



Autenticación de usuarios  
de Google Workspace en  
**UDS Enterprise 3.5**

[www.udsenderprise.com](http://www.udsenderprise.com)



# Autenticación de usuarios de Google Workspace en **UDS Enterprise 3.5**

[www.udsenderprise.com](http://www.udsenderprise.com)

Introducción .....	3
Creación de aplicación SAML de Google.....	3
Creación del autenticador SAML .....	6
Configuración de la aplicación SAML.....	10
Definición de atributos en SAML.....	13
Acceso a través del autenticador .....	16
Habilitar Global logout.....	19
Sobre Virtual Cable.....	20



## Introducción

El presente documento muestra cómo realizar la integración de un autenticador de tipo SAML de UDS Enterprise 3.5 para validar usuarios existentes en Google Workspace.

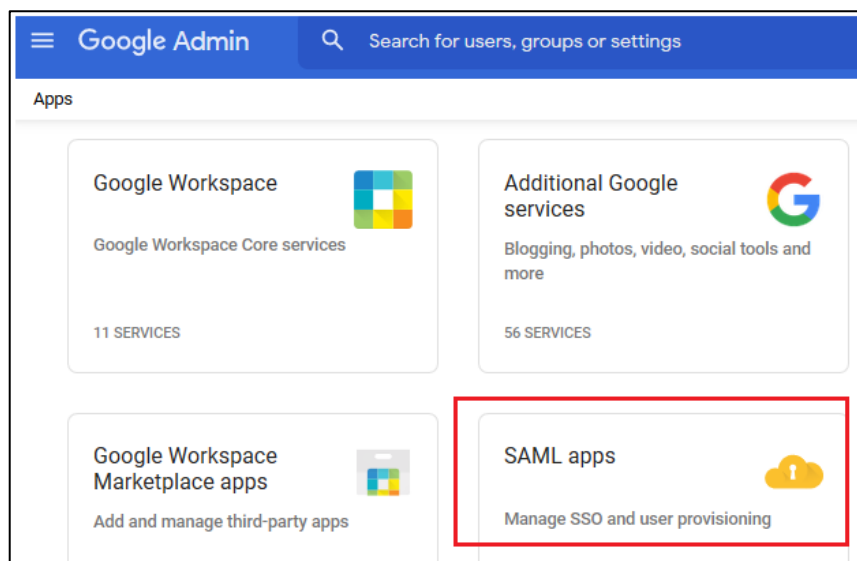
Una vez creado el nuevo autenticador en UDS Enterprise e integrado con Google Workspace, los usuarios existentes en este entorno podrán acceder a los servicios publicados en UDS Enterprise.

Para poder realizar esta integración, será necesario disponer de un usuario dado de alta en UDS Enterprise y un usuario de la plataforma Google Workspace, ambos con permisos de administración sobre sus diferentes entornos.

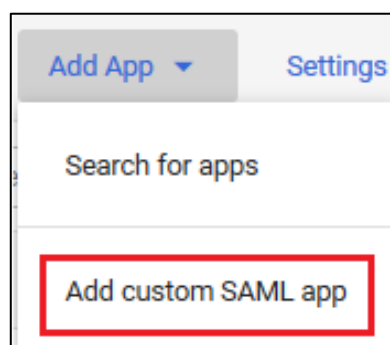
## Creación de aplicación SAML de Google

La primera tarea la realizaremos en el panel de administración de Google Workspace. Necesitaremos un usuario con permisos de administración.

Accedemos al panel de administración de Google Workspace y seleccionamos “**SAML apps**”.



Deberemos dar de alta una nueva aplicación SAML personalizada:





# Autenticación de usuarios de Google Workspace en UDS Enterprise 3.5

www.udsenderprise.com


En el asistente de configuración indicamos un nombre para identificar la aplicación y podremos añadir un icono para que los usuarios puedan localizar el servicio fácilmente.

