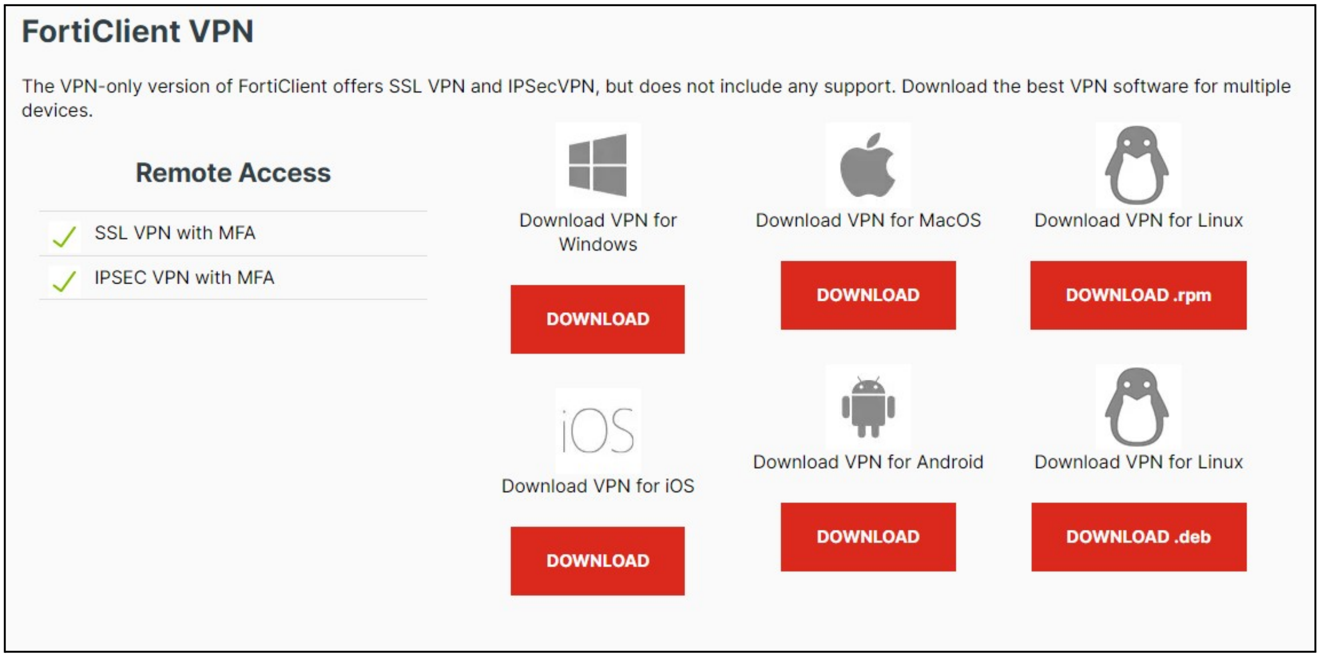
<u>Using Mac:</u>

1. Visit https://www.fortinet.com/support/product-downloads and locate the **Forticlient VPN** located towards the bottom of the page and select the (**Download for MacOS**) option.



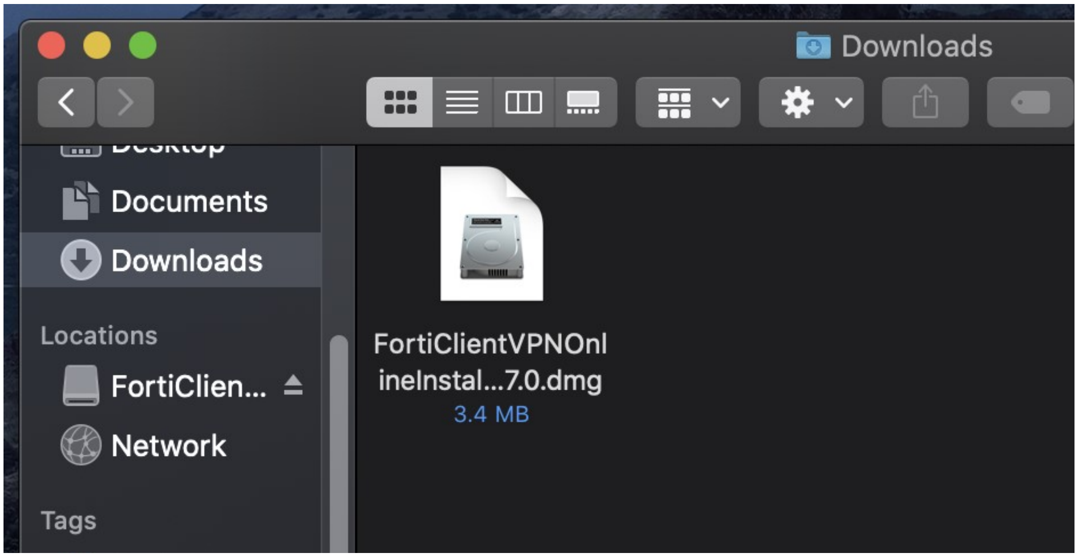
FortiClient VPN

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.

