Privacy & Security for Zoom Video Communications

Pre-Meeting Settings

Securing your Zoom Meetings can start before your event even begins, with a robust set of pre-meeting features.

- **Waiting Rooms**: IT Admins can enforce waiting rooms at the account, group, or user level. You can also require them for all participants, or just for guests not included in your account. If made optional, meeting hosts can enable Waiting Rooms in the "Settings" menu of their Zoom profile.

- **Passcodes**: Passcodes can be set at the individual meeting level or can be enabled at the user, group, or account level for all meetings and webinars. Account owners and admins can also lock passcode settings, to require passcodes for all meetings and webinars on their account.

- **Join by Domain**: Only authenticated users can join meetings which requires individuals to sign into a zoom account and/or ensure their e-mail address is on an approved list before allowing them to join.

In-Meeting Settings

Zoom has controls at your fingertips to ensure your meetings are secure and disruption-free.

- **Security options in toolbar**: Meeting hosts have a Security icon in the toolbar for quick access to essential in-meeting security controls. See it in action!

- **Lock the meeting**: When a host locks a Zoom Meeting that's already started, no new participants can join, even if they have the meeting ID and passcode (if you have required one).

- **Put participant on hold**: You can put an attendee on hold and their video and audio connections will be disabled momentarily.

- **Remove participants**: From that Participants menu, you can mouse over a participant's name, and several options will appear, including "Remove".

- **Report a user**: Hosts/co-hosts can report users to Zoom's Trust & Safety team, who will review any potential misuse of the platform and take appropriate action.

- **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, which is a good option for large meetings.

- **Turn off file transfer**: In-meeting file transfer allows people to share files through the in-meeting chat.

- **Turn off annotation**: You can disable the annotation feature in your Zoom settings to prevent people from writing all over the screens.

- **Disable private chat**: 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.

- **Control screen sharing**: The meeting host can turn off screen sharing for participants.

- **Control recording**: The ability to record to the cloud or locally is something an account admin can control. If they have recording access, the host can decide to enable/disable a participant or all participants to record.

- **Do not allow participants to rename their ID**: The host can disable the ability for participants to rename their onscreen identity.

- **Turn on waiting rooms**: The meeting host can turn on waiting rooms from within the meeting.

Protecting your data

You are entrusting us with your valuable data and information, and we take great care to ensure your data is secure at all times.

- **Encryption**: Protecting your event content by encrypting the session's video, audio, and screen sharing. This content is protected with the Advanced Encryption Standard (AES) 256 using a one-time key for that specific session when using a Zoom client.

- **Audio Signatures**: Embeds a user's personal information into the audio as an inaudible watermark if they record during a meeting. If the audio file is shared without permission, Zoom can help identify which participant recorded the meeting.

- **Watermark Screenshots**: Superimposes an image, consisting of a portion of a meeting participant's own email address, onto the shared content they are viewing and the video of the person who is sharing their screen.

- **Local Recording Storage**: Recordings stored locally on the host's device can be encrypted if desired using various free or commercially available tools.

- **Cloud Recording Storage**: Cloud Recordings are processed and stored in Zoom's cloud after the meeting has ended; these recordings can be passcode-protected or available only to people in your organization. If a meeting host enables cloud recording and audio transcripts, both will be stored encrypted.

- **File transfer storage**: If a meeting host enables file transfer through in-meeting chat, those shared files will be stored encrypted and will be deleted within 31 days of the meeting.

- **Cloud recording access**: Meeting recording access is limited to the meeting host and account admin. The meeting/webinar host authorizes others to access the recording with options to share publicly, internal-only, add registration to view, enable/disable ability to download, and an option to protect the recording.

How to Keep Uninvited Guests Out of Your Zoom Event
A couple of reminders on using Zoom to host public events:

- When you share your meeting link on social media or other public forums, that makes your event … extremely public. **ANYONE** with the link can join your meeting.

- Avoid using your Personal Meeting ID (PMI) to host public events. Your PMI is basically one continuous meeting and you don't want random crashing your personal virtual space after the party's over. Learn about meeting IDs and how to generate a random meeting ID (at the 0:27 mark) in this video tutorial.

