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

Project Introduction

Our project, “Optimizing User, Group, and Role Management with Access Control and Workflows in ServiceNow,” focuses on improving how user roles and permissions are managed in an organization.

It aims to streamline access control and automate workflows so that each user gets the right level of access based on their job role. Using Role-Based Access Control (RBAC) and Flow Designer, the system automatically handles approvals, assigns tasks, and ensures data security.

This helps reduce manual work, prevent unauthorized access, and improve accountability. The project also includes features like user impersonation for testing, dynamic dashboards, and automated data imports, making it a secure, scalable, and efficient identity management solution built on the ServiceNow platform.

Project Overview

The objective of this project is to enhance the management of users, groups, and roles in ServiceNow through the use of automated workflows and access control mechanisms.

It focuses on establishing secure, role-based access, minimizing manual administrative work, and ensuring regulatory compliance and accountability. The solution is designed to improve operational efficiency, data security, and organizational governance.

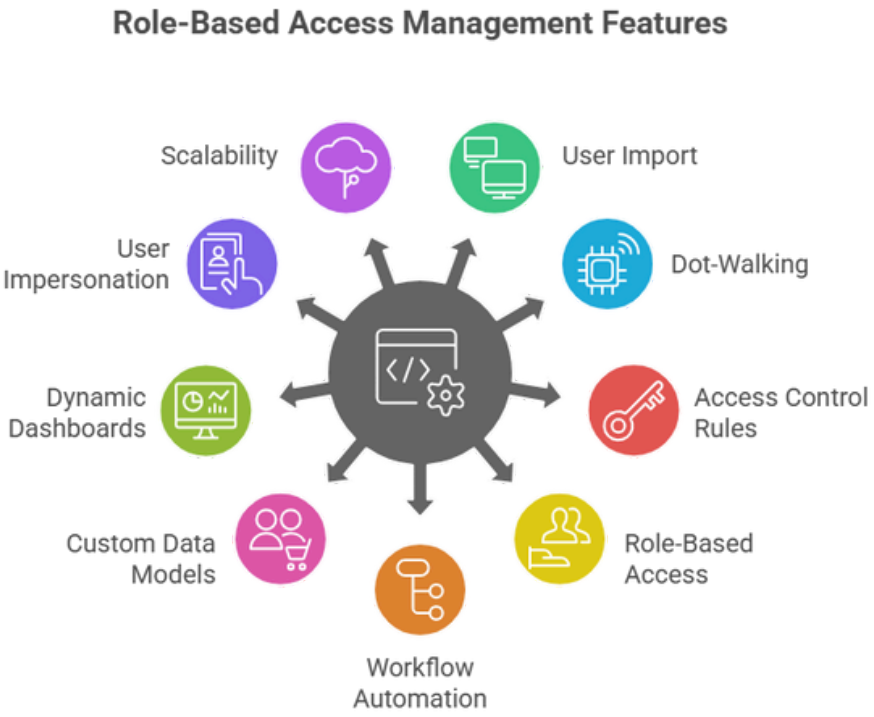
Description

This project aims to build a robust and scalable system within the ServiceNow platform to effectively manage identity and access across an organization.

By leveraging Role-Based Access Control (RBAC) and workflow automation, the system automates user provisioning, role assignments, and approval processes. It ensures that users have access only to the data and resources necessary for their roles.

Key components include Import Sets, Access Control Lists (ACLs), Flow Designer automation, and user impersonation testing to validate permissions.

Ultimately, the solution provides a secure, efficient, and compliant framework for managing user access and improving organizational productivity.



Project Features

- User, Group, and Role Import: Imports user, group, and role data using Import Sets and Transform Maps for accurate identity mapping.
- Dot-Walking Relationships: Automatically retrieves related details like department, location, and manager for consistent data.
- Access Control Rules (ACLs): Enforces secure, role-based access to tables, forms, and fields across the system.
- Role-Based Access Management: Assigns and controls permissions for Admins, Managers, and End Users using RBAC principles.
- Workflow Automation: Automates role assignment and approval processes using Flow Designer for faster operations.
- Custom Data Models: Creates custom tables and fields to manage extra data such as audit logs and workflow triggers.
- Dynamic Dashboards and Reports: Provides real-time insights into user distribution, access patterns, and compliance status.
- User Impersonation for Testing: Allows admins to test access controls and workflows by impersonating users.
- Scalability and Optimization: Ensures high performance, secure access, and smooth operation for enterprise-scale use.

Project Feature

- The project aims to solve challenges in managing user roles and access within a small project team by implementing a structured ServiceNow solution.
- Currently, unclear access controls and manual approvals cause confusion and delays.
- The proposed idea focuses on defining user roles, implementing secure access control, and automating workflows using ServiceNow.

This will help ensure accountability, improve team coordination, and enhance data governance with minimal manual intervention.

Requirement Analysis Phase

- Create two users (Alice and Bob).
- Create two groups for organizing users.
- Define roles and assign them to users.
- Create tables to store project and task data.
- Assign users to groups and roles to users.
- Set up Access Control Lists (ACLs) to secure fields and tables based on roles.
- Design a Flow to automatically assign operation tickets to groups.
- Test and verify all links, access permissions, and workflow functionality.

Project Planning Phase

- Divide the project into phases: Ideation, Requirement Analysis, Design, Development, Testing, and Review.
- Define risks like wrong role assignments, ACL errors, or workflow delays.
- Create mitigation plans such as approval workflows and access reviews.
- Allocate tasks among team members with time estimates.
- Use tools like ServiceNow Studio, Flow Designer, ACL Editor, and Performance Analytics.
- Conduct testing using user impersonation to validate roles and permissions.
- Review final results and prepare documentation for deployment.

Risk Management

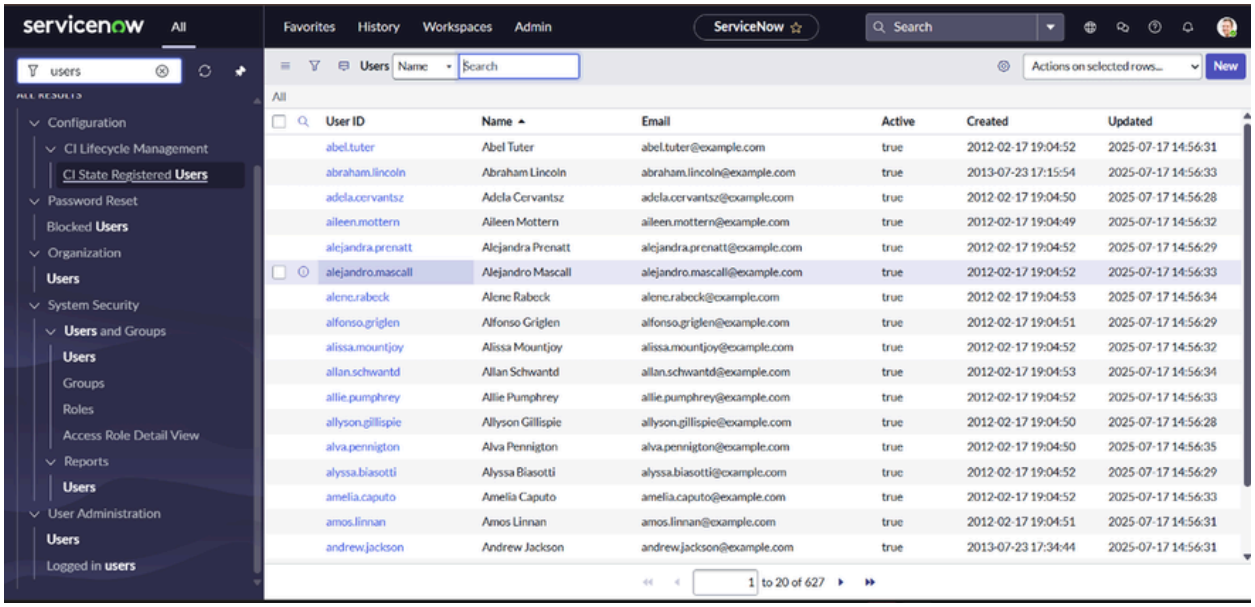
Risk	Impact	Probability	Mitigation Strategy
Incorrect role assignment grants	High	Medium	Implement approval
Misconfigured ACLs expose	High	Medium	Enforce least-privilege access
Role revocation delays after user	High	Medium	Automate de-provisioning using
Workflow misrouting delays	High	Low	Test all approval paths and set

