

A photograph of a woman with short blonde hair, wearing a pink and white striped shirt, leaning over a desk and pointing at a laptop screen. A young girl with long brown hair, wearing a pink shirt, is sitting at the desk, looking at the screen with her hand resting on her chin. The background shows a classroom with a whiteboard filled with math problems and colorful charts.

---

iLearnNH

**ZOOM K-12  
RECOMMENDED  
SETTINGS**

---





---

# TABLE OF CONTENTS

Select a topic to navigate to the subject of your choice, or move through the document step-by-step.

## 1. Key Considerations

- a. Locking Settings
- b. Using External SSO for Students

## 2. Zoom Account Management

- a. Security
- b. Schedule Meetings
- c. In Meeting (Basic)
- d. In Meeting (Advanced)
- e. Other Notable Features

# KEY CONSIDERATIONS FOR MANAGING YOUR ZOOM ACCOUNT

---

As an iLearnNH Partner, your school or SAU receives free access to a Zoom sub-account within the iLearnNH instance. Your IT team is responsible for performing day-to-day administrative functions that relate to your user needs (e.g. authentication setup, on/off-boarding users, group administration, etc.). The iLearnNH and Zoom support teams are here to assist you throughout the onboarding process.

You can access Zoom for [technical support](#) at any time. For issues with the integration of Zoom with Canvas and Kaltura, please submit a ticket to [iLearnNH](#).

Before you begin configuring your Zoom account, take some time and consider two factors that will support student safety and account management.

## PART 1 - LOCKING SETTINGS

---

Zoom uses a tiered approach to account settings based on the account, group, and user. Account-level settings are the default state for all user settings. Group settings allow you to configure one set of permissions for one group (i.e. school, grade, subject, etc.) and a different set of permissions for another. You will configure your settings based on the needs of your school or SAU.

Locking a setting prevents users from changing it. Any user can change a setting that is not locked at the account or group level. For example, if you want to disable the use of private chat for all users, you would toggle the account setting to 'off' and lock it, preventing users from enabling the feature in their personal profiles. If a setting is 'off' and 'unlocked,' users can still choose to enable the setting.

Using groups will grant only specific groups access to certain features. For example, groups will allow you to unlock the private chat setting at the account-level but lock the private chat setting for one group (e.g. fourth graders) and leave it unlocked or on for another (e.g. teacher professional development). This group-based approach will provide the most flexibility for future changes and diverse teacher and student needs.

For more information on settings in Zoom, please refer to the user guides on [changing account settings](#) or [using tiered settings](#).

## PART 2 - EXTERNAL SSO FOR STUDENTS

---

Zoom and iLearnNH recommend against creating student user accounts. Instead, we strongly suggest using external SSO/SAML-based authentication to allow students to join meetings. By using external SSO to authenticate, you eliminate the need for student accounts, making accounts easier to manage for IT. This also supports student safety and prevents student information from being stored in the Zoom cloud.

Using external SSO with the 'only authenticated users can join meetings' setting will prevent any external users from joining a Zoom meeting.

When SSO is used with the 'only authenticated users can join meetings' setting, breakout rooms cannot be assigned when scheduling a meeting. Instead, they must be pre-assigned via a CSV upload using school-issued student email addresses. Note that Zoom client and web portal interfaces only allow you to assign users within your Zoom instance.

For meetings with guests (e.g. parent-teacher conferences, board meetings, guest speakers, etc.), account owners and admins can allow authentication exceptions. For example, if a school authenticates meeting participants against their school IDP, they can create an exception to allow a guest speaker to join the meeting. You can enable this feature at the account or group level.

For more information on external SSO setup, please see [Zoom's step-by-step guide](#).



You can allow **authentication exceptions** in order to grant parents, speakers, board members, and other school guests permission to join meetings without having a Zoom account.



# ZOOM ACCOUNT MANAGEMENT: RECOMMENDED SETTINGS

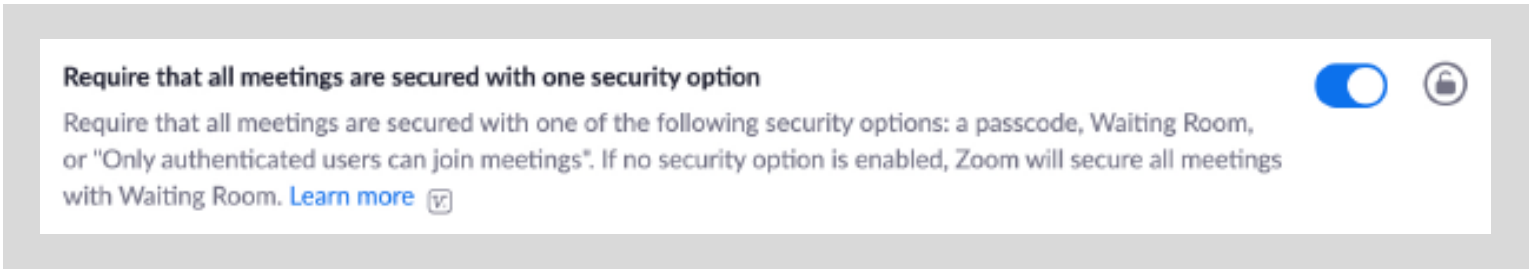
When you are ready to dive into Zoom account management, follow the screenshots below to enable the recommended K-12 settings. If you would prefer a visual guide that excludes the best practice overview, please see the Zoom Quick Start Guide.

