UNIVERSITY OF MARYLAND
SCHOOL OF PUBLIC POLICY

Best Practices for Securing your Zoom Meetings

Covered in this guide:

- A checklist for securing your meetings
  - Setting up your meeting
  - Managing your meeting
- Advanced – Options to secure public meetings

Checklist for securing your meetings

Setting up your meeting

- ❑ Do not use your Personal Meeting ID – always Generate Meeting ID's automatically
- ❑ Require a password to join your meetings
- ❑ Allow only authenticated users to join your meetings
- ❑ Prevent removed participants from rejoining the meeting
- ❑ Allow only hosts to share their screen
- ❑ Disable the Chat function to prevent meeting participants sending messages that can be seen by all
- ❑ Disable the File Transfer function
- ❑ Enable your Waiting Room
- ❑ Add a co-host to help you manage your meeting

Managing your meeting

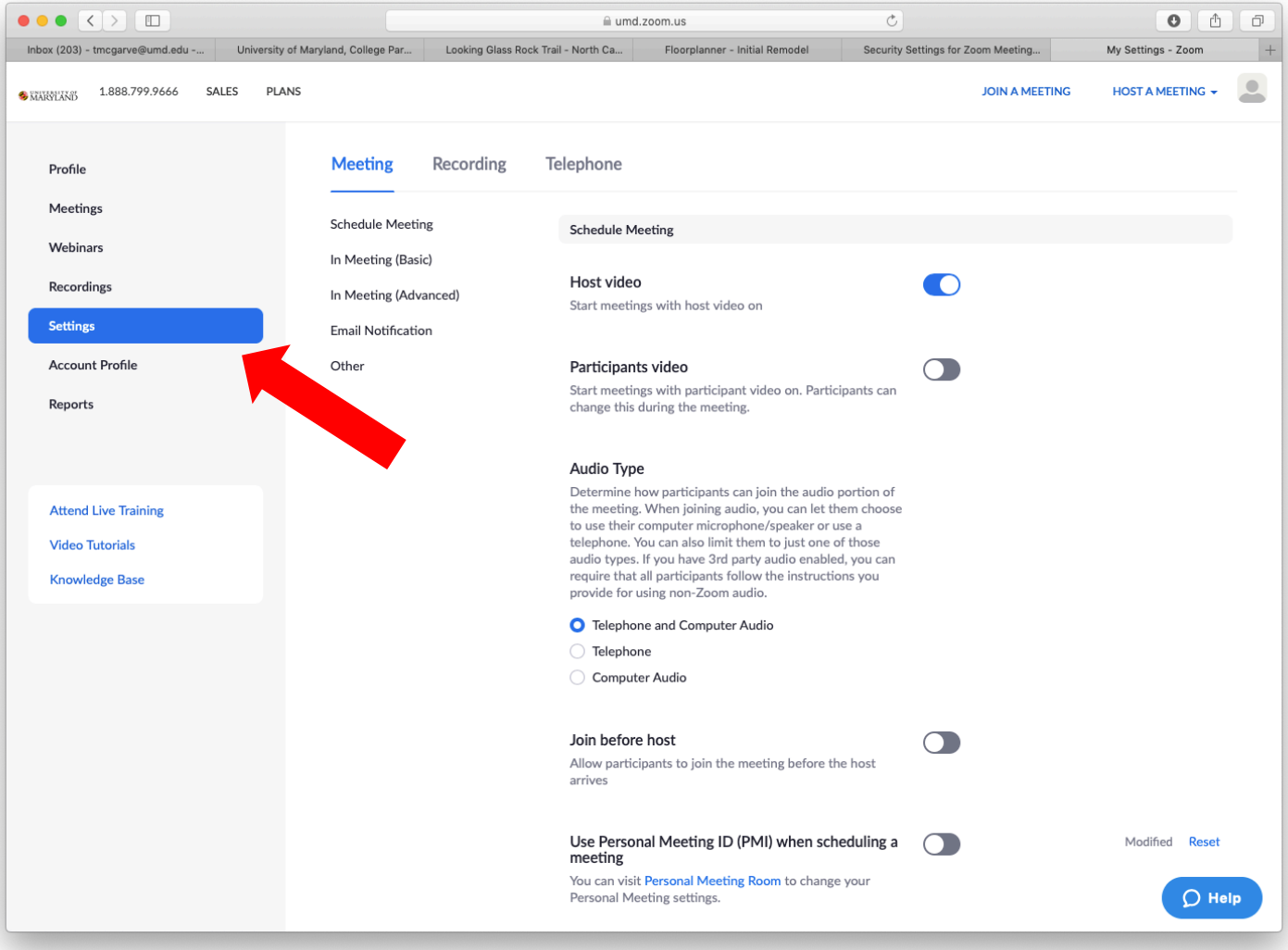
- ❑ Removing participants from your meeting
- ❑ Admitting participants from the waiting room
- ❑ Prevent meeting participants from unmuting themselves
- ❑ Prevent meeting participants from renaming themselves

UNIVERSITY OF MARYLAND
SCHOOL OF PUBLIC POLICY

Best Practices for Securing your Zoom Meetings

Setting up your meeting

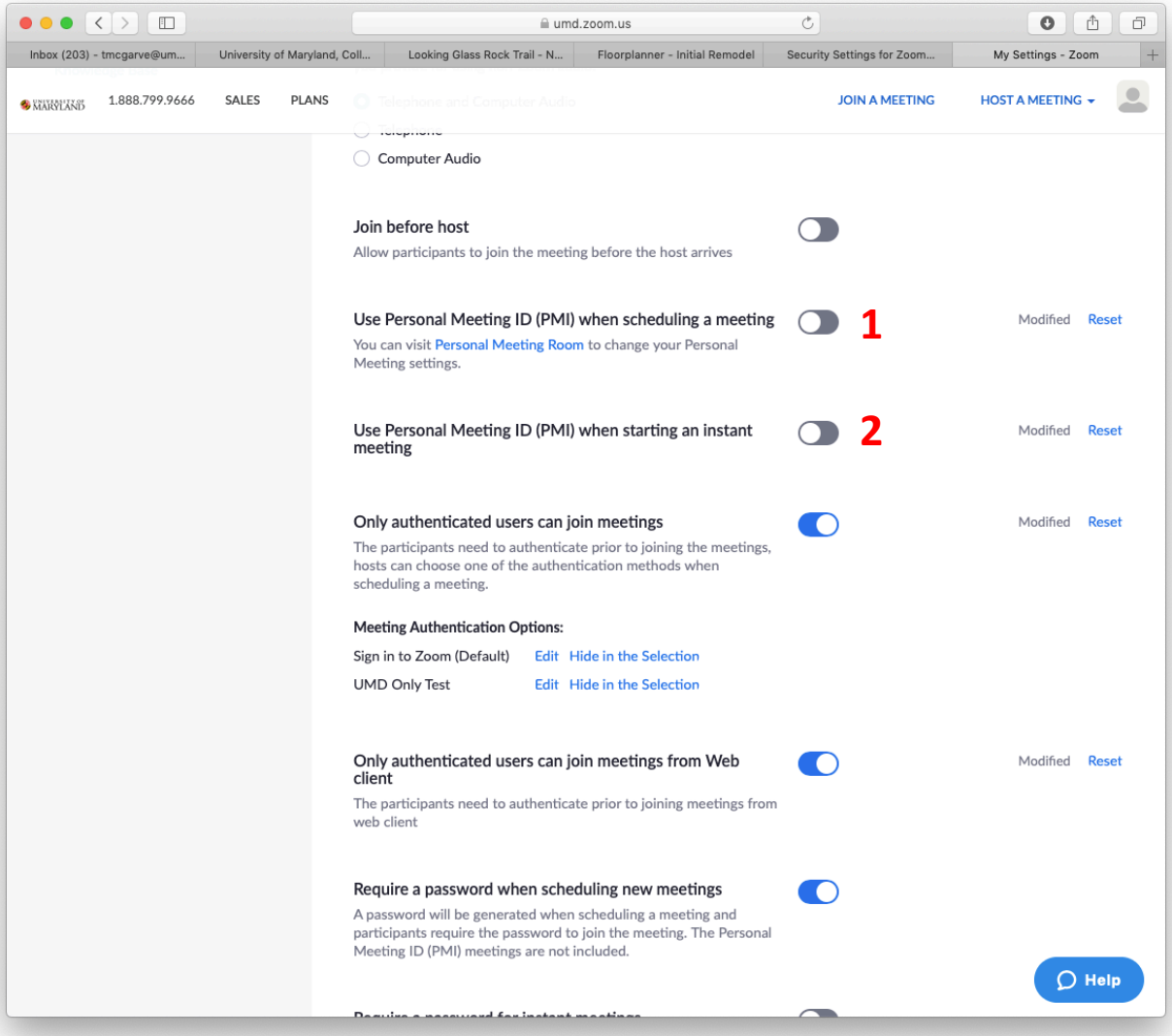
Accessing your Zoom Settings



- All the following settings can be changed within the Settings section of your Zoom profile
- Open umd.zoom.us in your web browser
- Select “Sign In” and log in with your Directory ID, password, and Duo authentication
- From the left-hand menu, select “Settings”

NOTE: Once you change these settings, they will become the default settings for any meetings you schedule – i.e. you will not need to specify these settings each time you scheduled a meeting

