Grandstream Networks, Inc.

OpenVPN®

Client-to-Site Configuration Guide

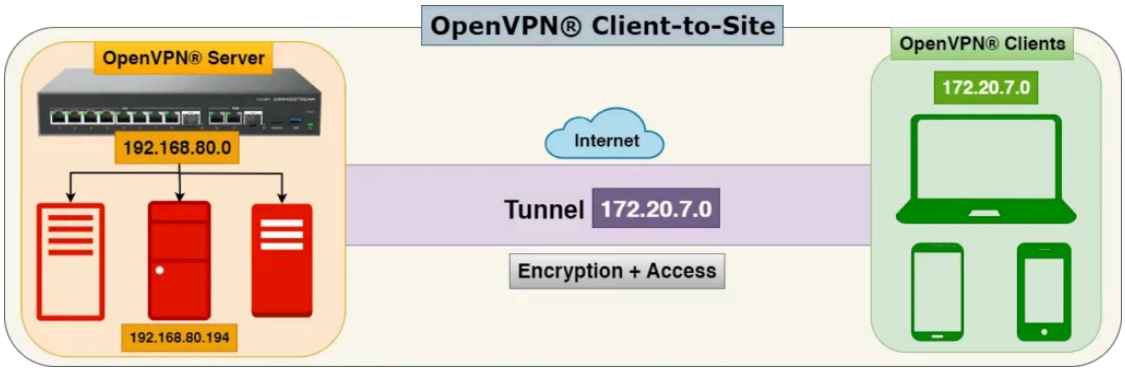
Overview

This guide explains how to set up **OpenVPN® Client-to-Site VPN** on a Grandstream router, so remote users can securely access your local network (LAN) from outside the office. In this deployment, the Grandstream router operates as the **OpenVPN® Server**, while a remote device (PC, laptop, or mobile device) connects as an **OpenVPN® Client**.

After the VPN connection is established, the remote client is securely tunneled into the LAN and can reach internal resources as if it were on-site (for example, local servers, web interfaces, and other LAN services), depending on your network permissions and configuration.

This guide covers the following high-level workflow:

1. Configure the router as an OpenVPN® server.
2. Create a remote user and export the client **.ovpn** profile.
3. Import the **.ovpn** profile on the client device and verify connectivity.



OpenVPN® Client to Site Overview

Supported Devices

This guide applies to Grandstream routers and convergence devices that support OpenVPN® in Client-to-Site mode. The device on the local network acts as the OpenVPN® server, while remote users connect using an OpenVPN® client application on a computer or mobile device.

Device Series	Models
GWN700x Series Routers	GWN7001, GWN7002, GWN7003
GWN70x2 Series Routers	GWN7062, GWN7052, GWN7052F
GWN7062E(T) Series Routers	GWN7062E, GWN7062ET
GCC6010 Series	GCC6010, GCC6010W, GCC6011
GCC6020 Series	GCC6020, GCC6021

Supported Devices

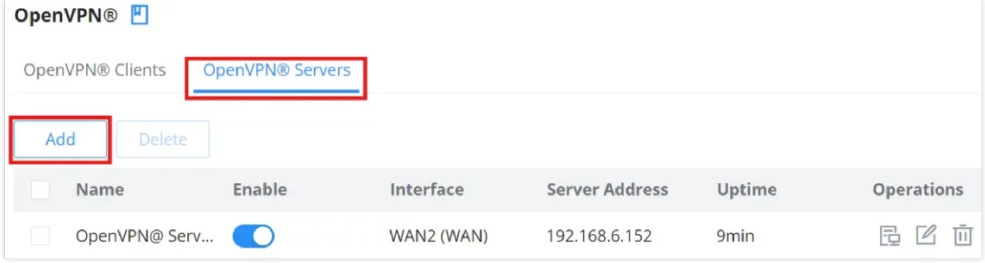
A – Router Side (OpenVPN® Server Configuration)

In this section, you will configure the router as an **OpenVPN® server**, then create a **remote user** and **download the `.ovpn` profile** that will be imported on the client side.

1) Add the OpenVPN® Server

Step 1: Open the OpenVPN® Servers page

Go to **VPN** → **OpenVPN®**, select the **OpenVPN® Servers** tab, then click **Add**.

