Technical Guide

Remote VPN

Copyright Notification

Edgecore Networks Corporation

Table of Contents

1. Introduction

Virtual private networks (VPNs) provide a way for secure connections to be established across the public network by tunneling the traffic. VPNs generally fall into two types—remote-access VPN and site-to-site VPN. Remote-access VPNs can be used to securely connect a host to a private network. For example, companies can allow staff to remotely access the file servers or other resources on the headquarters' intranet from an outside network using remote VPNs. With site-to-site VPNs, separate private networks could be joined for data sharing or other purposes. For example, private networks of different office branches of a company or even private networks of different companies can be joined.

In this technical guide, the Remote VPN feature on the controller is introduced, and guidance on how to setup and configure remote VPNs on the controller as well as on client devices is provided.

2. Setup of Remote VPN - PPTP

2.1   WLAN Controller Configuration

Step 1.

Enter controller's IP address/domain name in browser and login as administrator.
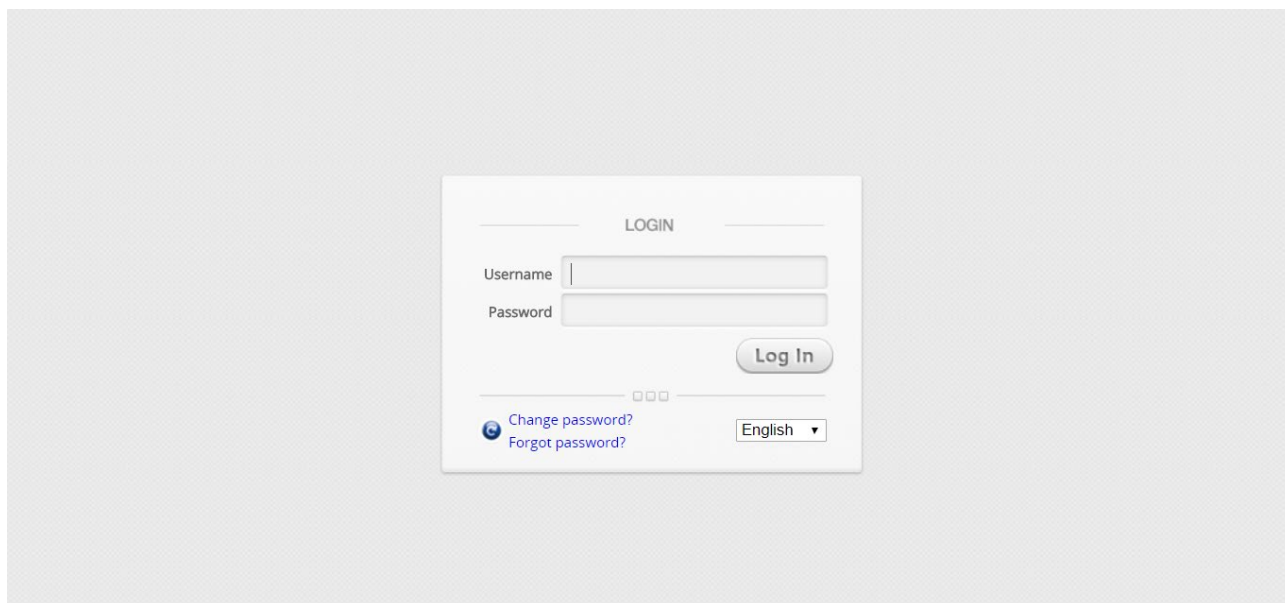

Figure 2-1-1. Controller's WMI Login Page

Step 2.

Create some accounts in the local database for remote VPN connections if local authentication is preferred. When other authentication methods are used, make sure accounts are created in the databases.

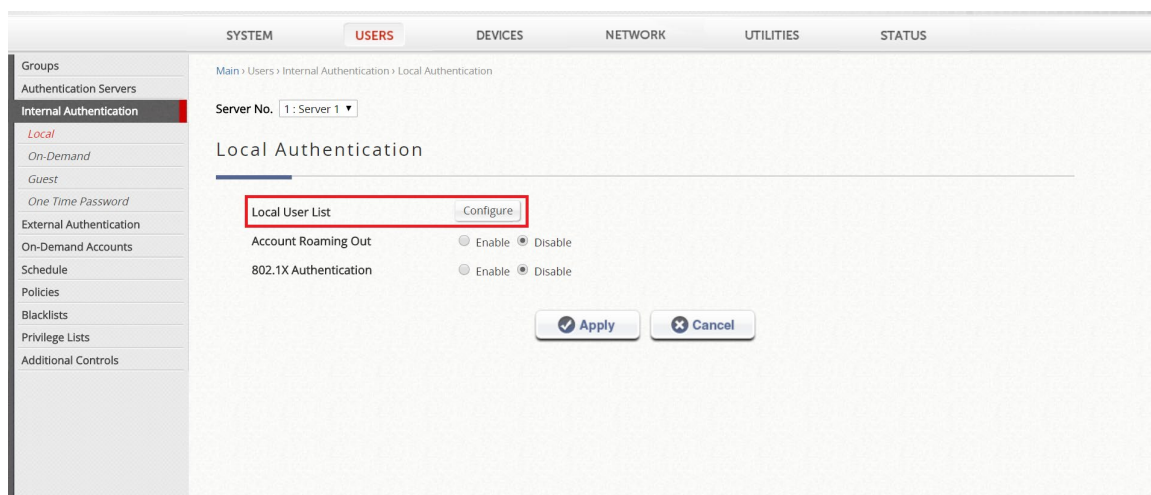Go to *Users > Internal Authentication > Local > Local User List* to create local user accounts.

Figure 2-1-2. Create local user accounts

After accounts are created, administrator can view the accounts' details in Local User List.
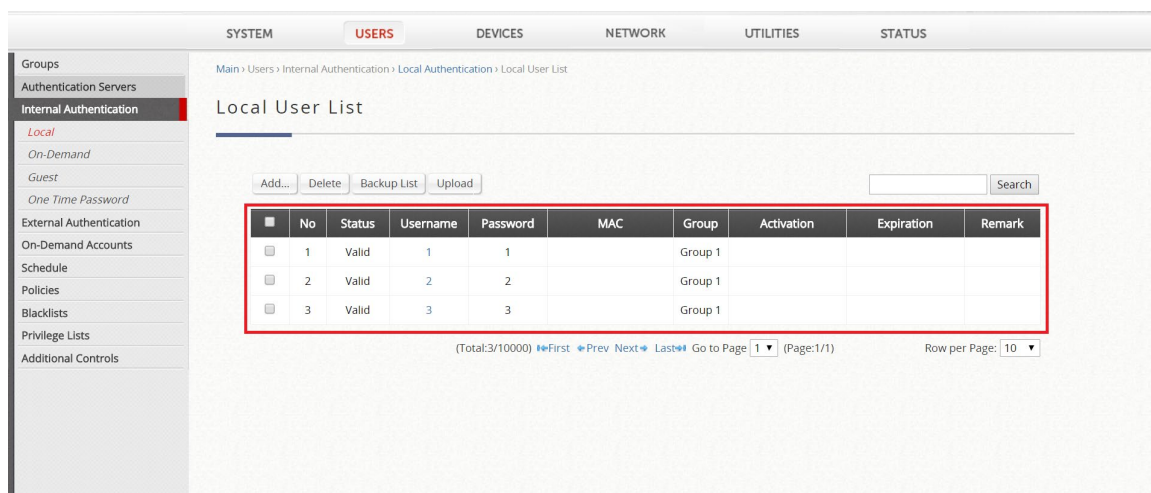

Figure 2-1-3. Local User List

Step 3.

Go to **Network > VPN > Remote VPN PPTP** and enable the function.
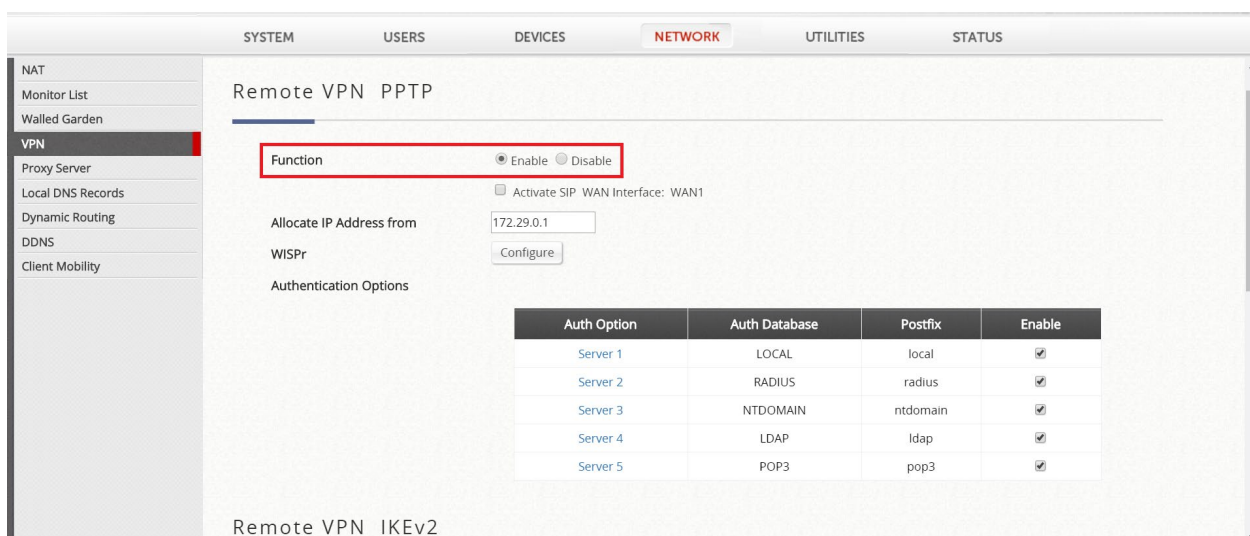

Figure 2-1-4. Enable Remote VPN PPTP

Step 4.

