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

内容

概要

このドキュメントでは、802.1xセキュリティとProtected Extensible Authentication Protocol(PEAP)をExtensible Authentication Protocol(EAP)として使用するワイヤレスローカルエリアネットワーク(WLAN)をセットアップする方法について説明します。 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

次の項目に関する基本的な知識が推奨されます。

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

注：このドキュメントは、PEAP-MS-CHAPv2認証にfreeRADIUSサーバで必要な設定の例を読者に示すことを目的としています。このドキュメントに記載されている freeRADIUS サーバの設定は、ラボでテスト済みであり、予期されているとおりに機能することが判明しています。Cisco Technical Assistance Center（TAC）は freeRADIUS サーバ設定をサポートしていません。

使用するコンポーネント

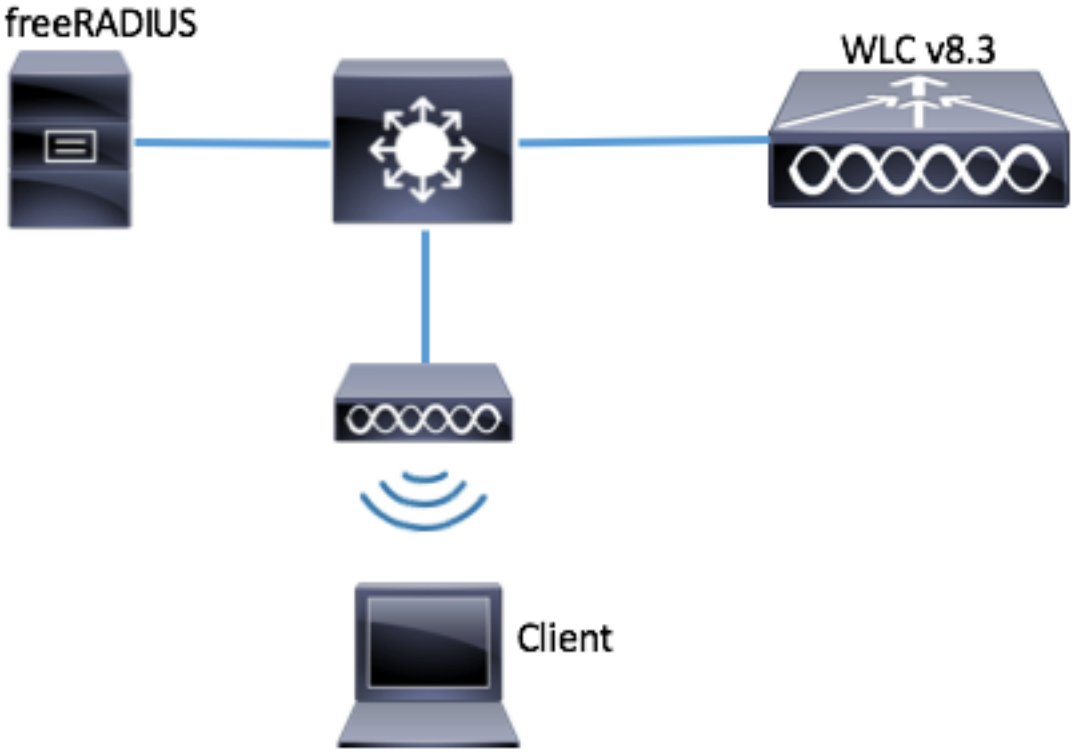
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CentOS7またはRed Hat Enterprise Linux 7(RHEL7)（推奨1 GB RAMおよび20 GB HDD）
- WLC 5508 v8.3
- MariaDB（MySQL）
- FreeRADIUS
- PHP 7

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定

ネットワーク図



httpd サーバと MariaDB のインストール

ステップ 1：次のコマンドを実行して httpd サーバと MariaDB をインストールします。

```
[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) と MariaDB サーバを起動し、有効にします。

```
[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：MariaDB の初期設定を行い、この DB を保護します。

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

> **注：**このスクリプトのすべての部分を実行します。実稼働環境で使用するすべての MariaDBサーバに推奨されます。各手順を注意深く読んでください。

```
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!
```

ステップ 4：freeRADIUS のデータベースを設定します (ステップ 3 で設定したパスワードを使用します) 。

```
[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
```

CentOS 7 への PHP 7 のインストール

ステップ 1：次のコマンドを実行して PHP 7 を CentOS7 にインストールします。

```
[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
```

FreeRADIUS のインストール

ステップ 1：次のコマンドを実行して、FreeRADIUS をインストールします。

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

ステップ2:**mariadb.serviceの後に**radius.serviceを**開始します。**

次のコマンドを実行します。

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

[Unit] セクションに 1 行追加します。

```
After=mariadb.service
```

[Unit] セクションは次のように設定されている必要があります。

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

ステップ 3：freeradius を開始し、起動時に開始できるようにします。

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

ステップ 4：セキュリティのため firewalld を有効にします。

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

ステップ 5： http、https、および radius サービスを許可する永続的なルールをデフォルト ゾーンに追加します。

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

ステップ 6： 変更を有効にするため、firewalld をリロードします。

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

FreeRADIUS

MariaDB を使用するように FreeRADIUS を設定するには、次の手順に従います。

ステップ1:RADIUSデータベーススキームをインポートして、RADIUSデータベースを入力します。

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

ステップ2:/etc/raddb/mods-enabledの下にStructured Query Language(SQL)用のソフトリンクを作成します。

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

ステップ 3：SQL モジュール /raddb/mods-available/sql を設定し、ご使用の環境に合わせてデータベース接続パラメータを変更します。

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

SQLセクションは次のようになります。

```
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”
```

ステップ 4：/etc/raddb/mods-enabled/sql のグループ権限を radiusd に変更します。

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

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

ステップ 1：WLC の共有キーを設定するため、/etc/raddb/clients.conf を編集します。

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

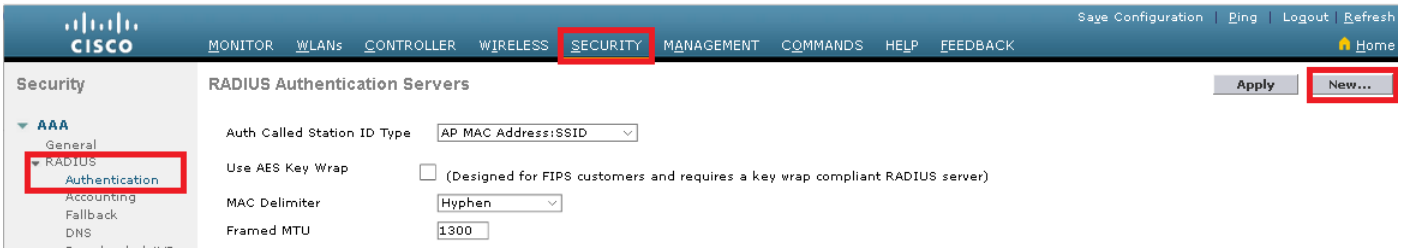
ステップ2：下部に、コントローラのIPアドレスと共有キーを追加します。

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

WLC上のRADIUSサーバとしてのFreeRADIUS

GUI：

ステップ1:WLCのGUIを開き、図に示すように[SECURITY] > [RADIUS] > [Authentication] > [New]に移動します。



ステップ2：図に示すように、RADIUSサーバ情報を入力します。

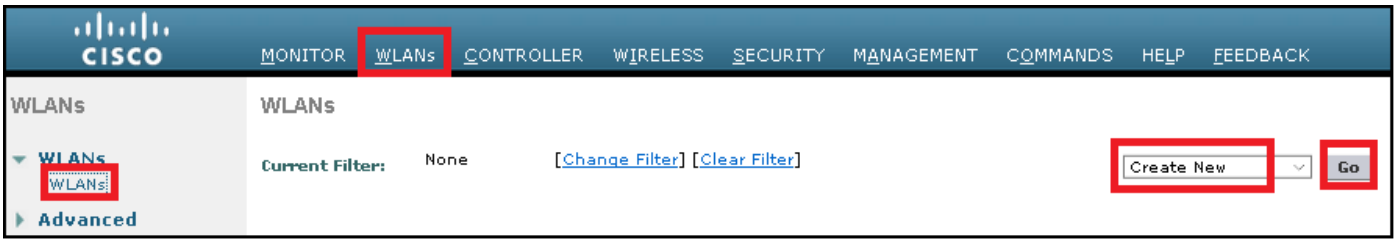
CLI：

```
> 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>
```

