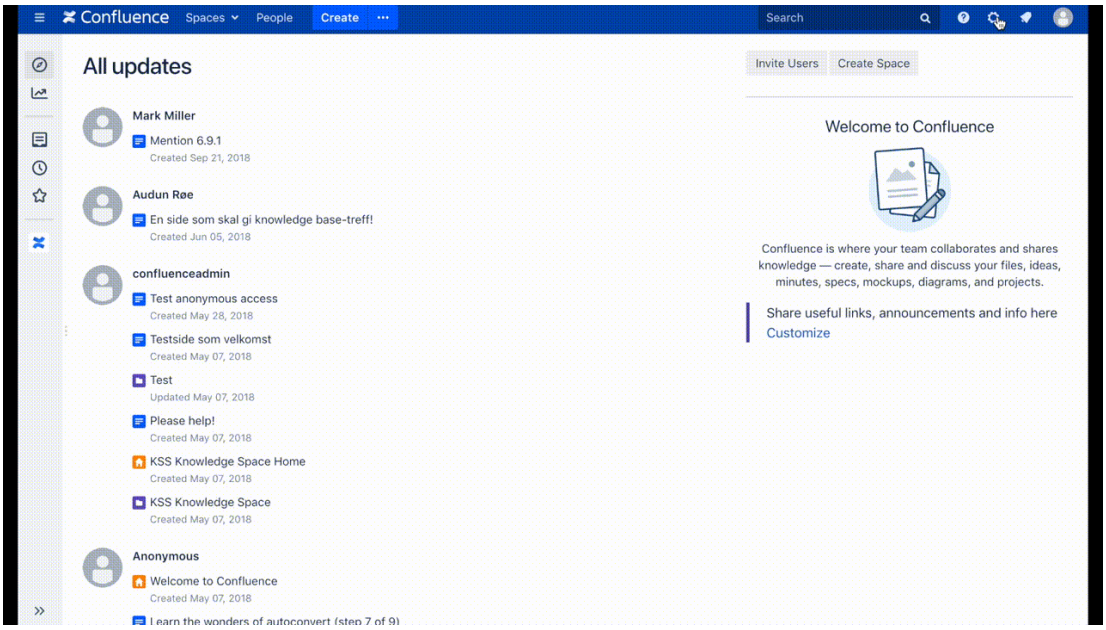
Keycloak

Setup guide for Keycloak login with Atlassian server and datacenter products.

This setup guides assumes that Kantega SSO is installed as an add-on to your Atlassian product (Jira, Confluence, Bitbucket, Bamboo, or FeCru).

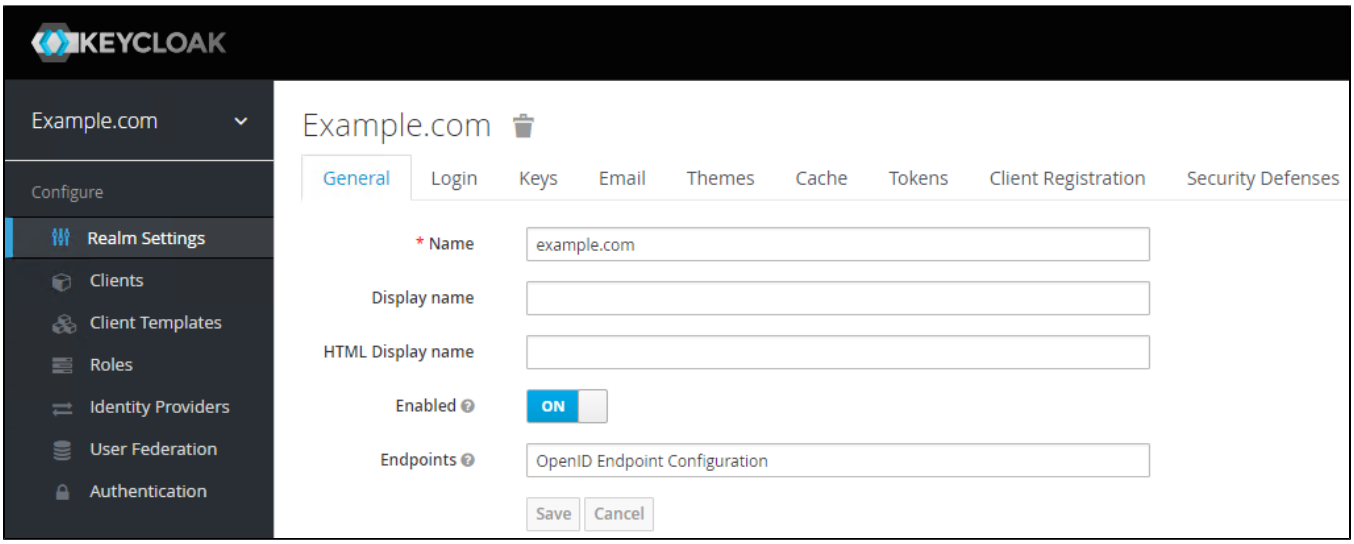
Context: This setup starts in the Configuration page of the Kantega SSO add-on. This configuration page can be found by pressing "**Configure**" on "Kantega Single Sign-On (SSO)" in list of installed add-ons.



Log into Keycloak admin

Log into Keycloak and select your realm. We are using the realm **example.com**

Prior to this guide, User Federation with LDAP has been set up in Keycloak, against the Active Directory domain example.com. This allows provision of the same users and groups into Jira/Confluence/etc using an LDAP user directory. If you cannot use LDAP, you will need to use SAML JIT provisioning instead. This makes Kantega SSO create new users in Internal Directory the first time they log in. We'll get into the details later.



