FortiClient 7.2.3 Installation – macOS Ventura and higher

Installation Instructions

- Go to www.concordia.ca
- Login to your My CU Account
- Go to Apps & software – VPN client (FortiClient) to
- download the installer file.
- Double click on the downloaded dmg file to mount the installer

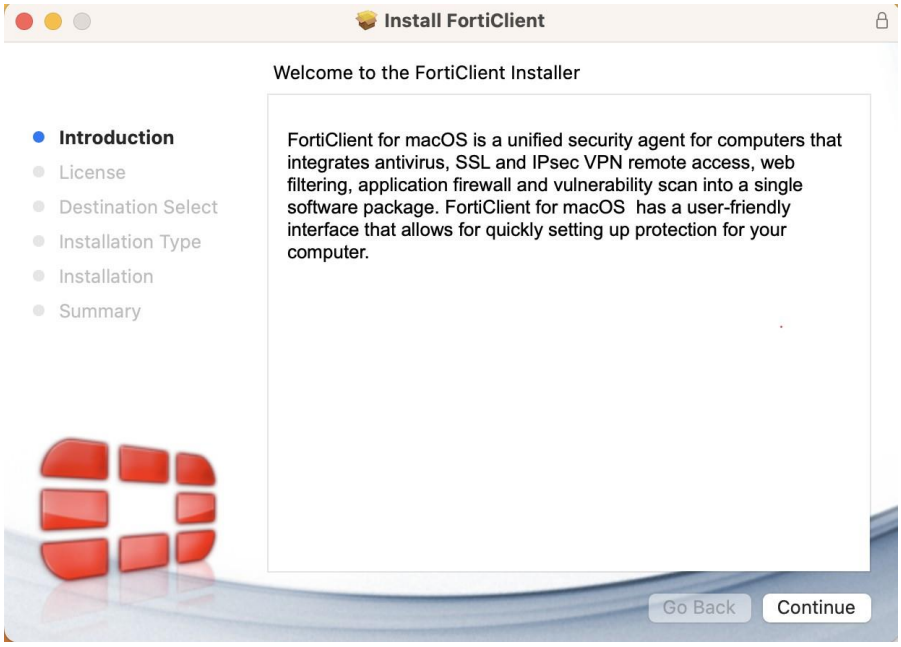
FortiClient .dmg file

- Double click on the FortiClient icon.

