Configuring an EIGR-V Gigabit IP Router as an OpenVPN Server

For network savvy customers, Contemporary Controls offers a Self-HostedVPN solution which allows users to set up and maintain their own secure, remote access without subscription fees and without the need for a cloud-based VPN server.

Contemporary Controls' EIGR-V Skorpion Gigabit IP router can be configured to operate in OpenVPN server mode which allows the router to act as the VPN server with the ability to support our wired and cellular routers as VPN clients. OpenVPN® is a well-supported open-source VPN technology that incorporates SSL/TLS security with encryption. Any IP program (TCP or UDP) can communicate via Self-HostedVPN. Once the VPN connection is established, messages can originate from either side –eliminating the need for port-forwarding.

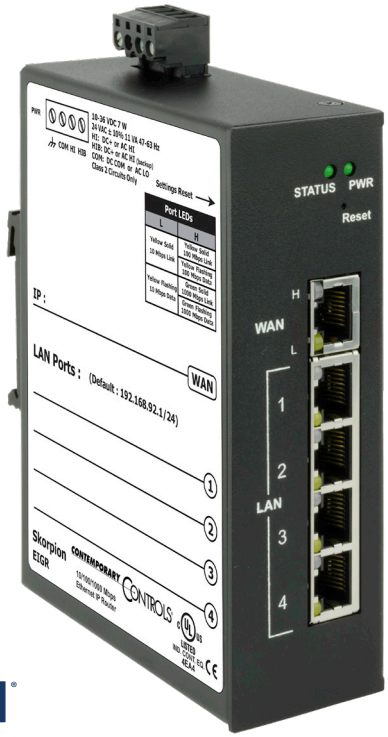
Setting up an OpenVPN server on your own is not trivial. It typically involves setting up a root certificate authority and generating certificates and keys for the OpenVPN server and for each client device that intends to connect to this server. However, the EIGR-V router has a built-in webpage interface to generate certificates and keys for VPN client devices, without requiring users to download software or having to learn the complexities of setting up a VPN.

For Self-HostedVPN, users are responsible for setting up a fixed public IP address for the EIGR-V operating as the OpenVPN server. The OpenVPN server router can also be connected behind an existing firewall/router with a public IP and use port forwarding to access the OpenVPN server. This OpenVPN server can reside at the client site or any other convenient site and uses the Internet for communicating to OpenVPN clients without any cloud service involved. This specification differs from our RemoteVPN solution, where there is no requirement of a static public IP address because the OpenVPN server is provided by RemoteVPN. Both the Self-HostedVPN and RemoteVPN solutions work for legacy IP devices where it is not possible to configure an IP gateway address on the device.

One EIGR-V in OpenVPN server mode can support up to 15 IP routers in OpenVPN client mode, allowing access to 15 remote sites via cellular (EIGR-C) or wired VPN routers (EIGR-V /EIPR-V). Additionally, 15 PC/tablet/phone OpenVPN clients are supported with access control permissions configurable via the EIGR-V's built-in webpage. These VPN clients can be located anywhere that has Internet connectivity. With this arrangement, PC/tablet/cell phone clients and client routers in remote locations can communicate securely using the services of this one EIGR-V OpenVPN server to devices behind the VPN client routers. An additional benefit is that each PC client can be configured to communicate with one or more router clients independent of each other.

The Self-HostedVPN solution provides secure, remote access to any IP device by just using the VPN IP address for a device. There is no additional requirement to setup Network Address Translation (NAT) or port forwarding on the client routers as they initiate outbound connections to the OpenVPN server.

Furthermore, the OpenVPN client devices only require internet access – there is no requirement for a static or public IP address. Only the EIGR-V router running the OpenVPN server needs to be publicly accessible on a single IP port.



Self-HostedVPN

OPENVPN

Configure the EIGR-V to act as a OpenVPN Server

1. Setup the Current Time

Select the menu option **Setup -> Time**.

This should be done first as the time will be used when the Certificates are generated.

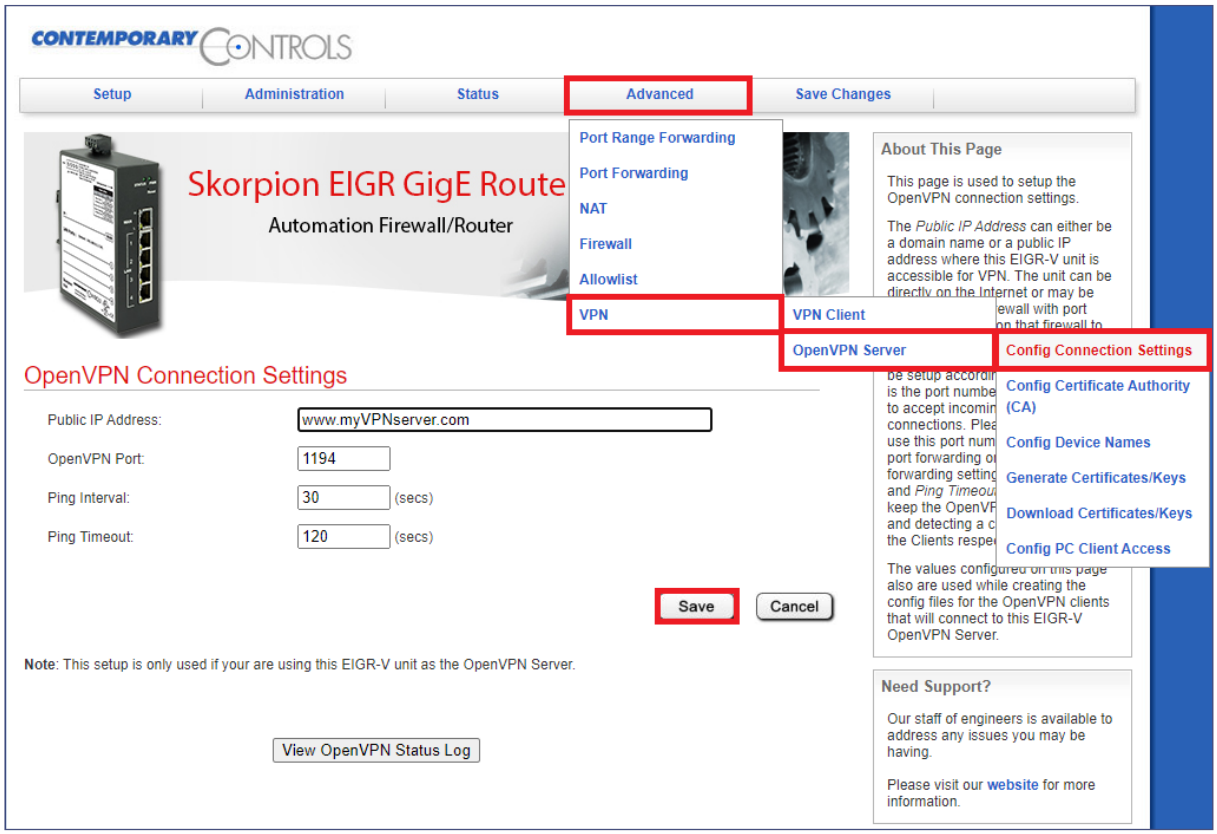
2. Set the Connection Settings

Select the menu option **Advanced -> VPN-> OpenVPN Server -> Config Connection Settings**.

Setup the Public IP address/hostname, port, and ping interval/timeout here.

Click **Save** when done.

Note: The **View OpenVPN Status Log** button can be used to view the connected devices, the public IP addresses associated with the VPN client location, connection time, etc.



3. Setup the Certificate Authority (CA) and generate CA key

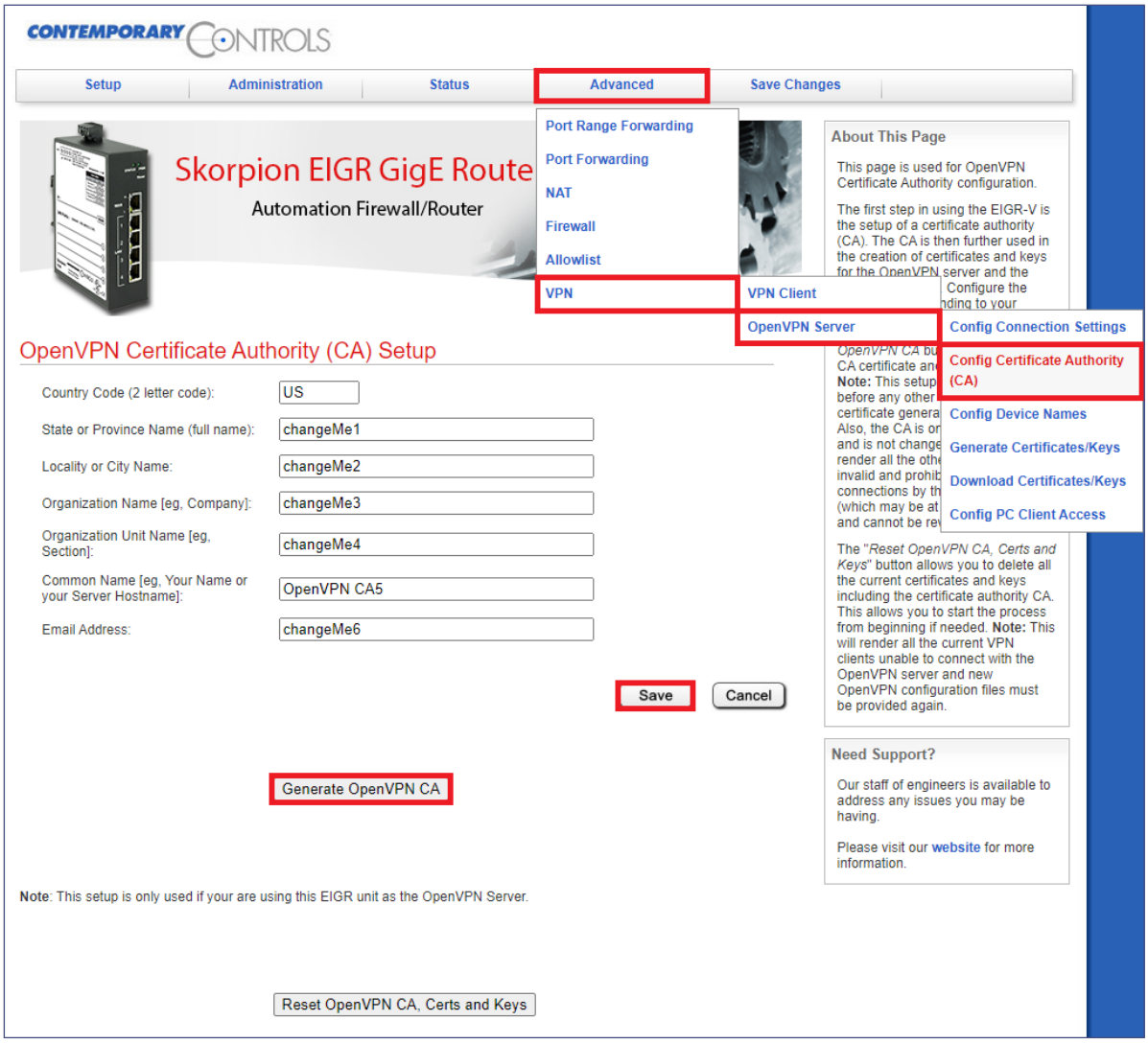
Select the menu option **Advanced -> VPN -> OpenVPN Server -> Config Certificate Authority**.

Configure the CA options per your location and click **Save**.

Then, click the **Generate OpenVPN CA** button. This will generate the CA key and the button will be disabled.

Note: This is a one-time setup.

The **Reset OpenVPN CA, Certs and Keys** button deletes all the OpenVPN files in case the files need to be generated again.