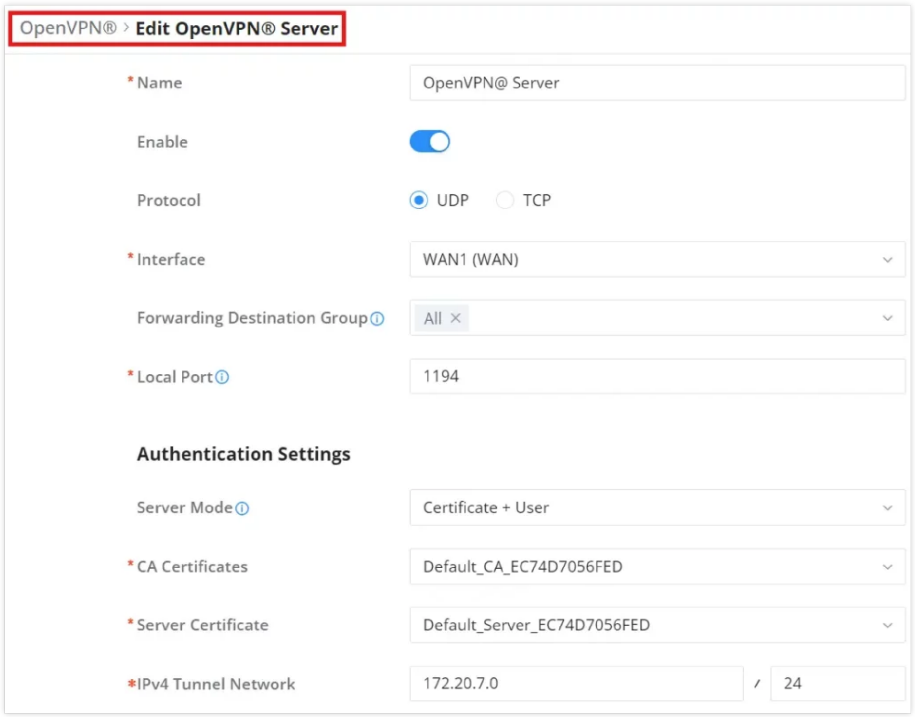


Add OpenVPN® Server

Step 2: Configure how clients connect to the server

Then, configure the connection settings that remote clients must match:

- Set **Enable** to **On**.
- Set **Protocol** to **UDP** (recommended for most deployments).
- Set **Interface** to the **WAN** interface remote clients will reach (example: `WAN1`).
- Set **Local Port** to **1194** (keep the default unless you need a different port).



Configure how clients connect to the server

Step 3: Configure authentication (Server Mode)

Set **Server Mode** to define how remote clients authenticate. This choice determines what you will configure later under **VPN → Remote Users**.

- **Certificate + User (recommended):** Client certificate **and** username/password.
- **Certificate:** Client certificate only.
- **User Authentication:** Username/password only.
- **PSK:** Pre-shared key authentication.

Note: *Only if you select **Certificate** or **Certificate + User**, configure:*

- **CA Certificates:** Select the CA used by this server profile.
- **Server Certificate:** Select the certificate that the router presents to clients.

