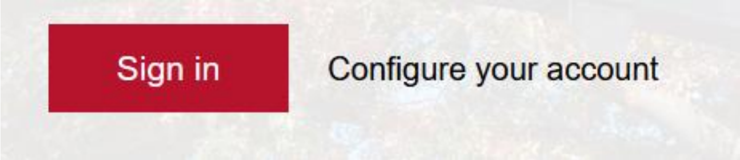
Bloustein School Faculty/Staff Zoom Security Recommendations

Zoom has had problems with intruders barging into meetings and disrupting them in various ways. These attacks are referred to as Zoombombing. If you are using Zoom, it is important that you utilize certain settings to ensure that your meetings remain secure. It should be noted that even with the best security in place, it is still possible that you could encounter an intrusion and you should have a plan in place that you communicate to your students. For example, you could let your students know that if an intrusion does take place, that you will end the meeting immediately and post new meeting information in Canvas to resume the class.

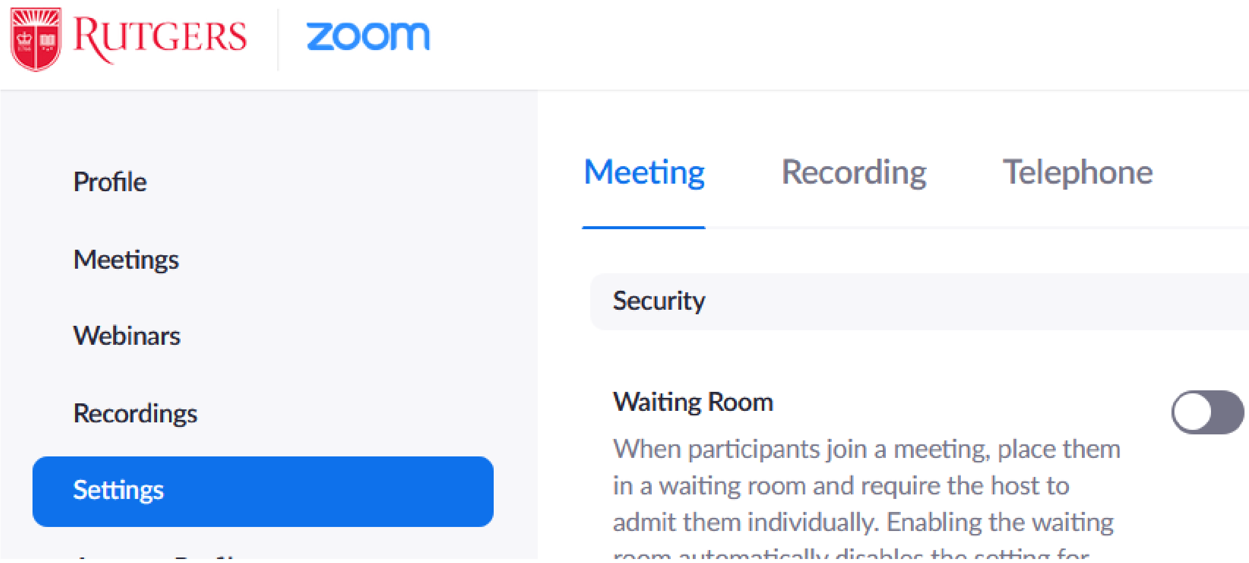
It is important to note that there are pre-meeting settings and in-meeting settings and both can be used to help you keep your meetings secure. A good overview of the security you can use in Zoom can be found here:

Best Practices for Securing your Zoom Meetings

We also have specific guidance on changing certain settings in your profile. The settings for your profile can be found by logging into https://rutgers.zoom.us and use the sign in option to configure your account.



You can then go to the settings option on the left and that will bring you to the meeting settings area.

