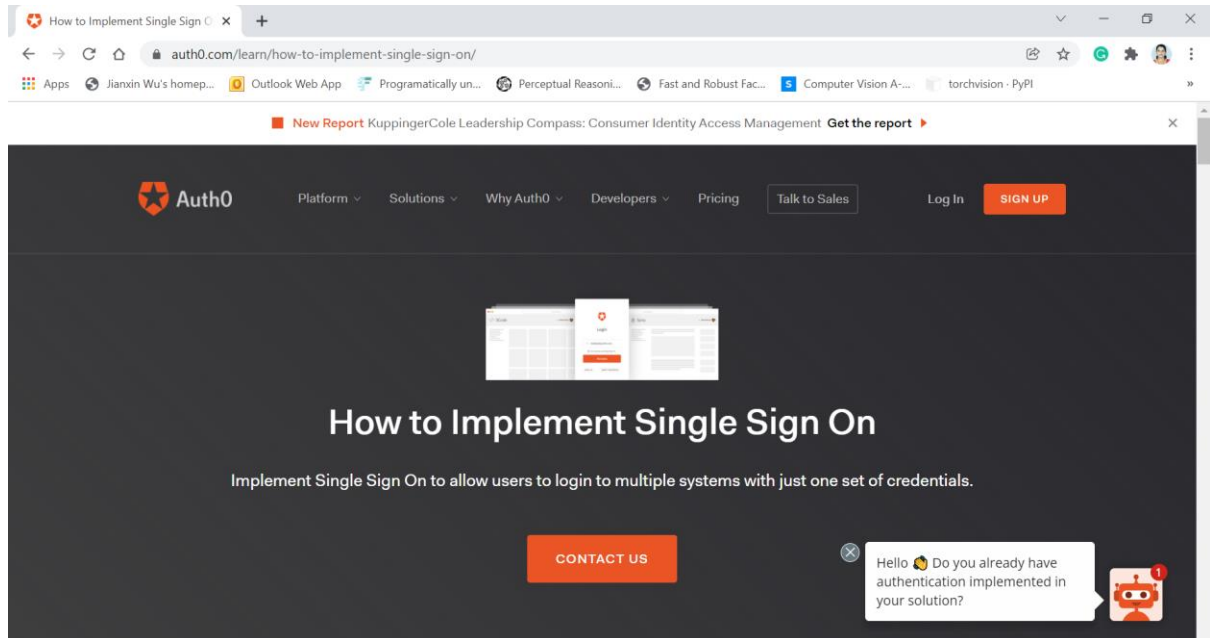


Practical No 8

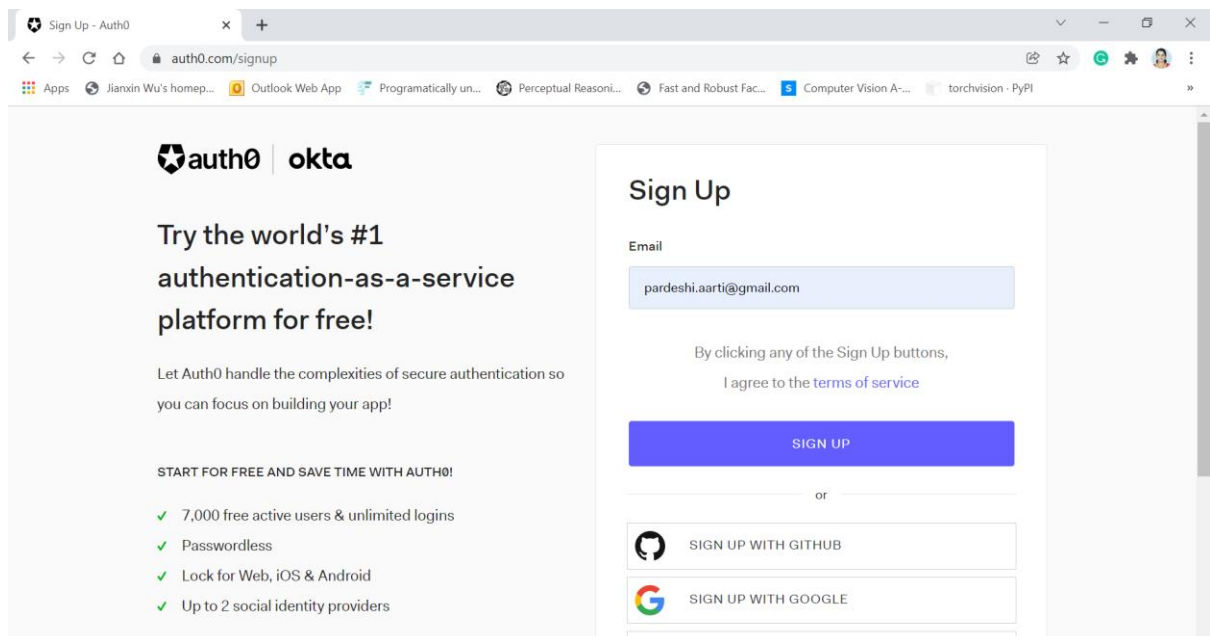
AIM: Study and Implementation of single-sign-on.

