VIRTUAL CABLE

Multi Factor Authentication in UDS Enterprise (MFA)

Indice

INTRODUCTION

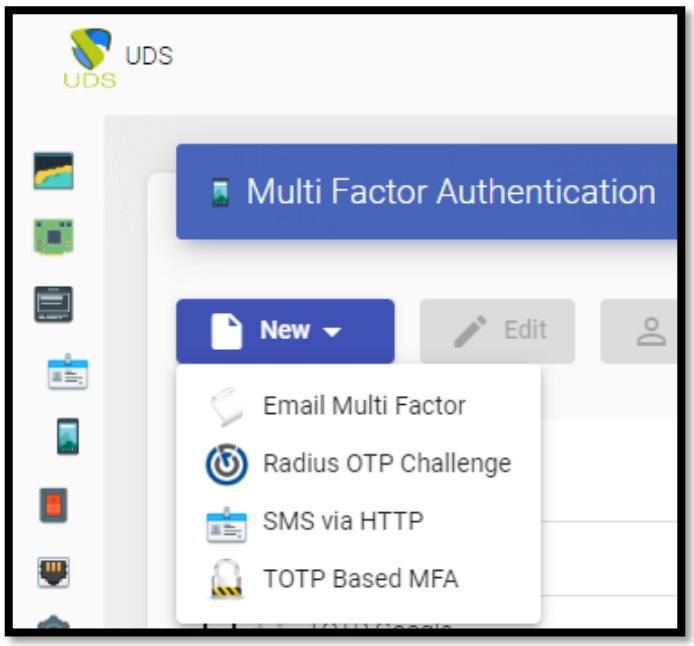
The following manual details the steps to follow to achieve double authentication for our users when they access the UDS Enterprise platform.

This double authentication can be carried out in any of the existing authenticators in UDS

NOTE: It is very important in the case of using MFA with UDS to have the time of the UDS appliances correctly configured, otherwise errors may appear at the time of authentication.

Double authentication methods

In UDS Enterprise, 4 main double authentication methods have been incorporated.



The configuration of this method will be done in the UDS control panel by accessing the "Multifactor" tab.

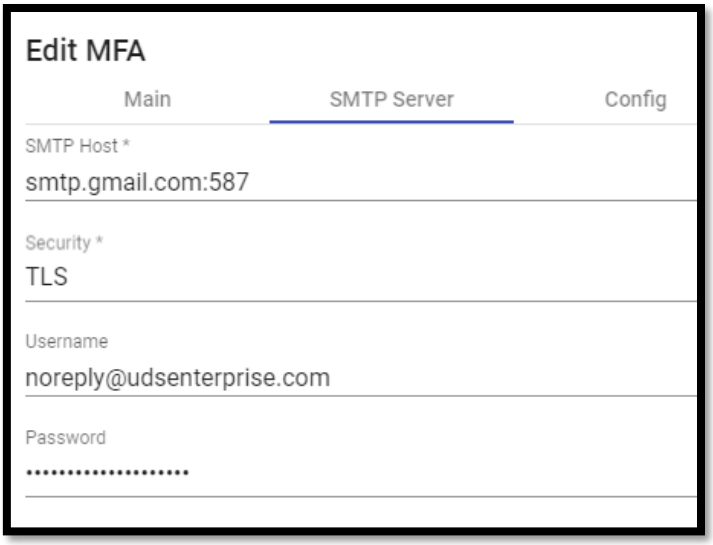
1. Email Multi Factor

Using this method, the user will first authenticate with their username and password and then be redirected to a second authentication process where they will receive an email with the necessary code to finally authenticate on their UDS Enterprise platform.

