VIRTUAL CABLE

Autenticación de usuarios de Google Workspace en UDS Enterprise 3.6

UDS ENTERPRISE 3.6

índice

Introducción 2
Creación de aplicación SAML de Google 2
Creación del autenticador SAML 5
Configuración de la aplicación SAML 9
Definición de atributos en SAML 12
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 3.6 para validar usuarios existentes en Google Workspace.

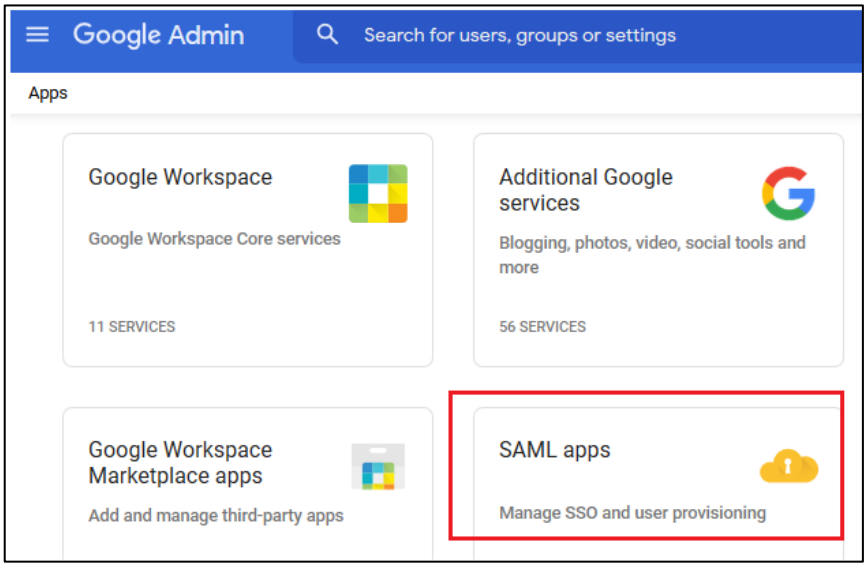
Una vez creado el nuevo autenticador en UDS Enterprise e integrado con Google Workspace, los usuarios existentes en este entorno podrán acceder a los servicios publicados en UDS Enterprise.

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.

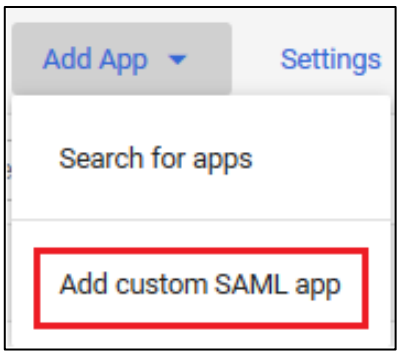
Creación de aplicación SAML de Google

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

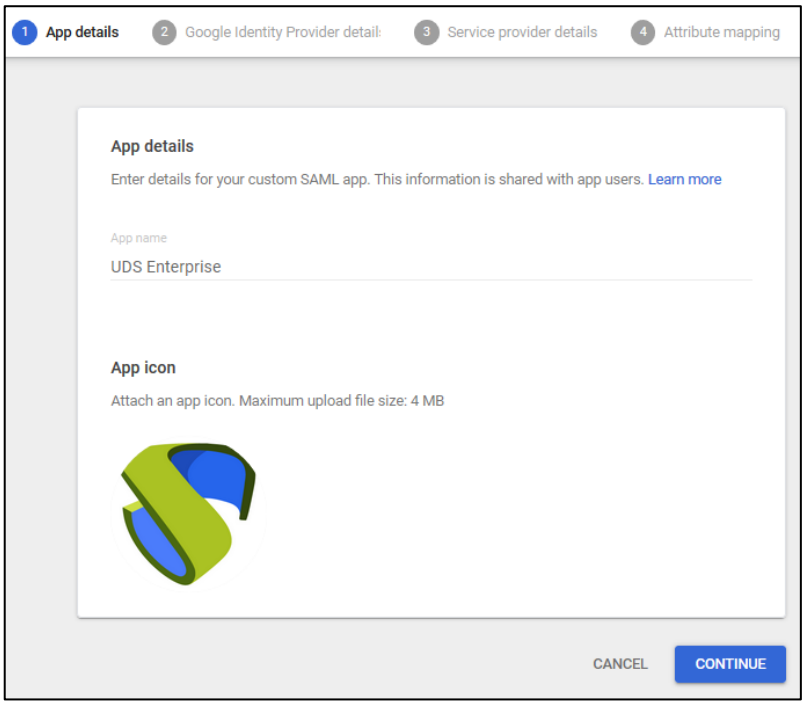
Accedemos al panel de administración de Google Workspace y seleccionamos "**SAML apps**".



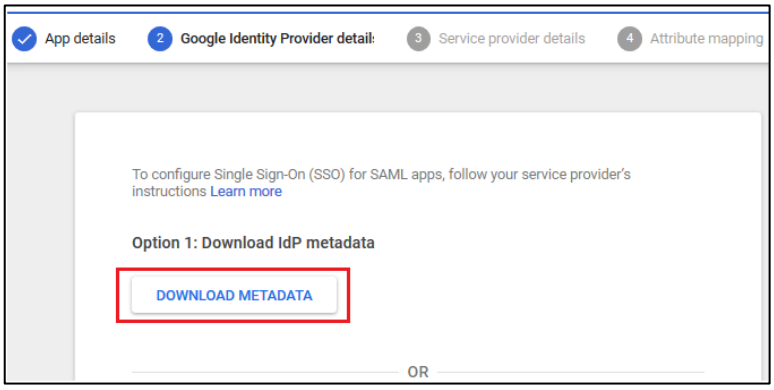
Deberemos dar de alta una nueva aplicación SAML personalizada:



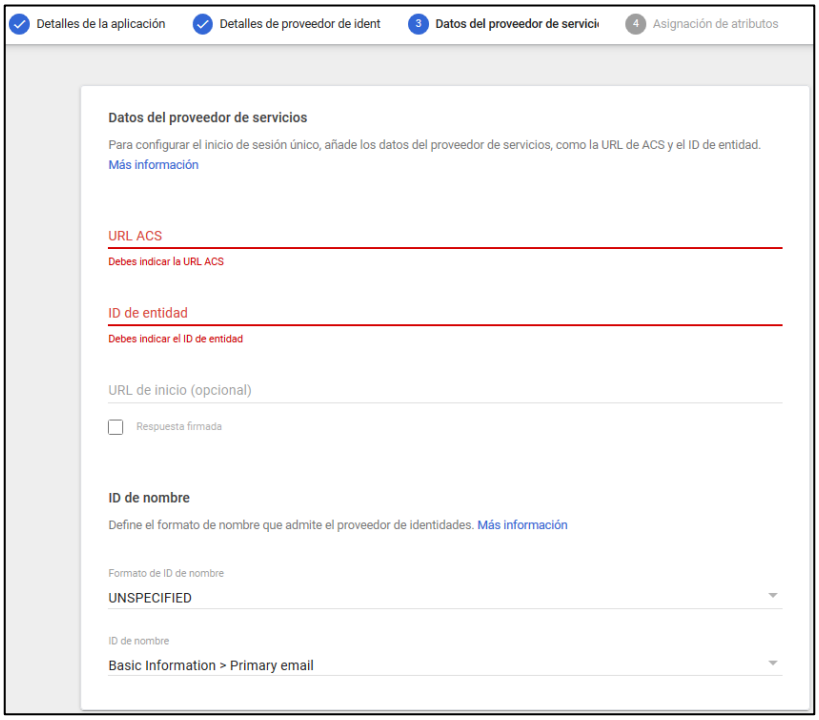
En el asistente de configuración indicamos un nombre para identificar la aplicación y podremos añadir un icono para que los usuarios puedan localizar el servicio fácilmente.



Ahora descargamos los metadatos y continuamos el asistente:



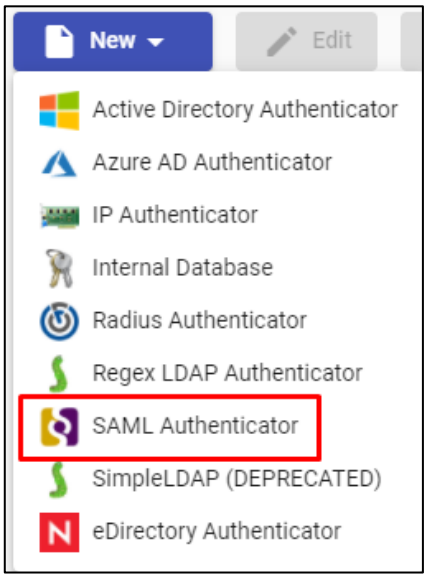
En el paso 3 del asistente, deberemos indicar la "**URL ACS**" y el "**ID de entidad**":



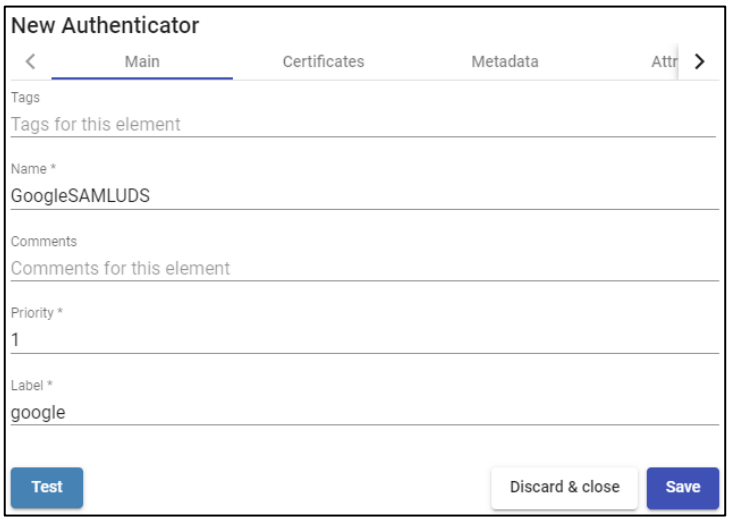
Para obtener estos datos, deberemos acceder a la administración de nuestro entorno UDS Enterprise y crear un nuevo autenticador de tipo SAML. Una vez tengamos los datos, seguiremos completando los diferentes apartados del asistente hasta su finalización.

Creación del autenticador SAML

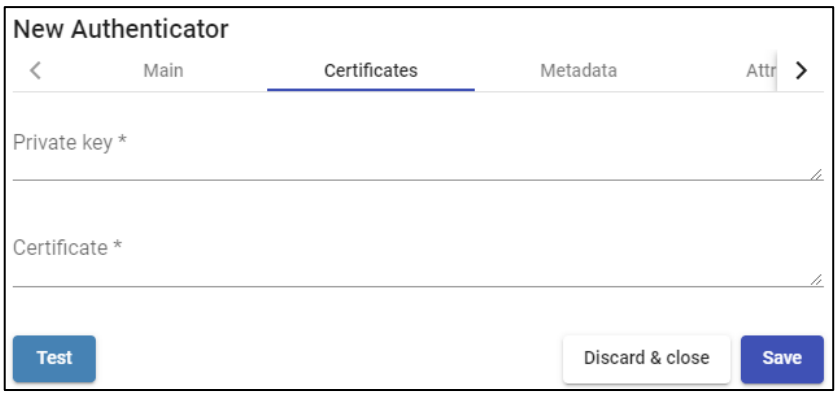
Accedemos a la administración de UDS Enterprise y nos situamos en el apartado "**Authenticators**", seleccionamos "**New**" y elegimos "**SAML Authenticator**".