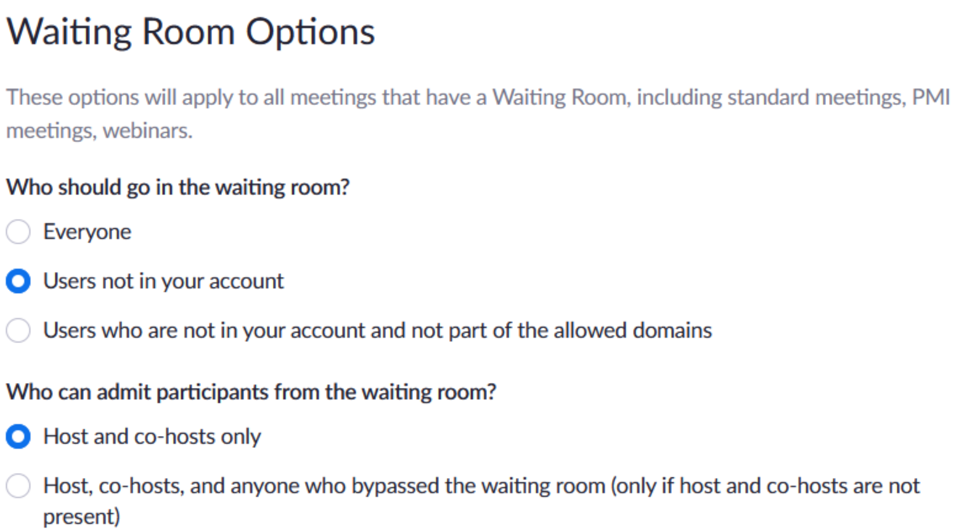


Waiting Room

When participants join a meeting, place them in a waiting room and require the host to admit them individually. Enabling the waiting room automatically disables the setting for

Waiting Rooms

Using the waiting room is a great way to maintain security for your sessions. However, this will require that you admit participants, and this may not be practical based on your class size. However, one way you can use waiting rooms effectively would be to turn it on and change the Waiting Room Options to reflect the following:



Waiting Room Options

These options will apply to all meetings that have a Waiting Room, including standard meetings, PMI meetings, webinars.

Who should go in the waiting room?

○ Everyone

● Users not in your account

○ Users who are not in your account and not part of the allowed domains

Who can admit participants from the waiting room?

● Host and co-hosts only

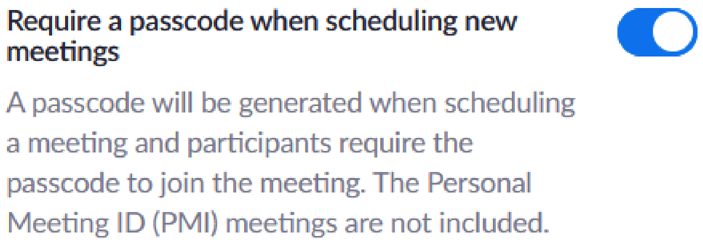
○ Host, co-hosts, and anyone who bypassed the waiting room (only if host and co-hosts are not present)

Please note that this will require that users login using their Rutgers credentials for your meetings. If any users access your meeting without logging in with their Rutgers credentials.

Please review this video for additional information on waiting rooms: https://support.zoom.us/hc/en-us/articles/115000332726-Waiting-Room

Passcode Protected Meetings

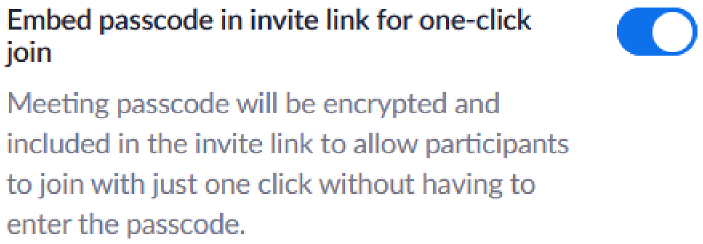
By default, a passcode is generated for your meetings and you should leave this setting intact. Using passcodes for your meetings is one of the best ways to secure your meetings.



Require a passcode when scheduling new meetings

A passcode will be generated when scheduling a meeting and participants require the passcode to join the meeting. The Personal Meeting ID (PMI) meetings are not included.

It is important to note that another default setting related to passcodes is the Embed passcode in invite link for one-click join, which is also enabled by default.



Embed passcode in invite link for one-click join

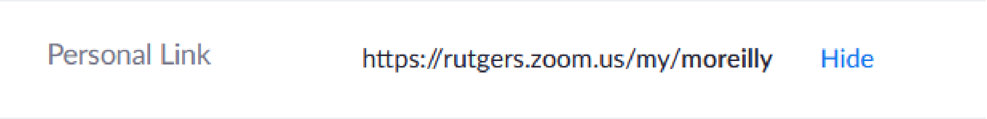
Meeting passcode will be encrypted and included in the invite link to allow participants to join with just one click without having to enter the passcode.

When you schedule a meeting, the invite link will embed the necessary passcode so that participants do not need to enter it. Using this feature is convenient for participants, but your invitation needs to be kept private for your meeting to remain secure. You should not post the meeting invite on any public sites. Posting the information in Canvas is the best way to securely promote your class sessions if you use embedded passcodes.

