**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)**
* **Anybus Defender**
* 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 the EZOpenVPNToolkit executable Windows is required)

(There is a possibility of Linux Support if requested)

* **For FlexEdge Devices:** Crimson 3.2 (Tested working on version 3.2.1028.0)
* **FTP Client software (I used WinSCP)**

**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

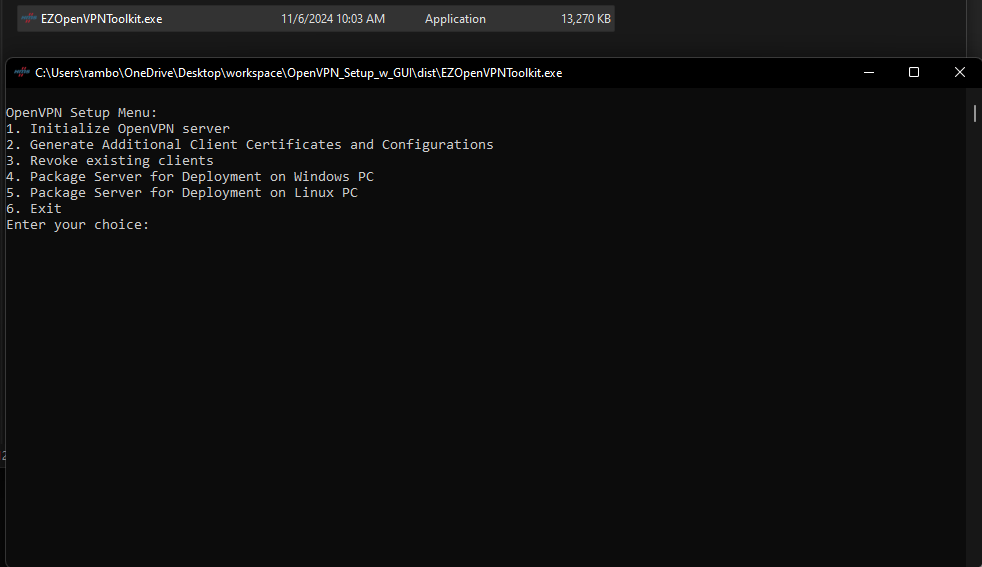
3. Revoke existing clients

4. Package Server for Deployment on Windows PC

5. Package Server for Deployment on Linux PC

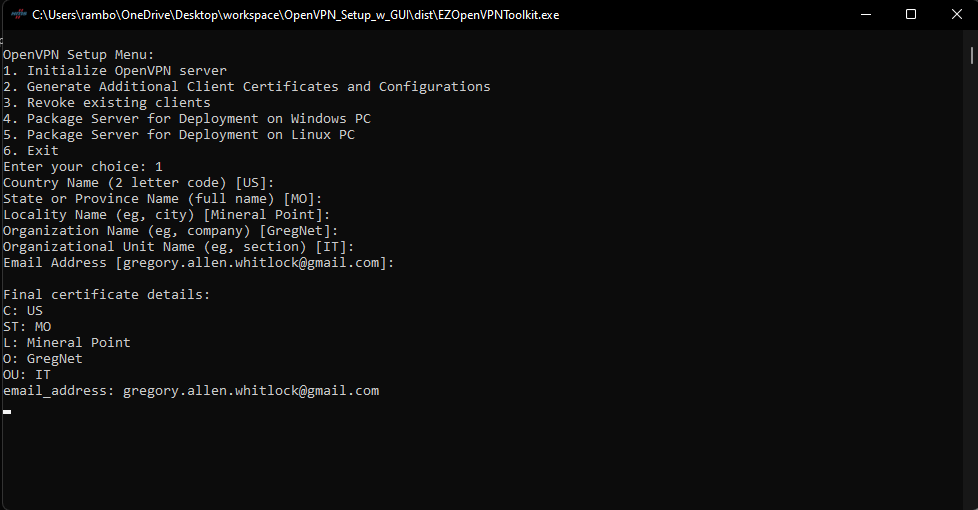
6. Exit

Enter your choice:



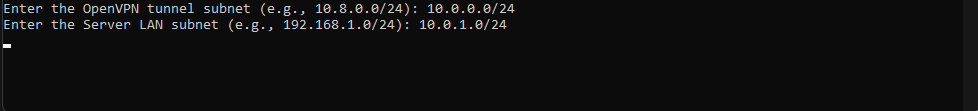
**Step 2: Initialize the OpenVPN Server**

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))



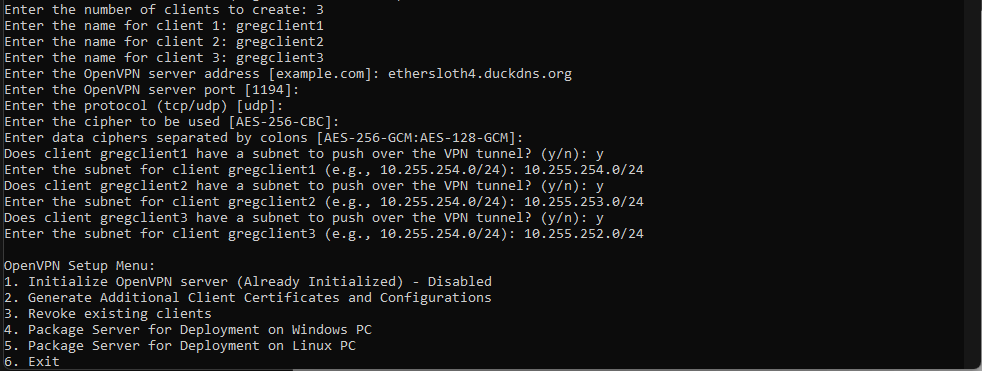
The program will then generate the Certificate Authority files and OpenVPN tunnel configuration, asking for:

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



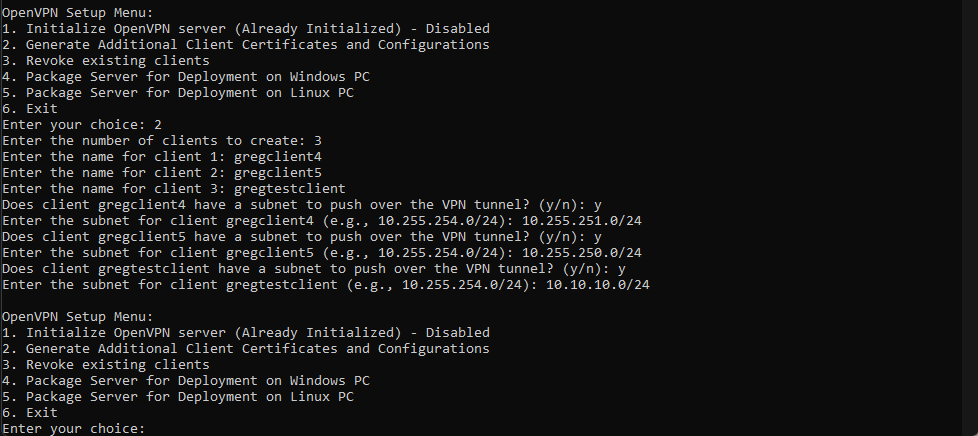
(NOTE: The process may hang here because generating the Diffie-Hellman pem file takes a while)

**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**

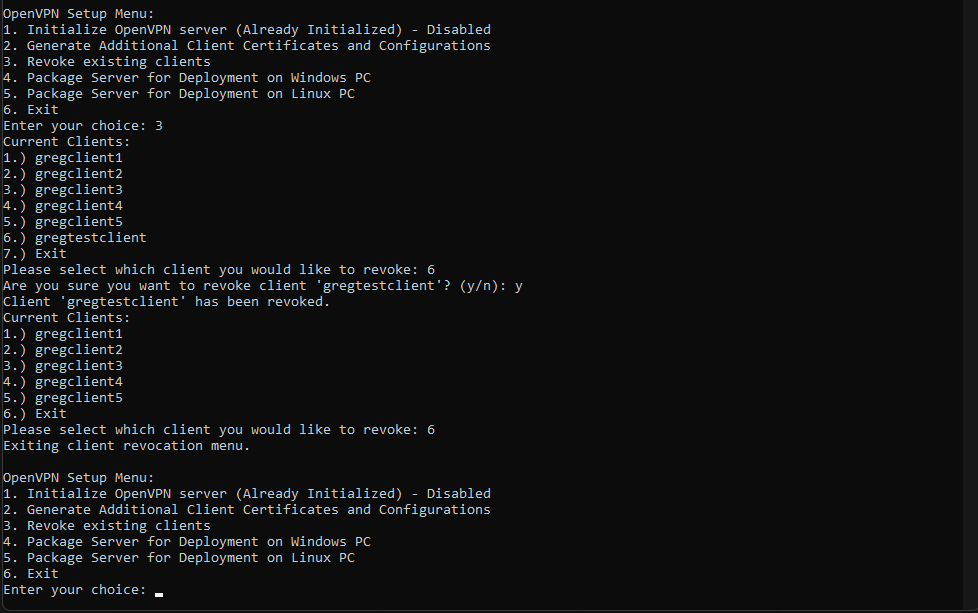
1. **Select Option 2** from the main menu.
2. Enter the number of clients and their names. If a client needs a specific subnet pushed, you will be prompted to enter it.



This will update the crl (certificate revocation list) which will update the server configuration. . This means that if in the future you create any additional clients, you will need to redeploy the server configuration to your chosen OpenVPN server.

**Step 4: Revoke Existing Clients**

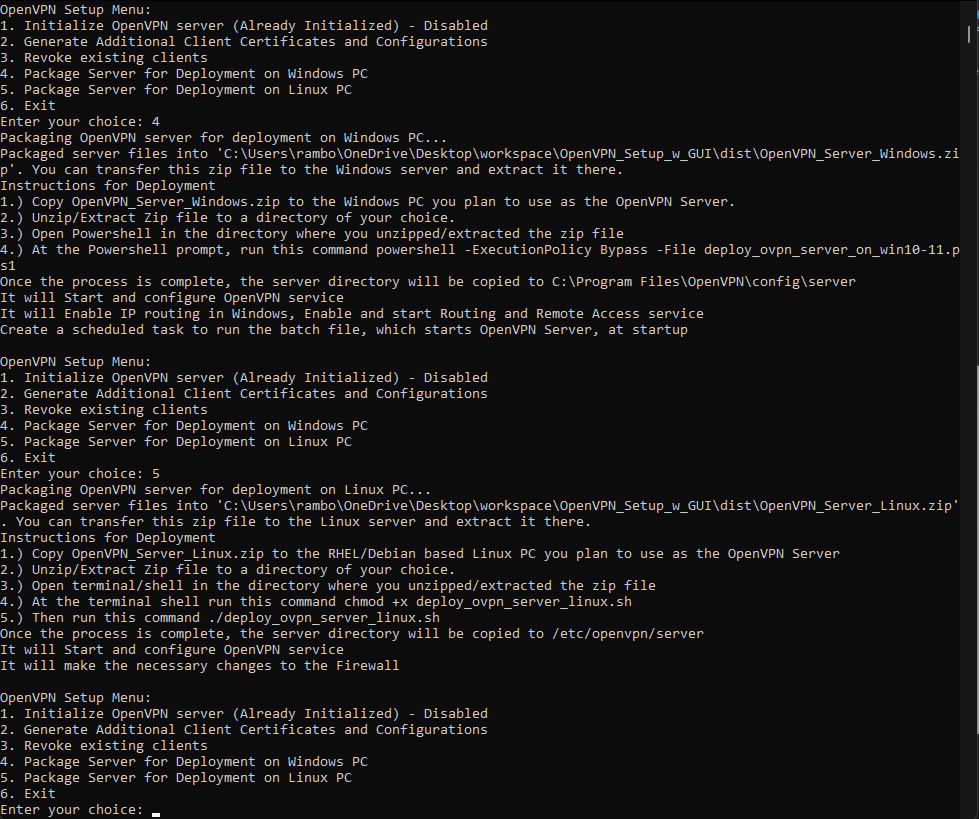
1. **Select Option 3** from the menu.
2. Choose the client you wish to revoke. Confirm the choice, and the client’s configuration, certificates, and routes will be removed from the setup.

