

Configure SSO Between redOrange.ai and Google Workspace

Overview

This guide walks you through the process of setting up Single Sign-On (SSO) between redOrange.ai and Google Workspace using SAML 2.0. After configuration, users can log in to redOrange.ai using their Google Workspace credentials.

Prerequisites

- Google Workspace administrator privileges
- redOrange.ai administrator access
- Access to both Google Admin Console and redOrange.ai SSO settings

Step 1: Log in to Google Admin Console

- Go to <https://admin.google.com/> and sign in with your administrator account.

Step 2: Add a Custom SAML App

1. From the Admin console home page, go to **Apps > Web and mobile apps**.
2. Click **Add App > Add custom SAML app**.

Step 3: Configure App Details

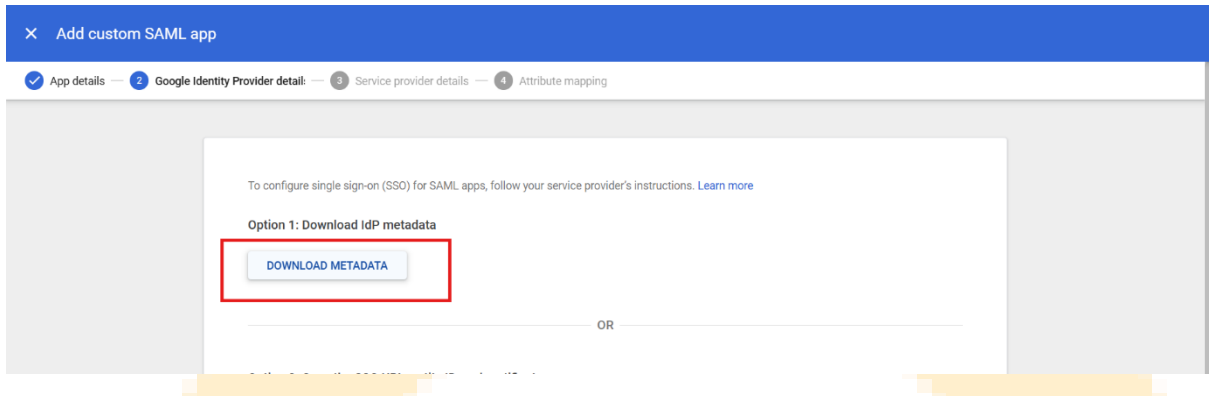
- Enter a name such as **redOrange SSO** and optionally upload a logo.
- Click **Continue**.

The screenshot shows the 'Add custom SAML app' interface in the Google Admin Console. The page has a blue header bar with the title 'Add custom SAML app'. Below the header, there is a white form area with the following sections:

- App details**: A heading followed by the instruction 'Enter details for your custom SAML app. This information is shared with app users. [Learn more](#)'.
- App name**: A text input field containing 'redOrange SSO'.
- Description**: A text input field containing 'Custom SAML Application redOrange AI Application'.
- App icon**: A section with the instruction 'Attach an app icon. Maximum upload file size: 4 MB' and a preview of the redOrange logo.

Step 4: Download Google IDP Metadata

- On the **Google IdP Information** page, download the **IDP metadata** XML file.
- Keep this file handy; you will upload it to redOrange.ai later.
- Click **Continue**.

