

Optimizing User, Group, and Role Management with Access Control and Workflows in ServiceNow

Project Documentation Format

1. Introduction

- **Project Name:** Optimizing User, Group, and Role Management with Access Control and Workflows
- **Team ID:** LTVIP2025TMID29880
- **Team Leader:** Sanku Narayana Swami Gari Sharanya Lakshmi
- **Team Members:** Ruddum Suraiah Khaisar, Pesala Raja Sree, Chagal Samreen, P Umme Suliem Lubaba

2. 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.

3. 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.

4. 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.

5. 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.

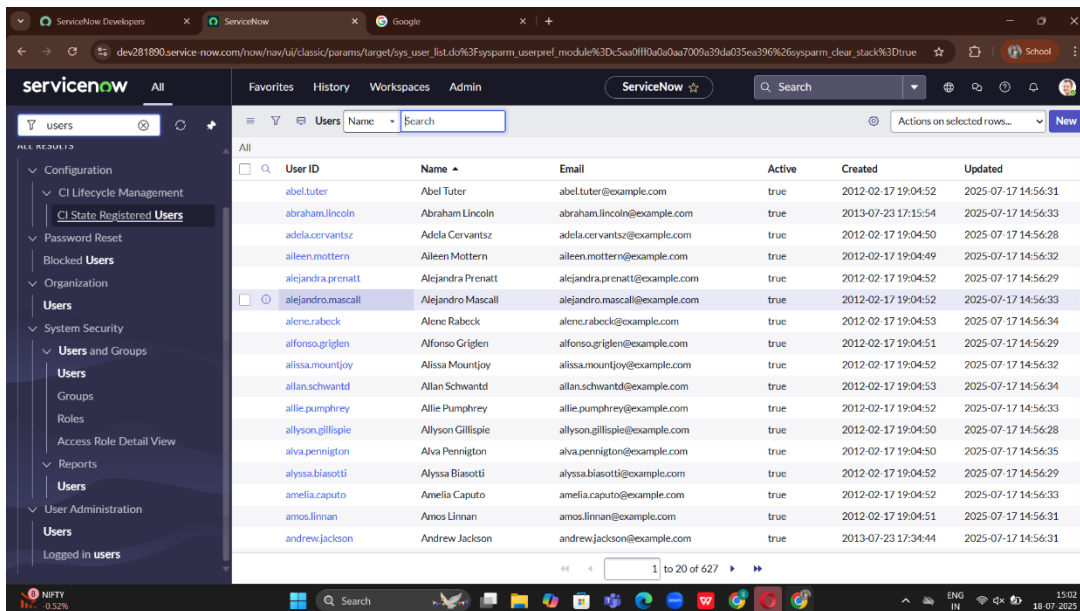
3. Task Allocation:

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

6. Project Design Phase

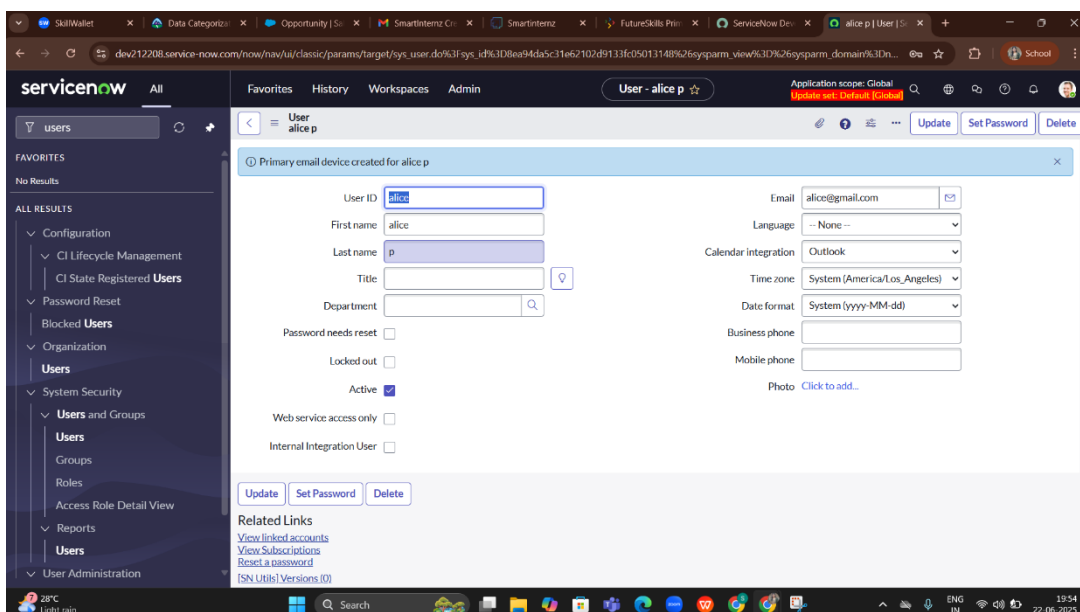
1. Create Users

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



User ID	Name	Email	Active	Created	Updated
abel.tuter	Abel Tuter	abel.tuter@example.com	true	2012-02-17 19:04:52	2025-07-17 14:56:31
abraham.lincoln	Abraham Lincoln	abraham.lincoln@example.com	true	2013-07-23 17:15:54	2025-07-17 14:56:33
adela.cervantsz	Adela Cervantsz	adela.cervantsz@example.com	true	2012-02-17 19:04:50	2025-07-17 14:56:28
aleen.mottern	Aleen Mottern	aleen.mottern@example.com	true	2012-02-17 19:04:49	2025-07-17 14:56:32
alejandra.prenatt	Alejandra Prenatt	alejandra.prenatt@example.com	true	2012-02-17 19:04:52	2025-07-17 14:56:29
alejandro.mascall	Alejandro Mascall	alejandro.mascall@example.com	true	2012-02-17 19:04:52	2025-07-17 14:56:33
alene.rabeck	Alene Rabeck	alene.rabeck@example.com	true	2012-02-17 19:04:53	2025-07-17 14:56:34
alfonso.griglen	Alfonso Griglen	alfonso.griglen@example.com	true	2012-02-17 19:04:51	2025-07-17 14:56:29
alissa.mountjoy	Alissa Mountjoy	alissa.mountjoy@example.com	true	2012-02-17 19:04:52	2025-07-17 14:56:32
allan.schwandt	Allan Schwandt	allan.schwandt@example.com	true	2012-02-17 19:04:53	2025-07-17 14:56:34
allie.pumphrey	Allie Pumphrey	allie.pumphrey@example.com	true	2012-02-17 19:04:52	2025-07-17 14:56:33
allyson.gillisple	Allyson Gillisple	allyson.gillisple@example.com	true	2012-02-17 19:04:50	2025-07-17 14:56:28
alva.pennigton	Alva Pennigton	alva.pennigton@example.com	true	2012-02-17 19:04:50	2025-07-17 14:56:35
alyssa.biasotti	Alyssa Biasotti	alyssa.biasotti@example.com	true	2012-02-17 19:04:52	2025-07-17 14:56:29
amelia.caputo	Amelia Caputo	amelia.caputo@example.com	true	2012-02-17 19:04:52	2025-07-17 14:56:33
amos.linnan	Amos Linnan	amos.linnan@example.com	true	2012-02-17 19:04:51	2025-07-17 14:56:31
andrew.jackson	Andrew Jackson	andrew.jackson@example.com	true	2013-07-23 17:34:44	2025-07-17 14:56:31

