Google for Education

Découvrez plus de 30 façons d'utiliser les éditions payantes de Google Workspace for Education

goo.gle/use-edu-workspace

Comment utiliser cette présentation ?

Cette présentation est une sélection des cas d'utilisation les plus courants des **éditions payantes de Google Workspace for Education**. Ces éditions incluent des outils qui peuvent contribuer à améliorer **la sécurité des données, l'efficacité des enseignants, l'implication des élèves, la collaboration au niveau de tout l'établissement** et bien plus encore.

Cette présentation est organisée de la manière suivante : la **fonctionnalité** décrite est suivie des **cas d'utilisation courants** et d'**instructions** simples expliquant comment se servir de cette fonctionnalité. Consultez l'intégralité de la présentation pour découvrir tout ce que vous pouvez faire avec Google Workspace for Education.

Éditions payantes de Google Workspace for Education

Les trois éditions payantes de Google Workspace for Education vous offrent plus de choix, de contrôle et de flexibilité pour répondre aux besoins de votre organisation.

Google Workspace for Education Standard

Des outils avancés de sécurité et d'analyse qui vous donnent plus de visibilité et de contrôle sur l'ensemble de l'environnement d'apprentissage afin de réduire les risques et les menaces

Teaching and Learning Upgrade

Des outils pédagogiques améliorés qui enrichissent les expériences de communication et d'apprentissage, et favorisent l'intégrité académique

Google Workspace for Education Plus

Une solution complète qui inclut toutes les fonctionnalités des éditions Education Standard et Teaching and Learning Upgrade, tout en offrant à votre communauté scolaire l'environnement d'apprentissage le plus efficace et le plus unifié qui soit

Sommaire

Outils d'analyse et de sécurité

Disponibles dans **Education Standard** et **Education Plus**

Outil d'investigation

- Partage de contenus abusifs
- Partage accidentel de fichiers
- Tri des e-mails
- Hameçonnage et logiciels malveillants par e-mail
- Arrêter les acteurs malveillants

Tableau de bord de sécurité

- Volume de spam
- Partage de fichiers externe
- Applications tierces
- Tentative d'hameçonnage

État de sécurité

- Recommandations pour les zones à risque
- Suivre l'évolution des bonnes pratiques
- Bonnes pratiques concernant la sécurité
- Améliorer la sécurité d'une école en pleine croissance

Commandes d'administration avancées

- Lois réglementaires sur les données
- Réglementation des authentifications
- Restrictions sur les applications
- Gérer des appareils mobiles
- Migrer des données

Sommaire

Outils d'enseignement et d'apprentissage

Disponibles dans **Teaching and Learning Upgrade** et **Education Plus**

Rapports sur le degré d'originalité

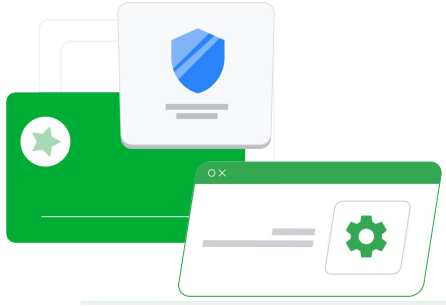
- Détecter les cas de plagiat
- Apprendre de ses erreurs avec la détection des cas de plagiat

Google Meet

- Visioconférences sécurisées
- Améliorer la sécurité des visioconférences
- Enregistrer les cours
- Enregistrer les réunions d'établissement
- Cours manqués
- Réunions diffusées en direct
- Événements de l'établissement diffusés en direct
- Poser des questions
- Rassembler des données
- Petits groupes d'élèves
- Suivi de la participation

Outils d'analyse et de sécurité

Contrôlez mieux votre domaine à l'aide d'outils de sécurité proactive qui vous aident à vous prémunir contre les menaces, à analyser les incidents de sécurité et à protéger les données des élèves et des enseignants.



- Outil d'investigation
- Tableau de bord de sécurité
- Page "État de sécurité"
- Commandes d'administration avancées

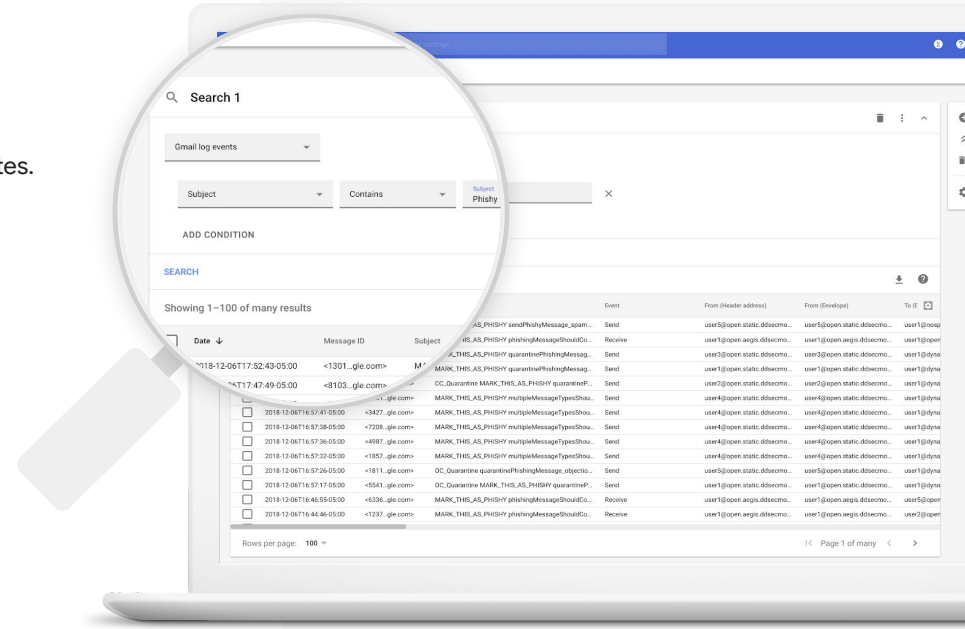
Outil d'investigation

De quoi s'agit-il ?

L'outil d'investigation permet d'identifier les problèmes de sécurité et de confidentialité sur votre domaine, de les trier et de prendre les mesures adéquates.

Cas d'utilisation

Partage de contenus abusifs	Instructions détaillées
Partage accidentel de fichiers	Instructions détaillées
Tri des e-mails	Instructions détaillées
Hameçonnage/Logiciels malveillant par e-mail	Instructions détaillées
Arrêter les acteurs malveillants	Instructions détaillées



Je sais qu'un fichier avec des contenus abusifs a été partagé. Je veux connaître sa date de création et son auteur, et savoir qui l'a partagé, qui l'a reçu et qui l'a modifié. Je veux aussi le supprimer."

Instructions détaillées

Partage de contenus abusifs

Les journaux Drive de l'**outil d'investigation** peuvent vous aider à rechercher, à localiser et à isoler ou à supprimer les fichiers indésirables de votre domaine. Dans vos journaux Drive, voici ce que vous pouvez faire :

- Rechercher les documents par nom, par acteur, par propriétaire, etc.
- Intervenir en modifiant les autorisations du fichier ou en le supprimant
- Voir toutes les informations du journal en lien avec ce document
  - Date de création
  - Propriétaire, utilisateurs ayant consulté le fichier et personnes l'ayant modifié
  - Date de partage

Documents pertinents du centre d'aide

Conditions pour les événements de journaux Drive

Actions liées aux événements de journaux Drive

Fichiers partagés accidentellement

Un fichier a été partagé accidentellement avec un groupe qui NE devait PAS y avoir accès. Je veux supprimer cet accès."

Les journaux Drive de l'**outil d'investigation** peuvent vous aider à localiser les problèmes de partage de fichiers et à les résoudre. Dans vos journaux Drive, voici ce que vous pouvez faire :

- Rechercher les documents par nom, par acteur, par propriétaire, etc.
- Voir toutes les informations du journal en lien avec ce document, y compris le nom des utilisateurs l'ayant consulté et la date/l'heure de partage
- Intervenir en modifiant les autorisations du fichier et en désactivant le téléchargement, l'impression et la copie

Instructions détaillées

Documents pertinents du centre d'aide

Conditions pour les événements de journaux Drive

Actions liées aux événements de journaux Drive

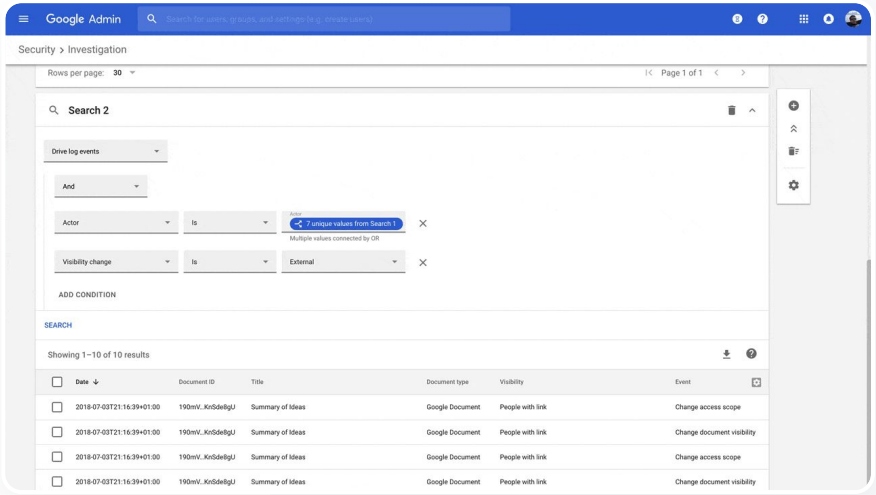
Instructions – Événements de journaux Drive

Analyser la situation

- Connectez-vous à la **console d'administration**.
- Cliquez sur **Sécurité** > **Outil d'investigation**.
- Sélectionnez **Événements de journaux Drive**.
- Cliquez sur **Ajouter une condition** > **Rechercher**.

Intervenir

- Sélectionnez les fichiers concernés dans les résultats de recherche.
- Cliquez sur **Actions** > **Vérifier les autorisations des fichiers** pour ouvrir la page "Autorisations".
- Cliquez sur **Utilisateurs** pour afficher le nom des personnes qui ont accès aux fichiers.
- Cliquez sur **Liens** pour afficher ou modifier les paramètres de partage par lien des fichiers sélectionnés.
- Cliquez sur **Modifications en attente** pour passer en revue vos modifications avant de les enregistrer.



Documents pertinents du centre d'aide

Conditions pour les événements de journaux Drive

Actions liées aux événements de journaux Drive

Tri des e-mails

Les **journaux Gmail** de l'**outil d'investigation** peuvent vous aider à identifier les e-mails dangereux ou abusifs sur votre domaine et à agir en conséquence. Dans vos journaux Gmail, voici ce que vous pouvez faire :

- Rechercher des e-mails spécifiques par objet, par ID du message, par pièce jointe, par expéditeur, etc.
- Voir les détails de l'e-mail, y compris son auteur, ses destinataires, ses ouvertures et ses transferts
- Intervenir en fonction des résultats de recherche (vous pouvez supprimer le message Gmail, le restaurer, le marquer comme spam ou hameçonnage, l'envoyer dans la boîte de réception ou l'envoyer en quarantaine)

> Quelqu'un a envoyé un e-mail qu'il N'aurait PAS dû. Nous voulons connaître les destinataires de ce message, savoir s'ils l'ont ouvert et s'ils y ont répondu, et le supprimer. Nous voulons aussi connaître le contenu de l'e-mail."

Instructions détaillées

Documents pertinents du centre d'aide

- Conditions pour les journaux et messages Gmail
- Actions liées aux messages et aux événements de journaux Gmail
- Procédure pour afficher le contenu d'un e-mail

“

Les utilisateurs ont reçu un e-mail d'hameçonnage ou contenant un logiciel malveillant. Nous voulons savoir s'ils ont cliqué sur le lien dans le message ou téléchargé la pièce jointe, car cela peut potentiellement représenter un danger pour eux et notre domaine."

