
OneLogin user
authentication at
UDS Enterprise
www.udsenterprise.com

Introduction

This document shows how to integrate a SAML type authenticator from UDS Enterprise 3.5 to validate existing users in IRONCHIP.

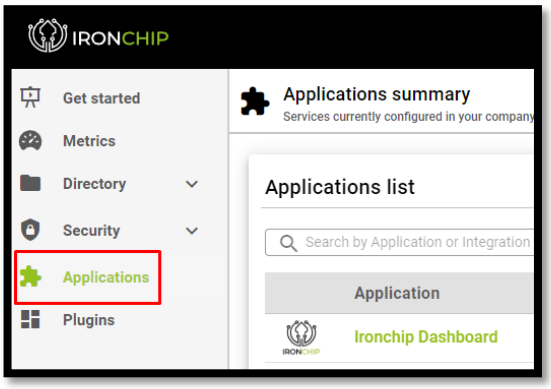
Once the new authenticator has been created in UDS Enterprise and integrated with IRONCHIP, existing users in this environment will be able to access the services published in UDS Enterprise.

In order to perform this integration, it will be necessary to have a user registered in UDS Enterprise and a user of the IRONCHIP platform, both with administration permissions on their different environments.

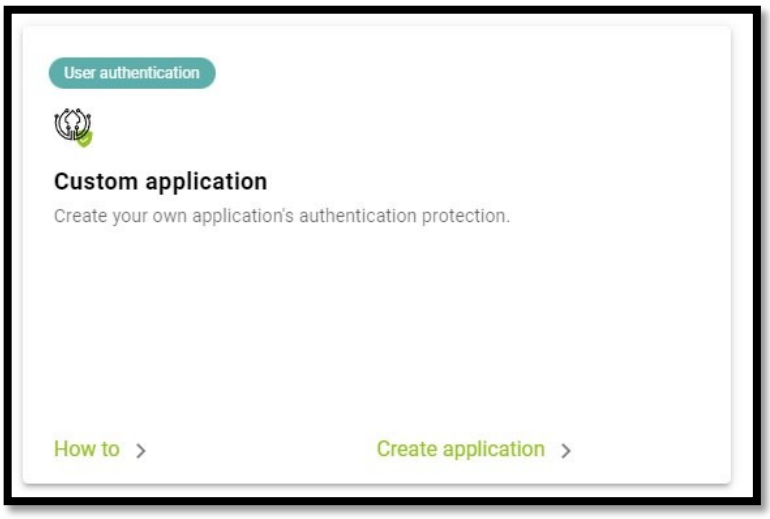
Creation of IRONCHIP SAML application

The first task will be performed in the IRONCHIP administration panel. We will need a user with administration permissions.

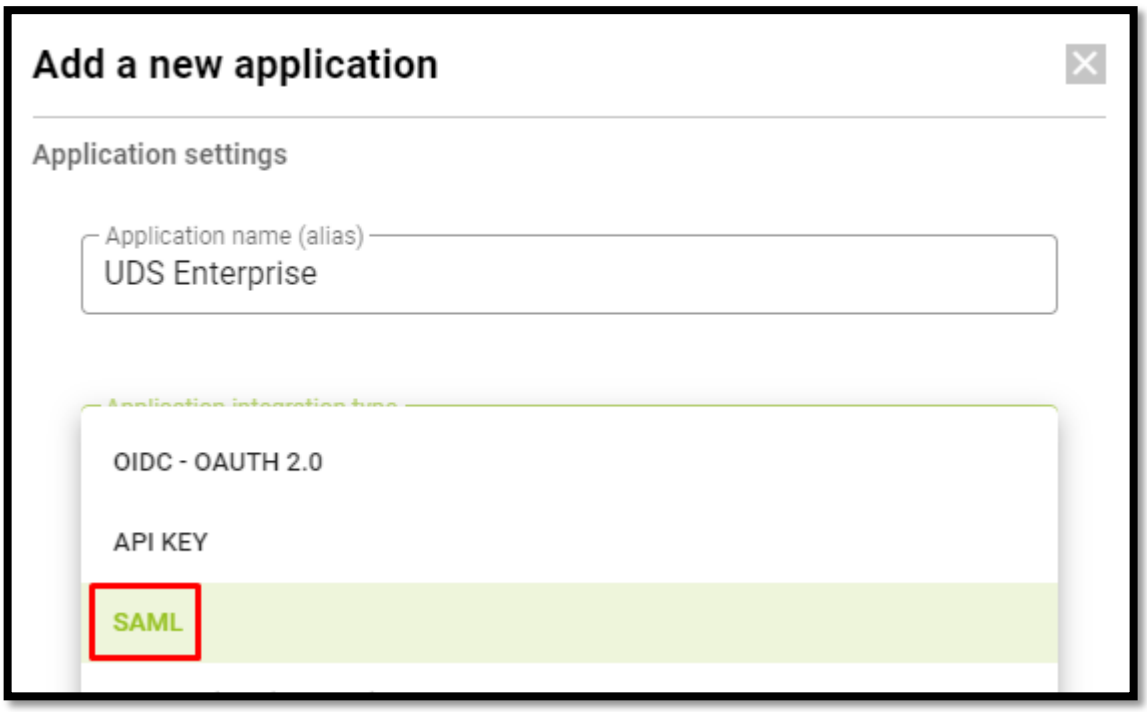
Access the IRONCHIP administration panel and select "**SAML apps**".