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

Ahora descargamos los metadatos y continuamos el asistente:

App details Google Identity Provider detail Service provider details 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

En el paso 3 del asistente, deberemos indicar la "URL ACS" y el "ID de entidad":

Detalles de la aplicación Detalles de proveedor de ident Datos del proveedor de servicio 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



# Autenticación de usuarios de Google Workspace en **UDS Enterprise 3.5**

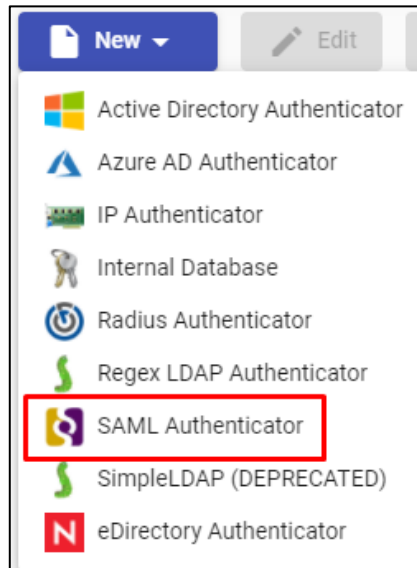
[www.udsenderprise.com](http://www.udsenderprise.com)

Para obtener estos datos, deberemos acceder a la administración de nuestro entorno UDS Enterprise y crear un nuevo autenticador de tipo SAML. Una vez tengamos los datos, seguiremos completando los diferentes apartados del asistente hasta su finalización.



## Creación del autenticador SAML

Accedemos a la administración de UDS Enterprise y nos situamos en el apartado “**Authenticators**”, seleccionamos “**New**” y elegimos “**SAML Authenticator**”.



En la pestaña “**Main**” indicaremos un nombre para el autenticador (no puede contener espacios), la prioridad y un “**Label**”.

New Authenticator				
<	Main	Certificates	Metadata	Attr >
Tags				
Tags for this element				
Name *				
GoogleSAMLUDS				
Comments				
Comments for this element				
Priority *				
1				
Label *				
google				
Test		Discard & close		Save

En la pestaña “**Certificates**” deberemos indicar un certificado válido y su clave. Tienen que estar en formato PEM:



# Autenticación de usuarios de Google Workspace en UDS Enterprise 3.5

www.udsenderprise.com

The screenshot shows a web form titled 'New Authenticator' with a navigation bar containing 'Main', 'Certificates', 'Metadata', and 'Attr'. The 'Certificates' tab is selected. Below the navigation bar are two text input fields labeled 'Private key \*' and 'Certificate \*'. At the bottom of the form are three buttons: 'Test', 'Discard & close', and 'Save'.

Si no se dispone de certificados, se puede generar uno con **OpenSSL**. Para generarlo, utilizaremos la siguiente sentencia (el servidor de UDS tiene instalado **OpenSSL**, puede utilizarse esta máquina para generar el certificado):

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

Once the certificate is generated, we must share the key with RSA, for this, we will use the following command:

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

Ejemplo de generación de certificado:

```
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]:
```

Ejecutamos el comando y completamos los datos necesarios para generar el certificado:

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

Ahora convertimos la clave a **rsa**:

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

Copiaremos el contenido del fichero del certificado y de la clave **rsa** en UDS:

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







# Autenticación de usuarios de Google Workspace en UDS Enterprise 3.5

www.udsenderprise.com

El apartado “**Entity ID**” lo dejaremos vacío, puesto que se rellenará automáticamente cuando guardemos el autenticador. Los datos se generarán en base a la URL utilizada en la conexión con el portal de UDS Enterprise.

Guardamos el autenticador (deberemos indicar cualquier dato en la pestaña “**Attributes**” para que nos permita guardar. En los siguientes pasos volveremos a este apartado y se aplicará la configuración definitiva) y al volver a editarlo podremos obtener los datos del “**Entity ID**” necesarios para poder seguir configurando la aplicación personalizada SAML en la consola de Google.

