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

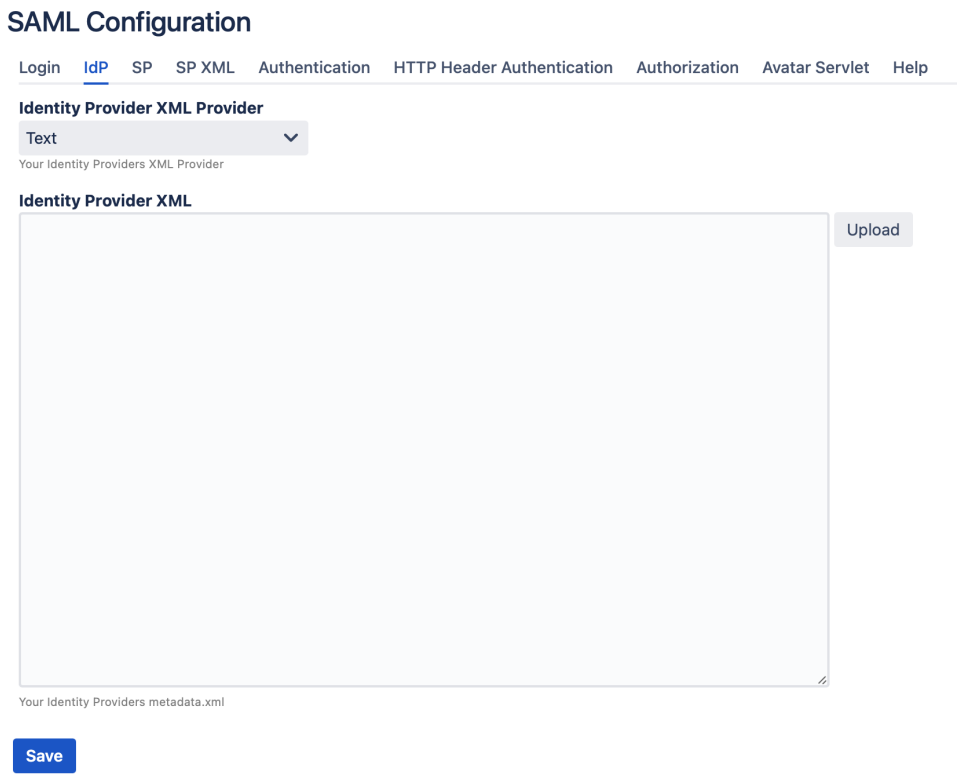
You can enable single logout. When a user initiates a logout, the identity provider logs the user out of all applications in the current identity provider login session.

