Online Zoom Meeting Hosting Guidelines

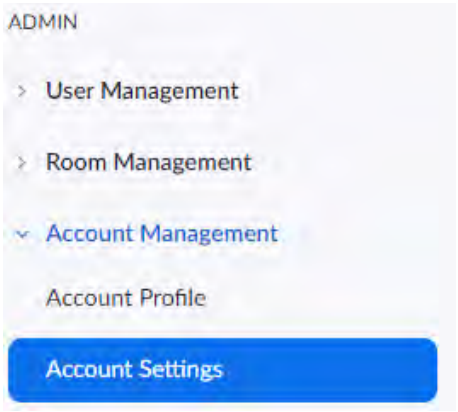
Purpose: to protect everyone's anonymity, ensure smooth running of meetings, protect data & privacy.

1. Zoom settings

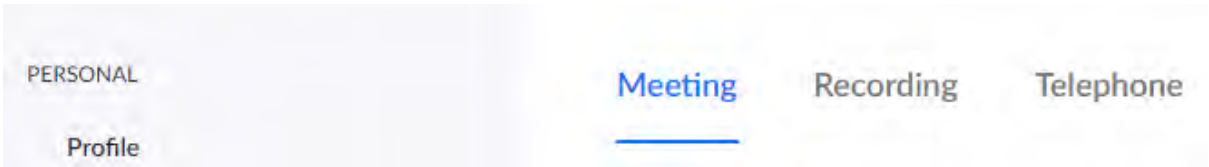
(needs to be done only once per account prior to setting up a meeting, not before every meeting)

On the Zoom website, log in with the account you use to host meetings. We suggest making settings in two areas; settings under your user profile and the admin account.

a. Navigate to ADMIN -> ACCOUNT MANAGEMENT -> ACCOUNT SETTINGS



b. In the center page you should now see the three tabs: Meeting (in blue), Recording, Telephone.



c. Under the Meeting tab set the sliders according to the following:

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

Join before host
Allow participants to join the meeting before the host arrives

Use Personal Meeting ID (PMI) when scheduling a meeting

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.

Only authenticated users can join meetings from Web client
The participants need to authenticate prior to joining meetings from web client

Meeting password requirement

- [ ] Have a minimum password length
- [ ] Have at least 1 letter (a, b, c...)
- [ ] Have at least 1 number (1, 2, 3...)
- [ ] Have at least 1 special character (!, @, #...)
- [ ] Only allow numeric password

Bypass the password when joining meetings from meeting list
When Zoom Rooms join a scheduled meeting on its meeting list, users do not need to manually enter the meeting password.

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

Calendar and Contact Integration
Integrate your calendar and contact service, such as Google account, Outlook, or Exchange with Zoom client.

Office 365 users can consent to enterprise applications accessing company data on their behalf
If turned off, the Office 365 administrator will need to consent to calendar integrations on behalf of the company. As an administrator, please choose the same settings configured in Office 365. View the settings on Office 365

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

Enforce to use OAuth 2.0 only for authenticate Office365 calendar integration
Enabling this setting will force users and Zoom Rooms to authenticate calendar service

Add watermark

Each attendee sees a portion of their own email address embedded as a watermark in any shared content and on the video of the participant who is sharing their screen. This option requires enabling "Only signed-in users can join the meeting" or "Only signed-in users with specified domains can join meetings".

Add audio watermark

If an attendee records the meeting, their personal information will be embedded in the audio as an inaudible watermark. This option requires enabling "Only signed-in users can join the meeting" or "Only signed-in users with specified domains can join meetings".

If you want to get details of who recorded a Zoom meeting, please submit your request online. The email content needs to include:

- Meeting Information (Meeting ID, date and time of occurrence)
- The recording file (video or audio file)

Always display "Zoom Meeting" as the meeting topic

Hide actual meeting topic and display "Zoom Meeting" for your scheduled meetings

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.

Require a password for meetings which have already been scheduled

Require a password for instant meetings

A random password will be generated when starting an instant meeting

Require a password for Personal Meeting ID (PMI)

- ( ) Only meetings with Join Before Host enabled
- (•) All meetings using PMI

Require a password for Room Meeting ID (Applicable for Zoom Rooms only)

A password will be generated for Room Meeting ID and participants require the password to join the 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.

Meeting password requirement

- [ ] Have a minimum password length
- [ ] Have at least 1 letter (a, b, c...)
- [ ] Have at least 1 number (1, 2, 3...)
- [ ] Have at least 1 special character (!, @, #...)
- [ ] Only allow numeric password

Bypass the password when joining meetings from meeting list

When Zoom Rooms join a scheduled meeting on its meeting list, users do not need to manually enter the meeting password.

