



## Recommended Settings for Admins

DPIA ZOOM 2022

Version 1

## Index

Privacy controls for Admins .....	3
1. Enable E2EE .....	3
2. EU Geolocation .....	4
Selecting datacenter regions for meetings / webinars .....	4
3. Public and private chat .....	5
4. Enable Advanced chat encryption .....	6
5. Use of SSO and Vanity URL .....	7
6. Prevent participants from saving chats .....	8
7. Sharing of files in chats .....	8
8. Do not enable Attendee Feedback .....	9
9. Do not enable Giphy .....	9
10. Mute individual or all participants upon entry .....	10
11. File transfer .....	10
12. Annotation .....	11
13. Prohibit the viewing and recording of the 'gallery' during screen sharing (Focus mode) .....	11
14. Visibility of participants .....	12
15. Co-hosts .....	13
16. Polling .....	13
17. API features and Marketplace apps .....	13
Marketplace Apps and GDPR .....	14
18. Integration of user calendar and contacts .....	15
19. Allow users to rename themselves .....	15

## Privacy controls for Admins

Administrators of Zoom Meetings Enterprise can exercise control over the data processing by Zoom in multiple ways.

Below, 19 different options are discussed, with references to Zoom's documentation how to effectuate the recommended setting. Settings impact functionality. The choice is up to the institution. Most of the times it is a trade-off between privacy and security at one hand and functionality in the other.

Additionally, SURF recommends admins to deploy Single Sign On and the use of a Vanity URL. These two measures prevent the transfer of names, e-mailaddresses and IP addresses to the USA. See '5 Use of SSO and Vanity URL' page 6.

### 1. Enable E2EE

**End-to-end encryption (E2EE) enabled is recommended.** Admins can enable end-to-end encryption for all Meetings. This is possible for all clients, except when Zoom is used via the browser. E2EE meetings are limited to 200 participants.

Admins can make E2EE mandatory for all users in their account, by clicking the lock icon, and then clicking *Lock* to confirm the setting.

Because Zoom can no longer see the contents of exchanged communications, the following functionality will no longer work:

- Join the meeting by telephone
- Join before host
- Cloud recording
- Live streaming
- Live transcription
- Breakout Rooms
- Polling
- Zoom Apps<sup>1</sup>

With up-to-date end user clients, the functionalities of meeting reactions and 1:1 Private Chats do still work. Admins can use local recording for Meetings.<sup>2</sup>

To enable End-to-end (E2EE) encrypted meetings for all users in the account:

1. Sign in to the Zoom web portal as an admin with the privilege to edit account settings.
2. In the navigation panel, click **Account Management** then **Account Settings**.
3. Click the **Meeting** tab.
4. Under **Security**, verify that **Allow use of end-to-end encryption** is enabled.

---

<sup>1</sup> Zoom, End-to-end (E2EE) encryption for meetings, last updated 14 January 2022, URL: <https://support.zoom.us/hc/en-us/articles/360048660871-End-to-end-E2EE-encryption-for-meetings>

<sup>2</sup> Zoom, Enabling and starting local recordings, last updated 23 January 2022, URL: <https://support.zoom.us/hc/en-us/articles/201362473-Enabling-and-starting-local-recordings>

5. If the setting is disabled, click the toggle to enable it. If a verification dialog displays, click **Turn On** to verify the change.
6. (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.
7. Under **Security**, choose the **Default encryption type**.
8. Click **Save**.

