Example: Setup of Aras Innovator SAML 2.0 Authentication with Azure as Identity Provider

This section provides an example of configuring a deployment to log in to Aras Innovator using an external user and the SAML2 protocol. For this Deployment, logging in using a Google account will be configured.

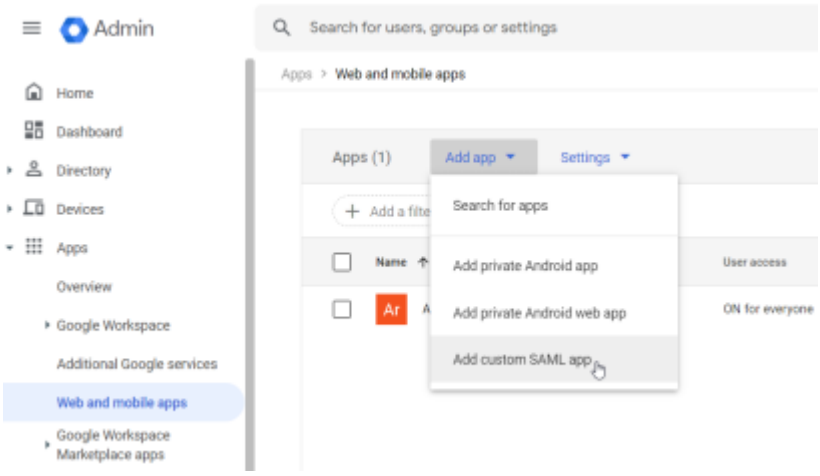
The following sections outline the process of configuring external authentication.

Configure external identity provider (e.g. add app registry)

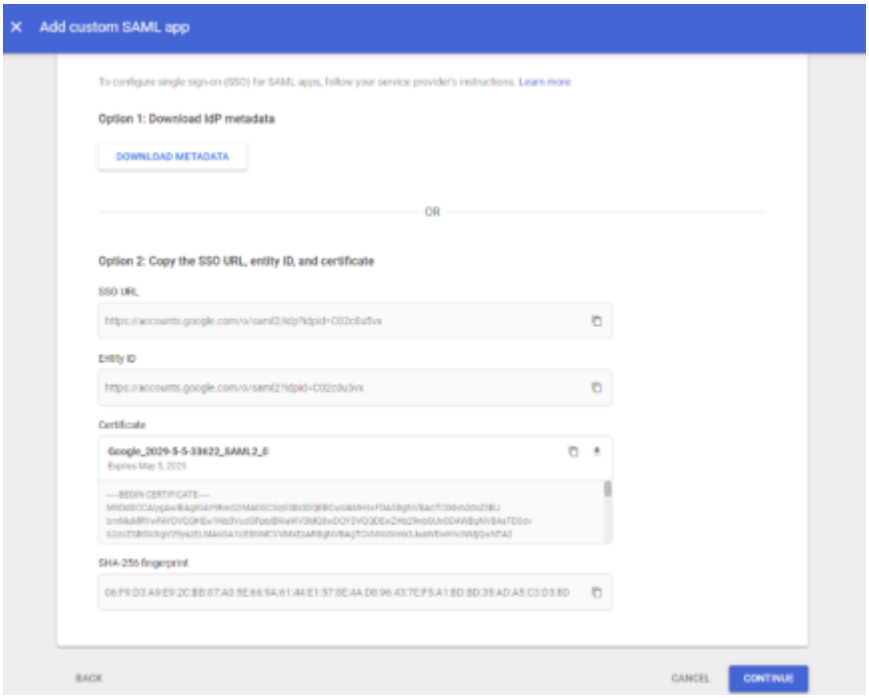
For more details, refer to the manual: https://support.google.com/a/answer/6087519 .

