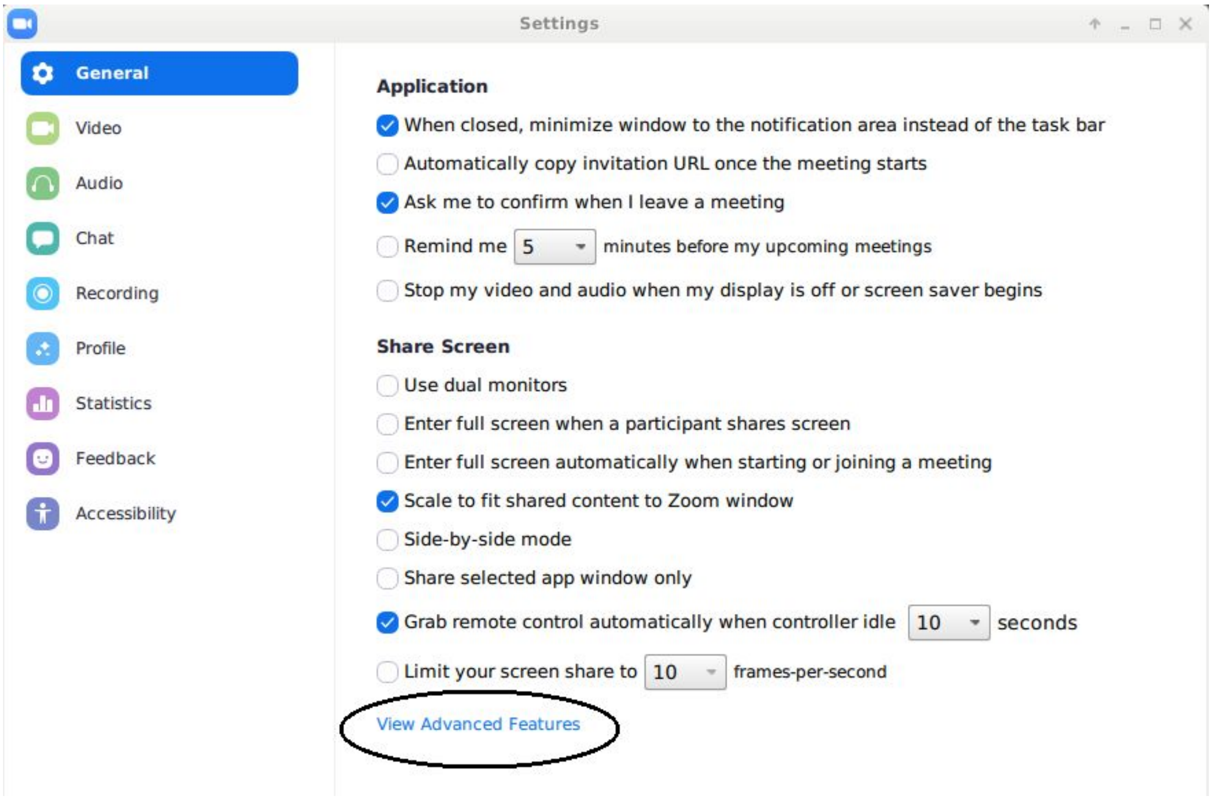
Suggested Settings for Security and Convenience in use of Zoom Cloud Meeting App

To access all the settings of Zoom Cloud Meeting App, the user has to log into the web version of Zoom account. The same can be accessed also from right top corner 'Settings' icon (or 'Settings' menu item from user profile icon) of Desktop App by clicking 'View More Settings' / 'View Advanced Features' as given below.



