

OPENVPN CONFIGURATION SETUP FOR eTRACS REMOTE ACCESS

A step-by-step guide for **eTRACS Remote Access via OpenVPN configuration.**

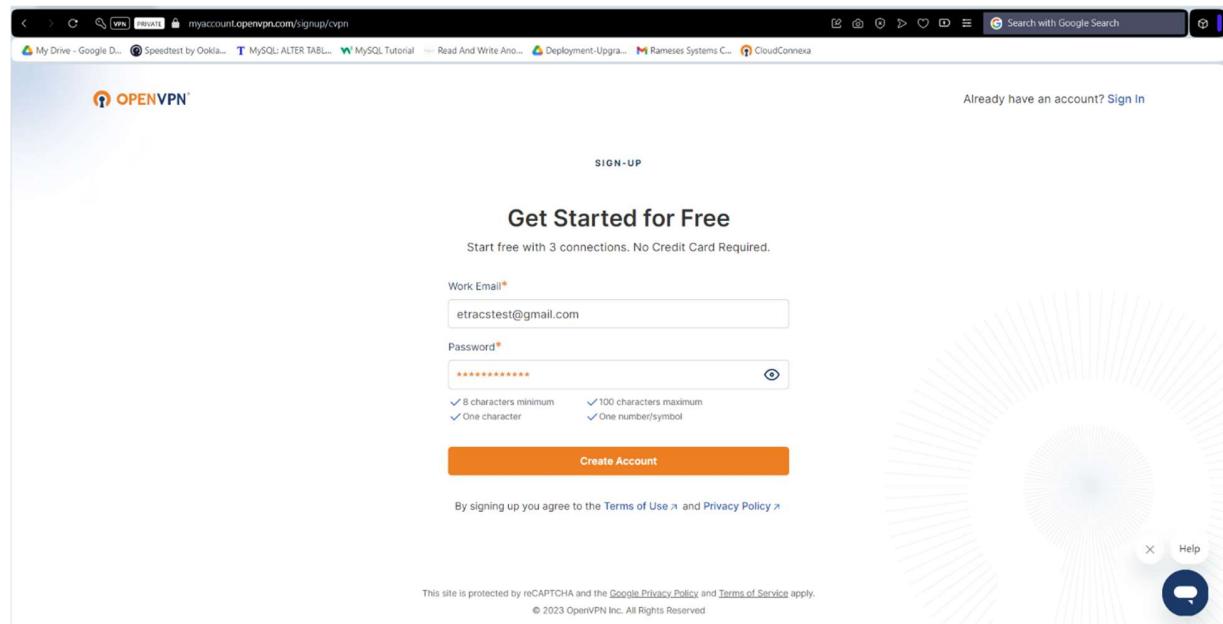
Pre-requisite requirements:

- Stable Internet Connection
- Gmail Account

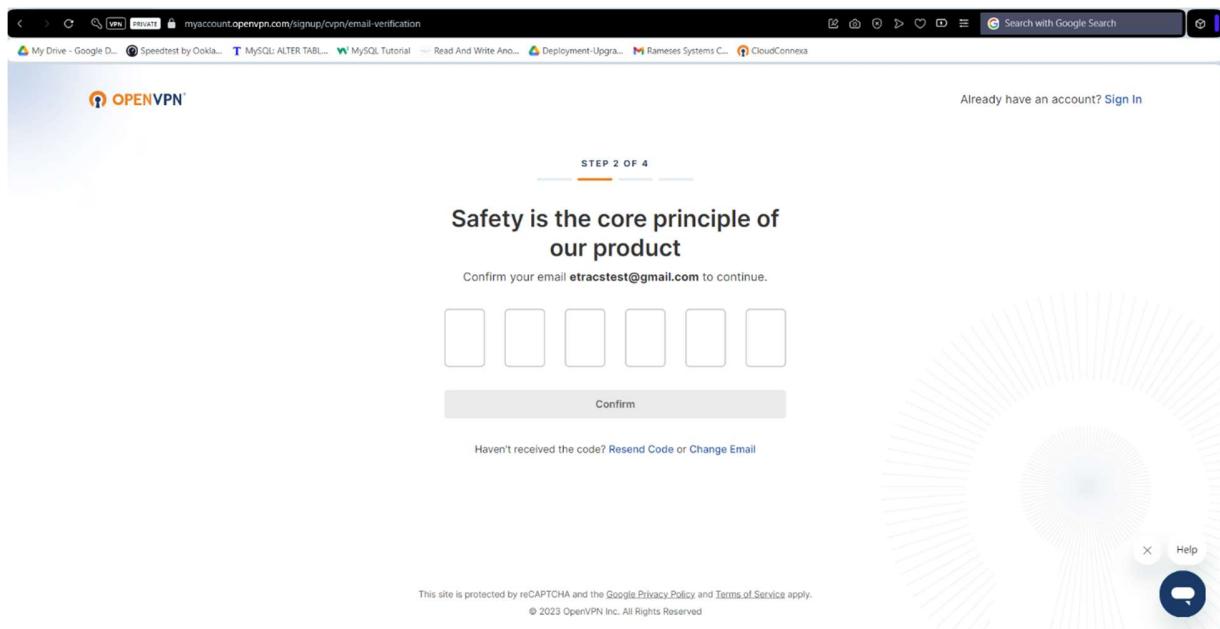
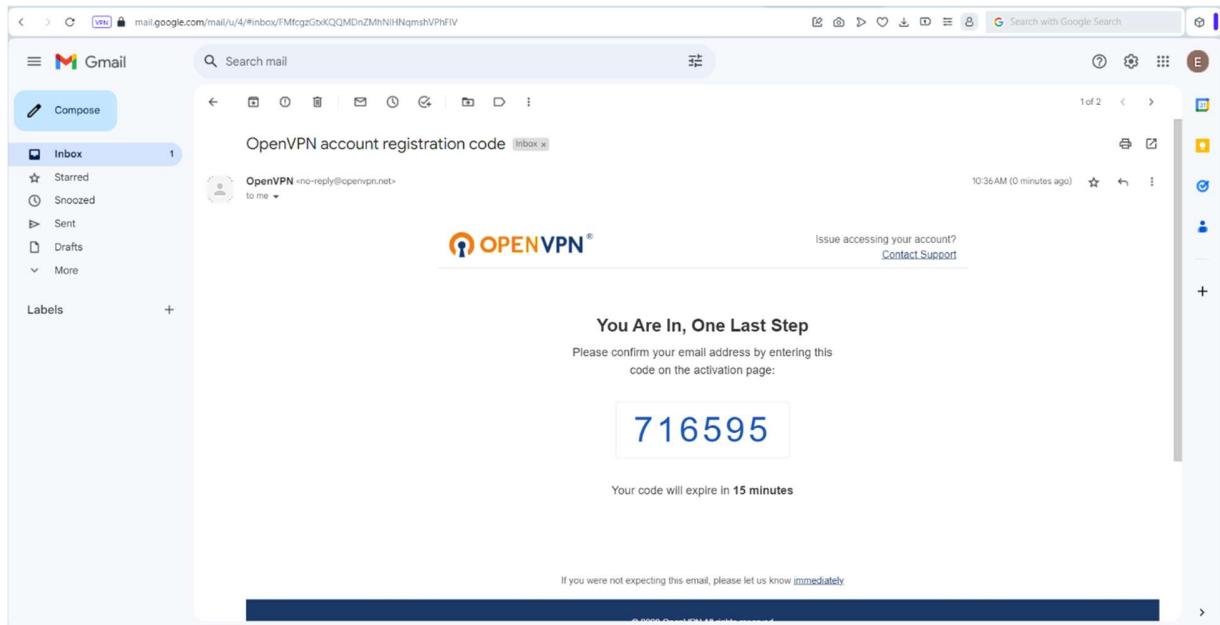
PART ONE: OpenVPN Configuration

1. Create a separate Gmail account intended for OpenVPN.
2. Create an account in **OpenVPN – CloudConnexa**. Signup using the newly created Gmail account.

<https://myaccount.openvpn.com/signup/cvpn>



3. Open your Gmail Account, copy the OTP sent by OpenVPN and confirm your email to continue with the signup process.



4. Continue with the signup process and fill-out the required fields accordingly.

STEP 3 OF 4

Just a Few More Details

Help us customize your experience.

Name

First Name*
Etracs

Last Name*
Test

Initial Configuration

How do you plan to use Cloud Connexa?*
Secure Remote Access

How many connections?*
2-3

Company

Company Name*
Rameses

Your Role*
IT Administration

Industry*
Technology

Country*
Philippines

Confirm

5. Create your Cloud ID. This will be the URL for your OpenVPN - CloudConnexa Account. Ideally, use your filipizen group naming convention.

Ex: **bohol-tagbilaran.openvpn.com**

STEP 4 OF 4

Create Your Wide-area Private Cloud (WPC)

Use your company name to personalize access to your account. Once your WPC is created, your Cloud ID cannot be changed.

