



Google Workspace user authentication in UDS 4.0



#SmartDigitalWorkplace

VIRTUAL CABLE

Index

Introduction	2
Creation of Google's SAML application.....	2
Creating the SAML authenticator	5
Configuring the SAML application.....	9
Defining attributes in SAML	13
Access through authenticator	17
Global logout.....	20
THE SMART DIGITAL WORKPLACE SOLUTION BY VIRTUAL CABLE.....	21
About UDS Enterprise.....	21
About Virtual Cable.....	21

Introduction

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

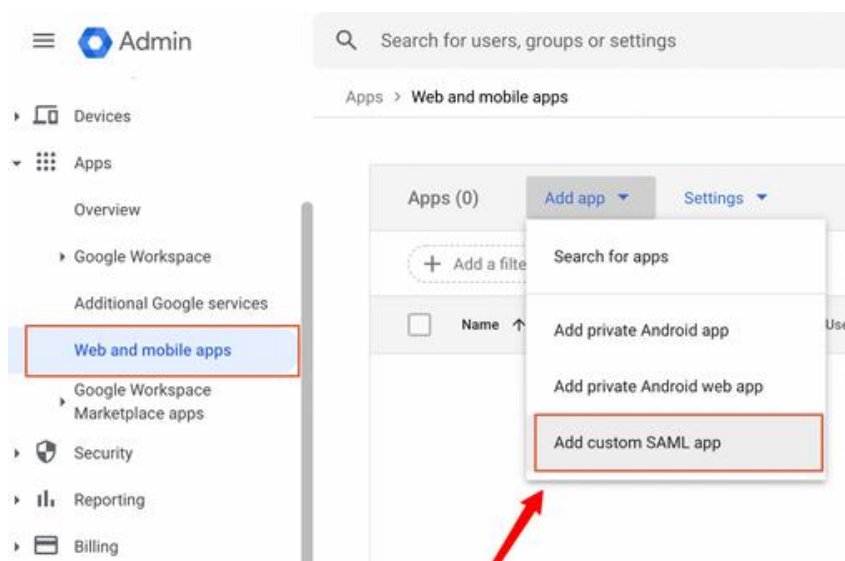
Once the new authenticator has been created in UDS Enterprise and integrated with Google Workspace, existing users in this environment will be able to access the services published in UDS Enterprise.

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.

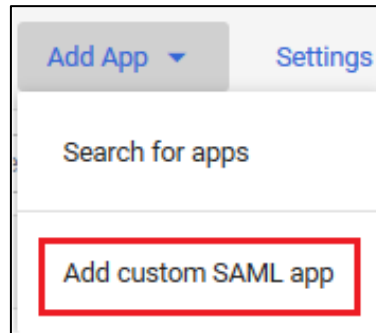
Creation of Google’s SAML application

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

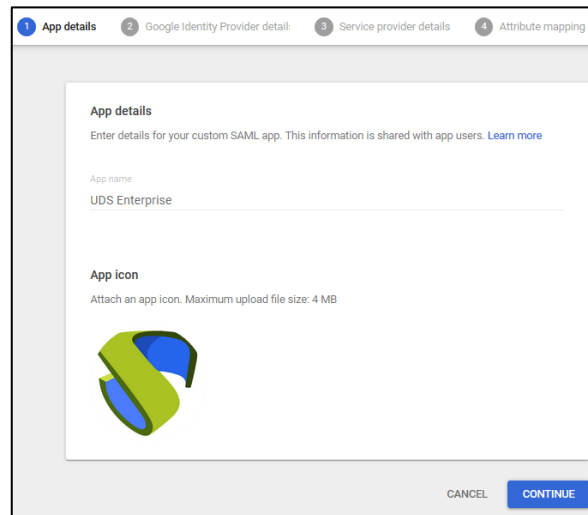
Access into the Google Workspace administration dashboard and select **“Add custom SAML app”**.



