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

Contemporary Controls' EIGR-VB Skorpion Gigabit IP router can be configured as a wired bridge VPN server for single-site, remote access solutions. With this configuration, users set up and maintain their own secure remote access without subscription fees and without the need for a cloud-based VPN server.

The EIGR-VB high-speed router links two 10/100/1000 Mbps Internet Protocol (IPv4) networks — passing appropriate traffic while blocking all other traffic. One network is the local-area-network (LAN); the other is the wide-area-network (WAN). The built-in stateful firewall passes communication initiated on the LAN-side while blocking WAN-side initiated communication.

The lower part of the router connects the LAN side. The upper part connects the WAN side. A firewall (which can be disabled by the user) separates the two parts. A firewall controls the passing of messages from one side of a router to the other. A stateful firewall acts on the structure of the message and who is initiating and who is responding. Originating requests from the LAN side and corresponding responses from the WAN side pass through the firewall. But traffic originating from the WAN side is blocked from the LAN side unless the firewall is adjusted to allow it. This protects the LAN side from unauthorized WAN access.

With Port Address Translation (PAT), LAN-side clients can access the Internet. Network Address Translation (NAT) allows a one-to-one translation between LAN-side and WAN-side devices. With Port Forwarding, LAN-side devices can be accessed from the Internet. The EIGR-VB incorporates a four-port Ethernet switch for multiple LAN-side connections. An external Ethernet-based modem — cable or DSL— can be used to connect to the Internet. DSL modems connect via Point-to-Point Protocol over Ethernet (PPPoE).

The EIGR-VB includes real-time clock and OpenVPN* client/server functionality. Operating in OpenVPN server mode, up to 10 VPN clients (Windows/Linux PCs) can be supported. The VPN clients are bridged to the LAN side and are provided an IP address from the LAN subnet which provides the same application experience as if the client device were part of the LAN of the EIGR-VB. This allows passage of multicast and broadcast messages through the VPN tunnel. This facilitates remote access for BACnet systems and eliminates the need for BBMD.

Although the EIGR-VB has many of the same features found in high-end routers, it is simpler to install and commission. A resident DHCP server on the LAN-side will provide IP addresses to LAN-side clients, while a DHCP client on the WAN-side will accept IP address assignments from the attached network. Static addressing is accommodated as well. Configuration is via a web browser using authentication.

*OpenVPN® is a well-supported open-source VPN technology that incorporates SSL/TLS security with encryption.

BridgeVPN

OPENVPN®

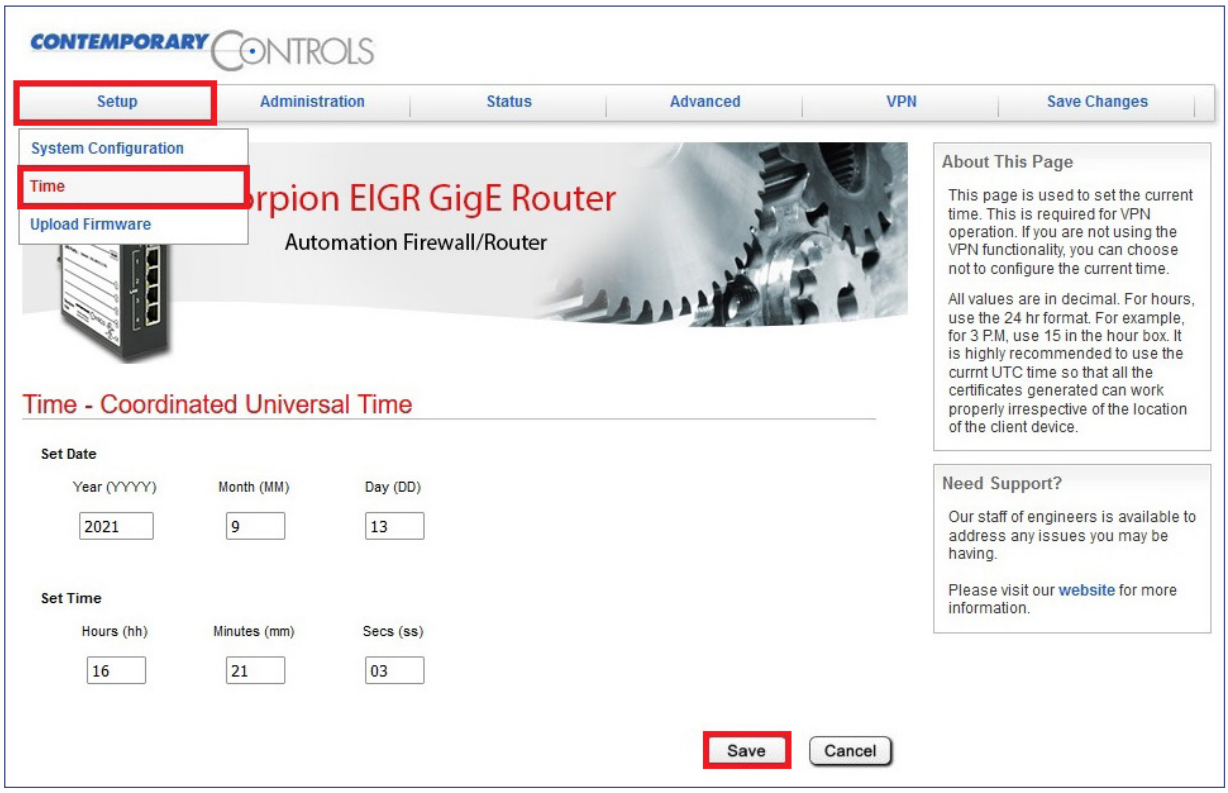
Configure the EIGR-VB to act as a OpenVPN Server

