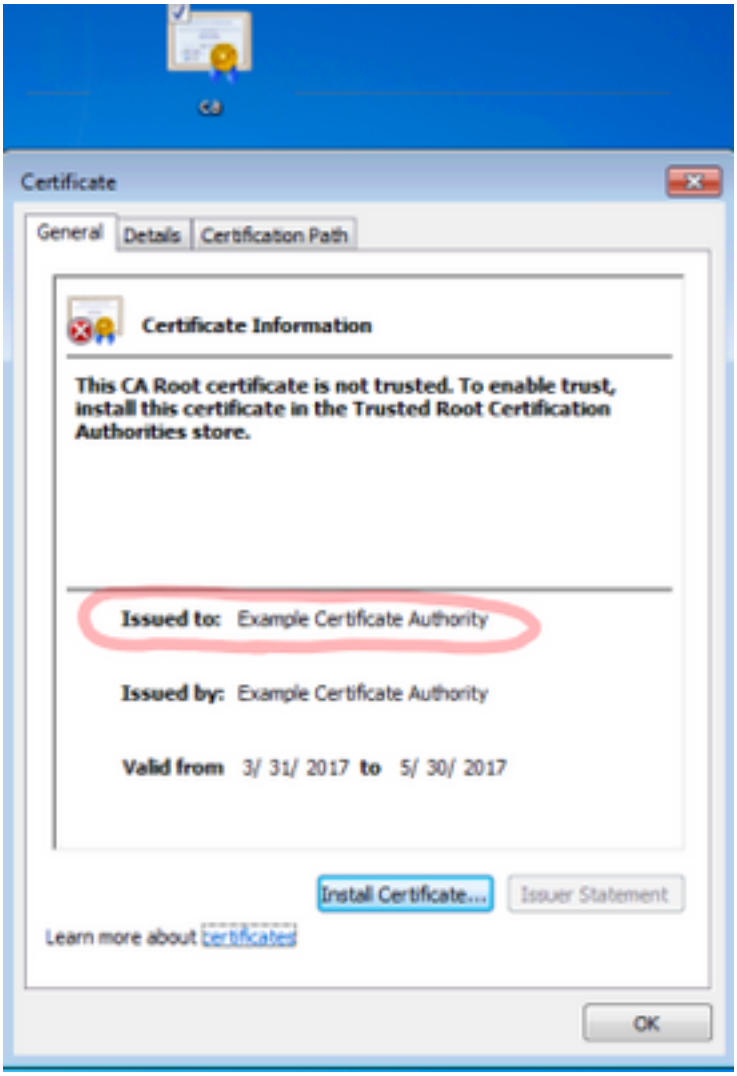
freeRADIUS でインストールされるデフォルト認証を使用する場合エンド デバイスに freeRADIUS サーバから EAP 認証をインポートするために次の手順に従って下さい。

ステップ 1. FreeRadius から証明書を得て下さい:

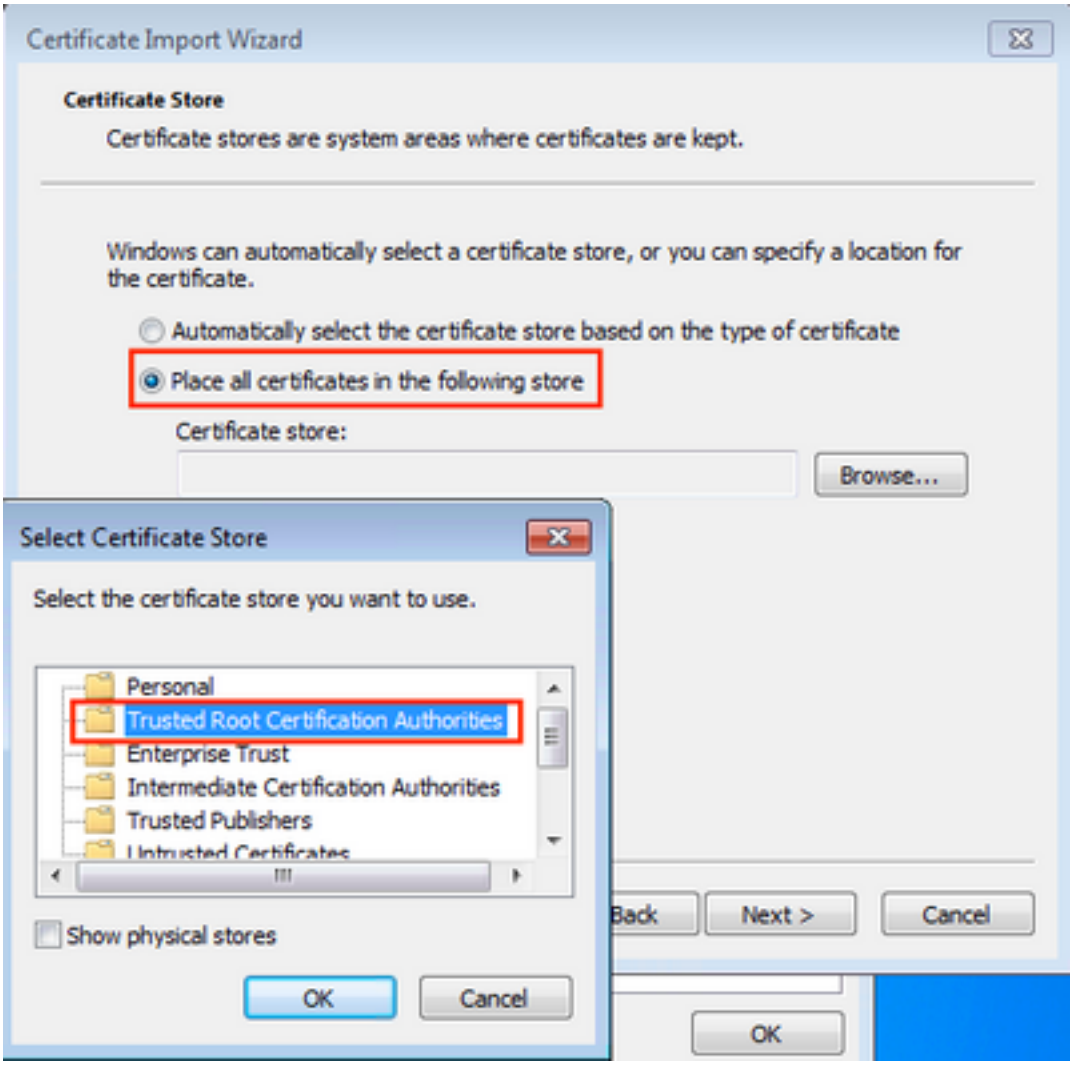
```
[root@tac-mxwireless ~]#mysql_secure_installation
```