Instructions détaillées

Hameçonnage et logiciels malveillants par e-mail

L'**outil d'investigation**, en particulier les **journaux Gmail**, peut vous aider à rechercher et à identifier les e-mails malveillants sur votre domaine. Dans vos journaux Gmail, voici ce que vous pouvez faire :

- Rechercher des contenus spécifiques dans les e-mails, y compris dans les pièces jointes
- Voir les informations concernant des e-mails spécifiques, y compris leurs destinataires et leurs ouvertures
- Consulter les messages et le fil de discussion pour savoir s'ils sont malveillants
- Intervenir en marquant les messages comme spam ou hameçonnage, en les envoyant dans une boîte de réception spécifique ou en quarantaine, ou en les supprimant

Documents pertinents du centre d'aide

Conditions pour les journaux et messages Gmail

Actions liées aux messages et aux événements de journaux Gmail

Procédure pour afficher le contenu d'un e-mail

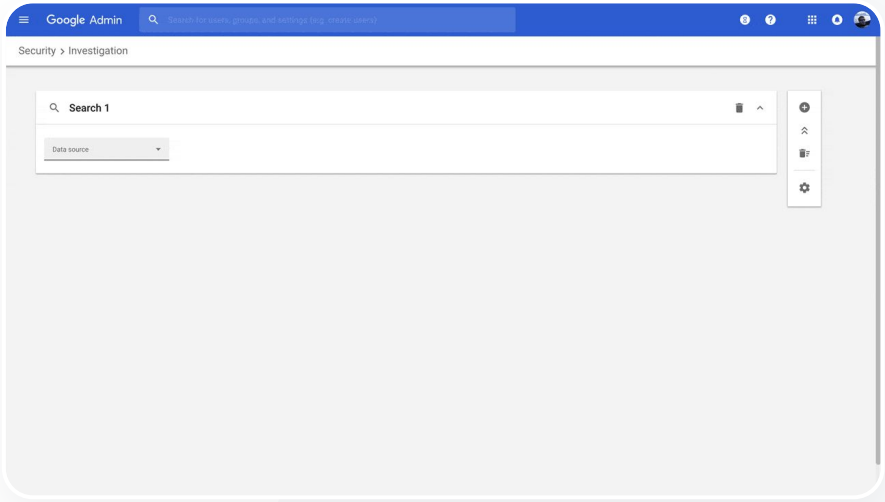
Instructions – Journaux Gmail

Analyser la situation

- Connectez-vous à la **console d'administration**.
- Cliquez sur **Sécurité** > **Outil d'investigation**.
- Sélectionnez **Événements de journaux Gmail** OU **Messages Gmail**.
- Cliquez sur **Ajouter une condition** > **Rechercher**.

Intervenir

- Sélectionnez les messages concernés dans les résultats de recherche.
- Cliquez sur **Actions**.
- Sélectionnez **Supprimer le message de la boîte de réception**.
- Cliquez sur **Supprimer de la boîte de réception**.
- Pour confirmer l'action, cliquez sur **Afficher** en bas de la page.
- Dans la colonne **Résultat**, vous pouvez afficher l'état de l'action.



Documents pertinents du centre d'aide

Conditions pour les journaux et messages Gmail

Actions liées aux messages et aux événements de journaux Gmail

Procédure pour afficher le contenu d'un e-mail

Arrêter les acteurs malveillants

Un acteur malveillant cible constamment des utilisateurs importants de mon domaine et je suis obligé de jouer au chat et à la souris pour essayer de l'arrêter. Que puis-je faire pour que ça s'arrête ?"

Instructions détaillées

Voici ce que le **journal des utilisateurs** de l'**outil d'investigation** peut vous aider à faire :

- Identifier et étudier les tentatives de piratage des comptes utilisateur dans votre organisation
- Contrôler les méthodes de validation en deux étapes dont se servent les utilisateurs de votre organisation
- En savoir plus sur les tentatives de connexion infructueuses des utilisateurs de votre organisation
- Créer des règles d'activité à l'aide de l'outil d'investigation : bloquer automatiquement les messages et autres activités malveillantes d'acteurs spécifiques
- Mieux protéger les utilisateurs importants avec le Programme Protection Avancée
- Restaurer ou suspendre des comptes utilisateur

Documents pertinents du centre d'aide

Rechercher et examiner les événements de journaux d'utilisateurs

Créer des règles d'activité à l'aide de l'outil d'investigation

Instructions – Événements de journaux des utilisateurs

Analyser la situation

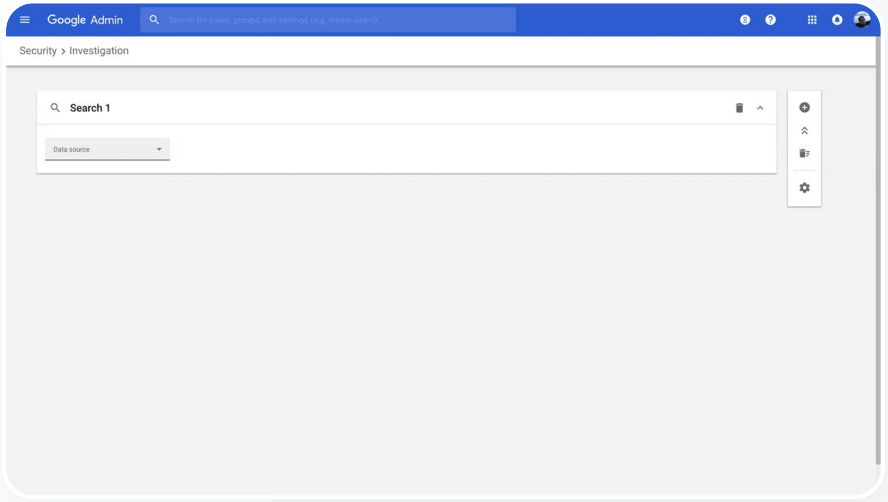
- Connectez-vous à la **console d'administration**.
- Cliquez sur **Sécurité** > **Outil d'investigation**.
- Sélectionnez **Événements de journaux des utilisateurs**.
- Cliquez sur **Ajouter une condition** > **Rechercher**.

Restaurer ou suspendre des comptes utilisateur

- Dans les résultats de recherche, sélectionnez un ou plusieurs utilisateurs.
- Cliquez sur le menu déroulant **Actions**.
- Cliquez sur **Restaurer le compte utilisateur** ou **Suspendre le compte utilisateur**.

Afficher les détails sur un utilisateur spécifique

- Sur la page des résultats de recherche, sélectionnez un seul utilisateur.
- Dans le menu déroulant ACTIONS, cliquez sur **Afficher les détails**.



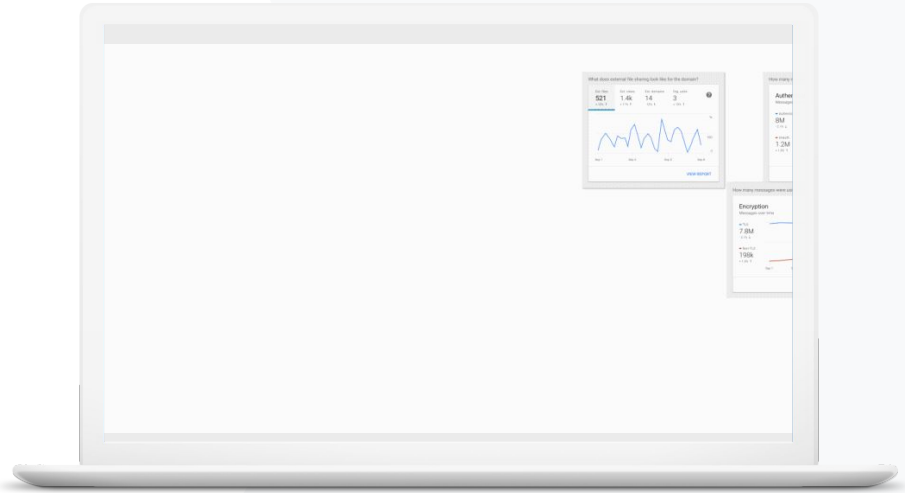
Documents pertinents du centre d'aide

Rechercher et examiner les événements de journaux d'utilisateurs

Tableau de bord de sécurité

De quoi s'agit-il ?

Le tableau de bord de sécurité permet d'afficher un aperçu de vos différents rapports de sécurité. Par défaut, un rapport récapitulant les données de sécurité des sept derniers jours est affiché dans chaque panneau. Vous pouvez personnaliser le tableau de bord pour afficher les données sur différentes périodes : "Aujourd'hui", "Hier", "Cette semaine", "La semaine dernière", "Ce mois-ci", "Le mois dernier" ou "Début de la période (jusqu'à 180 jours auparavant)".



Cas d'utilisation

Volume de spam	Instructions détaillées
Partage de fichiers externe	Instructions détaillées
Applications tierces	Instructions détaillées
Tentative d'hameçonnage	Instructions détaillées

Volume de spam

Le **tableau de bord de sécurité** vous donne accès à une représentation visuelle de l'activité sur tout votre environnement Google Workspace for Education, y compris pour les menaces suivantes :

- Spam
- Hameçonnage
- Logiciels malveillants
- Pièces jointes suspectes
- Autres types de menaces

> Je veux contrôler les e-mails excessifs et inutiles tout en réduisant les menaces de sécurité pour mon école."

Instructions détaillées

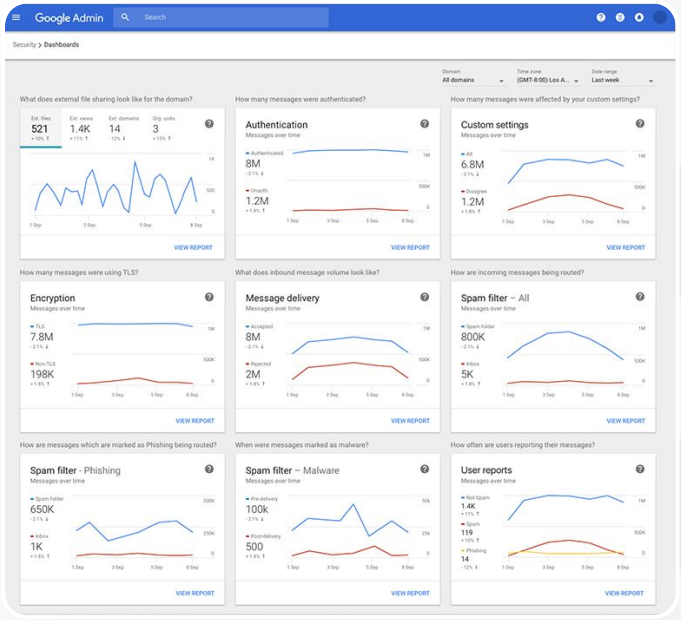
Documents pertinents du centre d'aide

À propos du tableau de bord de sécurité

Instructions – Présentation du tableau de bord

Afficher le tableau de bord

- Connectez-vous à la **console d'administration**.
- Cliquez sur **Sécurité > Tableau de bord.**
- Dans le tableau de bord de sécurité, vous pouvez explorer les données, les exporter dans Sheets ou dans un outil tiers, ou lancer une enquête dans l'outil d'investigation.



Documents pertinents du centre d'aide

À propos du tableau de bord de sécurité

Partage de fichiers externe

Je veux voir l'activité de partage externe de fichiers pour éviter que les données sensibles ne soient transmises à des tiers."

