CONNECT YOUR DIRECTORY

# Google Workspace

Designate Google Workspace as the directory for your REVIEWIT workspace, via OpenID Connect, with a clear rule on strong authentication.

VERSION
**2.0 · October 2026**

DURATION
**Twenty minutes, in three steps**

DISTRIBUTION
**Confidential · REVIEWIT customers**

## WHAT YOU NEED

01 **The setup link** received by e-mail from REVIEWIT. It is valid until the date it states, and anyone who opens it can connect a directory to your workspace: do not forward it.

02 A Google Workspace super administrator (for 2-Step Verification, section 4) and an account that can create an OAuth client in a Google Cloud project of your organization.

03 **Twenty minutes**, in the order of this guide: first the application at your directory, then the REVIEWIT wizard, in three steps.

## THE WIZARD, IN THREE STEPS

STEP 1

### Connect the directory

Your directory describes itself, TrustGate verifies it; nothing is saved before its answer.

STEP 2

### Prove the door opens

A real sign-in, with no session or right: proof that the door opens, and for whom.

STEP 3

### Activate the workspace

You become the first administrator; the setup link dies.

## IN THIS GUIDE


1 How REVIEWIT federates with your directory

2 The two return addresses to register

3 Create the application at Google Workspace

4 Strong authentication (MFA)

5 The setup wizard, in three steps

6 What REVIEWIT receives, and what it never receives

7 After activation

8 Troubleshooting and checklist

## 01 How REVIEWIT federates with your directory

REVIEWIT never stores or verifies your users' passwords. Authentication is delegated to your directory, through **REVIEWIT TrustGate**, REVIEWIT's identity authority in your hosting region. Your directory remains the sole authority on who your users are and how they sign in; every REVIEWIT application stands behind this single, auditable boundary.

ON YOUR SIDE
**Your directory**
Authenticates the user and hands over a standard OpenID Connect token.

→

YOUR REGION
**TrustGate**
Verifies the proof, normalizes the identity, opens the session.

→

BEHIND THE BOUNDARY
**REVIEWIT applications**
Never talk to your directory, never see its tokens.

**GUIDING PRINCIPLE**

TrustGate asks your directory what it can ask, and believes only what it can verify. A requested strong authentication is never taken for granted: only the proof returned in the token counts.

**SUPPORT**

Google Workspace is supported through the wizard's "OpenID Connect" type: Google is a standard OpenID Connect provider, and its issuer is https://accounts.google.com. One documented limit: Google does not attest the second factor in its tokens. Section 4 explains how REVIEWIT accounts for this, and what you attest in its place.

## 02 The two return addresses to register

A directory refuses any sign-in whose return address it does not know. REVIEWIT uses two for your workspace: one for the wizard's proof sign-in, the other for every sign-in that follows. They are stable: you register them once and for all, on the application you create for REVIEWIT.

| PURPOSE | RETURN ADDRESS (REDIRECT URI) |
|---|---|
| **Proof sign-in** | `https://auth.<region>.we-reviewit.com/federation/callback-candidate/<your workspace ID>` |
| **All subsequent sign-ins** | `https://auth.<region>.we-reviewit.com/federation/callback/<your workspace ID>` |

**WHERE TO FIND THEM**

The wizard shows them ready to copy, at its first step, under "Return addresses to register in your directory". Do not retype them: the authority serving your workspace and the workspace ID exist only there. You can open the link, copy both addresses, and come back to the wizard later: it resumes exactly where you left it.

# 03 Create the application at Google Workspace

An administrator creates, in the Google Cloud console, an OAuth client dedicated to REVIEWIT TrustGate, in a project belonging to your Workspace organization. The consent screen is of type Internal: only accounts from your domain can sign in.

01 **Google Cloud console › choose a project of your organization**

Create one if needed (e.g. reviewit-trustgate). It must belong to your Workspace organization, not to a personal account.

02 **APIs & Services › OAuth consent screen (Google Auth Platform › Audience)**

User type Internal. App name: REVIEWIT. Support e-mail: your team's. No sensitive scope to declare: openid, email and profile require no Google verification.

03 **Credentials › Create credentials › OAuth client ID**

Type Web application. Name: REVIEWIT TrustGate.

