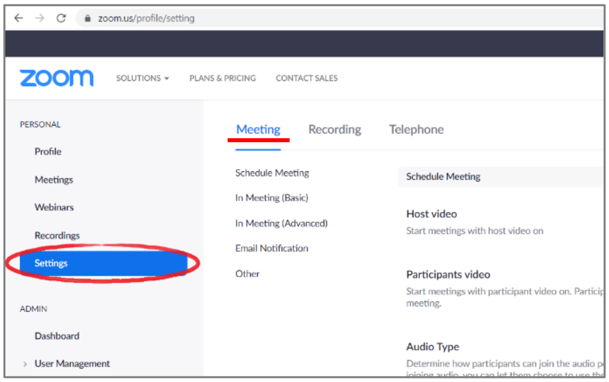
Zoom MEETING Safety Settings

There are a couple different places where you can manage safety settings when creating your Zoom meeting link, and before the meeting takes place. Then there are a few additional safety measures you can click once you are in the room and the meeting has started. The breakdowns below walk you through these settings step-by-step in order as you should see them in on your screen.

All of these settings are recommended for optimal security for a basic council meeting. If you are wanting a more advanced council meeting, or a CLE webinar, please contact the Sections Department for additional information and a different list of settings.



Schedule Meeting

Host video
Start meetings with host video on

Participants video
Start meetings with participant video on. Particip
meeting.

Audio Type
Determine how participants can join the audio p

Set-up Settings (found in your My Account page, click Settings)

- Meeting Tab
  - Host Video ON
  - Participants Video ON
  - Audio Type TELEPHONE AND COMPUTER AUDIO
  - Join before host OFF
  - Personal Meeting ID OFF
  - Only authenticated users can join meetings OFF
    If this feature is enabled, it is an added level of security, but requires all of your participants to have a verified Zoom account. Some members of your section may not feel comfortable creating an account and giving their personal information to Zoom. For a basic council meeting, if you are enabling all other recommended security features, enabling only authenticated users is not strictly required.
  - Only authenticated users can join meetings from Web client OFF
  - Require a password when scheduling new meetings ON
  - Require a password for instant meetings ON
  - Embed password in meeting link for one-click join OFF
    If this feature is enabled, meeting password will be encrypted and included in the originally sent 'join meeting' link, to allow participants to join with just one click without having to enter the password. This becomes confusing to some attendees because the invitation will include a password, but they will not be prompted to enter it. Though the meeting is secure, they will question its security. We recommend skipping the confusion turning off this feature.
  - Require password for participants joining by phone ON
    Zoom-bombers can enter a meeting by call-in only as well, so it is highly recommended you require a password for all attendees, including call-in only. This function will generate a numeric password to be required for participants joining by phone.
  - Mute participants upon entry OFF
    We find automatically muting participants upon meeting entry causes confusion. It is better to allow them to mute themselves, or announce before the meeting starts that the host/co-host will now mute everyone.
  - Upcoming meeting reminder OPTIONAL
    If enabled, this feature will send the host only, a desktop notification popup reminder.
  - Require encryption for 3rd party endpoints (SIP/H.323) OFF
    If this feature is enabled, H.323/SIP devices will be required to use additional encryption when dialing in to the meeting. Most attendees will not know how to comply, or what that means. By default, Zoom already employs standard encryption for all data, so if all other recommended safety features are enabled, you are not required to enable 3rd party endpoint encryptions.
  - Chat ON
    This is an optional feature that you can turn off for larger meetings if desired. But for a basic council meeting, if all other safety recommendations are followed, allowing participants to chat is appropriate.

