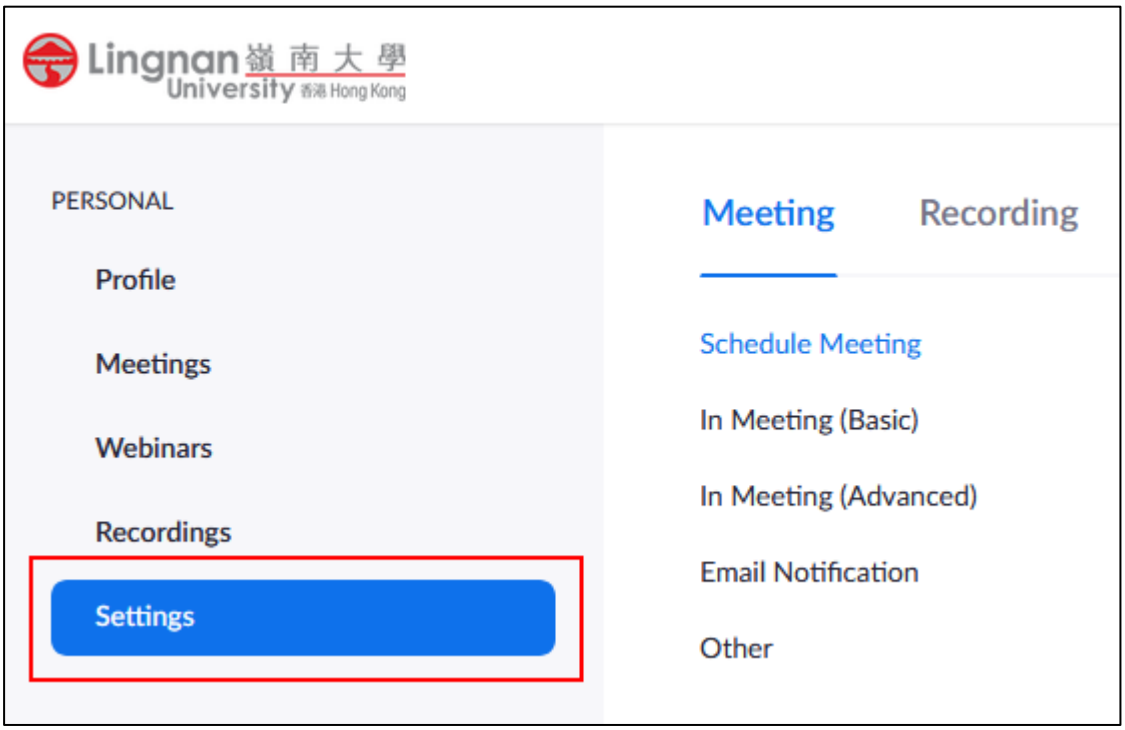
# Zoom Security Features Update

## Control Your Zoom Data Routing (For Hosts only)

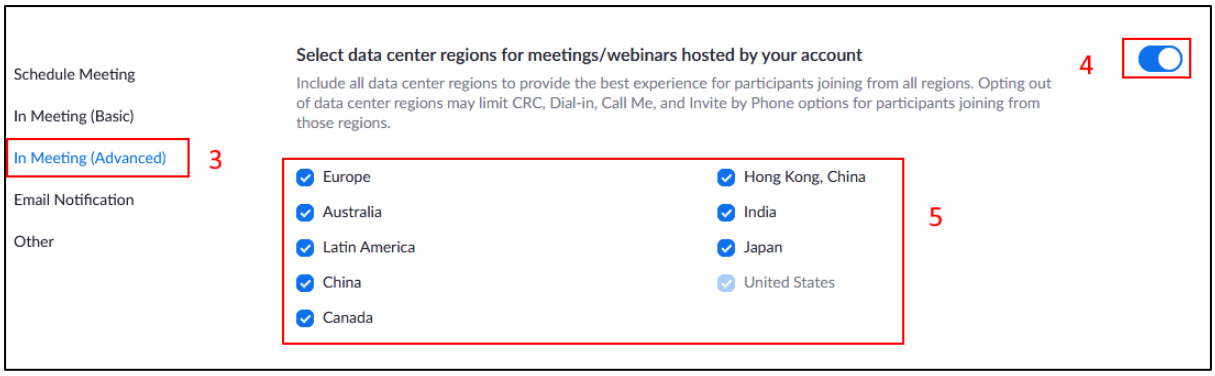
You can now opt in or out of a specific data center region for your meetings or Webinars. This will determine the meeting servers and Zoom connectors that can be used to connect to Zoom meetings or webinars you are hosting and ensure the best-quality service. You cannot opt out the “United States” as this is the region where Lingnan’s account is provisioned.

