Zoom – Recommended Settings for Instructors

Updated 9/15/2020; Zoom version: 5.2.3
See Zoom download page for current client

This document summarizes the Zoom settings SAS IT recommends for instructors as well as the rationale and potential trade-offs behind them so that you can choose what makes sense for your circumstances.

Zoom security has been improving but Zoom bombing remains a concern. *Bombing* is when uninvited guests manage to enter your Zoom session and try to disrupt it.

OIT has recently enabled a key option – Rutgers-only authentication – that will help prevent bombers from easily accessing your Zoom sessions. There are several other options that may also minimize the risk of such intrusions happening, particularly when meetings can't reasonably be restricted to Rutgers-only, as well as the degree of disruption that is possible should an unwanted guest manage to get into your session.

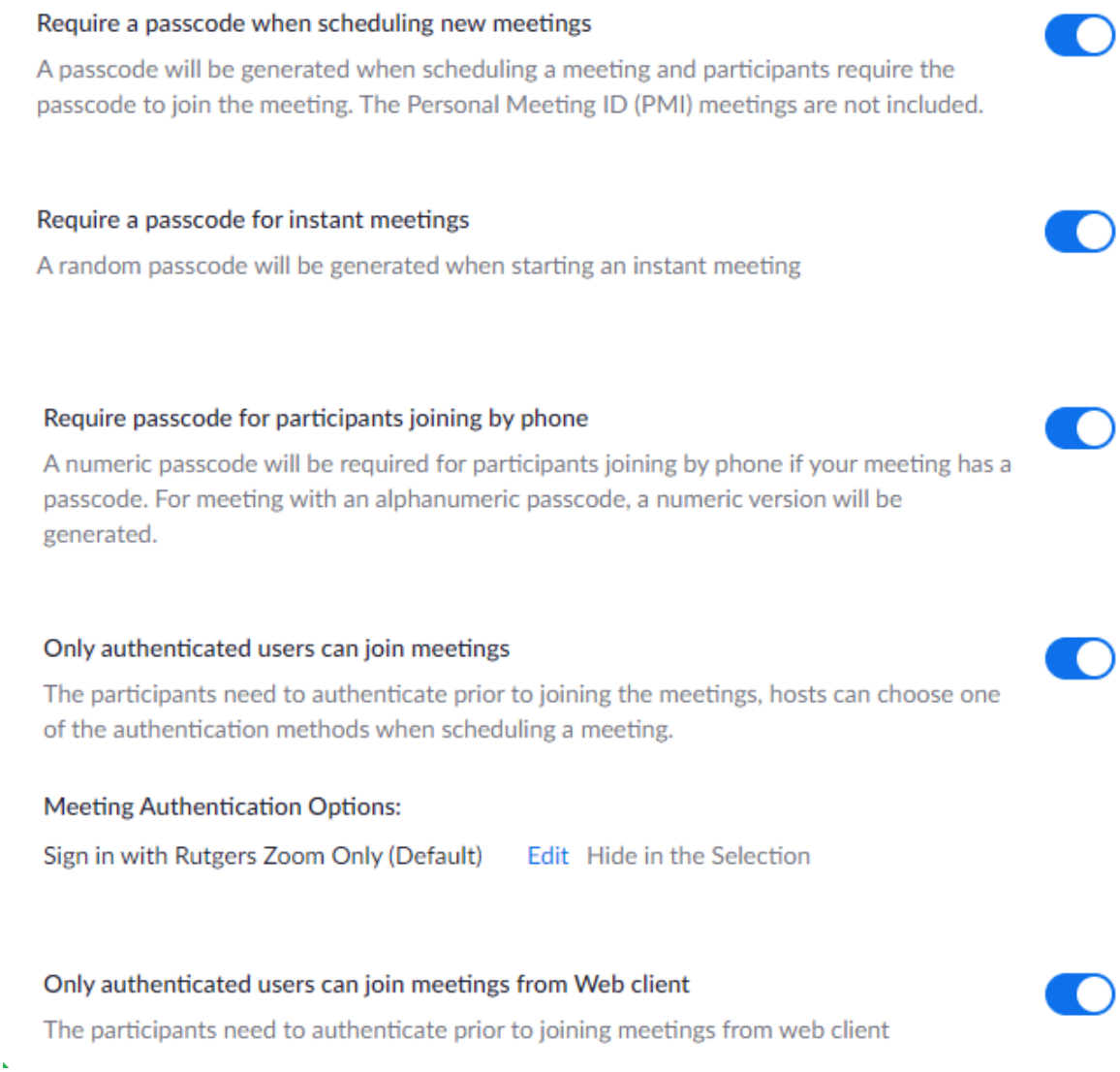
All settings mentioned below are available via your Rutgers Zoom profile at https://rutgers.zoom.us/profile/setting. Hint: Try using your browser's built-in search mechanism (press Ctrl-F) to locate settings on this page. Some settings may also be applied to or overridden by the settings for individual meetings, which may be edited via https://rutgers.zoom.us/meeting. After making changes in your profile, you may want to spot-Edit an already-scheduled meeting or three to verify the settings are as you expect, and then possibly create a new test meeting to verify that future meetings will behave as desired. Always test, test, test ahead of time.