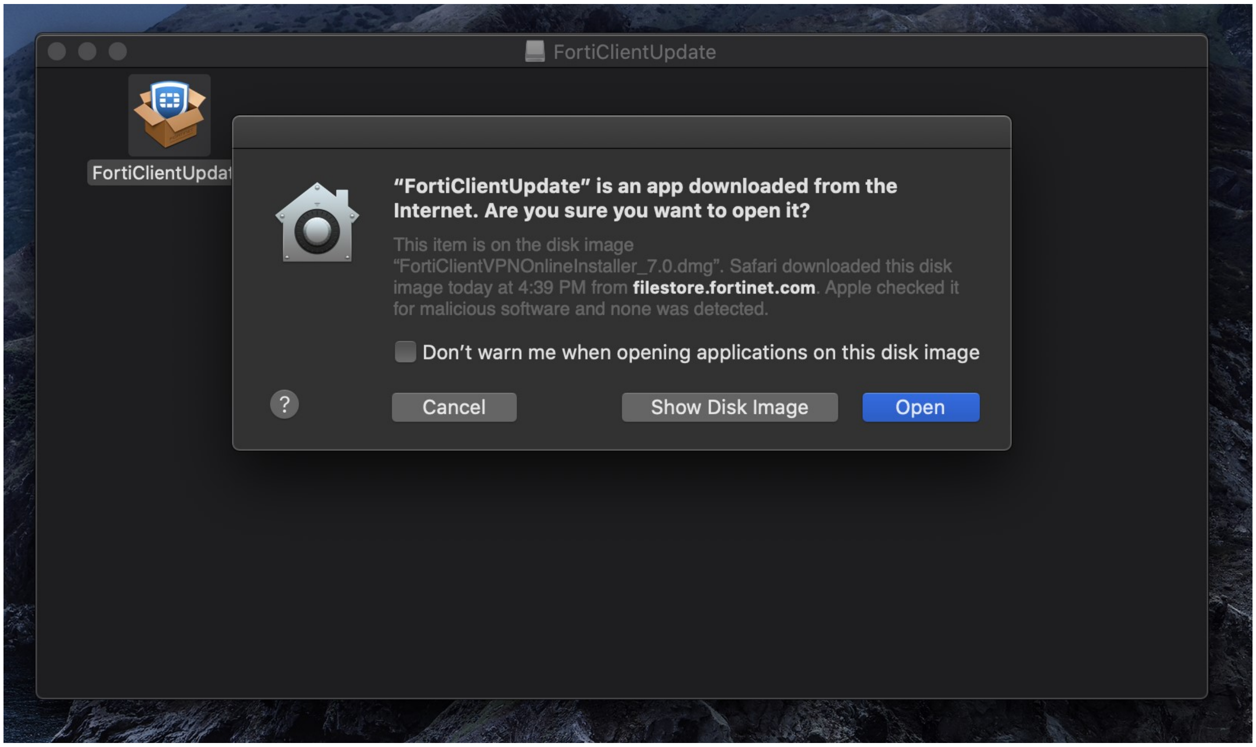
Remote Access

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

2. Open and **run** the downloaded **FortiClient.dmg** file which will proceed to download the **FortiClientUpdate** package.



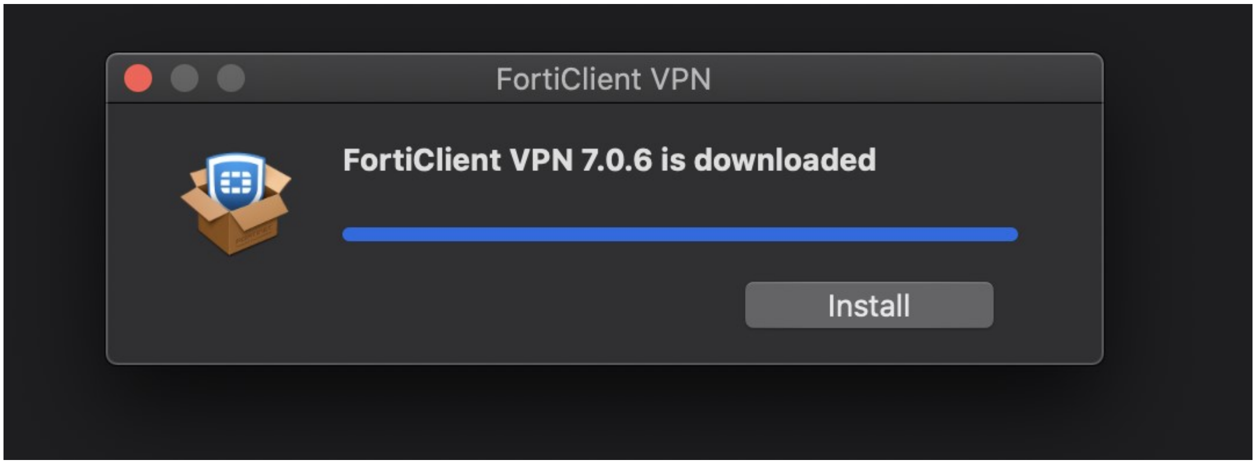
3. **Run** the newly downloaded **FortiClientUpdate** package. It will ask for permission to download and install the app.



