ZOOM : LUTTER CONTRE LES ACTES DE MALVEILLANCE

Objectif : Prévenir et combattre les actes de malveillance sur Zoom

Préambule

Ce tutoriel a pour objectif de sécuriser les interactions entre vous et vos étudiants sur Zoom, ainsi que de vous donner des pistes pour réagir en cas de dérive.

Même si les incidents de malveillance restent extrêmement marginaux, dès lors qu'on permet une interaction (micro, vidéo, partage d'écran, annotation) une action de malveillance peut se produire. C'est via le le paramétrage que vous pourrez éviter ces actes. Toutefois, il n'y a pas de paramétrage absolu, celui-ci dépendra du contexte et des usages qui sont les vôtres.

Pour bénéficier de toutes les fonctionnalités de sécurité de Zoom, nous vous recommandons très fortement d'utiliser l'application de bureau Zoom et de la mettre à jour régulièrement. Certaines fonctionnalités détaillées dans ce tutoriel n'apparaissent que suite à une mise à jour de Zoom (donc si vous ne les voyez pas c'est que votre application de bureau Zoom doit être mise à jour).

Note : Si vous ne savez pas comment mettre à jour Zoom, veuillez-vous référer au tutoriel dédié.

Prévenir les actes de malveillance : Le paramétrage à mettre en place avant la réunion

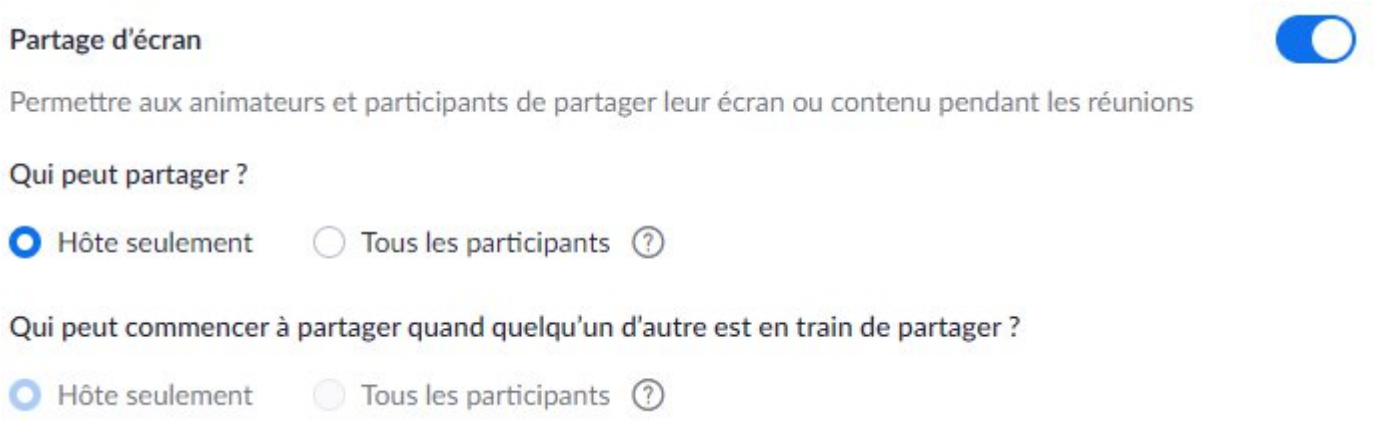
L'ensemble des paramétrages globaux (qui s'appliqueront à toutes les réunions) sont accessibles depuis le client web : https://univ-grenoble-alpes-fr.zoom.us/profile/setting

Vous accéderez également à une liste de paramètres avancés disponibles uniquement depuis ce lien. Ces paramétrages ne sont pas définitifs et pourront être modifiés en cours de réunion.

1. Le partage d'écran

Exemple d'acte de malveillance : diffusion d'une vidéo inappropriée.

Nous vous recommandons de ne permettre le partage d'écran que pour l'Hôte.



Ainsi, les étudiants ne pourront pas partager leur écran et diffuser des contenus malveillants.

Si vous avez des intervenants dans votre réunion ou un autre collègue pour lequel vous souhaitez autoriser le partage, nous vous recommandons de nommer ces personnes co-animateurs. Et de veiller à ne pas autoriser le partage à tous les participants (cela permettrait aux étudiants de prendre le contrôle).