## SECURITY

### Require that all meetings are secured with one security option:

Ensures that hosts select at least one security option: Waiting Room, passcode, or 'Only authenticated users can join meetings.' If no security option is enabled, Zoom will secure all meetings with Waiting Room.

**Recommendation: ON** – This guarantees that meetings will be secured by at least one of the methods available to hosts.



### Waiting Room:

When participants join a meeting, they are placed into a virtual waiting room. The host must admit the participants to the meeting, which they can do individually or all at once. This can be applied to all participants or only participants outside of the account. You can also whitelist specific domains to bypass the waiting room.

Account owners and admins can enable an account-level security setting to place participants in the waiting room if the host/co-hosts are not present or if they lose interest connection during a meeting. Previously this feature had to be enabled by Zoom.

**Recommendation: ON** – This allows the meeting host to admit students when they are ready. It also gives the host full control over who is joining a meeting, and ensures that a host can regain access if they lose connection during a meeting.

## Waiting Room



When participants join a meeting, place them in a waiting room and require the host to admit them individually. Enabling the waiting room automatically disables the setting for allowing participants to join before host.

### Waiting Room Options

The options you select here apply to meetings hosted by users who turned 'Waiting Room' on

- ✓ Users who are not in your account and not part of your whitelisted domains will go in the waiting room
- ✓ Host and co-hosts only can admit participants from the waiting room

[Edit Options](#) [Customize Waiting Room](#)

## Waiting Room Options

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

### Who should go in the waiting room?

- ☐ Everyone
- ☐ Users not in your account
- ☒ Users who are not in your account and not part of the allowed domains

\*.ilearnnh.org

- ☐ Users invited during the meeting by the host or co-hosts will bypass the waiting room

### 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)

If the host and co-hosts are not present or if they lose connection during a meeting:

- ☒ Move participants to the waiting room if the host dropped unexpectedly

The feature "Allow participants to join before host" will be disabled

Continue

Cancel

### Passcodes:

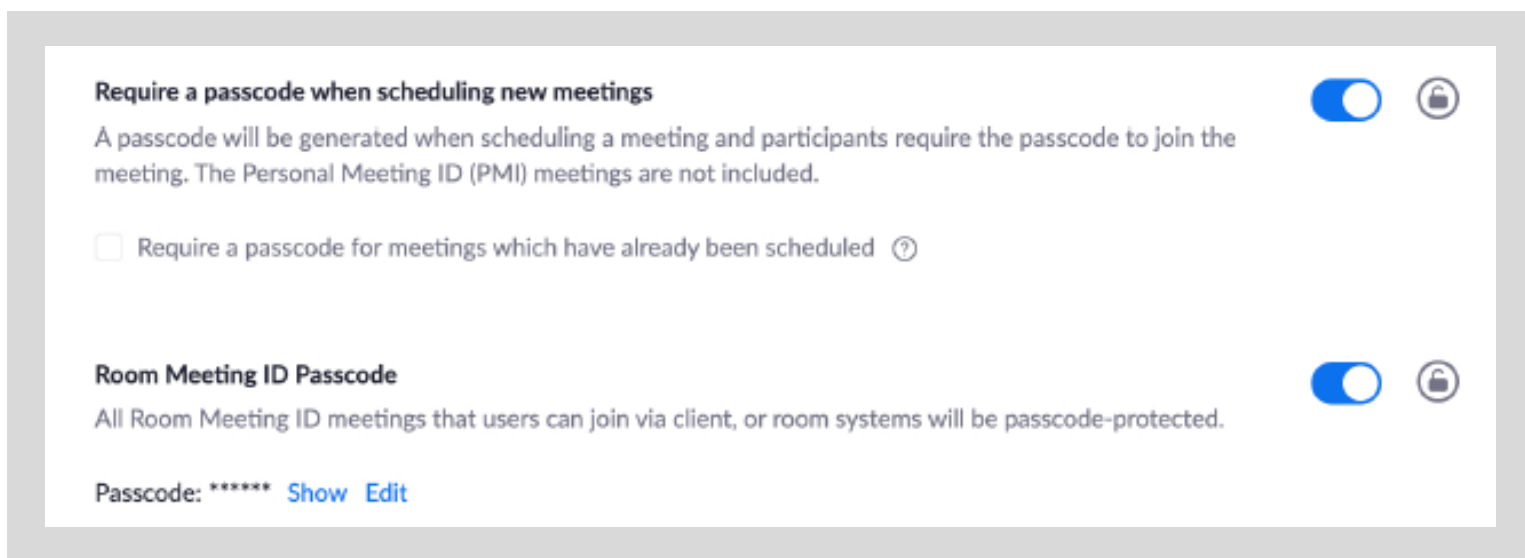
Passcodes provide an extra layer of protection to meetings. Participants who manually enter the meeting ID will need to enter the password. You can choose to embed the password into the meeting link, which allows anyone who clicks the link to join without entering a password. Adding a passcode eliminates the “wrong number” scenario in which someone mistypes a meeting ID and inadvertently enters your meeting.

**Recommendation: ON** - With ‘embed passcode into meeting link’ for scheduled meetings to balance security with ease of use.

### Passcode Requirements:

Outlines the required level of complexity for generated passcodes.