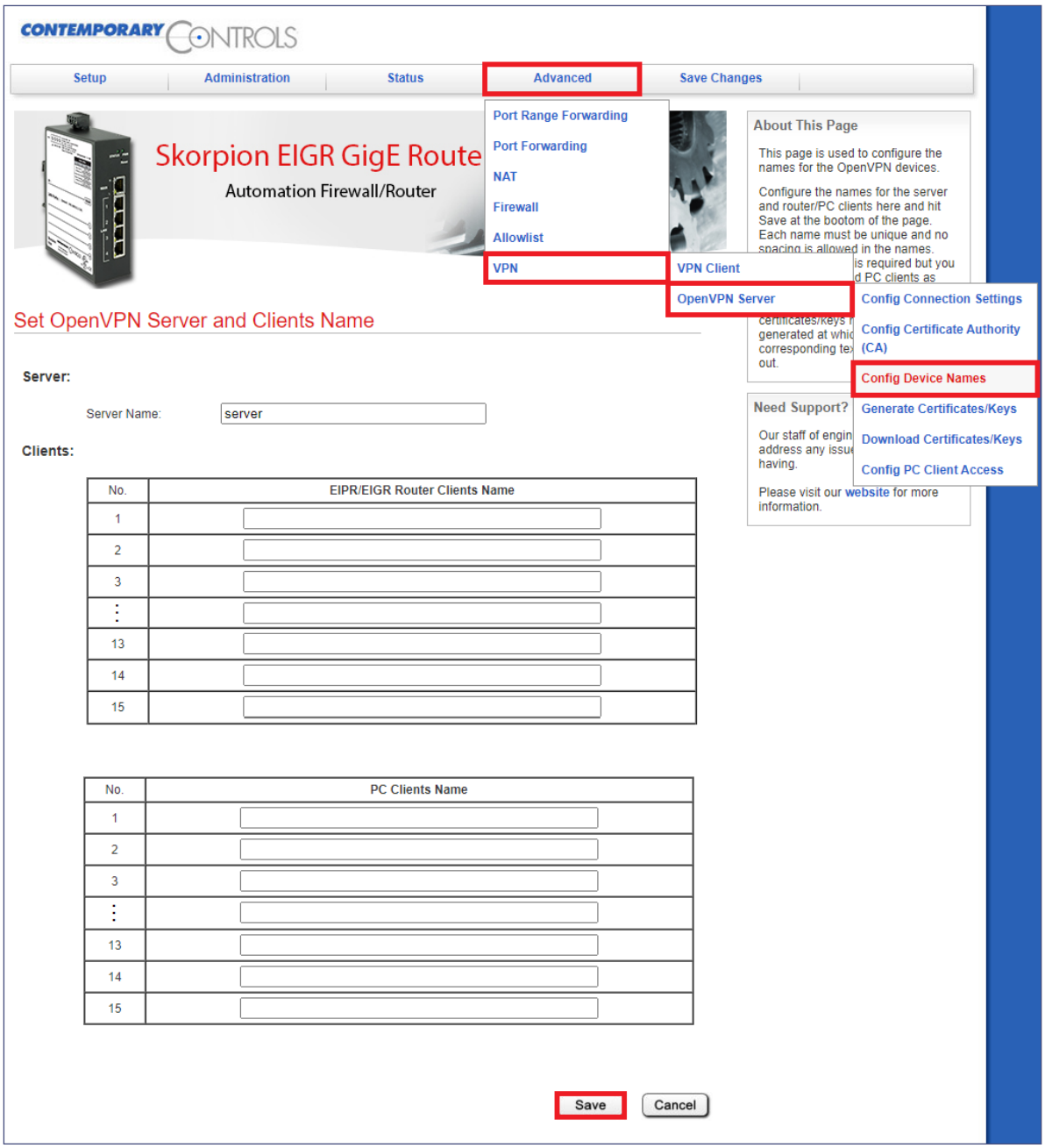
4. Setup the Device Names

Select the menu option **Advanced -> VPN -> OpenVPN Server -> Config Device Names**.

Set the server name and clients' names for up to 15 routers and 15 PC clients.

Click **Save** at the bottom of the page.

Note: All the names must be unique and contain no spaces.

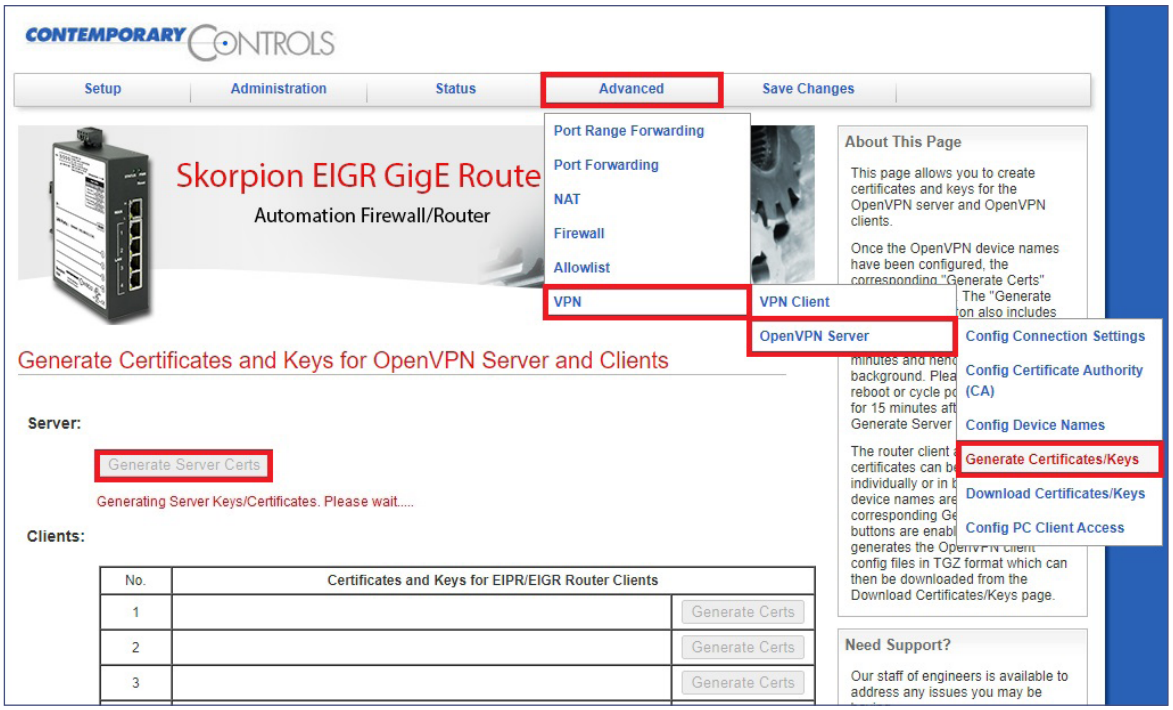


5. Create Server Certificates

Select the menu option **Advanced -> VPN -> OpenVPN Server -> Create Certificates/Keys**.

