

TITTLE : Optimizing User, Group, And Role Management With Access Control And Workflows

INTRODUCTION

PROJECT OVERVIEW:

This project focuses on optimizing user, groups, and role management by implementing robust access control and workflows. The goal is to enhance security, streamline user access, and improve operational efficiency through a structured approach to permissions management. This involves defining clear roles, assigning appropriate access levels, and automating workflows for user management and access request.

PURPOSE:

Optimizing user, group, and role management with access control and workflows aims to enhance security, streamline operations, and improve overall efficiency within an organization. By carefully managing user access through roles and workflows, organizations can minimize security risks, ensure data protection, and boost productivity.

IDEATION PHASE

PROBLEM STATEMENT:

The core problem is streamlining user, group, and role management with access control and workflows to enhance security, efficiency, and compliance while minimizing administrative overhead. This involves addressing issues like role explosion, privilege creep, and the complexities of managing diverse access needs across multiple systems. Optimizing these areas reduces security risks, streamlines user onboarding and offboarding, and improves overall operational

OBJECTIVE:

The core objective of optimizing user, group, and role management with access control and workflows is to enhance security, improve efficiency, and simplify administration by ensuring that users only have the necessary access to resources based on their roles within an organization. This approach minimizes the risk of unauthorized access, streamlines workflows, and reduces the administrative burden of managing user permissions

REQUIREMENT ANALYSIS

SOLUTION REQUIREMENT:

DATE	
TEAM ID	LTVIP2025TMID30796
PROJECT NAME	Optimizing Idee, Group, And Role Management With Access Control And Workflows

FUNCTIONAL REQUIREMENTS:

Following are the functional requirements.

FR NO	FUNCTIONAL REQUIREMENT	SUB REQUIREMENT
FR-1	Users	Create Users
FR-2	Groups	Create Groups
FR-3	Roles	Create Roles
FR-4	Tables	Create Tables
FR-5	Assign Roles To Users	Assign User To project Team Group
FR-6	Assign Roles To Users	Assign Roles To Alice User Assign Roles To Bob User
FR-7	Application Access	Assign Table access To Application

FR-8	Access control list	Create ACL
FR-9	Flow	Create A flow Assign Operations Ticket To Group

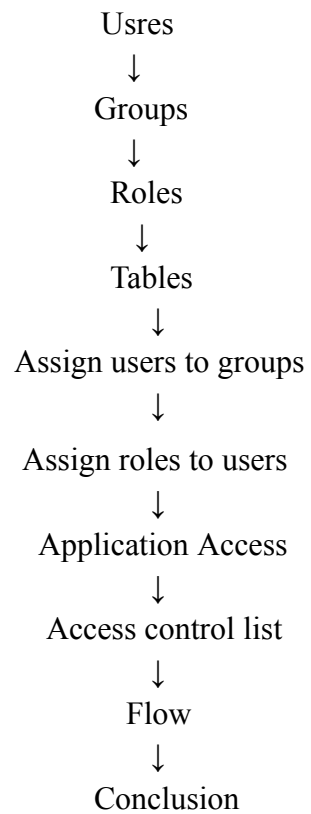
NON-FUNCTIONAL

Following are the functions requirements

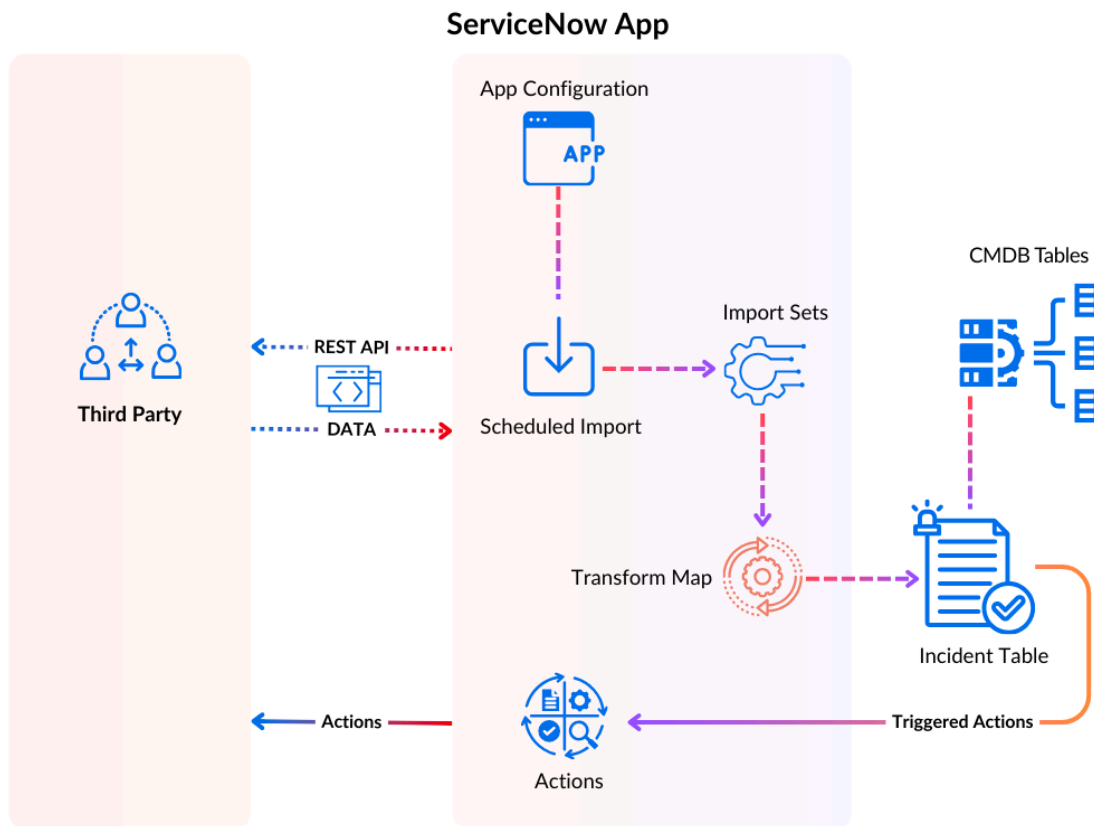
FR NO	Non functional requirements	Description
NFR-1	Usability	Optimizing user group role management with access control and workflow focuses on improving usability by streamlining user access, reducing administrative overhead, and enhancing security. This involves clearly defining roles, implementing role-based access control (RBAC), and establishing efficient workflows that align with user needs.
NFR-2	Security	Optimizing User, Group, and Role Management with Access Control and Workflow from a Security perspective involves strengthening identity governance, reducing risks, and ensuring compliance. Here's a breakdown of how to design and optimize this system securely:
NFR-3	Reliability	This is achieved through role-based access control (RBAC), which assigns permissions based on roles rather than individual users, reducing administrative overhead and the risk of errors.
NFR-4	Performance	streamlining user access, reducing administrative overhead, and enhancing security. This involves using Role-Based Access Control (RBAC) principles, such as grouping users by roles and assigning permissions to those roles rather than directly to individuals
NFR-5	Availability	implementing a system where users are grouped based on their roles, with each role assigned specific permissions to access resources and perform actions.
NFR-6	Scalability	Implementing Role-Based Access Control (RBAC) and adhering to best practices like least privilege, along with efficient workflows, ensures security and manageability as the system grows.