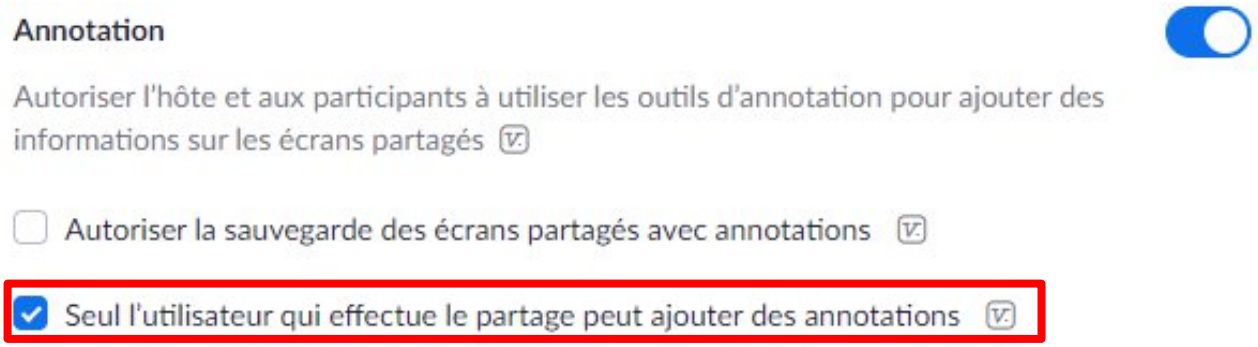
Néanmoins, cela implique que le paramétrage « Co-animateur » soit activé.

Le co-animateur aura également la main sur un ensemble de contrôles en cours de réunion (couper le micro d'un participant, le déplacer en salle d'attente, couper sa vidéo, etc.). Plus d'informations sur les contrôles ici.

2. Les annotations lors d'un partage d'écran

Exemple : dessins inappropriés sur votre PowerPoint.

Si vous voulez activer les annotations, nous vous recommandons de cocher la case « seul l'utilisateur qui effectue le partage peut ajouter des annotations ».

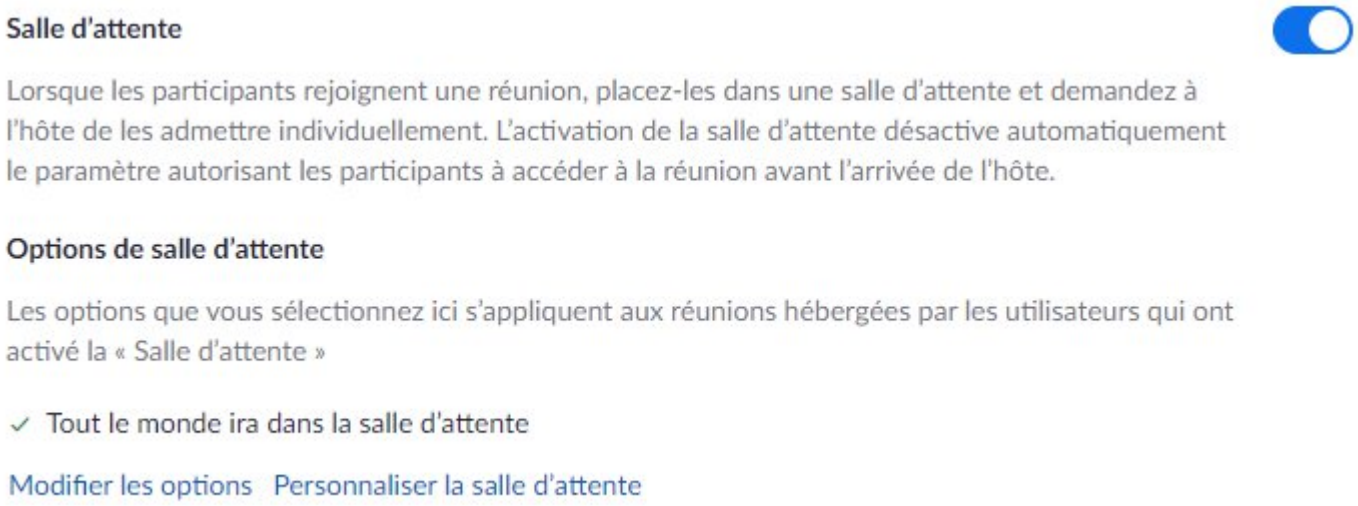


Vous pourrez ainsi annoter le Powerpoint et les étudiants seront dans l'impossibilité d'agir.

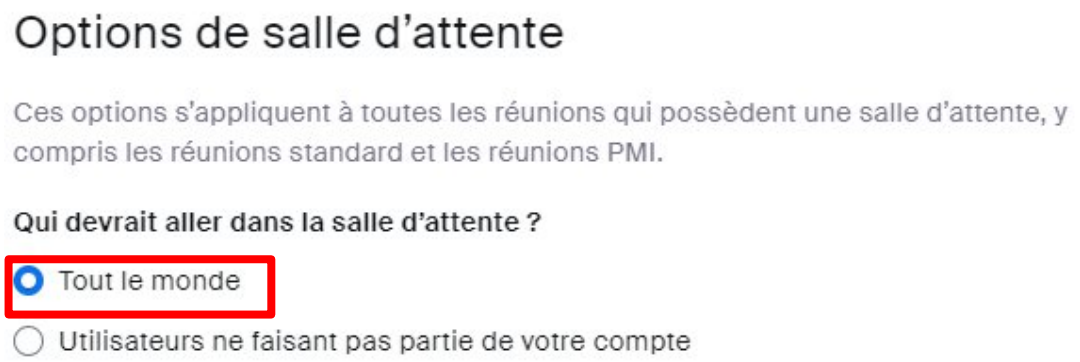
Et si vous souhaitez leur permettre d'annoter lors d'une activité prévue à cet effet, vous pourrez activez la fonctionnalité en cours de réunion (voir ici)

3. La Salle d'attente

La salle d'attente est une fonctionnalité importante car elle constitue une barrière. Les personnes avec de mauvaises intentions peuvent posséder plusieurs comptes, ainsi cela permet de se prémunir d'une authentification sur un autre compte (lorsque les participants sont en salle d'attente ils seront isolés, ils ne peuvent ni agir sur la réunion, ni vous entendre). Il est également possible de réactiver la salle d'attente en cours de réunion pour neutraliser un utilisateur spécifique.



