SEARCH HIGH-TECH CRIME TRAINING SERVICES

April 2020

Zoom Configuration Resource Guide

By Lauren Wagner
High-Tech Crime Training Specialist
SEARCH

Configuring a Zoom account will depend on the needs of the organization and user. Users with business accounts may have their settings set by their Zoom administrator and these may not be configurable at the user level. The settings below are a suggestion of best practices for a higher level of security. While some of the following settings are the default, it's always important to check that they are set appropriately for the sake of good security.

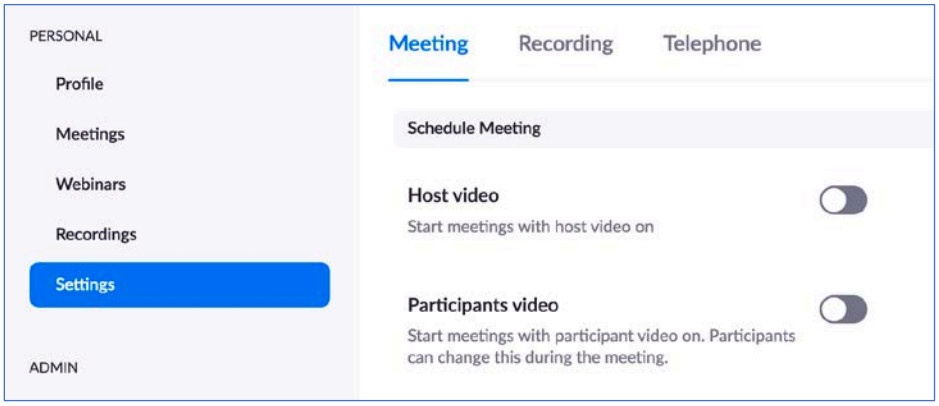
Settings to Configure via Browser

Open a web browser and navigate to https://zoom.us/. Click **MY ACCOUNT** in the upper right-hand corner.

Navigate to **Settings** on the right-hand side and start in the **Meeting** area.

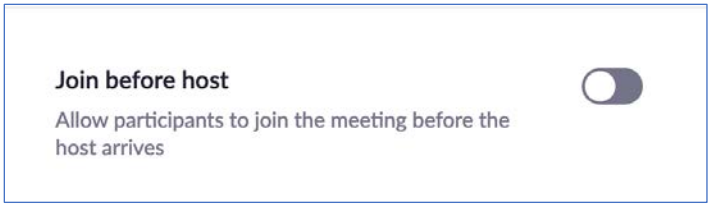
- Turn off **Host video** and **Participants video**

  This will ensure that video will not broadcast prior to the presenter being ready and prepared to proceed with the meeting.



- Turn off **Join before host**

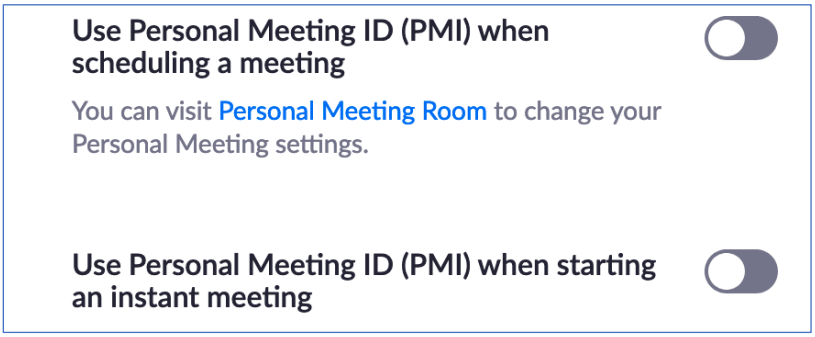
  *It is critical to turn off this setting, especially when using a waiting room. There is an unknown security flaw found by Citizen Lab,[1] a research group within the University of Toronto, which reported a waiting room vulnerability to Zoom. Turning off **Join before host** will add additional security to your Zoom waiting room.*



