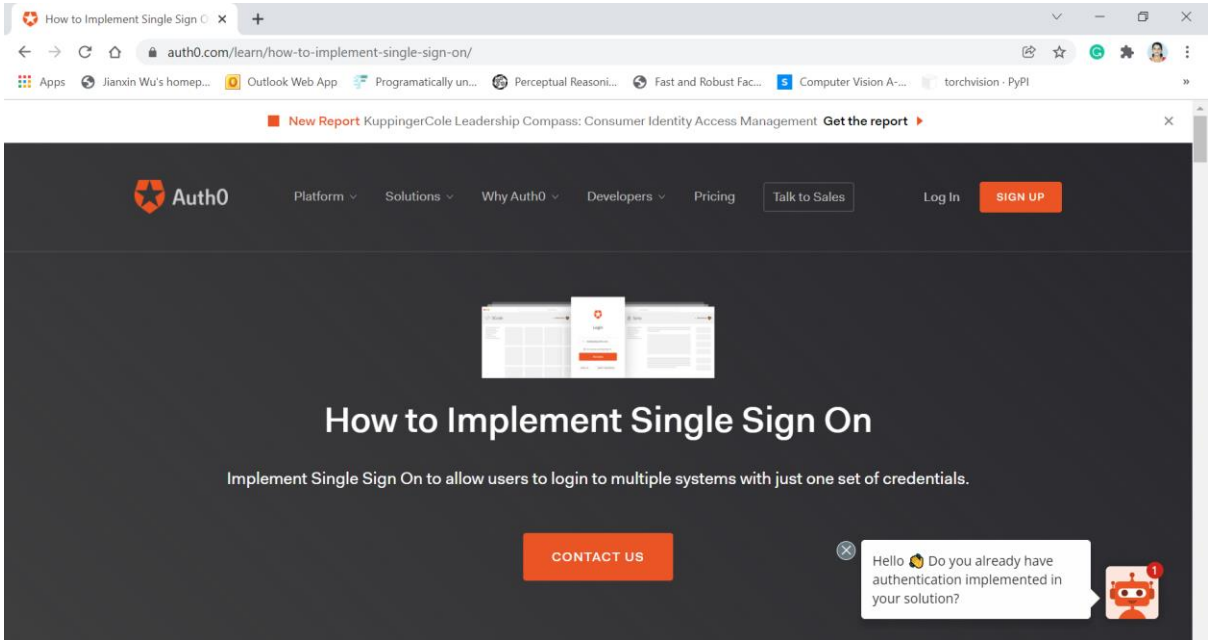
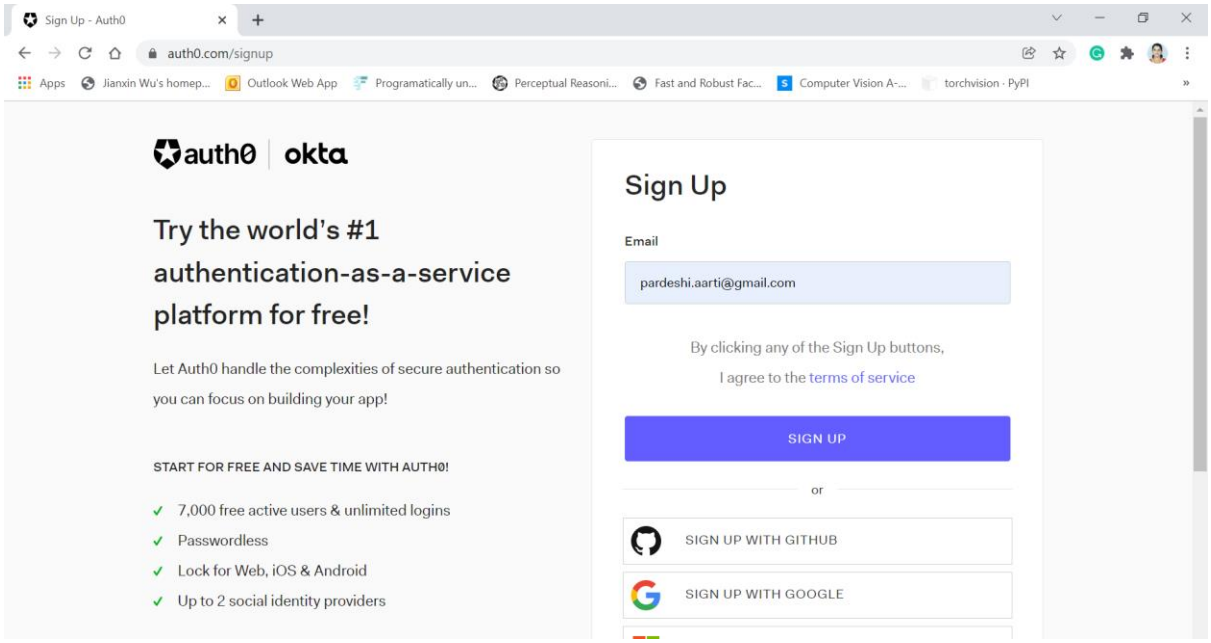
Practical No 8

