

## EPS Instructional Computing Facility (GM 103C and GM 103B)

### For Mac Users

The EPS Department maintains an Instructional Computing Facility (ICF) to support teaching and student research. The facility is located in Geological Museum 103C (17 workstations) and Geological Museum 103B (9 workstations). When not scheduled for courses, computers are available for undergraduate and graduate research and study by EPS students. Check the current schedule for class use of the ICF at <https://eps.harvard.edu/teaching-labs-and-schedules>.

The EPS ICF computers may be used in person or be accessed remotely via Windows Remote Desktop (RDP). Please do not save any items to the Desktop or hard drive of the machines, as these may be removed at any time. Use a cloud storage service (Google Drive, Dropbox, Sharepoint, etc.) or a USB drive to save your work.

### To use a computer in person:

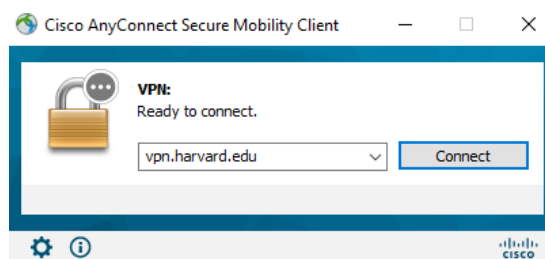
1. Check the status of the lab computers at <https://eps.harvard.edu/icf-computer-status>. Computers shown in green are available for use. Computers shown in blue or gray are currently unavailable. Identify an available computer in either 103C or 103B (machines are labeled by room and workstation number, e.g. EPS-103C-10).
2. Log in using your Harvard Key.
3. Please log out of the computer when leaving the room.

### To use a computer remotely:

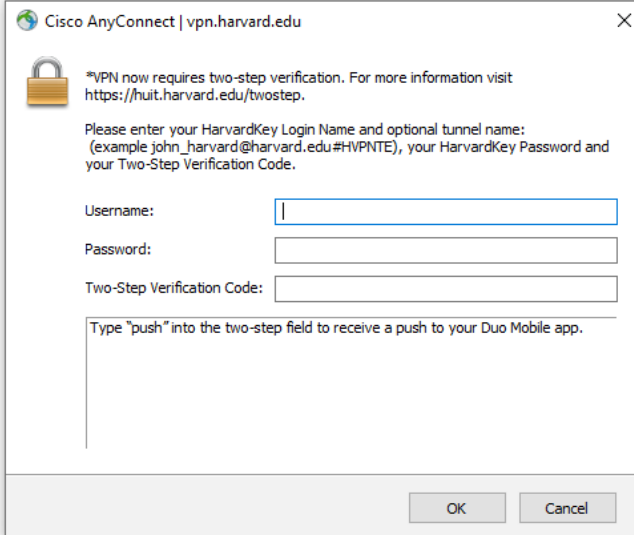
1. Connect to Harvard VPN using Cisco AnyConnect App.

*If you are not already set up with VPN, please follow the instructions below for installing the CiscoAnyConnect App and Connecting to Harvard VPN. You can also find these articles by searching the KB numbers on <https://harvard.service-now.com/ithelp>. For any questions on general VPN setup, please contact [ithelp@harvard.edu](mailto:ithelp@harvard.edu).*

- Installing the Cisco AnyConnect App (KB0017208)- [https://harvard.service-now.com/ithelp?id=kb\\_article&sys\\_id=f1766696db1e9418441560fdd39619ef](https://harvard.service-now.com/ithelp?id=kb_article&sys_id=f1766696db1e9418441560fdd39619ef)
- Connecting to Harvard VPN (KB0012966)- [https://harvard.service-now.com/ithelp?id=kb\\_article&sys\\_id=f1a542efdb90d7c483a2f3f7bf9619ec](https://harvard.service-now.com/ithelp?id=kb_article&sys_id=f1a542efdb90d7c483a2f3f7bf9619ec)
  - a. Open Cisco AnyConnect Secure Mobility Client or equivalent app on your computer. Type in **vpn.harvard.edu** and click Connect.



- b. Enter your Harvard Key username and password. Click 'OK'. Approve the two-step verification request. Click 'Accept' on the dialog box.



Cisco AnyConnect | vpn.harvard.edu

🔒 VPN now requires two-step verification. For more information visit <https://huit.harvard.edu/twostep>.

Please enter your HarvardKey Login Name and optional tunnel name:  
(example john\_harvard@harvard.edu#HVPNTE), your HarvardKey Password and your Two-Step Verification Code.

