# AA District 2 Zoom meeting guide

## AA District 2 Zoom security measures update

*Updates: 27 April 2020*

To reduce malicious disruptions in AA meetings on the Zoom platform, we are enacting the following measures:

## Temporary measures to stabilize meetings:

- Tell participants at the beginning of meeting about issues and new measures
- Enable “mute participants on entry”
- Enable waiting rooms
    - Ask anyone we don’t know to briefly turn on their video or talk to them for a moment before entering
    - Consider enabling this 5 min after meeting start?
- Disable “Allow participants to unmute themselves”
    - Have chairs tell participants to use “raise hand” and call on people and we will unmute them to share
- Disable “allow participants to chat with other guests” and only allow chat to host
- Use multiple co-hosts in meetings, at least one per page
- If meeting is to be shut down due to attacks, host must choose “end the meeting for everyone” or attackers and all attendees will be able to remain in the meeting

## Consider updating community:

- Let people know security changes that have been made
- Allow for public commenting
- Dissuade panic and let them know what to do if there’s a problem

## Next phase after disruptions have been reduced/eliminated:

- Revisit measures that are most restrictive, including
    - Re-opening chat

    - “Allow participants to un-mute themselves.
- Consider whether waiting rooms are helpful to keep
- Consider whether multiple co-hosts are helpful to keep

## Practice emergency measures:

Anyone who wants to, participate in practicing emergency measures, including:

- **Mute All Attendees and disable self-unmuting**
- Turn off an Attendee’s video and remove them
- Lock the meeting

## Other considerations:

I don’t believe that at this time it’s helpful to use other measures which are geared toward identifying bad actors to report to Zoom, such as:

- Enable watermarking
- Require participants to log in
- Require participants to enable video
- Talk to Area,  other nearby areas and how can we be of service to them, share wisdom?

*Updates: 3 April 2020*

District 2 has adopted the following guidelines for security for online meetings on the Zoom format. These configurations are in place on the district Zoom accounts. If you have your own Zoom account for your group, consider adopting these settings.

These recommendations were adopted from the following sources. GSO has not published specific guidelines for Zoom at this time.

- NYIG Toolkit for Handling Unwanted Meeting Disruptions
- Zoom blog
- GSO  press release on Groups Using Digital Platforms

## Best practices Zoom security settings:

(details with screenshots here)

- Disable “Screen Sharing” for all but the Host

- Disable chat “File transfer”
- Disable “Allow removed participants to rejoin"
- “Allow Host to put Attendee on Hold”
- Disable video recording

## Emergency measures:

If your meeting should face unwanted disruptions, here are some emergency measures you can immediately take (details with screenshots here):

- **Mute All Attendees and disable self-unmuting**
- Turn off an Attendee’s video and remove them
- Lock the meeting

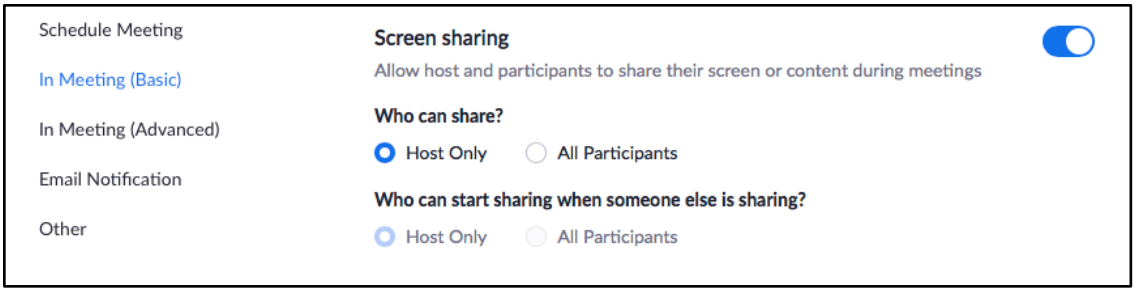
## Other considerations:

- If people are concerned about attendees without video, you might require video on for everyone, or for a short time, to protect the anonymity of all and to ensure everyone’s good intent. Or perhaps the chairperson might greet unknown persons without video before the meeting.

