



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.

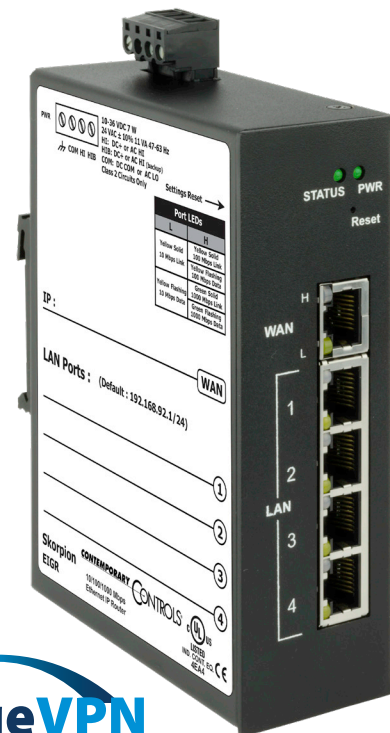
With Port Address Translation (PAT), LAN-side clients can access the Internet. Network Address Translation (NAT) allows a one-to-one translation between LAN-side and WAN-side devices. With Port Forwarding, LAN-side devices can be accessed from the Internet. The EIGR-VB incorporates a four-port Ethernet 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**.

The screenshot displays the Contemporary Controls web interface for a Scorpion EIGR GigE Router. The top navigation bar includes tabs for Setup, Administration, Status, Advanced, VPN, and Save Changes. The Setup tab is active, and a dropdown menu shows 'System Configuration' with 'Time' selected. The main content area is titled 'Time - Coordinated Universal Time' and contains fields for setting the date and time. The date is set to Year (YYYY) 2021, Month (MM) 9, and Day (DD) 13. The time is set to Hours (hh) 16, Minutes (mm) 21, and Seconds (ss) 03. A 'Save' button is highlighted with a red box. On the right, there is an 'About This Page' section explaining the importance of setting the current time for VPN operation and a 'Need Support?' section with contact information.

CONTEMPORARY CONTROLS

Setup Administration Status Advanced VPN Save Changes

System Configuration

Time

Upload Firmware

Scorpion EIGR GigE Router

Automation Firewall/Router

Time - Coordinated Universal Time

Set Date

Year (YYYY) Month (MM) Day (DD)

2021 9 13

Set Time

Hours (hh) Minutes (mm) Secs (ss)

16 21 03

Save **Cancel**

About This Page

This page is used to set the current time. This is required for VPN operation. If you are not using the VPN functionality, you can choose not to configure the current time.

All values are in decimal. For hours, use the 24 hr format. For example, for 3 P.M., use 15 in the hour box. It is highly recommended to use the current UTC time so that all the certificates generated can work properly irrespective of the location of the client device.

Need Support?

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

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

CONTEMPORARY CONTROLS

Setup Administration Status Advanced **VPN** Save Changes

Skorpion EIGR GigE Router
Automation Firewall/Router

OpenVPN Connection Settings

Public IP Address:

OpenVPN Port:

Ping Interval: (secs)

Ping Timeout: (secs)

VPN Client IP Address: . . .

Save **Cancel**

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

[View OpenVPN Status Log](#)

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

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

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

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

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:

Save

Generate OpenVPN CA

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.

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.

The screenshot shows the web interface of the Skorpion EIGR GigE Router. The top navigation bar includes tabs for Setup, Administration, Status, Advanced, and VPN (which is highlighted). Below the navigation bar, there is a dropdown menu for VPN configuration with options: VPN Client, OpenVPN Server (highlighted), Config Connection Settings, Config Certificate Authority (CA), Config Device Names (highlighted), Generate Certificates/Keys, and Download Certificates/Keys. The main content area is titled "Set OpenVPN Server and Clients Name". It features a "Server:" section with a "Server Name:" field containing the text "server". Below this is a "Clients:" section with a table for configuring up to 10 clients. The table has two columns: "No." and "PC Clients Name". At the bottom of the page, there are "Save" and "Cancel" buttons. A "Need Support?" section is visible on the right side of the page.

