OPTIMIZING USER, GROUP, AND ROLE MANAGEMENT WITH ACCESS CONTROL AND WORKFLOWS

Submitted by

Team Leader

Kapil Navajan V C (910022104301)

Team Members

Viknesh Kumar S (910022104046)

Ajay S (910022104001)

In partial fulfilment for the award of the degree

BACHELOR OF ENGINEERING

in

COMPUTER SCIENCE AND ENGINEERING

NAAN MUDHALVAN LAB

ANNA UNIVERSITY REGIONAL CAMPUS MADURAI-625-019

ANNA UNIVERSITY: CHENNAI 600 025

NOVEMBER 2024

Supervised by

Dr. Srie Vidhya Janani, M.E., Ph.D.,

BONAFIDE CERTIFICATE

This is to certify that the project report titled **" OPTIMIZING USER, GROUP, AND ROLE MANAGEMENT WITH ACCESS CONTROL AND WORKFLOWS "** is the Bonafide work of **Kapil Navajan V C (910022104301), Viknesh Kumar S (910022104046), Ajay S (910022104001)** who carried out the project work under my supervision in the Naan Mudhalvan Lab.

30/10/25

SIGNATURE

HEAD OF THE DEPARTMENT

30/10/25

SIGNATURE

FACULTY

Department of Computer Science and Engineering,

Anna University Regional Campus Madurai-625-019

ACKNOWLEDGEMENT

I extend my heartfelt gratitude to **Dr. Srie Vidhya Janani**, **M.E., Ph.D.,** Faculty Incharge of Naan Mudhalvan Lab, for her guidance and support throughout this project. I also thank my peers and family for their encouragement, without which this project would not have been possible.

I am deeply grateful to **Dr. V. Sasikala, M.E., Ph.D.,** Head of the Department, for her constant support and guidance.

I extend my sincere thanks to all teaching and non-teaching staff of the Department of Computer Science and Engineering and my peers for their support and encouragement.

Finally, I thank my family and friends, whose encouragement and patience motivated me to complete this project successfully.

Team Leader

Kapil Navajan V C (910022104301)

Team Members

Viknesh Kumar S (910022104046)

Ajay S (910022104001)

ABSTRACT

Efficient management of users, groups, and roles is crucial for maintaining security, productivity, and accountability within any organizational system. This project, *"**Optimizing User, Group, and Role Management with Access Control and Workflows**,"* focuses on designing an automated framework to streamline the assignment of user privileges, enforce role-based access policies, and simplify administrative operations. By integrating access control mechanisms with intelligent workflows, the system ensures that each user receives appropriate permissions based on their role and responsibilities, minimizing the risk of unauthorized access. Automated workflows handle user creation, modification, approval, and deactivation processes, reducing manual effort and human error. The project enhances transparency and traceability through activity logs and approval histories. Overall, the proposed solution provides a secure, scalable, and efficient model for managing identity and access across enterprise environments.

Problem Statement:

In many organizations, managing users, groups, and roles manually often leads to inconsistencies, security vulnerabilities, and administrative overhead. Lack of centralized access control can result in unauthorized permissions, delayed approvals, and difficulties in tracking user activities. As systems grow in complexity, ensuring that every user has the right level of access while maintaining operational efficiency becomes a major challenge. There is a need for an automated, workflow-based solution that can optimize user management, enforce access control policies, and streamline the approval process while maintaining security, accountability, and compliance.

Objectives:

1. To design and implement a system that automates user, group, and role management within an organization.
2. To integrate workflow automation for handling user access requests, approvals, and modifications.
3. To establish a secure access control mechanism based on user roles and responsibilities.
4. To reduce administrative effort and human error through centralized management and automation.
5. To ensure transparency and traceability by maintaining detailed activity logs and audit trails.
6. To enhance overall system security, scalability, and compliance with organizational policies.

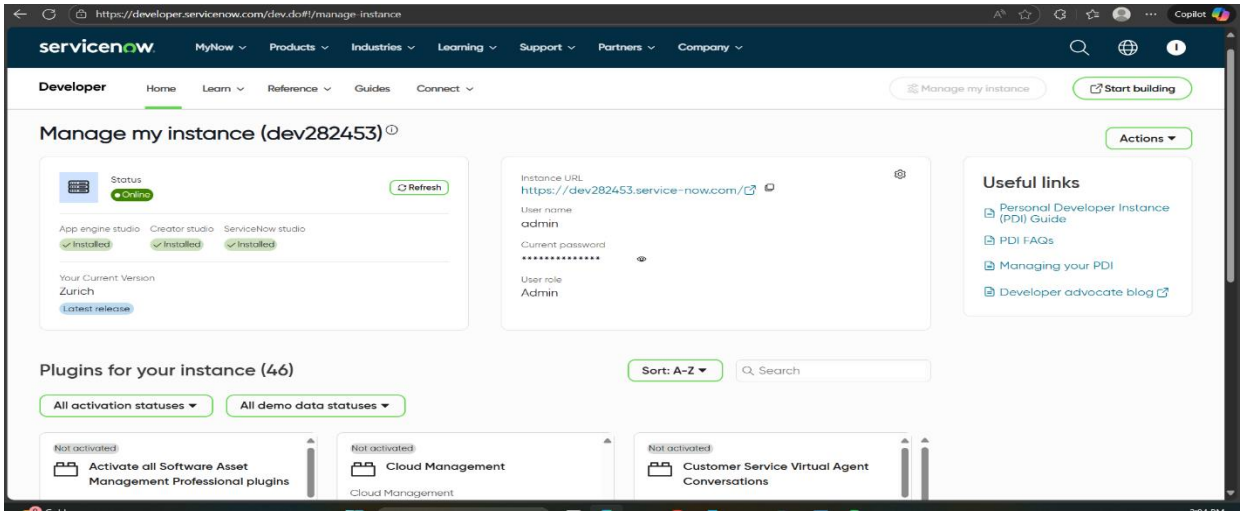
Skills:

TASK INITIATION

Milestone 1: Setting up ServiceNow Instance

Activity: Setting up ServiceNow Instance

1. Sign up for a developer account on the ServiceNow Developer site "https://developer.servicenow.com".
2. Once logged in, navigate to the "Personal Developer Instance" section.
3. Click on "Request Instance" to create a new ServiceNow instance.
4. Fill out the required information and submit the request.
5. You'll receive an email with the instance details once it's ready.
6. Log in to your ServiceNow instance using the provided credentials.