Application

☑ When closed, minimize window to the notification area instead of the task bar

□ Automatically copy invitation URL once the meeting starts

☑ Ask me to confirm when I leave a meeting

□ Remind me 5 minutes before my upcoming meetings

□ Stop my video and audio when my display is off or screen saver begins

Share Screen

□ Use dual monitors

□ Enter full screen when a participant shares screen

□ Enter full screen automatically when starting or joining a meeting

☑ Scale to fit shared content to Zoom window

□ Side-by-side mode

□ Share selected app window only

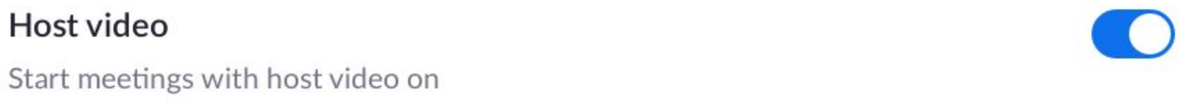
☑ Grab remote control automatically when controller idle 10 seconds

□ Limit your screen share to 10 frames-per-second

View Advanced Features

Following settings are suggested for better security and convenience in use of Zoom application.

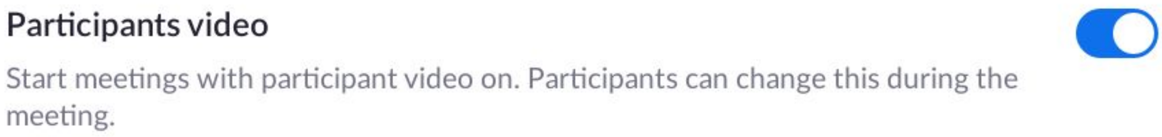
1. For ensuring that the video is by default switched on when the meeting is started so that the user is not required to always switch it on at the start of the meeting, the following setting should be kept on:



Host video

Start meetings with host video on

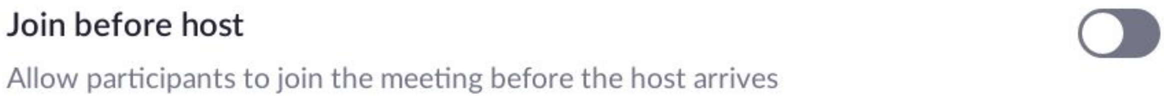
2. Similarly, for ensuring that the participant doesn't have to always click on the video/movie icon for starting the video, the following setting should be kept on:



Participants video

Start meetings with participant video on. Participants can change this during the meeting.

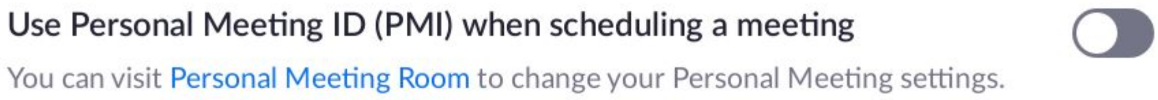
3. To ensure that after sending the link, the participants join after the host has joined, the following setting should be kept off:



Join before host

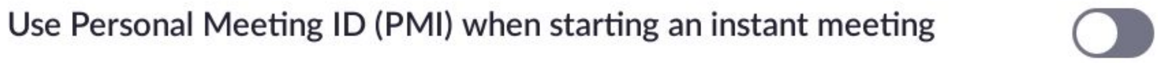
Allow participants to join the meeting before the host arrives

4. It is advisable that, in case of scheduled meeting or an instant meeting, the Personal Meeting ID (which is always same for the particular user account) is not used but a random instant meeting ID is used. For the same, following two settings should be kept off:



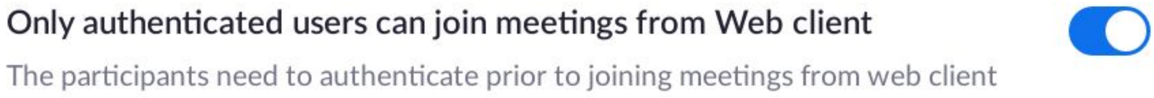
Use Personal Meeting ID (PMI) when scheduling a meeting

You can visit Personal Meeting Room to change your Personal Meeting settings.



