

Zoom-Einstellungen für die DSGVO-EKD-konforme Nutzung

Bei Rückfragen wenden Sie sich gerne an Landesonlinepfarrer Andreas Erdmann:

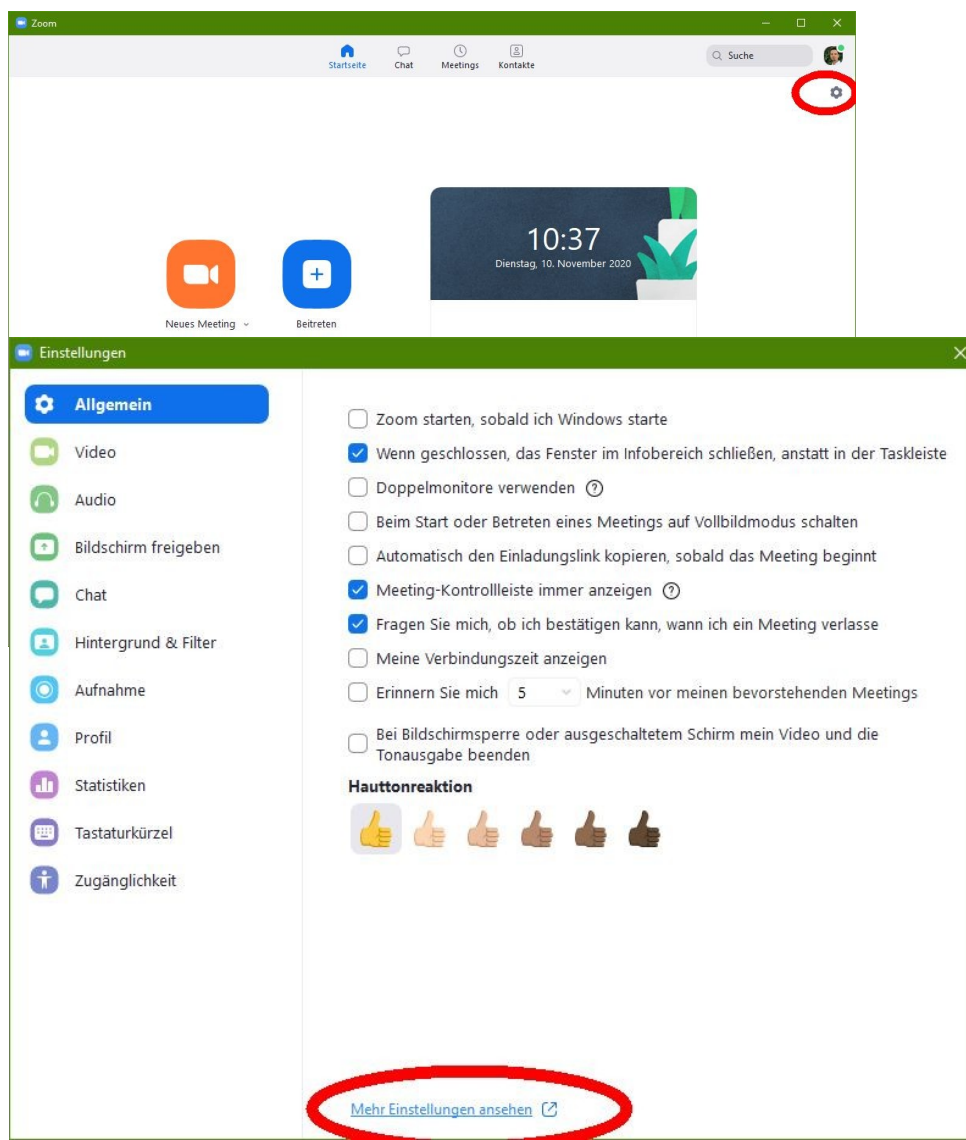
E-Mail: a.erdmann@ekbo.de, Instagram: @loppreist, Telefon: 030-243 44-382, Signal: 01511 84 66 457

Standardmäßig verläuft der Datenverkehr der Zoom-Teilnehmenden über die us-amerikanischen Server von Zoom.us und sind auch nicht DSGVO-EKD konform. Der deutsche Anbieter Connect4Video hat sich dem Datenschutzgesetz der EKD (DSG-EKD) unterworfen und bietet entsprechende Einstellungsmöglichkeiten an, um den Datenverkehr über die europäische Infrastruktur laufen zu lassen. Den Account nur über Connect4Video zu beziehen genügt allein noch nicht. Sie müssen die Einstellungen zunächst manuell für den Benutzertypen auf „lokal“ (onPrem) setzen, ansonsten besteht kein Unterschied zu einem bei Zoom.us bezogenen Account.