“FortiClientUpdate” is an app downloaded from the Internet. Are you sure you want to open it?

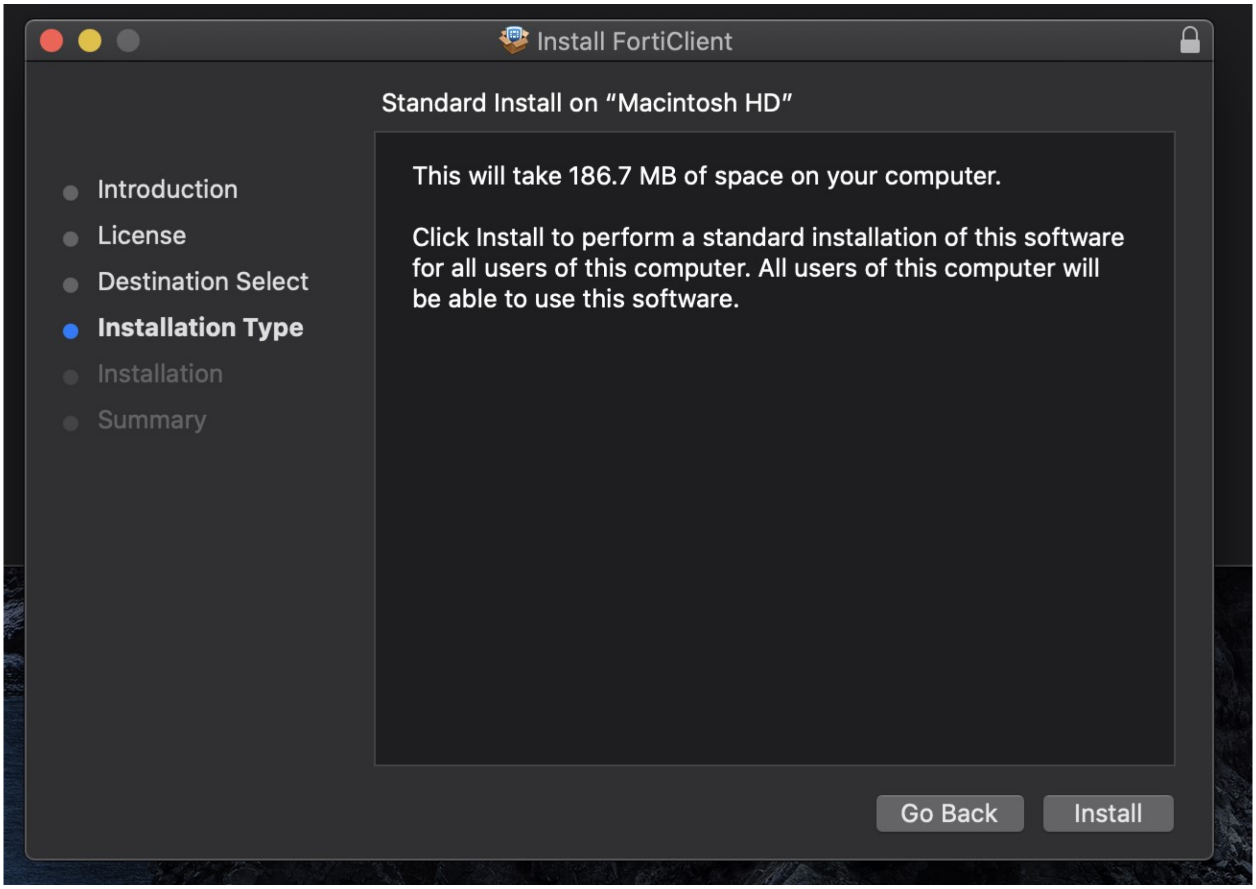
This item is on the disk image “FortiClientVPNOnlineInstaller_7.0.dmg”. Safari downloaded this disk image today at 4:39 PM from **filestore.fortinet.com**. Apple checked it for malicious software and none was detected.

□ Don’t warn me when opening applications on this disk image



FortiClient VPN 7.0.6 is downloaded

4. **Proceed** with the installation wizard, choosing install destination and accepting license agreements. Finally, click **install**.