Le **rapport "Exposition des fichiers"** du **tableau de bord de sécurité** vous donne accès aux métriques sur les partages externes de fichiers pour votre domaine. Voici ce qu'il vous indique entre autres :

- Nombre de partages avec des utilisateurs extérieurs à votre domaine pendant une période donnée
- Nombre de vues comptabilisées pour un fichier externe reçu pendant une période donnée

Instructions détaillées

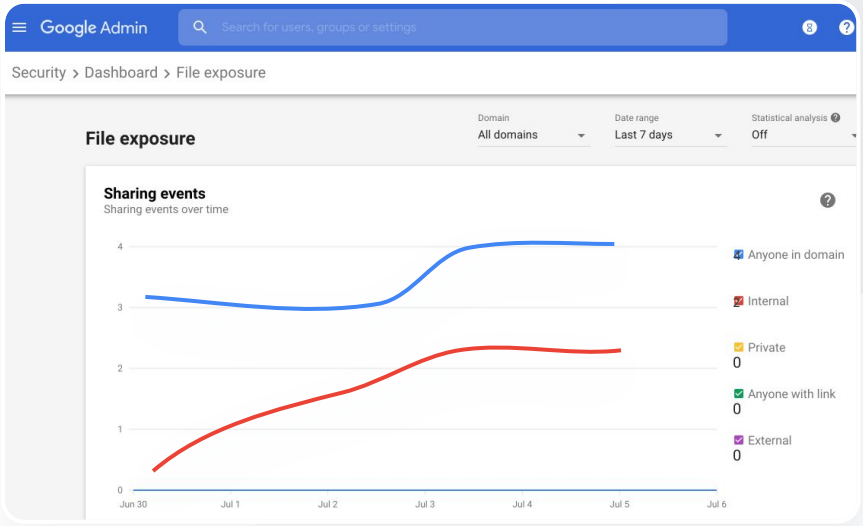
Documents pertinents du centre d'aide

Premiers pas avec la page "État de sécurité"

Instructions – Rapport "Exposition des fichiers"

Afficher le rapport

- Connectez-vous à la **console d'administration**.
- Cliquez sur **Sécurité** > **Tableau de bord**.
- Dans le panneau intitulé **Qu'en est-il du partage externe sur le domaine ?**, cliquez sur **Afficher le rapport** en bas à droite.



Documents pertinents du centre d'aide

À propos du tableau de bord de sécurité
Rapport "Exposition des fichiers"

Applications tierces

Je veux savoir quelles applications tierces ont accès aux données de mon domaine."

Utilisez le **rapport "Modification des authentifications OAuth"** du **tableau de bord de sécurité** pour surveiller les applications tierces connectées à votre domaine et contrôler le type de données auxquelles elles peuvent accéder.

- L'authentification OAuth autorise des services tiers à accéder aux informations de compte d'un utilisateur sans divulguer son mot de passe. Vous pouvez limiter l'accès de certaines applications tierces.
- Utilisez le panneau "Modification des authentifications OAuth" pour contrôler les modifications des authentifications par application, par champ d'application ou par utilisateur, et pour mettre à jour les autorisations d'authentification.

Instructions détaillées

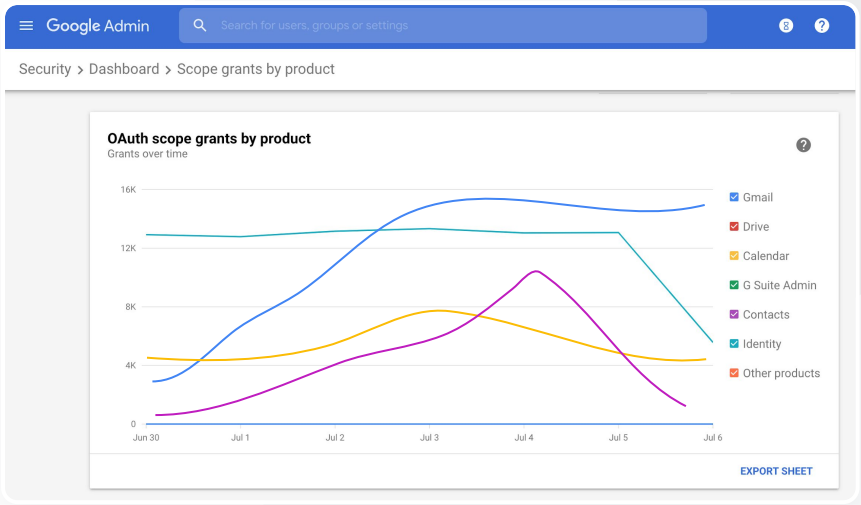
Documents pertinents du centre d'aide

Rapport "Modification des authentifications OAuth"

Instructions – Rapport "Modification des authentifications OAuth"

Afficher le rapport

- Connectez-vous à la **console d'administration**.
- Cliquez sur **Sécurité** > **Tableau de bord**.
- En bas de l'écran, cliquez sur **Afficher le rapport**.
- Vous pouvez afficher l'activité des authentifications OAuth par produit (application), par champ d'application ou par utilisateur.
- Pour filtrer les informations, cliquez sur **Application**, **Champ d'application** ou **Utilisateur**.
- Pour créer le rapport sous forme de feuille de calcul, cliquez sur **Exporter la feuille**.



Documents pertinents du centre d'aide

Rapport "Modification des authentifications OAuth"

Tentative d'hameçonnage

Le panneau **Rapports utilisateur** du **tableau de bord de sécurité** vous permet de connaître le nombre de messages qui ont été signalés comme e-mails d'hameçonnage ou spam sur une période donnée. Vous pouvez afficher des informations concernant ceux signalés comme e-mails d'hameçonnage (telles que leurs destinataires et leurs ouvertures).

- Les rapports utilisateur indiquent comment les utilisateurs ont marqué leurs messages (comme spam, non spam ou hameçonnage) pendant une période donnée.
- Vous pouvez personnaliser le graphique afin d'afficher uniquement des détails sur certains types de messages (par exemple pour voir s'ils ont été envoyés en interne ou en externe, pour les afficher par plage de dates, etc.).

> Les utilisateurs ont signalé une tentative d'hameçonnage. Je veux pouvoir savoir quand l'e-mail d'hameçonnage a été reçu et connaître le contenu exact de ce message ainsi que le risque encouru par les utilisateurs qui l'ont reçu."

Instructions détaillées

Documents pertinents du centre d'aide

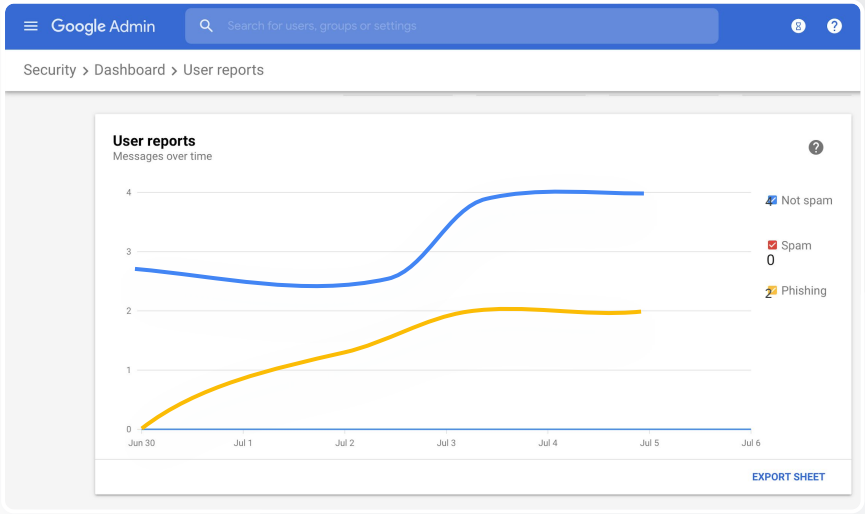
Comment les utilisateurs marquent-ils leurs e-mails ?

Rapports utilisateur

Instructions – Panneau "Rapports utilisateur"

Afficher le rapport

- Connectez-vous à la **console d'administration**.
- Cliquez sur **Sécurité** > **Tableau de bord**.
- En bas à droite du panneau **Rapports utilisateur**, cliquez sur **Afficher le rapport**.



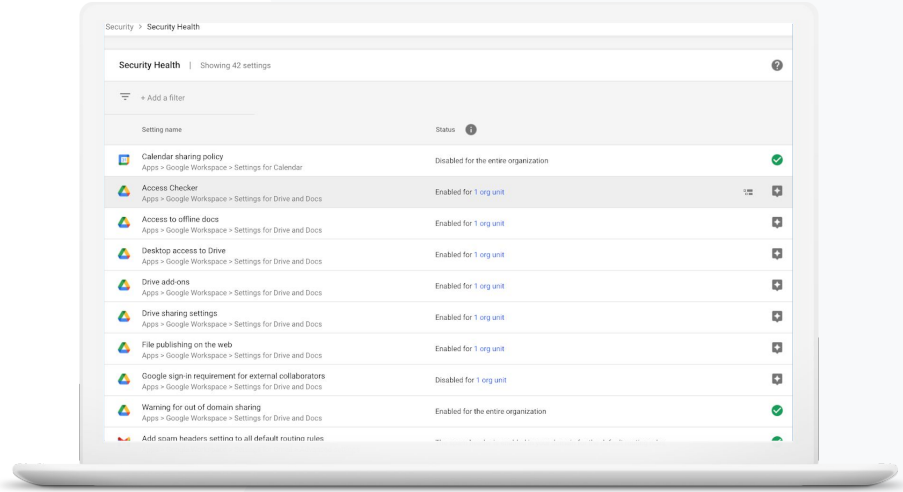
Documents pertinents du centre d'aide

À propos du tableau de bord de sécurité
Rapport "Exposition des fichiers"

État de sécurité

De quoi s'agit-il ?

La page "État de sécurité" donne un aperçu complet de l'état de sécurité de votre environnement Google Workspace. Elle vous permet de comparer vos configurations aux recommandations de Google pour protéger votre organisation de manière proactive.



Cas d'utilisation

Recommandations pour les zones à risque	Instructions détaillées
Suivre l'évolution des bonnes pratiques	Instructions détaillées
Bonnes pratiques concernant la sécurité	Instructions détaillées
Améliorer la sécurité d'une école en pleine croissance	Instructions détaillées

Recommandations pour les zones à risque

"Je veux un instantané qui récapitule les paramètres de sécurité de mon domaine et qui fournit les recommandations à suivre pour résoudre les problèmes liés aux potentielles zones à risque."

La page **État de sécurité** évalue la configuration de la sécurité sur votre domaine et signale certaines modifications recommandées. Voici ce que vous pouvez faire sur cette page :

- Identifier rapidement les potentielles zones à risque de votre domaine
- Obtenir des recommandations concernant les paramètres à utiliser pour améliorer l'efficacité de vos mesures de sécurité
- En savoir plus et consulter des articles d'aide sur ces recommandations

Instructions détaillées

Documents pertinents du centre d'aide

Premiers pas avec la page "État de sécurité"

Suivre l'évolution des bonnes pratiques

Je gère notre domaine, mais je ne peux pas être au courant de tout. J'ai besoin d'aide pour que tout soit sécurisé avec les bons paramètres."

Instructions détaillées

La page **État de sécurité** évalue la configuration de la sécurité sur votre domaine et signale certaines modifications recommandées. Voici ce que vous pouvez obtenir sur cette page :

- Recommandations pour les potentielles zones à risque de votre domaine
- Recommandations sur les paramètres à utiliser pour améliorer l'efficacité de vos mesures de sécurité
- Informations supplémentaires et articles d'aide

Documents pertinents du centre d'aide

Premiers pas avec la page "État de sécurité"

Bonnes pratiques concernant la sécurité

"Orientez-moi vers les bonnes pratiques et vers les recommandations à suivre pour configurer des règles de sécurité."

