# ANJALAI AMMAL MAHALINGAM ENGINEERING COLLEGE

## DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

# NAAN-MUDHALVAN

## OPTIMIZING USER, GROUP, AND ROLE MANAGEMENT THROUGH ACCESS CONTROL AND WORKFLOWS USING SERVICENOW

**Team Id:** NM2025TMID00534

**Team size:** 4

**Team Leader : AAKASH S**

**Team Member 1: ARUN KUMAR R.A**

**Team Member 2: AHAMED ASARUDEEN S**

**Team Member 3: KIRTHIK SARVASH S**

## 1. Introduction

Effective project management is crucial for ensuring that projects are completed on time, within budget, and to the desired quality standards. ServiceNow Project Management offers a comprehensive platform for managing projects by providing tools that help plan, execute, track, and report on project activities with accuracy and transparency. It integrates automation, real-time dashboards, and analytics to improve collaboration, increase efficiency, and deliver business objectives.

In the context of a small project management team comprising a Project Manager and a Team Member, using structured user roles, access controls, and workflow automation can greatly enhance task accountability and progress tracking. Defining clear roles and permissions ensures that project tasks are assigned efficiently, and structured workflows improve communication and monitoring throughout the project lifecycle.

This project aims to optimize user, group, and role management combined with access control and automated workflows to streamline task assignments and accountability in managing project tasks, ultimately fostering better collaboration and project success. This approach aligns with the best practices encouraged by modern project portfolio management platforms like ServiceNow, which emphasize resource management, task prioritization, and timely project delivery through integrated tools and controlled processes.

## 1. Project Overview

- **Objective:**

  The objective of this project is to streamline user, group, and role management by implementing access controls and automated workflows. It ensures secure, role-based access, reduces manual effort, and improves compliance through audit-ready processes. This enhances operational efficiency and governance across the organization.

- **Description:**

  This project focuses on enhancing enterprise-level identity and access management by streamlining the assignment and control of users, groups, and roles. The goal is to build a scalable system that automates user provisioning, group associations, and role-based access control (RBAC) using clearly defined workflows. It ensures that users only have access to the resources they need based on their job functions, improving security and reducing administrative overhead. By integrating approval workflows and dynamic access policies, the system provides better compliance, auditing, and operational efficiency.

- **Key Features**

| Feature | Description |
|---|---|
| **User, Group & Role Import** | Imports user, group, and role data from external systems using Import Sets and Transform Maps to ensure accurate identity mapping. |
| **Dot-Walking Relationships** | Automatically fetches related information (e.g., department, location, manager) from linked user/group records for seamless data consistency. |
| **Access Control Rules (ACLs)** | Enforces strict access to forms, fields, and tables based on assigned roles, ensuring secure and compliant data handling. |
| **Role-Based Access Management** | Manages permissions for various personas like Admins, Managers, and End Users using RBAC principles for fine-grained control. |
| **Custom Data Models** | Builds custom tables and fields to manage additional metadata such as access levels, audit logs, and workflow triggers. |
| **Workflow Automation** | Implements approval and review workflows for role assignments and access changes, streamlining governance. |
| **Dynamic Dashboards & Reports** | Enables real-time reporting based on roles, departments, or access levels to monitor user distribution and access patterns. |
| **User Impersonation for Testing** | Allows impersonation of users to test access controls, visibility, and assigned workflows in real-time without needing separate logins. |
| **Scalability & Optimization** | Designed to scale across enterprise environments, ensuring fast performance, secure access control, and efficient bulk data handling. |

## 2. Project Ideation Phase

---

- **Project Title:** Optimizing User, Group, and Role Management with Access Control and Workflows in ServiceNow
- **Problem Statement:** In a small project management team consisting of a Project Manager (Alice) and a Team Member (Bob), there is a need to efficiently manage project tasks and ensure accountability throughout the project lifecycle. The current system lacks clear role definitions, access controls, and a structured workflow, leading to confusion regarding task assignments and progress tracking.

## 3. Requirement Analysis Phase

---

- **Users:** Create two users.
- **Groups:** Create two groups.
- **Roles:** Create roles for the users.
- **Tables:** Create table to store the data.
- **Assignments:** Assign users to groups, Assign roles to users and Assign Table access to application.
- **Access Control List (ACL):** Secure fields based on roles.
- **Flow:** Create a Flow to Assign Operations Ticket to Group.
- **Results:** Test outcome—verify links and field population.
- **Conclusion:** Evaluate success and readiness for deployment.

## 4. Project Planning Phase

---

### 1. Project Timeline:

- Break your project into phases:
    - Ideation
    - Requirement Analysis
    - Design
    - Development (Users, Groups, Roles, Tables, ACL s and Flows)
    - Testing
    - Report generation
    - Review & Conclusion

## 2. Risk Management:

| Risk | Impact | Probability | Mitigation Strategy |
|---|---|---|---|
| Incorrect role assignment grants excessive access | High | Medium | Implement role approval workflows and conduct periodic access reviews. |
| Misconfigured ACLs expose sensitive data | High | Medium | Enforce least privilege access and thoroughly test ACLs using user impersonation. |
| Role revocation delays after user status changes | High | Medium | Automate de-provisioning using flows triggered by user status updates or offboarding. |
| Workflow misrouting delays access approvals | High | Low | Test all approval flow paths and set alerts for failures or stuck requests. |

## 3. Task Allocation:

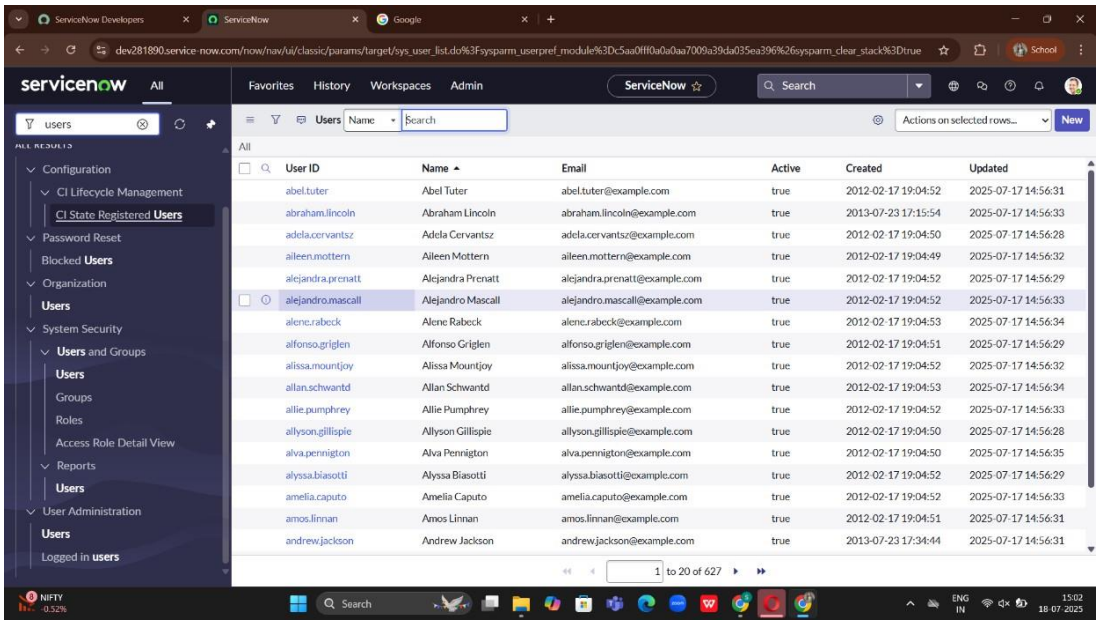
| Task | Assigned To | Time Estimate | Tools Required |
|---|---|---|---|
| User & Group Data Import Setup | Developer | 2 Days | ServiceNow Studio, Import Sets |
| Role Mapping & Assignment Logic | Developer | 2 Days | Role Management Module, Flow Designer |
| ACL Definition & Testing | Admin | 2 Days | ACL Editor, Impersonation Tool |
| Workflow for Role Approvals | Developer | 2 Days | Flow Designer, Approval Workflow |
| Group Membership Automation Rules | Developer | 1 Day | Script Includes, Business Rules |
| Access Review Dashboard | Analyst | 1 Day | Performance Analytics, Report Builder |
| User Impersonation Testing | Tester/Admin | 1 Day | Impersonate Feature in ServiceNow |