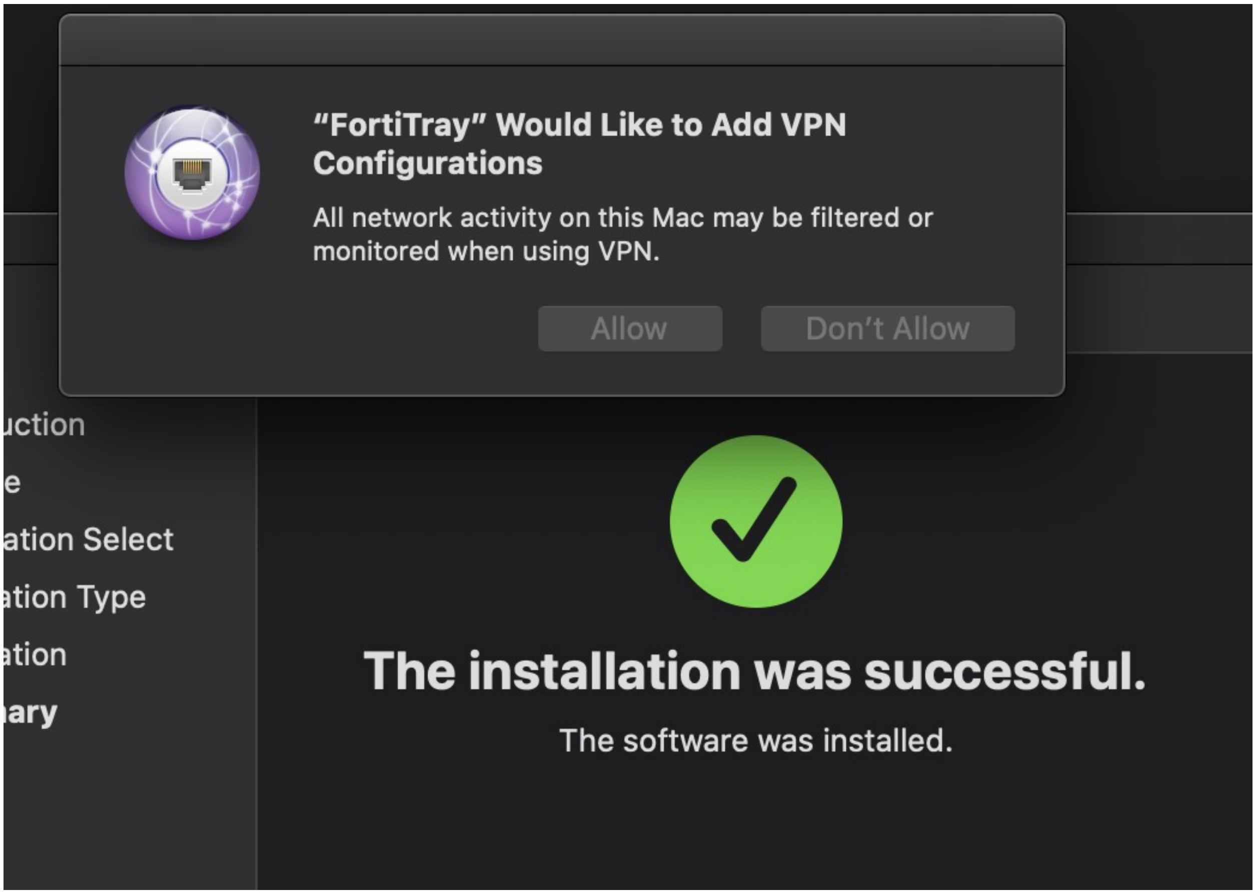


Standard Install on "Macintosh HD"

This will take 186.7 MB of space on your computer.

Click Install to perform a standard installation of this software for all users of this computer. All users of this computer will be able to use this software.

5. After a successful installation, it will ask for permission to add **FortiTray VPN Configurations** to your device. Click **Allow** and proceed.