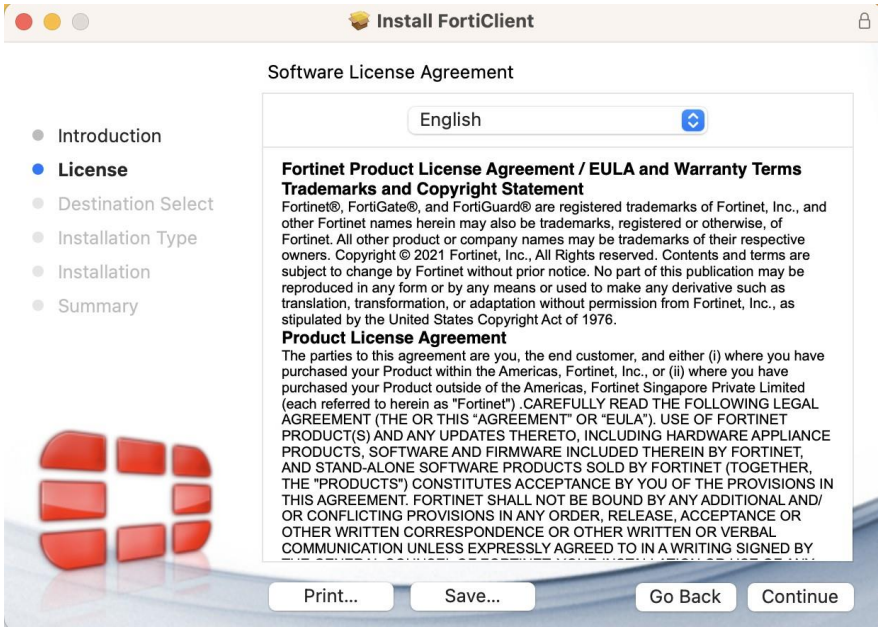
Forticlient icon

- Double click on installer.mpkg

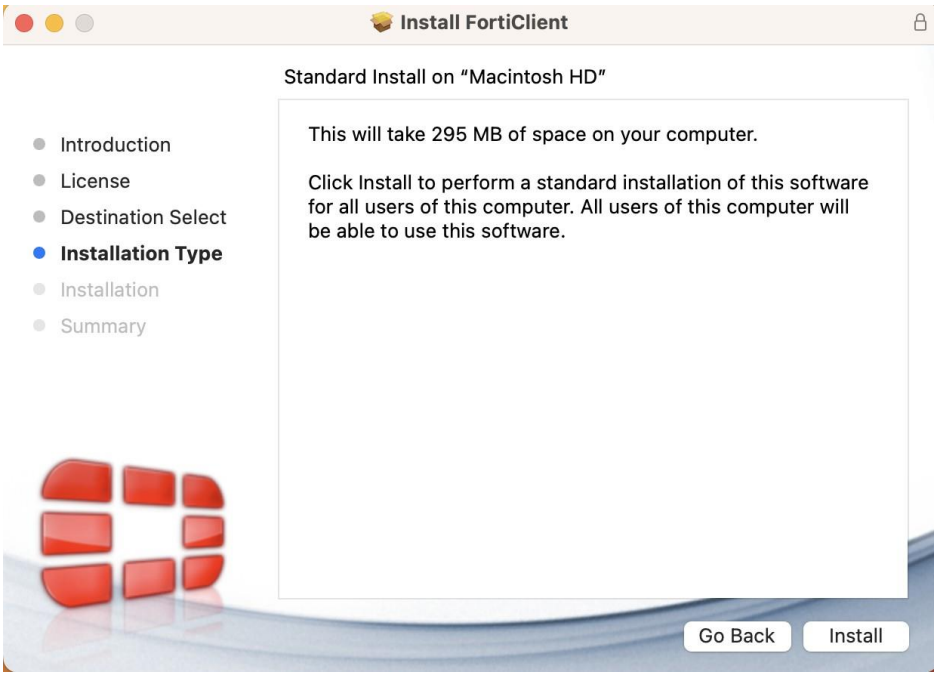
- Click continue



- Read the Software License Agreement and click continue and then “Agree”



- Click on install to begin the installation

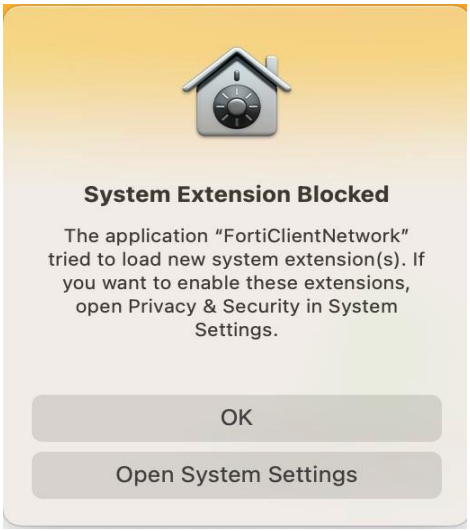


- macOS will prompt you for your password, enter it and click ‘Install Software’

- During the installation, you will be prompted to provide your password again so that FortiClientAgent can make changes to the System Trust Certificate settings. Immediately afterwards, macos security will also prompt for your password

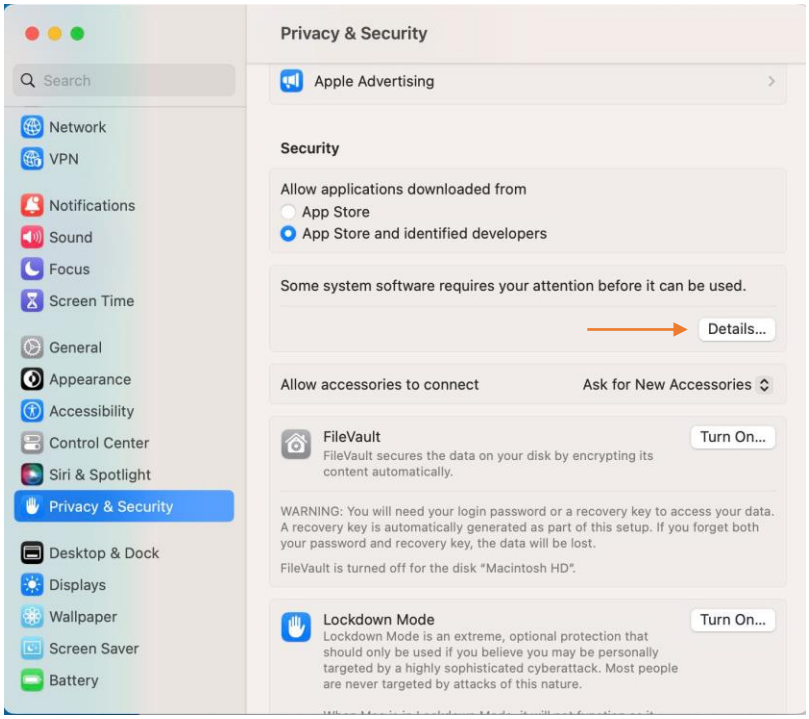
- Click “Allow” for FortiTray

- MacOS Ventura, click on open system settings to Allow “FortiClientNetwork”.
- For older macOS versions please use “security preferences”.

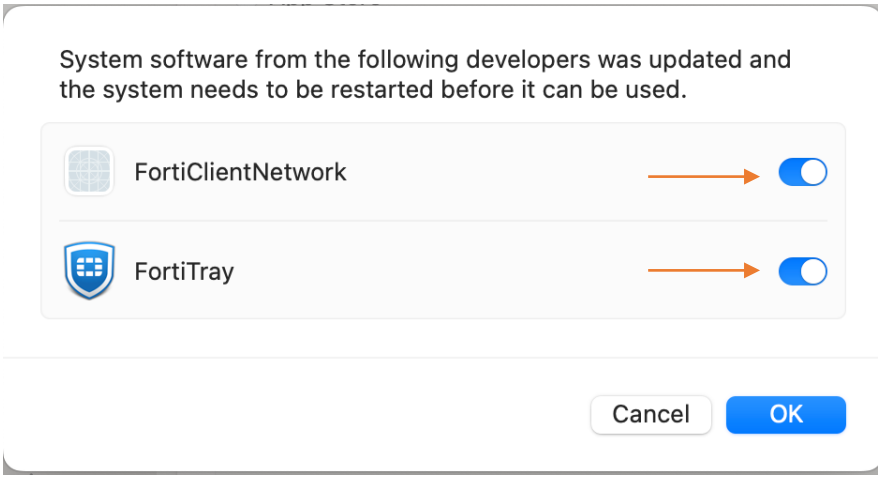


- Open system settings to Allow “FortiTray”.

- Click on Details to allow the extensions.
- Enter your password and click on Modify Settings.

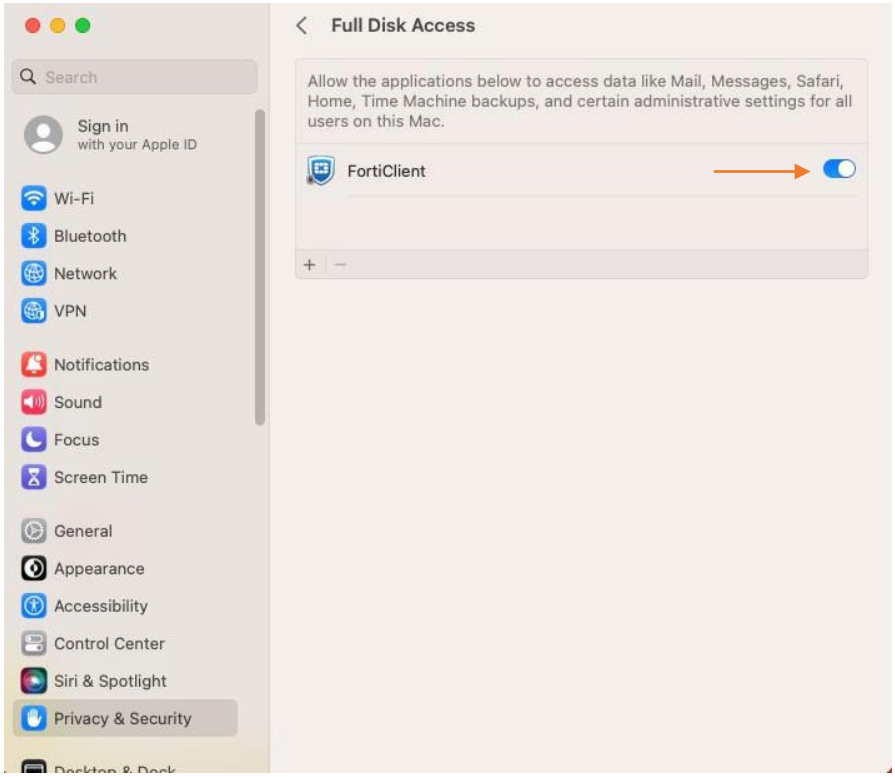


- Enable extensions

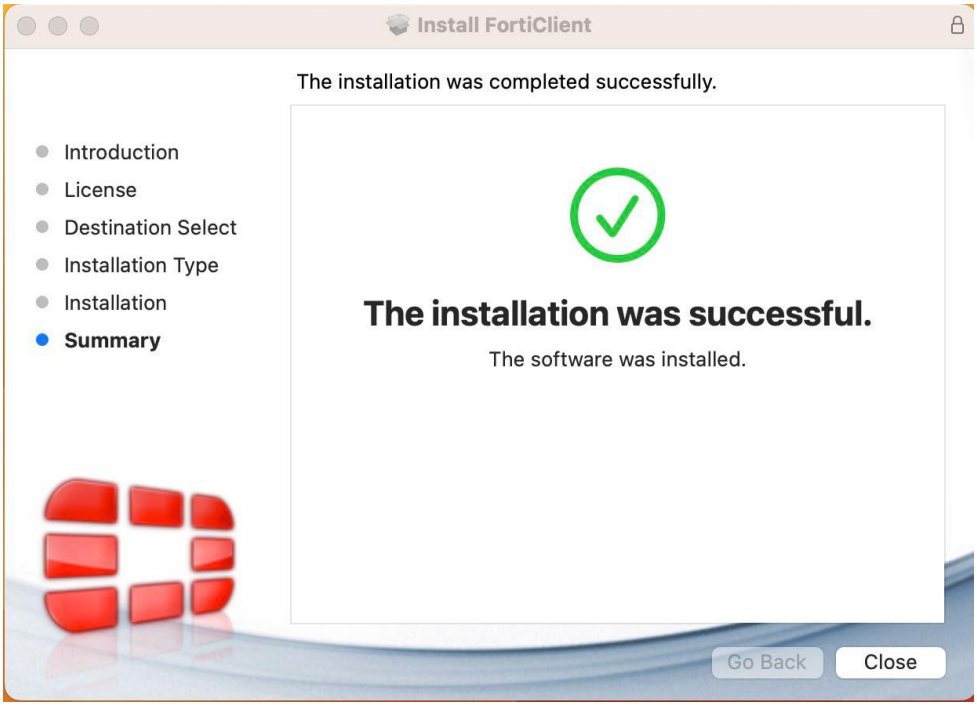


- Click OK and then enter your password and click on Modify Settings

- Enable Full Disk Access.

