# NAAN MUDHALVAN PROJECT

Project Title:  Access Control for Project Table

## Team Members

| s.no | Name | Naan Mudhalvan- ID | E Mail-ID |
|------|------|--------------------|-----------|
| 1. | Athirala Ganesh | au723921243003 | athiralaganesh004@gmail.com |
| 2. | Bandaru Manoj | au723921243004 | bandarumanoj382@gmail.com |
| 3. | Vupathi Manoj | au723921243059 | manojmodaliyar10@gmail.com |
| 4. | Gattamaneni Nikhil | au723921243056 | nikhilgattamaneni25@gmail.com |
| 5. | Vukoti Praharsha | au723921243058 | Praharshasingle@gmail.com |

ARJUN COLLEGE OF TECHNOLOGY- COIMBATORE

DEPARTMENT OF

ARTIFICIAL INTELLIGENCE & DATA SCIENCE

## Abstract:

In a bid to optimize user experience and enhance data security, this project focuses on customizing the ServiceNow Project table to implement access control mechanisms. The primary objective is to enable ServiceNow Product Managers to hide specific fields from employees, particularly those with the "Employee Management" user role, ensuring that these users only see the fields pertinent to their responsibilities.

# Implementation

**Step 1 :** Sign in to ServiceNow.
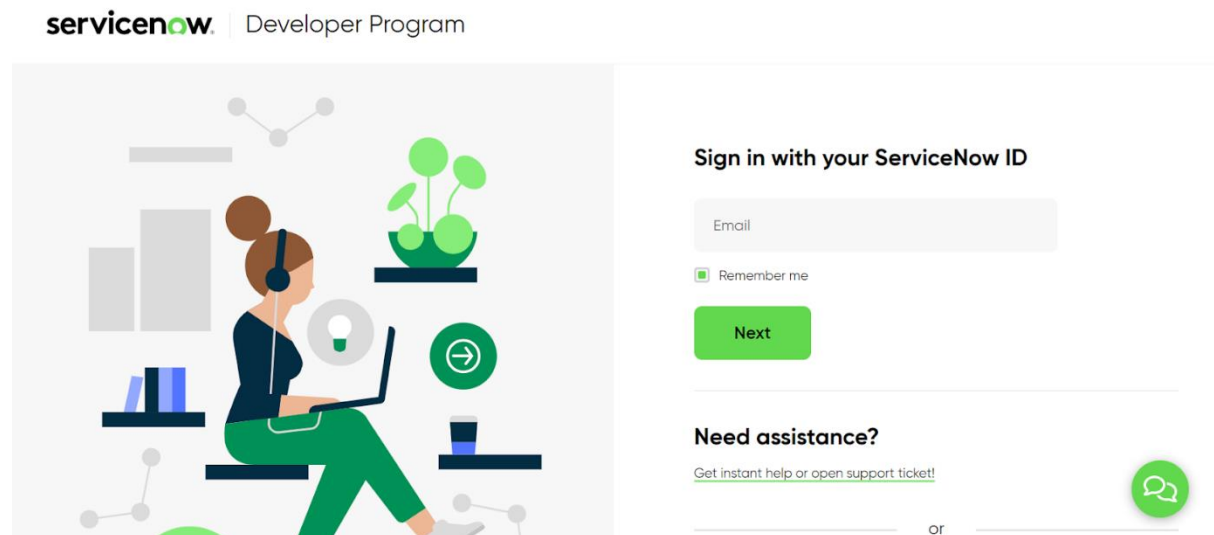


**Step 2 :** Sign up for a developer account on the ServiceNow Developer site "https://developer.servicenow.com".

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

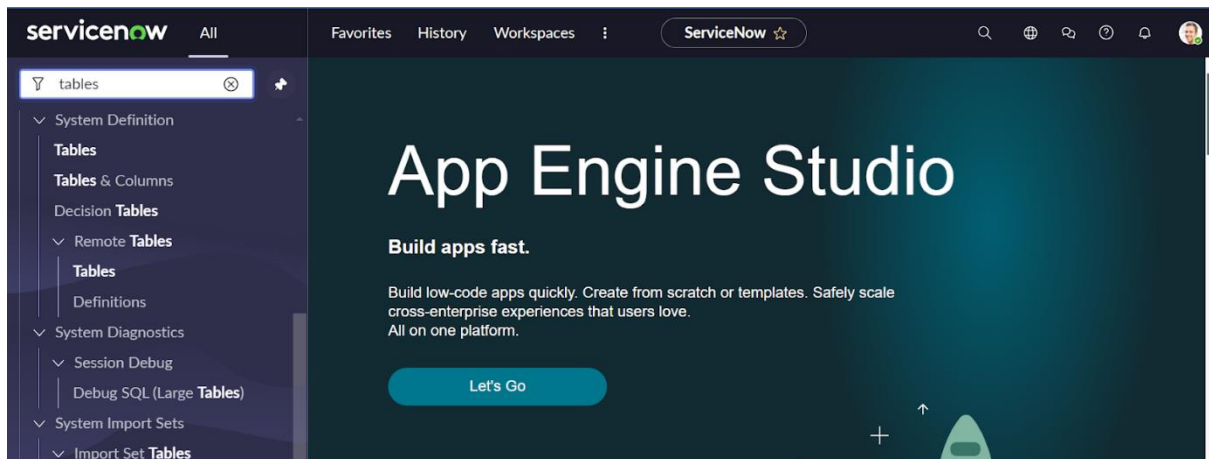Click on "Request Instance" to create a new ServiceNow instance.

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

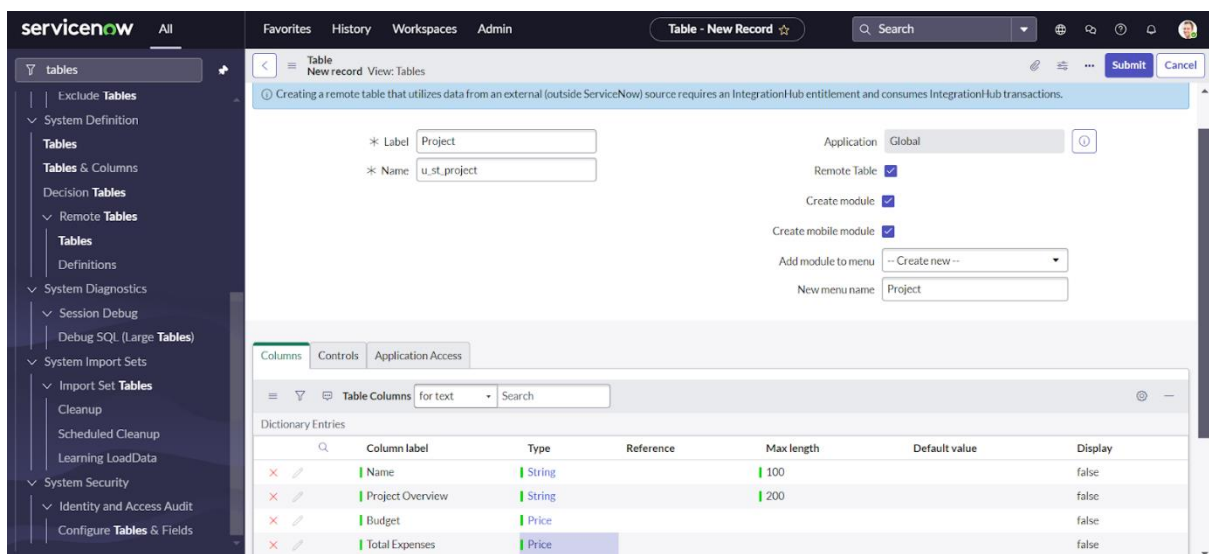**Step 5 :** You'll receive an email with the instance details once it's ready.

