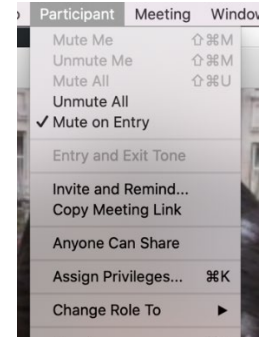


## Cisco Webex Securing your WebEx Meetings

### Mute participants on entry

Ensure participants are on mute as soon as they enter the meeting so that the main presenter can be uninterrupted upfront. If necessary, the user can unmute themselves at a later time or the meeting host can unmute them.

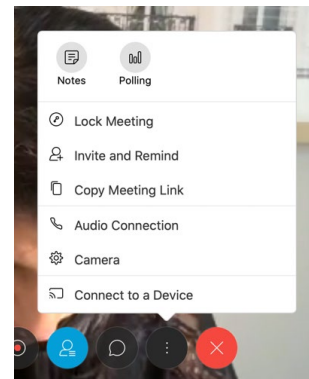


### Disable "Anyone can share"

Avoid unauthorized screen/application sharing by unchecking "Anyone can share". If necessary, the host can designate specific users as presenters in the course of the meeting.

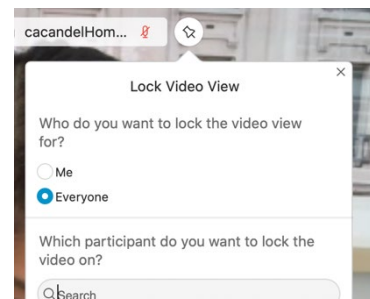
### Lock your meeting room

Once all the participants are in the meeting, the host can lock the meeting. Anyone trying to join after the meeting room has been locked will be placed in the lobby and will require authorization to enter the meeting.



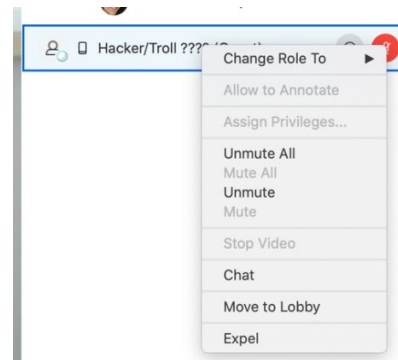
### Lock video view

To avoid users being distracted by other participants, pin the video of the presenter for everyone in the meeting.



### Keep participant panel easily accessible and learn the actions you can take.

In the event a participant is disruptive there are several actions the host can take. These are available by right clicking on the user in the participant panel. The key ones are **Mute**, **Stop Video**, and in extreme cases **Expel** the participant. If the room is locked, the user will not be able to return, unless authorized by the host.





# Information Technology Services

Guest accounts must be admitted from the Waiting Room.

Anyone joining your meeting who is not logged in to an HCCC WebEx account will be placed into the Waiting Room. You will need to allow them into the meeting.

Under **Waiting to Join**, do one of the following:

- To let in individual people, click **Let in** next to their name.
- To let in everyone who's waiting, click **Let everyone in**.

