Secure your zoom Meeting

Why so secure?

With the nationwide shift from in person to online business interactions, organizations throughout the country including government entities have experienced "Zoombombing". "Zoombombing" is the practice of bad actors joining Zoom meetings to share racist, misogynistic, and/or vulgar content via both screen-sharing and chat communications.

The good news is, every Zoom host can take large steps to prevent this by adjusting their Zoom settings and in meeting host controls to enhance the security of the Zoom client and keep these bad actors at bay. By implementing the steps listed below into your Zoom desktop client and web application, you will strengthen the security of your Zoom meetings and better ensure you remain in control.

We understand at times, it may not be possible to complete all the steps below for every meeting you host. However, it is important to keep in mind that any time a security setting is relaxed, the risk increases.

What can you do?

Are you a Participant?

1. *Make updating your Zoom client a habit.*
You can check for updates anytime by logging into your **Zoom Desktop Application**, clicking on your profile photo (or initials) and selecting Check for Updates from the drop-down list.

Are you a Host?

Step 1 above and:

From the Zoom Web Application (https://zoom.us/) set the following global settings. *A global setting will apply to all future meetings and will not need to be set again.*

2. Click on MY ACCOUNT in the upper right corner.

3. Then, select your Zoom Settings located on the left-hand side of the screen and do the following:

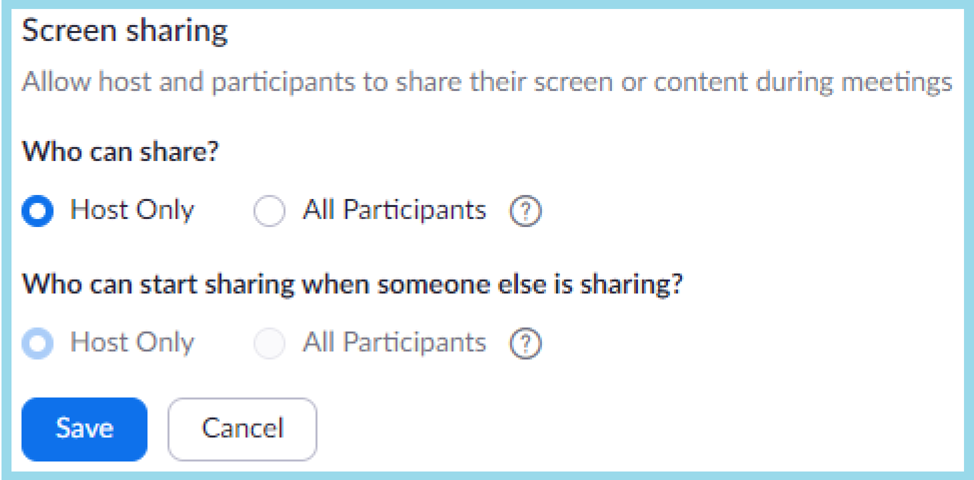
- **Enable Auto Saving Chats**
- **Disable File Transfer**
- **Limit Screen Sharing to Host Only**

tech tip!

You will know that the setting is disabled when the slider turns gray.

Enabled features will show as a blue slider.

Don't forget to save!



Screen sharing

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

Who can share?

● Host Only ○ All Participants ?

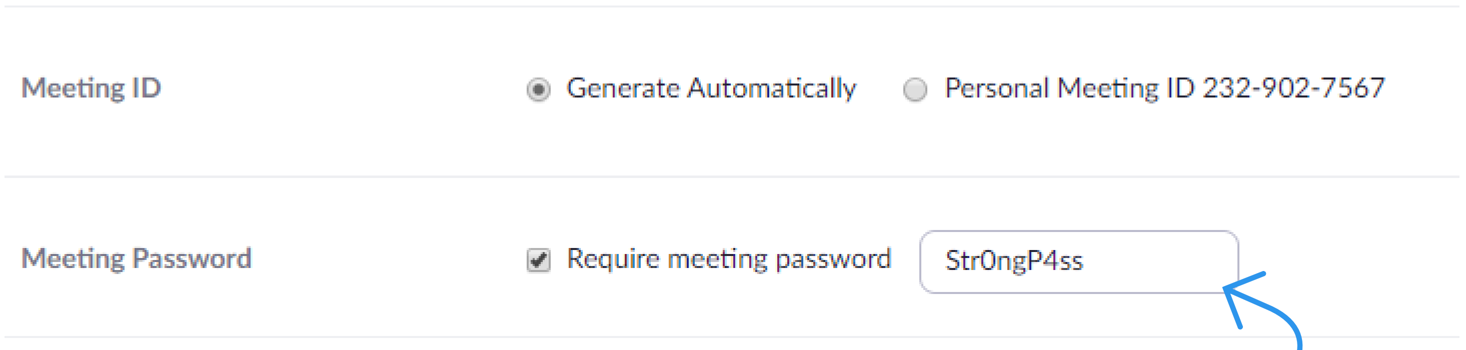
Who can start sharing when someone else is sharing?

● Host Only ○ All Participants ?

- **Disable Annotation**
- **Disable Allow removed participants to rejoin**
- **Enable the Waiting Room**

4. From either the Zoom Desktop or Zoom Web Application set the following per-meeting settings. *Per-meeting settings only apply to the selected meeting and will need to be reset for every meeting you host.*

- **Set your Meeting ID to Generate Automatically**



Meeting ID ● Generate Automatically ○ Personal Meeting ID 232-902-7567

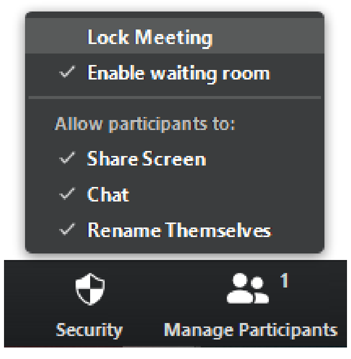
Meeting Password ☑ Require meeting password StrOngP4ss

tech tip!

Set a new password for each meeting you host.

- **Enable Join before Host**
- **Deselect**

5. Once your meeting has started, lock-down your meeting to uninvited guests by selecting Security from the bottom navigation bar and then selecting Lock Meeting.



What additional measures can you take?

- Assign an Alternative Host before the meeting in your global settings or a Co-host during the meeting to assist with waiting room, chat, and participant monitoring. (These features are only available for paid Zoom users.)
- *Never* post any links to join meetings on the web, social media, or through a mass distribution list. Provide the link directly to the specific people who need to attend the meeting.
- Do not allow single sign-on with social media accounts. Login must be through a password.
- Create a strong password for each meeting. Change the meeting password for each meeting you host.
- Do not use your personal meeting ID for any business meeting.