

MacSonik Google Workspace Backup Tool

Google API Scopes & Data Access Guide

A transparency document explaining exactly what Google data our tool can access, why it needs that access, and what is planned next, written for IT administrators, security reviewers, and compliance teams evaluating the tool.

Product reference: [MacSonik Google Workspace Backup Tool](#).

This tool backs up and migrates **Gmail, Contacts, Calendars, Tasks, Notes**, and **Google Drive** (including Docs, Sheets, and Slides) to formats such as PST, PDF, MBOX, CSV, VCF, and ICS, and can migrate directly to Microsoft 365 (OneDrive), SharePoint Online, or another Google Workspace domain.

1. Why Does This Document Exist?

When you connect your Google Workspace account to the **MacSonik Google Workspace Backup Tool**, Google's consent screen asks you to approve a list of "**scopes**"; permissions that define exactly what the application is allowed to see and do. Most users skim past this screen, and most vendors don't explain it. This document exists to remove that gap: for every scope our application requests, we explain in plain language what it unlocks, which feature of the tool depends on it, and what the tool explicitly cannot do with it.

We follow the principle of least privilege throughout: we request **read-only access** wherever the feature only needs to read data, and we request **write access** only where a feature genuinely needs to create or move data.

(for example, writing migrated emails into a destination mailbox). Section 7 lists broader, all-access alternatives we deliberately avoided, and why.

2. What the Tool Backs Up & Migrates Today?

Based on the currently shipped feature set of the MacSonik Google Workspace Backup Tool:

- **Gmail (Mailbox Migration mode):** Emails, attachments, and labels exported to **PST, PDF, MBOX, or CSV**, with options to skip folders, filter by date and sender/subject/CC/BCC, skip duplicates, and split large PST files.
- **Google Contacts:** Exported to VCF.
- **Google Calendar:** Events exported to ICS.
- **Google Tasks:** Task lists included in backup exports.
- **Google Keep (Notes):** Notes included in backup exports alongside **Contacts, Calendars, and Tasks.**
- **Google Drive (Google Drive Migration mode):** My Drive, Shared Drives, Shared with Me, and Trash, with Google Docs, Sheets, and Slides auto-converted to DOCX, XLSX, and PPTX respectively, and original folder hierarchy preserved.
- **Direct migration destinations:** Microsoft 365 (OneDrive), SharePoint Online, and another Google Workspace domain, each reachable via **Single User** or **Workspace Admin (DWD)** authentication depending on the destination.
- **Multi-user/batch migration:** CSV import for mapping and migrating hundreds of mailboxes/accounts in a single admin-run operation, supporting **one-to-one, one-to-many, many-to-one, and many-to-many** mapping types (mergers, offboarding, department consolidation, user reassignment).

2.1 Three Authentication Modes

The tool supports three distinct ways to connect a Google account, and it matters which one applies because only two of them use the **Google OAuth scopes** documented in Section 3:

- **OAuth 2.0/Modern Auth:** An individual user signs in through Google's standard OAuth 2.0 consent screen and approves the scopes in Section 3 for their own account only. Used for single-account backups or one-off migrations.
- **IMAP + App Password:** A Gmail address plus a Google App Password (requires 2-step verification enabled) is used to connect directly over IMAP for mailbox migration only. This path does not use Google OAuth or any of the scopes in this document at all. It authenticates at the protocol level, not through Google's API consent screen.
- **Workspace Admin (DWD):** A Workspace super admin authorizes a service account once, at the domain level, using a JSON or P12 service account key.

This lets the tool act on behalf of any user in the domain without each employee individually signing in required for CSV batch migration and cross-Workspace-domain migration. The Admin Directory scope (Section 3.7) is what makes this mode possible.

A fourth option, Saved Accounts/Quick Access, simply lets a user reconnect to an already-authorized account without re-entering credentials each session. It does not introduce any new scope.

3. Currently Active Scopes

The scopes below live in the product today. Each table includes what the scope technically grants, the feature it powers, and the specific data fields the tool reads or writes under that permission.

3.1 Gmail API

Scope: <https://mail.google.com/>

Access: Full (Read/Write/Delete)

Why is it Used?

