

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.

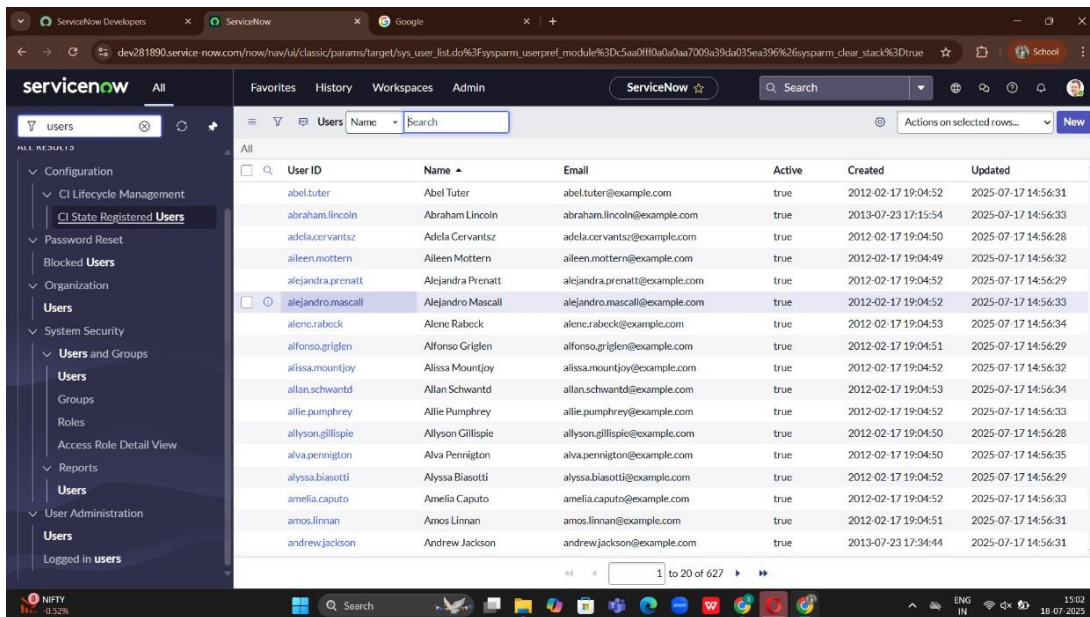
3. Task Allocation:

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

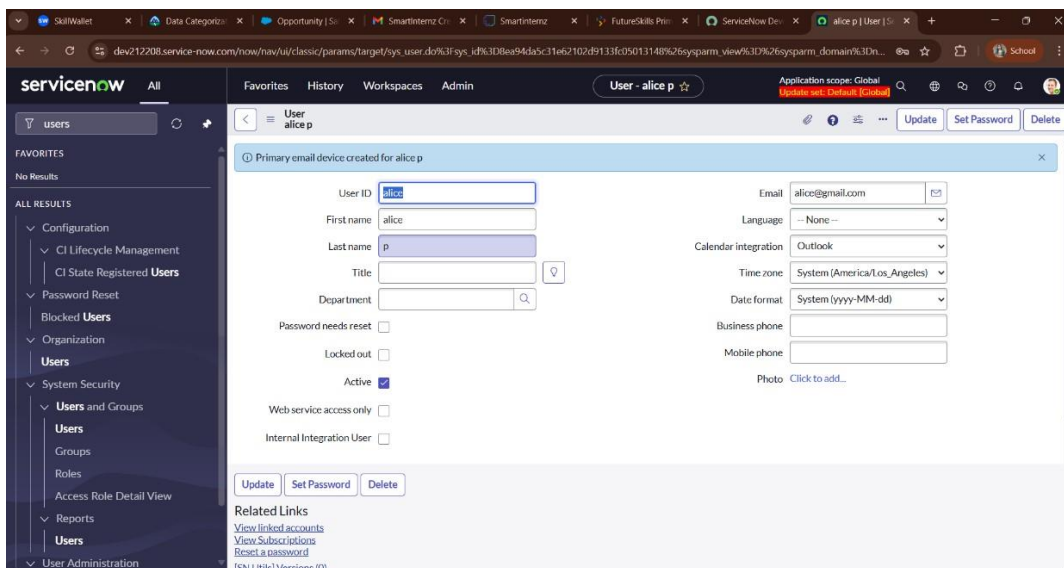
5. Project Design Phase

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”.

