



**Optimizing User, Group, and Role Management
with Access Control and Workflows**

NAAN MUDHALVAN REPORT

Submitted by

DEFFINA EMMIMAL S(953422104022)

CHRISLIN RESHMA D(953422104021)

CHERMA PON UDHAYA M(953422104020)

DILAKA BHARATHI J(953422104024)

in partial fulfillment for the award of the degree

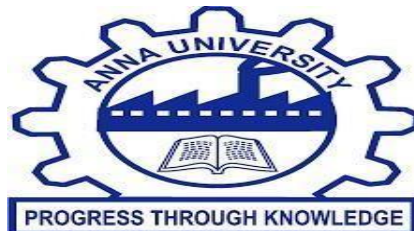
Of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE AND ENGINEERING

V V COLLEGE OF ENGINEERING , TISAIYANVILAI



ANNA UNIVERSITY : CHENNAI 600 025

NOVEMBER 2025

BONAFIDE CERTIFICATE

Certified that this project report “**OPTIMIZING USER, GROUP AND ROLE MANAGEMENT WITH ACCESS CONTROL AND WORKFLOWS**” is the Bonafide work of “**DEFFINA EMMIMAL S (953422104022) , CHRISLIN RESHMA D(953422104021), CHERMA PON UDHAYA (953422104020) , DILAKA BHARATHI J (953422104024)**” who carried out the naan mudhalvan project work under my supervision.

SIGNATURE

Mrs.T.Premalatha.,M.Tech.,

SUPERVISOR

SIGNATURE

Dr.R.Jensi.,M.E.,Ph.D.,

HEAD OF THE DEPARTMENT

Submitted for the viva-voce held on -----

Internal Examiner

External Examiner

TABLE OF CONTENTS

CHAPTER NO.	TITLE NO	PAGE
1.	INTRODUCTION	
2.	IDEATION PHASE	
3.	REQUIREMENT PHASE	
4.	PROJECT DESIGN	
5.	PROJECT PLANNING & SCHEDULING	
6.	FUNCTIONAL & PERFORMANCE TESTING	
7.	RESULTS	
8.	ADVANTAGES AND DISADVANTAGES	
9.	CONCLUSION	
10.	FUTURE SCOPE	
11.	APPENDIX	

1. INTRODUCTION

1.1 PROJECT OVERVIEW

The project “**Optimizing User, Group, and Role Management with Access Control and Workflows**” focuses on enhancing security, efficiency, and automation in managing user access within an organization using ServiceNow. In many organizations, managing users, assigning them to groups, and defining roles are often done manually through spreadsheets or email requests. This manual approach can lead to inconsistencies, unauthorized access, and delays in onboarding or offboarding employees.

Using **ServiceNow’s Role-Based Access Control (RBAC)** and **workflow automation**, this project introduces a structured and automated system to manage users, groups, and roles effectively. The system ensures that each user receives the right level of access based on their job function or department. When a new user is added, the workflow automatically assigns them to the appropriate group and roles, routes the request to the manager for approval, and updates records in real-time. Similarly, when users change departments or leave the organization, their access is modified or revoked automatically.

This project highlights how ServiceNow’s **Access Control Rules, Approval Workflows, and Automation Policies** can be utilized to streamline identity and access management. It ensures compliance, reduces administrative workload, and enhances data security by maintaining proper authorization at every step of the process.

1.2 PURPOSE

The main purpose of this project is to automate and optimize the management of users, groups, and roles in ServiceNow by implementing Access Control and workflow automation. This ensures that the right people have the right access at the right time, improving security and efficiency.

Objectives:

- Automate user, group, and role creation and updates.
- Implement approval workflows for controlled access requests.
- Apply Access Control Rules (ACLs) to secure data and permissions.
- Minimize manual administrative effort through workflow automation.

Benefits:

1. **Enhanced Security:** Ensures users only access data and applications relevant to their roles.
2. **Operational Efficiency:** Automates role assignments and access approvals, minimizing manual intervention.
3. **Transparency:** All access-related actions are logged and traceable within the ServiceNow platform.
4. **Faster Onboarding/Offboarding:** New users get the necessary access quickly, and departing users are automatically deactivated.
5. **Centralized Management:** Administrators can easily monitor, review, and audit user permissions, ensuring compliance and consistency across the system.

2. IDEATION PHASE

2.1 PURPOSE

The main purpose of this project is to automate and streamline the management of users, groups, and roles within ServiceNow using Access Control and workflow automation. This ensures that every user receives appropriate access based on their responsibilities, improving security, consistency, and operational efficiency across the organization.

By utilizing ServiceNow's automation capabilities, the project aims to create a digital workflow where access requests are systematically recorded, reviewed, and approved. Each request is routed to the appropriate authority for validation and implemented without manual intervention.

2.2 GOALS AND CHALLENGES:

Goals:

- To automate and simplify user, group, and role management within ServiceNow.
- To ensure secure and controlled access through Access Control and approval workflows.
- To improve operational efficiency and maintain compliance across the organization.

Challenges:

- 1) Ensuring accurate role assignments and avoiding excessive access permissions.
- 2) Managing complex approval workflows and maintaining proper authorization levels.
- 3) Integrating Access Control with existing systems without disrupting operations.

Pain Points:

- Repetitive manual work.
- Delayed responses.
- Lack of centralized record keeping.

Needs:

- Secure Access
- Automation
- Compliance

2.3 BRAINSTROMING

Ideas Generated:

- Design a centralized module in ServiceNow for managing **Users, Groups, and Roles**.
- Add mandatory fields: User Name, Department, Role Type, Access Level, and Approval Status.
- Create a **Flow Designer workflow** to automate role assignment and approval routing.
- Enable automatic **email notifications** for role assignment, access approval, and revocation.
- Provide a **dashboard** for administrators to monitor user access requests, approvals, and activity logs.

