

Using Windows:


1. Visit <https://www.fortinet.com/support/product-downloads> and locate the **Forticlient VPN** located towards the bottom of the page and select the appropriate Operating System (**Windows**)

FortiClient VPN

The VPN-only version of FortiClient offers SSL VPN and IPsecVPN, but does not include any support. Download the best VPN software for multiple devices.


Remote Access

- ✓ SSL VPN with MFA
- ✓ IPSEC VPN with MFA




Download VPN for Windows

DOWNLOAD




Download VPN for MacOS

DOWNLOAD




Download VPN for Linux

DOWNLOAD .rpm




Download VPN for iOS

DOWNLOAD



Download VPN for Android

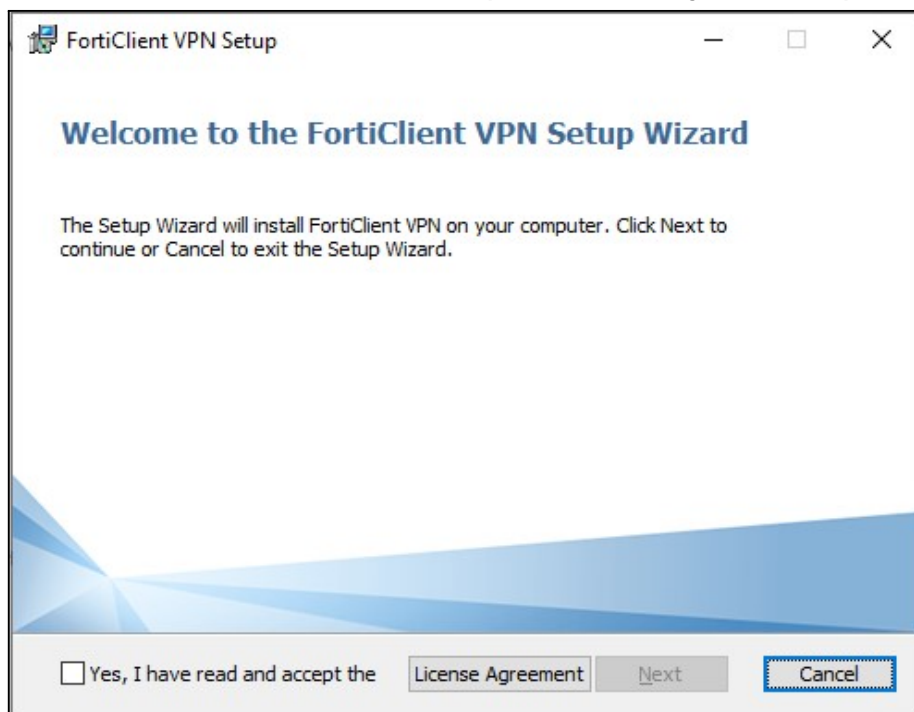
DOWNLOAD



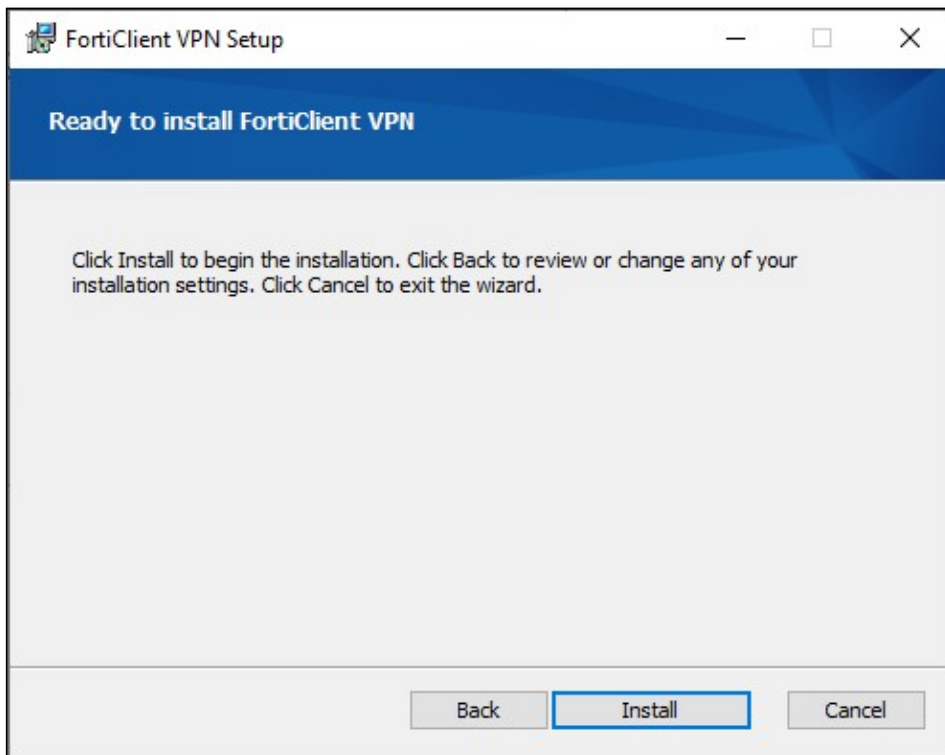
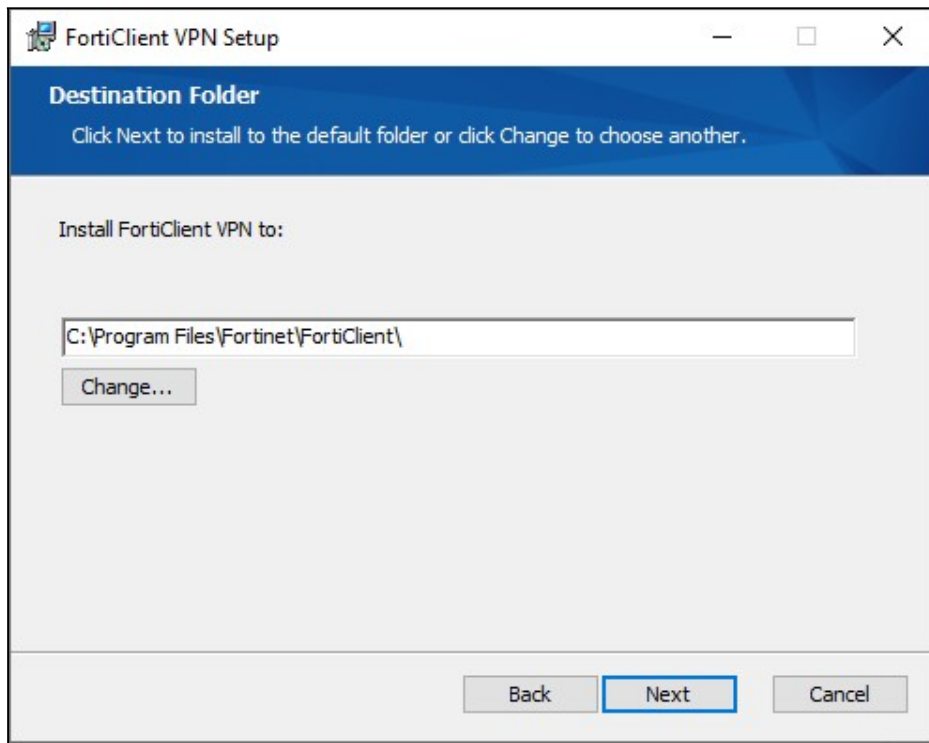
Download VPN for Linux

