NIBE Uplink™{api}

Authentication Examples

Example: Authorization Code Grant

The Authorization Code Grant takes place in 4 steps as outlined below. Before starting to authenticate you need to have registered your application and received a client id and secret.

1. Redirect the user's browser to the OAuth2 authorization page.

Redirect the user's browser to the address outlined below. Make sure to exchange the [CLIENT_ID], [SCOPES] and [REDIRECT_URI] with the correct values for your application.

```
https://api.nibeuplink.com/oauth/authorize?response_type=code&client_id=[CLIENT_ID]&scope=
[SCOPES]&redirect_uri=[REDIRECT_URI]&state=[STATE]
```

2. The user authorizes your application.

The user will now be prompted with a login form (if not already logged in) and the question whether they would like to give your application access to their data.

3. The user is redirected to your application with authorization data.

When the user has authorized your application he/she will be redirected back to the redirect_uri you specified to the authorize endpoint with the data you need to gain access to the account. Always check that the state parameter returned is equal to the one supplied to the authorization endpoint.

```
[REDIRECT_URI]?code=[AUTHORIZATION_CODE]&state=[STATE]
```

4. Your application uses this authorization data to gain access to the account.

Using the data you received in the last step you can call the token endpoint and get an access token and a refresh token that can be used in the following communication.

```
POST /oauth/token HTTP/1.1
Host: api.nibeuplink.com
Content-Type: application/x-www-form-urlencoded;charset=UTF-8


grant_type=authorization_code&client_id=[CLIENT_ID]&client_secret=[CLIENT_SECRET]&code=
[AUTHORIZATION_CODE]&redirect_uri=[REDIRECT_URI]&scope=[SCOPES]


HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache


{
   "access_token":[ACCESS_TOKEN],
   "expires_in":300,
   "refresh_token":[REFRESH_TOKEN],
   "scope":[SCOPES],
   "token_type":"bearer"
}
```

5. Authenticate the subsequent requests.

Once the access token has been retrieved it can be used immediately and until the expires_in seconds has passed to access resources in the NIBE Uplink API. To access token needs to be provided as a bearer token to the API endpoints.

```
GET /api/v1/systems HTTP/1.1
Host: api.nibeuplink.com
Authorization: Bearer [ACCESS_TOKEN]
```

Example: Refresh Token

Once the access token has been retrieved it can be used immediately and until the expires_in seconds has passed. After that the access token has to be renewed and this can be done using the refresh_token (only available in the Authorization Code Grant flow). This is done by calling the token endpoint with the refresh token.

```
POST /oauth/token HTTP/1.1
Host: api.nibeuplink.com
Content-Type: application/x-www-form-urlencoded;charset=UTF-8


grant_type=refresh_token&client_id=[CLIENT_ID]&client_secret=[CLIENT_SECRET]&refresh_token=
[REFRESH_TOKEN]


HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache


{
  "access_token":[ACCESS_TOKEN],
  "expires_in":300,
  "refresh_token":[REFRESH_TOKEN],
}
```

Example: Authorization

To authorize your application with any of the API endpoints you need to provide the access token you get from the OAuth token endpoint as a bearer token in the Authorizaton HTTP header.

```
GET /api/v1/systems HTTP/1.1
Host: api.nibeuplink.com
Authorization: Bearer [ACCESS_TOKEN]
```