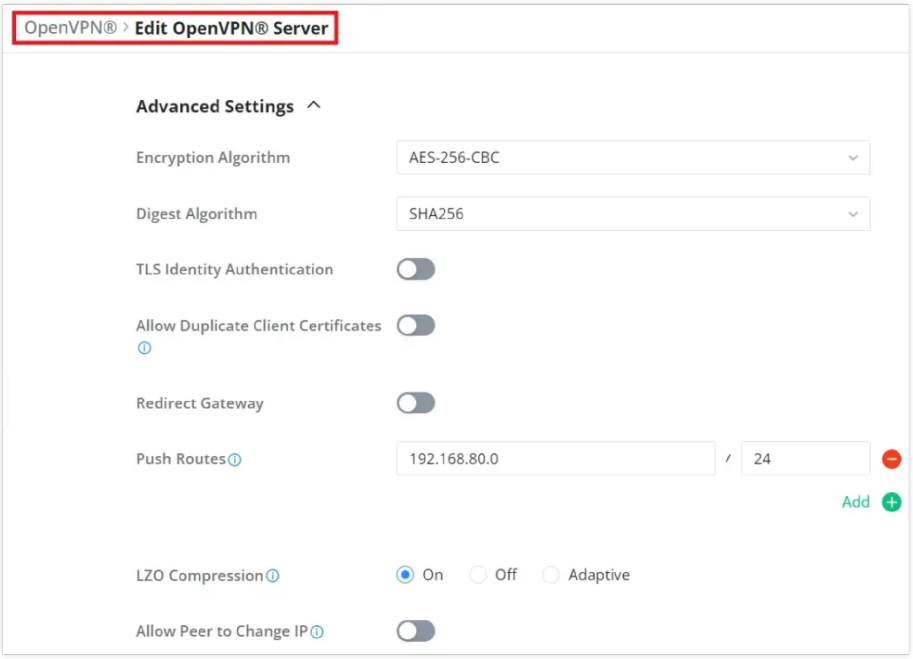
Step 4: Set the tunnel network

Set **IPv4 Tunnel Network** to define the VPN subnet that will be assigned to connected clients (example: `172.20.7.0/24`). Use a subnet that does not overlap with your LAN subnet.

Step 5: Define what clients can reach through the VPN (Push Routes)

Under **Advanced Settings**, use **Push Routes** to tell the VPN clients which internal networks should go through the tunnel.

Add your LAN subnet (example: `192.168.80.0/24`). After the client connects, it will be able to access devices in that subnet through the VPN (*for example, PCs, servers, printers, or other LAN resources*). Traffic to other networks that are not listed in **Push Routes** will not be routed through the VPN by default.



Define what clients can reach through the VPN Push Routes

OpenVPN® Server Options Reference

Use this table as a reference for what each field controls and when you might change it. The step-by-step procedure above only covers the required settings to get a working client-to-site VPN.

Field	Description
Name	Label for this OpenVPN® server profile. Useful when you have multiple VPN profiles.
Enable	Turns this server profile on or off. Disabling stops new connections and may drop existing ones.
Protocol	Transport used by OpenVPN®. UDP is typically preferred for performance and stability. TCP can help when UDP is blocked but may be slower.
Interface	The WAN interface where the server listens for incoming VPN connections. Choose the WAN that remote clients can reach from the internet.
Forwarding Destination Group	Controls which interfaces/targets are included for forwarding behavior. Leaving it as All is common so newly added interfaces are included.
Local Port	Listening port for OpenVPN® on the selected interface (default commonly 1194). Clients must connect to the same port, and it must not conflict with another service.
Server Mode	Defines how clients authenticate: Certificate + User (certificate + username/password), Certificate (certificate only), User Authentication (username/password only), PSK (shared key). This choice determines what you configure later under Remote Users.
CA Certificates	Certificate Authority used to validate/sign certificates for this VPN. Must match the CA used to sign client certificates when certificate-based modes are used.
Server Certificate	Certificate presented by the router during the TLS handshake. Clients use it (and the CA) to verify the server identity. Relevant for certificate-based modes.

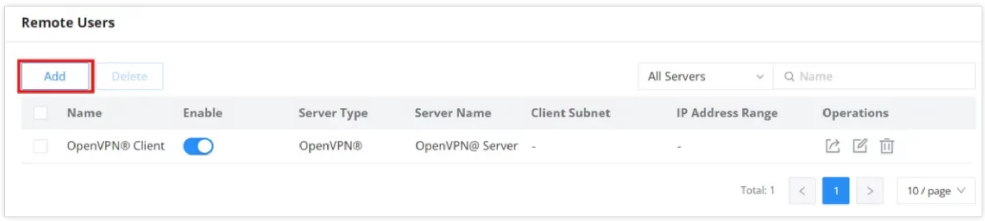
IPv4 Tunnel Network	VPN subnet assigned to connected clients (e.g., 172.20.7.0/24). Choose a subnet that does not overlap with LAN or routed subnets.
Encryption Algorithm	Cipher used to encrypt tunnel traffic (e.g., AES-256-CBC). Defaults are typically secure; change only for compliance or client compatibility.
Digest Algorithm	Hash/integrity algorithm used for authentication/integrity checks (e.g., SHA256). Change only for interoperability requirements.
TLS Identity Authentication	Adds an additional TLS identity check using a pre-shared TLS key. Clients must match this setting if enabled.
Allow Duplicate Client Certificates	Allows multiple devices to connect using the same client certificate. Convenient but reduces traceability and per-device control. Not applicable in PSK mode.
Redirect Gateway	If enabled, routes client internet traffic through the VPN (full-tunnel). Leave disabled for split-tunnel access to internal networks only.
Push Routes	Defines which internal networks clients can reach through the VPN (e.g., 192.168.80.0/24). Client traffic to these networks is sent through the tunnel.
LZO Compression	Compression behavior for tunnel traffic. Ensure client settings match; mismatched compression can cause traffic issues. Adaptive negotiates based on conditions.
Allow Peer to Change IP	Allows the client source IP/port to change during a session. Useful for roaming/mobile clients whose network changes while connected.

