



Autenticación de usuarios
de OneLogin en
UDS Enterprise

www.udsenderprise.com



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

Introducción	3
Creación de aplicación SAML de IRONCHIP	3
Creación del autenticador SAML en UDS Enterprise	5
Configuración de la aplicación SAML en IRONCHIP	9
Definición de atributos en SAML en UDS Enterprise	12
Acceso a través del autenticador	14
Sobre Virtual Cable.....	16



Autenticación de usuarios de Google Workspace en UDS Enterprise

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.

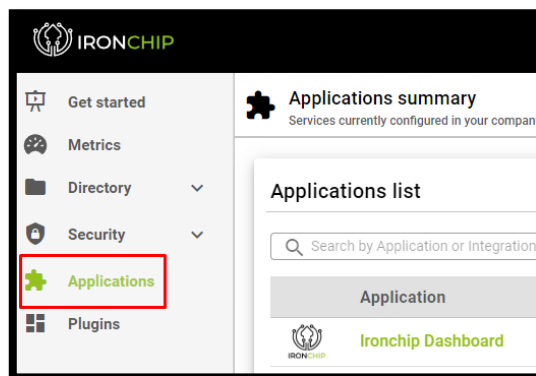
Una vez creado el nuevo autenticador en UDS Enterprise e integrado con IRONCHIP, los usuarios existentes en este entorno podrán acceder a los servicios publicados en UDS Enterprise.

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.

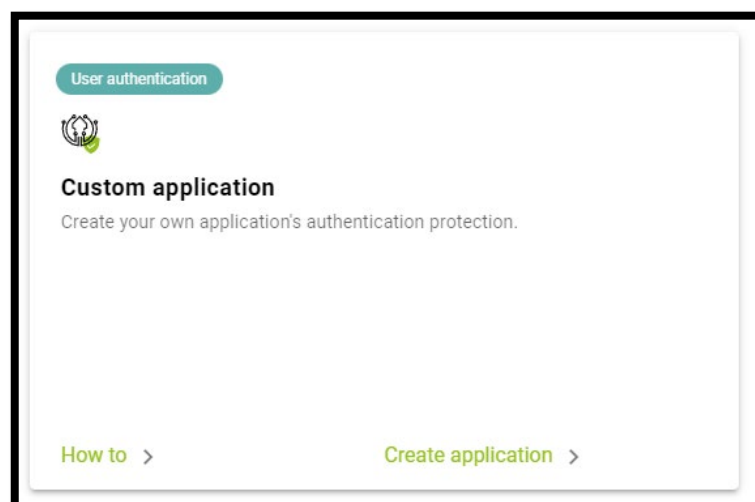
Creación de aplicación SAML de IRONCHIP

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:





Autenticación de usuarios de Google Workspace en UDS Enterprise

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**”:

Add a new application [X]

Application settings

Application name (alias)
UDS Enterprise

Application integration type

OIDC - OAUTH 2.0

API KEY

SAML

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

SAML service configuration

SAML integration allows you to connect SAML services through the location based authentication identity provider. This integration requires your service provider metadata file that is going to be downloaded from the URL you specify below.

Metadata URL

Download Ironchip's **SAML IDP metadata** to enable your Service Provider to properly communicate:

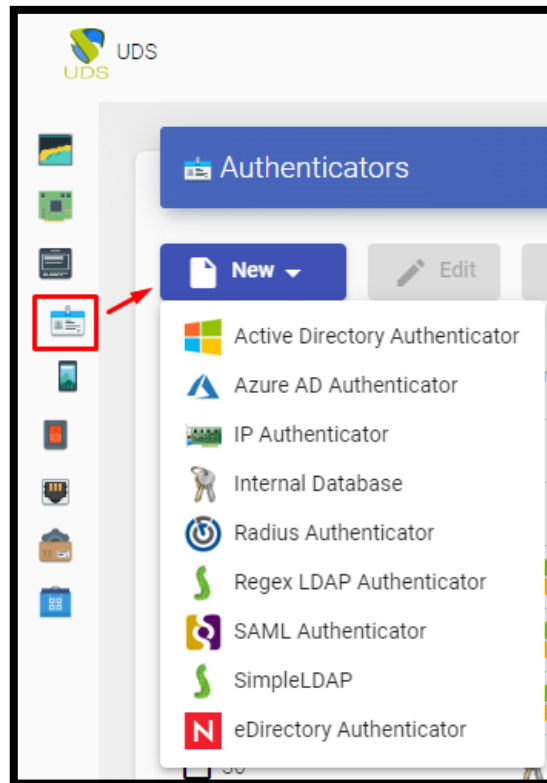
Download metadata file

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”.





Autenticación de usuarios de Google Workspace en UDS Enterprise

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

The screenshot shows the 'New Authenticator' form with the following fields and values:

- Tags: Tags for this element
- Name *: IRONCHIP
- Comments: Comments for this element
- Priority *: 1
- Label *: ironchip

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

The screenshot shows the 'New Authenticator' form with the following fields and buttons:

- Private key *
- Certificate *
- Buttons: Test, Discard & close, 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:



Autenticación de usuarios de Google Workspace en UDS Enterprise

```
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:~#
```

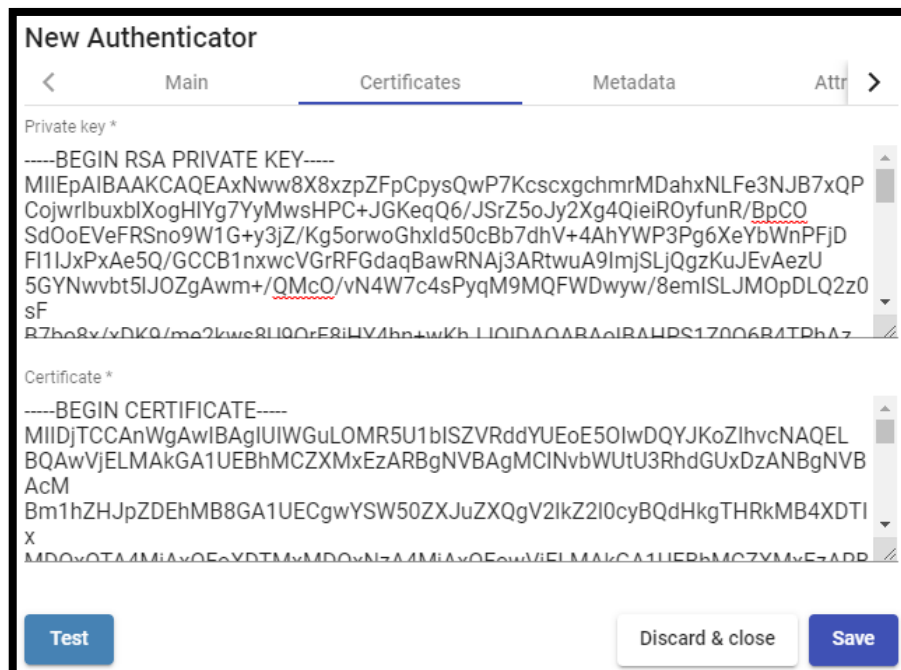
Ahora convertimos la clave a **rsa**:

```
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:~#
```

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





Autenticación de usuarios de Google Workspace en UDS Enterprise

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...):

New Authenticator

Main Certificates **Metadata** Attributes Advanced

IDP Metadata *

```
<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"></EncryptionMethod>
<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes192-cbc"></EncryptionMethod>
<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"></EncryptionMethod>
<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"></EncryptionMethod>
</KeyDescriptor>
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://idp.ironchip.com/saml/slo/646ccaeb36bc936923fc8022"></SingleLogoutService>
<NameIDFormat urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://idp.ironchip.com/saml/sso/646ccaeb36bc936923fc8022"></SingleSignOnService>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://idp.ironchip.com/saml/sso/646ccaeb36bc936923fc8022"></SingleSignOnService>
</IDPSSODescriptor>
</EntityDescriptor>
```

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

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.

Edit Authenticator

Main Certificates **Metadata** Attributes Advanced

IDP Metadata *

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" validUntil="2023-05-31T15:25:45.29Z"
cacheDuration="PT48H" entityID="https://idp.ironchip.com/saml/metadata/646ccaeb36bc936923fc8022">
```

Entity ID
https://demoaslan.udsenderprise.com/uds/page/auth/info/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.

Add an application image (optional)

UE Change image

SAML service configuration

SAML integration allows you to connect SAML services through the location based authentication identity provider. This integration requires your service provider metadata file that is going to be downloaded from the URL you specify below.

Metadata URL

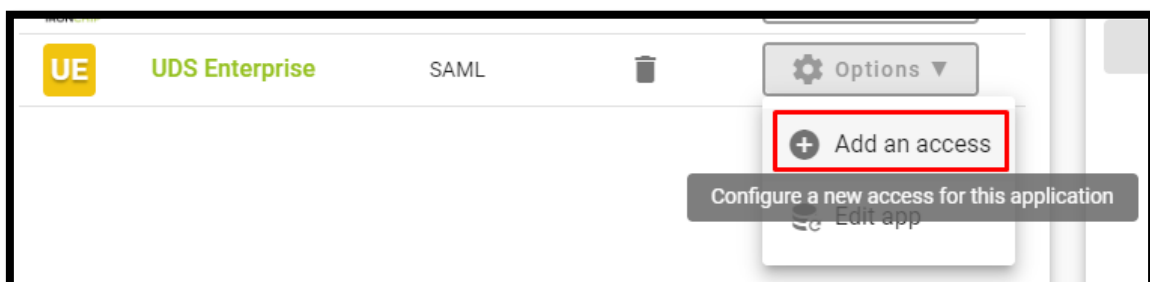
Download Ironchip's **SAML IDP metadata** to enable your Service Provider to properly communicate:

Download metadata file

Need help? Add service

Una vez introducida la URL, finalizaremos el asistente.

