

Conditions d'accès aux données Gmail en lecture seule

Ces conditions expliquent l'accès Gmail inbound que DynamicMail demande lorsqu'un utilisateur ou administrateur autorise de l'organisation cliente connecte Gmail pour l'ingestion de documents.

Ce document couvre uniquement Gmail inbound. Il ne doit pas être utilisé comme conditions complètes d'accès aux données Google Workspace pour Google Drive.

Portée

DynamicMail demande <https://www.googleapis.com/auth/gmail.readonly> uniquement lorsqu'un utilisateur ou administrateur autorise de l'organisation cliente connecte Gmail inbound pour l'ingestion de documents. Cette portée permet à DynamicMail de consulter les messages et les paramètres Gmail du compte Google connecté. DynamicMail l'utilise pour un traitement entrant en lecture seule et ne l'utilise pas pour envoyer, modifier, supprimer, archiver, étiqueter ou déplacer des messages Gmail.

Les portées d'identité Google Sign-In telles que `openid`, `email` et `profile` sont séparées de ce consentement d'accès aux données Gmail. Se connecter avec Google ne vaut pas acceptation de l'accès Gmail inbound.

Données auxquelles DynamicMail peut accéder

Lorsque Gmail inbound est connecté, DynamicMail peut accéder aux données Gmail nécessaires pour trouver et traiter les documents professionnels entrants, notamment:

- les identifiants de messages, les identifiants de fils de discussion, les identifiants d'historique, les références de libelles et les curseurs de synchronisation;
- l'expéditeur, le destinataire, l'objet, la date, les en-têtes et les autres métadonnées de message;
- les corps de message et extraits nécessaires pour identifier le contexte du document;
- les pièces jointes et fichiers intégrés qui peuvent contenir des factures, avis, accords, recus ou autres documents de l'organisation cliente;
- les paramètres Gmail uniquement lorsque l'API Gmail les exige pour la portée `readonly` ou pour le comportement de synchronisation du compte;
- les données dérivées créées à partir du contenu Gmail, comme le texte OCR, les champs de document analysés, les libelles de classification, les résultats d'extraction, les résumés, les événements d'audit et les enregistrements de documents.

DynamicMail ne devrait pas demander ni traiter de données Gmail sans rapport avec la fonctionnalité visible d'ingestion de documents entrants.

Finalité

DynamicMail utilise les données Gmail en lecture seule pour fournir la source Gmail inbound choisie par l'organisation cliente. Les finalités prévues sont:

- détecter les messages entrants susceptibles de contenir des documents professionnels de l'organisation cliente;
- importer les pièces jointes ou le contenu de message que l'organisation cliente choisit de traiter;
- extraire, classer et acheminer les documents dans les flux de travail DynamicMail;
- rapprocher l'état de synchronisation afin que le même message ne soit pas importé plusieurs fois;
- afficher l'état de connexion, de synchronisation et de traitement aux utilisateurs autorisés de l'organisation cliente;
- effectuer les activités de dépannage, de sécurité, d'audit et de conformité juridique autorisées par les politiques applicables et l'accord avec l'organisation cliente.

DynamicMail ne doit pas vendre les données Gmail, les utiliser pour la publicité ou le ciblage, les transférer à des courtiers en données, les utiliser à des fins de surveillance, ni les utiliser pour déterminer la solvabilité ou l'éligibilité à un prêt.

Conservation

DynamicMail conserve les données dérivées de Gmail uniquement aussi longtemps que nécessaire pour la fonctionnalité visible d'ingestion de documents entrants, les paramètres de conservation des documents de l'organisation cliente, les enregistrements d'audit, la sécurité, le traitement des litiges ou la conformité juridique. Les jetons OAuth et les métadonnées de synchronisation sont conservés uniquement pendant la durée nécessaire pour exploiter la source Gmail inbound connectée ou pour conserver les enregistrements d'audit requis.

Le contenu brut des messages Gmail, les pièces jointes et les données de document dérivées devraient être supprimées ou anonymisées lorsqu'ils ne sont plus nécessaires à la finalité déclarée, sauf si une obligation juridique, de sécurité, d'audit ou de conservation de l'organisation cliente exige leur conservation continue.