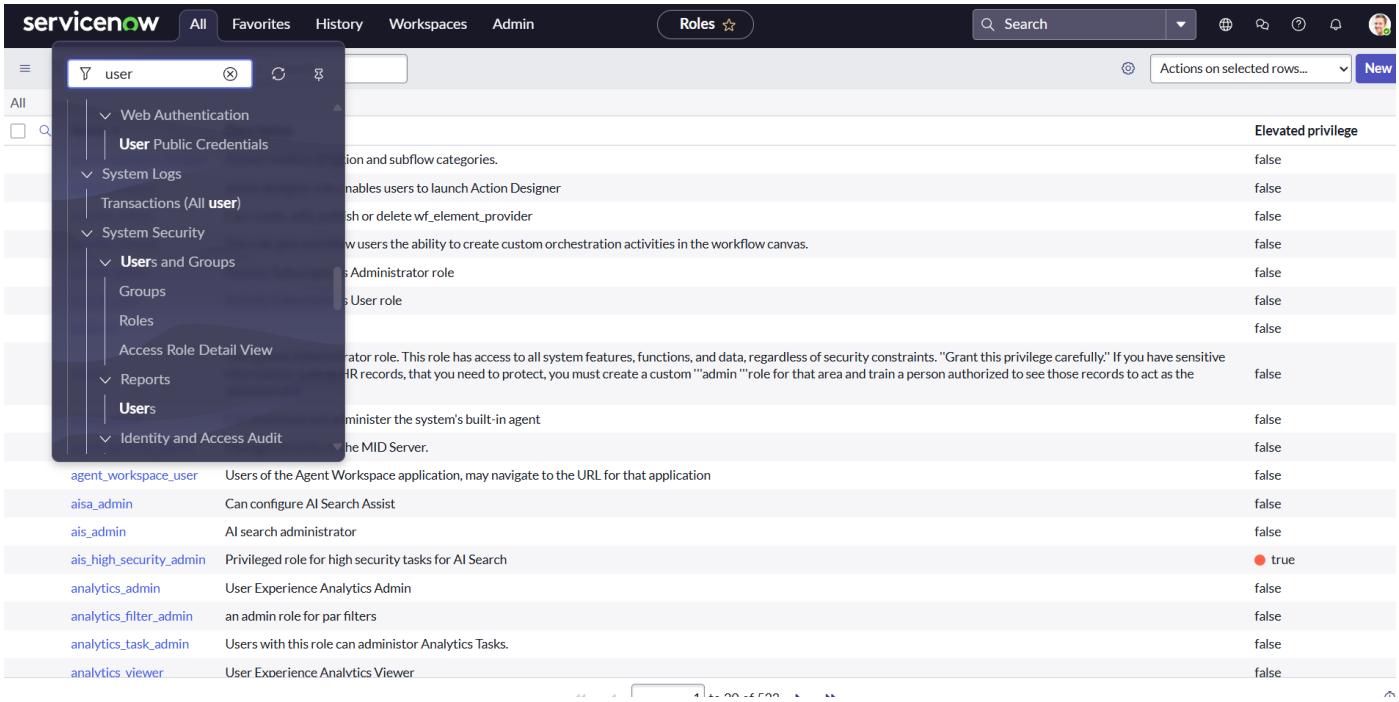


7. Now you will navigate to the ServiceNow.

Milestone 2: Creation of New User

Activity: Creation of New User

1. Open service now



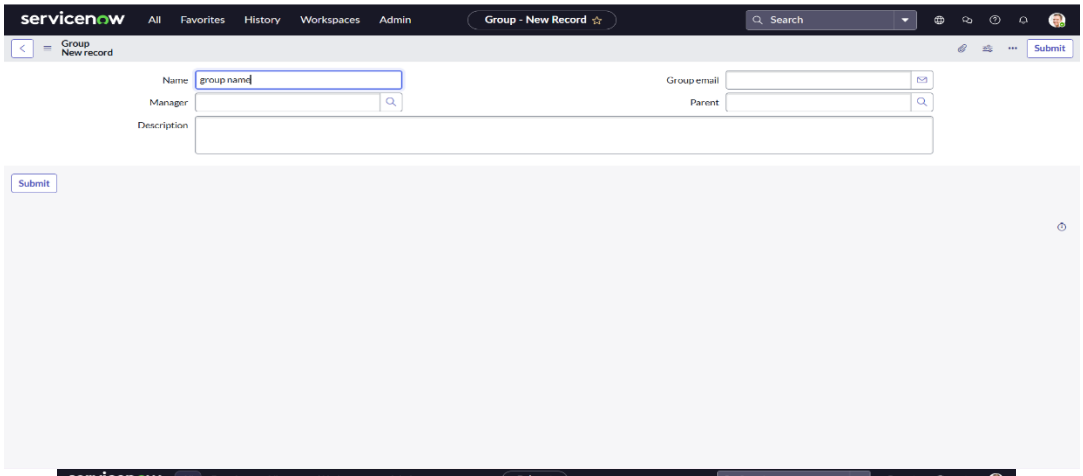
2. Click on All >> search for users
3. Select Users under system security
4. Click on new
5. Fill the following details to create a new user

