Track and Trace (DHL Supply Chain)

v 1.2.2

Division: DHL Supply Chain

Best for:

- Providing access to the **Transport Order information** at any time
- Customer-centric **contract logistics** solutions
- **Business customers** of **DHL Supply Chain**

Region: Global
Used for: Tracking

Overview

The Track & Trace API comes in two versions that enables you to use services to access Order information provided by DHL Supply Chain in the MySupplyChain Track & Trace visibility solution (previously called Connected View).

Track and Trace - Transport Orders Only

- This is a request to receive ONLY Transport Orders matching a key and country.

Track and Trace - All Orders Types

- This API has two calls, the first returns a list of orders matching the key and country. A second API is then called with a unique reference to return the order details.

The order types available are Purchase Order, Customer Order, Warehouse Order and Transport Order.

Documents and POD documents

- This API has two calls, the first returns documents and POD documents. A second API is then called with a document identifier to return the Document or POD document details.

Scope

These versions of the APIs can return all Order types or just Transport Order data (shipments) and Documents or POD documents with detail.

The type of information available through the public API is the same as the one users can find on the MySupplyChain Track & Trace public web search without logging in.

Using the API

The **Transport Orders Only API** takes only 3 key parameters and is easy to setup.

All that is needed is a Transport order reference and a country code for where the order originates. The final parameter is a period of days in the past to search, this is a maximum of 120 days.

The **All Order Types API** takes only 2 key parameters in the first call. An order reference and a country code are required.

Within the payload returned by this API will be a unique key, "order_id", this must be used as the required parameter for the second API call.

Calling the second API with the "order_id" will return the Order Detail information regardless of the Order type.

The **Document and POD documents API** takes only one key parameter in the first call. An select is required with possibility to choose what to retrieve in response documents, pod_documents or both.

Within the payload returned by this API will be a unique key, "document_identifier", this must be used as the required parameter for the second API call.

Calling the second API with the "documentId" for Documents or "podId" will return the detail for relevant document.

The MySupplyChain Track & Trace public API is a Restful API which uses GET HTTP requests.

Example Use Cases

Find the location of a shipment

You can use the API to help you build a website or application that enables DPDHL customers to see the location of their shipment.

Discover when a shipment will arrive

You can use the API to help you build a website or application that enables DPDHL customers to see when they can expect a delivery.

Get information on shipment Status

Some customers want to be informed of the current status of their request.   Is it "Awaiting Dispatch", "In Transit" or "Delivered". These APIs can provide them with the information regarding shipment Status.   With the "All Order Types" API it is possible to return the status events for Purchase, Customer and Warehouse Orders along with the Transport Order information. For example: have the goods been picked in the warehouse?

Customize my web application language

Customize your web application based on your users' needs. You can use the API to create language-specific web applications, so that customers can track their shipment in their native language.

User Guide

Get Access

To obtain the credentials please contact DHL Supply Chain Representative. You will receive separate credentials for the Sandbox and Production environment.

If you are not a DHL Supply Chain Customer, contact one of our experts here.

Authentication

The API Key and the key secret should be sent as HTTP basic authentication credentials. Also, the API Key has to be sent in an HTTP header named WSAPIKey.

This is the successful response which you will see when successfully authenticated.

```
HTTP Response Status Code 200
```

This is the failed response which you will see in the browser in case of invalid credentials.

```
HTTP Response Status Code 401 Unauthorized
{
```

```
  "error" : "invalid_client",
  "error_description" : "Client authentication failed (e.g.
unknown client, no client authentication included, or
unsupported authentication method).
  The authorization server MAY return an HTTP 401 (Unauthorized)
status code to indicate which HTTP authentication schemes are
supported. "
}
```

Available Authentication Methods

DHL provides access to its APIs via the following mechanisms:

- API Key
- OAuth 2.0
- JWT (JSON Web Token)

Each API will describe its particular access mechanism with regards of how to transmit the authentication within a single request. Credentials to use a certain API can be requested via the DHL Developer Portal.