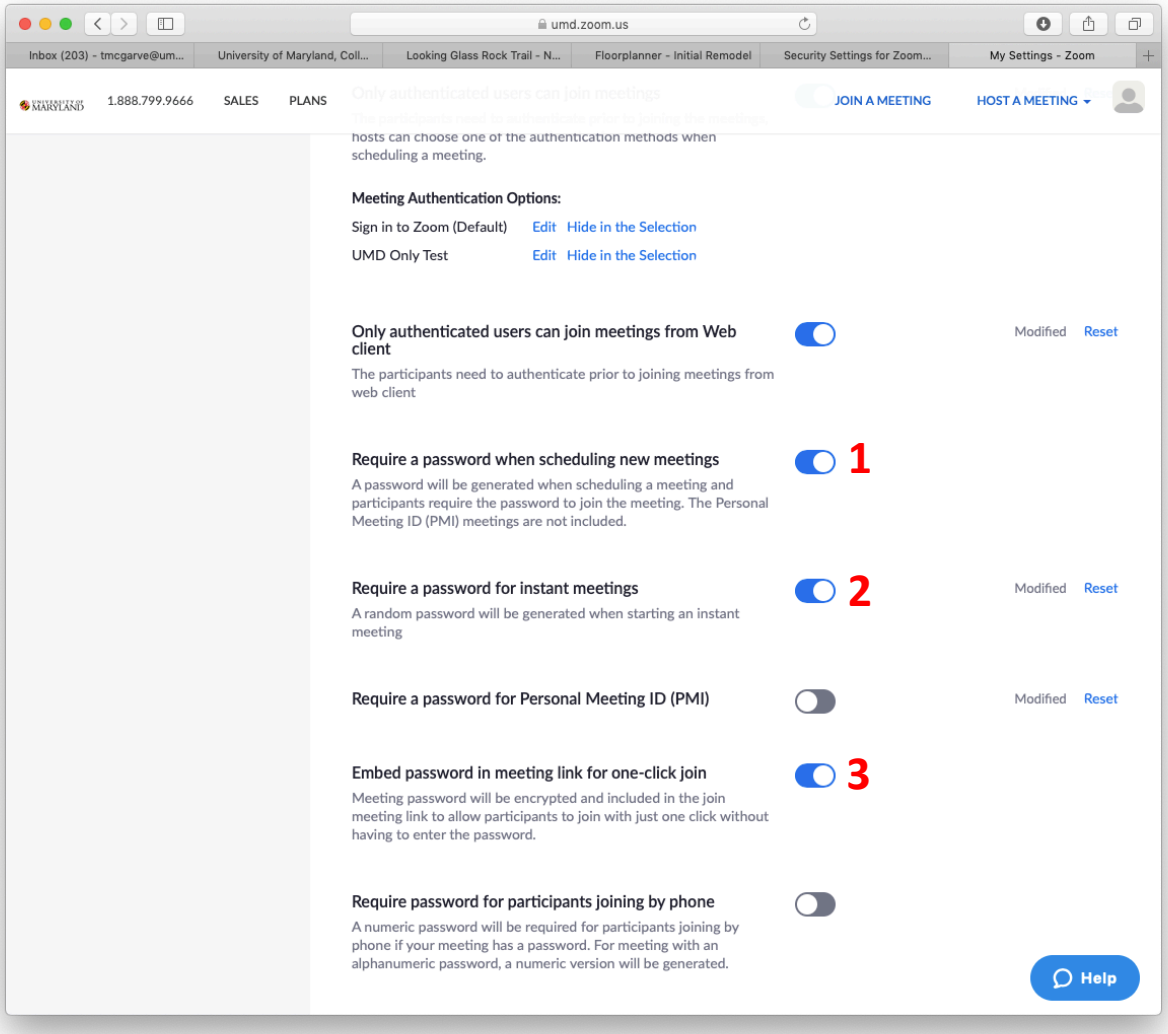
Generate Meeting IDs Automatically



- When scheduling a meeting, the meeting number can either be your Personal Meeting ID or a randomly generated ID
- Your Personal Meeting ID never changes, and as such, once someone has it, they can continue connecting to it as they please
- If you have no other security settings enable (e.g. passwords), they will be able to join any meeting you are hosting
- Hence, **always use randomly generated IDs** for your meetings, and **never use your Personal Meeting ID**

1. Disable “Use Personal Meeting ID (PMI) when scheduling a meeting”
2. Disable “Use Personal Meeting ID (PMI) when starting an instant meeting”

Require a password to join your meetings



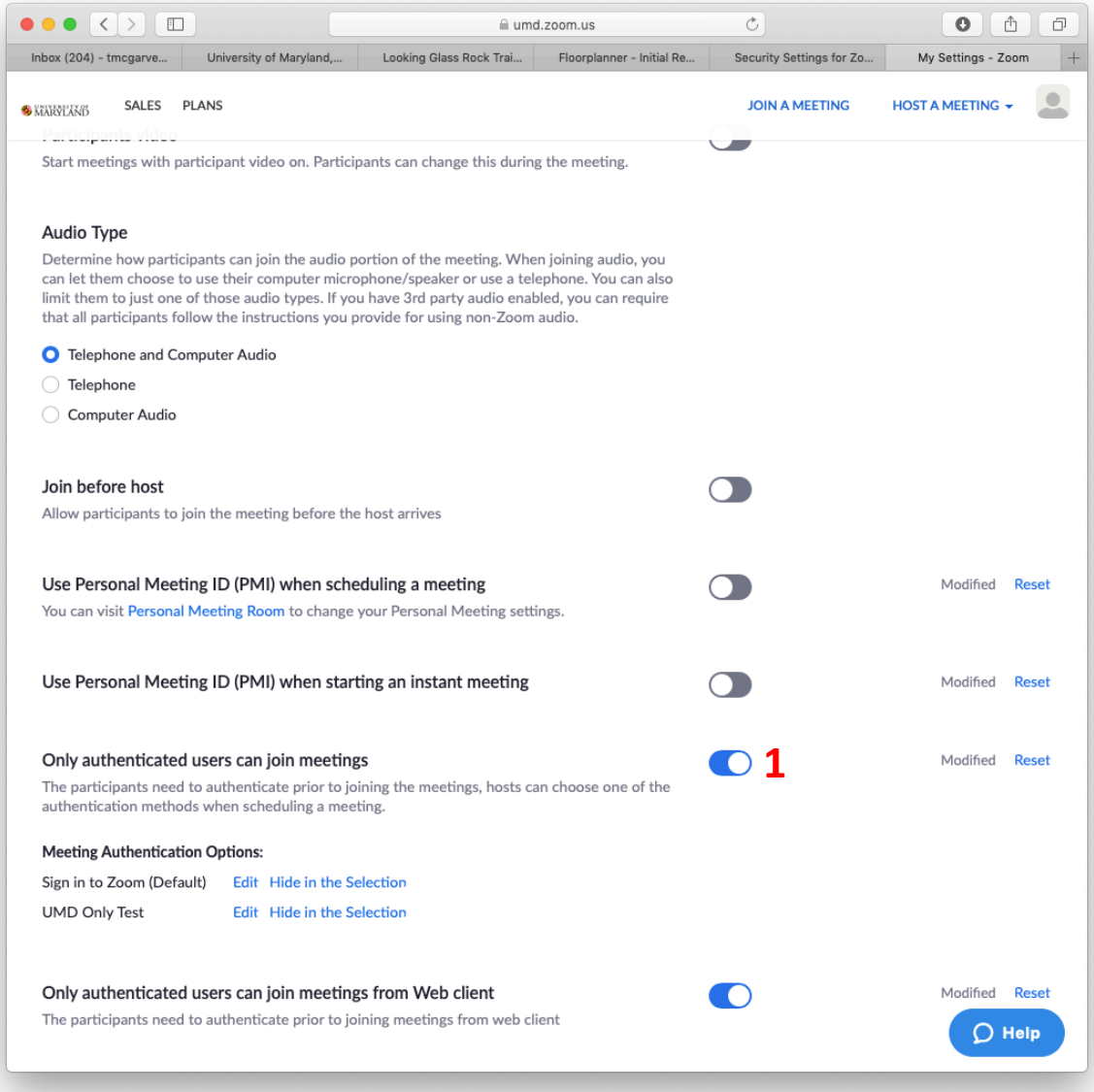
- By requiring a password to join meetings, your meeting participants will need both the Meeting ID and a password to connect

1. Enable “Require a password when scheduling new meetings”
2. Enable “Require a password for instant meetings”

- For ease-of-use for your meeting participants, you can embed the password in the Zoom link – this will allow participants to click the link and have the password automatically entered

3. Enable “Embed password in meeting link for one-click join”

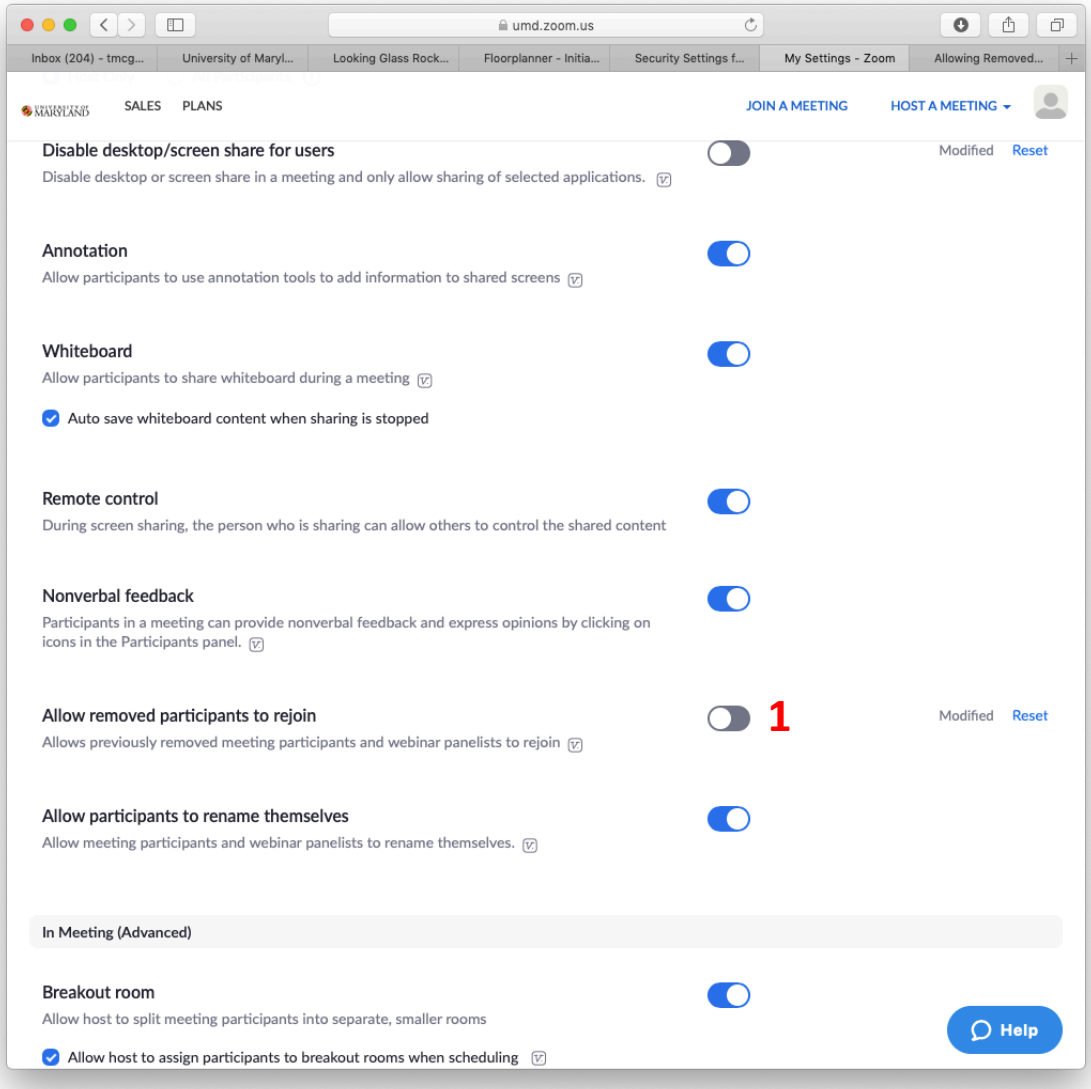
Allow only authenticated users to join your meetings



- Authenticated users are those with a UMD directory ID, which includes all faculty, staff and students
- Enabling this setting will keep out any non-UMD people
  - **NOTE:** If you have attendees that are outside of the University, this setting will need to be disabled to allow them access to the meeting

