SMTP Authentication API

API Documentation

Corresponding software version:
Celonis Process Mining 4.7.3.2

Revision History

Version	Date	Description	Author
1.0	10.10.2022	Initial creation	Andrii Kovalenko

Table of Content

Description

Each mail service provider has different rules, limits and API for authentication token update (refresh, rotation). Hence, Celonis can not implement an auto-refresh mechanism. Instead, our application exposes an API endpoint for SMTP password/token updates. If your SMTP provider only supplies short-lived tokens, we recommend implementing and configuring periodic auto-refresh scripts, using your preferred tools (script languages, scheduled jobs, etc.).

Notes:

- For now only an API to update the SMTP password (token) is available.
- For now only the authentication type *OAuth 2.0 (XOAUTH2) SASL* is available.

Prerequisites

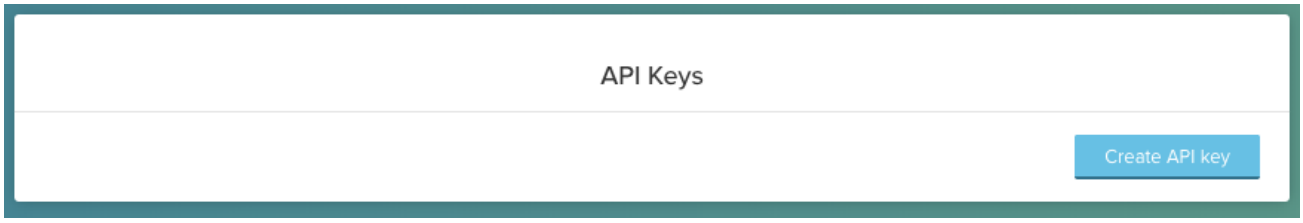
Celonis User & API Key Setup

In order to operate the SMTP Authentication API, it is recommended to set up a separate Celonis user with API token access. The endpoints will be accessed in the name of this user.

The following has to be configured for the user:

- *System Administrator* role
- the user needs to have a valid Celonis API key

To create the Celonis API key, log into the profile of the respective user and open the *My Profile* section. The bottom of the page shows the option to create an API key:

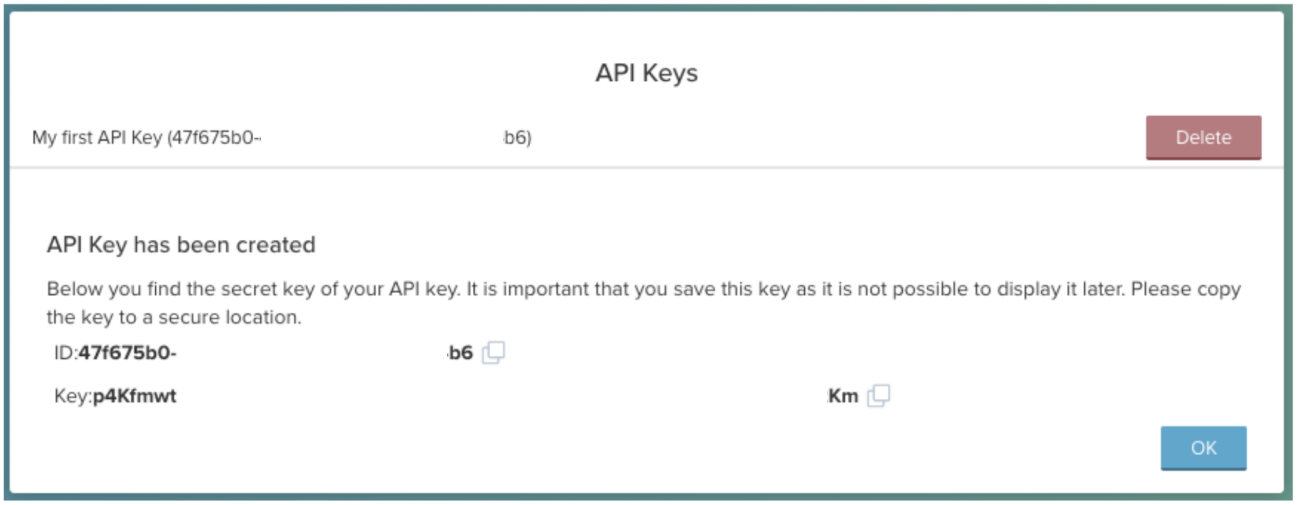


API Keys configuration

After creating the key, the **key-ID** (**X-API-ID**) and the **token key** (**X-API-TOKEN**) are displayed. These two values, together with the username (**X-API-USER**) are required for authentication to the endpoints.

Notes:

- The key is *only* valid for the respective user (**X-API-USER** in the following) on the CPM4 instance it is created on
- The token key (**X-API-TOKEN**) is only visible once upon creation of the API Key. After clicking “OK” in the bottom right corner, it is no longer visible. Store it in a safe place.
  If the token is lost, a new API key has to be created.



API Key configuration

First-time *Mail → SMTP Server Configuration* setup

Pre-configure your SMTP connection in the Web UI:

1. Navigate to *System Settings → Mail*
2. Select either *ssl* or *tls* authentication
3. Select the `OAuth 2.0 (XOAUTH2)` SASL Authentication type
4. The password field is now used for the OAuth token

Methods

Update SMTP password (token)

Request

Method	URL
PUT	api/configuration/smtp/password

Type	Params	Values
HEAD	Content-Type	application/json
HEAD	X-API-USER	string
HEAD	X-API-ID	string
HEAD	X-API-TOKEN	string
PAYLOAD (JSON)	password	string

X-API-USER
`X-API-USER` must be sent with all client requests. This refers to the *username* that was used to create the `X-API-TOKEN` and helps the server to validate the request source.

X-API-ID and **X-API-TOKEN**
`X-API-ID` and `X-API-TOKEN` must be sent with all client requests. This helps the server to validate the request source. The Token is equivalent to the API Key generated here.

Curl example

```
$ curl -v -X PUT 'http://<server-url>/api/configuration/smtp/password \
     -H 'Content-Type: application/json' \
     -H 'X-API-USER:sysadmin \
     -H 'X-API-ID:3ec99906-b10f-4ed2-8690-150596873256'
     -H 'X-API-TOKEN:djLRlkxi4mM2dwLPFA89sDbjcM3x1opuDdJhDhlglyW9ogqtoVt7' \
     --data '{"password":"ABCDEFGH123456789"}'
```

Response

Status	Response
204	No Content
403	<<no content>>
400	{"globalErrors":["Password must be not blank"]}
404	{"globalErrors":["SMTP connection is not configured"]}
500	{"globalErrors":[...]"}

Glossary

Conventions

- **Client** - HTTP Client tool
- **Status** - HTTP status code of response.

Status Codes

All status codes are standard HTTP status codes. The below ones are used in this API.

2XX - Success
4XX - Error from client side (permissions, request format errors etc)
5XX - Error occurred on server side