**Recommendation:** We suggest requiring a **minimum passcode length of six characters**. You may choose to make passcodes more complex depending on the needs and abilities of your users.

A screenshot of the Zoom settings interface for passcodes. The background is a light gray. The main content area is white. At the top, there's a section titled "Require a passcode when scheduling new meetings" with a blue toggle switch turned on and a lock icon to its right. Below this title, a description reads: "A passcode will be generated when scheduling a meeting and participants require the passcode to join the meeting. The Personal Meeting ID (PMI) meetings are not included." Underneath, there's a checkbox labeled "Require a passcode for meetings which have already been scheduled" with a question mark icon to its right. Further down, another section titled "Room Meeting ID Passcode" has a blue toggle switch turned on and a lock icon to its right. Below this title, it says: "All Room Meeting ID meetings that users can join via client, or room systems will be passcode-protected." At the bottom, it shows "Passcode: \*\*\*\*\*" followed by "Show" and "Edit" links in blue.

### Only Authenticated Users Can Join Meetings:

Requires meeting participants to sign into an account in order to join a meeting, allowing users to verify who is joining a meeting and improving the accuracy of reporting. Participants will not be able to join a meeting without providing a name or email.

There are four primary ways for users to authenticate an account:

1. Sign into any Zoom account
2. Sign into a Zoom account with a specific email domain
3. Authenticate using an external SSO provider such as G-Suite, Azure, Okta, Clever, etc.
4. Allow authentication exceptions

In addition to verifying identities and ensuring more accurate reporting, options two and three only allow users within your organization to attend meetings. You are able to create up to 10 authentication profiles per account, and you can choose which settings you want to enable at a group-level or for an individual.



If only authenticated users are allowed to join the meeting, account owners and admins can allow authentication exceptions to allow guests to join a meeting. For example, if a school authenticates meeting participants against their school IDP, they can create an exception to allow a guest speaker to join the meeting. You can enable this feature at the account or group level.

**Recommendation:** It is **highly recommended** to use this setting for meetings with students and external guests. The preferred login method for K-12 is via external SSO. Forcing users to authenticate using a Zoom account would require you to create accounts for students, which is not recommended. If accounts are required for students over 16, you can create basic accounts to avoid using paid licenses.

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.[Learn more](#)

Meeting Authentication Options:

Sign in to Zoom (Default) [Edit](#) Hide in the Selection

☒

 Allow authentication exception 

?

If Waiting Room is enabled, phone-only users will be placed in the Waiting Room.  
If Waiting Room is not enabled, phone dial-in only users will:

☒

 Be allowed to join the meeting

☐

 Be blocked from joining the meeting

Save

Cancel

My Meetings > Schedule a Meeting

Schedule a Meeting

Topic

My Meeting

Description (Optional)

Enter your meeting description

When

03/26/2021

10:00

AM

Duration

1

hr

0

min

Time Zone

(GMT-4:00) Eastern Time (US a

☐

 Recurring meeting

Registration

☐

 Required

Meeting ID

☒ Generate Automatically ☐ Personal Meeting ID 336 974 8568

Security

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

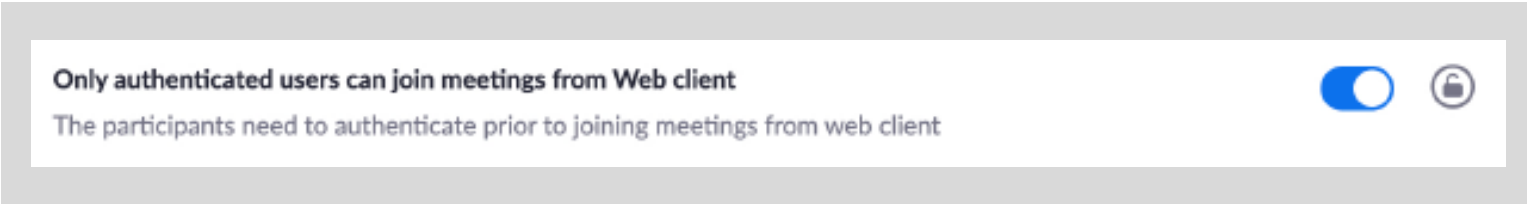
☒ Waiting Room  
Only users admitted by the host can join the meeting

☒ Require authentication to join: Sign in to Zoom  
Authentication Exception [Add](#)

### Only authenticated users can join meetings from Web client:

Requires users joining a meeting directly from a web browser to first authenticate.

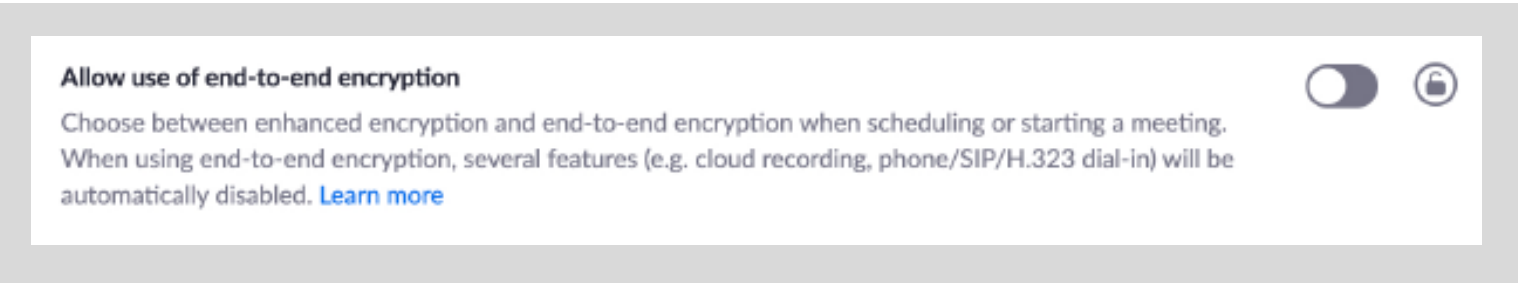
**Recommendation: ON** – This setting ensures that users joining meetings via a web browser are held to the same security requirements as client users. Districts using Chromebooks without the Zoom app may find this setting particularly useful.



