

# 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

**Email**

Enabled :  Yes  No

Number of digits : 6

Subject : Your authentication code is \${PIN}

Body : Your authentication code is \${PIN}

Number of failures to lock the token : 10

**SMS**

Enabled :  Yes  No

Number of digits : 6

Url to send the SMS : https://www.ovh.com/cgi-bin/sms/http2sms.cgi?account=sms-bg490971-1&password=

HTTP Method : GET

HTTP Headers : HTTP Headers

POST data to send : POST data to send

Text to be present in the HTTP response : Text to be present in the HTTP response

Number of failures to lock the token : 10

**Voice (alternative to SMS)**

Enabled :  Yes  No

Url to send the voice message : https://rest.clicksend.com/v3/voice/send

HTTP Method : POST

HTTP Headers : Authorization: Basic asdfakslfdjfkasjfkasjckalsjdfklsdjflkasjdfklajsdfkjkaskdfjaskdfj

POST data to send : {"messages": [{"to": "\${PHONE}", "body": "This is a Spffod voice call. Your PIN is....."}]}

Text to be present in the HTTP response : Text to be present in the HTTP response

**Time based HMAC Token**

Enabled :  Yes  No

Number of digits : 6

Algorithm : HmacSHA1

Issuer : Issuer

Number of failures to lock the token : 10

**Event based HMAC Token**

Enabled :  Yes  No

Number of digits : 6

Algorithm : HmacSHA1

Issuer : Issuer

Number of failures to lock the token : 10

**Security PIN**

Enabled :  Yes  No

Minimum PIN length : 8

Number of digits from the PIN to ask : 3

Number of failures to lock the token : 10

[Confirm changes](#)

# 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 HTTP 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 HTTP header, including Basic or Bearer authentication tokens. The header must include the header name and header value. For instance:

```
Authorization: Basic xxxxxxxxxxxxxxxOUVCRS1DMzE0LTlzMzAtQkY0Qy05RDgwRTMyQUQ4OUY=
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

|                        |   |
|------------------------|---|
| <b>Confirm changes</b> | Allows you to save the updates and quit the page. |
|------------------------|---|

---

Revision #4

Created 17 June 2022 07:21:18

Updated 30 November 2022 10:19:56