

REMOTE CONNECTION VIA VPN (LINUX-UBUNTU)

1 REQUIREMENTS FOR USING THE VPN

To connect a computer that is not part of the PCB network to the Park's VPN, the following is needed:

- That the computer is connected to the internet
- Administrator permission on the computer
- Have a strong two-factor authentication set up for your username

2 INSTALLING THE OPENCONNECT VPN CLIENT

With the introduction of two-factor validation, the VPN client has to open a browser in which the user authentication will be carried out. The Ubuntu 22.04 LTS version already includes the packages in its repositories that integrate this entire process.

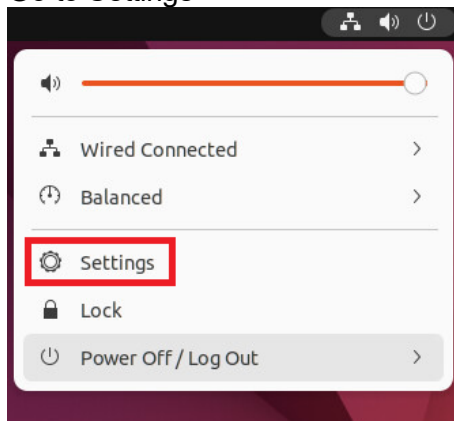
To install the necessary packages, execute the commands:

```
sudo apt update (to update the repository sources)
sudo apt install network-manager-openconnect-gnome
```

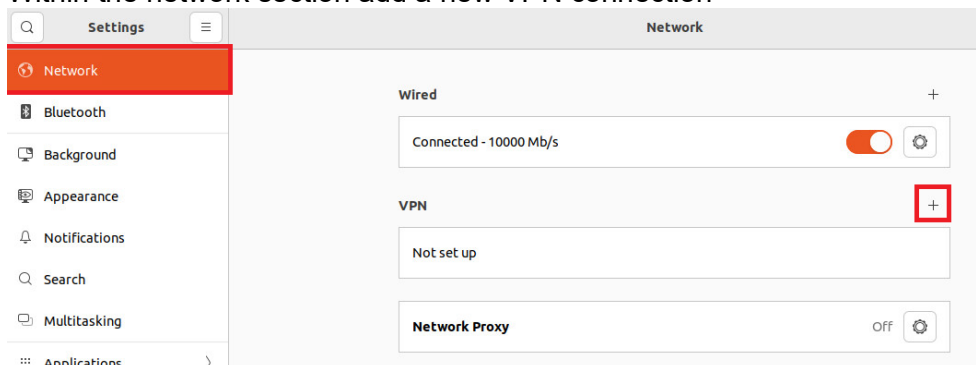
3 SETTING UP THE VPN

Once you have the installed client you must set up the VPN connection following this procedure:

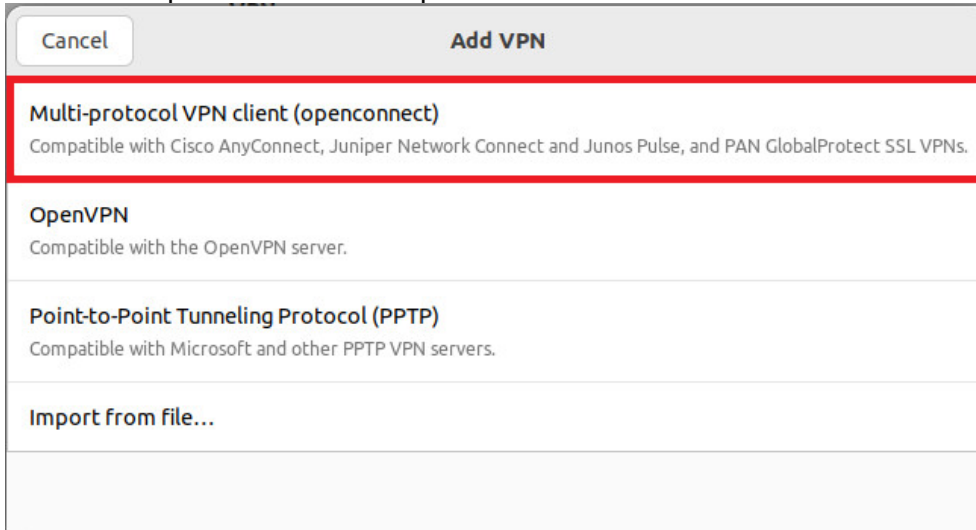
- Go to Settings



- Within the network section add a new VPN connection



- Select the Openconnect client option



Cancel Add VPN

Multi-protocol VPN client (openconnect)
Compatible with Cisco AnyConnect, Juniper Network Connect and Junos Pulse, and PAN GlobalProtect SSL VPNs.

