

# Conducting Zoom Calls with Confidence

A visual guide to adjusting your global settings  
and best practices for safe online meetings

Rafael Brinner, Director of Jewish Community Security

April 28, 2020

# Overview

This visual guide is designed to help you navigate the virtual landscape of Zoom meetings as safely as possible. It covers:

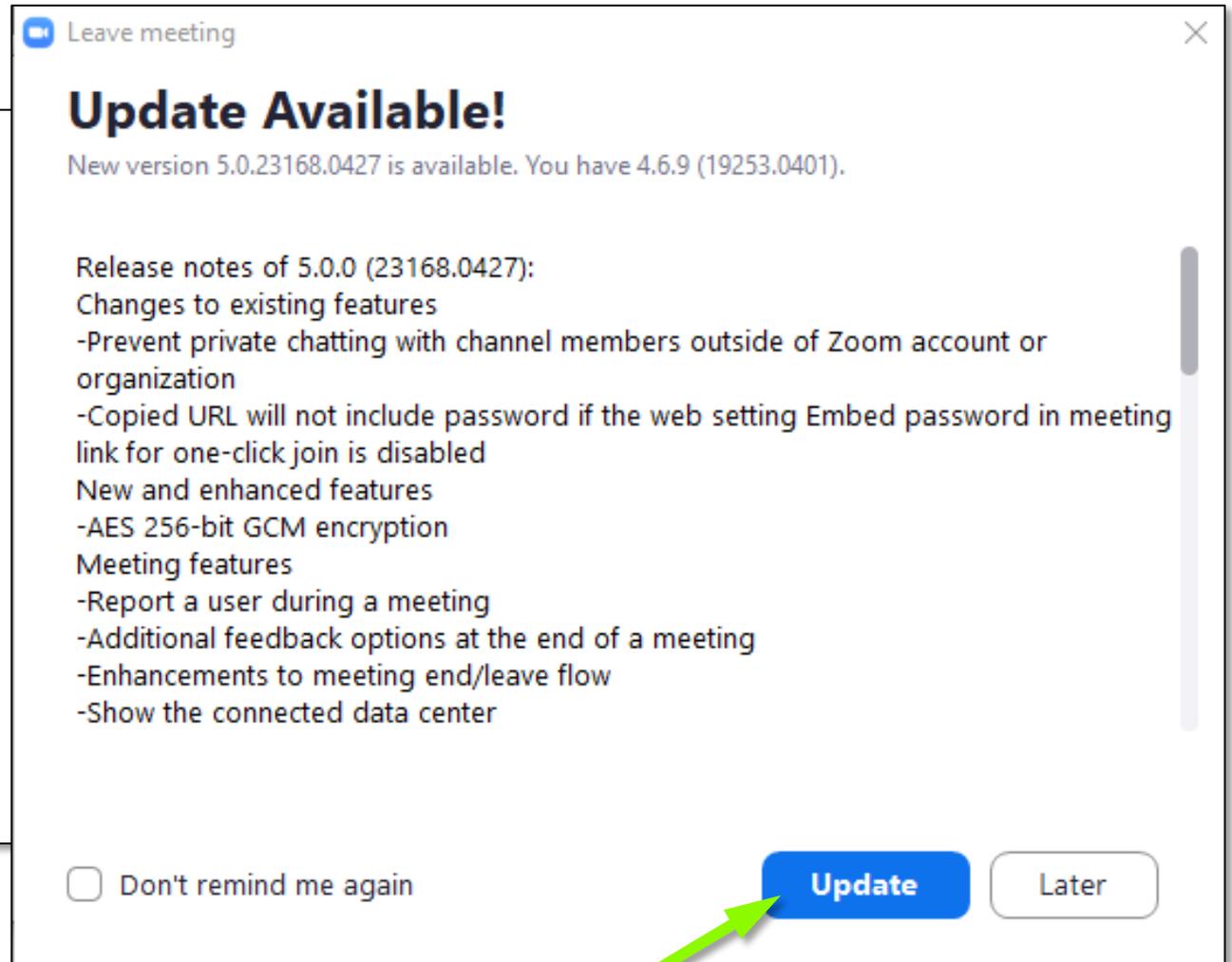
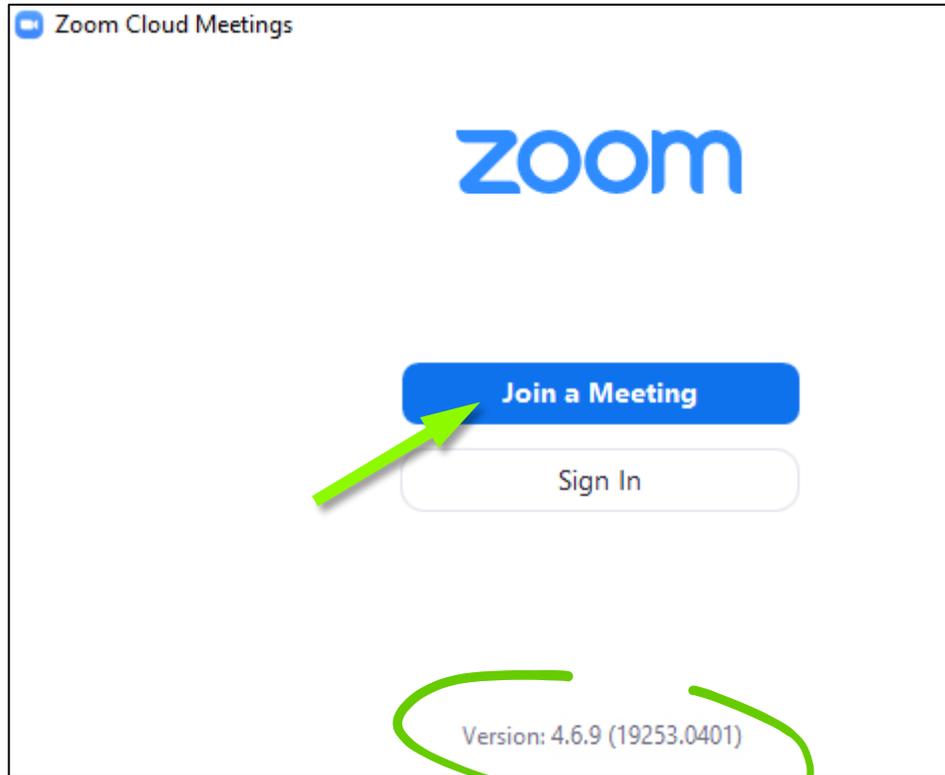
How to upgrade your Zoom software to the latest version.

