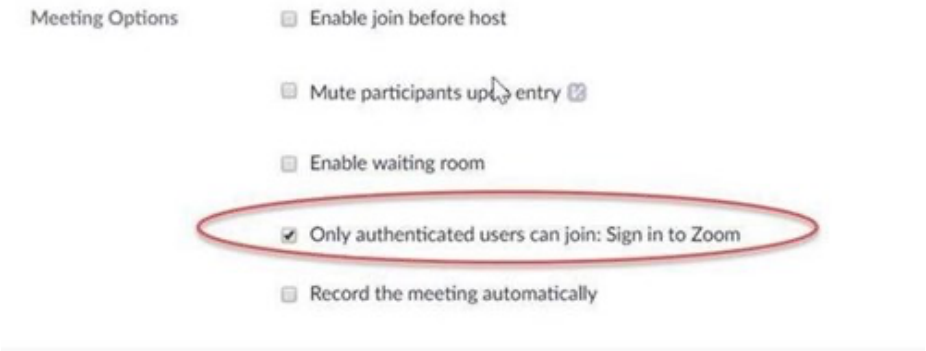
# Best practices for a Secure Zoom experience

**The University's Information Technology Department asks all faculty and staff members who host meetings (events, classes, etc.) via Zoom to review the following best practices for a secure experience:**

- Do not share your meeting link on social media or any public forum. Posting it to Blackboard or within your group in Teams is fine, that is a protected space, but forward-facing media is not private or protected and anyone can get to that link.

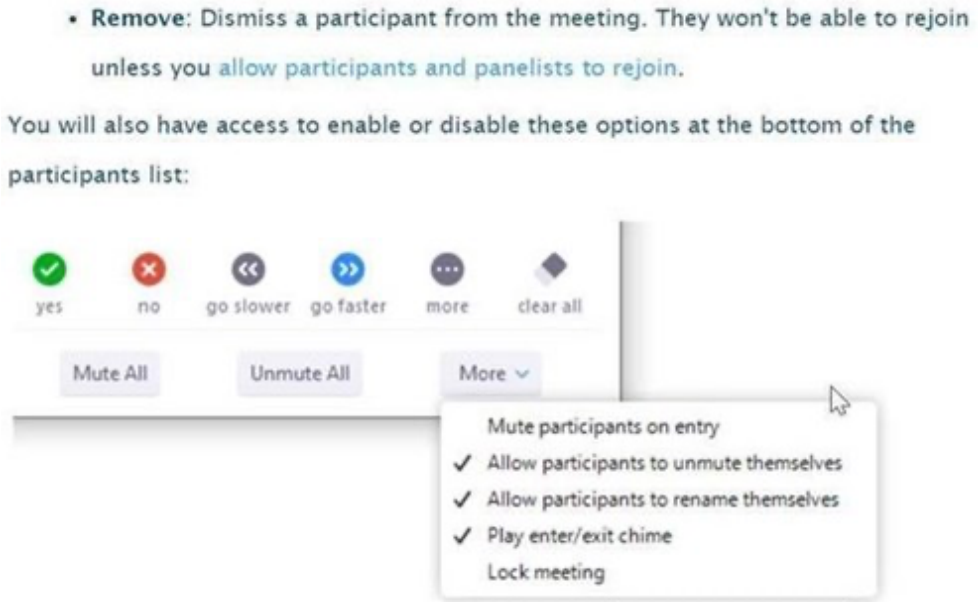
- Avoid using your Personal Meeting ID (PMI) in public events. The PMI is basically one continuous meeting, and if someone has access to that, they can join any Zoom session you host. For University courses, use your PMI. But, if you are going to post the Meeting ID on a front-facing website, always choose to "automatically generate" your Meeting ID. This way it is a random number and not your personal Meeting ID shared publicly.

- Allow only signed-in users to join. Please view Zoom's Authentication Profiles for meetings and webinars page. When you set up your meeting, if you are only inviting USI students and not any outside guests, you can choose the option to allow only authenticated users to join. They must sign into Zoom (see screenshot of the Meeting Options to check). This means they must have a registered Zoom account and login to it to join.




- You can lock the meeting. However, if a student/participant gets "kicked out" (loses connection) during a meeting once it is locked, they cannot be readmitted.

- You can remove unwanted participants and prevent them from rejoining. You can also use the settings features in the participants list (see screenshot).



- Prevent participants from screen sharing. The University's default setting in our global Zoom account has been set so that the host is the only one who can share. This is a precaution taken to ensure that the host controls screen sharing control.

    - It's best to limit this to those who you know need to share their screen. To do this, the best practice is to make each one of those individuals a co-host (you can have unlimited co-hosts). This way each person that needs screen-sharing power has the ability, and you have full awareness of who has the power.

- There are two ways to control who has admittance to your meetings. You can enable the Waiting Room and/or set a passcode. **After September 27, for security purposes, you MUST have either a Waiting Room enabled or a passcode set**.

    - By enabling the Waiting Room, you must admit each participant. You can also customize the Waiting Room by choosing to admit participants on a case-by-case basis or admit them all at once.

    - You can also set a passcode for your meeting for an extra layer of protection, but keep in mind that you will need to make sure you remind your students/meeting participants of the password if one is set. USI has enabled the feature that embeds the passcode into the web link, so that students can pass right into the class if need be, but anyone that only has the meeting ID and no passcode will not be able to join.