LACCD Guidance for Safe Hosting Of Zoom Video Conferences

BACKGROUND

The Los Angeles Community College District (LACCD) has implemented Zoom video conferencing, provided by the California Community College Chancellor's (CCC) Office, to assist in the District's online instructional efforts. Due in part to Zoom's wide-spread use in education environments, security issues arising from classroom disruptions (i.e. "ZoomBombing") have caused concern. Zoom has recently updated its' default security settings to greatly reduce the opportunity for malicious users to disrupt Zoom classes, and provides a number of additional security features to enhance the security of Zoom meetings.

This document provides guidance on utilizing Zoom's built-in security features to provide a safe and secure virtual meeting environment for LACCD.

GENERAL GUIDELINES

When hosting Zoom virtual meetings or class discussions, LACCD faculty and staff are encouraged to:

1. Understand Zoom Default Security Settings
2. Consider Additional Security Settings
3. Actively Manage Zoom Meetings
4. Report Incidents to the LACCD Information Security Office

Detailed instructions for each of these guidelines are provided below.

Understand Zoom Default Security Settings

When an LACCD employee creates a Zoom account on the LACCD platform https://laccd.zoom.us, Zoom implements several security features by default. Do not disable these features without a thorough understanding of why they are disabled, and the consequences of disabling them:

Password protect meetings: By default, Zoom establishes a new password for each meeting an LACCD user creates. Do not turn off this feature.

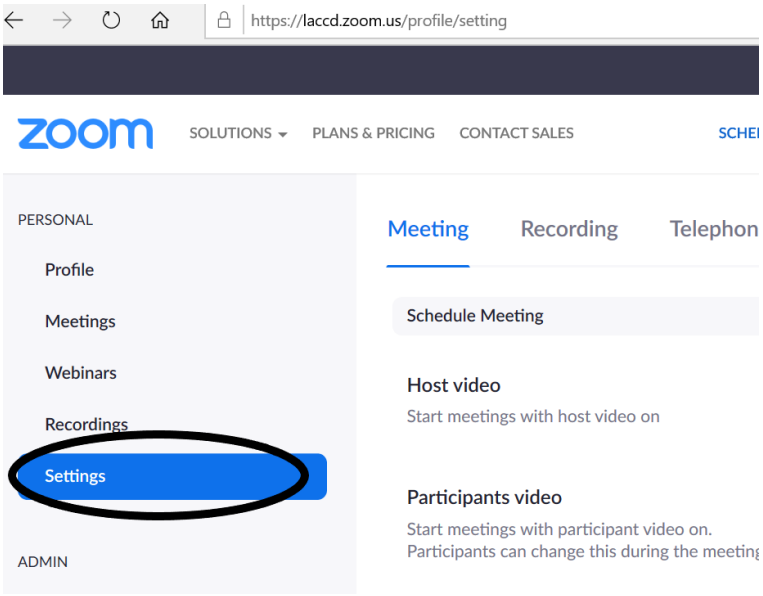
Use a waiting room: Zoom creates a "waiting room" when an LACCD user creates a Zoom session. The meeting creator (or meeting "host") can select individuals to admit to the meeting from the waiting room, or enable all users as a group. Once the meeting has started, if a new attendee comes late, the host will receive a pop-up window asking if they want to admit or deny access to the latecomer.

Disable Screen Sharing: Zoom disables screen sharing by default, so only the host can share content on the screen. Do not enable screen sharing until you need to invite a specific user to share their screen.

Do not post meeting information: Zoom meetings can be set up through Canvas, or a Zoom host can send invitations via email. Do not post meeting information (time, date, meeting ID or password) on social media sites, websites, etc. Where required, send email invitations to individual people; do not email distribution lists or email accounts with generic names.