Task Allocation

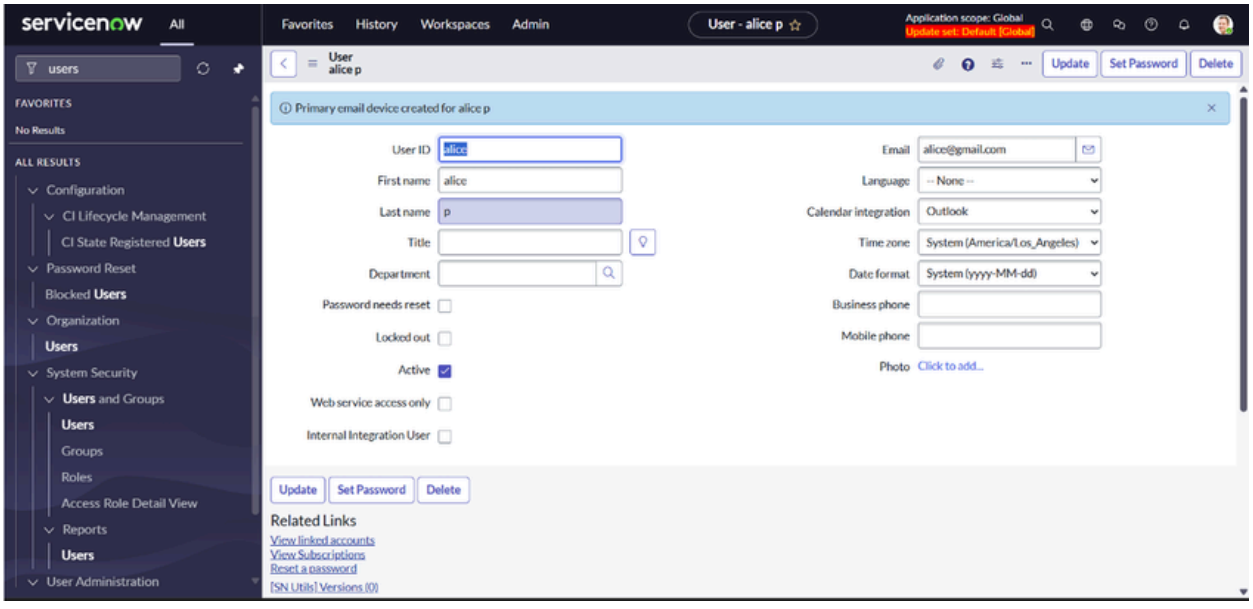
Task	Assigned To	Time Estimate	Tools Used
User & Group Data Import	Developer	2 Days	ServiceNow Studio, Import
Role Mapping & Assignment Logic	Developer	2 Days	Role Management Module, Flow
ACL Definition & Testing	Admin	2 Days	ACL Editor, Impersonation
Workflow for Role Approvals	Developer	2 Days	Flow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

Project Design

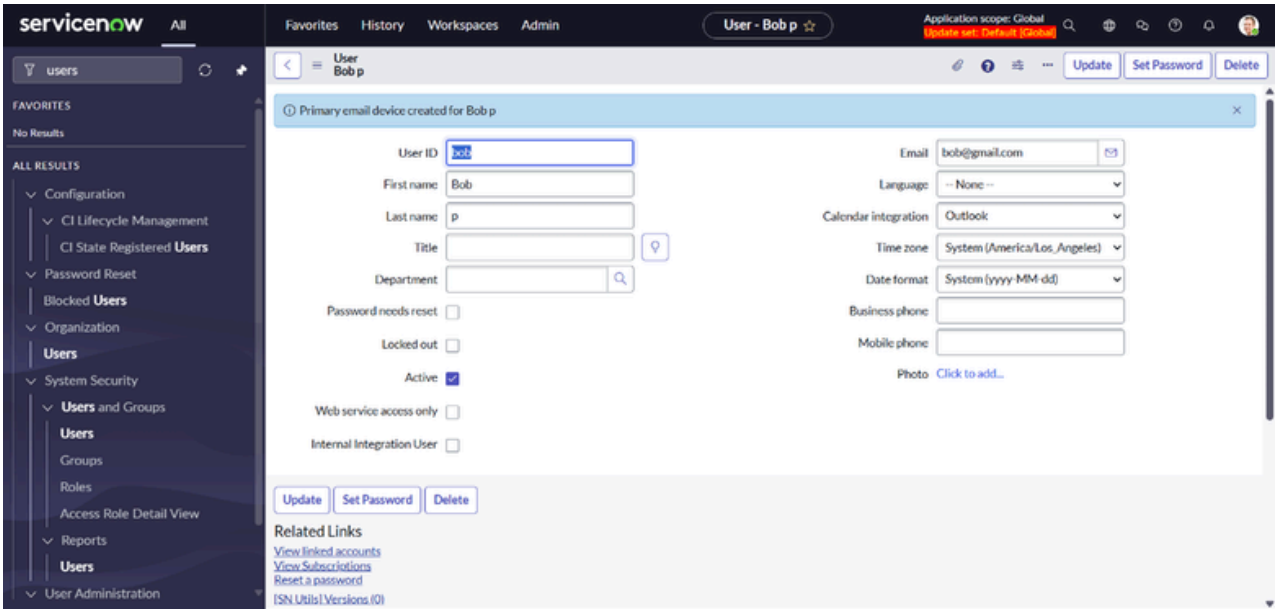
1. Open service now
2. Click on All >> search for users
3. Select Users under system security
4. Click on new



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

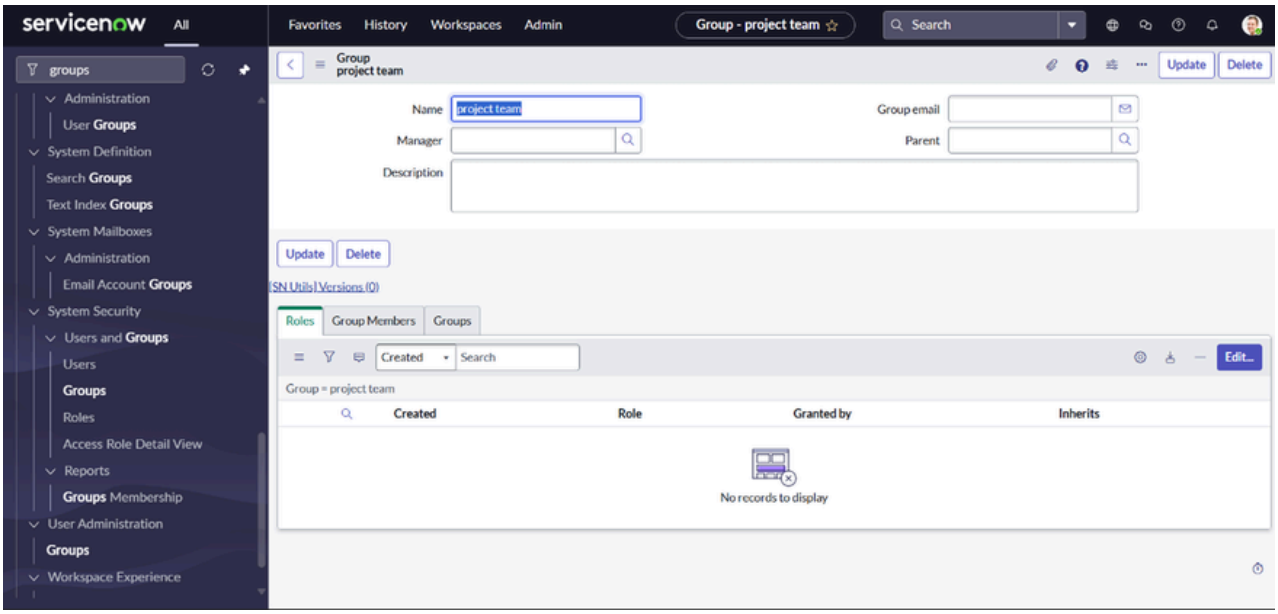


7.Create one more user:
8.Create another user with the following details
9.Username: “bob p”.
10.Click on submit.



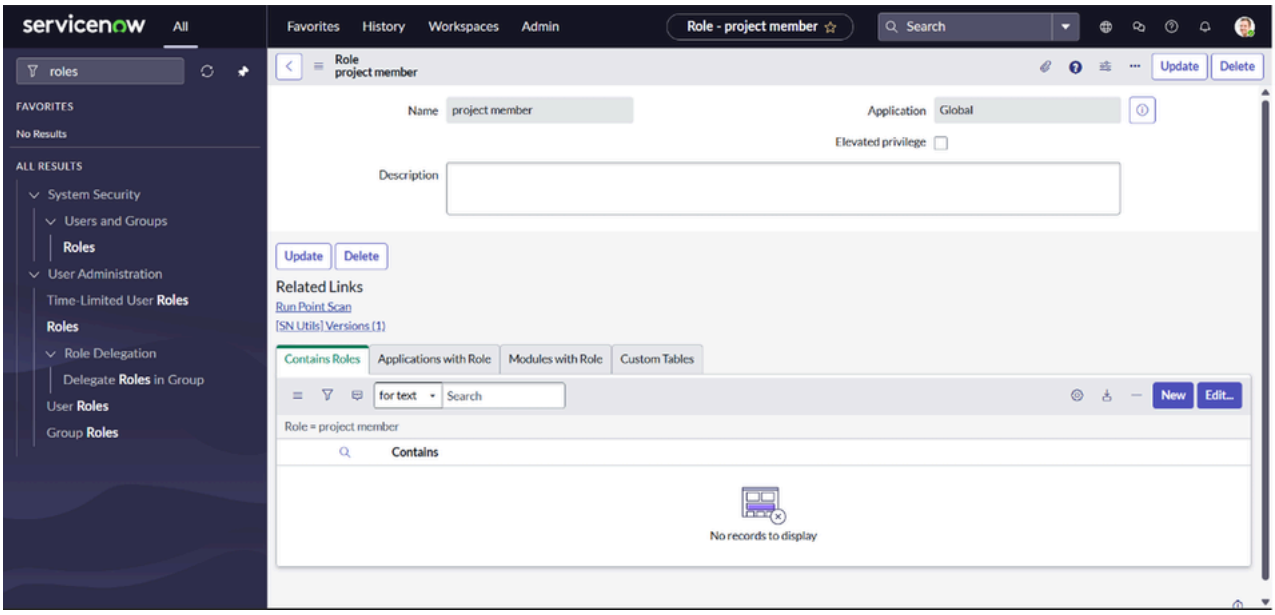
Create Group

1. Open service now.
2. Click on All >> search for groups
3. Select groups under system security
4. Click on new
5. Fill the following details to create a new group
6. Click on submit