Nous vous recommandons de définir que tout le monde ira en salle d'attente par défaut.

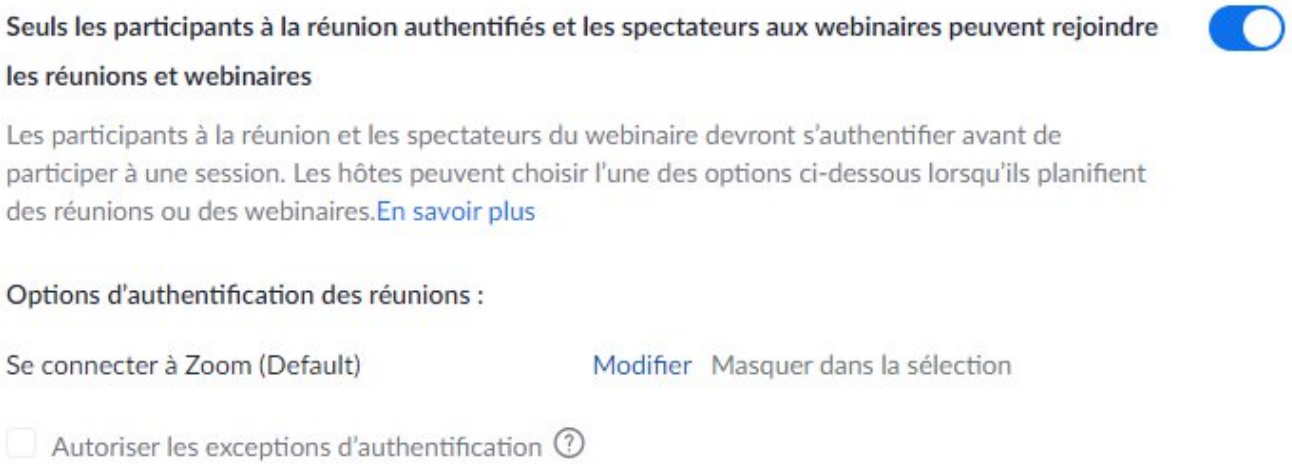


4. Les conditions d'accès aux réunions Zoom

Lorsque vous programmez une réunion, vous avez la possibilité de paramétrer ses conditions d'accès. Vous pouvez ainsi définir que les utilisateurs peuvent rejoindre la réunion sans compte Zoom (ils n'auront qu'à définir un pseudo).

L'autre possibilité étant que les participants doivent se connecter à Zoom. Attention, la connexion à Zoom dans ce cas n'implique pas nécessairement l'utilisation du compte Zoom universitaire. Un étudiant peut très bien se créer un compte avec une adresse mail personnelle (par exemple gmail, yahoo, etc.) et pourra s'authentifier à la réunion.

Cette protection peut cependant être facilement contournée car les individus malveillants peuvent disposer de plusieurs comptes Zoom. Nous vous recommandons donc de toujours associer la salle d'attente.



5. Se renommer

Par défaut les étudiants peuvent se renommer. Il est donc nécessaire de **désactiver** cette fonctionnalité.

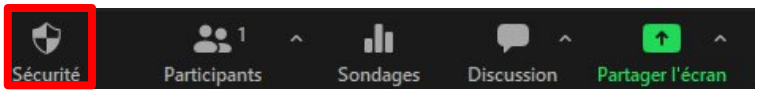
2 intérêts à cela :

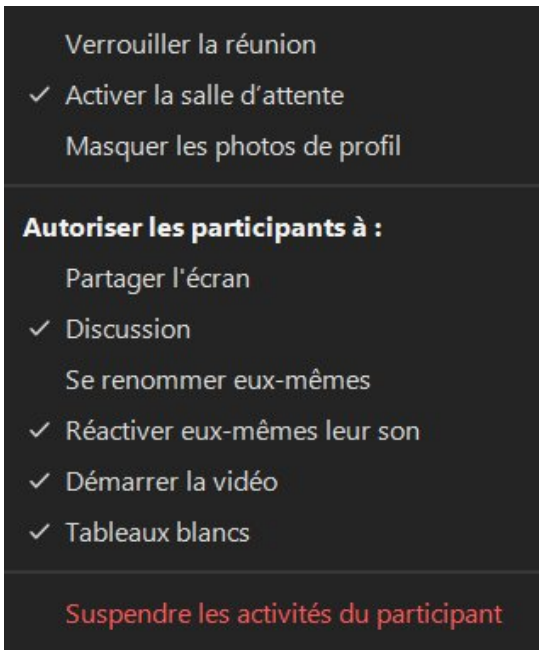
- les empêcher de prendre des noms offensants (jeux de mots racistes, insultes, etc.)
- les empêcher de prendre l'identité de quelqu'un d'autre (par exemple un étudiant qui ouvre son micro pour vous insulter après avoir préalablement pris le nom d'un autre participant –ou qui changera son nom à posteriori pour ne pas être identifiable. Des noms/pseudos inappropriés peuvent être un indice sur la volonté de malveillance de la personne. Dans ce cas, vous pouvez lui demander de décliner son identité ou le mettre en salle d'attente.

