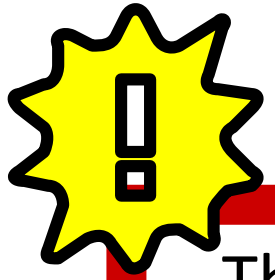
- Extra edition -

Strengthened Security Settings for Zoom

If you host a meeting, please confirm this manual carefully.

Ritsumeikan Asia Pacific University, ver.1_2020.4.9



The information contained in this document is designed to help prevent intrusions from malicious third parties via Zoom (Zoombombing) by strengthening Zoom's built-in security settings.

Please read this information carefully and make sure to choose the appropriate settings for any of your meetings.

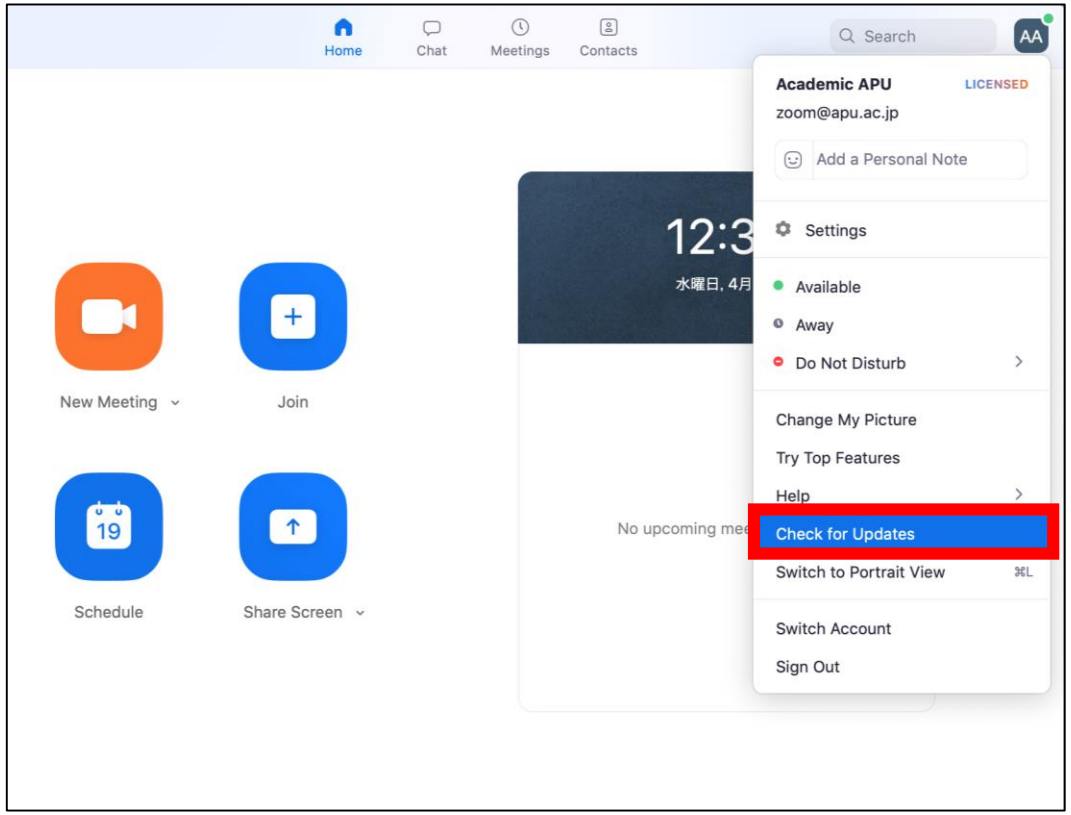
※Zoom is strengthening its security measures, so please be aware that some functions may become restricted or removed without warning.