## 5. Project Design Phase

---

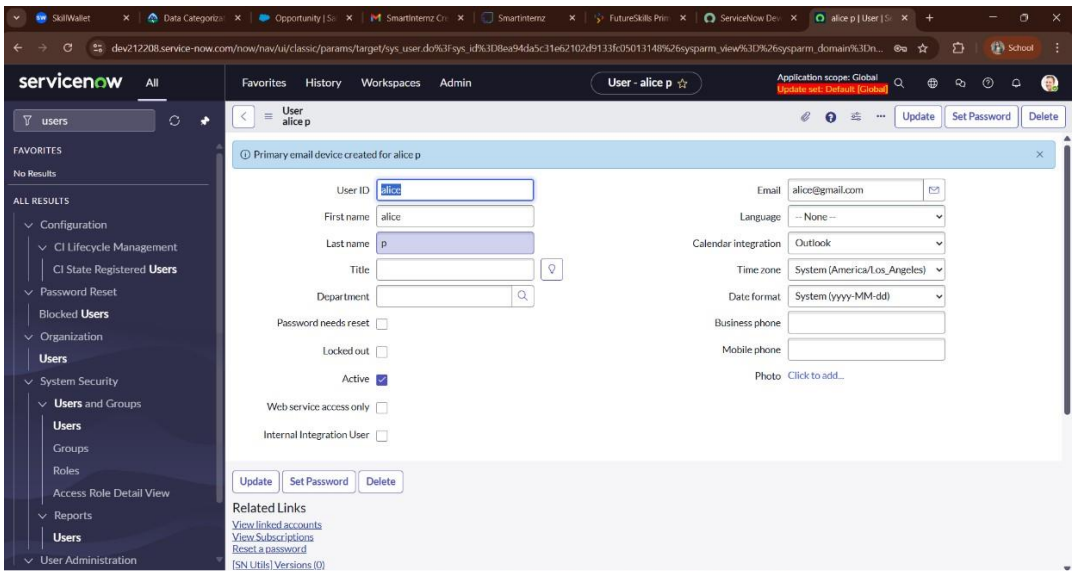
# 1. Create Users

- Open service now.
- Click on **All** >> search for **Users**
- Select Tables under **system security**
- Click on **New**

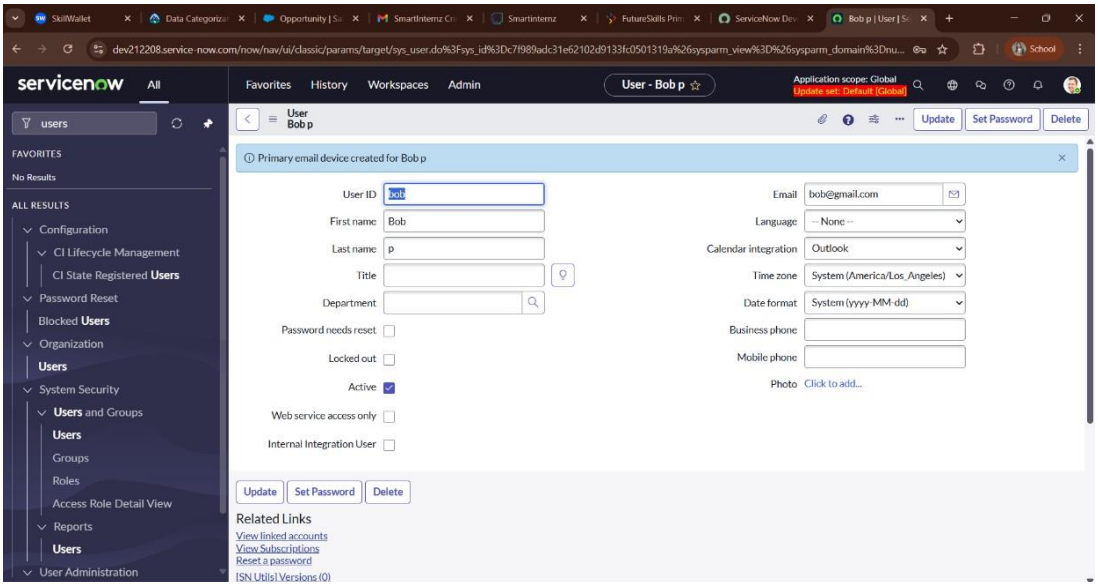



- Fill the following details to create a new users

- Create a user named as “alice p”.

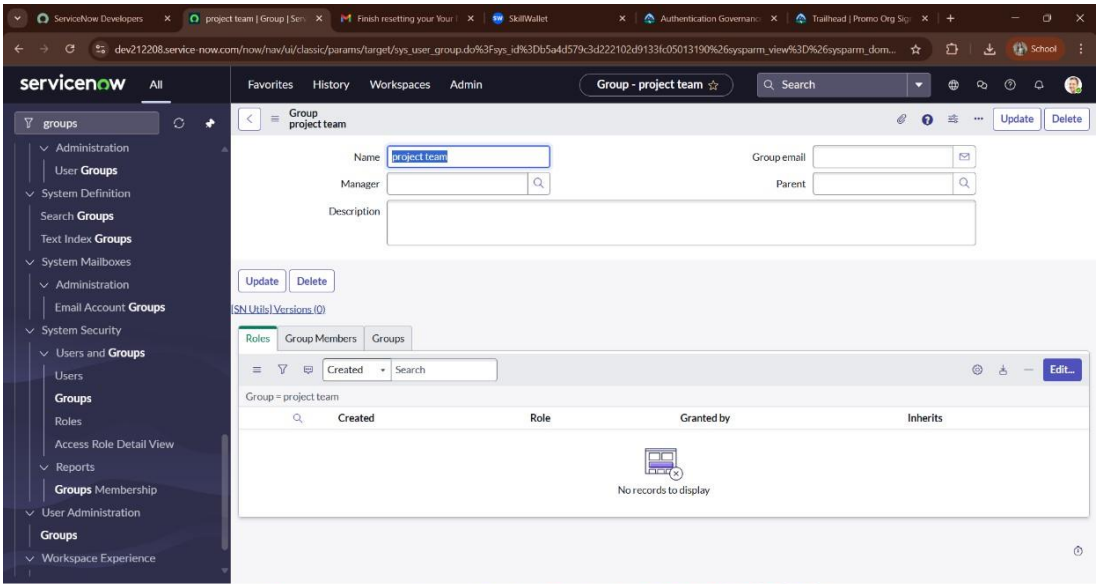


- **Create one more user:**
- Create another user with the following details
- Username: “bob p”.
- Click on submit.