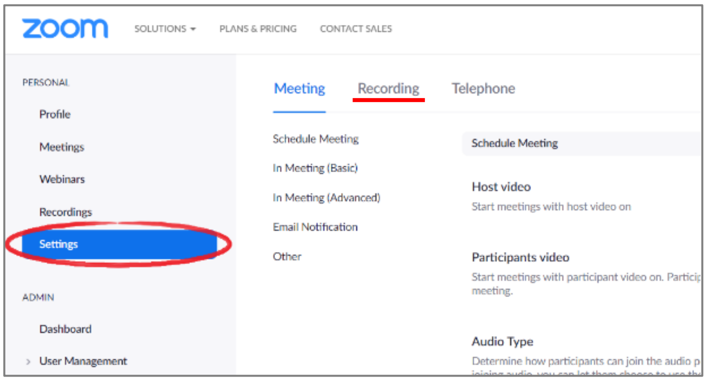
- Prevent participants from saving chat ON
  Check this box and prevent participants from saving a chat. This feature goes hand in hand with recording the meetings. The Sections Department will never save chats from any council meeting, unless specifically asked to do so, and then only with participant notification. Sections are not subject to open meetings, but they are subject to public record requests. A saved chat creates a public record that may then be requested. We recommend you do not save chats, but if you do, you should notify participants before and during the meeting.
- Private chat OPTIONAL
  If enabled, this function allows participants to send a private chat 1 on 1, instead of a public chat to the entire meeting. Some sections find it helpful to be able to ask/answer questions privately using this method. Other sections find it distracting to have this additional option, and prefer participants to only chat with the group as a whole. If all other safety recommendations are followed, enabling or disabling private chat will not impact the security of your meeting.
- Auto saving chats OFF
  If enabled, this function would automatically save all in-meeting chats so that hosts do not need to manually save the text of the chat after the meeting starts. But we strongly recommend not saving chats period, so this function is not needed.
- Play sound when participants join or leave OFF
  Most sections find it distracting to have a sound ping anytime a participant joins or leaves the meeting, especially if someone is having technical difficulties in the middle of the meeting.
- File transfer OFF
  If enabled, hosts and participants can send files through the in-meeting chat. It is much more secure if files are shared via email or posted on the section website before or after a meeting, rather than being transferred via chat in the Zoom meeting.
- Feedback to Zoom OPTIONAL
  If enabled, this feature adds 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 OPTIONAL
  If enabled, this feature allows participants to respond to 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 ON
  If enabled, this feature allows hosts to assign Co-hosts, giving those individuals the same in-meeting controls as the host. Assigning your council officers as co-hosts adds security to your meeting by lessening the response time to any issue. Hosts should notify individuals that they have been made co-hosts at the start of a meeting, so they are empowered to act if something goes wrong.
- Polling OPTIONAL
  If enabled, this allows the host to survey the attendees in-meeting.
- Always show meeting control toolbar ON
  If enabled, this allows attendees easier access to their controls.
- Show Zoom windows during screen share OFF
  Zoom windows include the Chat box, Participant box, etc. If enabled, you would see the host's Zoom windows when they share their screen. This is typically unnecessary and takes up room in the window that is better used on zooming in on the actual document being shared.
- Screen sharing ON
  If all other security recommendations are followed, you can have a secure meeting with screen share enabled. As host, if you are certain you will not need to share your screen, it is recommended you turn this option off.
- Who can share? HOST ONLY
  If screen sharing is enabled, it is highly recommended only hosts have the ability to share. Remember, co-hosts have the same in-meeting abilities as hosts, this includes screen sharing.