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



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

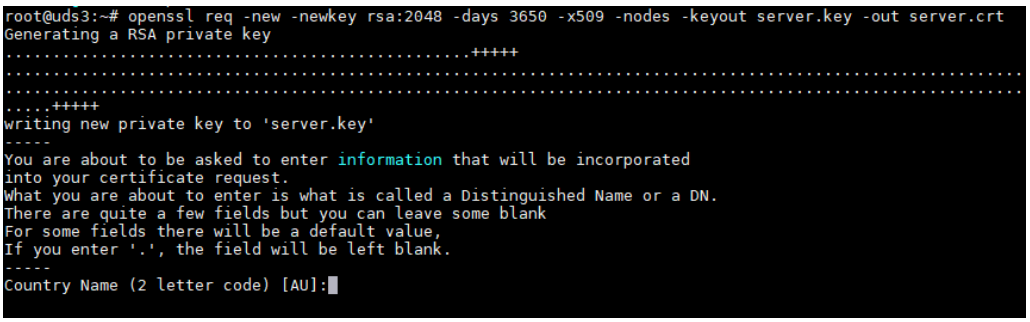


Si no se dispone de certificados, se puede generar uno con **OpenSSL**. Para generarlo, utilizaremos la siguiente sentencia (el servidor de UDS tiene instalado **OpenSSL**, puede utilizarse esta máquina para generar el certificado):

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

Una vez generado el certificado debemos compartir la clave con RSA, para ello utilizaremos el siguiente comando: `openssl rsa -in server.key -out server_rsa.key`

Ejemplo de generación de certificado:



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:**

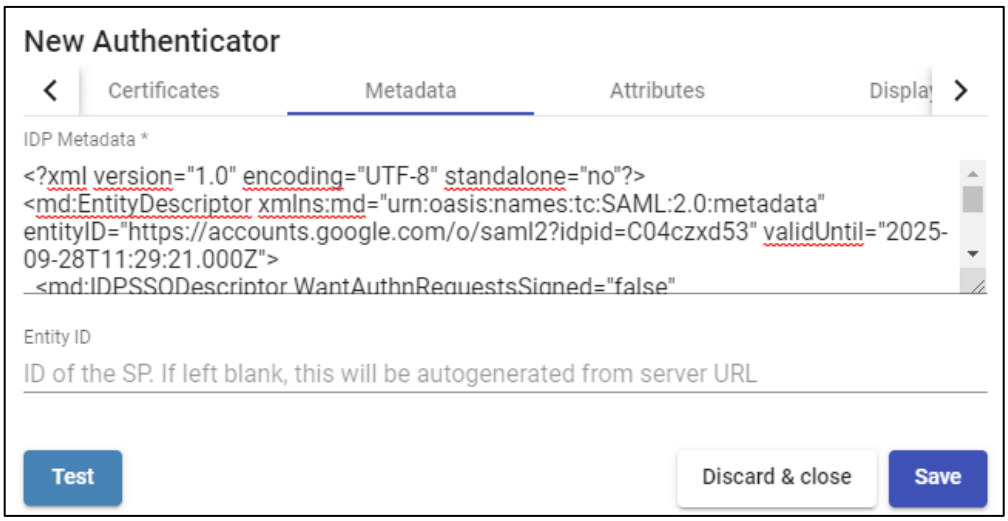
```
root@uds3:~# openssl rsa -in server.key -out server_rsa.key
writing RSA key
root@uds3:~#
```