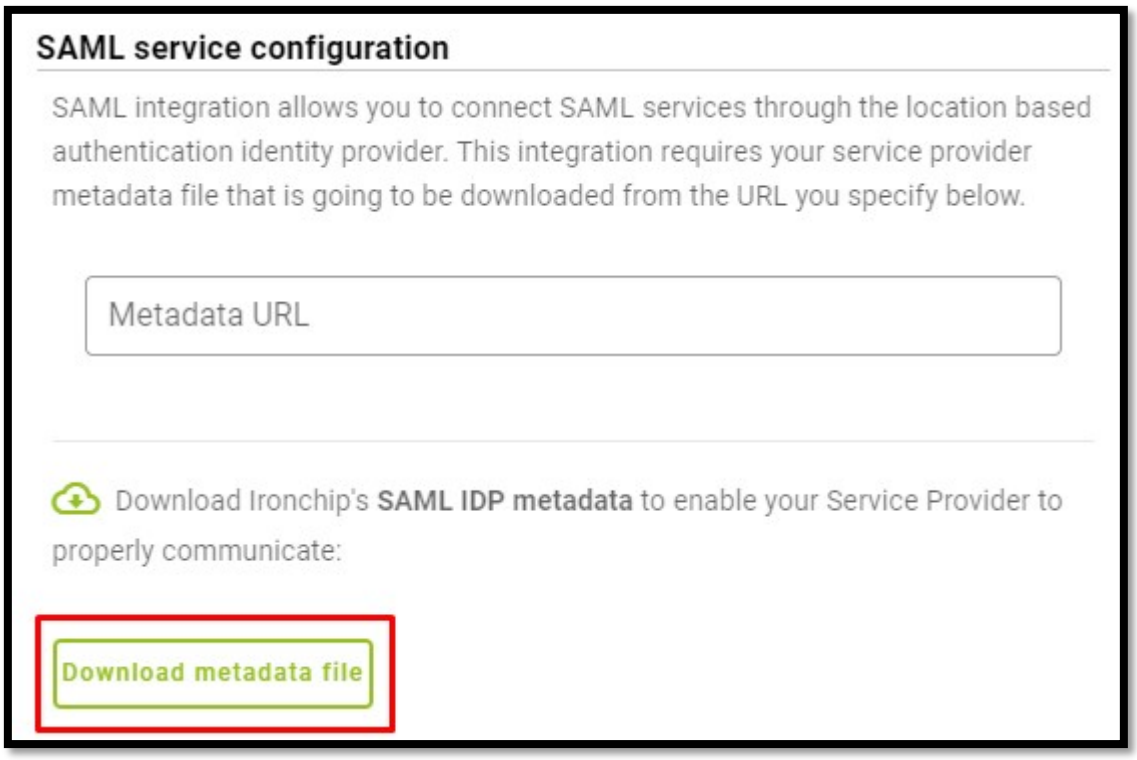
We will have to register a new customized SAML application:



In the configuration wizard we indicate a name to identify the application and select the type of integration we want to do, which will be of type "**SAML**":



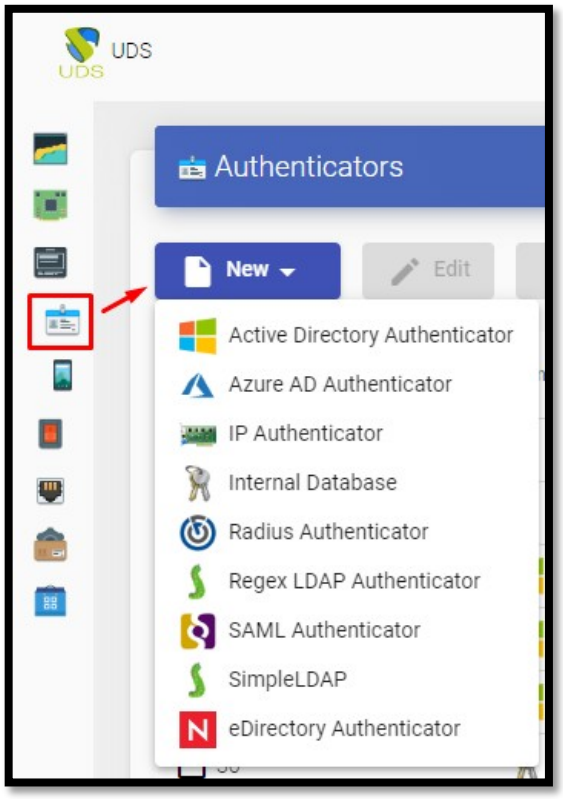
Once this option is selected we can download the Metadata generated by IRONCHIP:



Once downloaded, leave this window open and move on to the next step

Creation of the SAML authenticator in UDS Enterprise

Access the UDS Enterprise administration and go to the "**Authenticators**" section, select "**New**" and choose "**SAML Authenticator**".



In the "**Main**" tab we will indicate a name for the authenticator (it cannot contain spaces), the priority and a "**Label**".

In the "**Certificates**" tab we must indicate a valid certificate and its key. They must be in PEM format:

If you do not have certificates, you can generate one with **OpenSSL**. To generate it, we will use the following sentence (the UDS server has **OpenSSL** installed, 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, we must share the key with RSA, for this, we will use the following command:

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

Example of certificate generation:

```
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:~#
```