Mute participants upon entry

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

Calendar and Contact Integration

Integrate your calendar and contact service, such as Google account, Outlook, or Exchange with Zoom client.

Office 365 users can consent to enterprise applications accessing company data on their behalf

If turned off, the Office 365 administrator will need to consent to calendar integrations on behalf of the company. As an administrator, please choose the same settings configured in Office 365. View the settings on Office 365

Upcoming meeting reminder

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

Enforce to use OAuth 2.0 only for authenticate Office365 calendar integration

Enabling this setting will force users and Zoom Rooms to authenticate calendar service

In Meeting (Basic)

Require Encryption for 3rd Party Endpoints (H323/SIP)

Zoom requires encryption for all data between the Zoom cloud, Zoom client, and Zoom Room. Require encryption for 3rd party endpoints (H323/SIP).

Chat

Allow meeting participants to send a message visible to all participants

Prevent participants from saving chat

Private chat

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

Auto saving chats

Automatically save all in-meeting chats so that hosts do not need to manually save the text of the chat after the meeting starts.

Play sound when participants join or leave

Play sound when participants join or leave

File transfer

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

Feedback to Zoom

Add a Feedback tab to the Windows Settings or Mac Preferences dialog, and also enable users to provide feedback to Zoom at the end of the meeting

Display end-of-meeting experience feedback survey

Display a thumbs up/down survey at the end of each meeting. If participants respond with thumbs down, they can provide additional information about what went wrong.

Co-host

Allow the host to add co-hosts. Co-hosts have the same in-meeting controls as the host.

Polling

Add 'Polls' to the meeting controls. This allows the host to survey the attendees.

Always show meeting control toolbar

Always show meeting controls during a meeting

Show Zoom windows during screen share

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

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

Nonverbal feedback
Participants in a meeting can provide nonverbal feedback and express opinions by clicking on icons in the Participants panel.

Allow removed participants to rejoin
Allows previously removed meeting participants and webinar panelists to rejoin

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)

Breakout room
Allow host to split meeting participants into separate, smaller rooms

Remote support
Allow meeting host to provide 1:1 remote support to another participant

Closed captioning
Allow host to type closed captions or assign a participant/third party device to add closed captions

Save Captions
Allow participants to save fully closed captions or transcripts

Far end camera control
Allow another user to take control of your camera during a meeting

Group HD video
Activate higher quality video for host and participants. (This will use more bandwidth.)

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

Identify guest participants in the meeting/webinar
Participants who belong to your account can see that a guest (someone who does not belong to your account) is participating in the meeting/webinar. The Participants list indicates which attendees are guests. The guests themselves do not see that they are listed as guests.

Auto-answer group in chat
Enable users to see and add contacts to 'auto-answer group' in the contact list on chat. Any call from members of this group will be automatically answered.

Peer to Peer connection while only 2 people in a meeting
Allow users to directly connect to one another in a 2-person meeting.

Only show default email when sending email invites
Allow users to invite participants by email only by using the default email program selected on their computer

Use HTML format email for Outlook plugin
Use HTML formatting instead of plain text for meeting invitations scheduled with the Outlook plugin

DSCP marking
Determine classification for network traffic. Enable DSCP marking for signaling and media packets. (Default is 56 for audio, 40 for video, and 40 for signaling.)

Allow users to select stereo audio in their client settings
Allow users to select stereo audio during a meeting

Allow users to select original sound in their client settings
Allow users to select original sound during a meeting

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

Show a "Join from your browser" link
Allow participants to bypass the Zoom application download process, and join a meeting directly from their browser. This is a workaround for participants who are unable to download, install, or run applications. Note that the meeting experience from the browser is limited

Allow live streaming meetings

Allow Skype for Business (Lync) client to join a Zoom meeting
Allow internal or external Skype for Business (Lync) client to connect to a Zoom meeting. Learn more

Email Notification

When a cloud recording is available
Notify host when cloud recording is available

When attendees join meeting before host
Notify host when participants join the meeting before them

When a meeting is cancelled
Notify host and participants when the meeting is cancelled

When an alternative host is set or removed from a meeting
Notify the alternative host who is set or removed

When someone scheduled a meeting for a host
Notify the host there is a meeting is scheduled, rescheduled, or cancelled

When the cloud recording is going to be permanently deleted from trash

Notify the host 7 days before the cloud recording is permanently deleted from trash

When the meeting duration exceeds the limit

Notify the specified users when the meeting duration exceeds the limit

Admin Options

Blur snapshot on iOS task switcher

Enable this option to hide potentially sensitive information from the snapshot of the Zoom main window. This snapshot display as the preview screen in the iOS tasks switcher when multiple apps are open.