04 **Authorized redirect URIs: both return addresses**

Add the two addresses from section 2, one after the other, exactly. No "Authorized JavaScript origin" is needed.

05 **Note the Client ID and Client secret**

The Client ID ends with .apps.googleusercontent.com. The secret must only be entered in the wizard (section 5); do not pass it to anyone.

### WHAT YOU WILL ENTER IN THE WIZARD

| WIZARD FIELD | VALUE |
|---|---|
| **Directory** | OpenID Connect |
| **Name shown to your users** | Your organization's name, as your users recognize it — "Contoso", not "Google". |
| **OIDC authority** | `https://accounts.google.com` |
| **Client ID** | The Client ID (…apps.googleusercontent.com). |
| **Client secret** | The OAuth client's secret. |
| **My directory enforces 2-Step Verification…** | Ticked, after step 02 of section 4. |

# 04 Strong authentication (MFA)

REVIEWIT's administration consoles require an elevated session: at the right moment, TrustGate asks your directory for multi-factor authentication, then reads the proof in the returned token. Two claims are authoritative: `amr` (the authentication methods used) and `acr` (the authentication class satisfied). By default, the value `mfa` in amr attests the second factor; any other vocabulary is declared in the wizard, under "MFA settings".

**01** **Google Admin console › Security › Authentication › 2-Step Verification**

Tick Allow users to turn on 2-Step Verification, then Enforcement: On, for the whole organization or at least for your REVIEWIT administrators' organizational unit. Leave a reasonable enrollment period before enforcement.

**02** **Choose the method**

Any, or Only security key if your administrators have FIDO2 keys or passkeys: that is the only path to phishing-resistant authentication at Google.

**03** **In the wizard, tick the declared trust**

"My directory enforces 2-Step Verification on every account; count its sign-ins as multi-factor". You commit your organization through this declaration: REVIEWIT will count every sign-in from Google as multi-factor authentication, and the audit trail will record it as declared, not proven.

**IN THE WIZARD — MFA SETTINGS**

**amr values / acr context**
Leave empty. Google does not emit them; filling them in would change nothing.

**Declared trust**
Ticked. Without it, every Google session counts as a single factor, and the administration consoles stay closed to your administrators.

**WHY A DECLARATION, NOT A PROOF**

Google's ID token carries neither amr nor acr: it does not say how the person authenticated. Since TrustGate can verify nothing, it assumes nothing — you attest that the directory enforces the second factor on all its accounts. This trust only elevates the session to MFA level, never to the phishing-resistant level, and every session so elevated keeps the trace of its origin ("declared_mfa").

# 05 The setup wizard, in three steps

Open the setup link. It tells you who the workspace belongs to, until when it is valid, and that nobody can sign in until the directory is connected. Click **Start**.

## STEP 1 Connect your directory

The wizard first shows the two return addresses (section 2), then asks for your directory. Nothing is saved until the directory has answered.

01 **Choose the directory type**
OpenID Connect for Google Workspace — as for Okta, Ping or Keycloak. The "Microsoft Entra ID" type is reserved for a Microsoft 365 tenant.

02 **Enter the display name, OIDC authority, client ID and client secret**
The secret is never shown again nor written to a log: it is only opened by the component that signs your users in, and every opening leaves a receipt.

03 **Adjust the MFA settings if section 4 asked you to**
Otherwise, leave them empty: the defaults apply.

04 **Click "Verify directory"**
TrustGate reads your directory's discovery document and runs five checks, in order: the address responds; it is a readable OpenID Connect document; it announces an issuer, an authorization endpoint and a token endpoint; it publishes signing keys; your directory accepts the client ID and secret. A failure names the failing check.

05 **Click "Save and continue"**
The directory is declared as candidate: it serves nobody yet.

## STEP 2 Prove the door opens

Click "Sign in with my directory". You are sent to your directory, you authenticate there (with the second factor if your policy requires it), and you return to the wizard. No session is opened and no right is granted: REVIEWIT only records that the door opens, for whom, and with what authentication strength.

If the sign-in fails, nothing is adopted and nothing has changed. "Edit configuration" takes you back to step 1: the setting most often corrected at this point is the one from section 4, when the directory announces the second factor under another name.