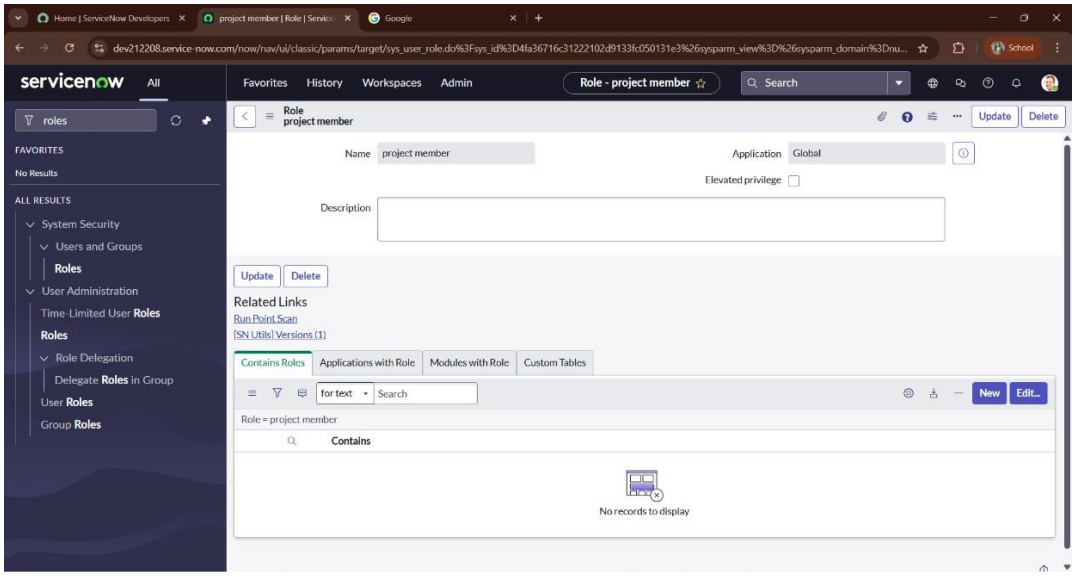

## 2. Create Groups

- Open service now.
- Click on All >> **search for groups**
- Select groups under system security
- Click on new
- Fill the following details to create a new group
- Click on submit

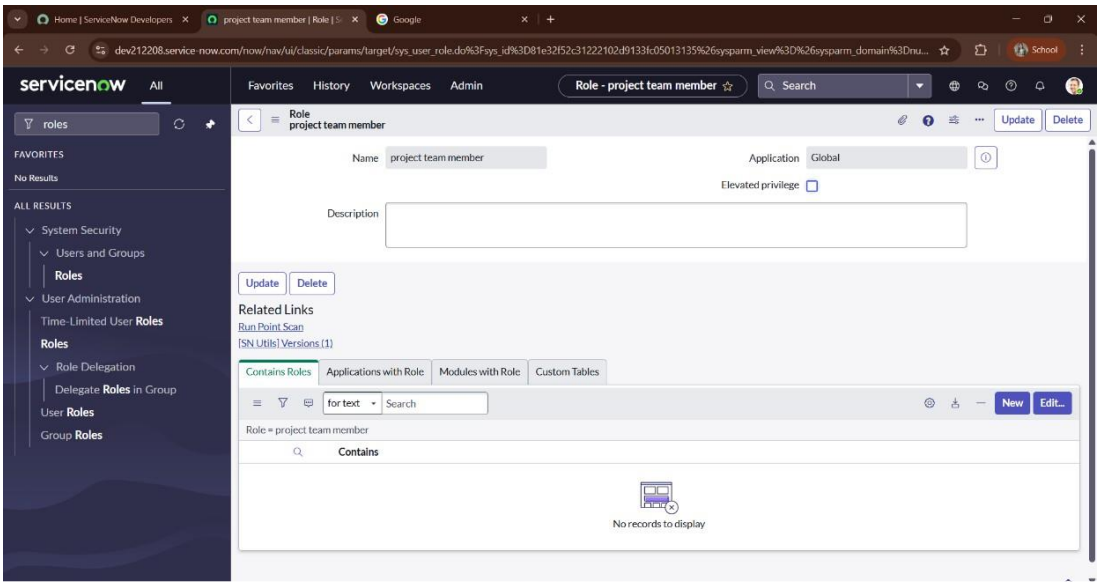



## 3. Create Roles

- Open service now.
- Click on All >> **search for roles**
- Select roles under system security
- Click on new
- Fill the following details to create a new role
- Click on submit

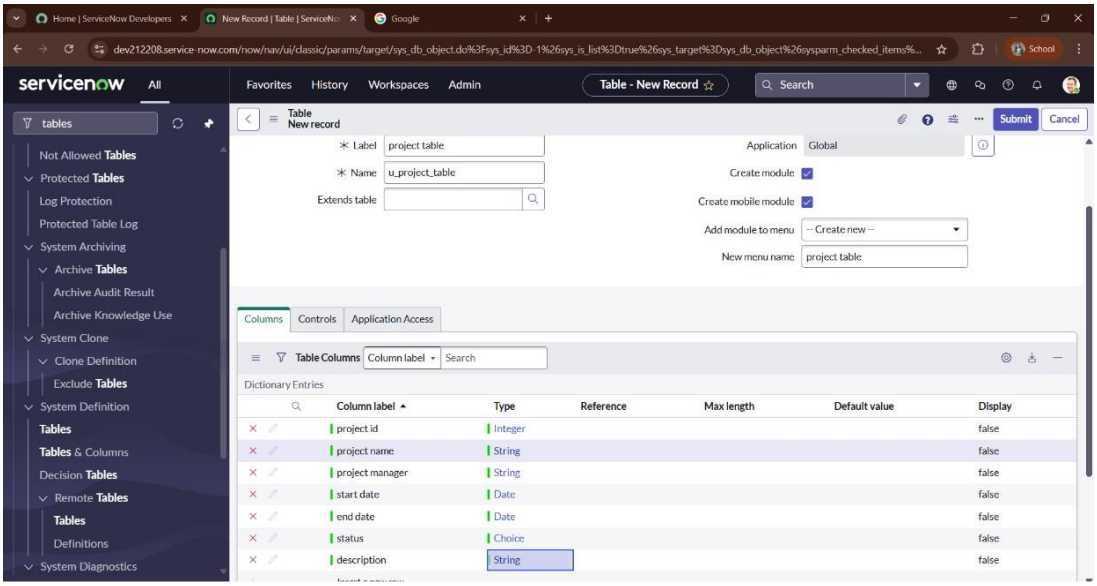


- **Create one more role:**
- Create another role with the following details
- Click on submit

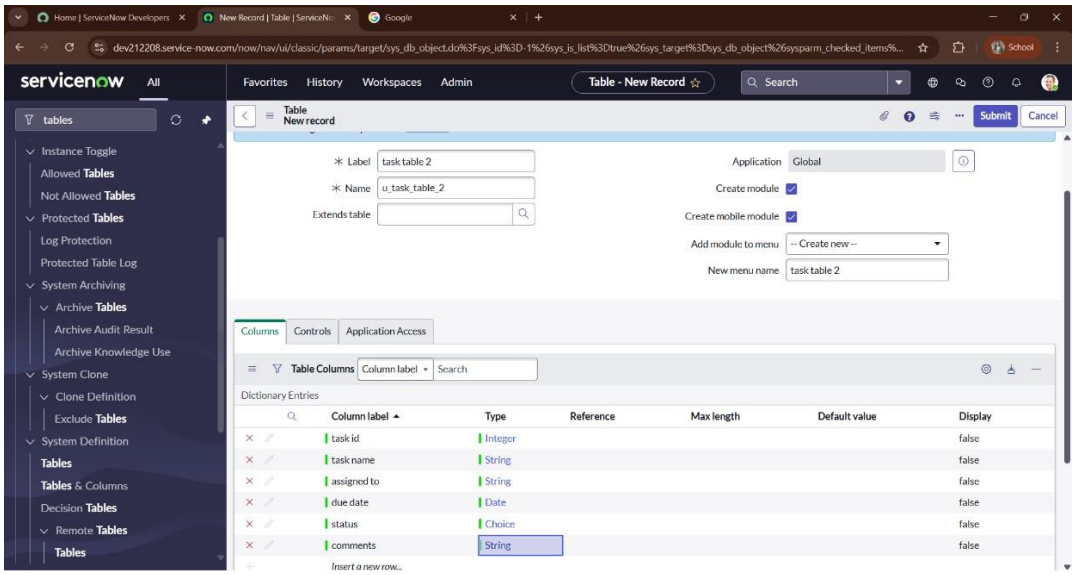



## 4. Create Tables

- Open service now.
- Click on All >> **search for tables**
- Select tables under system definition
- Click on **new**
- Fill the following details to create a new table
  Label : **project table**
  Check the boxes Create module & Create mobile module
- Under new menu name : **project table**
- Under table columns give the columns

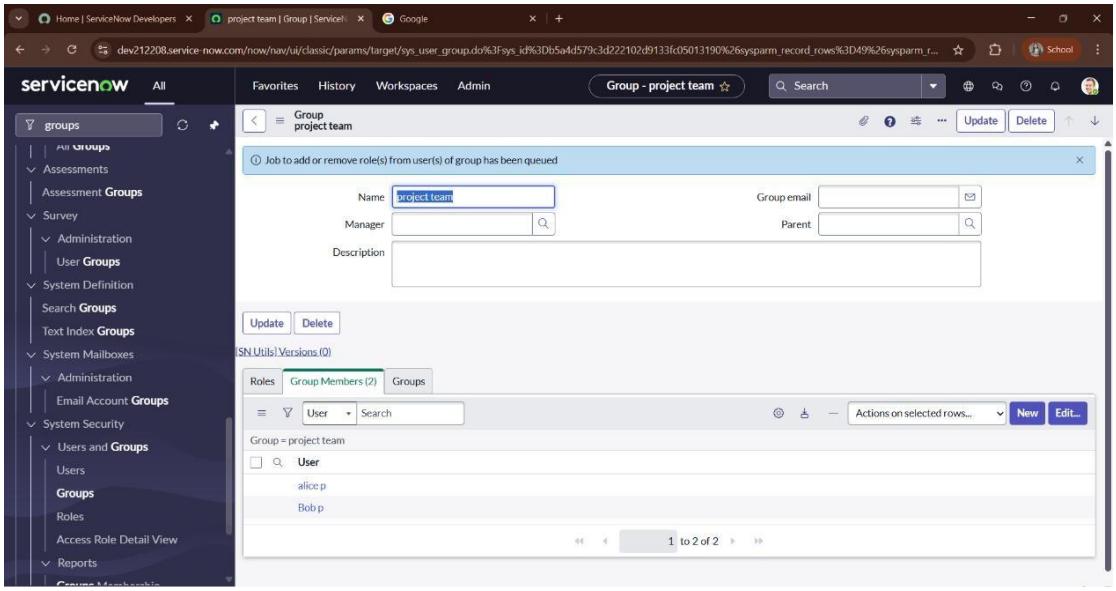



- Click on submit
- **Create one more table:**
- Create another table as:task table 2 and fill with following details.
- Click on **submit**.



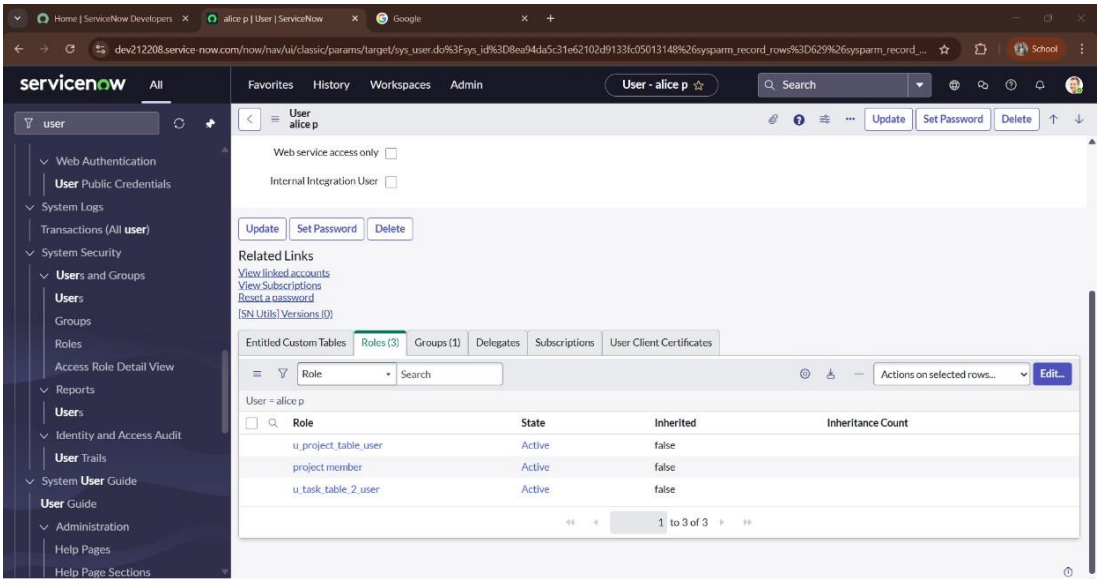
## 5. Assign users to project team group

- Open service now
- Click on All >> **search for groups**
- Select tables under system definition
- Select the project team group
- Under group members
- Click on edit
- Select **alice p** and **bob p** and save.

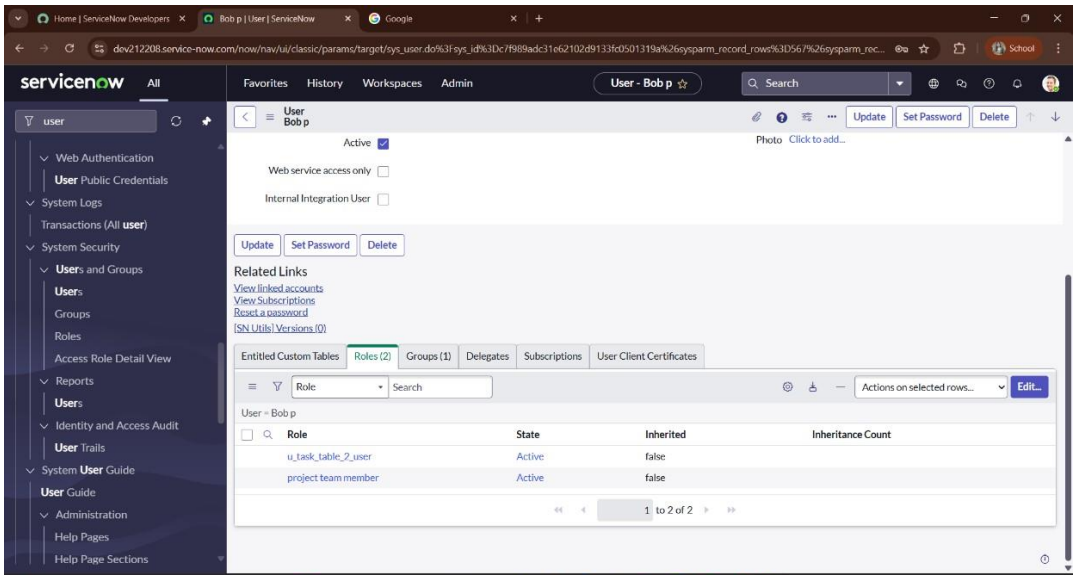



## 6. Assign roles to users

- **Assign roles to alice user**
- Open servicenow
- Click on All >> **search for user**
- Select tables under system definition
- Select the **project manager user**
- Under **project manager**
- Click on edit
- Select **project member** and save
- Click on edit add **u_project_table** role and **u_task_table** role
- Click on **save** and **update** the form.

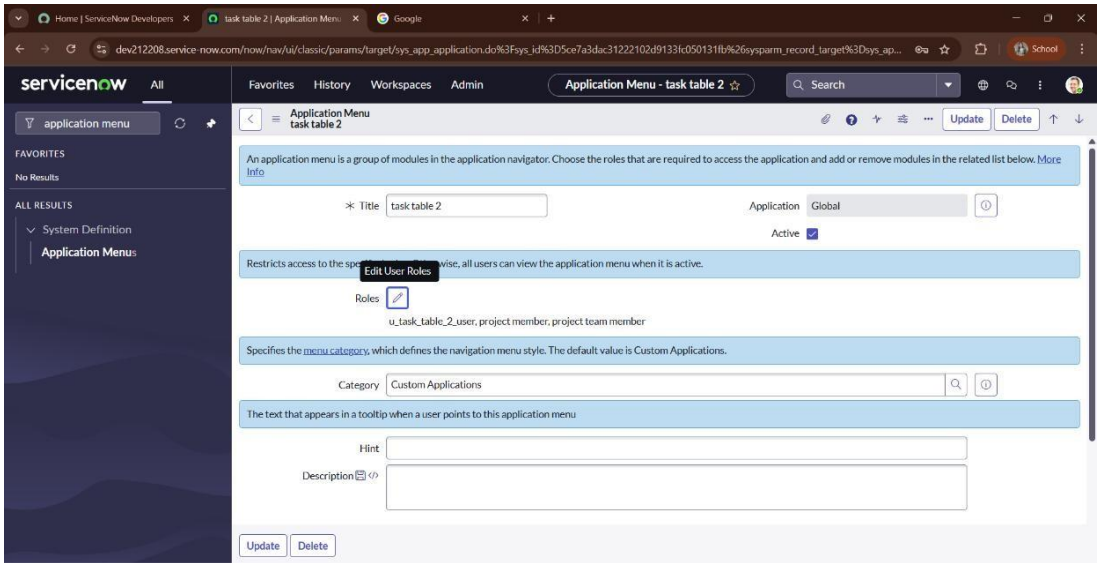


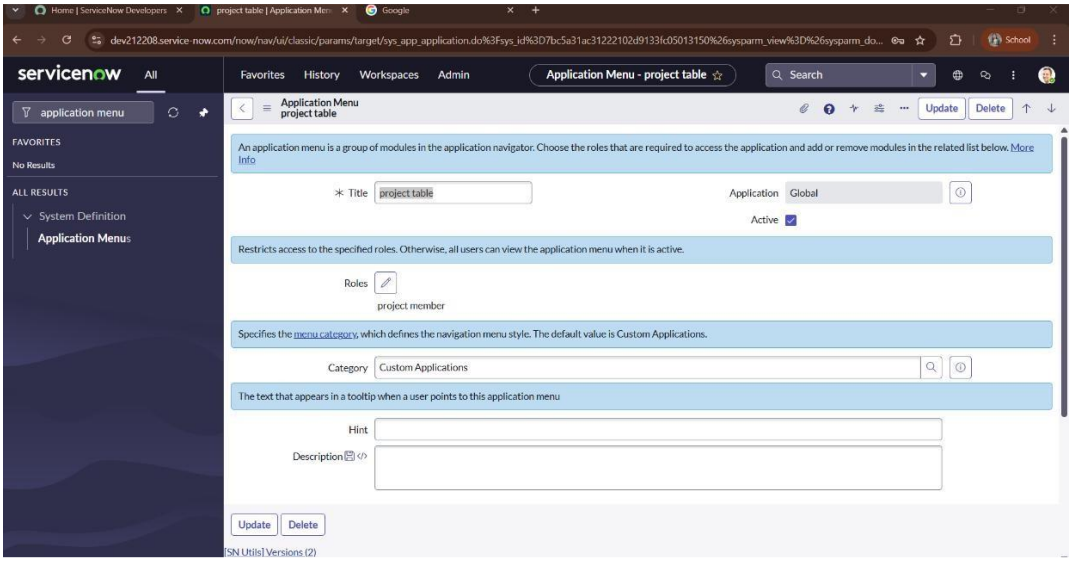

- **Assign roles to bob user**
- Open servicenow
- Click on All >> **search for user**
- Select tables under system definition
- Select the **bob p** user
- Under **team member**
- Click on edit
- Select **team member** and give **table role** and save
- Click on profile icon **Impersonate user to bob**
- We can see the **task table2**



# 7. Application access

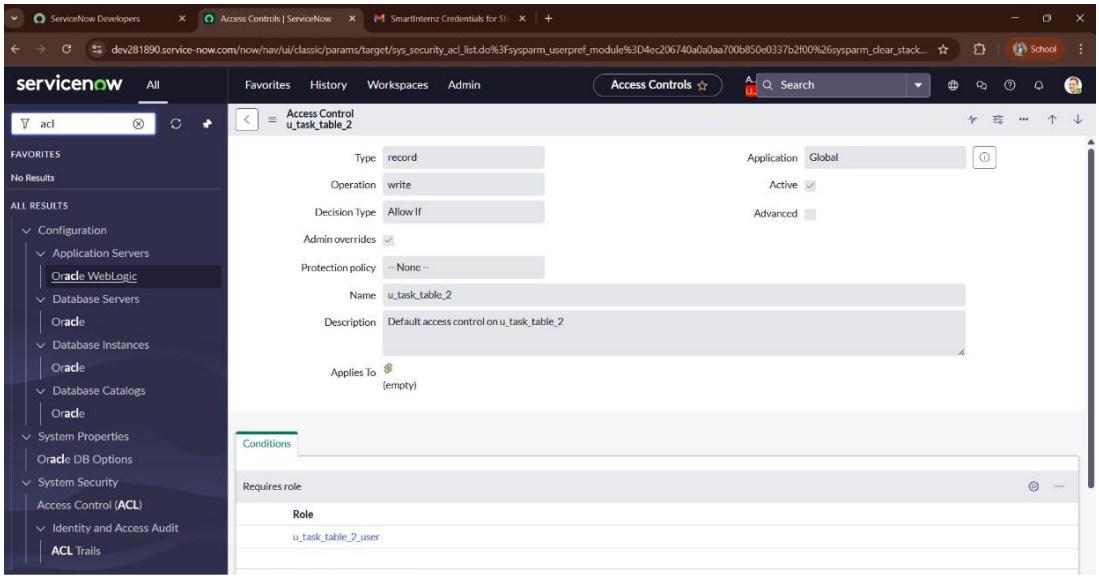
- **Assign table access to application**
- While creating a table it automatically create a application and module for that table
- Go to application navigator search for search project table application
- Click on edit module
- Give project member  roles to that application
- Search for task table2 and click on edit application.
- Give the project member and team member role for task table 2 application.