OpenVPN® Server Options Reference

2) Add a Remote User

Step 1: Open the Remote Users page

Go to **VPN** → **Remote Users**, then click **Add**.

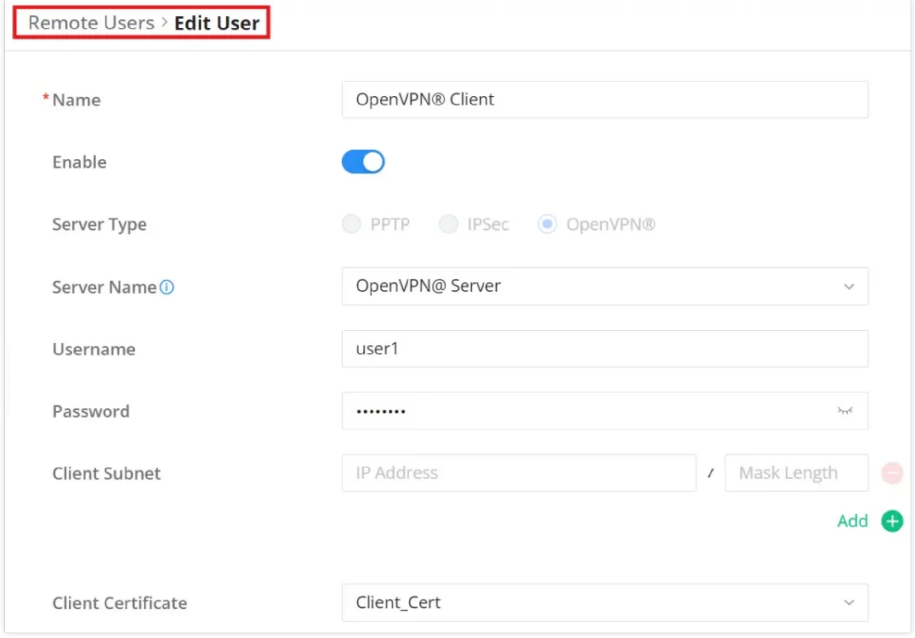


Step 1 Open the Remote Users page

Step 2: Link the remote user to your OpenVPN® server profile

After clicking add a remote user, configure the following:

- Enter a **Name** for this remote user (example: `user1` or `OpenVPN® Client`).
- Set **Enable** to **On**.
- Set **Server Type** to **OpenVPN®**.
- Set **Server Name** to the OpenVPN® server profile you created earlier (*example:* `OpenVPN® Server`).



Step 2 Link the remote user to your OpenVPN® server profile

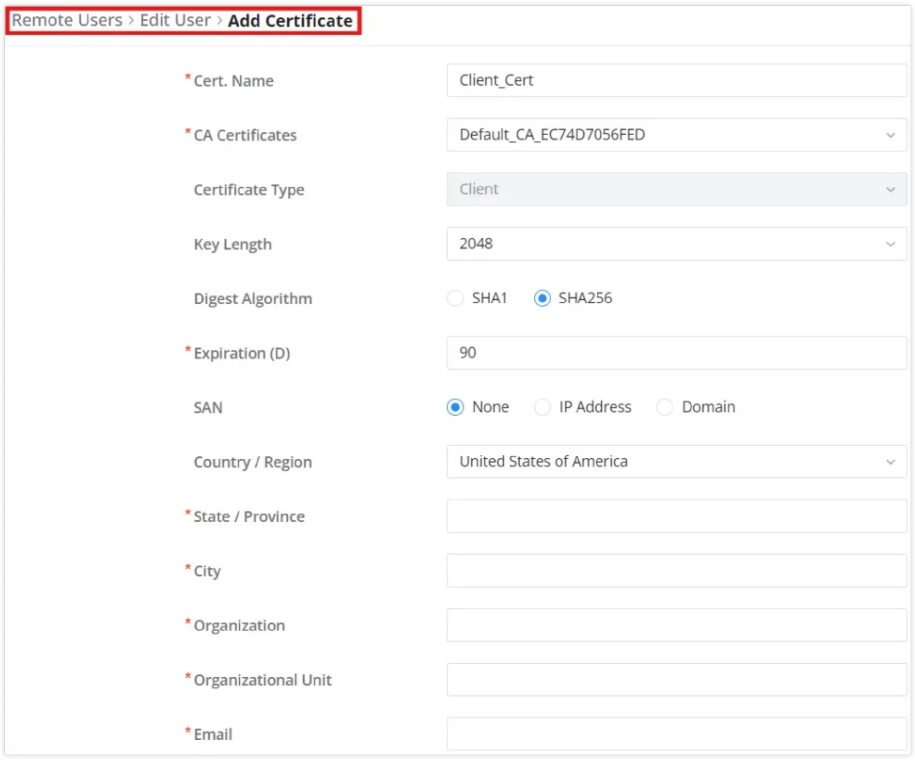
Step 3: Enter the authentication details (based on Server Mode)

