easymeet24
by Connect4Video

in cooperation with zoom

Stand: Juli 2020

Sichere Zoom Meetings

Als deutsche Unified Communication Plattform bietet easymeet24 eine Reihe von Möglichkeiten, Ihre wichtigen Meetings bestmöglich zu schützen. Unsere Server betreiben wir in D-A-CH nach deutschem Datenschutzrecht. Außerdem sind Zoom-Meetings grundsätzlich verschlüsselt. Zusätzlich können die Hosts und Co-Hosts in Ihrem Unternehmen vor, während und nach dem Meeting wichtige Einstellungen zu Privatsphäre und Datensicherheit vornehmen. Viele Optionen kann der Administrator sogar im Voraus für den gesamten Account, bestimmte Gruppen oder einzelne Nutzer festlegen.

Wichtig: Damit Ihre Meetings tatsächlich nur über unsere Connect4Video-Server stattfinden, müssen Ihre Nutzer auf „On-Prem (Lokal)“ eingestellt sein (s. Seite 2).

Vor dem Meeting

Passwortgeschützte Meetings: Vor dem Eintritt in ein Meeting muss jeder Nutzer ein Passwort eingeben. Das Passwort wird automatisch mit der Einladung generiert. Die Passwort-Option lässt sich auch für Telefonteilnehmer aktivieren.

Teilnahme vor Host deaktivieren: Ein Host kann verhindern, dass Teilnehmer vor ihm den Meetingraum betreten und das Treffen ohne ihn beginnen. Dies bietet zusätzliche Sicherheit und mehr Kontrolle über die Meetingräume.

Warteraum: Bevor die Teilnehmer ins Meeting dürfen, müssen sie im Warteraum bleiben, bis der Host einzelnen oder allen den Eintritt gewährt.

Nur angemeldete Zoom-Nutzer / spezifische Domains dürfen beitreten: Admins können festlegen, dass nur angemeldete Zoom-Nutzer an den Meetings teilnehmen dürfen, bei Bedarf sogar nur solche mit bestimmten E-Mail-Domains.

Während des Meetings

Meeting abschließen: Hosts und Co-Host können weitere Beitritte zum Meeting unterbinden, sogar wenn Nutzer Meeting-ID und Passwort kennen. Ideal, um sensible Meetings abzuschotten.

Teilnehmer entfernen: Hosts können Teilnehmer entfernen, wenn diese nicht im Meeting erwünscht sind.

Fremde Teilnehmer identifizieren: Teilnehmer, die nicht im Unternehmens-Account registriert sind, werden in der Teilnehmerliste mit Orange gekennzeichnet.

Einzelne Anwendung teilen: Anstatt ihren gesamten Bildschirm preiszugeben, können Teilnehmer die Freigabe auf einzelne Anwendungen beschränken. Admins können das Teilen des Bildschirms sogar komplett unterbinden.

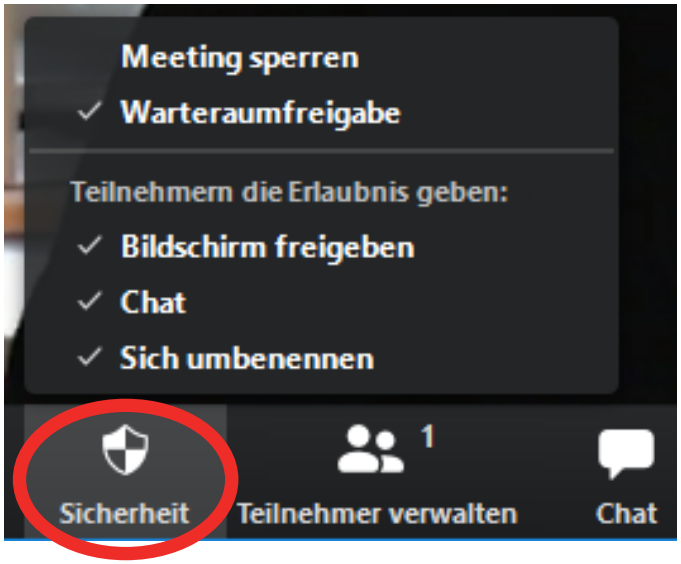
Nach dem Meeting

Sicheres Recording: Mitschnitte von Meetings lassen sich passwortgeschützt in der Zoom Cloud speichern. Zudem kann der Zugriff auf bestimmte Domains beschränkt werden.