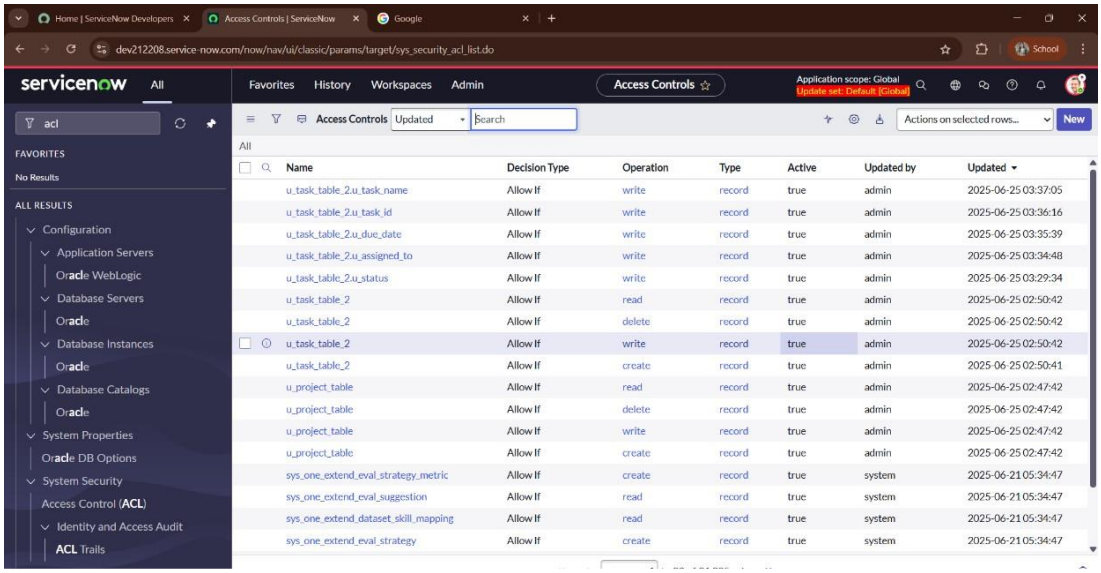



## 8. Access control list

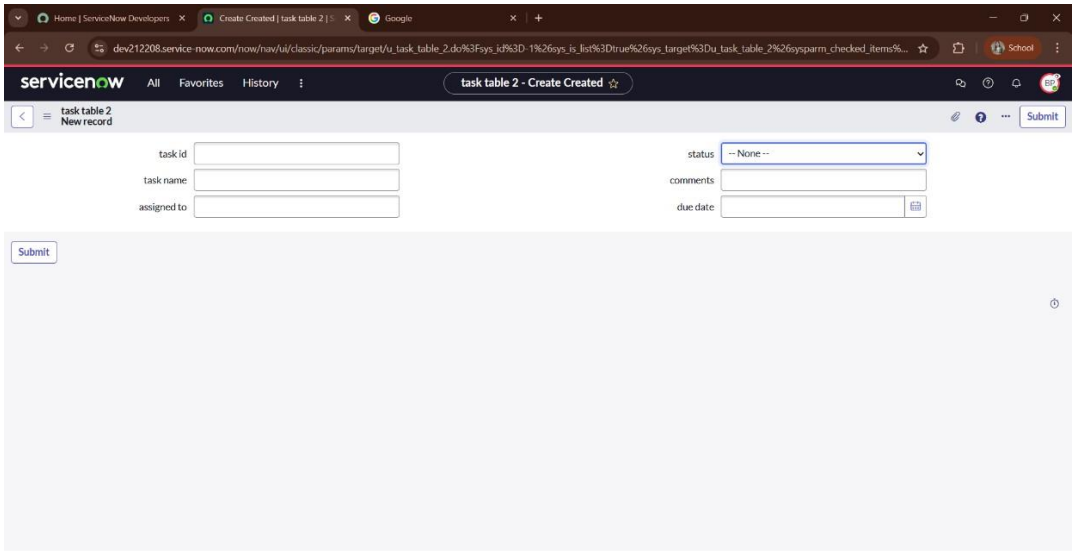
- **Create ACL**
- Open service now.
- Click on All >> **search for ACL**
- Select **Access Control(ACL)** under system security
- Click on elevate role
- Click on new
- Fill the following details to create a new ACL




- Scroll down under requires role
- Double click on insert a new row
- Give task table and team member role
- Click on submit
- Similarly create 4 **acl** for the following fields

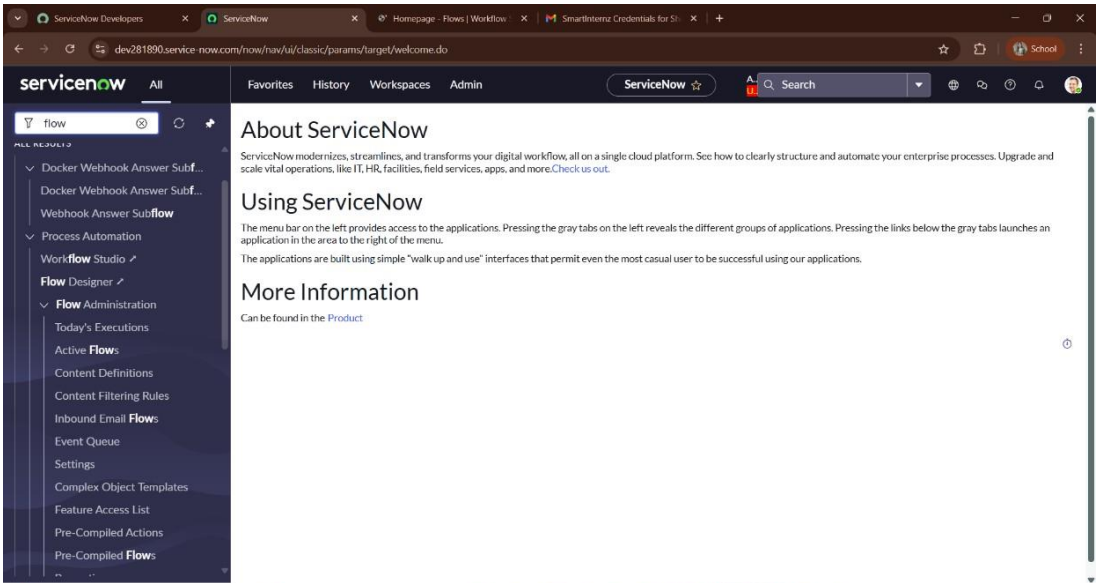


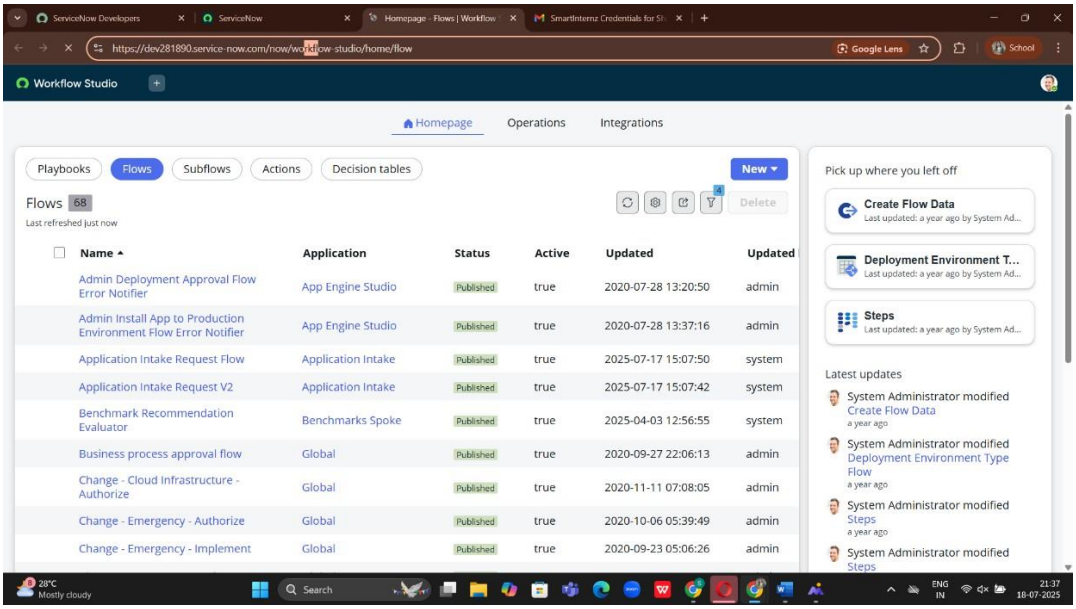

- Click on profile on top right side
- Click on **impersonate user**
- Select **bob** user
- Go to all and select **task table2** in the application menu bar
- Comment and status fields are have the edit access

