



Google Workspace user
authentication in
UDS Enterprise 3.5

www.udsenderprise.com



Google Workspace user authentication in UDS Enterprise 3.5

www.udsenderprise.com

Introduction.....	3
Creation of Google's SAML application.....	3
Creating the SAML authenticator	5
Configuring the SAML application	9
Defining attributes in SAML.....	12
Access through authenticator.....	15
Enable Global logout.....	17
About Virtual Cable.....	18



Introduction

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

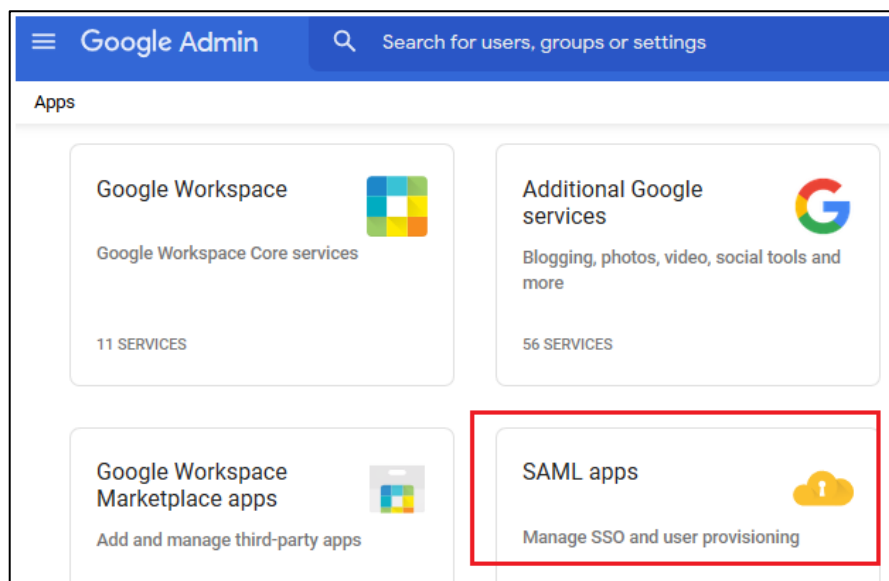
Once the new authenticator has been created in UDS Enterprise and integrated with Google Workspace, existing users in this environment will be able to access the services published in UDS Enterprise.

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.

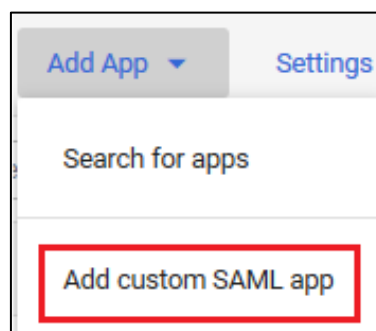
Creation of Google's SAML application

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:





Google Workspace user authentication in UDS Enterprise 3.5

www.udsenderprise.com

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.

1 App details 2 Google Identity Provider detail 3 Service provider details 4 Attribute mapping

App details
Enter details for your custom SAML app. This information is shared with app users. [Learn more](#)

App name
UDS Enterprise

App icon
Attach an app icon. Maximum upload file size: 4 MB

CANCEL CONTINUE

Now download the metadata and continue with the wizard:

App details 2 Google Identity Provider detail 3 Service provider details 4 Attribute mapping

To configure Single Sign-On (SSO) for SAML apps, follow your service provider's instructions. [Learn more](#)

Option 1: Download IdP metadata

[DOWNLOAD METADATA](#)

OR

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

1 Detalles de la aplicación 2 Detalles de proveedor de ident 3 Datos del proveedor de servicio 4 Asignación de atributos

Datos del proveedor de servicios
Para configurar el inicio de sesión único, añada 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

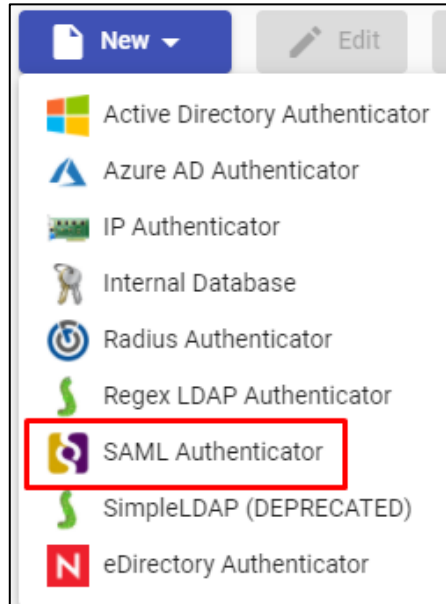
ID de nombre
Basic Information > Primary email

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**”.

