



PgUS Guide to Security on Zoom

This document was put together to provide general guidance on increasing the security of meetups that run on Zoom platform.

Add meeting password

Set a password for your meeting to prevent unanticipated guests from joining.

How to share password with participants:

- send password only to registered participants
- post the password for a meeting in a separate post via your social media
- Create google doc where you will have all the information about your meet-up as well as meet-up link and password.

! Never post both the meeting ID and password together (or a URL combining both) on a public-facing Web site.

Use waiting room

Use the Waiting room controls when participants join the session.

Limit screen sharing to a host

This will prevent attendees to write on screen during your meeting.

Speakers: There is an option of adding co-host with the same permission, so you can do that for your speakers.

Webinar

Depending on Zoom subscription level, you might be able to run a Webinar. This option makes it easier to navigate between different types of participants and their controls.

Here is what your regular Zoom meeting setup will look like:

The screenshot shows the Zoom meeting settings interface. It includes sections for Security, Video, Audio, Calendar, and Advanced Options. In the Security section, 'Passcode' is set to 'test123'. In the Video section, both Host and Participants are set to 'Off'. In the Audio section, 'Telephone and computer audio' is selected. In the Calendar section, 'Google Calendar' is chosen. In the Advanced Options section, 'Mute participants upon entry' is checked. Alternative hosts listed are 'cohost@email.com' and 'cohost2@email.com', and 'Allow alternative hosts to add or edit polls' is checked.

If you want to read more on the topic we suggest this [article](#) about Zoom settings and [this](#) webinar vs. regular meeting comparison. Still have questions? Contact us on ugcomm@postgresql.us