DOWNLOAD .deb

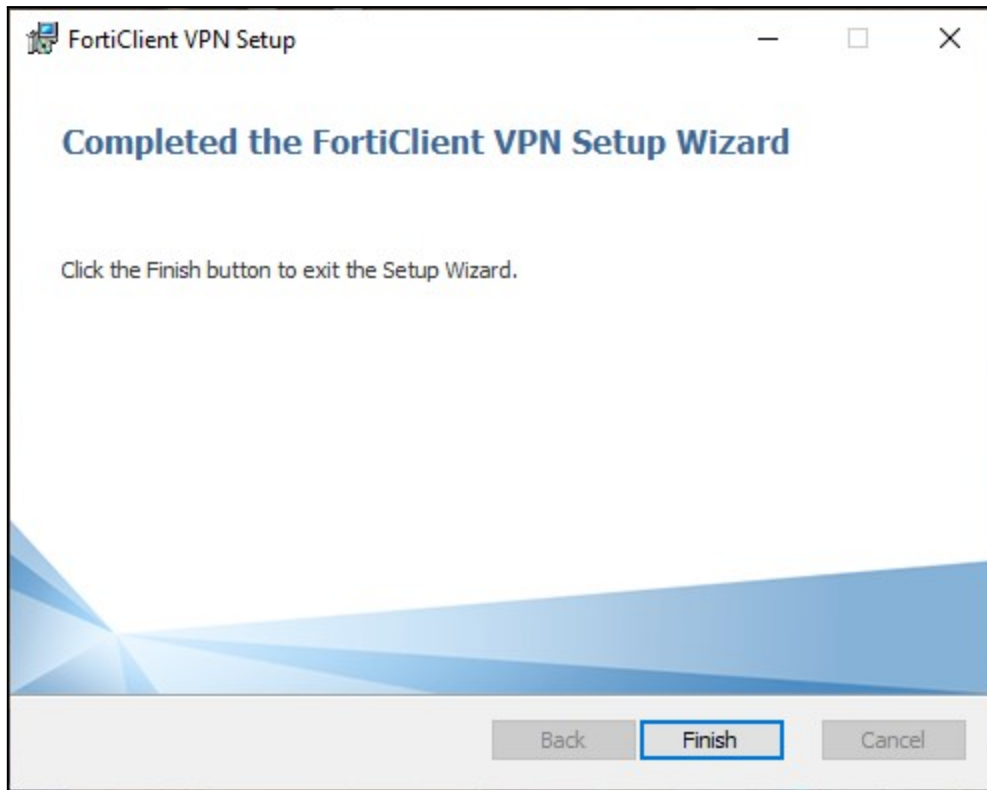
2. Run the downloaded installer and proceed through the setup wizard.



3. Read and accept the license agreement, then select the folder location and click **Next**, then **Install**



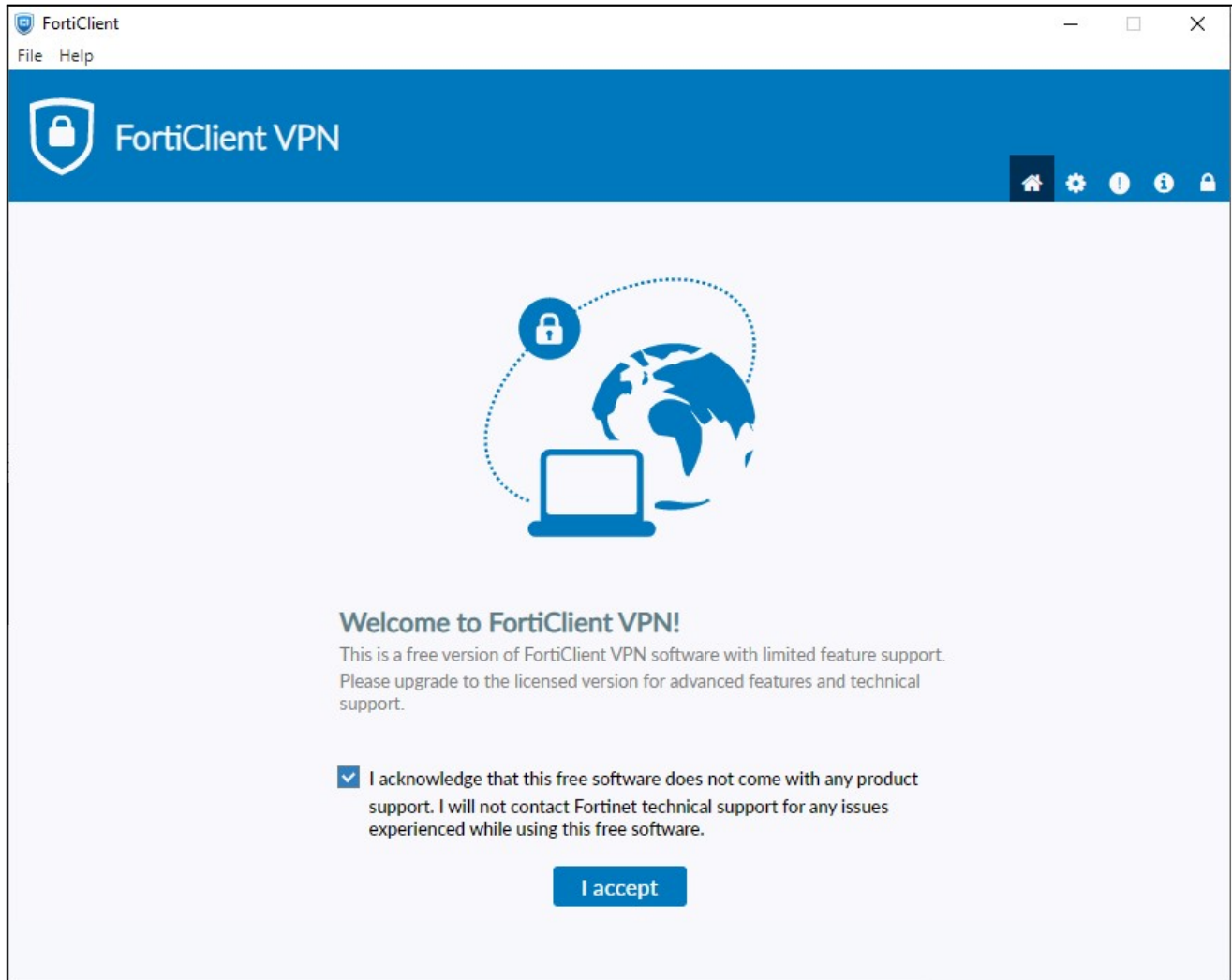
4. Once the **Installation** is finished click **Finish**.



