Telefónica
Global Solutions

SUGUS

Users Manual for MFA Configuration

Internal use only

10 de marzo de 2023

Index

1. Introduction

The purpose of this user manual is to describe the steps to configure the Multifactor Authenticator (MFA) in the SUGUS portal.

2. Prerequisites

Before starting with the configuration, it is necessary to achive some prerequisites depending on the MFA method that is going to be used.

Below you will find the prerequisites for each method.

2.1. E-mail

This method is only available for users registered in SUGUS with an e-mail not belonging to the telefonica.com domain.

2.2. smartphone

To use your smartphone as a second authentication factor, it is necessary to have installed one of the two MFA applications supported by SUGUS: Microsoft Authenticator or Latch. Both applications can be downloaded from the smartphone's marketplace: Play Store in case of Android or App Store in case of IOS.

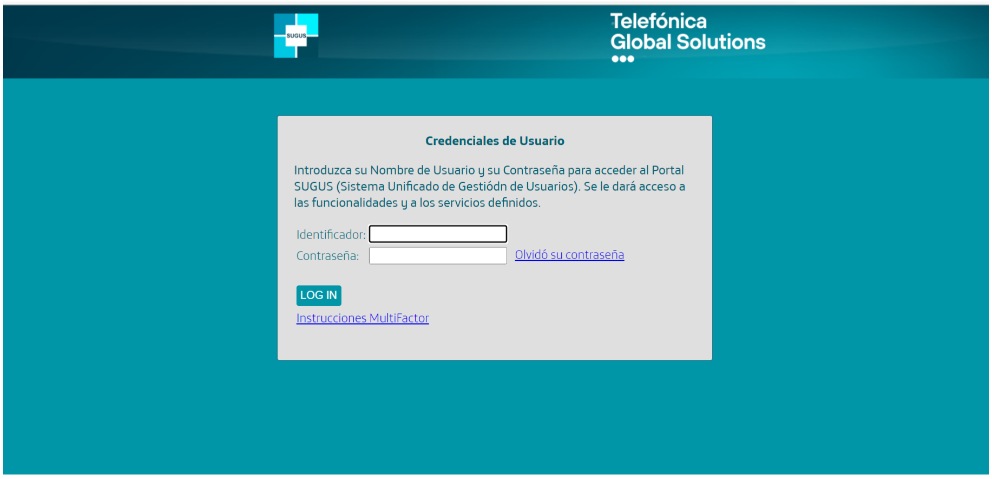
Once the application has been downloaded, follow the steps below depending on the application.

3. Instructions for configuring MFA

Bellow you can find instrucctions for each of the MFA methods:

3.1. APP Latch

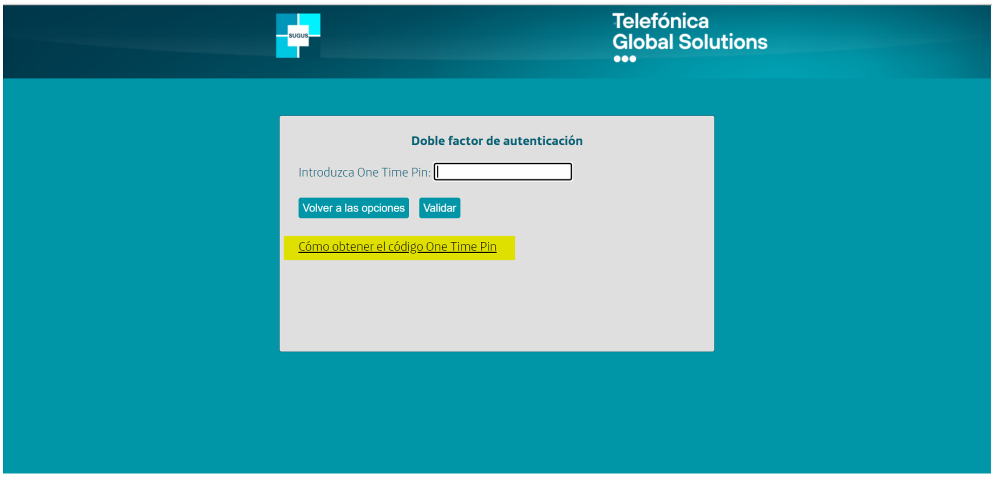
1- Access the SUGUS portal (https://sugus.telefonica.com/) and enter your username and password:



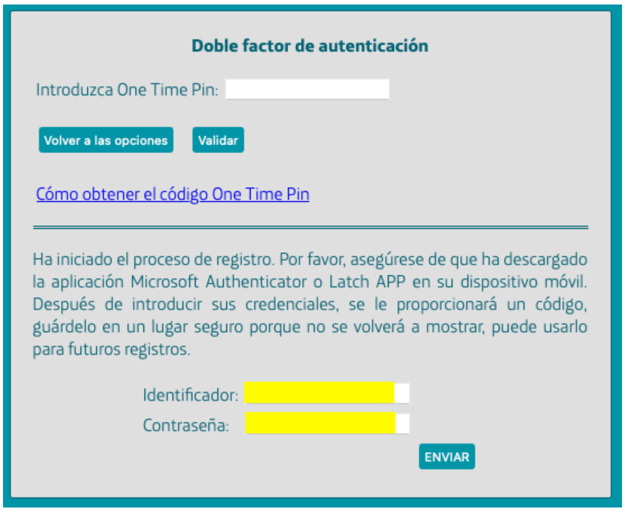
Credenciales de Usuario

Introduzca su Nombre de Usuario y su Contraseña para acceder al Portal SUGUS (Sistema Unificado de Gestiódn de Usuarios). Se le dará acceso a las funcionalidades y a los servicios definidos.

2- On the next screen, click on the option “how to obtain the one time pin code”.



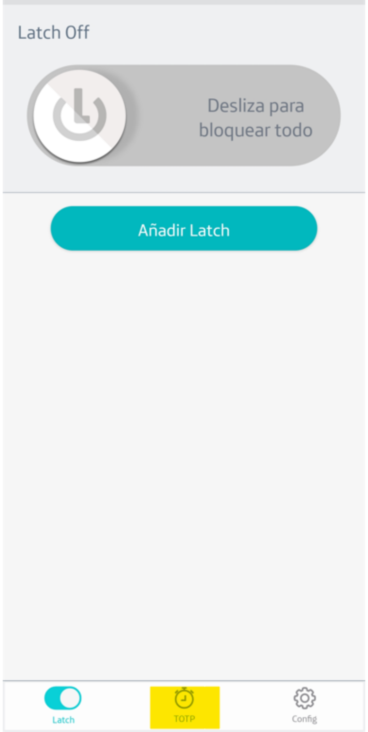
3- A screen will be shown asking for the SUGUS credentials in order to show the QR code that to be scaned from the mobile APP.

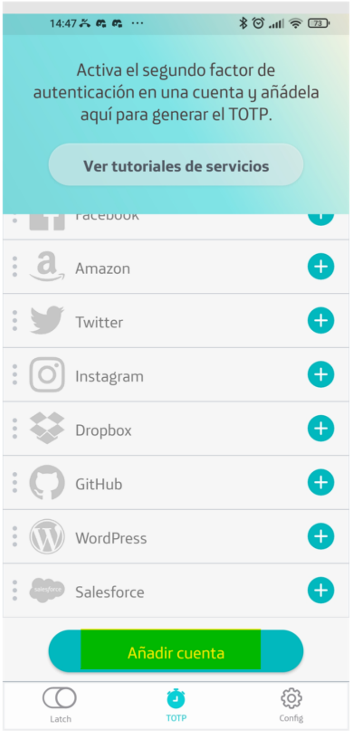

Doble factor de autenticación
Introduzca One Time Pin:
Volver a las opciones
Validar
Cómo obtener el código One Time Pin

