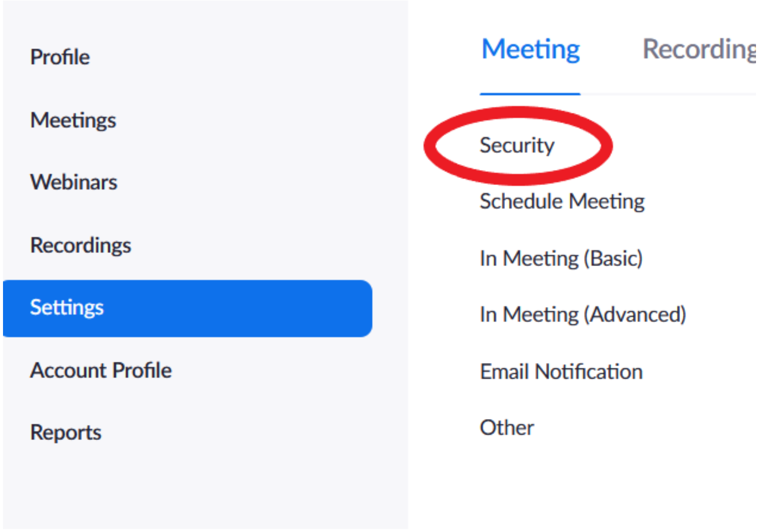
Preventing Unwanted Zoom Spammers/Bombers.

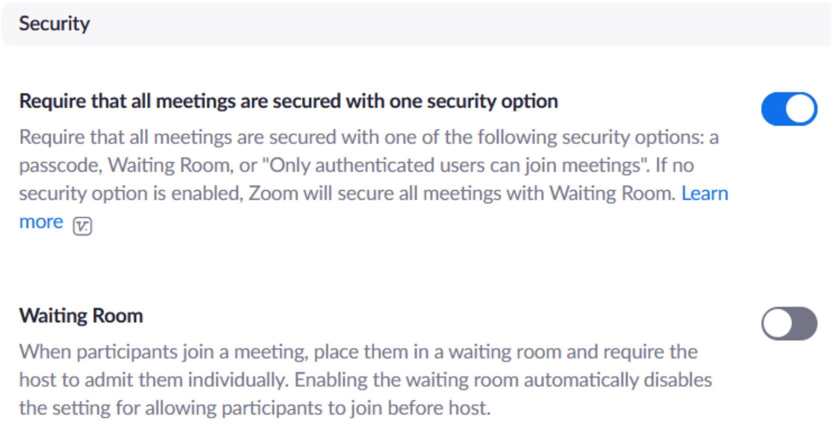
Zoom bombing is when someone, who is not supposed to be in your meeting, enters your Zoom meeting and begins spamming the chat or video feeds with unwanted dialogue or content. They may also post malicious links into chat in an effort to get participants to click on them. Although rare, for the obvious reasons, we will want to prevent that, so here are a few tips to make your Zoom meeting as secure as possible.

- If you are creating a Zoom meeting via your personal account, go into the account settings and make sure you have the following options selected. The Educ Zoom rooms, bookable via Booker, will have most of these account settings turned on by default.

  First go to Settings > Security.



  Now make sure you have “Require that all meetings have at least one security option.” Set to on.



Security

Require that all meetings are secured with one security option

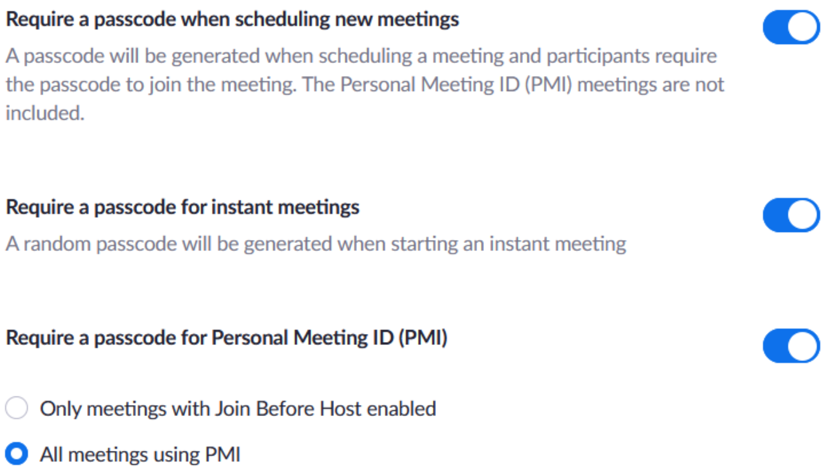
Require that all meetings are secured with one of the following security options: a passcode, Waiting Room, or "Only authenticated users can join meetings". If no security option is enabled, Zoom will secure all meetings with Waiting Room. Learn more

