Zoom Security

23.07.2024 04:14:13

FAQ-Artikel-Ausdruck

Kategorie:	Kommunikation & Kollaboration::Video- / Telefonkonferenzen	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	en	**Letzte Aktualisierung:**	10:11:17 - 20.04.2023

Schlüsselwörter

Zoom, Encryption

Lösung (öffentlich)

End-to-end encryption (E2EE)

You can enable encryption for Zoom meetings so that only the participants are able to decrypt the transmitted content. Encryption is especially recommended when particularly sensitive communications are conducted via Zoom meetings.

Requirements for all users
- (free) Zoom account (verified by phone number with valid billing option)
- Use of Zoom Desktop Client or Zoom Mobile App (Version 5.4.0 or higher)

Unavailable features and restrictions
- maximum of 200 participants
- Polling
- Livestreaming
- Join before host
- Join by telephone
- Live-Transcription
- Meeting reactions (available as of version 5.5.0)
- 1:1 private chats (available as of version 5.5.0)

Activation

First, you need to enable the option via [1]Zoom's web interface in your account settings. The link will take you to the settings, where you scroll down to the bottom of the "Security" section. There, enable the "Allow use of end-to-end encryption" option and in the "Default encryption type" setting that appears below that, enable the "End-to-end encryption" option.

For more information, see the [2]Zoom help article.

Tips

To ensure that you can hold your video conferences via Zoom without any interruptions, please note the following instructions.

Create meeting

Make sure that a random identifier is created with the "Generate automatically" option under "Meeting ID", do not use a Personal Meeting ID (PMI) for non-public or ongoing conferences.
The PMI is for your personal meeting room, it does not change. This room is for instant meetings with people you meet with on a regular basis. If your personal meeting is running, anyone who knows the link or PMI of your personal room can join at any time. This can be prevented by locking the meeting or activating the waiting room to control entry.

Regulate access

You can include or exclude participants based on specified regions when scheduling a meeting. Either use the allow or blocklist method here.

Also, make sure that once removed, people cannot rejoin. To do this, the "Allow removed participants to rejoin" option must be disabled in your Zoom settings under "In Meeting (Basic)".

Invitations

You should not distribute the invitation link and identification code of your meeting on public platforms. You can send the invitation data to the participants via secure channels such as e-mail or text message.

Password

Zoom automatically generates an identification code when you schedule a meeting. This code is encrypted and included in the invitation link so that attendees can join the meeting directly without entering the code.

However, it is recommended that you make the passcode available only to a specific group of people and do not make it public. To avoid receiving a link with an embedded password, disable the "Embed the passcode in the one-click join invitation link" option in your Zoom settings in the Meeting section under Security.

Waiting room

If possible, you should always set up a waiting room for meetings with an undefined group of people. Participants do not enter the meeting room directly, but first enter the waiting room. Moderators can then admit or

remove each participant individually from the waiting room into the meeting.

Lock meeting

If the participants are known in advance, you can check whether everyone is present in the meeting. The meeting can then be blocked for further entries. To do this, go to the "Security" item at the bottom left of the menu bar and select the "Lock meeting" item there.

Clear names

Ask participants in advance of the meeting to provide their full clear name. This makes it easier for moderators to remove unwanted guests from the meeting.

Recording

Local and cloud recording is available.
[3]https://tu-dresden.zoom.us/profile/setting , tab 'Recording'.
Only recordings with a normal or high protection level should be stored in the cloud.

For more hints on settings in Zoom, click [4]here (only available in English).

[1] https://tu-dresden.zoom.us/profile/setting
[2] https://support.zoom.us/hc/en-us/articles/360048660871-End-to-end-E2EE-encryption-for-meetings
[3] https://tu-dresden.zoom.us/profile/setting
[4] https://www.eff.org/deeplinks/2020/04/harden-your-zoom-settings-protect-your-privacy-and-avoid-trolls