**Note:** Because of the limitations of E2EE, we recommend to review the settings carefully.

Scheduling a meeting with End-to-End encryption from the Zoom client:



Scheduling a meeting with End-to-End encryption from the Zoom portal:

1. Sign in to the Zoom web portal with your Zoom account
2. In the navigation panel click Meetings then Schedule a meeting



## 2. EU Geolocation

Until Zoom has completed its EU Cloud (by the end of 2022) admins should use the option to have all streaming content data processed in Zoom’s EU data centers (in Germany). This setting applies to all data exchanged in Meetings, including cloud recordings and meeting transcripts, as well as files that are exchanged during a meeting.<sup>3</sup>

By mid-2022 Zoom commits to offer a choice to have all Support Data exclusively processed by its Romanian subprocessor, in the EU. Once that choice is active, admins will see an option to provide specific consent if they want to authorise Zoom to transfer incidental support requests to its subprocessors in the Philippines and the USA, when an organisation needs urgent support, outside of EU working hours.

### Selecting datacenter regions for meetings / webinars.


To select data center regions for all users in the account:

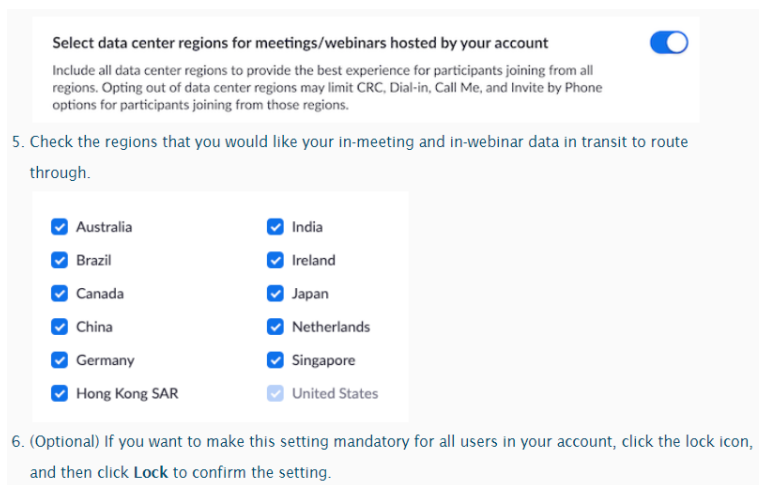
1. Sign in to the Zoom web portal as an admin with the privilege to edit account settings.
2. In the navigation menu, click **Account Management** then Account Profile.

---

<sup>3</sup> Zoom, FAQs: Transferring EEA & UK Residents’ Data to the US, URL: [https://zoom.us/docs/doc/EEA\\_Transfer\\_of\\_Data.pdf](https://zoom.us/docs/doc/EEA_Transfer_of_Data.pdf)

3. In the **Transit Data** section, click the **Customize data center regions for meeting/webinar data in transit** toggle to enable or disable it.
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 in transit to route through.<sup>4</sup>
6. Click **Save** to confirm changes.

(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.



### 3. Public and private chat

Admins can enable or disable chat for all users in the account or for specific groups in the account. Admins can also disable private chat, which prevents participants from sending private messages to other participants in the meeting. Participants will still be able to privately message with the host.<sup>4</sup>

To enable or disable **Chat** for all users in the account:

1. Sign in to the Zoom web portal as an admin with the privilege to edit account settings.
2. In the navigation panel, click **Account Management** then **Account Settings**.
3. Click the **Meeting** tab.
4. Under **In Meeting (Basic)**, click the **Chat** toggle to enable or disable it. If you disable **Chat**, the [Private chat](#) and [Auto saving chats](#) features will also be disabled.  
**Note:** You may see separate settings for **Meeting chat** and **Webinar chat** if you requested this to be enabled by Zoom.
5. If a verification dialog appears, click **Turn On** or **Turn Off** to verify the change.

---

<sup>4</sup> Zoom, Enabling or disabling in-meeting chat, last updated 15 December 2021, URL: <https://support.zoom.us/hc/en-us/articles/115004809306-Enabling-or-disabling-in-meeting-chat>

6. (Optional) Change these setting for chat permissions, then click **Save**:

**Note:** These settings only work properly if the host is on client version 5.7.3 and above.

- **Allow participants to chat with:** Specify who meeting participants and webinar panelists can chat with using in-meeting or in-webinar chat.
- **Allow users to save chats from the meeting:** Enable or disable the ability to [save the chat transcript](#) for **Hosts and co-hosts** or **Everyone**.