Key Questions:

1. Who should authorize the creation or modification of user roles?
2. How should administrators be notified about pending access requests?
3. Should the system include automated deactivation for inactive or offboarded users?

3. REQUIREMENT PHASE

3.1 OBJECTIVE

To design and implement a **User, Group, and Role Management System** in ServiceNow that automates access provisioning, approval workflows, and access control enforcement to ensure data security and compliance

Current Challenges:

- MaManual user and role assignments leading to inconsistent permissions.
- Lack of transparency in access approvals and change history.
- Difficulty in tracking user access during onboarding and offboarding

Expected Outcomes:

1. Centralized platform for managing users, groups, and roles.
2. Automated access approval workflows and real-time notifications.
3. Enhanced compliance and visibility into access control operations.

Scope:

- User and role creation and management.
- Access Control Rules (ACL) configuration.
- Automated approval and notification workflows.
- Integration with HR or identity systems for onboarding/offboarding.
- Role-based reporting and audit tracking.

Stakeholders:

1. Employees (Access Requesters)
2. Managers (Approvers)
3. System Administrators (Access Controllers)
4. IT Security Team (Auditors and Reviewers)

Success Metrics:

- 90% reduction in manual access management tasks.
- 100% tracking of all access requests and approvals.
- Access provisioning time reduced by at least 70%.

3.2 SOLUTIONS REQUIREMENTS**Functional Requirements:**

- Create a centralized module for managing Users, Groups, and Roles.
- Automate workflow routing for access approval and role assignment.
- Enable real-time notifications for user creation, modification, or revocation.
- Provide dashboards for monitoring access requests and activity logs.

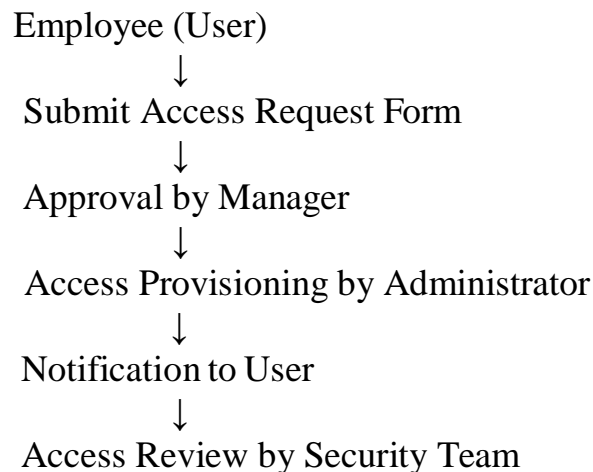
Non-Functional Requirements:

- Simple and responsive design.
- 24/7 accessibility via Service Portal.
- Secure access with proper role-based permissions.

Technical Requirements:

- 1) Use of ServiceNow modules: **Flow Designer, Access Control Rules, Notifications.**
- 2) Configuration via **Update Sets** for version control and migration.
- 3) Integration with **User, Group, and Role tables** for automation and reporting.

3.3 FLOW DIAGRAM



This logical flow ensures controlled access, clear accountability, and complete traceability of user and role management activities.

3.4 TECHNOLOGY STACK:

Platform: ServiceNow ITSM

Automation: Flow Designer, Workflow Editor, and Business Rules

Notification: Email, ServiceNow Alerts, and In-App Notifications

Scripting: JavaScript and Glide Scripting for server-side and client-side logic

Access Control: Role-Based Access Control (RBAC) using ACLs, Groups, and Roles for secure data and function management

4. PROJECT DESIGN

4.1 TECHNOLOGY STACK

Core Platform: ServiceNow ITSM

Workflow Automation: Flow Designer

Notification System: Email Templates

Database: ServiceNow Tables

Security: Role-based Access Control

4.2 PROPOSED SOLUTION

The solution focuses on automating **User, Group, and Role Management** in ServiceNow to streamline access control processes. It enables the automatic routing of access requests through defined approval workflows, ensuring that only authorized users receive the correct level of access.

Benefits :

- Reduces manual workload for administrators and managers.
- Improves transparency in access approvals and modifications.
- Provides real-time status updates and complete access history.
- Enhances scalability and security across organizational departments.

4.3 SOLUTION ARCHITECTURE

1. Define User Roles (Requester, Approver, Administrator, Security Auditor).
2. Build Access Request Form for users.
3. Develop Approval Workflow in Flow Designer.
4. Configure Access Control Rules and Notifications.
5. Test and validate all approval and access scenarios.
6. Deploy to Service Portal for end-user accessibility.

5. PROJECT PLANNING & SCHEDULING

PHASE	DURATION
Requirement Analysis	1 Hour
Form and Role Configuration	1 Hour
Workflow Development	2 Hours
Notification Setup	1 Hour
Access Control Setup	30 Minutes
Testing & Debugging	2 Hours
Documentation	1 Hour

6. FUNCTIONAL AND PERFORMANCE TESTING

6.1 PERFORMANCE TESTING

- Test workflow execution time and access assignment speed.
- Verify system stability under multiple concurrent access requests.
- Ensure smooth performance during heavy load conditions.

