# **ZOOM Security**

Never share Zoom meeting/webinar links or passwords publicly, on websites, or social media.

*Instead, share the event registration link for advertising your event.*

Table of Contents

[Moderately Interactive Zoom Meeting - RECOMMENDED SECURITY 2](#_Toc65431986)

[Security: 3](#_Toc65431987)

[Schedule Meeting: 6](#_Toc65431988)

[In Meeting (Basic): 7](#_Toc65431989)

[In Meeting (Advanced): 11](#_Toc65431990)

[Settings for Scheduling a Meeting 12](#_Toc65431991)

[Less Interactive Zoom Webinar - MOST SECURE 14](#_Toc65431992)

[Security: 15](#_Toc65431993)

[In Meeting (Basic): 16](#_Toc65431994)

[In Meeting (Advanced): 16](#_Toc65431995)

[Schedule A Webinar 18](#_Toc65431996)

[Start of Zoom Meeting 20](#_Toc65431997)

[Disruption: 22](#_Toc65431998)

[End the Meeting: 23](#_Toc65431999)

[Registration 25](#_Toc65432000)

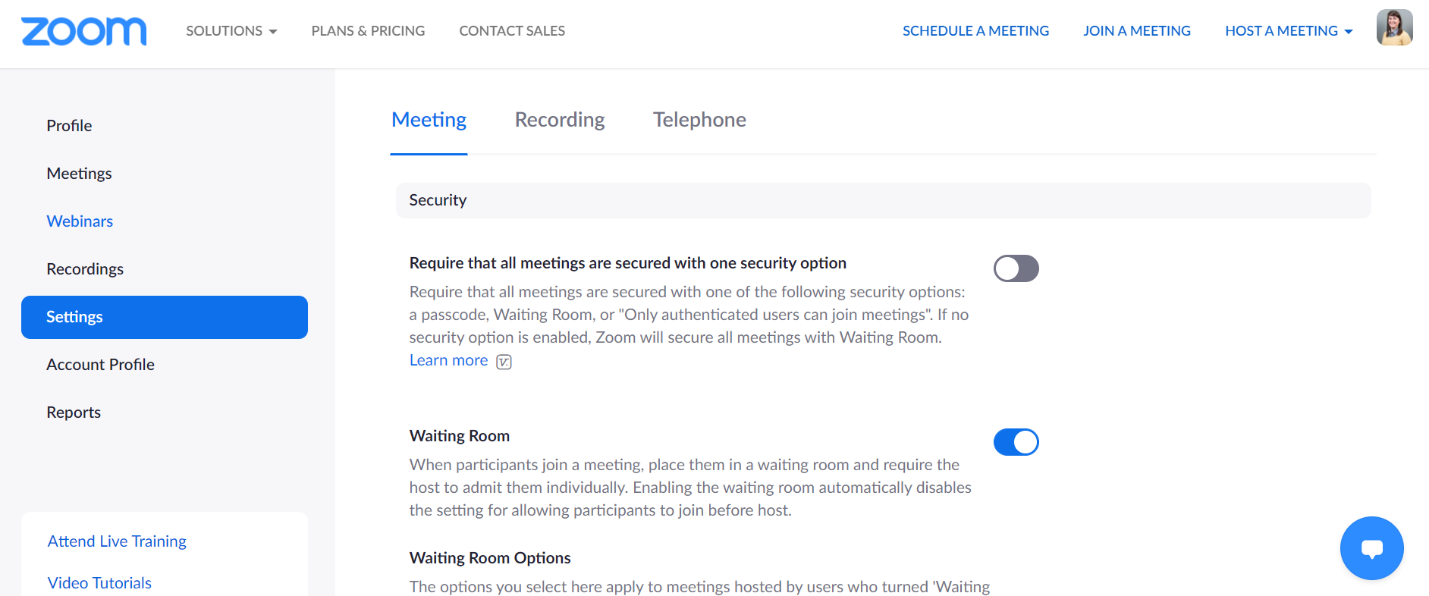
[Registration Process 28](#_Toc65432001)

## Moderately Interactive Zoom Meeting - RECOMMENDED SECURITY

When hosting an event that will be open to the general public and/or Penn State Community, the best practice is to create your meeting using the Penn State Zoom website at psu.zoom.us.

**Before creating your meeting, review your overall settings to make sure you are secure.**

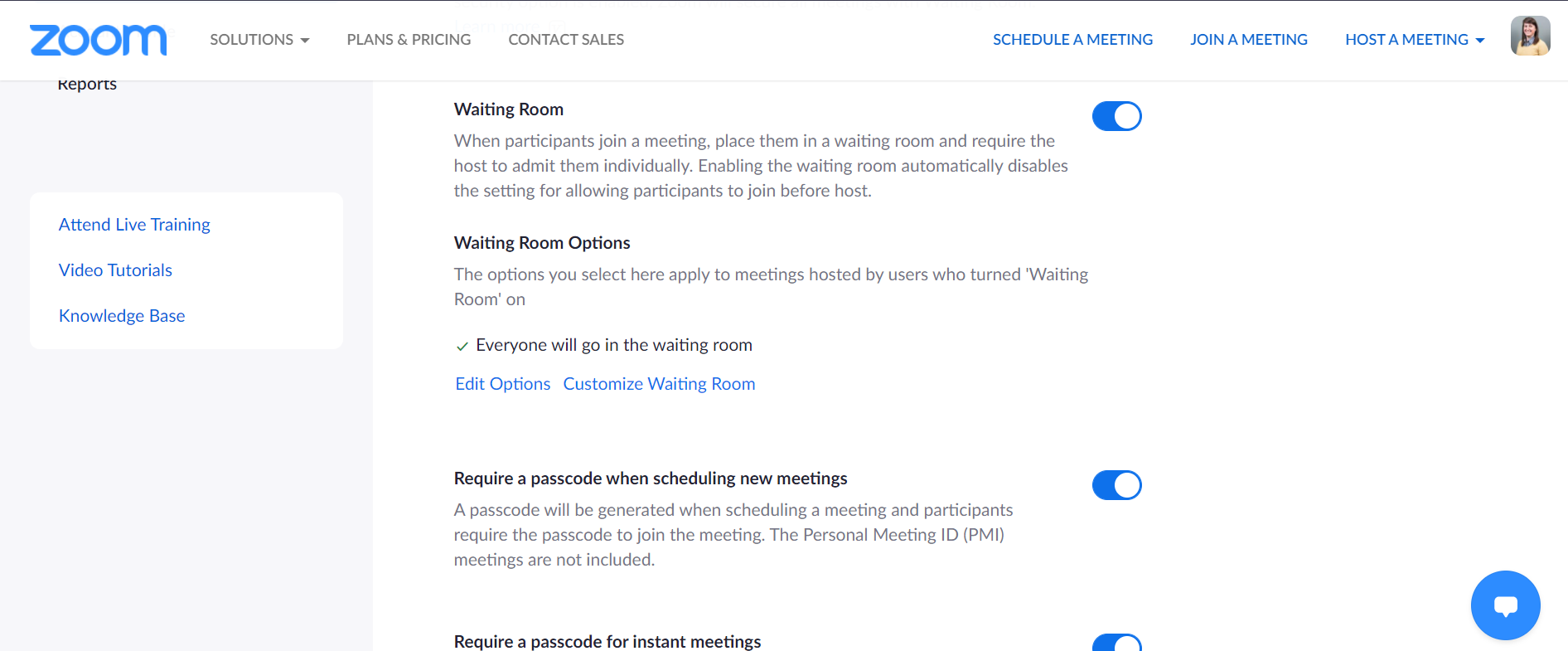
1. Sign into your account at zoom.psu.edu
2. Click on the “Settings” tab on the menu bar on the left-hand side of the screen.
3. Make sure the “Meeting” tab is selected at the top. (It should be automatically selected.)



1. The Settings are divided into headers. They are as follows:
   * Security
   * Schedule Meeting
   * In Meeting (Basic)
   * In Meeting (Advanced)
   * Email Notification
   * Other
2. You can review the recommended settings for each below or clicking on the header above to go to that part of the document. The following are the settings you should check, verify, and or consider for your meeting format.

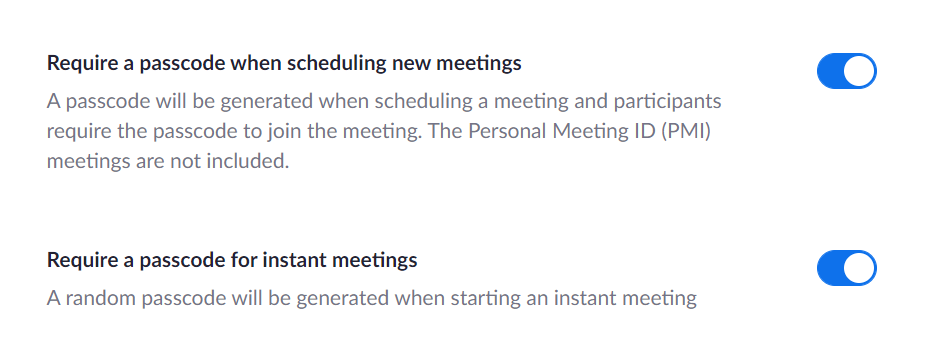
### Security:

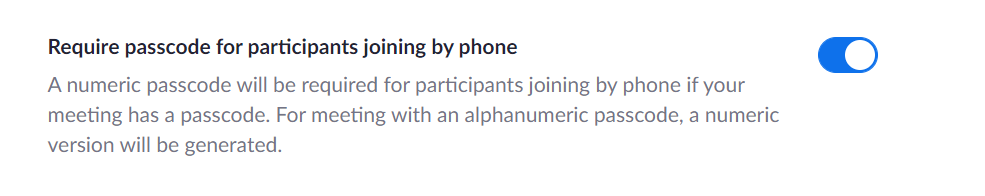
1. Waiting Room – Turned ON with Everyone going into the waiting room. Turn on Waiting Room- by Penn State default, everyone will go into the waiting room, which is the recommended setting (see red box below.