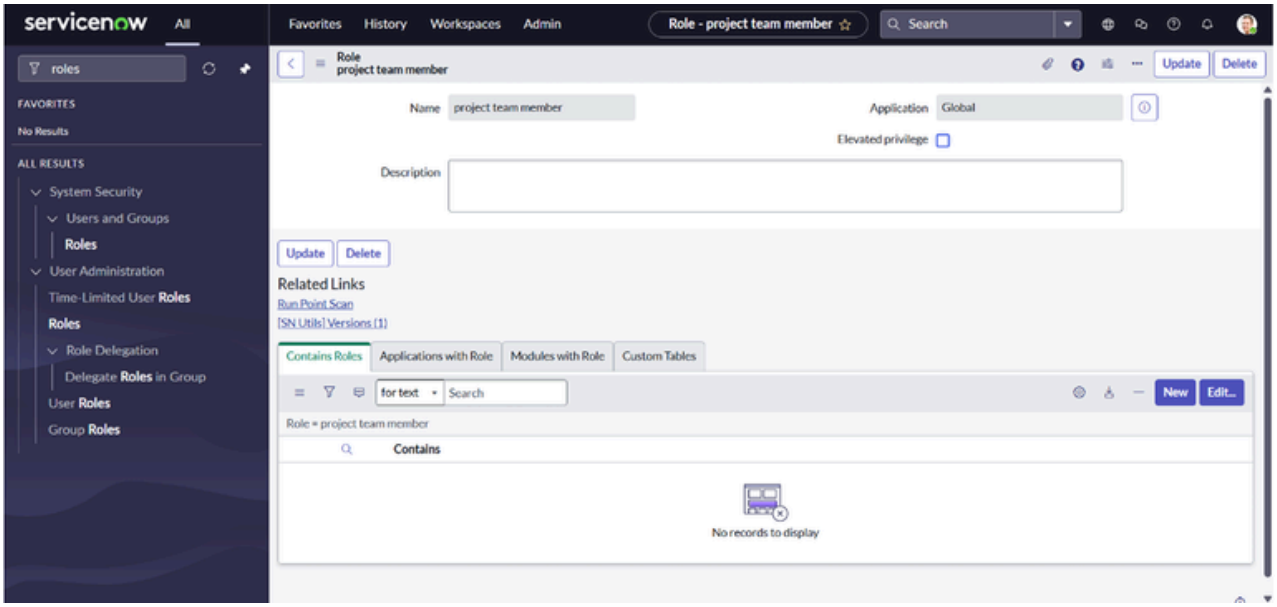


Create Roles

1. Open service now.
2. Click on All >> search for roles Select roles under system security
3. Click on new
4. Fill the following details to create a new role
5. Click on submit

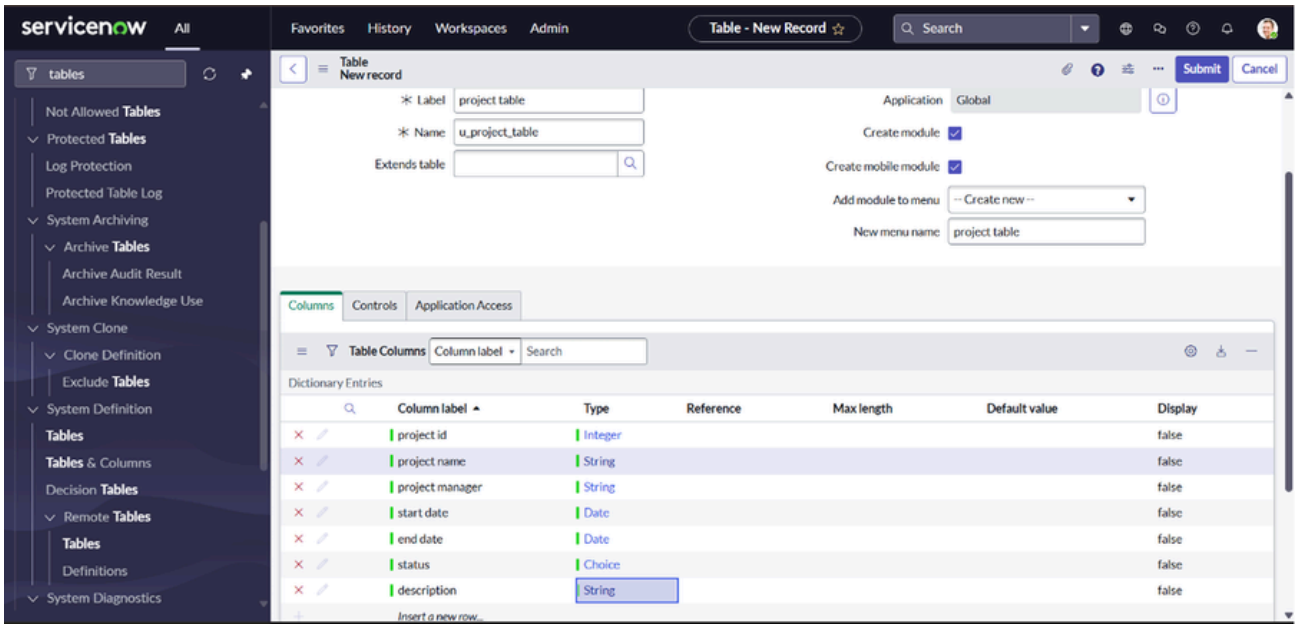


6.Create one more role:
7. Create another role with the following details
8.Click on submit