1. Enable “Only authenticated users can join meetings”

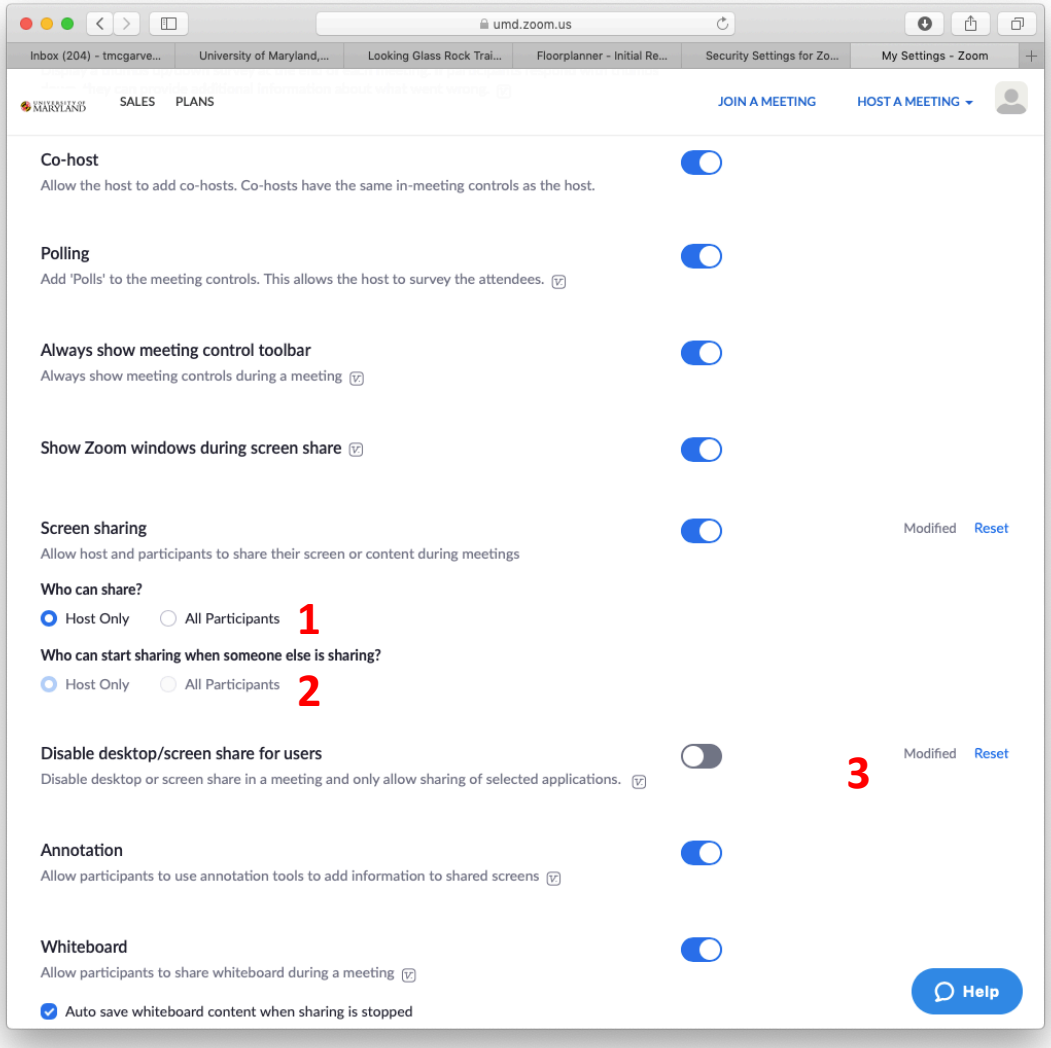
Prevent removed participants from rejoining



- As a host during a meeting, you can remove a participant from the meeting at any time
- By default, that participant can rejoin the meeting
- Disabling this feature will mean that once you have removed a participant from a meeting, they are not able to rejoin

1. Disable “Allow removed participants to rejoin"

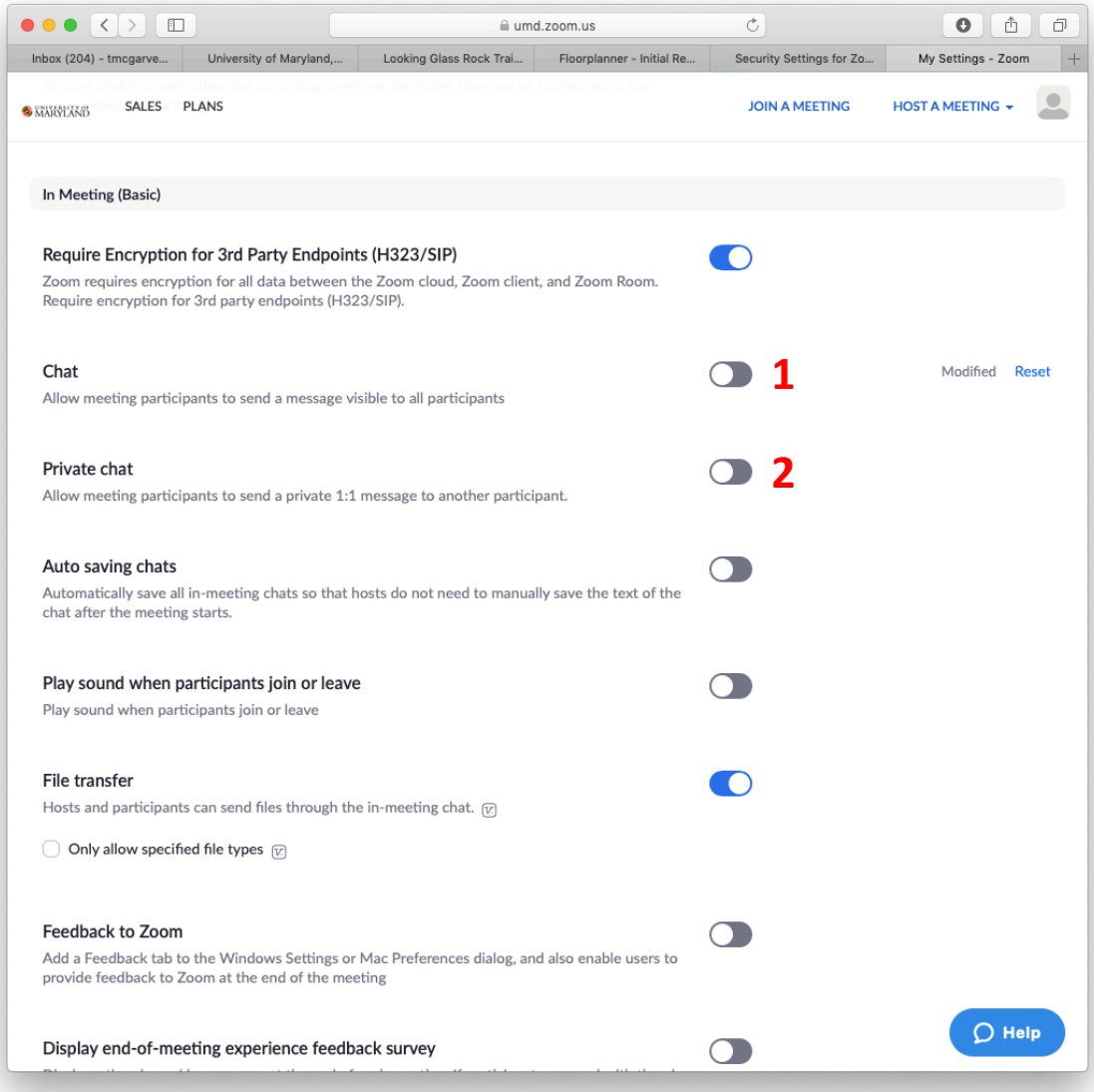
Allow only hosts to share their screen



- To prevent meeting participants from using the screen share feature to introduce unwanted visual content in your meetings, restrict the ability to share the screen to hosts only
- Scroll down to the “In Meeting (Basic)” settings section

1. Under “Screen Sharing” and “Who can share?”, select “Host Only”
2. Under “Who can start sharing when someone else is sharing?”, select “Host Only”

Disable the Chat function

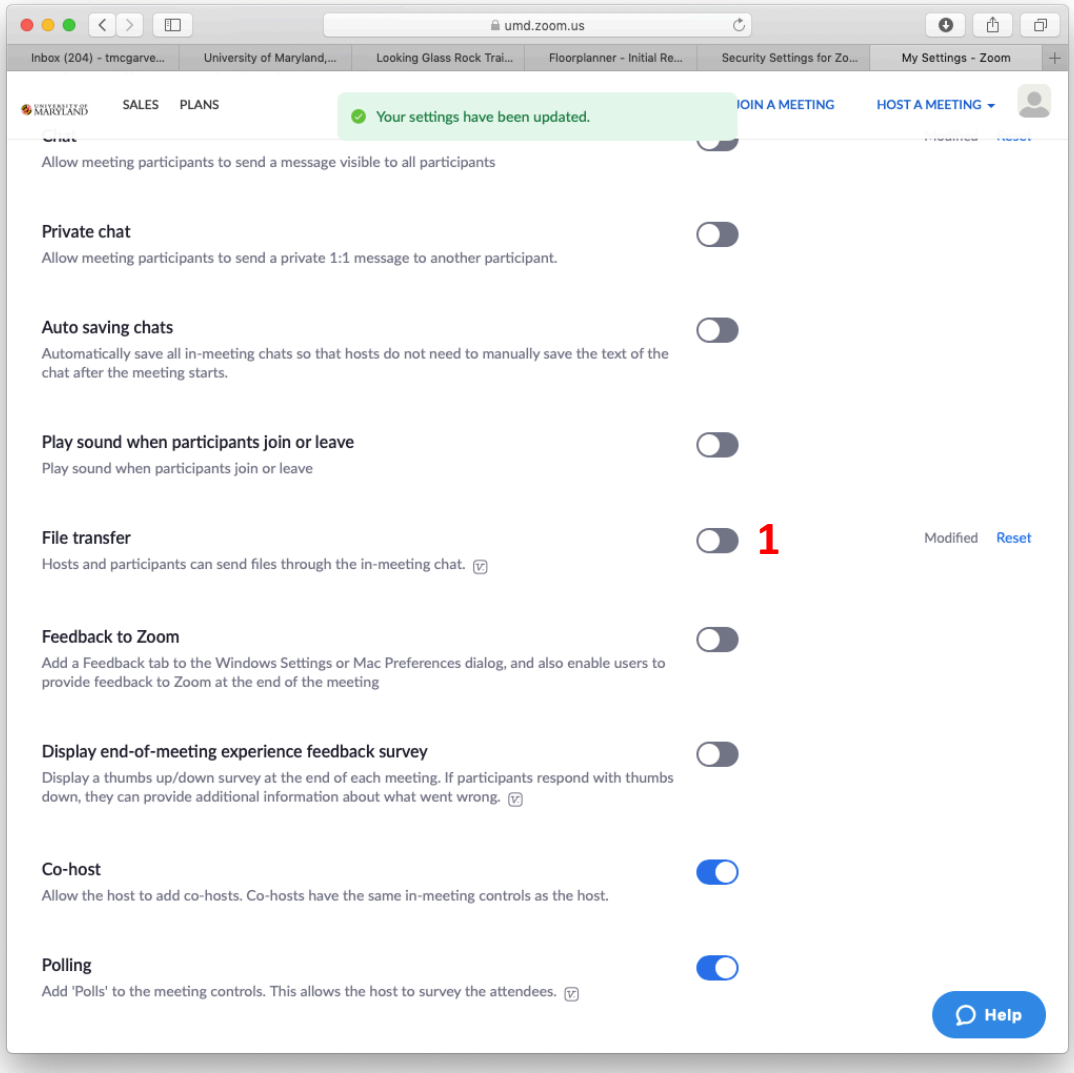


- Under default settings, the chat function will allow meeting participants to send messages that can be seen by all
- Scroll down to the “In Meeting (Basic)” settings section