User Federation

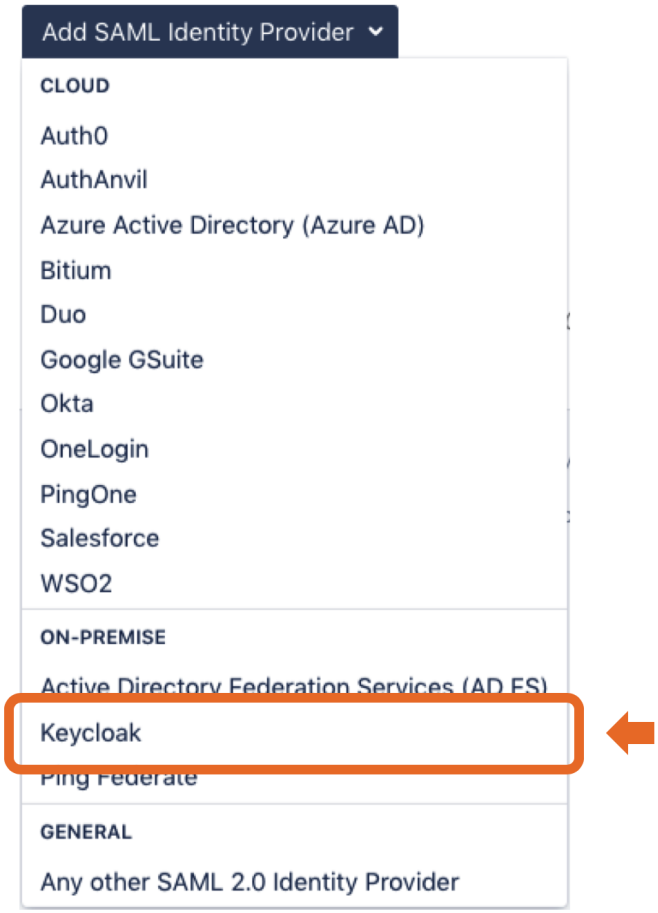
We will configure userPrincipalName as the Keycloak username attribute. These settings are found under User Federation for the example.com realm in Keycloak.

Settings:
Username LDAP attribute: userPrincipalName
RDN LDAP attribute: userPrincipalName

Mappers:
LDAP Mappers,username, LDAP Attribute: userPrincipalName

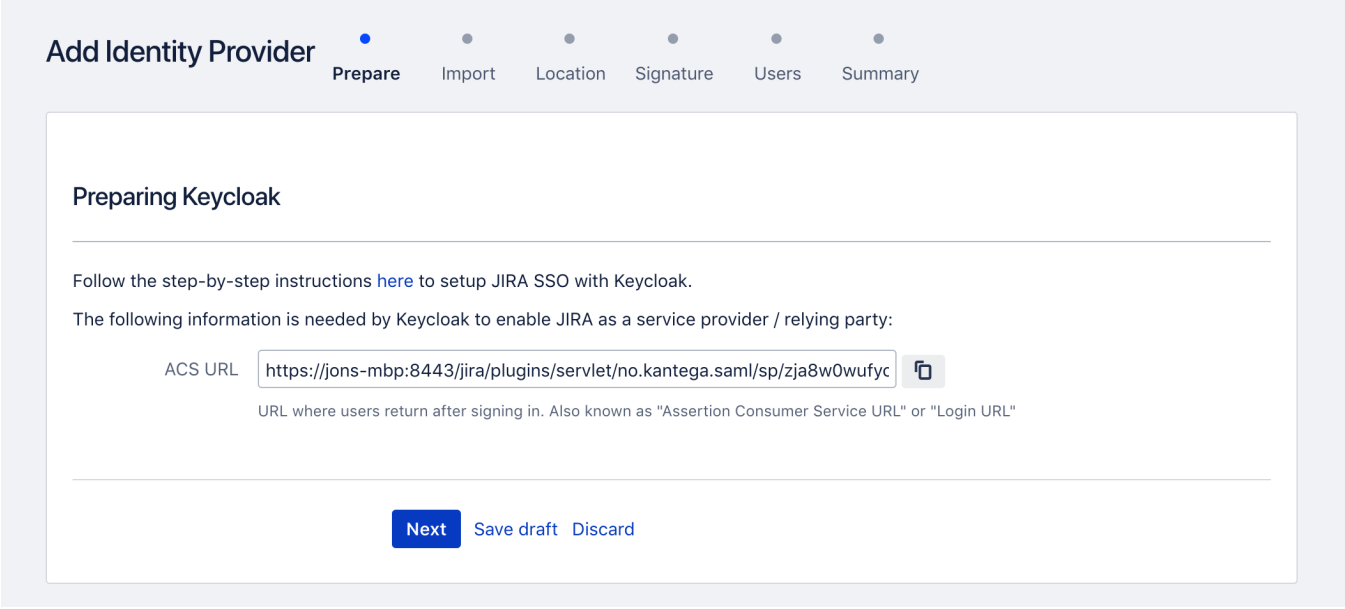
Adding an Identity Provider

In Kantega Single Sign-on add an identity Provider of the type "Any SAML 2.0 Identity Provider".



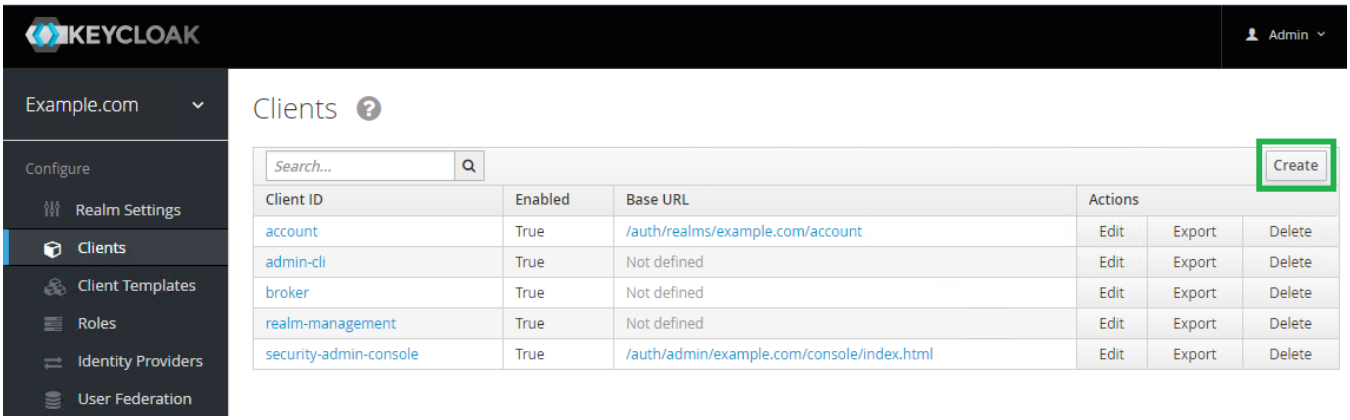
Prepare

- Copy the ACS URL value and save it for later.
- Press Next.

