SWINBURNE UNIVERSITY OF TECHNOLOGY

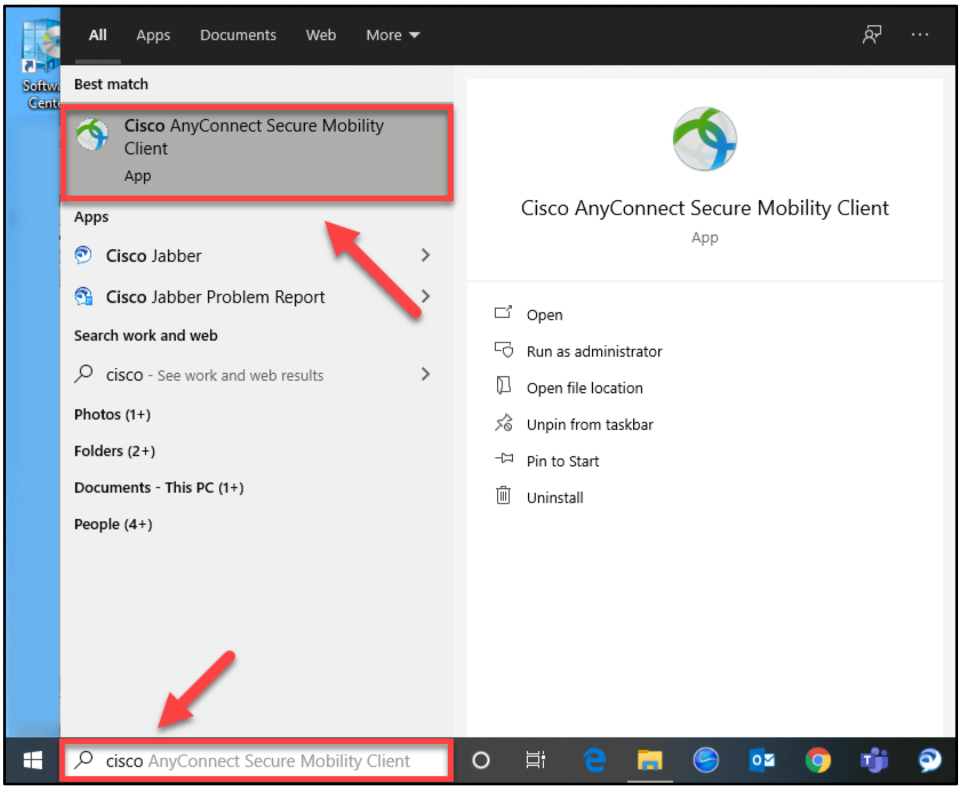
USING CISCO VPN WITH MULTI-FACTOR AUTHENTICATION

USER GUIDE

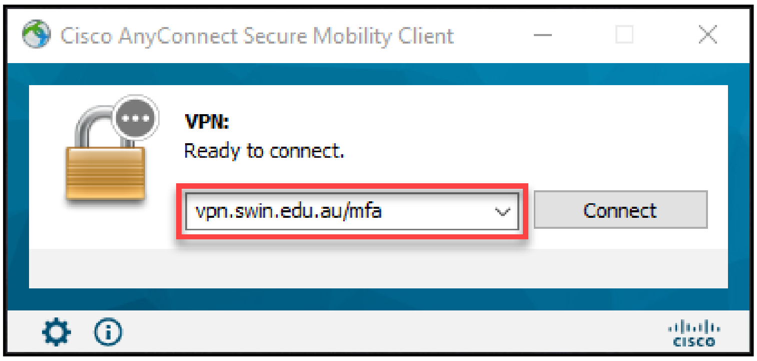
USING CISCO ANYCONNECT WITH MULTI-FACTOR AUTHENTICATION (MFA)

01

Open the **Cisco AnyConnect Secure Mobility Client** on your computer.