This is Gmail's broadest OAuth scope, equivalent to full IMAP-level access to the mailbox. The tool requests it rather than a narrower read-only scope for two concrete reasons:

1. **Read side:** Full-fidelity raw MIME export (needed to preserve headers, attachments, and formatting exactly when converting to PST/EML/MSG) requires this level of access.
2. **Write side:** Google Workspace-to-Google Workspace migration and Gmail-to-Gmail migration insert messages directly into the destination mailbox, which is a write operation this scope enables.

In **Single User Mode**, this only ever applies to the signed-in user's own mailbox. In Admin Mode, it applies per-mailbox, only for the users an admin explicitly selects or imports via CSV.

Why not gmail.readonly?

Because the destination side of a GSuite → GSuite migration needs to write into a mailbox, a single combined scope keeps the OAuth consent process to one screen instead of two separate app registrations for "**source**" and "**destination**" roles. A read-only variant is listed in Section 7 as an alternative we reviewed.

Note: This scope only applies to the **OAuth 2.0/Modern Auth** and **Workspace Admin (DWD)** connection modes; see Section 2.1. Current mailbox export formats are **PST**, **PDF**, **MBOX**, and **CSV**.

3.2 Google Contacts API (People API)

Scope: <https://www.googleapis.com/auth/contacts.readonly>

Access: Read-only

Why is it Used?

- Reads contact records; names, email addresses, phone numbers, organization/job title fields, and contact groups. So they can be included in a backup or exported to VCF.
- The tool never edits, deletes, or writes back to the source Contacts list; this scope cannot be used to do so even if instructed.

3.3 Google Calendar API

Scope: <https://www.googleapis.com/auth/calendar.readonly>

Access: Read-only

Why is it Used?

- Reads calendar events, attendee lists, locations, descriptions, and recurrence rules across the user's calendars, for export to ICS.
- Read-only access means the source calendar can never be modified, double-booked, or have events deleted by the tool.

3.4 Google Tasks API

<u>Scope</u>	<u>Access</u>	<u>Why is it used?</u>
https://www.googleapis.com/auth/tasks.readonly	Read-only	Reads task lists and individual task items (title, notes, due date, completion status) for inclusion in the account backup export.

3.5 Google Keep API

<u>Scope:</u> https://www.googleapis.com/auth/keep.readonly
<u>Access:</u> Read-only
<u>Why is it Used?</u> Reads Keep notes, lists, and attached images for inclusion in the account backup, alongside Contacts, Calendars, and Tasks. Important note: The Google Keep API is only available for Google Workspace accounts, so this scope is only exercised in the Workspace Admin (DWD) connection mode. It is not available for personal Gmail accounts connecting via OAuth 2.0/Modern Auth.

3.6 Google Drive API

<u>Scope:</u> https://www.googleapis.com/auth/drive.readonly
<u>Access:</u> Read-only
<u>Why is it Used?</u> Downloads file content from the source Drive including native Google Docs, Sheets, and Slides, which are auto-converted to DOCX, XLSX, and PPTX respectively during export, for backup, or for migration into OneDrive/SharePoint (Microsoft 365) or another Google Drive.
<u>Scope:</u> https://www.googleapis.com/auth/drive.metadata.readonly

Access: Read-only (metadata only)

Why is it Used?

Reads file and folder metadata; names, unique IDs, MIME types, folder hierarchy, sharing/permission settings, and timestamps without downloading the file content itself.

Used first, before any content transfer, to build an accurate migration file tree and validate folder structure. This is significantly faster and lighter than requesting full metadata through the content-scoped calls for every file.

3.7 Workspace Admin Directory API

Scope: <https://www.googleapis.com/auth/directory.readonly>

Access: Read-only

Why is it Used?

- Used only in Admin Mode, by a Workspace super admin, to enumerate the list of user accounts in the domain (names, primary emails, org unit, suspension status).
- This is what powers the CSV batch-migration feature. Instead of an admin typing in every user's email by hand, the tool can list and pre-fill the domain's users for mapping and selection.
- This scope is never used in Single User Mode and never grants the ability to create, suspend, or modify a user account.

3.8 OpenID Connect/Identity Scopes

<u>Scope</u>	<u>Access</u>	<u>Why is it used?</u>
openid	Identity	Enables the standard OAuth 2.0/OpenID Connect sign-in flow, letting the tool securely verify who is signing in without ever seeing the Google account password.
email	Identity	Retrieves the authenticated user's email address, shown in the tool's UI so the user can

		confirm the correct account is connected before a backup/migration job starts.
profile	Identity	Retrieves basic profile info (display name, profile photo) purely for display on the account-connection screen.

