Autenticación de usuarios de OneLogin en UDS Enterprise

www.udsenterprise.com

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 IRONCHIP.

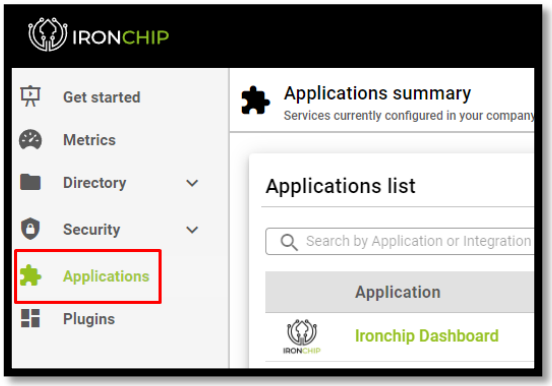
Una vez creado el nuevo autenticador en UDS Enterprise e integrado con IRONCHIP, los usuarios existentes en este entorno podrán acceder a los servicios publicados en UDS Enterprise.

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

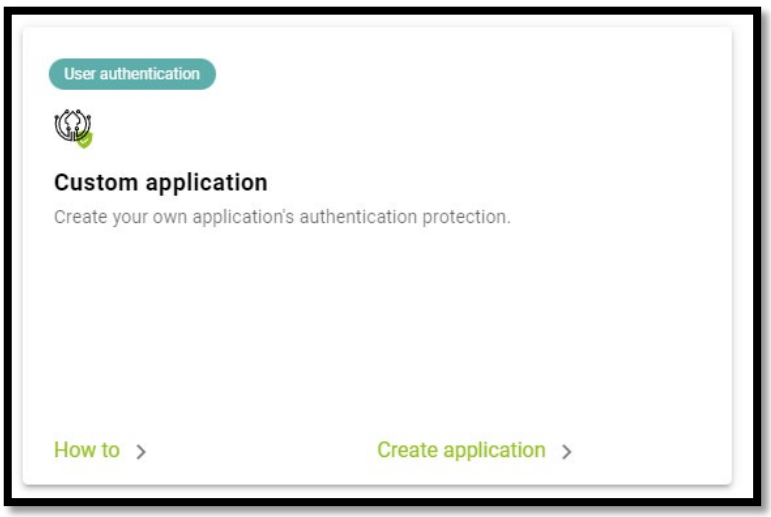
Creación de aplicación SAML de IRONCHIP

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

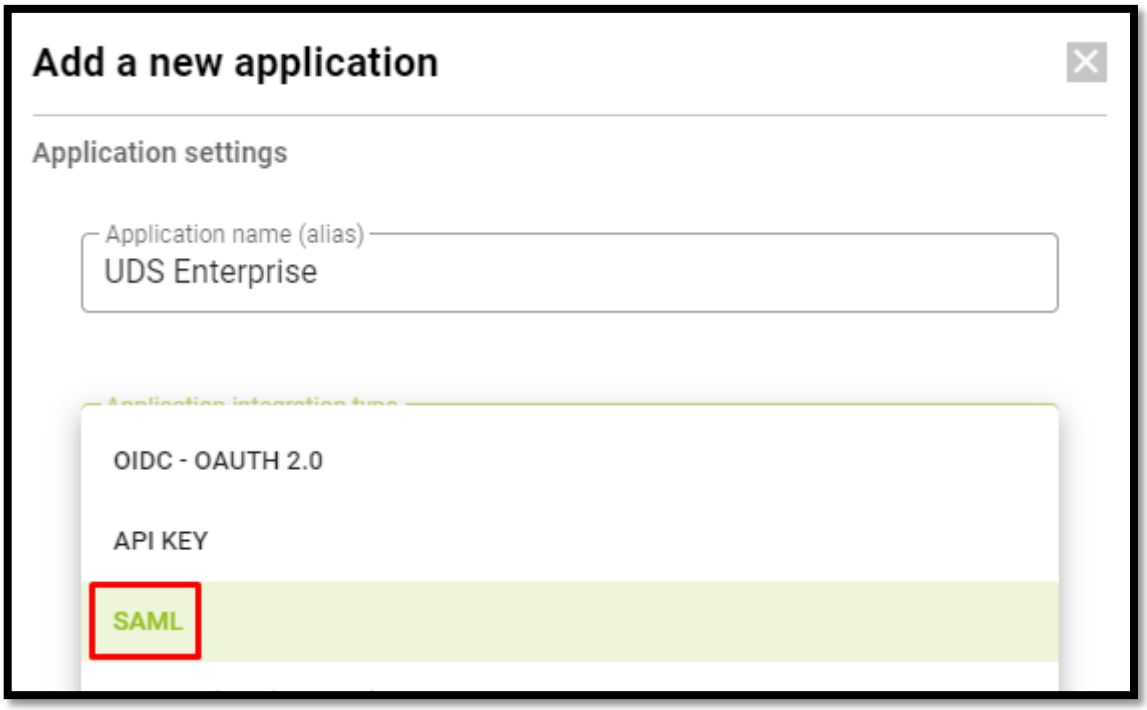
Accedemos al panel de administración de IRONCHIP y seleccionamos "**SAML apps**".