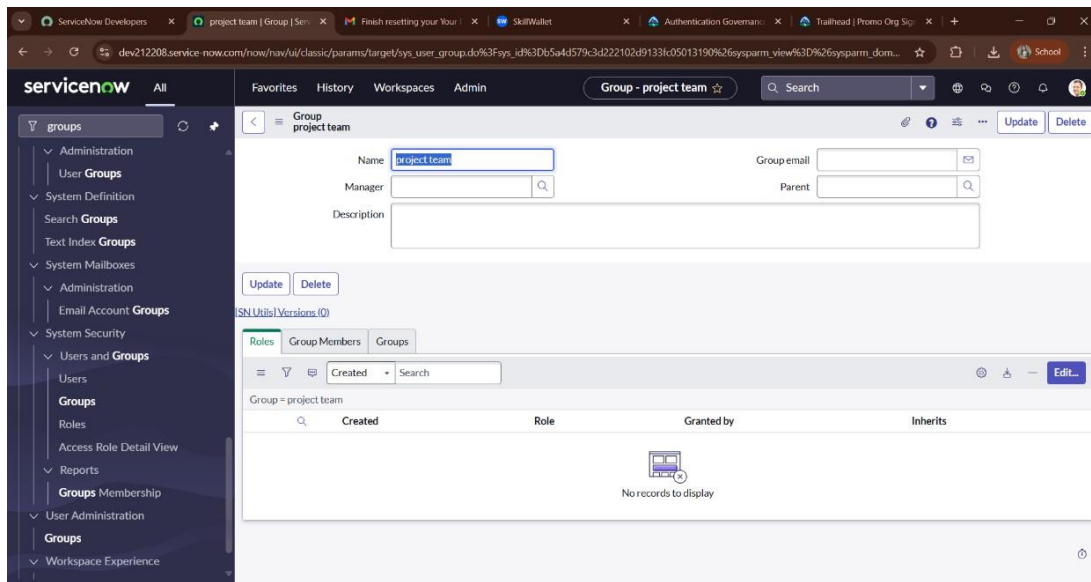


- **Create one more user:**
- Create another user with the following details
- Username: “bob p”.
- Click on submit.

The screenshot shows the ServiceNow User Administration interface. The left sidebar contains a navigation menu with categories like Configuration, Password Reset, Blocked Users, Organization, System Security, and Reports. The main content area displays the details for a user named "Bob p". The user ID is "bob", and the email is "bob@gmail.com". The user is currently active. The form includes fields for First name, Last name, Title, Department, Password needs reset, Locked out, Active, Web service access only, and Internal Integration User. There are also dropdown menus for Language, Calendar integration, Time zone, and Date format. At the bottom, there are buttons for "Update", "Set Password", and "Delete".

