ANJALAI AMMAL MAHALINGAM ENGINEERING COLLEGE

DEPARTMENT OF INFORMATION TECHNOLOGY

NM-SERVICE NOW ADMINISTRATOR

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

Team Members:

NAME	REGISTER NUMBER
S.Saranya	820422205070
J.Shibika	820422205074
L.Sweatha	820422205085
R.Vigneshwari	802422205091

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

Abstract:

The project titled **"Optimizing User, Group, and Role Management with Access Control and Workflows"** focuses on streamlining user administration processes within ServiceNow. The main goal of this project is to enhance system security, improve workflow automation, and ensure efficient role-based access control. Manual management of users and roles often leads to inefficiencies, duplication, and human error. Through the implementation of ServiceNow's platform capabilities, such as role-based access, workflow automation, and custom UI design, this project aims to provide a centralized and automated solution for user and role management. The outcome is an optimized process that enhances visibility, accountability, and performance across IT and business operations.

1.Introduction:

In modern organizations, effective management of **users, groups, and roles** is essential to maintain data security, compliance, and operational efficiency. With the increasing complexity of IT systems, manual handling of user access and permissions becomes error-prone and time-consuming.

ServiceNow was chosen for this project due to its powerful automation tools, scalability, and integrated IT Service Management (ITSM) capabilities. ServiceNow enables organizations to design, automate, and manage workflows with high efficiency, ensuring that the right users have the right access at the right time.The objective of this project is to **implement a structured and automated access control system** using ServiceNow's features like **Access Control Lists (ACLs), Role Assignments, Workflows, and Catalog Management**. The project also focuses on improving the user experience through well-designed forms and interfaces that support efficient role-based operations.

2.Problem Statement:

In many organizations, managing users, groups, and roles is still handled through **manual processes**, which are time-consuming, error-prone, and difficult to scale as the organization grows. These traditional methods often lead to **inconsistent access permissions**, **delayed approvals**, and **security vulnerabilities** due to lack of centralized control. Additionally, administrators face challenges in tracking user activities, monitoring access changes, and ensuring compliance with organizational policies.

The absence of **system visibility** and **automated workflows** further complicates access management. Without a unified platform, it becomes difficult to identify who has access to what resources, leading to potential risks of **unauthorized access** or **data breaches**. Moreover, when user onboarding, role changes, or deactivation processes are done manually, it increases administrative workload and slows down overall business operations.

This project aims to solve these challenges by implementing an optimized **User, Group, and Role Management system** using **ServiceNow**. By introducing **automated**

workflows and **Role-Based Access Control (RBAC)**, the solution eliminates manual inefficiencies, enhances visibility into user access, ensures consistent permission management.

3.Methodology/System Design:

The project **"Optimizing User, Group, and Role Management with Access Control and Workflows"** follows a systematic approach to design, develop, and implement a secure and automated user management system using **ServiceNow**. The methodology includes several key phases to ensure efficiency, scalability, and reliability in managing users, roles, and workflows.

3.1. Requirement Analysis:

In this phase, the existing user management processes were studied to identify inefficiencies such as manual role assignments, lack of approval workflows, and limited access visibility. Stakeholder interviews and data analysis were conducted to gather functional and security requirements.

3.2. System Design:

The system is designed based on **Role-Based Access Control (RBAC)** principles. Each user is assigned to specific groups and roles according to their job responsibilities. The design includes:

- **User Management Module:** Handles user creation, modification, and deactivation.
- **Group Management Module:** Organizes users into functional groups for easy permission control.
- **Role Management Module:** Defines access levels and permissions for each role.
- **Workflow Automation:** Automates approval processes for new user requests, role changes, and access revocations.
- **Access Control Policies:** Ensures secure data access based on predefined rules.

3.3. Implementation Using ServiceNow:

ServiceNow's built-in modules and tools such as **Flow Designer**, **Access Control Lists (ACLs)**, and **User Administration** were used to build the system. The workflows were configured using Flow Designer to automate user onboarding, role approval, and access revocation processes.

3.4. Testing and Validation:

Comprehensive testing was performed to verify functionality, security, and accuracy. Unit testing, integration testing, and user acceptance testing (UAT) were conducted to ensure the workflows and access controls worked as expected.

3.5. Deployment and Monitoring:

After successful validation, the system was deployed in the live environment. Continuous monitoring and auditing mechanisms were implemented to track user activities, detect anomalies, and ensure compliance with organizational policies.

3.6. Documentation and Training:

User manuals and admin guides were created to assist in managing the system. Training sessions were conducted to familiarize administrators and end-users with the new automated workflows.

4.Design Approach:

The design approach for the project **"Optimizing User, Group, and Role Management with Access Control and Workflows"** is centered on creating a **secure, scalable, and automated system** for managing user access and organizational workflows using the **ServiceNow platform**. The goal is to simplify administrative operations, enhance visibility, and ensure data security through structured role-based access control (RBAC) and workflow automation.

4.1. Design Philosophy:

The system design follows the principles of **modularity, automation, security, and usability**:

- **Modularity:** Each component (User, Group, Role, and Workflow) is designed as an independent yet interconnected module, allowing easy customization and scalability.
- **Automation:** Manual processes are replaced with automated workflows to improve efficiency and reduce human error.
- **Security:** Role-Based Access Control (RBAC) ensures users can only access resources relevant to their roles.
- **Usability:** A user-friendly interface is provided for administrators and end-users to easily request, approve, and manage access without technical complexity.

4.2. Key ServiceNow Features and Modules Used:

a) ServiceNow Studio:

Used to develop and customize applications for user, group, and role management. It enables the creation of tables, forms, scripts, and UI components specific to the project requirements.

b) Service Catalog:

Provides a self-service interface where users can request access, role changes, or group assignments. Catalog items trigger automated approval workflows, improving efficiency and transparency.

c) Flow Designer:

Used to build and automate workflows such as user onboarding, access requests, and role approvals. It eliminates manual intervention by automatically routing tasks to the appropriate approvers.

d) Access Control Lists (ACLs):
Implements security rules to restrict data visibility and operations (read, write, delete) based on user roles and permissions. ACLs form the backbone of the RBAC model in ServiceNow.
e) User and Group Management Module:
Handles user account creation, modification, and deactivation. Groups are used to organize users by department or function for easier permission handling.
f) Role Management Module:
Defines and assigns roles to users and groups, ensuring each role has specific access privileges aligned with organizational policies.
g) Incident Management (optional integration):
Can be integrated to track access-related issues or unauthorized access attempts, allowing administrators to respond quickly to potential security incidents.

4.3. Expected Outcome:

By using these ServiceNow features, the design ensures:

- Streamlined user and role management.
- Automated and auditable workflows.
- Enhanced security through precise access control.
- Reduced administrative effort and increased operational transparency.

5.System Architecture:

The system architecture for the project **"Optimizing User, Group, and Role Management with Access Control and Workflows"** is designed to provide a **centralized, secure, and automated environment** for managing user identities, access permissions, and workflow processes. It integrates various ServiceNow modules and custom applications to form a unified solution that simplifies administration while maintaining strong security and compliance.

5.1. Architectural Overview:

The architecture follows a **three-tier structure** — **Presentation Layer**, **Application Layer**, and **Data Layer** — ensuring modularity, scalability, and efficient data flow.
a) Presentation Layer (User Interface):
This layer provides the interface through which users, administrators, and managers interact with the system.

- **Components:**
  - **Service Portal / Service Catalog:** For users to submit access requests, role changes, or group membership updates.
  - **Admin Dashboard:** For administrators to monitor, approve, and manage users, roles, and workflows.

- **Notifications & Approvals:** Real-time alerts and approval tasks are sent to the respective managers or role owners.

b) Application Layer (Business Logic):

This is the core layer where the system's logic and automation processes are implemented.

- **Key Components:**
  - **Flow Designer:** Automates workflows for user onboarding, access approval, and deactivation.
  - **Access Control Lists (ACLs):** Define rules that control who can view, edit, or manage records based on their assigned roles.
  - **Business Rules & Scripts:** Enforce policies and automate backend operations such as automatic role assignments or data synchronization.
  - **ServiceNow Studio:** Used to build and customize the application's functionality and UI.

c) Data Layer (Database & Storage):

This layer stores all user, group, role, and workflow data securely in ServiceNow's relational database.

- **Tables Used:**
  - **sys_user:** Stores user information and profile details.
  - **sys_user_group:** Maintains group membership and department-level associations.
  - **sys_user_role:** Defines role-based permissions and access controls.
  - **Custom Tables:** Created for workflow history, audit logs, and access request tracking.

5.2. Integration Components:

The system can integrate with external tools or organizational systems to ensure smooth synchronization and reporting.

- **LDAP / Active Directory Integration:** Automatically imports and updates user information from corporate directories.
- **Email Notification System:** Sends automated emails for approvals, role change confirmations, or access expirations.
- **Incident Management Integration:** Links access issues or unauthorized access attempts to the Incident module for resolution and tracking.

5.3. Data Flow:

1. **User Request Initiation:** A user submits an access or role request through the Service Catalog.

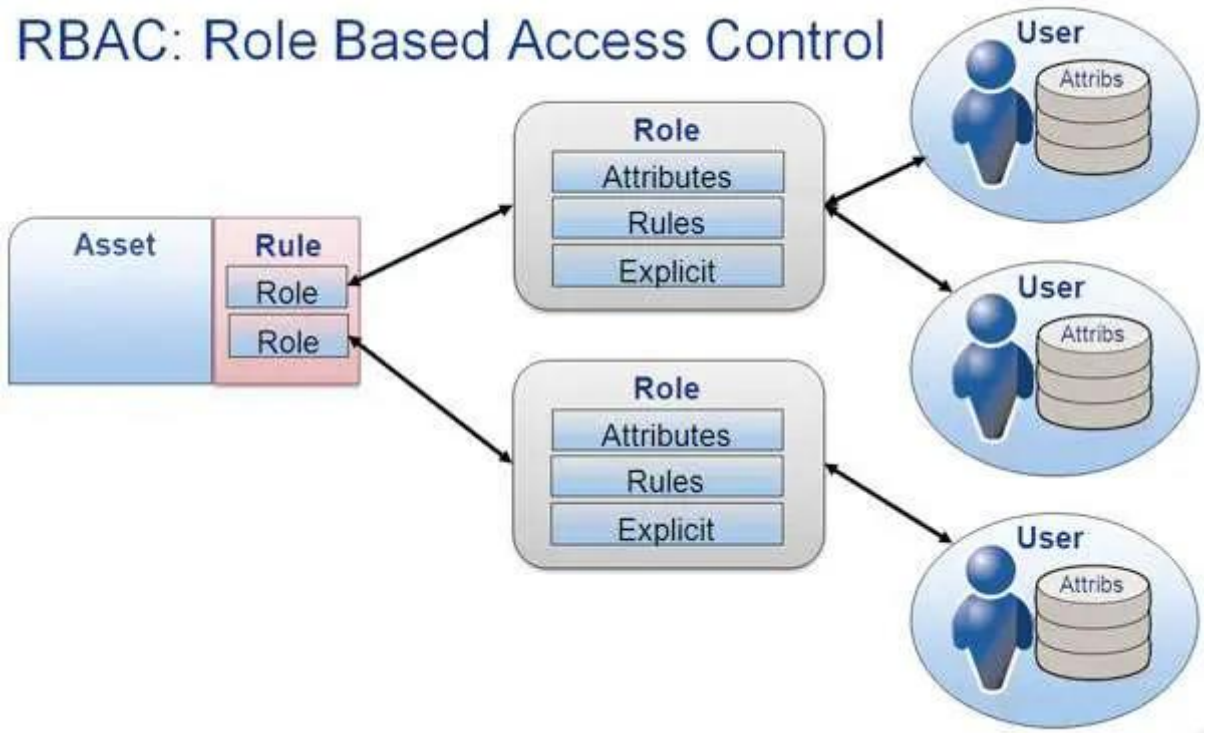
2. **Workflow Automation:** The Flow Designer routes the request to the appropriate approver (e.g., manager or admin).
3. **Approval and Role Assignment:** Upon approval, the system automatically assigns the required role or group to the user.
4. **Access Control Enforcement:** ACLs ensure that the user's access aligns with their assigned role.
5. **Audit and Reporting:** All actions are logged in the system for transparency and compliance monitoring.