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

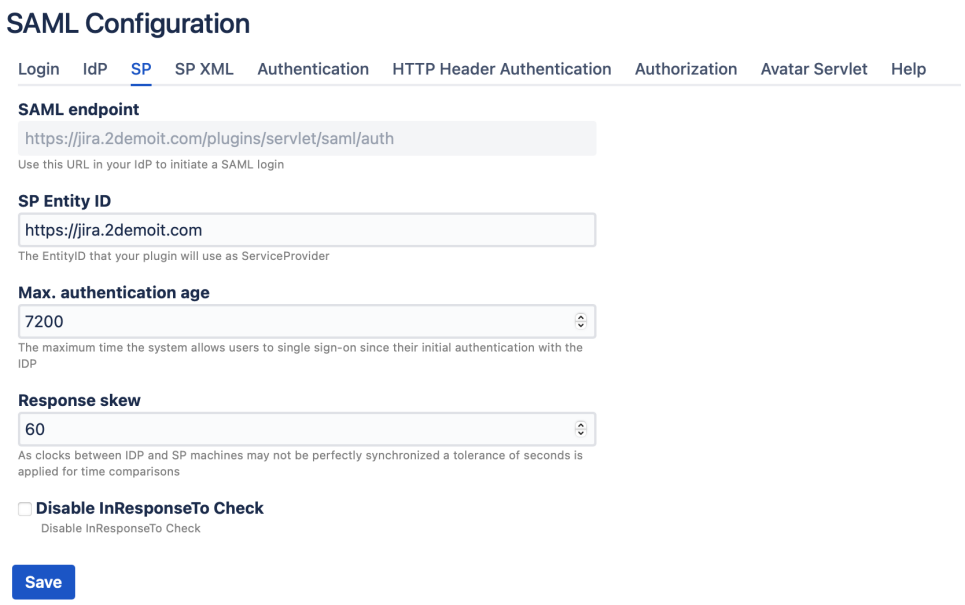
<baseUrl>/plugins/servlet/saml/logout

Upload IdP XML

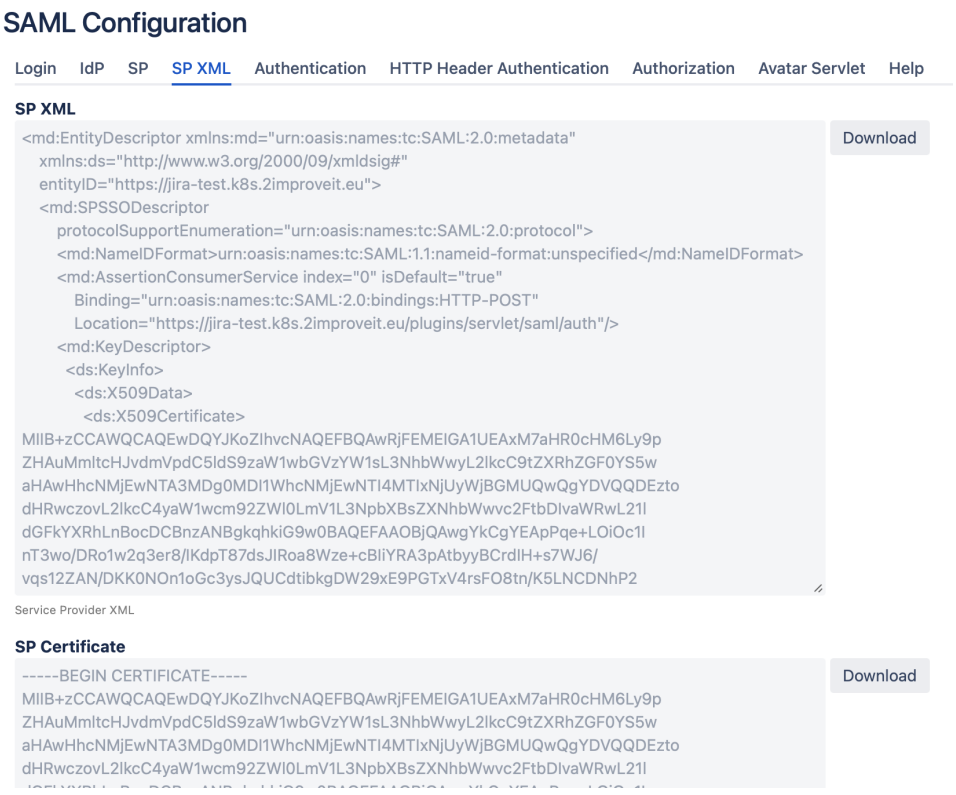
Select a IdP XML file and upload it



Disable InResponseTo check

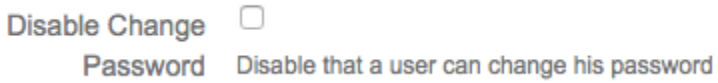


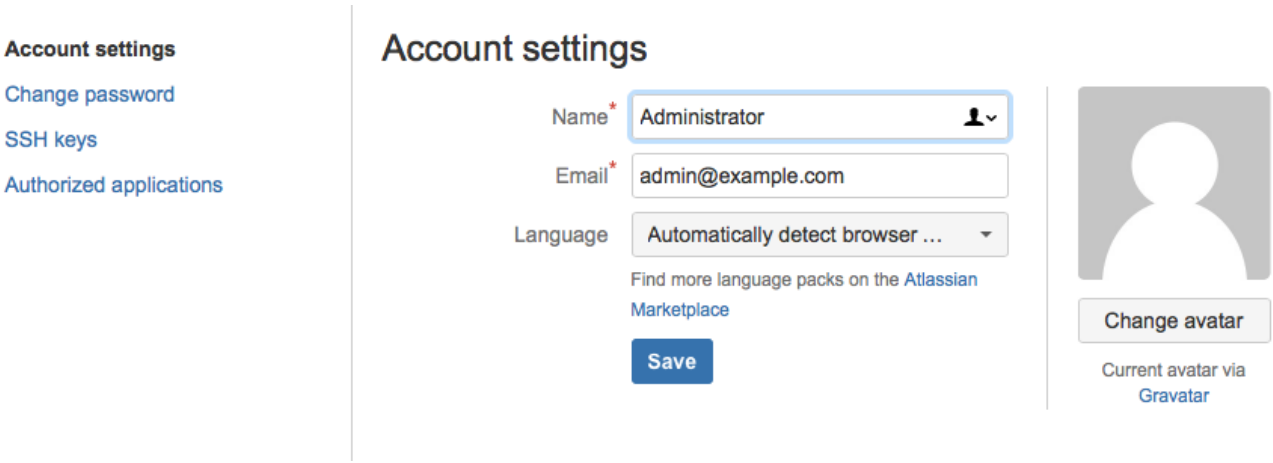