Cloud ID* ⓘ

etracs-test.openvpn.com

✓ Starts and ends with letter or digit ✓ Letters, digits, hyphen only
✓ 3-60 characters long

Confirm

© 2023 OpenVPN Inc. All Rights Reserved

6. The Quick Start Page will appear after creating your OpenVPN – CloudConnexa Cloud ID.

The screenshot shows the CloudConnexa interface. On the left, a sidebar menu includes 'Status', 'Users', 'Networks' (which is expanded), 'Hosts', 'Access', 'Shield', 'AppHub', 'Settings', 'Documentation' (selected), and 'Quick Start'. A message at the bottom of the sidebar says 'You are using a free subscription plan with 3 connections'. The main content area is titled 'Connecting & Status' and contains instructions for connecting via OpenVPN Connect. It includes a 'Download a Client' section with four steps and a 'View Network Connections' section. A small inset window on the right shows the 'Get Connected' screen of the OpenVPN Cloud interface.

7. In the Left Side Panel, navigate to the **Networks** Option. Select **Remote Access** in Select Network Scenarios and Click **Continue**.

The screenshot shows the 'Select Network Scenarios' page of a wizard. The left sidebar has 'Networks' selected. The main content area has three options: 'Remote Access' (checked), 'Site-to-site' (unchecked), and 'Secure Internet Access' (unchecked). A note below 'Remote Access' says: 'Connect your private resources to CloudConnexa. Provide remote access to your resources, which are hosted on IaaS Cloud, and on-premises resources.' A button at the bottom says 'Continue'.

8. Define Network

Choose a name for your Virtual Network. You may also include a short description for your Virtual Network.

Ex: **Etracs - Tagbilaran**

The screenshot shows the CloudConnexa interface with the 'Network Configuration' page open. On the left, there's a sidebar with 'Status', 'Users', 'Networks' (selected), 'Applications', 'IP Services', and 'Connectors'. Below that are 'Hosts', 'Access', 'Shield', and 'AppHub'. A message says 'You are using a free subscription plan with 3 connections' and has an 'Upgrade Your Plan' button. At the bottom left is the user info 'etracstest@g... Owner'. The main area has a 'Define Network' form with 'Name*' set to 'etracstest' and 'Description (Optional)' set to 'Remote Access Network for Etracs 255'. To the right, a sidebar lists 'Scenarios selected: Remote Access' and a numbered list from 1 to 5: 1. Define Network, 2. Deploy Network Connector, 3. Add Application, 4. Add Routes and IP Services, 5. Configure Access Group (Optional). There's also a 'Next' button at the bottom of the form.

Add Connector

Set a name for your connector. The connector will provide constant connectivity from your server to CloudConnexa. In this setup, the connector will be installed on the etracs server machine to maximize efficiency.

Ex: **Etracs Server**

Choose **Singapore** as your region. You may also add a short description for your connector to indicate the details of the server machine, the connector was installed.

9. Deploying Network Connector (Etracs Server)

Select the Operating System on which your connector will be installed. In a Standalone Linux and a Docker Environment, we will be dealing with **Linux Operating System**.

Select the Appropriate Linux Distribution from the drop-down list.

Network Configuration

Deploy Network Connector (Etracs Server)

Connector Details

Name: Etracs Server Region: Singapore

Each Connector must be installed and connected to CloudConnexa. Select where you would like to deploy Network Connector.

Operating Systems: Linux

Connector can be launched on Linux and IaaS Public Cloud.

① Select Linux Distribution: Ubuntu 18.04

② Execute the following script to install Connector on Linux:

```
curl -o https://network-management-gw.openvpn.com/network-gate/api/v1/scripts/WJ1bnR110E4LjA0/network-management-gw_18.04.sh
chmod +x ubuntu_18.04.sh
./ubuntu_18.04.sh
```

Click Generate Token button to generate new token, which is needed to launch openvpn-connector-setup. When you generate new token, previously generated token will be invalidated.

Scenarios selected:
• Remote Access

Define Network
2 Deploy Network Connector
Etracs Server
3 Add Application
4 Add Routes and IP Services
5 Configure Access Group (Optional)

Generate Token

10. Login to your etracs server via **Git Bash** or **Terminal**.

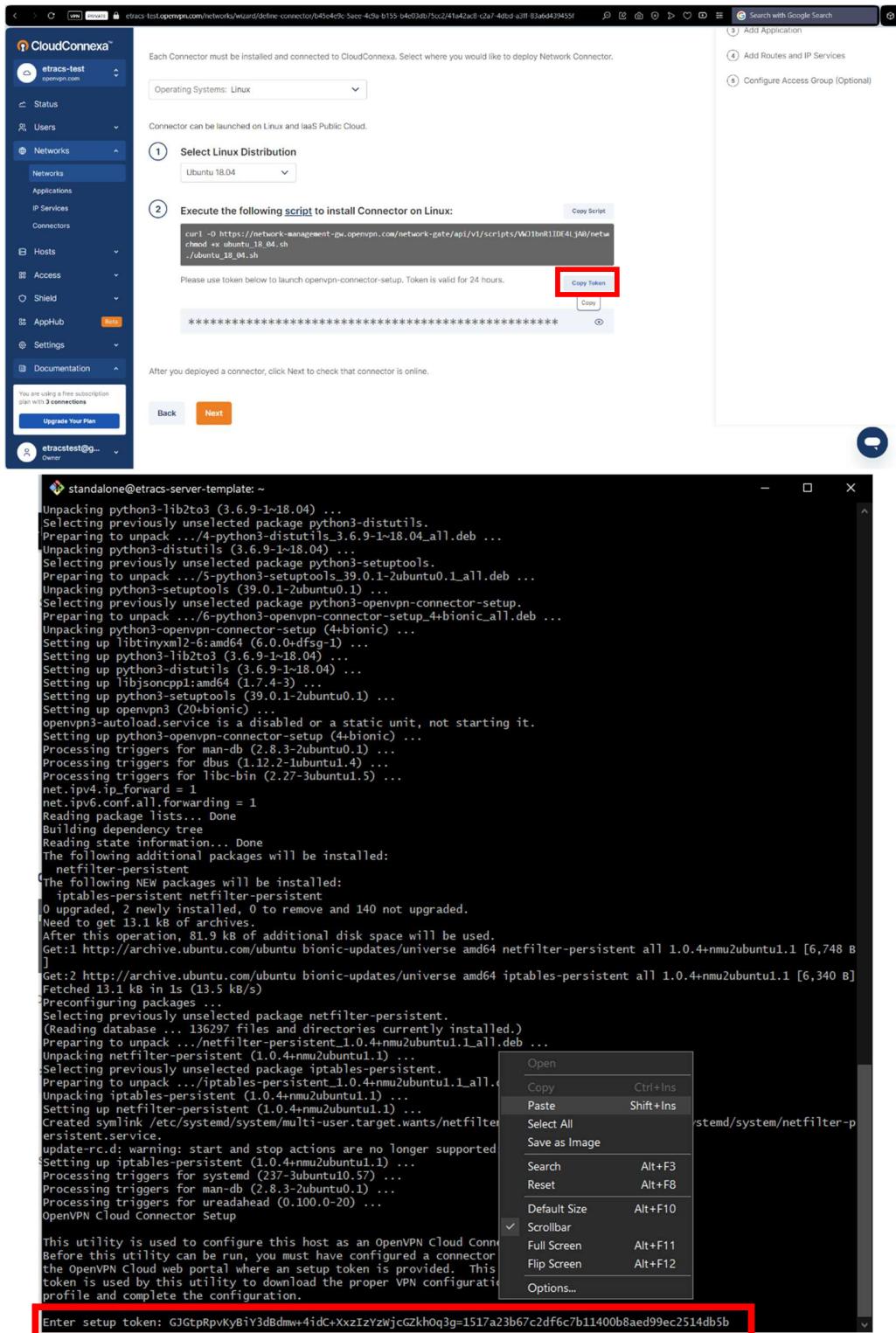
Execute the generated script to install Connector on your Linux Server.

You may click on the **Copy Script** button on the upper right portion of the script to copy the script directly on your clipboard.

