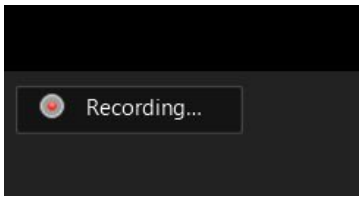
Privacy considerations when using Zoom



One of the most important things to remember is that a Host can record a Zoom session, including the video and audio, to their computer. Therefore, be careful saying or physically 'revealing' anything that you would not want someone else to potentially see or know about.

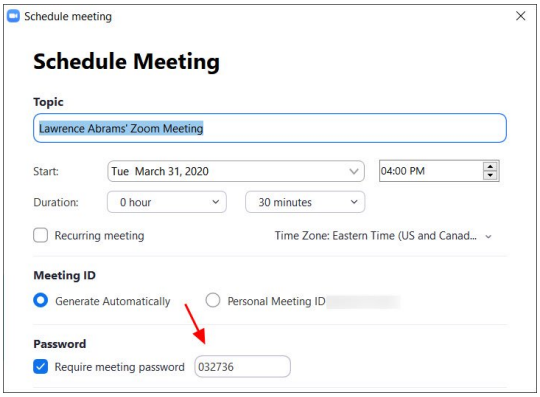
Meeting participants will know when a meeting is being recorded as there will be a 'Recording...' indicator displayed in the top left of the meeting as shown below.

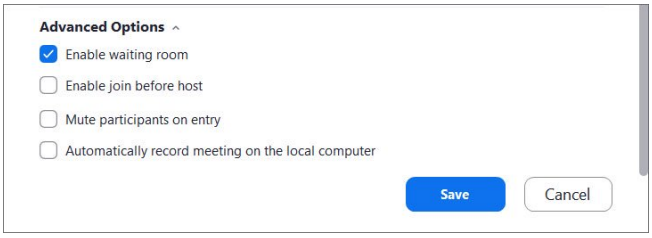
It's also important to remember that a user can download their chat logs before leaving a meeting. These logs will only contain messages that you could see, but not the private chat messages of other users.

Securing your Zoom meetings

Add a password to all meetings!

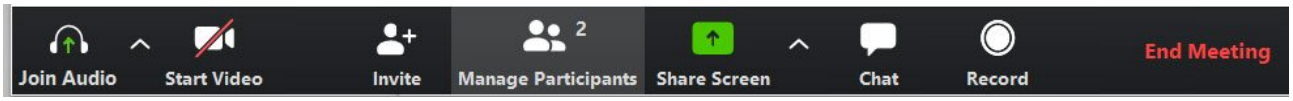
When creating a new Zoom meeting, Zoom will automatically enable the "Require meeting password" setting and assign a random 6 digit password. You should not uncheck this option as doing so will allow anyone to gain access to your meeting without your permission



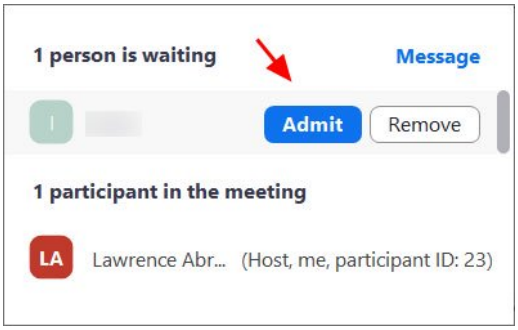


Use waiting rooms

Zoom allows the host (the one who created the meeting) to enable a waiting room feature that prevents users from entering the meeting without first being admitted by the host.
This feature can be enabled during the meeting creation by opening the advanced settings, checking the 'Enable waiting room' setting, and then clicking on the 'Save' button.
When enabled, anyone who joins the meeting will be placed into a waiting room where they will be shown a message stating "Please wait, the meeting host will let you in soon."
The meeting host will then be alerted when anyone joins the meeting and can see those waiting by clicking on the 'Manage Participants' button on the meeting toolbar.



You can then hover your mouse over each waiting user and 'Admit' them if they belong in the meeting.

