Last updated 15.12.2023

OAuth2-Authorization Flow in Production

Attention should be paid to:

We can only map the processes that are the same for all retailers and take place in the OTTO Market API or in OTTO Partner Connect. All other processes are very individual and can therefore not be described in detail.

If you have any questions, please contact us at: Helpdesk

Content

Last updated 15.12.2023

Create an app as a developer to connect with a partner

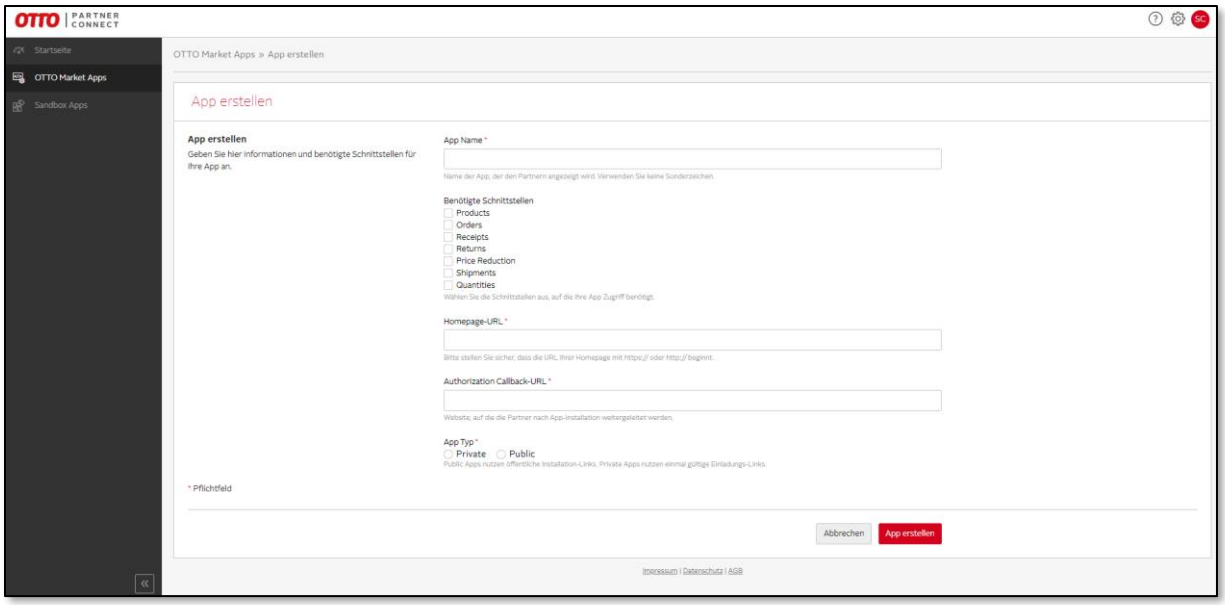
Prerequisite

Have been released for production, have the permission for private production apps and are able to create private apps. (see https://api.otto.market/docs#section/Developer-Program/Private-and-Public-Access-for-Service-Provider)

Create app

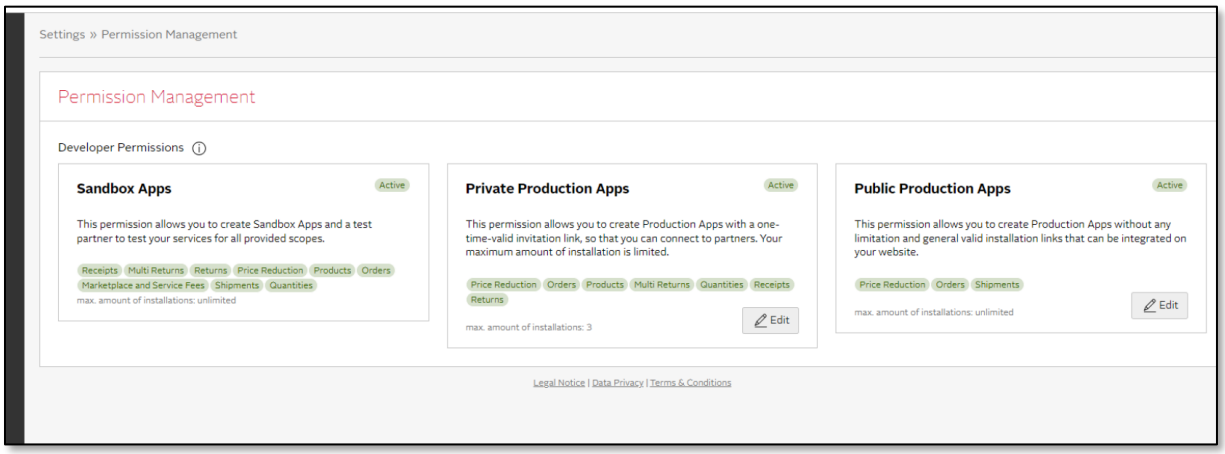
Create a new app (see https://api.otto.market/docs#section/Developer-Program/Private-and-Public-Apps) with the following values (see https://api.otto.market/docs#section/Developer-Program/Access-to-Production):