- Fill the following details to create a new users
- Create a user named as “alice p”.



Application scope: Global
Update set: Default [Global]

Primary email device created for alice p

User ID:
First name:
Last name:
Title:
Department:
Email:
Language:
Calendar integration:
Time zone:
Date format:
Business phone:
Mobile phone:
Photo: [Click to add...](#)

Active: ☒
Web service access only: ☐
Internal Integration User: ☐

Update Set Password Delete

Related Links
[View linked accounts](#)
[View Subscriptions](#)
[Reset a password](#)
[\[SN Utils\] Versions \(0\)](#)

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

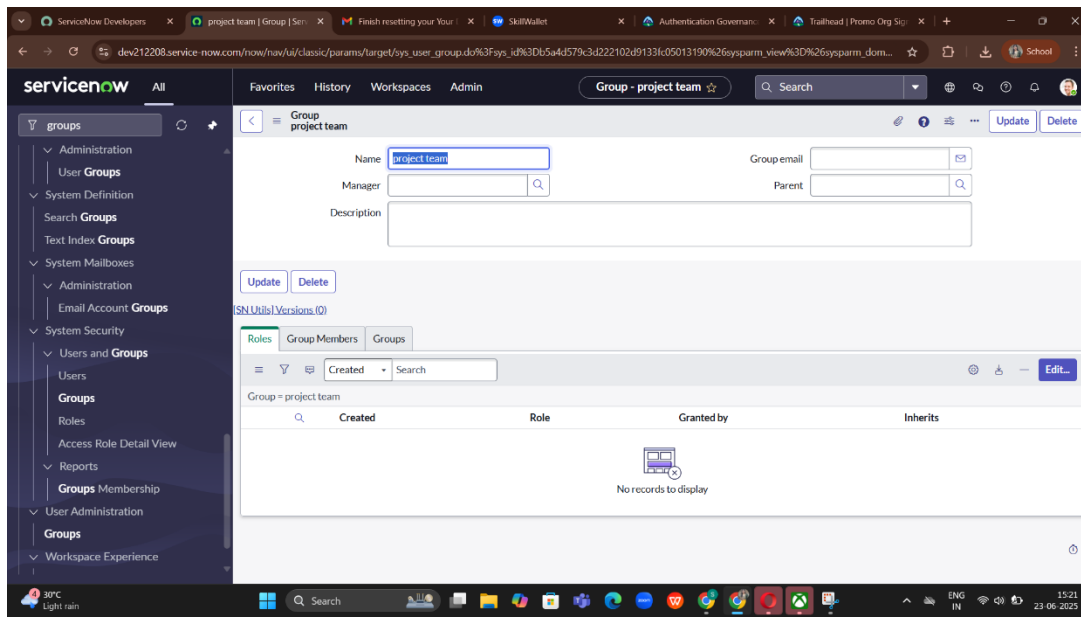
The screenshot shows the ServiceNow user creation interface. The left sidebar contains a navigation menu with categories like Configuration, Password Reset, Organization, System Security, Reports, and User Administration. The main content area is titled 'User - Bob p' and contains a form with the following fields:

- User ID:** bob
- First name:** Bob
- Last name:** p
- Title:** (empty)
- Department:** (empty)
- Email:** bob@gmail.com
- Language:** None
- Calendar integration:** Outlook
- Time zone:** System (America/Los Angeles)
- Date format:** System (yyyy-MM-dd)
- Business phone:** (empty)
- Mobile phone:** (empty)
- Photo:** Click to add...
- Password needs reset:** ☐
- Locked out:** ☐
- Active:** ☒
- Web service access only:** ☐
- Internal Integration User:** ☐

At the bottom of the form are buttons for 'Update', 'Set Password', and 'Delete'. Below the form, there are 'Related Links' including 'View linked accounts', 'View Subscriptions', 'Reset a password', and 'ISN Links | Versions (0)'.