1. To eliminate the ability for participants to use the chat function to send obscene messages, disable ”Chat”
2. Disabling “Chat” will also automatically disable the ability for meeting participants to privately chat with each other, eliminating the possibility that bad actors target meeting participants in a manner that can’t be seen by the meeting host

- **NOTE:** Meeting participants will still be able to message the meeting host (i.e. they can still communicate questions/concerns to you as the instructor)

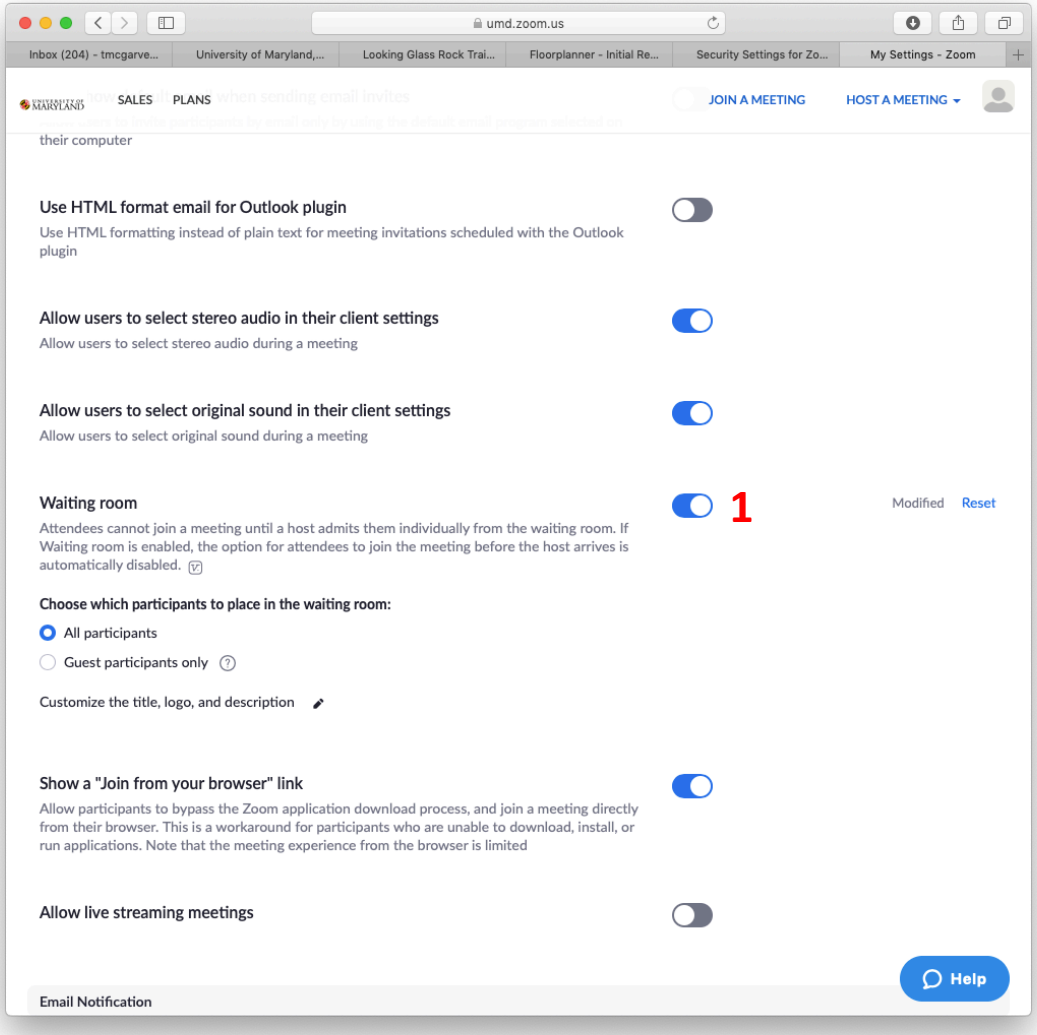
Disable the File Transfer function



- Under default settings, meeting participants can send any file to all meeting participants via the Chat function
- Scroll down to the “In Meeting (Basic)” settings section

1. To eliminate the ability for participants to send unauthorized files, disable “File transfer”

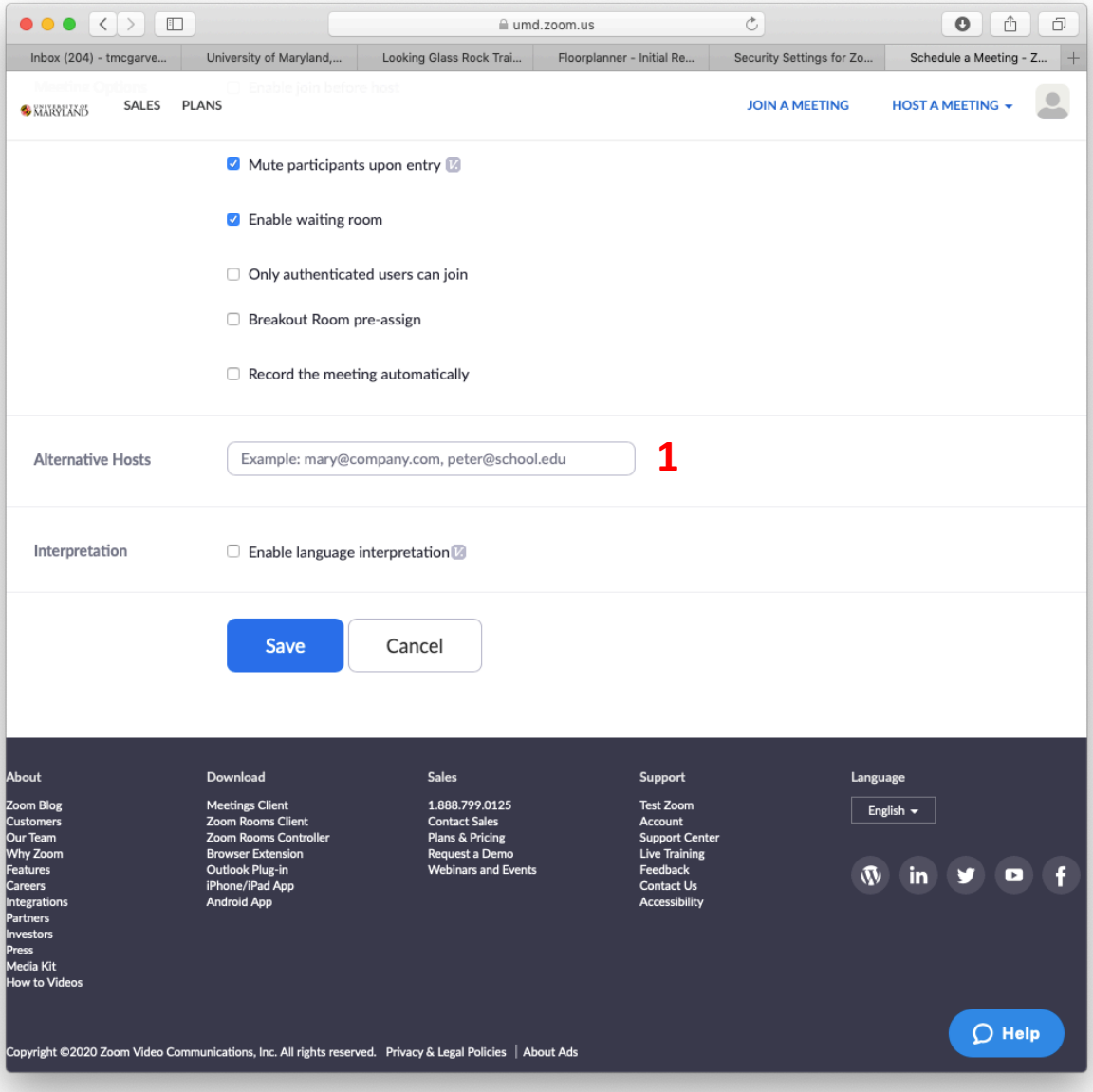
Enable your Waiting Room



- When Waiting Room is enabled, upon connecting to a meeting, participants are placed into a virtual waiting room where they cannot interact with any other participants (versus automatically joining the meeting and being able to interact with others)
- As the host, you must “Admit” the participant to the meeting, giving you the ability to pick and choose who is allowed into the meeting

1. To do so, scroll down to the “In Meeting (Advanced) section and enable “Waiting Room”
    - You can further specify whether all participants are placed in the waiting room, or just guests (those non-UMD users)

Add a co-host to help you manage the meeting



- A co-host is granted many of the same functions as you, the host, allowing them to assist you in managing the meeting
- For example, they can admit or remove participants, mute participants, and message participants

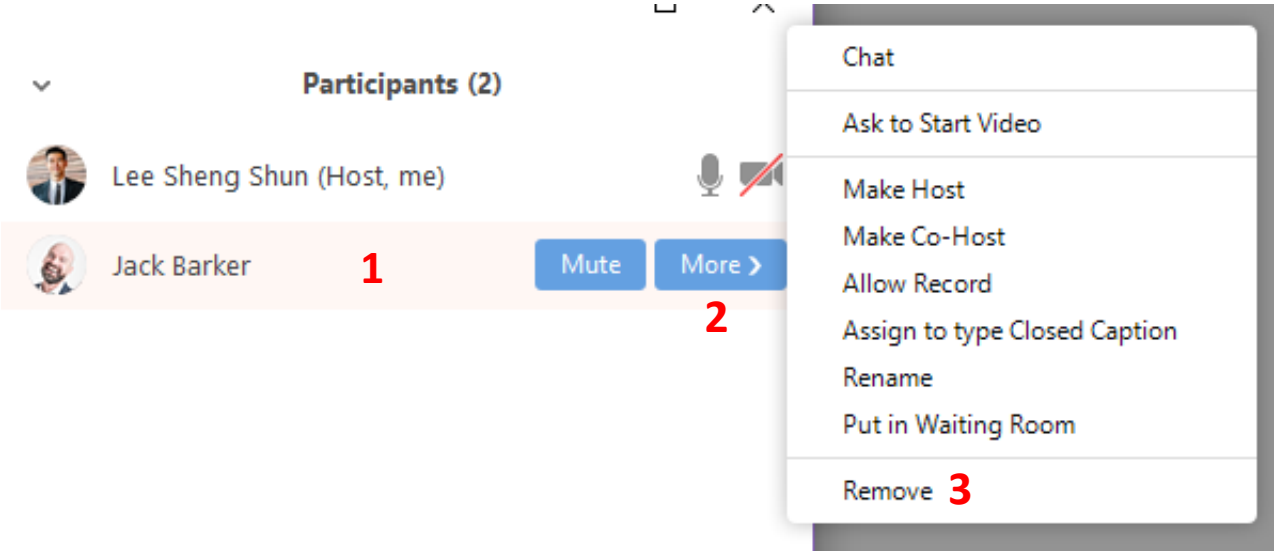
1. Co-hosts are added when scheduling individual meetings – you can enter their email address at the bottom of settings window for each meeting you schedule