#### 4. Enable Advanced chat encryption

Admins can enable Advanced chat encryption. Zoom explains: “When advanced chat encryption is enabled, Content Data at rest is encrypted by keys generated & operated on chat participants’ devices.”<sup>5</sup> **Recommended setting is ON**

To enable the advanced chat encryption for all members of your organization:

1. Sign in to the Zoom web portal.
2. In the navigation panel, click **Account Management** then [IM Management](#).
3. Click the [IM Settings](#) tab.
4. Verify that the **Enable advanced chat encryption** option 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.
5. (Optional) If enabling advanced chat encryption, select the **Enable link preview** check box to enable link previews.

When enabled, link previews will be shown to users who send or receive chat messages with links. The local application will detect the link in the sender's message before it is encrypted, and the preview will be shared between the sender and recipient. Only URLs are detected by this link preview feature and they must match **http://** or **https://** followed by a non-empty space. This feature is disabled by default.

6. After enabling advanced chat encryption, chats in the Zoom desktop client and mobile app tab will display a lock icon to indicate that advanced chat encryption is enabled.



Users will not see the encrypted chat until they open Zoom. Notifications (including those on the lock screen) will state that they have received an encrypted chat.

---

<sup>5</sup> Zoom, Advanced chat encryption, 1 February 2022, URL: <https://support.zoom.us/hc/en-us/articles/207599823>

## 5. Use of SSO and Vanity URL

**Recommended is to use SSO and a Vanity URL.** Organisations can deploy SSO for employees to subscribe to Zoom, with an organisational subdomain.<sup>6</sup> Such a Vanity URL<sup>7</sup> creates three privacy controls:

Use email aliases. Zoom explains: *“In most email systems it is possible to create multiple aliases for each user that are routed to the same user inbox. Customers can thus create an alias for each of their users to ensure that they are not easily identifiable by their email address. An admin can choose to only provide these pseudonymous addresses to Zoom.”*

Remove or replace first name and surname. Zoom explains it does not need the full name of the user to provide its services. *“The customer can decide to delete these data from existing accounts, use a generic organisation name (such as: University of Harderwijk), and/or not to provide any details for new users. The service will still work, even though the display name may be blank/anonymised. This may make existing waiting room functionality hard, but video waiting rooms would mitigate this.”*<sup>8</sup>

Prevent use of cookies and transfer of IP addresses and device identifiers of end users to the USA when they sign in via their browser on Zoom’s publicly accessible website. All traffic to an EU Customer’s Vanity URL stays within the EU.

Set-up SSO:

Apply for your vanity URL (such as <https://universityofHarderwijk.zoom.us>) on your Account Profile page. You will need to wait for this to be approved before you can configure the SSO on the Zoom side.

First, configure your IdP to send us the following:

- Any unique identifier linked to nameID such as eduPersonTargetedID, persistentID, or mail
- (Optional) Accepted attributes are email (urn:oid:0.9.2342.19200300.100.1.3), sn (urn:oid:2.5.4.4), and givenName (urn:oid:2.5.4.42).

Second, enter your SSO information at <https://zoom.us/account/sso>. See the attached example from your idP xml metadata.

- Sign-in page URL: <SingleSignOnService>
- Sign-out page URL: <SingleLogoutService>
- Certificate: <X509Certificate> **\*Note: Remove the Begin Certificate and End Certificate\***
- Issuer: <ID of EntityDescriptor>
- Binding: Choose http-post or http-redirect
- Default user type: Basic or Pro

---

<sup>6</sup> Zoom, Quick start guide for SSO, last updated 15 December 2021, URL: <https://support.zoom.us/hc/en-us/articles/201363003-Quick-start-guide-for-SSO>

<sup>7</sup> Zoom, Guidelines for Vanity URL requests, Last updated 9 April 2021, URL: <https://support.zoom.us/hc/en-us/articles/215062646-Guidelines-for-Vanity-URL-Requests>

<sup>8</sup> Zoom reply to part A of the DPIA, 19 March 2021, p. 16.