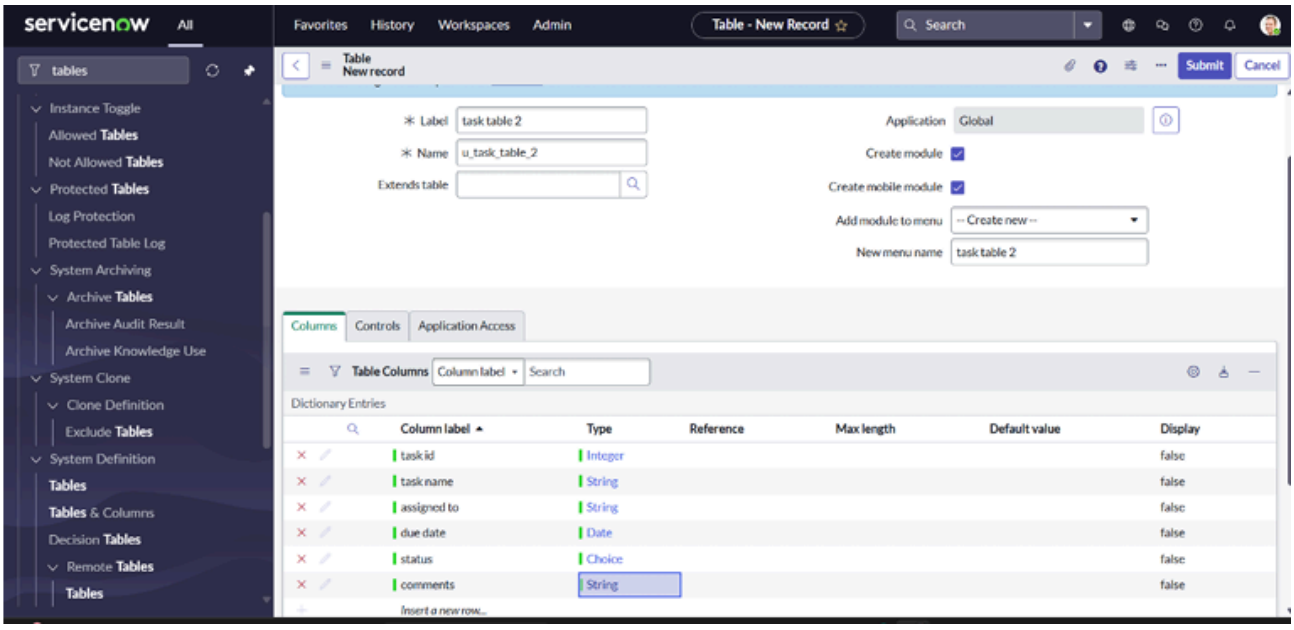


Create Tables

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

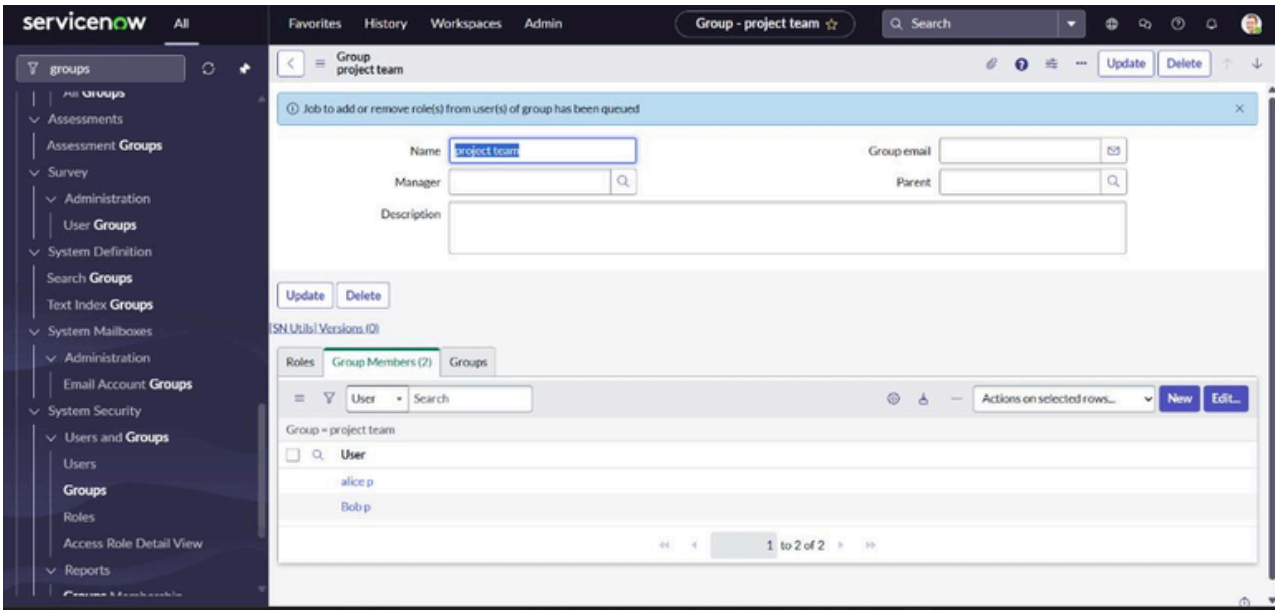


8. Click on submit
9. Create one more table:
10. Create another table as:task table 2 and fill with following details.
11. Click on submit.



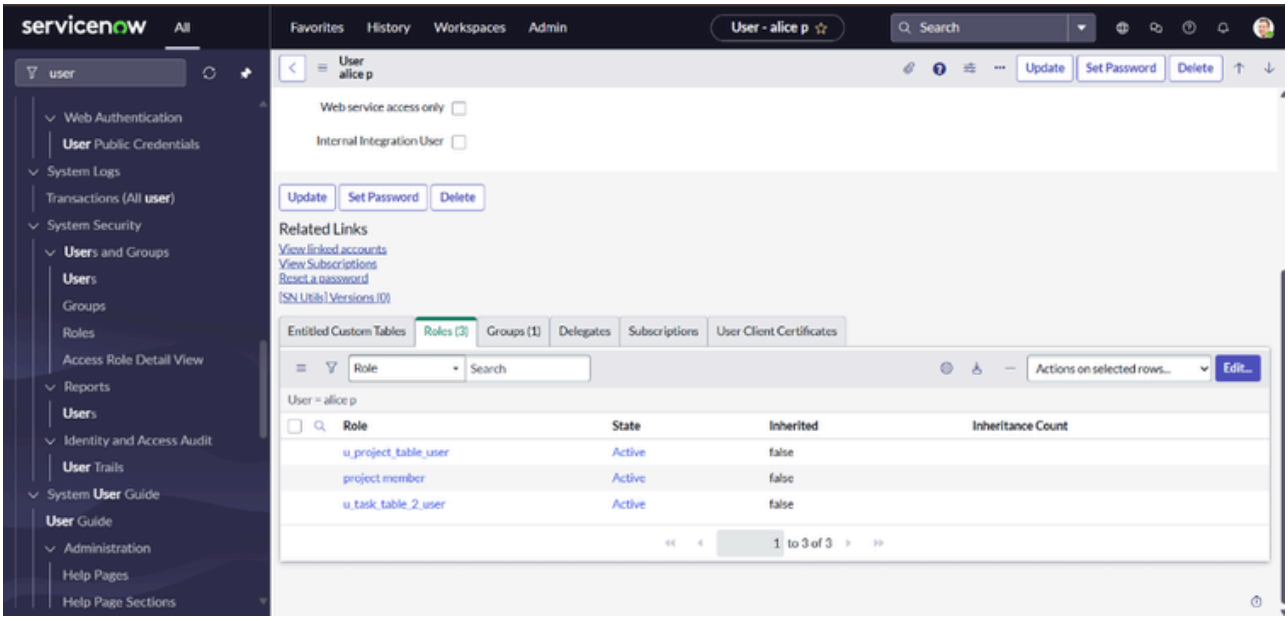
Assign users to project team group

1. Open service now
2. Click on All >> search for groups
3. Select tables under system definition
4. Select the project team group
5. Under group members
6. Click on edit
7. Select alice p and bob p and save.

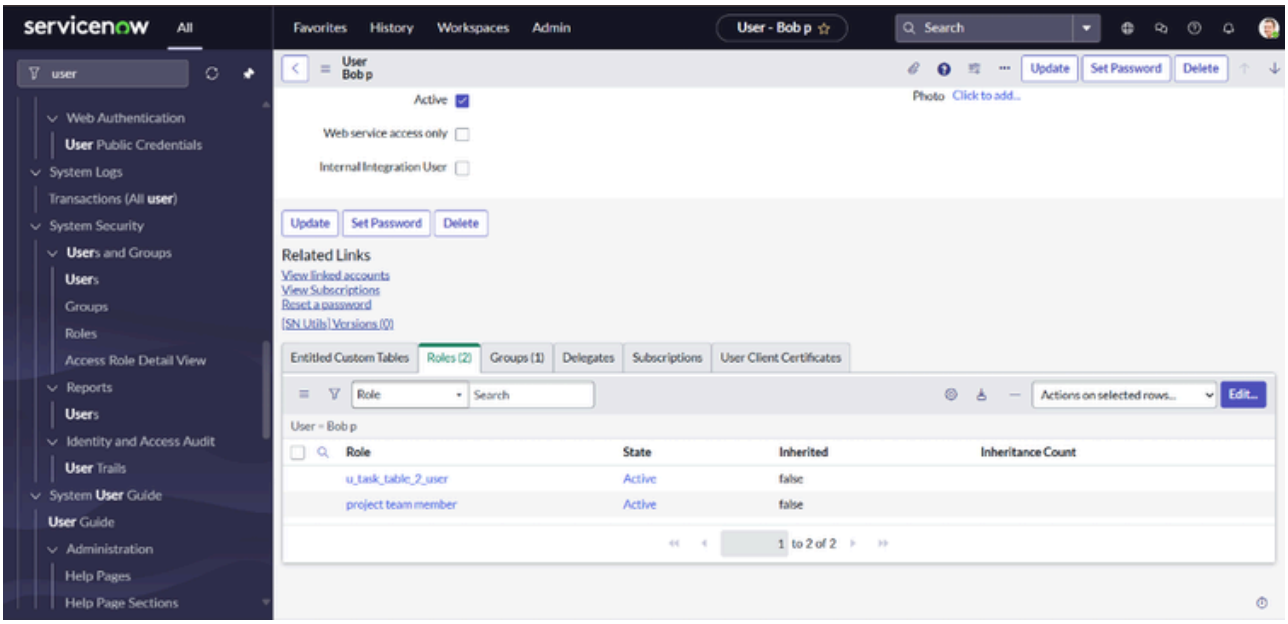


Assign roles to users

1. Assign roles to alice user
2. Open servicenow
3. Click on All >> search for user
4. Select tables under system definition
5. Select the project manager user
6. Under project manager
7. Click on edit
8. Select project member and save
9. Click on edit add u_project_table role and u_task_table role
10. Click on save and update the form.

