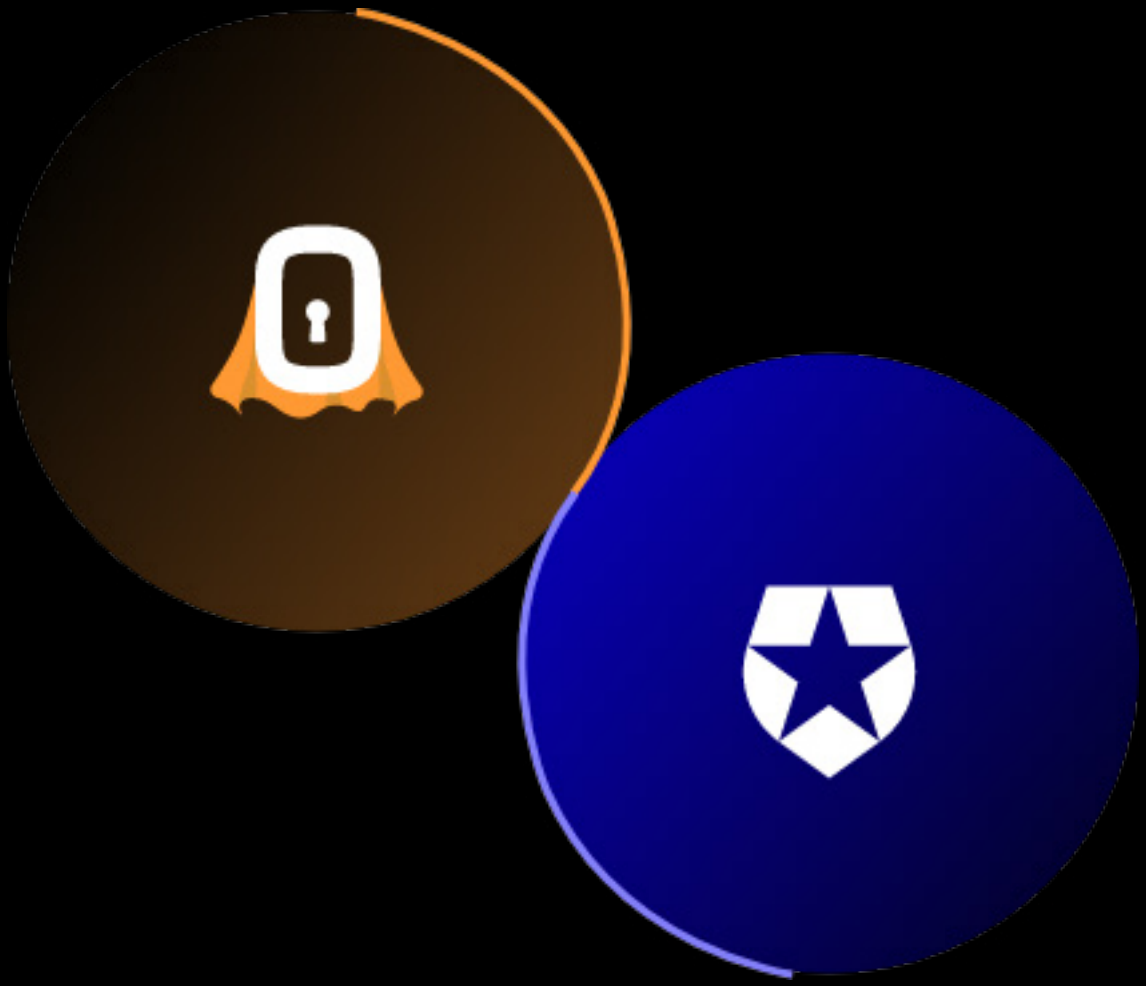

SUPERTOKENS VS AUTH0

Table of Contents

16. If you want to add a password strength meter to registration, how does it work?

17. If a session expires is there a pop-up? Does the user have to handle it?

18.RBAC, check properly, how to get the role of the user within the API for custom logic for both frontend and backend.

19. Is there a mechanism for protecting routes (similar to the supertokens auth wrapper). How easy is it to protect multiple pages and what does the code look like?

