Usage instructions:

1. Launch the product via 1-click from AWS Marketplace. **Wait** until the instance status changes to 'Running' and passes all health checks. Then, connect to your instance using your Amazon private key and the '**ubuntu**' user."

To update software, use:

```
sudo apt update && sudo apt upgrade -y
```

2. Then view the first-login file, run:

```
sudo cat /home/ubuntu/first-login.txt
```

You will see:

- Admin URL
- Client URL
- Admin username
- Admin password
- VPN endpoints/ports

3. Sign in to the Admin Web UI

1. Open the **Admin Web UI** link shown in first-login.txt (usually):
    - **https://Your_Instance_Public_IP:943/admin**
2. Your browser will warn about a **self-signed certificate** the first time. Proceed anyway.
3. Log in using the admin username/password shown in first-login.txt.
4. Immediately **change the admin password** in the Admin UI (recommended).

4. Create VPN users

In the Admin Web UI:

1. Go to **User Management** (or similar section).
2. Create one or more users (username + password).
3. Apply/Save changes if prompted.

5. Download a VPN client profile and connect

1. Open the **Client Web UI** link shown in first-login.txt (usually):
    - **https://Your_Instance_Public_IP:943/**
2. Sign in as one of the VPN users you created.
3. Download:
    - the OpenVPN Connect client (if needed), and/or

- a user profile (client configuration)

4. Import the profile into your OpenVPN client and connect.

6. Basic verification

On the instance, confirm the container is running:

```
sudo docker ps
```

You should see a container named openvpn-as in a healthy “Up …” state.

Self-signed cert warning is expected *initially. You can later place a trusted cert in front of it (optional).*

AWS Data

- Data Encryption Configuration: This solution does not encrypt data within the running instance.
- User Credentials are stored: /root/.ssh/authorized_keys & /home/ubuntu/.ssh/authorized_keys
- Monitor the health:
  - Navigate to your Amazon EC2 console and verify that you're in the correct region.
  - Choose Instance and select your launched instance.
  - Select the server to display your metadata page and choose the Status checks tab at the bottom of the page to review if your status checks passed or failed.

Extra Information: (Optional)

Allocate Elastic IP

To ensure that your instance **keeps its IP during restarts** that might happen, configure an Elastic IP. From the EC2 console:

1. Select ELASTIC IPs.
2. Click on the ALLOCATE ELASTIC IP ADDRESS.
3. Select the default (Amazon pool of IPv4 addresses) and click on ALLOCATE.
4. From the ACTIONS pull down, select ASSOCIATE ELASTIC IP ADDRESS.
5. In the box that comes up, note down the Elastic IP Address, which will be needed when you configure your DNS.
6. In the search box under INSTANCE, click and find your INSTANCE ID and then click ASSOCIATE.

7. Your instance now has an elastic IP associated with it.
8. For additional help: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html