More secure Zoom meetings

The number of video meetings has increased now when many work and teach from home. Unfortunately, unauthorised persons are also aware of this. Zoom bombing is when unwanted participants show up in your Zoom meeting and sabotage it through writing spam in the chat or sharing disturbing images via the Share screen option. Most of these intrusions happen when the link to the meeting has been made public by mistake.

Please note! When you use Zoom at Umeå University you must follow the university's guidelines. All communication in Zoom is encrypted and personal data is handled within the EU. However, the service is not intended for sensitive personal data or classified information.

Recommended settings

Below is a list of security measures that you, as a host, can take to protect your meetings from unwanted participants.

Keep in mind that:

- You should not publish the meeting link on for example social media. Send the link directly to the participants instead.
- If you need to, you can choose to not make the meeting public. There are two alternative ways to do this. Either by setting a password for the meeting or by letting participants first enter a waiting room and only giving access to participants that are allowed to participate.
- You can also limit the opportunity for participants to share their screens and write in the chat. This means that only the host can do this.
- You should make sure that Zoom is updated to the latest version at all times.

Take control over who joins your meetings

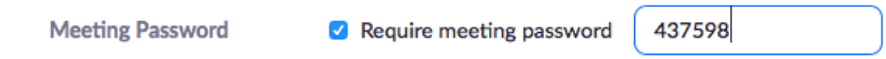
There are different settings that enable you to get better control over who joins your meetings. Choose the setting that best serves the purpose of your meeting.

- Limit the number of meetings with your personal meeting ID

Your personal meeting ID (PMI) in Zoom is basically a recurring meeting. People who have received your personal meeting ID can click the link at any time to join a meeting. This is a good thing when a colleague that you're often in contact with want to meet with you. It is easy to find your Zoom meeting. The downside is that users who have access to the link can join your meeting at any time, for instance while another meeting is in session.

When you teach and want to use the same meeting link for a period of time it is best to create a *Recurring Meeting* with an automatically created meeting ID. This prevents you from being disturbed in meetings using your personal meeting ID.

- Give your meeting a password



To prevent unauthorised participants entering your meeting you can protect it with a password. This means that only the participants with the meeting ID and the password can join the meeting. Create a password when you schedule a meeting by ticking the box *Require meeting password*. You can choose your own password or let Zoom generate one automatically. When a participant tries to join your meeting they will be asked to write the password to join.

- Waiting Room

The *Waiting Room* function gives the host control over which participants can join the meeting and when they are allowed to join. As a host, you can manually allow participants to join, one at a time, or allow everyone in at the same time. This is function creates more work for you but it gives you a better overview of the participants.

Please note that if a student is late in joining the meeting a pop up window will appear and you can choose to let them in.

You can add a personal message in the Waiting Room that the participants receive when they join. The message can, for example, be information about the framework for the meeting.

- Only authenticated users can join meetings

This function allows you to activate that only *authenticated users* can join your meeting. This means that all the participants must login with their Umu-ID or Zoom account to get access to the meeting. The function is found under *Advanced options* when you schedule a new meeting.

- Disable Join Before Host

If *Join Before Host* is not activated the participants can't join the meeting until you, the host, have started it. Participants waiting to join will automatically enter the meeting when it has started.

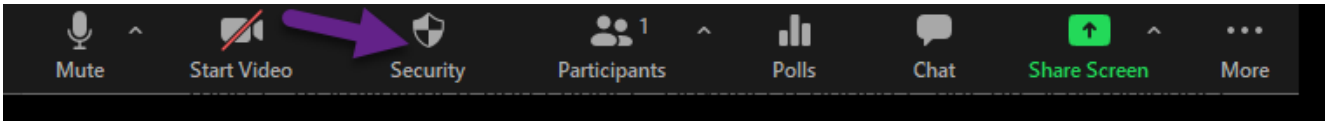
You can change this setting when you schedule a meeting under *Meeting options*. If you want to change this setting for all upcoming scheduled meetings you can do that under *Settings* and *Schedule meetings*.

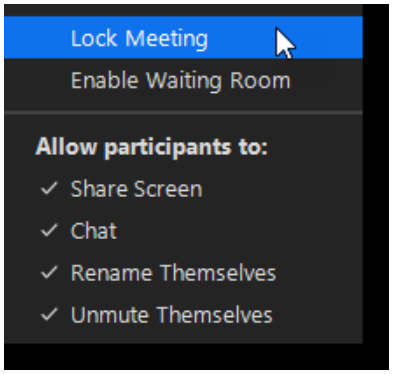
Control an ongoing meeting

- Lock meeting

As a host or co-host you can lock a meeting. If you lock it, no new participants can join, even if they have access to the meeting link.