**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



## Configuración de la aplicación SAML

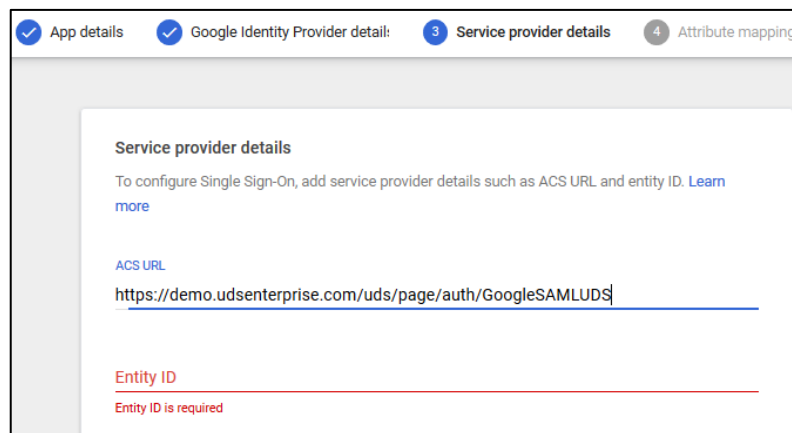
Retomamos el paso 3 del asistente de configuración de Google para crear una aplicación SAML personalizada, donde nos pedirá la “URL ACS” y el “ID de entidad”.

Para indicar los datos ACS (Assertion Consumer Service), descargaremos el fichero “**Entity ID**” que ha generado UDS automáticamente al guardar el autenticador (pondremos la URL indicada en un navegador y lo descargaremos. En este ejemplo sería: <https://demo.udsenderprise.com/uds/page/auth/info/GoogleSAMLUDS>)

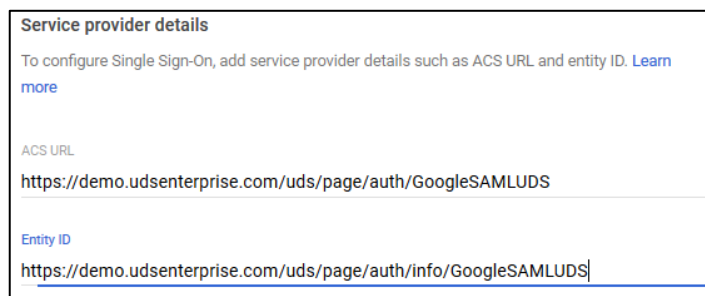
Dentro del fichero descargado, buscaremos: **AssertionConsumerService**

```
<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>
```

Copiaremos la URL facilitada en el campo “URL ACS”:



Por último, para terminar de configurar el paso 3, indicaremos el “ID de entidad”. Será el autogenerated por UDS Enterprise en el campo “Entity ID” de la pestaña “Metadata” del autenticador:





# Autenticación de usuarios de Google Workspace en UDS Enterprise 3.5

www.udsenderprise.com

Dejaremos el resto de opciones por defecto y seguimos con el paso 4. Ahí definiremos los atributos que serán utilizados por UDS Enterprise para validar usuarios y configurar grupos:

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

ADD MAPPING

En este ejemplo se utilizarán los siguientes atributos:

- Para realizar el login del usuario se usará el “**Primary email**”, el cual lo etiquetaremos como “**login**”.
- Para mostrar el nombre del usuario, utilizaremos “**First name**”, el cual lo etiquetaremos como “**username**”.
- Para definir la pertenencia a grupos de los usuarios, utilizaremos “**Department**”, el cual lo etiquetaremos como “**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	×