Download SP XML and/or SP certificate

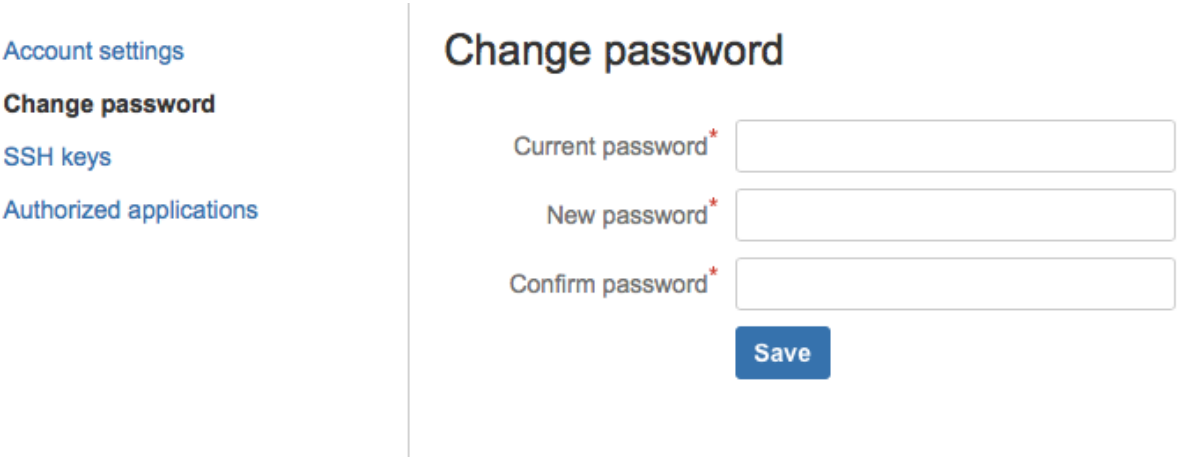


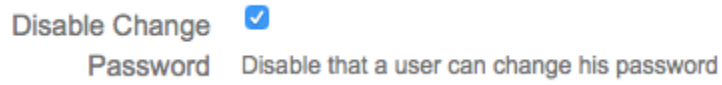
Disable Change Password

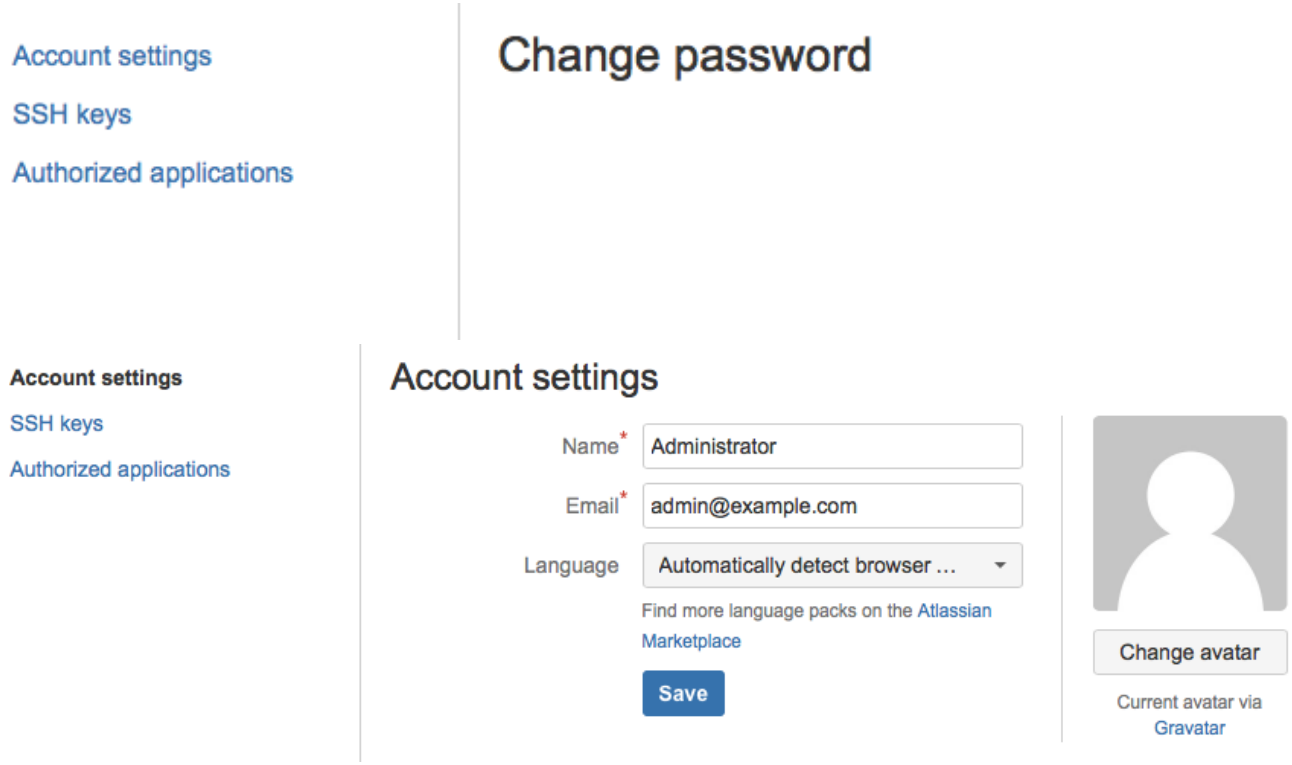
When enabling this feature the users will not be able to change their password




Account settings
Change password
SSH keys
Authorized applications
Account settings
Name*
Administrator
Email*
admin@example.com
Language
Automatically detect browser ...
Find more language packs on the Atlassian Marketplace
Save
Change avatar
Current avatar via Gravatar


Account settings
Change password
SSH keys
Authorized applications
Change password
Current password*
New password*
Confirm password*
Save