- Turn off **Use Personal Meeting ID (PMI) when scheduling a meeting** and
  Turn off **Use Personal Meeting ID (PMI) when starting an instant meeting**

  The personal meeting ID (PMI) is a permanently assigned personal meeting room that a Zoom user can start any time or schedule for future single or reoccurring use. The Zoom user's PMI is part of a personal meeting URL; for example, a Zoom user with the PMI of **2010284593** will use **https://zoom.us/j/2010284593** to open a personal meeting room. However, a PMI is open to exploit because once a third party knows the Zoom user's PMI, they can try repeatedly to open the user's personal meeting room; and if the room is in use, they can potentially gain unauthorized entry.

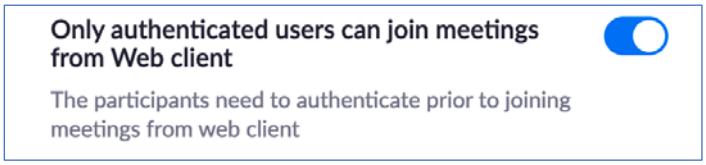
  Using an automatically generated meeting ID will prevent a PMI from potential exploitation. By turning off the PMI when scheduling a meeting or starting an instant meeting, Zoom will automatically assign a one-time-use meeting ID.



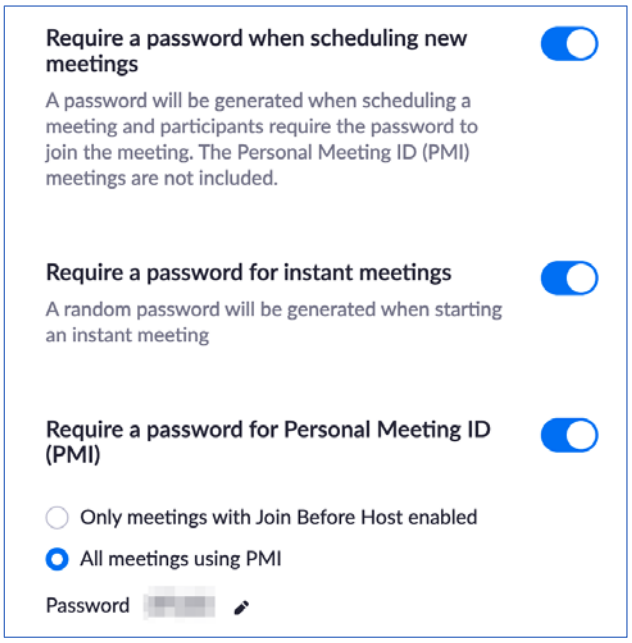
[1] https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/

- Turn on **Only authenticated users can join meetings from the Web client**

  The Zoom web client allows users to join a meeting without signing in. This setting prevents access by guests unless they are authenticated.



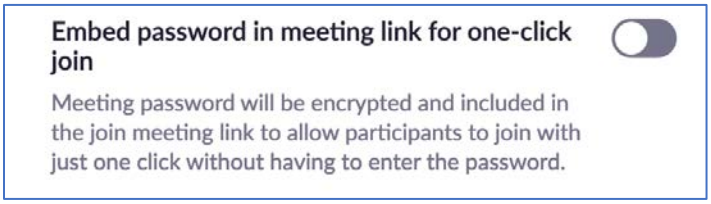
- Turn on these settings: **Require a password when scheduling new meetings**, **Require a password for instant meetings** and **Require a password for Personal Meeting ID**



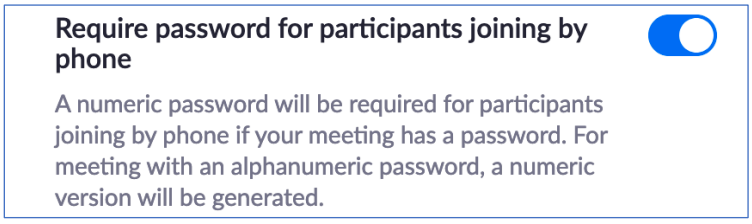
- Decide on a setting for **Embed password in meeting link for one-click join**

  If the password is embedded, the meeting password is included in the Join Meeting link. This allows participants to join the meeting with one click and not have to type the password. While this makes it easier for users to join (and Zoom claims the password is encrypted when the invitation is sent, so it should be secure), Zoom encryption has come under fire for potentially being unsecure.

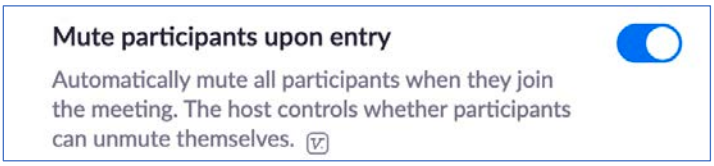
  Users who want a higher level of security should turn this setting off. Participants will have to type the meeting password instead of being able to join using one click.



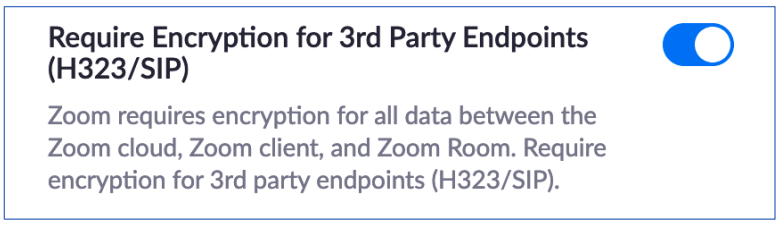
- Turn on **Require password for participants joining by phone**



- Turn on **Mute participants upon entry**

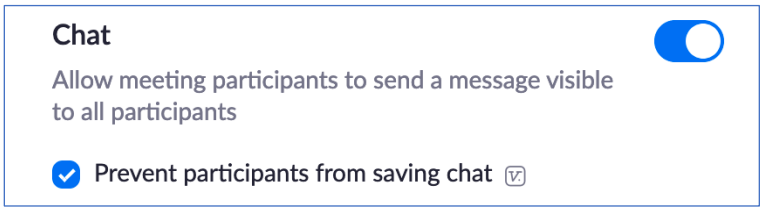


- Turn on **Require Encryption for 3rd Party Endpoints**

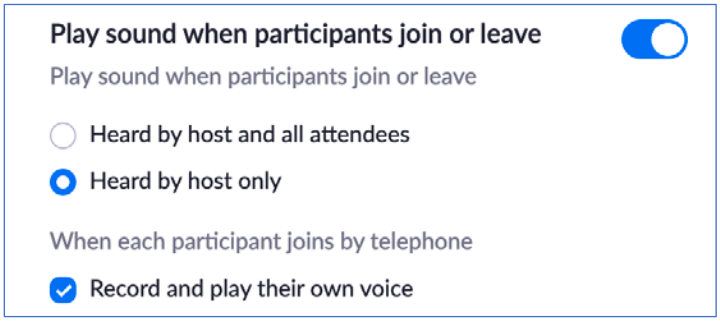


- For increased security, check **Prevent participants from saving chat**

  It's important to remember than any features that are disabled with saving text or video can always be bypassed with third-party screenshotting and screen recording software. Zoom settings just prevent the data from being easily accessible.



