UCMC Tip Sheet for Accessing IT Applications Remotely

Access to the UCMC network and resources must be done through the established channels outlined in this tip sheet. Use of personal devices are **not** permitted except as outlined within this document or otherwise explicitly authorized by IT.

Remote Access Policy Reminder

General Remote Access

- Users must enroll in 2Factor authentication
- No printing at home
- No saving files or data locally on personal computers (such as laptops or desktops)
- UCM email must be used for all email communications
- Access to the UCM VPN should be conducted with a UCM managed device
- Access to third party applications (such as the Cloud) should be conducted through the UCMC WebApps/Citrix system
    - Note: this is to prevent the accidental storage of data on a personal device
- For telecommuting and video conferencing, use Zoom
    - Use only BSD, UCM or Ingalls credentials for Zoom, **do not use or create any other personal or free profile on Zoom for business purposes.**
    - The only instances that **UCM users should be using** to host a meeting are:
        - **BSD or UCM : uchicagomedicine.zoom.us**
        - **Ingalls : ucmedicinegroup.zoom.us**
    - **Use of text messaging between mobile devices to discuss any PHI is not permitted**.
- For instant messaging needs, use Zoom's Chat feature
- If your electronic device is lost or stolen, or if you have any other use or incident outside of these guidelines, notify the Privacy Program as soon as possible at 773-834-9716 or hpo@bsd.uchicago.edu

Personal Devices

Devices that are not purchased and/or managed by UCMC can only be used in specific limited ways. This policy is in place to limit the spread of confidential information into unprotected and unmanaged devices, as well as protecting the health of the UCMC network and information systems.

- Consult the Personal Computing Device policy , and follow the specific instructions outlined within this Tip Sheet
- Access to UCMC resources should be done through the UCM WebApps/Citrix system.
    - Note: The only permitted use of personal desktops and laptops is to UCM WebApps/Citrix
- Use of personal mobile devices (tablet or smartphone) is permitted only when configured according to this tip sheet

- You are permitted to forward your UCMC desk phone to your personal phone in order to continue to receive calls from your main number.
    - Note: any calls made out from your personal phone will not be run through the UCMC phone system. Your personal phone number will be exposed.

Technology Configuration Guidance

2Factor Authentication

The 2nd factor that you will enroll will be your smartphone or tablet. You will need to download the DUO Mobile Application on your mobile device. When logging into a system protected by 2Factor Authentication you will be asked to ACCEPT the login from this DUO Mobile Application. As such you will need your mobile device with you when accessing your accounts remotely.

1. Navigate to https://2fa.uchicago.edu
2. Click on Go to Two-Factor
3. Sign in with your UCHAD/CNETID credentials
4. Enroll your device, following the instructions outlined

Accessing UCMC Resources Remotely from Home from a Personal Device

All users should leverage the UCM WebApps system to conduct your normal work. To access this system follow the below instructions.

1. Log into WebApps
    a. You will need Citrix installed on your personal laptop or desktop. Instructions on how to install Citrix can be found on the UCM IT Intranet site.
    b. On your personal laptop/desktop go to the following email address: https://www.uchicagomedicine.org/
    c. Scroll down to Employee Login (last section of the page on the lower right)
    d. Click on Employee Login then click on Intranet and UCM Applications
    e. Enter your employee credentials
    f. If you have not set up 2 Factor Authentication, set it up. Link for set up is right above employee login credentials

2. Once logged in on the Citrix homepage, determine whether you have access to all your applications needed to successfully complete your work function

3. If there are missing applications on the Citrix homepage, contact the help desk 23456 to see if they can add the application

Mobile Devices - Email

Employees may use their personal mobile devices (smartphones or tablets) to access their UCMC email **only** if the following instructions have been followed.

1. Encrypt your device:
    a. If you have an Apple device, ensure your phone has a passcode or password; no further actions are needed
    b. If you have an Android device, you need to take the following actions:
        i. Ensure that your password is enabled
        ii. Go to the Security screen by opening the Settings screen -> Security
        iii. Tap the "Encrypt Phone" to start the encryption process. Be cognizant of the warning!
        iv. Enter your PIN in order to start the encryption process. *Do not interrupt the phone while it is encrypting.* You will see a progress indicator as the encryption process starts. Once the indicator completes your mobile phone will be encrypted.
2. Connect your device to the email system by following the instructions on the UCM IT Intranet Site

Accessing Cloud/Remote Hosted Applications

In order to access your remote applications, as you normally would from a UCMC device on the UCMC network, you will first need to log in to the UCMC WebApps system. Please conduct all your third party/cloud access work from within the WebApps/Citrix system in order to protect the security of our sensitive data.

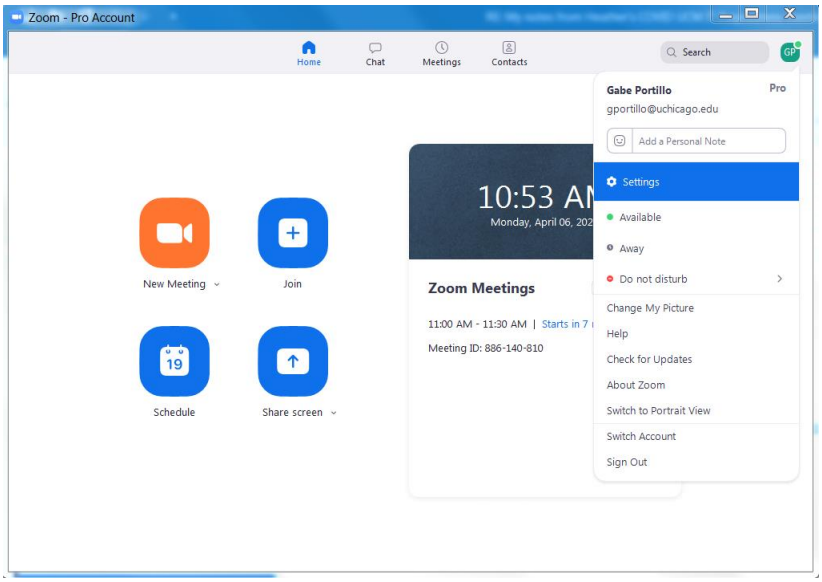
You might need to copy commonly used URLs into a text file and store this on your U: drive so it can be accessible via the WebApps/Citrix system.

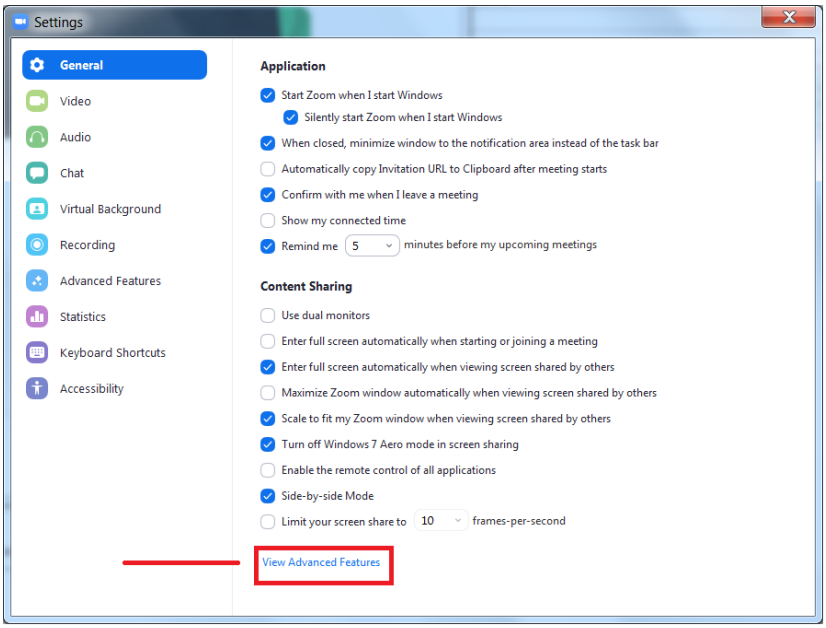
Zoom

UCM uses the Zoom teleconferencing cloud service to host virtual voice and video meetings. This service is provided by the University of Chicago ITS department. Details on access can be found here: https://its.uchicago.edu/web-conferencing/

