Group memberships

There are two different ways of handling groups during SAML login, -**Managed groups** and **Default groups**.

Managed Groups

Setting up **Managed groups**, see screenshot below) will only add a group to a user during login if this user has the same group in his SAML response.

Background

Atlassian applications perform authorization by looking at the user's group memberships. Group Memberships are usually delegated to external User Directories such as Microsoft Active Directory.

However, this might not work for all use cases:

- User accounts might live in a directory which is not supported by Atlassian's Embedded Crowd
- The application might be hosted in an environment which lacks network access to the directory

In these cases, its useful to allow Kantega SSO to manage group memberships based on Group Claims included in the SAML response sent by the Identity Provider. We call this feature "Managed groups".

When a group is configured as managed in Kantega SSO, the following will happen when a user is logged in:

- Does the SAML response include a group claim for the managed group? If so, make sure the user is added as a member.
- No group claim found for the managed group? Make sure the user is removed from the group.

Only groups which are explicitly configured as managed by Kantega SSO will be affected by this feature. All other groups will be ignored, so you will still be able to manage some groups locally if you wish.

Configuring the identity provider

The first step is configuring the IDP to include group claims in SAML Responses when users log in. This is typically done in the IDP's administration console and depends on the IDP. We have included guides for some frequently requested IDPs below. If you can't find your IDP in the list, let us know and we'll investigate. You may also consult your IDP's documentation directly.

AD FS

See: Managed groups: AD FS

Azure AD

See: Managed groups: Azure AD

Okta

See: Managed groups: Okta

Keycloak

See: Managed groups: Keycloak

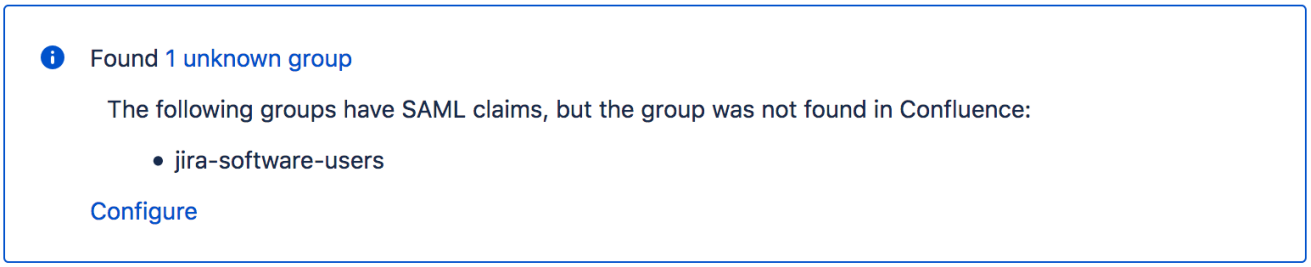
Other identity providers

Please contact our support team, we'll be happy to help you set up your identity provider with group claims.

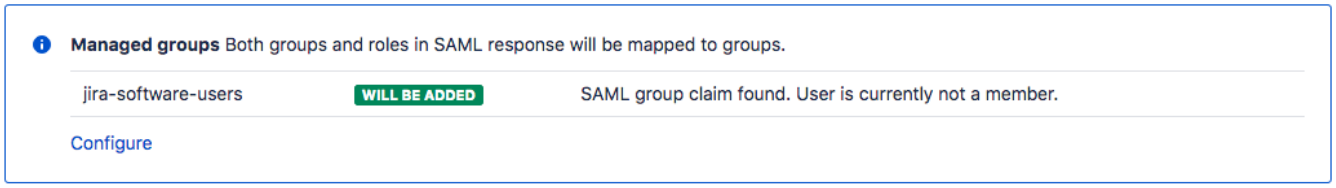
Test that the IDP is sending group claims

Once the identity provider is configured, run a **SAML authentication test** to verify that the identity provider actually sends the expected group claims. If group claims are detected, the test page will notify you of this and provide options for further configuration.

The example test result below shows that the user is a member of the jira-software-users group:



In the test results page, the following change to the managed group during login may appear:



Also "No change" and "Will be removed" are valid messages for changes for Managed groups.

Default groups

Setting up groups in **Default groups** will give the selected groups to all users logging in via SAML. So in the example below, all users will be given the group ***Users*** during login. The group *Users* is only an example.

Group memberships given during login via AD FS

SAML managed groups

Groups assigned to individual users according to Group Claims in the SAML response during login. Both groups and roles in SAML response will be mapped to groups.

For each managed group, Kantega SSO will perform the following before logging in a user:

- If the group claim is found: Add the user to the group
- When the group claim is no longer found: Remove the user from the group

Note: Your IDP must be configured to send group claims (attribute: `http://schemas.xmlsoap.org/claims/Group`) for managed groups. If the IDP does not send such claims, users will effectively be removed from any managed group.

See more details on how to set up managed groups.

Add SAML-managed group

jira-administrators

jira-software-users

Default groups

Groups assigned to all users when they login through AD FS.

Add default group

Users

Group handling is updated

Now is a good time to run a SAML authentication test, allowing you to verify which group claims are sent and preview any memership updates.

Assignment of managed and default groups requires that the underlying user directory is writable and handles group memberships locally.