

**ARInsights ARchitect**  
**Single Sign-On (SSO)**  
**Information and Guide**

## ARInsights Single Sign-On (SSO) Implementation

ARInsights ARchitect has implemented SSO authentication for our customers to be able to use the authentication service provided by the customer's Identity provider (IdP).

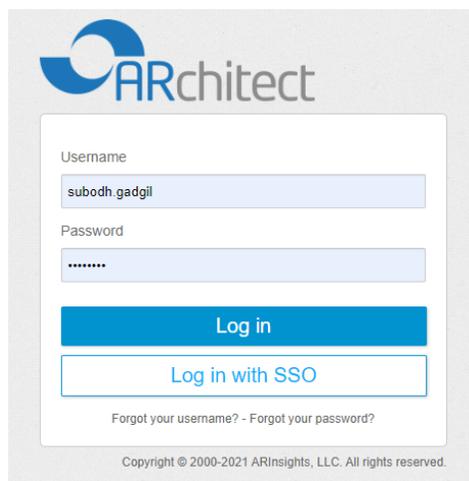
This document will provide information on the process of configuring ARchitect to use the SSO mechanism to sign in.

The following sections provide implementation details and identify the information required from the customer for ARchitect to communicate with the customer's IdP for authentication.

### ARchitect SSO Login Process

When the SSO has been enabled for a customer, all active users of the customer site must use the SSO process.

When a user tries to log into Architect, they will be presented with the following screen:



All users of the customer must select the 'Login with SSO' button. The user will be presented with the SSO login screen:



The user should provide his/her email and press 'Login.'

The system will direct the user to the login process of the customer's IdP. After authentication by the IdP, the user's email must be returned by the IdP to ARchitect. ARchitect will perform its own authentication and log the user in.

## ARInsights SSO Setup Requirements

Currently we support the SAML2 protocol. Current SSO implementation is a Service Provider initiated SAML transaction. IdP initiated transactions are not yet supported.

ARchitect requires the following information from the customer to enable the SSO authentication with customer's IdP:

EntityID	The EntityID is the IdP name / identifier
URLs	The Base URL and end-point URLs for the customer's SAML environment
Certificate	The certificate file, provided as a .pfx or .cer file format, for the active certificate used for the connection.
Metadata	We would prefer the metadata location (URL) for the IdP. We would also request the IdP's metadata in a document. This file contains additional details that may be required.
Expected Attributes	Provide the email of the current user. The provided email address will be used to sign in to ARchitect.

Once ARInsights receives the above information, an environment will be established, and a metadata export will be provided of the ARInsights' configuration information. The following information applies:

For staging environments:

EntityID = <https://architectstage.arinsights.com/Saml2>

Location (ACS) = <https://architectstage.arinsights.com/Saml2/Acs>

For production environments:

EntityID = <https://architect.arinsights.com/Saml2>

Location (ACS) = <https://architect.arinsights.com/Saml2/Acs>

## Customer's Technical Information

This checklist should be reviewed and completed by the organization responsible for the technical implementation of SSO within your company. The questions reflect the technical details needed to qualify and configure the SSO environment.

SSO Parameter	Client Reply
Confirm SAML 2.0 is supported?	<input checked="" type="checkbox"/> Yes (Mandatory) <input type="checkbox"/> No
Please indicate the name of the Identify Provider you use (e.g., ADFS, Ping, Siteminder, OKTA, OneLogin, etc.)	Identity Provider Name/Description:
Test environment (Please also provide the Metadata file)	Entity ID= Redirect URL= Metadata URL=
Production environment (Please also provide the Metadata file)	Entity ID= Redirect URL= Metadata URL=

Certificate file name and type	File Name= File Type= <input type="checkbox"/> .cer <input type="checkbox"/> .pfx
Identity attribute to be provided	Attribute name = email (case sensitive) <RequestedAttribute isRequired="true" Name="urn:email" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:Unspecified" FriendlyName="email" >/>

## Sample Settings for an OKTA IdP

Below are the requirements and details for managing SSO for OKTA.

1. ARchitect should be defined as one of the applications under OKTA.
2. During the definition of the application, please add 'email' as an attribute.
3. Please refer to the 'Expected Attributes' row in the 'Required Parameters Table' for more information.

Below is an example of an ARchitect application:

The screenshot displays the Okta Admin Console interface. On the left is a navigation menu with options: Dashboard, Directory, Applications, Self Service, Security, Workflow, Reports, and Settings. The 'Applications' section is expanded, and the 'Applications' sub-item is selected. The main content area is titled 'Applications' and includes buttons for 'Create App Integration', 'Browse App Catalog', 'Assign Users to App', and 'More'. Below these buttons is a search bar and a table of applications. The table has columns for 'STATUS' and a count. The 'Architect' application is listed as 'ACTIVE' with a count of 1. Other applications shown are 'Okta Admin Console' (INACTIVE, 0) and 'Okta Browser Plugin' (INACTIVE, 0).

STATUS	Count	Application Name
ACTIVE	1	Architect
INACTIVE	0	Okta Admin Console
INACTIVE	0	Okta Browser Plugin



Please provide the information from this page as specified in the 'Required parameters table' below.

**Required parameters table**

EntityID	Provide the 'Identity Provider Issuer' value here (Item # 2)
URLs	Provide the 'Identity Provider Single Sign-On URL' value here (Item #1)
Certificate	Please click the 'Download Certificate' button (below Item #3) to download the certificate. Provide the downloaded file.
Metadata	Copy the contents from the 'Optional Item #1- IDP Metadata' into a file and provide the file. Also, ask for the metadata URL (typically Item # 1 appended with '/Metadata')
Expected Attributes	While defining the application please specify the attribute (or subsequently edit to set the attribute value as below): Name: email Name format: unspecified Value: user.email

Once filled, please send over this table to ARInsights to enable the SSO connectivity to your OKTA server.