Disable Change Password
Disable that a user can change his password

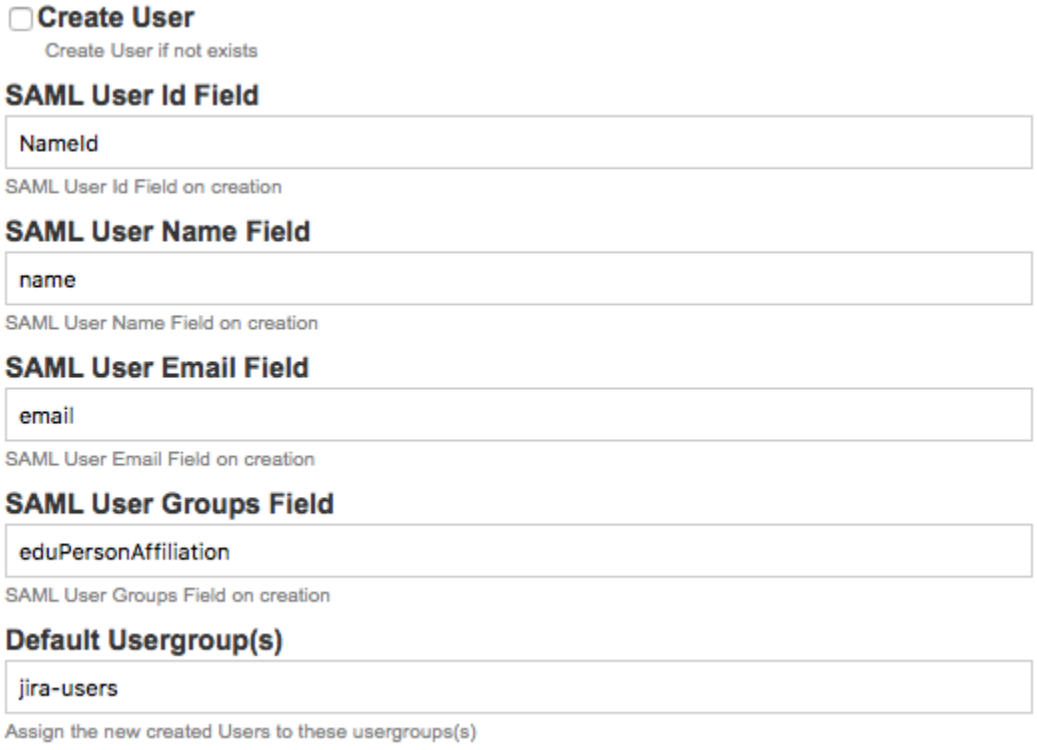


Specify Login Username from IdP

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



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.