Suppression

Un utilisateur ou administrateur autorisé de l'organisation cliente peut demander la suppression des données Google mises en cache, des pièces jointes importées, du texte extrait et des enregistrements de documents dérivés. DynamicMail devrait supprimer ou

anonymiser les données demandées lorsque les paramètres de conservation de l'organisation cliente et le droit applicable le permettent.

La suppression des enregistrements importés dans DynamicMail ne supprime pas nécessairement l'e-mail ou la pièce jointe d'origine dans Gmail, car la portée Gmail readonly ne donne pas à DynamicMail l'autorisation de modifier ou supprimer des messages Gmail.

Revocation et déconnexion

L'organisation cliente peut déconnecter Gmail inbound dans DynamicMail. Après une déconnexion ou une révocation locale du consentement, DynamicMail doit cesser d'utiliser les jetons OAuth stockés pour Gmail inbound et doit cesser de lire d'autres messages Gmail depuis le compte connecté.

Le propriétaire du compte Google peut également révoquer l'autorisation de l'application dans les paramètres du compte Google. Si l'autorisation Google est révoquée, DynamicMail doit cesser l'accès à l'API Gmail lorsque l'actualisation des jetons ou les appels API échouent, et la connexion devrait être affichée comme déconnectée ou nécessitant une reconnexion.

La révocation locale ne supprime pas automatiquement les documents DynamicMail déjà importés. Ces enregistrements sont traités selon les règles de suppression et de conservation ci-dessus.

Utilisation de l'IA, de l'OCR et de l'extraction

DynamicMail peut utiliser l'OCR, l'analyse, la classification, le résumé et d'autres traitements assistés par l'IA sur le contenu des messages et les pièces jointes dérivées de Gmail uniquement pour fournir ou améliorer le flux de travail visible d'ingestion de documents entrants pour l'organisation cliente. Les données Gmail et les données dérivées ne doivent pas être utilisées pour créer, entraîner ou améliorer un modèle d'apprentissage automatique ou d'IA à usage général en dehors de la fonctionnalité demandée par l'organisation cliente.

Les résultats assistés par l'IA peuvent être incorrects. DynamicMail devrait présenter les données extraites comme une sortie de flux de travail que les utilisateurs autorisés peuvent examiner, corriger, approuver, rejeter ou supprimer selon le parcours produit.

Accès par le support et par des personnes

Le personnel, les contractants ou les sous-traitants de DynamicMail ne devraient pas lire des messages Gmail, pièces jointes, textes extraits ou données Gmail dérivées spécifiques, sauf si l'une des conditions suivantes s'applique:

- l'utilisateur a explicitement demandé une assistance qui nécessite l'accès à des données spécifiques;

- l'accès est nécessaire pour une enquête de sécurité, la prévention des abus ou la réponse à un incident;
- l'accès est nécessaire pour se conformer à la loi, à une procédure juridique ou à une instruction contraignante de l'organisation cliente;
- les données sont agrégées ou anonymisées pour les opérations internes et aucun contenu Gmail d'un utilisateur spécifique n'est lisible.

L'accès par le support devrait être fondé sur le moindre privilège, limité dans le temps lorsque cela est pratique, et journalisé à des fins d'audit.

Il s'agit d'un support d'implémentation et de localisation, pas d'un avis juridique final. Il ne doit pas être présenté comme portant une approbation de Google, une validation par un conseil externe ou une autorisation de production pour portée restreinte sans preuve de revue distincte.

References sources

- DynamicMail restricted-scope contract:
Documentation/DynamicMail/LocalizedIntegrations/google-restricted-scope-compliance-contract-2026-06-02.md
- Google API Services User Data Policy: <https://developers.google.com/terms/api-services-user-data-policy>
- Google Workspace API user data and developer policy:
<https://developers.google.com/workspace/workspace-api-user-data-developer-policy>
- Gmail API scopes: <https://developers.google.com/workspace/gmail/api/auth/scopes>
- Google restricted-scope verification guidance:
<https://developers.google.com/identity/protocols/oauth2/production-readiness/restricted-scope-verification>