Zoom - Securing Your Meeting

Issue:
I want to make sure my WSU Zoom meetings are secure.

Solution:
This guide covers measures you can take in order to prevent unwanted participants from joining your Zoom meetings or to restrict specific in-meeting features from being used by guests/participants. All of these measures can help prevent what is known as 'Zoom-bombing.'

Each security method is presented with the advantages (and disadvantages) of that method in order to assist you in choosing the appropriate security measure for your Zoom meeting environment.

Any of these settings can be enabled or disabled by signing in to your Zoom profile, located here: https://wsu.zoom.us/profile/setting

Note: Any of the methods mentioned in this documentation can be applied to meetings that are already scheduled by editing the meeting settings or by changing your user settings before the scheduled meeting becomes active (or starts).

Notice 3/14/2022 - Changes to Default Security Settings at WSU

As of 3/14/2022, WSU unlocked the requirement for participants (WSU and non-WSU) to sign in to Zoom before joining a WSU Zoom meeting. The new setting policy is that all meetings must use one of the following security options:

- Passcodes
- Waiting Rooms
- Require Sign-in to join meetings

If no option is selected Waiting Rooms will be enforced by default.

How will this impact my meetings?
This will impact newly scheduled meetings moving forward, all existing meetings will retain the settings they originally had. If you would like to change these security settings for the existing meetings, you will need to edit the meeting or meeting series via https://wsu.zoom.us/meeting#/upcoming

Adding Passcodes to Previously Scheduled Meetings, or your Personal Meeting Room (User Settings)

Note: All meetings will have the passcode protection on by default, with the option allowing you to opt-out if you so choose.

Advantage: Passcodes protect your meetings from randomly being 'Zoom-bombed'. Individuals with large amounts of previously scheduled meetings, especially recurring ones, should update these meetings with passcodes in order to protect them.

Drawback: Users may be prompted to enter a passcode, before joining your meetings, because they have not received an updated join link or meeting invitation.

Refer to How Can I Find the Passcode for My Meeting? and How to Remove Requiring Passcodes for All Meetings

Enabling Waiting Room feature (In-Meeting and User Settings)

The Waiting Room feature allows the host to control when a participant joins the meeting.

Advantage: Grants host full control over which participants are able to participate in their Zoom meetings.

Drawback: Requires Host to micromanage the Waiting Room. The Host will need to constantly check the Waiting Room to admit participants.

Refer to this guide to enable this feature: Enable Waiting Room

Settings can be selected via https://wsu.zoom.us/profile/setting to specify which Participants join the Waiting Room when they join the Zoom Meeting.

Click Edit Options to select who you want to admit to the Waiting Room.

- Everyone: All participants joining your meeting will be admitted to the Waiting Room.
- Users not in your account: Only participants who are not members of the WSU Zoom account or are not logged in will be admitted to the Waiting Room. If not logged in, they will have an option to log in.
• **Users who are not in your account and not part of the allowed domains**: Users who are not members of the WSU Zoom account or signed in to a Zoom account at the domains you list will bypass the Waiting Room. After selecting this option, enter the domain(s) here, separating multiple domains by a comma.

To Enable and Manage the Waiting Room during a Meeting follow this guide: [Waiting Room In-Meeting](#)

**Enforce Host Only Screen Sharing (In-Meeting and User Settings)**

This method allows screen sharing only for the following participants: the meeting host (you), and alternate hosts/co-hosts.

**Advantage**: This prevents participants from being able to share their screen at any time during your meeting. This is especially effective in an Academic Zoom meeting.

**Drawback**: This requires the host (and any co-host) to be **actively paying attention to participants** who may need to share their screen (i.e. vendors, sales representatives, staff members, etc.). If the host or co-host is not present, then participants will not be able to share their screen during the meeting.

Instructions can be found in the following knowledge base article: [Zoom - How to set Screen Share to Host Only](#)

**Note**: Adding alternate hosts when scheduling your meeting can help facilitate any screen sharing during your meeting.

**Enforce Chat Restrictions (In Meeting and User Settings)**

This restricts chat in your Zoom meetings so that participants are not allowed to chat, and can also prevent participants from having private one-on-one chats during the meeting.

**Advantage**: This prevents participants, especially students, from chatting within the meeting. This also helps prevent the sharing of information during quizzes, tests, polls, and any other scenario where you would not want your participants to be privately sharing information without your knowledge.

**Drawback**: Participants are not able to collaborate in chat during the meeting. If private chat functions are disabled, all chats would be public to the entire meeting, which can be difficult to manage if you have a large number of participants.

**In Meeting - Click on the 'Security' button on the meeting control toolbar, and uncheck 'Chat'**

![Meeting control toolbar with Security and Manage Participants options](https://wsu.zoom.us/profile/setting)
Disabling Whiteboarding and Annotations (User Settings)

This restricts the ability of participants to draw, or write, anything on top of the current screen sharing in the meeting.

**Advantage:** Participants (malicious or otherwise) will not be able to deface the content you are currently screen sharing (writing, making inappropriate comments, etc).

**Drawback:** Participants are not able to easily collaborate on content being presented by making annotations. **Note:** this feature cannot be enabled from within an active Meeting

Remove the Ability for Participants to Unmute their Audio, or Video (In Meeting)

This is an in-meeting feature, which allows the host to actively manage who is allowed to unmute their audio, or video.

**Advantage:** If participants are being disruptive, either by unmuting the microphone and interrupting the meeting or by displaying inappropriate content (through their camera - virtual backgrounds, obscene pictures in the background, costumes, etc) - removing the ability for them to unmute themselves will mitigate this issues.

**Drawback:** Participants, who are not malicious, could remain muted (audio, or video) and not be able to turn it back on without the host's intervention. Participants would need to send a chat (if enabled) to the host requesting their audio, or video, to be unmuted.

- Mute Participants on Entry
  - Allow Participants to Unmute Themselves
  - Allow Participants to Rename Themselves
- Play Enter/Exit Chime
- Put Participants in Waiting Room on Entry
- Lock Meeting

More detailed use of the Security button can be found here:

*Zoom In Meeting Security*
Related articles

- Utilizing the Multi-Factor Authentication Options - Setup Videos
- How to Complete FERPA Training
- Security Key Options for Multi-Factor Authentication (MFA)
- Report Fraudulent Multi-Factor Authentication (MFA) requests
- MFA (Multi-Factor Authentication) By Device