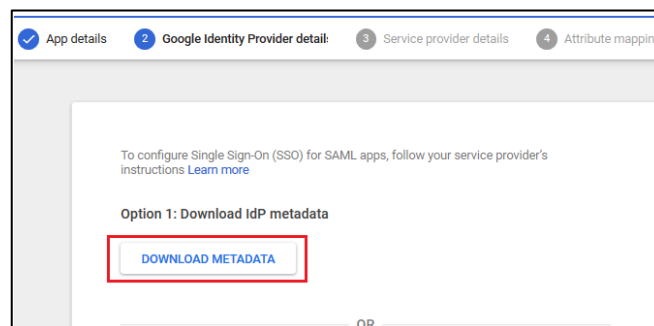
Register a new custom SAML application:



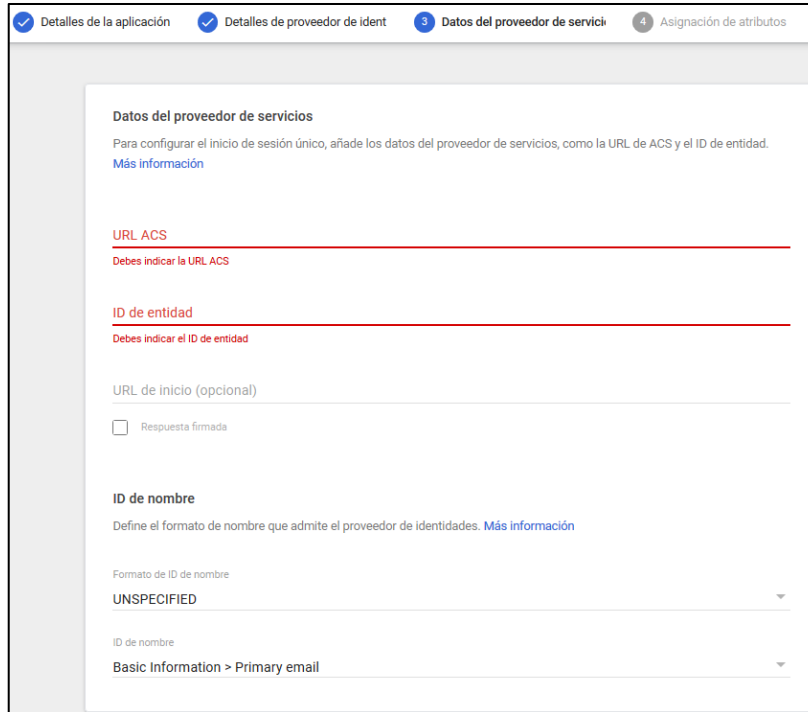
Indicate a name to identify the application in the configuration wizard. It is possible to add an icon so that users can easily find the service.



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":



The screenshot shows a configuration wizard with four steps: 1. Detalles de la aplicación, 2. Detalles de proveedor de ident, 3. Datos del proveedor de servicio (active), and 4. Asignación de atributos.

Datos del proveedor de servicios
 Para configurar el inicio de sesión único, añade los datos del proveedor de servicios, como la URL de ACS y el ID de entidad. [Más información](#)

URL ACS
 Debes indicar la URL ACS

ID de entidad
 Debes indicar el ID de entidad

URL de inicio (opcional)

Respuesta firmada

ID de nombre
 Define el formato de nombre que admite el proveedor de identidades. [Más información](#)

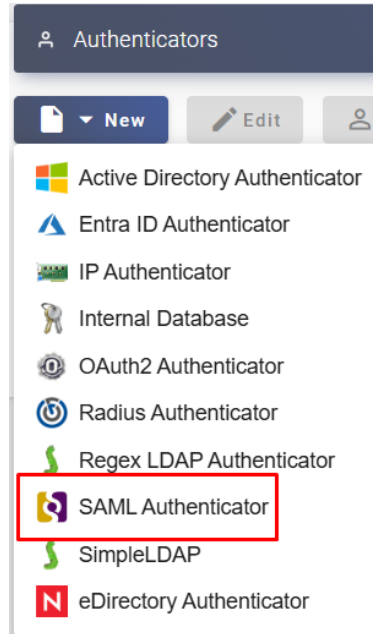
Formato de ID de nombre
 UNSPECIFIED

ID de nombre
 Basic Information > Primary email

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"**.

