



Version:

Date: 2020-12-22



- ☎ Support: +86-592-5503301
- ✉ Support: support@yeastar.com
- 🌐 <https://www.yeastar.com>

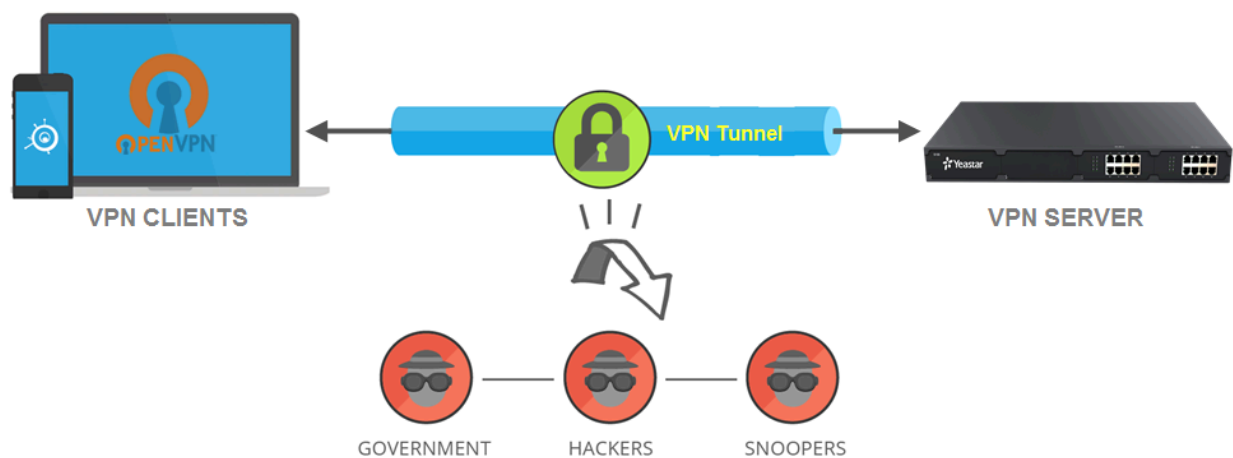
# Contents

<b>VPN Server.....</b>	<b>1</b>
OpenVPN Certificates and Keys.....	1
Install OpenVPN on Windows.....	2
Generate OpenVPN Certificates and Keys.....	4
Check the Generated OpenVPN Certificates and Keys.....	7
OpenVPN Server Configurations.....	8
Set up Yeastar S-Series VoIP PBX as an OpenVPN Server.....	8
OpenVPN Clients Configurations.....	16
Connect Yeastar S-Series VoIP PBX to another Yeastar S-Series VoIP PBX.....	16
Connect to Yeastar S-Series VoIP PBX with Windows.....	18
Connect to Yeastar S-Series VoIP PBX with iOS Device.....	21
Connect to Yeastar S-Series VoIP PBX with Android Device.....	27
Connect Yealink Phones to Yeastar S-Series VoIP PBX.....	31
Check the Client Status.....	35

# VPN Server

Yeastar S-Series VoIP PBX VPN Server provides flexible VPN solutions for small and medium company which does not set up a VPN network for whole company. With VPN connection, you can set up multiple VPN clients to access Yeastar S-Series VoIP PBX safely and securely wherever and whenever.

- Yeastar S-Series VoIP PBX supports OpenVPN protocol.
- VPN Sever App is supported on Yeastar S-Series VoIP PBX version 30.2.0.8 or later.



## About This Guide

This guide is intended to help you to set up the Yeastar S-Series VoIP PBX VPN server, and connect Yeastar S-Series VoIP PBX server via OpenVPN with the following clients:

- Windows
- iOS
- Android
- Yealink IP phone
- Yeastar S-Series VoIP PBX

## OpenVPN Certificates and Keys


Before you start to set up the OpenVPN network, you need to make the related certificates and keys for VPN server and VPN clients.

This topic describes how to set up your own Certificate Authority (CA) and generate certificates and keys for an OpenVPN server and multiple clients on Windows 10 via OpenVPN.

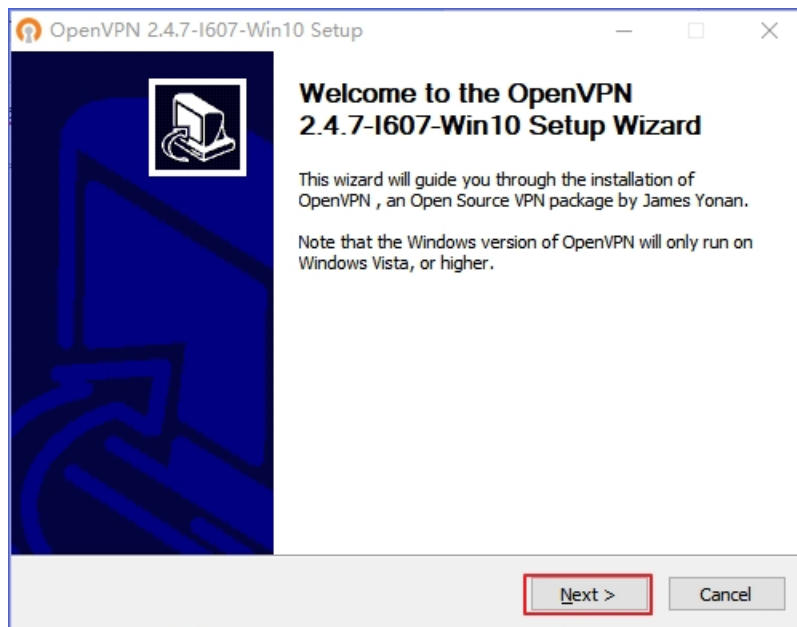
## Install OpenVPN on Windows

You need to install OpenVPN on your PC, and then get sample configuration files and make OpenVPN keys and certificates.

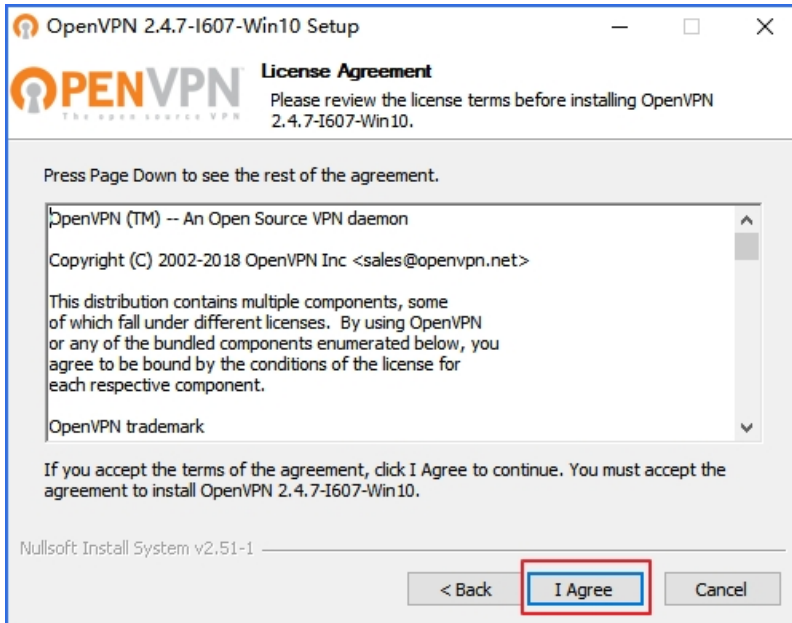
1. [On the OpenVPN download page](#), select a suitable OpenVPN installer to download.

 **Note:** OpenVPN must be installed and run by a user who has administrative privileges.

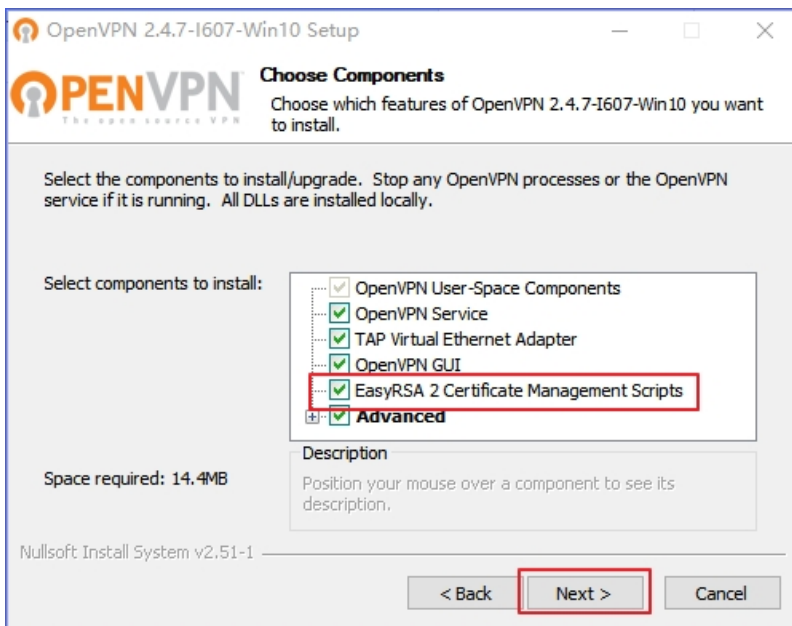
2. Double click the OpenVPN installer to start installation.
3. Click **Next**.