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:~#
```

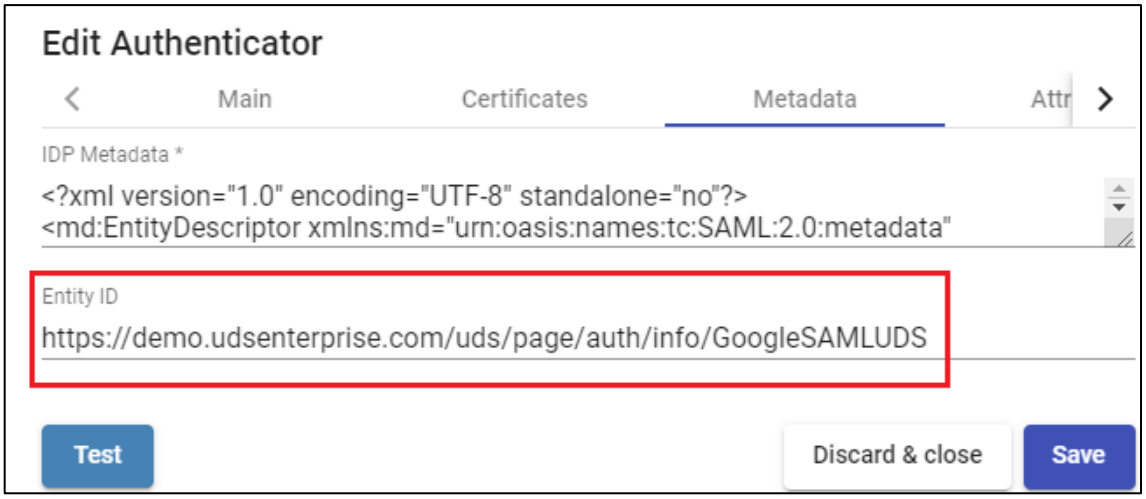
La clave la copiaremos en el apartado "**Private Key**" y el certificado en "**Certificate**":

En la siguiente pestaña, "**Metadata"**, completaremos el apartado "**IDP Metadata**" con los metadatos descargados de Google en pasos anteriores (paso 2 del alta de aplicación SAML personalizada). Es importante copiar el contenido completo del fichero. Para ello se recomienda abrir el fichero con una aplicación adecuada y nunca con un navegador (oculta partes del código…):



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.

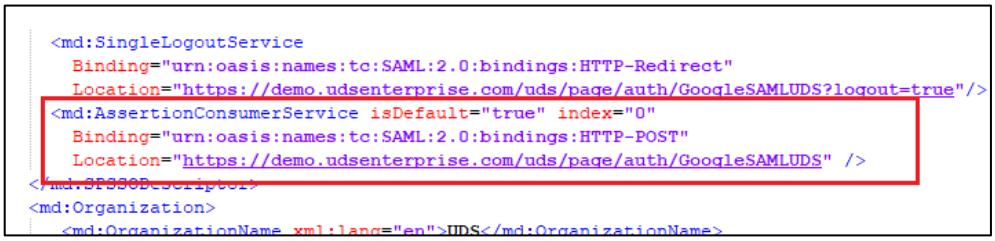


Configuración de la aplicación SAML

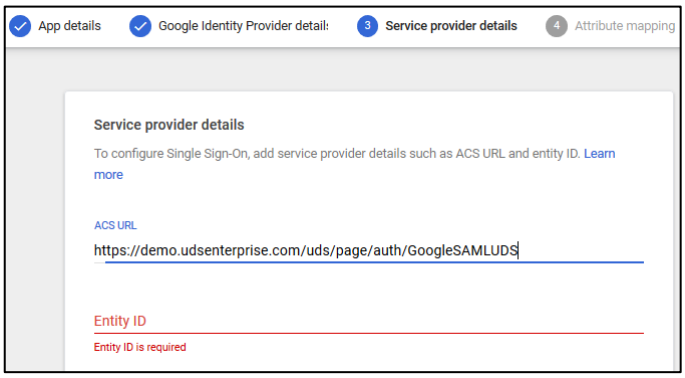
Retomamos el paso 3 del asistente de configuración de Google para crear una aplicación SAML personalizada, donde nos pedirá la "**URL ACS**" y el "**ID de entidad**".

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.udsenterprise.com/uds/page/auth/info/GoogleSAMLUDS)

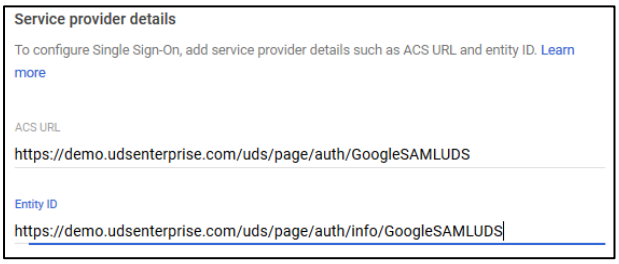
Dentro del fichero descargado, buscaremos: **AssertionConsumerService**