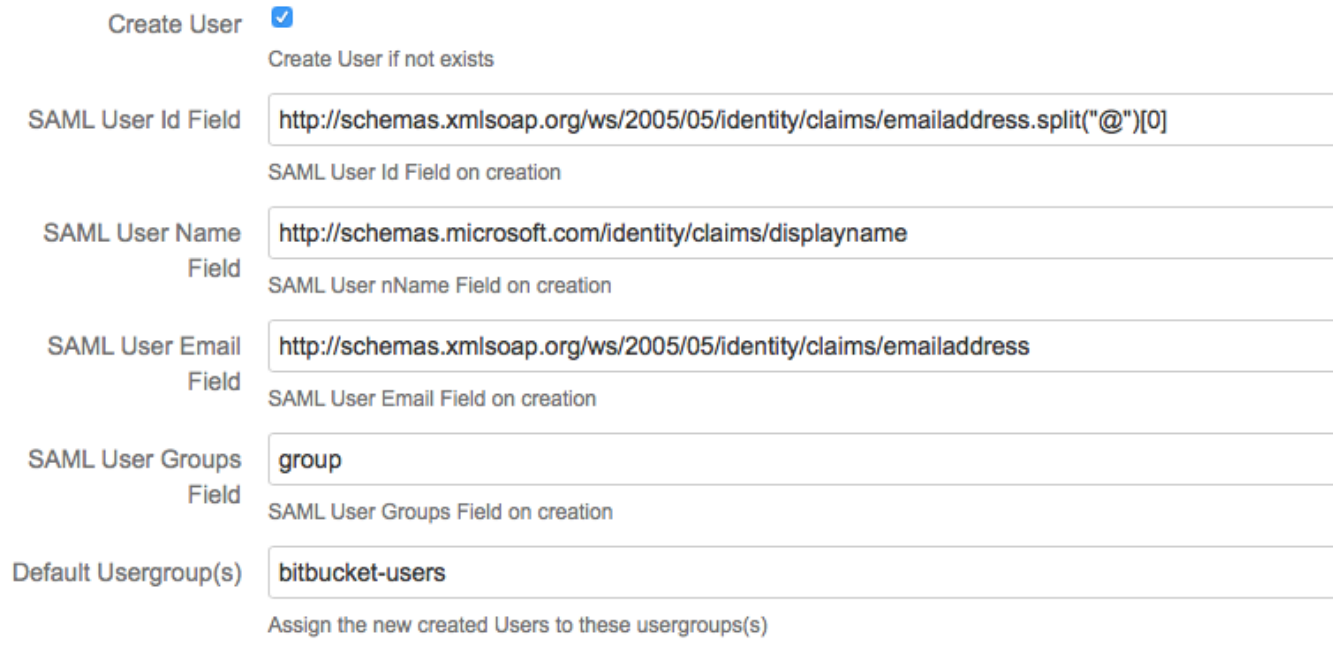
Creation and Assigning Usergroups

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



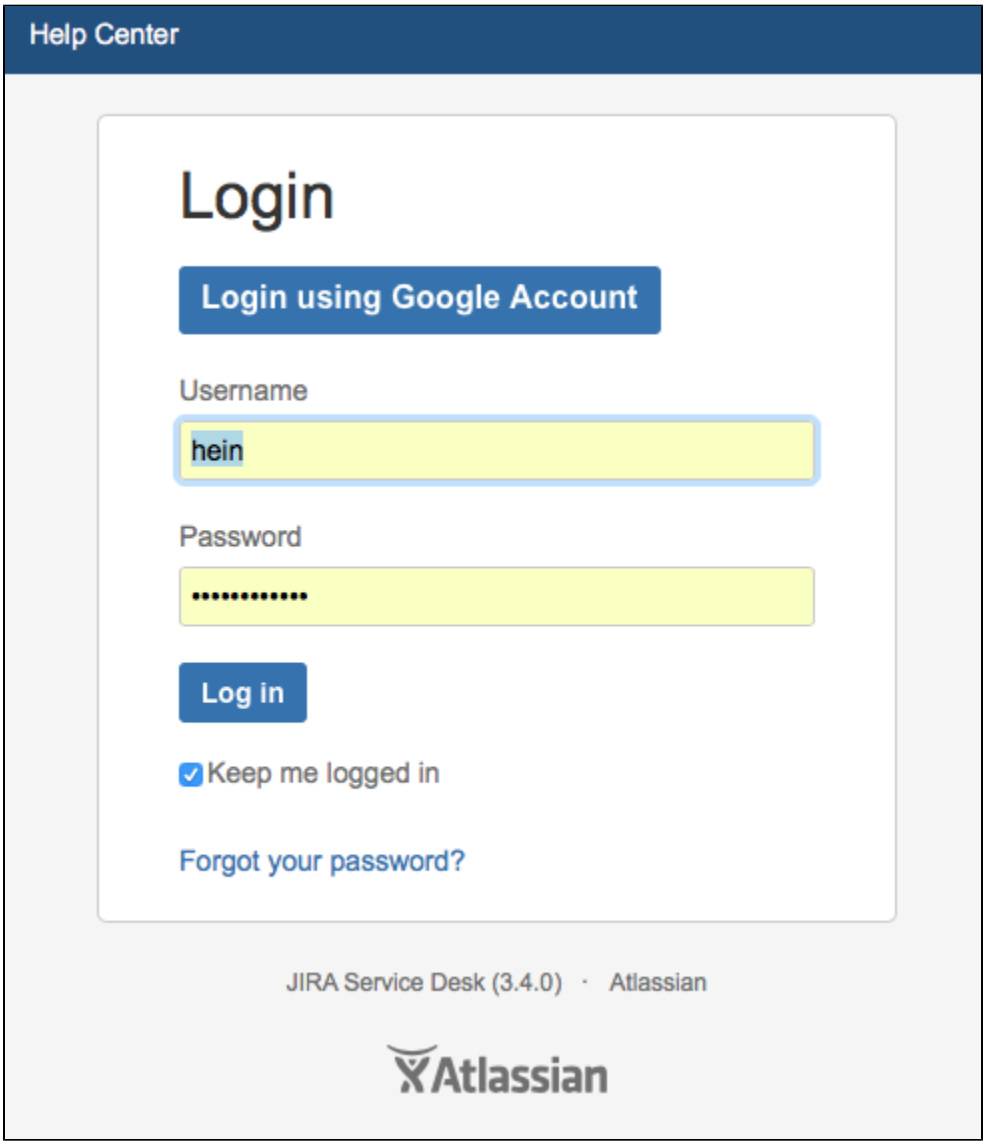
Examples

expression	value of NameId/SAML Attributes	value of Field	

NameId.split("@")[0]	NameId : '**username@emaildomain.com**'	