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.

   Click **Save**.



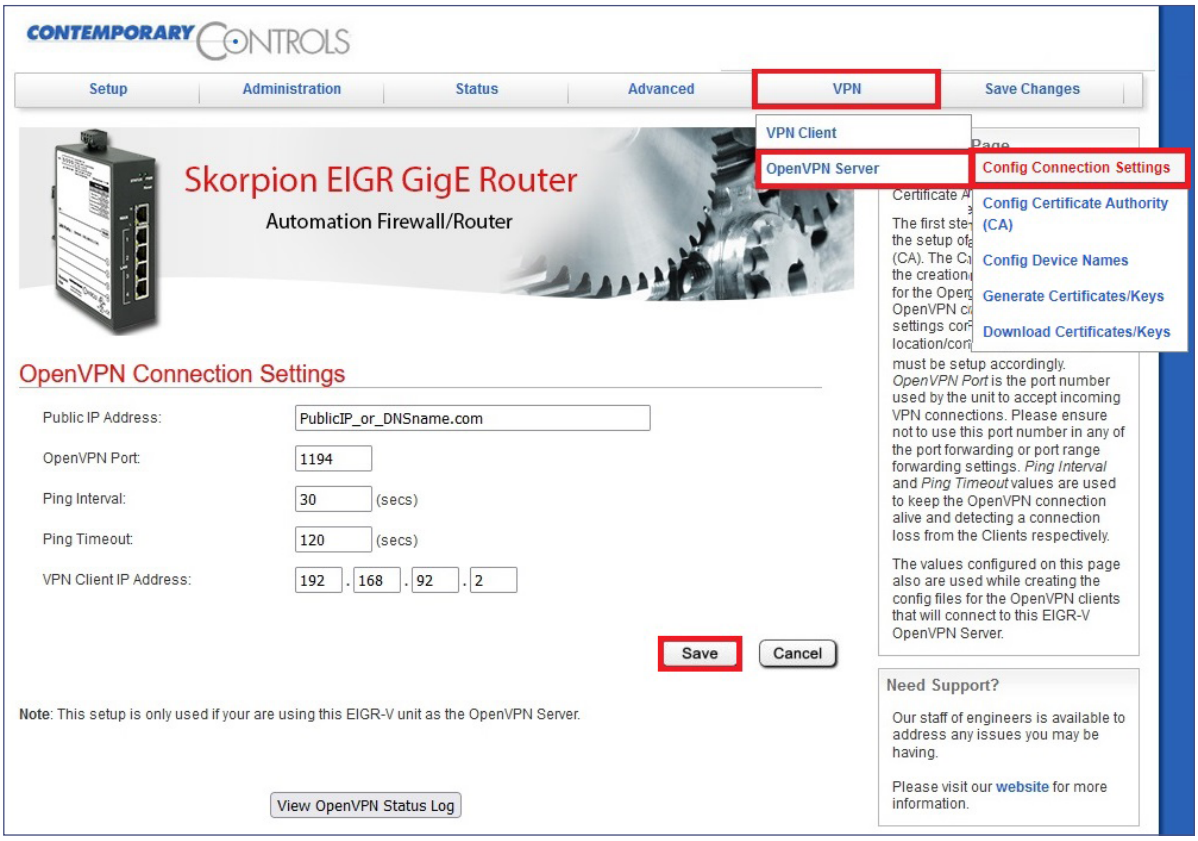
2. Set the Connection Settings

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

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



Ten contiguous IP addresses are reserved for the VPN clients. Please ensure they don't conflict with other devices on the EIGR LAN subnet.

