# Zoom Security Protocol

## Information Security Application Note

## Introduction

The following Zoom security protocols/practices are required for campuses, programs, academic departments, offices, faculty or staff that have or use a license to Zoom for any CUNY related activities.

Please note that CUNY does not have an enterprise-wide license for this service. If you wish to use Zoom, check with your campus IT department to be sure that your campus has a license for its use.

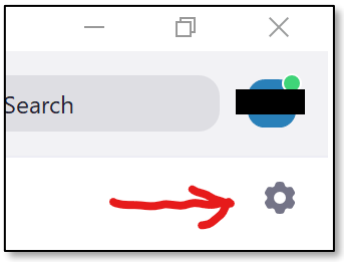
The following chart summarizes security protocol requirements and recommendations when using Zoom:

| Protocol | Required | Recommended |
|---|---|---|
| **Don't publicize Zoom classroom meetings on social media or public forums** | ✓ | |
| **Set a password for all meetings** | ✓ | |
| **Turn off file transfer** | ✓ | |
| **Keep the Zoom application updated to the most recent version** | ✓ | |
| **Don't use a Personal Meeting ID (PMI) to host a classroom or large event meeting** | ✓ | |
| **Disable private chat** | ✓ | |
| **Allow chat with host only** | | ✓ |
| **Set "Screen Sharing" to "Host Only"** | | ✓ |
| **"Lock Meeting" after all participants have joined** | | ✓ |
| **Turn off annotation when not needed** | | ✓ |
| **Use "Waiting Room"** | | ✓ |

## Follow these Practices for Using Zoom Securely

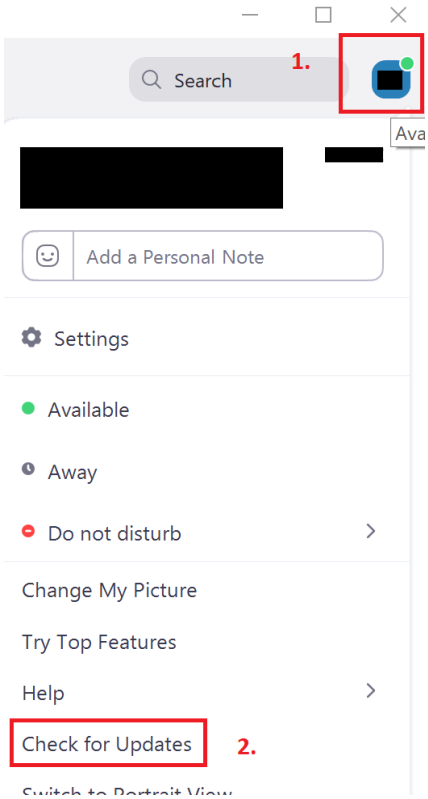
- DON'T share your meeting link on social media or other public forums. Doing that can publicize your meeting to potential abusers, as without additional measures, anyone with the link can join your meeting.
- DON'T use your Personal Meeting ID (PMI) to host public events. Your PMI is basically one continuous meeting that outsiders can abuse. Learn about meeting IDs and how to generate a random meeting ID (at the 0:27 mark) in this video tutorial.
- DO set a password for all meetings.

- DO familiarize yourself with Zoom's settings and features so you understand how to protect your virtual space. For example, the Waiting Room is a helpful feature for hosts to control who comes and goes. You can access Zoom settings within the desktop application by clicking on the "gear" icon located near the upper-right of the Zoom window.




Additional settings for your Zoom account are accessed through the Zoom website.

- DO keep the Zoom desktop application updated to the most recent version and encourage meeting participants to do the same. Choose "Check for Updates" after clicking on the user icon within the application.

