

Configure Google Apps

Goto <https://admin.google.com>

Admin console


0 ?

Thanks for choosing G Suite

Welcome to Admin console


[Watch a video](#) to learn about what's new.
Set up G Suite before you begin

START SETUP




Users

Add, rename, and manage users




Company profile

Update information about your company




Billing

View charges and manage licenses




Apps

Manage apps and their settings



Device management

Settings and security for devices



Support

Talk with our support team


Click on Apps

Apps

? :

APPS SETTINGS

Marketplace settings




8

G Suite

Gmail, Calendar, Drive & more

These services are governed by your G Suite agreement.




50

Additional Google services

Blogging, photos, video, social tools and more


These services are not governed by your G Suite agreement, and other terms apply. [Learn more](#)



0

Marketplace apps

[More about Marketplace apps](#)



1

SAML apps

Manage SSO and User Provisioning

Click on SAML apps

Step 1

×

Enable SSO for SAML Application

Select an service/App for which you want to setup SSO

Services

Provisioning supported

Amazon Web Services

>

BlueJeans

>

Box

>

Cigna

>

Citrix GotoMeeting

>

Concur

>

Coupa

>

SETUP MY OWN CUSTOM APP

Select SETUP MY OWN CUSTOM APP

Step 2 of 5



Google IdP Information

Choose from either option to setup Google as your identity provider. Please add details in the SSO config for the service provider. [Learn more](#)

Option 1

SSO URL <https://accounts.google.com/o/saml2/idp?idpid=C016ap3v0>

Entity ID <https://accounts.google.com/o/saml2?idpid=C016ap3v0>

Certificate

 DOWNLOAD

----- OR -----

Option 2

IDP metadata

 DOWNLOAD

PREVIOUS

CANCEL

NEXT

Download IDP metadata, this you will need to enter in the Idp XML Field when configuring the SAML Plugin

Step 4 of 5



Service Provider Details

Please provide service provider details to configure SSO for your Custom App. The ACS url and Entity ID are mandatory.

ACS URL *

Entity ID *

Start URL

Signed Response ☐

Name ID

Name ID Format

PREVIOUS

CANCEL

NEXT

Fill in the URL and Entity ID as configured in the SAML Plugin

Step 5 of 5



Attribute Mapping

Provide mappings between service provider attributes to available user profile fields.

Some providers require you to map application attributes to user fields. You should check the application's documentation to see if this is required. You can always come back later to complete the mapping.

There are currently no mappings for this application

ADD NEW MAPPING

PREVIOUS

CANCEL

FINISH

Click on Finish

Setting up SSO for Bitbucket



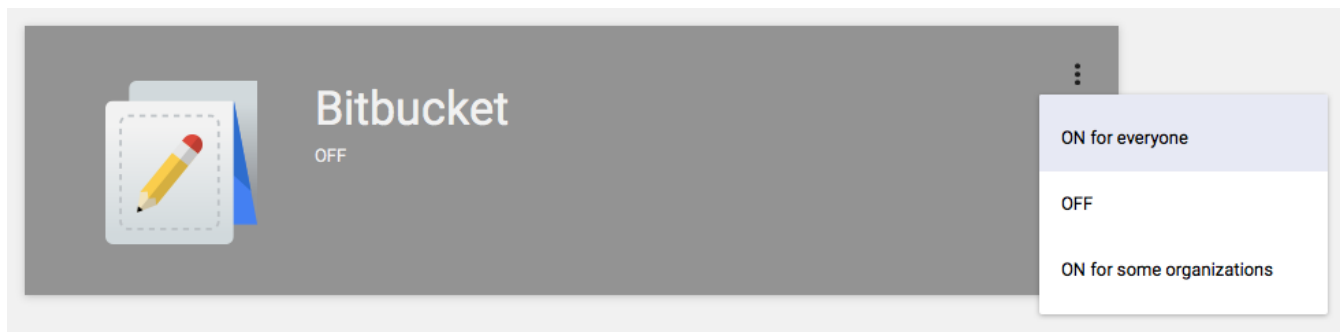
- ✓ Application details saved
- ✓ Mandatory attribute mapping successfully configured



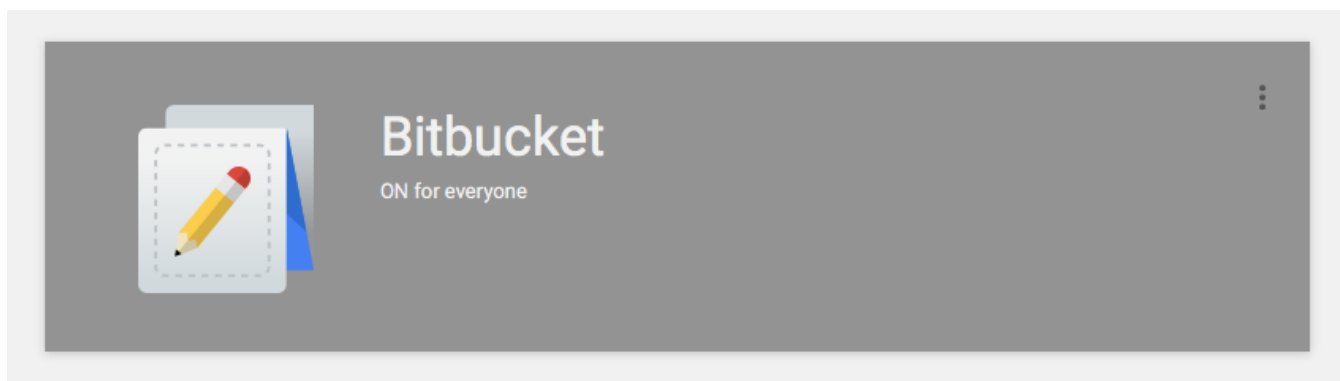
You'll need to upload Google IDP data on Bitbucket administration panel to complete SAML configuration process