AIM: Study and Implementation of single-sign-on.

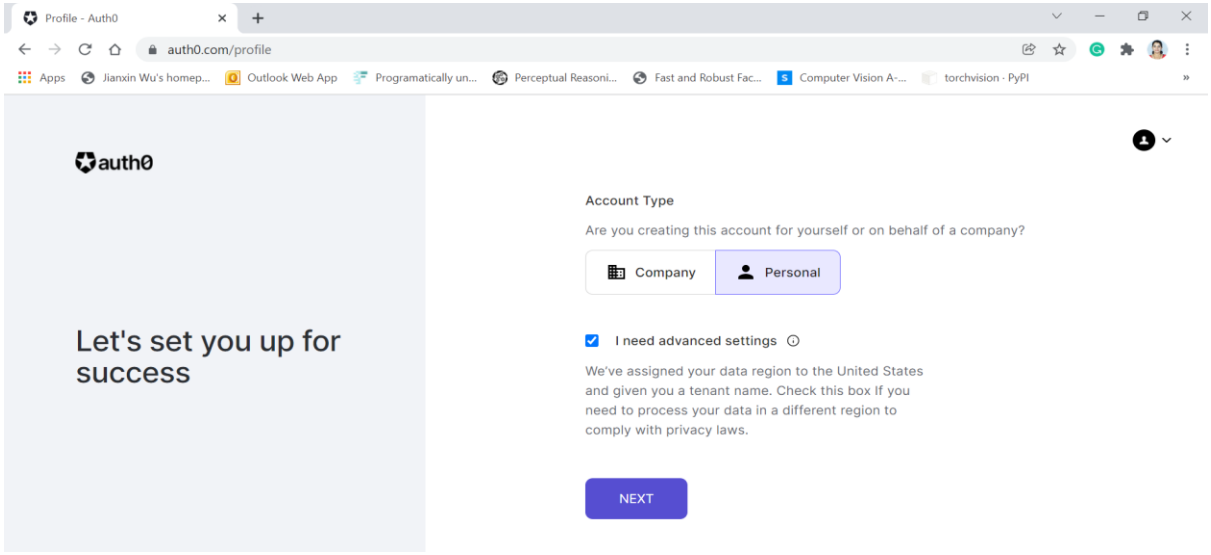
- Go to following links.
  https://auth0.com/learn/how-to-implement-single-sign-on/