Use Personal Meeting ID (PMI) when starting an instant meeting

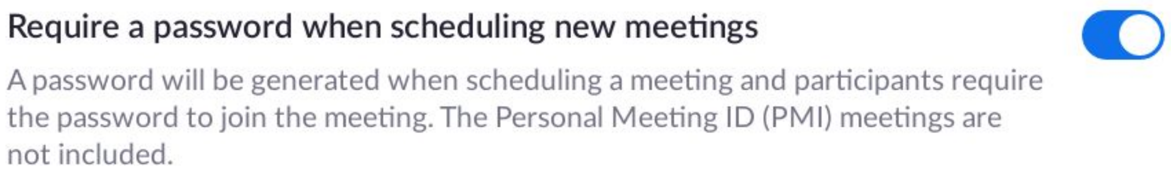
5. The Zoom application has also facility of allowing the participants to join from the web-browser and also without having to login to their account. It is advisable that, when the participant joins from such web-client, he/she joins only after authentication. For the same, the following setting should kept on:



Only authenticated users can join meetings from Web client

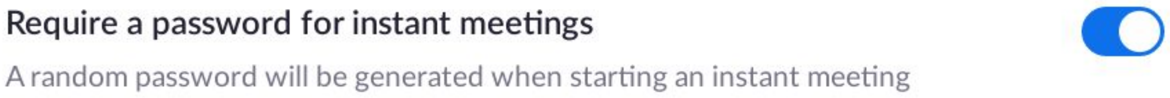
The participants need to authenticate prior to joining meetings from web client

6. It is necessary that while initiating new scheduled or instant meetings, the same should be with password so that someone just having meeting ID is not able to jump into the meeting. For the same, the following settings should be kept on:



Require a password when scheduling new meetings

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

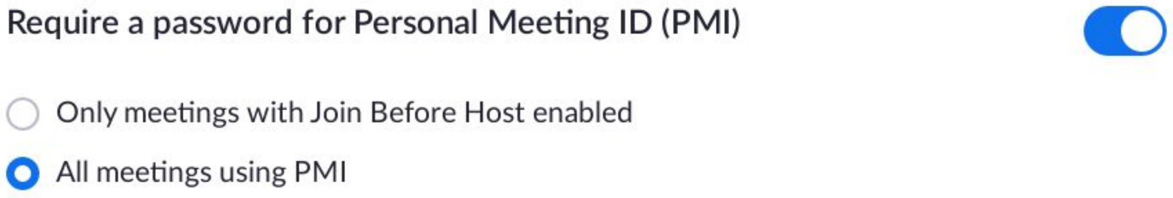


Require a password for instant meetings

A random password will be generated when starting an instant meeting

Note: For such meetings, the Meeting Invite (URL) can have embedded passwords as given at Sr. No. 8 hereinbelow.

7. Similarly, whenever for any reasons, if the host user wants to initiate a meeting with Personal Meeting ID (which is not advisable and should be avoided), the same should always be a password protected meeting. For the same, the following should be kept on with 'All meetings using PMI' also on:

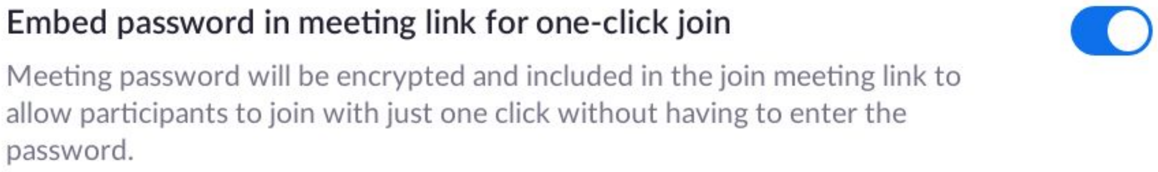


Require a password for Personal Meeting ID (PMI)

○ Only meetings with Join Before Host enabled

● All meetings using PMI

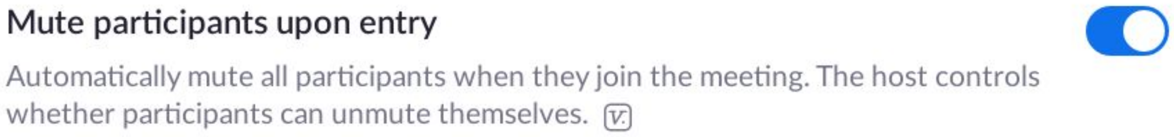
8. For the reasons of convenience and avoiding time lag between one meeting and another meeting, if the joinees are identified trusted users, the following setting may be kept on so that the Meeting Invite URL (meeting ID link) contains the password in encrypted form in the link itself:



Embed password in meeting link for one-click join

Meeting password will be encrypted and included in the join meeting link to allow participants to join with just one click without having to enter the password.