6.2 FUNCTIONAL TESTING

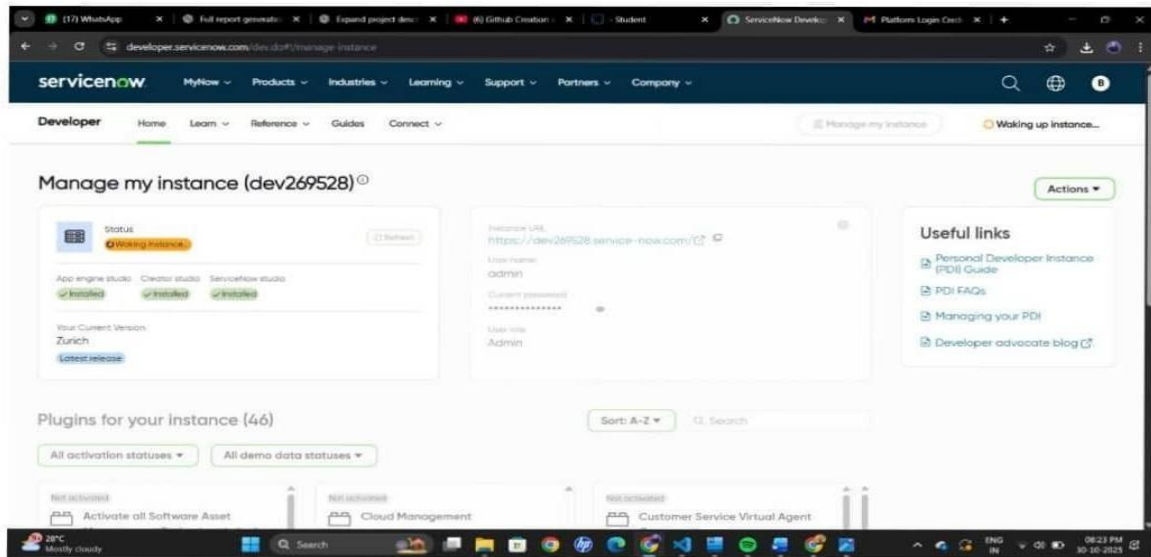
- **Validate user and role creation forms.**
- **Verify approval routing and access modification workflows.**
- **Ensure notifications trigger correctly for each action.**
- **Confirm that administrators can view and manage access logs accurately.**
-

7. RESULTS

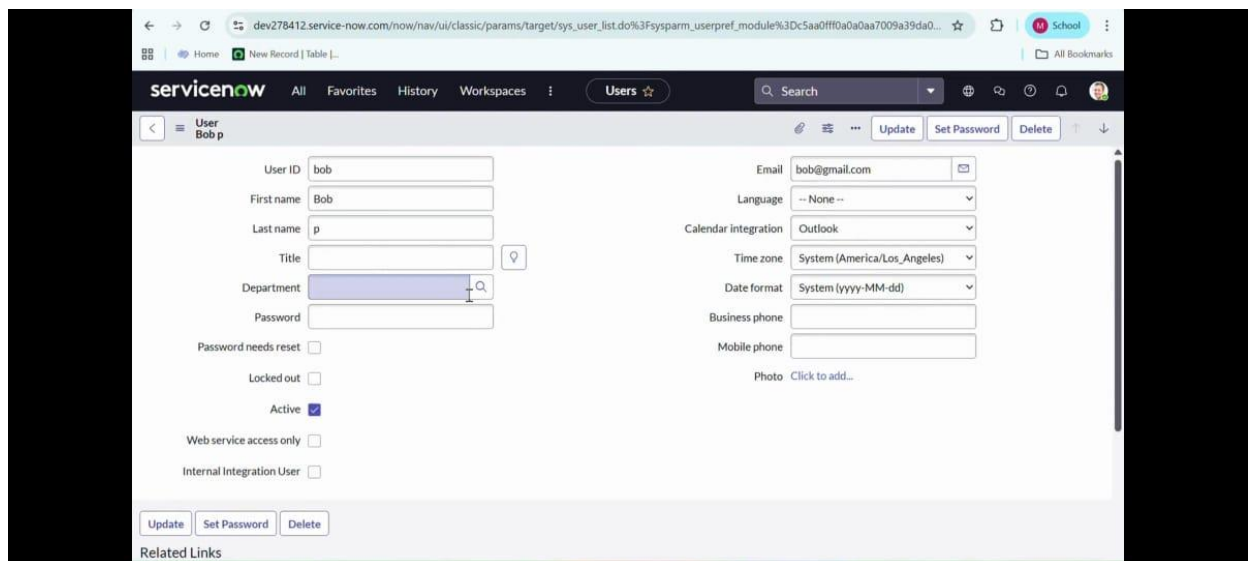
Output Screens:

- Creation of users.
- Creation of Groups.
- Creation of roles.
- Assigning Roles to user.
- Assign table access to application.
- Creation of Access control list (ACL).
- Create a flow to assign operations Tickets to group
- Testing the Flow

