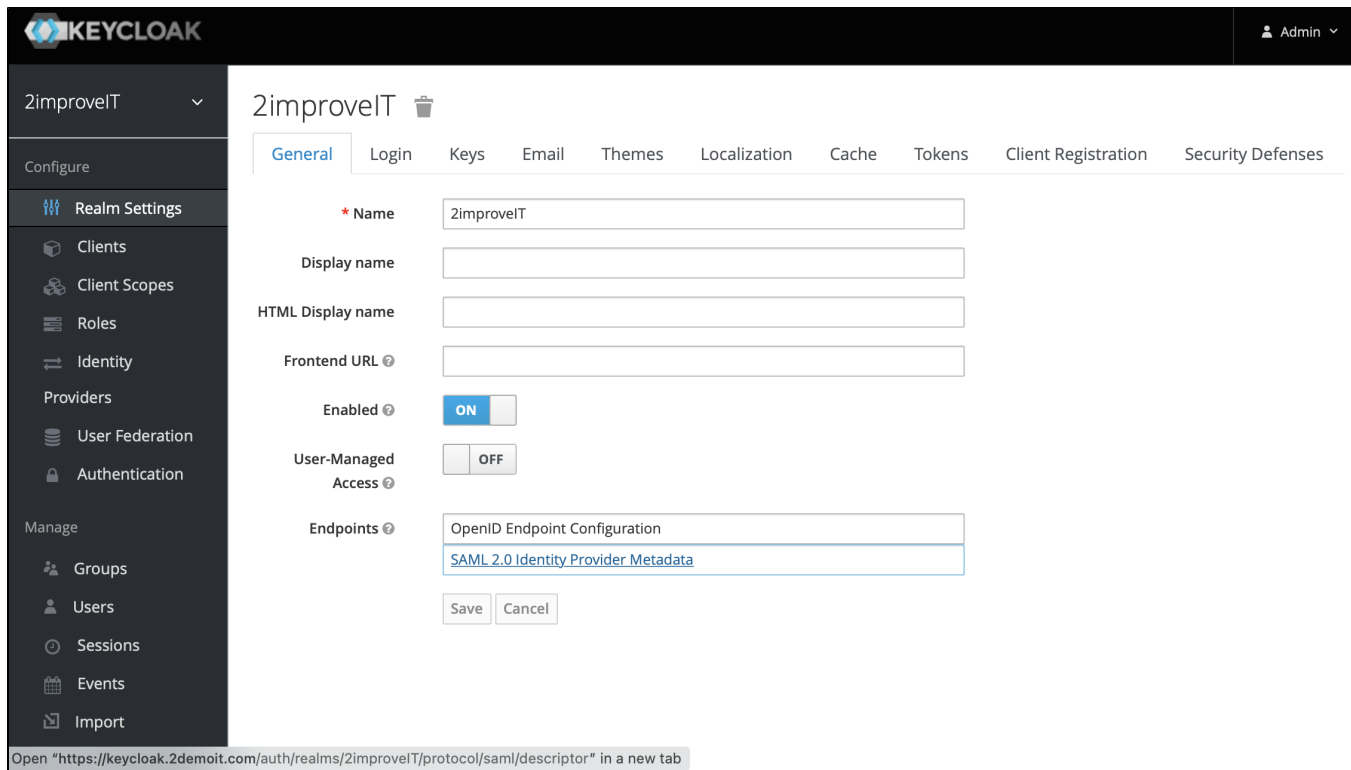


# Configure KeyCloak

Open Keycloak

Select or Create a new Realm in KeyCloak



The screenshot shows the Keycloak Admin Console interface. The top navigation bar includes the Keycloak logo and a user profile dropdown labeled 'Admin'. The left sidebar contains a menu with categories: 'Configure' (Realm Settings, Clients, Client Scopes, Roles, Identity), 'Providers' (User Federation, Authentication), and 'Manage' (Groups, Users, Sessions, Events, Import). The main content area is for the '2improveIT' realm, with tabs for General, Login, Keys, Email, Themes, Localization, Cache, Tokens, Client Registration, and Security Defenses. The 'General' tab is active, showing fields for Name (2improveIT), Display name, HTML Display name, Frontend URL, Enabled (ON), User-Managed Access (OFF), and Endpoints. The 'Endpoints' field contains 'OpenID Endpoint Configuration' and 'SAML 2.0 Identity Provider Metadata', with the latter highlighted. At the bottom, a tooltip reads: 'Open "https://keycloak.2demoit.com/auth/realms/2improveIT/protocol/saml/descriptor" in a new tab'.

**Copy the link pointing to the SAML 2.0 Identity Provider Metadata**

This is a url : <keycloak-url>/auth/realms/<realm-name>/protocol/saml/descriptor

Open the Atlassian Application

**Select the URL option as Identity Provider and paste the in the link**

and press on Save

## Saml Configuration

[Login](#) [IdP](#) [SP](#) [SP XML](#) [Authentication](#) [HTTP Header Authentication](#) [Authorization](#) [Avatar Servlet](#) [Help](#)

## Identity Provider XML Provider

Url

Your Identity Providers XML Provider

## Identity Provider XML

<https://keycloak.2demoit.com/auth/realms/2improveIT/protocol/saml/descriptor>

Your Identity Providers metadata.xml

**Save**

**Copy the SP XML and create a new File e.g. sp.xml and paste the content in this file**

If you don't see the SP Certificate, log out and log in again

## Saml Configuration

[Login](#) [IdP](#) [SP](#) [SP XML](#) [Authentication](#) [HTTP Header Authentication](#) [Authorization](#) [Avatar Servlet](#) [Help](#)