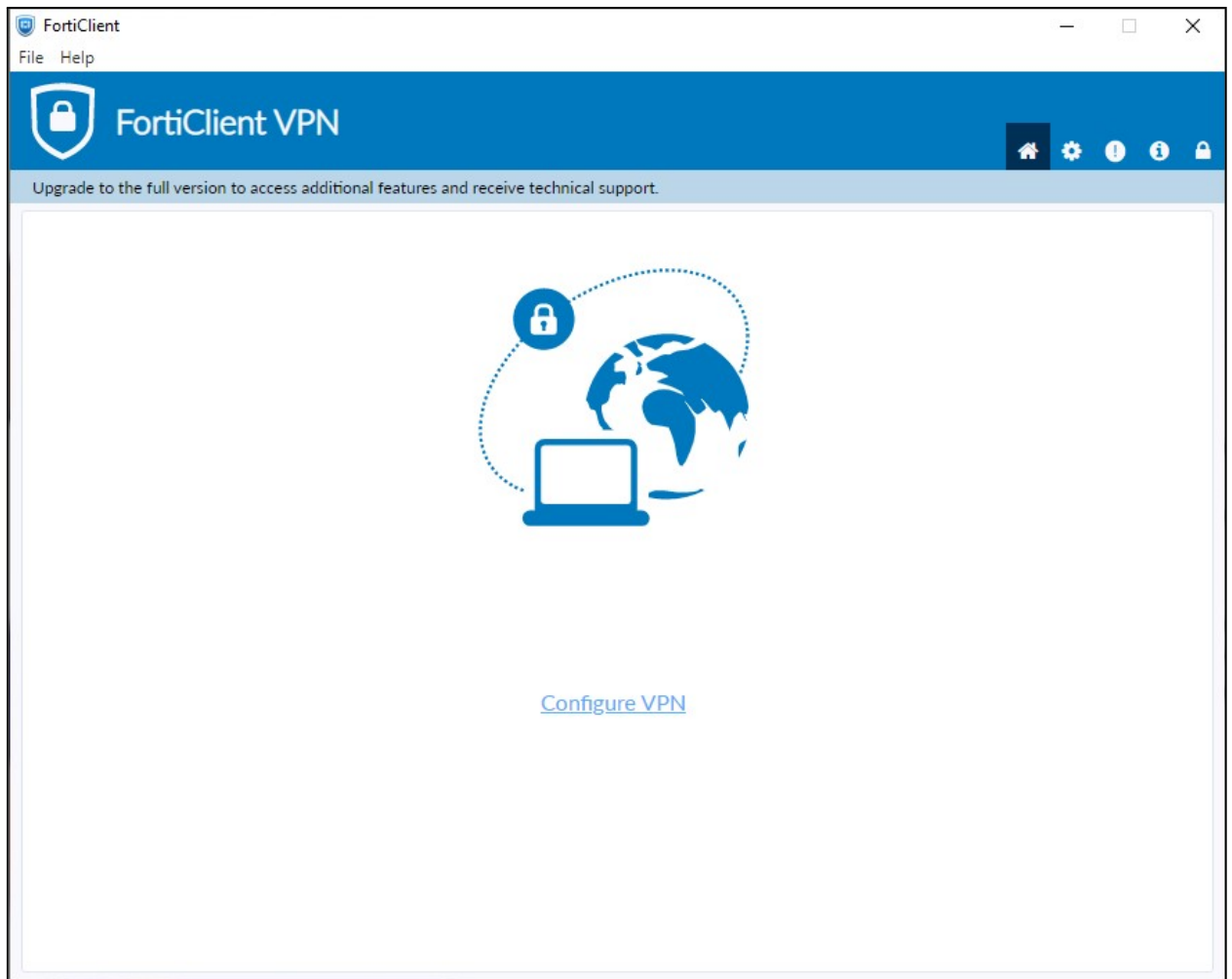
5. Locate and **Double-Click** the “Forticlient VPN” shortcut on your **desktop**



