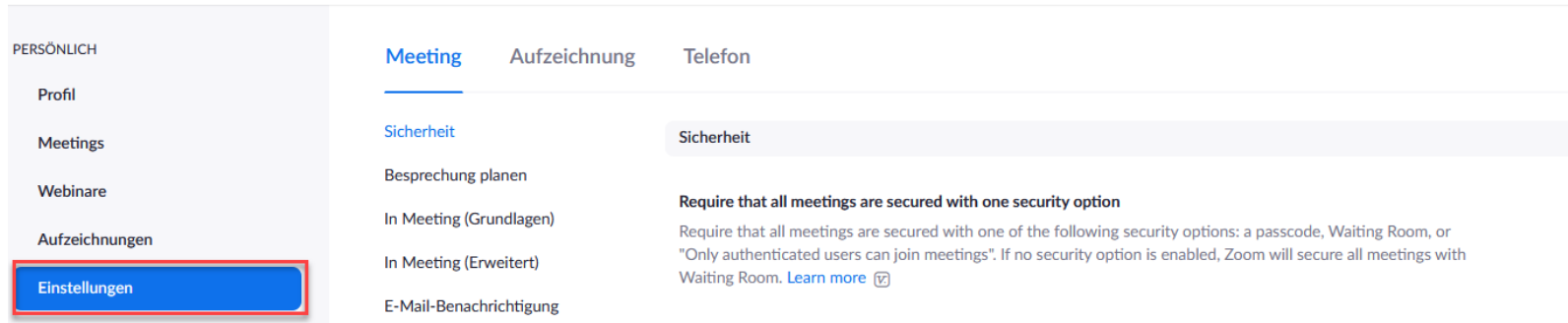


# Empfehlungen Nutzung von Zoom

# Technische Empfehlungen – Grundlegende Einstellungen

- Im Bereich „Einstellungen“ können Lehrende einige Konfigurationen vornehmen:



The screenshot shows the Zoom settings interface. On the left, a sidebar under the heading 'PERSÖNLICH' lists 'Profil', 'Meetings', 'Webinare', 'Aufzeichnungen', and 'Einstellungen'. The 'Einstellungen' item is highlighted with a red border. The main content area has three tabs: 'Meeting' (selected), 'Aufzeichnung', and 'Telefon'. Under the 'Meeting' tab, there is a 'Sicherheit' section. The 'Sicherheit' section is highlighted with a light blue background and contains the following text: 'Require that all meetings are secured with one security option'. Below this, a paragraph explains: 'Require that all meetings are secured with one of the following security options: a passcode, Waiting Room, or "Only authenticated users can join meetings". If no security option is enabled, Zoom will secure all meetings with Waiting Room. [Learn more](#) [icon]'.

# Technische Empfehlungen – Grundlegende Einstellungen

- Chat kann vorab deaktiviert werden, wenn dieser nicht zum Einsatz kommen soll:

## Chat

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

## Privater Chat

Meetingteilnehmer können eine private Nachricht an einen anderen Teilnehmer senden.



- Sofern der Chat aktiviert ist, kann verhindert werden, dass Chat gespeichert wird:

## Chat

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



Verhindert, dass Teilnehmer den Chat speichern 

# Technische Empfehlungen – Grundlegende Einstellungen

- Sofern keine Dateien übertragen werden sollen, kann folgende Einstellung vorgenommen werden:

## Dateiübertragung

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



- Auch die Bildschirmfreigabe kann durch folgende Konfigurationen eingeschränkt werden:

## 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?

Nur Host  Alle Teilnehmer 

Speichern

Abbrechen

## Technische Empfehlungen – Grundlegende Einstellungen

- Störer/-innen können durch folgende Funktion dauerhaft aus Meetings ausgeschlossen werden:

**Entfernten Teilnehmern den erneuten Beitritt erlauben**

Gestattet zuvor entfernten Teilnehmern und Webinar Teilnehmern den erneuten Beitritt 



- Sollen TN sich nicht mehr umbenennen können, kann folgende Einstellung vorgenommen werden:

**Teilnehmern erlauben, sich umzubenennen**

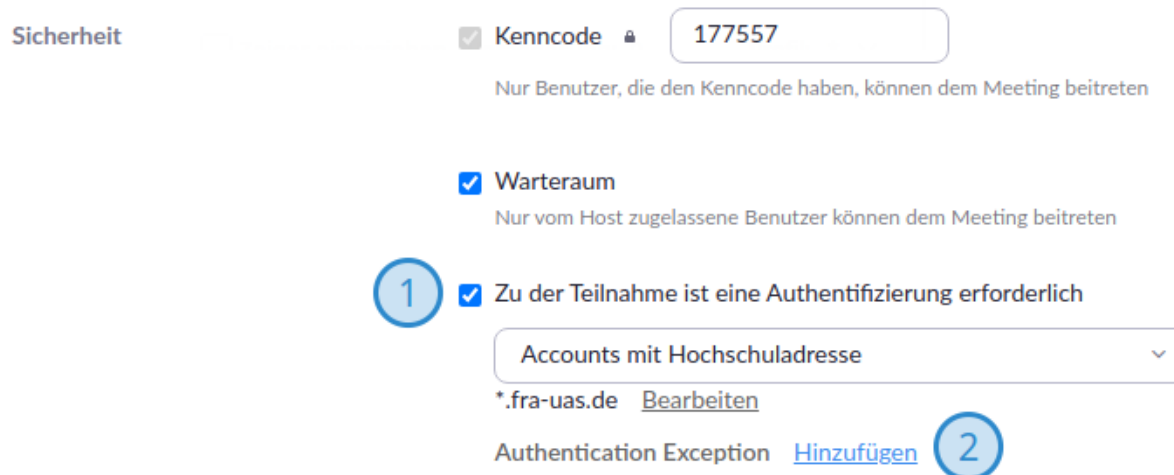
Erlauben Sie den Meetingteilnehmern und Diskussionsteilnehmern der Webinare, sich selbst umzubenennen. 