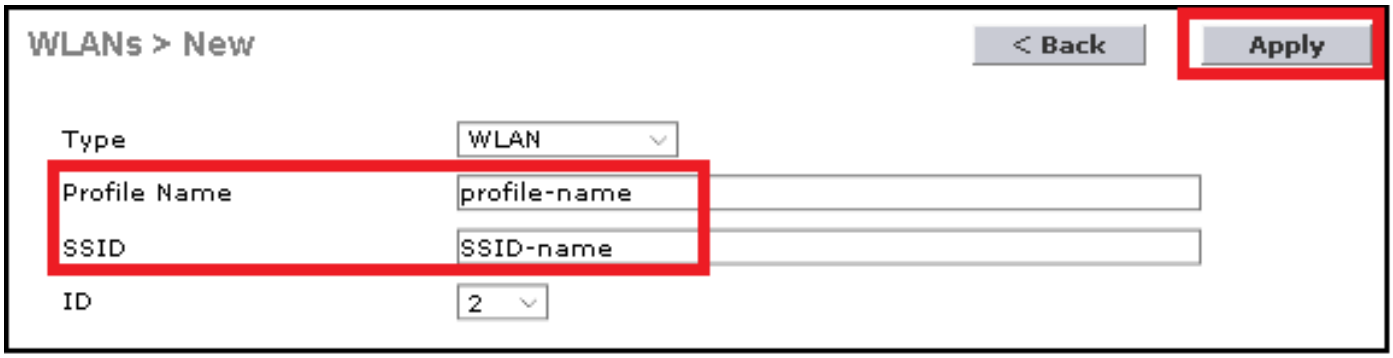
WLAN

GUI：

ステップ1:WLCのGUIを開き、図に示すように[WLANs] > [Create New] > [Goas]に移動します。



ステップ2：サービスセット識別子(SSID)とプロファイルの名前を選択して、図に示すように[Apply]をクリックします。



CLI：

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

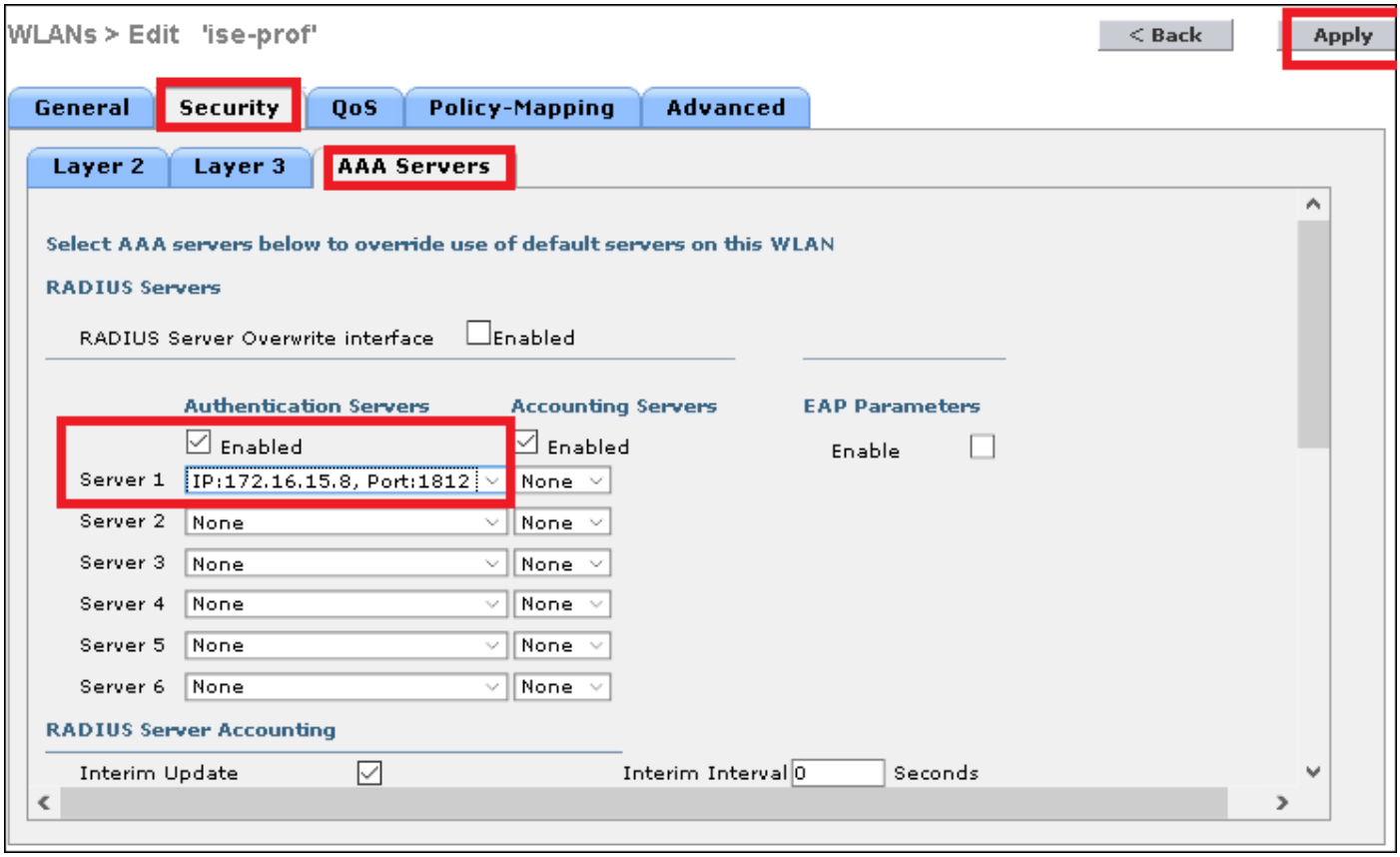
ステップ 3：WLAN に RADIUS サーバを割り当てます。

CLI：

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

GUI：

[Security] > [AAA Servers]に移動し、目的のRADIUSサーバを選択し、図のように**[Apply]**をクリックします。



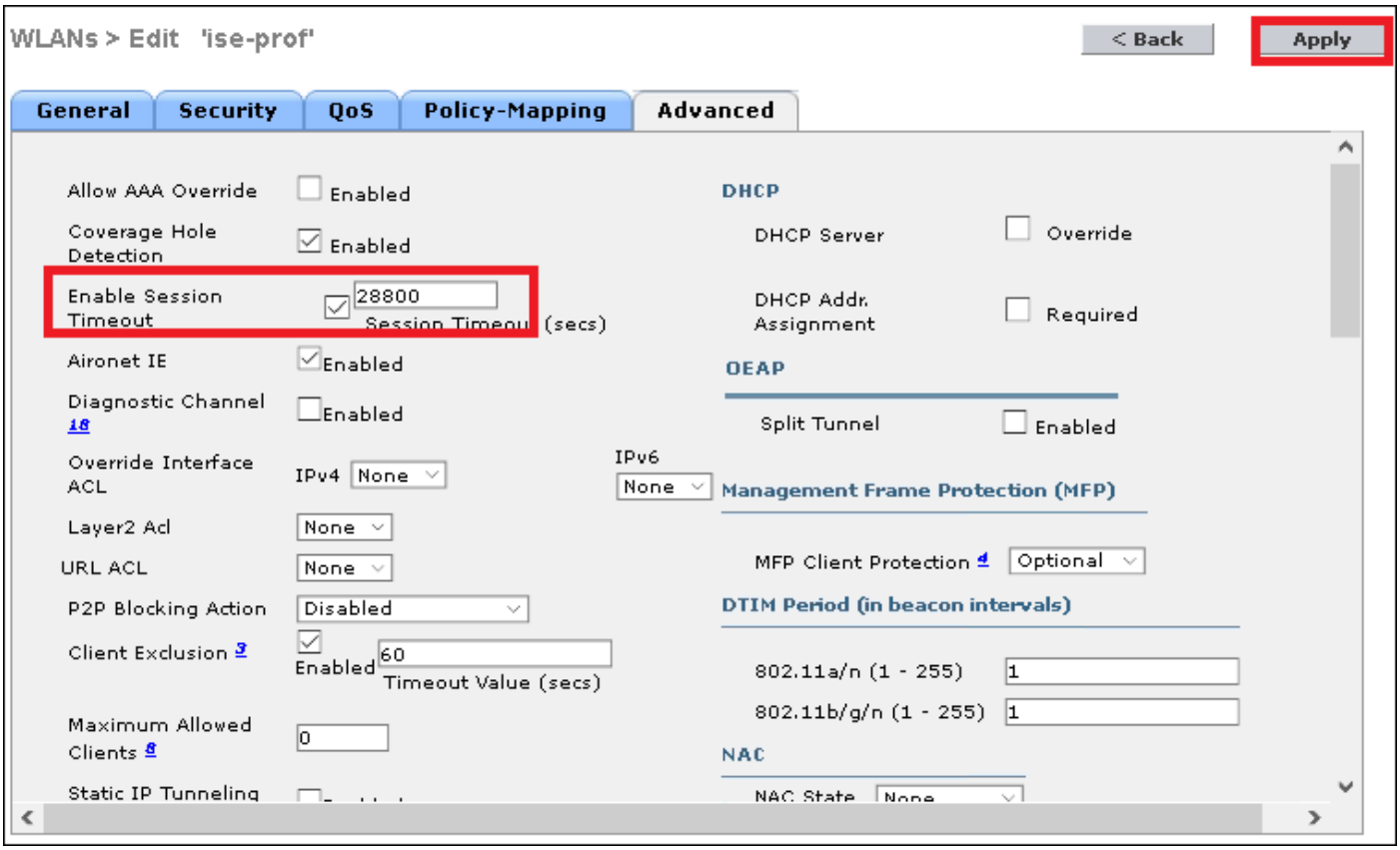
ステップ4：オプションでセッション時間を増やします。

CLI：

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

GUI：

図に示すように、[Advanced] > [Enable Session Timeout]に移動し、[Apply]をクリックします。



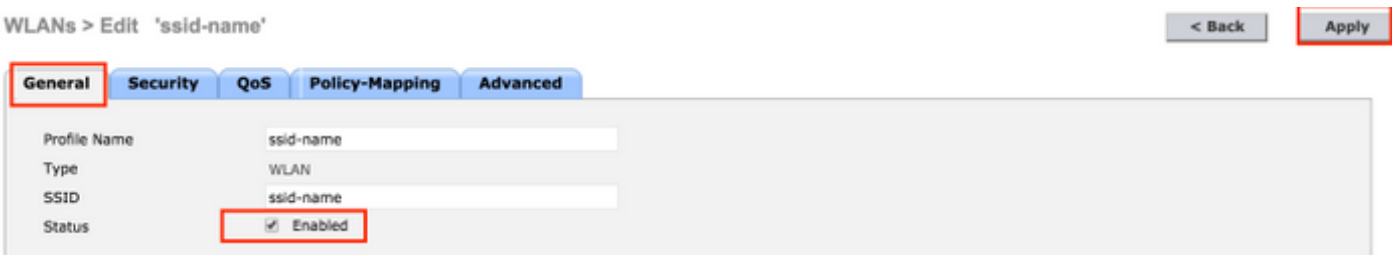
ステップ 5：WLAN を有効にします.

CLI：

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

GUI：

図に示すように、[General] > [Status] > [Tick Enabled] > [Apply]をクリックします。



freeRADIUS データベースへのユーザの追加

デフォルトでは、クライアントは PEAP プロトコルを使用しますが、freeRadius ではその他の方

式もサポートしています（このガイドでは説明しません）。

ステップ 1：ファイル **/etc/raddb/users** を編集します。