Click the **Generate Server Certs** button to create the server config. This also involves creating the Diffie-Hellman key and takes up to 15 minutes in the background. Don't reboot or power cycle the router for 15 minutes after clicking this button.

The status of the server certificates is shown below the **Generate Server Certs** button. When the Server Certs are finished, the status message shows Done!



6. Create Client Certificates

Select the menu option **Advanced -> VPN -> OpenVPN Server -> Create Certificates/Keys**.

This is the same page as **Step 5** above.

If the client device names have been configured, they are shown here, and the corresponding **Generate Certs** button is also enabled. Both the router and PC client certs can be generated with this page.

As more client names are added, the corresponding **Generate Certs** buttons become enabled.

7. Download Client Certificates

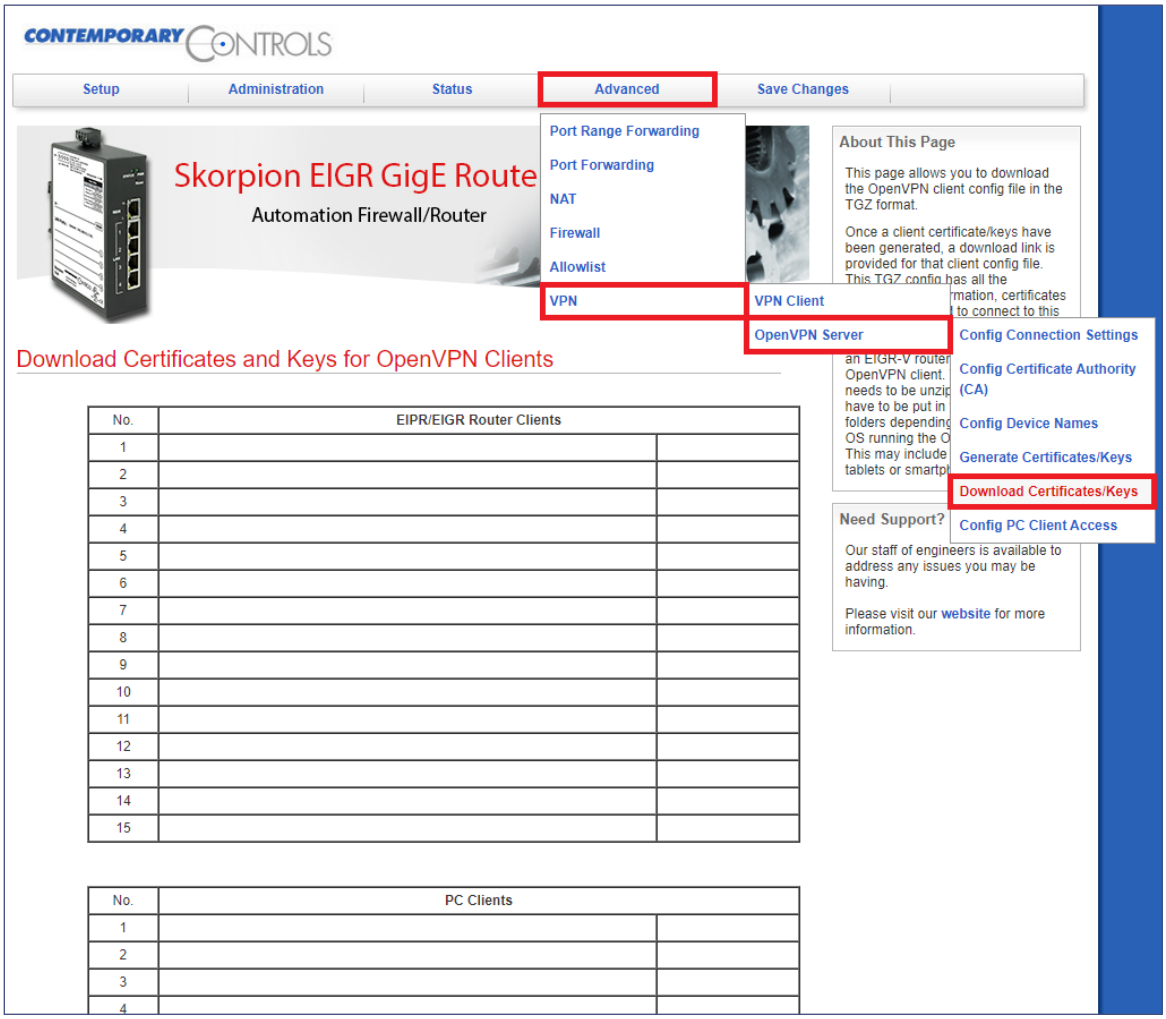
Select the menu option **Advanced -> VPN -> OpenVPN Server -> Download Certificates/Keys**.

After generating the certificates, the client certificates can be downloaded here.
The client name and a download link will be available on this page.

Individual router and PC config files in .tgz format can be downloaded from this page.

Router .tgz file can be uploaded to EIGR-V client router directly.

The .tgz file needs to be unzipped to get the .ovpn file for the PC client.
Note: these steps are explained in OpenVPN Client Configuration below.

