Zoom

Zoom ist eine Software, mit der Videokonferenzen - sogenannte Meetings - mit bis zu 300 Teilnehmern zeitlich unbegrenzt durchgeführt werden können. Neben privaten und öffentlichen Chat-Funktionen und der Übertragung von Video- und Audioquellen bietet Zoom die Möglichkeit zu Bildschirmfreigaben, Umfragen und virtuelle Gruppenräume. So können Sie digitale Lehrveranstaltungen und andere Online-Sitzungen (Gremien, Arbeitsgruppen etc.) umsetzen. Alle Mitglieder der Universität Leipzig können sich im Rahmen der Erfüllung der gesetzlichen Aufgaben der Universität Leipzig mit Ihrem Uni-Login anmelden, eine Videokonferenz einrichten oder an einer teilnehmen.

https://uni-leipzig.zoom.us

Mehr Informationen zu Zoom: https://www.urz.uni-leipzig.de/dienste/videokonferenzen/webkonferenzsystem-zoom/

- Nutzungshinweise
- Hinweise zum Umgang mit Videokonferenzen
- Login
- Ende-zu-Ende-Verschlüsselung
- ZoomInfo Notification

Nutzungshinweise

Anleitungen

Die Homepage des Herstellers Zoom Video Communications, Inc., stellt Ihnen eine Vielzahl von Anleitungen bereit:

https://support.zoom.us/

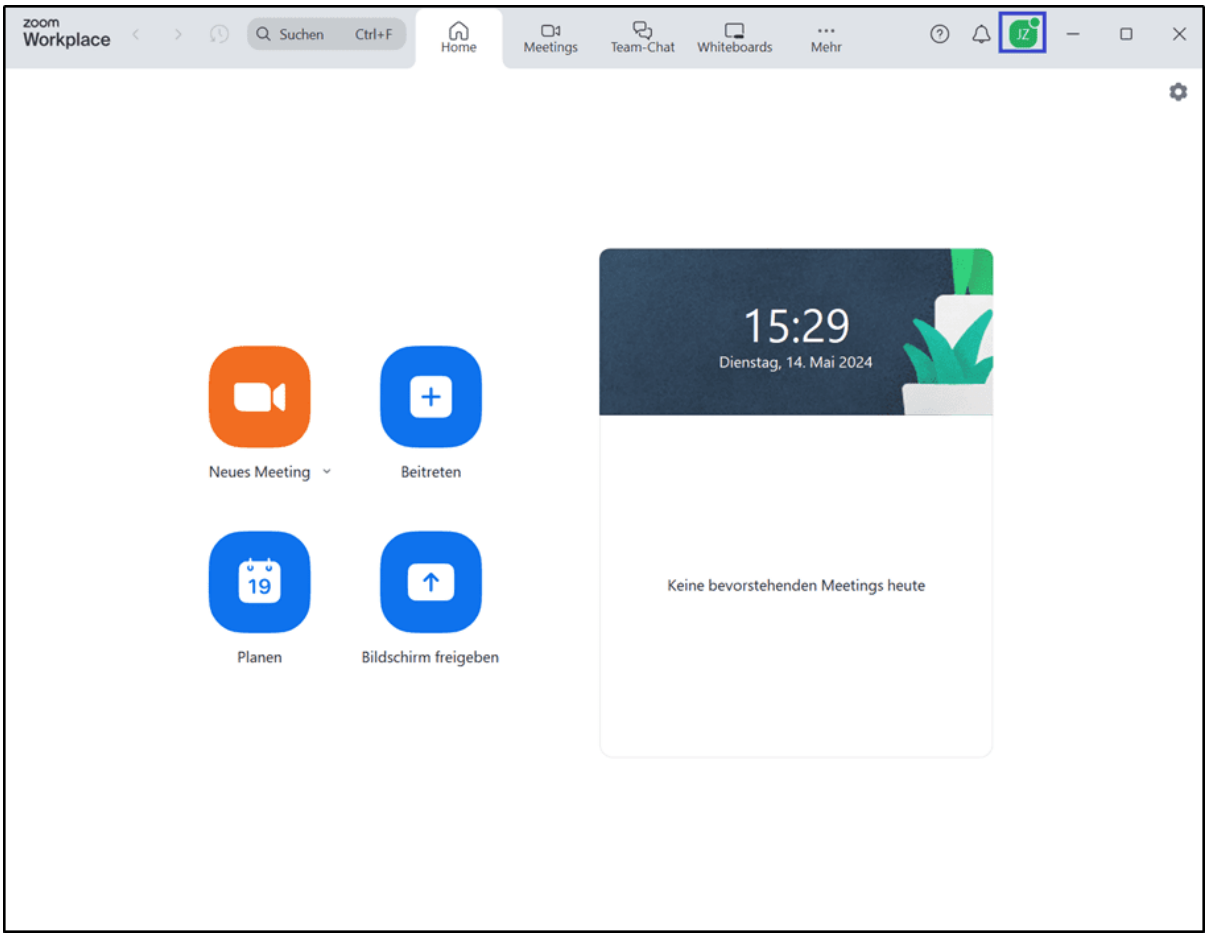
Zudem finden Sie Hier eine Übersicht der verschiedenen Funktionen, die Zoom anbietet.

Lizenz

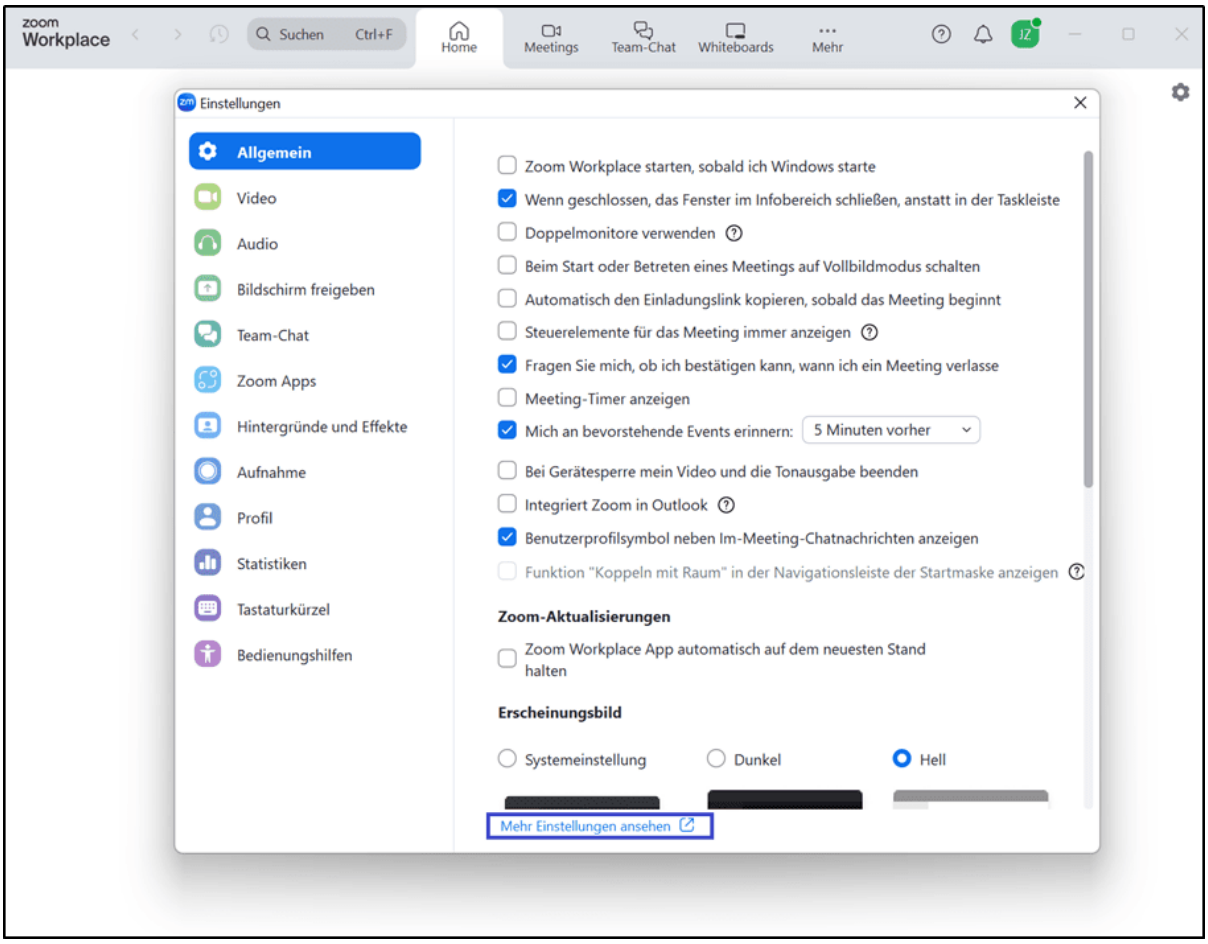
> Standardmäßig verfügen Sie über eine Lizenz für Videokonferenzen bis 300 Teilnehmende. Falls Sie Meetings mit mehr Teilnehmenden veranstalten wollen, gibt es 500 oder 1000 Erweiterungen. Wenden Sie sich dafür bitte an zoom@uni-leipzig.de.