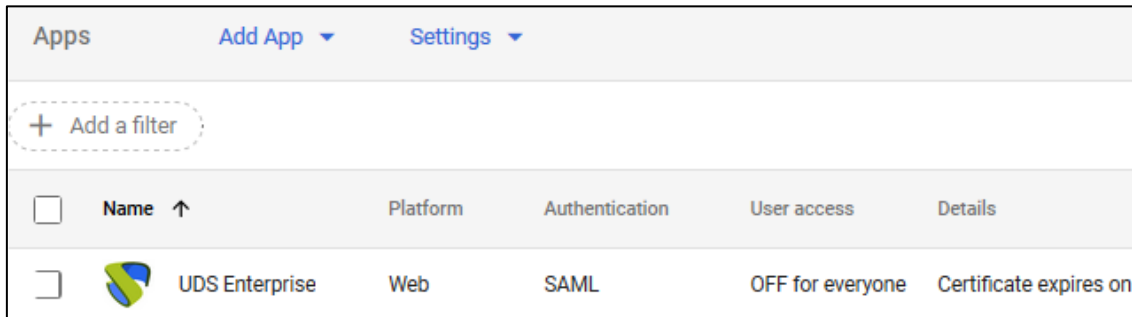
ADD MAPPING



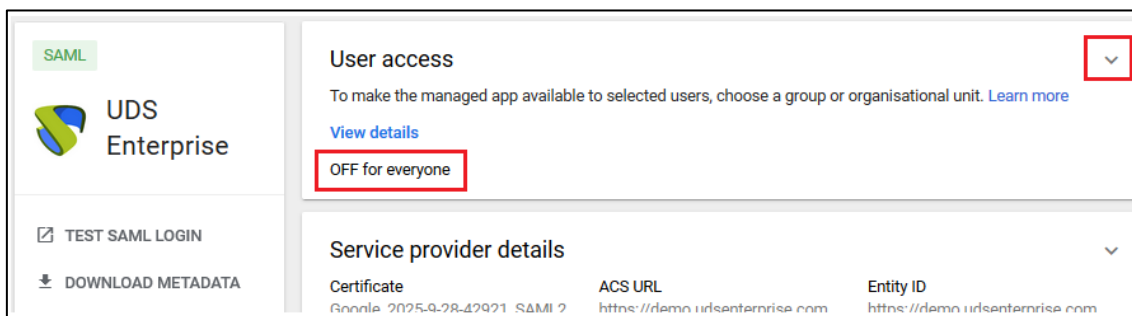
# Autenticación de usuarios de Google Workspace en UDS Enterprise 3.5

Podremos utilizar o añadir atributos personalizados. En este ejemplo se usarán los atributos por defecto facilitados por Google.

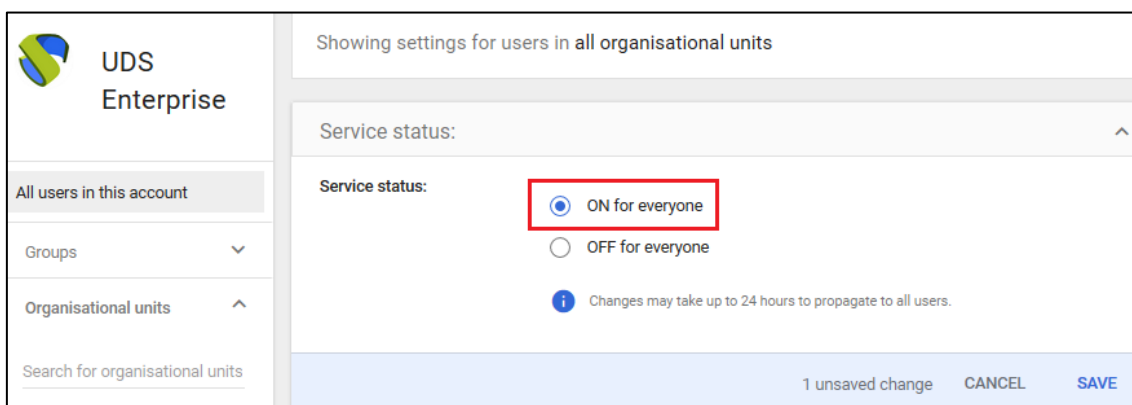
Una vez seleccionados los atributos necesarios, finalizaremos el asistente.



Si entramos en la aplicación creada, veremos que por defecto está desactivada para todos los usuarios y deberemos habilitarla. Para ello accedemos a las opciones de “**User Access**”:



En este ejemplo la aplicación estará activada para todos los usuarios, pero es posible acotar por grupos.