6. Once the Client is open click the **box located next to the acknowledged agreement** and click **“I accept”**.



7. Click **Configure VPN**.



8. Enter the **configurations** for the VPN as follows:
- a. VPN: Select **IPsec VPN**.
 - b. Connection Name: **Name of your choosing** (e.g. **CS VPN**)
 - c. Description: **Any**
 - d. Remote Gateway: **128.82.11.11**
 - e. Authentication Method: **Pre-shared key**
 - f. Pre-shared key: **DnS6fS7Zm^&***

New VPN Connection

VPN SSL-VPN **IPsec VPN** XML

Connection Name

Description

Remote Gateway ✕
 + Add Remote Gateway

Authentication Method Pre-shared key ▼

Authentication (XAuth) ☒ Prompt on login ☐ Save login ☐ Disable

Failover SSL VPN [None] ▼

+ Advanced Settings

Cancel Save

8. Click the + next to **Advanced Settings**. (Advanced Settings should be set as followed)

a. Click the + next to **VPN Settings**:

- i. IKE: **Version 1**.
- ii. Mode: **Main**.
- iii. Options: **Mode Config**.

— VPN Settings

IKE ☒ Version 1 ☐ Version 2

Mode ☒ Main ☐ Aggressive

Options ☒ Mode Config ☐ Manually Set ☐ DHCP over IPsec

b. Click the + next to **Phase 1**:

- i. Click the **box next to Dead Peer Detection**.

Phase 1

IKE Proposal

Encryption AES128 Authentication SHA1

Encryption AES256 Authentication SHA256

DH Group

1 2 5 14 15

16 17 18 19 20

Key Life 86400 sec

Local ID Optional

☒ Dead Peer Detection

☒ NAT Traversal

☐ Enable Local LAN

9. Once these settings are applied click **Save**.

Cancel Save

10. Select your created VPN Connection from the **drop down menu**. Enter your ODU **CS Credentials** and click **Connect**.



VPN Name
Username
Password

VPN Connection 1 ▼

Personal VPNs

VPN Connection 1



☐ Save Password

Connect



VPN Name
Username
Password

VPN Connection 1 ▼


cs_



☐ Save Password

Connect

Note: To edit or add a connection click the **3 lines (Hamburger)** next to the **VPN name**:



The interface features a blue icon at the top center depicting a globe with a laptop in front of it and a padlock icon above the laptop, all connected by a dotted line. Below this icon, on the left, are labels for 'VPN Name', 'Username', and 'Password'. To the right of these labels are input fields. The 'VPN Name' field is a dropdown menu currently showing 'VPN Connection 1'. To the right of the dropdown is a hamburger menu icon (three horizontal lines). Below the dropdown, there are two empty input fields for 'Username' and 'Password'. Below these fields is a checkbox labeled 'Save Password'. At the bottom center is a blue button labeled 'Connect'.

VPN Name

VPN Connection 1

Username

Password

☐ Save Password

Connect

- Add a new connection
- Edit the selected connection
- Delete the selected connection

11. After clicking connect, you will receive a DUO push notification to your mobile device.