New Authenticator

< **Main** Certificates Metadata Attributes

Tags
Tags for this element

Name *
GoogleSAMLUDS

Comments

Priority *
1

Label *
google

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

New Authenticator

< Main Certificates Metadata Attributes Advanced

Private key *

Certificate *

Test

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:

```
root@broker-400:~# openssl req -new -newkey rsa:2048 -days 3650 -x509 -nodes -keyout server.key -out server.crt
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
```

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

```
root@broker-400:~# ls
server.crt server.key
root@broker-400:~# █
```

Now convert the key to **rsa** :

```
root@broker-400:~# openssl rsa -in server.key -out server_rsa.key
writing RSA key
root@broker-400:~# █
```

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

```
root@broker-400:~# ls
server.crt server.key server_rsa.key
root@broker-400:~# █
```

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

Edit Authenticator

<
Main
Certificates
Metadata
Attributes
Advanced
Security
Orga >

Private key *

```
-----BEGIN RSA PRIVATE KEY-----
MIIJKQIBAAKCAgEAsomi1KMSISyBCcy6XjkDB1Dd9qlwPzOgwTEiUwD3jRFq5IRU
7nejO7WqTalN5wUeTfl3aZcK7pe3KpysAtRrTwXTfGGJeiVwiaZ0MFkXsicPfeEO
O9j6MQGT3CA74mamRoGE75e4ZZ4uZ4VQL6CmpaKXtkrRcyjY2BLL/gI8530MkbH
hf6PV7BwBEq5AesWbVDvRFXF2DH6/ZAiPRB3nbElstyt5voFeE+SJmTRKJuwbz0C9
```

Certificate *

```
-----BEGIN CERTIFICATE-----
MIIFYDCCA0igAwIBAgIJAI0c5K1qC43qMA0GCSqGSIb3DQEBCwUAMEUxCzAJBgNV
BAYTAkFVMRMwEQYDQQIDApTb211LVN0YXRIMSEwHwyDVQKDBhJbnRlcm5ldCBX
aWRnaXRzIFR0eSRMdG0wHhcNMTRxMTI3MTI1ODI1?WhcNMTkxMTI3MTI1ODI1?WiRF
```

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...):

Edit Authenticator

[Main](#)
[Certificates](#)
[Metadata](#)
[Attributes](#)
[Advanced](#)
[Security](#)
[Orga](#)

IDP Metadata *

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" validUntil="2023-11-10T09:21:07.412Z" cacheDuration="PT48H"
entityID="https://idp.ironchip.com/saml/metadata/646ccaeb36bc936923fc8022">
  <IDPSSODescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
```

Entity ID

ID of the SP. If left blank, this will be autogenerated from server URL

Metadata validity duration

0

Metadata cache duration

0

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.

Edit Authenticator

[Main](#)
[Certificates](#)
[Metadata](#)
[Attributes](#)
[Advanced](#)
[Security](#)
[Orga](#)

IDP Metadata *

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" validUntil="2023-11-10T09:21:07.412Z" cacheDuration="PT48H"
entityID="https://idp.ironchip.com/saml/metadata/646ccaeb36bc936923fc8022">
  <IDPSSODescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
```

Entity ID

<https://demo.udsenterprise.com/uds/page/auth/info/googleSAMLUDS>

Metadata validity duration

0

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.udsenderprise.com/uds/page/auth/info/GoogleSAMLUDS>)