Five best practices for making your Zoom calls:

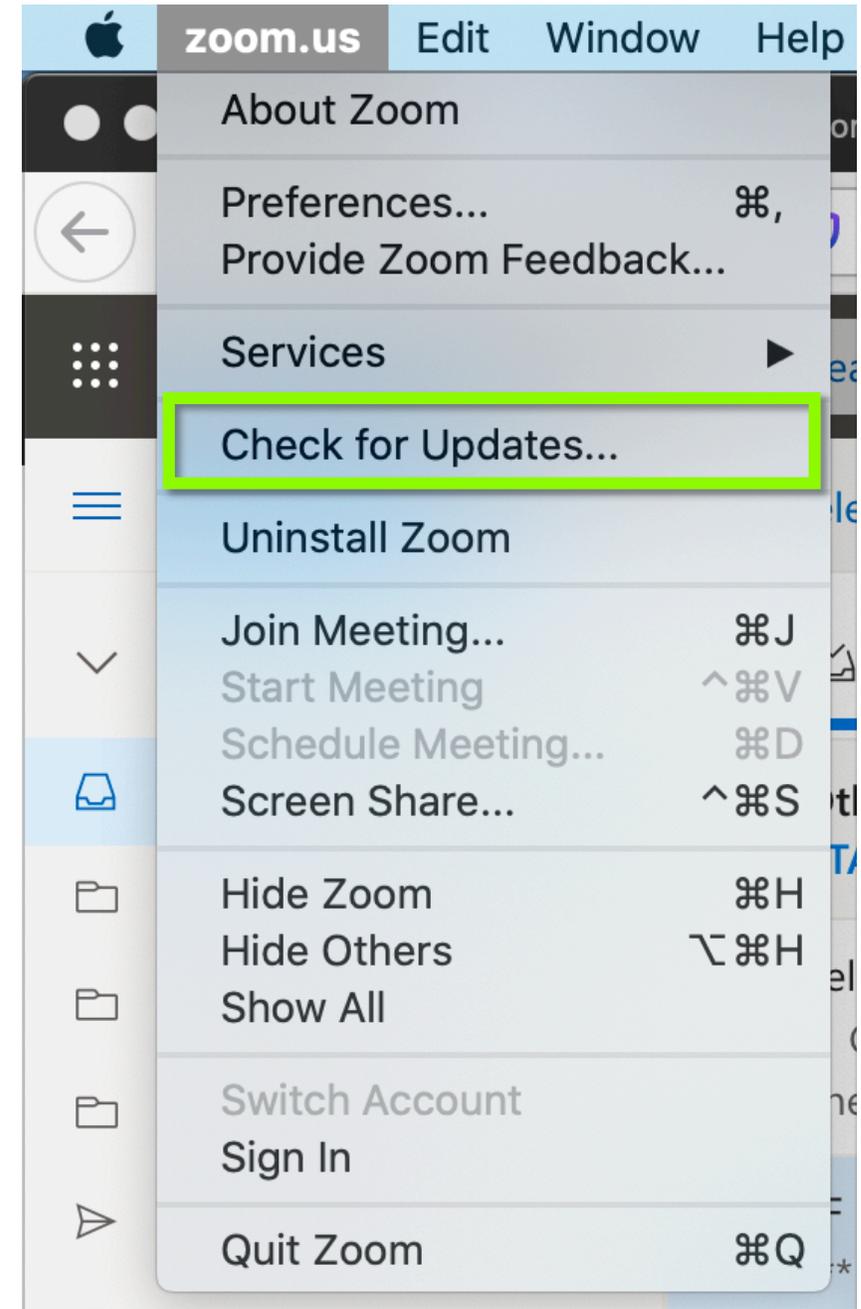
- harder to intentionally disrupt
- easier to manage if crashers show up

How to report an incident

# Upgrade to the latest version of Zoom (for Windows)



# Upgrade to the latest version of Zoom (for Mac OS)



# Five Best Practices

---

1 Adjust your account settings < *Block unwanted visuals*  
*Restrict written communication*

2 Use the Registration feature

3 Appoint a bouncer

4 Lock the room

5 Record your call

# / Adjust your account settings

[SCHEDULE A MEETING](#)

Profile

Meetings

Webinars

Recordings

Settings

Account Profile

Reports



Meeting

Recording

Telephone

Schedule Meeting

In Meeting (Basic)

In Meeting (Advanced)

Email Notification

Other

Schedule Meeting

**Host video**

Start meetings with host video on



**Participants video**

Start meetings with participant video on. Participants can change this during the meeting.



**Audio Type**

Determine how participants can join the audio portion of the meeting. When joining audio, you can let them choose to use their computer microphone/speaker or use a telephone. You can also limit them to just one of those audio types. If you have 3rd party audio enabled, you can require that all participants follow the instructions you provide for using non-Zoom audio.

Telephone and Computer Audio

Telephone

Computer Audio

SCROLL DOWN



Profile  
Meetings  
Webinars  
Recordings  
**Settings**  
Account Profile

**Meeting**

Recording

Telephone

Schedule Meeting

In Meeting (Basic)

In Meeting (Advanced)

Email Notification

Other

**Join before host**

Allow participants to join the meeting before the host arrives



**Use Personal Meeting ID (PMI) when scheduling a meeting**

You can visit [Personal Meeting Room](#) to change your Personal Meeting settings.



**Use Personal Meeting ID (PMI) when starting an instant meeting**



**Only authenticated users can join meetings**

The participants need to authenticate prior to joining the meetings, hosts can choose one of the authentication methods when scheduling a meeting.



**Require a password when scheduling new meetings**

A password will be generated when scheduling a meeting and participants require the password to join the meeting. The Personal Meeting ID (PMI) meetings are not included.



Avoid using the same meeting link recurringly or using short or guessable passwords.



Profile  
Meetings  
Webinars  
Recordings  
**Settings**  
Account Profile

**Meeting**

Recording

Telephone

Schedule Meeting

In Meeting (Basic)

In Meeting (Advanced)

Email Notification

Other



**CONSIDER  
DISABLING**

Schedule Meeting

**Embed password in meeting link for one-click join**

Meeting password will be encrypted and included in the join meeting link to allow participants to join with just one click without having to enter the password.