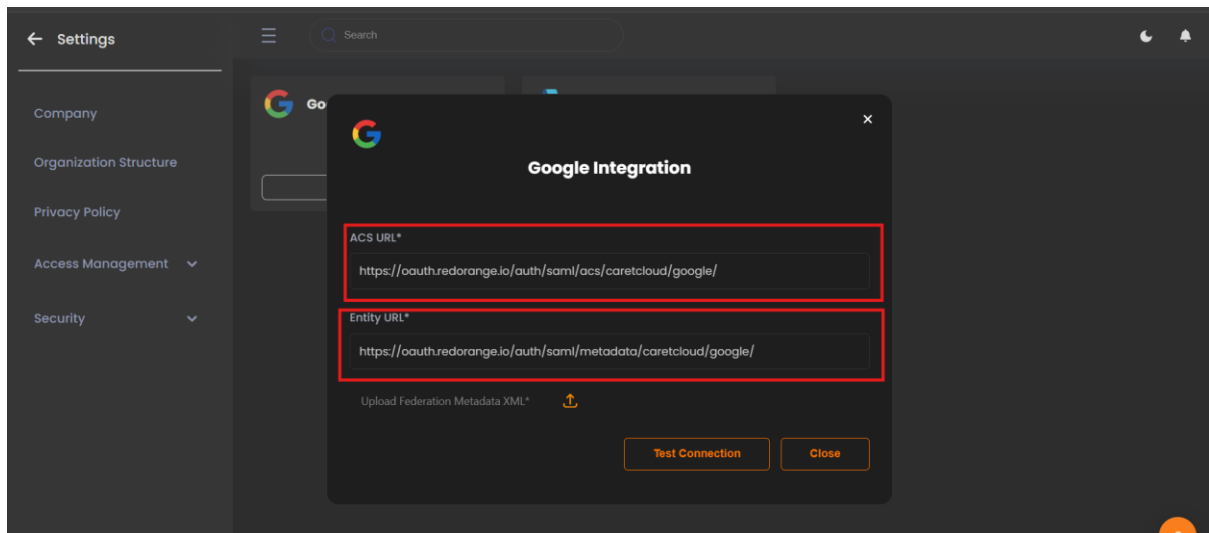


Step 5: Configure Service Provider Details in Google

- On the **Service Provider Details** page, enter the following:

Field	Value
ACS URL	[Obtain from redOrange.ai SSO Settings]
Entity ID	[Obtain from redOrange.ai SSO Settings]
Start URL	(leave blank)
Signed Response	Checked (enable)
Name ID Format	UNSPECIFIED
NAME ID	Basic Information > Primary Email

- Click **Continue**.



✕ Add custom SAML app

ACS URL
https://oauth.redorange.io/auth/saml/acs/carecloud/google/

Entity ID
https://oauth.redorange.io/auth/saml/metadata/carecloud/google/

Start URL (optional)
☒ Signed response

Name ID
Defines the naming format supported by the identity provider. [Learn more](#)

Name ID format
UNSPECIFIED

Name ID
Basic Information > Primary email

BACK CANCEL CONTINUE

Step 6: Attribute Mapping

- Map the following attributes:

Google Directory Attribute	SAML Attribute Name
Primary email	email

- Click **Finish**.

Add custom SAML app

Attributes
Add and select user fields in Google Directory, then map them to service provider attributes. Attributes marked with * are mandatory. [Learn more](#)

Google Directory attributes
Basic Information >
Primary email

App attributes
email

Group membership (optional)
Group membership information can be sent in the SAML response if the user belongs to any of the groups you add here.

Google groups
Search for a group

App attribute
Groups

BACK CANCEL **FINISH**

Step 7: Upload Google IdP Metadata to redOrange.ai

- Log in to redOrange.ai as an administrator.
- Navigate to **Settings > Security > Identity Providers**.
- Click **Add Identity Provider** and select **Google Workspace**.
- Upload the Google IDP metadata XML file you downloaded earlier.
- Click on Test Connection.

Google Integration

ACS URL*

`https://oauth.redorange.io/auth/saml/acs/carecloud/google/`

Entity URL*

`https://oauth.redorange.io/auth/saml/metadata/carecloud/google/`

Upload Federation Metadata XML*

Axia-SSO.xml

redOrangeAI-SSO (2).xml

Successful Google Workspace connected successfully!

Step 8: Test the SSO Setup

- Save all settings in both Google Workspace and redOrange.ai.
- Attempt to log in to redOrange.ai via the SSO login option.
- You should be redirected to Google Workspace for authentication.
- Upon successful login, you will be redirected back to redOrange.ai with access granted.

Step 9: Enable SSO for Your Organization

- In Google Admin Console, ensure the redOrange.ai SAML app is turned **ON for everyone** or for the desired organizational units.
 - Communicate the new login process to your users.
-

Additional Tips

- Ensure that user email addresses in Google Workspace exactly match the email addresses of redOrange.ai user accounts for proper SSO authentication.
 - Review user role assignments in redOrange.ai after provisioning via SSO.
-

Support

For further assistance, contact:

- Email: support@redorange.ai