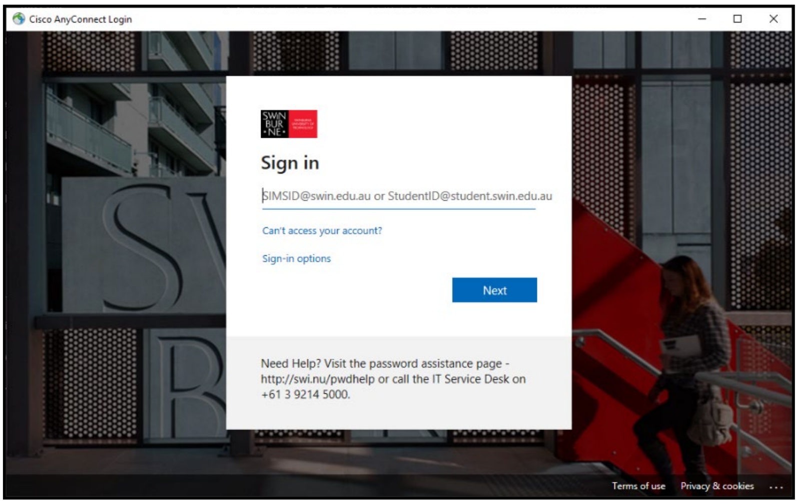
02



Ensure that the server field in the **Cisco AnyConnect Secure Mobility Client** has "**vpn.swin.edu.au/mfa**" filled in, then press the **Connect** button.

03

You will be prompted to log in using your Swinburne email address and password using the standard email login form.



Sign in

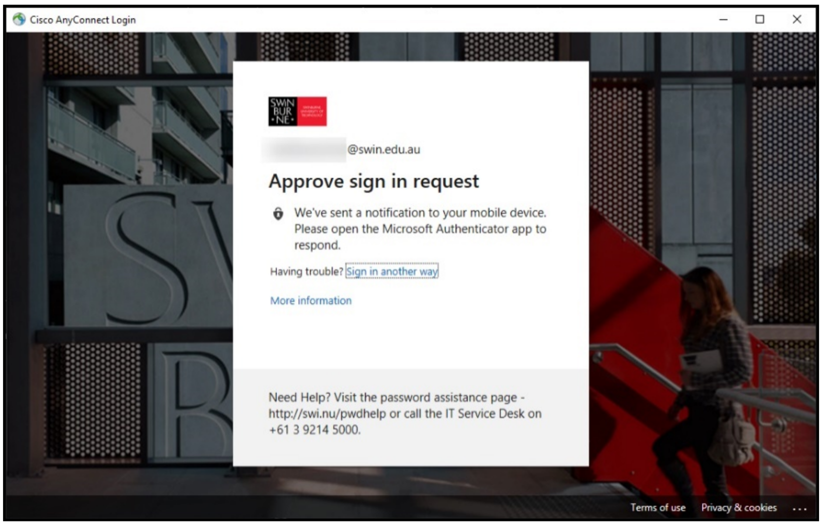
SIMSID@swin.edu.au or StudentID@student.swin.edu.au

Can't access your account?

Sign-in options

Need Help? Visit the password assistance page - http://swi.nu/pwdhelp or call the IT Service Desk on +61 3 9214 5000.

04



[redacted]@swin.edu.au

Approve sign in request

We've sent a notification to your mobile device. Please open the Microsoft Authenticator app to respond.

