



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

Contemporary Controls' EIGR-VB and EIGR-C Skorpion Gigabit IP routers can be configured as a wired and wireless 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 and EIGR-C high-speed routers link 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 EIGR-C routers add support for cellular networks on the WAN side allowing use at sites without Internet access. 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 and EIGR-C incorporate 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 routers include real-time clock and OpenVPN* client/server functionality. The router, set to OpenVPN server

mode and assigned a Static Public IP address, resides at the remote site and uses the Internet for communicating to OpenVPN clients. 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 assigned an IP address from the LAN subnet which provides the same application experience as if the client device were part of the router's LAN. 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 and EIGR-C have many of the same features found in high-end routers, they are 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.



Follow the steps below to configure the EIGR-VB or EIGR-C as an 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**.

The screenshot displays the Contemporary Controls web interface. At the top, the logo "CONTEMPORARY CONTROLS" is visible. Below it, a navigation bar contains tabs for "Setup", "Administration", "Status", "Advanced", "VPN", and "Save Changes". The "Setup" tab is selected and highlighted with a red box. A dropdown menu is open under "Setup", with "Time" selected and highlighted with a red box. Other options in the menu include "System Configuration" and "Upload Firmware". The main content area features a banner for "Corporation EIGR GigE Router" and "Automation Firewall/Router" with an image of a network device. Below the banner, the page title is "Time - Coordinated Universal Time". The "Set Date" section has input fields for Year (2021), Month (9), and Day (13). The "Set Time" section has input fields for Hours (16), Minutes (21), and Seconds (03). At the bottom right, there are "Save" and "Cancel" buttons, with the "Save" button highlighted with a red box. On the right side of the page, there are two informational boxes: "About This Page" explaining the purpose of the page and "Need Support?" providing contact information.

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.

The screenshot displays the 'OpenVPN Connection Settings' page for a 'Skorpion EIGR GigE Router'. The interface features a top navigation bar with tabs for 'Setup', 'Administration', 'Status', 'Advanced', 'VPN', and 'Save Changes'. The 'VPN' tab is active, and a dropdown menu is open, showing 'OpenVPN Server' and 'Config Connection Settings' as selected options. The main content area contains a form with the following fields:

- Public IP Address:
- OpenVPN Port:
- Ping Interval: (secs)
- Ping Timeout: (secs)
- VPN Client IP Address: . . .

A red box highlights the 'Save' button. Below the form, there is a 'View OpenVPN Status Log' button and a note: 'Note: This setup is only used if your are using this EIGR-V unit as the OpenVPN Server.' On the right side, a sidebar contains a 'Need Support?' section and several links: 'Config Certificate Authority (CA)', 'Config Device Names', 'Generate Certificates/Keys', and 'Download Certificates/Keys'.

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.

CONTEMPORARY CONTROLS

Setup Administration Status Advanced **VPN** Save Changes

Skorpion EIGR GigE Router
Automation Firewall/Router

OpenVPN Certificate Authority (CA) Setup

Country Code (2 letter code):

State or Province Name (full name):

Locality or City Name:

Organization Name [eg. Company]:

Organization Unit Name [eg. Section]:

Common Name [eg. Your Name or your Server Hostname]:

Email Address:

Need Support?

Our staff of engineers is available to address any issues you may be having.

Please visit our [website](#) for more information.

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.

CONTEMPORARY CONTROLS

Setup Administration Status Advanced **VPN** Save Changes

Skorpion EIGR GigE Router
Automation Firewall/Router

VPN Client
OpenVPN Server
Config Connection Settings
Config Certificate Authority (CA)
Config Device Names
Generate Certificates/Keys
Download Certificates/Keys

names for th
Configure th
and PC clie
the bootom
must be uni
allowed in th
name is req
PC clients a
can be chan
corresponding certificates/keys
have not been generated at which
point the corresponding textbox will
be grayed out.

Need Support?
Our staff of engineers is available to
address any issues you may be
having.
Please visit our [website](#) for more
information.

Set OpenVPN Server and Clients Name

Server:
Server Name:

Clients:

No.	PC Clients Name
1	<input type="text"/>
2	<input type="text"/>
3	<input type="text"/>
4	<input type="text"/>
5	<input type="text"/>
6	<input type="text"/>
7	<input type="text"/>
8	<input type="text"/>
9	<input type="text"/>
10	<input type="text"/>

Save

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!**

CONTEMPORARY CONTROLS

Setup Administration Status Advanced **VPN** Save Changes

Skorpion EIGR GigE Router
Automation Firewall/Router

Generate Certificates and Keys for OpenVPN Server and Clients

Server:

Generate Server Certs
Generating Server Keys/Certificates. Please wait....

Clients:

No.	Certificates and Keys for PC Clients	
1	Client_Certificate1	Generate Certs
2		Generate Certs
3		Generate Certs
4		Generate Certs
5		Generate Certs
6		Generate Certs
7		Generate Certs
8		Generate Certs
9		Generate Certs
10		Generate Certs

Note: This setup is only used if you are using this EIGR unit as the OpenVPN Server.