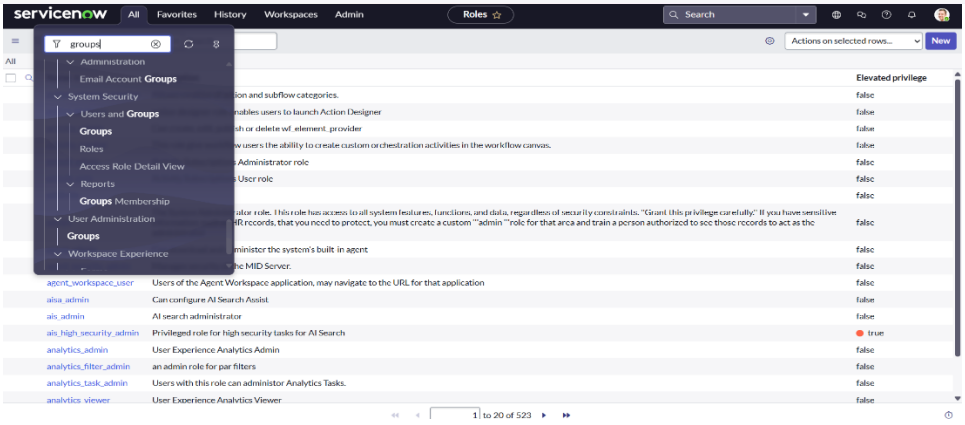
   User : alice,bob
6. Click on submit

Milestone 3: Creation of Group

Activity: Creation of New Group

1. Go to All >> In the filter search for Group > click on New

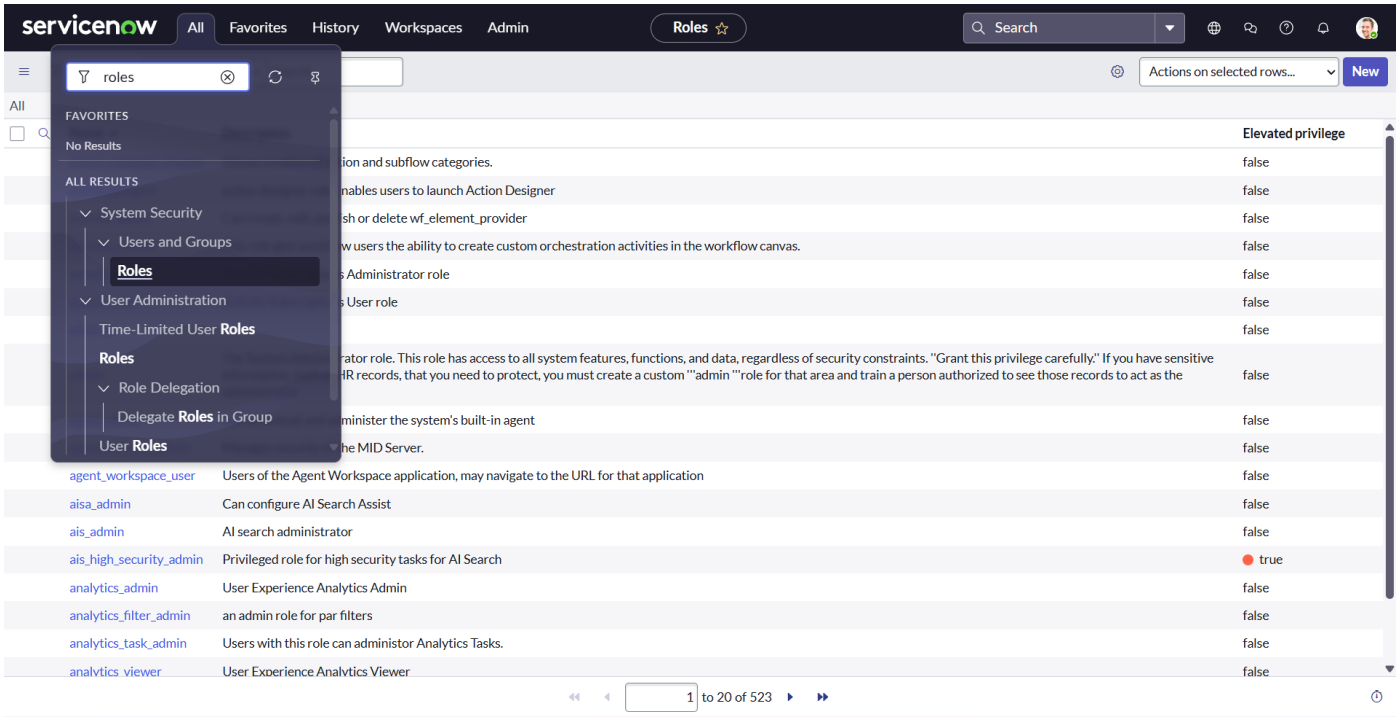




1. Select groups under system security
2. Click on new
3. Fill the following details to create a new group

   Group Name: project team
4. Click on submit

Milestone 4: Creation of Roles

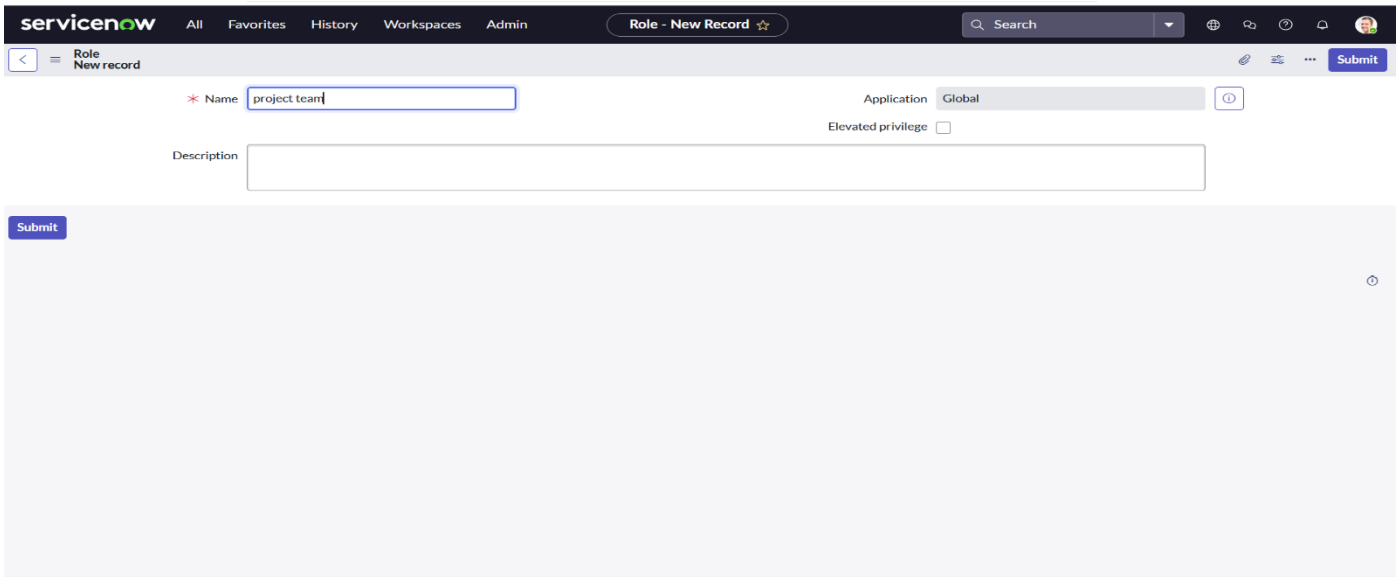


1. Go to All > In the filter search for Roles> click on New.
2. Select roles under system security
3. Click on new

4. Fill the following details to create a new role

   Name of Role: project member

5. Click on submit
6. Go to the Header and right click there >> click on Save.