*OPTIONAL: To allow more interaction: Can customize logo, meeting topic, and waiting room description under “Customize Waiting Room.”*

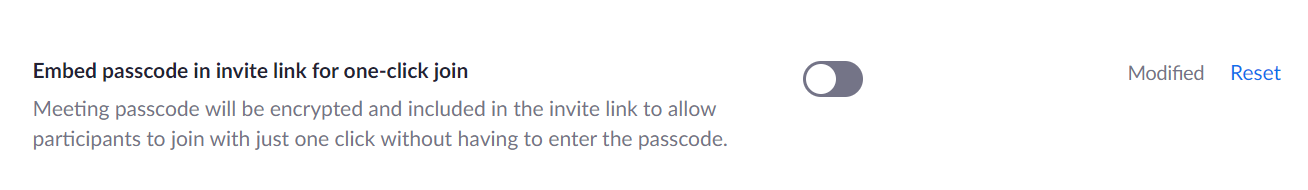
1. Require a passcode when scheduling new meeting and for instant meetings, as well as those joining by phone.
   * That includes when scheduling new meetings, instant meetings, and participants joining by phone
   * For open programs ***NEVER*** use your Personal Meeting ID (PMI)





1. Turn off Embed passcode in invite link for one-click join.

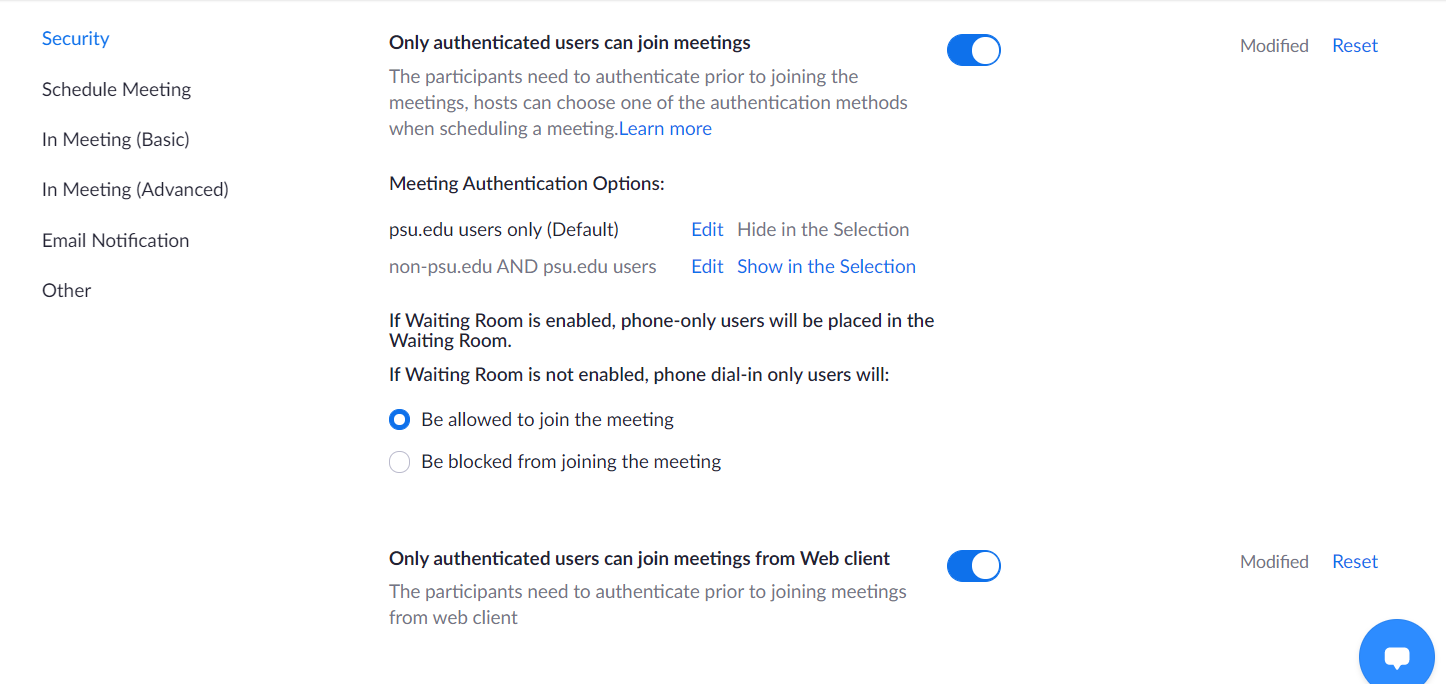
By default, Penn State’s settings has this option turned on. To provide an extra layer of security, we recommend **turning this off** and having participants re-enter the passcode for programs and open meetings.



A message will appear letting you know your settings do not align with the Penn State baseline. In this case, that is okay.

1. Turn on Require authentication to join (PSU or Zoom).
   * The highest security is to only allow psu.edu users.Click the option to “Hide in the Selection” next to non-psu.edu AND psu.edu users to prevent non-psu.edu users from joining.

By default, Penn State’s settings has this option turned on. To provide an extra layer of security, we recommend **turning this off** and having participants re-enter the passcode for programs and open meetings.



A message will appear letting you know your settings do not align with the Penn State baseline. In this case, that is okay.

* + If you need to include non-psu.edu users, it is less secure but making sure they are authenticated will help prevent spoof or fake email registrants from joining.

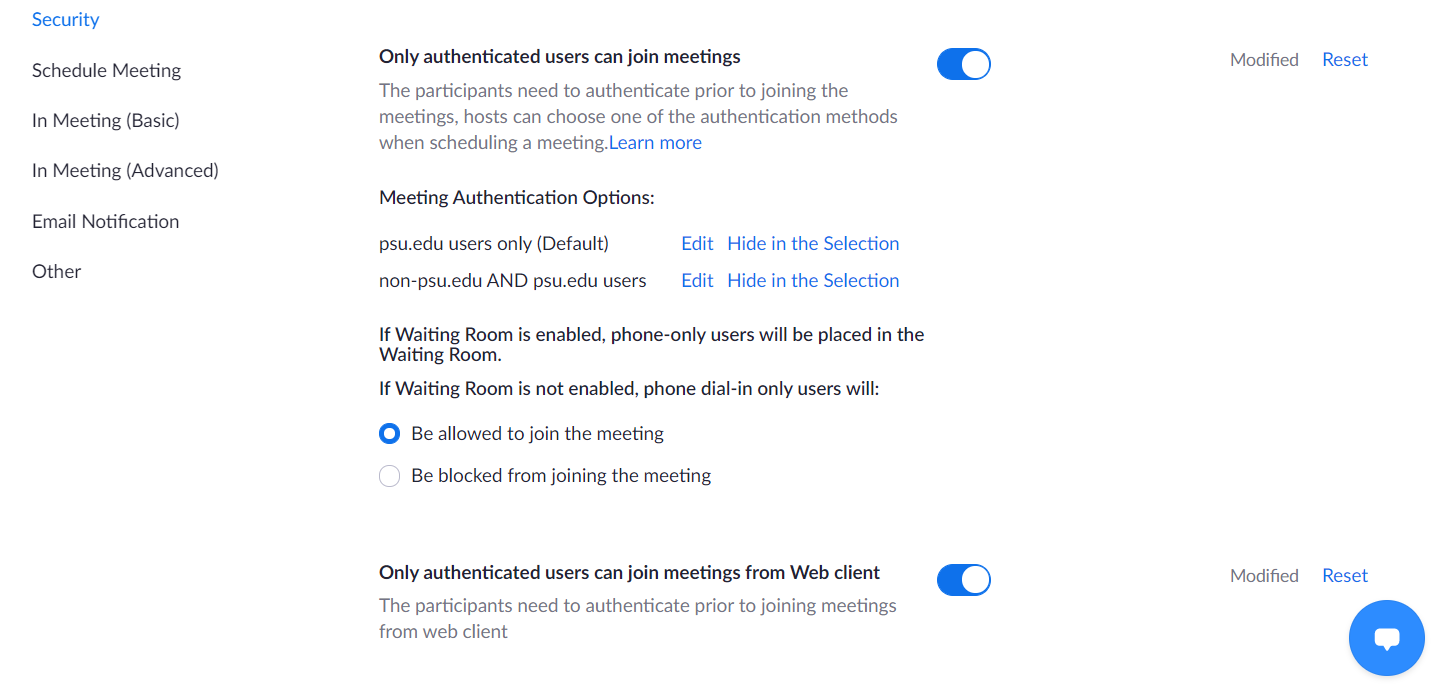
*We recommend you employ registration and reach out to non psu.edu registrants with the following message:*

“Dear \_\_\_\_\_\_\_,

I am reaching out because I see you registered for our event, \_\_\_\_\_\_\_\_\_\_. I am contacting you because you RSVP’d with a non-psu.edu address (Hotmail, Yahoo, Gmail, etc.). We are asking all participants to register with their psu.edu email address. Please let me know if this is possible. If you are a community member, please discuss your affiliation and interest with Penn State and the event so that can be taken into consideration in approving your participation.”

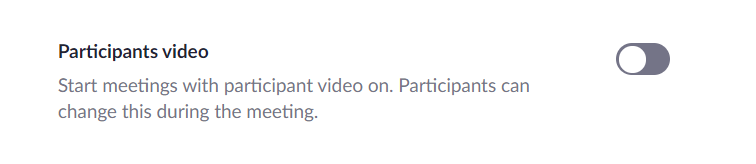
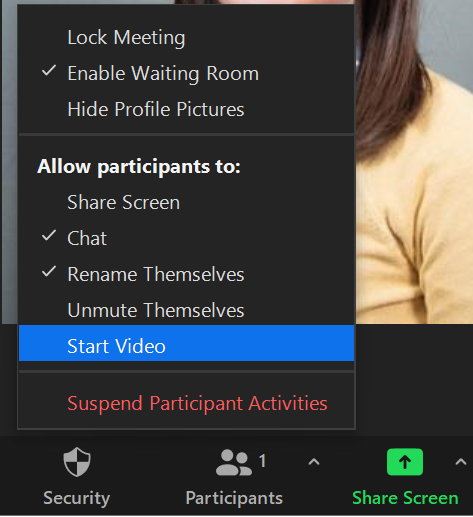
*If the individual does not reply or re-register for the event, cancel their registration to prevent them from joining.*

The highest security setting is psu.edu users only. If you want to make your event open to the public, then still require authenticated users but make sure non-psu.edu AND psu.edu users are showing in the selection.