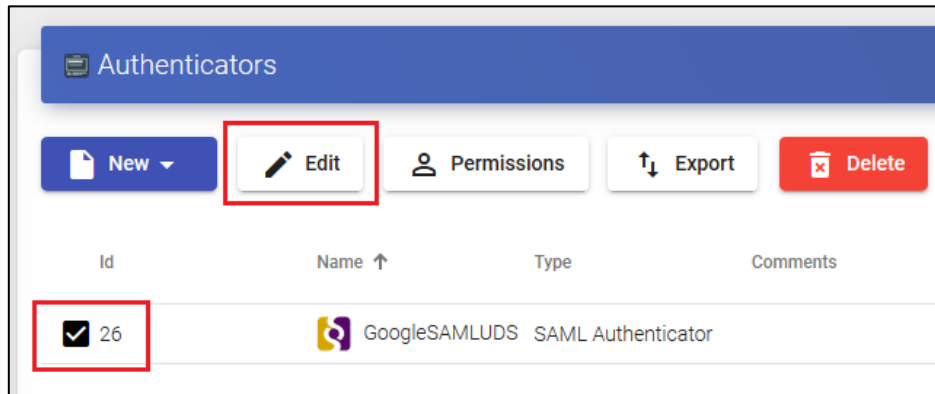


Salvamos para aplicar el cambio.

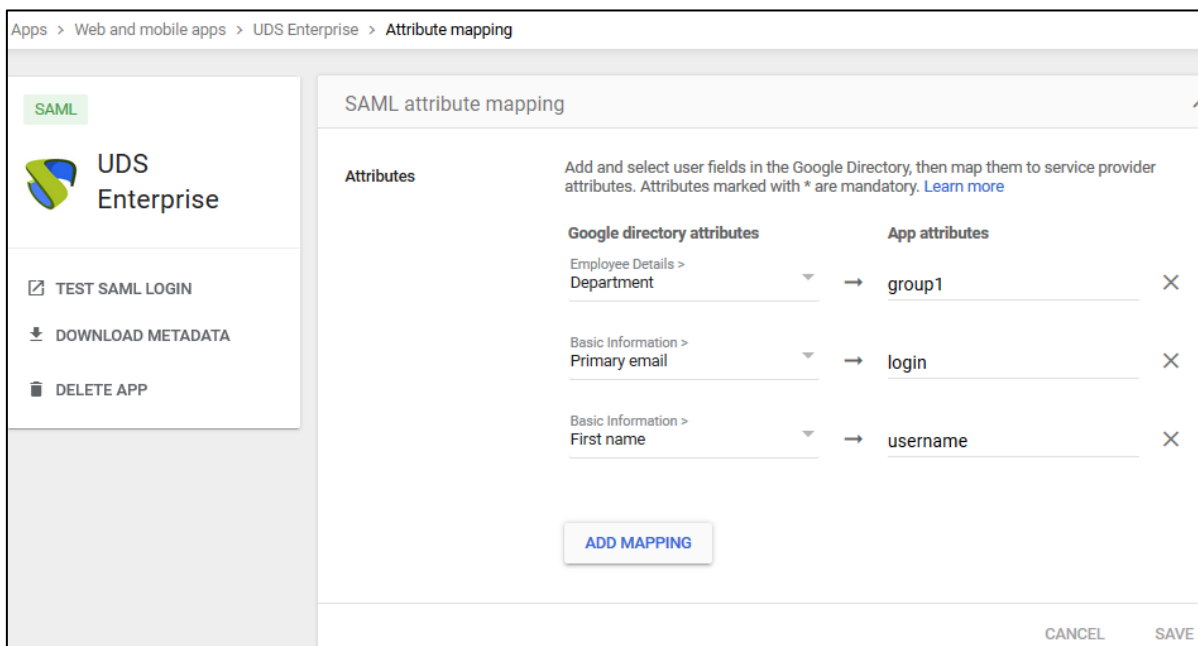


## Definición de atributos en SAML

Accedemos a la administración de UDS Enterprise, seleccionamos el autenticador SAML previamente creado y lo editamos.



En el apartado “**Attributes**” indicaremos los atributos correctos. Están definidos y son visibles en la ampliación SAML de Google creada en pasos anteriores:



Como vemos en el ejemplo:

- El atributo definido anteriormente “**login**”, que será el “**primary email**” del usuario en Google Workspace, se empleará para realizar login en UDS Enterprise, puesto que está definido en “**User name attrs**”.
- El atributo “**username**”, que será el “**First name**” del usuario en Google Workspace, se utilizará en UDS Enterprise para mostrar el nombre del usuario. Está definido en “**Real name attrs**”.
- El atributo “**group1**”, que será el “**Department**” al que pertenece un usuario en Google Workspace, se usará en UDS Enterprise como grupo de pertenencia de los usuarios. Está definido en “**Group name attrs**”.