UNIVERSITY OF MARYLAND
SCHOOL OF PUBLIC POLICY

Best Practices for Securing your Zoom Meetings

Managing your meeting

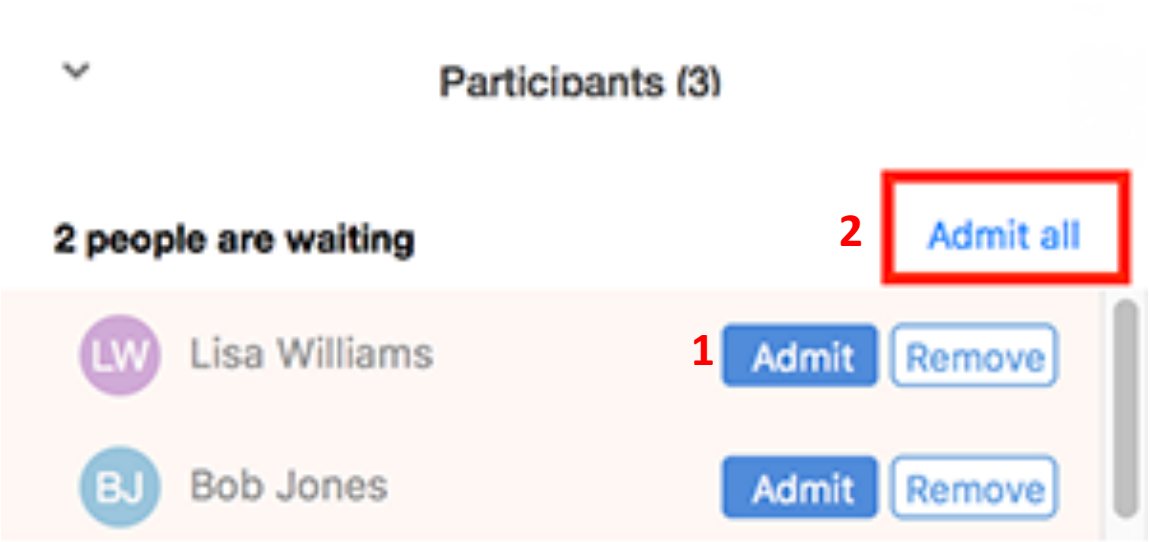
Removing participants from your meeting



- As the host of the meeting, you can remove a participant at any time
- If you have disabled the “Allow removed participants to rejoin” setting, once you remove a participant, they will not be able to get back into your meeting

1. From the meeting window, select “Manage Participants” to show all participants
2. Hover over the participant you wish to remove, and click “More”
3. Click “Remove” to remove the participant from your meeting

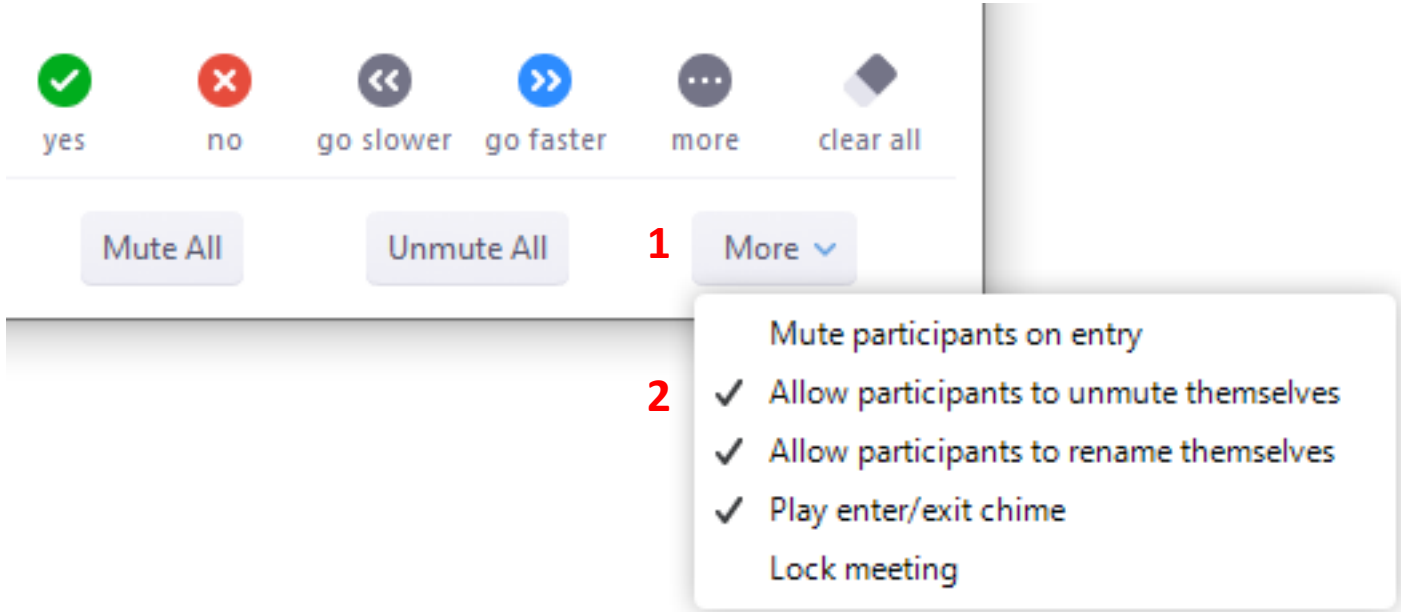
Admitting participants from the waiting room



- If you have enabled the Waiting Room in your meeting settings, all participants connecting to your meeting will first be placed into this room
- To admit them into the meeting, from the meeting window select “Manage Participants” to show the participants panel
- Any participant in the Waiting Room will be displayed at the top of the “Manage Participants” panel

1. Click “Admit” to move the participant into the meeting
2. If you would like to admit everyone in the Waiting Room, click “Admit all”

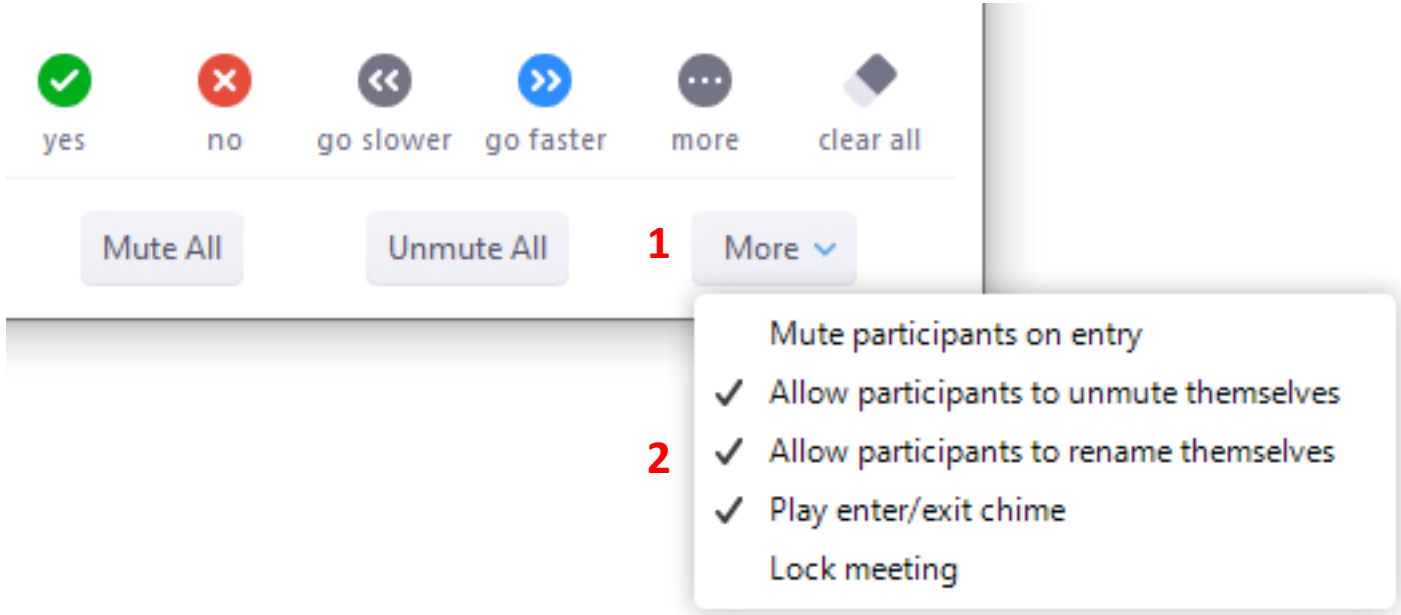
Prevent participants from unmuting themselves



- If you would like the host to be the only person that can unmute a participant to speak, you can disable the ability for participants to unmute themselves
- To disable this ability, from the meeting window select “Manage Participants” to show the participants panel

1. At the bottom of the “Manage Participants” panel, select “More”
2. Uncheck the option that says “Allow participants to unmute themselves”

Prevent participants from renaming themselves



- If you would like to avoid situations where bad actors use their display name to communicate obscene material, you can disable their ability to change their name from what is specified in their account
- To disable this ability, from the meeting window select “Manage Participants” to show the participants panel

