OIDC Federation Setup Guide (SSO)

This document describes the requirements for setting up Single Sign-On (SSO) via OpenID Connect (OIDC) between your Identity Provider (IdP) and the Adhese platform.

---

1. Overview

We use OIDC-based identity federation to allow your users to log in to the Adhese platform using your organisation's Identity Provider (IdP). Our platform acts as the Service Provider (SP)/Relying Party (RP), while your IdP handles user authentication.

---

2. Information We Need From You

To configure the connection on our side, we need the following from your IdP:

Item	Description
Discovery URL	Your OIDC discovery endpoint, typically `https://<your-idp>/.well-known/openid-configuration`. If not available, provide the individual endpoints below.
Authorization endpoint	URL where we redirect users to authenticate
Token endpoint	URL where we exchange the authorisation code for tokens
UserInfo endpoint	URL where we can retrieve additional user claims (if not all included in the ID token)
JWKS URI	URL to your public signing keys for token validation
Client ID	The client identifier registered for Adhese in your IdP
Client Secret	The client secret associated with the Client ID
Supported scopes	Confirmation that the required scopes (see section 4) are available

> If your IdP supports a discovery endpoint, most of the above can be derived automatically. In that case, providing the discovery URL, Client ID, and Client Secret is sufficient.

---

3. Information We Provide To You

You will need the following from us to configure your IdP:

Item	Description
Redirect URI (Callback URL)	We will provide the exact redirect URI that must be registered as an allowed callback in your IdP.
Required scopes	See section 4
Required claims	See section 4

---

4. Required Scopes and Claims

Required Scopes

Scope	Purpose
`openid`	Mandatory for OIDC. Returns the `sub` (subject) claim.
`email`	Required. Must return the `email` and `email_verified` claims.

Required Claims

Claim	Scope	Required	Expected Value	Description
`sub`	`openid`	Yes	Unique user ID	Unique identifier for the user
`email`	`email`	Yes	Valid email address	The user's email address
`email_verified`	`email`	Yes	`true`	Must be `true`. Users with `email_verified: false` or a missing `email_verified` claim will be denied access.

> **Important:** The `email_verified` claim is an optional claim per the OIDC specification, meaning IdPs are not required to include it by default. Please verify that your IdP is configured to include this claim in the ID token when the `email` scope is requested. Additionally, the value must be `true` — users whose email address has not been verified at the IdP level will not be able to log in.

Optional Scopes and Claims

The `profile` scope is not required but recommended. It enables us to display user-friendly names in the Adhese UI.

Claim	Scope	Required	Description
`name`	`profile`	No	Full display name
`given_name`	`profile`	No	First name
`family_name`	`profile`	No	Last name
`preferred_username`	`profile`	No	Username

---

5. Role Mapping (Optional)

User roles can be managed directly within the Adhese platform. However, if you prefer to manage roles centrally from your IdP, we support automatic role assignment based on a custom claim in the ID token.

How It Works

- You choose the claim name (e.g., `adhese_role`) — let us know which name you use so we can configure the mapping on our side.
- The claim value can be a single role (string) or multiple roles (array).
- Roles are mapped automatically on each login, so changes in your IdP are reflected immediately.

Single role example:

```
{
  "adhese_role": "admin"
}
```

Multiple roles example:

```
{
  "adhese_role": ["viewer", "creative_approver"]
}
```

Available Roles — Classic UI

Role	Description
`classic_admin`	Full admin. Has full permissions in the Classic UI.
`classic_read_only`	Read-only access to the Classic UI.

Available Roles — New UI

Role	Description
`admin`	Full administrator
`creative_approver`	Can approve creatives
`creative_master`	Full creative management
`managed_ad_master`	Managed advertising management
`self_service_ad_master`	Self-service advertising management
`viewer`	Read-only access
`access_all_advertisers_debtors_brands`	Access across all advertisers, debtors, and brands

> If you do not configure role mapping, roles will be managed manually within the Adhese platform by an administrator.

---

6. Setup Checklist

Your side (IdP)

- ☐ Register a new OIDC client/application for Adhese

- ☐ Configure the redirect URI provided by us as an allowed callback URL
- ☐ Ensure the `openid` and `email` scopes are enabled
- ☐ Verify that the `email_verified` claim is included in the ID token with a value of `true`
- ☐ (Optional) Enable the `profile` scope
- ☐ (Optional) Configure a custom claim for role mapping
- ☐ Share the Client ID, Client Secret, and discovery URL (or individual endpoints) with us

Our side (Adhese)

- ☐ Provide the redirect URI
- ☐ Configure the IdP connection with the provided endpoints and credentials
- ☐ Configure scope requests (`openid`, `email`, and optionally `profile`)
- ☐ Configure essential claim validation for `email_verified`
- ☐ (Optional) Configure role mapping based on the agreed custom claim
- ☐ Perform a test login together

---

7. Testing

Once both sides are configured, we recommend performing a joint test:

1. Initiate a login on the Adhese platform
2. Verify that the redirect to your IdP works correctly
3. Authenticate with a test user
4. Verify that the callback to Adhese succeeds
5. Confirm that the user's email and profile information are correctly displayed
6. (If applicable) Confirm that role mapping is applied correctly

If the login fails with an error related to the essential claim, the most common causes are:

- The `email` scope is not enabled on the IdP
- The `email_verified` claim is not included in the ID token
- The user's email is not verified at the IdP level (`email_verified: false`)

Revision #4
Created 15 April 2026 07:41:00 by Wout De Rooms
Updated 27 May 2026 11:32:11 by Kevin Voortmans