ステップ 2.前の手順の出力をテキストファイルにコピー アンド ペーストし、.crt に拡張を変更して下さい

ステップ 3.ファイルをダブル クリックし、イメージに示すように... 『install certificate』 を選択して下さい。

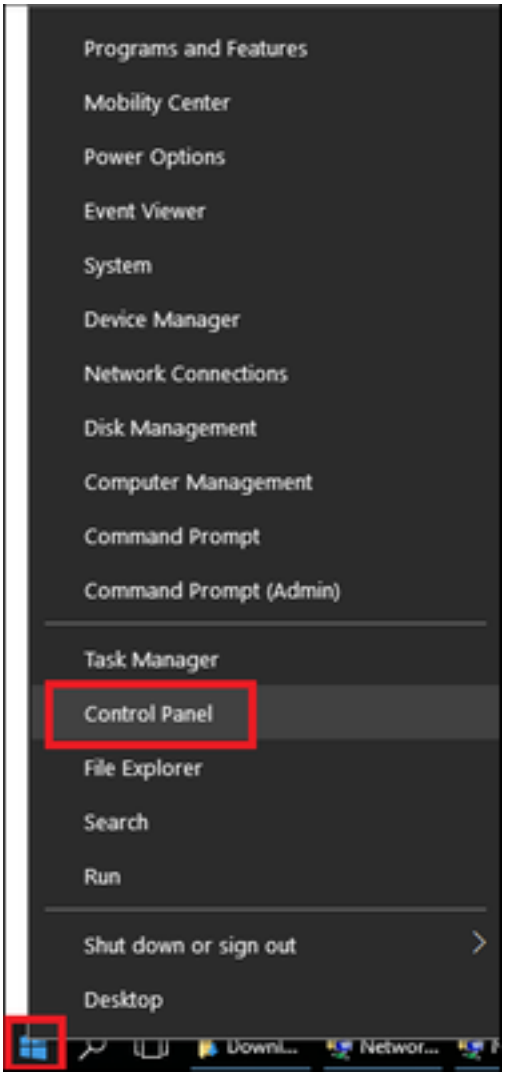


ステップ 4.イメージに示すように**信頼されたルート認証局** ストアに認証をインストールして下さい。

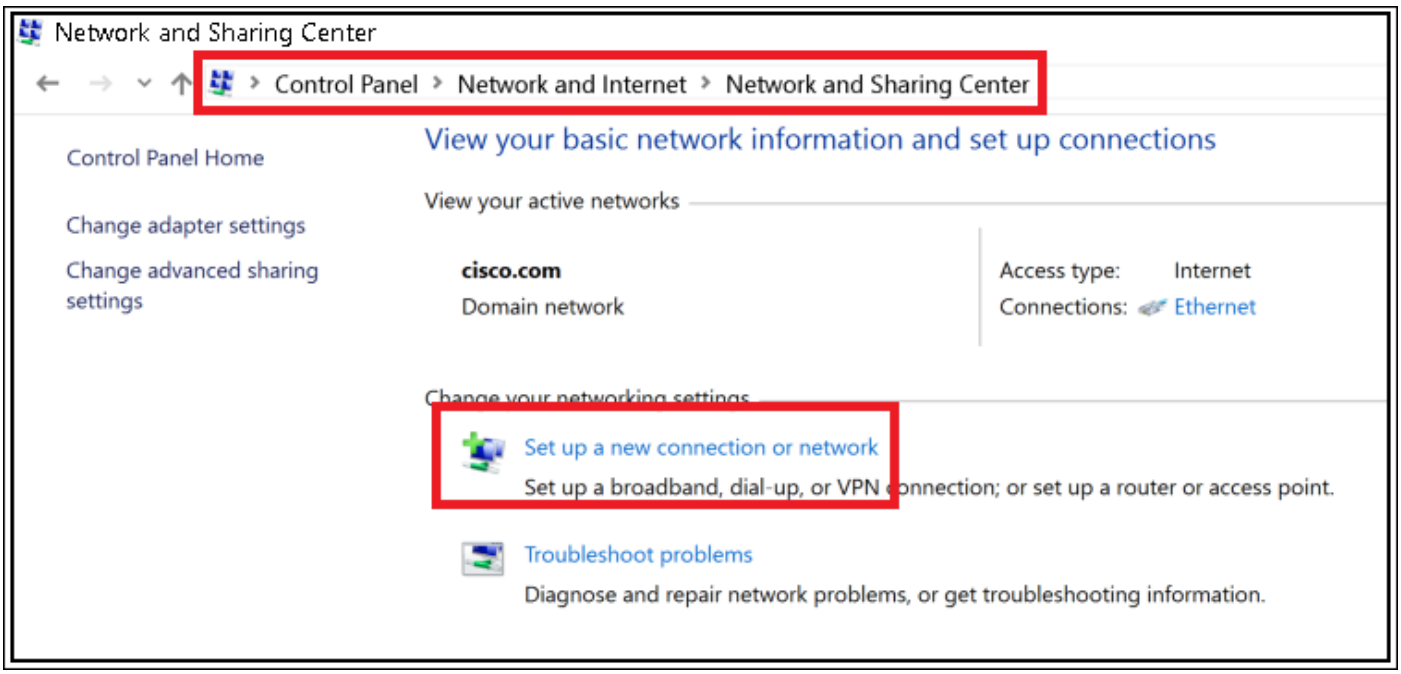


WLAN プロファイルを作成して下さい

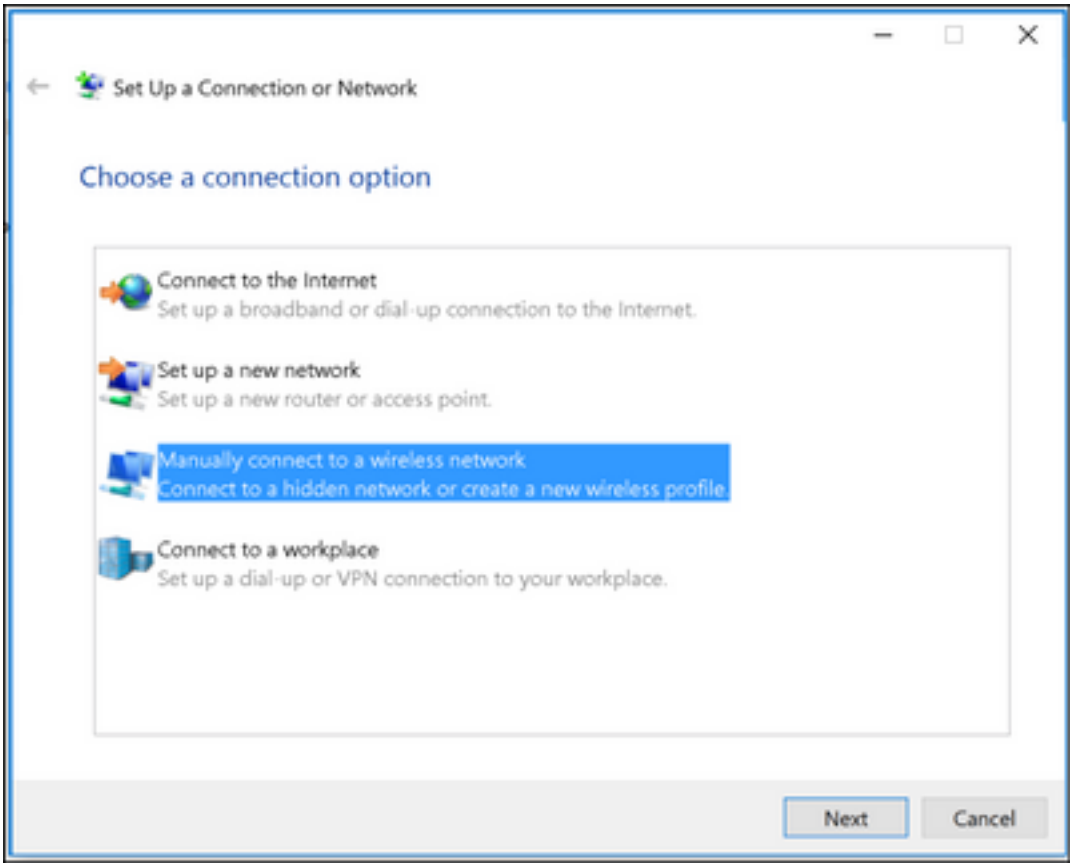
ステップ 1. Start アイコンを右クリックし、イメージに示すように『Control Panel』 を選択 して下さい。



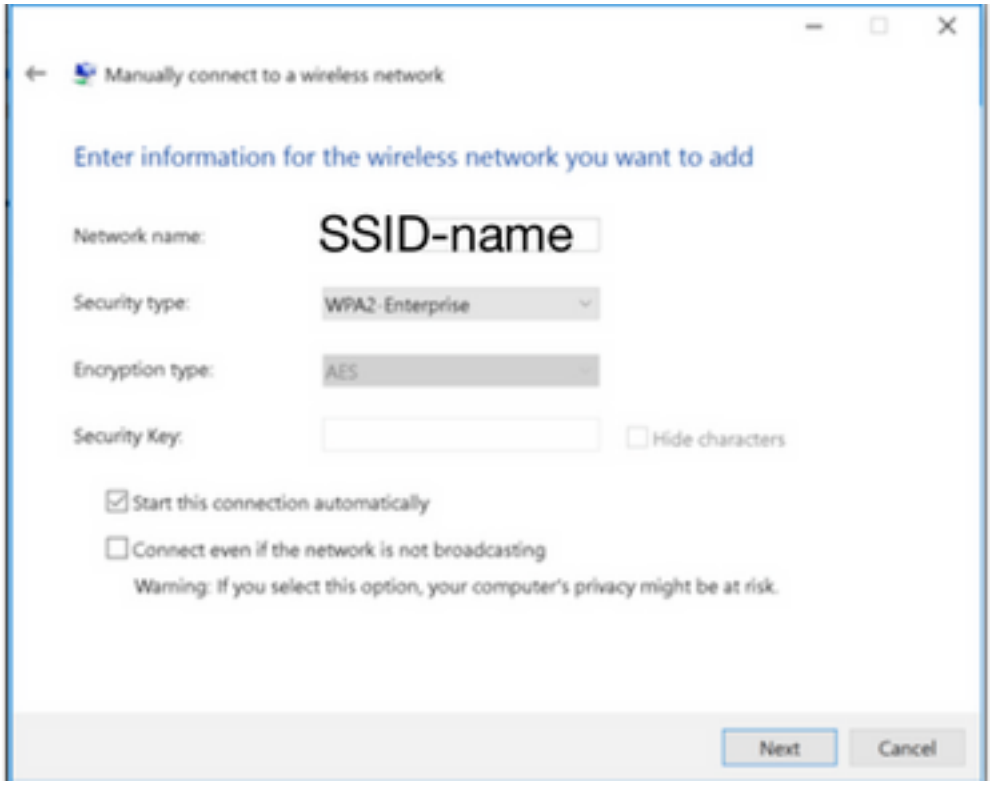
ステップ 2.**ネットワークおよびインターネット > ネットワークおよび共有センター**へのナビゲートはイメージに示すように **> 新しい接続かネットワークを『Setup』 をクリック します。**



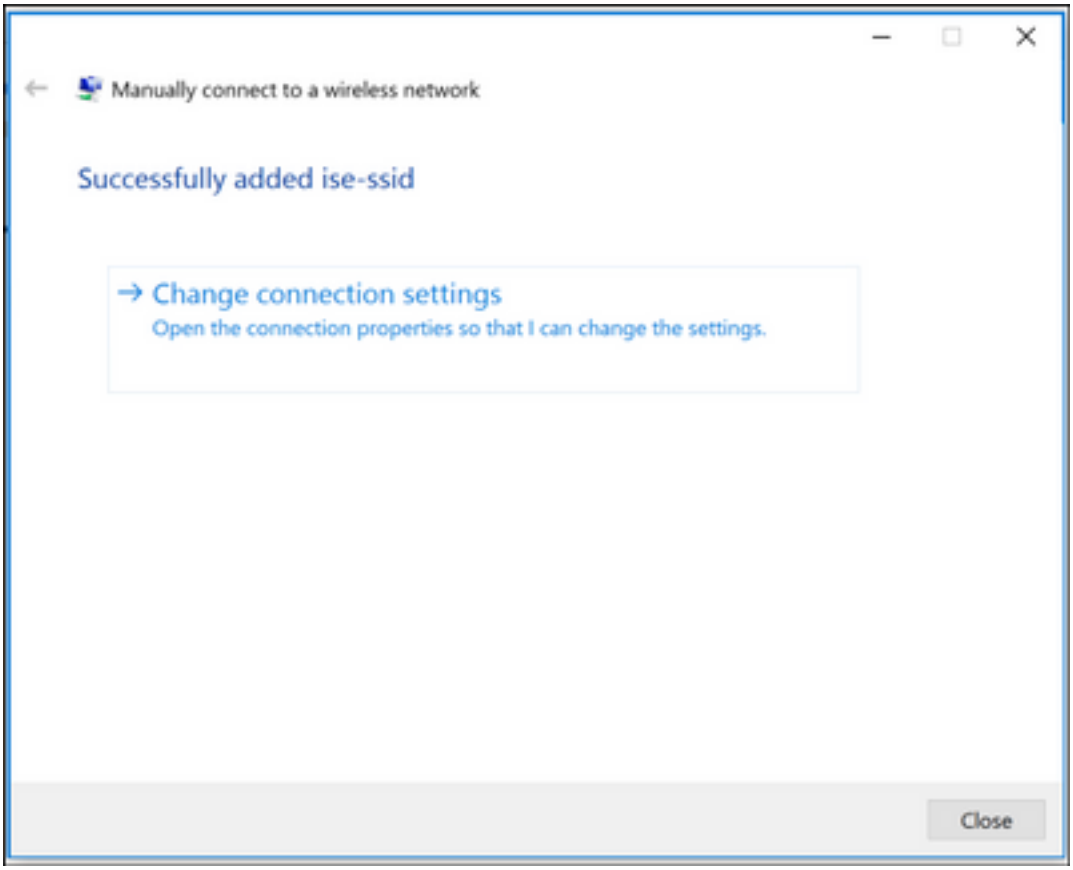
ステップ 3.**手動で接続し、無線ネットワークに**クリックしますイメージで示されている **Nextas を**選択して下さい。



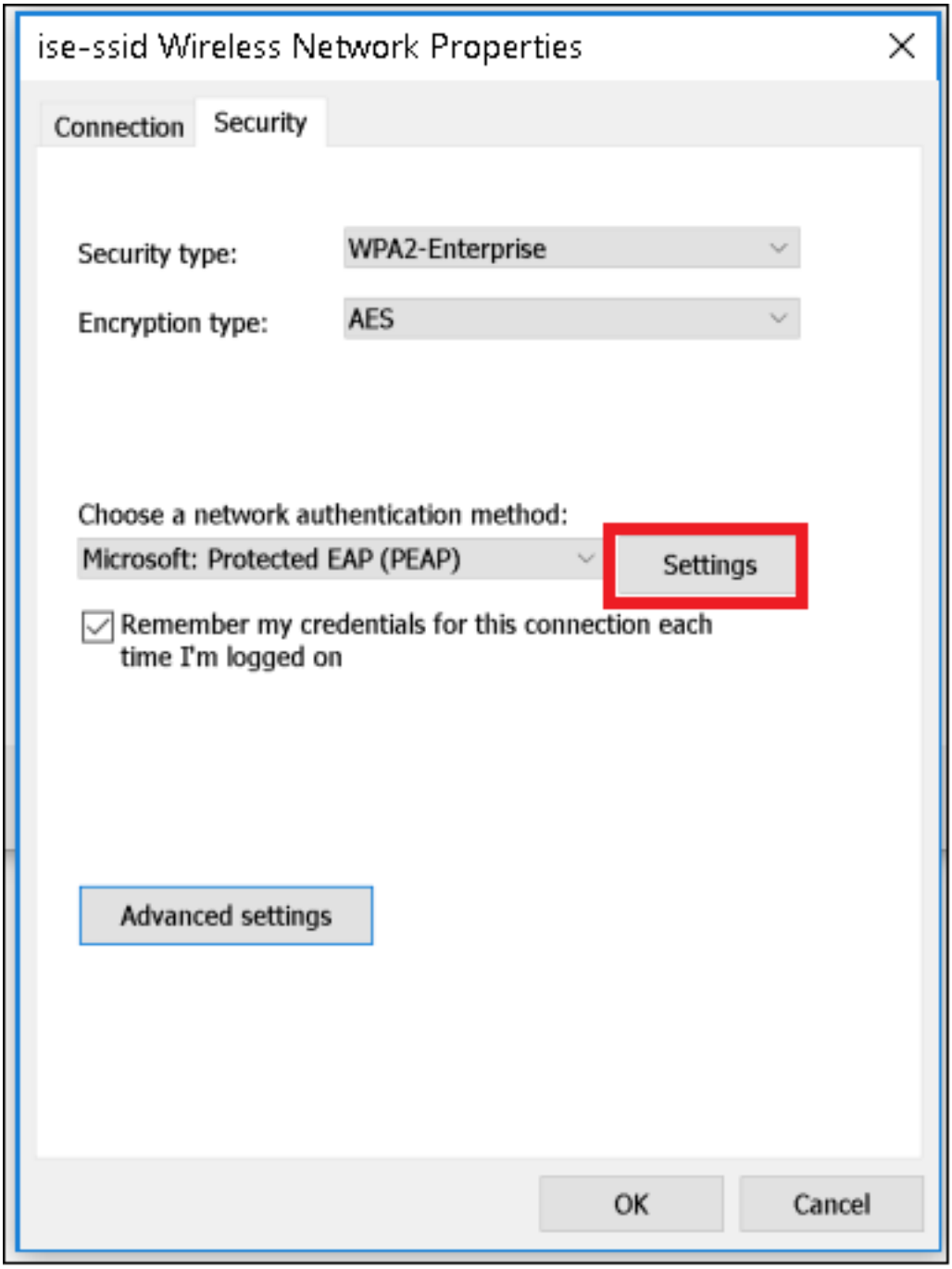
ステップ 4. SSID およびセキュリティ型 WPA2-Enterprise の名前の情報を入力し、イメージに示すように『Next』 をクリック して下さい。



ステップ 5.イメージに示すように WLAN プロファイルの設定をカスタマイズするために**接続 設定を**『Change』 を選択 して下さい。



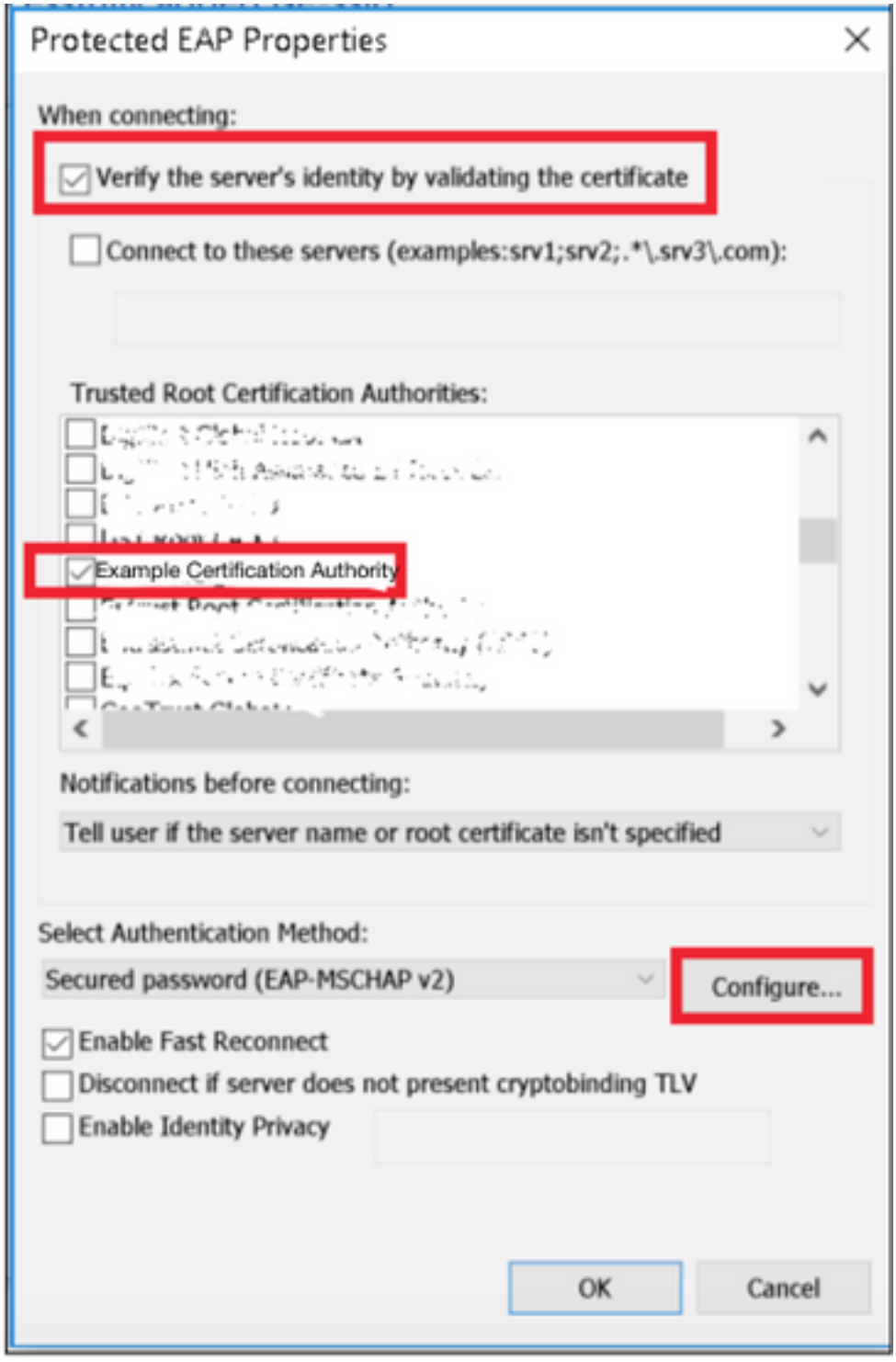
ステップ 6. **Security タブ**にナビゲートし、イメージに示すように『Settings』 をクリック して下さい。