Waiting Room

When participants join a meeting, place them in a waiting room and require the host to admit them individually. Enabling the waiting room automatically disables the setting for allowing participants to join before host.

Unless you are going to be the only person using your account, do not turn on waiting rooms in your security settings or your during meeting schedule settings. The waiting room can be manually turned on by anyone you give the host code to when they enter the meeting. Turning them on prior to the meeting will mean that everybody arriving, including the person who will need to claim host, will become stuck in the waiting room until the account admin can let them in.

The rest of your security settings should look like this (below).



Require a passcode when scheduling new meetings

A passcode will be generated when scheduling a meeting and participants require the passcode to join the meeting. The Personal Meeting ID (PMI) meetings are not included.

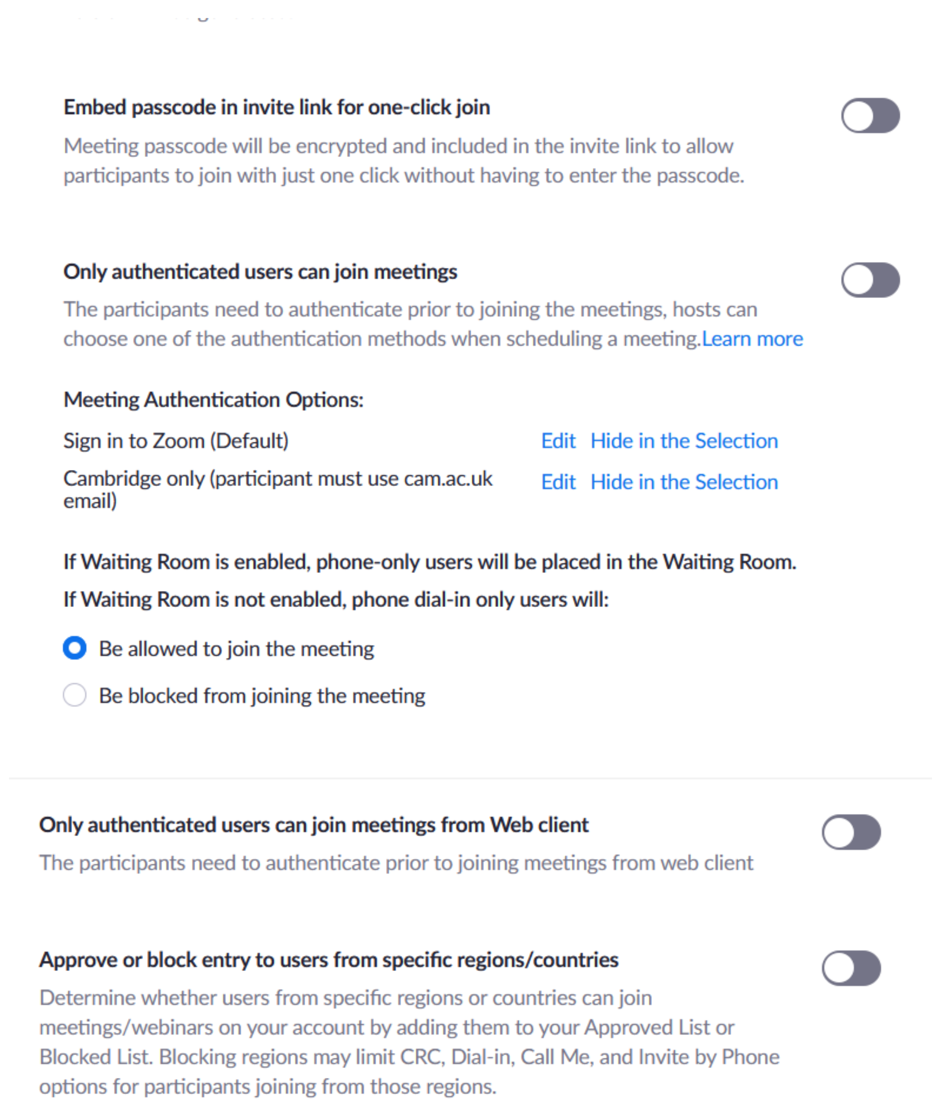
Require a passcode for instant meetings

A random passcode will be generated when starting an instant meeting

Require a passcode for Personal Meeting ID (PMI)

○ Only meetings with Join Before Host enabled

