Information Technology Services
RANCHO SANTIAGO Community College District
Santa Ana College • Santiago Canyon College
SANTA ANA COLLEGE
Santiago Canyon College

ConferZoom

How to Avoid the "ZoomBomb" (Secure Zoom Meeting Tips)

Credit: Sable Cantus, CISSP at RioHondo

Original link: https://tinyurl.com/securezoom

For further assistance, please contact the RSCCD ITS Help Desk.

714-564-4357 | Ext 44357 | helpdesk@rsccd.edu | webhelpdesk.rsccd.edu | Mon-Fri, 7:30am-4:30pm

Contents

Keep your Zoom client updated

The best way to stay protected with the most current security features is to keep your Zoom client updated. **ITS recommends updating the Zoom client as frequently as possible to get all new security features and protection from vulnerabilities found.**

How do I download the latest version of Zoom?

Zoom provides a pop-up notification when there is a new mandatory or optional update within 24 hours of logging in.

To manually download the latest version of the Zoom client, go to this site: https://zoom.us/support/download

For more information on Zoom client updates, please reference this Zoom Help Center article: https://support.zoom.us/hc/en-us/articles/201362233-Where-Do-I-Download-The-Latest-Version-

What version of Zoom am I running now?

To find out what version of Zoom you are currently running, see this article for details: https://support.zoom.us/hc/en-us/articles/201362393

Where can I find more information on Zoom Updates and new security features?

Please refer to the end of this document for the latest Zoom Software Release information. We will this update this document accordingly, as new security features are released.

You can also refer to the Zoom Help Center release notes here: https://support.zoom.us/hc/en-us/sections/201214205-Release-Notes

How to Avoid the “ZoomBomb”

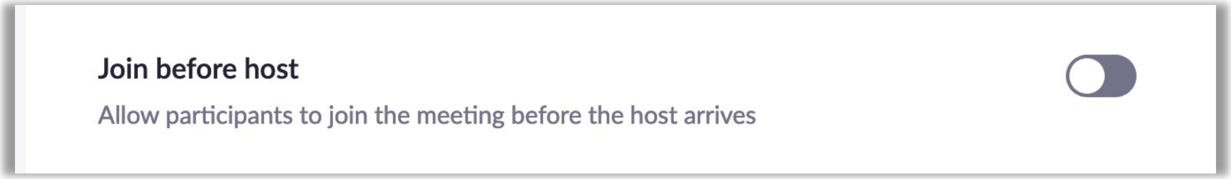
By Sable Cantus, CISSP

These changes to the default settings and best practices are recommended for anyone who is hosting Zoom conferences open to the public or with children attending. Changing these settings will help you keep control of your meeting and focus on your content.

Join before host

The participants could be having a party without you there to monitor.

Recommendation: **Turn off**



Join before host

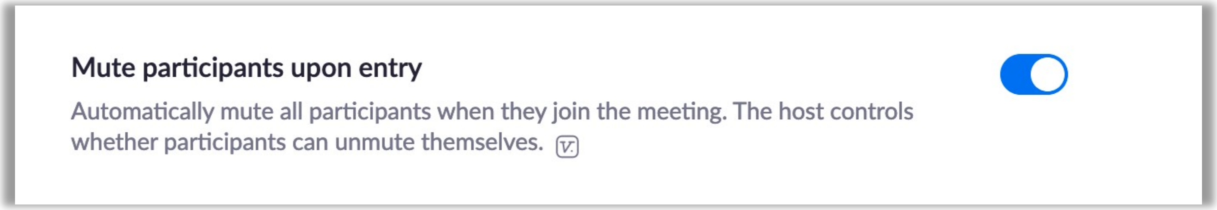
Allow participants to join the meeting before the host arrives

Mute participants upon entry

Barking dogs and crying babies can take over your meeting unintentionally. So can the participant who is singing their favorite heavy metal song at the top of their voice.