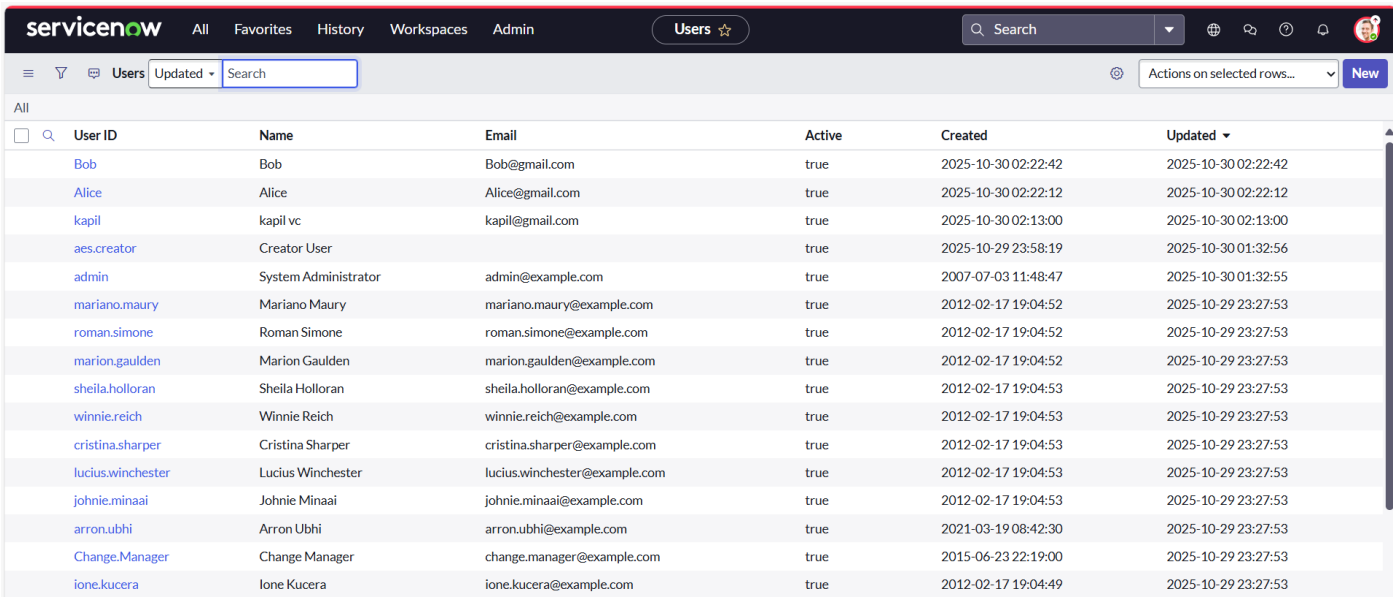
Milestone 5: Assign the Roles to Users

Activity 1: Assign Role to alice

1. Log in to your ServiceNow instance.
2. In the left navigation pane, click on All and search for User.
3. Under System Definition, select the Tables module.
4. Locate and open the record for the Project Manager user.
5. Within the user record, click Edit in the Groups related list.
6. Add the Project Member group to associate the user with project-related activities, then click Save.
7. Next, click Edit in the Roles related list.
8. Add the following roles to the user:

   u_project_table

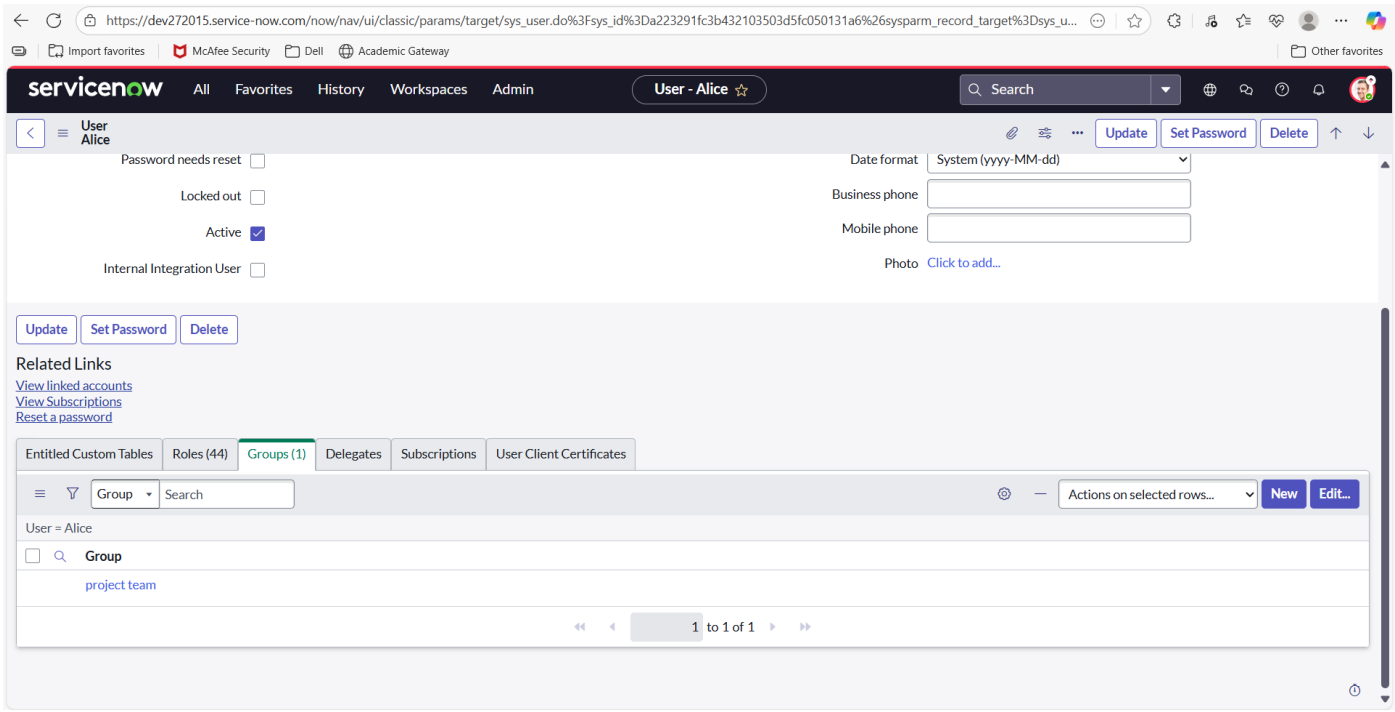
   u_task_table
9. Click Save to apply the changes and then click Update to finalize the record.