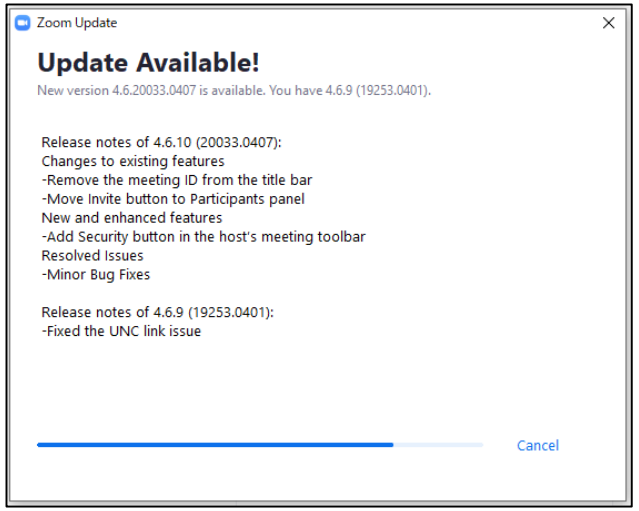
【PART 1】
Required Settings

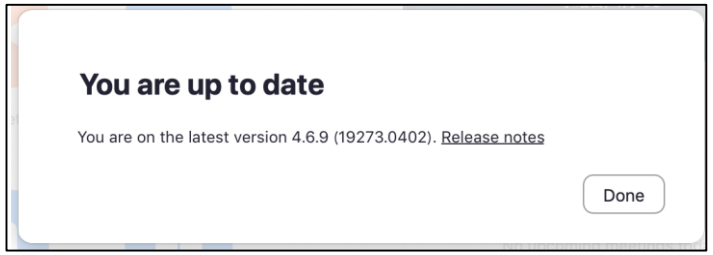
Keep Zoom Updated

Update Zoom whenever you see an Update Available Notification

Zoom

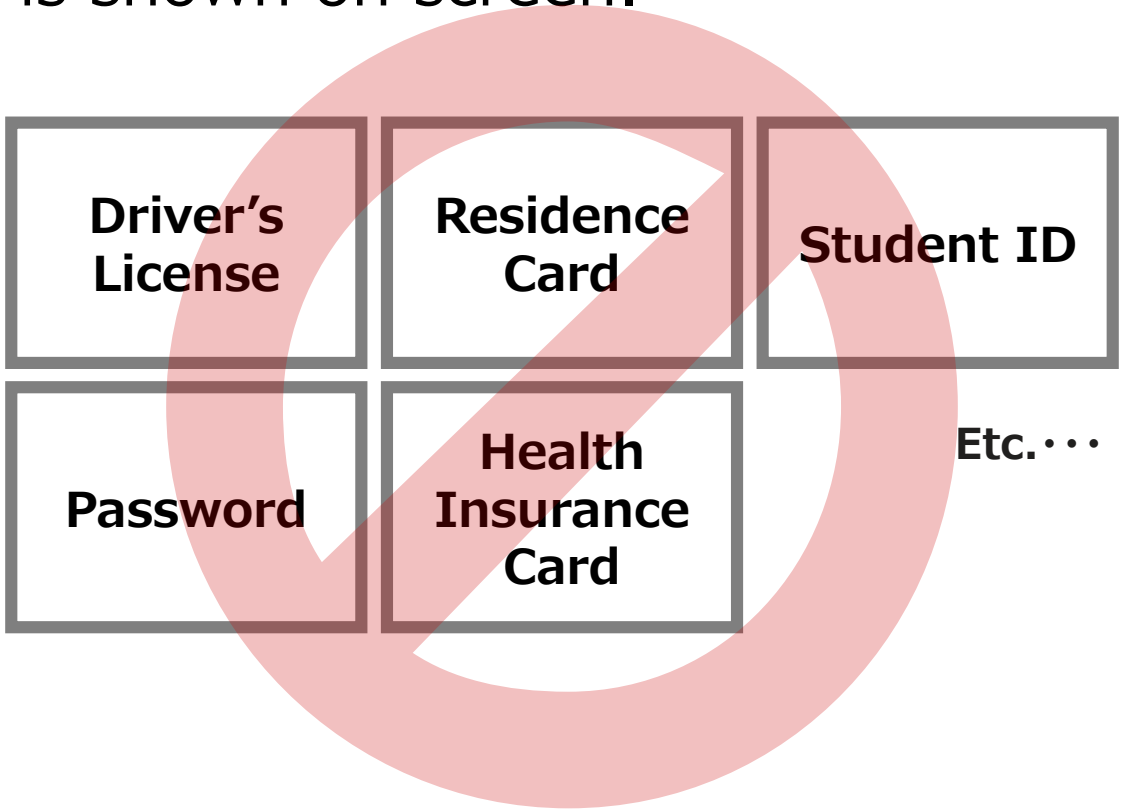






Don’t Share Personal Information

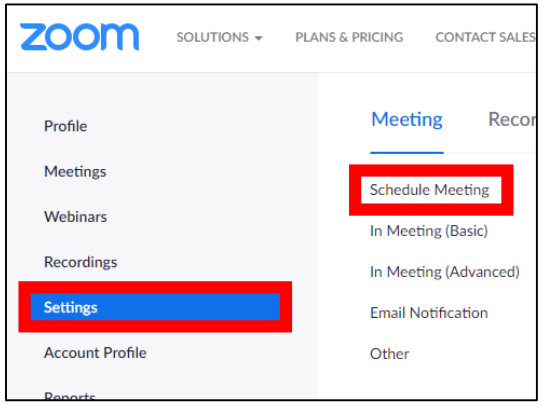
Don’t share personal information. If you need to check ID for an interview or consultation, turn on Video and check using information that would only be known by the person in question. When screensharing, make sure no personal information is shown on screen.

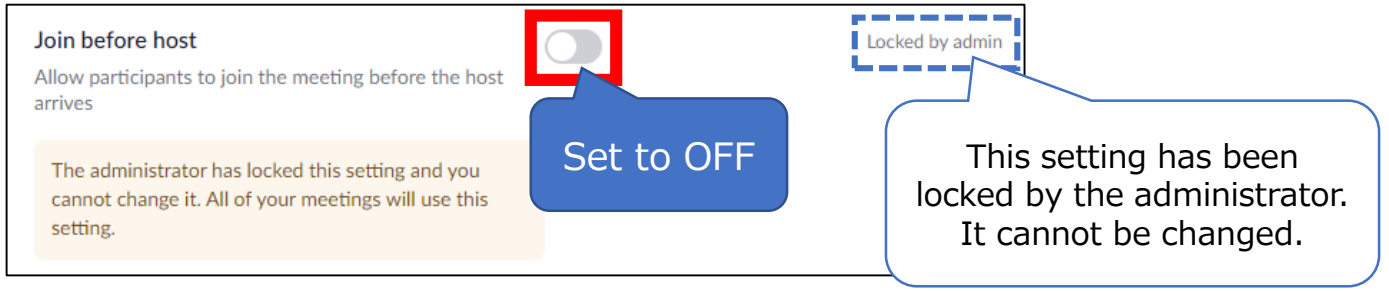


Disable [Join Before Host]