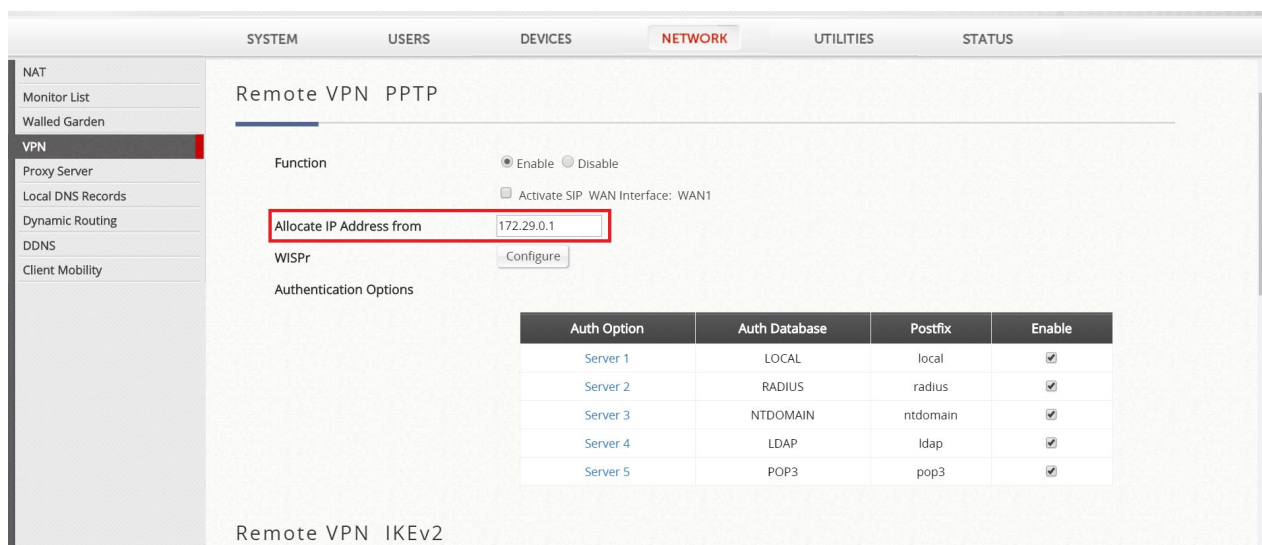Enter start IP address to be assigned to remote clients.

Figure 2-1-5. Select start IP address for Remote VPN PPTP

Step 5.

Select authentication databases to be used for remote VPN connection.
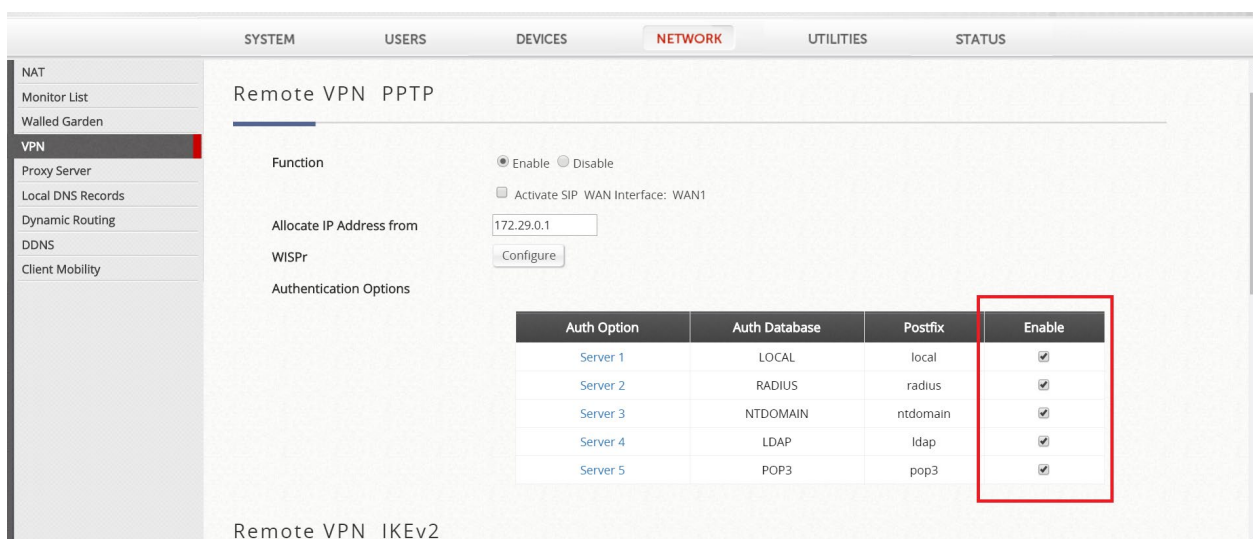

Figure 2-1-6. Select authentication databases for Remote VPN PPTP

Step 6.

Click *Apply* button at the bottom of the page and reboot the controller in order for the configuration to be effective.
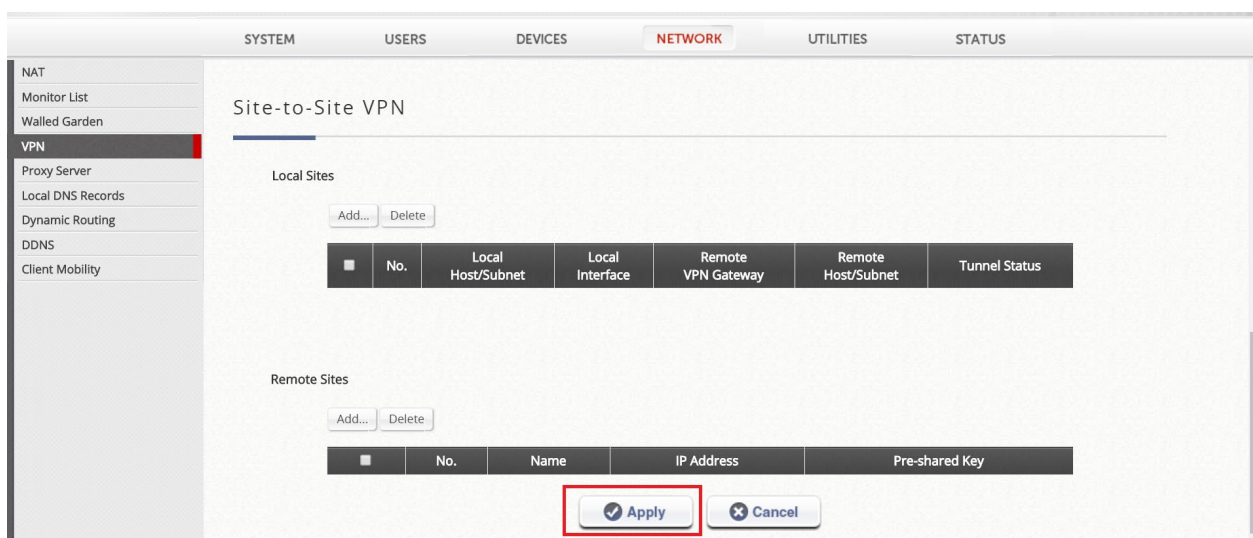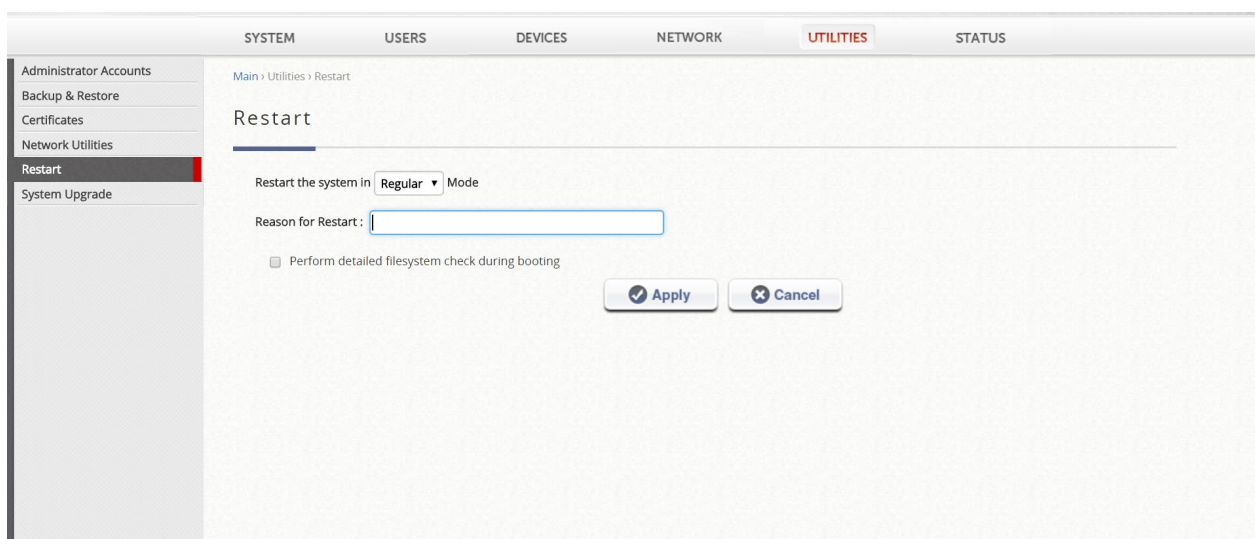

Figure 2-1-7. Apply the configuration

Figure 2-1-8. Restart the controller for the new configuration to take effect

2.2   Remote Client Configuration

2.3   Windows 10 Configuration

Step 1.

