User provisioning

Introduction

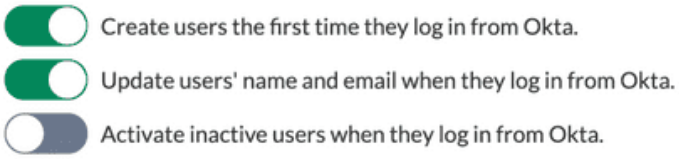
Kantega SSO allows users to sign in using the Kerberos or SAML protocols. However, user accounts and groups must still exist in Jira, Confluence or Bitbucket, Bamboo or Fisheye/Crucible.

On-premise user provisioning is well supported by the base Atlassian application via LDAP and Crowd user directories. Kerberos environments are inherently on-premise, with LDAP/AD readily available, so user provisioning is mainly a concern for SAML environments. As organizations move their user management to cloud solution like Azure AD, Okta or GSuite, LDAP and Crowd are no longer viable solutions.

Kantega SSO offers two ways to provision cloud users: Just-in-time provisioning and Cloud Connectors.

Just-in-time provisioning

Just-in-time provisioning, or JIT, allows user accounts to be created, updated and activated in the Internal user directory on-the-fly, when they log in with SAML. User data is provided by the identity provider through attributes included in the SAML response. The attributes to use can be further customized through attribute mappings at both the IDP side, and in Kantega SSO.



JIT provisioning can be combined with SAML group claims to keep the user's group memberships up to date.

Connectors

Connectors are currently available for Azure, GSuite and Okta. Configuring a connector gives you a synchronized user directory with your cloud users and memberships, functionally similar to the LDAP and Crowd directories you are already familiar with. A background process regularly retrieves updates from the cloud provider, keeping users and group memberships up to date. The synchronization interval can be configured, the default is every hour.

You can also configure filters to limit the set users being exported to Atlassian. The screenshot below shows an example of how Group filters can be defined to only include members of particular groups.

Read more about Connectors for cloud user provisioning.

Pros and cons

Which provisioning option to use isn't always obvious, and they both have their pros and cons. Below, we've tried to summarize the main points.

Just-in-time provisioning

+ Scales to an "unlimited" number of user accounts (whatever the user database can handle - we've never seen anyone hit a practical limit)
+ User accounts only created when they're needed.
+ Groups can be kept in sync every time the user logs in
+ No network dependencies: All info passed through the SAML token.
+ Can be used with any SAML provider.

- Users can only be created in the Internal Directory. If you would prefer to have cloud users in a separate user directory, JIT can't provide that.
- Cannot remove or deactivate users automatically, as user accounts only get updated if the user logs in. Granted, users deactivated in the cloud can't actually log in as they can no longer use SAML, but they'll stick around in the user directory unless they're manually removed.
- Configuring group claims in order to manage memberships can be cumbersome for certain cloud providers, Azure AD in particular. Configuring a connector is far easier.

Connectors

+ Easily synchronize users and group memberships from supported cloud providers (Azure AD, Okta, GSuite)
+ Periodic sync takes care of all user updates, including user account removal and deactivation: No need for manual account cleanup.
+ Cloud users are created in a separate user directory (similar to having an LDAP directory), making it easy to disable or remove the entire connector directory if needed.

- Azure AD, Okta and Google GSuite only.
- Only limited username attribute customization/transformation possible. If you need to map onto an existing/mature Atlassian instance and need things to line up with existing usernames so that users keep their history, some manual database migration may be required.
- Does not scale to larger user databases, works best with small to medium sized tenants. There's no hard limit as every environment is different, but when sync passes start exceeding ~5 minutes, you may begin to see stability issues. The only way to know for sure is to set it up and test.