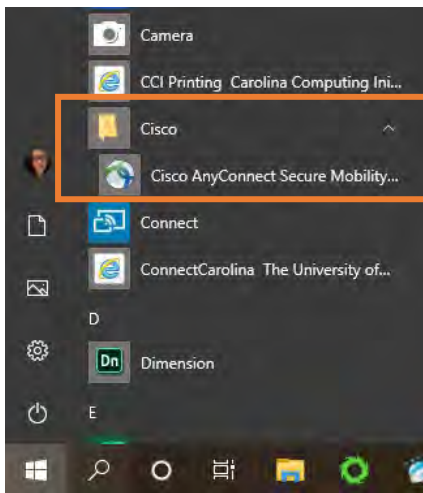


The University of North Carolina at Chapel Hill (UNC-CH) uses Cisco AnyConnect as its Virtual Private Network (VPN). This application provides you with an encrypted connection (secure tunnel) from off campus to gain access to UNC-CH internal network applications and shared network drives such as B:, to complete work that may require secure access, just as if you were physically on campus.

Note: You must download and install Cisco AnyConnect prior to completing the steps below.

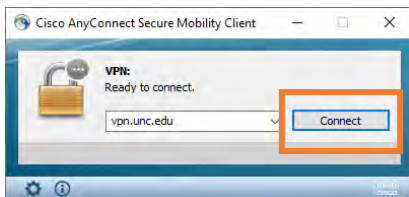
Connecting to Cisco AnyConnect (VPN)

1. Select **Cisco AnyConnect Secure Mobility Client** from the Start menu.



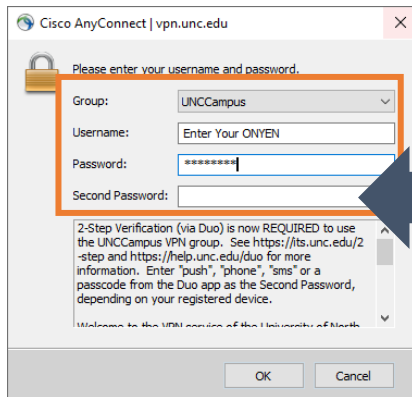
Result: The Cisco AnyConnect Secure Mobility Client and Cisco AnyConnect |vpn.unc.edu and pop-up windows will appear.

2. Click **Connect** by the VPN: Ready to connect drop down menu.



Note: The **Cisco AnyConnect VPN Client** should be pre-configured. If the entry screen does not appear as below, type **vpn.unc.edu** into the "Ready to connect" drop-down window next to the "Connect" button.

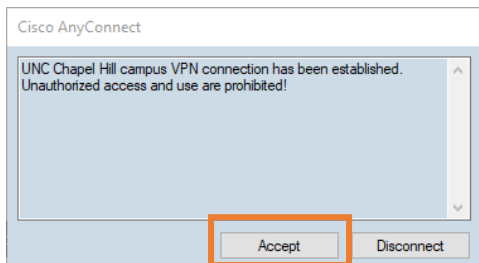
3. On the pop-up menu please choose the following:
 - a. Group is auto populated. (Unless instructed otherwise, this field should be UNCCampus.)
 - b. Enter your ONYEN
 - c. Enter the password associated with your ONYEN as the Password.
 - d. Enter a DUO command. For additional instructions, please see the section Understanding Second Passwords & DUO Commands on the next page.



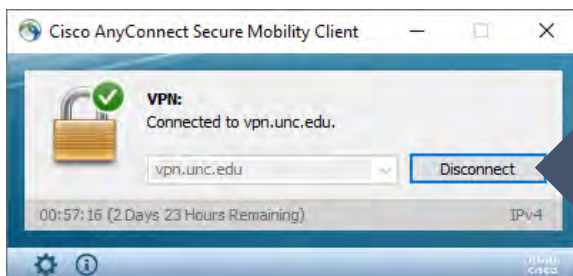
Second Password
 Be sure to enter a DUO command that is configured with your account. For example, if you type in “push” it will send a push notification to your phone/device.

Result: You will receive a DUO Authentication confirmation request based on the DUO command you enter from Step 3d.

4. Confirm you DUO Authentication based on the command you entered from Step 3d.
5. Click **Accept** on the Cisco AnyConnect pop-up that will appear.



Result: You will be connected to the VPN and a green check mark will appear over the lock icon.



Disconnecting from VPN
 To disconnect from the VPN locate Cisco AnyConnect icon on your Task Bar (🌐) or complete step 1 from the first page. Then click the **Disconnect** button.

Understanding Second Passwords & DUO Commands

Use the table below to identify the Second Password you should enter for first, second, or third types of DUO Commands. If you do not have access to your Primary method of Duo Command, you can select Second and Third DUO Commands that are configured with your account to confirm your DUO authentication.

DUO Command Options	Description	Primary DUO Command	Second DUO Command	Third DUO Command
push	Push a login request to your phone (if you have Duo Mobile app installed and activated on your iOS, Android, or Windows device). Just review the request and tap "Approve" to log in.	push	push2	push 3
phone	Authenticate via phone call back.	phone	phone2	phone3
sms	Get a new batch of SMS passcodes. Your login attempt will fail — log in again with one of your new passcodes.	sms	sms2	sms3
passcode	Log in using a passcode, either generated with Duo Mobile app, sent via SMS, generated by your hardware token, or provided by an administrator.	Enter code (For example: 123456 or 1456789)		