Empfohlene Einstellungen

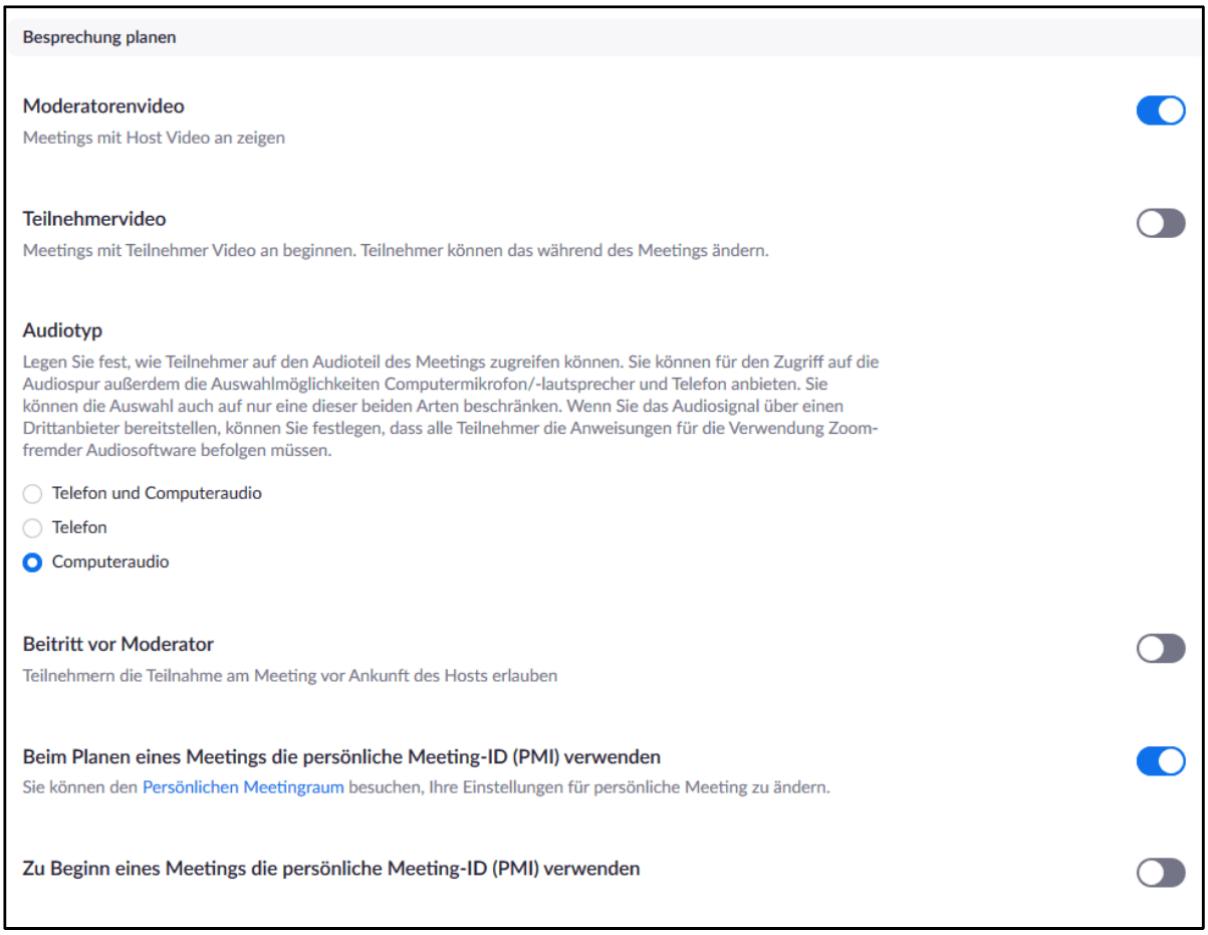
Es gibt einige Einstellungsmöglichkeiten, die wir Ihnen grundsätzlich nahelegen wollen. Bitte beachten Sie jedoch, dass es abhängig von Ihrem Anwendungsfall notwendig sein kann, von diesen Einstellungen abzuweichen.
Klicken Sie im Client oben rechts auf Ihr Profil. Unter mehreren Auswahlmöglichkeiten sollte der Reiter `Einstellungen` zu finden sein.

