How to use OTP in Soffid

Introduction

Soffid allows administrator users to config the access authentication with OTP as the second-factor authentication (2FA). This is the way to add a extra layer of protection used to ensure the security of online accounts beyond just a username and password.

The administrator user could config the proper OTP implementations that wants to use.

> To know how to config the diffent options you can visit the OTP settings page.

There are three points where OTP can be used in Soffid

1. Login Federation
2. Access to pages
3. XACML Rules
4. Password Recovery

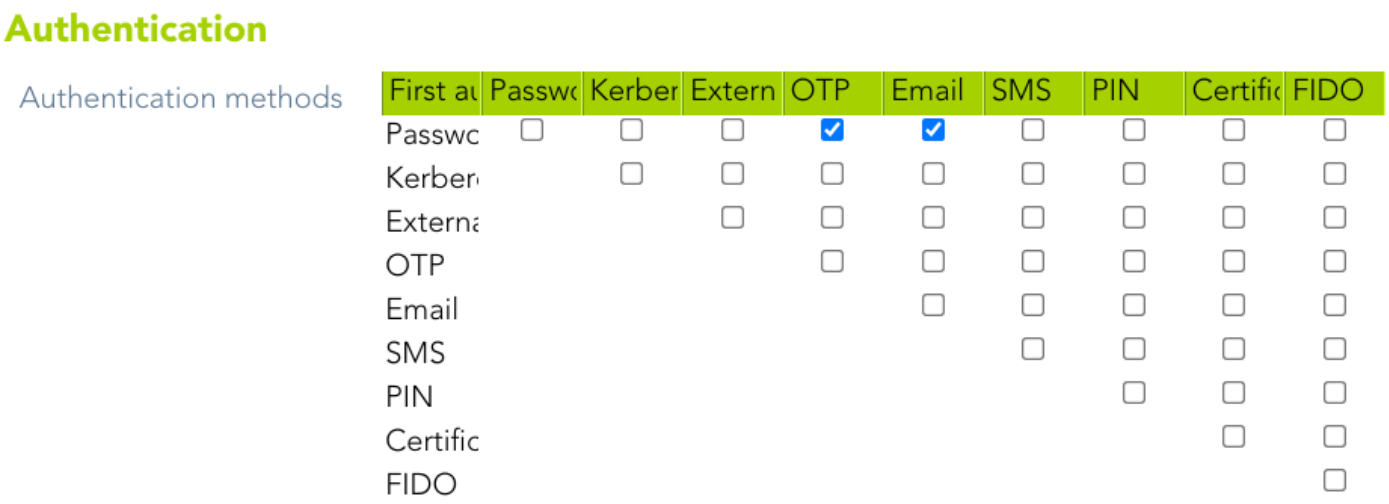
Federation

When you are configuring Soffid as Identity Provider, on the Authentication section you could config the OTP as a second authentication factor (2FA).

> You can visit the How to deploy the identity & service provider step by step page for more detailed information

Example

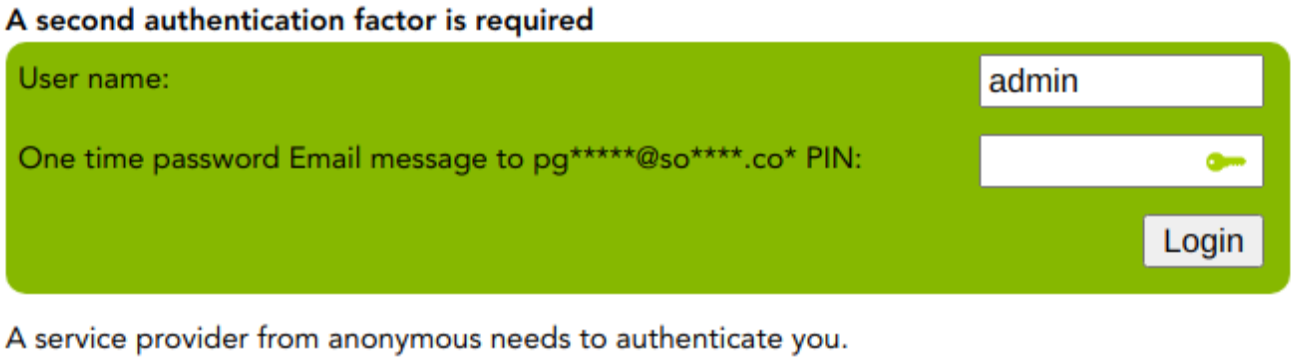
First of all, configure the OTP as a second factor authentication at the Identity & service providers page



Then, when users login, they must write their credentials



If the credentials written are ok, finally Soffid will ask for the 2FA



Authentication

Regarding to the access to pages, you will be able to config the specific Soffid console pages that will require OTP authentication. In addition, you will be able to config if the second-factor

authentication will be required to all the users or only to users with enabled token.

