

## Grandstream Networks, Inc.

---

WP820

Enterprise Portable Wi-Fi Phone

**OpenVPN® Guide**



## Table of Contents

<b>OVERVIEW</b> .....	<b>3</b>
<b>ENABLE OPENVPN® FEATURE</b> .....	<b>4</b>
<b>OPENVPN® MODES</b> .....	<b>4</b>
Simple Mode .....	4
Professional Mode (Expert Mode) .....	6

## Table of Figures

Figure 1: VPN Architecture Overview .....	3
Figure 2: OpenVPN® Settings Page - Simple Mode .....	4
Figure 3: OpenVPN® Settings Page - Expert Mode .....	6
Figure 4: Expert Mode ZIP file .....	6

## Table of Tables

Table 1: OpenVPN® Settings – Simple Mode .....	5
--	---



## OVERVIEW

VPN (Virtual Private Network) is a network that communicates by creating a dedicated and encrypted network channel (tunnel) on the public network, which can help remote users, company branches, business partners and suppliers in practical applications. Establish a secure and trusted network connection between them.

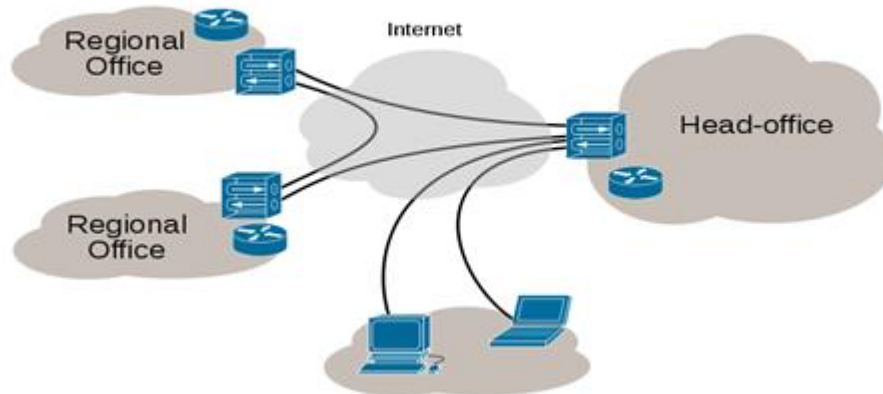


Figure 1: VPN Architecture Overview

OpenVPN® is a well-known open source VPN software, very stable and reliable to use, its main features: open source, cross-platform, easy to use, stable and secure. The WP820 can be used as a client to connect to a VPN server using the OpenVPN® function for remote communication. This article briefly describes how the WP820 uses the OpenVPN® feature.

## ENABLE OPENVPN® FEATURE

If users want to use the OpenVPN function, they need to set the OpenVPN related configuration from the WP820 Web GUI as follow:

1. Log in to the WP820 Web GUI page
2. Navigate to **Network Settings** → **OpenVPN® Settings** page
3. Check **Enable OpenVPN®**
4. Select either **Simple Mode** or **Expert Mode**, Then Configure related parameters or upload a configuration file to save the configuration.

## OPENVPN® MODES

The WP820 supports two modes:

- **Simple Mode**: only configure some basic or common parameter configurations.
- **Expert Mode**: support configuration file upload, fully customized.