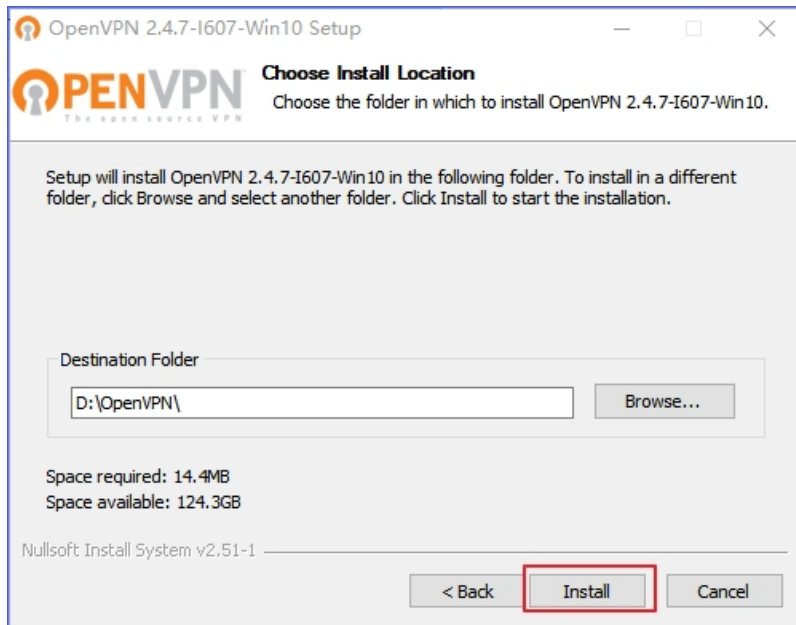
4. Click **I Agree**.



5. Check **EasyRSA2 Certificate Management Scripts**, click **Next**.



6. Choose the install location for OpenVPN, and click **Install** to start installation.  
In this example, we set the destination folder to `D:\OpenVPN`.



7. Click **Finish**.

## Generate OpenVPN Certificates and Keys

Generate OpenVPN certificates and keys for Yeastar S-Series VoIP PBX and clients.

**⚠ Important:** Commands below are executed in one Command Prompt window.

If you want to open a new Command Prompt window to execute commands (i.e. create certificates for new client):

- Each time you open a new Command Prompt window, you need to execute `vars` command first, then execute other commands.
- You don't need to execute `init-config` command, unless you want to edit `vars.bat` file again.

## Initialize the OpenVPN configuration

1. Press **Windows** Key and **R** key, type `cmd` and press **Enter** key.
2. Navigate to `%ProgramFiles%\OpenVPN\easy-rsa` (e.g. `D:\OpenVPN\easy-rsa`).

```
cd D:\OpenVPN\easy-rsa
```

3. Initialize the configurations.

```
init-config
```

4. Open the `vars.bat` file in a text editor.

```
notepad vars.bat
```

- a. Change the `KEY_SIZE` settings.

Usually, set the private key size to `1024` or `2048`.

```
set KEY_SIZE=2048
```

- b. Edit the following lines to display your address and company.

Later, when you make CA, certificates and keys, you will be asked to enter information that will be incorporated into your certificate request. If you change the default variables below, you don't have to enter these information each time.

```
set KEY_COUNTRY=CN
set KEY_PROVINCE=FJ
set KEY_CITY=Xiamen
set KEY_ORG=Yeostar
set KEY_EMAIL=support@yeostar.com
```

- c. Save the `vars.bat` file and back to Command Prompt window.

5. Run the following commands, make sure you are operating in a clean environment.

 **CAUTION:** This will remove all certificates and keys from the `keys` directory.

```
vars
clean-all
```


## Build Certificate Authority (CA)

1. Run the following command to create the `ca.crt` and `ca.key` file in the `keys` directory.

```
build-ca
```

2. When prompted to enter information that will be incorporated into your certificate request, enter your country, organization, etc.

Or press the **Enter** key to use the preset values appeared in brackets.

 **Important:** The only parameter that must be explicitly entered is the **Common Name**. In the example below, we set Common Name to `OpenVPN_CA`.

```
Country Name (2 letter code) [CN]:
State or Province Name (full name) [FJ]:
Locality Name (eg, city) [Xiamen]:
Organization Name (eg, company) [Yeostar]:
Organizational Unit Name (eg, section) [changeme]:admin
Common Name (eg, your name or your server's hostname)
[changeme]:OpenVPN_CA
Name [changeme]:Yeostar
Email Address [support@yeostar.com]:
```

## Build certificate and key for server

1. Run the following command to create the `{server_name}.crt` and `{server_name}.key` file in the `keys` directory.

In the command below, we create `server.crt` and `server.key`.

```
build-key-server server
```

2. When prompted to enter information that will be incorporated into your certificate request, enter your country, organization, etc.

Or press the **Enter** key to use the preset values appeared in brackets.

**⚠ Important:** The only parameter that must be explicitly entered is the **Common Name**. Enter the same name as `{server_name}`. In the example below, we set Common Name to `server`.

```
Country Name (2 letter code) [CN]:
State or Province Name (full name) [FJ]:
Locality Name (eg, city) [Xiamen]:
Organization Name (eg, company) [Yeastar]:
Organizational Unit Name (eg, section) [changeme]:admin
Common Name (eg, your name or your server's hostname) [changeme]:server
Name [changeme]:Yeastar
Email Address [support@yeastar.com]:
```

3. When prompted to sign the certificate and commit, type `y` and press the **Enter** key.

```
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y
```

## Build certificate and key for client

1. Run the following command to create the `{client_name}.crt` and `{client_name}.key` file in the `keys` directory.

In the command below, we create `client.crt` and `client.key`.

```
build-key client
```

2. When prompted to enter information that will be incorporated into your certificate request, enter your country, organization, etc.

Or press the **Enter** key to use the preset values appeared in brackets.

**⚠ Important:** The only parameter that must be explicitly entered is the **Common Name**. Enter the same name as `{client_name}`. In the example below, we set Common Name to `client`.

```
Country Name (2 letter code) [CN]:
State or Province Name (full name) [FJ]:
```



```

Locality Name (eg, city) [Xiamen]:
Organization Name (eg, company) [Yeastar]:
Organizational Unit Name (eg, section) [changeme]:admin
Common Name (eg, your name or your server's hostname) [changeme]:client
Name [changeme]:Yeastar
Email Address [support@yeastar.com]:

```

3. When prompted to sign the certificate and commit, type `y` and press the **Enter** key.

```

Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y

```

4. Repeat steps 1 to 3 to create Certificate & Key for each client respectively.

For each client, choose a name to identify, such as `Windows.crt` and `Windows.key` for Windows PC.

## Build a ta.key

Run the following command to create `ta.key` file in the `keys` directory.

```
OpenVPN --genkey --secret keys/ta.key
```


## Generate Diffie Hellman parameters

```
build-dh
```

## Check the Generated OpenVPN Certificates and Keys

After generating certificates and keys on the Command Window, you can find the certificates and keys in the `%ProgramFiles%\OpenVPN\easy-rsa` (e.g. `D:\OpenVPN\easy-rsa`).

**Table 1. Explanation of generated certificates and keys**

File	Needed by	Purpose
<code>ca.crt</code>	server and clients	Root CA certificate
<code>ca.key</code>	key signing machine only	Root CA key
<code>server.crt</code>	server only	Server Certificate
<code>server.key</code>	server only	Server Key
<code>client.crt</code>	client only	Client certificate
<code>client.key</code>	client only	Client key
<code>dh2048.pem</code>	server only	Diffie Hellman parameters.  <b>Note:</b> If the <code>KEY_SIZE</code> in the <code>vars.bat</code> file is set to <code>1024</code> , the DH PEM file name is <code>dh1024.pem</code> .
<code>ta.key</code>	server and clients	TLS authentication key.

**Table 1. Explanation of generated certificates and keys (continued)**

File	Needed by	Purpose
		 <b>Note:</b> If SSL/TLS is enabled on the OpenVPN server, you should upload the <code>ta.key</code> to the OpenVPN server and OpenVPN clients.

## OpenVPN Server Configurations

### Set up Yeastar S-Series VoIP PBX as an OpenVPN Server

Yeastar S Series PBX - VPN Server App helps you configure the PBX as an OpenVPN server. There is a Graphical User Interface for administrator to set up an OpenVPN server.

