



Recommended Settings for End Users & Hosts

DPIA ZOOM 2022

Version 1

Index

Privacy controls for End Users and Hosts	4
1. Installing Zoom app on a mobile device (iOS and Android)	4
2. Privacy choices and default settings in Zoom user account.....	6
2.1. Enable E2EE in Account Settings – Meeting- Security (default Off)	6
2.2. Mirror my video (default Off).....	6
2.3. Apply Video Filters.....	6
2.4. Use Virtual Backgrounds	7
2.5. Share Screen.....	7
2.6. Edit profile picture (there is no default picture)	7
2.7. Touch up my appearance (default Off)	7
2.8. Enable the remote control of all applications (default Off)	8
2.9. Show message preview (default On).....	8
2.10. Record video during screen sharing (default On, if E2EE is not enabled)	8
3. Privacy choices and default settings for users when they host a meeting	10
3.1. Access security options via the security icon in the toolbar for quick access to essential in-meeting security controls.....	10
3.2. Create a custom (privacy) disclaimer when users join a meeting or sign-in to their account	10
3.3. Add a Feedback tab to the Windows Settings or Mac Preferences	11
3.4. Use Focus mode, giving participants view of videos without seeing each other.....	11
3.5. Allow meeting participants to send a message visible to all participants (default On)	11
3.6. Prevent participants from saving chat)	12
3.7. Lock the meeting	13
3.8. Put participants on hold	13
3.9. Remove participants.....	13
3.10. Report a user	13
3.11. Disable video	13
3.12. Mute participants.....	13
3.13. Turn off file transfer	13
3.14. Turn off annotation	14



- 3.15. Control screen sharing14
- 3.16. Control recording14
- 4. Privacy and security settings for Hosts.....15
 - 4.1. Waiting Room (default Off)15
 - 4.2. Only authenticated users can join meetings (default Off)15
 - 4.3. Only authenticated users can join meetings from Web client (default Off)16

Privacy controls for End Users and Hosts

End Users & Hosts of Zoom Meetings Enterprise can exercise control over the data processing by Zoom in multiple ways. This document describes the default settings and how you can adjust these settings. This document describes the 4 different sets of options for end users to minimise the data processing by Zoom. These 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 you host a Meeting
4. limiting visibility of your personal data to other participants when you participate in a Meeting

Some of these privacy choices depend on settings determined by the administrator. The options for administrators are discussed in “Recommended Settings for Admins – DPIA ZOOM 2022”. If the end user or host can exercise 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. 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).

End users can block push messages, and do not have to give access to their Calendar and Contact Data. **Recommended setting is to deny access.**

Permissions requested by the Zoom mobile app on iOS

The Zoom mobile app may ask you to authorize access to the following permissions with a pop-up, depending on which features you are accessing in Zoom. You can enable these options before-hand or at your overall discretion by going to **Settings**, then scrolling down and selecting **Zoom** on your device. The following permissions are requested by Zoom:

- **Location:** Allows Zoom to access your location, so it can generate an Emergency Response Location, for when dialing emergency services from Zoom phone.
- **Contacts:** Utilized for Phone Contact Matching (not available for iPads or iPadOS).
- **Calendars:** Allows Zoom to add a meeting as an event in the Calendar app, when a Zoom meeting is scheduled.

- **Photos:** Allows Zoom the ability to access your local photo albums, for adding images to chat messages, or for screen sharing during a meeting or webinar.
- **Microphone:** Joining using built-in audio devices in a meeting or webinar.
- **Camera:** Sharing your video in a meeting or webinar.
- **Siri & Search:** Enables the ability to add Siri Shortcuts including Join the Next Meeting, View Today's Meetings, Start My Personal Meeting.
- **Notifications:** Allows Zoom the ability to display notifications for chat messages, upcoming meetings, and more.
- **Background App Refresh:** Allows for notifications for Meeting invites when the app is closed and not actively running.
- **Local network:** Requested when connecting to a Peer-to-Peer meeting, performing a DNS query for Zoom Phone, or when pairing your mobile app with a local Zoom Room.

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.¹ In this Section only some privacy options are listed.

2.1. Enable E2EE in Account Settings – Meeting- Security (default Off)

The recommended setting is to enable E2EE. To enable End-to-end (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 Off)

To 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 "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 options: General,

¹ Zoom, Changing settings in the desktop client/mobile app, last updated 15 December 2021, URL: <https://support.zoom.us/hc/en-us/articles/201362623-About-Settings>

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

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 options: 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. To share a screen during a Zoom meeting:



2. 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**.
You can view and edit the following settings:
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. 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 up my appearance**.
4. Use the slider to adjust the effect.

2.8. 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 option 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.

2.9. Show message preview (default On)

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"

2.10. 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"

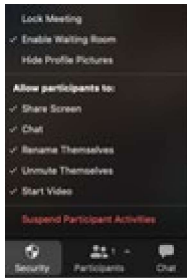


3. Privacy choices and default settings for users when they host a meeting

Zoom offers separate data protection controls to users when they act as host. The summary below is a summary of these controls.