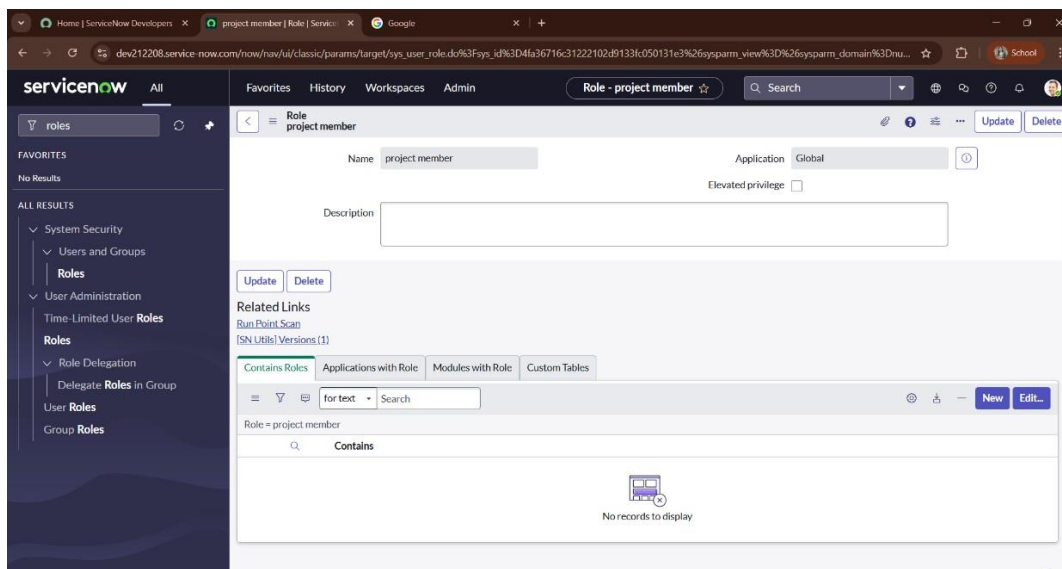
2. Create Groups

- 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

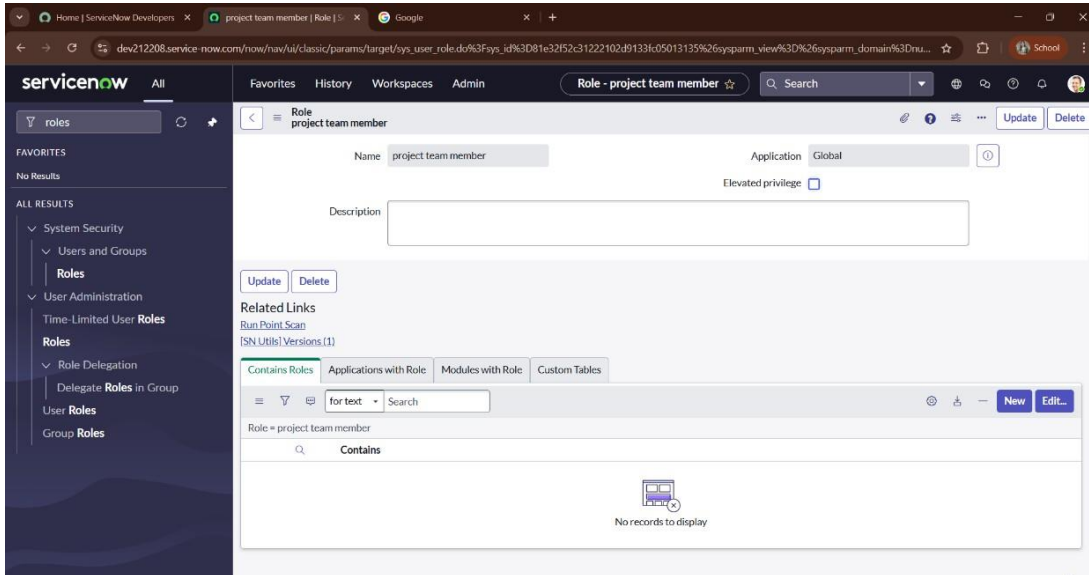


3. Create Roles

- 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

The screenshot shows the 'Table - New Record' form in ServiceNow. The left sidebar contains a navigation menu with options like 'Not Allowed Tables', 'Protected Tables', 'Log Protection', 'Protected Table Log', 'System Archiving', 'Archive Tables', 'Archive Audit Result', 'Archive Knowledge Use', 'System Clone', 'Clone Definition', 'Exclude Tables', 'System Definition', 'Tables', 'Tables & Columns', 'Decision Tables', 'Remote Tables', 'Definitions', and 'System Diagnostics'. The main form area has fields for 'Label' (project table), 'Name' (u_project_table), and 'Extends table'. On the right, there are checkboxes for 'Create module' and 'Create mobile module', a dropdown for 'Add module to menu' (set to 'Create new'), and a text field for 'New menu name' (project table). Below these are tabs for 'Columns', 'Controls', and 'Application Access'. The 'Columns' tab is active, showing a table of 'Dictionary Entries'.

	Column label	Type	Reference	Max length	Default value	Display
X	project id	Integer				false
X	project name	String				false
X	project manager	String				false
X	start date	Date				false
X	end date	Date				false
X	status	Choice				false
X	description	String				false