**Note:** After switching modes, the phone needs to be restarted for the new settings to take effect.

## Simple Mode

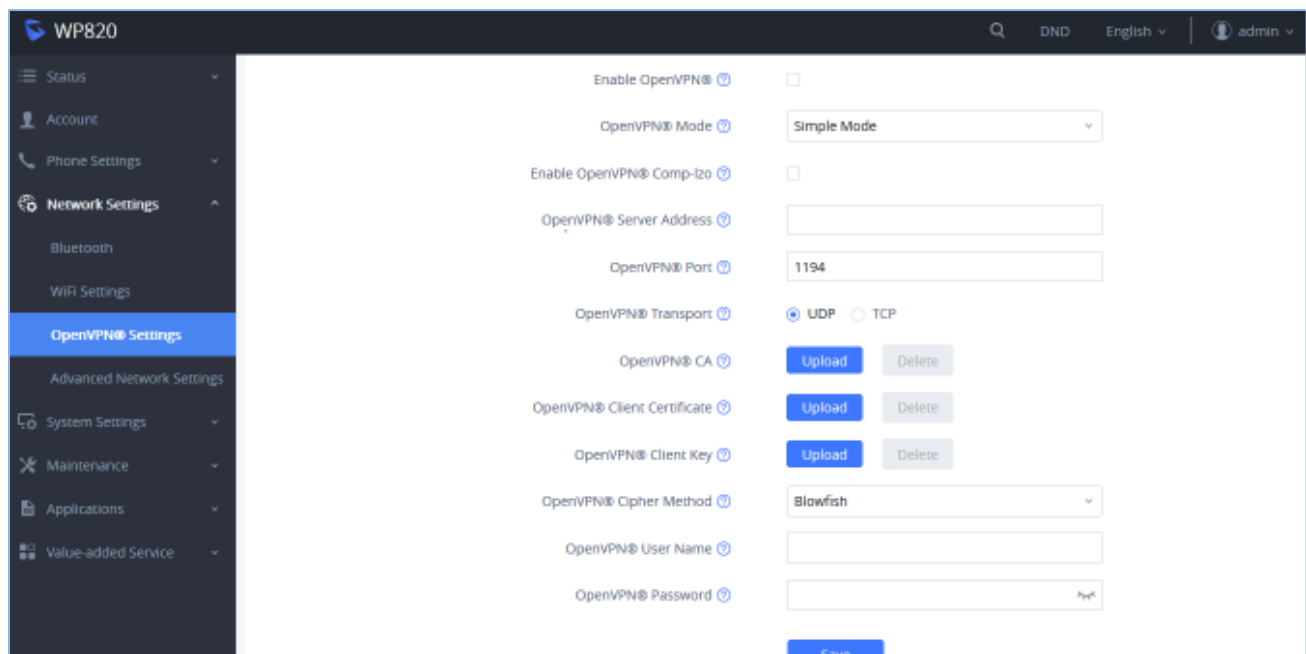


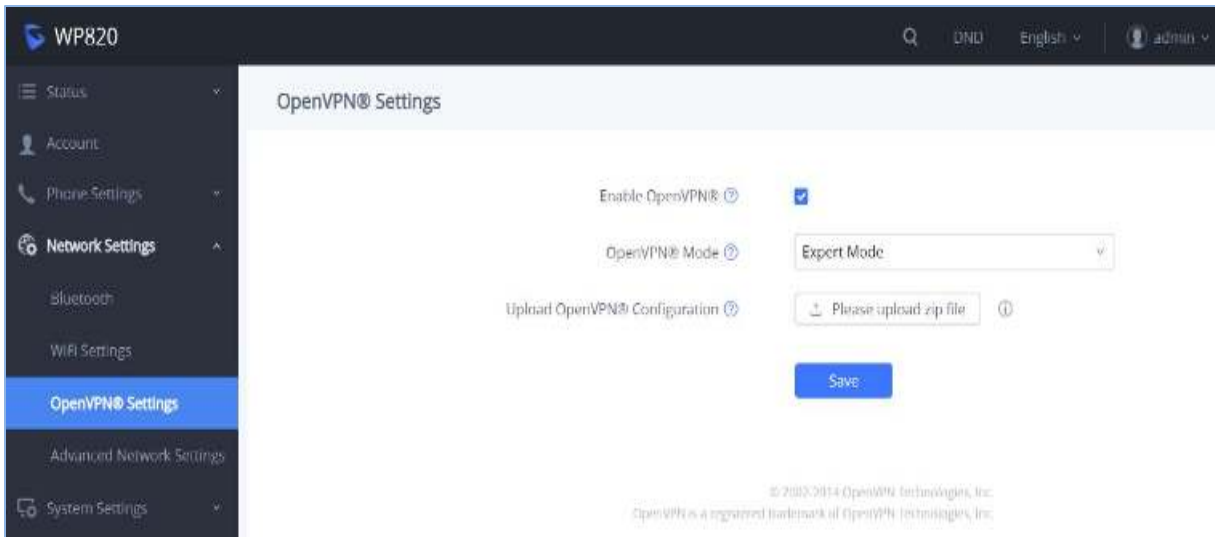
Figure 2: OpenVPN® Settings Page - Simple Mode