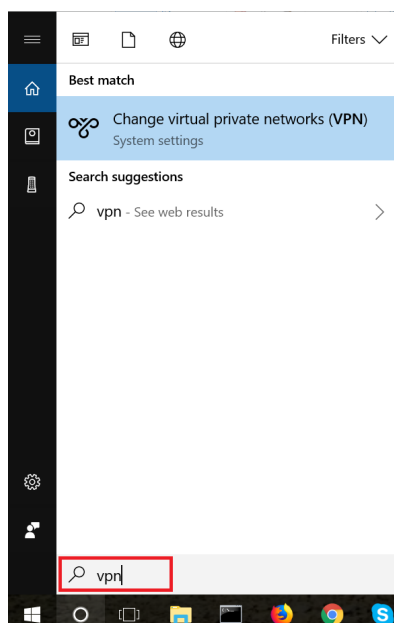On Window 10 device, search for VPN in search bar to open VPN configuration.

Figure 2-2-1-1. VPN Configuration on Windows10 Device

Step 2.

Select **Add a VPN connection** to create a new VPN connection.

Figure 2-2-1-2. Add a new VPN connection

Step 3.

Fill in the VPN configuration details and save it.

VPN provider: Select *Windows (built-in)*.
Connection name: It can be anything you prefer.
Server name or address: Enter your server address.
VPN type: Select *Point to Point Protocol (PPTP)*.
Type of sign-in info: Select *User name and password*.
User name (optional): Enter your remote user account username. E.g. 1@local
Password (optional): Enter your remote user account password.

Figure 2-2-1-3. VPN PPTP Configuration Details

Step 4.

After saving the connection, it will be shown in the VPN connection list. Click on **Connect** for establishing the connection.
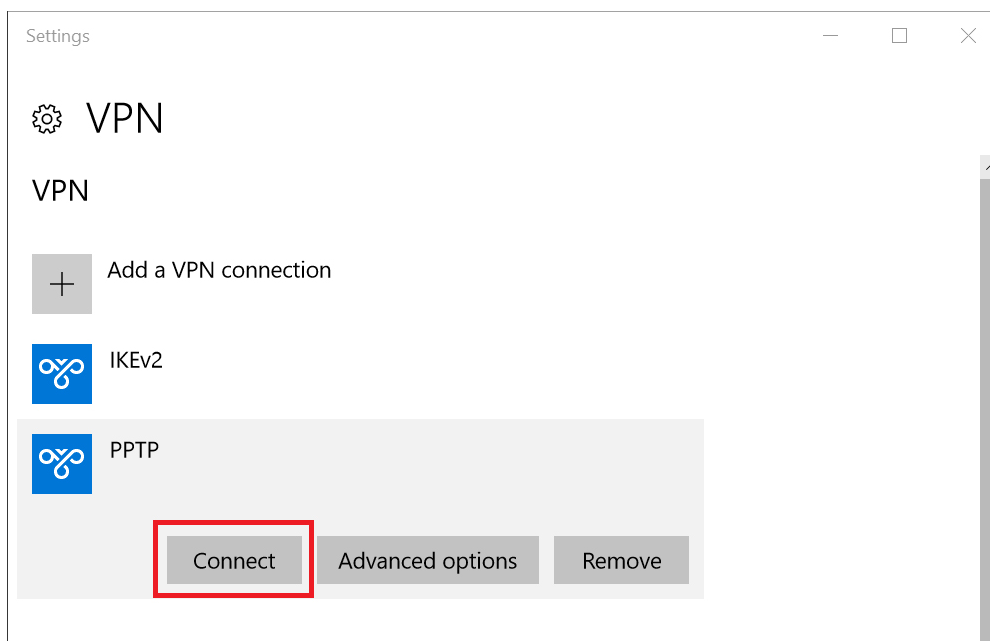

Figure 2-2-1-4. Establish VPN connection

Step 5.

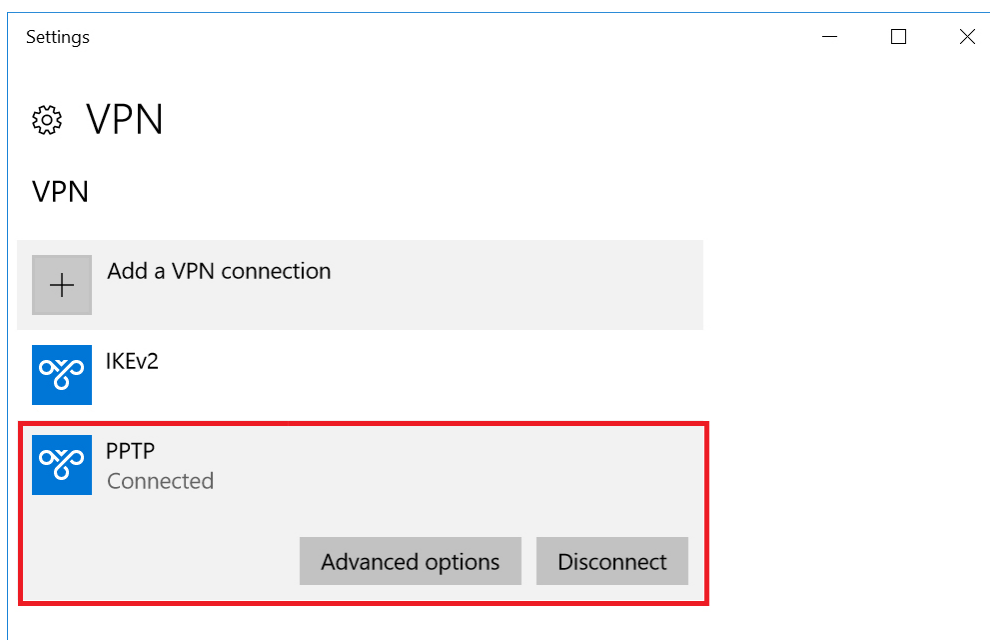After a while, it will connect and show "Connected" status.

Figure 2-2-1-5. Establish VPN connection

10

2.4 iPhone Configuration

iPhone no longer supports VPN-PPTP option since iOS10.

2.5 Android Configuration

Step 1.

Go to **Settings > More connection settings > VPN**. Click on **ADD VPN** to create a new VPN connection.
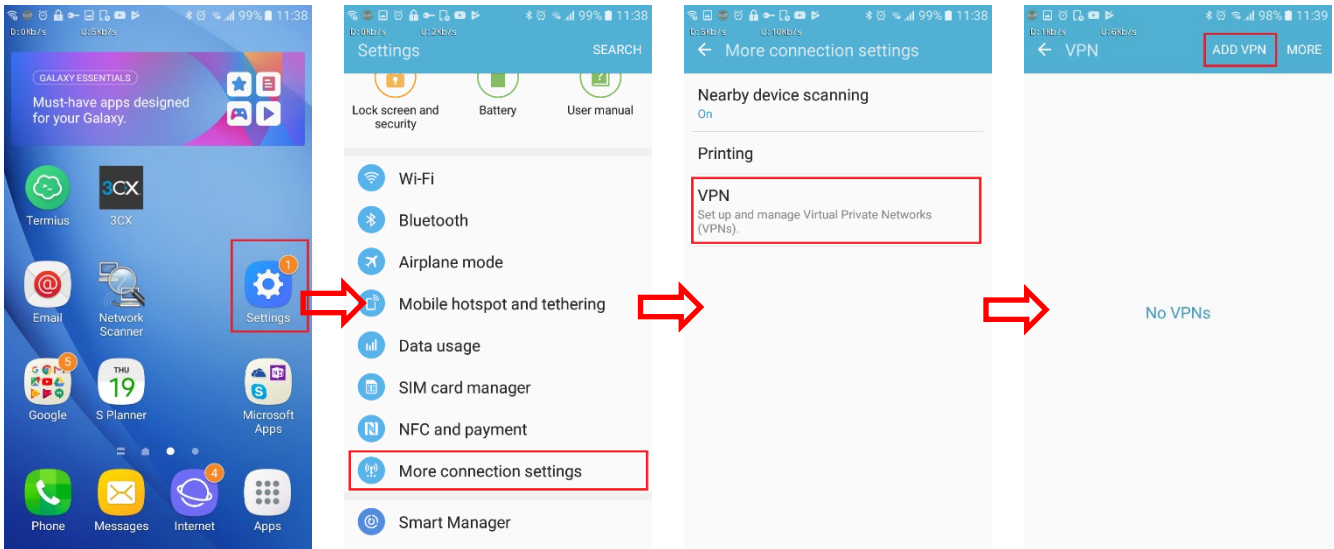

Figure 2-2-2-1. Add a new VPN connection

Step 2.

Fill in the VPN configuration details and click **SAVE** to save it.

Name: It can be anything you prefer.
Type: Select *PPTP*.
Server address: Enter your server name.
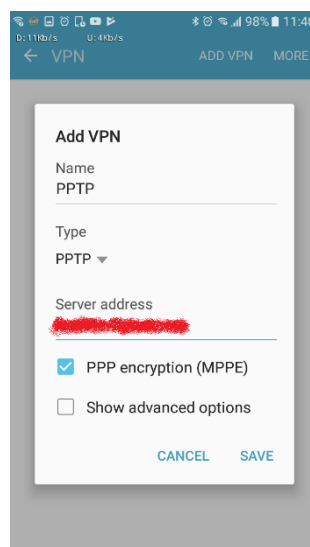**PPP encryption:** Enable the option.

Figure 2-2-2-2. Android VPN PPTP Configuration

Step 3.

After the VPN configuration is saved, it will be shown in the VPN page. Select the configuration for PPTP and tap it to establish VPN connection.
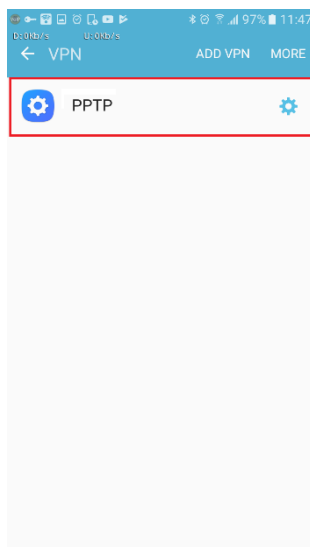

Figure 2-2-2-3. Establish VPN connection

Step 4.

