

ODU Computer Science VPN Documentation

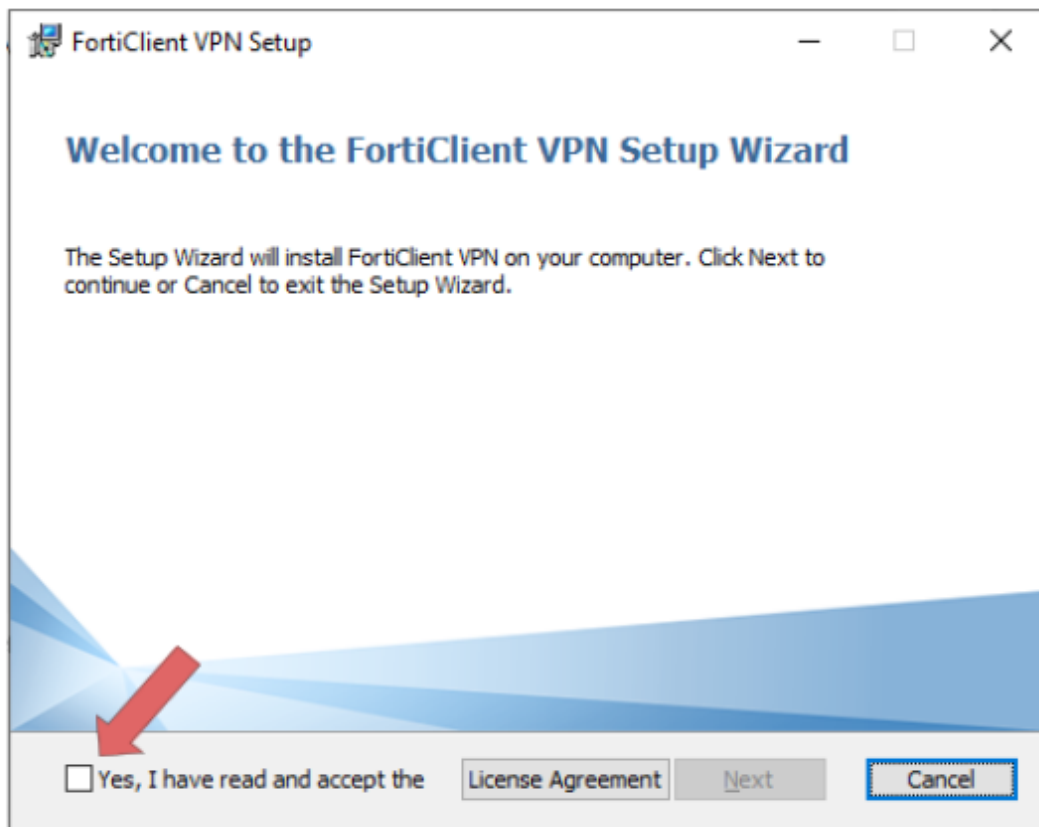
Using Windows:.....	2
Using Mac:.....	12
Using Linux:.....	21
FAQ/Trouble-shooting:.....	22

Using Windows:

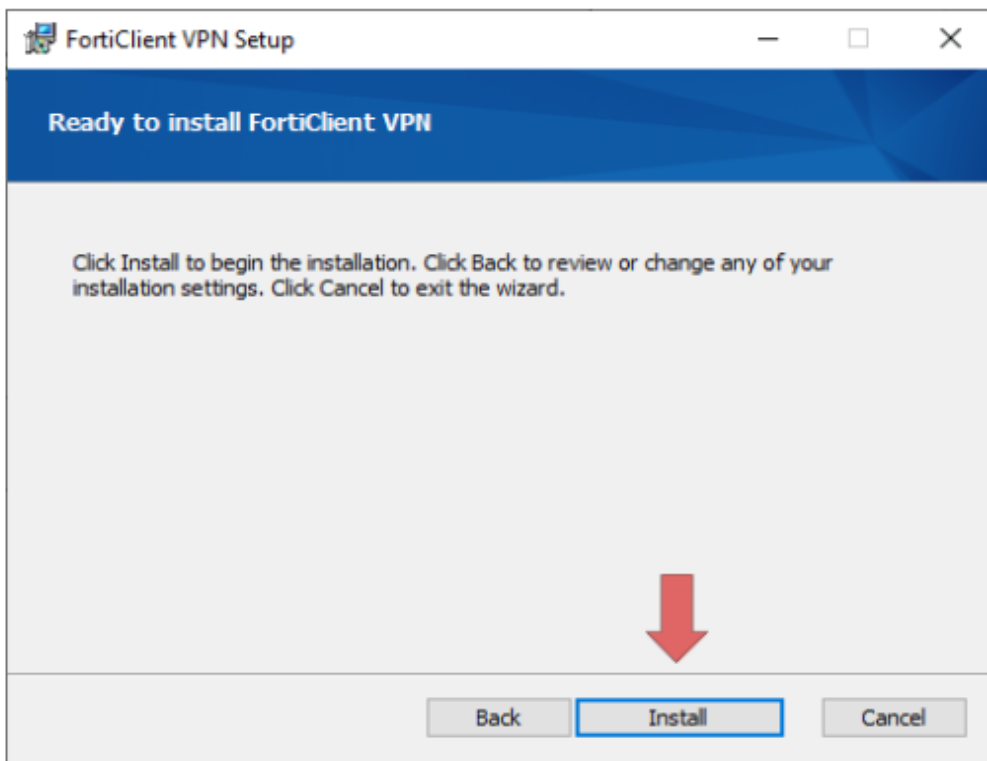
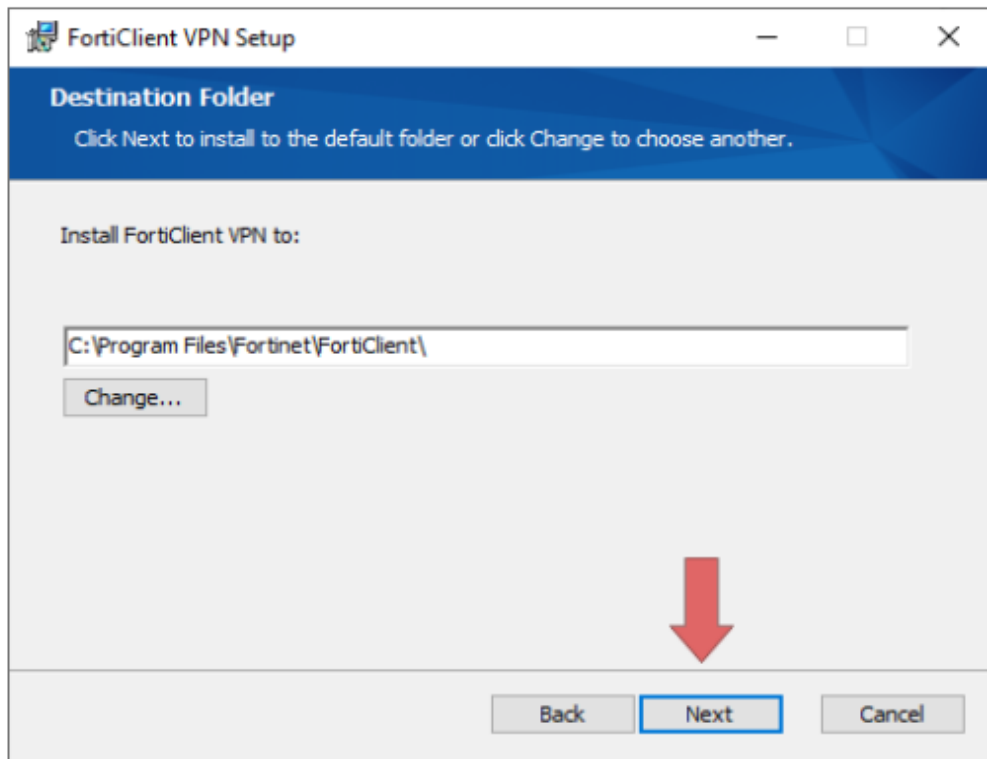
1. Visit <https://links.fortinet.com/forticlient/win/vpnagent> to download the Forticlient VPN (Windows).
 - a. This is a direct installation link, it will lead you to a blank page and prompt you to install.