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

ステップ2：ファイルの下部にユーザ情報を追加します。この例では、**user1**は**ユーザ**名、**Cisco123**は**パスワ**ードです。

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

ステップ 3：FreeRadius を再起動します。

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

freeRADIUS の証明書

FreeRADIUSには、デフォルトの認証局(CA)証明書と、パス/etc/raddb/certsに保存されているデバイス証明書が付属しています。*これらの証明書の名前*は、ca.pemとserver.pemです。server.pemは、クライアントが認証プロセスを通過するときに受信する証明書です。EAP 認証に異なる証明書を割り当てる必要がある場合は、これらの証明書を削除し、新しい証明書を正確に同じ名前で同じパスに保存するだけで行えます。

エンド デバイスの設定

802.1x 認証と PEAP/MS-CHAP（Microsoft の Challenge-Handshake Authentication Protocol）バージョン 2 を使用して SSID に接続するように、ラップトップ Windows マシンを設定します。

WindowsマシンでWLANプロファイルを作成するには、次の2つのオプションがあります。

1. 認証を実行するため、freeRADIUS サーバの検証および信頼に使用する自己署名証明書をマシンにインストールします。
2. RADIUS サーバの検証をバイパスし、認証の実行に使用するすべての RADIUS サーバを信頼します（これはセキュリティの問題となる可能性があるため、推奨されません）。 これらのオプションの設定については、「エンドデバイスの設定：WLANプロファイルの作成」を参照してください。

FreeRADIUS証明書のインポート

freeRADIUS にインストールされているデフォルト証明書を使用する場合は、次の手順に従い、freeRADIUS サーバからエンド デバイスに EAP 証明書をインポートします。