Enter remote user account's username and password and click **CONNECT** to continue establishing VPN connection.
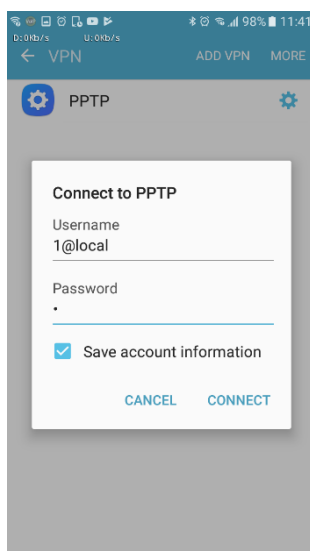

Figure 2-2-2-4. Establish VPN connection

Step 5.

After the connection has been established successfully, it will show **Connected** for the
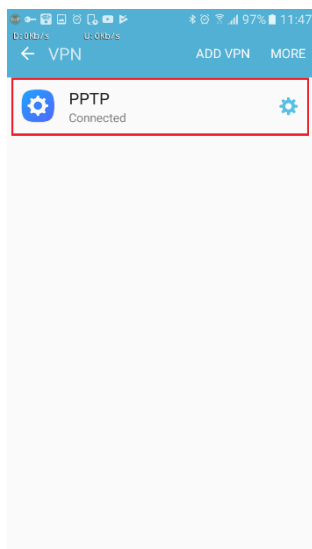
connection.

Figure 2-2-2-5. Successful VPN connection

3. Setup of Remote VPN - IKEv2

3.1   WLAN Controller Configuration

Step 1.

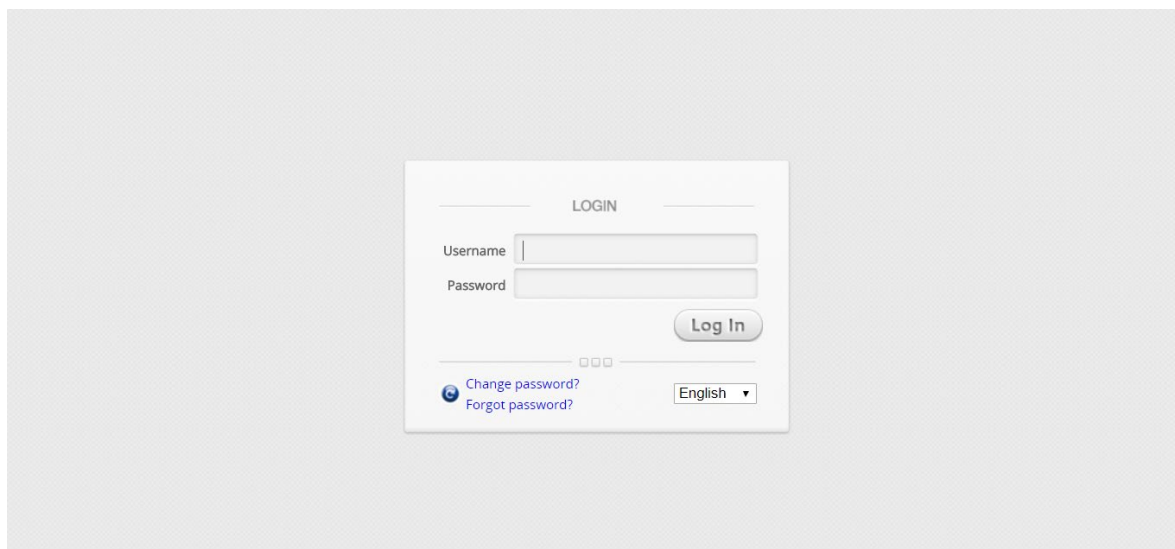Enter the controller's IP address/domain name in browser and login as administrator.

Figure 3-1-1. Controller's WMI Login Page

15

Step 2.

Create some accounts in the local database for remote VPN connections if local authentication is preferred. When other authentication methods are used, make sure accounts are created in the databases.

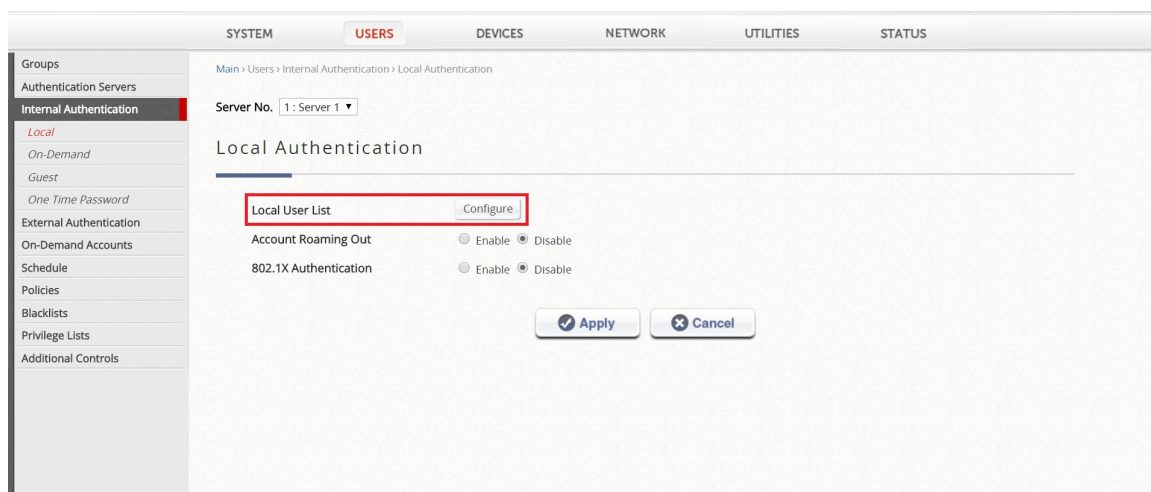Go to *Users > Internal Authentication > Local > Local User List* to create local user accounts.

Figure 3-1-2. Create local user accounts

After accounts are created, administrator can view the accounts' details in Local User List.
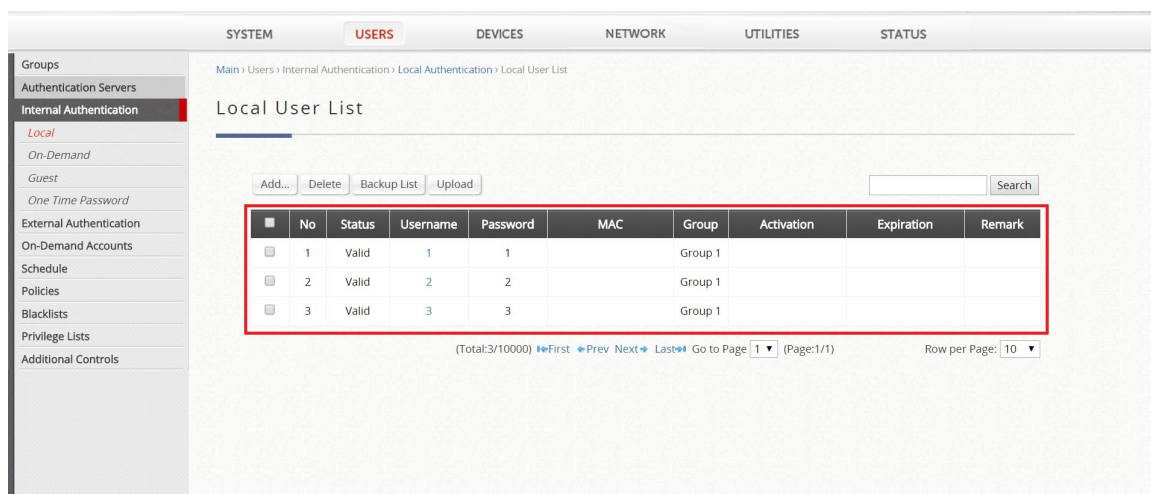

Figure 3-1-3. Local User List

Step 3.

Go to **Utilities > Certificates** and edit **System Certificate**.
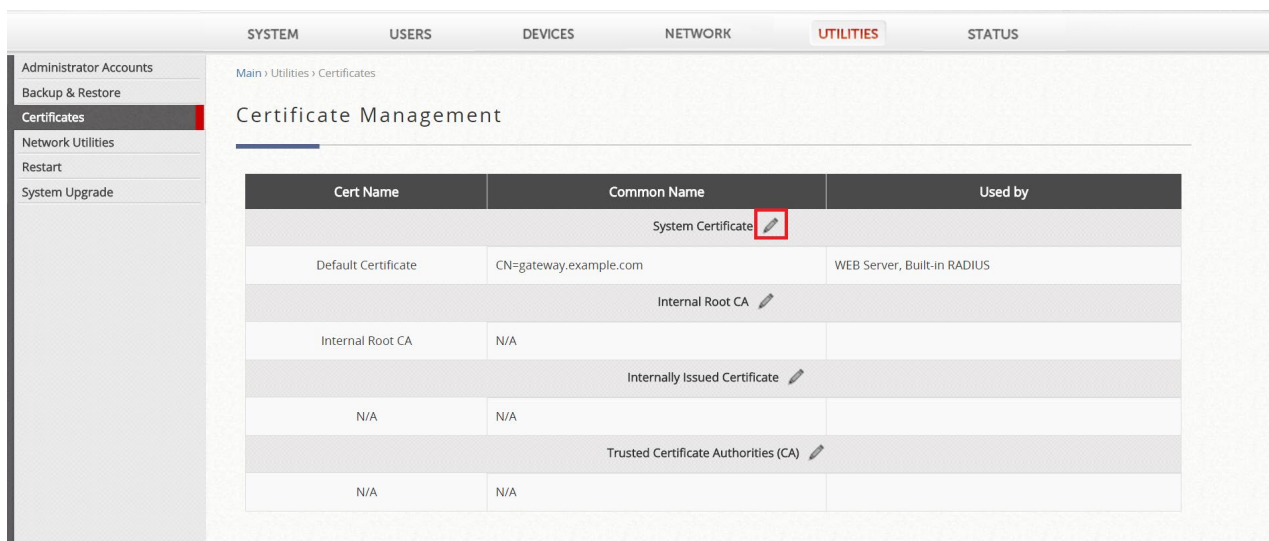

Figure 3-1-4. Edit System Certificate

Step 4.

