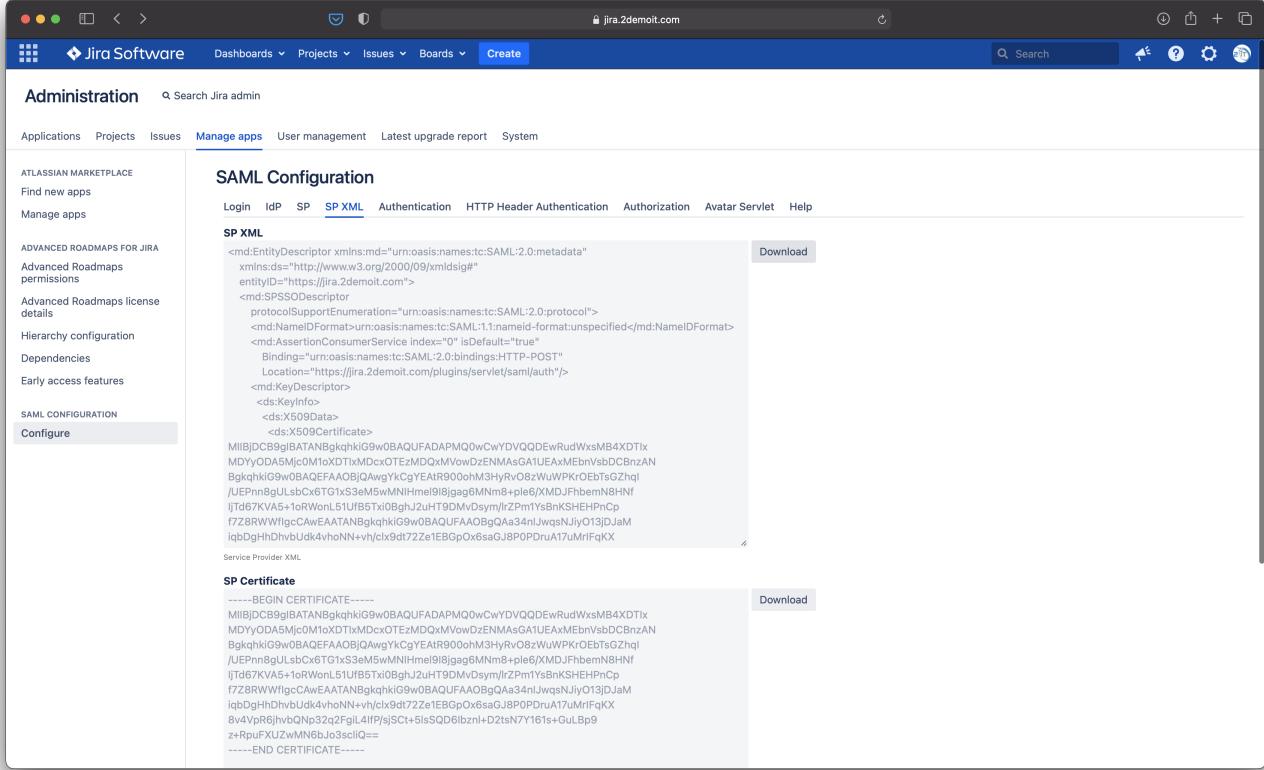


# Configure Azure Active Directory

## Single Login

In the SAML plugin configuration, download the "sp xml"



The screenshot shows the Jira Software Administration interface with the "Manage apps" section selected. Under "SAML Configuration", the "SP XML" tab is active, displaying the Service Provider XML code. A "Download" button is located next to the XML code.

