

Securing your Zoom Meetings

Security:

The introduction of Brightspace to Carleton University provides a new level of Zoom Security not previously possible with other Learning Management Systems, thanks to the integration of the Zoom plugin in Brightspace.

As of May 2nd, 2022, all Zoom meetings hosted by Carleton Zoom accounts are required to have at least one security setting enabled. If none is selected, the Waiting Room will be enabled by default, and hosts will not be able to disable it in the meeting.

Waiting Room:

Users other than Hosts and Alternative hosts must be allowed into the meeting by the hosts/cohosts. If the meeting requires a Passcode, it must be entered before a user can gain access to the Waiting Room.

Require authentication to join:

Hosts can choose from 2 options: Sign in to Zoom or Carleton University Account. Sign in to Zoom requires users to be signed into *any* Zoom account (basic, pro, Carleton, or external) and Carleton University Account requires users to follow [these steps](#) to sign into their Carleton University Zoom Account.

Securing Zoom with the Zoom Brightspace Integration:

Waiting Rooms work best for smaller meetings, but once meetings start getting larger, it is much more difficult to monitor who everyone is and “check ID’s at the door”. Many instructors prefer to forego the Waiting Room and instead secure their meetings with a Passcode and share that information with their students.

The trouble with this is that once the information is in the hands of the students, the Instructor no longer has control over who is entering the meeting, and it is no longer private and secure. The solution to this is for Instructors to enable One-Click Join in their settings, and only allow students to enter meetings through the Join button, inside of the Zoom in Brightspace Integration.

One Click Entry and Brightspace:

Instructors who use Zoom through the Integration with Brightspace benefit from having this feature enabled the most, as this means the Meeting ID and Passcode, as well as an

Authentication Command will be embedded into the Join Button students see in the Brightspace Zoom Plugin:

Meeting ID	
962 5377 4954	<input type="button" value="Join"/>
962 8138 7191	<input type="button" value="Join"/>
994 1078 0779	<input type="button" value="Join"/>

Students enrolled in your course will bypass entering the meeting ID and be granted immediate access to your meeting.

If students were to try and copy the link location and send it to anyone else, the link would not work due to the embedded Authentication Command. This eliminates the ability for students to take the Invite Link or Passcode and share it, thus eliminating the possibility for unwanted participants to join your meeting.

Description:

Zoom has a security setting called “Embed passcode in invite link for one-click join”. This setting has been turned on by default for Carleton Zoom users, however, please confirm in your [settings](#) that it is enabled, as it can be turned off at the user level. This setting allows anyone with the Invite Link to bypass entering the passcode, automatically admitting them into the meeting or waiting room.

This setting is applied to EVERY Zoom meeting the user has scheduled, both **INSIDE** and **OUTSIDE** of Brightspace. Any embedded links already shared will still work when the setting is turned off if the passcode has not been changed.

Enabling the Setting:

To access this setting, navigate to <https://zoom.us/profile/setting> and scroll through the Security settings:

Security

Schedule Meeting

In Meeting (Basic)

In Meeting (Advanced)

Email Notification

Other

Until you find this setting:

Embed passcode in invite link for one-click join



Meeting passcode will be encrypted and included in the invite link to allow participants to join with just one click without having to enter the passcode.

Using the Feature:

You can tell whether or not the setting is enabled while you are scheduling a meeting by checking the wording under the Passcode option.

If it says:

Passcode

Only users who have the passcode can join the meeting

then the One-Click Entry setting is **DISABLED** because the users must have the passcode.

However, if it says:

Passcode

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

then the One-Click Entry setting is **ENABLED** because the user can enter either by clicking on the link OR by clicking on Join A Meeting in the Zoom web portal or desktop app and typing in the 11-digit meeting ID and entering the passcode.

You can also tell whether or not the setting is enabled by looking at the Invite Link. When the setting is **disabled**, your Invite Links will look like this:

Security	✓ Passcode	*****	Show	✓ Waiting Room
	× Require authentication to join			

Invite Link	https://carleton-ca.zoom.us/j/99694087968
-------------	---

When the setting is **enabled**, your Invite Links will look like this:

Security	✓ Passcode	*****	Show	✓ Waiting Room
	× Require authentication to join			

Invite Link	https://carleton-ca.zoom.us/j/99694087968?pwd=b0grWTRaNnk5OUV3RU94cWxJVlJYQT09
-------------	---

The `?pwd=` followed by a series of nonsensical characters in the Invite Link indicates that the link has the password embedded into it, making it easy to tell at a glance what kind of link it is.