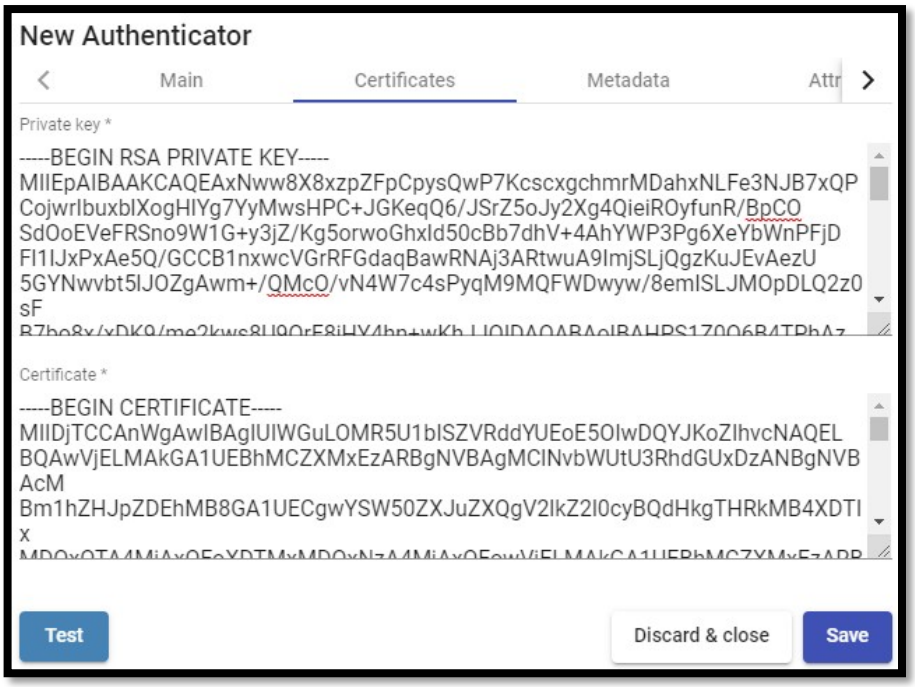
Now we convert the key to **rsa:**

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

Copy the contents of the certificate file and the **rsa** key to UDS:

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

The key will be copied in the "**Private Key**" section and the certificate in "**Certificate**":



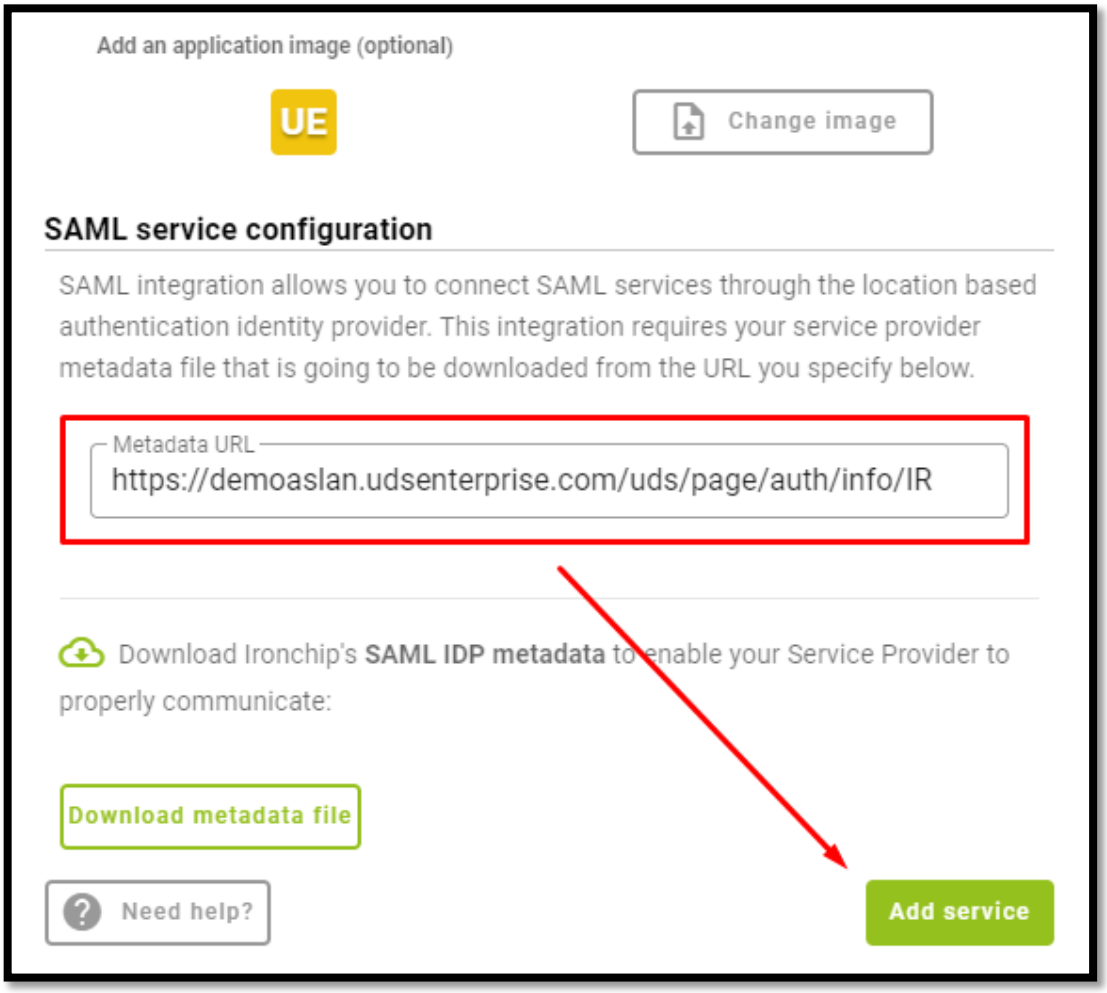
In the next tab, "**Metadata**", we will complete the "**IDP Metadata**" section with the metadata downloaded from IRONCHIP in previous steps (step 2 of the custom SAML application registration). It is important to copy the complete content of the file. To do so, it is recommended to open the file with a suitable application and never with a browser (it hides parts of the code...):

The "**Entity ID**" section will be left empty, as it will be automatically filled in when the authenticator is saved. The data will be generated based on the URL used in the connection to the UDS Enterprise portal.

We save the authenticator (we will have to indicate any data in the "**Attributes**" tab to allow us to save. In the following steps we will return to this section and the final configuration will be applied) and when editing it again we will be able to obtain the "**Entity ID**" data necessary to be able to continue configuring the SAML custom application in the IRONCHIP console.