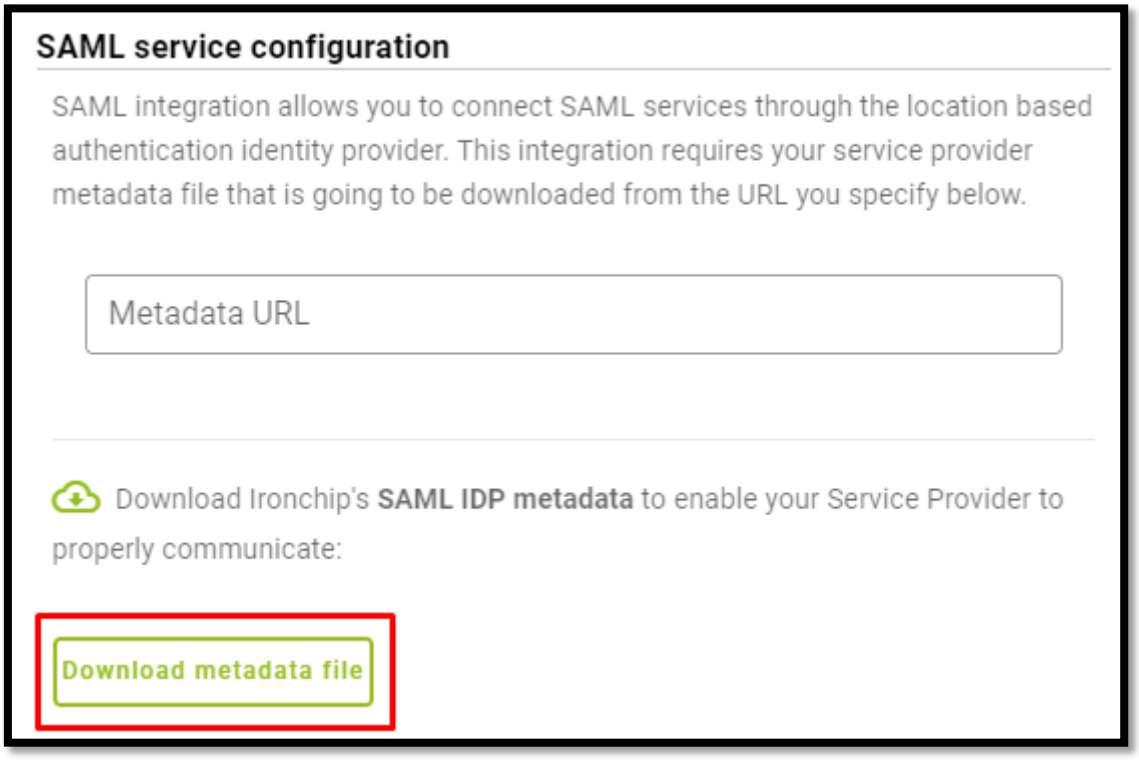
Deberemos dar de alta una nueva aplicación SAML personalizada:



En el asistente de configuración indicamos un nombre para identificar la aplicación y seleccionamos el tipo de integración que queremos hacer que será de tipo “**SAML**”:



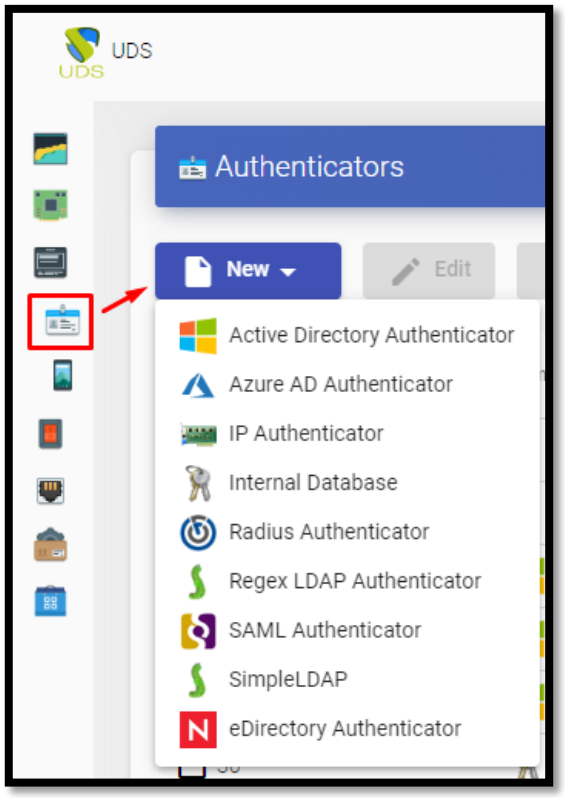
Una vez seleccionada esta opción podremos descargar el Metadata generado por IRONCHIP:



Una vez descargados dejaremos abierta esta ventana y pasaremos al siguiente paso

Creación del autenticador SAML en UDS Enterprise

Accedemos a la administración de UDS Enterprise y nos situamos en el apartado "**Autenticadores**", seleccionamos "**Nuevo**" 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:

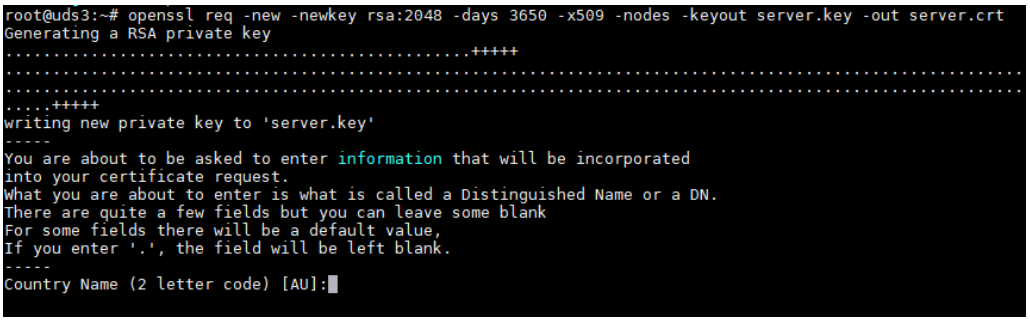
Si no se dispone de certificados, se puede generar uno con **OpenSSL**. Para generarlo, utilizaremos la siguiente sentencia (el servidor de UDS tiene instalado **OpenSSL**, puede utilizarse esta máquina para generar el certificado):

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

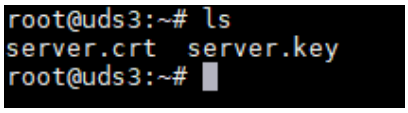
Once the certificate is generated, we must share the key with RSA, for this, we will use the following command:

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

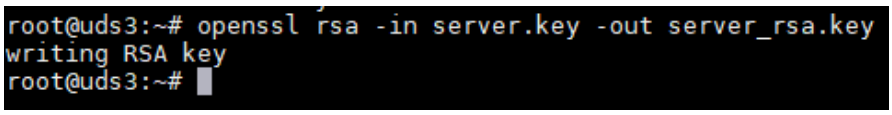
Ejemplo de generación de certificado:



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

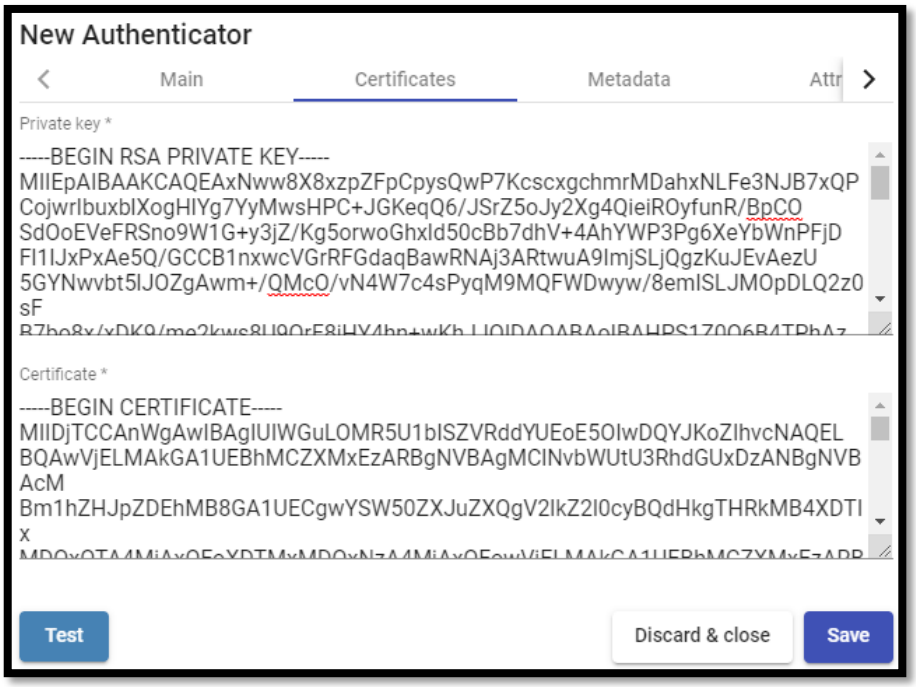


Ahora convertimos la clave a **rsa:**



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

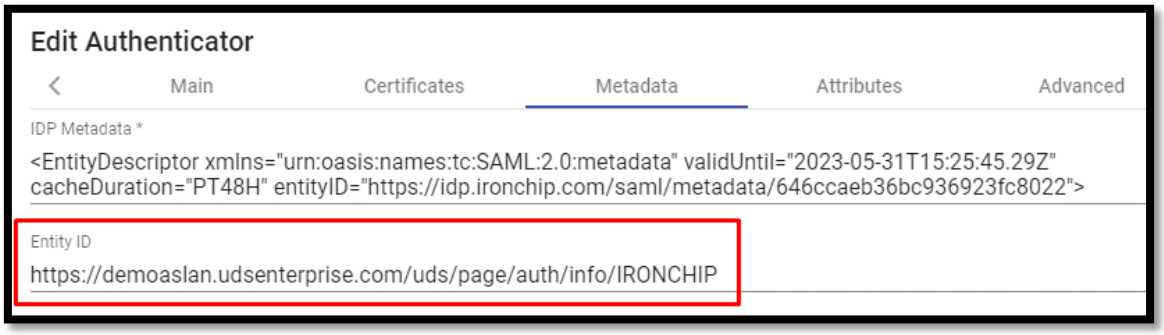
La clave la copiaremos en el apartado "**Private Key**" y el certificado en "**Certificate**":



En la siguiente pestaña, “**Metadata”**, completaremos el apartado “**IDP Metadata**” con los metadatos descargados de IRONCHIP 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…):

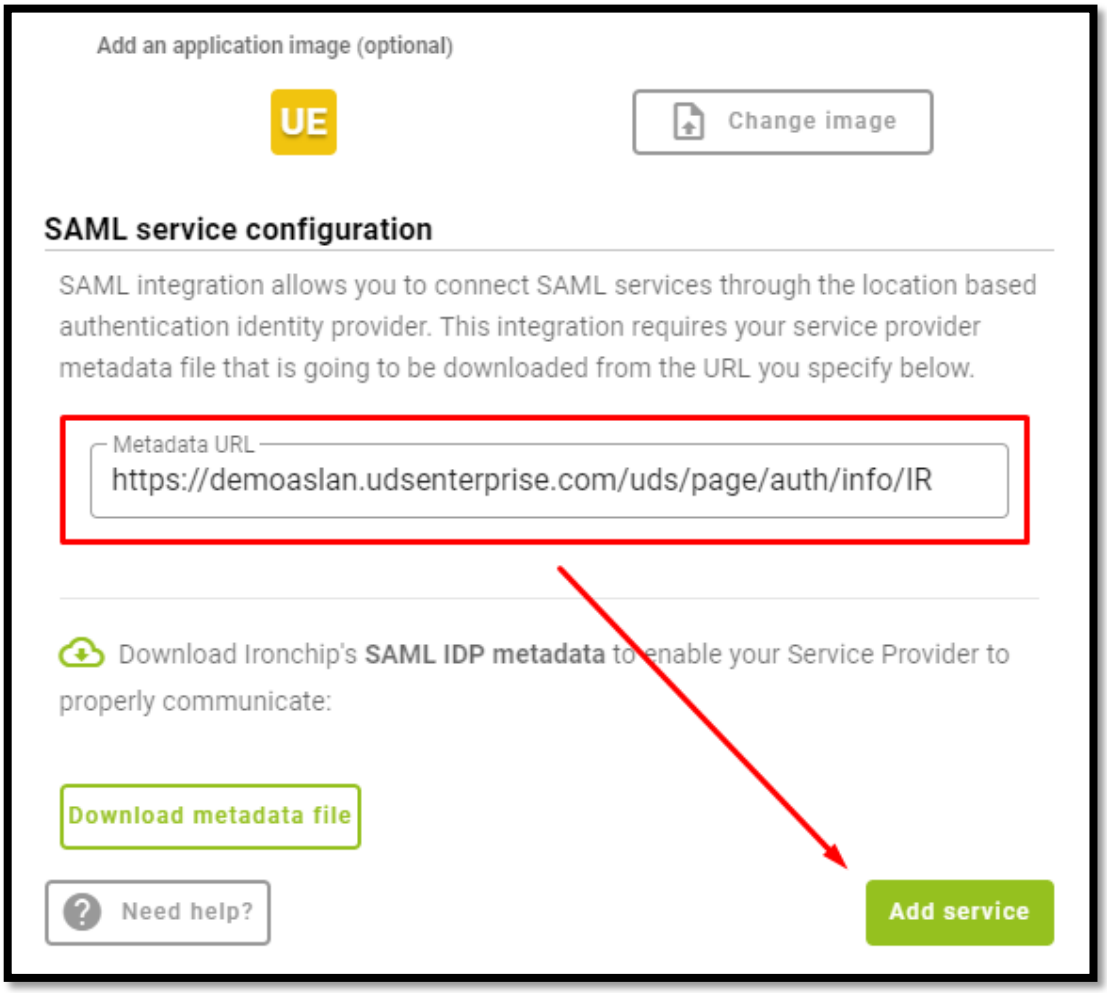
El apartado “**Entity ID**” lo dejaremos vacío, puesto que se rellenará automáticamente cuando guardemos el autenticador. Los datos se generarán en base a la URL utilizada en la conexión con el portal de UDS Enterprise.