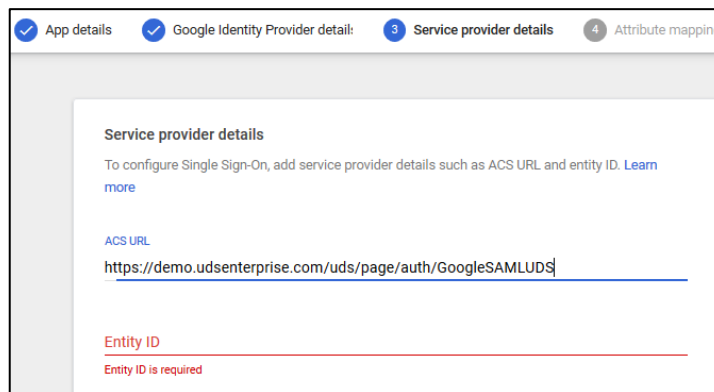
Inside the downloaded file, look for: **AssertionConsumerService**:

```

<md:SingleLogoutService
  Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
  Location="https://demo.udsenderprise.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.udsenderprise.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:

Service provider details

To configure Single Sign-On, add service provider details such as ACS URL and entity ID. [Learn more](#)

ACS URL

Entity ID

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:

✓ App details
✓ Google Identity Provider detail:
✓ Service provider details
4 Attribute mapping

Attributes

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

Google directory attributes

App attributes

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**".

Attributes

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

Google directory attributes		App attributes	
Basic Information >			
Primary email	→	login	×
Basic Information >			
First name	→	username	×
Employee Details >			
Department	→	group1	×

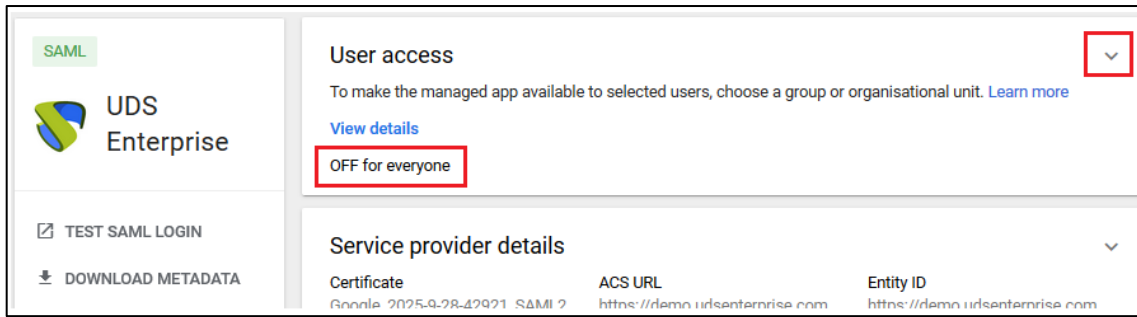
[ADD MAPPING](#)

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