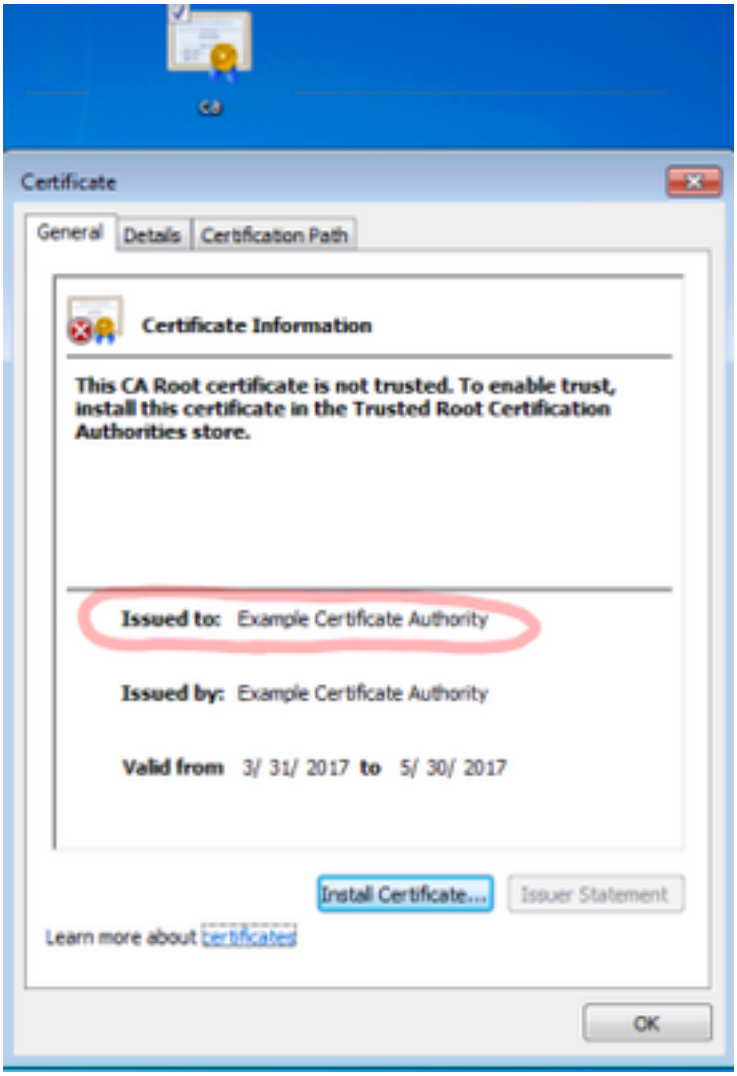
ステップ 1：FreeRadius から証明書を取得します。

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

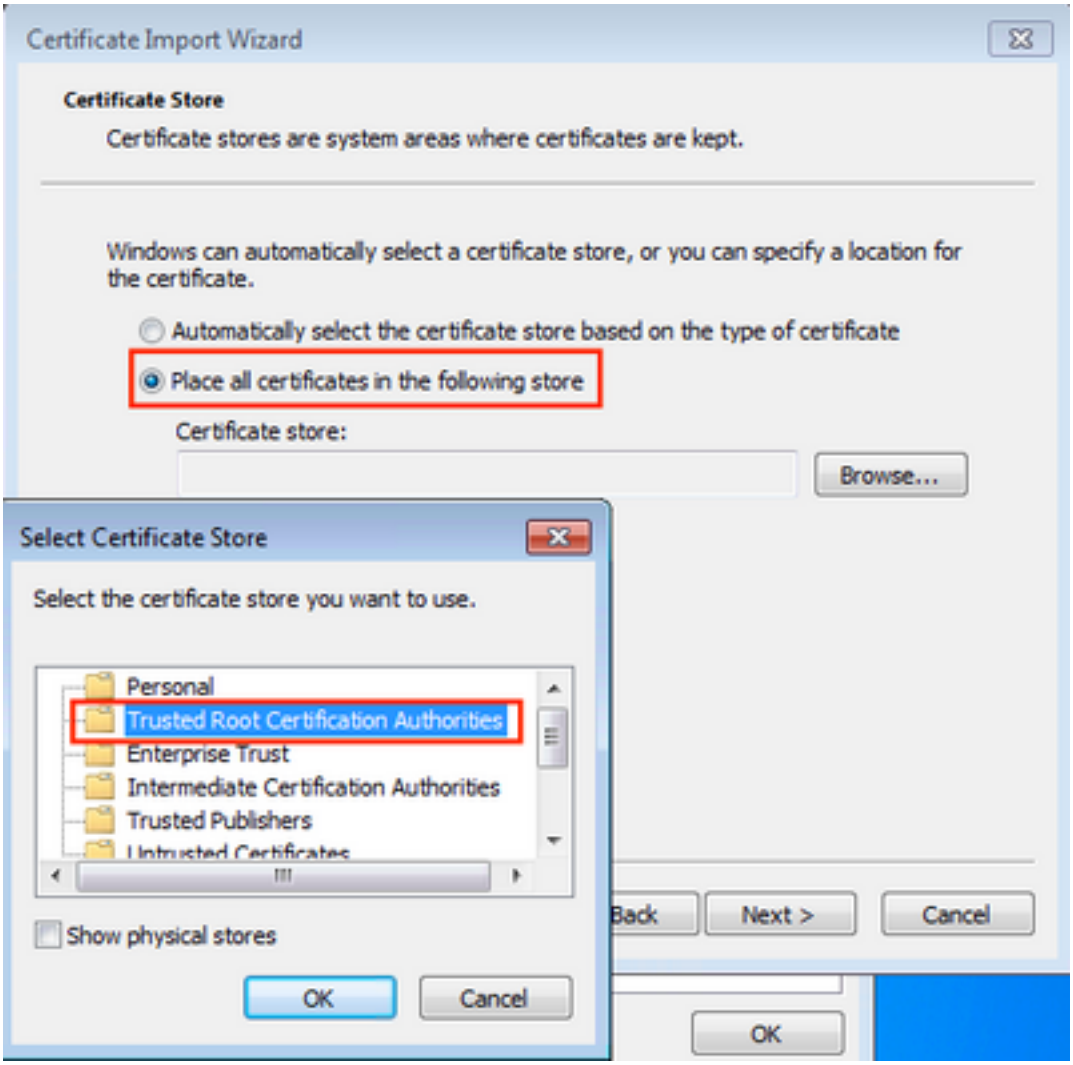
```
-----BEGIN CERTIFICATE-----
MIIE4TCCA8mgAwIBAgIJAKLmHn4eZLjBMA0GCSqGSIb3DQEBBQUAMIGTMQswCQYD
VQQGEwJGUjEPMA0GA1UECBMGUmFkaXVzMRIwEAYDVQQHEwlTb21ld2hlcmUxFTAT
BgNVBAoTDEV4YW1wbGUgSW5jLjEgMB4GCSqGSIb3DQEJARYRYWRtaW5AZXhhbXBs
ZS5jb20xJjAkBgNVBAMTHUV4YW1wbGUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4X
DTE3MDMzMTExMTIxNloXDTE3MDUzMDExMTIxNlowgZMxCzAJBgNVBAYTAkZSMQ8w
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-----
```

