twitch.json

misinformation

Page ID: 87

Source: https://dev.twitch.tv/docs/extensions/frontend-api-usage/

['authentic']

Using the Twitch API in an Extension Front End | Twitch Developers Asset 20 Products Showcase Support Blog Docs Tutorials Log in with Twitch Contents Overview Twitch API EventSub Chat & Chatbots Authentication Organizations Drops Embedding Twitch Extensions Get started Required Technical Background Designing Extensions Building Extensions Using the Twitch API in an Extension Front End Making a Twitch API Request Rate limits Response Codes Life Cycle Management Monetization A/B Testing Using Google Analytics Increase Feedback Load Testing Extensions Submission Best Practices Guidelines & Policies Reference Insights & Analytics Mobile Deep Links PubSub Video Broadcast Twitch CLI Changelog Product Lifecycle Using the Twitch API in an Extension Front End Twitch API support for front-end Extensions is available through the Extension helper .

A JWT token is provided in the authorization context, which can be used to authorize calls to Twitch API endpoints in place of app and user access tokens.

This “Helix JWT” is unique to each Extension viewer and is managed by Twitch with no action required from the developer.

Extension front ends can gain access to tokens, including this one specifically for Twitch API requests, with onAuthorized .

window .

Twitch .

ext .

['authentic']

onAuthorized ( function ( auth ) { console .

log ( 'The Helix JWT is ' , auth .

helixToken ); })

; Twitch API endpoints that support user access tokens and do not require scopes are accessible with this JWT (e.g. Get Streams, Get Users).

Endpoints that require scopes or do not support user access tokens are not available with this JWT (e.g. Update Channel Stream Schedule, Get EventSub Subscriptions).

Making a Twitch API Request In general, the Twitch API uses the Bearer authentication scheme with app access tokens and user OAuth tokens.

In order to support Extension front ends, the Twitch API also accepts an Extension authorization scheme that expects the provided Helix JWT.

See the example below that uses Extension instead of Bearer .

curl GET 'https://api.twitch.tv/helix/streams?first=10' \ -H 'client-id: gx2pv4208cff0ig9ou7nk3riccffxt' \ -H 'Authorization: Extension eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJvcGFxdWVfdXNlcl9pZCI6IlUzU3dqRWFWaHYyRnNybFRKYU5UMiIsImNsaWVudF9pZCI6Im9hZm43dnZ6Znl6eWNjd3J3cnQyMzMyMjFvZTV3cSIsImNyZWF0ZWRfYXQiOjE2MjM4ODc0NTl9.HsrA3qdzlP1W2M170cH6C1ufa8MiRIBxkAbhw72XlpI' Rate limits Helix JWTs have separate limits from the usual rate limits .

A rate limit of 30 requests per minute per Extension viewer is available.

If this limit is exceeded, an error is returned (HTTP 429 Too many requests).

This rate limit applies across all Twitch APIs that are accessible by the token.