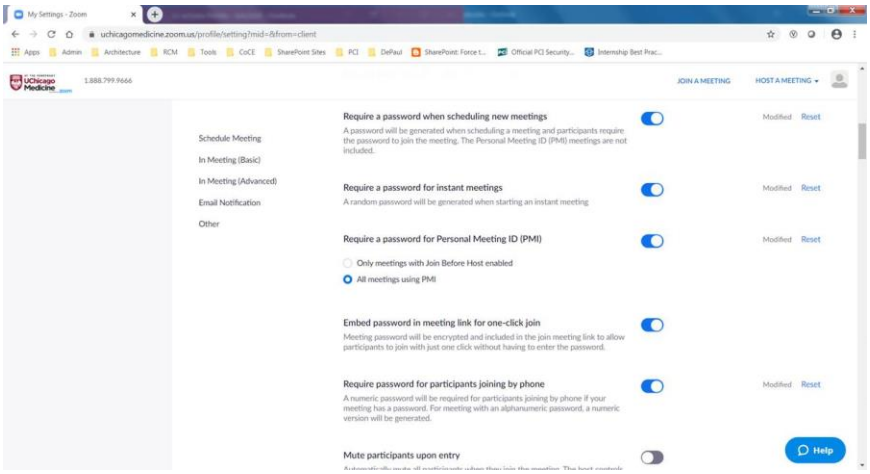
Password configuration for managing meetings

In order to modify the meetings with requirement of passwords please adjust the settings. You will be able to do this by accessing the advance settings in the zoom application:

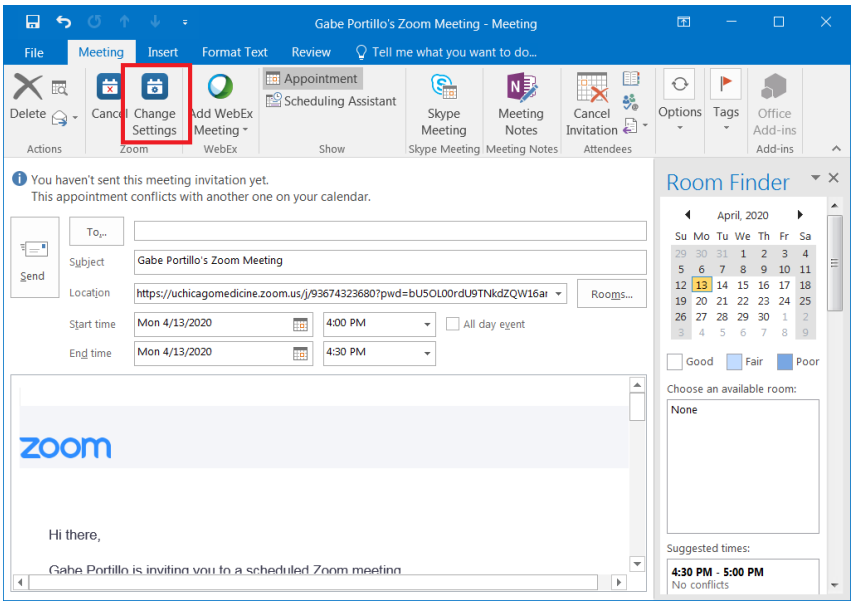


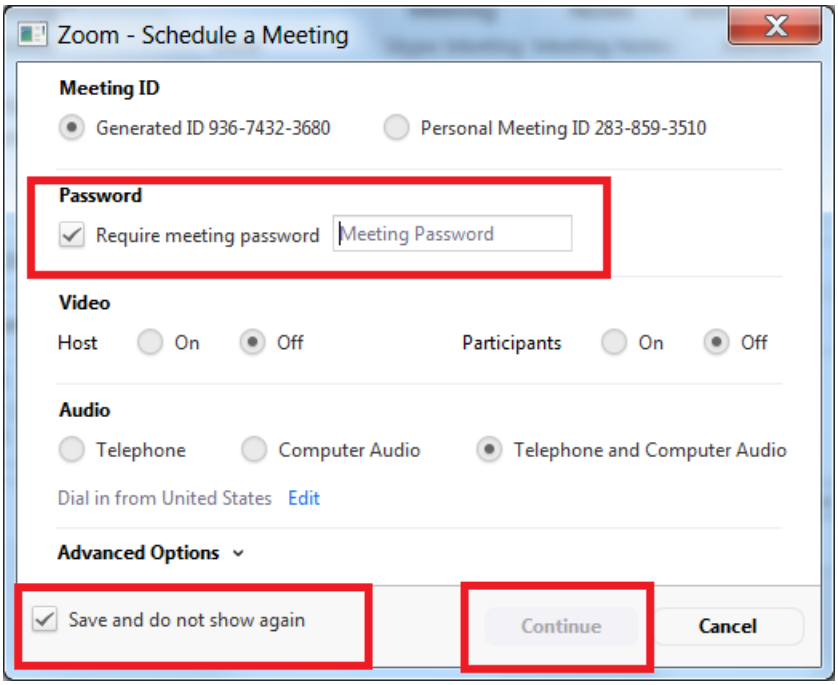


After logging in using BSD, UCM, or Ingalls credentials, select all options for password requirements under Schedule Meeting:



If you are leveraging the client Outlook Zoom Plug in, for any meeting that is in need of a password, the setting here will require updating, the password should auto generate based on profile default settings:





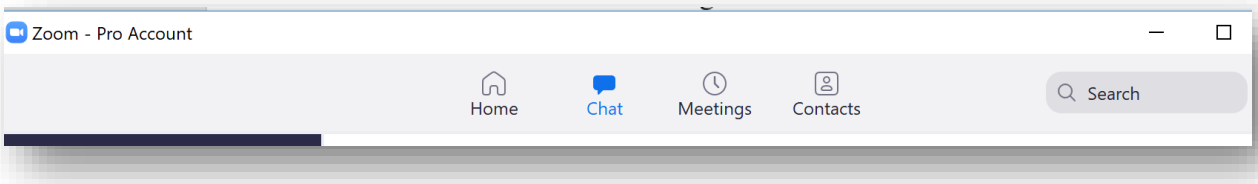
If you have an existing meeting that does not have a password, but need to include it in your link, you will need to remove the original Zoom link and replace it with a new one in an update to an invite. If that does not work well, cancel your current meeting and reschedule a new one.

Zoom Chat

Zoom also contains an instant messaging feature that can be used outside of the Zoom teleconferencing meetings. This feature requires the Zoom agent to be installed on your computer, which will be installed when you run a Zoom meeting. These messages are encrypted and secured and can be used to confidential communications.

To access the Chat feature, do the following:

1. Launch the Zoom client; it should say “Zoom – Pro Account” in the upper left hand corner
2. At the top ribbon select “Chat”
3. Within the Search feature, type in the name of the person you wish to chat with (make sure to confirm the spelling and person before sending a message)
4. Message accordingly



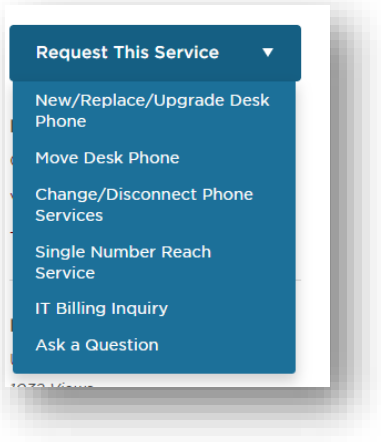
Receiving Phone Calls from your UCMC Phone Number

You have multiple options available to you for receiving phone calls on separate phones other than your provisioned UCMC Phone. You may either 1) Forward your phone to a separate phone number or 2) Set up your phone number to ring on multiple devices

Forwarding Phone

To forward your phone you can set your phone to forward to an outside number you'll have to contact UChicago ITS and put in a request to have the number forwarded over.

1. To submit a request, go to UChicago ITS' ServiceNow system and submit a ticket here: https://uchicago.service-now.com/it?id=its_sc_cat_item&sys_id=7e74c888139cb60027255eff3244b0e0
2. Select "Change/Disconnect Phone Services"



Ring on Multiple Devices

You also have the option of allowing your UCMC phone number to ring at your desk as well as other devices (such as a cell phone or home land line), or ring your UCMC desk phone first and then a secondary phone.

1. To set this feature up, submit a request to UChicago ITS using this specific link, defined as "Single Number Reach Service": https://uchicago.service-now.com/it?id=its_sc_cat_item_request&sys_id=c9ec72191352e20030c0bcaf3244b069

Accessing Voicemail Remotely

To access to your voicemail from offsite, follow these instructions:
https://knowledgebase.uchicago.edu/images/group68/19600/7965.pdf