Upload a valid certificate with its key and/or intermediate CA for the use of remote VPN IKEv2.

Figure 3-1-5. Upload Certificate for Remote VPN IKEv2
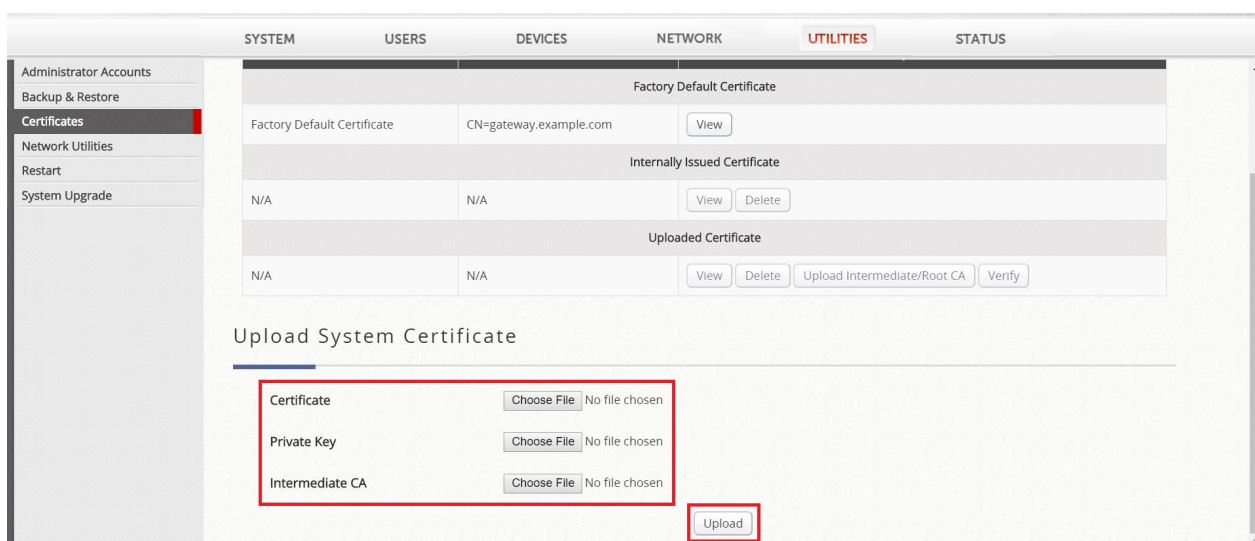
After uploading the certificate, administrator will be able to view it in the **System Certificate** page.
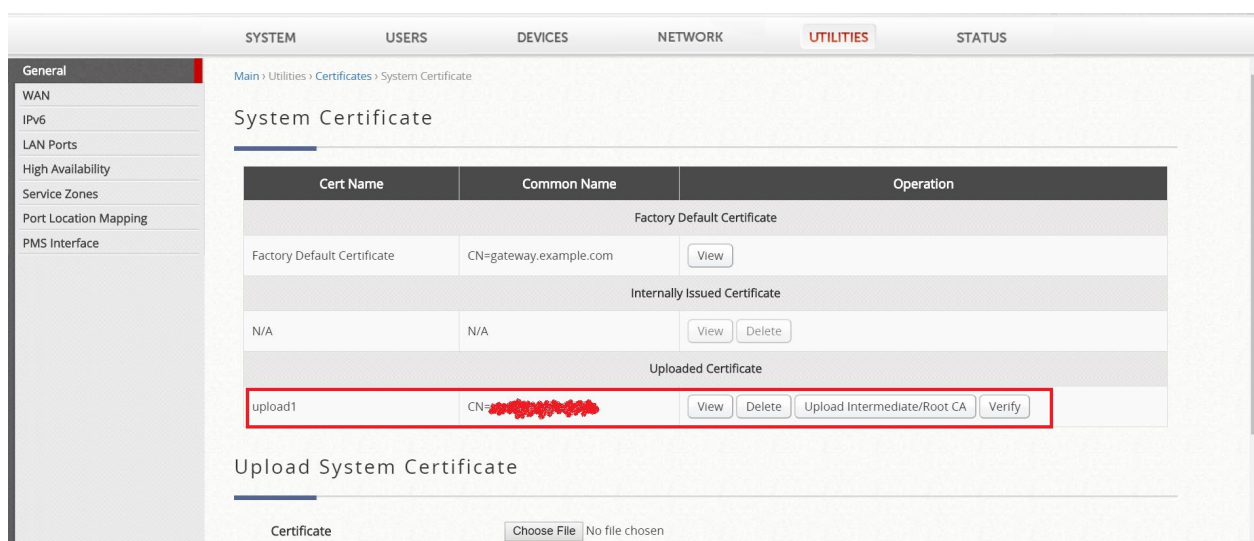

Figure 3-1-6. Uploaded Certificates Overview

Important: Make sure the server name matches certificate's CN and also the server name must be an existent domain name. Otherwise, Windows clients may fail to establish VPN connection with the controller.

Step 5.

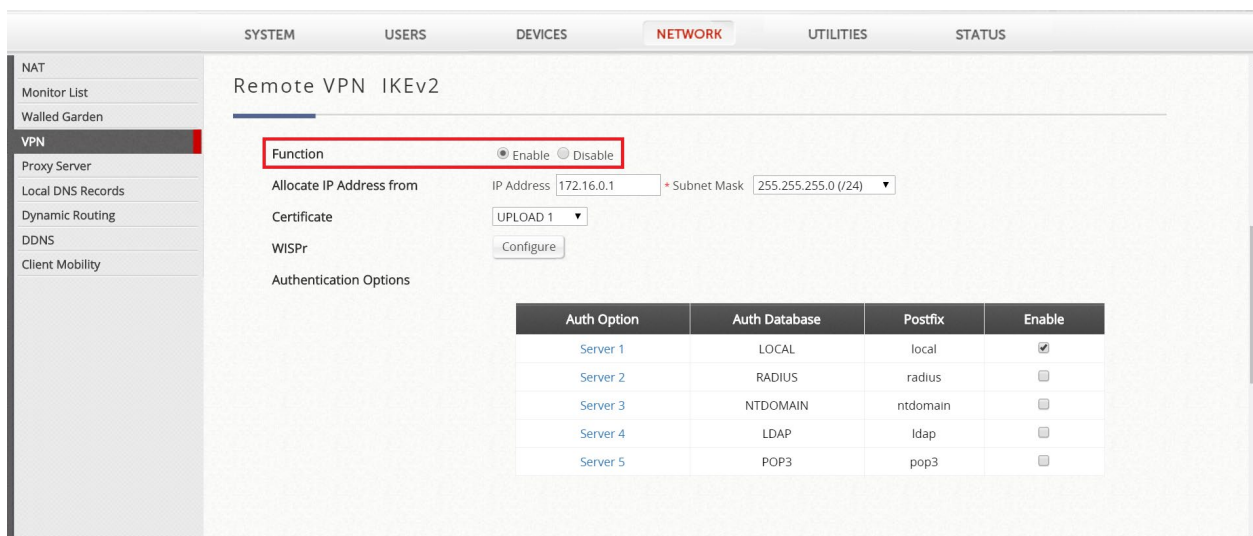Go to **Network > VPN > Remote VPN IKEv2** and enable the function.

Figure 3-1-7. Enable Remote VPN IKEv2

Step 6.

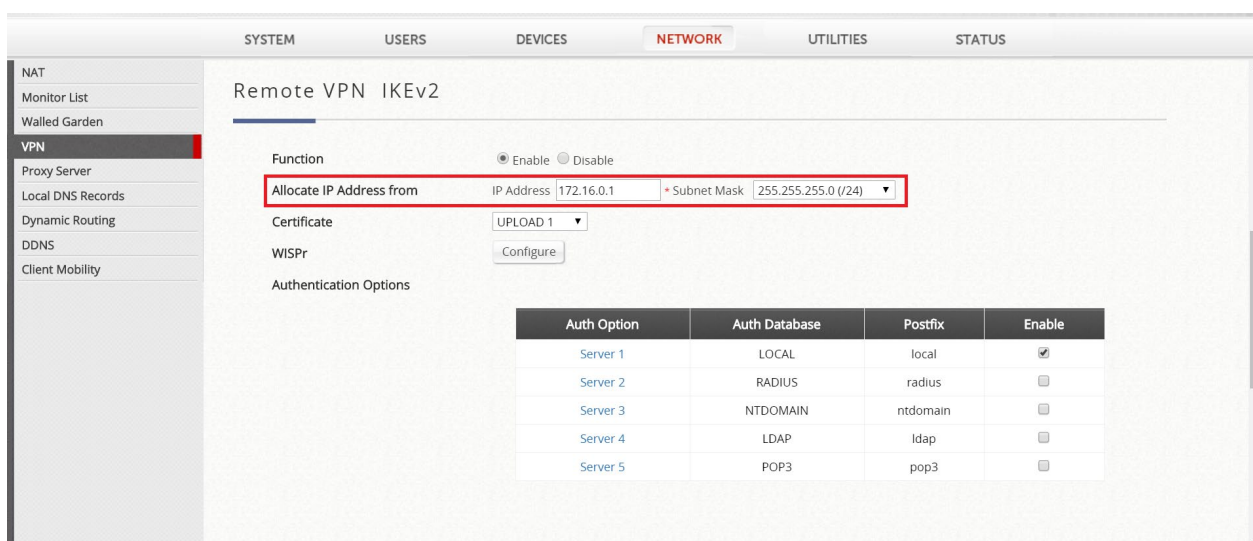Enter start IP address to be assigned to remote clients.