Lutter contre les actes de malveillance lors de la réunion

Le volet Sécurité : des actions globales

Il est accessible en tant qu'Hôte de la réunion et affecte tous les participants de la réunion. Attention, il peut y avoir des différences de nom selon les systèmes d'exploitation (Windows, Mac, etc.) et les versions de Zoom.



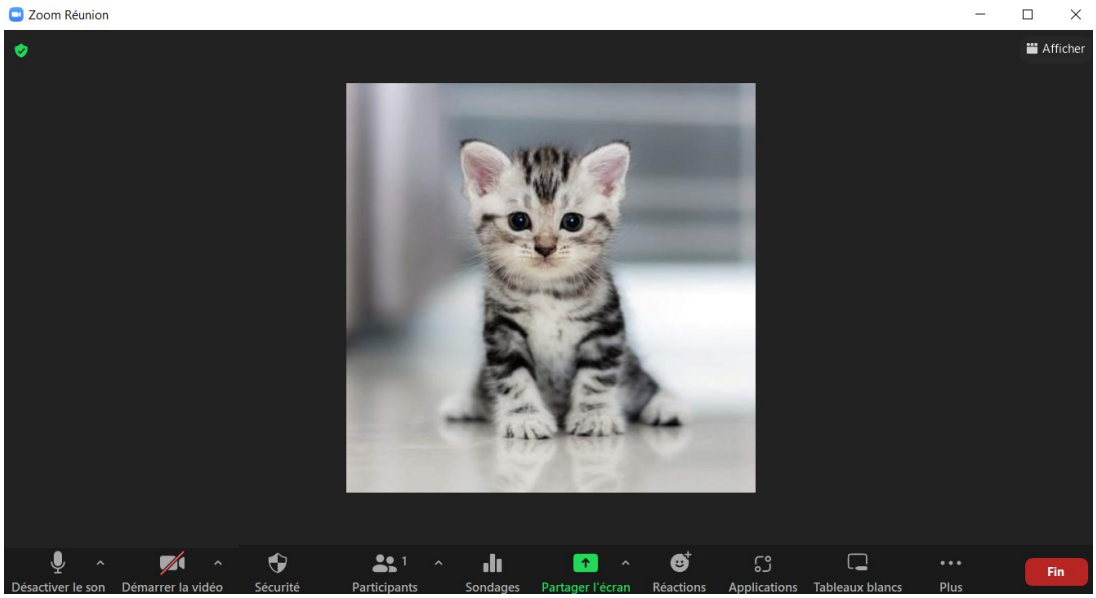


1. Verrouiller la réunion : en activant cette fonctionnalité, plus aucun participant ne peut rejoindre la réunion (même en disposant du code secret). Attention un étudiant qui est déconnecté (problème de connexion) ne pourra pas accéder à nouveau à la réunion. **Nous vous déconseillons donc cette fonctionnalité.**

2. Activer/désactiver la salle d'attente : La salle d'attente peut être activée et désactivée selon votre volonté et le déroulement de la réunion. Nous vous recommandons de la désactiver lorsque le cours commence (pour ne pas avoir à accepter manuellement les retardataires/les personnes qui subissent une déconnexion) et la réactiver en cas d'incident. Les participants déconnectés pourront être acceptés manuellement depuis la salle d'attente.

3. Masquer les photos de profil : dans zoom vous avez la possibilité de définir une photo de profil (depuis l'application par exemple).

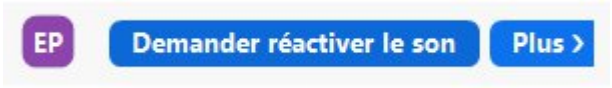
Celle-ci s'affichera lorsqu'un utilisateur n'active pas sa caméra. Exemple :



Si certaines photos sont innocentes, des individus avec des intentions malveillantes peuvent être tentés de mettre des photos inappropriées. Ce paramétrage masque pour tous les utilisateurs les photos de profil.

4. Autoriser les participants (si la fonctionnalité est cochée) à

- Partager l'écran : permet aux participants de partager leur écran.
- Discussion : permet de converser via le tchat de la réunion
- Renommer : permet aux participants de se renommer.
- Démarrer la vidéo : permet aux intervenants de démarrer leur vidéo au cours du webinaire.
- Réactiver eux-mêmes leur son : permet aux participants de rétablir leur son. Sans cela c'est à l'Hôte de demander manuellement l'activation pour un participant (via le volet participant).