Some common questions are, when do settings take immediate effect and when are they only defaults? Does changing a setting in my profile affect previously scheduled meetings? A rule of thumb might be this: If a setting is visible in the scheduler interface, that means it may be overridden for individual meetings. For these settings, the values you select in the settings page in your profile therefore act as a *default* value that you can adjust for any given new meeting and will not change the values attached to already-scheduled meetings. If you do not see a setting in the meeting scheduler, it is not one that can be controlled on a meeting-by-meeting basis, and therefore setting this in your profile will affect all meetings going forward. At least, this is how we currently understand the behavior. Note that changing some settings *may* impact currently running sessions but others may only take effect in future meetings.

Without further ado, **the recommended settings are as follows**.

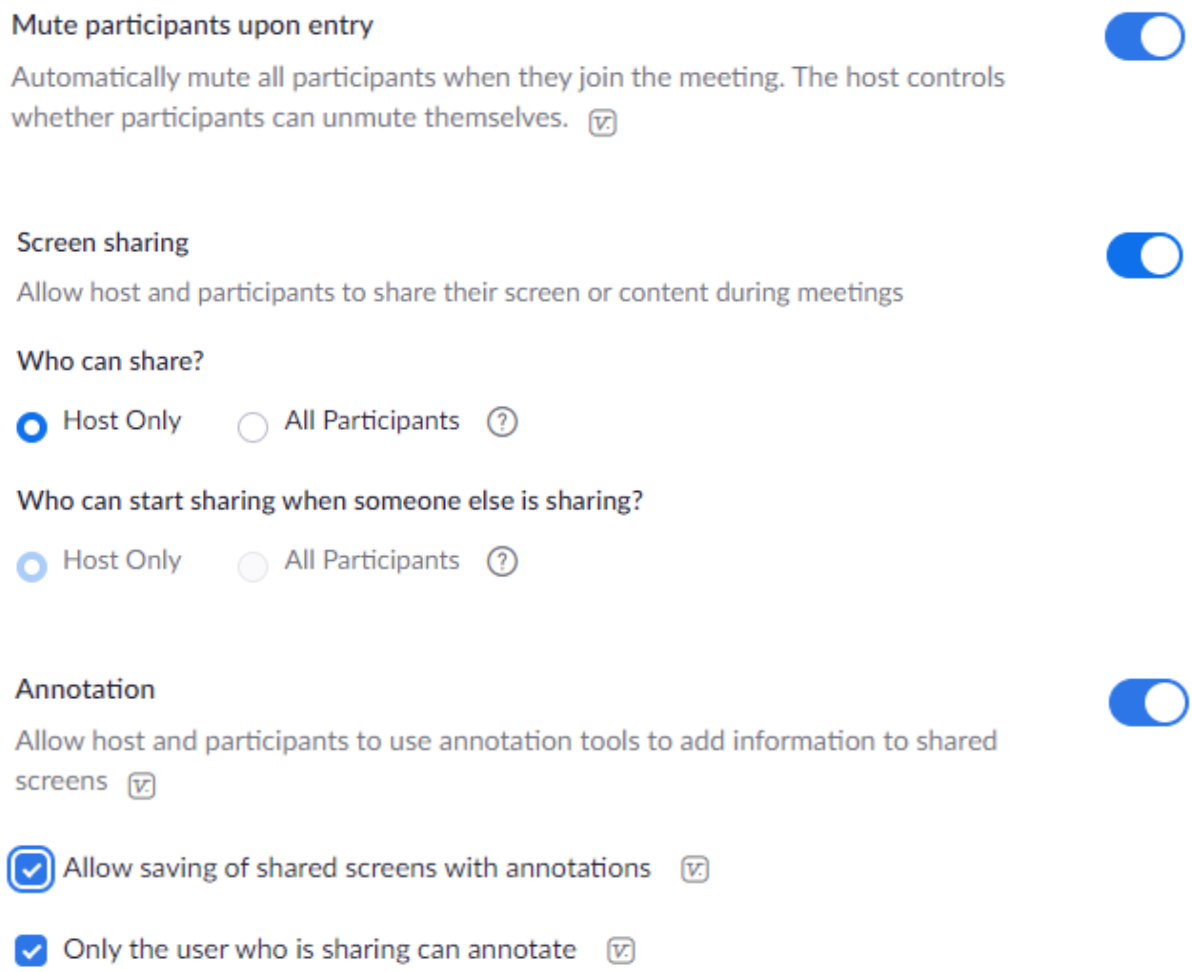
1. Authentication options**.** Enable these (see screenshots below)**:**
    a. Require a passcode when scheduling new meetings
    b. Require a passcode for instant meetings
    c. Require passcode for participants joining by phone
    d. Only authenticated users can join meetings