ステップ 2：前のステップでの出力をコピーし、テキスト ファイルに貼り付け、拡張子を .crt に変更します。

ステップ 3：ファイルをダブルクリックし、[Install Certificate...] を選択します。 図に示すように

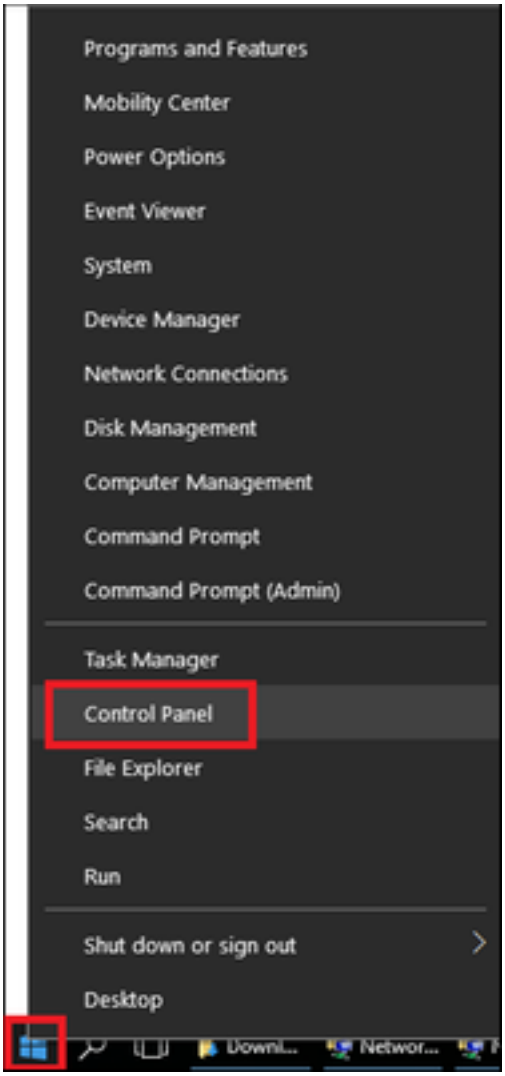


ステップ4：図に示すように、証明書をTrusted Root Certification Authoritiesストアにインストールします。

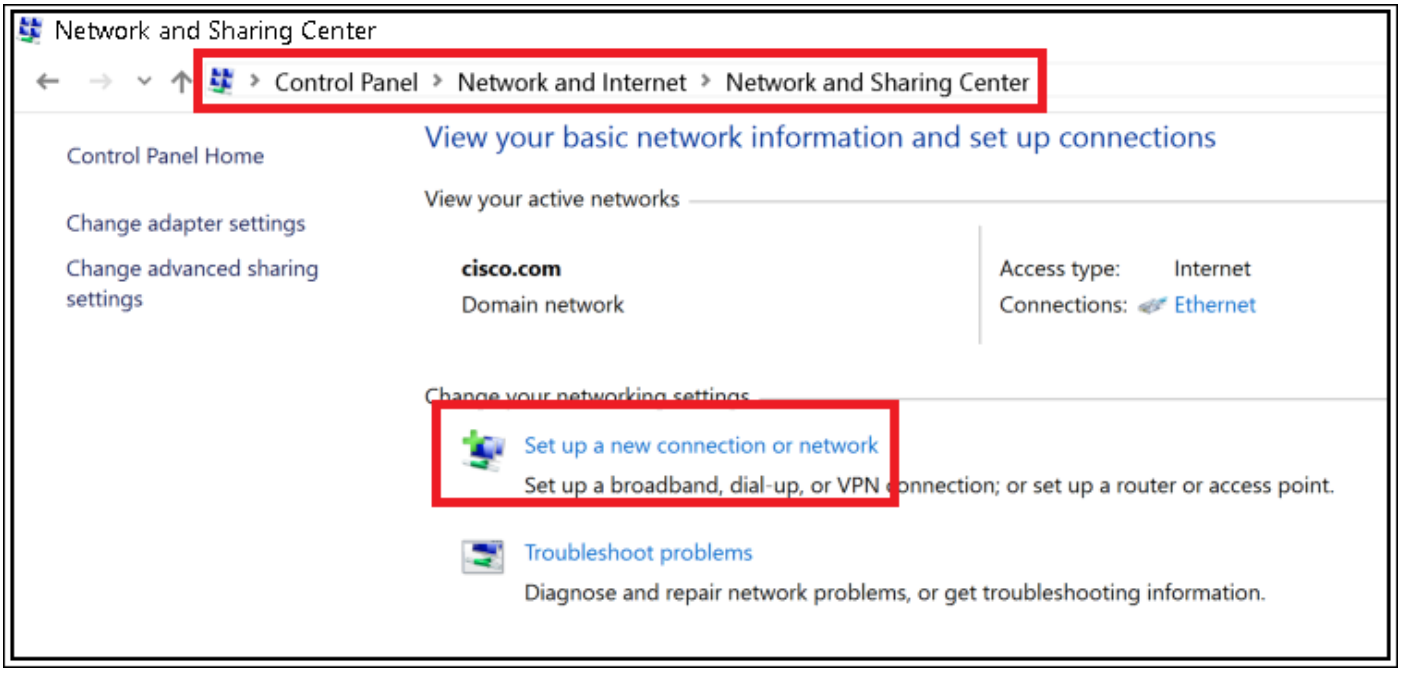


WLANプロファイルの作成

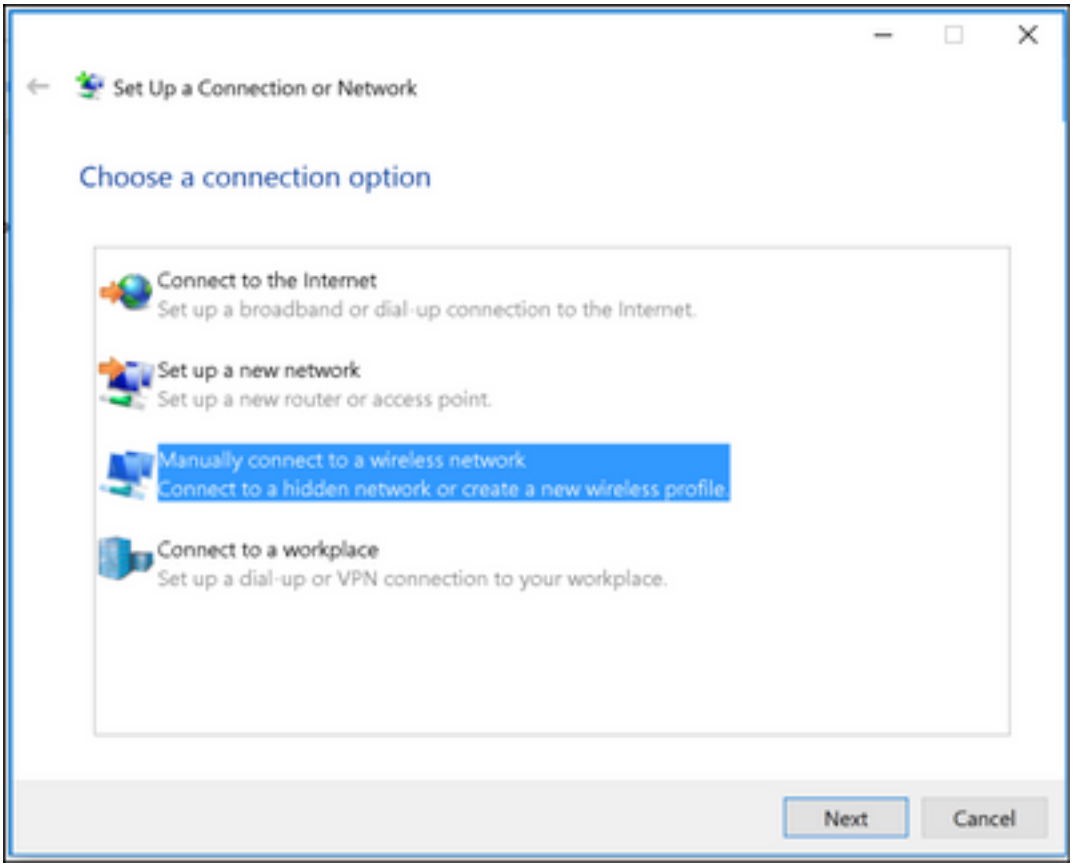
ステップ1：図に示すように、[スタート]アイコンを右クリックし、[コントロールパネル]を選択します。