Aber auch das alleine genügt noch nicht, weil der Hauptdatenstrom standardmäßig dennoch über us-amerikanische Server von Zoom läuft. Daher sind weitere Sicherheitseinstellungen notwendig, um die Cloud-Dienste von Zoom zu deaktivieren und die Ende-zu-Ende-Verschlüsselung zu aktivieren, die dann auch das Abgreifen von Metadaten durch Zoom.us unterbindet. Im Folgenden sind die Einstellungen für Sie einmal aufgeführt.

Nachdem Sie Zoom über Connect4Video bezogen haben, kommen Sie jederzeit über Ihren Zoom-Client zum Webinterface mit den erweiterten Einstellungen. Gehen Sie dazu wie folgt vor:

1. Öffnen Sie den Client, melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Kennwort an und klicken Sie anschließend oben rechts auf das kleine Zahnrad:



2. Klicken Sie

unten auf den Link für die erweiterten Einstellungen:

Daraufhin öffnet sich Ihr Browser und navigiert zur Homepage von Zoom. Dort melden Sie sich erneut mit Ihrer E-Mail-Adresse und Ihrem Kennwort Ihres Zoom-Accounts an.

3. Zunächst einmal ist es wichtig, dass Sie die Benutzereigenschaften ändern. Klicken Sie dafür im Menü links unter „Admin“ auf „Benutzer“ und dort ganz rechts bei Ihrem Account auf „Bearbeiten“:

Benutzer To add licensed users to your account, please purchase more licenses. Dokument

Benutzer Ausstehend Erweitert

Suche Erweiterte Suche Importieren Export + Benutzer hinzufügen

<input type="checkbox"/>	E-Mail/Namens-ID	Vorname	Nachname	Rolle	Typ	Abteilung	
<input type="checkbox"/>				Verantwortlicher	Lokal		<input type="button" value="Bearbeiten"/>

< 1 > 15/Seite 1 Ergebnisse

4. Nun können Sie den Benutzertypen auf „Lokal“ stellen, um ihn über die lokalen (europäischen) Server von Connect4Video hosten zu lassen.

Benutzer bearbeiten

E-Mails

Benutzertyp Basic Lizenziert Lokal Großes Meeting Webinar

Abteilung

Stellenbezeichnung

Ort

5. Bitte erweitern Sie auch die Kennwortrichtlinien im Menü unter „Admin“, „Sicherheit“ mindestens um das Erzwingen von Sonderzeichen als Teil des Kennwortes, um die Gefahr vor Brute-Force- und Dictionary-Attacken zu verringern.

Webinare
Aufzeichnungen
Einstellungen

ADMIN

- > Benutzerverwaltung
- > Raumverwaltung
- > Kontoverwaltung
- ▼ **Erweitert**
- App-Markt
- H.323/SIP Room Connector
- Meeting Connector
- Branding
- Sicherheit**
- Einmaliges Anmelden (SSO)
- Integration

Grundlegende Anforderungen an das Kennwort

- Mindestens 8 Zeichen
- Mindestens 1 Buchstaben (a, b, c,...) beinhalten.
- Mindestens 1 Zahl (1, 2, 3...) beinhalten.
- Auch Groß- und Kleinbuchstaben enthalten

Erweiterte Kennwortbedingungen

- Passwort muss eine Mindestlänge haben
- Mindestens 1 Sonderzeichen (!, @, #...) beinhalten.
- Darf keine bestimmten Zeichen beinhalten (z. B. "11111"; "12345"; "abcde" oder "qwertz")
- Erweiterte Erkennung schwacher Kennwörter benutzen ?

Kennwortrichtlinie

- Neue Benutzer müssen ihr Kennwort bei der ersten Anmeldung ändern.
- Passwörter laufen automatisch ab und müssen nach einer bestimmten Anzahl an Tagen geändert werden
- Benutzer können kein Passwort weiterverwenden, das in der vorherigen Anzahl von Fällen benutzt worden ist
- Benutzer können ihr Passwort alle 24 Stunden eine maximale Anzahl ändern

6. Weiter unten in der Rubrik Anmeldeverhalten deaktivieren Sie bitte außerdem die Option, dass sich Nutzer*innen mit ihrem Facebook- oder Google-Konto anmelden:

Anmeldeverhalten

Benutzern erlauben, sich mit ihrer E-Mail-Adresse anzumelden
Erlaubnis erteilen, dass Benutzer sich mit ihrer dienstlichen E-Mail-Adresse anmelden können

Benutzern erlauben, sich mit ihrem Google-Konto anzumelden
Erlaubnis erteilen, dass Benutzer sich mit ihrem Google-Konto anmelden können

Benutzern erlauben, sich mit ihrem Facebook-Konto anzumelden
Erlaubnis erteilen, dass Benutzer sich mit ihrem Facebook-Konto anmelden können