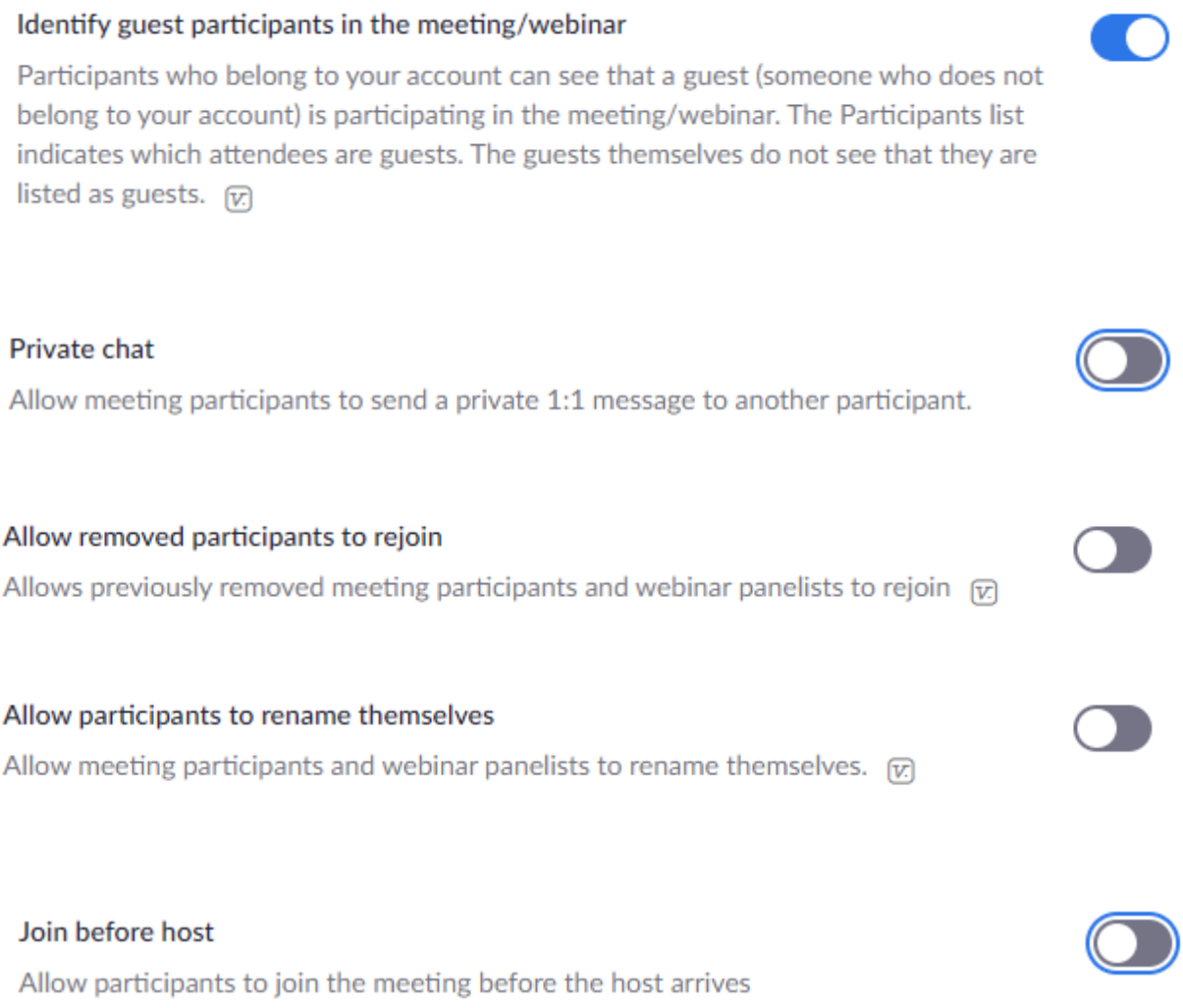
e. Meeting Authentication Options: automatically changes to Sign in with Rutgers Zoom only when requiring authentication
f. Only authenticated users can join meetings from Web client



