

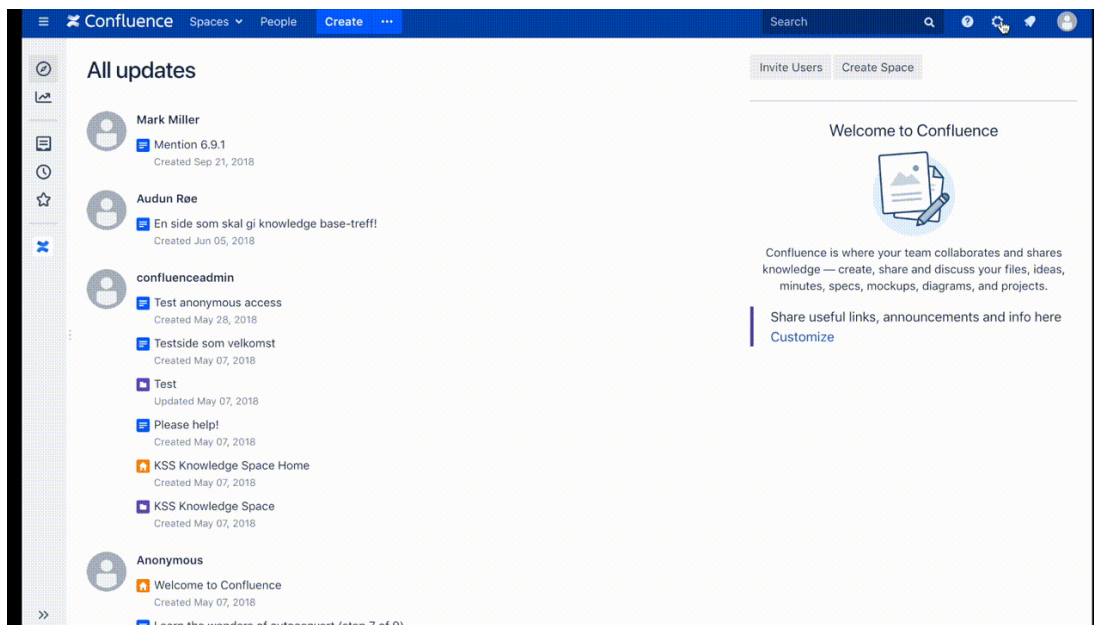
# Salesforce



Setup guide for adding Salesforce login to Atlassian server and datacenter products.

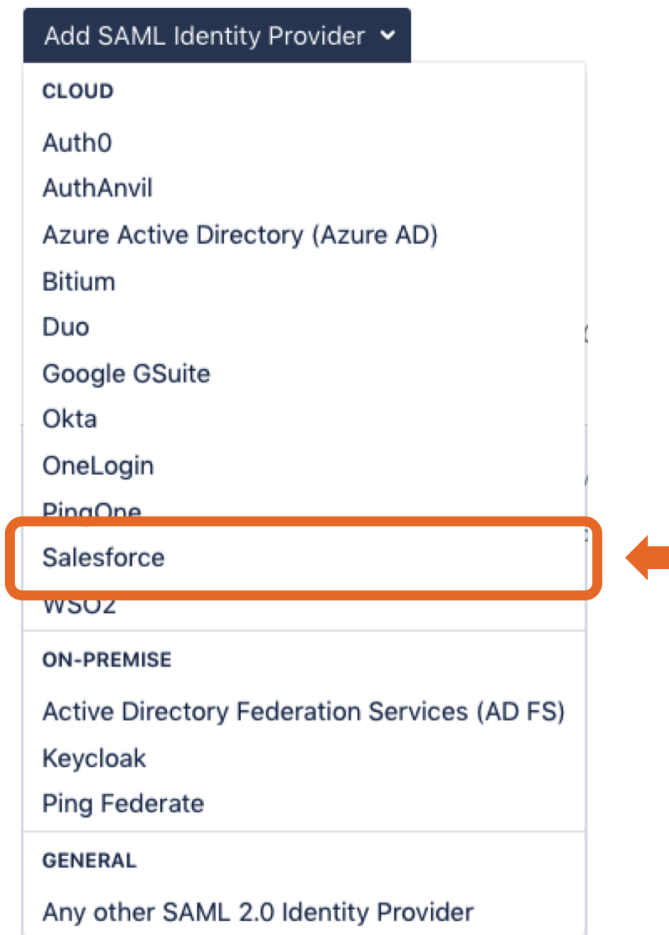
*Context:* This setup guides assumes that [Kantega SSO](#) is installed as an add-on to your Atlassian product ([Jira](#), [Confluence](#), [Bitbucket](#), [Bamboo](#), or [FeCru](#)).