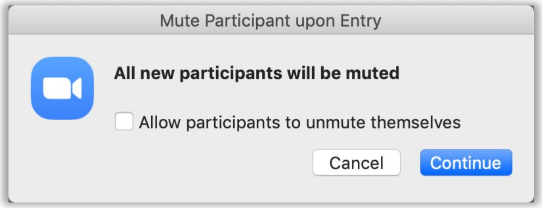
You might also consider disallowing participants to unmute themselves. In that case participants can use the “Raise hand” feature or the chat room to indicate when they want to speak. You can manually unmute them.

Recommendation: **Turn on**



Mute participants upon entry

Automatically mute all participants when they join the meeting. The host controls whether participants can unmute themselves.



Mute Participant upon Entry

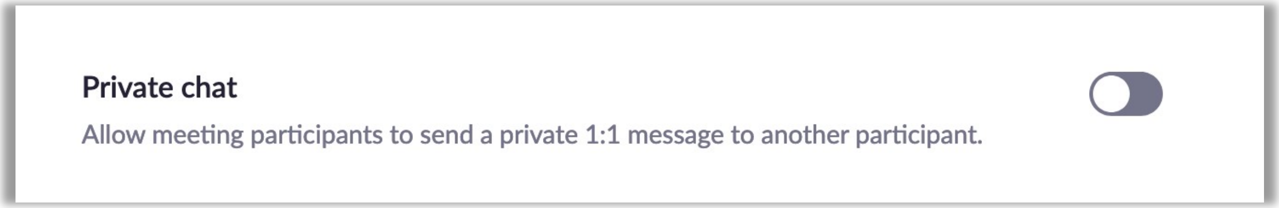
All new participants will be muted

□ Allow participants to unmute themselves

Private chat

The chatroom is one of the key ways to get live feedback and participation with your participants. We want to see all the communication that is happening. Disabling private chat will help tamp down any possible bullying or harassment during your meeting. They can use discord or text messages if they need a backchannel.

Recommendation: Turn off



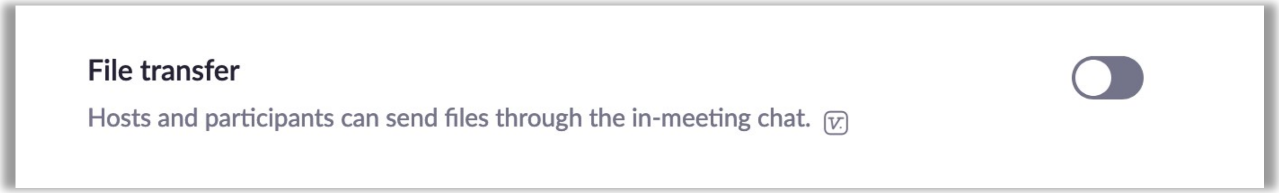
Private chat

Allow meeting participants to send a private 1:1 message to another participant.

File transfer

The ability to send files to your participants is very handy for you. Not so helpful if the participants are sending inappropriate (even unintentionally) files/gifs/images to the group. Put your files on Google Drive, Dropbox, 3C Media, etc. and give them download links.

Recommendation: Turn off



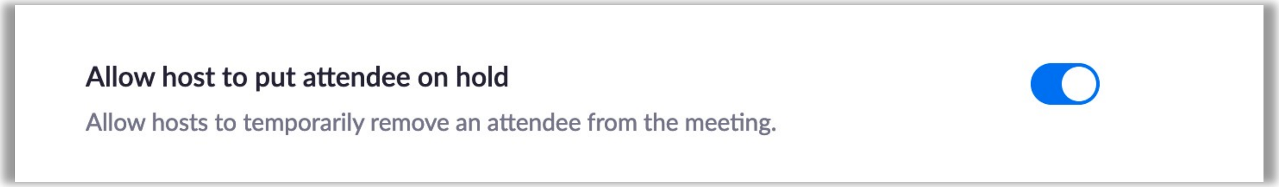
File transfer

Hosts and participants can send files through the in-meeting chat.