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    entityID="https://jira.2demoit.com">
    <md:SPSSODescriptor
        protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <md:NameIDFormat>urn:oasis:names:tc:SAML: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://jira.2demoit.com/plugins/servlet/saml/auth"/>
        <md:KeyDescriptor>
            <ds:KeyInfo>
                <ds:X509Data>
                    <ds:X509Certificate>
MIIBJDCB9gIBATANBgkqhkiG9w0BAQUFADAMQ0wCwYDVQQDEwRudWxsMB4XDThxMDYyODA5MjMj0M0t0XDTxMDcxOTezMDQzMVowDzENMASGA1UEAxMEbnvbDCBnzANBgkqhkiG9w0BAQEFAAOBJQawgYkCgYEAr90oohM3hyrO8zVuWPKrOEBTsGZhql/UEPn8gUlLsbCx6TGY1S3eM5wMNIIme9l8jgag6MNm8+ple6/XMDJFhbenNBHnfijTd67KVA5+1oRWonL51UIB5Tx0BghJ2uHT9DmVsDsym/lr2Pm1ybsnKSHEHnPnCpfZ8RWWVflgcCwEAATANBgkqhkiG9w0BAQUFFAAOBgQaA34nlJwgsNjUyO13dJaMiqbDgHhDhvbdUdk4vhoNN-vh/clk9dt72ze1EBGpOx6saQJBPOPDruA7uMlfqKXz+RpUFXU2wMNgbJo3scIQC=-----END CERTIFICATE-----
```

Goto <https://portal.azure.com>

Login and goto "Enterprise Applications"

Welcome to Azure!

Don't have a subscription? Check out the following options.

**Start with an Azure free trial**  
Get \$200 free credit toward Azure products and services, plus 12 months of popular [free services](#).

**Manage Azure Active Directory**  
Manage access, set smart policies, and enhance security with Azure Active Directory.

**Access student benefits**  
Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.

**Azure services**

Create a resource   Enterprise applications   User settings   Help + support   Users   All resources   Quickstart Center   Virtual machines   App Services   More services

**Navigate**

Subscriptions   Resource groups   All resources   Dashboard

**Tools**

Microsoft Learn   Azure Monitor   Security Center   Cost Management

Enterprise applications | All applications

New application   Columns   Preview features   Got feedback?

Try out the new Enterprise Apps search preview! Click to enable the preview. →

Name	Homepage URL	Object ID	Application ID
Didn't find what you're looking for? Click 'Add' above to add a new application.			

Overview   Diagnose and solve problems   Manage   Security   Activity   Troubleshooting + Support

Click "New Application", "Create your own application", enter a name and select "Integrate any other application .. (Non-gallery)."

Click "Create"

The screenshot shows the Microsoft Azure portal's Enterprise Applications section. On the left, there's a sidebar with links like Home, Enterprise applications, and a search bar. The main area displays various cloud platforms and on-premises applications. A modal window titled "Create your own application" is open on the right, prompting for the app name ("Jira") and asking what to do with it (options include "Configure Application Proxy", "Register an application to integrate with Azure AD", and "Integrate any other application you don't find in the gallery (Non-gallery)"). Below the modal, a list of recommended applications matching the search term "Jira" is shown.

This screenshot shows the "Overview" page for the "Jira" application within the Azure Enterprise Applications. The left sidebar contains navigation links for Overview, Deployment Plan, Properties, Owners, Roles and administrators (Preview), Users and groups, Single sign-on, Provisioning, Application proxy, Self-service, Conditional Access, Permissions, Token encryption, Sign-ins, Usage & insights, Audit logs, Provisioning logs, and Access reviews. The main content area includes sections for "Properties" (Name: Jira, Application ID: 3a5803f1-30cb-4b0c-806c-1..., Object ID: 5254f7a6-bb67-478a-aef9-c...), "Getting Started" (with four steps: Assign users and groups, Set up single sign on, Provision User Accounts, and Self service), and "What's New" (with three items: Sign in charts have moved!, Delete Application has moved to Properties, and Getting started has moved to Overview).

In the left menu. Click "Sing sign-on" and select "SAML".

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and a user profile for 'geert@2improve.it'. The main content area displays the 'Jira | Single sign-on' page under 'Enterprise Application'. On the left, a sidebar lists various management options like Overview, Deployment Plan, Properties, Owners, Roles and administrators, Single sign-on (which is selected), Provisioning, Application proxy, and Self-service. The main panel title is 'Select a single sign-on method' with a 'Help me decide' link. It lists four options: 'Disabled' (disabled), 'SAML' (selected), 'Password-based', and 'Linked'. The 'SAML' option is described as rich and secure authentication using the SAML protocol.

Click "Upload metadata file" and select the "sp xml" file you have downloaded. Click "Add". Click "Save".

