



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.

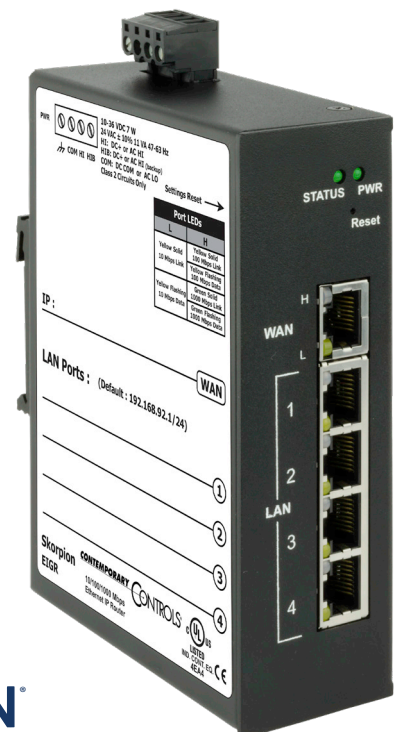
For Self-HostedVPN, users are responsible for setting up a fixed public IP address for the EIGR-V operating as the OpenVPN server. The OpenVPN server router can also be connected behind an existing firewall/router with a public IP and use port forwarding to access the OpenVPN server. This OpenVPN server 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.



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.



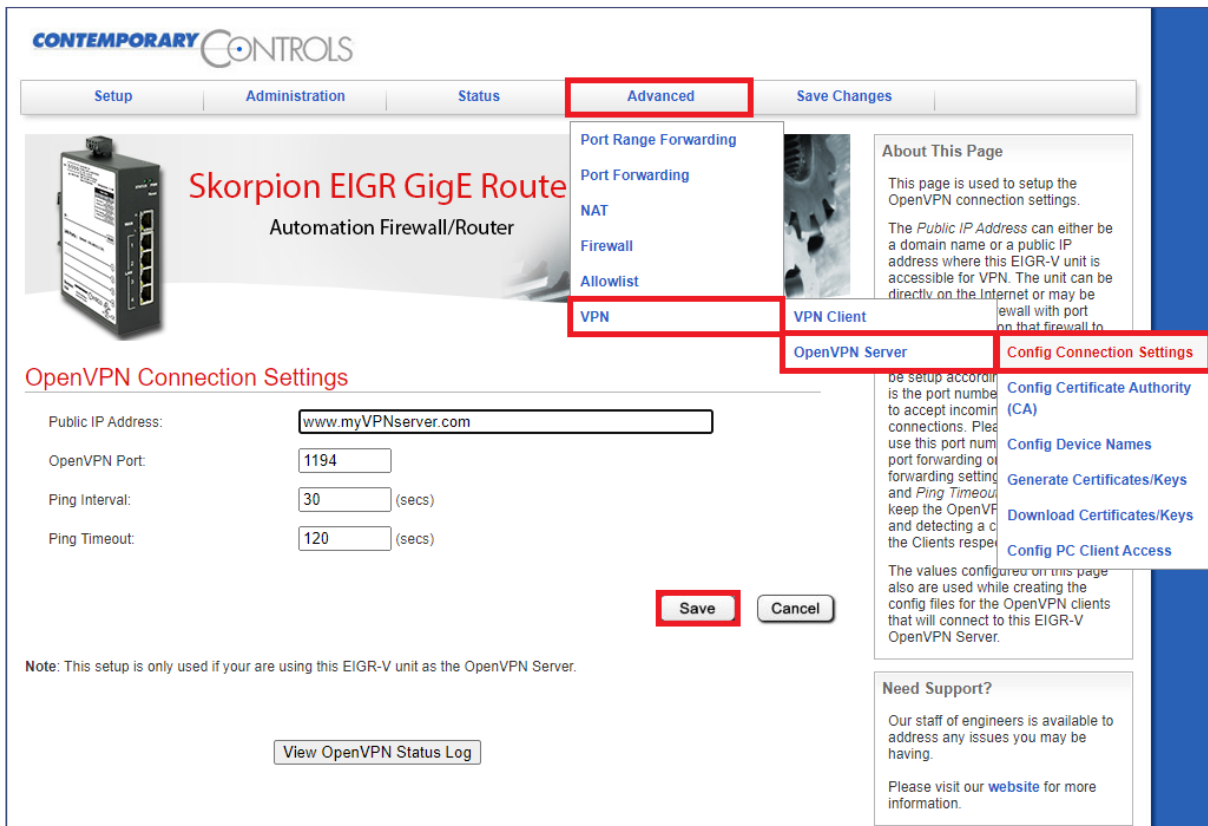
2. Set the Connection Settings

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.