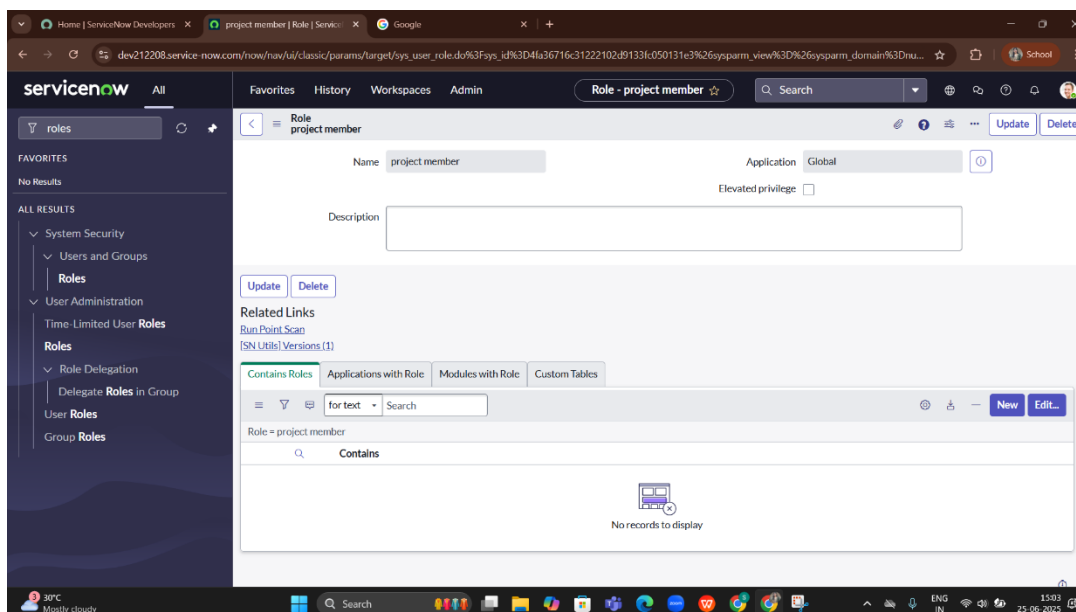
2. Create Groups

- 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

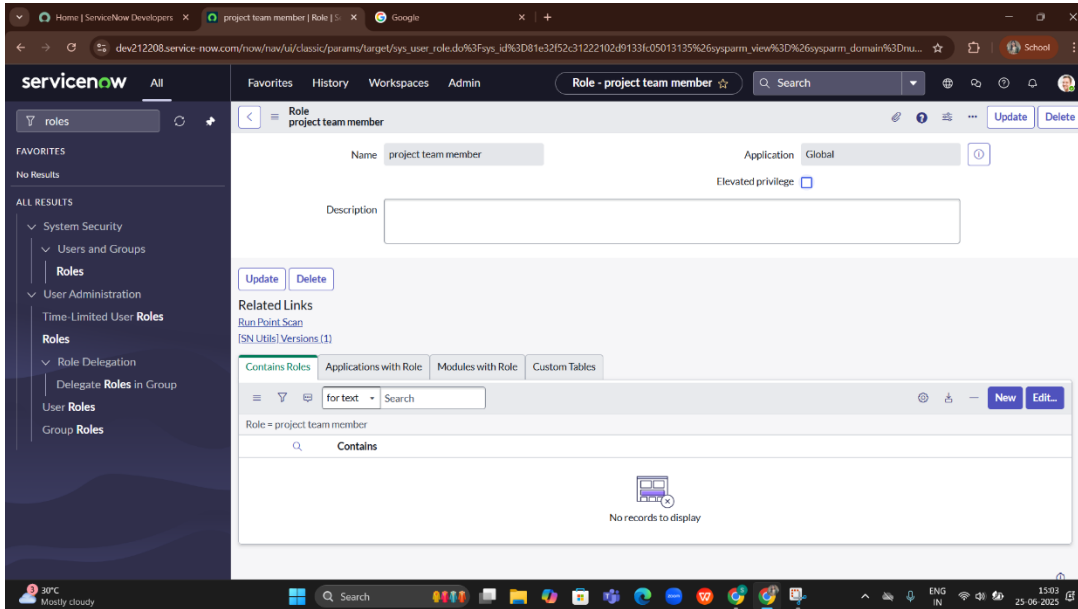


3. Create Roles

- 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

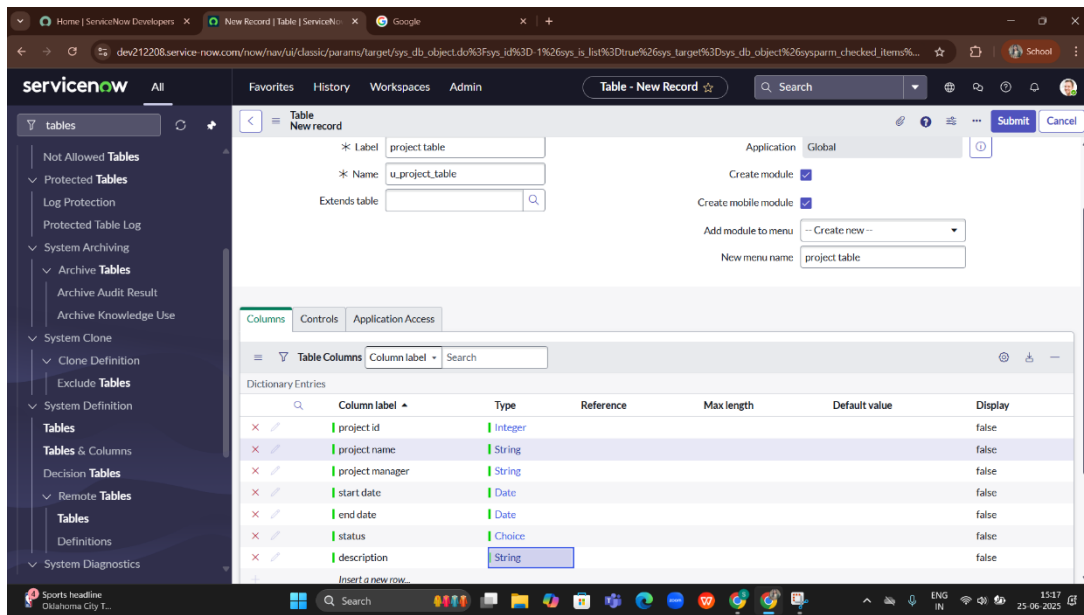


- **Create one more role:**
- Create another role with the following details
- Click on submit