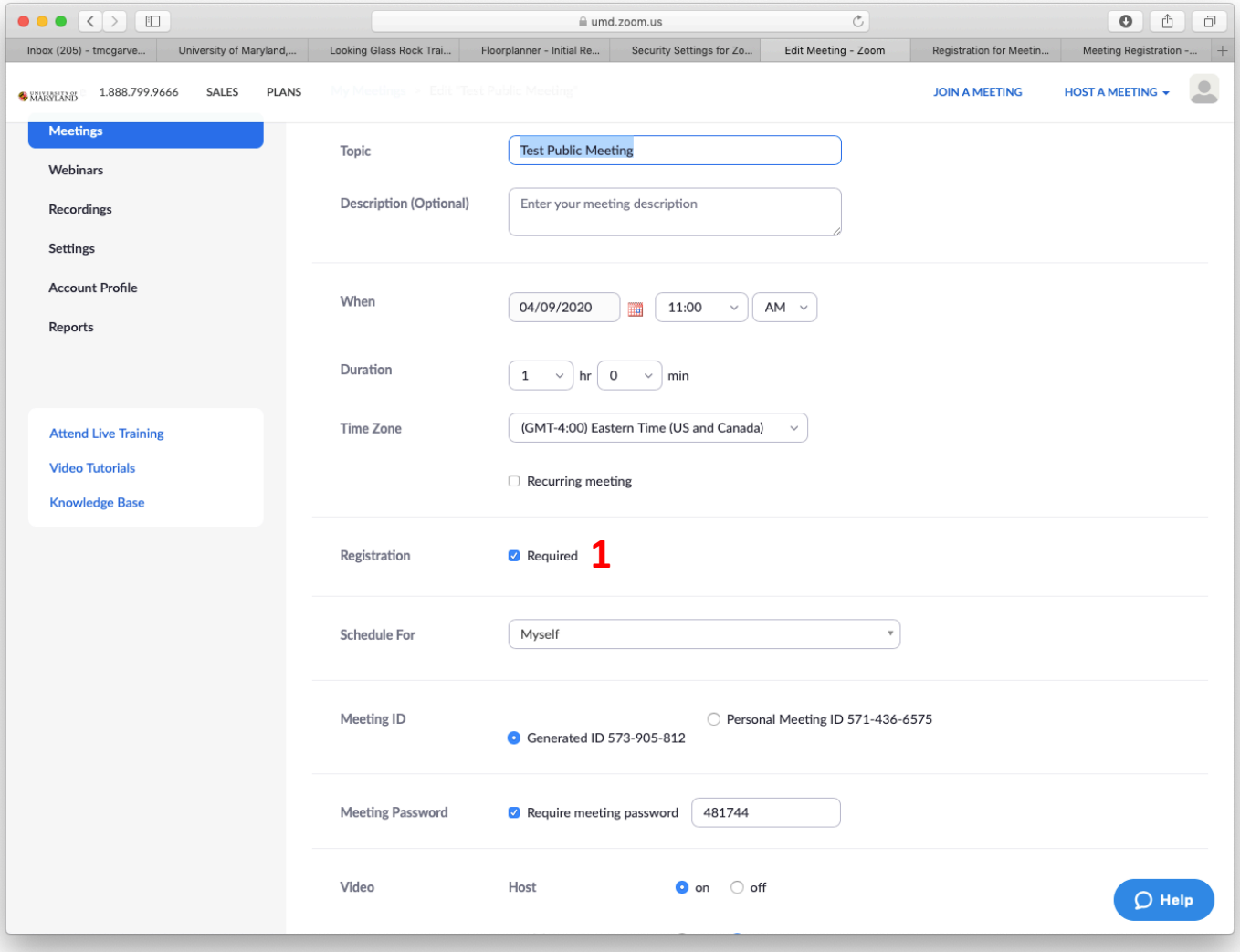
1. At the bottom of the “Manage Participants” panel, select “More”
2. Uncheck the option that says “Allow participants to rename themselves”

UNIVERSITY OF MARYLAND
SCHOOL OF PUBLIC POLICY

Best Practices for Securing your Zoom Meetings

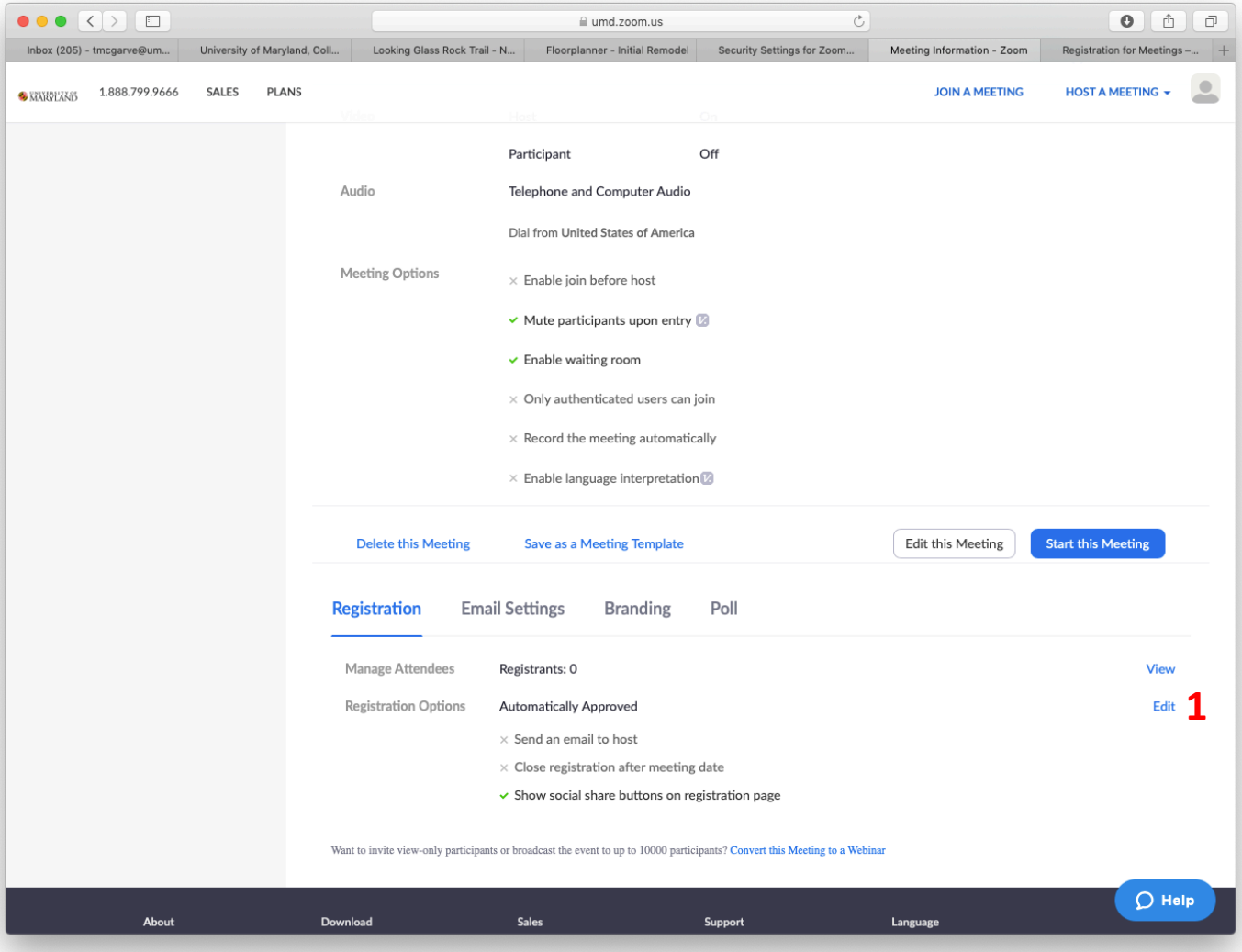
Advanced – Options for Securing Public Meetings

Requiring registration to join a meeting



- If you need to host a public meeting that prevents you from restricting access only to authenticated UMD users (that is, you will have participants joining that do not have a UMD directory account and hence you can't use the "allow only authenticated users" security option), you can require meeting participants to register to attend
- To require register, schedule a meeting as normal and select "Required" under "Registration"
- Click "Save" to schedule your meeting and access additional registration settings

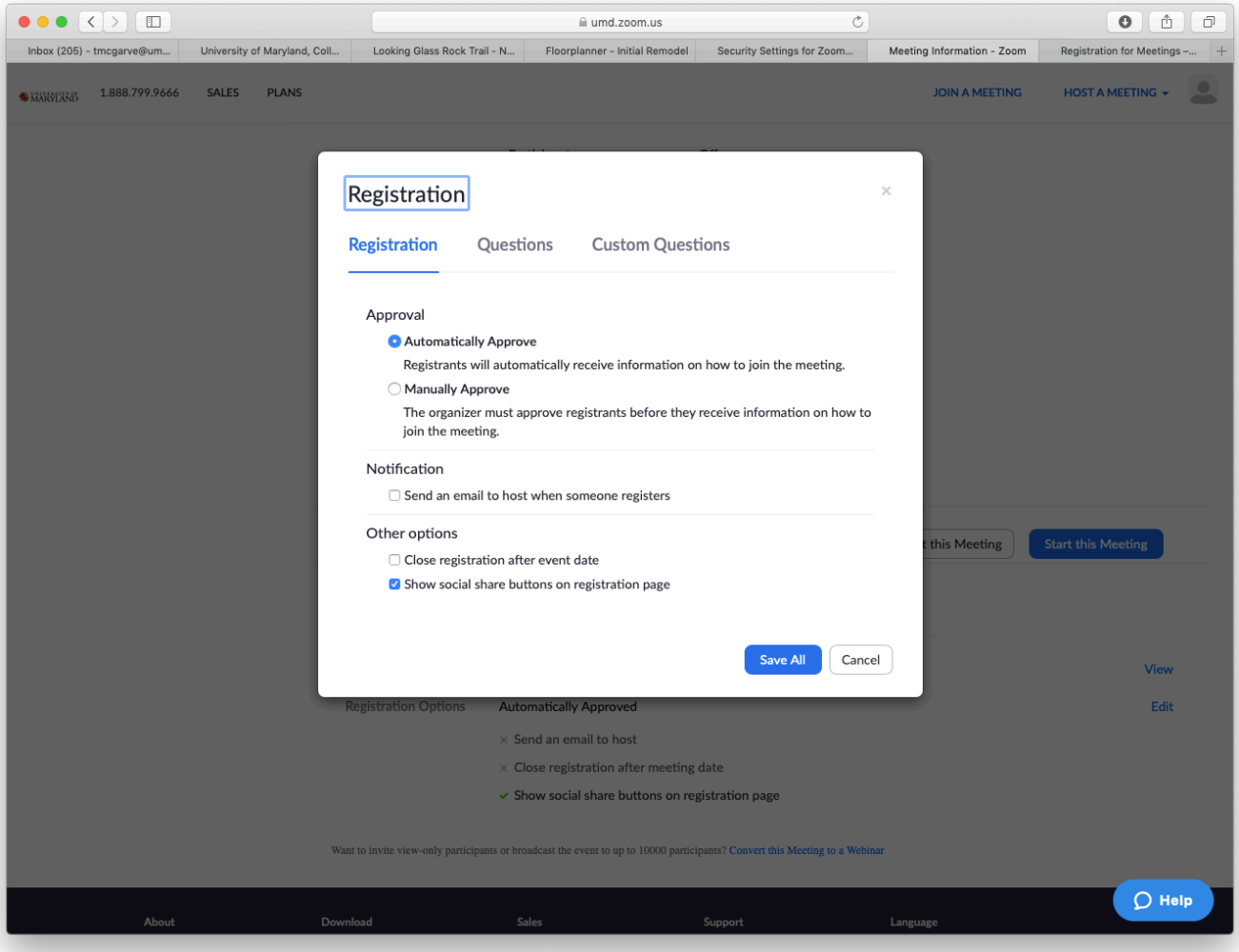
Specifying registration settings – Attendee Approval



