Virtual Private Network

Note, the Fortinet VPN service has been updated to improve the authentication process. As a result, all VPN users are required to use the 'FortiClient VPN (only) version 7' software as detailed in the instructions on this page for all devices.

> There are also an individual pages per device type *(click the icon to open the page)*:

The updated authentication process enables Single Sign-On (SSO). SSO is the standard Microsoft 365 sign-in as currently used for all Microsoft services and you will be asked to enter your university email address and password and authenticate with MFA as usual.

---------- ---------- ----------

Welcome to VPN guidance

What is VPN? - Virtual Private Network (VPN) is a service which allows users who are connected to the internet to access University-restricted web resources and other services off campus.

To increase the security of remote access services, Multi-Factor Authentication is a requirement during the connection process. VPN is ***only*** required when you ***cannot*** access a service off campus and a connection to the VPN should only be made during the time you need. A VPN connection shouldn't be left running if not needed as this could impact the performance for other users.

There are no restrictions in place for the number of concurrent connections a user may have - please respect the time and use of VPN connections.

To ensure the university bandwidth is not overloaded, please ensure you **only use the VPN for work activity**.

Please note, we no longer support third-party or lightweight VPN clients due to the changes with authentication.

Before you start

To use the VPN service, you must first take note and action the following steps:

Step 1 - Registering to use Multi-Factor Authentication (MFA)

The VPN service requires Multi-Factor Authentication for security and to approve the connection to the University network.

> To use the VPN, you will first need to set up a smartphone or iPad/tablet to work with multi-factor authentication (MFA).

Step 2 - Request access to the Fortinet VPN service

If you have not used the university VPN before and you are **not** a **permanent** member of staff, you will need to request access to the Fortinet VPN via the **IT Service Desk**.

Please note that access has been granted to all permanent university staff.

Installing FortiClient VPN

Download and install the FortiClient software from our remote.nottingham.ac.uk site, or, if you use a university-managed device then install using Company Portal (Windows) or Jamf (macOS). Please note, we no longer support alternative lightweight and built-in VPN software.

Step 3 - Install FortiClient VPN

University-managed devices

Please note: If you use a university-managed Windows or macOS device, you should install the FortiClient VPN software via Company Portal *(Windows)* or Jamf Self Service *(macOS)* - click the relevant tab below.

If you use a non-managed device, follow the steps below on the first tab.

Select the tab below for your type of device:

Renew your license to continue

Your evaluation license has expired. Contact your administrator to renew your Composition license.

Unsupported operating systems

For all unsupported operating systems, please use the "Quick Connection" web link at https://remote.nottingham.ac.uk to access a SSL VPN connection.

Setting up VPN

Once FortiClient is installed, follow the steps below for your operating system to set up and connect to the university VPN.

Step 4 - Configure FortiClient VPN

Note

Before following these instructions, you will need to have downloaded the appropriate Fortinet VPN client as detailed in Step 3 and have set-up Multi-Factor Authentication.

Follow the steps for your operating system to set-up FortiClient VPN:

Windows
Click here to view instructions...

If you use a university-managed Windows device, the VPN configuration may have already been installed.

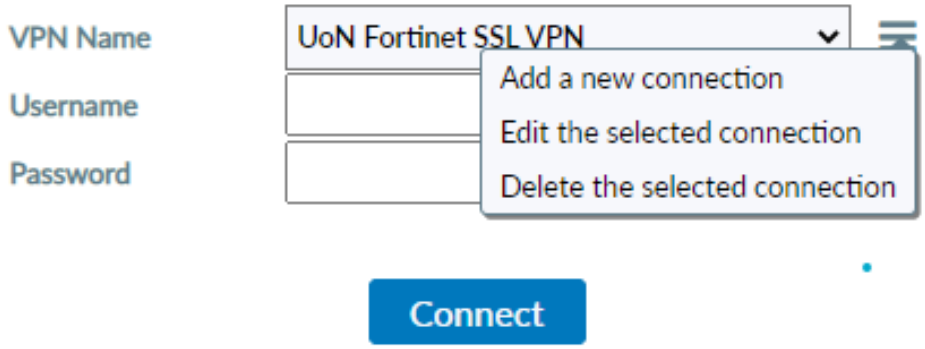
Windows

1. Open the FortiClient VPN software on your computer

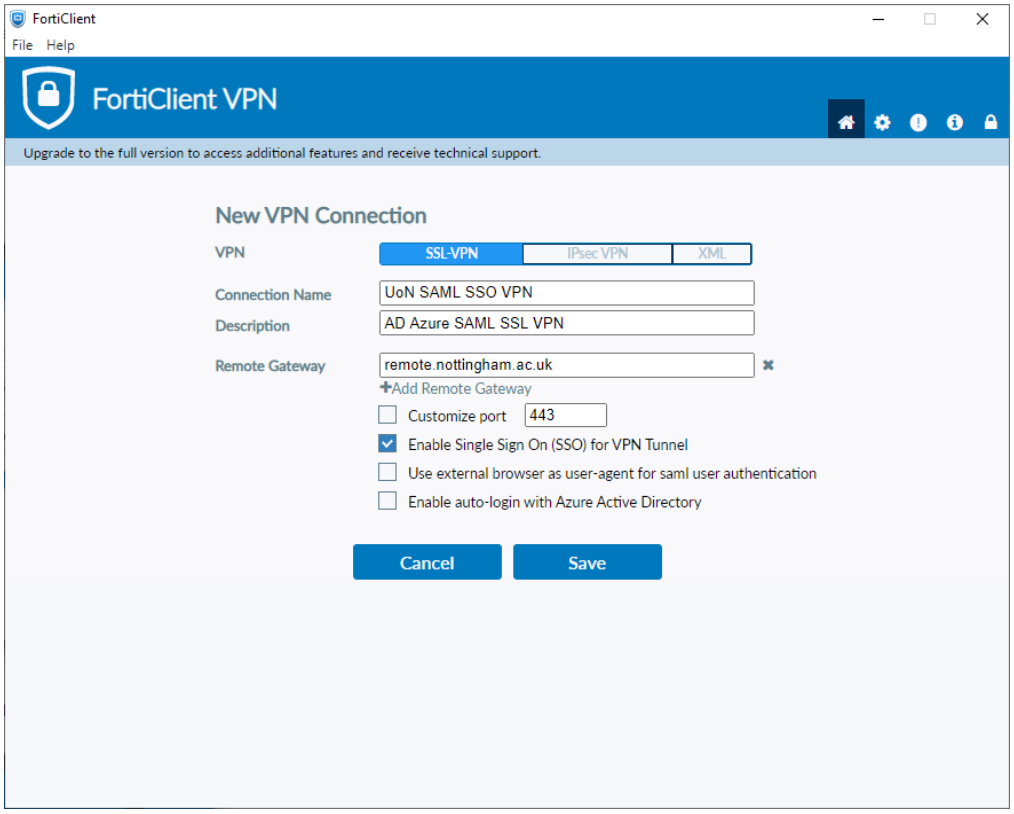
2. Set up the SSL-VPN connection:
    1. To configure a new VPN connection please click on the **Configure VPN** link, as shown below:

Configure VPN

2. In version 7 of the FortiClient, click on the icon with three horizontal lines next to VPN Name and click **Add a new connection,** as shown below:



3. Select the **SSL-VPN** tab



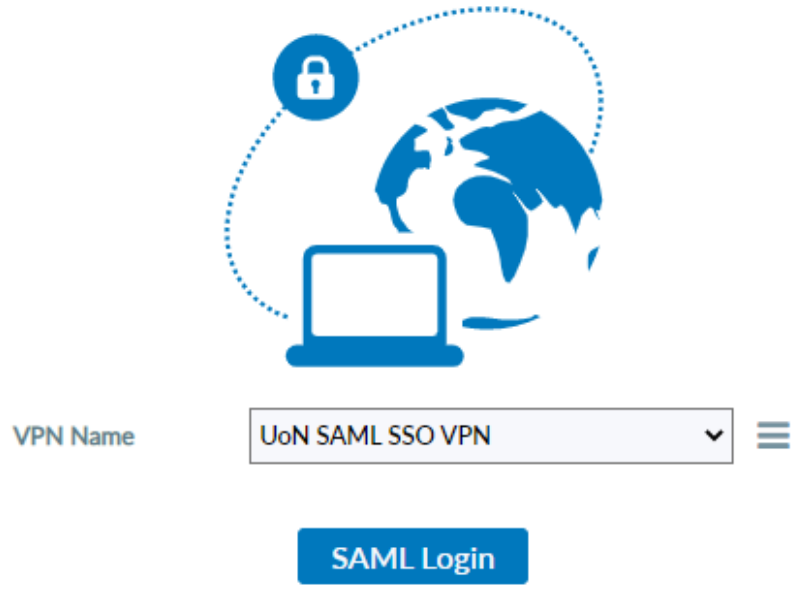
4. Enter the configuration settings as listed below:

   Configuration settings for SSL-VPN:

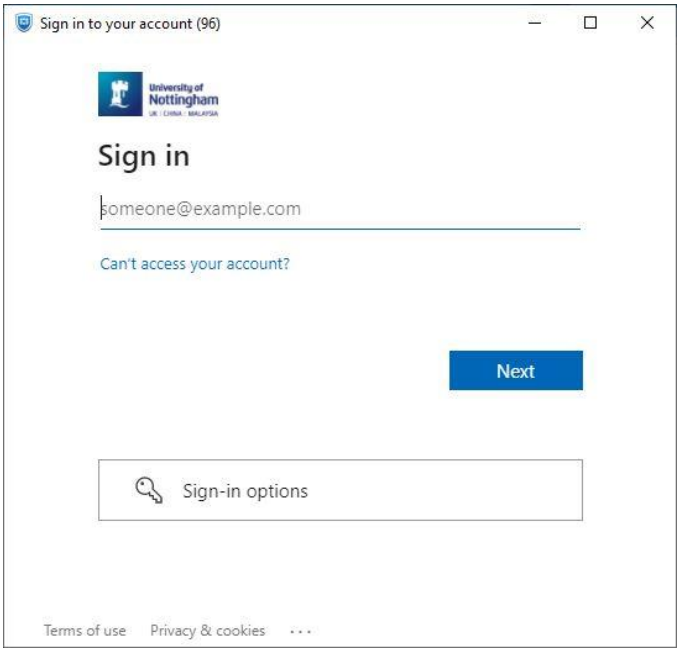
   - **Connection Name**: UoN SAML SSO VPN
   - **Description**: AD Azure SAML SSL VPN
   - **Remote Gateway**: remote.nottingham.ac.uk
   - **Port**: 443
   - **Tick the box**: Enable Single Sign On (SSO) for VPN Tunnel

5. Click **Save**

   You will now have the SAML Login button for connecting to the VPN:



3. **Connecting**
4. Connect to the Fortinet VPN by clicking the button **SAML Login**.



A pop up window will appear asking you to Sign in to your university Microsoft 365 account, enter your full university email address and click **Next**.

Then enter your password and click **Sign in**.

Top tip

Be prepared to approve the connection by having your authentication device ready before you sign in.

5. Click **Sign in**
6. Now, approve the connection from your mobile device that is set up with MFA.

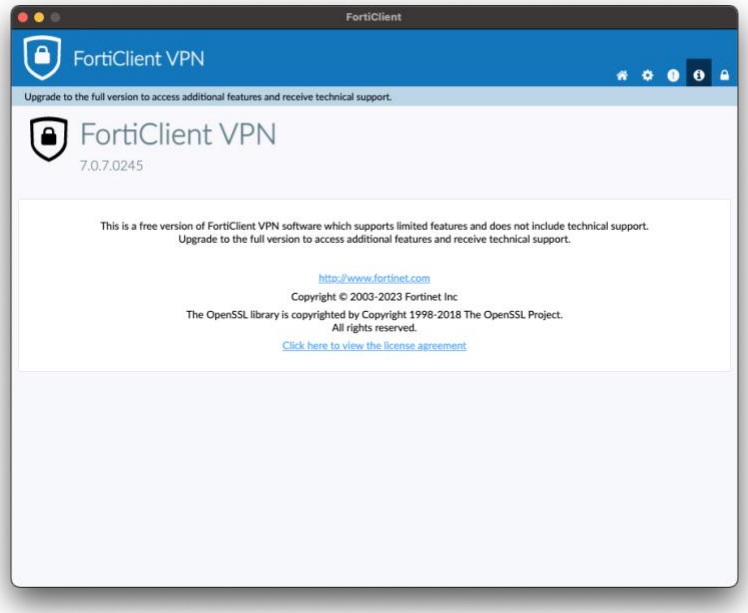
You will then be connected and a pop-up message should appear confirming that you are now connected to the VPN service.

