IUCLID Configuration for SAML-Based SSO with Azure Active Directory

IUCLID 6
ECHA
EUROPEAN CHEMICALS AGENCY
OECD
IUCLID 6 is developed by the European Chemicals Agency in association with the OECD

Legal Notice

The information in this document does not constitute legal advice. Usage of the information remains under the sole responsibility of the user. The European Chemicals Agency does not accept any liability with regard to the use that may be made of the information contained in this document.

Title: IUCLID Configuration for SAML-Based SSO with Azure Active Directory

Issue date: August 2023

Language: en

IUCLID 6 is developed by the European Chemicals Agency in association with the OECD.

© European Chemicals Agency, 2023

Reproduction is authorised provided the source is fully acknowledged in the form

“Source: European Chemicals Agency, http://echa.europa.eu/”, and provided written notification is given to the ECHA Communication Unit (publications@echa.europa.eu).

If you have questions or comments in relation to this document, please send them to ECHA via the information request form at the address below, quoting the reference and issue date given above:

https://echa.europa.eu/contact

European Chemicals Agency

Mailing address: P.O. Box 400, FI-00121 Helsinki, Finland

Visiting address: Telakkakatu 6, Helsinki, Finland

Changes to this document

Date	Modification
23/08/2023	Chapter 4.3: updated the configuration to enable SSO in IUCLID moving specific parameters from <jvm-options> to <system-property>
01/11/2022	Removed ending slash from the values of Identifier (Entity ID) and Reply URL Added extra configuration step to make sure Reply and Assertion are both signed. Added Sign-on URL config option to support IUCLID access through MS application directory.
26/04/2022	First public release.
12/01/2022	First version.

Table of Contents

Table of Figures

1. Introduction

The purpose of this document is to provide instructions regarding the configuration of the IUCLID application, for SAML-based Single Sign On (SSO) with Azure Active Directory acting as an external identity provider (IDP).

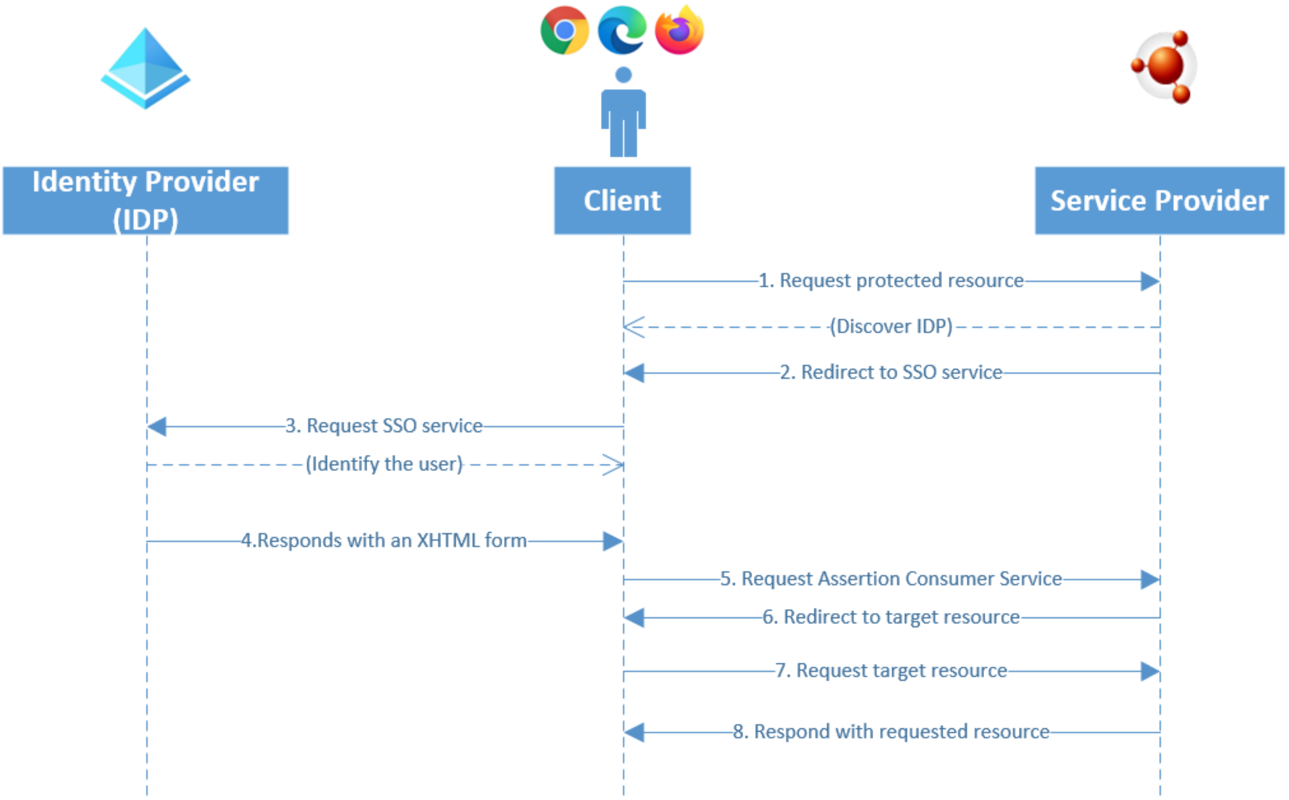
A successful integration of IUCLID with an external identity provider via SSO requires the collaboration between business and IT units of your organisation. They should work together to review existing authorisation policies both at organisation level and at IUCLID level. These policies should be reviewed to capture a streamlined configuration that's reflects the desired access to data and actions in IUCLID.

1.1. About SAML

Security Assertion Markup Language (SAML) is an open standard for exchanging authentication and authorization data between parties: an identity provider and a service provider.

The single most important use case that SAML addresses is single sign on (SSO) via a web browser. A user employs a user agent, usually a web browser, to request a web resource that is protected by a SAML service provider. The service provider, wishing to know the identity of the requesting user, issues an authentication request to a SAML identity provider through the user agent. The resulting protocol flow is depicted in the following diagram:

Figure 1: The protocol for Identity Provider (IDP) and Service Provider in Single Sign On (SSO)


Identity Provider (IDP)
Client
Service Provider
1. Request protected resource
(Discover IDP)
2. Redirect to SSO service
3. Request SSO service
(Identify the user)
4.Responds with an XHTML form
5. Request Assertion Consumer Service
6. Redirect to target resource
7. Request target resource
8. Respond with requested resource

Note: In this document the IUCLID application acts as the SAML service provider (above right), and Azure Active Directory has the role of the SAML identity provider (above left). The client in the middle of the above diagram is the user acting from a web browser.

The SAML standard defines a set of XML-based messages for security assertions:

- SAML Request, example fields: ID, Issuer, Assertion consumer URL
- SAML Response, example fields: ID, Issuer, In response to (ID), Recipient, Subject

The SAML messages are signed and potentially encrypted.

1.2. Mapping Azure Active Directory user data to IUCLID user data

The authentication and authorisation setup of IUCLID is built upon 4 main concepts:

- **Legal entities**: Several legal entities can be assigned to a user, however, when logged in, only one legal entity can be the user's *working legal entity*. This working legal entity is passed to the entities the user creates, e.g. substances, mixtures.
- **Roles**: Each role includes a set of permissions that determine the actions users can perform (read, write, delete) with each type of entity (substance, mixtures, dossiers, etc.) or inventory (reference substances, legal entities, etc.). Special permissions are included for general operations (print, export, import) and for system administration.
- **Security groups**: If Instance Based Security (IBS) is enabled, access is defined per individual entity, and can also be limited to the users belonging to certain security groups.
- **Users**: Per user, IUCLID stores the basic user information (username, first name, last name, etc.), and also the legal entities, roles, and security groups assigned to the user.

For more information about these concepts, refer to the document: Functionalities of IUCLID in the web interface.

The maintenance of user information can be delegated from IUCLID to an external identity provider (IDP), like Azure Active Directory, that supports Single Sign On (SSO) using the SAML standard. Thus, a centralised system can hold the user information, including the password. However, the data objects that will be assigned to users must first exist in IUCLID, e.g. IUCLID Roles, IUCLID Security Groups, and IUCLID Legal entities.

The main objects which need to be managed in Azure Active Directory are:

- **Users**: The user object contains information about the individual including password and logon credentials.
- **Groups**: Groups are primarily used for the purpose of managing and securing groups of users. Groups can also be used for representing different access rights of users in different systems of an organization.

Users are created in Azure Active Directory (AD) and they are assigned to different Azure AD Groups. An Azure AD user will correspond to a IUCLID user.

During configuring SSO in IUCLID it is possible to do the following mappings:

- Azure AD Groups -> IUCLID Roles
- Azure AD Groups -> IUCLID Security Groups (only if IBS is enabled in IUCLID)

- Azure AD Groups -> IUCLID Legal Entities

Different strategies can be applied when defining Azure AD Groups and IUCLID Roles/Security Groups/Legal Entities:

- One-to-one mapping: One Azure AD Group can correspond to a single IUCLID Role/Security Group/Legal Entity
- One-to-many mapping: One Azure AD Group can correspond to multiple IUCLID Roles/Security Groups/Legal Entities
- Combination of the above

After a successful authentication with a 3rd party SAML IDP provider, the IUCLID application updates the user information in its local database, and assigns the user to the relevant IUCLID Roles, IUCLID Security Groups, and IUCLID Legal entities.

