

# REST API Access

## Base URL

The API is accessed using the base URL of the API Server and the following URL:

```
http(s)://jtel-rest-api-server:port/rest/v1.0/{ClientsID}
```

The **ClientsID** must be provided with every request.

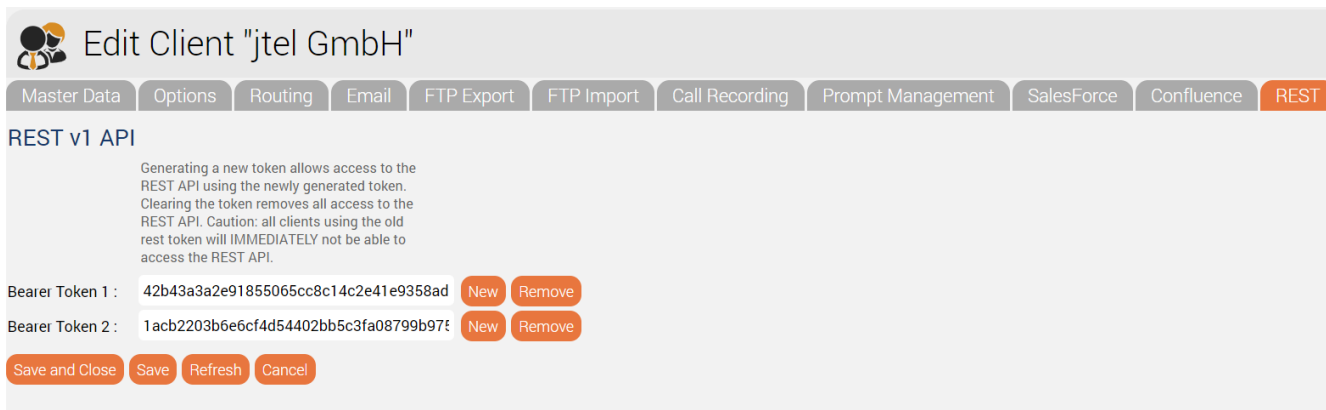
## Authorization

The Authorisation is **Bearer** token based authorization, using one of the tokens generated in the jtel portal.

To perform bearer authorization, provide the following http header with the request:

```
Authorization: Bearer {TOKEN}
```

The tokens are generated here:



The screenshot shows the 'Edit Client "jtel GmbH"' interface. At the top, there is a navigation bar with tabs: Master Data, Options, Routing, Email, FTP Export, FTP Import, Call Recording, Prompt Management, SalesForce, Confluence, and REST (which is highlighted in orange). Below the navigation bar, the 'REST v1 API' section is active. It contains a text box with instructions: 'Generating a new token allows access to the REST API using the newly generated token. Clearing the token removes all access to the REST API. Caution: all clients using the old rest token will IMMEDIATELY not be able to access the REST API.' Below this, there are two rows of token information. The first row shows 'Bearer Token 1 : 42b43a3a2e91855065cc8c14c2e41e9358ad' with 'New' and 'Remove' buttons. The second row shows 'Bearer Token 2 : 1acb2203b6e6cf4d54402bb5c3fa08799b97f' with 'New' and 'Remove' buttons. At the bottom of the section, there are four buttons: 'Save and Close', 'Save', 'Refresh', and 'Cancel'.

Generating a new token or removing the token will immediately invalidate the token.

## Headers

In addition to the authorization header, all functions which require POST data to be sent with the request, require that the following header be set:

Content-Type: application/json