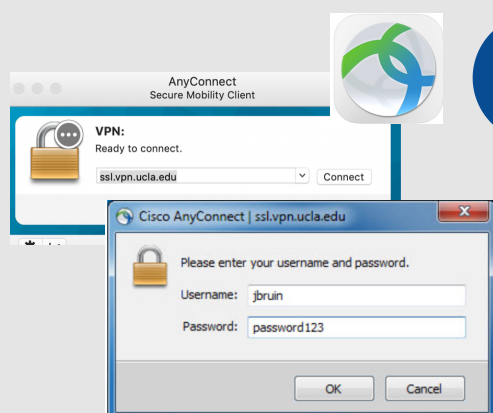


OFF CAMPUS SECURE REMOTE ACCESS

<https://www.library.ucla.edu/help/services-resources/connecting-from-off-campus/>



1

START VPN

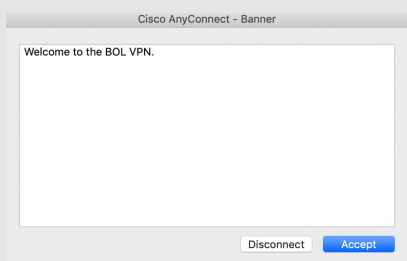
Once your computer is connected to the internet, use the Cisco AnyConnect software (from BOL) to establish a secure connection. Enter your UCLA Logon ID and password.



2

MFA

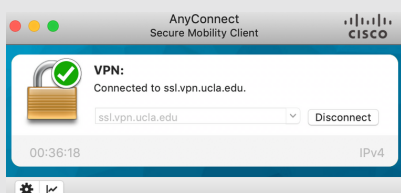
Multi-factor authentication double-checks that it's really you by sending a signal to another device. If you have the Duo app installed on your mobile phone, check your phone and authorize the logon.



3

YES, IT'S ME!

Back on your computer, VPN receives the authorization from your other device. Accept, and the VPN software adjusts your computer settings as if it has a campus internet connection.



4

VPN IS CONNECTED

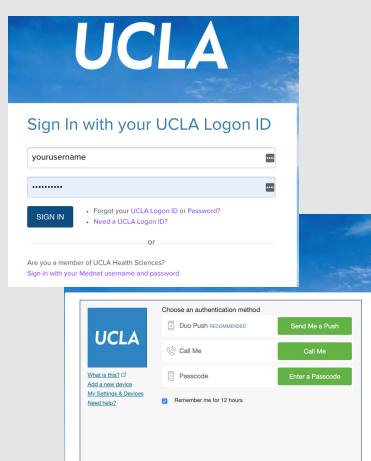
The secure network ensures that content you send and that you receive is encrypted. Think of VPN as an extra layer of protection when you work remotely.

Access provided by University of California, Los Angeles

5

TEST CONNECTION

Test VPN by going to a library resource that requires VPN, i.e., JStor: <http://jstor.org>. If you see a statement: "Access provided by University of California, Los Angeles" then you are connected!



6
7

DUAL AUTHENTICATION

If you log in to CCLE or MyUCLA now, you may still have to verify it's you with MFA.