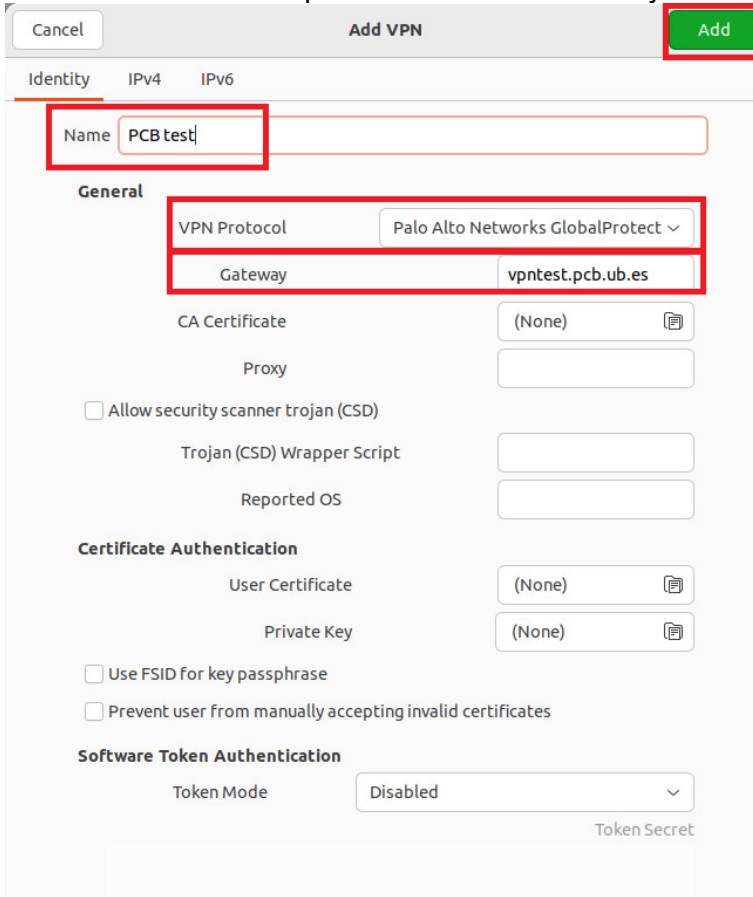
OpenVPN
Compatible with the OpenVPN server.

Point-to-Point Tunneling Protocol (PPTP)
Compatible with Microsoft and other PPTP VPN servers.

Import from file...

- Enter the name you wish to give to this connection, and as a protocol you must select “Palo Alto Networks GlobalProtect”. As a Gateway, enter the VPN portal that applies to you:
 - vnpn.pcb.ub.es for public environments
 - vpne.pcb.ub.es for private companies
 - vpnirb.pcb.ub.es for the IRB

Leave all of the other options as default and then you can add the settings



Cancel Add VPN Add

Identity IPv4 IPv6

Name PCB test

General

VPN Protocol Palo Alto Networks GlobalProtect

Gateway vpntest.pcb.ub.es

CA Certificate (None)

Proxy

Allow security scanner trojan (CSD)

Trojan (CSD) Wrapper Script

Reported OS

Certificate Authentication

User Certificate (None)

Private Key (None)

Use FSID for key passphrase

Prevent user from manually accepting invalid certificates

Software Token Authentication

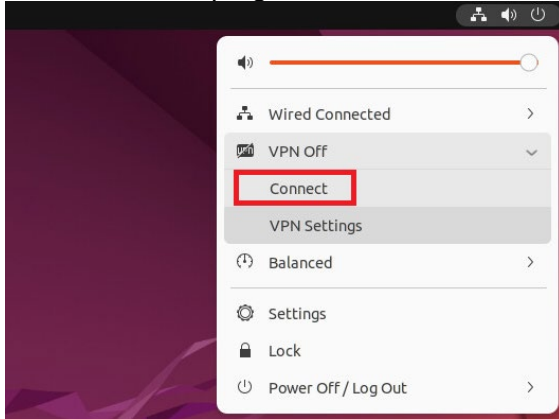
Token Mode Disabled

Token Secret

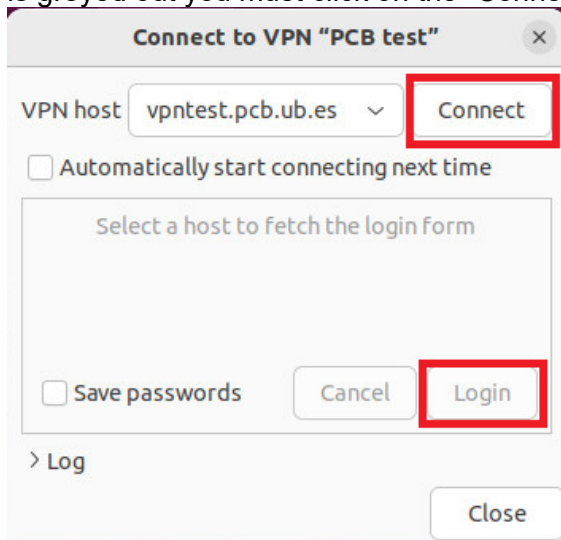
4 CONNECTING THE VPN

We can see this process in the video <https://youtu.be/C9Jno5aBER4>


Once we have configured the settings to connect the VPN, we need to deploy the VPN section in the top right-hand side of the desktop and select the Connect option.