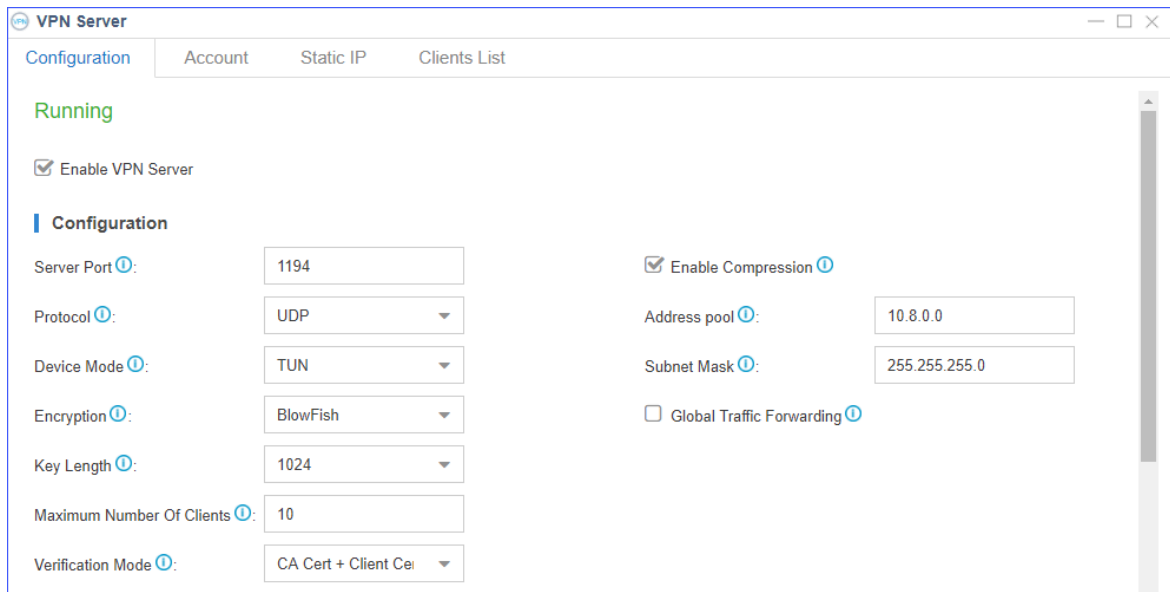
This topic shows you how to set up an OpenVPN server with OpenVPN authentication, and allocate a static IP address for each VPN client.

### Build up the OpenVPN Server

#### Step 1. Configure the OpenVPN server

1. Log in the PBX web interface, go to **VPN Server**, check the option **Enable VPN Server**.
2. Configure the OpenVPN server settings.

Here is an example of OpenVPN server settings:



**VPN Server**

Configuration | Account | Static IP | Clients List

**Running**

Enable VPN Server

**Configuration**

Server Port: 1194

Protocol: UDP

Device Mode: TUN

Encryption: BlowFish

Key Length: 1024

Maximum Number Of Clients: 10

Verification Mode: CA Cert + Client Ce




Enable Compression

Address pool: 10.8.0.0

Subnet Mask: 255.255.255.0

Global Traffic Forwarding

**Table 2. Description of OpenVPN settings**

Options	Description
Server Port	Specify which TCP/UDP port should OpenVPN listen on. The default port is 1194.
Protocol	Choose the protocol. <ul style="list-style-type: none"> <li>• TCP</li> <li>• UDP</li> </ul>
Device Mode	Choose the device mode: <ul style="list-style-type: none"> <li>• TUN: a TUN device is a virtual point-point IP link. If you choose TUN mode, you should allocate a static IP address for windows client because of TAP-WIN32 driver limitation.</li> <li>• TAP: a TAP device is a virtual Ethernet adapter. Android and iOS clients don't support TAP mode.</li> </ul> <p> <b>Note:</b> If Android, iOS, and other clients need to access to the PBX via OpenVPN network at the same time, we recommend that you use the TUN mode.</p>
Encryption	Choose encryption method. <ul style="list-style-type: none"> <li>• BlowFish</li> <li>• AES-128</li> <li>• AES-256</li> <li>• Triple-DES</li> </ul>
Key Length	Set the key length. <p> <b>Note:</b> The value must be the same as <code>KEY_SIZE</code> which were set in the <code>vars.bat</code> file.</p>
Maximum Number of Clients	Set the maximum number of clients that could connect to the OpenVPN server.
Verification Mode	Choose the Verification Mode of Client. <ul style="list-style-type: none"> <li>• CA Cert + Client Cert (recommend)</li> <li>• CA Cert + Client Cert + Account &amp; Password</li> <li>• CA Cert + Account &amp; Password</li> </ul> <p> <b>Note:</b> If you choose <b>CA Cert + Client Cert + Account &amp; Password</b> or <b>CA Cert + Account &amp; Password</b>, you need to <a href="#">configure OpenVPN username/password authentication</a> for each client later.</p>
Enable Compression	Whether to compress the VPN link.
Address pool	Define the address pool.
Subnet mask	Set the subnet mask.
Global Traffic Forwarding	If enabled, the client will configure a default gateway to the server after the connection is successful, and all the traffic will be forwarded by the server. (The OpenVPN server machine may


Options	Description
	<p>need to NAT or bridge the TUN/TAP interface to the internet in order for this to work properly).</p> <p>If disabled, only the communication data with the server will go through VPN tunnel, other traffic will go through the original forward routing.</p> <p>This feature may not take effect on some clients.</p>

### 3. Upload certificates and keys for server.

**Upload Cert**

CA Cert ⓘ:	<input type="text" value="Please select"/>	<input type="button" value="Browse"/>	<input type="button" value="Delete"/>	ca.crt
Public Server Cert ⓘ:	<input type="text" value="Please select"/>	<input type="button" value="Browse"/>	<input type="button" value="Delete"/>	server.crt
Private Server Key ⓘ:	<input type="text" value="Please select"/>	<input type="button" value="Browse"/>	<input type="button" value="Delete"/>	server.key
DH PEM ⓘ:	<input type="text" value="Please select"/>	<input type="button" value="Browse"/>	<input type="button" value="Delete"/>	dh2048.pem
<input checked="" type="checkbox"/> Enable SSL/TLS ⓘ:	<input type="text" value="Please select"/>	<input type="button" value="Browse"/>	<input type="button" value="Delete"/>	ta.key

**Table 3.**

Options	CA & Key
CA Cert	Upload ca.crt.
Public Server Cert	Upload the OpenVPN server certificate server.crt.
Private Server Key	Upload the OpenVPN server key server.key.
DH PEM	Upload the Diffie Hellman file dh2048.pem.   <b>Note:</b> If the KEY_SIZE is 1024, then upload the file dh1024.pem.
Enable SSL/TLS	Enable SSL/TLS on the VPN server, and then upload ta.key file.

### 4. Click **Save** and **Apply**.

## Step 2. Check the VPN server status

- Go to **Resource Monitor > Network > VPN Server**, check the OpenVPN status and virtual IP address.

**VPN Server**

Status: Running

Virtual IP Address: 10.8.0.1

### Step 3. Forward VPN server port

To ensure that VPN clients can access the PBX, you should forward VPN server port on your router. The default VPN server port is 1194.

Note down the public IP address of PBX and the external VPN server port. Later, you need to enter the remote IP address and remote server port in the client configuration file.

### Allocate a static IP address for a VPN client

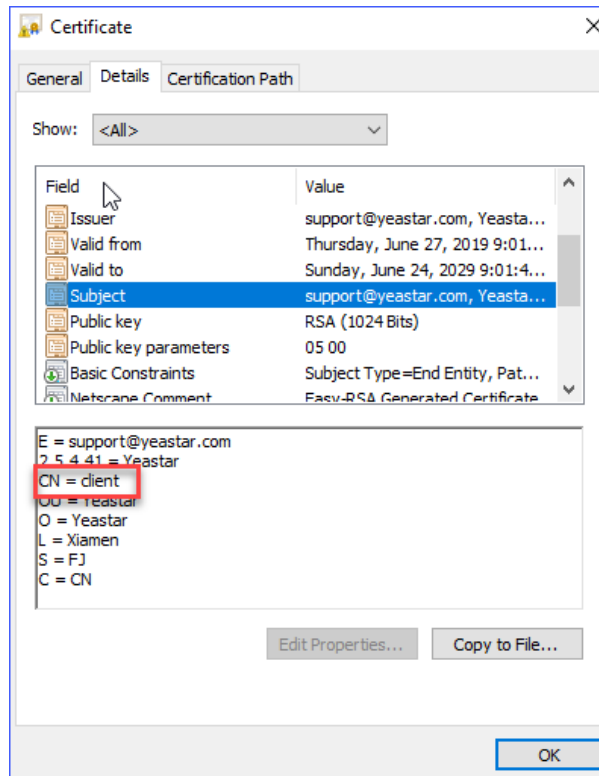
By default, Yeastar VPN Server dynamically assigns an IP address from its IP address pool to the VPN clients. To take more control of the client activities, you can assign a static IP address for the VPN clients. This article shows how to assign a fixed IP address to the VPN clients.

Allocation for static IP addresses is supported on Yeastar S-Series VoIP PBX version 30.4.0.25 or later.

### Allocate a static IP address for a client in TUN device mode

1. Log in the PBX web interface, go to **VPN Server > Static IP**, click **Add**.
2. Specify a client which you want to assign a static IP address to.
  - If you use [CA Cert + Client Cert](#) verification mode, enter the Common Name of this client in the **CN** filed.

You can double click the client certificate `client.crt`, go to **Details > Subject** and find **CN**.



- If you use [username/password authentication](#), and you have created an account for the specified client, select a client account from **Account Name** field.
3. Assign the IP address, subnet mask and TUN remote IP address to this client.

