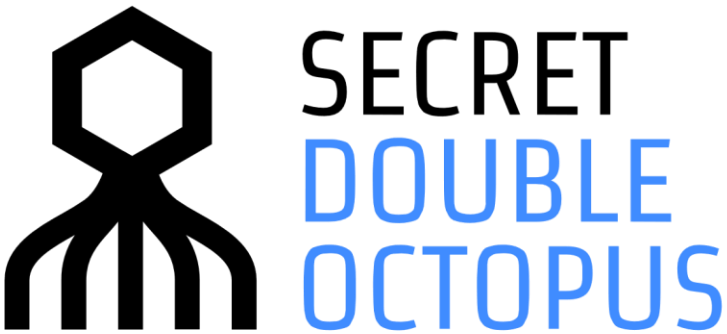
February 13, 2018



How to Configure Octopus Authenticator for Jira Software

Preface

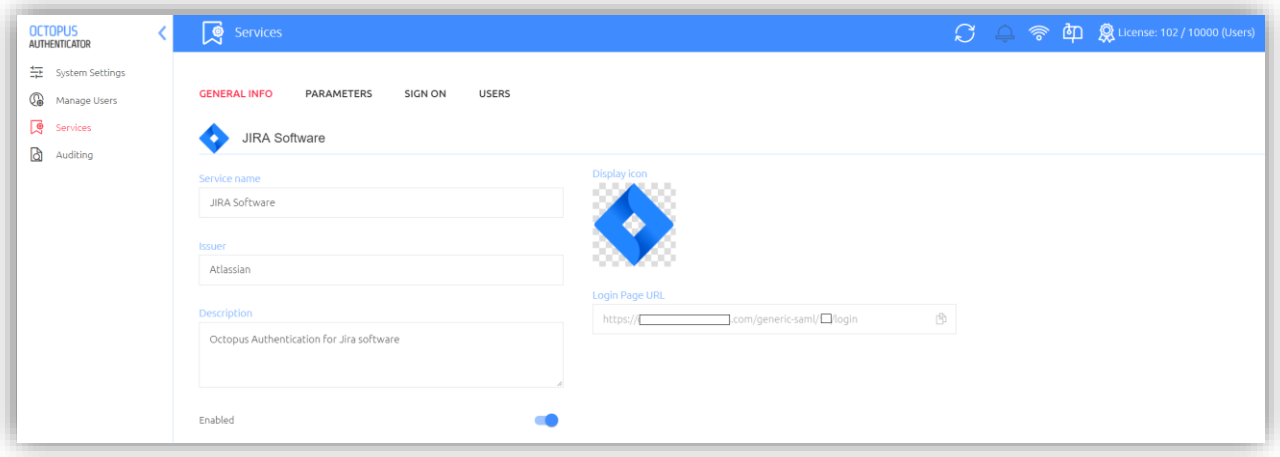
This document describes the configurations required for SAML2.0 integration between the Octopus Authenticator and Jira Software Service.

Octopus Authenticator SAML2.0 Service Configuration

- Login to Octopus Authenticator Console
- Select **Services** from the left pane
- Select Add Service
- Click **Generic SAML** service template

