

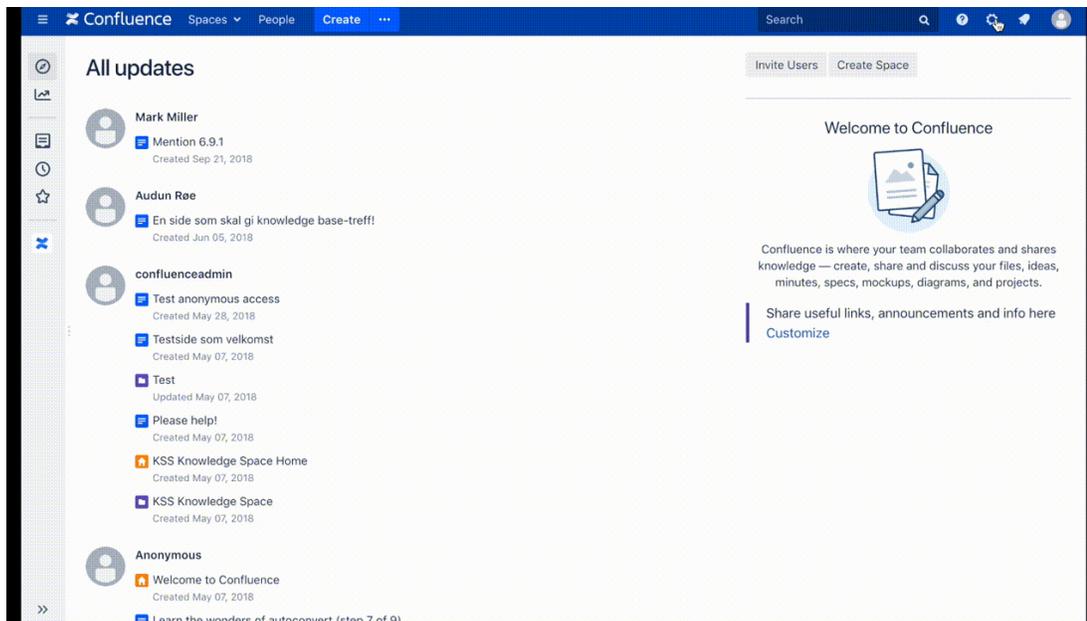
# Keycloak



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](#)).

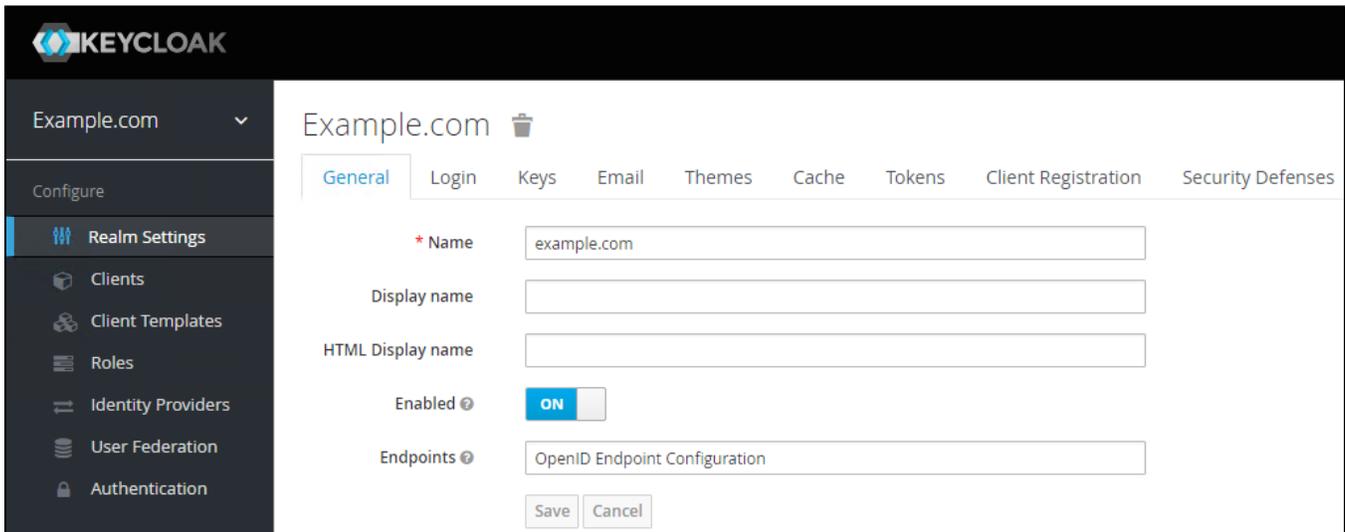
*Context:* This setup starts in the Configuration page of the Kantega SSO add-on. This configuration page can be found by pressing "**Configure**" on "Kantega Single Sign-On (SSO)" in list of installed add-ons.