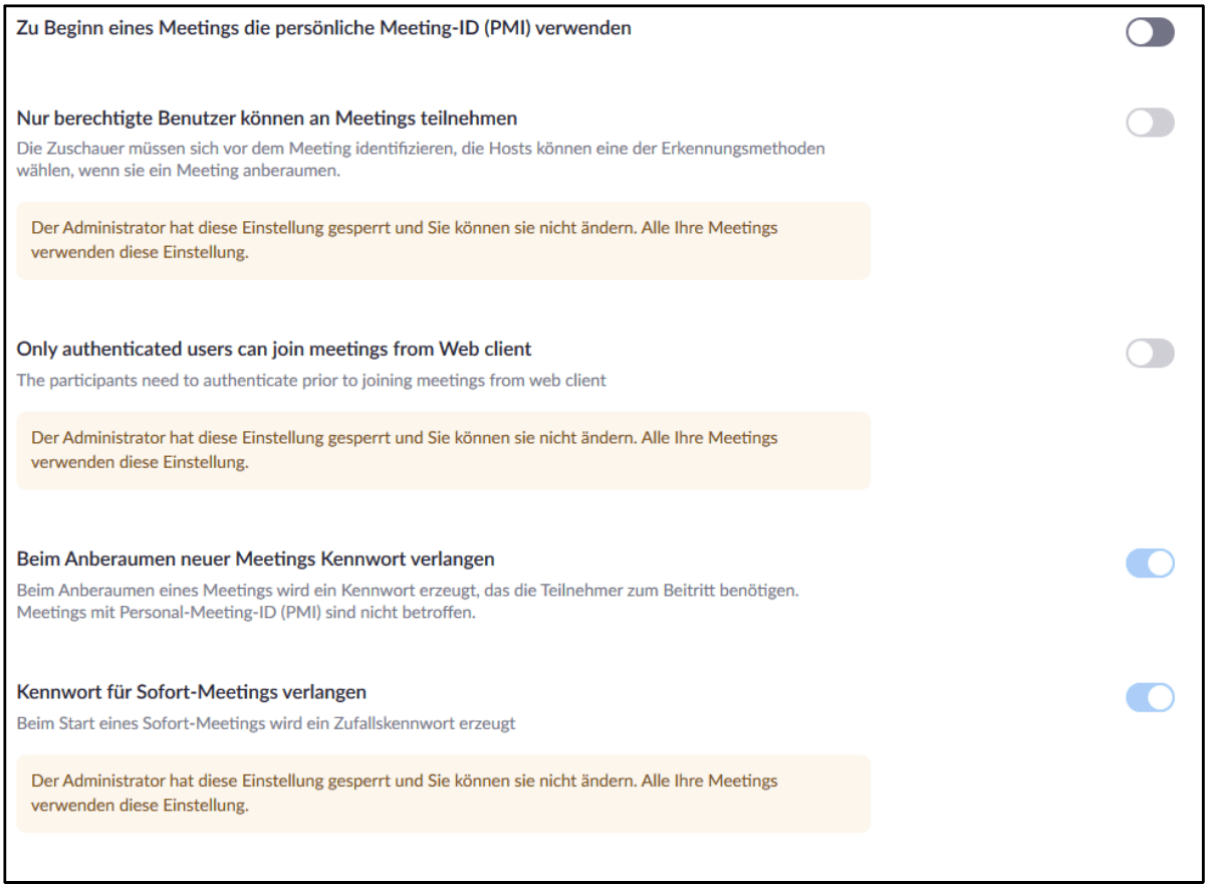


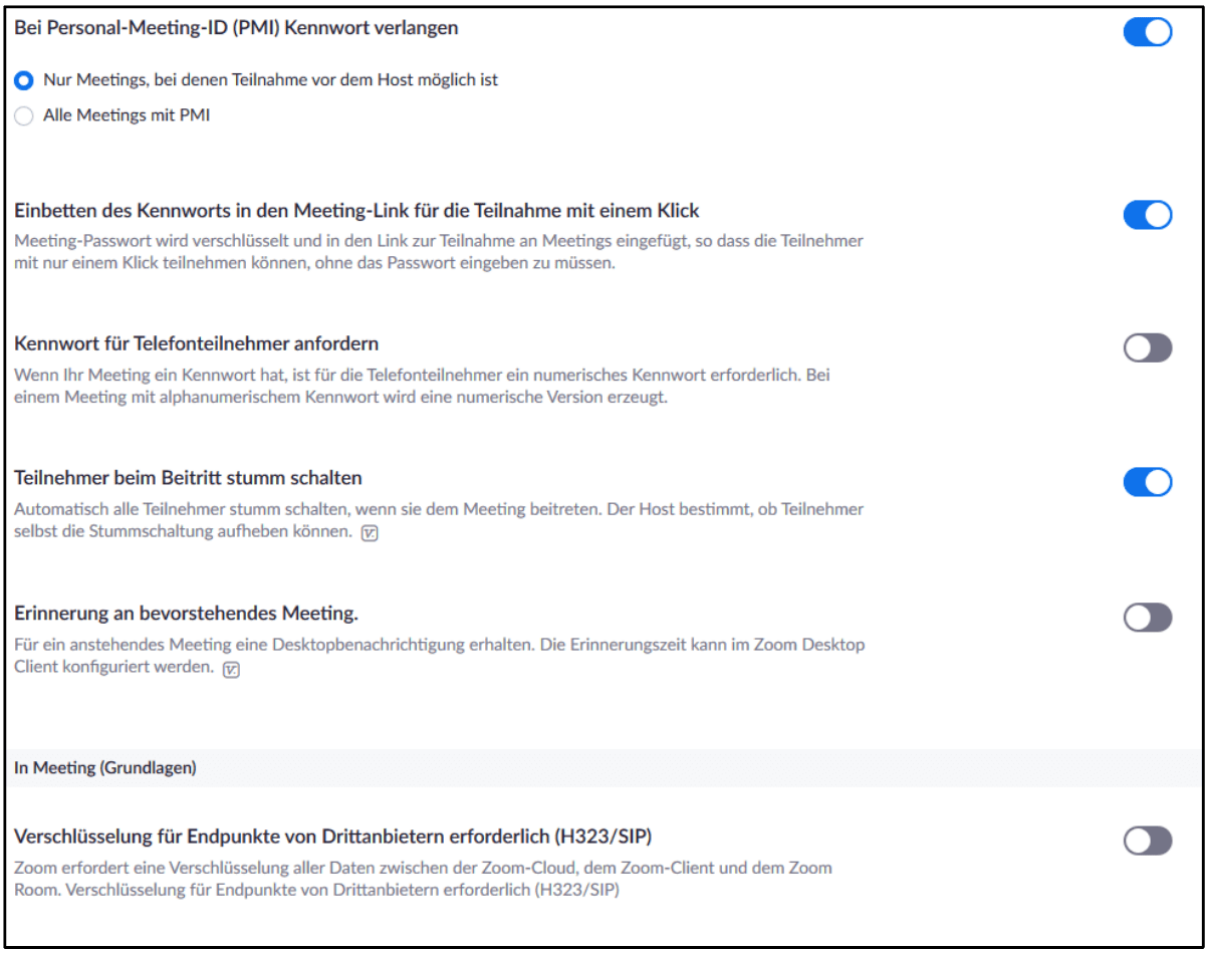
In dem dadurch geöffneten Fenster sehen Sie verschiedenste Konfigurationsmöglichkeiten. Für ausführlichere Einstellungen klicken Sie unter `Allgemein` auf den Link `Mehr Einstellungen ansehen`. Es öffnet sich ein Browserfenster, wo Sie sich gegebenenfalls mit `SSO` anmelden müssen. Sehen Sie hierfür unter der Seite für den Login in der Knowledge Base nach.



