Recommended settings for End Users and Hosts:

DPIA Zoom 2024

Version 2
Updated version after updateDPIA Zoom 2024
Version 1
DPIA Zoom 2022

Index

[1] Zoom, End-to-end (E2EE) encryption for meetings, last updated 28 February 2024, URL: https://support.zoom.us/hc/en-us/articles/360048660871-End-to-end-E2EE-encryption-for-meetings.

1. Privacy controls for end users and hosts

End Users & Hosts of Zoom Meetings can exercise control and influence data processing by Zoom in many ways. This document will describe several settings and how users and hosts may adjust these settings and minimize the data processing by Zoom. These 5 options are:

1. limiting push messages in the Zoom app on the mobile phone
2. limiting the processing purposes when creating a Zoom account
3. limiting the exchange of personal data when they host a Meeting
4. blocking participants from third countries when they host a Meeting
5. limiting visibility of their personal data to other participants when they participate in a Meeting

Some of these privacy choices depend on settings determined by the administrator. The options for administrators are discussed "Recommended Settings for Admins – DPIA Zoom 2024". If the end user or host can choices, it is up to them to disable or enable. Most of the times it is a trade-off between privacy and security at one hand and functionality in the other.

1.1 Installing Zoom app on a mobile device (iOS and Android)

When a user creates an account on a mobile device, Zoom requests permission to access the following data from (the sensors on) the device:

- Calendar
- Camera
- Contacts
- Precise location
- Microphone
- Telephone
- Storage
- Other (such as prevent phone from sleeping, change audio settings, use fingerprint hardware).

This is the personal data which is collected when installing an account on the device. Permissions are requested by the Zoom mobile app both on iOS and Android.

Please, find the display on the permission requests for Android Meetings apps and iOS Meetings app.

Figure 1: Permissions required in the Android Meetings app[2]

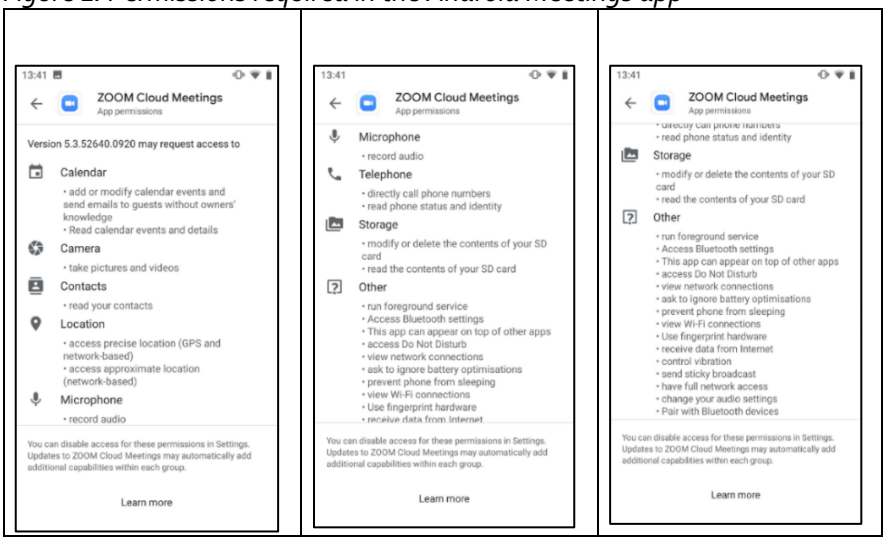
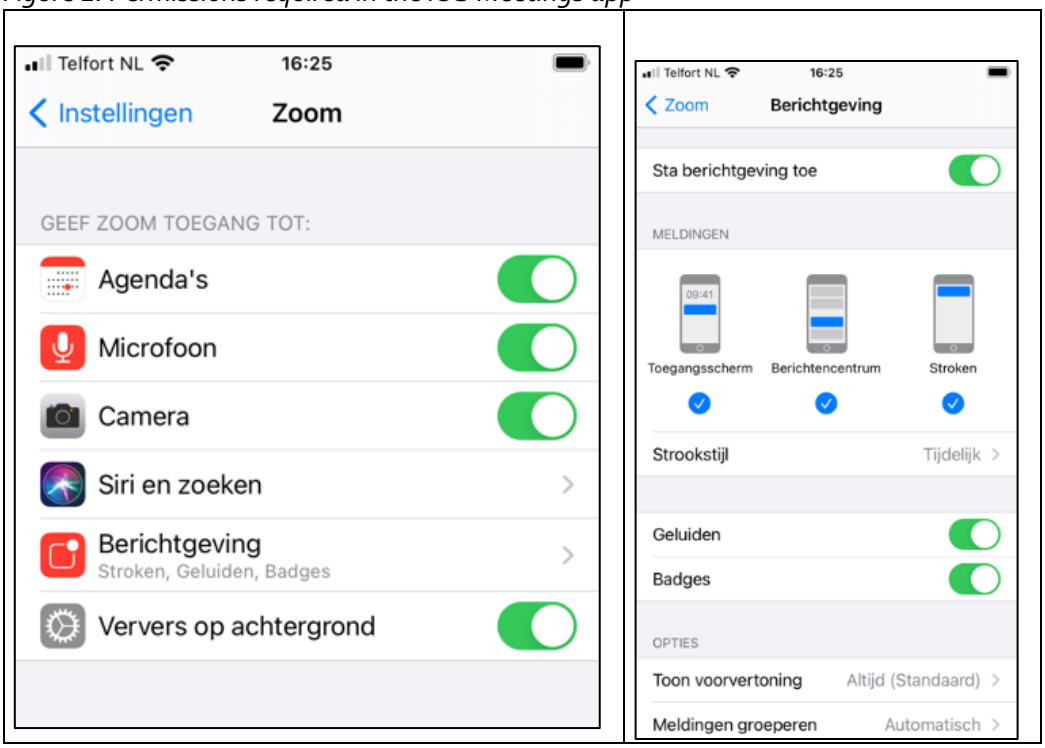