OK

Click on OK



Now turn on the SAML for you Organization



Here another example how you can configure the SAML Plugin : with auto provisioning and using the username in JIRA the part before the '@'-sign of the email address of Google Suite

☒ Show the login Button

Show / Hide the login Button

☒ Show the login Button in Service Desk

Show / Hide the login Button in Service Desk

Login Button Title

Login using Google Account

The text which is shown on the Login Button

SAML Endpoint

https://jira.2improveit.eu/plugins/servlet/saml/auth

Use this URL in your IdP to initiate a SAML login

Identity Provider XML

```
<?xml version='1.0' encoding='UTF-8'>
<ds:X509Certificate xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  KriKIJY/GGZ//WjsZHZDlvkqgc+bHoNVhqx+ig1pHuJa5UiGxQIDAQABMA0GCSqGSIb3DQEBCwU
  A
  A4lBAQApOGPf51Yed51a0NMZ3SIstY0nt3XU/OsajNRni0slq6vARY60JVbrU1TvSXZtwITsHuCL
  E62yw9DLiuf97z380E36lRN+44T3+qdg2G+PZkd2iSQJ9hSRNhEkazMzWu0JAjExaEVPJqX6M
  6A
  NgmjC5X5xdRi4DRW03DL4uljc0jzv+3LqjjHCAqKkZw1AwXNOKimOB89r9V/jr4rlwu4clqreG9m
  hVQfCJkkl9lh+Ofrrdnut2wrrl9SoP5LrdqnElf1wnRfTOiTXZNJmZLvpepPIOKbb+ugU0OFBYdx
  hvSzSIKEPa6LrJmHBSaCg42rZNYiMZud2H3vv1uyyt7r</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress</md:NameIDFormat>
<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://accounts.google.com/o/saml2/idp?idpid=C016ap3v0"/>
<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://accounts.google.com/o/saml2/idp?idpid=C016ap3v0"/>
</md:IDPSSODescriptor>
</md:EntityDescriptor>
```

Your Identity Providers metadata.xml

SP Entity ID

https://jira.2improveit.eu

The EntityID that your plugin will use as ServiceProvider

Max. Authentication Age

2592000

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

☐ Force SAML login

If checked, all logins will be made through SAML only. Please test SAML SSO first before checking this box.

☐ Create User

Create User if not exists

SAML User Name Field

NameId.split("@")[0]

SAML User Name Field on creation

SAML User DisplayName Field

first_name + ' ' + last_name

SAML User DisplayName Field on creation

SAML User Email Field

email

SAML User Email Field on creation

SAML User Groups Field

SAML User Groups Field on creation

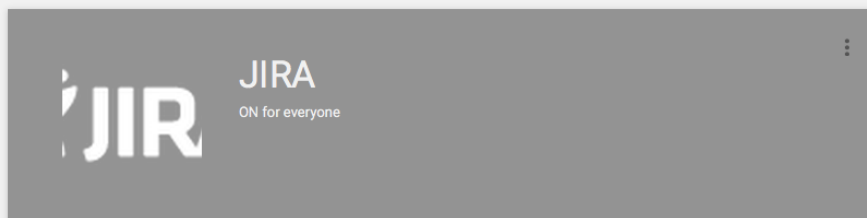
Default Usergroup(s)

Assign the new created Users to these usergroups(s)

☒ Disable Change Password

Disable that a user can change his password

Save



Service Provider Details

Please provide service provider details to configure SSO for JIRA. The ACS url and Entity ID are mandatory.

Application Name	JIRA	app-id: jira
Description	Atlassian JIRA	
ACS URL *	https://jira.2improveit.eu/plugins/servlet/saml/auth	
Entity ID *	https://jira.2improveit.eu	
Start URL	https://jira.2improveit.eu	
Signed Response	<input checked="" type="checkbox"/>	
Name ID	Basic Information	Primary Email
Name ID Format	UNSPECIFIED	

Attribute Mapping

Configure additional parameters that need to be sent to the service provider along with the authentication token

JIRA
ON for everyone

Service Provider Details
Set up basic service provider (SP) details like the ACS URL, entity id and more

^ **Attribute Mapping**

Provide mappings between service provider attributes to available user profile fields.

<input type="text" value="first_name"/>	<input type="text" value="Basic Information"/>	<input type="text" value="First Name"/>
<input type="text" value="last_name"/>	<input type="text" value="Basic Information"/>	<input type="text" value="Last Name"/>
<input type="text" value="email"/>	<input type="text" value="Basic Information"/>	<input type="text" value="Primary Email"/>

ADD NEW MAPPING