Meetings planen


Besprechung planen
Moderatorenvideo
Meetings mit Host Video an zeigen
Teilnehmervideo
Meetings mit Teilnehmer Video an beginnen. Teilnehmer können das während des Meetings ändern.
Audiotyp
Legen Sie fest, wie Teilnehmer auf den Audioteil des Meetings zugreifen können. Sie können für den Zugriff auf die Audiospur außerdem die Auswahlmöglichkeiten Computermikrofon/-lautsprecher und Telefon anbieten. Sie können die Auswahl auch auf nur eine dieser beiden Arten beschränken. Wenn Sie das Audiosignal über einen Drittanbieter bereitstellen, können Sie festlegen, dass alle Teilnehmer die Anweisungen für die Verwendung Zoom-fremder Audiosoftware befolgen müssen.
Telefon und Computeraudio
Telefon
Computeraudio
Beitritt vor Moderator
Teilnehmern die Teilnahme am Meeting vor Ankunft des Hosts erlauben
Beim Planen eines Meetings die persönliche Meeting-ID (PMI) verwenden
Sie können den Persönlichen Meetingraum besuchen, Ihre Einstellungen für persönliche Meeting zu ändern.
Zu Beginn eines Meetings die persönliche Meeting-ID (PMI) verwenden


Zu Beginn eines Meetings die persönliche Meeting-ID (PMI) verwenden
Nur berechtigte Benutzer können an Meetings teilnehmen
Die Zuschauer müssen sich vor dem Meeting identifizieren, die Hosts können eine der Erkennungsmethoden wählen, wenn sie ein Meeting anberaumen.
Der Administrator hat diese Einstellung gesperrt und Sie können sie nicht ändern. Alle Ihre Meetings verwenden diese Einstellung.
Only authenticated users can join meetings from Web client
The participants need to authenticate prior to joining meetings from web client
Der Administrator hat diese Einstellung gesperrt und Sie können sie nicht ändern. Alle Ihre Meetings verwenden diese Einstellung.
Beim Anberaumen neuer Meetings Kennwort verlangen
Beim Anberaumen eines Meetings wird ein Kennwort erzeugt, das die Teilnehmer zum Beitritt benötigen. Meetings mit Personal-Meeting-ID (PMI) sind nicht betroffen.
Kennwort für Sofort-Meetings verlangen
Beim Start eines Sofort-Meetings wird ein Zufallskennwort erzeugt
Der Administrator hat diese Einstellung gesperrt und Sie können sie nicht ändern. Alle Ihre Meetings verwenden diese Einstellung.


Bei Personal-Meeting-ID (PMI) Kennwort verlangen
Nur Meetings, bei denen Teilnahme vor dem Host möglich ist
Alle Meetings mit PMI
Einbetten des Kennworts in den Meeting-Link für die Teilnahme mit einem Klick
Meeting-Passwort wird verschlüsselt und in den Link zur Teilnahme an Meetings eingefügt, so dass die Teilnehmer mit nur einem Klick teilnehmen können, ohne das Passwort eingeben zu müssen.
Kennwort für Telefonteilnehmer anfordern
Wenn Ihr Meeting ein Kennwort hat, ist für die Telefonteilnehmer ein numerisches Kennwort erforderlich. Bei einem Meeting mit alphanumerischem Kennwort wird eine numerische Version erzeugt.
Teilnehmer beim Beitritt stumm schalten
Automatisch alle Teilnehmer stumm schalten, wenn sie dem Meeting beitreten. Der Host bestimmt, ob Teilnehmer selbst die Stummschaltung aufheben können.
Erinnerung an bevorstehendes Meeting.
Für ein anstehendes Meeting eine Desktopbenachrichtigung erhalten. Die Erinnerungszeit kann im Zoom Desktop Client konfiguriert werden.
In Meeting (Grundlagen)
Verschlüsselung für Endpunkte von Drittanbietern erforderlich (H323/SIP)
Zoom erfordert eine Verschlüsselung aller Daten zwischen der Zoom-Cloud, dem Zoom-Client und dem Zoom Room. Verschlüsselung für Endpunkte von Drittanbietern erforderlich (H323/SIP)

In Meeting

In Meeting (Grundlagen)

Verschlüsselung für Endpunkte von Drittanbietern erforderlich (H323/SIP)

Zoom erfordert eine Verschlüsselung aller Daten zwischen der Zoom-Cloud, dem Zoom-Client und dem Zoom Room. Verschlüsselung für Endpunkte von Drittanbietern erforderlich (H323/SIP)

Chat

Meetingteilnehmern erlauben, eine für alle Teilnehmer sichtbare Nachricht zu senden.

- [ ] Verhindert, dass Teilnehmer den Chat speichern

Privater Chat

Meetingteilnehmer können eine private Nachricht an einen anderen Teilnehmer senden.

Chats automatisch speichern

Alle Chats im Meeting automatisch speichern, so dass Hosts den Text des Chats nach Beginn des Meetings nicht manuell speichern müssen.

Sound wiedergeben, wenn Teilnehmer teilnehmen oder verlassen

Sound wiedergeben, wenn Teilnehmer teilnehmen oder verlassen

- ( ) Von Host und allen Teilnehmern gehört
- (•) Wird nur von Moderator gehört

Wenn jeder Teilnehmer über Telefon teilnimmt

- [ ] Aufzeichnen und Abspielen der eigenen Stimme

Dateiübertragung

Hosts und Teilnehmer können Dateien in einem Chat im Meeting senden.

Feedback an Zoom

Eine Registerkarte Feedback zu den Windows Einstellungen oder Dialogfeld Mac Einstellungen hinzufügen und auch Benutzern ermöglichen, Zoom am Ende des Meetings Feedback zu geben

Umfrage für Feedback zum Meeting anzeigen

Am Ende jedes Meetings eine positive/negative Umfrage anzeigen Wenn die Teilnehmer negativ antworten, können sie weitere Informationen darüber abgeben, was falsch gelaufen ist.

- (•) Anzeige für jedes Meeting
- ( ) Anzeige für Meetings nach dem Zufallsprinzip

Co-Moderator

Dem Host erlauben, Co-Hosts hinzuzufügen. Co-Hosts haben dieselben Kontrollen in Meetings wie der Host.

Umfragen

'Umfragen' zu den Kontrollen des Meetings hinzufügen. Dadurch kann der Host die Teilnehmer befragen.