### Allow use of end-to-end encryption:

Allows the meeting host to choose between enhanced encryption and end-to-end encryption when scheduling or starting a meeting.

**Recommendation: OFF** – Although end-to-end encryption is a helpful feature, enabling this setting for users/groups will prevent cloud recording and phone dial-in for all of their meetings. This feature should only be enabled for specific use cases (HIPAA/FERPA compliance, etc.).



# SCHEDULE MEETINGS

## Allow participants to join before host:

Sometimes referred to as ‘allow participants to join anytime,’ this setting allows participants to join the meeting before the meeting host. The use of a Waiting Room will essentially cancel out this setting.

**Recommendation: OFF** - We recommend using the Waiting Room instead, especially when the ‘disable auto-promotion host’ backend feature has been enabled.

Allow participants to join before host

Allow participants to join the meeting before the host arrives

## Personal Meeting ID vs. Randomly Generated Meeting ID:

Every Zoom meeting has an ID number associated with it. Every user also has their own unique personal meeting ID (PMI) that can be used to start a meeting at any time, regardless of whether it was scheduled ahead of time. This personal meeting ID does not change and may be used over and over again.

**Recommendation** - We recommend using a **randomly generated meeting ID** for scheduled meetings so that only the people who have been given a link can join the session. However, you do not need to disable PMI altogether, as it can be convenient for certain situations.

Use Personal Meeting ID (PMI) when scheduling a meeting

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



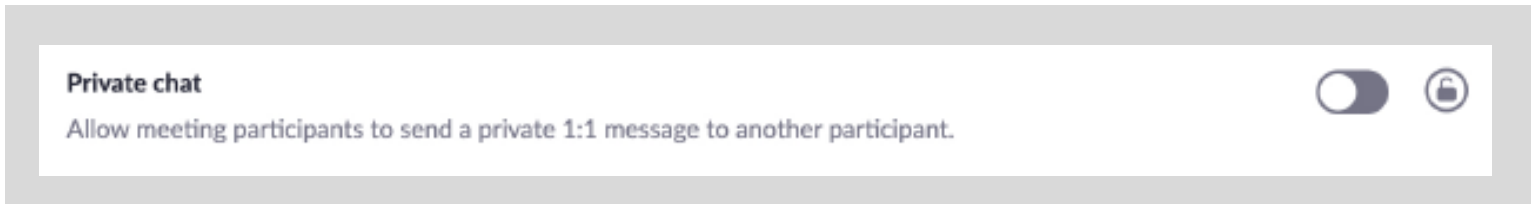
# IN MEETING (BASIC)

---

## Private Chat:

Allows meeting participants to send private 1:1 messages to other participants.

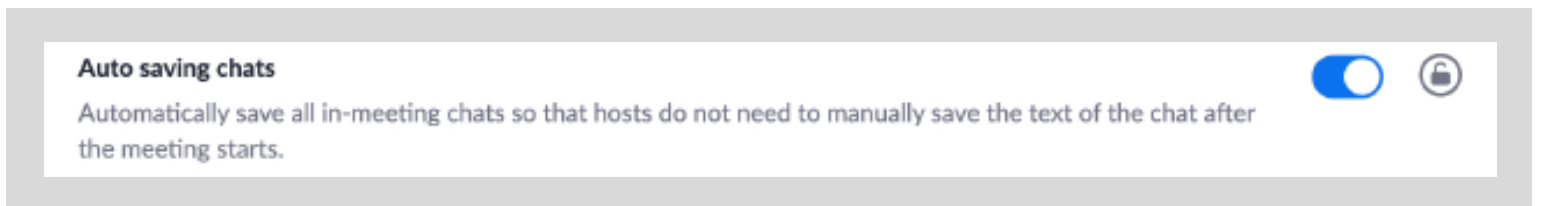
**Recommendation: OFF** – Disabling the private chat feature will likely reduce student distractions.



## Auto-Save In Meeting Chat:

Chats can be saved manually during a meeting, but this setting will automatically save the chat transcript as a .txt file locally to your computer whenever you host a meeting.