The setup starts in the Configuration page of the Kantega SSO add-on. This configuration page can be found by pressing "**Configure**" on "Kantega Single Sign-On (SSO)" in list of installed add-ons.



## Adding an identity provider

In Kantega Single Sign-on add an identity Provider of the type "Salesforce".



## Prepare

- Copy the ACS URL and Entity ID values and save them for later.

## Add Identity Provider

Prepare

Import

Location

Signature

Users

Summary

### Preparing Salesforce

Follow the step-by-step instructions [here](#) to setup JIRA SSO with Salesforce.

The following information is needed by Salesforce to enable JIRA as a service provider / relying party:

ACS URL  

URL where users return after signing in. Also known as "Assertion Consumer Service URL" or "Login URL"

Entity ID  

Same value as the ACS URL above. Also known as "Destination" or "Receipient".

**Next** [Save draft](#) [Discard](#)

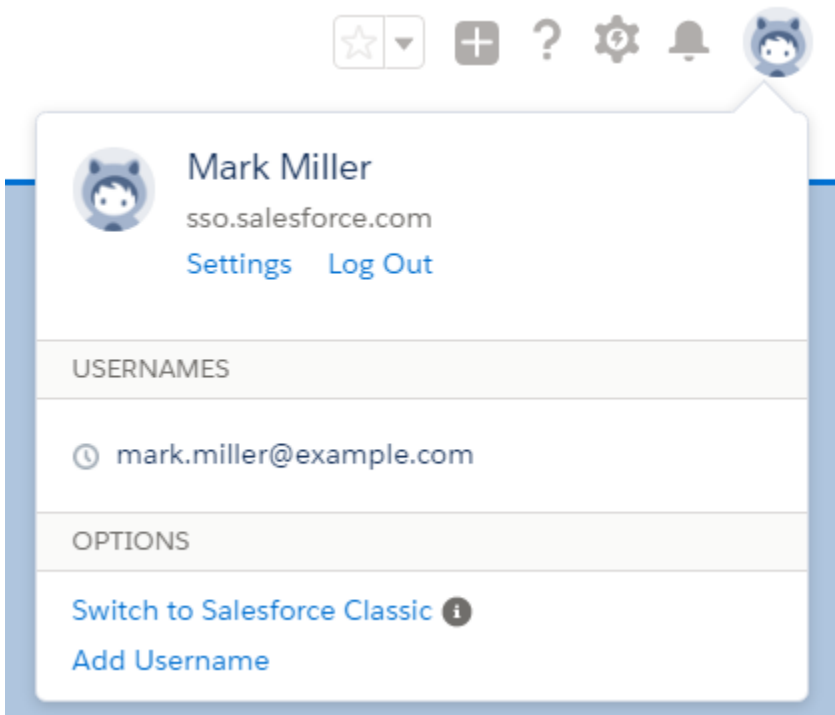
- Click **Next**.

## Adding an app in Salesforce

Our guide uses the Salesforce Classic user interface.