2. Prerequisites

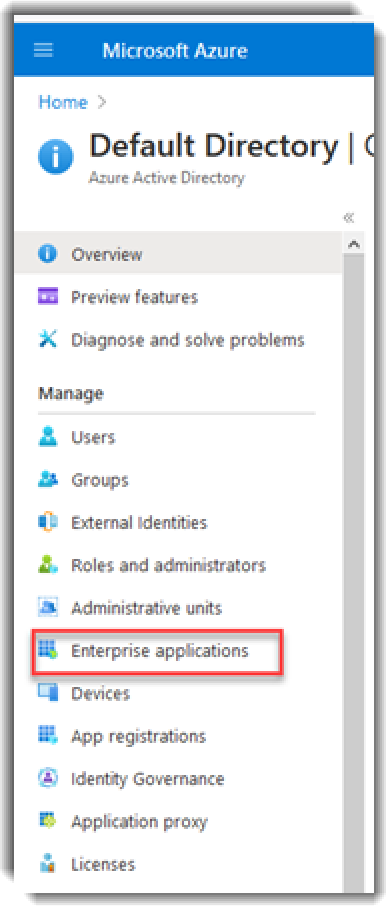
IUCLID 6 v6 is installed successfully. If you want to define IUCLID security groups in your SSO configuration Instance Based Security needs to be manually enabled during the installation process. See Installation and Update Instructions for IUCLID6 Server for details.

Azure Active Directory is available.

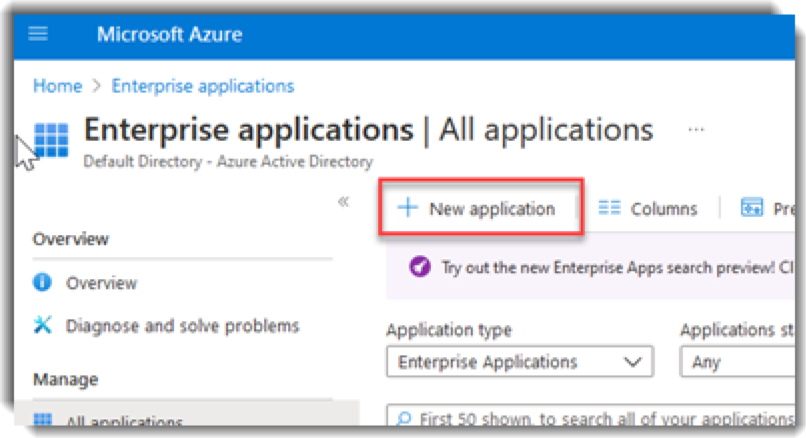
3. Configuring Azure Active Directory

3.1. Add the IUCLID application to the Azure AD tenant

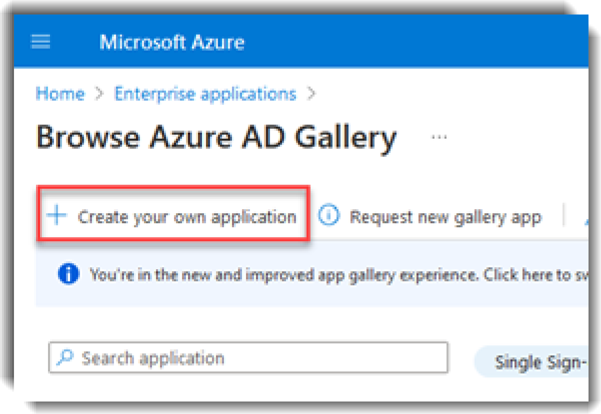
In the Azure AD portal, select *Enterprise applications*.



Click on *New application*.


Microsoft Azure
Home > Enterprise applications
Enterprise applications | All applications ...
Default Directory - Azure Active Directory
+ New application
Columns
Pre
Try out the new Enterprise Apps search preview! Cl
Application type
Enterprise Applications
Applications st
Any
Overview
Overview
Diagnose and solve problems
Manage
All applications
First 50 shown, to search all of your applications

Click on *Create your own application*.



Microsoft Azure

Home > Enterprise applications >

Browse Azure AD Gallery ...

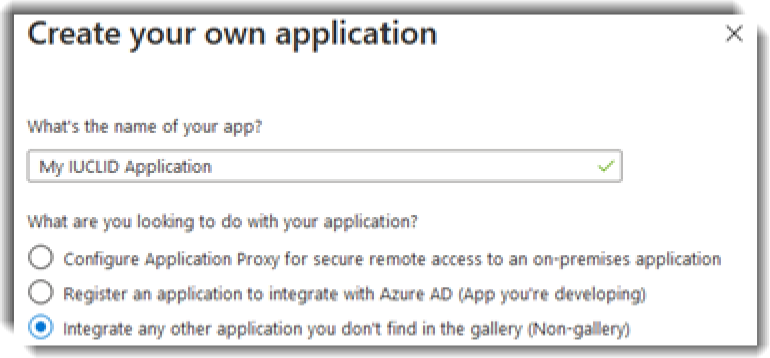
+ Create your own application | ⓘ Request new gallery app

ⓘ You're in the new and improved app gallery experience. Click here to sw

Search application | Single Sign-

Enter the application name and select the option:

Integrate any other application you don't find in the gallery (Non-gallery).



Create your own application

What's the name of your app?

My IUCLID Application ✓

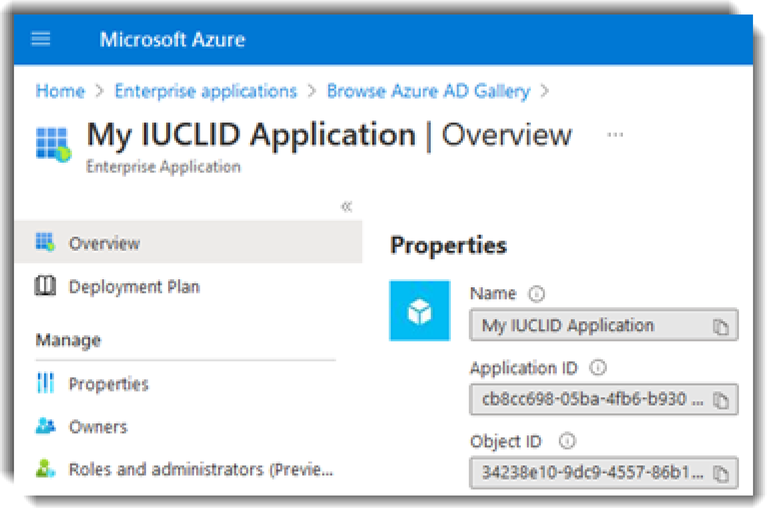
What are you looking to do with your application?

○ Configure Application Proxy for secure remote access to an on-premises application

○ Register an application to integrate with Azure AD (App you're developing)

● Integrate any other application you don't find in the gallery (Non-gallery)

The application is created.



Microsoft Azure

Home > Enterprise applications > Browse Azure AD Gallery >

My IUCLID Application | Overview ...

Enterprise Application

Overview

Deployment Plan

Manage

Properties

Owners

Roles and administrators (Previe...

Properties

Name ⓘ

My IUCLID Application

Application ID ⓘ

cb8cc698-05ba-4fb6-b930 ...

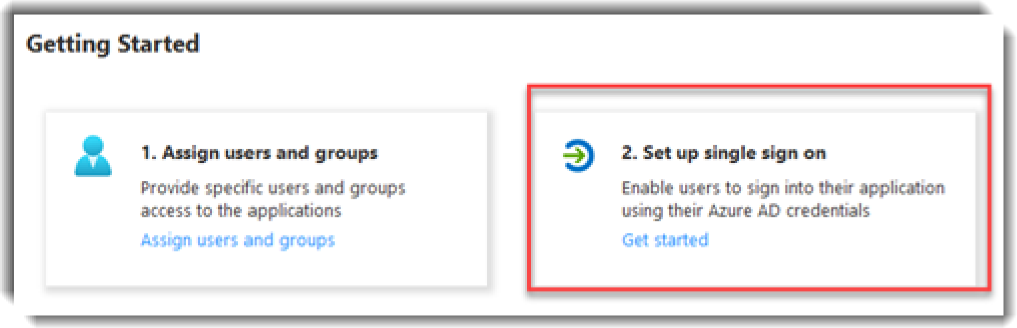
Object ID ⓘ

34238e10-9dc9-4557-86b1...

3.2. Set up SAML-based SSO for IUCLID in the Azure AD tenant

In the Azure AD portal in the overview page of the newly created application:

Click on *Set up single sign on*.

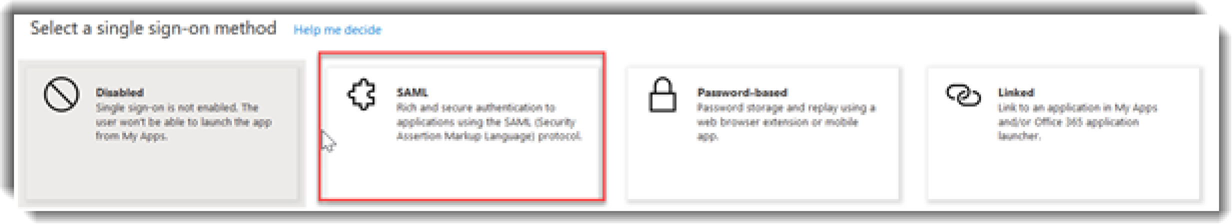


Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
Get started

Select the single sign on method *SAML*.



Select a single sign-on method Help me decide

Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

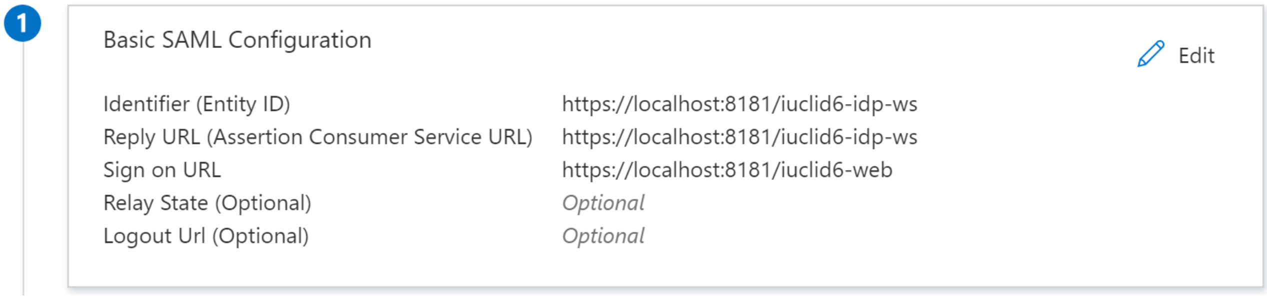
SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based
Password storage and replay using a web browser extension or mobile app.

