How to Connect to the EOS VPN with MFA / Duo

Vincent Wu - 2025-02-18 - Network

If you do not have access to the EOS VPN, click here to email the helpdesk for access.

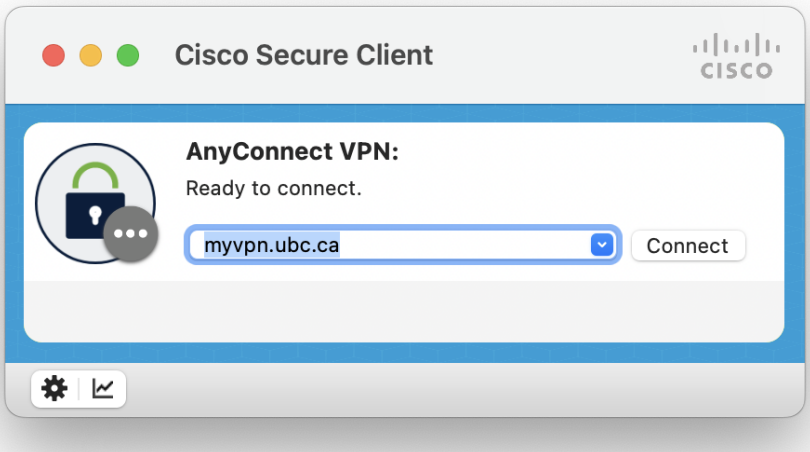
For regular UBC VPN connectivity, click here to view instructions.

Multi-factor Authentication on VPN has a different experience from web apps, since it uses the Cisco Secure Client native app instead of a browser. If you have not enrolled for UBC or want to manage your MFA devices, click here.

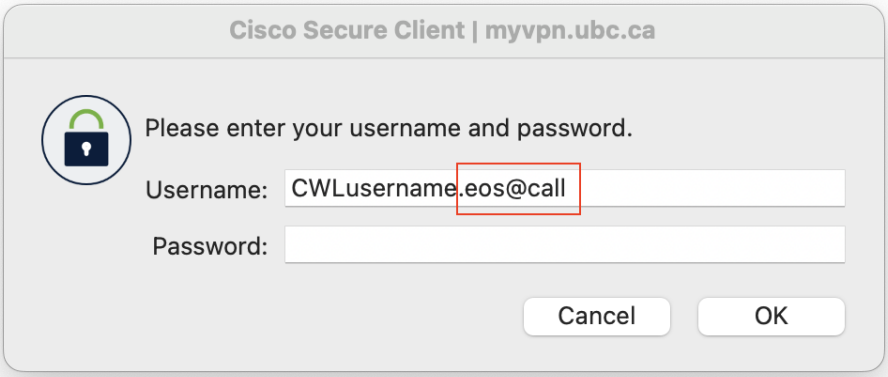
Once a connection for a particular VPN session has been established you will not be challenged with an authentication request for any other application or service while securely connected (unless you are attempting to access an application that contains confidential or highly secure information).

To connect to VPN with MFA, follow the steps below or watch the video (replace vpnpool with eos).

- Open the *Cisco Secure Client*



- Enter your CWL username and append .eos at the end.

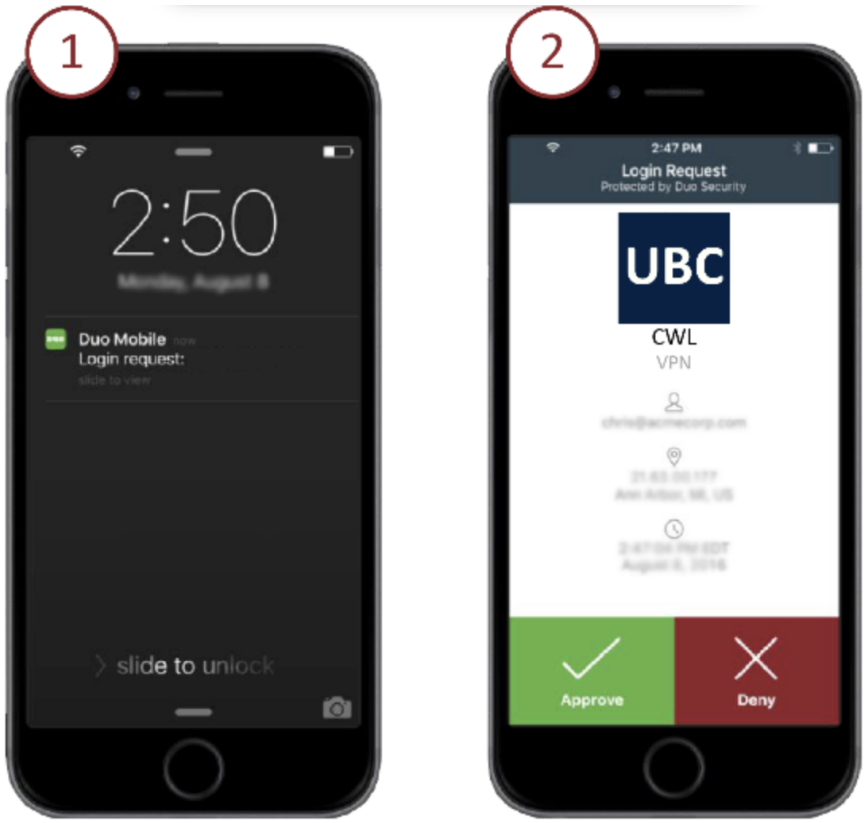


- **The new additional step** is to type “@” after your username along with how you want to authenticate.

Duo App	Enter **username.eos@app** if you wish to authenticate using your smartphone
Phone Call	Enter **username.eos@call** if you wish to authenticate by a phone call either to a landline (deskphone) or mobile phone. Please note that if you used username.eos@phone before, this '@phone' prefix still works too.
Passcode	Enter **username.eos@******** if you wish to authenticate using a passcode generated by a hardware token or a soft token using the Duo app.

If any information is entered incorrectly or forgotten you will see an error message reminding you of the extra information required to authenticate

- Once entered correctly, an authentication request will be sent to your method of choice



    - You will not see a separate message on the Secure client specifying that a response is waiting
    - You will know that the authentication has been approved when the Secure Client dialog box changes to “Establishing VPN Session”

- Once a connection is established you will be able to proceed as usual
  The Secure client will recall the information entered from your previous session.
  If you authenticate using the same method for each request, you will simply:

    1. Open the *Cisco Secure Client*
    2. The username and method of authentication will already be populated
    3. Enter your password and click ‘Okay’
    4. An authentication request will be sent to the method specified
    5. You will know that the authentication has been approved when the *Secure Client* dialog box changes to “Establishing VPN Session”

Additional instructions from UBC IT:
https://ubc.service-now.com/kb_view.do?sysparm_article=KB0016157

Adapted from: https://mfadevices.id.ubc.ca/vpn