### Schedule Meeting:

1. Participants Video – Have turned off, which is the Penn State baseline default.



* + Then, when you start the meeting, if you want to ensure participants cannot turn on video, go to the “Security” button. Uncheck “Start Video” as an option for participants to prevent them from turning on video.

The security button in the Zoom meeting will show you what participants are allowed to do. When you launch the meeting, confirm “start video” is not checked. If it is, uncheck it to prevent participants from turning on video.

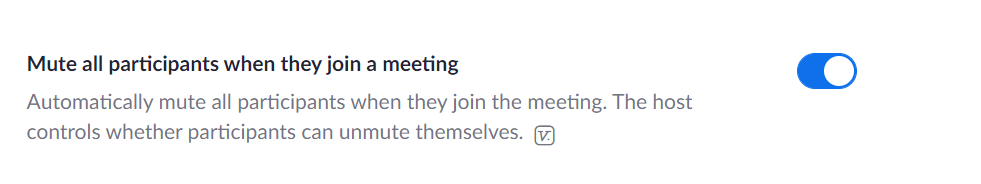
1. Allow participants to join before host – Turn off to allow you to review and admit participants individually.

By default, Penn State’s setting has this option turned on. To provide an extra layer of security, we recommend **turning this off** to ensure you can review and approve attendees prior to having them join.



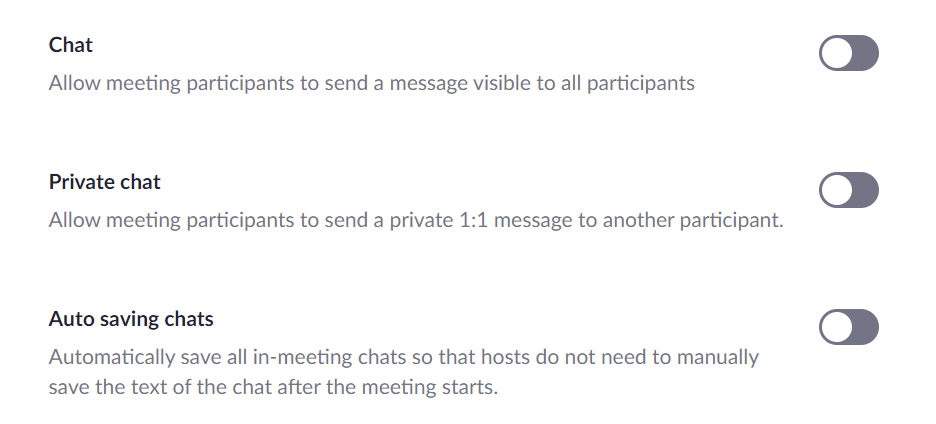
A message will appear letting you know your settings do not align with the Penn State baseline. In this case, that is okay.

1. Mute all participants when they join a meeting. This is turned off by Penn State baseline by default.



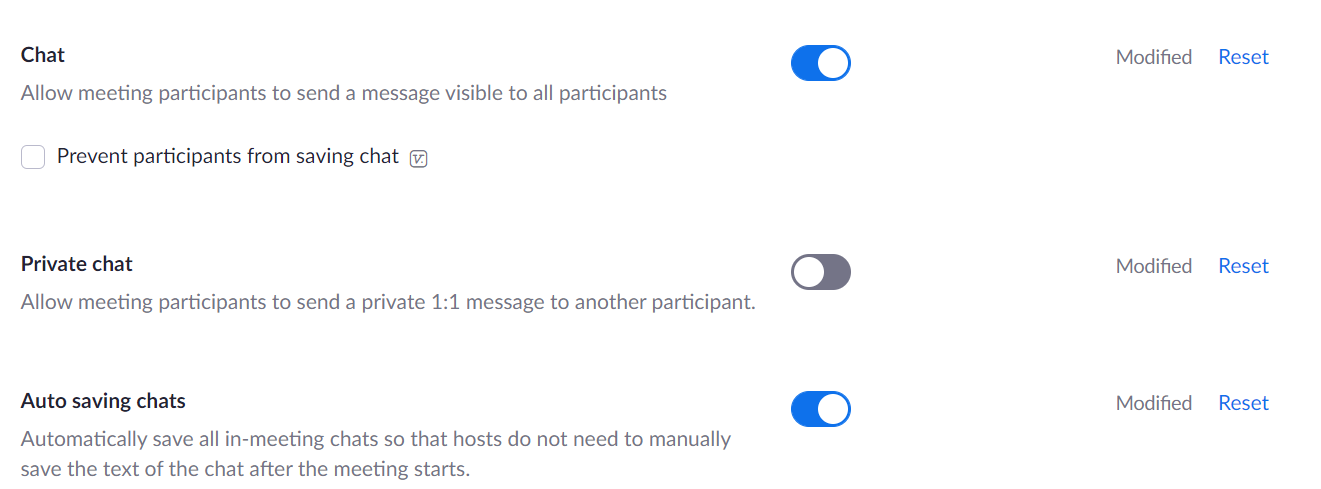
### In Meeting (Basic):

1. Chat and Private Chat turned off is the highest security setting. This is turned off by Penn State baseline by default.
   * When you remove the chat option, the Auto Saving Chat setting automatically turns off given there is no chat to save.

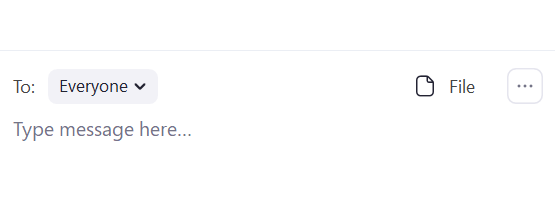


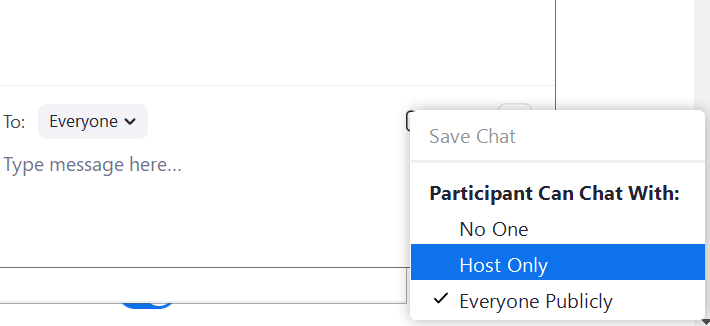
* + If you want to include chat for interaction, you should still turn off private chat and having the chats auto save. While less secure, it is a more interactive option.

Messages will appear letting you know your settings do not align with the Penn State baseline. By selecting this option your meeting is less secure, but you can have more interaction.



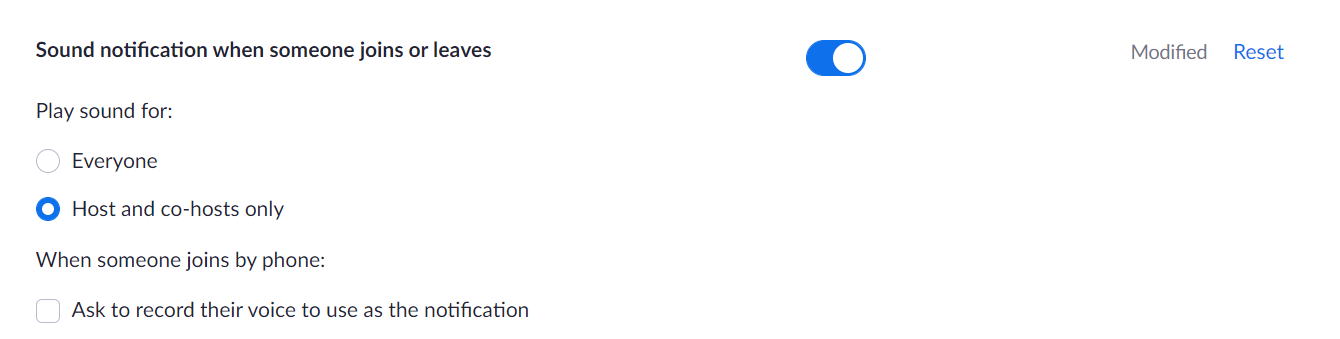
If you want to allow chat, you **MUST** turn **off** private chat and turn **on** auto saving chats.

* + The safest modification to allowing chats for interaction is to change settings to only allow chats to go to you or co-hosts. See how to update those settings in your Zoom meeting.
    - When you join your Zoom meeting, click on the “Chat” button. The chat will pop up and you will see symbol in the bottom right corner. Click on that.
    - From there you can select who the participant can chat with and change it host only. By only allowing chats to come to you, you prevent an offensive comment from being sent directly to attendees.

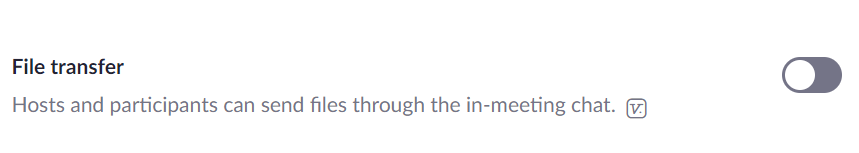


1. Sound notification when someone joins or leaves should be turned on to alert you if someone new joins your meeting.
   * This setting should only be for hosts and co-hosts, not everyone. Once you turn on this setting, you will need to switch from “Everyone” to “Host and co-hosts only.”