DATA FLOW DIAGRAM

Optimizing Users, Groups And role management with Access control and workflow



TECHNOLOGY STACK



PROJECT DESIGN

Proposed solution:

S.NO	PARAMETERS	DESCRIPTION
1	Problem statement	Modern digital systems, especially in large organizations or platforms, require efficient and secure user management
2	Idea	In modern organizations, managing access to systems and data is critical for security, compliance, and operational efficiency
3	Novelty	While access control and user management are not new concepts, this solution introduces innovations in

		automation, intelligence, and scalability that address the limitations of conventional systems. Here's what sets it apart:
4	Social impact	In a digitally connected world, effective access control systems are not just technical tools — they have a significant social and organizational
5	Business model	cloud-based SaaS platform that helps organizations manage users, groups, roles, and access rights with automated workflows, intelligent recommendations, and built-in compliance features
6	Scalability of solution	Scalability refers to the ability of the system to handle growth — in users, roles, permissions, workflows, integrations, and audit requirements — without compromising performance, usability, or security.

PROJECT PLANNING & SCHEDULING

Note: Request you to please click on "Tick mark ✓" after assigning the activities for each milestone.

Assign Roles & Responsibilities to Team

→ Proceed to Workspace

Users



Create L



* Kaldi Usharani



Groups



Create C



* Kaldi Usharani



Roles



Create F



* Karaggi Mounika



Table



Create T



* Karaggi Mounika



Assign L



Assign L



* Karaggi Mounika



Assign r



Assign r



* Himarika Nagamani



Assign r



Assign r



* Himarika Nagamani



Applicat



Assign t



* Himarika Nagamani



Access c



Create F



* Kancharana Pramee



MILESTONE-1: Users

ACTIVITY-1 : Create users

PURPOSE : This knowledge is crucial for designing effective and user-centered experiences.

By analyzing user behavior and preferences, designers can optimize user flows, personalize interactions, and create interfaces that are both intuitive and satisfying.

USES : Users refers to individuals who interact with a product, service, or system. In the context of technology, a user is someone who utilizes a computer, software, or website

STEPS :

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 User
6. Click on submit

User ID:

First name:

Last name:

Title:

Department:

Email:

Language:

Calendar integration:

Time zone:

Date format:

Business phone:

Mobile phone:

Photo:

☐ Password needs reset

☐ Locked out

☒ Active

☐ Web service access only

☐ Internal Integration User

Related Links

[View linked accounts](#)

[View Subscriptions](#)

[Reset a password](#)

Entitled Custom Tables: **Roles (3)** | Groups (1) | Delegates | Subscriptions | User Client Certificates

Role: Search

Actions on selected rows...

Role	State	Inherited	Inheritance Count
Project member	Active	false	
u_project_table_user	Active	false	
u_task_table_2_user	Active	false	

8. Create one more user:
9. Create another user with the following details
10. Click on submit

MILESTONE -2: Groups

PURPOSE :

The purpose of creating groups varies depending on the context, but generally, groups are formed. Groups can be formal, like teams in an organization, or informal, like social clubs.

USES : Groups are used for a variety of purposes, primarily collaboration, communication, and organization. They can be used to share information, manage projects, and foster a sense of community.

ACTIVITY -1. : Create groups

STEPS :

