Two factor authentication (2FA)

OTP - One Time Password

- Introduction to OTP
- How to install OTP addon in Soffid
- How to use OTP in Soffid
- OTP Management
  - OTP settings
  - Users OTP devices
- Self service portal
  - My OTP devices
- SCIM for OTP devices
- SCIM for OTP devices
  - Getting Started
  - SCIM OTP devices examples
  - SCIM OTP devices Workflows examples

Introduction to OTP

What is OTP?

> A **one time password (OTP)** is a password that is valid for only one login session or transaction, on a computer system or other digital device.

> The most important advantage addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks

OTP is use as **second-factor authentication (2FA)**. The 2FA is an extra layer of protection used to ensure the security of online accounts beyond just a username and password

Soffid Implementations

Soffid provides different OTP implementations. Users with the proper permissions could configure the OTP services on Soffid Console, they could configure one or more OTP implementations.

Once the OTP is configured, the end-users could config their owns OTP devices.

> You can visit My OTP devices page for more information.

Email

An email with the OTP will be send to the end-user. Then, the end-user will write the received code into Soffid to verify the token.

SMS

An SMS message will be send to the end-user to use it for authentication. Then, the end-user will write the received code into Soffid to verify the token.

Test messaging is a commns technology used for delivery OTPs. That is a secure authorisation method to send a numeric code to a mobile number.

Time based HMAC Token

The end-user must scan a QR code with an OTP application (Free Otp+, Google Authenticator and Microsoft Authenticator are the most used). Then, the end-user will write the received code into Soffid to verify the token.

Event based HMAC Token

The end-user must scan a QR code with an OTP application (Free Otp+, Google Authenticator and Microsoft Authenticator are the most used). Then, the end-user will write the received code into Soffid to verify the token.

Security PIN

The end-user can configure a security PIN into Soffid.

Soffid will ask for a specific number of digits from the PIN to verify the access. When Soffid ask for a number of digits, the user would write these numbers to confirm.

---

https://en.wikipedia.org/wiki/One-time_password

How to install OTP addon in Soffid

Installation

Download

Please download the Soffid OTP add-on.

You can download it at the following link http://www.soffid.com/download/enterprise/ if you have Soffid user with authorization, or in the following http://download.soffid.com/download/ by registering.

Upload

Once the OTP add-on is downloaded, please log in to IAM Console.

> You need to be an administrator user of the Soffid console or a user with permissions to upload addons.

> It is recommended to upload the addons to master, this is the way to maintain updated all, master and tenants if there are.

In the Soffid console, please go to: "Main Menu > Administration > Configure Soffid > Global Settings > Plugins" and upload the addon file, for more information visit the Addons Getting started page

Finally, when the addon is installed, it will be required to restart the Soffid Console.

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

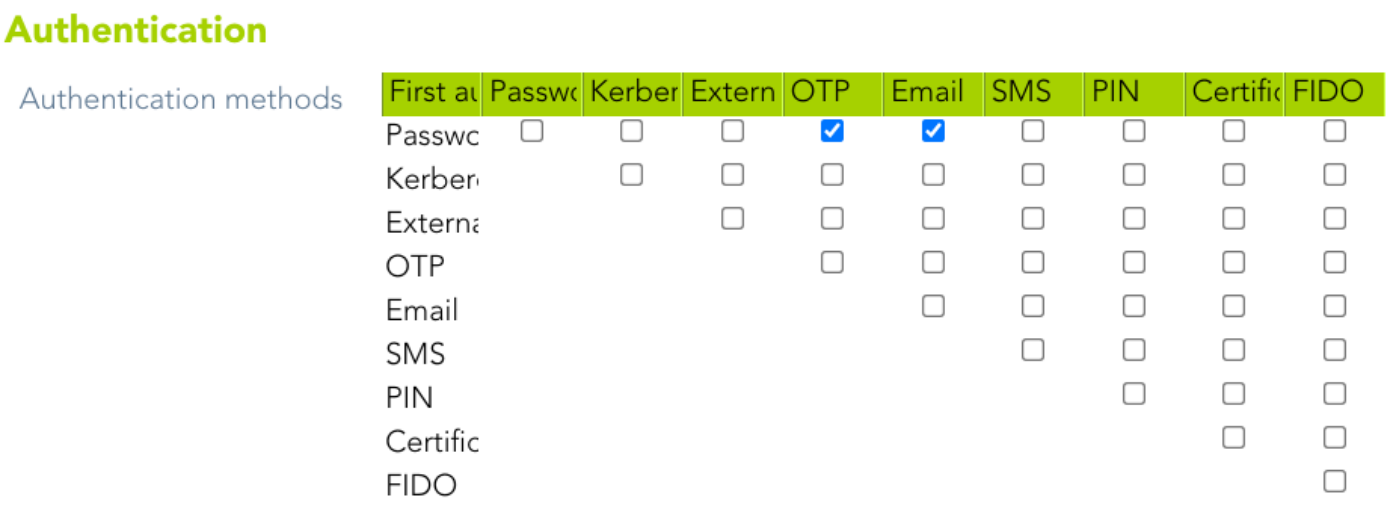
When you are configuring Soffid as Identity Provider, on the Authentication section you could config the OTP as a second authentication factor (2FA).

