### Access Control for Project Table

## Project Overview

## The "Access Control for Project Table" project implements role-based access control (RBAC) to secure project data by assigning user-specific permissions (e.g., read, write, edit, delete) based on roles like admin, manager, or team member. This ensures only authorized users access or modify project data, enhancing data security and compliance while supporting streamlined collaboration within the organization.

# Objectives

* **Streamline Access Control Process:** Automate and standardize user permissions from setup to approval to ensure efficient and secure access management.
* **Enhance Accessibility:** Enable users to quickly and easily access the project table according to their role-based permissions.
* **Improve Decision Making:** Ensure authorized team members have timely access to accurate project data for better decision-making.
* **Minimize Redundant Permissions:** Maintain accurate, relevant permissions to avoid duplications and reduce risks associated with unnecessary access.

# 3.Key Features and Concepts Utilized

* + **Role-Based Access Control (RBAC): Assigns permissions by role (e.g., admin, team member) for secure access.**
  + **Granular Permissions: Controls read, write, edit, delete options per user role.**
  + **Audit Trails: Logs all access and actions for accountability.**
  + **Dynamic Permissions: Easily update roles as team needs change.**
  + **Authentication Integration: Works with SSO and MFA for secure access.**
  + **Access Requests: Automated approval process for new access needs.**

# 4.Detailed Steps

# Step-1: Sign in to ServiceNow.

# 

# Step 2 : Sign up for a developer account on the ServiceNow Developer site “[https://developer.servicenow.com](https://developer.servicenow.com/)”.

# Step 3 : Once logged in, navigate to the "Personal Developer Instance" section.

# Click on "Request Instance" to create a new ServiceNow instance.

# Step 4 : Fill out the required information and submit the request.

# Step 5 : Log in to your ServiceNow instance using the provided credentials.

# Now you will navigate to the ServiceNow.

# 

# Step 6 :  Open “Tables” >> New.

# Step 7 : Fill the details of the table with fields as below >> Save.

# 

# Step 8 : Open User  >> New.

# 

# Step 9 : Create Two Users Product Manager and Employe Management.

# 

# 

# Step 10 : Open Role >>New

# 

# Step 11 : Create Employee Role.

# Step 12 : Go to the Project table >> Controls >> copy the role name from the table.

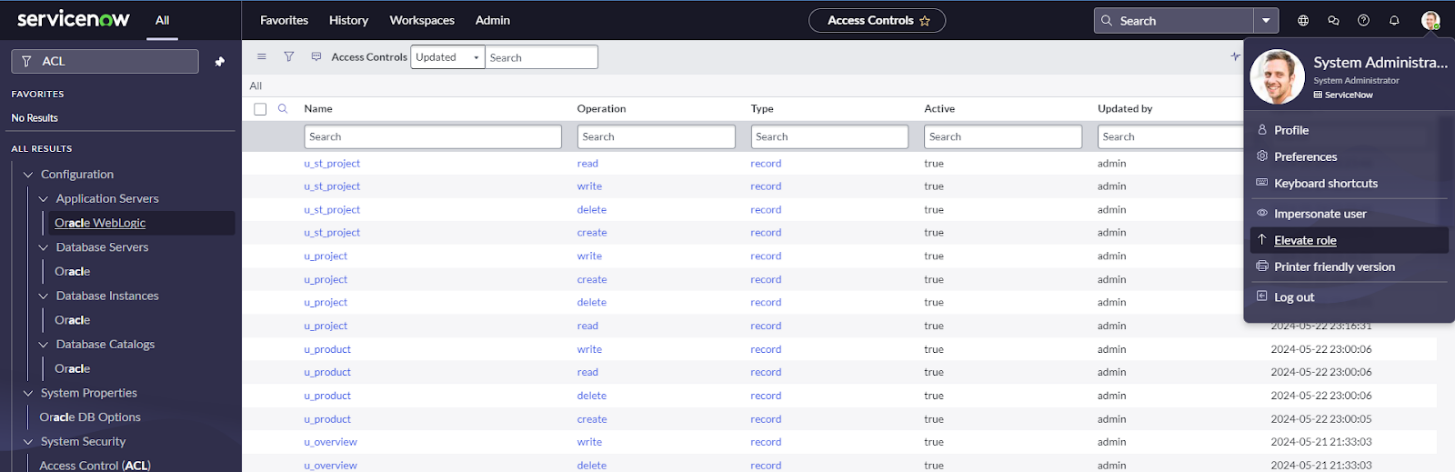
# Go to Product Management User and add role : u\_project\_user to it.

# 

# Step 13 : Go to Employe Management User and add role : Employe role to it.

# 

# Step 14 : Click on the Profile avatar >>  Elevate Role >> Grant the high security



**Step 15:** Search & Open ACL >> New.

# 

# Step 16 :Fill the details below and Create Read Operation Table Level ACL(none) on Employee role Save.

# 

# Step 17 :New >> Fill the details below and Create Read Operation Field Level ACL(Budget) on  role: u\_project\_user >> Save.

# 

# Step 18 :New >> Fill the details below and Create Read Operation Field Level ACL(Total Expenses) on  role: u\_project\_user >> Save.

# 

# Step 19 : Impersonate User >> Product Management.

# Step 20 : All >> Project >> New(We can see that the product Manager has all the CRWD access).

# Step 21 : Create 3 Records with any details .

# 

# 5.Testing and Validation:

## Access Control Testing: Verify role-based permissions by testing each role (admin, manager, team member) for correct access (read, write, edit, delete) to ensure compliance with predefined rules.

## User Access Scenarios: Test various user scenarios, such as role changes and permission updates, to confirm that permissions are updated dynamically and accurately.

## 6.Key Scenarios Addressed by ServiceNow in the Implementation Project:

**Automated Access Control:** ServiceNow manages role-based permissions, automating the assignment and updating of user access levels for enhanced security.

**Review and Approval Workflow**: Articles are routed to reviewers and approvers based on pre-defined workflows. Automated notifications remind stakeholders of pending actions.

**Centralized Access Management**: ServiceNow provides a single platform for managing access control, making it easier for administrators to view, modify, and audit permissions.

**Audit and Compliance Tracking:** ServiceNow maintains a comprehensive log of access activities, supporting compliance audits and accountability.

# 7.Conclusion

In conclusion, implementing access control for the project table using ServiceNow enhances data security, ensures compliance, and streamlines permission management. Role-based access control allows for tailored, efficient access that aligns with organizational needs. The integration with authentication protocols strengthens data protection, while automated workflows and audit trails ensure accountability and ease of management. Overall, this solution empowers teams with secure, scalable access to project data, supporting effective collaboration and informed decision-making.