20. Email is not verified but password reset is done, does that verify email?

21. How well do they support various platforms and SDKs?

22. How to disallow sign up and only have sign in?

23. Changing Email for social provider, how it works?

01 Describe the dev setup experience (how many steps and what are they + time overall)

Auth0

Basic setup for Frontend

- After signing the getting started page lists how you can configure Auth0 and set it up in your app
- These steps are
  - Previewing and Customizing the Auth screen
  - Integrating auth0 into your app
  - Adding social providers
  - Integrating auth0 into your app
- The integrating auth0 with your app guide is as follows
  - Create an app from their dashboard, it can be of the following types
  - Native apps
  - SPA
  - Regular web apps
  - CLI Apps
- For the React app setup was fast and straightforward
- When creating my application on the dashboard it asks you to choose the type of app. For SPA the options were
  - Angular
  - React
  - JavaScript
  - Vue

- The react guide gives you a sample demo and a step by step process of integrating auth0 with your frontend
- We were able to set up Auth0 add login, logout, and profile functionality to our frontend within 15-20 mins
- The process requires you to add an auth0 provided wrapper around your root in your react app
- You can then use the auth0 useAuth0 hook in your components to get functions to check if the user is authenticated, login, logout, get user information etc...

Basic Setup for backend

- Auth0 provides a guide for setting up your backend
- Installing the express-jwt and jwks-rsa dependencies
- After configuration, the above-mentioned libraries will be used as middleware for express and will check if the jwt exists in the incoming request and it has the correct params.
- The routes you choose to protect can be customized by adding the unprotected routes to a list.

SuperTokens

- See video here

- **FRONTEND**
  - Install frontend SDK
  - Call the init function
  - Add routing handler
  - Add session interceptor (if using axios)

- **BACKEND**
  - Install backend SDK
  - Call the init function
  - Add middleware and error handler
- **CORE**
  - If managed service
    1. Sign up
    2. Select region
    3. Use instance
  - If self hosted
    1. Download docker image / zip binary
    2. Install binary (if used that)
    3. Run the core

Connect core to your db

02 Can you easily add a custom social provider?

Auth0

Auth0 allows you to easily add custom oauth service providers through their dashboard. The setup form asks you to enter the authorization URL, token URL, scope, client id, client secret and a fetch user profile script(queries the OAuth2 API with the accessToken).

SuperTokens

Yes. We support any OAuth 2.0 provider: See docs. All the code required to add a custom provider + extract profile info from their payload is within your own back-end SDK, as a simple callback function.

03 How to go about sending emails yourself if you want to?

Auth0

Auth0's inbuilt test smtp mail server cannot be used in production and requires the user to setup smtp.

- In the dashboard users can select from a list of supported smtp providers.
- These are
  - Amazon SES
  - Mandrill
  - SendGrid
  - SparkPost
  - Mailgun
- Auth0 allows you to set a custom email provider and set the requires smtp provider settings
- Added my zoho mail credentials

SuperTokens

We have callback functions for sending email, which you can use to send custom designed emails using whichever method you want.

04 How to implement sign out functionality?

Auth0

The useAuth0 hook provides a logout function. The function redirects the user to auth0's logout endpoint before redirecting back to the app. This will clear the auth0 sso cookies. It can be configured to even logout the user from the identity provider they logged in from(ex. if user used google to log into auth0, the logout will logout them out from both the app and google)

SuperTokens

The API for sign out is automatically exposed via our backend SDK. You have to use the signOut function exposed by the frontend SDK and you are done.

05 How to go about customising the email design and or the sender's domain?

Auth0

Auth0 allows for complete customization of all emails(Welcome, password reset, email verification, change password etc...). The sender's domain, Subject and message contents can be completely changed from the dashboard. The message HTML can be completely changed

SuperTokens

We have callback functions for sending email, which you can use to send custom designed emails using whichever method you want.

06 How would adding custom sign up validators work?

Auth0

Auth0 allows you to add custom sign up fields,

- In the dashboard navigate to the branding/Universal Login section
- The dashboard allows you to customize the HTML of the login
- In the script section the config's `additionalSignUpFields` attribute is used to add additional fields.

  - The additional SignUpFields attribute takes the following params
- name: string
- placeholder: string
- validator: function

There are also a number of additional params that can be set like a logo can be set using the icon param, also the type of input can be modified.

The custom field type can be modified using the type param

ex.

- The custom field type can be modified using the `type` param
- When the type param is set to select, you can provide users with a number of options ex. `additionalSignUpFields: [{ type: "select", name: "location", placeholder: "choose your location", options: [{value: "us", label: "United States"}, {value: "fr", label: "France"}, {value: "ar", label: "Argentina"}], // The following properties are optional icon: "https://example.com/assests/location_icon.png", prefill: "us" }]`

An icon and prefill param can also be set.