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

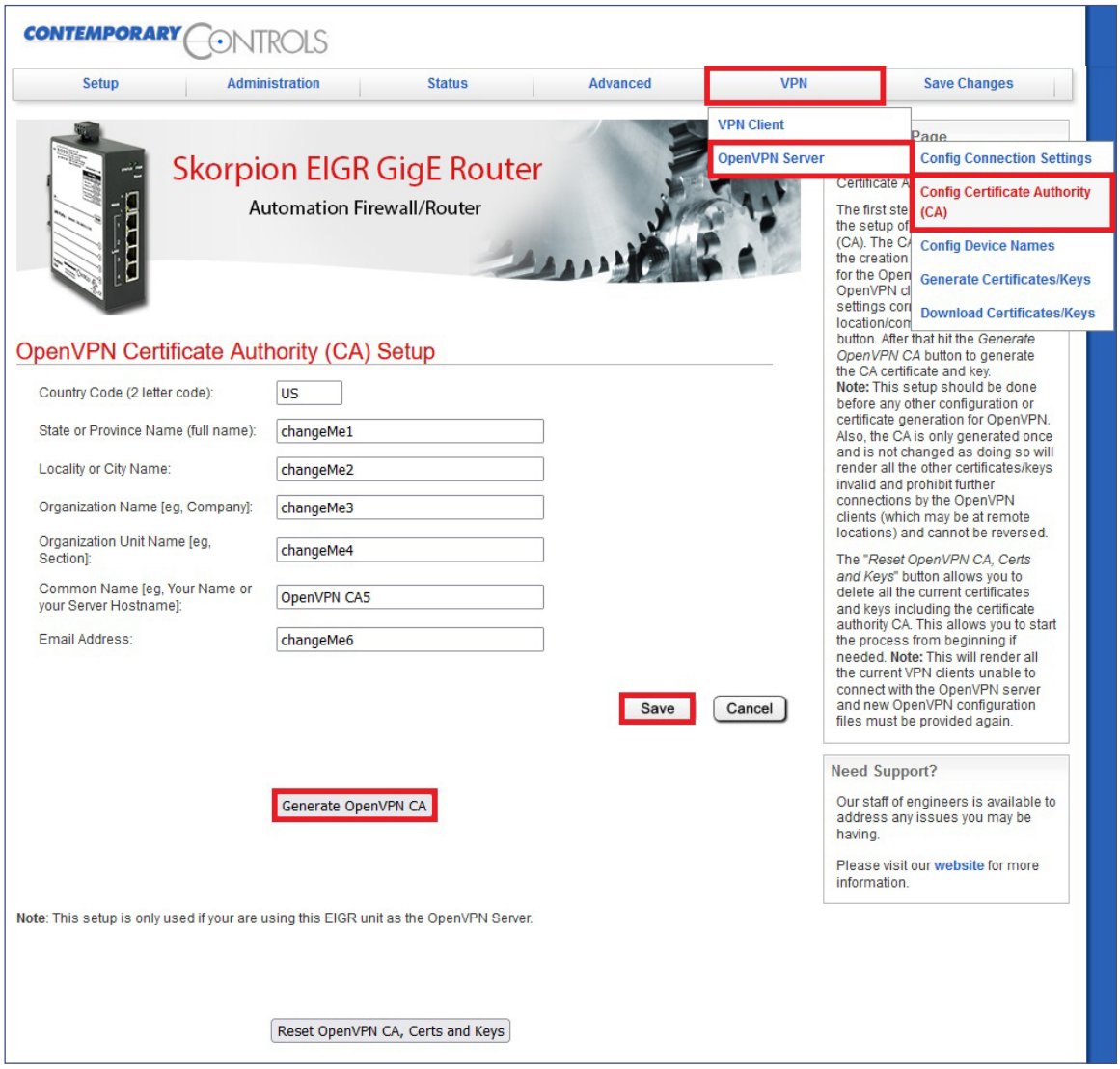
Select the menu option **VPN -> OpenVPN Server -> Config Certificate Authority**.

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.