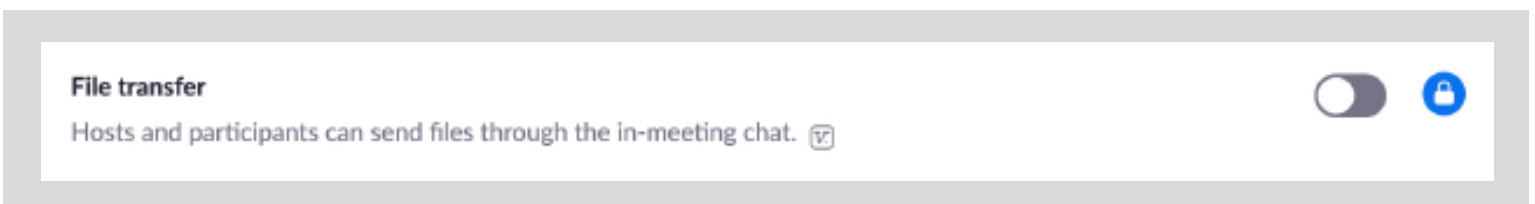
**Recommendation: ON** – Enabling this feature will ensure that there is always a record of the chat in case someone needs to reference it later.



## File Transfer:

Allows hosts and participants to send files through the in-meeting chat.

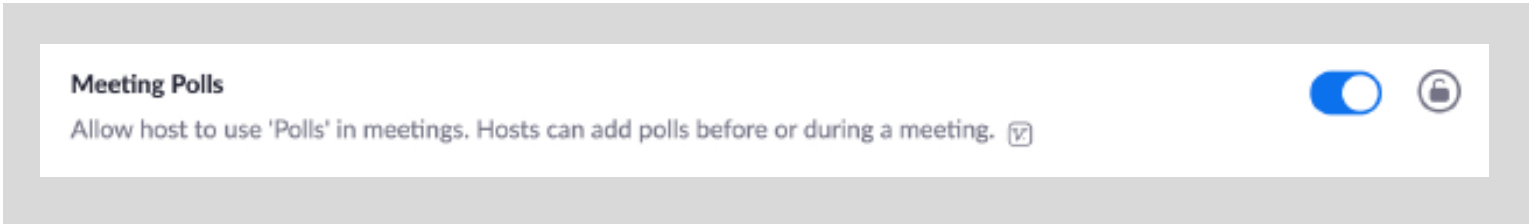
**Recommendation: OFF** – We do not recommend transferring files through Chat. This could lead to the inadvertent upload of a file infected with a virus or malware. Instead, we recommend that hosts and participants paste links to documents from shared servers like Google Apps, Office 365, etc.



### Polling:

Allows you to create and ask questions during a meeting. Polls can be developed in advance, once a meeting has been scheduled, or once the meeting has started. A poll report can be run after the meeting ends to see how each participant answered the poll question(s).

**Recommendation: ON** – Note that you must enable the poll setting in Zoom account settings in order for a user to see the polling option in the meeting controls toolbar.



### Show Zoom Windows During Screen Share:

By default, Zoom windows will be hidden when screen sharing so they do not block any content. Even though the Zoom window will be visible to the person sharing, the rest of the meeting participants will not be able to see the Zoom window. This setting will allow participants to see Zoom windows, which is very helpful for anyone who needs to demonstrate how to use Zoom.

In order to enable this feature, the 'Show my Zoom Windows to other participants when I am screen sharing' setting in the Zoom Desktop Client must also be enabled, as shown in the screenshot below.

**Recommendation: ON** - Allows staff/instructors to assist others with Zoom.

### Screen Sharing:

Certifies that only the host or meeting participants can share their screen.

**Recommendation: Allow 'Host Only' to share.** This setting applies to co-hosts as well. If an instructor wants to give one student permission to share, rather than opening it up to everyone, they can simply promote the student to co-host and then demote them once they have finished.

This screenshot shows the 'Screen sharing' settings in Zoom. The settings are as follows:

- Show Zoom windows during screen share:** Enabled (toggle on), Locked (lock icon).
- Screen sharing:** Enabled (toggle on), Locked (lock icon).
  - Allow host and participants to share their screen or content during meetings
- Who can share?:** Host Only (selected), All Participants (unselected).
- Who can start sharing when someone else is sharing?:** Host Only (selected), All Participants (unselected).
- Disable desktop/screen share for users:** Disabled (toggle off), Locked (lock icon).
  - Disable desktop or screen share in a meeting and only allow sharing of selected applications.

**Annotation: Sub-Setting – ‘Only the person sharing can annotate.’**

Ensures that only the person sharing their screen is allowed to use the annotation tools.

**Recommendation: ON** – This can be changed in the in-meeting security settings if there is a reason to open it up to everyone, but limiting annotations allows you to eliminate the ability for anyone to draw on the screen without permission.

This screenshot shows the 'Annotation' settings in Zoom. The settings are as follows:

- Annotation:** Enabled (toggle on), Locked (lock icon).
  - Allow host and participants to use annotation tools to add information to shared screens
- Allow saving of shared screens with annotations:** Enabled (checkbox checked).
- Only the user who is sharing can annotate:** Enabled (checkbox checked).



### Allow Removed Participants to Rejoin:

**Recommendation: OFF** – Once someone has been actively removed by the host, they will not be permitted to rejoin the same session.

