

Features

- Current Features
 - AutoRedirect
 - Show/Hide SAML Login Button
 - Rename the SAML Login Button
 - Force SAML
 - Single Logout
 - Upload IdP XML
 - Disable InResponseTo check
 - Download SP XML and/or SP certificate
 - Disable Change Password
 - Specify Login Username from IdP
 - SAML UserId Field
 - Autoprovision Users
 - SAML Username Field
 - SAML User Email Field
 - SAML UsersGroup Field
 - Default Usergroup(s)
 - Creation and Assigning Usergroups
 - Determine Username, Displayname, Email, Groups using the SAML Attributes and expressions
 - Support for ServiceDesk
 - Authentication using Http Headers
 - JIRA
 - CONFLUENCE
 - OTHER ATlassian PRODUCTS
 - Authorization
 - Avatar Servlet
 - Use REST call to update saml configuration
 - Read configuration
 - Write configuration
- Upcoming Features

Current Features

AutoRedirect

When you use the SAML Login Button of the Force SAML feature, you will be redirected to the URL of the page you want to access initially.

So when you click on a link in an email, you will be redirected to this link after you will be authenticated by the SAML IdP

Show/Hide system login

Show or hide the system login. At least one login methods is required.

Show/Hide SAML Login Button

When disabling the SAML Login Button, the login button will not longer be shown on the Login Pages.

You can still use the SAML plugin, using the SAML Login url `<baseUrl>/plugins/servlet/saml/auth` . This will redirect to the default page of the Application after logging in using SAML

If you want to be redirected to another page, you can use `<baseUrl>/plugins/servlet/saml/auth?samlRedirectUrl=<relative path>`.

E.g. in JIRA you can auto login and goto your open issues using the url `<baseUrl>/plugins/servlet/saml/auth?samlRedirectUrl=/issues/?filter=-1`

Rename the SAML Login Button

You can specify what the text needs to be for the SAML Login Button

Force SAML

When enabling this feature all requests which need a login screen will be redirected automatically to the SAML IdP server

Single Logout

You can enable single logout. When a user initiates a logout, the identity provider logs the user out of all applications in the current identity provider login session.

In your IdP provider use the url below as logout url:

<baseUrl>/plugins/servlet/saml/logout

Upload IdP XML

Select a IdP XML file and upload it

SAML Configuration

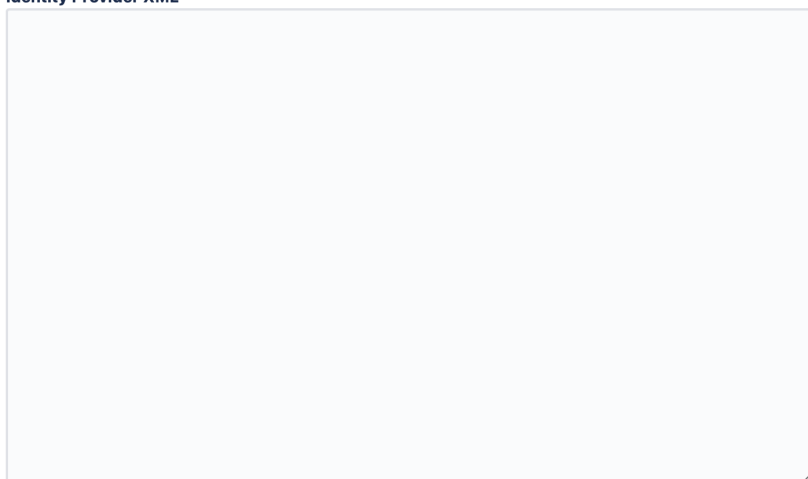
[Login](#) [IdP](#) [SP](#) [SP XML](#) [Authentication](#) [HTTP Header Authentication](#) [Authorization](#) [Avatar Servlet](#) [Help](#)

Identity Provider XML Provider

Text

Your Identity Providers XML Provider

Identity Provider XML



Upload

Your Identity Providers metadata.xml

Save

Disable InResponseTo check

SAML Configuration

Login IdP **SP** SP XML Authentication HTTP Header Authentication Authorization Avatar Servlet Help

SAML endpoint

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

Use this URL in your IdP to initiate a SAML login

SP Entity ID

https://jira.2demoit.com

The EntityID that your plugin will use as ServiceProvider

Max. authentication age

7200

The maximum time the system allows users to single sign-on since their initial authentication with the IDP

