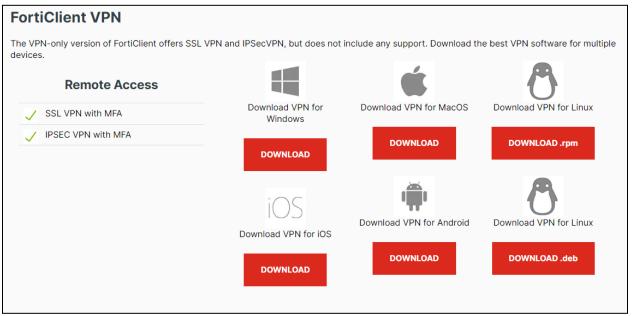
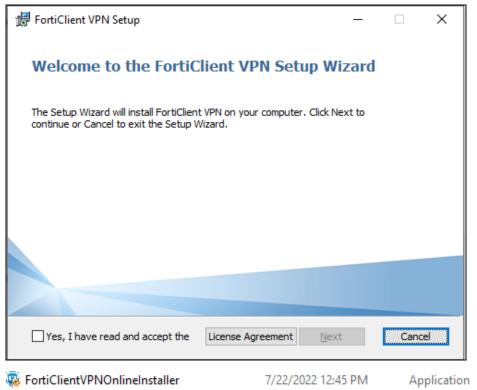
Using Windows:

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



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

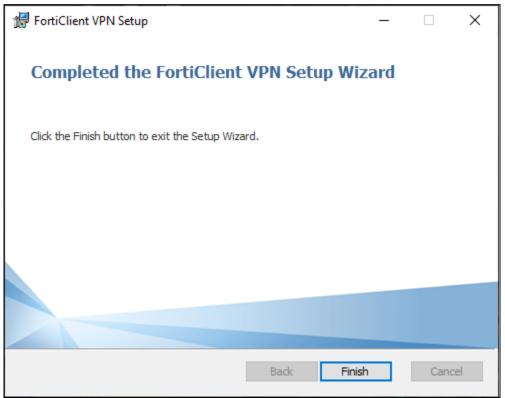


3,142 KB

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

🕼 FortiClient VPN Setup	—		×
Destination Folder Click Next to install to the default folder or dick Change to choos	e another.	1	
Install FortiClient VPN to:			
C:\Program Files\Fortinet\FortiClient\			
Change			
Back	Next	Cance	el 🛛
🔀 FortiClient VPN Setup	_		×
Ready to install FortiClient VPN			×
	 nge any of y		×
Ready to install FortiClient VPN Click Install to begin the installation. Click Back to review or chan			×
Ready to install FortiClient VPN Click Install to begin the installation. Click Back to review or chan			×
Ready to install FortiClient VPN Click Install to begin the installation. Click Back to review or chan			×

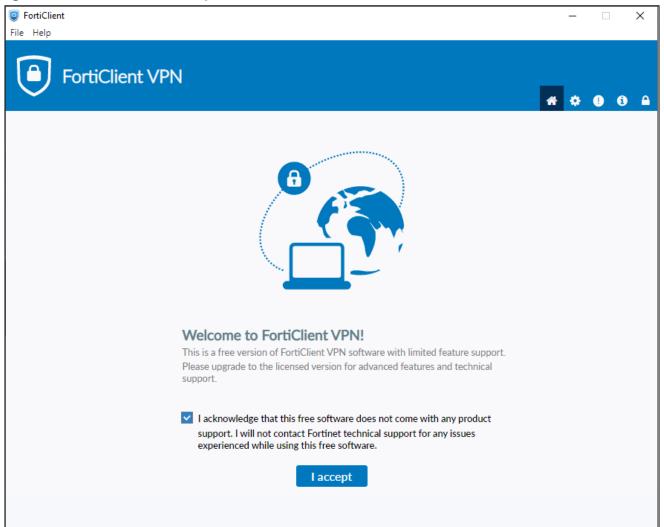
4. Once the **Installation** is finished click **Finish**.



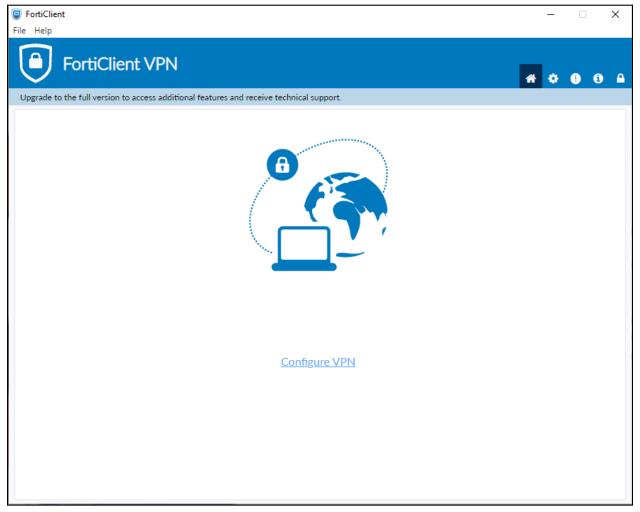
5. Locate and **Double-Click** the "Forticlient VPN" shortcut on your desktop