Allow host to put attendee on hold

Sometimes participants have environmental consideration that require you to step in and pause them. The participant could have someone enter the room. They could have a TV running behind them. They might have forgotten to dress appropriately…

Recommendation: Turn on



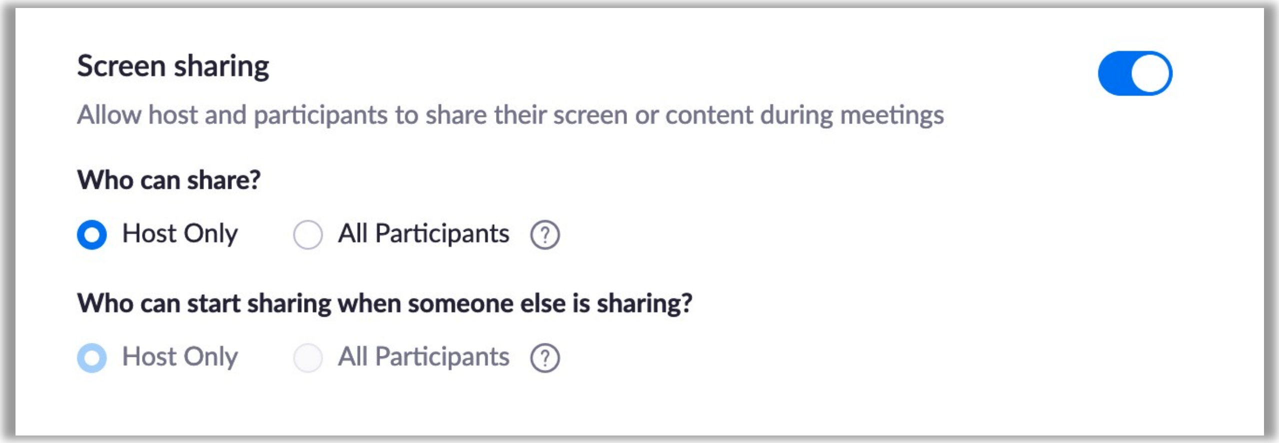
Allow host to put attendee on hold

Allow hosts to temporarily remove an attendee from the meeting.

Screen sharing

Your company department meeting is a great place for colleagues to share their business work with the group. Your classroom might not be. Participants can take over the session share and put anything they would like on screen for all in attendance. You can make a participant a cohost if you would like someone else to share their screen.

Recommendation: Turn on ***"Host Only"***



Screen sharing

Allow host and participants to share their screen or content during meetings

Who can share?

● Host Only ○ All Participants

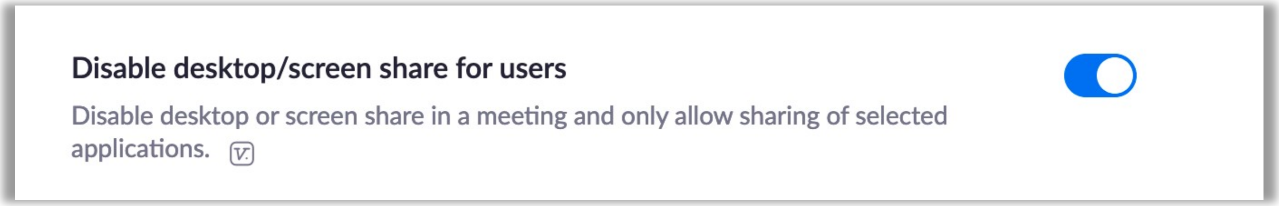
Who can start sharing when someone else is sharing?

● Host Only ○ All Participants

Disable desktop/screen share for users

We don't need to see the personal photos and information of your co-host when they share. This setting will enable them to share an Application (PowerPoint, Firefox, Chrome, PowerShell, etc.) only. You should consider only sharing applications yourself.