➤ 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.

The screenshot shows the Auth0 profile setup page in a web browser. The browser's address bar shows 'auth0.com/profile'. The page has a light blue header with the Auth0 logo and a user profile icon. The main content area is divided into two columns. The left column has a large light blue box with the text 'Let's set you up for success'. The right column is titled 'Account Type' and asks 'Are you creating this account for yourself or on behalf of a company?'. There are two buttons: 'Company' and 'Personal'. The 'Personal' button is selected and highlighted in purple. Below these buttons, there is a checkbox labeled 'I need advanced settings' which is checked. A paragraph of text explains that the data region is assigned to the United States and that the user can check the box if they need to process data in a different region. At the bottom of the right column is a purple button labeled 'NEXT'.

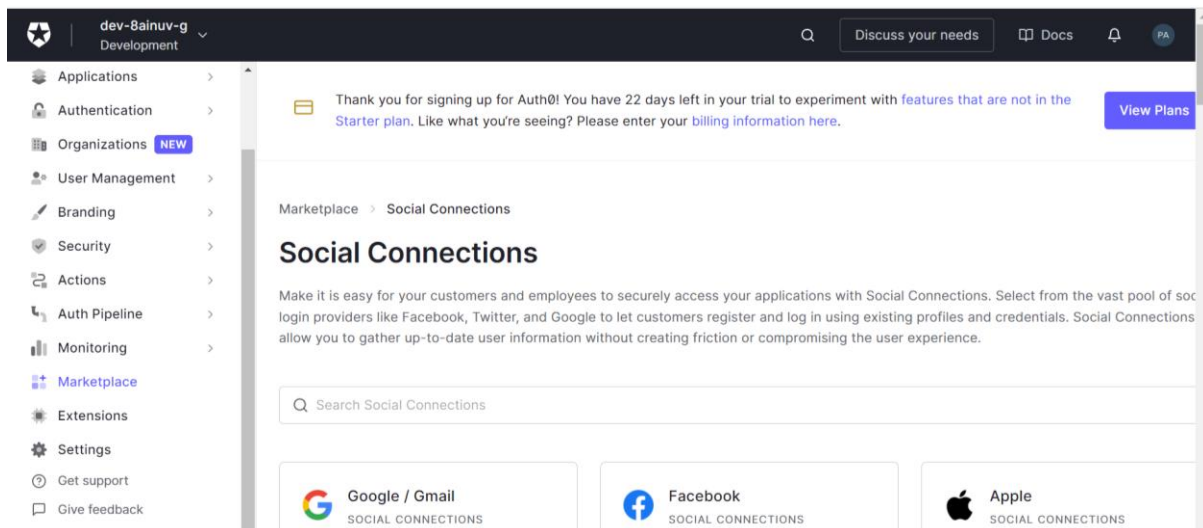
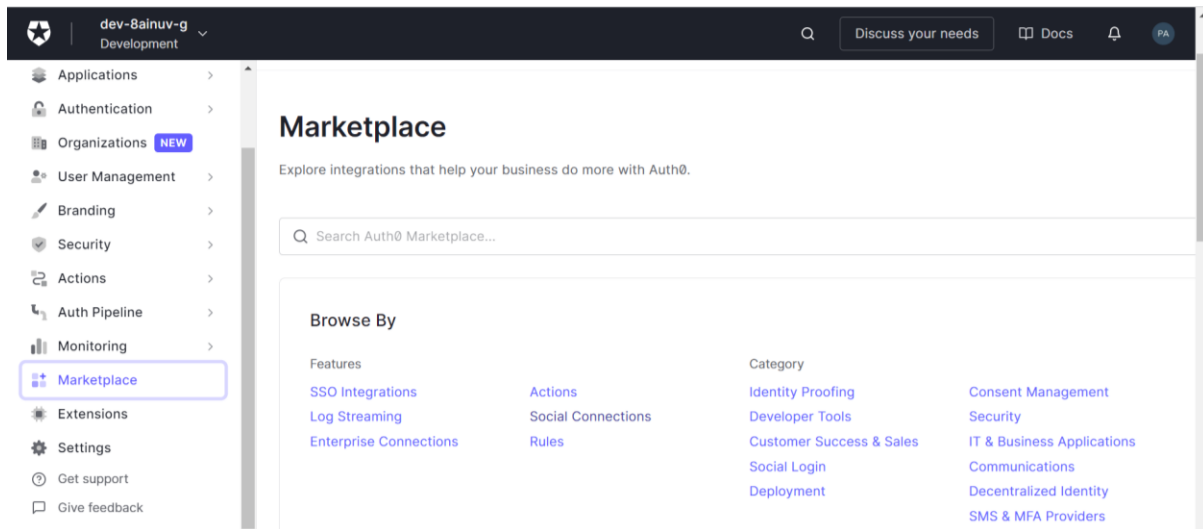
- Now you will get “TENANT DOMAIN” And “REGION” For your account and click on “NEXT”. You won’t be able to edit it. So, keep it as it is. Save it.