**i Tip:** The virtual client IP address and TUN remote IP address must be taken from successive /30 subnets in order to be compatible with Windows clients and the TAP-Windows driver. Specifically, the last octet in the IP address of the virtual client IP address and TUN remote IP address must be taken from the following:

```
[ 5, 6] [ 9, 10] [ 13, 14] [ 17, 18] [ 21, 22] [ 25, 26] [ 29, 30]
[ 33, 34] [ 37, 38]
[ 41, 42] [ 45, 46] [ 49, 50] [ 53, 54] [ 57, 58] [ 61, 62] [ 65, 66]
[ 69, 70] [ 73, 74]
[ 77, 78] [ 81, 82] [ 85, 86] [ 89, 90] [ 93, 94] [ 97, 98] [101,102]
[105,106] [109,110]
[113,114] [117,118] [121,122] [125,126] [129,130] [133,134] [137,138]
[141,142] [145,146]
[149,150] [153,154] [157,158] [161,162] [165,166] [169,170] [173,174]
[177,178] [181,182]
[185,186] [189,190] [193,194] [197,198] [201,202] [205,206] [209,210]
[213,214] [217,218]
[221,222] [225,226] [229,230] [233,234] [237,238] [241,242] [245,246]
[249,250] [253,254]
```

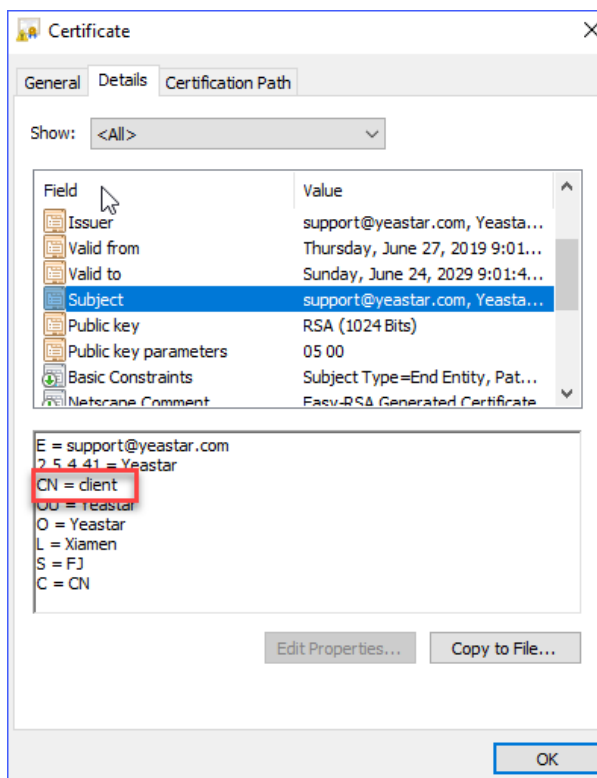
In this example, the IP address is set to *10.8.0.5*, then the TUN remote IP address must be *10.8.0.6*.

4. Click **Save** and **Apply**.

## Allocate a static IP address for a client in TAP mode

1. Log in the PBX web interface, go to **VPN Server > Static IP**, click **Add**.
2. Specify a client which you want to assign a static IP address to.
  - If you use **CA Cert + Client Cert** verification mode, enter the Common Name of this client in the **CN** filed.

You can double click the client certificate `client.crt`, go to **Details > Subject** and find **CN**.



- If you use **username/password authentication**, and you have created an account for the specified client, select a client account from **Account Name** field.

3. Assign the IP address to this client in the **IP Address** field.

**Note:** The IP address should be in the address pool of the VPN server. The allowed IP range is from XXX.XXX.XXX.3 to XXX.XXX.XXX.253.

4. Enter the subnet mask in the **Subnet Mask** field.

5. Click **Save** and **Apply**.

## OpenVPN Username/Password Authentication

OpenVPN needs to verify the authenticity of the connecting clients to ensure security. OpenVPN Authentication allows the OpenVPN server to securely obtain a username and password from a connecting client, and to use that information as a basis for authenticating the client.

This topic shows you how to configure username/password authentication on the OpenVPN server and clients.

### Set Username/Password Authentication on OpenVPN server

1. Log in the PBX web interface, go to **VPN Server**, set the **Verification Mode** to `CA Cert + Client Cert + Account & Password Of CA Cert + Account & Password`.
2. Click **Save**.

### Set Username/Password for each client on OpenVPN server

1. Click **Account** tab, and then click **Add Account** to set the username and password for VPN client.
2. Enter the client's name and assign an password for the client.



**Add Account**

Account: client

Password: clientpass

Remarks:

Save Cancel

3. Click **Save**.

Repeat above steps to set username/password for each client.

	Account	Password	Remarks	Edit	Delete
<input type="checkbox"/>	Android	Androidpass			
<input type="checkbox"/>	S300	S300pass			
<input type="checkbox"/>	Yealink	Yealinkpass			
<input type="checkbox"/>	client	clientpass			
<input type="checkbox"/>	iPhone	iPhonepass			
<input type="checkbox"/>	windows	password			

## Create an authentication file for each client

1. Create a new text document.
2. Enter the username and password according to the account/password settings on VPN server.

Line1: Enter the username.

Line2: Enter the password.

```
1 client
2 clientpass
```

3. Save the file, and rename the file as `passfile` without ".txt" extension.



**Note:** For yealink IP phone, you need to rename this file to `pwd` without ".txt" extension.

- Specify `passfile` to identify where to obtain the account and password in client configuration file.

```
auth-user-pass passfile
```

- Import the `passfile` file to client.

## OpenVPN Clients Configurations

### Connect Yeastar S-Series VoIP PBX to another Yeastar S-Series VoIP PBX

This topic shows you how to set up Yeastar S-Series VoIP PBX as an OpenVPN client, and to connect to Yeastar S-Series VoIP PBX via OpenVPN network.

- Log in the S300 PBX web interface, go to **Settings > System > Network > OpenVPN**, check **Enable OpenVPN**.
- Set the **Type** to **Manual Configurations**, and configure the following settings according to the VPN server configurations.

**Settings**

Basic Settings | **OpenVPN** | DDNS Settings | Static Routes | Cellular Network | ICMP Detec

Enable OpenVPN

Type: Manual Configuration

Server Address: 110.80.36.162 | Server Port: 7086

Protocol: UDP | Device Mode: TUN

Username: S300 | Password: \*\*\*\*\*

Encryption: AES-256 |  Compression

Proxy Server: | Proxy Port:

CA Cert: Please select | Browse | Delete | ca.crt

Cert: Please select | Browse | Delete | client.crt

Key: Please select | Browse | Delete | client.key

TLS Authentication

TA Key: Please select | Browse | Delete | ta.key

Save | Cancel

**Table 4. Description of OpenVPN settings**

Options	Description
Server Address	Enter the IP address of the OpenVPN server.
Server Port	Enter the OpenVPN server port.
Protocol	Select the same protocol as the OpenVPN server.
Device Mode	Select the same mode as the OpenVPN server.
Encryption	Select the same type as the OpenVPN server.
Username	If the <a href="#">OpenVPN username/password authentication</a> is required on server, enter user name.
Password	If the <a href="#">OpenVPN username/password authentication</a> is required on server, enter password.
Compression	Compression on the VPN link. The client and server must be the same setting.

3. Upload certificates and keys for client.

CA Cert ⓘ:    ca.crt

Cert ⓘ:    s300.crt

Key ⓘ:    s300.key

TLS Authentication ⓘ

TA Key ⓘ:    ta.key

**Table 5.**

Options	CA & Key
CA Cert	Upload ca.crt.
Public Server Cert	Upload the client certificate s300.crt.
Private Server Key	Upload the client key s300.key.
TLS Authentication	If you enable SSL/TLS on the VPN server, enable this option.
TA Key	If you enable TLS Authentication, upload ta.key file.

4. Click **Save** and **Apply**.

5. Go to **Settings > Resource Monitor > Network**, check the VPN client status and IP address.

VPN Client	
Status:	Running
P.t.P:	10.8.0.4
IP Address:	10.8.0.3
Subnet Mask:	255.255.255.255
Preferred DNS Server:	114.114.114.114
Alternative DNS Server:	

## Connect to Yeastar S-Series VoIP PBX with Windows

This topic shows you how to configure a client file for Windows PC, and to connect to Yeastar S-Series VoIP PBX via OpenVPN network.

### Create a Client File for Windows Client

You can create a client file with `.ovpn` extension with a text editor (e.g. notepad++), or [download a client.ovpn sample file](#).

 **Note:** The line beginning with “;” is considered to disable the corresponding option.

1. Open the `client.ovpn` file with a text editor.
2. Edit the following options according to the VPN server settings on your PBX.

 **Note:** The client and server must use the same settings.

- a. Specify the hostname/IP and port of VPN server.

In this example, we have forwarded the VPN server 10.8.0.1 1194 to 110.80.36.162 7086.

```
remote 110.80.36.162 7086
```

- b. Set the protocol to UDP or TCP.

In this example, UDP is enabled, and TCP is disabled.

```
proto udp
;proto tcp
```

- c. Set the device mode to TAP or TUN.

In this example, TAP is enabled, and TUN is disabled.

```
dev tap
```

```
;dev tun
```

- d. Set the cryptographic cipher.

