Zoom Meeting Security Guidelines

Zoom desktop conferencing is a key tool in our modern hybrid environment, enabling remote collaboration and instruction. However, there are individuals with malicious intent who may try to disrupt your Zoom meetings in a practice commonly known as "Zoombombing." Applying some or all of the following best practices can help to keep you and your virtual environment safe.

Know Your Security Settings

Security settings are provided at the account level, during the meeting scheduling stage and with a meeting in progress.

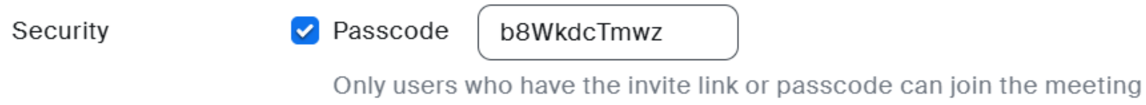
To enforce restrictions that will apply to *every* meeting, log into your account at https://vcu.zoom.us/ and go to **Settings > Meeting > Security.**

We recommend taking *at least one* of these precautions, and preferably several:

- **Passcodes**:
  Commonly used as a first line of defense, passcodes are especially effective at blocking troublemakers who may discover or guess your meeting link.

  Enable "**Require a passcode when scheduling new meetings**" to ensure that *all* your meetings get passcodes. Also consider applying passcodes by default to all **"instant" meetings** (those not scheduled in advance) and your **Personal Meeting Room** (which is especially vulnerable as the link never changes).

  You also have the option to apply a passcode when scheduling an individual meeting.

  Security ☑ Passcode b8WkdcTmwz

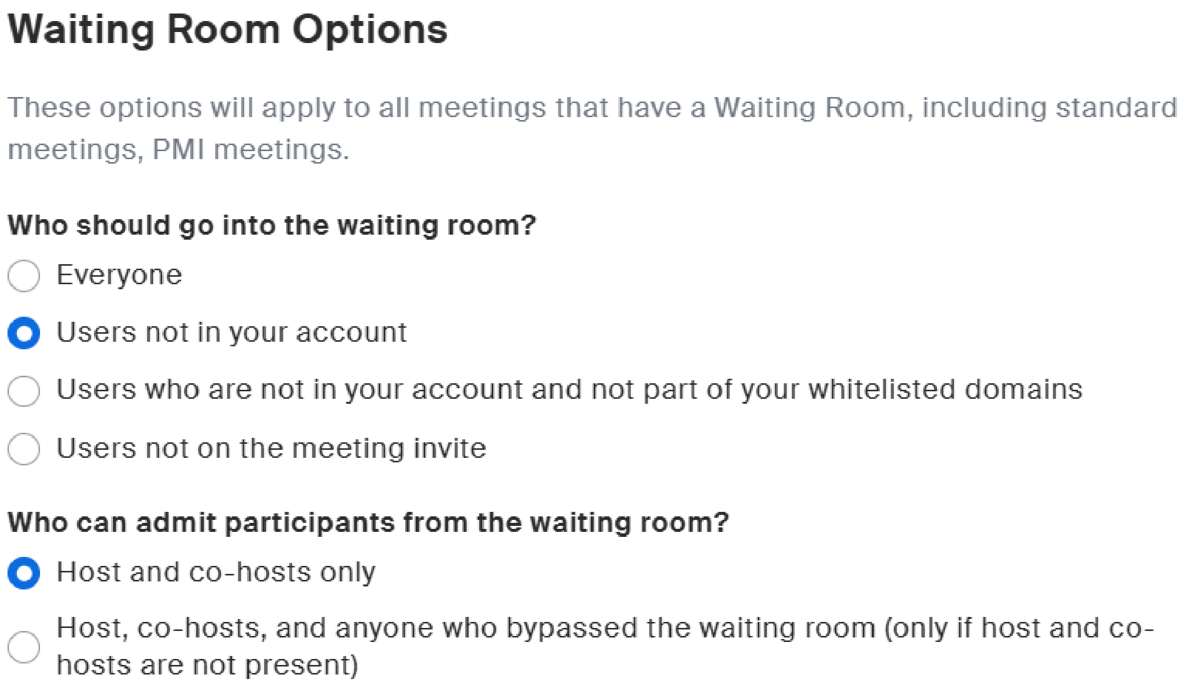
  Only users who have the invite link or passcode can join the meeting

  By default, your passcodes will be randomly generated by Zoom, but you could also invent your own. If so, be sure to make them hard to guess, and bear in mind they'll need to be at least 10 characters in length.