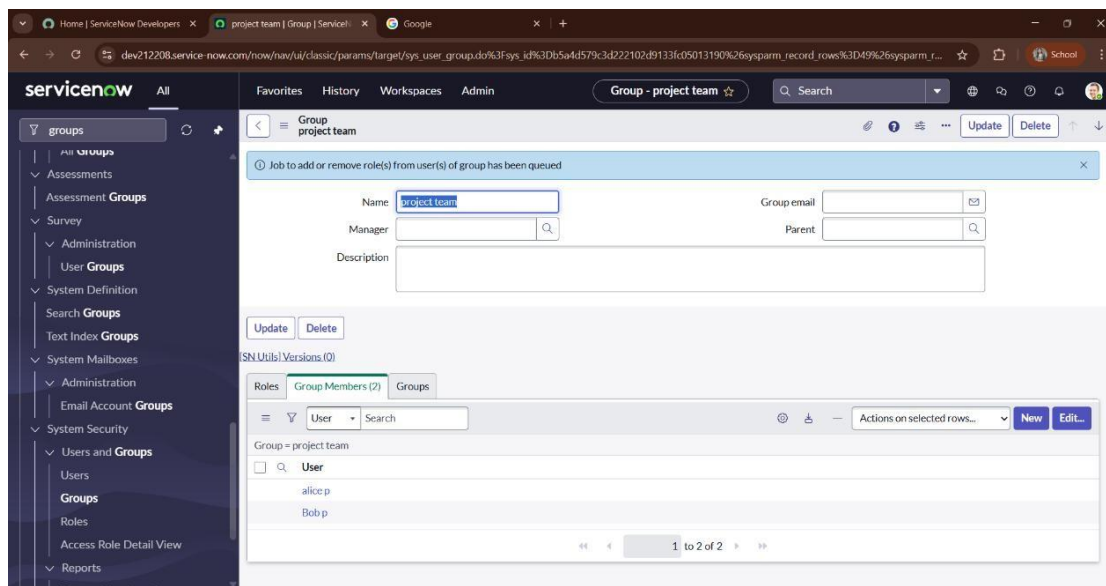
- Click on submit
- **Create one more table:**
- Create another table as:task table 2 and fill with following details.
- Click on **submit**.

The screenshot shows the 'Table - New Record' form in ServiceNow for a table named 'task table 2'. The left sidebar is the same as the previous screenshot. The main form area has fields for 'Label' (task table 2), 'Name' (u_task_table_2), and 'Extends table'. On the right, there are checkboxes for 'Create module' and 'Create mobile module', a dropdown for 'Add module to menu' (set to 'Create new'), and a text field for 'New menu name' (task table 2). Below these are tabs for 'Columns', 'Controls', and 'Application Access'. The 'Columns' tab is active, showing a table of 'Dictionary Entries'.

	Column label	Type	Reference	Max length	Default value	Display
X	task id	Integer				false
X	task name	String				false
X	assigned to	String				false
X	due date	Date				false
X	status	Choice				false
X	comments	String				false

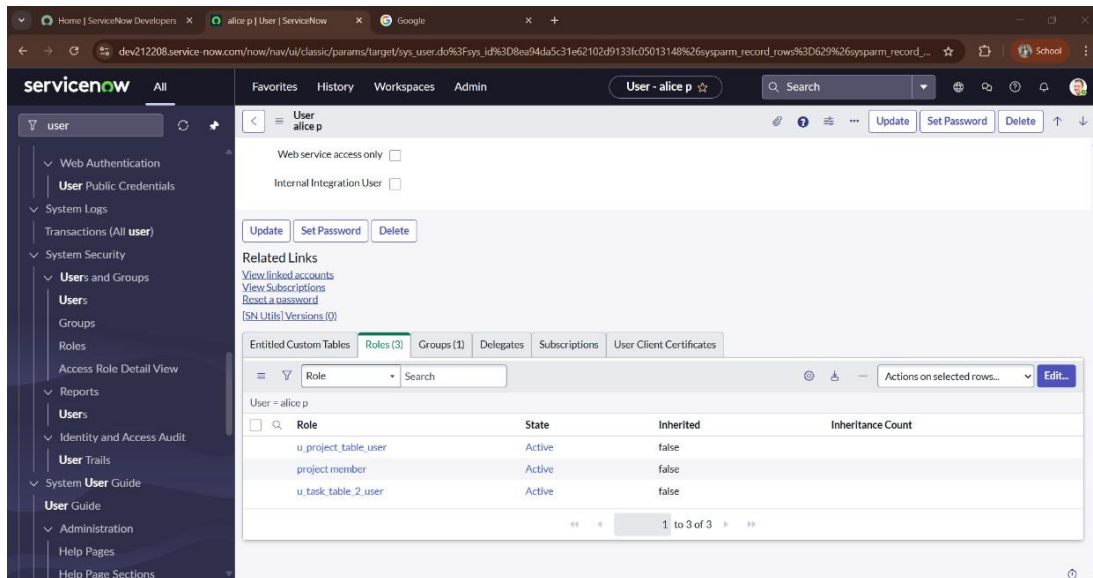
5. Assign users to project team group

- 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.