Linked
Link to an application in My Apps and/or Office 365 application launcher.

Set up Single Sign-On with SAML:

- Basic SAML configuration:
  - Identifier (Entity ID): *https://<IUCLID URL>/iuclid6-idp/ws*
    E.g.: `https://localhost:8181/iuclid6-idp-ws`
  - Reply URL (Assertion Consumer Service URL): *https://<IUCLID URL>/iuclid6-idp/ws*
    E.g.: `http://localhost:8181/iuclid6-idp-ws`
  - Sign-on URL: *https://<IUCLID URL>/iuclid6-web*
    E.g.: `https://localhost:8181/iuclid6-web`



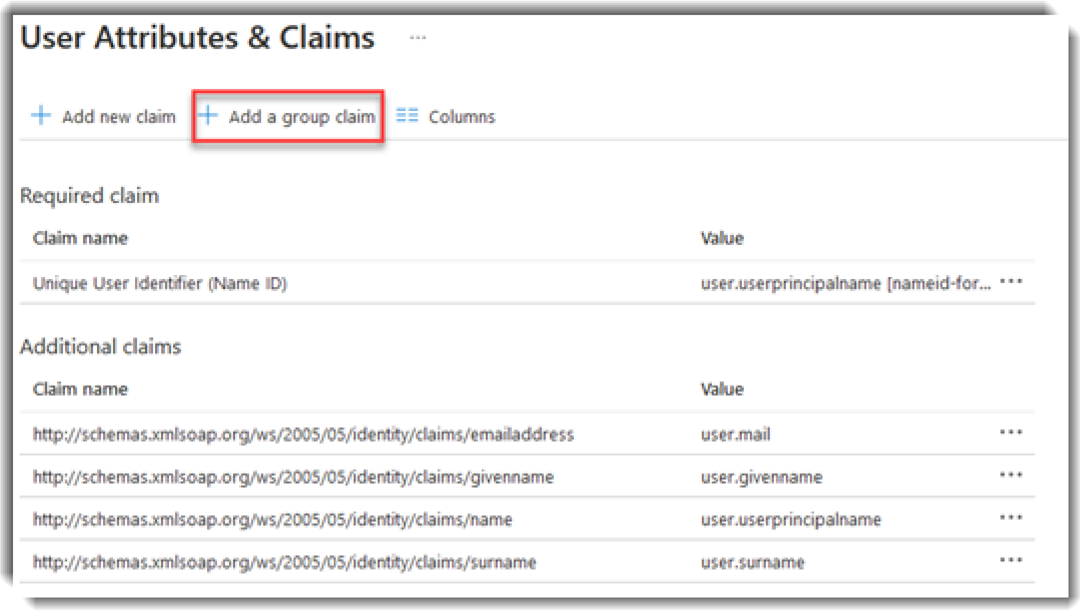
Basic SAML Configuration

Edit

Identifier (Entity ID)	https://localhost:8181/iuclid6-idp-ws
Reply URL (Assertion Consumer Service URL)	https://localhost:8181/iuclid6-idp-ws
Sign on URL	https://localhost:8181/iuclid6-web
Relay State (Optional)	*Optional*
Logout Url (Optional)	*Optional*

- User Attributes & Claims
  - *user.givenname*
  - *user.surname*
  - *user.mail*

  - *user.userprincipalname*
  - *user.groups* [SecurityGroup]
- Use *user.userprincipalname* as the *Unique User Identifier*
- Add the security groups to *User Attributes & Claims*



User Attributes & Claims ···

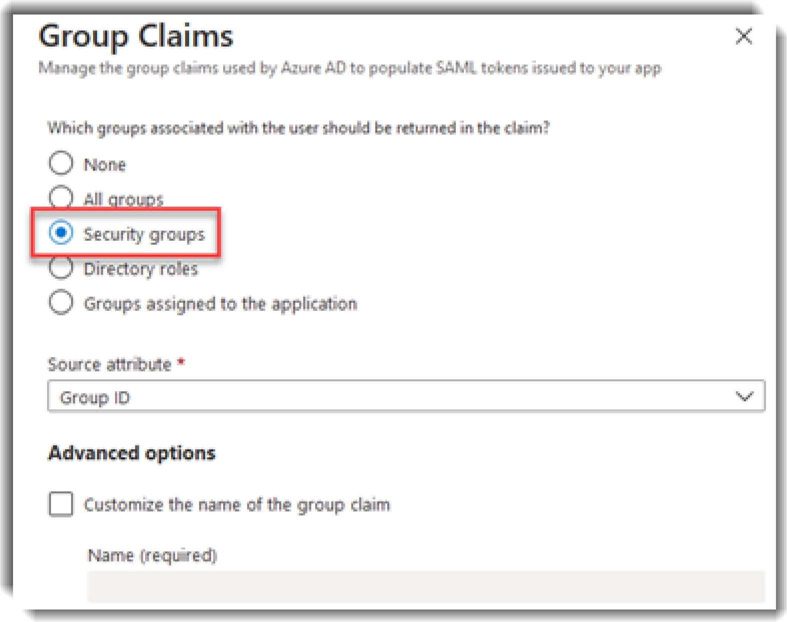
Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for... ···

Additional claims

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail ···
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname ···
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname ···
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname ···

- In the opened dialog select *Security groups*.



Group Claims

Manage the group claims used by Azure AD to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

○ None
○ All groups
● Security groups
○ Directory roles
○ Groups assigned to the application

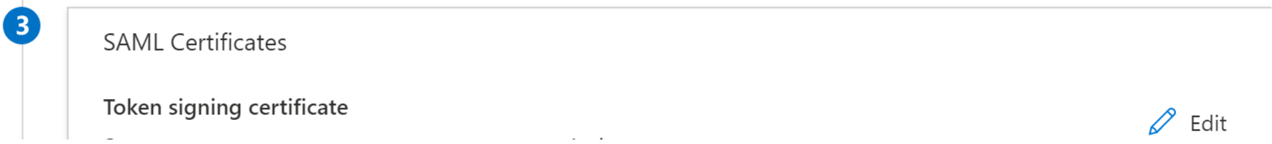
Source attribute *
Group ID

Advanced options

□ Customize the name of the group claim

Name (required)

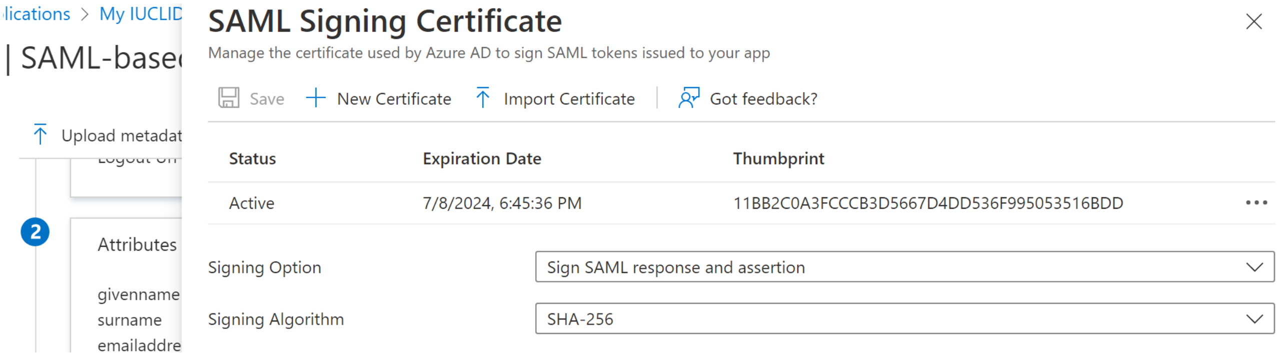
- In the section *SAML Certificates* (#3) press *Edit*:



SAML Certificates

Token signing certificate

Set *Signing Option* to `Sign SAML response and assertion`



SAML Signing Certificate

Manage the certificate used by Azure AD to sign SAML tokens issued to your app

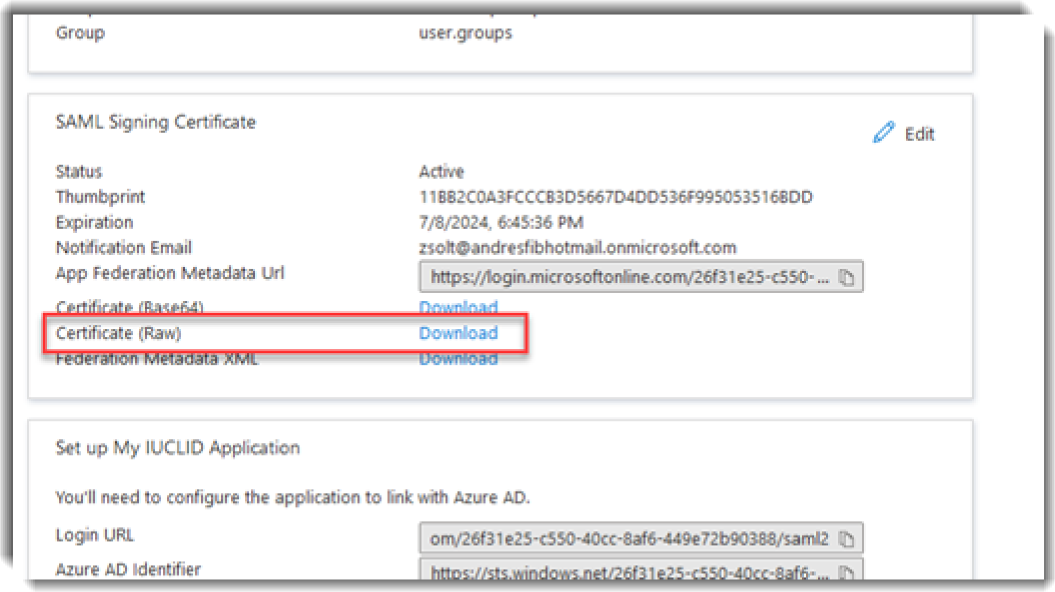
Status	Expiration Date	Thumbprint
Active	7/8/2024, 6:45:36 PM	11BB2C0A3FCCCB3D5667D4DD536F995053516BDD

Signing Option: Sign SAML response and assertion

Signing Algorithm: SHA-256

3.3. Collect information needed to configure SSO in IUCLID

Download the file *SAML Signing Certificate*.