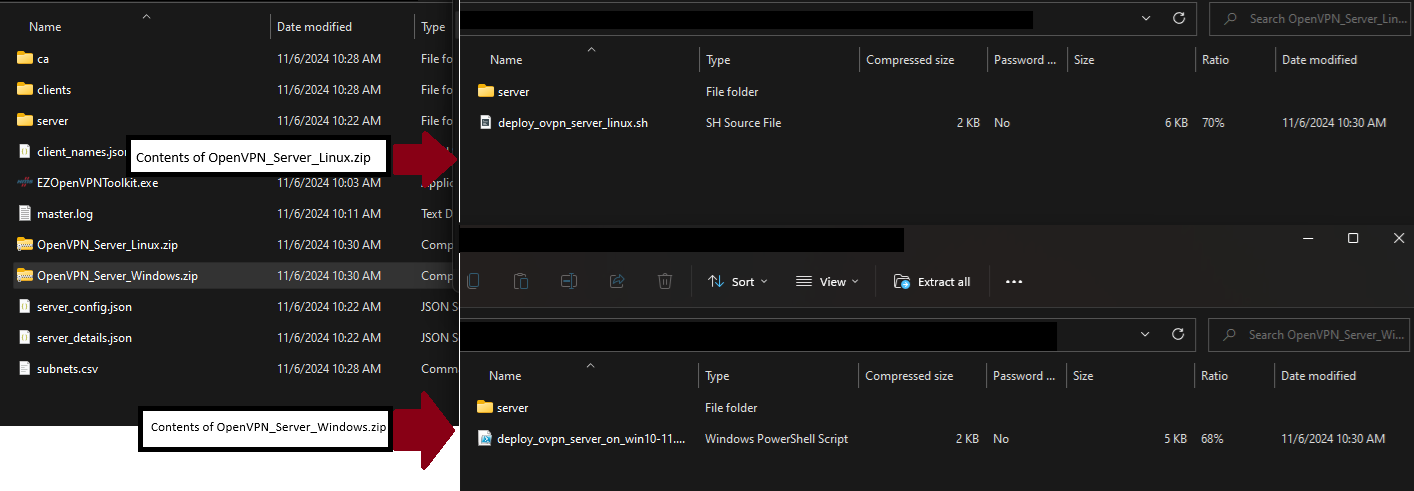


This will revoke the client certs/keys so they can no longer connect to the server. Since this process updates the crl (certificate revocation list) the server.conf file is updated as well. This means that if in the future you revoke any clients, you will need to redeploy the server configuration to your chosen OpenVPN server.

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

1. **Select Option 4** to package the OpenVPN server for Windows or **Option 5** for Linux or Option 6 for FlexEdge
2. A zip file (OpenVPN\_Server\_Windows.zip or OpenVPN\_Server\_Linux.zip or OpenVPN\_Server\_FlexEdge.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:

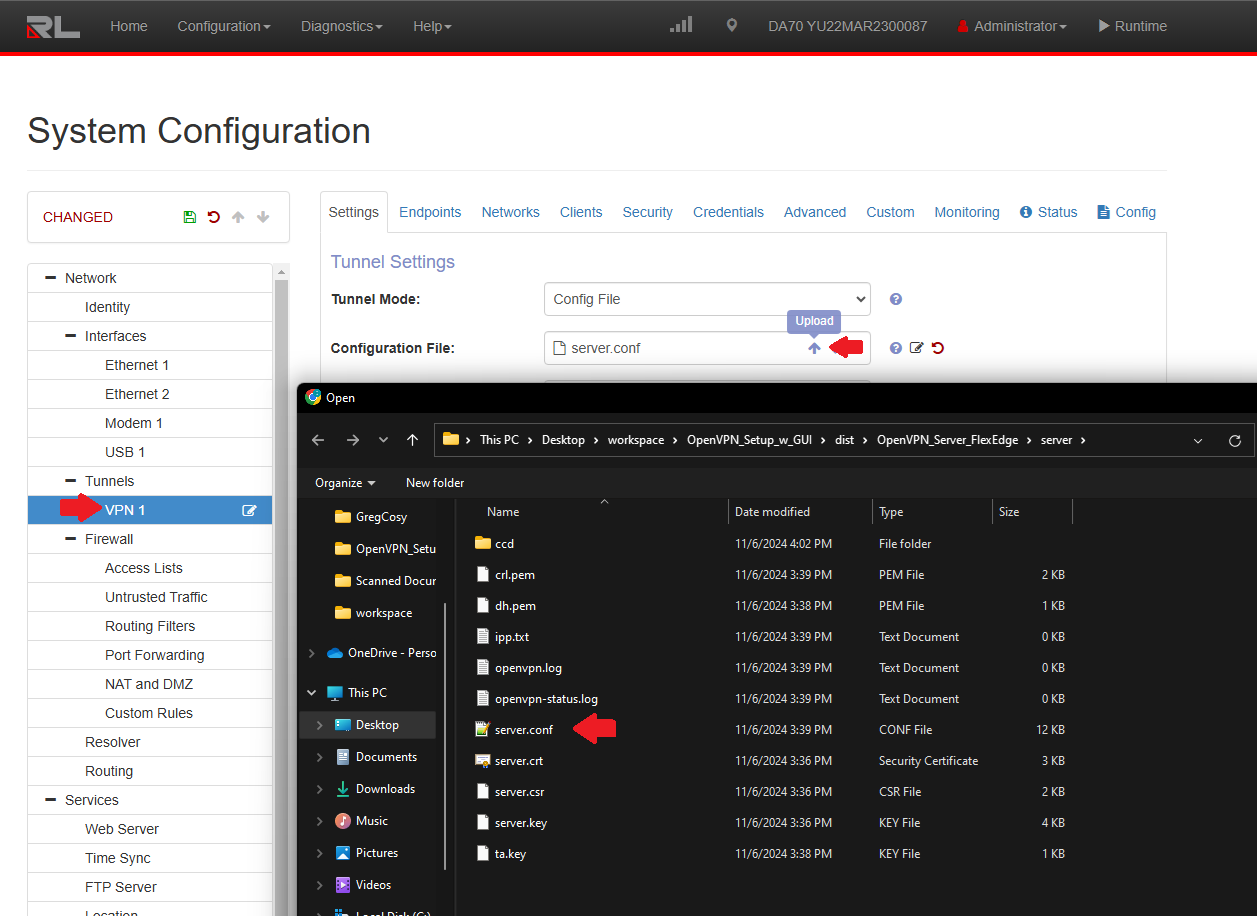
**chmod +x deploy\_ovpn\_server\_linux.sh**