  Note there is an option to **embed the passcode in the meeting link**, saving your guests the trouble of typing it in after they arrive. With the passcode tacked on, the resulting link will be much longer and harder to guess, but beware of advertising it widely as anyone who obtains it can enter the meeting as easily as if you had no passcode at all.

- **Waiting rooms**
  With a Waiting Room enabled, arriving guests are placed in a “virtual lobby” where you as the host will see them listed by name. You can decide who to admit on a case-by-case basis, denying entry to unknown and potentially malicious users.

  In your account settings you can edit the “Waiting Room Options” to control who will and will not be automatically sent to the Waiting Room. For example, maybe you want everyone who’s signed into a VCU Zoom account to bypass the Waiting Room and pass directly into your meeting.



Waiting Room Options

These options will apply to all meetings that have a Waiting Room, including standard meetings, PMI meetings.

Who should go into the waiting room?

○ Everyone

● Users not in your account

○ Users who are not in your account and not part of your whitelisted domains

○ Users not on the meeting invite

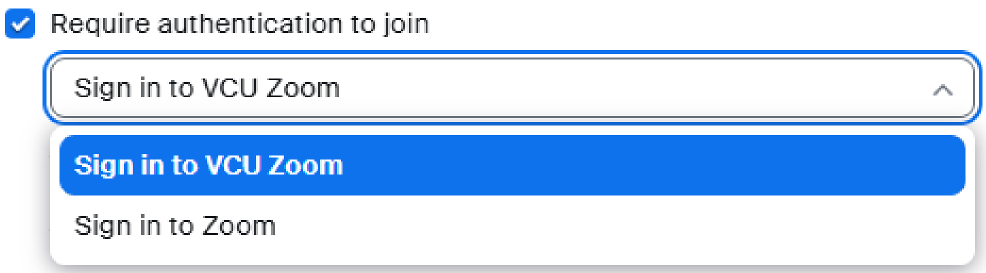
Who can admit participants from the waiting room?

● Host and co-hosts only

○ Host, co-hosts, and anyone who bypassed the waiting room (only if host and co-hosts are not present)

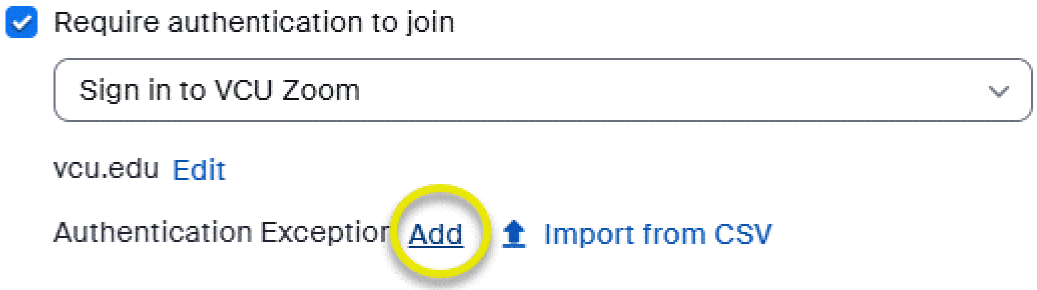
- **Authenticated users**
  Also under **Settings > Meeting > Security** is the option, “**Only authenticated meeting participants and webinar attendees can join meetings and webinars.”** With this enabled, all your attendees must be logged in to a valid Zoom account to join your meeting. Based on your preferences, entry can be strictly limited to fellow members of the VCU account (“**Sign in to VCU Zoom**”) or you could open it up to include owners of ANY Zoom account, even if they’re not from VCU (“**Sign into Zoom**”). Either way, you’ll weed out Zoombombers who try to join anonymously or under false names.

  If you want to enforce authorization for *some* meetings but not others, you can choose to enable or disable it for each individual meeting you schedule.


☑ Require authentication to join

Sign in to VCU Zoom

Note that if you use the “**Sign in to VCU Zoom**” option (for example, to admit only students who are enrolled in your class), you can add an exception for specific non-VCU individuals, for example a guest lecturer.