Lastly, once configured, you can get the SP metadata XML file from:

<https://yourcompany.zoom.us/saml/metadata/sp>

Once configured, users can sign in with SSO.

## 6. Prevent participants from saving chats

**Recommended setting is to disable this feature and prevent participants from saving chats.** Chats are automatically saved. Organisations may want to disable this feature and prevent participants from saving chats that may contain personal data, not just from participants, but also remarks about, or data from, other individuals.<sup>9</sup>

To enable or disable **Auto saving chats** for all users in the account:

1. Sign in to the Zoom web portal as an admin with the privilege to edit account settings.
2. In the navigation menu, click **Account Management** then **Account Settings**.
3. Click the **Meeting** tab.
4. Under **In Meeting (Basic)**, click the **Auto saving chats** toggle to enable or disable it.
5. If a verification dialog displays, click **Enable** or **Disable** to verify the change.



## 7. Sharing of files in chats

Admins can set limits to the type and size of files that can be shared in chats:

- Only allow specified file types (optional): Specify the file types that users can send in chat. Zoom desktop client version 5.4.0 or higher is required.
- Maximum file size (optional): Specify the maximum file size (MB) that users can send in chat and in-meeting chat. Zoom desktop client version 5.4.0 or higher is required.<sup>10</sup>

To enable or disable **sending files via meeting chat** for all users in the account:

1. Sign in to the Zoom web portal as an admin with the privilege to edit account settings.
2. In the navigation menu, click **Account Management** then **Account Settings**.
3. Click the **Meeting** tab.
4. Under **In Meeting (Basic)**, click the **send files via meeting chat** toggle to enable or disable it.

---

<sup>9</sup> Zoom, (Disabling) auto saving chats, last updated 11 January 2022, URL: <https://support.zoom.us/hc/en-us/articles/360060889932-Enabling-auto-saving-chats>

<sup>10</sup> Zoom, Sharing, URL: [https://support.zoom.us/hc/en-us/articles/203749815#h\\_01EH3B3FMB1ZRY9RF5Z1RJSMQV](https://support.zoom.us/hc/en-us/articles/203749815#h_01EH3B3FMB1ZRY9RF5Z1RJSMQV)



### 8. Do not enable Attendee Feedback

**Recommended setting is to disable attendee feedback.** Zoom has disabled this survey request by default for its EU Education and Enterprise customers.<sup>11</sup> As the survey contains an open text field, there is a possibility that end users provide personal data in this text box. To mitigate this risk, Zoom has disabled this functionality by default.

To enable or disable **end-of-meeting experience feedback survey** for all users in the account:

1. Sign in to the Zoom web portal as an administrator with the privilege to edit account settings.
2. In the navigation panel, click **Account Management** then **Account Settings**.
3. Click the **Meeting** tab.
4. Under **In Meeting (Basic)**, click the **Display end-of-meeting experience feedback survey** toggle to enable or disable it.
5. If a verification dialog displays, click **Enable** or **Disable** to verify the change.



Display end-of-meeting experience feedback survey



Display a thumbs up/down survey at the end of each meeting. If participants respond with thumbs down, they can provide additional information about what went wrong. 

### 9. Do not enable Giphy

**Recommended setting is to disable Giphy.** The US American company Giphy enables users to search for illustrations based on keywords, based on its archive of millions of GIFs, stickers and video clips/animations. Facebook bought Giphy in May 2020. If the organisation has enabled advanced chat encryption, use of Giphy is technically impossible. To prevent traffic to Giphy/Facebook as a third party (Zoom does not have a subprocessor agreement with Giphy or Facebook) admins should not enable this integration in the Zoom chats.<sup>12</sup>

To enable or disable **the sending of animated gif images** for all users in the account:

1. Sign in to the Zoom web portal as an administrator with the privilege to edit account settings.
2. In the navigation panel, click **Account Management** then **IM Management**.
3. Click the **IM Settings** tab.
4. click the **Animated GIF images** toggle to enable or disable it.