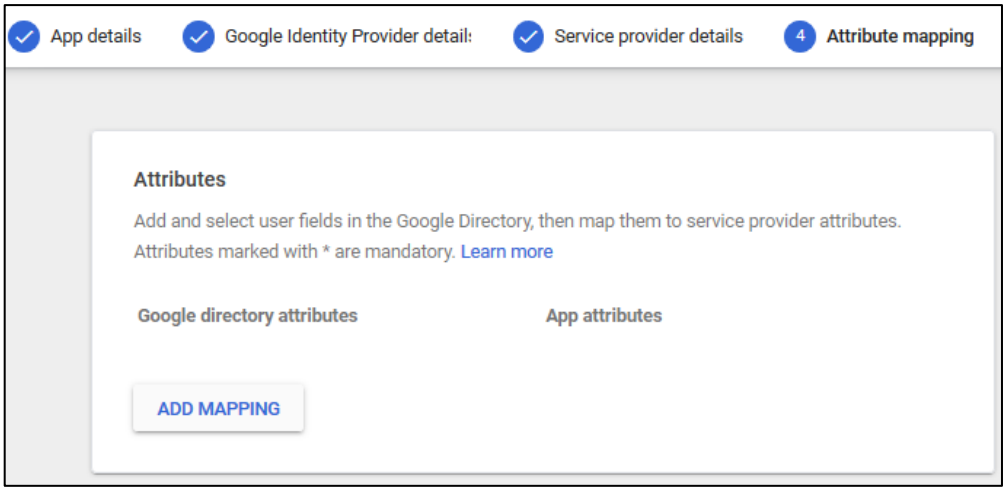
Copiaremos la URL facilitada en el campo "**URL ACS**":



Por último, para terminar de configurar el paso 3, indicaremos el "**ID de entidad**". Será elautogenerado por UDS Enterprise en el campo "**Entity ID**" de la pestaña "**Metadata**" delautenticador:

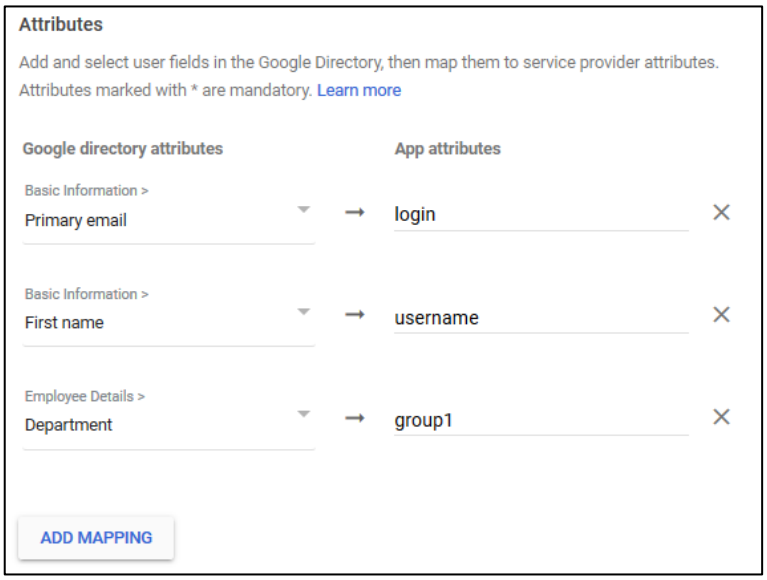


Dejaremos el resto de opciones por defecto y seguimos con el paso 4. Ahí definiremos los atributos que serán utilizados por UDS Enterprise para validar usuarios y configurar grupos:



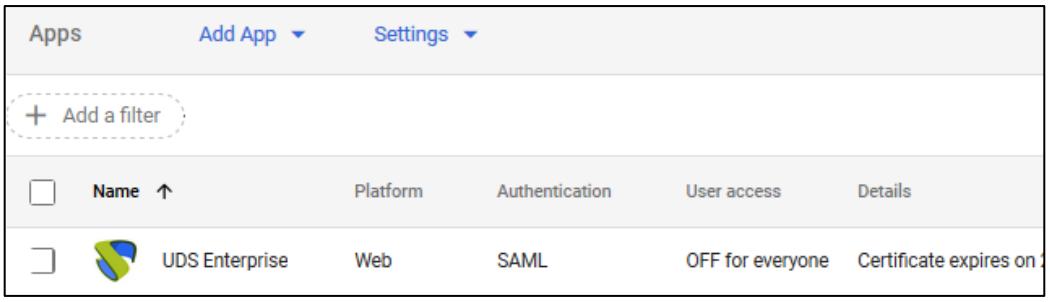
En este ejemplo se utilizarán los siguientes atributos:

- 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**".

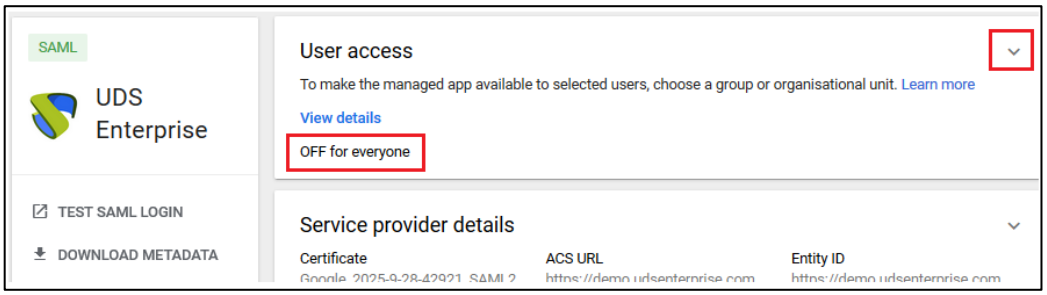


Podremos utilizar o añadir atributos personalizados. En este ejemplo se usarán los atributos por defecto facilitados por Google.

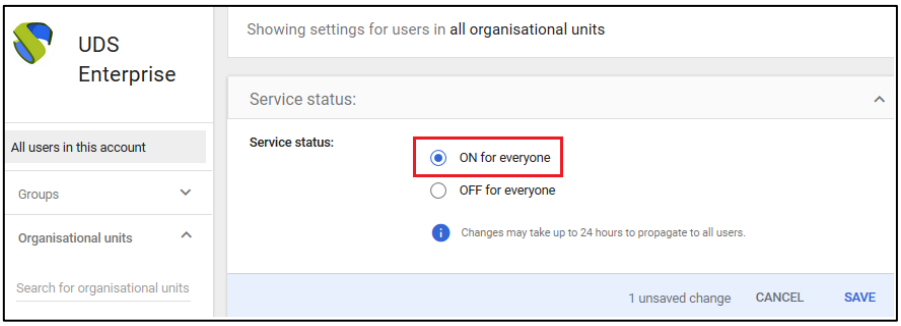
Una vez seleccionados los atributos necesarios, finalizaremos el asistente.



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**":



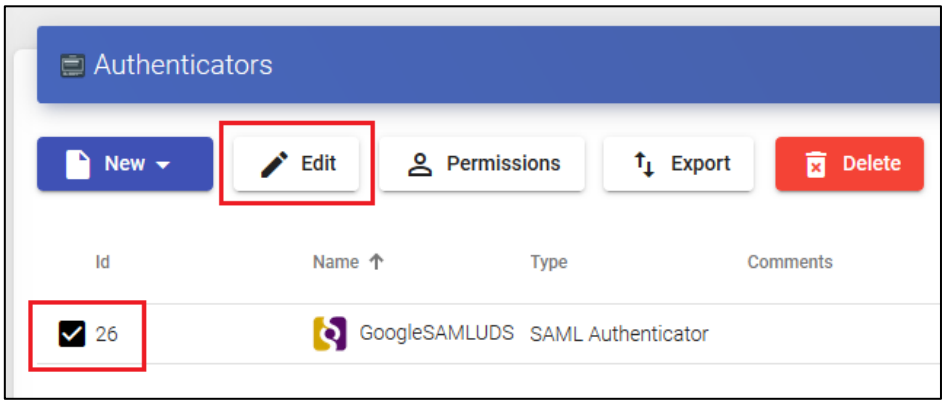
En este ejemplo la aplicación estará activada para todos los usuarios, pero es posible acotar por grupos.