By default, Penn has this setting turned off. To provide an extra layer of security, we recommend **turning this on** to alert hosts to a new participant joining.



A message will appear letting you know your settings do not align with the Penn State baseline. In this case, that is okay.

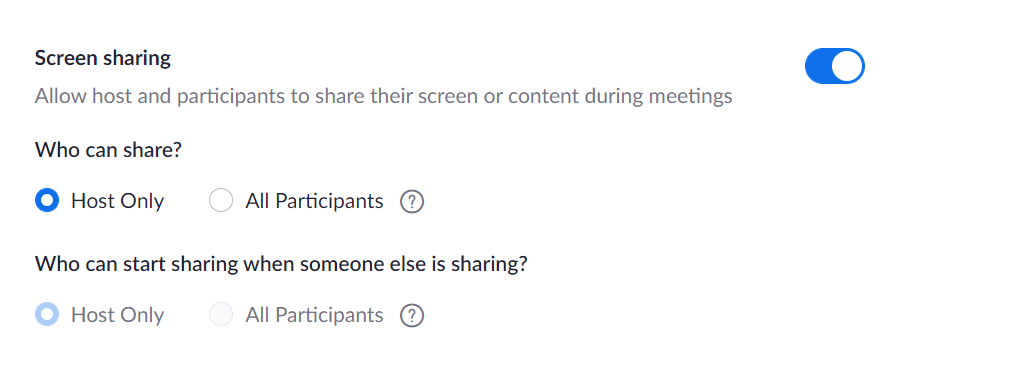
1. Make sure File transfer is turned off. This is turned off by Penn State baseline by default.
2. You should make sure your meeting control toolbar is always showing, thus in the event of a Zoom bombing, you able to quickly locate the removal and report tools to respond.

By default, Penn has this setting turned off. To provide an extra layer of security, we recommend **turning this on** to enable hosts to quickly respond to disruptive participants.



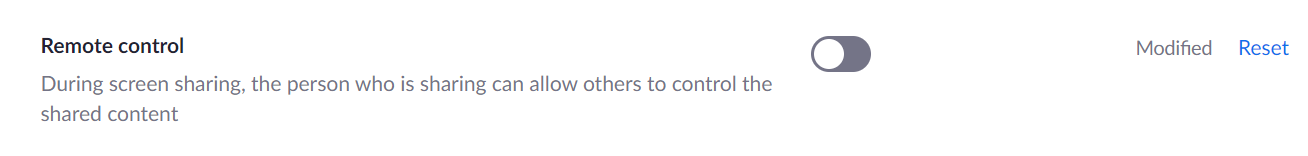
A message will appear letting you know your settings do not align with the Penn State baseline. In this case, that is okay.

1. With screen sharing, make sure that “Host Only” is selected. You can change to allow others to share their screen in meeting if needed. This is already set by Penn State baseline by default.



1. Turn off Remote Control to prevent participants from taking control of shared screen.

By default, Penn State’s setting has this option turned on. To provide an extra layer of security, we recommend **turning this off** to ensure you can review and approve attendees prior to having them join.

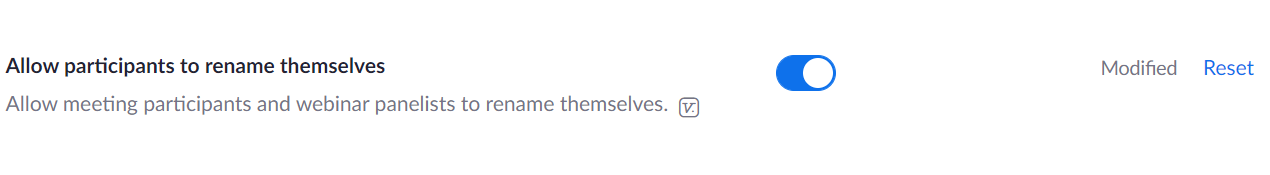


A message will appear letting you know your settings do not align with the Penn State baseline. In this case, that is okay.

1. Makes sure your, “Allow removed participants to rejoin” is turned off. This is turned off by Penn State baseline by default.



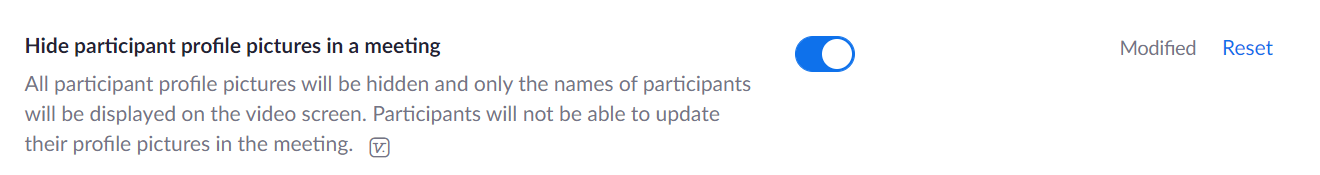
1. Allow participants to rename themselves in order to promote inclusion for pronouns and name changes. This is turned off by Penn State baseline by default.
   * If you want to allow people to add their pronouns, you **MUST** turn **on** the option to let participants rename themselves Just be mindful to monitor the participant list for any individuals who decide to use this setting to share an offensive name or inappropriate message and remove them.



This message will appear letting you know your settings do not align with the Penn State baseline. By selecting this option your meeting is less secure, but you can be more inclusive.

1. Hide participant profile pictures in a meeting should be turned on to prevent offensive pictures from being displayed and added/or changed in real-time during your session.

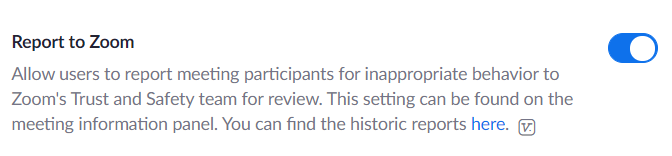
By default, Penn has this setting turned off. To provide an extra layer of security, we recommend **turning this on** to prevent participants from uploading an offensive profile picture during the meeting.



A message will appear letting you know your settings do not align with the Penn State baseline. In this case, that is okay.

### In Meeting (Advanced):

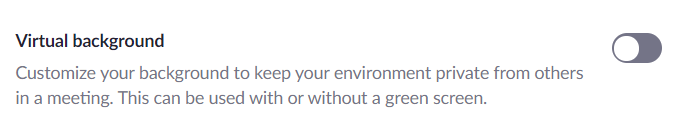
1. If there is inappropriate behavior in a Zoom meeting, there is an option to report the participant to Zoom for review. This is turned on as part of the Penn State baseline.



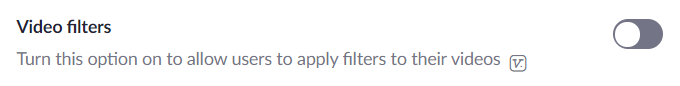
1. Do not allow virtual backgrounds, videos for virtual backgrounds,

or video filters. They should be turned off.

By default, Penn State’s setting has this option turned on. To provide an extra layer of security, we recommend **turning these off** to prevent offensive virtual backgrounds and filters from disrupting your meeting.

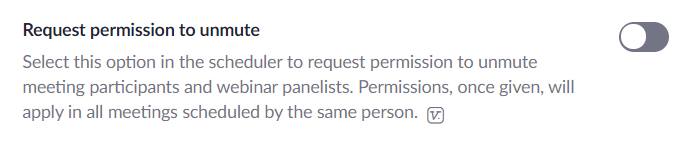
 

Zoom screenshot showing "Allow use of videos for virtual backgrounds" unchecked. 



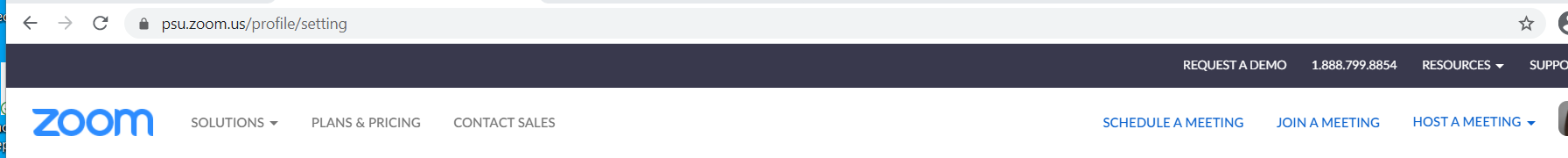
A message will appear letting you know your settings do not align with the Penn State baseline. In this case, that is okay.

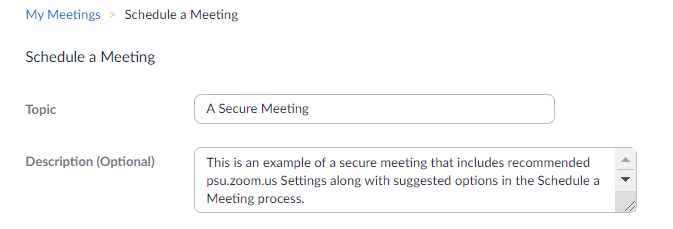
1. Due to privacy and security, the host cannot unmute other participants without their consent. This option allows, when the meeting is scheduled, for pre-approval to be unmuted by the host. This is turned off.



### Settings for Scheduling a Meeting

The settings recommended above are just a part of the overall meeting setup. This section will highlight the key settings used when you **Schedule a Meeting**.

Log in to zoom.psu.edu to **Schedule A Meeting**. 



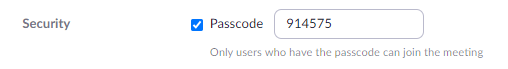
1. Require **Registration** for participants. Accept or Decline registrants manually after reviewing their registration information. Require multiple Question/Custom Question fields to be completed by registrant. Registration prevents non-vetted participants from entering your meeting.



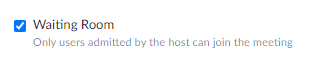
1. **Generate Meeting ID Automatically**. Do not use a Personal Meeting ID for more than casual meetings with colleagues.