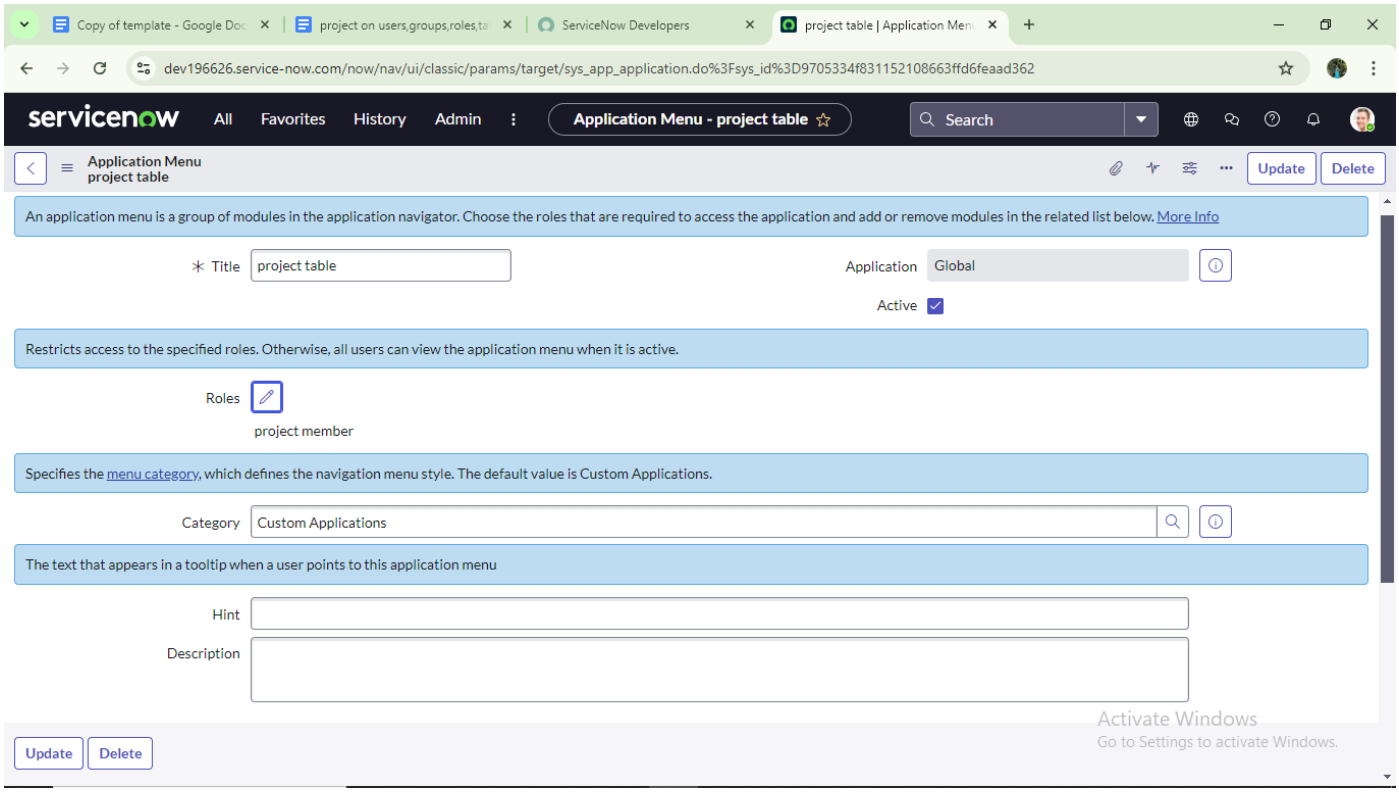
User ID	Name	Email	Active	Created	Updated
Bob	Bob	Bob@gmail.com	true	2025-10-30 02:22:42	2025-10-30 02:22:42
Alice	Alice	Alice@gmail.com	true	2025-10-30 02:22:12	2025-10-30 02:22:12
kapil	kapil vc	kapil@gmail.com	true	2025-10-30 02:13:00	2025-10-30 02:13:00
aes.creator	Creator User		true	2025-10-29 23:58:19	2025-10-30 01:32:56
admin	System Administrator	admin@example.com	true	2007-07-03 11:48:47	2025-10-30 01:32:55
mariano.maury	Mariano Maury	mariano.maury@example.com	true	2012-02-17 19:04:52	2025-10-29 23:27:53
roman.simone	Roman Simone	roman.simone@example.com	true	2012-02-17 19:04:52	2025-10-29 23:27:53
marion.gaulden	Marion Gaulden	marion.gaulden@example.com	true	2012-02-17 19:04:52	2025-10-29 23:27:53
sheila.holloran	Sheila Holloran	sheila.holloran@example.com	true	2012-02-17 19:04:53	2025-10-29 23:27:53
winnie.reich	Winnie Reich	winnie.reich@example.com	true	2012-02-17 19:04:53	2025-10-29 23:27:53
cristina.sharper	Cristina Sharper	cristina.sharper@example.com	true	2012-02-17 19:04:53	2025-10-29 23:27:53
lucius.winchester	Lucius Winchester	lucius.winchester@example.com	true	2012-02-17 19:04:53	2025-10-29 23:27:53
johnie.minaai	Johnie Minaai	johnie.minaai@example.com	true	2012-02-17 19:04:53	2025-10-29 23:27:53
arron.ubhi	Arron Ubhi	arron.ubhi@example.com	true	2021-03-19 08:42:30	2025-10-29 23:27:53
Change.Manager	Change Manager	change.manager@example.com	true	2015-06-23 22:19:00	2025-10-29 23:27:53
ione.kucera	Ione Kucera	ione.kucera@example.com	true	2012-02-17 19:04:49	2025-10-29 23:27:53

Activity 2: Assign Role to alice

1. Log in to your ServiceNow instance.
2. In the left navigation pane, click on All, then search for User.
3. Under System Definition, select Tables.
4. Locate and open the user record for Bob P.
5. In the Team Member section, click Edit to modify group membership.
6. Add Team Member to the user and assign the necessary table roles.
7. Click Save to apply the changes.
8. To test access, click on the Profile icon (top-right corner) and choose Impersonate User → Bob P.
9. Once impersonated, verify that the Task Table 2 is visible, confirming the role assignment and access control functionality.

