Aras Innovator External Authentication using SAML 2.0 Authentication

Aras Innovator allows administrators to control the maintenance of user logins. One method is the SAML 2.0 Authentication Plugin, which provides a way to log into Aras Innovator using the SAML 2.0 authentication protocol.

To view the documentation of the SAML 2.0 protocol, visit https://www.oasis-open.org/standards/#samlv2.0 .

SAML 2.0 is a protocol for exchanging authentication and authorization data between security domains. The XML-based protocol uses security tokens containing assertions to pass information about a principal (usually an end user) between a SAML authority, known as an Identity Provider, and a SAML consumer, known as a Service Provider. SAML 2.0 enables web-based, cross-domain single sign-on (SSO), which helps to reduce the administrative overhead of distributing multiple authentication tokens to a user.

The Aras Innovator logon may be customized using the SAML 2.0 Authentication Plugin described in this section. This plugin provides a way to use external identity providers by the SAML 2.0 protocol for Aras Innovator. The customization requires changes in the OAuth server configuration to enable the SAML 2.0 authentication plugin.

The SAML 2.0 protocol includes the following:

- An identity provider authenticates users and gives the service provider an authentication assertion if successful.
- A service provider relies on the identity provider to authenticate users. The OAuth server acts as a service provider in the system.

The following steps outline the high-level process of SAML2 authentication configuration:

1. Configure external identity provider (e.g., add application registry).
2. Add Transformations for the Aras.OAuth.Server.Plugins.Saml2Authentication plugin and the GenericUserMapper plugin.
3. Run CI **Pipeline** and **Deploy Pipeline**.
4. Create a user that corresponds to the mapping.
5. Configure access to the external identity provider (e.g., DNS settings).