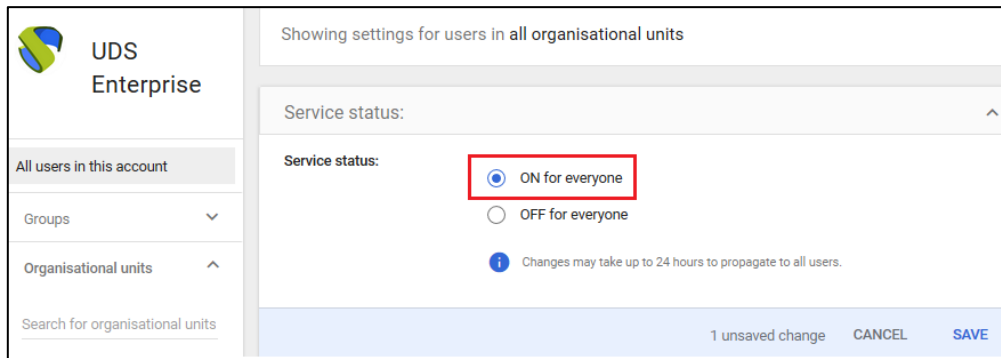
Once the necessary attributes have been selected, finish the wizard.

Apps Add App ▾ Settings ▾					
+ Add a filter					
	Name ↑	Platform	Authentication	User access	Details
<input type="checkbox"/>	UDS Enterprise	Web	SAML	OFF for everyone	Certificate expires on

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.

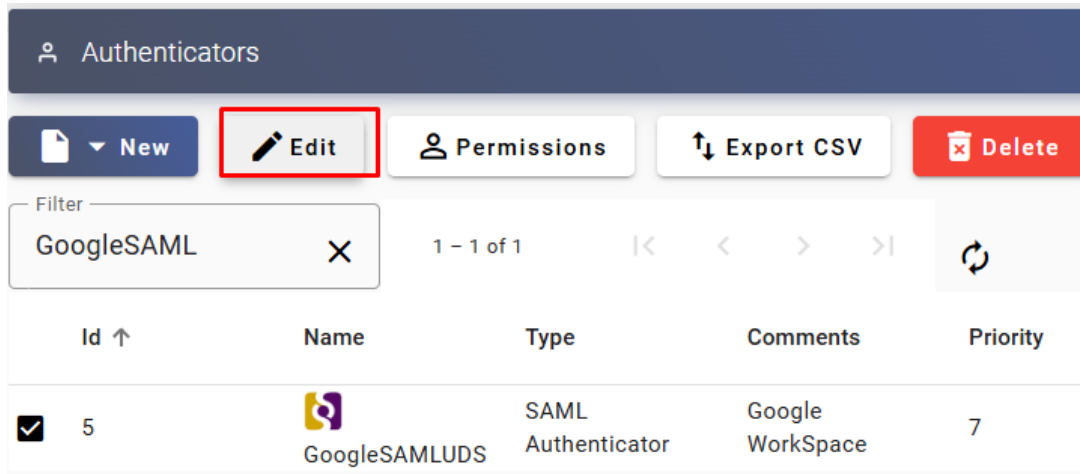


To finish in the groups section we will have to manually specify which groups will have access.

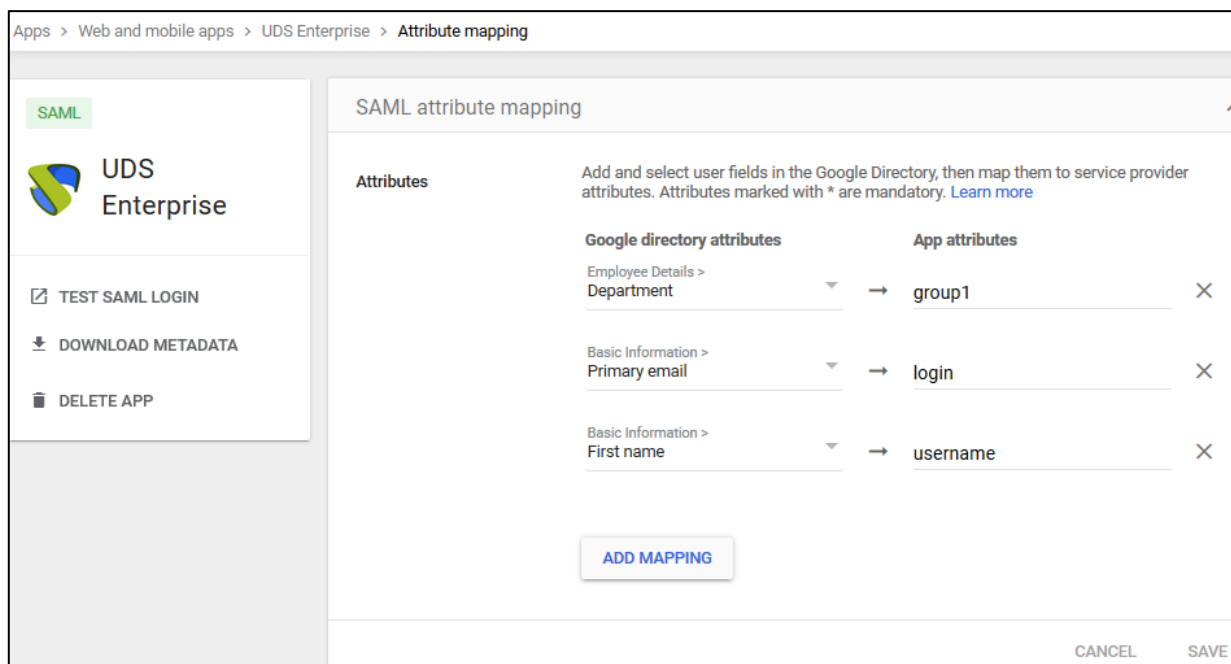
Save to apply the change.

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"**.

Edit Authenticator

< Main Certificates Metadata **Attributes** Advanced

User name attrs *

login

Group name attrs *

grupo1
info

Real name attrs *

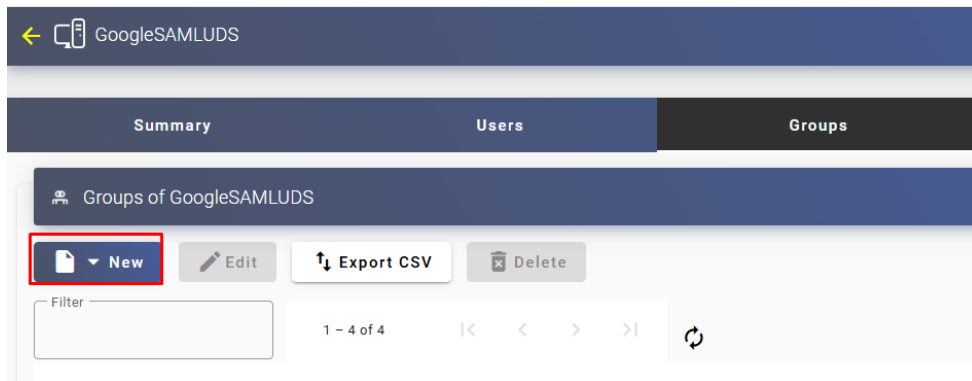
username

Test

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:

New group

Group

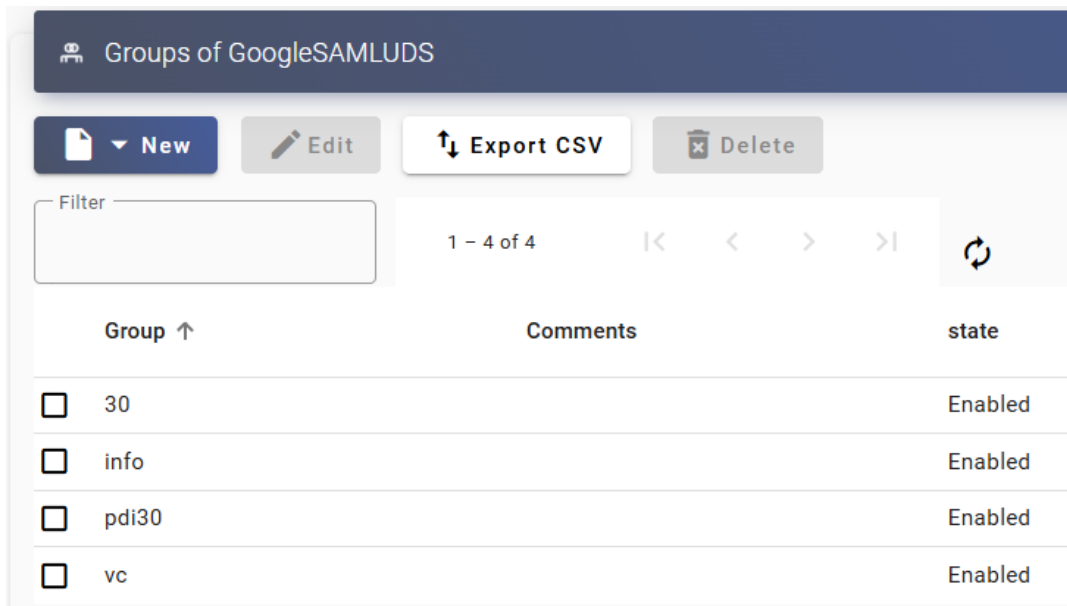
Comments

State

Skip MFA

Service Pools

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"**):

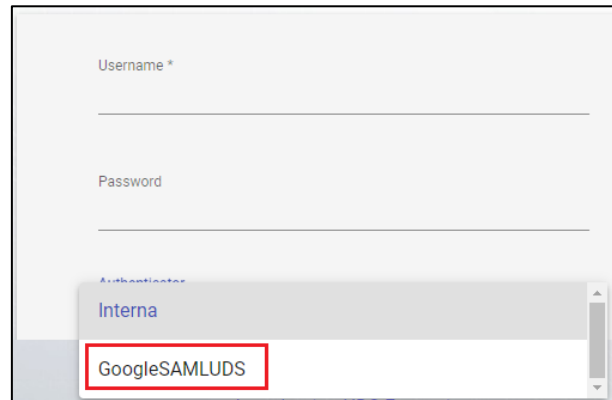


Group ↑	Comments	state
<input type="checkbox"/> 30		Enabled
<input type="checkbox"/> info		Enabled
<input type="checkbox"/> pdi30		Enabled