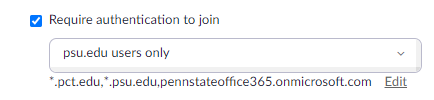
1. Use a Secure **Passcode**. Don’t embed the passcode with the meeting URL for ease. Having the participant enter the passcode to join is an extra security measure.



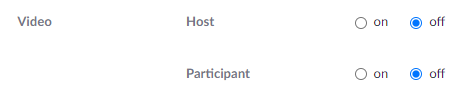
1. Send all participants to the **Waiting Room**. Don’t admit them all at once. If participants try to join late or in a group, that could be an indicator of malintent to disrupt.



1. Allow only **authenticated users can join**. By default, this includes Penn State accounts. If this can’t work for you event, you can uncheck this option and review the notes about outside users under Security, point 4.



1. **Video** for the Host and Participants should be **off** by default.



1. **Don’t allow participants to join anytime**. This would give someone the opportunity to scope out the meeting in advance. This shouldn’t happen if all participants are sent to the waiting room. This is an added precaution.



1. **Mute participants upon entry**. This prevents unwanted audio.



1. Assigning an **Alternative Host** is not recommended. Co-hosts and alternative hosts are different settings. A co-host can essentially perform the same functions as a host, but only when a meeting has already started. This is the role you would want for someone who is helping you manage a meeting. Alternative host is the next level of that. An alternative host is designated to have the same role as the original host. With this role the alternative host essentially has the key to your house and can come and go as they please. They can start a meeting with or without you present, etc. This role has its place, however for a recurring meeting and especially for a meeting using someone’s personal meeting ID, this is discouraged. A personal meeting ID is for your own use and for you alone.

## Less Interactive Zoom Webinar - MOST SECURE

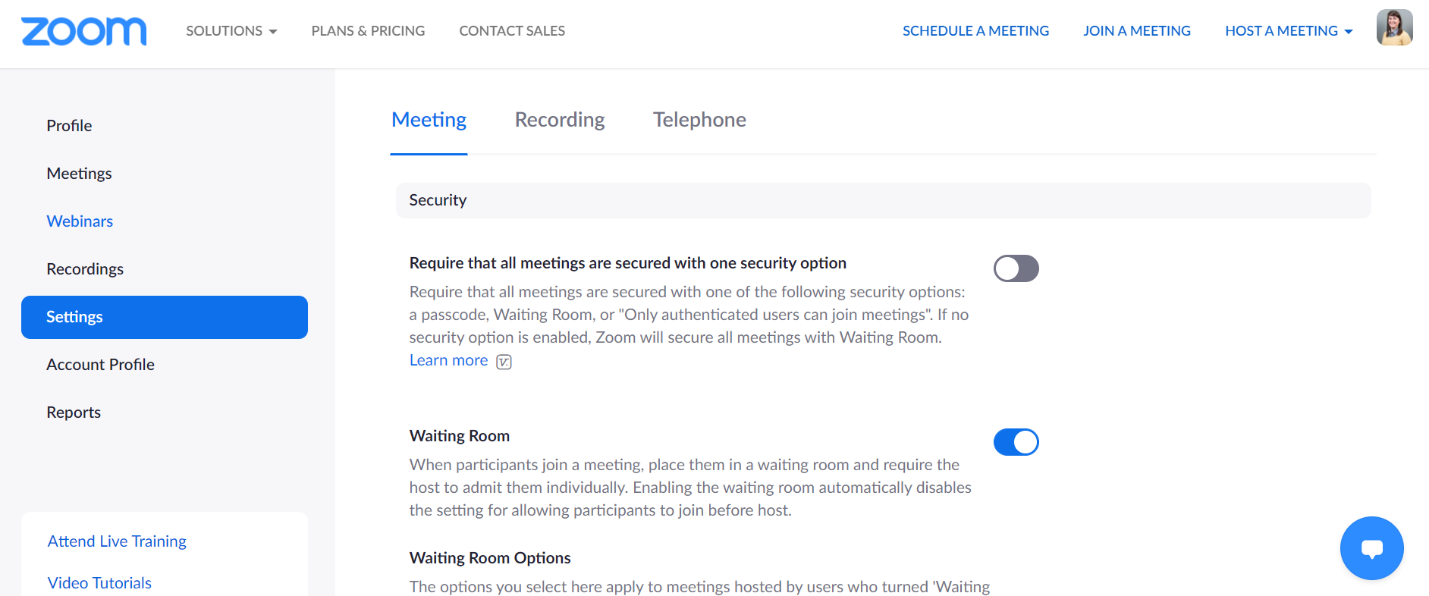
Hosting a webinar is a more secure platform that still provides a level of virtual interaction to engage your participants.

* Host and panelists can share video, audio, and screen.
* Attendees are view only.
* Attendees have ability to Q&A, Chat, Polling, Survey.
* Host can allow attendee to talk.

**Before creating your webinar, review your overall settings to make sure you are secure.**

1. Sign into your account at zoom.psu.edu
2. Click on the “Settings” tab on the menu bar on the left-hand side of the screen.
3. You should see the following options below.

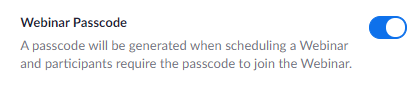
Make Sure the “Meeting” tab is selected at the top. You should automatically, be placed into this page when you select settings

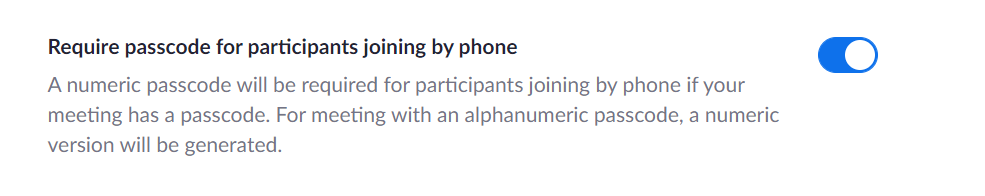


1. The Settings are divided into headers. They are as follows:
   1. Security
   2. Schedule Meeting
   3. In Meeting (Basic)
   4. In Meeting (Advanced)
   5. Email Notification
   6. Other
2. You can review the recommended settings for each below or clicking on the header above to go to that part of the document. While there are the Penn State recommended settings, the following are the settings applicable to a webinar that you should check, verify, and or consider.

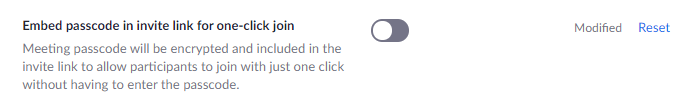
### Security:

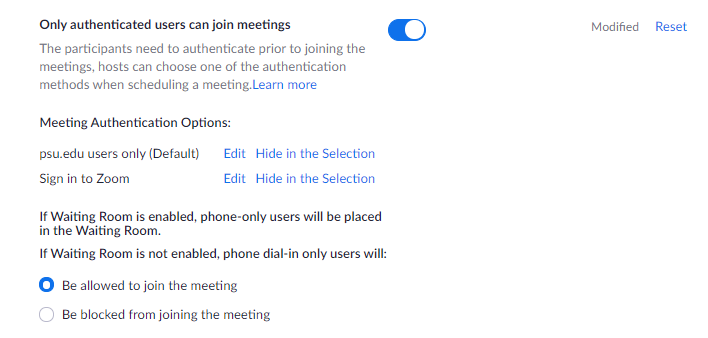
1. Webinar Passcode on. Use a Secure **Passcode**. Don’t embed the passcode with the webinar URL for ease. Having the participant enter the passcode to join is an extra security measure.



1. Require passcode for participants joining by phone on.
2. Turn off Embed passcode in invite link for one-click join.

A message will appear letting you know your settings do not align with the Penn State baseline. In this case, that is okay.



1. Allowing only authenticated users to join meetings (webinars) adds an additional layer of security since the user must log in to zoom to participate. Turn this option ON. 

A message will appear letting you know your settings do not align with the Penn State baseline. In this case, that is okay.

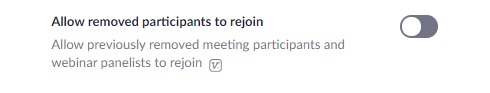
1. Only authenticated users can join meetings (webinars) from the web client. Turn this option ON.



A message will appear letting you know your settings do not align with the Penn State baseline. In this case, that is okay.

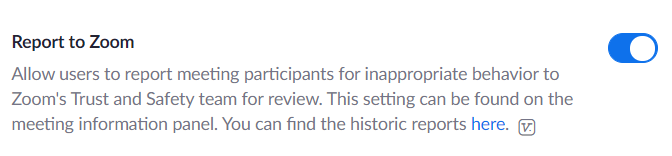
### In Meeting (Basic):

1. If a disruptive participant was removed by the host, it is best practice to not allow the removed participants to rejoin the webinar. This option should remain OFF.

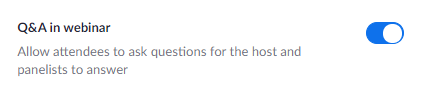


### In Meeting (Advanced):

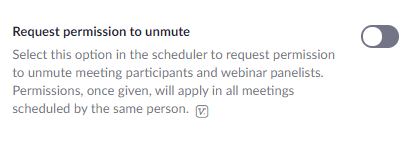
1. If there is inappropriate behavior in a Zoom meeting, there is an option to report the participant to Zoom for review. This is turned on as part of the Penn State baseline.



1. Allow attends to ask questions for the host and panelists through the Q&A in webinar option.



1. Due to privacy and security, the host cannot unmute other participants without their consent. This option allows, when the meeting is scheduled, for pre-approval to be unmuted by the host. This is turned off.