Resource Owner Password Grant Type

For Mobile and Desktop apps, Single Sign-On for T&T Service supports the Resource Owner Password OAuth 2.0 grant type. This password grant type is for highly trusted apps where resource owners share their credentials directly with the app.
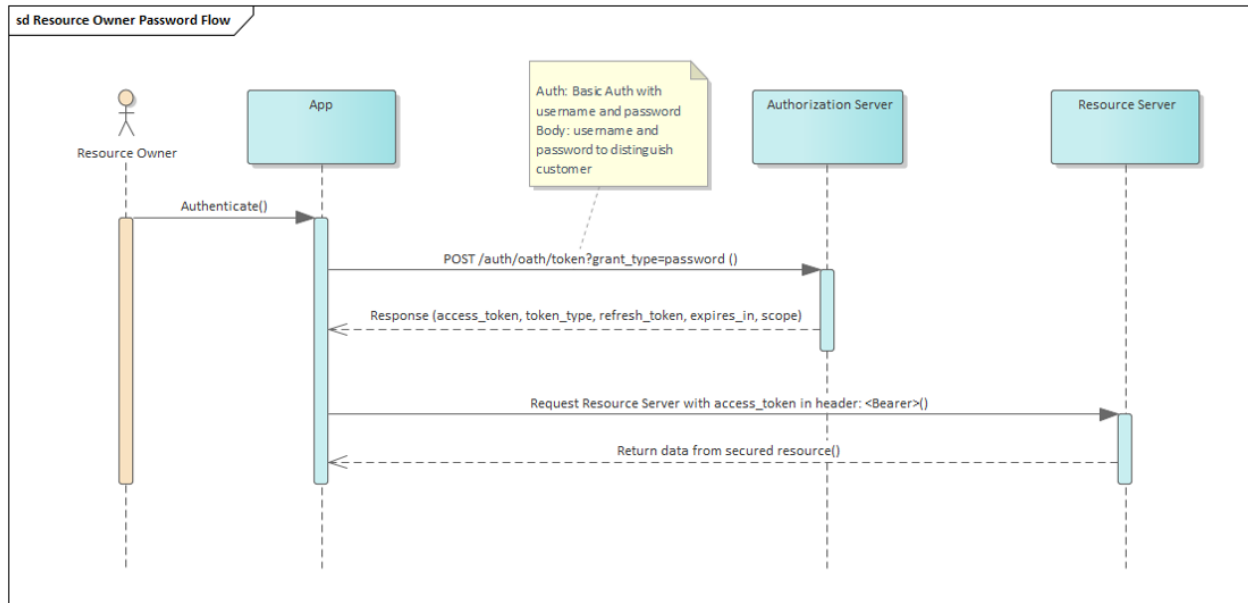
Resource Owner Password Grant Type Roles

The Resource Owner Password grant type uses the following roles:

- **Resource Owner**: A person or system capable of granting access to a protected resource.
- **App**: A client that makes protected requests using the authorization of the resource owner.

- **Authorization Server (T&T)**: The Single Sign-On server that issues access tokens to client apps after successfully authenticating the resource owner.
- **Resource Server (T&T)**: The server that hosts protected resources and accepts and responds to protected resource requests using access tokens. Apps access the server through APIs.

Resource Owner Password Flow

The diagram shows the flow for the Resource Owner Password grant type

The flow of the Resource Owner Password grant type is:

1. **Authenticate**: The user authenticates with the app using their username and password.
2. **POST /auth/oauth/token?grant_type=password**: The app sends the username and password in Auth section (common technical user for all API calls but different per environment) and username and password in request body (different per customer) to the authorization server for validation.
3. **Response (access_token, token_type, refresh_token, expires_in, scope)**: The authorization server validates the username and password and response an access token, token_type, refresh_token, expires_in and scope.

4. **Request resource server:** The app attempts to access the resource from the resource server by presenting the access token (instead of access token has to be used refresh token if access token expires).
5. **Return Resource**: If the access token is valid, the resource server returns the resources that the user authorized the app to receive.

Access Token

An OAuth Access Token is a string that the OAuth client uses to make requests to the resource server.

Access tokens may be either "bearer tokens" or "sender-constrained" tokens. Sender-constrained tokens require the OAuth client to prove possession of a private key in some way in order to use the access token, such that the access token by itself would not be usable.

JSON Web Token (JWT) access tokens conform to the JWT standard and contain information about an entity in the form of claims. They are self-contained therefore it is not necessary for the recipient to call a server to validate the token.

Access tokens issued for the Management API and access tokens issued for any custom API that you have registered with Auth0 follow the JWT standard, which means that their basic structure conforms to the typical JWT structure, and they contain standard JWT claims asserted about the token itself.