The screenshot shows the Auth0 tenant setup page. The browser's address bar shows 'auth0.com/profile'. The page has a light blue header with the Auth0 logo and a user profile icon. The main content area is divided into two columns. The left column has a large light blue box with the text 'Welcome to Auth0' and 'Help us setup your first tenant and start authenticating.'. The right column is titled 'Tenant Domain' and shows a text input field with 'dev-8ainuv-g' and a green checkmark, followed by '.us.auth0.com'. Below this, there is a paragraph of text explaining that a tenant domain name has been selected for the user. The next section is titled 'Region' and shows four buttons: 'AU', 'EU', 'Japan', and 'US'. The 'US' button is selected and highlighted in purple. Below these buttons, there is a paragraph of text explaining that the user can host all of their data in any of these regions. At the bottom of the right column is a purple button labeled 'Create Account →'.

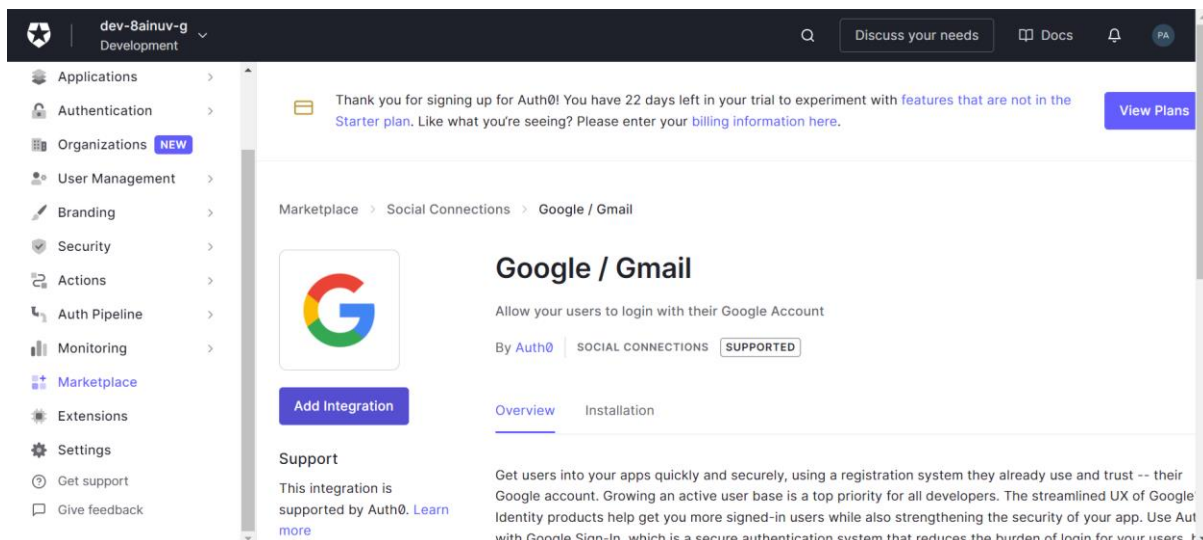
- Click on “Create Account”.

The screenshot shows the Auth0 dashboard. The top navigation bar is dark blue and contains the Auth0 logo, the text 'dev-8ainuv-g Development', a search icon, a button 'Discuss your needs', a 'Docs' icon, a bell icon, and a user profile icon. The left sidebar is dark blue and contains a list of navigation items: 'Getting Started', 'Activity FIRST', 'Applications', 'Authentication', 'Organizations NEW', 'User Management', 'Branding', 'Security', 'Actions', 'Auth Pipeline', 'Monitoring', 'Marketplace', 'Extensions', and 'Settings'. The main content area is white and has a header with a yellow envelope icon and the text 'Thank you for signing up for Auth0! You have 22 days left in your trial to experiment with features that are not in the Starter plan. Like what you're seeing? Please enter your billing information here.' and a purple button 'View Plans'. Below this header is a section titled 'Getting Started'. It contains two cards. The first card is titled 'Try your Login box' and has a play button icon. It contains the text 'With Auth0 your authentication experience is ready to go. Customize it to match your brand identity and try it now to see how it works.' and two links: 'Try it out →' and 'Customize →'. The second card is titled 'Invite your team members' and has a plus icon. It contains the text 'Add additional admins to help with your integration and act as a backup'.

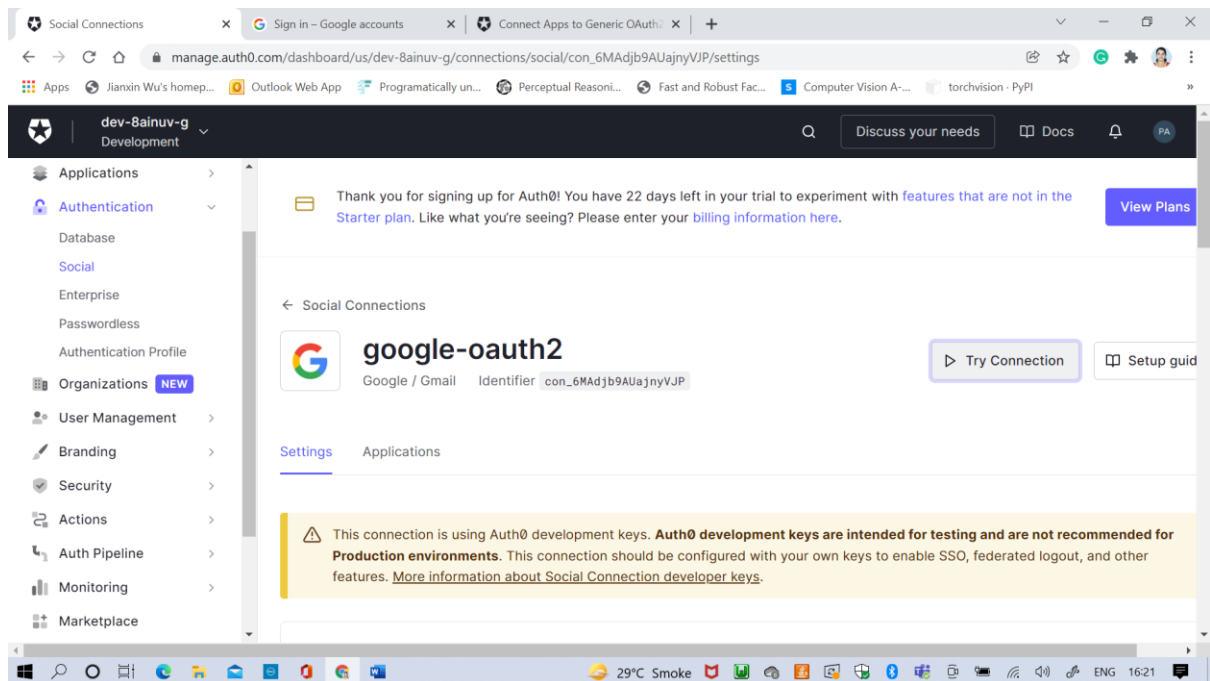
- Click on “Marketplace” from Left Hierarchy. Click on “Social Connection”.