# Autenticación de usuarios de Google Workspace en UDS Enterprise 3.5

www.udsenderprise.com

**Edit Authenticator**

< Metadata **Attributes** Display >

User name attrs \*  
login

Group name attrs \*  
group1

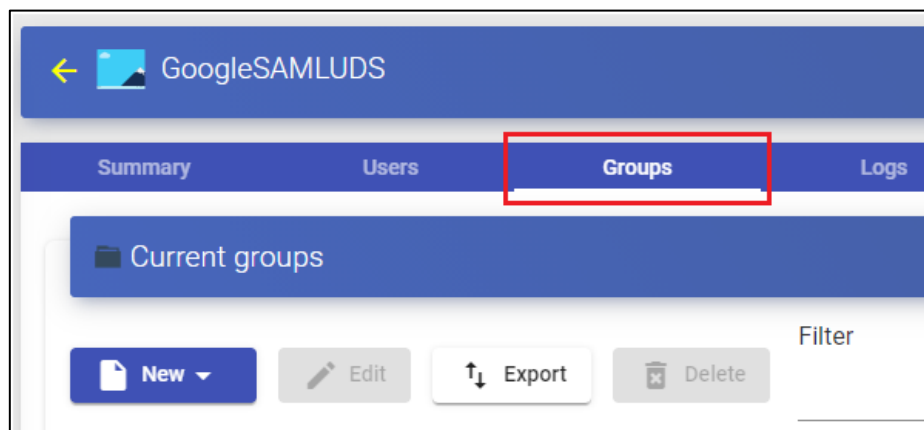
Real name attrs \*  
username

Test Discard & close Save

**NOTA:** En UDS Enterprise es posible indicar varios atributos o utilizar expresiones regulares. Por ejemplo, para indicar nuevos atributos de pertenencia a grupos.

Una vez definidos correctamente los atributos, guardamos y accedemos al autenticador creado en UDS Enterprise.

Dentro del autenticador, accedemos al apartado “**Groups**” para añadir los grupos necesarios.





# Autenticación de usuarios de Google Workspace en UDS Enterprise 3.5

www.udsenderprise.com

Los grupos los tendremos que añadir manualmente, ya que la búsqueda automática no aplica con este tipo de autenticador:

**New group**

Group  
30

Comments

State  
Enabled

Service Pools

Cancel Ok

Añadimos todos los grupos necesarios (en este ejemplo, se añaden los diferentes departamentos a los que pertenecen los usuarios, puesto que el atributo de pertenencia a grupos utilizado de Google Workspace es el “**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

Con la configuración aplicada en este ejemplo, todos los usuarios que tengan en su atributo “**department**” un valor de 25, 30 o 40, podrán realizar login en el portar de UDS Enterprise.



## Acceso a través del autenticador

Para confirmar que toda la configuración es correcta, accedemos al portal de UDS Enterprise a través del autenticador SAML recién creado:

Username \*

Password

Authenticator

Interna

GoogleSAMLUDS

Al seleccionar el autenticador SAML, automáticamente se nos redireccionará a la página del proveedor. El sistema nos solicitará unas credenciales válidas:

Google

Pepito Perez

pperez@virtualcable.es

Enter your password

.....

Show password

[Forgot password?](#) [Next](#)

English (United Kingdom) Help Privacy Terms

**NOTA:** El modo de validación será el configurado en el propio proveedor. Es decir, si disponemos de validación de los usuarios vía MFA, se utilizará.