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 (DnS6fS7Zm^&*)

VPN	SSL-VPN	IPsec VPN	XML	
Connection Name	VPN Connection 1			
Description	Connection to ODU	VPN		
Remote Gateway	128.82.11.11			×
	+Add Remote Gatewa	У		
Authentication Method	Pre-shared key		~	
	•••••			
Authentication (XAuth)	Prompt on login (🔵 Save login 🔵 Di	isable	
Failover SSL VPN	[None]		~	
+ Advanced Settin				
- Advanced Setem	8-			
_				
	Cancel	Save		

- 9. 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	O Main 🔿 Aggressive
Options	O Mode Config ○ Manually Set ○ DHCP over IPsec

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

- Phase 1	
IKE Proposal	Encryption AES128 V Authentication SHA1 V
	Encryption AES256 V Authentication SHA256 V
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

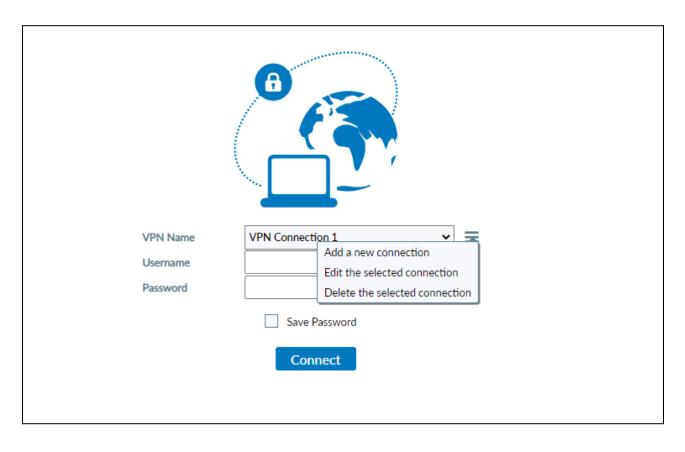
i. Click the box next to Dead Peer Detection.

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

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

VPN Name	VPN Connection 1	/ ≡
Username	Personal VPNs	
Password	VPN Connection 1	
	Save Password	

VPN Name	VPN Connection 1	≡
Username	cs_	
Password		
	Save Password	



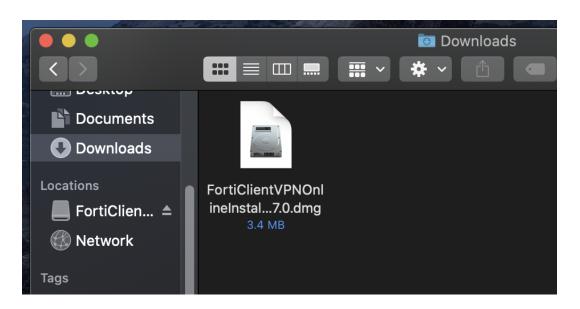
Note: To edit or add a connection click the **3 lines (Hamburger)** next to the **VPN name**:

Using Mac:

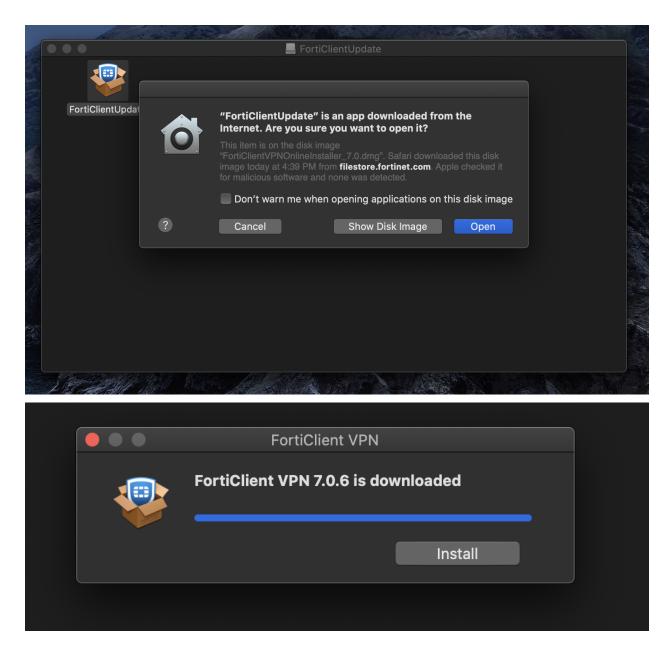
1. Visit <u>https://www.fortinet.com/support/product-downloads</u> and locate the **Forticlient VPN** located towards the bottom of the page and select the (**Download for MacOS**) option.