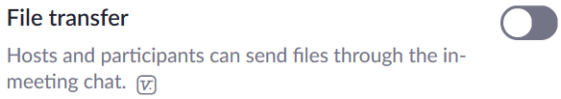
Consider Additional Security Settings

LACCD Zoom users may add additional security settings by default to any meeting they create by logging into t=https://laccd.zoom.us, and clicking "Settings" in the left menu under their "PERSONAL":

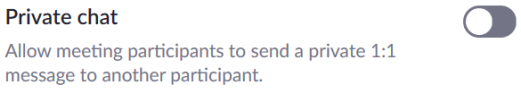


The Information Security Office recommends that all LACCD users ALWAYS change the following default settings:

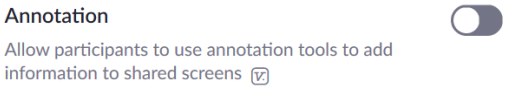
Disable "file transfer": Malicious files can potentially be sent purposefully or inadvertently via file transfer. Disable this capability for all meetings.



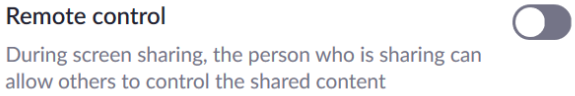
Disable "Private chat": Assuring all conversations are public to the entire meeting reduces the opportunity for bullying or harassment. Disable it for all meetings; it can be re-enabled during the meeting if it is absolutely required.



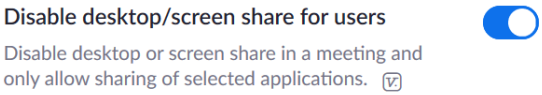
Disable "annotation": Annotation allows a user to write on the screen of the presenter. Disable it at all times to prevent this feature from being abused.



Disable "remote control": Remote control is potentially appropriate for one-on-one support sessions, but is generally inadvisable for group meetings.

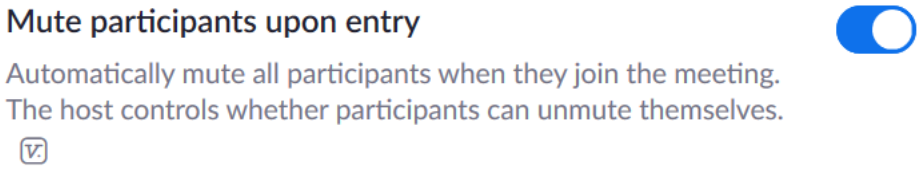


Enable "Disable desktop/screen share for users": This setting requires a user to share specific applications (i.e. PowerPoint, Chrome, etc.) rather than their entire desktop. Disabling desktop sharing reduces the possibility that inappropriate or private materials are displayed during screen sharing.

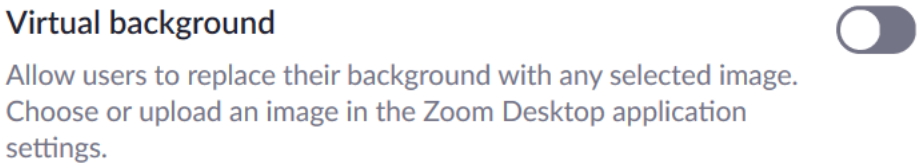


In addition to the settings changes described above, the LACCD Information Security Office also recommends that LACCD users consider the following additional settings where prudent:

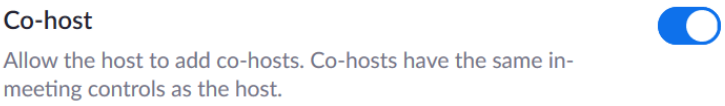
Enable" Mute participants upon entry": This disables participants ability to speak until the host enables it. While a host may consider it desirable to let attendees "mingle" before a meeting starts, muting all participants reduces the possibility of inappropriate public conversation prior to the start of the meeting.



Disable "Virtual background": The "Virtual background" feature enables attendees to display an image behind them during the meeting. While this typically is harmless, some users may display inappropriate images. Consider disabling this feature.



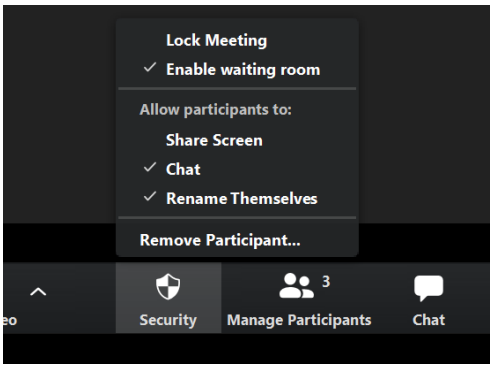
Enable" Co-host": While not appropriate for some meetings, on occasion a host may wish to delegate active meeting management to a second person so the host may concentrate on delivering content. This feature allows a host to provide meeting management features to a second attendee.