**Table 6.**

Cryptographic cipher on server	Cryptographic cipher on client
BlowFish	cipher BF-CBC
AES-128	cipher AES-128-CBC
AES-256	cipher AES-256-CBC
Triple-DES	cipher DES-EDE3-CBC

In this example, AES-256 is set on server, then enable AES-256-CBC.

```
;cipher BF-CBC
;cipher AES-128-CBC
cipher AES-256-CBC
;cipher DES-EDE3-CBC
```

- e. If **Compression** is enabled on server, you need to enable compression on the VPN client.

```
comp-lzo
```

- f. If [Username/Password Authentication](#) is used on server, you need to specify the passfile file.

```
auth-user-pass passfile
```

- g. If **SSL/TLS** and a `ta.key` is used on the server, you need to specify the TLS Authentication & TA Key.

```
tls-auth ta.key 1
```

- h. Specify the CA certificate file used on server.

```
ca ca.crt
```

3. Specify the Windows client certificate and key file.

In this example, `Windows.crt` and `Windows.key` is specified.

```
cert Windows.crt
key Windows.key
```

4. Edit other options according to your need.

```
persist-key
persist-tun
verb 3
resolv-retry infinite
remote-cert-tls server
nobind
;dev-node MyTap
;remote-random
```

```

;http-proxy-retry
;http-proxy [proxy server] [proxy port #]
;mute-replay-warnings
;mute 20

```

### 5. Save the client file.

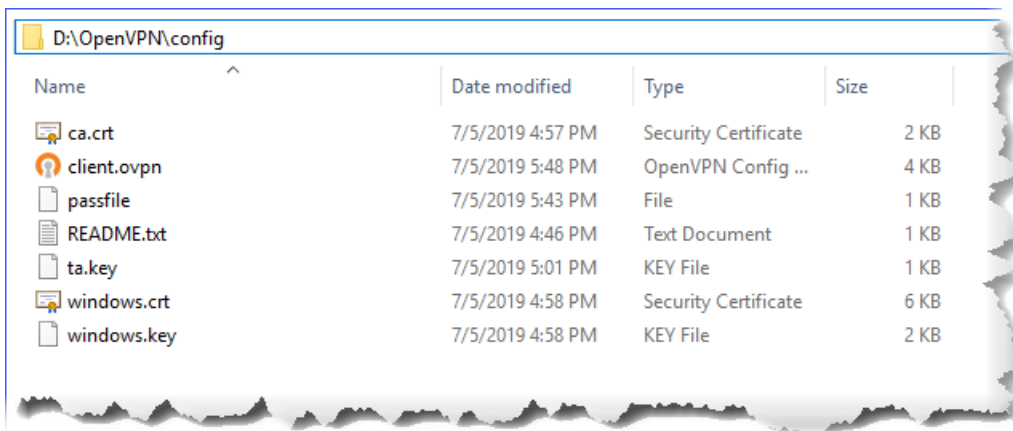
You can rename `client.ovpn` to identify, such as: `Windows.ovpn`.

## Connect Windows PC to Yeastar S-Series VoIP PBX via OpenVPN

Before connecting your Windows PC to Yeastar S-Series VoIP PBX, you need to [download and install OpenVPN](#) on your Window PC.

The OpenVPN GUI  appears on the desktop of the PC, and you can use the OpenVPN GUI to connect to the Yeastar S-Series VoIP PBX later.


### 1. Copy the following files to `config` folder (e.g. `D:\OpenVPN\config`).



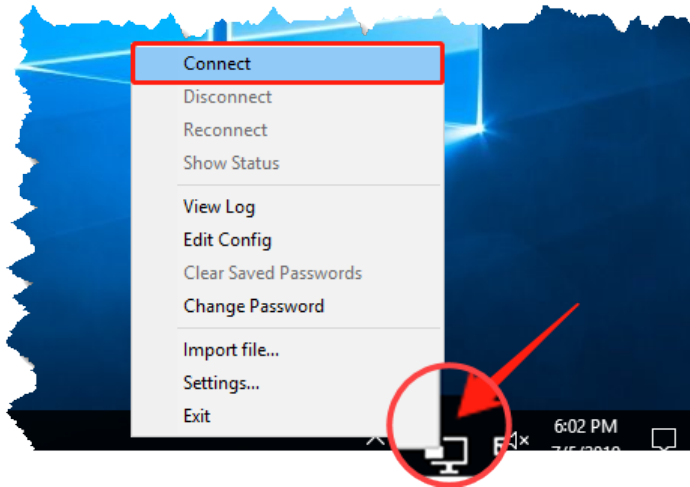
**Table 7. Files for Windows client**

File	Note
<code>ca.crt</code>	Root Certificate Authority
<code>Windows.crt</code>	a certificate file for Windows client
<code>Windows.key</code>	a key file for Windows client
<code>Windows.ovpn</code>	an OpenVPN connection file
<code>passfile</code>	Required for <a href="#">OpenVPN username/password authentication</a>
<code>ta.key</code>	Required for client when <b>SSL/TLS</b> is enabled on the OpenVPN server

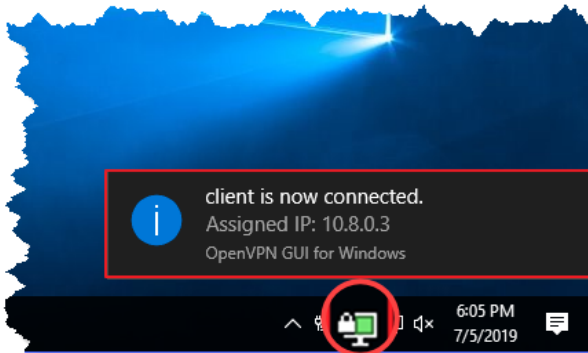
### 2. Connect to the OpenVPN server.

- a. Right click the OpenVPN GUI  on the desktop, and run as administrator.

- b. Find the OpenVPN GUI in the bottom right corner, right click the icon, and click **Connect**.



- c. If the client is connected to the PBX server, you will see the status shows as below.



**Troubleshooting:** If you are prompted "The local and remote VPN endpoints must exist within the same 255.255.255.252 subnet.", you should [allocate a static IP address](#) for Windows client if using TUN device mode.

## Connect to Yeastar S-Series VoIP PBX with iOS Device

This topic shows you how to configure a client file for iOS, and to connect to Yeastar S-Series VoIP PBX via OpenVPN network.

## Create a Configuration File for iOS Client

You can create a client file with `.ovpn` extension with a text editor (e.g. notepad++), or [download a client.ovpn sample file](#).

**Note:** The line beginning with “;” is considered to disable the corresponding option.

1. Open the `client.ovpn` file with a text editor.
2. Edit the following options according to the VPN server settings on your PBX.

 **Note:** The client and server must use the same settings.

- a. Specify the hostname/IP and port of VPN server.

In this example, we have forwarded the VPN server 10.8.0.1 1194 to 110.80.36.162 7086.

```
remote 110.80.36.162 7086
```

- b. Set the protocol to UDP or TCP.

In this example, UDP is enabled, and TCP is disabled.

```
proto udp
;proto tcp
```

- c. Set the device mode to TUN.

```
dev tun
```

- d. Set the cryptographic cipher.

**Table 8.**

Cryptographic cipher on server	Cryptographic cipher on client
BlowFish	cipher BF-CBC
AES-128	cipher AES-128-CBC
AES-256	cipher AES-256-CBC
Triple-DES	cipher DES-EDE3-CBC

In this example, AES-256 is set on server, then enable AES-256-CBC.

```
;cipher BF-CBC
;cipher AES-128-CBC
cipher AES-256-CBC
;cipher DES-EDE3-CBC
```

- e. If **Compression** is enabled on server, you need to enable compression on the VPN client.

```
comp-lzo
```

- f. If [Username/Password Authentication](#) is used on server, you need to specify the `passfile` file.

```
auth-user-pass passfile
```

- g. If **SSL/TLS** and a `ta.key` is used on the server, you need to specify the TLS Authentication & TA Key.



```
tls-auth ta.key 1
```

h. Specify the CA certificate file used on server.

```
ca ca.crt
```

3. Specify the iOS client certificate and key file.

In this example, iOS.crt and iOS.key is specified.

```
cert iOS.crt
key iOS.key
```

4. Edit other options according to your need.

```
persist-key
persist-tun
verb 3
resolv-retry infinite
remote-cert-tls server
nobind
;dev-node MyTap
;remote-random
;http-proxy-retry
;http-proxy [proxy server] [proxy port #]
;mute-replay-warnings
;mute 20
```

5. Save the client file.

You can rename `client.ovpn` to identify, such as: `iOS.ovpn`.

## Connect iOS Phone to Yeastar S-Series VoIP PBX via OpenVPN

Before connecting your iOS phone to Yeastar S-Series VoIP PBX, you need to install the OpenVPN on your phone.

