Protect your Zoom meeting space and class sessions

W itconnect.uw.edu/connect/phones/conferencing/zoom-video-conferencing/security-settings

Questions about UW Zoom privacy? Consult the FAQ

Overview of Zoom security

Zoom's default settings for meetings allow anyone with the link to join a Zoom meeting. This low barrier of entry makes Zoom easy to use. However, with ease comes risk. People (or bots) with access to the link can join the meeting, including those who were not invited to the meeting but were able to gain access to the meeting URL or ID.

Zoom offers a number of security options that you can use to prevent unwelcome participants from joining your meeting or to limit their ability to share inappropriate content.

Several options are listed below, but it is not necessary to change all of these settings to protect the security of your meeting. Choose the options that will best address your specific concerns while still creating a convenient meeting space for you and your meeting participants. You can adjust settings while a meeting is in progress or when scheduling a meeting. Some security options are available only through the Zoom web portal at washington.zoom.us.

Set security for all future meetings

The settings you configure will apply to all future meetings. These options are all available when you go to the web portal at washington.zoom.us and sign into Zoom. From the left navigation, select **Settings**. You may need to scroll down a bit to find some of these settings.

Adjust default settings for Join Before Host, Mute Participants Upon Entry, and meeting passwords to your preference. These options can be customized for individual meetings — the Settings options control what is set by default when scheduling a new meeting.
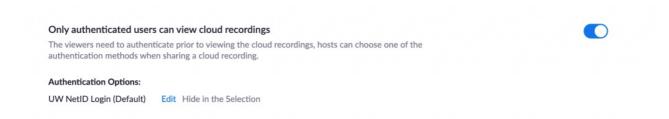
- For **Screen Sharing** set **Who can share?** to **Host Only**.
- Turn off **Allow Removed Participant to Rejoin** to ensure that if a participant is removed for inappropriate behavior, they cannot rejoin.
- Turn off **File Transfer** or limit file types that can be shared to prevent sharing of inappropriate or virus-ridden files with other participants.

Set security for all cloud recordings

To secure the Zoom cloud recordings you create, navigate to your Zoom recording settings page. These options apply to all the Zoom recordings you create.

Restrict viewing of recordings to authenticated users

To restrict viewing, enable **Only authenticated users can view cloud recordings** from the Zoom recording settings page. When this setting is enabled, users must have a UW NetID to view the recording.

Only authenticated users can view cloud recordings

The viewers need to authenticate prior to viewing the cloud recordings, hosts can choose one of the authentication methods when sharing a cloud recording.

Authentication Options:

UW NetID Login (Default)   Edit   Hide in the Selection

Set password protection for recordings

To set password protection, enable **Require password to access shared cloud recordings** from the **Zoom recording settings page**. When this setting is enabled, a random password will be generated that can be modified by the meeting host. This setting applies only to recordings generated after the setting is turned on.

Require password to access shared cloud recordings

Password protection will be enforced for shared cloud recordings. A random password will be generated which can be modified by the users. This setting is applicable for newly generated recordings only.
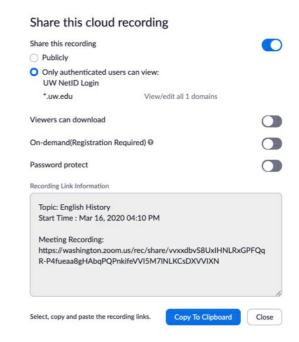
Disable downloads of recordings

To prevent people who can watch your Zoom cloud recordings to download them, follow these steps.

1. Navigate to the Zoom recordings page
2. Select **Share**
3. Disable **Viewers Can Download**

Individual recordings

Viewers can download

To change security settings for individual recordings, navigate to your Zoom recordings page, then select **Share**. Turn on or off the settings you choose.

Set security for a single meeting while scheduling

When scheduling a meeting, you can configure security settings to:

- Prevent participants from joining the meeting before a Host or Alternative Host arrives.
- Require users to authenticate themselves
- Require a meeting password

You can configure any or all of these options.

On the **Schedule Meetings** page/screen, under **Meeting Options**:

- Clear **Enable join before host** to prevent participants from joining the meeting until a Host or Alternative Host arrives.
- Check **Only authenticated users can join** to ensure that all participants are logged into UW Zoom accounts.
- Check **Require meeting password** to require password authentication when users enter the meeting. Passwords can be up to 10 characters. By default, the meeting invitation will include the password for participants, as well as a Join Meeting link that will enter the password automatically for invited participants. These settings can be changed in your User Settings in the Zoom web portal at washington.zoom.us.

Set security for a single meeting during the meeting

During a meeting you can prevent participants from sharing their screen, keep participants muted, or remove participants.

Prevent participants from sharing their screen while a meeting is in progress

You can prevent participants from sharing their screen unless you have assigned them the role of Host, Co-Host, or Alternative Host.

1. At the bottom of the Zoom meeting, click the small arrow to the right of the green Share button.
2. From the menu, select **Advanced Sharing Options**.
3. Under **Who can share?** select **Only Host**.
4. Close out of the **Advanced Sharing Options** menu.

Control additional participant behaviors

Via the Participants window, you can keep participants muted, enable the waiting room, lock the meeting to additional participants, or remove participants.

1. At the bottom of the Zoom meeting, click the Participants button to open a list of participants.
2. At the bottom-right corner of the list of participants, click "More" to open a menu.
3. Toggle the options as desired:
   - Clear **Allow Participants to Unmute Themselves** to ensure that only hosts can unmute participants
   - Check **Put attendee in waiting room upon entry** to require that hosts manually admit new participants rather than having them join the meeting automatically. Learn more about the Zoom Waiting Room feature.
   - Check **Lock meeting** to prevent any additional participants from joining the meeting after this option is selected.

Remove participants who are behaving inappropriately

1. At the bottom of the Zoom meeting, click the **Participants** button to open a list of participants.
2. In the participant list, hover your cursor over the name of the participant you wish to remove, then click the **More** button that appears to the right.
3. From the bottom of the menu, select **Remove**.
4. A dialog box will open asking you to confirm your choice. Click **OK** to remove the participant.

How Zoom security settings work together

As noted above, you do not need to change all security settings to protect your Zoom meeting space. The table suggests combinations of settings you can configure to achieve the level of security you want.

Setting	Least Secure → Most Secure					
Disable Join Before Host	X	√	√	√	√	√
Enable Waiting Room	X		√	√	√	√
Limit Sharing to the Host	X			√	√	√
Meeting Password	X				√	√
Restrict Access to Join a Meeting	X					√

Learn more about specific security settings

Disable Join Before Host — Clear **Enable join before host** to prevent participants from joining the meeting until a Host or Alternative Host arrives.

Enable Waiting Room — Allows the host to control when a participant joins the meeting.

Limit Sharing to the Host — Prevents participants from screen sharing.

Meeting Password — Require passwords for meeting to add an additional layer of security

Restrict Access to Join a Meeting — Allows a host to restrict participants who can join a meeting to those who are logged into Zoom, and even restrict it to Zoom users whose email address uses a certain domain.

Last reviewed April 1, 2020

See a problem on this page? Let us know.