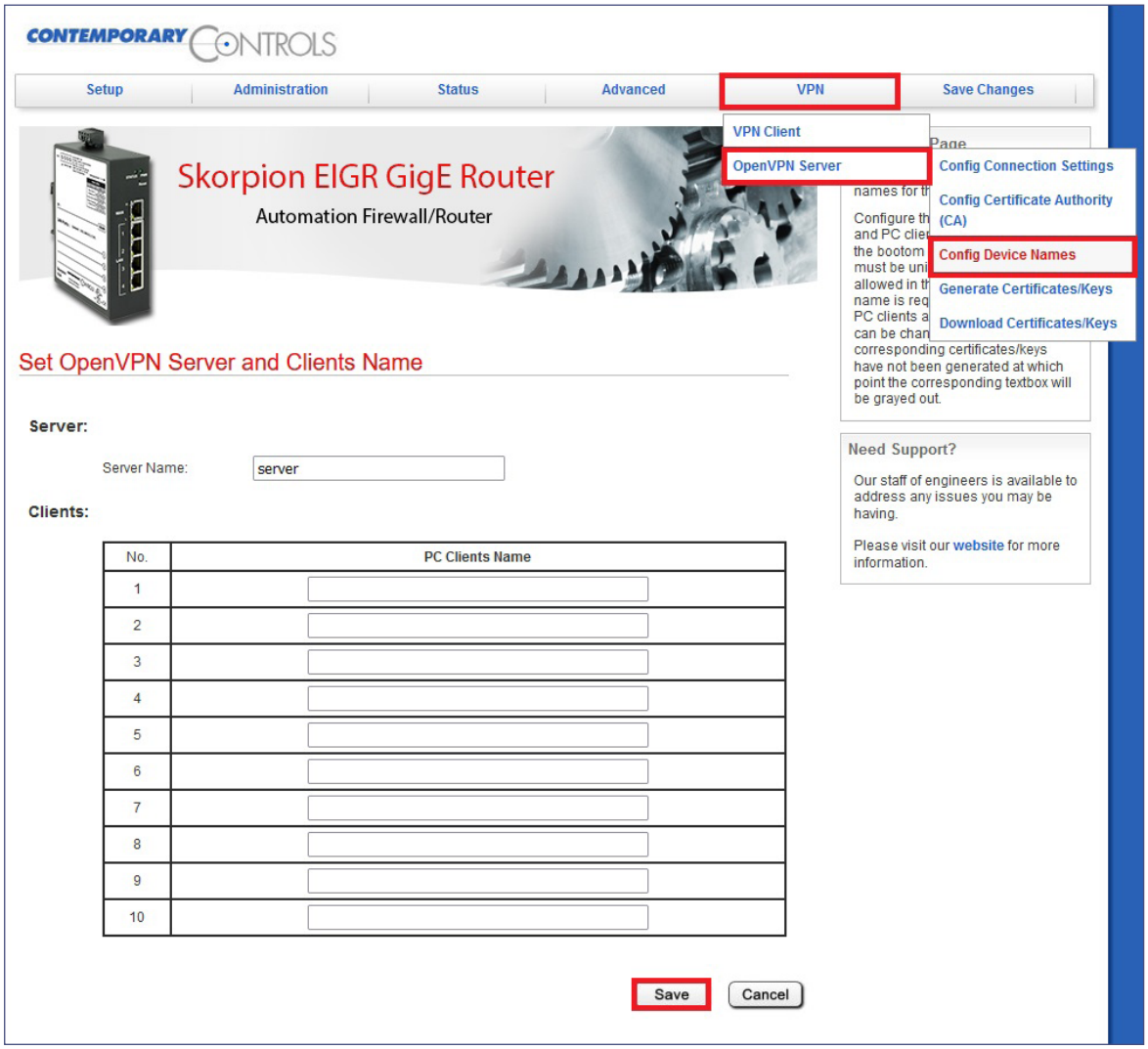
4. Setup the Device Names

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

Set the clients' names for up to 10 clients on PC/tablet/cell phone.