Attention, ces actions ne sont pas rétroactives ! Cela signifie que si vous désactivez la possibilité d'activation des micros, cela ne désactivera pas les micros déjà actifs ! (se reporter à la section correspondante)

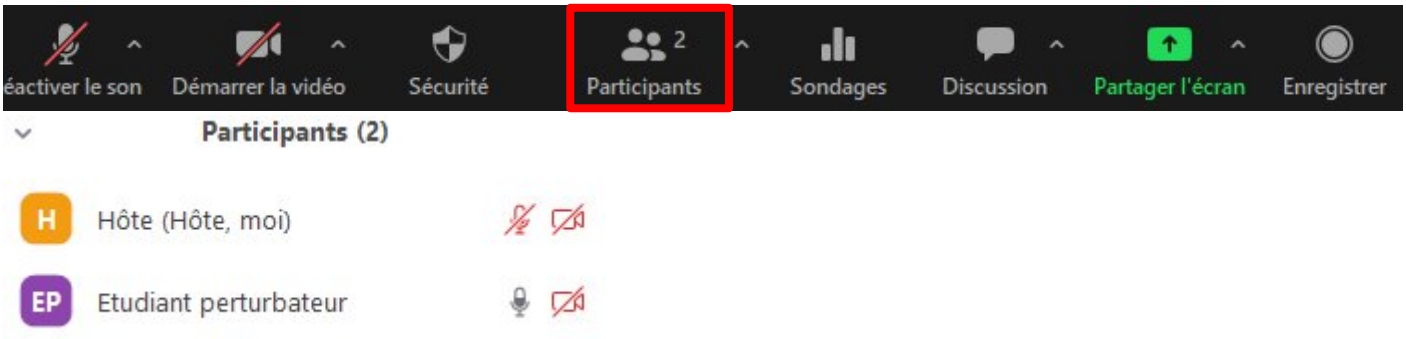
5. Supprimer les activités du participant : il s'agit d'un cumul d'actions,

- Les micros et la vidéo de tous les participants seront désactivés et ces derniers ne seront plus en mesure de les réactiver.
- La réunion sera verrouillée [faire le lien vers 1.]
- Si un participant (hors Hôte) partage son écran, le partage sera interrompu et ils ne pourront pas partager à nouveau
- Le tchat sera désactivé
- Les divisions en salle de petit groupe s'arrêtent

Les actions localisées sur les participants

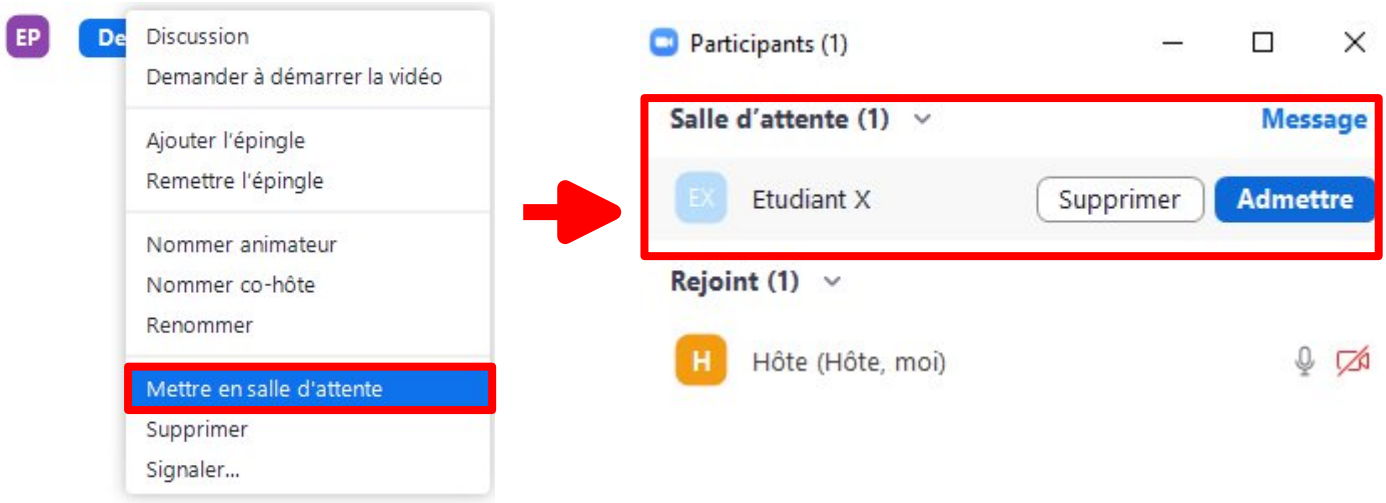
Mettre un participant en salle d'attente

Il faut pour cela que la salle d'attente soit active (cf. ici et ici) puis cliquer sur « Participants » pour afficher la liste des participants.