Many of these controls are self-explanatory. Where needed more guidance is given.

3.1. Access security options via the security icon in the toolbar for quick access to essential in-meeting security controls.



3.2. Create a custom (privacy) disclaimer when users join a meeting or sign-in to their account

Recommended setting is to enable this feature. To enable a custom disclaimer for all users in the account:

- Sign in to the Zoom web portal as an admin with the privilege to edit account settings.
- In the navigation panel, click **Account Management** then **Account Settings**.
- Click the **Meetings** tab.
- Under In Meeting (Advanced), verify that Show a custom disclaimer when starting or joining a meeting is enabled.
- If the setting is disabled, click the toggle to enable it. If a verification dialog appears, click **Enable** to verify the change.
- (Optional) If you want to make this setting mandatory for all users in your account, click the lock icon, and then click **Lock** to confirm the setting.

To setup and customize the disclaimer for meetings and webinars

1. Make sure the [disclaimer is enabled](#).
2. Click Manage Disclaimer.
3. Change these settings:
 - Display For: Specify if the disclaimer is displayed to internal or external users. You must select at least one option.
 - Internal participants: Display the disclaimer to internal users that start or join meetings.
 - External participants: Display the disclaimer to external users that join meetings hosted by internal users.
 - Show the same disclaimer to internal and external users?: If you selected both of the above options, you can use one disclaimer for both user types or have separate disclaimers.
 - Frequency: Specify how often the disclaimer is shown.
 - Every time: Show the disclaimer every time users join or start a meeting, regardless of whether they click Allow or Agree.

- First time only: Show the disclaimer until they click Allow (desktop client) or Agree (mobile app). If they click Cancel, they will see the same disclaimer the next time they join or start a meeting.
Note:
 - This applies to internal and external users depending on the Display For setting.
 - If you enabled the disclaimer for external users and they clicked Allow or Agree, they will not see the disclaimer again the next time they join a meeting hosted by an internal user.
 - Every month, Every quarter, Every 6 months, Every year: After a user accepts the disclaimer, repeat the disclaimer in the specified interval.
 - Languages: If you have translated versions of the disclaimer, select the relevant languages.
4. Click Next
 5. Enter the title and description of the disclaimer. Click Preview to see how the disclaimer is displayed in the desktop client.
Note: The disclaimer in the desktop client will always state, This disclaimer was generated by your account admin.
 6. Click Save.

3.3. *Add a Feedback tab to the Windows Settings or Mac Preferences*

Recommended setting is to disable this feature. To enable the Feedback to Zoom feature for your own use:

1. Sign in to the Zoom web portal.
2. Click **Account Management > Account Settings** (if you are an account administrator) or **Settings** (if you are an account member).
3. Navigate to the **Feedback to Zoom** option on the **Meeting** tab and verify that the setting is enabled.
If the setting is disabled, click the toggle to enable it. If a verification dialog displays, choose **Turn On** to verify the change.



3.4. *Use Focus mode, giving participants view of videos without seeing each other*

Recommended setting is to enable this feature. To enable or disable Focus mode for your own use:

1. Sign in to the Zoom web portal.
2. In the navigation menu, click Settings.
3. Click the Meeting tab.
4. Under In Meeting (Advanced), click the Focus Mode toggle to enable or disable it.
5. If a verification dialog appears, click Enable or Disable to verify the change.
Note: If the option is grayed out, it has been locked at the account or group level and needs to be changed at that level.
6. (Optional) Select the check box next to Allow host to enable focus mode when scheduling, then click Save. This option allows you to [schedule meetings](#) with focus mode to start automatically when the meeting starts, in order to provide fewer distractions to all meeting participants.

3.5. *Allow meeting participants to send a message visible to all participants (default On)*

Recommended setting is to disable this feature. If you're the meeting host, you can change the in-meeting chat settings.

1. While in a meeting, click Chat  in the meeting controls.
2. Click the ellipses icon  to display in-meeting chat settings.
3. You can access the following options:
 - [Save chat](#): Save all chat messages in a TXT file. Saved to the same location as local recording files.
 - Participant can chat with: Control who participants can chat with.
 - No one: Disables in-meeting chat.
 - Host and co-hosts: Only the host and co-host can send messages to everyone. Participants can still send private messages to the host.
 - Everyone: Participants can only send public messages. Public messages are visible to all participants. Participants can still send private messages to the host.
 - Everyone and anyone directly: Participants can send public or private messages. Public messages are visible to all participants. Private messages are sent to a specific participant, and are not visible to the host.

3.6. Prevent participants from saving chat)

Recommended setting is to disable the feature that allows participants to save chats. Saving chats can lead to out-of-context use of messages shared in the specific setting of a possibly confidential meeting.