> 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

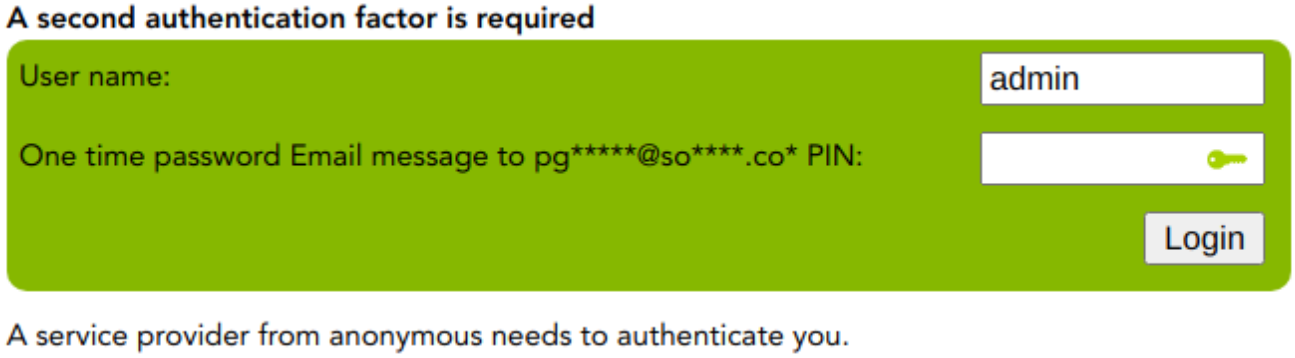
`Main Menu > Administration > Configuration > Web SSO > Identity & Service providers`



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 theAuthentication page for more information

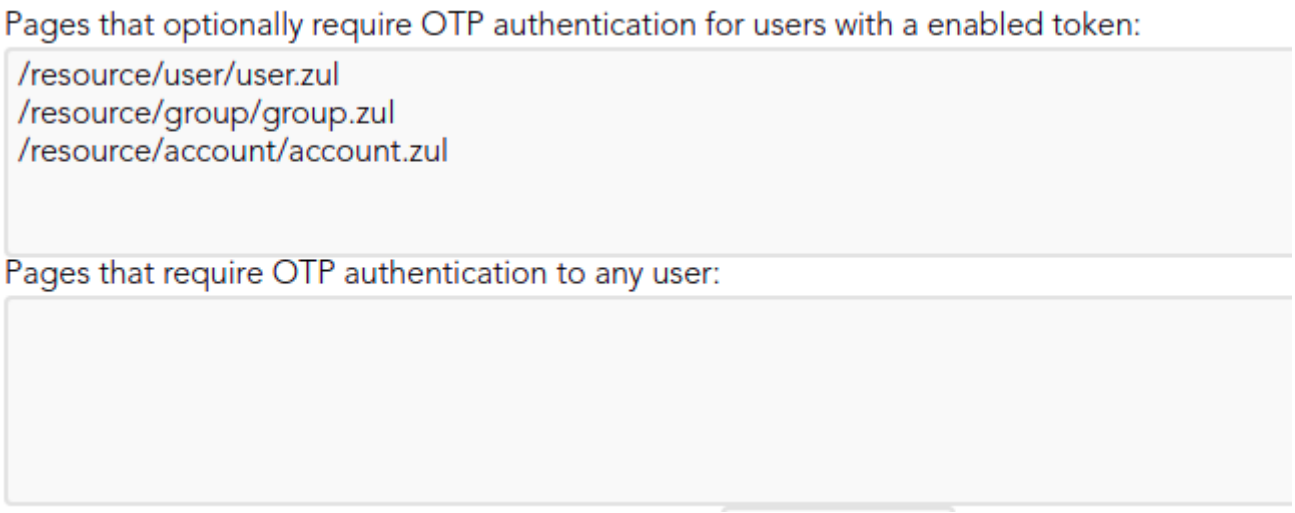
Example

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.

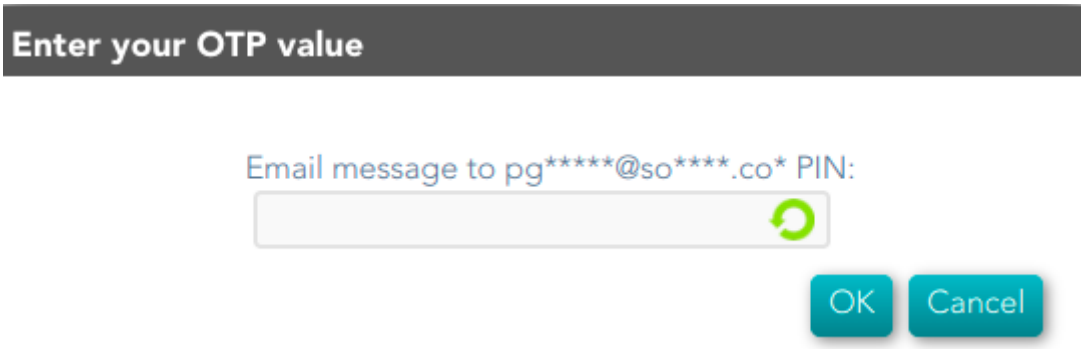
Administrator user can configure the XACML policies.