Actively Manage Zoom Meetings

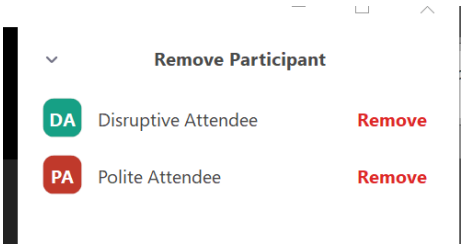
Once a meeting has started, the host has a number of security features available in Zoom to control the meeting environment.All LACCD Zoom users are encouraged to familiarize themselves with the following features:

Security Button: Zoom displays a "Security" button at the bottom of the host screen that gives the host several options to control the flow of the meeting:

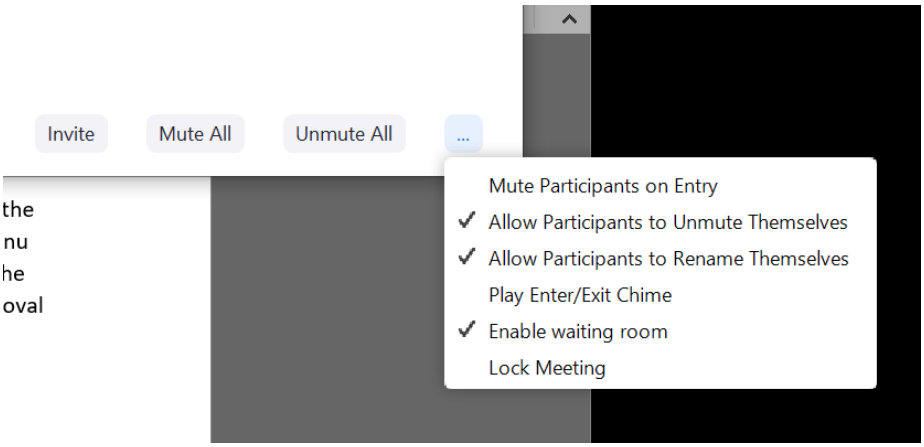


The following controls can be managed through the Security button:

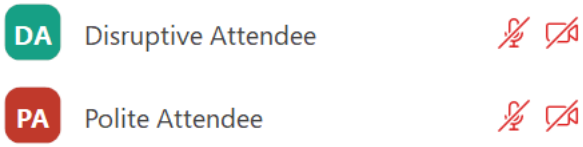
- **Lock Meeting:** Selecting "Lock Meeting" temporarily locks the meeting so no new attendees can be admitted. The meeting can be locked and unlocked as required.
- **Share Screen:** Selecting Allow participants to "Share Screen" enables the host to allow an attendee to share their screen. The meeting host should enable this only when participant sharing is required, and then disable it once the host has determined participant sharing is no longer required.
- **Chat:** The host may enable or disable chat for the entire meeting using this control.
- **Rename Themselves:** Participants may typically rename how they appear in the Zoom window. Most users use this feature to allow other participants to easily identify them, but some participants use the feature to be disruptive. Enable or disable this feature as prudent.
- **Remove Participant:** The host may remove participants who are disruptive, and by default the user may not rejoin the meeting. Selecting "Remove Participant" changes the right-side menu of Zoom so that the host may elect to remove one or more participants, as shown below. The host may also click "cancel" under the list of participant names if they no longer desire removal of a participant.



Mute Features: The host may mute or unmute all participants using the appropriate button located at the bottom of the Participant window in Zoom. Clicking "…" enables additional controls.



The host may also mute or unmute the audio or video of individual participants by clicking on the microphone or camera icons next to the participant name:



Report Incidents to the LACCD Information Security Office

Should any LACCD employee experience a security incident related to a Zoom conference, please contact your location's IT department by referring to:

- https://www.laccd.edu/Departments/InformationTechnology/Pages/default.aspx

Please provide the meeting date, time, class or meeting description, and the nature of the incident. The LACCD Information Security Office will forward the report to the appropriate District officials for review and guidance, as appropriate.