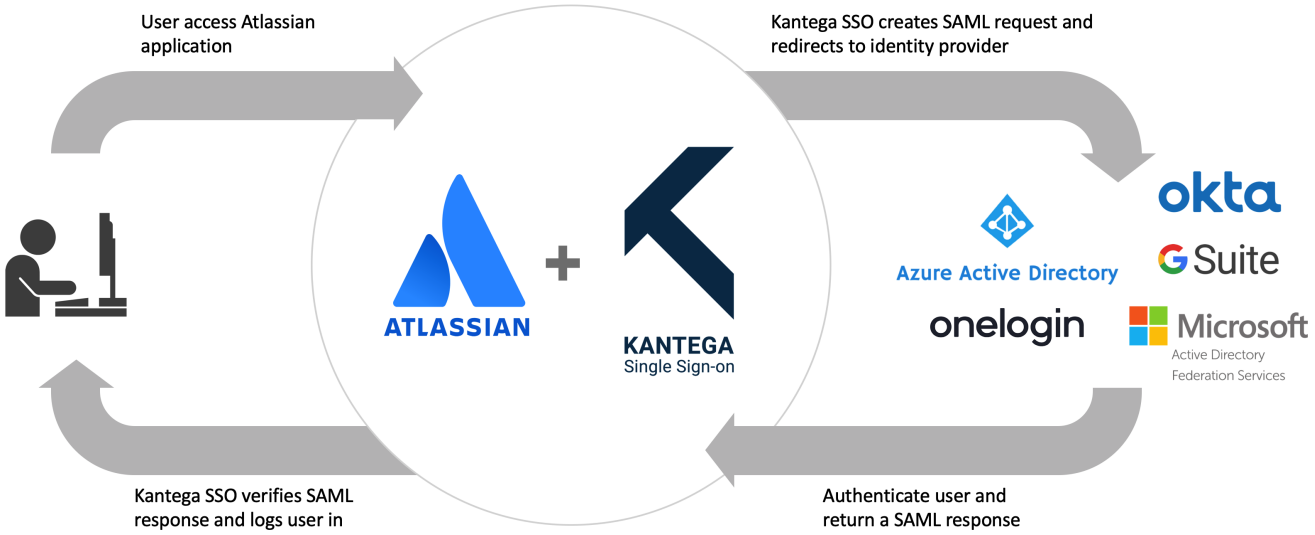
SSO with SAML

The SAML standard facilitates secure exchange authentication and authorization information, so users are allowed to login to the Atlassian products **through third party identity providers**.



SAML is flexible and widespread solution for single sign-on. It offers the ability to identify users in your Atlassian server products via practically any SAML 2.0 identity provider on the web. And there are probably thousands of these services. We have prepared wizard support and guides for the top 10-15 most common, but you should be able to use any SAML 2.0 compliant IdP.

SAML integration guides:

Cloud

- Azure AD
- Google GSuite
- Okta
- OneLogin
- PingOne
- Auth0
- AuthAnvil
- Bitium
- Duo
- Salesforce
- WSO2

On premise

- AD FS
- Keycloak
- Ping Federate

General

- Any other SAML 2.0 provider

SAML was designed for the WWW. In SAML, when users access the Atlassian server or data center product without a valid session, they are redirected to an Identity Provider (IdP) login portal. This is typically a centralized web service for establishing users' identities and can range from the company's internal ADFS or KeyCloak server, to cloud providers like Google GSuite, Okta and Ping. Due to this redirection, and because most IdP authentication is username and password based, SAML is more "noticeable" for the user than IWA / Kerberos. However, SAML does not require a centralized KDC and so avoids the local network/intranet restriction.

By also activating the **cloud user provisioning** feature in your SAML setup, we offer you to have a clean architecture by keeping the user and access management in your the cloud. Whenever a user is created, removed or changes roles, this is synchronized through the connector to your favorite Atlassian products. The cloud connector creates a virtual user directory that your Atlassian products see containing all your users and groups. Currently, Kantega SSO has cloud user provisioning support for Azure AD, Google G-Suite and Okta.

It is perfectly fine to combine SAML with other SSO mechanisms such as **Kerberos (Integrated Windows Authentication)**. In a combination with Kerberos, Kerberos provides password-free login experiences when the user is present at his desktop machine on the office, while SAML enable the user to log in when they on the run outside the office or when accessing from cellphones or other non-Kerberos compatible devices.

SAML FAQ

Kantega Single Sign-on FAQ

Requesting support