**Require password for participants joining by phone**

A numeric password will be required for participants joining by phone if your meeting has a password. For meeting with an alphanumeric password, a numeric version will be generated.



**Mute participants upon entry**

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



**Upcoming meeting reminder**

Receive desktop notification for upcoming meetings. Reminder time can be configured in the Zoom Desktop Client.



Disabling embedded passwords adds inconvenience but can also deter crashers looking for the easiest meetings to disrupt.

- Profile
- Meetings
- Webinars
- Recordings
- Settings**
- Account Profile

**Meeting**   Recording   Telephone

- Schedule Meeting
- In Meeting (Basic)
- In Meeting (Advanced)
- Email Notification
- Other

**CONSIDER  
DISABLING**

In Meeting (Basic)

**Chat**  
 Allow meeting participants to send a message visible to all participants 

Prevent participants from saving chat 

You have enabled "Save chat messages from the meeting / webinar" in cloud recording. You can go to [Recording Settings](#) to turn it off and not share the chat along with the recording. 

**→**

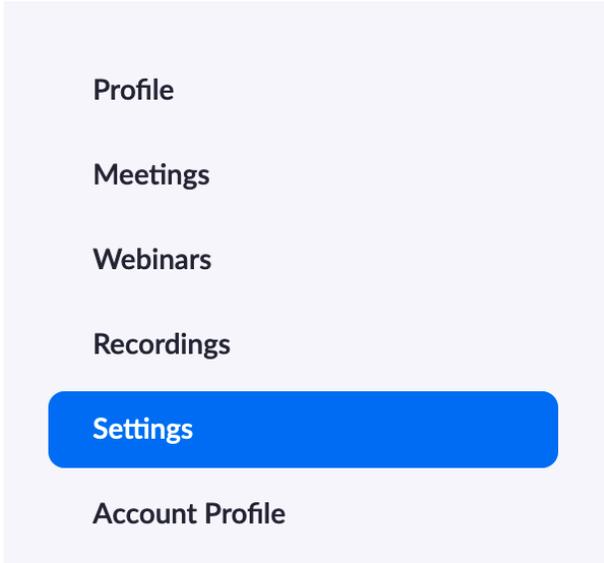
**Private chat**  
 Allow meeting participants to send a private 1:1 message to another participant. 

**→**

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

If you are not relying on the chat function, disable it to prevent crashers abusing it.





Meeting

Recording

Telephone

Schedule Meeting

In Meeting (Basic)

In Meeting (Advanced)