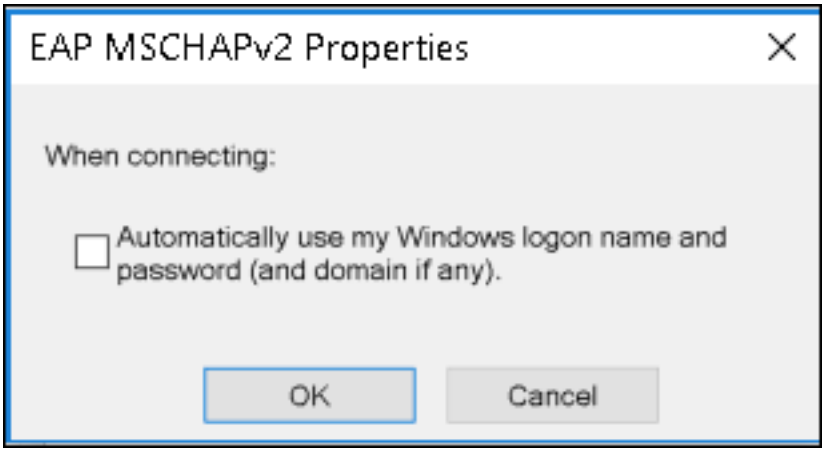


ステップ 7. RADIUSサーバを検証されますまたはない『IF』 を選択 して下さい。

Yes の場合は、イネーブルは**認証の検証によって**および**信頼されたルート認証局**から**サーバの識別を確認します:** リストは freeRADIUS の自己署名証明書を選択します。

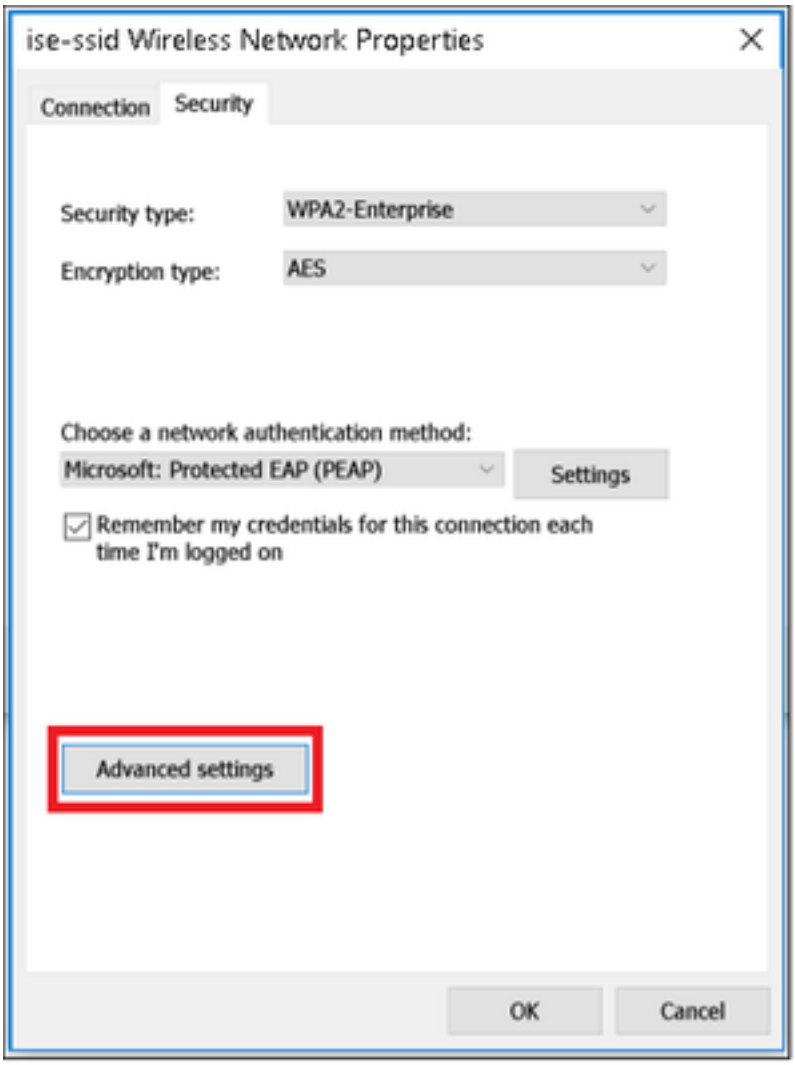
後それは『Configure』 を選択 し、**使用を Windows ログオン名前およびパスワード…自動的に**ディセーブルにしましたり、そしてイメージに示すように『OK』 をクリック します。