**Table 1: OpenVPN® Settings – Simple Mode**

Name	Description
<b>Enable OpenVPN®</b>	This enables/disables OpenVPN® functionality and requires the user to have access to an OpenVPN® server. <b>Notes:</b> <ul style="list-style-type: none"> <li>To use OpenVPN® functionalities, users must enable OpenVPN® and configure all of the settings related to OpenVPN®, including server address, port, OpenVPN® CA, certificate and key.</li> <li>Additionally, the user must also set the SIP account to use "OpenVPN" for the "NAT Traversal" under Account → General Settings → Network Settings</li> </ul>
<b>OpenVPN® Mode</b>	Select either <b>Simple Mode</b> (Default) or <b>Expert Mode</b> .
<b>Enable OpenVPN® Comp-izo</b>	Choose to enable/disable the LZO compression. When the LZO Compression is enabled on the OpenVPN server, you must turn on it at the same time. Otherwise, the network will fail to connect.
<b>OpenVPN® server address</b>	The URL/IP address for the OpenVPN® server.
<b>OpenVPN® port</b>	Set up the network port to communicate with the OpenVPN® server. The default port is 1194.
<b>OpenVPN® Transport</b>	Determines network protocol used for OpenVPN® (UDP or TCP). The default setting is <b>TCP</b> .
<b>OpenVPN® CA</b>	The OpenVPN® certificate used for authentication with OpenVPN® servers. Click " <b>Upload</b> " to upload the certificate file (ca.crt) to the device.
<b>OpenVPN® client certificate</b>	The OpenVPN® Client Certificate used for authentication with OpenVPN® servers. Click " <b>Upload</b> " to upload the client certificate file (*.crt) to the device.
<b>OpenVPN® client key</b>	The OpenVPN® client key used for authentication with the OpenVPN® server. Click " <b>Upload</b> " to upload the client certificate file (*.key) to the device.
<b>OpenVPN® ® Cipher Method</b>	Set the OpenVPN® encryption method, you must use the same encryption method as the OpenVPN® server. Supported encryption methods are Blowfish, AES-128 and AES-256.
<b>OpenVPN® username</b>	Set the OpenVPN® username (optional).
<b>OpenVPN® password</b>	Set the OpenVPN® password (optional).

## Professional Mode (Expert Mode)

Professional mode supports configuration file upload in zipped format, which is totally customized by need, please refer to <https://openvpn.net> for more information.



**Figure 3: OpenVPN® Settings Page - Expert Mode**

The below example shows the Professional mode (**Expert Mode**) related configuration:

1. Select OpenVPN mode as **Expert Mode**,
2. Click “upload zip file” and browse your local directory to select the custom configuration file.

### Notes:

- A zip format file is required for the upload feature.
- The zip file must contain the “**client.conf**” and a **certificate file (.crt)**
- The zip file should contain the files as shown in below screenshot:

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
ca.crt	1,712	1,070	Security Certificate	12/18/2018 6:1...	81386A26
client.conf	1,556	951	CONF File	4/23/2019 7:09...	847989DA
client1.crt	5,436	2,773	Security Certificate	12/18/2018 6:1...	AF8B7F72
client1.key	1,704	1,312	KEY File	12/18/2018 6:1...	12A26606

**Figure 4: Expert Mode ZIP file**

The contents of the **client.conf** file format are as follows:



```
# Indicates that the file is a client configuration file
client
# The tun mode is used. Currently OpenVPN® only supports this mode.
dev tun
# Connection method used
proto udp
#VPN Service address
remote 192.168.124.110 1194
# Connection failed number of attempts
connect-retry 3

# Whether to bind local address and port
;nobind

# Indicates whether the server push routing configuration
# When the attribute is not configured, the custom route and server push route will take effect.
# If this attribute is configured, the custom route and server push route will not take effect.
#route-nopull

# Indicates whether to redirect all traffic to OpenVPN as shown below to indicate that ipv4 is redirected to OpenVPN
# Can use "!" to express the opposite
# Configurable value ipv4 ipv6. If not configured, the default is redirect all traffic to OpenVPN.
redirect-gateway !ipv4 ipv6
persist-key
persist-tun

# Configuring custom routes
route 192.168.126.1 255.255.255.0
route 192.168.124.1 255.255.255.0

# Configure account and password
# The first parameter is the account name
# The second is the account password
;auth -user -pass Account Passwd

# Certificate configuration path. The configuration file needs to be an absolute file path.
ca /data/openvpn/ca.crt
cert /data/openvpn/client1.crt
key /data/openvpn/client1.key

# Specify DNS resolution retry interval
resolv-retry infinite

# Configuring DNS. Generally using DNS delivered by the VPN server
dhcp-option DNS 114.114.114.114

# Transmission encryption
cipher BF-CBC
# Whether to enable the lzo compression algorithm and other OpenVPN custom features
comp-lzo

# Specify the server verification method.
ns-cert-type server
# Debugging log level
verb 3
```

*\*OpenVPN is a registered trademark of OpenVPN Inc*

