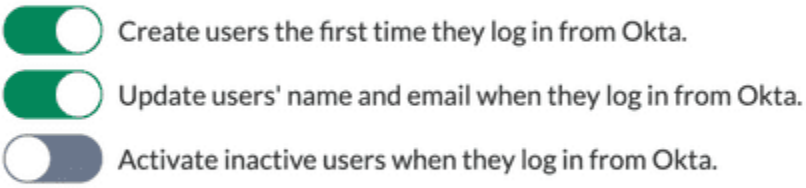
Just-in-time (JIT) provisioning

JIT provisioning allow user accounts to be created, updated and activated in the Internal User directory when they log in using SAML.



The SAML identity provider (e.g. Azure AD, Okta, OneLogin and so on) include additional user attributes (or claims) for users when they log in, like full name and e-mail. If Kantega SSO sees that the incoming user has never logged in before (in other words can't find an existing user account), a new user is created on the fly using attributes of the SAML response.

In the same way, the IDP can include *group claims* allowing Kantega SSO to manage the user's group memberships in the Atlassian application based on the groups received from the identity provider, so that the administrator only has to manage this on the IDP side. It is also possible to configure default groups so that all SAML users will receive a specific role. Default groups are frequently used when access to the Atlassian application is managed on the IDP side itself, so that any incoming and valid SAML response represents a user who should have access.

From experience, the hardest part of JIT provisioning is in configuring group claims on the IDP side. We have created guides for some specific IDPs, see the additional pages below this space. If your IDP is not covered by our documentation, feel free to drop us a line at atlassian.support@kantega.no.