<input type="checkbox"/> vc		Enabled

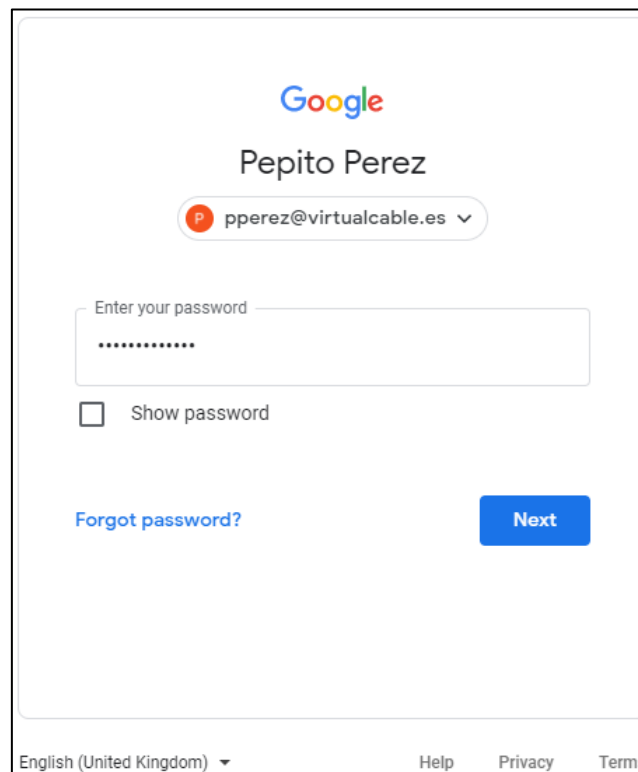
With the configuration applied in this example, all users who have a value of 25, 30 or 40 in their "**department**" attribute, will be able to log in to the UDS Enterprise platform.

Access through authenticator

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

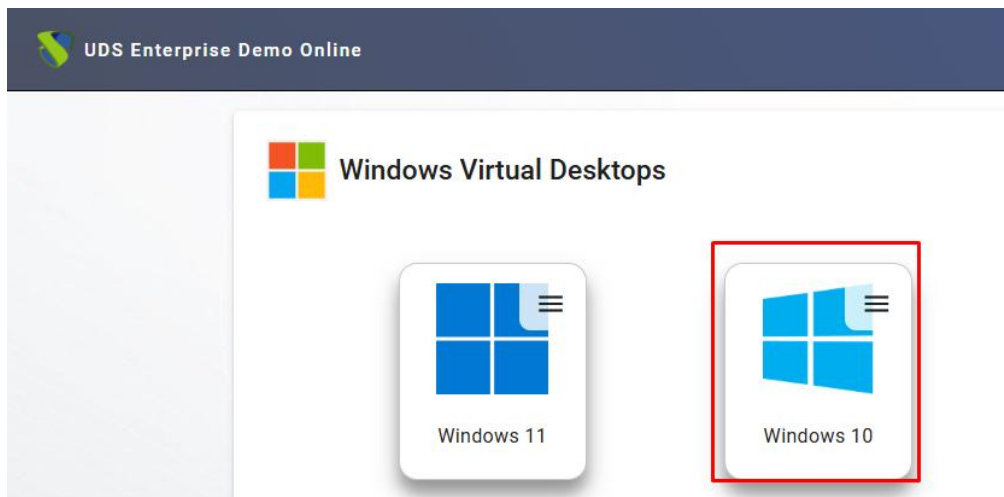


By selecting the SAML authenticator, you will automatically be redirected to the provider's page. The system will ask you for valid credentials:



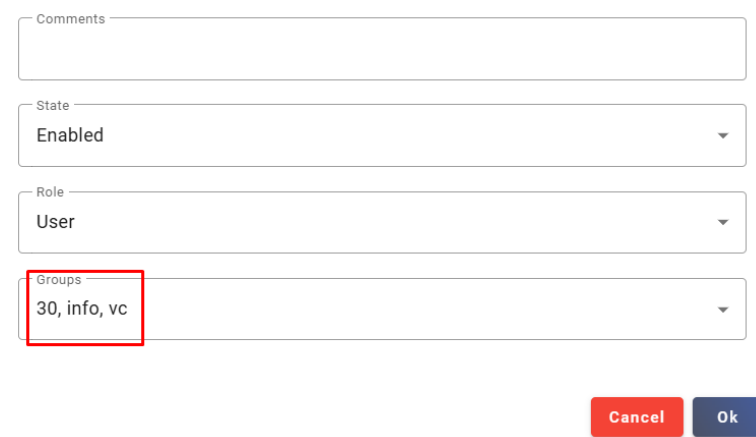
NOTE: The validation mode will be the one configured in the provider itself. That is, if you have user validation via MFA, it will be used.

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:



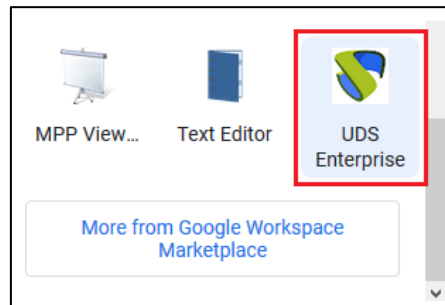
The form contains the following fields:

- Comments:
- State:
- Role:
- Groups: (This field is highlighted with a red border)

Buttons:

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:



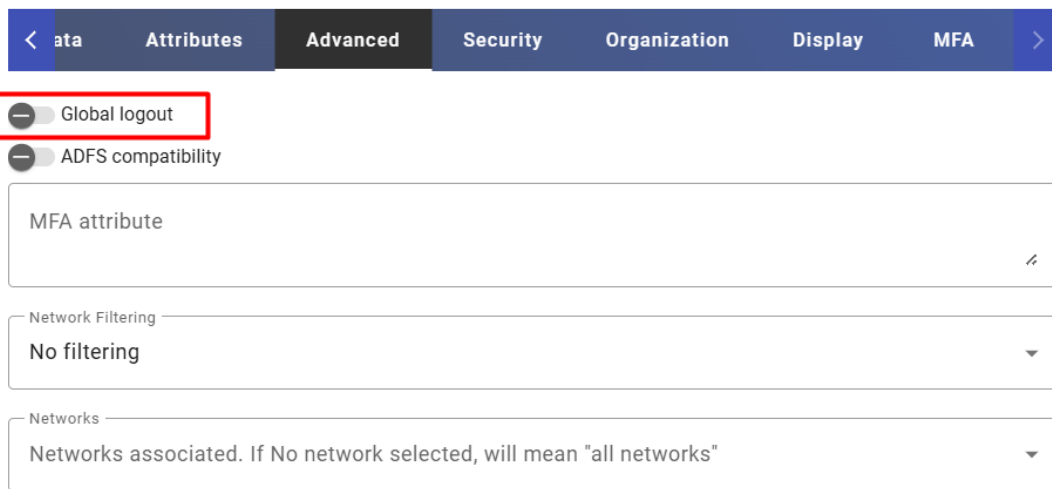
Global logout

The Check Global Logout will allow us not only to log out of UDS but also to the IDP that we have configured, in this case Google is not compatible with this feature so we will have to always have it disabled.