## SP XML

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:xsi="http://www.w3.org/2000/09/xmldsig#"
entityID="https://confluence.2demoit.com/">
<md:SPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<md:NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-
format:specified<-md:NameIDFormat>
<md:AssertionConsumerService index="0" isDefault="true"
Binding="urn:oasis:names:tc:SAML:2.0:bindings/HTTP-POST"
Location="https://confluence.2demoit.com/pluginservlet/saml/auth"/>
<md:KeyDescriptor>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>
MIIBBzCCAACQAwEgYkZjIjVncNAQEFBAQwPEJBMDAgaUxvMzAxMzhhR0hmChMyLjRl
X2ljG9haYy44dWV2OTI0MTNmS9hdXR0LjJlYWVwcGFtY2cw92ZUluZW48XDZl
MDUybnZnAA3NidWovOXZkdXM0YXNzeENrTgzNoVwPEJBMDAgaUxvMzAxMzhhR0hmChMyLjRl
X2ljG9haYy44dWV2OTI0MTNmS9hdXR0LjJlYWVwcGFtY2cw92ZUluZW48XDZl
CQSqS5BlZDQ0eDA4AGNAOCIBK8Q6RFmygzWkqP2mW6KdWlBRvPWPlQzQN
8r0Wt4dW87YTICKoxy8szGzjlbg3qlseVdeHrSImp4TGisn4drlBPwg
```

Service Provider XML

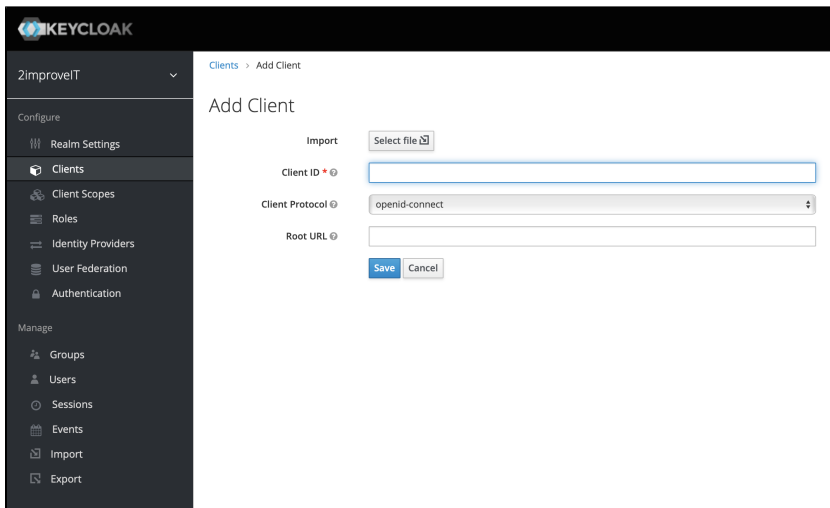
## SP Certificate

[illegible]

Service Provider Certificate

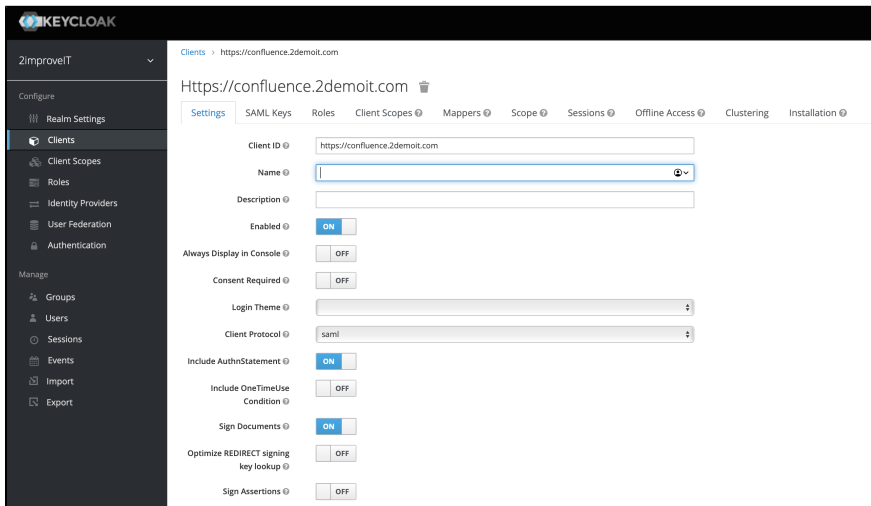
## Open Keycloak

## Select Clients and Create a new Client



The image shows the 'Add Client' form in the Keycloak administration console. The left sidebar contains navigation links for 'Configure' (Realm Settings, Clients, Client Scopes, Roles, Identity Providers, User Federation, Authentication) and 'Manage' (Groups, Users, Sessions, Events, Import, Export). The main content area is titled 'Add Client' and includes an 'Import' button with a file icon, a 'Client ID' text input, a 'Client Protocol' dropdown menu set to 'openid-connect', and a 'Root URL' text input. At the bottom are 'Save' and 'Cancel' buttons.

**Import the sp.xml file and click on Save**



The image shows the 'Settings' tab for a client in the Keycloak administration console. The client is named 'https://confluence.2demoit.com'. The 'Settings' tab is active, and other tabs like 'SAML Keys', 'Roles', 'Client Scopes', 'Mappers', 'Scope', 'Sessions', 'Offline Access', 'Clustering', and 'Installation' are visible. The 'Client ID' is 'https://confluence.2demoit.com', and the 'Name' is