Tab-1: General Information

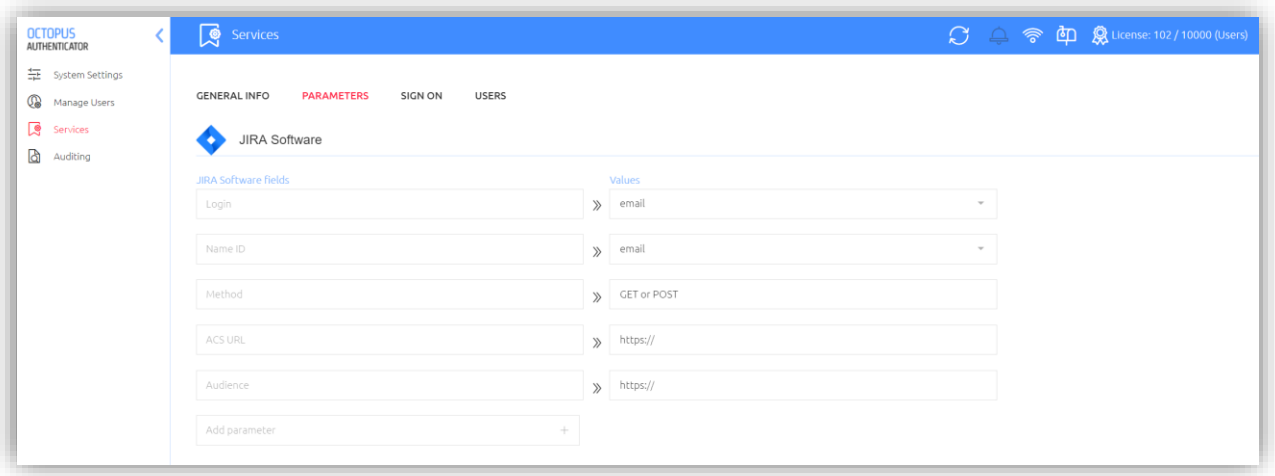
The following field and values are displayed



Fields name	Fields Value
Service name	Jira Software
Issuer	Atlassian
Description	Octopus Authentication for Jira Software
Service status	Enable (default)
Display icon	
Login page URL	<https://<Enterprise Base URL>/generic-saml/<No.>/login>

Tab-2: Parameters

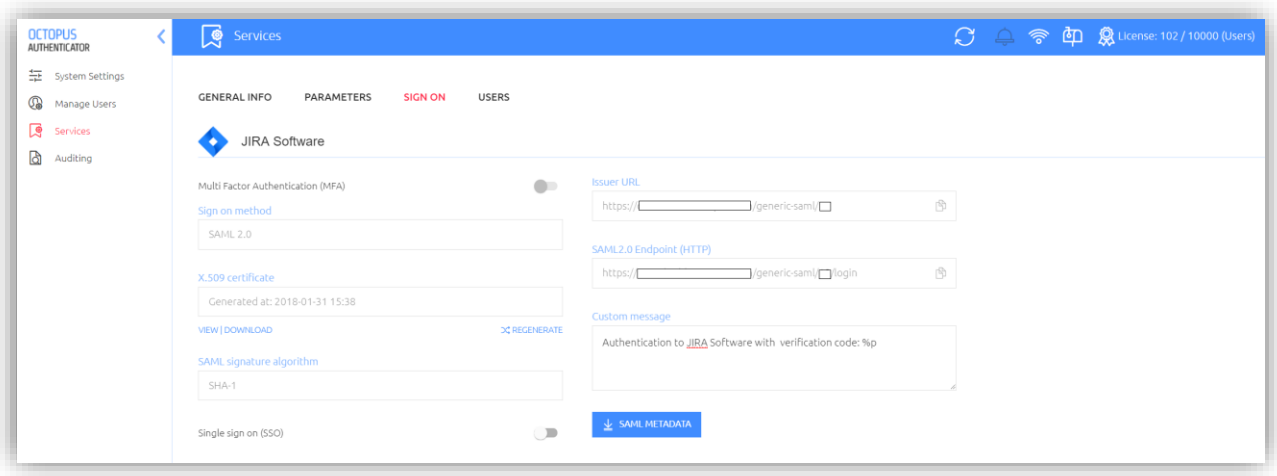
The following field and values are displayed



Field name	Field value
Login	Octopus Authenticator user's login method (email by default)
Name ID	Jira Software user's login method (email by default)
Method	Jira SAML's request binding mechanism (e.g. GET or POST)
ACS URL	Jira Assertion Consumer Service (ACS) URL
Audience	Jira SAML's Single Sign-On SP Entity ID URI
+ Add parameter	Optional