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

MILESTONE -3: Roles

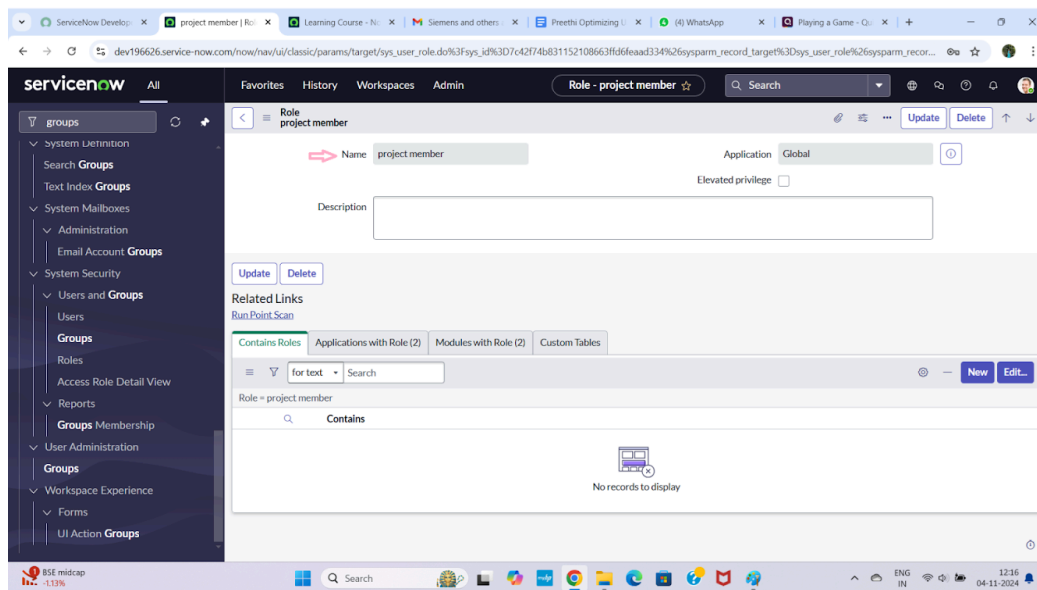
ACTIVITY -1 : Create roles

PURPOSE : Roles are a fundamental aspect of any organization or group; they provide clarity, structure, and accountability, enabling individuals to understand their specific duties and how their work aligns with the organization's goals.

USES : in the context of cloud computing and security, "roles" refer to a set of permissions that define what actions an entity (like a user or an application) can perform. Additionally, "roles" can describe the different functions or responsibilities individuals or groups have in various contexts, such as in a team, organization, or even in social settings.

STEPS :

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



Create one more role:

7. Create another role with the following details
8. Click on submit

MILESTONE-4 : Table

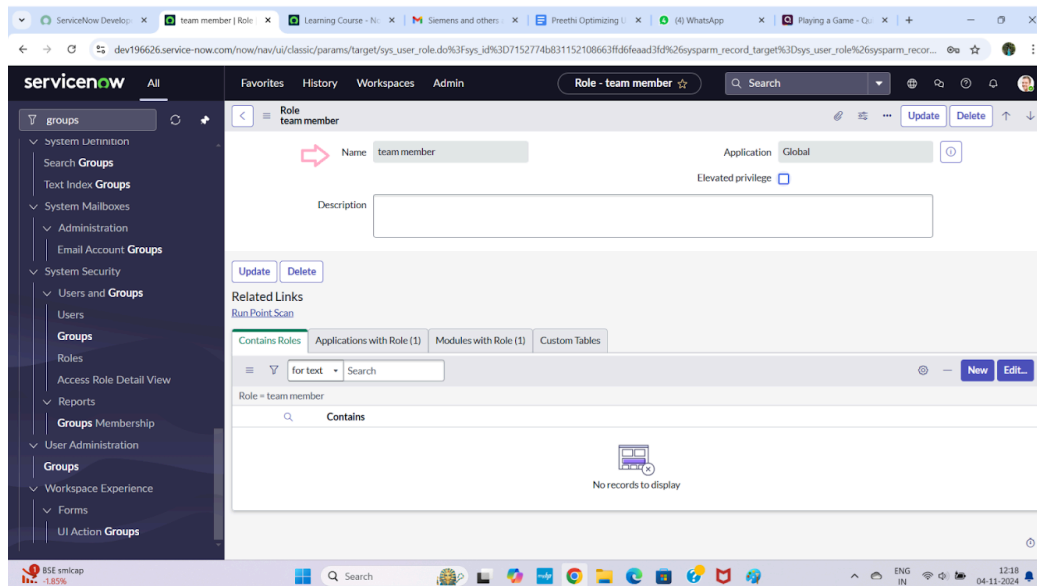
ACTIVITY-1 : create tables

PURPOSE : This allows for efficient comparison and analysis of information, whether it's statistical data, text, or other forms of content. Tables also help users quickly locate specific information and can be used to identify trends and patterns.

USES : They consist of rows and columns, allowing for efficient comparison and analysis of data, and are commonly used in databases, spreadsheets, and documents. Beyond data, tables also serve as functional pieces of furniture, providing a flat surface for various activities.

STEPS :

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

servicenow All Favorites History Workspaces Table - New Record

* Name

Extends table

Create module ☒

Create mobile module ☒

Add module to menu -- Create new --

New menu name

Columns Controls Application Access

Table Columns for text Search

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

Create one more table:

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

servicenow All Favorites History Workspaces Table - task table 2

Delete Update Delete All Records

Table Columns for text Search

1 to 6 of 6 New

Column label	Type	Reference	Max length	Default value	Display
Updated by	String	(empty)	40		false
Updates	Integer	(empty)	40		false
Updated	Date/Time	(empty)	40		false
Sys ID	Sys ID (GUID)	(empty)	32		false
Created by	String	(empty)	40		false
Created	Date/Time	(empty)	40		false
task id	Integer				false
task name	String				false
assigned to	String				false
due date	Date				false
status	Choice				false
comments	String				false

Insert a new row...

Delete Update Delete All Records

MILESTONE -5 : Assign users to group.

ACTIVITY: Assign users to project team group

PURPOSE : Assigning users to groups is a method of managing access and permissions in a system by associating users with predefined roles or sets of privileges through group membership

USES :Assign users to groups to assign roles and privileges to multiple users at a time and to manage user roles and privileges

STEPS :

- 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

The screenshot displays the ServiceNow 'Group Members' page for the 'project team' group. At the top, there is a breadcrumb trail: '< Group project team'. Below this, a status bar indicates 'Job to add or remove role(s) from user(s) of group has been queued'. The main form contains fields for 'Name' (filled with 'project team'), 'Group email', 'Manager', 'Parent', and 'Description'. Below the form, there are 'Update' and 'Delete' buttons. The 'Group Members' tab is active, showing a search bar with 'User' selected. The search results list 'alice p' and 'Bob P'. At the bottom, a status bar shows '1 to 1 of 1'. A small inset window in the bottom right corner shows a 'Shipping Tool' interface.