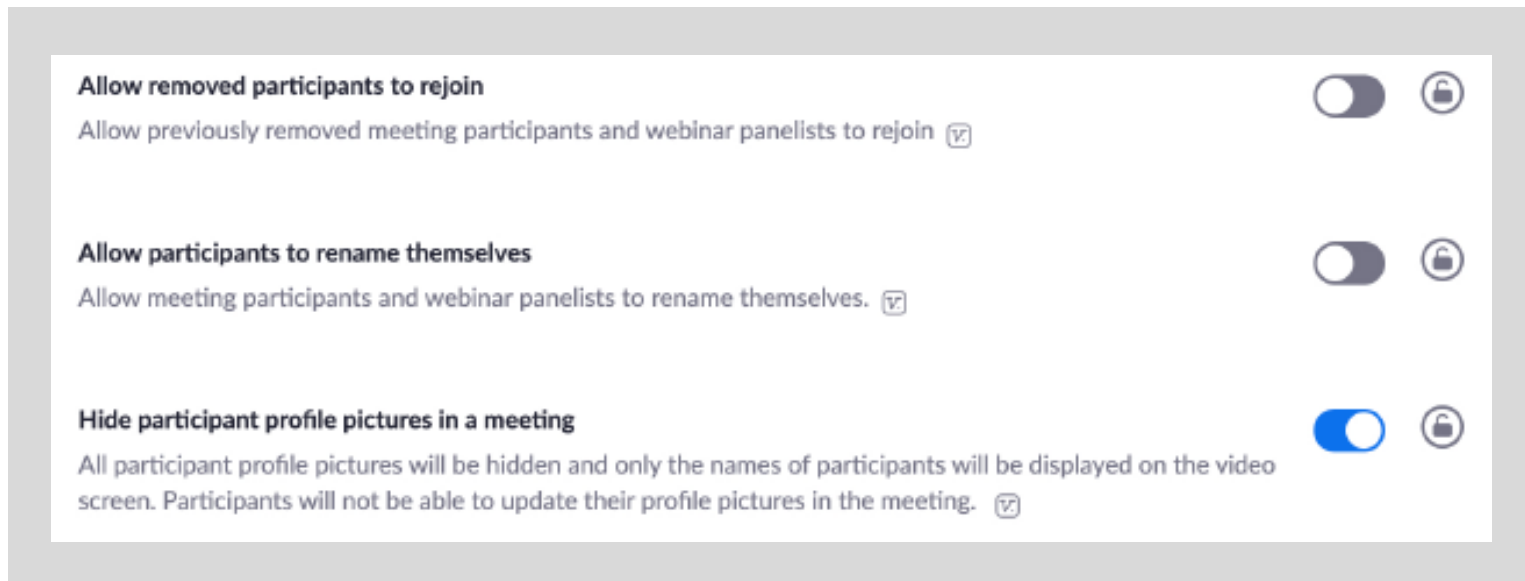
### Allow Participants to Rename Themselves:

**Recommendation: OFF** – This feature will ensure that the student's name appears as the name on their account (if they have an account) or whatever name is sent from your IDP via an external SSO. The host is able to rename anyone in the meeting, but participants cannot choose this option for themselves.

### Hide Participant Profile Picture in a Meeting:

Reveal a black box with a participant name rather than a profile picture if a participant's video is off.

**Recommendation: ON** – This can be toggled on and off from within the meeting itself, but this will remove the ability for a student to upload an inappropriate profile picture and have it seen by other participants.



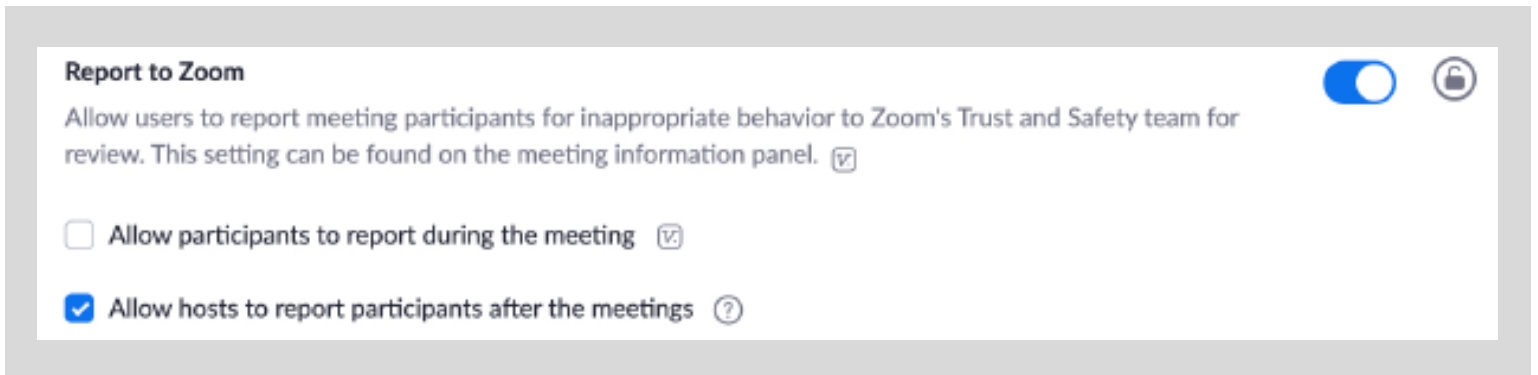
## IN MEETING (ADVANCED)

---

### Report to Zoom:

Allows you to report participants to Zoom's Trust and Safety Team for review, which can result in that person being banned from using Zoom.