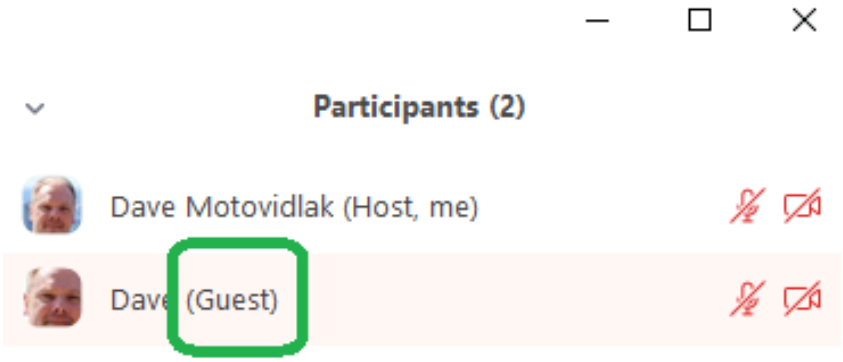
Rationale and trade-offs: These settings maximize control over access to meetings, even if the invitation link is made public. Participants dialing in via phone will encounter the extra encumbrance of needing to type a numeric pass code. Anonymous and non-Rutgers Zoom users will be unable to attend the meeting either via the app or the web client. If you need to meet with non-Rutgers people, you must disable the authentication options (at least for that single meeting) and fall back to relying on keeping the invitation link + password known to only the people you wish to attend. Note that you can still Lock any meeting after all the participants have joined, and you may enable the Waiting Room feature to control entry on a person by person basis. You may also Remove disruptive participants or employ any other in-app control mechanism offered via the Security panel, the Participants panel, or the individual participant tile for a given participant.

2. <u>In-meeting and startup behavior.</u> Match these:
    a. Mute participants upon entry: Enabled
    b. Screen sharing: Enabled
    c. Who can share? Host Only
    d. Who can start sharing when someone else is sharing? Host Only
    e. Annotation: Enabled
    f. Only the user who is sharing can annotate: Enabled
    g. Identify guest participants in meeting/webinar: Enabled
    h. Private chat: Disabled
    i. Allow removed participants to rejoin: Disabled
    j. Allow participants to rename themselves: Disabled
    k. Join before host: Disabled



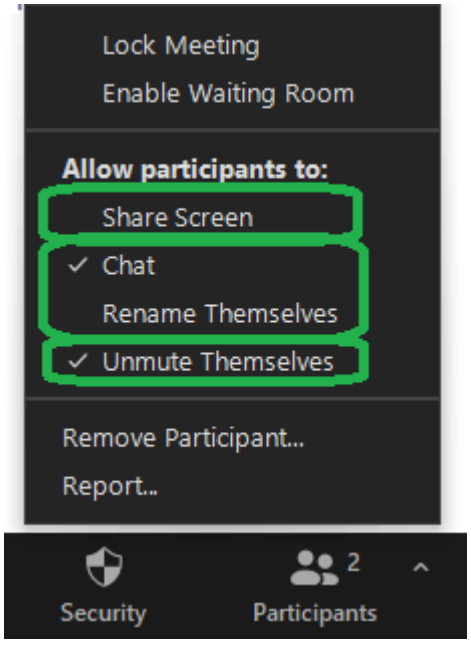


Rationale / trade-offs: Should a bomber manage to gain access to your meeting, the preceding settings will make it more difficult for them to cause large scale disruption. For instance, microphones will be muted by default, only the Host will be able to Share their screen, and only the Host will be able to take over the Share feature if someone else is sharing (e.g., if sharing for attendees was temporarily enabled). Thus, any bomber that does manage to gain entrance would be unable to speak, play sounds, or share images. Because "Guest" status (non-Rutgers people) will be clearly indicated in the Participants panel, the intruder should be easier to identify and eject.