5.4. Custom Applications:

A **custom "User Access Management" application** is developed using **ServiceNow Studio** to provide enhanced functionality:

- Custom forms for role requests and approvals.
- Automated deactivation of inactive users.

- Real-time dashboards showing user-role mappings and pending approvals.



6.User Interface (UI) and User Experience (UX):

The **User Interface (UI)** and **User Experience (UX)** design of the project **"Optimizing User, Group, and Role Management with Access Control and Workflows"**

focus on creating an **intuitive, user-friendly, and efficient environment** for administrators, managers, and end-users. The design ensures that all tasks — such as requesting access, approving workflows, or managing user roles — can be performed easily with minimal training or errors.

6.1. UI Design Overview:

The UI is developed using **ServiceNow Studio** and **Service Portal**, which allows for a clean and structured layout aligned with ServiceNow's modern design standards. The interface is divided into role-based dashboards and forms that enhance usability and clarity.

Key Design Features:

- **Consistent Layout:** Every module (User, Group, Role) follows a consistent layout for easy navigation.
- **Color Coding:** Different colors are used to distinguish between request states (e.g., *Pending – Yellow*, *Approved – Green*, *Rejected – Red*).
- **Responsive Design:** The UI adapts to different screen sizes, ensuring accessibility on desktops, tablets, and mobile devices.

- **Minimal Click Navigation:** Important functions like "Request Access," "View Roles," and "Approve Requests" are accessible from the home dashboard.

6.2. User Forms and Layouts:

a) User Request Form:

- **Purpose:** To allow users to request new access, role assignment, or group membership.
- **Fields Included:**
  - User Name (auto-filled)
  - Department
  - Requested Role or Group
  - Purpose of Request
  - Manager Approval Section
- **Features:**
  - Auto-validation for existing roles.
  - Dynamic dropdowns that show only available roles.
  - Submit and track request status directly from the form.

b) Role Management Form:

- **Purpose:** For administrators to define and manage user roles.
- **Fields Included:**
  - Role Name

    - Description
    - Permissions (Read, Write, Delete)
    - Associated Groups
- **Features:**
    - Editable role permissions.
    - Linked list view of all users assigned to each role.

c) Group Management Form:

- **Purpose:** To organize users into functional or departmental groups.
- **Fields Included:**
    - Group Name
    - Group Type (e.g., IT, HR, Finance)
    - Group Members
    - Group Approver
- **Features:**
    - Bulk add/remove users.
    - View group activity history.

d) Workflow Approval Form:

- **Purpose:** For managers and admins to review and approve user access requests.
- **Features:**
    - Approval buttons (Approve / Reject / Request Info).
    - Comments section for decision justification.
    - Automatic notification on approval or rejection.

6.3. Dashboards and Navigation:

- **Admin Dashboard:** Displays system statistics such as total users, pending approvals, and access change requests. Includes shortcuts to manage roles, groups, and workflow logs.
- **Manager Dashboard:** Shows pending access requests from team members and allows one-click approvals or comments.
- **User Dashboard:** Displays current roles, group memberships, and request statuses for transparency.

6.4. User Flows:

a) User Access Request Flow:

1. User logs into the Service Portal.
2. Navigates to “Access Management” → “Request Access.”
3. Fills out and submits the request form.

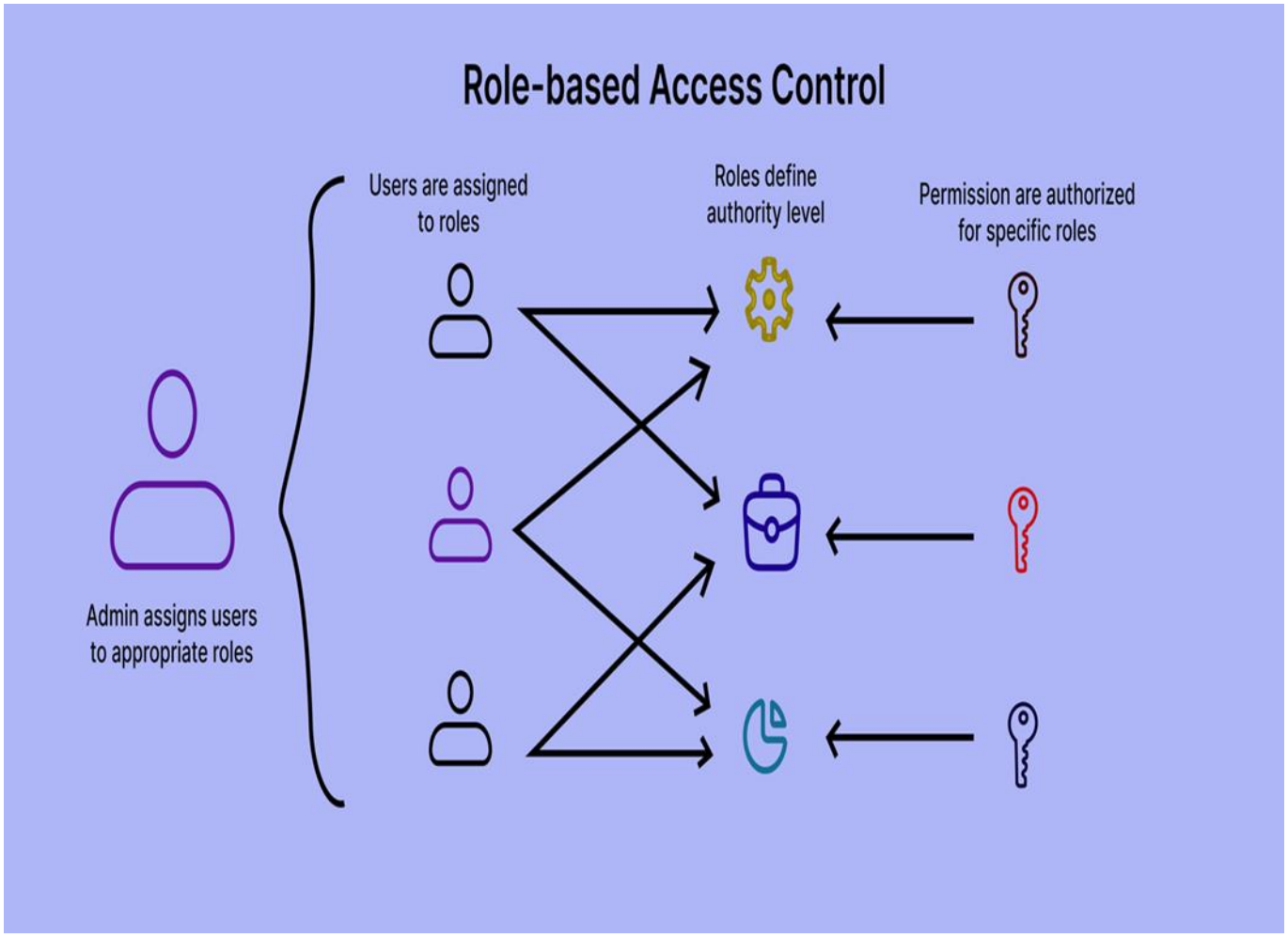
4. Manager receives a notification for approval.
5. Once approved, the system auto-assigns the role.
6. User receives confirmation and can view changes in their dashboard.

b) Role Management Flow (Admin):

1. Admin opens “Role Management” module.
2. Creates or edits a role and defines access permissions.
3. Assigns the role to specific users or groups.
4. System updates ACLs automatically to enforce permissions.

6.5. UX Design Principles Applied:

- **Simplicity:** Only essential information is shown to reduce clutter.
- **Accessibility:** Forms and dashboards follow ServiceNow’s accessibility standards for all users.
- **Feedback Mechanism:** Success or error messages guide users at every step.
- **Transparency:** Users can track the progress of their requests at any time.



7.Implementation Details:

The implementation of the project **"Optimizing User, Group, and Role Management with Access Control and Workflows"** was carried out using the **ServiceNow platform**. The process involved three major phases — **Platform Setup**, **Development and Customization**, and **Workflow Implementation** — each contributing to building a secure, efficient, and automated system for managing users, groups, and roles.

7.1. Platform Setup:

a) Instance Configuration:

- A **ServiceNow developer instance** was obtained and configured for the project.
- The **administrative roles** (admin, developer) were assigned to enable customization and module creation.
- System properties such as **time zone**, **language**, and **notification settings** were configured to match the organizational requirements.
- Modules like **User Administration**, **Flow Designer**, and **Service Catalog** were enabled for use in the project.

b) User and Group Creation:

- Created base users such as **Administrator, Manager, Employee**, and **Guest** with unique roles.
- Defined **user groups** (e.g., IT Support, HR, Finance, and Operations) to organize users by function.
- Each user was linked to a **specific group and role** to simplify permission management.
- Default access controls were tested to ensure proper data isolation between group

7.2. Development and Customization:

Development was carried out using **ServiceNow Studio**, which allowed for the creation of custom applications, tables, and UI enhancements tailored to the project's needs.

a) Custom Tables:

- **User_Access_Request:** Stores user access or role change requests with fields such as Request ID, Requested By, Role Name, Status, and Approval Date.
- **Role_Approval_Log:** Tracks the approval workflow history for audit and compliance purposes.
- **Deactivation_Records:** Maintains data on users whose access has been revoked or deactivated.

b) Custom Fields:

- Added new fields like *Access Type*, *Justification*, *Department*, and *Manager Comments* in the access request forms.
- Created reference fields linking users to their corresponding roles and groups for easier data mapping.

c) Client Scripts and Business Rules:

- **Client Scripts:** Used to automatically populate user information when a request form is opened, improving form efficiency.
- **Business Rules:**
  - Automatically set default status to "Pending Approval" when a request is submitted.
  - Update user roles and groups automatically upon approval.
  - Trigger notifications for request status changes (e.g., Approved, Rejected).

d) UI Policies and Actions:

- **UI Policies:**
  - Hide or disable irrelevant fields based on user role.
  - Make mandatory fields visible only during submission.
- **UI Actions:**
  - Custom buttons such as *Approve*, *Reject*, and *Escalate* were added to streamline manager decision-making.

7.3. Workflow Implementation:

Workflows were developed using **Flow Designer** to automate the approval and notification processes related to user, role, and access management.

a) Access Request Workflow:

- **Trigger:** When a user submits an access request through the Service Catalog.
- **Steps:**
  1. System captures request details and assigns a unique Request ID.
  2. The request is routed to the user's manager for approval.
  3. On manager approval, the workflow updates the user's role in the sys_user_role table.
  4. Automatic email notifications are sent to the user and administrator.
  5. Workflow status changes to *Completed*.

b) Role Change Workflow:

- Enables managers or admins to modify existing user roles.
- Includes conditional approvals where high-privilege role changes require multiple approvals (e.g., Admin or HR roles).
- Maintains full history of changes for audit tracking.

c) Deactivation Workflow:

- Automatically triggered when a user leaves the organization or is inactive for a defined period.
- Removes roles and group memberships.
- Sends alerts to IT and Security teams for final verification.

d) Integration with Incident Management (Optional):

- If access issues occur, an incident ticket is automatically created in the **Incident Management** module.
- The workflow links the incident with the affected user and notifies the IT Support team for resolution.