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 IRONCHIP.



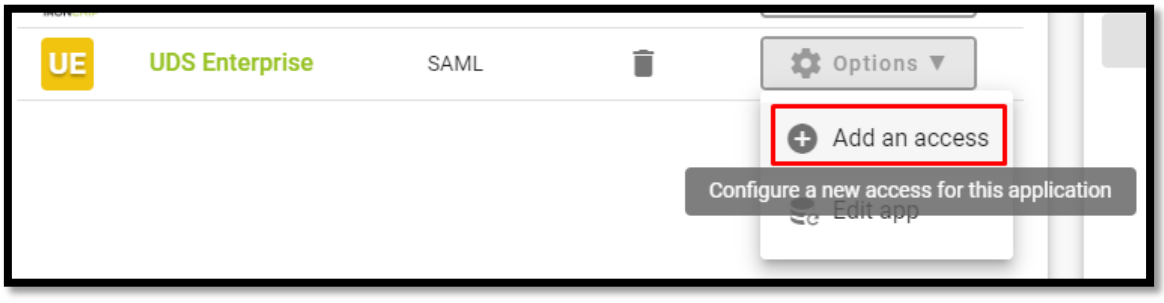
Configuración de la aplicación SAML en IRONCHIP

Retomamos el asistente de configuración de IRONCHIP para crear una aplicación SAML personalizada, donde nos pedirá la "**Metadata URL**" generada en el paso anterior una vez que hemos guardado y vuelto a editar el autenticador en UDS Enterprise.

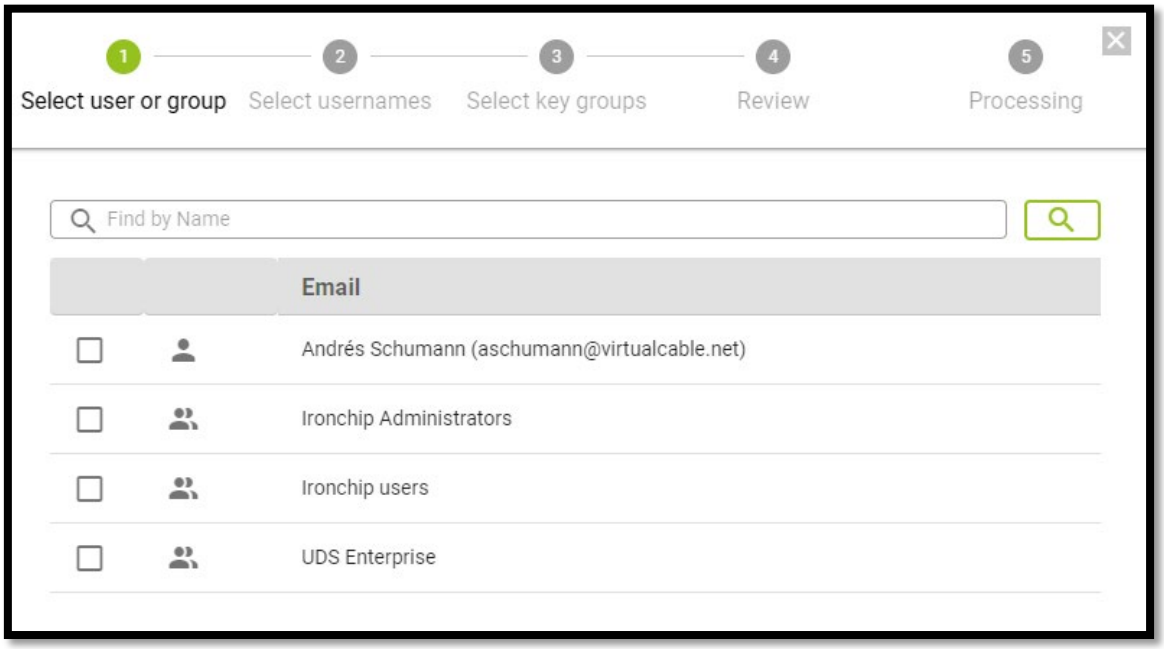


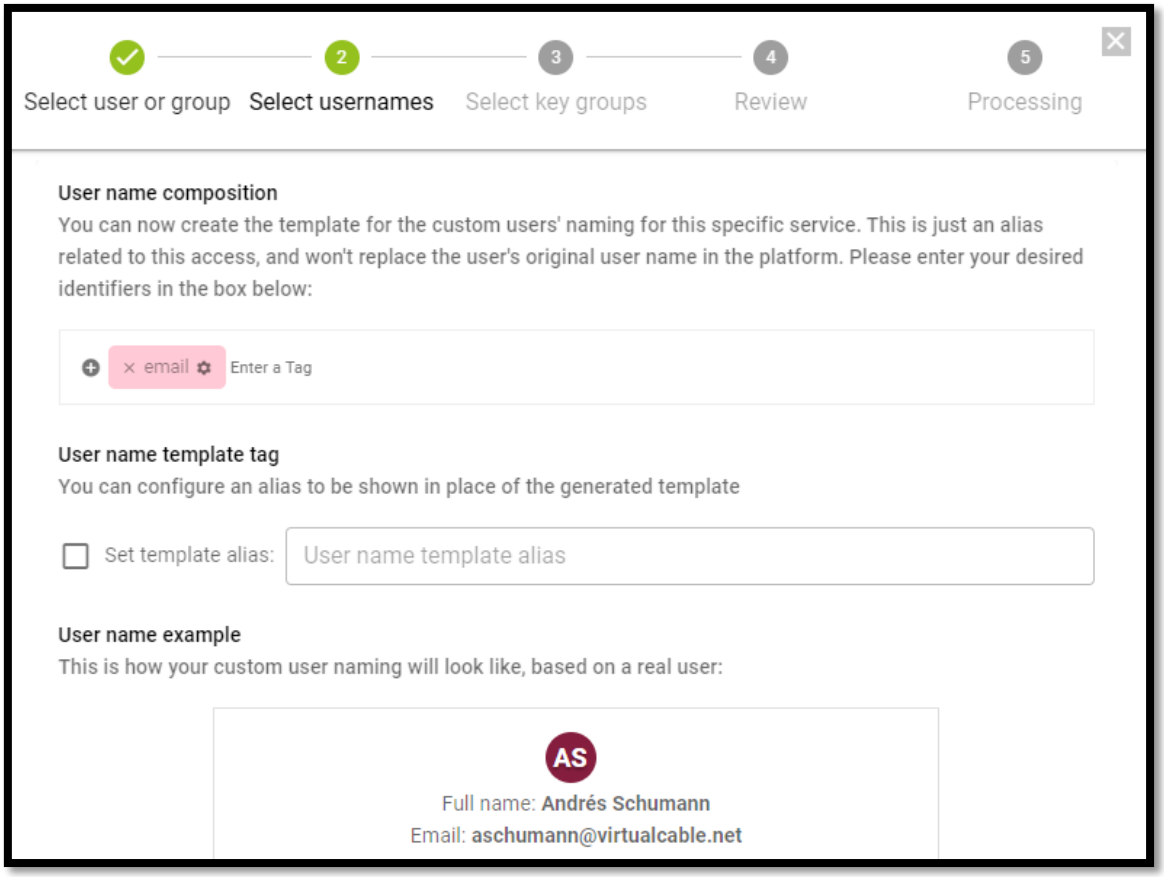
Una vez introducida la URL, finalizaremos el asistente.

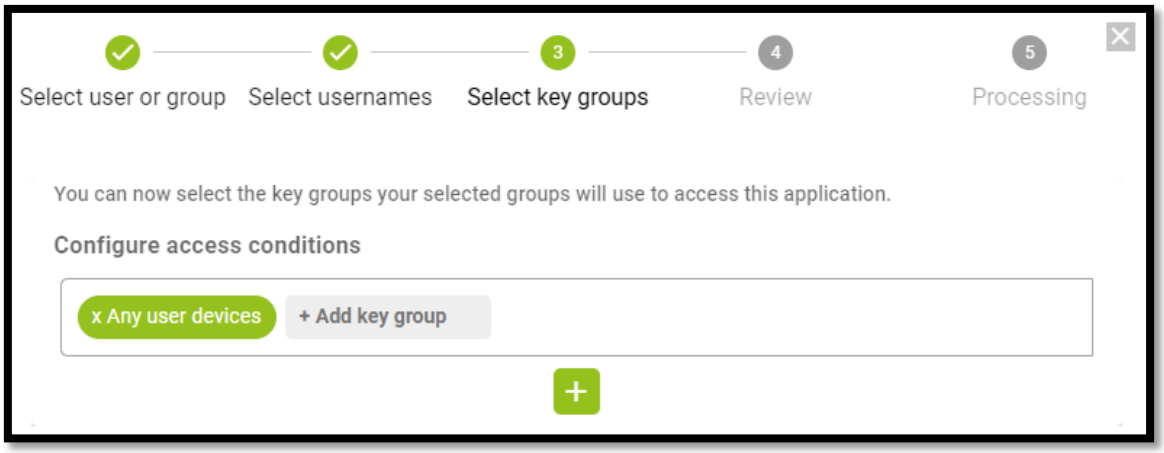
El siguiente paso será dar acceso a nuestros usuarios a dicha aplicación creada:

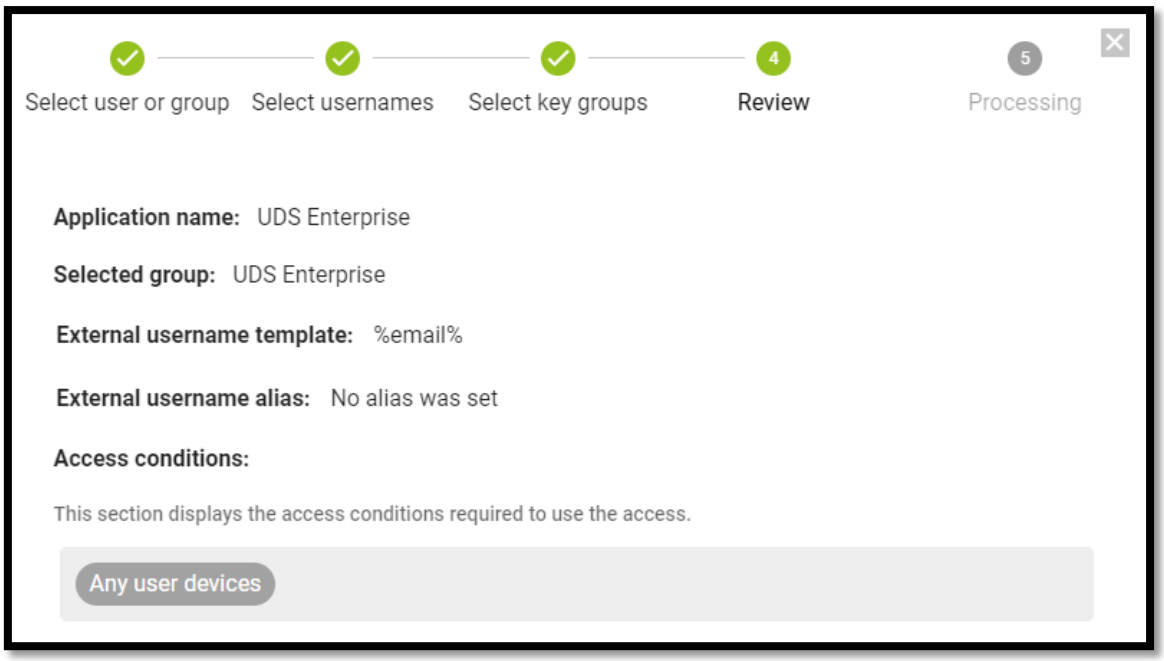


Podremos añadir usuarios individualmente o grupos de usuarios:





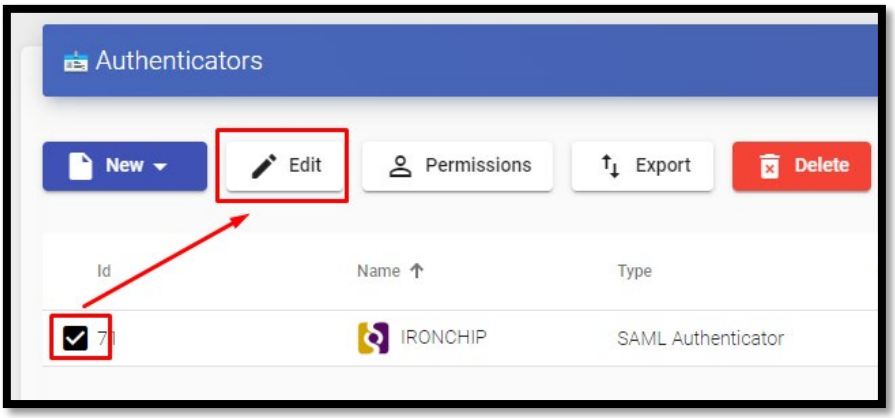




Con estos pasos tendremos creado nuestra aplicación en IRONCHIP y podremos continuar con el siguiente punto.

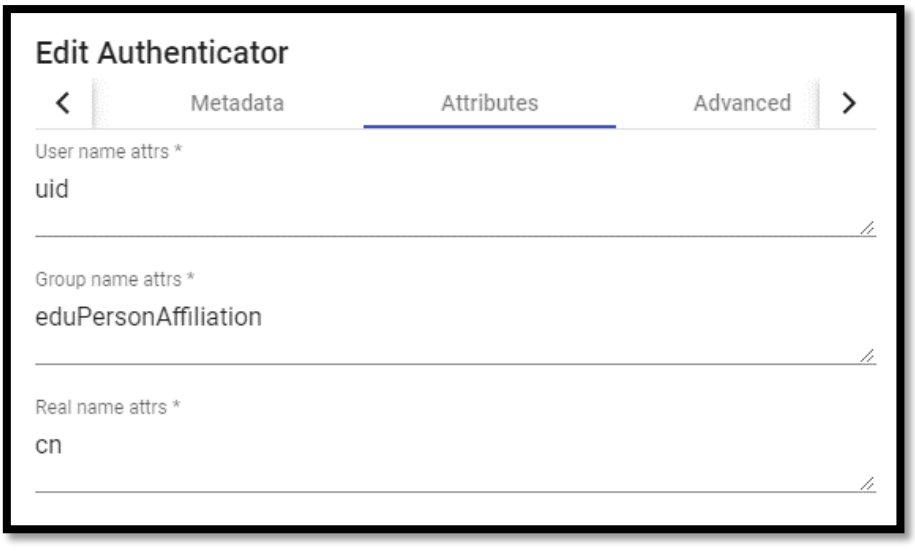
Definición de atributos en SAML en UDS Enterprise

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 documentación de IRONCHIP que por defecto son:

Description	Friendly Name	SAML Name
User Name	uid	urn:oid:0.9.2342.19200300.100.1.1
User Email	mail	urn:oid:0.9.2342.19200300.100.1.3
User given Name	givenName	urn:oid:2.5.4.42
User common Name	cn	urn:oid:2.5.4.3
User Groups	eduPersonAffiliation	urn:oid:1.3.6.1.4.1.5923.1.1.1.1

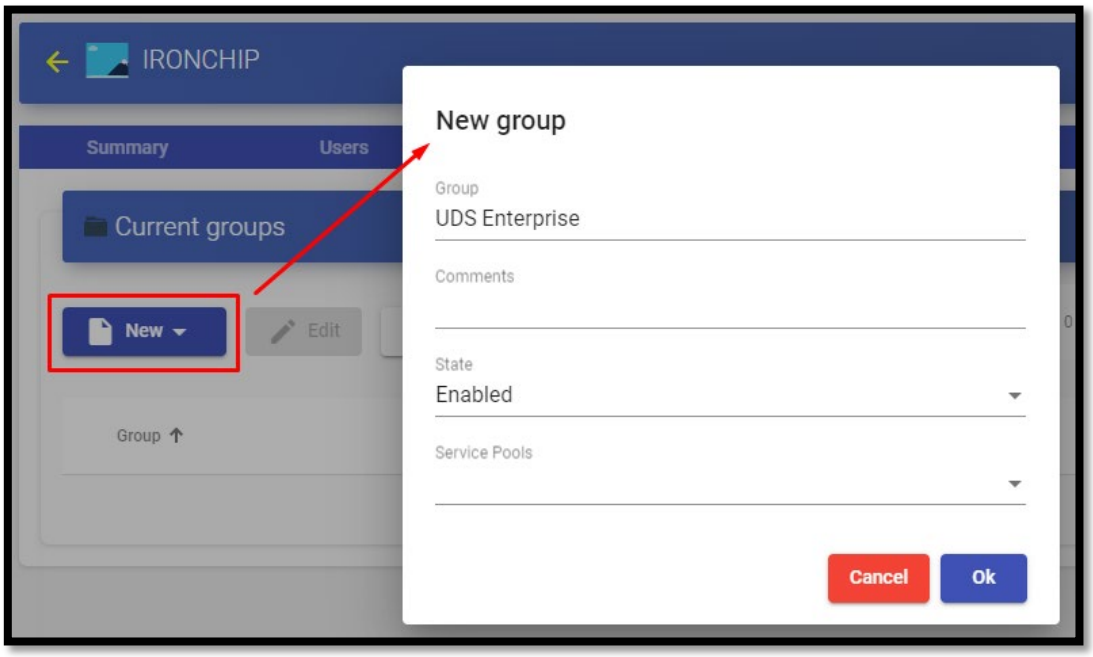


NOTA: En UDS Enterprise es posible indicar varios atributos o utilizar expresiones regulares. Por ejemplo, para indicar nuevos atributos de pertenencia a grupos.