Ouvrez la page "État de sécurité" pour connaître les bonnes pratiques concernant les règles de sécurité. Voici ce que vous y trouverez :

- Recommandations pour les potentielles zones à risque de votre domaine
- Recommandations sur les paramètres à utiliser pour améliorer l'efficacité de vos mesures de sécurité
- Liens directs vers les paramètres
- Informations supplémentaires et articles d'aide

Instructions détaillées

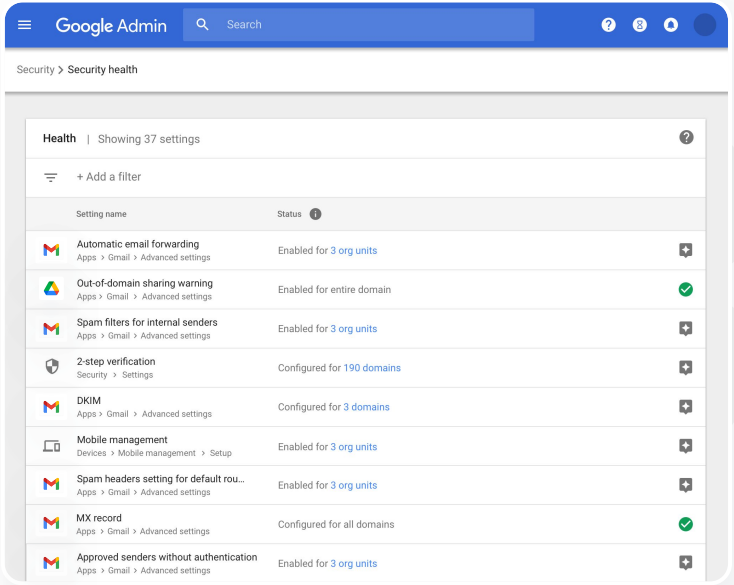
Documents pertinents du centre d'aide

Premiers pas avec la page "État de sécurité"

Instructions – Recommandations sur la sécurité

Afficher les recommandations

- Connectez-vous à la **console d'administration**.
- Cliquez sur **Sécurité** > **État de sécurité**.
- Consultez les paramètres d'état dans la colonne de droite.
  - Une coche verte indique que le paramètre est sécurisé.
  - Une icône grise indique qu'il y a une recommandation concernant ce paramètre : cliquez sur l'icône pour en savoir plus et obtenir les instructions à suivre.



Documents pertinents du centre d'aide

Premiers pas avec la page "État de sécurité"

> Je veux m'assurer que mon école est aussi sécurisée que possible, même si nous avons de plus en plus d'élèves et d'enseignants."

Instructions détaillées

Améliorer la sécurité d'une école en pleine croissance

Les administrateurs informatiques doivent suivre ces bonnes pratiques de sécurité pour renforcer la sécurité et la confidentialité des données de l'entreprise. Pour appliquer chacune des bonnes pratiques de cette checklist, vous pouvez utiliser un ou plusieurs paramètres de la console d'administration Google.

- Recommandations pour éviter le piratage et restaurer les comptes piratés
- Mesures à mettre en œuvre pour limiter le partage et la collaboration en dehors de votre domaine
- Fonctionnalités pour contrôler l'accès des tiers aux services principaux

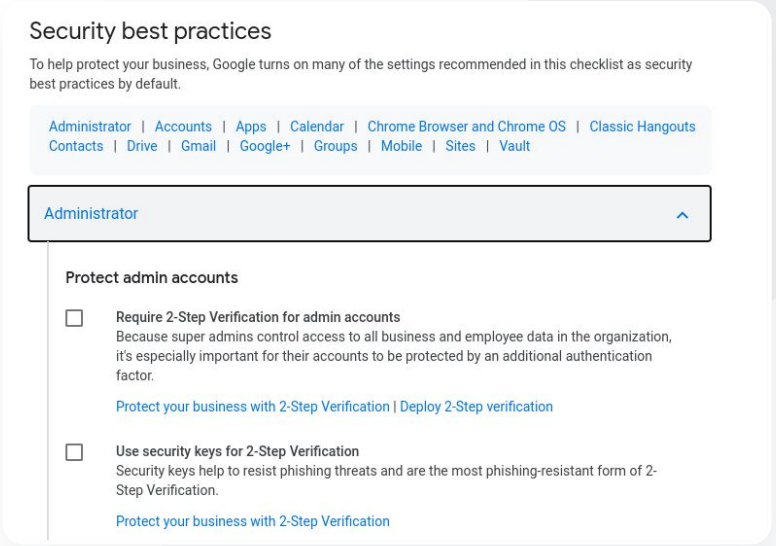
Documents pertinents du centre d'aide

Checklist de sécurité pour les moyennes et grandes entreprises

Instructions – Checklist de sécurité

Pour vous aider à protéger votre organisation, Google active par défaut la plupart des paramètres recommandés dans cette checklist, car leur utilisation fait partie des bonnes pratiques de sécurité. Nous vous conseillons d'examiner d'un peu plus près les paramètres présentés ci-dessous.

- **Administrateur :** permet de protéger les comptes administrateur
- **Comptes :** permet d'empêcher le piratage et de restaurer les comptes piratés
- **Applications :** permet de contrôler l'accès des applications tierces aux services principaux
- **Agenda :** permet de limiter le partage d'agendas en externe
- **Drive :** permet de limiter le partage et la collaboration en dehors de votre domaine
- **Gmail :** permet de configurer l'authentification et l'infrastructure
- **Vault :** permet de contrôler, d'auditer et de sécuriser les comptes Vault



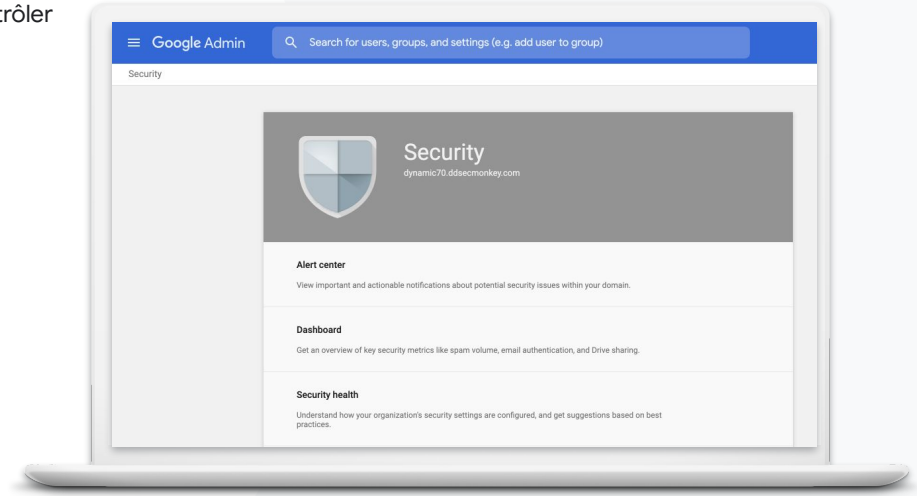
Documents pertinents du centre d'aide

Surveiller l'état de vos paramètres de sécurité

Commandes d'administration avancées

De quoi s'agit-il ?

Les commandes d'administration avancées vous permettent de surveiller et de contrôler les utilisateurs et appareils qui ont accès à votre domaine ainsi qu'à vos données.



Cas d'utilisation

Lois réglementaires sur les données	Instructions détaillées
Réglementation des authentifications	Instructions détaillées
Restrictions sur les applications	Instructions détaillées
Gérer des appareils mobiles	Instructions détaillées
Migrer des données	Instructions détaillées

Lois réglementaires sur les données

Les données des élèves, des enseignants et des membres du personnel de l'établissement doivent rester aux États-Unis pour des questions réglementaires."

Instructions détaillées

En tant qu'administrateur, vous pouvez stocker vos données dans un emplacement géographique spécifique (vous avez le choix entre les États-Unis et l'Europe/le Royaume-Uni) en utilisant une **règle pour la région des données**.

- Vous pouvez choisir une région pour stocker les données de certains utilisateurs, ou différentes régions pour les données de services ou équipes spécifiques.
- Placez les utilisateurs dans une unité organisationnelle (pour appliquer le paramètre en fonction du service) ou ajoutez-les dans un groupe de configuration (pour appliquer le paramètre à des utilisateurs dans plusieurs services).
- Les utilisateurs ne disposant pas de licence Education Standard ou Education Plus n'ont pas accès aux règles pour les régions des données.

Documents pertinents du centre d'aide

Choisir l'emplacement géographique de vos données

Réglementation des authentifications

"Les travaux de recherche de l'établissement doivent rester aux États-Unis pour des questions de réglementation des authentifications."

En tant qu'administrateur, vous pouvez stocker les travaux de recherche des enseignants dans un emplacement géographique spécifique (vous avez le choix entre les États-Unis et l'Europe) en utilisant une **règle pour la région des données**.

- Les règles pour les régions des données couvrent les principales données au repos (y compris les sauvegardes) de la plupart des services principaux de Google Workspace for Education présentés ici.
- Pesez le pour et le contre avant de définir une règle pour la région de vos données. Les utilisateurs situés en dehors de la région où leurs données sont stockées peuvent subir une latence accrue dans certains cas.

Instructions détaillées

Documents pertinents du centre d'aide

Choisir l'emplacement géographique de vos données

Instructions – Régions des données*

Définir les régions des données

- Connectez-vous à la **console d'administration**.
  - Remarque : Vous devez être connecté en tant que super-administrateur.
- Cliquez sur **Profil de l'entreprise** > **Afficher plus** > **Régions de données**.
- Sélectionnez l'**unité organisationnelle ou le groupe de configuration** auxquels vous voulez attribuer une région de stockage des données, ou sélectionnez toute la colonne pour inclure l'ensemble des unités et des groupes.
- Sélectionnez la région. Vous avez le choix entre **"Aucune préférence", "États-Unis" ou "Europe"**.
- Cliquez sur **Enregistrer**.

Documents pertinents du centre d'aide

Choisir l'emplacement géographique de vos données

* Seuls les établissements qui disposent d'Education Standard ou d'Education Plus peuvent utiliser la fonctionnalité des régions des données pour stocker leurs données dans une région spécifique.

Restrictions sur les applications

Je veux limiter l'accès à certaines applications lorsque les utilisateurs sont sur le réseau."

Grâce à l'**accès contextuel***, vous pouvez créer des règles précises d'accès aux applications, sur la base d'attributs comme l'identité des utilisateurs, le lieu, le niveau de sécurité des appareils et l'adresse IP. Vous pouvez même restreindre l'accès des applications externes au réseau.

- Vous pouvez aussi appliquer des règles d'accès contextuel pour les services principaux de Google Workspace for Education.
- Par exemple, si un utilisateur se connecte à un service principal de Google Workspace dans son établissement scolaire, puis se rend dans un café, une règle d'accès contextuel pour ce service est de nouveau vérifiée lorsqu'il change d'emplacement.

Instructions détaillées

Documents pertinents du centre d'aide

Présentation de l'accès contextuel

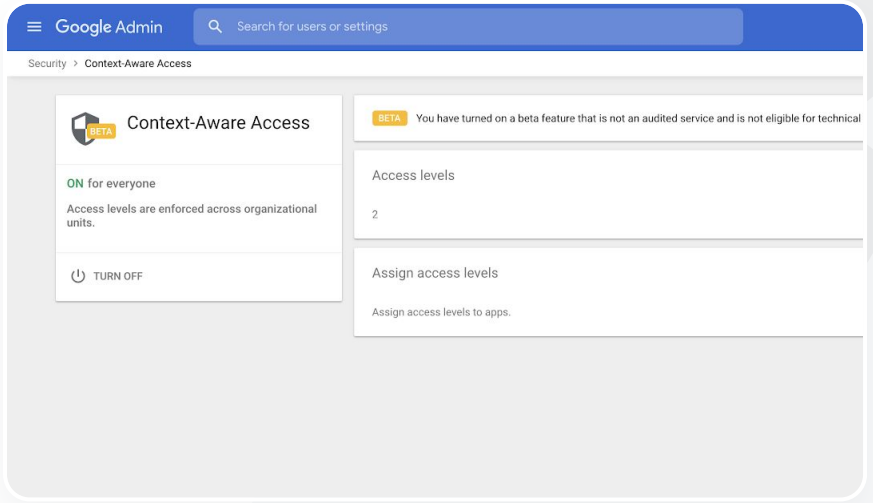
Attribuer des niveaux d'accès contextuel aux applications

* Seuls les établissements qui disposent d'Education Standard ou d'Education Plus peuvent appliquer des règles d'accès contextuel.

