



(August 2022 Revision)

Recommended Security Settings/Practices for All Public-Facing SCCD Zoom Meetings

(For hosts/co-hosts of public-facing sccd.zoom.us meetings to reference and apply)

Update your Zoom Software (click the link below)

<https://zoom.us/support/download>

Review “[How to Keep Uninvited Guests Out of Your Zoom Meetings](#)”

Before the Meeting

Sign into your account on sccd.zoom.us >Click **Settings** on the left navigation menu> Click the **Meeting** tab, then follow the steps outlined below:

Disable Screen Sharing

1. Scroll to “**Screen sharing**” and “**Who can share?**”
2. Select Host Only
3. Click

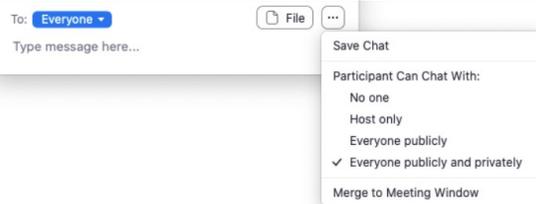
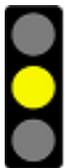
Consider Disabling Private Chat

1. Scroll to “**Chat**”.
2. Click the toggle to disable private chat. (Should now look like this:).

Disable Participants Video

1. Scroll to “**Participants video**”.
2. Click the toggle to disable all participant video at meeting start.

Manage Chat to Prevent Inappropriate Communications



Additional Settings

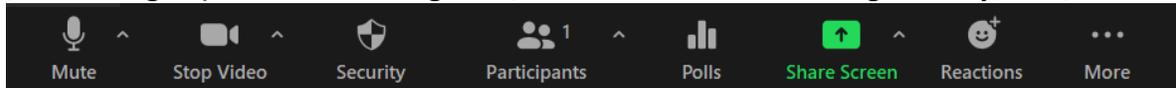
The following pre-meeting scheduling settings are strongly recommended.¹

- **Enable passwords** to require login authentication when joining a meeting.
- **Enable waiting rooms** to screen/prevent unauthorized participants from joining.
- **Disable annotation** to prevent participants from writing on screens.
- **Disable renaming onscreen ID** to prevent participants from altering their on-screen identity.
- **Mute participants** to block audio from individual (or all) participants.
- **Mute upon entry** to block audio from all participants when entering meeting.

¹ Call or e-mail your local helpdesk for assistance with configuring any of these settings.

Regain Control During a Meeting

Meetings with 25 or more attendees should have a designated “Moderator” ... (w/co-host rights) to assist meeting Host/Presenters with in meeting security/chat/etc...



Take the following steps to regain control of a Zoom meeting if security issues arise:

Click **Security**  (Located on toolbar)

The following settings/actions can be enabled/enacted from the in-meeting security menu:

- **Lock Meeting:** Locks the meeting, keeping new participants from joining the meeting.
- **Enable Waiting Room:** Enables [Waiting Room](#) for incoming new participants or to move current participants into the Waiting Room.
- **Hide Profile Pictures:** Hide all profile pictures, including the host. Display names are shown instead.
- **Disable Participants Ability To:**
 - **Share Screen:** Allows participants to [share their screens](#).
 - **Chat:** Allows participants to use the chat function.
 - **Rename Themselves:** Allows participants to rename themselves from the **Participants** panel.
 - **Unmute Themselves:** Allows participants to unmute themselves without the host's permission.
 - **Start Video:** Allows participants to start their video in the meeting.
 - **Annotate on Shared Content:** Allows participants to [annotate](#) over content shared during the meeting. The host can enable or disable annotation when the host is sharing.
- **Remove Participant:** Allows the removal of a participant from a meeting. The participant cannot re-join unless **Allow removed participants to rejoin** is enabled in [Meeting settings](#).
- **Report:** Allows you to [report a user](#) to Zoom's Trust and Safety team. You will be able to select which user to report and provide details about the problem. You can also upload evidence, such as screenshots.
- **Suspend Participant Activities:** Turn off all participant's video, audio, and ability to share their screen. Also lock the meeting to prevent participants from joining. This will apply to all participants including co-hosts.