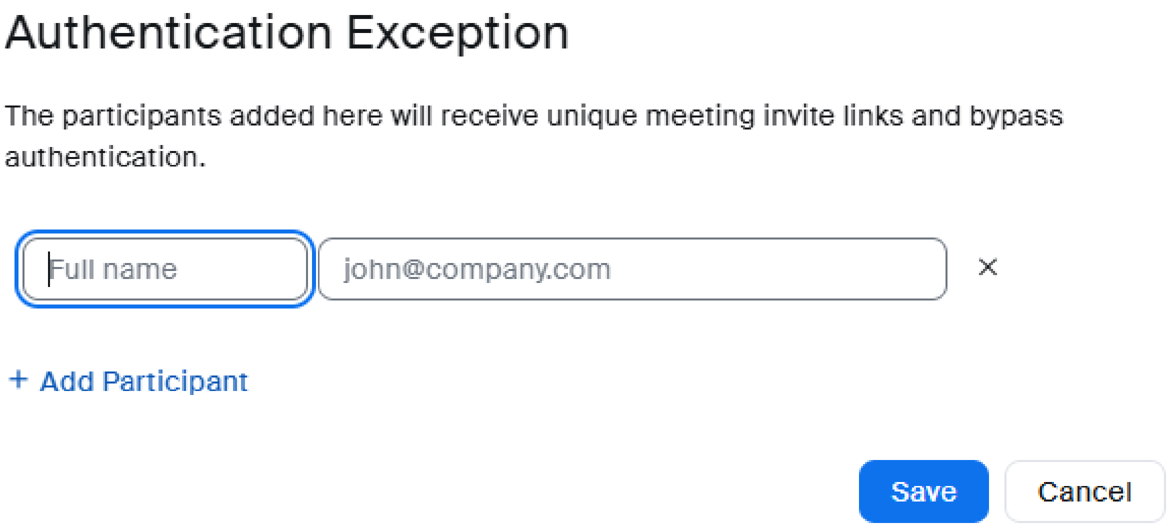

☑ Require authentication to join

Sign in to VCU Zoom

vcu.edu Edit

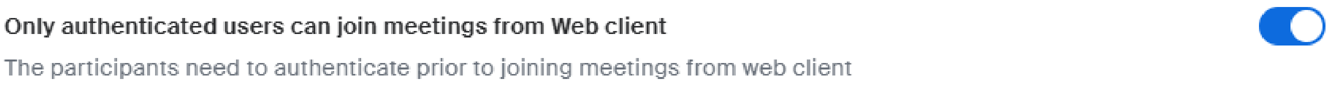
Authentication Exception Add Import from CSV

Type in the person’s name and the email address they use for Zoom, and they’ll be admitted when they arrive.


Authentication Exception

The participants added here will receive unique meeting invite links and bypass authentication.

There is a separate account setting called “**Only authenticated users can join meetings from Web Client**.” Enabling this will require any user who joins via a web browser to be logged into a Zoom account (“Basic” Zoom accounts are free to anyone). This is an effective means of barring not only “anonymous” Zoombombers but also automated bots that exploit the web client to join meetings.