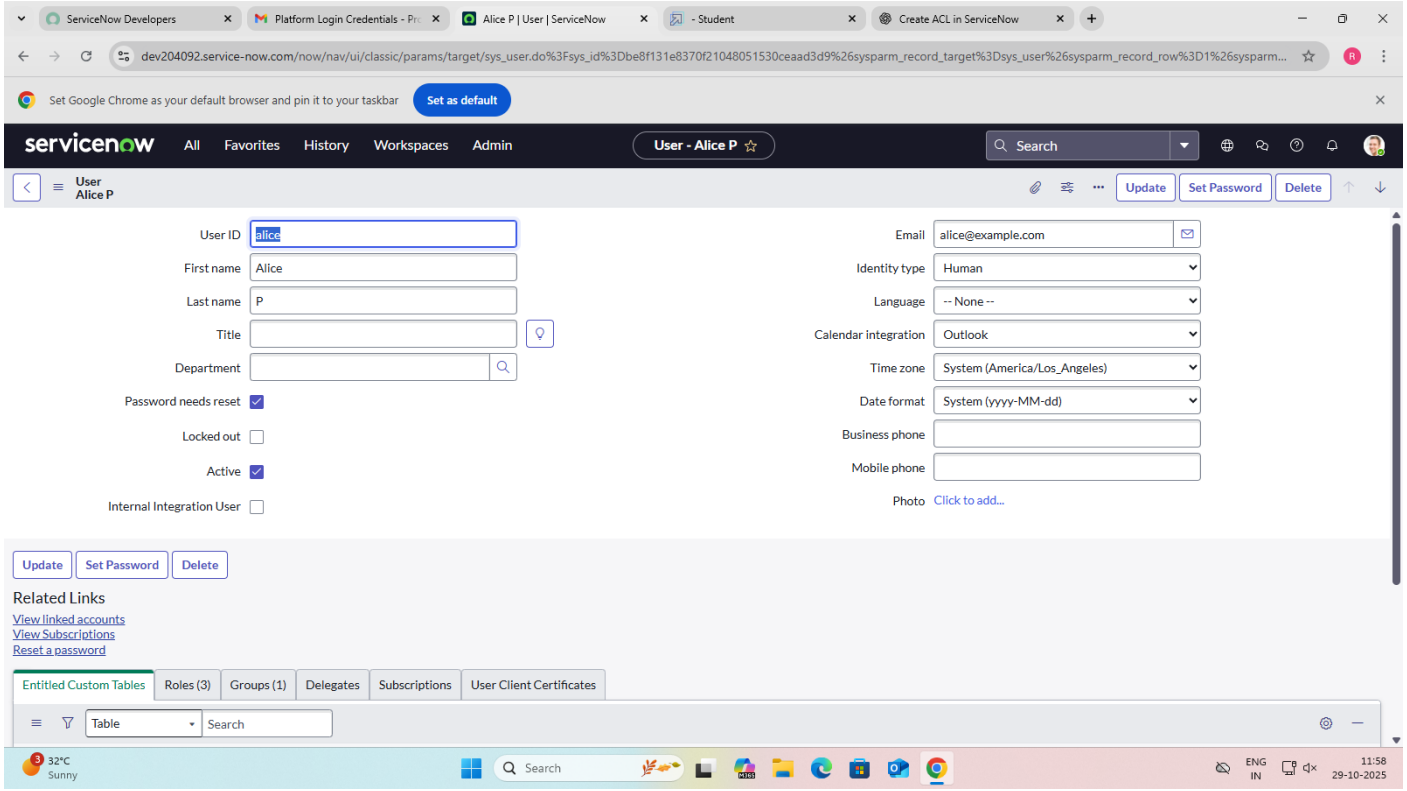
7.4. Outcome:

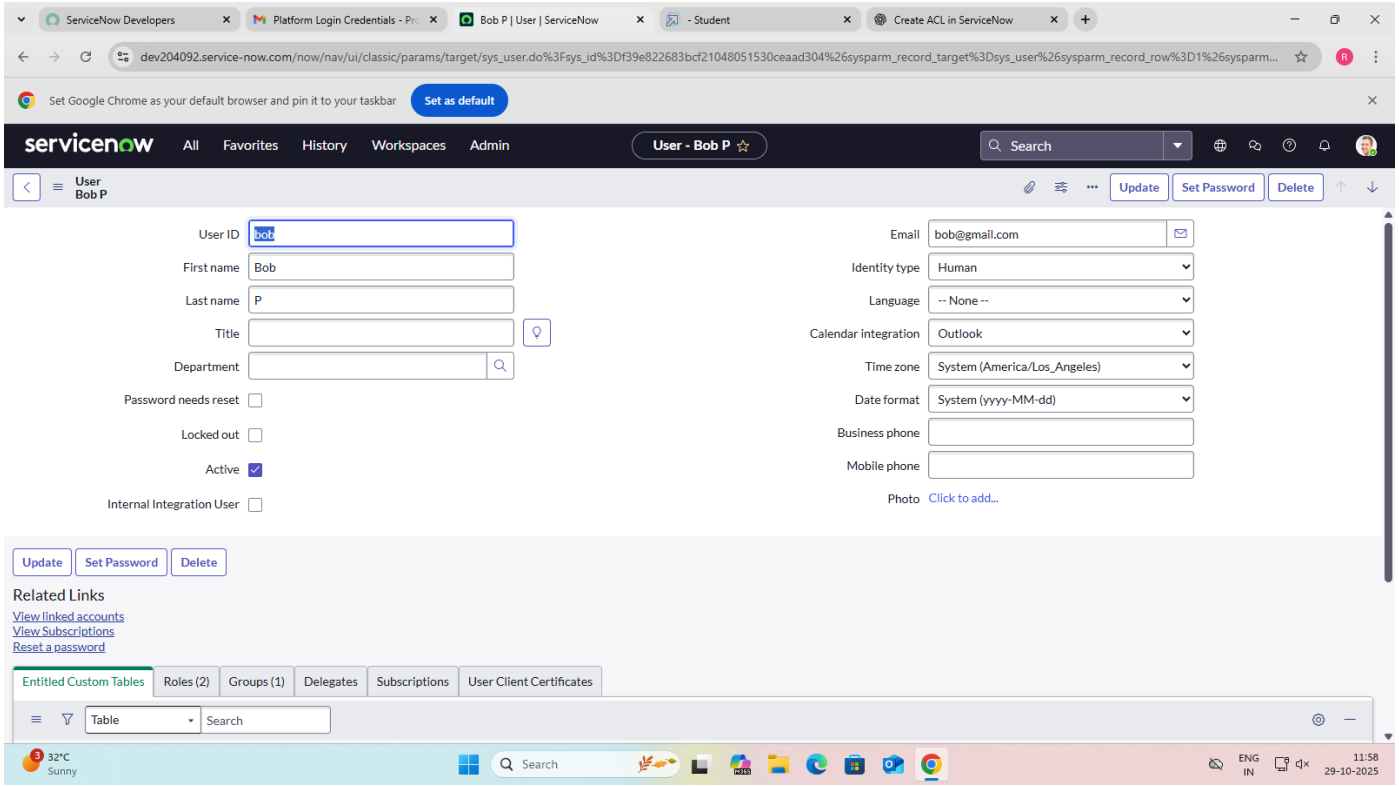
The implementation successfully automated the core aspects of **user, group, and role management** in ServiceNow.

- Reduced manual effort in approvals and role assignments.
- Improved data accuracy and traceability through audit logs.
- Enhanced security with clearly defined access controls and workflows.
- Delivered a seamless user experience with intuitive forms and automated notification.

STEP 1: Create Users

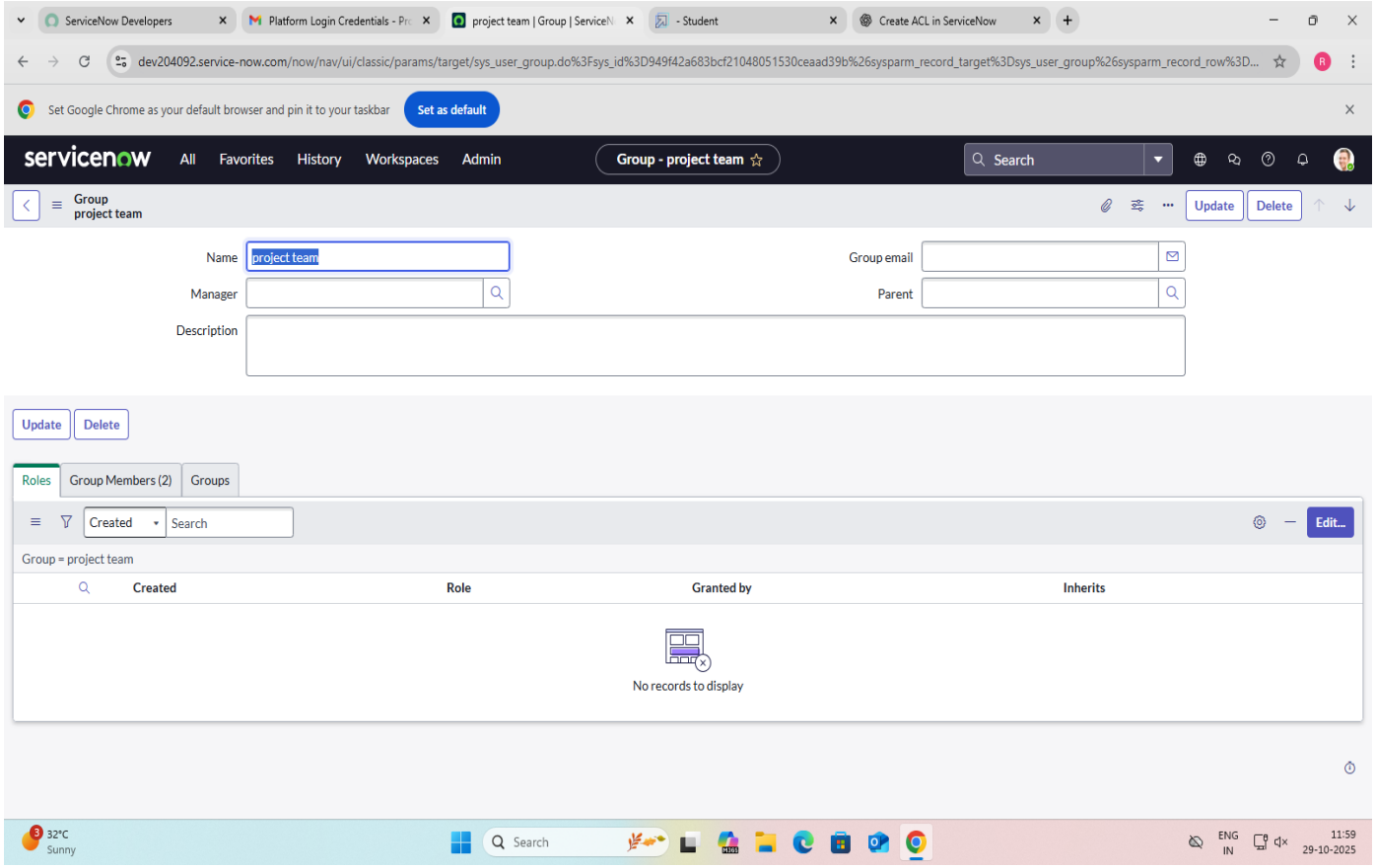
1. Open service now
2. Click on All >> search for users
3. Select Users under system security
4. Click on new
5. Fill the following details to create a new user
6. Click on submit
7. Create one more user:
8. Create another user with the following details
9. Click on submit


ServiceNow Developers
Platform Login Credentials - Pr
Alice P | User | ServiceNow
- Student
Create ACL in ServiceNow
dev204092.service-now.com/now/nav/ui/classic/params/target/sys_user.do%3Fsys_id%3Dbe8f131e8370f21048051530ceaad3d9%26sysparm_record_target%3Dsys_user%26sysparm_record_row%3D1%26sysparm...
Set Google Chrome as your default browser and pin it to your taskbar
Set as default
servicenow
All
Favorites
History
Workspaces
Admin
User - Alice P
Search
User
Alice P
Update
Set Password
Delete
User ID
alice
First name
Alice
Last name
P
Title
Department
Password needs reset
Locked out
Active
Internal Integration User
Email
alice@example.com
Identity type
Human
Language
-- None --
Calendar integration
Outlook
Time zone
System (America/Los_Angeles)
Date format
System (yyyy-MM-dd)
Business phone
Mobile phone
Photo
Click to add...
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
Table
Search
32°C
Sunny
Search
ENG
IN
11:58
29-10-2025