7.1 SETTING UP SERVICE NOW INSTANCE



7.2 CREATION OF USER

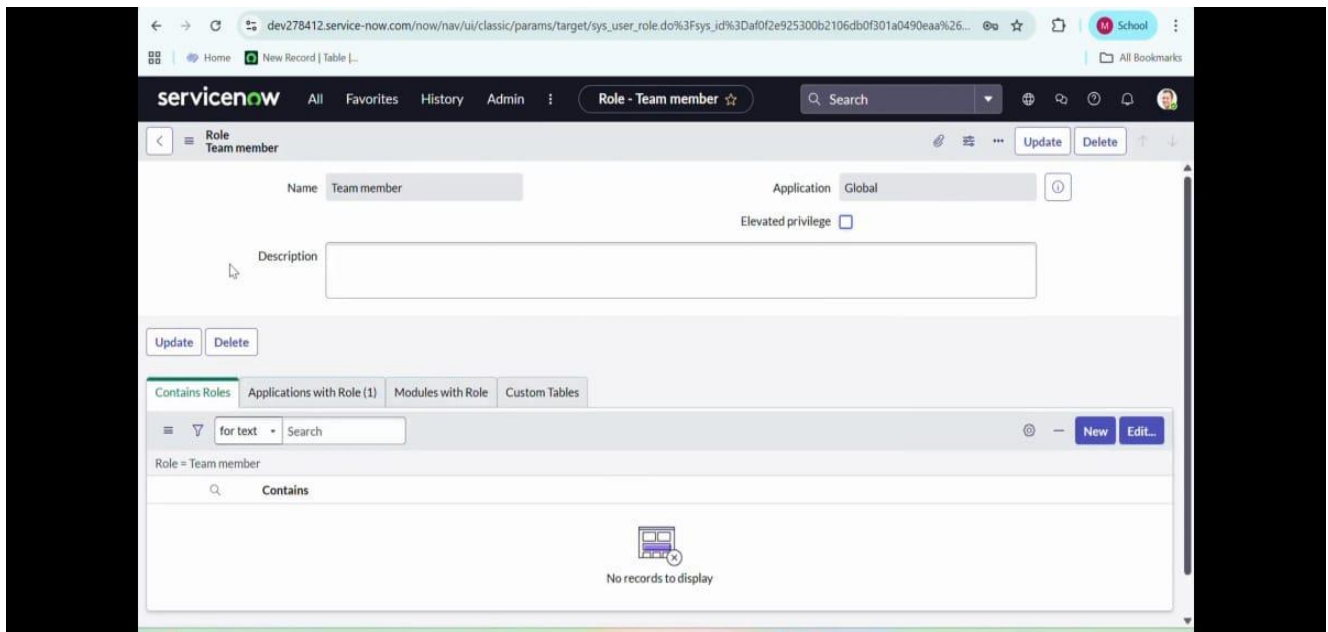


7.3 CREATION OF GROUPS

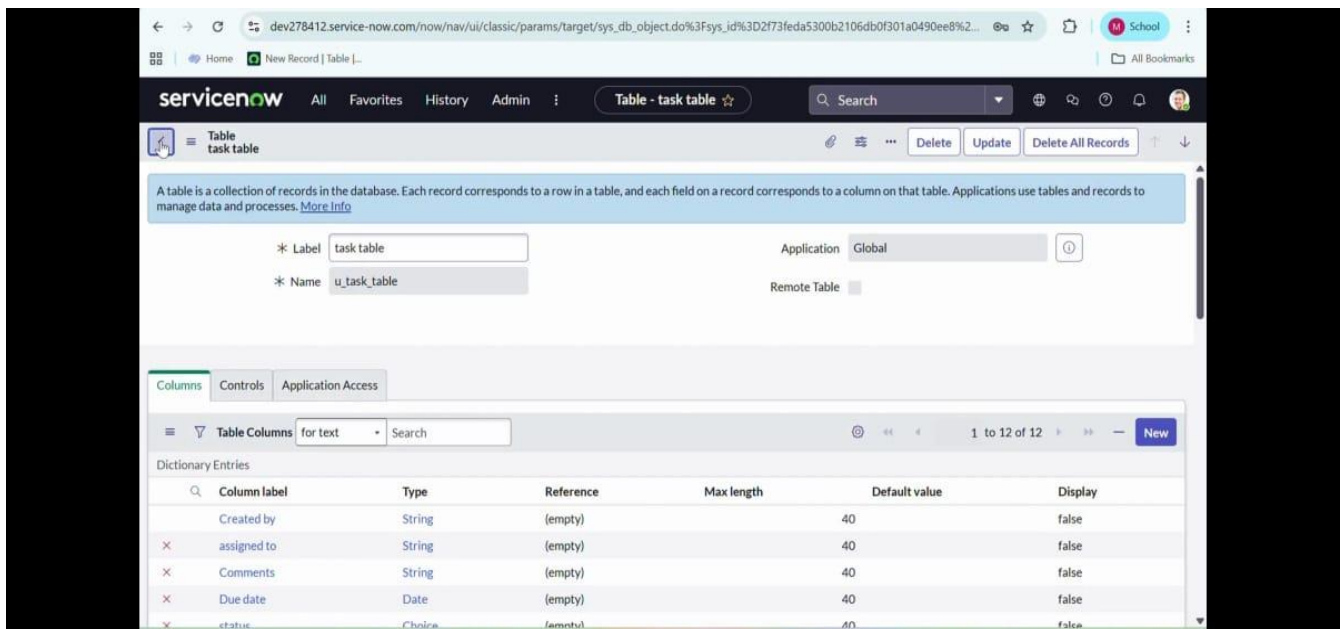
The screenshot shows the ServiceNow interface for creating a group. The browser address bar displays a URL from dev278412.service-now.com. The top navigation bar includes 'All', 'Favorites', 'History', 'Workspaces', and a breadcrumb 'Group - project team'. The main form has fields for 'Name' (filled with 'project team'), 'Group email', 'Manager', 'Parent', and a large 'Description' text area. Below the form are 'Update' and 'Delete' buttons. A tabbed interface shows 'Roles', 'Group Members (2)', and 'Groups'. The 'Roles' tab is active, showing a table with columns 'Created', 'Role', 'Granted by', and 'Inherits'. The table is empty, with a message 'No records to display' at the bottom.

7.4 CREATION OF ROLES:

The screenshot shows the ServiceNow interface for creating a role. The browser address bar displays a URL from dev278412.service-now.com. The top navigation bar includes 'All', 'Favorites', 'History', and a breadcrumb 'Role - project member'. The main form has fields for 'Name' (filled with 'project member'), 'Application' (set to 'Global'), and 'Elevated privilege' (unchecked). There is a large empty 'Description' text area. Below the form are 'Update' and 'Delete' buttons. A tabbed interface shows 'Contains Roles', 'Applications with Role (2)', 'Modules with Role', and 'Custom Tables'. The 'Contains Roles' tab is active, showing a table with columns 'for text' and 'Search'. The table is empty, with a message 'No records to display' at the bottom.