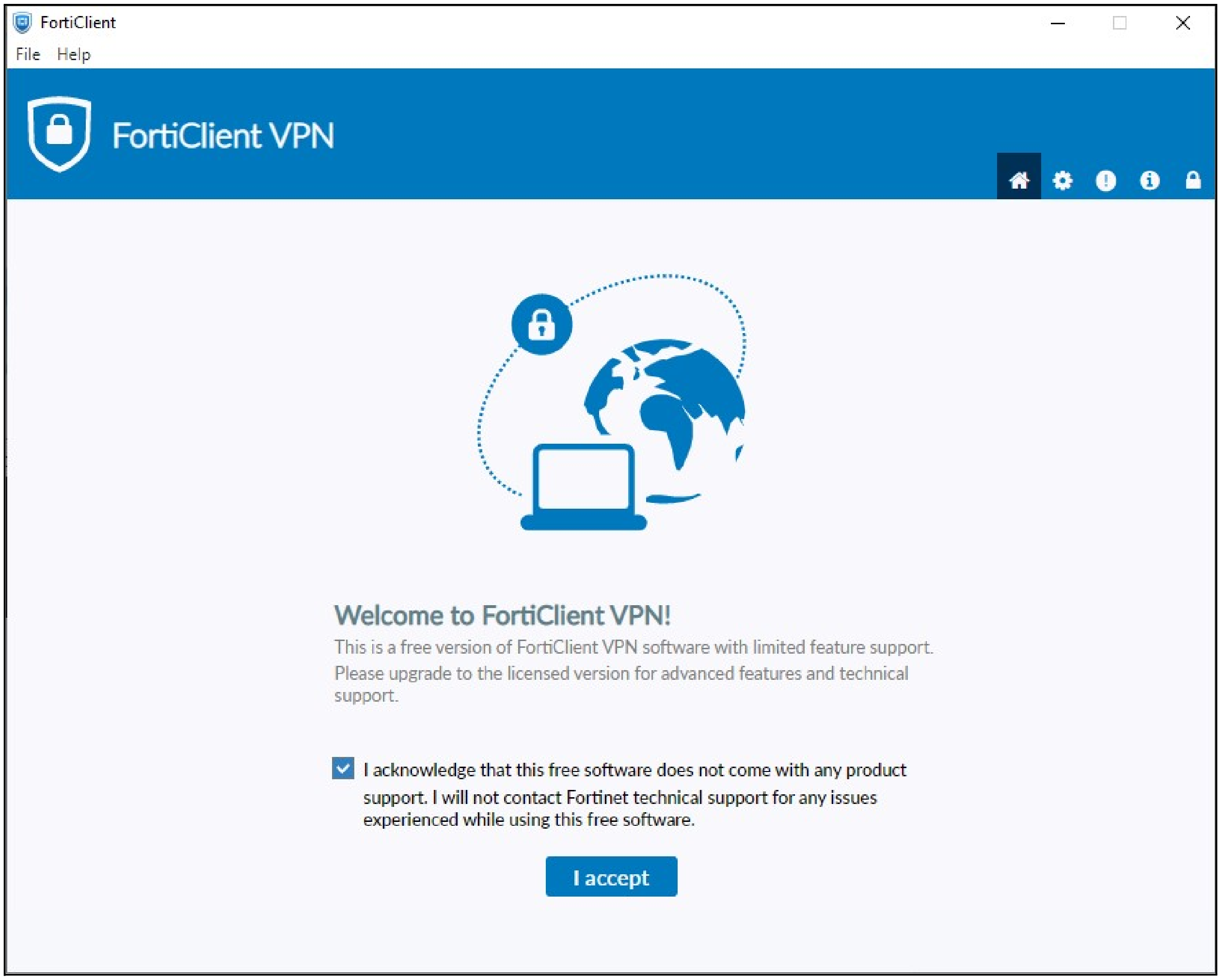
“FortiTray” Would Like to Add VPN Configurations

All network activity on this Mac may be filtered or monitored when using VPN.

The installation was successful.

The software was installed.

6. After it has been installed, search Finder for the newly installed **FortiClient**. Once the Client is open click the **box located next to the acknowledged agreement** and click “**I accept**”.