Instructions – Accès contextuel

Utiliser l'accès contextuel

- Connectez-vous à la **console d'administration**.
- Sélectionnez **Sécurité** > **Accès contextuel** > Attribuer.
- Sélectionnez **Attribuer des niveaux d'accès** pour afficher votre liste d'applications.
- Sélectionnez **une unité organisationnelle ou un groupe de configuration** pour trier la liste.
- Sélectionnez **Attribuer** à côté de l'application concernée.
- Sélectionnez un ou plusieurs niveaux d'accès.
- Créez plusieurs niveaux si vous voulez que les utilisateurs remplissent plusieurs conditions d'accès.
- Cliquez sur "**Enregistrer**".



Documents pertinents du centre d'aide

Présentation de l'accès contextuel

Attribuer des niveaux d'accès contextuel aux applications

Gérer des appareils mobiles

Je dois pouvoir gérer les règles et les appliquer sur tous les types d'appareils (iOS, Windows 10, etc.) de mon secteur (pas uniquement les Chromebooks), en particulier si la sécurité de l'un d'eux est compromise."

Instructions détaillées

La **gestion avancée des appareils mobiles** peut vous aider à mieux contrôler les données de votre organisation sur ce type d'appareils. Vous pouvez restreindre les fonctionnalités d'un appareil mobile, exiger le chiffrement de l'appareil, gérer les applications sur les appareils Android, les iPhone et les iPad, et effacer les données d'un appareil.

- Vous pouvez également approuver, bloquer, débloquer ou supprimer des appareils depuis la console d'administration.
- Si un utilisateur perd un appareil ou quitte l'école, vous pouvez effacer son compte, son profil et même toutes ses données de l'appareil géré dont il se servait. L'utilisateur pourra toujours accéder à ses données sur un ordinateur ou dans un navigateur Web.

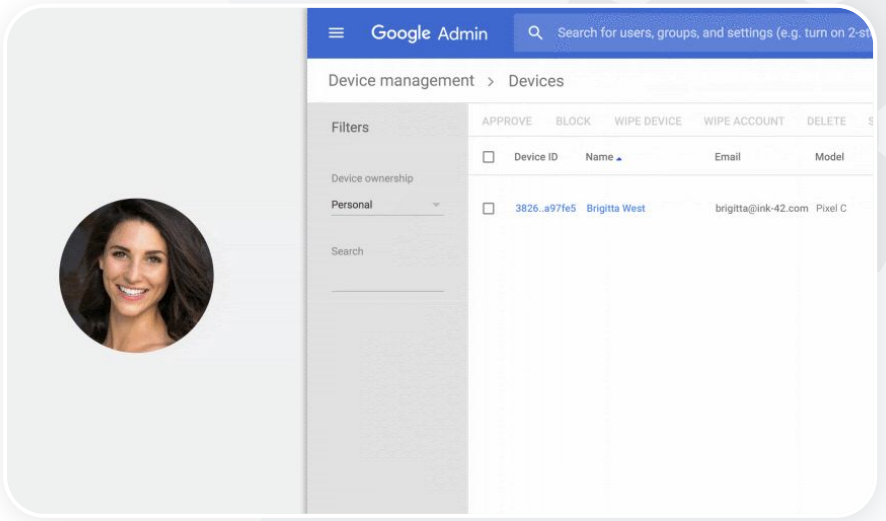
Documents pertinents du centre d'aide

Configurer la gestion avancée des appareils mobiles
Approuver, bloquer, débloquer ou supprimer un appareil
Effacer les données d'un appareil

Instructions – Activer la gestion avancée des appareils mobiles

Activer la gestion avancée des appareils mobiles

- Connectez-vous à la **console d'administration**.
- Dans la **console d'administration**, sélectionnez **Appareils**.
- Sur la gauche, cliquez sur **Paramètres** > **Paramètres universels**.
- Cliquez sur **Général** > **Gestion des appareils mobiles**.
- Pour appliquer le paramètre à tous les utilisateurs, vérifiez que l'unité organisationnelle racine est sélectionnée. Sinon, sélectionnez une unité organisationnelle enfant.
- Sélectionnez **Avancé**.
- Cliquez sur **Enregistrer**.



Documents pertinents du centre d'aide

Configurer la gestion avancée des appareils mobiles

Approuver, bloquer, débloquer ou supprimer un appareil

Effacer les données d'un appareil

Migrer des données

Les **guides de migration** vous aideront à transférer les données de toute votre organisation (comme les e-mails, les agendas, les contacts, les dossiers, les fichiers et les autorisations) vers Google Workspace.

> Nous passons à Google Workspace et nous devons migrer toutes nos données vers notre nouvel environnement Google."

Données pour moins de 1 000 utilisateurs

Consultez la matrice des outils de migration pour déterminer la solution la plus adaptée aux besoins de votre établissement.

En savoir plus

Données pour plus de 1 000 utilisateurs

Utilisez Google Workspace Migrate pour migrer de grandes quantités de données efficacement.

En savoir plus

Instructions détaillées

Documents pertinents du centre d'aide

Effectuer la migration des données de votre organisation vers Google Workspace

Matrice des outils de migration de Google Workspace

À propos de Google Workspace Migrate

Installer et configurer Google Workspace Migrate

Instructions – Google Workspace Migrate

Avant de commencer

Connectez-vous à la version bêta et vérifiez que vous disposez de la configuration système requise.

Instructions

1. Configurer la **console Google Cloud**

Activer des API
Créer l'ID client Web OAuth
Créer un compte de service Google Workspace

1. Configurer la **console d'administration**

Configurer les rôles d'administrateur
Autoriser votre ID client

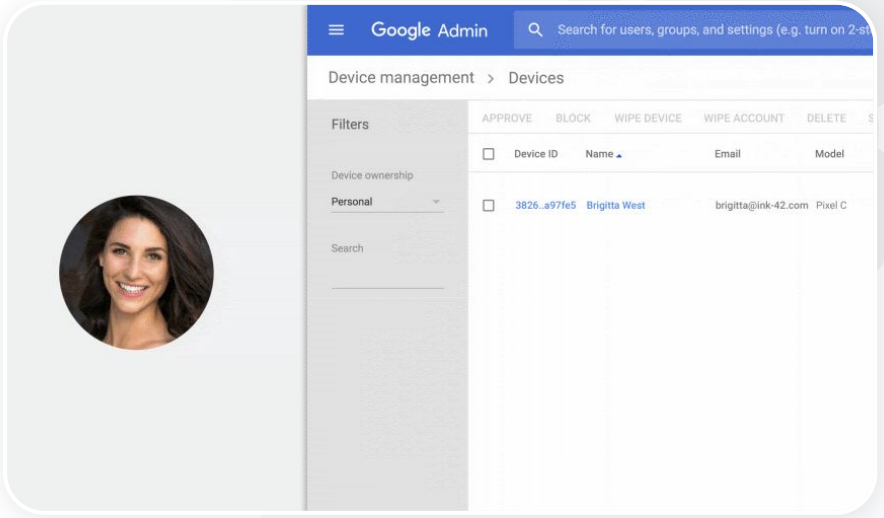
3. **Télécharger et installer**

Télécharger les programmes d'installation
Installer les bases de données
Installer et configurer la plate-forme
Installer les serveurs de nœuds
(Facultatif) Configurer le serveur de nœuds pour utiliser le protocole TLS

3. **Configurer les outils de migration**

Configurer la clé de chiffrement
Configurer les paramètres de base de données
Configurer l'adresse de rappel
Ajouter les serveurs de nœud
Créer un projet

Besoin d'aide ? Contactez un partenaire Google Cloud.

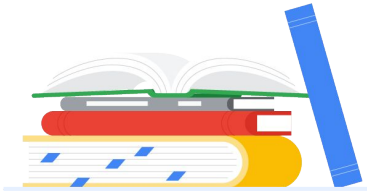


Documents pertinents du centre d'aide

À propos de Google Workspace Migrate
Installer et configurer Google Workspace Migrate
Effectuer la migration des données de votre organisation vers Google Workspace
Matrice des outils de migration de Google Workspace

Outils d'enseignement et d'apprentissage

Permettez à vos enseignants d'accéder à des fonctionnalités supplémentaires dans votre environnement d'apprentissage numérique. Ils pourront ainsi bénéficier d'une communication vidéo améliorée, d'expériences en classe plus riches et d'outils favorisant l'intégrité académique.



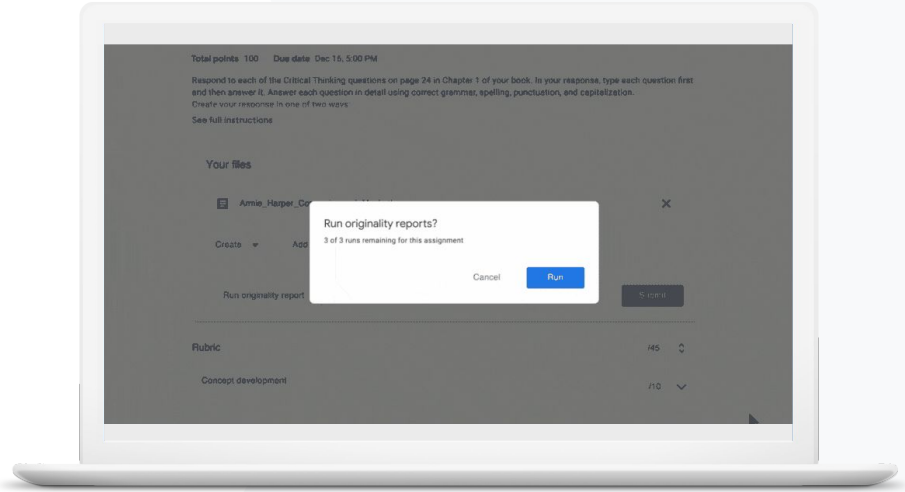
Rapports sur le degré d'originalité

Google Meet

Rapports sur le degré d'originalité

De quoi s'agit-il ?

Les rapports sur le degré d'originalité permettent aux enseignants et aux élèves de vérifier l'authenticité des devoirs. Ces rapports comparent le travail des élèves à des milliards de pages Web et à des millions d'ouvrages à l'aide de la recherche Google. Ils affichent ensuite des liens vers les pages Web détectées et signalent le texte dont l'auteur n'est pas cité.



Cas d'utilisation

Détecter les cas de plagiat	Instructions détaillées
Apprendre de ses erreurs avec la détection des cas de plagiat	Instructions détaillées

Détecter les cas de plagiat

Je veux détecter les cas de plagiat et les citations incorrectes dans les devoirs de mes élèves."

Les enseignants peuvent contrôler l'authenticité des devoirs de leurs élèves en s'aidant des **rapports sur le degré d'originalité**. Ces rapports comparent le travail des élèves à des milliards de pages Web et à des millions d'ouvrages à l'aide de la recherche Google.

- Les enseignants qui utilisent Teaching and Learning Upgrade ou Education Plus bénéficient d'un accès illimité aux rapports sur le degré d'originalité.
- Actuellement, ces rapports sont uniquement disponibles :
  - dans les comptes Google dont la langue a été définie sur "Anglais" ;
  - pour les devoirs réalisés dans Docs ;
  - dans les comptes Google for Education.