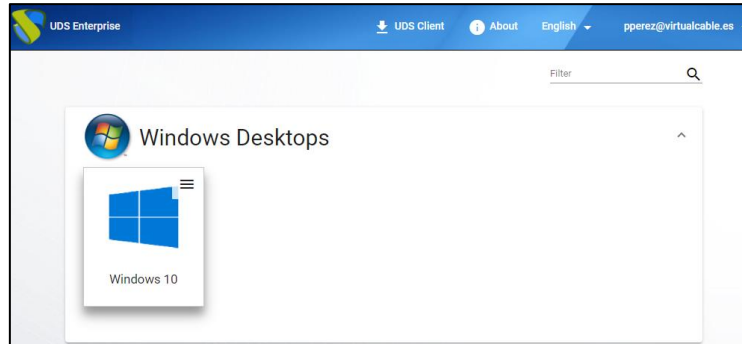




# Autenticación de usuarios de Google Workspace en UDS Enterprise 3.5

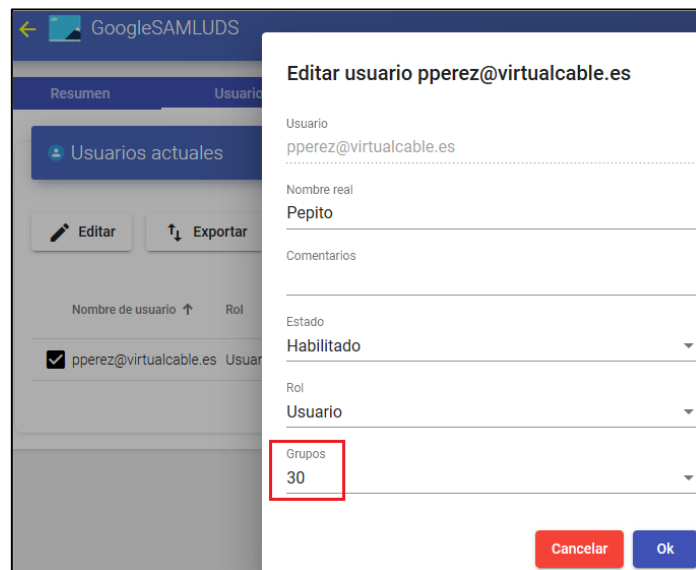
www.udsenderprise.com

Una vez realizado el login en Google Workspace, se efectuará una redirección y volveremos a la página de servicios de UDS Enterprise:



**NOTA:** Si el grupo al que pertenece el usuario tiene servicios asignados, se le mostrarán y podrá acceder a ellos.

Podemos comprobar a qué grupos pertenece un usuario si lo editamos. Para ello, accedemos al autenticador y editamos el usuario:



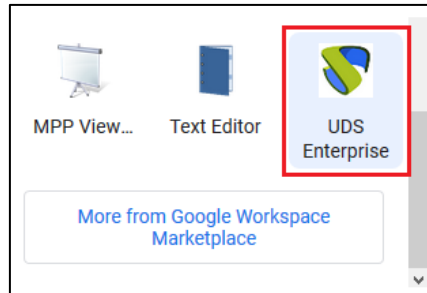
Podemos comprobar que en este ejemplo, el usuario *pperez* pertenece al departamento 30 y, como está dado de alta como grupo en el autenticador, puede acceder.

Si hemos habilitado el acceso de nuestros usuarios a la aplicación, también les aparecerá en su listado de aplicaciones de Google Workspace y automáticamente accederán al entorno VDI después de su validación:



# Autenticación de usuarios de Google Workspace en **UDS Enterprise 3.5**

[www.udsenderprise.com](http://www.udsenderprise.com)