Click on *Security*

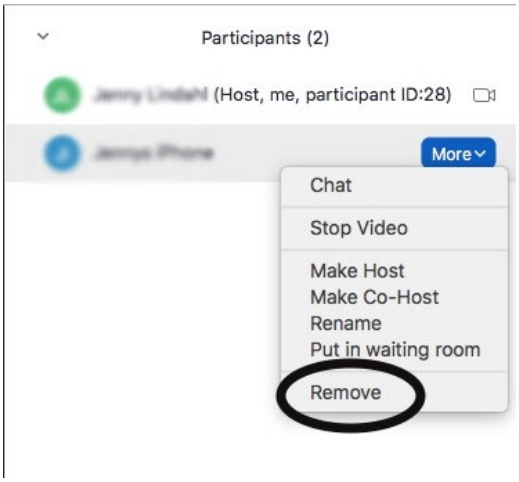




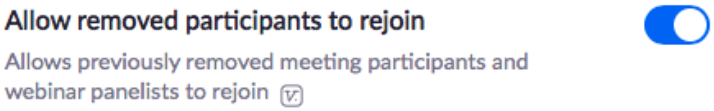
Choose *Lock meeting*.
If someone wants to join the meeting after it has been locked you will not receive a notification. That is why it is important to make sure that all particpants are in attendance before locking the meeting.

- Remove a participant from the meeting

If a meeting is in session and you notice an unwanted participant it is easy to remove the participant from the meeting.



Click *Manage Participants* at the bottom of the Zoom meeting. The list of participants will appear (see image above). Click *More* beside the participants name and choose *Remove*.

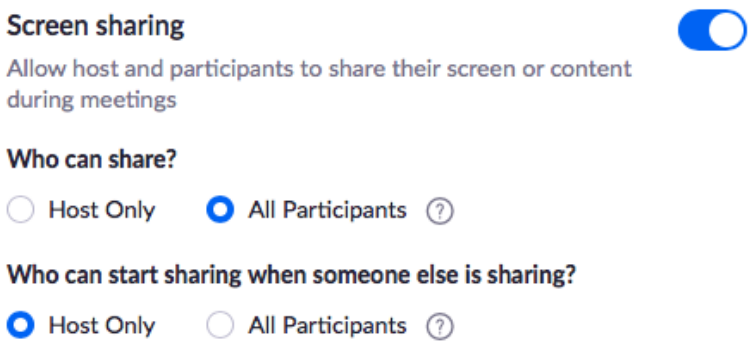


If you have removed a participant by mistake you can change this by going to *Settings* and then to *In meeting (basic)* on your Zoom account. Scroll down to *Allow removed participants to rejoin* and activate that function (see image above).

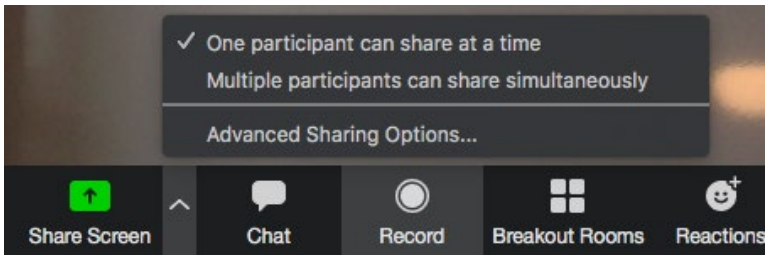
- Limit the Share screen option

As a host it can be important to not let anyone else take control of what is shown on the screen. You do not want someone to share inappropriate content with the

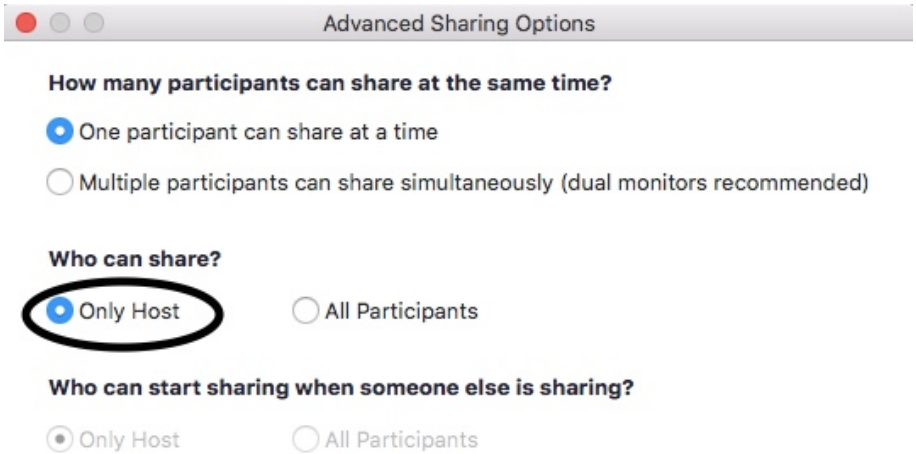
participants. You can limit the Share screen option for the participants before or during a meeting. This means that only you as the host can share your screen. Be aware that the standard setting is that both host and participants can share their screens.