Benutzern erlauben, sich mit ihrer Apple-ID anzumelden
Erlaubnis erteilen, dass Benutzer sich mit ihrer Apple-ID anmelden können

Haftungshinweis anzeigen, wenn Benutzer sich bei Zoom anmelden

7. Grenzen Sie sicherheitshalber die Teilnahmemöglichkeit aus anderen Ländern auf solche Länder ein, von denen Sie Teilnehmende erwarten. In den meisten Fällen könnte es hier sogar reichen, ausschließlich Deutschland auf die Liste der erlaubten Länder zu setzen. Wichtig ist in jedem Fall, dass Sie die durchgehende Verschlüsselung für Meetings (E2E) aktivieren und den Verschlüsselungstyp auf „end-to-end-encryption“ setzen, um zu verhindern, dass Metadaten an Zoom gesendet werden.

Sicherheit


Besprechung planen

In Meeting (Grundlagen)


In Meeting (Erweitert)


E-Mail-Benachrichtigung

Sonstiges

Approve or block entry to users from specific regions/countries 

Determine whether users from specific regions or countries can join meetings/webinars on your account by adding them to your Approved List or Blocked List



Allow only users from: Deutschland, Norwegen, Belgien, Finnland, Schweiz, Dänemark, Litauen, Luxemburg, Kroatien, Lettland, Schweden, Österreich, Polen, Niederlande 

Durchgehend (E2E) verschlüsselte Meetings Technical Preview 


Die durchgängige Verschlüsselung bietet zusätzliche Sicherheit, da nur Sie und Ihre Meetingteilnehmer das Meeting entschlüsseln können, Zoom und andere Dritte aber nicht. Durchgängig verschlüsselte Meetings verfügen derzeit nicht über Cloud-basierte Funktionen wie Cloud-Aufzeichnung, Telefoneinwahl und andere.

Default encryption type


If the admin locks this setting, users will not be able to change the encryption type for meetings (i.e. scheduled, instant, PMI).

Enhanced encryption  End-to-end encryption 

Besprechung planen

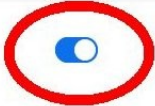










Moderatorenvideo 

Meetings mit Host Video an zeigen

Teilnehmervideo 

Meetings mit Teilnehmer Video an beginnen. Teilnehmer können das während des Meetings ändern.

8. Sie können sicherheitshalber auch die Verschlüsselung für die Endpunkte von Drittanbietern aktivieren, auch wenn Sie keine Kommunikation zu Drittanbietern haben dürften. In jedem Fall unterbinden Sie bitte die Feedbackfunktion an Zoom:

Sicherheit	In Meeting (Grundlagen)	
Besprechung planen	Verschlüsselung für Endpunkte von Drittanbietern erforderlich (SIP/H.323) Zoom erfordert in der Regel eine Verschlüsselung aller Daten, die zwischen der Zoom-Cloud, dem Zoom-Client und dem Zoom Room übermittelt werden. Setzen Sie diese Einstellung, um Verschlüsselung auch für Endpunkte von Drittanbietern vorzuschreiben (SIP/H.323)	
In Meeting (Grundlagen)		
In Meeting (Erweitert)	Chat Meetingteilnehmern erlauben, eine für alle Teilnehmer sichtbare Nachricht zu senden.	
E-Mail-Benachrichtigung	<input type="checkbox"/> Verhindert, dass Teilnehmer den Chat speichern 	
Sonstiges	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.	
	Ton abspielen, wenn jemand einsteigt oder geht	
	Dateiübertragung Hosts und Teilnehmer können Dateien in einem Chat im Meeting senden. 	
	<input type="checkbox"/> Nur bestimmte Dateitypen zulassen 	
	<input type="checkbox"/> Maximum file size 	
	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	

9. Unter den persönlichen Einstellungen für das Meeting können Sie sicherstellen, dass für alle Meetings ein Kenncode erforderlich ist. Zudem können Sie den Warteraum aktivieren, der es Ihnen ermöglicht, zu verhindern, dass sich ungebetene Gäste automatisch in ihre Sitzung einklinken können, sobald sie die Zugangsdaten dafür erhalten haben (sinnvoll z.B. für Einzelgespräche zu bestimmten Sprechstundenzeiten).

PERSÖNLICH

- Profil
- Meetings
- Webinare
- Aufzeichnungen
- Einstellungen**

ADMIN

- > Benutzerverwaltung
- > Raumverwaltung
- > Kontoverwaltung
- > Erweitert

An Live-Schulung teilnehmen
Videotutorials
Wissensdatenbank

Meeting Aufzeichnung Telefon

Sicherheit

Besprechung planen

In Meeting (Grundlagen)

In Meeting (Erweitert)

E-Mail-Benachrichtigung

Sonstiges

Sicherheit

Wartezimmer

Wenn Teilnehmer einem Meeting beitreten, setzen Sie sie in einen Warteraum und weisen Sie den Host an, sie einzeln einzulassen. Wenn Sie den Warteraum freigeben, wird die Einstellung für den Eintritt von Teilnehmern vor dem Host automatisch gesperrt.