Instructions détaillées

Documents pertinents du centre d'aide

Activer les rapports sur le degré d'originalité

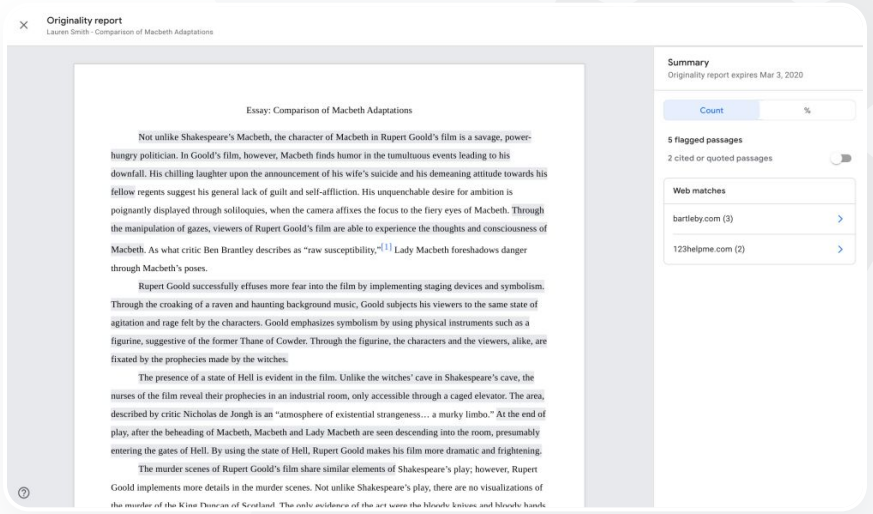
Instructions – Post-vérifications par l'enseignant

Activer les rapports sur le degré d'originalité pour un devoir

- Connectez-vous à votre compte Classroom sur **classroom.google.com**.
- Dans la liste, sélectionnez la classe concernée et cliquez sur **Travaux et devoirs**.
- Sélectionnez **Créer** > **Devoir**.
- Cochez la case à côté de **Rapports sur le degré d'originalité** pour activer la fonctionnalité.

Générer un rapport sur le degré d'originalité d'un devoir

- Dans la liste, sélectionnez le fichier de l'élève concerné et cliquez dessus pour l'ouvrir dans l'outil de notation.
- Sous le devoir de l'élève, cliquez sur **Vérifier l'absence de contenu plagié**.



Documents pertinents du centre d'aide

[Activer les rapports sur le degré d'originalité]

“

Je veux que mes élèves puissent identifier les cas de plagiat dans leurs devoirs pour qu'ils apprennent à corriger d'eux-mêmes de telles erreurs."

Instructions détaillées

Apprendre de ses erreurs avec la détection des cas de plagiat

Avant de rendre leur travail, les élèves peuvent générer jusqu'à trois **rapports sur le degré d'originalité** par devoir pour vérifier s'il contient des contenus involontairement plagiés ou dont les auteurs n'ont pas été cités. Ces rapports comparent le fichier Docs du devoir réalisé avec différentes sources et signalent les textes dont les auteurs n'ont pas été cités. Grâce aux rapports sur le degré d'originalité, les élèves peuvent apprendre de leurs erreurs et corriger leurs devoirs pour les rendre en toute confiance.

- Dans Teaching and Learning Upgrade et Education Plus, les enseignants peuvent activer les rapports sur le degré d'originalité de façon illimitée, tandis que dans Education Fundamentals, ils ne peuvent activer la fonctionnalité que cinq fois par cours.
- Lorsque l'élève a rendu son travail, Classroom génère automatiquement un rapport que seul l'enseignant peut voir. Si l'élève annule l'envoi d'un devoir et qu'il le renvoie, Classroom génère un nouveau rapport sur le degré d'originalité pour l'enseignant.

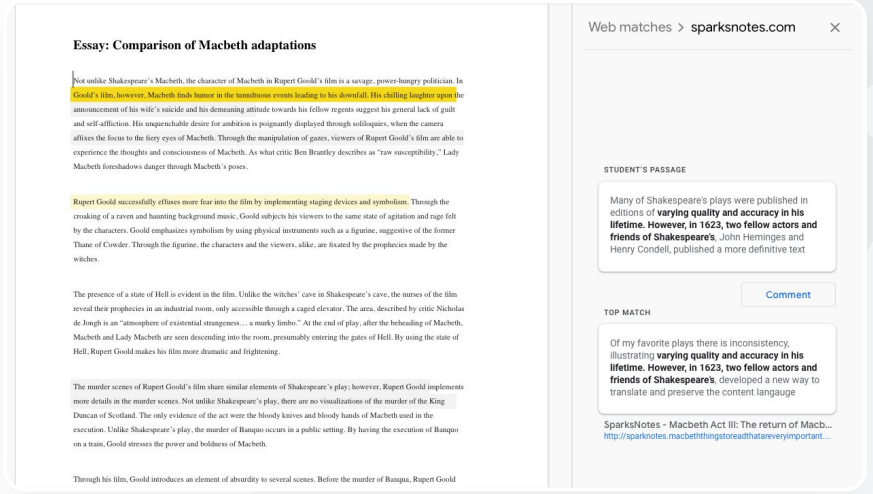
Documents pertinents du centre d'aide

Générer un rapport sur le degré d'originalité de votre travail

Instructions – Vérifications préalables par l'élève

Générer des rapports sur le degré d'originalité (pour l'élève)

- Connectez-vous à votre compte Classroom sur classroom.google.com.
- Dans la liste, sélectionnez la classe concernée et cliquez sur **Travaux et devoirs**.
- Dans la liste, sélectionnez le devoir concerné et cliquez sur **Afficher le devoir**.
- Sous **Votre devoir**, **importez** ou **créez votre fichier**.
- Cliquez sur **Exécuter** à côté de **Rapports sur le degré d'originalité**.
- Sous le nom de fichier du devoir, cliquez sur **Afficher le rapport sur le degré d'originalité** pour ouvrir le rapport.
- Pour réviser le devoir, le modifier ou citer correctement les passages signalés, cliquez sur **Modifier** en bas de la page.



Documents pertinents du centre d'aide

Générer un rapport sur le degré d'originalité de votre travail

Google Meet

De quoi s'agit-il ?

Google Meet propose différentes fonctionnalités avancées comme la diffusion en direct, les sessions en petits groupes, les enregistrements des réunions stockés sur Drive, les réunions pouvant accueillir jusqu'à 250 participants, les rapports de participation et bien plus encore.

Cas d'utilisation

Visioconférences sécurisées	Instructions détaillées
Améliorer la sécurité des visioconférences	Instructions détaillées
Enregistrer les cours	Instructions détaillées
Enregistrer les réunions d'établissement	Instructions détaillées
Cours manqués	Instructions détaillées
Réunions diffusées en direct	Instructions détaillées
Événements de l'établissement diffusés en direct	Instructions détaillées
Poser des questions	Instructions détaillées
Rassembler des données	Instructions détaillées
Petits groupes d'élèves	Instructions détaillées
Suivi de la participation	Instructions détaillées

Visioconférences sécurisées

Avec Google Meet, les établissements d'enseignement bénéficient de l'infrastructure sécurisée à la conception, de la protection intégrée et du réseau mondial qui permettent à Google de sécuriser vos informations et de protéger la confidentialité de vos données. Vous pouvez faire confiance aux mesures de sécurité suivantes dans Google Meet :

> Google Meet : est-ce vraiment sécurisé ?"

- **Confidentialité et conformité :** nous respectons des normes éducatives strictes pour sécuriser davantage les données des élèves et de l'établissement.
- **Chiffrement :** toutes les données en transit entre le client et Google sont chiffrées.
- **Mesures pour lutter contre les abus :** elles permettent au modérateur de contrôler les participants et de s'assurer que seules les bonnes personnes sont présentes.
- **Déploiement, accès et paramètres sécurisés :** différentes mesures de précaution sont prises pour garantir la confidentialité et la sécurité des réunions.
- **Gestion des incidents :** elle représente un aspect essentiel du programme global de sécurité et de confidentialité de Google. Elle est indispensable pour assurer la conformité avec les réglementations internationales sur la confidentialité des données.
- **Fiabilité :** l'infrastructure cloud native multicouche est conçue pour évoluer et pour supporter les pics d'utilisation.
- **Contrôle des accès :** nous avons apporté des améliorations à la gestion groupée des demandes de participation et à leur blocage quand certains critères sont remplis.
- **Commandes de verrouillage :** les modérateurs peuvent contrôler qui peut discuter dans le chat, présenter son écran ou même parler pendant une réunion virtuelle.

Instructions détaillées

Améliorer la sécurité des visioconférences

Comment puis-je mieux sécuriser les visioconférences pour mon établissement ?"

Pour lutter contre les abus, Teaching and Learning Upgrade et Education Plus appliquent des mesures telles que l'autorisation obligatoire pour les participants externes, les commandes améliorées pour la modération des réunions et les **réunions avec un alias** afin d'empêcher les utilisateurs de réutiliser les réunions terminées. Dès que le dernier participant a quitté une réunion, plus aucun autre participant ne peut la rejoindre. Les élèves ne peuvent pas participer à nouveau à une réunion avec un alias tant que l'enseignant ne l'a pas redémarrée.

- Dans les **réunions avec un alias**, dès que le dernier participant a quitté une réunion, les participants ne peuvent plus la rejoindre et le code de réunion à 10 chiffres n'est plus valide.
- Les élèves ne peuvent pas participer à nouveau à une réunion avec un alias tant que l'enseignant ne l'a pas redémarrée.
- L'enseignant peut mettre fin à la réunion pour tous les participants afin d'éviter qu'ils y restent une fois qu'il l'a quittée.

Instructions détaillées

Documents pertinents du centre d'aide

Sécurité et confidentialité dans Meet pour l'éducation

Démarrer une visioconférence avec Google Meet

Instructions – Réunions avec un alias

Créer une réunion avec un alias

- Utilisez un lien court tel que g.co/meet/[SAISIR L'ALIAS].
- Accédez à meet.google.com ou à l'application mobile Google Meet, puis saisissez un alias de réunion dans le champ **Rejoindre ou démarrer une réunion**.

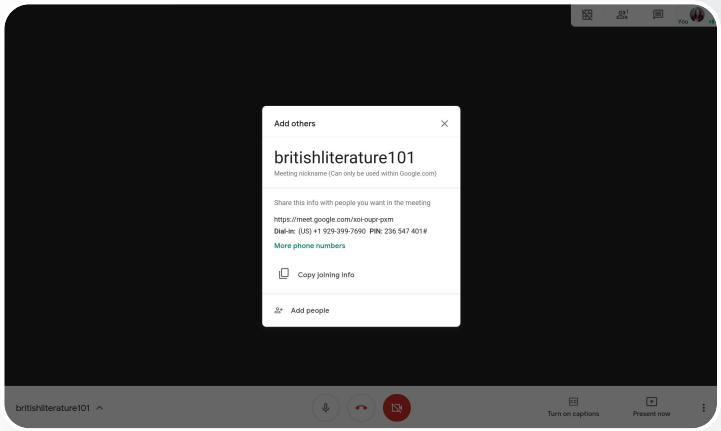
Fonctionnement

Lorsqu'un enseignant démarre une réunion avec un alias, un code de réunion à 10 caractères est créé et temporairement associé à l'alias.

Une fois que la dernière personne a quitté la réunion ou que l'enseignant y a mis fin, le code de réunion temporaire expire, ainsi que l'association entre l'alias et le code de la réunion.

Si les élèves n'ont pas l'autorisation de créer des réunions, ils ne peuvent pas utiliser l'alias ni le code de la réunion.

Les enseignants peuvent réutiliser l'alias. Dans ce cas, un nouveau code de réunion temporaire est généré et les élèves peuvent ensuite rejoindre la réunion à l'aide de l'alias.



Documents pertinents du centre d'aide

Sécurité et confidentialité dans Meet pour l'éducation

Démarrer une visioconférence avec Google Meet

Enregistrer les cours

Les utilisateurs de Teaching and Learning Upgrade et Education Plus peuvent **enregistrer** leurs réunions et faire en sorte qu'elles soient automatiquement stockées dans Drive, sans limite de temps. Cela permet d'archiver et de partager facilement des cours, des ateliers et des sessions de travail.