Figure 3-1-8. Select start IP address for Remote VPN IKEv2

Step 7.

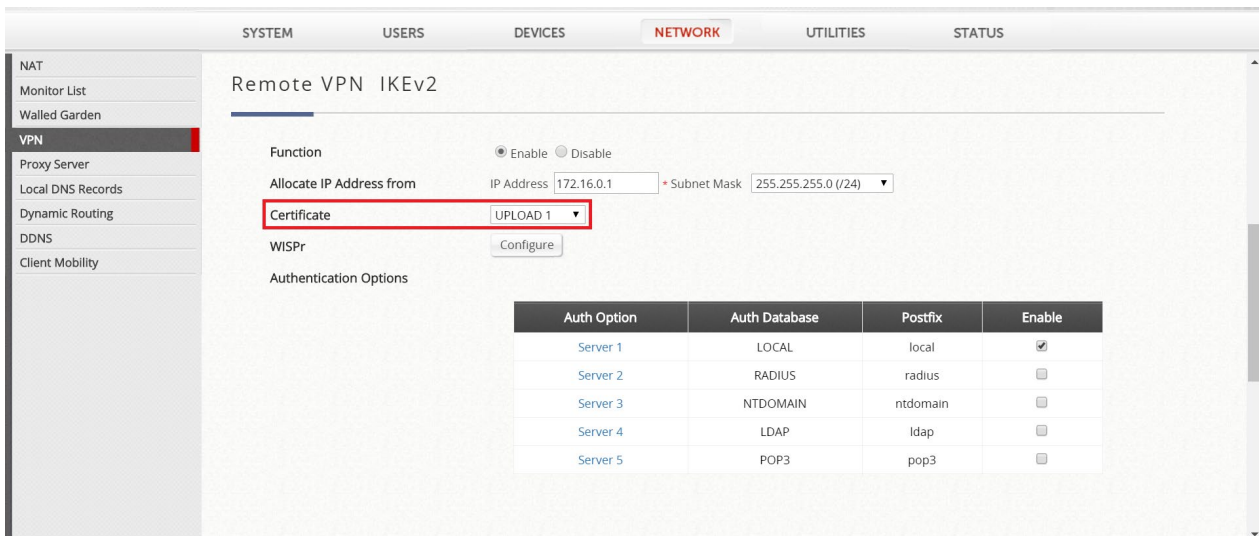Select Certificate to be used for remote VPN connection.

Figure 3-1-9. Select Certificate for Remote VPN IKEv2

Step 8.

Select authentication databases to be used for remote VPN connection.
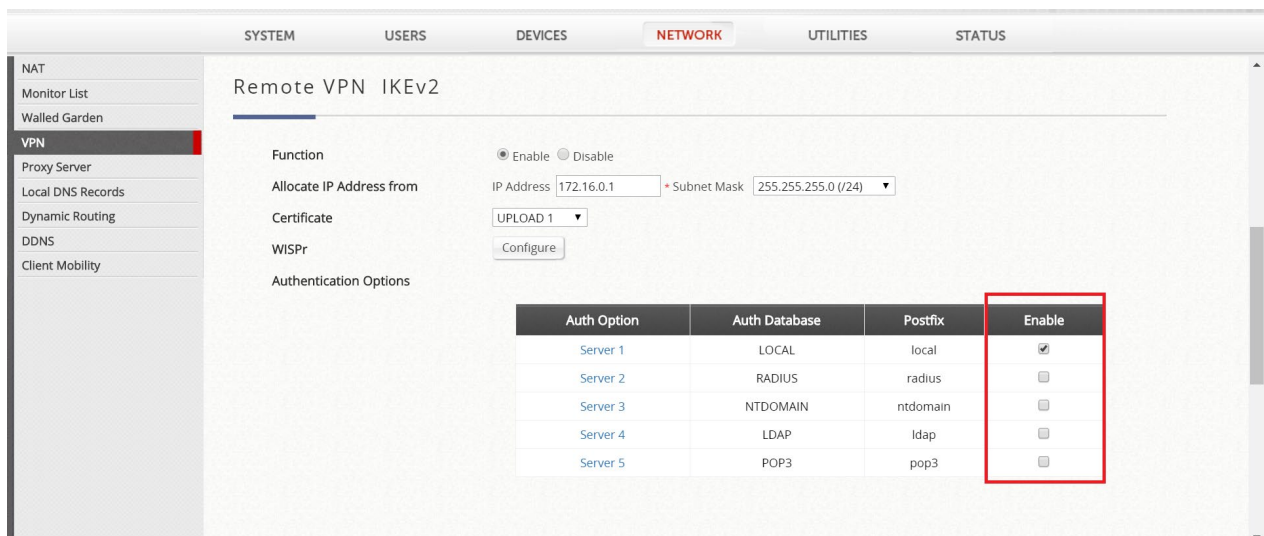
Figure 3-1-10. Select authentication databases for Remote VPN IKEv2

Step 9.

Click **Apply** button at the bottom of the page and reboot the controller in order for the configuration to be effective.
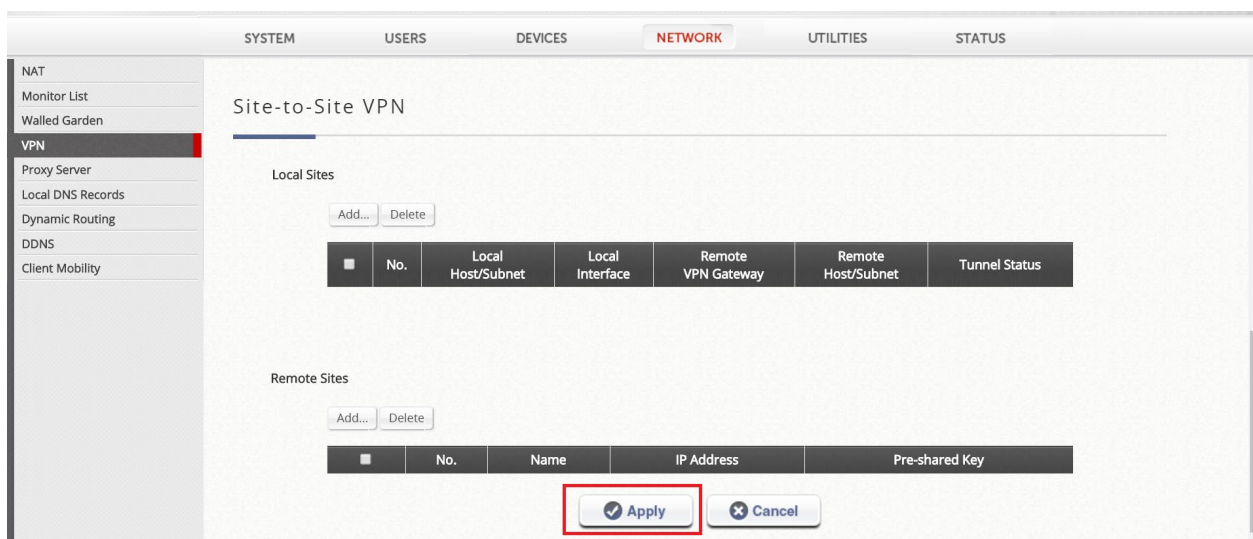
Figure 3-1-11. Apply the configuration

Figure 3-1-12. Restart WHG for the new configuration to be effective

3.2   Remote Client Configuration

3.3   Windows 10 Configuration

Step 1.

On a Window 10 device, search for VPN in search bar to open VPN configuration.

Figure 3-2-1-1. VPN Configuration on Windows 10 Device

Step 2.

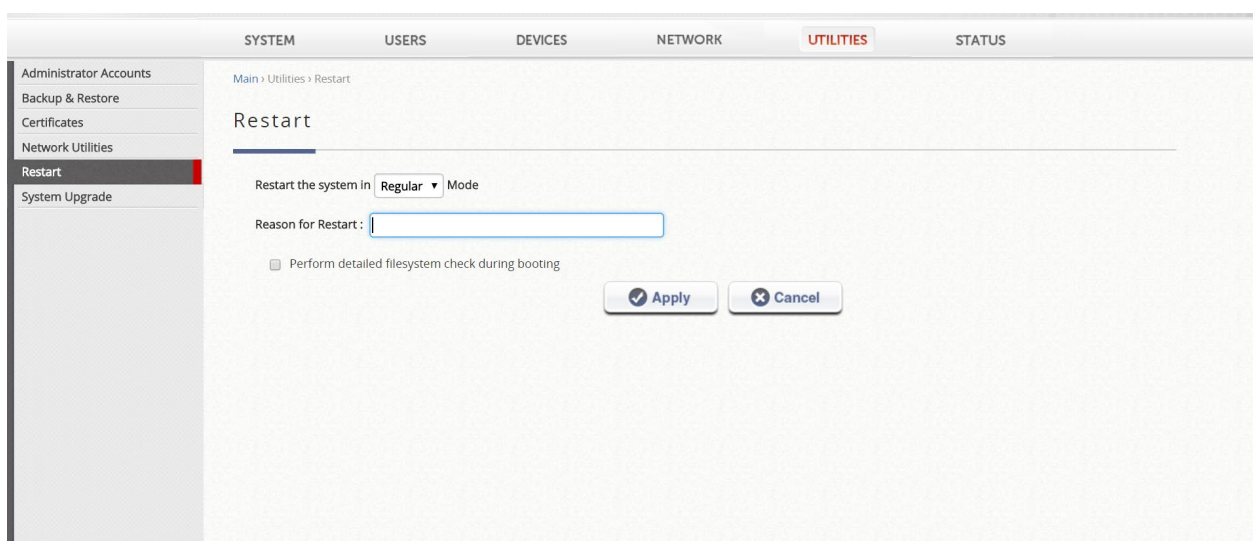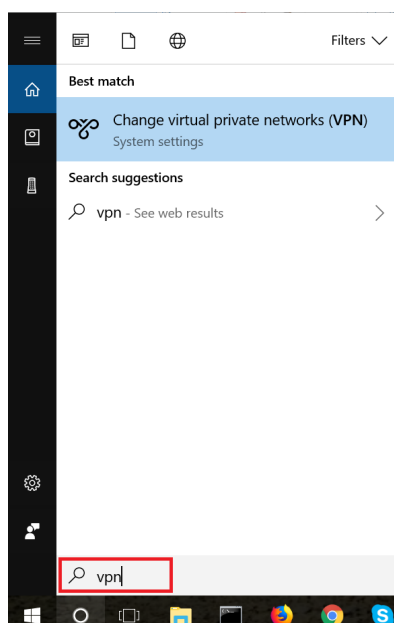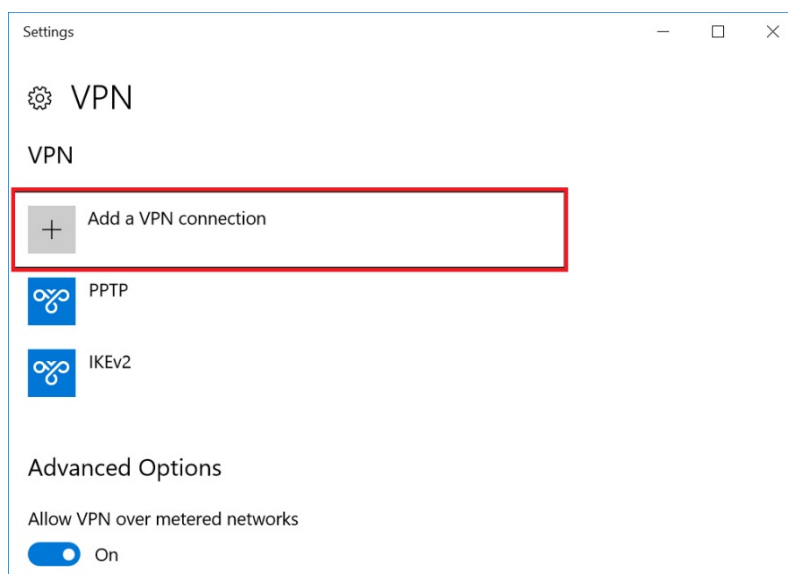Select *Add a VPN connection* to create a new VPN connection.