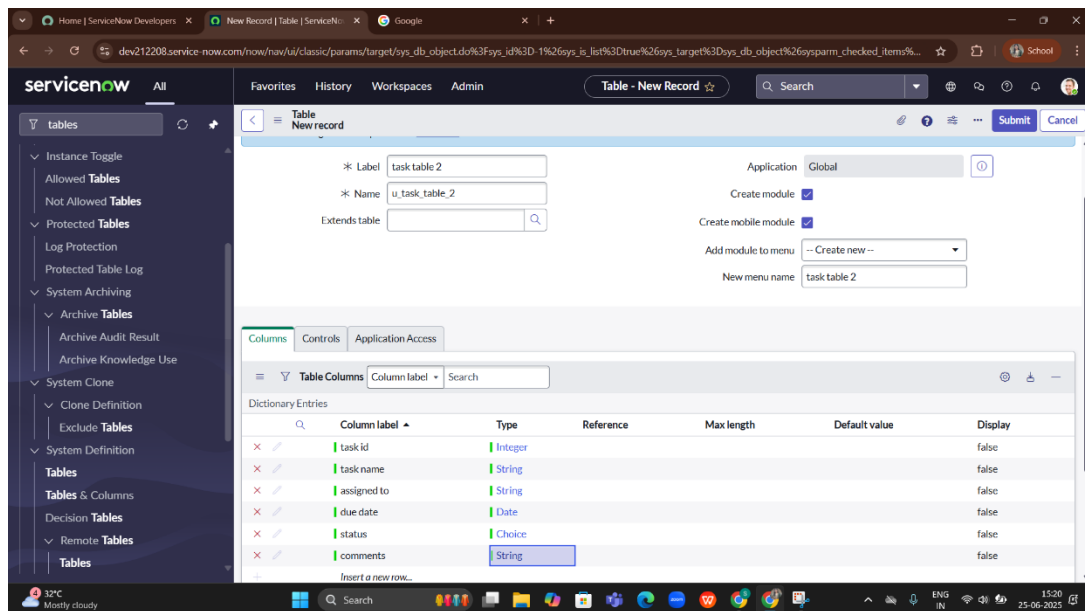


4. Create Tables

- 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

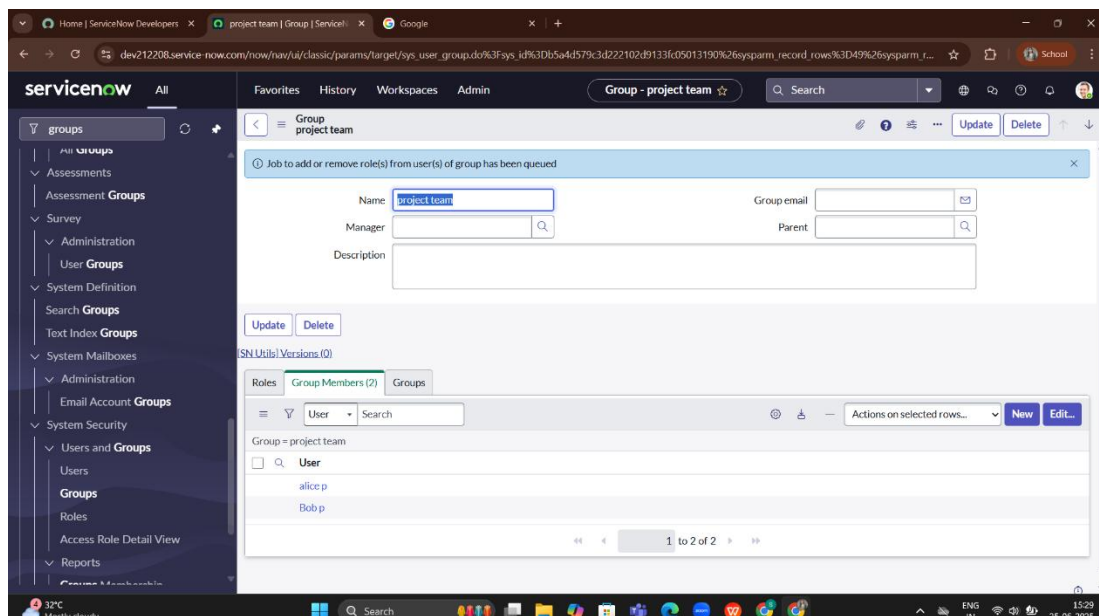


- Click on submit
- **Create one more table:**
- Create another table as:task table 2 and fill with following details.
- Click on **submit**.



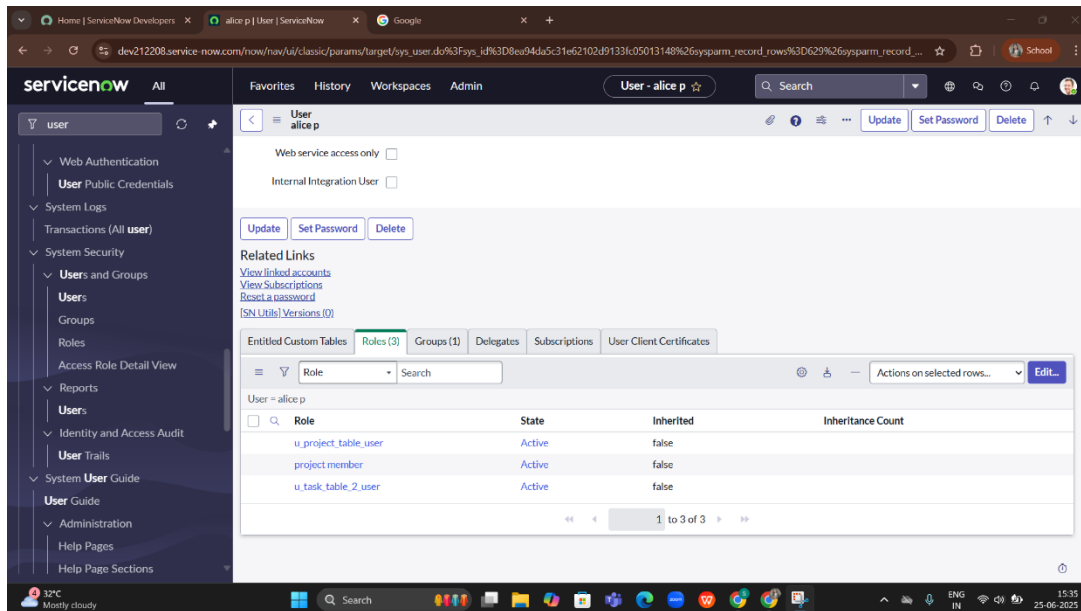
5. Assign users to project team group

- 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.