Personal Meeting Rooms

Your personal meeting room in Zoom is a convenient way to have instant meetings and to hold office hours. However, you should try to limit the use of your personal meeting rooms as much as possible and you should never use your personal meeting room for a class session.

The default address for your personal meeting room is https://rutgers.zoom.us/my/netid , where netid is your NetID. You can confirm the address to your personal room by going to profile and confirming your "Personal Link":



Personal Link https://rutgers.zoom.us/my/moreilly

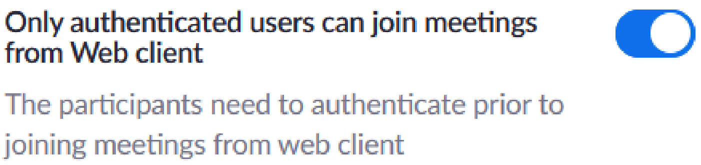
Personal Meeting Rooms requires a passcode for participants. You can change that passcode under settings in the meeting tab under the "Require a passcode for personal Meeting ID (PMI)". In that area,
click on the pencil icon next to your existing passcode to change it:

✎

Your passcode can be up to 10 characters and we recommend using a 10-character password that includes upper- and lower-case letters as well as numbers and punctuation. You should also change this password regularly to keep your personal meeting room secure.

Require Participants to Authenticate

Another helpful security setting is related to only allowing authenticated users to join meetings. This option is set by default, but you should also enable the same setting for participants who use the web client.



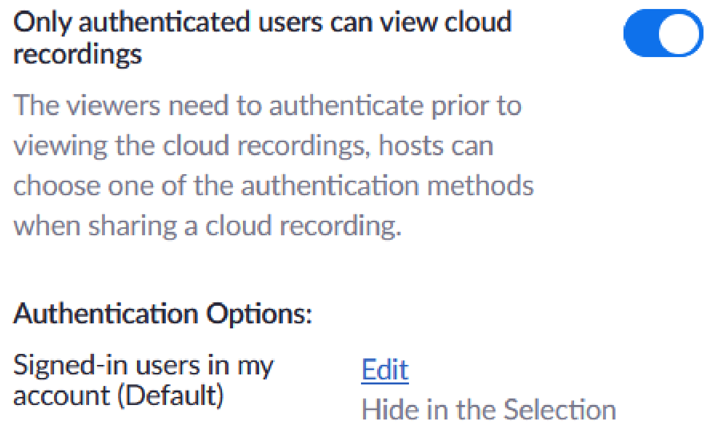
Only authenticated users can join meetings from Web client

The participants need to authenticate prior to joining meetings from web client

The settings area has many customizations and preferences that you can change. Some other important settings that may be of interest include setting chat options, including personal chats between students, limiting who can annotate, and muting participants upon entry. You can change these settings during a meeting, but if you want to have certain default settings, you should change those in your settings area.

Securing Cloud Recordings

Any class sessions that are recorded should be uploaded to Canvas. If you need guidance on how to do that, please see this link . If you are using Zoom for other meetings and plan on using the cloud recording option, please be aware that there have been many recorded Zoom meetings that have been accessed by unintended viewers. To secure such recordings, you can update default recording preferences in the Recording tab of settings. One setting we recommend you change is for Only allowing authenticated users to view cloud recordings. We recommend enabling that option.



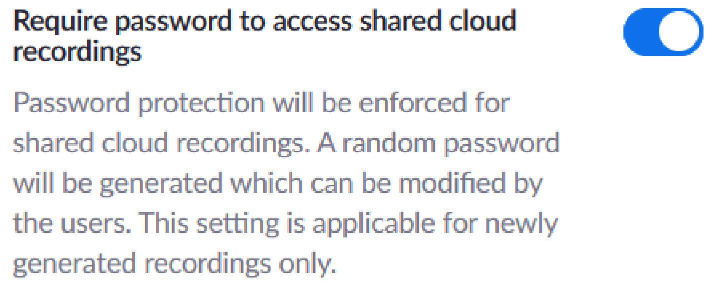
Only authenticated users can view cloud recordings ●

The viewers need to authenticate prior to viewing the cloud recordings, hosts can choose one of the authentication methods when sharing a cloud recording.