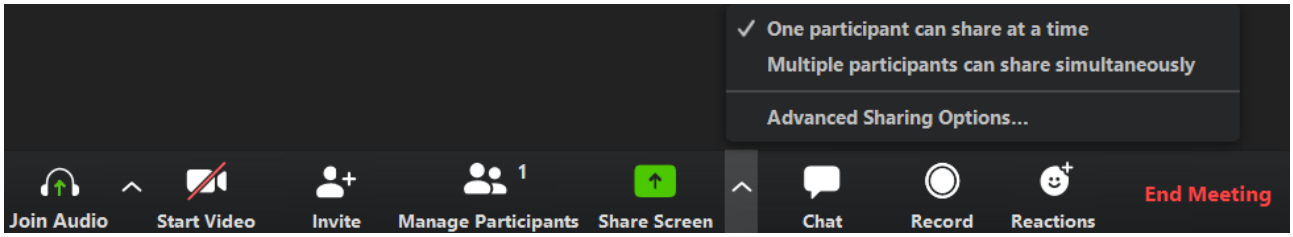


Do not share your meeting ID

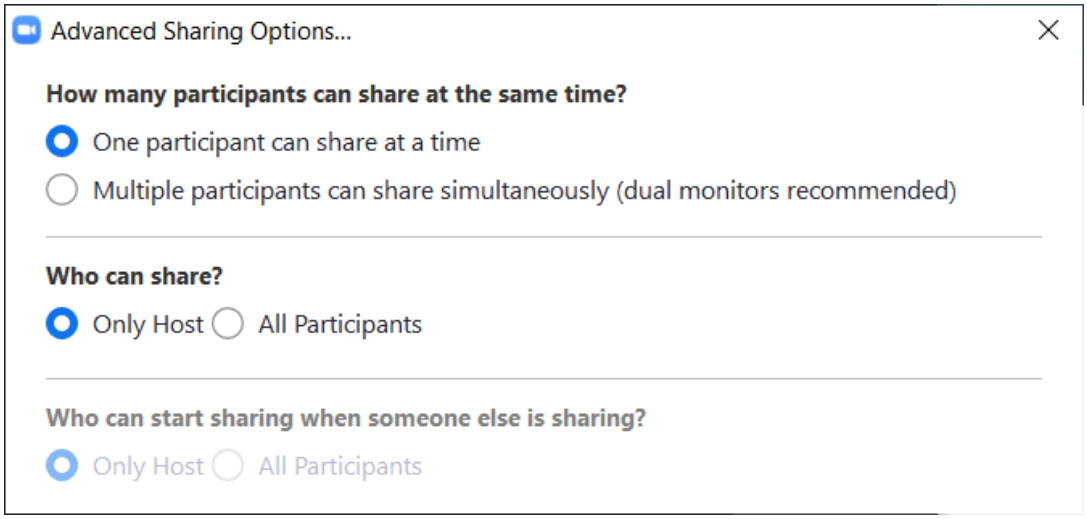
Each Zoom user is given a permanent 'Personal Meeting ID' (PMI) that is associated with their account.
If you give your PMI to someone else, they will always be able to check if there is a meeting in progress and potentially join it if a password is not configured.
Instead of sharing your PMI, create new meetings each time that you will share with participants as necessary.

Disable participant screen sharing

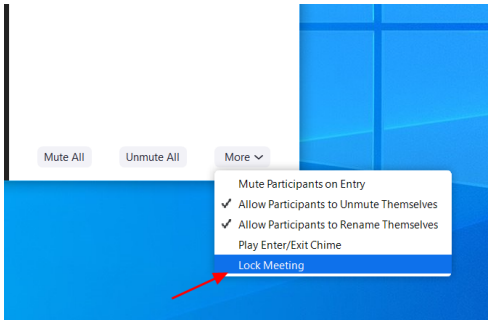
To prevent your meeting from being hijacked by others, you should prevent participants other than the Host from sharing their screen.
As a host, this can be done in a meeting by clicking on the up arrow next to 'Share Screen' in the Zoom toolbar and then clicking on 'Advanced Sharing Options' as shown below.



When the Advanced Sharing Options screen opens, change the 'Who Can Share?' setting to 'Only Host'.



Lock meetings when everyone has joined

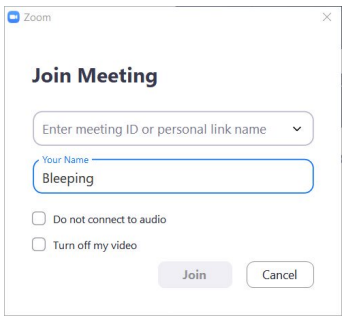


If everyone has joined your meeting and you are not inviting anyone else, you should Lock the meeting so that nobody else can join.
To do this, click on the 'Manage Participants' button on the Zoom toolbar and select 'More' at the bottom of the Participants pane. Then select the 'Lock Meeting' option as shown below.

Be careful posting pictures of your Zoom meetings online

If you take a picture of your Zoom meeting than anyone who sees this picture will be able to see its associated meeting ID. This can then be used uninvited people to try and access the meeting.
For example, the Prime Minister Boris Johnson tweeted a picture of the "first ever digital Cabinet" and included in the picture was the meet ID.

This could have been used by attackers to try and gain unauthorised access to the meeting by manually joining via the displayed ID.
Thankfully, the virtual cabinet meeting was password-protected but does illustrate why all meetings need to use a password or at least a waiting room.



Thankfully, the virtual cabinet meeting was password-protected but does illustrate why all meetings need to use a password or at least a waiting room