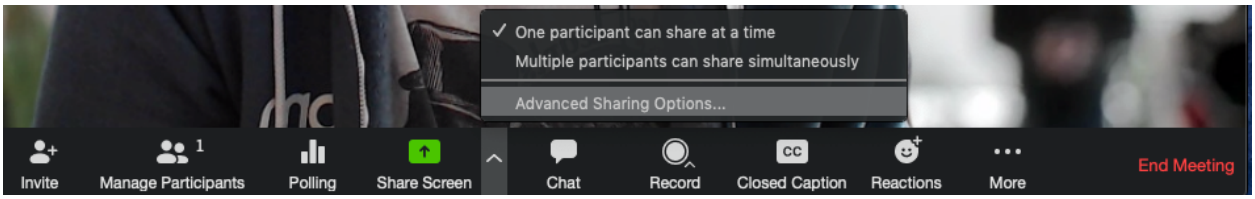
- Familiarize yourself with Zoom's settings and features so you understand how to protect your virtual space when you need to. For example, the Waiting Room is an unbelievably helpful feature for hosts to control who comes and goes. (More on that below.)

Manage screen sharing

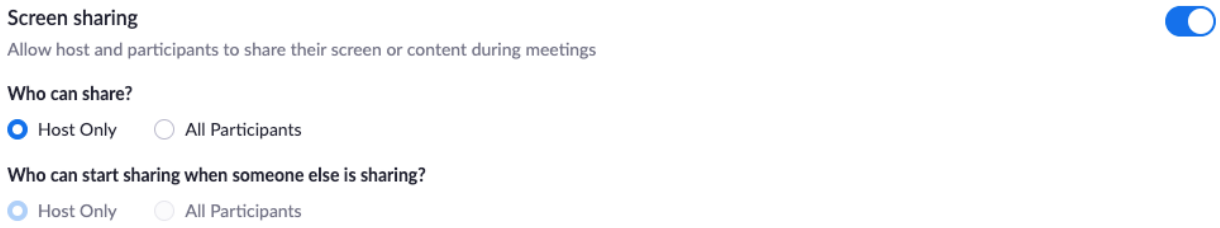
The first rule of Zoom Club: Don't give up control of your screen.

You *do not* want random people in your public event 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're the only one who can screen-share.

To prevent participants from screen sharing during a call, using the host controls at the bottom, click the arrow next to Share Screen and then Advanced Sharing Options.



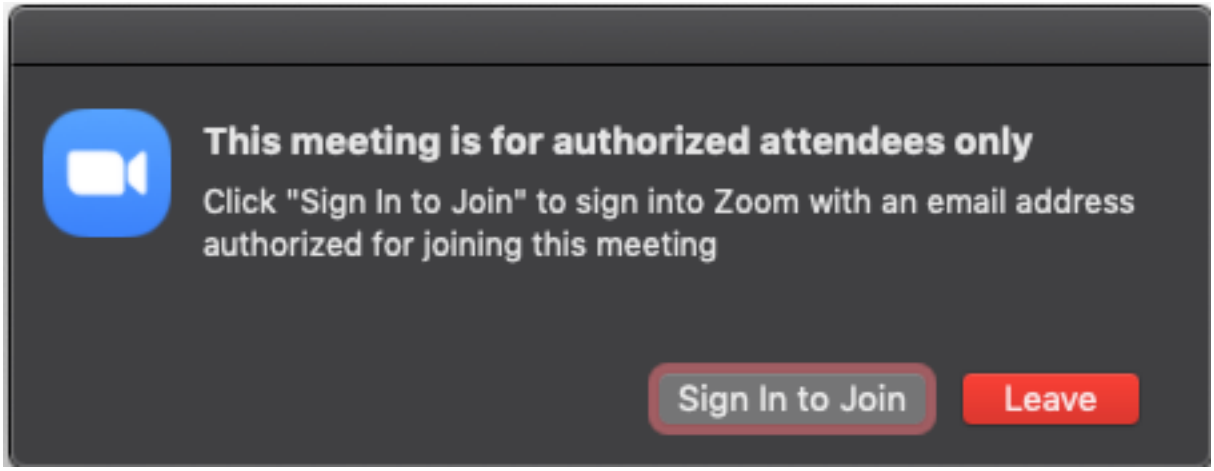
Under "Who can share?" choose "Only Host" and close the window. You can also lock the Screen Share by default for all your meetings in your web settings.



Manage your participants

Some of the other great features to help secure your Zoom event and host with confidence:

- **Allow only signed-in users to join:** If someone tries to join your event and isn't logged into Zoom with the email they were invited through, they will receive this message:



This is useful if you want to control your guest list and invite only those you want at your event — other students at your school or colleagues, for example.

- **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.

- **Set up your own two-factor authentication:** You don't have to share the actual meeting link! Generate a random Meeting ID when scheduling your event and require a password to join. Then you can share that Meeting ID on Twitter but only send the password to join via DM.