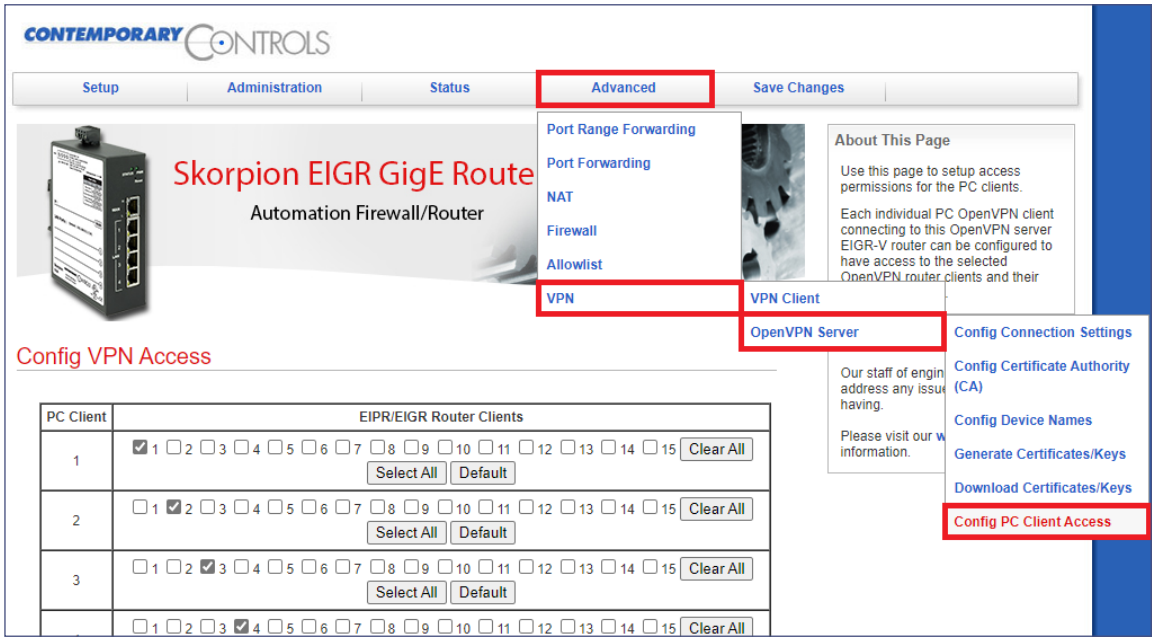


8. Setup PC Client Access

Select the menu option **Advanced -> VPN -> OpenVPN Server -> Config PC Client Access**.

Select the access permission for each PC client to the EIGR clients and click the **Save** button at the bottom of the page.

Note: You can click **Select All** to configure 15 routers clients for each PC or click **Default** to return to the default router client for each PC (PC Client 1 = Router Client 1, etc.)



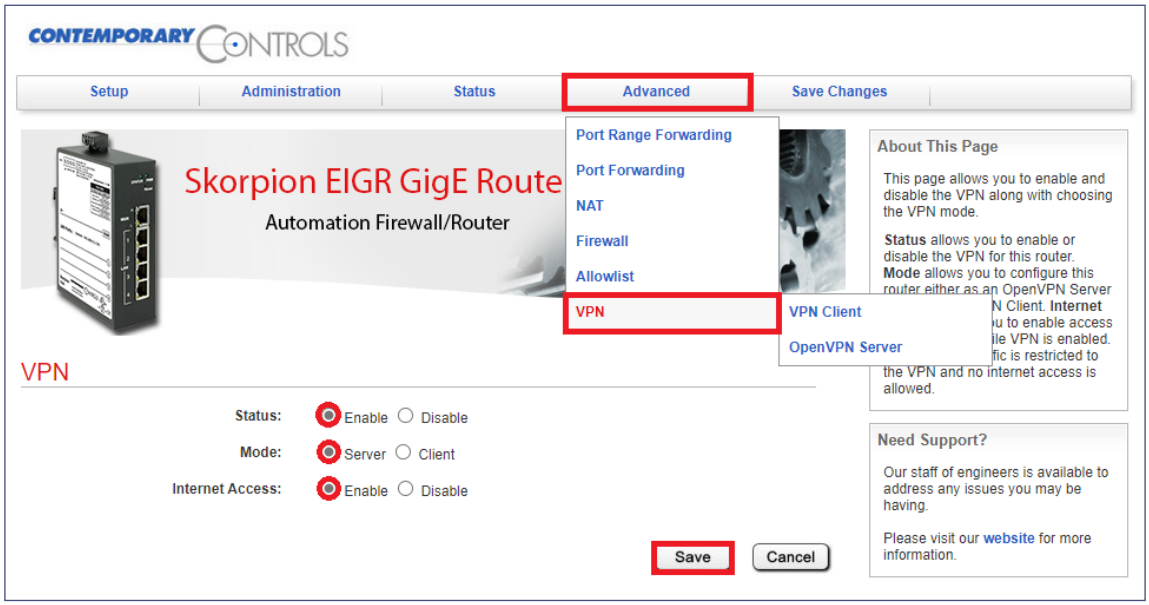
9. Setup the Mode and Enable VPN

Select the menu option **Advanced -> VPN**.

Set:

- Status to **Enable**
- Mode to **Server**
- Internet Access to **Enable**

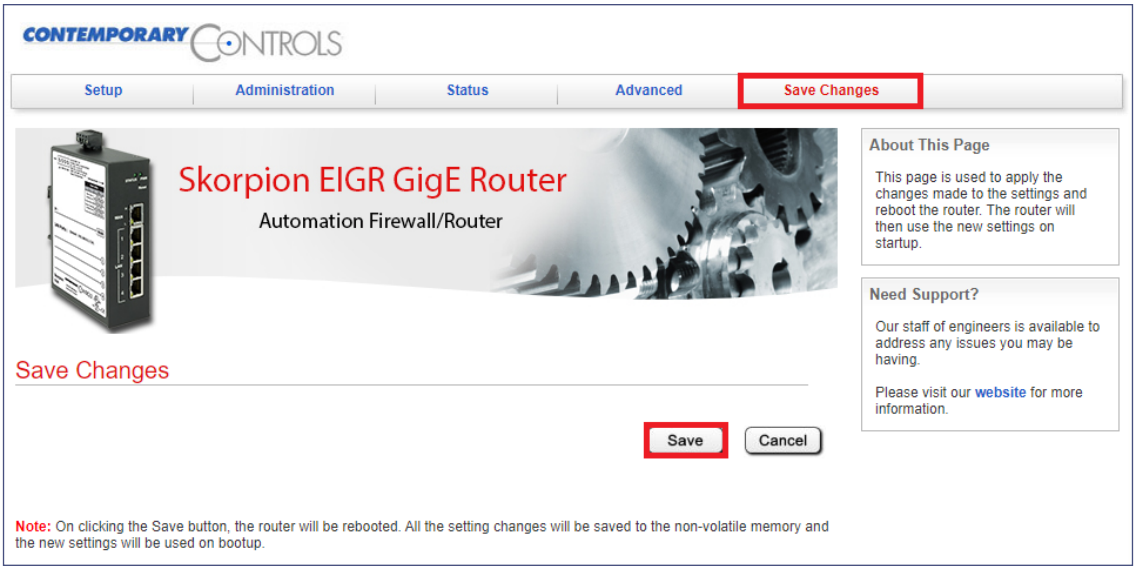
Then, click **Save**.



