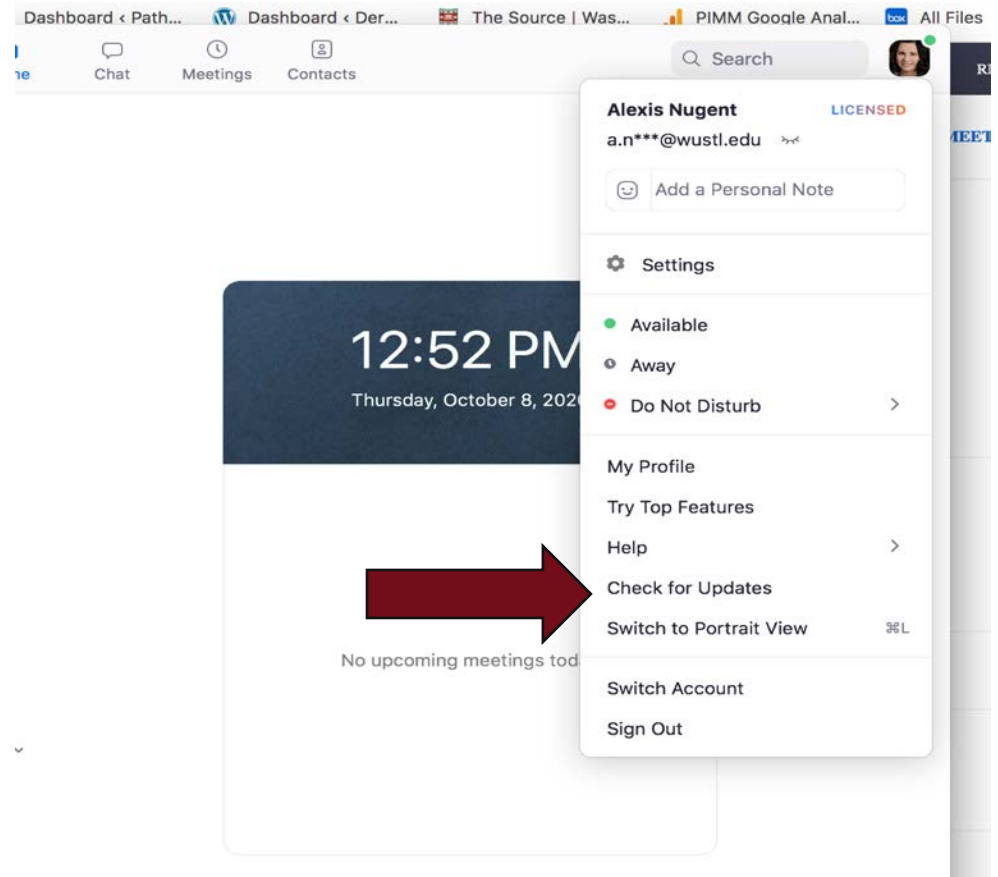


Zoom Security Tips

Department of Pathology & Immunology

Install Latest Version of Zoom or Update

- Go to your profile picture in the Zoom desktop client and click on it.
- A drop down list will appear, click on Check for Updates.



Screen Sharing Defaulted to Host Only

- As a precaution it is best to only have the host screen sharing enabled. This can be achieved in the settings section of the Zoom desktop client or in the meeting itself.
- If someone besides the host needs to screen share, they can be elevated to co-host so they can share as well, even during a meeting. Settings can be found in the Zoom desktop client as well as the live environment.