CONTEMPORARY CONTROLS

Setup Administration Status Advanced **VPN** Save Changes

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

Skorpion EIGR GigE Router
Automation Firewall/Router

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 **Cancel**

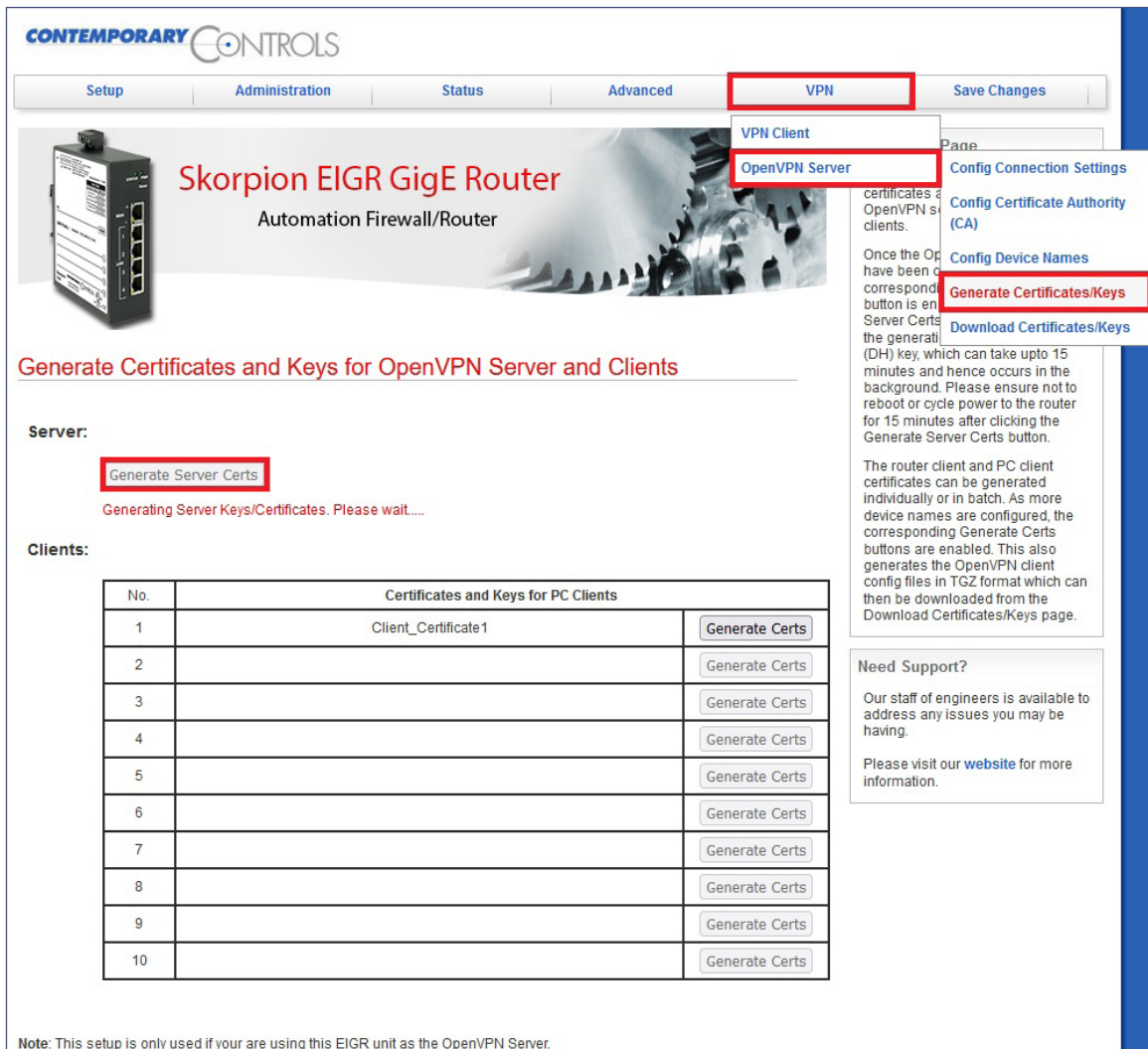
Need Support?
Our staff of engineers is available to address any issues you may be having.
Please visit our [website](#) for more information.