In its configuration we will indicate the following data at least:

Main tab:

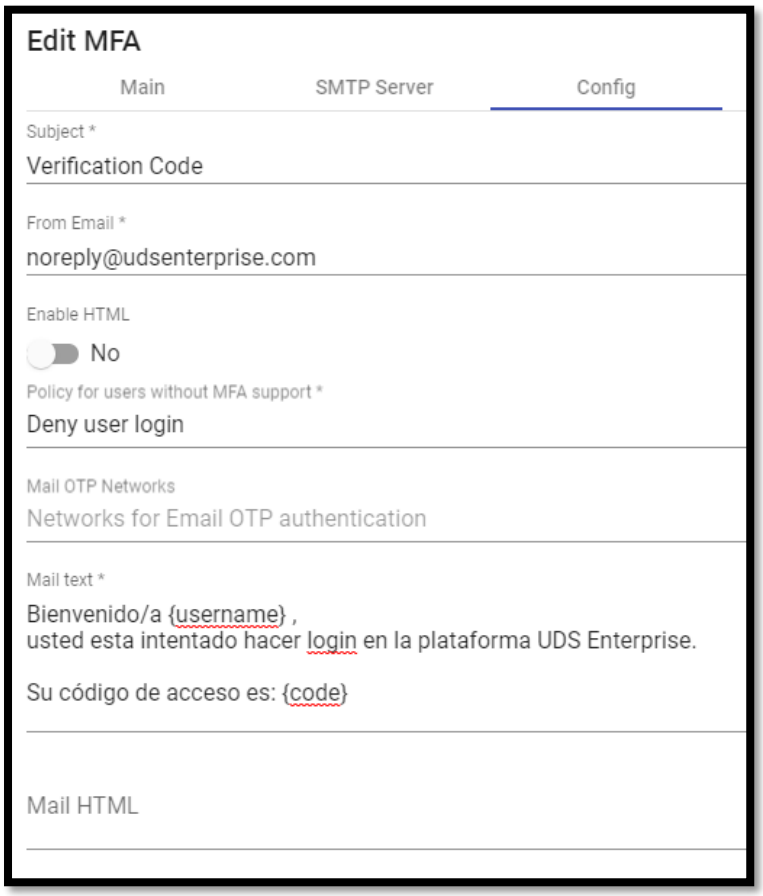
- Name: Name of the Method
- Device caching: Time in hours to cache the device so that MFA is not needed again. User based.
- Validity of the MFA code: Time in minutes to allow the use of the MFA code.



"SMTP Server" Tab:

This tab will be where we will indicate the data related to our email server where it is capable of sending the corresponding emails and has it activated.

In this example Gmail is used.



- **Subject**: shown in the email.

- **Origin Email**: The sender of the email.

- **Enable HTML**: combined with: "**Mail HTML**" we can enter HTML code in the sent email.

- **Policy for users without MFA support**: Explained below.

-**Mail OTP Networks**: the networks to which the MFA will be applied, if left empty it applies to any network.

- **Mail Text** : plain text to be displayed in the email.

NOTE you can indicate {username} with the user name, {IP} the user's origin IP and the most important: the {code} where the code necessary for the MFA will be filled in.

1.1. Policy for users without MFA support

With the chosen policy we can:

- Allow user login (ALL NETWORKS): even if the user cannot authenticate via MFA, access will be **ACCEPTED**.

- Deny user login (ALL NETWORKS): If the user cannot authenticate via MFA, access will be **DENIED**. (This is the most recommended option).

- Allow user to login if it IP is in the networks list (NETWORKS, IPs, Ranges... included in the NETWORKS section): if the user cannot authenticate via MFA but their IP belongs to the NETWORK list, access will be **ACCEPTED**.

