

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 the user 'Admin'. The left sidebar contains a menu with categories: Configure, Realm Settings, Clients, Client Scopes, Roles, Identity, Providers, User Federation, Authentication, Manage, Groups, Users, Sessions, Events, and Import. The main content area is for the realm '2improveIT' and includes 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 (OpenID Endpoint Configuration and SAML 2.0 Identity Provider Metadata). A tooltip at the bottom indicates the URL for the SAML 2.0 Identity Provider Metadata endpoint.

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/2improvet/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:ds="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:unspecified</md:NameIDFormat>
    <md:AssertionConsumerService index="0" isDefault="true"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="https://confluence.2demoit.com/plugins/servlet/saml/auth"/>
    <md:KeyDescriptor>
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>
MIIB6zCCA/VQCAQEwDQYJKoZIhvcNAQEFBQAwPjE8MDoGA1UEAxMzaHR0cHM6Ly9r
ZXJlbG9haY4yZGVtb2l0LmNvbS9hdXRoL3JlYXtscy8yaW1wcm92ZUJlM0R4XDTIx
MDUyNzA3NDliOVVoDlRlMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYx
MDUyNzA3NDliOVVoDlRlMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYx
CSqGSIb3DQEBAQUAA4GNADCBiQkgBQoDFMygzwKqD+2mW6kXdWIBfnVwwPLjQnzQN
8r0Wot4wStDdJY71CXosy88zszgZjlb3qlse9xVDEHRS1Mtp4TG5n4DplBrEG
-----
          