- Who can start sharing when someone else is sharing? HOST ONLY
  Only hosts (and co-hosts) should be able to share, you do not want participants to have the ability to interrupt what the host is currently sharing.
- Disable desktop/screen share for users ON
  If enabled, this feature allows the host to share their full desktop, rather than just a application/document.
- Annotation OFF
  If enabled, participants have the ability to write information across the screen as the host shares their screen. This feature is a huge Zoom-bomb risk. You don't want someone to scribble a nasty word or drawn an obscene doodle across your screen share. We highly recommend you turn this feature off for the security of your meeting.
- Whiteboard OFF
  If enabled, this feature is similar to annotations, but allows participants to write/draw and share with the meeting at any time during the meeting. We highly recommend you turn this feature off for the security of your meeting.
- Remote control OFF
  If enabled, during screen sharing, the person who is sharing can allow others to control the shared content. This is a huge Zoom-bomb risk. You do not want to allow attendees to control your window. We highly recommend you turn this feature off for the security of your meeting.
- Nonverbal feedback ON
  If enabled, attendees have access to Zoom emojis (thumbs up/down, applause, yes/no, etc.)
- Allow removed participants to rejoin OFF
  Hosts and co-hosts have the ability to remove an unwanted participant from the meeting. For the security of your meeting, we highly recommend you turn off this feature so the removed individual is unable to renter the meeting.
- Allow participants to rename themselves ON
  If all other security recommendations are followed, this is a helpful function for attendees to have. Hosts and co-hosts always have the ability to rename a participant, whether this feature is turned on or off.
- Hide participant profile pictures in a meeting ON
  If an attendee turns off their video, their profile picture will be shown instead. If all other security recommendations are followed, this is a helpful function for attendees to have.
- Report participants to Zoom ON
  If you are required to remove an unwanted individual, you should then report that Zoom-bomber to Zoom in hopes that their account can be blocked from Zoom.
- Breakout room OFF
  If enabled, this function allow hosts to split meeting participants into separate, smaller rooms. Please contact the Sections Department for additional information if this is a feature you may want to take advantage of in your next meeting.
- Remote support ON
  If enabled, this function allows the host to provide 1:1 remote support to another participant by taking control of their computer.
- Closed captioning OPTIONAL
  If enabled, this function allows the host to type closed captions or assign a participant/third party device to add closed captions.
- Save Captions OFF
  This feature goes hand in hand with recording the meetings. The Sections Department will never save captions from any council meeting, unless specifically asked to do so, and then only with participant notification. Sections are not subject to open meetings, but they are subject to public record requests. A saved caption creates a public record that may then be requested. We recommend you do not save captions, but if you do, you should notify participants before and during the meeting.

- Language Interpretation OPTIONAL
  If enabled, this function allows the host to assign participants as interpreters who can interpret one language into another in real-time.
- Far end camera control OFF
  If enabled, this function allows another user to take control of your camera during a meeting. This is a privacy risk. For security, we highly recommend you turn off far end camera control.
- Group HD video OFF
  If enabled, this function activates higher quality videos, but will use much more bandwidth.
- Virtual background ON
  If all other security recommendations are followed, this is a helpful function for attendees to have.
- Identify guest participants in the meeting/webinar OFF
  This feature is mostly for people who share accounts, and does not apply to our meetings.
- Auto-answer group in chat OFF
  This feature does not apply to our meetings.
- Only show default email when sending email invites OFF
  If enabled this feature allows you to only send Zoom invites using the default email program, instead of the ability to select your preferred email program (Gmail, Outlook, etc.)
- Use HTML format email for Outlook plugin OFF
  It is recommended you send Zoom invites using plain text instead of HTML, to ensure all recipients can view the email.
- Allow users to select stereo audio in their client settings OFF
  This feature does not apply to our meetings.
- Allow users to select original sound in their client settings OFF
  This feature does not apply to our meetings.
- Select data center regions for meetings/webinars hosted by your account OFF
  This feature does not apply to our meetings.
- Waiting room OPTIONAL
  If enabled, the waiting room function is an added level of security to your meeting, but you are then required to click through each individual participant, allowing or denying them entry to the meeting. This takes time and knowledge (do you know all of your participants' email addresses/screen names?) If you enable this option we recommend you assign a host/co-host and not a speaker to be in charge of this feature, because you may have some participants running late to the meeting, or have some that need to jump on and off the meeting, meaning you will have to admit them from the waiting room to the meeting in the middle of a presentation that has already started. For a basic council meeting, if you are enabling all other recommended security features, a waiting room is not strictly required.
- Show a "Join from your browser" link OFF
  If enabled, this function allows 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. But the meeting experience from the browser is much more limited and as such is not recommended if it can be avoided.
- Allow live streaming meetings OPTIONAL
  Mostly used for CLEs, not basic Council Meetings. Call the Sections Department for additional information if this is a feature you may want to take advantage of in your next meeting.
- When a cloud recording is available OFF
- When attendees join meeting before host OFF
- When a meeting is cancelled OFF
- When an alternative host is set or removed from a meeting OFF
- When someone scheduled a meeting for a host OFF
- When the cloud recording is going to be permanently deleted from trash OFF