Figure 2: Permissions required in the iOS Meetings app



[2] As recorded on 28 September 2020, in Android app version 5.3.52640.0920, last updated 21 September 2020.

2. Privacy choices and default settings in Zoom user account

When a user creates a Zoom account, Zoom presents the users with security and privacy choices.[3] In this Section only some privacy options are listed. They have the following default settings:

2.1 Meeting- Security (default Off)[4] - Enable E2EE in Account Settings

The recommended setting is to enable E2EE, encrypted meetings, for your own use:

1. Sign in to the Zoom web portal.
2. In the navigation panel, click Settings.
3. Click the Meeting tab.
4. Under Security, verify that Allow use of end-to-end encryption is enabled.
5. If the setting is disabled, click the toggle to enable it. If a verification dialog displays, click Turn On to verify the change.

   Note: If the option is grayed out, it has been locked at either the group or account level. You need to contact your Zoom admin.
6. Under Security, choose the Default encryption type.
7. Click Save.
   Note: Because of the limitations of E2EE, we recommend using Enhanced encryption as the default encryption type and using end-to-end encryption for meetings where additional protection is required.

2.2 Mirror my video (default on)

To access settings in the Zoom desktop client:

1. Sign in to the Zoom desktop client.

[3] Zoom, Changing settings in the desktop client/mobile app, last updated 26 February 2024, URL: https://support.zoom.us/hc/en-us/articles/201362623-About-Settings.
[4] Zoom, End-to-end (E2EE) encryption for meetings, last updated 28 February 2024, URL: https://support.zoom.us/hc/en-us/articles/360048660871-End-to-end-E2EE-encryption-for-meetings.

2.Click your profile picture, then click Settings.

This will open the settings window, giving you access to the following opinions: General, Video, Audio, Share Screen, Phone, Chat, Zoom Apps, Background and Filters, Recording, Profile, Statistics, Feedback, Keyboard Shortcuts, Accessibility.

3.Select “Video”

4. Select “Camera Settings and check / uncheck “Mirror my video”

2.3 Apply video filters

To apply video filters, access settings in the Zoom desktop client:

1.Sign in to the Zoom desktop client.

2.Click your profile picture, then click Settings.

This will open the settings window, giving you access to the following opinions: General, Video, Audio, Share Screen, Phone, Chat, Zoom Apps, Background and Filters, Recording, Profile, Statistics, Feedback, Keyboard Shortcuts, Accessibility.

3.Select “Background and Filters”

4.Select “Video filters”

5.Select the required filter or “None” to disable this filter

2.4 Use virtual backgrounds (there is no default background)

Recommended setting is to use a virtual background. Applying a virtual background is a good idea to prevent accidental sharing of confidential information about your private home or work environment. You can select a background by accessing the settings menu in the Zoom desktop client:

1.Sign in to the Zoom desktop client.

2.Click your profile picture, then click Settings.