**Step 6 :** Log in to your ServiceNow instance using the provided credentials.

Now you will navigate to the ServiceNow.
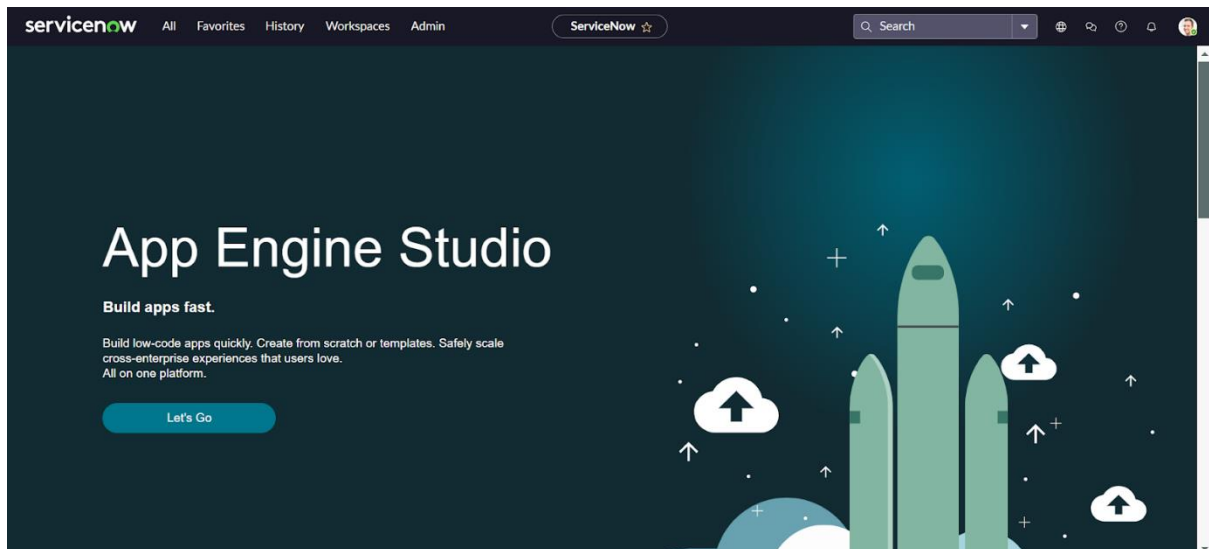
**Step 7 :** Open "Tables" >> New.



**Step 8 :** Fill the details of the table with fields as below >> Save.

**Step 9 :** Open User >> New.

**Step 10 :** Create Two Users Product Manager and Employee Management.



**Step 11 :** Open Role >>New



**Step 10 :** Create Employee Role.

**Step 11 :** 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 12 :** Go to Employe Management User and add role : Employe role to it.



**Step 13 :** Click on the Profile avatar >> Elevate Role >> Grant the high security

**Step 14 :** Search & Open ACL >> New.



**Step 15 :** Fill the details below and Create Read Operation Table Level ACL(none) on Employee role >> Save.

**Step 16 :** New >> Fill the details below and Create Read Operation Field Level ACL(Budget) on  role: u_project_user >> Save.



**Step 17 :** New >> Fill the details below and Create Read Operation Field Level ACL(Total Expenses) on  role: u_project_user >> Save.
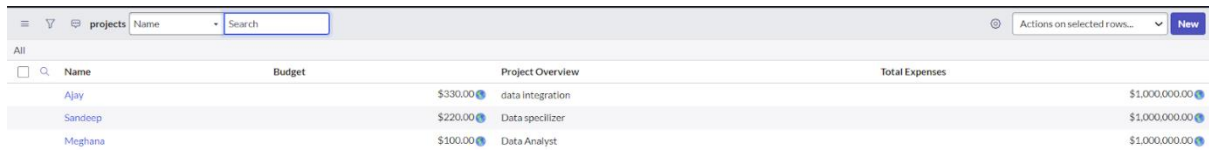


**Step 18 :** Impersonate User >> Product Management.

**Step 19 :** All >> Project >> New(We can see that the product Manager has all the CRWD access).

**Step 20** : Create 3 Records with any details .



# Conclusion:

Implementing access control on the ServiceNow Project table is crucial for ensuring data security and enhancing the productivity of employees. Through the outlined steps, the ServiceNow Product Manager can successfully configure access restrictions, thereby hiding certain fields from employees, particularly those with the "Employee Management" user role.

This project demonstrates a comprehensive approach to customizing the ServiceNow platform, leveraging skills in form, application, module, tables, and Access Control Lists (ACL). By carefully following these steps, the organization can create a streamlined user experience, allowing employees to focus solely on the fields and tasks pertinent to their roles.

Ultimately, this customization not only enhances security by restricting access to sensitive information but also optimizes workflow efficiency, making the ServiceNow environment more tailored and effective for all users involved.