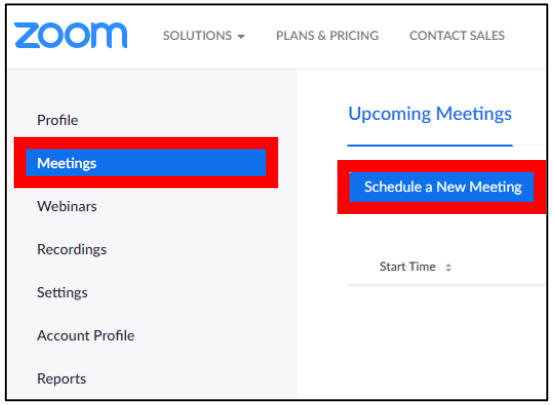
Disable join before host to prevent hijacking before you start the class.
(※This function has been locked by the administrator for all users.)

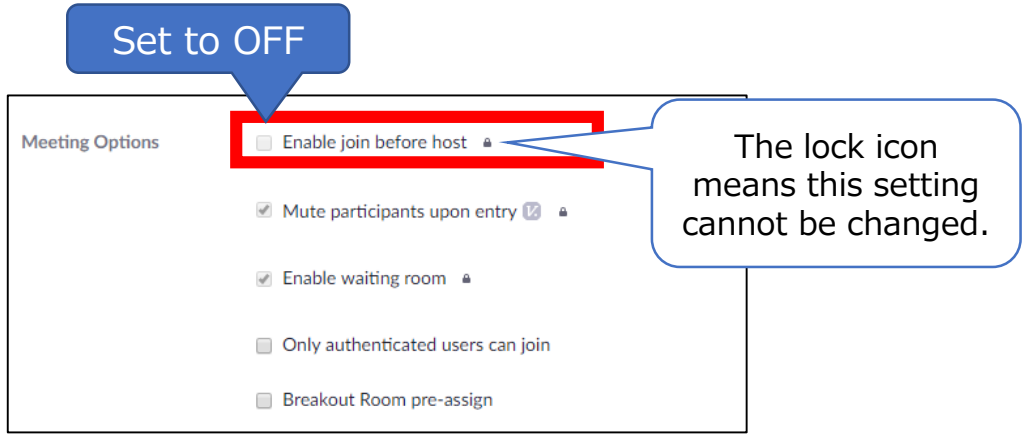
1.Check Settings





2. When Scheduling Meetings





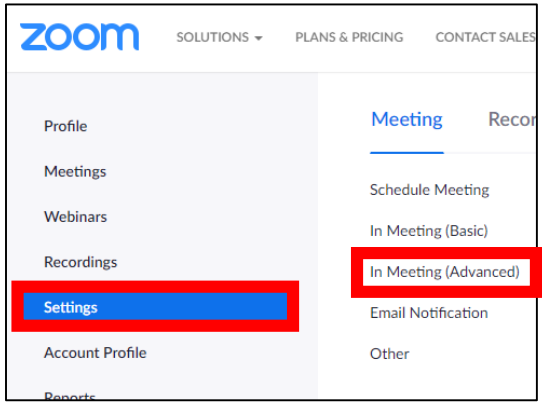
Set [Waiting Room] to ON

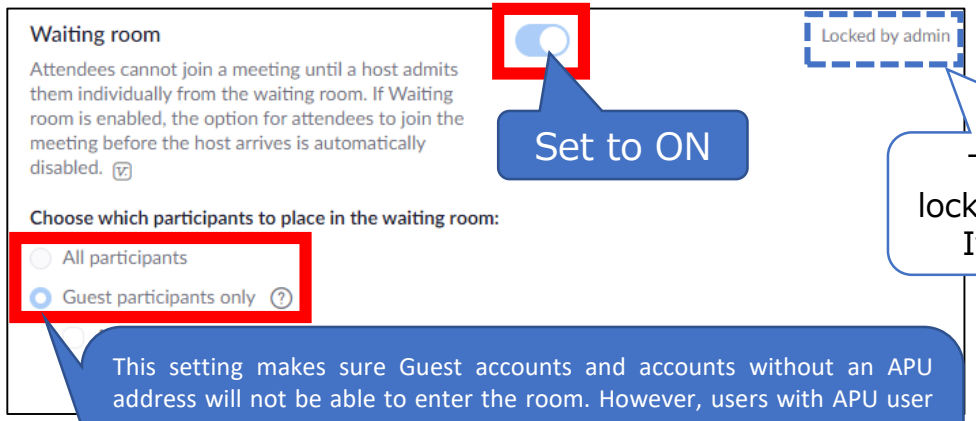
(※This function has been locked by the administrator for all users.)