## STEP 3 Activate the workspace

The wizard summarizes the organization, the directory and the identity that just signed in, then states what activation changes:

- this identity becomes the workspace's first administrator;
- every subsequent sign-in goes through your directory;
- the setup link stops working.

Click "Activate my workspace". A confirmation is sent to the contact designated at order time, and "Open my workspace" takes you to your console, where you sign in through your directory.

## 06 What REVIEWIT receives, and what it never receives

| RECEIVED IN THE TOKEN | USE AT REVIEWIT |
|---|---|
| `sub` | The person's stable identifier at Google. Together with the issuer, this is what binds the identity to its REVIEWIT account — never the e-mail address. |
| `email` | The Workspace address, lower-cased. Used for display, entitlements and notifications; never as a binding. |
| `amr, acr / acrs` | The proof of strong authentication (section 4). Read, never assumed. |
| `auth_time` | The moment of the actual authentication. Sensitive actions require a recent authentication: without this claim, they are refused. |
| `name` | The display name, for information. It never counts as identity. |

**NEVER RECEIVED, NEVER REQUESTED**

**No password**
Entry happens at your directory, on its page.

**No access to your resources**
TrustGate only requests the openid, profile and email scopes. Nothing allows reading your mail, your files or your directory.

**No list of your users**
A REVIEWIT account is born at a person's first sign-in, and only if it was decided to grant it; that account carries no right by itself.

**No matching by e-mail address**
Identity is bound by the issuer + stable identifier pair. A reused address never gives access to someone else's account.

## 07 After activation

Your directory is administered from the Subscription Manager, under **Settings › Identity provider**. The page lists the declared directories, their state, and carries the declaration form — collapsed, because declaring a directory is a rare act. Every action requires a reason, written as-is into the audit trail.

| | |
|---|---|
| **Switching directory without ever locking anyone out** | The new directory is declared as candidate, proven by a real sign-in, then adopted. Until adoption, the directory in service keeps serving. |

| | |
|---|---|
| **Deactivating a directory** | Refused if no door would remain: nobody can lock themselves out. |
| **Renewing the client secret** | A Google secret does not expire on its own, but you can rotate it. Create the new secret in the Google Cloud console, declare the directory again (same authority, new secret reference), prove it, adopt it; delete the old secret at Google afterwards. REVIEWIT support deposits the new secret's value in the authority's vault under the reference you declared. |
| **Revoking a person** | Deactivate them at your directory, and their next sign-in is refused. To cut a session already open, deactivate their account in REVIEWIT: sessions are revalidated every five minutes. |

# 08 Troubleshooting

| WHAT YOU SEE | CAUSE | WHAT TO DO |
|---|---|---|
| **Error 400: redirect_uri_mismatch** | One of the two return addresses is missing or differs by one character. | Copy both addresses again from the wizard into "Authorized redirect URIs". |
| **Error 403: org_internal** | The person does not belong to your Workspace organization. This is the expected protection. | Sign in with an account from your domain. |
| **Error 401: invalid_client** | Secret mis-copied, or Client ID from another project. | Check the Client ID + secret pair of the Web application client created in section 3. |
| **"This address does not respond as an OpenID Connect provider"** | The authority carries an extra path. | Enter exactly https://accounts.google.com. |
| **Proof succeeds, but the administration console still asks for an elevated session** | The declared trust is not ticked. | Tick it at step 1 of the wizard (after enforcing 2-Step Verification), then redo the proof. |
| **Google asks the user to turn on 2-Step Verification** | The enrollment period is over and the account is not enrolled. | Your policy is applying; the person enrolls, then signs in again. |

## Checklist before opening the link

6 ITEMS

- [ ] The REVIEWIT TrustGate OAuth client (Web application type) exists in a project of your organization.
- [ ] The consent screen is of type Internal.
- [ ] Both return addresses from the wizard are in "Authorized redirect URIs", exactly.
- [ ] The Client ID and Client secret are copied.
- [ ] 2-Step Verification is enforced on your REVIEWIT administrators, at least.
- [ ] You know you will tick the declared trust in the wizard.

This guide is provided to REVIEWIT customers as part of opening their workspace. Menu paths are those of the vendors' consoles at publication date; they may change. In case of discrepancy, REVIEWIT support will assist you.