 FortiClientVPNOnlineInstaller 7/22/2022 12:45 PM Application 3,142 KB

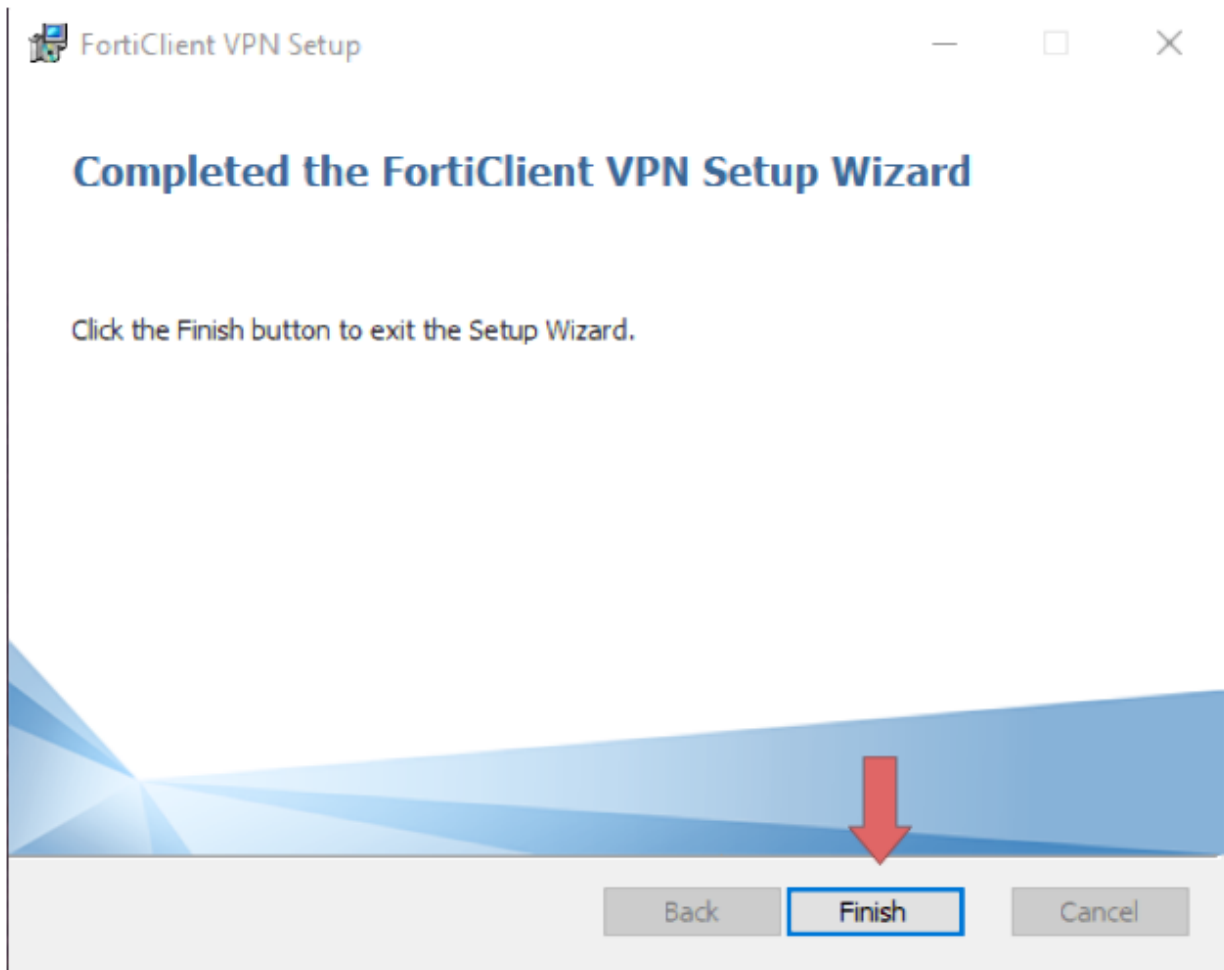
2. Run the downloaded installer and proceed through the setup wizard.



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



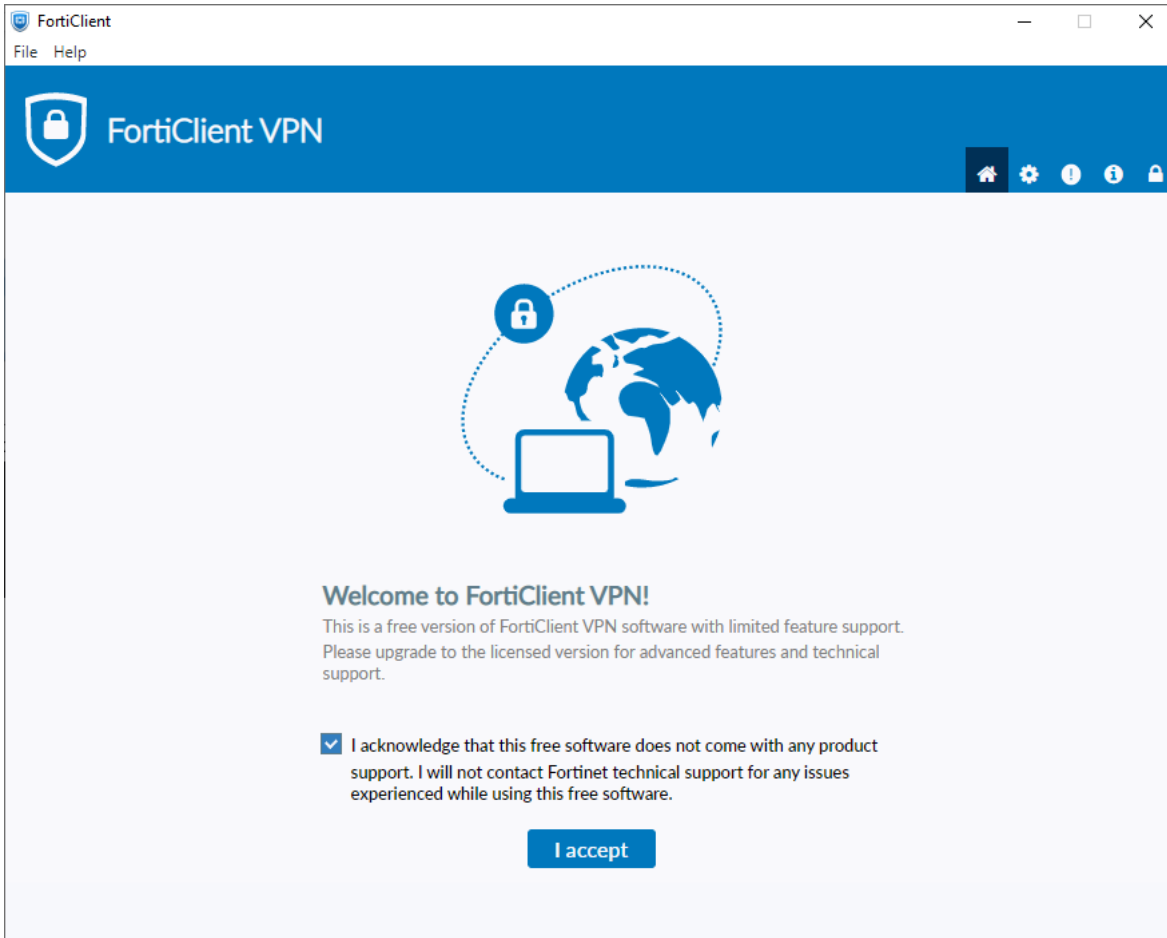
4. Once the Installation is finished click **Finish**.



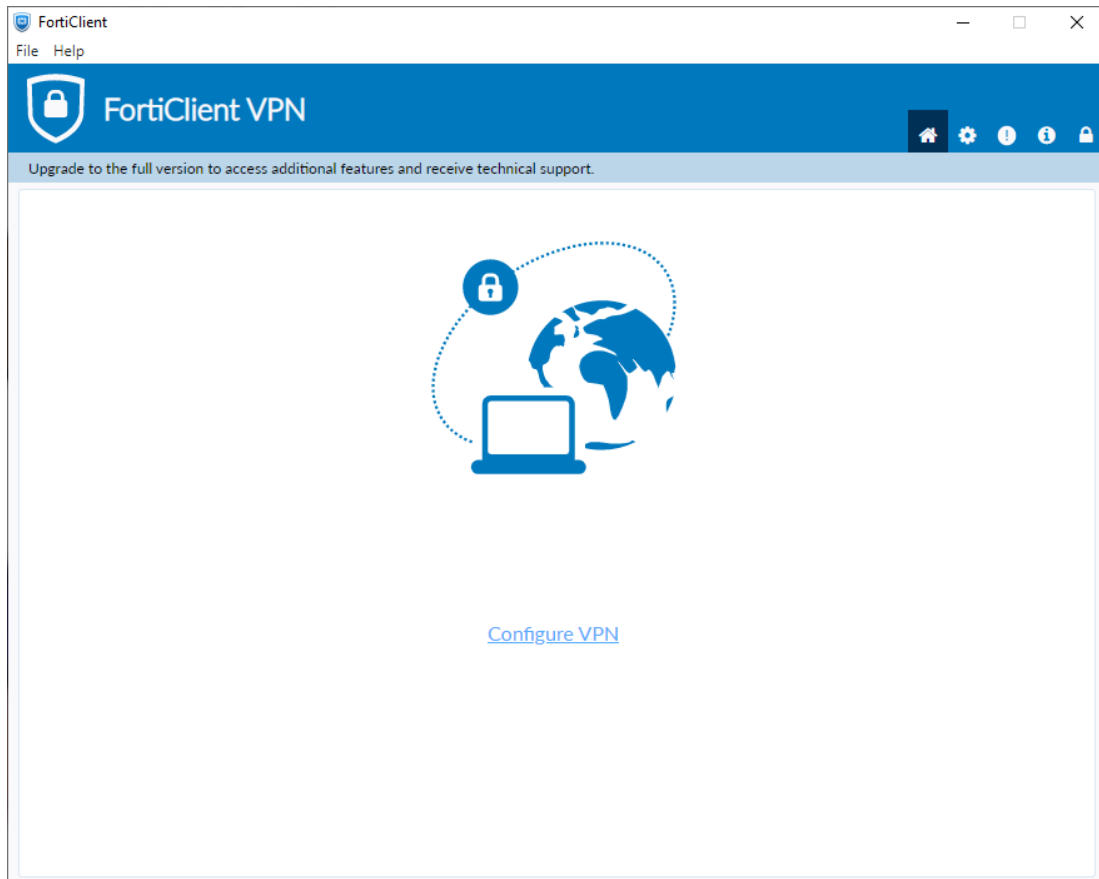
5. Locate and double-click the "**Forticlient VPN**" shortcut on your desktop.



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., ODU CS VPN)
 - c. Description: **Any**
 - d. Remote Gateway: **128.82.11.12**
 - e. Authentication Method **Pre-shared key**
 - i. Pre-shared key: **1HtXv1^^27**

Edit VPN Connection

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

Connection Name:

Description:

Remote Gateway: ✕
[+Add Remote Gateway](#)

Authentication Method: Pre-shared key ▼

Authentication (EAP): Prompt on login Save login Disable

Fallover SSL VPN: [None] ▼

[+ Advanced Settings](#)

9. Click the + next to **Advanced Settings**, configure as follows:
 - a. Click the + next to **VPN Settings**:

Edit VPN Connection

VPN: SSL-VPN IPsec VPN XML

Connection Name:


Description:

Remote Gateway: ✕
[+Add Remote Gateway](#)

Authentication Method: ▼

Authentication (EAP): Prompt on login Save login Disable

Fallback SSL VPN: ▼

 [+ Advanced Settings](#)

- i. IKE: **Version 2**
- ii. Options: **Mode Config**

VPN Settings

IKE: Version 1 Version 2

Options: Mode Config Manually Set DHCP over IPsec

- b. Click the + next to **Phase 1**:
 - i. Algorithms: **AES128, AES256**
 - ii. Authentication: **SHA256, SHA512**
 - iii. Diffie-Hellman Groups: **5, 14**

Phase 1

IKE Proposal	Encryption	<input type="text" value="AES128"/>	Authentication	<input type="text" value="SHA256"/>
	Encryption	<input type="text" value="AES256"/>	Authentication	<input type="text" value="SHA512"/>
DH Group	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input checked="" type="checkbox"/> 5	<input checked="" type="checkbox"/> 14
	<input type="checkbox"/> 16	<input type="checkbox"/> 17	<input type="checkbox"/> 18	<input type="checkbox"/> 15
Key Life	<input type="text" value="86400"/>	sec	<input type="checkbox"/> 19	<input type="checkbox"/> 20
Local ID	<input type="text" value="Optional"/>			
	<input checked="" type="checkbox"/>	Dead Peer Detection		
	<input checked="" type="checkbox"/>	NAT Traversal		
	<input type="checkbox"/>	Enable Local LAN		

- c. Click the + next to **Phase 2**:
- i. Algorithms: **AES128, AES256**
 - ii. Authentication: **SHA1, SHA1**
 - iii. Diffie-Hellman Group: **5**

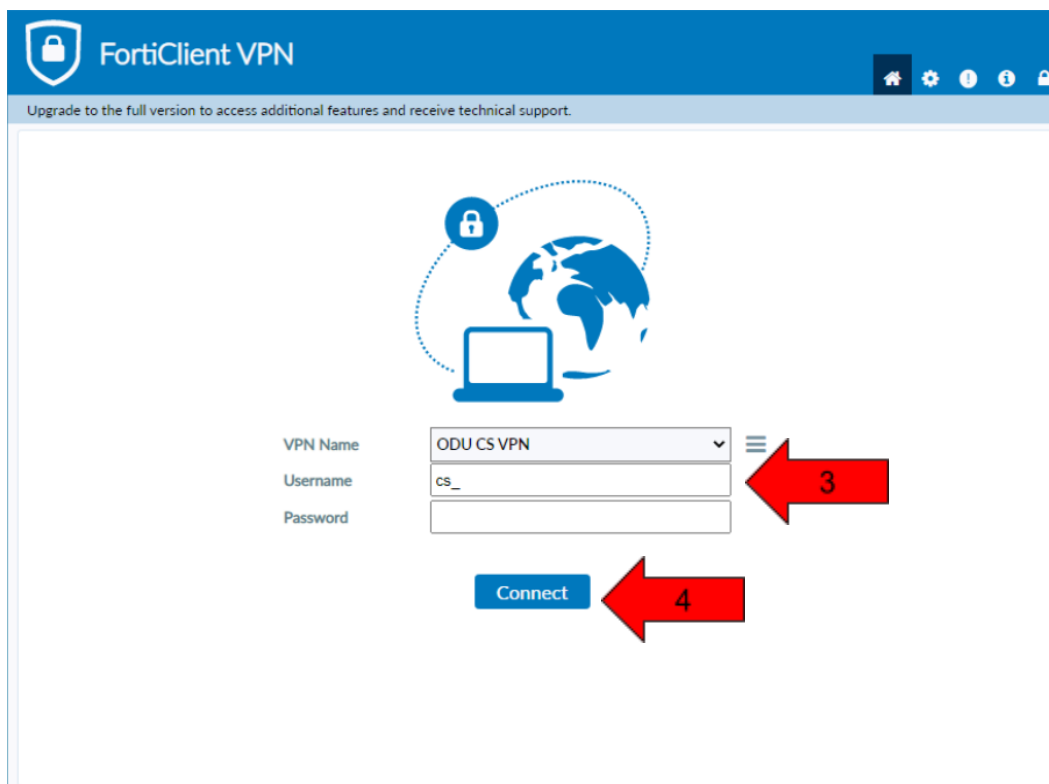
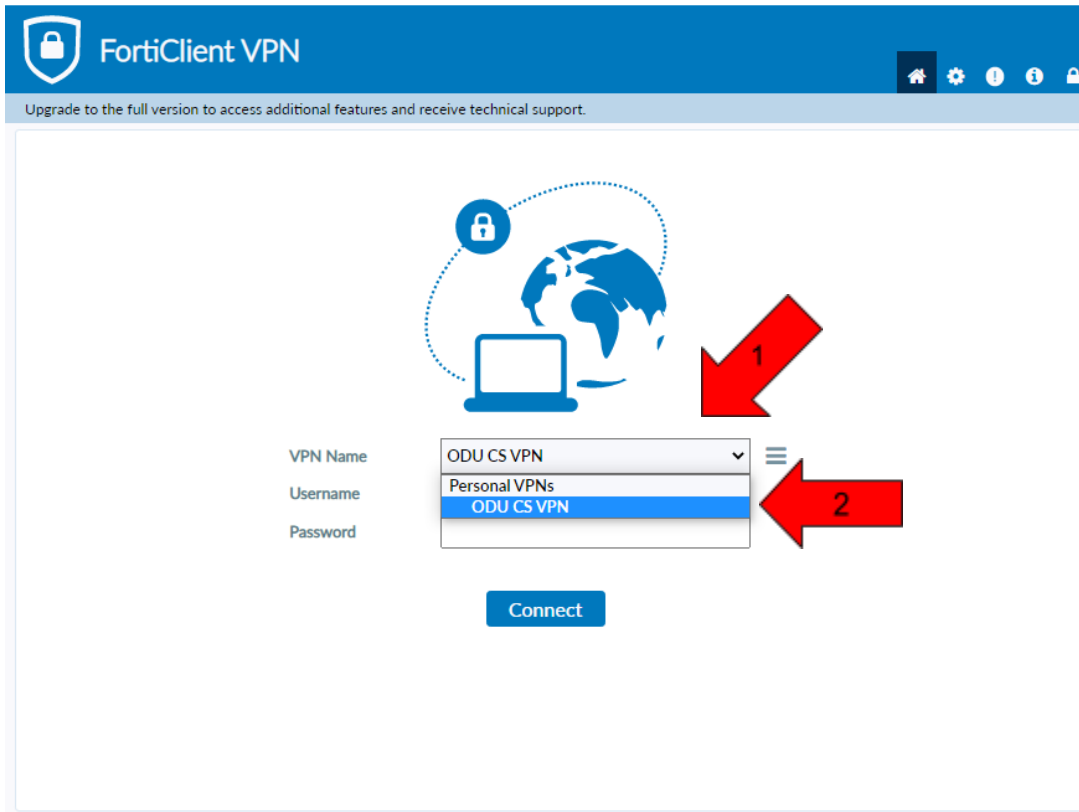
Phase 2