This will open the settings window, giving you access to the following opinions: General, Video, Audio, Share Screen, Phone, Chat, Zoom Apps, Background and Filters, Recording, Profile, Statistics, Feedback, Keyboard Shortcuts, Accessibility

3.Select “Background and Filters”

4. Select “Virtual Backgrounds”

5. Select the background of your choice or “None” to work without a virtual background

2.5 Share Screen

- A user can turn this on, if the admin and host have permitted this.
- Press a button ‘Share Screen’.
- Select the desktop, app or screen you want to share.

2.6 Edit profile picture (there is no default picture)

To change your Zoom profile picture:

1. Sign in to the Zoom web portal

2. In the navigation menu, click Profile.

3. Click your profile picture to add or change it. You can also adjust the crop area on your current picture or upload a new one. You can delete your profile picture by clicking **Delete.**

2.7 Integrate Zoom with Outlook (default Off)

2.8 Touch up my appearance (default Off)

The Touch up my appearance feature gives your picture display a softer focus and enhances your digital appearance in real-time.

1. In the Zoom desktop client, click your profile picture then click Settings.
2. Click the video tab.
3. Click Touch my appearance.
4. Use the slider to adjust the effect.

2.9 Enable the remote control of all applications (default Off)

Recommended setting is to disable remote control (default)

1. Sign in to the Zoom web portal.

2. In the navigation menu, click Settings.

3. Click the Meeting tab.

4. Under In **Meeting (Basic)**, click the **Remote control** toggle to enable or disable it.

5. If a verification dialog appears, click **Enable** or **Disable** to verify the change.
   Note: If the opinion is grayed out, it has been locked at the account or group level, and needs to be changed at that level by an account admin.

6. (Optional) Select the check box next to **Allow remote controlling user to share clipboard** to allowed copied information to be shared across Zoom during remote control. Click Save to confirm changes.

2.10 Show message preview (default On. Zoom explains: "*uncheck this option for privacy*")

Recommended setting is to disable show message preview. To change the message preview setting, access settings in the Zoom desktop client:

1. Sign in to the Zoom desktop client.

2. Click your profile picture, then click Settings.

   This will open the settings window, giving you access to the following options: General, Video, Audio, Share Screen, Phone, Chat, Zoom Apps, Background and Filters, Recording, Profile, Statistics, Feedback, Keyboard Shortcuts, Accessibility

3. Select "Chat"

4. Check / Un-Check "Show message preview"

2.11 Record video during screen sharing (default On, if E2EE is not enabled)

Recommended setting is to disable this feature.

1. Sign in to the Zoom desktop client.

2. Click your profile picture, then click Settings.

   This will open the settings window, giving you access to the following options: General, Video, Audio, Share Screen, Phone, Chat, Zoom Apps, Background and Filters, Recording, Profile, Statistics, Feedback, Keyboard Shortcuts, Accessibility

3.Select “recording”

4.Check / Un-Check “Record video during screensharing

2.12 Review feature: Thumbs up/down

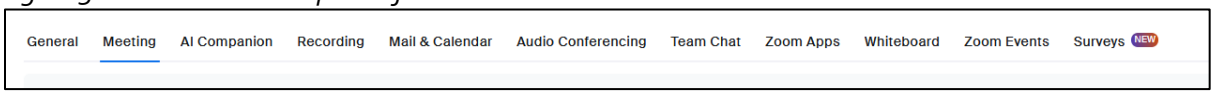
As was mentioned in the final text of the updated DPIA 2024, Zoom disabled by default the option to submit Feedback with a thumbs up or thumbs down symbol at the end of a meeting for its EU Education customers.

This was default On for end-users but default Off for the entire organization. Zoom also gives users a choice if they want to give third parties access to their Zoom Account via the API. Users may want to give such access, or otherwise integrate third party apps, if they for example want to authorize a chatbot to send messages on their behalf in Zoom. Access to the API is turned Off by default. Even if the admin permits the use of the API, the user needs to authorize any permissions asked by third party applications.

3. Privacy choices and default settings for Hosts

Zoom offers separate data protection controls to users when they act as host. The menu contains 4 main sections, each with many different controls. See Figure 3 below.

Figure 3: Menu with main options for hosts



Recommended settings to enhance data protection controls are:

1. Access security options via **the security icon** in the toolbar for quick access to essential in-meeting security controls.
2. Add a **Feedback tab** to the Windows Settings or Mac Preferences
3. **Use Focus mode**, giving participants view of videos without seeing each other[5]
4. Allow meeting participants to send a message visible to **all participants** (default On)
5. **Prevent** participants from saving chat (default Off)
6. **Lock the meeting**: When a host locks a Zoom Meetings that is already started, no new participants can join, even if they have the meeting ID and passcode (if the host has required one).
7. **Put participants on hold**: Hosts can put an attendee on hold and their video and audio connections will be disabled momentarily.
8. **Remove participants**: From that Participants menu, hosts can mouse over a participant's name, and several options will appear, including "Remove".
9. **Report a user**: Hosts/co-hosts can report users to Zoom's Trust & Safety team.
10. **Disable video**: Hosts can turn someone's video off (default Off).
11. **Mute participants**: Hosts can mute/unmute individual participants or all of them at once. There is an option to 'Mute (everybody) Upon Entry' (default Off).
12. **Turn off file transfer**: In-meeting file transfer allows people to share files through the in-meeting chat (default On). Hosts can specify allowed file types and maximize file size.