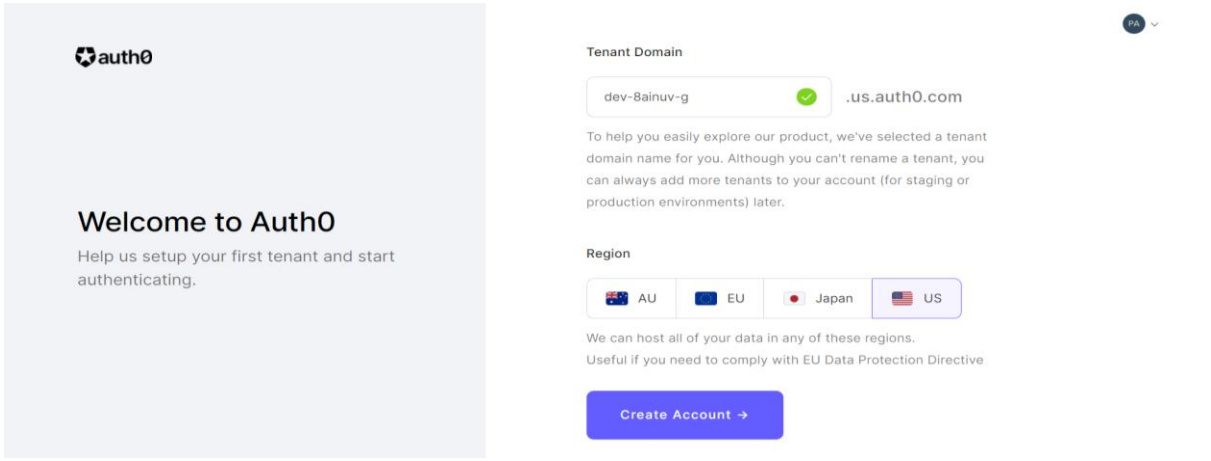
- Enter ID And password for your account and click ok "**SIGN UP**".



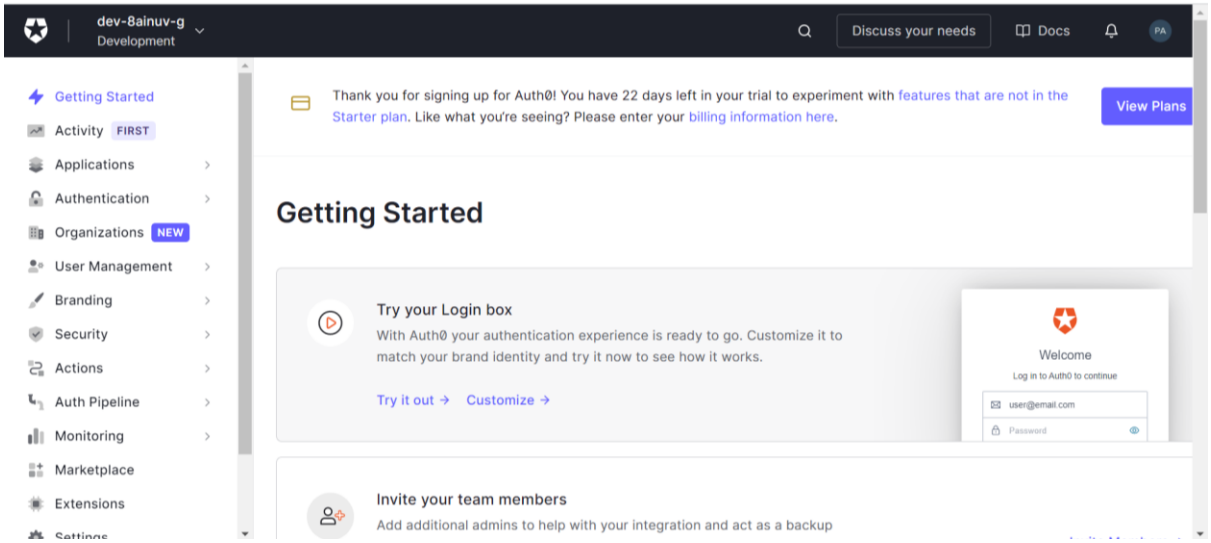
- Choose “Personal” type of account.