Note: *Please only use the VPN during the time when you need to access university web resources or systems that are not available off campus.*

macOS

Open the VPN app

Start the FortiClient application and check the version by clicking the **i** button in the top right corner. Version must be 7.0.7 or higher:



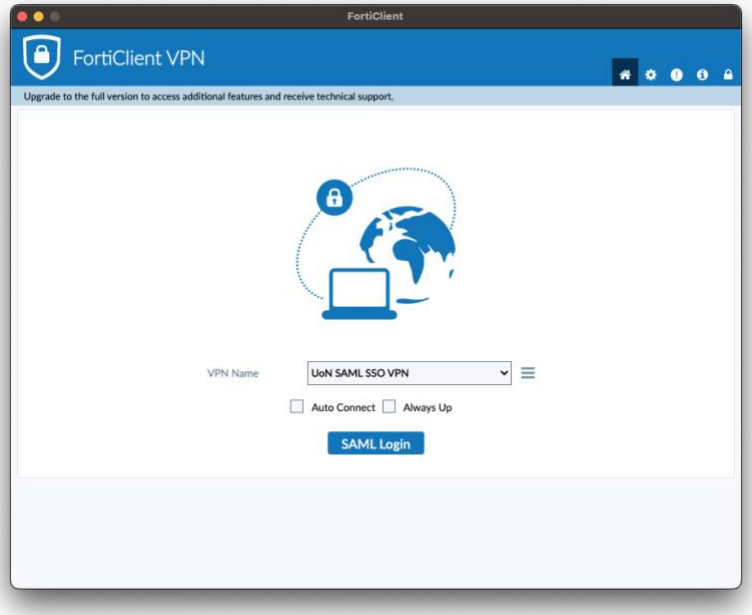
Setting up the VPN connection

Create a new VPN connection, select the SSL-VPN tab, and enter the following information:

Connection name: **UoN SAML SSO VPN**
Description: **AD Azure SAML SSL VPN**
Remote Gateway: **remote.nottingham.ac.uk**
Tick: **"Enable Single Sign On (SSO) for VPN Tunnel"**

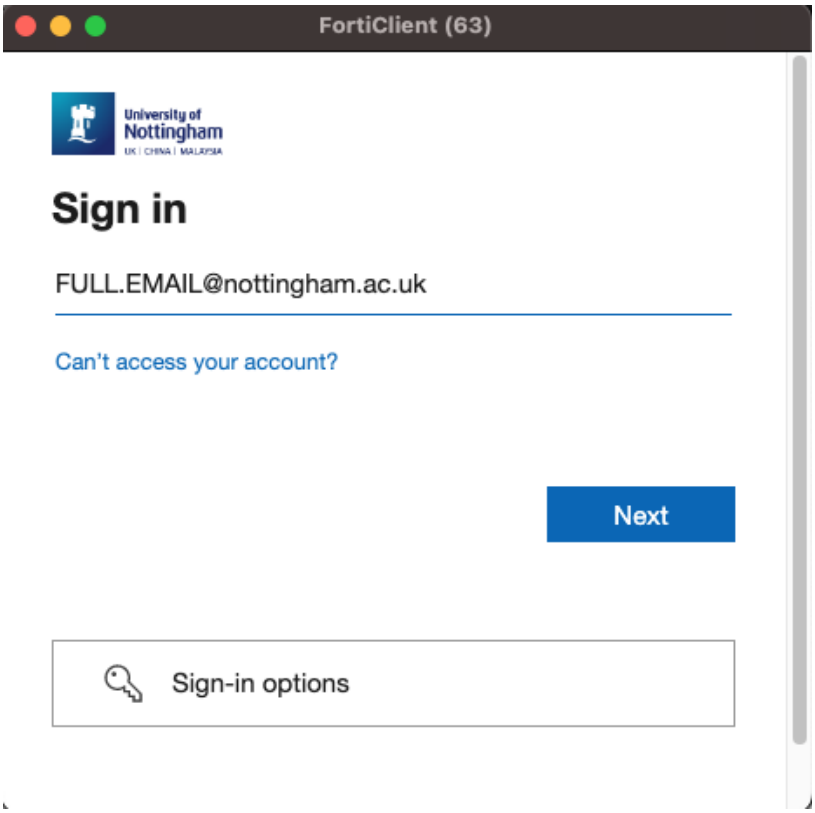
Save this connection.

To connect, click **SAML Login**.



You will then be prompted for Microsoft 365 credentials (use your full university email address).