ServiceNow Developers
Platform Login Credentials - Pr
Bob P | User | ServiceNow
- Student
Create ACL in ServiceNow
dev204092.service-now.com/now/nav/ui/classic/params/target/sys_user.do%3Fsys_id%3Df39e822683bcf21048051530ceaad304%26sysparm_record_target%3Dsys_user%26sysparm_record_row%3D1%26sysparm...
Set Google Chrome as your default browser and pin it to your taskbar
Set as default
servicenow
All
Favorites
History
Workspaces
Admin
User - Bob P
Search
User
Bob P
Update
Set Password
Delete
User ID
bob
First name
Bob
Last name
P
Title
Department
Password needs reset
Locked out
Active
Internal Integration User
Email
bob@gmail.com
Identity type
Human
Language
-- None --
Calendar integration
Outlook
Time zone
System (America/Los_Angeles)
Date format
System (yyyy-MM-dd)
Business phone
Mobile phone
Photo
Click to add...
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
Table
Search
32°C
Sunny
Search
ENG
IN
11:58
29-10-2025

STEP 2:Create Groups

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

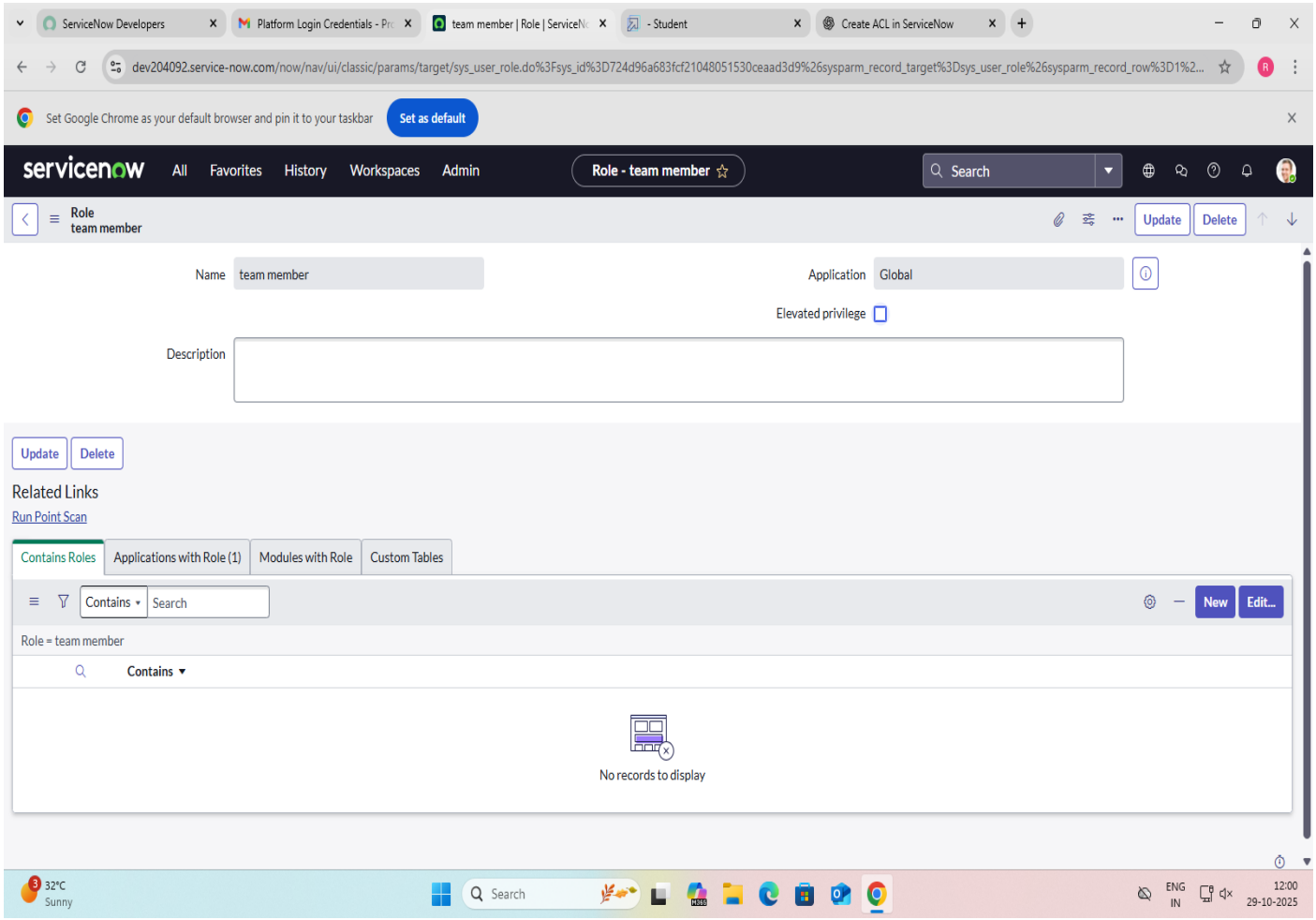


STEP 3: Create Roles

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:

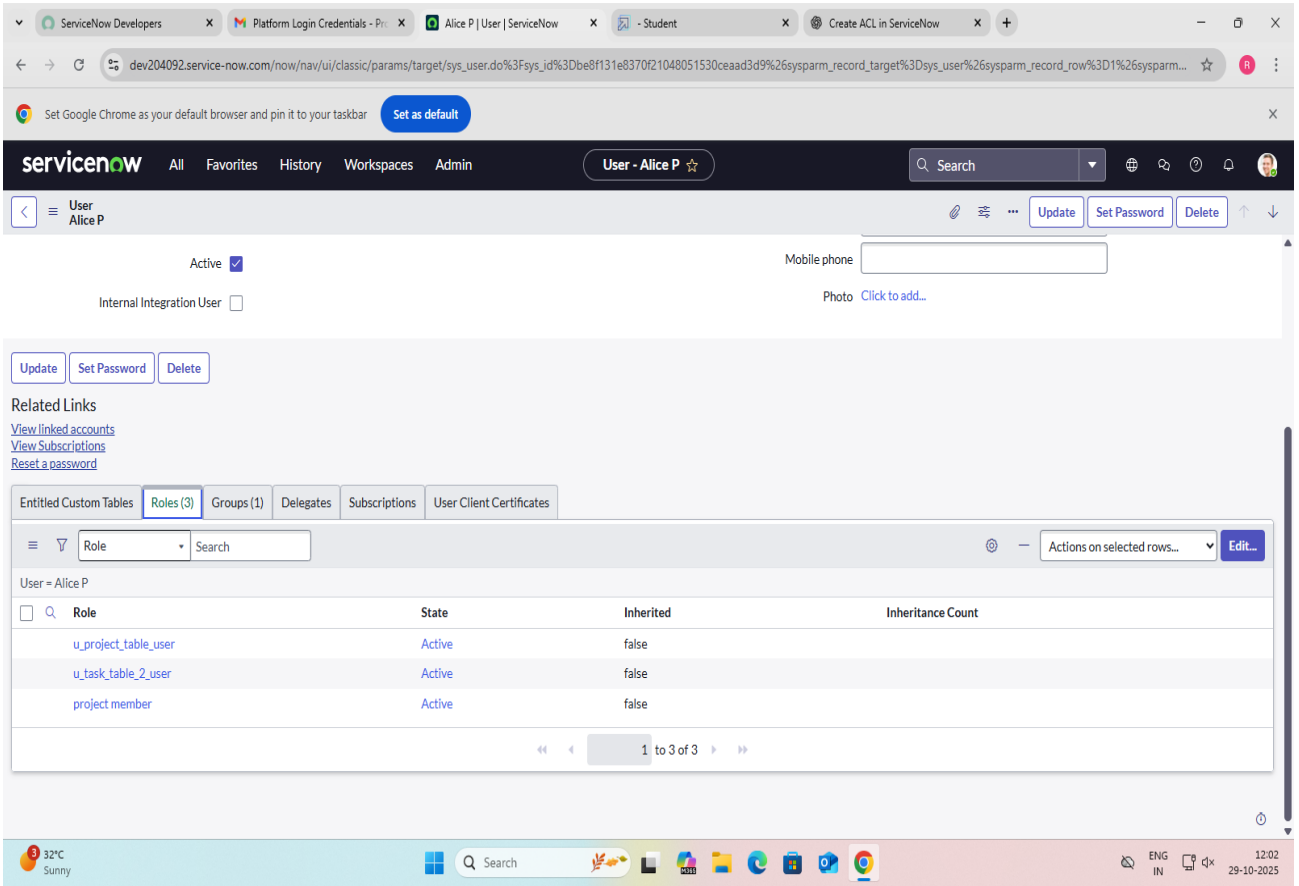
7. Create another role with the following details
8. Click on submit



STEP 4: Assign users to groups:

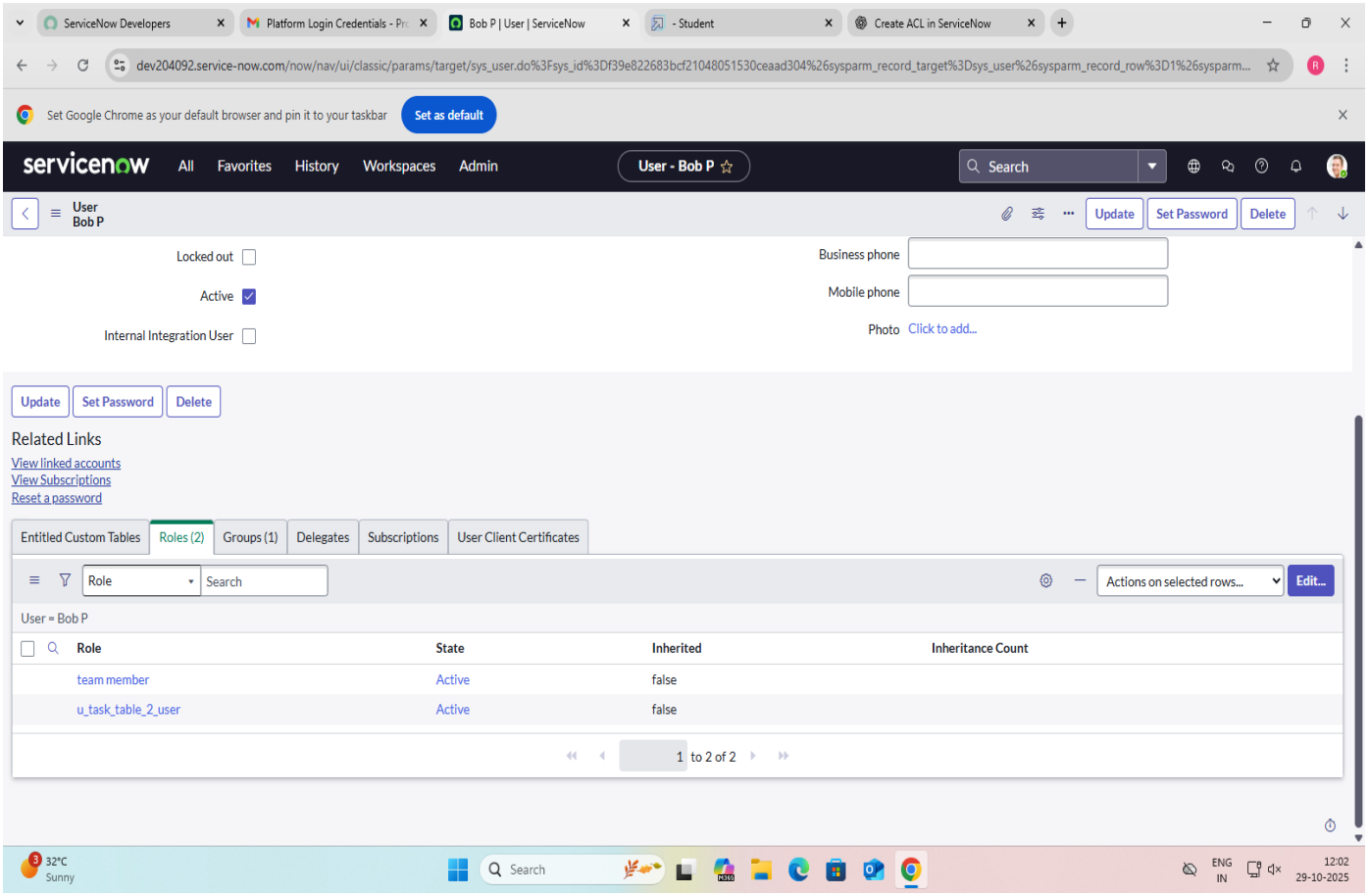
STEP 4.1: Assign roles to alice user

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.