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

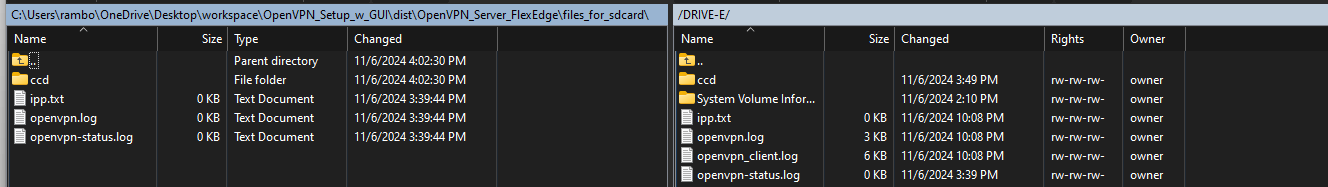
1. The script will install OpenVPN, configure firewall settings, and start the OpenVPN service.

**For FlexEdge**

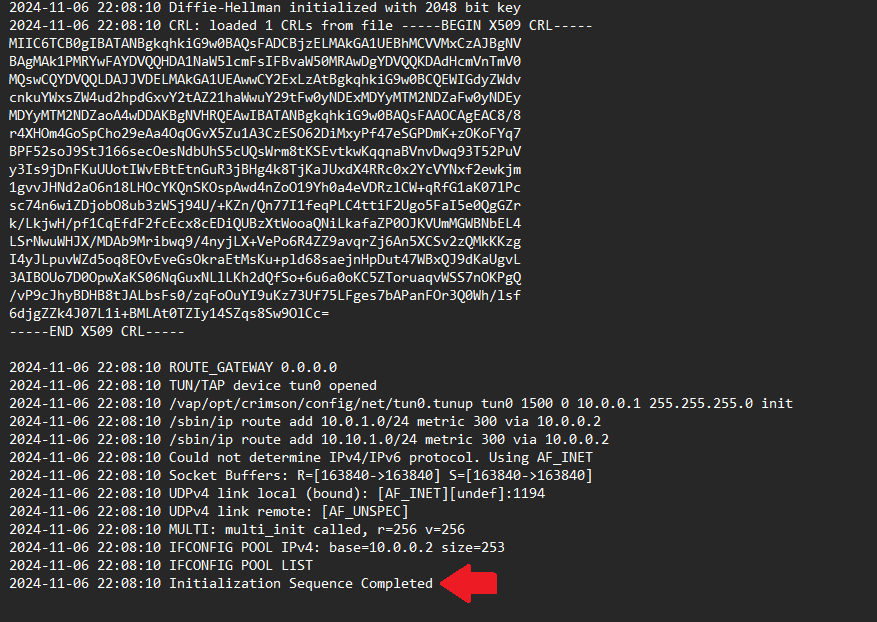
1. Locate the OpenVPN\_Server\_FlexEdge.zip archive and extract it to a folder of your choice
2. You will now have two subfolders files\_for\_sdcard and server
3. The server.conf file is in this server folder
4. Use Crimson or the Web GUI, navigate to **Device Configuration > Tunnels > OpenVPN Tunnels**, and add the configuration file.
5. Under **Device > Configuration > Software Configuration > VPN1**, select **Tunnel Mode: Config File** and choose the appropriate server configuration.



1. Get a microSD card (~32GB worked for me, format as Fat32) copy all files and folders in the files\_for\_sdcard folder to the root of the microSD card.