10. Save Changes and Reboot

Select the menu option **Save Changes**.

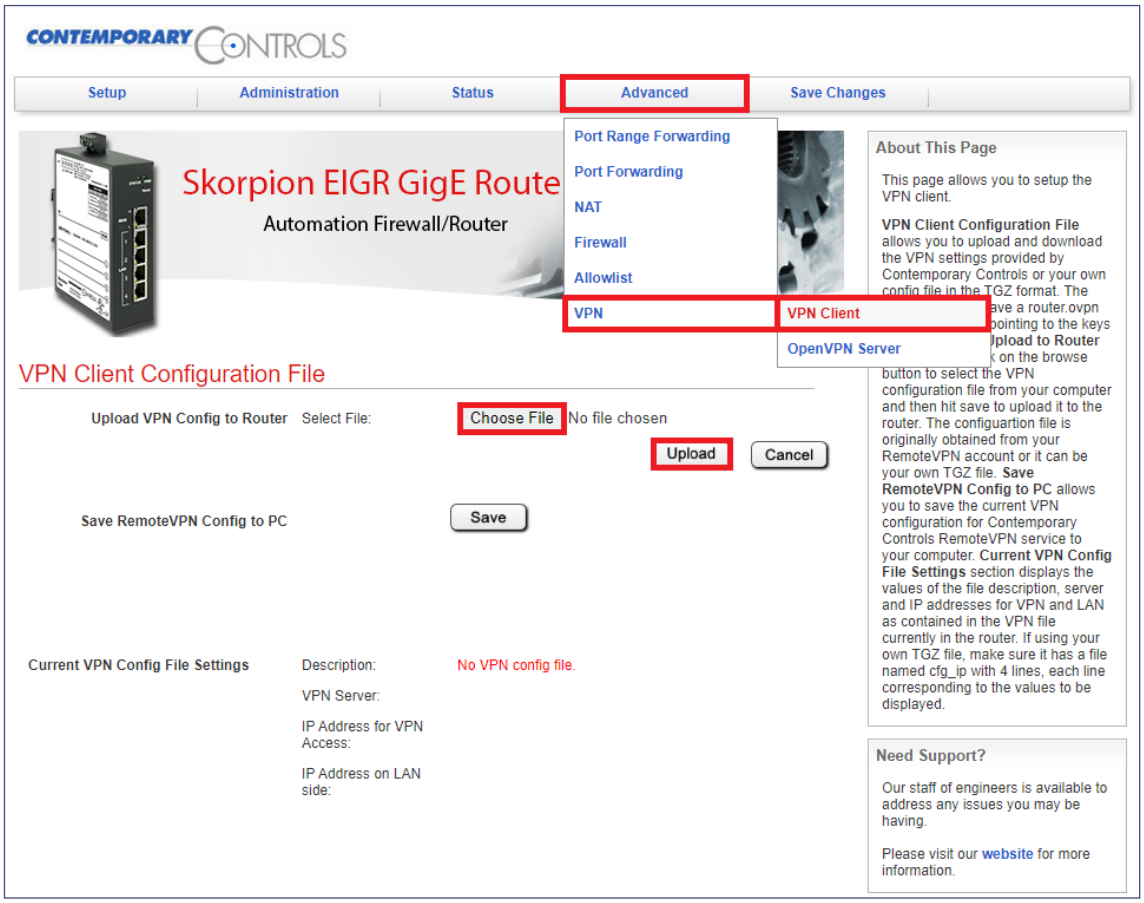
Please ensure that 15 minutes have passed since you clicked the **Generate Server Certs** button in step 5. Select the menu option **Save Changes** to reboot the router.



OpenVPN Router Client Configuration

1. Select the menu option **Advanced -> VPN -> VPN Client**.

   Upload the router .tgz config file from the EIGR-V using the **Browse/Choose File** (browser dependent) button and then click **Upload**. The configuration settings from the uploaded config file are then shown at the bottom section of the webpage.