IKE Proposal	Encryption	<input type="text" value="AES128"/>	Authentication	<input type="text" value="SHA1"/>
	Encryption	<input type="text" value="AES256"/>	Authentication	<input type="text" value="SHA1"/>
Key Life	<input checked="" type="checkbox"/>	<input type="text" value="43200"/>	Seconds	
	<input type="checkbox"/>	<input type="text" value="5120"/>	KBytes	
	<input checked="" type="checkbox"/>	Enable Replay Detection		
	<input checked="" type="checkbox"/>	Enable Perfect Forward Secrecy (PFS)		
DH Group	<input type="text" value="5"/>			

10. Finally, click **Save**.



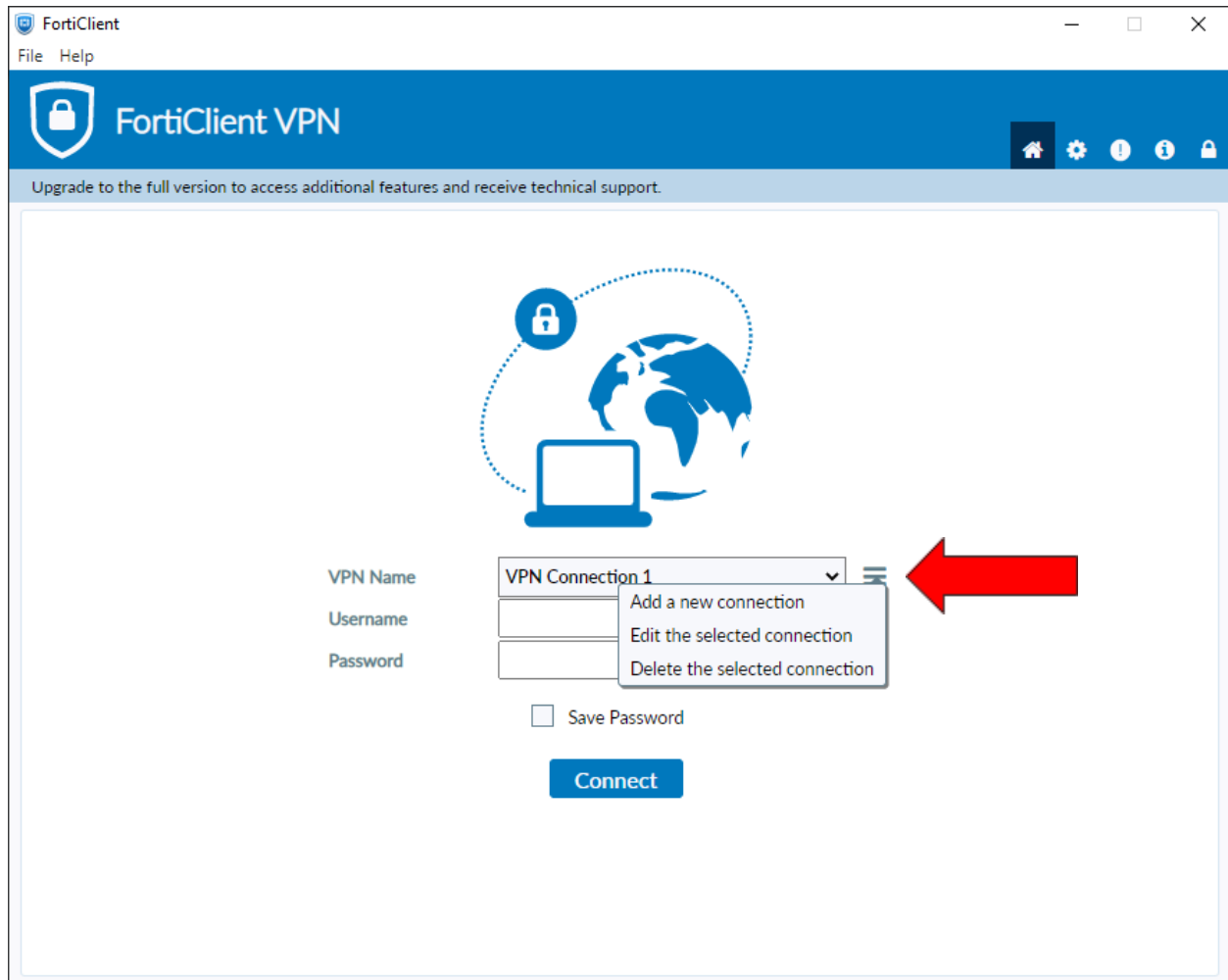
11. Select your created VPN Connection from the **drop down menu**. Enter your **ODU CS Credentials** and click **Connect**.



12. After clicking **connect**, you will receive a **DUO push** notification to your mobile device to confirm the Authentication process.