3.9 Summary: All Currently Active Scopes

<u>Scope</u>	<u>Access</u>	<u>Why is it used?</u>
mail.google.com	Full	Gmail backup & migration (read source, write destination)
contacts.readonly	Read-only	Contacts backup (VCF export)
calendar.readonly	Read-only	Calendar backup (ICS export)
tasks.readonly	Read-only	Tasks backup
keep.readonly	Read-only	Notes backup (Workspace/DWD accounts only)
drive.readonly	Read-only	Drive & Docs/Sheets/Slides backup/migration
drive.metadata.readonly	Read-only	Drive structure mapping (pre-migration)
directory.readonly	Read-only	Admin Mode: tenant user enumeration for CSV batch migration
openid	Identity	Secure sign-in
email	Identity	Account confirmation in UI
profile	Identity	Display name/photo in UI

4. Planned Scopes: In Development & Near-Term Roadmap

The following scopes support features that are either in active development or confirmed for the near-term roadmap. They are listed here ahead of release so clients evaluating the tool today have visibility into what's coming.

4.1 Google Chat API: In Development

STATUS: IN DEVELOPMENT

Scope: <https://www.googleapis.com/auth/chat.messages>

Access: Full (Read/Write/Manage)

Why is it Used?

Reads Chat messages from the source account for backup, and recreates them in the destination space during Chat migration, preserving sender, timestamp, and thread context where Google's API allows it.

Scope: <https://www.googleapis.com/auth/chat.spaces>

Access: Full (Create/Read/Manage)

Why is it Used?

Reads the list of source Chat spaces to determine what needs to be migrated, and creates matching spaces on the destination side so conversations land in an equivalent structure rather than a flat dump.

4.2 Google Sites API: Planned

STATUS: PLANNED

<u>Scope</u>	<u>Access</u>	<u>Why is it used?</u>
https://www.googleapis.com/auth/sites.readonly	Read-only	Reads Google Sites page content and structure for backup, or for migrating a site to SharePoint (Microsoft 365) or another Google Site.

4.3 Google Groups: Planned (via Admin Directory API)

STATUS: PLANNED

<u>Scope</u>	<u>Access</u>	<u>Why is it used?</u>
https://www.googleapis.com/auth/groups	Read-only	Enumerates Google Groups (mailing

com/auth/admin.directory.group.readonly		lists/distribution groups) in the domain so they appear as selectable items for migration.
https://www.googleapis.com/auth/admin.directory.group.member.readonly	Read-only	Reads each group's membership list, so the group can be recreated with the correct members on the destination as an Microsoft 365 Group/Distribution List, or as a Google Group in another Workspace domain for GSuite-to-GSuite migration.

5. Future Roadmap: Additional Google Services Under Evaluation

Beyond the confirmed roadmap in Section 4, the following Google services are candidates for future support based on demand for more complete Workspace coverage (photo archives, forms/survey data, and notes). Each is listed with the scope it would require and an honest note on any current limitation in Google's own API for that service, so expectations are set correctly ahead of release.

5.1 Google Photos

STATUS: UNDER EVALUATION

Scope:

https://www.googleapis.com/auth/photoslibrary.readonly.appcreateddata

Access: Read-only (app-created content only)

Why is it Used?

Would allow backup of photo/video albums and items that the migration tool itself created or uploaded.

Important limitation: Google restricted the Photos Library API in March 2025 apps can no longer read a user's entire photo library, only content the app itself created.

- Full-library photo backup is therefore not possible through this API alone;

it would need to be paired with Google Takeout-based export or Google's Data Portability API for a complete photo backup, which we are evaluating.

5.2 Google Forms

STATUS: PARTIALLY LIVE/UNDER EVALUATION

Today, Google Forms already appears as a selectable file type in the Google Drive Migration file-type filter (alongside Docs, Sheets, Slides, and custom extensions). This uses the existing Drive scope (Section 3.6) and lets an admin include or exclude Forms files from a Drive migration job like any other Drive item. What the Drive scope cannot do is read a form's actual questions or collected responses that requires the dedicated Forms API below, which is under evaluation for a future release focused on full form content backup.