<sup>11</sup> Zoom, End-of-meeting experience feedback survey, 11 January 2022, URL: <https://support.zoom.us/hc/en-us/articles/115005855266-End-of-meeting-experience-feedback-survey>

<sup>12</sup> Zoom, Managing IM groups, last updated 13 December 2021, URL: <https://support.zoom.us/hc/en-us/articles/203749815>

**Animated GIF images**

Allow users to search GIF images from Giphy.

### 10. Mute individual or all participants upon entry

This meeting setting can help manage participants and prevent distractions and interruptions during a meeting (Zoom-bombing).<sup>13</sup>

To enable or disable **Mute all participants when they join a meeting** for all users in the account:

1. Sign in to the Zoom web portal as an admin with the privilege to edit account settings.
2. In the navigation menu, click **Account Management** then **Account Settings**.
3. Click the **Meeting** tab.
4. Under **Schedule Meeting**, click the **Mute all participants when they join a meeting** toggle to enable or disable it.
5. If a verification dialog displays, click **Enable** or **Disable** to verify the change.

**Mute all participants when they join a meeting**

Automatically mute all participants when they join the meeting. The host controls whether participants can unmute themselves.

### File transfer

**Recommended setting is to disable file transfer.** To prevent accidental data breaches, file transfer is disabled by default.<sup>14</sup>

File transfer allows you to send files to other meeting participants during the meeting (or webinar) through the in-meeting chat. Files can be specifically sent to all participants, directly to one participant, or specific predefined groups, such as all panellists in a webinar.

To enable / disable in-meeting file transfer for all members of your organization:

1. Sign in to the Zoom web portal as an administrator with the privilege to edit account settings.
2. In the navigation menu, click **Account Management** then **Account Settings**.
3. On the **Meeting** tab under the **In Meeting (Basic)** section, locate the **Send files via meeting chat** setting and verify that is enabled.

<sup>13</sup> Zoom, Muting all participants when they join a meeting, last updated 15 December 2021, URL: <https://support.zoom.us/hc/en-us/articles/360060860512-Muting-all-participants-when-they-join-a-meeting>

<sup>14</sup> Zoom, Sending a file in meetings and webinars, last updated 15 December 2021, URL: <https://support.zoom.us/hc/en-us/articles/209605493-Sending-a-file-in-meetings-and-webinars>

4. If the setting is disabled, click the toggle to enable it. If a verification dialog displays, click **Enable** to verify the change.
5. (Optional) To restrict the allowed file types, check **Only allow specified file types** and add the file type extensions, separated by commas.
6. (Optional) To restrict the allowed file types, check **Maximum file size** and adjust the maximum file size.



## 11. Annotation

**Recommended setting is to disable annotation.** Enabling annotation tools allows meeting participants to collaborate, brainstorm, and draw over shared content. This functionality is disabled by default.<sup>15</sup>

To enable / disable annotation for all users in the account:

1. Sign in to the Zoom web portal
2. In the navigation panel, click **Account Management** then **Account 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.
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.



## 12. Prohibit the viewing and recording of the 'gallery' during screen sharing (Focus mode)

**Recommended setting is to prohibit the viewing and recording of the 'gallery' during screen sharing.**

Admins can prohibit viewing and recording of the gallery with participants when a screen is shared. This means the teacher can see the students, but the students do not see each other, nor are they recorded. This helps guarantee the public character of meetings and recordings.

To enable Focus mode for all users in the account:

1. Sign in to the Zoom web portal as an admin with the privilege to edit account settings.
2. In the navigation menu, click **Account Management** then **Account Settings**.