empty. The 'Description' is empty. The 'Enabled' toggle is 'ON'. The 'Always Display in Console' toggle is 'OFF'. The 'Consent Required' toggle is 'OFF'. The 'Login Theme' is empty. The 'Client Protocol' is 'saml'. The 'Include AuthnStatement' toggle is 'ON'. The 'Include OneTimeUse Condition' toggle is 'OFF'. The 'Sign Documents' toggle is 'ON'. The 'Optimize REDIRECT signing key lookup' toggle is 'OFF'. The 'Sign Assertions' toggle is 'OFF'.

**Put Client Signature Required and put it on OFF and save again**



The image shows a close-up of the 'Client Signature Required' toggle switch. The text 'Client Signature Required' is followed by a question mark icon. The toggle switch is currently in the 'OFF' position.

**Open Atlassian Application**

**Log out and Click on the Button Login using SAML IDP Server**

The screenshot shows a login interface with the title "Log in". Below the title is a horizontal line. Underneath this line is a blue button labeled "Login using SAML IDP Server". Below the button is another horizontal line with the word "or" centered between two short segments. Underneath this line are two input fields: "Username" and "Password". Below the "Password" field is a checkbox labeled "Remember me". At the bottom of the form are two elements: a blue button labeled "Log in" and a text link labeled "Forgot your password?".

this should redirect to keycloak

The screenshot shows a login interface with the title "2IMPROVEIT" at the top. Below the title is a white box with a blue border. Inside the box, the text "Sign in to your account" is centered. Below this text are two input fields: "Username or email" and "Password". Below the "Password" field is a blue button labeled "Sign In".

## Single Logout

To enable single logout in Keycloak:

- Turn on "Front Channel Logout"
- Enter the logout url in the "Fine Grain SAML Endpoint Configuration" (see "Logout Service POST binding URL")

Force POST Binding ⓘ

OFF

Front Channel Logout ⓘ

ON

Force Name ID Format ⓘ

OFF

Name ID Format ⓘ

username

Root URL ⓘ

Valid Redirect URIs ⓘ

https://jira.2demoit.com/plugins/servlet/saml/auth

+

Base URL ⓘ

Master SAML Processing URL ⓘ

