ORACLE

Single Sign-On (SSO) for Oracle Aconex

SSO for Oracle Aconex using Oracle Identity and
Access Management (IAM) and the Construction
and Engineering Lobby

Oracle Aconex supports SAML-based identity federation using Oracle Identity and Access Management (IAM)

This capability allows customers to integrate Oracle Aconex into their existing SAML-based Single Sign-On (SSO) infrastructure

Architecture

Federated sign-on is implemented through the Oracle Construction and Engineering Lobby, which is an application written on top of Oracle Identity and Access Management (IAM).
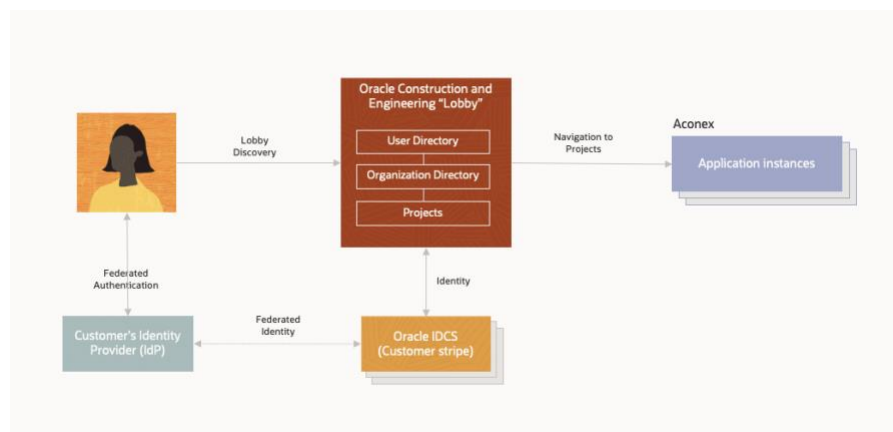
A user navigates to the Lobby to sign in and this request is forwarded to IAM to authenticate the user. If SSO federation is configured, the authentication request is forwarded to the Customer's Identity Provider. Once authentication is successful, the user is redirected back to the Lobby with the relevant claims in place to meet the SAML 2.0 protocol.

Supported protocols

Any protocols supported by IAM will be usable with the Lobby for authentication with Aconex.

Oracle IAM SAML integration currently supports the following features:

- SP initiated Web SSO
- IdP initiated Web SSO
- SP initiated Single Logout
- IDP initiated Single Logout

You can find more information about SAML support in the Oracle Identity Cloud Service Documentation.

Getting started with SSO

For details of the process to start using SSO as an Aconex customer through the Lobby follow these steps on Support Central.

You can read more about SSO support in Aconex in the SSO Essentials section of Support Central.
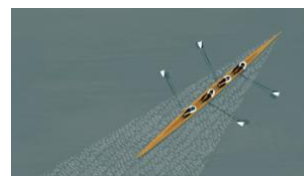
Single Sign-On benefits

- Provides more control over system access with the customer's login standards always enforced.

- Easier user management and administration, including the ability to disable a user in the IdP and remove access to all applications, instances and projects.

ORACLE

Single Sign-On FAQs

What is Oracle Identity Cloud Service (IDCS)?
IDCS was the service used by Oracle Cloud before IAM. IDCS customers are being transitioned to IAM in 2023 and new customers will start receiving IAM Identity Domains as part of this transition.

Can I manage users in my own IAM Identity Domain and have these changes populate to Oracle Aconex using SCIM or similar?
No. Oracle Aconex SSO is a service for authentication only. User administration takes place within the Oracle Aconex application.

Can SSO be used with Azure Active Directory?
Yes, SSO through IAM supports SAML 2 integration with Azure AD.

Do all users in my organization have to use SSO?
No. An administrator can configure authentication requirements for users individually within IAM. SSO authentication can also be enforced as part of a role within Oracle Aconex and can be controlled individually for each user.

Can I use multiple identity providers in my organization?
No. One Lobby organization's users can only be mapped to a single Identity Provider (IdP).

Can I authenticate for API calls with SSO?
Not at present. See "Authentication for Aconex APIs" above.

Can I use SSO for all my company's organizations in Aconex?
Multiple organizations across multiple Aconex instances can use your company SSO service as long as they meet these requirements:
- The organization is a subsidiary or parent company of the organization with an Aconex subscription.
- An admin user on each of the organizations is available to make configuration changes in Aconex.

Can I require subcontractors and other organizations to sign in using my company's SSO?
No. This violates the Aconex terms of service that allows any project participants at least 14 days notice when their access to project information is removed.

Related products

Single Sign-On through the Lobby is also possible with the following related products:

- Oracle Primavera Cloud
- Oracle Preconstruction
- Oracle Primavera Unifier
- Oracle Textura Payment Management
- Other Oracle Cloud services

Glossary

TERM	DEFINITION
SAML 2	The protocol by which SSO authentication is negotiated between different identity providers
Identity Provider (IdP)	A service that stores and manages digital identities for users of systems. Examples are Oracle Identity Cloud Service and Microsoft's Azure Active Directory and Active Directory Federation Services.
Single Sign-On	An authentication scheme that allows a user to securely sign in to several related systems with a single username and password.

Single Sign-On (SSO) for Oracle Aconex / Version 2.1

ORACLE

Fulfilment request checklist for paying Aconex customers

Complete all sections. If you need assistance contact your Customer Success Manager or Aconex Support.

INFORMATION REQUIRED	
Customer Name: (As shown on the order.)	
Customer Admin Email Address: (This person will usually be responsible for activating the cloud account and is usually the main contact for the account. They can then create another admin user who will be the technical contact to configure the SSO details.)	
Oracle Contact Email Address: (Usually the CSM)	
Is there an existing IAM or IDCS account you will use? Many customers will already have an IAM or IDCS account because they are using P6, Primavera Cloud or any other Oracle product.	Yes No If "Yes" IAM or IDCS Account URL (Paste your console URL in here.) `eg. https://idcs-<ID>.identity.oraclecloud.com/ui/v1/myconsole`
OCI region: (This is the region in which user details will be stored.)	
SaaS Product Name: (As shown on the Aconex order.)	
Subscription ID: (As shown on the Aconex order.)	
Order Number: (As shown on the Aconex order. Enter Aconex order number if your order was before October 2020.)	
Then, for **each organization in Aconex,** include the following - **exactly** as they appear in Aconex: • **Organization Name:** • **Trading Name:** • **Organization Postcode:** • **Organization Country:** • **Org ID:** • **Aconex Instance:** (e.g. "US1", "MEA" or "AU1")	

ORACLE

Fulfilment request checklist for non-paying Aconex 0rganizations

Complete all sections. If you need assistance contact Aconex Support.

INFORMATION REQUIRED	
Organization Name: (As shown in Aconex.)	
Organization Admin Email Address: (This person will usually be responsible for activating the cloud account and is usually the main contact for the account. They can then create another admin user who will be the technical contact to configure the SSO details.)	
IAM or IDCS Account URL (Paste your console URL in here)	`eg. https://idcs-<ID>.identity.oraclecloud.com/ui/v1/myconsole`
Then, for **each organization in Aconex**, include the following - exactly as they appear in Aconex (include a separate file if needed): • **Organization Name:** • **Trading Name:** • **Organization Postcode:** • **Organization Country:** • **Org ID:** • **Aconex Instance:** (e.g. "US1", "MEA" or "AU1")	

Connect with us

Call **+1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle