Configuring FortiClient VPN for Windows and MacOS users

This is the setup page if you are installing and setting up FortiClient VPN for Windows and MacOS. If you have not already downloaded the installer for your OS, they are available here:

Offline installer (links to DocHub; see **Canvas Files** for the actual files): Windows, macOS
Online installer: Windows, macOS

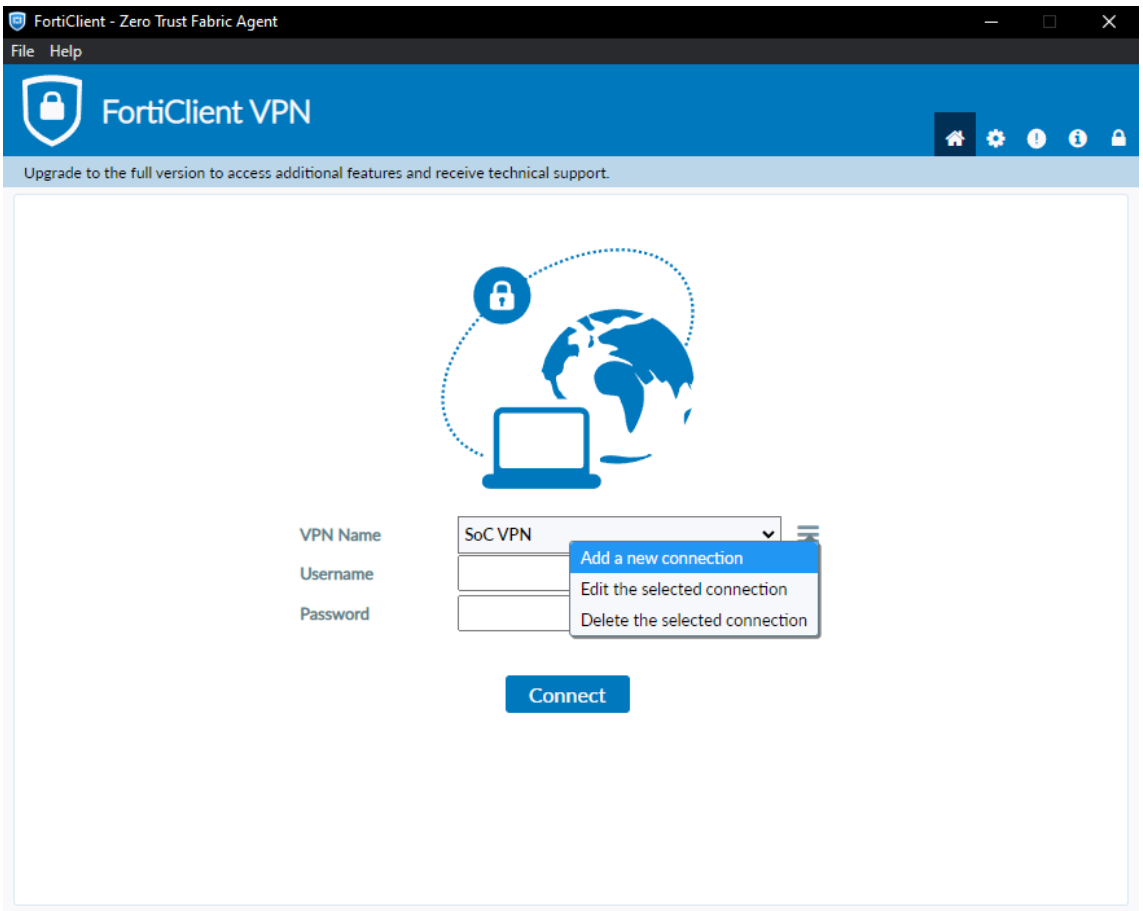
Before you begin, here are some important points to note:

- For Windows 10/11 users:
    - Please note that the FortiClient App from the Microsoft Store CANNOT BE USED anymore. You may proceed to uninstall it if you have previously used it to connect to SoC VPN.
    - We deeply regret to inform you that FortiClient VPN for Windows does not work on systems using ARM-based processors. Should you only require SSH access to the SoC Research Network, Compute Cluster or Practical Examination Servers, you may use the SSH Jump Host Service.
    - **[15/4/2025]** We are aware of an error causing users to not be able to log in and use the VPN service after completing the Microsoft SSO process, despite entering your NUS-ID credentials correctly and clearing the MFA prompt. If you are using versions 7.4.0, 7.4.1 or 7.4.2 of FortiClient VPN, and get this error "Credential or SSLVPN configuration is wrong. (-7200)" after the MFA prompt, please uninstall it, download and reinstall the latest version of FortiClient VPN (current version: 7.4.3).
- For macOS users:
    - FortiClient works properly only when you grant permissions to access the full disk in the *Security & Privacy* pane for the following services: fctservctl2 and FortiClient. Please refer to this link for the guide on addressing this issue.

When you have installed FortiClient, perform these steps as part of the initial setup of the application:

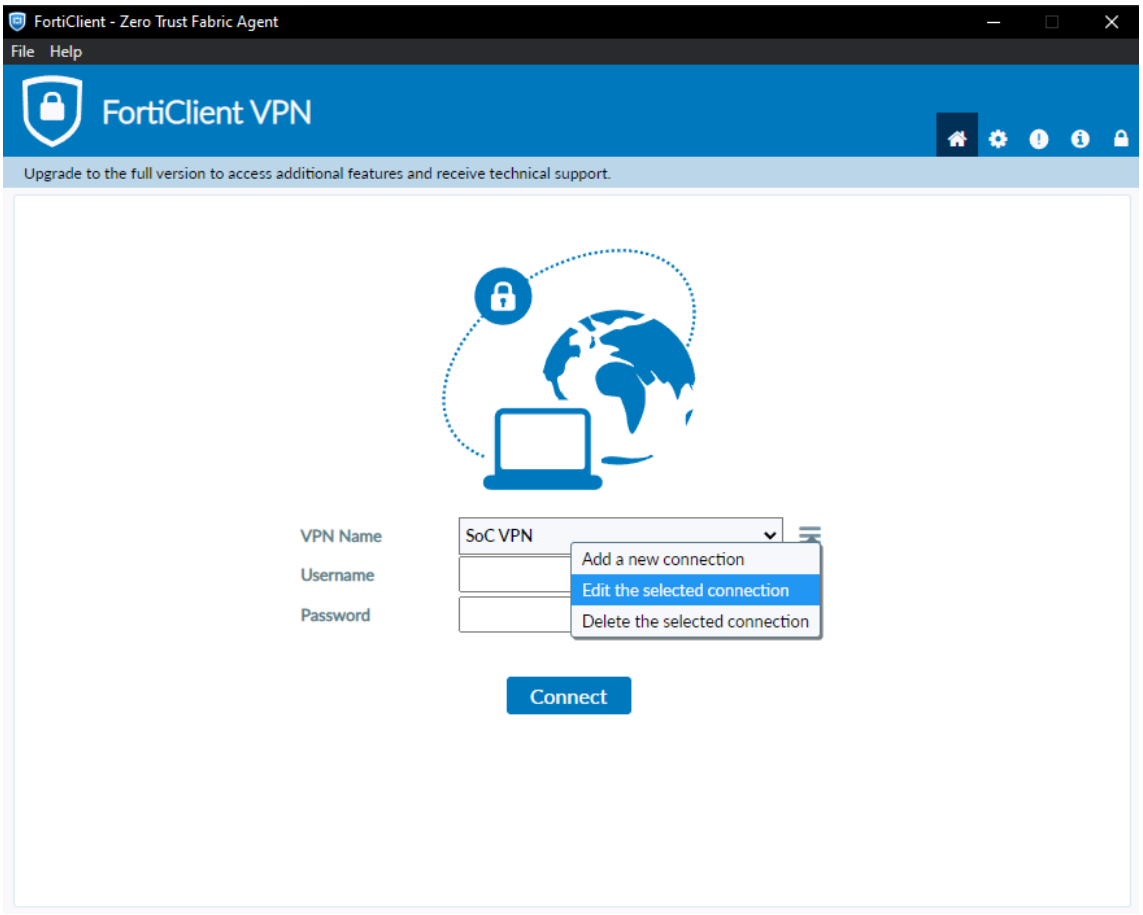
1. Double-click the FortiClient VPN icon on your desktop (Windows 10/11) or click on the FortiClient icon then "Open FortiClient Console" (macOS) to open the FortiClient VPN application.

