CUYAMACA · COLLEGE ·

SAFELY SETTING UP ZOOM MEETINGS / EVENTS

1. Avoid sharing your meeting links publicly. Instead, schedule a meeting or event that requires participants to register with their name and email address.

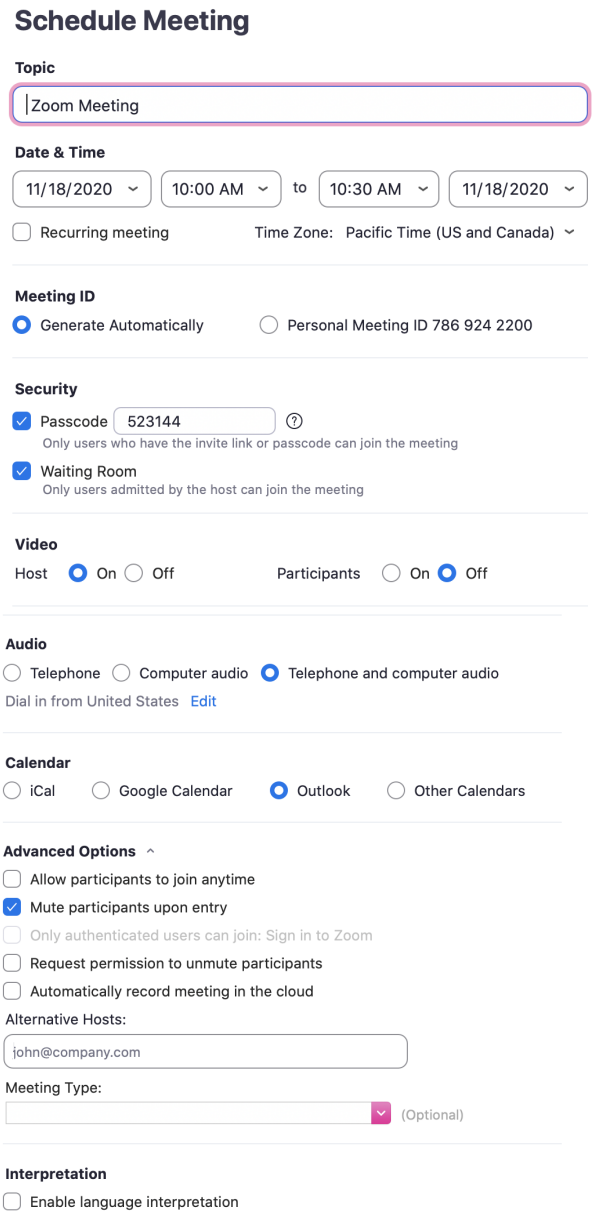
2. For added security, require a password that participants must enter before being allowed into a meeting.

3. For public meetings and events, NEVER use your Personal Meeting ID (PMI). Your PMI is set up as one continuous meeting, once someone has a link to your PMI they can enter it any time. Always set up public meetings/events using random meeting IDs.

4. Enable a Waiting Room so you have control over who can enter your meeting. The Waiting Room feature gives hosts greater control over session security.

5. Additionally, do not allow others to join a meeting before you, as the host, have arrived. You can enforce this setting for a group under "Account Settings."

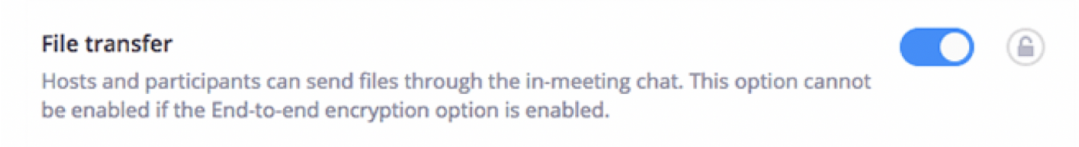
6. Mute participants upon entry. Having attendees muted as they join will reduce ambient noise and minimize disruption.