- Once you have saved your meeting, you will be shown the meeting confirmation page where you can specify additional settings

1. To change the settings related to registration, scroll down to the “Registrations” section and click “Edit”

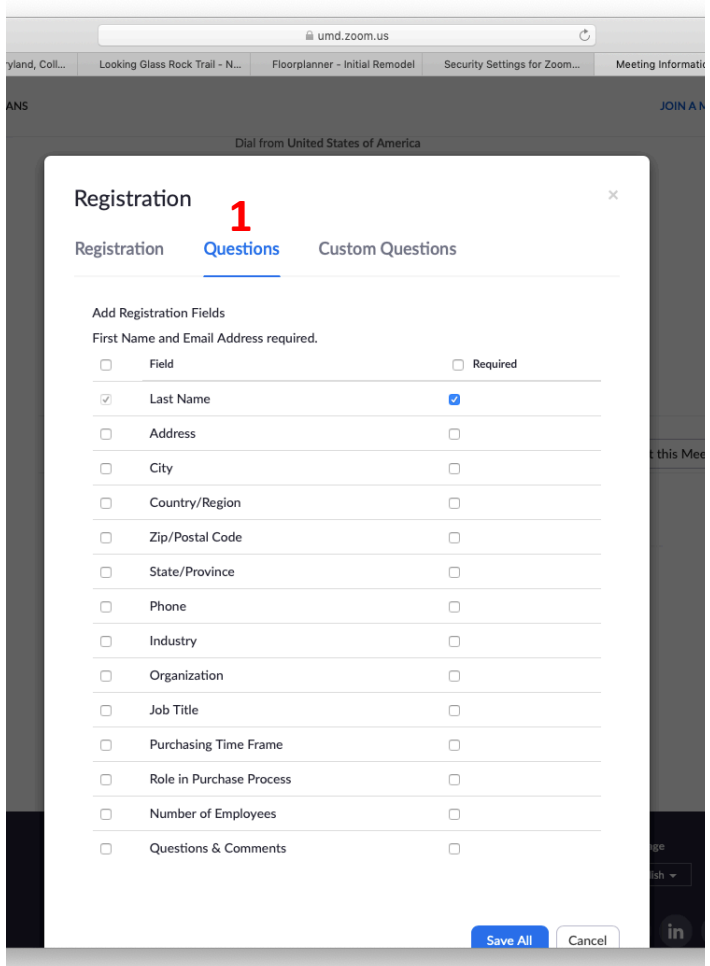
Specifying registration settings – Attendee Approval (cont.)

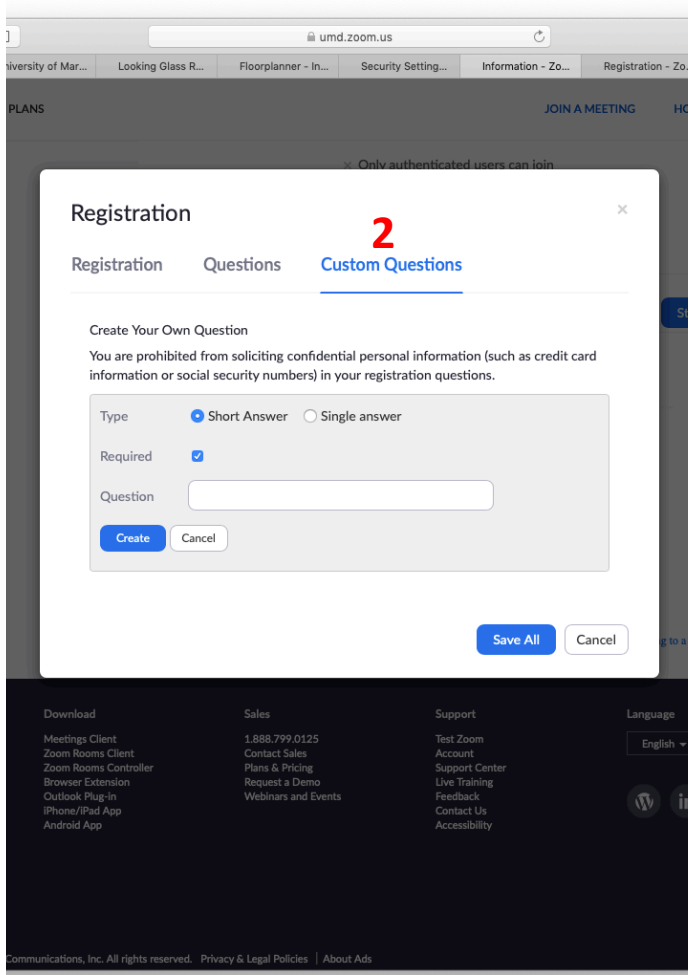


- From the Registration tab, you can specify how participants are approved
  - "Automatically Approve" will send the meeting connection details to anyone who completes the registration form
  - "Manually Approve" will allow the meeting host to review registrants and either approve or reject participants – only participants who are approved will be sent the meeting connection details

1

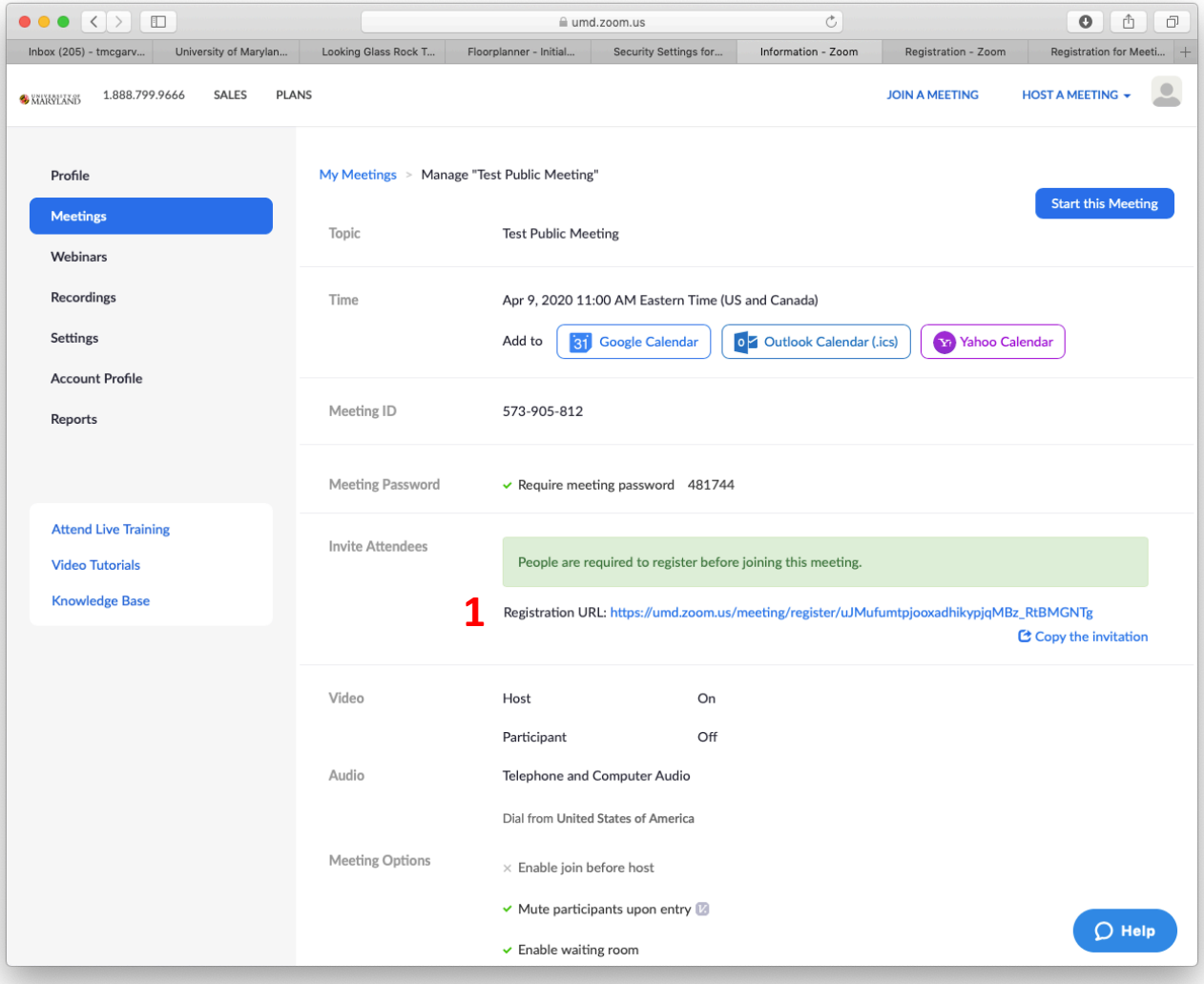
Specifying registration settings – Registration Questions





- By default, a participant will be asked to provide their first and last name, and email address
- You can request/require participants answer additional questions
    1. Under the “Questions” tab, you can select from a list of preset questions
    2. Under the “Custom Questions” tab, you can create your own questions to answer