Access the Authenticator, section "**Advanced**".

Parameter "**Global logout**":

Edit Authenticator



The screenshot shows the 'Edit Authenticator' configuration page with the 'Advanced' tab selected. The 'Global logout' toggle is disabled (indicated by a grey circle) and is highlighted with a red rectangular box. Below it, the 'ADFS compatibility' toggle is also disabled. The 'MFA attribute' field is empty. The 'Network Filtering' dropdown is set to 'No filtering'. The 'Networks' dropdown is set to 'Networks associated. If No network selected, will mean "all networks"'. Navigation tabs include 'ata', 'Attributes', 'Advanced', 'Security', 'Organization', 'Display', and 'MFA'.

THE SMART DIGITAL WORKPLACE SOLUTION BY VIRTUAL CABLE

About UDS Enterprise

[UDS Enterprise](#) is a new software concept for creating a **fully customized workplace virtualization** platform. It provides **secure 24x7 access** from **any location and device** to all applications and software of an organization or educational center.

It allows you to combine Windows and Linux **desktop and application virtualization** in a single console, as well **as remote access** to Windows, Linux and macOS computers. Its Open Source base guarantees **compatibility with any third-party technology**. It can be deployed on-premises, in a public, private, hybrid or **multicloud**. You can even combine several environments at the same time and perform automatic and **intelligent overflows** to optimize performance and efficiency. All with a **single subscription**.

About Virtual Cable

[Virtual Cable](#) is a company specialized in the digital **transformation of the workplace**. The company develops, supports and markets UDS Enterprise. It has recently been recognized as an **IDC Innovator in Virtual Client Computing** worldwide. Its team of experts has designed **smart digital workplace solutions (VDI, vApp and remote access to physical computers)** tailored to each sector to provide a unique user experience fully adapted to the needs of each user profile. Virtual Cable professionals have **more than 30 years** of experience in IT and software development and more than 15 years in virtualization technologies. **Everyday millions of Windows and Linux virtual desktops** are deployed with UDS Enterprise around the world.