SAFETY TIPS DURING ZOOM MEETINGS / EVENTS

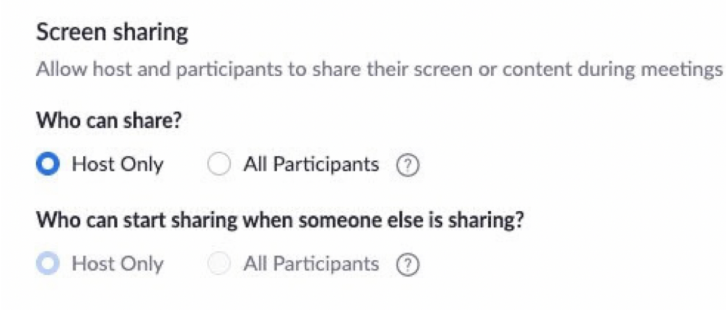
USING CHAT SAFELY

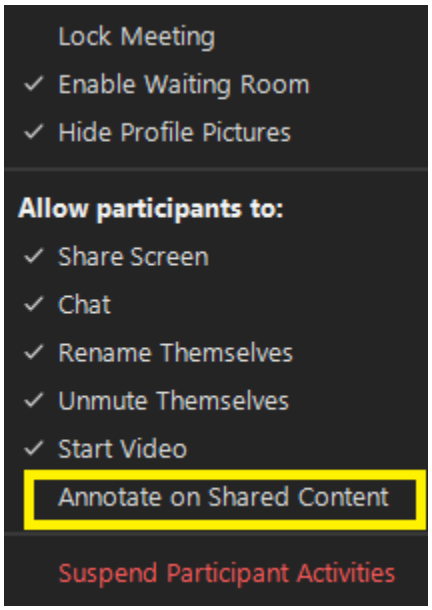
The chat feature allows varying levels of safety, and they can all be changed during the meeting if you need to make adjustments. For events with external (non-Cuyamaca) attendees, it is recommended all chat functions are disabled. Additionally, the file transfer option should be disabled. In addition to the unwanted sharing of information, malware can be shared via a Zoom file transfer.



ENABLE SCREEN SHARE FOR "HOST ONLY"

Preventing others from screen sharing will secure your meeting from unwanted and disruptive visuals, videos, etc. Attendees may request permission to share screen, and it can be granted during a meeting, only trusted attendees should be granted this access.





Know that when you grant screen sharing privileges, you automatically enable the annotation function. The annotation function allows another user to "write/type" on a shared screen. As soon as you screen share, click the "Security" shield button and ensure the "Annotate on Shared Content" is disabled!

MULTIPLE CO-HOSTS

Use a Co-Host or an Alternative Host to help monitor activity during your meeting. Co-host and/or Alternative Hosts should have responsibilities as the meeting/event begins. Some of those responsibilities may include:

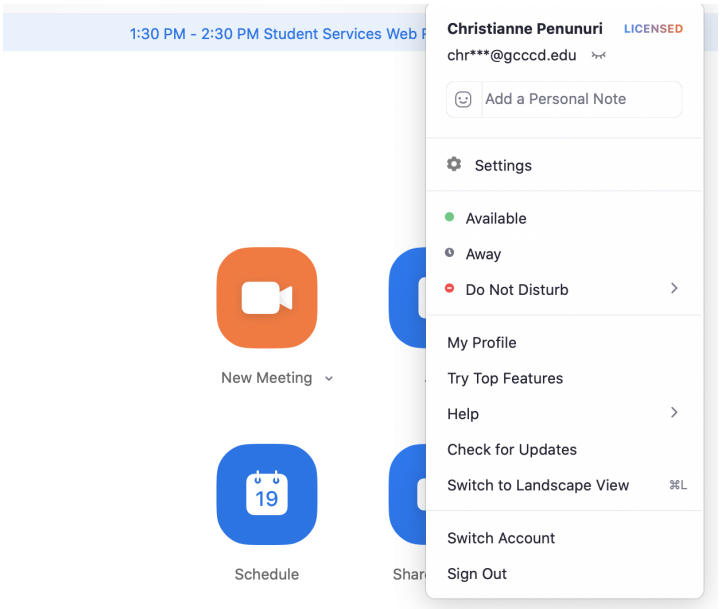
1. Disable video
2. Monitor the chat

3. Check for disruptive images/video /virtual background

PREPARING YOURSELF FOR ZOOM MEETINGS/EVENTS

CHECK FOR UPDATES

Ensure your settings are updated. Zoom deploys patches and augments functionality to best meet the needs of users based upon their feedback. In your desktop profile, click in the upper right corner, and select “Check for updates.”