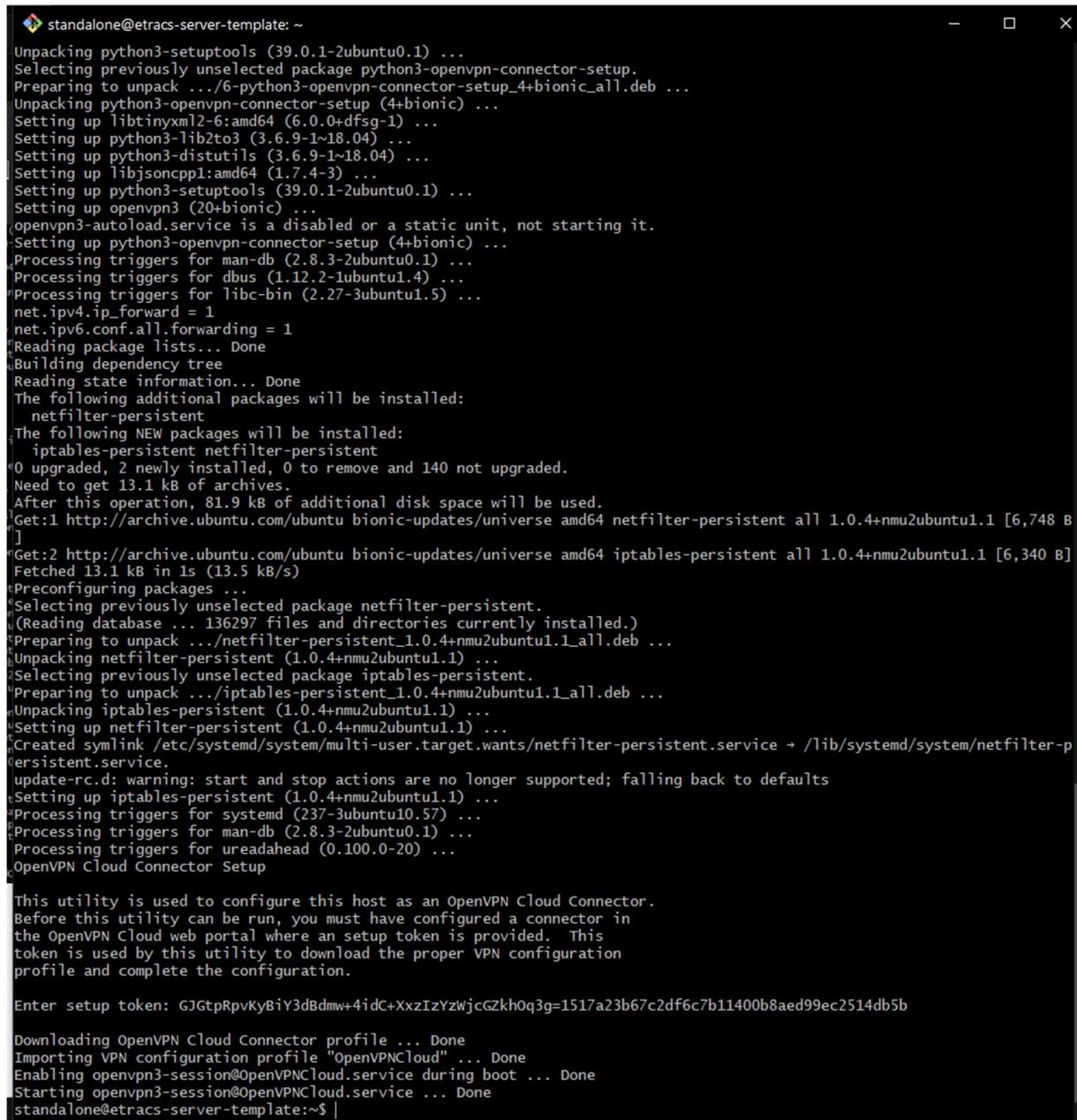
Wait for the download and installation to finish.

Press **Y** then **ENTER** when prompted to continue the installation of the OpenVPN Connector.

11. Go back to the OpenVPN – CloudConnexa Network Configuration page in your browser and click on the **Generate Token** button. Click on the **Copy Token** button on the right portion to copy the token and paste it on your **Git Bash or Terminal**.



- 12.** Wait until configuration is finished.



```
standalone@etracs-server-template: ~
Unpacking python3-setuptools (39.0.1-2ubuntu0.1) ...
Selecting previously unselected package python3-openvpn-connector-setup.
Preparing to unpack .../6-python3-openvpn-connector-setup_4+bionic_all.deb ...
Unpacking python3-openvpn-connector-setup (4+bionic) ...
Setting up libtinyxml2-6:amd64 (6.0.0+dfsg-1) ...
Setting up python3-lib2to3 (3.6.9-1~18.04) ...
Setting up python3-distutils (3.6.9-1~18.04) ...
Setting up libjsoncpp1:amd64 (1.7.4-3) ...
Setting up python3-setuptools (39.0.1-2ubuntu0.1) ...
Setting up openvpn3 (20+bionic) ...
openvpn3-autoload.service is a disabled or a static unit, not starting it.
Setting up python3-openvpn-connector-setup (4+bionic) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for dbus (1.12.2-1ubuntu1.4) ...
Processing triggers for libc-bin (2.27-3ubuntu1.5) ...
net.ipv4.ip_forward = 1
net.ipv6.conf.all.forwarding = 1
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  netfilter-persistent
The following NEW packages will be installed:
  iptables-persistent netfilter-persistent
0 upgraded, 2 newly installed, 0 to remove and 140 not upgraded.
Need to get 13.1 kB of archives.
After this operation, 81.9 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu bionic-updates/universe amd64 netfilter-persistent all 1.0.4+nmu2ubuntu1.1 [6,748 B]
]Get:2 http://archive.ubuntu.com/ubuntu bionic-updates/universe amd64 iptables-persistent all 1.0.4+nmu2ubuntu1.1 [6,340 B]
Fetched 13.1 kB in 1s (13.5 kB/s)
Preconfiguring packages ...
Selecting previously unselected package netfilter-persistent.
(Reading database ... 136297 files and directories currently installed.)
Preparing to unpack .../netfilter-persistent_1.0.4+nmu2ubuntu1.1_all.deb ...
Unpacking netfilter-persistent (1.0.4+nmu2ubuntu1.1) ...
Selecting previously unselected package iptables-persistent.
Preparing to unpack .../iptables-persistent_1.0.4+nmu2ubuntu1.1_all.deb ...
Unpacking iptables-persistent (1.0.4+nmu2ubuntu1.1) ...
Setting up netfilter-persistent (1.0.4+nmu2ubuntu1.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/netfilter-persistent.service → /lib/systemd/system/netfilter-persistent.service.
update-rc.d: warning: start and stop actions are no longer supported; falling back to defaults
Setting up iptables-persistent (1.0.4+nmu2ubuntu1.1) ...
Processing triggers for systemd (237-3ubuntu10.57) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for ureadahead (0.100.0-20) ...
OpenVPN Cloud Connector Setup

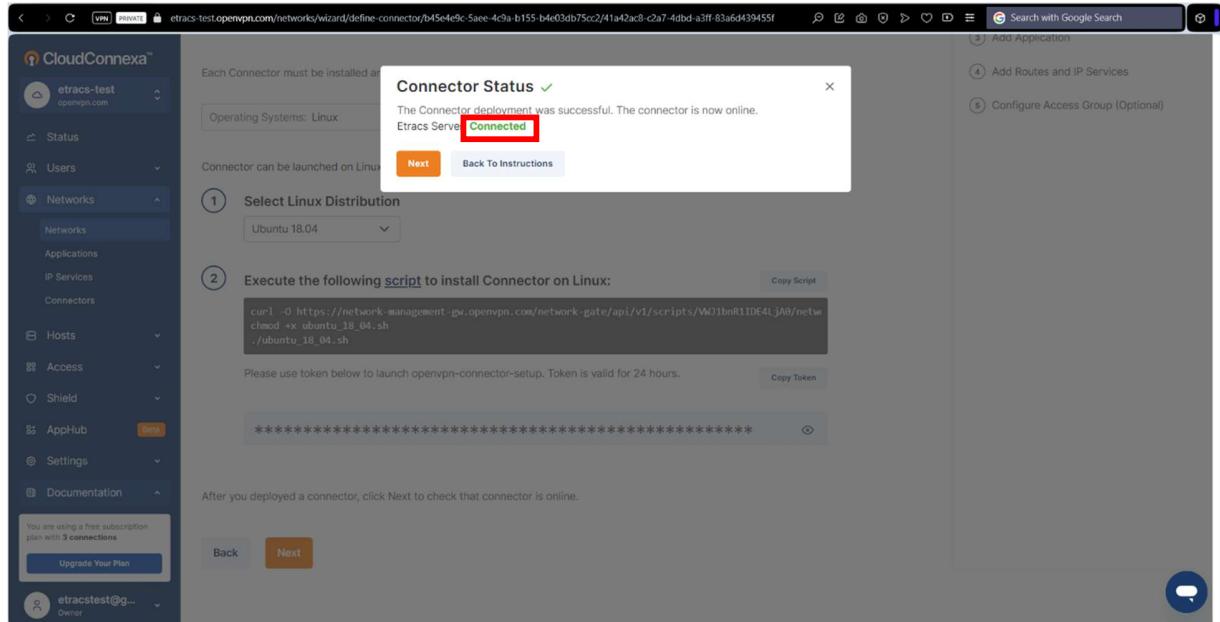
This utility is used to configure this host as an OpenVPN Cloud Connector.
Before this utility can be run, you must have configured a connector in
the OpenVPN Cloud web portal where an setup token is provided. This
token is used by this utility to download the proper VPN configuration
profile and complete the configuration.

Enter setup token: GJGtpRpVkyBiY3dBdmw+4idC+XxzIzYzWjcgZkh0q3g=1517a23b67c2df6c7b11400b8aed99ec2514db5b

Downloading OpenVPN Cloud Connector profile ... Done
Importing VPN configuration profile "OpenVPNCloud" ... Done
Enabling openvpn3-session@OpenVPNCloud.service during boot ... Done
Starting openvpn3-session@OpenVPNCloud.service ... Done
standalone@etracs-server-template:~$ |
```

- 13.** After the Connector has been successfully installed in the Linux Environment, go back to the **Network Configuration** page on your browser and click on **Next**. A pop-up dialog box will appear showing the Connector Status. If the Connector is already **Connected**, you may now proceed by clicking on **Next**.