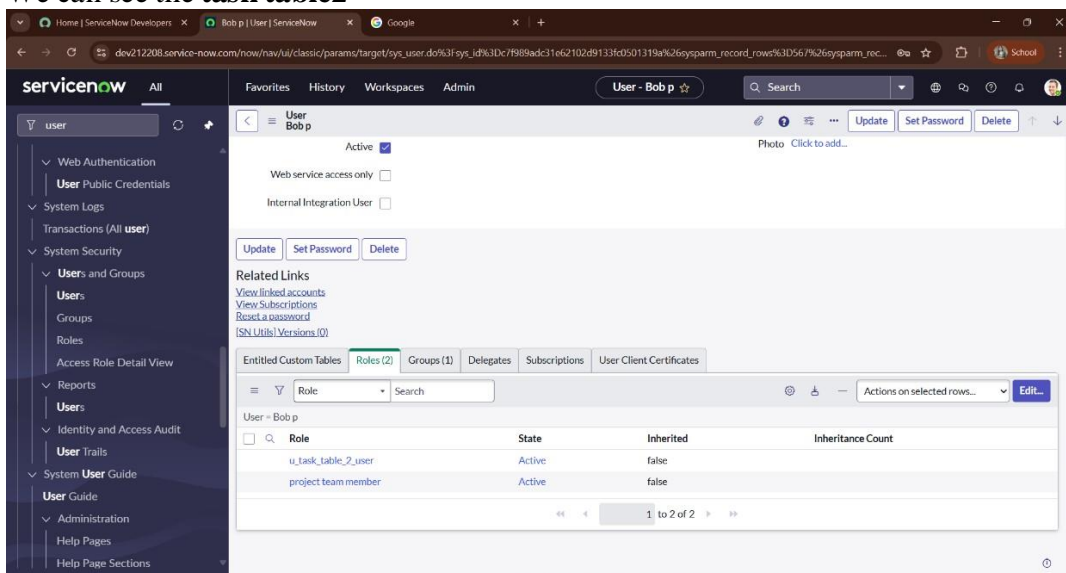


6. Assign roles to users

- **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 configuring an application menu. The left sidebar has a search bar with 'application menu' and a list of results under 'ALL RESULTS' including 'System Definition' and 'Application Menus'. The main content area is titled 'Application Menu - task table 2' and contains 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.** (This section is highlighted with a blue box and has an 'Edit User Roles' button next to it.)
- 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 of the form are 'Update' and 'Delete' buttons.

The screenshot shows the ServiceNow interface for configuring an application menu. The left sidebar has a search bar with 'application menu' and a list of results under 'ALL RESULTS' including 'System Definition' and 'Application Menus'. The main content area is titled 'Application Menu - project table' and contains 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.**
- 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 of the form are 'Update' and 'Delete' buttons.

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 area contains the following fields:

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

Below the main form, there is a 'Conditions' section and a 'Requires role' table. The 'Requires role' table has one row with the role 'u_task_table_2_user'.

Role
u_task_table_2_user

- 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

The screenshot shows the ServiceNow 'Access Controls' page. The left sidebar contains a navigation menu with categories like Configuration, Application Servers, Database Servers, Database Instances, Database Catalogs, System Properties, System Security, and Access Control (ACL). The main area displays a table of records with columns: Name, Decision Type, Operation, Type, Active, Updated by, and Updated. The table lists various records for 'u_task_table_2' and 'u_project_table'.

