

Ende-zu-Ende- Verschlüsselung

In Meetings, in denen Ende-zu-Ende-Verschlüsselung aktiviert ist, hat niemand außer dem jeweiligen Teilnehmer Zugang zu den Schlüsseln, die zur Verschlüsselung des Meetings genutzt werden, nicht einmal die Zoom-Server.

Aktivieren der Ende-zu-Ende- Verschlüsselung für Meetings

Da sich Ende-zu-Ende-Verschlüsselung noch in der technischen Vorschau befindet und einige andere Funktionen deaktiviert, wird empfohlen, Ende-zu-Ende-Verschlüsselung nur für Meetings zu nutzen, für die ein zusätzlicher Schutz benötigt wird. Nachdem Sie Ende-zu-Ende-Verschlüsselung aktiviert haben, können Sie Ihre Standardverschlüsselung auswählen.

Benutzer

So aktivieren Sie Meetings mit Ende-zu-Ende-Verschlüsselung zur eigenen Nutzung:

1. Melden Sie sich im Zoom Login Uni Leipzig an.



UNIVERSITÄT
LEIPZIG

Zoom Video Conferencing

Join

An einer Videokonferenz teilnehmen
Connect to a meeting in progress

Host

Eine Videokonferenz beginnen
Start a meeting

Sign in

Ihren Zugang konfigurieren
Configure your account

2. Klicken Sie im Navigationsfenster auf **Einstellungen**.

Profil

Meetings

Persönliche Audiokonferenz

Persönliche Kontakte

Persönliche Geräte

Whiteboards

Notizen

Umfragen

Aufzeichnungen

Clips

Buchungskalender

Einstellungen

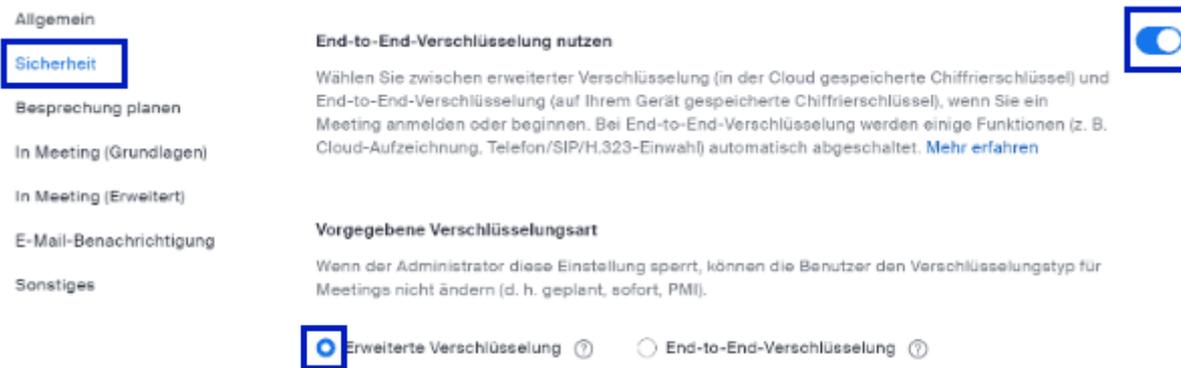
Berichte

Kontoprofil

3. Klicken Sie auf die Registerkarte **Meeting**.

< AI Companion Allgemein **Meeting** Aufzeichnung Calendar Audiokonferenzen Zoom Apps Whiteboard Notizen Clip >

4. Überprüfen Sie unter **Sicherheit**, ob **Nutzung von End-to-End-Verschlüsselung** erlauben aktiviert ist.

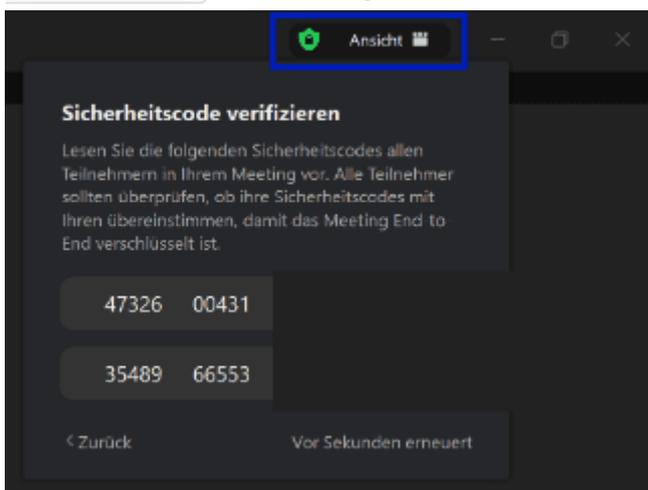


5. Ist die Einstellung deaktiviert, aktivieren Sie diese. Wenn ein Bestätigungsdialogfeld angezeigt wird, klicken Sie auf **Einschalten**, um die Änderung zu bestätigen.

Hinweis: Wird die Option in Grau angezeigt, wurde sie entweder auf Gruppen- oder Kontoebene gesperrt. In diesem Fall müssen Sie sich mit Ihrem Zoom-Administrator in Verbindung setzen.

6. Klicken Sie auf **Speichern**.

Hinweis: Aufgrund der Beschränkungen von Ende-zu-Ende-Verschlüsselung empfehlen wir, **Erweiterte Verschlüsselung** als Standardverschlüsselung auszuwählen und **End-to-End-Verschlüsselung** für Meetings zu nutzen, für die ein zusätzlicher Schutz benötigt wird.



Verwenden der Ende-zu-Ende-Verschlüsselung für Meetings

Sobald Sie dem Meeting beigetreten sind, halten Sie nach dem grünen Schutzschild-Symbol in der oberen linken Ecke des Meetingfensters Ausschau.



Der Meeting-Host kann zudem den Sicherheitscode laut vorlesen, damit die Teilnehmer überprüfen können, ob ihre Codes übereinstimmen.

Verwendungsfälle Ende-zu-Ende-Verschlüsselung

Ende-zu-Ende-Verschlüsselung ist dann die beste Lösung, wenn Sie sich für Ihre Meetings eine verbesserte Privatsphäre und optimalen Datenschutz wünschen. Es ist ein zusätzlicher Risikoschutz, insbesondere für vertrauliche Meetinginhalte. Ende-zu-Ende-Verschlüsselung bietet zwar eine verbesserte Sicherheit, allerdings sind einige Zoom-Funktionen eingeschränkt (siehe oben). Die einzelnen Zoom-Benutzer sollten vor der Aktivierung entscheiden, ob sie diese Funktionen benötigen.

Folgende Funktionen stehen nicht zur Verfügung

- Beitritt vor Moderator
- Cloud-Aufzeichnung
- Livestreaming
- Live-Transkription
- Konferenzräume
- Umfragen
- Zoom Apps
- Meetingreaktionen*
- Private Einzelchats*

Benutzer können nicht per Telefon, von SIP/H.323-Endgeräten, lokalen Konfigurationen, dem Zoom Web Client, Drittanbieter-Clients, die das Zoom SDK nutzen, oder Lync-/Skype-Clients ausbeitreten, da eine End-to-End-Verschlüsselung dieser Endpunkte nicht möglich ist.

Ende-zu-Ende verschlüsselte Meetings sind unabhängig von Large Meeting-Lizenzen auf 200 Teilnehmer begrenzt.

***Hinweis:** Ab Version **5.5.0** für Desktop, Mobile und Zoom Rooms werden diese Funktionen in Ende-zu-Ende-verschlüsselte Meetings unterstützt.