9. To avoid chaos and unnecessary noise in the meeting room, it is advisable that, by default the participants are in 'Mute' position while they join the meeting. For the same, the following setting may be kept on.

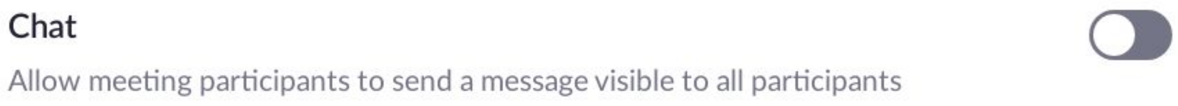


Mute participants upon entry

Automatically mute all participants when they join the meeting. The host controls whether participants can unmute themselves.

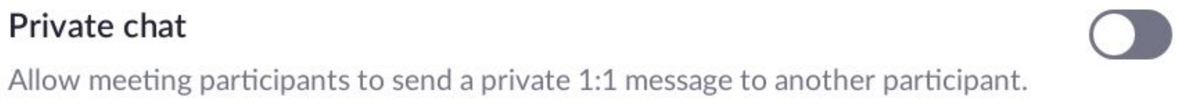
On joining and when they need to speak, they can unmute their microphones.

10. To avoid unnecessary text (chat) messaging interruptions during the meetings, the following settings should be kept off:



Chat ○

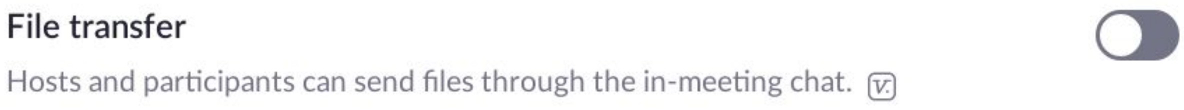
Allow meeting participants to send a message visible to all participants



Private chat ○

Allow meeting participants to send a private 1:1 message to another participant.

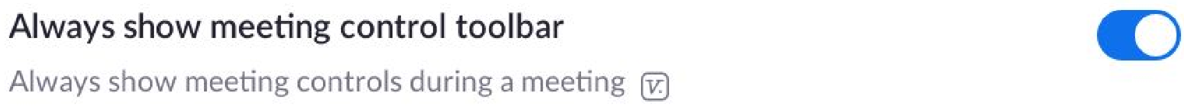
11. For security purposes, the facility of File Transfer between host/participants, should be kept off



File transfer ○

Hosts and participants can send files through the in-meeting chat.

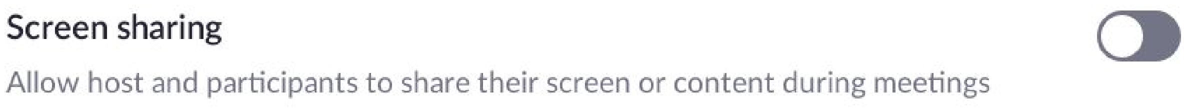
12. For ease of use of new users, the toolbar showing various icons of controlling the meeting should be kept on:



Always show meeting control toolbar ●

Always show meeting controls during a meeting

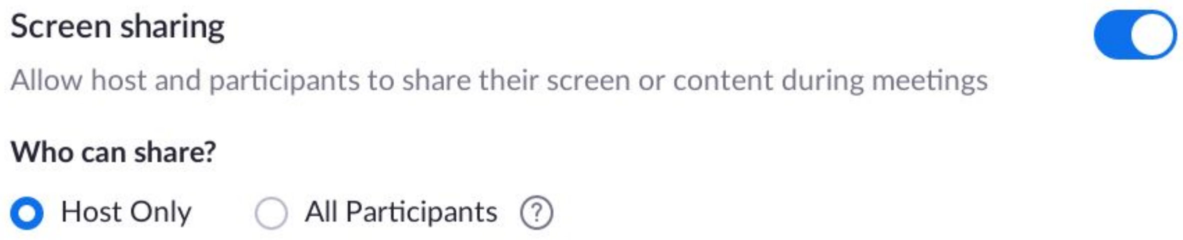
13. For security purposes and interruption free meetings, the screen sharing facility must be kept off.



