



**Ganpat
University**

॥ विद्यया समाजोत्कर्षः ॥

**Institute of
Computer
Technology**

Name: Tushar Panchal

En.No: 21162101014

Sub: CS(Cloud Security)

Branch: CBA

Batch:71

-----PRACTICAL 13-----

An online learning platform named offers a variety of courses to students. To protect students' personal information and course materials, requires users to log in before accessing their courses. The platform uses IBM Cloud App ID for managing user authentication and authorization.

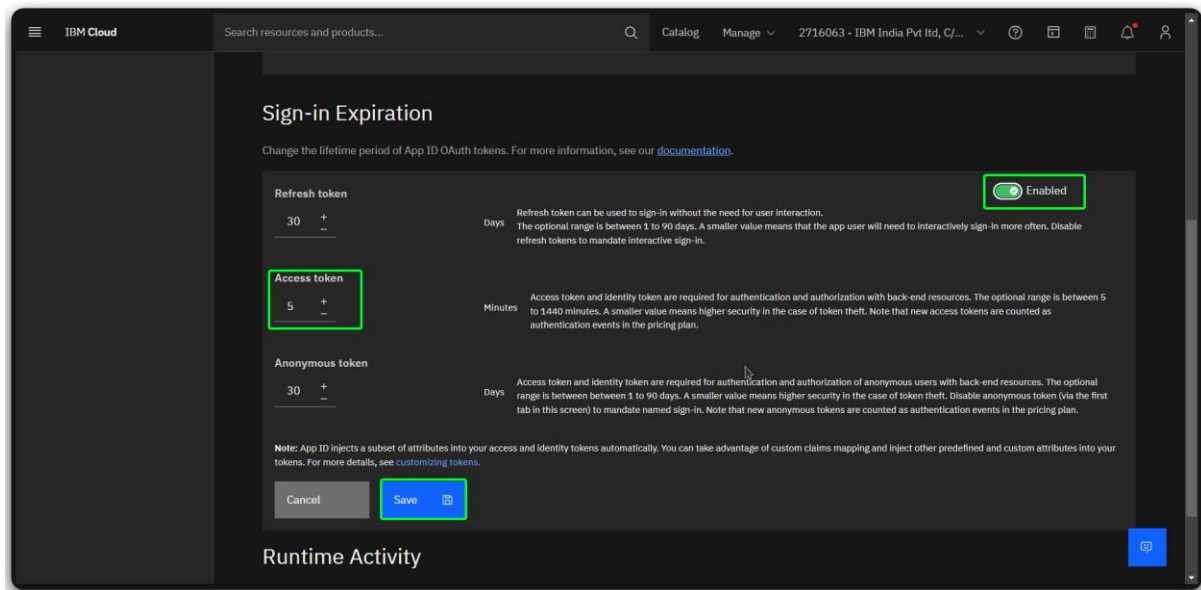
13.1: To ensure a smooth user experience, wants users to stay logged in while studying without frequent re-authentication prompts. Since access tokens have a short expiration time (e.g., 15 minutes), the platform uses refresh tokens to generate new access tokens when the original token expires, allowing users to stay logged in and access resources seamlessly.

Demonstrate how the refresh token can be used to regenerate the access token without any need to login again.

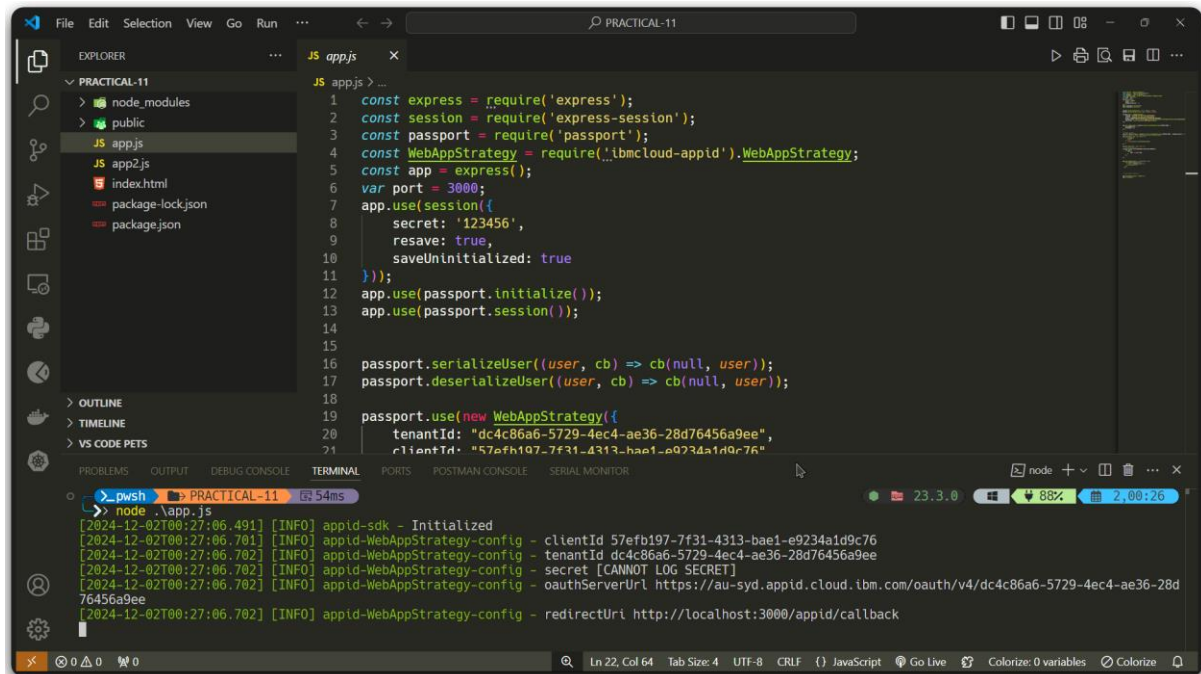
13.2: As part of enhancing authentication for your application, set up an on IBM Cloud to connect external user repositories to your IBM Cloud account. This will allow users to log in with their organization's credentials, enabling seamless access without needing individual account invites.


Create a new and configure it and finally test the configuration by logging in using a user from the external directory to ensure that authentication works as expected.


1. Turn on Refresh Token settings for AppID instance and set minimum duration of Access Token




2. Use previous code of practical 11 to access the node app after logging into AppID, which return access, identity, refresh tokens in console after login, copy them






 Login with Facebook


 Login with Google

or

Email

 tusharpanchai21@gnu.ac.in

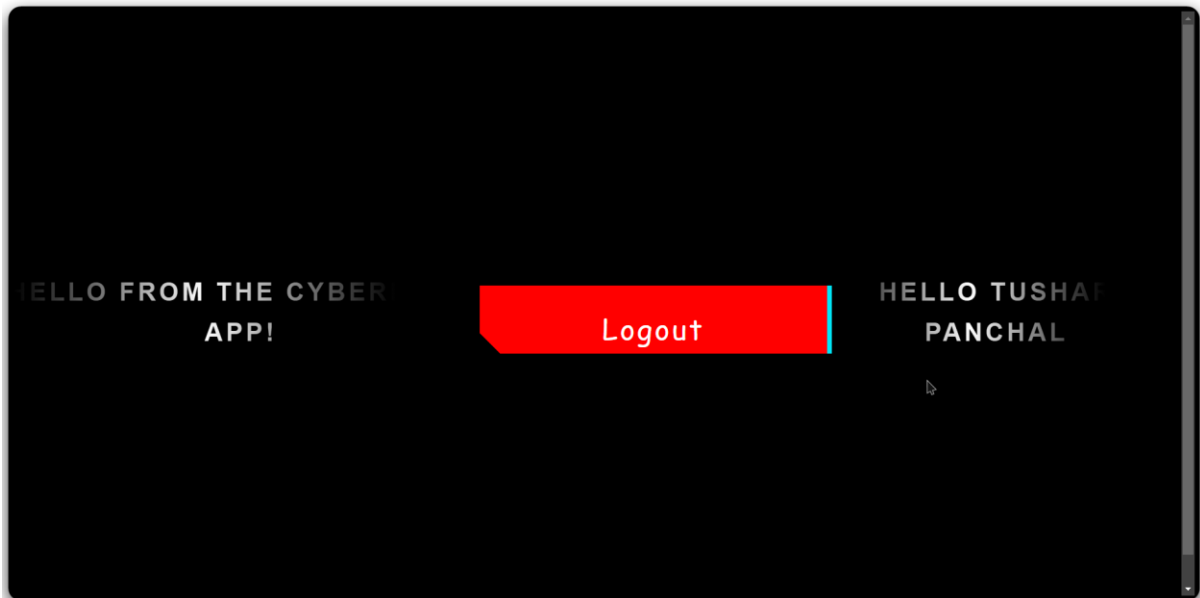
Password

 *****

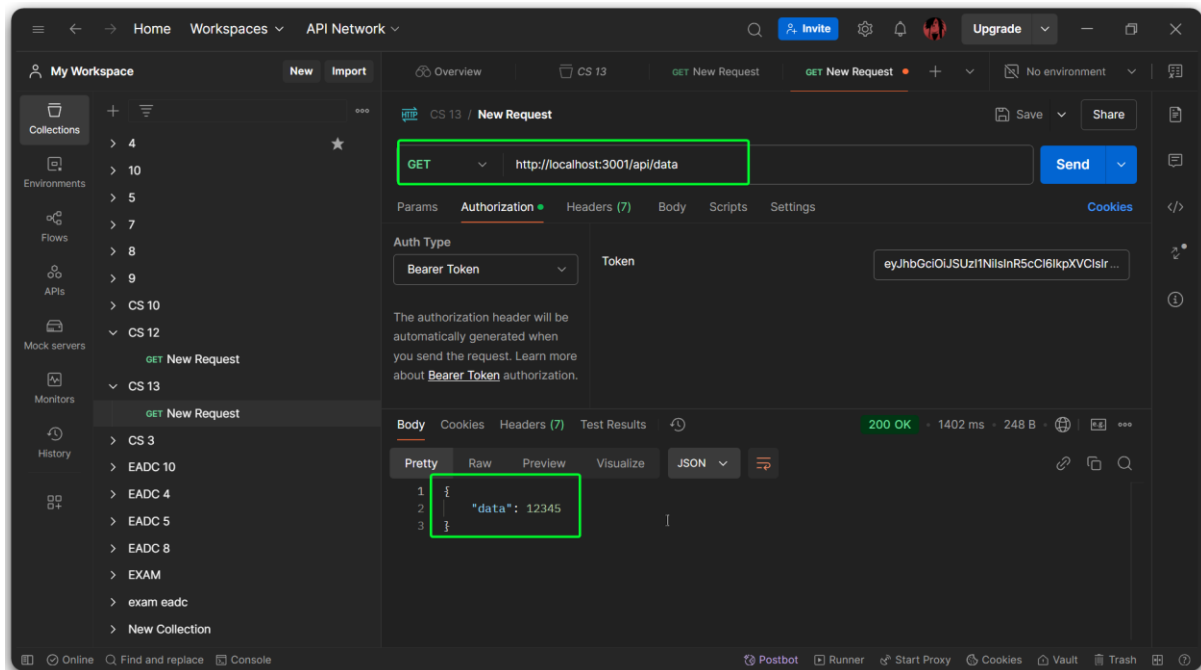
[Forgot password?](#)

Sign In

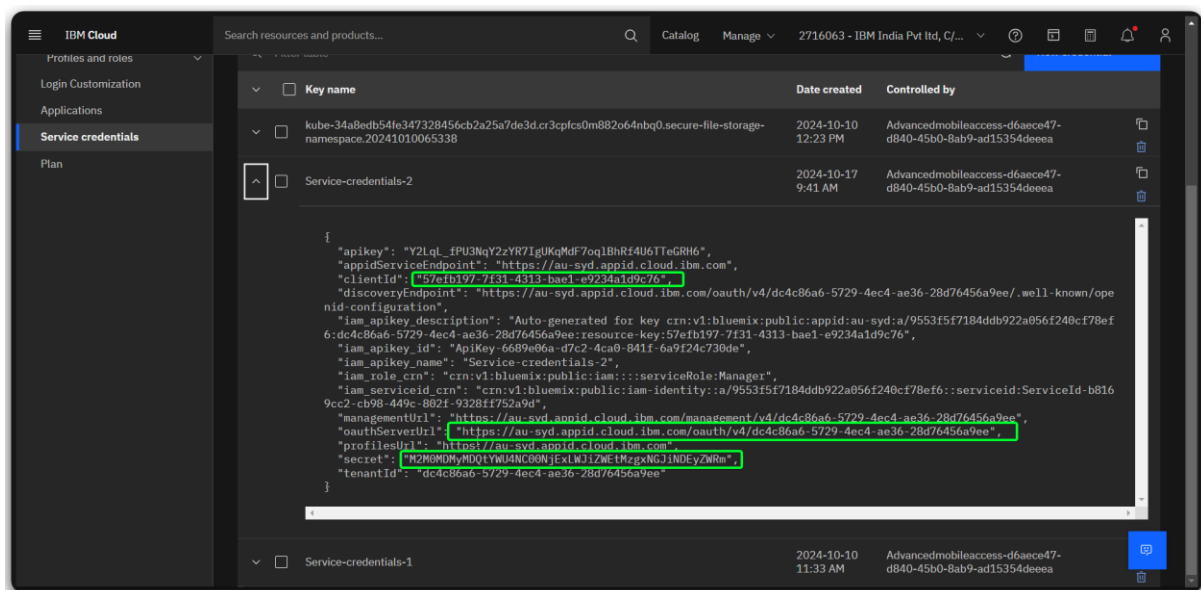
[Don't have an account? Sign up!](#)

[illegible]

3. Run another app2.js code to use WebApp Strategy to access data using access token copied above

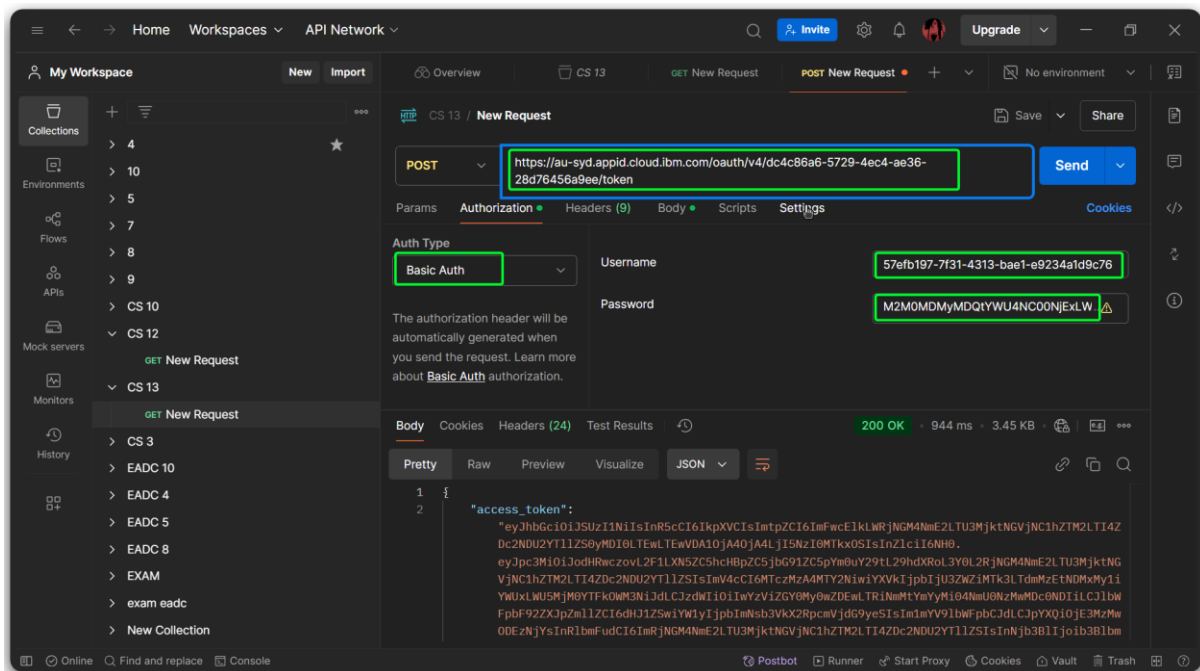


Copy outhserverurl ,client id ,and secret

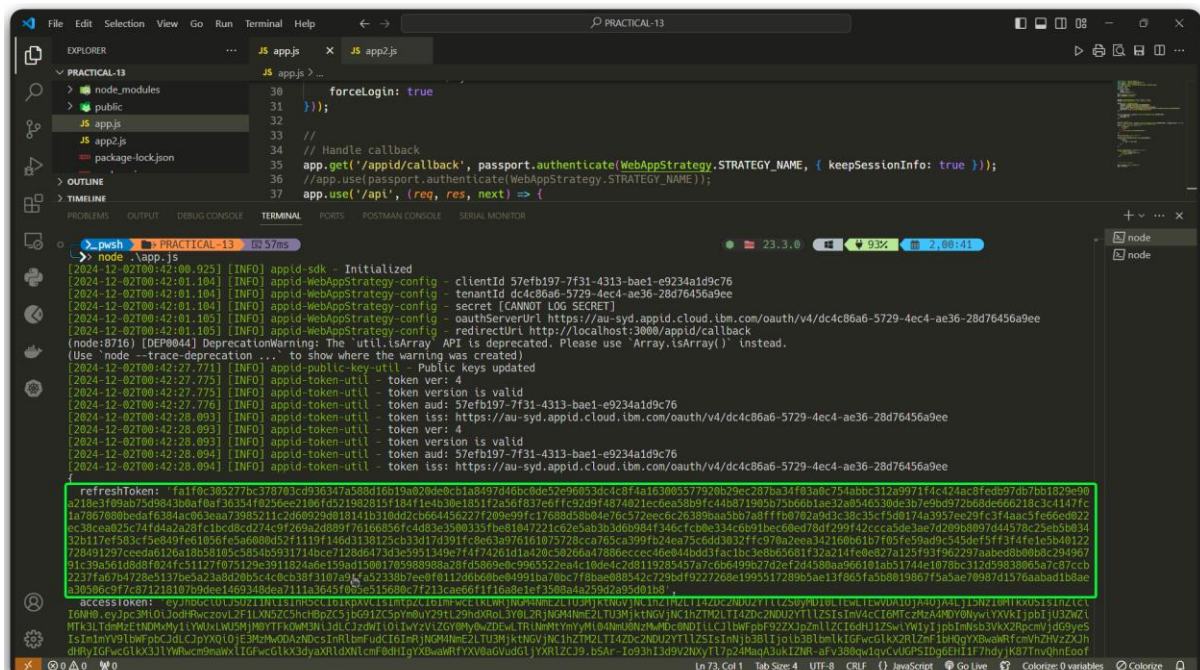


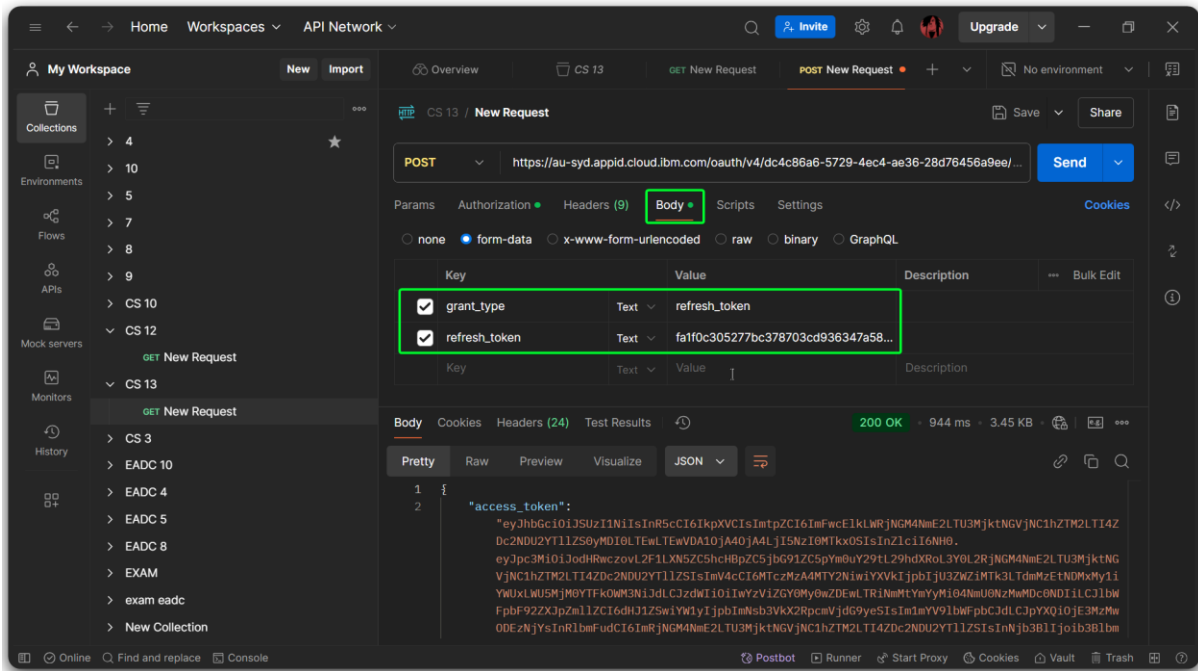
And past those into postman like below

ClientID into username and secret into password

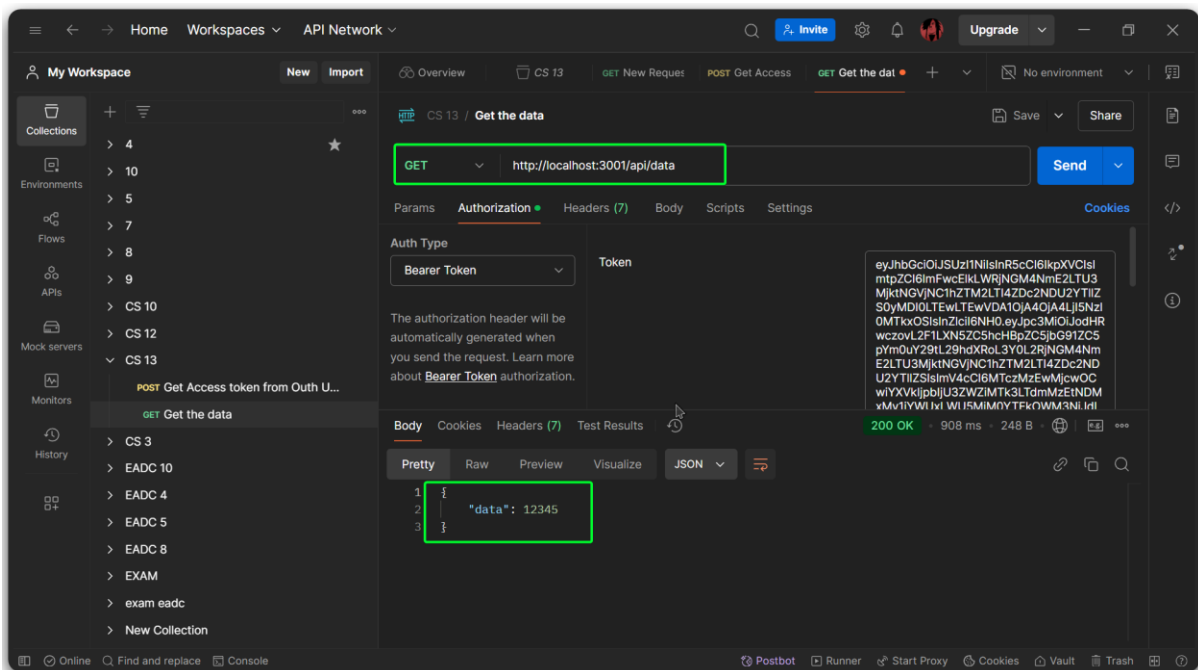


And in body select form-data and set this type and enter access token that generate in terminal

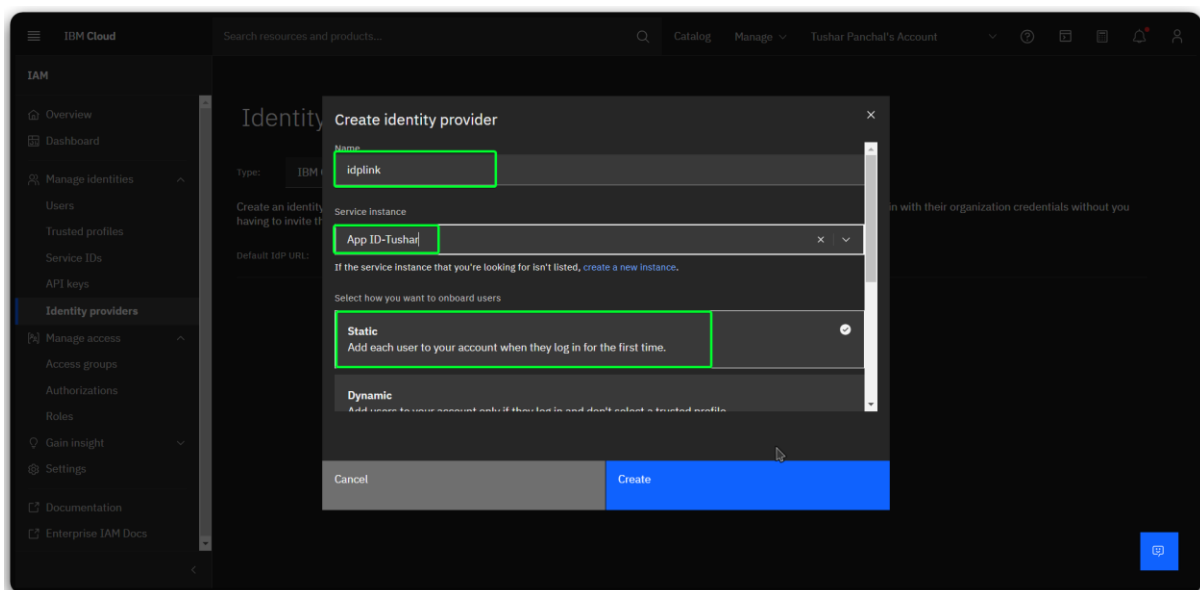
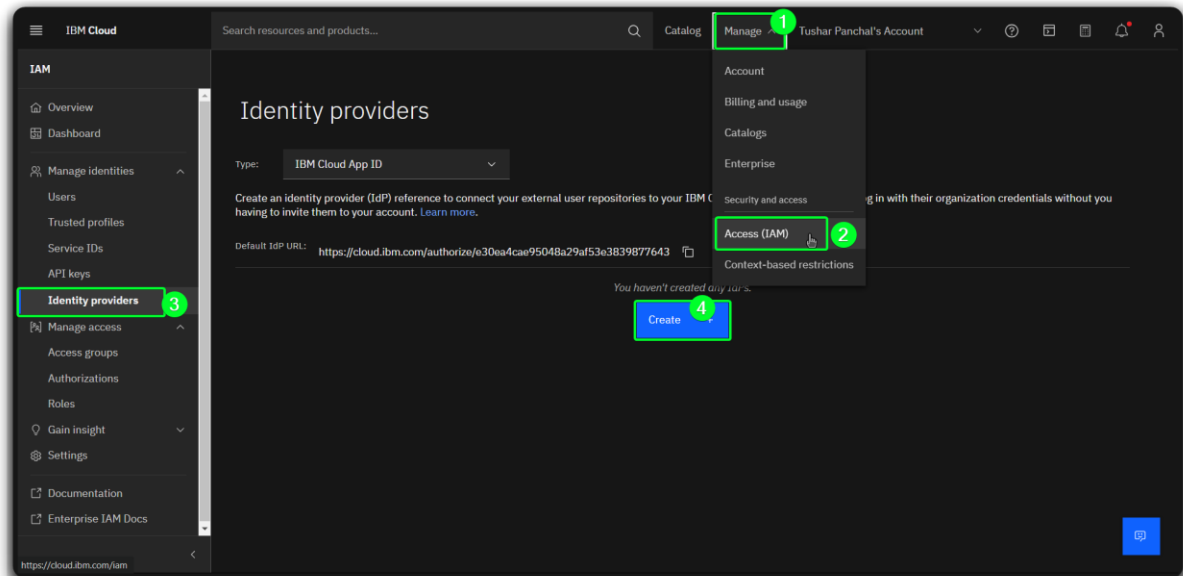


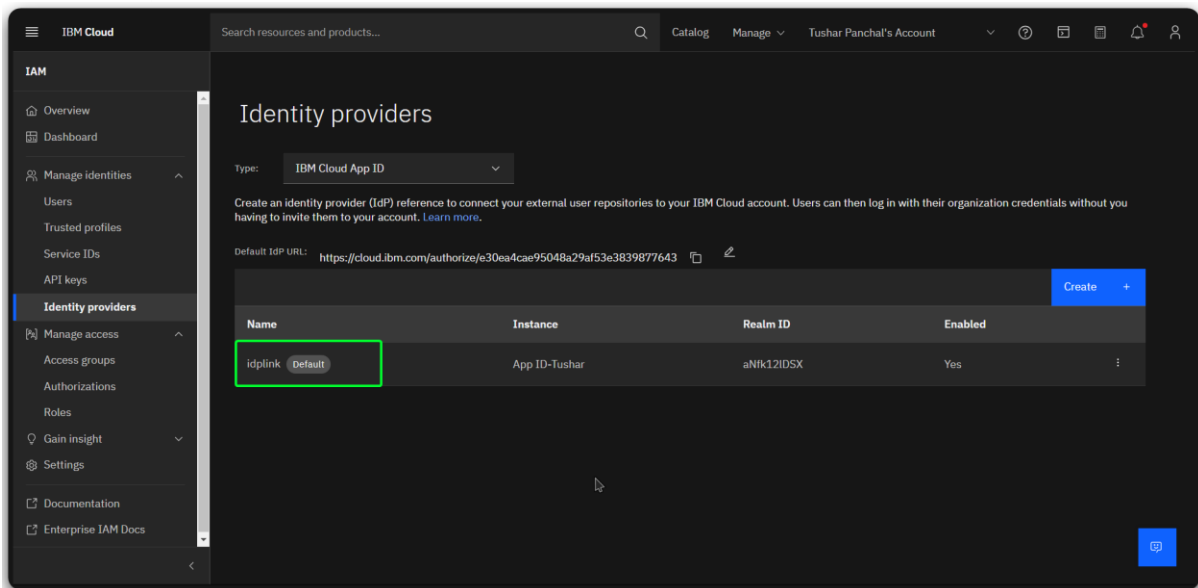


After doing authorization and body part send request to generate refresh token without logging again.



For reliable access using IAM, we can use identity provider link to automate adding IAM users on their signup and first login (access to resources must be specified explicitly for that user, it just allows to login)





IBM Cloud

Search resources and products...

Catalog Manage Tushar Panchal's Account

IAM

- Overview
- Dashboard
- Manage identities
 - Users
 - Trusted profiles
 - Service IDs
 - API keys
 - Identity providers**
- Manage access
 - Access groups
 - Authorizations
 - Roles
- Gain insight
- Settings
- Documentation
- Enterprise IAM Docs

Identity providers

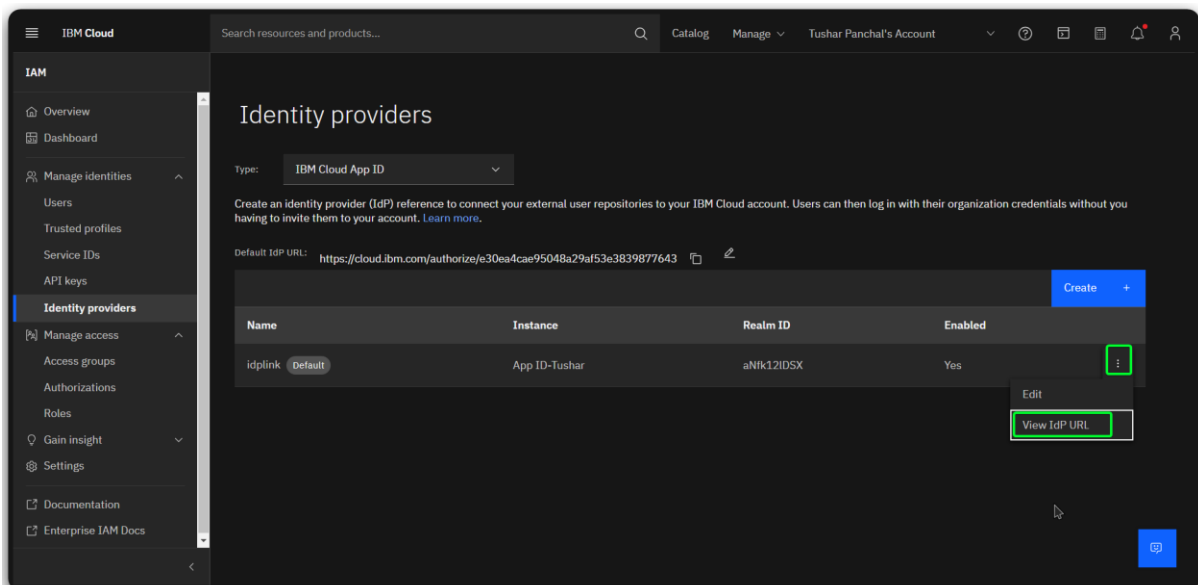
Type: IBM Cloud App ID

Create an identity provider (IdP) reference to connect your external user repositories to your IBM Cloud account. Users can then log in with their organization credentials without you having to invite them to your account. [Learn more.](#)

Default IdP URL: <https://cloud.ibm.com/authorize/e30ea4cae95048a29af53e3839877643>

Create +

Name	Instance	Realm ID	Enabled
idplink <small>Default</small>	App ID-Tushar	aNfk12IDSX	Yes



IBM Cloud

Search resources and products...

Catalog Manage Tushar Panchal's Account

IAM

- Overview
- Dashboard
- Manage identities
 - Users
 - Trusted profiles
 - Service IDs
 - API keys
 - Identity providers**
- Manage access
 - Access groups
 - Authorizations
 - Roles
- Gain insight
- Settings
- Documentation
- Enterprise IAM Docs

Identity providers

Type: IBM Cloud App ID

Create an identity provider (IdP) reference to connect your external user repositories to your IBM Cloud account. Users can then log in with their organization credentials without you having to invite them to your account. [Learn more.](#)

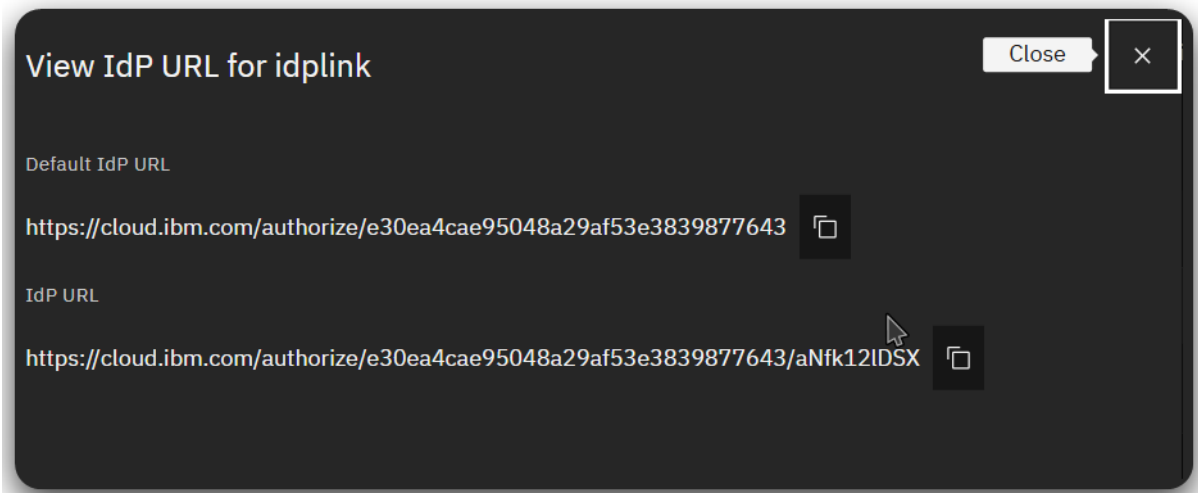
Default IdP URL: <https://cloud.ibm.com/authorize/e30ea4cae95048a29af53e3839877643>

Create +

Name	Instance	Realm ID	Enabled
idplink <small>Default</small>	App ID-Tushar	aNfk12IDSX	Yes

Edit

View IdP URL



View IdP URL for idplink

Close X

Default IdP URL

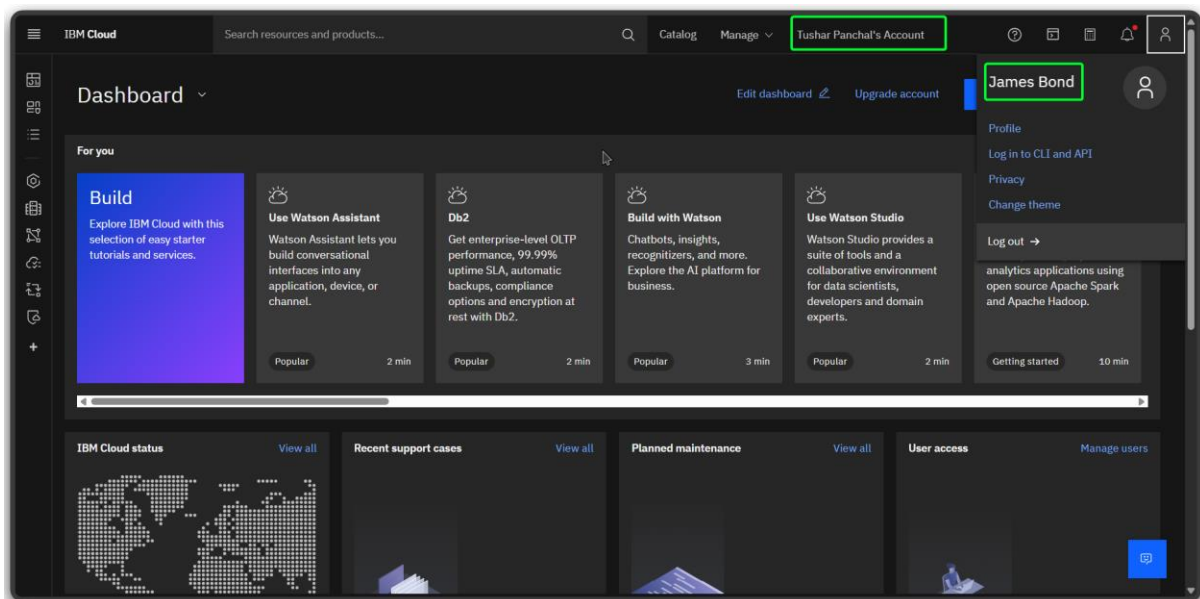
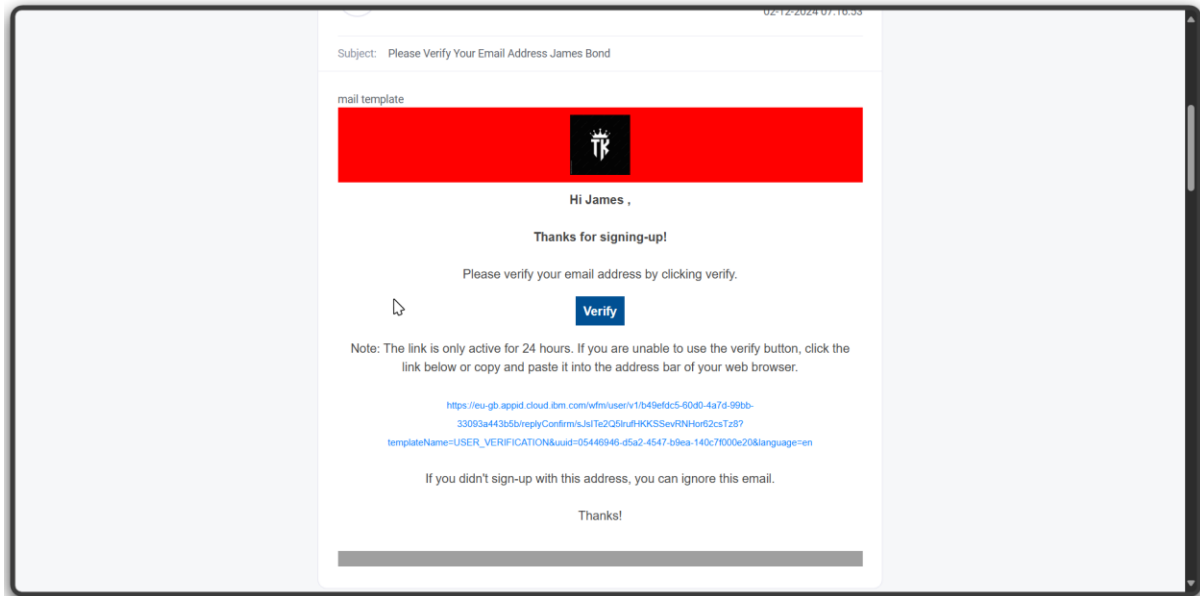
<https://cloud.ibm.com/authorize/e30ea4cae95048a29af53e3839877643>

IdP URL

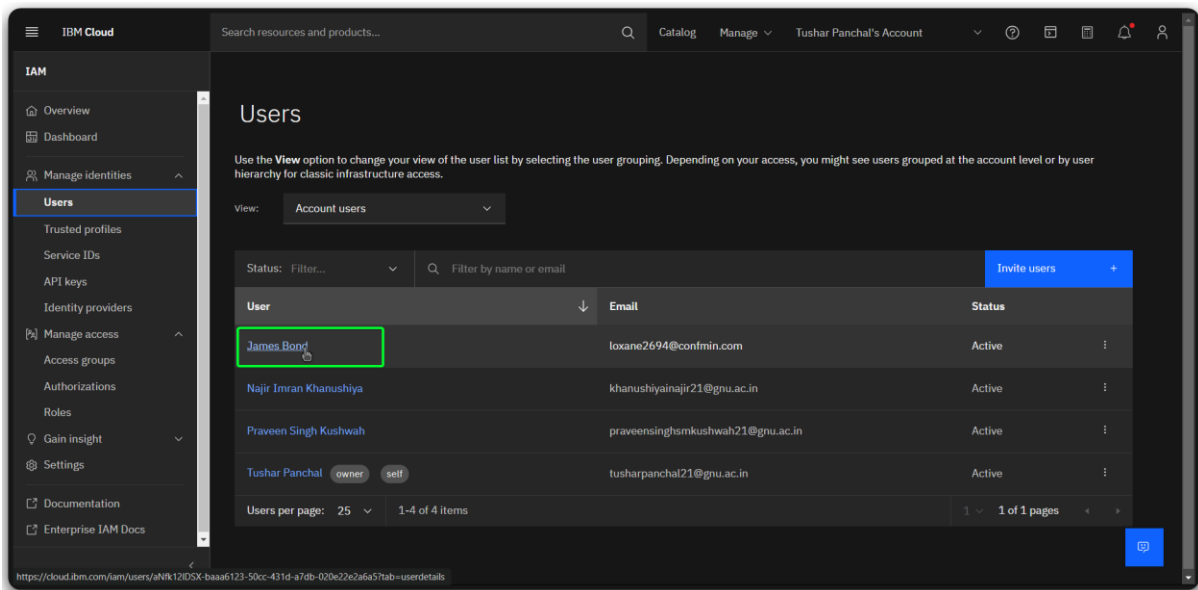
<https://cloud.ibm.com/authorize/e30ea4cae95048a29af53e3839877643/aNfk12IDSX>

7. Open this link or share with anyone to add user on signup and first login using AppID provider (open in second browser where you have not logged in IBM Cloud)

I have signed up with james bond name



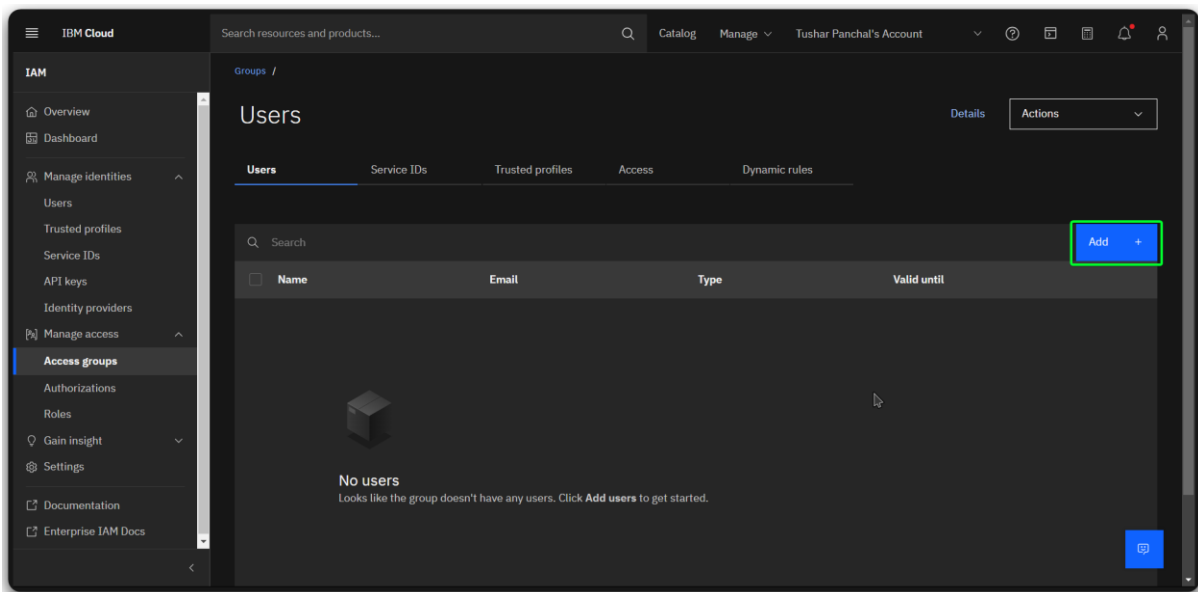
As you can see above my account name is James Bond and using Tushar Panchal's Authorized account by ID purl



The screenshot shows the IBM Cloud IAM 'Users' page. The left sidebar has 'Users' selected under 'Manage identities'. The main content area shows a list of users with columns for 'User', 'Email', and 'Status'. The 'View' dropdown is set to 'Account users'. A green box highlights the 'James Bond' user entry. Below the table, it says 'Users per page: 25' and '1-4 of 4 items'. The URL at the bottom is `https://cloud.ibm.com/iam/users/aNik12DSX-baaa6123-50cc-431d-a7db-020c22c2a6a5?tab=userdetails`.

User	Email	Status
James Bond	loxane2694@confmin.com	Active
Najir Imran Khanushiya	khanushiya.najir21@gnu.ac.in	Active
Praveen Singh Kushwah	praveensinghsmkushwah21@gnu.ac.in	Active
Tushar Panchal (owner self)	tusharpanchal21@gnu.ac.in	Active

Assign access to user or group as personal preferences and check if the resources are accessible or not



The screenshot shows the IBM Cloud IAM 'Groups' page. The left sidebar has 'Access groups' selected under 'Manage access'. The main content area shows a 'No users' message with a green box around the 'Add' button. The URL at the bottom is `https://cloud.ibm.com/iam/groups/aNik12DSX-baaa6123-50cc-431d-a7db-020c22c2a6a5?tab=users`.

No users
Looks like the group doesn't have any users. Click **Add users** to get started.

The screenshot shows the IBM Cloud IAM 'Users' page. A message at the top states: 'The following list of users can be added to the group. To add a user, their status must be active, pending, or disabled.' Below this, a table lists users. 'James Bond' is selected, highlighted with a green box. A blue bar at the top of the table indicates '1 item selected' and includes 'Add to group' and 'Cancel' buttons. A warning message says: 'Existing members You can't select or remove a user that is already a member of the group.'

User	Email	Status
<input checked="" type="checkbox"/> James Bond	loxane2694@confmin.com	Active
<input type="checkbox"/> Najir Imran Khanushiya	khanushiya.najir21@gnu.ac.in	Active
<input type="checkbox"/> Praveen Singh Kushwah	praveensinghmkushwah21@gnu.ac.in	Active
<input type="checkbox"/> Tushar Panchal (owner self)	tusharpanchal21@gnu.ac.in	Active

Users per page: 25 | 1-4 of 4 items | 1 of 1 pages

The screenshot shows the IBM Cloud IAM 'Users' page with the 'Access' tab selected. A green box highlights the 'James Bond' user in the table. A success message at the top right says: 'Access group User successfully removed from access group.'

Name	Email	Type	Valid until
<input checked="" type="checkbox"/> James Bond	loxane2694@confmin.com		

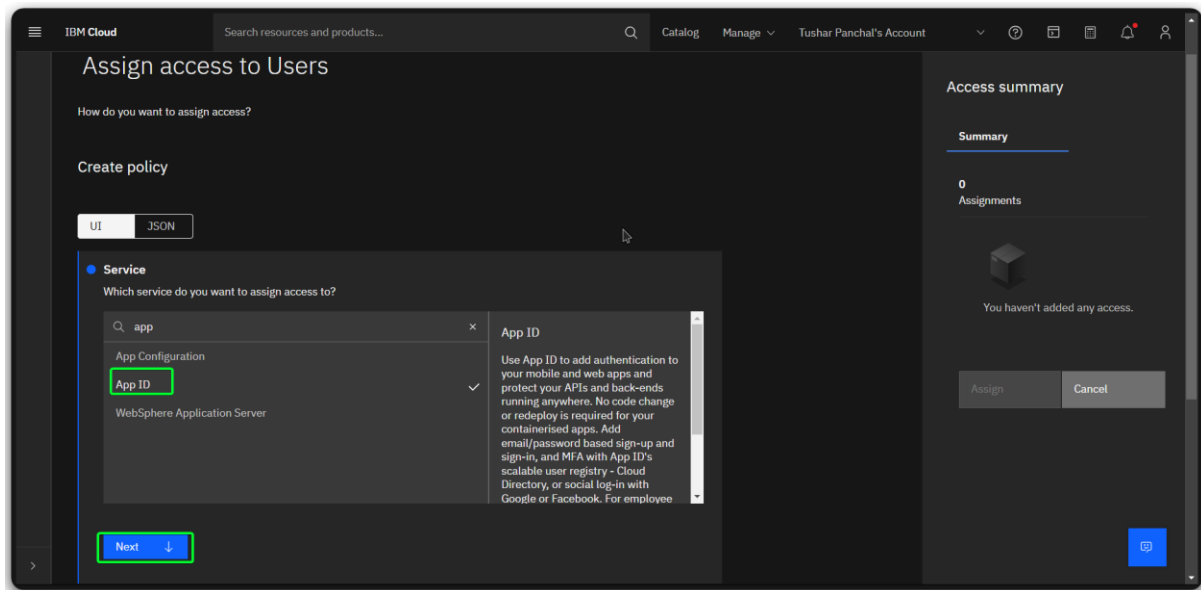
Items per page: 25 | 1-1 of 1 item | 1 of 1 page

The screenshot shows the IBM Cloud IAM 'Users' page with the 'Access' tab selected. A green box highlights the 'Access' tab. Below the tab, a table is used to assign access policies. The table has columns: Service, Resources, Role, Conditions, and Last permit. A blue button 'Assign access' is visible. Below the table, a section titled 'Access policies' states: 'You can find your resources here after you create them.'

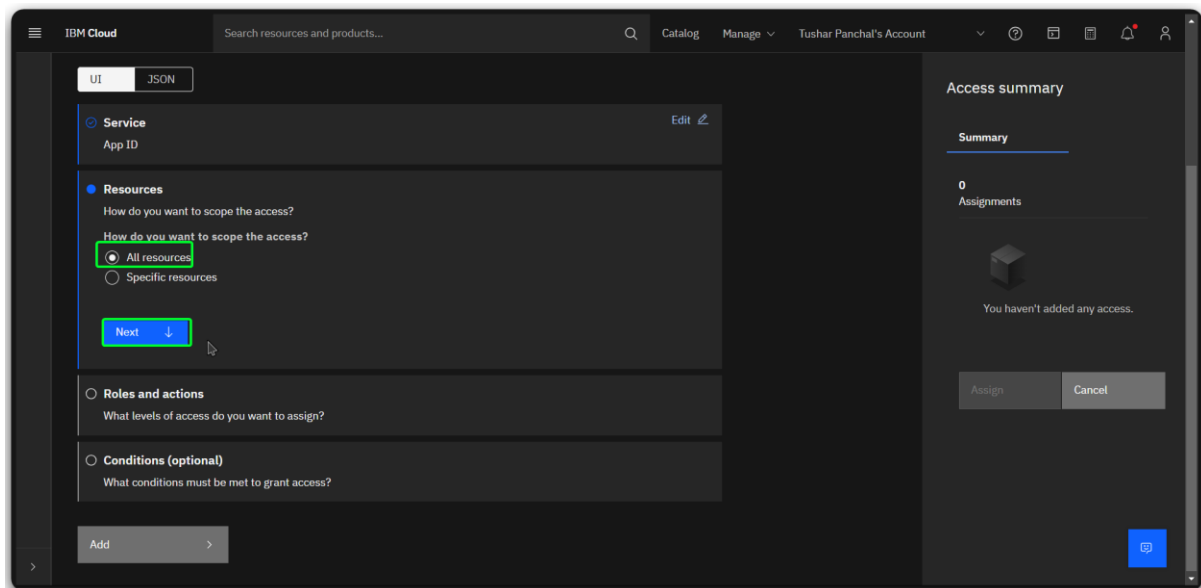
Service	Resources	Role	Conditions	Last permit
---------	-----------	------	------------	-------------

Access policies
You can find your resources here after you create them.

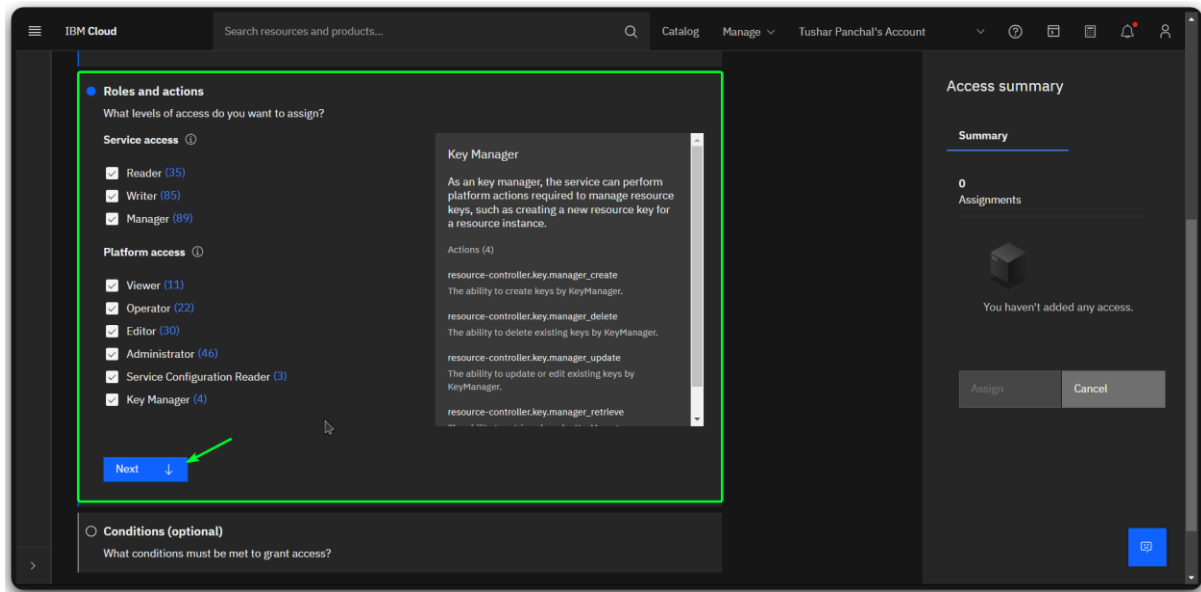
You can give any other service access also but I am giving appid access



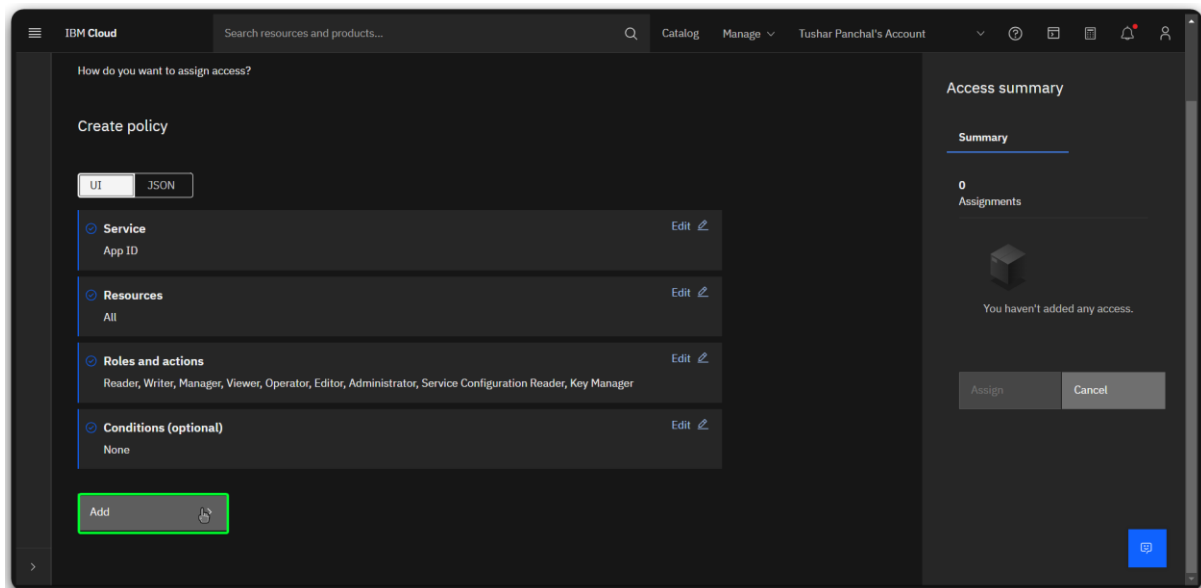
Selecting all resources in below

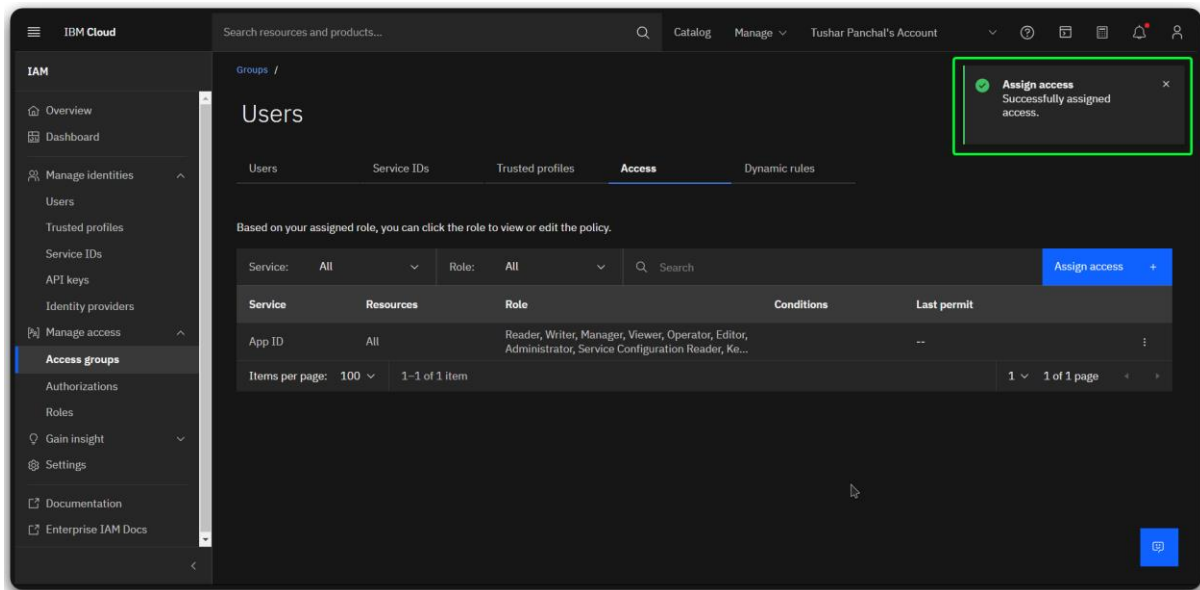


Giving all roles and actions too



Then hit add button to review and then hit assign button to give access.





Now we can access app id on that idp url created account