● All meetings using PMI



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.

Only authenticated users can join meetings

The participants need to authenticate prior to joining the meetings, hosts can choose one of the authentication methods when scheduling a meeting.Learn more

Meeting Authentication Options:

Sign in to Zoom (Default)	Edit Hide in the Selection
Cambridge only (participant must use cam.ac.uk email)	Edit Hide in the Selection

If Waiting Room is enabled, phone-only users will be placed in the Waiting Room.

If Waiting Room is not enabled, phone dial-in only users will:

● Be allowed to join the meeting

○ Be blocked from joining the meeting

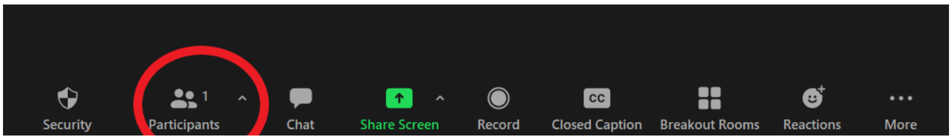
Only authenticated users can join meetings from Web client

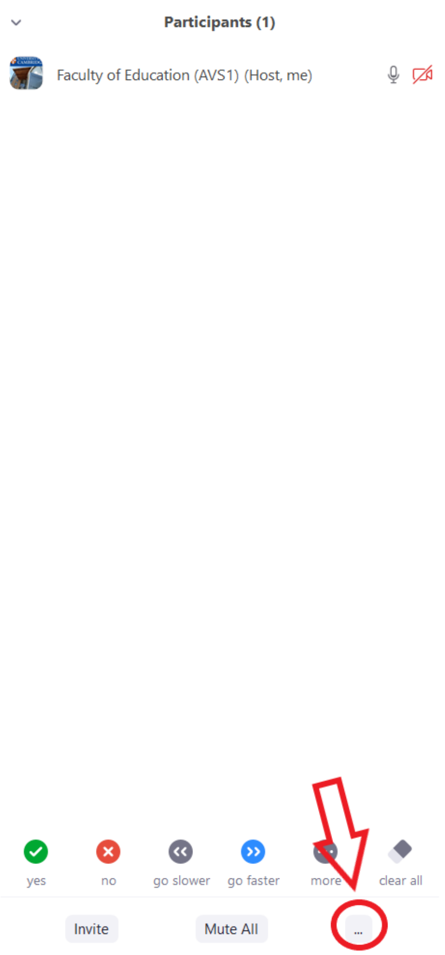
The participants need to authenticate prior to joining meetings from web client

Approve or block entry to users from specific regions/countries

Determine whether users from specific regions or countries can join meetings/webinars on your account by adding them to your Approved List or Blocked List. Blocking regions may limit CRC, Dial-in, Call Me, and Invite by Phone options for participants joining from those regions.