**username**	This will take the NameId, 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





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.

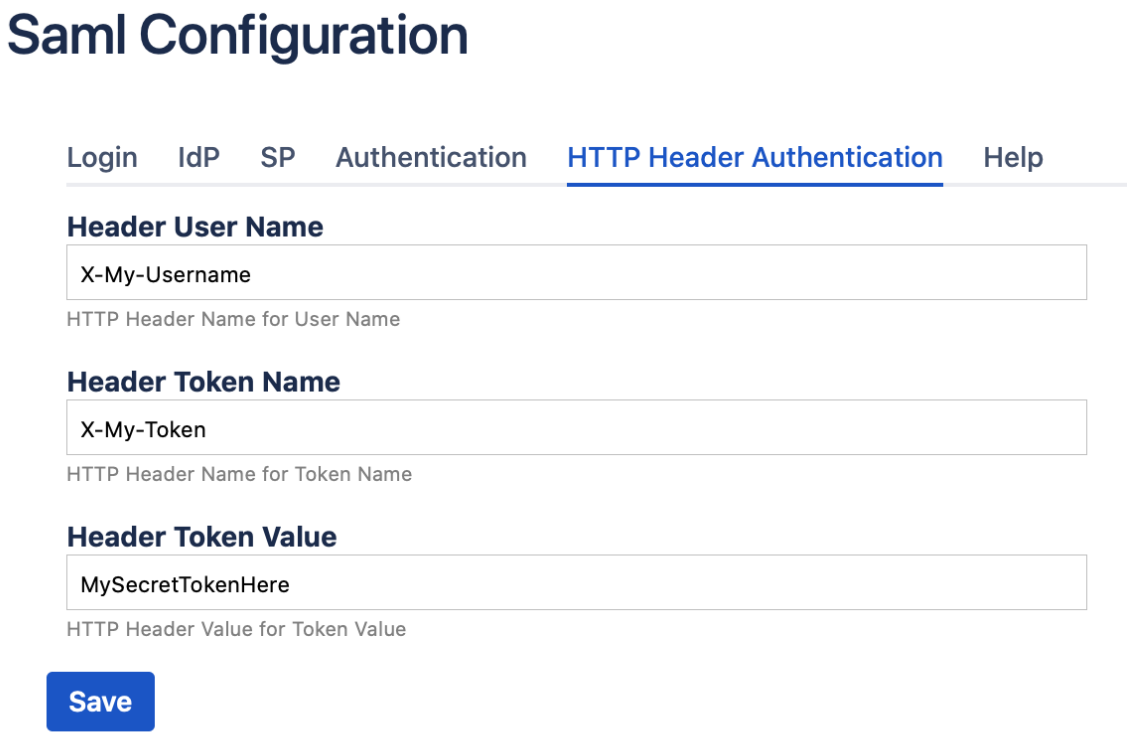
Use following url to login using headers: **<baseurl>/dologin.action?os_destination=/default.jsp**