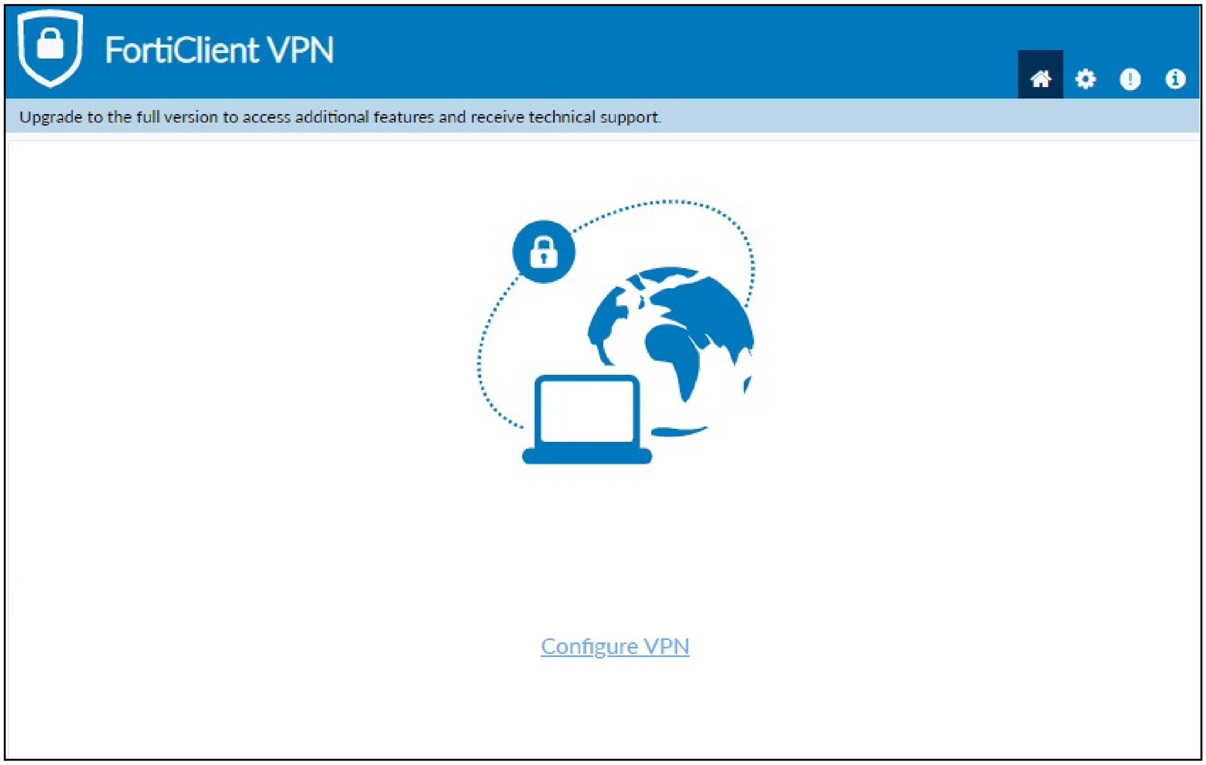


Welcome to FortiClient VPN!

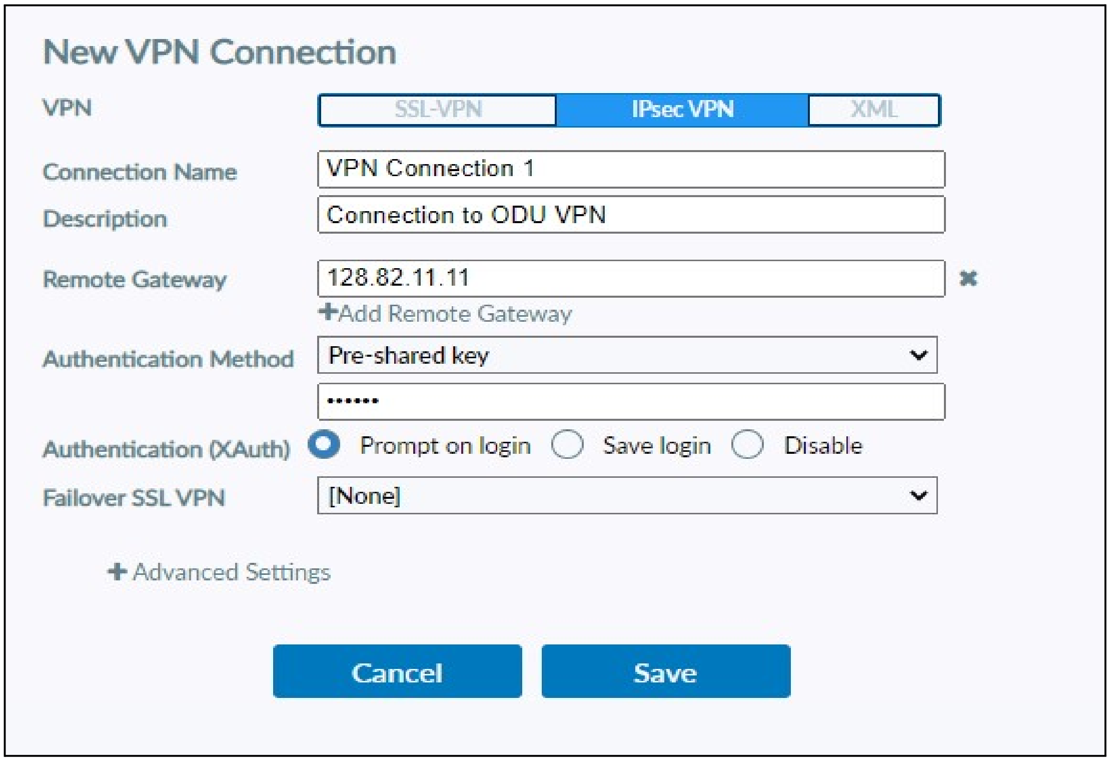
This is a free version of FortiClient VPN software with limited feature support. Please upgrade to the licensed version for advanced features and technical support.

☑ I acknowledge that this free software does not come with any product support. I will not contact Fortinet technical support for any issues experienced while using this free software.