<u>Scope</u>	<u>Access</u>	<u>Why is it used?</u>
https://www.googleapis.com/auth/forms.body.readonly	Read-only	Would read a form's structure questions, sections, and settings for backup or migration to an equivalent format.
https://www.googleapis.com/auth/forms.responses.readonly	Read-only	Would read submitted form responses, so response data is preserved alongside the form structure rather than backing up an empty template.

5.3 Google Docs, Sheets & Slides: No New Scope Needed

These are already covered today under the existing Drive scope (Section 3.6). Google Docs, Sheets, and Slides files live inside Drive and are returned by the Drive API, which the tool already uses to auto-convert them to DOCX, XLSX, and PPTX on export. No additional permission is required to extend or improve this feature.

5.4 Jamboard Files: No New Scope Needed

Jamboard boards (.jam files) are also stored in Google Drive and are already reachable through the existing Drive scope. Note that Google retired the standalone Jamboard app in October 2024; existing .jam files remain in Drive and

exportable, but no new Jamboard-specific boards can be created going forward. This is a Google-side change, not a limitation of our tool.

6. Destination-Side Permissions: Microsoft Graph API

This document is primarily about Google API scopes, since that's the source side of a Google Workspace backup or migration job. But when the destination is Microsoft 365 or SharePoint Online, the tool also requests permissions on that side through the **Microsoft Graph API**. We include them here because a client's IT admin evaluating "what can this tool access" needs the full picture, not just the Google half.

Per MacSonik's own product documentation, a Microsoft 365 administrator must grant the following Graph API permissions, with tenant-wide admin consent, before a Google→Microsoft 365 migration can run:

<u>Graph API Permission</u>	<u>Access</u>	<u>Why is it used?</u>
Mail.ReadWrite	Full (Read/Write)	Allows the tool to create and write migrated messages into the destination mailbox in Microsoft 365.
Contacts.ReadWrite	Full (Read/Write)	Allows the tool to write migrated Google Contacts into the destination Microsoft 365 mailbox's Contacts folder.
Calendars.ReadWrite	Full (Read/Write)	Allows the tool to write migrated Google Calendar events into the destination Microsoft 365 Calendar.
User.ReadWrite.All	Full (Read/Write, tenant-wide)	Allows the tool to look up and act on behalf of the correct destination user accounts across the Microsoft 365 tenant – necessary for CSV batch migration, where source Google accounts are mapped to

		destination Microsoft 365 accounts in bulk.
--	--	---

Why admin consent, specifically?

Without tenant-wide admin consent, the application cannot read or write to mailbox, OneDrive, SharePoint, contacts, or calendar data for any user other than the one who is signed in. Granting admin consent authorizes these permissions across the entire Microsoft 365 tenant in one step, which is what makes unattended, bulk, cross-account migration possible the same trade-off as the Google-side Workspace Admin (DWD) mode in Section 2.1.

7. Reference: Broader Scopes Reviewed but Implemented

During scope planning, we evaluated broader, full-access alternatives for several APIs and deliberately chose the narrower read-only scopes documented in Section 3 instead. This table is kept as an audit trail. It's the most common question we get from security reviewers and Google's own OAuth verification team ("why not just request full access and simplify things?"), so we answer it here directly.

<u>Scope</u>	<u>Access</u>	<u>Why is it used?</u>
gmail.readonly	Read-only Gmail	Not requested as a separate scope superseded by mail.google.com, which the tool already needs for write access on the destination side of a migration.
contacts (full)	Read/write Contacts	Not requested the tool only ever reads Contacts for backup and never writes back to or deletes from the source.
calendar (full)	Read/write Calendar	Not requested read-only is sufficient for backup; the tool never creates, edits, or deletes source calendar events.

tasks (full)	Read/write Tasks	Not requested read-only is sufficient for backup.
drive (full)	Read/write Drive	Not requested, the tool only reads the source Drive; all writing happens on the destination platform (OneDrive/SharePoint, or a destination Google Drive), never on the source.

Keeping requested scopes at the minimum needed for each feature (least-privilege access) reduces the size of the consent screen shown to your users, simplifies Google's app verification review, and limits the potential impact of any future credential compromise.

8. Questions or Concerns

If your IT or security team has questions about any scope in this document including requests for a narrower Single-User-only build, a data flow diagram, or a signed data processing addendum please reach out to our support team and we'll be glad to walk through it.