**Generating a Self-Provisioned OpenVPN Certificate Authority and Configuration File for Server and Clients**

**Products**

This solution works with the following products:

* FlexEdge Server/Client (DA50A and DA70A)
* Ewon (Flexy/Cosy) Client Support is in Progress.
* Windows 10/11 Server/Client
* Debian or RHEL based Linux OS Server/Client (Debian/Ubuntu/RHEL/Fedora/etc.)

**Required Software**

* EZOpenVPNToolkit.exe
* Windows 10/11
* **For FlexEdge Devices:** Crimson 3.2 (Tested working on version 3.2.1028.0)

**Introduction**

Virtual Private Networks (VPNs) provide a secure connection between remote networks. This project uses OpenVPN to facilitate secure communication between Red Lion/HMS Ewon devices (e.g., FlexEdge, Ewon Cosy+, and Flexy) and a Windows or Linux OpenVPN server. This guide outlines setting up a self-managed OpenVPN Certificate Authority (CA), server, and multiple client configurations.

**Quick Setup Overview:**

1. **Run (Double-click) On EZOpenVPNToolkit.exe**
2. **Initialize the OpenVPN Server.**
3. **Generate Additional Client Configurations** as needed.
4. **Revoke Clients** if necessary.
5. **Package Server for Deployment** on Windows/Linux/FlexEdge.
6. **Deploy** OpenVPN on the desired server and client devices.

**Step 1: Run EZOpenVPNToolkit.exe**

1. Double-click on the EZOpenVPNToolkit.exe file.



1. The program will display a menu with the following options:

OpenVPN Setup Menu:

1. Initialize OpenVPN server

2. Generate Additional Client Certificates and Configurations

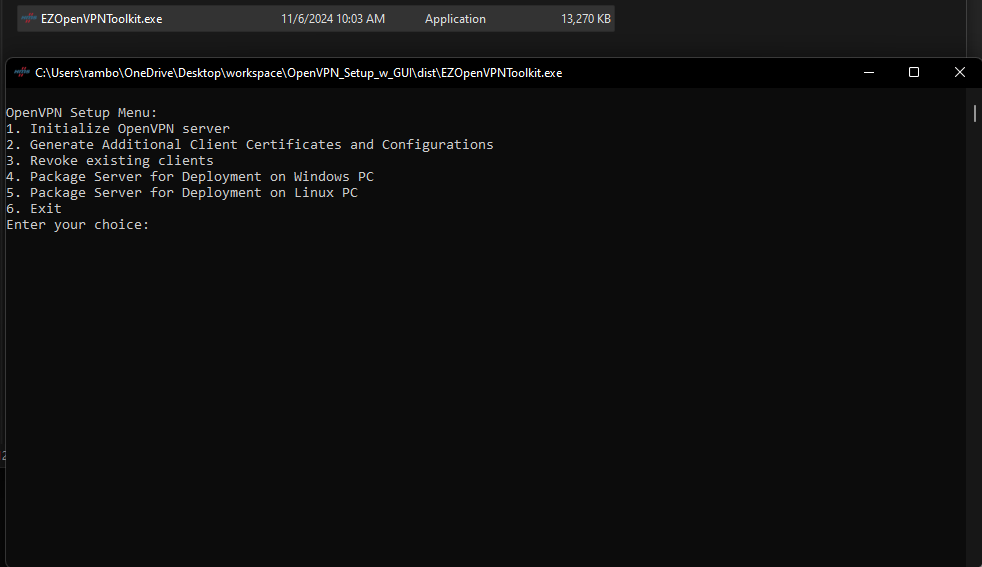
3. Revoke existing clients

4. Package Server for Deployment on Windows PC

5. Package Server for Deployment on Linux PC

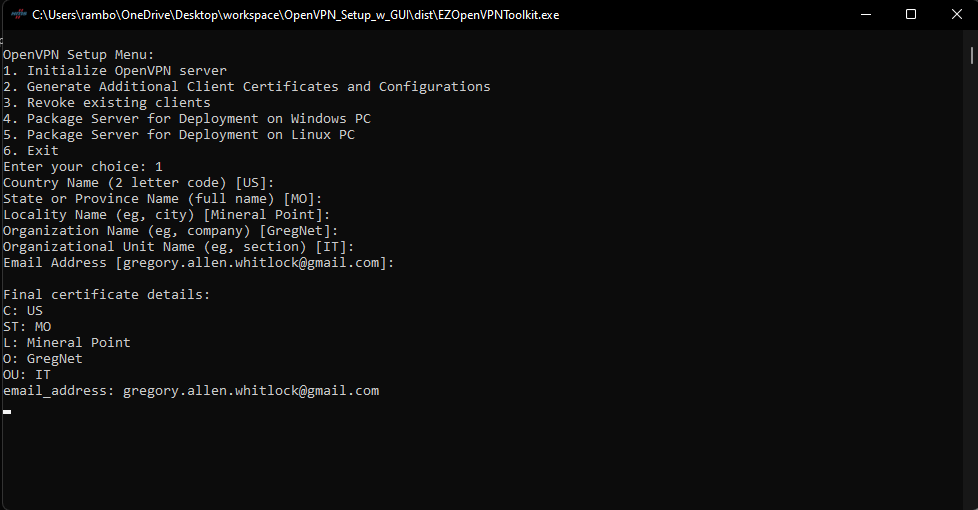
6. Exit

Enter your choice:



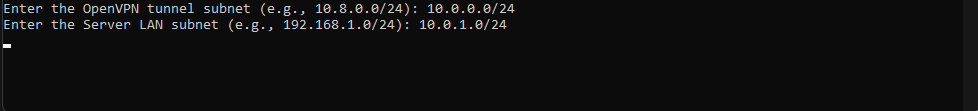
**Step 2: Initialize the OpenVPN Server**

1. **Select Option 1** to initialize the OpenVPN server. This process will prompt you to enter details for the Certificate Authority, such as:
   * Country Code (e.g., US)
   * State or Province Name (e.g., MO)
   * Locality Name (e.g., Mineral Point)
   * Organization Name (e.g., GregNet)
   * Organizational Unit Name (e.g., IT)
   * Email Address (e.g., [gregory.allen.whitlock@gmail.com](mailto:gregory.allen.whitlock@gmail.com))



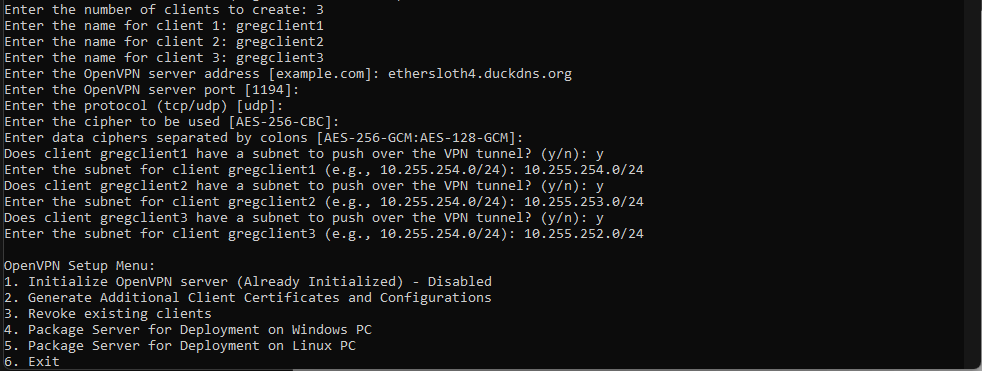
The program will then generate the Certificate Authority files and OpenVPN tunnel configuration, asking for:

* + **OpenVPN Tunnel Subnet** (e.g., 10.0.0.0/24)
  + **Server LAN Subnet** (e.g., 10.0.1.0/24)



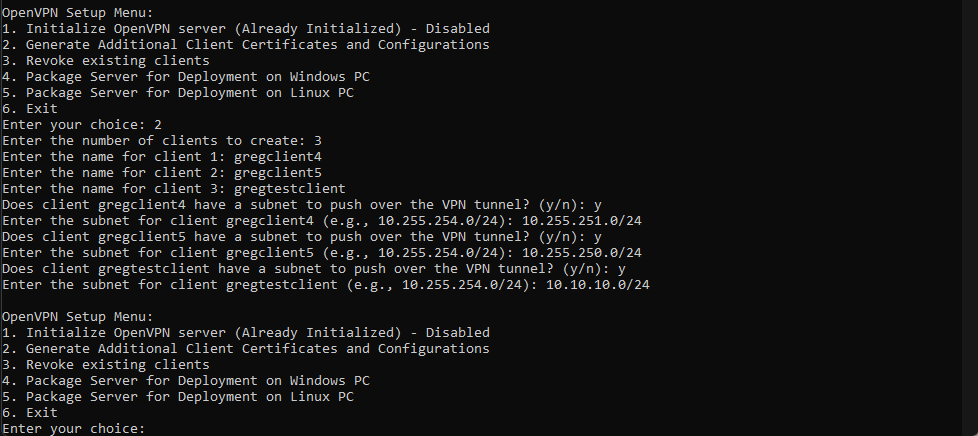
(NOTE: The process may hang here because generating the Diffie-Hellman pem file takes a while)

**Specify Client Details**: Enter the number of clients and provide a unique name for each client. If any client has a unique subnet to push over the VPN tunnel, specify it here. Subnet entries are validated to prevent overlaps.



