Authentication in Core Kit SFA Web SDK

Let's look at the general authentication flow at Web3Auth.

When a user logs in with Web3Auth, a user's account can be in two states:

- Account Without MFA
- : When the User logs in with only social login and key is secured by Web3Auth network.
- Account With MFA
- : When the User enables MFA by adding other shares like password, backup share, device share, etc., to their existing account.

warning This SDK only works for users who havenot enabled MFA .

For MFA enabled users, you'll seeError("User has already enabled mfa, please use the Web3Auth PnP Web or Mobile SDKs for login with mfa");

Without Openlogin Redirection Flowâ

By default, to reconstruct key in both states, Web3Auth SDKs redirects the user tohttp://app.openlogin.com . Where all the computation to reconstruct the key is done. The advantage of this approach is that it makes it easy for applications to integrate web3auth SDK without having to worry about the key reconstruction process. But sometimes, applications want to reconstruct the key in their application context, where the authentication flow described can be used with this SDK.

CreateCustom Auth

Verifierâ

Once you click on theCreate Verifier button on Web3Auth Dashboard, you'll see a toggle similar to these, where you can create a custom verifier for your use case.

VisitAuth Provider Setup to learn more about creating custom verifiers.

Filled Custom JWT Verifierâ

note These verifier details will be used in the next step.Edit this page Previous Initialize Next Usage