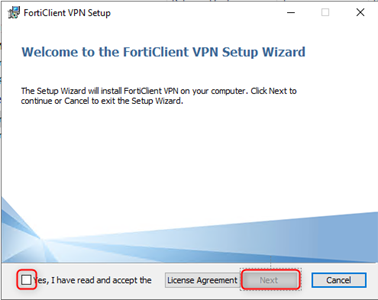
**Install Forticlient VPN 7 & configure the client**

KI 0844

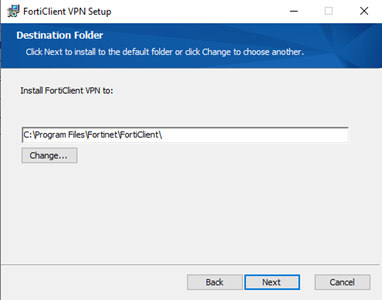
The below instructions are for users that had to uninstall their version of the FortiClient as it was a version prior to 6.4.

**How do I install version 7?**

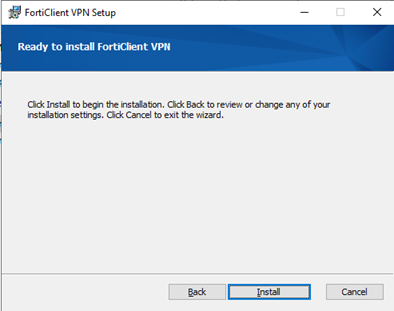
1. Go to <https://ulcampus-my.sharepoint.com/:u:/g/personal/service_deskitd_ul_ie/ETJY5aKfB5lMhMsOywi1GwEBtsbgCrf_WYR3yQr0B-IbKA?e=YGcoMx>and download the installation files.
2. After the file has been successfully downloaded, go to the location of where you saved the file – note the default location is your downloads folder.
3. Click on
4. When prompted allow this app to make changes to your device.
5. Accept the license agreement.



1. Select ‘Next’ on the Destination Folder.



1. On the Ready to install FortiClient VPN screen, click ‘Install’



8. Click Finished when prompted.  
  
**How do I configure version 7?**  
  
1. Open the FortiClient VPN & select Configure VPN or Add new Connection (If an existing profile exists).  
2. Set the below settings (see screenshot)

* Verify SSL-VPN is selected
* Connection Name: UL SAML (Can be set to anything)
* Remote gateway: ulssl.ul.ie
* Tick “Enable Single Sign On (SSO) for VPN Tunnel”



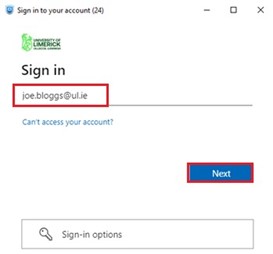
3. Click Save.

**How do I connect to the SSL VPN (FortiClient VPN)**  
  
1. Select the name you gave your SAML configuration in the drop-down menu and then click “SAML Login”.

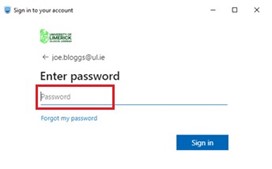


2. You will be prompted for your username.

* Username: firstname.last@ul.ie (**N.B** must include @ul.ie)



3. You will then be prompted for your computer account password (this is the same password you use to access email)



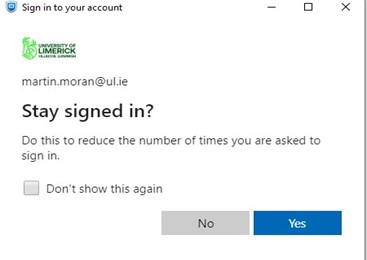
4. Next you will be prompted to complete your Multifactor Authentication (MFA).   
    Approve sign in request on your mobile device. This is multi factor authentication and is the same method you would follow for   
    approving a request when logging into your email.

* Non ITD managed / Public machines **N.B don’t tick this option** as it will store these credentials on this device.
* ITD Managed machines only can select this option “Don’t ask again for 60 days”. You will not be prompted for a username and password the next time you connect.

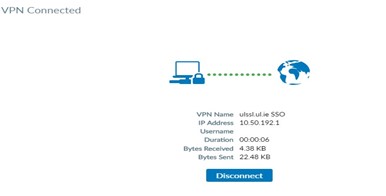


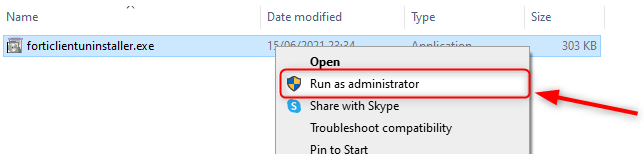
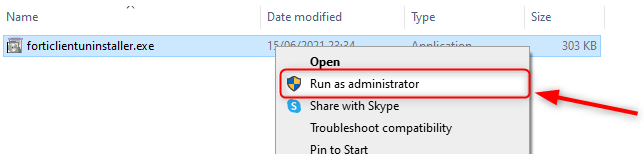
5. For the following screen select

* Non ITD managed / Public machines **N.B select No** to prevent another user on that machine using your account to connect to the ssl vpn.
* ITD Managed machines only can select Yes. You will not be prompted for a username and password until your token expires.



6. You should now be connected to the SSL VPN client using MFA Authentication.



Top of Form

Bottom of Form