If you wish to limit screen sharing before a meeting, go to your Zoom account. Go to *Settings* and under *In meeting (basic)* you can choose if *Host only* or *All participants* can share their screen. The image above shows the options available.

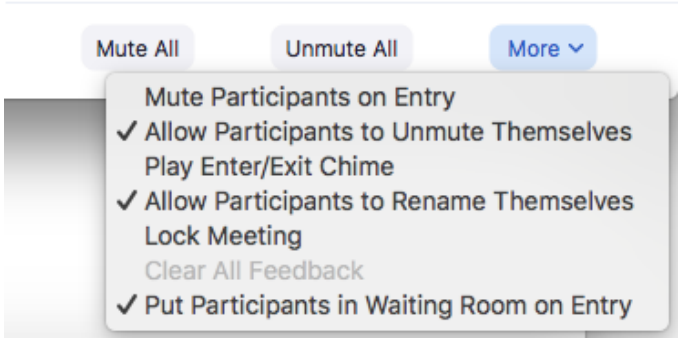


If you wish to limit screen sharing during an ongoing meeting, click the arrow beside Share screen and choose *Advanced Sharing Options* (see image above). A pop-up window will appear where you can choose that *Only Host* can share the screen (see image below).

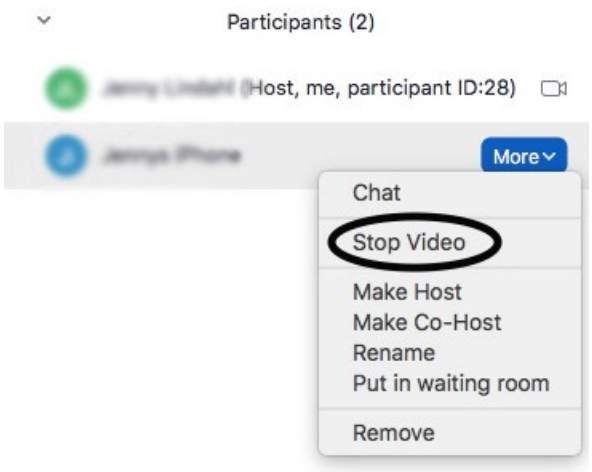


- Turn off participants microphones or videos

You can control the participants' videos or microphones as a host in a meeting.



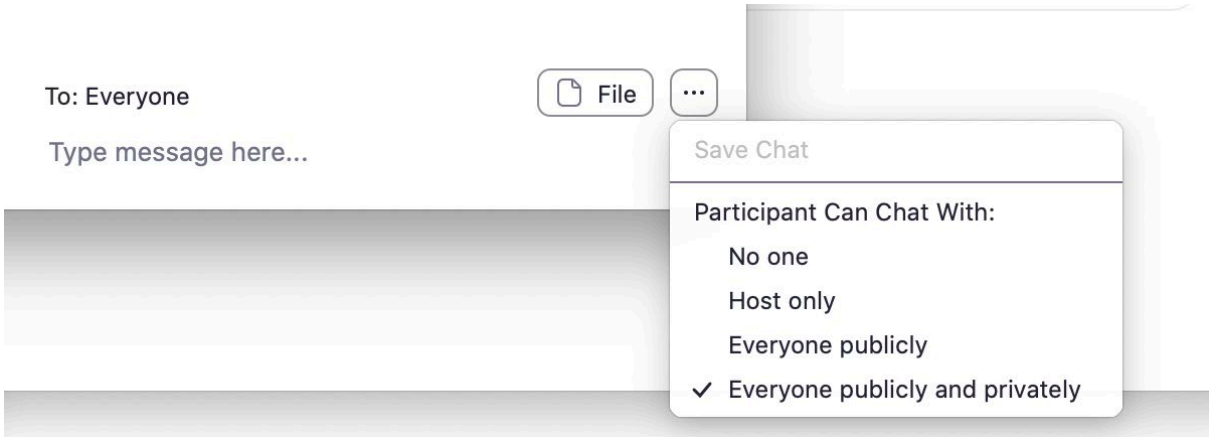
To see the settings for the participants' microphones, click *Manage Participants*. The list of participants will appear. Click *More* in the bottom right corner of the list. Options for the participants' microphones will appear.