> You can visit the Authentication page for more information

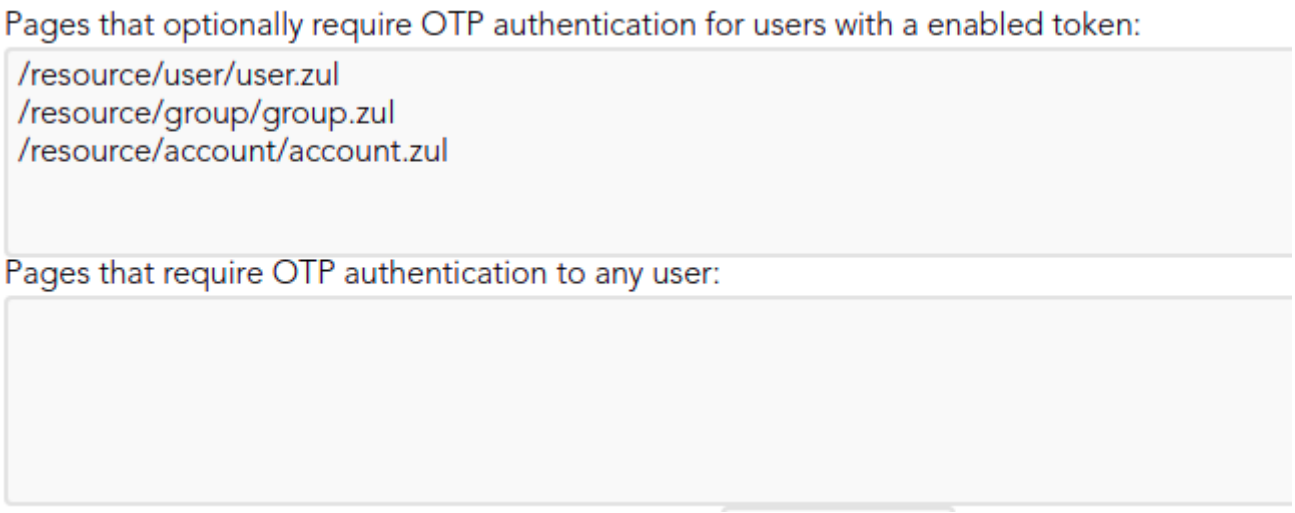
Example

The following is an example of how for a given configuration, a user can access certain pages, or how a second authentication factor is required for the user.

Second factor authentication configuration

Soffid will require the PIN to access to the specified pages to users with a enabled token

`Main Menu > Administration > Configuration > Security settings > Authentication`



User access

https://www.youtube.com/embed/D0m8kWgFLGg?rel=0

XACML

OTP can also be used at **XACML Policy Management**. This policies allow adding more complex and restricted rules to the authorizations.

> You can visit the XACML book for more information.

Example

A 2FA is required to launch the connection to some servers.

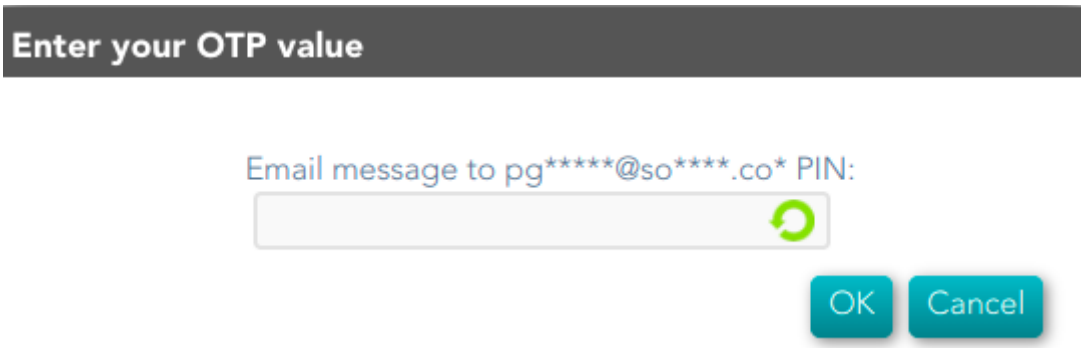
Administrator user can configure the XACML policies.

`Main Menu > Administration > Configuration > Security settings > XACML Policy Management`

Obligations

	Obligation	Full fill on	Attribute	Value
☐	urn:soffid:obligation:message	Permit	text	This is a protected system. Do not enter without authorization, please.
☐	urn:soffid:obligation:otp	Permit	timeout	30

When dilbert launch the connection, Soffid will ask for the 2FA



Password Recovery

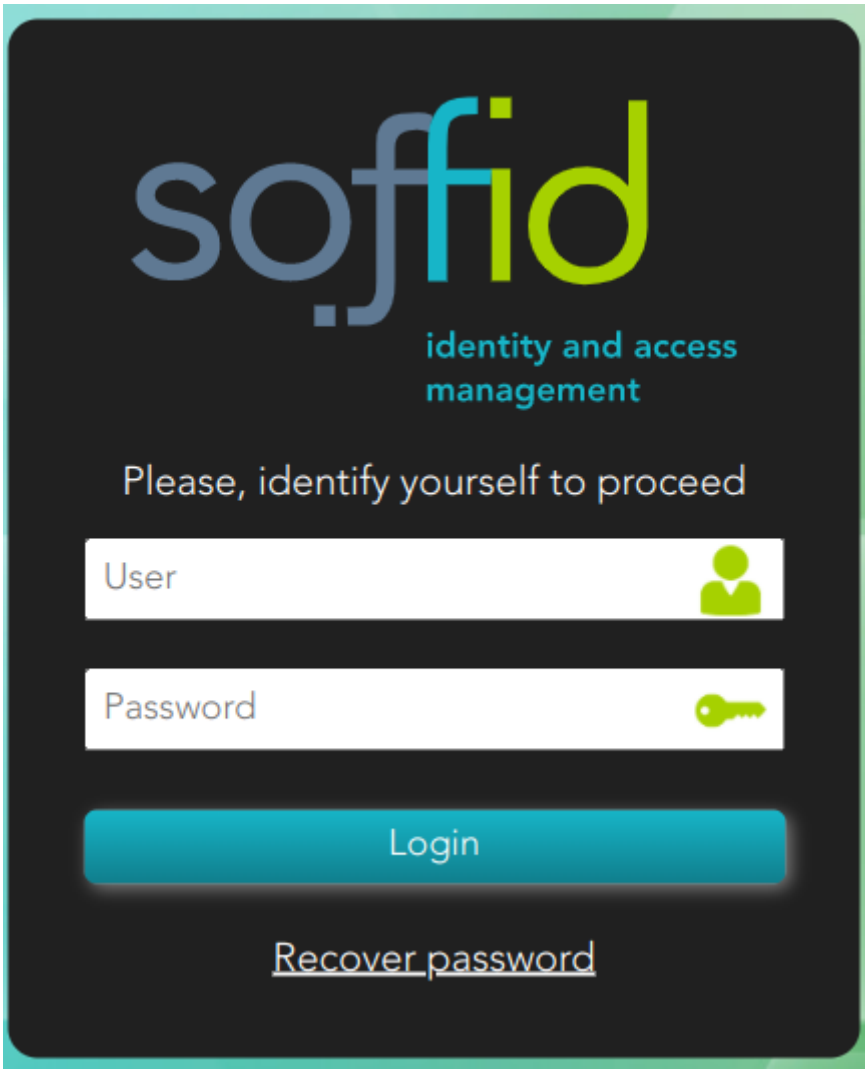
OTP can be use by end-user to recover the password.

> You can visit the Password Recovery book for more information.

Example

A end-user wants to recover his password.

Soffid allows to recover by clicking on the recover password option:



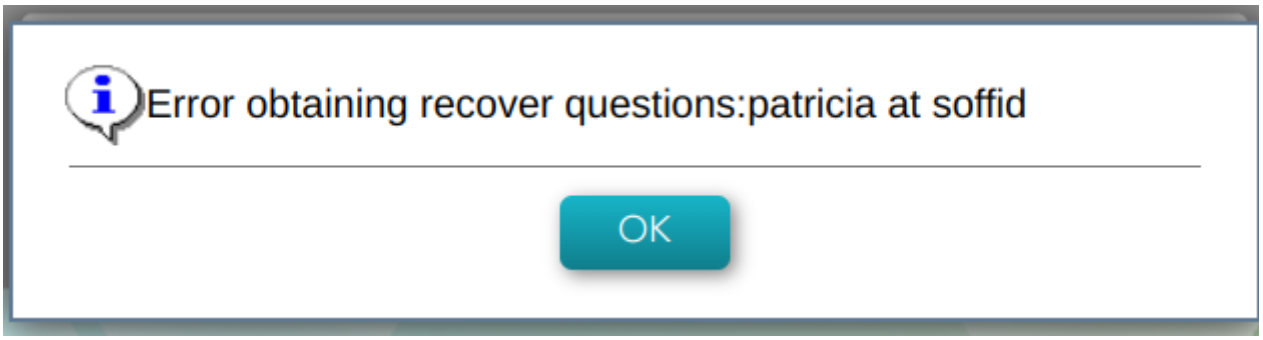
Then, the end-user must identify himself:



And Soffid requires to enter the PIN



If the end-user has not configured the OTP devices, a error message will be display.



Revision #15
Created 20 December 2021 09:58:11
Updated 24 February 2023 08:40:14