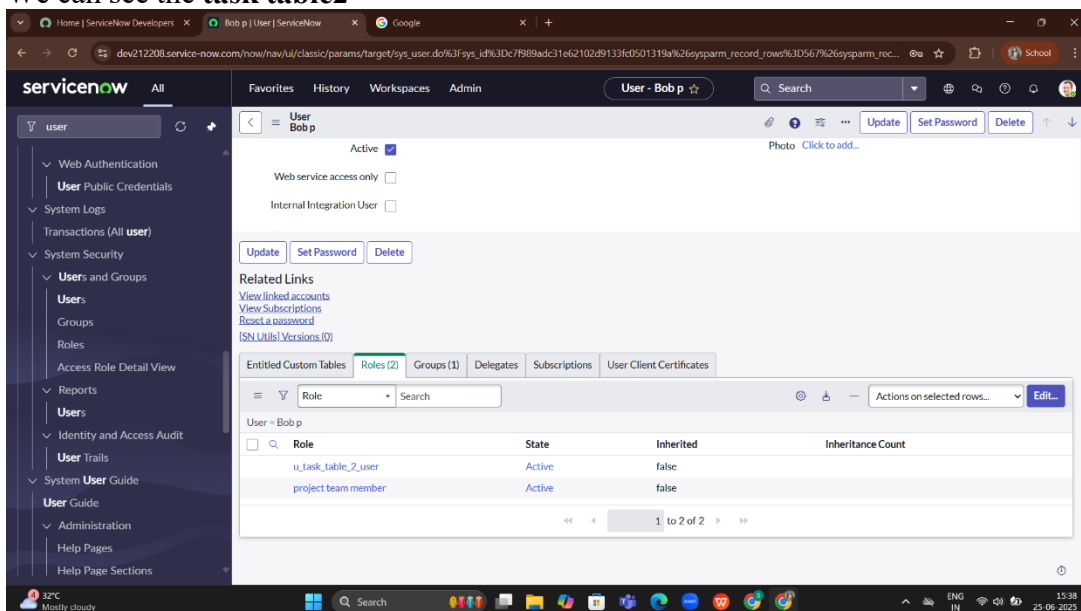


6. Assign roles to users

- **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.

The screenshot shows the ServiceNow interface for editing the 'task table 2' application menu. The left sidebar contains the 'application menu' search bar and a list of results under 'System Definition' including 'Application Menus'. The main content area has the following fields:

- Title:** task table 2
- Application:** Global
- Active:** ☒
- Restricts access to the specified roles. Otherwise, all users can view the application menu when it is active.** (with an 'Edit User Roles' link)
- Roles:** u_task_table_2_user, project member, project team member
- Specifies the menu category, which defines the navigation menu style. The default value is Custom Applications.**
- Category:** Custom Applications
- The text that appears in a tooltip when a user points to this application menu**
- Hint:** (empty text box)
- Description:** (empty text box)

At the bottom are 'Update' and 'Delete' buttons, and a link to 'SN UIs | Versions (1)'.

The screenshot shows the ServiceNow interface for editing the 'project table' application menu. The left sidebar contains the 'application menu' search bar and a list of results under 'System Definition' including 'Application Menu:'. The main content area has the following fields:

- Title:** project table
- Application:** Global
- Active:** ☒
- Restricts access to the specified roles. Otherwise, all users can view the application menu when it is active.** (with an 'Edit User Roles' link)
- Roles:** project member
- Specifies the menu category, which defines the navigation menu style. The default value is Custom Applications.**
- Category:** Custom Applications
- The text that appears in a tooltip when a user points to this application menu**
- Hint:** (empty text box)
- Description:** (empty text box)

At the bottom are 'Update' and 'Delete' buttons, and a link to 'SN UIs | Versions (2)'.

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

The screenshot shows the ServiceNow interface for creating an Access Control (ACL) record. The left sidebar displays the navigation menu with 'Access Control (ACL)' selected. The main form contains the following fields:

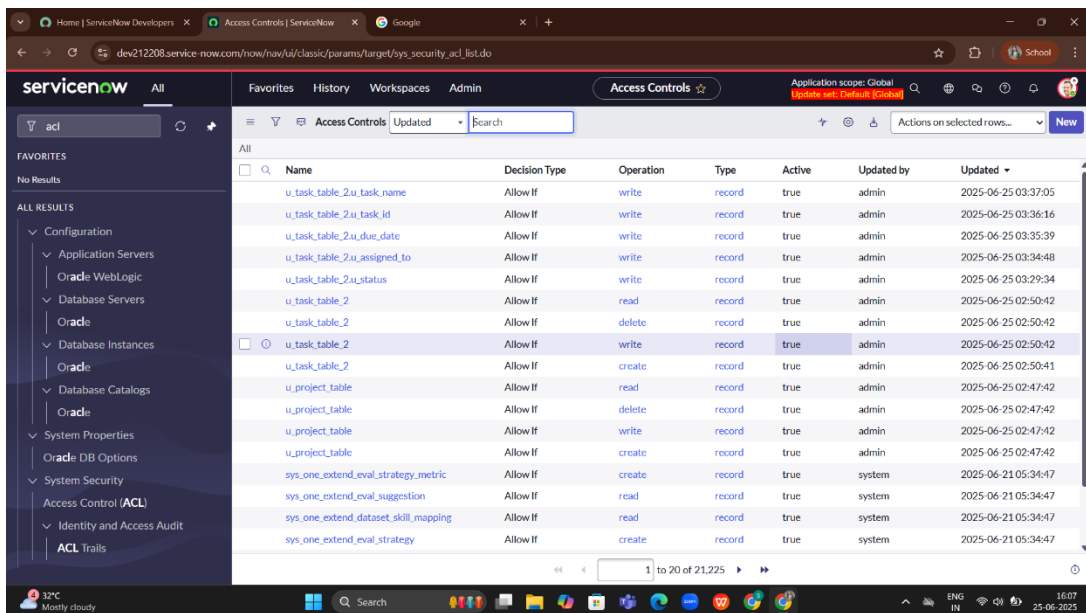
- Type:** record
- Operation:** write
- Decision Type:** Allow If
- Application:** Global
- Active:** ☒
- Advanced:** ☐
- Admin overrides:** ☒
- Protection policy:** -- None --
- Name:** u_task_table_2
- Description:** Default access control on u_task_table_2
- Applies to:** (empty)

Below the main form, there is a 'Requires role' section with a table:

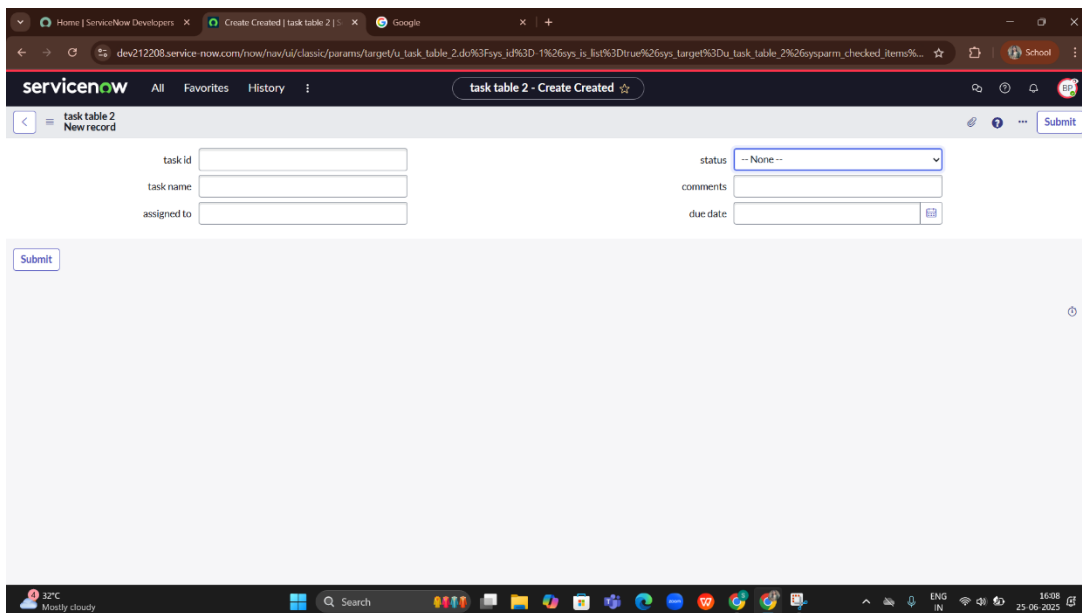
Role
u_task_table_2_user

At the bottom, there is a 'Security Attribute Condition' section.

- 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

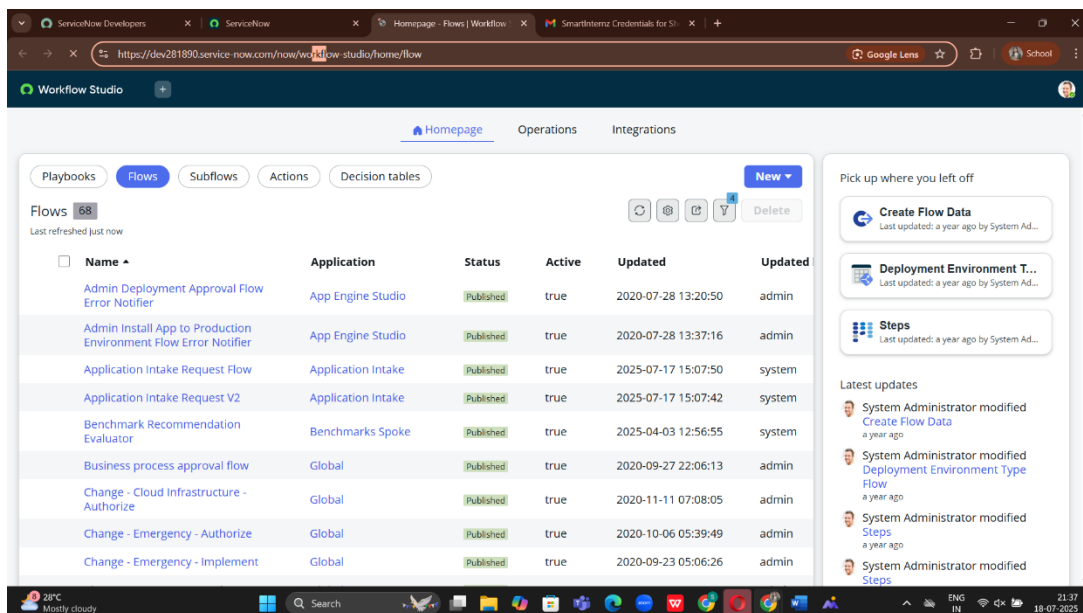
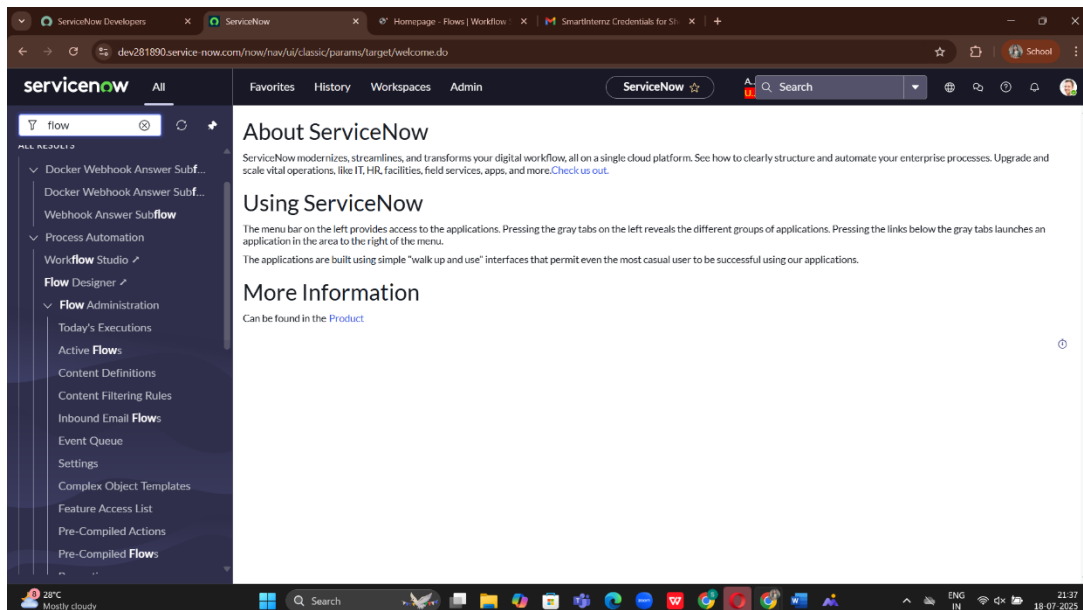