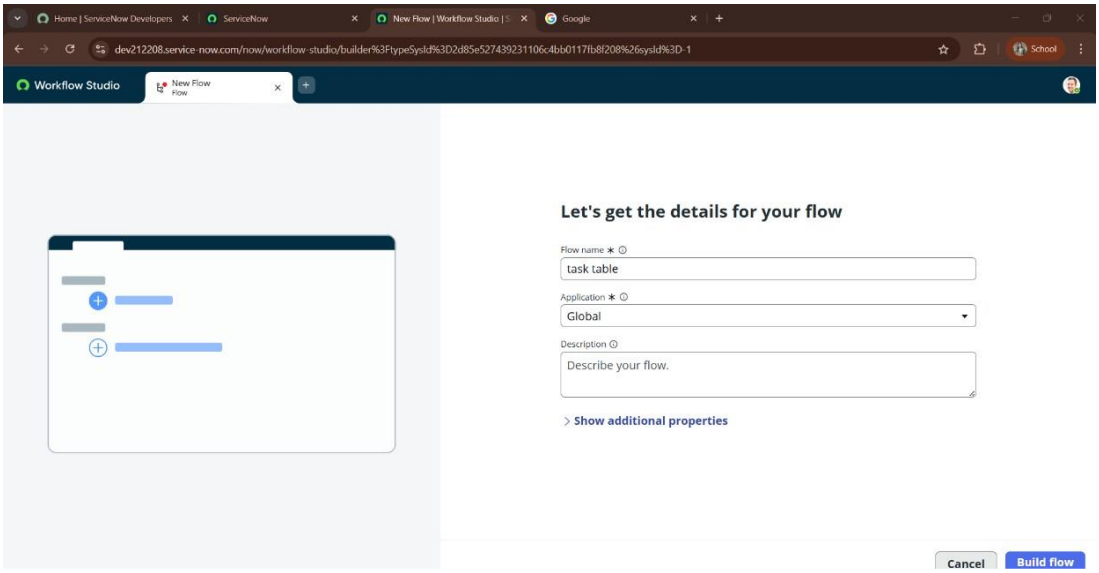


## 9. Flow

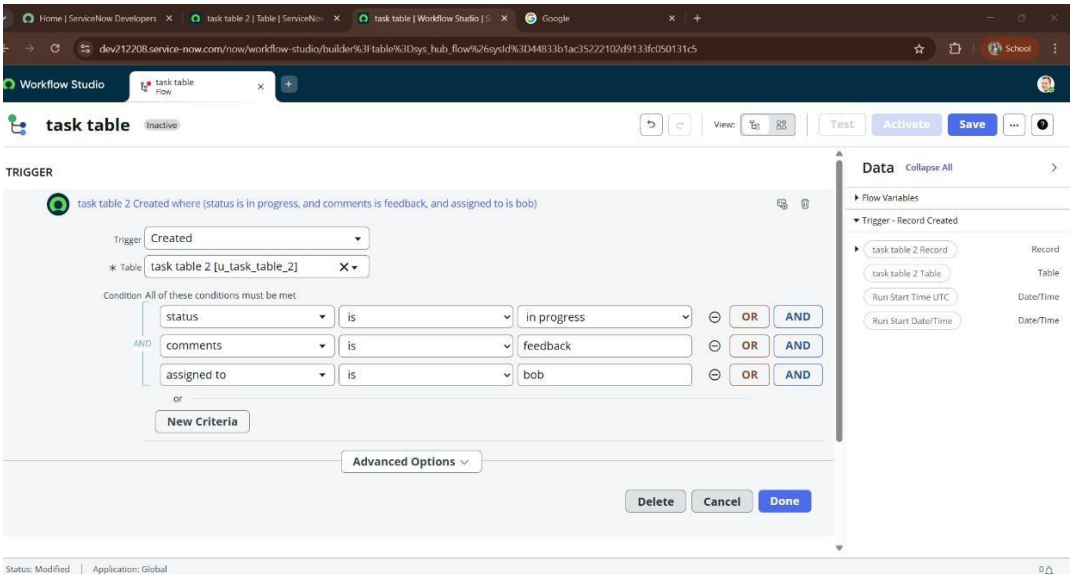
- **Create a Flow to Assign operations ticket to group**
- Open service now.
- Click on All >> search for **Flow Designer**
- Click on Flow Designer under Process Automation.
- After opening Flow Designer Click on new and select Flow.
- Under Flow properties Give Flow Name as " **task table**".
- Application should be **Global**.
- Click build flow.



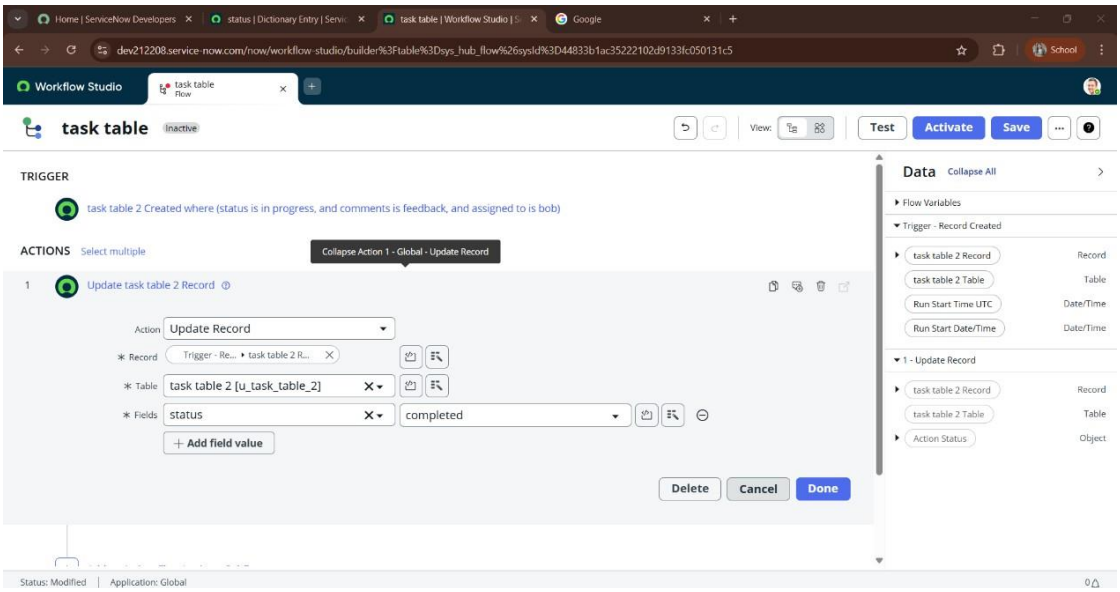





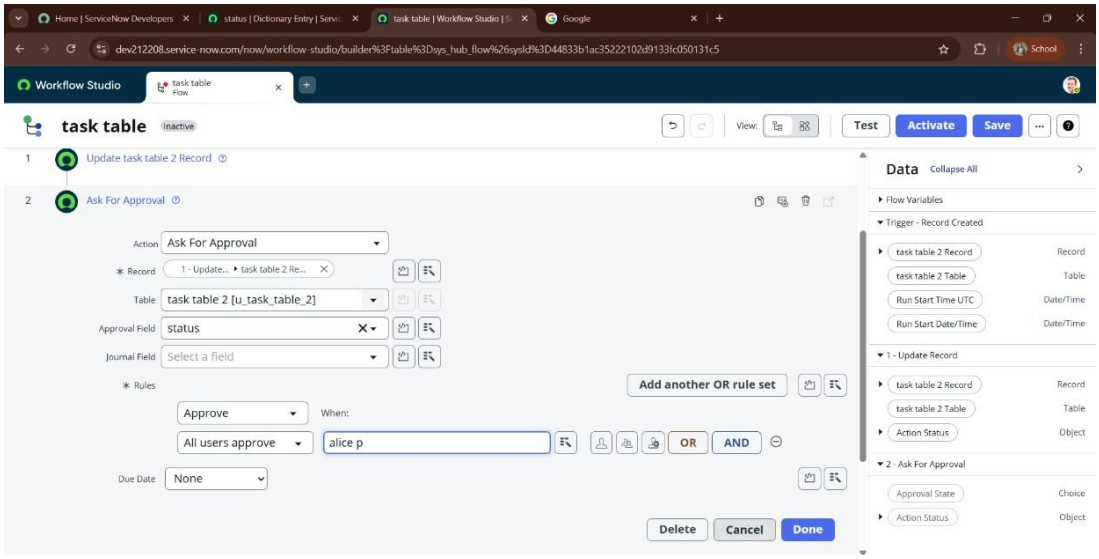

- Define ACL (Employees) Click on Add a trigger
- Select the trigger in that Search for "**create record**" and select that.
- Give the table name as " **task table** ".
- Give the Condition as:
- Field : status Operator :is Value : in progress
- Field : comments Operator :is Value : feedback
- Field : assigned to Operator :is Value : bob
- After that click on Done.