## Technische Empfehlungen – Meeting planen

**Meeting planen: Authentifizierung (Geht nur über <https://fra-uas.zoom.us/> und nicht über den Client!)**

- Wenn Sie Ihr Meeting planen, können Sie einstellen, dass nur Personen, die in Zoom mit Ihrem Hochschul-Account angemeldet sind, an Ihrem Meeting teilnehmen können. **Bitte beachten Sie, dass Sie mit dieser Einstellung ggf. verhindern, dass externe Personen (z. B. Gäste) an Ihren Meetings teilnehmen können.**



Sicherheit

Kenncode 

Nur Benutzer, die den Kenncode haben, können dem Meeting beitreten

Warteraum

Nur vom Host zugelassene Benutzer können dem Meeting beitreten

**1**  Zu der Teilnahme ist eine Authentifizierung erforderlich

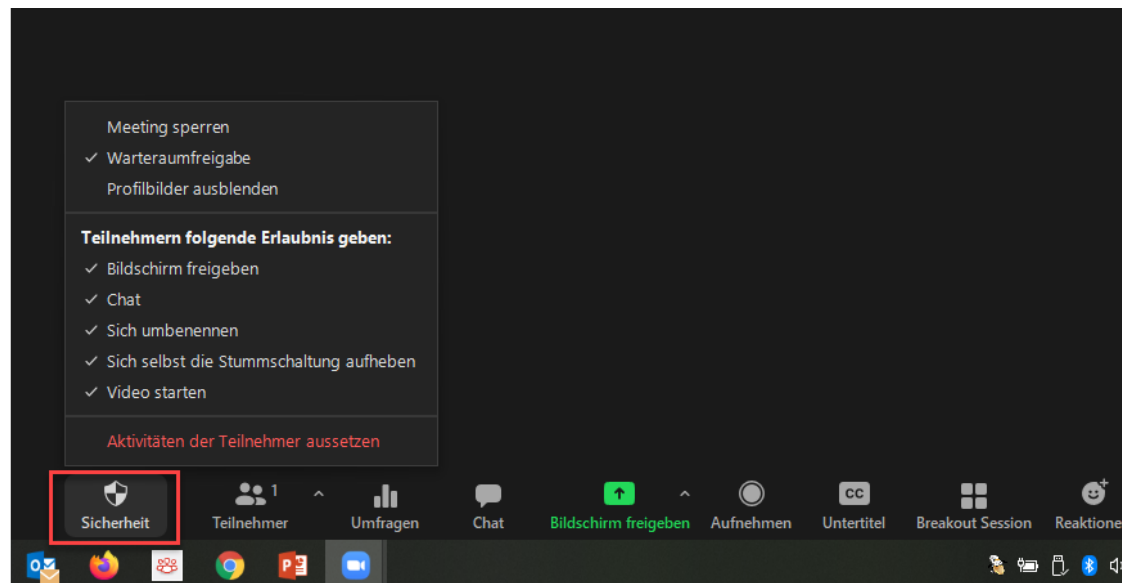
\*.fra-uas.de [Bearbeiten](#)

Authentication Exception [Hinzufügen](#) **2**

- Sobald Sie in einem Meeting eine Authentifizierung fordern (sieh Screenshot, Markierung 1), haben Sie die Möglichkeit Authentication Exception hinzuzufügen (Markierung 2). Klickt man dort auf Hinzufügen, können einzelne Namen/E-Mail Adressen als Ausnahmen deklariert werden.

## Technische Empfehlungen – Im Meeting

- Während des Meetings können Sie über den Sicherheitsbutton folgende Sicherheitseinstellungen vornehmen:



## Weitere Ideen und Empfehlungen

- Hinweis auf [House-Keeping](#) Rules, Confluence [Seite „Umgang mit Störer\\*innen“](#) oder [Etikette in Webmeetings](#) (S. 10-11) z. B. in Moodle Kurs oder erster Lehrveranstaltung
- Machen Sie Screenshots der Vorfälle
- Sofern möglich, zweite Person vorsehen, um z. B. den Chat zu beobachten, Störer/-innen zu in den Warteraum zu setzen (z. B. Studierende, Tutoren)
- Bei großen TN-Zahl abwägen, ob Aufzeichnung (z. B. über Panopto) oder Streaming (z. B. über Panopto in Moodle-Kurs) nicht sinnvoller als Zoom-Live-Meeting