Display meetings scheduled for others

If disabled, users will only see their meetings even if they have schedule-for privilege for others

Use content delivery network (CDN)

Allow connections to different CDNs for a better web browsing experience. All users under your organization will use the selected CDN to access static resources.

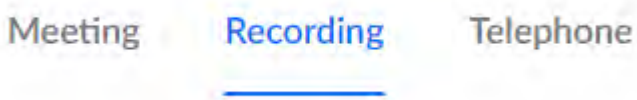
Allow users to contact Zoom's Support via Chat

Show Zoom Help badge on the bottom right of the page

Show one person meetings on Reports

Meetings with only one person will also be displayed on reports.

d. Still in the ADMIN settings navigate to the RECORDINGS tab



e. set the sliders according to the following:

Local recording

Allow hosts and participants to record the meeting to a local file

Cloud recording

Allow hosts to record and save the meeting / webinar in the cloud

Automatic recording

Record meetings automatically as they start

Prevent hosts from accessing their cloud recordings

By turning on this setting, the hosts cannot view their meeting cloud recordings. Only the admins who have recording management privilege can access them.

Cloud recording downloads

Allow anyone with a link to the cloud recording to download

IP Address Access Control

Allow cloud recording access only from specific IP address ranges

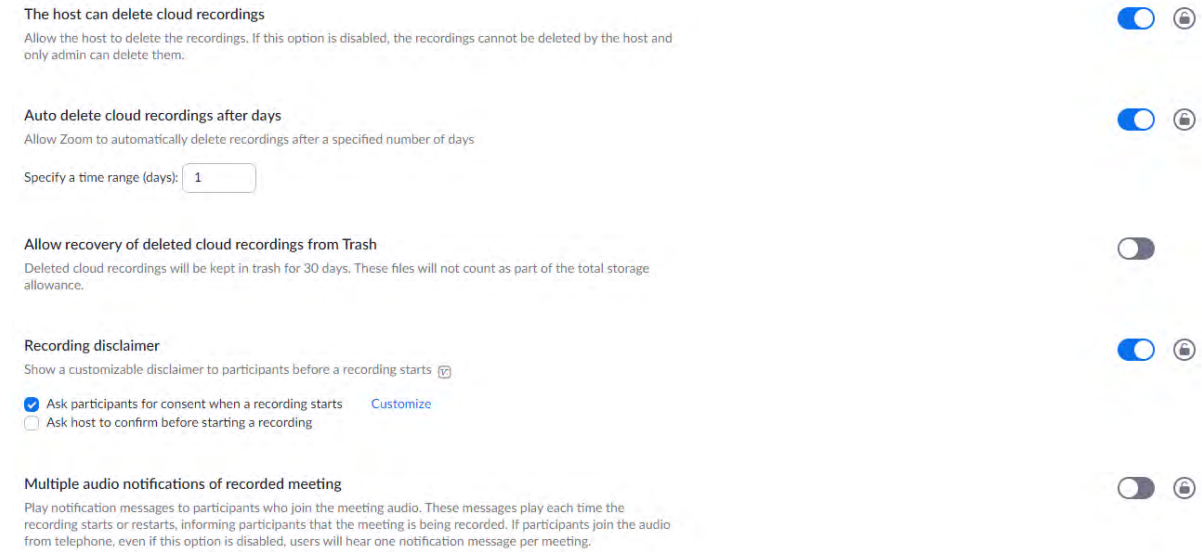
Only authenticated users can view cloud recordings

The viewers need to authenticate prior to viewing the cloud recordings, hosts can choose one of the authentication methods when sharing a cloud recording.

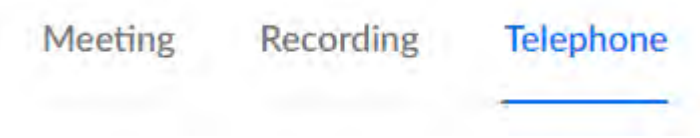
Require password to access shared cloud recordings

Password protection will be enforced for shared cloud recordings. A random password will be generated which can be modified by the users. This setting is applicable for newly generated recordings only.