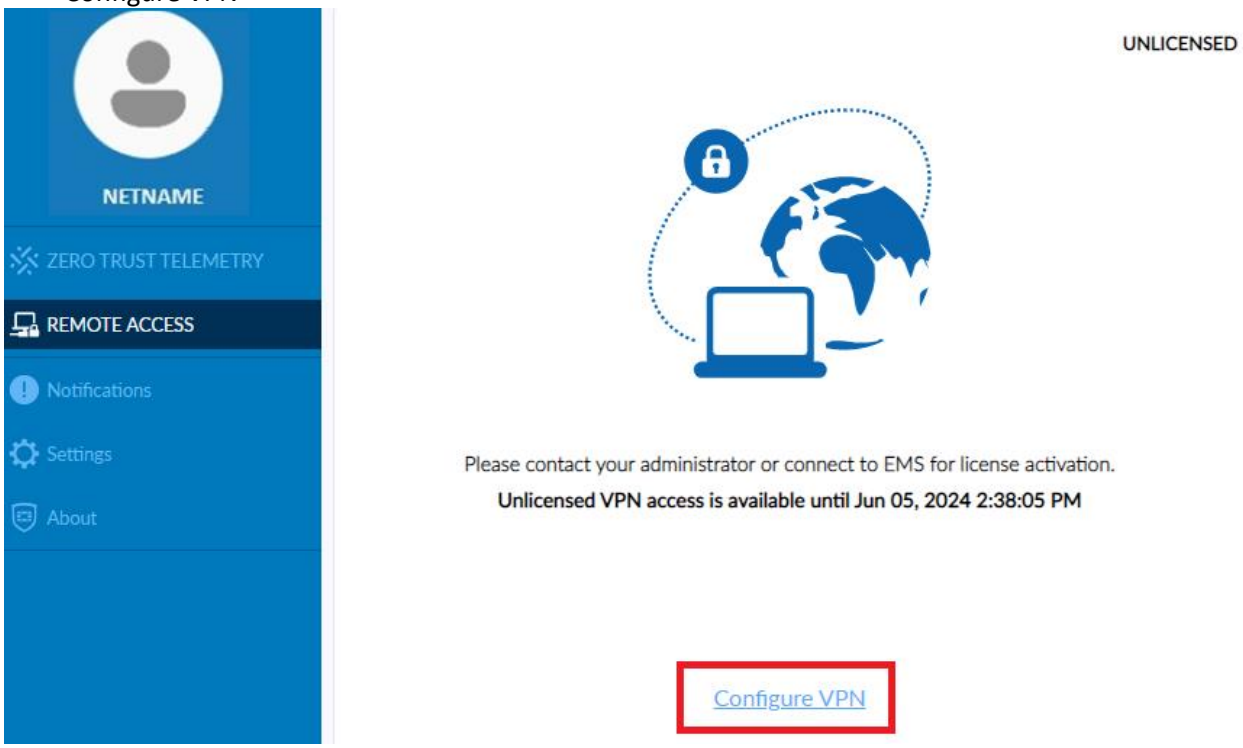


- Click close to complete the software installation

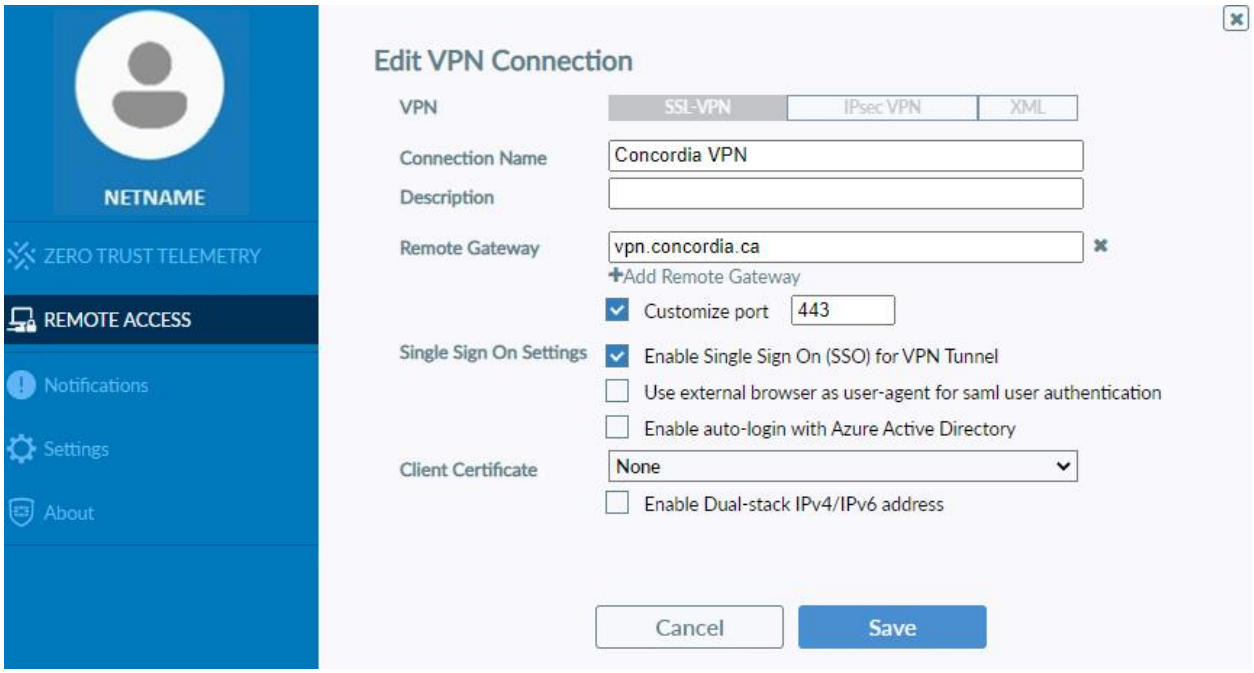


Configuring the VPN Connection and Licensing the Software

1. Click on “Remote Access” on the left side of the FortiClient window. In here, select “Configure VPN”



2. Configure the settings on this screen as below:
   - Connection Name: Concordia VPN
   - Remote Gateway: vpn.concordia.ca
   - ✅ Customize port: 443
   - ✅ Enable Single Sign On (SSO) for VPN Tunnel