The image shows the 'New Authenticator' form in the 'Main' tab. The form has the following fields and values:

- Tags: Tags for this element
- Name *: GoogleSAMLUDS
- Comments: Comments for this element
- Priority *: 1
- Label *: google

At the bottom of the form, there are three buttons: 'Test', 'Discard & close', and 'Save'.

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



Google Workspace user authentication in UDS Enterprise 3.5

www.udsenderprise.com

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@uds3:~# openssl req -new -newkey rsa:2048 -days 3650 -x509 -nodes -keyout server.key -out server.crt  
Generating a RSA private key  
.....+++++  
.....+++++  
.....+++++  
writing new private key to 'server.key'  
-----  
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.  
-----  
Country Name (2 letter code) [AU]:
```

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

```
root@uds3:~# ls  
server.crt server.key  
root@uds3:~#
```

Now convert the key to **rsa** :

```
root@uds3:~# openssl rsa -in server.key -out server_rsa.key  
writing RSA key  
root@uds3:~#
```

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



Google Workspace user authentication in UDS Enterprise 3.5

```
root@uds3:~# ls
server.crt  server.key  server_rsa.key
root@uds3:~#
```

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

New Authenticator

< Main
Certificates
Metadata
Attr >

Private key *

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAACAQEAxNww8X8xpZFpCpysQwP7KcscxgchmrMDahxNLFe3NJB7xQP
CojwrlbuxblXogHIYg7YyMwsHPC+JGKeqQ6/JSrZ5oJy2Xg4QieiROyfunR/BpCO
SdOoEVeFRSno9W1G+y3jZ/Kg5orwoGhxd50cBb7dhV+4AhYWP3Pg6XeYbWnPfJd
F11JxPx Ae5Q/GCCB1nxwcVGrRFGdaqBawRNAj3ARTwuA9ImjSLjQgzKuJEvAezU
5GYNwvbt5lJOZgAwm+/QMcQ/vN4W7c4sPyqM9MQFWDwyw/8emISLJMOpDLQ2z0
sF
R7hc8y/vDKQ/me2kwc8LiQOrE8iLV4hp+wkB LIQIDAQABoIRAHPS17006B4TPbA7
-----
```

Certificate *

```
-----BEGIN CERTIFICATE-----
MIIDjTCCAnWgAwIBAgIUWGULOMR5U1bISZVRddYUEoE5OIwDQYJKoZIhvcNAQEL
BQAwwVjELMAKGA1UEBhMCZXMxEzARBgNVBAgMCINvbWUtU3RhdGUxZDZANBgNBV
AcM
Bm1hZHJpZDEhMB8GA1UECgwYSW50ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMB4XDTE
x
MDQvOTM0MjAxOFEwYXNja3RARTwuA9ImjSLjQgzKuJEvAezU
-----
```

Test
Discard & close
Save

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...):

New Authenticator

< Certificates
Metadata
Attributes
Display >

IDP Metadata *

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="https://accounts.google.com/o/saml2?idpid=C04czxd53" validUntil="2025-
09-28T11:29:21.000Z">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="false"
-----
```

Entity ID

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

Test
Discard & close
Save



Google Workspace user authentication in UDS Enterprise 3.5

www.udsenderprise.com

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** Attr >

IDP Metadata *

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
```

Entity ID

<https://demo.udsenderprise.com/uds/page/auth/info/GoogleSAMLUDS>

Test Discard & close Save



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”:

App details Google Identity Provider detail: 3 Service provider details 4 Attribute mapping

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

Entity ID is required

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



Google Workspace user authentication in UDS Enterprise 3.5

www.udsenderprise.com

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:

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

ADD MAPPING

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



Google Workspace user authentication in UDS Enterprise 3.5

www.udsenderprise.com

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.

Apps		Add App	Settings		
+ Add a filter					
<input type="checkbox"/>	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:

SAML

UDS Enterprise

TEST SAML LOGIN

DOWNLOAD METADATA

User access ▼

To make the managed app available to selected users, choose a group or organisational unit. [Learn more](#)

[View details](#)

OFF for everyone

Service provider details ▼

Certificate	ACS URL	Entity ID
Google 2025-9-28-42921 SAML 2	https://demo.udsenderprise.com	https://demo.udsenderprise.com

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

UDS Enterprise

Showing settings for users in all organisational units

Service status: ^

Service status:

ON for everyone

OFF for everyone

Changes may take up to 24 hours to propagate to all users.