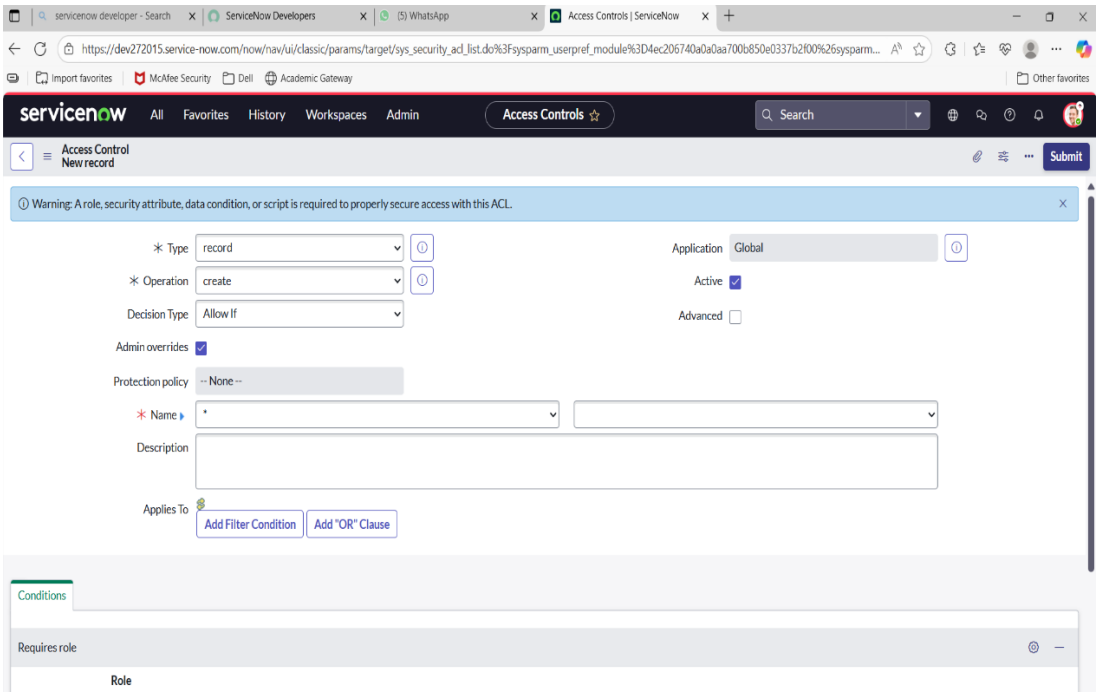


Milestone 6:Application Access



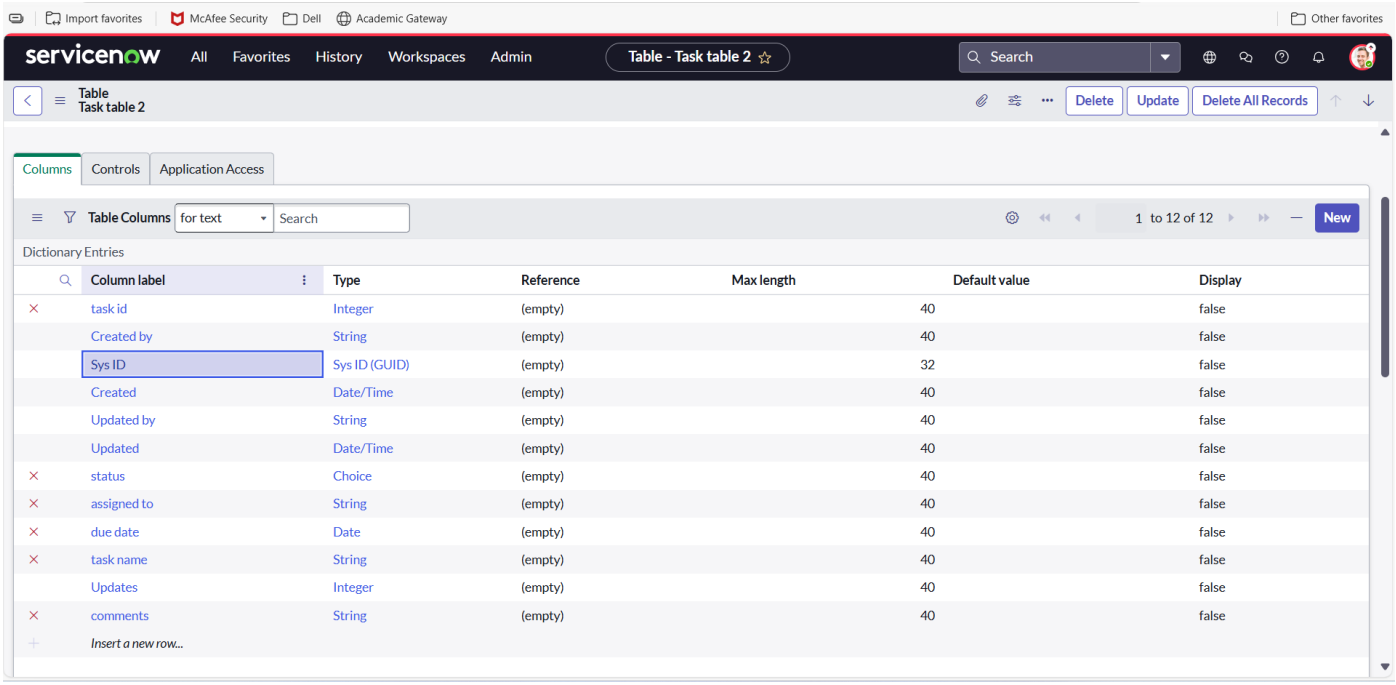
1. When a new table is created in ServiceNow, an application and module are automatically generated for it.

2. In the Application Navigator, search for the Project Table application.
3. Click on Edit Module to modify its access settings.
4. Assign the Project Member role to this application to control access.
5. Next, search for the Task Table 2 application in the Application Navigator.
6. Open the Edit Application option for Task Table 2.
7. Assign both the Project Member and Team Member roles to ensure appropriate permissions.
8. Click Save to apply and update the access settings for both applications.



Milestone 7:Access Control List

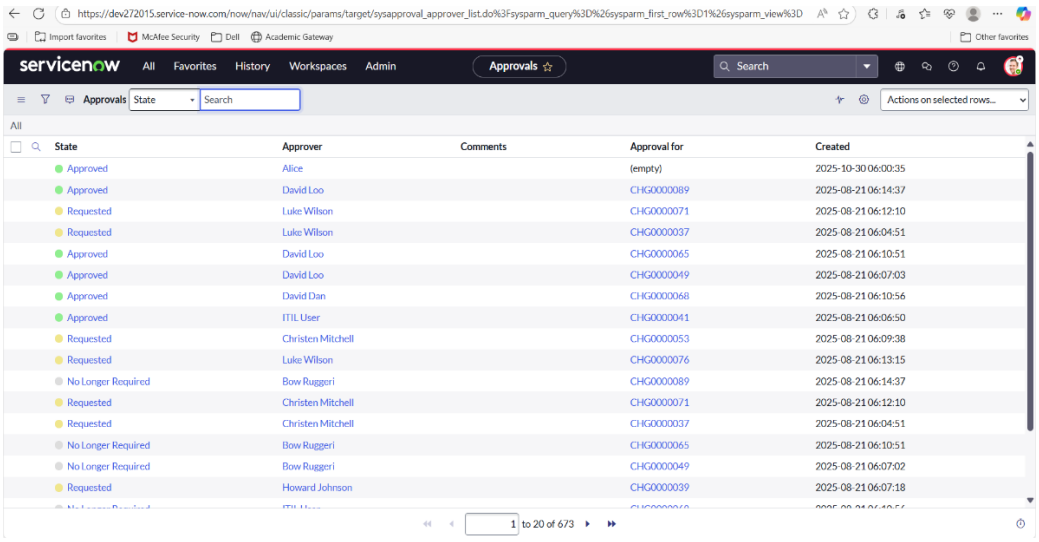
Activity 2: Create ACL



In the Application Navigator, type Access Control (ACL) and select System Security → Access Control (ACL).

1. Select Access Control (ACL) under system security
2. Click on elevate role
3. Click on new
4. Click New to create a new Access Control Rule.
5. Select the table or field you want to secure.
    - u_project_table.name
    - u_project_table

10. Use the Condition Builder to specify access logic.
    - Active is true
11. In the Requires Role field, enter the roles that should have access to this table or field.
    Example:
    - project_member
    - team_member
12. Add Optional Script Logic
13. The script returns true to grant access or false to deny it.
14. Click Submit to save the ACL rule.
15. Use the Test Security option (shield icon) to check which roles have access.
16. Try impersonating a user (e.g., Bob P) to verify that access behaves as expected.