The screenshot displays the 'OpenVPN Certificate Authority (CA) Setup' configuration page. The navigation menu at the top includes 'Setup', 'Administration', 'Status', 'Advanced', and 'Save Changes'. The 'Advanced' menu is expanded, showing options like 'Port Range Forwarding', 'Port Forwarding', 'NAT', 'Firewall', 'Allowlist', 'VPN', 'VPN Client', and 'OpenVPN Server'. The 'VPN' menu is further expanded to show 'OpenVPN Server', which is selected, leading to a sub-menu where 'Config Certificate Authority (CA)' is highlighted. The main content area contains several input fields: 'Country Code (2 letter code):' with 'US', 'State or Province Name (full name):' with 'changeMe1', 'Locality or City Name:' with 'changeMe2', 'Organization Name [eg, Company]:' with 'changeMe3', 'Organization Unit Name [eg, Section]:' with 'changeMe4', 'Common Name [eg, Your Name or your Server Hostname]:' with 'OpenVPN CA5', and 'Email Address:' with 'changeMe6'. Below these fields are 'Save' and 'Cancel' buttons. A 'Generate OpenVPN CA' button is located below the 'Save' button. At the bottom of the page, there is a 'Reset OpenVPN CA, Certs and Keys' button. A 'Need Support?' section is also visible on the right side of the page.

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.

CONTEMPORARY CONTROLS

Setup Administration Status **Advanced** Save Changes

Skorpion EIGR GigE Router
Automation Firewall/Router

Port Range Forwarding
Port Forwarding
NAT
Firewall
Allowlist
VPN
VPN Client
OpenVPN Server
Config Connection Settings
Config Certificate Authority (CA)
Config Device Names
Generate Certificates/Keys
Download Certificates/Keys
Config PC Client Access

Set OpenVPN Server and Clients Name

Server:
Server Name:

Clients:

No.	EIPR/EIGR Router Clients Name
1	<input type="text"/>
2	<input type="text"/>
3	<input type="text"/>
⋮	<input type="text"/>
13	<input type="text"/>
14	<input type="text"/>
15	<input type="text"/>

No.	PC Clients Name
1	<input type="text"/>
2	<input type="text"/>
3	<input type="text"/>
⋮	<input type="text"/>
13	<input type="text"/>
14	<input type="text"/>
15	<input type="text"/>

Save Cancel

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!**

The screenshot shows the 'Advanced' configuration page for the Skorpion EIGR GigE Router. The 'VPN' menu is expanded, and 'OpenVPN Server' is selected. On the 'OpenVPN Server' page, the 'Generate Server Certs' button is highlighted. Below it, a table titled 'Certificates and Keys for EIGR/EIGR Router Clients' is visible, with three rows and a 'Generate Certs' button for each row.

No.	Certificates and Keys for EIGR/EIGR Router Clients	Generate Certs
1		Generate Certs
2		Generate Certs
3		Generate Certs

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.

The screenshot shows the 'Skorpion EIGR GigE Router' configuration page. The 'Advanced' menu is open, showing 'VPN' selected. The 'VPN' sub-menu is also open, showing 'OpenVPN Server' selected. The 'OpenVPN Server' sub-menu is open, showing 'Download Certificates/Keys' selected. The main content area displays 'Download Certificates and Keys for OpenVPN Clients' with two tables for client configurations.

Download Certificates and Keys for OpenVPN Clients

No.	EIPR/EIGR Router Clients	
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		

No.	PC Clients	
1		
2		
3		
4		

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.)

The screenshot shows the Contemporary Controls web interface for a Skorpion EIGR GigE Router. The navigation menu includes Setup, Administration, Status, **Advanced**, and Save Changes. The **Advanced** menu is expanded, showing options like Port Range Forwarding, Port Forwarding, NAT, Firewall, Allowlist, **VPN**, VPN Client, and OpenVPN Server. The **VPN** menu is further expanded to show **OpenVPN Server**, which is then expanded to show **Config PC Client Access**. The main content area is titled "Config VPN Access" and contains a table for configuring access for PC clients to EIGR/EIGR Router Clients.