- Recording Tab
  - TURN ALL OF THESE SETTINGS OFF!

    The Sections Department will never record any council meeting, unless specifically asked to do so, and then only with participant notification. Sections are not subject to open meetings, but they are subject to public record requests. A video recording of a meeting creates a public record that may then be requested. We recommend you do not record council meetings, but if you do, you should notify participants before and during the meeting.

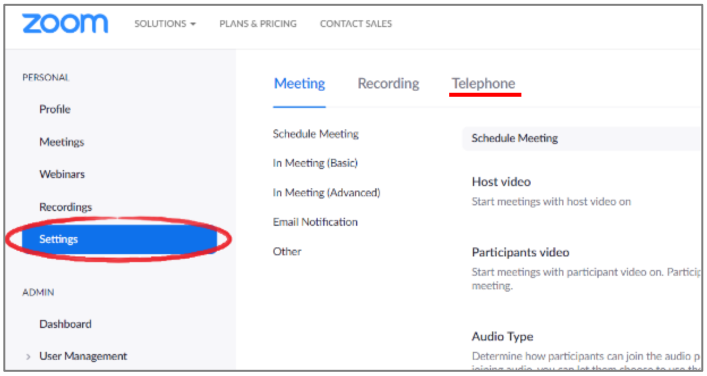


Host video
Start meetings with host video on

Participants video
Start meetings with participant video on. Particip
meeting.

Audio Type
Determine how participants can join the audio p

- Telephone Tab
  - Turn all of these settings OFF



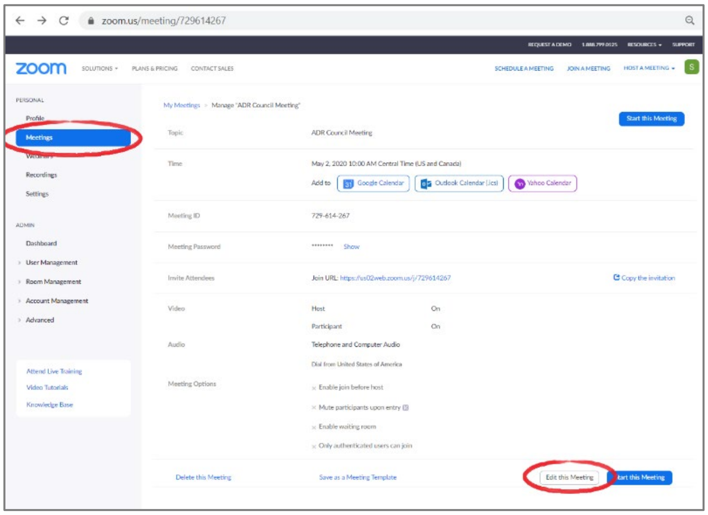
Host video
Start meetings with host video on

Participants video
Start meetings with participant video on. Particip
meeting.