2. Setup the Mode and Enable VPN

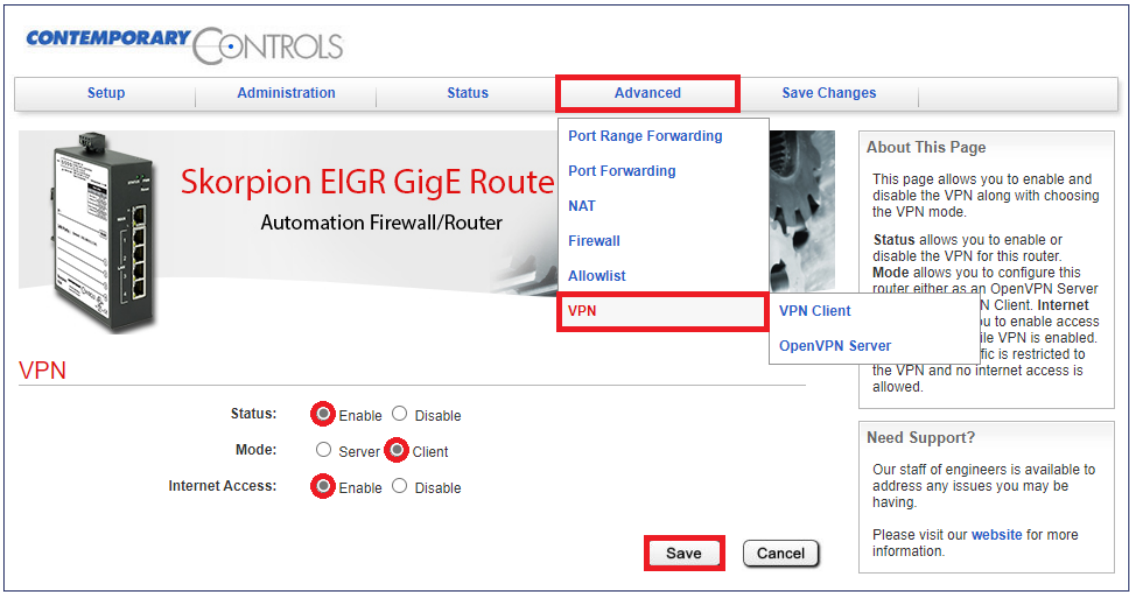
Select menu option **Advanced -> VPN**.

Set:

- Status to **Enable**
- Mode to **Client**
- Internet Access to **Enable**

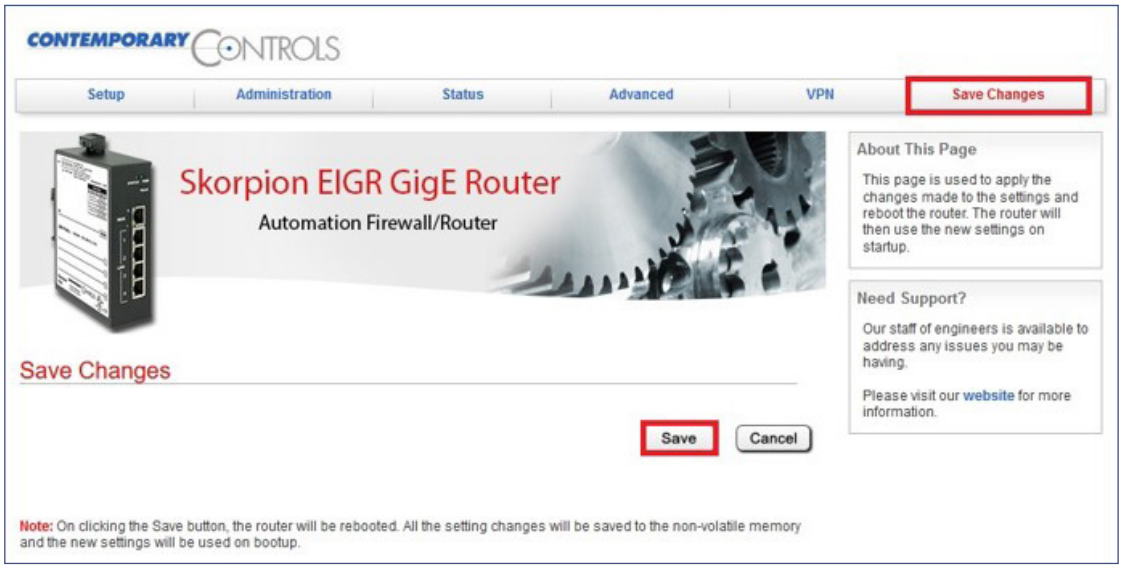
Then, click **Save**.

Note: The traffic can be restricted to the VPN tunnel only with no internet access, if desired, by setting Internet Access to **Disable**.



3. Reboot the router

Select menu option **Save Changes.** Then, click **Save**.



Self-HostedVPN PC/Mobile Device OpenVPN Client Configuration

Configuring the VPN clients for PC/mobile devices involves installing the software (if not already installed) and importing the configuration file in **.ovpn** format. The OpenVPN software for PC is available to download from openvpn.net, Google Play Store for Android devices and App Store for iOS devices.

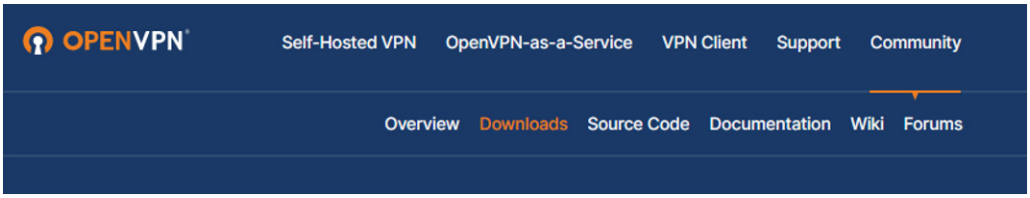
- Unzip the .tgz file.
- Import the .ovpn file to the VPN client.
- For mobile devices (e.g., phone/tablet):
  - Email and save to device.
  - For instructions on how to use an OpenVPN File on Android devices, refer to **Using OpenVPN File on Android**.
  - For instructions on how to use an OpenVPN File on iOS devices, refer to **Using OpenVPN File on iOS**.
- For the PC:
  - Windows OpenVPN clients can be downloaded from openvpn.net.
  - Linux clients can be installed using the specific Linux distribution commands.

OpenVPN has versions 2.x and 3.x

- Version 2.x installs as OpenVPN GUI.
- Version 3.x installs as OpenVPN Connect.

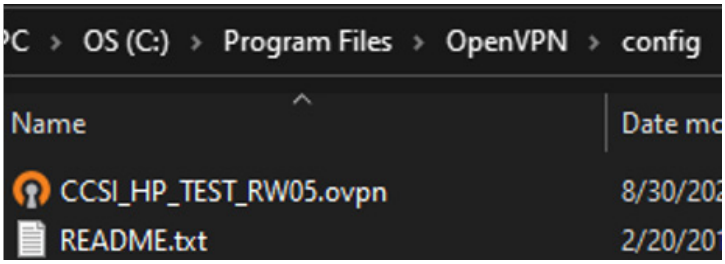
OpenVPN Windows PC Client 2.x Download

Go to openvpn.net and select the **Community → Downloads** menu. Install the VPN client.



