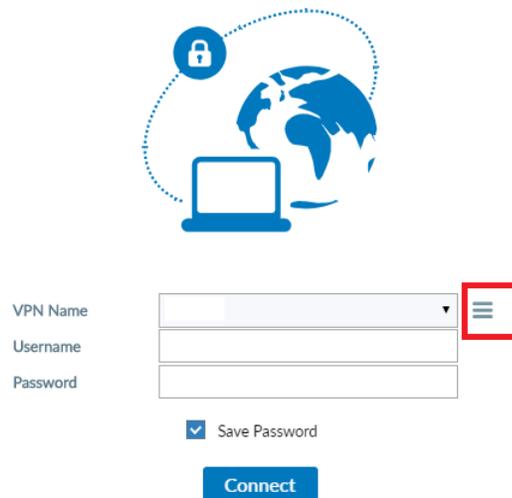
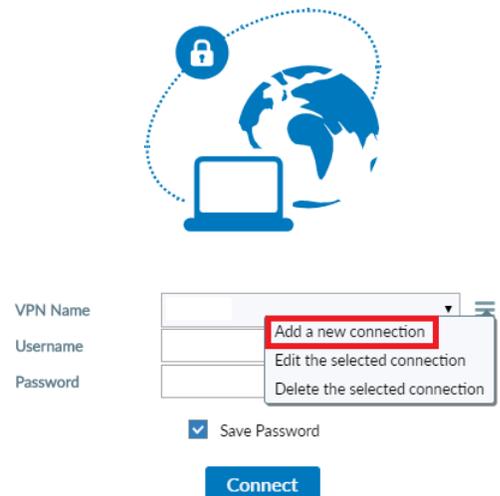


IPsec VPN Configuration

- 1) Download the Forticlient from <https://www.fortinet.com/support/product-downloads#vpn>
- 2) Download the appropriate file based on your installed Operating System. You can find 4 files for different operating systems, please choose the compatible one:
 - IOS
 - Android
 - Windows
 - MAC
- 3) Download the Forticlient exe file. Once downloaded, please install the application on your device.
- 4) Follow the installation steps to download this software and make sure that the VPN client is installed successfully.
- 5) Make sure to accept the license agreement and choose secure remote access:
FortiClientMiniSetup_X: meaning FortiClientMiniSetup_Operating System
- 6) Click on the  → **Add a new connection**



The image shows the FortiClient VPN configuration interface. At the top, there is a blue icon of a globe with a padlock and a laptop. Below this, there are three input fields: "VPN Name", "Username", and "Password". To the right of the "VPN Name" field is a hamburger menu icon (three horizontal lines) enclosed in a red square. Below the input fields is a checked checkbox labeled "Save Password" and a blue "Connect" button.



The image shows the FortiClient VPN configuration interface with a dropdown menu open. The dropdown menu is positioned over the "VPN Name" field and contains three options: "Add a new connection", "Edit the selected connection", and "Delete the selected connection". The "Add a new connection" option is highlighted with a red box. Below the input fields is a checked checkbox labeled "Save Password" and a blue "Connect" button.

- 7) Choose **IPsec VPN**

New VPN Connection

VPN SSL-VPN **IPsec VPN**

Connection Name

Description

Remote Gateway ✕
 +Add Remote Gateway

Authentication Method Pre-shared key ▼

Authentication (XAuth) Prompt on login Save login Disable

+ Advanced Settings

Cancel **Save**

8) Enter the below:

Connection Name: **cpanel**

Description: **cpanel**

Remote Gateway: **194.126.14.20**

Authentication Method: Pre-Shared Key → **Please contact the support team if you don't have it**

Authentication (XAuth) → choose **Prompt on login**

New VPN Connection

VPN SSL-VPN **IPsec VPN**

Connection Name

Description

Remote Gateway ✕
 +Add Remote Gateway

Authentication Method Pre-shared key ▼

Authentication (XAuth) Prompt on login Save login Disable

9) Click on **Advanced Settings**

10) The VPN Settings should be as below:

— VPN Settings

IKE Version 1 Version 2 (not available with the free client)

Mode Main Aggressive

Options Mode Config Manually Set DHCP over IPsec

11) Click on **Phase 1**

12) The configuration should be as below:

— Phase 1

IKE Proposal Encryption Authentication

Encryption Authentication

DH Group 1 2 5 14 15

16 17 18 19 20

Key Life sec

Local ID

Dead Peer Detection

NAT Traversal

13) Click on **Phase 2**

14) The configuration should be as below:

— Phase 2

IKE Proposal Encryption Authentication

Encryption Authentication

Key Life Seconds

KBytes

Enable Replay Detection

Enable Perfect Forward Secrecy (PFS)

DH Group

15) Click on **Save**

16) Once configuration done, from the FortiClient Console, click on **Remote Access icon** → choose your personal account registered above → enter your VPN credentials:

Username → **enter your VPN Username** (ex: abcdef.vpn)

Password → **enter your VPN Password**

17) Click on **Connect** and you will be successfully connected to the VPN



VPN Name **cpanel**
IP Address **x.x.x.x**
Username **abcdef.vpn**
Duration 00:00:03
Bytes Received 2.06 KB
Bytes Sent 6.65 KB

Disconnect