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

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

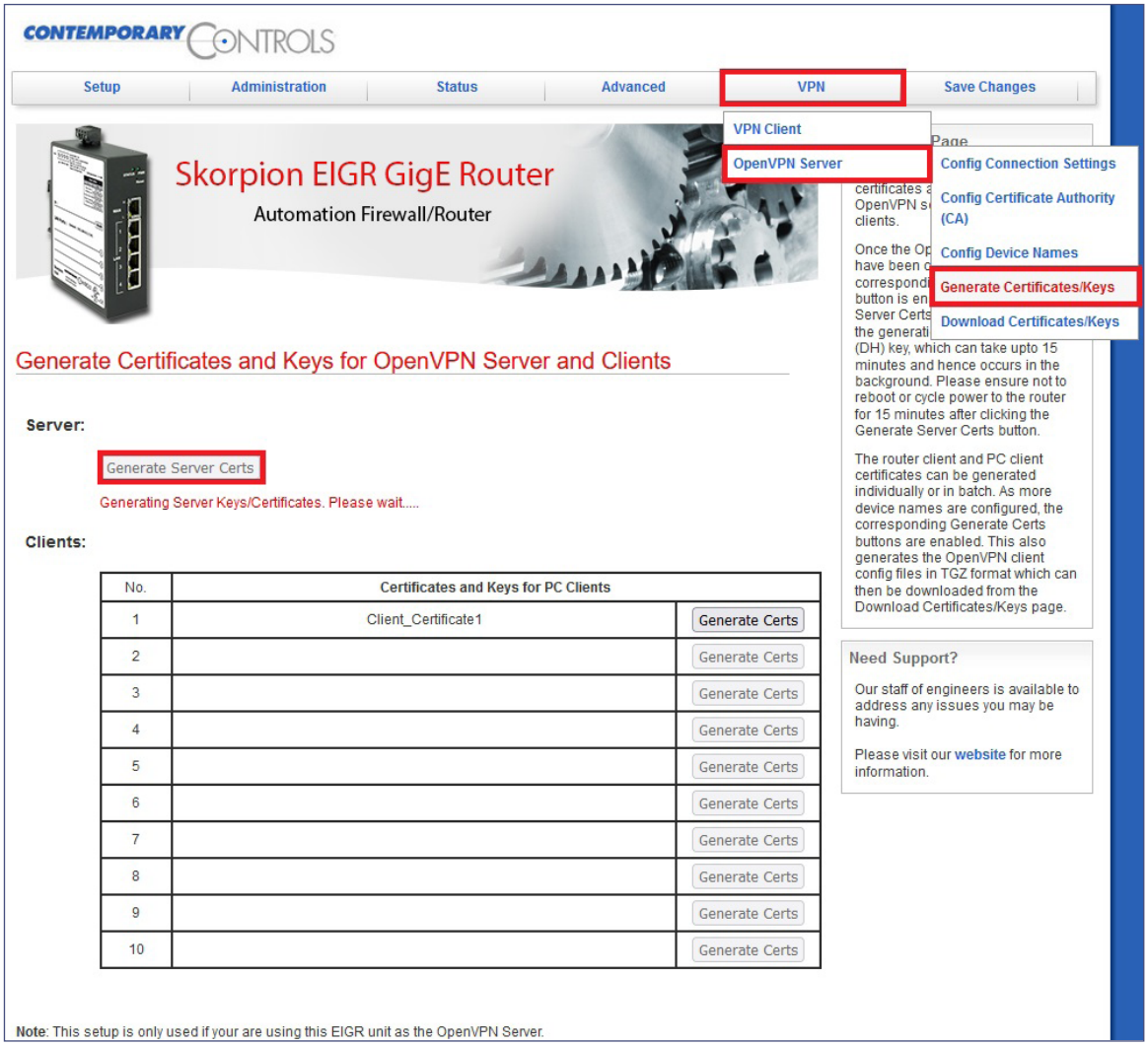


5. Create Server Certificates

Select the menu option **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

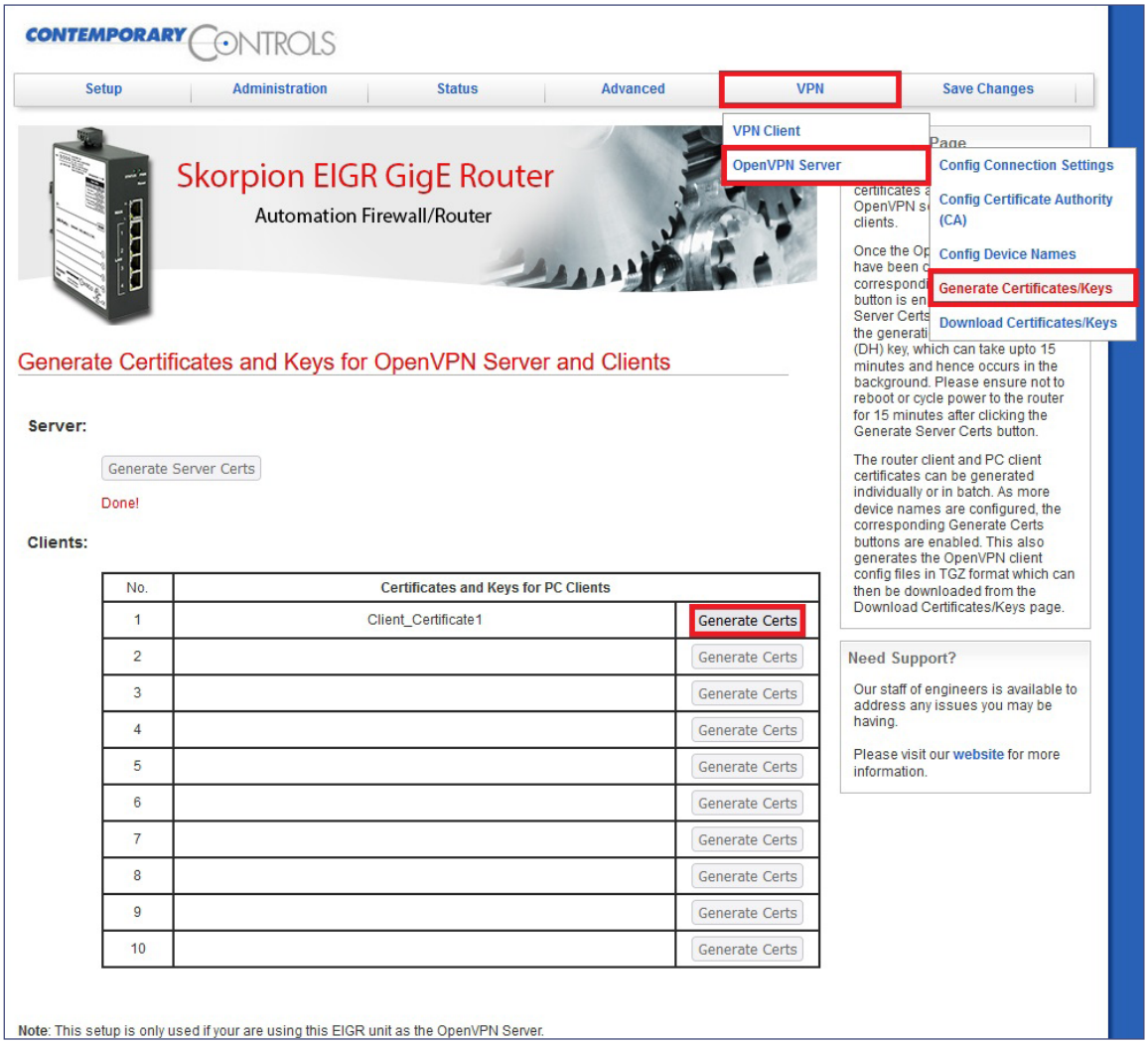
Select the menu option **VPN -> OpenVPN Server -> Create Certificates/Keys**.

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.