Group user.groups

SAML Signing Certificate

Status	Active
Thumbprint	11BB2C0A3FCCCB3D5667D4DD536F995053516BDD
Expiration	7/8/2024, 6:45:36 PM
Notification Email	zsolt@andresfibhotmail.onmicrosoft.com
App Federation Metadata Url	https://login.microsoftonline.com/26f31e25-c550-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

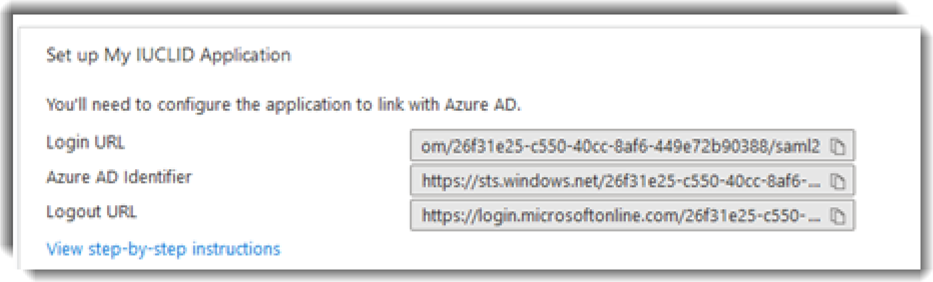
Set up My IUCLID Application

You'll need to configure the application to link with Azure AD.

Login URL	om/26f31e25-c550-40cc-8af6-449e72b90388/saml2
Azure AD Identifier	https://sts.windows.net/26f31e25-c550-40cc-8af6-...

Make a record of the values of the following parameters, for later use:

- *Login URL*
- *Azure AD Identifier*
- *Logout URL*



Set up My IUCLID Application

You'll need to configure the application to link with Azure AD.

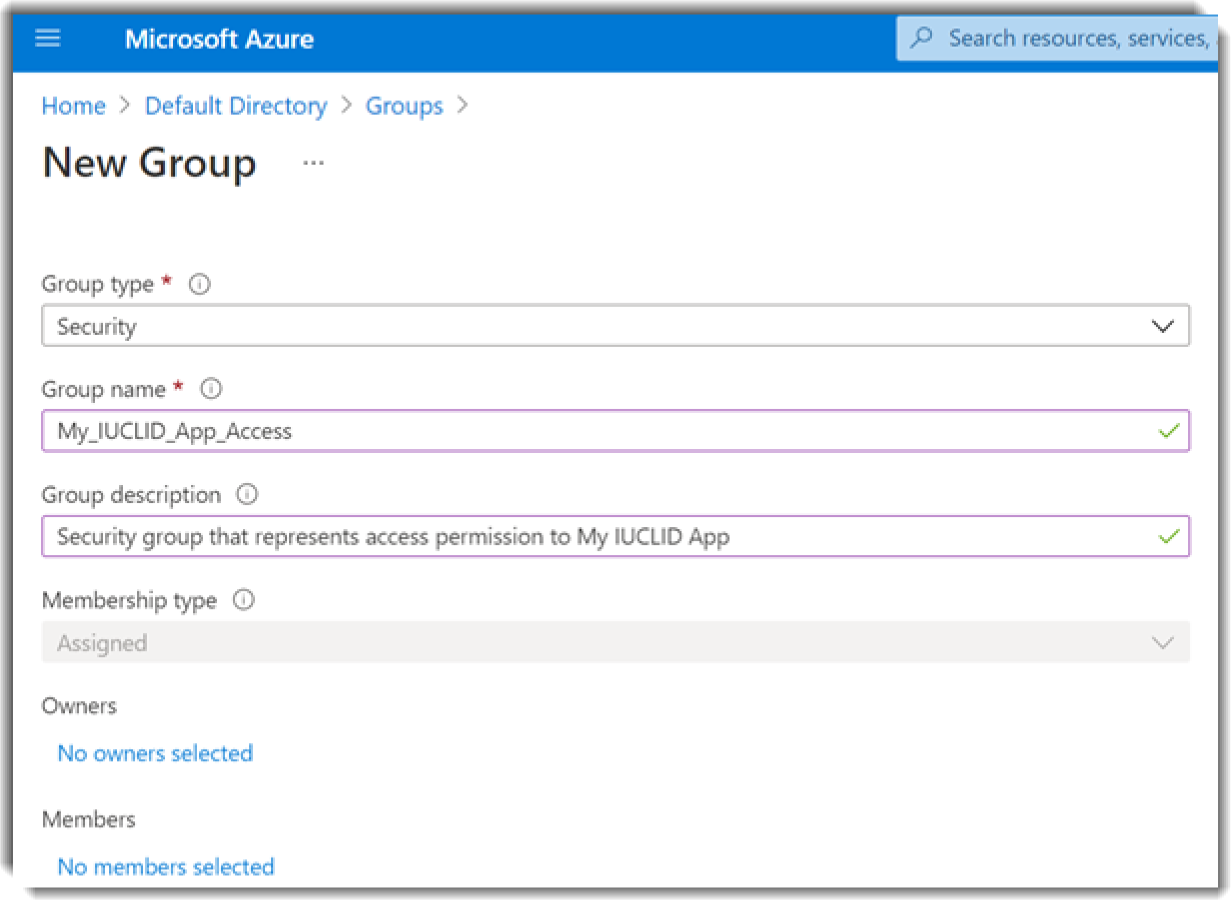
Login URL om/26f31e25-c550-40cc-8af6-449e72b90388/saml2

Azure AD Identifier https://sts.windows.net/26f31e25-c550-40cc-8af6-...

Logout URL https://login.microsoftonline.com/26f31e25-c550-...

3.4. Create a group that represents access permission to IUCLID

Create a group that represents access permission to the instance of the IUCLID application.



Microsoft Azure
Search resources, services,
Home > Default Directory > Groups >

New Group

Group type * Security

Group name * My_IUCLID_App_Access

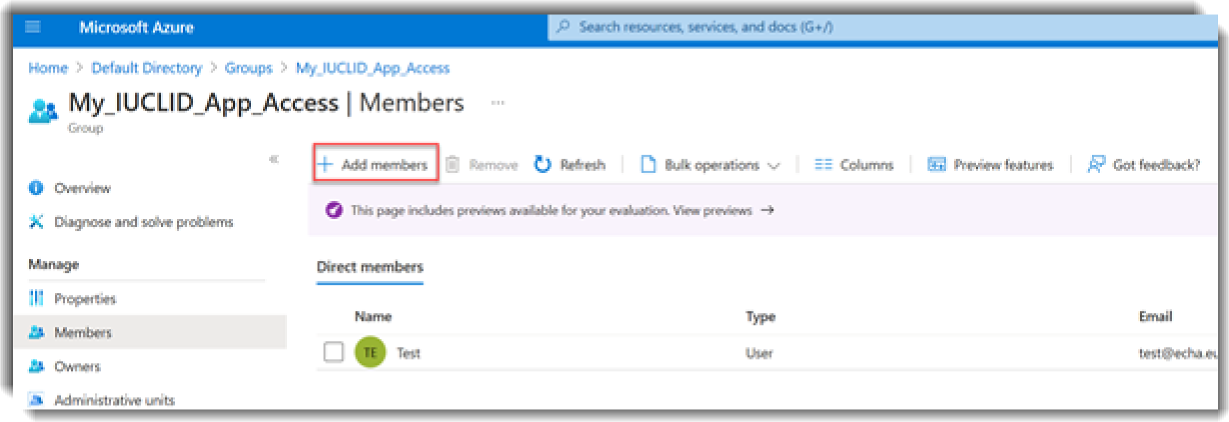
Group description Security group that represents access permission to My IUCLID App

Membership type Assigned

Owners No owners selected

Members No members selected

Add users to the group.