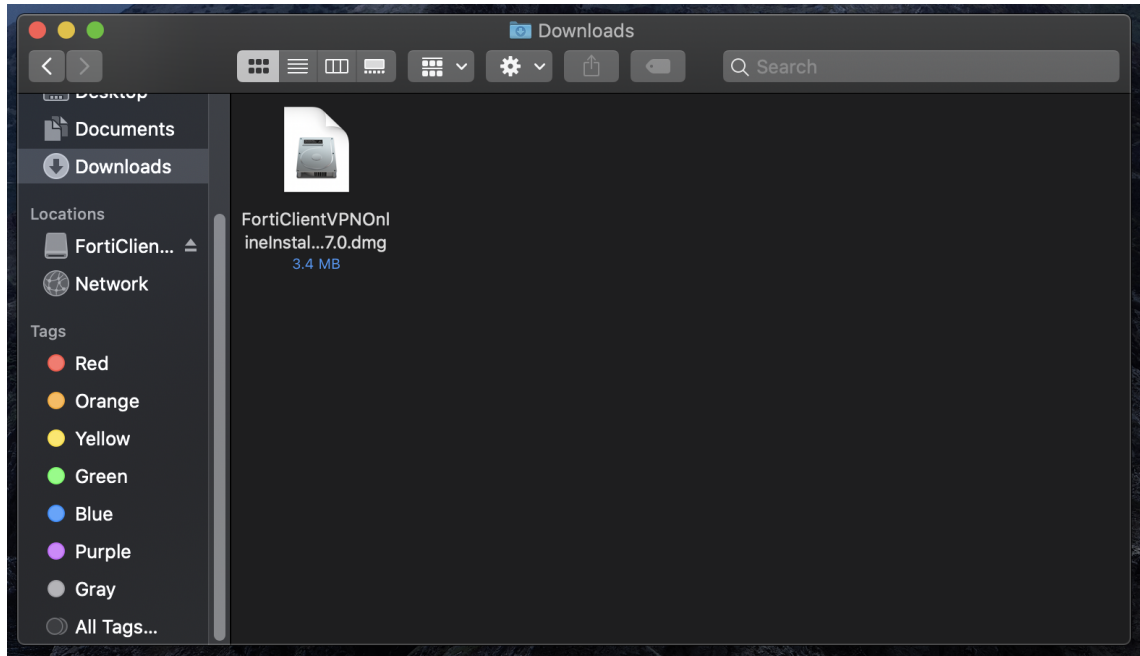
a. **Check the DUO mobile app if you do not receive a notification.**

b. To edit or add a connection click the **three lines** on the **right side of the VPN Name box**:

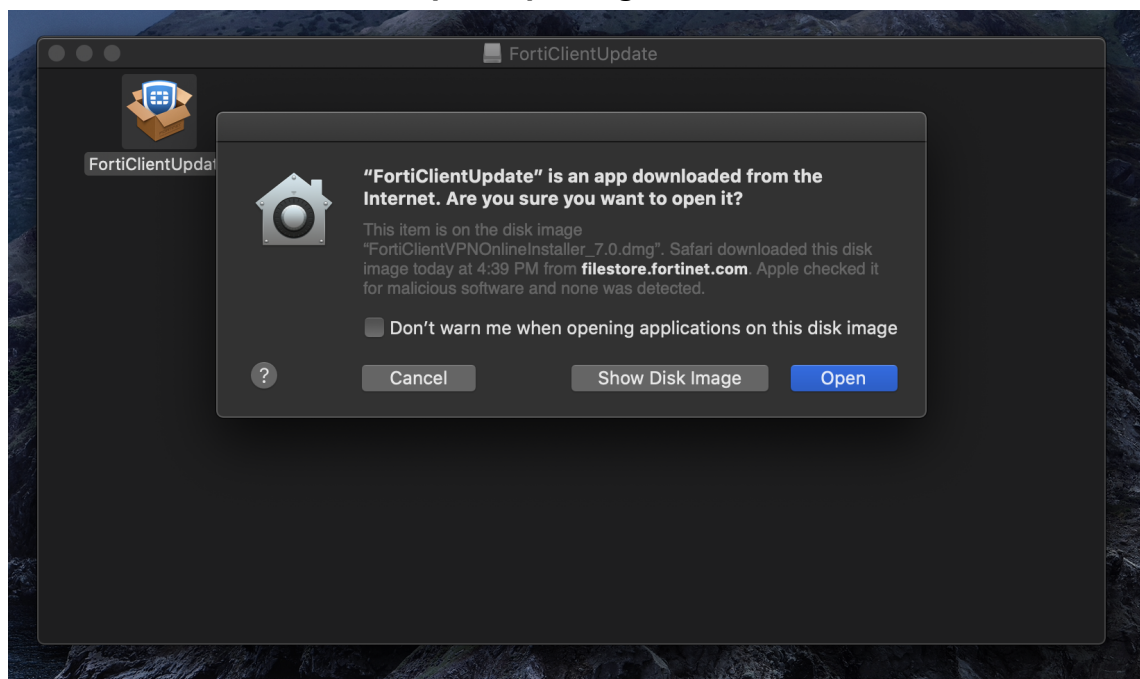


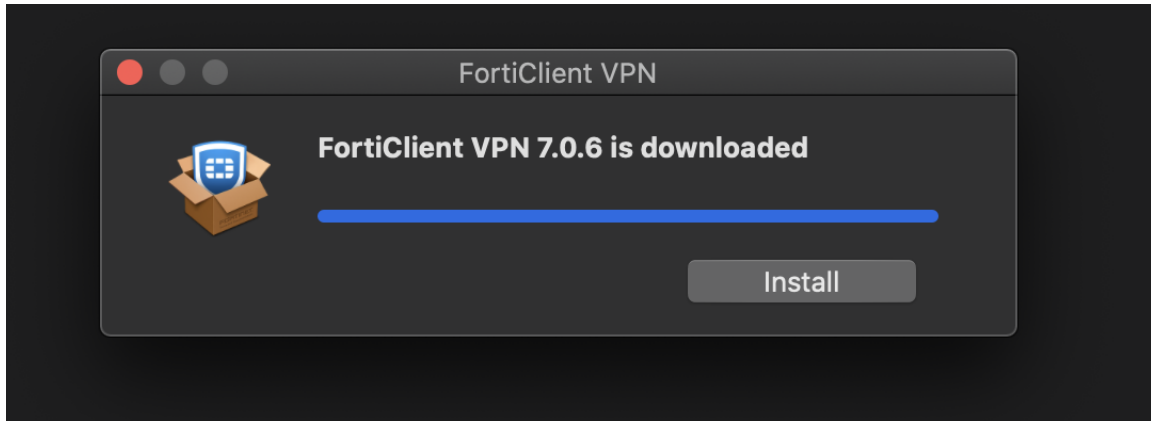
Using Mac:

1. Visit <https://links.fortinet.com/forticlient/mac/vpnagent> to download the Forticlient VPN (Mac).
 - a. **This is a direct installation link**, it will lead you to a blank page and prompt you to install.