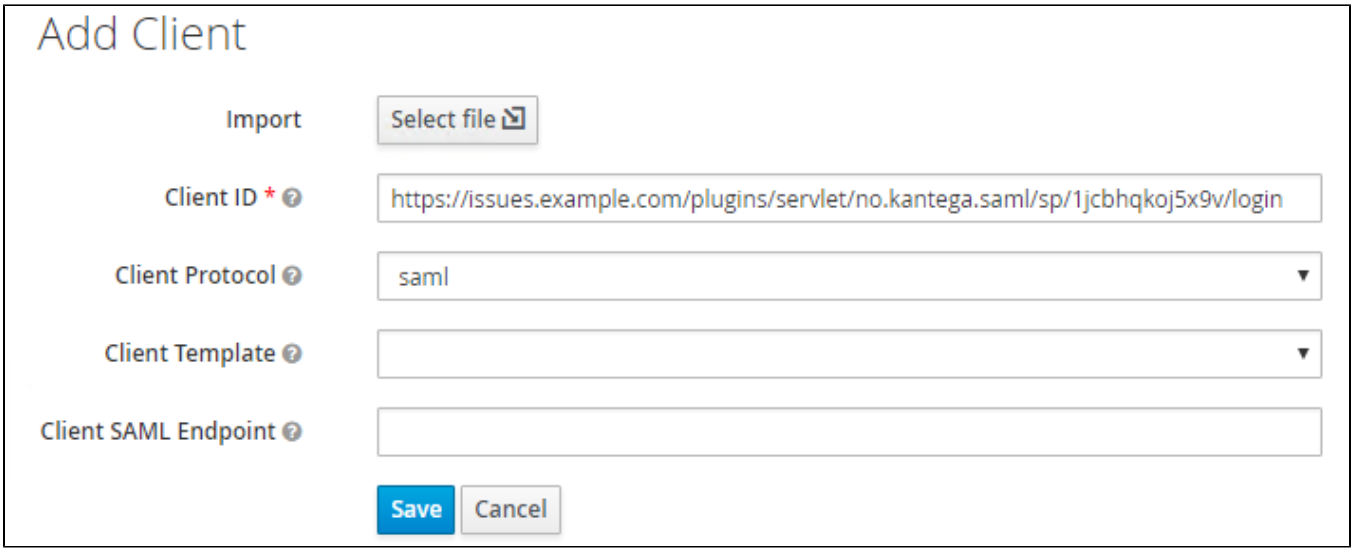


Add a Client in Keycloak

- Make sure the correct realm is selected.
- Select Clients, then Create.



- In Client ID, paste the ACS URL from the Prepare step above.
- Select SAML as the Client Protocol.
- Press Save.



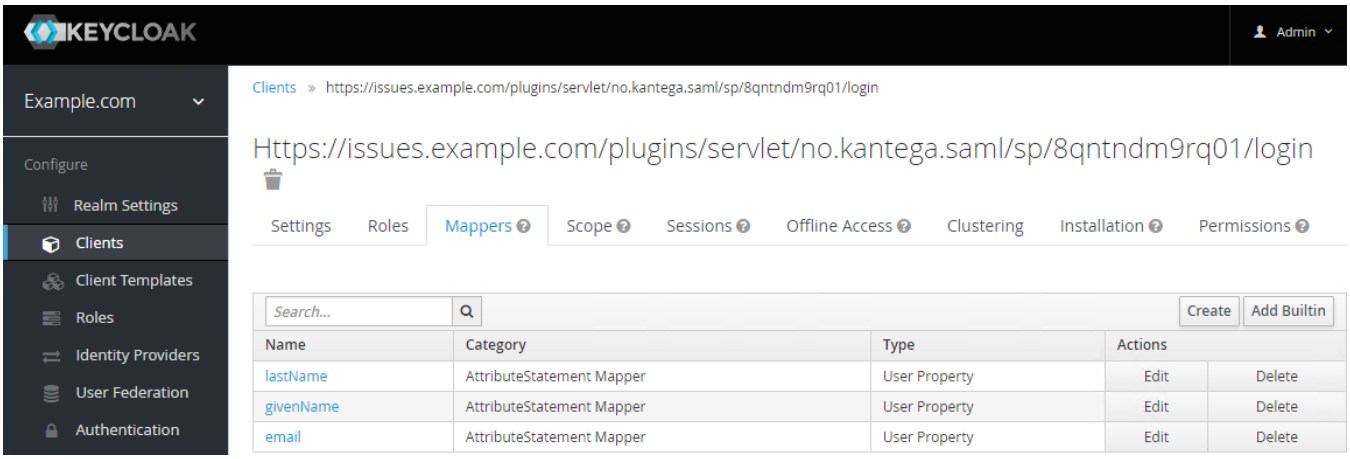
Settings

- Set Client Signature Required to Off
- Paste the ACS URL into the following fields:
    - Valid Redirect URIs.
    - Master SAML Processing URL.