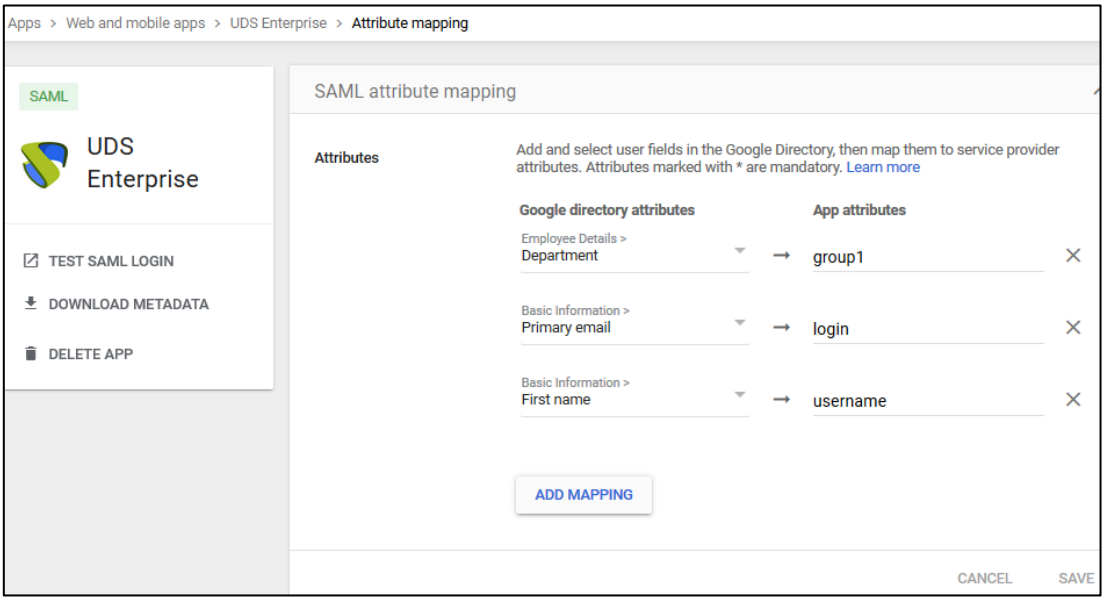
Salvamos para aplicar el cambio.

Definición de atributos en SAML

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

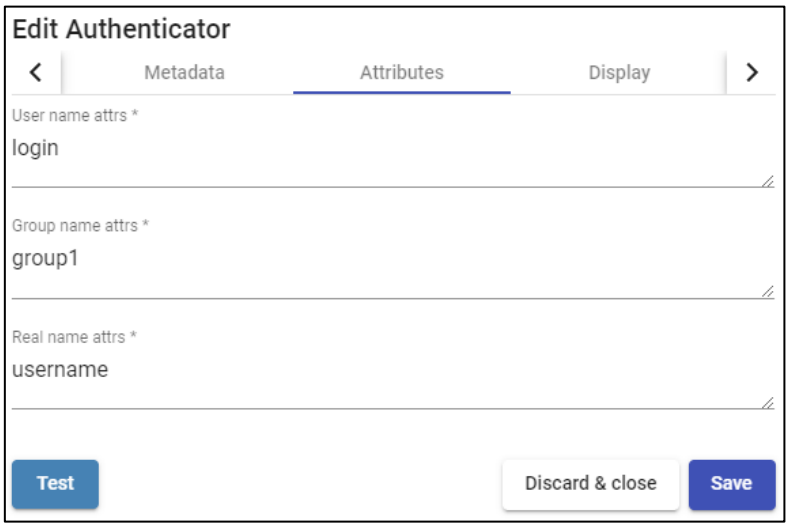


En el apartado "**Attributes**" indicaremos los atributos correctos. Están definidos y son visibles en la ampliación SAML de Google creada en pasos anteriores:



Como vemos en el ejemplo:

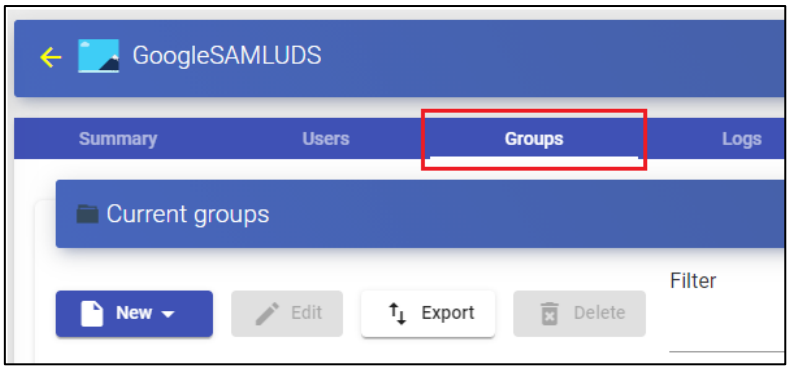
- El atributo definido anteriormente "**login**", que será el "**primary email**" del usuario en Google Workspace, se empleará para realizar login en UDS Enterprise, puesto que está definido en "**User name attrs**".
- El atributo "**username**", que será el "**First name**" del usuario en Google Workspace, 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**".



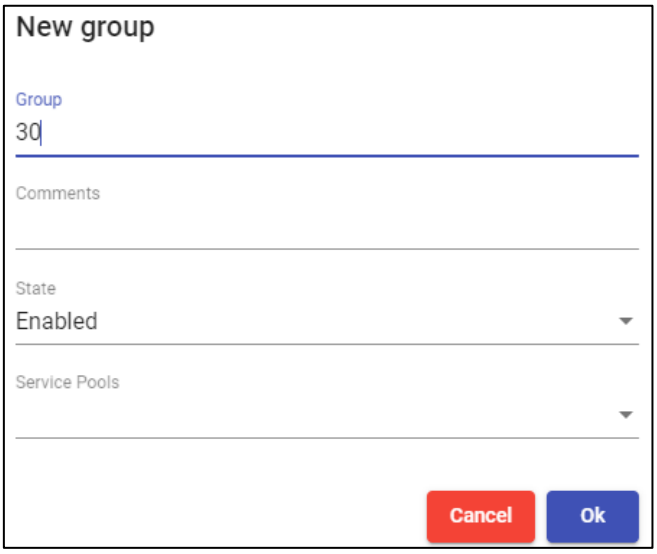
NOTA: En UDS Enterprise es posible indicar varios atributos o utilizar expresiones regulares. Por ejemplo, para indicar nuevos atributos de pertenencia a grupos.

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

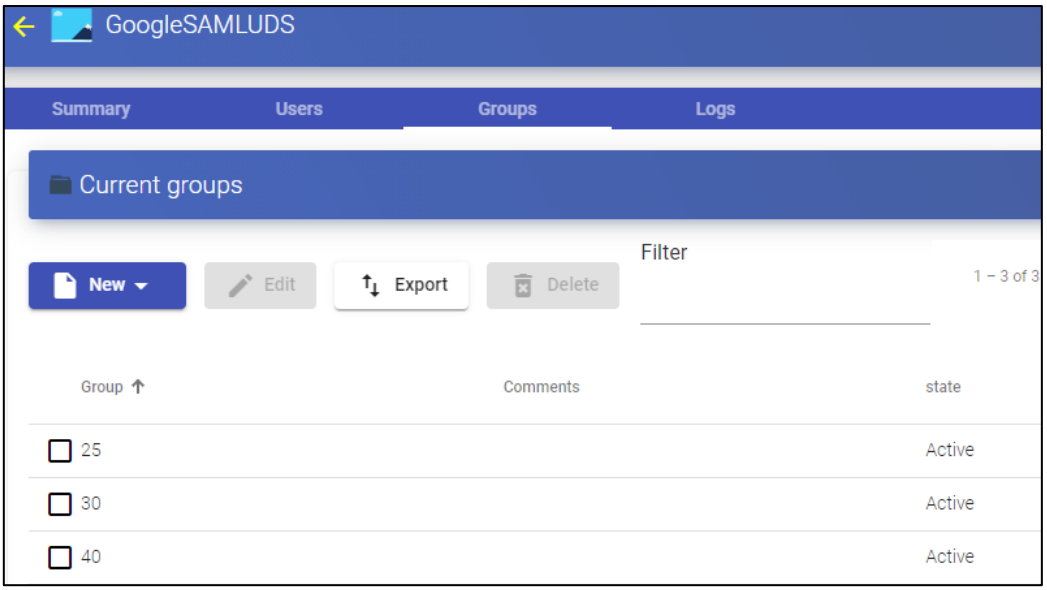