- unique name / App Name
- Homepage URL
- Authorization Callback URL - Refer below section for more info
- Scopes - Only scopes approved for you will be shown
- App type (only if the service provider has public access)

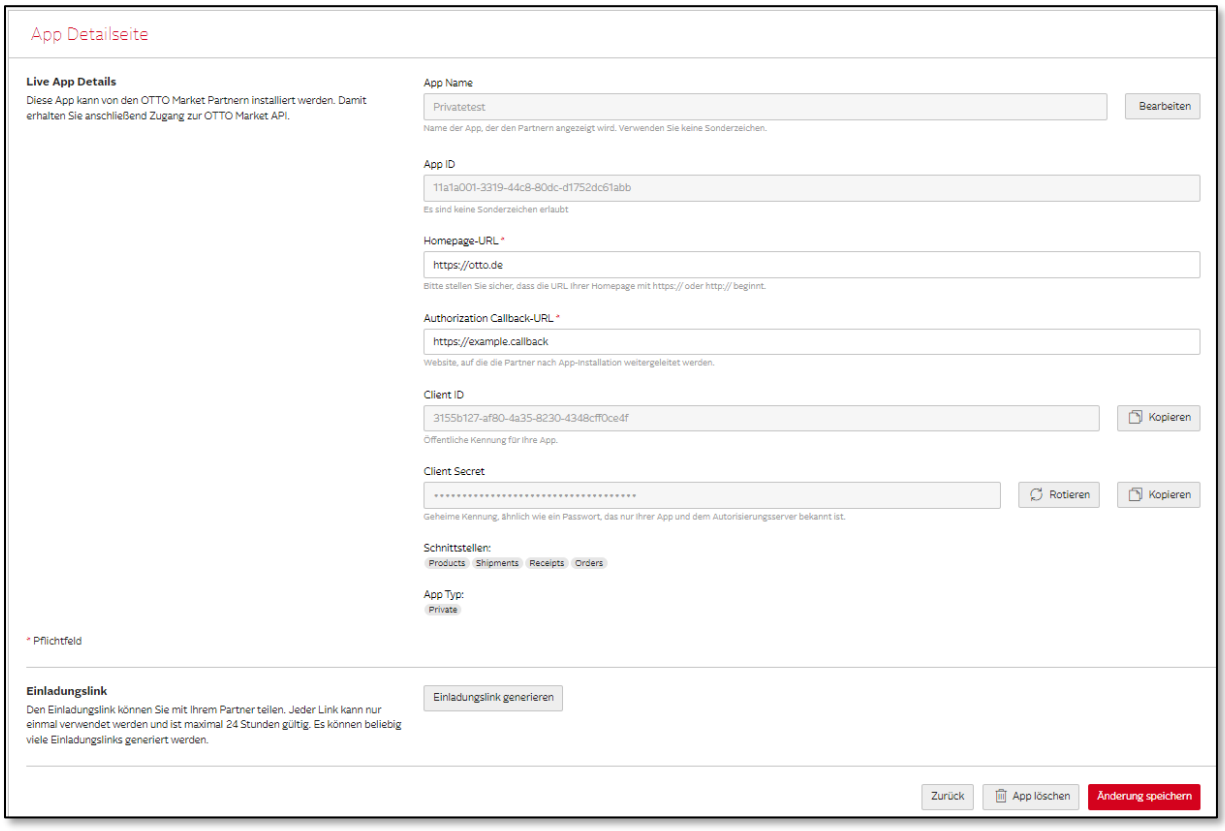


Difference between Private and Public

After you have been activated for the Private Production Apps, you are able to create OTTO Market Apps with the App Type “private”. When you are approved for the permission "Public Production Apps" (in the permission management – see Screenshot) you can create Apps with the App Type "public" as well.