With this setting, only users you choose will be allowed to enter the room.

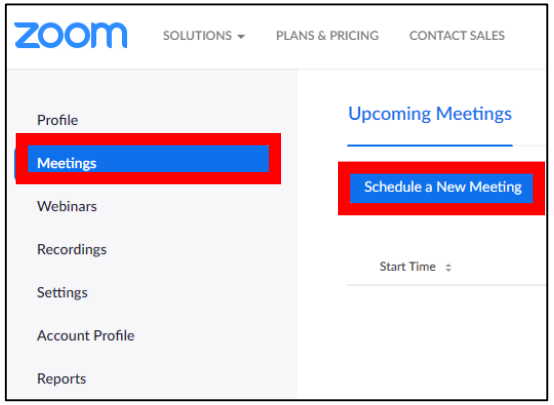
(Note) This is also a useful function for holding individual meetings or consultations.

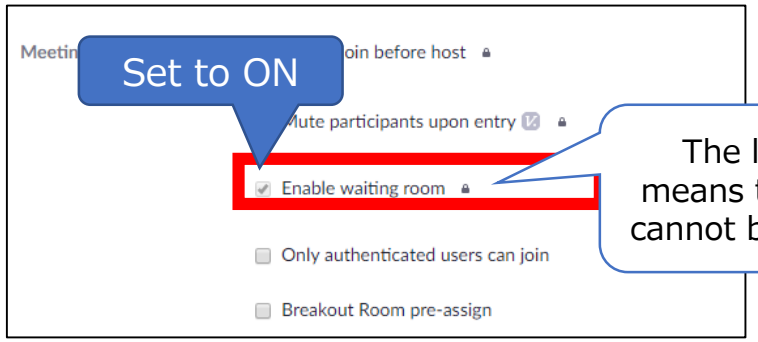
1.Check Settings





2. When Scheduling Meetings

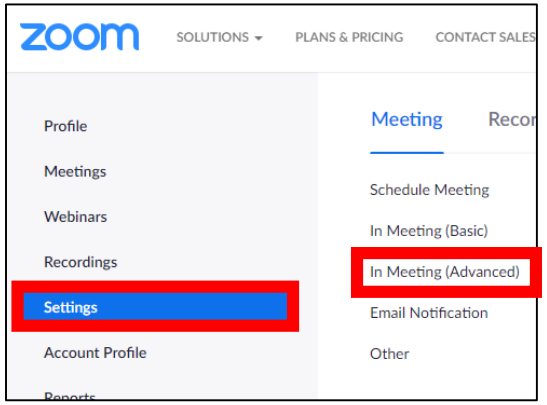


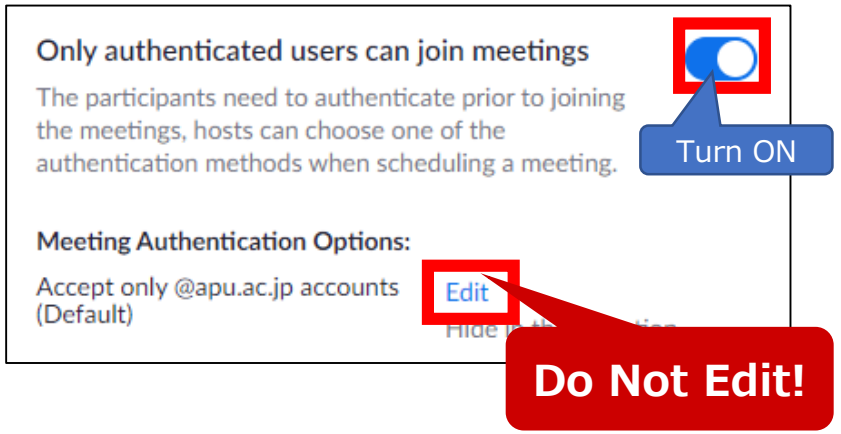


Set [Authentication] to ON

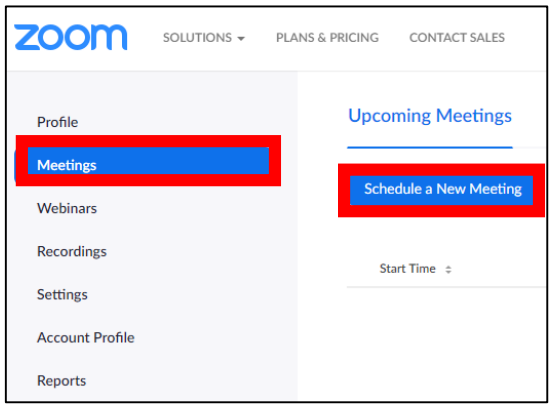
Always turn authentication ON and restrict access to “apu.ac.jp” accounts only.

1.Check Settings





2. When Scheduling Meetings



[NOTE]

This setting permits only signed-in users with APU email addresses to join the room. This is **A VERY IMPORTANT SETTING, and if you do not turn this on then security will be severely reduced,** so please check it carefully.