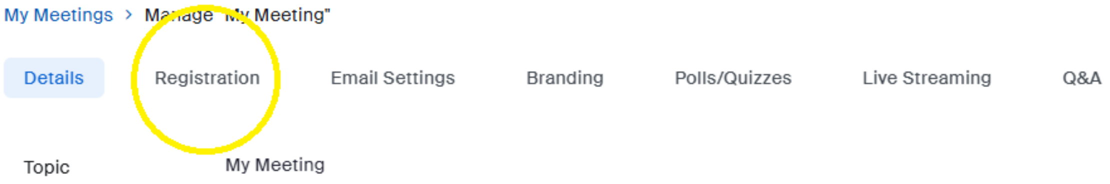


Only authenticated users can join meetings from Web client

The participants need to authenticate prior to joining meetings from web client

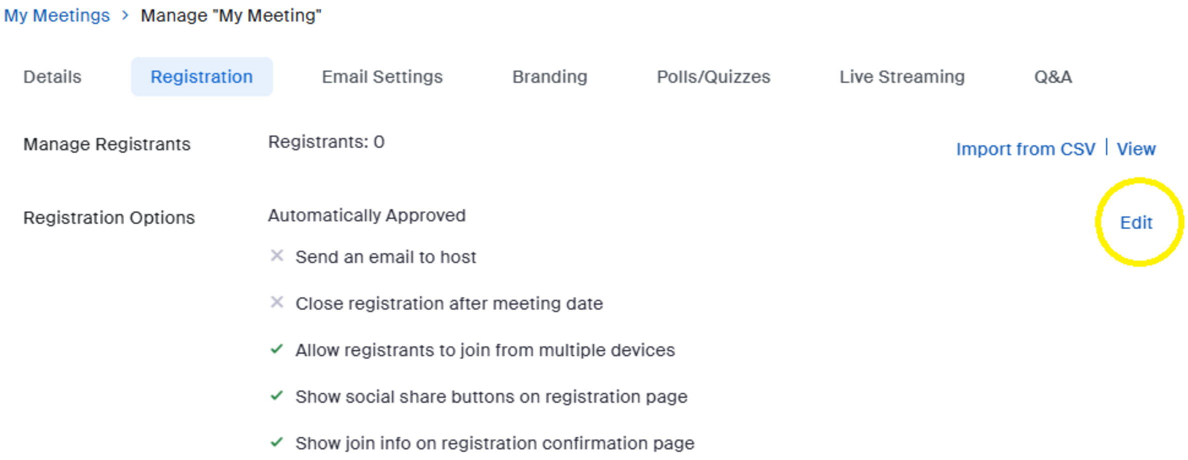
- **Registration**
  When you enforce registration for your meeting, a unique webpage is created with a form for your guests to fill in and submit. Once they’ve done so, they’ll receive the actual meeting link via email. The registration page URL is much safer to widely advertise than the meeting link itself, making this a useful tool for public-facing meetings where passcodes or authentication are not practical but you still want some level of security.

  Registration can only be added to meetings scheduled via the VCU Zoom portal (vcu.zoom.us) and not the desktop app. Once the meeting is scheduled but before you share the link, you should go to the Registration tab…



Topic My Meeting

…and make a couple of important adjustments using the “Edit” option.