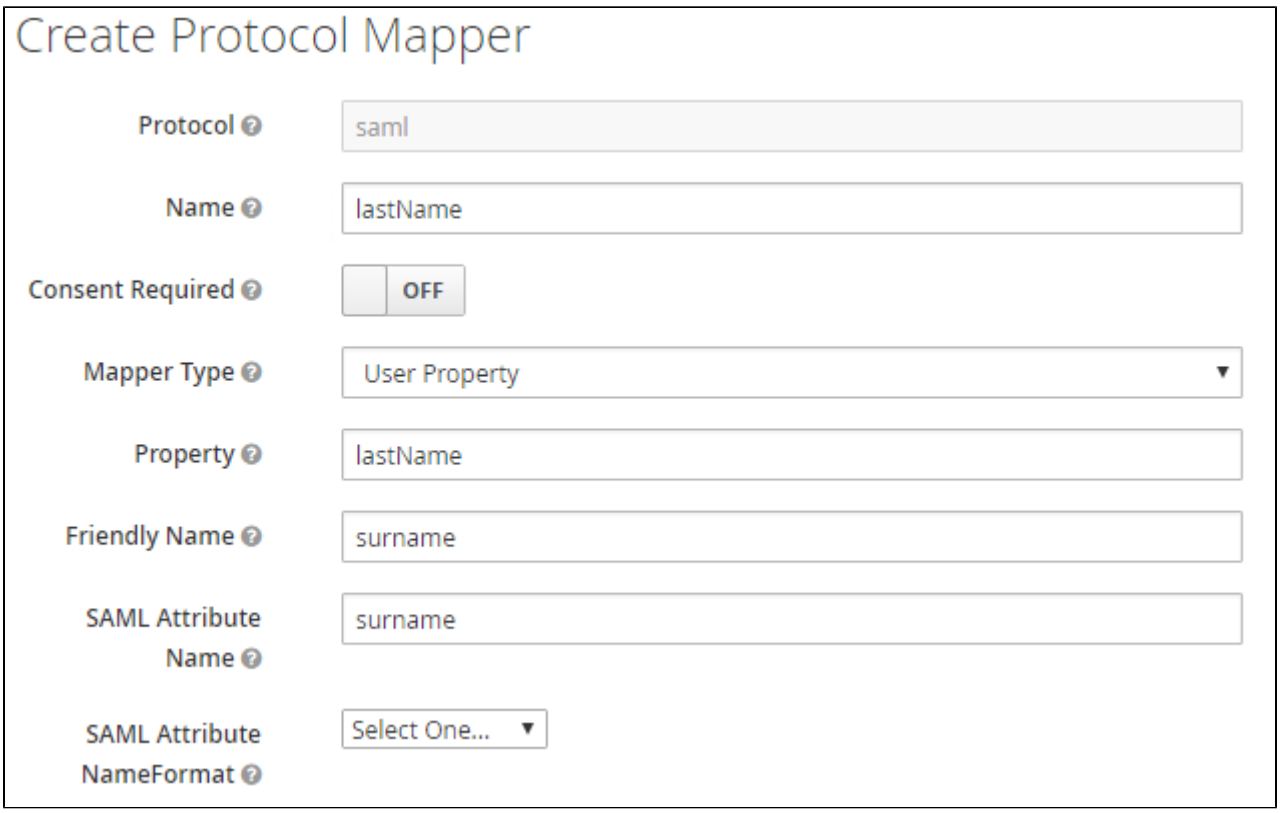
Mappers

Mappes are only needed if you want to have users automatically created on login using SAML JIT provisioning. Mappers make Keycloak include the SAML Response attributes required to create new users in the Internal Directory. If users already exist in JIRA (using LDAP or some other means of provisioning), you can skip this step.

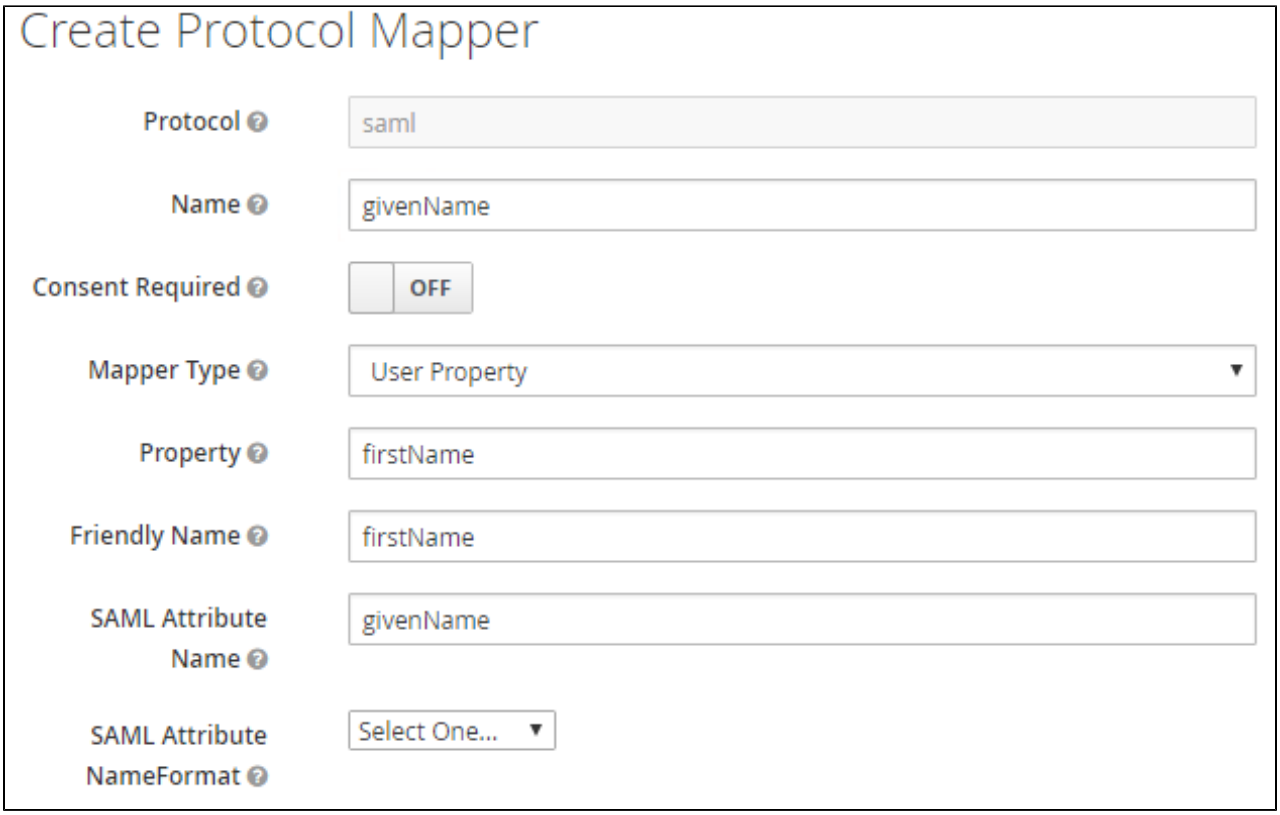
- In Mappers, we are going to add:
    - lastName
    - givenName
    - email
    - managed groups sent via SAML response