e.g. firstname.lastname1@nottingham.ac.uk

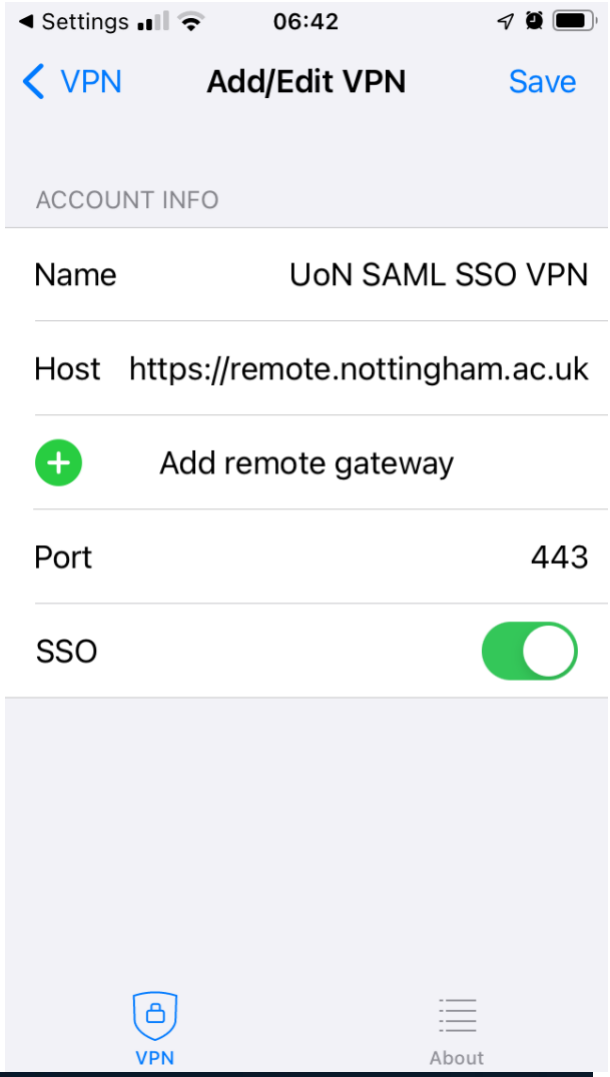


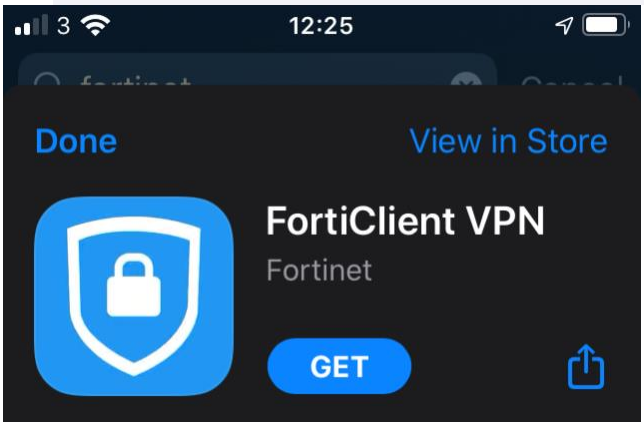
Click **Next** and then enter your university password to Sign in. You will be prompted to approve the connection using MFA.

To disconnect from the VPN when finished, click **Disconnect**.

iOS (iPhone, iPad)

1. Download the **FortiClient VPN** app from your App Store.





2. Once downloaded, open the app and press **I accept** the Privacy Policy.
3. You will be asked to 'Add VPN Configurations', press **Allow**.

4. Press **Select Connection** and then press **Add Configuration...** to start adding a connection.
5. Enter the configuration settings as listed below:

   Configuration settings:

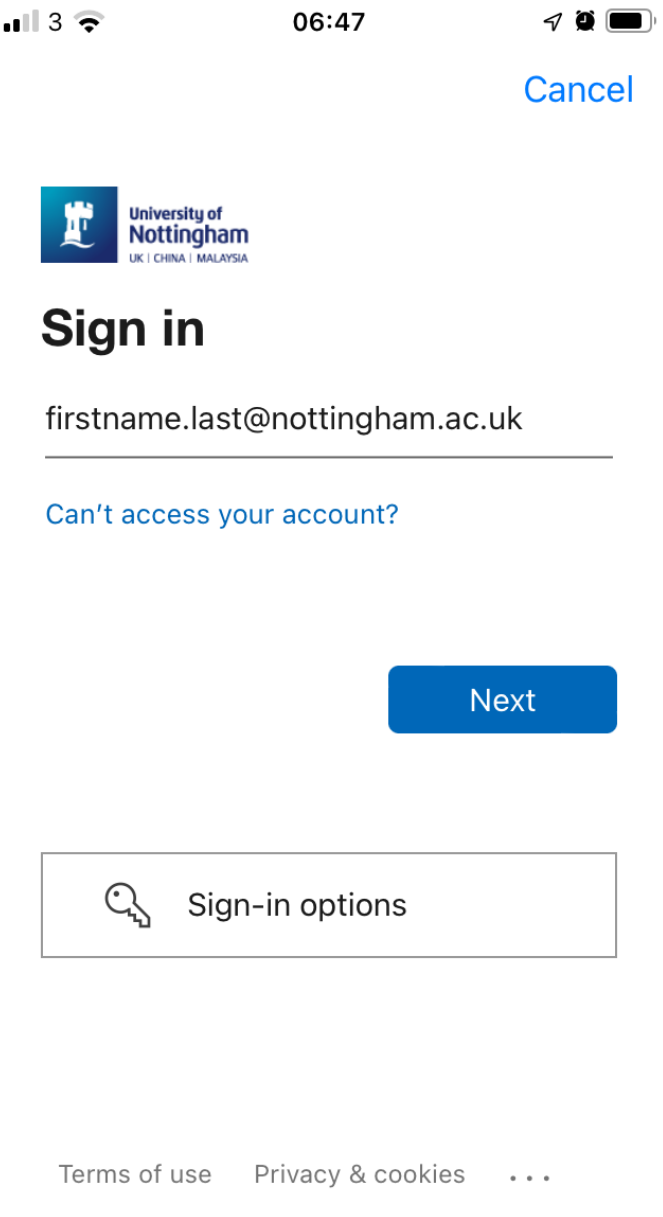
   a. **Name**: UoN SAML SSO VPN
   b. **Host**: remote.nottingham.ac.uk
   c. **Port**: 443
   d. **SSO**: enable the slider for SSO