Audio Type
Determine how participants can join the audio p

Manage Meetings Settings (found in the Meetings page, when you create or edit a meeting)

- Title FILL IN AT WILL
- Description FILL IN AT WILL
- When FILL IN AT WILL
- Duration FILL IN AT WILL
- Time Zone FILL IN AT WILL
- Recurring Meeting FILL IN AT WILL
- Registration OFF
  Mostly used for CLEs, not Council Meetings. Call the Sections Dept for more details if desired.
- Meeting ID GENERATE ID
  NEVER use the Personal Meeting ID. The PMID is associated with your Zoom account and can lead to zoom-bombing. The Generated ID is always randomly generated and is more secure.
- Meeting Password ON
- Video Host ON
- Video Participant ON
- Audio BOTH
- Join before host OFF
- Mute participants upon entry OFF
- Enable waiting room OPTIONAL
  If enabled, the waiting room function is an added level of security to your meeting, but you are then required to click through each individual participant, allowing or denying them entry to the meeting. This takes time and knowledge (do you know all of your participants' email addresses/screen names?) If you enable this option we recommend you assign a host/co-host and not a speaker to be in charge of this feature, because you may have some participants running late to the meeting, or have some that need to jump on and off the meeting, meaning you will have to admit them from the waiting room to the meeting in the middle of a presentation that has already started. For a basic council meeting, if you are enabling all other recommended security features, a waiting room is not strictly required.



Topic: ADR Council Meeting

Time: May 2, 2020 10:00 AM Central Time (US and Canada)

Add to

Meeting ID: 729-614-267

Meeting Password: ********

Invite Attendees: Join URL: https://us02web.zoom.us/j/729614267

Video: Host On
Participant On

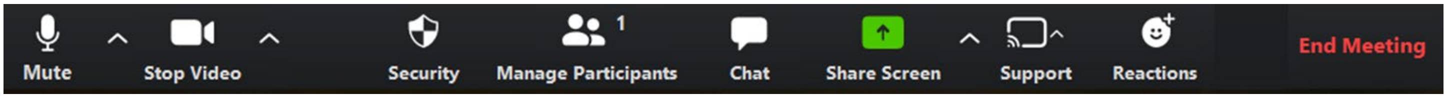
Audio: Telephone and Computer Audio
Dial from United States of America

Meeting Options:
× Enable join before host
× Mute participants upon entry
× Enable waiting room
× Only authenticated users can join

- Only authenticated users can join OFF
  If this feature is enabled, it is an added level of security, but requires all of your participants to have a verified Zoom account. Some members of your section may not feel comfortable creating an account and giving their personal information to Zoom. For a basic council meeting, if you are enabling all other recommended security features, enabling only authenticated users is not strictly required.
- Alternative Hosts
  Some sections create a Zoom account that is shared among the officers, others use personal Zoom accounts that are not shared. Either way is fine, anyone with access to your Zoom account can start/host a meeting you create. If you setup a Zoom meeting, but are unable to start the meeting yourself, and do not wish to share your Zoom account information with anyone else, this feature allows you to enter the email address of alternative host who can start the meeting in your stead.

In the Meeting

When you enter the meeting, all of your previous security settings will be applied, but you have a few quick action controls you can access to overwrite your original settings in an emergency, all of which can be found in your control bar.



- Security
  - Lock/Unlock Meeting
    When you lock the meeting, no new participants can join, even if they have the meeting ID and password.
  - Enable/Disable Waiting Room
    When you enable the waiting room, no new participants can join until the host clicks to allow them entry.
  - Allow Participants to Screen Share
    We highly recommend you to always keep this option OFF.
  - Allow Participants to Chat
    Click to turn this feature off in an emergency.
  - Allow Participants to Rename Themselves
    Click to turn this feature off in an emergency.
- Manage Participants
  Click this button to open up your Participant box as soon as you enter the meeting, so you can view and manage participants from the start.
- Chat
  Click this button to open up your Chat box as soon as you enter the meeting, so you can view and manage chats from the start.
- Support
  If enabled, this function allows the host to provide 1:1 remote support to another participant by taking control of their computer.
- End Meeting
  At the end of a meeting and in an emergency, the host has the ability to completely shut down the meeting. Click the End Meeting button and select End Meeting for All.