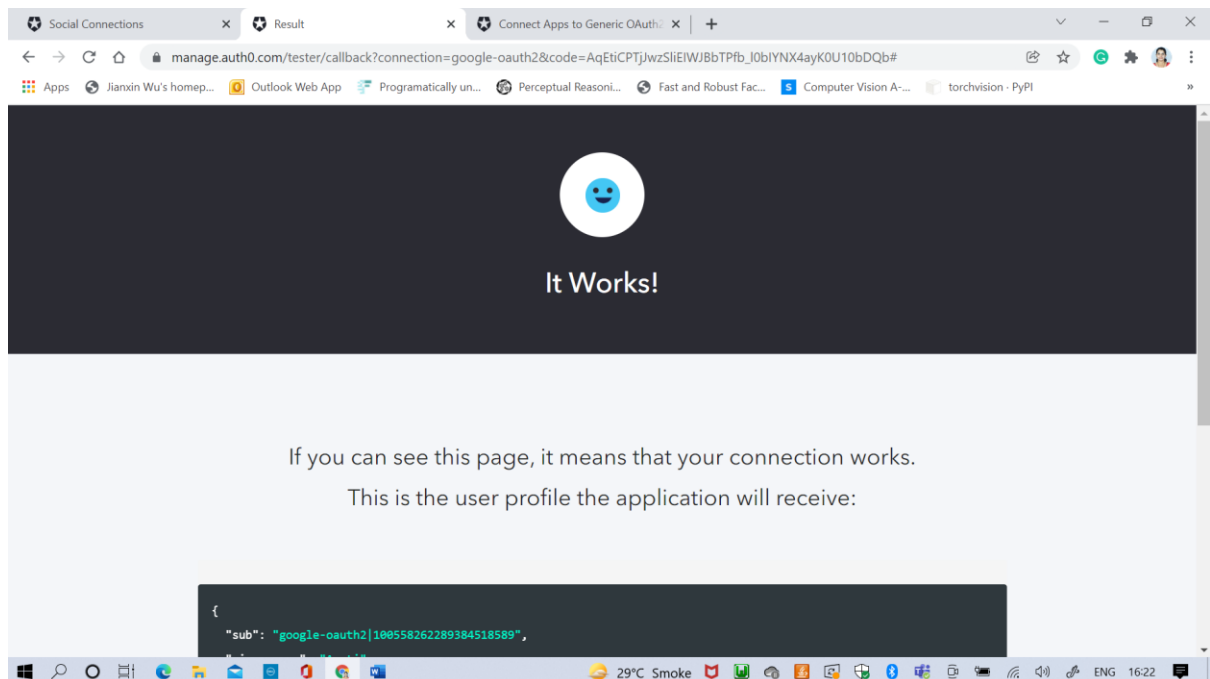
- Click on “Google/Gmail”. Click on “Add Integration”



➤ 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.

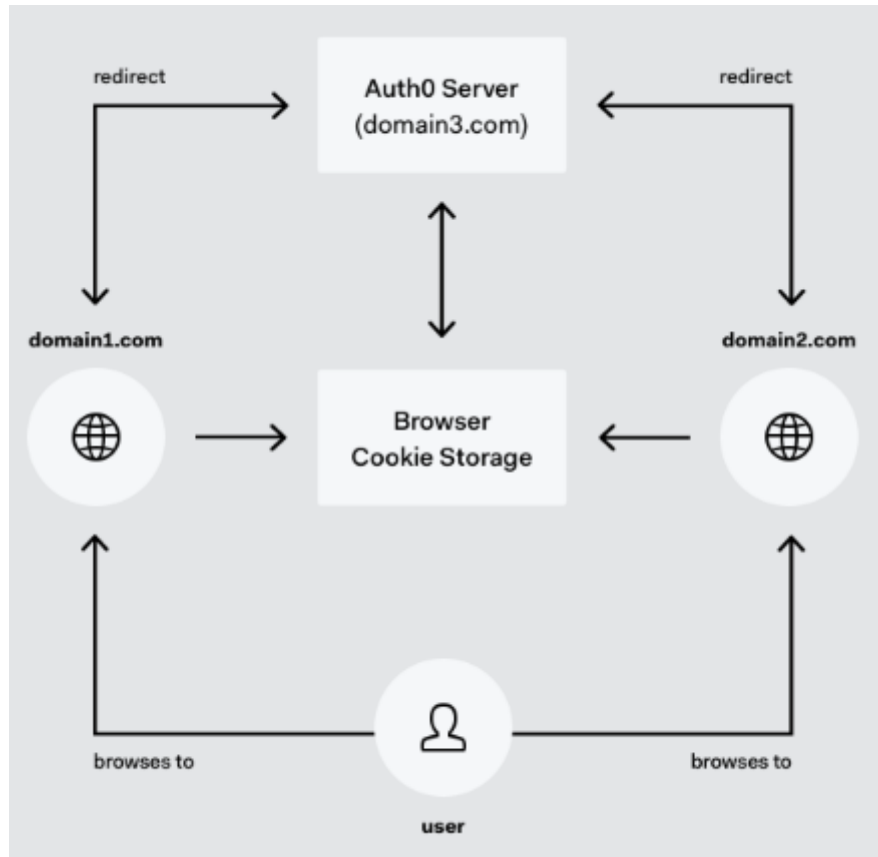
HOW DOES IT SINGLE-SIGN-ON WORKS?

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.