CONFLUENCE

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

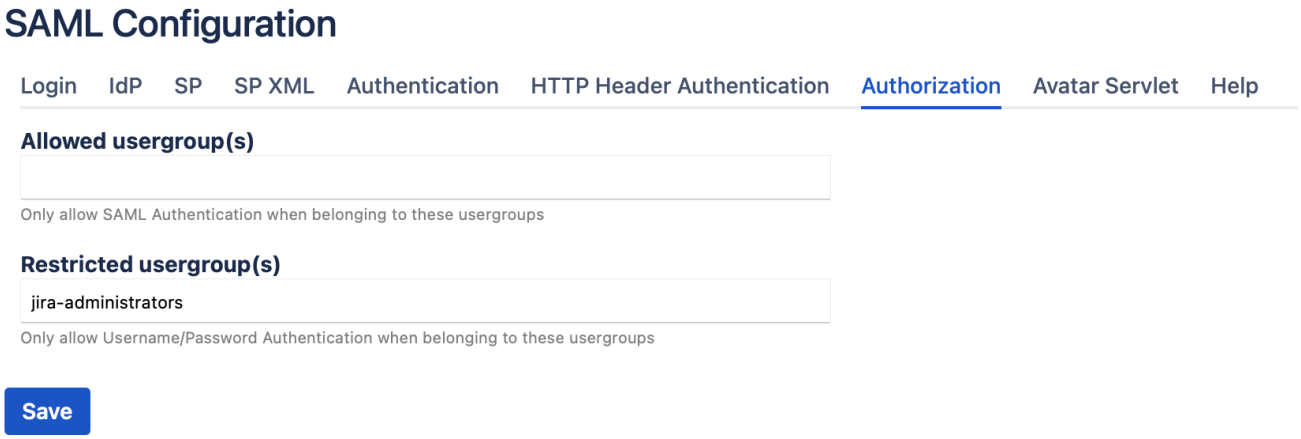
OTHER ATLASSIAN PRODUCTS

Use default login url



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



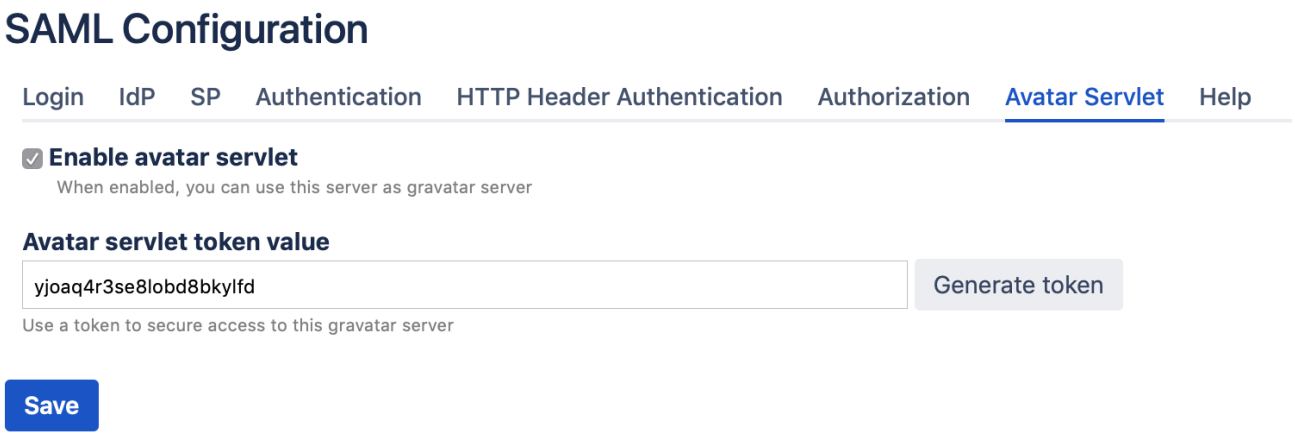
Avatar Servlet

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>/**



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