- Turn on **Play sound when participants join or leave** and select **Heard by host only**. Also, under "When each participant joins by telephone," select **Record and play their own voice**. *These options will alert the host when people join and leave the meeting.*

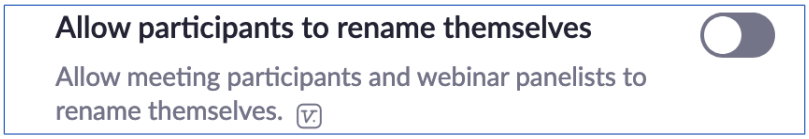


- Decide on a setting for **Remote control**

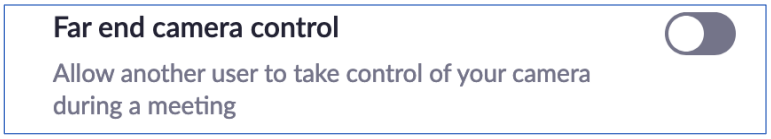
  This can be a powerful collaboration tool for team meeting sessions, but it can also be a security vulnerability when others can control shared content by the host.

- Uncheck **Allow participants to rename themselves**

  *This setting prevents phishing attacks by people purporting to be someone they are not. While there are instances where you might want people to change their name once a meeting has begun, it is a good security measure to have it turned off by default. Once an individual meeting has begun, you can change this setting using the **Participants** tab.*

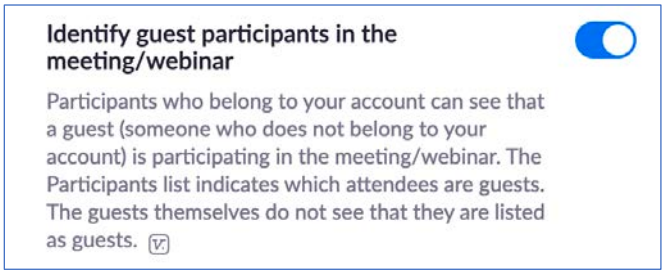


- Uncheck **Far end camera control**



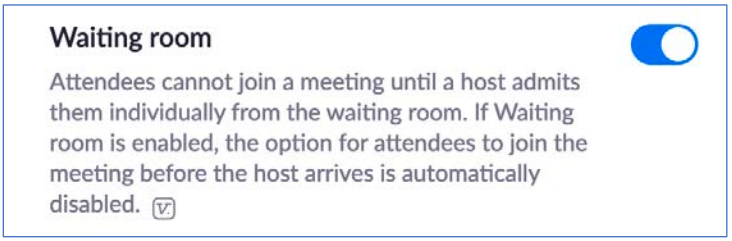
- Turn on **Identify guest participants in the meeting/ webinar**

  This setting creates awareness of who is currently in a meeting that may contain sensitive data. Participants who belong to your account can see that a guest (someone who does not belong to your account) is participating in the meeting/webinar. The Participants list indicates which attendees are guests.



- Turn on **Waiting room**

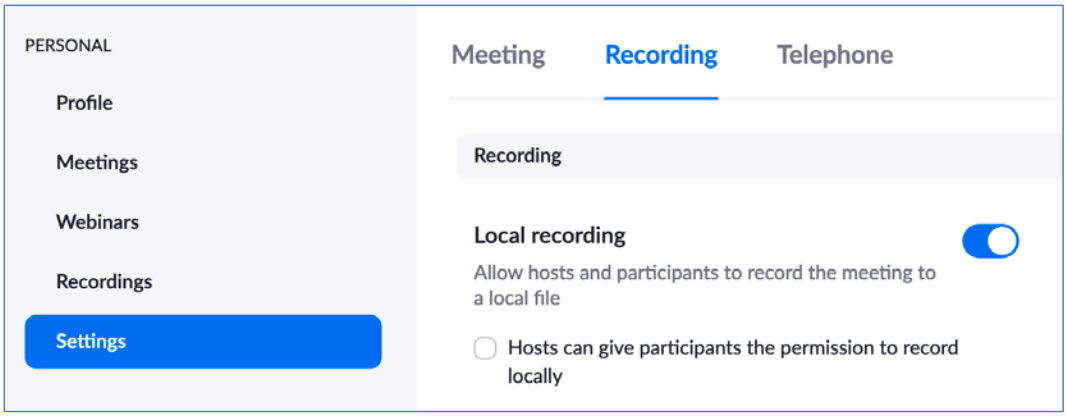
  A waiting room allows a host to control when a participant joins a meeting. It is one of the strongest security features provided by Zoom. If a waiting room is enabled, potential participants will see a message to "please wait until the meeting host lets you in."