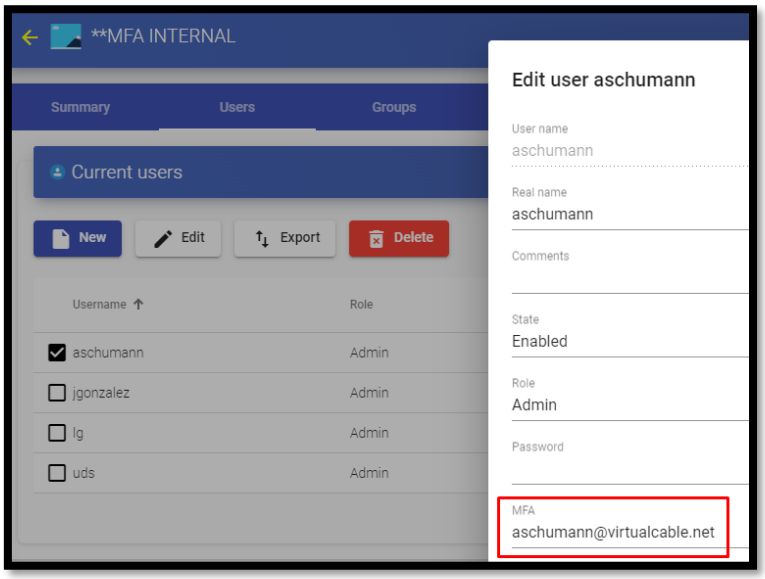
- Deny user to login if it IP is in the networks list: if the user cannot authenticate via MFA and their IP belongs to the NETWORK list, access will be **DENIED**.

1.2. Mail Atribute

For this type of method to work correctly, the recipient email is needed so that the end user can receive the emails.Existen dos métodos para conseguir esta información:

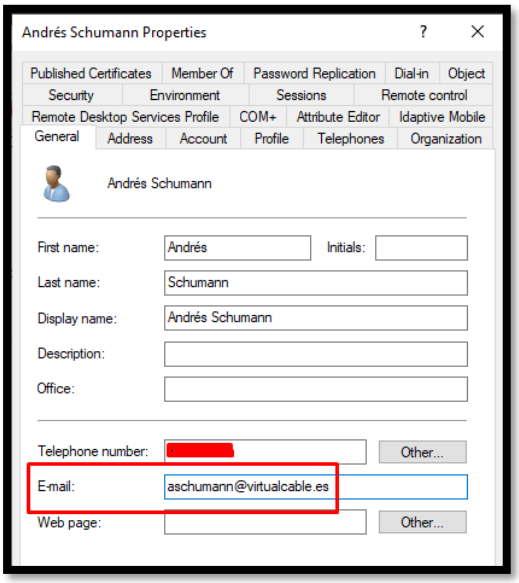
Internal Database

To obtain the user's email in authenticators such as "internal database", for example, we must indicate their email when editing or creating a user in the "**MFA**" section:



Active Directory

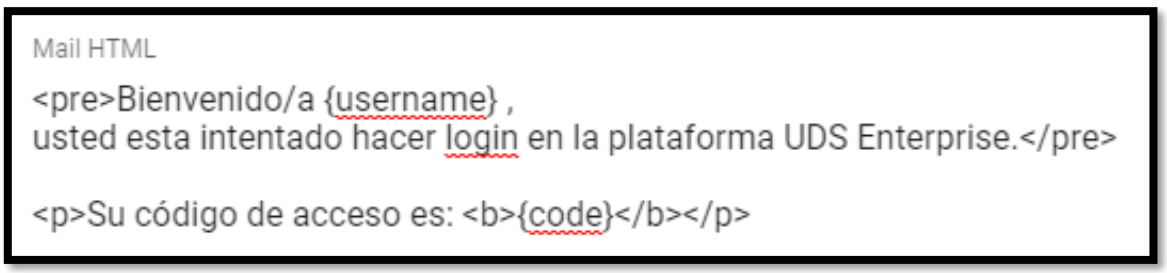
In the case that we are using a domain, the mail will be extracted directly from the user information/attributes in the domain:

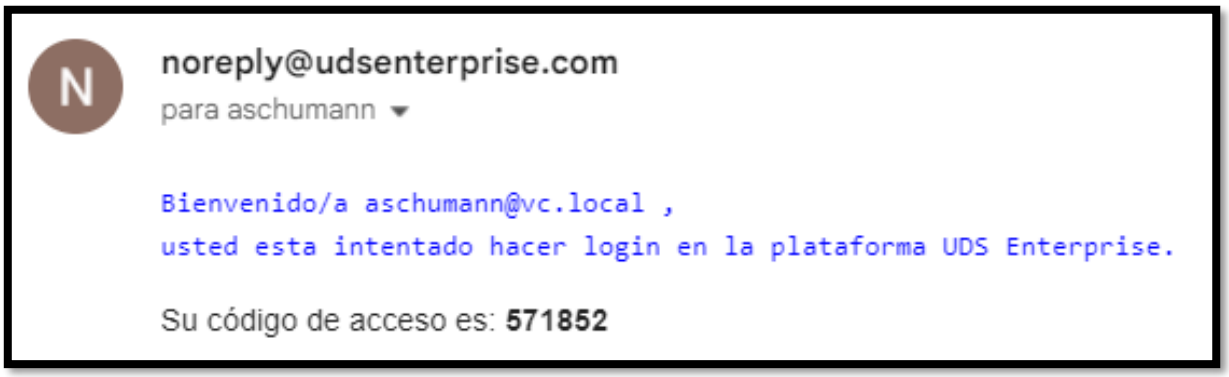


1.3. RESULTS

RESULTS WITH ONLY TEXT

RESULTS WITH HTML CODE

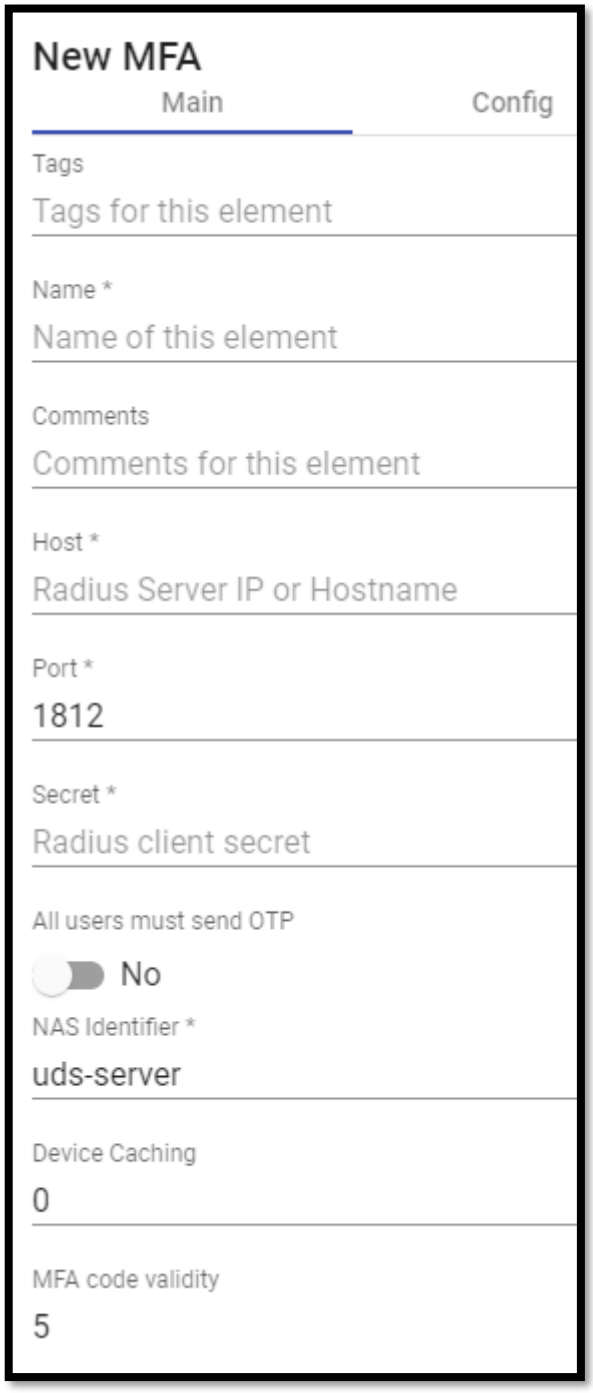




2. Radius OTP Challenge

Using this method, the user will first authenticate with their username and password and then be redirected to a second authentication process where they must enter the corresponding code provided by their radius server to finally be able to authenticate on their UDS Enterprise platform.

When creating and configuring this method, the following data must be indicated at least:



"Main" Tab

- **Name**: Name of the method.