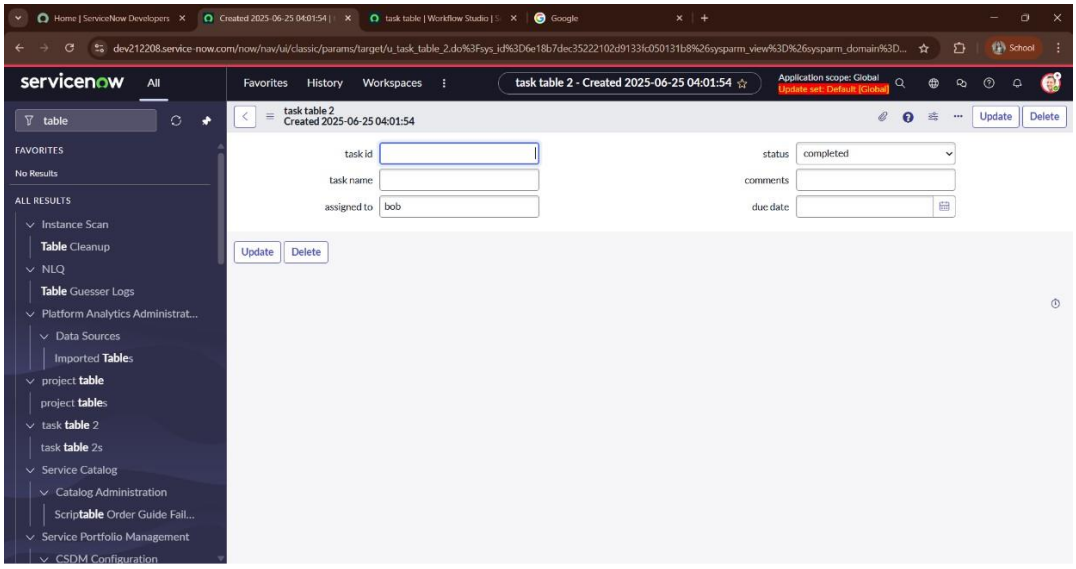
- Click on Add an action.
- Select action in that ,search for " **update records**".
- In Record field drag the fields from the data navigation from Right Side(Data pill)
- Table will be auto assigned after that
- Add fields as "**status**" and value as "**completed**"
- Click on Done.



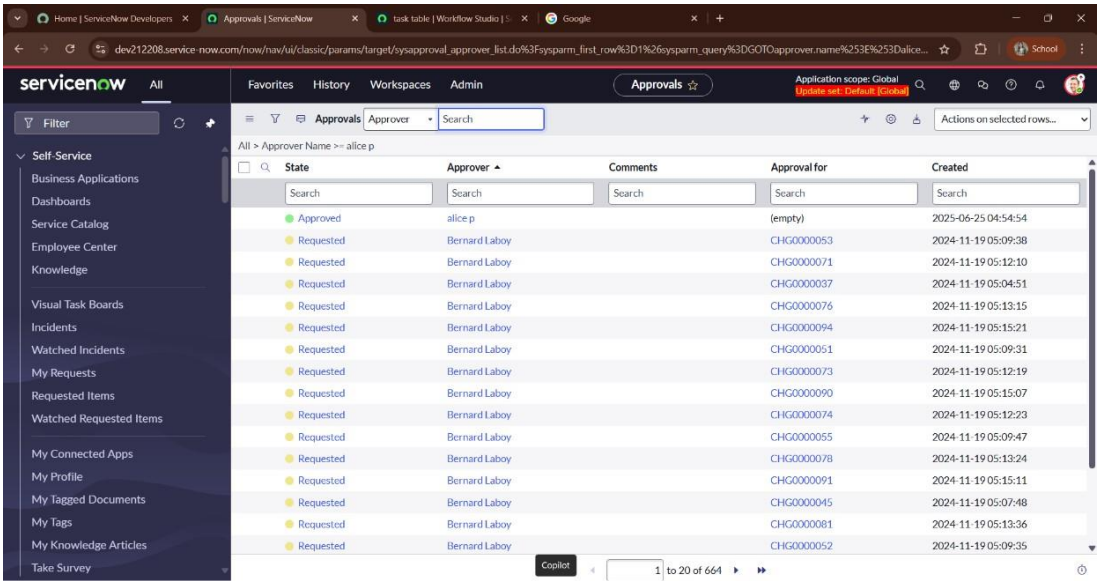

- Now under Actions.
- Click on Add an action.
- Select action in that ,search for " **ask for approval** ".
- In Record field drag the fields from the data navigation from Right side
- Table will be auto assigned after that
- Give the approve field as "**status**"
- Give approver as **alice p**
- Click on Done.

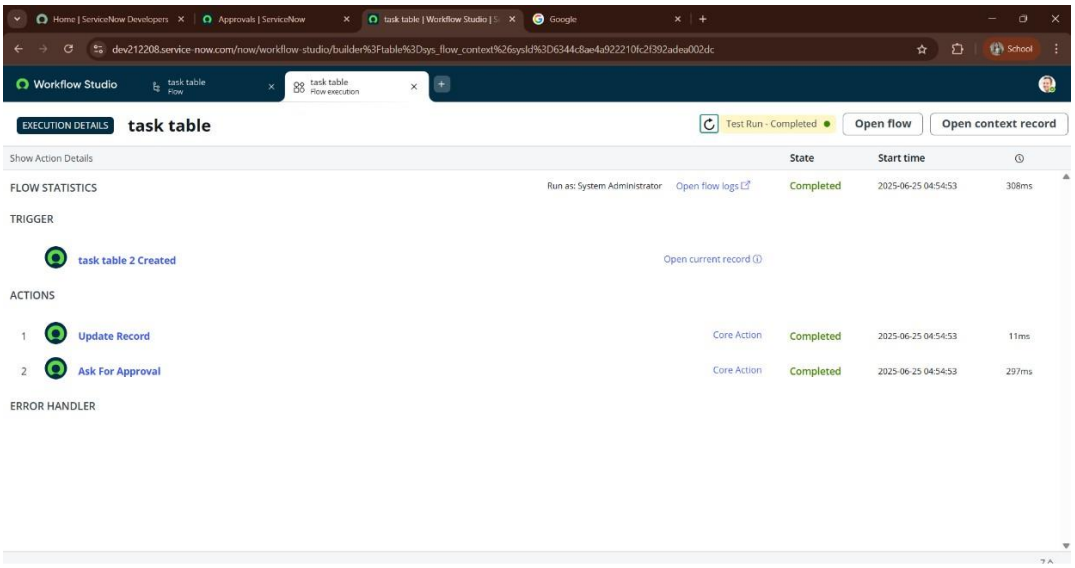



- Go to application navigator search for task table.
- It status field is updated to completed



- Go to application navigator and search for my approval
- Click on my approval under the service desk.
- **Alice p** got approval request then right click on requested then select approved



## 6. Final Conclusion

Effective optimization of user, group, and role management—combined with robust access control and streamlined workflows—is essential for maintaining data security, enforcing compliance, and enhancing operational efficiency. By defining clear roles, automating user provisioning, and applying granular access policies, organizations can minimize risks, reduce administrative overhead, and ensure that the right individuals have access to the right resources at the right time. Ultimately, a well-structured identity and access management strategy supports scalability, improves user experience, and aligns IT processes with business goals.