Email Notification

Other



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

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



Annotation

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



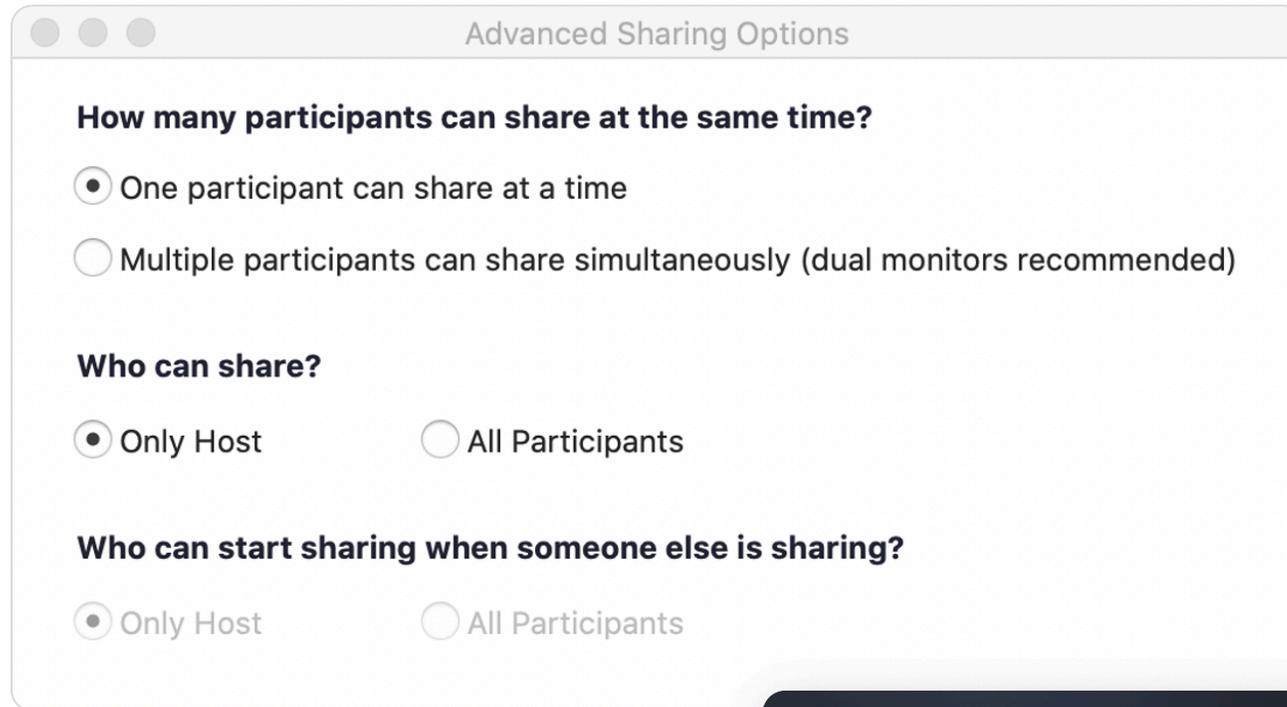
Whiteboard

Allow participants to share whiteboard during a meeting ?

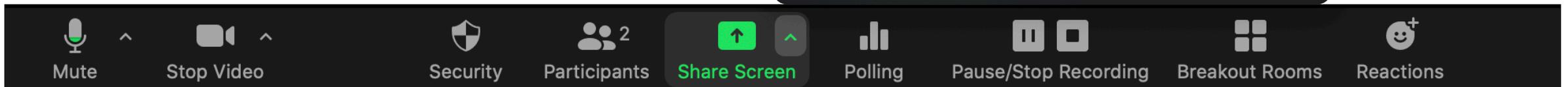
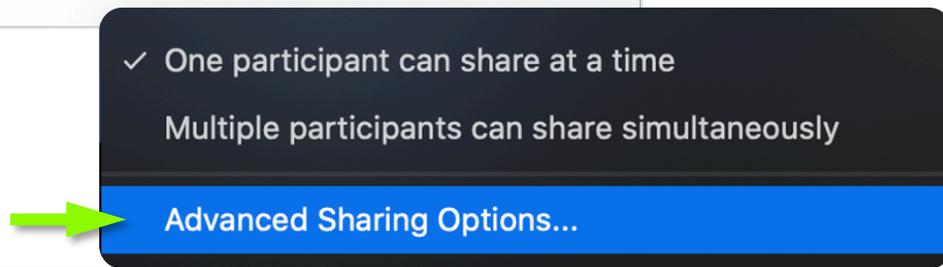


Adjusting these controls keeps crashers from sharing offensive visual content or drawing on the slides.





Note you can also change sharing permissions during the meeting



- Profile
- Meetings
- Webinars
- Recordings
- Settings**
- Account Profile

**Meeting**

Recording

Telephone

Schedule Meeting

In Meeting (Basic)

In Meeting (Advanced)

Email Notification

Other



**In Meeting (Basic)**

**Allow participants to rename themselves**

Allow meeting participants and webinar panelists to rename themselves.

**Hide participant profile pictures in a meeting**

All participant profile pictures will be hidden and only the names of participants will be displayed on the video screen. Participants will not be able to update their profile pictures in the meeting.

**In Meeting (Advanced)**



**Virtual background**

Allow users to replace their background with any selected image. Choose or upload an image in the Zoom Desktop application settings.