Cliquer sur « Plus » sur la ligne correspondant au participant que vous souhaitez mettre en salle d'attente

Choisissez l'option « Mettre en salle d'attente »

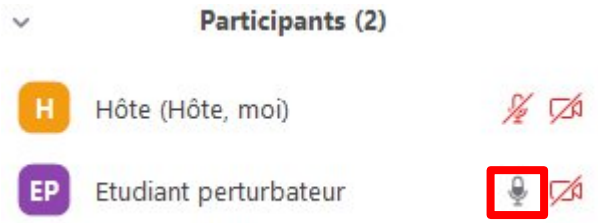


Couper le son d'un participant

La première action peut-être simplement de demander au participant concerné de couper son micro (il peut s'agir simplement d'une inattention de sa part).

Vous pouvez identifier le participant bruyant via l'icône de micro située en face de son nom dans le volet Participants.

- Participant ayant son micro désactivé
- Participant silencieux
- Participant émettant du son

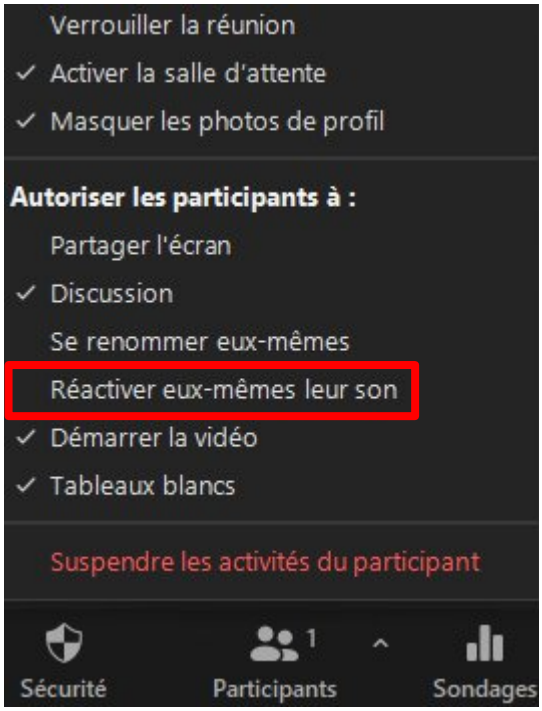


Si cette première action n'est pas suffisante vous pouvez désactiver son micro en positionnant le curseur de votre souris sur le participant et en cliquant sur « Désactiver le son ».

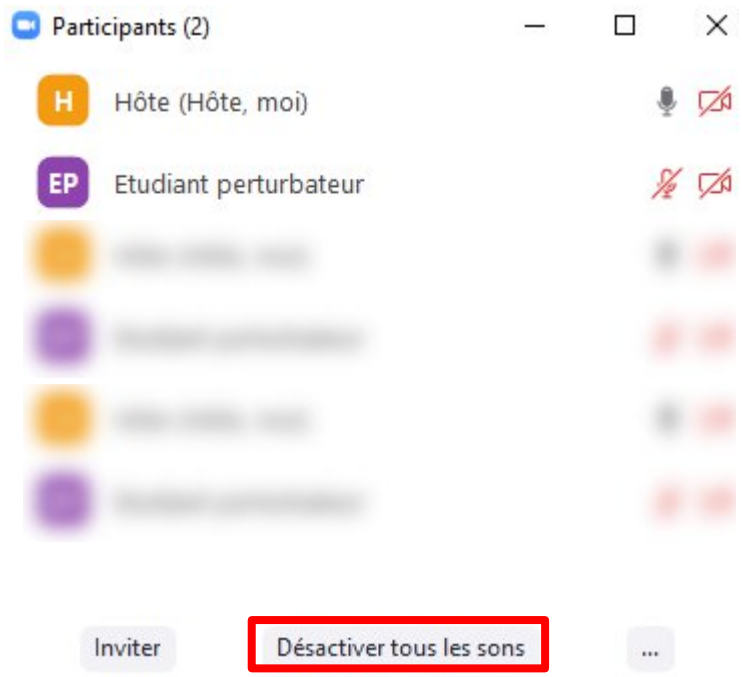
Attention, pour rappel, les participants peuvent réactiver leur micro sauf si vous avez désactivé cette possibilité.

Désactiver le micro de tous les participants

Il peut être difficile d'identifier la personne bruyante lorsque vous avez beaucoup de participants. Il est également possible que plusieurs participants soient à l'origine de nuisances. Pour ce faire, vous pouvez couper le micro de tous les participants. Nous vous recommandons dans un premier temps de désactiver la réactivation des micros.



Puis d'ouvrir le volet des Participants et de cliquer en bas sur « Désactiver tous les sons ».