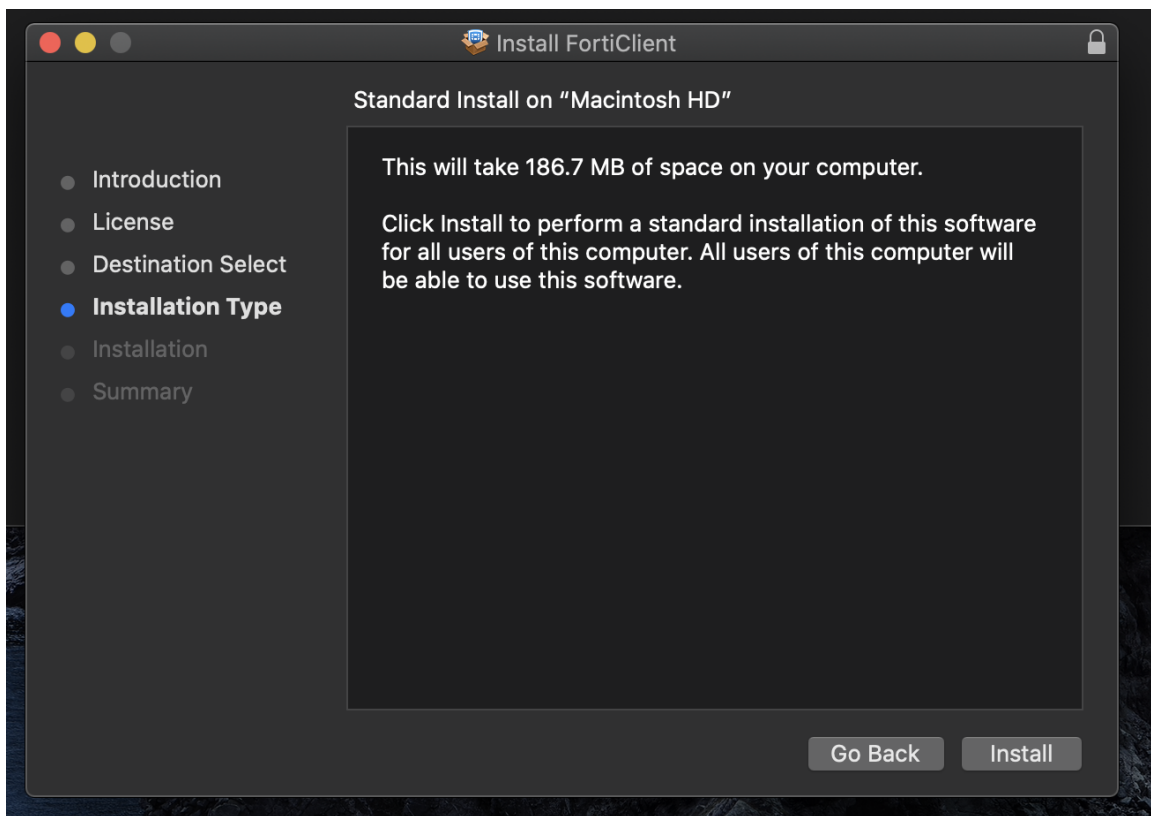


2. Open and run the downloaded **FortiClient.dmg** file which will proceed to download the **FortiClientUpdate** package.

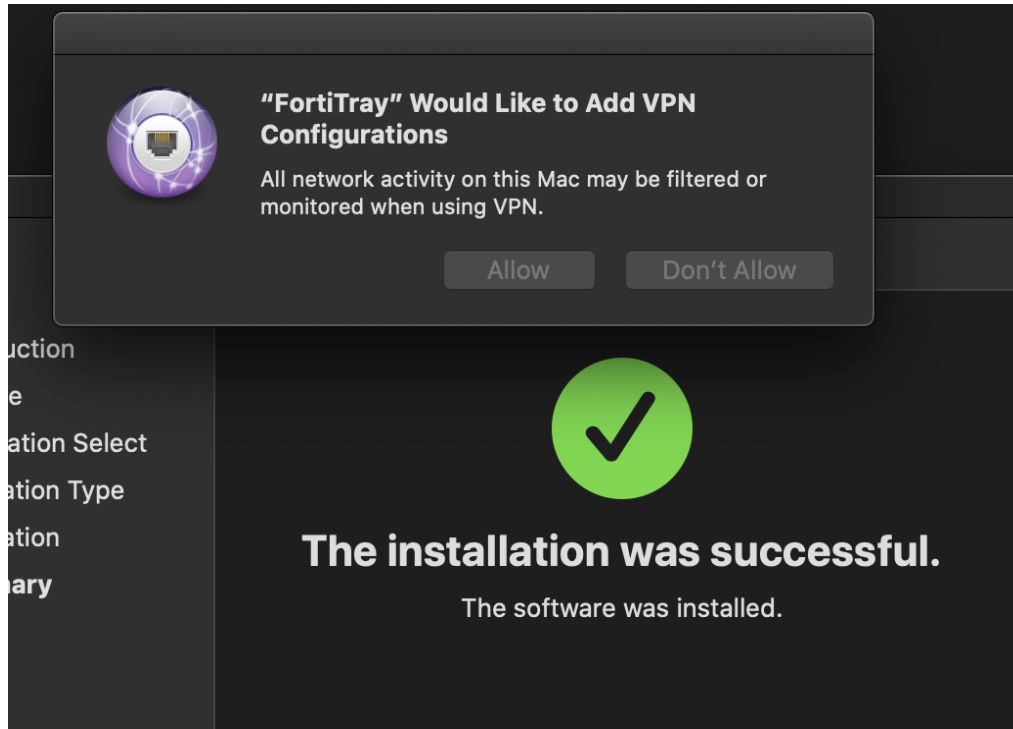




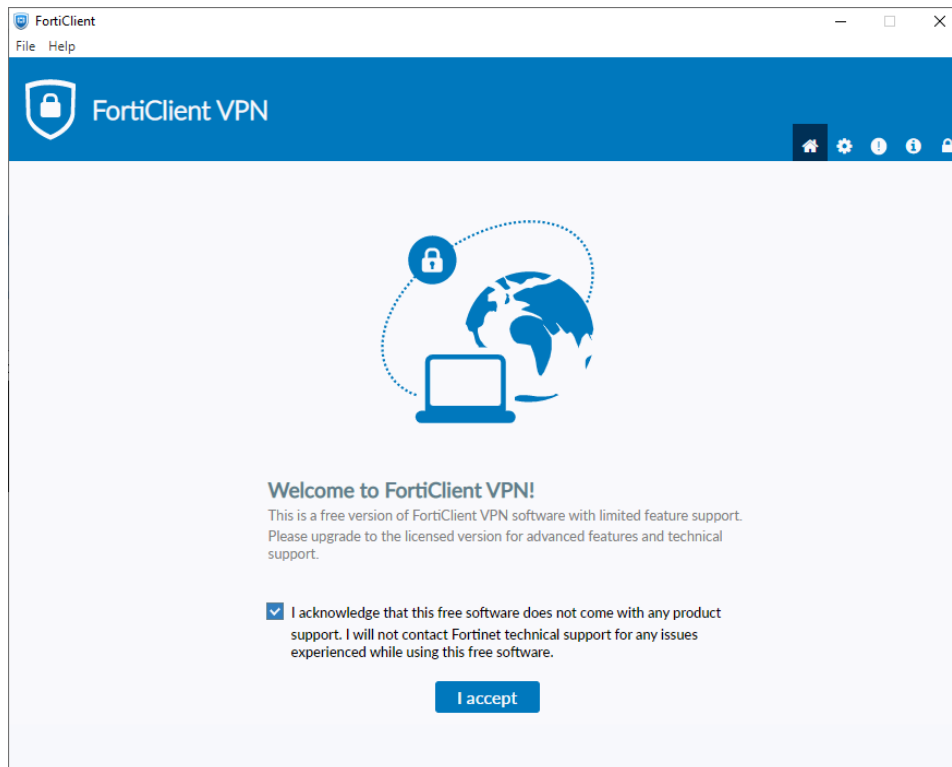
3. Run the **FortiClientUpdate** package and select **Open** to download and **install FortiClient VPN**.



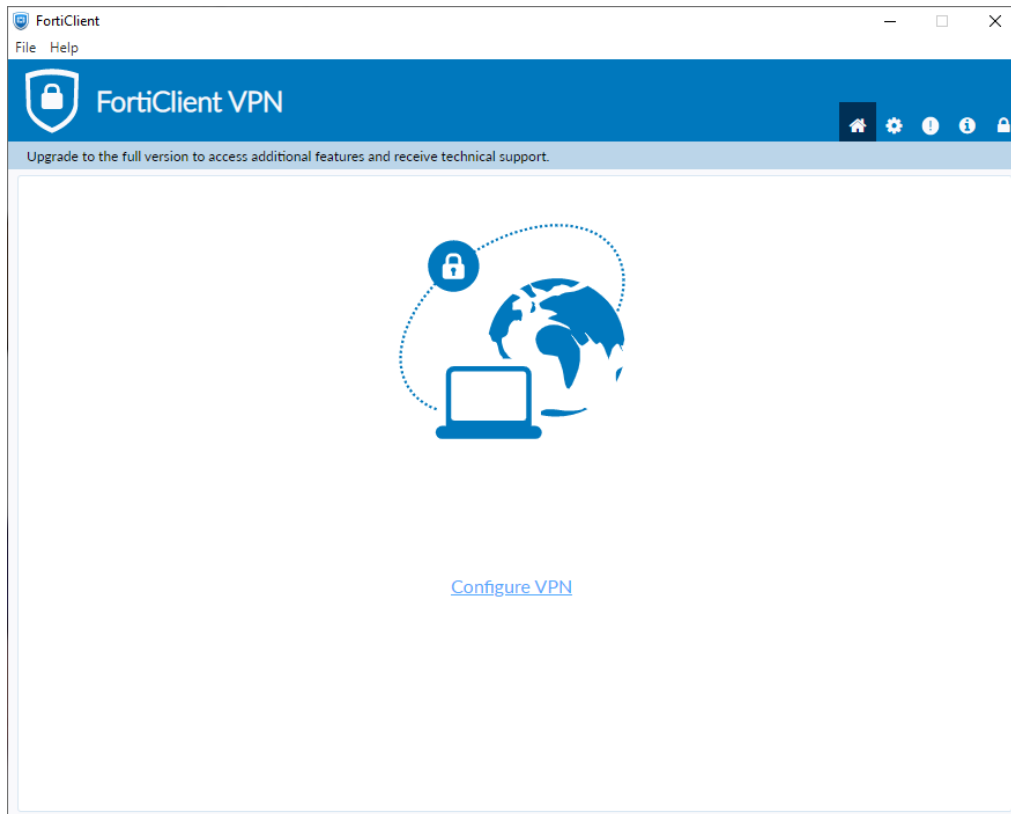
- After a successful installation, it will ask for permission to add FortiTray VPN Configurations to your device, click **Allow** to continue.