7. Click **Configure VPN**.


FortiClient VPN
Upgrade to the full version to access additional features and receive technical support.
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 (**DnS6fS7Zm^&***)



New VPN Connection

VPN: SSL-VPN | **IPsec VPN** | XML

Connection Name: VPN Connection 1

Description: Connection to ODU VPN

Remote Gateway: 128.82.11.11 ✖

+Add Remote Gateway

Authentication Method: Pre-shared key

••••••

Authentication (XAuth): ● Prompt on login ○ Save login ○ Disable

Failover SSL VPN: [None]

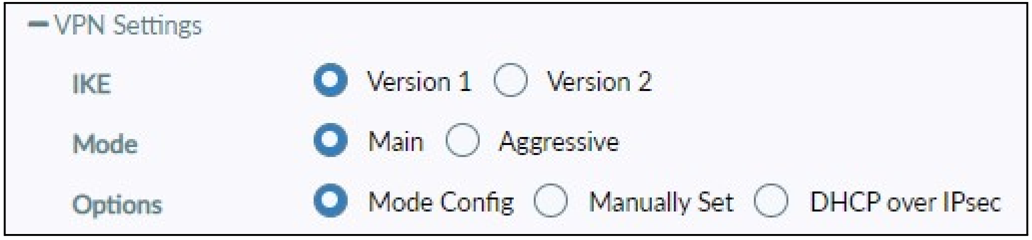
9. Click the **+** next to **Advanced Settings**. (Advanced Settings should be set as followed)

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

      i. IKE: **Version 1.**

      ii. Mode: **Main.**

      iii. Options: **Mode Config**.