```

Service Provider XML

SP Certificate

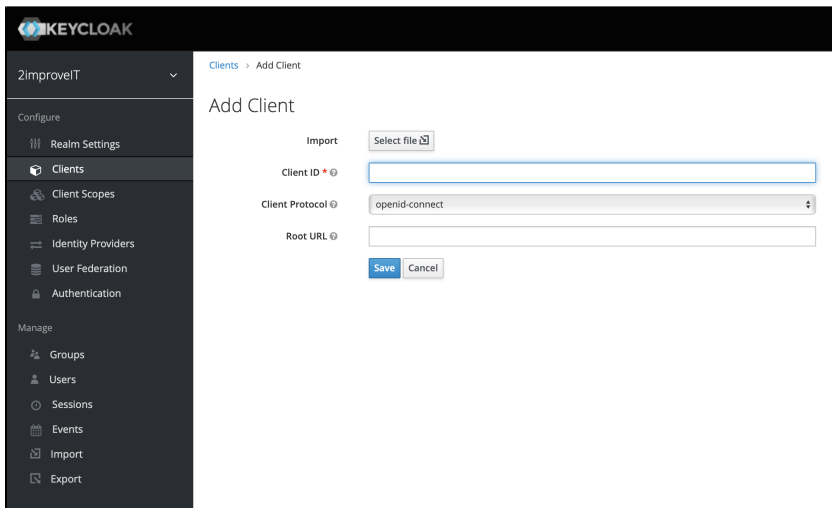
```
-----BEGIN CERTIFICATE-----
MIIB6zCCA/VQCAQEwDQYJKoZIhvcNAQEFBQAwPjE8MDoGA1UEAxMzaHR0cHM6Ly9r
ZXJlbG9haY4yZGVtb2l0LmNvbS9hdXRoL3JlYXtscy8yaW1wcm92ZUJlM0R4XDTIx
MDUyNzA3NDliOVVoDlRlMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYx
MDUyNzA3NDliOVVoDlRlMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYx
CSqGSIb3DQEBAQUAA4GNADCBiQkgBQoDFMygzwKqD+2mW6kXdWIBfnVwwPLjQnzQN
8r0Wot4wStDdJY71CXosy88zszgZjlb3qlse9xVDEHRS1Mtp4TG5n4DplBrEG
/7vBXi071ThkGYSRWntnRIVTOB7DvrMqjamuTjXFYR9dky45zmEBqbbceQJX
PyT1OY+KwiDAQBMAOGCSqGSIb3DQEBBQUAA4GBAIS25qhEitnWazmlkT2AJmSj
CrJ3zZYLujqDvaz6RvYeYtmGvcm00uJzNidipvSWCe2a1GIZXEkHu+JbPwITuc
PQAqMzK7jclNvVtZKLiIdG61B25AVDDbJsD0ipC6gkj2tXFxoM2EZBHNQuWxkAh
Nxs5Xj67GctkoD0gkly5r
-----END CERTIFICATE-----

```

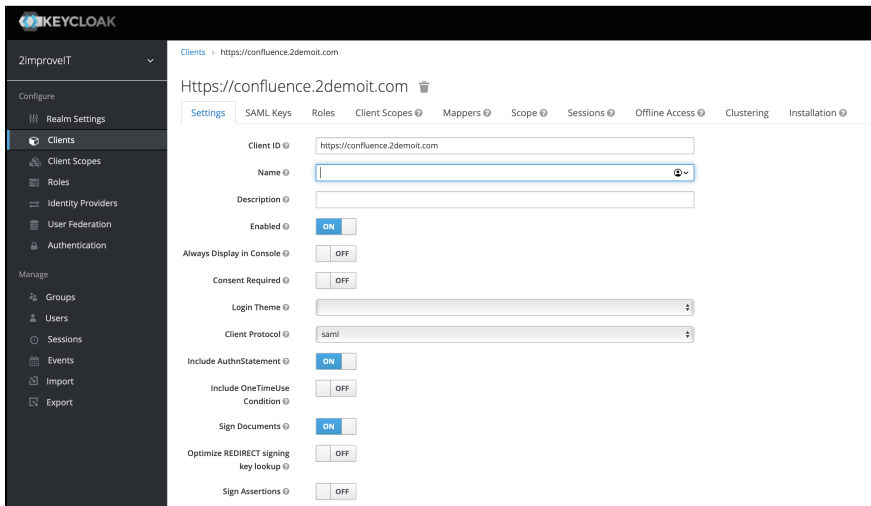
Service Provider Certificate

Open Keycloak

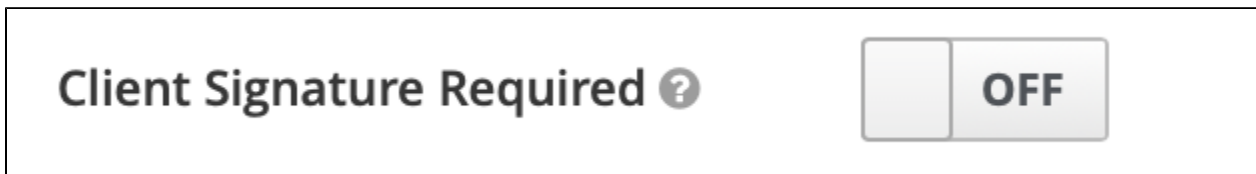
Select Clients and Create a new Client



Import the sp.xml file and click on Save



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



Open Atlassian Application

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

The screenshot shows a login interface. At the top left, the text "Log in" is displayed. Below it is a horizontal line. In the center, there is a blue button with the text "Login using SAML IDP Server". Below this button is another horizontal line with the word "or" centered between two short dashes. Underneath, there are two input fields: "Username" and "Password". Below the "Password" field is a checkbox labeled "Remember me". At the bottom left, there is a blue "Log in" button, and to its right is a link that says "Forgot your password?".

this should redirect to keycloak

The screenshot shows a sign-in page for "2IMPROVEIT". The background is dark with a geometric pattern. At the top, the text "2IMPROVEIT" is displayed in white. Below this, the text "Sign in to your account" is centered. There are two input fields: "Username or email" and "Password". Below the "Password" field is a blue "Sign In" button.

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