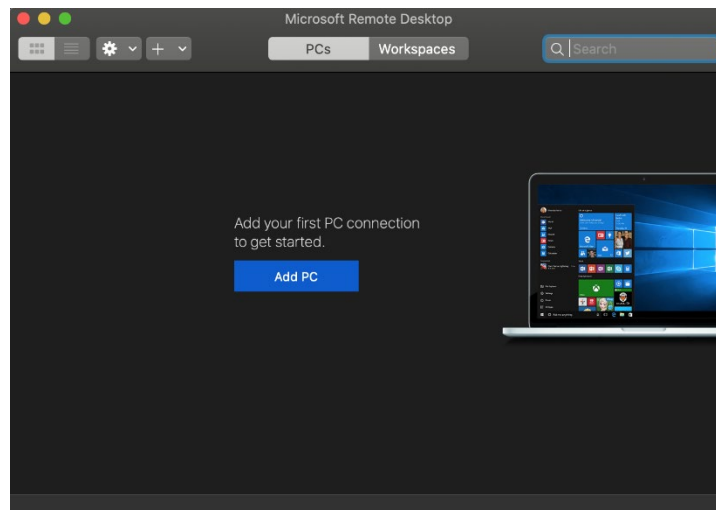
Username:

Password:

Two-Step Verification Code:

Type "push" into the two-step field to receive a push to your Duo Mobile app.

2. Check the status of the lab computers at <https://eps.harvard.edu/icf-computer-status> (note that the computer images are not links). Computers shown in green are available for use. Computers shown in blue or gray are currently unavailable. Identify an available computer and take note of the workstation name (e.g. EPS-103C-10).
3. Download the Microsoft Remote Desktop app using the link below and then open the app. <https://apps.apple.com/us/app/microsoft-remote-desktop/id1295203466?mt=12>. Please note you will need to know your devices Apple ID and password to complete the installation.
4. When in Microsoft Remote Desktop, select 'Add PC'.



- In the dialog box, type the name of the computer you wish to connect to (from the available computers shown on <https://eps.harvard.edu/icf-computer-status>) as the computer name, followed by ad.fas.harvard.edu. For example, if you choose to use EPS-103C-10, type **EPS-103C-10.ad.fas.harvard.edu** for the name of the computer.

**Add PC**

PC name:

User account:

**General** | Display | Devices & Audio | Folders

Friendly name:

Group:

Gateway:

Bypass for local addresses

Reconnect if the connection is dropped

Connect to an admin session

Swap mouse buttons

- Click the dropdown arrow next to 'User account:' and 'Add User Account...' Enter your username as your "**University\yourNetID**", replacing **yourNetID** with your 3 letter, 3 number Harvard NetID. Note the **backslash** between University and yournetid. To find your Harvard NetID, follow the instructions in the following knowledge article (KB0015034): [https://harvard.servicenow.com/ithelp?id=kb\\_article&sys\\_id=507aca5a1b653700efd8a79b2d4bcb59](https://harvard.servicenow.com/ithelp?id=kb_article&sys_id=507aca5a1b653700efd8a79b2d4bcb59). (Or go to Harvard Key website, Manage Your Account & Services, and your NetID will be under the account information.)

Leave 'Password:' field blank. Click 'Add' to add the User Account. And then click 'Add' to add the PC.

**Add a User Account**

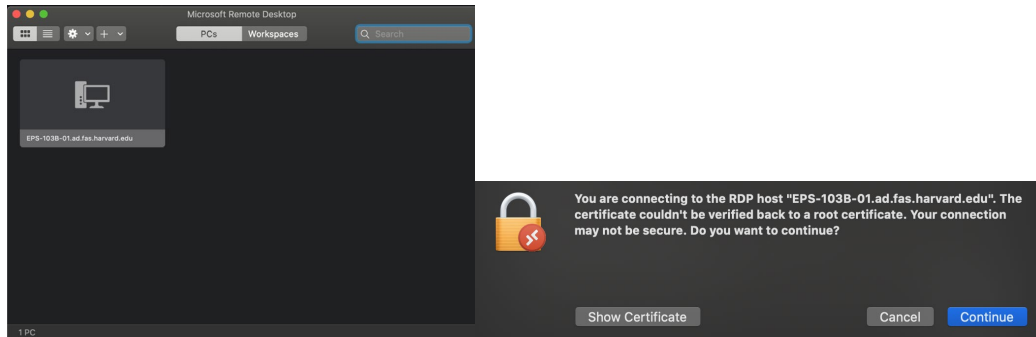
Username:

Password:

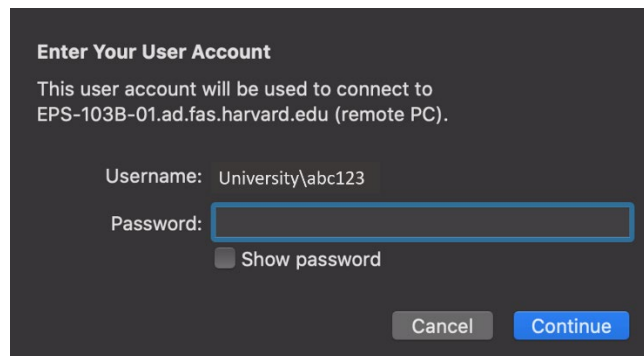
Show password

Friendly name:

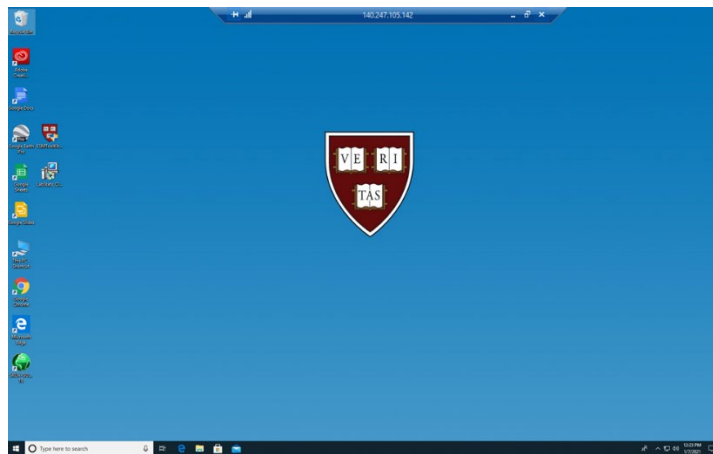
- Now the PC you have just added will appear in Microsoft Remote Desktop. Double click the PC. You may receive an error message about a secure connection. To prevent this message in the future, click the "Show Certificate" button, then select the "do not prompt..." checkbox. Click Continue.



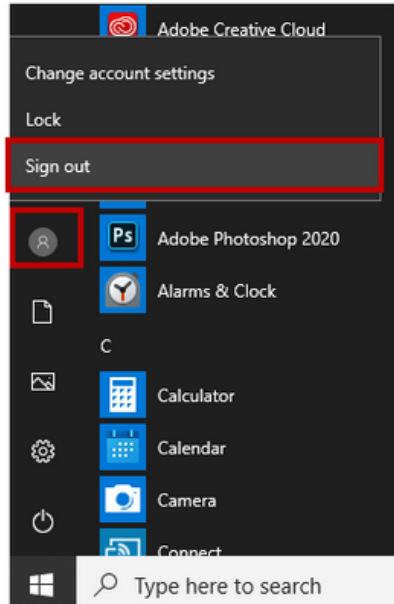
- Enter your Harvard Key password and click Continue.



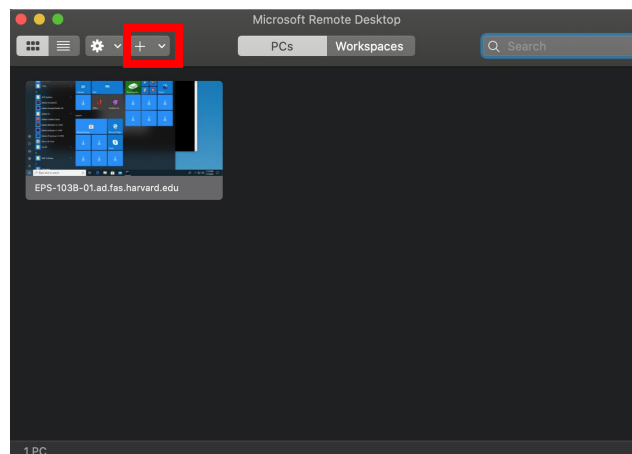
- Your screen should show the remote computer desktop, as below.



- IMPORTANT:** When you are done, please log out of the remote desktop session by clicking on the Windows start icon and then the person icon, then "Sign out." This will log you off from the machine and is important to make sure the computer is available for other students



11. After signing out, the machine you just connected to will appear in the Microsoft Remote Desktop. To reconnect to this machine, just double click and re-enter your password. To connect to a different machine, click the + in the top left, and 'Add PC'.



## Notes about remote sessions:

- Security updates may be installed on Saturdays between 2am and 5am. Users may be requested to reboot the computer at that time.
- Remote use of university computers is subject to the same guidelines and policies as on campus use.
- Active sessions are limited to 6 hours. If you need to continue, please end your session and begin a new one.
- After one idle hour (no use of the remote machine), your session will be ended automatically. (Codes running in the background are considered active use.)