Tab-3: Sign On

The following field and values are displayed

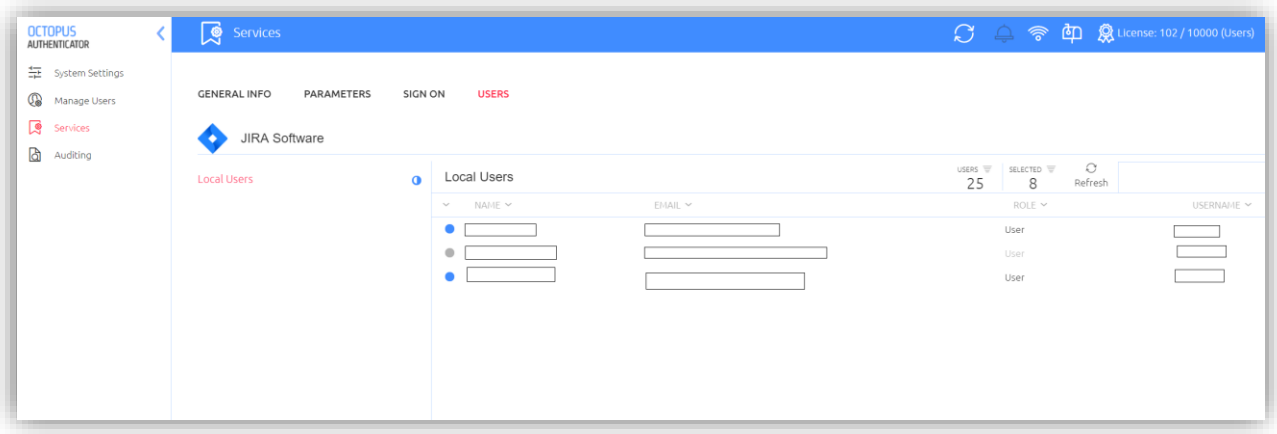


Field name	Field value
Multi Factor Authentication (MFA)	Off (default)
Sign-on Method	SAML 2.0
X.509 Certificate	
SAML signature algorithm	SHA-1 (default)
Single Sign On (SSO)	Off (default)
Issuer URL	https://<Enterprise base URL>/generic-saml/<No.>
SAML 2.0 Endpoint (HTTP)	https://<Enterprise base URL>/generic-saml/login
Custom message	Jira Software authentication request with verification code %p

Note: Secret Double Octopus recommendation is to leave the default field values as displayed.

Step-4: Users

To configure the users of the service



- Select users either from "**Local Users**" or "**LDAP Users**" lists
- You can select either:
    - A group of users to import, by clicking on the dot next to one of the folders
    - An individual user to import, by clicking on the dot next to that user

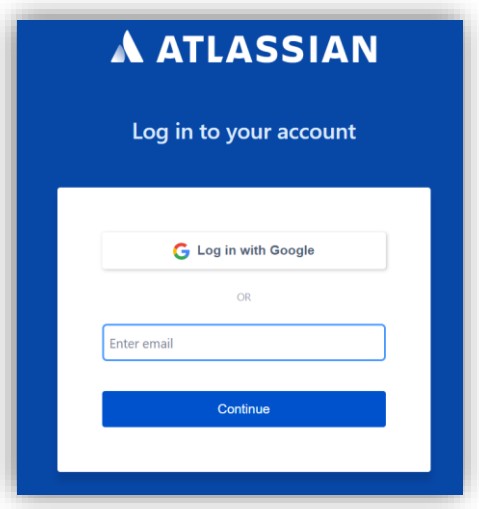
The corresponding dot will then be colored blue. When you select only some of the users in the group, the dot adjacent to the group will be colored partially.

Upon save settings, the selected users will be enrolled in the service.