Check the **Server Mode** you selected in the OpenVPN® server profile, then fill in the matching fields:

- If **Server Mode = Certificate + User**: enter **Username** and **Password**, and select a **Client Certificate**.
- If **Server Mode = Certificate**: select a **Client Certificate** only.
- If **Server Mode = User Authentication**: enter **Username** and **Password** only.
- If **Server Mode = PSK**: no username/password or client certificate is used. Clients authenticate using the same **pre-shared key** configured on the OpenVPN® server.

Step 4: Add a client certificate (only if required by Server Mode)

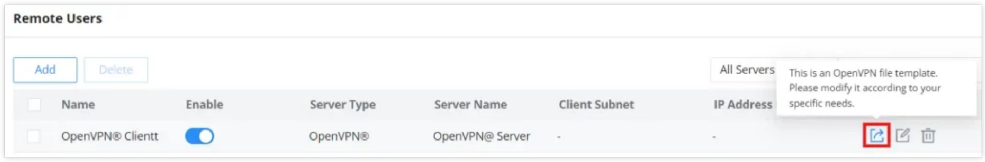
If your server mode requires a client certificate and you do not already have one available, click **Add** next to **Client Certificate** to create one. After it is created, make sure it is selected in the **Client Certificate** field.



Step 4 Add a client certificate only if required by Server Mode

Step 5: Download the .ovpn client profile

Back on the **Remote Users** list, find the remote user you created, then click the **Download/Export** icon in the **Operations** column to download the `.ovpn` file. This file will be imported on the client side in the next section.



Step 5 Download the ovpn client profile

Field Reference (Remote User & Client Certificate)

Use the tables below to understand what each field controls and when you would change it. The step-by-step procedure above only covers what's required to generate a working `.ovpn` profile.

- **Remote User Field Reference**: Covers the fields under **VPN → Remote Users → Add/Edit User**.

Field	Description
Name	A label for this remote user entry. Use a name that helps you identify the user/device later (e.g., user1-laptop, sales-iphone).
Enable	Enables or disables this remote user. Disabling is a simple way to revoke access without deleting the entry.
Server Type	VPN type this user belongs to (OpenVPN®, IPsec, PPTP, etc.). For this guide, select OpenVPN® so the user is linked to an OpenVPN® server profile.
Server Name	The OpenVPN® server profile this user will connect to. Must match the server profile created under VPN → OpenVPN®. The exported .ovpn profile is generated from this association.
Username	Login name for this remote user. Required only when the server's Server Mode uses user authentication (User Authentication or Certificate + User).
Password	Password for this remote user. Required only when the server's Server Mode uses user authentication (User Authentication or Certificate + User). Use a strong password if the service is reachable from the internet.
Client Subnet	Optional. Use only if you need to assign or restrict addressing/routing behavior for this specific user. In typical client-to-site deployments, leave empty.
Client Certificate	Certificate used to authenticate this remote user when the server's Server Mode includes certificates (Certificate or Certificate + User). Best practice is one certificate per user/device for easy revocation.

Remote User Field Reference

- **Client Certificate Field Reference**: Covers the fields under **Remote Users → Edit User → Add Certificate**.