Recommendation: Turn on



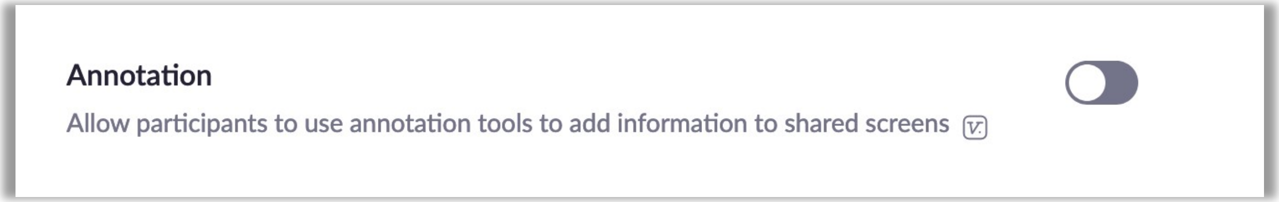
Disable desktop/screen share for users

Disable desktop or screen share in a meeting and only allow sharing of selected applications.

Annotation

Annotation gives you the ability to "draw" over the screen. It also gives that to your participants. They can draw anything that comes to mind over your presentation, your face, or anything else.

Recommendation: Turn off



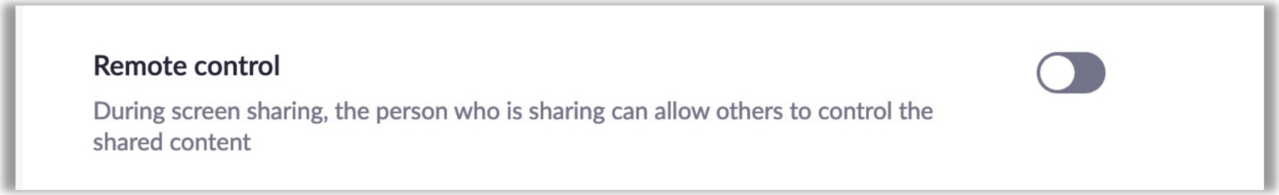
Annotation

Allow participants to use annotation tools to add information to shared screens

Remote control

This is a handy support feature in a 1:1 session. You don't want participants constantly requesting remote control of your desktop during meetings.

Recommendation: Turn off



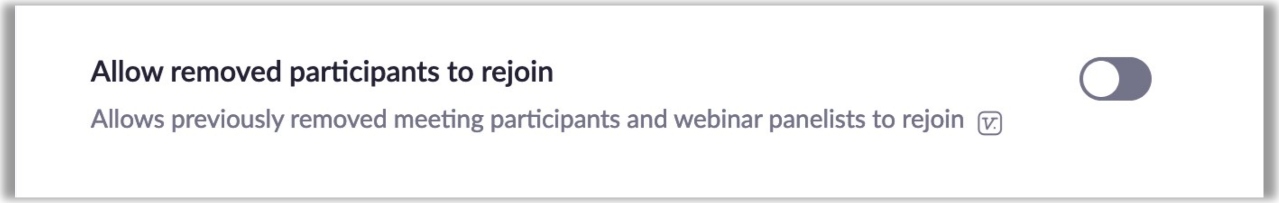
Remote control

During screen sharing, the person who is sharing can allow others to control the shared content

Allow removed participants to rejoin

When you kick someone out of your meeting for any reason, they shouldn't be able to come back.