**CONSIDER ENABLING**



**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.



# 2 Use the Registration feature

[My Meetings](#) > Schedule a Meeting

## Schedule a Meeting

Topic

Meeting Setup Demo

Description (Optional)

Enter your meeting description

When

04/28/2020



8:30



AM



Recurring meeting

Registration

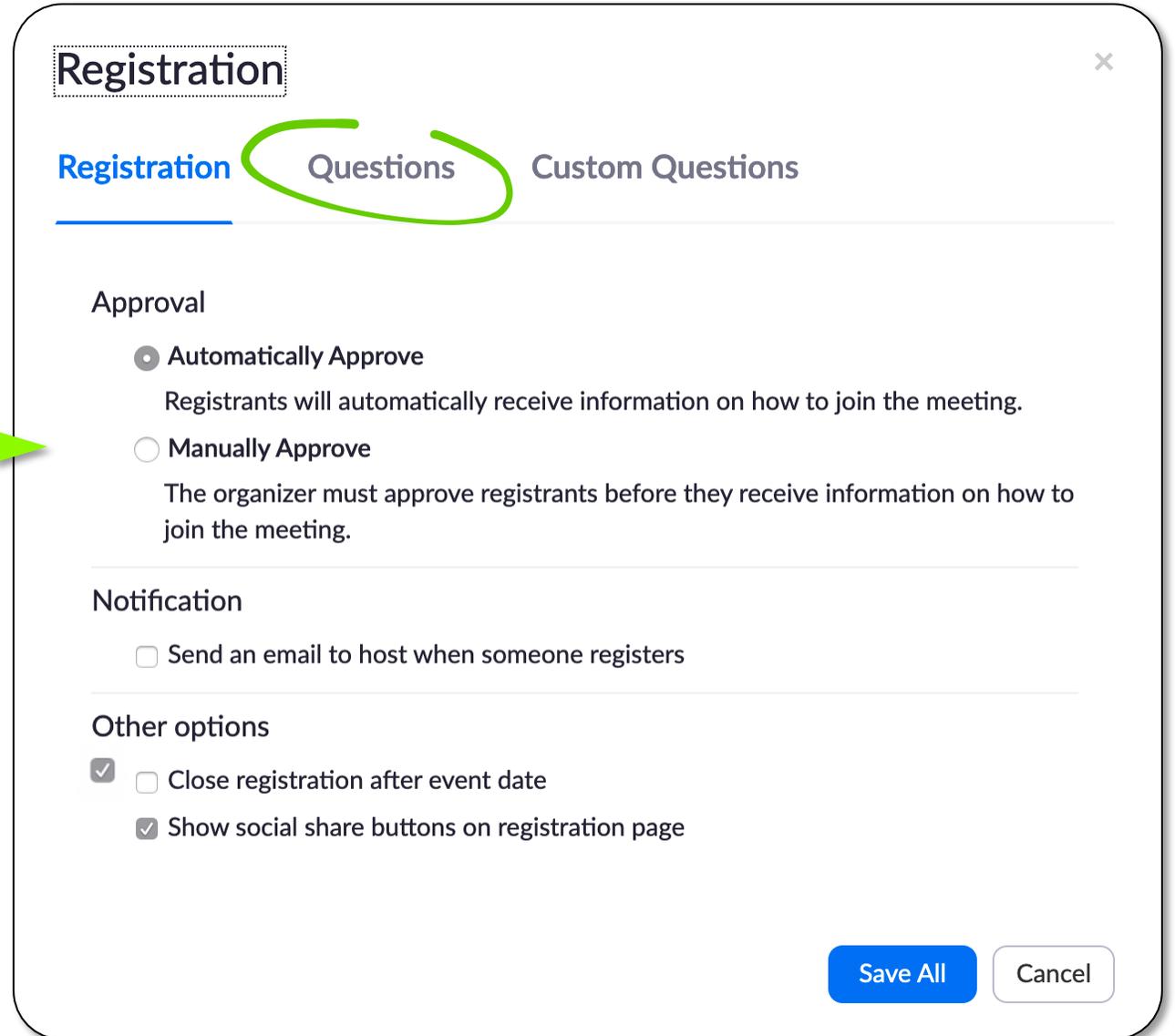
Required

Registration adds a step, but it lets you know ahead who will be on your call.



## 2 Use the Registration feature

Select Manually Approve if the number of people you anticipate does not make this burdensome.



**Registration** [Close]

**Registration** Questions Custom Questions

**Approval**

- Automatically Approve  
Registrants will automatically receive information on how to join the meeting.
- Manually Approve  
The organizer must approve registrants before they receive information on how to join the meeting.

**Notification**

- Send an email to host when someone registers

**Other options**

- Close registration after event date
- Show social share buttons on registration page

**Save All** **Cancel**

## 2 Use the Registration feature

Require fields like Zip Code and Organization so that anomalies stand out and supply data points for verifying people you don't recognize.