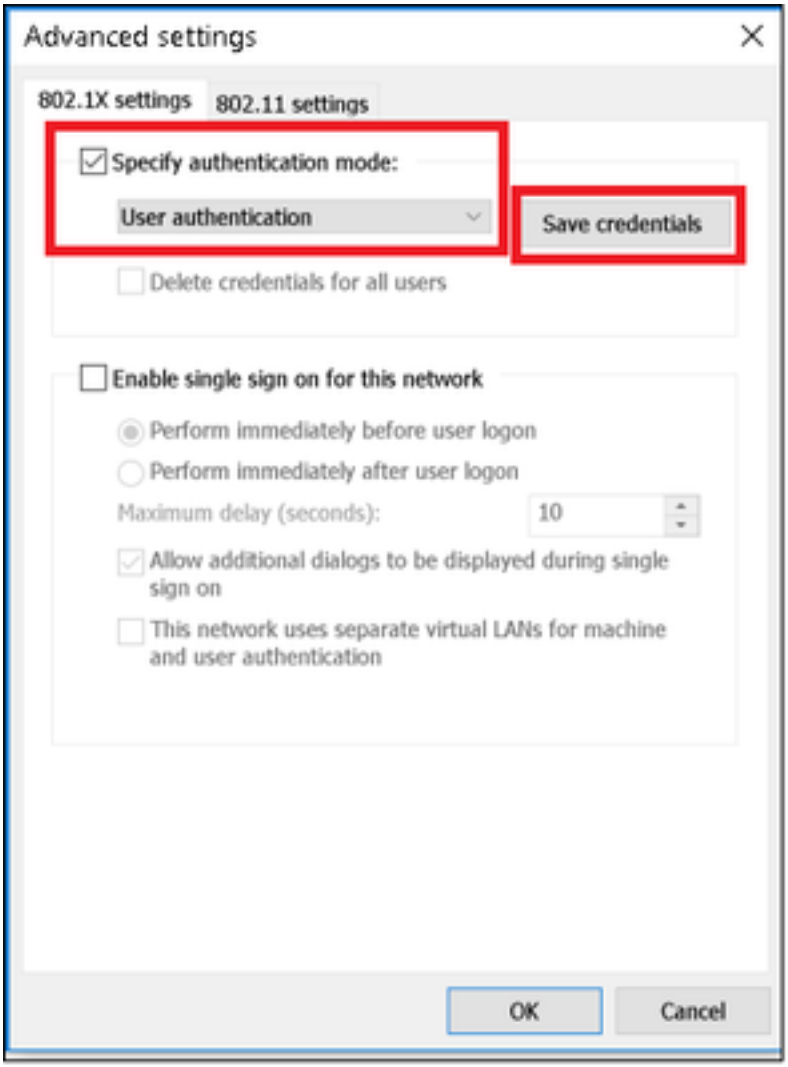


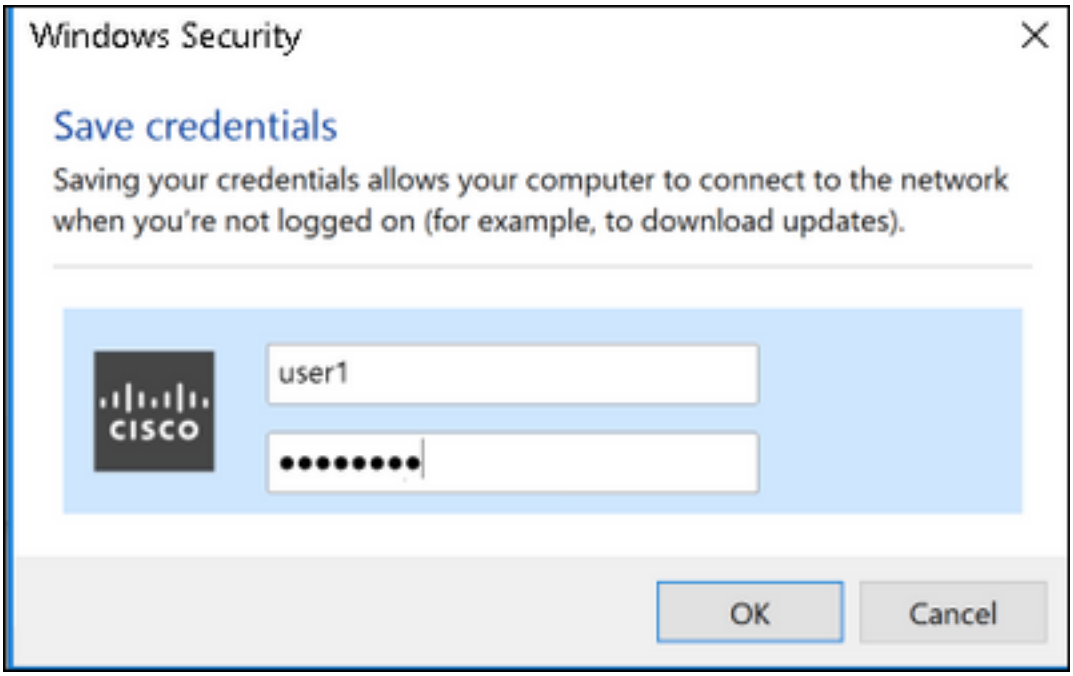


ステップ 8.ユーザーの資格情報を設定して下さい。

Security タブに戻って、**設定を**『Advanced』 を選択 し、**ユーザ認証**として認証モードを規定 し、イメージに示すようにユーザを認証するために freeRADIUS で設定された信任状を保存して下さい。







確認

このセクションでは、設定が正常に機能していることを確認します。

WLC の認証プロセス

特定のユーザ向けの認証プロセスを監視するために次のコマンドを実行して下さい:

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

デバッグ クライアント出力を理解する簡単な方法に関してはワイヤレス デバッグ アナライザ ツールを使用して下さい:

ワイヤレス デバッグ アナライザ

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。