CONNECT YOUR DIRECTORY

Okta

Designate your Okta organization as the directory for your REVIEWIT workspace: standard OpenID Connect, no agent, no schema change, with proven 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 An Okta Super Administrator or Application Administrator account and, for section 4, the right to edit authentication policies.

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 Okta

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

Okta is supported through the wizard's "OpenID Connect" type. Strong authentication is proven: Okta reports the methods used in amr and, on request, the class satisfied in acr.

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 Okta

An Okta administrator creates an app integration dedicated to REVIEWIT TrustGate: an OpenID Connect Web application, to which the users who access REVIEWIT are assigned.

01 **Admin Console › Applications › Applications › Create App Integration**

Sign-in method: OIDC – OpenID Connect. Application type: Web Application.

02 **General settings**

App integration name: REVIEWIT TrustGate. Grant type: Authorization Code only (no Refresh Token, no Implicit). Client authentication: Client secret.

03 **Sign-in redirect URIs: both return addresses**

Paste the two addresses from section 2, one after the other, exactly. Leave "Sign-out redirect URIs" empty; REVIEWIT handles its own sign-out.

04 **Assignments**

Limit access to selected groups: your REVIEWIT users' groups — or Allow everyone in your organization. An unassigned person is refused by Okta before ever reaching REVIEWIT.

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

The secret must only be entered in the wizard (section 5); do not pass it to anyone.

06 **Choose the authority**

The org authorization server is suitable: https://<your-org>.okta.com. A custom authorization server (https://<your-org>.okta.com/oauth2/default) also works, if its access rules let the REVIEWIT application through. The authority entered must be the exact issuer published by /.well-known/openid-configuration.

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 "Okta".
OIDC authority	`https://<your-org>.okta.com (or your custom authorization server's issuer)`
Client ID	The integration's Client ID.
Client secret	The integration's Client secret.
MFA settings	See 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 Security › Authentication policies

Create a REVIEWIT policy (or reuse your MFA policy): Password + Another factor, or Any 2 factor types. For phishing-resistant authentication, require Possession › Phishing resistant (FIDO2 / WebAuthn, Okta FastPass).

02 Apply it to the application

Applications › REVIEWIT TrustGate › Sign On › Authentication policy: select the policy. Your users must be enrolled in at least one second factor (Okta Verify, FIDO2 key).

03 Let TrustGate request the step-up

Upon entering an administration console, TrustGate sends acr_values=urn:okta:loa:2fa:any: Okta then requires the second factor for that sign-in, and reports acr in the token. Without this setting, only the policy from step 02 applies, at every sign-in.

IN THE WIZARD — MFA SETTINGS

Authentication context (acr)
urn:okta:loa:2fa:any. TrustGate requests it at step-up and only grants the elevated session if it reads it back in acr.

amr values attesting MFA
Leave empty — Okta emits mfa when two factors were presented, and that is the default. Add otp, sms, swk, hwk if you want each method counted even without mfa.

amr values attesting phishing resistance
hwk (FIDO2 / WebAuthn hardware key), if you distinguish that level.

CUSTOM AUTHORIZATION SERVER

On a custom authorization server, the email claim is only present if the email scope is allowed by an access rule, and amr only appears in ID tokens. If the proof sign-in fails with "token without email", check the server's access rules — or use the org authorization server.

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 Okta — as for Google Workspace, 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 Okta. Together with the issuer, this is what binds the identity to its REVIEWIT account — never the e-mail address.
`email, preferred_username`	The sign-in 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.
Rotating the client secret	Okta lets you keep two secrets active. Generate the new one in the integration, declare the directory again (same authority, new secret reference), prove it, adopt it; deactivate the old secret at Okta 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
400 Bad Request: redirect_uri not registered	One of the two return addresses is missing or differs by one character.	Copy both addresses again from the wizard into "Sign-in redirect URIs".
User is not assigned to the client application	The person is not assigned to the integration.	Applications › REVIEWIT TrustGate › Assignments: add the person or their group.
401: invalid_client	Secret mis-copied, or Client ID from another integration.	Check the Client ID + Client secret pair of the integration created in section 3.
"This address does not respond as an OpenID Connect provider"	The authority does not match the published issuer.	Open https://<your-org>.okta.com/.well-known/openid-configuration and enter the exact issuer value.
Proof succeeds, but the administration console still asks for an elevated session	acr or amr missing, or under a different vocabulary.	Enter urn:okta:loa:2fa:any as context (section 4); check the authentication policy; redo the proof.
The proof sign-in returns "token without email"	Custom authorization server without an access rule on the email scope.	Allow the openid profile email scopes in an access rule, or use the org authorization server.

Checklist before opening the link

6 ITEMS

- [ ] The REVIEWIT TrustGate integration (OIDC, Web Application, Authorization Code) exists.
- [ ] Both return addresses from the wizard are in "Sign-in redirect URIs", exactly.
- [ ] The users (or groups) who access REVIEWIT are assigned to the integration.
- [ ] The Client ID and Client secret are copied.
- [ ] A two-factor authentication policy is applied to the integration.
- [ ] The authorization server's exact issuer is at hand.

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.