## 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".

Add SAML Identity Provider ▾

- CLOUD
  - Auth0
  - AuthAnvil
  - Azure Active Directory (Azure AD)
  - Bitium
  - Duo
  - Google GSuite
  - Okta
  - OneLogin
  - PingOne
  - Salesforce
  - WSO2
- ON-PREMISE
  - Active Directory Federation Services (AD FS)
  - Keycloak**
  - Ping Federate
- GENERAL
  - Any other SAML 2.0 Identity Provider



## Prepare

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

Add Identity Provider

Prepare Import Location Signature Users Summary

### Preparing Keycloak

Follow the step-by-step instructions [here](#) to setup JIRA SSO with Keycloak.

The following information is needed by Keycloak to enable JIRA as a service provider / relying party:

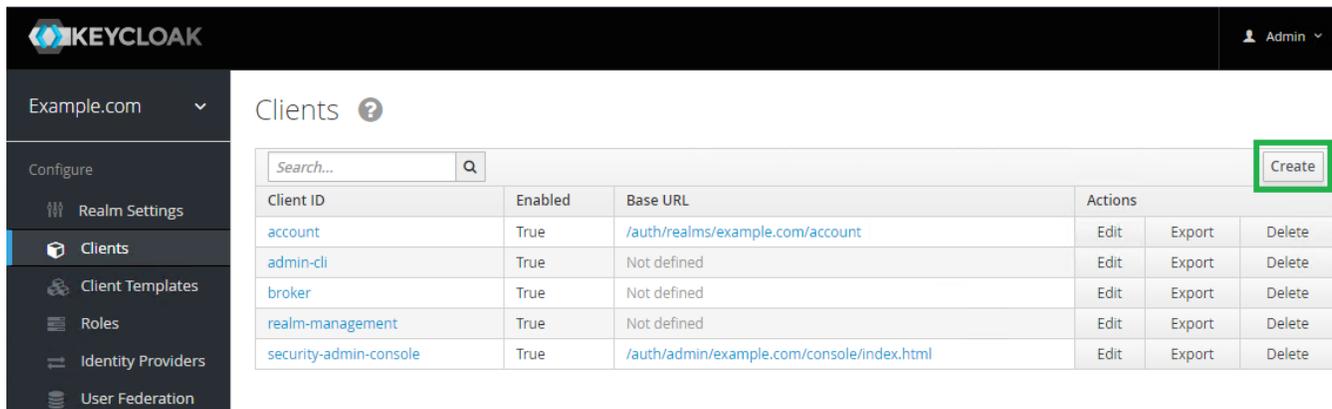
ACS URL

URL where users return after signing in. Also known as "Assertion Consumer Service URL" or "Login URL"

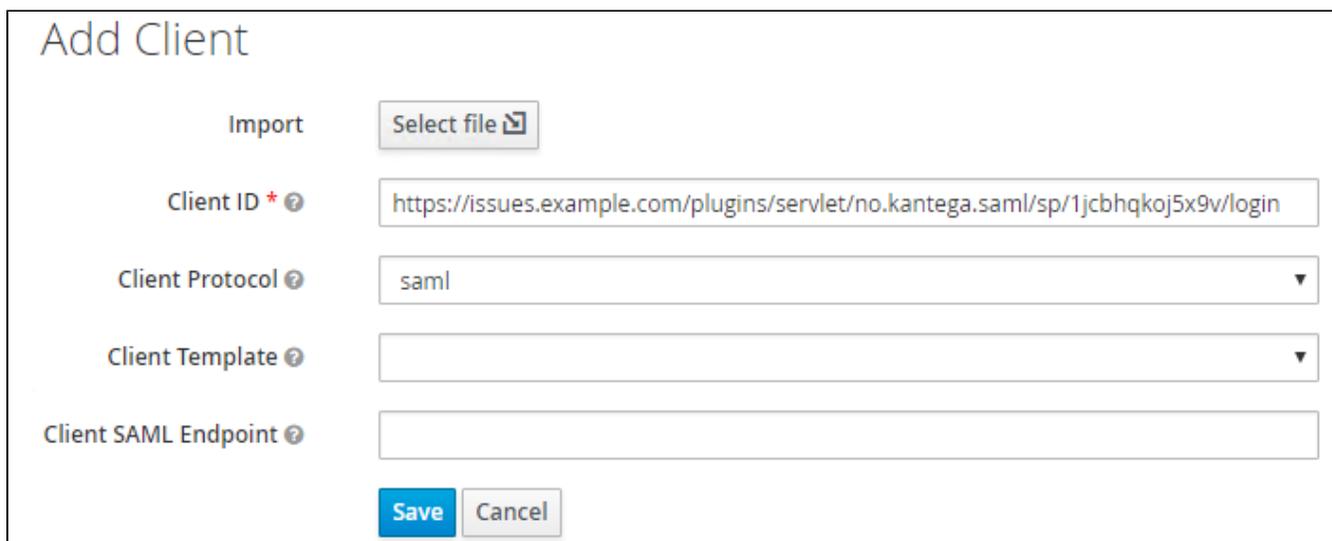
**Next** Save draft Discard

## 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

Mappers 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

**KEYCLOAK** Admin

Example.com

Configure

- Realm Settings
- Clients**
- Client Templates
- Roles
- Identity Providers
- User Federation
- Authentication

