CONNECT YOUR DIRECTORY

Microsoft Entra ID

Designate your Entra ID tenant as the directory for your REVIEWIT workspace, with enforceable strong authentication scoped to the administration consoles only.

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 account in your tenant that can create an app registration and grant admin consent (Application Administrator or Global Administrator role) and, for section 4, that can create a Conditional Access policy.

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 Microsoft Entra ID

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

Microsoft Entra ID is supported natively, through the wizard's "Microsoft Entra ID" type. Strong authentication is enforceable: TrustGate requests an authentication context, Conditional Access enforces it, and the token carries the proof.

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 Microsoft Entra ID

An administrator of your tenant creates, in the Microsoft Entra admin center, an app registration dedicated to REVIEWIT TrustGate. It serves nothing else, and nothing else shares it.

01 **Identity › Applications › App registrations › New registration**

Name: REVIEWIT TrustGate. Supported account types: accounts in this organizational directory only (single tenant).

02 **Web platform, with both return addresses**

Under "Redirect URI", choose Web and paste the first address from section 2. After creation, open Authentication › Add URI and paste the second. Both must be present, exactly.

03 **Token configuration › Add optional claim**

Token type ID: tick auth_time and email. Accept, if Entra offers it, the matching Microsoft Graph email permission.

04 **API permissions › Grant admin consent**

The delegated Microsoft Graph permissions openid, profile and email are sufficient. Admin consent spares every user a consent prompt at first sign-in.

05 **Certificates & secrets › New client secret**

Copy the value immediately: it is never shown again. Note its expiry date. It must only be entered in the wizard (section 5); do not pass it to anyone. You can replace this secret with a certificate renewed by REVIEWIT after activation (section 7).

06 **Overview: note three identifiers**

Application (client) ID, Directory (tenant) ID and Object ID. The first two are for the wizard; the third will be used when switching to a certificate.

WHAT YOU WILL ENTER IN THE WIZARD

WIZARD FIELD	VALUE
Directory	Microsoft Entra ID
Name shown to your users	Your organization's name, as your users recognize it — "Contoso", not "Entra".
OIDC authority	`https://login.microsoftonline.com/<Directory (tenant) ID>/v2.0`
Client ID	The registration's Application (client) ID.
Client secret	The value of the secret created at step 05.

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 **Protection › Conditional Access › Authentication contexts › New authentication context**

Display name REVIEWIT MFA, ID c1 (or one of your choice — you will enter it in the wizard), Publish to apps ticked.

02 **Conditional Access › New policy**

Users: all, or your REVIEWIT administrators group. Target resources › Authentication context › c1. Grant › Require multifactor authentication — or Require authentication strength (e.g. "Phishing-resistant MFA") if your administrators have FIDO2 keys or Windows Hello for Business. Enable the policy.

03 **Nothing else changes on your side**

The policy only triggers when a sign-in requests context c1, and only REVIEWIT requests it, upon entering an administration console. Your other applications are unaffected.

IN THE WIZARD — MFA SETTINGS

Authentication context (acr)
c1 — the value from step 01. Entra reports the contexts actually satisfied in the acrs claim; TrustGate only grants the elevated session if it reads c1 there.

amr values attesting MFA
Leave empty. The default (mfa, ngcmfa) covers Entra.

amr values attesting phishing resistance
Leave empty, unless you enforce a phishing-resistant authentication strength and want REVIEWIT to distinguish it.

WITHOUT ENTRA ID P1

Authentication contexts require a Microsoft Entra ID P1 (or P2) license. Without it, leave the "Authentication context" field empty: TrustGate then requests the second factor through the amr claim, and the token reports it if your tenant enforces MFA on the user (security defaults, per-user MFA). That request is not enforceable: a tenant with no MFA policy may ignore it, and the elevated session is then refused — never granted on trust.

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**
Microsoft Entra ID for a Microsoft 365 tenant. With any other type, the proof sign-in fails at its last step.

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
`oid`	The person's stable identifier in your tenant. Together with the issuer, this is what binds the identity to its REVIEWIT account — never the e-mail address.
`preferred_username, email`	The sign-in address (UPN first), 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.
Switching from secret to certificate	On the "How REVIEWIT proves its identity to your directory" card, enter the application's Object ID and click "Prepare certificate". Download the public part and upload it under Certificates & secrets › Certificates › Upload certificate. REVIEWIT adopts it on its own within ten minutes, then renews it before expiry with no action on your side: you can then delete the client secret. A secret expires on a fixed date — and on that day nobody signs in.
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
AADSTS50011: the redirect URI does not match	One of the two return addresses is missing or differs by one character.	Copy both addresses again from the wizard, on the registration's Web platform.
AADSTS65001: the user or administrator has not consented	Admin consent has not been granted.	API permissions › Grant admin consent, then redo the proof.
"This address does not respond as an OpenID Connect provider"	The authority is incomplete or carries an extra path.	Enter exactly https://login.microsoftonline.com/<tenant ID>/v2.0.
"Your directory rejects this client ID and secret"	Secret mis-copied or expired, or Object ID entered instead of Application ID.	Create a new secret and enter the Application (client) ID.
Proof succeeds, but the administration console still asks for an elevated session	Context c1 is not published, the policy is not enabled, or the ID entered differs.	Check the context and the policy (section 4); redo the proof after fixing.
AADSTS50105: the user is not assigned	The registration requires assignment ("Assignment required").	Assign your users' group under Enterprise applications › REVIEWIT TrustGate › Users and groups.

Checklist before opening the link

7 ITEMS

- [ ] The REVIEWIT TrustGate registration exists, single tenant, Web platform.
- [ ] Both return addresses from the wizard are registered there, exactly.
- [ ] Optional claims auth_time and email are added to the ID token.
- [ ] Admin consent is granted on openid, profile, email.
- [ ] The client secret is copied, and its expiry date noted.
- [ ] Authentication context c1 is published and its Conditional Access policy is enabled (Entra ID P1).
- [ ] You have the Application (client) ID and Directory (tenant) ID 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.