Navigate to the **Recording** area under **Settings**

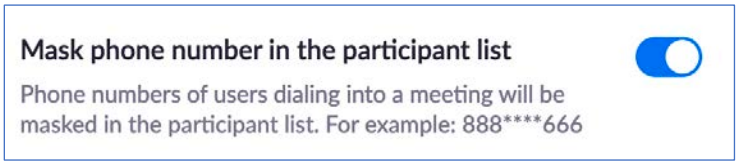
- Uncheck **Hosts can give participants the permission to record locally**

  A more secure option is for the host to create the recording and make that recording available to participants using a different method after the meeting has concluded.



Navigate to the **Telephone** area under **Settings**

- Turn on **Mask phone number in the participant list**



Following these settings will ensure that the default security of a Zoom meeting setup is as high as possible. When you create a Zoom meeting, you can check these settings as well.

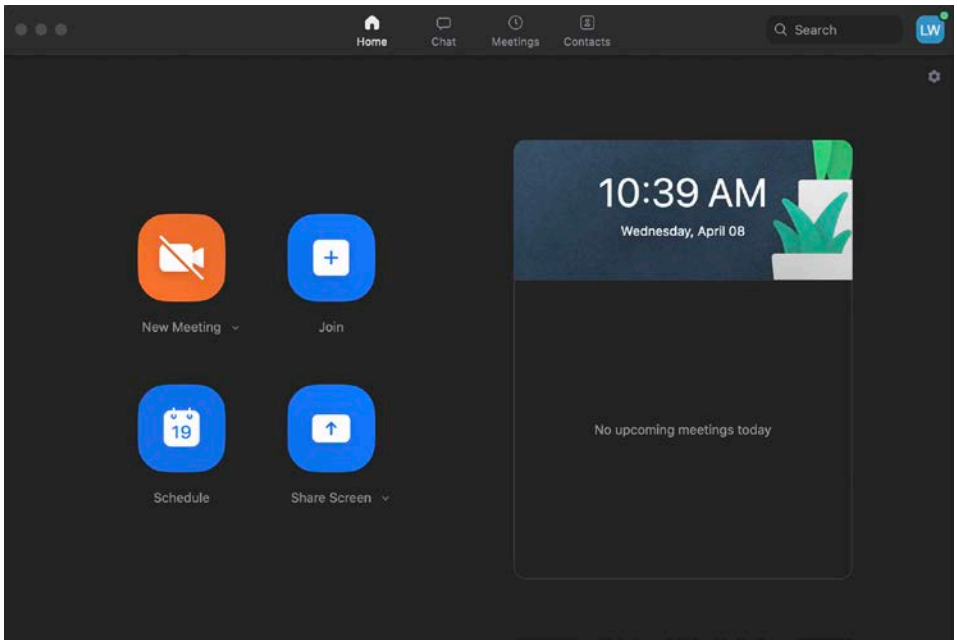
Optional Settings to Consider

In addition to the settings described above, Zoom offers some additional settings that can be set globally depending on the types of meetings an organization is hosting. For example, if using Zoom to deliver training or information to large public groups, it might be a good idea to turn off chat, private chat, screen share by participants, annotation, and whiteboard. While these are all powerful tools for collaboration, they can also be misused if your Zoom meetings are beyond a closed group of trusted individuals.

Settings to Configure via the Zoom App

If you configure Zoom profiles via a browser and use the above settings, most of these settings using the Zoom app will just be double checking.

From the main screen, click **Schedule** to access full configuration settings



For the highest level of security use the following guidelines:

- Set the meeting topic and date/time

  Scheduled meetings can be scheduled on the hour or half-hours only.