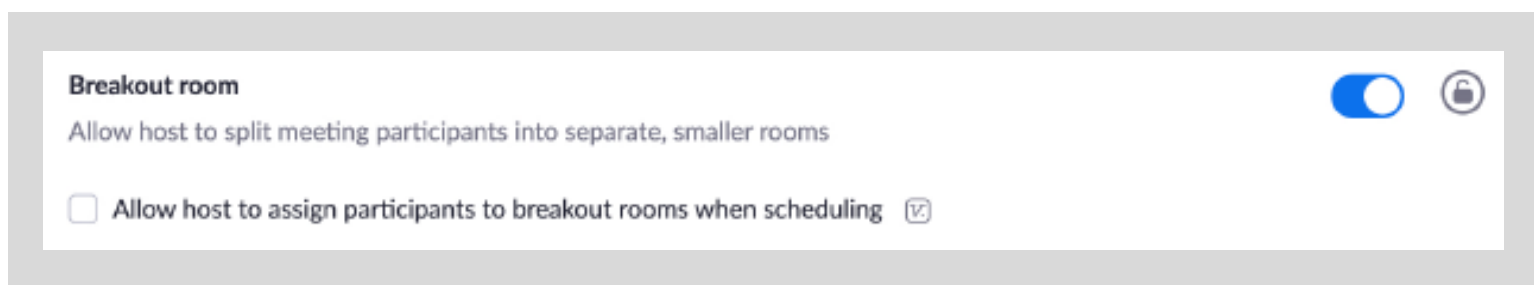
**Recommendation: OFF** - Handling inappropriate student behavior internally ensures that the student will be able to participate in future Zoom meetings. If you need to address inappropriate activity from someone outside of your organization, the host can submit a report following the end of the Zoom meeting.



### Breakout Rooms:

Allows you to split your meeting into smaller groups that act as standalone sessions underneath the umbrella of the main meeting. The host may travel from room to room, but participants are restricted to the room they are assigned unless the host allows students to choose their own breakout rooms.

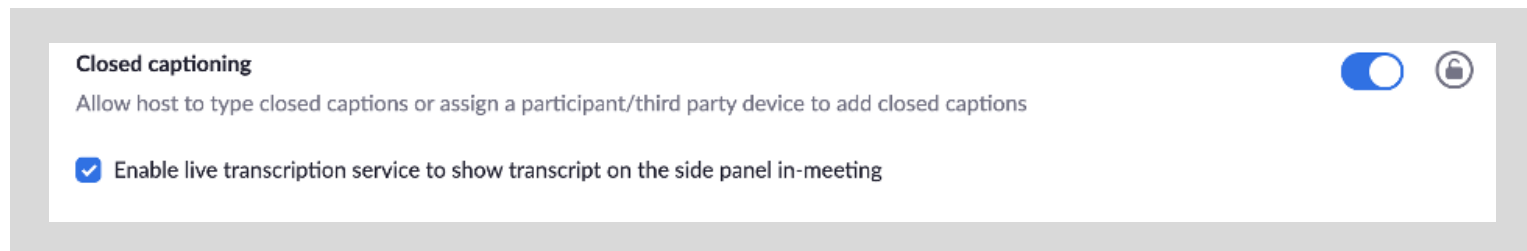
**Recommendation: ON** - This setting is mutually exclusive with remote support sessions, but breakout rooms are used far more frequently in educational settings.



### Closed Captioning: Sub-setting – ‘live transcription.’

Allows you to enable a live transcript to play at the bottom of your screen during meetings. This feature is particularly helpful for supporting student accessibility and ensuring IEP/504 compliance.

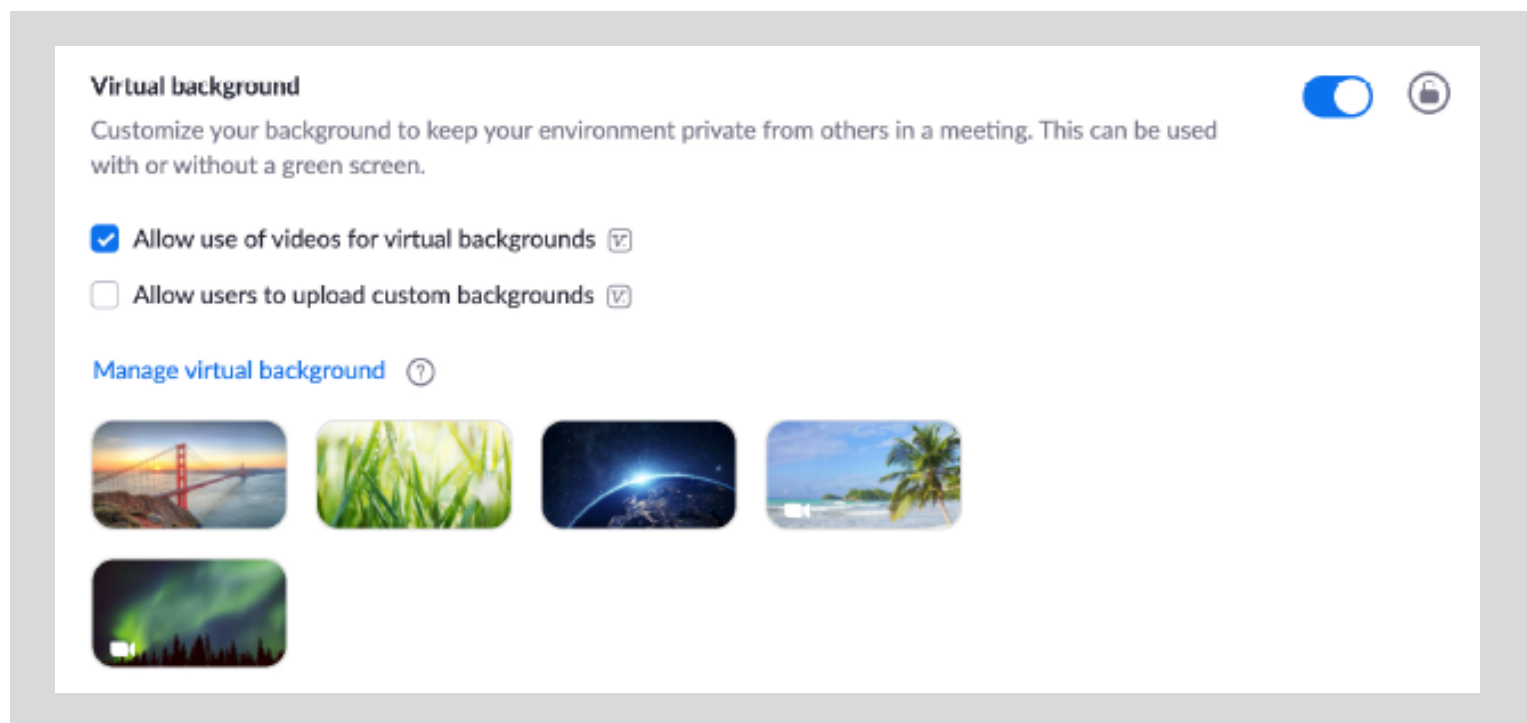
**Recommendation: ON** - This feature supports accessibility. It is currently available only to K-12 accounts.



