
Google Workspace user
authentication in
UDS Enterprise 3.5
www.udsenterprise.com

Introduction

This document shows how to make the integration of a UDS Enterprise's SAML authenticator to validate existing users in Google Workspace.

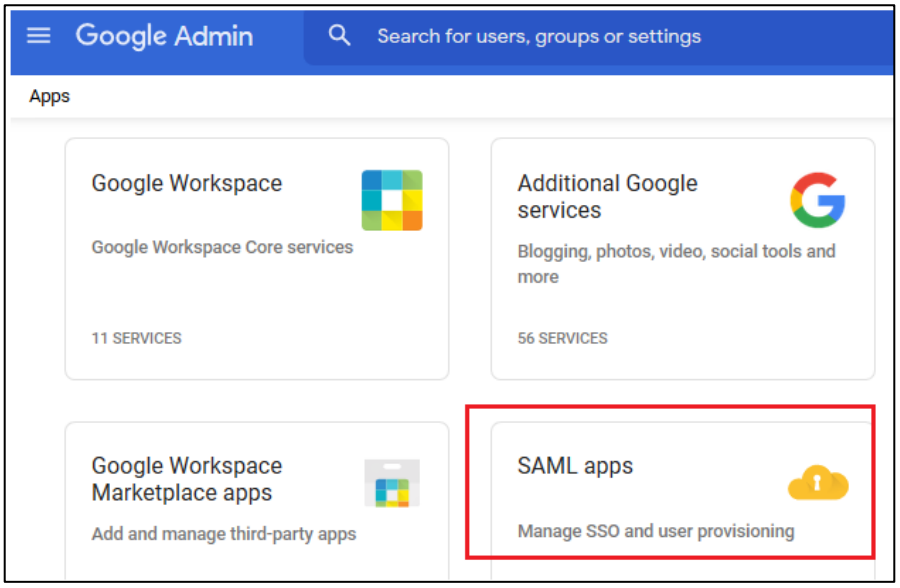
Once the new authenticator has been created in UDS Enterprise and integrated with Google Workspace, existing users in this environment will be able to access the services published in UDS Enterprise.

In order to carry out this integration, it will be necessary to have a registered user in UDS Enterprise and a user belonging to Google Workspace platform, both with administration permissions on their different environments.

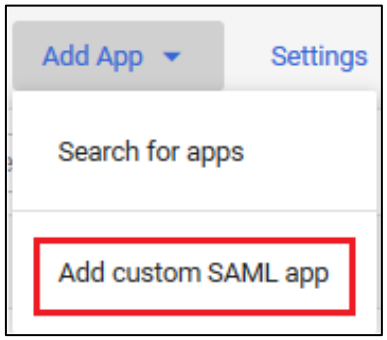
Creation of Google's SAML application

The first task will be performed in the administration dashboard of Google Workspace. A user with administration permissions is needed.

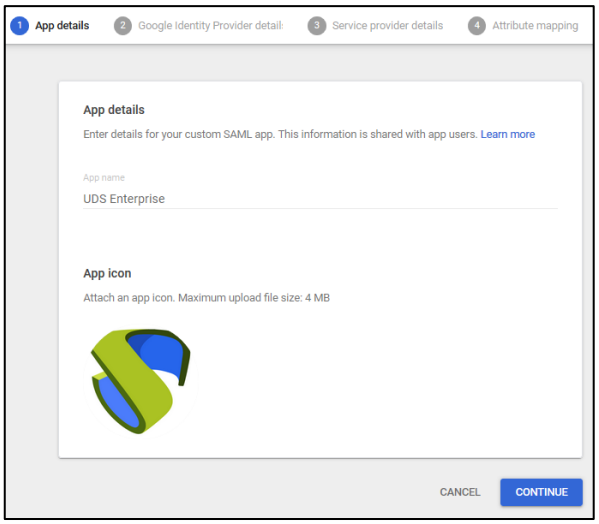
Access into the Google Workspace administration dashboard and select "**SAML apps**".



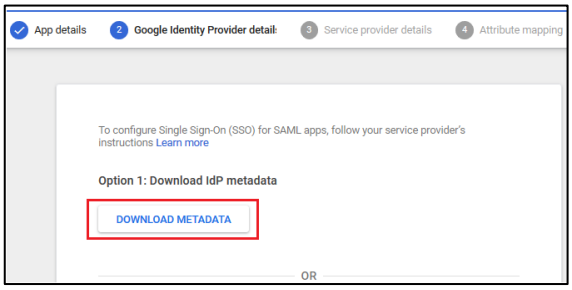
Register a new custom SAML application:



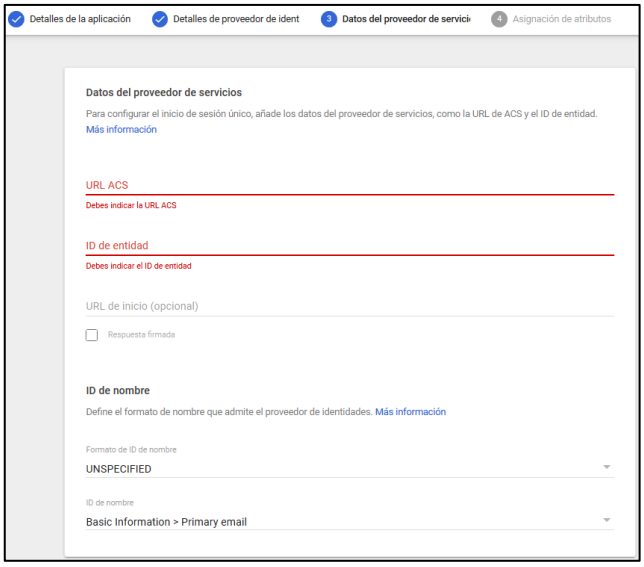
Indicate a name to identify the application in the configuration wizard. It is possible to add an icon so that users can easily find the service.