Click **Generate Certs**.

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



7. Download Client Certificates

Select the menu option **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.

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

Router .tgz file can be uploaded to EIGR-VB 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 the Mode and Enable VPN

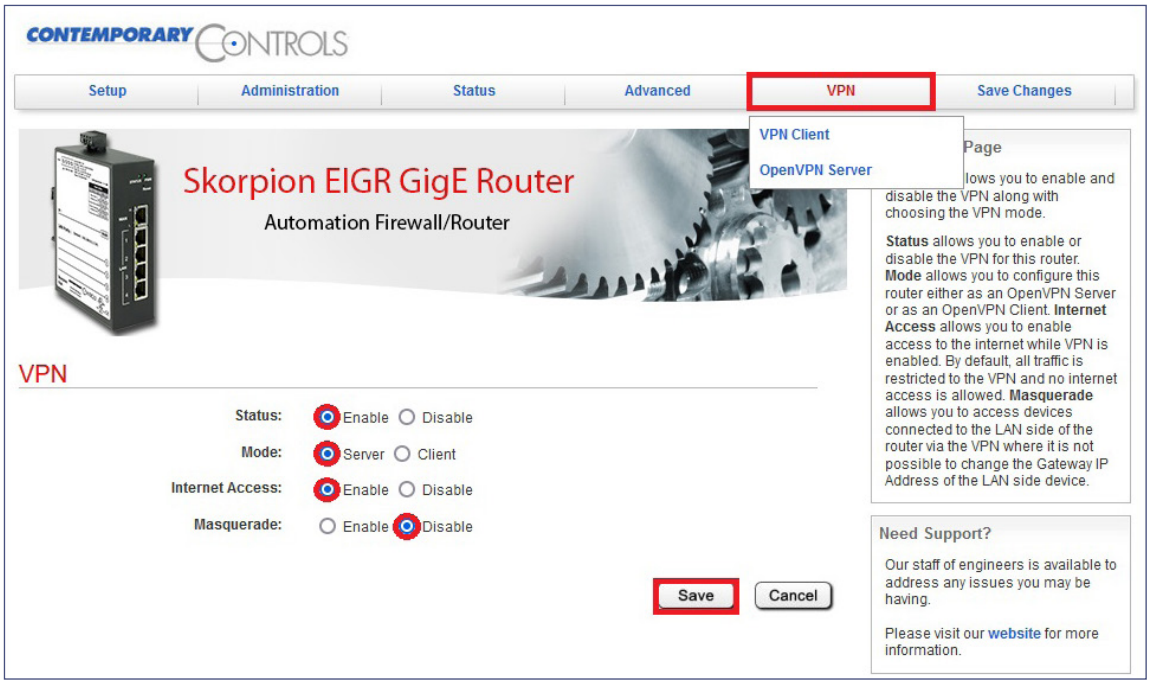
Select the menu option **VPN**.