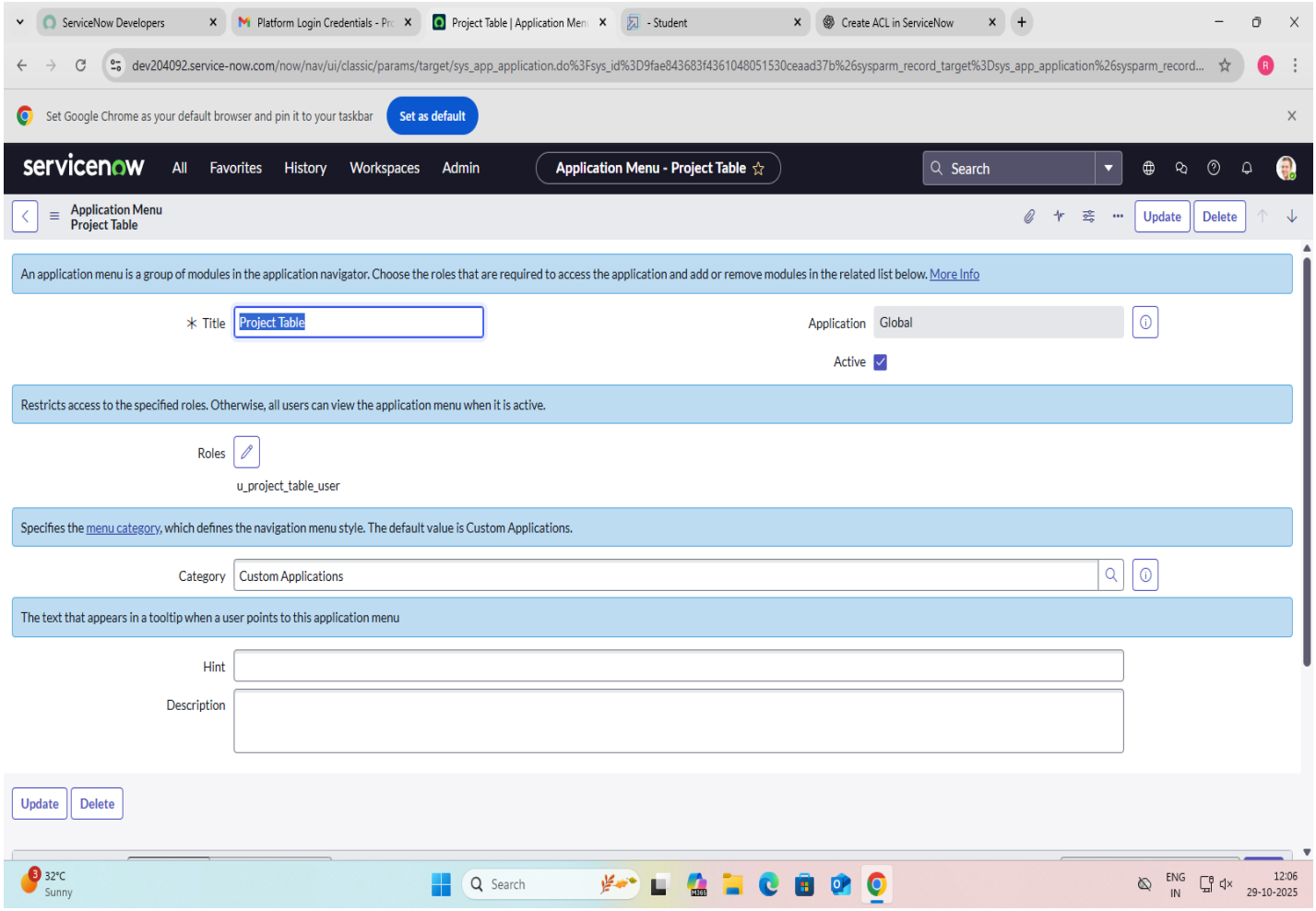
STEP 4.2: Assign roles to bob user

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.



STEP 5: Assign table access to application

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



ServiceNow Developers | Platform Login Credentials - Pr | task table 2 | Application Menu | - Student | Create ACL in ServiceNow

dev204092.service-now.com/now/nav/ui/classic/params/target/sys_app_application.do%3Fsys_id%3De9ca1e6e83bcf21048051530ceaad3e8%26sysparm_record_target%3Dsys_app_application%26sysparm_record...

Set Google Chrome as your default browser and pin it to your taskbar | Set as default

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

Application Menu
task table 2

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: task table 2

Application: Global

Active: ☑

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

Roles: project member, u_task_table_2_user

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:

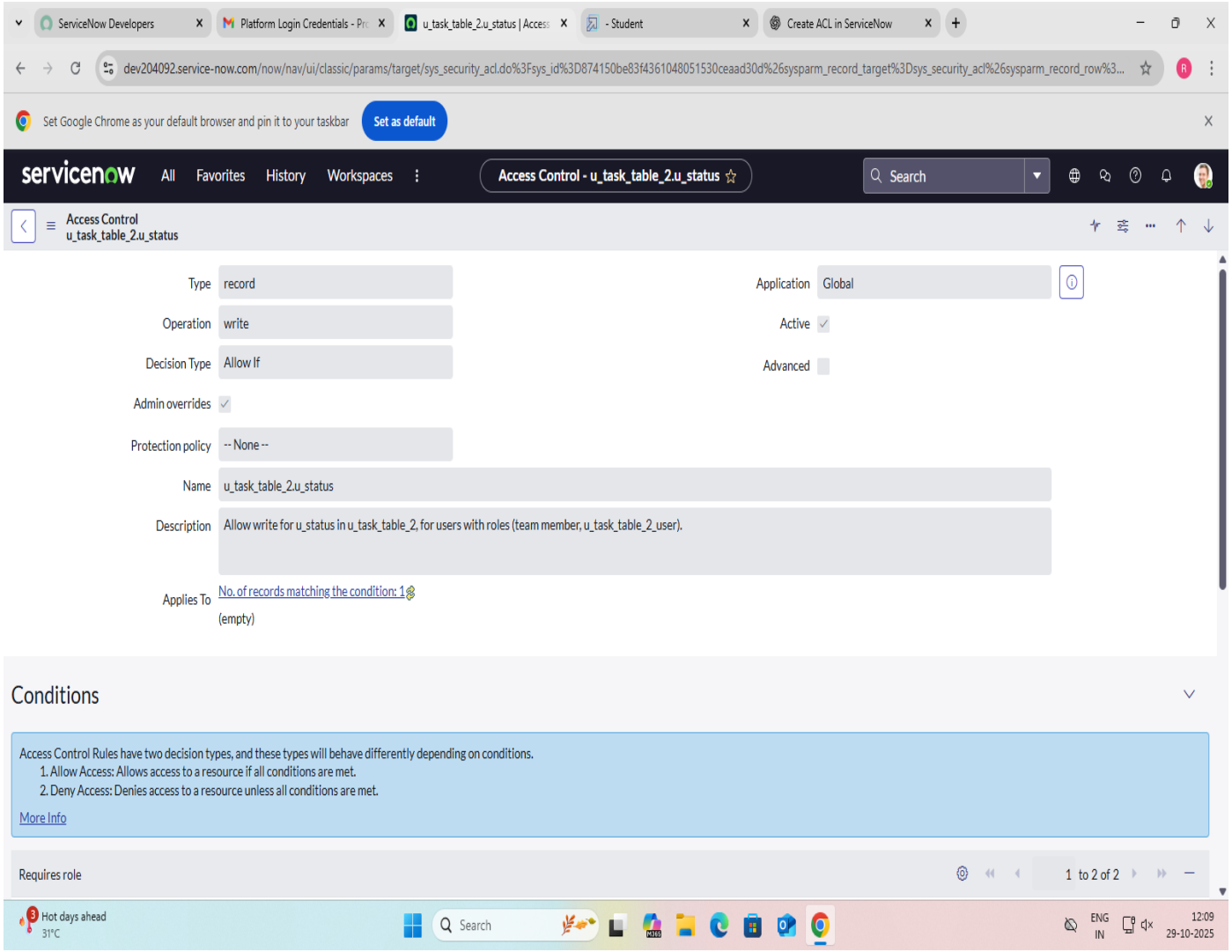
Description:

Update | Delete

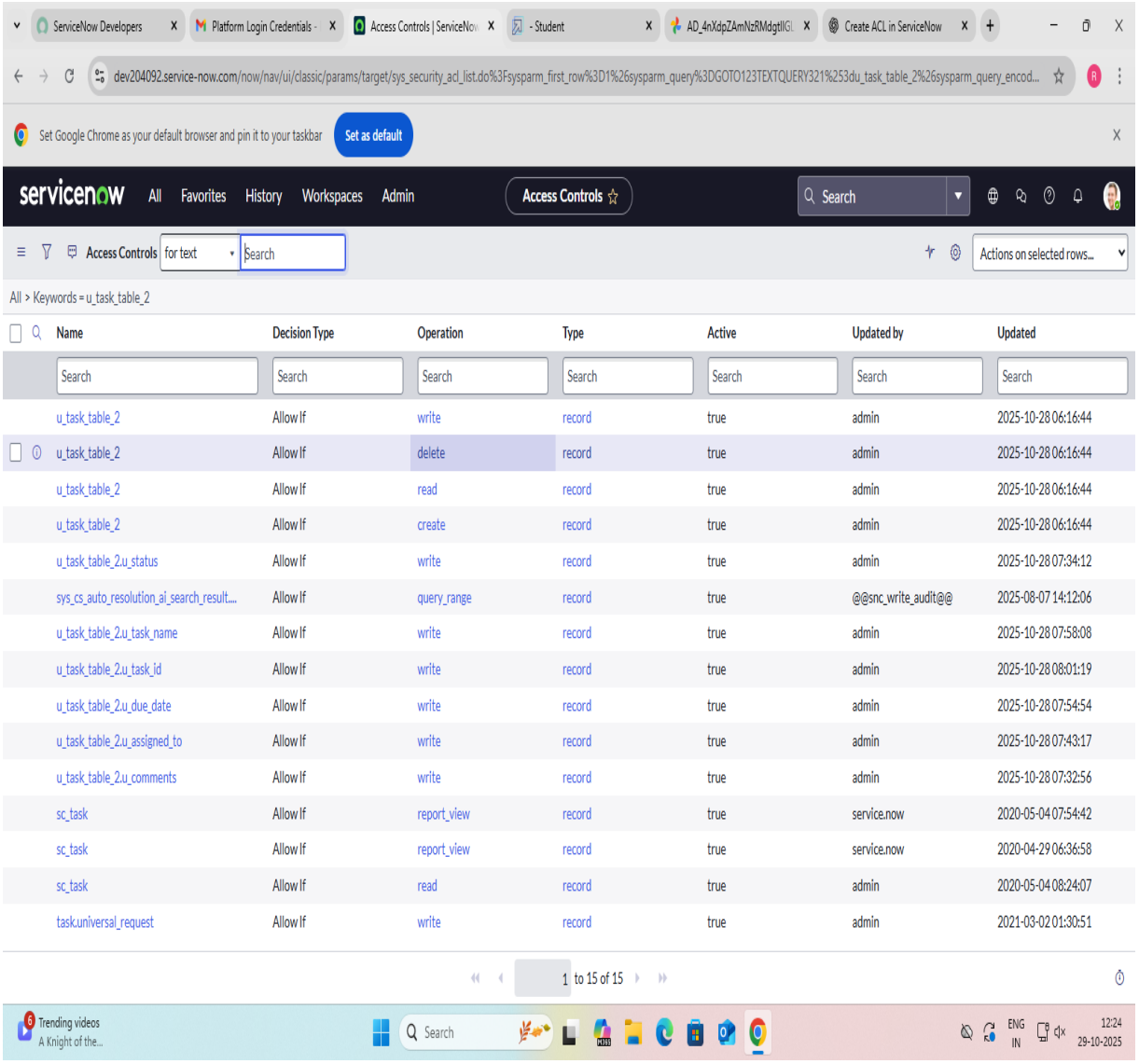
32°C Sunny | Search | ENG IN | 12:06 29-10-2025