Now download the metadata and continue with the wizard:



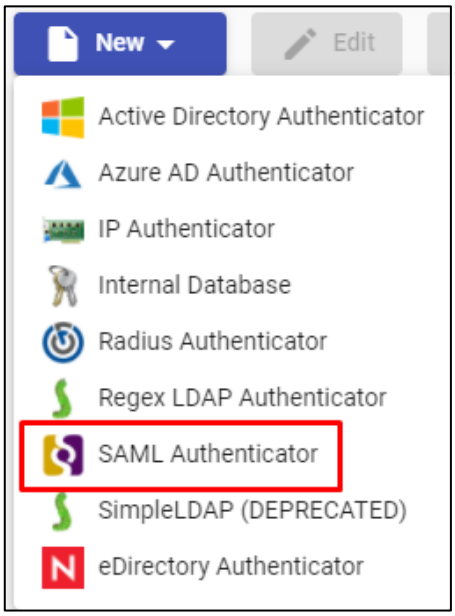
In step 3 of the wizard, it is necessary indicate the "**ACS URL**" and the "**Entity ID**":



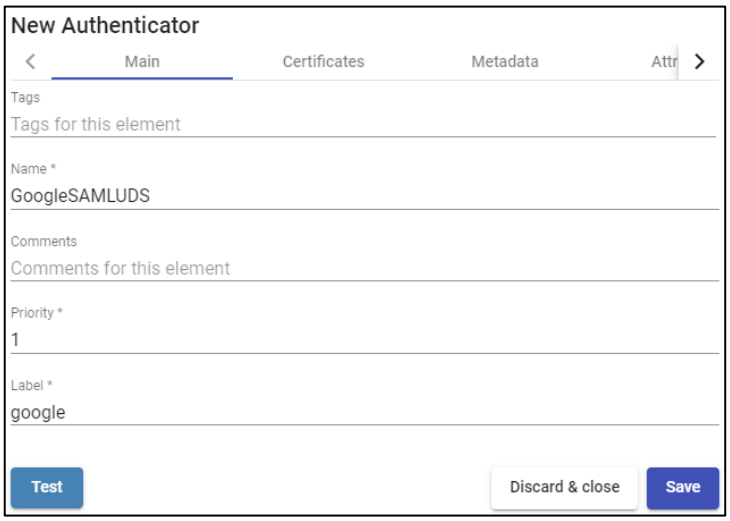
To obtain this data, access the administration of your UDS Enterprise environment and create a new SAML authenticator. Once you have the data, fill in the different sections of the wizard until it finishes.

Creating the SAML authenticator

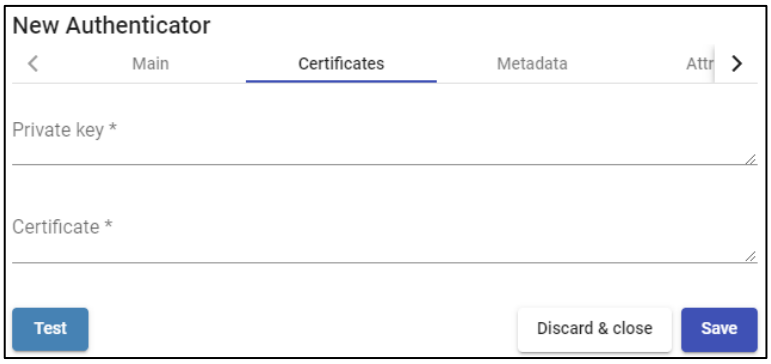
Access into the UDS Enterprise administration and go to the “**Authenticators**” section. Select “**New**” and choose “**SAML Authenticator**”.



In the "**Main**" tab, type a name for the authenticator (it cannot contain spaces), the priority and a "**Label**".



In the "**Certificates**" tab, it is necessary to indicate a valid certificate and its password. It must be in PEM format:



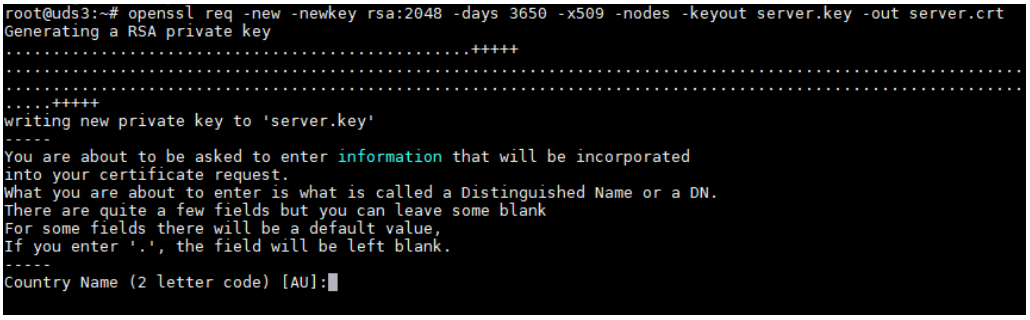
If you don't have certificates, you can generate one with **OpenSSL**. To create it, use the following statement (the UDS server has **OpenSSL** installed, so this machine can be used to generate the certificate):

```
openssl req -new -newkey rsa:2048 -days 3650 -x509 -nodes -keyout
server.key -out server.crt
```

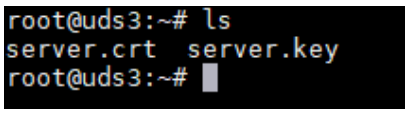
Once the certificate is generated, share the key with RSA. Use the following command:

```
openssl rsa -in server.key -out server_rsa.key
```

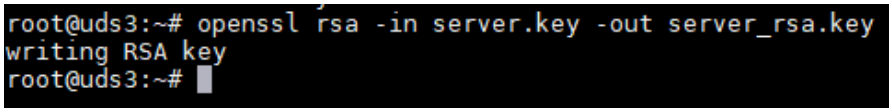
Certificate generation example:



Execute the command and fill in the necessary data to generate the certificate:



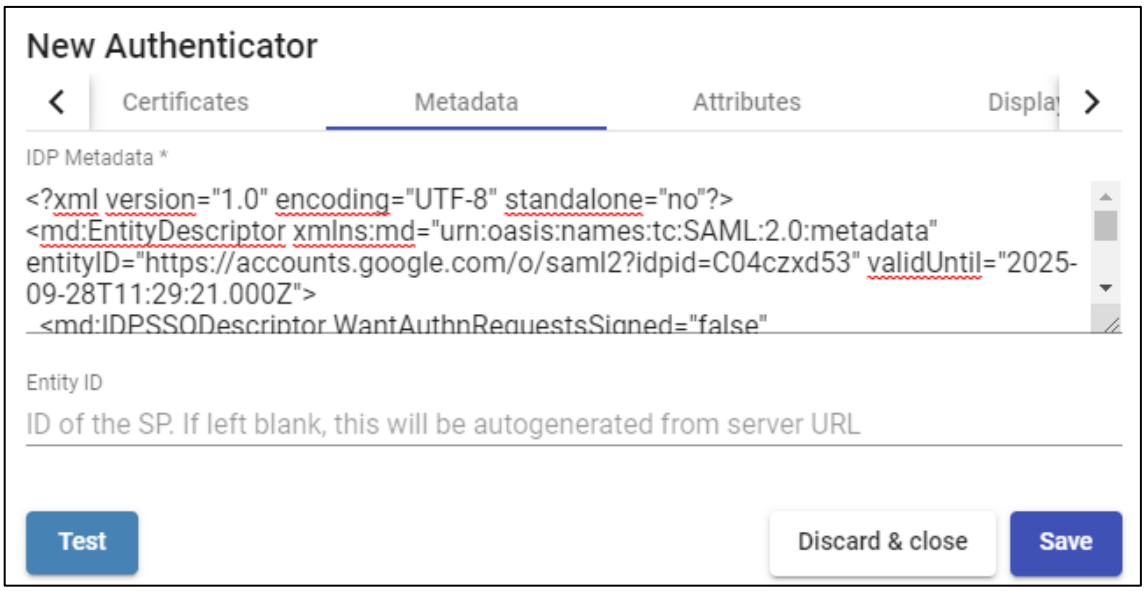
Now convert the key to **rsa** :