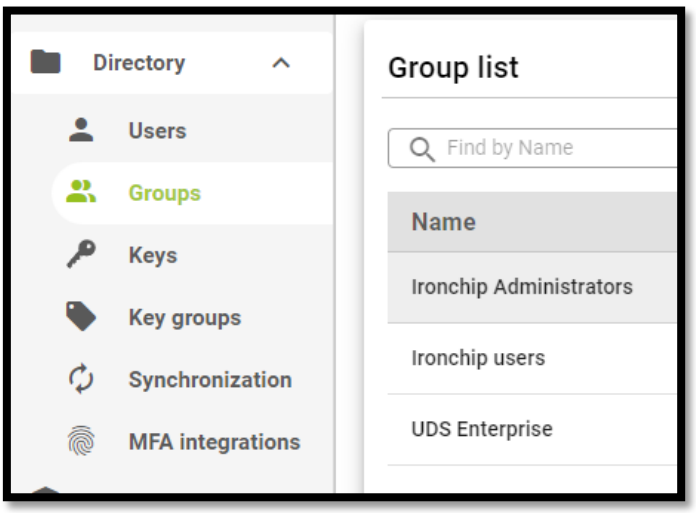
Una vez definidos correctamente los atributos, guardamos y accedemos al autenticador creado en UDS Enterprise.

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:

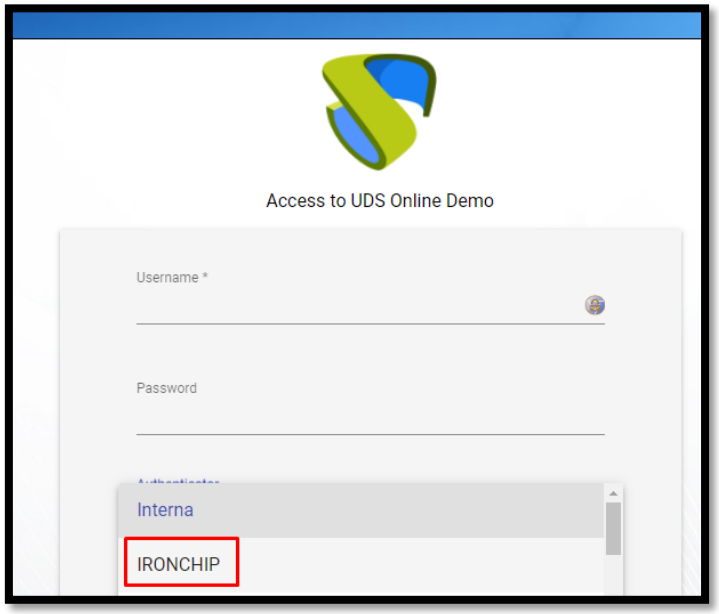


Añadimos todos los grupos necesarios (en este ejemplo, se añaden los diferentes departamentos a los que pertenecen los usuarios, puesto que el atributo de pertenencia a departamentos utilizado de IRONCHIP es el "**Groups**"):