NOTE: You can select the Questions & Comments field to solicit input ahead of your meeting.

First Name and Email Address required.

<input type="checkbox"/>	Field	<input type="checkbox"/> Required
<input checked="" type="checkbox"/>	Last Name	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Address	<input type="checkbox"/>
<input type="checkbox"/>	City	<input type="checkbox"/>
<input type="checkbox"/>	Country/Region	<input type="checkbox"/>
<input type="checkbox"/>	Zip/Postal Code	<input type="checkbox"/>
<input type="checkbox"/>	State/Province	<input type="checkbox"/>
<input type="checkbox"/>	Phone	<input type="checkbox"/>
<input type="checkbox"/>	Industry	<input type="checkbox"/>
<input type="checkbox"/>	Organization	<input type="checkbox"/>
<input type="checkbox"/>	Job Title	<input type="checkbox"/>
<input type="checkbox"/>	Questions & Comments	<input type="checkbox"/>



# 2 Use the Registration feature

Click [View](#) to check who has registered and identify those who are unfamiliar.

[My Meetings](#) > Manage "Conducting Zoom Calls with Confidence"



**Registration**

Email Settings

Branding

Poll

Manage Attendees

Registrants: 55

[View](#)

Registration Options

Automatically Approved

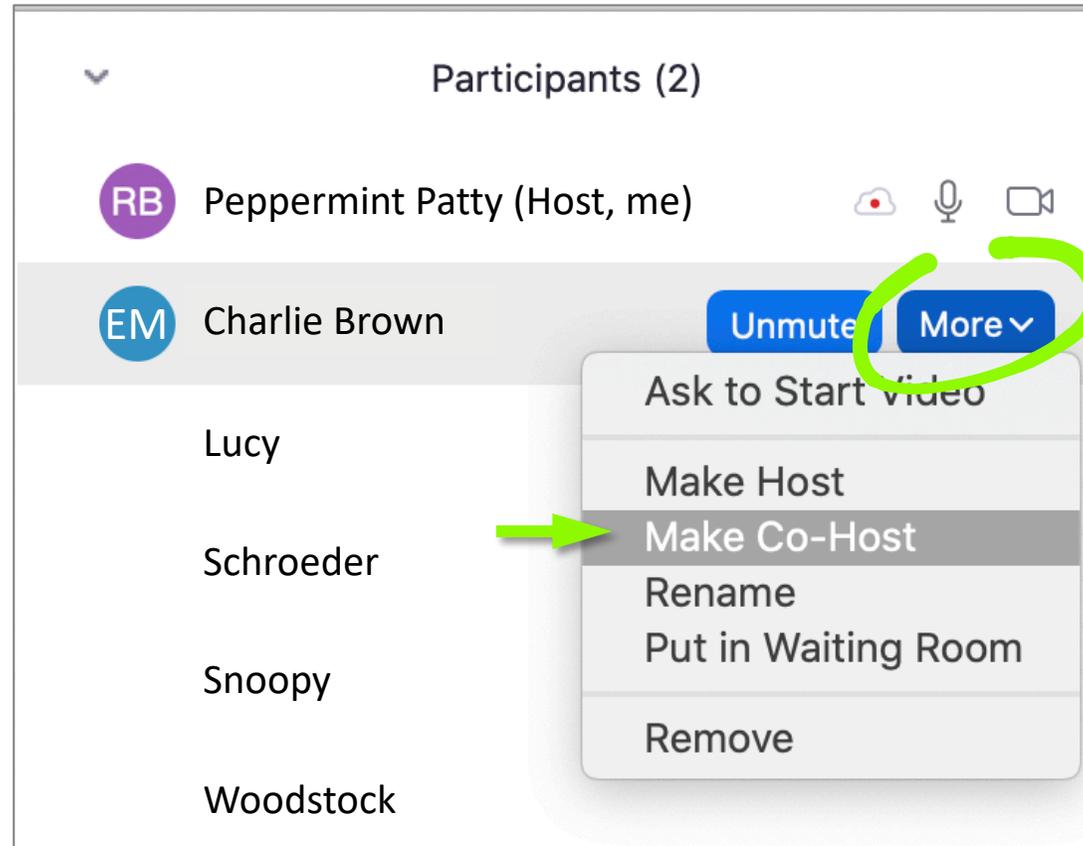
[Edit](#)

× Send an email to host

✓ Close registration after meeting date

# 3 Appoint a bouncer

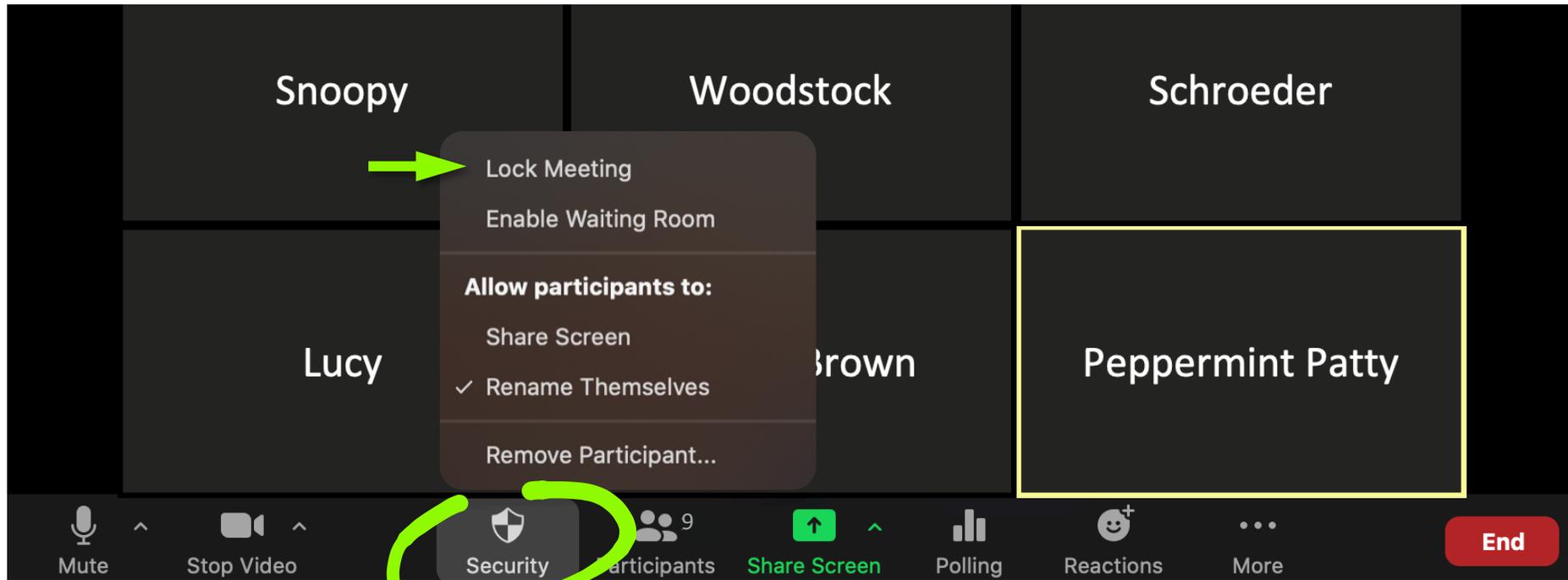
Identify co-hosts and assign them distinct tasks, such as muting open mics or removing disruptive people.



# 4 Lock the room

Use the Lock feature if everyone you need has arrived in the meeting, or if you can afford to exclude late-comers.

NOTE: If someone drops due to connection problems, they won't be able to rejoin.



# 5 Record your call

Even if you don't record the whole meeting, you or a co-host should hit record if a crasher engages in unwelcome behavior.

Video footage, and any relevant chat transcript, serves as evidence against crashers.



# Five Best Practices

---

1 Adjust your account settings < *Block unwanted visuals*  
*Restrict written communication*

2 Use the Registration feature

3 Appoint a bouncer

4 Lock the room

5 Record your call

# How to report an incident

If someone explicitly threatened you or your organization with violence, call 911.

Report Internet crime of any sort, including unauthorized access to a Zoom meeting, by filing a complaint with FBI's Internet Crime Complaint Center: [www.ic3.gov](http://www.ic3.gov)

Report hate speech or a hate incident to the Anti-Defamation League: <https://www.adl.org/reportincident>