MILESTONE - 6: Assign roles to users

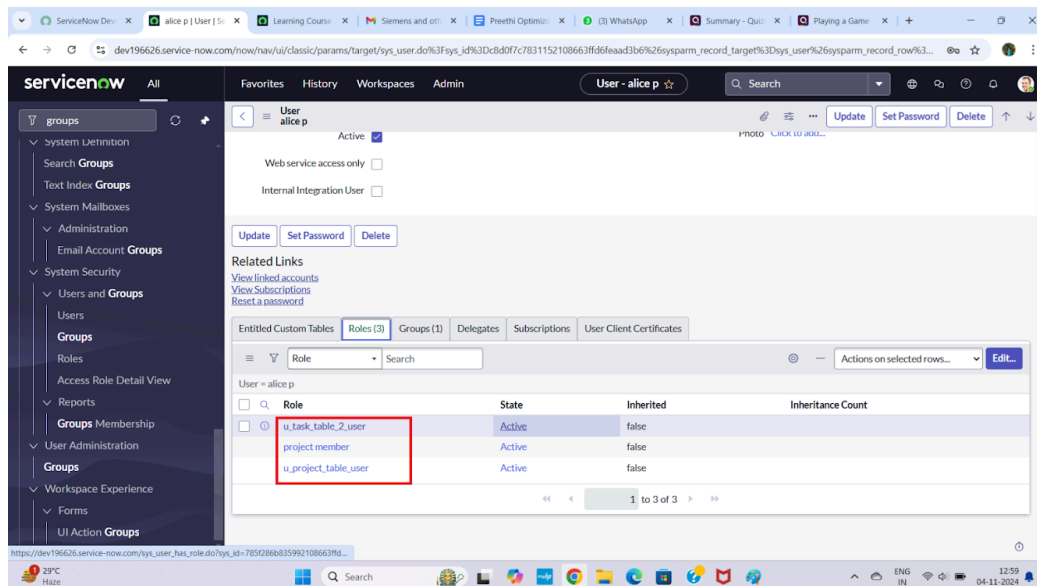
ACTIVITY -1: Assign roles to Alice users

PURPOSE: granting specific permissions and responsibilities, defining what actions users can perform within a system or application. This allows for better security management, streamlined workflows, and a more organized user experience.

USES: helps manage user access, ensuring that individuals only have the necessary privileges to perform their tasks, promoting security and organization.

STEPS:

1. Open servicenow. Click on All >> search for user
2. Select tables under system definition
3. Select the project manager user
4. Under project manager
5. Click on edit
6. Select project member and save
7. click on edit add u_project_table role. and u task table role
8. click on save and update the form.



ACTIVITY -2: Assign roles to bob users

PURPOSE: Managing access and permissions within a system. It allows administrators to define what actions users can perform, ensuring security and efficiency. Essentially, roles dictate

the specific permissions and responsibilities assigned to users, controlling what they can see, do, and manage within the system.

USES :Allows administrators to grant specific sets of privileges to users based on their responsibilities and needs, ensuring appropriate access control and security.

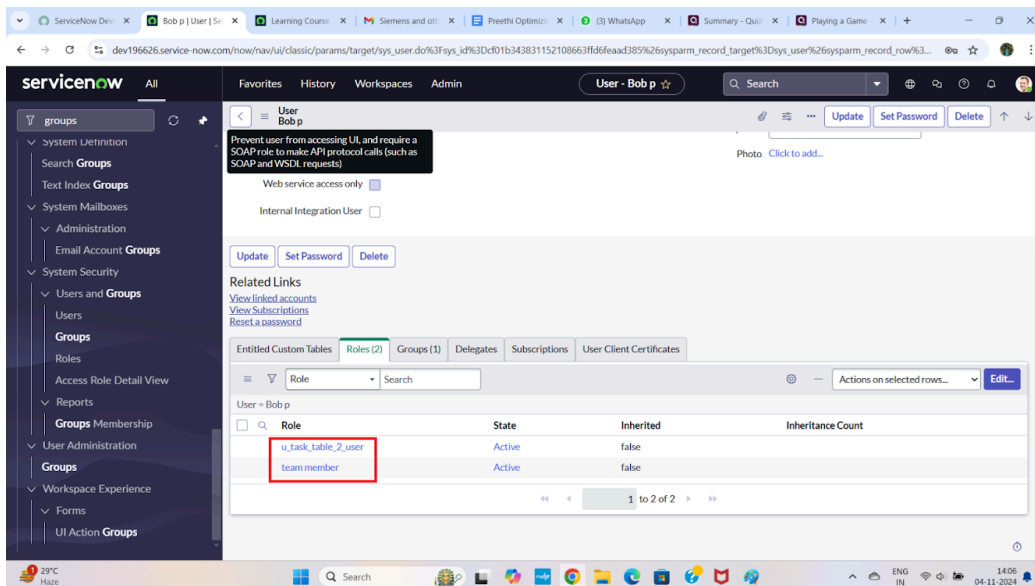
STEPS:

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

MILESTONE - 6: Assign roles to users

ACTIVITY -1 : Assign roles to Alice users

STEPS :



The screenshot displays the ServiceNow user management interface. The left sidebar shows the navigation menu with 'Users and Groups' selected. The main content area shows the 'User - Bob p' profile. The 'Roles' tab is active, displaying a table of roles assigned to the user. The table has columns for 'Role', 'State', 'Inherited', and 'Inheritance Count'. Two roles are listed: 'ui_task_table_2_user' and 'team member', both with a state of 'Active'. The 'ui_task_table_2_user' role is highlighted with a red box.

Role	State	Inherited	Inheritance Count
ui_task_table_2_user	Active	false	
team member	Active	false	

MILESTONE-7: Application Access

ACTIVITY -1: Assign table to Access to application

PURPOSE:Control which users or roles have access to which data. It allows for granular control over data visibility and modification, ensuring that users only interact with the information relevant to their roles and responsibilities.

USES :Controlling access and ensuring data security. Access to tables is typically managed through roles, which define the level of access users or groups have to the data.