6. Press **Save** once done and press **< VPN** to return to the main screen.

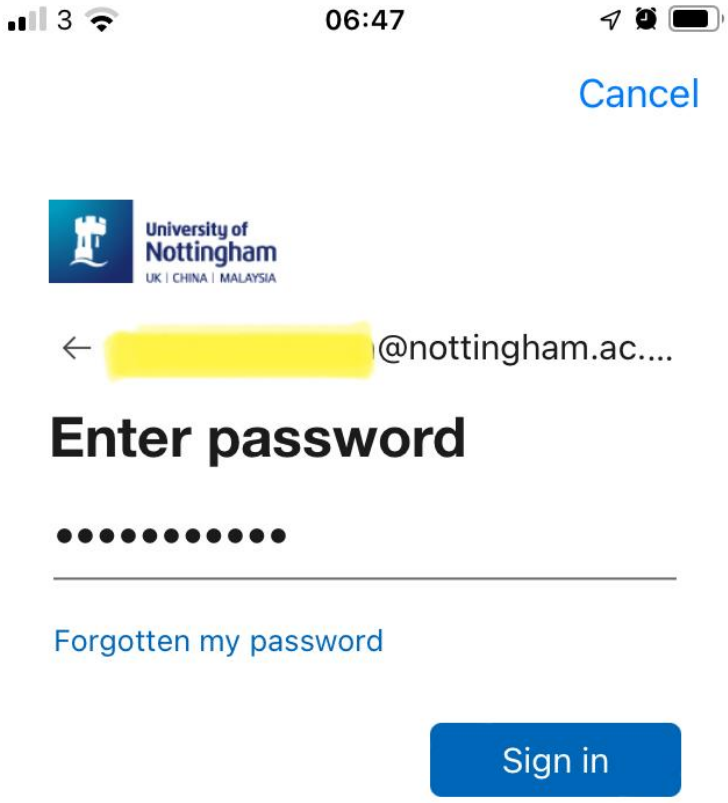
Connecting

7. To connect, press the slider next to VPN.

8. You will be directed to the Microsoft 365 Sign in page, enter your full **university email address**.



9. Now enter your **university password**.



Top tip

Be prepared to approve the connection by having your Authenticator device ready.

10. Press **Sign in**.
11. Now approve the connection from your mobile device that is set up with MFA.

    You will then be connected to the VPN service.

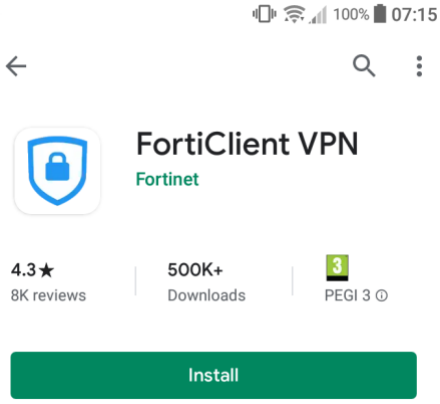
    Note: *Please only use the VPN during the time when you need to access university web resources or systems that are not available off campus.*

Android
Click here to view instructions...

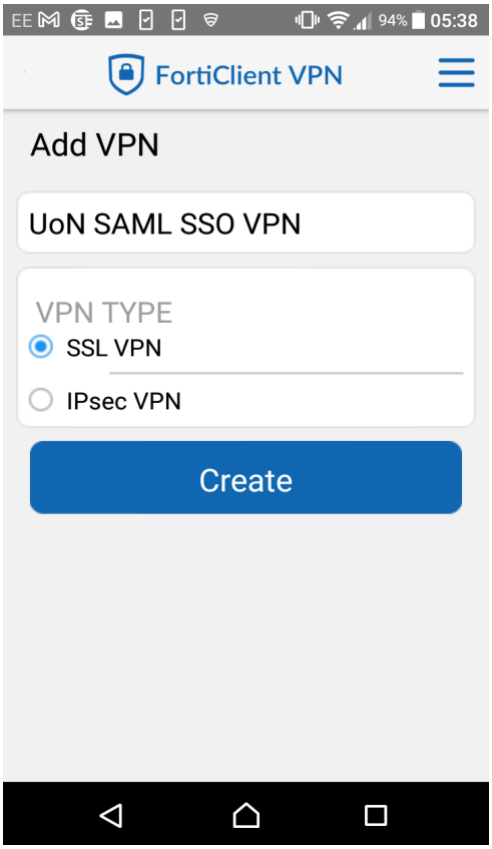
Note, you can click the images below to enlarge.

Android

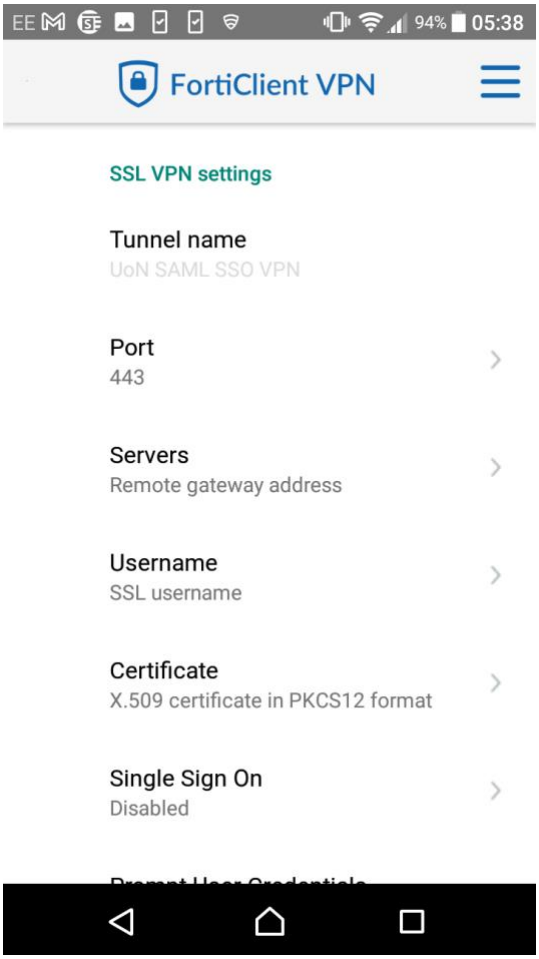
1. Download the **FortiClient VPN** app from your Google Play Store.



2. Open the FortiClient VPN app and select New VPN *(if visible)*.
3. You can **deny** access to files on your device.
4. Click **New VPN**, which will take you to the screen below
5. Input the VPN Name **UoN SAML SSO VPN** and **select SSL VPN** as the VPN type. Click **Create**