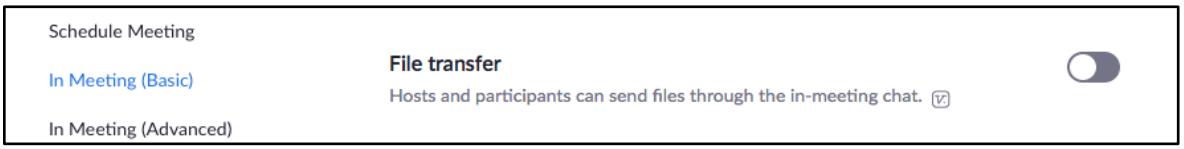
## Best practices Zoom security settings detail

All found in Zoom Admin Configuration on the Zoom website:

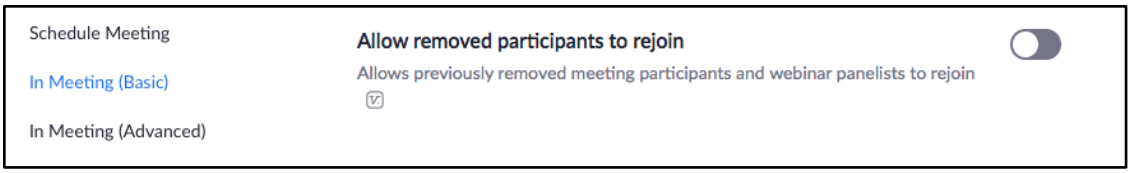
- Under “Screen sharing,” select “Host only”:



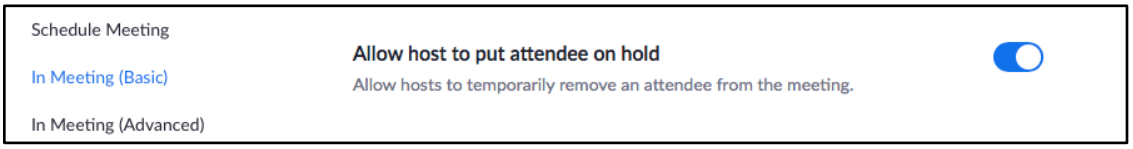

- Disable chat “File transfer”



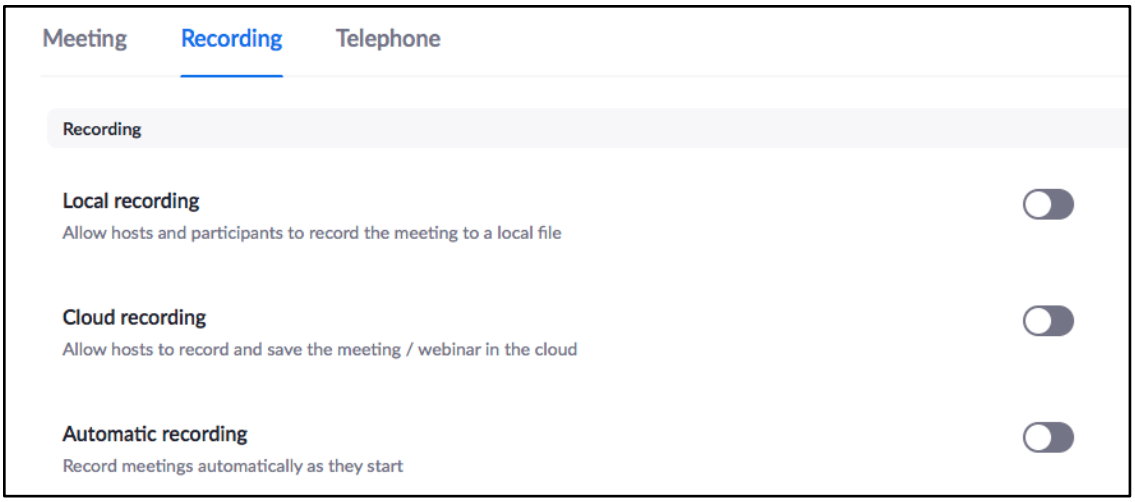

    - Disable “Allow removed participants to rejoin"




- "Allow Host to put Attendee on Hold"