 **Note:** Make sure that the **TUN** device mode is set on VPN server.

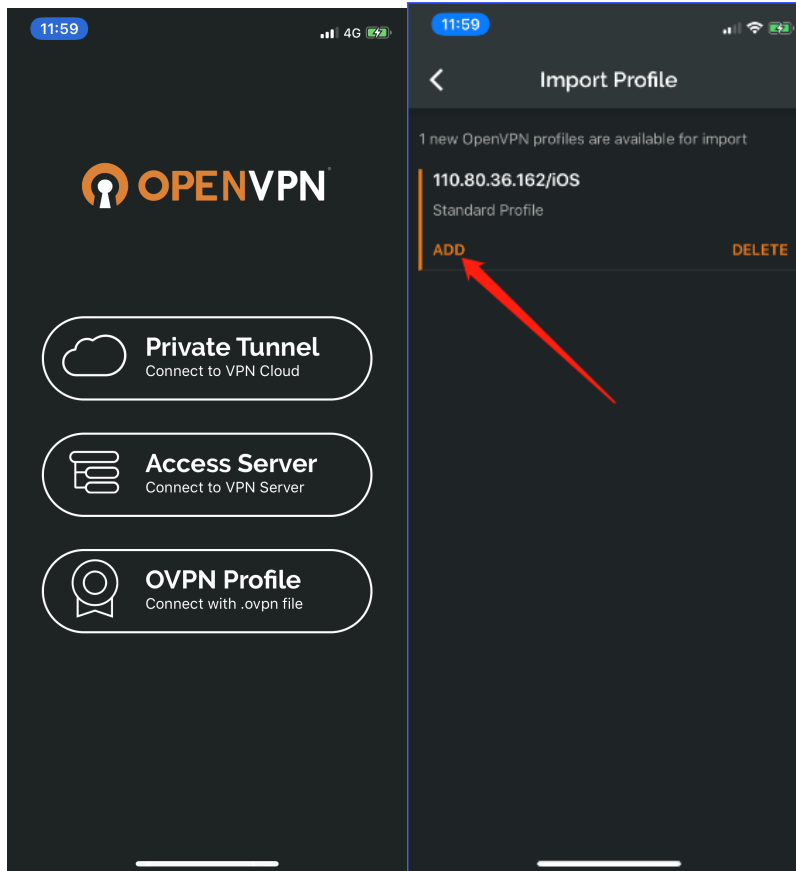
1. Connect your phone to PC, select your device on iTunes, go to OpenVPN under the **Apps** tab, and drop the OpenVPN connection files into the file sharing window.



**Table 9. Files for iOS client**

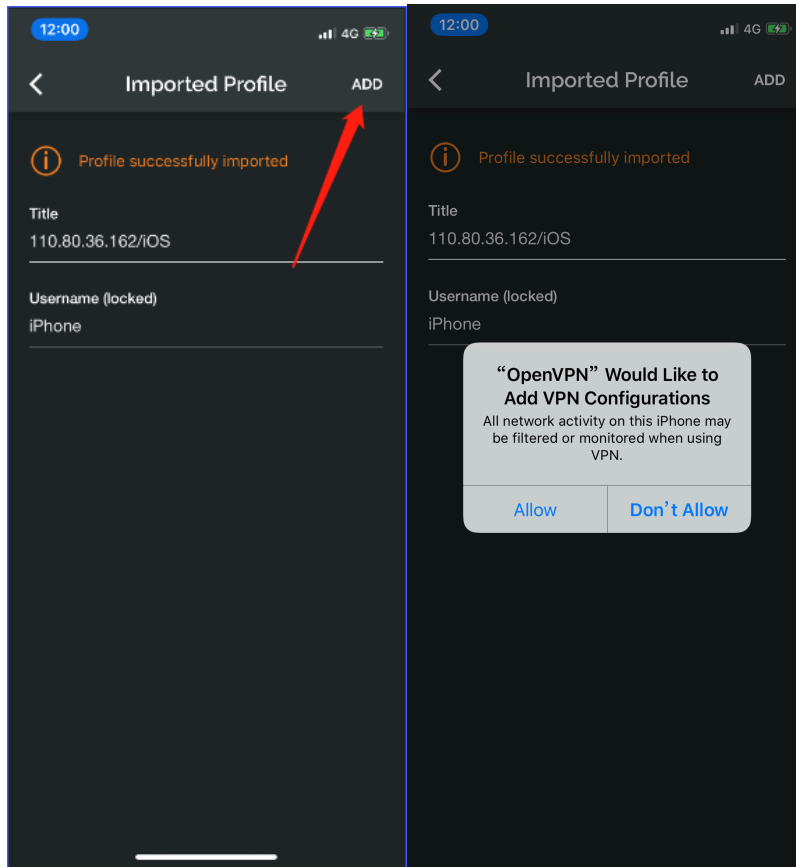
File	Note
ca.crt	Root Certificate Authority
iOS.crt	a certificate file for iOS client
iOS.key	a key file for iOS client
iOS.ovpn	an OpenVPN connection file
passfile	Required for <a href="#">OpenVPN username/password authentication</a> .
ta.key	Required for client when <b>SSL/TLS</b> is enabled on the OpenVPN server.

2. Open the OpenVPN app on your iPhone.
3. Tap **OVPN Profile**, and then tap the **ADD** under the file you want to add.



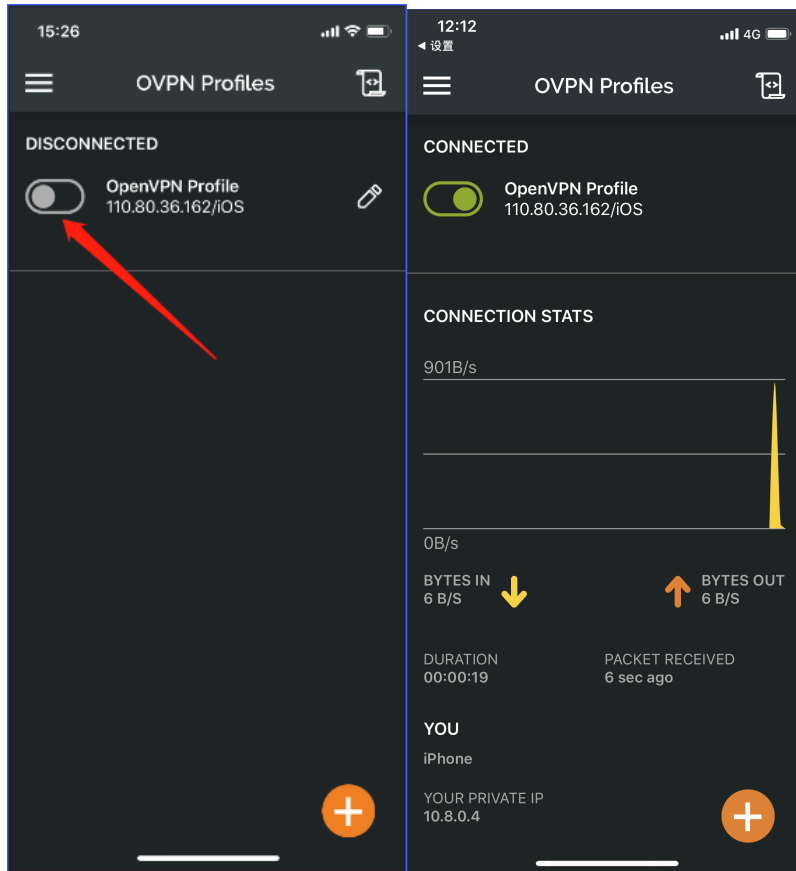
4. Tap the **ADD**, and then tap **Allow** to import the OpenVPN connection file.

You may need to confirm VPN Configuration by using Touch ID or another security method set on your iOS device.



5. Tap on the gray slider to start the connection.

If the connection has been established, the slider will become green and the state will change to **CONNECTED**.



**Troubleshooting:** If you are prompted "tun\_prop\_error: if config address are not is the same /30 subnet (toplogy net30).", you should [allocate a static IP address](#) for iOS client.

## Connect to Yeastar S-Series VoIP PBX with Android Device

This topic shows you how to configure a client file for Android, and to connect to Yeastar S-Series VoIP PBX via OpenVPN network.

## Create a Client File for Android Client

You can create a client file with `.ovpn` extension with a text editor (e.g. notepad++), or [download a client.ovpn sample file](#).

**Note:** The line beginning with “;” is considered to disable the corresponding option.

1. Open the `client.ovpn` file with a text editor.
2. Edit the following options according to the VPN server settings on your PBX.

**Note:** The client and server must use the same settings.

- a. Specify the hostname/IP and port of VPN server.

In this example, we have forwarded the VPN server 10.8.0.1 1194 to 110.80.36.162 7086.

```
remote 110.80.36.162 7086
```

- b. Set the protocol to UDP or TCP.

In this example, UDP is enabled, and TCP is disabled.

```
proto udp
;proto tcp
```

- c. Set the device mode to TUN.

```
dev tun
```

- d. Set the cryptographic cipher.

**Table 10.**

Cryptographic cipher on server	Cryptographic cipher on client
BlowFish	cipher BF-CBC
AES-128	cipher AES-128-CBC
AES-256	cipher AES-256-CBC
Triple-DES	cipher DES-EDE3-CBC

In this example, AES-256 is set on server, then enable AES-256-CBC.

```
;cipher BF-CBC
;cipher AES-128-CBC
cipher AES-256-CBC
;cipher DES-EDE3-CBC
```

- e. If **Compression** is enabled on server, you need to enable compression on the VPN client.

```
comp-lzo
```

- f. If [Username/Password Authentication](#) is used on server, you need to specify the `passfile` file.

```
auth-user-pass passfile
```

- g. If **SSL/TLS** and a `ta.key` is used on the server, you need to specify the TLS Authentication & TA Key.

```
tls-auth ta.key 1
```

- h. Specify the CA certificate file used on server.

```
ca ca.crt
```

### 3. Specify the Android client certificate and key file.

In this example, `Android.crt` and `Android.key` is specified.

```
cert Android.crt
key Android.key
```

### 4. Edit other options according to your need.

```
persist-key
persist-tun
verb 3
resolv-retry infinite
remote-cert-tls server
nobind
;dev-node MyTap
;remote-random
;http-proxy-retry
;http-proxy [proxy server] [proxy port #]
;mute-replay-warnings
;mute 20
```

### 5. Save the client file.

You can rename `client.ovpn` to identify, such as: `Android.ovpn`.