1. Insert the microSD card into the FlexEdge and then power it on.

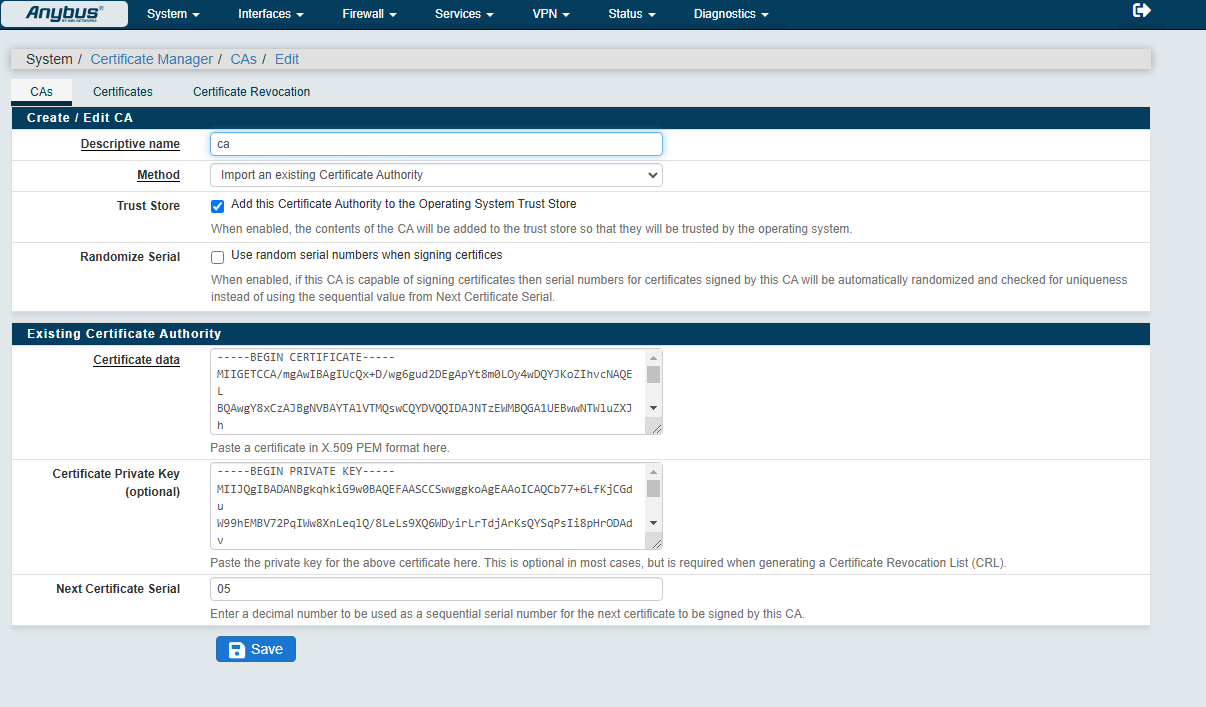


As you can see from the above screenshot, the server config is now initialized and waiting for client connections

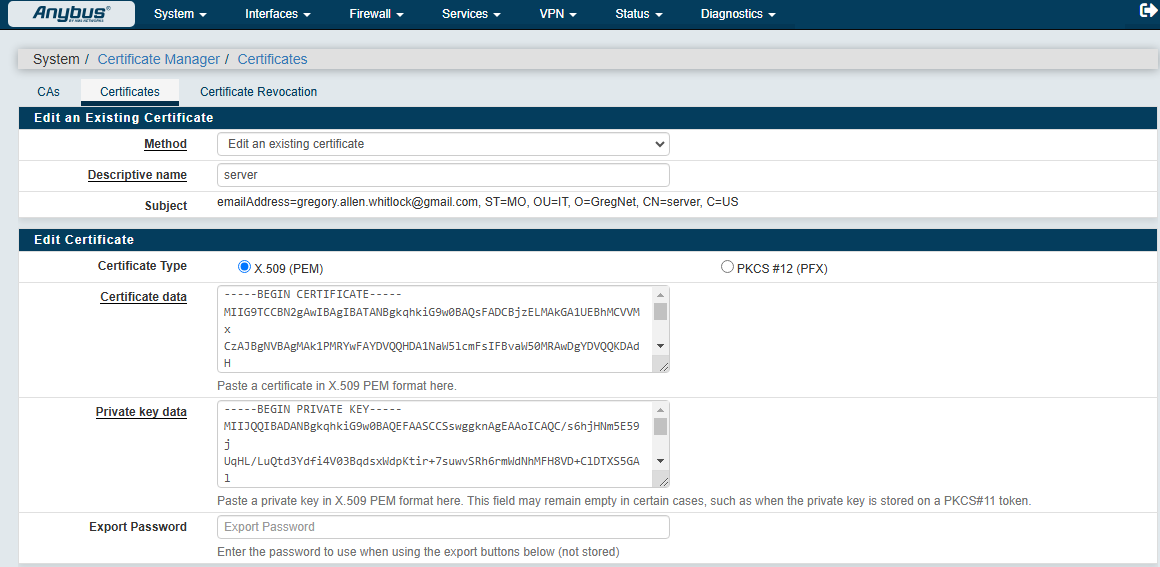
**For Anybus Defender**

Because of the way Anybus Defender is set up, there is no way to upload just one file. First go to System>Cert Manager.

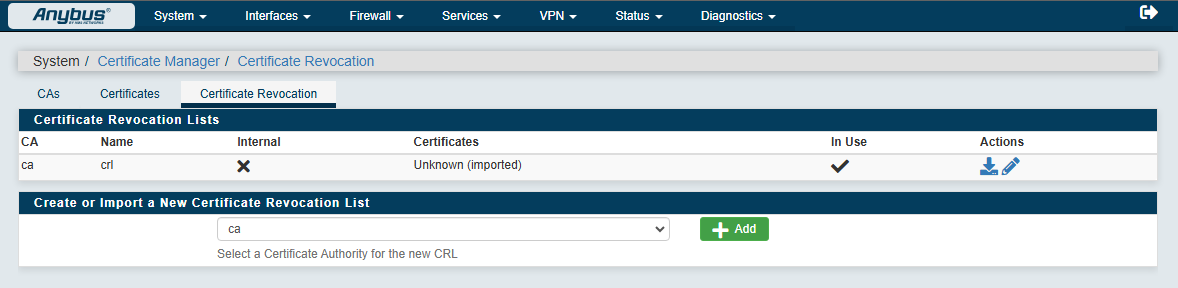
Add the ca.crt and ca.key files from your ca folder, then click Save