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

VPN Client
OpenVPN Server

Config Connection Settings
Config Certificate Authority (CA)
Config Device Names
Generate Certificates/Keys
Download Certificates/Keys

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.

certificates and OpenVPN server clients.
Once the OpenVPN server has been configured, the corresponding Generate Certs button is enabled. The Generate Server Certs button generates the Diffie-Hellman (DH) key, which can take up to 15 minutes and hence occurs in the background. Please ensure not to reboot or cycle power to the router for 15 minutes after clicking the Generate Server Certs button.
The router client and PC client certificates can be generated individually or in batch. As more device names are configured, the corresponding Generate Certs buttons are enabled. This also generates the OpenVPN client config files in TGZ format which can then be downloaded from the Download Certificates/Keys page.

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

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

Skorpio 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

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.

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.



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		

VPN Client
OpenVPN Server

Config Connection Settings
Config Certificate Authority (CA)
Config Device Names
Generate Certificates/Keys
Download Certificates/Keys

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

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

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**.

CONTEMPORARY CONTROLS

Setup Administration Status Advanced **VPN** Save Changes

Skorpion EIGR GigE Router
Automation Firewall/Router

VPN

Status: ☒ Enable ☐ Disable

Mode: ☒ Server ☐ Client

Internet Access: ☒ Enable ☐ Disable

Masquerade: ☐ Enable ☒ Disable

Save **Cancel**

VPN Client
OpenVPN Server

disables the VPN along with choosing the VPN mode.

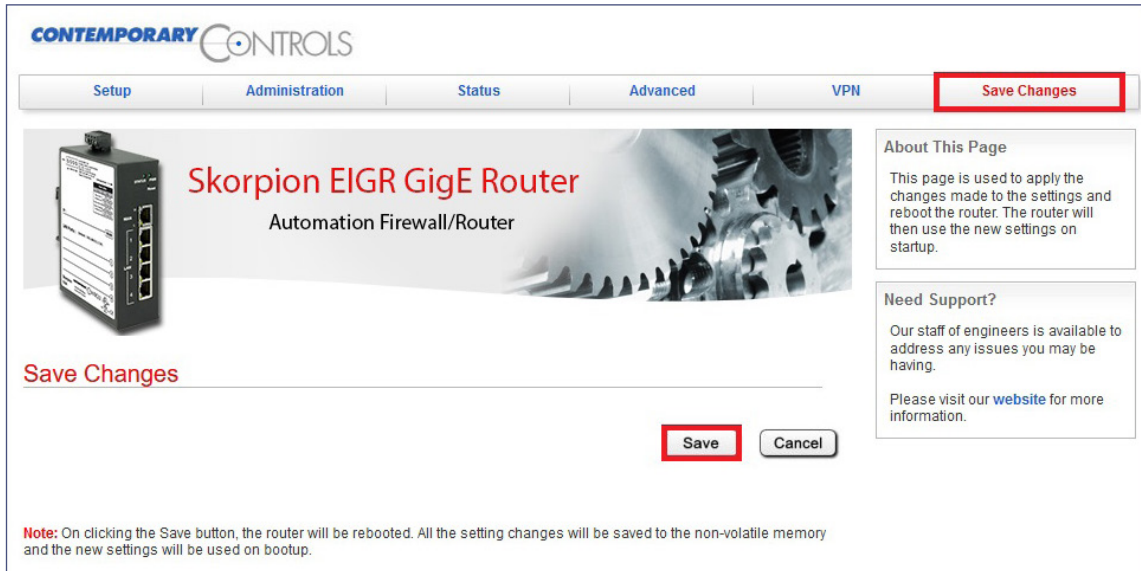
Status allows you to enable or disable the VPN for this router. **Mode** allows you to configure this router either as an OpenVPN Server or as an OpenVPN Client. **Internet Access** allows you to enable access to the internet while VPN is enabled. By default, all traffic is restricted to the VPN and no internet access is allowed. **Masquerade** allows you to access devices connected to the LAN side of the router via the VPN where it is not possible to change the Gateway IP Address of the LAN side device.

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

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.

