TEACHING AND LEARNING SERVICES

Scheduling a Secure Zoom Meeting

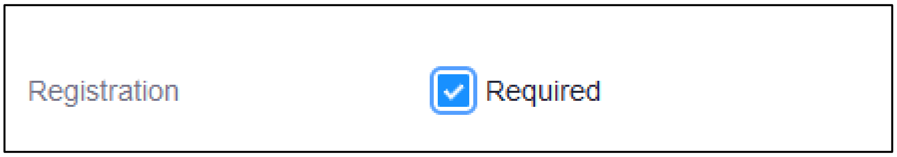
This guide is designed to help Carleton Zoom users create secure Zoom meetings that are less vulnerable to malicious actors. The guide will outline security settings that you should Enable in Zoom, as well as recommendations for overall better meeting security.

Enabling Security Settings

Follow these steps when scheduling a Zoom meeting using the Zoom app or within a Brightspace course. For more information on how to ~~do~~ schedule a Zoom meeting, see our support page: Scheduling a Zoom meeting in Brightspace.

To ensure the highest possible level of meeting security, confirm that the following settings are selected:

1. **Registration** is set to *Required.*

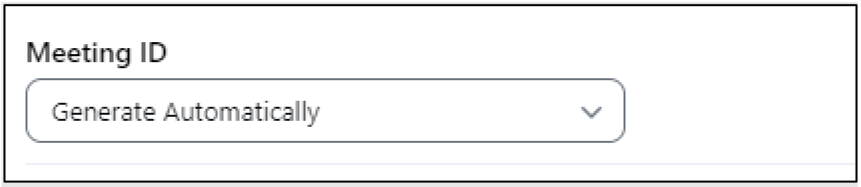


Registration ☑ Required

Use this setting for publicly posted Zoom meetings. When Registration is set to Required, participants will be required to register for the meeting with their e-mail and name. This ensures that:

- You can see who will be joining your session.
- You can generate meeting registration reports after the session.
- No one can join the meeting using the Zoom web client. This can prevent some participants from accessing your meeting. This option is best used for publicly advertised meetings.

2. **Meeting ID** is set to *Generate Automatically*.

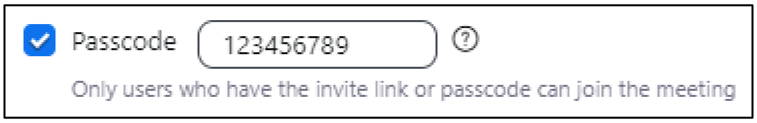


Meeting ID

Generate Automatically

Automatically generating a Meeting ID reduces the ability of uninvited users to join your meetings.

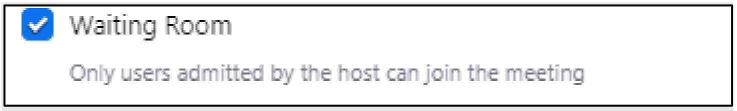
3. **Passcode** is selected with a unique passcode entered.



☑ Passcode 123456789 ⓘ
Only users who have the invite link or passcode can join the meeting

Always use a new password for your meetings. Even for recurring meetings, the password for each meeting you host should be unique. For meetings with staff or faculty, you can share the password via your Carleton University email or calendar invitation. For meetings with students, only allow access via the Zoom LTI in Brightspace so only students who are registered can access the virtual classroom.

4. **Waiting Room** is enabled.

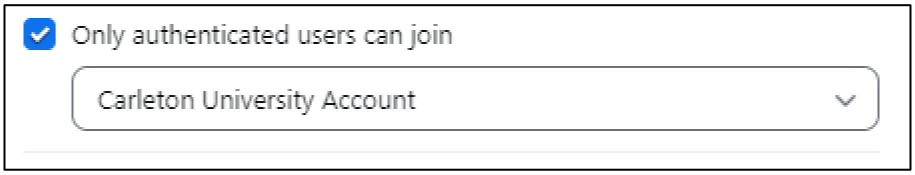


☑ Waiting Room
Only users admitted by the host can join the meeting

Use the waiting room function to:

- Review the list of participants prior to admitting them to the meeting.
- Prevent unwanted participants from joining your meetings.
- Allow entry to the meeting when you're ready to have participants join.
- Prevent access to the meeting when the host is not yet present in the meeting.

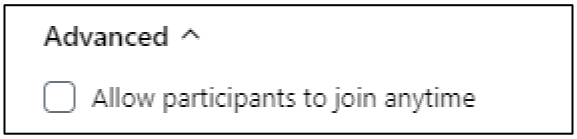
5. **Authentication** is set to *Only authenticated users can join*.



☑ Only authenticated users can join
Carleton University Account

This setting ensures that only Carleton University Zoom Users can access your meetings.

6. Uncheck **Allow participants to join anytime.**



Advanced ^
□ Allow participants to join anytime

Disabling this option ensures that no users can enter your Zoom meeting until you are in attendance.

Security Recommendations

Follow these security recommendations in all your meetings, regardless of settings, to ensure the highest possible meeting security. For more security setting recommendations, review our Security by Scenario table.

- Do not use your Personal Meeting ID (PMI) for public events. Your PMI is essentially one continuous meeting, which users can join at any time. For this reason, it is best to use your PMI for limited private events.

- Do not share your Zoom meeting links on publicly accessible forums. Instead, schedule or import meetings in the Zoom LTI tool in Brightspace, so that only enrolled students can access the virtual classroom.

- Do not re-use the password for your Zoom meetings, even if you are scheduling a recurring meeting for a class. Unique passwords ensure the highest level of meeting security. You can further protect your Zoom sessions by ensuring the *Embed Passcode in Invite Link for One-Click Join* setting is enabled in your Security Settings.

- Avoid publicly posting images of private and virtual class meetings on social media or elsewhere online to protect the privacy of students, staff, and faculty.

If you have any questions after reviewing this guide, or any other of our resources on the Zoom at Carleton support page, please reach out to us at tlssupport.carleton.ca.