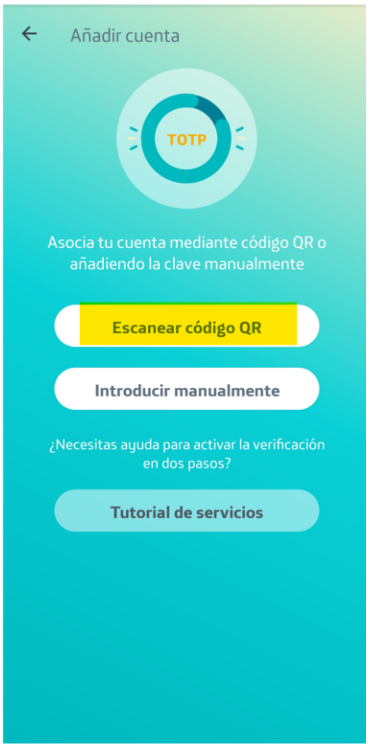
Ha iniciado el proceso de registro. Por favor, asegúrese de que ha descargado la aplicación Microsoft Authenticator o Latch APP en su dispositivo móvil. Después de introducir sus credenciales, se le proporcionará un código, guárdelo en un lugar seguro porque no se volverá a mostrar, puede usarlo para futuros registros.

4- On the smartphone, register in the Latch APP if you do not have a user yet.

5- On the main screen of the APP Latch after logged in, click on the TOP option, in the next screen go down until the “add account” option is visible and click on it. On the next screen, select the option to scan the QR code and give permission for the APP to use the smartphone's camera.

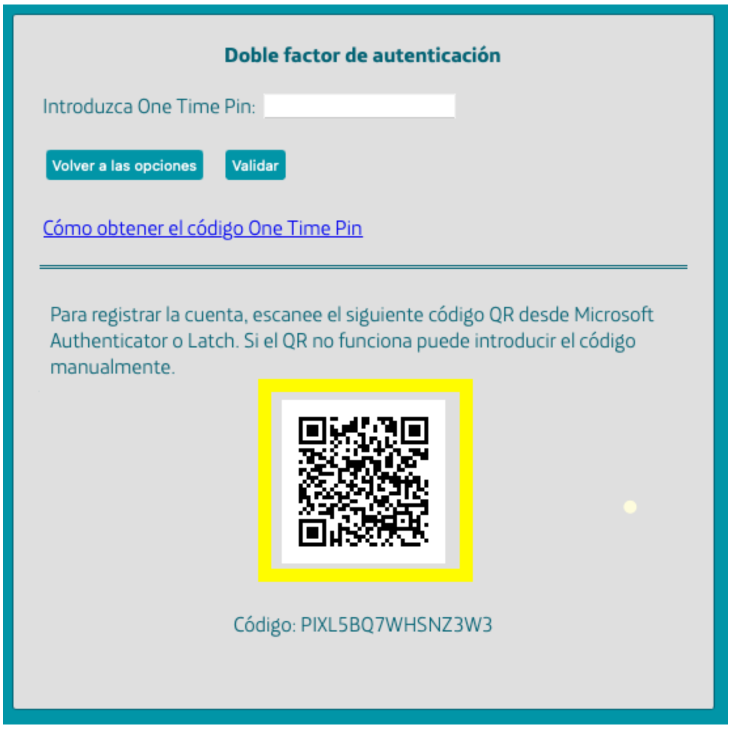



Activa el segundo factor de autenticación en una cuenta y añádela aquí para generar el TOTP.


Asocia tu cuenta mediante código QR o añadiendo la clave manualmente

¿Necesitas ayuda para activar la verificación en dos pasos?

6- Next, scan the QR code showed in SUGUS portal using the Latch APP. **This QR code will only be shown only once, in case you need to link more devices you must store this code in a safe place**.