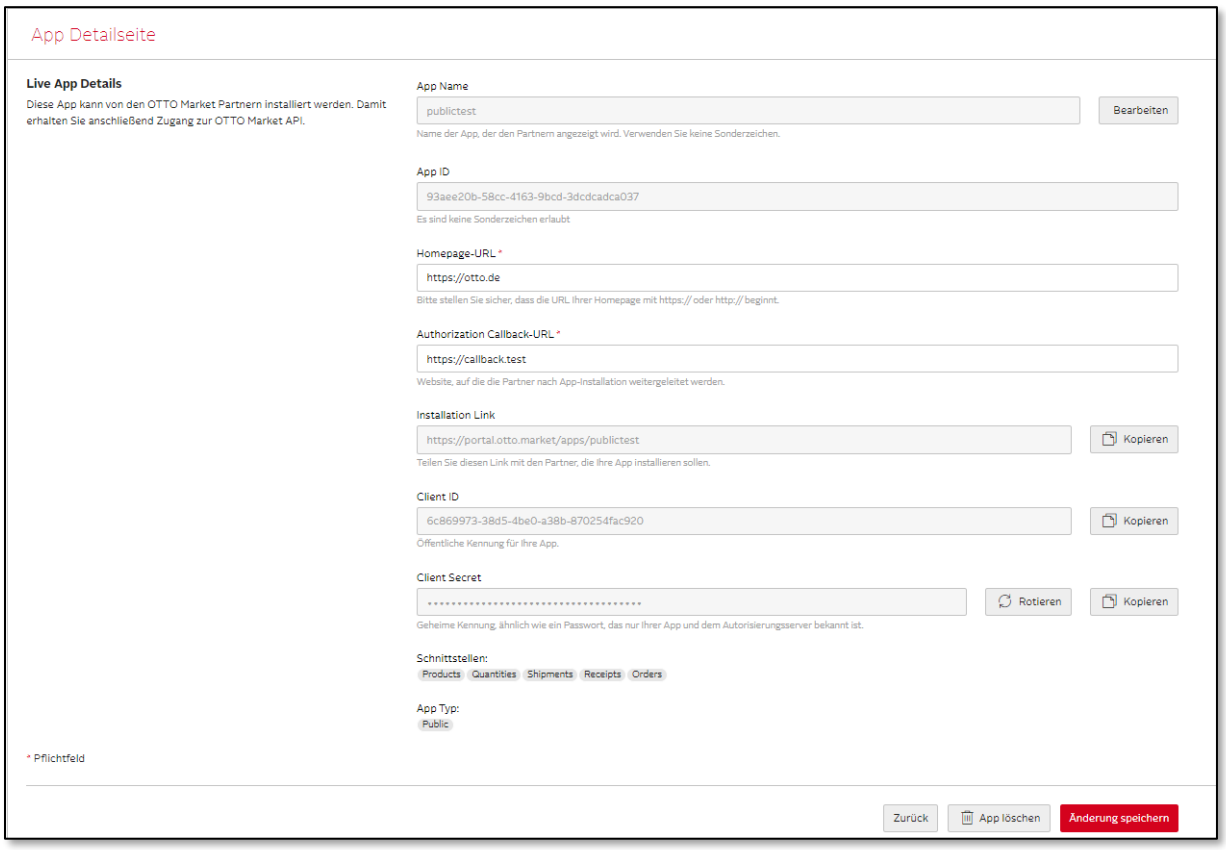


Private Apps:



After creating Private Apps, you will receive a Client Id and Client Secret as well as an App ID. Now you have the possibility to generate an invitation link. This invitation link is only applicable once for a partner. You must provide this to your customer in order to start the installation of your app with your client - Step 1 (for more information, see the graphic under the following link): https://api.otto.market/docs#section/Developer-Program/Installation-of-app-by-an-OTTO-Partner-(Sandbox-or-Production)

Public Apps:



After the creation of Public Apps, you will receive a Client ID and Client Secret as well as an App ID and an Installation Link. The installation link initiates the process of your customers installing your app within their respective otto accounts. This link is universally valid and remains consistent for all customers. You also can add an optional State parameter at the end of the Installation Link for individual cases. For a more detailed explanation, please refer to the graphic provided in the following link: https://api.otto.market/docs#section/Developer-Program/Installation-of-app-by-an-OTTO-Partner-(Sandbox-or-Production)