Copy the content of the certificate file and the **rsa** key in UDS:

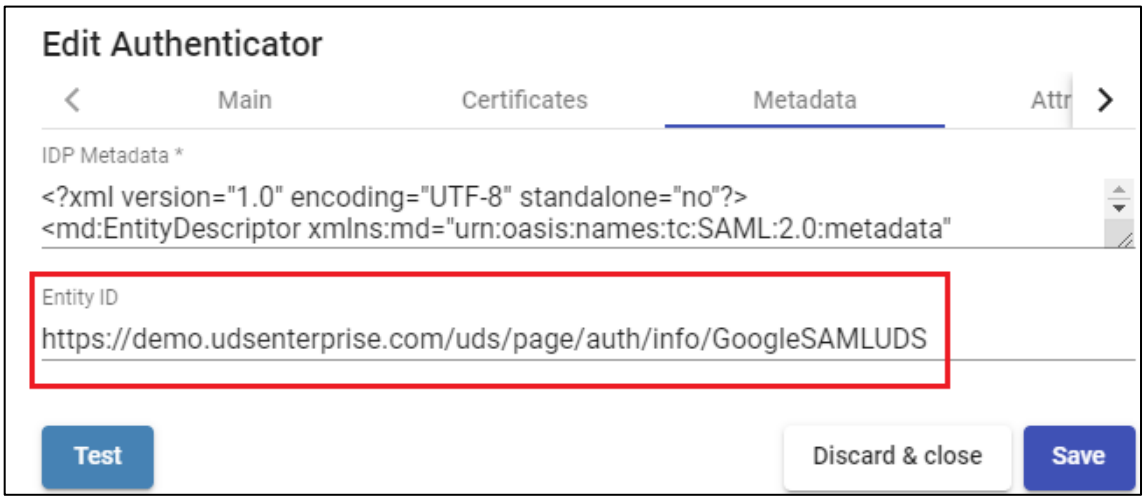
Copy the key in the "**Private Key**" section and the certificate in "**Certificate**":

In the next tab, "**Metadata**", complete the "**IDP Metadata**" section with the metadata downloaded from Google in previous steps (step 2 of the custom SAML application registration). It is important to copy all the content of the file. It is recommended to open the file with a suitable application and never with a browser (parts of the code can be hidden...):



Leave the "**Entity ID**" section empty, since it will be filled in automatically when the authenticator is saved. The data will be generated based on the URL used in the connection with the UDS Enterprise portal.

Save the authenticator (it is necessary to indicate some data in the "**Attributes**" tab so that it allows you to save. In the following steps we will return to this section and the final configuration will be applied) and when you edit it again you will be able to obtain the "**Entity ID**" data required to continue configuring the SAML custom application in the Google console.



Configuring the SAML application

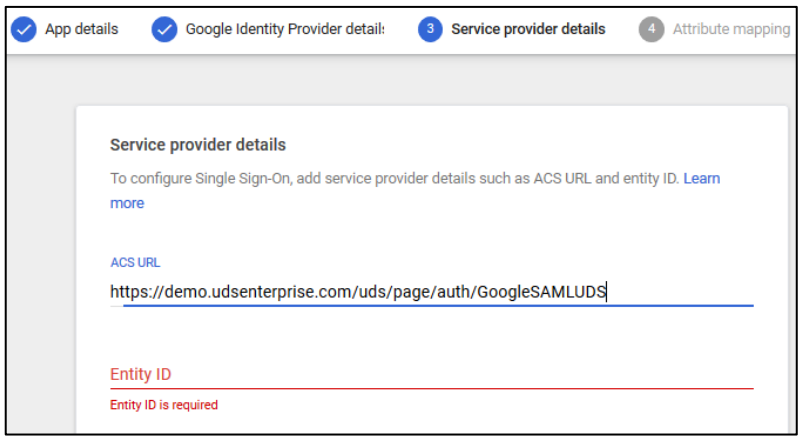
Go back to step 3 of the Google configuration wizard to create a custom SAML application, where the system will ask for the "**ACS URL**" and the "**Entity ID**".

To indicate the ACS (Assertion Consumer Service) data, download the "**Entity ID**" file that UDS has generated automatically when saving the authenticator (enter the indicated URL in a browser and download it. In this example it would be: https://demo.udsenterprise.com/uds/page/auth/info/GoogleSAMLUDS)

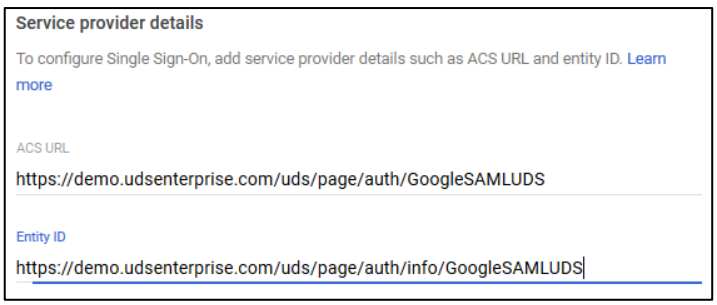
Inside the downloaded file, look for: **AssertionConsumerService:**

```
<md:SingleLogoutService
  Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
  Location="https://demo.udsenterprise.com/uds/page/auth/GoogleSAMLUDS?logout=true"/>
<md:AssertionConsumerService isDefault="true" index="0"
  Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Location="https://demo.udsenterprise.com/uds/page/auth/GoogleSAMLUDS" />
</md:SPSSODescriptor>
<md:Organization>
  <md:OrganizationName xml:lang="en">UDS</md:OrganizationName>
```