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





Autenticación de usuarios de Google Workspace en UDS Enterprise

Podremos añadir usuarios individualmente o grupos de usuarios:

The screenshot shows the first step of a five-step process: 'Select user or group'. The progress bar at the top indicates steps 1 through 5. Below the progress bar is a search bar labeled 'Find by Name' with a magnifying glass icon. A table lists four options, each with a checkbox and a person icon:

	Email
<input type="checkbox"/>	Andrés Schumann (aschumann@virtualcable.net)
<input type="checkbox"/>	Ironchip Administrators
<input type="checkbox"/>	Ironchip users
<input type="checkbox"/>	UDS Enterprise

The screenshot shows the second step of the process: 'Select usernames'. The progress bar at the top indicates steps 1 through 5, with step 2 highlighted. The main content area contains the following sections:

- User name composition**
You can now create the template for the custom users' naming for this specific service. This is just an alias related to this access, and won't replace the user's original user name in the platform. Please enter your desired identifiers in the box below:
- User name template tag**
You can configure an alias to be shown in place of the generated template
 Set template alias:
- User name example**
This is how your custom user naming will look like, based on a real user:

Full name: Andrés Schumann
Email: aschumann@virtualcable.net



Autenticación de usuarios de Google Workspace en UDS Enterprise

The screenshot shows a progress bar at the top with five steps: 1. Select user or group (checked), 2. Select usernames (checked), 3. Select key groups (active), 4. Review, and 5. Processing. Below the progress bar, the text reads: "You can now select the key groups your selected groups will use to access this application." Underneath, there is a section titled "Configure access conditions" with a list containing one item: "x Any user devices". To the right of this item is a "+ Add key group" button. A green "+" button is centered below the list.