- **Server**: IP o FQDN of the Radius Server.

- **Port**: Port used by the radius server

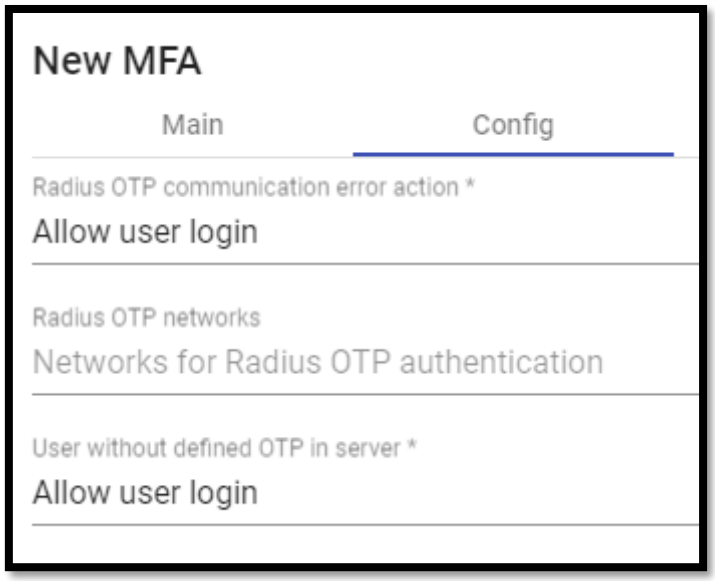
- **Secret**: generated when creating the radius client.

- **NAS Identifier**: identifying name.

- **Device caching**: Time in hours to cache the device so that MFA is not needed again. User based.

- **MFA code Validity**: Time in minutes to allow the use of the MFA code.

"Configuration" Tab:



For both the "Radius OTP communication error action" option and for "User without OTP defined on server" the action that will be carried out is defined when the user cannot perform the OTP due to some type of error or does not have it. defined on the server, among the 4 options to choose from are:

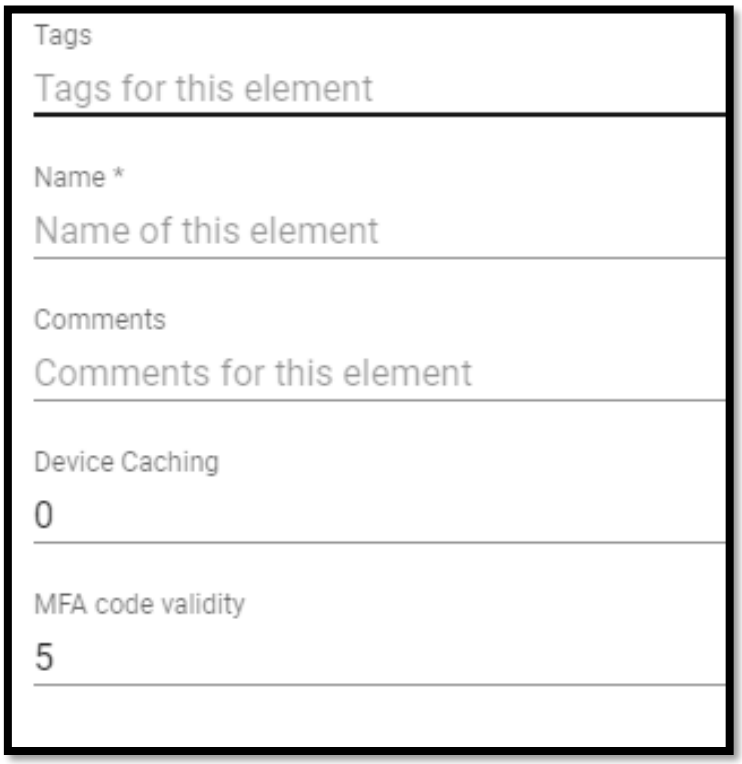
- Allow user login (ALL NETWORKS): even if the user cannot authenticate via MFA, access will be **ACCEPTED.**
- Deny user login (ALL NETWORKS): If the user cannot authenticate via MFA, access will BE **DENIED**. (This is the most recommended option).
- Allow user to login if it IP is in the networks list (NETWORKS, IPs, Ranges... included in the NETWORKS section): if the user cannot authenticate via MFA but their IP belongs to the NETWORK list, access will be **ACCEPTED**.
- Deny user to login if it IP is in the networks list: if the user cannot authenticate via MFA and their IP belongs to the NETWORK list, access will BE **DENIED**.