- Disable video recording

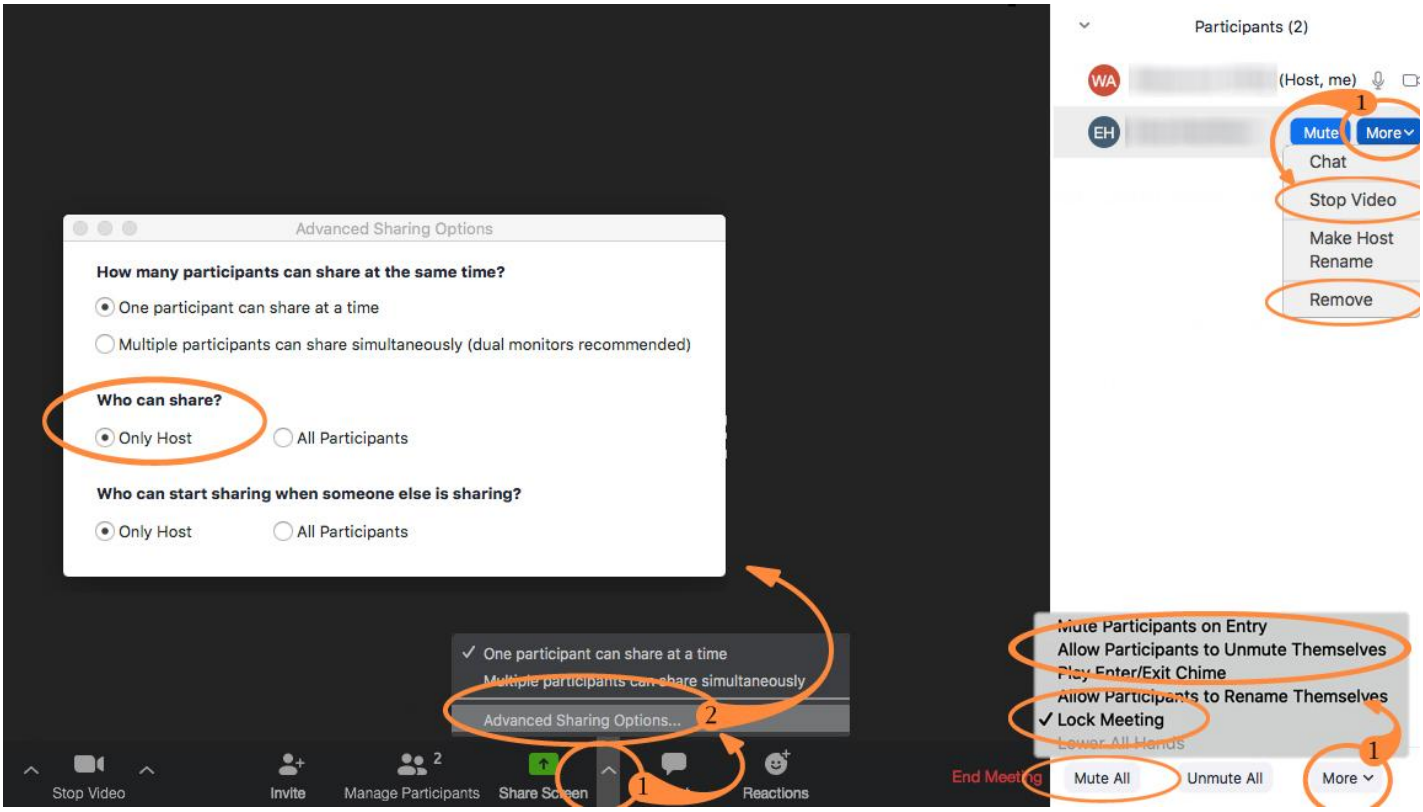



## Emergency measures detail

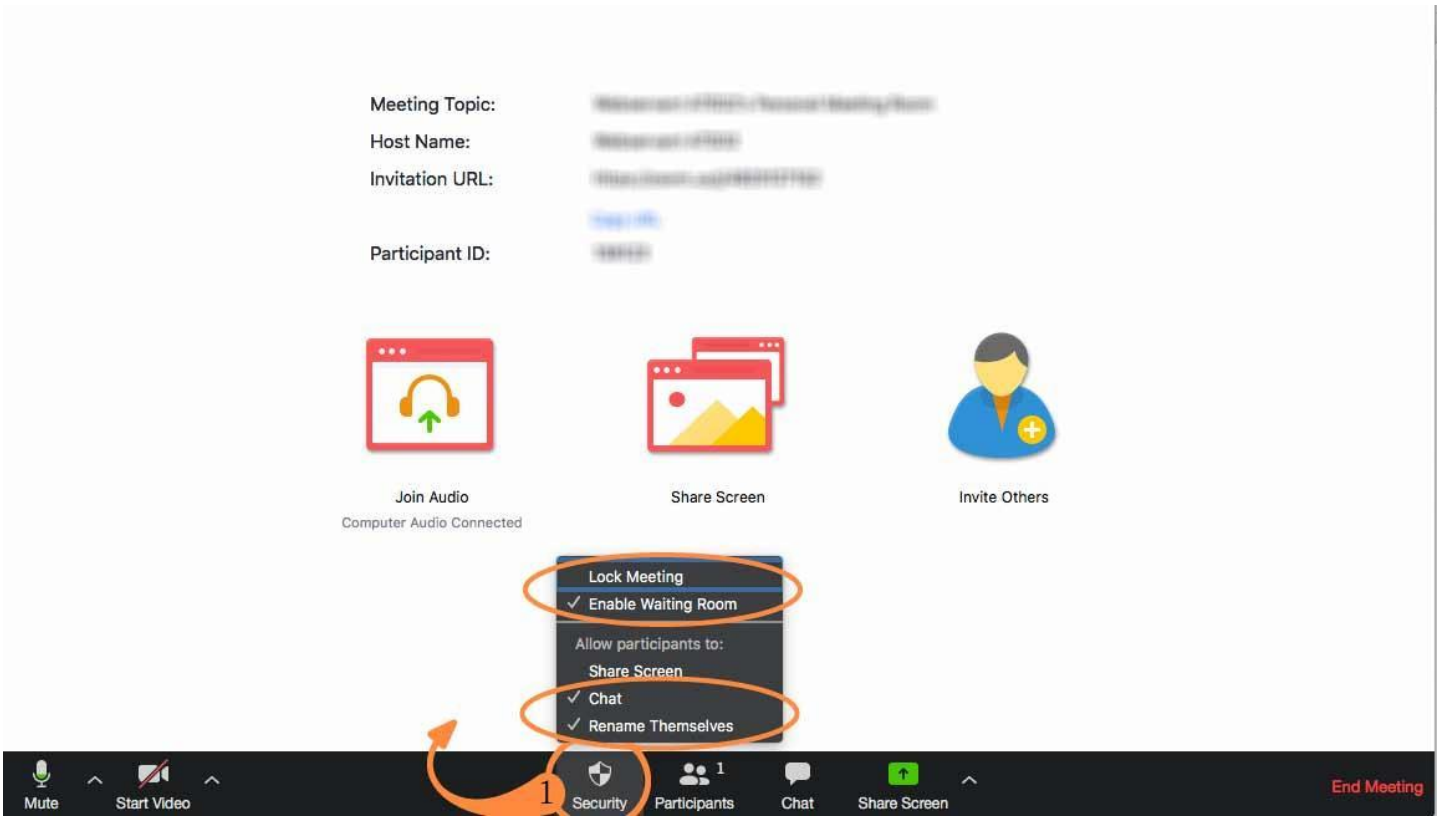
There are three areas the "host" can use to take control of the room: One in Advanced Sharing Options and the other two are found in the Participants column (if you don't see this, click "Manage Participants").

Remember that the "host" can always assign the host role to another person in the room.

- **Mute All Attendees and disable self-unmuting**
- Turn off an Attendee's video and remove them
- Lock the meeting




New “Security” button for Hosts, added in April 2020:


Meeting Topic:
Host Name:
Invitation URL:
Participant ID:
Join Audio
Computer Audio Connected
Share Screen
Invite Others
Lock Meeting
Enable Waiting Room
Allow participants to:
Share Screen
Chat
Rename Themselves
Mute
Start Video
1
Security
Participants
Chat
Share Screen
End Meeting