Figure 3-2-1-2. Add a new VPN connection

Step 3.

Fill in the VPN configuration details and save it.

VPN provider: Select *Windows (built-in)*.
Connection name: It can be anything you prefer.
Server name or address: Enter your server name.
VPN type: Select *IKEv2*.
Type of sign-in info: Select *User name and password*.
User name (optional): Enter your remote user account username. E.g. 1@local
Password (optional): Enter your remote user account password.
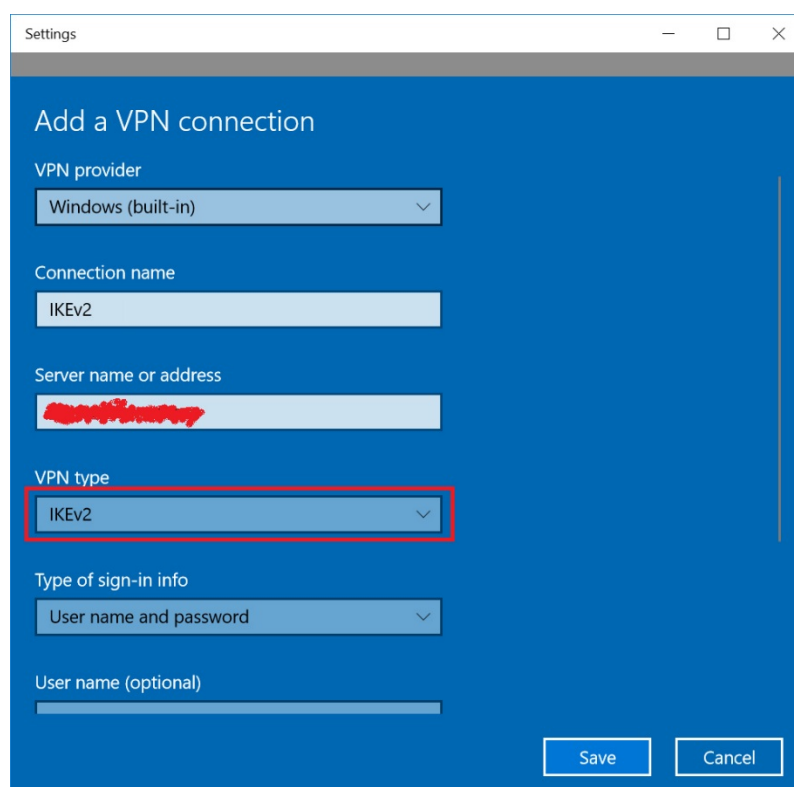
Figure 3-2-1-3. VPN IKEv2 Configuration Details

<u>Important:</u> Make sure the server name matches certificate's CN and also the server name must be an existent domain name. Otherwise, Windows clients may fail to establish VPN connection with the controller.

Step 4.

After saving the connection, it will be shown in the VPN connection list. Click on **Connect** for establishing the connection.
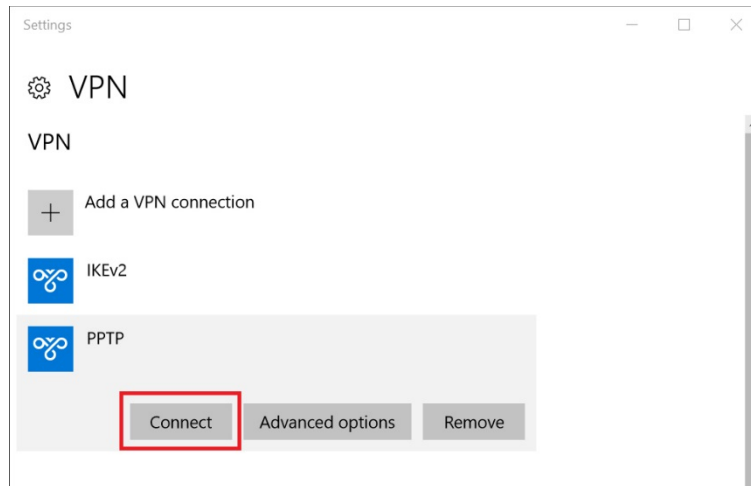
Figure 3-2-1-4. Establish VPN connection

Step 5.

After a while, it will connect and show **Connected** status.
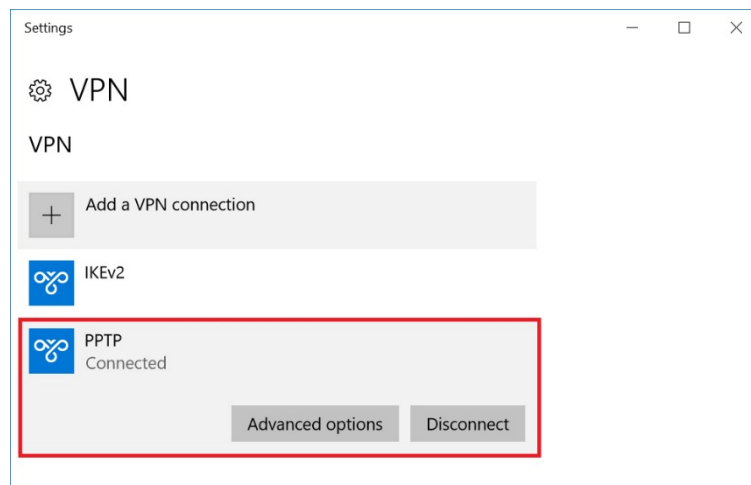
Figure 3-2-1-5. Successful VPN Connection

3.4   iPhone Configuration

Step 1.

On an iPhone, go to **Settings > General > VPN**. Click on **Add VPN Configuration** to create a new VPN connection.
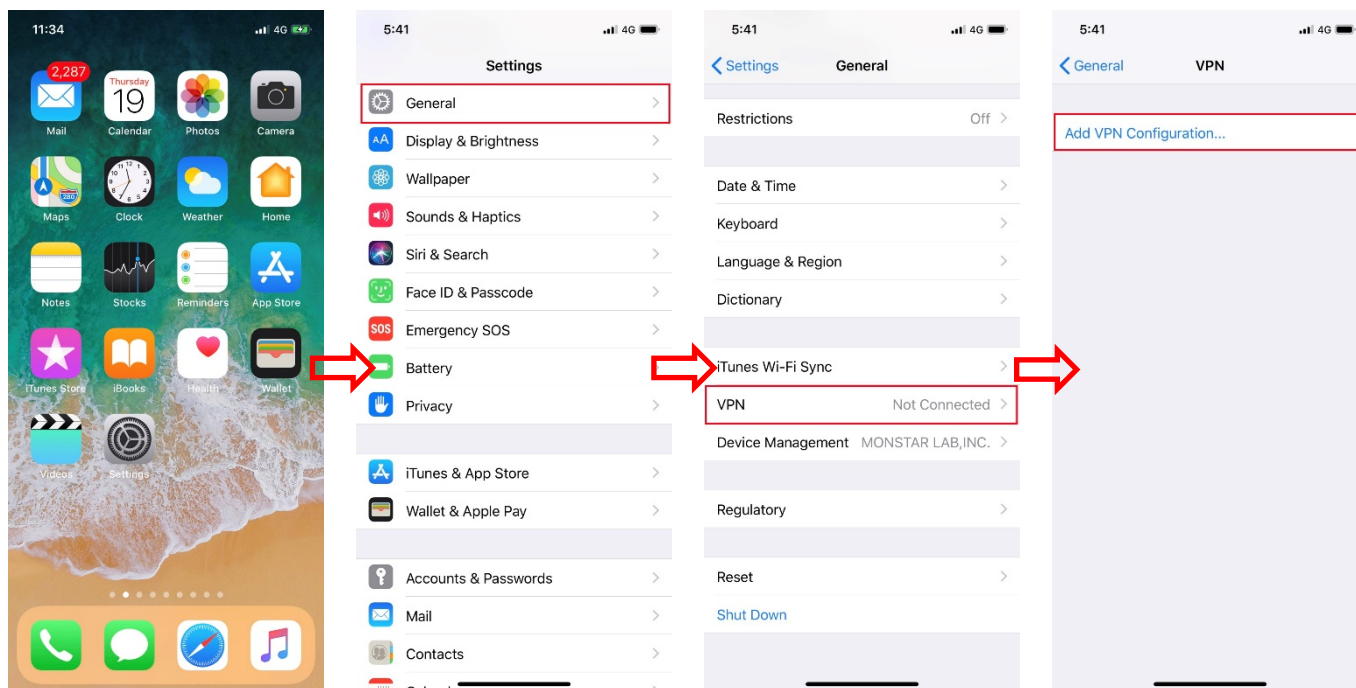
Figure 3-2-2-1. Add a new VPN connection

25

Step 2.

