Authentication and Authorization

This page describes how authentication occurs in UnifiedAPI, explaining what the user must do in order to authorize apps.

- Authentication
- Authenticated user

Authentication

To make requests to UnifiedAPI, you must register an App to a User account. The User must authorize the App to make requests in their name. The process generates an access token that is sent to UnifiedAPI as detailed below.

As Query-Parameters

To use an access token in the query part of the request, you must send the parameter `accessRequestToken`.

Please note that you need to place the word "Bearer" before the token.

The request to list phone calls becomes:

HTTP Request

```
GET /uapi/phoneCalls/userId/extensionNumber/?accessRequestToken=<token>
HOST <hostname>
Content-Type: application/json
Content-Length: xxx
```

As HTTP header

To use an access token in the query part of the request, you must send the *Authorization* header set to the value of the token.

The request to list phone calls becomes:

HTTP Request

```
GET /uapi/phoneCalls/userId/extensionNumber/
HOST <hostname>
Authorization: Bearer <token>
Content-Type: application/json
Content-Length: xxx
```

Authenticated user

UnifiedAPI defines an authenticated User, the User that granted access to the App and is identified by the access token.

Related Topics
VoipNow Apps