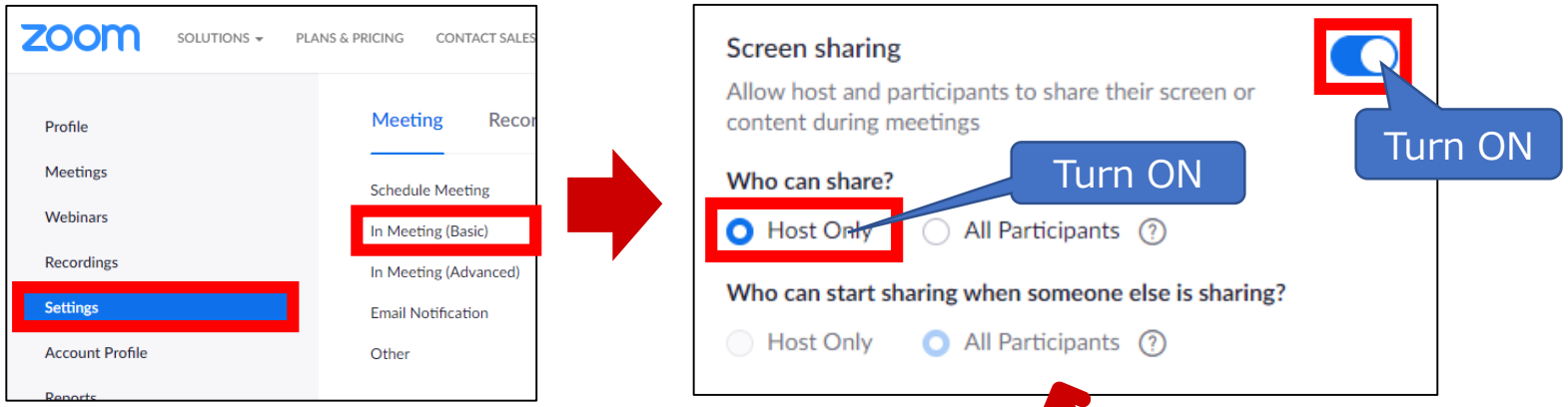
[The Only Exception]

In some cases it may be necessary to allow non-APU account holders to join. ONLY in such cases is it acceptable to turn this to Off. However, in such cases it is recommended to ① Pre-register and ② require a Password.

Set Screensharing To [HOST ONLY]

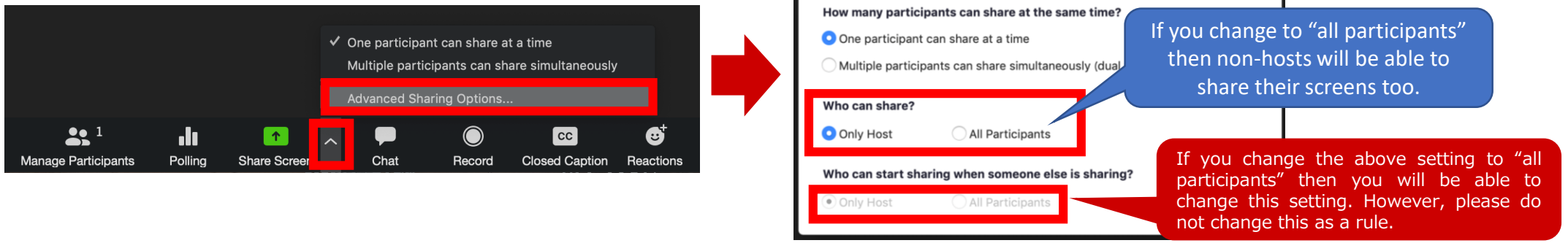
Do not allow everyone to share their screen when there are many students present. Only allow the host to screenshare during the meeting.