The screenshot shows the 'Jira | SAML-based Sign-on' configuration page. The left sidebar remains the same as the previous screenshot. The main panel has several tabs at the top: 'Upload metadata file', 'Change single-sign-on mode', 'Test this application', and 'Got feedback?'. The 'Upload metadata file' tab is active, showing a file input field containing 'saml-sp.xml'. Below it are four numbered steps: 1. 'Reply URL (Assertion Consumer Service URL)' (Required), 'Sign on URL' (Optional), 'Relay State' (Optional), and 'Logout Url' (Optional). Step 2, 'User Attributes & Claims', lists mappings between user attributes and claims. Step 3, 'SAML Signing Certificate', shows certificate details including status, thumbprint, expiration, and download links for certificate files. Step 4, 'Set up Jira', provides a link to configure the application with Azure AD.

**Basic SAML Configuration**

Identifier (Entity ID) \*

Reply URL (Assertion Consumer Service URL) \*

Sign on URL

Relay State

Logout Url

User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

SAML Signing Certificate

Status	Active
Thumbprint	9AB3A1F7C7935A6B4CEE68043679F6/28/2024, 1:55:42 PM
Expiration	6/28/2024, 1:55:42 PM
Notification Email	geert@2improveit.eu
App Federation Metadata Url	<a href="https://login.microsoftonline.com/ce64c959-adc7-4...">https://login.microsoftonline.com/ce64c959-adc7-4...</a>
Certificate (Base64)	<a href="#">Download</a>
Certificate (Raw)	<a href="#">Download</a>
Federation Metadata XML	<a href="#">Download</a>

Set up Jira

You'll need to configure the application to link with Azure AD.

Login URL

Refresh the "Single sign-on" page. Copy the "App Federation Metadata Url". Go back to the SAML plugin configuration and paste the url in "IdP provider xml" field.

**Basic SAML Configuration**

Identifier (Entity ID)

Reply URL (Assertion Consumer Service URL)

Sign on URL

Relay State

Logout Url

User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

SAML Signing Certificate

Status	Active
Thumbprint	9AB3A1F7C7935A6B4CEE68043679F5FFB71813B5
Expiration	6/28/2024, 1:55:42 PM
Notification Email	geert@2improveit.eu
App Federation Metadata Url	<a href="https://login.microsoftonline.com/ce64c959-adc7-4...">https://login.microsoftonline.com/ce64c959-adc7-4...</a>
Certificate (Base64)	<a href="#">Download</a>
Certificate (Raw)	<a href="#">Download</a>
Federation Metadata XML	<a href="#">Download</a>

Set up Jira

You'll need to configure the application to link with Azure AD.

Login URL

The screenshot shows the Jira Software Administration interface. The top navigation bar includes links for Jira Software, Dashboards, Projects, Issues, Boards, Create, and a search bar. Below the navigation is a sub-navigation bar with links for Applications, Projects, Issues, Manage apps, User management, Latest upgrade report, and System. The main content area is titled "SAML Configuration" under the "Manage apps" tab. It has tabs for Login, IdP, SP, SP XML, Authentication, HTTP Header Authentication, Authorization, Avatar Servlet, and Help. The "IdP" tab is selected. A sub-section titled "Identity Provider XML Provider" shows a dropdown menu set to "Url" and a text input field containing the URL "https://login.microsoftonline.com/ce64c959-adc7-460b-9e19-9c8340569522/federationmetadata/2007-". A "Save" button is located below the URL input. On the left sidebar, there are sections for ATLASSIAN MARKETPLACE, ADVANCED ROADMAPS FOR JIRA, and SAML CONFIGURATION, with "Configure" currently selected.

Do not forget to change the **maxAuthenticationAge**

Here is an example how to configure the create User

The screenshot shows the "Create User" configuration dialog. It includes a checkbox labeled "Create User" with a checked status. Below it is a sub-section titled "Create User if not exists". The configuration fields are listed on the left, and their corresponding values are on the right:

SAML User Id Field	<code>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress.split("@")[0]</code>
SAML User Name Field	<code>http://schemas.microsoft.com/identity/claims/displayname</code>
SAML User Email Field	<code>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress</code>
SAML User Groups Field	<code>group</code>
Default Usergroup(s)	<code>bitbucket-users</code>

Below the configuration fields, a note states: "Assign the new created Users to these usergroups(s)".

**Create User**

Create User if not exists

**SAML User Name Field**

NameId

SAML User Name Field on creation

**SAML User DisplayName Field**

<http://schemas.microsoft.com/identity/claims/displayname>

SAML User DisplayName Field on creation

**SAML User Email Field**

<http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress>

SAML User Email Field on creation

**SAML User Groups Field**

SAML User Groups Field on creation

**Default Usergroup(s)**

Assign the new created Users to these usergroups(s)

**Disable Change Password**

Disable that a user can change his password

## Single Logout

To enable single logout.

- Enter the logout url in your Azure Single Sign-on settings

- And check the "Enable single logout" checkbox in the SAML plugin settings