Doble factor de autenticación

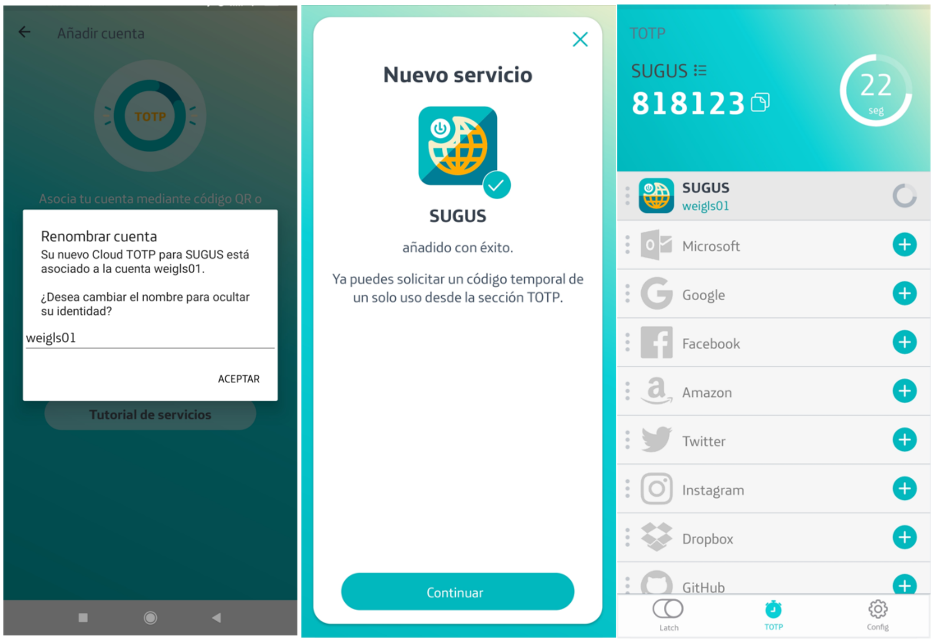
Introduzca One Time Pin:

Cómo obtener el código One Time Pin

Para registrar la cuenta, escanee el siguiente código QR desde Microsoft Authenticator o Latch. Si el QR no funciona puede introducir el código manualmente.

Código: PIXL5BQ7WHSNZ3W3

7- Latch APP you will show a screen to rename the SUGUS service, press continue. Next screen will show that the SUGUS service has been successfully added, press continue. On the next screen you will see all the services that you have already linked in Latch. Each time you access the SUGUS portal, after entering the username and password in the portal, you will be asked to enter the MFA code shown in the Latch APP for the SUGUS service. Remember that the displayed code has an expiration period indicated in seconds.



Renombrar cuenta

Su nuevo Cloud TOTP para SUGUS está asociado a la cuenta weigls01.

¿Desea cambiar el nombre para ocultar su identidad?

weigls01

Nuevo servicio

SUGUS

añadido con éxito.

Ya puedes solicitar un código temporal de un solo uso desde la sección TOTP.

TOTP

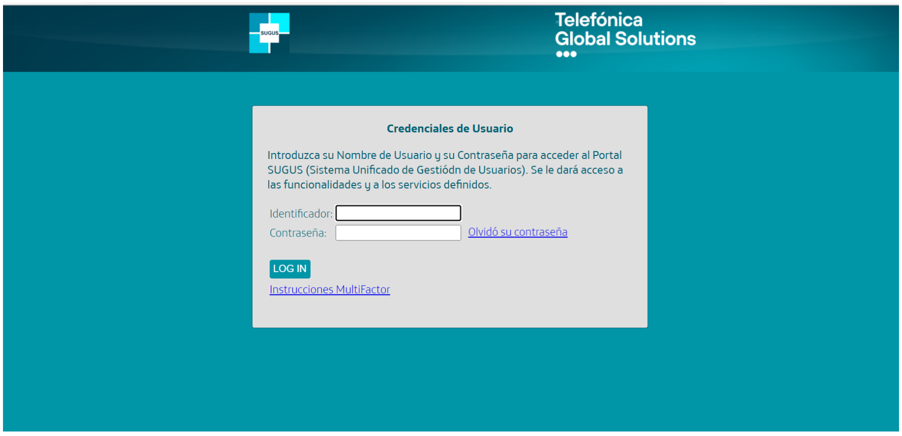
SUGUS

818123

22 seg

3.2. APP Microsoft Authenticator

1- Access the SUGUS portal (https://sugus.telefonica.com/) and enter your username and password:



Credenciales de Usuario

Introduzca su Nombre de Usuario y su Contraseña para acceder al Portal SUGUS (Sistema Unificado de Gestiódn de Usuarios). Se le dará acceso a las funcionalidades y a los servicios definidos.

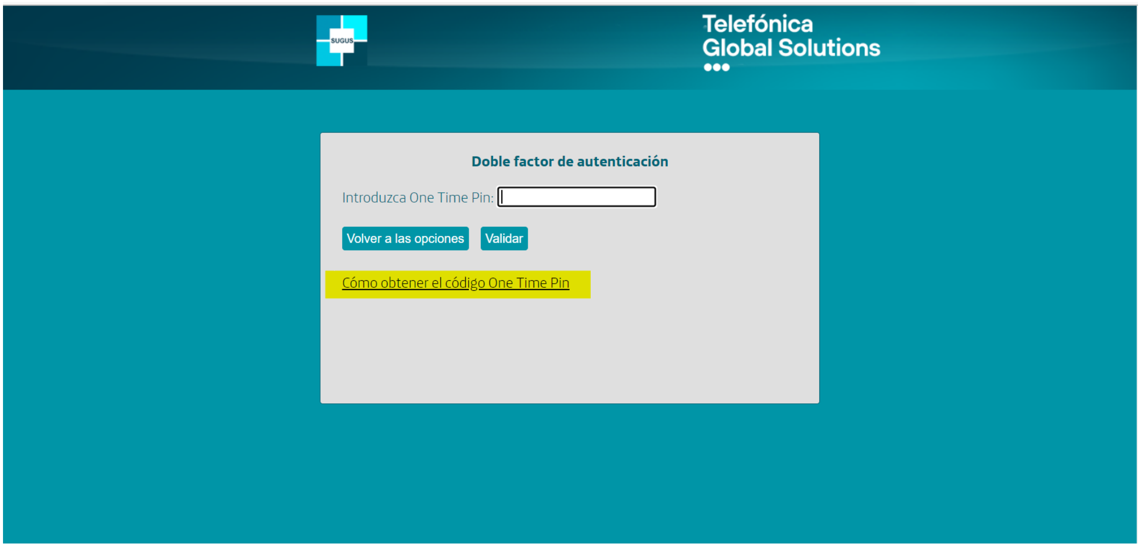
Identificador:

Contraseña: Olvidó su contraseña

LOG IN

Instrucciones MultiFactor

2- On the next screen, click on the option "how to obtain the one time pin code".



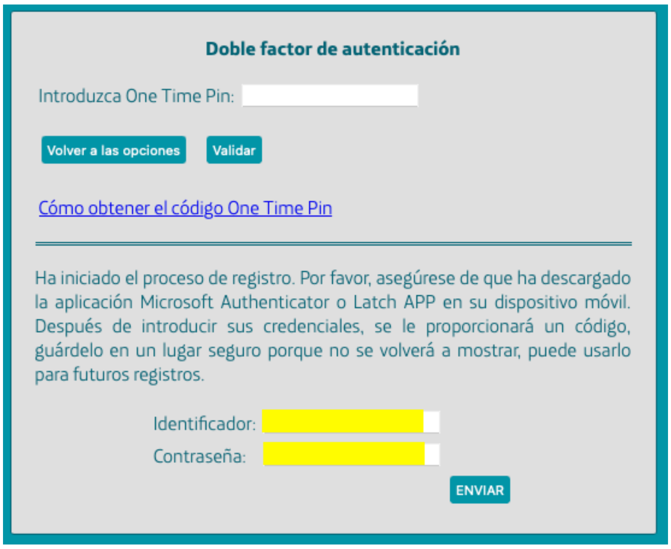
Doble factor de autenticación

Introduzca One Time Pin:

Volver a las opciones Validar

Cómo obtener el código One Time Pin

3- A screen will be shown asking for the SUGUS credentials in order to show the QR code that you will have to scan from the mobile APP.