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

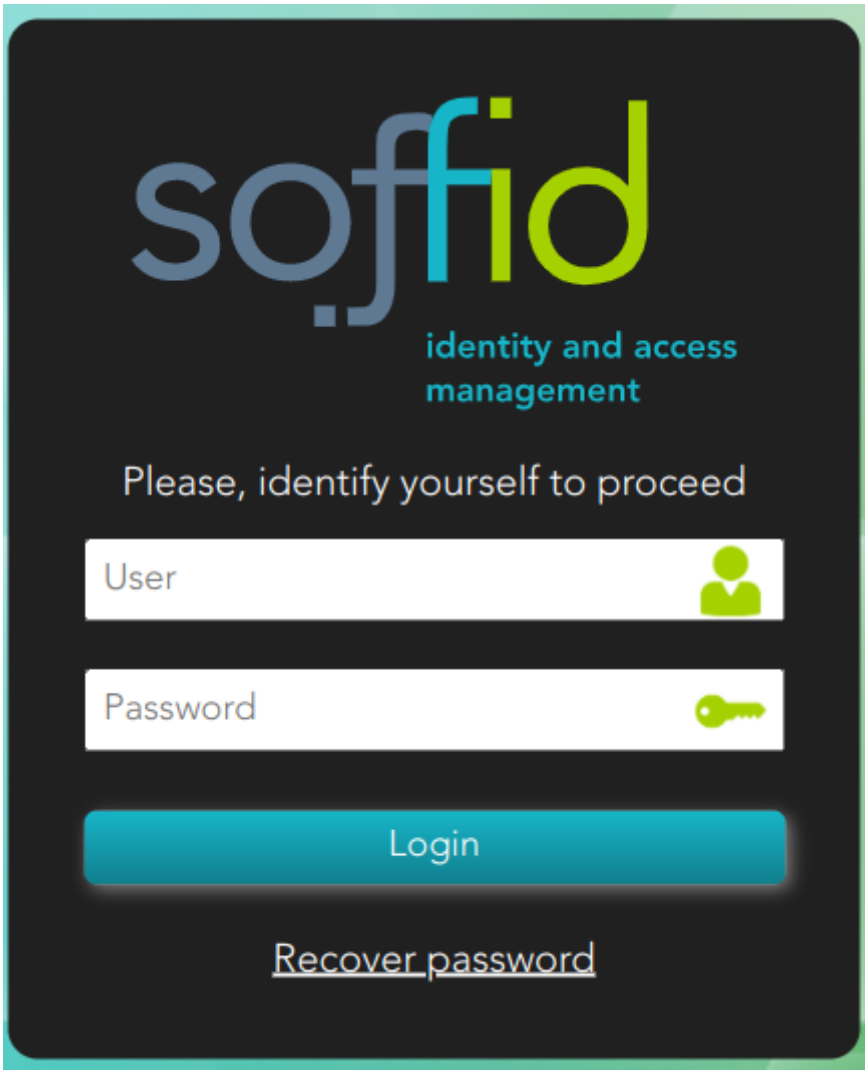
OTP can be use by end-user to recover the password.

> 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:



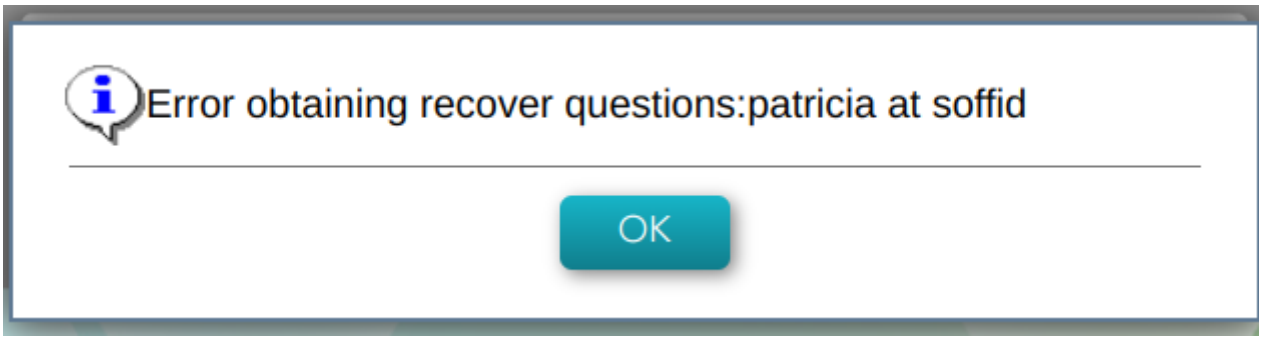
Then, the end-user must identify himself:



And Soffid requires to enter the PIN



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


Error obtaining recover questions:patricia at soffid
OK

OTP Management

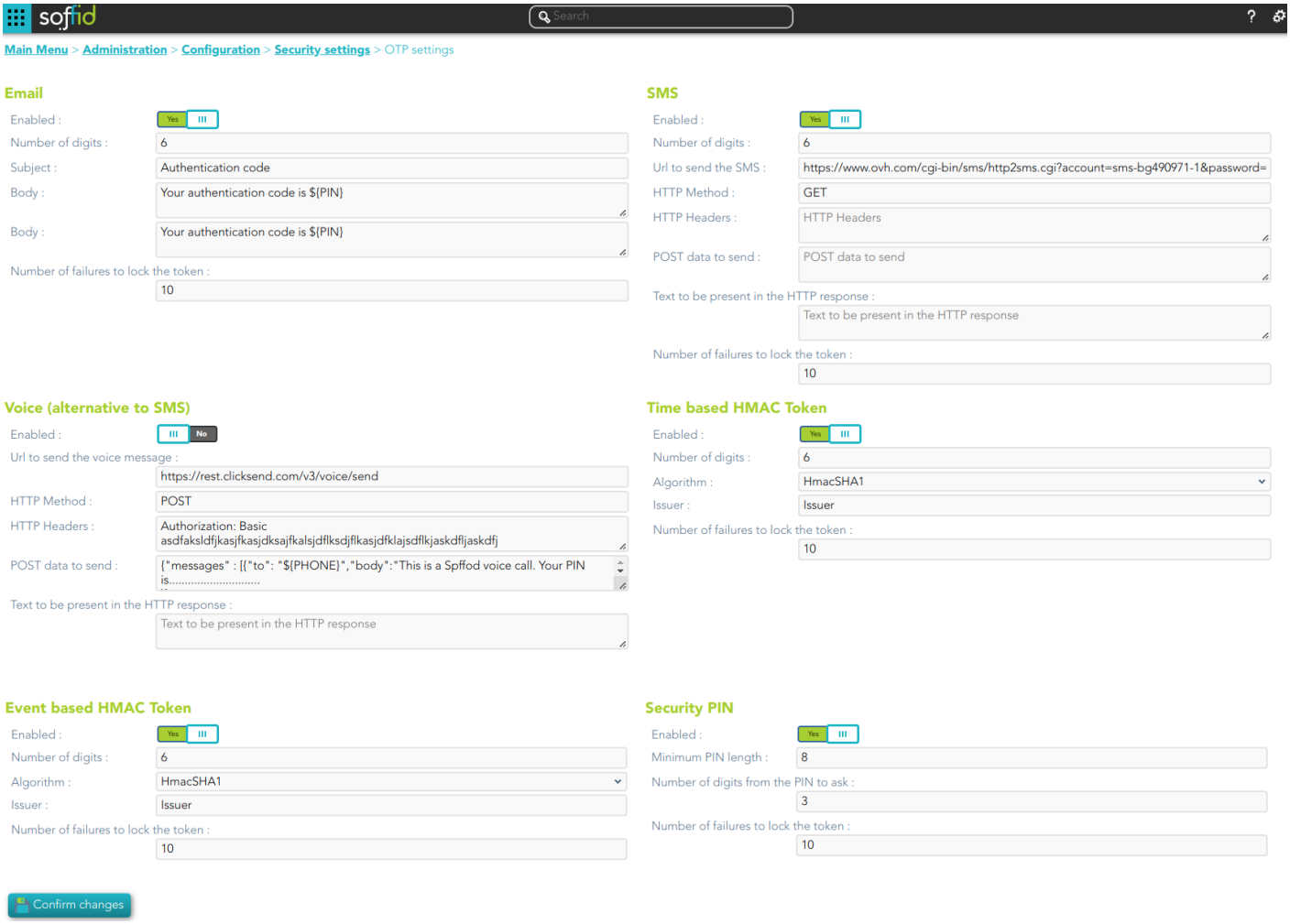
OTP settings

Definition

The OTP settings allow the administrator users to configure the available OPT options. Soffid provides four different OTP implementations.

Main Menu > Administration > Configuration > Security settings > OTP settings

Screen overview



Standard attributes

Email

- **Enabled**: allows you to enable or disable the OTP implementation.
- **Number of digits**: number of digits of the PIN code that will be generated.
- **Subject**
- **Body**
- **Number of failures to lock the token**

> To send an email, will be mandatory to fill in the value of the **mail.from** parameter. You can visit the mail server parameters.

SMS

- **Enabled**: allows you to enable or disable the OTP implementation.
- **Number of digits**: number of digits of the PIN code that will be generated.
- **URL to send the SMS**: enter the URL of your SMS provider rest service

```
https://www.xxxxxxx.com/cgi-bin/sms/http2sms.cgi?account=sms-bg490971-1&password=XXXXXXt&login=user&from=SOFFID&to=${PHONE}&message=This is your access PIN: ${PIN}&noStop&contentType=application/json&class=0
```

- **HTTP Method**: enter POST or GET depending on your provider documentation
- **HTTP Header**: optionally, you can add any HTTY header, including Basic or Bearer authentication tokens. The header must include the header name and header value. For instance:
  `Authorization: Basic dXNlcjpwYXNzd29yZA==`
- **POST data to send** Enter the body of the HTTP request
- **Text to be present in the HTTP response**: Soffid will check the response from your SMS Provider contains this text

```
"status":100
```

- **Number of failures to lock the token**

The URL and POST data to be sent, the administrator can use some tags that will be replaced by some target user attributes:

- ${PHONE}: The target phone number
- ${PIN}: The one-time password to be entered by the user
- ${userAttribute}: Any of the standard or custom user attributes, like ${fullName} or ${userName}

Voice (alternative to SMS)

- **Enabled**: allows you to enable or disable the OTP implementation.
- **URL to send the SMS**: enter the URL of your voice call provider rest service
- **HTTP Method**: enter POST or GET depending on your provider's documentation
- **HTTP Header**: optionally, you can add any HTTY header, including Basic or Bearer authentication tokens. The header must include the header name and header value. For instance:

  ```
  Authorization: Basic xxxxxxxxxxxxxxOUVCRS1DMzE0LTI3MzAtQkY0Qy05RDgwRTMyQUQ4OUY=
  Content-Type: application/json
  Accept: application/json
  ```

- **POST data to send** Enter the body of the HTTP request.

  ```
  Text to be present in the HTTP response: Soffid will check the response from your SMS Provider contains this text
  ```

  The POST data to be sent, the administrator can use some tags that will be replaced by some target user attributes:

- ○ ${PHONE}: The target phone number
  ○ ${PIN}: The one-time password to be entered by the user
- **Number of failures to lock the token**

Time based HMAC Token

- **Enabled**: allows you to enable or disable the OTP implementation.
- **Number of digits**: number of digits of the PIN code that will be generated.
- **Algorithm**: allows you to select an HMAC algorithm.
- **Issuer**
- **Number of failures to lock the token**

Event based HMAC Token

- **Enabled**: allows you to enable or disable the OTP implementation.