3. SMS over HTTP

Through this method, the user will first authenticate with their username and password and then be redirected to a second authentication process where they will receive an SMS with the necessary code to finally be able to authenticate on their UDS Enterprise platform.

In an "SMS Via HTTP" The minimum parameters to be configured are:

"Main" tab:



Name: The name that the item will be given to you.

Device caching: Time in hours to cache the device so that MFA is not needed again.

MFA Code Validity: Time in minutes to allow MFA code usage.

"HTTP Server" tab:

URL Pattern for SMS Sending: URL Pattern for SMS Sending.

In the API documentation of each company or application that provides this technology, there should be a base URL to be able to act and perform actions with the API.

SMS Forwarding Method: Method that will be used to send SMS.

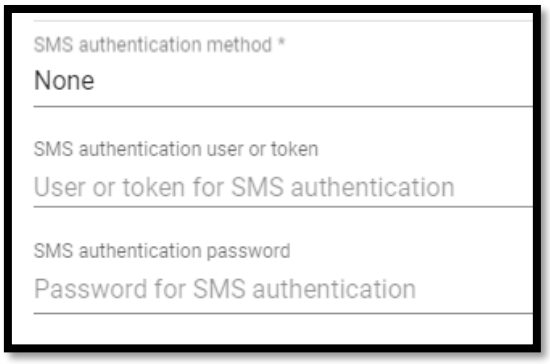
Parameters for sending POST/PUT SMS: the data necessary to send the code to the user must contain at least the {code} for the user to receive the security code. For a custom message, it can contain the following variables:

* {code} - The code to be sent
* {phone/+phone} - Phone number
* {username} - Username
* {justUsername} - the username without @....

Headers for SMS requests: the API of the different technologies may need specific headers for its proper functioning, so you should read the documentation if it exists for that specific technology.

SMS Encoding: Encoding that will be used to send SMS.

"HTTP Authentication" tab:



SMS Authentication Method: SMS API Authentication Method

SMS Authentication User or Token: User or token for SMS authentication

SMS Authentication Password: Password for SMS Authentication

"Configuration" tab:

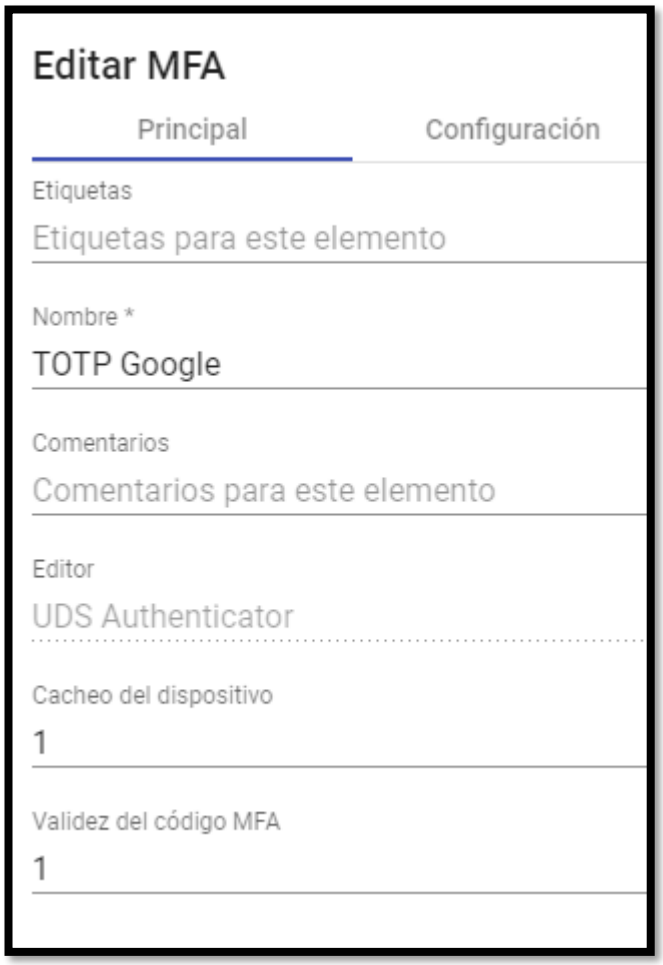
SMS Response Error Action: Action to be taken by the server in the event of an error