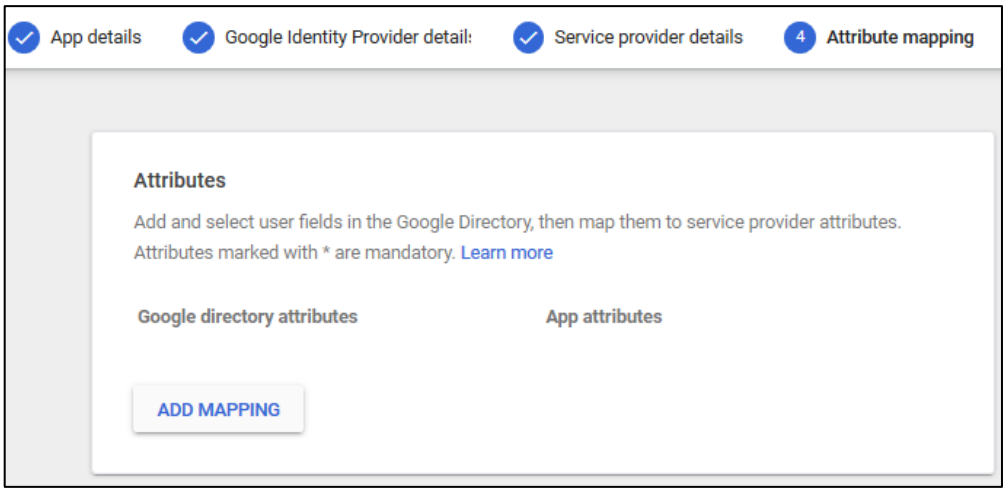
Copy the URL provided in the field "**URL ACS**":



Lastly, to finish configuring step 3, enter the "**Entity ID**". It is auto generated by UDS Enterprise in the "**Entity ID**" field of the "**Metadata**" tab of the authenticator:

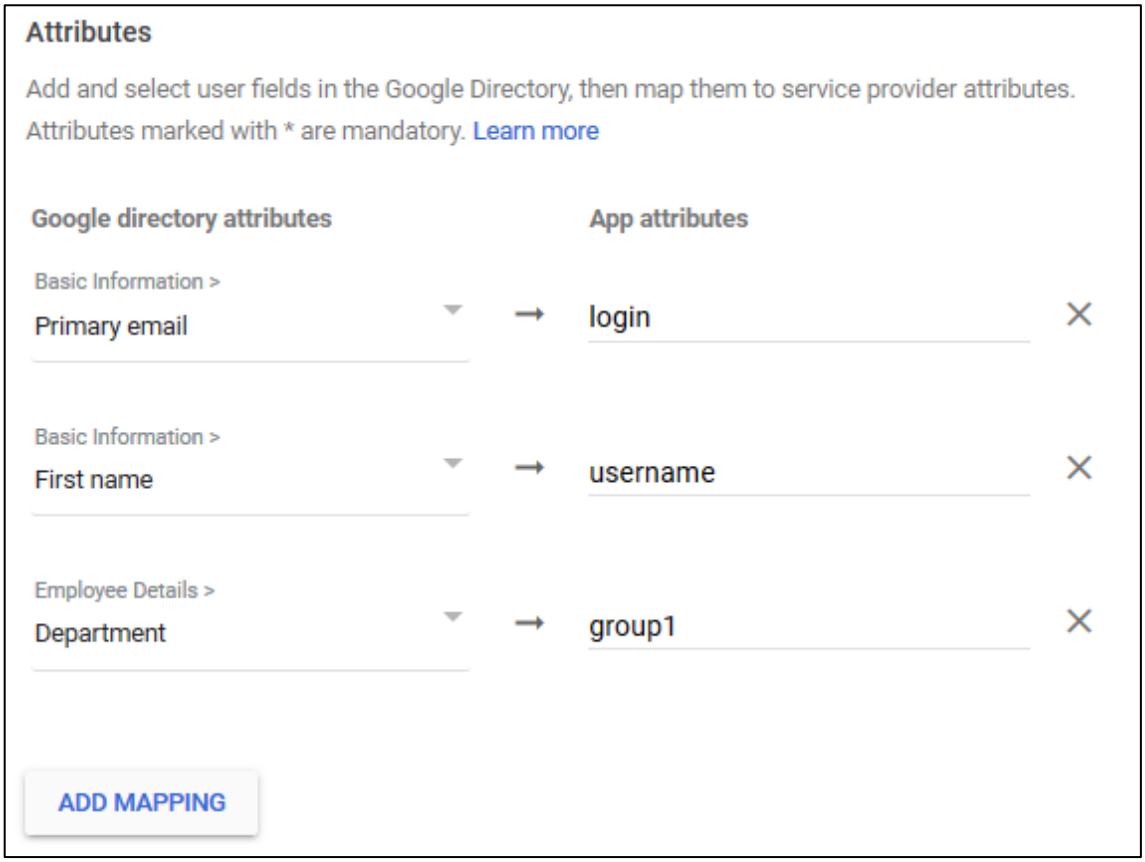


Leave the other default options and continue with step 4. There you will define the attributes that will be used by UDS Enterprise to validate users and configure groups:



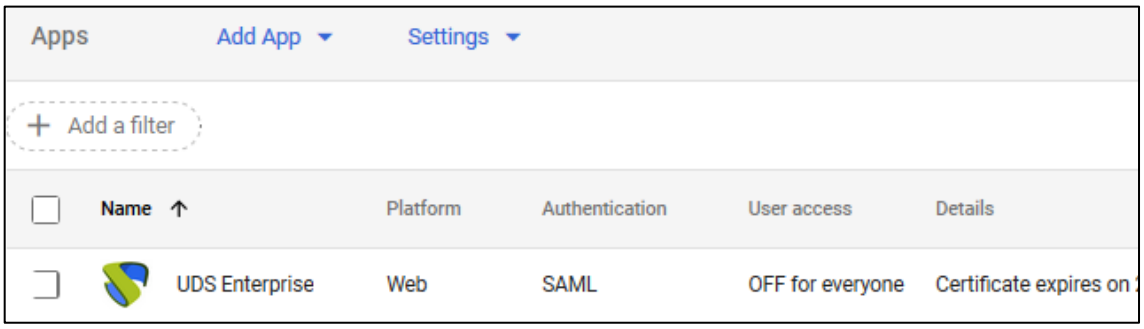
In this example, the following attributes will be used:

- The "**Primary email**" will be used for user login. It will be labelled as "**login**".
- To display the name of the user, use "**First name**". It will be labelled as "**username**".
- To define the group membership of the users, use "**Department**". It will be labelled as "**group1**".