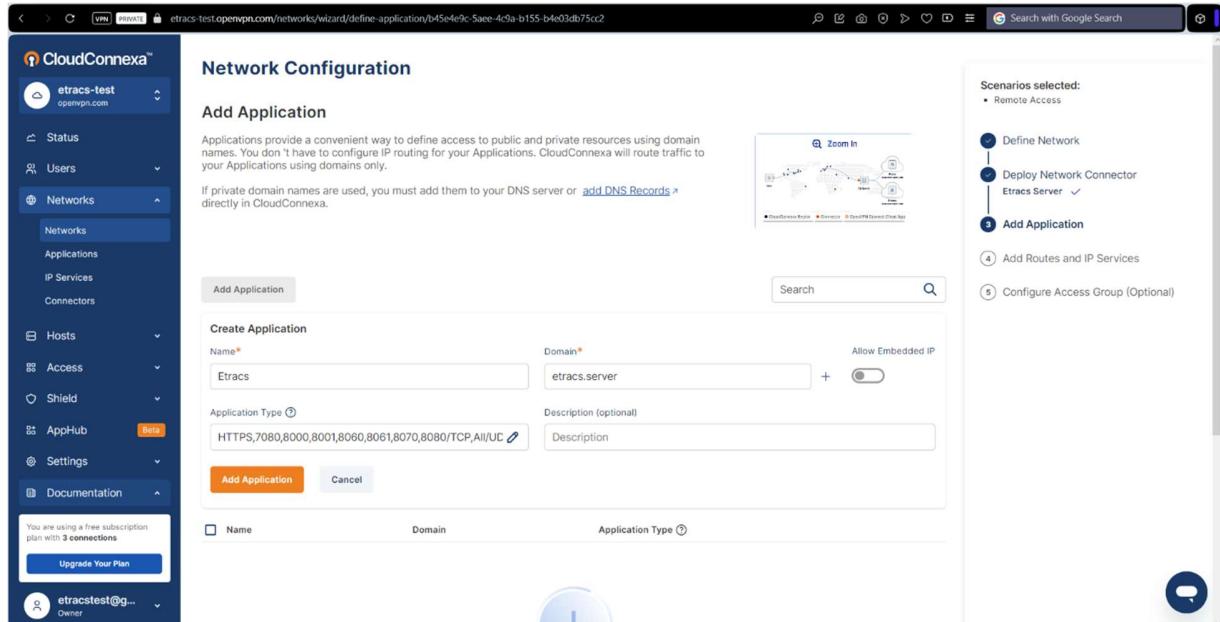
Otherwise, if the Connector Status is **Offline**, close the pop-up dialog box and wait for a few seconds before clicking on **Next**, again.



14. Add Application

Create an application named **Etracs** and set a domain to access the application in the future. The domain will be used to access the application (etracs server) instead of using its IP address.

Ex: **etracs.server**



In the **Application Type** field, select the following options to specify the protocols to be used. For **TCP**, these are the ports to be used for etracs: **7080,8000,8001,8060,8061,8070,8080,8095**.

You can add a short description to provide details of your Application/Etracs Server. Once done, click **Add Application** to proceed.

Verify the Application created. You can edit the Application configurations using the pencil tool on the right portion.

15. Add Route

Enter the IP address of the etracs server. CloudConnexa will automatically convert your input IP Address into the Subnet/Network Group of your server.

Ex: **192.168.1.0/24**

The screenshot shows the CloudConnexa interface with the 'Network Configuration' tab selected. In the left sidebar, 'Networks' is expanded, and 'Add Route' is selected. The main area displays a 'Create Route' form with an 'IP Address or Subnet' field containing '192.168.1.0/24' and a 'Description' field containing 'Etracs Network Group'. Below the form is a large blue circular button with a white plus sign labeled 'Add a Route'. To the right, a vertical sidebar titled 'Scenarios selected:' shows a step-by-step process: 'Define Network', 'Deploy Network Connector Etracs Server', 'Add Application', and 'Add Routes and IP Services'. Step 4 is highlighted in green, and a note below it says '(5) Configure Access Group (Optional)'. A message at the top right says 'Subnet 192.168.1.0/24 was added'.

You can add a short description to specify the details of the IP Address. Once done, click on the **Add Route** button to create the route. Verify that the Subnet was added into the Routes list.

This screenshot shows the same interface after the route has been added. The 'Add Route' form now shows the previously entered subnet. The 'Add a Route' button is no longer visible. The vertical sidebar on the right still shows the scenario steps, but the message at the top right now says 'Subnet 192.168.1.0/24 was added'.

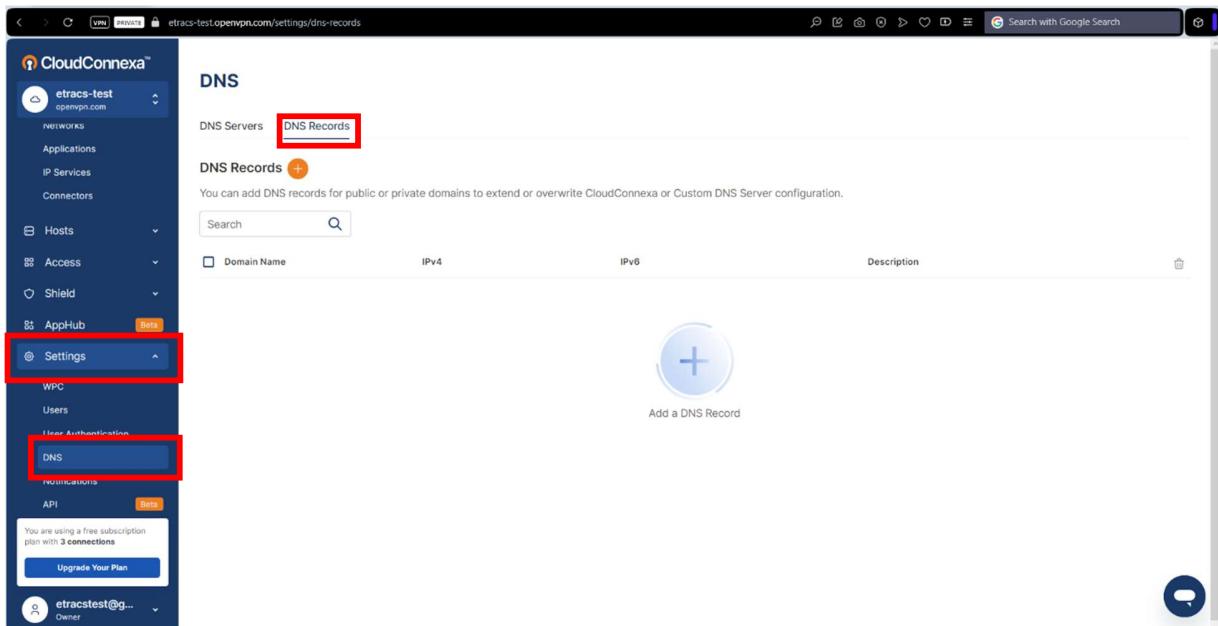
16. Configure Access Group

Select the **Default Full Mesh Access Group** and click on **Finish** to proceed.

Alternatively, you may also create an access group for specific users.

17. Verify the configurations.

18. After verifying the configurations, on the left side pane, navigate to the **DNS** tab under the **Settings** Option.