---

<sup>15</sup> Zoom, Enabling or disabling annotation tools for meetings, last updated 10 December 2021, URL: <https://support.zoom.us/hc/en-us/articles/4409894568845-Enabling-or-disabling-annotation-tools-for-meetings>

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.
6. (Optional) Select the check box next to **Allow host to enable focus mode when scheduling**, then click **Save**. This option allows users to [schedule meetings](#) with focus mode to start automatically when the meeting starts, in order to provide fewer distractions to all meeting participants.



### 13. Visibility of participants

**Recommended setting of visibility of participant is restricted.** Admins can allow users to see each other's contact details, depending on classification in one of three visibility groups (IM Groups). Zoom explains:

- **Private:** Only members can see the group automatically. Users who are not in the group can search for users who are in the group.
- **Shared:** All people in the account can see the group and members automatically.
- **Restricted:** No one can see the group or find the members of the group using search except for those in the group.”<sup>16</sup>

Changing the default IM group will only affect new users being added. To change the default IM group:

1. Sign in to the **Zoom web portal**.
2. In the navigation menu, click **User Management** then **Users**.
3. Click the **Advanced** tab.
4. Scroll down to the **Change IM Group** section.
5. Click the drop down menu labelled **Set default IM Group**, then select the appropriate name.
6. Click **Save**.

To move users from one group to another:

1. Sign in to the **Zoom web portal**.
2. In the navigation menu, click **User Management** then **Users**.
3. Click the **Advanced** tab.
4. Scroll down to the **Change IM Group** section.
5. Click the drop down menu labelled **Switch IM Group**, then select the appropriate name.
6. Click **Switch User Group**.

---

<sup>16</sup> Zoom, Managing IM groups, Last Updated 13 December 2021, URL: <https://support.zoom.us/hc/en-us/articles/203749815>

### 14. Co-hosts

There is a control for co-hosts. The admin can use this to enable hosts to add co-hosts. Co-hosts have the same in-meeting controls as the host.<sup>17</sup>

To enable / disable co-hosts for all users in the account:

1. Sign in to the Zoom web portal
2. In the navigation panel, click **Account Management** then **Account 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.



### 15. Polling

With the control for polling, the admin can add 'Polls' to the meeting controls. This allows hosts to survey the attendees.<sup>18</sup> As shown in [Appendix 1](#) the surveys involve the use of a cookie from the US based company Wootric, and hence, traffic with a.o. IP addresses to the USA. The company is included in the list of authorised subprocessors from Zoom, and thus bound to the same data protection guarantees as Zoom itself.

To enable / disable meeting (and webinar) polls and quizzes for all users in the account:

1. Sign in to the Zoom web portal
2. In the navigation panel, click **Account Management** then **Account Settings**.
3. Click the **Meeting** tab.
4. Under **In Meeting (Basic)**, verify that **Meeting Polls / quizzes** and **Meeting Polls / quizzes** is disabled.



### 16. API features and Marketplace apps

**Recommended setting is to turn off API features and marketplace apps**, to prevent the unauthorised transfer of personal data to third parties. An admin has access to a number of API features. Access to the API is turned Off by default. This means the admin has to pre-approve use of all apps in the Marketplace. There is an option for admins to enable API access to all users' chat messages in this

<sup>17</sup> Zoom, Host and co-host controls in a meeting, last updated 21 January 2022, URL: <https://support.zoom.us/hc/en-us/articles/201362603>

<sup>18</sup> Zoom, Enabling polling for meetings, last updated 15 December 2021, URL: <https://support.zoom.us/hc/en-us/articles/4412324684685>

account. By default, the admin has to approve all authorisation requests from end-users (See Figure below).