- Si vos enseignants utilisent Classroom, l'intégration de Google Meet leur permet de créer un lien unique pour chaque cours affiché sur les pages "Flux" et "Travaux et devoirs" de Classroom.
- Ce lien fait office d'espace de réunion pour chaque cours, ce qui permet aux enseignants et aux élèves d'y participer facilement.
- Enregistrez facilement vos cours grâce à l'intégration de Google Meet.

> Notre campus propose de nombreux cours en ligne que nous devons enregistrer pour l'enseignement à distance et pour les élèves qui ne peuvent pas être présents."

Instructions détaillées

Documents pertinents du centre d'aide

Configurer Meet pour l'enseignement à distance

Enregistrer les réunions d'établissement

Teaching and Learning Upgrade et Education Plus permettent de stocker automatiquement les **enregistrements** des visioconférences sur Drive. Ces enregistrements restent disponibles aussi longtemps que l'utilisateur en a besoin. Cela permet d'archiver et de partager facilement les réunions, les cours de formation professionnelle ou les réunions de direction.

- Nous recommandons aux administrateurs informatiques de n'activer l'enregistrement que pour les enseignants et le personnel.
- Vous pouvez ajouter des unités organisationnelles distinctes pour vos enseignants et vos élèves, puis appliquer des règles d'accès différentes.
- Si vous utilisez Classroom et que vos enseignants sont validés, vous pouvez activer l'accès pour votre groupe d'enseignants.

> Nous avons régulièrement des réunions en ligne avec le personnel et nous devons toutes les enregistrer. De plus, nous voulons enregistrer les cours de formation professionnelle, de même que les réunions de direction."

Instructions détaillées

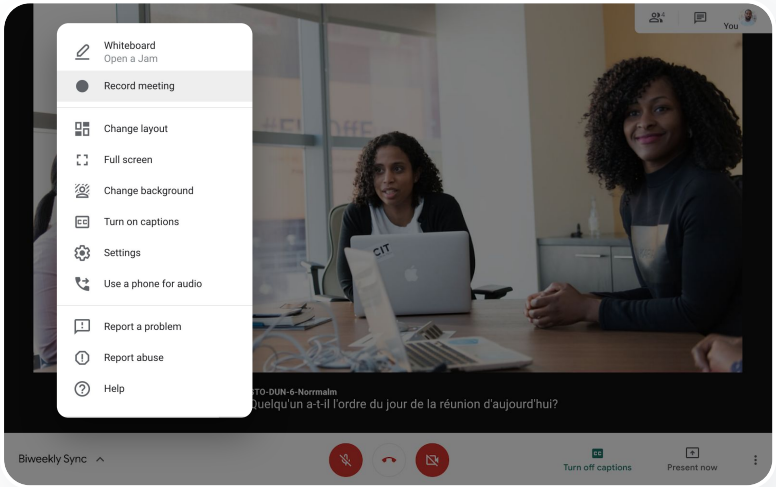
Documents pertinents du centre d'aide

Configurer Meet pour l'enseignement à distance

Instructions – Enregistrement

Enregistrer une réunion

- Dans Agenda, ouvrez la réunion et sélectionnez **Participer avec Google Meet**.
- Sur la page de confirmation de la réunion, cliquez sur les trois points verticaux en bas à droite pour **ouvrir le menu d'options**.
- Cliquez sur **Enregistrer la réunion**. Un point rouge s'affiche en bas à droite de l'écran pour indiquer que la réunion est en cours d'enregistrement.
- Le fichier vidéo de la réunion est automatiquement enregistré dans votre Drive.



Documents pertinents du centre d'aide

[Configurer Meet pour l'enseignement à distance]

Cours manqués

Je veux obtenir l'enregistrement du cours que j'ai manqué."

Tous les utilisateurs ont accès à un espace de stockage Drive sur le domaine de leur établissement. Dans Teaching and Learning Upgrade et Education Plus, les enregistrements des visioconférences sont automatiquement enregistrés dans l'espace de stockage Drive de l'organisateur de la réunion. Pour **visionner** la réunion enregistrée, demandez le lien de l'enregistrement à l'organisateur ou accédez-y depuis l'événement d'agenda.

- Les enregistrements sont conservés dans l'espace de stockage Drive de l'organisateur de la réunion.
- Les participants qui appartiennent à la même unité organisationnelle que celle de l'organisateur de la réunion ont automatiquement accès aux enregistrements.
- Si l'organisateur de la réunion change, le lien vers l'enregistrement de la réunion est envoyé au créateur initial de l'événement.

Instructions détaillées

Documents pertinents du centre d'aide

Enregistrer une visioconférence

Instructions – Afficher et partager des enregistrements

Partager un enregistrement

- Sélectionnez le fichier.
- Cliquez sur l'icône **Partager**.
- **Ajoutez** les utilisateurs approuvés.

OU

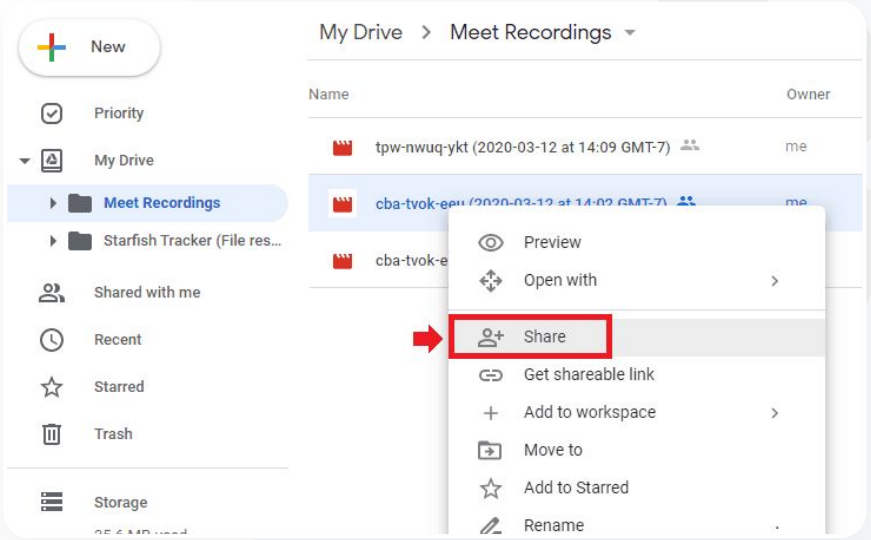
- Sélectionnez l'icône **Lien**.
- **Collez** le lien dans un e-mail ou dans un message Chat.

Télécharger un enregistrement

- Sélectionnez le fichier.
- Cliquez sur l'icône **Plus** > **Télécharger**.
- **Double-cliquez** sur le fichier téléchargé pour le lire.

Lire un enregistrement depuis Drive

- Dans Drive, double-cliquez sur le fichier de l'enregistrement pour l'ouvrir en lecture seule. Tant qu'il n'est pas prêt, un message s'affiche pour indiquer qu'il est en cours de traitement.
- Pour ajouter un enregistrement à votre Drive, sélectionnez le fichier souhaité, puis cliquez sur **Ajouter à Mon Drive**.



Documents pertinents du centre d'aide

Enregistrer une visioconférence

> Nous devons être en mesure de diffuser en direct les réunions du personnel ou des enseignants pour les parents et d'autres personnes concernées."

Instructions détaillées

Réunions diffusées en direct

Vous pouvez diffuser vos réunions en direct pour 10 000 utilisateurs de votre domaine au maximum avec Teaching and Learning Upgrade et pour 100 000 utilisateurs de votre domaine au maximum avec Education Plus. Les participants peuvent rejoindre la réunion en cliquant sur le lien de la diffusion en direct que l'organisateur leur a envoyé dans une invitation Agenda ou par e-mail. Vérifiez auprès de votre administrateur informatique que vous disposez bien des droits de diffusion en direct.

- Nous recommandons aux administrateurs informatiques de n'activer la diffusion en direct que pour les enseignants et le personnel.
- Pour bénéficier d'une meilleure expérience lors des grands événements, choisissez une diffusion en direct plutôt qu'une visioconférence interactive que les utilisateurs rejoignent.
- Si un utilisateur manque la diffusion en direct, il peut la voir en différé une fois que la réunion est terminée.

Documents pertinents du centre d'aide

Configurer Meet pour l'enseignement à distance

> Nous aimerions diffuser en direct nos événements sportifs, ainsi que d'autres événements importants, tels que les cérémonies de remise des diplômes ou les soirées de l'établissement, pour ceux qui ne peuvent pas y assister en personne."

Instructions détaillées

Événements de l'établissement diffusés en direct

Toute la communauté scolaire peut assister aux événements de l'établissement grâce à la **diffusion en direct**. Pour cela, il suffit de cliquer sur le lien de diffusion en direct que l'organisateur de l'événement a envoyé dans une invitation Agenda ou par e-mail. Vérifiez auprès de votre administrateur informatique que vous disposez bien des droits de diffusion en direct. À défaut d'y assister en direct, il est possible de voir la diffusion en différé une fois que la réunion est terminée.

- Utilisez la fonctionnalité de diffusion en direct de Google Meet pour que toute votre communauté puisse participer aux cérémonies de remise des diplômes, aux événements sportifs ou aux conseils d'école.
- Vous pouvez diffuser vos réunions en direct pour 10 000 utilisateurs de votre domaine au maximum avec Teaching and Learning Upgrade et pour 100 000 utilisateurs de votre domaine au maximum avec Education Plus.

Documents pertinents du centre d'aide

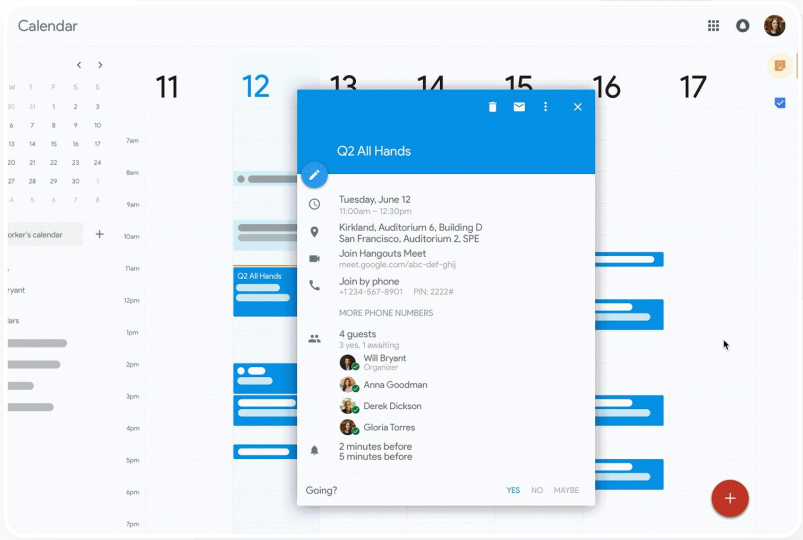
Configurer Meet pour l'enseignement à distance

Instructions – Diffusion en direct

Autoriser la diffusion en direct

- Ouvrez **Google Agenda**.
- Cliquez sur l'icône **Plus** > **Créer** > **Autres options**.
- Ajoutez les détails de l'événement tels que la date, l'heure et la description.
- Vous pouvez inviter jusqu'à 250 participants pouvant bénéficier de toutes les fonctionnalités de visioconférence. Cela signifie que l'on pourra les voir et les entendre, et qu'ils pourront présenter la visioconférence. Vous pouvez ajouter des participants extérieurs à votre organisation.
- Cliquez sur **Ajouter une conférence** > **Meet**.
- À côté de "Participer avec Google Meet", cliquez sur la **flèche vers le bas**, puis sur **Ajouter une diffusion en direct**.
- Pour inviter autant de personnes du domaine que le permet votre édition payante, cliquez sur **Copier**, puis partagez l'URL de la diffusion en direct par e-mail ou dans un message Chat.
- Sélectionnez **Enregistrer**.
- La diffusion en direct ne démarre pas automatiquement.
  Au début de la réunion, cliquez sur **Plus** > **Démarrer la diffusion**.