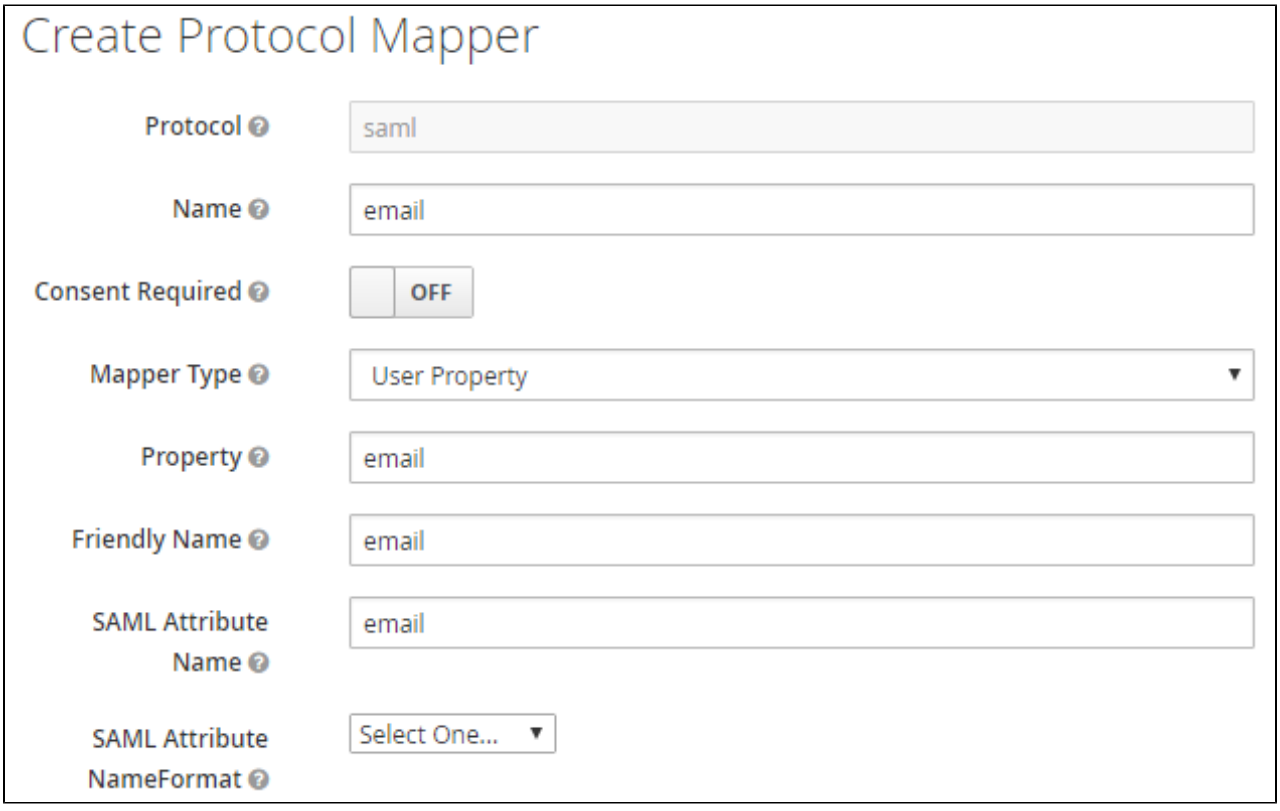
Create mapper for lastName:



Create mapper for givenName

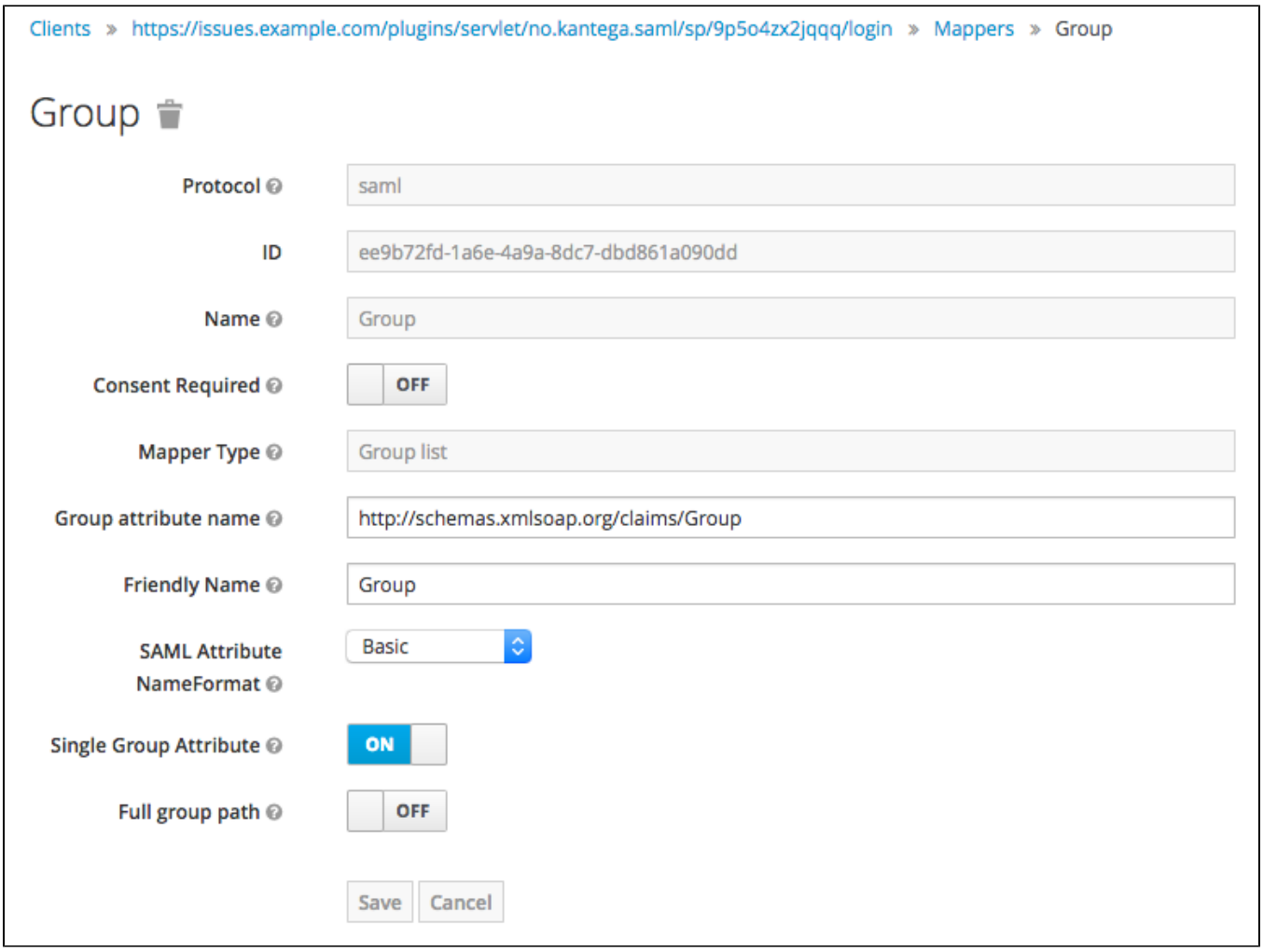


Create mapper for email:



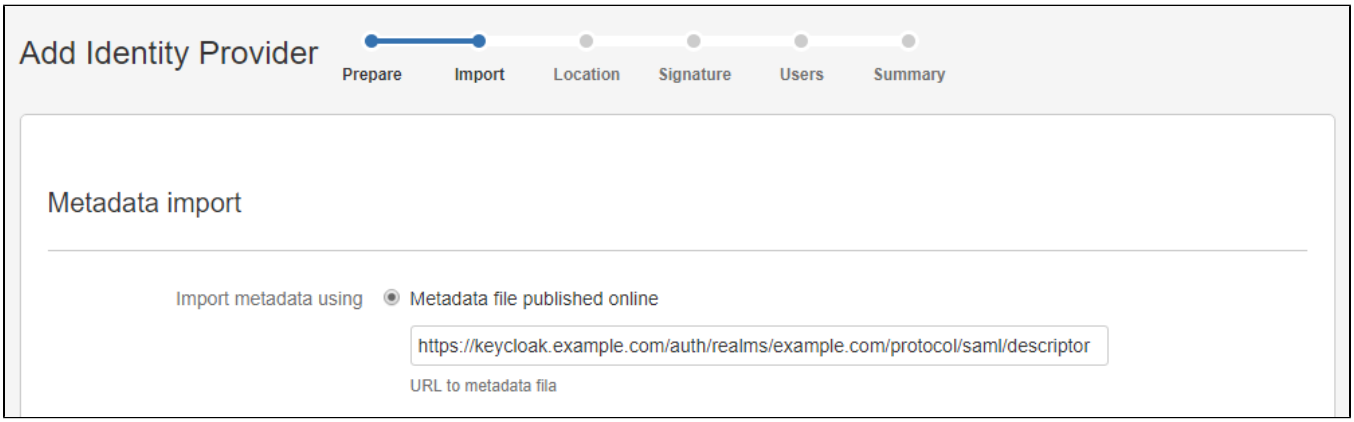
Create mapper for managed group claims:

- Set **Name** and **Friendly Name** to *Group*
- Set **Group** attribute name to http://schemas.xmlsoap.org/claims/Group
- Set **Full group path** to OFF



