CONNECT YOUR SOLUTION

Google Workspace

Connect your Google Workspace organisation to REVIEWIT: a Google Cloud service account, delegated domain-wide, acting on behalf of an administrator, read-only.

VERSION
1.0 · November 2026

DURATION
Forty minutes, in four steps

DISTRIBUTION
Confidential · REVIEWIT customers

WHAT YOU NEED

01 **A Google Workspace super administrator** (`admin.google.com` console) and an **owner of a Google Cloud project** — often the same person.

02 **A REVIEWIT account** with the subscription administrator role, to open the Subscription Manager.

03 **The time stated**, in the order of this guide: first the credential at Google Workspace, then the REVIEWIT wizard, in four steps.

THE WIZARD, IN FOUR STEPS

STEP 1	STEP 2	STEP 3	STEP 4
Solution	**Prepare**	**Credential**	**Verification**
Pick Google Workspace from your subscription's catalog.	Tick what REVIEWIT must collect; the wizard derives the rights to grant.	Enter what Google Workspace handed you; REVIEWIT verifies it before saving.	One verdict per resource: what is covered, what remains to be granted.

IN THIS GUIDE

1 How REVIEWIT connects to Google Workspace
2 What REVIEWIT will read, and the rights it takes
3 Create the credential at Google Workspace
4 What you will enter in the wizard
5 The connection wizard, in four steps
6 What REVIEWIT receives, and what it never receives
7 After the connection
8 Troubleshooting and checklist

01 How REVIEWIT connects to Google Workspace

REVIEWIT reviews **access**: who can reach what, and whether it is still justified. To do so it reads, **read-only**, the inventory of your resources and their rights at Google Workspace, from your hosting region. It never writes on your side, never reads any content, and keeps the credential you hand it in a vault that only the collector opens.

ON YOUR SIDE
Google Workspace
You create a technical credential, limited to the read rights the wizard lists.

→

YOUR REGION
REVIEWIT collector
Verifies the credential with a real call, then reads the inventory at the frequency of your collection plans.

→

YOUR CONSOLES
Workspace Manager
Campaigns, reviews and reports: never a direct call to Google Workspace.

GUIDING PRINCIPLE

REVIEWIT believes only what it has observed by calling: a right granted but not verified stays "unverified" until the next health pass. What a connection cannot collect is stated **resource by resource**; a resource that cannot be collected can still be imported as a report.

SUPPORT

All Google Workspace editions. Administration and report scopes require a **super administrator** to impersonate; Google Chat, Keep and Marketplace reports also require those services to be enabled in your organisation.

02 What REVIEWIT will read, and the rights it takes

The wizard computes the exact list of rights from the resources you tick at the **Prepare** step, and hands it to you ready to copy ("Copy the plan"). The table below gives the rights of the most commonly retained resources; your plan may hold fewer.

RIGHT OR GESTURE	RESOURCES IT OPENS
`admin.directory.user.readonly` · `admin.directory.orgunit.readonly`	Users, organisational units, guests; the base of Drive, Gmail, Calendar, Sites, Keep
`admin.directory.group.readonly` · `apps.groups.settings`	Google Groups, members and group settings
`drive.readonly`	Google Drive, shared drives and their members, shared links, Sites, Apps Script deployments
`calendar.readonly` · `calendar.acls.readonly` · `admin.directory.resource.calendar.readonly`	Calendars, calendar shares, resources (rooms)
`gmail.settings.basic`	Delegates, forwarding rules, send-as addresses of mailboxes
`chat.admin.spaces.readonly` · `chat.admin.memberships.readonly`	Google Chat spaces and their members
`admin.directory.rolemanagement.readonly`	Privileged roles and role assignments
`admin.directory.user.security` · `admin.reports.audit.readonly`	OAuth grants, Marketplace apps
`cloud-identity.userinvitations.readonly` · `admin.directory.device.*.readonly`	Pending invitations, Chrome and mobile devices
`script.projects.readonly` · `script.deployments.readonly` · `keep.readonly`	Apps Script projects and deployments, Google Keep

03 Create the credential at Google Workspace

An administrator creates, in the Google Cloud console, **a service account dedicated to REVIEWIT**, then authorises it in the Google Workspace admin console to act on behalf of an administrator, for the read scopes of the plan only. No user signs in; no password is shared.

01 **In `console.cloud.google.com`, create (or pick) a dedicated project, for instance "REVIEWIT Collector"**

A separate project isolates the key and its logs; it needs no billing.

02 **Enable the plan's APIs under APIs & Services › Library**

Admin SDK API, Google Drive API, Google Calendar API, Gmail API, Groups Settings API, Google Chat API, Google Keep API, Apps Script API, Cloud Identity API. A disabled API returns 403 at collection time, never at verification.

03 **Create the service account: IAM & Admin › Service accounts › Create**

Free name; no IAM role is needed on the project. Note its **unique client ID** (OAuth 2 Client ID, a string of digits) on its page.

04 **Create a key: Keys › Add key › Create new key › JSON**

The JSON file downloads once: it is what the REVIEWIT wizard asks for. Do not keep it elsewhere after entering it.

05 **In `admin.google.com`, open Security › Access and data control › API controls › Manage domain-wide delegation**

Click **Add new**, paste the service account's client ID, then the list of scopes **copied from the REVIEWIT wizard** (Prepare step › "Copy the plan"), and authorise.

06 **Note your organisation's Customer ID: Account › Account settings › Profile**

A string of the form `C0xxxxxxx`. It is the wizard's "Customer ID" field.

07 **Choose the administrator to impersonate**

The address of an active **super administrator**: the Admin SDK only acts on behalf of a domain administrator. Prefer a dedicated admin account, without a personal mailbox.

SCOPES: DO NOT GUESS THEM

Domain-wide delegation refuses any scope absent from its list, and the list must match exactly what REVIEWIT will request. Copy the plan from the wizard; if you add resources later, the wizard returns the missing scopes, to be completed in the same delegation.

04 What you will enter in the wizard

The **Credential** step only shows the fields Google Workspace declares to REVIEWIT. The connection name is the one you will read in tables and alerts.

WIZARD FIELD	VALUE
Connection name	Free — for instance "Google Workspace · <your domain>".
Customer ID	The organisation's Customer ID (`C0xxxxxxx`), noted at step 6. It is the connection's external identifier.
Service account key (JSON)	The content of the JSON file downloaded at step 4, pasted as is. REVIEWIT checks it is readable before saving it.
Admin to impersonate	The super administrator address chosen at step 7.

A JSON KEY IS A SECRET

It carries the service account's private key. Entered once, it is stored in the vault and referred to by reference; no screen shows it again. An invalid JSON blocks the save: it would overwrite the stored key with unreadable text.

05 The connection wizard, in four steps

In the Subscription Manager, open **Data sources** › **Connections**, then **Connect a solution** (or **Connect an instance** on the solution's tile if it is already present). Nothing is saved before Google Workspace answers.

STEP 1 Solution

The catalog lists only what is not connected yet. A "probe available" solution is verified by a real call; a "declarable" one is recorded on your word, at the level you choose.

STEP 2 Prepare

Tick the resources to collect: the list of rights to grant follows. Copy the plan, grant it at Google Workspace, then come back. The wizard never applies that plan itself.

STEP 3 Credential

Name the connection and fill in the fields. **Verify the connection** calls Google Workspace; **Save without verifying** keeps the connection inactive, to verify later.

Google types its identity (the Customer ID): "Save without verifying" opens as soon as the name and Customer ID are filled; the key can be added later.

STEP 4 Verification

Google Workspace answered: the wizard shows the identity it read and, resource by resource, a verdict. **Save and activate** puts the connection in service; **Save inactive** keeps it for later.

Verification requests a token from Google on behalf of the administrator, then reads the organisation: an `unauthorized_client` refusal points to a missing or incomplete delegation (section 8).

06 What REVIEWIT receives, and what it never receives

RECEIVED FROM GOOGLE WORKSPACE	USE AT REVIEWIT
`Customer ID · organisation name`	The connection's identity and display name.
`Admin SDK Directory`	Users, groups, members, organisational units, roles: who exists and who holds what.
`Drive · Sites · Calendar · Chat · Keep`	The objects, their owners, members and permissions — never their content.
`Gmail settings`	Delegates, forwarding rules and send-as addresses of mailboxes — never an e-mail.
`"domain" permissions · organisation-wide links`	The **Overshared** signal: a shared drive or site open to the domain, a My Drive rich in organisation links, counted and dated, never named.

NEVER RECEIVED, NEVER REQUESTED

No user password
The credential is technical, created for REVIEWIT; no person's account is used.

No content
No message, file or e-mail: REVIEWIT reads lists of objects and rights, never what they contain.

No write
The rights requested are read rights; remediation, where it exists, is a separate module, enabled separately.

No secret shown again
The secret is entered once, stored in the vault and referred to by reference; no screen or log shows it again.

07 After the connection

The connection is managed from **Data sources › Connections**. A health pass replays the verification **every 24 hours**; "Verify all connections" runs it on demand. Each tile states how many resources are ready, to configure or unverified.

A right is missing	The resource stays "unverified" and the wizard says which one. Grant it at Google Workspace, then "Check rights".

Renew the secret	Create a **new JSON key** on the service account (IAM › Service accounts › Keys), enter it under "Connections › Add a credential", verify, then delete the old key on the Google side. Domain-wide delegation is bound to the service account's client ID: it does not change.
A resource that cannot be collected	Import its report from **Data sources** › **Collect** › **Choose a report**: the exact CSV contract downloads from the drawer.
Disconnect	Deactivate the connection; then revoke the credential at Google Workspace. Collection plans that relied on it stop.

08 Troubleshooting

WHAT YOU SEE	CAUSE	WHAT TO DO
`unauthorized_client` at verification	Domain-wide delegation does not authorise this service account, or not all the requested scopes.	Under "Manage domain-wide delegation", check the client ID and paste the full scope plan again.
`invalid_grant` / "Invalid email or User ID"	The administrator to impersonate does not exist, is suspended, or is not an administrator.	Enter the address of an active super administrator.
A resource returns 403 "Not Authorized to access this resource/api"	The matching API is not enabled on the project, or the service is disabled in the organisation.	Enable the API in the project's library; check the service (Chat, Keep…) is enabled for users.
"The JSON is not readable"	Truncated file, or a copy of another key type (P12, public key).	Create a new JSON key and paste the whole file, braces included.
The Customer ID is refused	It does not match the organisation the key serves.	Read it in `admin.google.com › Account › Account settings`, on the same organisation as the impersonated administrator.

CHECKLIST BEFORE OPENING THE WIZARD — 6 items

- [ ] I have a Google Workspace super administrator and a dedicated Google Cloud project.
- [ ] The plan's APIs are enabled on the project.
- [ ] The service account exists; its JSON key is downloaded and ready to paste.
- [ ] Domain-wide delegation carries **the service account's client ID** and **the scopes copied from the wizard**.
- [ ] I know the organisation's Customer ID (`C0xxxxxxx`) and the administrator address to impersonate.
- [ ] I open the Subscription Manager with a subscription administrator account.

This guide is provided to REVIEWIT customers to connect their solutions. Menu paths are those of the vendors' consoles at publication date; they may change. In case of discrepancy, the REVIEWIT wizard prevails: it shows the exact plan computed for your subscription.