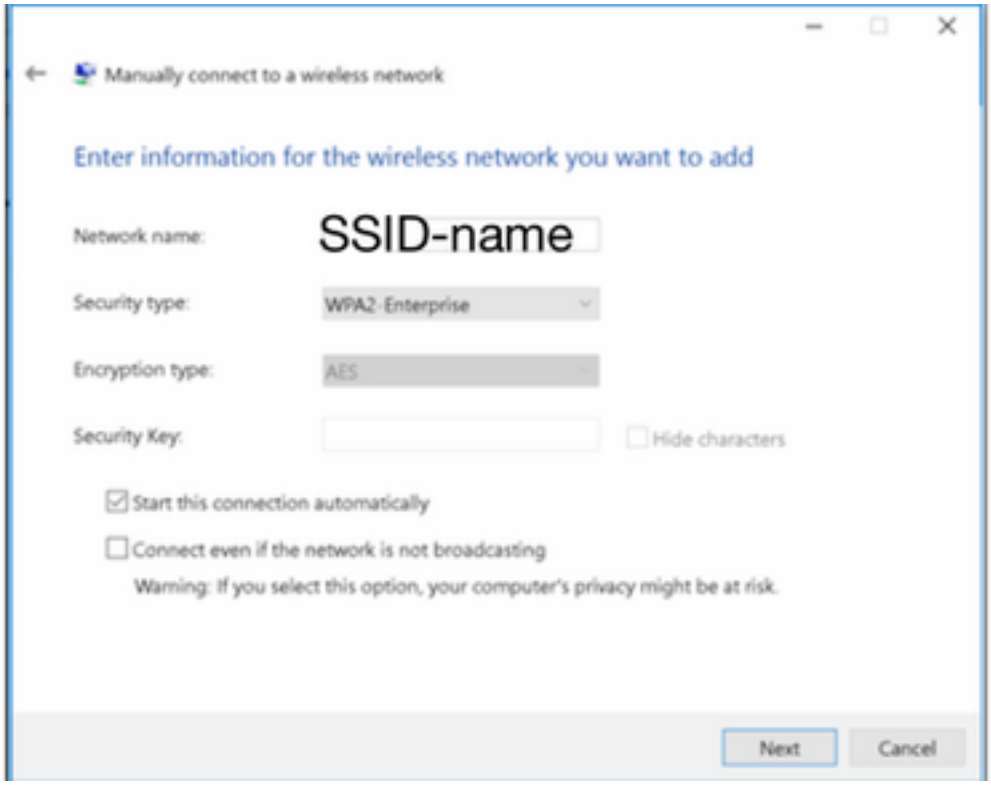
ステップ2：図に示すように、[Network and **Internet] > [Network and Sharing Center] > [Set up a new connection or network]をクリック**します。



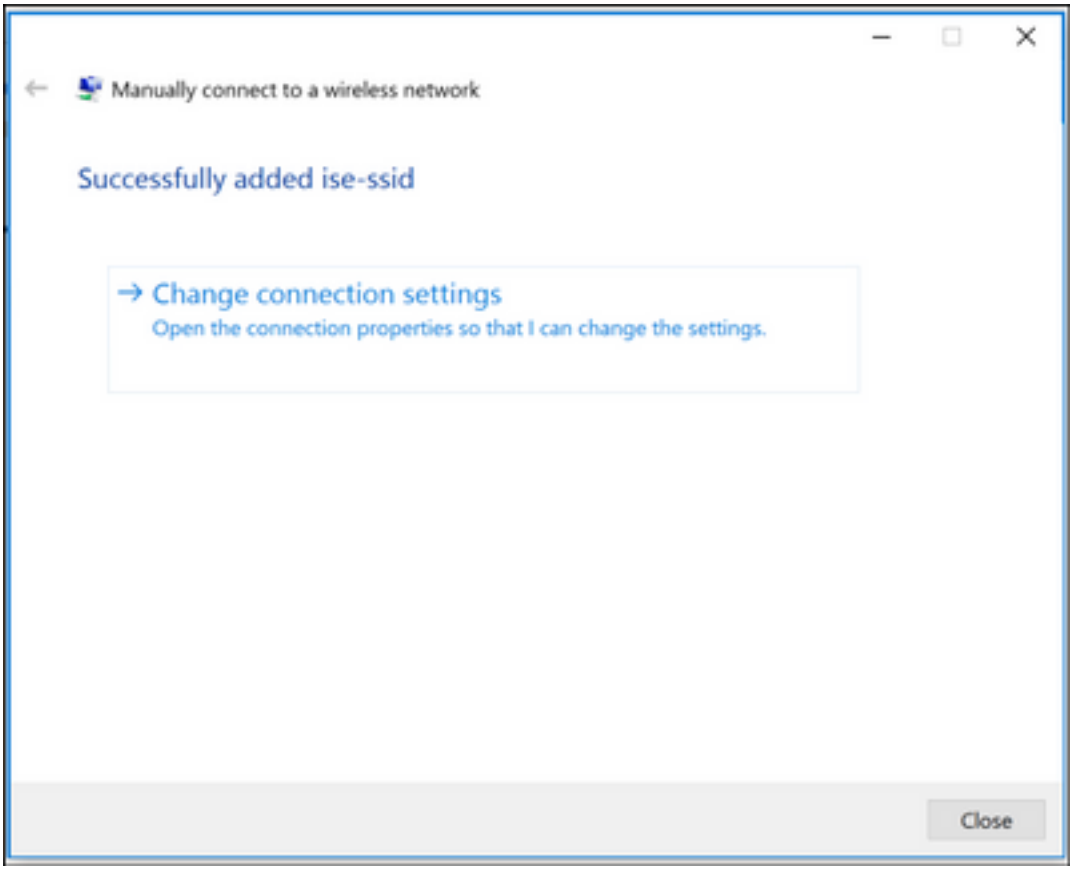
ステップ3:**[Manually connect to a wireless network]を選択し、**図に示す[Nextas]をクリックします。



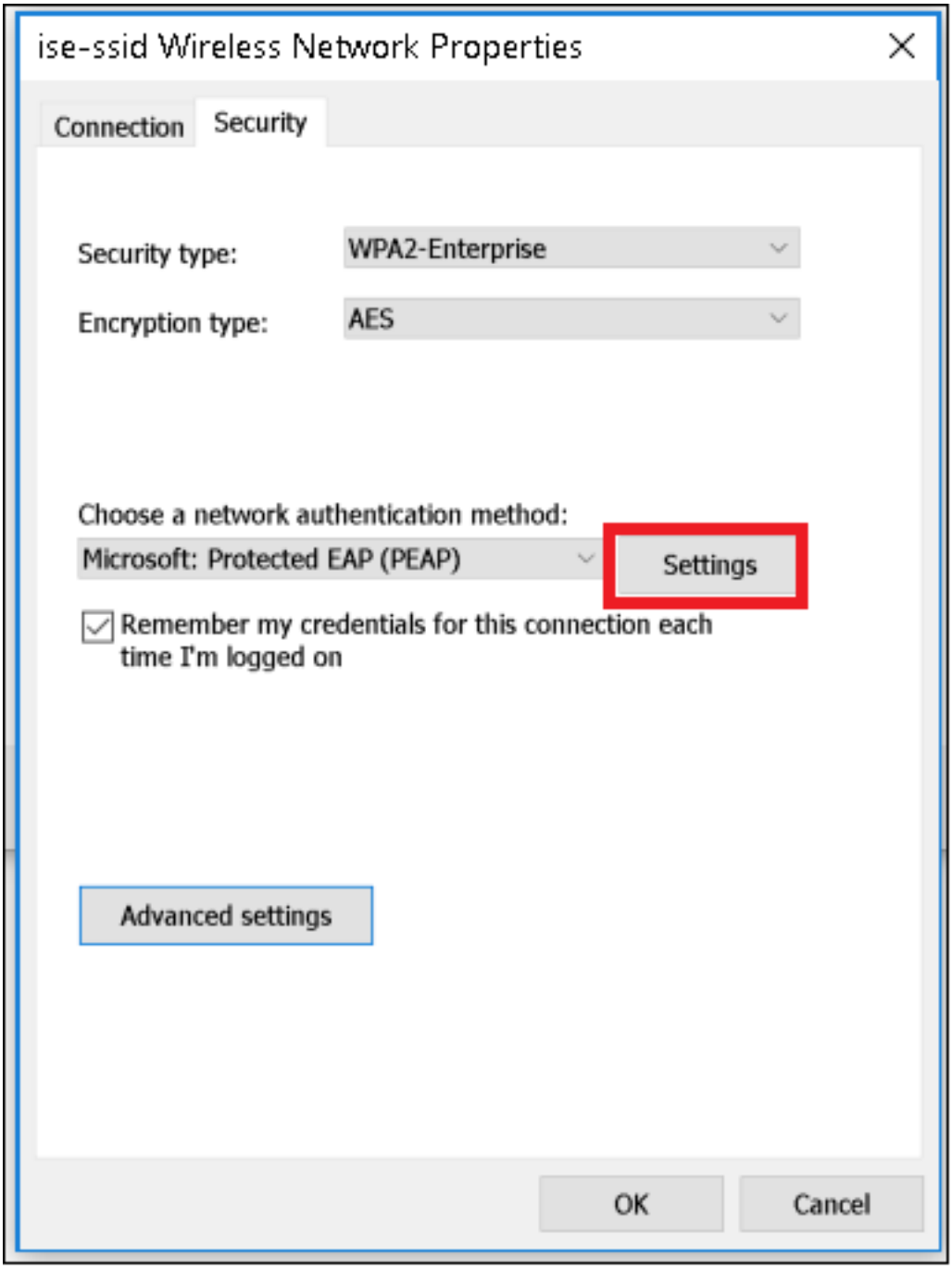
ステップ4:SSIDの名前とセキュリティタイプWPA2-Enterpriseの情報を入力し、図に示すように[**Next**]をクリックします。



