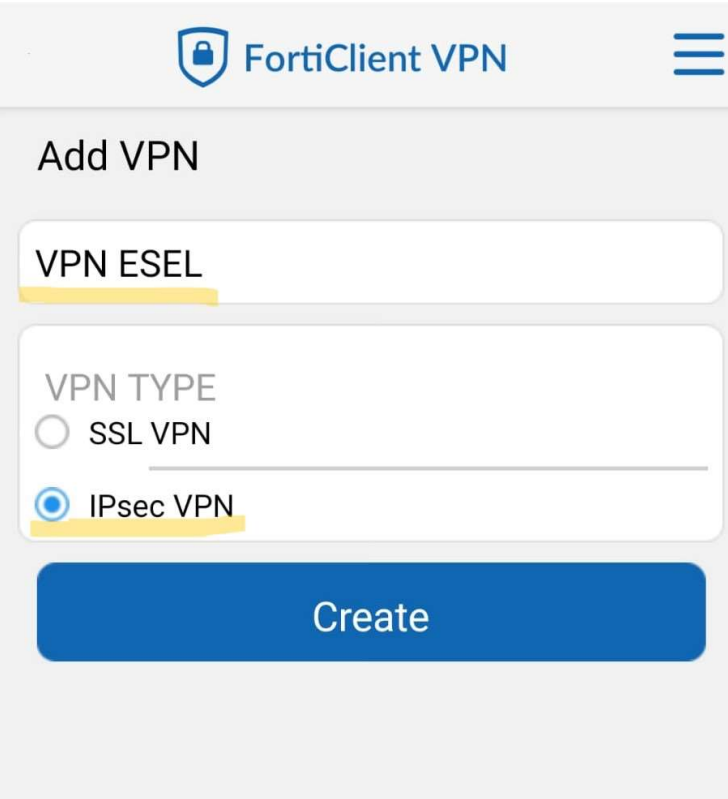


# VPN ESEL

Configuração

# Passo 1



FortiClient VPN

Add VPN

VPN ESEL

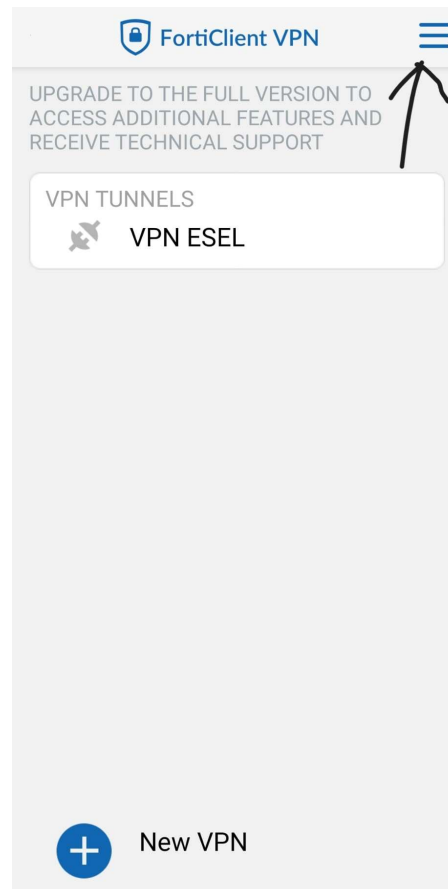
VPN TYPE

SSL VPN

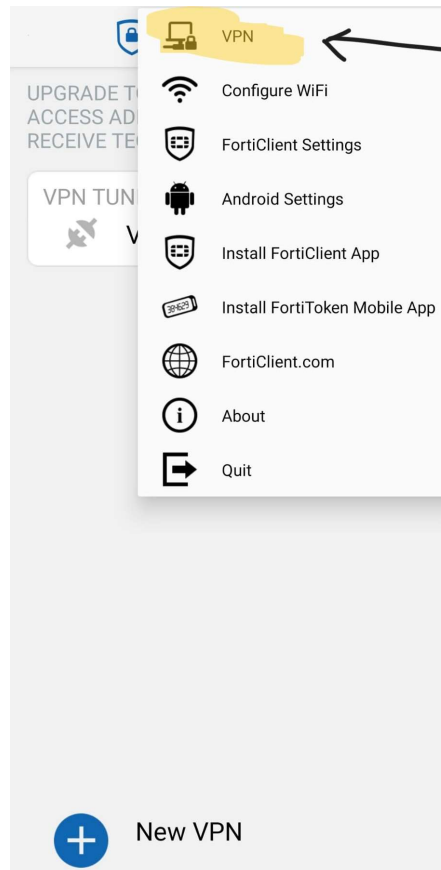
IPsec VPN

Create

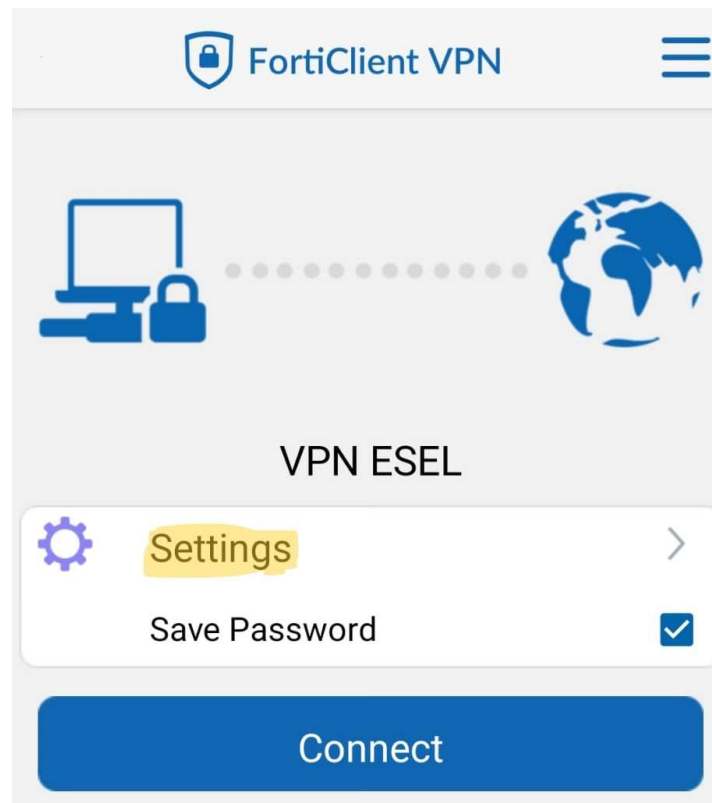
# Passo 2



# Passo 3



# Passo 4



# Passo 5

FortiClient VPN

IPsec VPN settings

Tunnel name  
VPN ESEL

Server settings  
Remote gateway settings

IPsec phase 1 settings  
Encryption and authentication for phase 1

IPsec XAuth settings  
XAuth and user settings

IPsec phase 2 settings  
Encryption and authentication for phase 2

---

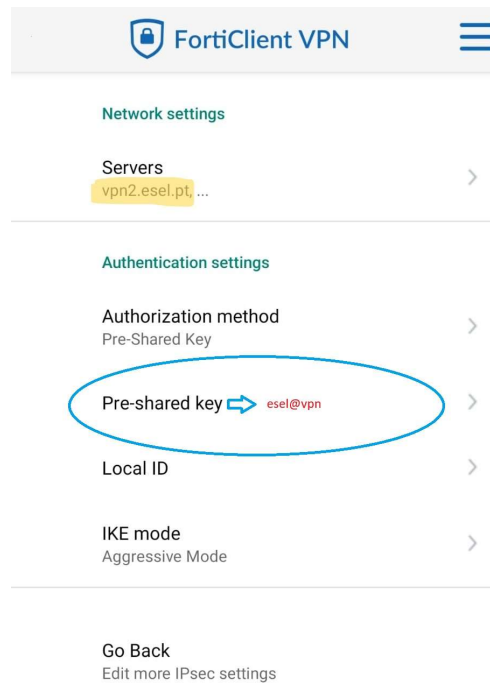
Delete VPN

Delete this VPN tunnel profile  
Lose all these settings and remove it from the list of VPN tunnels

# Passo 6

**Pre-shared key:**  
esel@vpn

**Servers -> Remote Gateways:**  
vpn2.esel.pt



The screenshot shows the FortiClient VPN settings interface. At the top, there is a header with the FortiClient VPN logo and a menu icon. Below the header, the settings are organized into sections: Network settings, Authentication settings, and IKE mode. Under Network settings, there is a 'Servers' section with a list item 'vpn2.esel.pt, ...'. Under Authentication settings, there are four items: 'Authorization method' (Pre-Shared Key), 'Pre-shared key' (with a blue arrow pointing to 'esel@vpn'), 'Local ID', and 'IKE mode' (Aggressive Mode). At the bottom, there is a 'Go Back' button and a link to 'Edit more IPsec settings'.

FortiClient VPN

Network settings

Servers  
vpn2.esel.pt, ...

Authentication settings

Authorization method  
Pre-Shared Key

Pre-shared key → esel@vpn

Local ID

IKE mode  
Aggressive Mode

Go Back  
Edit more IPsec settings

# Passo7