- **Number of digits**: number of digits of the PIN code that will be generated.
- **Algorithm**: allows you to select an HMAC algorithm.
- **Issuer**
- **Number of failures to lock the token**

Security PIN

- **Enabled**: allows you to enable or disable the Security PIN implementation.
- **Minimum PIN length**: minimum number of digits that the PIN has to have.
- **Number of digits from the PIN to ask**: number of digits that Soffil will ask to verify the identity.
- **Number of failures to lock the token**

Actions

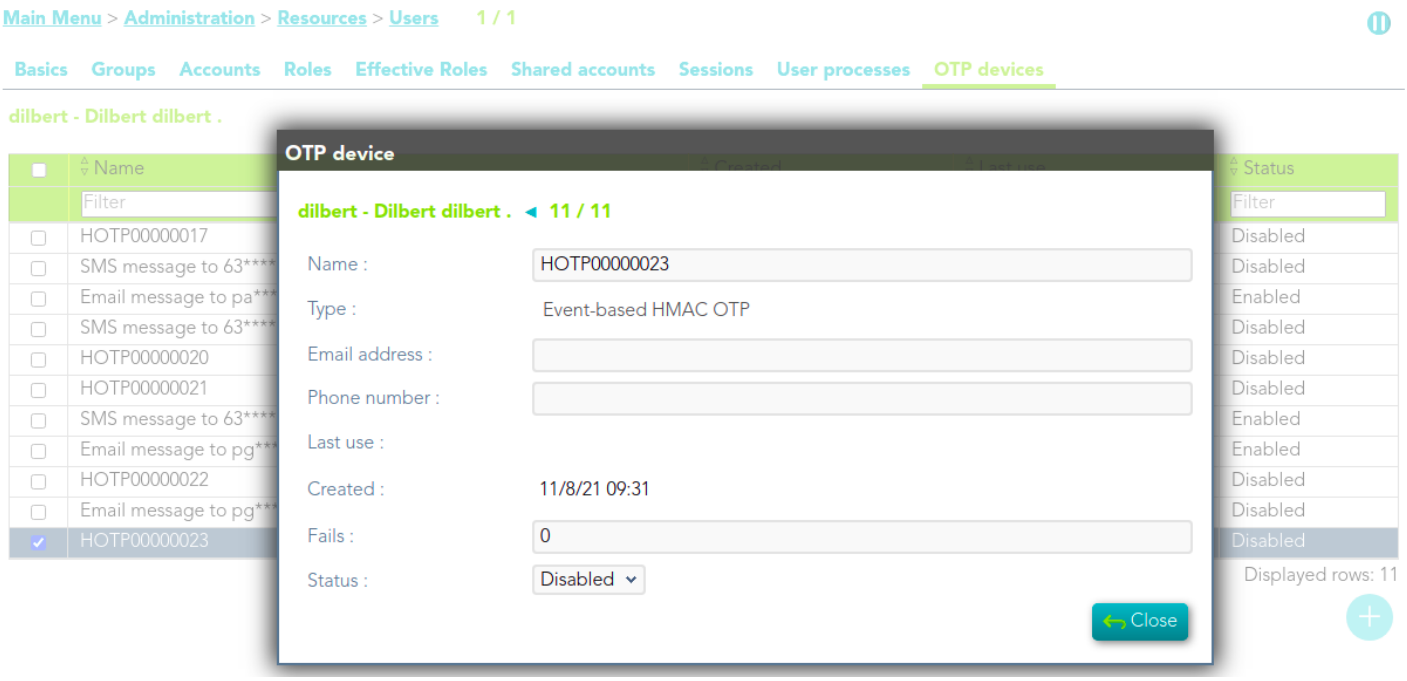
Confirm changes	Allows you to save the updates and quit the page.

Users OTP devices

Description

Soffid allows you to manage the OTP devices for each user. That option will be availavle on the User window. You need to query the user on the Users window, click the proper user and go to the OTP devices Tab, here you could manage the OTP devices for that user.

Screen overview



Standard attributes

- **Name**: authomatic name assigned to the OTP device.
- **Type**: selected type
- **Email address**
- **Phone number**
- **Last use**

- **Created**
- **Fails**: fails number when the OTP device was created.
- **Status**:
  - Created
  - Enabled
  - Locked
  - Disabled

Actions

Add	Allows you to add a new OTP devices. To add a new OTP devices you need clic the add button (+), the Soffid will display a new wizard to config the OTP devices. Fist of all you need select the OTP device Type and then Apply changes.
Delete	Allows you to delete one or more OTP devices for a specific user. To delete OTP devices first select the devices, then click on the subtract button (-), then Soffid will ask you to confirm or cancel the operation.
Change Status	Allows you to change the OTP device status. First of all you need click the proper OTP device, then change the status and finally close the window.

Self service portal

My OTP devices

Description

My OTP devices are part of a Soffid Self-service portal that allows end-users to access their OTP devices configured.

That option display to each user, all their OTP devices and also allows you to manage those and add new OTP devices.

> Soffid Administrator user can configure the available OTP types. For more information, you can visit the OTP settings page.

> This option will only be available if the OTP addon is installed in the Soffid console. Visit the Two factor authentication book for more information

Screen overview

https://www.youtube.com/embed/faw-C7dwYYc?rel=0

Standard attributes

- **Name**: automatic name assigned to the OTP device
- **Created**: created date and time.
- **Last use**: last used date and time.
- **Status**
  - Created
  - Enabled
  - Locked

- Disabled

Actions

Add	Allows you to add a new OTP device. To add new OTP devices you need to click the add button (+), then Soffid will display a new wizard to config the OTP devices. First of all, you need to select the OTP device Type, once the type is selected, you need to fill in the required fields, which depend on the Type selected. If you select an Event-based or Time-based HMAC Token, you will need to scan the QR code and write the PIN. Finally, you must Apply changes.
Delete	Allows you to delete one or more OTP devices. To delete OTP devices first select the devices, then click on the subtract button (-), then Soffid will ask you to confirm or cancel the operation.

SCIM for OTP devices

SCIM for OTP devices

SCIM for OTP devices

SCIM for OTP devices

Getting Started

Introduction

> Soffid allows you to combine two of the most powerful addons you can use into Soffid Console, **SCIM,** and **OTP**.