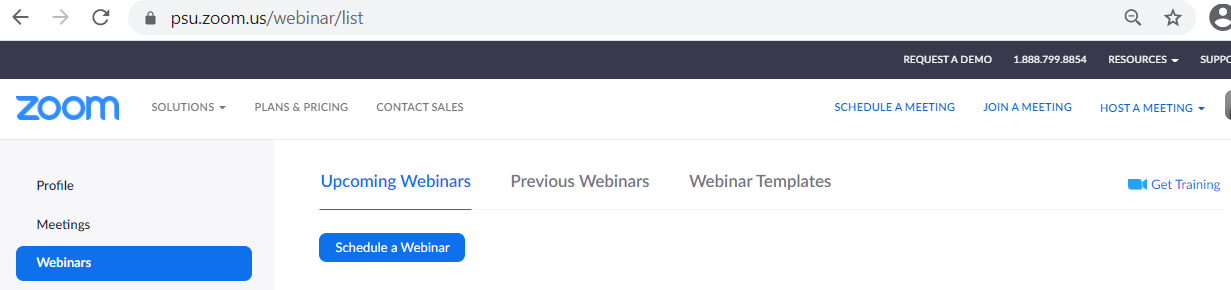


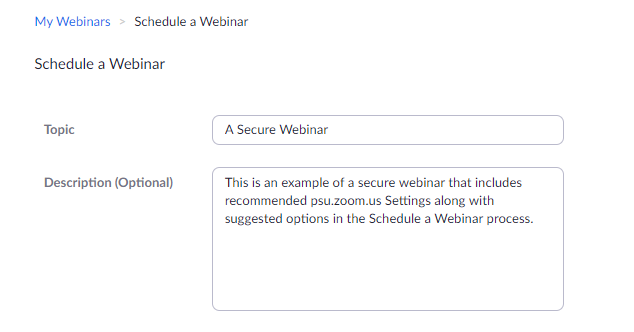
### Schedule A Webinar

The settings recommended above are just a part of the overall webinar setup. This section will highlight the key settings used when you **Schedule a Webinar**.

Log in to zoom.psu.edu to **Schedule a Webinar**.

Select Webinars from the left side navigation menu. Then select Schedule a Webinar.





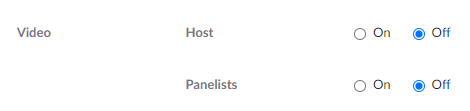
1. Require **Registration** for participants. Accept or Decline registrants manually after reviewing their registration information. Require multiple Question/Custom Question fields to be completed by registrant. Registration prevents non-vetted participants from entering your meeting.



1. Use a Secure **Passcode**. Don’t embed the passcode with the webinar URL for ease. Having the participant enter the passcode to join is an extra security measure.



1. **Video** for the Host and Participants should be **off** by default.



Webinar Options:

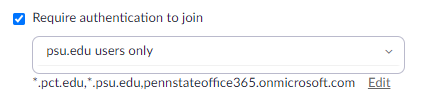
1. Click on **Q&A** to enable participants and hosts to engage through Questions and Answers during the webinar.



1. Click on **Enable Practice Session** to test any time in advance. This allows the host, alternative host, and panelist to join the webinar and become familiar with the webinar controls.



1. Allow only **authenticated users can join**. By default this includes Penn State accounts. If this can’t work for you event, you can uncheck this option.



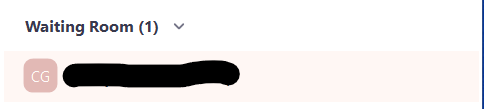
1. Assigning an **Alternative Host** is not recommended. Co-hosts and alternative hosts are different settings. A co-host can essentially perform the same functions as a host, but only when a meeting has already started. This is the role you would want for someone who is helping you manage a meeting. Alternative host is the next level of that. An alternative host is designated to have the same role as the original host. With this role the alternative host essentially has the key to your house and can come and go as they please. They can start a meeting with or without you present, etc. This role has its place, however for a recurring meeting and especially for a meeting using someone’s personal meeting ID, this is discouraged. A personal meeting ID is for your own use and for you alone.

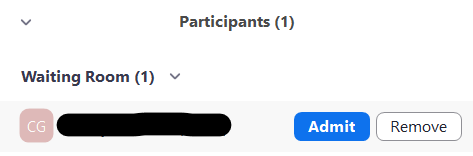
## Start of Zoom Meeting

1. Locate the **Security** button on the Zoom toolbar and verify the meeting settings. When security settings are adjusted the Security menu will close. Reopen it to address each option.

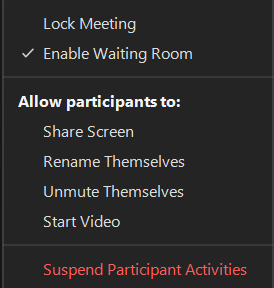


* + **Lock Meeting** is used to keep others from joining. This can be advantageous to avoid the distraction and possible risk of latecomers.
  + **Enable Waiting Room** should be checked indicating that it will be used.





* + **Uncheck** each of the **Allow participants** to settings which disables them. You can enable/disable them on demand if you need to. Host/Co-host are not impacted.
    1. **Share Screen**
    2. **Rename Themselves**
    3. **Unmute Themselves**
    4. **Start Video**

****

1. Set up meeting **recording** (optional and situational)  
   * Per Pennsylvania wiretapping law, you must inform participants if you plan to record the session. Also, discussion of High-risk or Restricted data (as defined in [AD95](https://guru.psu.edu/policies/AD95.html)) is not permitted while recording.
     1. Click the **Record** button in the menu bar at the bottom.
     2. Click the **Stop Recording** icon in the menu bar to finish the recording.

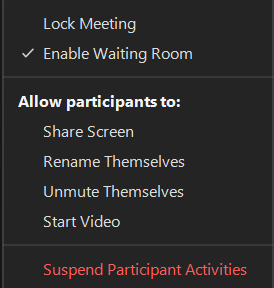
NOTE: Local recordings are automatically saved to the host's computer when the meeting is ended.

## Disruption:

1. Locate the **Security** button on the Zoom toolbar. The last two options can be used if someone disrupts your meeting.



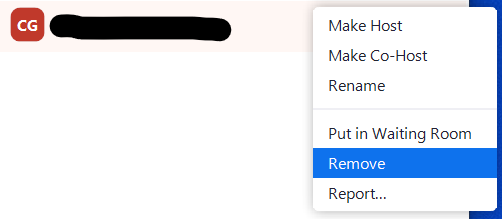
* + Click **Suspend Participant Activities**, then click **Suspend** on the pop-up dialogue box – this stops malicious activity and provides time to determine next steps. Participants audio and video will be turned off, screen-sharing will be disabled, and the meeting will be locked.

****

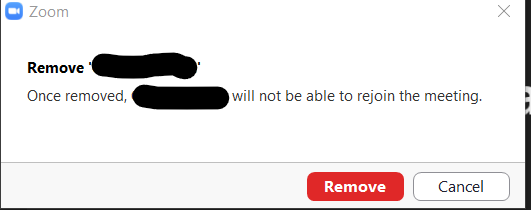
* + Click on participant to removed.



* Click on the More button.
* Start the process to remove the participant by selecting Remove.

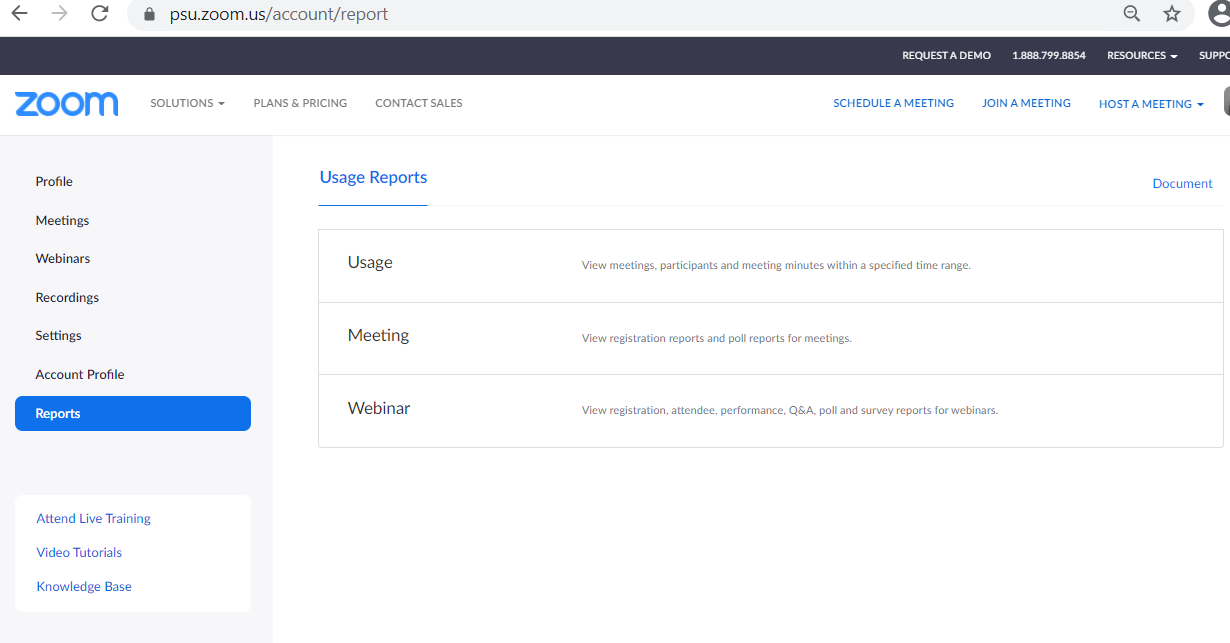


* A dialogue box will be displayed. Choose Remove to confirm that the participant should be removed from the meeting/webinar. Remove.