## Connect Android Phone to Yeastar S-Series VoIP PBX via OpenVPN

[OpenVPN for Android](#) is an open source client compatible with all versions of Android 4.x or later. Before connecting your Android phone to Yeastar S-Series VoIP PBX, you need to install the OpenVPN on your phone.

 **Note:** Make sure that the **TUN** device mode is used on VPN server.

### 1. Put the following files to your Android phone.

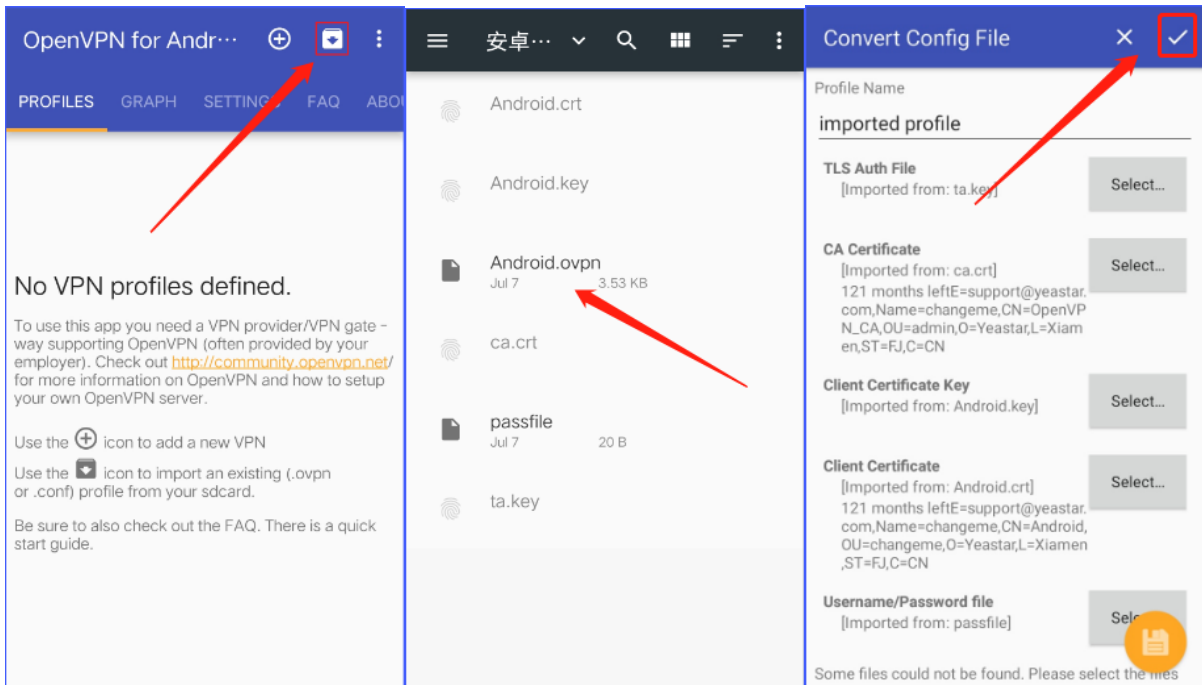
**Table 11. Files for Android client**

File	Note
<code>ca.crt</code>	Root Certificate Authority
<code>Android.crt</code>	a certificate file for Android client
<code>Android.key</code>	a key file for Android client
<code>Android.ovpn</code>	an OpenVPN connection file
<code>passfile</code>	Required for <a href="#">OpenVPN username/password authentication</a>
<code>ta.key</code>	Required for client when <b>SSL/TLS</b> is enabled on the OpenVPN server

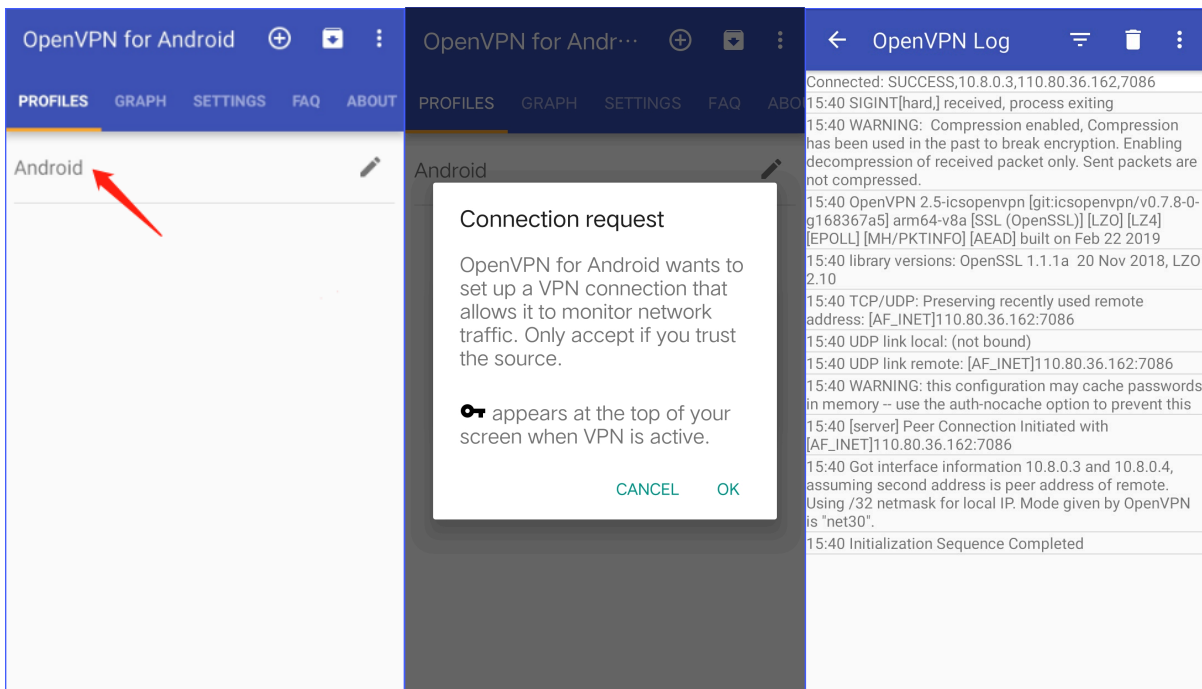
### 2. Open the OpenVPN app on your Android phone.

### 3. Tap the icon and navigate to the folder location where you copied the files.

4. Tap the OpenVPN connection file end with `.ovpn`, and then tap  to confirm the imported files.

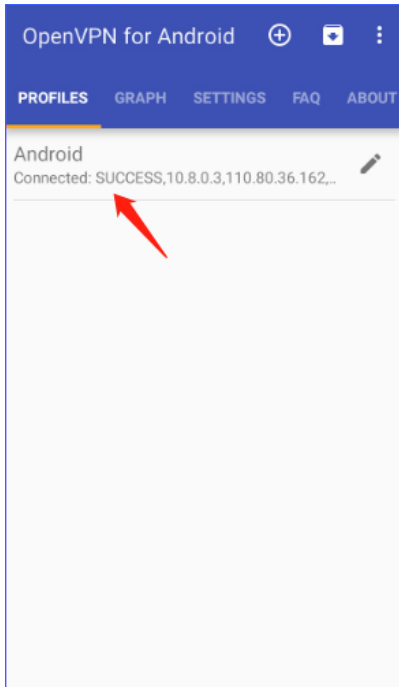


5. Tap the server name **Android**, and tap **OK** to accept the connection.  
The OpenVPN log shows you the connection process.



If the client is connected to the PBX server, you can see the status shown as below.





## Connect Yealink Phones to Yeastar S-Series VoIP PBX

This topic shows you how to configure a client file for Yealink, and to connect to Yeastar S-Series VoIP PBX via OpenVPN network

### Create a Configuration File for Yealink Phone

You can create a client file named "vpn.cnf" with a text editor (e.g. notepad++), or [download a client.ovpn sample file](#).

 **Note:** The line beginning with “;” is considered to disable the corresponding option.

1. Open the `vpn.cnf` file with a text editor.
2. Edit the following options according to the VPN server settings on your PBX.

 **Note:** The client and server must use the same settings.

- a. Specify the hostname/IP and port of VPN server.

In this example, we have forwarded the VPN server `10.8.0.1 1194` to `110.80.36.162 7086`.

```
remote 110.80.36.162 7086
```

- b. Set the protocol to **UDP** or **TCP**.

In this example, UDP is enabled while TCP is disabled.

```
proto udp
;proto tcp
```

- c. Set the device mode to **TAP** or **TUN**.

In this example, TAP is enabled while TUN is disabled.

```
dev tap
;dev tun
```

- d. Set the cryptographic cipher.