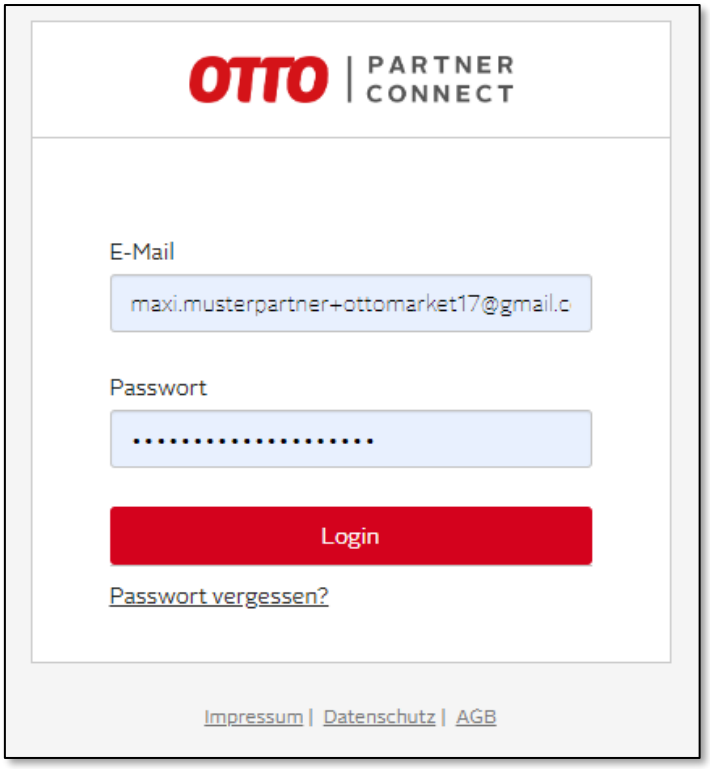
Install a developer app as an OTTO Market partner

Prerequisite

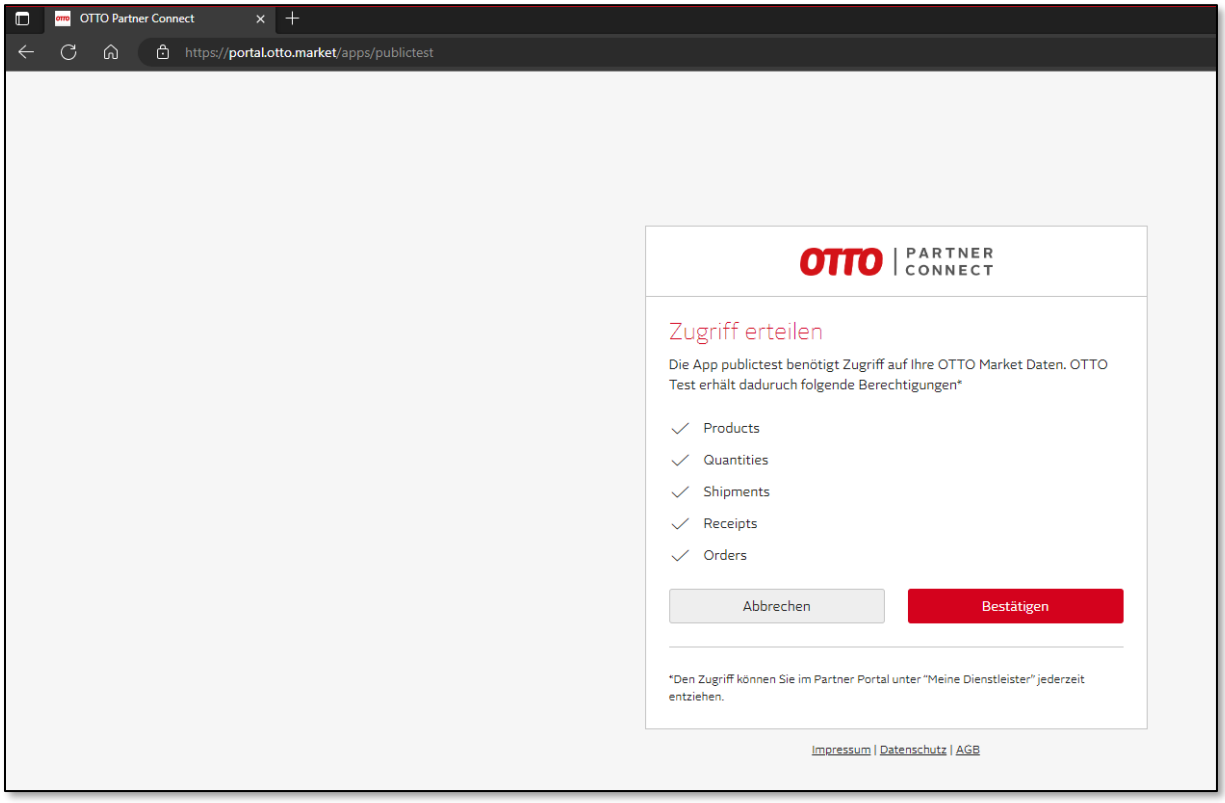
The User of the Partner has the right “Dienstleister Freigaben”. If not, the Partner has to process the following steps.