Screen sharing

Allow host and participants to share their screen or content during meetings



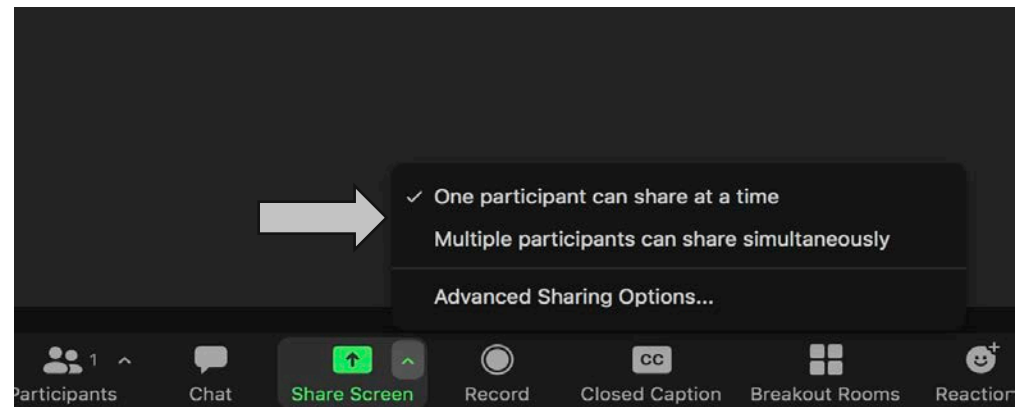
Who can share?

Host Only All Participants 



Who can start sharing when someone else is sharing?

Host Only All Participants 



Require Meeting Passcode Defaulted On

- This setting helps protect against unauthorized entries.
- There is also a setting within Zoom that will embed the encrypted passcode in the invite link to allow participants to join with just one click without having to enter the passcode. Settings can be found in the Zoom desktop client.

Require a passcode when scheduling new meetings

A passcode will be generated when scheduling a meeting and participants require the passcode to join the meeting. The Personal Meeting ID (PMI) meetings are not included.



Require a passcode for instant meetings

A random passcode will be generated when starting an instant meeting



Require a passcode for Personal Meeting ID (PMI)



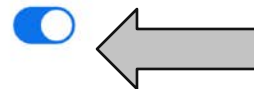
Require passcode for participants joining by phone

A numeric passcode will be required for participants joining by phone if your meeting has a passcode. For meeting with an alphanumeric passcode, a numeric version will be generated.



Embed passcode in invite link for one-click join


Meeting passcode will be encrypted and included in the invite link to allow participants to join with just one click without having to enter the passcode.



Personal Meeting ID Defaulted to Off

- Keep the Use Personal ID defaulted to off is best practice to ensure your meeting is secure. Using these IDs can be a key entry point for unwanted guests in Zoom meetings. The setting is found in the Settings on the Zoom desktop client

Enable Personal Meeting ID

A Personal Meeting ID (PMI) is a 9 to 11 digit number that is assigned to your account. You can visit [Personal Meeting Room](#) to change your personal meeting settings. [Learn more](#) 



Use Personal Meeting ID (PMI) when scheduling a meeting

You can visit [Personal Meeting Room](#) to change your Personal Meeting settings.



Use Personal Meeting ID (PMI) when starting an instant meeting



Waiting Room Zoom Feature

- This feature allows the host to keep those who sign into the meeting in a virtual room until the meeting is ready to start. The setting is found in the Settings on the Zoom desktop client.
- The host can either manually admit each person in or admit an entire group. There are also options that allow you to control whether everyone waits in the room, users that are not a WashU account or users who are not part of the WashU account and not part of our allowed domains.

Waiting Room

When participants join a meeting, place them in a waiting room and require the host to admit them individually. Enabling the waiting room automatically disables the setting for allowing participants to join before host.



Waiting Room Options

The options you select here apply to meetings hosted by users who turned 'Waiting Room' on

✓ Everyone will go in the waiting room

[Edit Options](#) [Customize Waiting Room](#)

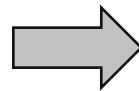


Waiting Room Options

These options will apply to all meetings that have a Waiting Room, including standard meetings, PMI meetings, webinars.

Who should go in the waiting room?