Warteroptionen

Die hier ausgewählten Optionen gelten für Meetings, die von Benutzern moderiert werden, bei denen 'Warteraum' eingeschaltet ist

✓ Alle will go in the waiting room

[Edit Options](#) [Customize Waiting Room](#)

Meetingkenncode

Alle direkten und angemeldeten Meetings, an denen Benutzer über Client, Telefon oder Raumsysteme teilnehmen dürfen, werden durch einen Kenncode geschützt.

Kenncode für Personal Meeting-ID (PMI)

Alle Meetings mit Persönlichen Meeting-IDs (PMI), an denen Benutzer über Client, Telefon oder Raumsysteme teilnehmen dürfen, werden durch einen Kenncode geschützt.

Passcode: ***** [Show](#) [Bearbeiten](#)

Kenncode für Telefonteilnehmer anfordern

Wenn Ihr Meeting einen Kenncode hat, ist er für die Telefonteilnehmer in numerischer Form erforderlich. Bei einem Meeting mit alphanumerischem Kenncode wird eine numerische Version erzeugt.

10. Grenzen Sie bitte auch die Rechenzentren, über die der Host laufen soll, auf Deutschland ein:

Sicherheit

Besprechung planen

In Meeting (Grundlagen)

In Meeting (Erweitert)

E-Mail-Benachrichtigung

Sonstiges

Wählen Sie Bereiche des Rechenzentrums für Meetings/Webinare aus, die von Ihrem Konto aus moderiert werden
Schließen Sie alle Bereiche der Rechenzentren ein, damit die Teilnehmern aus allen Bereichen den bestmöglichen Eindruck gewinnen. Das Auslassen von Rechenzentrumsbereichen kann die CRC-, Einwahl, Anruf- und telefonischen Einladungsoptionen für Teilnehmer aus diesen Bereichen einschränken.

- Australien
- Brasilien
- Kanada
- China
- Deutschland
- Hongkong SAR
- Indien
- Irland
- Japan
- Niederlande
- Singapur
- USA

Einen Link "Von Ihrem Browser teilnehmen" zeigen
Teilnehmern erlauben, das Herunterladen der Zoom Anwendung zu umgehen und an einem Meeting direkt von ihrem Browser teilzunehmen. Das ist eine Übergangslösung für Teilnehmer, die keine Anwendungen heruntergeladen, installieren oder ausführen können. Beachten Sie, dass das Meetingerlebnis vom Browser begrenzt ist.

Livestreaming der Meetings zulassen

Show a custom disclaimer when starting or joining a meeting
Create your own disclaimer that will be shown at the start of all meetings hosted by your account

11. Damit auch die Aufzeichnungen des Meetings nicht auf den us-amerikanischen Servern von Zoom in der Cloud gespeichert werden, deaktivieren Sie bitte die Cloud-Dienste. Sie finden diese Einstellung im Menü rechts unter „persönlich“, „Einstellungen“ und dann oben unter dem mittleren Reiter „Aufzeichnung“:

PERSONLICH

- Profil
- Meetings
- Webinare
- Aufzeichnungen
- Einstellungen**

ADMIN

- > Benutzerverwaltung
- > Raumverwaltung
- > Kontoverwaltung
- > Erweitert

An Live-Schulung teilnehmen

Videotutorials

Wissensdatenbank

Meeting **Aufzeichnung** Telefon

Aufzeichnung

Lokale Aufzeichnung
Hosts und Teilnehmern erlauben, das Meeting auf einer lokalen Datei aufzuzeichnen

- Hosts können Teilnehmern die Genehmigung zur lokalen Aufzeichnung erteilen

Cloud-Aufzeichnung
Hosts erlauben, Meeting/Webinar aufzuzeichnen und in der Cloud zu speichern

Automatische Aufzeichnung
Meetings bei Beginn automatisch aufzeichnen

IP-Adresszugriffskontrolle
Beschränkt den Zugriff auf die Cloud-Aufzeichnung auf bestimmte IP-Adressbereiche

Nur berechtigte Benutzer können Cloud-Aufzeichnungen einsehen.
Die Zuschauer müssen sich vor dem Ansehen der Cloud-Aufzeichnungen identifizieren, die Hosts können eine der Erkennungsmethoden wählen, wenn sie eine Cloud-Aufzeichnung teilen.

Geschafft! Die restlichen Optionen gehen Sie am besten einmal ganz in Ruhe durch und schauen sich an, was Sie davon für Ihre Arbeit benötigen. So können Sie hier z.B. auch Funktionen wie das Whiteboard oder Breakout-Rooms (de-)aktivieren.