A window will open in which you will have to select the “Login” option. If the “Login” button is greyed out you must click on the “Connect” button first.

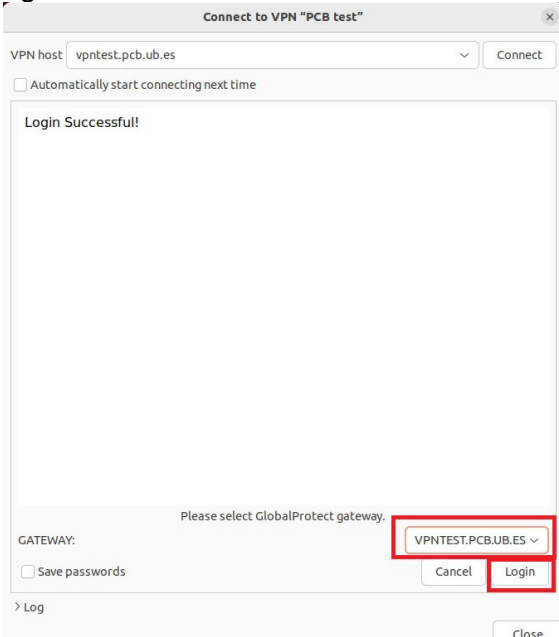


This will open the validation page where you will have to introduce your PCB services' username and password as well as the number that will simultaneously generate the two-factor validation you have set up for your username.



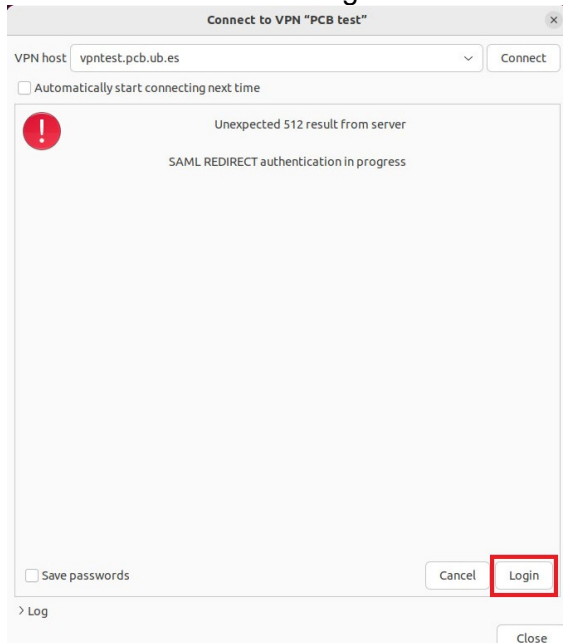
The screenshot shows a window titled "Connect to VPN 'PCB test'". At the top, the "VPN host" is set to "vpntest.pcb.ub.es" with a "Connect" button. Below this, it says "Contacting host, please wait...". There are language options: "English", "Español", and "Català". The Parc Científic de Barcelona logo and name are displayed. A blue box prompts the user to "Please, identify yourself." with a "User name:" field containing "nomusuari" and a "Login" button. Below this, a message states: "A service provider named https://vpntest.pcb.ub.es:443/SAML20/SP needs to authenticate you." At the bottom, there is a "Save passwords" checkbox, "Cancel" and "Login" buttons, and a "Close" button at the very bottom right.

Once correctly validated, check that the gateway is correct and click on the "Login" button again.



The screenshot shows the same "Connect to VPN 'PCB test'" window. The "VPN host" remains "vpntest.pcb.ub.es". A checkbox for "Automatically start connecting next time" is present. The main area displays "Login Successful!". Below this, it says "Please select GlobalProtect gateway." and a dropdown menu is set to "VPNTTEST.PCB.UB.ES", which is highlighted with a red box. There are "Cancel" and "Login" buttons, with the "Login" button also highlighted with a red box. At the bottom, there is a "Save passwords" checkbox, a "Log" link, and a "Close" button.

Now an error message will appear because the SAML authentication is in progress, you must then click on the “Login” button for a third time.



You will now be connected to the VPN and have access to the internal resources on the PCB network.

5 DISCONNECTING THE VPN

To disconnect the VPN, you just need to open the VPN section in the top right-hand side of the desktop again and select “Turn Off”.