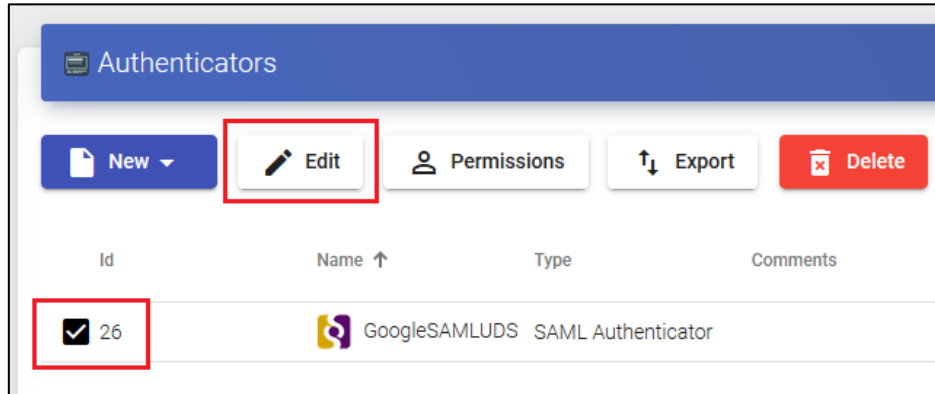
1 unsaved change CANCEL SAVE

Save to apply the change.

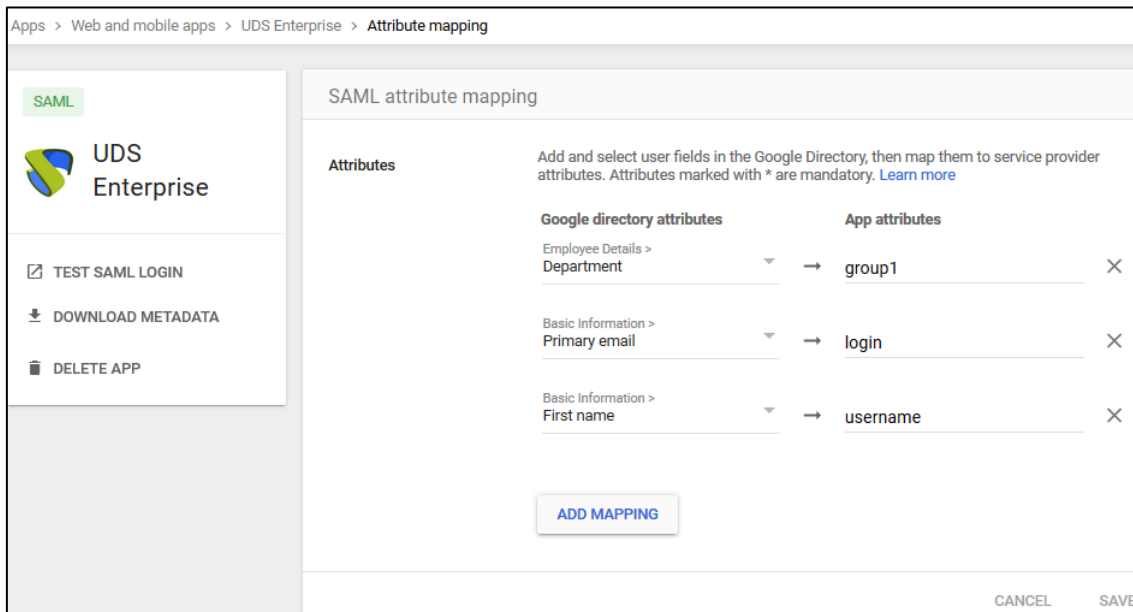


Defining attributes in SAML

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”.



Google Workspace user authentication in UDS Enterprise 3.5

www.udsenderprise.com

Edit Authenticator

< Metadata **Attributes** Display >

User name attrs *
login

Group name attrs *
group1

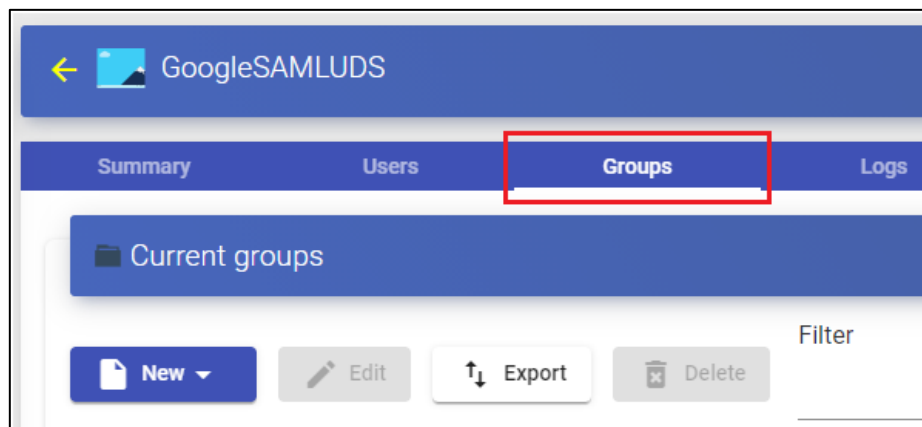
Real name attrs *
username

Test Discard & close Save

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.