Screen sharing ○

Allow host and participants to share their screen or content during meetings

If, for any unavoidable reasons, this facility has to be switched on, the same should be only for the host. This can be ensured by keeping setting as given below:



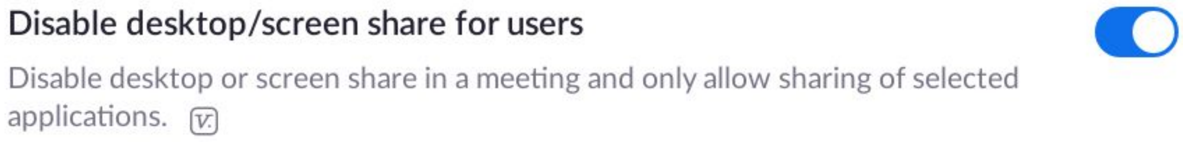
Screen sharing

Allow host and participants to share their screen or content during meetings

Who can share?

● Host Only ○ All Participants

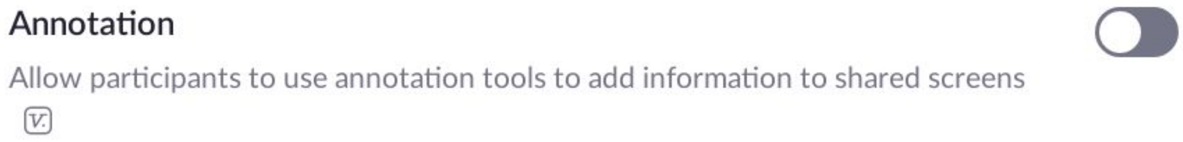
14. The screen sharing facility, if enabled, is advised not to be allowed for the whole desktop but selected applications only. For the same, the following setting may be kept on:



Disable desktop/screen share for users

Disable desktop or screen share in a meeting and only allow sharing of selected applications.

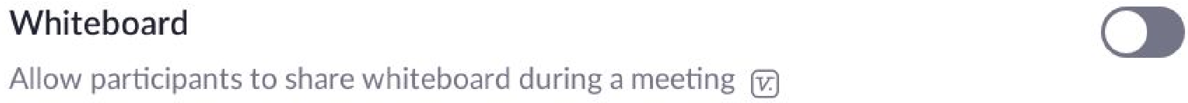
15. The users should not be allowed to annotate (write over the videos/screens) to avoid any misuse of the facility and ensuring distraction free meetings. For the same, the following setting should be kept off:



Annotation

Allow participants to use annotation tools to add information to shared screens

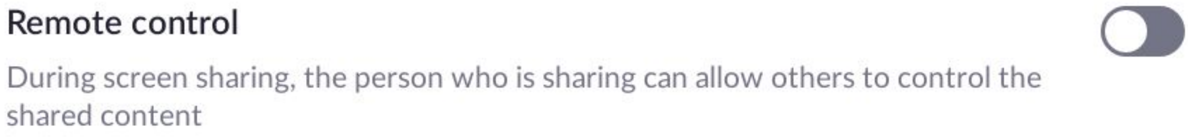
16. Whiteboard feature, which is useful for classroom session type of meetings or more interactive board meetings, should be kept off:



Whiteboard

Allow participants to share whiteboard during a meeting

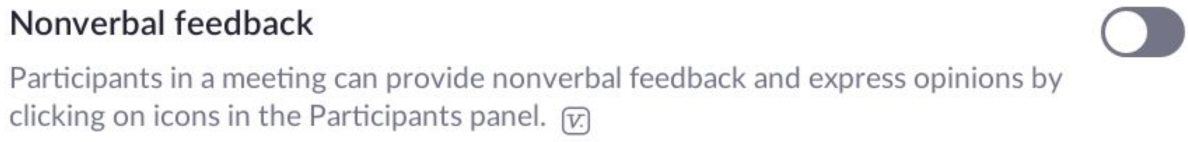
17. If the screen sharing is enabled for any reason, the following setting should be disabled under all circumstances:



Remote control

During screen sharing, the person who is sharing can allow others to control the shared content