Response skew

60

As clocks between IDP and SP machines may not be perfectly synchronized a tolerance of seconds is applied for time comparisons

Disable InResponseTo Check

Disable InResponseTo Check

Save

Download SP XML and/or SP certificate

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://jira-test.k8s.2improveit.eu">
  <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://jira-test.k8s.2improveit.eu/plugins/servlet/saml/auth"/>
    <md:KeyDescriptor>
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>
MIIB+zCCAQQCAQEWdQYJKoZIhvcNAQEFBQAwRjFEMEIGA1UEAxM7aHR0cHM6Ly9p
ZHAuMm1tcHJvdmlpdC5ldS9zaW1wbGVzYW1sL3NhbnWwyL2lkC9tZXRhZGF0YS5w
aHAwHhcNMjEwNTA3MDg0MDI1WhcNMjEwNTA3MDg0MDI1MjEwNTA3MDg0MDI1
dGFkYXRhLnBocDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEApPqe+L0iOc1l
nT3woj/DRo1w2q3er8/IKdpT87dsJIRoa8Wze+cBliYRA3pAtbyyBCrdIH+s7WJ6/
vqs12ZAN/DKK0NON1oGc3ysJQUCdtibkgDW29xE9PGTxV4rsFO8tn/K5LNCDNhP2

```

Download

Service Provider XML

SP Certificate