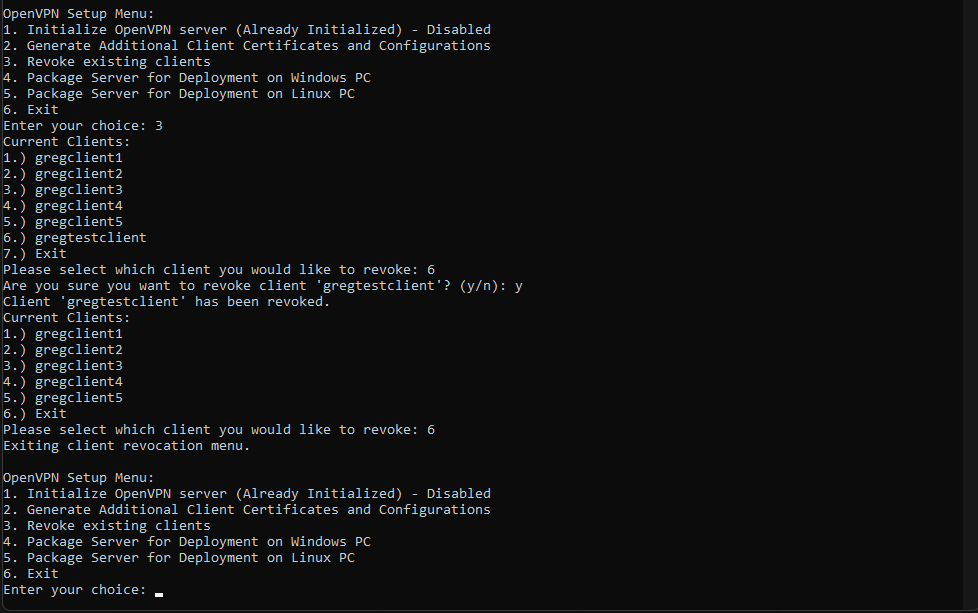
**Step 3: Generate Additional Client Certificates and Configurations**

1. **Select Option 2** from the main menu.
2. Enter the number of clients and their names. If a client needs a specific subnet pushed, you will be prompted to enter it.