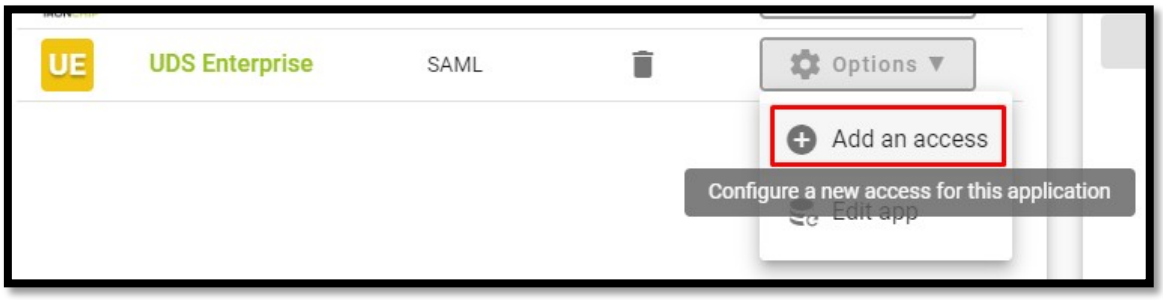
SAML application configuration in IRONCHIP

We return to the IRONCHIP configuration wizard to create a custom SAML application, where it will ask us for the "**Metadata URL**" generated in the previous step once we have saved and re-edited the authenticator in UDS Enterprise.

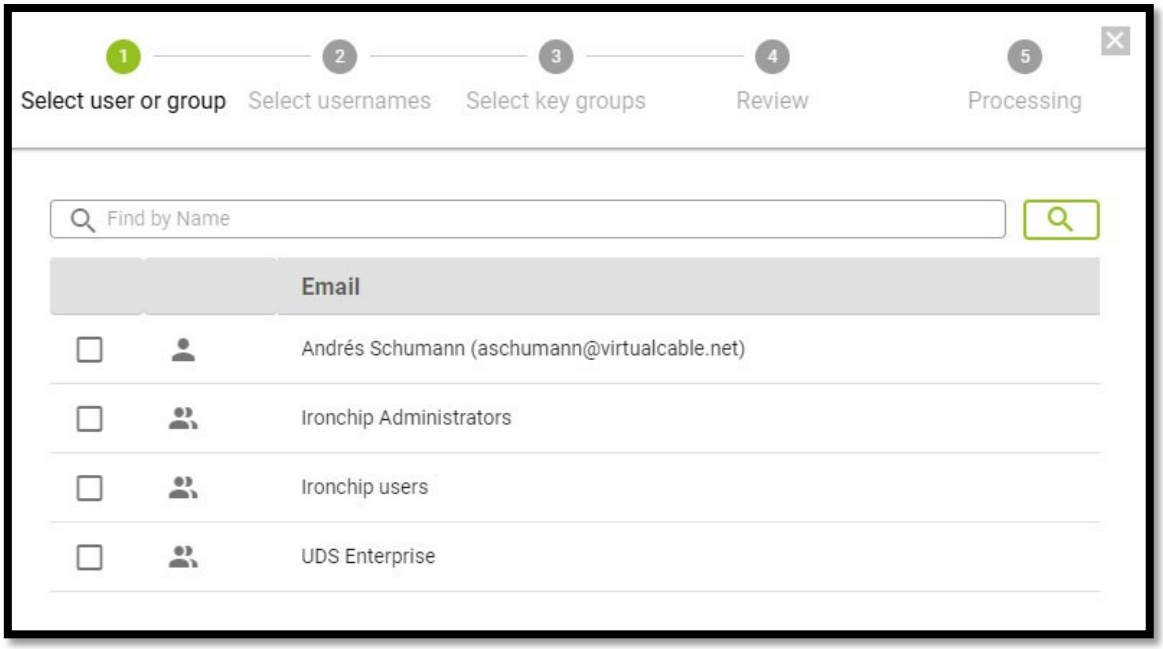


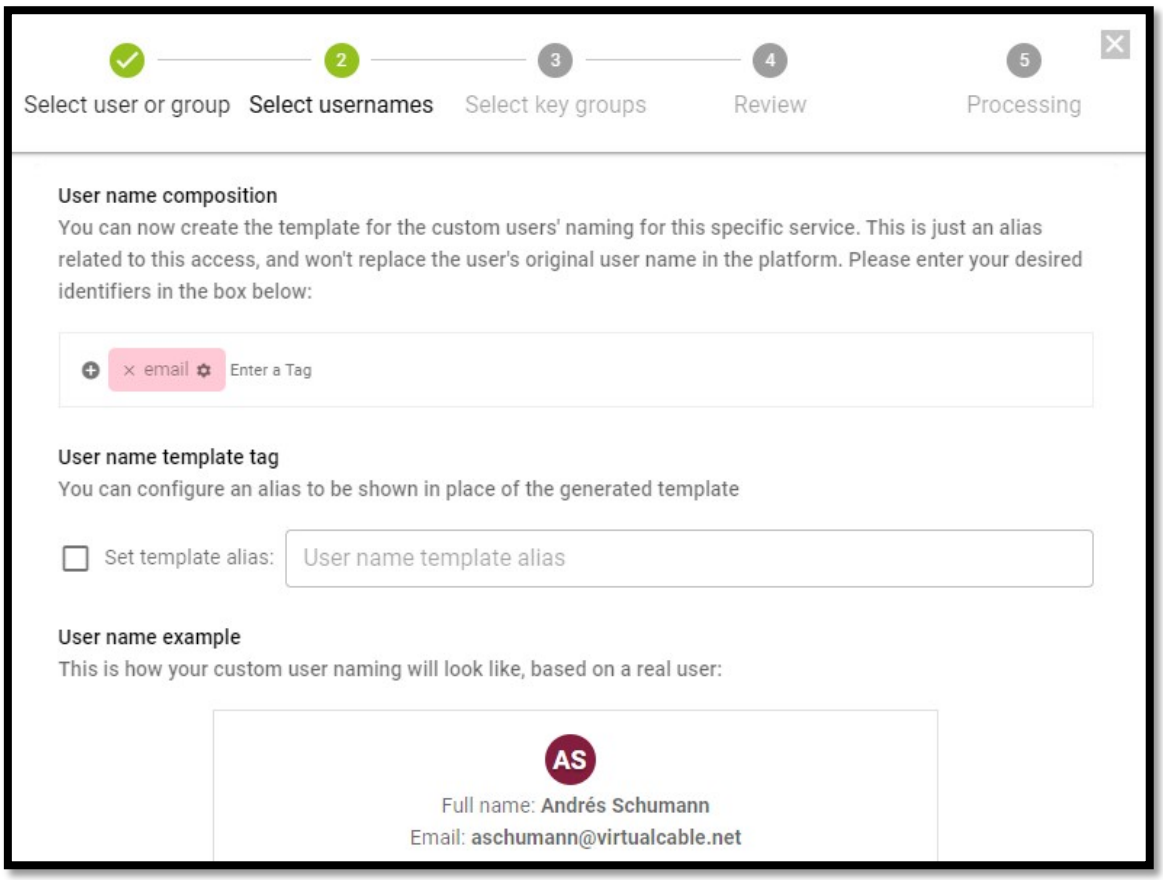
Once the URL has been entered, we will finish the wizard.