- Everyone
- Users not in your account
- Users who are not in your account and not part of the allowed domains

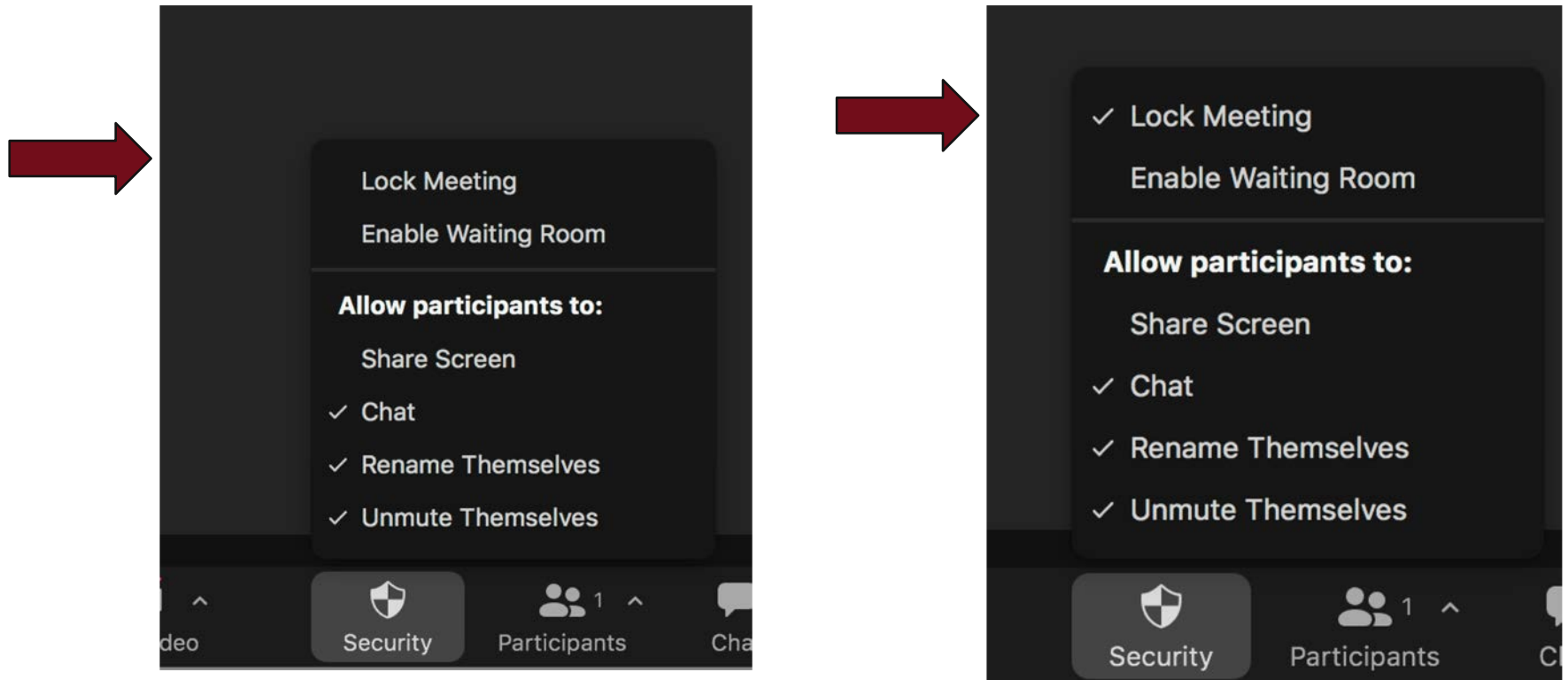


Continue

Cancel

Locking a Meeting After Start

- Once your meeting has begun, click Security at the bottom of your Zoom window. In the pop-up list, you will see a button that says Lock Meeting.
- When this feature is enabled no one will be able to enter the meeting so ensure everyone has joined before clicking on this setting. This setting is available in the live meeting view.



Mute Participants Upon Meeting Entry

- Zoom allows the host to mute audio and video for participants joining a meeting. These settings can be found in the Zoom desktop client.

Schedule Meeting

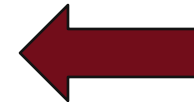
Host video

Start meetings with host video on



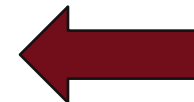
Participants video

Start meetings with participant video on. Participants can change this during the meeting.