- After it has been installed, search Finder for the newly installed FortiClient. Then click the box next to the acknowledgment agreement and click "I accept".



6. Click **"Configure VPN"**



7. 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: **128.82.11.12**
 - e. Authentication Method: **Pre-shared key**
 - i. Pre-shared key: **1HtXv1^^27**

Edit VPN Connection

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

Connection Name:

Description:

Remote Gateway: ✕
[+Add Remote Gateway](#)

Authentication Method: Pre-shared key ▼

Authentication (EAP): Prompt on login Save login Disable

Fallover SSL VPN: [None] ▼

[+ Advanced Settings](#)

8. Click the + next to **Advanced Settings**, configure as follows

Edit VPN Connection

VPN: SSL-VPN IPsec VPN XML

Connection Name:

Description:

Remote Gateway: ✕
+ Add Remote Gateway

Authentication Method: ▼

Authentication (EAP): Prompt on login Save login Disable

Failover SSL VPN: ▼

 + Advanced Settings

- a. Click the + next to **VPN Settings**:
- KE: **Version 2**
 - Options: **Mode Config**

— VPN Settings

IKE: Version 1 Version 2

Options: Mode Config Manually Set DHCP over IPsec

- b. Click the + next to **Phase 1**:
- Algorithms: **AES128, AES256**
 - Authentication: **SHA256, SHA512**
 - Diffie-hellman Groups: **5, 14**

Phase 1

IKE Proposal

Encryption: AES128

Authentication: SHA256

Encryption: AES256

Authentication: SHA512

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

- c. Click the + next to **Phase 2**:
- i. Algorithms: **AES128, AES256**
 - ii. Authentication: **SHA1, SHA1**
 - iii. Diffie-hellman Group: **5**

Phase 2

IKE Proposal

Encryption: AES128

Authentication: SHA1

Encryption: AES256

Authentication: SHA1

Key Life: 43200 Seconds
 5120 KBytes

Enable Replay Detection

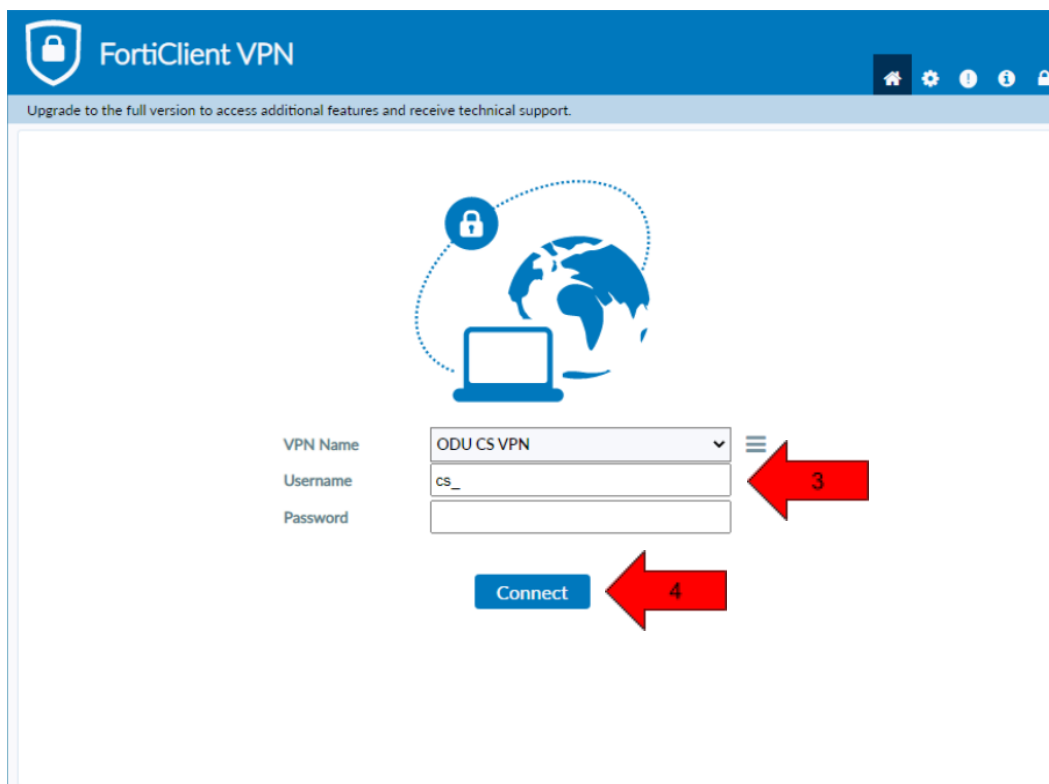
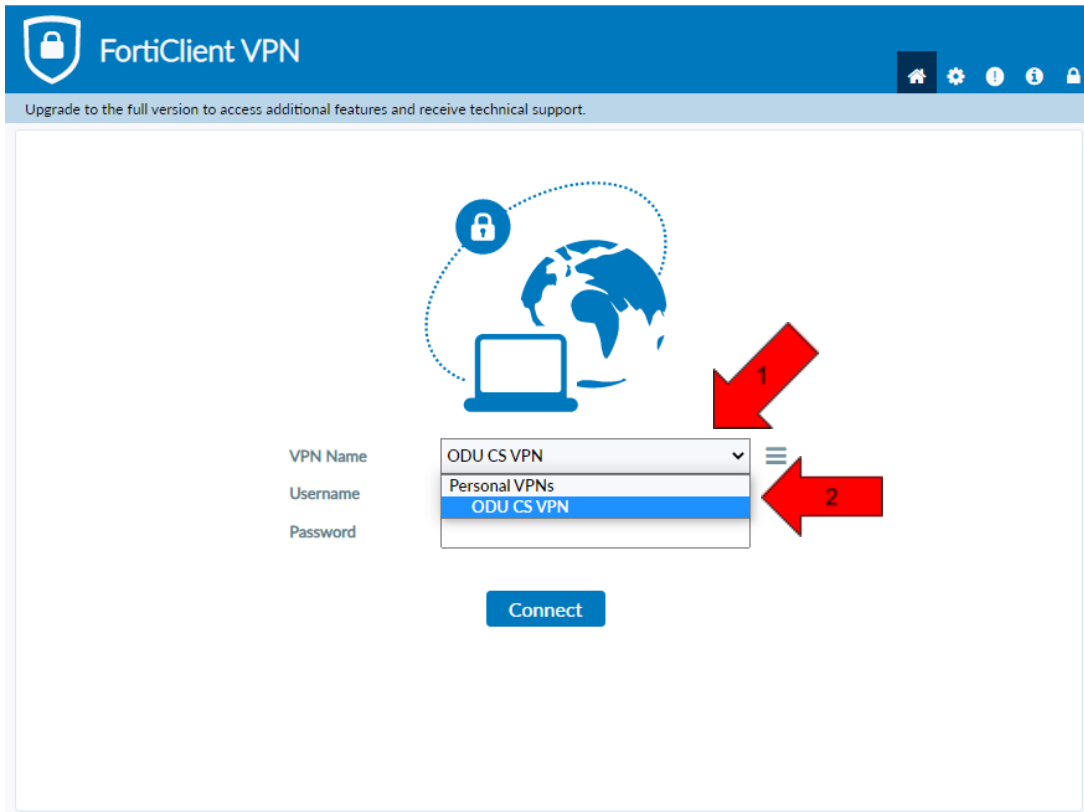
Enable Perfect Forward Secrecy (PFS)