Non-MFA User Policy: An action to be performed with users without an MFA policy configured.

4. TOTP-based MFA

By means of this method, the user will first authenticate with their username and password and then be redirected to a second authentication process where they must enter the TOTP code generated from time to time in our application such as Google Authenticator, Microsoft, etc. to finally be able to authenticate in their UDS Enterprise platform.

When creating and configuring this method, at least the following information must be provided:



-**Name**: Name of the method

- **Device Cache**: Time in hours to cache the device so MFA isn't needed again. User-based.

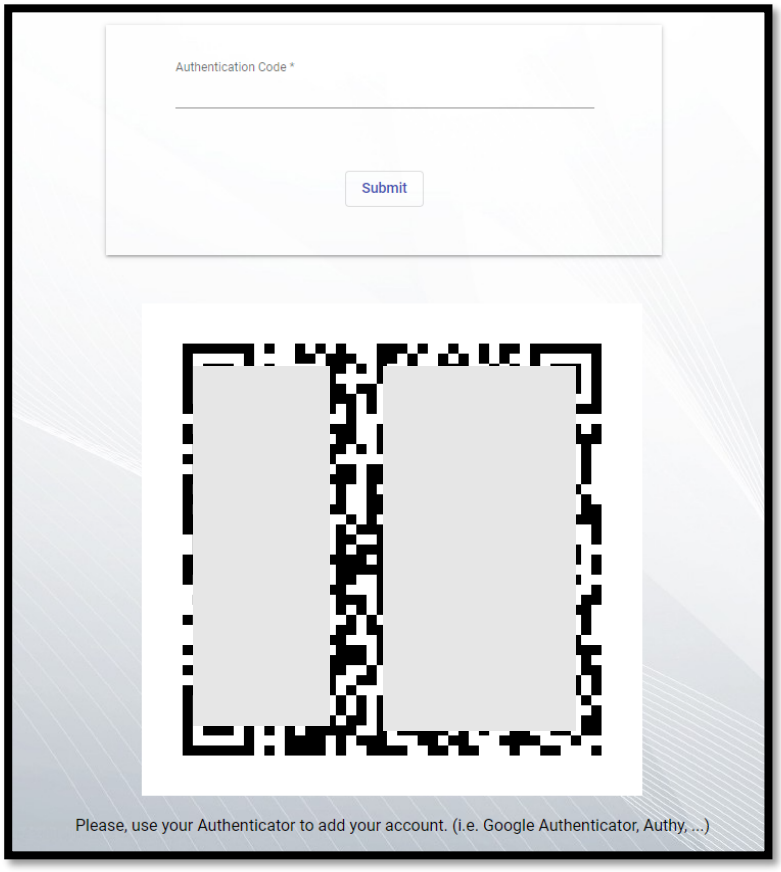
- **MFA Code Validity**: Time in minutes to allow MFA code usage.

"Configuration" tab:

Valid window: Number of valid codes before and after the current one.