Meeting-Kontrollleiste immer anzeigen

Immer die Meeting Kontrollen während des Meetings zeigen

Zoom-Fenster während der Bildschirmfreigabe anzeigen

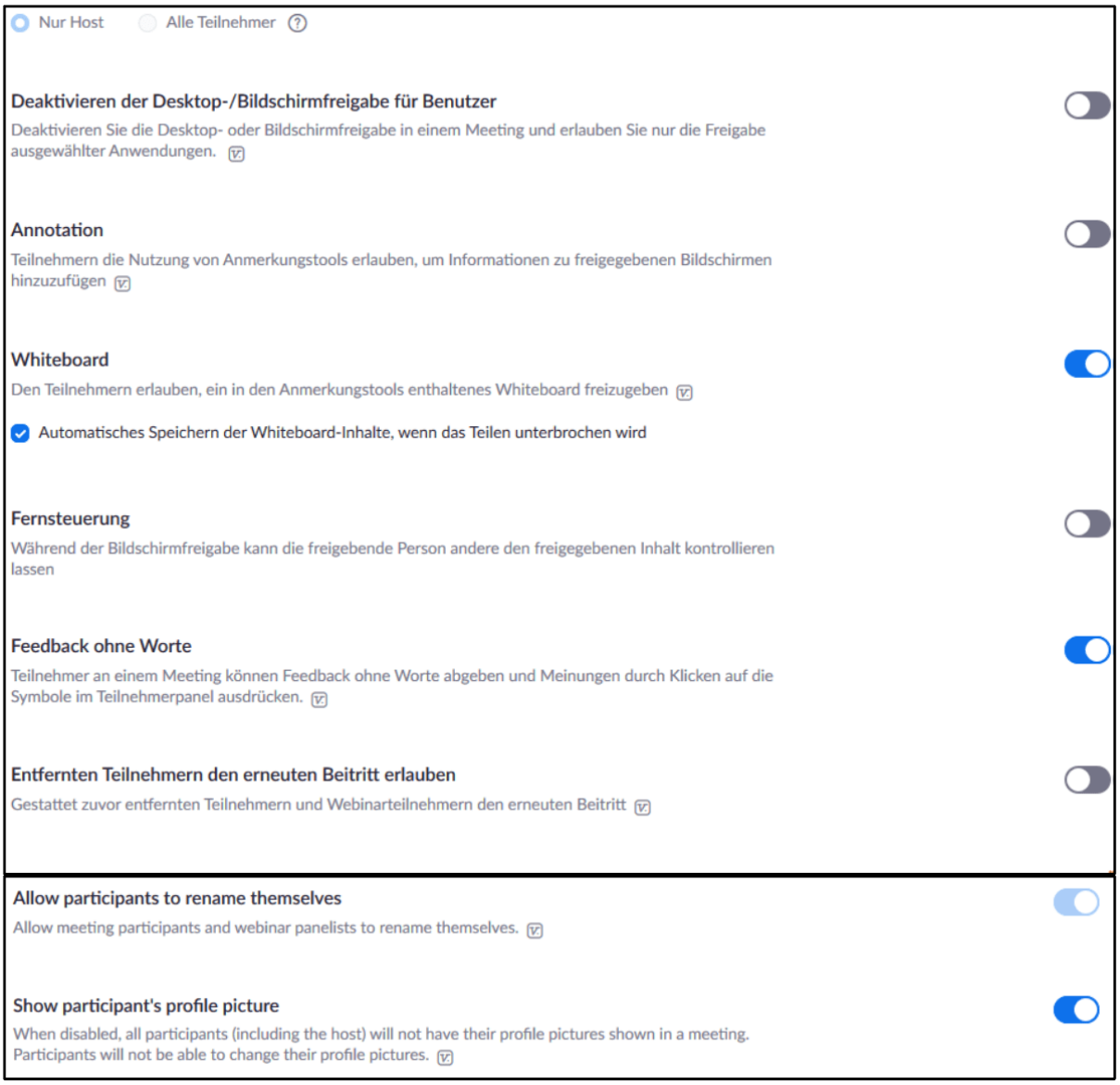
Bildschirmübertragung

Hosts und Teilnehmern erlauben, ihren Bildschirm oder Inhalt während der Meetings freizugeben

Wer kann freigeben?

(•) Nur Host ( ) Alle Teilnehmer

Wer kann die Freigabe starten, wenn eine andere Person die Freigabe verwendet?



In Meeting (Erweitert)

In Meeting (Erweitert)

Give hosts option to report participants to Zoom
Allow hosts to report meeting participants for inappropriate behavior to Zoom's Trust and Safety team for review. This setting can be found on the Security tab on the meeting controls toolbar.

Breakout-Raum
Dem Host erlauben, Meetingteilnehmer in separate, kleinere Räume aufzuteilen

- [x] Hier kann der Host Teilnehmer bei der Planung den Pausenräumen zuordnen

Remoteunterstützung
Dem Meetinghost erlauben, einem anderen Teilnehmer 1:1 Fernsupport zur Verfügung zu stellen

Untertitel
Dem Moderator erlauben, Untertitel einzugeben oder eine Person/ein Drittgerät zu Untertiteln hinzuzufügen

Untertitel speichern
Hier können die Teilnehmer Untertitel oder Transkriptionen speichern

Dolmetschen
Hier kann der Host Teilnehmer als Simultandolmetscher zwischen zwei Sprachen einsetzen. Das ist bei der Terminplanung oder während dem Meeting möglich.

Kamerafernsteuerung
Einem anderen Benutzer erlauben, die Kontrolle über Ihre Kamera während des Meetings zu übernehmen

Virtueller Hintergrund
Benutzern erlauben, ihren Hintergrund mit ausgewählten Bildern zu ersetzen. Ein Bild in den Zoom Desktop Anwendungseinstellungen wählen oder hochladen.

Gastteilnehmer im Meeting/Webinar identifizieren
Teilnehmer auf Ihrem Konto können sehen, dass ein Gast (jemand, der nicht auf Ihrem Konto ist) am Meeting/Webinar teilnimmt. Die Teilnehmerliste zeigt an, welche Teilnehmer Gäste sind. Die Gäste selbst sehen nicht, dass Sie als Gäste aufgeführt sind.

Automatische Antwort Gruppe in Chat
Den Benutzern ermöglichen, Kontakte zu sehen und sie der 'Automatische Antwort Gruppe' in der Kontaktliste auf Chat hinzufügen. Jeder Anruf von Mitgliedern dieser Gruppe wird automatisch beantwortet.

Nur Standard-E-Mail anzeigen, wenn E-Mail-Einladungen gesendet werden
Benutzern erlauben, Teilnehmer nur mit dem auf ihrem Computer ausgewählten Standard-E-Mailprogramm per E-Mail einzuladen

Für Outlook-Plug-in E-Mail im HTML-Format verwenden
HTML Formatierung anstatt Nur-Text für mit dem Outlook Plugin geplante Meeting Einladungen verwenden

Den Benutzern ermöglichen, in ihren Client-Einstellungen Stereoton zu wählen
Benutzern erlauben, Stereo-Audio während eines Meetings zu wählen

Den Benutzern ermöglichen, in ihren Client-Einstellungen den Originalton zu wählen
Benutzern erlauben, Originalton während eines Meetings zu wählen

Select data center regions for meetings/webinars hosted by your account
Include all data center regions to provide the best experience for participants joining from all regions. Opting out of data center regions may limit CRC, Dial-in, Call Me, and Invite by Phone options for participants joining from those regions.

After Apr 25, 2020, China will be deselected by default. If you would like to opt in to China data centers, please turn the toggle on before this date. ×

Warteraum
When attendees join a meeting, place them in a waiting room and require the host to admit them individually.

Vergleich der Einsatzszenarien

Übersicht zu möglichen Einsatzszenarien finden Sie auf der Website des URZ unter

https://www.urz.uni-leipzig.de/unsere-services/services-fuer-lehrende#c561196

Hinweise zum Umgang mit Videokonferenzen

Verbindung

- Bitte achten Sie auf eine stabile Netzverbindung. Um Übertragungsstörungen während der Konferenz zu vermeiden verbinden Sie sich, wenn möglich direkt über Kabel mit Ihrem Router.
- Zu Beginn der Konferenz sollten die Teilnehmenden alle ein Signal geben, dass Sie sich gut untereinander verstehen und sehen können.
- Wenn die Verbindung zu wackelig ist oder zusammenbricht, ist es hilfreich, wenn alle Teilnehmenden ihr Video ausschalten, um Datenvolumen zu reduzieren.