1. Login here https://portal.otto.market
2. Settings → open „Nutzerverwaltung“
3. Select user, who´ll install the developer app (click „…“ close to the username)
4. Click „Ansehen/Bearbeiten“
5. Select „Dienstleister Freigaben“
6. Save

7. Open the invitation link (Private App) or installation link (Public App) from the developer app
   a. Example link: https://portal.otto.market/apps/publictest
8. The chosen user with the role „Dienstleister Freigaben“ has to log on to OTTO Partner Connect

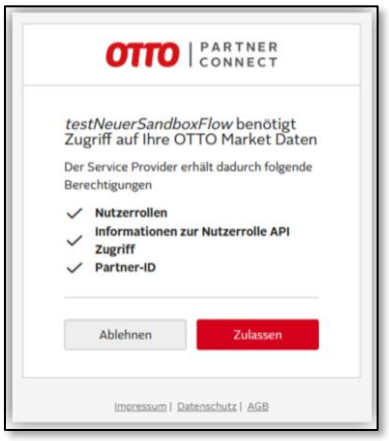


9. After login the user will see the modal with „Zugriff erteilen”
    a. Here are the scopes for which the trader gives access to the developer



10. After the successful authorization, the redirect to the callback URL configured in the app should take place. You need to process the Step 3.1. and redirect the user to the OTTO Portal again to authenticate against the app. Please also have a look here to get more information

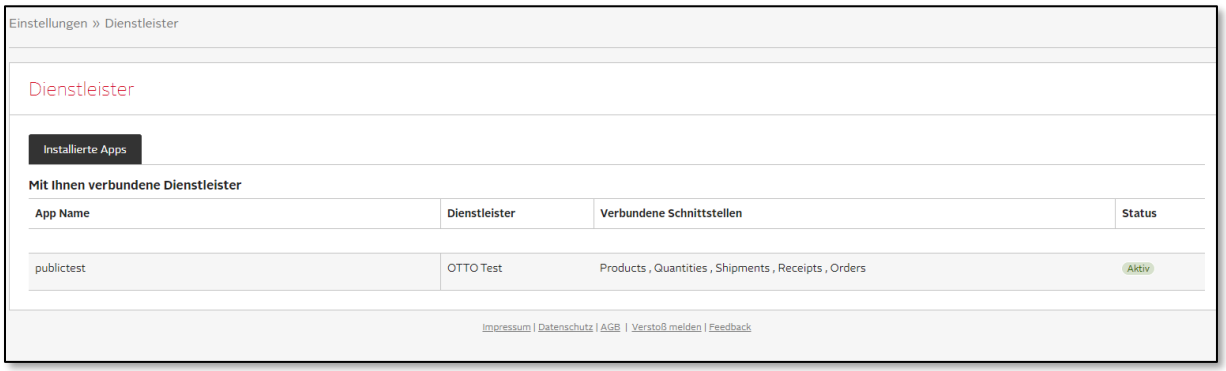
about the steps 3.1.-3.4. (https://api.otto.market/docs#section/Developer-Program/Installation-of-app-by-an-OTTO-Partner-(Sandbox-or-Production))



11. After the user clicks “Zulassen” the redirect to the callback URL will be proceed again. Now you should get the Auth code.
12. Please note: If the step 3.1.-3.3. does not happen, the app will be shown as “wird installiert” in the Overview for the partner and you cannot proceed with Step 4-6 because you are not getting back an Installation ID

Result:

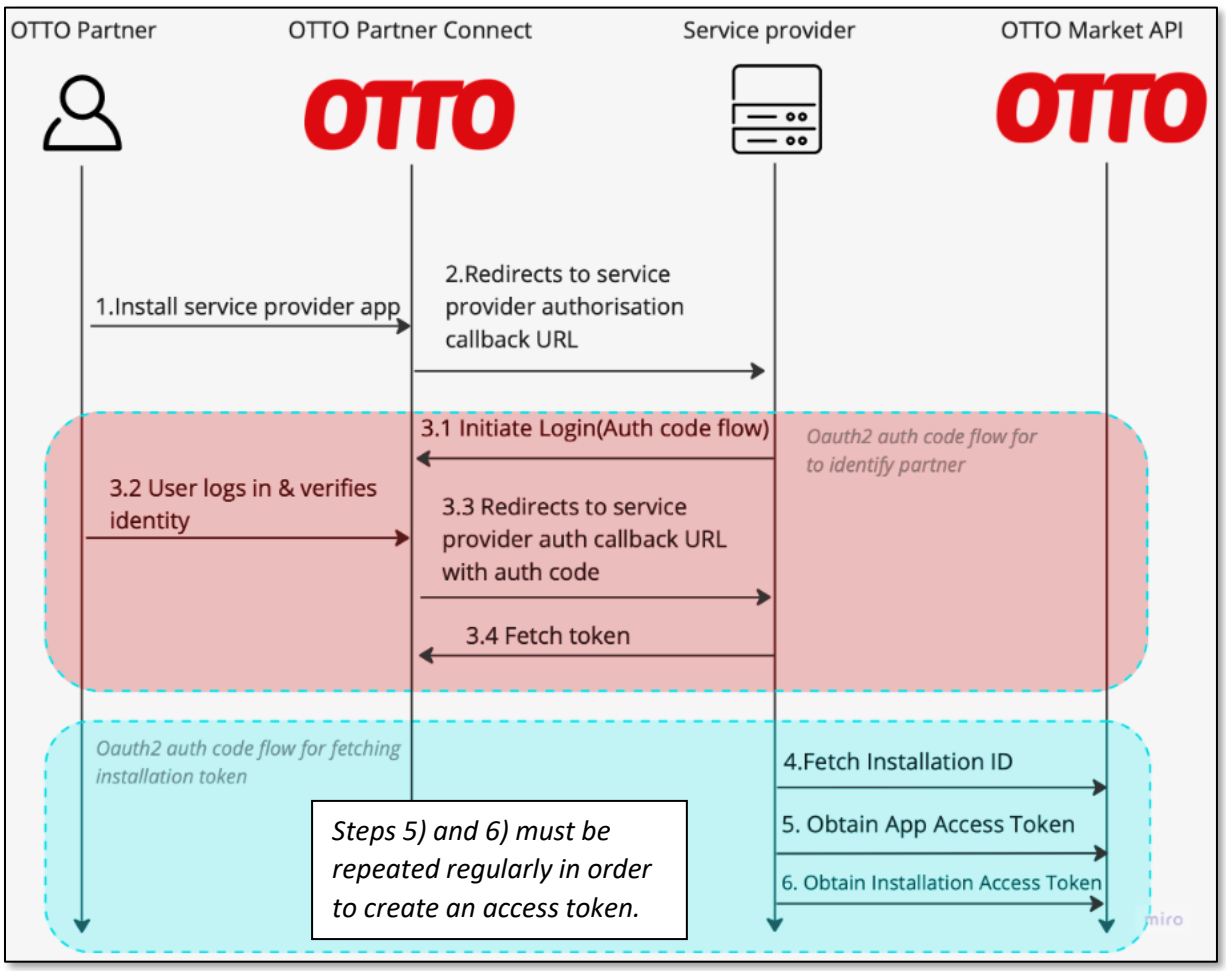
The partner can now view the installed app in OTTO Partner Connect (Settings -> Service provider) and also revoke access if necessary.