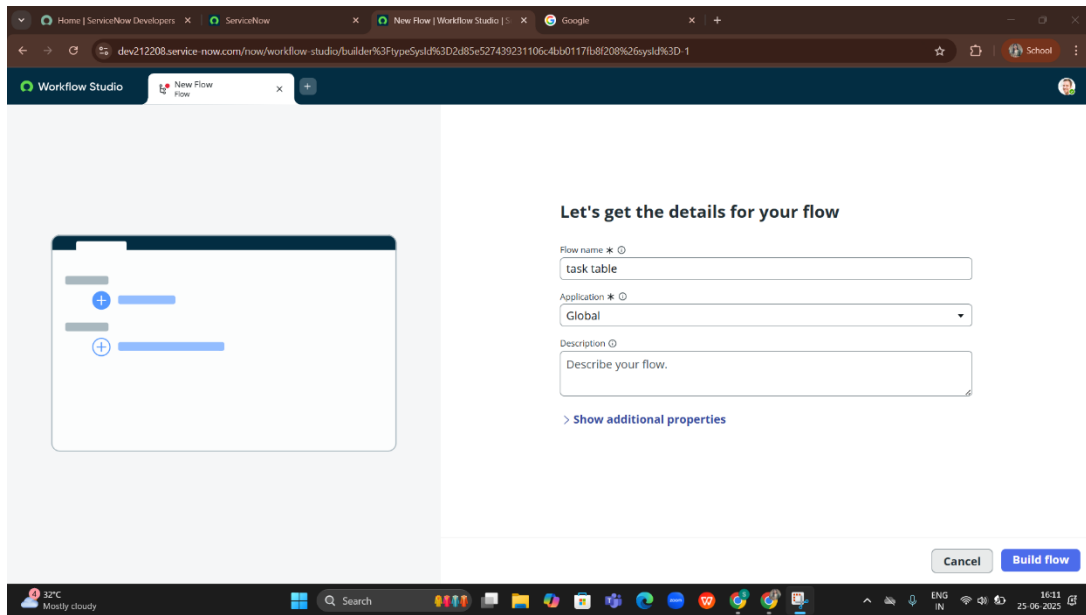
- Click on profile on top right side
- Click on **impersonate user**
- Select **bob** user
- Go to all and select **task table2** in the application menu bar
- Comment and status fields are have the edit access



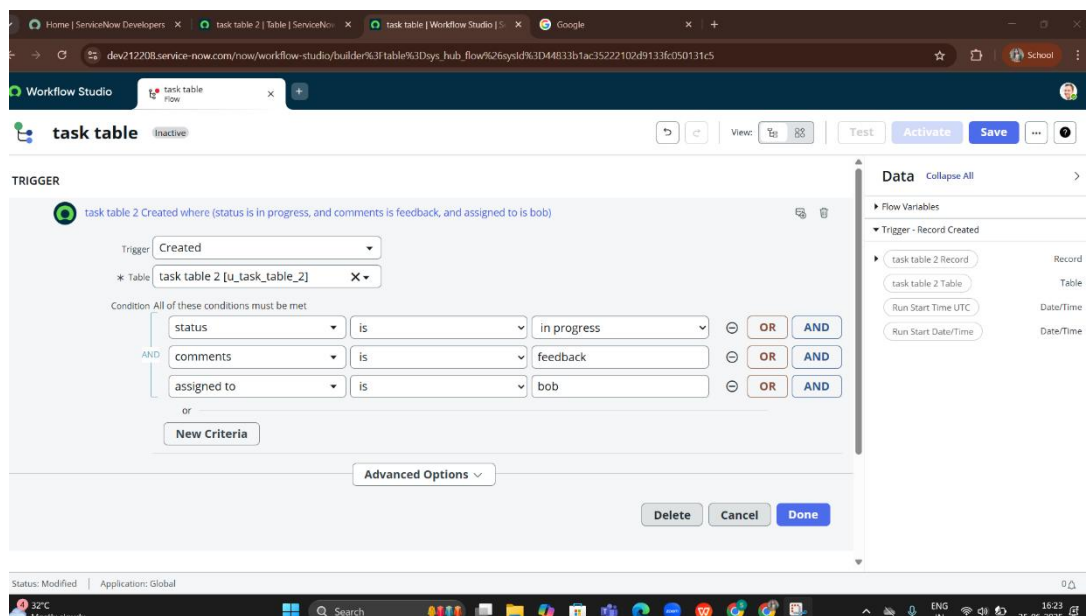
9. Flow

- **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.