The following steps outline the process of configuring the external identity provider:

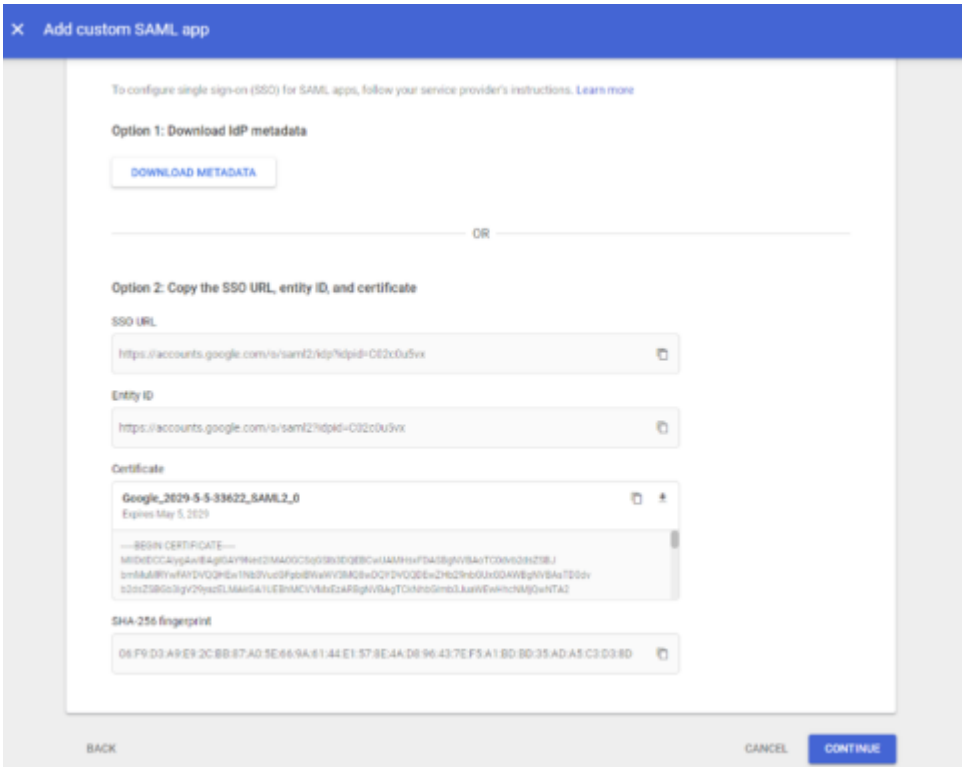
1. Ensure there is a Google admin account on admin.google.com . The e-mail should be of the domain which will be used as the Service provider (Aras Innovator). For example, if the instance is https://domain.com/instance/, the e-mail should be username@domain.com.
2. Log into https://admin.google.com/ .
3. From the left pane, Go to **Apps** and click **Web and mobile apps**.
4. Click **Add app**, then select **Add custom SAML Apps**.



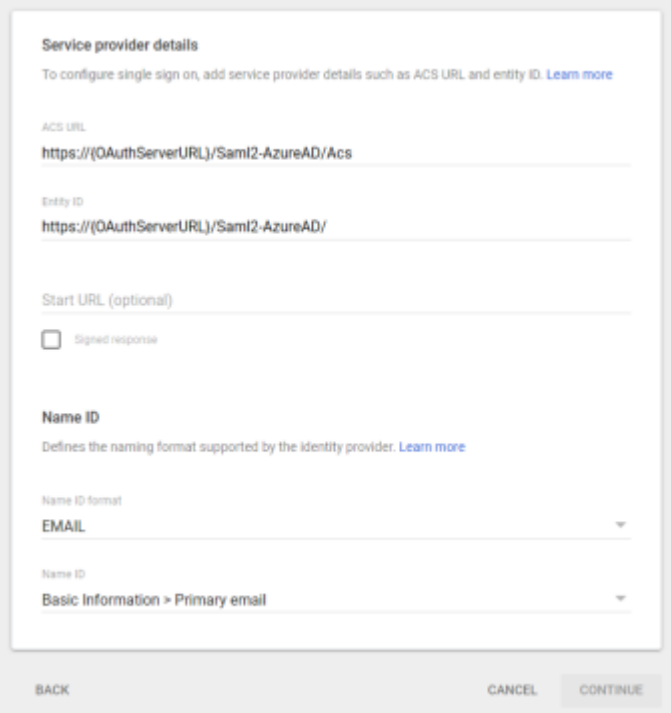
5. Fill in the **App** details.