Field	Description
Cert. Name	Label for the certificate inside the router UI. Use something that maps to the user/device (e.g., client_user1, laptop_sales_01).
CA Certificates	Certificate Authority that signs this client certificate. Must match the CA selected on the OpenVPN® server profile, otherwise the server will not trust the client certificate.
Certificate Type	Defines the certificate role. For remote users, this must be Client (server certificates are used only by the OpenVPN® server profile).
Key Length	RSA key size for the certificate. 2048 is the common default and a good balance of security and performance. Larger keys increase CPU cost.
Digest Algorithm	Hash algorithm used for the certificate signature. SHA256 is recommended. Use SHA1 only if you must support very old/legacy clients.
Expiration (D)	How long the certificate remains valid (in days). Longer validity reduces maintenance; shorter validity reduces risk if a certificate is compromised. Choose based on your security policy.

SAN	Subject Alternative Name. Most client certificates can keep None. Use IP Address or Domain only if you have a specific requirement to bind the certificate identity to an IP/FQDN.
Country / Region	Certificate subject attribute (identity metadata). Example: United States of America.
State / Province	Certificate subject attribute (region/state). Example: California.
City	Certificate subject attribute (locality/city). Example: San Francisco.
Organization	Certificate subject attribute (company/organization). Example: ExampleCorp.
Organizational Unit	Certificate subject attribute (department/team). Example: IT or Network.
Email	Certificate subject attribute (contact email). Example: vpn-admin@example.com.

Client Certificate Field Reference

B – Client Side (OpenVPN® Client Configuration)

After downloading the OpenVPN® client profile (`.ovpn`) from the router, import it into an OpenVPN client application such as OpenVPN Connect (Windows®/macOS®/Android®/iOS®). Some devices also provide a built-in OpenVPN® client and can import the same `.ovpn` file directly.

Step 1: Review and edit the `.ovpn` profile if needed (optional)

In most deployments, the downloaded `.ovpn` profile works without any changes. Edit it only when you must update connection details such as the server address (IP/hostname), port, or protocol.

Open the `.ovpn` file using a text editor, adjust only the required values, then save the file.

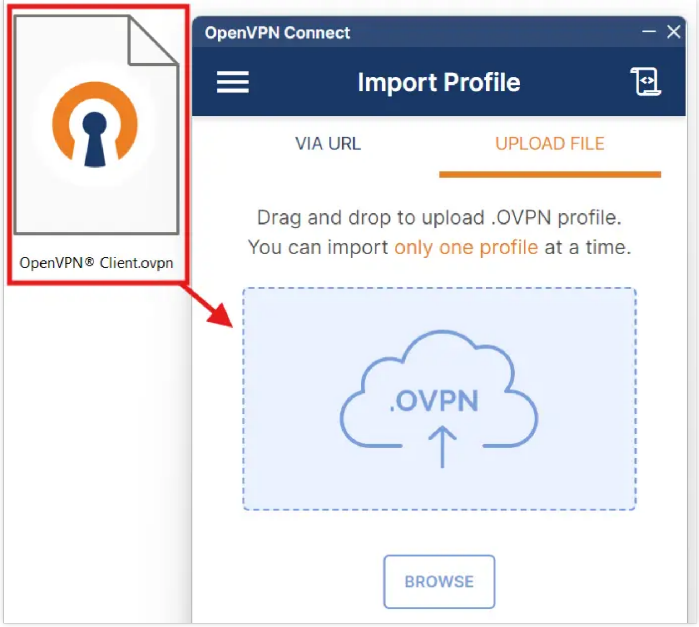
```
# Config for OpenVPN 2.x
# Enables connection to GUI
client
dev tun
resolv-retry infinite
proto udp
remote 192.168.6.152
port 1194
comp-lzo
data-ciphers AES-256-CBC
data-ciphers-fallback AES-256-CBC
auth SHA256
auth-user-pass

<ca>
-----BEGIN CERTIFICATE-----
MIIEvzCCA6egAwIBAgIJAIRrFIJj9A9oMA0GCSqGSIb3DQEBCwUAMIGWMQswCQYD
VQQGEwJVUzELMAkGA1UECAwCTUExDzANBgNVBAcMBkJvc3RvbjEUMBIGA1UECgwL
R3JhbmRzdHJlYW0xDDAKBgNVBAsMA0dXTjEgMB4GA1UEAwwXRGVmYXVsdF9DQV9F
Qzc0RDcwNTZGRUQxIzAhBgkqhkiG9w0BCQEWFGluZm9AZ3JhbmRzdHJlYW0uY29t
MB4XDTI0MTAzMDA4NTQyOFoXDTQ0MTAzMDA4NTQyOFowgZYxCzAJBgNVBAYTAlVT
MQswCQYDVQQIDAJNQTEPMA0GA1UEBwwGQm9zdG9uMRQwEgYDVQQKDAtHcmFuZHN0
cmVhbTEMMAoGA1UECwwDR1dOMSAwHgYDVQQDDBdEZWZhdWx0X0NBX0VDNzRENzA1
NkZFRDEjMCEGCSqGSIb3DQEJARYUaW5mb0BncmFuZHN0cmVhbS5jb20wggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDTJKUCcg4WoLaMBcXawxlkDrXgNzzU
g/Tim0u7p/YAXMWKYrOMZ6vzq7wWuVItkE1CSgVQhlUmYpgkhBkKzChgnKAetfXs
```