Mute participants upon entry

Automatically mute all participants when they join the meeting. The host controls whether participants can unmute themselves.



Disable Join Before Host

- If you are scheduling a meeting where sensitive information will be discussed, the recommendation is to turn off join before host.
- The join before host option can be convenient for allowing others to continue with a meeting if you are not available to start the meeting, but with this option enabled, the first person who joins the meeting will automatically be made the host and will have full control over the meeting. If you know you won't be able to start the meeting, you can designate an alternate host who can start the meeting.
- The setting is found in the Settings on the Zoom desktop client.

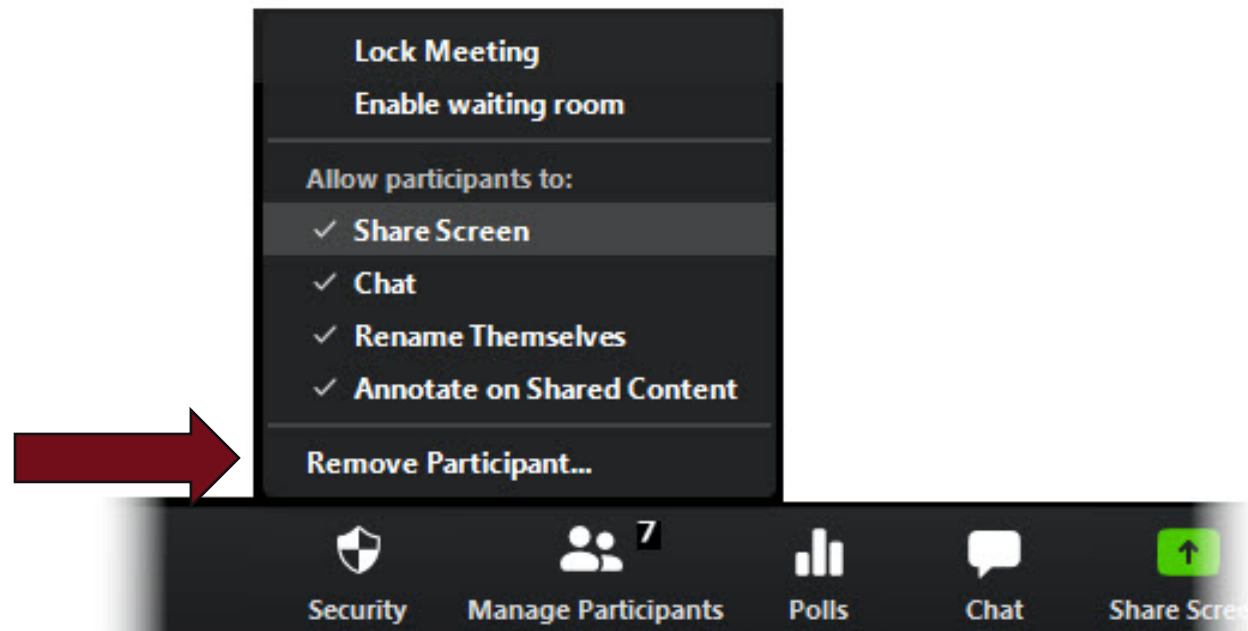
Join before host

Allow participants to join the meeting before the host arrives



Removing Disruptive Participants

- If someone does become disruptive during a meeting you can remove them from the meeting using the Security button at the bottom of the meeting screen.
- Please note that if you do remove a participant they will not be allowed back into the meeting.
- This setting is available in the live meeting view.



Other Helpful Zoom Tips & Resources

- Keep links to all Zoom meetings private. This will prevent unwanted participants. Do not share Zoom meeting links on public websites or on social media channels.
- Don't put zoom information in calendar invites, send the link to the Zoom meeting a day or two prior to the event to all attendees.
- Additional resources for Zoom can be found at <https://wustl.zoom.us/>.
- Many of the department assistants are available to help you with Zoom questions or concerns.