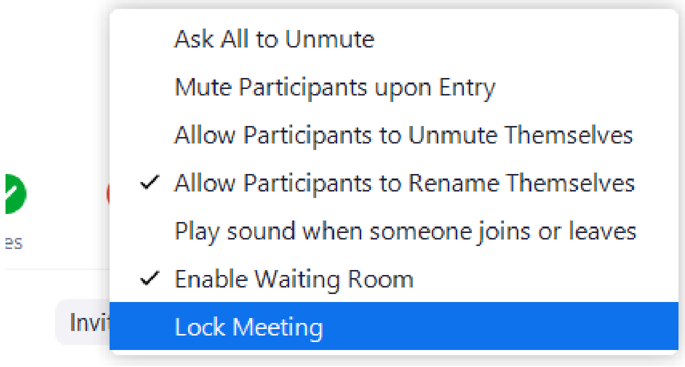
- Many security measures can be activated in the meeting itself, which is really useful if you are using one of the bookable Educ Zoom rooms. The most useful of these is the waiting room. To create a waiting room in your Zoom meeting, you must first either be the host, or claim host rights. To do this, you need to navigate to the Zoom toolbar – Usually located at the bottom of the screen, click on “Participants” and wait for the participants side-bar to pop out. At the very bottom right hand corner, you will see a tiny “…” icon. Click on that and select “Claim Host.” You will then be prompted to enter your host code.



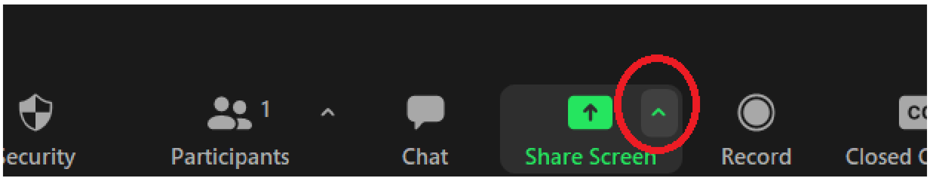


Once you have claimed host, you can now click on that same "…" icon again and select "Enable Waiting Room." Anyone arriving for the meeting will now be held in the waiting room and their names will appear in a waiting room box above the participants bar. You can then choose to admit or remove them. Nothing done within the main meeting room is visible or audible to those in the waiting room.

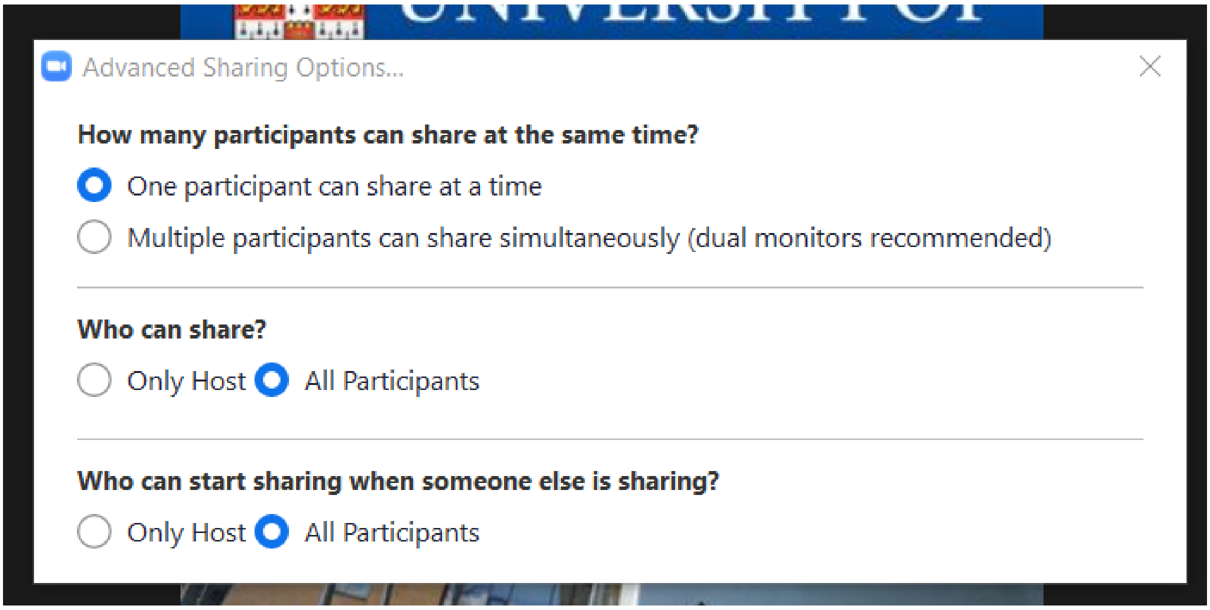
You can also set some meeting preferences via this menu, choosing to lock the meeting once everyone has arrived (it will need to be unlocked again if someone leaves and wishes to return) or making participants unable to unmute themselves. You can also mute all participants upon entry.


