Short partner documentation

1 Scope of this document

This document only describes how the partner gets access to the data of RIO customers and how the permissions are managed. It does not describe billing, business APIs or how the partner application is integrated into the marketplace.

2 Partner responsibilities

- Provide the following information
    - Name, short description (1-2 sentences) and a more detailed description of the application
    - Contact name and email address. This should be a mailing list of people responsible for application, not a individual person which quickly gets outdated. It will be used for important announcements, updates and possibly warnings in case of abuse.
    - Required OAuth scopes and permissions on the RIO platform (A concrete list of these is not available yet. The required scopes and permissions should be determined in collaboration with RIO.)
    - Required grant types
    - Callback URL for subscription confirmation callbacks (if applicable)
- React to emails send to the contact email address within a few days. Keep it up to date.

3 Marketplace integration for partners with backend integration

3.1 Partner application registration

Whenever a partner application is registered, the following happens:

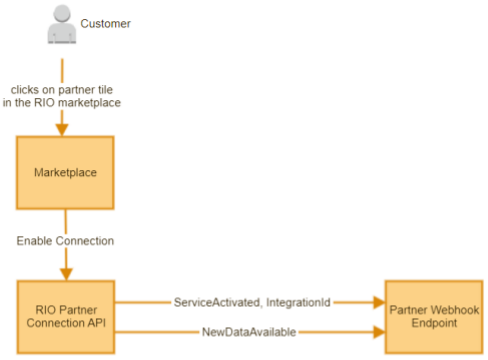
- A new client for the partner application is registered at the authorization server.
- The partner gets a client id and secret to initialize his application.
- The partner application is added to the marketplace.

3.2 Product subscription

Whenever a customer books an application in the marketplace we automatically push relevant information about the booking to the partner via a webhook mechanism. This information also includes an integration id which is required to get access tokens for retrieving data from the RIO APIs on behalf of the customer. The next section provides more information about the process of getting access tokens using the partner_integration grant type.

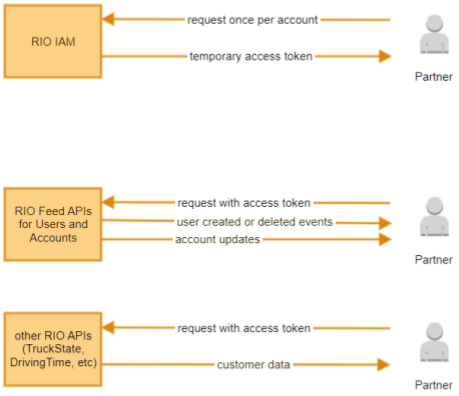
1

Initiate the connection customer <> partner



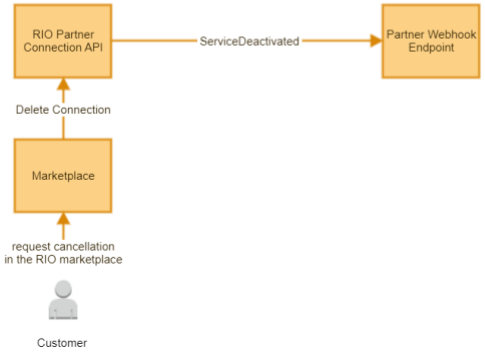
2

Query data of the customer



(3)

Terminate the connection customer <> partner



3.3 Partner integration grant type

The partner integration grant types provides a technical user for each account that has a subscription to the partner product using only the partner applications client_id and client_secret. This grant must only be used by confidential clients, that can safely keep a client_secret.

Parameters:

- Authorization (header, required): HTTP Basic authentication with client_id and client_secret
- Grant type (body, required): partner_integration
- Integration id (body, required): The integration id given to the partner during product activation

Example request:

```
POST /oauth/token HTTP/1.1
Host: auth.iam.rio.cloud
Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW
Content-Type: application/x-www-form-urlencoded
Accept: application/json
grant_type=partner_integration&integration_id=58cfbc07-4424-45b5-8638-
f24f9f734fcb
```

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"
}
```

The partner application can use the access token in the response to access the APIs in the scope directly. A refresh token is not issued, since the partner application can get a new access token whenever it needs to.

Example with curl

```
curl --user ${client_id}:${client_secret} -k -d
"grant_type=partner_integration&integration_id=${integration_id}"
https://auth.iam.rio.cloud/oauth/token
```

* * *