DH Group: 5

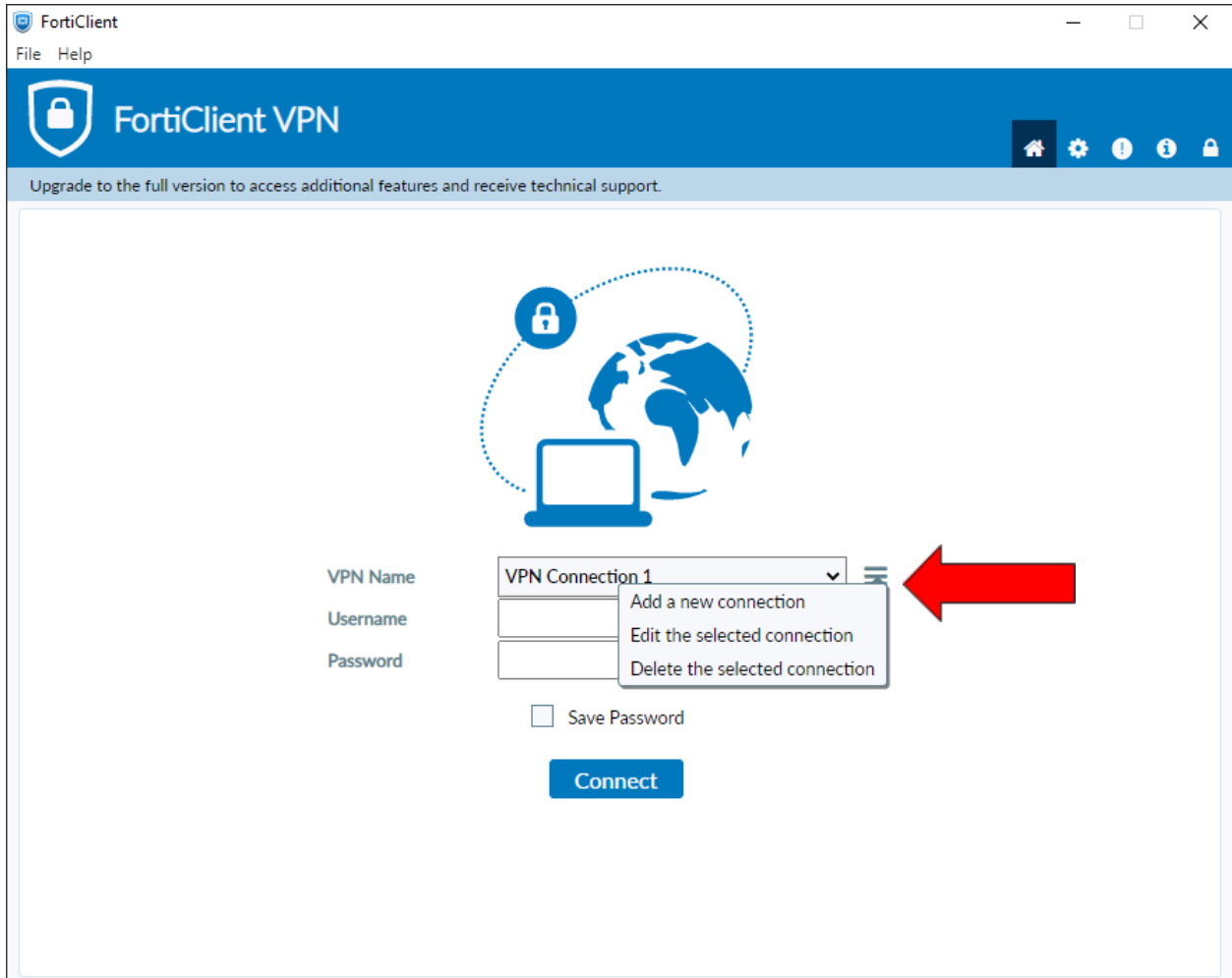
9. Finally, click **Save**.

Cancel Save 

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



11. After clicking **connect**, you will receive a **DUO push** notification to your mobile device to confirm the Authentication process
- a. **Check the Duo Mobile app if you do not receive a notification.**
 - b. To edit or add a connection click the **three lines** on the **right side of the VPN Name box**:



Using Linux:

1. Open the **terminal** to prepare for installation
 - a. Run this command to find out what Linux distribution you are using:
 - i. `cat /etc/os-release`
2. Install **Openconnect** using the correct command for your linux distribution:
 - a. Ubuntu / Debian
 - i. `sudo apt install openconnect`
 - b. Fedora
 - i. `sudo dnf install openconnect`
 - c. CentOS / RHEL
 - i. `sudo yum install openconnect`
 - d. Arch Linux
 - i. `sudo pacman -S openconnect`
3. Type in the **sudo** password, press **enter**, then press **y** to begin the installation
4. After installation run this **command**:
 - a. `sudo openconnect --protocol=gp gp.cs.odu.edu -u [cs_username]`

```
user@example.com:/$ sudo openconnect --protocol=gp gp.cs.odu.edu -u [cs_username]
```

5. Type in **sudo** password if prompted
6. Type in **cs account** password
7. You will receive a **DUO push notification** to your mobile device to confirm the Authentication process
 - a. **Check the Duo Mobile app if you do not receive a notification**

FAQ/Trouble-shooting:

- Issues connecting to the Forticlient VPN
 - Check that the correct version of Forticlient is installed
 - The version installed should be “**Forticlient VPN**” as listed on the **bottom of the download page**.
 - **DO NOT install Forticlient 7.0, ZTNA Edition, EPPI/APT Edition or Forticlient Endpoint Management Server (EMS)**
 - A **direct install link** is included in the [Windows](#) and [Mac](#) section of this document.
 - Check that you are connected to the internet
 - **You need a internet connection to use Forticlient VPN**
 - Check that you used the correct VPN settings
 - Instructions for **VPN setup** are available in the [Windows](#) and [Mac](#) section of this document
 - Common misconfigurations are the Pre-shared key, and advanced settings.
 - Check that you entered the right username and password
 - **You must enter your CS account username and password, DO NOT use your MIDAS credentials**
 - Make a **CS account** here at: <https://accounts.cs.odu.edu>
 - You can also use this link to reset your CS Account **password**.
 - If you see “Permission denied, please try again” **After** changing your **CS account password**, please contact root@cs.odu.edu
 - To reset a **faculty password**, see instructions in this link https://systems.cs.odu.edu/Account_Password
 - Connection problem not solved after following the previous troubleshooting step
 - On Windows 11: **Update network drivers**
 - You can find information on updating the driver here: <https://www.thewindowsclub.com/how-to-update-network-drivers-windows-11>.
 - Authentication **without** using DUO
 - It is **highly recommended** that you install the DUO app for authentication. The app can **downloaded for free** from your device’s **application store**

- For information about setting up Two-factor visit:
<https://ww1.odu.edu/ts/access/two-factor-authentication/get-started>
 - To login using **SMS authentication** on **Forticlient VPN** add “,sms” (without quotations) to the **end of your password**.
 - Example: cspassword,sms
 - You will see “wrong credentials” above the login boxes and you will receive a **list of codes** to your **phone**.
 - Type in the your password **again**, this time using one of the **codes** you received at the **end of your password**.
 - Example: cspassword,123456
- Issues with SSh and Linux project submission
 - Some CS classes have **VPN setup and SSH setup as an assignment**, please attempt to complete this task on your own if it is required for your course.
 - Contact your **instructor** or **TA** for assistance **before** reaching out to root@cs.odu.edu for assistance.
 - **We are unable to help with any homework questions or assignments.**