Manage Registrants Registrants: 0

Registration Options Automatically Approved

✕ Send an email to host

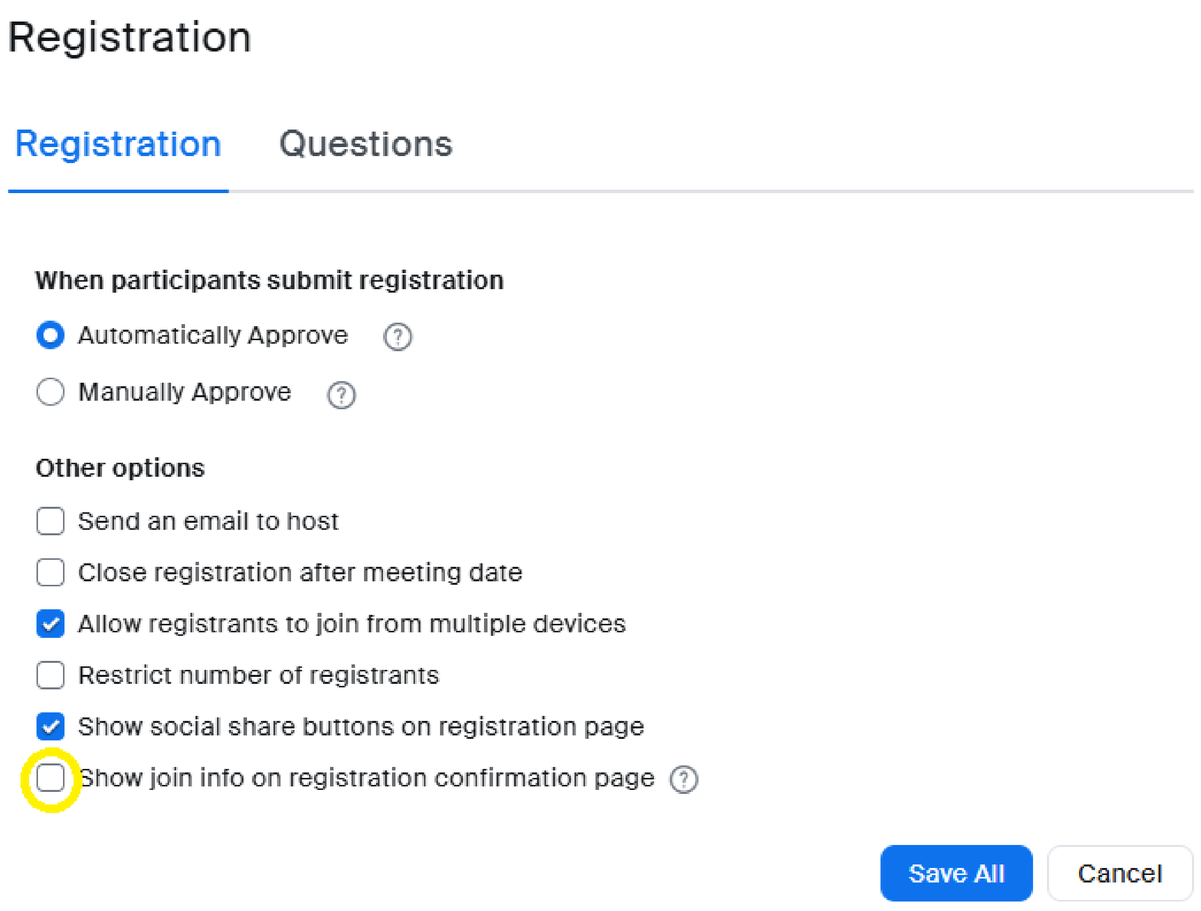
✕ Close registration after meeting date

✓ Allow registrants to join from multiple devices

✓ Show social share buttons on registration page

✓ Show join info on registration confirmation page

First, consider disabling “**Show join info on registration confirmation page**.” This is enabled by default, but it allows persons who register within 60 minutes of the meeting start time to see the meeting link *in their browser*, rather than waiting for it to arrive via email. This could allow a Zoombomber to join using a fake name and address.



Registration

Registration | Questions

When participants submit registration

● Automatically Approve ?

○ Manually Approve ?

Other options

□ Send an email to host

□ Close registration after meeting date

☑ Allow registrants to join from multiple devices

□ Restrict number of registrants

☑ Show social share buttons on registration page

□ Show join info on registration confirmation page ?

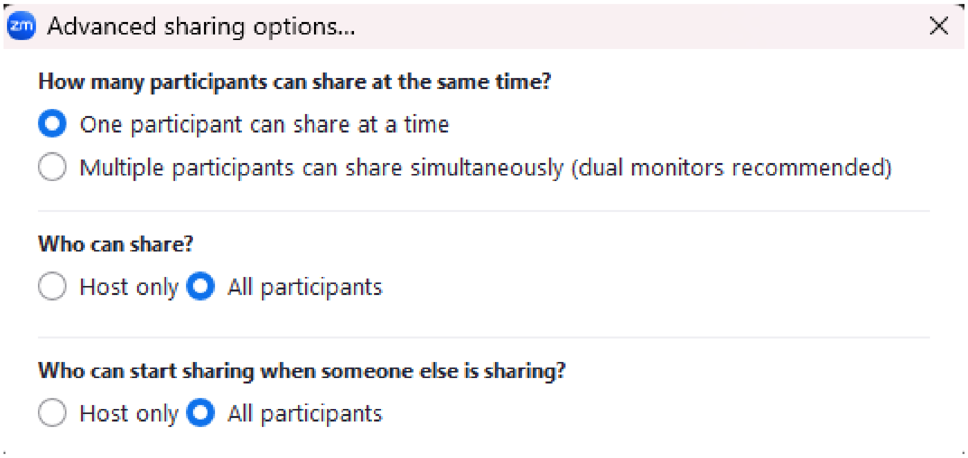
Save All | Cancel

It is also a good idea to **disable** "**show social share buttons on registration page**." With this turned on, visitors to the registration page can click on buttons to *advertise* your event on social media platforms, where Zoombombers often hang out.

Limit Participant Privileges

As a general rule, meeting participants should be granted the minimum level of privileges necessary for the meeting to function.

- **Screen sharing**:
  Unless it's necessary for meeting attendees to share content, consider limiting screen sharing to **"Host Only."** Apply this setting at the account level, or click on the "Share" icon in the meeting taskbar and look for "Advanced Sharing Options."



Advanced sharing options...

How many participants can share at the same time?

● One participant can share at a time

○ Multiple participants can share simultaneously (dual monitors recommended)

Who can share?

○ Host only ● All participants

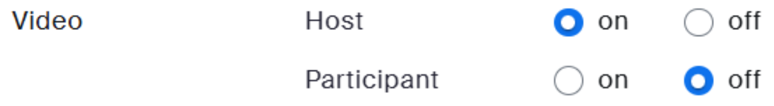
Who can start sharing when someone else is sharing?