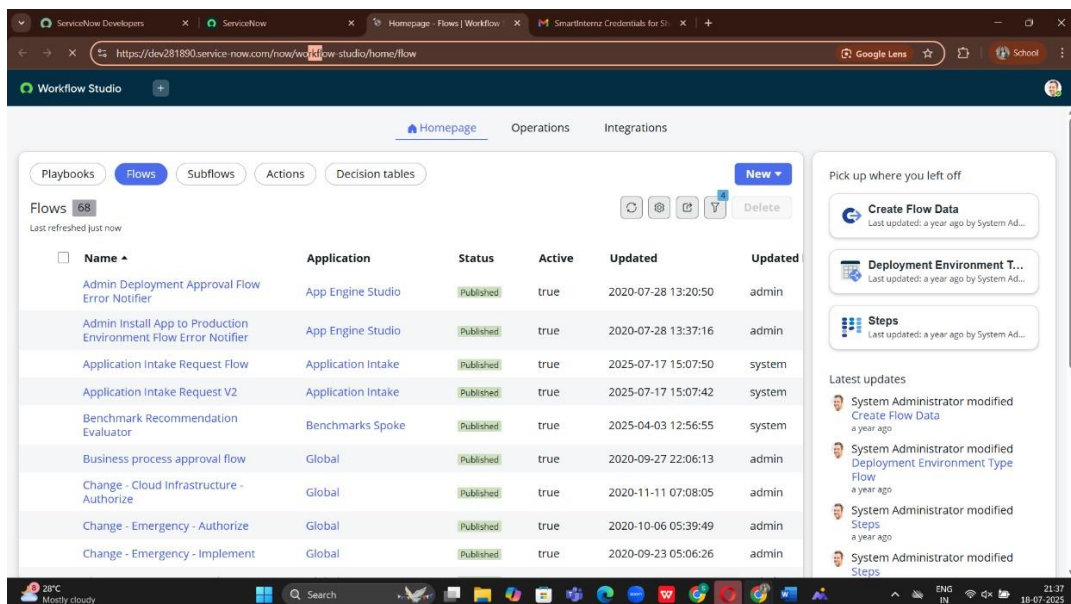
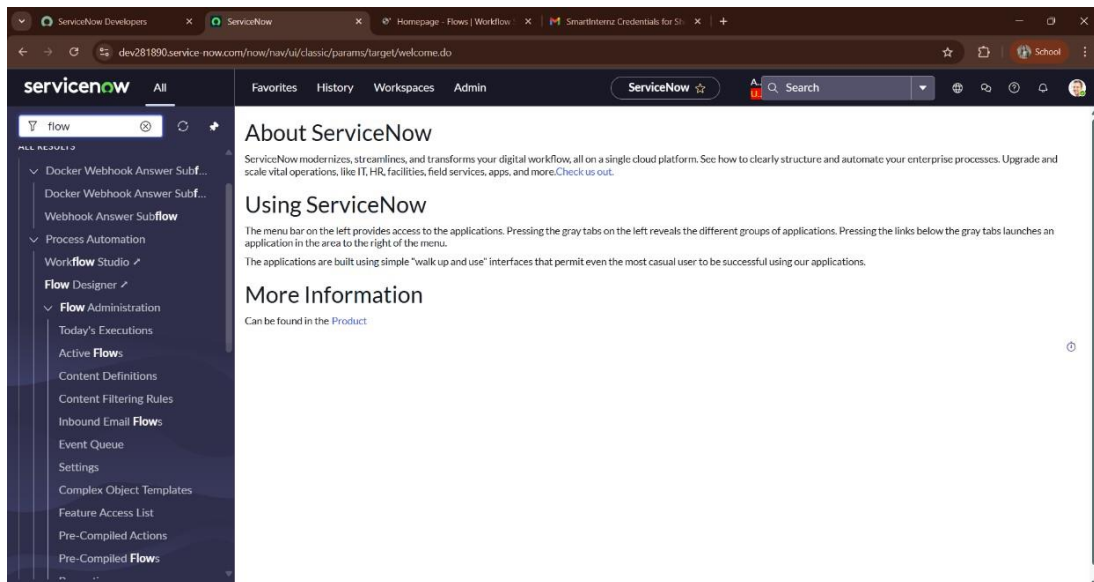
Name	Decision Type	Operation	Type	Active	Updated by	Updated
u_task_table_2.u_task_name	Allow If	write	record	true	admin	2025-06-25 03:37:05
u_task_table_2.u_task_id	Allow If	write	record	true	admin	2025-06-25 03:36:16
u_task_table_2.u_due_date	Allow If	write	record	true	admin	2025-06-25 03:35:39
u_task_table_2.u_assigned_to	Allow If	write	record	true	admin	2025-06-25 03:34:48
u_task_table_2.u_status	Allow If	write	record	true	admin	2025-06-25 03:29:34
u_task_table_2	Allow If	read	record	true	admin	2025-06-25 02:50:42
u_task_table_2	Allow If	delete	record	true	admin	2025-06-25 02:50:42
u_task_table_2	Allow If	write	record	true	admin	2025-06-25 02:50:42
u_task_table_2	Allow If	create	record	true	admin	2025-06-25 02:50:41
u_project_table	Allow If	read	record	true	admin	2025-06-25 02:47:42
u_project_table	Allow If	delete	record	true	admin	2025-06-25 02:47:42
u_project_table	Allow If	write	record	true	admin	2025-06-25 02:47:42
u_project_table	Allow If	create	record	true	admin	2025-06-25 02:47:42
sys_one_extend_eval_strategy_metric	Allow If	create	record	true	system	2025-06-21 05:34:47
sys_one_extend_eval_suggestion	Allow If	read	record	true	system	2025-06-21 05:34:47
sys_one_extend_dataset_skill_mapping	Allow If	read	record	true	system	2025-06-21 05:34:47
sys_one_extend_eval_strategy	Allow If	create	record	true	system	2025-06-21 05:34:47