PC Client	EIGR/EIGR Router Clients
1	<input checked="" type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="button" value="Clear All"/> <input type="button" value="Select All"/> <input type="button" value="Default"/>
2	<input type="checkbox"/> 1 <input checked="" type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="button" value="Clear All"/> <input type="button" value="Select All"/> <input type="button" value="Default"/>
3	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="button" value="Clear All"/> <input type="button" value="Select All"/> <input type="button" value="Default"/>
	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input checked="" type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="button" value="Clear All"/>

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**.

The screenshot shows the 'Advanced' configuration page for the 'Skorpion EIGR GigE Router'. A dropdown menu is open, showing options like 'Port Range Forwarding', 'Port Forwarding', 'NAT', 'Firewall', 'Allowlist', and 'VPN'. The 'VPN' option is highlighted. Below the menu, the 'VPN' configuration section has three radio button options: 'Status' (Enable selected), 'Mode' (Server selected), and 'Internet Access' (Enable selected). At the bottom, the 'Save' button is highlighted with a red box.

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.

The screenshot shows the 'Save Changes' configuration page for the 'Skorpion EIGR GigE Router'. The 'Save Changes' menu option is highlighted. The page contains a warning note: 'Note: On clicking the Save button, the router will be rebooted. All the setting changes will be saved to the non-volatile memory and the new settings will be used on bootup.' The 'Save' button is highlighted with a red box.

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.

The screenshot displays the Contemporary Controls web interface for the Skorpion EIGR GigE Router. The navigation menu at the top includes Setup, Administration, Status, **Advanced**, and Save Changes. The **Advanced** menu is expanded, showing options like Port Range Forwarding, Port Forwarding, NAT, Firewall, Allowlist, **VPN**, and **VPN Client**. The **VPN Client** option is selected, leading to the 'VPN Client Configuration File' section. This section contains two main areas: 'Upload VPN Config to Router' and 'Save RemoteVPN Config to PC'. The 'Upload' section has a 'Choose File' button (highlighted with a red box) and an 'Upload' button (also highlighted with a red box). The 'Save' section has a 'Save' button. Below these, the 'Current VPN Config File Settings' section shows 'Description: No VPN config file.' and fields for 'VPN Server', 'IP Address for VPN Access', and 'IP Address on LAN side'. A right-hand sidebar contains 'About This Page' and 'Need Support?' information.

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**.

The screenshot shows the 'Advanced' configuration page for the 'Skorpion EIGR GigE Router'. A dropdown menu is open, showing options like 'Port Range Forwarding', 'NAT', 'Firewall', 'Allowlist', and 'VPN'. The 'VPN' option is selected and highlighted. Below the menu, the VPN settings are displayed: Status is set to 'Enable', Mode is set to 'Client', and Internet Access is set to 'Enable'. The 'Save' button is highlighted with a red box.

3. Reboot the router

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

The screenshot shows the 'Save Changes' page for the 'Skorpion EIGR GigE Router'. The 'Save Changes' button is highlighted in the top navigation bar. Below the navigation bar, the 'Save Changes' button is highlighted in the main content area. The 'Save' button is highlighted with a red box.

Note: On clicking the Save button, the router will be rebooted. All the setting changes will be saved to the non-volatile memory and the new settings will be used on bootup.

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.

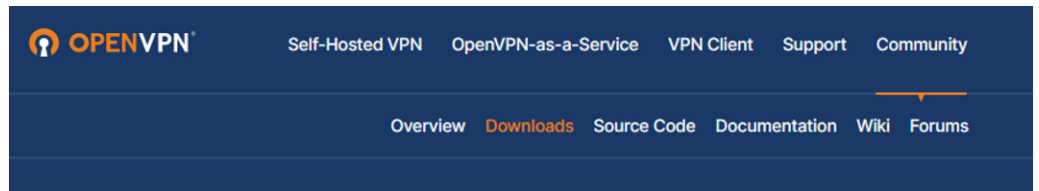
- Unzip the .tgz file.
- Import the .ovpn file to the VPN client.
- For mobile devices (e.g., phone/tablet):
 - Email and save to device.
 - For instructions on how to use an OpenVPN File on Android devices, refer to [Using OpenVPN File on Android](#).
 - For instructions on how to use an OpenVPN File 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.