Remarque : Seuls les invités appartenant à votre organisation peuvent accéder à la diffusion en direct.



Documents pertinents du centre d'aide

Configurer Meet pour l'enseignement à distance

Poser des questions

> Il me faut un moyen rapide de poser des questions, d'évaluer les connaissances des élèves et d'interagir avec eux pour continuer à capter leur attention."

La fonctionnalité **Questions/Réponses** de Google Meet vous aide à continuer à capter l'attention des élèves et à rendre la classe plus interactive. Les enseignants reçoivent même un rapport détaillé de toutes les questions et réponses à la fin du cours virtuel.

- Les modérateurs peuvent poser autant de questions que nécessaire. Ils peuvent filtrer ou trier les questions, les marquer comme répondues et même les masquer ou les classer par ordre de priorité.
- Après chaque réunion où la fonctionnalité Questions/Réponses est activée, un rapport sur les questions est automatiquement envoyé par e-mail au modérateur.

Instructions détaillées

Documents pertinents du centre d'aide

Poser des questions aux participants dans Google Meet

Instructions – Questions/Réponses

Poser une question :

- Lors d'une réunion, en haut à droite de l'écran, cliquez sur l'icône **Activités** > **Questions** (pour activer la fonctionnalité Questions/Réponses, cliquez sur **Activer Questions/Réponses**).
- Pour poser une question, cliquez sur **Poser une question** en bas à droite.
- **Saisissez vos questions**, puis cliquez sur **Publier.**

Consulter le rapport sur les questions :

- Après une réunion, le modérateur **reçoit par e-mail un rapport sur les questions.**
- Ouvrez l'e-mail > cliquez sur le **rapport en pièce jointe.**

Documents pertinents du centre d'aide

[Poser des questions aux participants dans Google Meet]

Rassembler des données

Il me faut un moyen facile de rassembler les données des élèves et des autres enseignants lorsque je donne un cours ou que j'assiste à une réunion du personnel."

La personne qui a planifié ou démarré une réunion virtuelle peut créer un **sondage** pour les participants de la réunion. Cette fonctionnalité permet de regrouper les informations de tous les élèves ou participants de façon rapide et conviviale.

- Les modérateurs peuvent enregistrer un sondage et le publier ultérieurement au cours d'une réunion. Ils sont enregistrés dans la section "Sondage" d'une réunion virtuelle.
- Après la réunion, un rapport avec les résultats du sondage est automatiquement envoyé par e-mail au modérateur.

Instructions détaillées

Documents pertinents du centre d'aide

Organiser des sondages dans Google Meet

Instructions – Organiser des sondages

Créer un sondage :

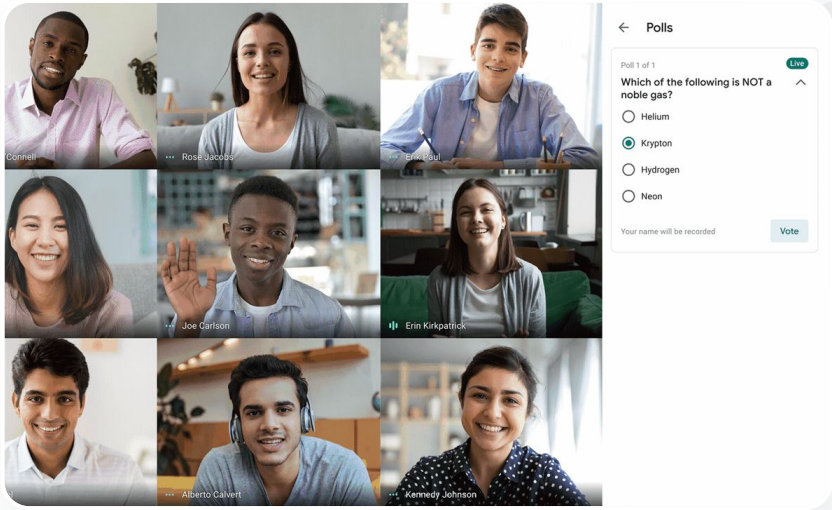
- En haut à droite de l'écran de réunion, cliquez sur l'icône **Activités** > **Sondage**.
- Cliquez sur **Démarrer un sondage**.
- Saisissez une question.
- Cliquez sur **Lancer** ou **Enregistrer**.

Modérer un sondage :

- En haut à droite de l'écran de réunion, cliquez sur l'icône **Activités** > **Sondage**.
- Pour que les participants d'un sondage puissent voir les résultats en temps réel, cliquez sur le bouton **Activer** à côté de l'option **Montrer les résultats à tout le monde**.
- Pour clôturer un sondage et ne pas autoriser les réponses, cliquez sur **Mettre fin au sondage**.
- Pour supprimer définitivement un sondage, cliquez sur l'icône **Supprimer**.

Afficher un rapport sur les sondages :

- Après une réunion, le modérateur **reçoit un rapport par e-mail**.
- Ouvrez l'e-mail > cliquez sur le **rapport en pièce jointe**.



Documents pertinents du centre d'aide

Organiser des sondages dans Google Meet

Petits groupes d'élèves

Les enseignants peuvent utiliser les **sessions en petits groupes** pour diviser leur classe en petits groupes lors des cours virtuels. Ce sont les modérateurs qui lancent ces sessions au cours d'un appel vidéo sur un ordinateur. Il est actuellement impossible de diffuser en direct ou d'enregistrer des sessions en petits groupes.

- Vous pouvez créer jusqu'à 100 sessions en petits groupes par réunion virtuelle.
- L'enseignant peut facilement passer d'une session à une autre pour aider les groupes, le cas échéant.
- Les administrateurs peuvent faire en sorte que seuls les enseignants ou le personnel soient autorisés à créer des sessions en petits groupes.

> Nous ne donnons que des cours à distance et nous aimerions pouvoir diviser la classe en petits groupes, parcourir la classe pour passer entre les groupes, participer aux discussions et rassembler facilement les groupes."

Instructions détaillées

Documents pertinents du centre d'aide

Utiliser les sessions en petits groupes dans Google Meet

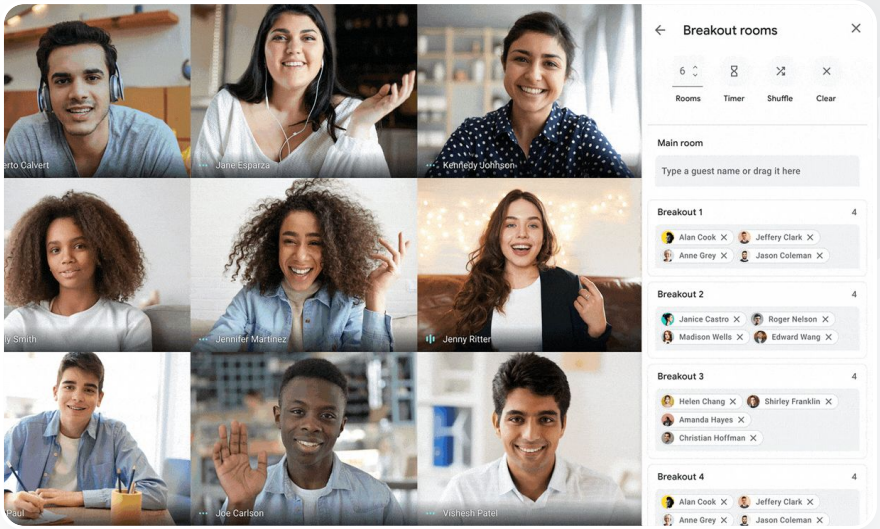
Instructions – Créer des sessions en petits groupes

Créer des sessions en petits groupes

- Démarrez un appel vidéo.
- En haut à droite, cliquez sur l'icône **Activités** > **Sessions en petits groupes**.
- Dans le panneau "Sessions en petits groupes", **choisissez le nombre de sessions en petits groupes** que vous souhaitez créer.
- Les élèves sont ensuite répartis dans les différentes sessions. Cependant, les modérateurs peuvent déplacer manuellement les participants d'une session à une autre si nécessaire.
- En bas à droite, cliquez sur **Ouvrir** les sessions.

Répondre aux questions dans les différentes sessions en petits groupes

- Chaque fois que des participants demandent de l'aide, une notification s'affiche en bas de l'écran du modérateur. Cliquez sur **Rejoindre** pour vous rendre dans la session de ces participants.



Documents pertinents du centre d'aide

Utiliser les sessions en petits groupes dans Google Meet

Suivi de la participation

"Nous avons du mal à suivre la participation des élèves aux cours en ligne. J'ai besoin de la contrôler facilement sur tout le domaine."

La fonctionnalité Suivi de la participation permet de créer un rapport de participation automatique pour les réunions comptant au moins cinq participants. Ce rapport indique le nom des participants qui ont rejoint la réunion, leur adresse e-mail et le temps qu'ils ont passé dans le cours virtuel.

- Avec les rapports sur les diffusions en direct, vous pouvez suivre la participation aux événements diffusés en direct.
- Les modérateurs peuvent activer ou désactiver le suivi de la participation et les rapports sur les diffusions en direct depuis une réunion ou un événement d'agenda.

Instructions détaillées

Documents pertinents du centre d'aide

Suivre la participation dans Google Meet

Instructions – Rapports de participation

Dans une réunion :

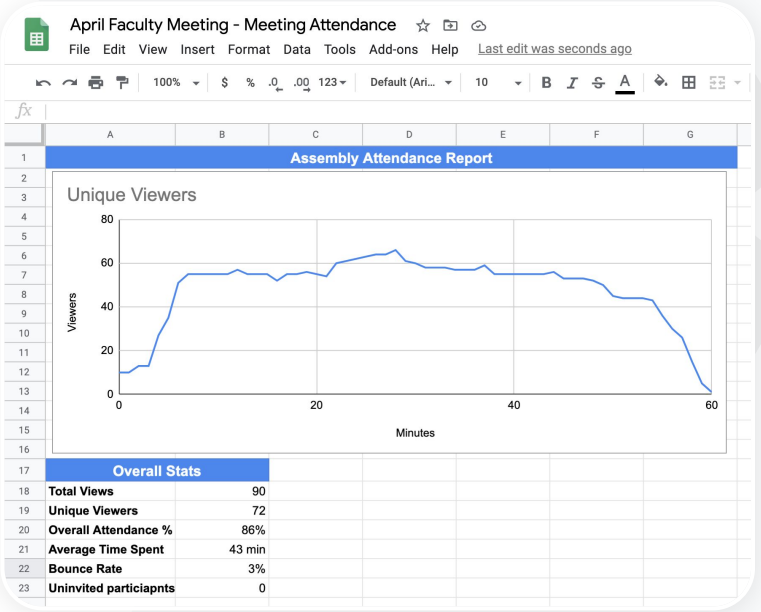
- Démarrez un appel vidéo.
- En bas de l'écran, cliquez sur l'**icône de menu**.
- Cliquez sur l'icône **Paramètres** > **Commandes de l'organisateur**.
- Activez ou désactivez l'option **Suivi de la participation**.

Dans Agenda :

- Dans un événement d'agenda, activez la fonctionnalité **Conférence de Google Meet**.
- Sur la droite, sélectionnez l'icône **Paramètres**.
- Cochez la case située à côté de **Suivi de la participation** > cliquez sur **Enregistrer**.

Obtenir le rapport de participation :

- Après une réunion, le modérateur **reçoit un rapport par e-mail**.
- Ouvrez l'e-mail > cliquez sur le **rapport en pièce jointe**.



Documents pertinents du centre d'aide

Suivre la participation dans Google Meet

Merci

Google for Education