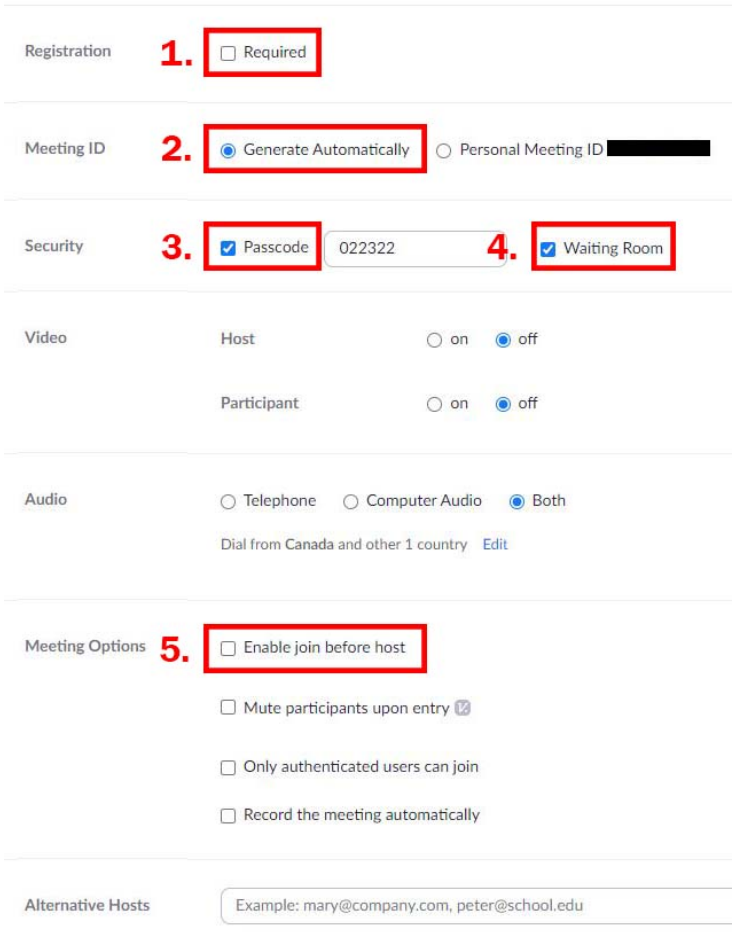
Scheduling a Secure Zoom Meeting

This document walks you through how to secure your Zoom meeting when you are *scheduling* your meeting. Be sure to also review our document on *Setting your Zoom Security Settings Before a Meeting*.

If you have any questions after reviewing this document, or any other of our resources on the Carleton TLS - Media Production Zoom Resources page, please email us at Zoom@carleton.ca

You can customize your meeting settings as needed, but here are a few guidelines for ensuring your scheduled meetings remain secure:

When you go to schedule a meeting, your options will look like this:



1. **Require Registration:** If you enable this option, participants will be required to register for the meeting with their e-mail and name. On the plus side, you can see who is joining your session, and you can also generate meeting registration reports after the session. However, requiring registration means that NO ONE can join the meeting using the Zoom web client. This can prevent your students from accessing your class. Learn more about registration here.

2. **ALWAYS use a randomly generated meeting ID.** Doing so will reduce the likelihood that uninvited users can join your meetings

3. **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, share the password via your course materials in cuLearn so only students who are registered can access the virtual classroom.

4. **Enable the Waiting Room:** By enabling the waiting room, you will be able to review the list of participants prior to allowing them into the Zoom session. This also allows you to prevent uninvited or unknown users from joining.

5. **Uncheck 'join before host':** Disabling this option ensures that NO ONE can enter your Zoom meeting until you are in attendance.

Top Security Recommendations

Follow these security recommendations regardless of the Zoom settings you enable or disable:

1. DON'T use your Personal Meeting ID (PMI) for public events. Your PMI is essentially one continuous meeting. Once people know the ID number, they can join the meeting at any time.

2. NEVER share your Zoom meeting links on publicly accessible forums. Instead, share link details through cuLearn so only enrolled students can access the virtual classroom.

3. NEVER use the same password for your Zoom meetings, even if you are scheduling a recurring meeting for a class. You can further protect your Zoom sessions by only sharing the password shortly before a class session.

4. AVOID publicly posting images of private and virtual class meetings on social media or elsewhere online. This is important to protect the privacy of students, staff, and faculty.

5. DON'T share sensitive or confidential information on Zoom. As a standard practice, Zoom data mines all information provided on their service. There are reports that Zoom is capturing the browser 'tabs' that are open at the same time as Zoom. To avoid having Zoom gather this information, open Zoom in a private/incognito browser and avoid opening any additional tabs within that browser.