Sowohl der Zoom Client als auch das Backend bieten viele Möglichkeiten, Zoom Meetings sehr sicher zu machen. Doch nicht alle Nutzer oder Administratoren nehmen sich die Zeit, alle Einstellungen entsprechend vorzunehmen. Daher hat Zoom im April 2020 einige Maßnahmen ergriffen, um Meetings per Grundeinstellung stärker abzusichern. Außerdem stehen dem Host eines Meetings nun die wichtigsten Einstellungen in der Menüleiste mit einem Klick zur Verfügung.

Einstellungen im Client

Das Sicherheits-Icon sieht nur der Host des jeweiligen Meetings. In der Abbildung rechts sehen Sie, welche Einstellungen per Default ein- und ausgeschaltet sind.



Meeting sperren: Dem Meeting können keine weiteren Teilnehmer beitreten.

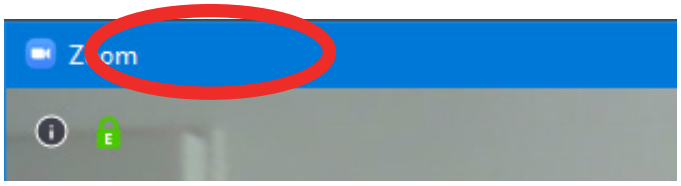
Warteraumfreigabe: Neue Teilnehmer werden zunächst in einen Warteraum geleitet. Der Host bekommt gleichzeitig eine Meldung und kann nun die Erlaubnis zum Eintritt ins Meeting geben.

Bildschirm freigeben: Um zu verhindern, dass Teilnehmer unerwünscht Inhalte teilen, kann die Bildschirmfreigabe blockiert werden.

Chat: Teilnehmer können sich normalerweise während des Meetings Textnachrichten über den internen Chat zusenden. Auch dies lässt sich abschalten.

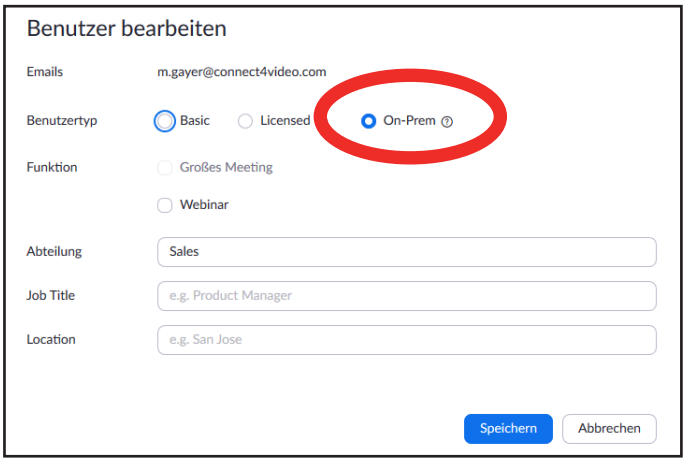
Sich umbenennen: damit lässt sich verhindern, dass sich Teilnehmer während eines Meetings umbenennen und so eventuell sogar eine falsche Identität vortäuschen.

Als weitere Maßnahme wurde die **Meeting-ID** aus der Kopfzeile des Zoom-Fensters entfernt, damit beim Teilen eines Screenshots die ID nicht öffentlich bekannt wird.



Einstellungen im Backend

Wichtig: User auf „On-Premises“ stellen: Dies ist Voraussetzung dafür, dass Ihre Meetings auf den Servern von Connect4Video in D-A-CH laufen. Gehen Sie in Ihrem Sie in Ihrem Profil zu Admin -> Benutzerverwaltung -> Benutzer. Klicken Sie bei dem betreffenden Benutzern auf „Bearbeiten“ und aktivieren Sie dann die Option „On-Prem (Lokal)“ .