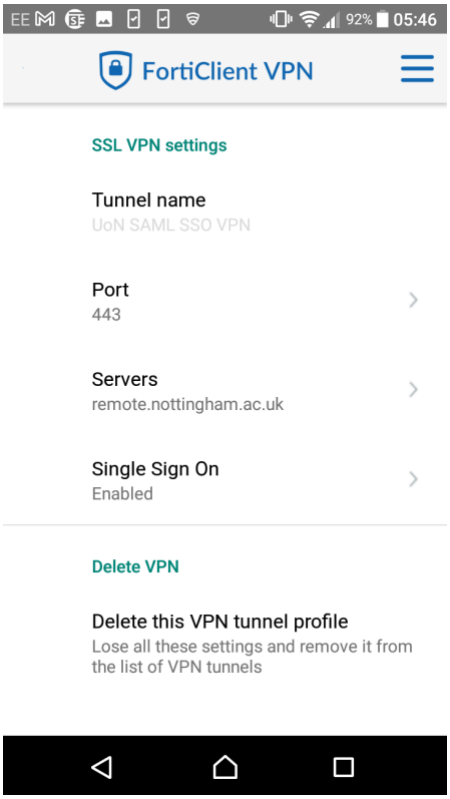


6. You will then see this screen



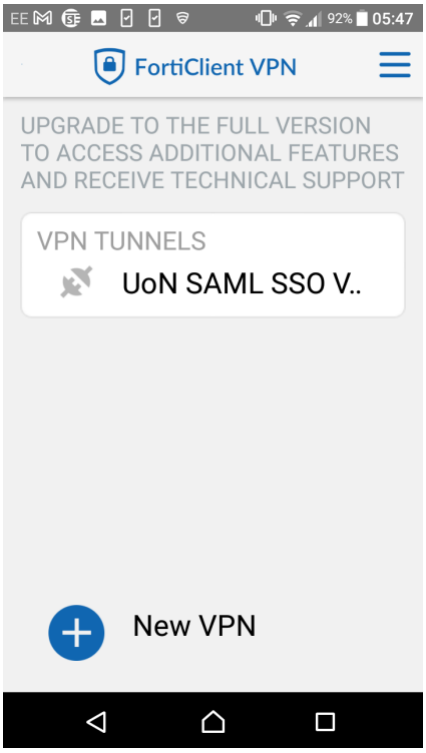
7. Click **Servers**. This will ask for a remote gateway address. Enter **remote.nottingham.ac.uk** and click **ok**, and then **ok** again

8. Click **Single Sign On**. Click the **Enabled** option

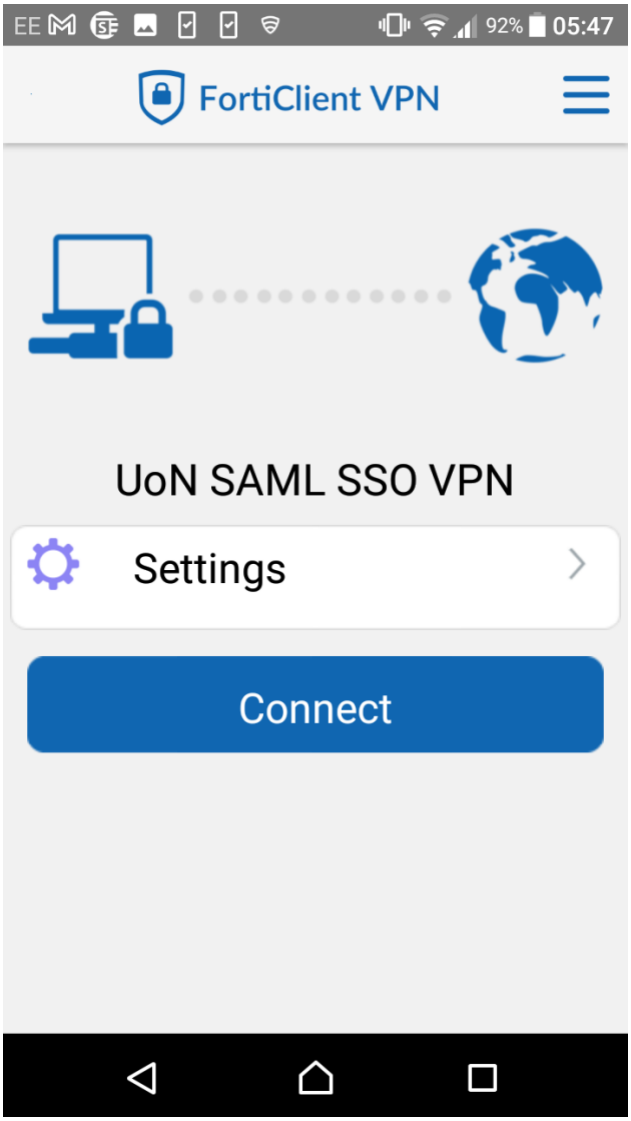


9. Press the menu icon (the three lines in the top right corner of the screen)

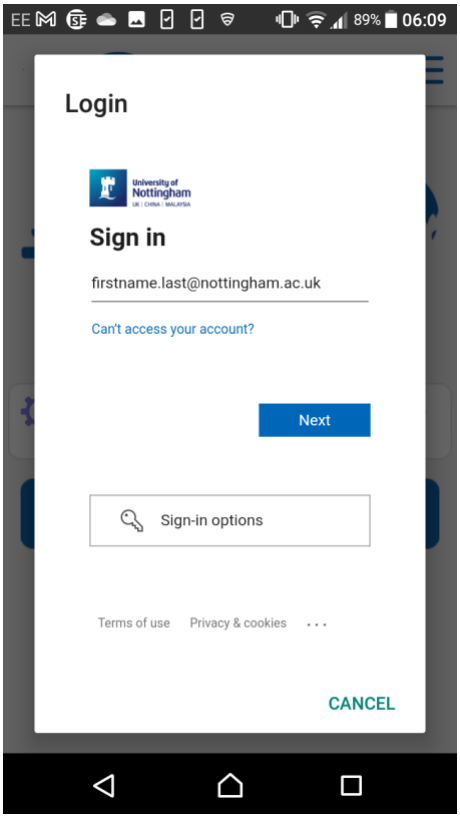
10. Press **VPN** and choose the **UoN SAML SSO VPN**



11. You will then see the screen below. Click **Connect**



12. You will be prompted for your Microsoft 365 credentials, enter your full **university email address** and click **Next**



13. Now enter your **university password** and click **Sign in**

14. Finally, you will be asked to approve the connection from your mobile device that is set up with MFA (Microsoft Authenticator), or by entering a code when prompted. Once approved, you will then be connected to the UoN VPN service.

Top tip

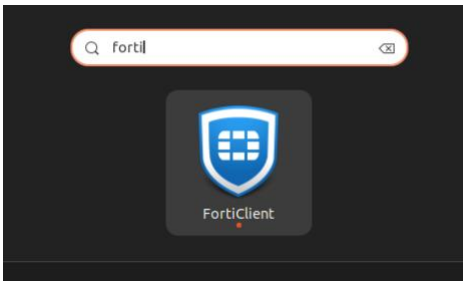
Be prepared to approve the connection by having the Microsoft Authenticator app open and ready on your mobile device before you press Sign in.