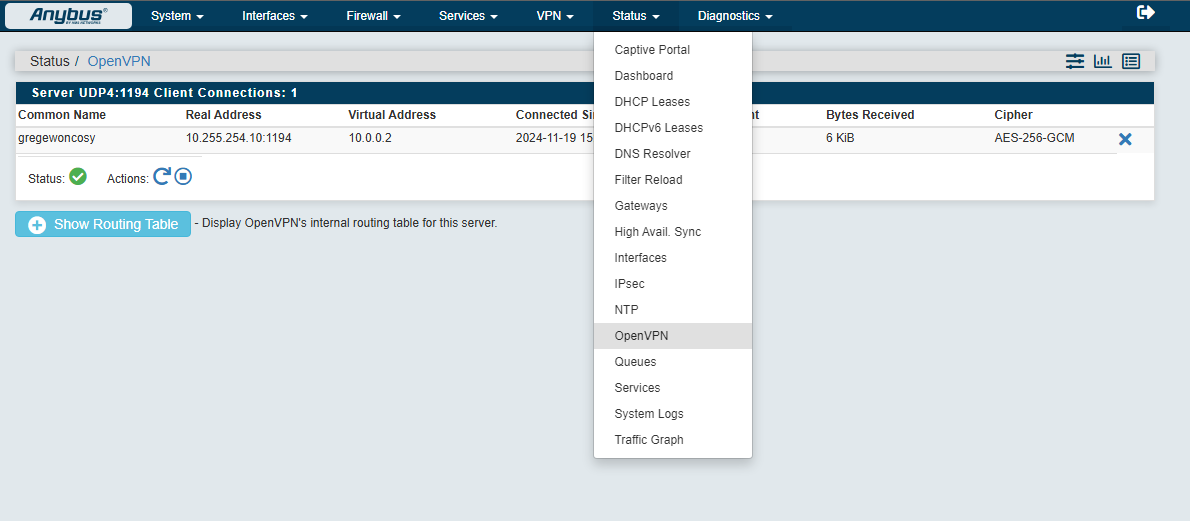
Then under Certificates copy and paste in your server.crt and server.key files from your server folder, then click Save



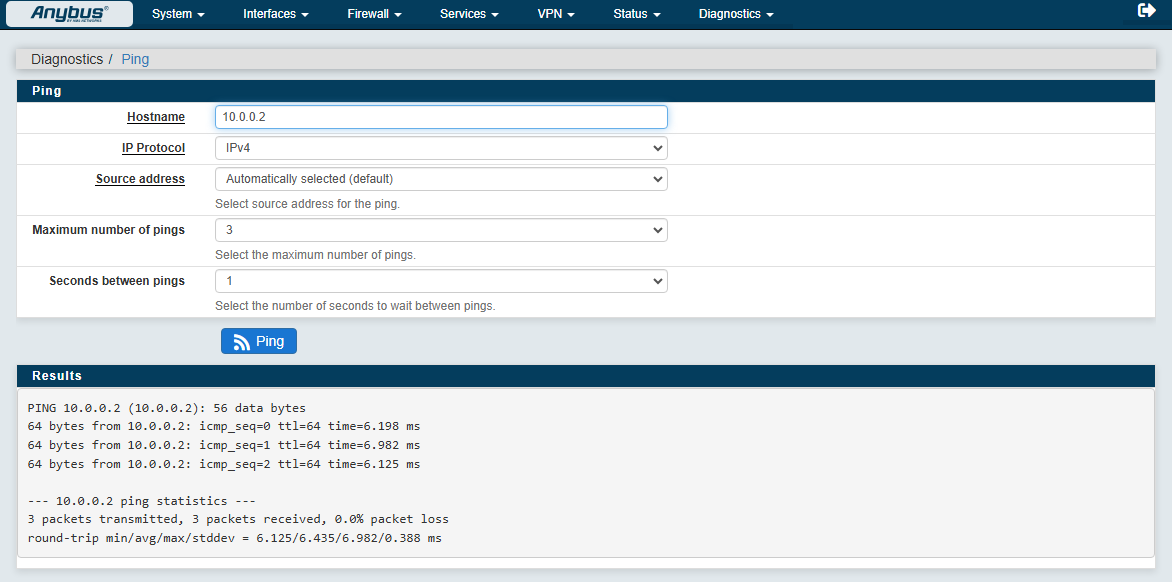
Then under Certificate Revocation, copy in your crl.pem file found in your server folder



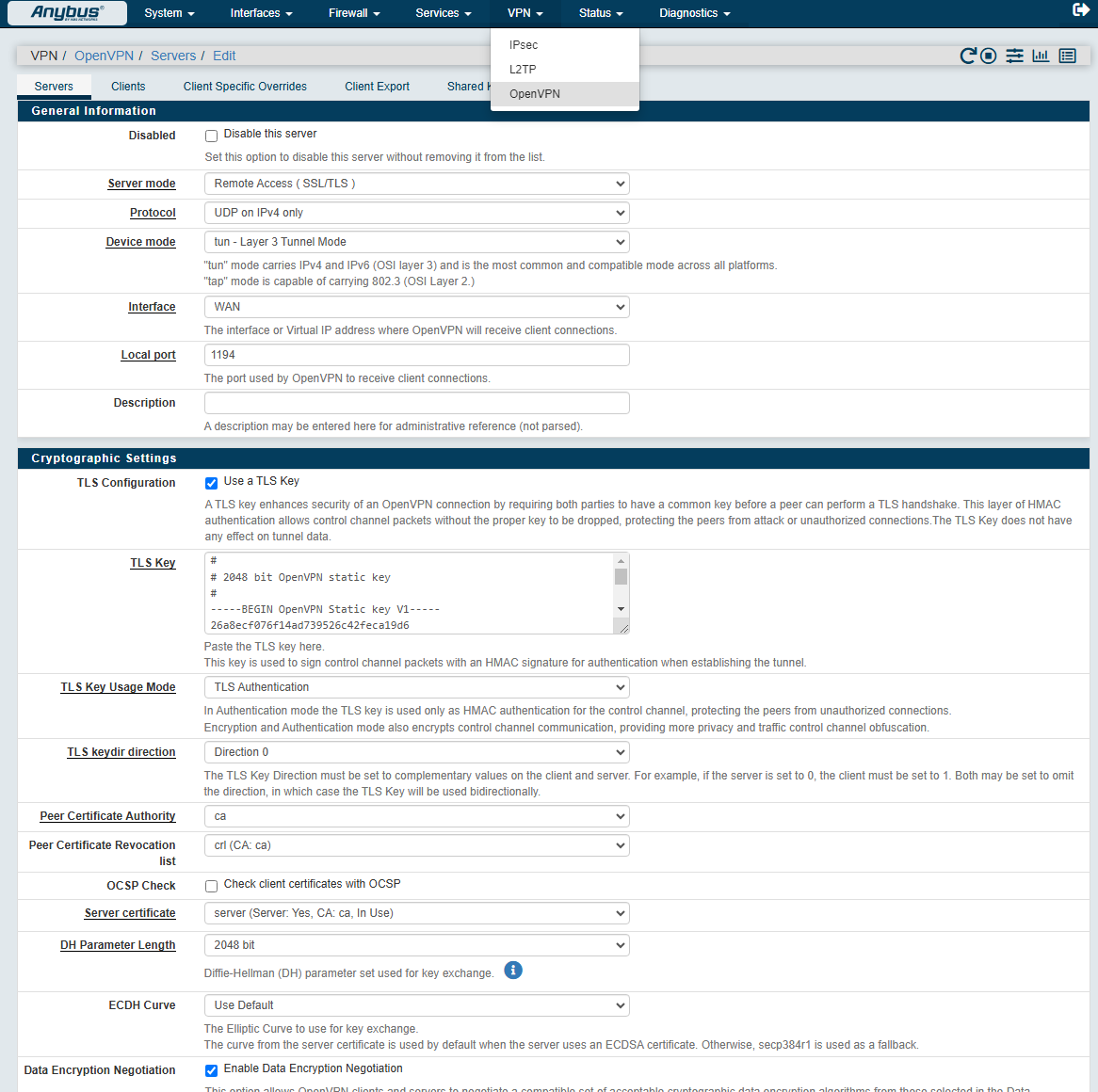
Here you can see the client connecting successfully