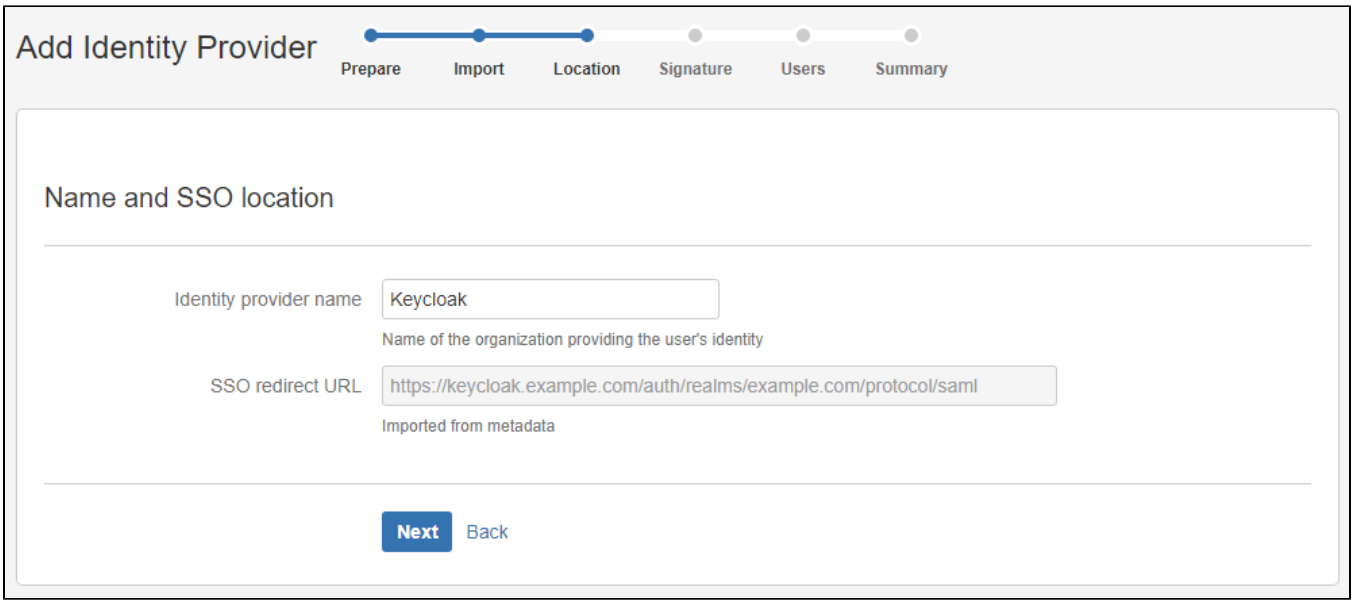
Metadata import

- In Kantega Single Sign-on, go to the metadata import step.
- Importing metadata can be done by providing the metadata URL, or by uploading a metadata file.
  - Via URL: https://keycloak.example.com/auth/realms/example.com/protocol/saml/descriptor
    - Substitute keycloak.example.com with the actual DNS of your keycloak server.
    - Substitute the realm identifier example.com with your realm.
  - Import via file:
    - Navigate to Installation
    - Select format option: SAML Metadata IDPSSODescriptor
- Press Next.



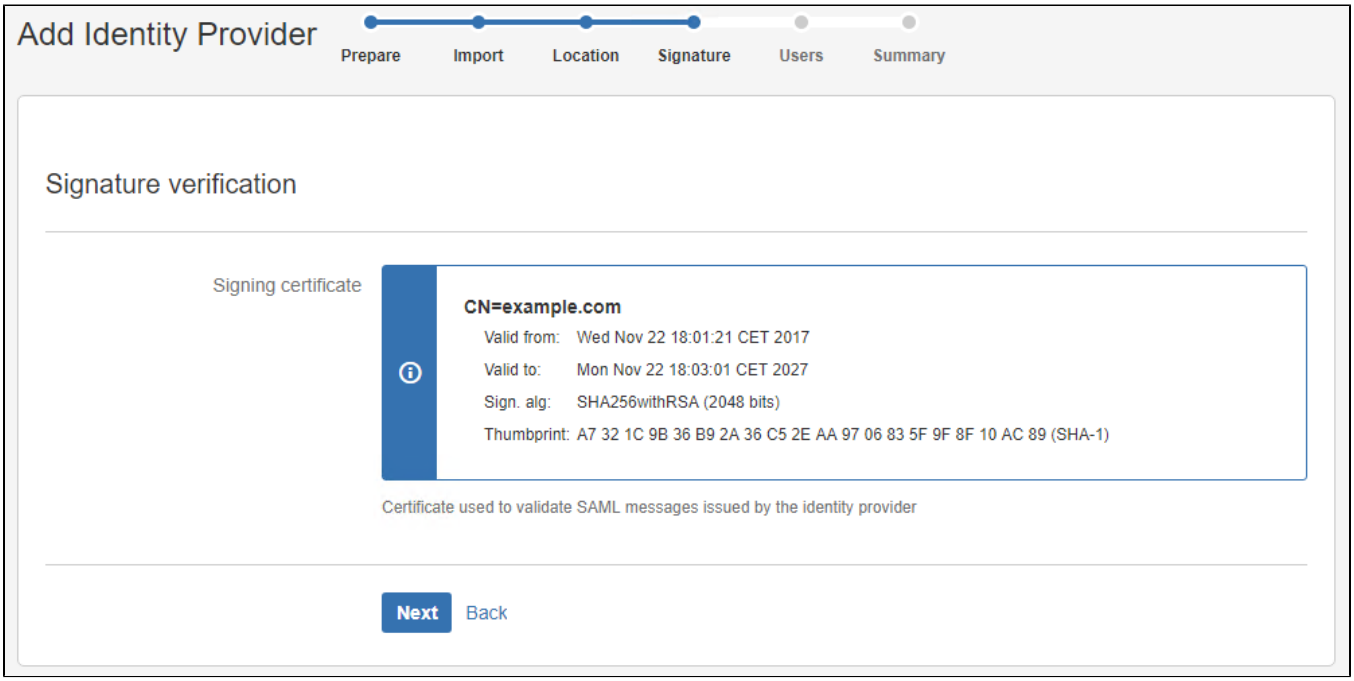
Location

- Give the Identity Provider a name. (This name is visible to end users.)
- The SSO Redirect URL is automatically imported from the metadata.
- Press Next.