ステップ5：図に示すように**WLANプロファイル**の設定をカスタマイズするには、[Change connection settings]を選択します。



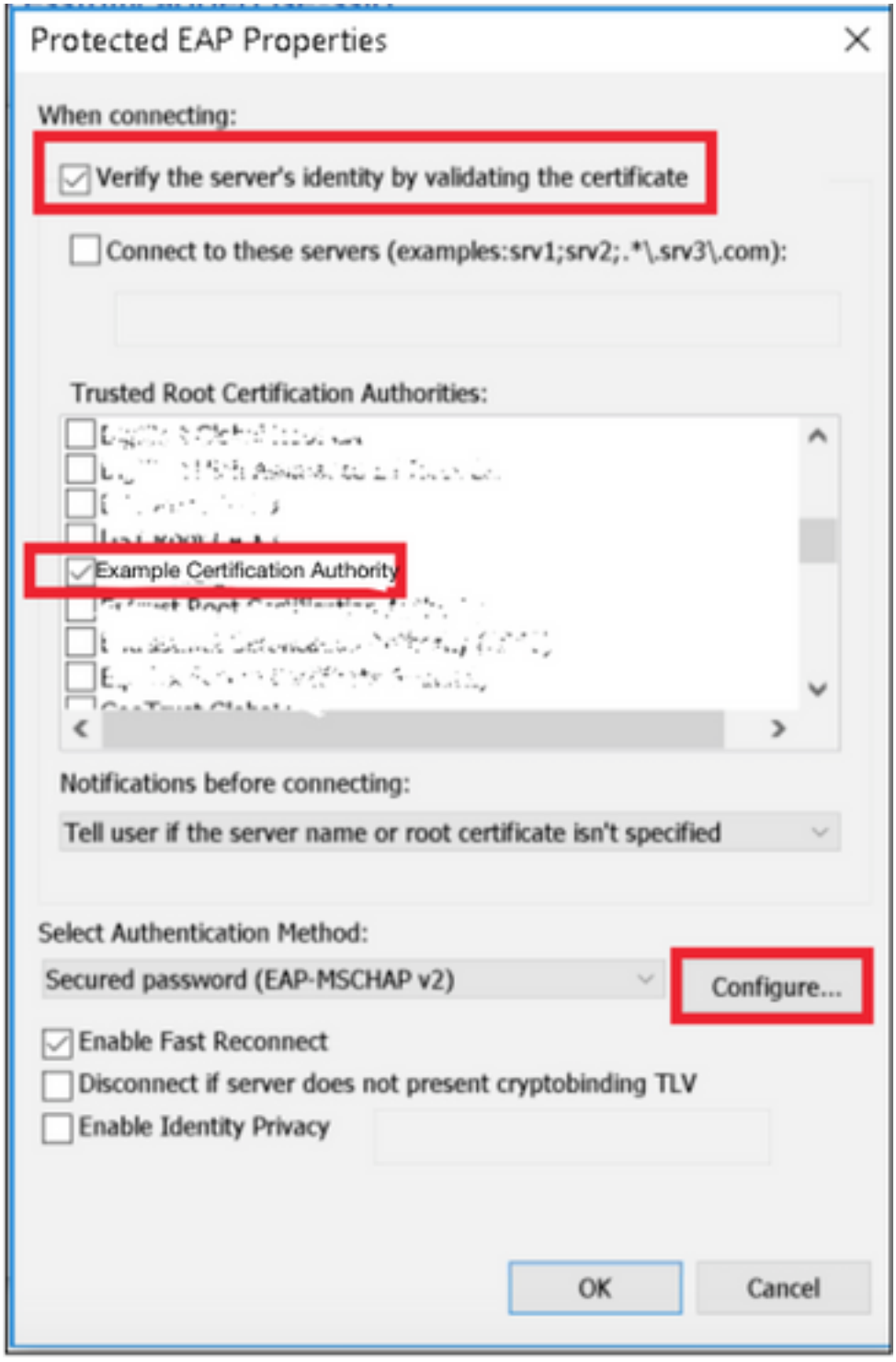
ステップ6：図に示すように、[セキュリティ]タブに移動し[設定]をクリックします。

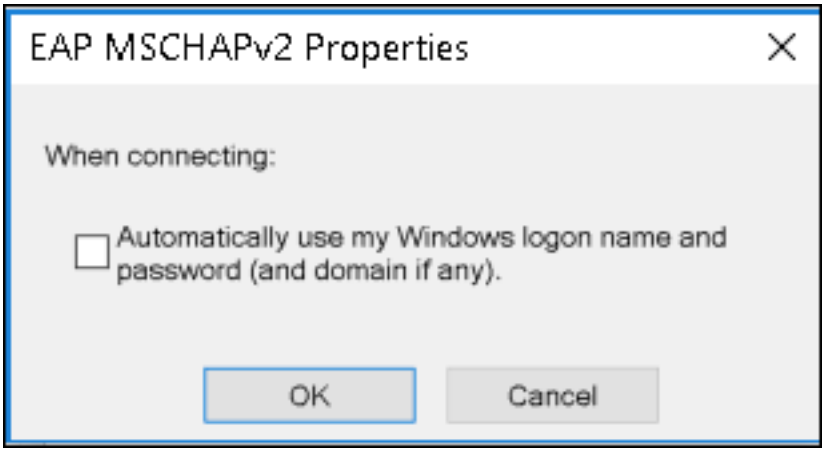


ステップ 7：RADIUS サーバが有効になっているかいないか選択します。

検証する場合は [Verify the server's identity by validating the certificate] **を有効にし、[Trusted Root Certification Authorities:]** リストから freeRADIUS の自己署名証明書を選択します。

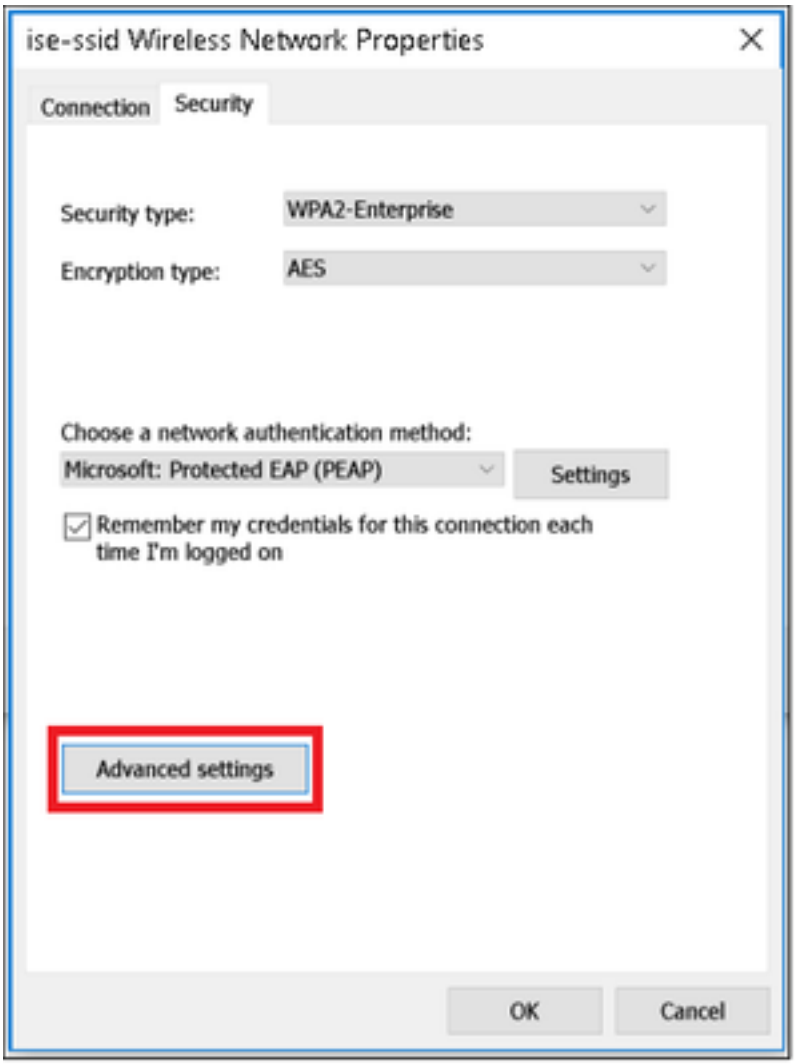
その後、[Configure]を選択し、**[Automatically use my Windows logon name and password...]を無効にして**、図のように**[OK]**をクリックします。

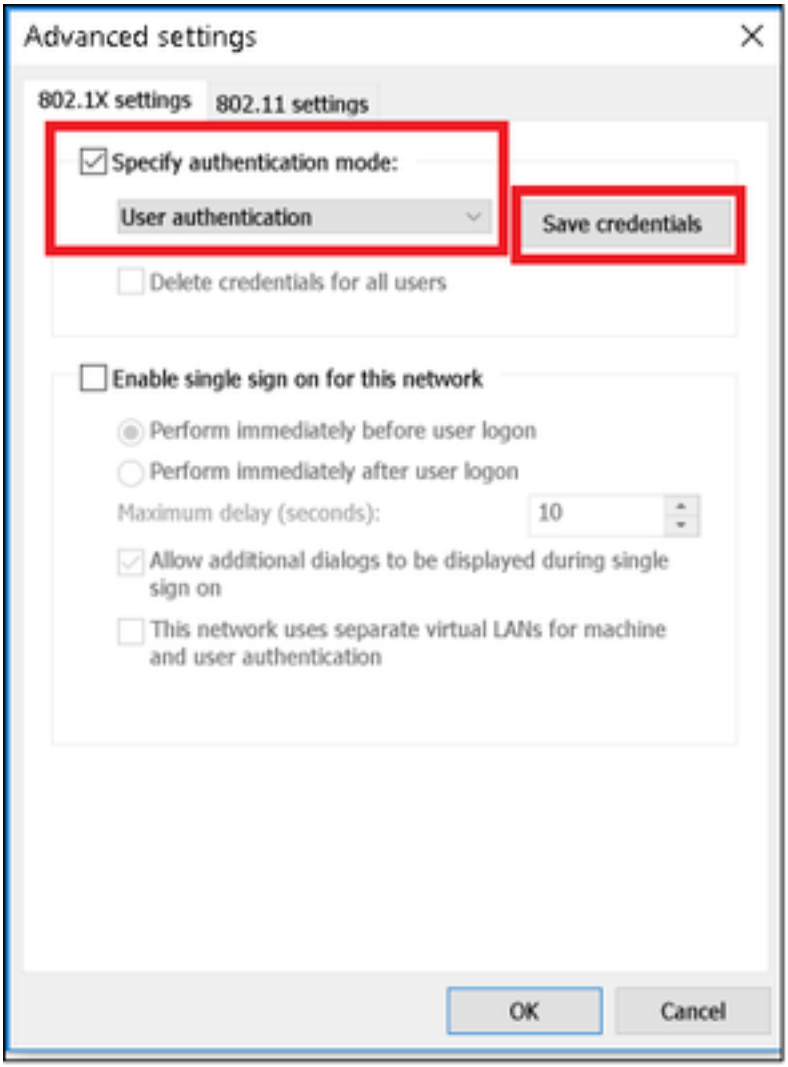


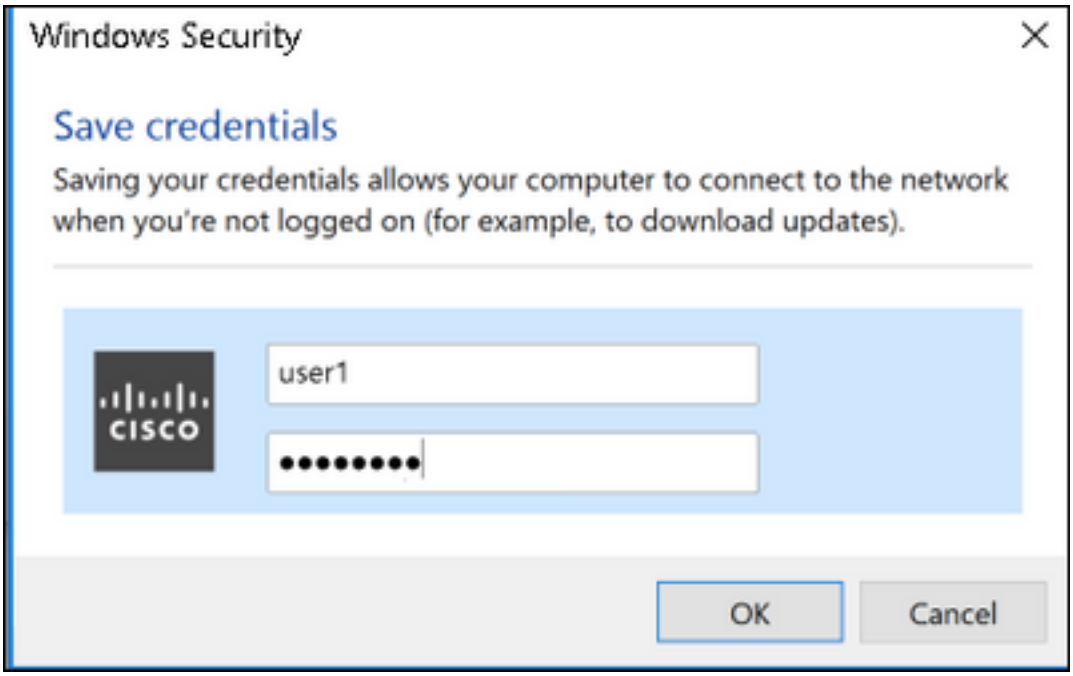


ステップ 8：ユーザ クレデンシャルを設定します。

[Security]タブに戻り、[Advanced settings] を選択し、[User authentication]として認証モードを指定して、ユーザを認証するためにfreeRADIUSで設定したクレデンシャルを保存します。







確認

ここでは、設定が正常に機能しているかどうかを確認します。

WCL での認証プロセス

特定のユーザの認証プロセスをモニタするため、次のコマンドを実行します。

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

デバッグ クライアントの出力を簡単に読むための手段として、ワイヤレス デバッグ アナライザ ツールを使用します。

ワイヤレス デバッグ アナライザ

トラブルシュート

現在、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。