```
-----BEGIN CERTIFICATE-----
MIIB+zCCAQQCAQEWdQYJKoZIhvcNAQEFBQAwRjFEMEIGA1UEAxM7aHR0cHM6Ly9p
ZHAuMm1tcHJvdmlpdC5ldS9zaW1wbGVzYW1sL3NhbnWwyL2lkC9tZXRhZGF0YS5w
aHAwHhcNMjEwNTA3MDg0MDI1WhcNMjEwNTA3MDg0MDI1MjEwNTA3MDg0MDI1
dGFkYXRhLnBocDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEApPqe+L0iOc1l
nT3woj/DRo1w2q3er8/IKdpT87dsJIRoa8Wze+cBliYRA3pAtbyyBCrdIH+s7WJ6/
vqs12ZAN/DKK0NON1oGc3ysJQUCdtibkgDW29xE9PGTxV4rsFO8tn/K5LNCDNhP2
-----END CERTIFICATE-----
```

Download

Disable Change Password

When enabling this feature the users will not be able to change their password

Disable Change

Password Disable that a user can change his password

Account settings

[Change password](#)

[SSH keys](#)

[Authorized applications](#)

Account settings

Name * 

Email *

Language

Find more language packs on the [Atlassian Marketplace](#)



Current avatar via [Gravatar](#)

[Account settings](#)

Change password

[SSH keys](#)

[Authorized applications](#)

Change password

Current password*

New password*

Confirm password*

Disable Change

Password Disable that a user can change his password

- Account settings
- SSH keys
- Authorized applications

Change password

- Account settings
- SSH keys
- Authorized applications

Account settings

Name*

Email*

Language

Find more language packs on the [Atlassian Marketplace](#)



Current avatar via [Gravatar](#)

Specify Login Username from IdP

SAML UserId Field

The SAML Attribute that will be used to specify the Application username, use the value NameId if you want to use the default NameId of the SAML Response

Autoprovision Users

Create User
Create User if not exists

SAML User Id Field

SAML User Id Field on creation

SAML User Name Field

SAML User Name Field on creation

SAML User Email Field

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)

When the Username is not know by the application, you can opt to create this user in the application.

In order to be able to create this user, we need to specify the SAML Attributes we will use as DisplayName, Email and the groups the user will be assigned to.

SAML Username Field

The SAML Attribute that wil used to specify the DisplayName to the new user

SAML User Email Field

The SAML Attribute that will be used to specify the Email of the new user

SAML UsersGroup Field

The SAML Attribute that will be used to specify to which groups the new user will be assigned to.

Default Usergroup(s)

If the group field in the SAML Attributes is empty or doesn't exists we can specify the usergroups (comma separated) that this user needs to be assigned to.

Creation and Assigning Usergroups

When a new user is created, he is assigned to the usergroups which are the attribute values of the SAML Attribute with the name defined in the SAML UserGroups field.

If there are no attribute values, the user is assigned to the usergroups defined in the default Usergroups(s)

These usergroups are created if they do not exist.

Determine Username, Displayname, Email, Groups using the SAML Attributes and expressions

Create User

Create User if not exists

SAML User Id Field

SAML User Id Field on creation

SAML User Name Field

SAML User nName Field on creation

SAML User Email Field

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)

Examples

expression	value of NameId/SAML Attributes	value of Field	

Named.split("@")[0]	Named : 'username@emaildomain.com'	username	This will take the Named, and return the part before '@' . make sure you use the ascii quotes " and not the `
first_name + ' ' + last_name	first_name : 'John' last_name : 'Field'	'John Field'	This will concatenate the two attributes with a space between them

Support for ServiceDesk

Show the login Button in Service Desk

Show / Hide the login Button in Service Desk

Authentication using Http Headers

When you want to allow authentication using http headers, you can do this by defining these 3 fields in the HTTP Header Authentication

If these headers and token are defined, and are present in the request, the user specified in the **Header User Name** is Authenticated on condition that the value of the **Header Token Name** is equal to the **Header Token Value**.

For security reasons, no direct access should be allowed to the application, all traffic should be done using a reverse proxy, and the reverse proxy should remove this headers when they are present in the request.

Use following url to login using headers: <baseurl>/dologin.action?os_destination=/default.jsp

CONFLUENCE

Use following url to login using headers: <baseurl>/dologin.action?os_destination=/index.action

OTHER ATlassian PRODUCTS

Use default login url

Saml Configuration

[Login](#) [IdP](#) [SP](#) [Authentication](#) [HTTP Header Authentication](#) [Help](#)

Header User Name

HTTP Header Name for User Name

Header Token Name

HTTP Header Name for Token Name

Header Token Value

HTTP Header Value for Token Value

Save

Authorization

- You can allow SAML authentication only for users belonging to a specific user group
- You can restrict Jira authentication for users belonging to a specific user group

SAML Configuration

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

Allowed usergroup(s)

Only allow SAML Authentication when belonging to these usergroups

Restricted usergroup(s)

Only allow Username/Password Authentication when belonging to these usergroups

Save

Avatar Servlet

You can use your server as a gravatar server (only available for Jira, Confluence and Bitbucket)

If you do not care about security you can enable the Avatar Servlet without using a token (leave empty).

The url for the gravatar server will be: **<baseUrl>/plugins/servlet/saml/avatar/**

When using a token, the url for the gravatar server will be: **<baseUrl>/plugins/servlet/saml/avatar/<token>/**

SAML Configuration

Login IdP SP Authentication HTTP Header Authentication Authorization **Avatar Servlet** Help

Enable avatar servlet

When enabled, you can use this server as gravatar server

Avatar servlet token value

Generate token

Use a token to secure access to this gravatar server

Save

Use REST call to update saml configuration

Read configuration

```
curl -v -u admin:admin 'http://localhost:2990/jira/plugins/servlet/saml/common-config' -H 'Accept: application/json'
```

Write configuration

```
curl -v -u admin:admin 'http://localhost:2990/jira/plugins/servlet/saml/common-config' \
-XPUT \
-H 'Content-Type: application/json' \
--data-binary '{"":"http://localhost:2990/jira/plugins/servlet/saml/auth", "showButton":true, "serviceDesk":true, "forceSAML":false, "buttonTitle":"SAML Login", "spEntityId":"http://localhost:2990/jira", "maxAuthenticationAge":"7200", "responseSkew":"60", "allowedUsergroups":"","headerUserName":"","headerTokenName":"","headerTokenValue":"","createUser":false, "createUserId":"NameId", "createUserName":"name", "createUserEmail":"email", "canCreateUsergroups":false, "canUpdateUsergroups":false, "canRemoveUsergroups":false, "createUserGroups":"eduPersonAffiliation", "defaultUsergroup":"","disableChangePassword":false, "idpXmlProvider":"Url", "idpXml":"https://idp.2improveit.eu/simplesaml/saml2/idp/metadata.php"}'
```

Upcoming Features

These are the features which will be available in the next Release, If you already need these features, please contact us using the [SAML Service Desk](#)