- Select **Generate a Meeting ID Automatically**

- Check **Require meeting password** and use a strong password

  A strong password should not be easily guessed, not have repeating or sequential patterns (1111 or qwerty), and be a complex password with both uppercase and lowercase letters, special characters, and numbers. When this box is checked, a numerical only password will also be generated for people joining by phone.

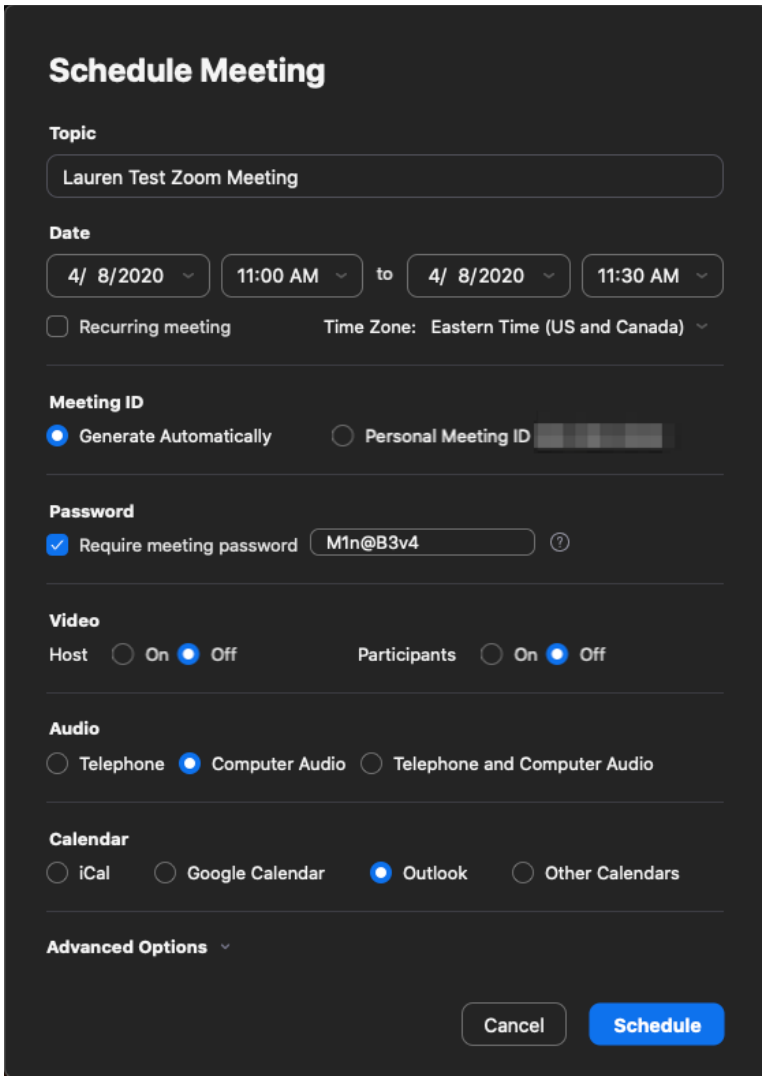
- Set **Video** to **Off** for both Host and Participants

  Video can be turned on after the meeting is started.

- Set **Audio** for the meeting requirements

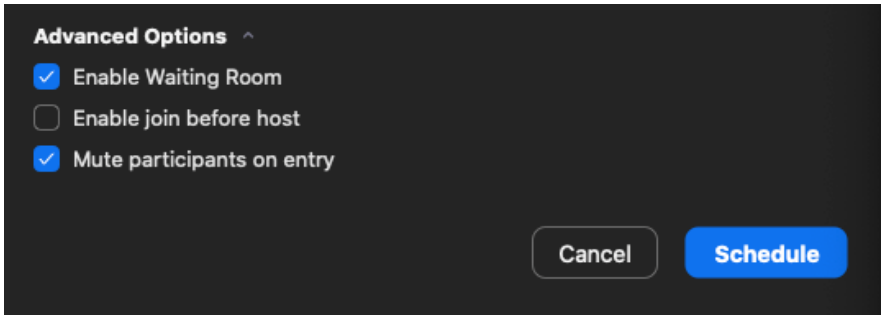
  *If both telephone and computer audio are needed, select both. But if attendees will only be using computer audio, configure the setting to **Computer Audio** only. Same with **Telephone** only.*