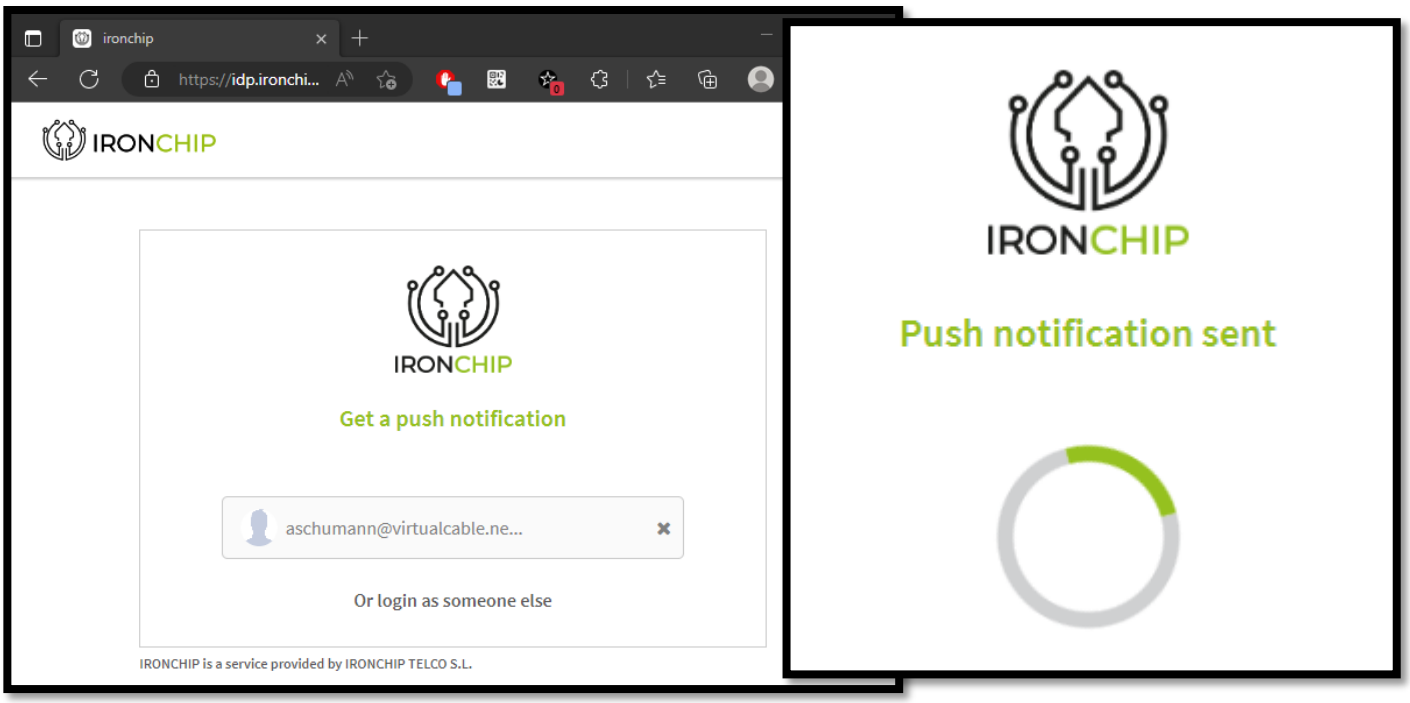


Acceso a través del autenticador

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

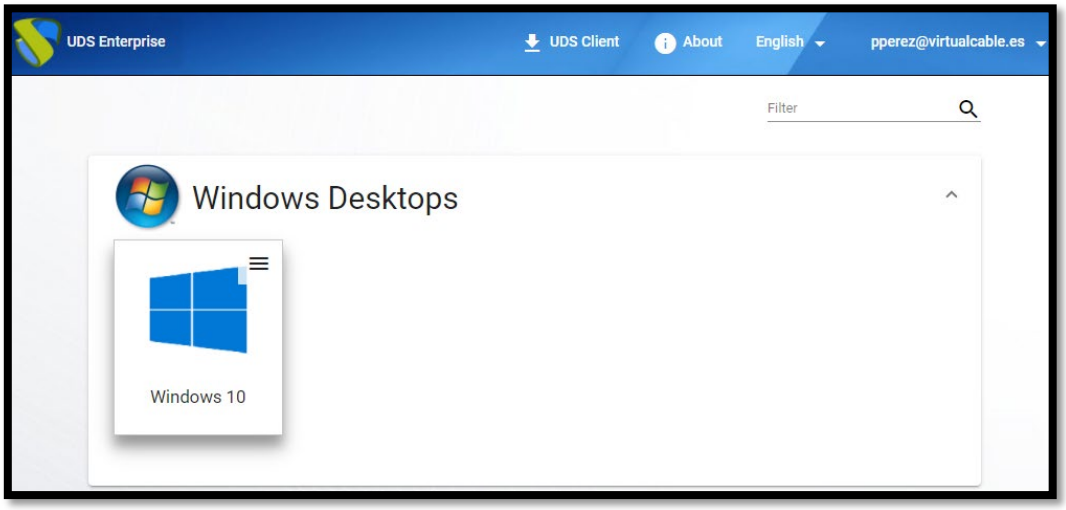


Al seleccionar el autenticador SAML, automáticamente se nos redireccionará a la página del proveedor. El sistema nos solicitará en este caso el email del usuario al que se le mandara un PUSH:



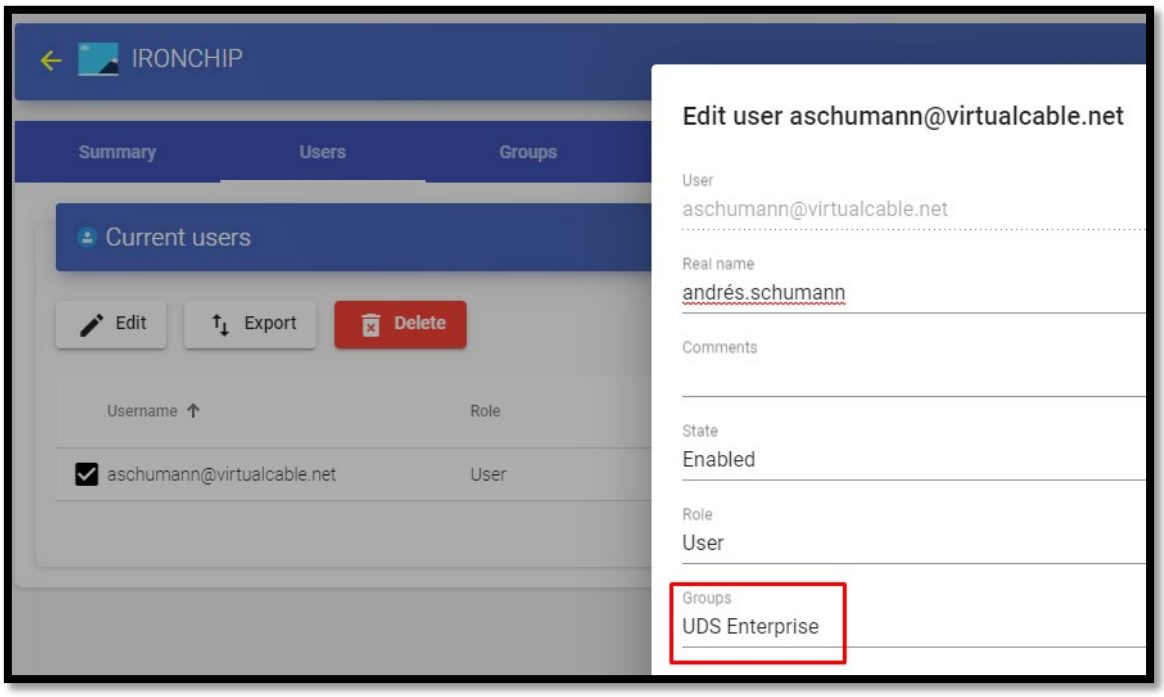
NOTA: El modo de validación será el configurado en el propio proveedor. Es decir, si disponemos de validación de los usuarios vía MFA, se utilizará.

Una vez realizado el login en IRONCHIP, 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 *andres* pertenece al grupo UDS Enterprise y, como está dado de alta como grupo en el autenticador, puede acceder.

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.udsenterprise.com o envíenos un email a info@udsenterprise.