Umgebung

- Bitte halten Sie sich in einer möglichst störungsfreien Umgebung auf. Des Weiteren ist darauf zu achten, die richtigen Lichtverhältnisse zu schaffen, damit alle Teilnehmenden Sie deutlich sehen können.
- Bitte achten Sie darauf keine persönlichen Gegenstände in Sichtweite der Kamera zu haben, die Sie oder die anderen Teilnehmenden stören könnten oder Einsicht in Ihr Privatleben bieten.
- Wenn Sie die Kamera für die Konferenz nicht unbedingt benötigen, schalten Sie sie aus. Somit wird das System deutlich weniger belastet und Sie müssen sich über die zuvor genannten Punkte keine Gedanken machen.
- Achten Sie darauf, ob das Kamerasymbol unten durchgestrichen ist.

Das Mikrofon

- Da Mikrophone nicht zwischen Umgebungsgeräuschen und eigener Stimme unterscheiden ist es ratsam das Mikro, wenn sie nicht an der Reihe sind, stumm zu schalten. So werden die anderen Teilnehmer nicht durch private Gespräche oder Unterbrechungen gestört.

- Hinweis: Die Stummschaltung ist vor allem wichtig, wenn Sie über ihr Smartphone verbunden sind, da dieses besonders empfindlich auf Hintergrundgeräusche reagiert.
- Achten Sie hierbei auf das Mikrofonsymbol unten.

Die Konferenz

- Schalten Sie sich ein paar Minuten früher zu, damit Sie Ton, Licht und Bild überprüfen können.
- Gehen Sie sicher, dass alle Teilnehmer mit dem Ablauf und Themen der Konferenz vertraut sind.
- Beachten Sie die Gesprächsreihenfolge und lassen Sie sich gegenseitig aussprechen. (Mit einem Klick auf Ihren Namen können sie im Status das Handzeichen auswählen).
- Widmen Sie der Konferenz ihre komplette Aufmerksamkeit und vermeiden Sie Nebengespräche.
- Folgen Sie den Verhaltensregeln einer „realen“ Konferenz.

Sicherheit

Jedes Zoom Meeting hat eine eigene, eindeutige Meeting-ID. Dies ist die Zugangsnummer, über die andere Personen Ihr Meeting finden.
Es gibt zwei Arten von Meeting-IDs:

1. Automatisch erzeugte zufällige Meeting-ID.
   Dies ist die Standardeinstellung beim Erstellen von Meetings.
2. Persönliche Meeting-ID (PMI)
   Die PMI ist ein permanenter virtueller Konferenzraum mit einer initial zufälligen Meeting-ID, die Sie nur manuell verändern können.

Die automatisch generierten Meeting-IDs sind datenschutztechnisch sicherer. Falls Sie die PMI dennoch nutzen möchten, nutzen Sie diese nicht für aufeinander folgende Meetings oder große Personengruppen. Sobald ein TN den Link zu Ihrer PMI hat, kann er jederzeit in Ihren persönlichen Konferenzraum eintreten (auch in andere Meetings, die mit dem Zugang stattfinden). Es sei denn, Sie

- sperren das Meeting oder
- verwenden die Funktion Warteraum zur individuellen Aufnahme der TN.

Login

Login über den Browser

Zugang zum Zoom-Service erhalten Sie über https://uni-leipzig.zoom.us/ Zum Login halten Sie bitte Ihren Uni-Login sowie das Passwort bereit. Der Browser führt Sie durch die weiteren Schritte.

Login über den Client

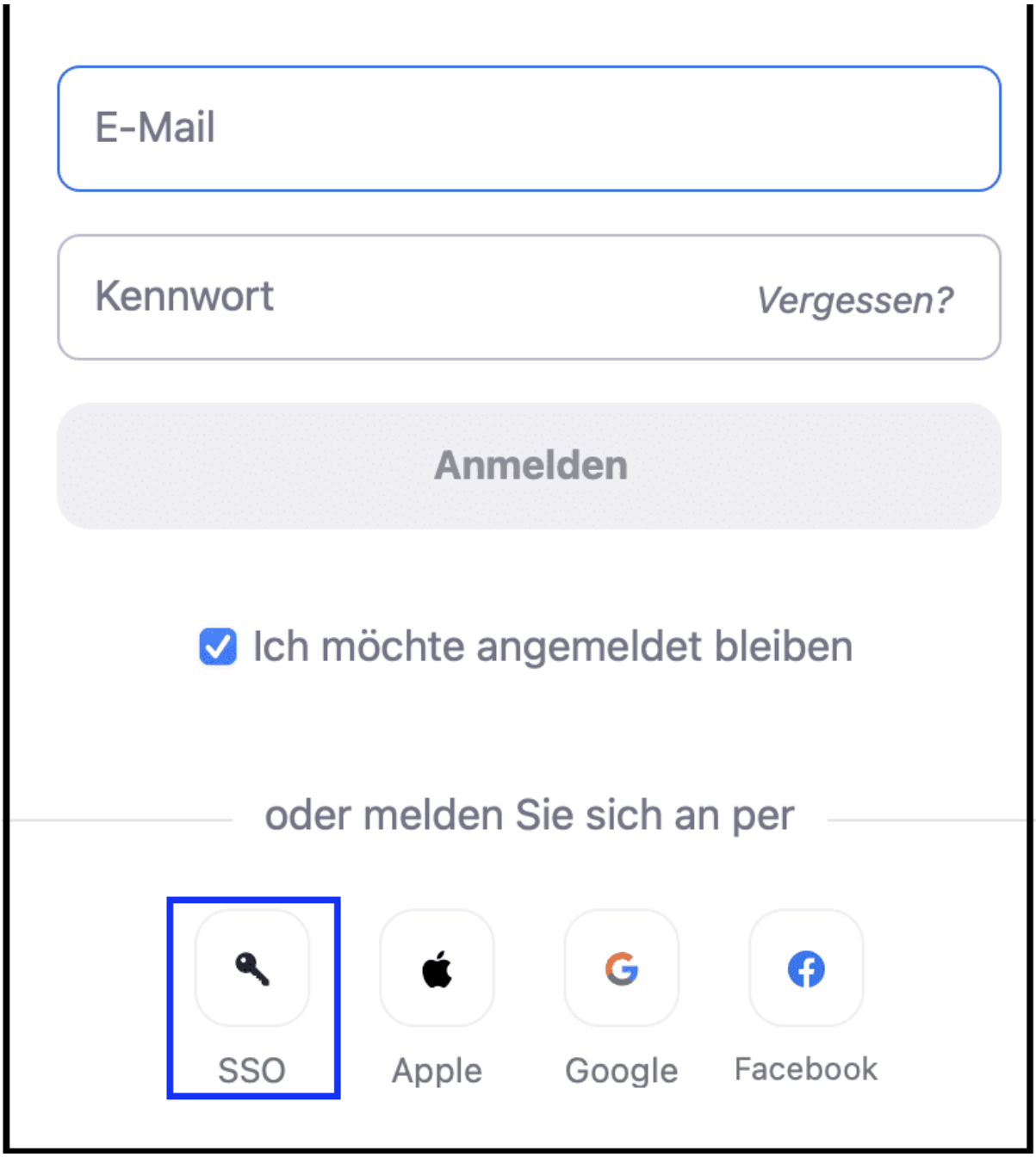
Neben der Nutzung über den Browser können Sie sich auch den Client für Ihren Rechner herunterladen. Der Zoom-Client für folgende Betriebssysteme verfügbar:

- Windows
- macOS
- Android
- iOS/iPadOS

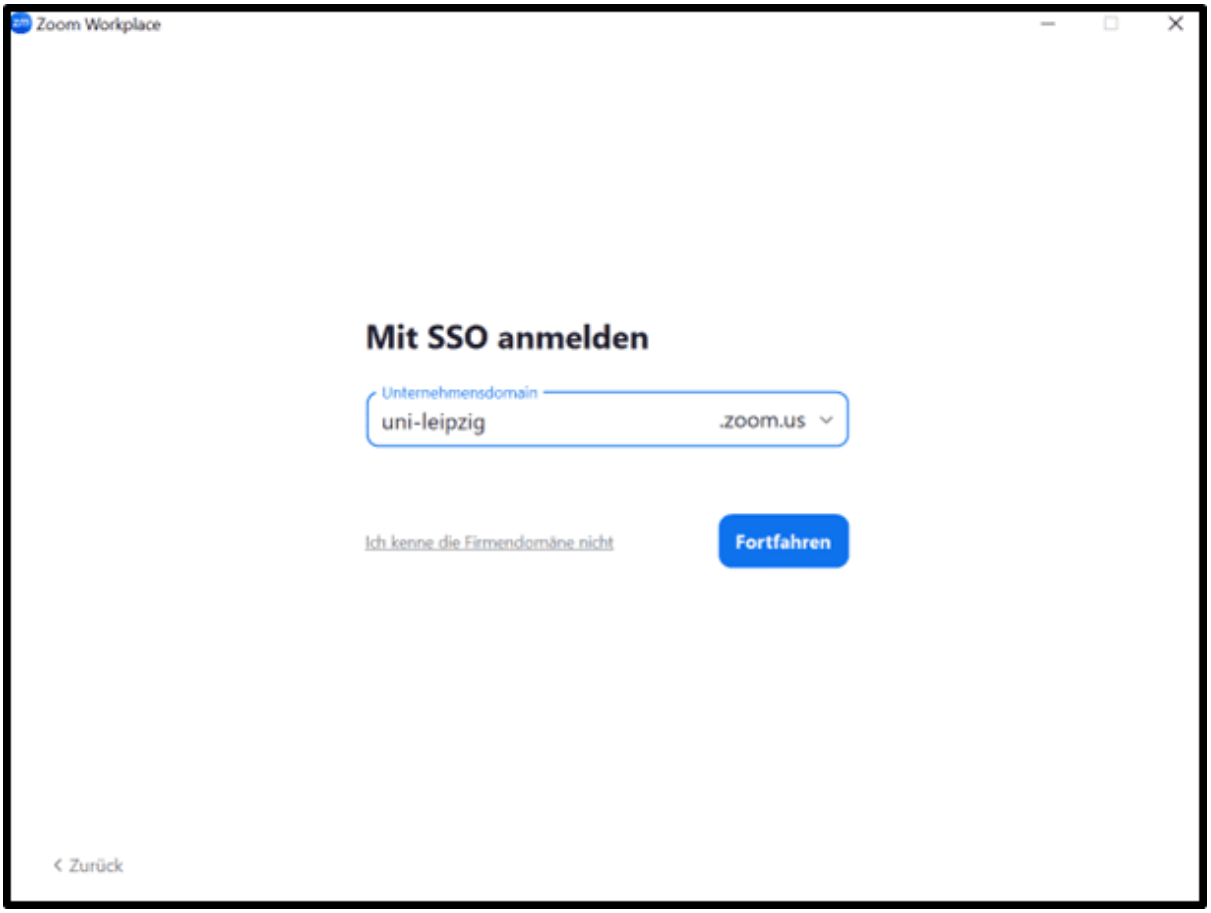
Wir empfehlen die Nutzung des Clients, da diese einen benutzerfreundlichen, direkteren Zugriff auf alle wichtigen Funktionen von Zoom und die Verwaltung Ihrer Meetings über eine eigene Software gewährt.

Nach der Installation des Clients öffnen Sie den Zoom-Client auf Ihrem Rechner.

Es erscheint die Anmeldeoberfläche von Zoom. Klicken Sie auf `SSO`.


E-Mail
Kennwort
Vergessen?
Anmelden
Ich möchte angemeldet bleiben
oder melden Sie sich an per
SSO
Apple
Google
Facebook

Danach werden Sie nach der Unternehmensdomain gefragt. Geben Sie dafür `uni-leipzig` an. Es öffnet sich das gewohnte Anmeldefenster der Universität Leipzig in das Sie Uni-Login und Passwort eingeben.



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

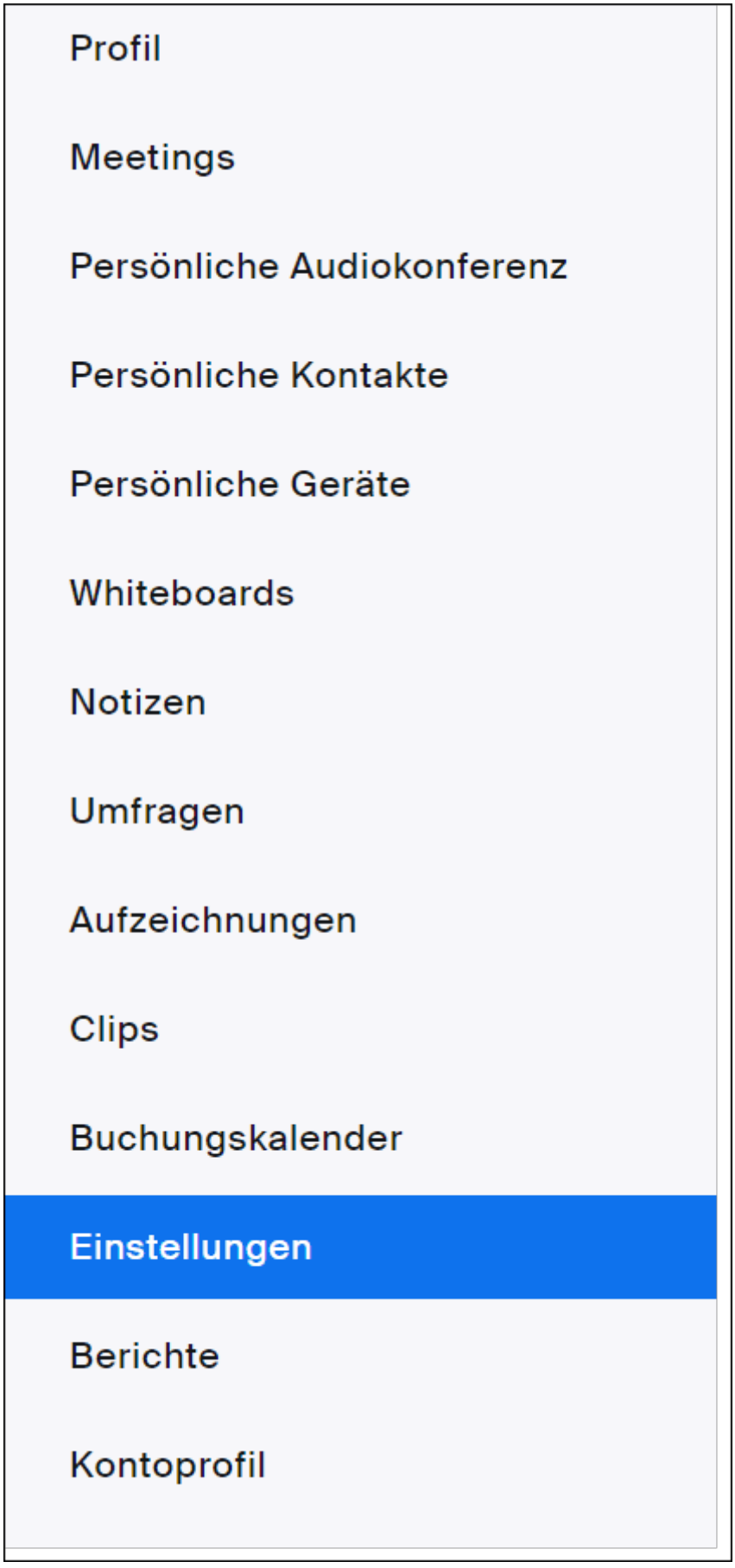
Da sich Ende-zu-Ende-Verschlüsselung noch in der technischen Vorschau befindet und einige andere Funktionen deaktiviert, wird empfohlen, Ende-zu-Ende-Verschlüsselung nur für Meetings zu nutzen, für die ein zusätzlicher Schutz benötigt wird. Nachdem Sie Ende-zu-Ende-Verschlüsselungaktiviert haben, können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