STEP 6: Create ACL

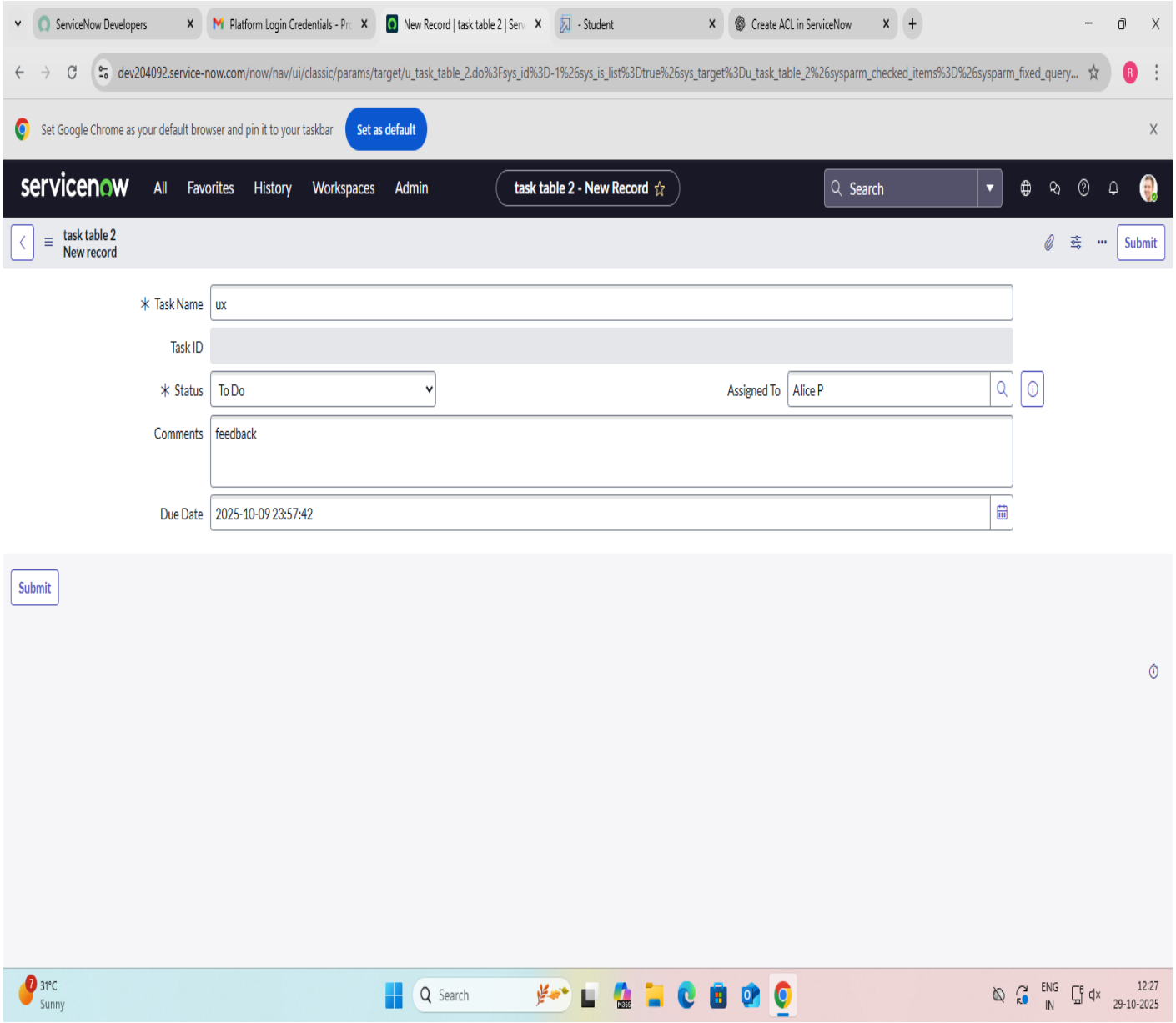
1. Open service now.
2. Click on All >> search for ACL
3. Select Access Control(ACL) under system security
4. Click on elevate role
5. Click on new
6. Fill the following details to create a new ACL



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

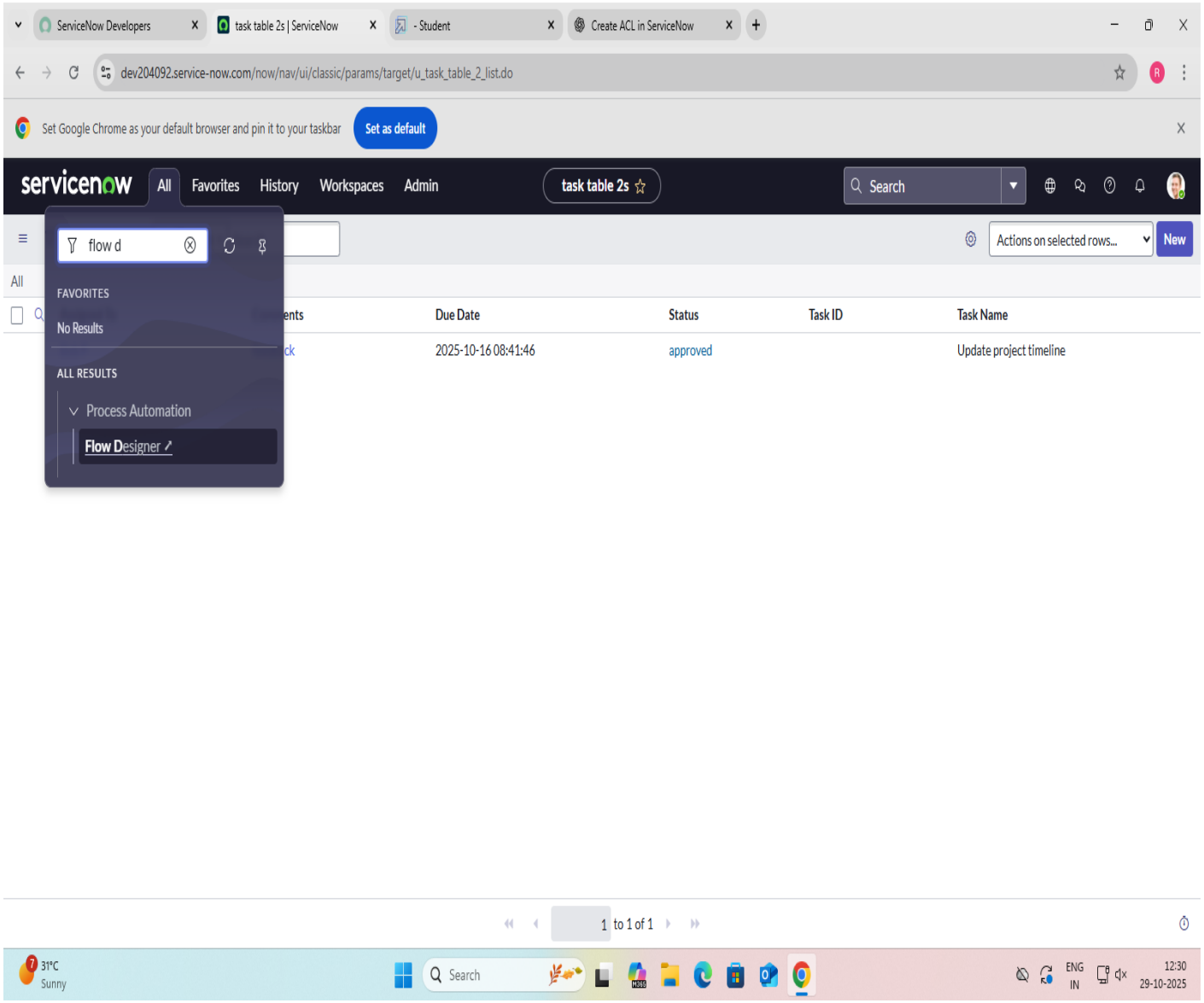


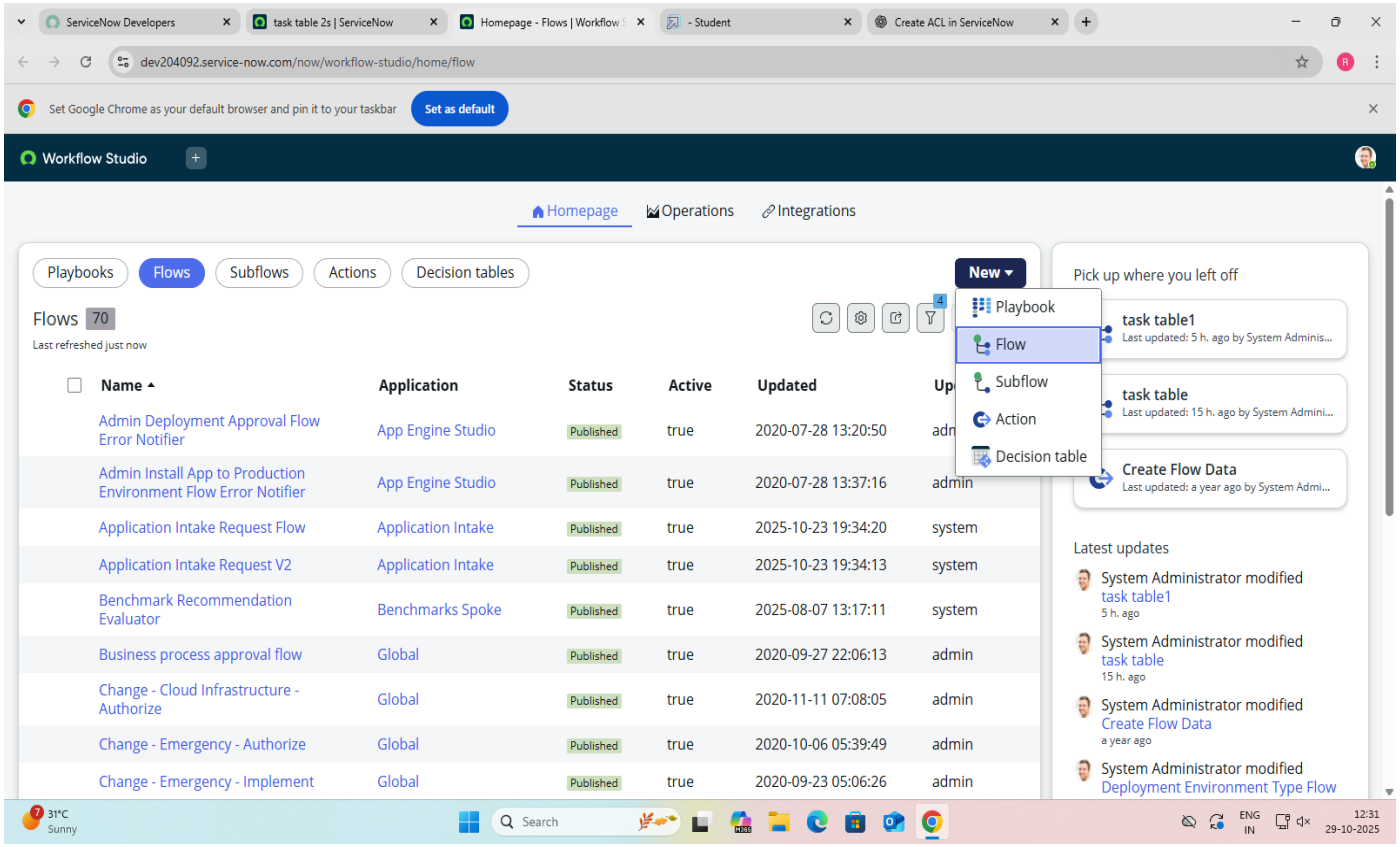
12. Click on profile on top right side
13. Click on impersonate user
14. Select bob user
15. Go to all and select task table2 in the application menu bar
16. Comment and status fields are have the edit access