To configure pre-approval of apps:

1. Sign in to the **Zoom web portal**.
2. In the navigation menu, click **Advanced**, then **App Marketplace**.
3. In the top right corner of the page, click **Manage**.
4. In the **ADMIN APP MANAGEMENT** section, click **Permissions**.
5. Enable the followings as desired:
6. In the **Publicly listed apps** box:

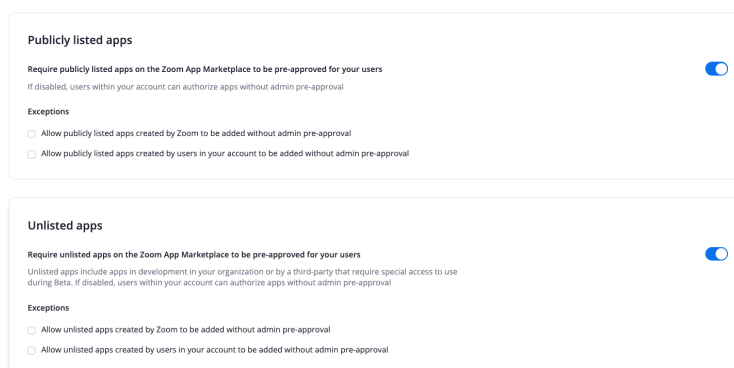


- (Optional) Check **Allow publicly listed apps created by Zoom to be added without admin pre-approval** to exempt Zoom-created apps from pre-approval by an admin.
- (Optional) Check **Allow publicly listed apps created by users in your account to be added without admin pre-approval** to exempt apps created by a member of your organization from pre-approval by an admin.

7. In the **Unlisted apps** box:



8. (Optional) Check **Allow unlisted apps created by Zoom to be added without admin pre-approval** to exempt Zoom-created apps from pre-approval by an admin.
9. (Optional) Check **Allow unlisted apps created by users in your account to be added without admin pre-approval** to exempt apps created by a member of your organization from pre-approval by an admin.



### Marketplace Apps and GDPR

The integrations provided in the Zoom Marketplace provide integration with applications apps that are possible located outside of the EU, and can process the personal data from the Zoom environment for their own purposes, such as behavioural advertising and profiling

Before enabling or approving the installation of integrations from the Zoom Marketplace, confirm that the integration meets GDPR requirements. .

### 17. Integration of user calendar and contacts

**Recommended setting is to disable integration of user calendar and contacts.** Zoom account administrators can enable users to integrate their calendar and contacts. Zoom supports Google Calendar, Microsoft Exchange and Microsoft Office 365. This is a relevant privacy choice, as these Customer Content Data fall outside of the subset of Customer Content Data for which admins can determine that they may only be stored in the EU (in Germany). This will change after the end of 2022, when Zoom processes all personal data of its EU Education and Enterprise customers exclusively in the EU.

To enable / disable integration of user calendar and contacts for all users in the account:

1. Sign in to the Zoom web portal
2. In the navigation panel, click **Account Management** then **Account Settings**.
3. Click the **Meeting** tab.
4. Under **calendar and contacts**, verify that **calendar and contacts integration** is disabled.

#### Calendar and Contacts

##### Calendar and contacts integration





Allow users to integrate calendar and contacts services (Google, Exchange, Office 365) with Zoom



### 18. Allow users to rename themselves

**Recommended setting is to disable the allowance for users to rename themselves.** Controls for host and co-host allows for participants, meeting and webinar panellists to rename themselves.

To avoid misuse of the self provided labels administrators have the option to deny the capability of users renaming themselves.

1. Sign in to <https://zoom.us/signin>
2. From the navigation panel, select **Account Management** then **Account Settings**.
3. Click the **Meeting** tab.
4. To enable **Allow participants to rename themselves**, click the toggle. In the **Enable "Allow participants to rename themselves"** popup window, click **Enable**.
5. (Optional) If you want to make this setting mandatory for all members of the entire account, click the lock icon  and in  the **Lock "Allow participants to rename themselves"** pop-up window, click **Lock**.