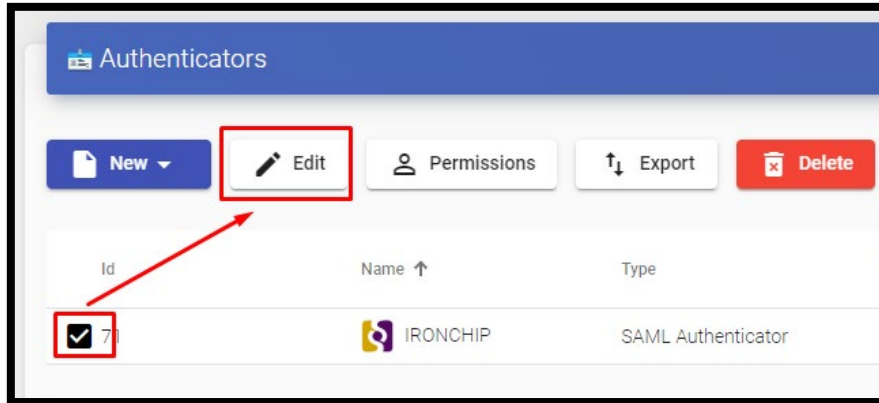
The screenshot shows the same progress bar, but now step 4 "Review" is active. The configuration details are as follows:
Application name: UDS Enterprise
Selected group: UDS Enterprise
External username template: %email%
External username alias: No alias was set
Access conditions:
This section displays the access conditions required to use the access.
Below this text is a list containing one item: "Any user devices".

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



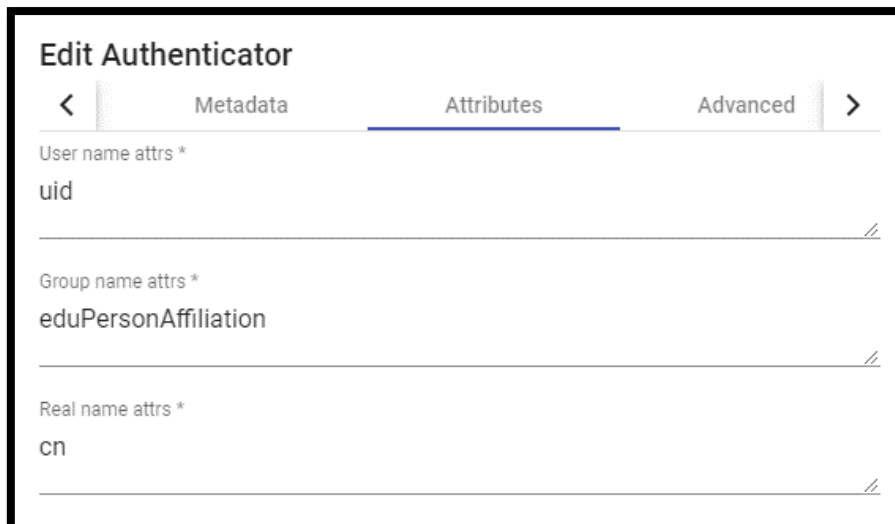
Definición de atributos en SAML en UDS Enterprise

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





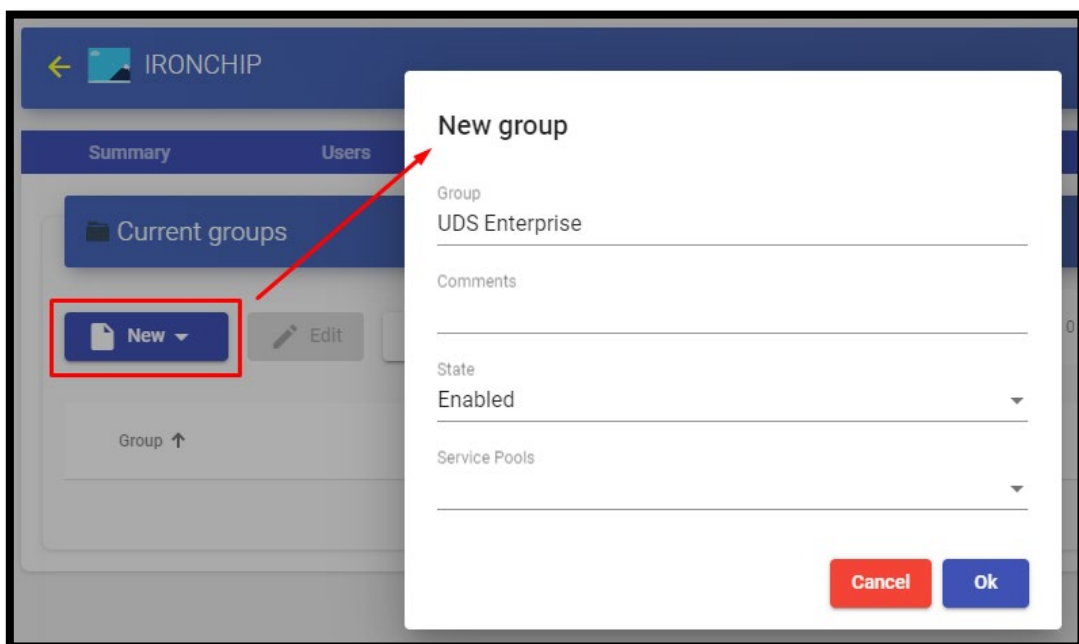
Autenticación de usuarios de Google Workspace en UDS Enterprise

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