1.Check Settings



Same Settings

2. When Scheduling Meetings

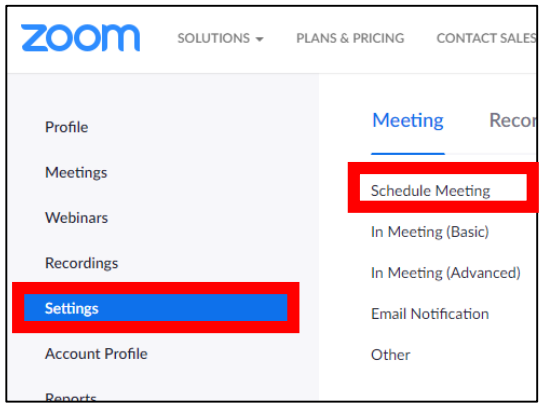


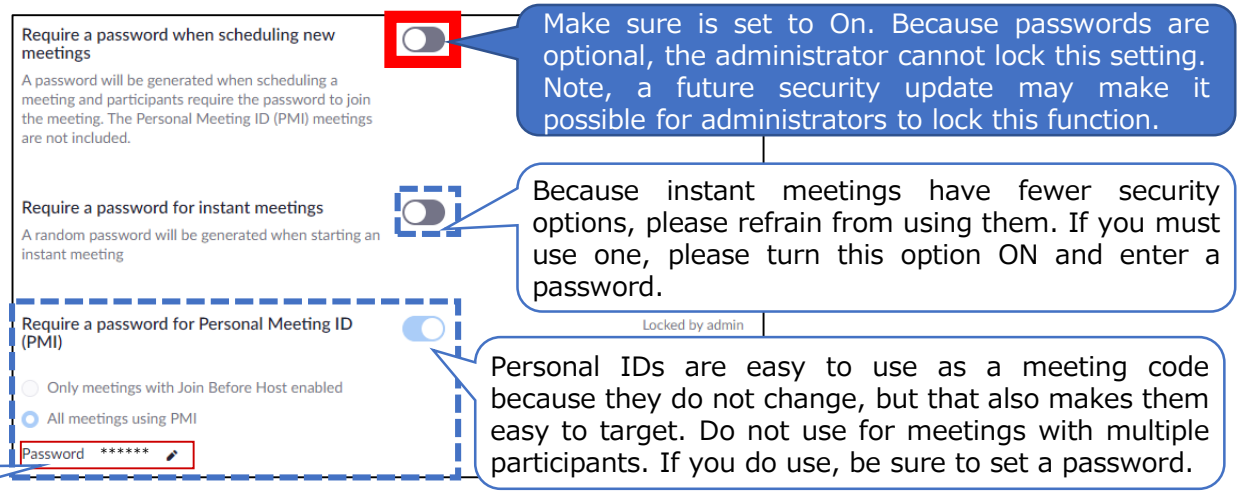
【PART 2】
Strongly Recommended Settings

Use A [Meeting Password]

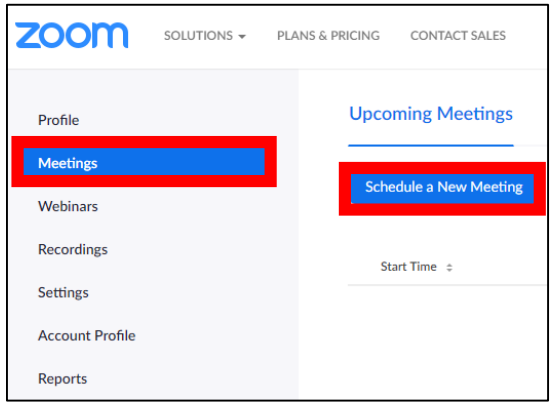
We strongly recommend you set a meeting password.
Users who do not know the password cannot enter the room, and even if the password leaks they will have to take the time to enter it.

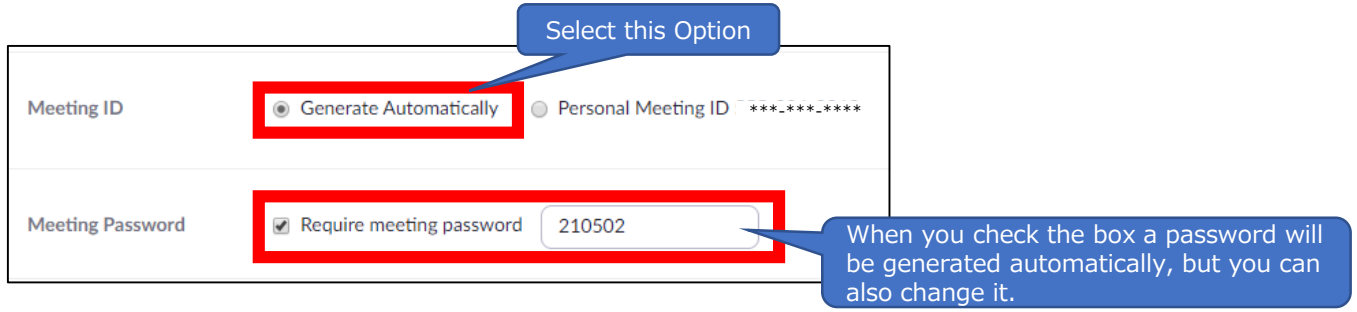
1.Check Settings





2. When Scheduling Meetings

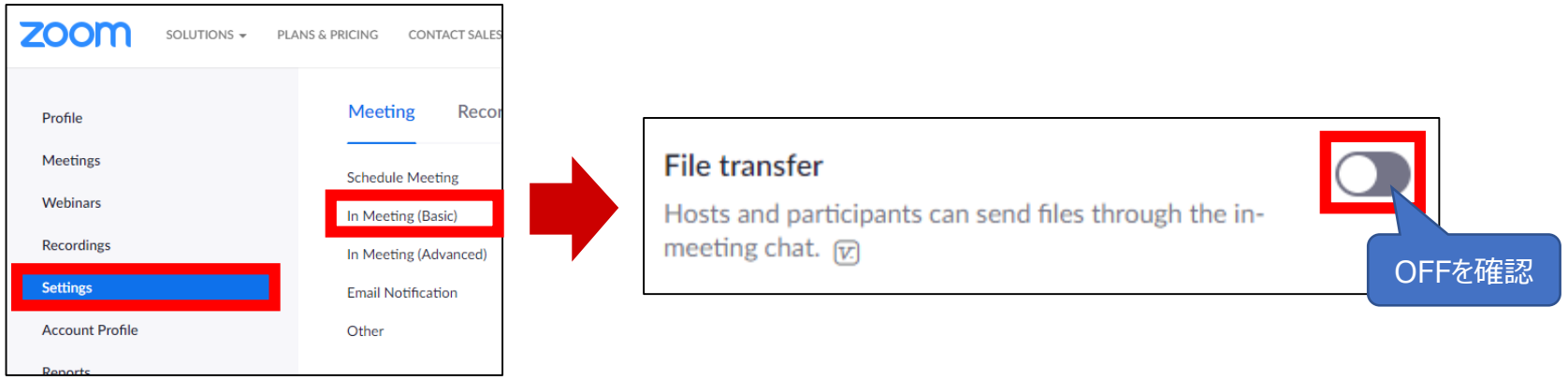




Turn OFF [File Transfer]

