



# Quick Reference

## How to Secure Your Zoom Meetings

With the significant increase of remote work due to COVID-19, there have been some concerns regarding the security of online meetings hosted in Zoom. This document provides some valuable information on how to ensure the security of your Zoom meetings.

### Some of the in-meeting security capabilities that are available to the meeting host include:

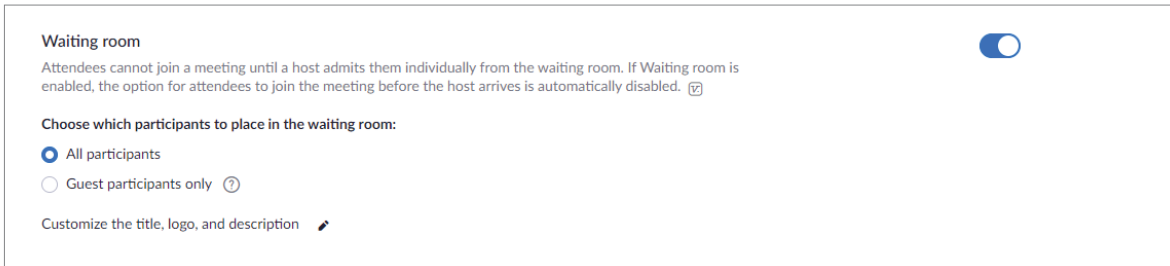
- Secure a meeting with end-to-end encryption
- Create waiting rooms for attendees
- Require the host to be present before the meeting starts
- Expel a specific participant or all participants
- Lock a meeting
- Screen share watermarks
- Create audio signatures
- Enable/disable a participant or all participants to record
- Temporarily pause screen-sharing when a new window is opened
- Password-protect a meeting
- Allow only individuals with a given email domain to join


### Here are five easy steps to follow to further secure your Zoom meetings:


1. When you set up Zoom, you are given a Personal Meeting ID. This means that as a meeting host you have a dedicated meeting room that never changes. To keep your meetings secure, generate a random meeting ID each time. To do so, go to your Zoom Web Settings and select **Schedule a Meeting**:

Meeting ID	<input checked="" type="radio"/> Generate Automatically	<input type="radio"/> Personal Meeting ID <span style="background-color: black; color: black;">XXXXXXXXXX</span>
Meeting Password	<input checked="" type="checkbox"/> Require meeting password	<input type="text" value="672080"/>

2. You can then enable the **Waiting Room** option for your meeting, which provides a holding area and the ability to customize a message with guidelines on who is allowed to join. Under **Settings**, select **In Meeting (Advanced)** then **Waiting Room**.





**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. 

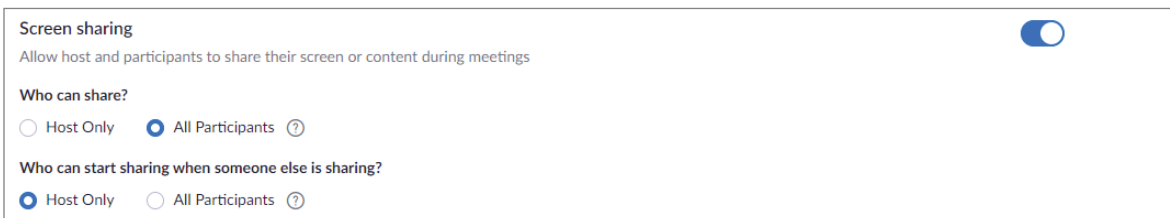
**Choose which participants to place in the waiting room:**


All participants

Guest participants only 

Customize the title, logo, and description 


3. You can select who is allowed to share their screen during the meeting. In **Web Settings**, go to **In Meeting (Basic)** and lock the **Screen Sharing** as a default option.




**Screen sharing** 

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

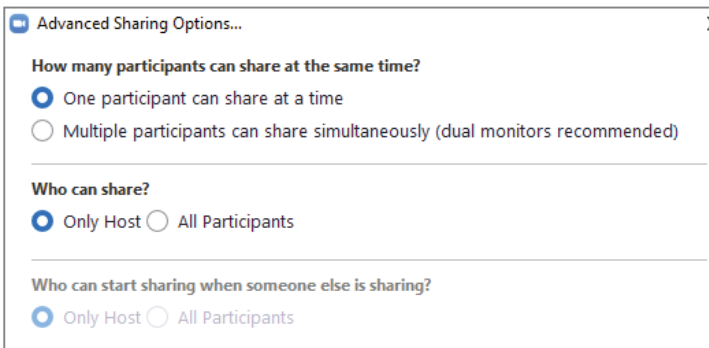
**Who can share?**


Host Only  All Participants 

**Who can start sharing when someone else is sharing?**

Host Only  All Participants 

While in the meeting, click on **Share Screen**, click **Advanced Options**, and then select **Only Host** can share.



**Advanced Sharing Options...** 

**How many participants can share at the same time?**

One participant can share at a time

Multiple participants can share simultaneously (dual monitors recommended)

---

**Who can share?**

Only Host  All Participants

---

**Who can start sharing when someone else is sharing?**

Only Host  All Participants

4. Unless there is a very specific reason, you can disable file sharing. Go to **Settings**, click **In Meeting (Basic)**, then disable **File Transfer**.



**File transfer** 

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

5. You can also strictly control who joins the meetings (i.e., if they are not on the list, they cannot get in). Go to **Web Settings**, click **Schedule Meeting**, and then enable **Only Authenticated Users Can Join Meetings**. Even if someone finds the meeting links and password, they still need to be logged in to Zoom. You can also lock down further by requiring them to be in a specific domain.

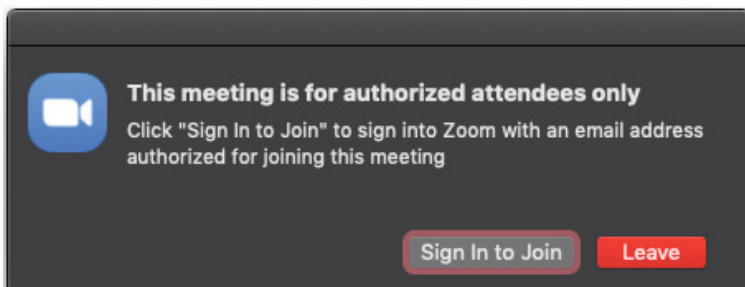
**Only authenticated users can join meetings**

The participants need to authenticate prior to joining the meetings, hosts can choose one of the authentication methods when scheduling a meeting.

**Meeting Authentication Options:**

Sign in to Zoom (Default) [Edit](#) [Hide in the Selection](#)

If they are not logged into Zoom, this is what they see:



If they are logged in with the wrong email domain, this is what they see:

