
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

Authentication

Authentication methods	First authentication	Password	Kerberos	External	OTP	Email	SMS	PIN	Certificate	FIDO
Password	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kerberos			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
External				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
OTP					<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Email						<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SMS							<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
PIN								<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Certificate									<input type="checkbox"/>	<input type="checkbox"/>
FIDO										<input type="checkbox"/>

Then, when users login, they must write their credentials

Please, identify yourself.

User name:

Password:

Login

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

A second authentication factor is required

User name:

One time password Email message to pg*****@so****.co* PIN:

Login

A service provider from anonymous needs to authenticate you.

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

Pages that optionally require OTP authentication for users with a enabled token:

```
/resource/user/user.zul  
/resource/group/group.zul  
/resource/account/account.zul
```

Pages that require OTP authentication to any user:

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

<input type="checkbox"/>	△ ▾ Obligation	△ ▾ Full fill on	△ ▾ Attribute	△ ▾ Value
<input type="checkbox"/>	urn:soffid:obligation:message	Permit	text	This is a protected system. Do not enter without authorization, please.
<input type="checkbox"/>	urn:soffid:obligation:otp	Permit	timeout	30



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

Enter your OTP value

Email message to pg*****@so****.co* PIN:



OK

Cancel

Password Recovery

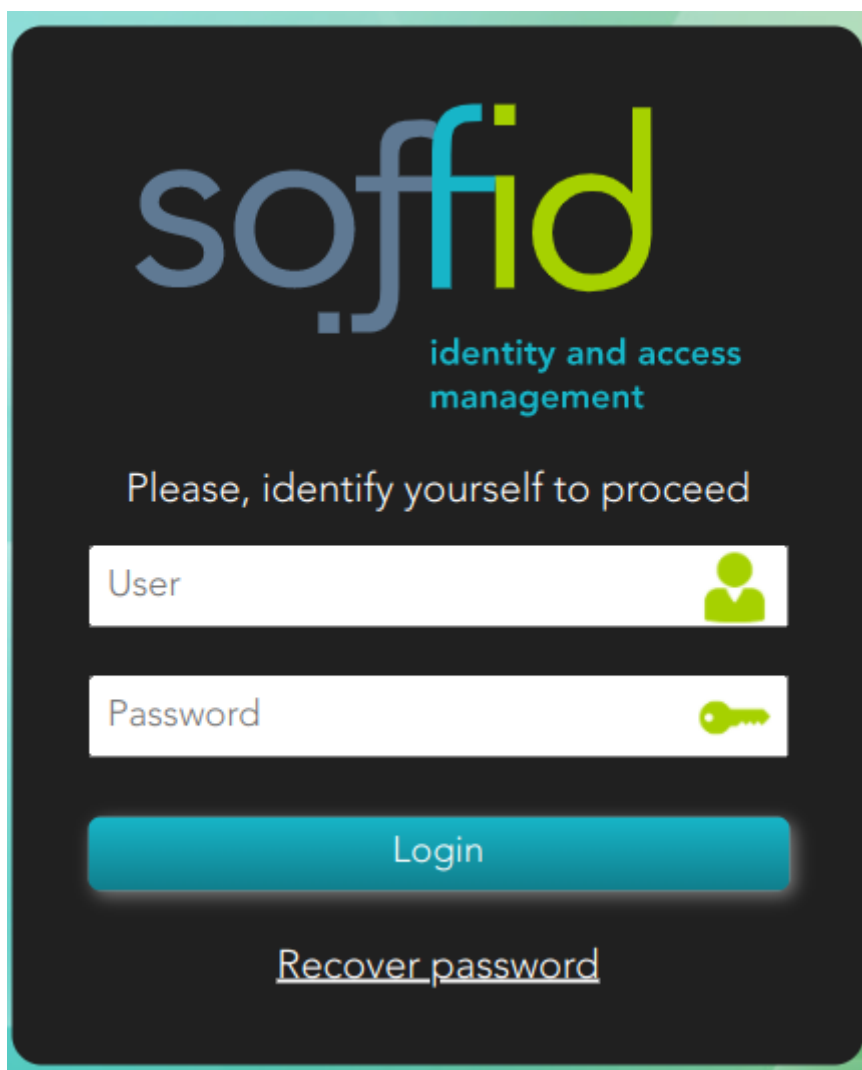
OTP can be use by end-user to recover the password.

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:

The image shows a login and password recovery interface for Soffid. At the top, the Soffid logo is displayed in a stylized font with 'soff' in grey and 'fid' in blue and green. Below the logo, the text 'identity and access management' is written in a smaller, teal font. The main instruction 'Please, identify yourself to proceed' is centered. Below this, there are two input fields: 'User' with a person icon and 'Password' with a key icon. A large teal 'Login' button is positioned below the password field. At the bottom, there is a link labeled 'Recover password'.

Then, the end-user must identify himself:

The image shows a login interface for Soffid. At the top, the Soffid logo is displayed in a stylized font with 'soff' in grey, 'fid' in blue, and 'id' in green. Below the logo, the text 'identity and access management' is written in a smaller, teal font. The main instruction 'Please, identify yourself to proceed' is centered in white. Below this, the label 'User:' is followed by a long, empty white text input field. At the bottom, there are two teal buttons: 'Password recovery questions' and 'Cancel'.

And Soffid requires to enter the PIN

The image shows a PIN entry screen for Soffid. The Soffid logo and 'identity and access management' text are at the top. The instruction 'Enter the answers to the following questions' is centered. Below this is a table with two columns: 'Question' and 'Answer'. The first row of the table has the question 'PIN for device: TOTP00000039' in the 'Question' column and an empty white input field in the 'Answer' column. At the bottom, there are two teal buttons: 'Recover' and 'Close'.

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



Error obtaining recover questions:patricia at soffid

OK

Revision #15

Created 20 December 2021 09:58:11 by pgarcia@soffid.com

Updated 24 February 2023 08:40:14 by pgarcia@soffid.com