○ Host only ● All participants

Even if you leave participant sharing enabled, consider limiting it to "**One participant at a time**" to prevent disruptions.

- **Annotation**:
  This feature allows users to draw and place text on shared content and whiteboards. Unless necessary for achieving your meeting goals, consider restricting this ability to yourself as host. You can enable it for participants as needed during your meeting.

- **Video:**
  Misuse of the camera feed is one of the primary methods used by Zoombombers to disrupt meetings. If your attendees do not need to be seen, set "Participant Video" to "**OFF**" when scheduling your meeting. If you need to see them, you can grant individual participants permission to turn their camera on with the meeting in progress.

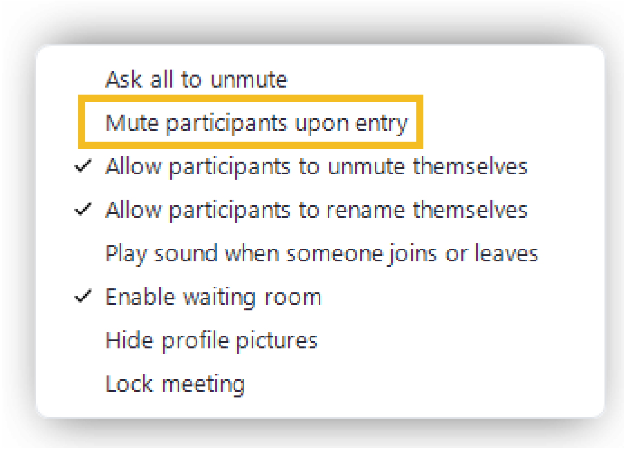


Video	Host	● on	○ off
	Participant	○ on	● off

NOTE: To prevent participants from enabling their video after the meeting has started, uncheck "show video" under the Host Tools control (see page 8).

You might also consider enabling **Focus Mode**. This feature allows the Host and Co-Hosts to see video from all participants, but the attendees will only see the Host, Co-Hosts and any users the Host chooses to "spotlight." This feature is especially useful when proctoring quizzes or focusing attention on student presentations. Look for it under the "more" (three "dots") button on the far right of your meeting taskbar.

- **Microphone:**
  Consider enabling "**Mute participants on entry**" to reduce the risk of disruptions via unwanted audio. Use this setting when scheduling your meeting, or via the "Participants" window with a meeting in progress.



Ask all to unmute

Mute participants upon entry

✓ Allow participants to unmute themselves

✓ Allow participants to rename themselves

Play sound when someone joins or leaves

✓ Enable waiting room

Hide profile pictures

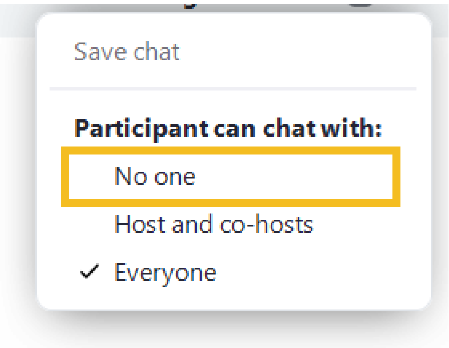
Lock meeting

Bear in mind that once they arrive, participants may choose to unmute themselves. You can prevent this by removing the “check” mark next to that setting.

- **Profile pics**:
  The “profile pictures” that appears when participants’ cameras are off can be vectors for harmful imagery. You can disable them in your account settings or using the “Participants” controls or Host Tools in your meeting.

- **User names:**
  You can allow or disallow users the ability to change their displayed names. Go to Host Tools in your taskbar and look for “**Allow all participants to…Rename themselves**.” You can also disallow this by default for *all your meetings* via your account settings

- **Chat:**
  The chat window could be another outlet for bad behavior. You can choose to disable Chat entirely at the account level, or use the “Participants” controls in a meeting to specify whether an attendee may address everyone, only you as the host, or no one at all.