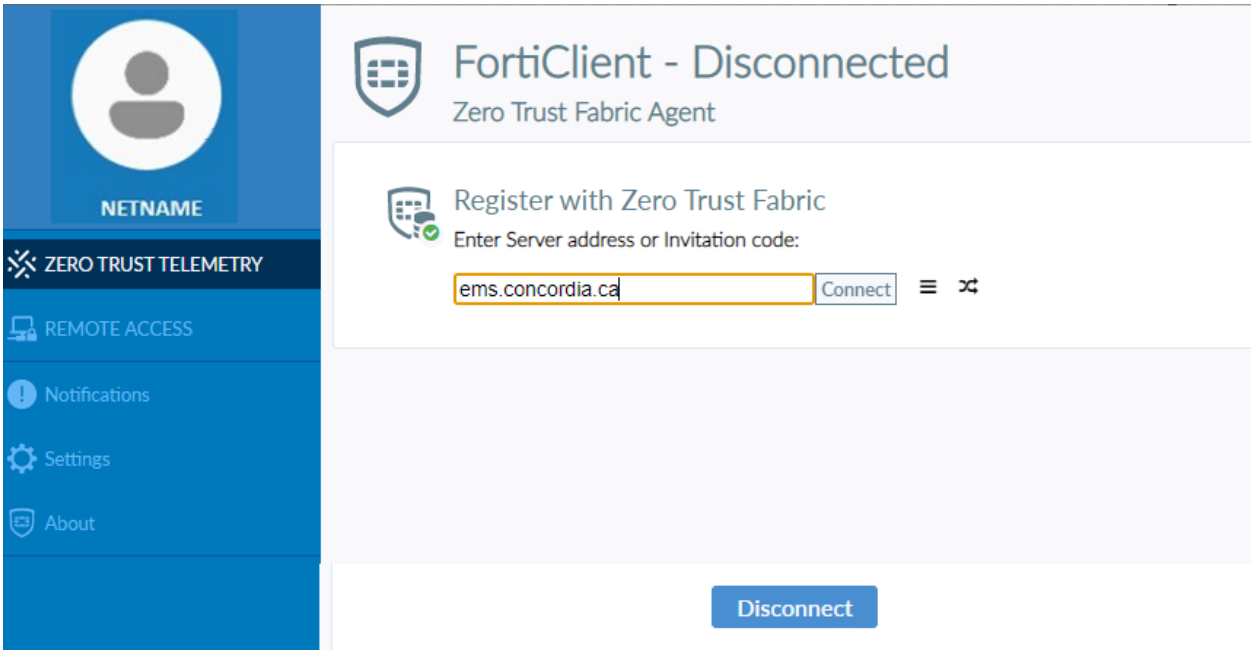


Afterwards, click Save.

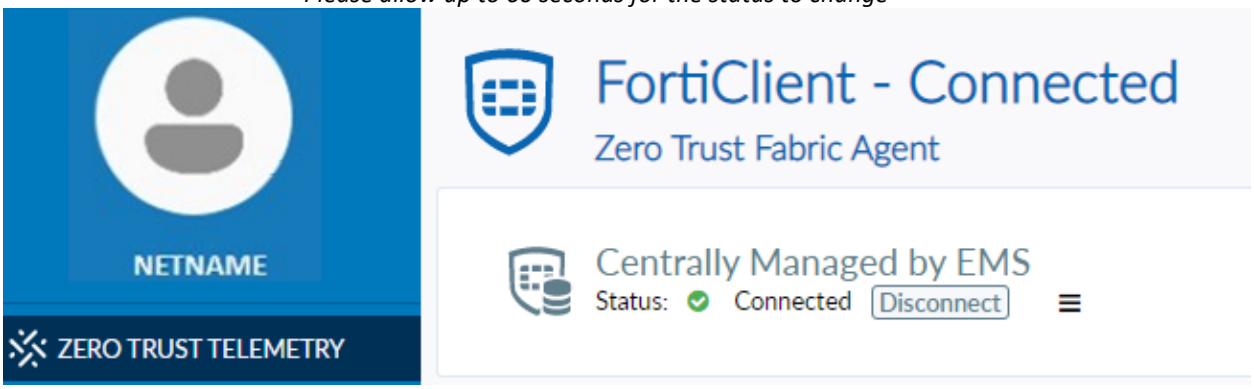
3. Once the connection has been created, click on “Connect” and provide your credentials to establish a connection to the VPN

4. Once successfully connected, click on the “Zero Trust Telemetry” tab and type in the EMS server address then click connect.

- Server Address: **ems.concordia.c**a



5. Once you have connected, you will see “Centrally Managed by EMS”.
   - **Please allow up to 60 seconds for the status to change*



Once you have completed the above steps, you will not need to follow them again unless you are installing the VPN on another device.

Should you click “Disconnect” on the Zero Trust Telemetry tab, you will have to manually type in the EMS server address to properly connect again. Please be aware that connection to the EMS server is only possible while on the campus network or when currently connected to the VPN in the “Remote Access” tab.