7.5 ASSIGNING ROLES TO USER:



7.6 ASSIGN TABLE ACCESS TO APPLICATION:

The screenshot shows the ServiceNow configuration page for a table named 'project table'. The page is titled 'Table - project table' and includes a search bar and navigation links. Below the title, there is a description: 'A table is a collection of records in the database. Each record corresponds to a row in a table, and each field on a record corresponds to a column on that table. Applications use tables and records to manage data and processes. [More Info](#)'. The configuration fields include: Label (project table), Name (u_project_table), Application (Global), and Remote Table (unchecked). Below these fields, there 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
Updated	Date/Time	(empty)	40		false
status	Choice	(empty)	40		false
start date	Date	(empty)	40		false
Created by	String	(empty)	40		false
end date	Date	(empty)	40		false

The screenshot shows the ServiceNow configuration page for a group named 'project team'. The page is titled 'Group - project team' and includes a search bar and navigation links. Below the title, there are fields for Manager, Parent, and Description. Below these fields, there are 'Update' and 'Delete' buttons. The 'Roles' tab is active, showing a table of 'Group Members (2)'. The table has columns for 'User' and 'Groups'. The 'User' column is selected, and the table shows two users: 'alice p' and 'Bob p'.

User	Groups
alice p	
Bob p	

dev278412.service-now.com/now/nav/ui/classic/params/target/sys_user.do%3Fsys_id%3De87bee525300b2106db0f301a0490e03%26sys...

servicenow All Favorites History Admin User - alice p Search

User - alice p Internal Integration User ☐

Update Set Password Delete

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... Edit...

User = alice p

<input type="checkbox"/>	Role	State	Inherited	Inheritance Count
<input type="checkbox"/>	project member	Active	false	
<input type="checkbox"/>	u_task_table_user	Active	false	
<input type="checkbox"/>	u_project_table_user	Active	false	

1 to 3 of 3

https://dev278412.service-now.com/sys_user_role.do?sys_id=57012965300b...

dev278412.service-now.com/now/nav/ui/classic/params/target/sys_user.do%3Fsys_id%3Df82ca2d2534c72106db0f301a0490e86%26sysp...

servicenow All Favorites History Admin User - Bob p Search

User - Bob p Active ☒ Photo Click to add...

Web service access only ☐

Internal Integration User ☐

Update Set Password Delete

Related Links
[View linked accounts](#)
[View Subscriptions](#)
[Reset a password](#)

Entitled Custom Tables Roles (2) Groups (1) Delegates Subscriptions User Client Certificates

Role Search Actions on selected rows... Edit...

User = Bob p

<input type="checkbox"/>	Role	State	Inherited	Inheritance Count
<input type="checkbox"/>	u_task_table_user	Active	false	
<input type="checkbox"/>	Team member	Active	false	

1 to 2 of 2

dev278412.service-now.com/now/nav/ui/classic/params/target/sys_app_application.do%3Fsys_id%3D2f01be1a5300b2106db0f301a0490... School

servicenow All Favorites History 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 Application

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

The text that appears in a tooltip when a user points to this application menu

Hint

Description

dev278412.service-now.com/now/nav/ui/classic/params/target/sys_app_application.do%3Fsys_id%3Dba447a5e5300b2106db0f301a0490... School

servicenow All Favorites History Application Menu - task table Search

Application Menu
task 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 Application

Active ☒

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

Roles
u_task_table_user, project member, Team member

Specifies the [menu category](#), which defines the navigation menu style. The default value is Custom Applications.

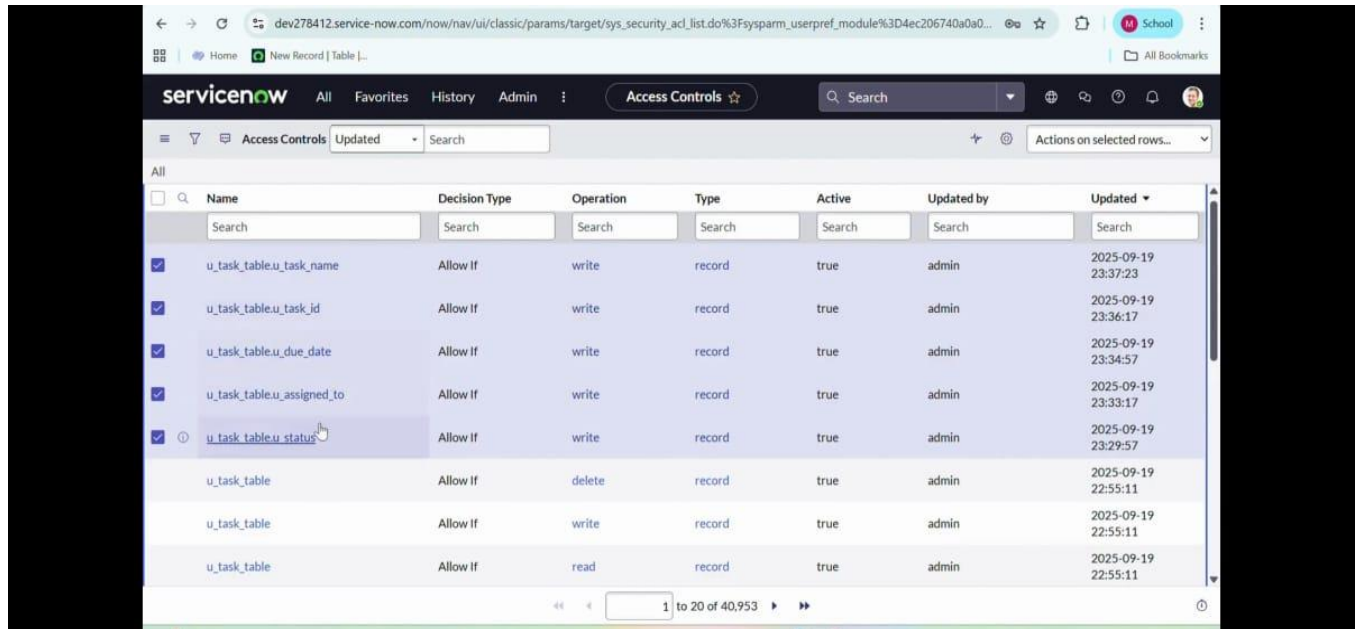
Category

The text that appears in a tooltip when a user points to this application menu

Hint

Description

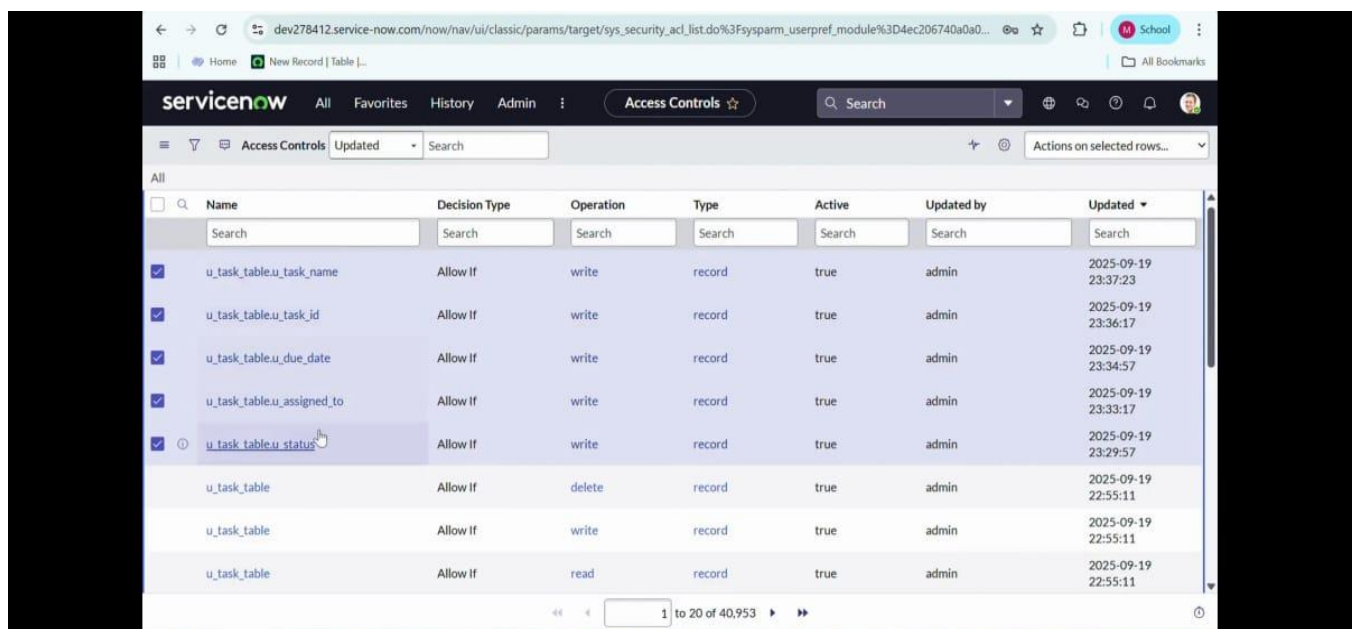
7.7 CREATION OF ACCESS CONTROL LIST(ACL):



The screenshot shows the ServiceNow 'Access Controls' list. The table contains the following data:

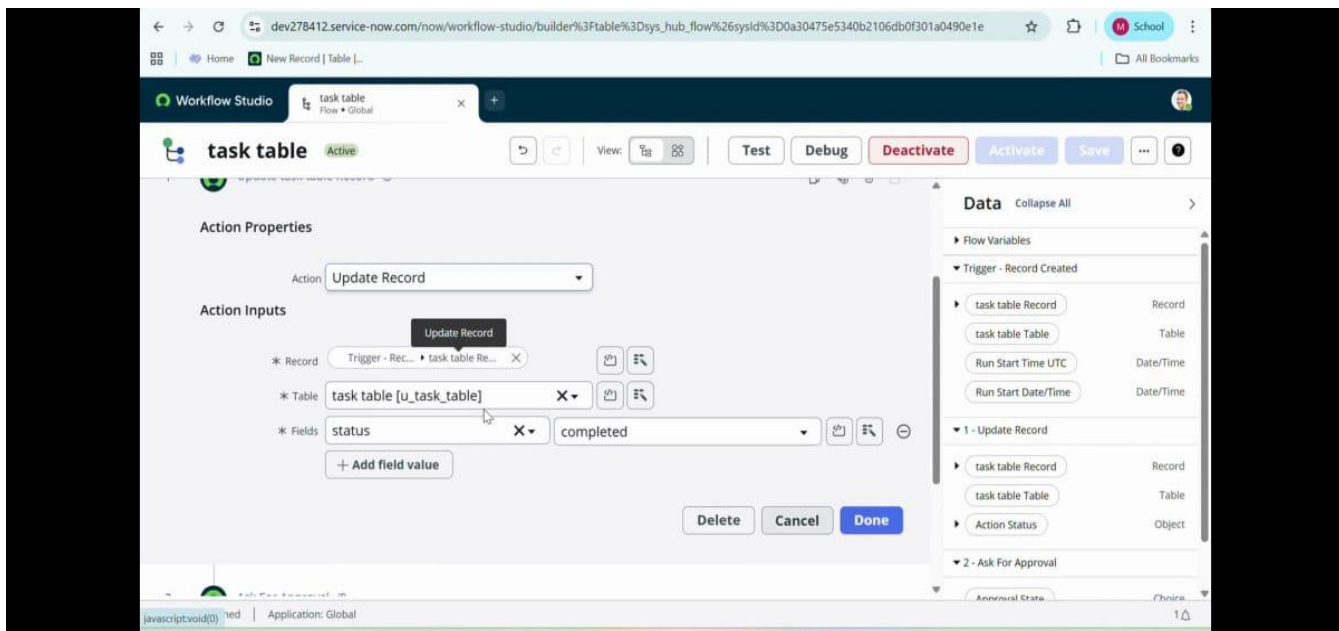
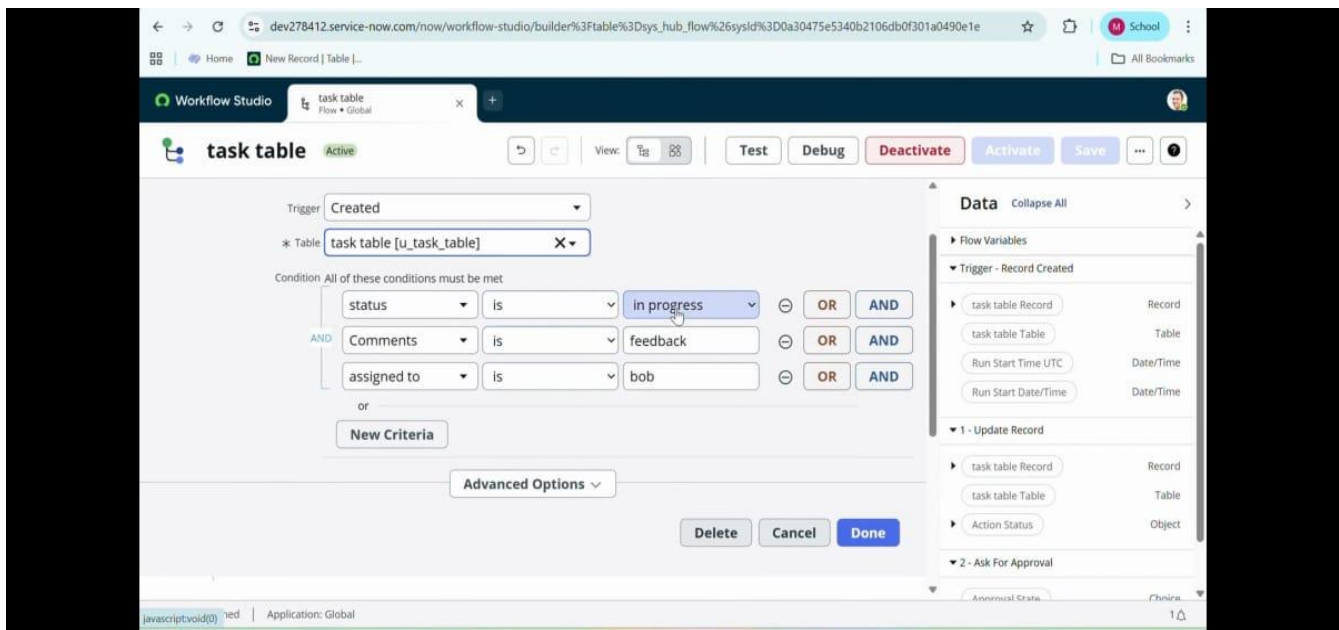
Name	Decision Type	Operation	Type	Active	Updated by	Updated
u_task_table.u_task_name	Allow If	write	record	true	admin	2025-09-19 23:37:23
u_task_table.u_task_id	Allow If	write	record	true	admin	2025-09-19 23:36:17
u_task_table.u_due_date	Allow If	write	record	true	admin	2025-09-19 23:34:57
u_task_table.u_assigned_to	Allow If	write	record	true	admin	2025-09-19 23:33:17
u_task_table.u_status	Allow If	write	record	true	admin	2025-09-19 23:29:57
u_task_table	Allow If	delete	record	true	admin	2025-09-19 22:55:11
u_task_table	Allow If	write	record	true	admin	2025-09-19 22:55:11
u_task_table	Allow If	read	record	true	admin	2025-09-19 22:55:11

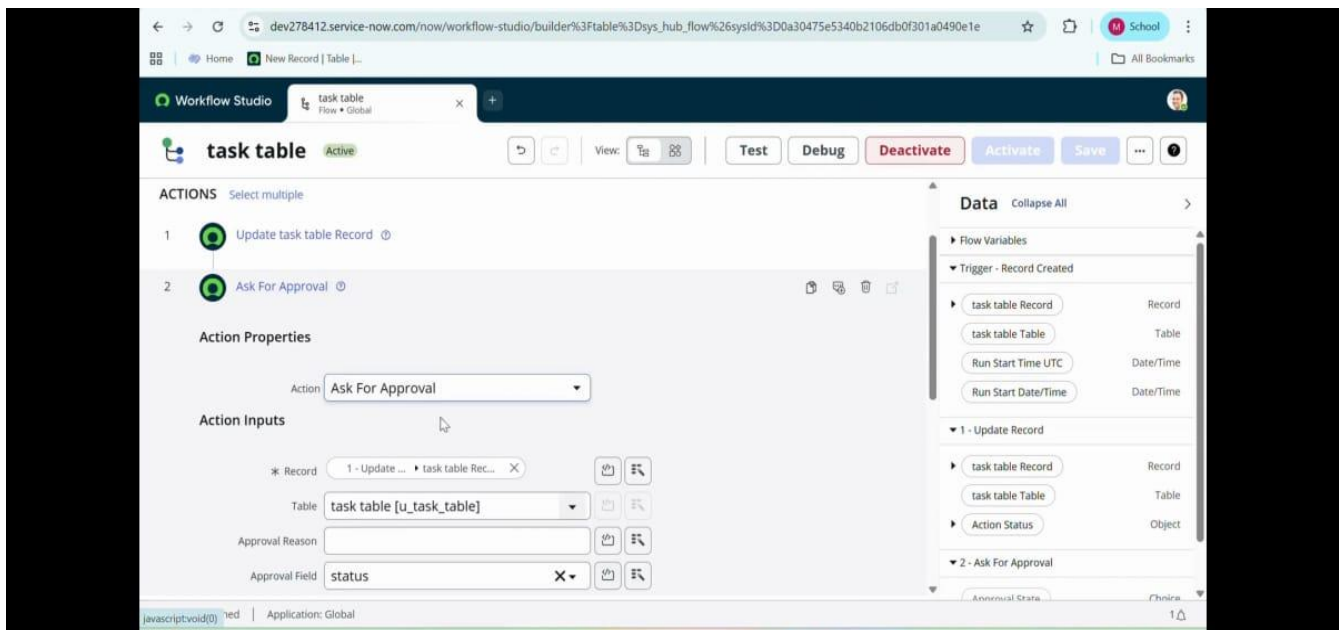
7.8 CREATE A FLOW TO ASSIGN OPERATION TICKETS TO GROUPS:



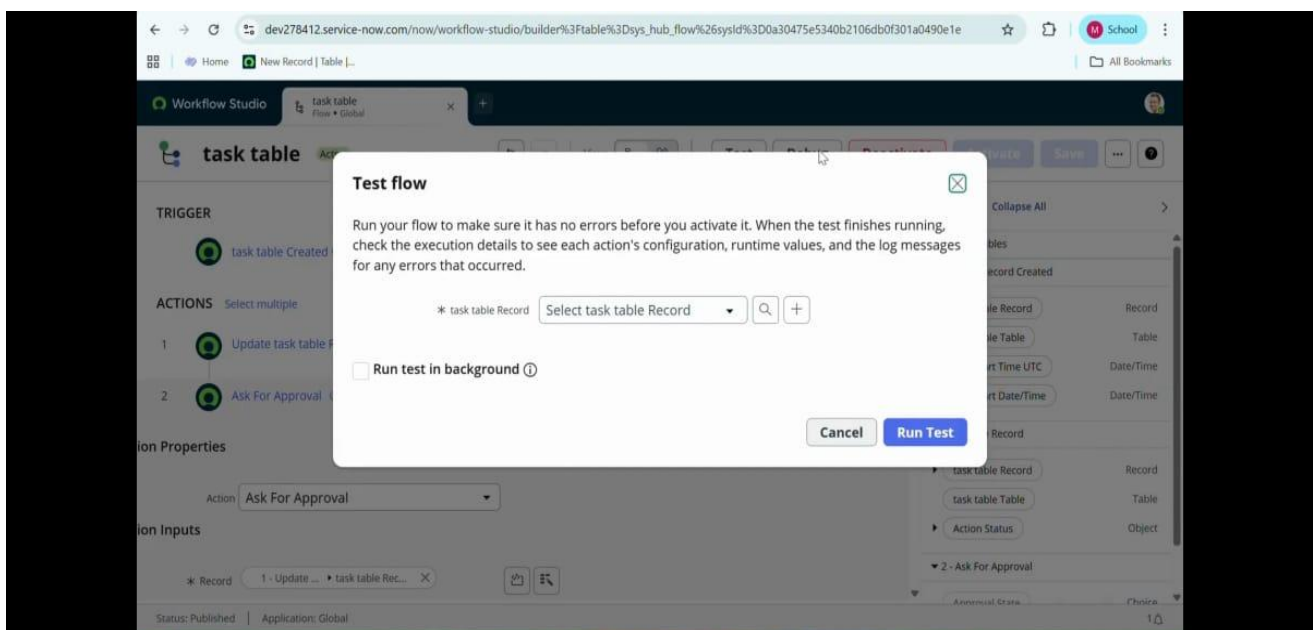
The screenshot shows the ServiceNow 'Access Controls' list, identical to the one above. The table contains the following data:

Name	Decision Type	Operation	Type	Active	Updated by	Updated
u_task_table.u_task_name	Allow If	write	record	true	admin	2025-09-19 23:37:23
u_task_table.u_task_id	Allow If	write	record	true	admin	2025-09-19 23:36:17
u_task_table.u_due_date	Allow If	write	record	true	admin	2025-09-19 23:34:57
u_task_table.u_assigned_to	Allow If	write	record	true	admin	2025-09-19 23:33:17
u_task_table.u_status	Allow If	write	record	true	admin	2025-09-19 23:29:57
u_task_table	Allow If	delete	record	true	admin	2025-09-19 22:55:11
u_task_table	Allow If	write	record	true	admin	2025-09-19 22:55:11
u_task_table	Allow If	read	record	true	admin	2025-09-19 22:55:11





7.9 TESTING THE FLOW:



8.ADVANTAGES AND DISADVANTAGES

Advantages:

- 1)Improved Security
- 2)Centralized Management
- 3) Automated Workflows
- 4)Time Efficiency
- 5)Scalability
- 6)Audit and Compliance

Error Reduction

Disadvantages:

- 1)Complex Setup
- 2)Maintenance Overhead
- 3)Performance Issues
- 4)User Frustration

9.CONCLUSION:

Optimizing user, group, and role management enhances security and efficiency through automation and access control. It minimizes errors and ensures proper authorization across systems. Though complex initially, it offers lasting benefits for modern organizations.

10. FUTURE SCOPE

- 1)Future developments may include AI-driven access control for smarter role assignments.
- 2)Integration with cloud-based identity platforms will enhance scalability and security.
- 3)Automation and analytics will predict and prevent unauthorized access.
- 4)Overall, the focus will shift toward adaptive, intelligent, and zero-trust security systems.

11.APPENDIX:

Source Code: No source code; used ServiceNow Platform

Dataset Link: Not applicable

Git hub :

<https://github.com/dilakabharathi2004125-droid/Optimize-Users-Groups-and-Role-Management>

Demo:

<https://drive.google.com/file/d/1Hpk9fFz1EmtyvKIyHSRaT46Mqhpy01yE/view?usp=sharing>