Please note that the SCIM REST Web Service Add-on installed must be installed, please check this part in How to use SCIM in Soffid # Installation

Please note that a user with the authentication is required, please check this part in How to use SCIM in Soffid # Confirm authorization

Please note that is recommended to use a REST client, please see our example in Testing tool # RESTer

Please note that the correct header parameters must be used, please browse them in SCIM in Soffid # HTTP request

Please note that the OTP addon must be installed and configured, check it in OTP Settings

OTP Device Types

OTP device types available

- **TOTP**: Time based HMAC Token
- **HOTP**: Event based HMAC Token
- **EMAIL**
- **SMS**
- **PIN**: Security PIN

OTP Device Status

OTP device status available :

- C: **Created**
- V: **Validated**
- L: **Locked**
- D: **Disabled**

OTP Operations

Soffid provides an API that allows you to connect to the OTP microservices.

The available operations are the following

- List all
- List by filter
- Query by id
- Create
- Update
- Validate
- Send SMS
- Delete

> You can visit the SCIM OTP devices examples page for more detailed information

Workflows

With the previous operations, using the SCIM OTP API, we can define some workflows.

> You can visit the SCIM OTP devices Workflows examples page

SCIM OTP devices examples

Operations

This page shows the operations that can be performed for the OTP devices object.

List all

Request

```
GET http://<your-domain>/soffid/webservice/scim2/v1/OtpDevice
```

Response 200 OK


```
{
   "schemas": [
      "urn:ietf:params:scim:api:messages:2.0:ListResponse"
   ],
   "totalResults": 25,
   "startIndex": 1,
   "Resources": [
      {
         "lastUsed": "2021-10-14 06:57:00",
         "created": "2021-10-14 06:44:43",
         "meta": {
            "location": "http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/4022880",
            "links": {
               "requestChallenge":
"http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/4022880/requestChallenge",
               "responseChallenge":
"http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/4022880/responseChallenge"
            },
            "resourceType": "OtpDevice"
```

```
    },
    "schemas": [
      "urn:soffid:com.soffid.iam.addons.otp.common.OtpDevice"
    ],
    "name": "TOTP00000001",
    "id": 4022880,
    "type": "TOTP",
    "user": "franck",
    "fails": 0,
    "status": "D"
  },
  {
    "created": "2021-10-14 08:37:38",
    "meta": {
      "location": "http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/4024384",
      "links": {
        "requestChallenge":
"http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/4024384/requestChallenge",
        "responseChallenge":
"http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/4024384/responseChallenge"
      },
      "resourceType": "OtpDevice"
    },
    "schemas": [
      "urn:soffid:com.soffid.iam.addons.otp.common.OtpDevice"
    ],
    "name": "Email message to pg*****@so****.co*",
    "id": 4024384,
    "type": "EMAIL",
    "user": "patricia",
    "fails": 0,
    "email": "patricia@soffid.com",
    "status": "D"
  },
  {
    "created": "2021-10-14 11:17:52",
    "meta": {
      "location": "http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/4024416",
      "links": {
        "requestChallenge":
```

```
"http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/4024416/requestChallenge",
                "responseChallenge":
"http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/4024416/responseChallenge"
            },
            "resourceType": "OtpDevice"
        },
        "schemas": [
            "urn:soffid:com.soffid.iam.addons.otp.common.OtpDevice"
        ],
        "phone": "666555444",
        "name": "SMS message to 66*****44",
        "id": 4024416,
        "type": "SMS",
        "user": "agatha",
        "fails": 0,
        "status": "V"
    },
    .............
    .............
  ]
}
```


List by filter

List all the OTP devices with a filter expression.

> It is allowed to use pagination and sort the information, for more information visit the Sorting and Pagination information.

Request

```
GET http://<your-domain>/soffid/webservice/scim2/v1/OtpDevice?filter=type eq "TOTP"
```

Response 200 OK


```
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:ListResponse"
```

```
    ],
    "totalResults": 7,
    "startIndex": 1,
    "Resources": [
        {
            "lastUsed": "2021-10-14 06:57:00",
            "created": "2021-10-14 06:44:43",
            "meta": {
                "location": "http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/4022880",
                "links": {
                    "requestChallenge":
"http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/4022880/requestChallenge",
                    "responseChallenge":
"http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/4022880/responseChallenge"
                },
                "resourceType": "OtpDevice"
            },
            "schemas": [
                "urn:soffid:com.soffid.iam.addons.otp.common.OtpDevice"
            ],
            "name": "TOTP00000001",
            "id": 4022880,
            "type": "TOTP",
            "user": "franck",
            "fails": 0,
            "status": "D"
        },
      .............
      .............
    ]
}
```


Query by id

Query a OTP device by its id (primary key).

Request

```
GET http://<your-domain>/soffid/webservice/scim2/v1/OtpDevice/5007882
```

Response 200 OK


```
{
   "created": "2022-02-22 07:46:51",
   "meta": {
      "location": "http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/5007882",
      "links": {
         "requestChallenge":
"http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/5007882/requestChallenge",
         "responseChallenge":
"http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/5007882/responseChallenge"
      },
      "resourceType": "OtpDevice"
   },
   "schemas": [
      "urn:soffid:com.soffid.iam.addons.otp.common.OtpDevice"
   ],
   "name": "TOTP00000035",
   "id": 5007882,
   "type": "TOTP",
   "user": "admin",
   "fails": 0,
   "status": "C"
}
```


Create

Allows you to create a new OTP device. It is important the type of the OTP you want to create, and depending on this, it will be mandatory to add new attributes to the request.