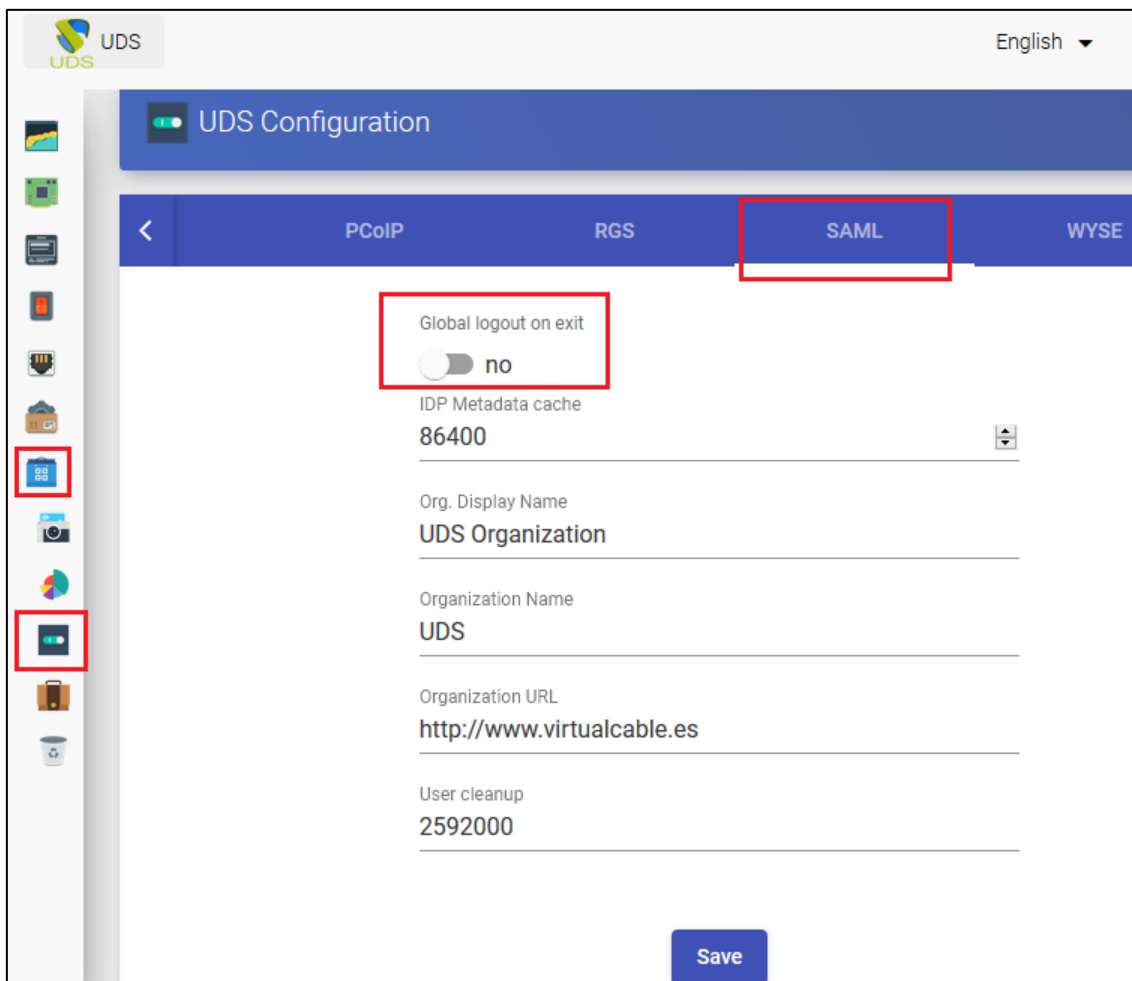




## Habilitar Global logout

Hay que tener en cuenta que cuando un usuario acceda desde UDS Enterprise e inicie sesión con su cuenta de Google, al cerrar sesión desde UDS, por defecto no se cerrará la sesión de su cuenta de Google. Si se desea realizar un logout global (tanto de UDS, como de la cuenta de Google), será necesario indicarlo en la administración de UDS Enterprise:

Accedemos a la administración de UDS Enterprise, apartado “Herramientas” – “Configuración” pestaña “SAML”, parámetro “Global logout on exit”:



Una vez habilitado el logout global, deberemos salvar los cambios y reiniciar los servidores UDS (máquinas UDS-Server) o sus servicios (uds y udsweb) para que se apliquen los cambios.



## Sobre Virtual Cable

Virtual Cable desarrolla y comercializa UDS Enterprise mediante un modelo de suscripción, incluyendo soporte y actualizaciones, según el número de usuarios.

Además, Virtual Cable ofrece servicios profesionales para instalar y configurar UDS Enterprise.

Para más información, visite [www.udsenderprise.com](http://www.udsenderprise.com) o envíenos un email a [info@udsenderprise](mailto:info@udsenderprise).