Doble factor de autenticación

Introduzca One Time Pin:

Volver a las opciones | Validar

Cómo obtener el código One Time Pin

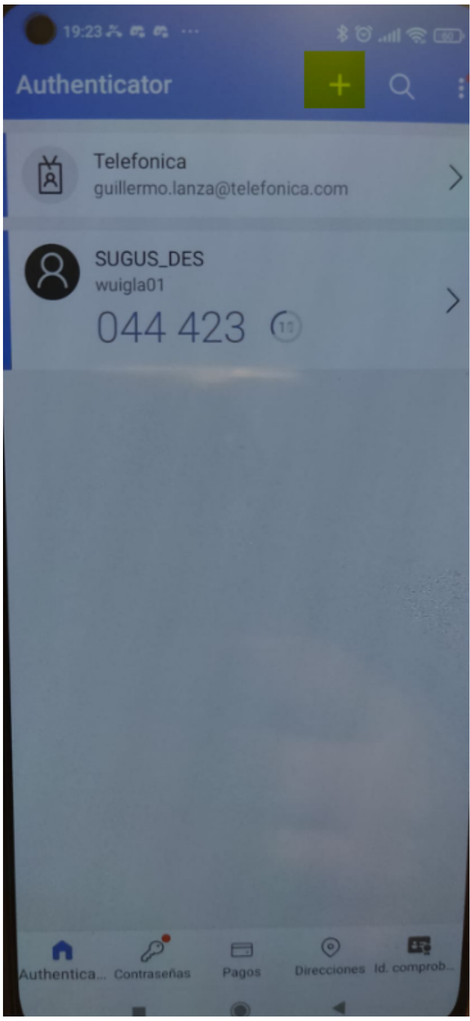
Ha iniciado el proceso de registro. Por favor, asegúrese de que ha descargado la aplicación Microsoft Authenticator o Latch APP en su dispositivo móvil. Después de introducir sus credenciales, se le proporcionará un código, guárdelo en un lugar seguro porque no se volverá a mostrar, puede usarlo para futuros registros.

Identificador:

Contraseña:

ENVIAR

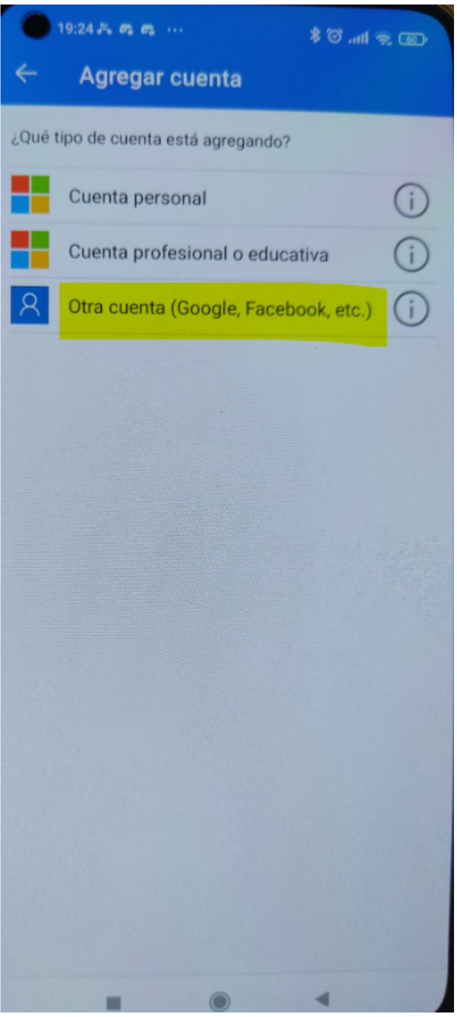
4- On the smartphone, register on the MS Authenticator APP if you do not have a user yet. On the main screen of the APP once you logged in, click on "+" to add a new service, then select the option "Other account (Google, Facebook, etc.)", this will activate the camera to scan the QR code shown in the SUGUS portal.



