CONNECT YOUR DIRECTORY

PingOne

Designate your PingOne environment (Ping Identity) as the directory for your REVIEWIT workspace: standard OpenID Connect, PingID or PingOne MFA as the second factor, proven by the authentication policy the token reports.

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 PingOne Environment Admin (or Organization Admin) account on your users' environment and, for section 4, the right to edit authentication policies and MFA 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 PingOne

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

PingOne is supported through the wizard's "OpenID Connect" type. Strong authentication is proven through acr: PingOne reports in the token the name of the authentication policy completed, and TrustGate requests it through acr_values. PingOne's amr claim only announces the password (pwd): it is not enough, and the policy is what counts.

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 PingOne

A PingOne administrator creates, in your users' environment, an application dedicated to REVIEWIT TrustGate: an OIDC Web App, to which your authentication policies are attached.

01 **Applications › Applications › +**

Application Name: REVIEWIT TrustGate. Application Type: OIDC Web App. Save.

02 **Configuration › edit: the protocol**

Response Type: Code. Grant Type: Authorization Code only (no Implicit, no Refresh Token). Token Endpoint Authentication Method: Client Secret Post (Client Secret Basic also works). PKCE Enforcement: Optional.

03 **Redirect URIs: both return addresses**

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

04 **Resources: the scopes**

Resources tab › edit: tick openid, profile and email. Nothing else: TrustGate does not read your resources.

05 **Enable the application**

The toggle at the top of the application panel must be blue. If only a population or a group may access REVIEWIT, set it in your policies (section 4): PingOne then refuses the others before they ever reach REVIEWIT.

06 **Note the Client ID and Client Secret, then the issuer**

Configuration tab: Environment ID, Client ID, Client Secret ("Generate New Secret" if needed). The authority is https://auth.pingone.<region>/<Environment ID>/as — .eu, .com, .ca, .asia or .com.au depending on your environment's region, or your custom domain followed by /as. Check it in /.well-known/openid-configuration: the exact issuer is what must be entered. 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 "PingOne".
OIDC authority	`https://auth.pingone.<region>/<Environment ID>/as (or https://<your domain>/as)`
Client ID	The application's Client ID.
Client secret	The application's Client Secret.
Authentication context (acr)	The name of your second-factor policy — Multi_Factor by default (section 4).

PINGFEDERATE, ON PREMISES

If your users authenticate on PingFederate rather than PingOne, the path is the same: an OAuth client (Applications › OAuth › Clients; Authorization Code, Client Secret, both return addresses, openid profile email scopes, an OpenID Connect policy that issues sub, email and amr). The authority is the server's base address (https://sso.<your-domain>), which publishes /.well-known/openid-configuration and must be reachable from the Internet with a public certificate. The PingID second factor is reported by the PingID adapter in amr, or in acr through a Requested AuthN Context Selector: declare in the wizard the value your policy emits.

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 **Authentication › MFA: an MFA policy**

Check the environment's MFA policy (or create one): the allowed methods (PingID or PingOne MFA app, FIDO2, TOTP, SMS) and your administrators' enrollment. It only applies through an MFA step of an authentication policy.

02 **Authentication › Authentication: a second-factor policy**

Create a Multi_Factor policy (the name already exists in many environments) with two steps: Login (password), then Multi-Factor Authentication — or PingID Authentication for a Workforce environment — bound to the MFA policy from step 01. Under "None or incompatible methods", choose Block: a person with no enrolled second factor is refused, never admitted on their word.

03 **Attach the policies to the application**

Applications › REVIEWIT TrustGate › Policies tab › edit: select your single-factor policy (Single_Factor) and Multi_Factor. The first in the list applies by default; TrustGate requests Multi_Factor through acr_values upon entering an administration console, and PingOne reports it in acr. A policy not attached to the application cannot be requested.

IN THE WIZARD — MFA SETTINGS

Authentication context (acr)
Multi_Factor — or the exact name of your second-factor policy. TrustGate requests it at step-up and only grants the elevated session if it reads that name back in acr. Without this line, every entry into an administration console is refused.

amr values attesting MFA
Leave empty. PingOne only announces pwd in amr; the proof comes from acr.

amr values attesting phishing resistance
Leave empty. PingOne does not distinguish the method in the token.

DAVINCI POLICIES

If your environment uses DaVinci policies instead of PingOne policies, the context to declare is the flow policy ID (32 hexadecimal characters), not its name, and acr reports it as-is. An application can attach only one kind of policy.

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 PingOne — as for Google Workspace, Okta 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 PingOne (their user ID). 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	In Applications › REVIEWIT TrustGate › Configuration, click Generate New Secret; PingOne keeps the previous secret valid for as long as you choose. Declare the directory again (same authority, new secret reference), prove it, adopt it; revoke the previous secret afterwards ("Revoke Previous Client Secret"). 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
Redirect URI mismatch	One of the two return addresses is missing or differs by one character.	Copy both addresses again from the wizard into "Redirect URIs".
invalid_client: "Your directory refuses this client ID and secret"	Secret mis-copied or revoked, or token endpoint authentication method set to None or Private Key JWT.	Check the Client ID + Client Secret pair, and set "Token Endpoint Authentication Method" to Client Secret Post.
"This address does not respond as an OpenID Connect provider"	The authority does not match the published issuer: wrong region, missing /as, or another environment's Environment ID.	Open https://auth.pingone.<region>/<Environment ID>/as/.well-known/openid-configuration and enter the exact issuer value.
PingOne refuses the sign-in before reaching REVIEWIT	The application is not enabled, or the person is refused by the policy (population, group, no enrolled second factor).	Enable the application (section 3, step 05); check the policy and the person's MFA enrollment.
Proof succeeds, but the administration console still asks for an elevated session	The context is not declared, its name differs from the policy's, or the policy is not attached to the application.	Declare the exact name (section 4); attach the policy in the Policies tab; redo the proof.
The proof sign-in returns "token without email"	The email scope is not ticked under Resources, or the person has no e-mail address in PingOne.	Tick openid, profile and email (section 3, step 04); fill in the person's address.

Checklist before opening the link

6 ITEMS

- [ ] The REVIEWIT TrustGate application (OIDC Web App, Authorization Code, Client Secret Post) exists and is enabled.
- [ ] Both return addresses from the wizard are in "Redirect URIs", exactly.
- [ ] The openid, profile, email scopes are ticked under Resources.
- [ ] The Client ID and Client Secret are copied; the Environment ID and region are at hand.
- [ ] A second-factor authentication policy (Multi_Factor) exists, blocks without an enrolled method, and is attached to the application.
- [ ] The exact issuer (…/as) published by /.well-known/openid-configuration 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.