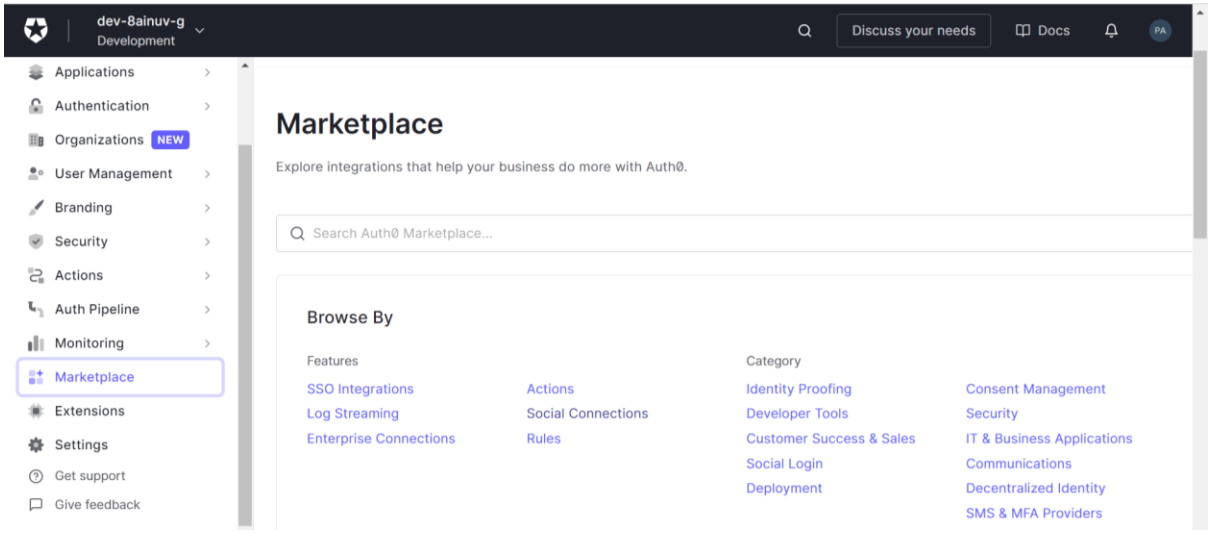
- Now you will get “**TENANT DOMAIN”** And “**REGION**” For your account and click on “**NEXT**”. You won’t be able to edit it. So, keep it as it is. Save it.

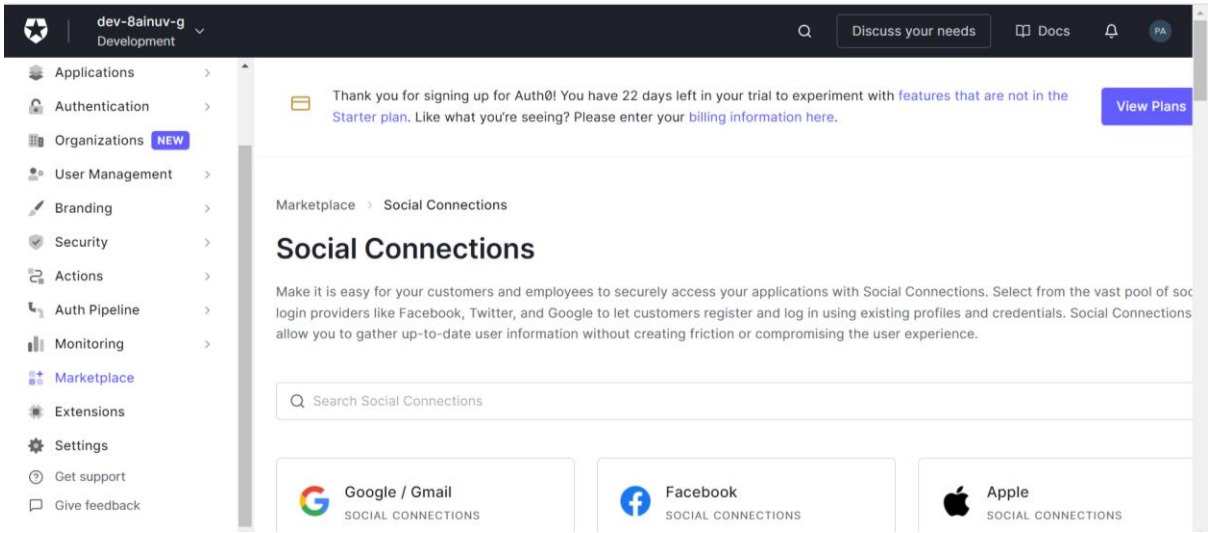


- Click on “Create Account”.