Authenticator +

Telefonica
guillermo.lanza@telefonica.com

SUGUS_DES
wuigla01
044 423



Agregar cuenta

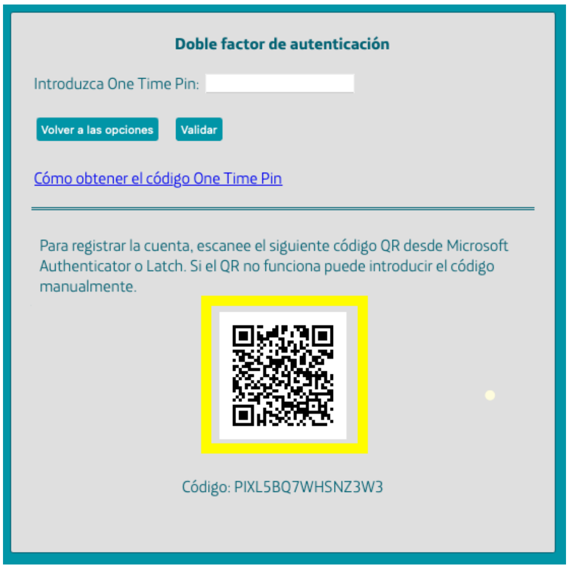
¿Qué tipo de cuenta está agregando?

Cuenta personal

Cuenta profesional o educativa

Otra cuenta (Google, Facebook, etc.)

5- Next, scan the QR code shown in the SUGUS portal through the Latch APP. **This QR code will only be shown once, in case you need to link more devices you must store this code in a safe place**.



Doble factor de autenticación

Introduzca One Time Pin:

Para registrar la cuenta, escanee el siguiente código QR desde Microsoft Authenticator o Latch. Si el QR no funciona puede introducir el código manualmente.

Código: PIXL5BQ7WHSNZ3W3

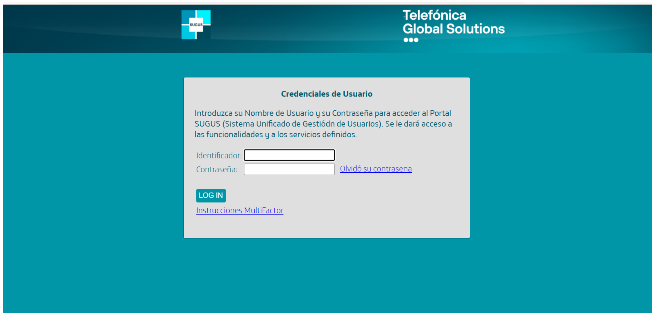
6- Next screen you will show all the services that you have already linked in MS Authenticator. Every time you access the SUGUS portal, after entering your username and password, you will be asked for the MFA code that you will find in the MS Authenticator APP for the SUGUS service. Remember that the displayed code has an expiration period indicated in seconds.

3.3. E-mail

If your user registered in SUGUS has an e-mail not belonging to Telefonica domain (@telefonica.com), you will have the option to get OTP code through your email address.