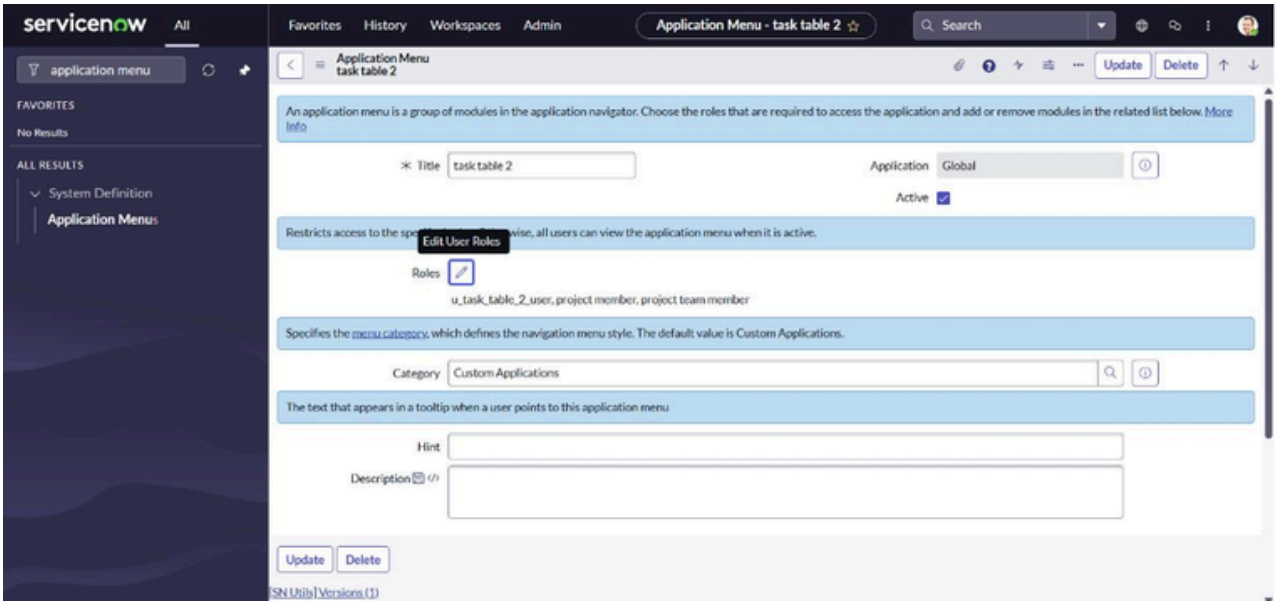


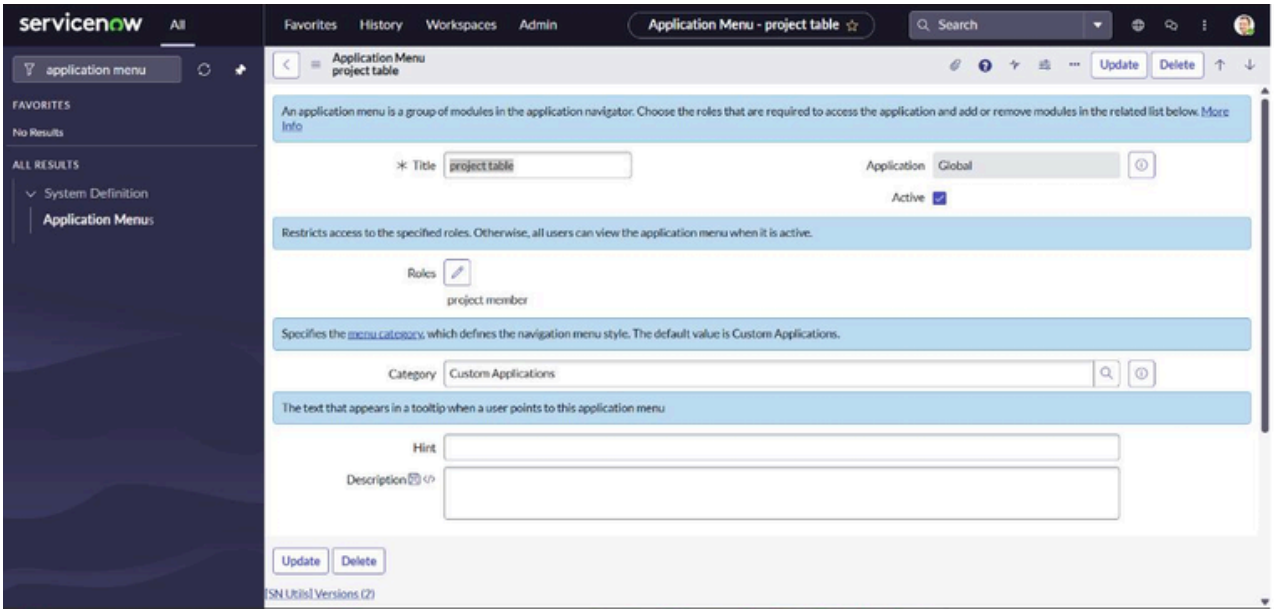
1. Assign roles to bob user
2. Open servicenow
3. Click on All >> search for user Select tables under system definition
4. Select the bob p user
5. Under team member
6. Click on edit
7. Select team member and give table role and save
8. Click on profile icon Impersonate user to bob
9. We can see the task table2



Application access

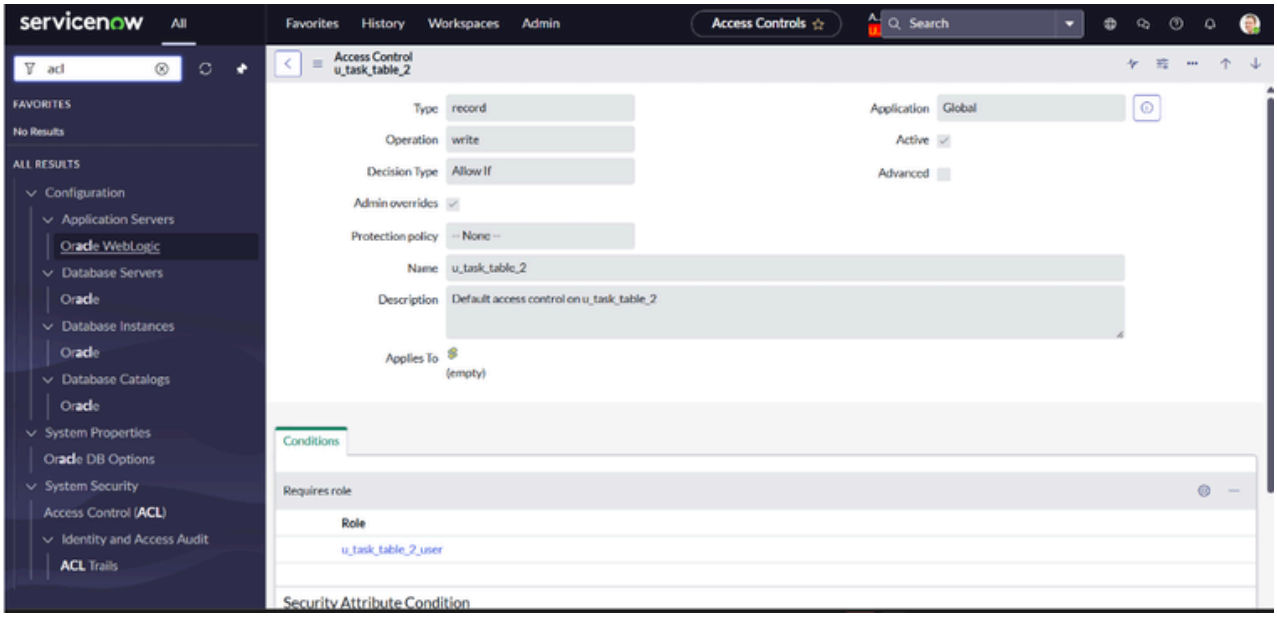
1. Assign table access to application
2. While creating a table it automatically create a application and module for that table
3. Go to application navigator search for search project table application
4. Click on edit module
5. Give project member roles to that application
6. Search for task table2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