1. Sign in to the Zoom web portal.
2. Click [Settings](#).
3. Navigate to “in meeting (Basic)”
4. In “Chat” Check / Un-Check “prevent participants from saving chat

3.7. Lock the meeting



3.8. Put participants on hold

Hosts can put an attendee on hold and their video and audio connections will be disabled momentarily.

To put an attendee on hold:


5. Select the attendee in the participant list
6. Click “More”
7. Click “put on hold”

3.9. Remove participants

From that Participants menu, hosts can mouse over a participant’s name, and several options will appear, including “Remove”.

3.10. Report a user

Hosts/co-hosts can report users to Zoom’s Trust & Safety team.

1. As the meeting host or a participant, click the meeting information icon  in the top-left corner of the window.
2. In the bottom-left corner of the meeting information dialog, click Report.
3. Enter the participant(s) you would like to report.
4. Select the reason for reporting the participant.
5. If you are not currently signed in to your Zoom account, enter your email address.
6. (Optional) Select the Include desktop screenshot check box to include a current screenshot of your desktop.
7. Click Submit.

You will receive a notification that your report was sent successfully.

3.11. Disable video

Recommended setting is to enable this feature. Hosts can turn someone’s video off (default Off).

This option is available from the participants list. Click “more” behind a participant name and select “stop video”

3.12. Mute participants

Recommended setting is to enable this feature. Hosts can mute/unmute individual participants or all of them at once. There is an option to ‘Mute (everybody) Upon Entry’ (default Off). This prevents noisy starts of Meetings, if participants join from a noisy location.

3.13. Turn off file transfer

Recommended setting is to disable this feature.

1. In-meeting file transfer allows people to share files through the in-meeting chat (default On)
2. To disable in meeting file transfer:

3. Login on the Zoom portal
4. Click on “Settings”
5. Navigate to “in meeting (basics)”
6. Slide the toggle for “send files via meeting chat” to the off position

3.14. Turn off annotation

Recommended setting is to disable this feature. Hosts can disable the annotation feature in their Zoom settings to prevent people from writing all over the screens (default On)

To enable / disable annotation 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 In Meeting (Basic), verify that Annotation 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. (Optional) Click the check box to allow saving of shared screens with annotations.
7. (Optional) Click the check box to restrict annotation to only the user sharing content.

3.15. Control screen sharing

Recommended setting is to enable this feature. The meeting host can turn off screen sharing for participants (default On).

To prevent participants from screen sharing:



2. Under **Who can share?** Choose **Only Host**.
3. Close the window.

3.16. Control recording

Recommended setting is to disable this feature. The ability to record to the cloud or locally is something an account admin can control. If enabled, the host can decide to enable/disable a participant or all participants to record.

To enable or disable local recording for your own use:

1. Sign in to the Zoom web portal.
2. In the navigation menu, click **Settings**.
3. Click the **Recording** tab.
4. Click the **Local Recording** toggle to enable or disable it.
5. If a verification dialog appears, 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, and you will need to contact your Zoom administrator.
6. (Optional) Select the check boxes to enable or disable additional features, then click **Save**:



- **Save chat messages from the meeting/webinar:** Allows you to save in-meeting chat messages in the local recording files (not recommended).
- **Save closed caption as a VTT file:** Allows you to save closed caption files in local recordings.
- **Hosts can give meeting participants permission to record locally:** Allows you to give permission to record locally as well.

4. Privacy and security settings for Hosts

4.1. Waiting Room (default Off)

Recommended setting is to enable this feature. When turned On, the Host has to admit participants individually and users cannot join before the Host has started the meeting)

To enable Waiting Room 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 Waiting Room 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 administrator.
6. Click Edit Options to specify Waiting Room options.

4.2 Require a passcode

Recommended setting is to enable this feature. when scheduling new meetings (default On), for instant meetings (default on) and for Personal Meeting ID (default off) To enable passcode settings for your own use:

1. Sign into the Zoom web portal and navigate to [Settings](#).
2. In the Security section, verify that the passcode settings that you would like to use for your meetings and webinars are enabled.
If the setting is disabled, click the toggle to enable it. If a verification dialog displays, choose Turn On to verify the change.
Note: If the option is grayed out, it has been locked at either the Group or Account level, and you will need to contact your Zoom administrator.

4.2. Only authenticated users can join meetings (default Off)

Recommended setting is to enable this feature. Functionality depends on the permissions set by admins. To enable or disable Only authenticated users can join meetings for your own use:

1. Sign in to the Zoom web portal.
2. In the navigation menu, click Settings.
3. Click the Meeting tab.



4. Under Security, click the Only authenticated users can join meetings toggle to enable or disable it.
5. If a verification dialog displays, click Enable or Disable 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.

4.3. Only authenticated users can join meetings from Web client (default Off)

Recommended setting is to enable this feature. Functionality depends on the permissions set by admins. To enable or disable Only authenticated users can join meetings from Web client 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, click the Only authenticated users can join meetings from Web client toggle to enable or disable it.
5. If a verification dialog displays, click Enable or Disable 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.