- **SMS**: add to the JSON the phone attribute
- **EMAIL**: add to the JSON the email attribute
- **PIN**: add to the JSON the pin attribute

Request

```
http://<your-domain>/soffid/webservice/scim2/v1/OtpDevice
```

JSON

```
{
   "meta": {
      "location": "http://<your-domain>/webservice/scim2/v1/OtpDevice",
      "resourceType": "OtpDevice"
   },
   "schemas": [
      "urn:soffid:com.soffid.iam.addons.otp.common.OtpDevice"
   ],
   "type": "TOTP",
   "user": "admin"
}
```


Response 200 OK


```
{
   "image":
"iVBORw0KGgoAAAANSUhEUgAAAMgAAADIAQAAAACFI5MzAAAC3klEQVR4Xu2XP66jMBDGB7lwFy5gydeg40rkAoR
cgFzJna+B5AtA58Ji9hueQvJWu8UbS6stMoqiwA9lrPn7Qfw3o99vnPYhHyL2L0mghhOz2Xue+tJGIltBIm9haQPdgufsB
utxp4LQlc1M+C5tSLt1TSWJyy26Jvipd2NfTTJPHU/kmlxariS8RX6w2fhwwt+i82OC/ER3fX2+Ze7HBJbp0iGieCQh54dp
SaCBaOz8SmbukfY0C1STJAHIZkdQe947d6khkYau3KKZrNktzs77MwYawoTCuTFqEDytHY1PPxqSEQPPwY3WoOeu0
WzPbGtIoNH6tTdzt1BX2ky3w7mSZAnkA95sQge3eRmfMdAQhh8pwLFL94ACR/9VkOzvbB5oX0LnuaEz9xoS/YORcN
ROGY7jn/nREE5bwCRwFwtveOQtBgoSJc9rnzggOWm27nUCBcnws1wI3OPgeOpVVQqCkdynqU+rLWQx+fwxEtTEEZ
XBLoO4KjcpzAqScZWQbczRNphZOq+CBHcNkuQmSs+hm4enHw1hXBWM9o39PS4XW161oyBhIZt2MishP/imy3kC
DUEAyo3LpZe2m/BUDYlmtdjbUoDYtIQNyRUkLPj7jdNE5g4hIKVUQWK5BszRQh3PWBf0pncUJCAhRjJDGPZokbdtpiC
MooYHs8rZ4WehKuIhnZqM0YIKSo+czsmnIRFKpxyyArfd8FY7GoKRzlSg7gSInqsj2UwdYVZh+c+9jATMZj2J0rUi7ix0Y
sFsFt9qIrtR5PA9o10wYPx0nlpDjJRhD4Xi0MoP6NnTj4KEQ4WJFvNbXlDWZ+1oCCwujWhYg7S3sVQR0bDUYj3GI+3xp
a81BPoah+3T/UvDygqqlShDNxIq2q8dftD7W4GGRLyBYT0ujdRRedOwOgKRgvMiS446z2JqwjKfMJUJextCm87dqCHlj
+xGj0WxMbT/8v7G8mPyZ/uQDxH7n8kvJ2XgRr9Rxi0AAAAASUVORK5CYII=",
   "created": "2022-02-22 07:46:51",
   "meta": {
      "location": "http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/5007882",
      "resourceType": "OtpDevice"
   },
   "schemas": [
      "urn:soffid:com.soffid.iam.addons.otp.common.OtpDevice"
   ],
   "name": "TOTP00000035",
   "id": 5007882,
   "type": "TOTP",
   "user": "admin",
```

```
    "fails": 0,
    "status": "C"
}
```

Example JSON SMS

```
{
    "type": "SMS",
    "user": "dilbert",
    "phone": "6665552222"
}
```

Example JSON EMAIL

```
{
    "type": "EMAIL",
    "user": "dilbert",
    "email": "dilbert@soffid.com"
}
```

Example JSON PIN

```
{
    "type": "PIN",
    "user": "dilbert",
    "email": "123456789"
}
```

Update partial

Only attributes with changes will be updated, the other will mantain the same value. This example shows how to enable an OTP device.

Request

```
PATCH http://<your-domain>/soffid/webservice/scim2/v1/OtpDevice/5007882
```

JSON

```
{
   "Operations":
   [
      {
         "op": "replace",
         "path": "status",
         "value": "V"
      }
   ]
}
```

Response 200 OK

```
{
   "created": "2022-02-22 07:46:51",
   "meta": {
      "location": "http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/5007882",
      "links": {
         "requestChallenge":
"http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/5007882/requestChallenge",
         "responseChallenge":
"http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/5007882/responseChallenge"
      },
      "resourceType": "OtpDevice"
   },
   "schemas": [
      "urn:soffid:com.soffid.iam.addons.otp.common.OtpDevice"
   ],
   "name": "TOTP00000035",
   "id": 5007882,
   "type": "TOTP",
   "user": "admin",
   "fails": 0,
   "status": "V"
}
```

Request Challenge

This operation allows Soffid to obtain the PIN code for a specific OTP device. We can use this method to send an email or SMS, depending on the type of OTP device.

Request

```
GET http://<your-domain>//soffid/webservice/scim2/v1/OtpDevice/<OTP_ID>/requestChallenge
```

Response 200 OK

```
{
   "cell": "PIN",
   "cardNumber": "SMS message to 66*****22"
}
```

Response Challenge

This operation allows you to validate a PIN code for a specific OTP device.

Request

```
POST http://<your-domain>//soffid/webservice/scim2/v1/OtpDevice/<OTP_ID>/responseChallenge
```

JSON

```
{
   "pin": "12345678"
}
```

Response 200 OK

```
{
   "success": false,
   "locked": false
}
```

Delete

In this case, delete operation will cancel the TaskInstace, but does not be deleted form database.