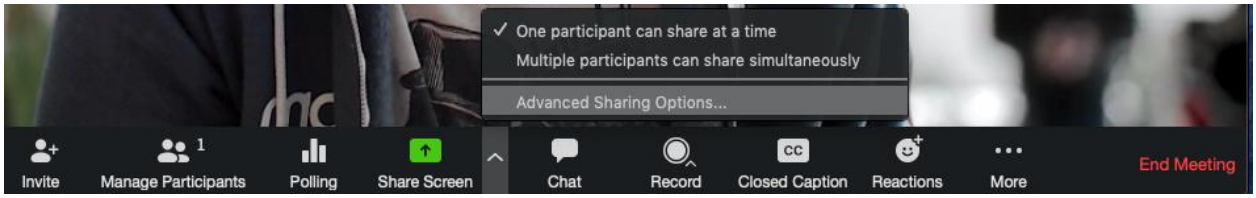


# Manage Screen Sharing

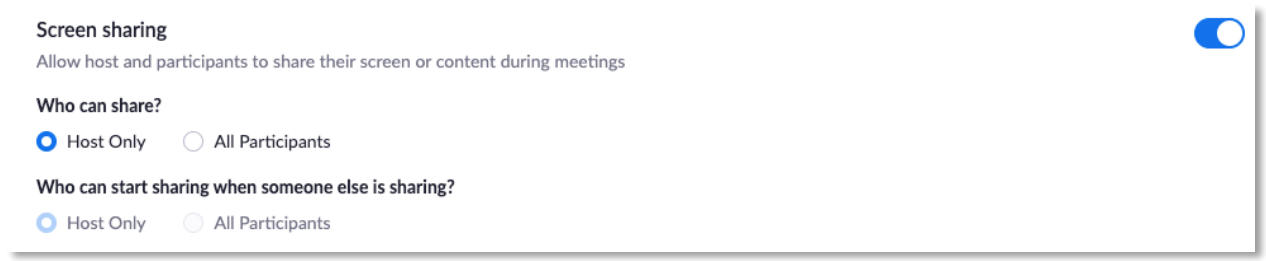
You **DO NOT** want random people taking control of the screen and sharing unwanted content with the group. You can restrict this—before the meeting and during the meeting in the host control bar—so that you as the meeting host are the only one who can screen-share.

To prevent participants from screen sharing during a call:

1. Using the host controls at the bottom, click the arrow next to Share Screen and then Advanced Sharing Options.




2. Under “Who can share?” choose “Only Host” and close the window. You can also lock the Screen Share by default for all your meetings in your web settings.




# Manage Your Meeting Participants

Some other features to help secure your Zoom event and host with confidence include:

**Lock the meeting**

It’s always smart to lock your front door, even when you’re inside the house. When you lock a Zoom Meeting that’s already started, no new participants can join, even if they have the meeting ID and password (if you have required one). In the meeting, click Participants at the bottom of your Zoom window. In the Participants pop-up, click the button that says Lock Meeting.

**Remove unwanted or disruptive participants**

From the Participants menu, you can mouse over a participant’s name, and several options will appear, including Remove. Click that to kick someone out of the meeting.

**Put participants on hold**

You can put everyone else on hold, and the attendees' video and audio connections will be disabled momentarily. Click on someone's video thumbnail and select Start Attendee On Hold to activate this feature. Click Take Off Hold in the Participants list when you're ready to have them back.

**Disable video**

Hosts can turn someone's video off. This will allow hosts to block unwanted, distracting, or inappropriate gestures on video.

**Mute participants**

Hosts can mute/unmute individual participants or all of them at once. Hosts can block unwanted, distracting, or inappropriate noise from other participants. You can also enable Mute Upon Entry in your settings to keep clamor at bay in large meetings.

**Turn off file transfer**

In-meeting file transfer allows people to share files through the in-meeting chat. Toggle this off to keep unsolicited pics, GIFs, memes, and other content off the chat.

**Turn off annotation**

You and your attendees can doodle and mark up content together using annotations during screen share. You can disable the annotation feature in your Zoom settings to prevent people from writing all over the screens.

**Control chat access**

Zoom has in-meeting chat for everyone or participants can message each other privately. Restrict participants' ability to chat amongst one another while your event is going on and cut back on distractions or limit chat with the host only. This prevents anyone from getting unwanted messages during the meeting.

# Use the Waiting Room Feature

The Waiting Room is a virtual staging area that stops participants from joining until they are admitted by the meeting host.

Meeting hosts can customize Waiting Room settings for additional control, and personalize the message people see when they hit the Waiting Room so they know they're in the right spot. This message is also useful for posting any rules/guidelines for your meeting, like for whom it's intended.