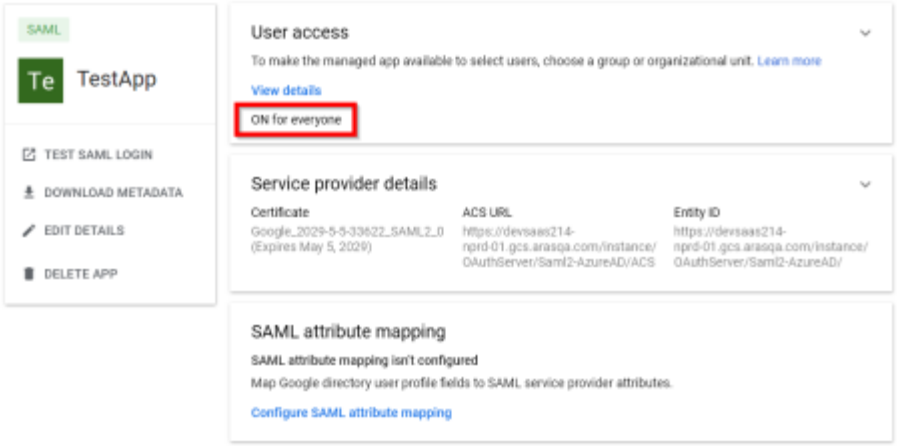
6. Click the **Continue** button.
7. Download metadata on the computer and copy **EntityId** (download the signing certificate, if required).



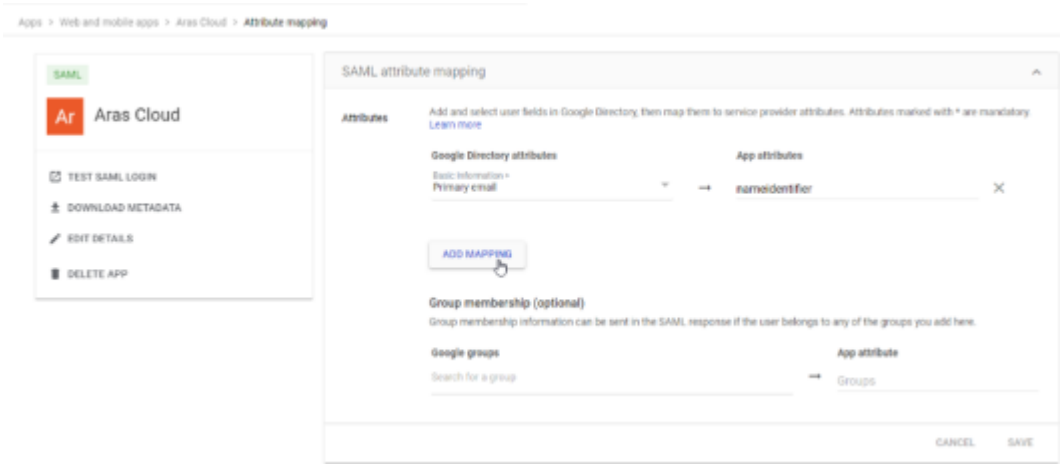
8. Click the **Continue** button.
9. Enter the **ACS URL** for the instance. For example, https://{OAuthServerURL}/Saml2-AzureAD/Acs.
10. Enter **Entity ID** for the instance. For example, https://{OAuthServerURL}/Saml2-AzureAD/.



11. Click the **Continue** button and save.
12. Click **Apps**, click on **Web and mobile apps**, and check if user access is **ON for everyone**.



13. Click **Add Mapping** and change mapping options to receive the correct claim after logging into Google.



14. Go to the **Home** Tab, and in the **Users** section, assign users to log in.

Refer to the following Microsoft link about configuring Azure as an identity provider: https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/add-application-portal-setup-sso .