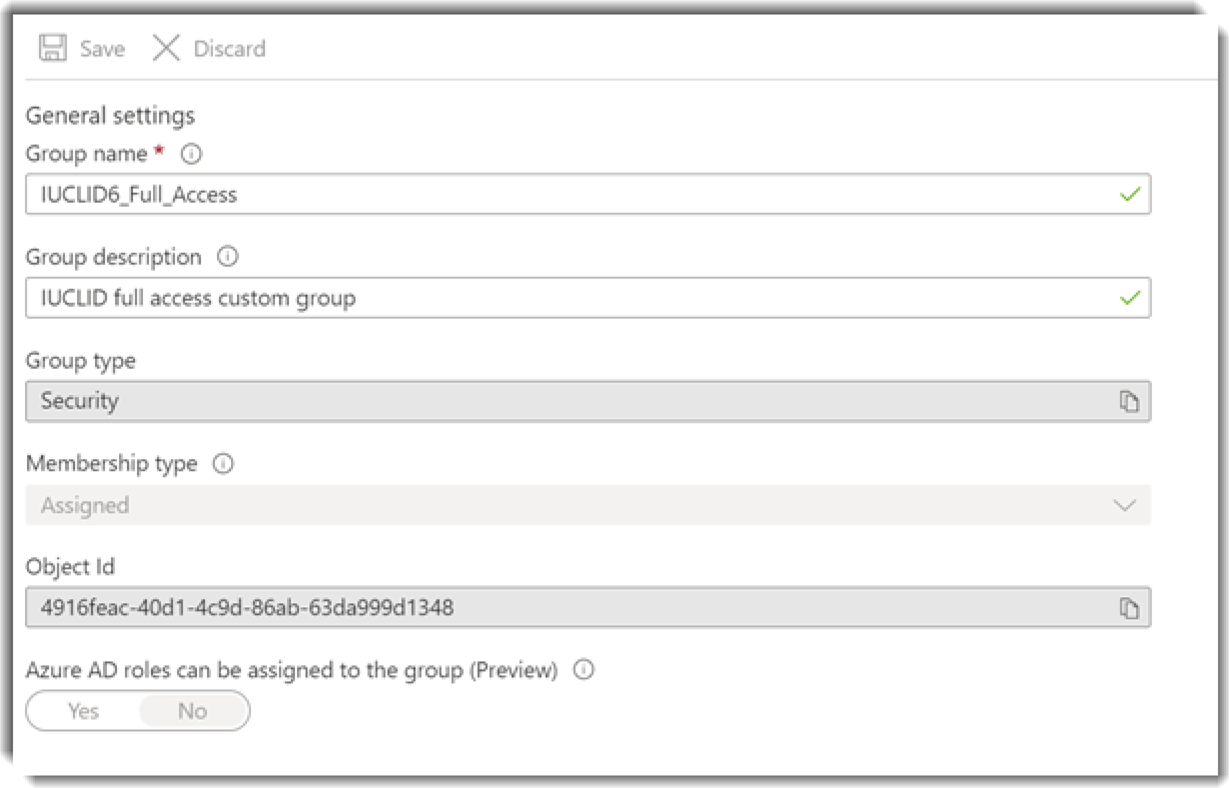


This page includes previews available for your evaluation. View previews →

Name	Type	Email
TE Test	User	test@echa.eu

3.5. Create groups in Azure AD that map to IUCLID Roles and IUCLID Security Groups

Create Azure AD security groups that will be mapped to IUCLID Roles and IUCLID Security Groups in the IUCLID application. For example, an Azure AD security group that can be mapped to the IUCLID Role, *Full Access*.



General settings

Group name * : IUCLID6_Full_Access

Group description: IUCLID full access custom group

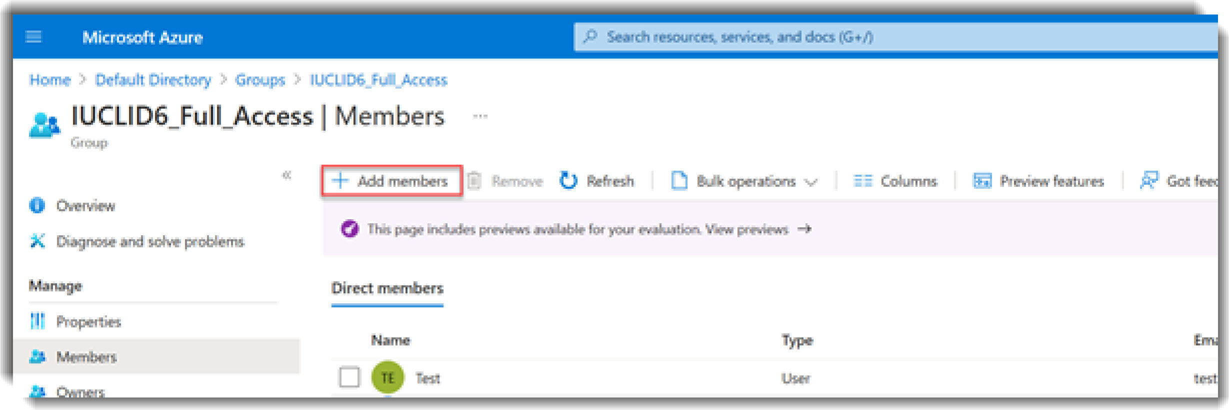
Group type: Security

Membership type: Assigned

Object Id: 4916feac-40d1-4c9d-86ab-63da999d1348

Azure AD roles can be assigned to the group (Preview): Yes [✓ No]

Add users to the group.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Default Directory > Groups > IUCLID6_Full_Access
IUCLID6_Full_Access | Members
Group
Add members
Remove
Refresh
Bulk operations
Columns
Preview features
Got feed
Overview
Diagnose and solve problems
Manage
Properties
Members
Owners
Direct members

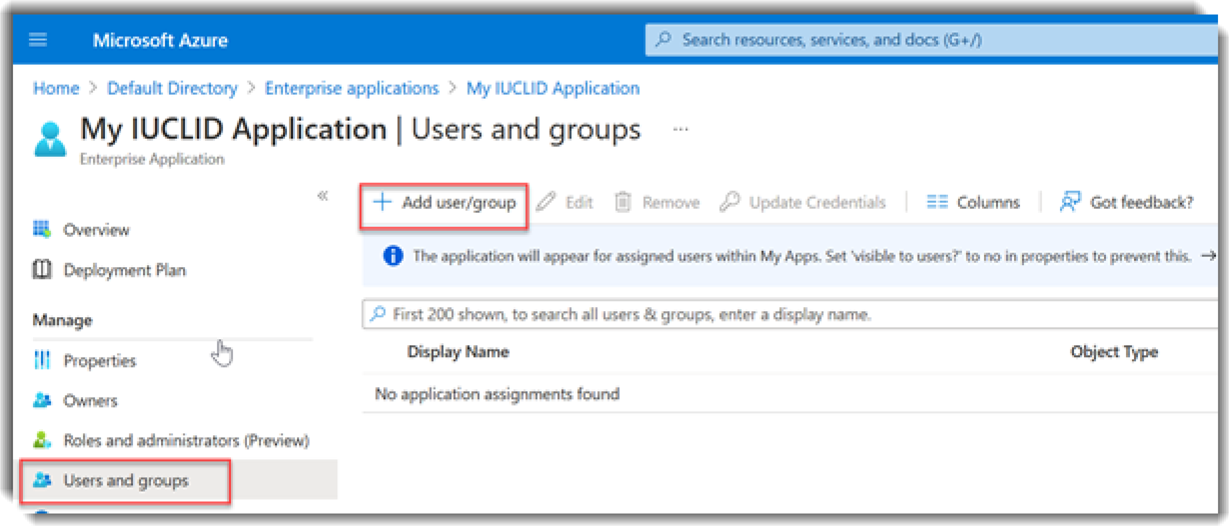
This page includes previews available for your evaluation. View previews →

Name	Type	Ema
TE Test	User	test

3.6. Assign users/groups in Azure AD to the IUCLID application

In Azure AD users can be assigned to a given application, as such specifying the set of users who can access the application. This serves the same purpose as the special security group that represents access permission to IUCLID (see above). Select *Add user/group* under:

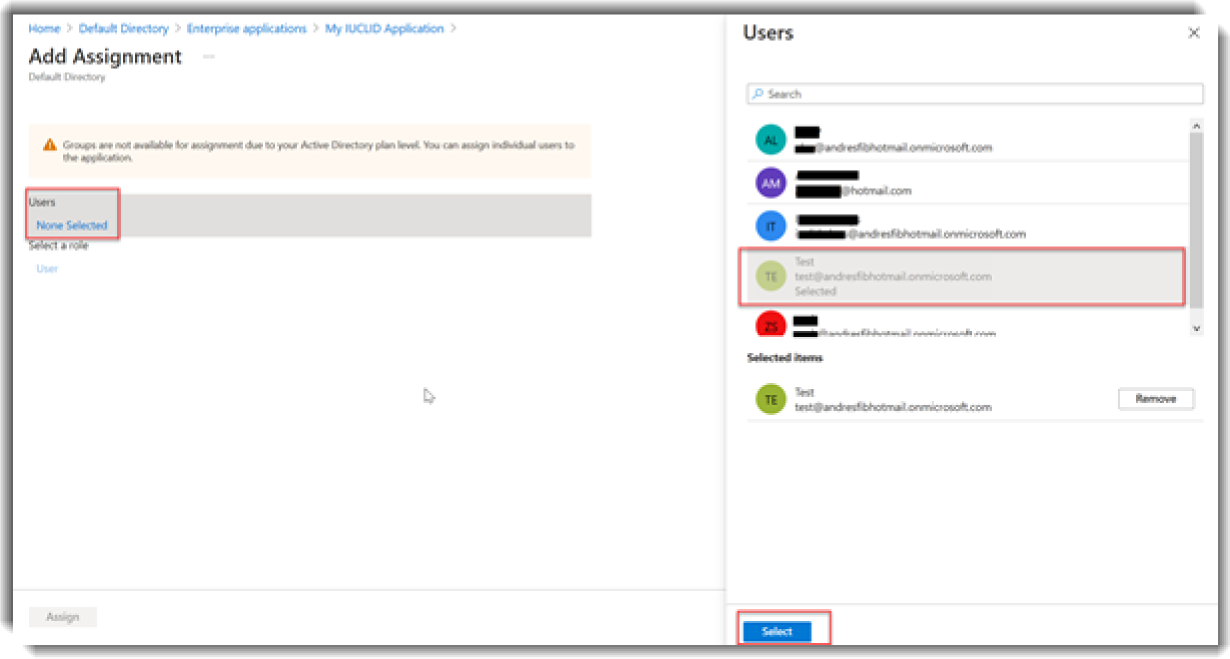
Enterprise Applications > My IUCLID Application > Users and groups


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Default Directory > Enterprise applications > My IUCLID Application
My IUCLID Application | Users and groups
Enterprise Application
Add user/group
Edit
Remove
Update Credentials
Columns
Got feedback?
Overview
Deployment Plan
Manage
Properties
Owners
Roles and administrators (Preview)
Users and groups

The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

First 200 shown, to search all users & groups, enter a display name.

Display Name	Object Type
No application assignments found	



Home > Default Directory > Enterprise applications > My IUCLID Application >

Add Assignment ...

Default Directory

⚠ Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.