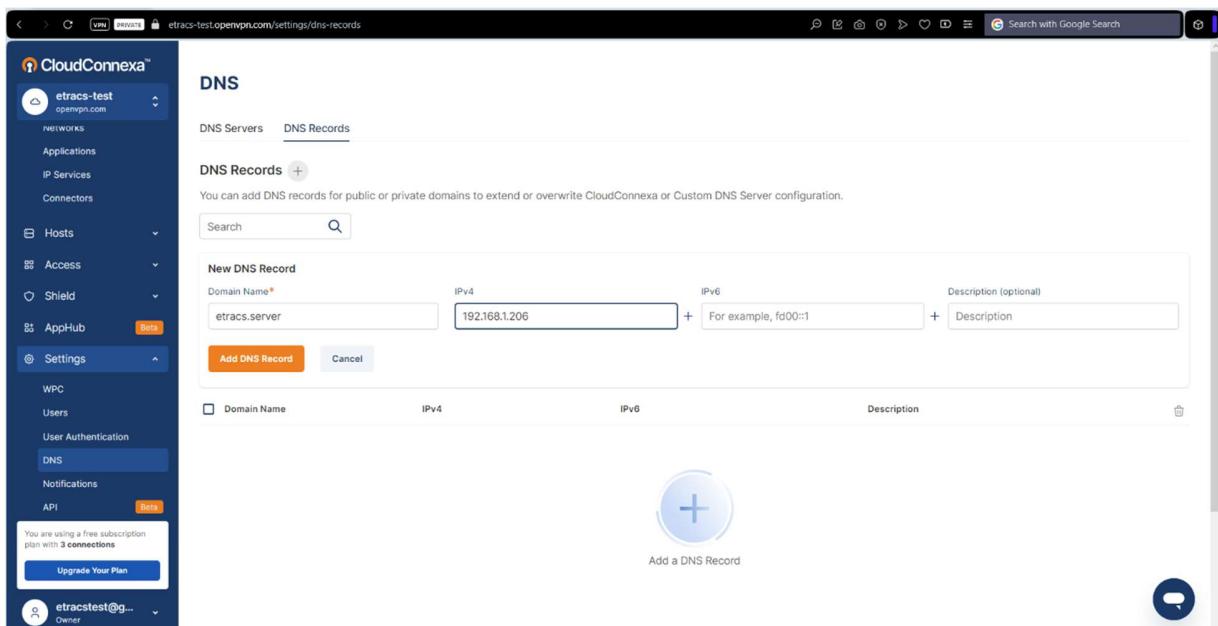


The screenshot shows the CloudConnexa web interface. The left sidebar has a dark blue background with various options: Networks, Applications, IP Services, Connectors, Hosts, Access, Shield, AppHub, Settings (which is expanded), WPC, Users, User Authentication, DNS (which is selected and highlighted with a red box), Notifications, API, and a free plan notice. The main content area is titled 'DNS' and shows the 'DNS Records' tab selected (also highlighted with a red box). It includes a search bar, a table with columns for Domain Name, IPv4, IPv6, and Description, and a large blue '+' button labeled 'Add a DNS Record'.

19. Click on **DNS Records** and a DNS Record by clicking on the **+** Button.

Input the domain name set for the etracs application and the IP address of the etracs server machine.

Click on the **Add DNS Record** button.



The screenshot shows the 'DNS Records' page with a new 'New DNS Record' dialog box open. The dialog has fields for 'Domain Name' (set to 'etracs.server'), 'IPv4' (set to '192.168.1.206'), and 'IPv6' (set to 'fd00::1'). There is also an optional 'Description' field. At the bottom of the dialog are 'Add DNS Record' and 'Cancel' buttons, with the 'Add DNS Record' button highlighted with a red box.

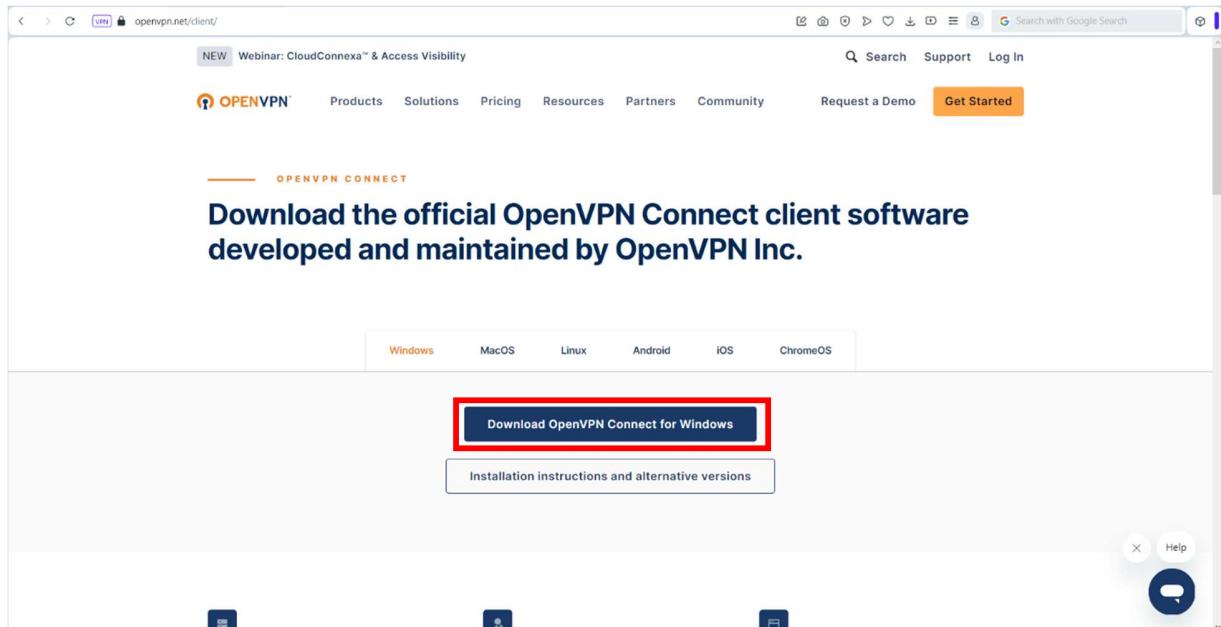
Verify that the DNS Record was added with the correct domain name and IPv4 Address.

PART TWO: Client Installation

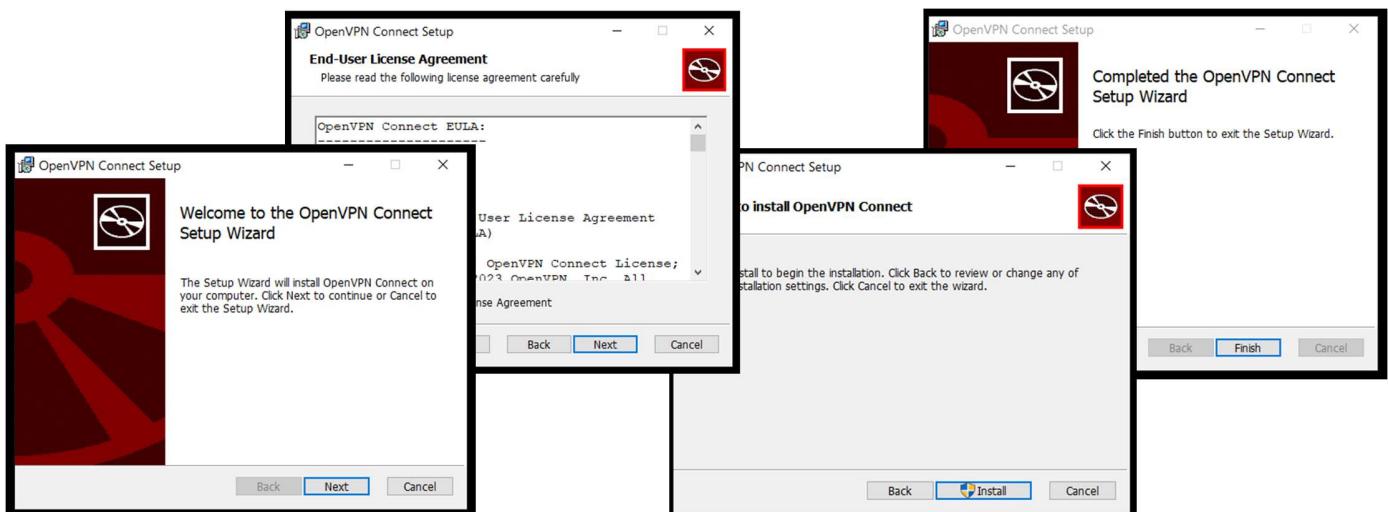
1. Download OpenVPN Connect Client Software

Click on **Download OpenVPN Connect for Windows** button to download the Client software for Windows or choose an alternative version for another operating system/windows version.