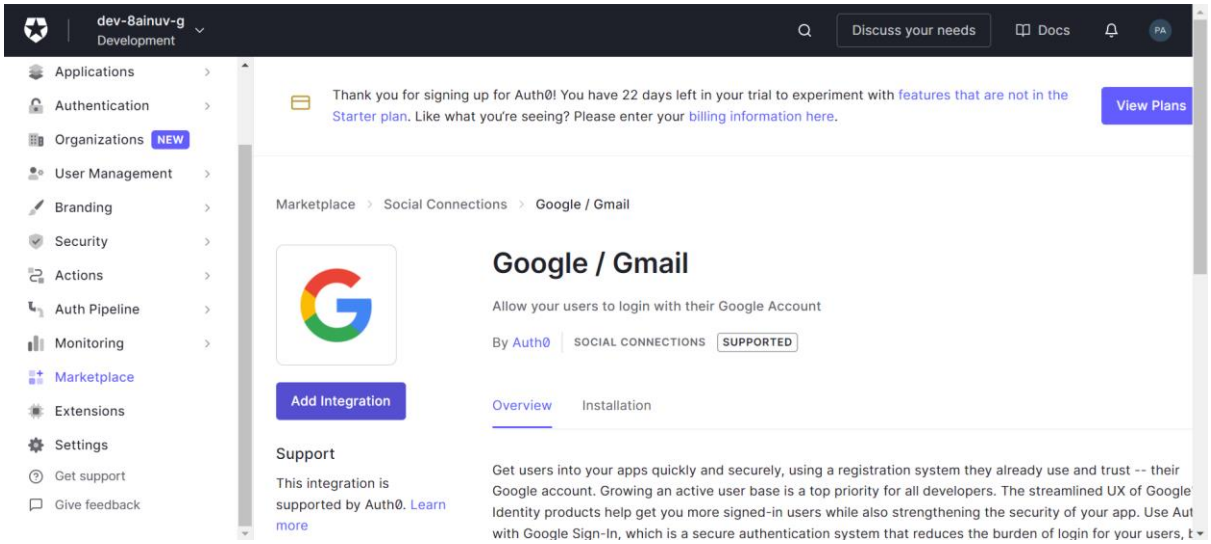


- Click on “Marketplace” from Left Hierarchy. Click on “Social Connection”.

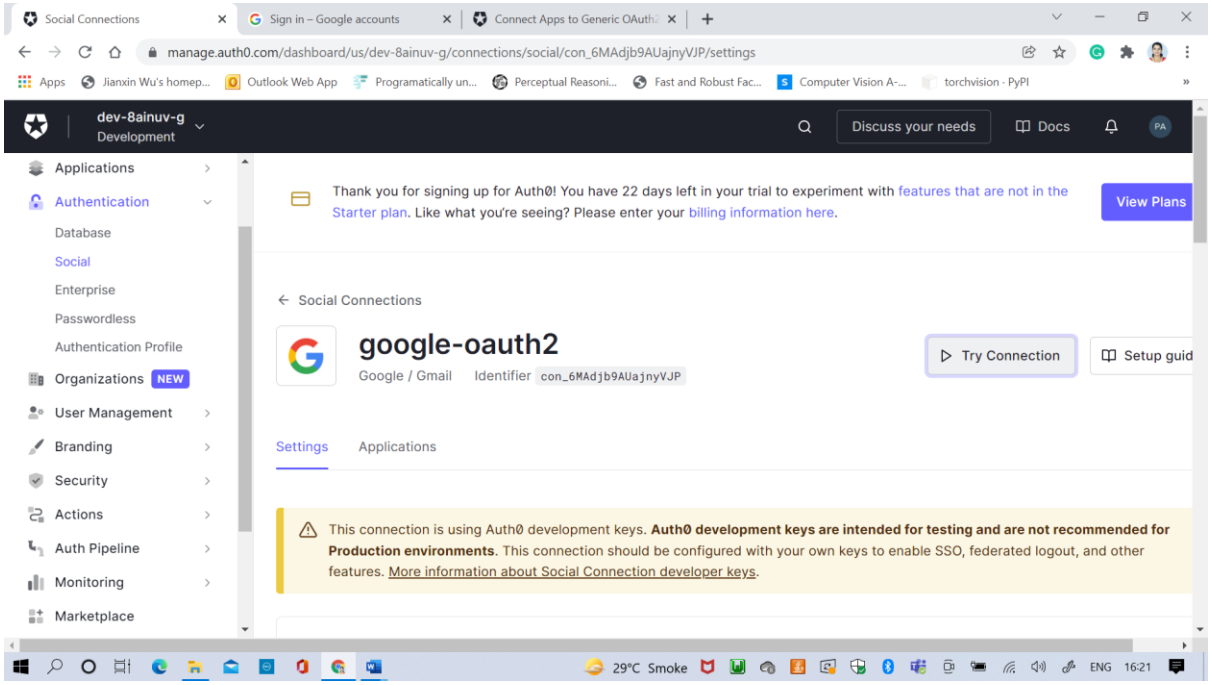




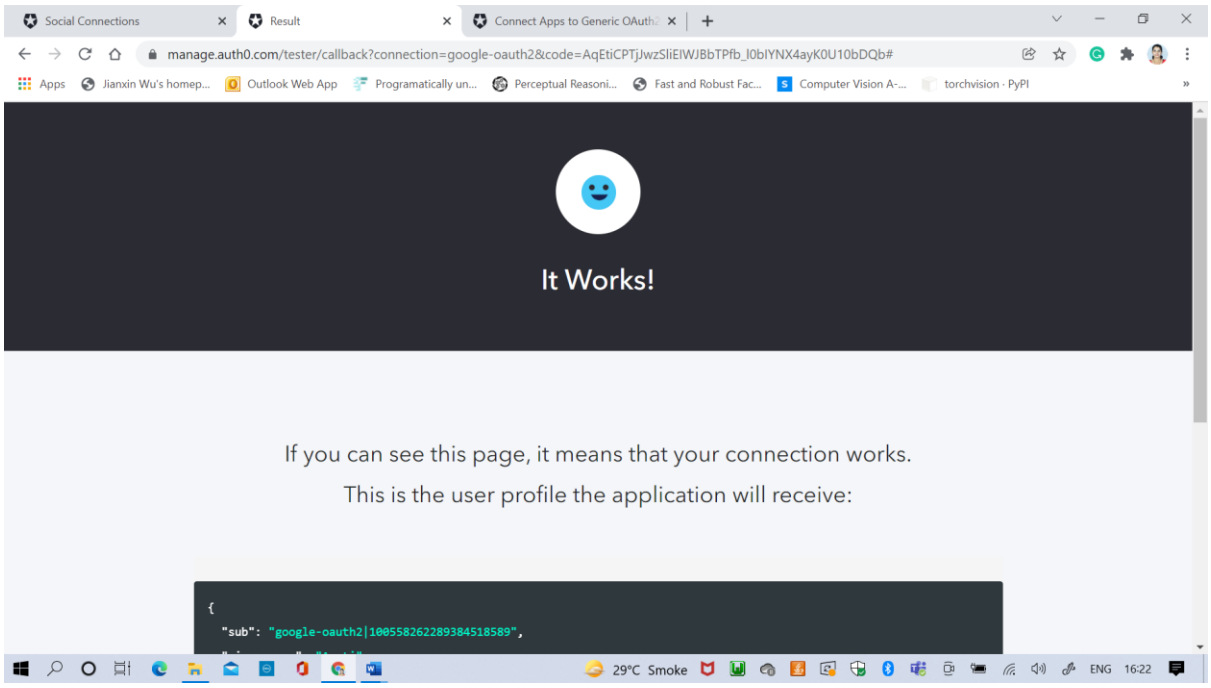
- Click on “Google/Gmail”. Click on “Add Integration”



- Click on “Try Connection”



- If you get the following window. Your practical is complete.



WHAT IS SINGLE-SIGN-ON?