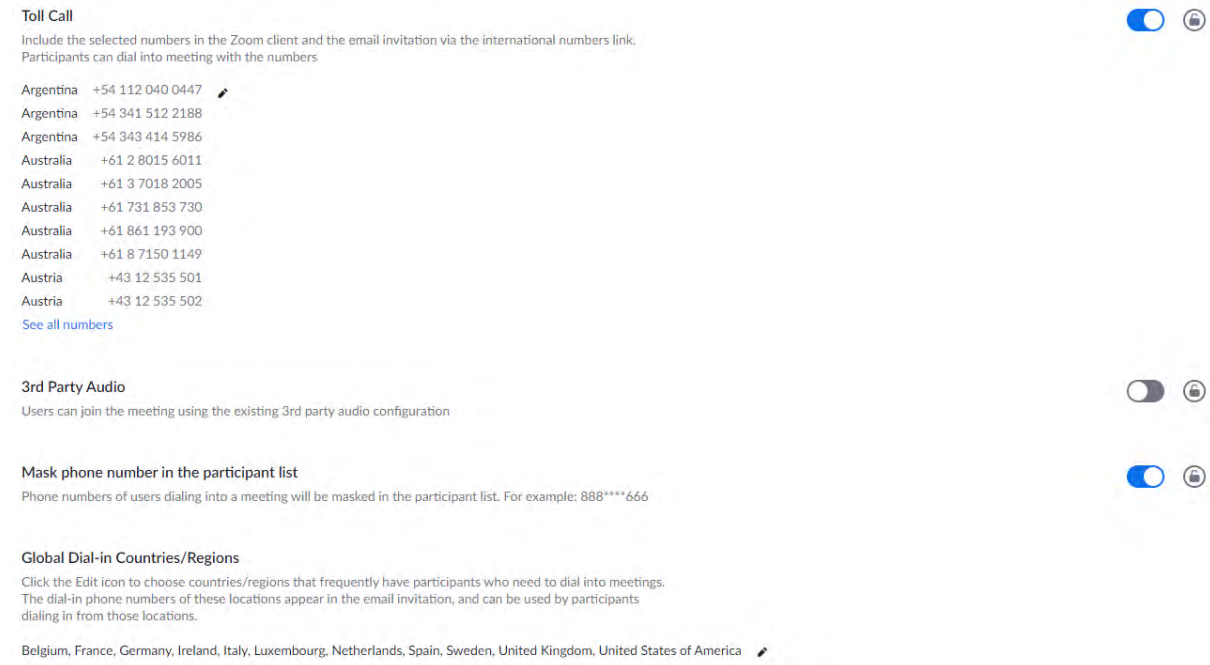
Require a password to access the existing cloud recordings



f. Still in the ADMIN settings navigate to the TELEPHONE tab



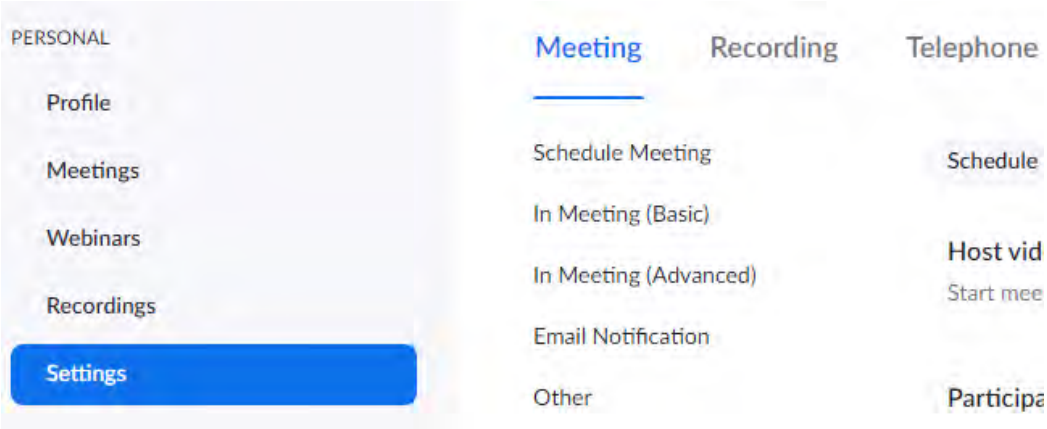
g. set the sliders according to the following:



Global Dial-in Countries/Regions

Select all the countries from the list on the left hand side, they will appear on the right. Click & drag a country to the top that you wish to be at the top of the phone numbers list. This will set the default region.

h. Navigate to PERSONAL-> SETTINGS -> Meetings



i. Verify/Set all of the above Meeting, Recording and Telephone settings (a. - g.) here as well.