> ***Note:*** *Please only use the VPN during the time when you need to access University web resources or systems that are not available off campus.*

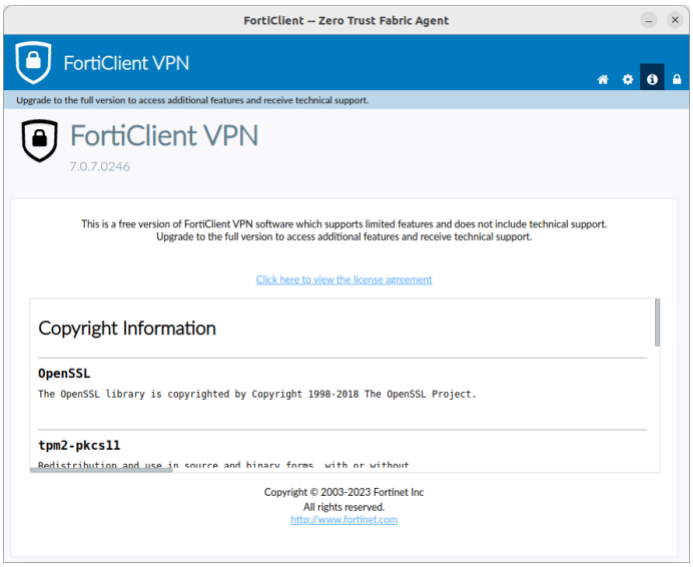
Linux
Click here to view instructions...

Setting up and connecting

Open FortiClient GUI.



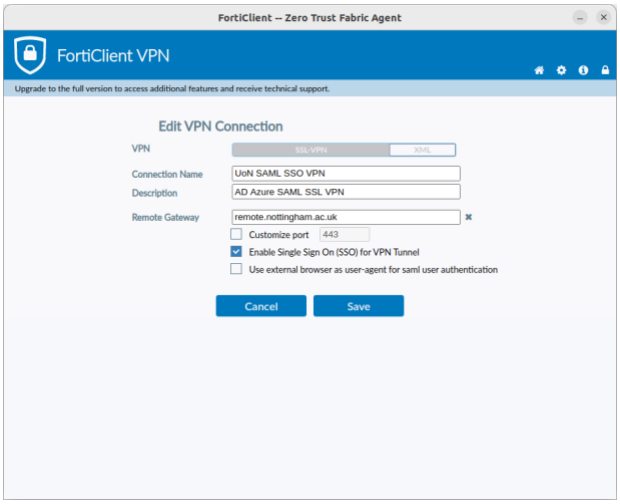
Check the version by clicking the **i** button in top right corner. Must be 7.0.7 or higher.



Create a new VPN connection from the home page (House icon).

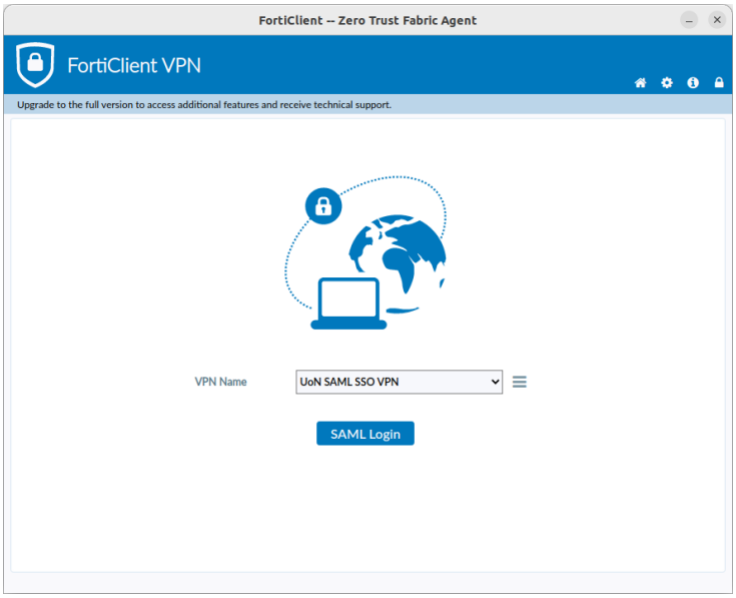
Select the **SSL-VPN** tab, and enter the following information:

Connection name: **UoN SAML SSO VPN**
Description: **AD Azure SAML SSL VPN**
Remote Gateway: **remote.nottingham.ac.uk**
Tick "**Enable Single Sign On (SSO) for VPN Tunnel**"

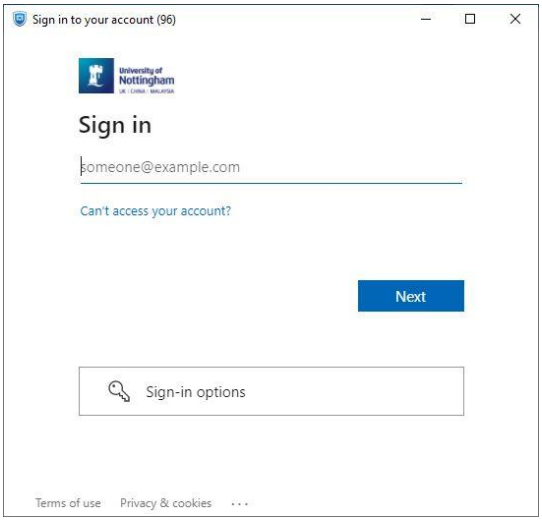


Save this connection.

To connect, click **SAML Login**.