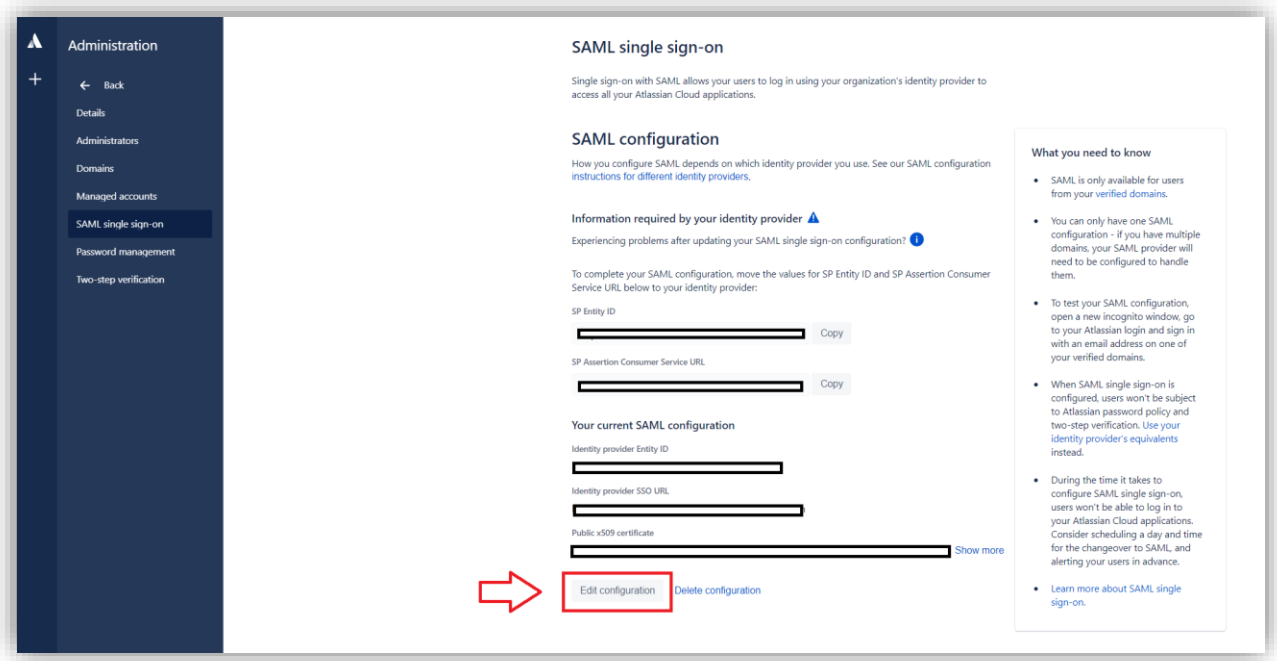
- Click "**Save Settings**"

Set up SSO for Atlassian Using Octopus Authenticator IdP

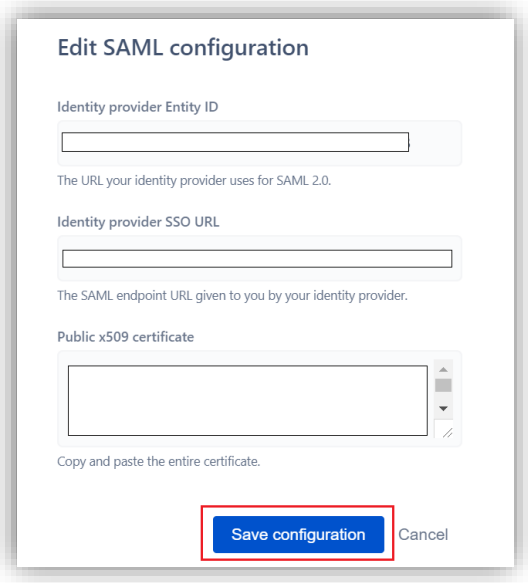
- Login to your Atlassian account as an Administrator