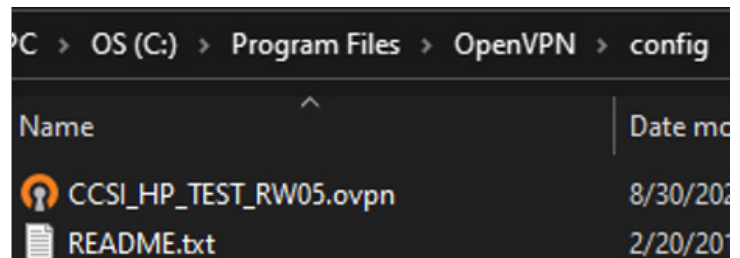
OpenVPN Windows PC Client 2.x Download

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



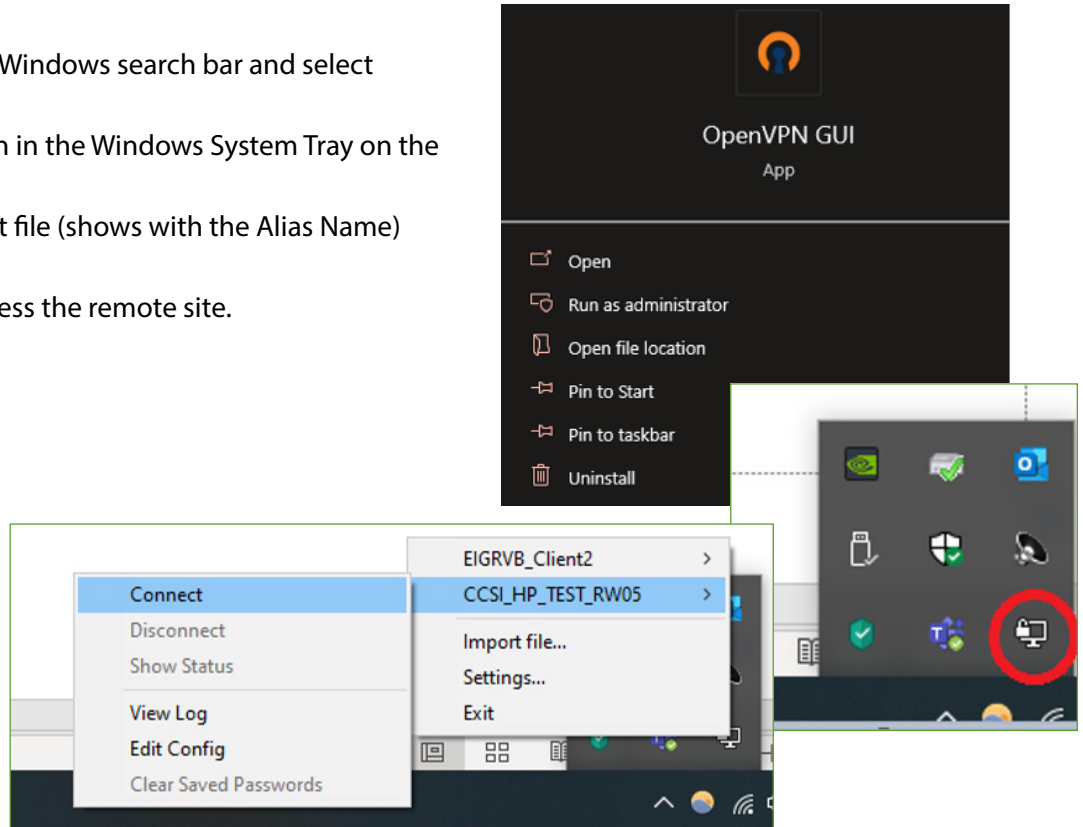
1. Install OpenVPN PC config file

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



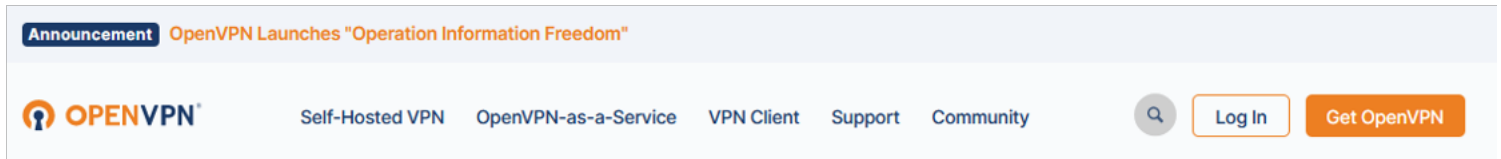
2. Start OpenVPN Client

- 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

<i>Model</i>	<i>RoHS</i>	<i>Description</i>
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

info@ccontrols.co.uk

Germany
Contemporary Controls GmbH

Tel: +49 341 520359 0
 Fax: +49 341 520359 16

info@ccontrols.de

www.ccontrols.com