Users

None Selected

Select a role

User

Assign

Users ×

Search

AL [redacted]
[redacted]@andresfibhotmail.onmicrosoft.com

AM [redacted]
[redacted]@hotmail.com

IT [redacted]
[redacted]@andresfibhotmail.onmicrosoft.com

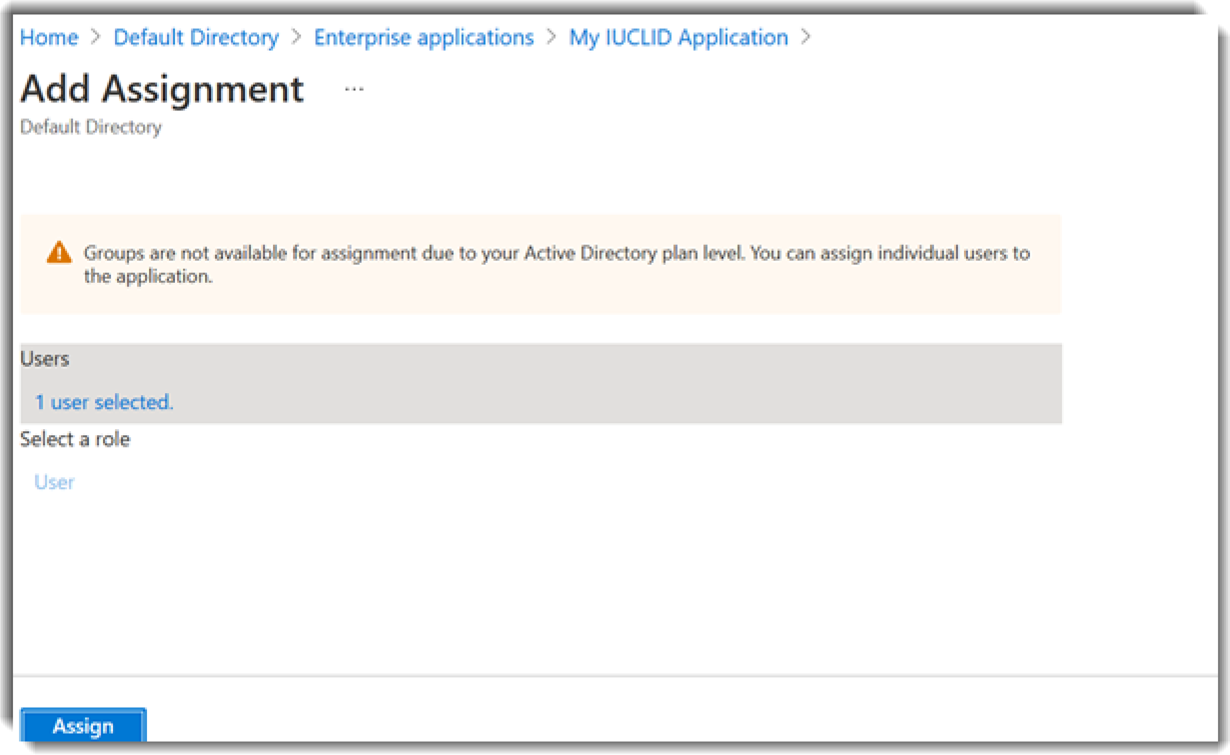
TE Test
test@andresfibhotmail.onmicrosoft.com
Selected

ZS [redacted]
[redacted]@andresfibhotmail.onmicrosoft.com

Selected items

TE Test
test@andresfibhotmail.onmicrosoft.com Remove

Select



Home > Default Directory > Enterprise applications > My IUCLID Application >

Add Assignment ...

Default Directory

⚠ Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.

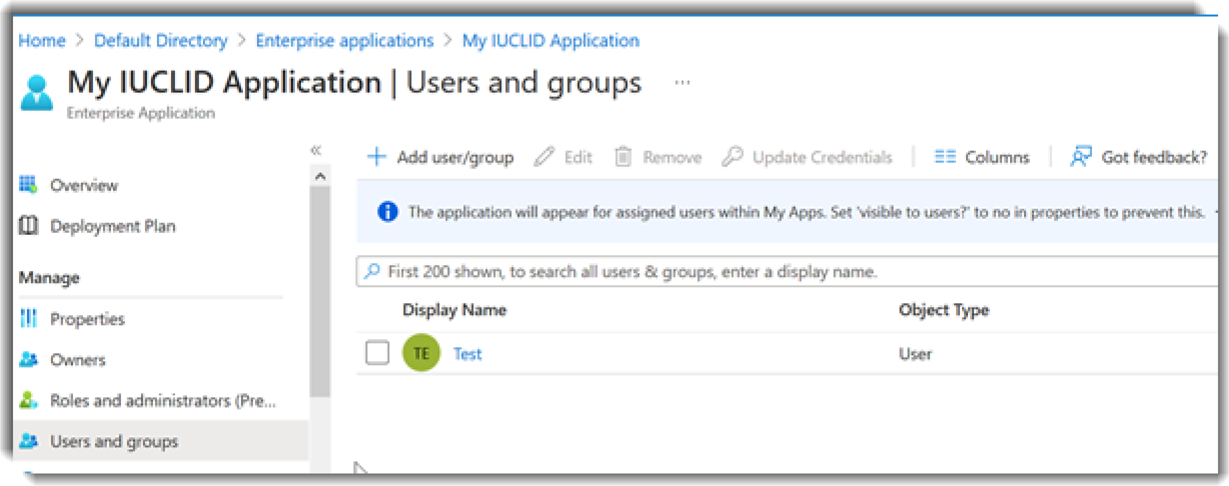
Users

1 user selected.

Select a role

User

Assign



Home > Default Directory > Enterprise applications > My IUCLID Application

My IUCLID Application | Users and groups ...

Enterprise Application

The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this.

First 200 shown, to search all users & groups, enter a display name.

Display Name	Object Type
□ TE Test	User

4. Configuring IUCLID

The configuration files referred to in this section are in the IUCLID installation at:

```
<iuclid6-installation-
folder>\glassfish4\glassfish\domains\domain1\config\
```

4.1. Configure public certificate of the external IDP

Import into the keystore of IUCLID, the *SAML Signing Certificate* which was downloaded in an earlier step. This is done from the command line, in the folder:

```
<iuclid6-installation-
folder>\glassfish4\glassfish\domains\domain1\config\
```

Ensure that the following file is present. It is delivered with IUCLID.

```
sso-default-third-party.jks
```

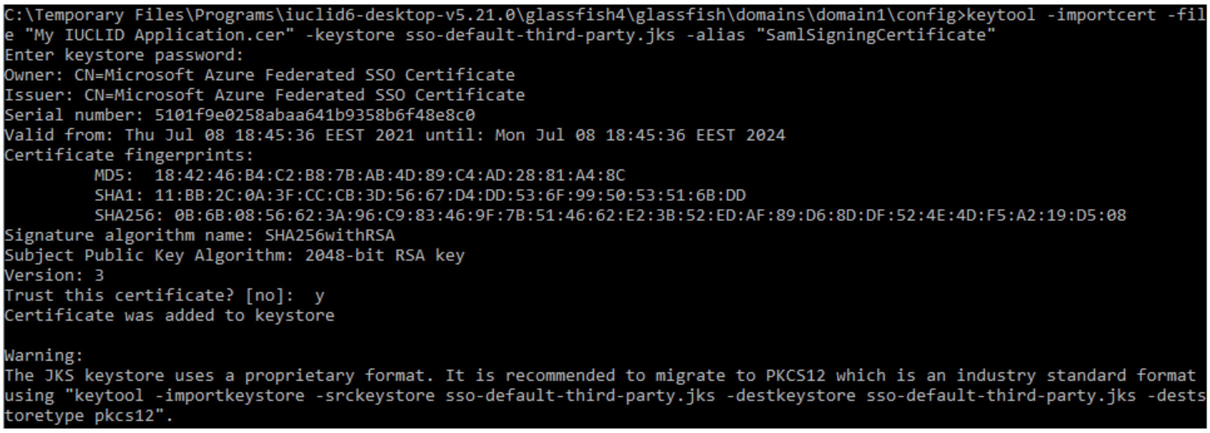
Ensure that the *SAML Signing Certificate* is present, for example in a file named:

```
My-IUCLID-Application.cer
```

Execute the command:

```
keytool -importcert -file My-IUCLID-Application.cer -keystore sso-
default-third-party.jks -alias SamlSigningCertificate
```

The default password for the keystore file is `admin12345_`.



```
C:\Temporary Files\Programs\iuclid6-desktop-v5.21.0\glassfish4\glassfish\domains\domain1\config>keytool -importcert -fil
e "My IUCLID Application.cer" -keystore sso-default-third-party.jks -alias "SamlSigningCertificate"
Enter keystore password:
Owner: CN=Microsoft Azure Federated SSO Certificate
Issuer: CN=Microsoft Azure Federated SSO Certificate
Serial number: 5101f9e0258abaa641b9358b6f48e8c0
Valid from: Thu Jul 08 18:45:36 EEST 2021 until: Mon Jul 08 18:45:36 EEST 2024
Certificate fingerprints:
         MD5:  18:42:46:B4:C2:B8:7B:AB:4D:89:C4:AD:28:81:A4:8C
         SHA1: 11:BB:2C:0A:3F:CC:CB:3D:56:67:D4:DD:53:6F:99:50:53:51:6B:DD
         SHA256: 0B:6B:08:56:62:3A:96:C9:83:46:9F:7B:51:46:62:E2:3B:52:ED:AF:89:D6:8D:DF:52:4E:4D:F5:A2:19:D5:08
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3
Trust this certificate? [no]:  y
Certificate was added to keystore

Warning:
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format
using "keytool -importkeystore -srckeystore sso-default-third-party.jks -destkeystore sso-default-third-party.jks -dests
toretype pkcs12".
```

4.2. Configure user data synchronization from IDP to IUCLID

Create a text file named `idp-user-sync-config.yml` in the folder:

```
<iuclid6-installation-
folder>\glassfish4\glassfish\domains\domain1\config\
```