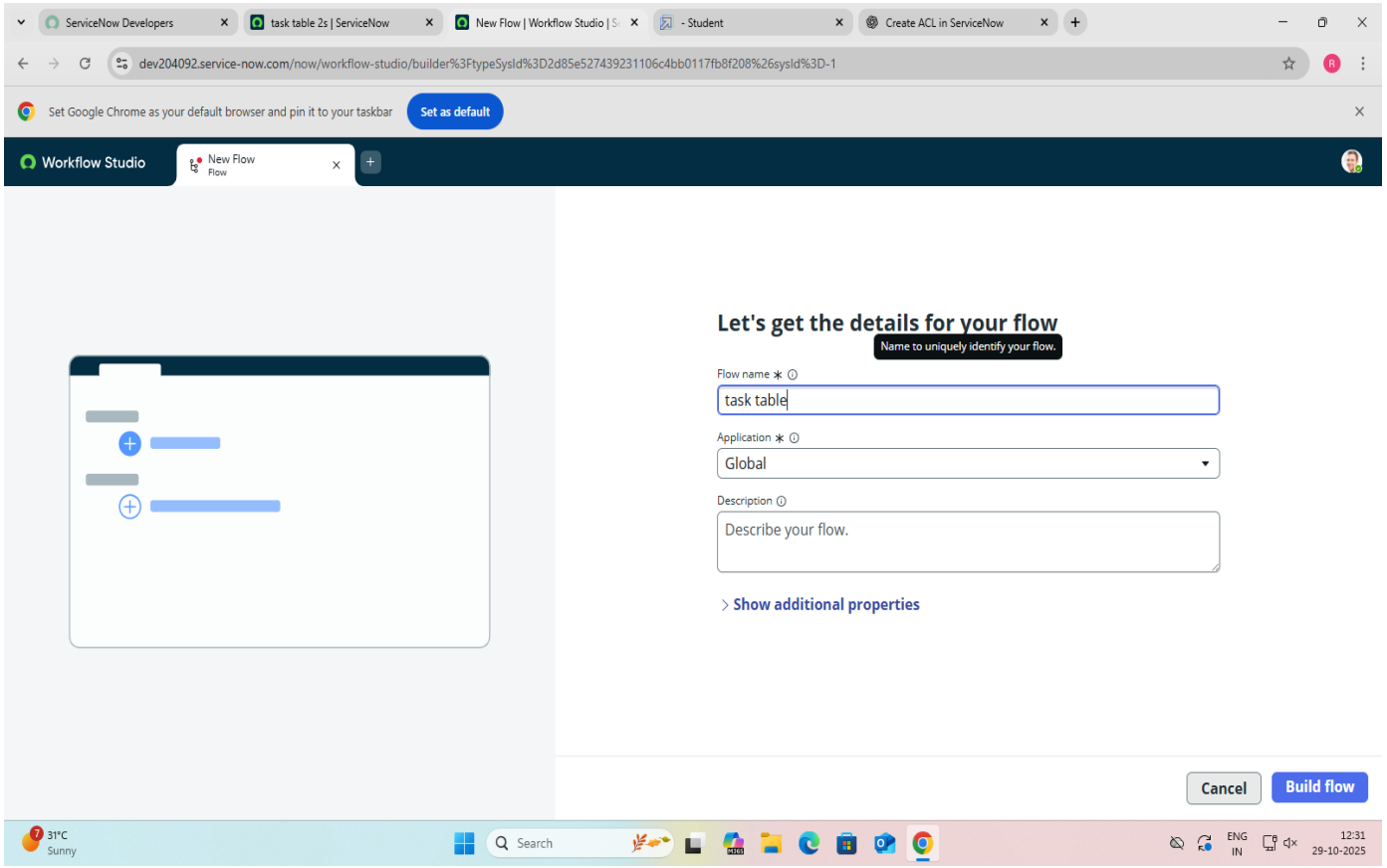


STEP 7: Create a Flow to Assign operations ticket to group

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.



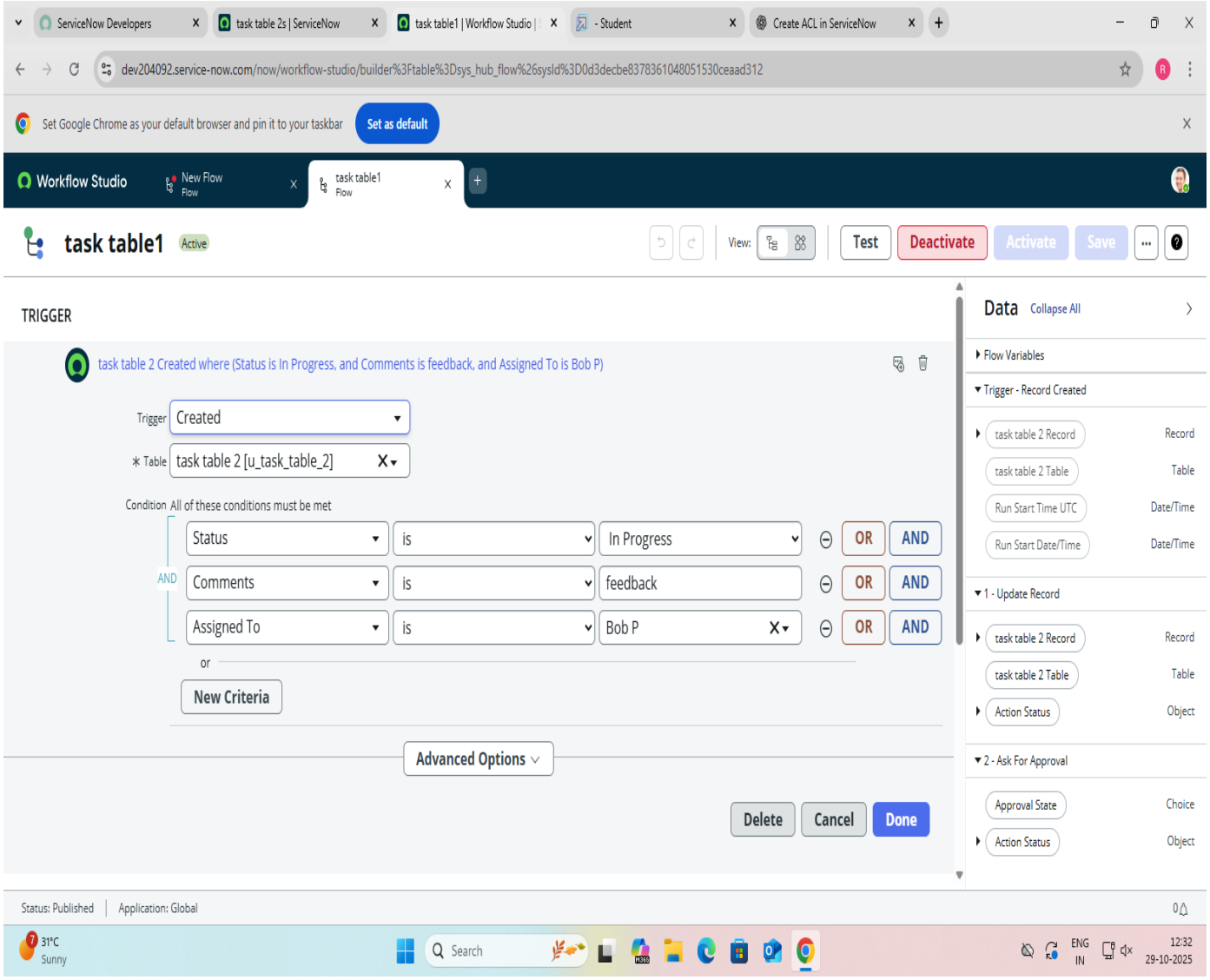

ServiceNow Developers
task table 2s | ServiceNow
Homepage - Flows | Workflow
- Student
Create ACL in ServiceNow
dev204092.service-now.com/now/workflow-studio/home/flow
Set Google Chrome as your default browser and pin it to your taskbar
Set as default
Workflow Studio
Homepage
Operations
Integrations
Playbooks
Flows
Subflows
Actions
Decision tables
New
Playbook
Flow
Subflow
Action
Decision table
Flows 70
Last refreshed just now
Name
Application
Status
Active
Updated
Admin Deployment Approval Flow Error Notifier
App Engine Studio
Published
true
2020-07-28 13:20:50
Admin Install App to Production Environment Flow Error Notifier
App Engine Studio
Published
true
2020-07-28 13:37:16
admin
Application Intake Request Flow
Application Intake
Published
true
2025-10-23 19:34:20
system
Application Intake Request V2
Application Intake
Published
true
2025-10-23 19:34:13
system
Benchmark Recommendation Evaluator
Benchmarks Spoke
Published
true
2025-08-07 13:17:11
system
Business process approval flow
Global
Published
true
2020-09-27 22:06:13
admin
Change - Cloud Infrastructure - Authorize
Global
Published
true
2020-11-11 07:08:05
admin
Change - Emergency - Authorize
Global
Published
true
2020-10-06 05:39:49
admin
Change - Emergency - Implement
Global
Published
true
2020-09-23 05:06:26
admin
Pick up where you left off
task table1
Last updated: 5 h. ago by System Adminis...
task table
Last updated: 15 h. ago by System Admini...
Create Flow Data
Last updated: a year ago by System Admi...
Latest updates
System Administrator modified task table1
5 h. ago
System Administrator modified task table
15 h. ago
System Administrator modified Create Flow Data
a year ago
System Administrator modified Deployment Environment Type Flow


ServiceNow Developers
task table 2s | ServiceNow
New Flow | Workflow Studio
- Student
Create ACL in ServiceNow
dev204092.service-now.com/now/workflow-studio/builder%3FtypeSysId%3D2d85e527439231106c4bb0117fb8f208%26sysId%3D-1
Set Google Chrome as your default browser and pin it to your taskbar
Set as default
Workflow Studio
New Flow
Flow
Let's get the details for your flow
Name to uniquely identify your flow.
Flow name
task table
Application
Global
Description
Describe your flow.
Show additional properties
Cancel
Build flow

next step:

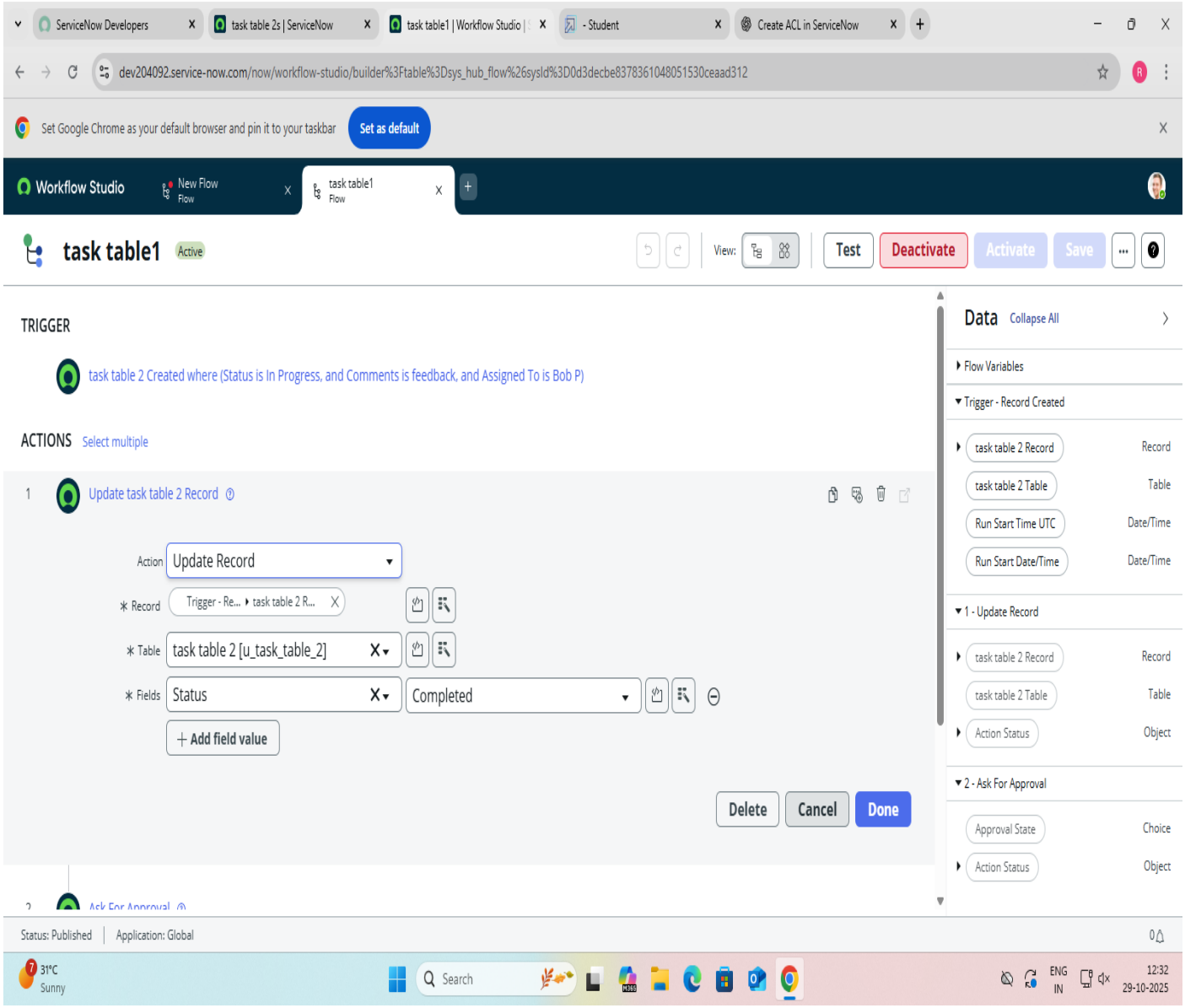
1. Click on Add a trigger
2. Select the trigger in that Search for “create record” and select that.
3. Give the table name as “ task table ”.
4. Give the Condition as