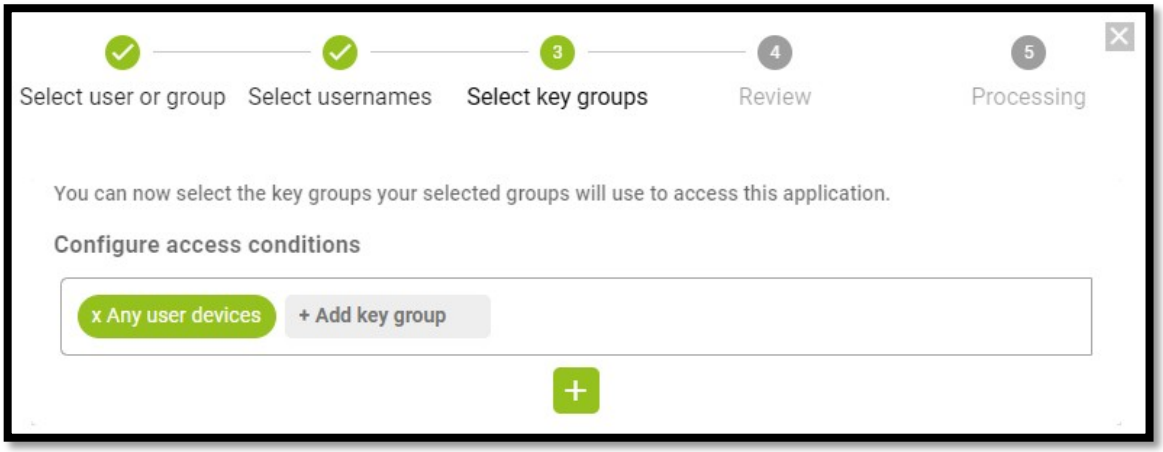
The next step will be to give our users access to the created application:

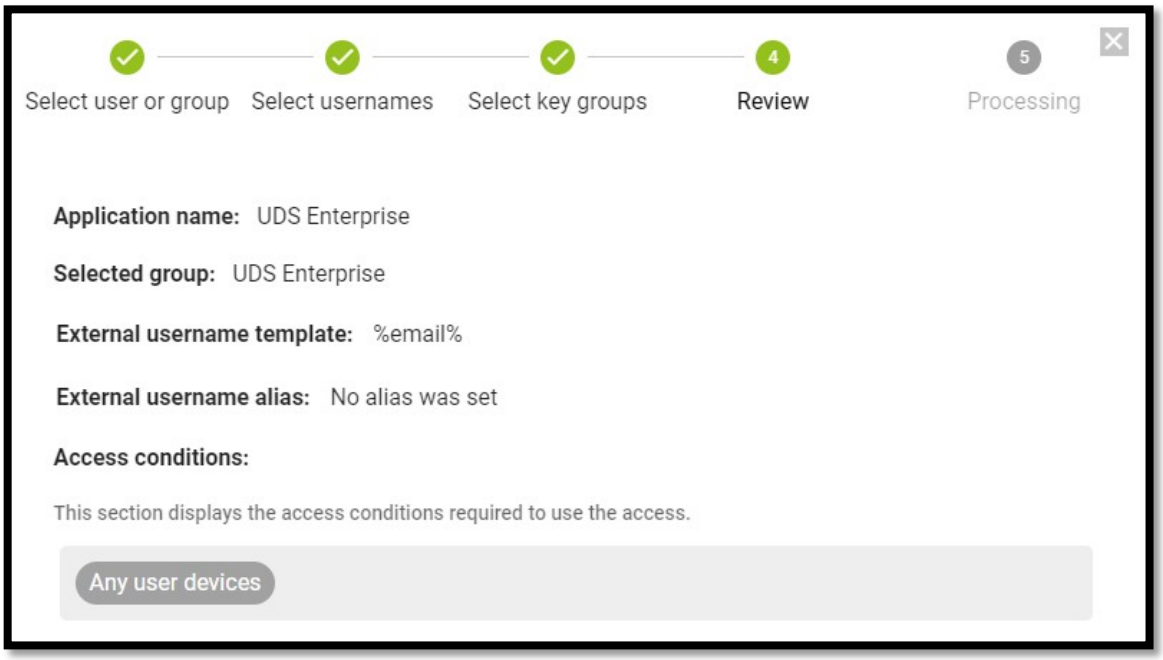


We will be able to add users individually or groups of users:





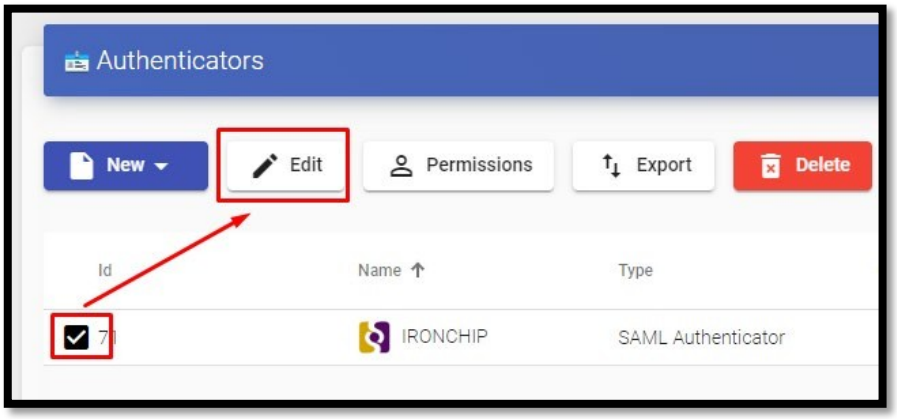




With these steps we will have created our application in IRONCHIP and we will be able to continue with the following point.

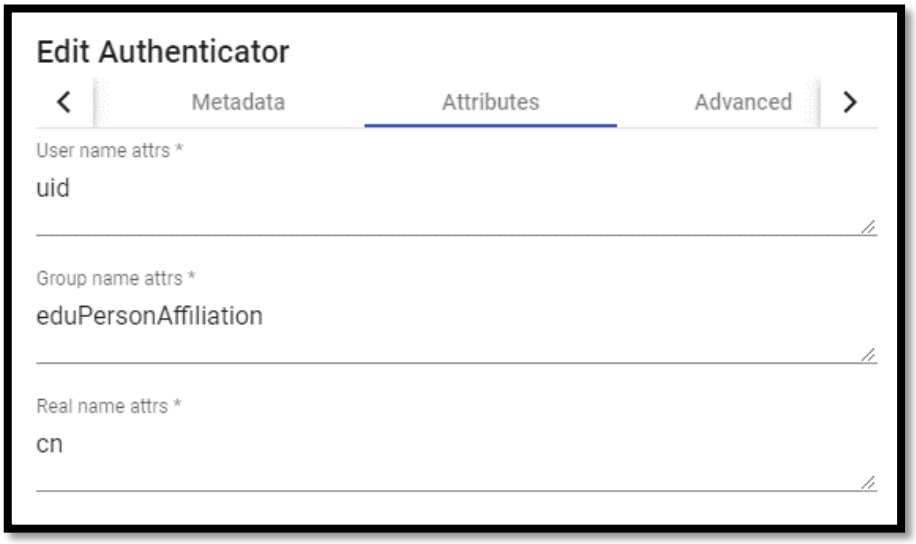
SAML Attribute Definition in UDS Enterprise

Access the UDS Enterprise administration, select the SAML authenticator previously created and edit it.



In the "**Attributes**" section we will indicate the correct attributes. They are defined and visible in the IRONCHIP documentation and by default they are:

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

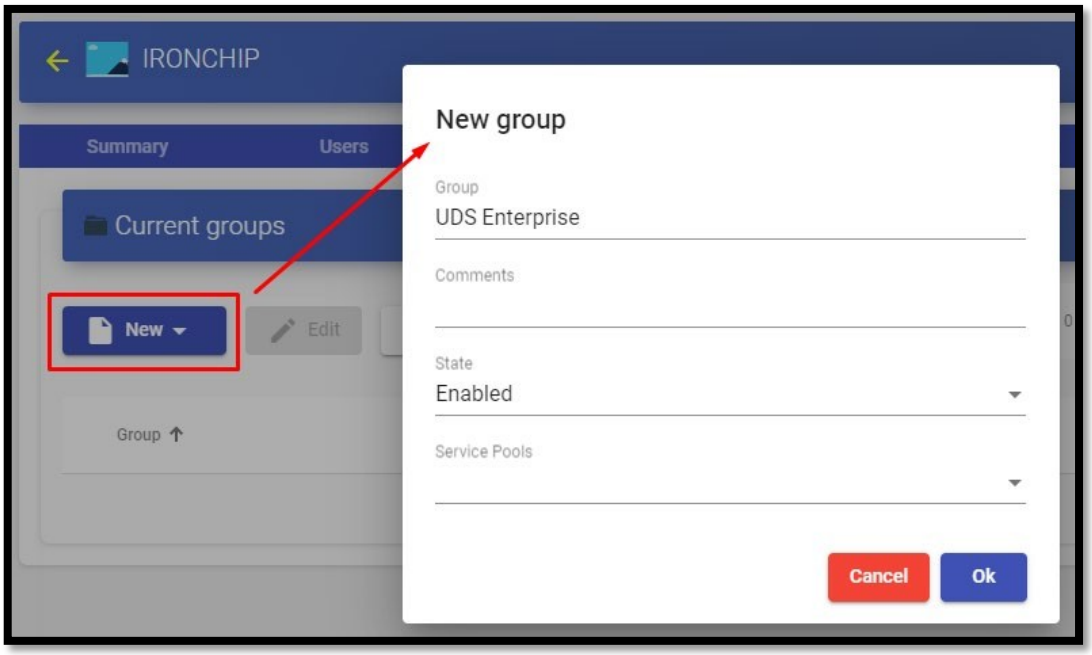


NOTE: In UDS Enterprise it is possible to specify several attributes or use regular expressions. For example, to specify new group membership attributes.