STEPS:

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

The screenshot shows the ServiceNow 'Application Menu - project table' configuration page. The page has a dark header with the ServiceNow logo and navigation tabs: All, Favorites, History, Admin. The main title is 'Application Menu - project table'. Below the title, there's a description: 'An application menu is a group of modules in the application navigator. Choose the roles that are required to access the application and add or remove modules in the related list below. [More Info](#)'. The form includes several fields: 'Title' (project table), 'Application' (Global), 'Active' (checked), 'Roles' (project member), 'Category' (Custom Applications), 'Hint', and 'Description'. At the bottom, there are 'Update' and 'Delete' buttons. An 'Activate Windows' watermark is visible in the bottom right corner.

servicenow All Favorites History Admin Application Menu - project table Search

< Application Menu project table Update Delete

An application menu is a group of modules in the application navigator. Choose the roles that are required to access the application and add or remove modules in the related list below. [More Info](#)

* 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

Description

Update Delete

Activate Windows
Go to Settings to activate Windows.

servicenow All Favorites History Admin Application Menu - task table 2 Search

Application Menu - task table 2

Active ☒

Restricts access to the specified roles. Otherwise, all users can view the application menu when it is active.

Roles u_task_table_2_user, project member, 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

Description

Modules Order Search

Activate Windows Go to Settings to activate Windows. Actions on selected rows...

MILESTONE-8 : Access control list

ACTIVITY - 1 : create ACL

PURPOSE: Manage and control access to resources, whether it's network traffic, files, or other protected resources. ACLs define who or what is allowed to access a resource and what actions they are permitted to perform. This helps organizations secure sensitive information, regulate network traffic, and optimize resource usage.

USES : Manage and restrict access to resources, whether they are network resources, files, or other objects within a system.

STEPS:

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

Warning: A role, security attribute, data condition, or script is required to properly secure access with this ACL.

* Type: record

* Operation: write

Decision Type: Allow If

Admin overrides: ☒

Protection policy: -- None --

* Name: task table 2 [u_task_table_2]

Description:

Applies To: No. of records matching the condition: 1

Add Filter Condition Add "OR" Clause

-- choose field -- -- oper -- -- value --

Application: Global

Active: ☒

Advanced: ☐

Submit

Conditions

Access Control Rules have two decision types, and these types will behave differently depending on conditions.

7. Scroll down under requires role

8. Double click on insert a new row

9. Give task table and team member role

10. Click on submit

11. Similarly create 4 acl for the following fields

Access Controls

Name Search

Actions on selected rows... New

All > Created on Today

Name	Decision Type	Operation	Type	Active	Updated by	Updated
u_leave_request	Allow If	delete	record	true	admin	2024-10-22 02:27:59
u_leave_request	Allow If	create	record	true	admin	2024-10-22 02:27:59
u_task_table	Allow If	read	record	true	admin	2024-10-22 04:21:28
u_task_table	Allow If	write	record	true	admin	2024-10-22 04:20:15
u_task_table.u_assigned_to	Allow If	write	record	true	admin	2024-10-22 04:33:53
u_task_table.u_due_date	Allow If	write	record	true	admin	2024-10-22 04:33:14
u_task_table.u_task_id	Allow If	write	record	true	admin	2024-10-22 04:27:47
u_task_table.u_task_name	Allow If	write	record	true	admin	2024-10-22 04:31:14
u_task_table_2	Allow If	write	record	true	admin	2024-10-22 21:05:07
u_task_table_2	Allow If	read	record	true	admin	2024-10-22 21:26:57
u_task_table_2	Allow If	read	record	true	admin	2024-10-22 21:05:07
u_task_table_2	Allow If	write	record	true	admin	2024-10-22 21:28:27
u_task_table_2	Allow If	create	record	true	admin	2024-10-22 21:05:06
u_task_table_2	Allow If	delete	record	true	admin	2024-10-22 21:05:07
u_task_table_2.u_assigned_to	Allow If	write	record	true	admin	2024-10-22 21:31:20

1 to 20 of 23

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

MILESTONE-9: Flow

ACTIVITY : create A flow to assign operations ticket to groups

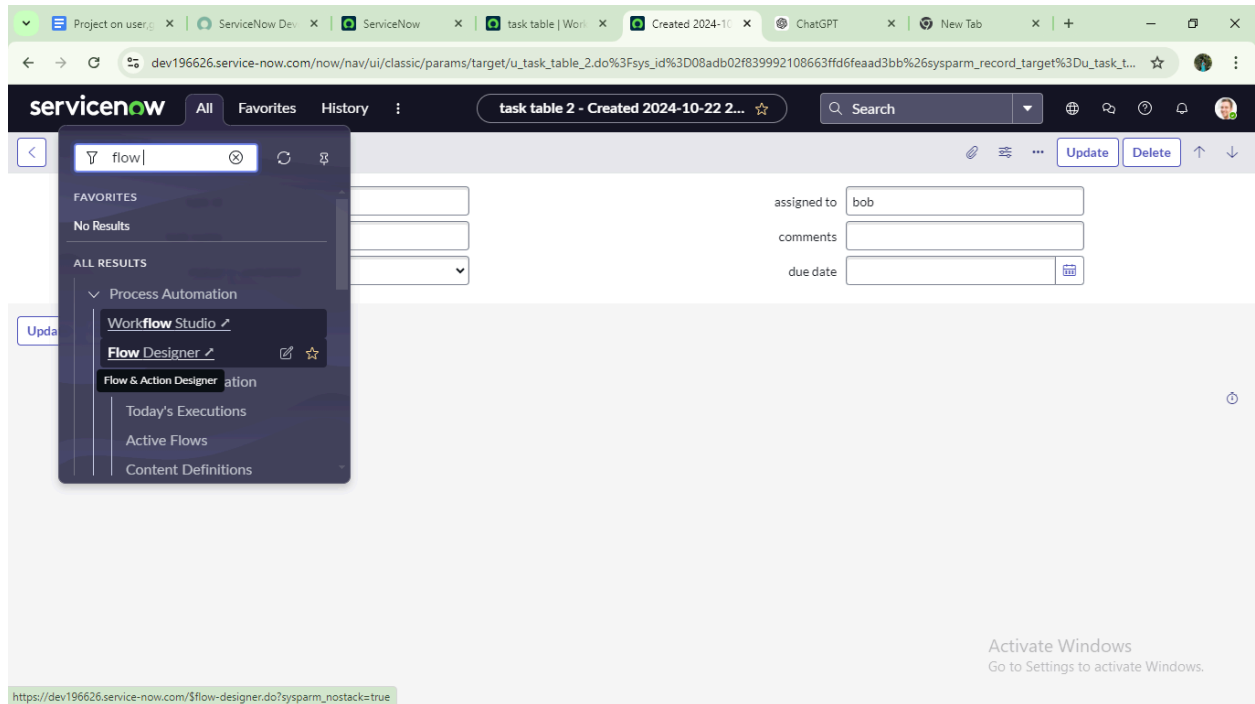
PURPOSE : Automate and streamline the process of distributing incoming tickets to the appropriate teams or individuals based on predefined criteria. This ensures efficient workload distribution, minimizes manual effort, and ultimately improves response times and overall operational efficiency.