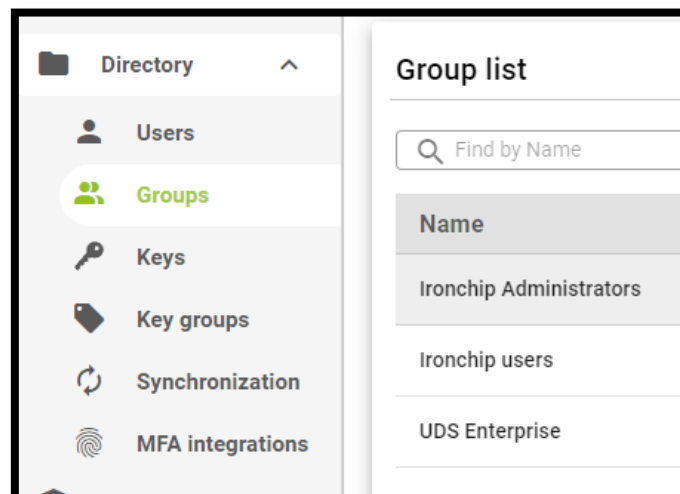
Una vez definidos correctamente los atributos, guardamos y accedemos al autenticador creado en UDS Enterprise.

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"**):

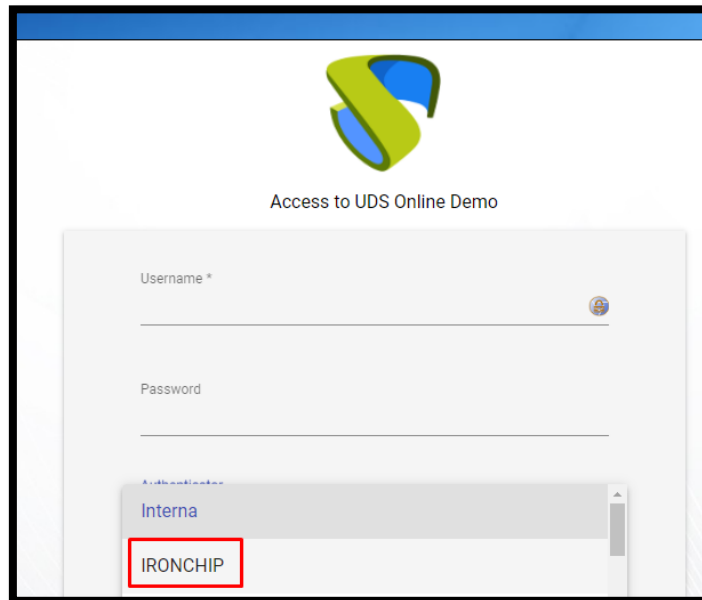




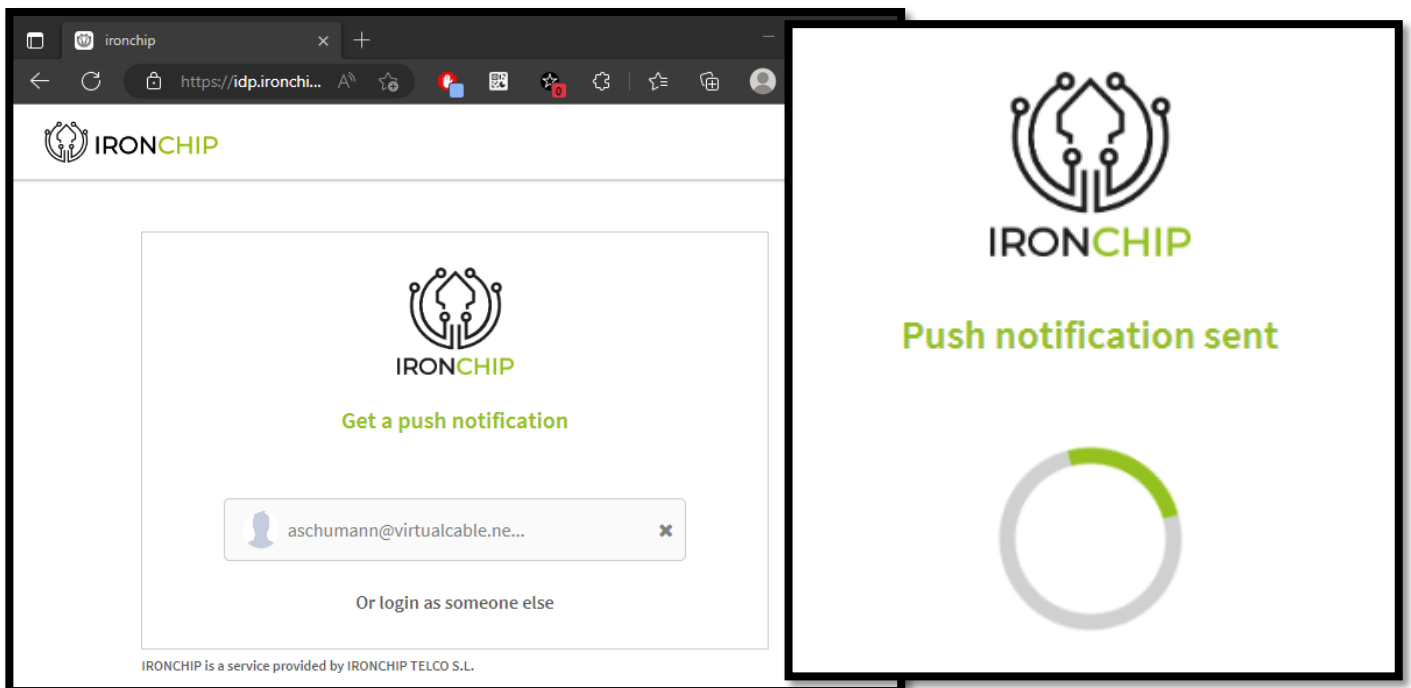
Autenticación de usuarios de Google Workspace en UDS Enterprise

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 en este caso el email del usuario al que se le mandará un PUSH:

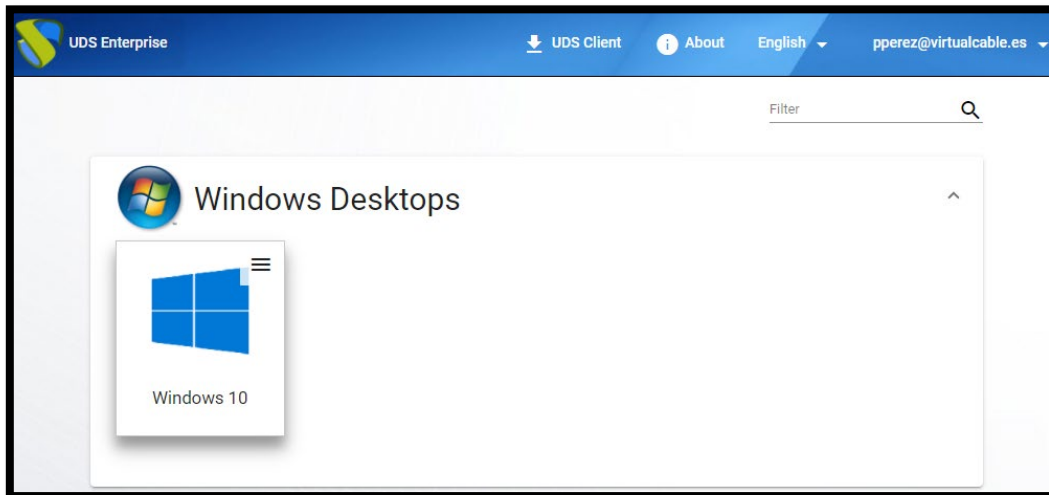




Autenticación de usuarios de Google Workspace en UDS Enterprise

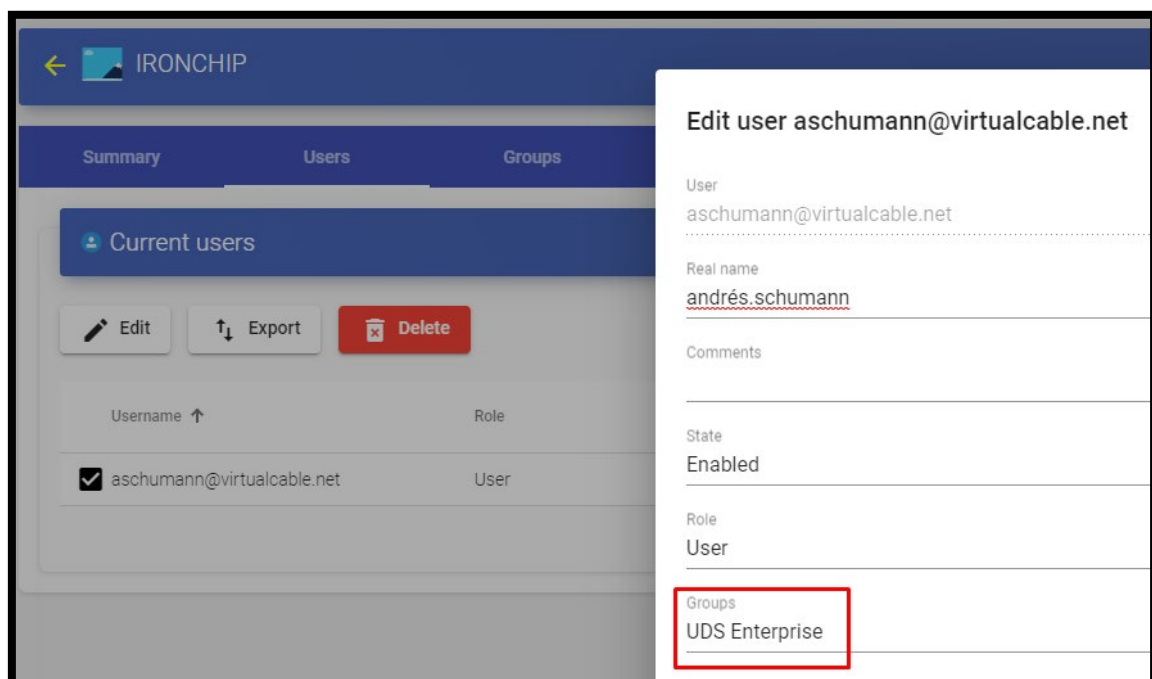
NOTA: El modo de validación será el configurado en el propio proveedor. Es decir, si disponemos de validación de los usuarios vía MFA, se utilizará.

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.



Autenticación de usuarios de Google Workspace en UDS Enterprise

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 o envíenos un email a info@udsenderprise.