4.1 Results

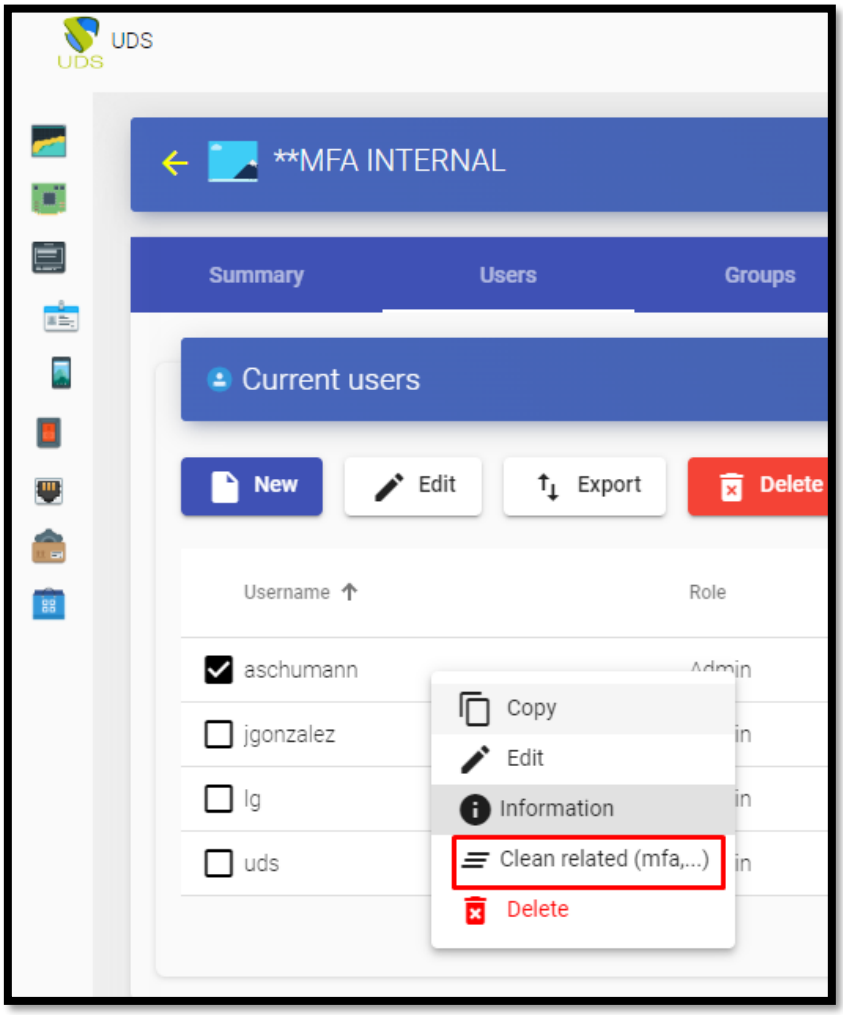
When the configuration is completely completed, a user who has indicated the chosen method in their authenticator will be logged in.



Apps such as Google Authenticator, Authy,.... can be used.

4.2 Reset TOTP MFA to a user.

If for some reason the user needs to reset their user so that they can show the QR again, they must access that user's authenticator and right-click on that user and click on "**Clean related (mfa,...)**"



UDS ENTERPRISE, THE VDI SOFTWARE OF VIRTUAL CABLE

About UDS Enterprise

UDS Enterprise is a new software concept to create a **fully** customized **desktop virtualization** platform. It provides **24x7, secure access** from anywhere **and** on any device **to all applications and software in an organization or school.**

It allows you to combine **virtualization** of Windows and **Linux** desktops and applications**, as well as** remote access **to Windows, Linux, and** macOS **computers**, in a single console . Its Open-Source base guarantees **compatibility with any** third-party technology. It can be deployed **on-premises**, in public, private, hybrid or **multicloud** cloud. Even **combine** multiple environments at the same time and perform **automatic and intelligent overflows** to optimize performance and efficiency. All with a **single subscription**.

About VirtualCable

Virtual Cable is a company specialized in the **digital transformation of the workplace**. The company develops, supports and markets UDS Enterprise. Its team of experts has designed **VDI** solutions tailored to **each sector** to provide a unique user experience fully adapted to the needs of each user profile. Virtual Cable professionals have **more than 30 years of experience in IT** and software development and more than 15 in virtualization technologies. **Millions of Windows and Linux virtual desktops with UDS Enterprise are deployed all over the world every day**.