Answer

- Single sign-on (SSO) is an authentication process that allows a user to access multiple applications with one set of login credentials.
- SSO is a common procedure in enterprises, where a client accesses multiple resources connected to a local area network (LAN).
- Single Sign-on (SSO) occurs when a user logs in to one application and is then signed in to other applications automatically, regardless of the platform, technology, or domain the user is using. The user signs in only one time hence the naming of the feature (Single Sign-on).
- Google's implementation of login for their products, such as Gmail, YouTube, Google Analytics, and so on, is an example of SSO.
- Any user that is logged in to one of Google's products are automatically logged in to their other products as well.
- SSO usually makes use of a *Central Service* which orchestrates the single sign-on between multiple applications. In the example of Google, this central service is Google Accounts. When a user first logs in, Google Accounts creates a cookie, which persists with the user as they navigate to other Google-owned services.

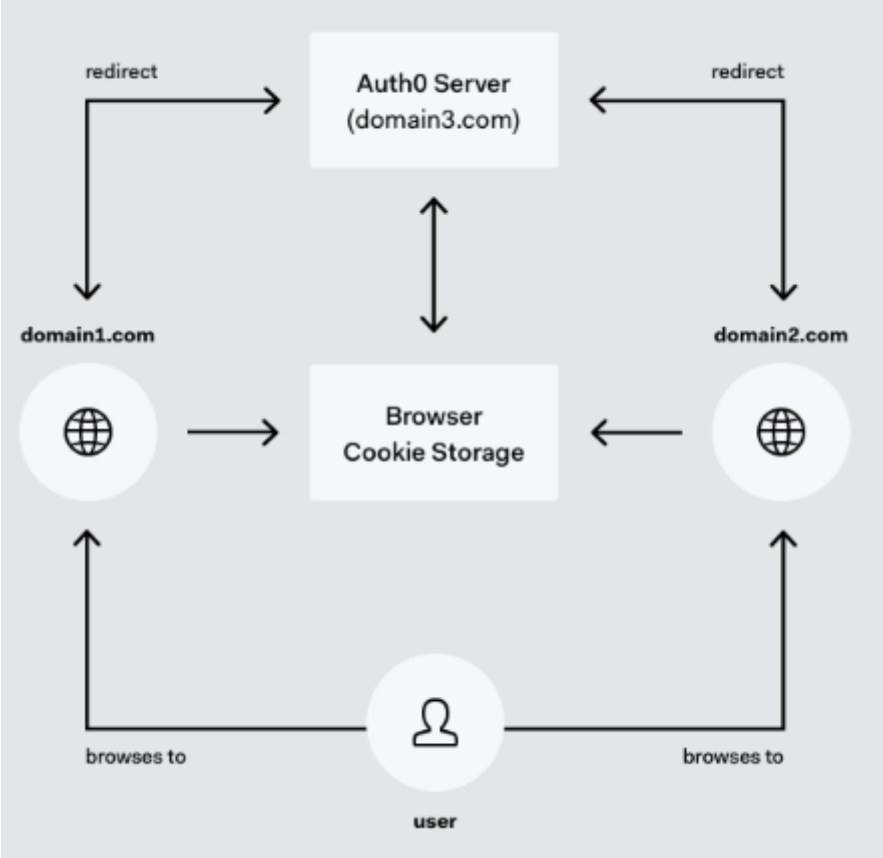
HOW DOES IT SINGLE-SIGN-ON WORKS?

ANSWER-

Authentication with SSO relies on a trust relationship between domains (websites). With single sign-on, this is what happens when you try to log in to an app or website:

- The website first checks to see whether you've already been authenticated by the SSO solution, in which case it gives you access to the site.
- If you haven't, it sends you to the SSO solution to log in.
- You enter the single username/password that you use for corporate access.
- The SSO solution requests authentication from the identity provider or authentication system that your company uses. It verifies your identity and notifies the SSO solution.
- The SSO solution passes authentication data to the website and returns you to that site.

- After login, the site passes authentication verification data with you as you move through the site to verify that you are authenticated each time you go to a new page.
- In SSO, authentication verification data takes the form of tokens.



The website redirects the user to the SSO website to log in. The user logs in with a single username and password. The SSO website verifies the user's identity with an identity provider, such as Active Directory.