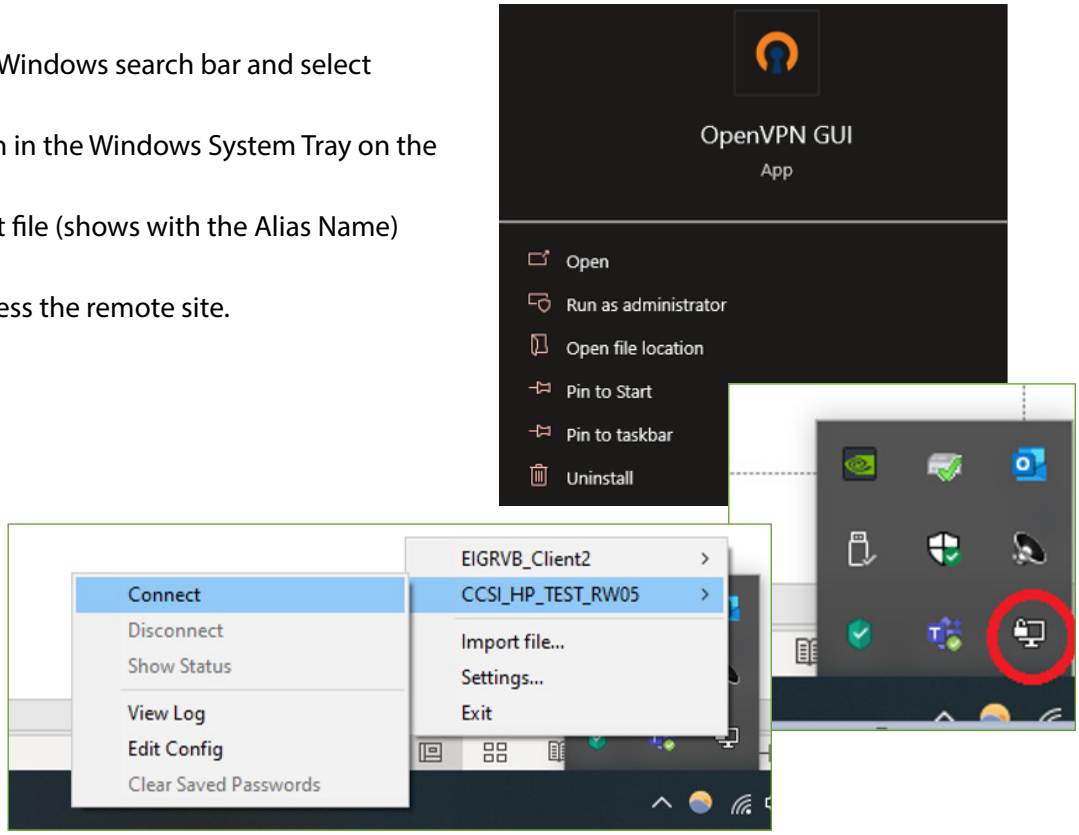
1. **Install OpenVPN PC config file**

   Copy the .ovpn client file to the OpenVPN/config folder under Program Files.



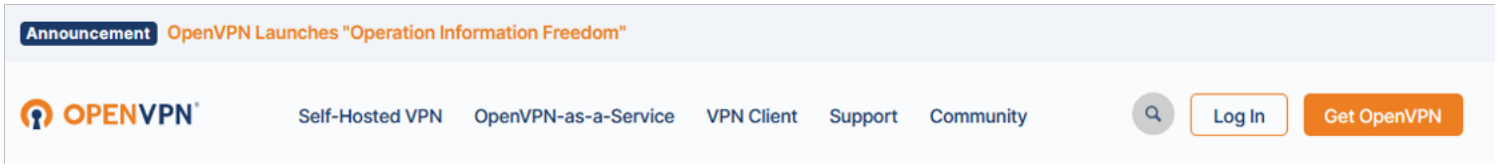
2. Start OpenVPN Client

- Type **OpenVPN GUI** in the Windows search bar and select **Run as administrator**.
- Click the OpenVPN GUI icon in the Windows System Tray on the right side.
- Choose the OpenVPN client file (shows with the Alias Name) and click **Connect**.
- Use the VPN address to access the remote site.



OpenVPN PC Client 3.x Download

Go to openvpn.net and click the **Get OpenVPN** button.



1. Install OpenVPN PC config file

- Scroll down on the webpage to locate the "OpenVPN Connect" download.
- Install OpenVPN Connect.

2. Start OpenVPN Client

- Start OpenVPN Connect.
- Import the .ovpn file and connect.
- Use the VPN address in the dashboard to access the remote site.

Self-HostedVPN Addresses and Considerations

- Router 1 is assigned 10.24.31.x/24 subnet
- Router 2 is assigned 10.24.32.x/24 subnet
- Router 3 is assigned 10.24.33.x/24 subnet
- Router 15 is assigned 10.24.45.x/24 subnet
- One-to-one VPN to LAN address Mapping like RemoteVPN
- No site-to-site access like RemoteVPN
- Setup current time on VPN Client router
- Setup Gateway address on LAN devices
  - Advanced->Firewall has Masquerade option on EIGR-V client

Ordering Information

Model	*RoHS*	*Description*
EIGR-V	✔	Skorpion GigE IP Router with VPN 0 to 60°C

United States
Contemporary Control Systems, Inc.
Tel: +1 630 963 7070
Fax:+1 630 963 0109
info@ccontrols.com

China
Contemporary Controls (Suzhou) Co. Ltd
Tel: +86 512 68095866
Fax: +86 512 68093760
info@ccontrols.com.cn

United Kingdom
Contemporary Controls Ltd
Tel: +44 (0)24 7641 3786
Fax:+44 (0)24 7641 3923
ccl.info@ccontrols.com

Germany
Contemporary Controls GmbH
Tel: +49 341 520359 0
Fax: +49 341 520359 16
ccg.info@ccontrols.com

www.ccontrols.com