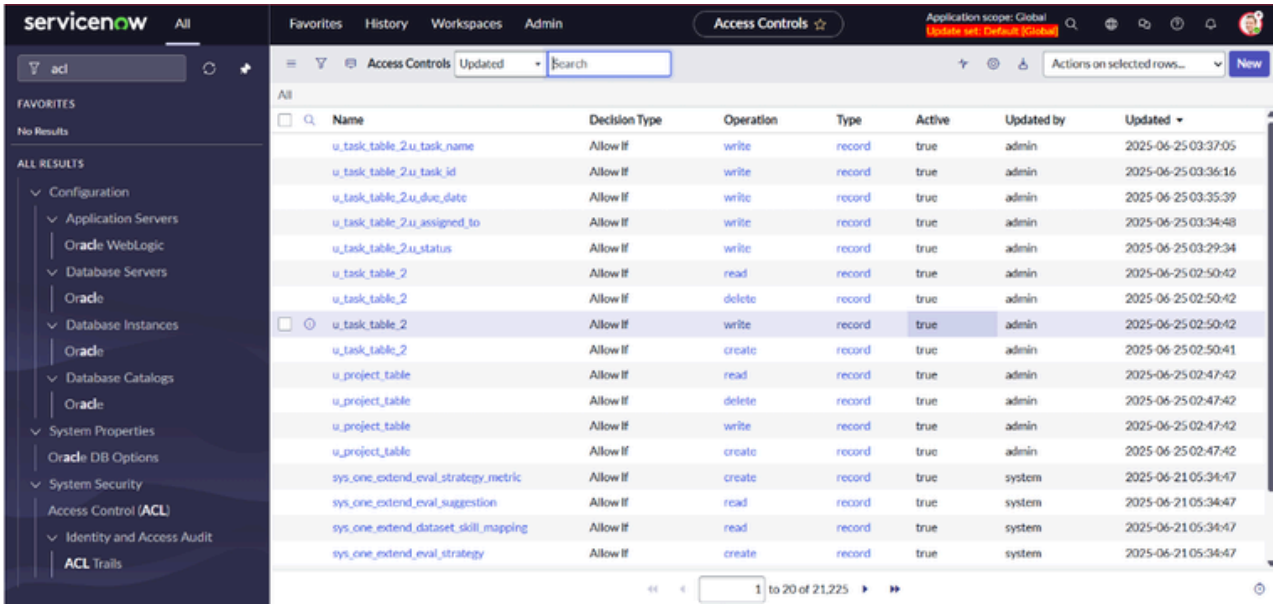


Access control list

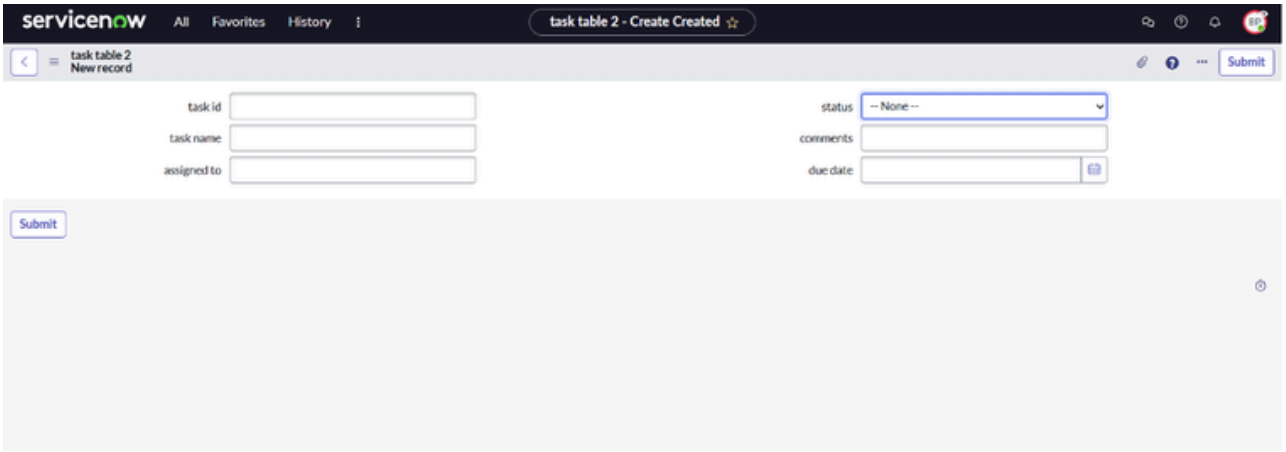
1. Create ACL
2. Open service now.
3. Click on All >> search for ACL
4. Select Access Control(ACL) under system security
5. Click on elevate role
6. Click on new
7. Fill the following details to create a new ACL



8.Scroll down under requires role
9.Double click on insert a new row
10.Give task table and team member role
11.Click on submit
12.Similarly create 4 acl for the following fields

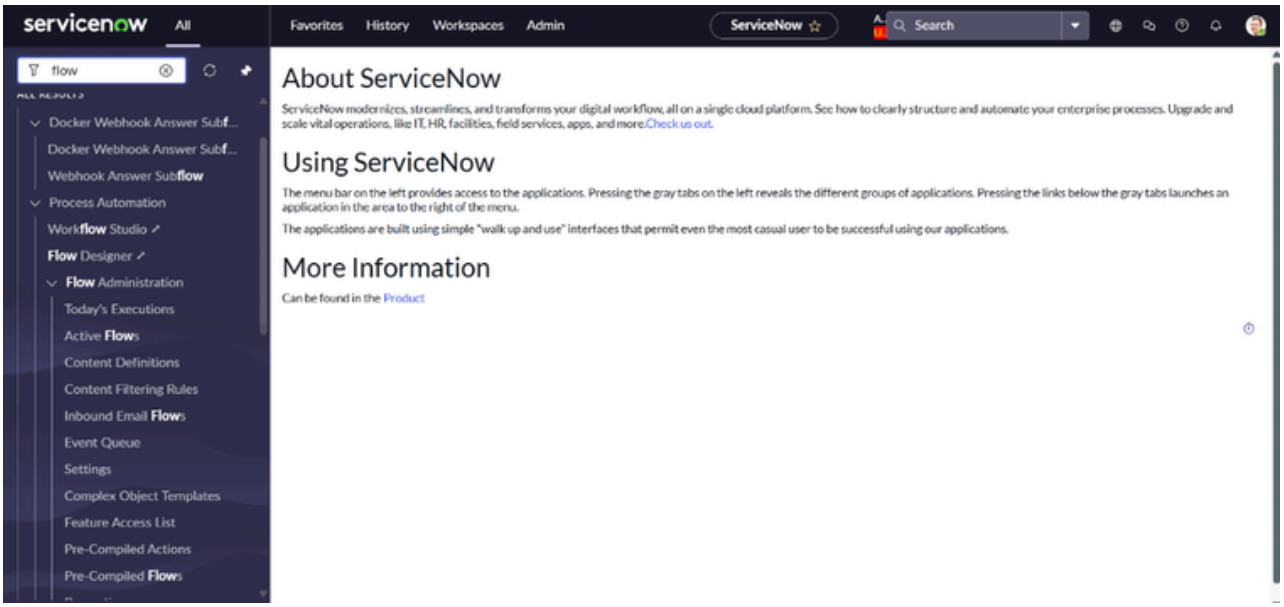


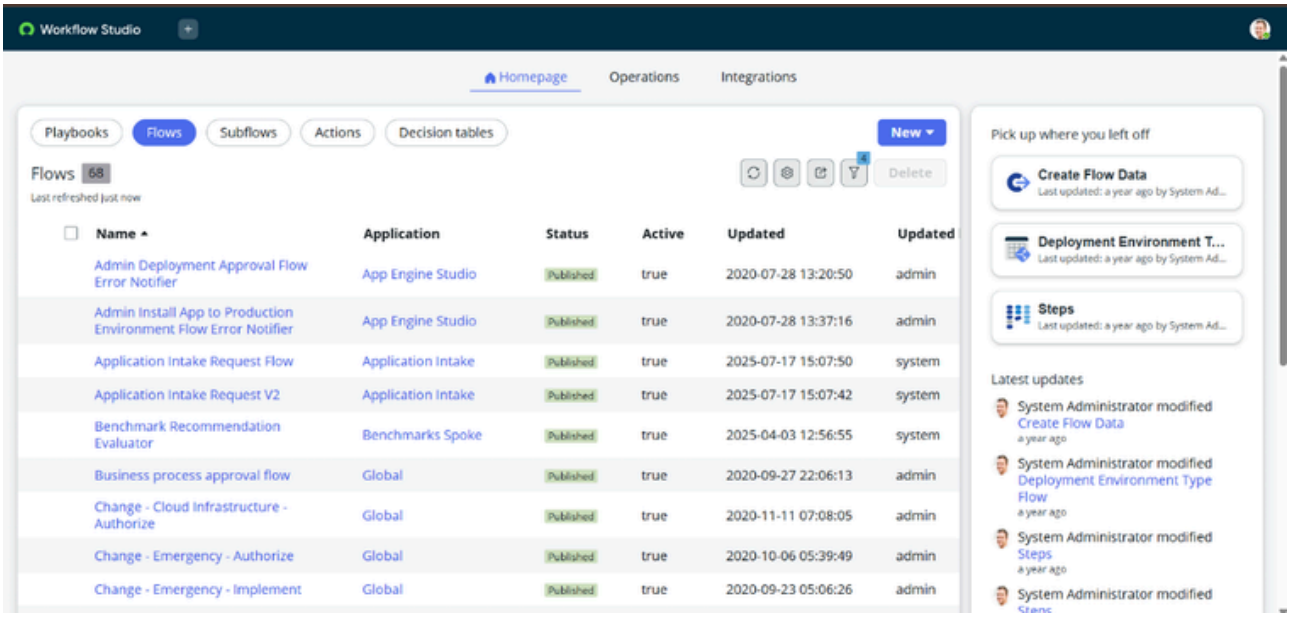
13.Click on profile on top right side
14.Click on impersonate user
15.Select bob user
16.Go to all and select task table2 in the application menu bar
17.Comment and status fields are have the edit access