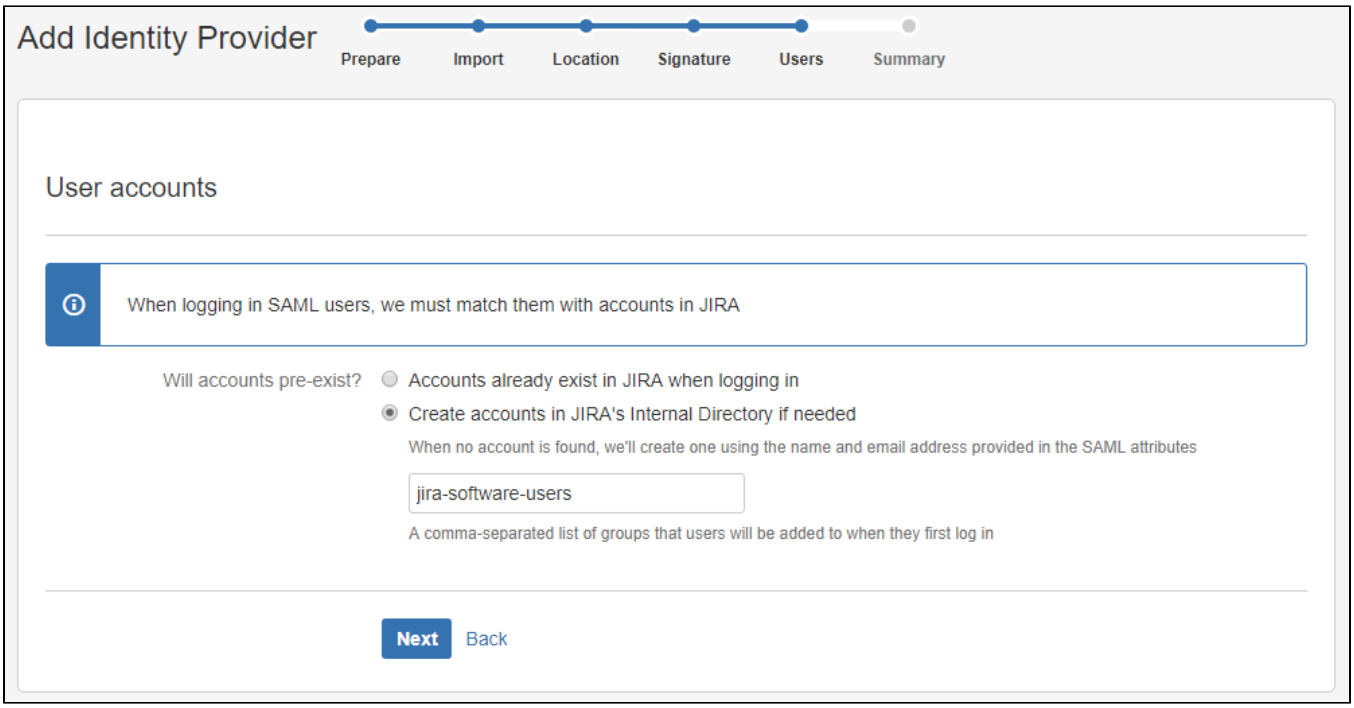
Signature

- Review the imported signing certificate (This step is purely informatinal.)
- Press Next.



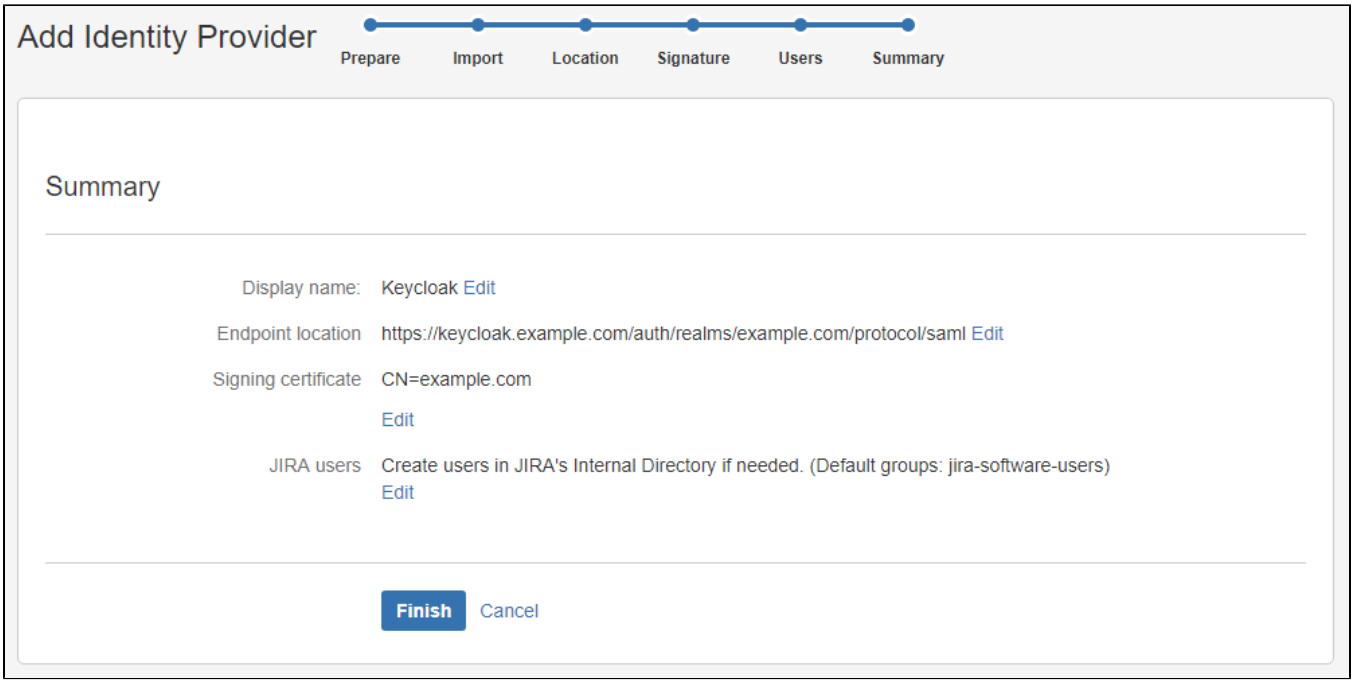
Users

- Select whether users already exist or if you wish to have users automatically created upon login. If using LDAP-provisioning, select "Accounts already exist in JIRA when logging in".
- Otherwise, select the second option to enable SAML JIT provisioning. Note that for users to be created, a name, username and an email must be sent in the SAML response (see instructions on configuring Mappers further back.)
- Optionally assign a default group for new users - all new users will be added to that group.
- (This can all be further configured and changed after initial setup as well)



Summary

- Review the Summary.
- Press Finish.



Testing/configuring the identity provider

After finishing the wizard, you will be sent to the test pages to finalize the setup. Here, you may also perform additional configuration. Follow this generic introduction to the test pages and final configuration. AD FS is used as the example here.