2. Meeting Setup

- Topic
  - Choose a meeting name that preferably does not include AA. This is for added anonymity if attending meetings in public spaces

- Disable: Registration
- Password: select require meeting password
- Video:
    - Enable Video OFF for Host and Participants (it means video is switched off when host or participant joins the meeting but can be turned on after that)
- Audio:
    - Enable: Both
        - Click Edit to update the country list if needed.
- Meeting Options:
    - Disable: Enable join before host *(This prevents people from joining the group before a host logs in. See "Enable Waiting Room")*
    - Enable: Mute participants upon entry
    - Enable: Enable Waiting Room *(helps you see who is trying to enter your meeting by placing them in a separate area at the top of your participants list until you let them into the main meeting. It also prevents you from getting flooded with disruptive people because it gives you a pre-emptive chance to see who is trying to enter your meeting. Wouldn't it be nice to be able to stop someone from naming themselves, say, "GateKrasherFU" or keep known bad actors from even entering your meeting at all in the first place? You'd also probably not want a participant with a naked or pornographic profile pic... Waiting Room let's you do just that. You're not going to catch everybody, of course but even that occasional bad actor that does get in won't be able to unmute themselves, upload files, take over screen share or chat anyway. And who knows, maybe they might even get sober? Of course, nothing prevents them from raising their hand and once called upon to start their obscene gibberish, but at least it's only one person, very easy to ban and not let back in for the rest of the meeting. Just like what happens at real meetings sometimes.)*
    - Disable: Only authenticated users can join

3. Suggested practices during a meeting

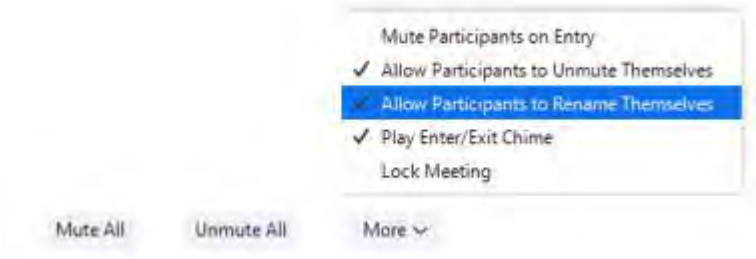
- **Ask someone to be your Co-Host (suggest 1 co-host per 20 participants)**

  This is a great way to do service.
  To make a participant co-host select their name in the participant list, click on MORE and make them co-host.

  Suggest host and co-hosts to divide tasks, prior to the meeting commencing:
  - admitting participants into the meeting and scanning usernames, potentially refusing to admit on the basis of offensive usernames or profile pictures.
  - monitor video feeds
  - manage participants (rename, remove…)
  - monitor chat (host only)
  - change chat to host only in the event of an attack (host only)

- **Disable: User Rename**

  A bad actor can post something nasty in your chat and then quickly rename themselves. Their posted chat will retain the old name but they will already be cloaked with their new name as you try to find them and ban them.



- **Video participation and names**

  Some may not have their video on. Others may show their full name in the participant box unintentionally. Using Video is not compulsory and participants are free to use whatever name they please. We suggest participants use video for an immersive experience for everyone.

  We suggest participants type their first name into the system when they join. It can be checked on their own screen and in the participant list. We suggest the host say and/or writes via chat message before meeting starts :

  "Using video during the meeting is your personal choice. We encourage you to enable video for a better meeting experience. We ask that you use your first name as your participant name, check your Zoom screen and/or participant box for your current username. Especially if it shows 'iphone' 'samsung' … etc., contact the host via the chat box or introduce yourself before the meeting requesting the host to rename you. The rename feature has been disabled for participants for security reasons. Before your next meeting we encourage you to learn how to name yourself ahead of joining. Here is a short How-To guide https://bit.ly/34r1ES7.'

- **Participation calls via Landline**

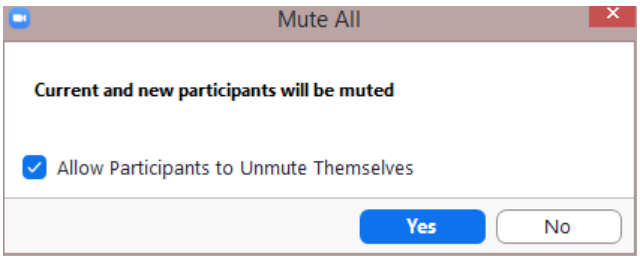
  Dialed in participants may not be able to mute/unmute themselves because their (landline) phone doesn't support it or they may be visually impaired. It is suggested that hosts ask the caller whether they can unmute themselves. If not they stay unmuted if at all possible throughout the entire meeting or suggest to keep them muted until invited by the host to share. Definitely ask them to introduce themselves so you can rename them in the participant box.