Recommendation: Turn off



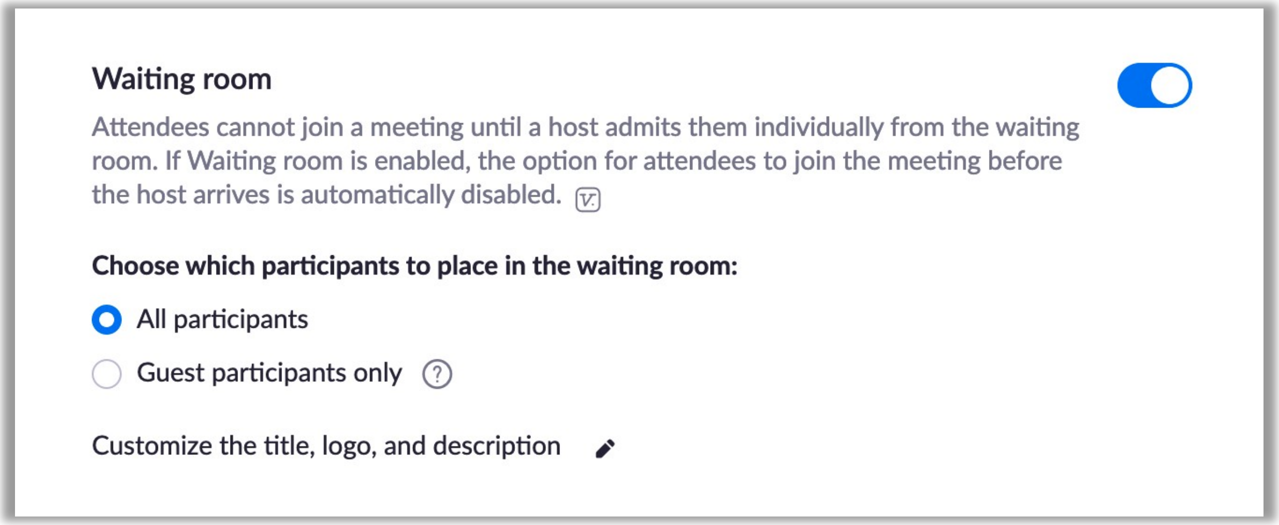
Allow removed participants to rejoin

Allows previously removed meeting participants and webinar panelists to rejoin

Waiting room

This is perhaps the most useful feature to help control your meeting or classroom. All participants will enter the waiting room before joining the main session. This allows you to let participants in as you are ready to receive them.

Recommendation: Turn on *and customize*



Waiting room

Attendees cannot join a meeting until a host admits them individually from the waiting room. If Waiting room is enabled, the option for attendees to join the meeting before the host arrives is automatically disabled.

Choose which participants to place in the waiting room:

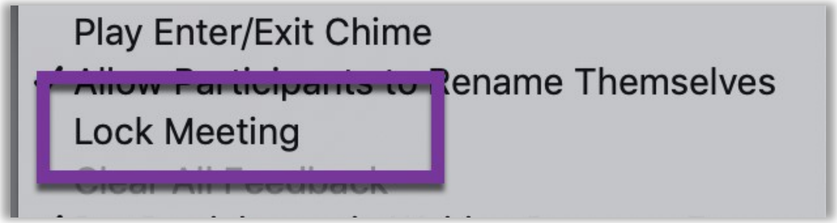
● All participants

○ Guest participants only

Customize the title, logo, and description

Optional: Consider locking your meeting once everyone is in attendance.