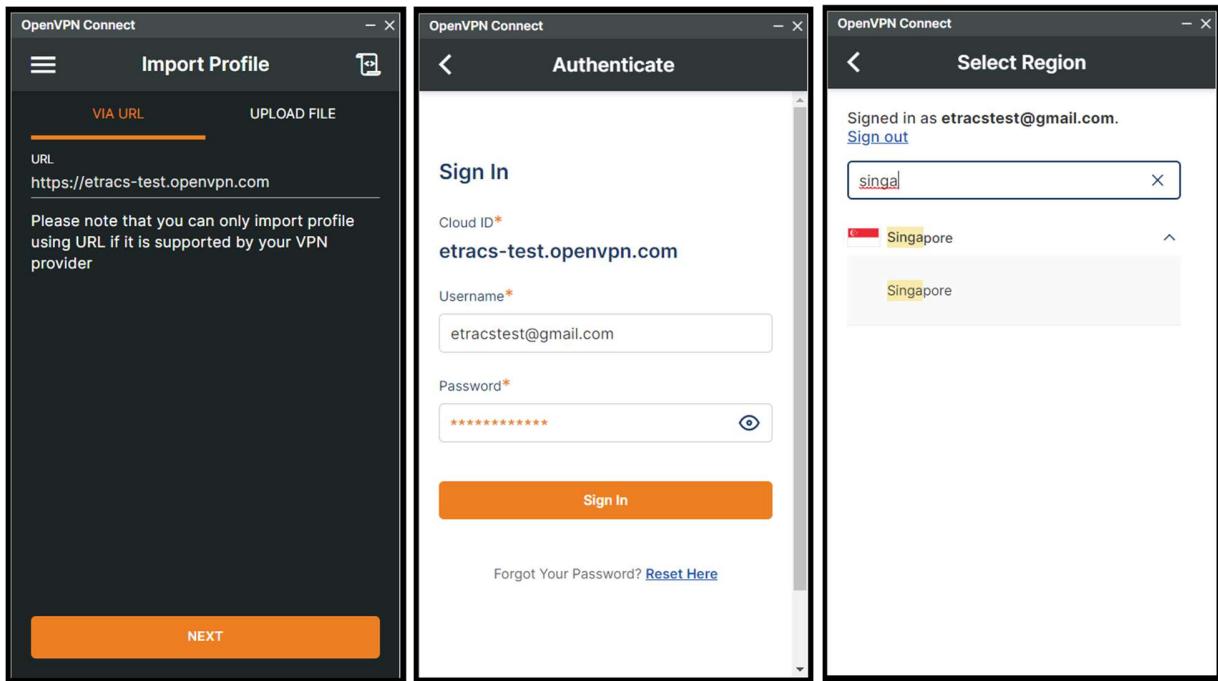
<https://openvpn.net/client/>



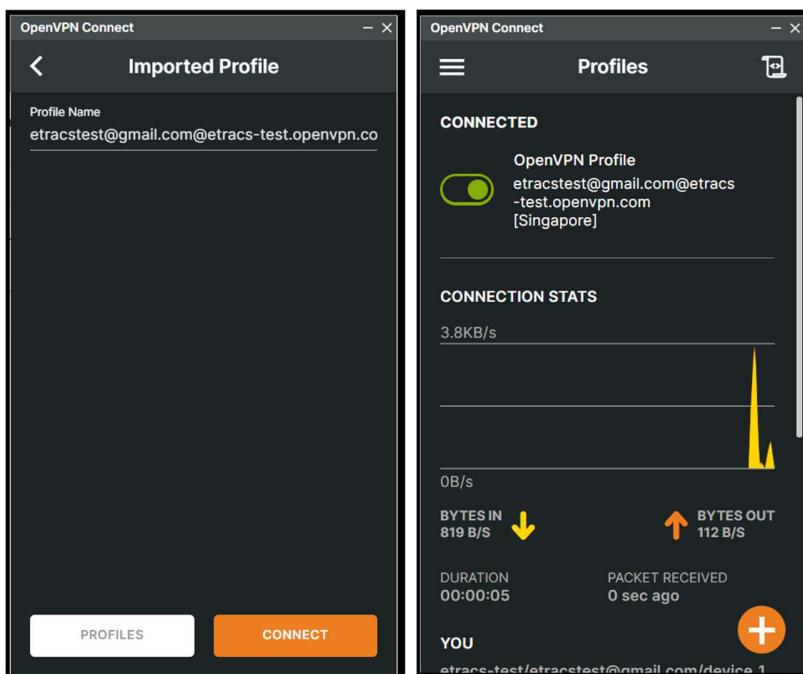
2. Complete the Installation Process.



3. Run the OpenVPN Connect Client Application. Input the Cloud ID / URL you created earlier and click on the **Next** button. Sign in into the OpenVPN and select **SINGAPORE** as region.

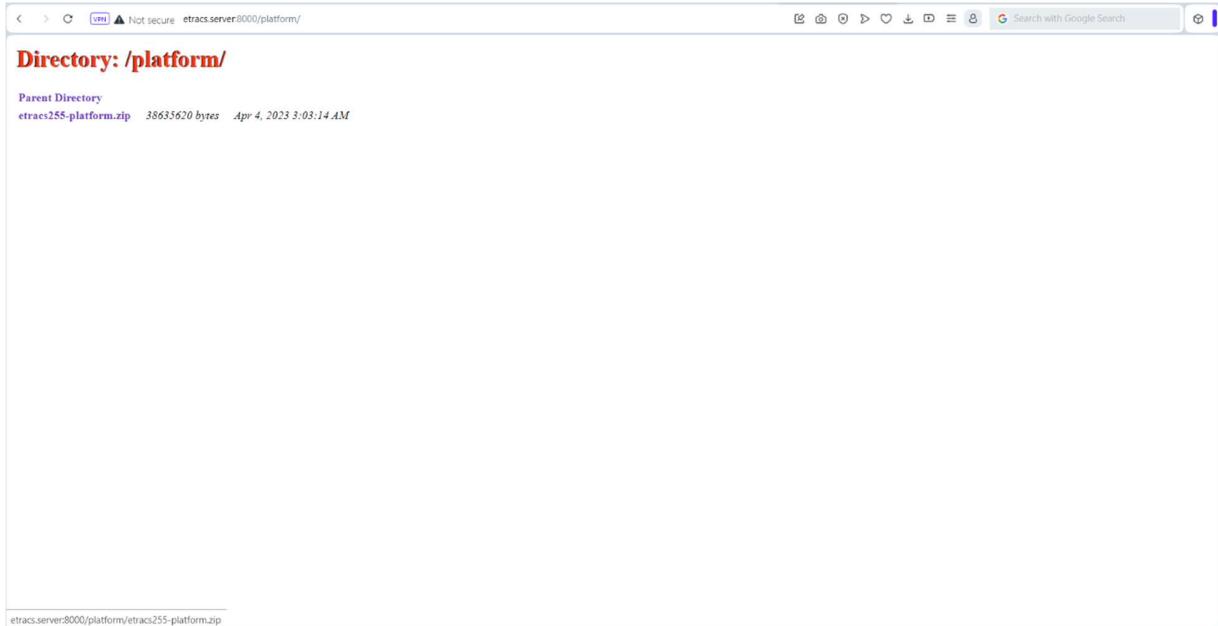


4. Connect to the Imported Profile. Wait for the OpenVPN Connect Client to connect to your virtual network.



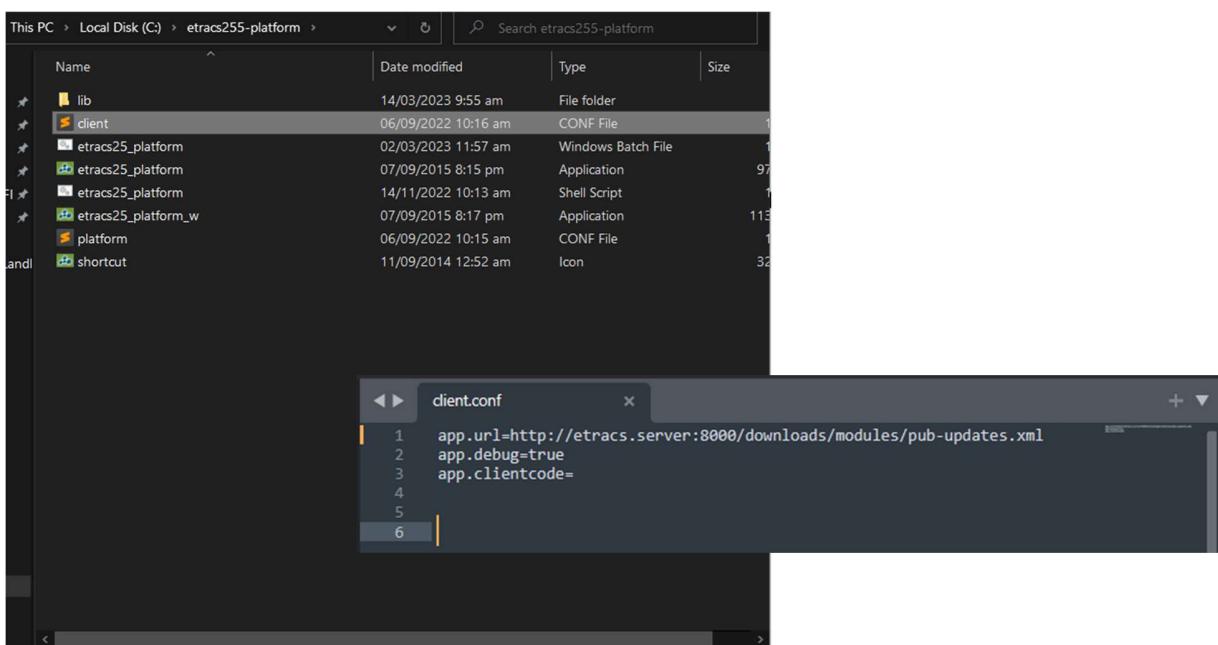
5. Once connected. Proceed to the etracs client installation. Use the domain name you set earlier as the URL/IP Address for the etracs server.