- 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

The screenshot shows the 'task table 2 - Create Created' form in ServiceNow. The form has a header bar with 'task table 2 - Create Created' and a 'Submit' button. Below the header, there are input fields for 'task id', 'task name', 'assigned to', 'status' (a dropdown menu), 'comments', and 'due date'. A 'Submit' button is located at the bottom left of the form.

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.



Workflow Studio

New Flow

Let's get the details for your flow

Flow name *

Application *

Description

[Show additional properties](#)

- 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.

Workflow Studio

task table

task table 2 Created where (status is in progress, and comments is feedback, and assigned to is bob)

Trigger: Created

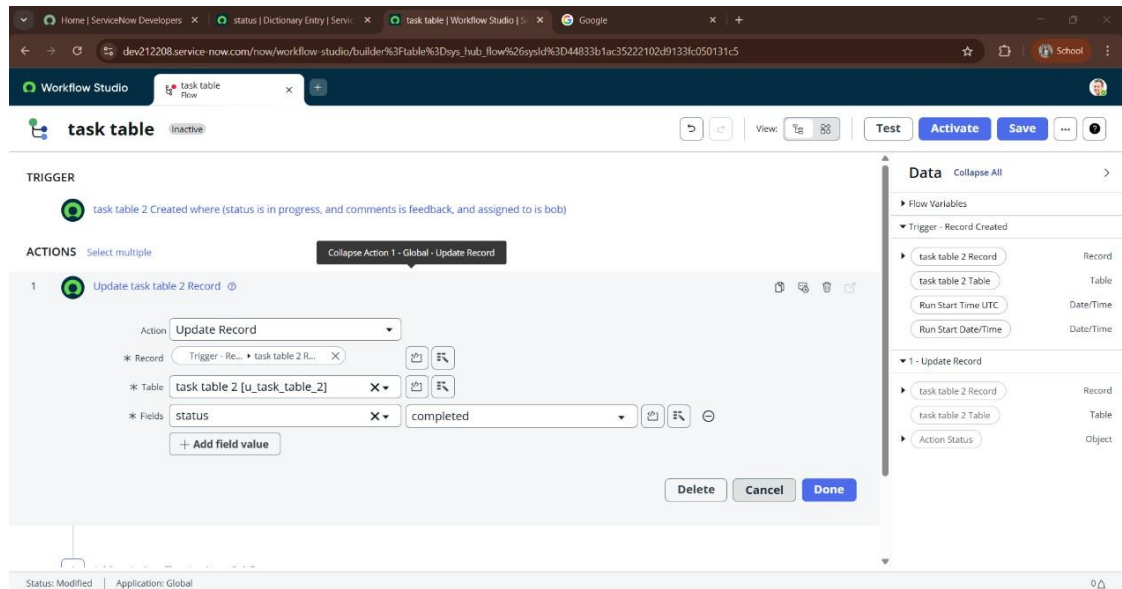
* Table: task table 2 [u_task_table_2]