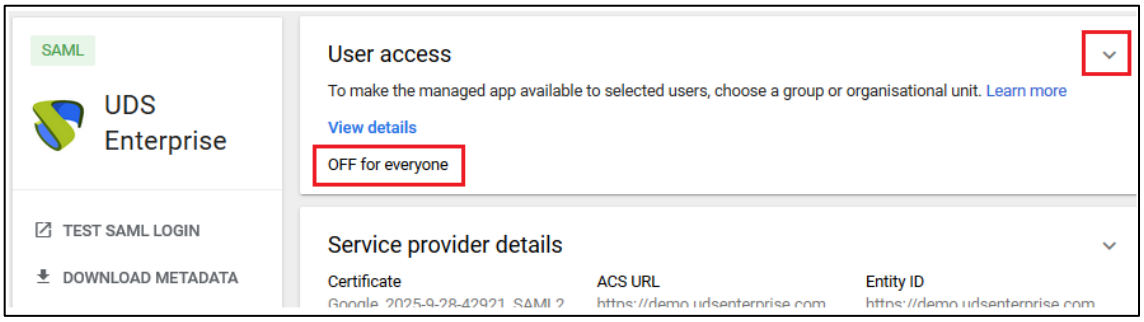


We can use or add custom attributes. In this example the default attributes provided by Google will be used.

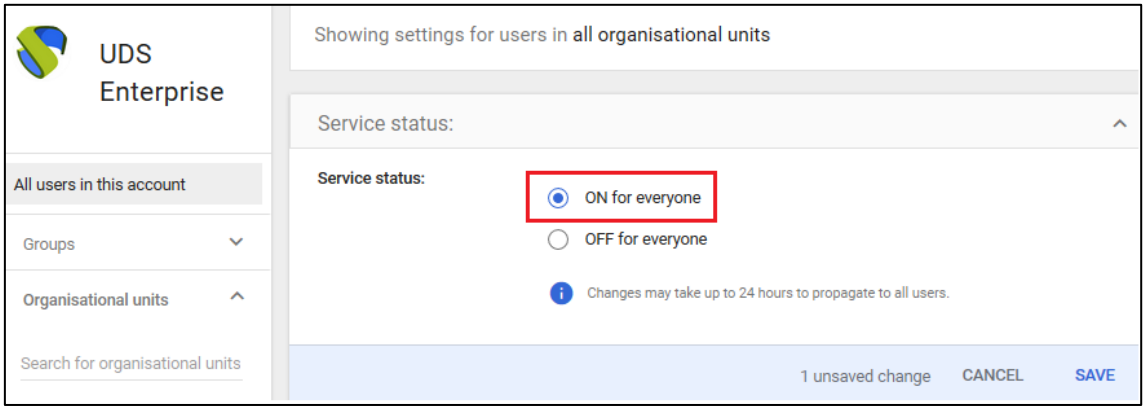
Once the necessary attributes have been selected, finish the wizard.



If you access the created application, you will see that by default it is deactivated for all users, so you must enable it. Access the "**User Access**" options:



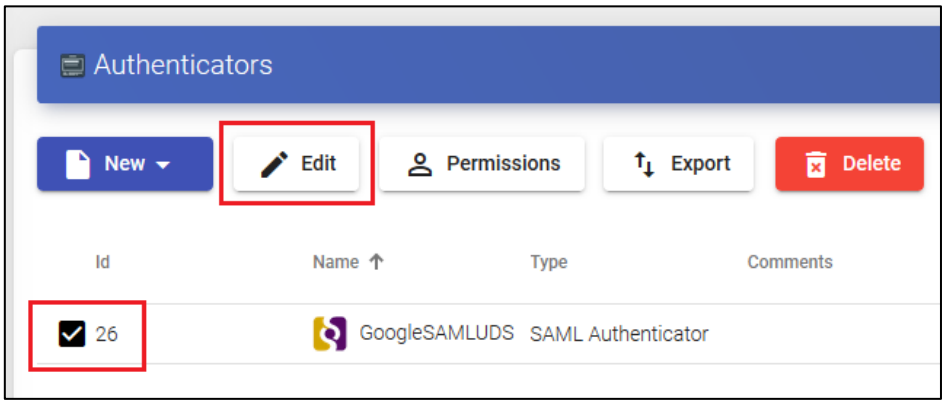
In this example the application will be activated for all users, but it is possible to limit it by groups.



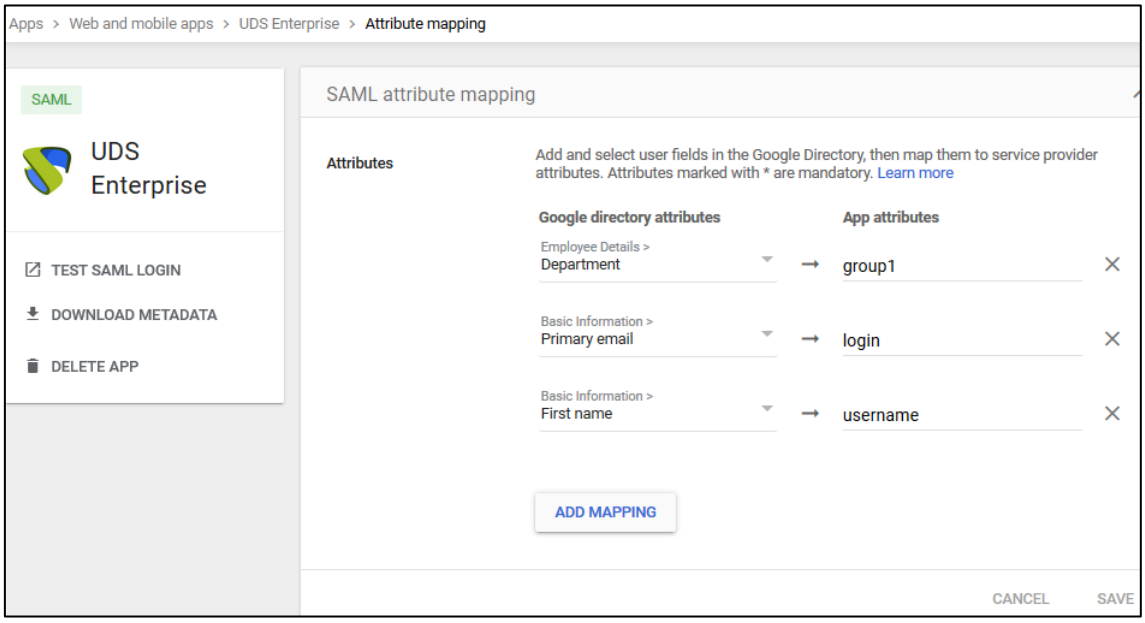
Save to apply the change.