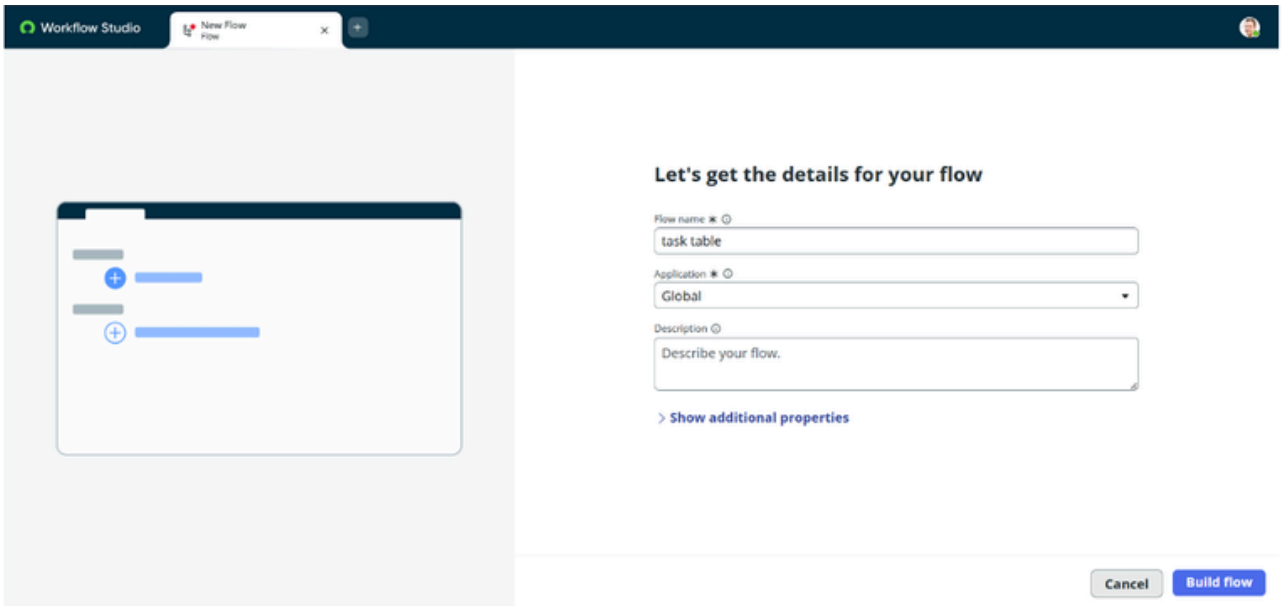


Flow

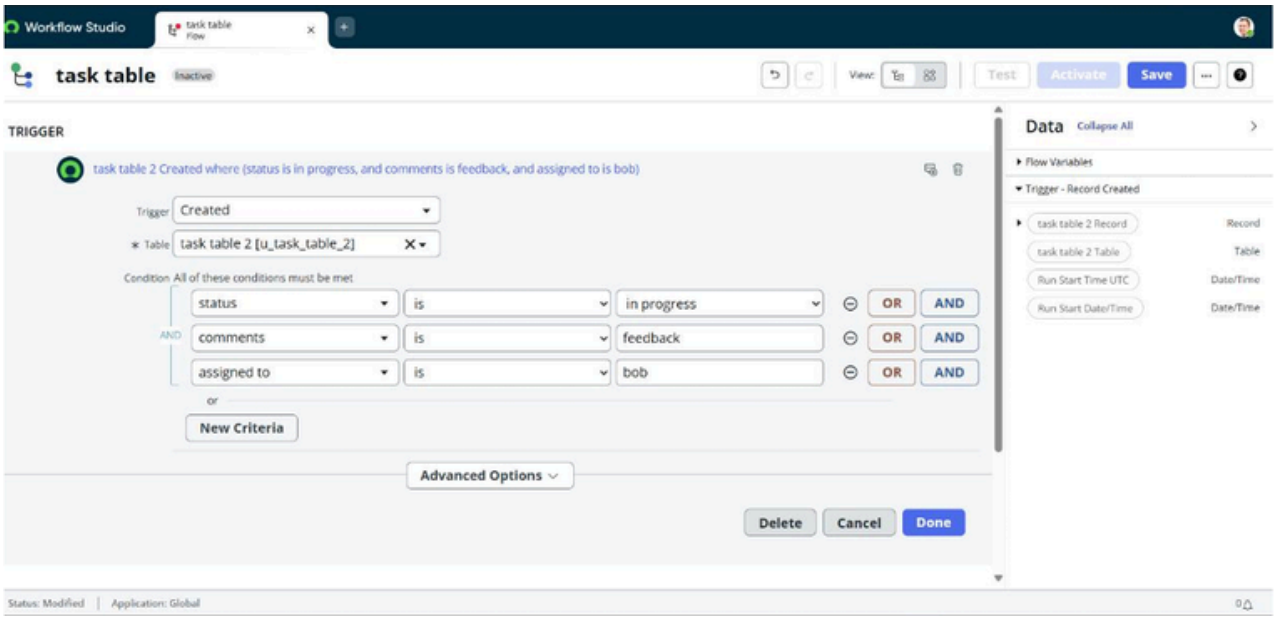
1. Create a Flow to Assign operations ticket to group
2. Open service now.
3. Click on All >> search for Flow Designer
4. Click on Flow Designer under Process Automation.
5. After opening Flow Designer Click on new and select Flow.
6. Under Flow properties Give Flow Name as " task table".
7. Application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



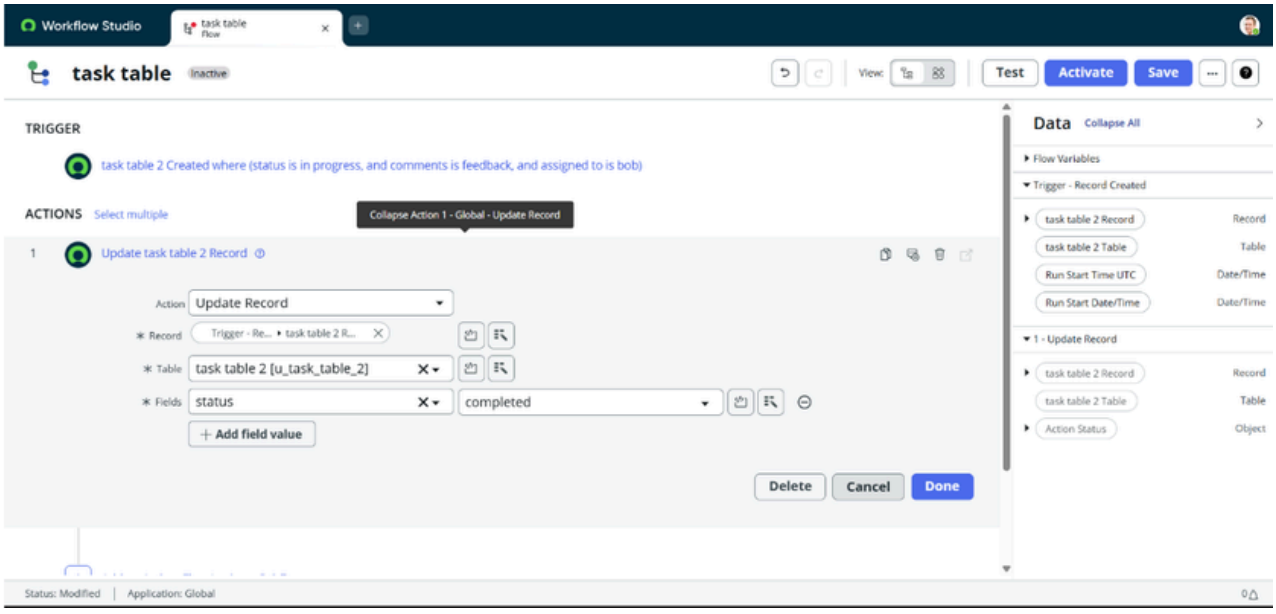




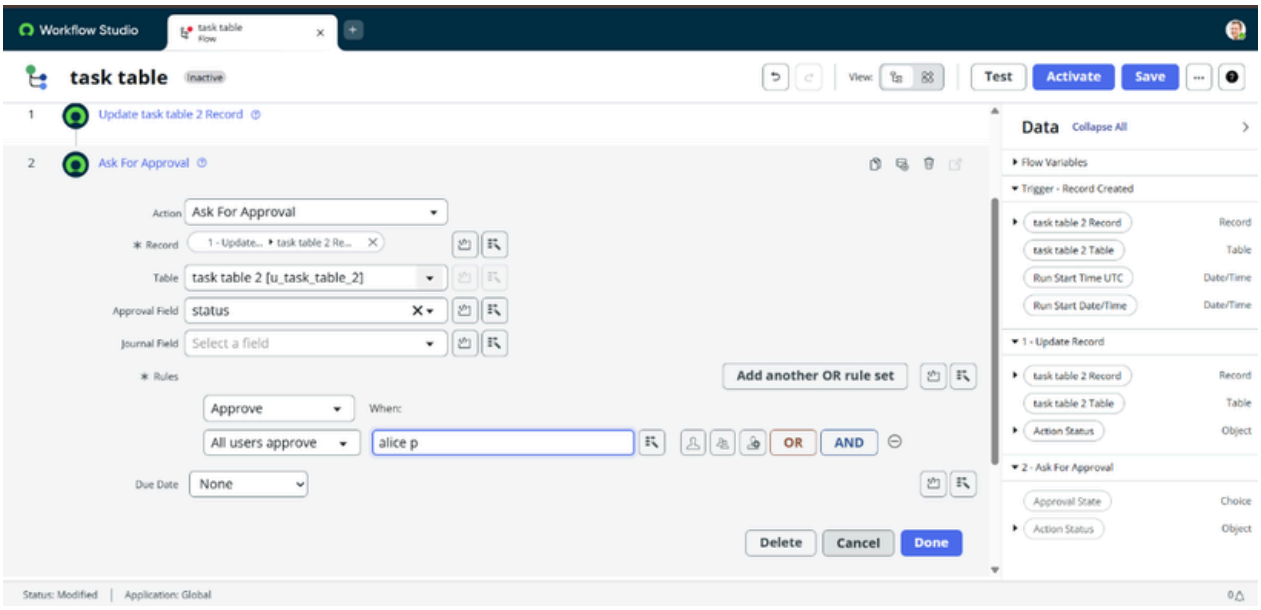
- Define ACL (Employees) Click on Add a trigger
- Select the trigger in that Search for “create record” and select that.
- Give the table name as “ task table ”.
- Give the Condition as:
- Field : status Operator :is Value : in progress
- Field : comments Operator :is Value : feedback
- Field : assigned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