Other type options include a checkbox field and a hidden field

SuperTokens

- See docs
- They would need to handle those custom fields themselves post sign up

07 Changing password validation(or some similar feature) for sign up does this get propagated to other places(- Signin, password reset)

Auth0

Auth0 has 3 methods of customizing auth flows

- Rules
- Auth0 hooks
- Auth0 actions

  - Rules

    - Rules are js functions that are executed during user authentication.
    - They run after the main authentication flow is completed, i.e. just before the response is submitted to the user.
    - The ID Token and/or Access Token passed to the Rules pipeline and then sent to the app.
    - Rules can be created from the dashboard, or they can be added through the management api.
    - Uses
      - They can be used for adding more data to the user object
      - Normalizing data
      - Sending notifications that authentication just occured

        - Creating a whitelist
        - Modifying the access token scopes
    - Auth0 hooks
        - Info can be found in question about post sign up callback
    - Actions
- In case of password validation, auth0 has a special place in the dashboard for setting up password strength. This change is propagated through any flow that requires the user to enter the password

SuperTokens

Yes

08 How do we do things like handle sign up success?

Auth0

Auth0 has a number of Extensibility Points, these are places in Auth0's flow where users can define nodejs based scripts that will run. These are called auth0 hooks. The available extensibility points are

- Client Credentials Exchange

You can modify the scopes and add custom claims to the tokens issued by the Auth0 API

- Post change password

  - Executed after a successful user password change

- Post User Registration (Action)

  - Executed after a new user is created

- Pre User Registration (action)

  - Executed before user registration, can prevent user creation or add custom metadata.

- Send Phone Message
- allows you to customize your SMS provider for multifactor authentication.

The Auth0 actions can involve calling your API endpoint if you want to add user details to your db as well. However, during dev, if your endpoints are on localhost that causes an issue since auth0 cannot call localhost. So you might have to do some tricky tunneling..

SuperTokens

- We have a frontend event that's fired that providers them details of the new user
- We allow users to easily override the backend (their backend) APIs that our SDK adds to handle post sign up like functionality. Within that override, they can call the original implementation so as to not have to implement everything within that API.

09 What if you want to embed the sign up / in page into your website UI (As opposed to opening a new tab..). Is that possible?

Auth0

Auth0 allows you to embed login into your website. They allow to use their login widget SDK in your app or just use the Auth0 SDK to query the auth endpoints.

SuperTokens

Yes. It is possible. See this as an example.

10 If one needs to do something like paginating across all users in the app in their API, how can they do that?

Auth0

- Auth0 provides an API for querying user information. It provides a number of options to filter data. The API takes attributes like page (index of the results to return), per page(the number of results per page)...
- Sample response: [{ “user_id”: “auth0|507f1f77bcf86cd799439020”, “email”: “john.doe@gmail.com”, “email_verified”: false, “username”: “johndoe”, “phone_number”: “+199999999999999”, “phone_verified”: false, “created_at”: “”, “updated_at”: “”, “identities”: [{ “connection”: “Initial-Connection”, “user_id”: “507f1f77bcf86cd799439020”, “provider”: “auth0”, “isSocial”: false }], “app_metadata”: {}, “user_metadata”: {}, “picture”: “”, “name”: “”, “nickname”: “”, “multifactor”: [“”], “last_ip”: “”, “last_login”: “”, “logins_count”: 0, “blocked”: false, “given_name”: “”, “family_name”: “” }]

SuperTokens

- Our SDK has functions for that.
- We also allow devs to export all users as CSV from our dashboard

11 Will their solution work with serverless env like in nextjs or netlify?

Auth0

Auth0 provides a nextjs sdk.

The setup is as follows:

- Create a auth0 app from the dashboard
- add the configuration keys to your next app, in .env.local
- Add an api route handler to your next app with handleAuth from the auth0 next package
- this will add the routes for login, logout and callback URLs.
- wrap pages/_app.js with the UserProvider component to get the user details on the frontend

SuperTokens

Yes

12 Sharing session across sub domains

Auth0

Test:

- Using ngrok to have two domains localhost:3000 and the ngrok domain
- Logged in on localhost
- Switched URL to the ngrok URL
- Got redirected to the login page
- On clicking login was signed in without having to enter details

SuperTokens

Possible by setting the cookieDomain to be `example.com` via our frontend and backend configs.

13 Documentation review

Auth0

Auth0's documentation is really good. Whenever you start an app and choose your techstack, you get a curated quick setup guide taking you through the setup process.

Each section in the dashboard gives information on how that section works.

That being said, a place that can be hard to navigate is the management API docs.

SuperTokens

- It is split into recipes.
- Each recipe doc has all the steps needed to use it from getting started to customisations, to overrides, to integrations with other frameworks like NextJS or AWS lambda or Hasura

14 Email verification with Social providers, how does it work

Auth0

- Email verification is turned on by default.
- Email verification is not enforced by default, user gets access to app immediately on signup.
- To enforce email verification a custom rule has to be created.

