TB Digital Services GmbH • Oskar-Schlemmer-Str. 19–21 • 80807 Munich

TB Digital Services GmbH
Oskar-Schlemmer-Straße 19–21
80807 Munich
Germany

+49 (0) 08 00 22 55 07 46
www.rio.cloud

Senior Management
Jan Kaumanns
Christopher Busch

Court of Registration
Amtsgericht München
HRB 234868
USt-IdNr. DE 314435023

Externe Dokumentation
Outbound Order Book
Security

1. Scope of this document

This document only describes how the partner gets access to the data of RIO Outbound Order Book. It does not describe billing, business APIs etc.

2. Partner responsibilities

- Provide contact name and email address. This should be a mailing list of people responsible for the application, not an individual person which quickly gets outdated. It will be used for important announcements, updates and possibly warnings in case of abuse.
- React to emails send to the contact email address within a few days. Keep it up to date.

3. Technical integration

We provide a technical user that grants access to Outbound Order Book. It must only be used by confidential clients, that can safely keep a client_secret.
To login, we use a standard OAUTH2 Client Credential grant (https://oauth.net/2/grant-types/client-credentials/) via https://auth.iam.rio.cloud

You will receive a client_id and client_secret that are used to request an access token.

Example request for login:

```
POST /oauth/token HTTP/1.1
Host: auth.iam.rio.cloud
Content-Type: application/x-www-form-urlencoded
Accept: application/json
Authorization: Basic client_id:client_secret
grant_type=client_credentials
```

Note: To be compliant to the OAuth 2.1 Authorization Framework specification, it is required to send all parameters in the body of the request via application/x-www-form-urlencoded (apart from the credentials which should be sent via the Authorization Header). The client requests will fail if query parameters are used.

The response looks like specified by RFC 6749:

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache
{
"access_token":"2YotnFZFEjr1zCsicMWpAA",
"token_type":"bearer",
"expires_in":3600,
"scope":"scope1 scope2"
}
```

Your application can use the access token contained in the response to access the APIs in the scope directly by using it as a Bearer token (https://oauth.net/2/bearer-tokens/).
A new access token can be requested whenever it is needed.
Be aware that the token will expire after 60 minutes.