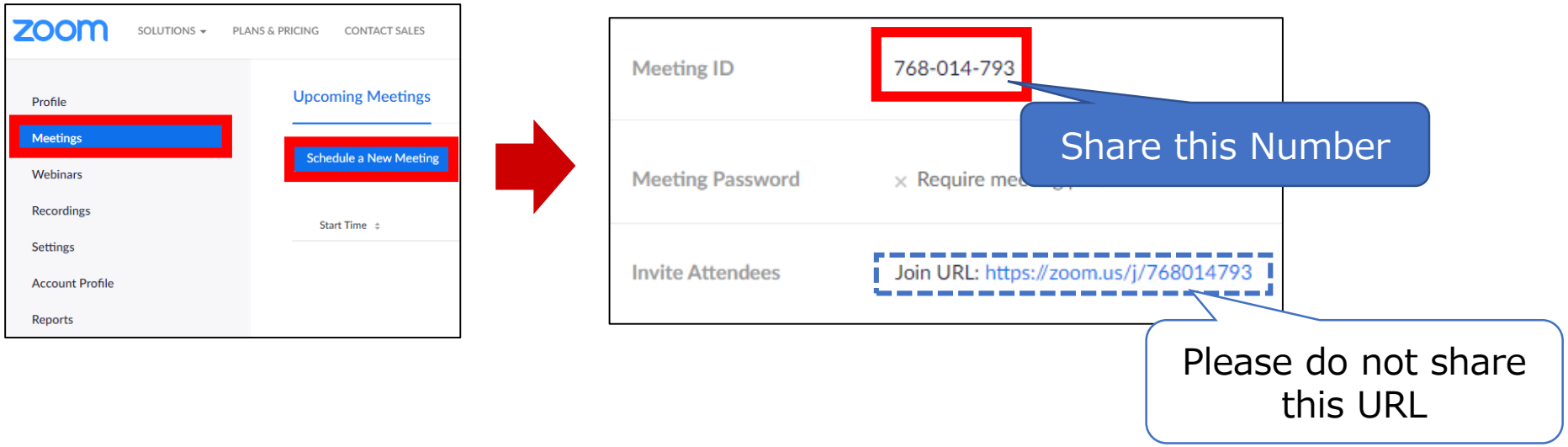
The file transfer option in Chat is useful, but there is the risk of malicious files being shared. NOTE, files can only be received by PCs, and cannot be received by tablets or smartphones.

In addition, it is also possible to use the chat function to send URLs that seem official but actually link to phishing sites. Please do not share or click on unnecessary URLs.



Invite via Meeting IDs instead of URLs

Meeting URLs are convenient because participants can join with one click. However, if you invite via Meeting ID then it increases the time/effort required by third parties to join. Also, please do not click unfamiliar meeting URLs or enter Meeting IDs from unknown sources.