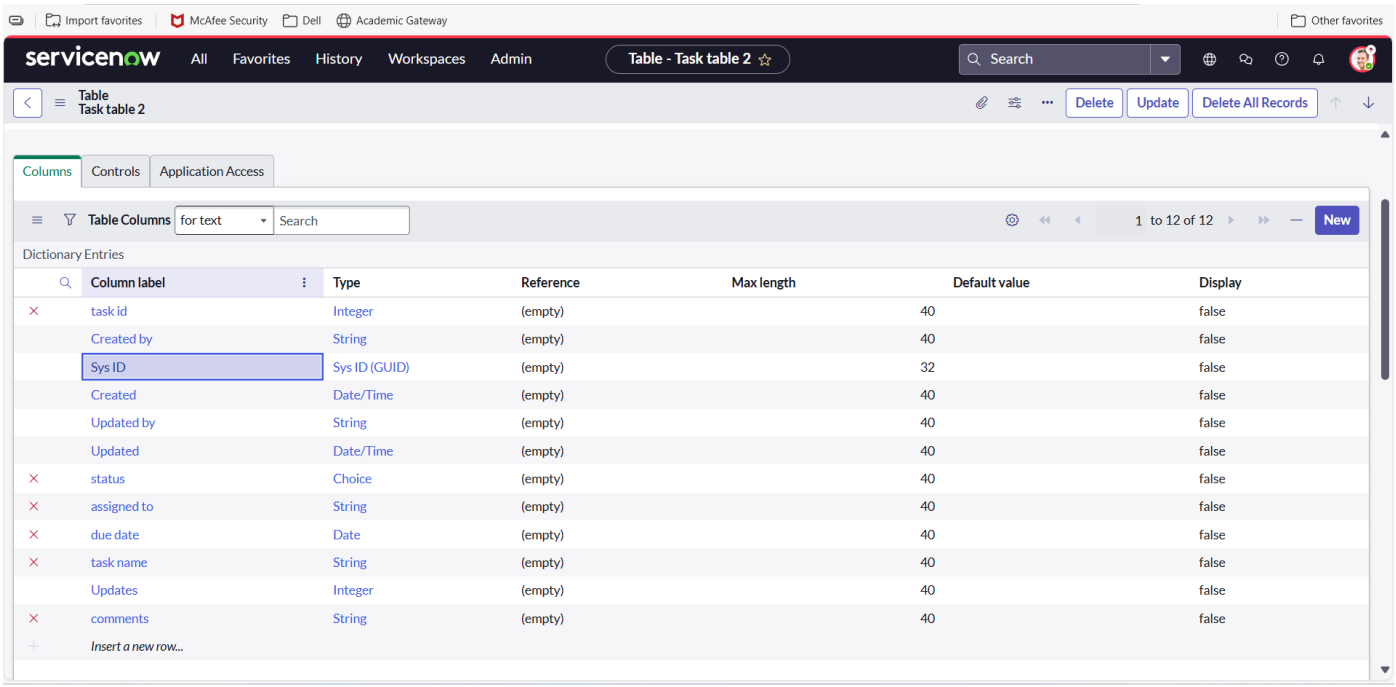
Milestone 7:Access Control List

Activity 1: Create Flow

1. Log in to your ServiceNow instance.
2. In the Application Navigator, click on All and search for Flow Designer.
3. Under Process Automation, select Flow Designer.

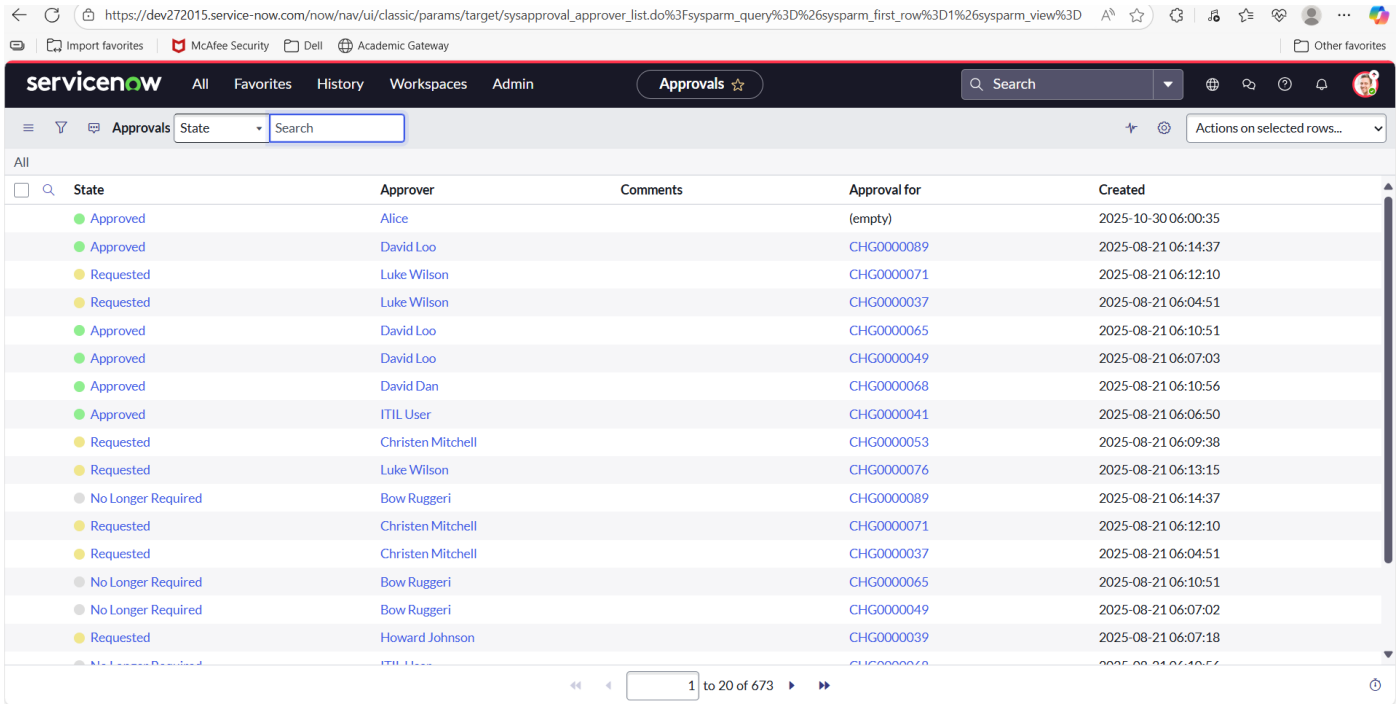
4 .Once the Flow Designer interface opens, click on New and choose Flow.

4. In the Flow Properties window:
    - Flow Name: Enter “Task Table Flow”.
    - Application: Select Global.
    - Description (optional): Automates record creation and updates for task management.
5. Click Submit or Build Flow to start designing your flow.



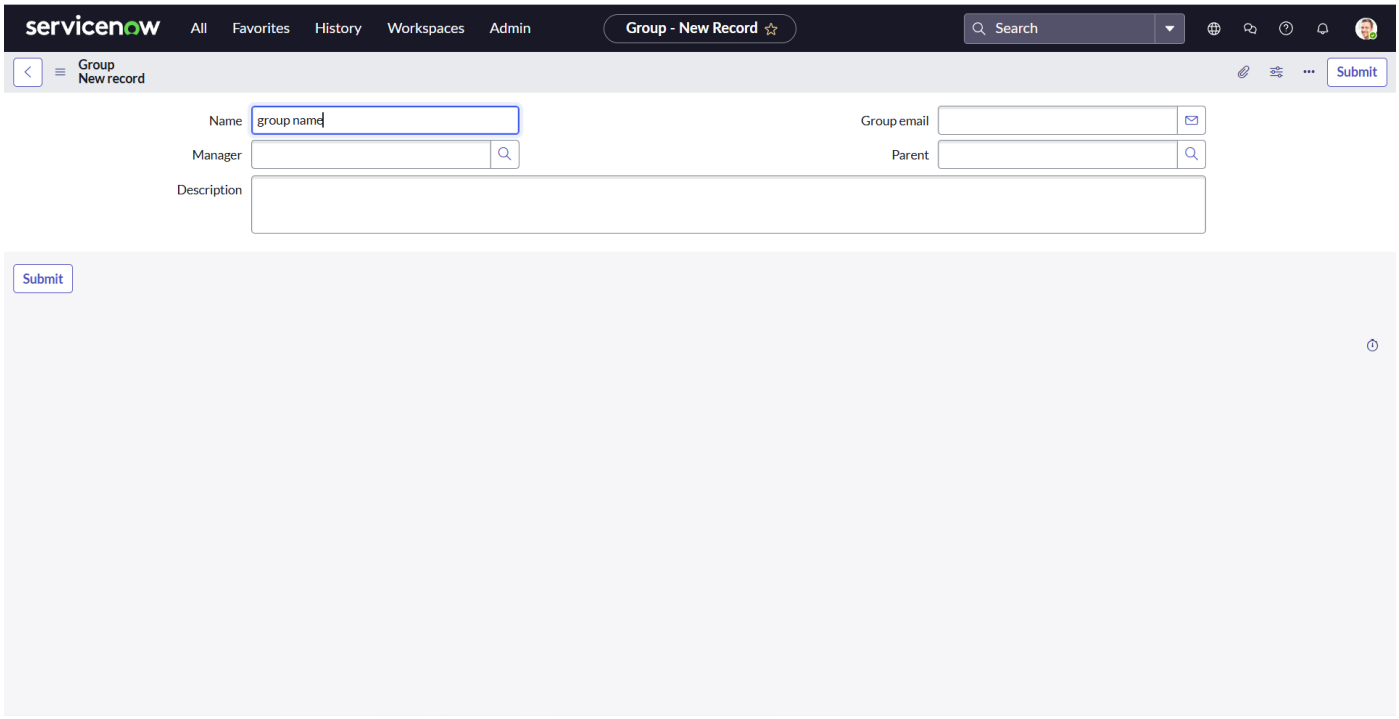
Activity 2: Adding a Trigger to the Flow