To customize data center routing for your own use:

1. Sign in to the Lingnan Zoom web portal (https://lingnan.zoom.us/signin)
2. In the navigation panel, click Settings.




3. Under In Meeting (Advanced), verify that “Select data center regions for meetings/webinars hosted by your account” is enabled.
4. If the setting is disabled, click the toggle to enable it. If a verification dialog displays, click Turn On to verify the change.
5. Check the regions that you would like your in-meeting and in-webinar data to route




Please note that:

1. If you opt-out the data center of a certain region, meeting experience of participants from that region may be affected.
2. Once you changed your personal data center settings, all the meetings you hosted in the future will be affected. Your data center settings will be suppressed by the host's preferences when you join a meeting as co-host or participant.

## Enhanced Security Settings

Following default settings has been applied

1. Enable Waiting room
2. Passwords are required for all type of meetings
3. The minimum length of meeting password is 8 characters long
4. Participant screen sharing was disabled
5. Only authenticated can join meetings was default enabled and set to “Authenticated Lingnan Users”
6. Join before host was default disabled

The following meeting settings are turned off for all users

1. In meeting File Transfer
2. Allow participants to rename themselves
3. “Join from your browser”, participants can only join a meeting using Zoom client
4. Domain contact visibility was disabled

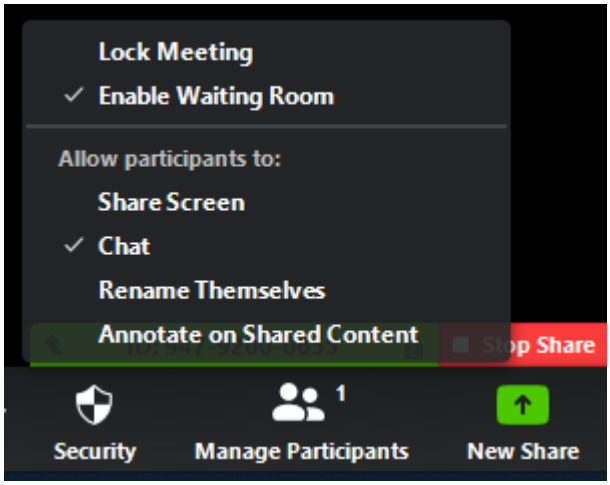
## In-meeting security options (For Hosts and Co-hosts)

The Security icon in the meeting controls allows the host or co-host (not participants) of a meeting to enable or disable options during a meeting to secure the meeting and minimize disruption during the meeting.

Latest version of Zoom client is required in order to display the Security icon.
To download the latest version of Zoom client, please visit:
https://lingnan.zoom.us/download

Available security settings are:

- Lock Meeting: Locks the meeting, keeping new participants from joining the meeting. Please note that if a participant leaves the meeting, he/she will not be able to join the meeting again.
- Enable Waiting Room: Enables Waiting Room for incoming new participants or to move current participants into the Waiting Room.
- Allow participants to:
    - Share Screen: Allows participants to start screen sharing (default disabled)
    - Chat: Allows participants to use the chat function (default enabled)
    - Rename Themselves: Allows participants to rename themselves from the Participants panel (default disabled)
    - Annotate on Shared Content: Allows participants to annotate over content shared during the meeting. The host can enable or disable annotation when the host is sharing (default disabled). This option is only visible during a screen sharing session.



## Security and Privacy Recommendations

1. Teachers should create online classes using the Moodle plugin directly, which avoid sending the meeting link via emails or put on publicly accessible places such as webpages or social media. For instructions, please refer to the user guide “Create a Zoom Online Class in Moodle”.
2. Only allow an authenticated user to join the meeting.
3. Enable the waiting room feature.
4. Avoid using Personal Meeting ID.
5. Always update your Zoom client to the latest version.
6. Meeting recordings should not upload to publicly accessible places.