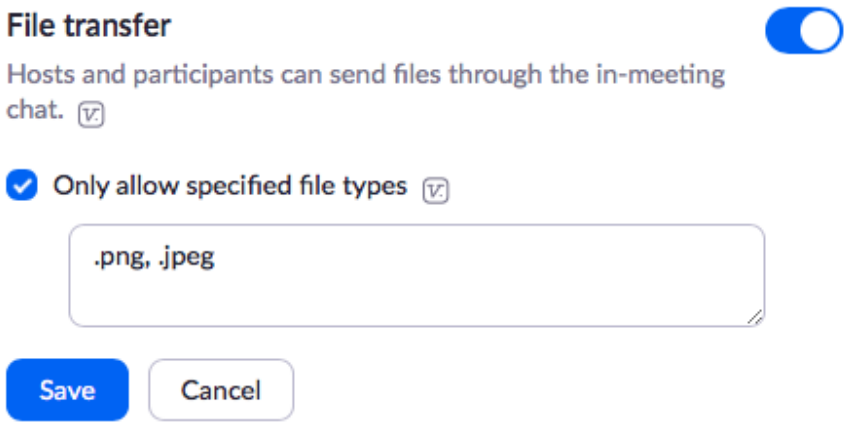
If you wish to stop a participant's video, click *Manage Participants*. Click *More* beside the participants name. If you choose *Stop Video* the participant can no longer use their video during the meeting.

- Limit the chat function and file transfers during a meeting

The enabled setting in Zoom is that everyone in a meeting can write both public and private messages in the chat. You can edit this setting as a host if needed. One security measure can be to turn off the possibility for private chat or turn off the chat function entirely. You can adjust this during an ongoing meeting by clicking the three dots in the bottom right corner of the chat window (see image below).



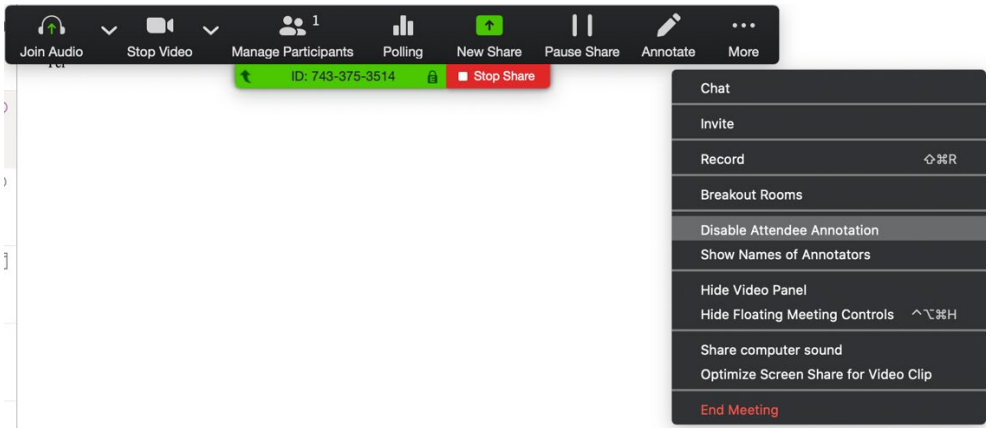
File transfer in the chat allows participants to send each other files during the meeting. If inappropriate files are shared you might want to disable the function *File transfer*.



Go to *Settings* in your Zoom account and go to *In meeting (basic).* Scroll to *File transfer* that you can choose to enable or disable. You can also check the box *Only allow specified file types* where you can specify exactly what kind of files can be shared. Write every format allowed and use a comma to separate the formats.

- Limit the use of annotation tools

You and your participants can make annotations together with comments during a screen share. You can disable this function to stop the participants from writing all over the screen. The setting appears under *More* while you are sharing the screen. (See image below.)



More recommendations for Zoom security

More recommendations can be found in the links below:

- https://security.berkeley.edu/resources/cybersecurity-and-covid-19/settings-preventing-zoom-bombing
- https://blog.zoom.us/wordpress/2020/03/20/keep-uninvited-guests-out-of-your-zoom-event/