− VPN Settings

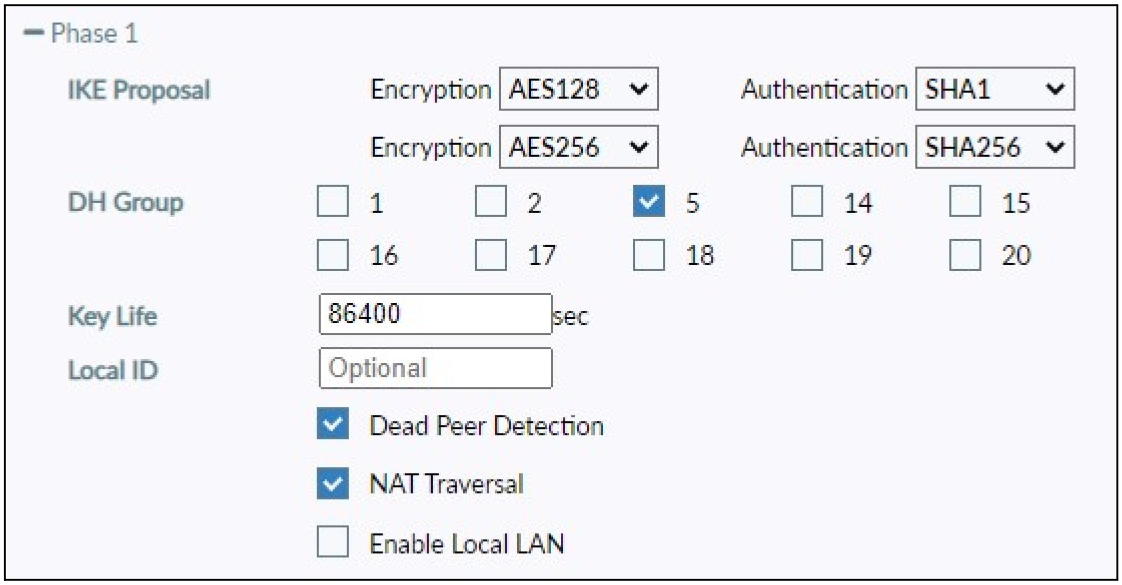
IKE: ● Version 1 ○ Version 2

Mode: ● Main ○ Aggressive

Options: ● Mode Config ○ Manually Set ○ DHCP over IPsec

   g. 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

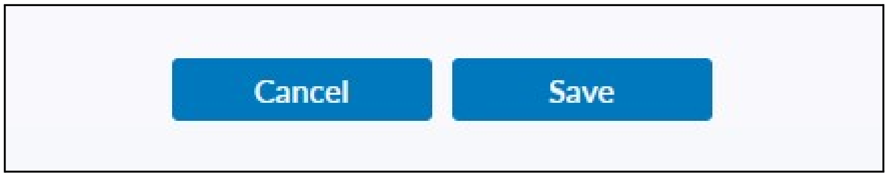
Local ID Optional

☑ Dead Peer Detection

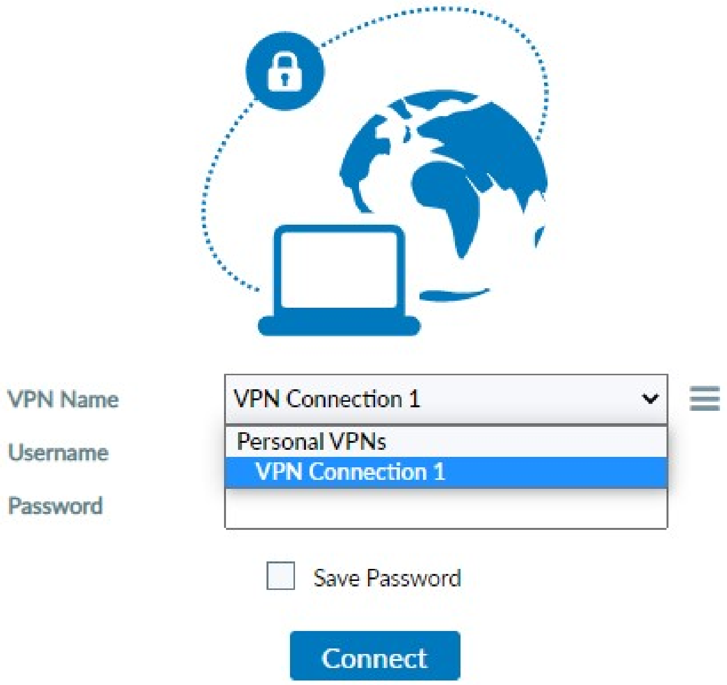
☑ NAT Traversal

☐ Enable Local LAN

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



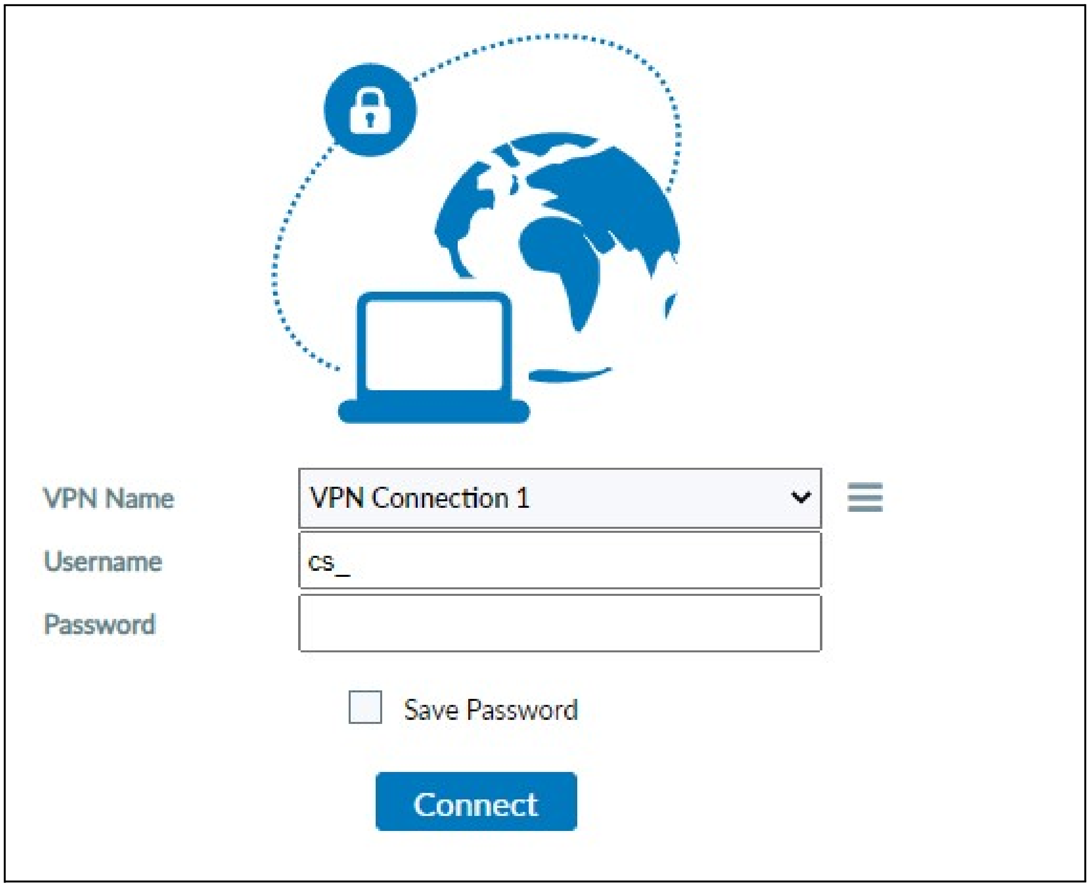
13. Select your created VPN Connection from the **drop down menu.** Enter your ODU **CS Credentials** and click **Connect.**



VPN Name: VPN Connection 1

Username

Password



VPN Name: VPN Connection 1

Username: cs_

Password