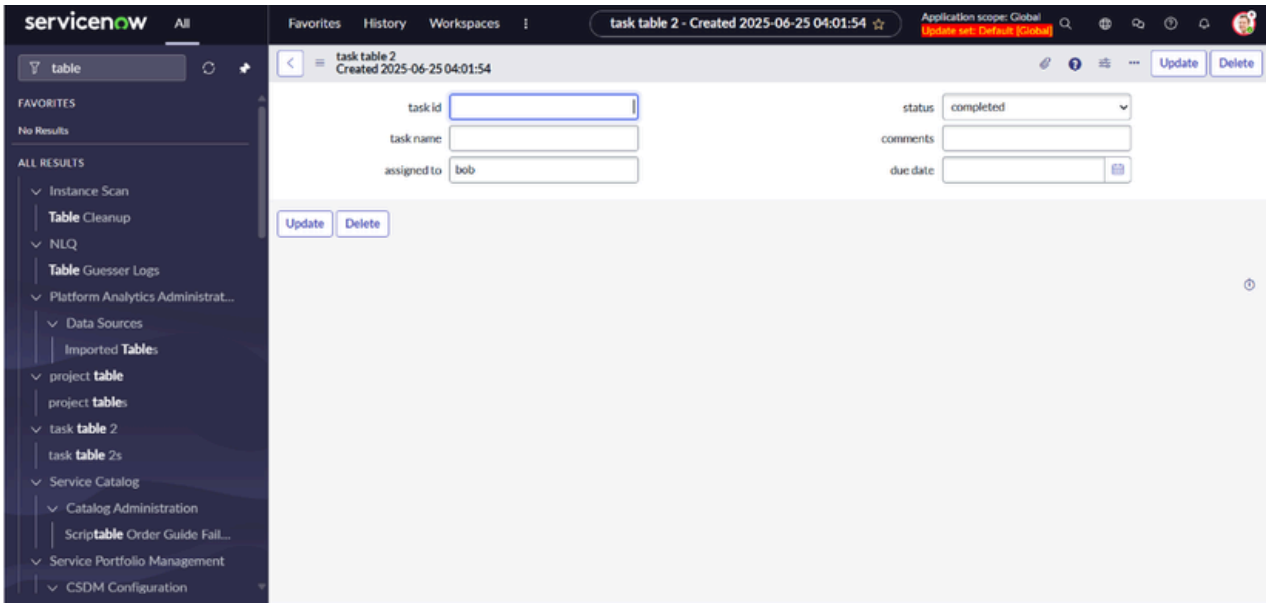
- Click on Add an action.
- Select action in that ,search for " update records".
- In Record field drag the fields from the data navigation from Right Side(Data pill)
- Table will be auto assigned after that
- Add fields as "status" and value as "completed"
- Click on Done.



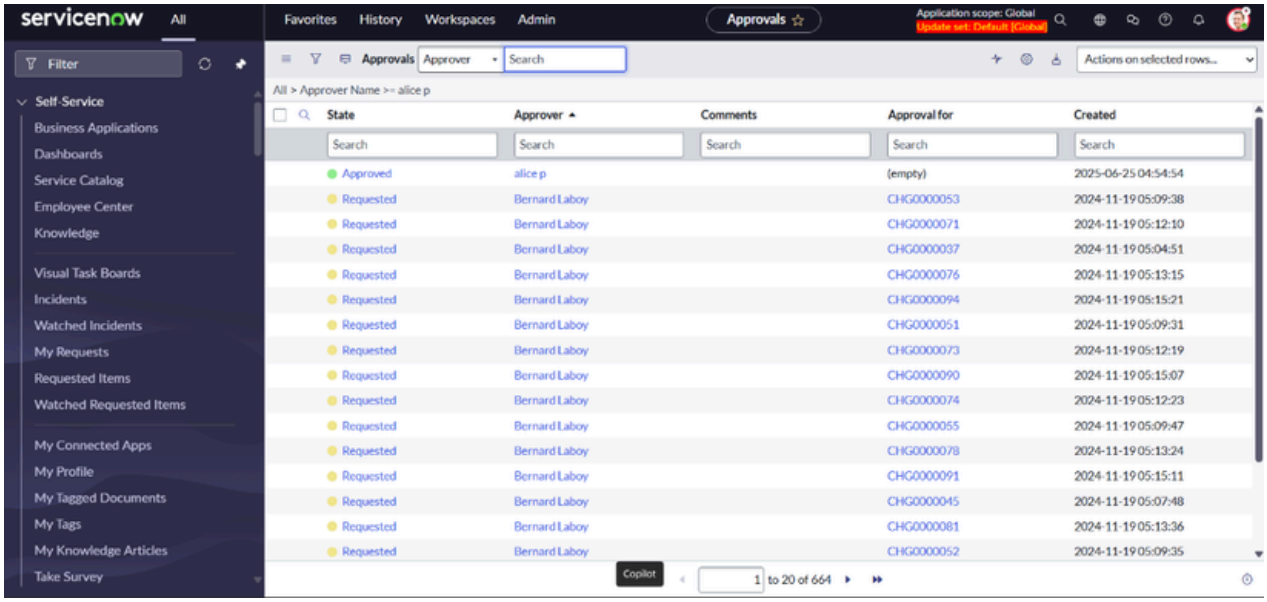
- Now under Actions.
- Click on Add an action.
- Select action in that ,search for " ask for approval ".
- In Record field drag the fields from the data navigation from Right side
- Table will be auto assigned after that
- Give the approve field as " status"
- Give approver as alice p
- Click on Done.

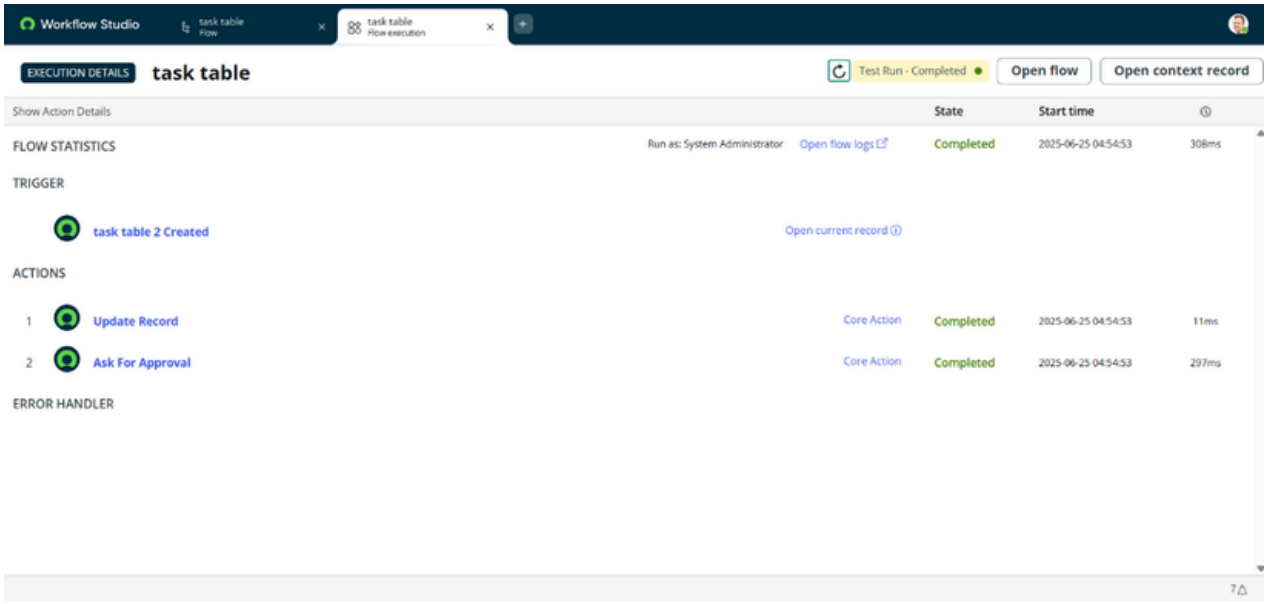


- Go to application navigator search for task table.
- It status field is updated to completed



- 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





Conclusion

The project “Optimizing User, Group, and Role Management with Access Control and Workflows in ServiceNow” successfully demonstrates how automation and access control can enhance organizational efficiency and data security.

By defining clear user roles, implementing Role-Based Access Control (RBAC), and automating workflows through Flow Designer, the system ensures that every user has appropriate access based on their responsibilities.

This approach minimizes manual work, prevents unauthorized access, and improves accountability through audit-ready processes.

Overall, the project provides a scalable, secure, and efficient framework for managing users, groups, and roles—supporting better governance, faster approvals, and enhanced productivity within the ServiceNow environment.