Ex: <http://etracs.server:8000/platform/>



6. Extract the etracs255-platform.zip file into **(C:) Drive**.

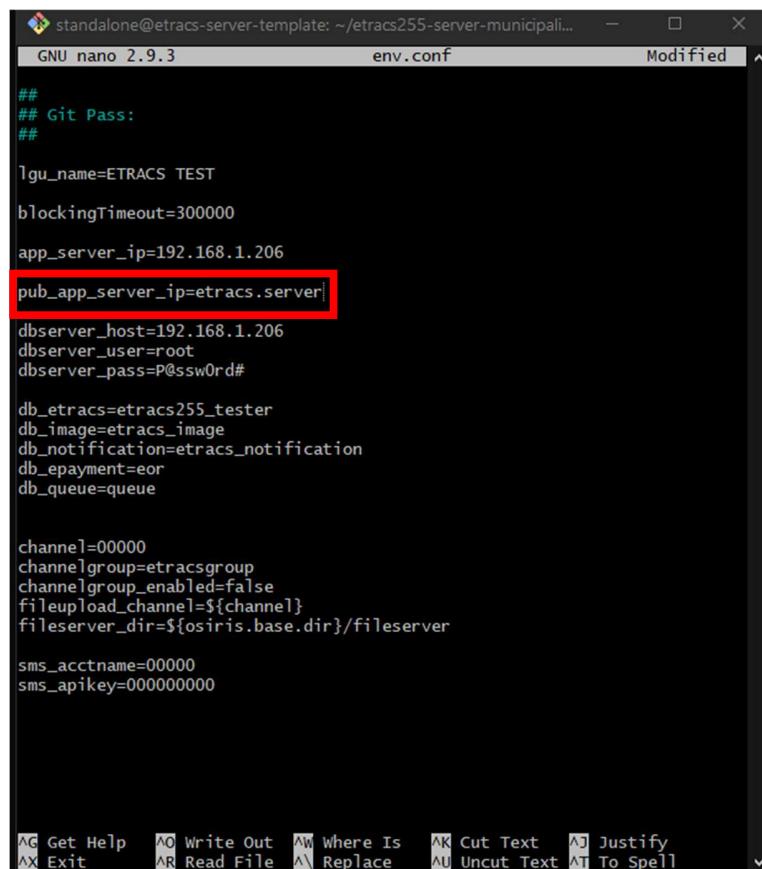
Open the folder and edit the **client.conf** file. Change the IP address into the domain name you set earlier. Change the **updates.xml** into **pub-updates.xml**. Save changes.



7. Go back to your etracs server on your **Terminal** or **Git Bash** session. Edit the env.conf file in the docker/_custom dir for docker environment, or {Server_DIR}/bin for standalone linux.

Edit or add the **pub_app_server_ip** into the domain name.

Ex: **pub_app_server_ip=etracs.server**



```
standalone@etracs-server-template: ~/etracs255-server-municipali... - X
GNU nano 2.9.3           env.conf          Modified ^

## Git Pass:
##

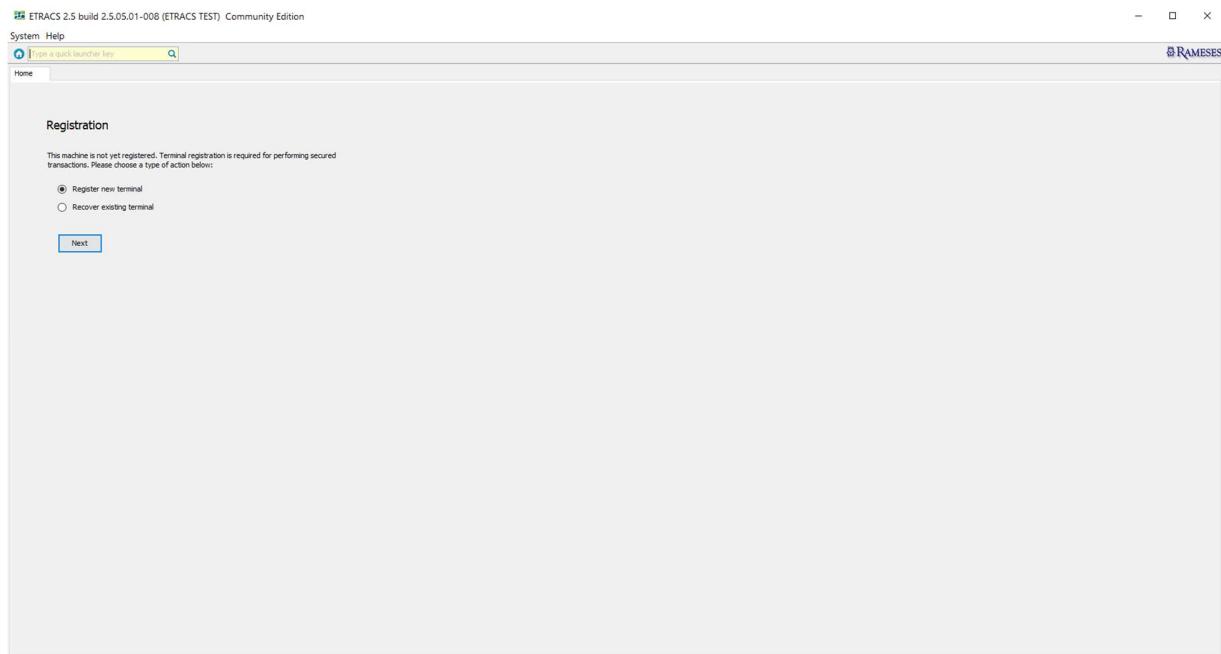
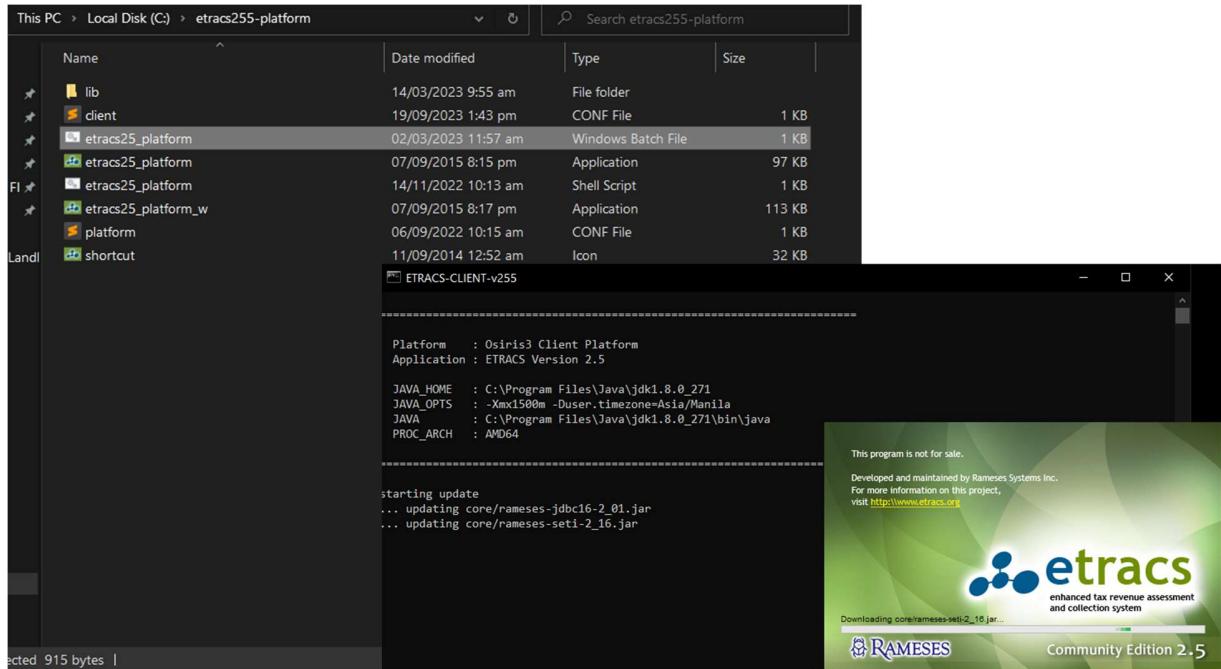
lgu_name=ETRACS TEST
blockingTimeout=300000
app_server_ip=192.168.1.206
pub_app_server_ip=etracs.server
dbserver_host=192.168.1.206
dbserver_user=root
dbserver_pass=P@ssw0rd#
db_etracs=etracs255_tester
db_image=etracs_image
db_notification=etracs_notification
db_epayment=eor
db_queue=queue

channel=00000
channelgroup=etracsgroup
channelgroup_enabled=false
fileupload_channel=${channel}
filesrvr_dir=${osiris.base.dir}/filesrvr

sms_acctname=00000
sms_apikey=0000000000
```