Set:

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

Note: Masquerade option is only used when the EIGR router is a VPN client.

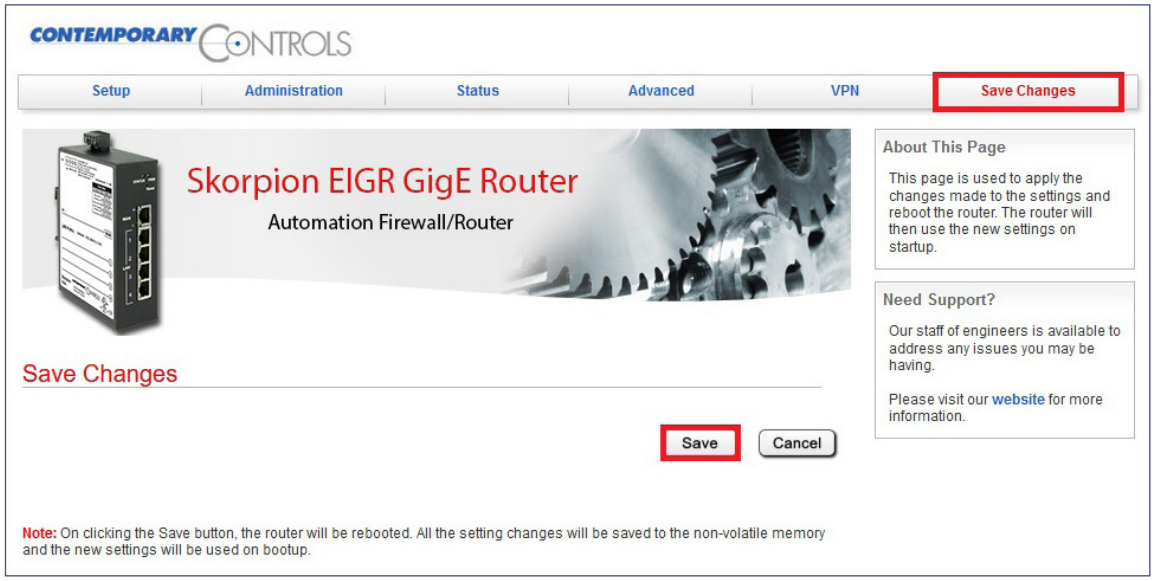
Then, click **Save**.



9. Save Changes and Reboot

Select the menu option **Save Changes**. Then click **Save** to reboot the router.

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

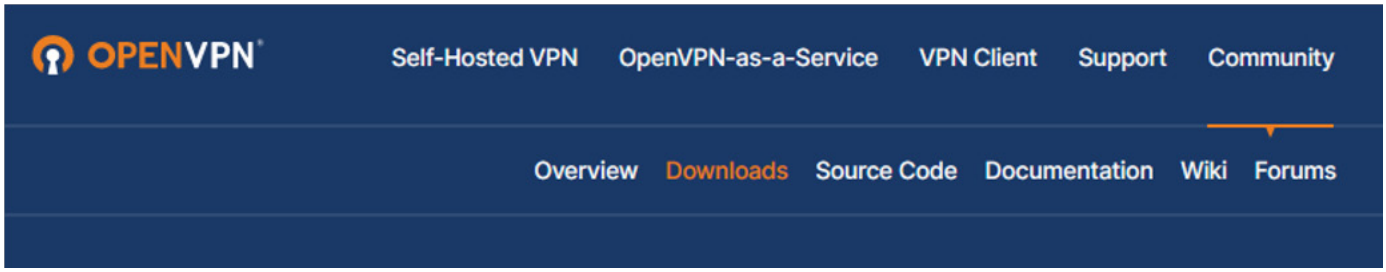


BRIDGEVPN — PC OpenVPN Client Configuration

Windows OpenVPN clients can be downloaded from openvpn.net, Version 2.x which supports TAP adaptors.