Save chat

Participant can chat with:

No one

Host and co-hosts

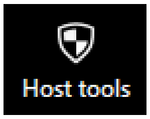
✓ Everyone

Use Your In-Meeting Controls

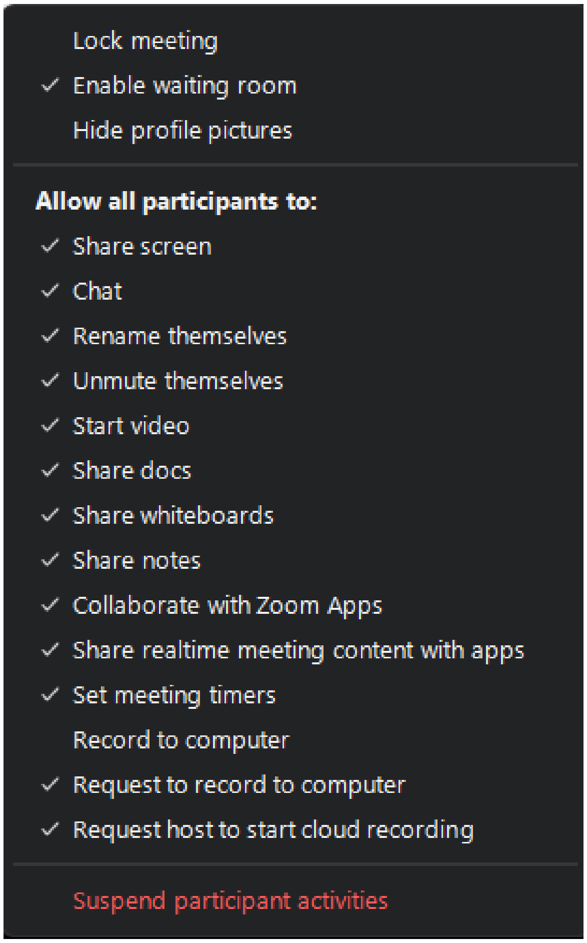
Even if you've taken precautions at the account level and during the scheduling phase, situations may arise in the course of your meeting that require quick action on your part. Fortunately, you have several options for performing real-time damage control.

- **Host Tools**

  Easily the most useful weapon in your in-meeting security arsenal is the "**Host Tools**" feature, providing you with one-stop access to all major security settings.



Every power granted to participants is listed here, and any of them can be taken away or restored at your discretion. Anything with a check mark displayed next to it is *enabled*, while anything without a check mark is *disabled*. Click next to the listed item to turn it on or off.



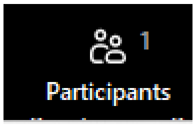
Lock meeting
✓ Enable waiting room
Hide profile pictures

Allow all participants to:
✓ Share screen
✓ Chat
✓ Rename themselves
✓ Unmute themselves
✓ Start video
✓ Share docs
✓ Share whiteboards
✓ Share notes
✓ Collaborate with Zoom Apps
✓ Share realtime meeting content with apps
✓ Set meeting timers
Record to computer
✓ Request to record to computer
✓ Request host to start cloud recording