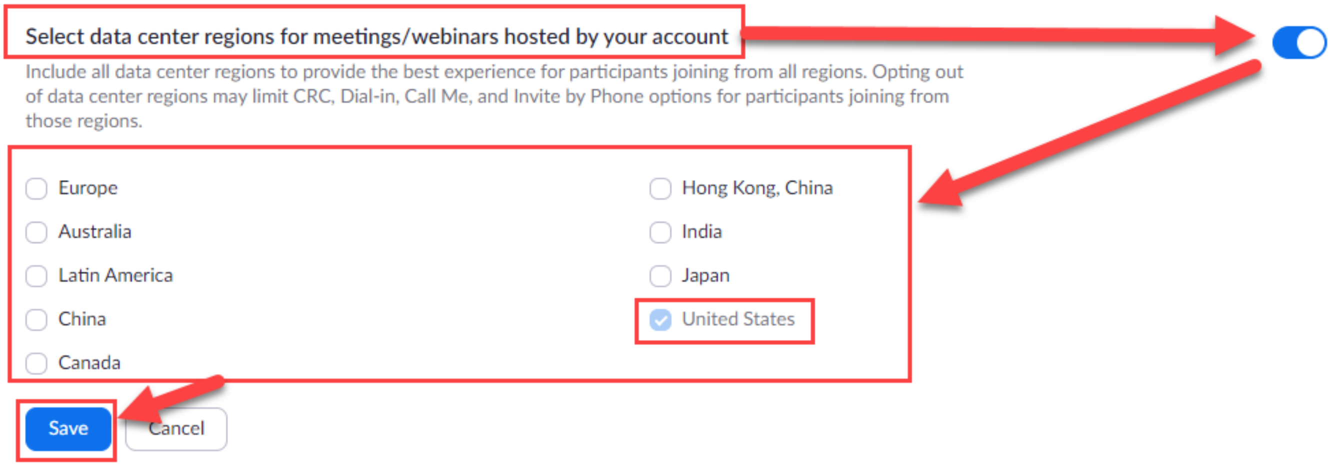
This is useful if you have a private meeting and know everyone is in attendance already. This will eliminate other unwanted participants from joining. This could also be used if you don't want people to enter after the start time.



Select data center regions for meetings/webinars hosted by your account (select *United States* only)

We strongly recommend to select "*United States*" as the only data center region to host your meetings.

Go to Settings > In Meeting (Advanced) > Toggle the option "Select data center regions for meetings/webinars hosted by your account" > Deselect all other regional servers, leaving "United States" selected by default > Click Save.



Select data center regions for meetings/webinars hosted by your account

Include all data center regions to provide the best experience for participants joining from all regions. Opting out of data center regions may limit CRC, Dial-in, Call Me, and Invite by Phone options for participants joining from those regions.

- ☐ Europe
- ☐ Australia
- ☐ Latin America
- ☐ China
- ☐ Canada
- ☐ Hong Kong, China
- ☐ India
- ☐ Japan
- ☑ United States

Zoom 5.0 Software Release

Version 5.0.0 (23168.0427)
Update as of 4/28/2020

Report a User Feature: Meeting hosts and co-hosts can report a user in their meeting who is misusing the Zoom platform. Found in the Security icon, the option sends a report to Zoom's Trust & Safety team for review. The report can include a specific offense, description, and optional screenshot. The Report a User function is on by default but can be turned off at the account, group, and user level in the Zoom web portal.

Profile Picture Control: Account admins and hosts can disable the ability for participants to show their profile picture and also prevent them from changing it in a meeting.

Leaving/Ending Meeting Enhancements: With this new UI update, hosts can clearly decide between ending or leaving a meeting. If the host leaves, they can now easily select a new host and have the confidence that the right person is left with host privileges. The host will now be required to assign a new host when leaving the meeting. Additionally, the pop-up message asking if the host would like to leave or end the meeting will now be displayed by the Leave button.

Setting to Allow Sharing of Cloud Recordings: Account owners and admins can enable or disable shared cloud recordings to prevent users from sharing their cloud recordings. This setting is available for individual recordings and at the account, group, and user level and can be locked at the group or account level.

Add Expiration Date for Shared Cloud Recordings: Users can now choose to expire the link for a cloud recording after a set number of days or on a custom date. This setting is available for individual recordings and at the account, group, and user level and can be locked at the group or account level.

Show the Connected Data Center: Users can see which data center they are connected to by clicking on by clicking on the info icon at the top left of the client window.

Minimum Password Length of 6 Characters for Meeting and Shared Recording Passwords: The minimum password length for both meeting and shared recording passwords will now be 6 characters.

New Password Requirements: This new setting allows account owners and admins to set meeting password and recording password requirements (on the account settings page). This change will affect the below API endpoints if your current meeting or recording passwords do not follow the new password requirement settings if enabled.