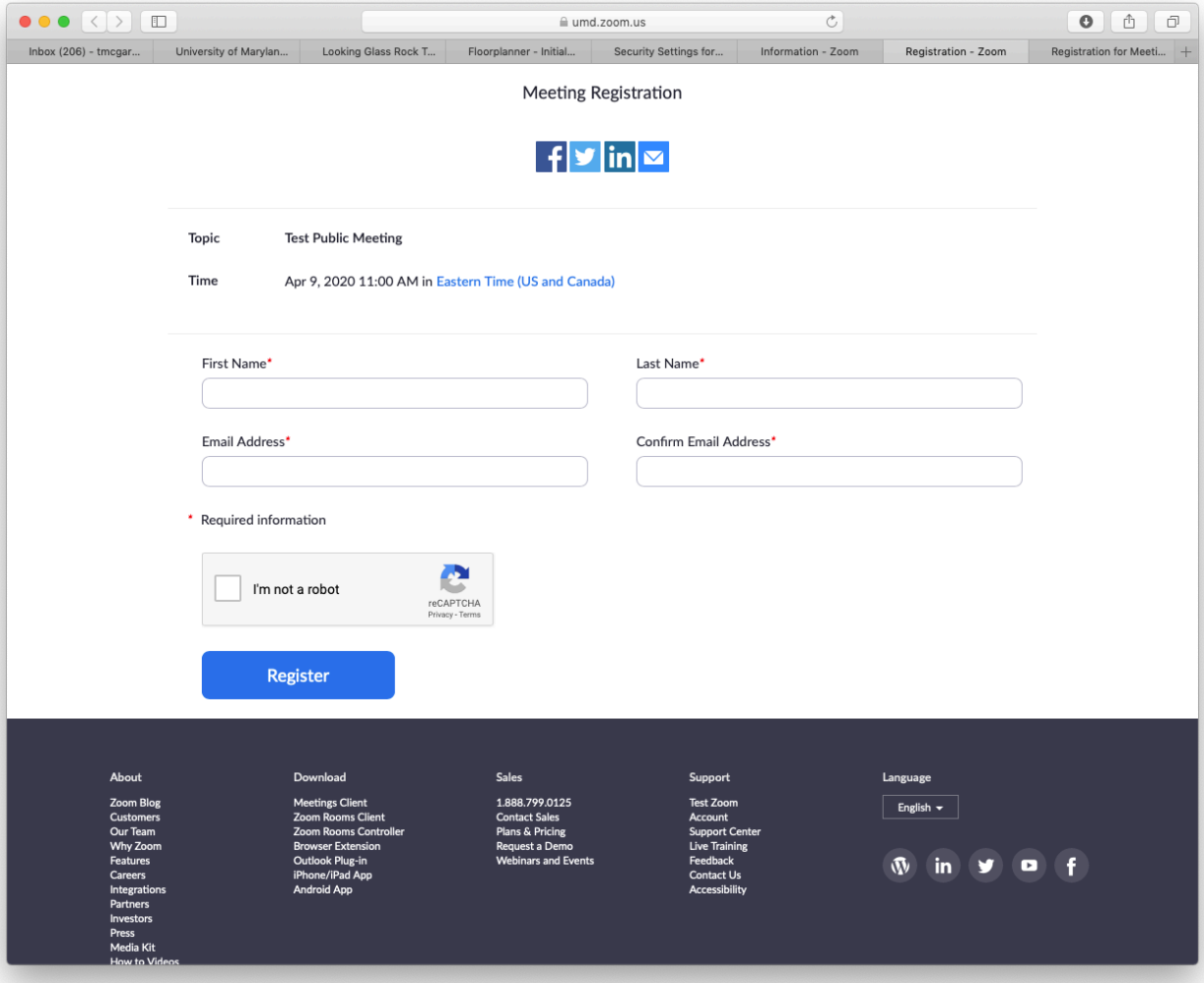
Participant Registration – Sharing the registration link



- In the meeting overview window, you can find the link to share with participants that will direct them to a webpage to enter their details

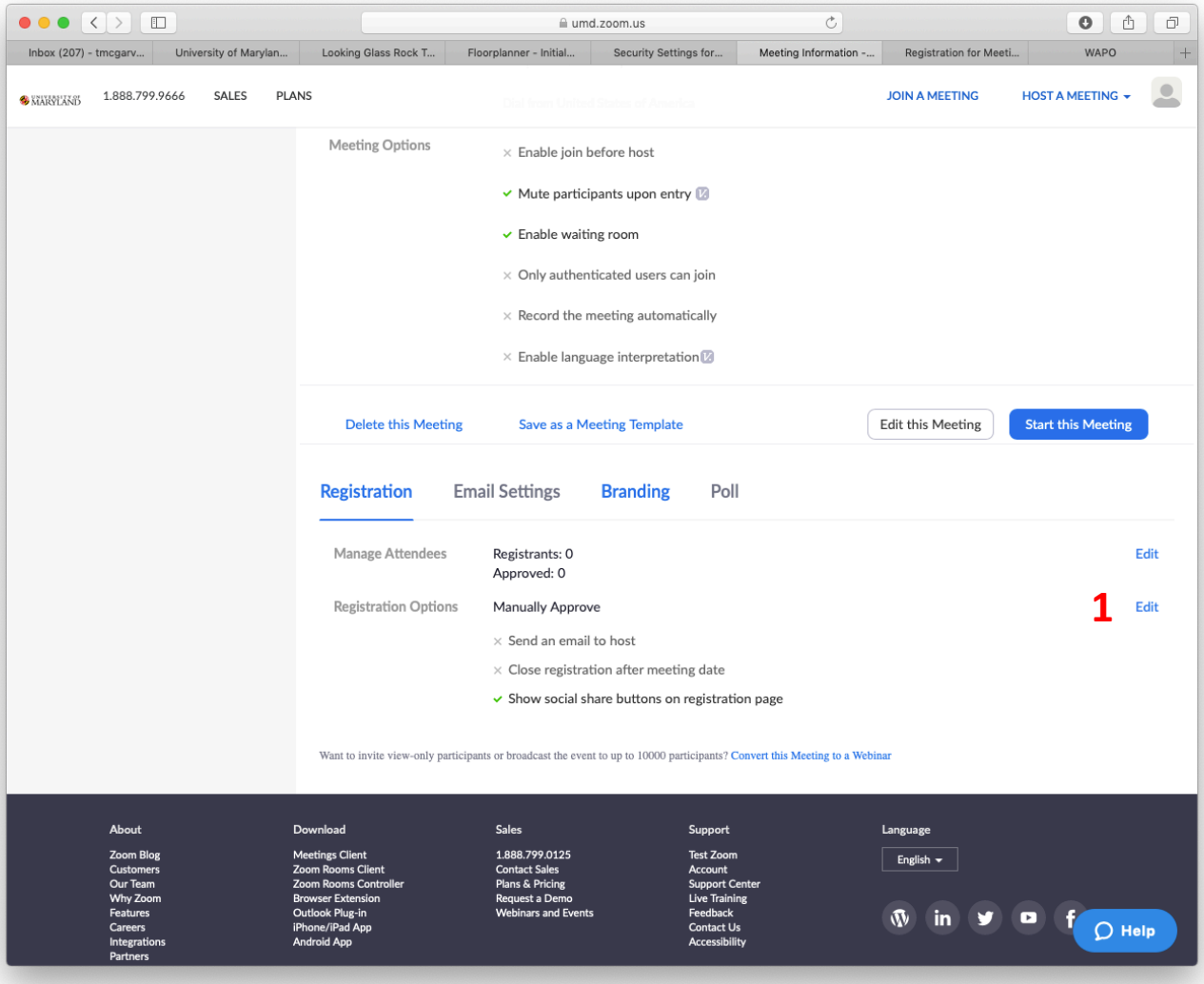
1. Copy and paste this link into whichever communication vehicle you are engaging with participants via

Participant Registration – What the participant sees



- When the participant clicks on the link, they will be taken to the registration page and shown the questions you have specified
- Once the fill in the required details, they click “Register”
- If you have set up your Attendee Approval to happen automatically, the participant will receive the meeting connection details directly to their email address
- If you have set up your Attendee approve to be manual, they will receive a notification that their registration has been submitted
    - As the host, you will now need to review and approve/reject registration requests

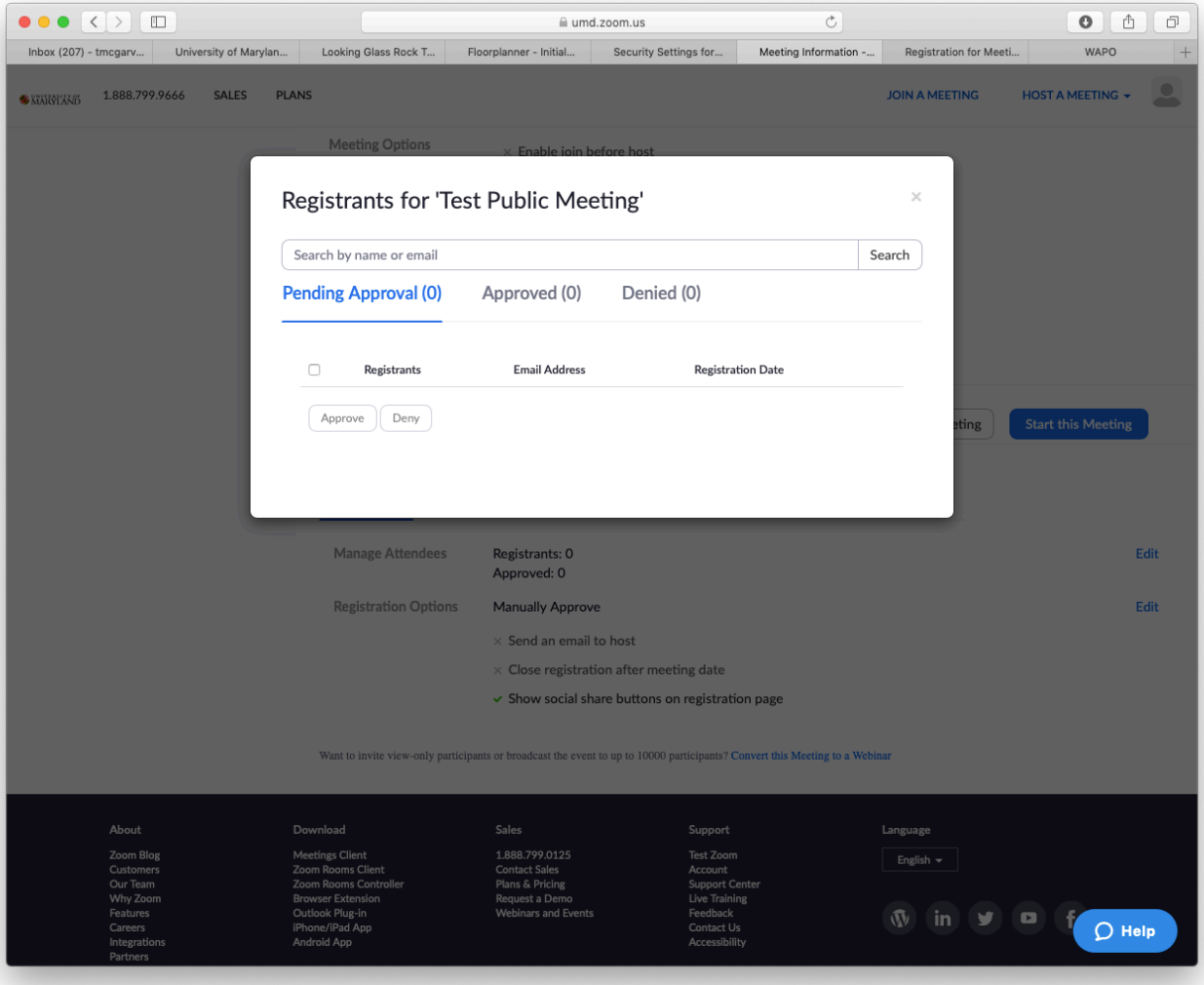
Approving Registration Requests



- If you have specified a manual approval process, you will need to review and accept/reject registration requests

1. To view registrants that have requested to join your meeting, click on “Edit” from the meeting overview page

Approving Registration Requests (cont.)



- From the window that opens, you can view registrants with Pending Approval (those that need to be review), those you have Approved, and those you have Denied
- To approve or deny registrants, select the check box next to their name and click either “Approve” or “Deny”
- Those registrants that you have approved will receive an email with the meeting connection details