Go through the OAuth2 flow as a developer

OAuth2-Process flow

The following steps must be technically mapped by the developer for the OAuth2 flow. The documentation can also be found below https://api.otto.market/docs#section/Developer-Program/Installation-of-app-by-an-OTTO-Partner-(Sandbox-or-Production)



Process flow described in text form

See https://api.otto.market/docs#section/Developer-Program/Access-to-Production-and-Integration-of-Production-Apps

1. The partner navigates to your application's installation link and installs your application. If desired, a "state" parameter can be added to the installation link for tracking the installer of your application.
2. After successful installation, the partner is redirected to your application's authorization callback URL. If a "state" query parameter was included in the installation link, it will be added to the callback URL, redirecting the user upon successful installation.
3. Within your callback logic, authenticate the partner user and obtain an access token by implementing the OAuth2 Authorization Code Flow:

   3.1. Redirect the user to the authorization endpoint with scopes `installation` and `partnerId`. The server should respond with a HTTP 302 response that redirects the user-agent to the authorization URL, which includes parameters like client_id, redirect_uri, response_type, and scope.

   - Sandbox: https://sandbox.api.otto.market/oauth2/auth?response_type=code&client_id={CLIENT_ID}&redirect_uri={REDIRECT_URI}&scope=installation%20partnerId
   - Production: https://api.otto.market/oauth2/auth?response_type=code&client_id={CLIENT_ID}&redirect_uri={REDIRECT_URI}&scope=installation%20partnerId

   Please note that 'REDIRECT_URI' is optional. It serves as the URI where your app can send and receive authentication responses. The protocol, host, and URL path (excluding query parameters) of the 'REDIRECT_URI' must align with your app's authorization callback URL.

   3.2 User logs in and verify their identity

   3.3. After the user grants authorization, your application will receive an authorization code at the redirect URI provided. The server will respond with a HTTP 302 that directs the user-agent to the provided redirect URI.

   3.4. Exchange the authorization code for an access token by making a POST request to the token endpoint, including the authorization code, redirect URI, and client ID in the body. Ensure the `Content-Type` header is set as `application/x-www-form-urlencoded`.

- Sandbox: https://sandbox.api.otto.market/oauth2/token
- Production: https://api.otto.market/oauth2/token

For more information on implementing the OAuth2 Authorization Code Flow, please refer to the OAuth 2.0 Authorization Code section of the OAuth2 standard documentation. You can retrieve the necessary endpoints from the OpenID Connect well-known configuration:

- Sandbox Well-Known Endpoint: Sandbox Well-Known Endpoint
- Production Well-Known Endpoint: Production Well-Known Endpoint

4. Upon successful user authentication, retrieve the Installation ID by sending a GET request to the endpoint `/v1/apps/{appId}/installation`. The domain will be sandbox.api.otto.market or api.otto.market based on whether you're in a sandbox or production environment. Replace `{appId}` with your specific service provider application's unique ID. Use the access token obtained in the previous step.

```
GET /v1/apps/{appId}/installation HTTP/1.1
Host: sandbox.api.otto.market or api.otto.market
Authorization: Bearer {access_token}
```

The response will be:

```
{
  "installationId": "string"
}
```

5. Implement the Client Credentials Flow to fetch an access token with the `developer` scope:

```
POST /oauth2/token HTTP/1.1
Host: sandbox.api.otto.market or api.otto.market
Content-Type: application/x-www-form-urlencoded

grant_type=client_credentials&client_id={CLIENT_ID}&client_secret={CLIENT_SECRET}&scope=developer
```

Replace `{CLIENT_ID}` and `{CLIENT_SECRET}` with your actual client ID and client secret.

6. With the obtained token, retrieve an installation access token by making a POST request to `/v1/apps/{appId}/installations/{installationId}/accessToken`. The request body should be `application/x-www-form-urlencoded` and include the `scope` parameter with the values such as `orders`, `shipments`, `receipts`. Please see Developer Program for list of available scopes. Multiple scope values should be space separated.

```
POST /v1/apps/{appId}/installations/{installationId}/accessToken HTTP/1.1
Host: sandbox.api.otto.market or api.otto.market
Authorization: Bearer {access_token}
Content-Type: application/x-www-form-urlencoded

scope={SCOPE_VALUES}
```

The response will be:

```
{
  "access_token": "token",
  "expires_in": 1800
}
```

Please note that in step 6, the Host header should be either `sandbox.api.otto.market` or `api.otto.market`. Additionally, the Authorization header should include the value `Bearer {access_token}` obtained in step 5.

You can now use this installation access token to authenticate your requests when accessing OTTO Market APIs. Include the access token in the Authorization header with the value Bearer {access_token} for subsequent API calls. Please note that once the access token expires, repeat steps 5 and 6 to obtain a new access token and installation access token respectively. Use the updated tokens for continued access to OTTO Market APIs.