To complete e-mail as OTP channel, follow next steps:

1. Access the SUGUS portal (https://sugus.telefonica.com/) and enter your username and password:



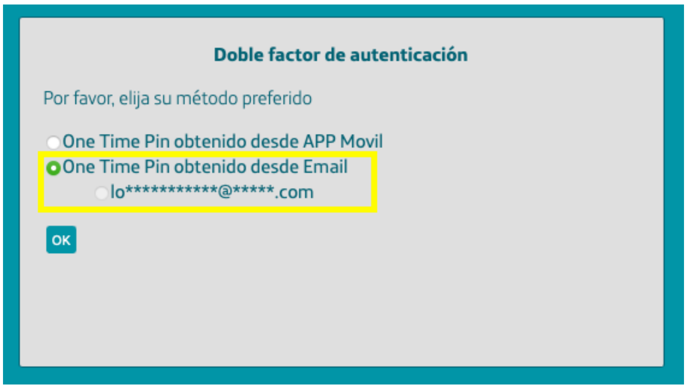
Credenciales de Usuario

Introduzca su Nombre de Usuario y su Contraseña para acceder al Portal SUGUS (Sistema Unificado de Gestiódn de Usuarios). Se le dará acceso a las funcionalidades y a los servicios definidos.

Identificador:

Contraseña:

2. Select the option “One Time Pin obtained from Email” and click OK



Doble factor de autenticación

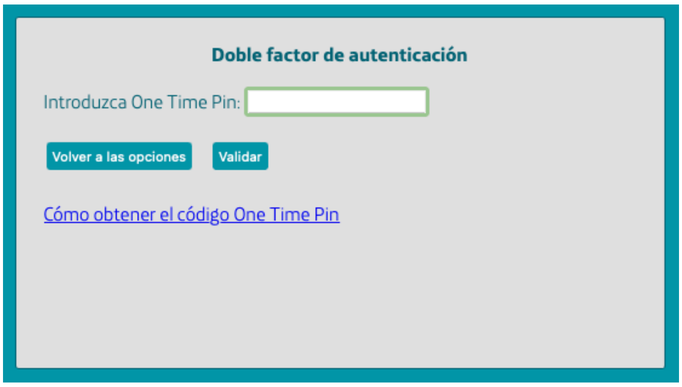
Por favor, elija su método preferido

○ One Time Pin obtenido desde APP Movil

● One Time Pin obtenido desde Email

○ lo***********@*****.com

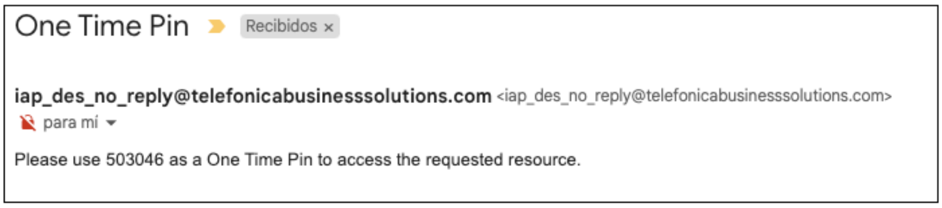
3. Next screen will ask you to enter the received PIN by e-mail:



Doble factor de autenticación

Introduzca One Time Pin:

The e-mail received in the e-mail address associated to the SUGUS user, will look like this:



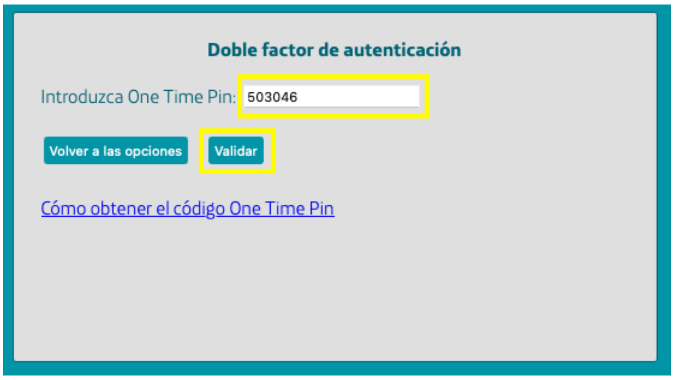
One Time Pin

iap_des_no_reply@telefonicabusinesssolutions.com <iap_des_no_reply@telefonicabusinesssolutions.com>

para mí

Please use 503046 as a One Time Pin to access the requested resource.

4. Enter the received pin and click on “Validate”



Doble factor de autenticación

Introduzca One Time Pin: 503046