[5] Zoom, Using focus mode, 29 November 2023, URL: https://support.zoom.us/hc/en-us/articles/360061113751.

13. **Turn off annotation**: Hosts can disable the annotation feature in their Zoom settings to prevent people from writing all over the screens (default On)
14. **Disable private chat**: Zoom has in-meeting chat for everyone, or participants can message each other privately. Hosts can restrict participants' ability to chat amongst one another (default On).
15. **Control screen sharing**: The meeting host can turn off screen sharing for participants (default On). The host may allow only the host, or all participants, and one participant at a time or multiple participants.

Zoom also offers some other privacy relevant **security settings** to Hosts:

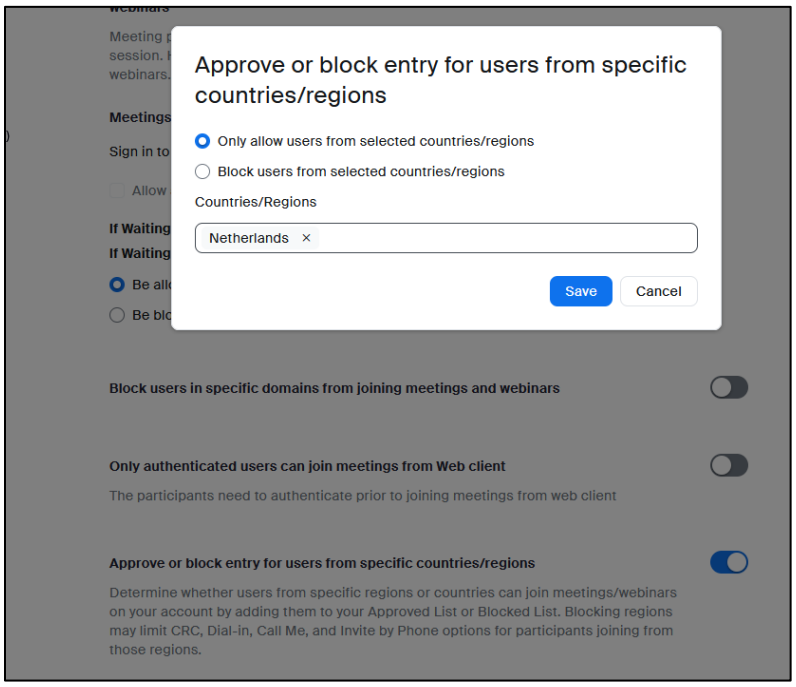
16. Waiting Room (default Off)
    - When **turned On**, the Host has to admit participants individually and users cannot join before the Host has started the meeting.
17. Require a passcode when **scheduling new meetings** (default On)
18. Require a passcode **for instant meetings** (default On)
19. Require a passcode for **Personal Meeting ID** (PMI) (default Off)
20. Only authenticated users can join meetings (default Off – depends on the permissions set by admins)
21. Only authenticated users can join meetings from Web client (default Off – depends on the permissions set by admins)
22. Allow Zoom Rooms to start meeting with **Host Key**: Allow Zoom Rooms to begin a meeting with a 6-digit code making the user with the code the host (default Off).[6]
23. **Add watermark**: Email addresses embedded into shred content and shared video feeds, or both. Hosts may choose where it is visible and the opacity of the mark.

4. Allowing or blocking users from specific regions

When users host a meeting, they can allow or block users from selected regions. *See* Figure 4 below.

[6] Zoom, Claiming host privileges in Zoom Rooms with the host key, Last Updated 11 December 2023, URL: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0069032 .

Figure 4: Approving or blocking users from specific regions[7]



5. Privacy choices and default settings for users when they participate in a meeting

When participating in a session, individual users have access to and can modify their username, alias, contact information, and organization name, and they have the option to include a photo. They also have the option to disable their camera and microphone features if they do not wish to make their picture or voice available to the rest of the participants.

[7] Zoom, Joining from specific countries/region, 25 March 2024, URL: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0064685.