Clients > https://issues.example.com/plugins/servlet/no.kantega.saml/sp/8qntndm9rq01/login

https://issues.example.com/plugins/servlet/no.kantega.saml/sp/8qntndm9rq01/login

Settings Roles **Mappers** Scope Sessions Offline Access Clustering Installation Permissions

Search...

Name	Category	Type	Actions	
lastName	AttributeStatement Mapper	User Property	Edit	Delete
givenName	AttributeStatement Mapper	User Property	Edit	Delete
email	AttributeStatement Mapper	User Property	Edit	Delete

Create mapper for lastName:

### Create Protocol Mapper

Protocol

Name

Consent Required  OFF

Mapper Type

Property

Friendly Name

SAML Attribute Name

SAML Attribute NameFormat

Create mapper for givenName

## Create Protocol Mapper

Protocol ?	<input type="text" value="saml"/>
Name ?	<input type="text" value="givenName"/>
Consent Required ?	<input type="checkbox"/> OFF
Mapper Type ?	<input type="text" value="User Property"/>
Property ?	<input type="text" value="firstName"/>
Friendly Name ?	<input type="text" value="firstName"/>
SAML Attribute Name ?	<input type="text" value="givenName"/>
SAML Attribute NameFormat ?	<input type="text" value="Select One..."/>

Create mapper for email:

## Create Protocol Mapper

Protocol ?	<input type="text" value="saml"/>
Name ?	<input type="text" value="email"/>
Consent Required ?	<input type="checkbox"/> OFF
Mapper Type ?	<input type="text" value="User Property"/>
Property ?	<input type="text" value="email"/>
Friendly Name ?	<input type="text" value="email"/>
SAML Attribute Name ?	<input type="text" value="email"/>
SAML Attribute NameFormat ?	<input type="text" value="Select One..."/>

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

## Group

Protocol ?	<input type="text" value="saml"/>
ID	<input type="text" value="ee9b72fd-1a6e-4a9a-8dc7-dbd861a090dd"/>
Name ?	<input type="text" value="Group"/>
Consent Required ?	<input type="checkbox"/> OFF
Mapper Type ?	<input type="text" value="Group list"/>
Group attribute name ?	<input type="text" value="http://schemas.xmlsoap.org/claims/Group"/>
Friendly Name ?	<input type="text" value="Group"/>
SAML Attribute NameFormat ?	<input type="text" value="Basic"/> 
Single Group Attribute ?	<input checked="" type="checkbox"/> ON
Full group path ?	<input type="checkbox"/> OFF
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

## 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.

### Add Identity Provider

Prepare **Import** Location Signature Users Summary

---

#### Metadata import

Import metadata using  Metadata file published online

URL to metadata file

## 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.

### Add Identity Provider

Prepare Import **Location** Signature Users Summary

---

#### Name and SSO location

Identity provider name   
Name of the organization providing the user's identity

SSO redirect URL   
Imported from metadata

**Next** Back

## Signature

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

### Add Identity Provider

Prepare Import Location **Signature** Users Summary

---

#### Signature verification

Signing certificate

**CN=example.com**

Valid from: Wed Nov 22 18:01:21 CET 2017

Valid to: Mon Nov 22 18:03:01 CET 2027

Sign. alg: SHA256withRSA (2048 bits)

Thumbprint: A7 32 1C 9B 36 B9 2A 36 C5 2E AA 97 06 83 5F 9F 8F 10 AC 89 (SHA-1)

Certificate used to validate SAML messages issued by the identity provider

**Next** Back

## 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)

## Add Identity Provider

Prepare Import Location Signature Users Summary

### User accounts

When logging in SAML users, we must match them with accounts in JIRA

Will accounts pre-exist?  Accounts already exist in JIRA when logging in  
 Create accounts in JIRA's Internal Directory if needed  
When no account is found, we'll create one using the name and email address provided in the SAML attributes

A comma-separated list of groups that users will be added to when they first log in

**Next** Back

## Summary

- Review the Summary.
- Press Finish.

## Add Identity Provider

Prepare Import Location Signature Users Summary

### Summary

Display name: Keycloak Edit

Endpoint location <https://keycloak.example.com/auth/realms/example.com/protocol/saml> Edit

Signing certificate CN=example.com  
[Edit](#)

JIRA users Create users in JIRA's Internal Directory if needed. (Default groups: jira-software-users)  
[Edit](#)

**Finish** Cancel

## 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.