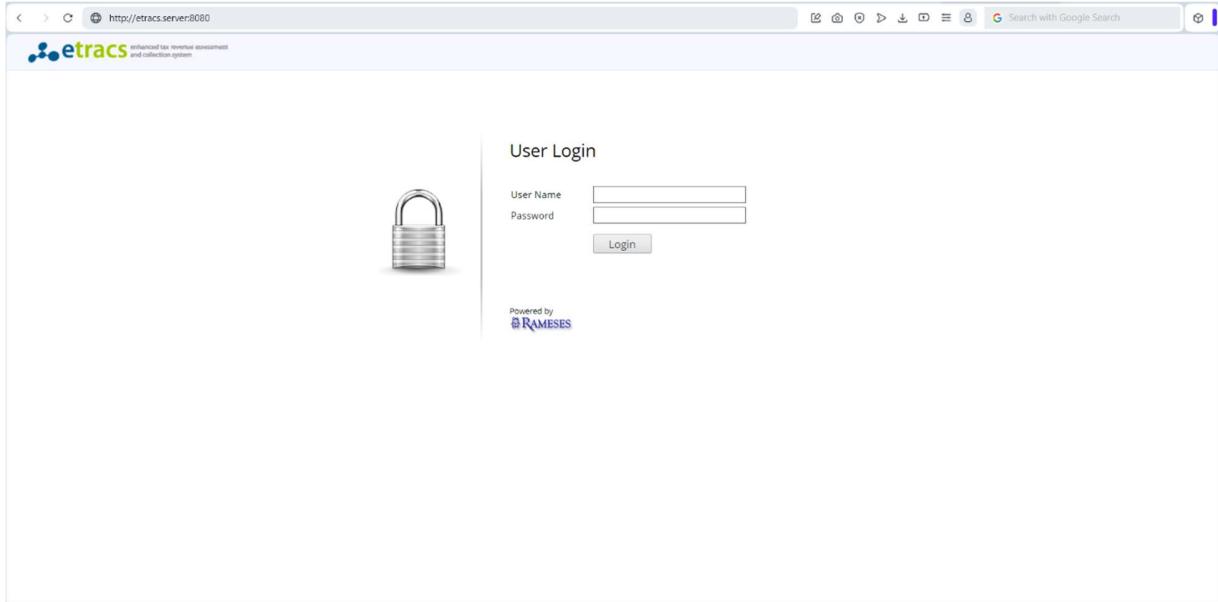
Restart the etracs server for the changes to take effect. **Inform the LGU before restarting the server.**

8. Run the `etracs25_platform.bat` Windows Batch File. Wait for the client to update the jars.



9. Register the New Terminal. Go to your browser and login into the etracs web portal using the domain name.

Ex: <http://etracs.server:8080>



10. Navigate to Administration > Terminals

Two screenshots of the etracs web interface. The top screenshot shows the 'Control Panel' with a red box highlighting the 'Administration' link. The bottom screenshot shows the 'Administration' section of the 'Console' with a red box highlighting the 'Terminals' link under the 'Registers' category.

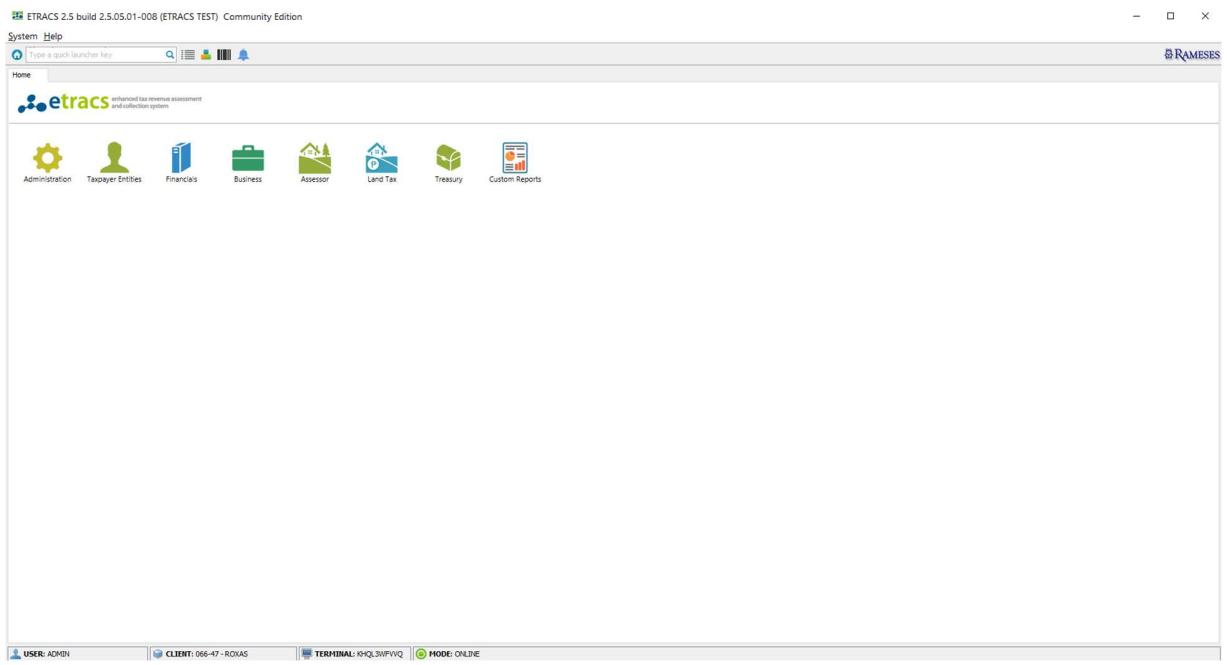
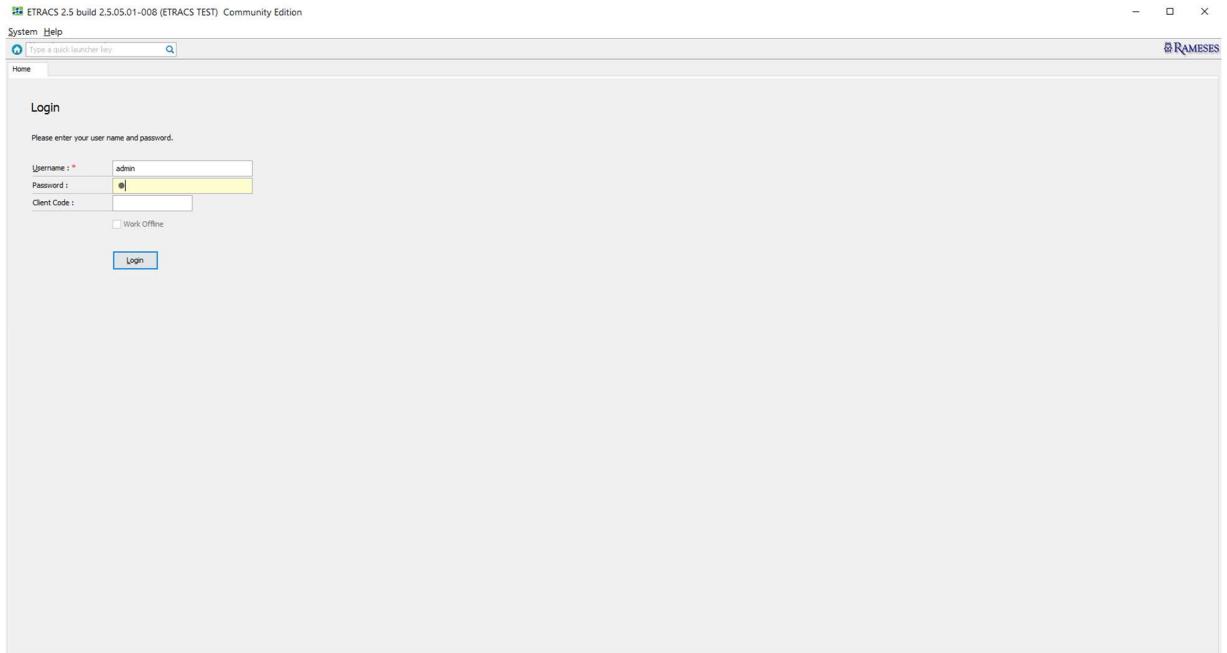
11. Copy a Terminal Key or Generate a new one.

The first screenshot shows a table of terminal keys with columns: Terminal Key, Mac Address, Date Registered, and Registered By. The second screenshot shows a 'Generate Keys' dialog box with an input field for the number of keys to generate, currently set to 10.

12. Paste the copied Terminal Key into the New Terminal Registration Window and click **Submit.**

The screenshot shows the 'New Terminal Registration' window with fields for 'Terminal Key' (containing 'KHQ3WFWQ') and 'Registered By' (containing 'ADMIN'). There are 'Back' and 'Submit' buttons at the bottom.

13. Login to Etracs.



You have successfully connected to the Etracs Server via Remote Access using **OpenVPN**.