Login to Salesforce as admin. In the upper right corner select your account and Switch to Salesforce Classic

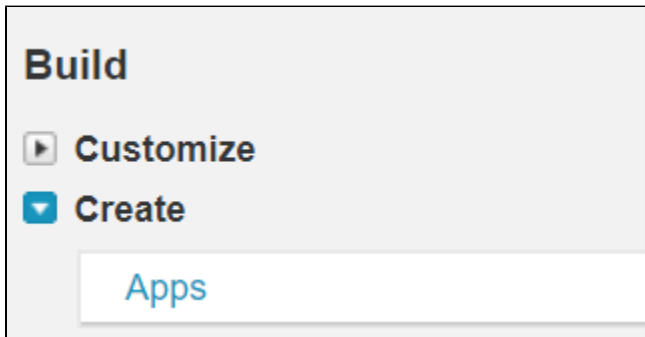
Then select Setup.



The image shows a user profile dropdown menu. At the top, there is a navigation bar with icons for a star, a plus sign, a question mark, a gear, a bell, and a user profile icon. The dropdown menu is open, showing the user's name "Mark Miller" and email "sso.salesforce.com". Below this, there are links for "Settings" and "Log Out". The menu is divided into sections: "USERNAMES" with a search icon and the text "mark.miller@example.com", and "OPTIONS" with links for "Switch to Salesforce Classic" (with an information icon) and "Add Username".

### New Connected App

- Locate Build in the left menu
- Select Create, then Apps



The image shows a "Build" menu. The "Build" header is at the top. Below it, there are two options: "Customize" with a right-pointing arrow icon, and "Create" with a blue square icon containing a white downward-pointing arrow. Below the "Create" option, there is a search bar with the text "Apps" entered.

### Create new Connected App

- Under Connected apps, press New



The image shows a header for "Connected Apps". The text "Connected Apps" is on the left, and a "New" button is on the right.

### Basic Information

- Fill in the required fields

## Basic Information

Connected App Name	<input type="text" value="JIRA"/>
API Name	<input type="text" value="JIRA"/>
Contact Email	<input type="text" value="mark.miller@example.com"/>
Contact Phone	<input type="text"/>
Logo Image URL	<input type="text"/>
	<a href="#">Upload logo image</a> or <a href="#">Choose one of our sample logos</a>
Icon URL	<input type="text"/>
	<a href="#">Choose one of our sample logos</a>
Info URL	<input type="text"/>
Description	<input type="text"/>

## Web App Settings

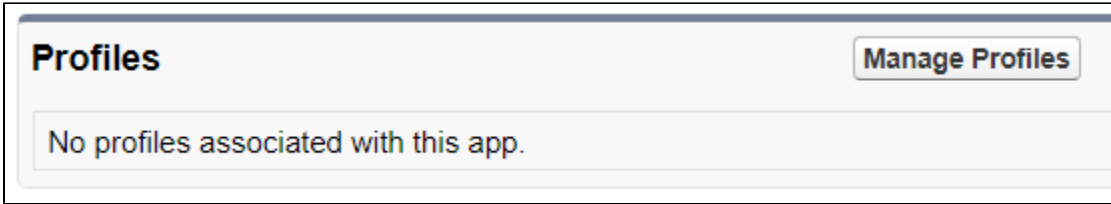
- Select Enable SAML
- From the Prepare step:
  - Fill Entity ID
  - Fill ACS URL
- Press Save, then Manage