Ask All to Unmute
Mute Participants upon Entry
Allow Participants to Unmute Themselves
✓ Allow Participants to Rename Themselves
Play sound when someone joins or leaves
✓ Enable Waiting Room
Lock Meeting
es
Invi

- Using the Screen Share settings in meeting, you can control who can share their screen with the rest of the participants. This is easily configured by clicking on the little arrow within the screen share icon on the Zoom toolbar, navigating to “Advanced options”



This should bring up your meeting’s advanced sharing options. From here you can control who can share their screen and how it can be shared. Once configured, you can click on the main part of the icon to get to the usual screen share options.



Advanced Sharing Options...

How many participants can share at the same time?

● One participant can share at a time

○ Multiple participants can share simultaneously (dual monitors recommended)

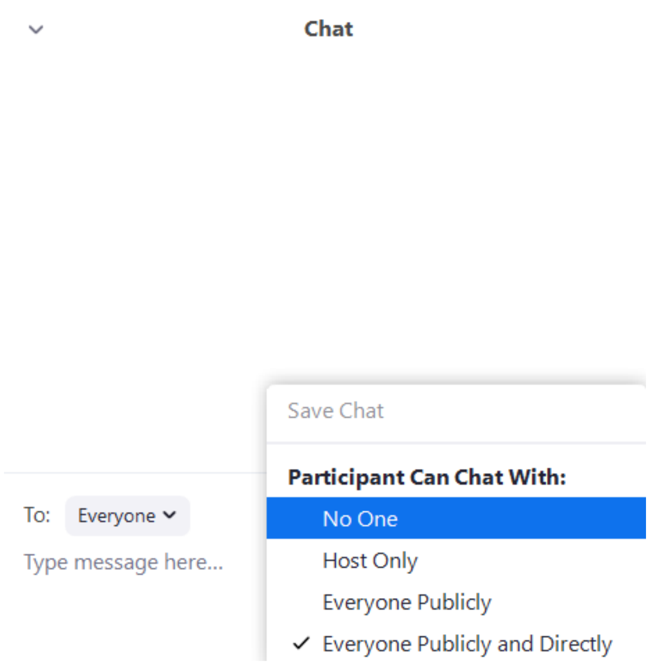
Who can share?

○ Only Host ● All Participants

Who can start sharing when someone else is sharing?

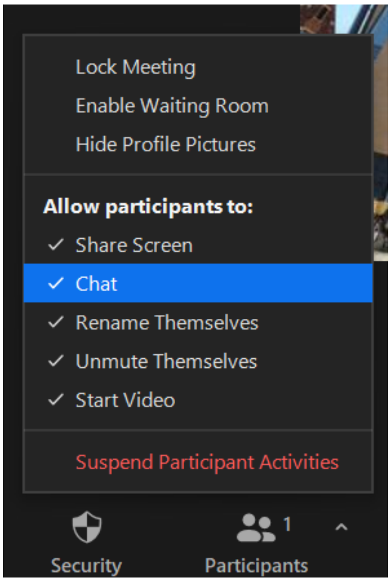
○ Only Host ● All Participants

- If your meeting does not require text chat, or you would like to restrict who sees chat messages, you can do this in your Zoom meeting by navigating to the Zoom toolbar and clicking on “Chat. “ This will open the chat, and you will see in the bottom right hand corner another “…” icon. Click on this for your chat options.



It should be set to “Everyone” by default, but you can change this in the meeting to suit your needs. This is very useful for Q&A’s and quickly shutting down spammers.

Alternatively, Chat can be disabled altogether by clicking on “Security” on the Zoom toolbar and unticking the “Chat” option.



- Through use of the above Security menu, you can also enable or disable Screen sharing, participants ability to start video and unmute themselves. Be aware that using the security menu in this way will deactivate these options for **all** participants.

- If someone does manage to slip through the net and enter the room anyway, you can remove them by clicking on their name in the participants list, then select “remove” from the drop down menu. If you have a waiting room enabled, you may see their name pop up there again, but unless someone admits them, they cannot re-enter the room or see anything that is happening in the meeting itself.