4. What to do if a meeting is attacked

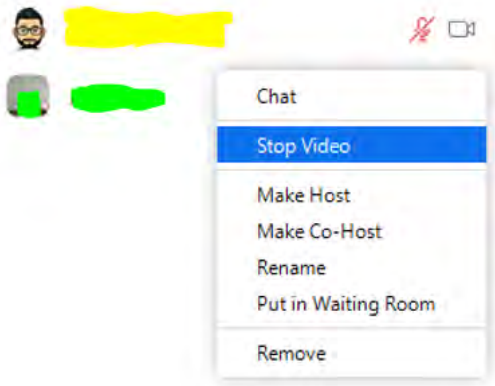
Expect explicit, obscene porn, lewd images, foul language and verbal abuse (often directed at the lead/chairperson to invoke chaos). First and foremost, remain calm, having expected to experience this. Shock is their primary goal. If you are calm, you can act quickly and decisively instead of react.

Having already blocked their ability to video-share and send files which is their primary weapon, the only thing that intruders can do now is post in the chat, show live video from their device, and/or verbally abuse, which they seem to like to do in gangs of many in order to rapidly overcome a meeting. Depending on whether the abuse is mainly verbal or video start taking action:

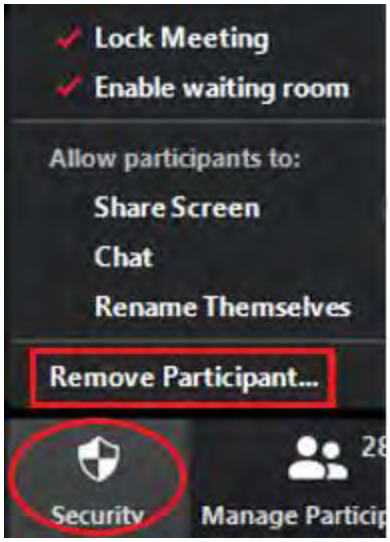
1. **Mute ALL** quickly go over to the participant list and immediately click the “Mute All” button. In the popup window unselect ‘Allow Participants to Unmute Themselves’.



2. **Stop their video** go to the participant list and click MORE on their name (if their main offence is video you may want to do this first)



3. Click the **Security** button at the bottom of your Zoom Window



- **ENABLE Lock Meeting**
- **DISABLE Chat**
- **DISABLE Rename Themselves**
- **REMOVE Participants**
  - This will add a red REMOVE button next to each participant in the participant list

4. This essentially gives Zoom-bombers no reason to stay on at this point, and they likely will start dropping once they see that you know how to take away their ability to disrupt a meeting. Under normal meeting circumstances, you want members to be able to mute and unmute themselves in order to engage more naturally with the group as we would in face-to-face meetings, so blocking attendees from unmuting themselves should be a temporary action until the intruders have left.

5. Feel free at any time, unmuting yourself and your co-hosts, to inform the audience what you're doing (while attendees remain force-muted, things tend to get awkward), putting a temporary hold on the meeting while the problem is being addressed. Let them know to **please raise their hand** if they wish to speak and that the meeting will restart shortly.

6. During this hold period, have your co-host(s) along with you, click on "Participants", go through and "**Remove**" all the obviously bad actors. You can also distinguish most of them from the names or images they post for themselves. Sometimes they will have video on, being their only chance left to show a shock video, with the camera pointing somewhere random like a ceiling fan. If you are unsure and don't want to drop someone who may be an actual AA member, unmute them and request that they identify themselves. Trolls either won't identify or they will say something making it obvious they are a troll, or they'll just stay silent or drop altogether.

7. Once you've experienced this a few times, it will be easier and troll groups will find your meeting "no fun" and will move on. If we get enough of our groups shutting them down, they will stop having any reason to Zoom-bomb our AA meetings.

8. Once all culprits have been successfully dealt with, feel free to allow participants to **unmute themselves** again and **re-enable the chat**.

9. Keep the meeting locked to prevent culprits from joining the meeting again. Anyone who wants to join and finds a meeting locked can communicate this in the WhatsApp group chat.