Fill in the VPN configuration details and click **Done** to save it.

Type: Select *IKEv2*.
Description: It can be anything you prefer.
Server: Enter your server name.
Remote ID: Enter your server name.
Local ID: Leave empty.
User Authentication: Select *username*.
Username: Enter your remote user account username. E.g. 1@local
**Password:** Enter your remote user account password.
Proxy: Select *Off*.

Figure 3-2-2-2. iPhone VPN IKEv2 Configuration

Step 3.

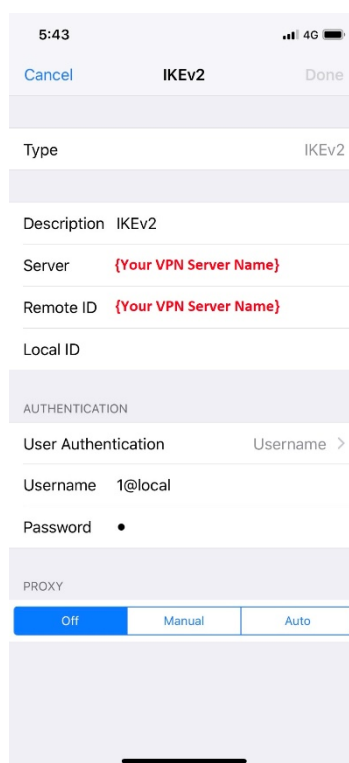After the VPN configuration is saved, it will be shown in the VPN page. Select the configuration for IKEv2 and tap the Status slider to establish VPN connection.
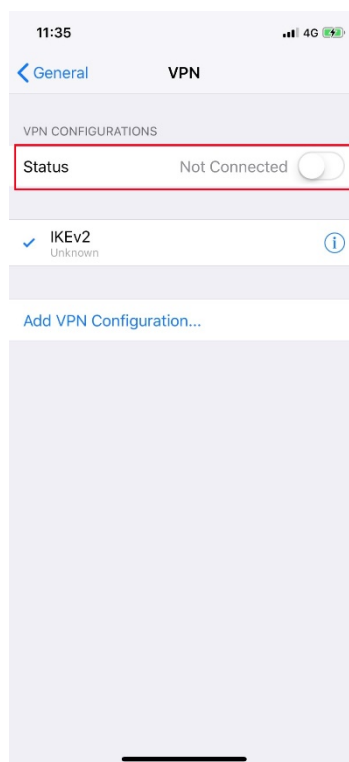

Figure 3-2-2-3. Establish VPN connection

Step 4.

After the connection has been established successfully, it will show **Connected** on the Status field.
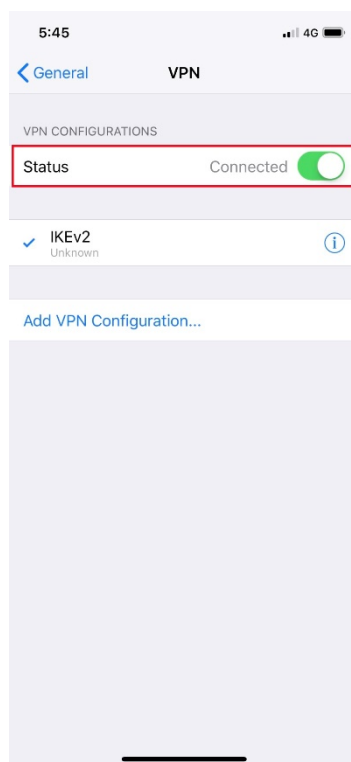

Figure 3-2-2-4. Successful VPN Connection

3.5 Android Configuration

EWS controller currently only supports EAP-only authentication in IKEv2 but not other types of authentication, such as IKEv2 PSK or IKEv2 RSA. However, built-in VPN function on Android devices only supports IKEv2 PSK or IKEv2 RSA; therefore, it is required to use a third-party VPN APP that supports EAP-IKEv2 to establish VPN IKEv2 connection with the controller. In this guide, we use strongSwan APP as an example, but another APP that has the same feature can also be used.

Step 1.

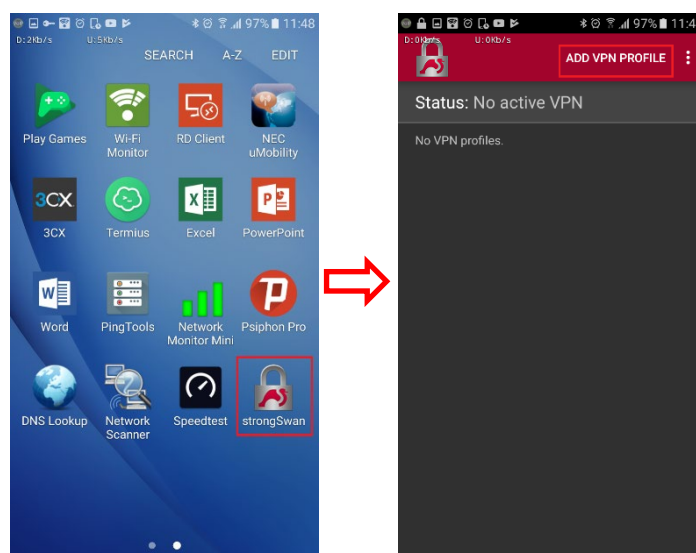Open strongSwan APP and click **ADD VPN PROFILE** to create a new VPN configuration.

Figure 3-2-3-1. Add a new VPN connection

Step 2.

Fill in the VPN configuration details and click **SAVE** to save it.

Server: Enter your server name.
VPN Type: Select *IKEv2 EAP (Username/Password)*.
Username: Enter your remote user account username. E.g. 1@local
Password (Optional): Enter your remote user account password.
CA certificate: Tick *Select automatically*.
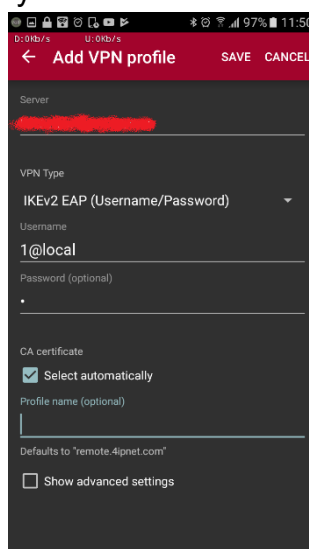**Profile name (optional):** Leave empty.

Figure 3-2-3-2. Android VPN IKEv2 Configuration

Step 3.

After the VPN configuration is saved, it will be shown in the strongSwan APP. Tap the configuration to establish VPN connection.
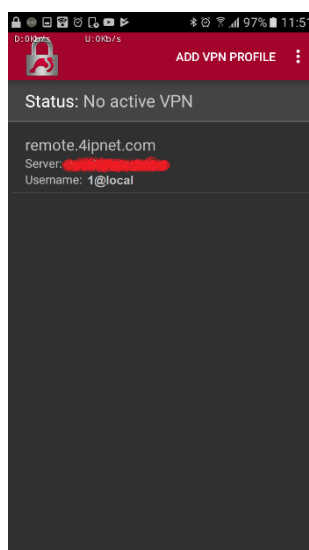

Figure 3-2-3-3. Establish VPN connection

Step 4.

After the connection has been established successfully, it will show **_Connected_** on the Status field in strongSwan APP. Additionally, it will also show **_Connected_** for the VPN connection in Android's VPN page.
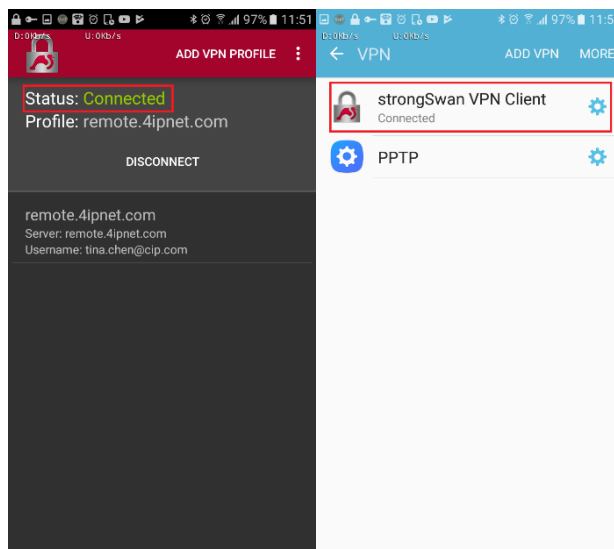

Figure 3-2-3-4. Successful VPN Connection

4. Conclusion

Some end users would like to access company network when they are outside of office or traveling so that they can access the file servers or have their internet traffic go through company network.

Remote VPN can be built using the EWS controller. Furthermore, any Local Accounts can remotely access the network resource under some certain wireless LAN environment, such as workplace, school, SMB, etc. That is, any employees could experience the wireless LAN of the certain application without any restriction.

5. Remarks

For more information, please contact your local Systems Integrator, or contact support@4ipnet.com for support.