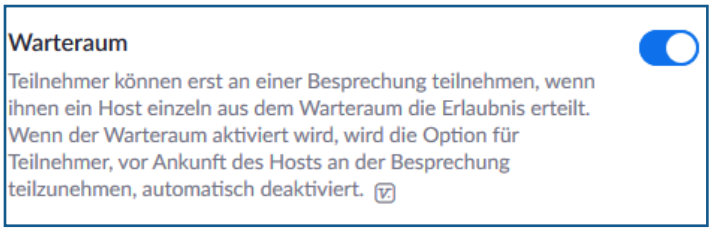


Weitere Einstellungen im Zoom Backend

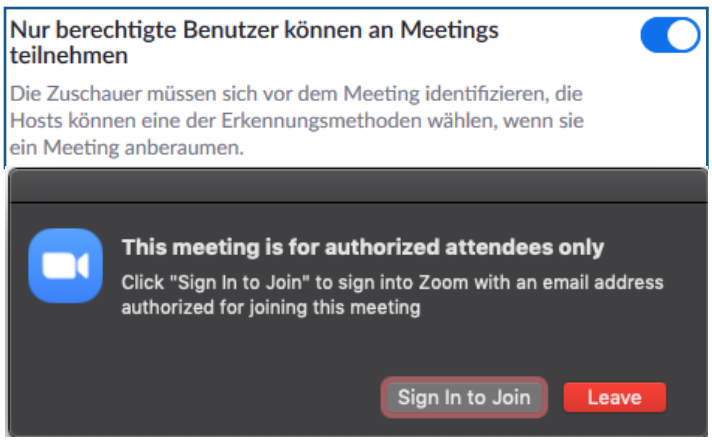
Die Meeting-Einstellungen finden Sie in Ihrem Profil unter
„Persönlich -> Einstellungen“
Hier einige Beispiele für die wichtigsten Sicherheitsmaßnahmen.

Es ist in allen Basic- und Pro-Accounts mit nur einer Lizenz per Default festgelegt, dass Teilnehmer den Meetingraum nur mit einem Passwort betreten können. Dies ist möglich für geplante und spontane Meetings sowie für Meetings, bei denen die persönliche Meeting-ID verwendet wird. Es lassen sich Passwort-Details festlegen, etwa die minimale Länge und erlaubte Sonderzeichen.

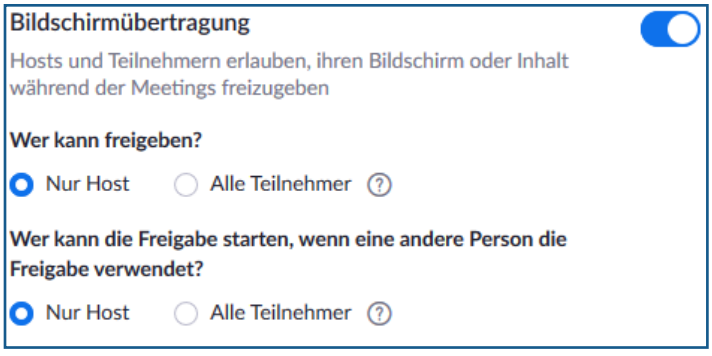
Der Warteraum ist per Default eingeschaltet. Neu hinzugekommen Teilnehmer müssen hier warten, bis der Host den Eintritt gewährt.



Der Eintritt Unbefugter lässt sich auch verhindern, indem nur die eingeladenen Teilnehmer zugelassen werden. Dazu müssen sie in Zoom mit der E-Mail-Adresse eingeloggt sein, an welche die Einladung ging.



Wenn Sie nicht möchten, dass Teilnehmer ungewünscht Bildschirminhalte teilen, können Sie bestimmen, dass nur der Host seinen Bildschirm freigeben darf.



Weitere Infos finden Sie hier in den **Release-Notes**.