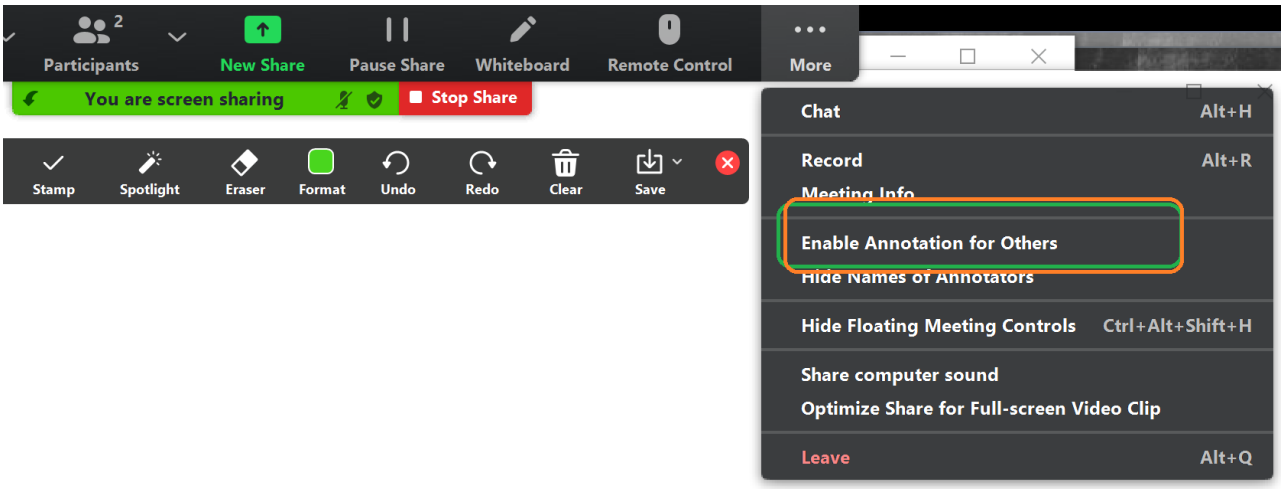


Private chat between participants will be disabled, thus also preventing bombers in the session from chatting directly to individual participants, which would be invisible to you as host. (You may also disable Chat altogether, thus preventing a chat message being sent to Everyone, but you might consider public Chat a critical feature and not worth disabling by default.) Additionally, participants that you've Removed will not be able to re-enter the meeting, participants won't be able to disguise themselves by changing their display name, and participants will not be able to enter the meeting before the host is there to keep things in order.

Note that most of these are *default* behaviors and that you can override many of them while in the meeting. For instance, the meeting host can use the Security toolbar item to temporarily enable Share Screen so that participants can share their screen. (Unfortunately, there is no way to give this right to only a single participant – except perhaps by making them co-host temporarily, though that probably gives them more power than you may like.) The other settings will prevent a different participant, including a bomber, from grabbing control of the share feature, and you can disable Sharing as soon as it is no longer needed.



Sharing security enhances Annotation security via the setting that allows only the sharing user to annotate. So sharing is limited, and annotation of shared windows is further limited. Thus, a bomber could not by default use the annotation feature to deface a screen that is being shared. However, if sharing is temporarily enabled, the sharing user retains the *option* to dynamically toggle on Annotation for others via the top menu bar. Naturally, dynamically enabling this feature or others opens a small window of opportunity for disruption, but this would require some lucky timing on the part of any bombers and thus significantly decreases the probability of a major incident.



Notably, some of the settings may *require* in-meeting practices to be effective. For instance, there appears to be no setting that disallows participants from unmuting themselves by default. Instead, you must click Security in the toolbar and uncheck "Unmute Themselves." Without doing this, a bomber that gets into a meeting could simply unmute himself and use the mic for nefarious purposes. Via this same panel you could also temporarily disable Chat altogether or Remove a disruptive participant. So it is probably a good idea to develop a habit of checking the Security panel at the start of every meeting to make sure the settings align with what you're trying to achieve and that you're mentally prepared for how to deal with a disruptive participant. If you remember at the start of the meeting to disable the Unmute Themselves option, for instance, the chances of a bomber using their mic to disrupt the session are dramatically reduced.

Of course, instructors must weigh the protection these settings and practices provide against the convenience and functionality they reduce. In meetings with fewer participants, for instance, instructors may choose to leave enabled the ability of participants to Unmute Themselves so that they can more readily interact with the class. Instructors might also decide that forcibly silencing their students just sets the wrong tone in their particular setting. On the other hand, in larger settings, instructors may rightly expect that students are there mostly to listen and not speak, and so keeping them silent until a proactive measure is taken by the instructor to Unmute them is the better default stance. Similarly, depending on your philosophy and aims, preventing students from chatting privately with each other might be deemed an advantage or a disadvantage. *Etcetera.*

It's up to you. Hopefully you now feel better armed to make those choices.