2. Click “I Agree” (both Windows and macOS).
3. Click on “Configure VPN” to create a new VPN connection.
    - If you are adding a new or a secondary VPN connection, click the three horizontal bars, then click on “Add a new connection” shown below:



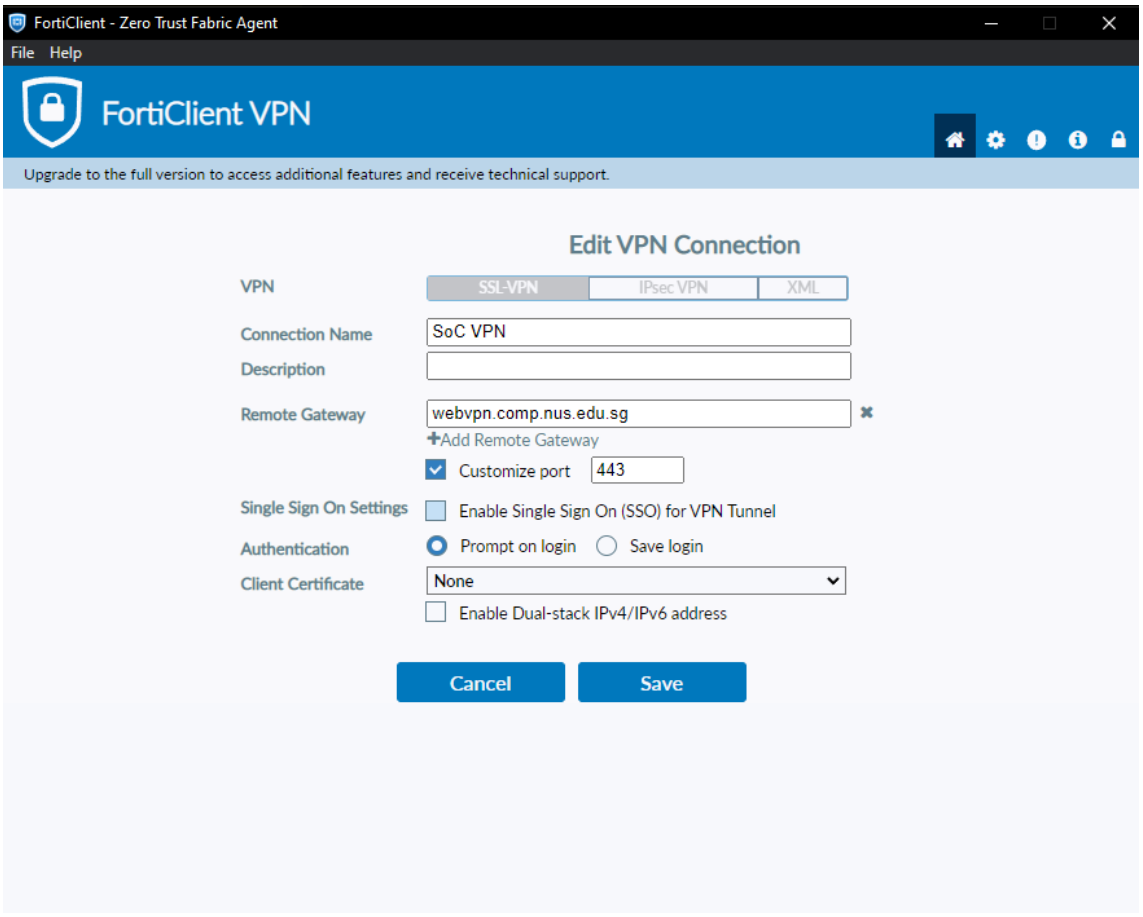
    - If you have previously set up your VPN connections and are changing to the SSO-based login, click the three horizontal bars, then click on “Edit

the selected connection" shown below:

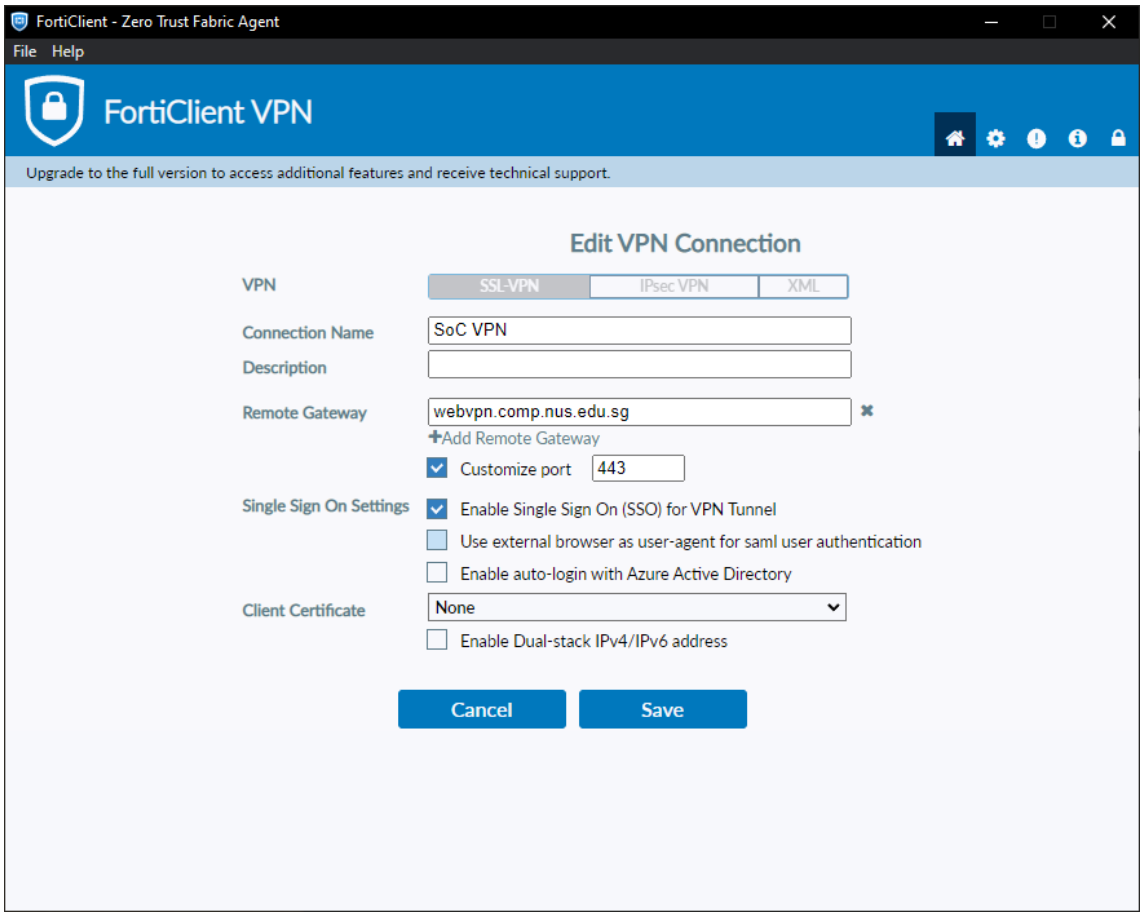


4. Use the following settings when adding a new connection:
    - Select **SSL-VPN**
    - Connection Name: **SoC VPN** (or **SoC Staff VPN** for staff users)
    - Description: optional
    - Remote Gateway: **webvpn.comp.nus.edu.sg** (or **staffvpn.comp.nus.edu.sg** for staff users)
    - Port: 443. There is no need to click on the "Customize Port" checkbox, unless it is already checked.

- Click the “Enable Single Sign On (SSO) for VPN Tunnel” checkbox.