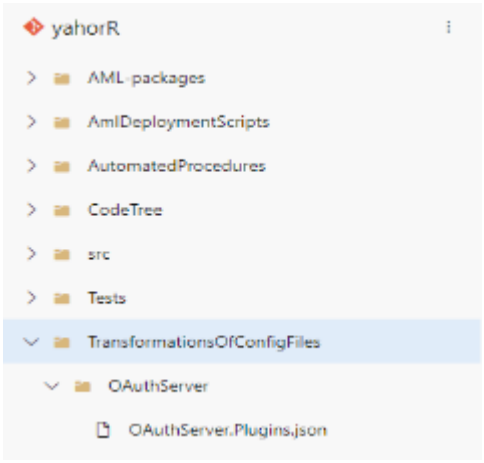
Add transformation for Aras.OAuth.Server.Plugins.Saml2Authentication plugin and for Aras.OAuth.Server.Plugins.GenericUserMapper plugin.

To turn on Aras Innovator SAML 2.0 Authentication, update the **OAuthServer.Plugins.json** settings with the Transformation mechanism using JDT Transformation.

The readme file in the TransformationsOfConfigFiles folder of the Work Repository in Azure DevOps contains more information.

The values of the required parameters can be obtained from the Configure external identity provider section.

The OAuthServer.Plugins.json file must be added to TransformationsOfConfigFiles/OAuthServer of the Repository.



The file should contain the JDT Transformation of the configuration of **Aras.OAuth.Server.Plugins.Saml2Authentication** and **Aras.OAuth.Server.Plugins.GenericUserMapper** plugins.

The following is an example of JDT Transformation using OAuthServer.Plugins.json file:

```
{
    "@jdt.merge": {
        "@jdt.path": "$.['OAuthServer.Plugins']",
        "@jdt.value": [
        {
            "Name": "Aras.OAuth.Server.Plugins.Saml2Authentication",
            "Enabled": true,
            "Options": [
                {
                    "AuthenticationType": "Saml2-AzureAD",
                    "DisplayName": "Saml2 Google",
                    "ServiceProviderOptions": {
                        "EntityId": "https://{OAuthServerURL}/Saml2-AzureAD/"
                    },
                    "IdentityProviderOptions": {
                        "EntityId": "https://accounts.google.com/o/saml2?idpid=C02c0u5vx",
                        "MetadataSource": "MetadataLocation",
                        "MetadataLocation": "/secure_files/sit_GoogleIDPMetadata.xml"
                    }
                }
            ]
        },
        {
            "Name": "Aras.OAuth.Server.Plugins.GenericUserMapper",
            "Enabled": true,
            "Options": [
                {
                    "AuthenticationType": "Saml2-AzureAD",
```

```
                    "InnovatorUserNameFormat": "{username}",
                    "ClaimActions": [
                        {
                            "ActionName": "CreateFrom",
                            "ActionOptions": {
                                "ClaimType": "username",
                                "SourceClaimType": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims
                                "ReplacePattern": "@.+",
                                "Replacement": "",
                                "PatternOptions": [ "IgnoreCase", "Singleline" ]
                            }
                        },
                        {
                            "ActionName": "Validate",
                            "ActionOptions": {
                                "ClaimType": "username",
                                "AllowPattern": ".+",
                                "DenyPattern": "^admin$|^root$|^vadmin$|^authadmin$|^esadmin$",
                                "PatternOptions": [ "IgnoreCase", "Singleline" ]
                                }
                        }
                    ]
                }
            ]
        }
        ]
    }
}
```

This Transformation of the **Saml2Authentication** plugin describes the basic minimum flow with metadata as a file and EntityId as a URL. The EntityId of the ServiceProviderOptions should contain a URL to the Saml2-AzureAD endpoint of OAuthServer. The EntityId and metadata file should be configured based on information provided by **identityProvider**.

More information about SAML configuration can be found in the SAML2 Authentication Plugin Configuration section.

This Transformation of the **Generic User Mapper** plugin signifies that the value received from the Identity provider (in this case, e-mail) will be transformed in the **CreateFrom** action, cutting out everything after and including the @ symbol. The Validate section will check if the resulting value equals the username that exists in Aras Innovator and pass the user to the Authentication plugin to authenticate.

