

Términos de acceso a datos de Gmail de solo lectura

Estos términos explican el acceso restringido de la función Gmail inbound que DynamicMail solicita para <https://www.googleapis.com/auth/gmail.readonly> cuando un usuario autorizado o un administrador del cliente conecta Gmail inbound para la recepción de documentos.

Este activo cubre únicamente Gmail inbound. No debe utilizarse como términos completos de acceso a datos de Google Workspace para Google Drive.

Alcance

DynamicMail solicita <https://www.googleapis.com/auth/gmail.readonly> solo cuando un usuario autorizado o un administrador del cliente conecta Gmail inbound para la recepción de documentos. El alcance permite que DynamicMail vea mensajes y ajustes de Gmail de la cuenta de Google conectada. DynamicMail usa el alcance para el procesamiento inbound de solo lectura y no lo usa para enviar, modificar, eliminar, archivar, etiquetar ni mover mensajes de Gmail.

Los alcances de identidad de Google Sign-In, como `openid`, `email` y `profile`, son independientes de este consentimiento de acceso a datos de Gmail. Iniciar sesión con Google no implica aceptar el acceso a Gmail inbound.

Datos a los que DynamicMail puede acceder

Cuando Gmail inbound está conectado, DynamicMail puede acceder a los datos de Gmail necesarios para encontrar y procesar documentos empresariales inbound, incluidos:

- identificadores de mensajes, identificadores de conversaciones, identificadores de historial, referencias de etiquetas y cursores de sincronización;
- remitente, destinatario, asunto, fecha, encabezados y otros metadatos del mensaje;
- cuerpos de mensajes y fragmentos necesarios para identificar el contexto del documento;
- archivos adjuntos y archivos insertados que pueden contener facturas, avisos, acuerdos, recibos u otros documentos del cliente;
- ajustes de Gmail solo cuando la API de Gmail los requiera para el alcance `readonly` o para el comportamiento de sincronización de la cuenta;
- datos derivados creados a partir del contenido de Gmail, como texto OCR, campos de documentos procesados, etiquetas de clasificación, resultados de extracción, resúmenes, eventos de auditoría y registros de documentos.

DynamicMail no debe solicitar ni procesar datos de Gmail que no estén relacionados con la función visible de recepción inbound de documentos.

Por qué DynamicMail usa datos de Gmail

DynamicMail usa datos de Gmail readonly para proporcionar la fuente Gmail inbound seleccionada por el cliente. Los fines previstos son:

- detectar mensajes inbound que puedan contener documentos empresariales del cliente;
- importar archivos adjuntos o contenido de mensajes que el cliente elija procesar;
- extraer, clasificar y enrutar documentos dentro de los flujos de trabajo de DynamicMail;
- conciliar el estado de sincronización para que el mismo mensaje no se importe repetidamente;
- mostrar el estado de conexión, sincronización y procesamiento a usuarios autorizados del cliente;
- realizar actividades de soporte, seguridad, auditoría y cumplimiento legal permitidas por las políticas aplicables y el acuerdo con el cliente.

DynamicMail no debe vender datos de Gmail, usarlos para publicidad o retargeting, transferirlos a intermediarios de datos, usarlos para vigilancia ni usarlos para determinar solvencia crediticia o elegibilidad para préstamos.

Retención

DynamicMail conserva datos derivados de Gmail solo durante el tiempo necesario para la función visible de recepción inbound de documentos, la configuración de retención de documentos del cliente, registros de auditoría, seguridad, gestión de disputas o cumplimiento legal. Los tokens OAuth y los metadatos de sincronización se conservan solo mientras sean necesarios para operar la fuente Gmail inbound conectada o para preservar registros de auditoría requeridos.

El contenido sin procesar de mensajes de Gmail, los archivos adjuntos y los datos de documentos derivados deben eliminarse o anonimizarse cuando ya no sean necesarios para el fin comunicado, salvo que una obligación legal, de seguridad, de auditoría o de retención del cliente requiera continuar conservándolos.

Eliminación

Un usuario autorizado o un administrador del cliente puede solicitar la eliminación de datos en caché derivados de Google, archivos adjuntos importados, texto extraído y registros de documentos derivados. DynamicMail debe eliminar o anonimizar los datos solicitados cuando lo permitan la configuración de retención del cliente y la ley aplicable.

Eliminar registros importados de DynamicMail no elimina necesariamente el correo electrónico o archivo adjunto original de Gmail, porque el alcance Gmail readonly no concede a DynamicMail permiso para modificar ni eliminar mensajes de Gmail.

Revocación y desconexión

El cliente puede desconectar Gmail inbound en DynamicMail. Después de la desconexión o de la revocación local del consentimiento, DynamicMail debe dejar de usar tokens OAuth almacenados para Gmail inbound y debe dejar de leer mensajes adicionales de Gmail desde la cuenta conectada.

El propietario de la cuenta de Google también puede revocar la autorización de la aplicación desde la configuración de la cuenta de Google. Si se revoca la autorización de Google, DynamicMail debe detener el acceso a la API de Gmail cuando fallen la renovación del token o las llamadas a la API, y la conexión debe mostrarse como desconectada o pendiente de reconexión.

La revocación local no elimina automáticamente los documentos ya importados en DynamicMail. Esos registros se gestionan mediante las reglas de eliminación y retención anteriores.

Uso de IA, OCR y extracción

DynamicMail puede usar OCR, procesamiento, clasificación, resúmenes y otros tratamientos asistidos por IA sobre contenido de mensajes y archivos adjuntos derivados de Gmail solo para proporcionar o mejorar el flujo visible de documentos inbound solicitado por el cliente. Los datos de Gmail y los datos derivados no deben usarse para crear, entrenar ni mejorar un modelo general de aprendizaje automático o IA fuera de la función solicitada por el cliente.

Los resultados asistidos por IA pueden ser incorrectos. DynamicMail debe presentar los datos extraídos como resultado del flujo de trabajo que usuarios autorizados pueden revisar, corregir, aprobar, rechazar o eliminar según el flujo del producto.

Acceso de soporte y acceso humano

El personal, contratistas o subprocesadores de DynamicMail no deben leer mensajes específicos de Gmail, archivos adjuntos, texto extraído ni datos derivados de Gmail salvo que se cumpla una de estas condiciones:

- el usuario ha solicitado explícitamente soporte que requiere acceso a datos específicos;
- el acceso es necesario para una investigación de seguridad, prevención de abuso o respuesta a incidentes;
- el acceso es necesario para cumplir con la ley, un proceso legal o una instrucción vinculante del cliente;

- los datos están agregados o anonimizados para operaciones internas y no es legible el contenido de Gmail de un usuario específico.

El acceso de soporte debe ser de privilegio mínimo, limitado en el tiempo cuando sea práctico y registrado para fines de auditoría.

Es material de implementación y localización, no asesoramiento legal final. No debe presentarse como si contara con respaldo de Google, revisión legal externa final o autorización de producción para alcances restringidos sin evidencia separada de revisión.

Referencias fuente

- Contrato de alcance restringido de DynamicMail:
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>