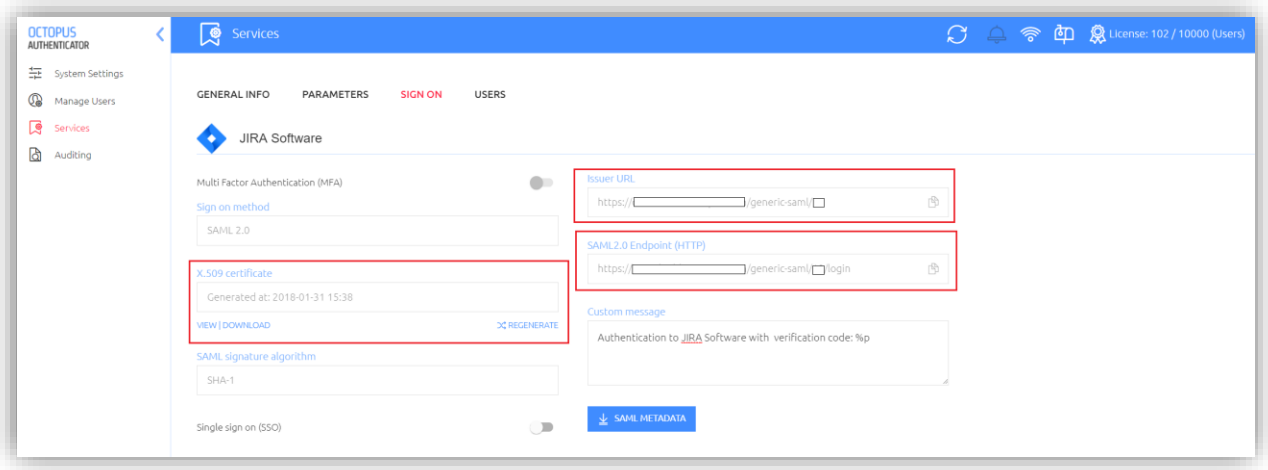
- From Jira "**Administration**" main page, under "**Organization & Security**" category, select "**SAML Single Sign-On**" option



- Click "**Edit Configuration**"