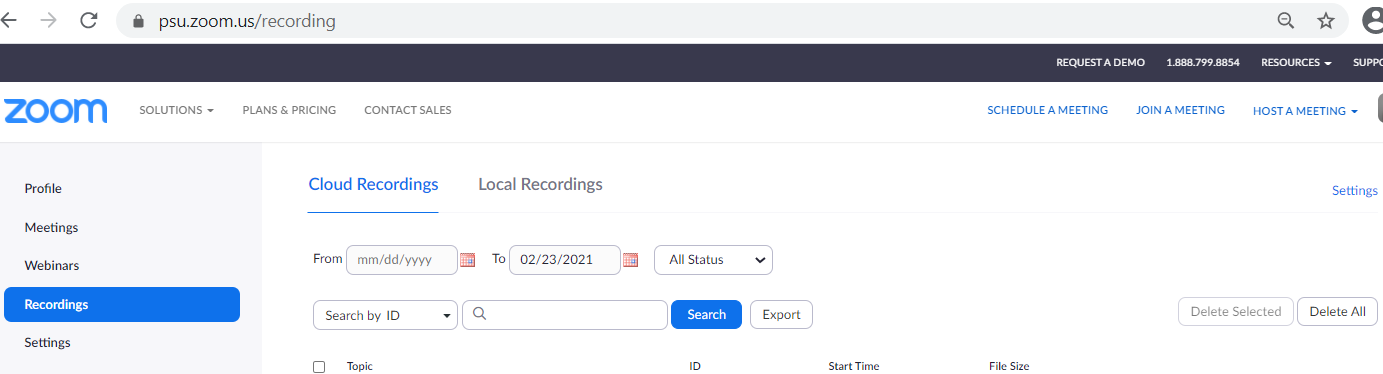


## End the Meeting:

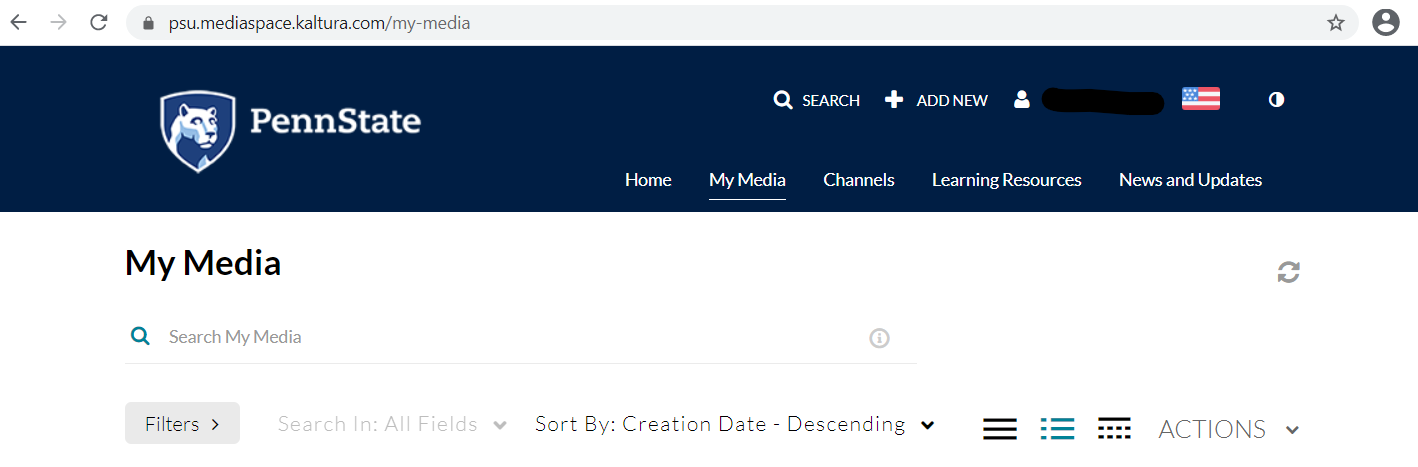
1. Click Stop recording (if applicable)
2. Click End meeting
3. Log in to zoom.psu.edu
4. Reports - Generate appropriate reports:
   * + Usage report
     + Meeting (Registration)
     + Webinar (Registration, Attendee)



1. Locate Meeting/Webinar recording by logging into zoom.psu.edu.
   * Recordings – note that there are Cloud Recordings and Local Recordings



* You may also find your Zoom Cloud Recordings in the Penn State Media Management platform, [Kaltura](https://psu.mediaspace.kaltura.com/home), under My Media.



1. Report any disruptions to University Police immediately police.psu.edu/report-crime
   * When calling the police (**814-863-1111**), an officer or detective will take the call over the phone. There is an option to report the incident via online: <https://www.police.psu.edu/report-crime> for those who may feel more comfortable submitting an online complaint.  
       
     Officers will ask initial questions as who the reporting person and take some basic contact information. Details such as **when, where, what class, how many people in attendance, what happened**, etc. will be asked. Specific information that is very helpful to the investigation include:  
     ◦ **Obtain Meeting ID  
     ◦ Obtain participant report (meeting host generated)  
     ◦ Obtain chat logs  
     ◦ Obtain session recordings if exist**  
     The investigation will be launched and follow up with the reporting person will likely be done by a detective. In regular circumstances, face-to-face communication is necessary, however, due to COVID restriction much communication is done via phone.

## Registration

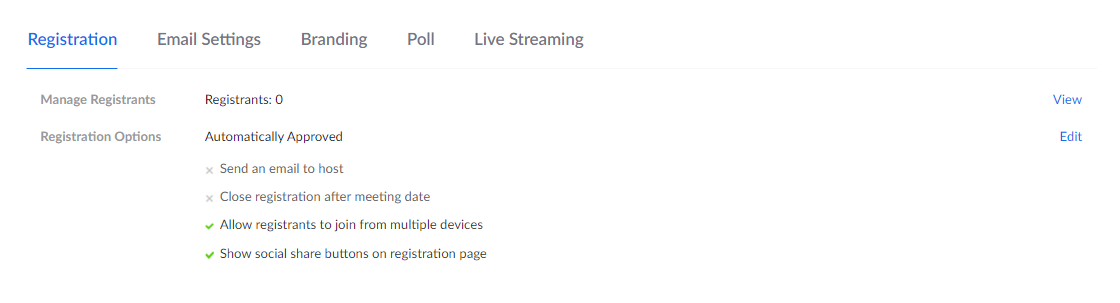
It is best practice to require Registration for your Meeting or Webinar. This provides increased security by providing the host the opportunity to vet the participant in advance.

To incorporate Registration to your Meeting or Webinar:

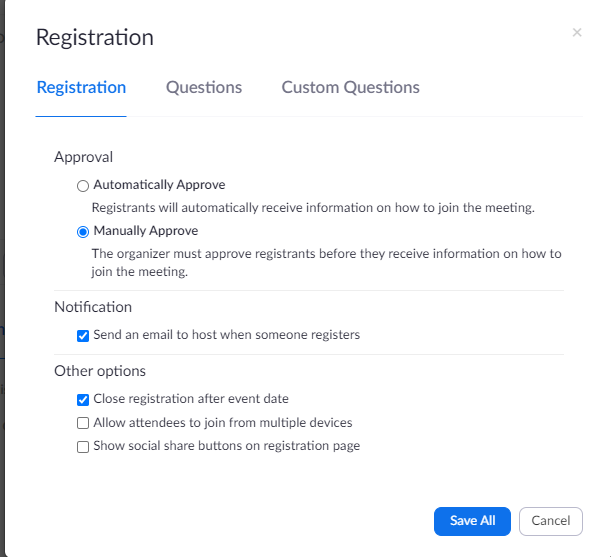
1. Log in to zoom.psu.edu
2. Select **Schedule a Meeting** or **Schedule a Webinar**
3. Begin to fill in the details of your event.
4. When you get to the Registration option, click on the Required checkbox to enable Registration.****
5. Continue with the rest of your Meeting or Webinar setup.
6. When the Meeting or Webinar is generated, the **Registration Link** will be generated along with an Invitation.

****

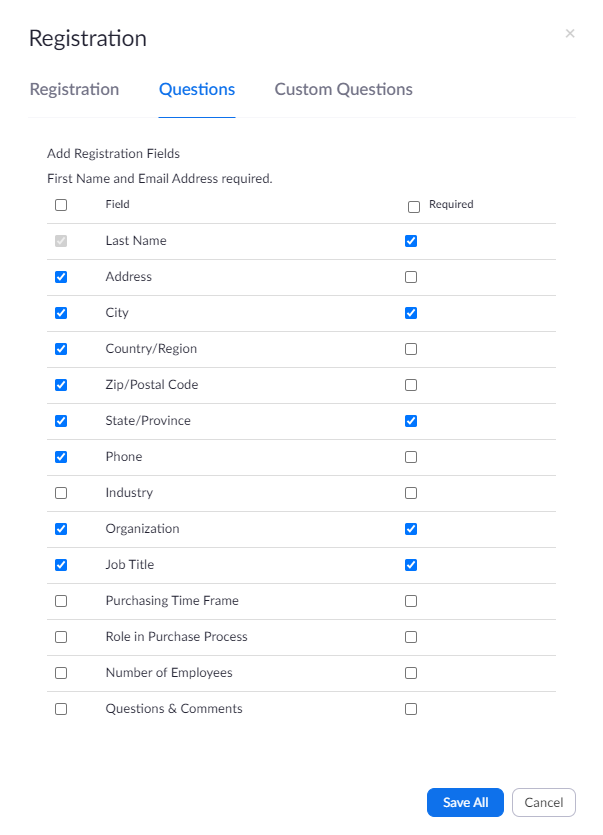
1. Scroll to the bottom of the Meeting or Webinar details. Select Edit to change the Registration options.

****

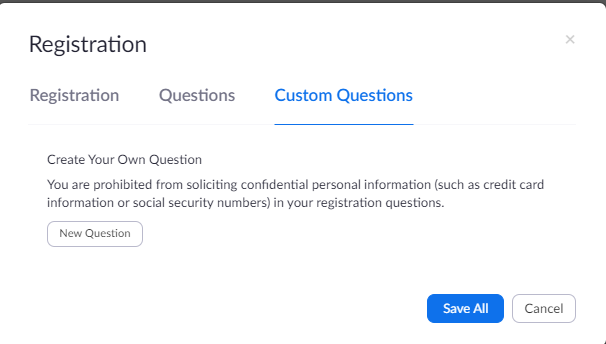
1. **Registration**. The default is to Automatically Approve a Registration. It is better practice to Manually approve if the event is small enough to vet each registrant. An email can be sent to notify the host when someone registers. Set the options for your Meeting/Webinar.

