# Loftware Cloud: Custom Identity Provider Configuration Customer Information

Version: October 10, 2025

Author: Loftware Colud Operations

Loftware Cloud can integrate with 'identity providers' to enable Single Sign On (SSO). Default supported identity providers are:

- Entra ID (formerly known as Azure Active Directory)
- Google

These can be configured by the customer and do not need Loftware involvement.

Other OIDC based systems can be configured but require a Loftware paid engagement (e.g. OKTA, Ping, Entra ID where the customer wants to own application registration).

**Please note the following restrictions and comments:**

- SAML is not supported
- PKCE is not currently supported – Authorization code flow pattern is used
- Assignment by groups is not supported
- 'Refresh Tokens' must be enabled
- All users required to use the new identity provider will need to be re-invited and must complete the signup process in order to gain access via the new provider (note that existing users of any previous identity provider can remain in place but usual practise is for them to be removed once the new users are in place. Native Loftware Cloud users can also be left in place if required).
- Once the new identity provider has been implemented, by default the Loftware Cloud login page will still display the Microsoft and Google logos. These can be disabled by Loftware but doing this has implications for access, for example by Loftware in a support scenario. If you wish to do this please contact Loftware Support for more information.
- The new login button for the custom provider can have custom text and logo but the customer must provide a public URL for the logo and exact the #HEX code for any specific background colour.
- Electronic (digital) signature for Workflows is not supported by default – it can be requested

To enable Loftware to configure an alternative identify provider, please provide the following:

## General Information:

| | |
|---|---|
| Customer name: | |
| Identity provider solution name:<br>(e.g. OKTA) | |
| Customer contact name:<br>(The person who can respond quickly to technical queries relating to identity provider configuration) | |
| Contact number: | |
| Contact email: | |

## System specific information:

Complete a table for each Loftware Cloud environment to be configured, even if connecting to the same identity provider instance. Pay particular attention to which OIDC instance (production, non-production etc.) is being connected.  Copy the table if more are required.

**Environment 1:**

| | |
|---|---|
| Loftware Cloud environment:<br>(e.g. Production, Sandbox etc) | |
| Loftware Cloud environment URL: | |
| OIDC metadata endpoint:<br>e.g. https://acme-prod.okta.com/.well-known/openid-configuration | |
| OIDC Web Application Client ID*: | See note below |
| OIDC Web Application Client Secret*: | See note below |

**Environment 2:**

| | |
|---|---|
| Loftware Cloud environment:<br>(e.g. Production, Sandbox etc) | |
| Loftware Cloud environment URL: | |
| OIDC metadata endpoint:<br>e.g. https://acme-prod.okta.com/.well-known/openid-configuration | |
| OIDC Web Application Client ID*: | See note below |
| OIDC Web Application Client Secret*: | See note below |

**Environment 3:**

| | |
|---|---|
| Loftware Cloud environment:<br>(e.g. Production, Sandbox etc) | |
| Loftware Cloud environment URL: | |
| OIDC metadata endpoint:<br>e.g. https://acme-prod.okta.com/.well-known/openid-configuration | |
| OIDC Web Application Client ID*: | See note below |
| OIDC Web Application Client Secret*: | See note below |

*Loftware recommends that the Client ID and Client Secret are provided by secure communication in accordance with your organization's security policies.  This is the customer's responsibility.

## Additional Information to Assist Configuration:

If the following information can be provided by the customer ahead of set-up it will reduce implementation time:

**Required claim mappings:**

These are properties returned from the requested scopes, see:

https://developer.okta.com/docs/api/openapi/okta-oauth/guides/overview/

https://auth0.com/docs/get-started/apis/scopes/sample-use-cases-scopes-and-claims

- **FullName** – user's full name (first name + last name)
  - Example - “name” or “display_name”
  - Customer: ______________________________________________________
- **Email** – user's email address
  - Example - “email” or “http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress”
  - Customer: ______________________________________________________
- **ProviderSpecificId** – uniquely identifies the user (i.e. can be a unique number or guid).
  - Example - “preferred_username” or other customer/provider specific claim
  - Customer: _______________________________________________________
- **IdName** – human-friendly user identifier (i.e. UPN). The value of this claim must be unique.
  - Example - “preferred_username” or other customer/provider specific claim
  - Customer: ________________________________________________________

## Information Provided to the Customer

The table below will be completed by Loftware Cloud Operations and provided to the customer when the cloud configuration has been completed:

| | | |
|---|---|---|
| Sign-In redirect URIs | URI to access Loftware Cloud via the new identity provide | Eg: https://logincp1.onnicelabel.com/customer<br>Actual customer URI: ________________________________________ |
| Sign-out redirect URIs | URI for signed out users | Eg: https:// logincp1.onnicelabel.com/Account/SignedOut?customerId=[EncodedCustomerId])<br>Actual customer URI:<br>________________________________________________________________________ |
| Grant type provided | | Authorization Code and Refresh Token grants are provided |
| Scopes | | openid profile offline_access email |