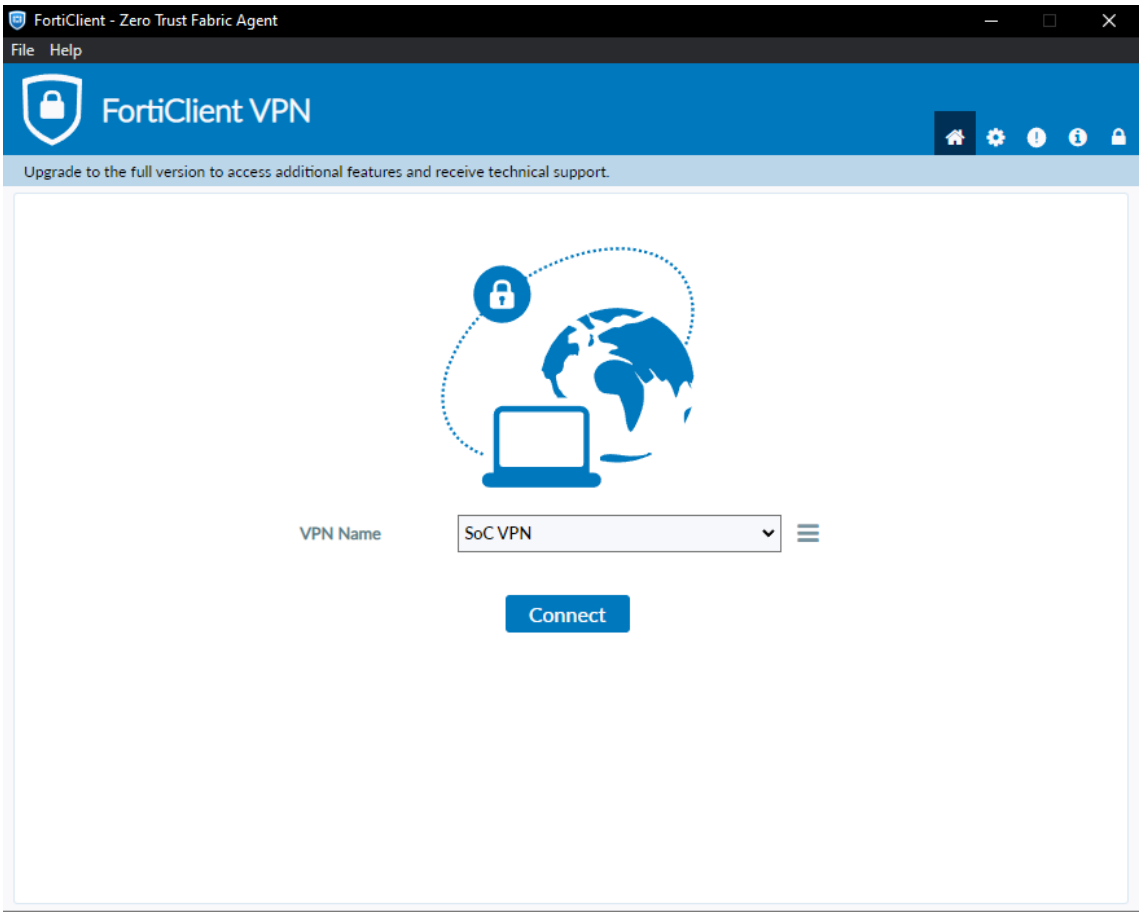
- The checkbox to “Use external browser as user-agent for saml user authentication” is optional.



  - If you intend to skip entering your credentials whenever you want to use SoC VPN, tick this box, and choose “Stay Logged In” in the Microsoft SSO login browser page when prompted. Please ensure that your device is not a shared/public device so that your credentials are not misused!

- Client Certificate: **None**
- Leave all other checkboxes, such as “Enable auto-login with Azure Active Directory” and “Enable Dual-stack IPv4/IPv6 address” **unchecked**. The latter option(s) may or may not appear depending on your FortiClient VPN version.
- Save the connection. The prompt to enter your username and password should disappear, and the only button you see is either “Connect” or

“SAML Login”, depending on your version of FortiClient VPN.



5. Repeat the above procedure if you are adding or changing another VPN.

When you are done, follow these steps to connect to SoC VPN here (see main VPN PDF).