Defining attributes in SAML

Access the UDS Enterprise administration, select the previously created SAML authenticator and click on “**Edit**”.

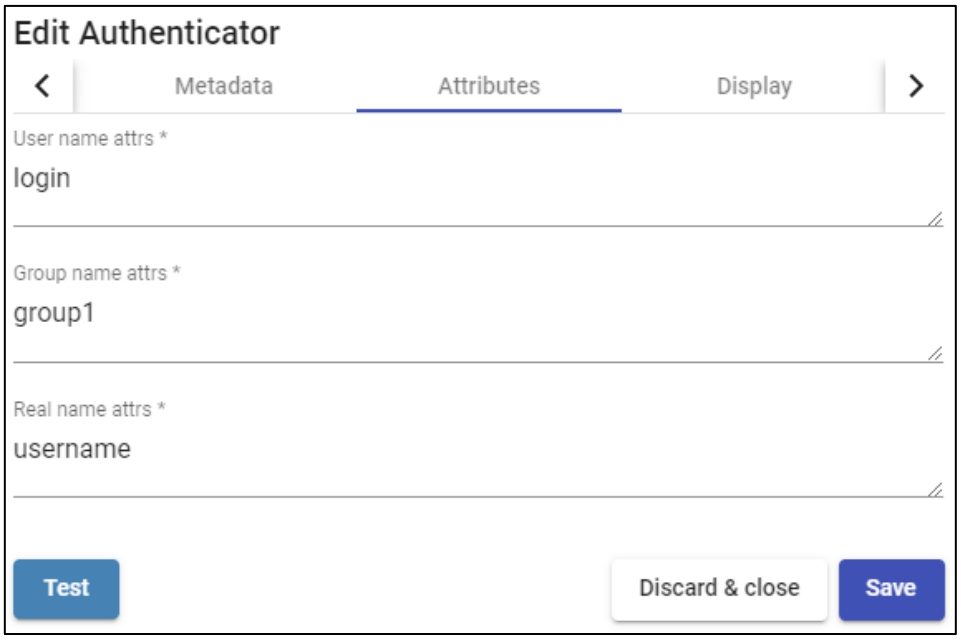


In the "**Attributes**" section indicate the correct attributes. They are defined and visible in the Google SAML extension created in previous steps:



As you can see in the example:

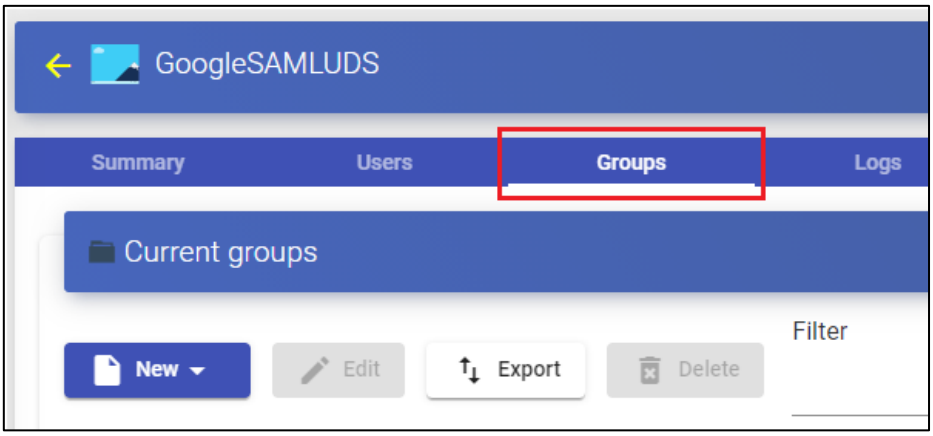
- The previously defined “**login**” attribute, which will be the user's “**primary email**” in Google Workspace, will be used to log in to UDS Enterprise, since it is defined in “**User name attrs**”.
- The “**username**” attribute, which will be the “**First name**” of the username in Google Workspace, will be used in UDS Enterprise to display the user's name. It is defined in "**Real name attrs**".
- The attribute "**group1**", which will be the "**Department**" to which a user belongs in Google Workspace, will be used in UDS Enterprise as the group to which the users belong. It is defined in "**Group name attrs**".



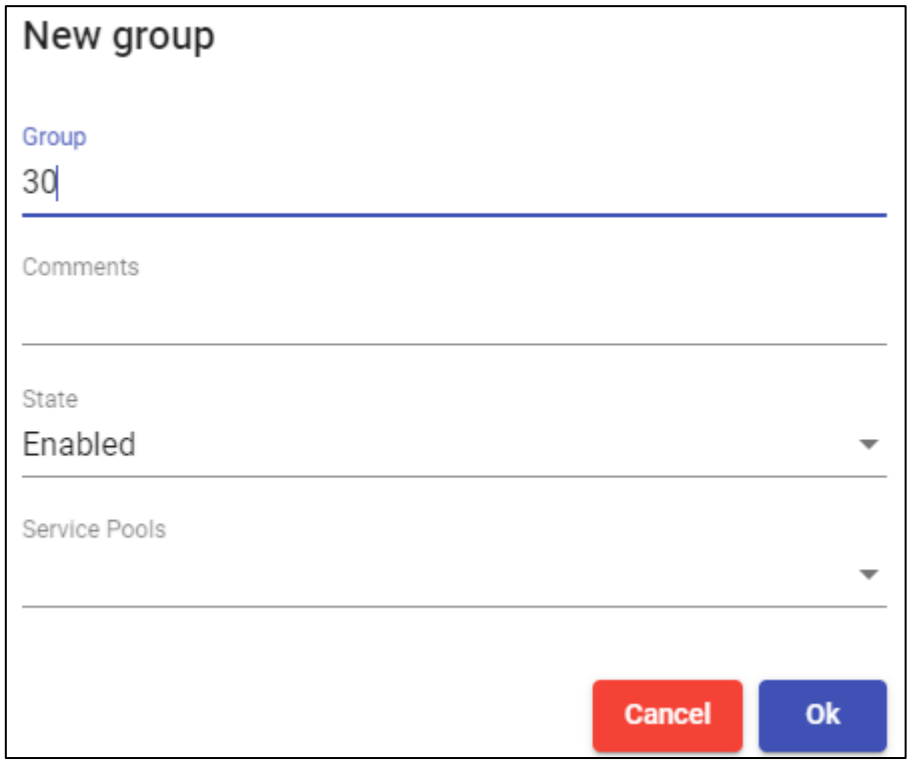
NOTE: In UDS Enterprise it is possible to indicate various attributes or use regular expressions. For example, to indicate new group membership attributes.