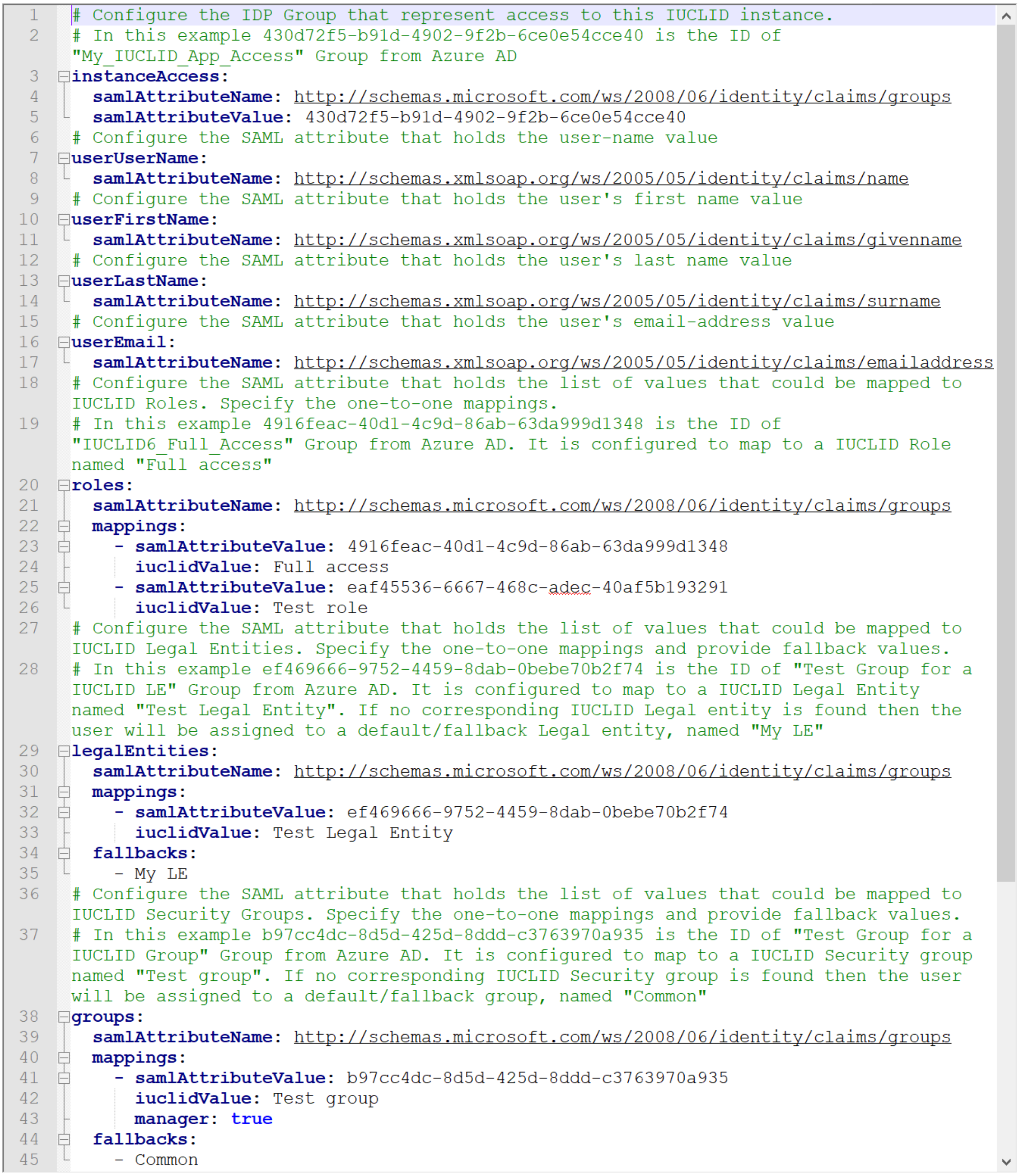
Note: an example is provided with this document, that can be used as a starting point. For more information on the different configuration parameters please see the annex.

The configuration file serves two main purposes:

1. Specifies how to read the SAML XML attributes in the response that is returned from IDP after a successful authentication. This is required to perform synchronization of user-data and to validate access, e.g.:
    a. A single IDP group or role indicating access permission to this specific IUCLID instance;
    b. User account data that is saved to the IUCLID database: username, first name, last name, email;
    c. List of mappings of groups in IDP, to Roles in IUCLID. This is used to assign IUCLID roles to the authenticated username;
    d. List of mappings of groups in IDP, to security groups in IUCLID. This is used to assign IUCLID security groups to the authenticated username. This setting is optional and is relevant only if Instance Based Security (IBS) is enabled in IUCLID;
    e. List of mappings of groups in IDP, to Legal entities in IUCLID. This is used to assign IUCLID Legal entities to the authenticated username. This setting is optional
2. Defines SAML specific configuration parameters:
    a. The URL of the external SAML provider;
    b. The path to the keystore file where the IDP's SAML signing certificate is stored;
    c. The alias of the IDP's SAML signing certificate provided when adding it in the keystore;
    d. The alias of IUCLID's SAML request signing certificate;
    e. The password of IUCLID's SAML request signing certificate;
    f. The URL that will be used when performing log-out.

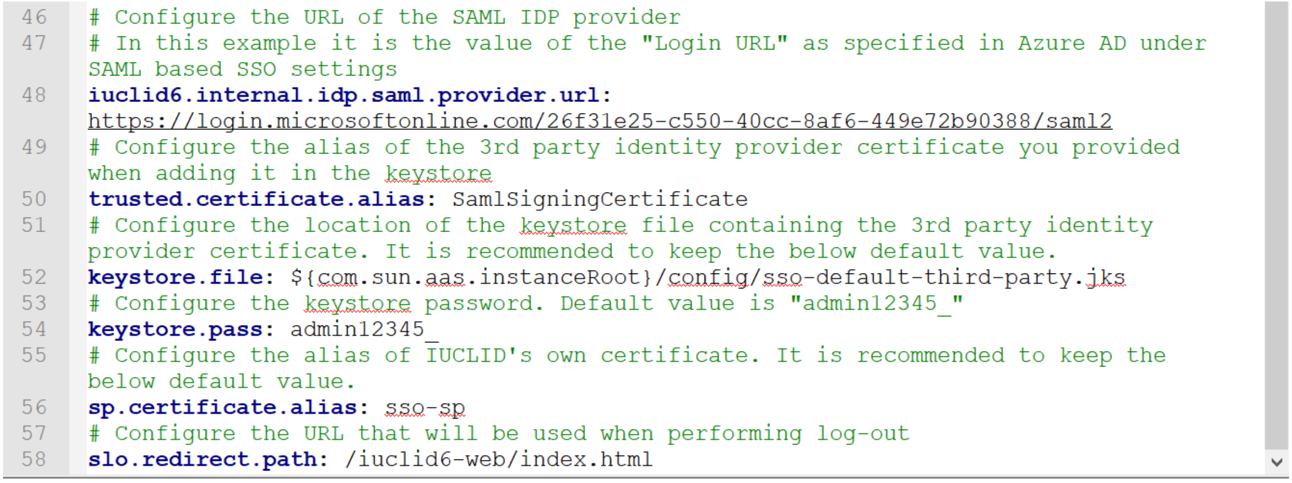
The image below is a screenshot from a text editor showing an example of the configuration file `idp-user-sync-config.yml`

It shows the first part of the file, which contains the configuration of how to read the attributes from the SAML response XML, based on the values in Azure AD, such as group object IDs, and the settings under *Single Sign-On with SAML > User Attributes & Claims*.



```
# Configure the IDP Group that represent access to this IUCLID instance.
# In this example 430d72f5-b91d-4902-9f2b-6ce0e54cce40 is the ID of "My_IUCLID_App_Access" Group from Azure AD
instanceAccess:
  samlAttributeName: http://schemas.microsoft.com/ws/2008/06/identity/claims/groups
  samlAttributeValue: 430d72f5-b91d-4902-9f2b-6ce0e54cce40
# Configure the SAML attribute that holds the user-name value
userUserName:
  samlAttributeName: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
# Configure the SAML attribute that holds the user's first name value
userFirstName:
  samlAttributeName: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
# Configure the SAML attribute that holds the user's last name value
userLastName:
  samlAttributeName: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
# Configure the SAML attribute that holds the user's email-address value
userEmail:
  samlAttributeName: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
# Configure the SAML attribute that holds the list of values that could be mapped to IUCLID Roles. Specify the one-to-one mappings.
# In this example 4916feac-40d1-4c9d-86ab-63da999d1348 is the ID of "IUCLID6_Full_Access" Group from Azure AD. It is configured to map to a IUCLID Role named "Full access"
roles:
  samlAttributeName: http://schemas.microsoft.com/ws/2008/06/identity/claims/groups
  mappings:
    - samlAttributeValue: 4916feac-40d1-4c9d-86ab-63da999d1348
      iuclidValue: Full access
    - samlAttributeValue: eaf45536-6667-468c-adec-40af5b193291
      iuclidValue: Test role
# Configure the SAML attribute that holds the list of values that could be mapped to IUCLID Legal Entities. Specify the one-to-one mappings and provide fallback values.
# In this example ef469666-9752-4459-8dab-0bebe70b2f74 is the ID of "Test Group for a IUCLID LE" Group from Azure AD. It is configured to map to a IUCLID Legal Entity named "Test Legal Entity". If no corresponding IUCLID Legal entity is found then the user will be assigned to a default/fallback Legal entity, named "My LE"
legalEntities:
  samlAttributeName: http://schemas.microsoft.com/ws/2008/06/identity/claims/groups
  mappings:
    - samlAttributeValue: ef469666-9752-4459-8dab-0bebe70b2f74
      iuclidValue: Test Legal Entity
  fallbacks:
    - My LE
# Configure the SAML attribute that holds the list of values that could be mapped to IUCLID Security Groups. Specify the one-to-one mappings and provide fallback values.
# In this example b97cc4dc-8d5d-425d-8ddd-c3763970a935 is the ID of "Test Group for a IUCLID Group" Group from Azure AD. It is configured to map to a IUCLID Security group named "Test group". If no corresponding IUCLID Security group is found then the user will be assigned to a default/fallback group, named "Common"
groups:
  samlAttributeName: http://schemas.microsoft.com/ws/2008/06/identity/claims/groups
  mappings:
    - samlAttributeValue: b97cc4dc-8d5d-425d-8ddd-c3763970a935
      iuclidValue: Test group
      manager: true
  fallbacks:
    - Common
```