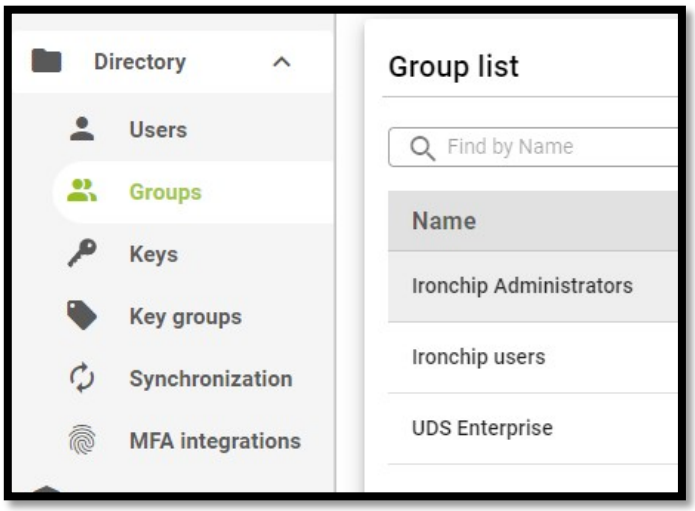
Once the attributes are correctly defined, we save and access the authenticator created in UDS Enterprise.

Within the authenticator, access the "**Groups**" section to add the necessary groups.

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

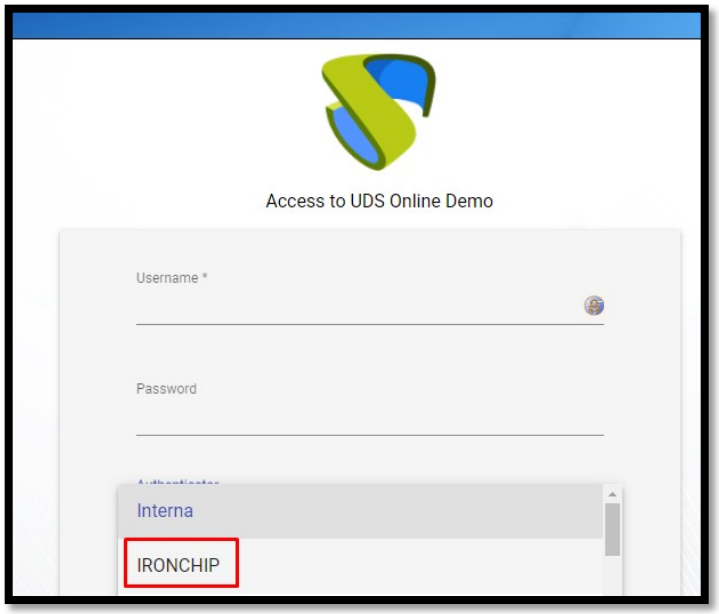


We add all the necessary groups (in this example, we add the different departments to which the users belong, since the IRONCHIP department membership attribute used is "**Groups**"):

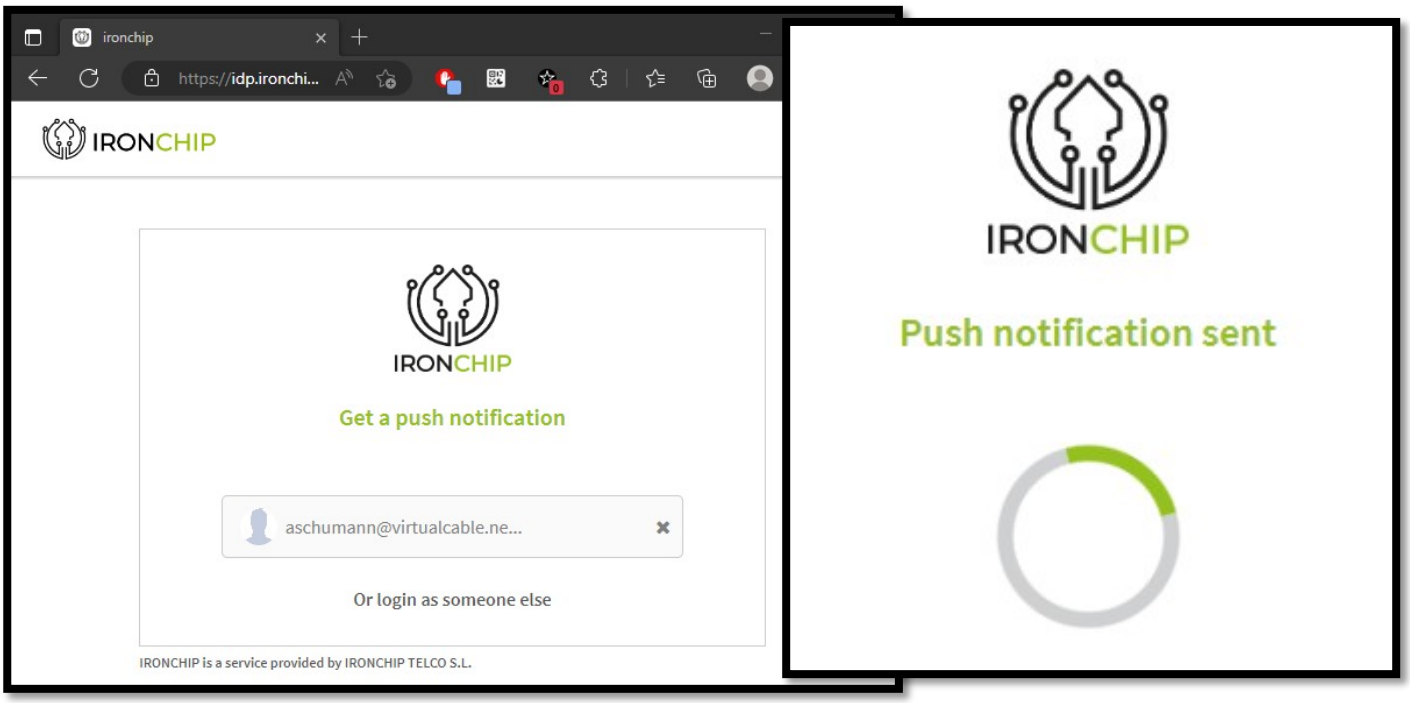


Access through the authenticator

To confirm that all the configuration is correct, we access the UDS Enterprise portal through the newly created SAML authenticator:

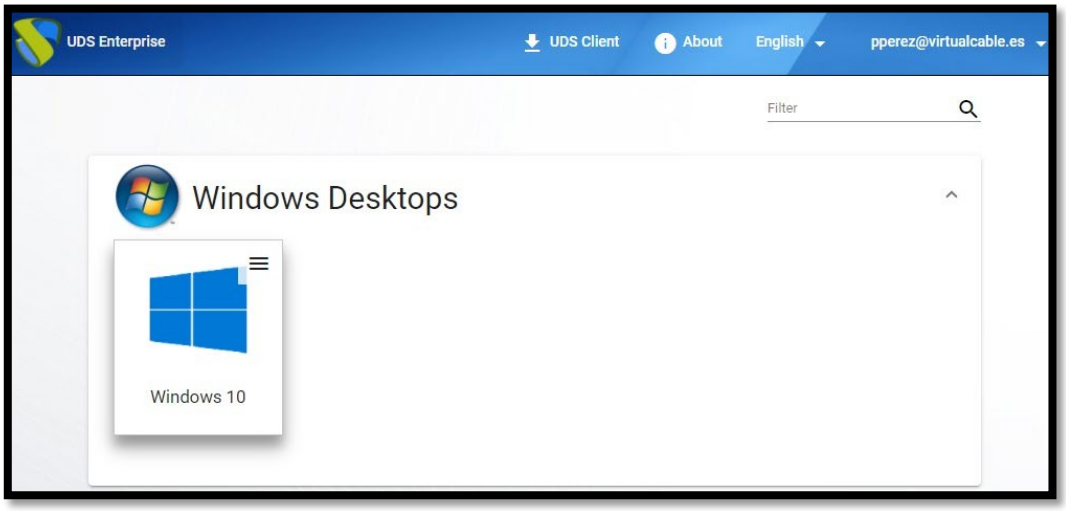


When selecting the SAML authenticator, we will be automatically redirected to the provider's page. In this case, the system will ask for the user's email address to which a PUSH will be sent:



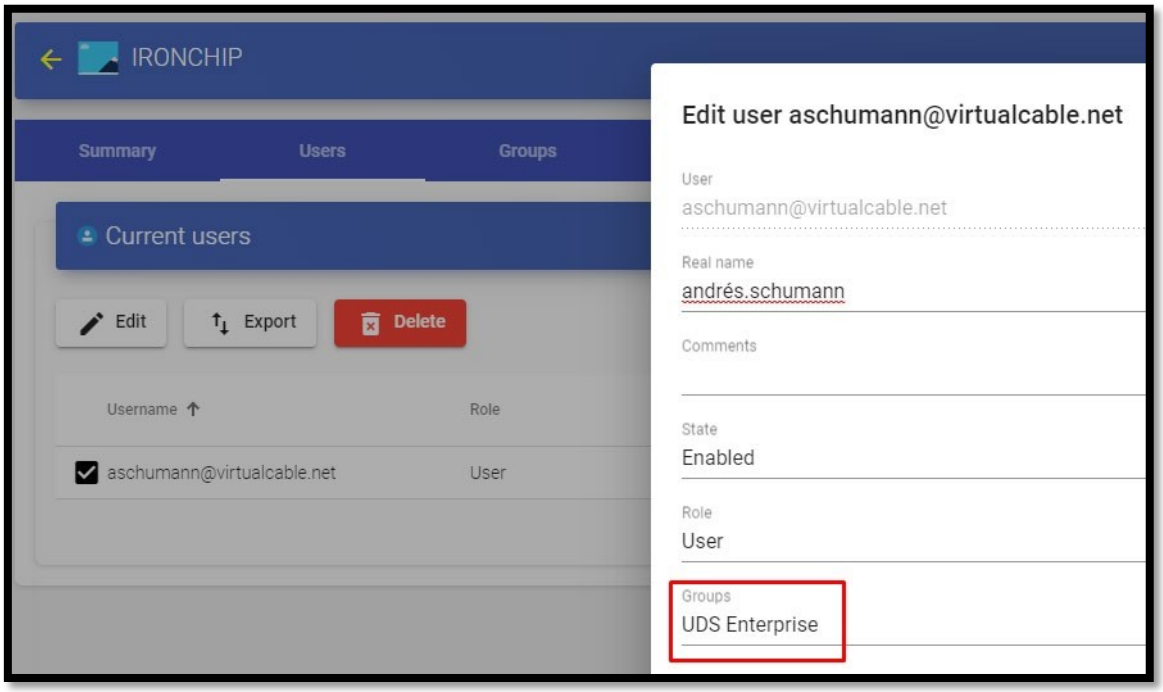
NOTE: The validation mode will be the one configured in the provider itself. That is, if we have user validation via MFA, it will be used.

Once the IRONCHIP login is done, a redirection will take place and we will return to the UDS Enterprise services page:



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

We can check which groups a user belongs to by editing it. To do this, access the authenticator and edit the user:



We can verify that, in this example, the user *andres* belongs to the UDS Enterprise group and, as he is registered as a group in the authenticator, he can access.

About Virtual Cable

Virtual Cable develops and markets UDS Enterprise through a subscription model, including support and upgrades, depending on the number of users.

In addition, Virtual Cable offers professional services to install and configure UDS Enterprise.

For more information, visit www.udsenterprise.com or send us an email at info@udsenterprise.