Dentro del autenticador, accedemos al apartado "**Groups**" para añadir los grupos necesarios.



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



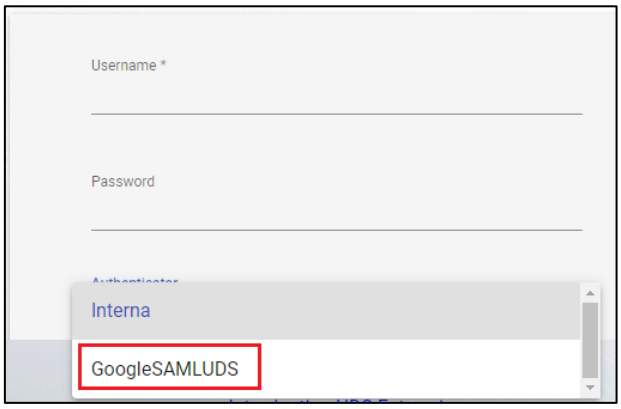
Añadimos todos los grupos necesarios (en este ejemplo, se añaden los diferentes departamentos a los que pertenecen los usuarios, puesto que el atributo de pertenencia a grupos utilizado de Google Workspace es el "**department**"):



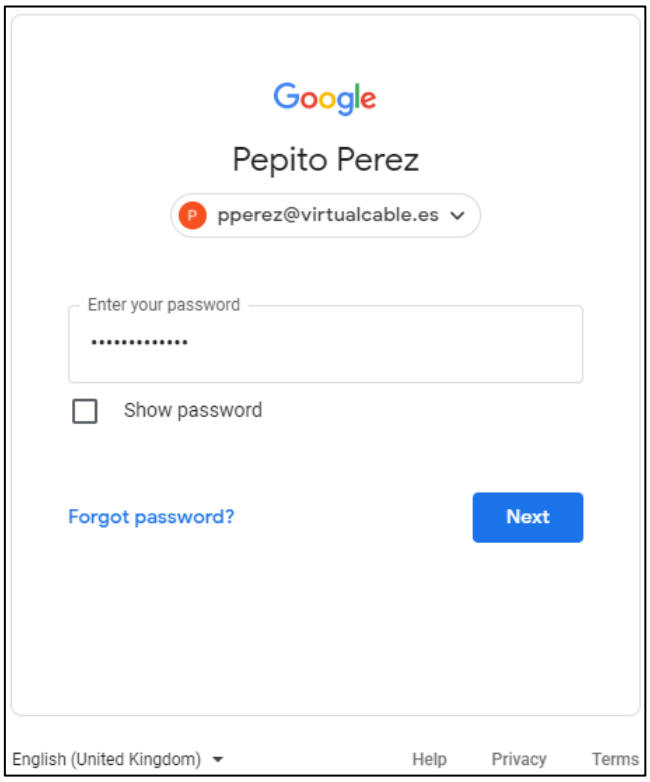
Con la configuración aplicada en este ejemplo, todos los usuarios que tengan en su atributo "**department**" un valor de 25, 30 o 40, podrán realizar login en el portar de UDS Enterprise.

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:

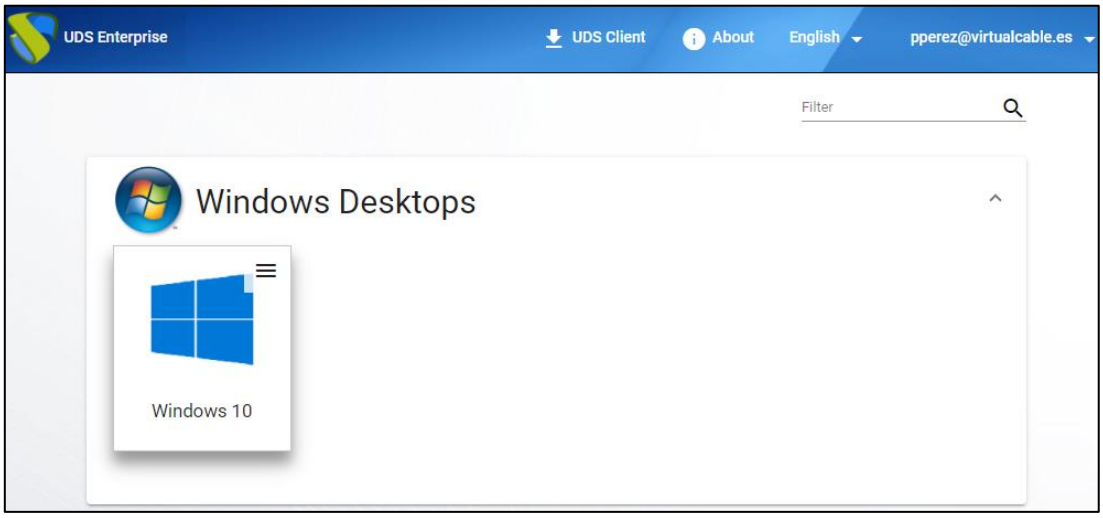


Al seleccionar el autenticador SAML, automáticamente se nos redireccionará a la página del proveedor. El sistema nos solicitará unas credenciales válidas:



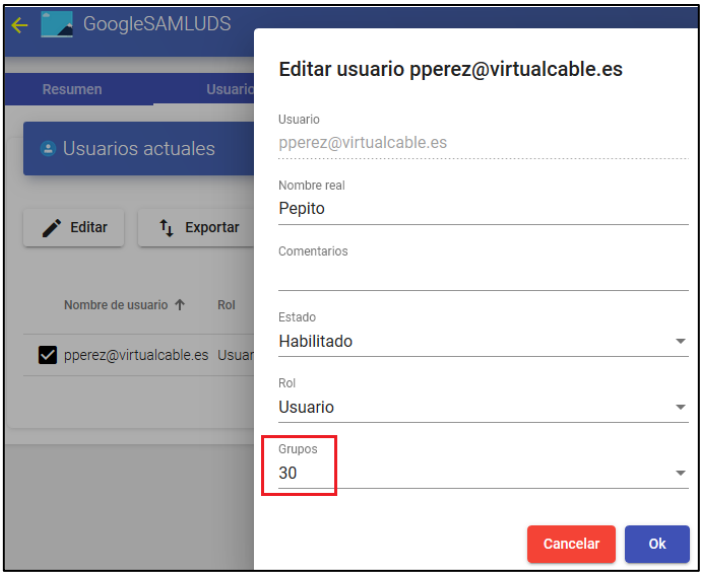
NOTA: El modo de validación será el configurado en el propio proveedor. Es decir, si disponemos de validación de los usuarios vía MFA, se utilizará.

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