Here you can see the client responding to ping from the server



Now under VPN>OpenVPN add a new server



Make sure to set these settings to match what you input in the EZOpenVPNToolbox executable

* Server Mode = Remote Access (SSL/TLS)
* Protocol = What you chose
* Device Mode = tun – Layer 3 Tunnel Mode
* Interface = WAN
* Local Port = What you chose
* TLS Configuration = Use a TLS Key
* TLS Key = copy and paste the contents of the ta.key you generated
* TLS Key Usage Mode = TLS Authentication
* TLS keydir direction = Direction 0
* Peer certificate Authority = select your ca file from the dropdown
* Peer Cert Revocation List = select your crl file from the dropdown
* Server Certificate = select your server file from the dropdown
* DH Parameter Length 2048 bit
* Data Encryption Negotiation = yes/enabled
* Data Encryption Algorithms = there are 2 text boxes here, make sure the –data-ciphers you selected during the server initialization process are in the left text box
* Fallback Data Encryption Algorithm = select the weakest cipher for ciphers you chose
* Auth digest algorithm = since we don’t se this during the server initialization we use the default here which is SHA1
* IPv4 Tunnel Network = **OpenVPN Tunnel Subnet**
* IPv4 Local Network = Server Lan Subnet
* Inter-client communication = yes/enabled
* Topology = subnet
* All other settings can be left as default

You can then click “Save”

**Deploying Client Configurations**

**For Windows PC**

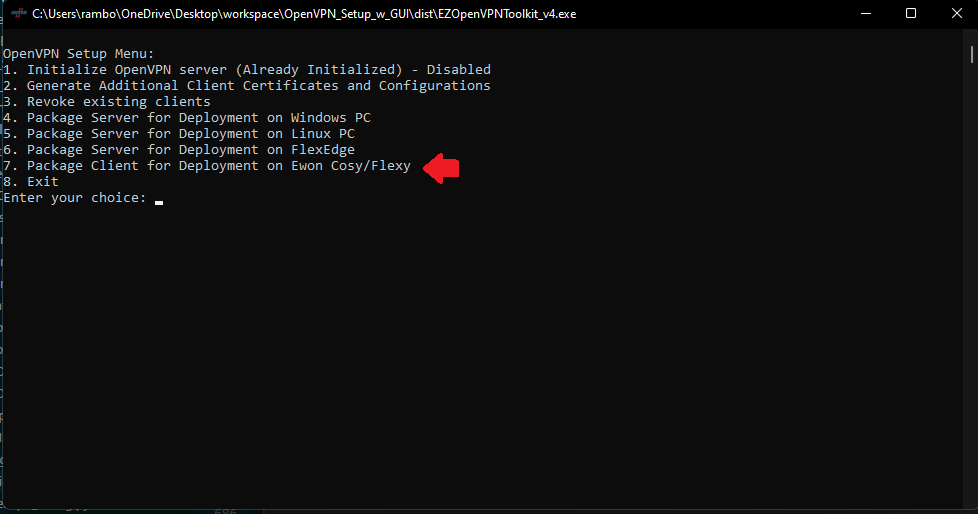
1. Copy the client configuration file to C:\Program Files\OpenVPN\config.
2. Open OpenVPN-GUI as administrator, right-click on the icon, select the new configuration, and click **Connect**.

**For FlexEdge**

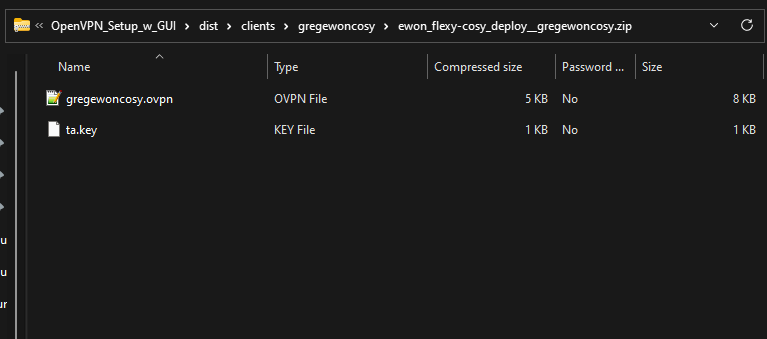
1. Use Crimson or the Web GUI, navigate to **Device Configuration > Tunnels > OpenVPN Tunnels**, and add the configuration file.
2. Under **Device > Configuration > Software Configuration > VPN1**, select **Tunnel Mode: Config File** and choose the appropriate client configuration.