- **Remove unwanted or disruptive participants:** From that 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.

- **Allow removed participants to rejoin:** When you do remove someone, they can't rejoin the meeting. But you can toggle your settings to allow removed participants to rejoin, in case you boot the wrong person.

- **Put 'em 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 or for that time your friend's inside pocket is the star of the show.

- **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 the 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 the chat from getting bombarded with unsolicited pics, GIFs, memes, and other content.

- **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.

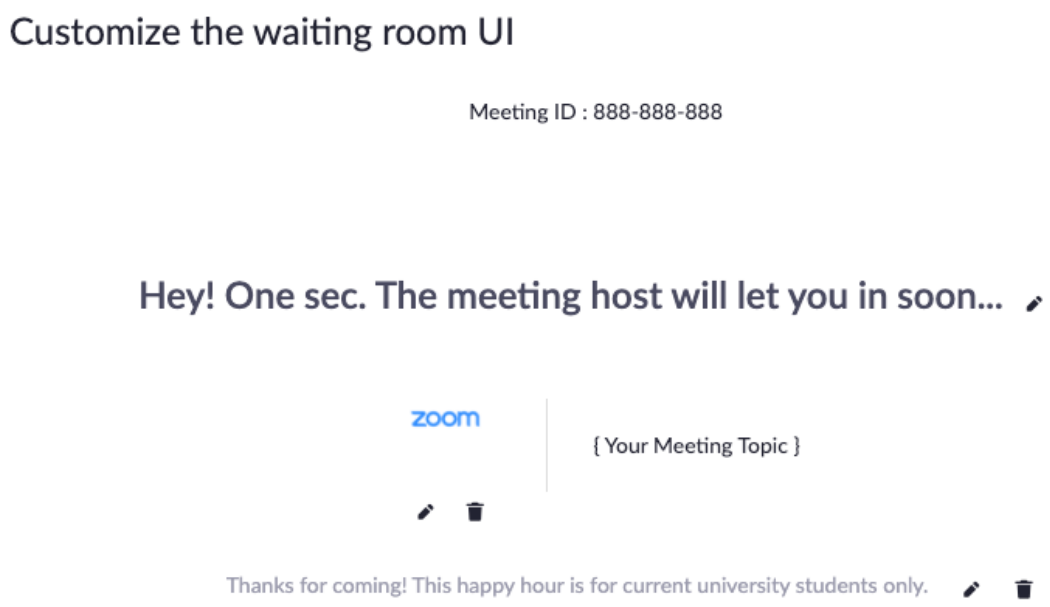
- **Disable private chat:** Zoom has in-meeting chat for everyone or participants can message each other privately. Restrict participants' ability to chat amongst one another while your event is going on and cut

back on distractions. This is really to prevent anyone from getting unwanted messages during the meeting.

Try the Waiting Room

One of the best ways to use Zoom for public events is to enable the Waiting Room feature. Just like it sounds, the Waiting Room is a virtual staging area that stops your guests from joining until you're ready for them. It's almost like the velvet rope outside a nightclub, with you as the bouncer carefully monitoring who gets let in.

Meeting hosts can customize Waiting Room settings for additional control, and you can even personalize the message people see when they hit the Waiting Room so they know they're in the right spot. This message is really a great spot to post any rules/guidelines for your event, like who it's intended for.



The Waiting Room is really a great way to screen who's trying to enter your event and keep unwanted guests out.

Keep Zooming responsibly

Zoom is a great way to stay connected right now, and we hope these tips will help you continue to host amazing events using our platform! If you're not sure whether a public Zoom event is the way to go, share the meeting link only with your close friends, co-workers, and clients. You can even password-protect it for another layer of security.

And keep those pictures from your Zoom virtual events coming! Share them with us on LinkedIn, Facebook, and Twitter, and we'll like, fave, or retweet a few!

References:

https://zoom.us/docs/en-us/privacy-and-security.html?zcid=3736&creative=431075689880&keyword=%2Bzoom%20%2Bhack&matchtype=b&network=g&device=c&gclid=EAIaIQobChMI8rWE1pKZ7AIVmYzICh0d_gWKEAAYASAAEgJgO_D_BwE

https://blog.zoom.us/keep-uninvited-guests-out-of-your-zoom-event/?_ga=2.245645324.984959980.1601752941-1988483905.1600794389&_gac=1.213706272.1601752944.EAIaIQobChMI8rWE1pKZ7AIVmYzICh0d_gWKEAAYASAAEgJgO_D_BwE