Please note after this delete, the account has to be created again to use it in the next examples.

Request

DELETE - http://<your-domain>/soffid/webservice/scim2/v1/OtpDevice/5007967

Response 204 No Content

204 No Content

Error response

For more information about error response visit

https://bookstack.soffid.com/link/116#bkmrk-error-response

SCIM OTP devices Workflows examples

Workflow Examples

Workflow 1

1. Create Email OTP device

Request

```
GET http://<your-domain>/soffid/webservice/scim2/v1/OtpDevice
```

JSON


```
{
   "type": "EMAIL",
   "user": "dilbert",
   "email": "dilbert@soffid.com"
}
```


Response 200 OK


```
{
   "created": "2022-03-09 13:39:52",
   "meta": {
      "location": "http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/5099461",
      "resourceType": "OtpDevice"
   },
   "schemas": [
      "urn:soffid:com.soffid.iam.addons.otp.common.OtpDevice"
```

```
    ],
    "name": "Email message to di*****@so****.co*",
    "id": 5099461,
    "type": "EMAIL",
    "user": "dilbert",
    "fails": 0,
    "email": "dilbert@soffid.com",
    "status": "C"
}
```


2. RequestChallenge to get the PIN code

Request

```
GET http://<your-domain>/soffid/webservice/scim2/v1/OtpDevice/5099461/requestChallenge
```

Response 200 OK


```
{
    "cell": "PIN",
    "cardNumber": "Email message to di*****@so****.co*"
}
```


3. ResponseChallenge to validate the PIN code

Request

```
POST http://<your-domain>/soffid/webservice/scim2/v1/OtpDevice/5099461/responseChallenge
```

JSON


```
{
    "pin": "839231"
}
```


Response 200 OK


```
{
    "success": true,
    "locked": false
```

```
}
```

4. Enable OTP device

Request

```
PATCH http://<your-domain>/soffid/webservice/scim2/v1/OtpDevice/5099461
```

JSON

```
{
   "Operations":
   [
      {
         "op": "replace",
         "path": "status",
         "value": "V"
      }
   ]
}
```

Response


```
{
   "created": "2022-03-09 13:39:52",
   "meta": {
      "location": "http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/5099461",
      "links": {
         "requestChallenge":
"http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/5099461/requestChallenge",
         "responseChallenge":
"http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/5099461/responseChallenge"
      },
      "resourceType": "OtpDevice"
   },
   "schemas": [
      "urn:soffid:com.soffid.iam.addons.otp.common.OtpDevice"
   ],
   "name": "Email message to di*****@so****.co*",
   "id": 5099461,
```

```
    "type": "EMAIL",
    "user": "dilbert",
    "fails": 0,
    "email": "dilbert@soffid.com",
    "status": "V"
}
```


Workflow 2

1. Get TOTP devices

Obtain all unused OTP devices by 2022.

Request

```
GET http://<your-domain>/soffid/webservice/scim2/v1/OtpDevice?filter=lastUsed le "2022-01-01"
```

Response 200 Ok


```
{
    "schemas": [
        "urn:ietf:params:scim:api:messages:2.0:ListResponse"
    ],
    "totalResults": 5,
    "startIndex": 1,
    "Resources": [
        {
            "lastUsed": "2021-10-14 06:57:00",
            "created": "2021-10-14 06:44:43",
            "meta": {
                "location": "http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/4022880",
                "links": {
                    "requestChallenge":
"http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/4022880/requestChallenge",
                    "responseChallenge":
"http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/4022880/responseChallenge"
                },
                "resourceType": "OtpDevice"
            },
```

```
        "schemas": [
            "urn:soffid:com.soffid.iam.addons.otp.common.OtpDevice"
        ],
        "name": "TOTP00000001",
        "id": 4022880,
        "type": "TOTP",
        "user": "admin",
        "fails": 0,
        "status": "E"
    },
    {
        "lastUsed": "2021-10-14 06:59:33",
        "created": "2021-10-14 06:58:05",
        "meta": {
            "location": "http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/4022891",
            "links": {
                "requestChallenge":
"http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/4022891/requestChallenge",
                "responseChallenge":
"http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/4022891/responseChallenge"
            },
            "resourceType": "OtpDevice"
        },
        "schemas": [
            "urn:soffid:com.soffid.iam.addons.otp.common.OtpDevice"
        ],
        "name": "TOTP00000002",
        "id": 4022891,
        "type": "TOTP",
        "user": "ckelp",
        "fails": 0,
        "status": "C"
    },
    .....
  ]
}
```


2. Disable OTP device

Disble the OTP devices one by one

Request

```
PATCH http://<your-domain>/soffid/webservice/scim2/v1/OtpDevice/4022880
```

JSON

```
{
   "Operations":
   [
      {
         "op": "replace",
         "path": "status",
         "value": "D"
      }
   ]
}
```

Response 200 Ok


```
{
   "lastUsed": "2021-10-14 06:57:00",
   "created": "2021-10-14 06:44:43",
   "meta": {
      "location": "http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/4022880",
      "links": {
         "requestChallenge":
"http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/4022880/requestChallenge",
         "responseChallenge":
"http://soffid.pat.lab:8080/soffid/webservice/scim2/v1/OtpDevice/4022880/responseChallenge"
      },
      "resourceType": "OtpDevice"
   },
   "schemas": [
      "urn:soffid:com.soffid.iam.addons.otp.common.OtpDevice"
   ],
   "name": "TOTP00000001",
   "id": 4022880,
   "type": "TOTP",
   "user": "admin",
   "fails": 0,
```

```
    "status": "D"
}
```