For Ewon Cosy/Flexy

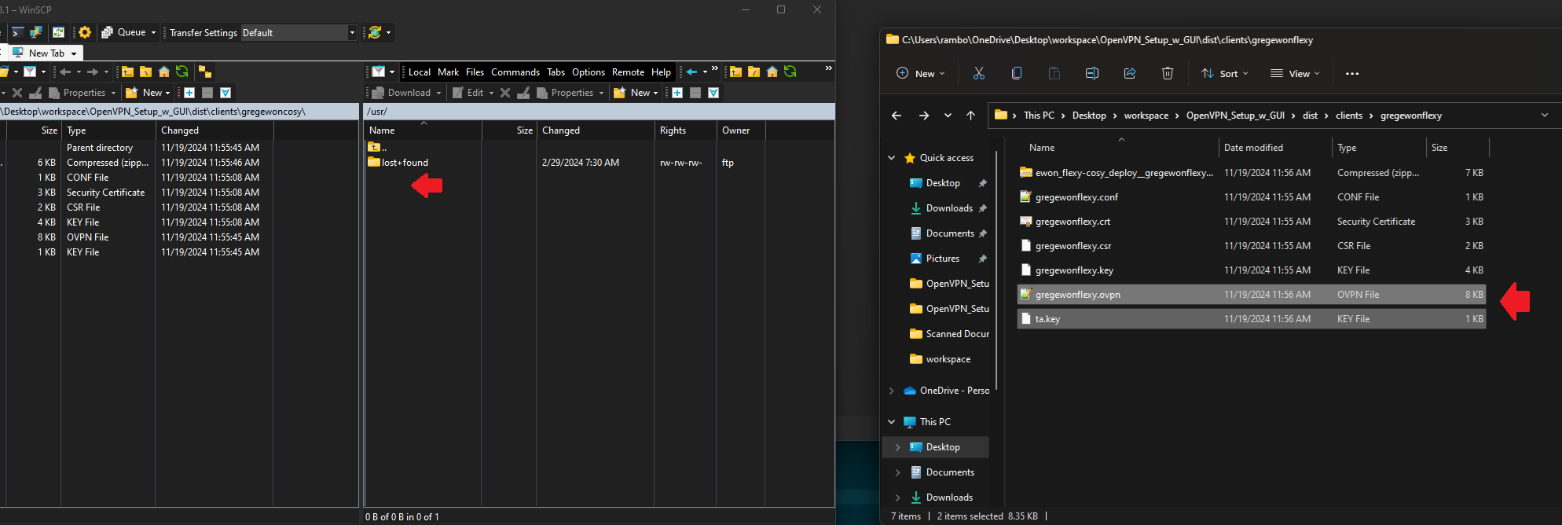
1. You can select option 7 for the EzOpenVPNTookit executable, and select which clients are Ewon devices



1. This will create a zip file in the client folder



1. Using an FTP client, connect to your Ewon device and drop the ovpn file and the ta.key file in the /usr directory.

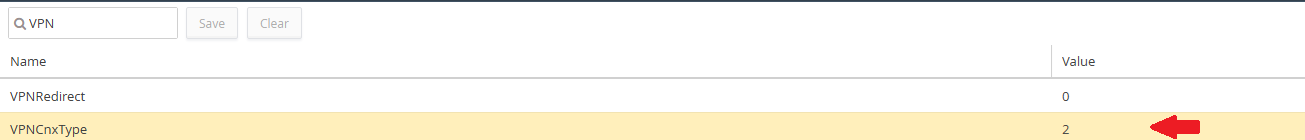


1. Then log into the web gui of the Ewon device, navigate to Setup> System> Storage> Tabular Edition> Edit COM cfg and modify these two variables, make sure to click ‘Save’ up top when you are done

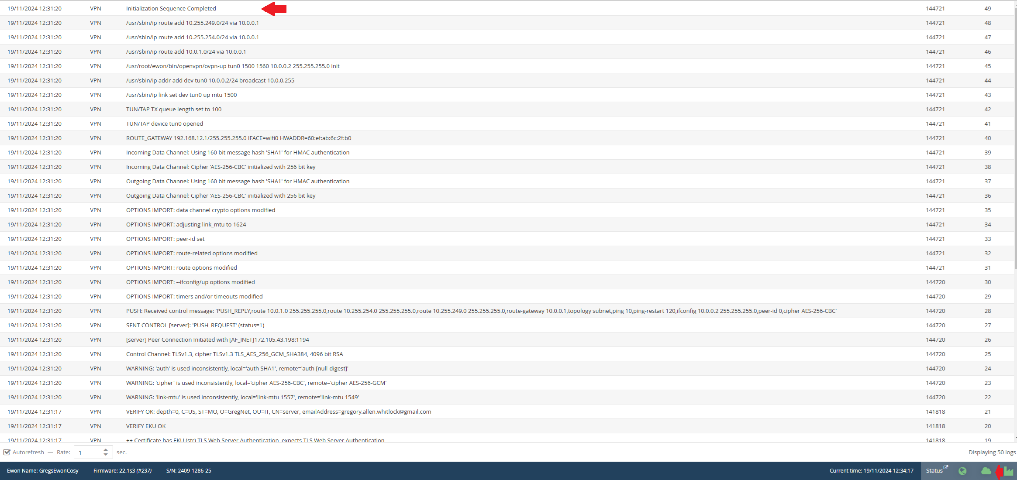
“VPNCfgFile” point this to the name of the openvpn file (ex. /usr/gregewoncosy.ovpn



“VPNCnxType” change this value to “2” so the device starts attempting OpenVPN connections



1. As you can see in the screenshot below the Ewon device is successfully connected to the OpenVPN server



**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.