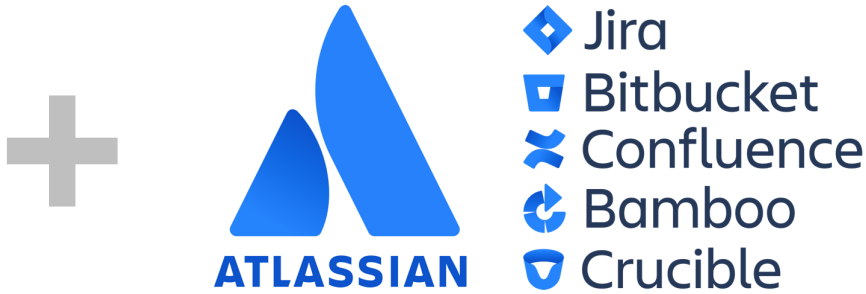


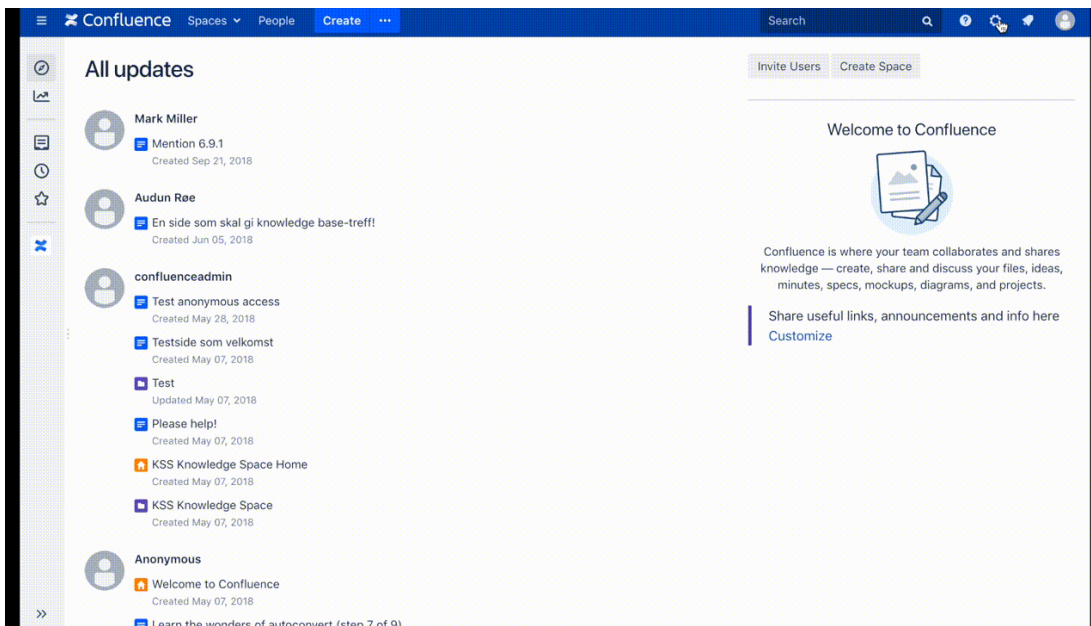
Salesforce



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".

Add SAML Identity Provider ▾

- CLOUD
 - Auth0
 - AuthAnvil
 - Azure Active Directory (Azure AD)
 - Bitium
 - Duo
 - Google GSuite
 - Okta
 - OneLogin
 - PingOne
 - Salesforce**
 - WSO2
- ON-PREMISE
 - Active Directory Federation Services (AD FS)
 - Keycloak
 - Ping Federate
- GENERAL
 - Any other SAML 2.0 Identity Provider



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 "Recipient".

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

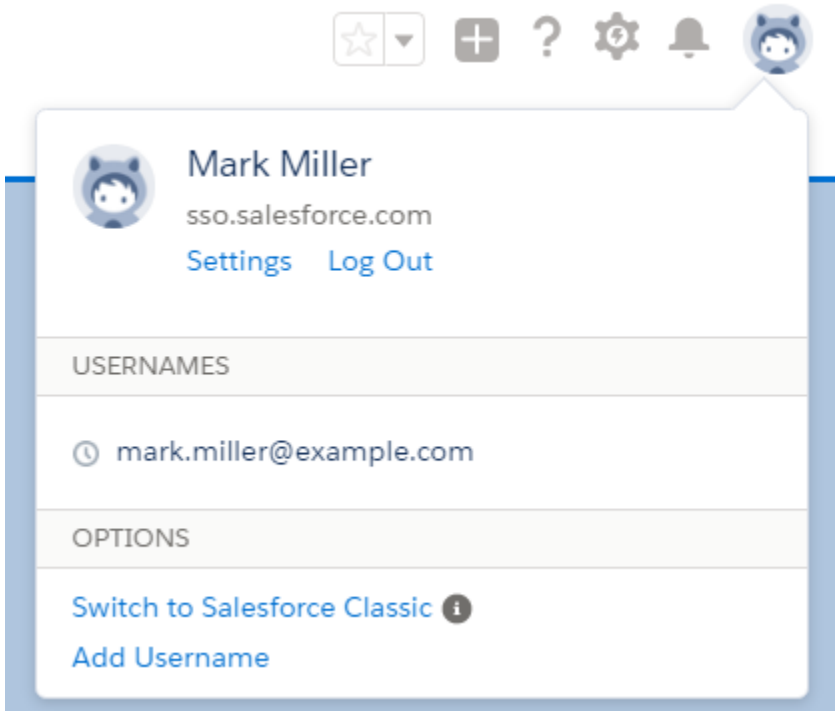
- Click **Next**.

Adding an app in Salesforce

Our guide uses the Salesforce Classic user interface.

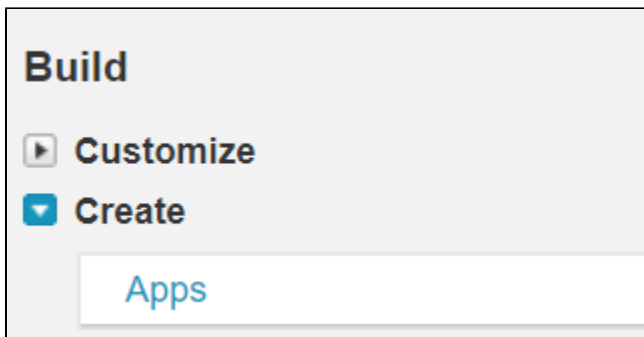
Login to Salesforce as admin. In the upper right corner select your account and Switch to Salesforce Classic

Then select Setup.



New Connected App

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



Create new Connected App

- Under Connected apps, press New




Connected Apps

New

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"/> Upload logo image or Choose one of our sample logos
Icon URL 	<input type="text"/> Choose one of our sample logos
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 


Enable SAML


Entity Id 


ACS URL 


Enable Single Logout 


Subject Type 

Name ID Format 

Issuer 

IdP Certificate 

Verify Request Signatures 

Encrypt SAML Response 

Give permissions

- Select Manage Profiles

Profiles [Manage Profiles](#)

No profiles associated with this app.

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

Application Profile Assignment

[« Back to Connected App Detail](#)

Select the appropriate profiles to choose which users have access to this application.

Select	Profiles
<input checked="" type="checkbox"/>	Force.com - Free User

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

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

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.