## Web App Settings

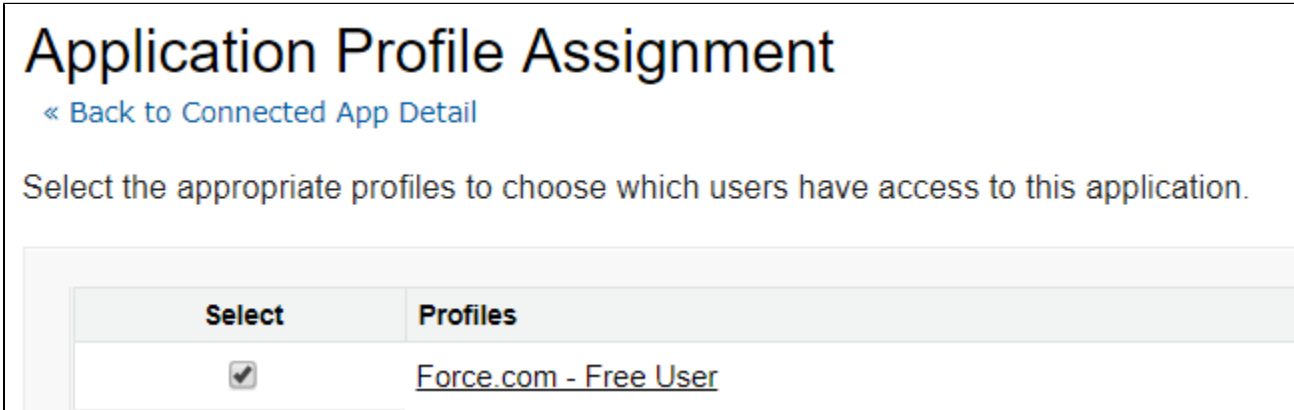
Start URL	<input type="text"/>
Enable SAML	<input checked="" type="checkbox"/>
Entity ID	<input type="text" value="https://issues.example.com/plugins/servlet/no.kantega.saml/sp/10pv"/>
ACS URL	<input type="text" value="https://issues.example.com/plugins/servlet/no.kantega.saml/sp/10pv"/>
Enable Single Logout	<input type="checkbox"/>
Subject Type	<input type="text" value="Username"/>
Name ID Format	<input type="text" value="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"/>
Issuer	<input type="text" value="https://kantegasso-dev-ed.my.salesforce.com"/>
IdP Certificate	<input type="text" value="Default IdP Certificate"/>
Verify Request Signatures	<input type="checkbox"/>
Encrypt SAML Response	<input type="checkbox"/>

## Give permissions

- Select Manage Profiles



- Give users permission to log into the App (In this test we use the profile Force.com - Free User)
- Press Save



## Metadata export

- Under SAML Login Information press "Download the metadata"
- Go back to Kantega Single Sign-on

## Metadata import

- Import the downloaded metadata
- Press Next

## Add Identity Provider

Prepare Import Location Signature Users Summary

### Metadata import

Import metadata using  Metadata file published online

URL to metadata file

Metadata file on my computer

Paste metadata XML from clipboard

[Back](#) [Skip import](#)

### Location

- Give the IDP a proper name
- The SSO redirect URL is imported from the metadata
- Press Next

## Add Identity Provider

Prepare Import Location Signature Users Summary

### Name and SSO location

Identity provider name

Name of the organization providing the user's identity

SSO redirect URL

Imported from metadata

[Back](#)

### Signature

- Review the imported signing certificate (This step is purely informational)
- Press Next

## Add Identity Provider

Prepare Import Location **Signature** Users Summary

### Signature verification

Signing certificate



C=USA, ST=CA, L=San Francisco, O=Salesforce.com, OU=00D0000000sj8J,  
CN=SelfSignedCert\_05Dec2017\_095736

Valid from: Tue Dec 05 10:57:36 CET 2017

Valid to: Wed Dec 05 01:00:00 CET 2018

Sign. alg: SHA256withRSA (2048 bits)

Thumbprint: 88 EC 18 3E 8D 20 68 37 9D 2F 6E 98 DB 59 65 F3 C4 C7 8A FC (SHA-1)

Certificate used to validate SAML messages issued by the identity provider

**Next** Back

## Users

- Select whether users already exist or if you wish to have users automatically created upon login.
  - To automatically create users, Salesforce needs to send a Name and the email in addition to the user name attribute (Not covered in this guide)

## Add Identity Provider

Prepare Import Location Signature **Users** Summary

### User accounts



When logging in SAML users, we must match them with accounts in JIRA

Will accounts pre-exist?  Accounts already exist in JIRA when logging in

Create accounts in JIRA's Internal Directory if needed

When no account is found, we'll create one using the name and email address provided in the SAML attributes

**Next** Back

## Testing/configuring the identity provider

After finishing the wizard, you will be sent to the test pages for verification of your setup. Here, you may also perform the last configuration parts. [Follow this generic introduction to the test pages and final configuration.](#) AD FS is used as the example here.