Google Workspace user authentication in UDS Enterprise 3.5

www.udsenderprise.com

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

New group

Group
30

Comments

State
Enabled

Service Pools

Cancel Ok

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**"):

GoogleSAMLUDS

Summary Users **Groups** Logs

Current groups

New Edit Export Delete Filter 1 - 3 of 3

Group ↑	Comments	state
<input type="checkbox"/> 25		Active
<input type="checkbox"/> 30		Active
<input type="checkbox"/> 40		Active

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:

The screenshot shows a login form with the following elements:

- Username * (input field)
- Password (input field)
- Authenticator dropdown menu with the following options:
 - Interna
 - GoogleSAMLUDS (highlighted with a red box)

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

The screenshot shows the Google authentication page for Pepito Perez. The page includes the following elements:

- Google logo
- User name: Pepito Perez
- Email address: pperez@virtualcable.es (with a dropdown arrow)
- Enter your password (input field with masked characters)
- Show password checkbox (unchecked)
- Forgot password? (link)
- Next (button)
- Language: English (United Kingdom) (dropdown)
- Help, Privacy, Terms (links)

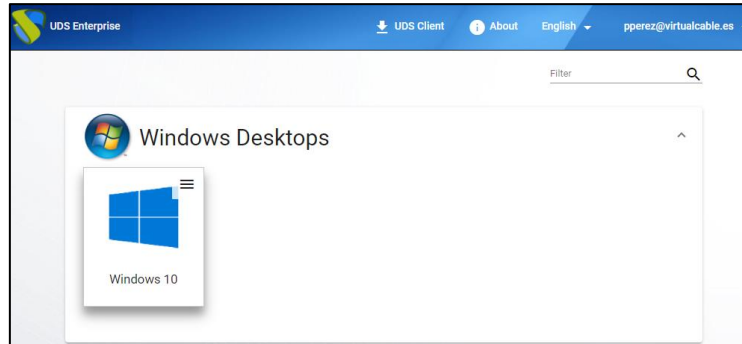
NOTE: The validation mode will be the one configured in the provider itself. That is, if you have user validation via MFA, it will be used.



Google Workspace user authentication in UDS Enterprise 3.5

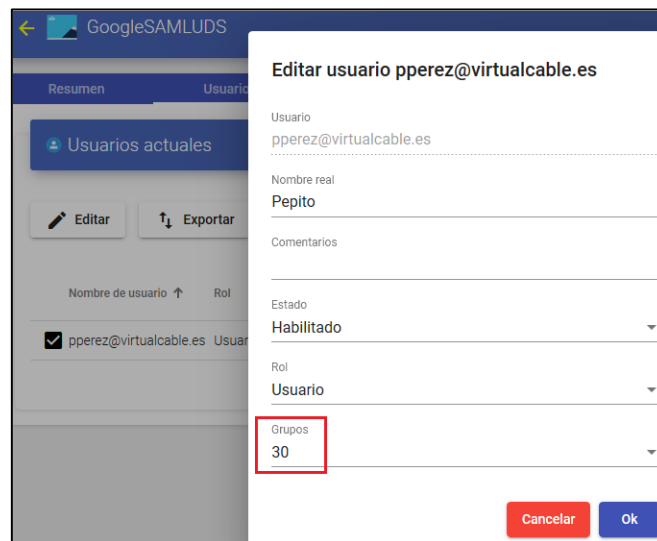
www.udsenderprise.com

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



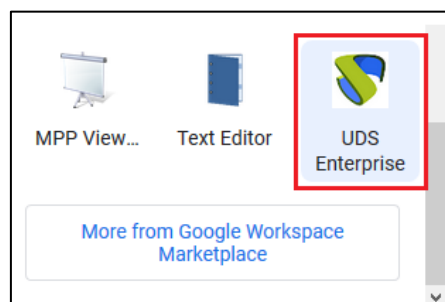
NOTE: If the group to which the user belongs has services assigned, they will be shown to him and he will be able to access them.

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**":

The screenshot shows the UDS Configuration interface. The top navigation bar includes 'UDS Configuration' and tabs for 'PCoIP', 'RGS', 'SAML', and 'WYSE'. The 'SAML' tab is selected and highlighted with a red box. On the left sidebar, the 'Tools' icon is highlighted with a red box. The main content area displays the 'Global logout on exit' toggle, which is currently set to 'no' and is also highlighted with a red box. Below this, the 'IDP Metadata cache' is set to '86400', 'Org. Display Name' is 'UDS Organization', 'Organization Name' is 'UDS', 'Organization URL' is 'http://www.virtualcable.es', and 'User cleanup' is '2592000'. A 'Save' button is located at the bottom right of the configuration area.

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.



Google Workspace user authentication in UDS Enterprise 3.5

www.udsenderprise.com

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.udsenderprise.com> or email us at info@udsenderprise.