### Virtual Backgrounds:

Allows you to project an image or video behind you during a meeting. You can allow users to upload their own image or you limit options to the stock images you provide.

**Recommendation: ON** – However, if you are going to create student accounts, we recommend that you provide pre-approved options and prevent students from uploading their own backgrounds.

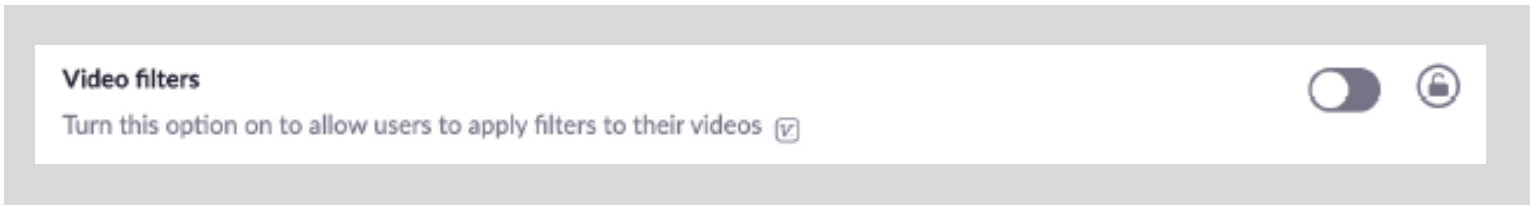




### Video Filters:

Allows you to select filters to layer over the top of your video feed or image.

**Recommendation: OFF, UNLOCKED** - While video filters can serve as a distraction to students when left unregulated, teachers may choose to incorporate video filters as an effective learning and engagement tool by unlocking video filters within their individual Zoom classrooms.

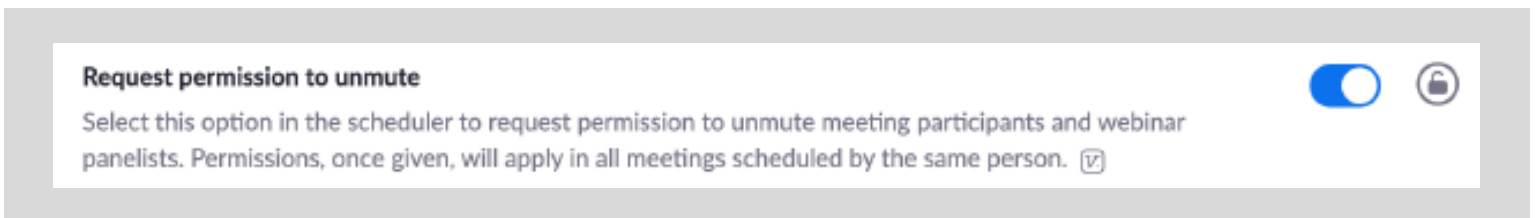


## OTHER NOTABLE FEATURES

### Request Permission to Unmute:

Due to privacy and security reasons, the host cannot unmute other participants without their consent. Hosts can choose to schedule the meeting with 'request permission to unmute participants' enabled, which will prompt the participants to be unmuted by the host with pre-approval. Once permission is granted, the host can mute and unmute people from the participants panel. Meeting participants can revoke their consent at any time in the client settings or by using the in-meeting controls.

This feature could be very useful in classroom situations where controlling audio and participation is important. For more information on this feature, review [this Zoom resource](#).



### Recording Disclaimer:

Prompts meeting participants to provide consent to participate in meeting or webinar recording. If 'recording disclaimer' is enabled, attendees will receive a notification when a recording begins or if they join a session that is already being recorded. The attendee can either consent to stay in the session or leave. Following the session, a host can generate a report listening which attendees provided consent.

See your school or SAU guidance on student consent forms and FERPA considerations. For more information on this feature, review [this Zoom resource](#).