1. **Important**

   Since the username field in Aras Innovator is limited by the number of symbols, mapping should consider this limitation.

Refer to the Generic User Mapper section for more information about **Generic User Mapper** configuration.

The above example demonstrates one of the basic SAML2 flows using a file configuration of EntityId and Metadata.

Following SAML2 flows are also supported:

- Configuration with URLs to an external provider.
- Configuration with external files, such as certificates and metadata files.

For more details about configuration with external files, refer to the Configuring Secure Files section.

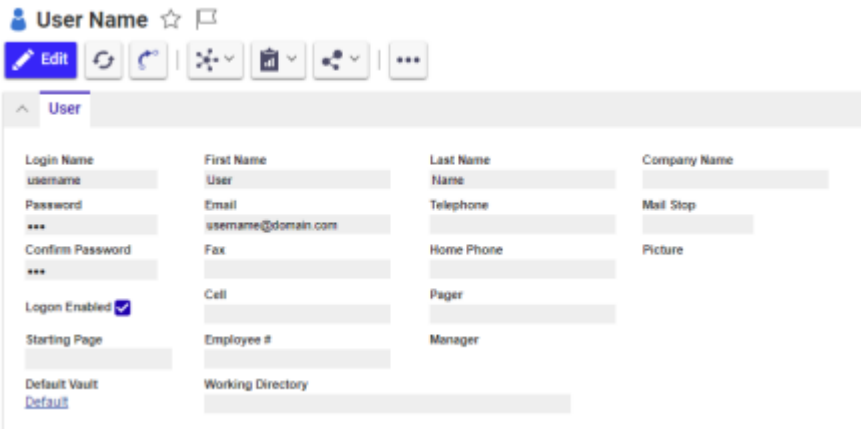
Commit Changes and Run Pipeline

Once all the changes are complete, commit the changes, run the CI Pipeline, and deploy the Pipeline.

Create a User for Corresponding Mapping

Login to the Aras Innovator instance as an administrator and create a user according to the mapping strategy. For example:

The Login Name will be the username of the e-mail address, which is the prefix of @.

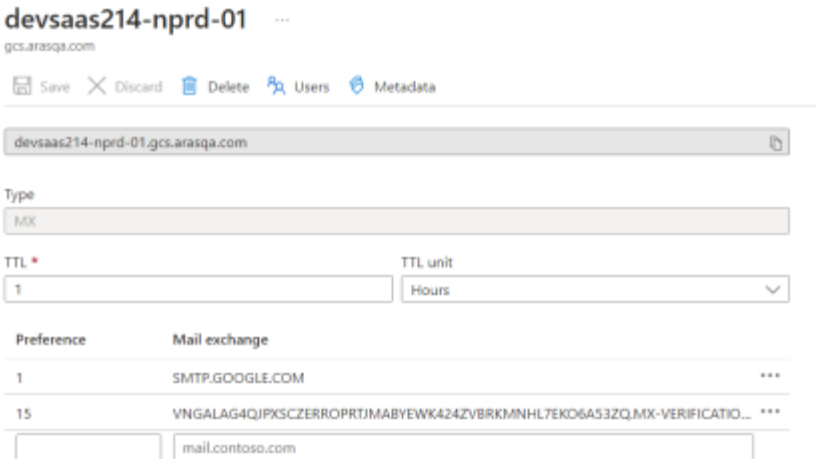


Configure access to the external identity provider (e.g., DNS settings)

If Google requests domain verification, please follow the provided instructions.

The following steps outline the process of configuring the communication between Google and the domain:

1. Open domain settings in admin.google.com and fill in the required properties. For more details, see the Configure External Identity Provider section.
2. Open the Azure portal DNS settings and follow the Google instructions about adding MX records for the domain to make the domain verified. Two records were added to DNS settings.



3. Continue verification in admin.google.com .

After following all the above steps, the login should be successful. For more details, refer to the SAML2 Authentication Plugin Configuration section.