SuperTokens

- If the provider gives us that the email is verified already, we mark it as verified in our db
- Else we show the email verification screen to the end user (if it is switched on by the dev).
- If the email changes on the social provider's side, it is marked as unverified again.

15 User has multiple sessions, only want to revoke a couple of them, how does that work

Auth0

Auth0 does not seem to supply methods in their SDK for revoking sessions. From what we have seen, the only way to invalidate the session is to clear the cookies on the frontend and then call revoke the refresh token from the server using Auth0's management API.

SuperTokens

Each session has a unique ID (that we call `sessionHandle`). You can call `revoke-session` with a specific `sessionHandle` in your backend.

16 If you want to add a password strength meter to registration, how does it work?

Auth0

In Auth0's dashboard you can choose to customize he HTML code of the login widget. This allows you to change the config of lock widget to add additional fields, change styling etc. Adding custom elements in their editor does not seem to be something they encourage though.

Auth0 has a password strength meter built into its lock UI. The password policy has a set of rules with a slider to customize how many rules to enforce

This can be modified from the database password policy tab

The rules are :

- No more than 2 identical characters in a row
- Special characters (!@#$%^&*)
- Lower case (a-z), upper case (A-Z) and numbers (0-9)
- Must have '' characters in length
- Non-empty password required

SuperTokens

You can override the specific component that show the password field, and add the password strength meter to it.

17 If a session expires is there a pop-up? Does the user have to handle it?

Auth0

- We tested by setting the id token and refresh token expiration to be very low.
- On expiry there is no pop-up.
- Currently using the `isAuthenticated` function from the `useAuth0` hook to display information. On session expiry this is false.

SuperTokens

As of now, the user has to handle it. But we have open issues for this.

18 RBAC, check properly, how to get the role of the user within the API for custom logic for both frontend and backend.

Auth0

Roles in Auth0 is just a method to group together permissions.

- In Auth0, a permission is the ability to perform an action on a resource. ex. read:data can be defined as a permission.
- After creating a permission, it can then be assigned to a role.
- Roles can then be assigned to a user.
- The role assigned to a user can be found in the accesstoken jwt after authentication under the permission attrubute
- On the backend the 'express-jwt-authz' can be used to create a middleware to check if the user has the required permission
- Roles can be created from the dashboard.
- Roles have a name, description, permissions and users associated with them
- Roles can be created using the Auth0 management API and can be assigned to a user
- Multiple roles can be assigned to a single user

SuperTokens

- Devs can add a role to a session on creation (based on the userID).
- This role can be fetched on the backend (post session verification) and on the frontend.
- Roles can be edited in the session on the backend (post session verification).

19 Is there a mechanism for protecting routes (similar to the supertokens auth wrapper). How easy is it to protect multiple pages and what does the code look like?

Auth0

Auth0 provides a HOC withAuthenticationRequired which can be used for protecting routes.

ex.

Create a component that uses withAuthenticationRequired

```
const ProtectedRoute = ({ component, ...args }) => (
<Route component={withAuthenticationRequired(component)} {...args} />
);
```

in your router set the path and the component to be protected using the new component

```
<ProtectedRoute path="/profile" component={Profile} />
```

SuperTokens

Yes

20 Email is not verified but password reset is done, does that verify email?

Auth0

Email does get verified.

- Tested:
- Signup
- Check that user is unverified
- reset password
- Email associated with the user is now verified.

SuperTokens

No. But this is an open issue at the moment.

21 How well do they support various platforms and SDKs?

Auth0

Auth0 supports the following SDK's with good documentation, quickstarts and sample apps:

- Frontend
  - Angular
  - JavaScript
  - React
  - Vue
- Backend
  - Laravel API
  - Node (Express) API
  - PHP API
  - Python API
  - Ruby On Rails API
- Native and Mobile
  - Android
  - Cordova
  - iOS Swift
  - React Native
  - Windows Universal App C#WPF / Winforms
  - Xamarin

SuperTokens

As of this writing, we have support for NodeJS and react + vanilla JS sessions. One can build their own UI + backend using our APIs (a few days of work), as long as we support sessions for their frontend (as that is really complex for them to build out).

22 How to disallow sign up and only have sign in?

Auth0

In Auth0's dashboard, under the database option, you can choose to disable sign-ups.

SuperTokens

- Can override the backend API to disallow sign up (by throwing an error in that case)
- Can override the frontend component that lets users switch to the sign up view

23 Changing Email for social provider, how it works?

Auth0

According to the forums changing the password for social providers is not supported.

SuperTokens

- Each login will update the email used by the end user in our db. So if the social provider has changed the email, ours will change too.