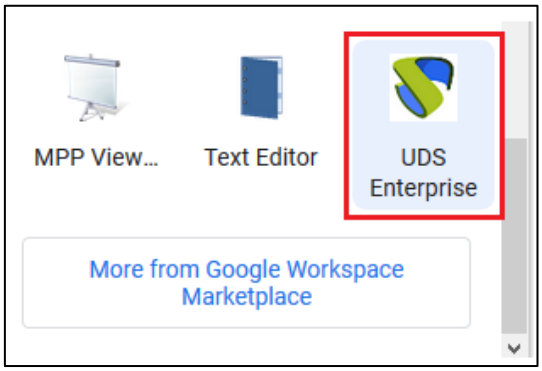
NOTA: Si el grupo al que pertenece el usuario tiene servicios asignados, se le mostrarán y podrá acceder a ellos.

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:

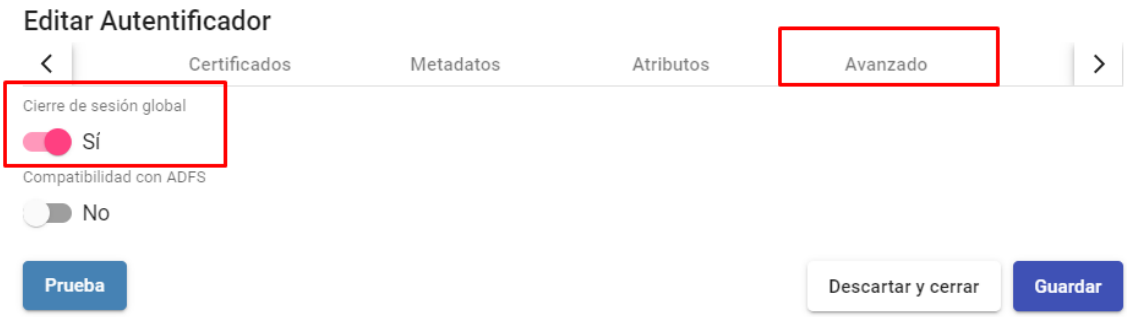


Habilitar Global logout

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 el autenticador SAML que hayamos configurado dentro de UDS Enterprise:

Accedemos al autenticador, en el apartado "**Avanzado"**:

Parámetro "**Cierre de sesión global**":



Sobre Virtual Cable

Virtual Cable es una compañía especializada en la **transformación digital** del **puesto de trabajo**. La compañía desarrolla, soporta y comercializa UDS Enterprise. Su equipo de expertos ha diseñado soluciones **VDI** a medida de **cada sector** para proporcionar una experiencia de usuario única y totalmente adaptada a las necesidades de cada perfil de usuario. Los profesionales de Virtual Cable tienen **más de 30 años de experiencia** en TI y desarrollo de software y más de 15 en tecnologías de virtualización. Cada día se despliegan **millones de escritorios virtuales Windows y Linux con UDS Enterprise en todo el mundo**.