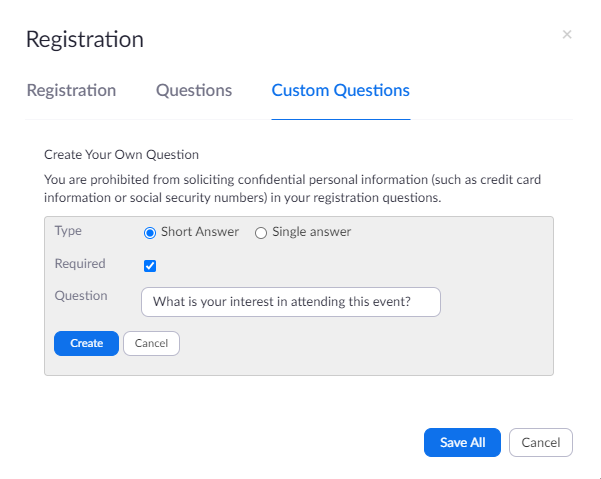
****

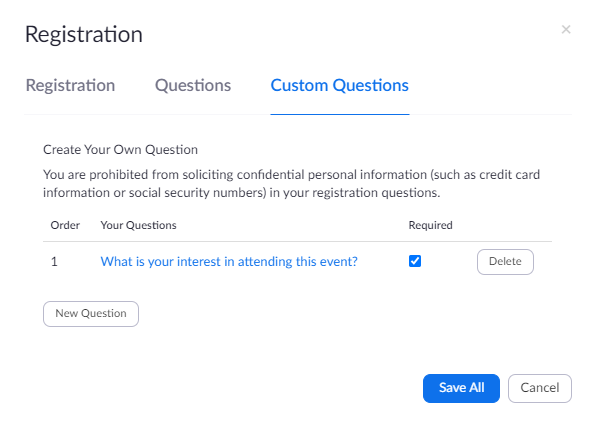
1. Click **Save All** after editing options.
2. **Questions**. The default requires only the completion of the Last Name. It is better practice to include more fields, some or all Required. This gathers more information from the registrant to use when vetting.

****

1. Click **Save All** after editing options.
2. **Custom Questions**. You may choose to create one or more Custom Questions to ask of your registrants. One such question could be ‘What is your interest in attending this event?’ Click New Question to add a question. Design your question. Click Create.

****

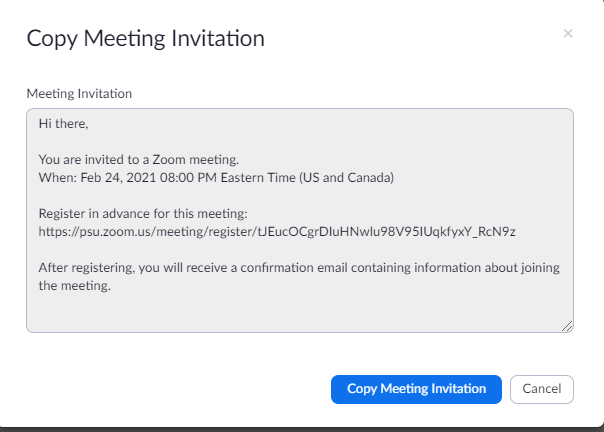
****

****

1. Click **Save All** when you have created your question(s).
2. When you have completed the Registration details, you can post the **Registration Link** on social media or send and invitation to target audiences. The Meeting/Webinar link and password will be automatically sent to approved registrants. **Never post the actual Meeting/Webinar link or password** on social media.

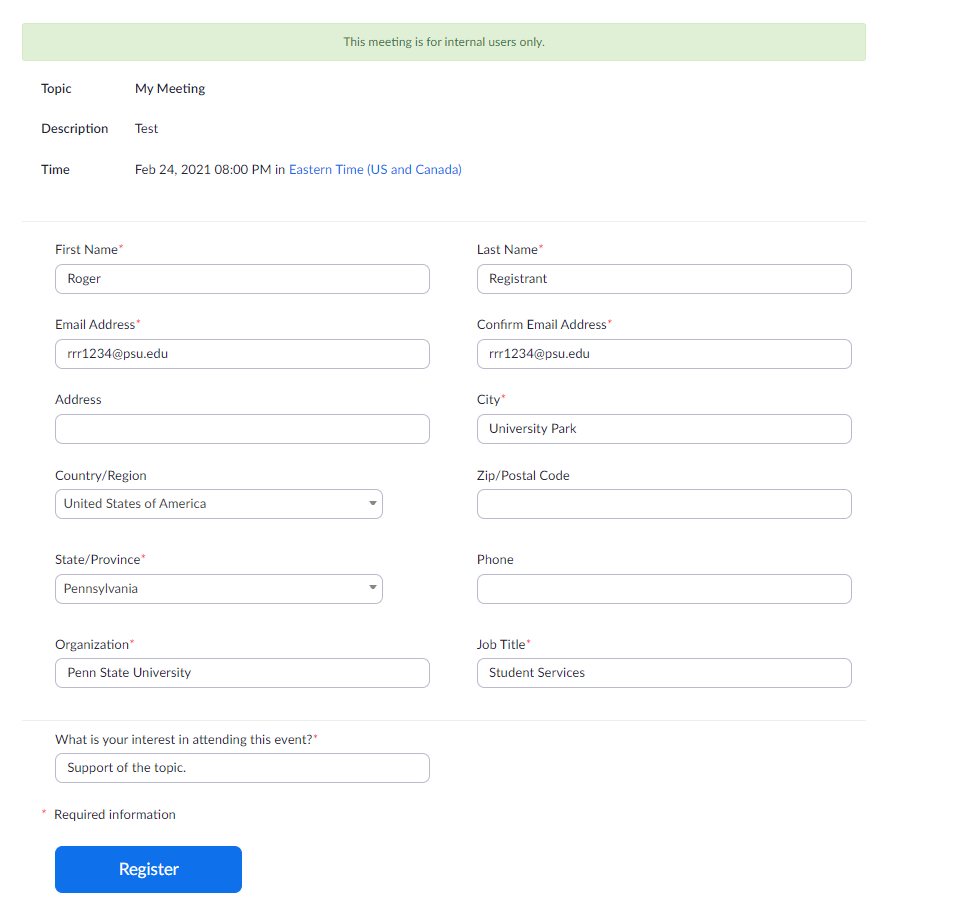
****

1. You can send an invitation to target audiences. The ‘Copy Invitation’ feature auto-generates an invitation. You can compose your own version.

****

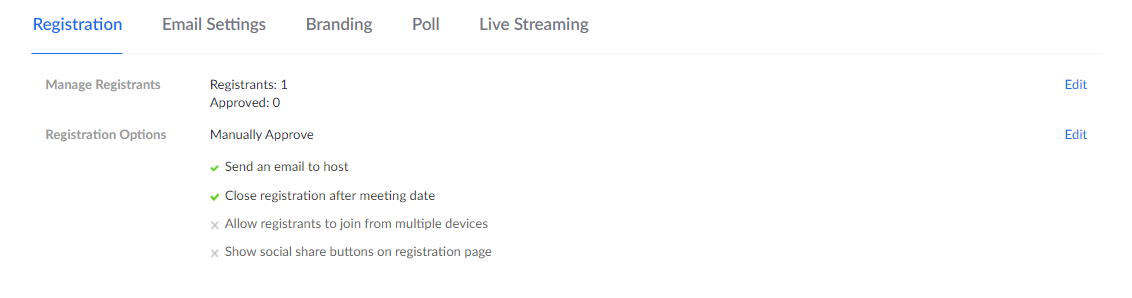
### Registration Process

The registration link directs to a form that contains the fields selected on the Meeting/Webinar Registration setup. Note that this Meeting requires authentication to join. This is indicated to the registrant with the ‘This meeting is for internal users only.’ bar.

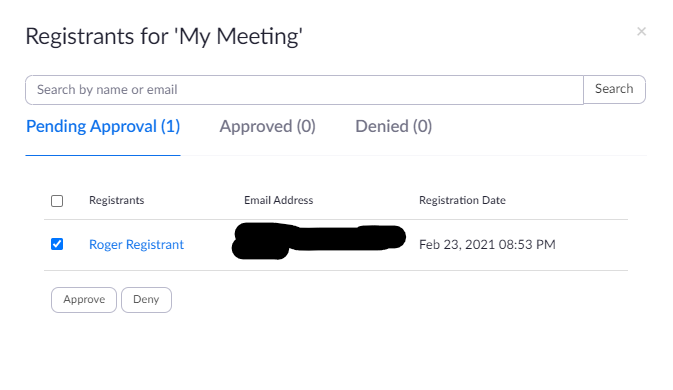


The interested registrant will complete the fields and click on Register. The email address will be validated by Zoom during this registration process. If the email address provided is not registered as a Zoom account, a link to the opportunity to Sign Up is provided. If the Meeting/Webinar is restricted to Penn State participants, a Penn State email address must be entered. reCAPTCHA is used to verify that the registrant is not a robot. Clicking on Register will then send the registration request to the Meeting/Webinar host.

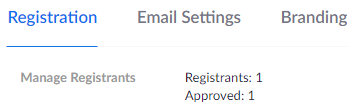
* The host will receive an email notification if that option was enabled.
* Log into psu.zoom.us and scroll to the bottom of the meeting to the Registration section.
* Note that there is 1 Registrant and 0 Approved Registrants in the example below.

****

Click on Edit to **Manage Registrants**.

****

Select a Registrant from the list and Approve or Deny accordingly. If approved the Registrant will receive an email with the Meeting/Webinar connection information. The link is unique to the Registrant and cannot be used by another. The Registrant can cancel their Registration at any time.

****