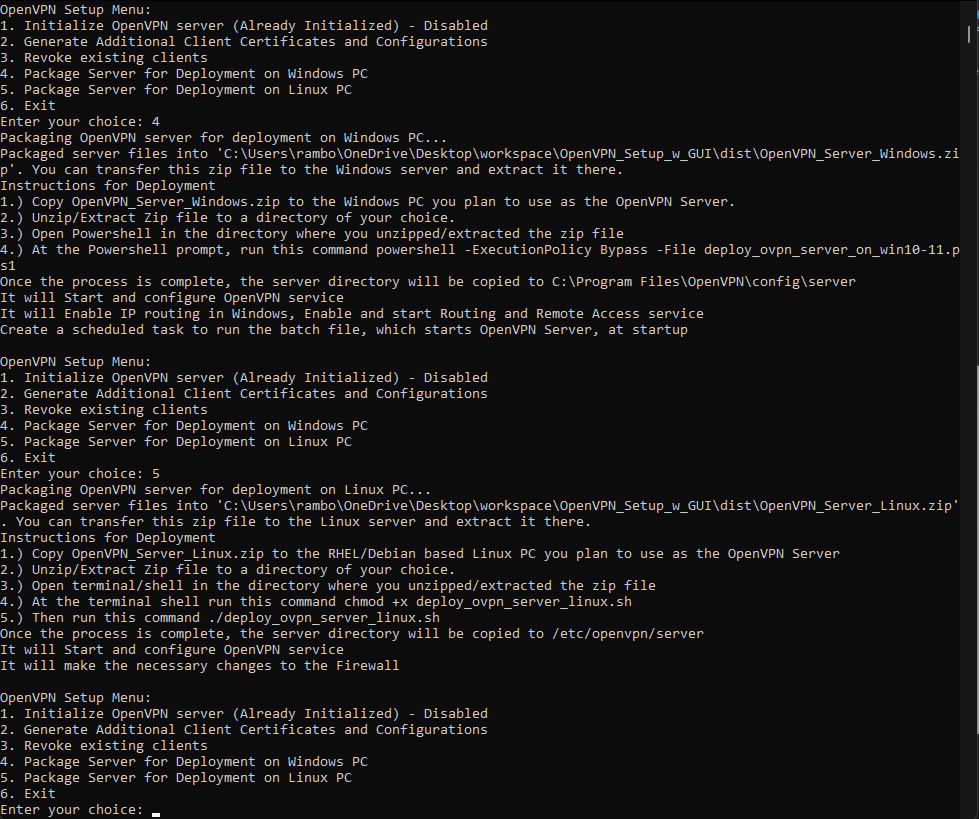
**Step 4: Revoke Existing Clients**

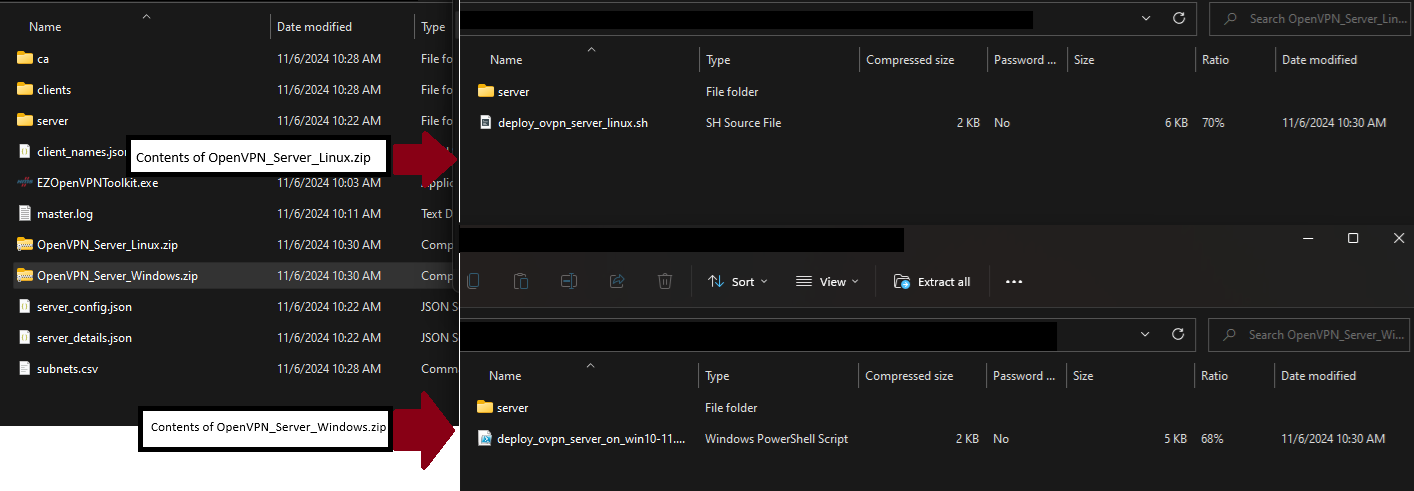
1. **Select Option 3** from the menu.
2. Choose the client you wish to revoke. Confirm the choice, and the client’s configuration, certificates, and routes will be removed from the setup.



**Step 5: Package the Server for Deployment**

1. **Select Option 4** to package the OpenVPN server for Windows or **Option 5** for Linux.
2. A zip file (OpenVPN\_Server\_Windows.zip or OpenVPN\_Server\_Linux.zip) will be generated. Follow the deployment instructions provided by the program to set up the server on your desired platform.





**Step 6: Deploying Server on Windows or Linux**

**For Windows:**

1. Transfer OpenVPN\_Server\_Windows.zip to the Windows server.
2. Extract the zip file to a directory of your choice.
3. Open PowerShell in the extracted directory and run:

powershell -ExecutionPolicy Bypass -File deploy\_ovpn\_server\_on\_win10-11.ps1

1. This process will start the OpenVPN service, enable IP routing, configure Routing and Remote Access, and set up a scheduled task for startup.

**For Linux:**

1. Transfer OpenVPN\_Server\_Linux.zip to the Linux server (tested on Fedora 40 and Debian 12).
2. Extract the zip file and run the following commands:

chmod +x deploy\_ovpn\_server\_linux.sh

sudo ./deploy\_ovpn\_server\_linux.sh

1. The script will install OpenVPN, configure firewall settings, and start the OpenVPN service.

**For FlexEdge**

1. Use Crimson or the Web GUI, navigate to **Device Configuration > Tunnels > OpenVPN Tunnels**, and add the configuration file.
2. Under **Device > Configuration > Software Configuration > VPN1**, select **Tunnel Mode: Config File** and choose the appropriate server configuration.

**Deploying Client Configurations**

**For Windows PC**

1. Copy the client configuration file to C:\Program Files\OpenVPN\config.
2. Open OpenVPN-GUI as administrator, right-click on the icon, select the new configuration, and click **Connect**.

**For FlexEdge**

1. Use Crimson or the Web GUI, navigate to **Device Configuration > Tunnels > OpenVPN Tunnels**, and add the configuration file.
2. Under **Device > Configuration > Software Configuration > VPN1**, select **Tunnel Mode: Config File** and choose the appropriate client configuration.

**Additional Notes:**

* **Server Config Updates**: After each client generation or revocation, the server configuration is updated. Redeploy the server configuration if you’re running it on a separate device.
* **Firewall Configuration**: Ensure that the necessary ports and protocols are open in your firewall settings.