FortiClient VPN			
The VPN-only version of FortiClient offers SSL V devices.	PN and IPSecVPN, but does not	include any support. Download th	e best VPN software for multiple
Remote Access		Ś	ð
SSL VPN with MFA	Download VPN for Windows	Download VPN for MacOS	Download VPN for Linux
✓ IPSEC VPN with MFA	DOWNLOAD	DOWNLOAD	DOWNLOAD .rpm
	Download VPN for iOS	Download VPN for Android	Download VPN for Linux
	DOWNLOAD	DOWNLOAD	DOWNLOAD .deb

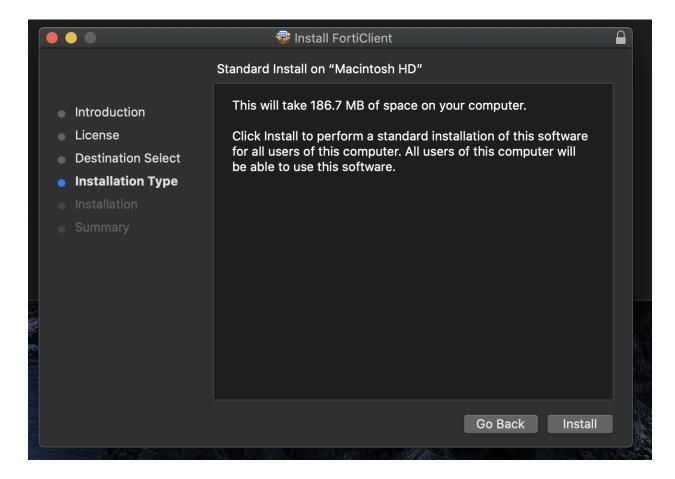
2. Open and **run** the downloaded **FortiClient.dmg** file which will proceed to download the **FortiClientUpdate** package.



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



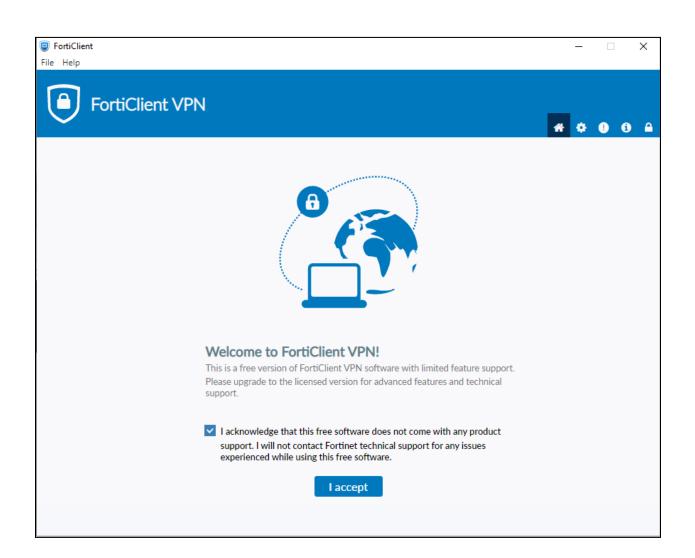
4. **Proceed** with the installation wizard, choosing install destination and accepting license agreements. Finally, click **install**.



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. Allow Don't Allow	
uction		
е		
ation Select		
ation Type		
ation	The installation was successful.	
ary	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**".



7. Click Configure VPN.

FortiClient VPN	*	•	i
Upgrade to the full version to access additional features and receive technical support.			
<u>Configure VPN</u>			

- 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^&*)

emote Gateway 128.82.11.11 Add Remote Gateway	 ×
Remote Gateway 128.82.11.11 +Add Remote Gateway Authentication Method	×
Authentication Method Pre-shared key	×
Authentication Method Pre-shared key	
	~
Authentication (XAuth) O Prompt on login O Save login O 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	O Main 🔘 Aggressive
Options	Mode Config Manually Set DHCP over IPsec

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

- Phase 1	
IKE Proposal	Encryption AES128 V Authentication SHA1 V
	Encryption AES256 V Authentication SHA256 V
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

i. Click the box next to Dead Peer Detection.

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

Cancel	Save
--------	------

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

VPN Name	VPN Connection 1	/ ≡
Username	Personal VPNs	
Password	VPN Connection 1	
	Save Password	

VPN Name	VPN Connection 1	≡		
Username	cs_			
Password				
	Save Password			