Having trouble? Sign in another way

More information

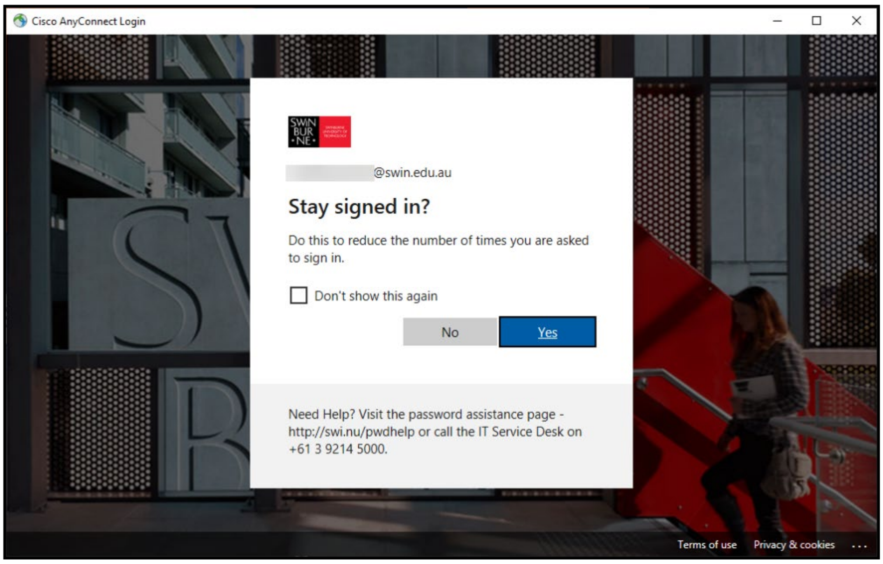
Need Help? Visit the password assistance page - http://swi.nu/pwdhelp or call the IT Service Desk on +61 3 9214 5000.

If you successfully entered your email and password, the VPN login will prompt your phone for MFA authorisation - please proceed with the steps on your screen which may vary depending on your MFA configuration.

05

Once approved, it will ask you if you wish to stay signed in. Press either Yes or No to continue with the connection.

Please note that due to security requirements, these options have no lasting effect; the next time you attempt to log into the VPN, you will be prompted for login details and MFA authorisation once more.



[redacted]@swin.edu.au

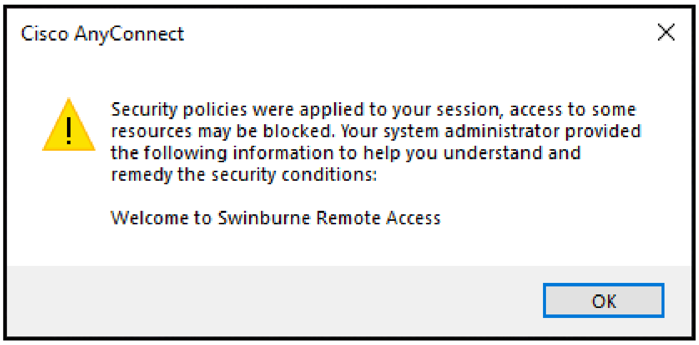
Stay signed in?

Do this to reduce the number of times you are asked to sign in.

□ Don't show this again

Need Help? Visit the password assistance page - http://swi.nu/pwdhelp or call the IT Service Desk on +61 3 9214 5000.

06



Cisco AnyConnect

Security policies were applied to your session, access to some resources may be blocked. Your system administrator provided the following information to help you understand and remedy the security conditions:

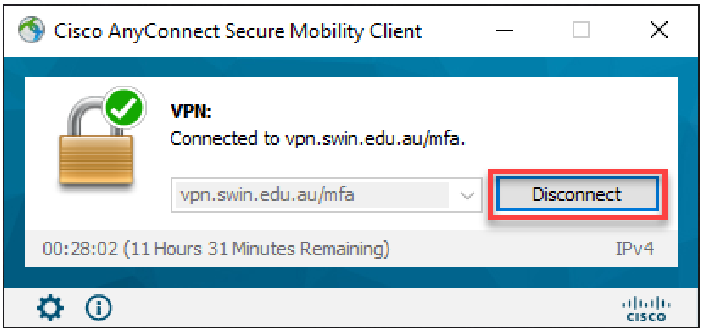
Welcome to Swinburne Remote Access

Once logged in, you will see this popup informing you that you are now connected to the Swinburne VPN.

For security reasons, your VPN session will time out after 12 hours, regardless of the level of activity detected.

07

To disconnect from the VPN environment, re-open the Cisco AnyConnect Secure Mobility Client and then press the Disconnect button to terminate the session.



Cisco AnyConnect Secure Mobility Client

VPN:
Connected to vpn.swin.edu.au/mfa.

vpn.swin.edu.au/mfa

00:28:02 (11 Hours 31 Minutes Remaining)

IPv4