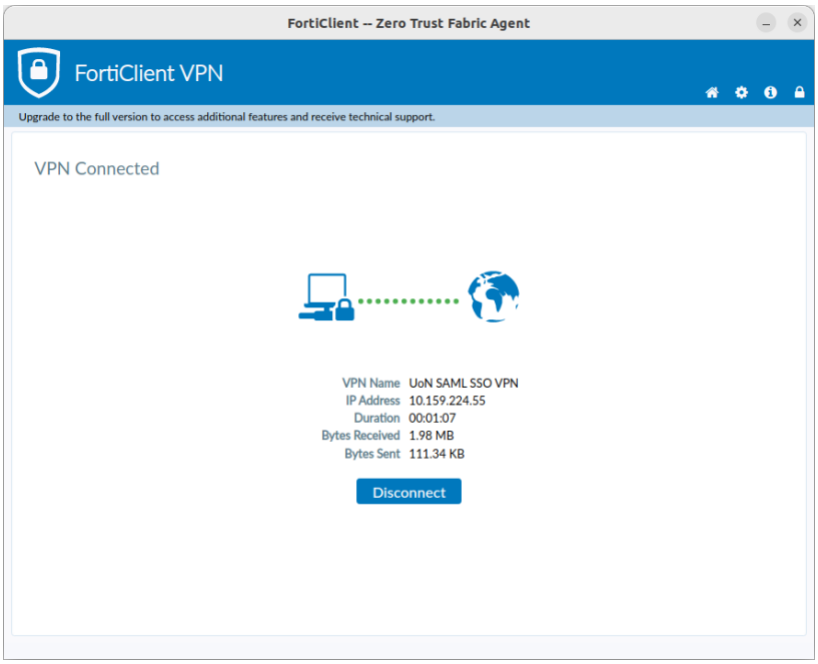


You will then be prompted for Microsoft 365 credentials (use your full university email address). e.g. firstname.lastname1@nottingham.ac.uk



Click **Next** and then enter your university password to Sign in. You will be prompted to approve the connection using MFA.

To disconnect from the VPN when finished, click **Disconnect**.



Using the University VPN service

Below are some additional guidance and questions about the VPN service.

Using the Web VPN

Using the web Quick Connection via remote.nottingham.ac.uk

Click here to view guide...

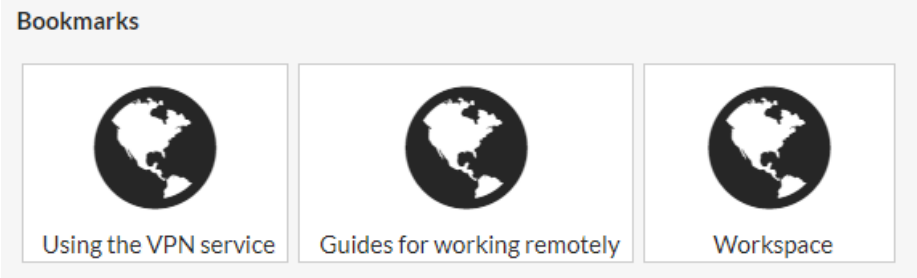
The Web VPN allows you to connect to University services without installation and configuration of a VPN client.

1. Visit https://remote.nottingham.ac.uk in any web browser (other than Internet Explorer).

2. You will be automatically be directed to the Microsoft 365 Sign in page - enter your University email address and password to sign in as usual.

3. Approve the connection from your mobile device that is set up with MFA (Microsoft Authenticator), or enter the code when prompted.

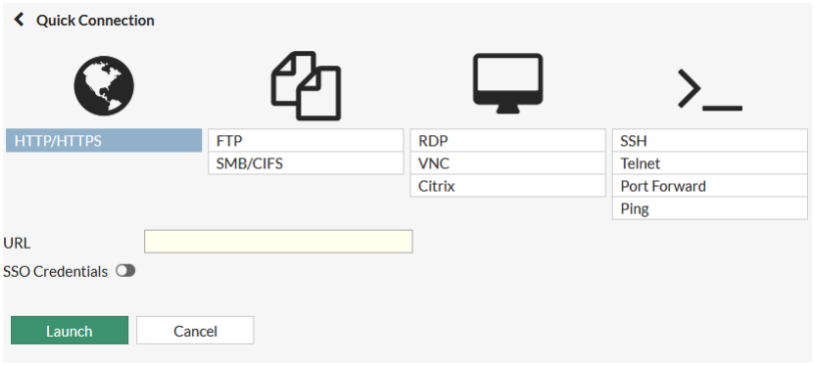
4. The main web page has three links pre-installed.



   1. Guide to using the VPN service
   2. Guides for working remotely
   3. Workspace

5. You can also create your own bookmarks, or launch a quick connection to a website (HTTP/HTTPS), SSH server, Remote Desktop etc. These connections will appear to come from the VPN itself, so are considered to be equivalent to being on campus.

   In this way you can access University resources that are campus-only. Simply enter the web link into the URL box and click Launch.



Please note, for the HTTP/HTTPS option, when entering a long website link in the URL box and clicking Launch, the page may not display due to a known limitation of URL length - an incomplete URL is passed through the connection.

If you are attempting to preview a CMS page with a long URL, please either add the missing characters to the URL or, for a much better experience use:

- the FortiClient VPN software as detailed on this page or
- the Virtual Desktop service.

Frequently Asked Questions

FAQs

When should I use the VPN service?

You should only use the VPN service when you ***cannot*** access University systems or web resources that are only available on campus.

A connection to the VPN should only be made during the time you need, remember to disconnect when you are not using it.

To ensure the University bandwidth is not overloaded, please ensure you **only use the VPN for work activity**. You should disconnect the VPN if you stream non-work related activity, such as YouTube, video streaming etc.

If you have an on campus Desktop PC that is connected to the university network, you will first need to connect to the VPN when off campus to access your Desktop PC.

I have requested access to the VPN but not heard from the IT Service Desk - what should I do?

Please note that VPN connections are limited. All staff can use this service without need to make a request. For all other users, approval of VPN requests will be prioritised according to criticality.

I don't use a Windows operating system, what should I do?

FortiClient VPN is available on many operating systems - follow the instructions in Step 3 and 4.

We no longer support any VPN software *(including lightweight or built-in clients on your computer)* other than the official FortiClient VPN application.

I don't have admin access on my University computer to install FortiClient, what should I do?

FortiClient VPN can be installed on a university managed computer without admin access via the Company Portal app (Windows) or Jamf (macOS).

Alternatively:

- FortiClient VPN can be installed on your home personal computer.
- There is also the Web VPN option as shown earlier on this page.

How is SSO more secure?

SSO authenticates a user based on who they are, opposed to which network they are on.

This ‘identify-based’ access model means only authorised users will be able to access the VPN service, enhancing the university’s cyber security infrastructure.