USES : leveraging workflow automation tools. This can streamline operations, improve efficiency, and ensure tickets are handled by the appropriate teams.

STEPS :

1. Open service now.
2. Click on All >> search for Flow Designer
3. Click on Flow Designer under Process Automation.

4. After opening Flow Designer Click on new and select Flow.
5. Under Flow properties Give Flow Name as “ task table”.
6. Application should be Global.
7. Click build flow.



Workflow Studio

task table Flow

Homepage Operations Integrations

Playbooks **Flows** Subflows Actions Decision tables

Flows 39
Last refreshed just now

Name	Application	Status	Active	Update
Benchmark Recommendation Evaluator	Benchmarks Spoke	Published	true	2024-09-11 07:08:05
Business process approval flow	Global	Published	true	2020-09-11 07:08:05
Change - Cloud Infrastructure - Authorize	Global	Published	true	2020-11-11 07:08:05
Change - Emergency - Authorize	Global	Published	true	2020-10-06 05:39:49
Change - Emergency - Implement	Global	Published	true	2020-09-23 05:06:26
Change - Emergency - Review	Global	Published	true	2020-10-27 04:18:08
Change - Normal - Assess	Global	Published	true	2020-10-06 05:37:05
Change - Normal - Authorize	Global	Published	true	2020-10-06 05:38:35
Change - Normal - Implement	Global	Published	true	2020-09-23 04:23:59

Pick up where you left off

- task table
Last updated: 14 min. ago by Syst...
- Create Flow Data
Last updated: 5 months ago by Sy...
- Steps
Last updated: 5 months ago by Sy...

Latest updates

- System Administrator modified task table
14 min. ago
- System Administrator modified Create Flow Data
5 months ago
- System Administrator modified Steps Settings to activate Windows.
5 months ago

Workflow Studio

task table Flow

Operations New Flow | Worl...

dev196626.service-now.com/now/workflow-studio/builder?typeSysId=2d85e527439231106c4bb0117fb8f208&sysId=-1

Let's get the details for your flow

Flow name *
task table

Description
Describe your flow.

Application *
Global

> Show additional properties

Activate Windows
Go to Settings to activate Windows.
Cancel Build flow

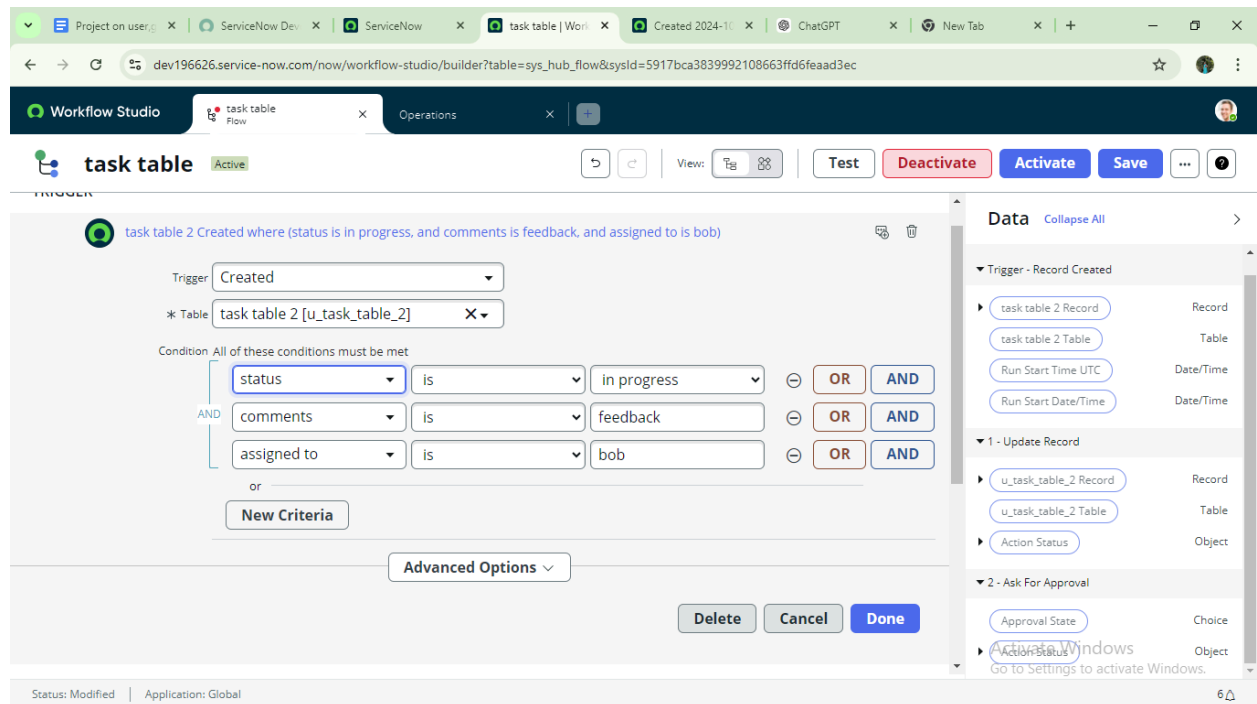
1. Click on Add a trigger
2. Select the trigger in that Search for "create record" and select that.
3. Give the table name as task table
4. Give the Condition as Field : status

Operator :is Value : in progress

Field : comments Operator :is Value : feedback

Field : assigned to Operator :is Value : bob

5.After that click on Done.