   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.



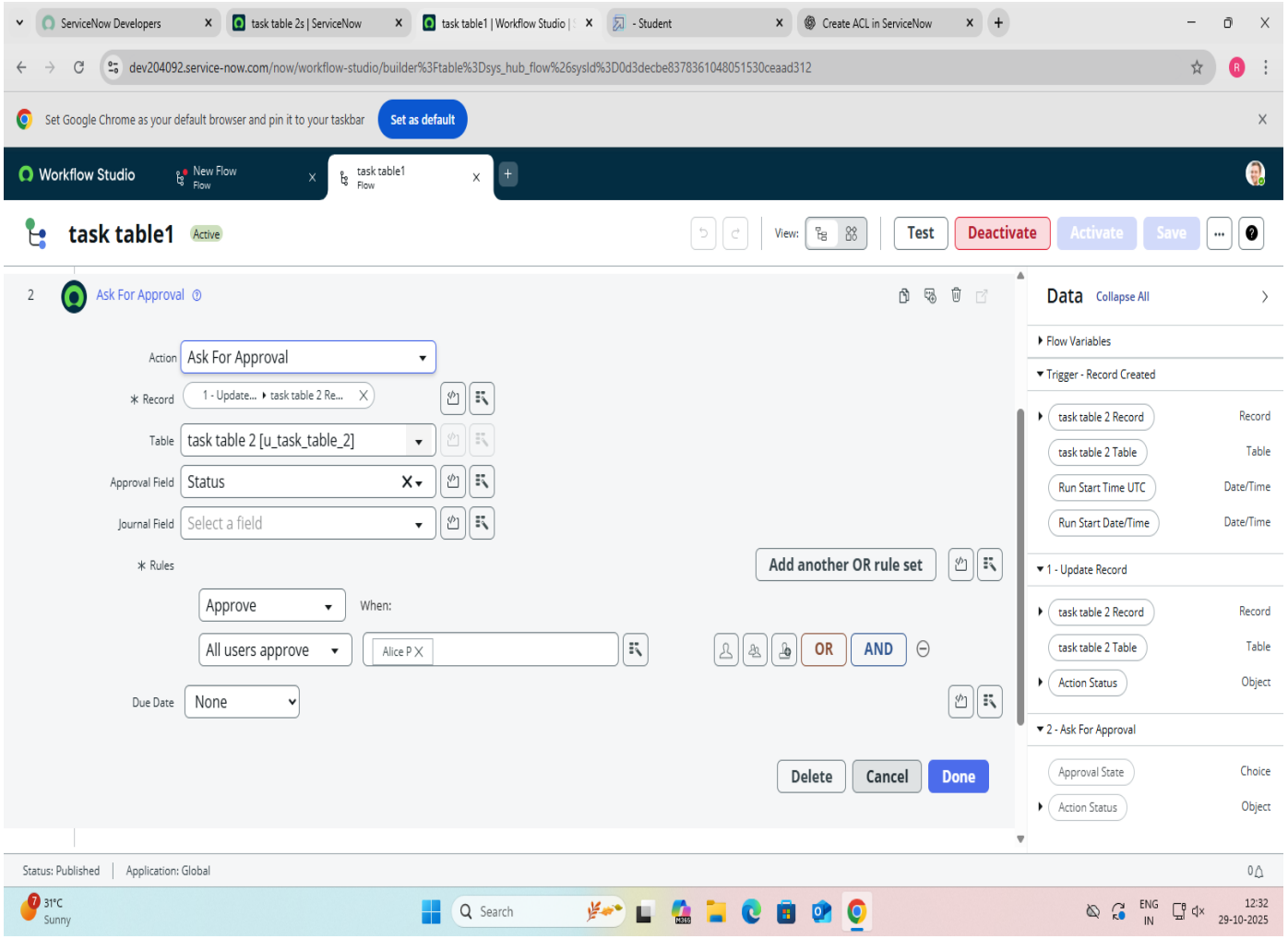
Next step:

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"
6. Click on Done.

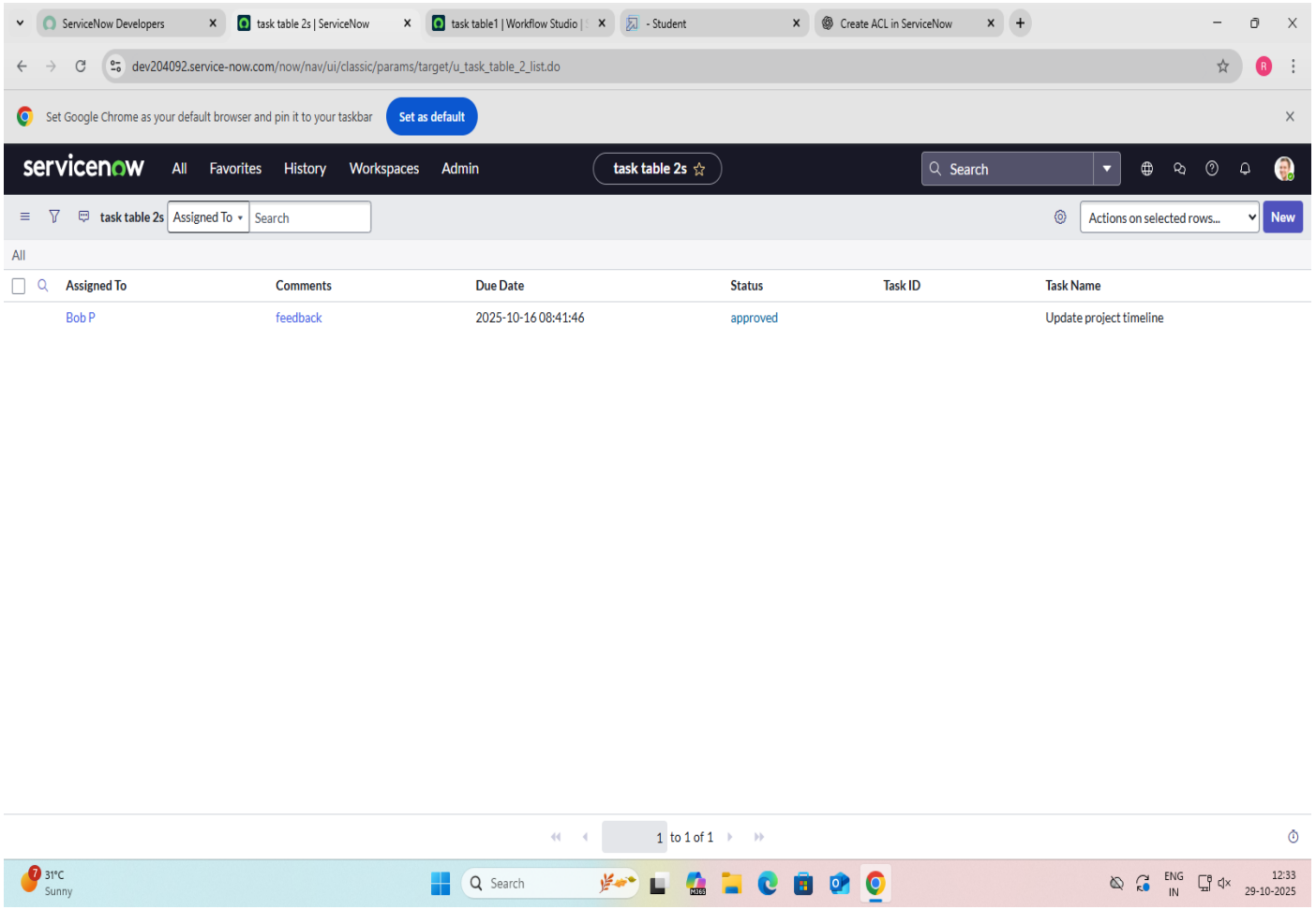


Next step:

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

ServiceNow Developers | Approvals | ServiceNow | task table1 | Workflow Studio | - Student | Create ACL in ServiceNow

dev204092.service-now.com/now/nav/ui/classic/params/target/sysapproval_approver_list.do%3Fsysparm_query%3D%26sysparm_first_row%3D1%26sysparm_view%3D

Set Google Chrome as your default browser and pin it to your taskbar | Set as default

servicenow | All | Favorites | History | Workspaces | Admin | Approvals | Search

Approvals | Approver | Search | Actions on selected rows...

All

State	Approver	Comments	Approval for	Created
Approved	Alice P		(empty)	2025-10-28 09:30:37
Requested	Bernard Laboy		CHG0000053	2025-08-06 06:09:38
Requested	Bernard Laboy		CHG0000071	2025-08-06 06:12:10
Requested	Bernard Laboy		CHG0000037	2025-08-06 06:04:51
Requested	Bernard Laboy		CHG0000076	2025-08-06 06:13:15
Requested	Bernard Laboy		CHG0000094	2025-08-06 06:15:21
Requested	Bernard Laboy		CHG0000051	2025-08-06 06:09:31
Requested	Bernard Laboy		CHG0000073	2025-08-06 06:12:19
Requested	Bernard Laboy		CHG0000090	2025-08-06 06:15:07
Requested	Bernard Laboy		CHG0000074	2025-08-06 06:12:23
Requested	Bernard Laboy		CHG0000055	2025-08-06 06:09:47
Requested	Bernard Laboy		CHG0000078	2025-08-06 06:13:24
Requested	Bernard Laboy		CHG0000091	2025-08-06 06:15:11
Requested	Bernard Laboy		CHG0000045	2025-08-06 06:07:48
Requested	Bernard Laboy		CHG0000081	2025-08-06 06:13:36
Requested	Bernard Laboy		CHG0000052	2025-08-06 06:09:35
Requested	Bernard Laboy		CHG0000049	2025-08-06 06:08:06

1 to 20 of 664

31°C Sunny | Search | ENG IN | 12:33 29-10-2025

Conclusion and Future Scope:

The project “Optimizing User, Group, and Role Management with Access Control and Workflows” successfully developed an automated and secure system using ServiceNow tomanage users, groups, and roles efficiently. It replaced manual processes with streamlined workflows, ensuring faster approvals, better access control, and reduced administrative effort.By implementing Role-Based Access Control (RBAC) and automated workflows, the system enhanced data security, accuracy, and transparency across the organization. The project achieved its goals of improving operational efficiency, minimizing errors, andstrengthening overall governance in user and role management.