In the lower part of the file, configuration parameters specific to SAML are defined.



```
# Configure the URL of the SAML IDP provider
# In this example it is the value of the "Login URL" as specified in Azure AD under SAML based SSO settings
iuclid6.internal.idp.saml.provider.url: https://login.microsoftonline.com/26f31e25-c550-40cc-8af6-449e72b90388/saml2
# Configure the alias of the 3rd party identity provider certificate you provided when adding it in the keystore
trusted.certificate.alias: SamlSigningCertificate
# Configure the location of the keystore file containing the 3rd party identity provider certificate. It is recommended to keep the below default value.
keystore.file: ${com.sun.aas.instanceRoot}/config/sso-default-third-party.jks
# Configure the keystore password. Default value is "admin12345_"
keystore.pass: admin12345_
# Configure the alias of IUCLID's own certificate. It is recommended to keep the below default value.
sp.certificate.alias: sso-sp
# Configure the URL that will be used when performing log-out
slo.redirect.path: /iuclid6-web/index.html
```

4.3. Enable SSO in IUCLID

In IUCLID, the configuration file for IDP/SSO is declared, and user management via the web interface is turned off. The settings are in the file `domain.xml` in the folder:

`<iuclid6-installation-folder>\glassfish4\glassfish\domains\domain1\config\`

Set the following system-properties elements in the section:

`<config name="server-config">`

Option	Description	Value
`iuclid6.admin.user.create`	Enables/disables user creation in the web UI.	`false`
`iuclid6.admin.user.assignToRole`	Enables/disables role assignment to users in the web UI.	`false`
`iuclid6.admin.user.assignToGroup`	Enables/disables group assignment to users in the web UI.	`false`
`idp.sso.config`	Path to the configuration file for the synchronization of user data.	`<path>`

Example:

```
…
   <system-property name="iuclid6.admin.user.create" value="false"></system-property>
<system-property name="iuclid6.admin.user.assignToRole" value="false"></system-property>
<system-property name="iuclid6.admin.user.assignToGroup" value="false"></system-property>
```

```
<system-property name="idp.sso.config"
value="${com.sun.aas.instanceRoot}/config/idp-user-sync-config.yml"></system-
property>


…
```

After doing the above steps restart the IUCLID application for the changes to take effect.

Appendix A. Example of the file idp-user-sync-config.yml

# Configure the IDP Group that represent access to this IUCLID instance.
# In this example `430d72f5-b91d-4902-9f2b-6ce0e54cce40` is the ID of the Group from Azure AD that is named `My_IUCLID_App_Access`.

```
instanceAccess:
  samlAttributeName:
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups
  samlAttributeValue: 430d72f5-b91d-4902-9f2b-6ce0e54cce40
```

# Configure the SAML attribute that holds the user-name value

```
userUserName:
  samlAttributeName: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
```

# Configure the SAML attribute that holds the user's first name value

```
userFirstName:
  samlAttributeName:
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
```

# Configure the SAML attribute that holds the user's last name value

```
userLastName:
  samlAttributeName:
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
```

# Configure the SAML attribute that holds the user's email-address value

```
userEmail:
  samlAttributeName:
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
```

# Configure the SAML attribute that holds the list of values that could be mapped to IUCLID Roles. Specify the one-to-one mappings.
# In this example `4916feac-40d1-4c9d-86ab-63da999d1348` is the ID of the Group from Azure AD that is named `IUCLID6_Full_Access`. It is configured to map to a IUCLID Role named `Full access`.

```
roles:
  samlAttributeName:
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups
  mappings:
    - samlAttributeValue: 4916feac-40d1-4c9d-86ab-63da999d1348
      iuclidValue: Full access
    - samlAttributeValue: eaf45536-6667-468c-adec-40af5b193291
      iuclidValue: Test role
```

# Configure the SAML attribute that holds the list of values that could be mapped to IUCLID Legal Entities. Specify the one-to-one mappings and provide fallback values.
# In this example `ef469666-9752-4459-8dab-0bebe70b2f74` is the ID of the Group from Azure AD that is named `Test Group for a IUCLID LE`. It is configured to map to a IUCLID Legal Entity named `Test Legal Entity`. If no corresponding IUCLID Legal entity is found then the user will be assigned to a default/fallback Legal entity, named `My LE`.

```
legalEntities:
  samlAttributeName:
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups
  mappings:
    - samlAttributeValue: ef469666-9752-4459-8dab-0bebe70b2f74
      iuclidValue: Test Legal Entity
  fallbacks:
    - My LE
```

# Configure the SAML attribute that holds the list of values that could be mapped to IUCLID Security Groups. Specify the one-to-one mappings and provide fallback values.
# In this example `b97cc4dc-8d5d-425d-8ddd-c3763970a935` is the ID of the Group named `Test Group for a IUCLID Group` which comes from Azure AD. It is configured to map to a IUCLID Security group named `Test group`. If no corresponding IUCLID Security group is found then the user will be assigned to a default/fallback group, named `Common`.

```
groups:
  samlAttributeName:
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups
  mappings:
    - samlAttributeValue: b97cc4dc-8d5d-425d-8ddd-c3763970a935
      iuclidValue: Test group
      manager: true
  fallbacks:
    - Common
```

# Configure the URL of the SAML IDP provider
# In this example it is the value of the `Login URL` as specified in Azure AD under SAML based SSO settings

```
idp.saml.provider.url: https://login.microsoftonline.com/26f31e25-c550-40cc-
8af6-449e72b90388/saml2
```

# Configure the alias of the 3rd party identity provider certificate you provided when adding it in the keystore

```
idp.certificate.alias: SamlSigningCertificate
```

# Configure the location of the keystore file containing the 3rd party identity provider certificate. It is recommended to keep the below default value.

```
keystore.file: ${com.sun.aas.instanceRoot}/config/sso-default-third-party.jks
```

# Configure the keystore password. Default value is `admin12345_`.

```
keystore.pass: admin12345_
```

# Configure the alias of IUCLID's own certificate. It is recommended to keep the below default value.

```
sp.certificate.alias: sso-sp
```

# Configure the URL that will be used when performing log-out

```
slo.redirect.path: /iuclid6-web/index.html
```

Appendix B. Documentation of the file idp-user-sync-config.yml

Property	Description	Remarks
`instanceAccess.samlAttributeName`	Defines the element of the SAML response that is searched for the instance access property.	Mandatory
`instanceAccess.samlAttributeValue`	Defines the value that the SAML response must contain for the user to have access to the IUCLID instance.	Mandatory
`userUserName.samlAttributeName`	Defines the element of the SAML response that is searched for the username of the user.	Mandatory
`userUserName.fallback`	Defines the username that will be used if no value is present in the above element.	Optional
`userFirstName.samlAttributeName`	Defines the element of the SAML response that is searched for the first name of the user.	Mandatory
`userFirstName.fallback`	Defines the first name that will be used if no value is present in the above element.	Optional
`userLastName.samlAttributeName`	Defines the element of the SAML response that is searched for the last name of the user.	Mandatory
`userLastName.fallback`	Defines the last name that will be used if no value is present in the above element.	Optional
`userEmail.samlAttributeName`	Defines the element of the SAML response that is searched for the email of the user.	Mandatory

Property	Description	Remarks
`userEmail.fallback`	Defines the email that will be used if no value is present in the above element	Optional
`roles.samlAttributeName`	Defines the element of the SAML response that is searched for roles.	Mandatory
`roles.mappings`	Defines a set of one-to-one role mappings between the SAML response role names and the IUCLID role names.	Optional (if fallbacks are set)

`roles.mappings.samlAttributeValue /`
`roles.mappings.iuclidValue`
	Defines an entry of a SAML response role name and the corresponding IUCLID role to which it will be mapped.	There is one instance of these per mapping.

`roles.fallbacks`	Defines a list of IUCLID roles that will be used in case no mapping is provided or no iuclid roles were mapped.	Optional (if mappings are set)
`groups.samlAttributeName`	Defines the element of the SAML response that is searched for the roles of the user.	Mandatory
`groups.mappings`	Defines a set of one to one group mappings between the SAML response group names and the IUCLID security group names.	Optional (if fallbacks are set)

`groups.mappings.samlAttributeValue /`
`groups.mappings.iuclidValue`
	Defines an entry of a SAML response group name and the corresponding IUCLID security group to which it will mapped.	There is one instance of these per mapping.

Property	Description	Remarks
`groups.fallbacks`	Defines a list of IUCLID security groups that will be used if no mapping is provided or no IUCLID security groups were mapped.	Optional (if mappings are set)
`legalEntities.samlAttributeName`	Defines the element of the SAML response that is searched for Legal entities.	Mandatory
`legalEntities.mappings`	Defines a set of one to one mappings between the SAML response legal entity names and the IUCLID legal entity names.	Optional (if fallbacks are set)
`legalEntities.mappings.samlAttributeValue / legalEntities.mappings.iuclidValue`	Defines an entry of a SAML response legal entity name and the corresponding IUCLID legal entity to which it will mapped.	There is one instance of these per mapping. There can be more than one legal entity with the same name in a IUCLID database. All matching legal entities are assigned to the user, but the first one is set as working legal entity.
`legalEntities.fallbacks`	A list of IUCLID Legal Entities that are used if no mapping is provided, or no IUCLID Legal Entities were mapped.	Mandatory
`idp.saml.provider.url`	The URL of the external SAML provider.	Mandatory

Property	Description	Remarks
`keystore.file`	The path to the keystore file that contains the IDP sync certificates.	Mandatory
`idp.certificate.alias`	The alias of the certificate of the third-party identity provider in the keystore	Mandatory
`keystore.pass`	The password of the certificate of the service provider.	Mandatory (Predefined value: admin12345_)
`sp.certificate.alias`	The alias of the certificate of the service provider (IUCLID)	Mandatory (Default Value: sso-sp)
`slo.redirect.path`	The URL to which the user is redirected on logging out of IUCLID.	Optional