Next step:

1.Click on Add an action.

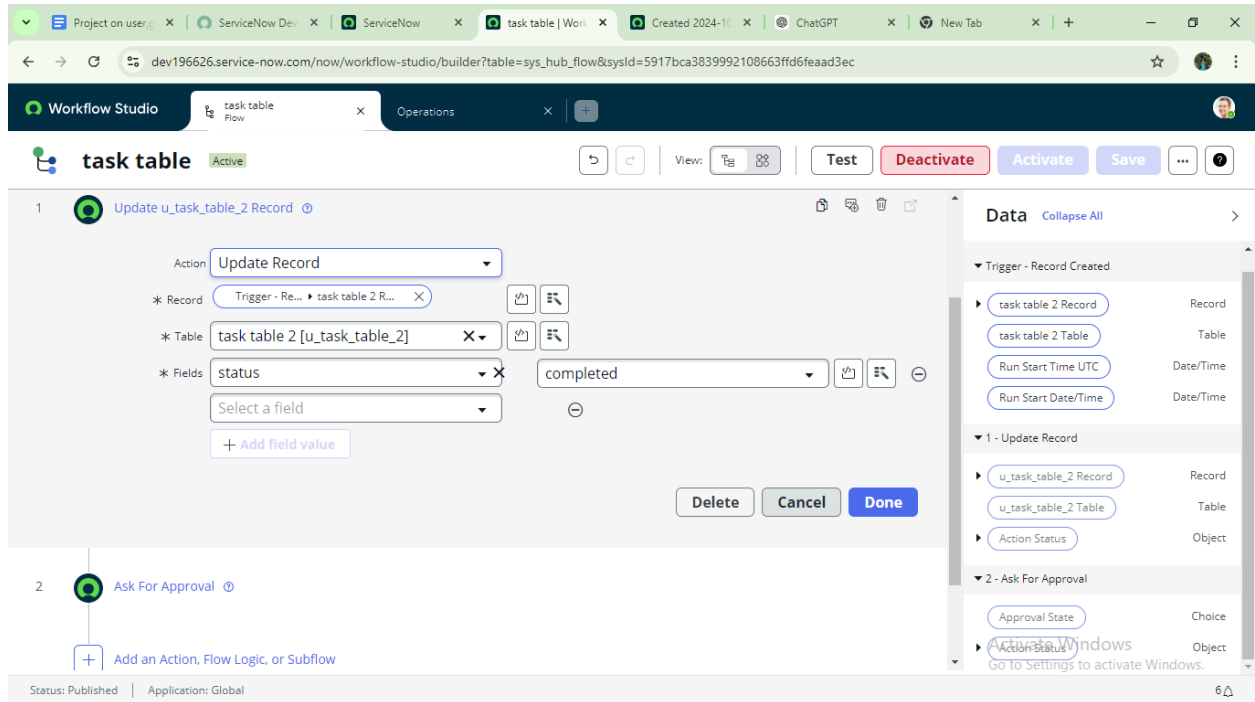
2.Select action in that ,search for “ update records”.

3.In Record field drag the fields from the data navigation from Right Side(Data pill)

4.Table will be auto assigned after that

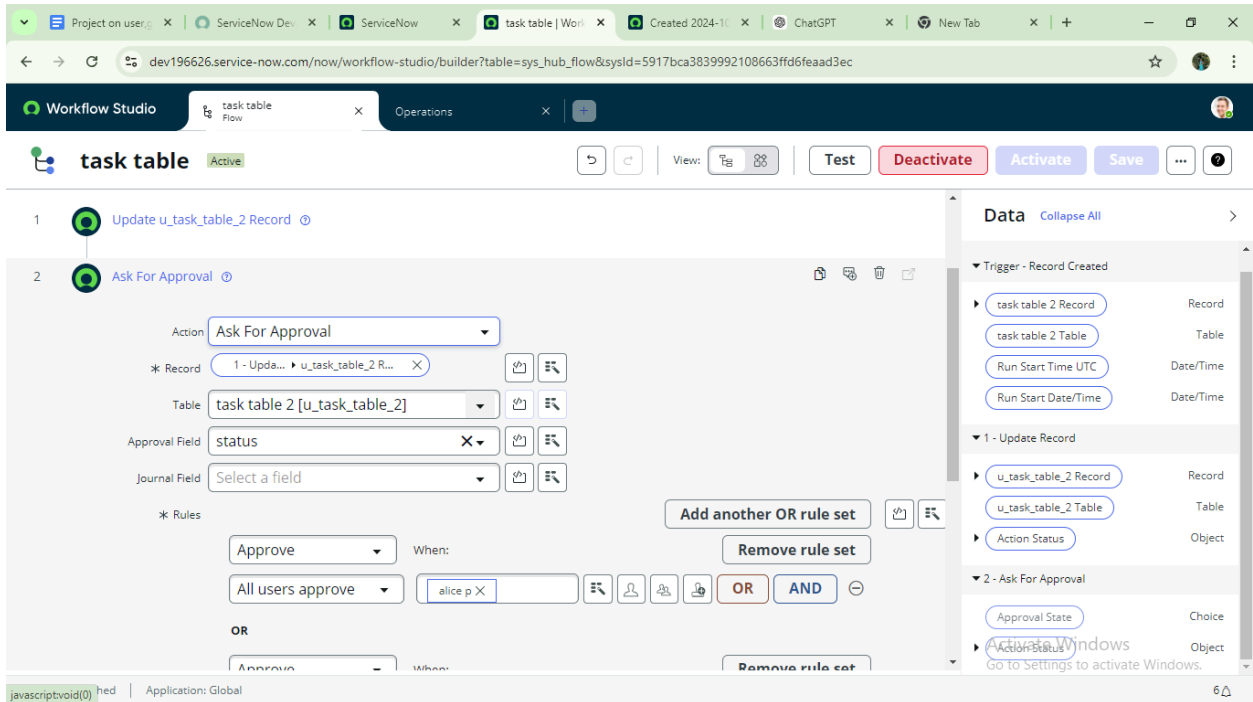
5.Add fields as “status” and value as “completed”

Click on Done.