- Pick a calendar format

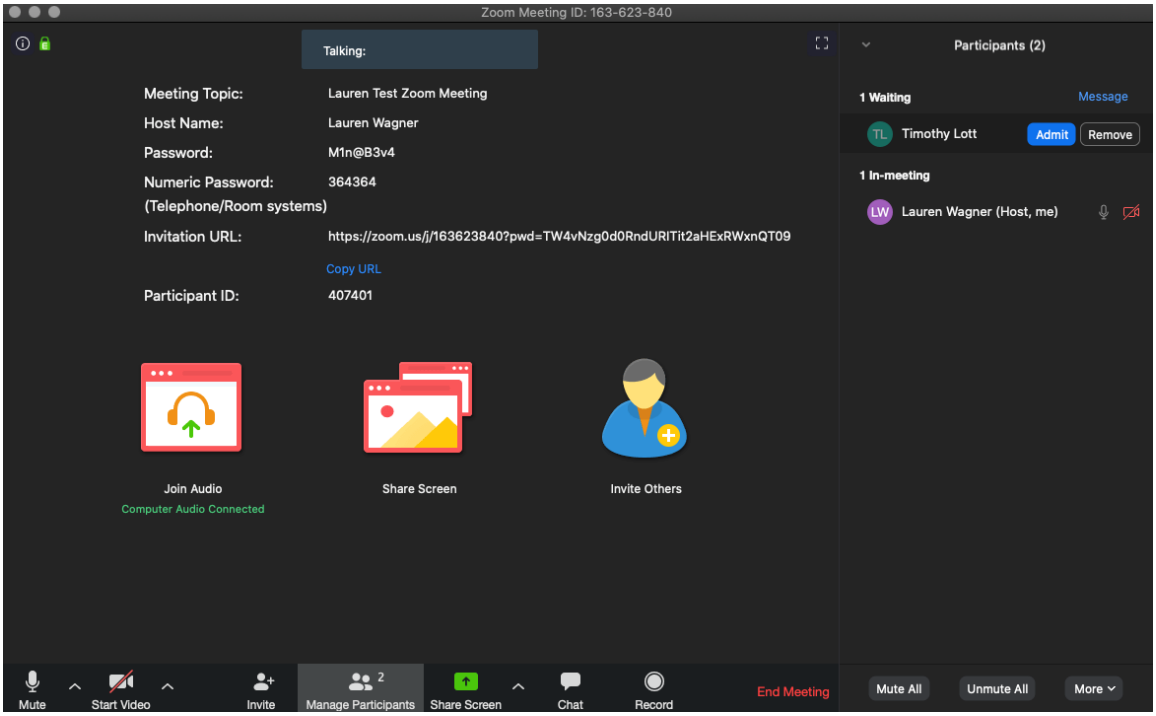


Open **Advanced Options** under the calendar format:

- Check **Enable Waiting Room**
- Uncheck **Enable join before host**
- Check **Mute participants on entry**
- Click **Schedule**



Once the meeting is started, the host will need to approve the participants using the Participants tab. Click **Manage Participants** to open the Participants tab.