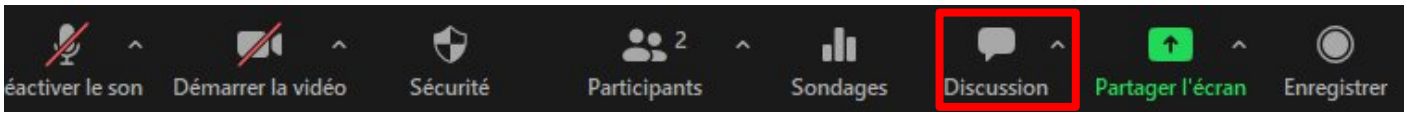
A noter que vous pouvez simplement cliquer sur « Désactiver tous les sons »

Mais il est important de respecter cet ordre, car autrement les étudiants pourront réactiver leur micro le temps que vous désactiviez la fonctionnalité.

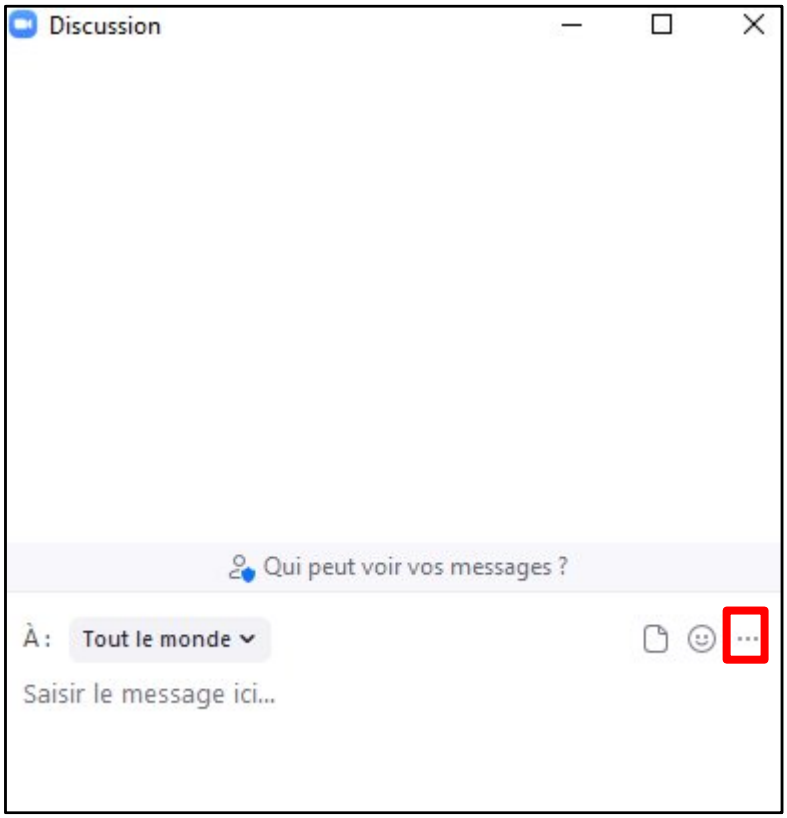
Changer les conditions d'utilisation du tchat en réunion :

Il est possible que certains étudiants utilisent le tchat à des fins malveillantes. Vous pouvez le désactiver via le volet Sécurité.

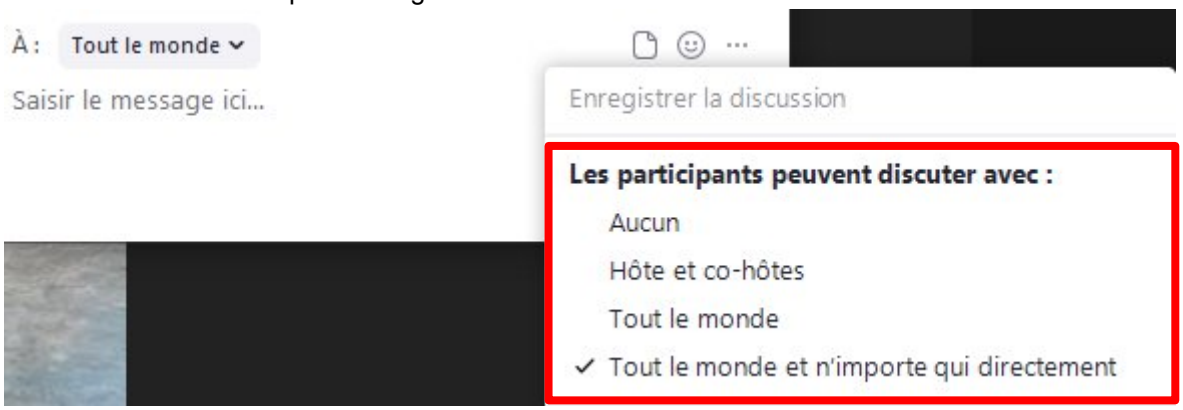
Mais vous pouvez aussi restreindre les communications (permettre aux participants de ne discuter qu'avec les Hôtes). Pour ce faire, cliquer sur Discussion (aussi appelé « Converser » selon les systèmes d'exploitation et les versions)



Puis cliquer sur les … en bas de la fenêtre.



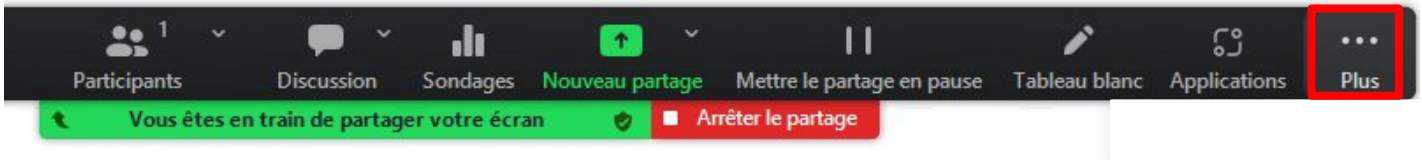
Et vous aurez accès au paramétrage du tchat.



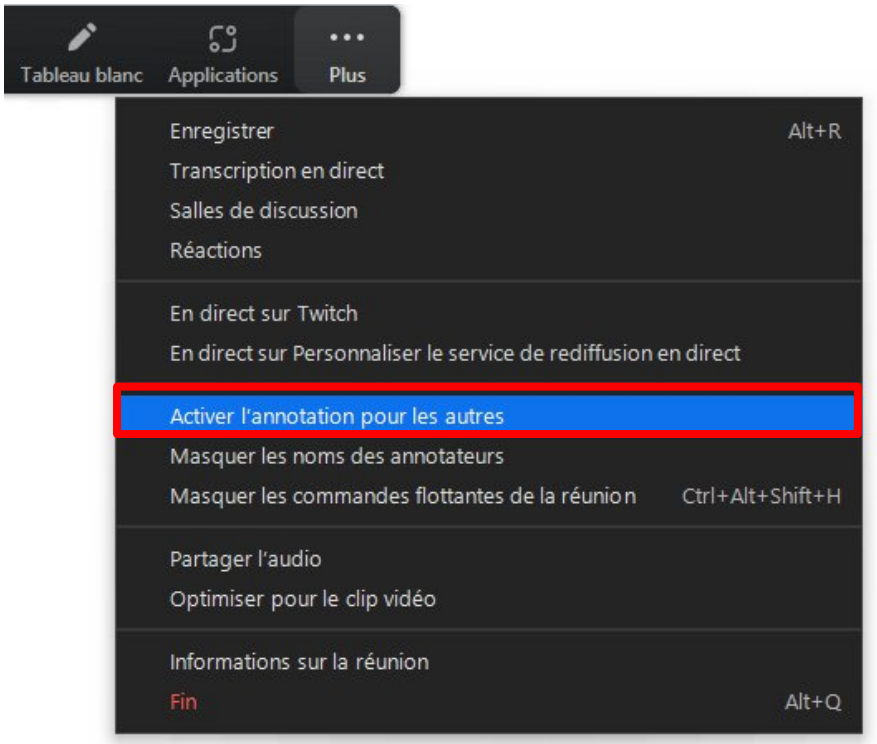
N.B : « n'importe qui directement » signifie qu'il peut y avoir des messages privés.

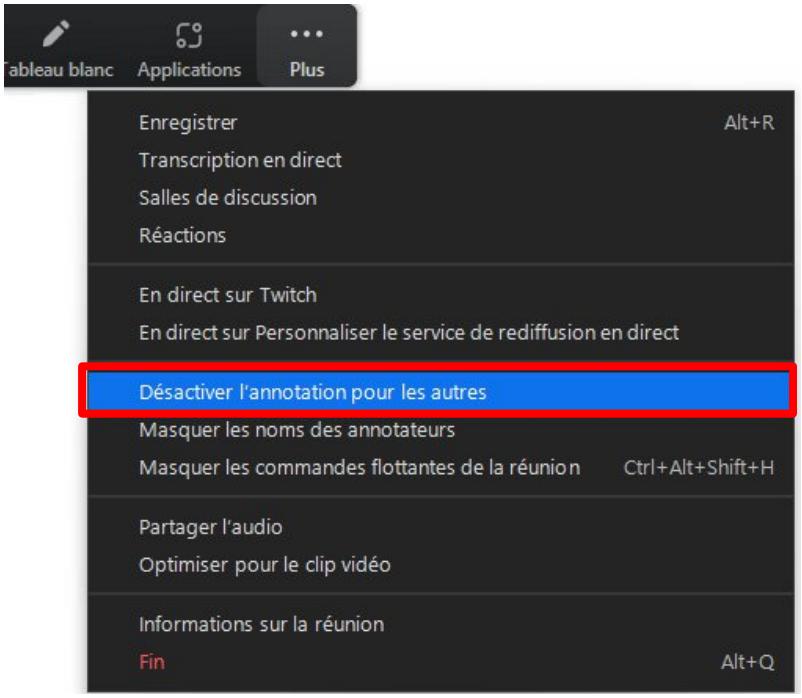
Permettre/désactiver les annotations par les autres participants :

En cours de partage, vous avez la possibilité via « Annotation » ou « Plus » de permettre ou non les annotations par les autres participants.



Vous pourrez activer ou désactiver les annotations.





Contact

Pour toute question, veuillez contacter : sos-dapi@univ-grenoble-alpes.fr