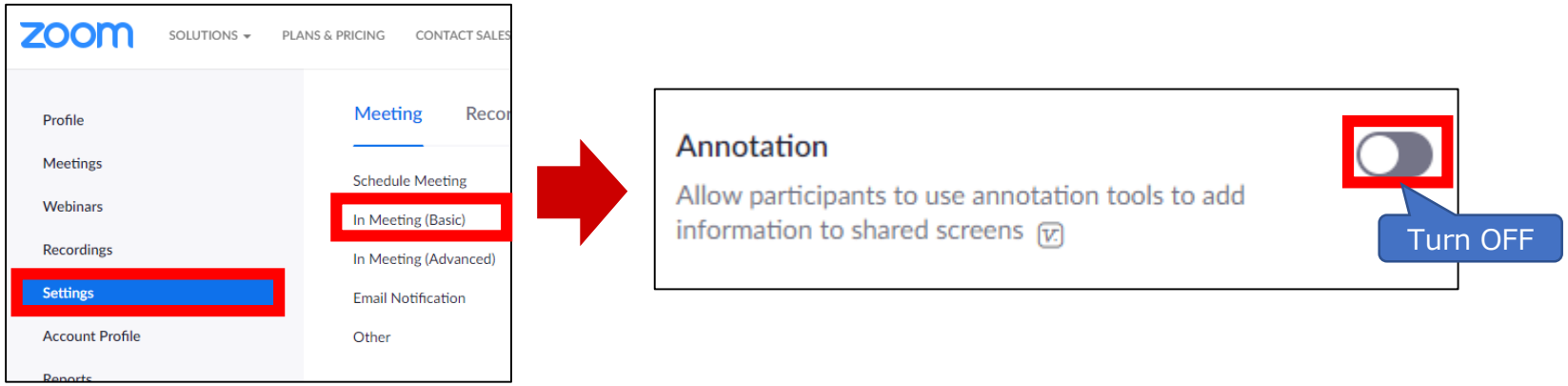


【PART 3】
Other Settings

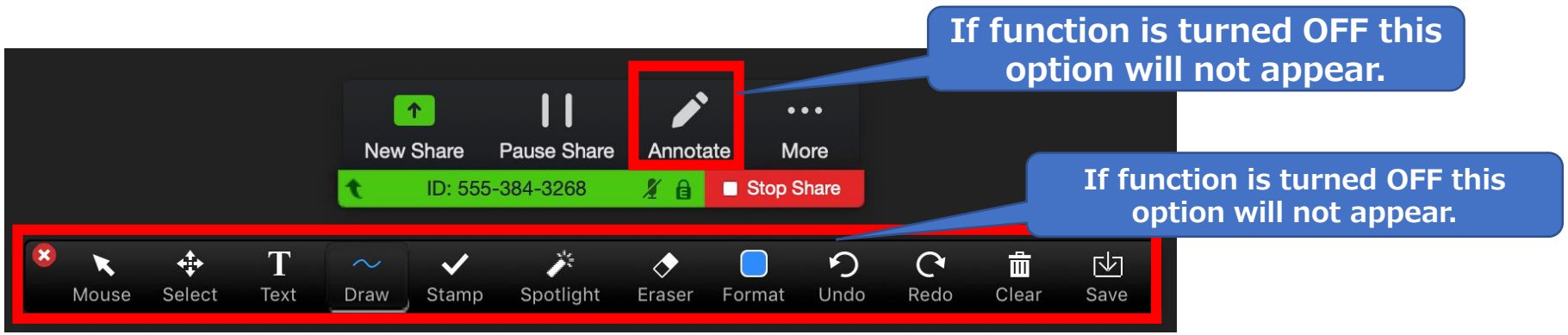
Turn Off [Annotations]

Screen Sharing function has a useful option to allow participants to write on the screen. However, this can also lead to disruptive behavior, so we recommend turning this off.

1.Check Settings



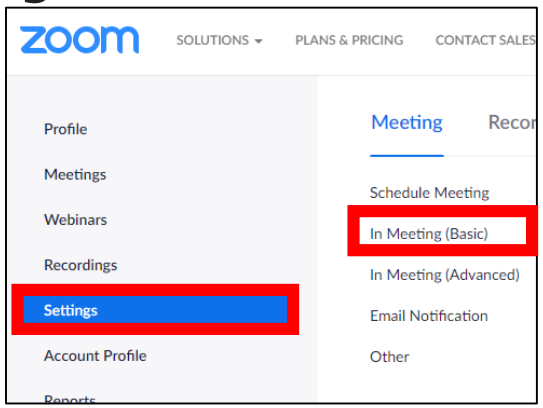
2. When Scheduling Meetings

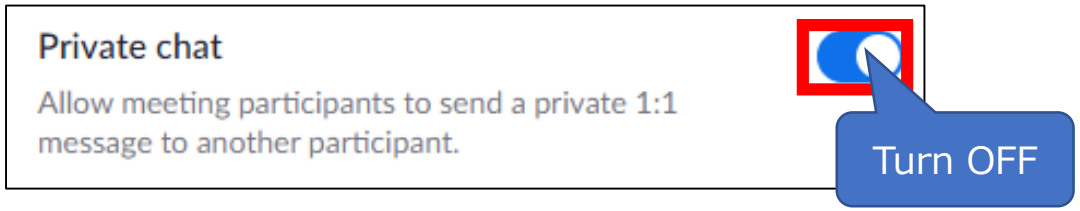


Turn Off [Private Chat]

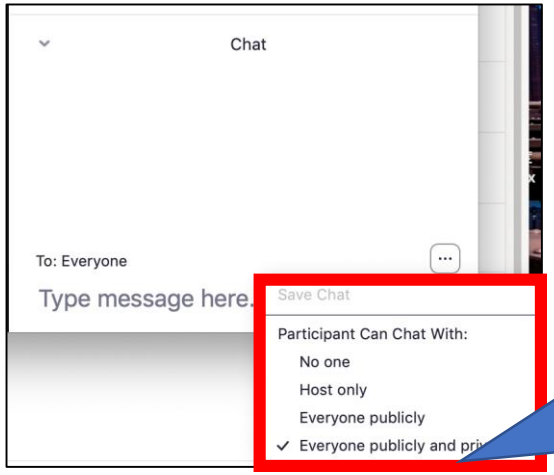
The Private Chat function allows participants to chat privately amongst themselves. It is useful, but we recommend disabling it because participants can to talk to each other during class.

1.Check Settings





2. When Scheduling Meetings



You can also choose these options to selectively disable the function:

1. No one – Completely disables the chat function. The Host can still chat to all participants (open) or send individual messages.
2. Host only – Participants can only send messages to the host.
3. Everyone publicly – Participants can send messages to the host or all participants (open) only.
4. Everyone publicly and privately – In addition to 3, participants can send each other private chats.