Review and edit the `ovpn` profile if needed optional

Step 2: Import the `.ovpn` profile into the OpenVPN client

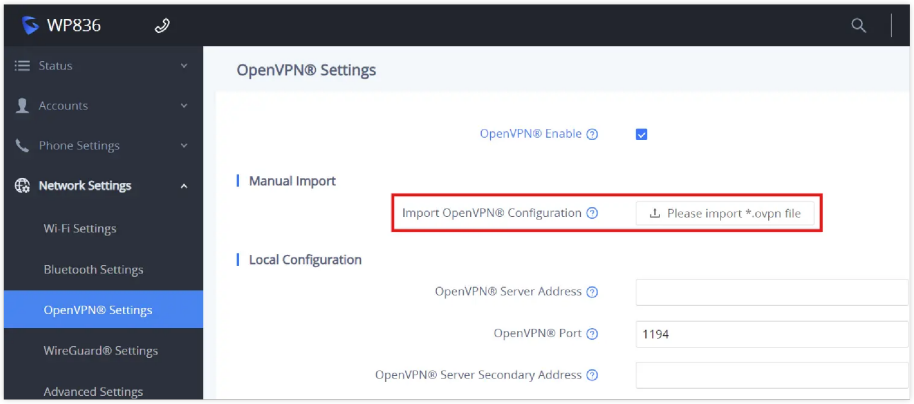
On the client device, open your OpenVPN application and import the profile.

In OpenVPN Connect (desktop), you can typically drag and drop the `.ovpn` file into the application or click **Browse** to locate and select it.



Import the `ovpn` profile into the OpenVPN client

If you are using a platform with built-in OpenVPN® support, import the `.ovpn` profile using the device's VPN/OpenVPN settings menu.

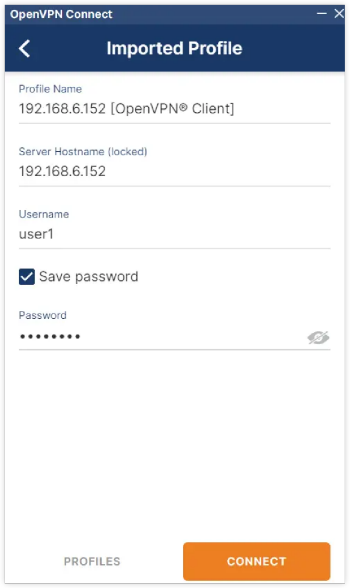


Import the `ovpn` profile into the OpenVPN client

Step 3: Enter authentication details and connect

After importing the profile, the client may prompt for authentication details. Use the same credentials that were configured earlier in Router Side under "Add a Remote User".

Then click Connect to establish the VPN tunnel.