Condition: All of these conditions must be met

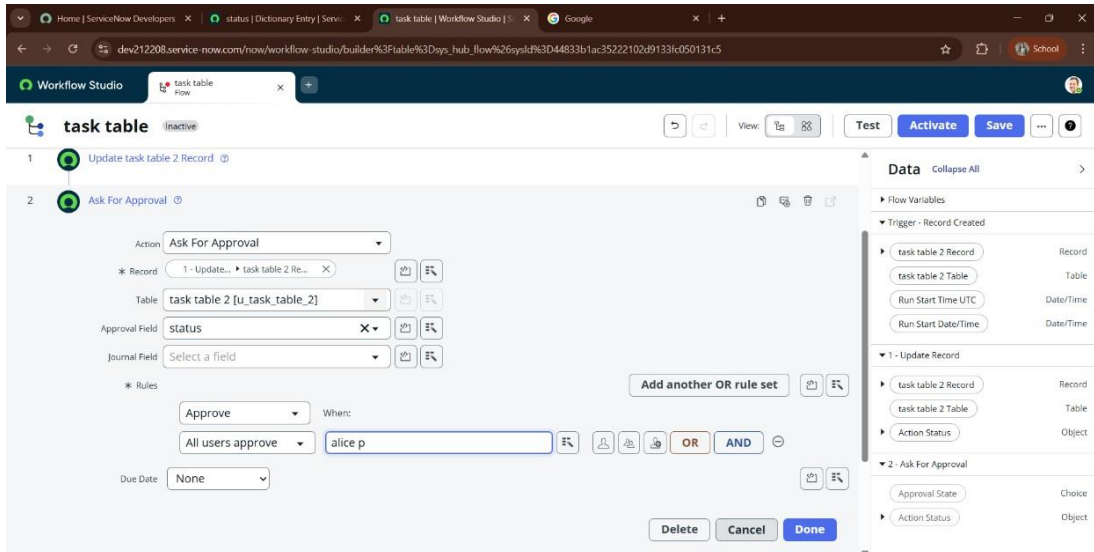
- status is in progress
- AND comments is feedback
- AND assigned to is bob

Status: Modified | Application: Global

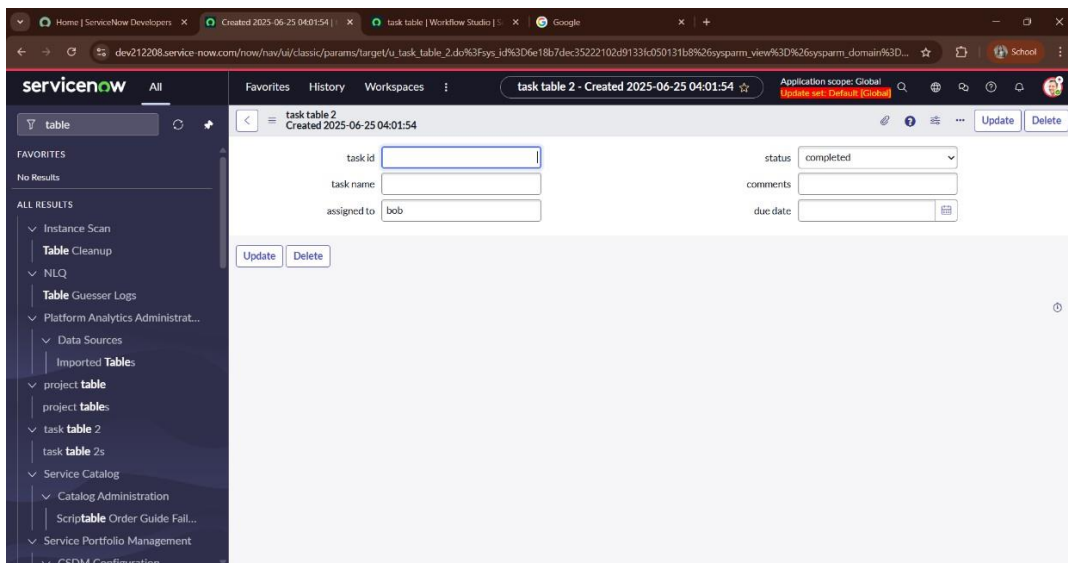
- Click on Add an action.
- Select action in that ,search for “ **update records**”.
- In Record field drag the fields from the data navigation from Right Side(Data pill)
- Table will be auto assigned after that
- Add fields as “**status**” and value as “**completed**”
- Click on Done.



- 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 interface with the 'Approvals' tab selected. The left sidebar contains the 'Self-Service' menu. The main content area displays a table of approval requests for the user 'alice p'. The table has columns for State, Approver, Comments, Approval for, and Created. The first row shows an 'Approved' state for 'alice p' with a creation time of 2025-06-25 04:54:54. Subsequent rows show 'Requested' states for 'Bernard Laboy' with various creation times.

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 interface. The 'task table' flow is selected, and the 'EXECUTION DETAILS' tab is active. The flow statistics show a 'Completed' state with a start time of 2025-06-25 04:54:53 and a duration of 308ms. The trigger is 'task table 2 Created'. The actions are 'Update Record' and 'Ask For Approval', both completed with durations of 11ms and 29ms respectively.

State	Start time	Duration
Completed	2025-06-25 04:54:53	308ms
Completed	2025-06-25 04:54:53	11ms
Completed	2025-06-25 04:54:53	29ms

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.