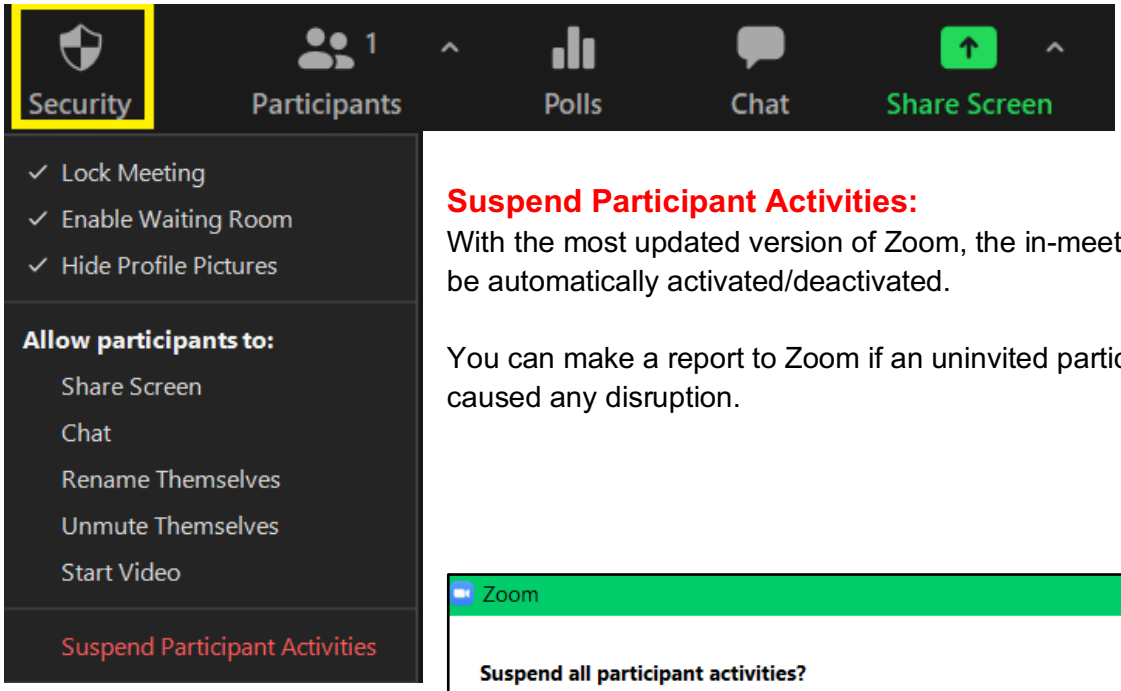
ADD YOUR NAME TO YOUR PHONE

If you need to call into a meeting/event from your phone, make sure your name is listed and not just your phone number.

IN CASE OF EMERGENCY

Should you need to remove someone from your meeting. Follow these steps:

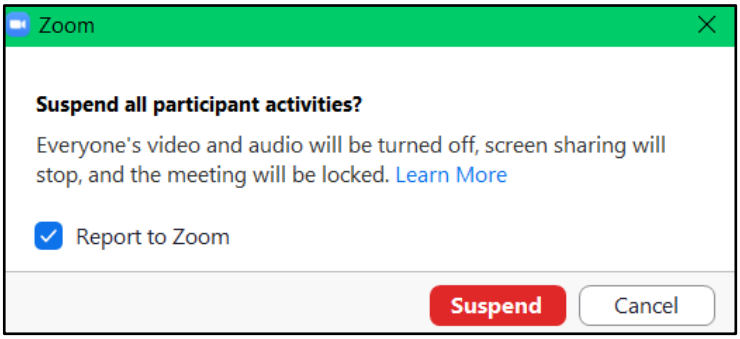
- Click the “Security” shield to ensure that your in-meeting securities are set for your meeting’s purpose. These in-meeting features can be activated/deactivated at any time during the meeting.
- In-meeting security options (below)

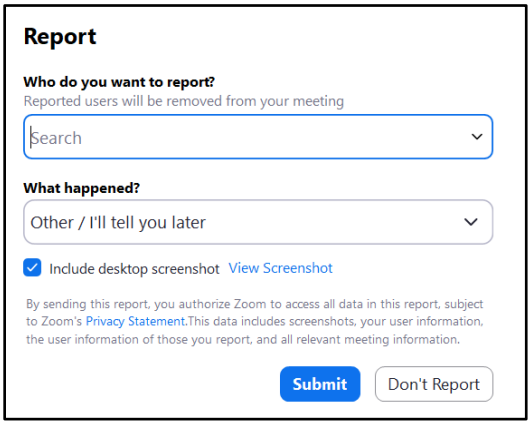


Suspend Participant Activities:

With the most updated version of Zoom, the in-meeting features will be automatically activated/deactivated.

You can make a report to Zoom if an uninvited participant(s) has caused any disruption.




Report
Who do you want to report?
Reported users will be removed from your meeting
Search
What happened?
Other / I'll tell you later
Include desktop screenshot
View Screenshot
By sending this report, you authorize Zoom to access all data in this report, subject to Zoom's Privacy Statement.This data includes screenshots, your user information, the user information of those you report, and all relevant meeting information.
Submit
Don't Report