IDP Initiated SSO URL Name ⓘ

IDP Initiated SSO Relay State ⓘ

Fine Grain SAML Endpoint Configuration ⓘ

Assertion Consumer Service POST Binding URL ⓘ

https://jira.2demoit.com/plugins/servlet/saml/auth

Assertion Consumer Service Redirect Binding URL ⓘ

Logout Service POST Binding URL ⓘ

https://jira.2demoit.com/plugins/servlet/saml/logout

Logout Service Redirect Binding URL ⓘ

Advanced Settings ⓘ

Authentication Flow Overrides ⓘ

Save

Cancel

- In the SAML plugin settings, check "Enable single logout"

jira.2demoit.com

You have temporary access to administrative functions. [Drop access](#) if you no longer require it. For more information, refer to the [documentation](#).

Jira Software

Dashboards ▾ Projects ▾ Issues ▾ Boards ▾ Create

Search

🔊 ⓘ ⚙️ 🌟

Administration

Search Jira admin

🔍

Applications Projects Issues **Manage apps** User management Latest upgrade report System

ATLASSIAN MARKETPLACE

Find new apps

Manage apps

ADVANCED ROADMAPS FOR JIRA

Advanced Roadmaps permissions

Advanced Roadmaps license details

Hierarchy configuration

Dependencies

Early access features

SAML CONFIGURATION

**Configure**

SAML Configuration

[Login](#)
[IdP](#)
[SP](#)
[SP XML](#)
[Authentication](#)
[HTTP Header Authentication](#)
[Authorization](#)
[Avatar Servlet](#)
[Help](#)

☒ Show the system login

Show / hide the system login

☒ Show the login button

Show / hide the login button

☒ Show the Service Desk login

Show / Hide the Service Desk login

☐ Show the login button in Service Desk

Show / Hide the login button in Service Desk

☒ Enable single logout

Enable SAML single logout

☐ Force SAML login

If checked, all logins will be made through SAML only. Please test SAML SSO first before checking this box.

Login button title

Login using SAML IDP Server

The text which is shown on the login button

Save

Atlassian Jira Project Management Software (v8.19.1#819001-sha1:ef46de)

[About Jira](#)
[Report a problem](#)

ATLASSIAN

Further Configuration :

- 1. Create a user in Keycloak
- 2. Autoprovision Users from Keycloak
- 3. Create User groups in Keycloak and assign them to a user
- 4. Autoprovision usergroups in Keycloak