Authentication Options:

Signed-in users in my account (Default) Edit Hide in the Selection

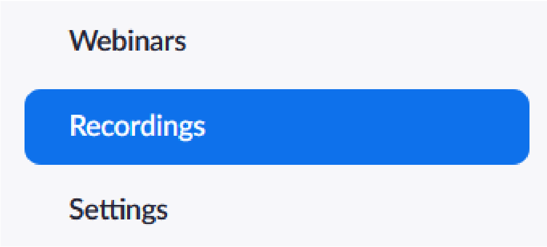
You should also leave the option on for requiring passwords for accessing shared cloud recordings:



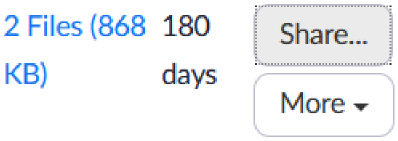
Require password to access shared cloud recordings ●

Password protection will be enforced for shared cloud recordings. A random password will be generated which can be modified by the users. This setting is applicable for newly generated recordings only.

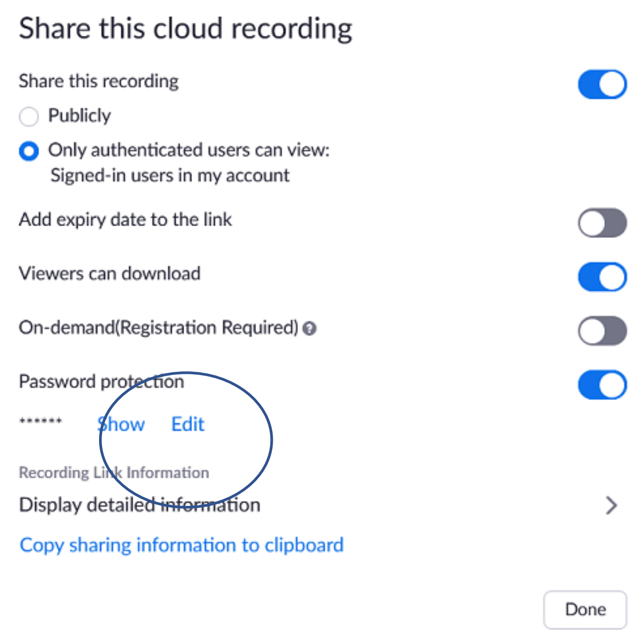
After a recording is processed, you will find it in the Recordings area:



You can then set options for sharing your recording using the Share button next to the recording entry:



Another thing you can do to improve the security of your recording is to improve the strength of the password protecting it. The default option is 8 characters, but you can make a much stronger password. To do that click on the edit option next to the password:



Share this cloud recording

Share this recording ☑

○ Publicly

● Only authenticated users can view:
Signed-in users in my account

Add expiry date to the link ☐

Viewers can download ☑

On-demand(Registration Required) ☐

Password protection ☑

****** Show Edit

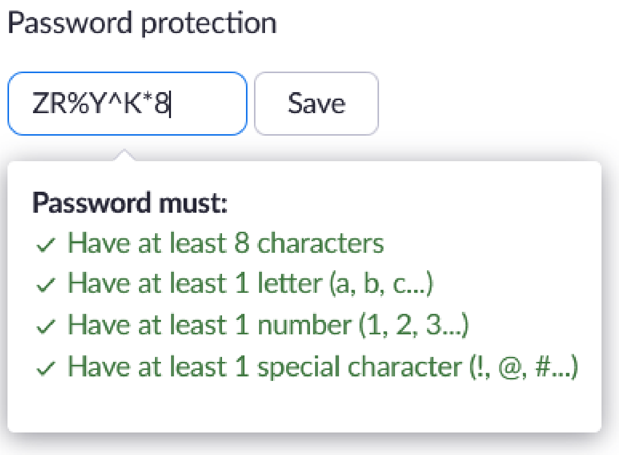
Recording Link Information

Display detailed information >

Copy sharing information to clipboard

Done

You can then change the randomly generated password of 8 characters to a password that is up to 64 characters long.



Password protection

ZR%Y^K*8 Save

Password must:

- ✓ Have at least 8 characters
- ✓ Have at least 1 letter (a, b, c...)
- ✓ Have at least 1 number (1, 2, 3...)
- ✓ Have at least 1 special character (!, @, #...)

The following site has a random password generator that allows you to specify the length of a password and then easily copy and paste it into Zoom to enhance the security of your recordings:

https://www.lastpass.com/password-generator
*Please note that we are not promoting lastpass although we do feel it is a solid product.

After updating the password for your recording, you can copy the sharing information to the clipboard and then post the information in Canvas.

Copy sharing information to clipboard

If you have questions about this information, or have other questions about using Zoom, please contact us at help@ejb.rutgers.edu.