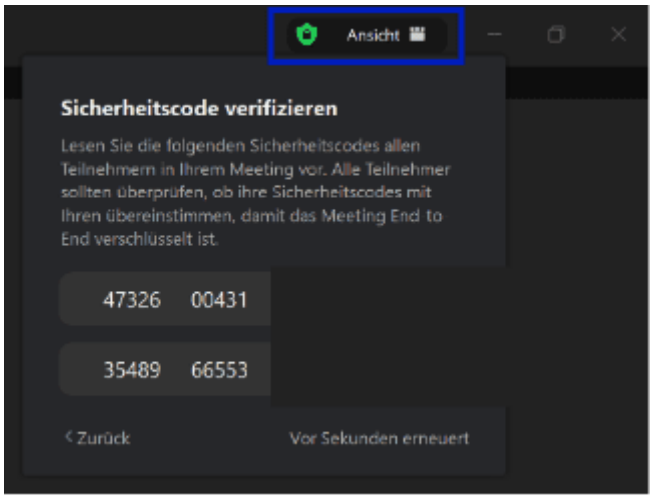
2. Klicken Sie im Navigationsfenster auf **Einstellungen**.



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

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.

Image nc

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 aus beitreten, da eine End-to-End-Verschlüsselung dieser Endpunkte nicht möglich ist.

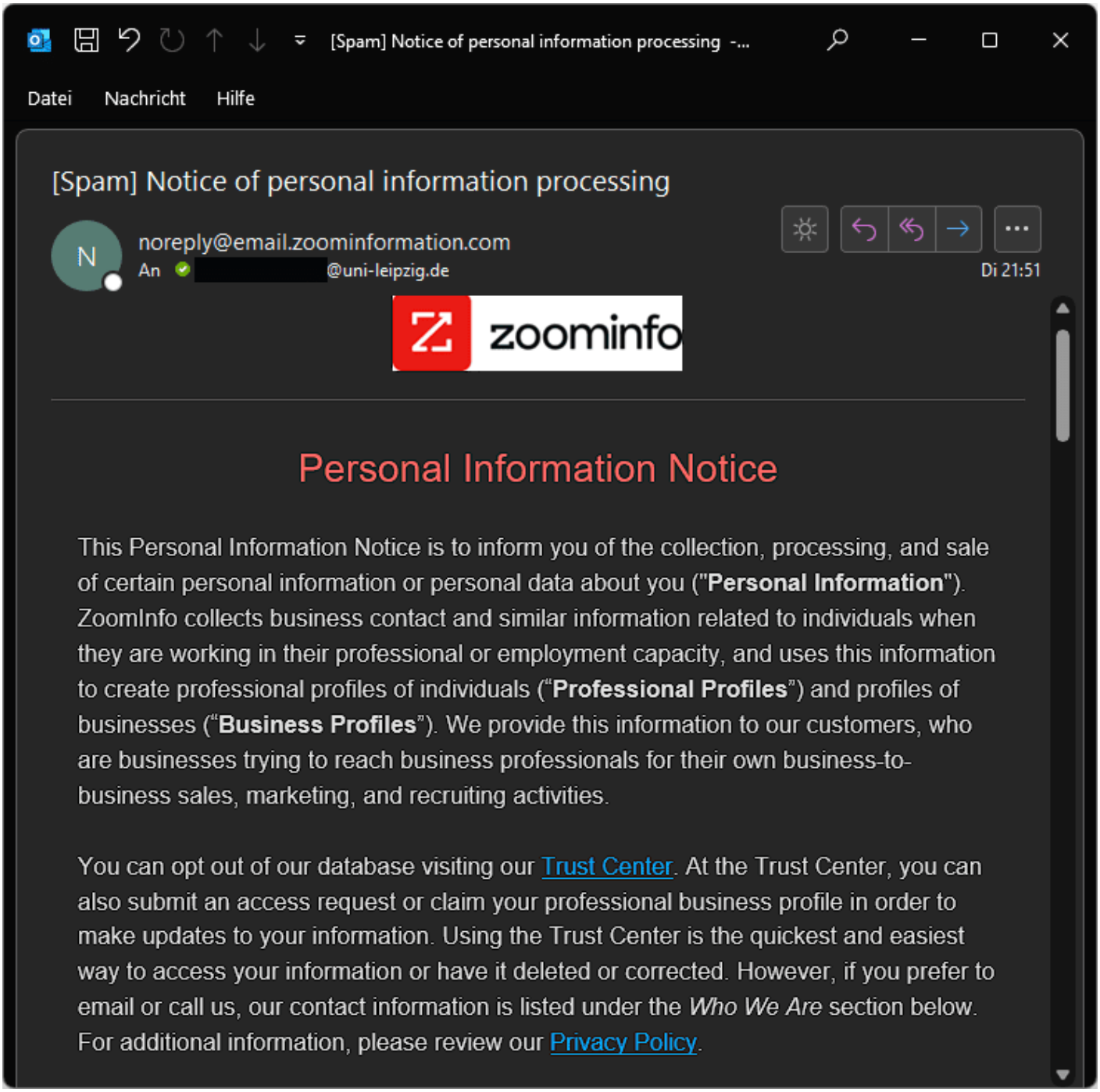
Ende-zu-Ende verschlüsselte Meetings sind unabhängig von Large Meeting-Lizenzen auf 200 Teilnehmer begrenzt.

> *__Hinweis__: Ab Version __5.5.0__ für Desktop, Mobile und Zoom Rooms werden diese Funktionen in Ende-zu-Ende-verschlüsselte Meetings unterstützt.

ZoomInfo Notification

Wenn Sie E-Mails von ZoomInfo Notification erhalten: Diese E-Mails stammen nicht von Zoom. ZoomInfo ist ein Unternehmen, das im Internet verfügbare Informationen über einzelne Personen sammelt und daraus Profile erstellt.

Die E-Mails sind wie folgt aufgebaut:



> Bitte klicken Sie keine Links an! Verschieben Sie diese Mails in den Spam-Ordner Ihres Postfachs.

Es ist ratsam, mit Hilfe von Suchmaschinen zu recherchieren, was und ob das Unternehmen von Ihnen gesammelt hat.