6. In the Flow Designer, click on Add a Trigger.
7. In the Trigger Selection window, search for Create Record and select it.
8. In the Table field, enter Task Table (for example: u_task_table).
9. Under Conditions, define the following criteria to determine when the flow will run:
    - Field: Status Operator: is Value: In Progress
    - Field: Comments Operator: is Value: Feedback
    - Field: Assigned To Operator: is Value: Bob
10. Once all conditions are added, click Done to save the trigger configuration.



Activity 3: Adding an Action to Update Records

11. In the Flow Designer, click on Add an Action.
12. From the action options, select Action, then search for Update Record and choose it.
13. In the Record field, drag the appropriate data pill from the Data Panel on the right-hand side to link the record from the trigger.
14. The Table name will be automatically populated based on the record data.
15. Under the Fields section, add the field to be updated:
    - Field: Status
    - Value: Completed
16. Once the field and value are set, click Done to save the action configuration.

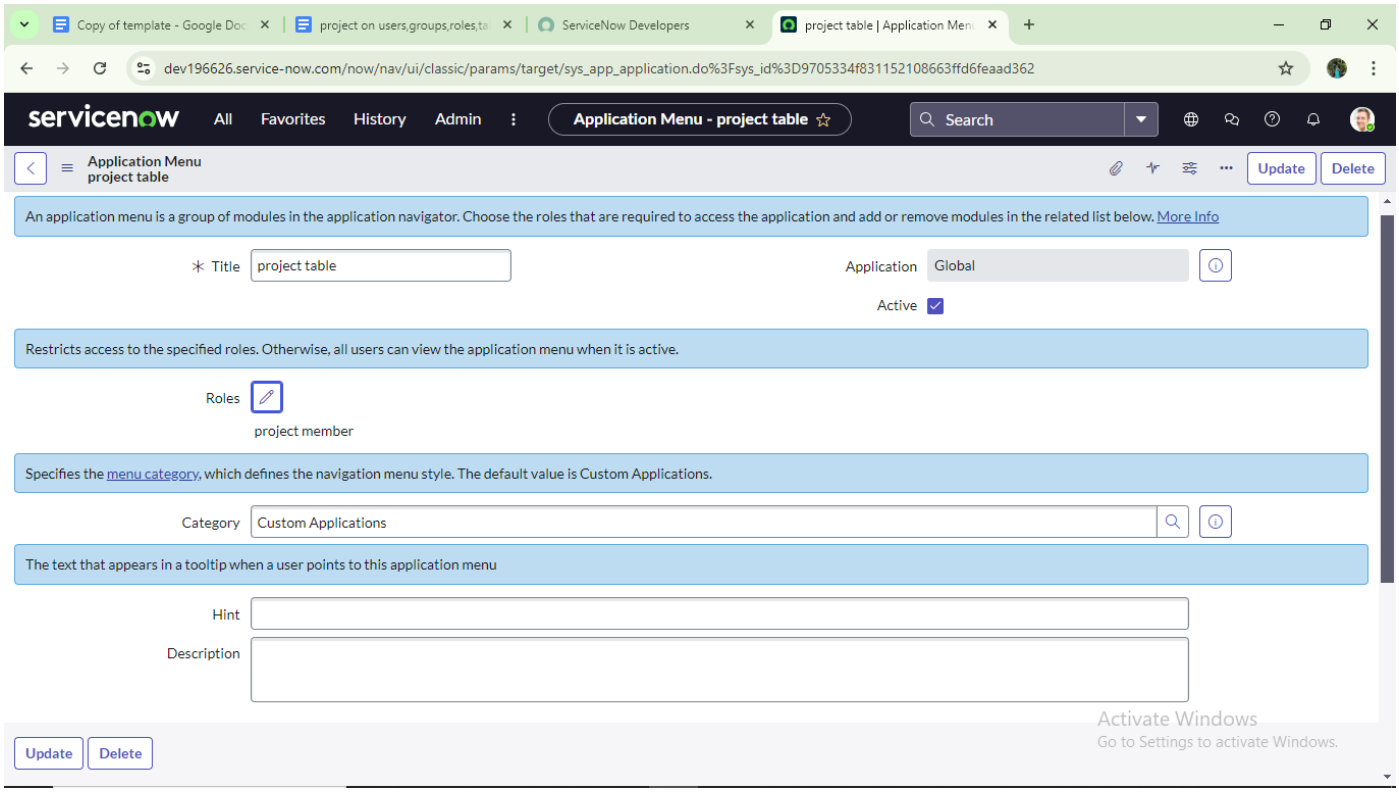


Activity 4: Adding an Approval Action in the Flow

17. In the Flow Designer, navigate to the Actions section.
18. Click on Add an Action.
19. From the list of available actions, select Action, then search for Ask for Approval and choose it.
20. In the Record field, drag and drop the corresponding record from the Data Panel on the right side.
21. The Table field will be automatically populated once the record is linked.
22. Under the Approval Configuration section:
23. Approve Field: Status
24. Approver: Alice P
25. Review the configuration, then click Done to save the approval step.
26. Click on Save

Activity 5: Testing the Flow and Approval Process

1. In the Application Navigator, search for Task Table and open it.
2. Verify that the Status field of the created task record has been automatically updated to Completed, as defined in the flow action.
3. Next, go back to the Application Navigator and search for My Approvals.
4. Under the Service Desk module, click on My Approvals to view pending approval requests.
5. Log in or impersonate user “Alice P”, who was assigned as the approver in the flow.
6. Locate the approval request generated for the task record.
7. Right-click on the request and select Approve to complete the approval process.



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.