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.

CONTEMPORARY CONTROLS

Setup Administration Status Advanced **VPN** Save Changes

Skorpion EIGR GigE Router
Automation Firewall/Router

VPN Client
OpenVPN Server

Generate Certificates/Keys

Generate Certificates and Keys for OpenVPN Server and Clients

Server:

Generate Server Certs

Done!

Clients:

No.	Certificates and Keys for PC Clients	
1	Client_Certificate1	Generate Certs
2		Generate Certs
3		Generate Certs
4		Generate Certs
5		Generate Certs
6		Generate Certs
7		Generate Certs
8		Generate Certs
9		Generate Certs
10		Generate Certs

Note: This setup is only used if you are using this EIGR unit as the OpenVPN Server.

Need Support?

Our staff of engineers is available to address any issues you may be having.

Please visit our [website](#) for more information.

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.

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.

CONTEMPORARY CONTROLS

Setup Administration Status Advanced **VPN** Save Changes

Skorpion EIGR GigE Router
Automation Firewall/Router

Download Certificates and Keys for OpenVPN Clients

No.	PC Clients	
1	Client_Certificate1	Download
2		
3		
4		
5		
6		
7		
8		
9		
10		

Note: This setup is only used if your are using this EIGR unit as the OpenVPN Server.

VPN Client
OpenVPN Server
Config Connection Settings
Config Certificate Authority (CA)
Config Device Names
Generate Certificates/Keys
Download Certificates/Keys

the OpenVPN TGZ format.
Once a client has been generated and provided for this TGZ configuration, certificates can connect to the router.
The router TGZ file can be loaded to an EIPR-V or an EIGR-V router configured as an OpenVPN client. The PC config file needs to be unzipped and the files have to be put in the corresponding folders depending on the device and OS running the OpenVPN client. This may include PCs, laptops, tablets or smartphones.

Need Support?
Our staff of engineers is available to address any issues you may be having.
Please visit our [website](#) for more information.

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**.

The screenshot shows the 'VPN' configuration page for the 'Skorpion EIGR GigE Router'. The interface includes a navigation bar with tabs for Setup, Administration, Status, Advanced, VPN (highlighted), and Save Changes. Below the navigation bar, there is a header for the router model and a description. The main configuration area contains four settings:

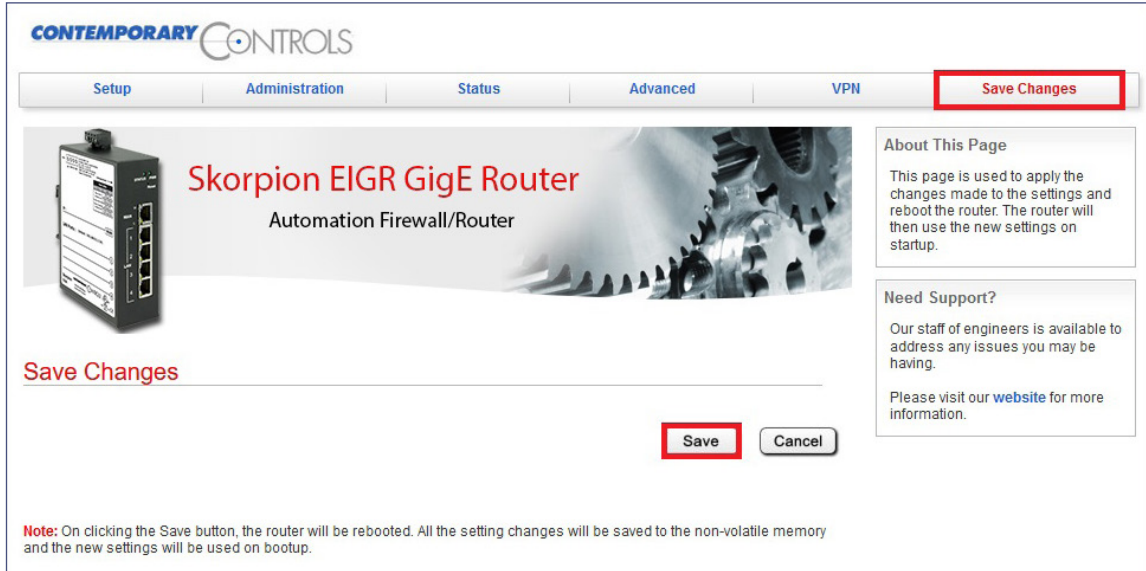
- Status:** Enable Disable
- Mode:** Server Client
- Internet Access:** Enable Disable
- Masquerade:** Enable Disable

At the bottom right of the configuration area, there are two buttons: 'Save' (highlighted with a red box) and 'Cancel'. To the right of the configuration area, there is a 'Need Support?' section with contact information for technical support.