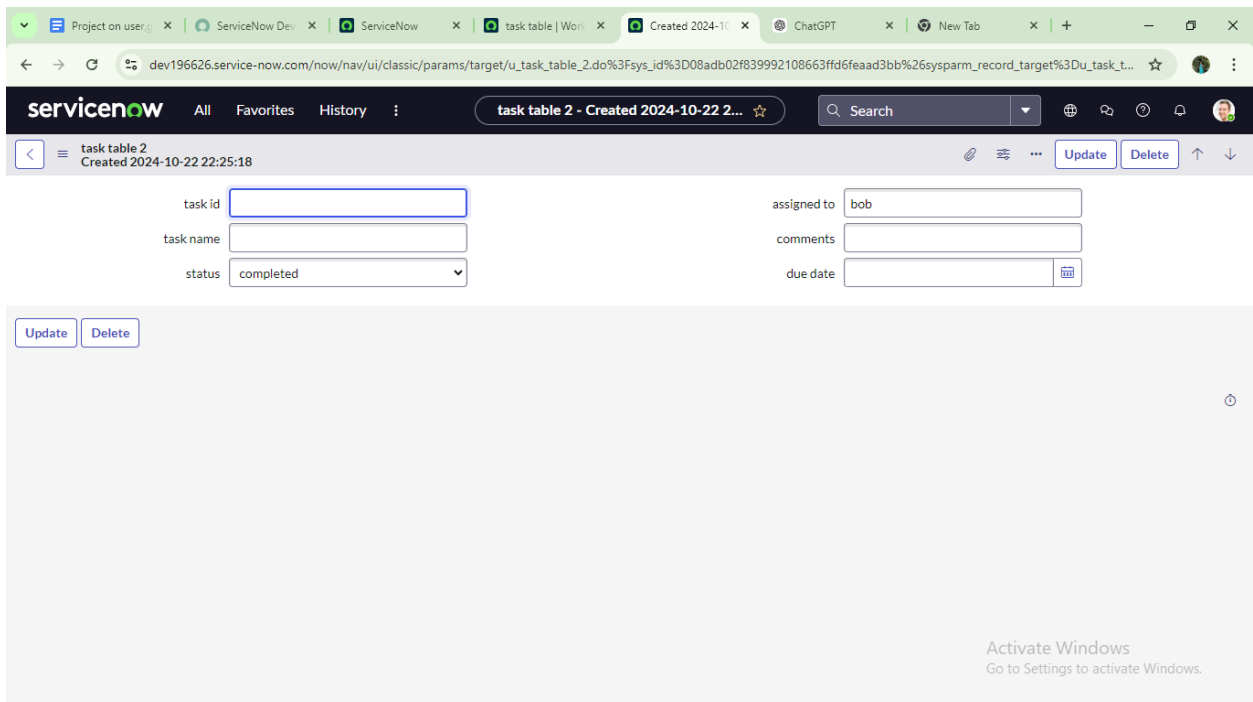


Next step:

1. Now under Actions.
2. Click on Add an action.
3. Select action in that, search for “ask for approval
4. In Record field drag the fields from the data navigation from Right side
5. Table will be auto assigned after that
6. Give the approve field as “status”
7. Give approver as alice p
8. Click on Done.



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



- 1.Go to application navigator and search for my approval
- 2.Click on my approval under the service desk.

3. Alice p got approval request then right click on requested then select approved

ADVANTAGES & DISADVANTAGES

ADVANTAGES:

Enhanced Security:

By limiting access to only the necessary resources based on roles, organizations can significantly reduce the risk of unauthorized access and data breaches. This granular control helps protect sensitive information and critical systems.

Improved Efficiency:

RBAC allows for the efficient assignment and management of permissions, streamlining workflows and improving productivity. Users can easily access the resources they need for their specific roles, reducing time wasted on navigating permissions or requesting access.

Simplified Administration:

Managing access rights becomes easier as permissions are tied to roles rather than individual users. This simplifies onboarding new employees, updating access rights, and auditing user activity.

Enhanced Compliance:

RBAC helps organizations adhere to regulatory requirements and internal policies by providing clear audit trails and controlled access. This simplifies compliance efforts and reduces the risk of penalties.

Reduced Errors:

Centralizing access control and using roles to define permissions reduces the likelihood of misconfigurations and errors associated with managing individual user permissions.

DISADVANTAGES

Complexity:

Designing and implementing RBAC can be complex, especially in large organizations with diverse roles and responsibilities. This complexity can increase the time and resources required for setup and maintenance.

Potential for Role Explosion:

In large organizations, the number of roles can become unwieldy, leading to "role explosion". This can make it difficult to manage roles and permissions effectively.

Maintenance Overhead:

Maintaining RBAC requires ongoing effort to update roles, permissions, and workflows as organizational structures and user responsibilities change.

Potential for Over-Permissioning:

While RBAC aims to minimize access, there's still a risk of over-permissioning, where users have access to more resources than they need. This can be mitigated by carefully designing roles and regularly reviewing access permissions.

Reliance on Accurate Role Definition:

RBAC's effectiveness depends on accurate and up-to-date role definitions. If roles are not defined correctly, it can lead to security vulnerabilities or inefficiencies.

CONCLUSION

This scenario highlights a structured approach to project management, showcasing the roles of Alice and Bob within a defined workflow. With Alice's oversight and Bob's execution, the team effectively collaborates to ensure project success. The use of tables organizes key information, facilitating easy tracking of projects, tasks, and progress updates. Overall, this system promotes accountability, enhances communication, and leads to the successful completion of projects.