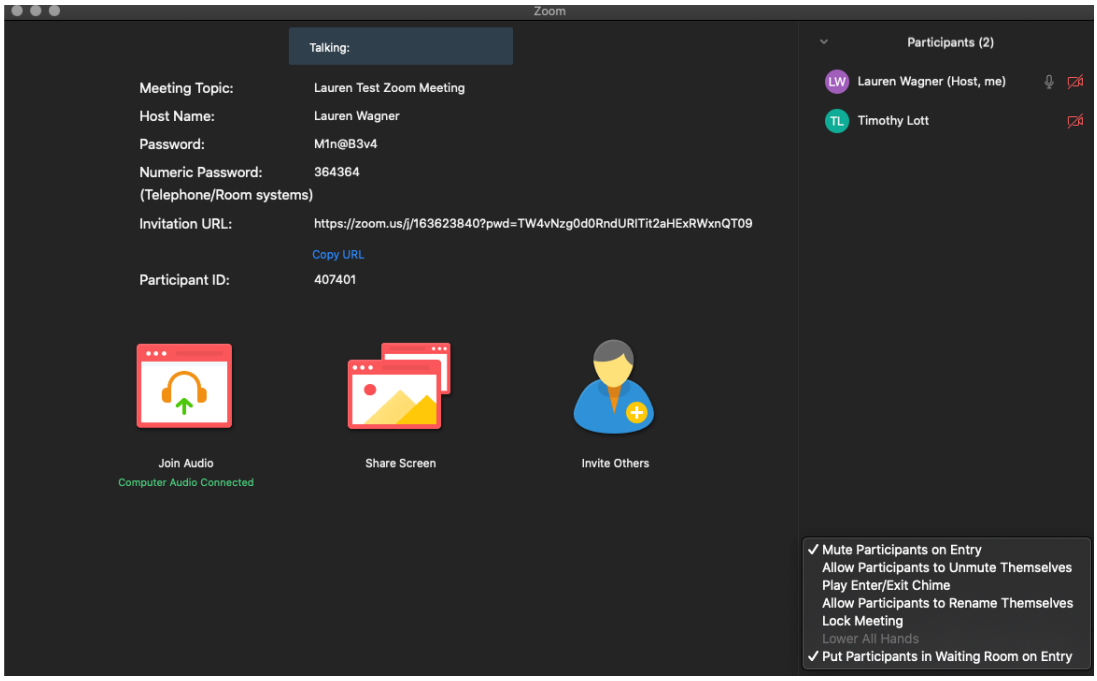
In the **Participants** area, click **Admit** or **Remove** for each attendee.

Once a meeting has begun, use the **Participants** area to make some additional security changes:

- Click **More**
- Decide on a setting for **Allow Participants to Unmute Themselves**. If using Zoom for anything other than team collaboration, uncheck **Allow Participants to Unmute Themselves**

  Preventing participants from unmuting themselves requires a host or co-host to be more diligent with unmuting people who might need to speak, but it gives more security and control to the meeting host. This will prevent users from screaming into their microphone or yelling profanity to hijack the meeting.
- Uncheck **Allow Participants to Rename Themselves**
- Once all participants have arrived, check **Lock Meeting**

  *This will prevent anyone additional from trying to enter the meeting once the meeting has begun. If an additional participant needs to enter, the meeting can be unlocked on the fly by clicking **Unlock Meeting** in the **Participants** area at any time.*



Assign a co-host (if possible). Co-hosts may not be available if using a free Zoom account. With a business account, a co-host may be assigned to anyone else within the same organization. Co-hosts cannot be assigned if they are not under the same business account. Co-hosts are a good security feature in case there is a breach of the original host. With only a single host, if that role gets compromised, there is no way to regain control for the rest of the attendees. If there is a co-host, they can take control back from the compromised host.

- Hover over the name of the participant and click **More** and then **Make co-host**

In addition to the Zoom configuration best practices outlined in this guide, SEARCH has created a *Best Practices* brief, "Best Practices for Securing a Zoom Meeting," which is available for request from the SEARCH website at https://www.search.org/resources/e-crime-investigative-tools/.