CONNECT YOUR DIRECTORY

AD FS

Designate Active Directory Federation Services (2016 or later) as the directory for your REVIEWIT workspace, in native OpenID Connect, without SAML.

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 administrator of the AD FS server (AD FS Management console) and, for section 4, an MFA provider configured in AD FS (Azure MFA, certificate authentication or a third-party adapter).

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 AD FS

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

AD FS 2016 or later is supported through the wizard's "OpenID Connect" type, thanks to its native OpenID Connect support. AD FS 2012 R2 (SAML / WS-Federation only) is not supported.

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 AD FS

An AD FS administrator creates an application group dedicated to REVIEWIT TrustGate. Two issuance rules add the e-mail address and the authentication methods, which REVIEWIT reads from the token.

01 **AD FS Management › Application Groups › Add Application Group**

Name: REVIEWIT TrustGate. Template: Server application accessing a web API.

02 **Server application: both return addresses**

Note the generated Client Identifier. Under Redirect URI, add the two addresses from section 2, one after the other, exactly.

03 **Generate a shared secret**

Tick the box and copy the secret immediately: it is never shown again. It must only be entered in the wizard (section 5); do not pass it to anyone.

04 **Web API**

Identifier: paste the Client Identifier from step 02. Access control policy: Permit everyone for now (section 4 adds MFA). Permitted scopes: openid, profile, email, allatclaims.

05 **Web API Issuance Transform Rules: two rules**

Send LDAP Attributes as Claims: attribute E-Mail-Addresses → outgoing claim type email (also add User-Principal-Name → upn). Pass Through or Transform an Incoming Claim: incoming claim Authentication Methods References → outgoing type amr. Without the first, the proof sign-in fails with "token without email"; without the second, no elevated session is possible.

06 **Note the authority**

https://<fs.your-domain>/adfs. Check that it publishes https://<fs.your-domain>/adfs/.well-known/openid-configuration and that its TLS certificate is issued by a public authority: the REVIEWIT authority, hosted outside your network, must be able to reach it.

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 "AD FS".
OIDC authority	`https://<fs.your-domain>/adfs`
Client ID	The Server application's Client Identifier.
Client secret	The shared secret generated at step 03.
amr values attesting MFA	`http://schemas.microsoft.com/claims/multipleauthn (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 An MFA provider in AD FS

AD FS Management › Service › Authentication Methods › Multi-factor Authentication Methods: enable Azure MFA, certificate authentication, or your third-party adapter, and check that your administrators are enrolled.

02 The Web API's access control policy

Application Groups › REVIEWIT TrustGate › Web API › Access Control Policy: Permit everyone and require MFA — or Permit specific group and require MFA with your REVIEWIT administrators' group, and a second "Permit everyone" rule for other users.

03 What the token reports

When MFA was required, AD FS adds http://schemas.microsoft.com/claims/multipleauthn to the authentication methods, which the issuance rule from section 3 sends in amr. This is the value TrustGate recognizes, once declared in the wizard.

IN THE WIZARD — MFA SETTINGS

amr values attesting MFA
http://schemas.microsoft.com/claims/multipleauthn. Without this declaration, TrustGate only recognizes the standard mfa value, which AD FS does not emit.

amr values attesting phishing resistance
Leave empty, unless your MFA provider emits a method specific to FIDO2 keys or certificates that you want to distinguish.

Authentication context (acr)
Leave empty. AD FS does not generally honor acr_values; the MFA requirement comes from the access control policy.

ON-DEMAND STEP-UP DOES NOT EXIST ON AD FS

TrustGate requests the second factor upon entering an administration console, but AD FS applies its policy at sign-in, not on demand. If the policy requires MFA from everyone, every REVIEWIT sign-in carries it; if it only requires it from a group, only its members get an elevated session. An administrator outside that group will be refused the console — never granted a session 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**
OpenID Connect for AD FS — as for Google Workspace, 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 AD FS. Together with the issuer, this is what binds the identity to its REVIEWIT account — never the e-mail address.
`email, upn`	The sign-in address, lower-cased, emitted by your rules. 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 shared secret	Generate a new secret on the Server application, declare the directory again (same authority, new secret reference), prove it, adopt it; remove the old secret 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
MSIS9224: invalid redirect_uri	One of the two return addresses is missing or differs by one character.	Copy both addresses again from the wizard into the Server application.
MSIS9605: unauthorized client / secret rejected	Secret mis-copied or expired, or Client Identifier from another group.	Regenerate the shared secret and check the Client Identifier.
"This address does not respond as an OpenID Connect provider"	The authority is not reachable from the Internet, its certificate is not public, or the path differs from /adfs.	Expose https://<fs>/adfs/.well-known/openid-configuration with a public certificate, and enter the authority with no extra path.
The proof sign-in returns "token without email"	The email issuance rule is missing on the Web API, or the allatclaims scope is not granted.	Add the LDAP rule E-Mail-Addresses → email and the allatclaims scope (section 3, steps 04 and 05).
Proof succeeds, but the administration console still asks for an elevated session	The amr rule is missing, the multipleauthn value is not declared in the wizard, or the policy does not require MFA.	Check the rule from section 3, the declaration from section 4 and the access control policy; redo the proof.
MSIS7012: the user is denied by policy	The access control policy excludes the person.	Adjust the Web API's policy (section 4).

Checklist before opening the link

7 ITEMS

- [ ] The REVIEWIT TrustGate application group exists (Server application + Web API).
- [ ] Both return addresses from the wizard are in the Server application, exactly.
- [ ] The shared secret is copied; the Client Identifier is at hand.
- [ ] The Web API allows the openid, profile, email, allatclaims scopes.
- [ ] The email and amr issuance rules are in place on the Web API.
- [ ] The access control policy requires MFA for your REVIEWIT administrators, at least.
- [ ] https://<fs>/adfs/.well-known/openid-configuration responds from the Internet, with a public certificate.

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.