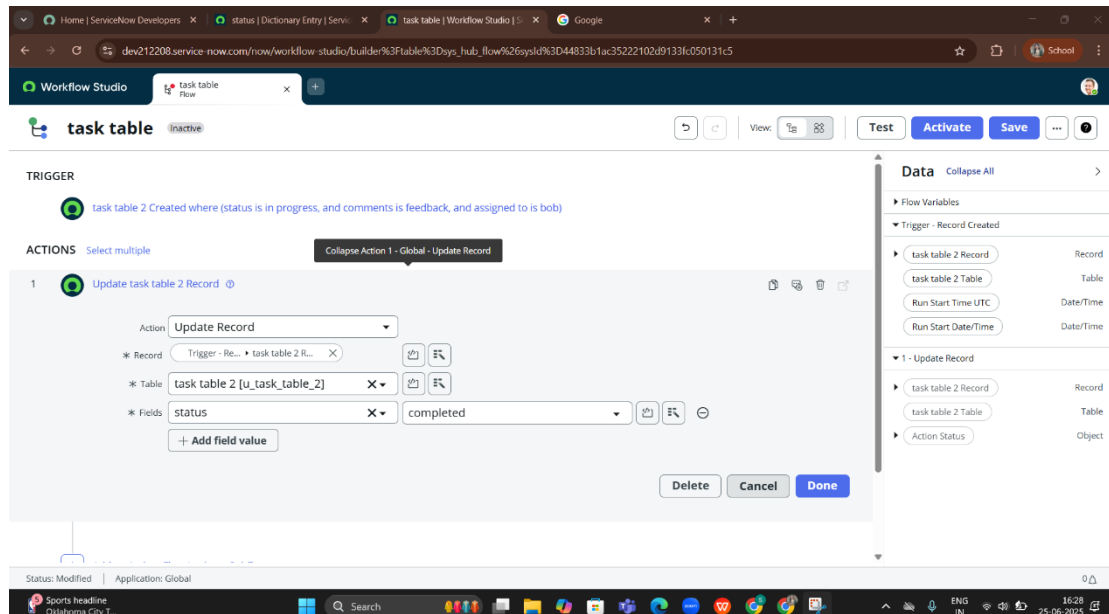




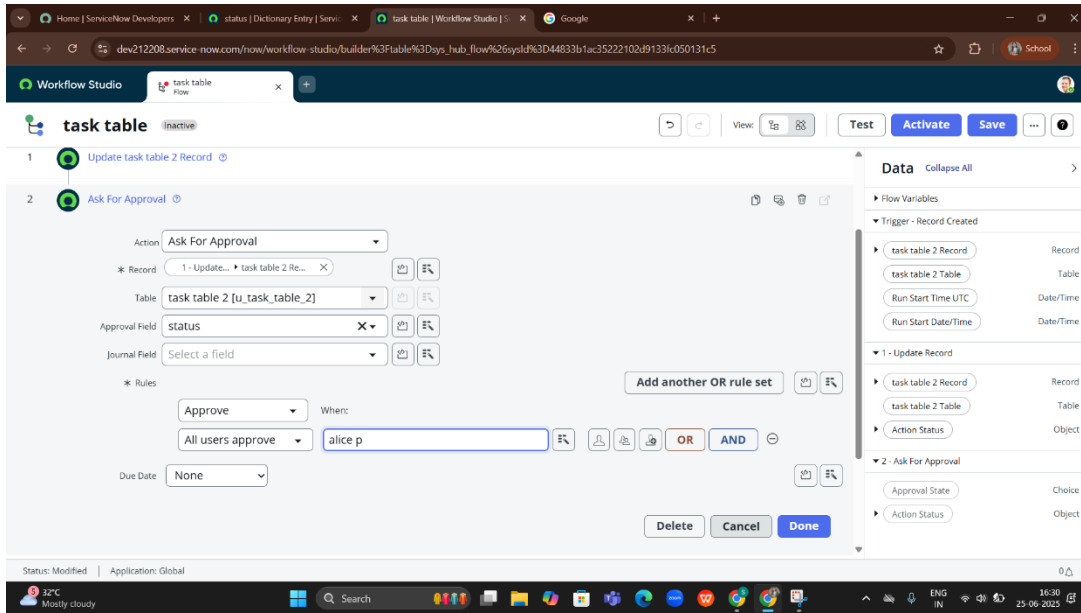
- Define ACL (Employees) Click on Add a trigger
- Select the trigger in that Search for “**create record**” and select that.
- Give the table name as “**task table**”.
- Give the Condition as:
- Field : status Operator :is Value : in progress
- Field : comments Operator :is Value : feedback
- Field :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



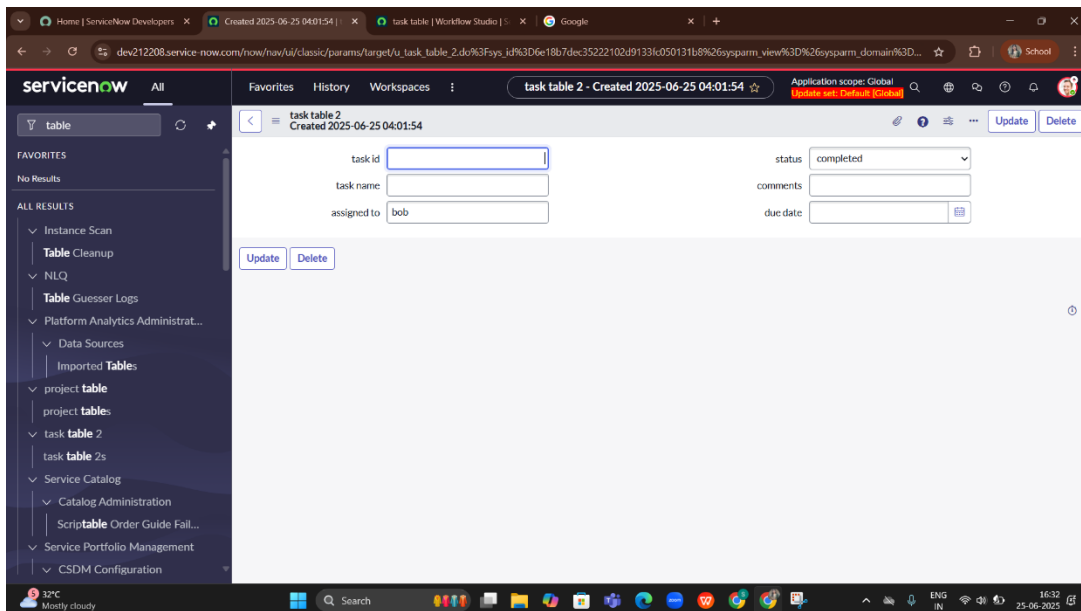
- Click on Add an action.
- Select action in that ,search for “ **update records**”.
- In Record field drag the fields from the data navigation from Right Side(Data pill)
- Table will be auto assigned after that
- Add fields as “**status**” and value as “**completed**”
- Click on Done.



- 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

The screenshot shows the ServiceNow 'Approvals' page. The left sidebar contains the 'Self-Service' menu with options like 'Business Applications', 'Dashboards', 'Service Catalog', 'Employee Center', 'Knowledge', 'Visual Task Boards', 'Incidents', 'Watched Incidents', 'My Requests', 'Requested Items', 'Watched Requested Items', 'My Connected Apps', 'My Profile', 'My Tagged Documents', 'My Tags', 'My Knowledge Articles', and 'Take Survey'. The main content area displays a table of approval requests for the user 'alice p'.

State	Approver	Comments	Approval for	Created
Approved	alice p		(empty)	2025-06-25 04:54:54
Requested	Bernard Laboy		CHG0000053	2024-11-19 05:09:38
Requested	Bernard Laboy		CHG0000071	2024-11-19 05:12:10
Requested	Bernard Laboy		CHG0000037	2024-11-19 05:04:51
Requested	Bernard Laboy		CHG0000076	2024-11-19 05:13:15
Requested	Bernard Laboy		CHG0000094	2024-11-19 05:15:21
Requested	Bernard Laboy		CHG0000051	2024-11-19 05:09:31
Requested	Bernard Laboy		CHG0000073	2024-11-19 05:12:19
Requested	Bernard Laboy		CHG0000090	2024-11-19 05:15:07
Requested	Bernard Laboy		CHG0000074	2024-11-19 05:12:23
Requested	Bernard Laboy		CHG0000055	2024-11-19 05:09:47
Requested	Bernard Laboy		CHG0000078	2024-11-19 05:13:24
Requested	Bernard Laboy		CHG0000091	2024-11-19 05:15:11
Requested	Bernard Laboy		CHG0000045	2024-11-19 05:07:48
Requested	Bernard Laboy		CHG0000081	2024-11-19 05:13:36
Requested	Bernard Laboy		CHG0000052	2024-11-19 05:09:35

The screenshot shows the ServiceNow 'Workflow Studio' page for a flow named 'task table'. The flow is in a 'Completed' state. The 'EXECUTION DETAILS' section shows the flow was run as 'System Administrator' on '2025-06-25 04:54:53' and took '308ms' to complete. The 'FLOW STATISTICS' section shows the flow was triggered by 'task table 2 Created'. The 'ACTIONS' section shows two actions: 'Update Record' (Core Action, Completed, 11ms) and 'Ask For Approval' (Core Action, Completed, 297ms). The 'ERROR HANDLER' section is empty.

7. 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.