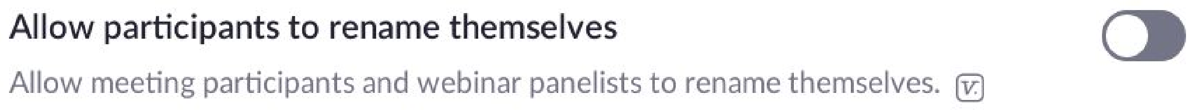
18. Facility of use of emoji like icons for expressing any non-verbal feedback/messages should be kept of as follows:



Nonverbal feedback

Participants in a meeting can provide nonverbal feedback and express opinions by clicking on icons in the Participants panel.

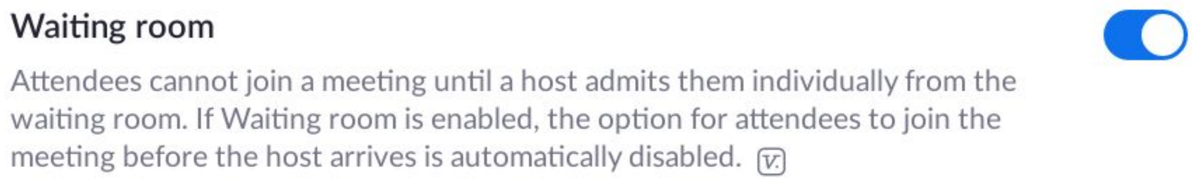
19. The participants are required to use their real name IDs during the meeting. They should not be allowed to rename themselves. For the same, the following setting should be kept off:



Allow participants to rename themselves

Allow meeting participants and webinar panelists to rename themselves.

20. Waiting Room feature is a way to identify participants before they are allowed to enter a meeting. This also gives the host greater control over session security. If required, this may be used by keeping the following setting on:

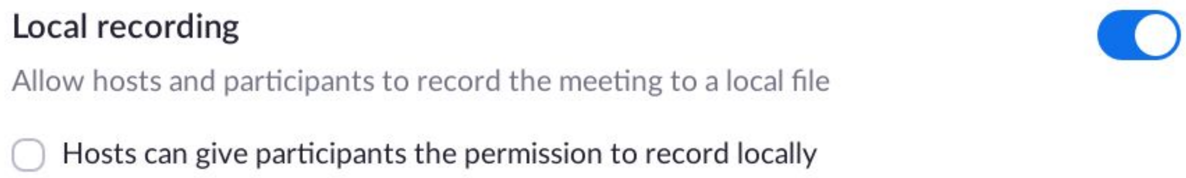


Waiting room

Attendees cannot join a meeting until a host admits them individually from the waiting room. If Waiting room is enabled, the option for attendees to join the meeting before the host arrives is automatically disabled.

Note: The host user should be careful in promptly seeing the Waiting Room and Admitting the identified users so that legitimate users should not be unnecessarily kept waiting in the Waiting Rooms.

21. Recording of video conferencing sessions should be kept for record purpose and should not be shared with anyone. But the option for recording should be enabled only for the host and host should not give permission to the participants for recording the sessions. For the same, the settings should kept as follows:

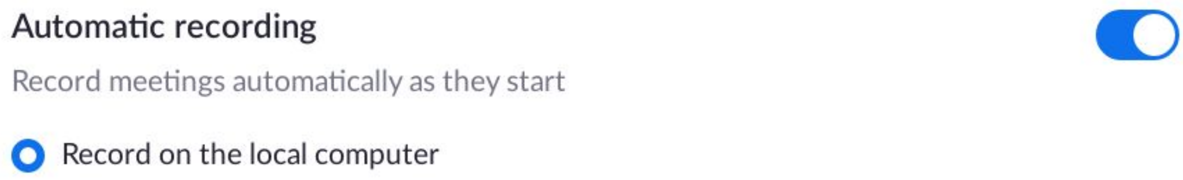


Local recording

Allow hosts and participants to record the meeting to a local file

☐ Hosts can give participants the permission to record locally

Automatic recording can also be enabled, if desired.



Automatic recording

Record meetings automatically as they start

◉ Record on the local computer