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.

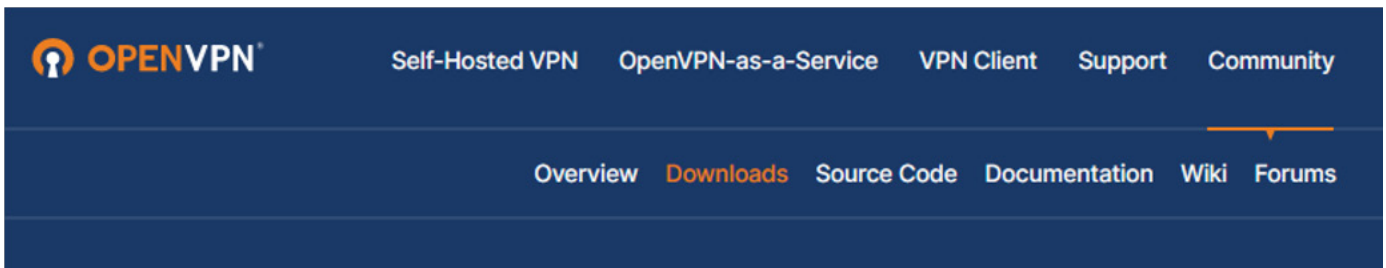


BRIDGEVPN — PC OpenVPN Client Configuration

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

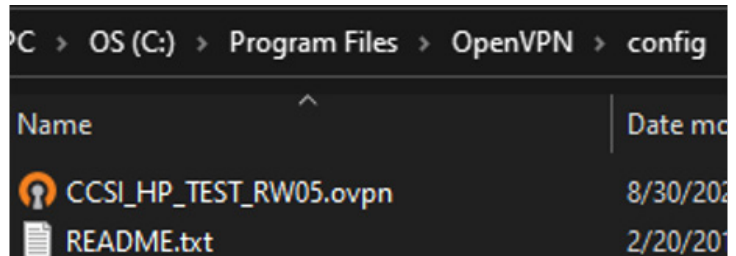
1. OpenVPN PC Client 2.x Download

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



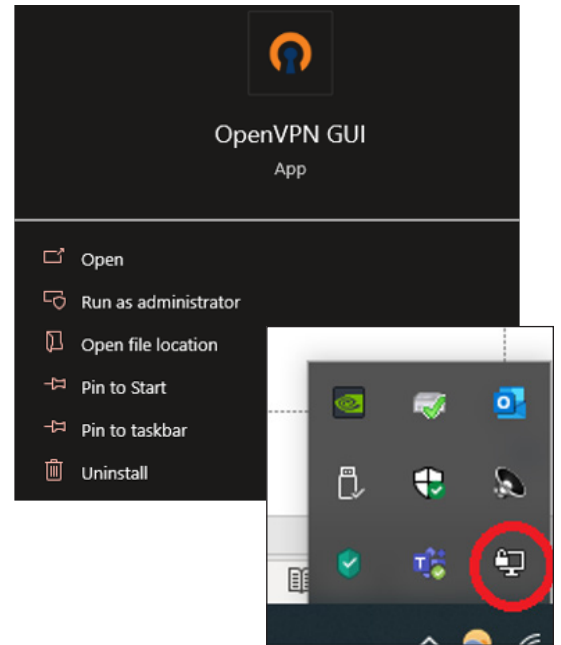
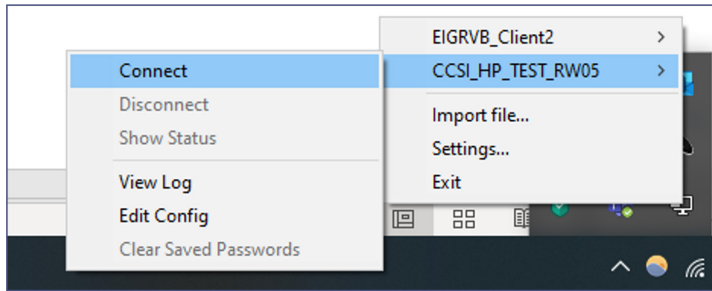
2. Install OpenVPN PC config file

- 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
EIGR-C2	✓	Skorpion GigE IP Router with Cellular (Europe) 0 to 60°C
EIGR-C3	✓	Skorpion GigE IP Router with Cellular (Verizon) 0 to 60°C Note: Two antennas are required but not included. Be sure to purchase two of either AC1Y001J-WHP or AC2H032C-DOM (listed below).
EIGR-C3X	✓	Skorpion GigE IP Router with Cellular (Verizon) –40 to +75°C Note: Two antennas are required but not included. Be sure to purchase two of either AC1Y001J-WHP or AC2H032C-DOM (listed below).
AC1Y001J-WHP		Cellular Straight Stick Whip Antenna
AC2H032C-DOM		Cellular IP67 Outdoor Antenna with 1 meter cable

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