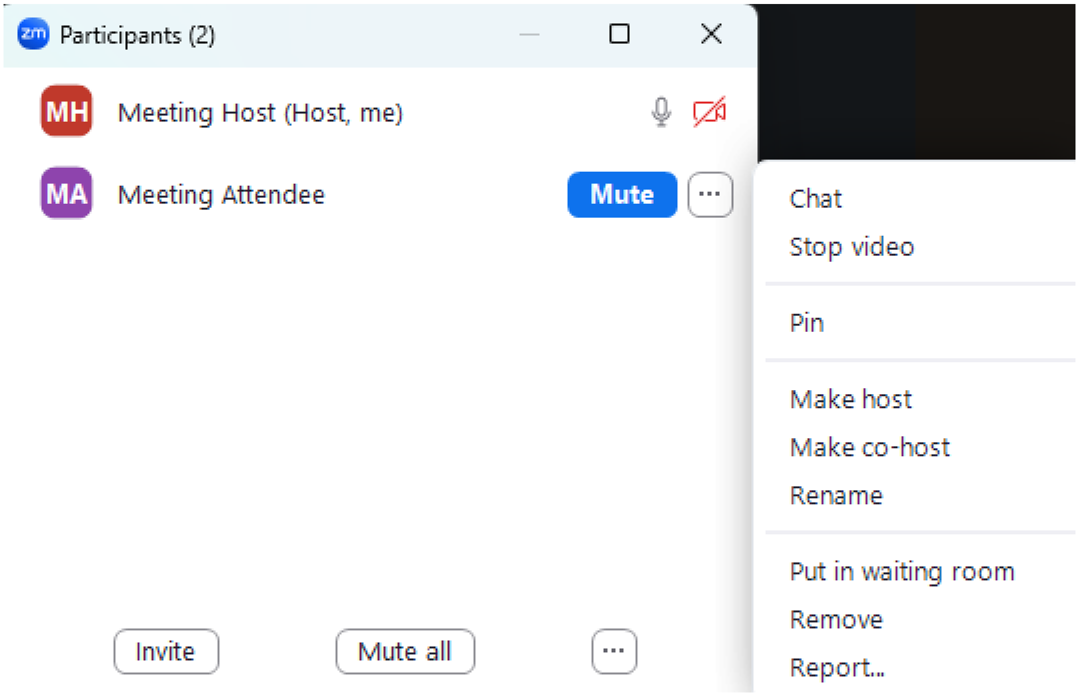
Suspend participant activities

This is also where you'll find the "**Lock meeting**" option. If you select this, no new attendees will be permitted to join your meeting, unless and until you unlock it again.

- **Participants Tool**



With the "**Participants**" tool you can see a list of all attendees and exercise control over individual users, including stopping their video or requesting they turn it on, muting microphones (including the "Mute all" function), elevating someone to the co-host role, moving them to the waiting room, or removing them from the meeting entirely.



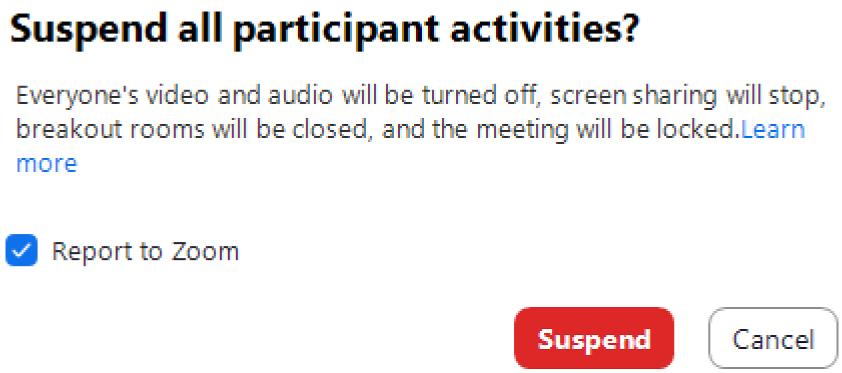
What to do if your meeting is compromised

In the unfortunate event a malicious user disrupts your meeting, there are steps you can take to regain control.

- **Remove the Offender**
  You can use the **Participants** menu to select "**Remove**" and eject the offender from the meeting. You can also select **Report**, which will notify Zoom's Trust and Safety team to investigate the user's behavior. By default, a removed user will be unable to rejoin

unless you have enabled “Allow removed participants to rejoin” in your account settings, but this is off by default for security reasons.

- **Suspend All Activity**
  A more drastic action is “**Suspend all participant activities**” which is located at the bottom of the Host Tools menu. If you choose to take this action, you’ll be presented with a red confirmation button, which when clicked will immediately: lock the meeting, turn off all attendee audio and video, suspend the meeting chat, stop any screen sharing, end any breakout rooms, turn off annotations, and stop any recordings. You will be asked if you wish to report the incident to Zoom. Once you press the “**Suspend**” button, the reported user will be removed and Zoom’s Trust and Safety team will be notified. You can then resume your meeting by using the Host Tools menu to enable all the features you feel safe with.



Suspend all participant activities?

Everyone's video and audio will be turned off, screen sharing will stop, breakout rooms will be closed, and the meeting will be locked.Learn more

☑ Report to Zoom

- **Report the Incident**
  If you do experience a Zoombombing or other security-related incident, please notify the VCU Zoom Support team at Zoom@vcu.edu and/or the VCU Information Security Office at iso@vcu.edu. Include as many details as you can, including the Meeting ID#, the nature of the offense and, if known, the suspected participant.

  If you feel that the incident involved criminal behavior, including hate speech or child sexual abuse material (CSAM), we may need to involve the VCU Police or other law enforcement authorities. If you feel it is helpful you may share screenshots, recordings, or chat logs. DO NOT share screen shots or recordings if CSAM is involved; any matters involving objectionable material of this nature must be handled by the police.