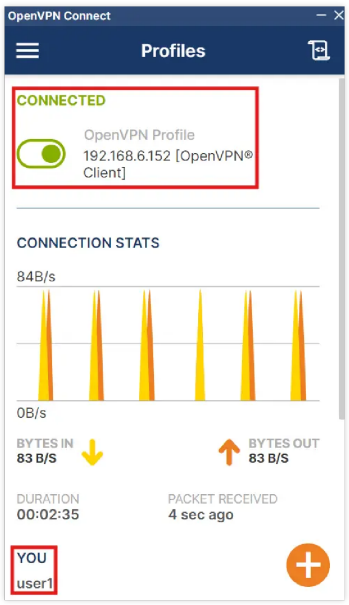


Enter authentication details and connect

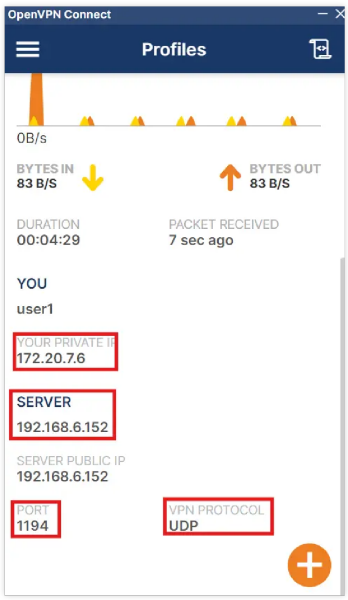
Verify the Connection

After you connect the OpenVPN® client, verify the VPN tunnel from the client side and from the router (server side). Then confirm that the client can reach a device inside the remote LAN.

1) Verify the connection on the OpenVPN client: On the client device, open the OpenVPN application and confirm the profile status shows **Connected**. Open the connection details to confirm key parameters such as the assigned tunnel IP, server address, port, and protocol.

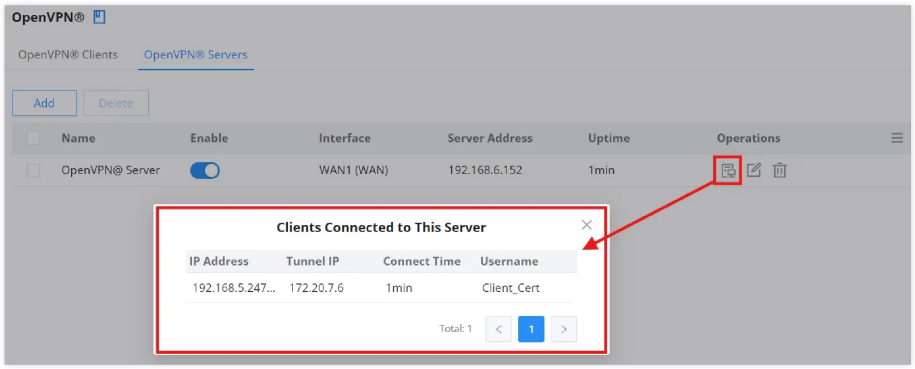


Verify the connection on the OpenVPN client part 1



Verify the connection on the OpenVPN client part 2

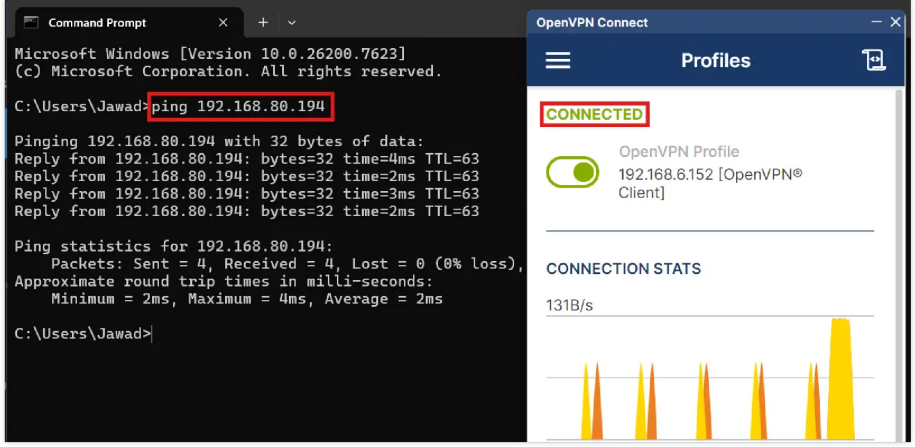
2) Verify the connection from the router (server-side): On the router Web UI, open the OpenVPN® server page and view the connected clients list. Confirm the client is listed and that a tunnel IP has been assigned.



Verify the connection from the router server side

3) Verify access to a host inside the remote LAN: From the connected client PC, test connectivity to a device located on the remote LAN that should be reachable through the VPN (for example, an internal server, PC, or IP phone on the subnet configured earlier on the OpenVPN® server).

In this example, the client successfully pings **192.168.80.194**, confirming that traffic can reach a host on the remote LAN through the VPN tunnel.



Verify access to a host inside the remote LAN