**Table 12.**

Cryptographic cipher on server	Cryptographic cipher on client
BlowFish	cipher BF-CBC
AES-128	cipher AES-128-CBC
AES-256	cipher AES-256-CBC
Triple-DES	cipher DES-EDE3-CBC

In this example, AES-256 is set on server, then you should enable AES-256-CBC on client.

```
;cipher BF-CBC
;cipher AES-128-CBC
cipher AES-256-CBC
;cipher DES-EDE3-CBC
```

- e. If **Compression** is enabled on server, you need to enable compression on the VPN client.

```
comp-lzo
```

- f. If [Username/Password Authentication](#) is used on server, you need to specify the `pwd` file.

```
auth-user-pass /config/openvpn/pwd
```

- g. If **SSL/TLS** and a `ta.key` is used on the server, you need to specify the TLS Authentication & TA Key.

```
tls-auth ta.key 1
```

- h. Specify the CA certificate file used on server.

```
ca /config/openvpn/keys/ca.crt
```

3. Specify the Yealink phone client certificate and key file.

In this example, `Yealink.crt` and `Yealink.key` is specified.

```
cert /config/openvpn/keys/Yealink.crt
key /config/openvpn/keys/Yealink.key
```

#### 4. Edit other options according to your need.

```

persist-key
persist-tun
verb 3
resolv-retry infinite
remote-cert-tls server
nobind
;dev-node MyTap
;remote-random
;http-proxy-retry
;http-proxy [proxy server] [proxy port #]
;mute-replay-warnings
;mute 20

```

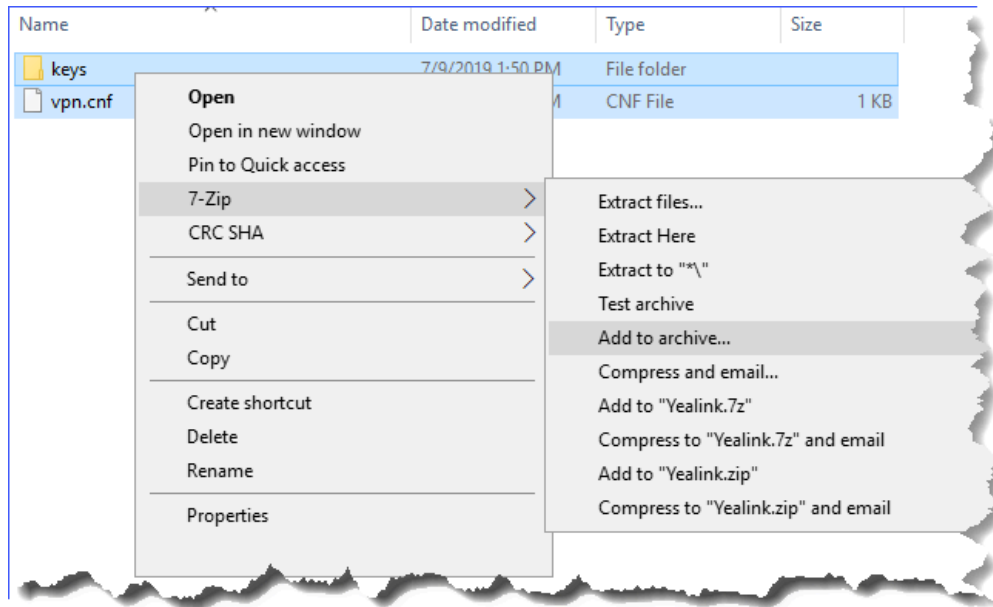
#### 5. Save the client file.

## Connect Yealink Phone to Yeastar S-Series VoIP PBX via OpenVPN

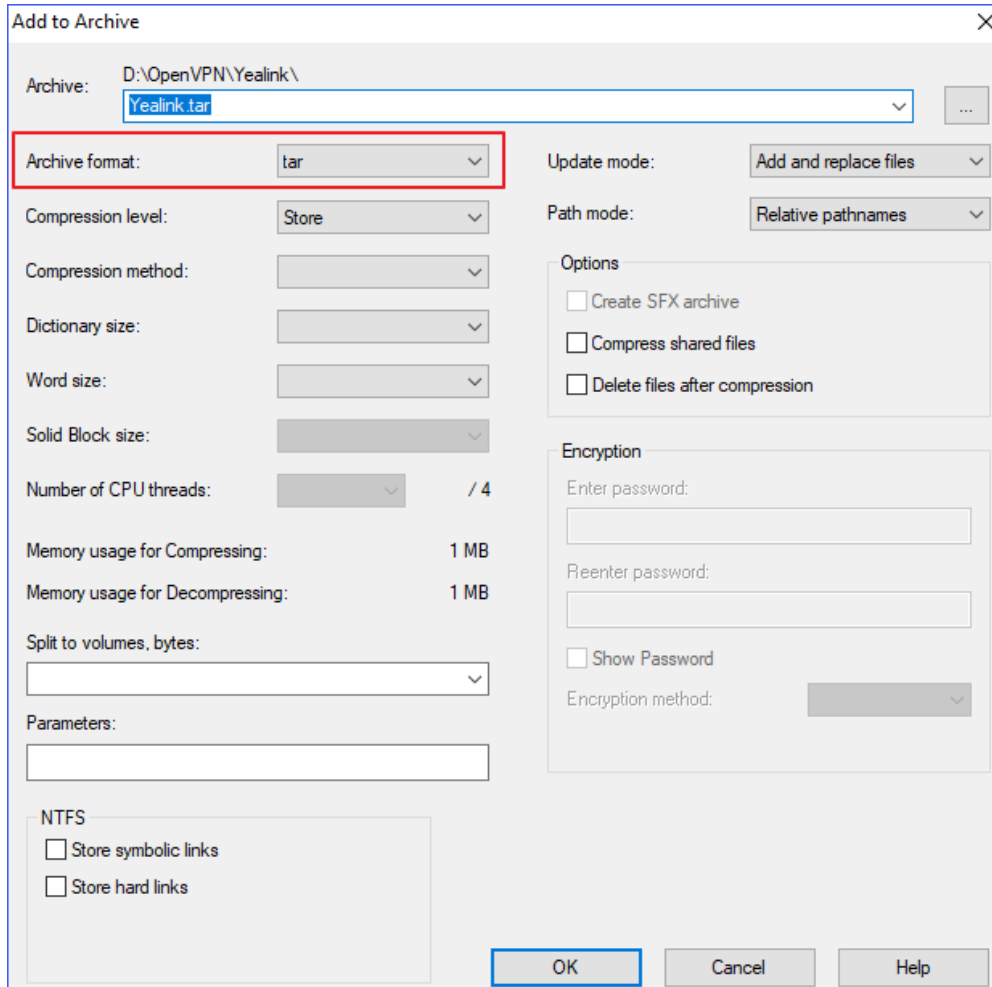
1. Put all the certifications and keys within the folder `keys`, and zip the `keys` folder and other files to a `.tar` file using the software **7z**.

**Table 13. Files for Yealink phone**

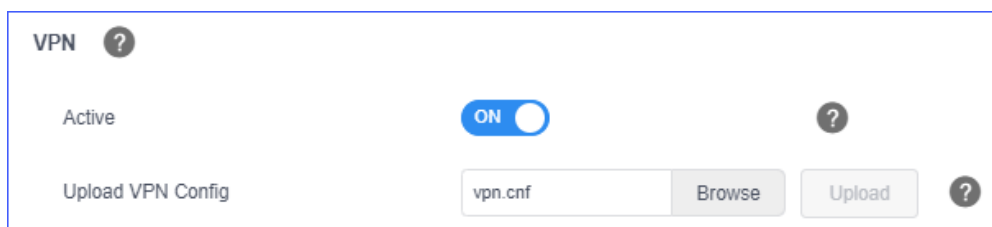
Folder	File	Note
keys	ca.crt	Root Certificate Authority
	Yealink.crt	a certificate file for Yealink IP phone client
	Yealink.key	a key file for Yealink IP phone client
	ta.key	Required for client when <b>SSL/TLS</b> is enabled on the OpenVPN server
/	vpn.cnf	an OpenVPN connection file
/	pwd	Required for <a href="#">OpenVPN username/password authentication</a>



In this example, we name the .tar file as Yealink.tar.



2. Log in the phone web interface, go to **Network > Advanced > VPN**.
3. Upload the `Yealink.tar` file.

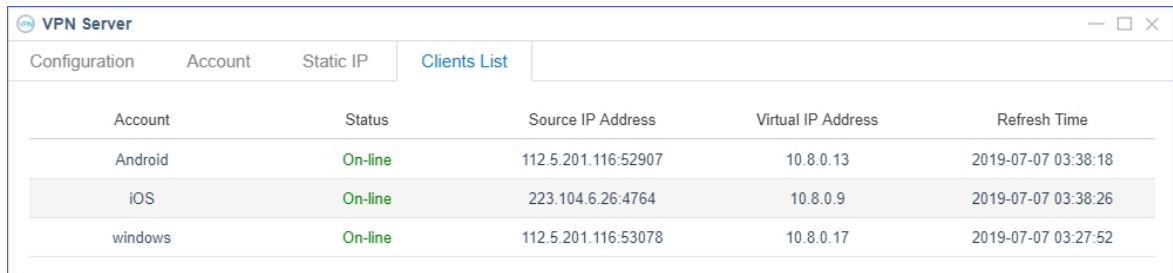


Yealink phone will reboot itself to apply changes. After phone rebooting, you can check the VPN connection status by checking a VPN icon shown on the Yealink LCD screen.

## Check the Client Status

You can check the connected clients and the virtual IP address assigned to the clients.

1. Log in the PBX web interface, go to **VPN Server > Clients List**.



Account	Status	Source IP Address	Virtual IP Address	Refresh Time
Android	On-line	112.5.201.116:52907	10.8.0.13	2019-07-07 03:38:18
iOS	On-line	223.104.6.26:4764	10.8.0.9	2019-07-07 03:38:26
windows	On-line	112.5.201.116:53078	10.8.0.17	2019-07-07 03:27:52