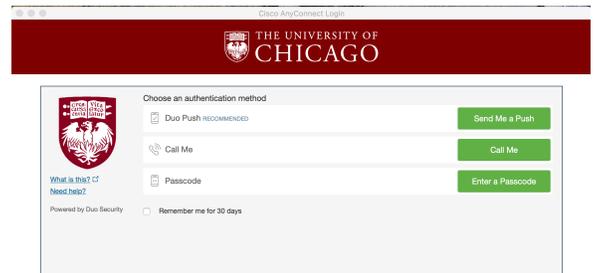


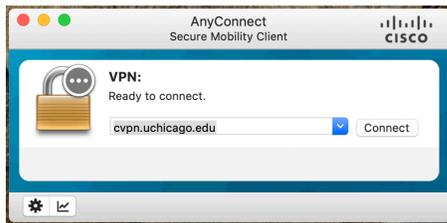
Connecting to a Microscopy Core computer via UChicago VPN - Mac

- 1) We've discovered that remote desktop login is not compatible with our usual cNet login system. Contact a Technical Director to be provided with the IP for the computer you wish to access and a local login for that computer — this will only be used in Step 7 or 10.
- 2) Only one remote connection is allowed at a time. Attempting to log in while someone else is connected could result in disconnecting the other person. Please use the online scheduler to reserve a workstation for remote use and respect others' reservations.

- 3) You must have two factor authentication in place for your cNetID. If you see this screen to the right and can get past it into something like email or Workday you already have two factor working and can move on to step 4. If you do not have two factor working, you can set it up at <https://cnet.uchicago.edu/2FA/index.htm>.



- 4) In order to access any core computer, you need to connect via the University's virtual private network (VPN). If you already have the University's Cisco VPN client installed and know how to use it, skip to step 6. Otherwise, instructions for how to install and activate cVPN on a Mac can be found through UChicago Information Technology Services https://uchicago.service-now.com/it?id=kb_article&sys_id=ee5929cfdbf644d07fd57b1cbf9619d6

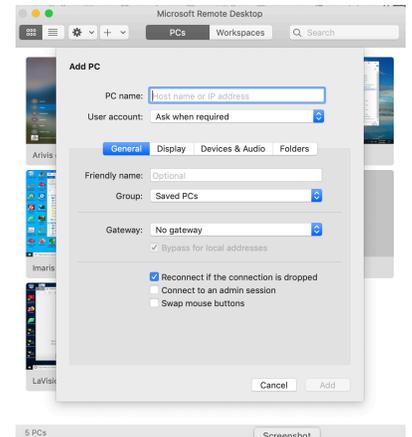


- 5) Once you have the Cisco VPN client installed, continue following the online instructions to connect through the VPN. You will be asked to input your cNetID and password and do two factor authentication again.

- 6) Next install the Microsoft Remote Desktop 10 app from the Apple App Store (it's free).

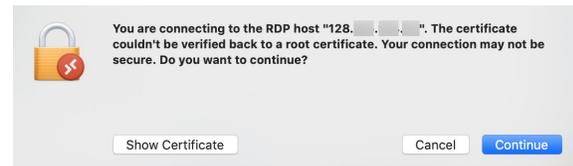


7) Open the Remote Desktop app. Use the pulldown under the + in the taskbar along the top to choose "Add PC". A new window will pop up. In the PC name section, type the IP for the computer you wish to connect TO (supplied by a Technical Director). I leave the user account section at "Ask when requested" but you can also put in the local login you were given by the Technical Director at this point. Enter a "Friendly name" like "Imaris computer". Leave all other fields as default. Hit Add.



8) To connect to the computer, double click on the picture of the computer you want to connect to. Later this picture will be of the desktop the way it looked last time you connected.

9) You may see a notification that the connection is not secure. This is OK, we're all a little insecure right now. Choose Continue.



10) If you did not store your user account information in step 7, you will be asked for the credentials to log in to the remote computer. Use the local login you were given by the Technical Director. This login is specific for the remote machine you are using and will not work anywhere else.

11) You should be connected to the remote computer and see that desktop as though you are sitting at that computer.

12) Note: Because of the local login needed in Step 7 or 10, the computer you are working on remotely will not automatically connect to the Core's data servers. You can map the server manually as you would from the lab using the Server Mapping Instructions (Windows version, you are on a PC now!!) on our home page <https://cpb-us-w2.wpmucdn.com/voices.uchicago.edu/dist/c/2275/files/2020/01/MappingToMicroscopyServerWIN-1.pdf>.

13) **When you are finished, LOG OUT** of the remote computer as you would if you were sitting in the Core. This will prevent excess charges on your bill and allow others (and you) to connect again later.

14) Close Remote Desktop.

15) If you saved data from the remote computer to a Core server, you can use the server mapping instructions (for a Mac this time) <https://cpb-us-w2.wpmucdn.com/voices.uchicago.edu/dist/c/2275/files/2020/01/MappingToMicroscopyServerMAC-1.pdf> to map the server from your Mac. You will need to remain connected through or turn on VPN as in Steps 4 and 5, but you DO NOT NEED Remote Desktop. Just connect through the VPN and then use the server mapping instructions.

16) When you have completed all your Core connected tasks, be sure to Disconnect and close the Cisco VPN client. Otherwise you will route all your personal web traffic through the University.