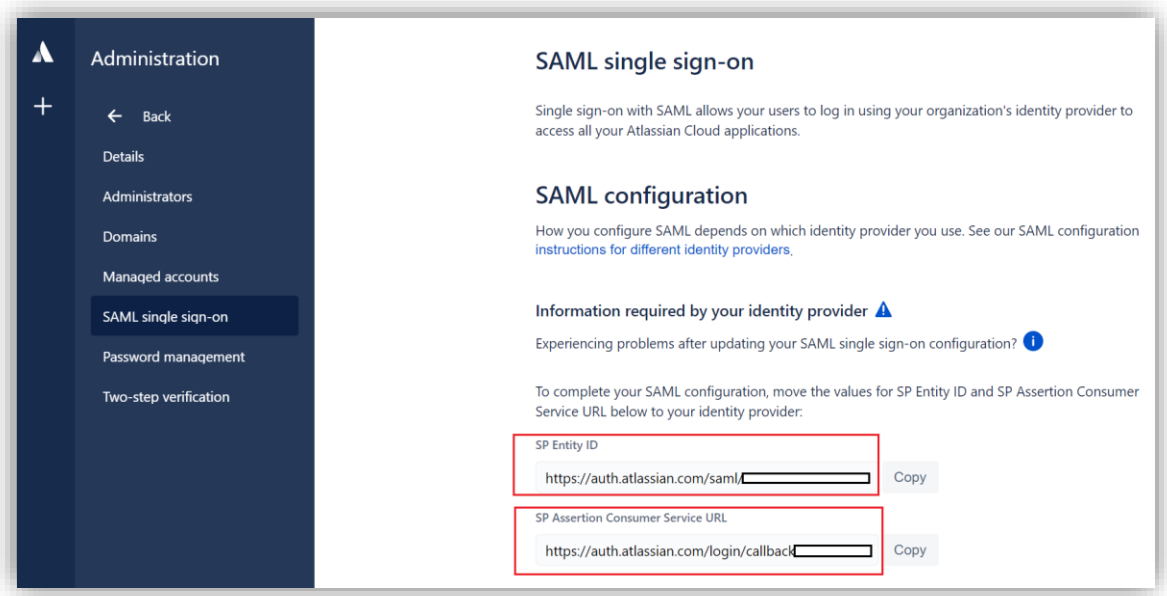


Field name	Field value
Identity Provider Entity ID	The Octopus Authentication Generic SAML → Sign-On → Issuer URL. (e.g. http://<Enterprise base URL>/generic-saml/<No.>)
Identity Provider SSO URL	The Octopus Authentication Generic SAML → Sign-On → SAML 2.0 Endpoint (HTTP) URL. (e.g. http://<Enterprise base URL>/generic-saml/<No.>/login)
Public x.509 certificate	The Octopus Authentication Generic SAML → Sign-On → X.509 Certificate



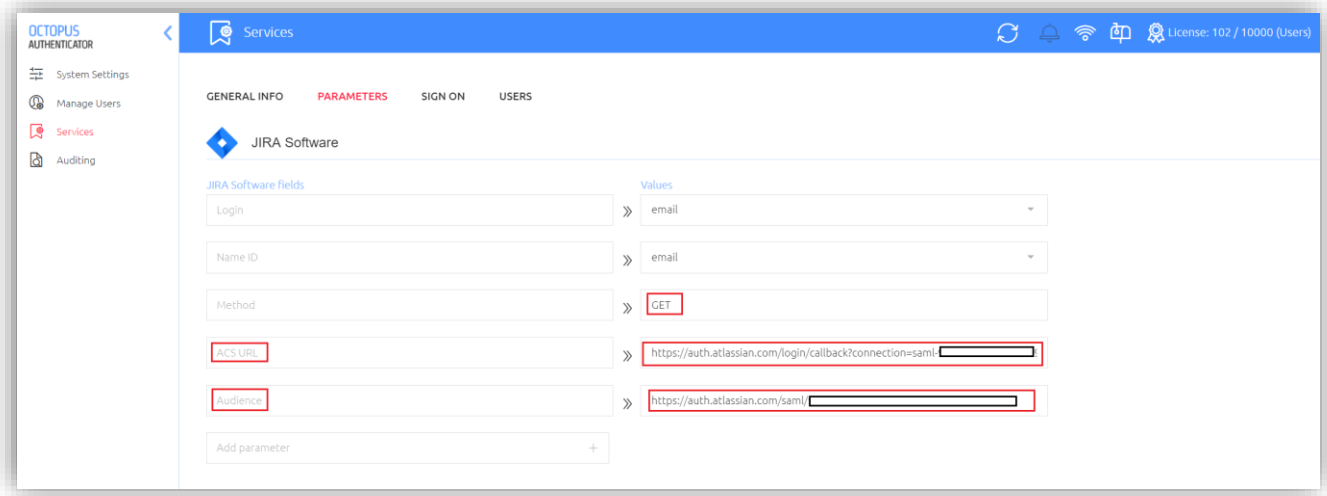
- Click "**Save cofiguration**"

- Upon succssful SAML setup, you will receive your Jira SAML Single Sign-On parameters:
  - SP Assertion Consumer Service URL (also known as ACS URL)
  - SP Entity ID



To complete the Octopus Authenticator and Jira Software SAML Integreation, you will require to configure the two Jira SAML parameters under the Octopus Authenticator Jira Generic SAML → Parameters tab

- Audience Value – Type the Jira SAML Single Sign-On SP Entity ID URI
- ACS URL – Type the Jira SAML Single Sign-On SP Assertion Consumer Service URL



- Click "**Save Settings**"