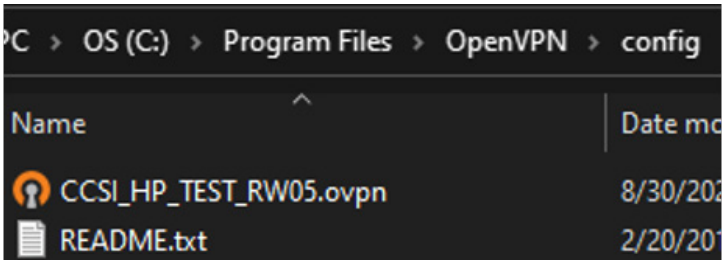
1. OpenVPN PC Client 2.x Download

Go to openvpn.net and click on **Community → Downloads** menu. Install the VPN client. This step is only required once.



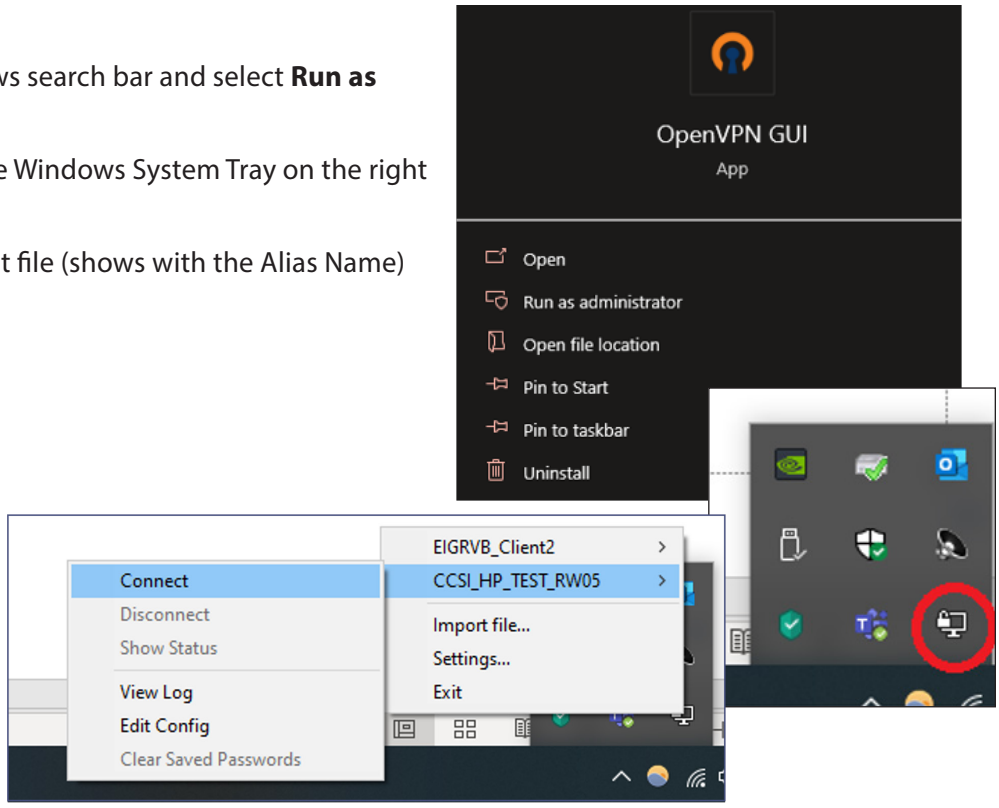
2. Install OpenVPN PC config file

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



3. 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 correct OpenVPN client file (shows with the Alias Name) and click **Connect**.



Note: Bridge Mode uses TAP virtual adapter. Users can access LAN-devices directly using the device address.

- No VPN address involved
- No Masquerade or Gateway IP

Ordering Information

Model	*RoHS*	*Description*
EIGR-VB	✔	Skorpion GigE IP Router with Bridge 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
info@ccontrols.co.uk

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

www.ccontrols.com