Refresh Token

An OAuth Access Token is a string that the OAuth client uses to make requests to the resource server.

Environments

The addressable API base URL/URI environments are:

Environment	Description

https://api-uat.dhl.com

Q&A Environment

https://api-sandbox.dhl.com

https://api.dhl.com

Production environment

Rate limits

Rate limits protect the DHL infrastructure from suspicious requests that exceed defined thresholds.

When the limit is reached, you will receive an HTTP Status code:

```
429: Too many requests.
```

Please contact api.dsc@dhl.com to get more information about it.

Additional Information

There is a rate card in place for the use of the MySupplyChain Track & Trace API. Please discuss potential commercials with your local MySupplyChain Track & Trace contact prior to API usage.

Example requests

Simple HTTP request example

```
curl -X GET
'https://apidsc-qa.dhl.com/order/v1/conview?num=2019015&c=GB&p=1
20' -H 'WSAPIKey:PasteHere_ConsumerKey'
```

The JSON payload explanations, parameters can be checked in the Reference Docs section.

The following parameters need to be included in the URL for the **Transport Only API**:

Parameter	Description	Examples
num	An order reference to search with	20190115
c	2-letter country code	GB, DE, ES, US, etc.
p	Hard-coded to 120	120

The following parameters need to be included in the URL for the **All Order Types API**:

API Call 1 (allorders):

Parameter	Description	Examples

num	An order reference to search with	20190115
c	2-letter country code	GB, DE, ES, US, etc.

API Call 2 (orderdetails):

Parameter	Description	Examples
order_id	A unique order reference to search with	String

Legal Terms

specifics for the use of Track & Trace (formally CONNECTEDVIEW) (DHL SUPPLY CHAIN) API

In addition to the preceding section, the following terms and conditions apply only to Your usage of data or information received through the Track & Trace (DHL SUPPLY CHAIN) API:

- Data requested and received via the Track and Trace (DHL SUPPLY CHAIN) API, such as estimated delivery date, actual delivery date, transport status, transport history is hereinafter referred to as "Tracking Data".
- Tracking Data is Confidential Information in the meaning of section "Communication" of the General Developer Portal Terms of Use. Other than set forth below You must not reveal and/or provide third parties with the Tracking Data and/or analyze, modify such data in any form and/or derive data/information especially for competitive purposes from it without our prior written consent.
- Tracking Data is provided to You and/or the entity you are authorized to represent (hereinafter "You"/"Your") under the prerequisite, that You retrieved the according housebill number (DHL shipment number) in compliance with the applicable law, especially in the field of data protection and competition law and that You use the Tracking Data solely for Your own or Your customers' legitimate tracking purposes.
- The use and submission of Tracking Data – including submission to any of Your subcontractors – shall always be in compliance with applicable laws and regulations, including – without limitation – data protection laws and competition/antitrust law.
- You shall not combine Tracking Data with advertisement or present it in a way that it could be regarded as advertisement.
- Unless otherwise agreed, You shall delete the Tracking Data (including the transport history) 120 days after the last delivery is completed. DHL Supply Chain shall not be required to provide Tracking Data to You that is 120 days after the last delivery. Should You share Tracking Data with Your Customers "Delivered by Deutsche Post DHL Group" shall be displayed to Your Customers in text (minimum font size 12) at the time it is presented/submitted to them.

Reference Docs

Download API Spec

Track and Trace - DHL Supply Chain

Servers
https://api-sandbox.dhl.com - For Orders Onlyhttps://api-uat.dhl.com - Retrieving POD
Authorize

Track And Trace - Transport Orders Only

Endpoints

GET

`/dsc/dhllink/order/v1/conview`

Get Order Details

Track And Trace - All Orders Types

Endpoints

GET

`/dsc/dhllink/msctt/v1/allorders`

Get Orders

GET

`/dsc/dhllink/msctt/v1/orderdetails`

Get Order Details

OAuth

Endpoints

POST

`/dsc-mysctt/oauth/token`

Get an authentication token

Documents And POD Documents

Endpoints

POST

`/dsc-mysctt/orders`

orders

POD Documents

Endpoints

GET

`/dsc-mysctt/pod/{podId}/content`

getPodContent

Documents

Endpoints

GET

`/dsc-mysctt/documents/{documentId}`

getDocument