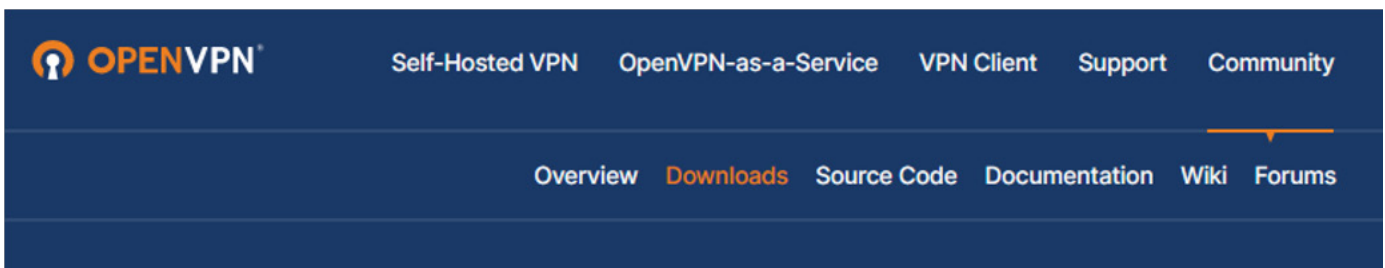


BRIDGEVPN — PC OpenVPN Client Configuration

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

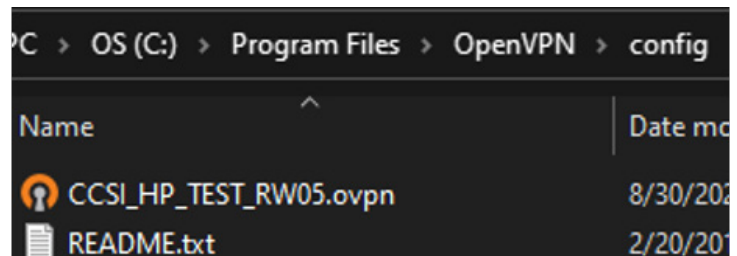
1. OpenVPN PC Client 2.x Download

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



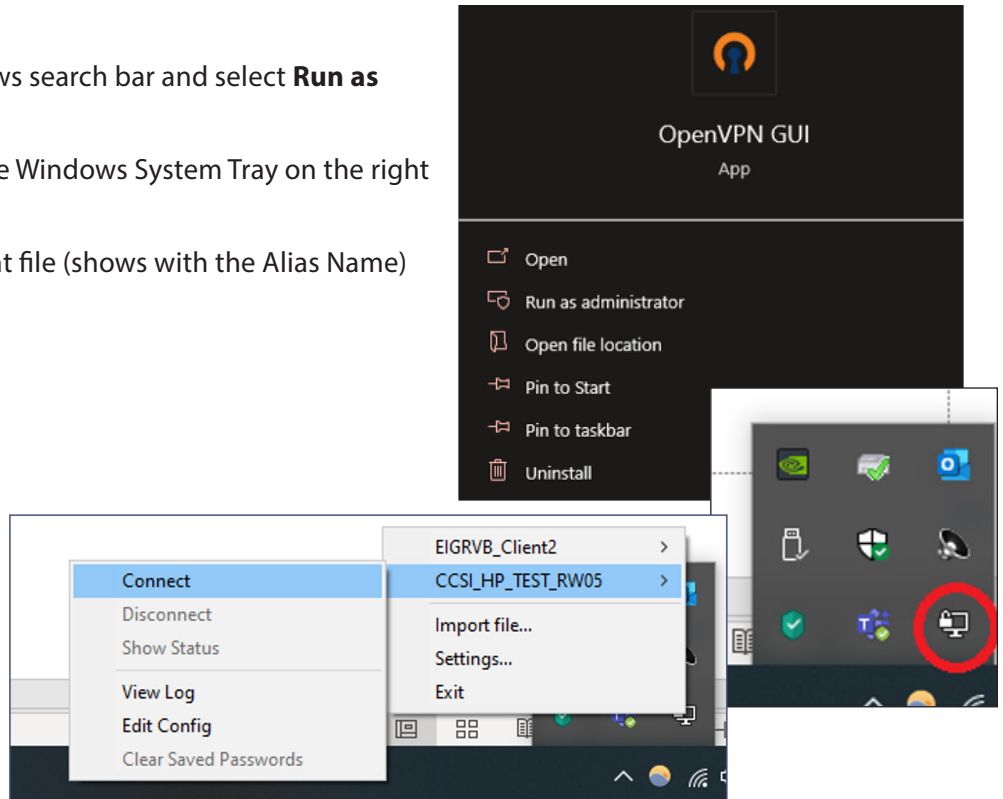
2. Install OpenVPN PC config file

- 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

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