Once the attributes are correctly defined, save and access the authenticator created in UDS Enterprise.

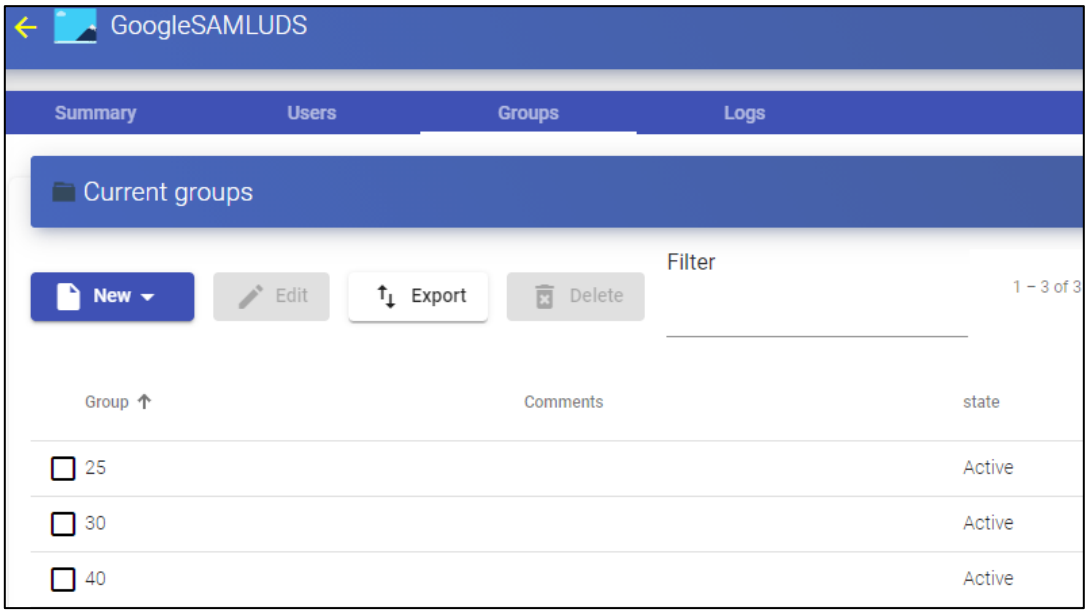
Within the authenticator, access the "**Groups**" section to add the necessary groups.



The groups will have to be added manually since the automatic search does not apply with this type of authenticator:



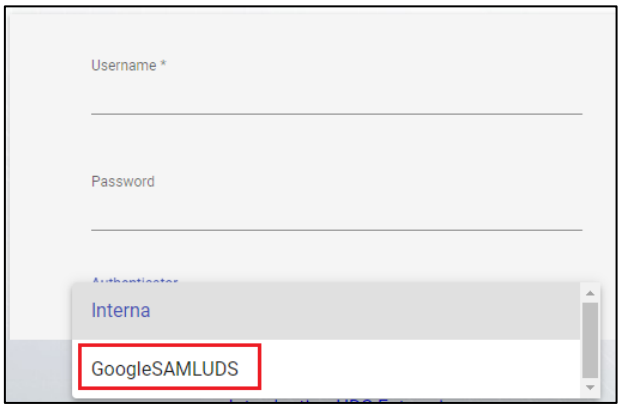
Add all the necessary groups (in this example, the different departments to which the users belong are added, since the group membership attribute used in Google Workspace is the "**department**"):



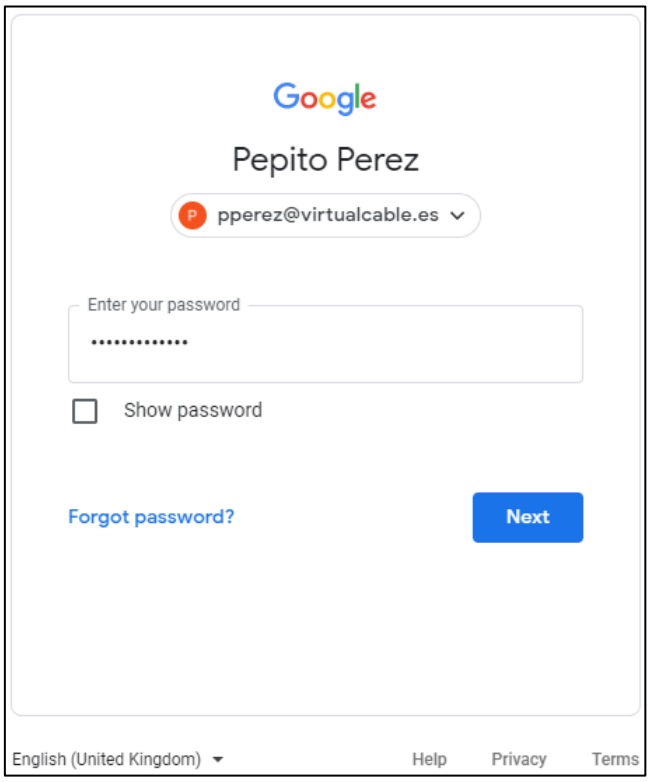
With the configuration applied in this example, all users who have a value of 25, 30 or 40 in their "**department**" attribute, will be able to log in to the UDS Enterprise platform.

Access through authenticator

To confirm that all settings are correct, access UDS Enterprise portal through the newly created SAML authenticator:

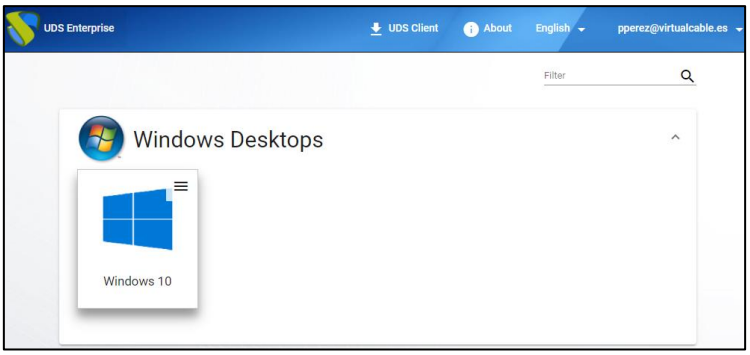


By selecting the SAML authenticator, you will automatically be redirected to the provider's page. The system will ask you for valid credentials:



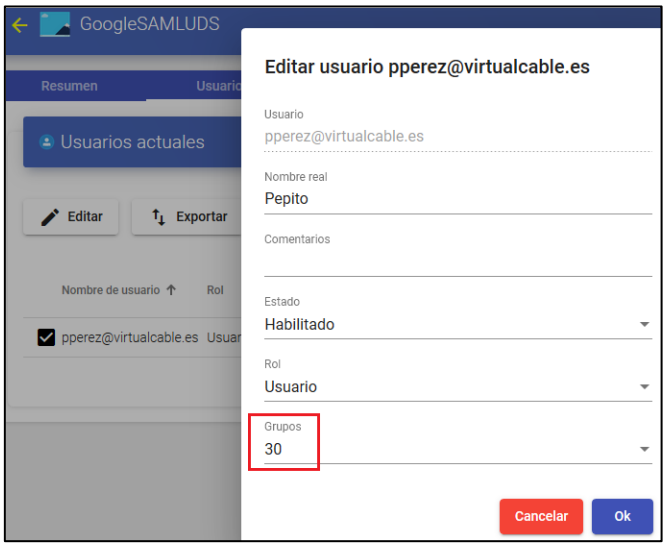
NOTE: The validation mode will be the one configured in the provider itself. That is, if you have user validation via MFA, it will be used.

Once you have log in Google Workspace, a redirection will be made and you will return to the UDS Enterprise services page:



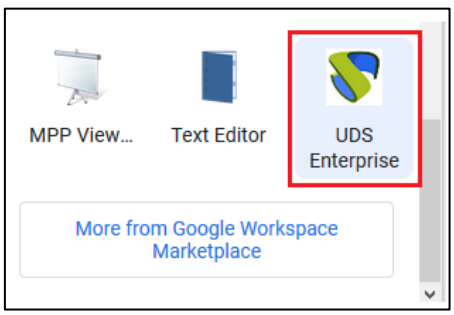
NOTE: If the group to which the user belongs has services assigned, they will be shown to him and he will be able to access them.

You can check which groups a user belongs to if you edit it. To do this, access the authenticator and edit the user:



You can verify that in this example, the user *pperez* belongs to department 30 and, since he is registered as a group in the authenticator, he can access.

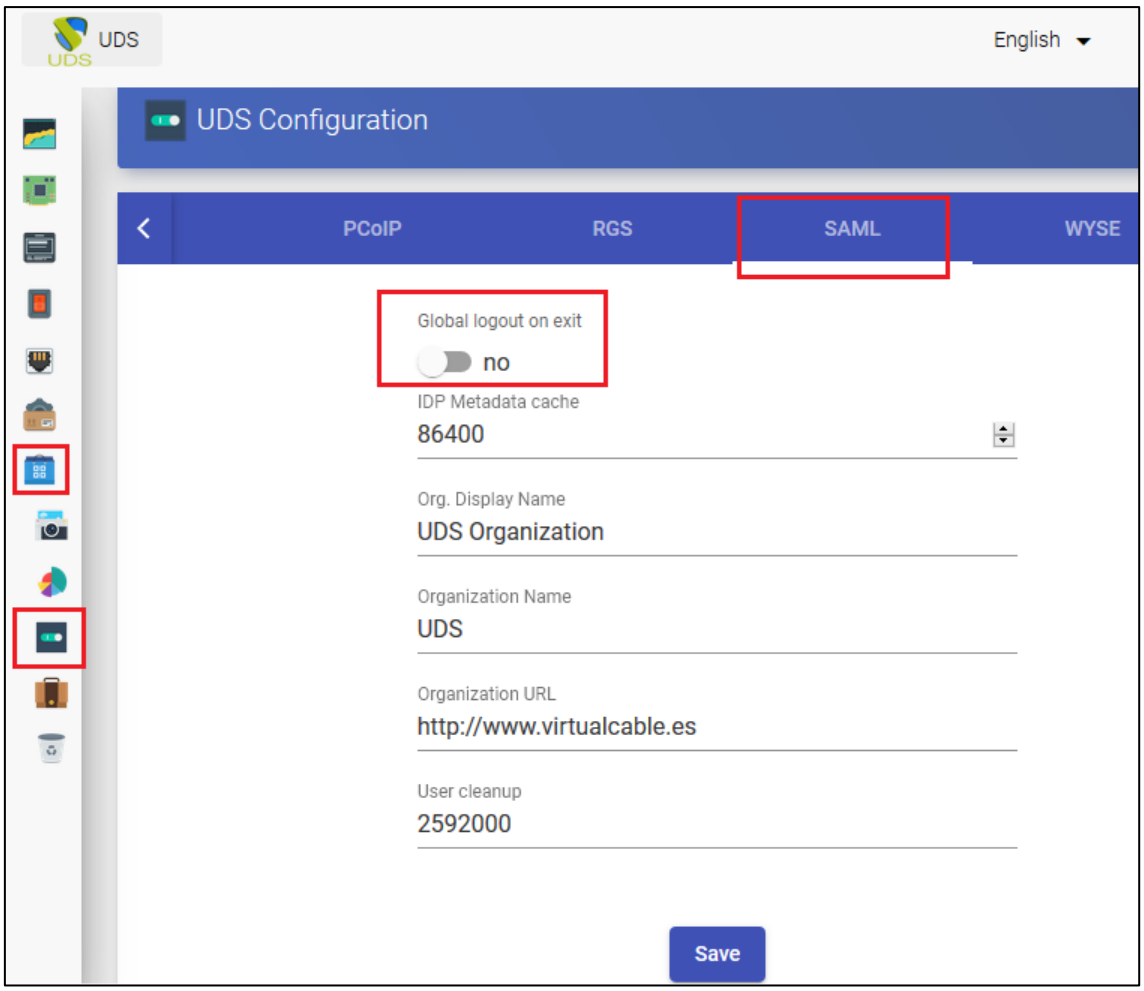
If you have enabled your users' access to the application, it will also appear in the list of Google Workspace applications and you will automatically access the VDI environment after validation:



Enable Global logout

It should be kept in mind that when a user accesses from UDS Enterprise and logs in with his Google account, when he closes his session from UDS, his Google account won't be closed by default. If you want to make a global logout (both from UDS and from the Google account), you will need to indicate it in the UDS Enterprise administration:

Access the UDS Enterprise administration, section "**Tools**" - "**Configuration**", "**SAML**" tab, parameter "**Global logout on exit**":



Once the global logout is enabled, it is necessary to save the changes and restart the UDS servers (UDS-Server machines) or their services (uds and udsweb) for the changes to be applied.

About Virtual Cable

Virtual Cable develops and markets UDS Enterprise through a subscription model according to the number of users, including support and updates.

In addition, Virtual Cable offers professional services to install and configure UDS Enterprise.

For more information, visit http://www.udsenterprise.com or email us at info@udsenterprise.