Getting Started REST API

Version: v4

REST API

NextAuth.js exposes a REST API that is used by the NextAuth.js client.

`GET` /api/auth/signin

Displays the built-in/unbranded sign-in page.

`POST` /api/auth/signin/:provider

Starts a provider-specific sign-in flow.

The POST submission requires CSRF token from `/api/auth/csrf`.

In case of an OAuth provider, calling this endpoint will initiate the Authorization Request to your Identity Provider. Learn more about this in the OAuth specification.

In case of using the Email provider, calling this endpoint will send a sign-in URL to the user's e-mail address.

This endpoint is also used by the `signIn` method internally.

`GET`/`POST` /api/auth/callback/:provider

Handles returning requests from OAuth services during sign-in.

For OAuth 2.0 providers that support the `checks: ["state"]` option, the state parameter is checked against the one that was generated when the sign in flow was started - this uses a hash of the CSRF token which MUST match for both the `POST` and `GET` calls during sign-in.

Learn more about this in the OAuth specification.

`GET` /api/auth/signout

Displays the built-in/unbranded sign out page.

`POST` /api/auth/signout

Handles signing the user out - this is a `POST` submission to prevent malicious links from triggering signing a user out without their consent. The user session will be invalidated/removed from the cookie/database, depending on the flow you chose to store sessions.

The `POST` submission requires CSRF token from `/api/auth/csrf`.

This endpoint is also used by the `signOut` method internally.

`GET` /api/auth/session

Returns client-safe session object - or an empty object if there is no session.

The contents of the session object that is returned are configurable with the `session` callback.

`GET` /api/auth/csrf

Returns object containing CSRF token. In NextAuth.js, CSRF protection is present on all authentication routes. It uses the "double submit cookie method", which uses a signed HttpOnly, host-only cookie.

The CSRF token returned by this endpoint must be passed as form variable named `csrfToken` in all `POST` submissions to any API endpoint.

`GET` /api/auth/providers

Returns a list of configured OAuth services and details (e.g. sign in and callback URLs) for each service.

It is useful to dynamically generate custom sign up pages and to check what callback URLs are configured for each OAuth provider that is configured.

> ⓘ **NOTE**
>
> The default base path is `/api/auth` but it is configurable by specifying a custom path in `NEXTAUTH_URL`

> e.g.
>
> `NEXTAUTH_URL=https://example.com/myapp/api/authentication`
>
> `/api/auth/signin` -> `/myapp/api/authentication/signin`

Edit this page

Last updated on ***May 16, 2024*** *by* ***Codie Newark***