

NAAN MUDHALVAN PROJECT

Project Title: Access Control for Project Table

Team Members

s.no	Name	Naan Mudhalvan- ID	E Mail-ID
1.	Chennapatnam Yaswanth	au723921243011	yaswanthyashuchannapatanam1@gmail.com
2.	Gangavarapu Mahendra	au723921243020	mahig4295@gmail.com
3.	Chutti Hemanth Kumar	au723921243014	chuttihemanth123@gmail.com

ARJUN COLLEGE OF TECHNOLOGY- COIMBATORE

DEPARTMENT OF

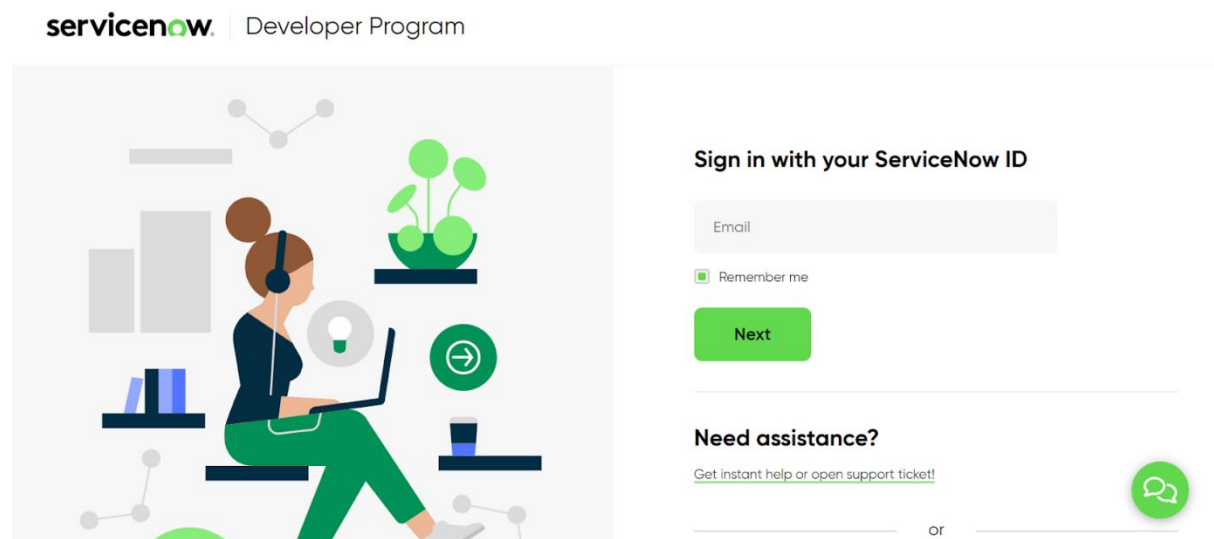
ARTIFICIAL INTELLIGENCE & DATA SCIENCE

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.



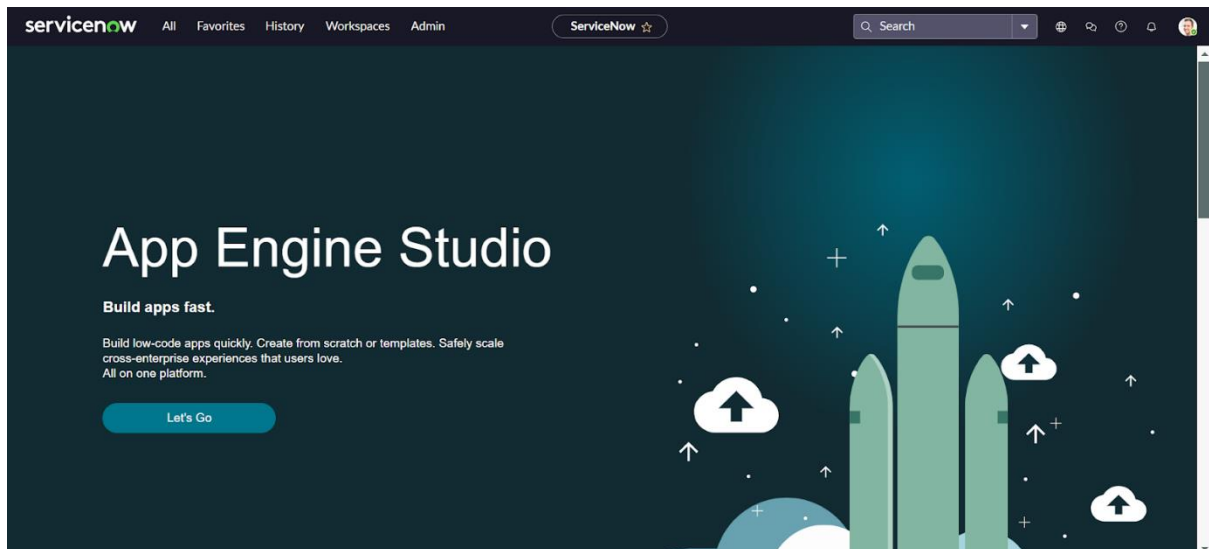
Step 2 : Sign up for a developer account on the ServiceNow Developer site
“<https://developer.servicenow.com>”.

Step 3 : Once logged in, navigate to the "Personal Developer Instance" section.
Click on "Request Instance" to create a new ServiceNow instance.

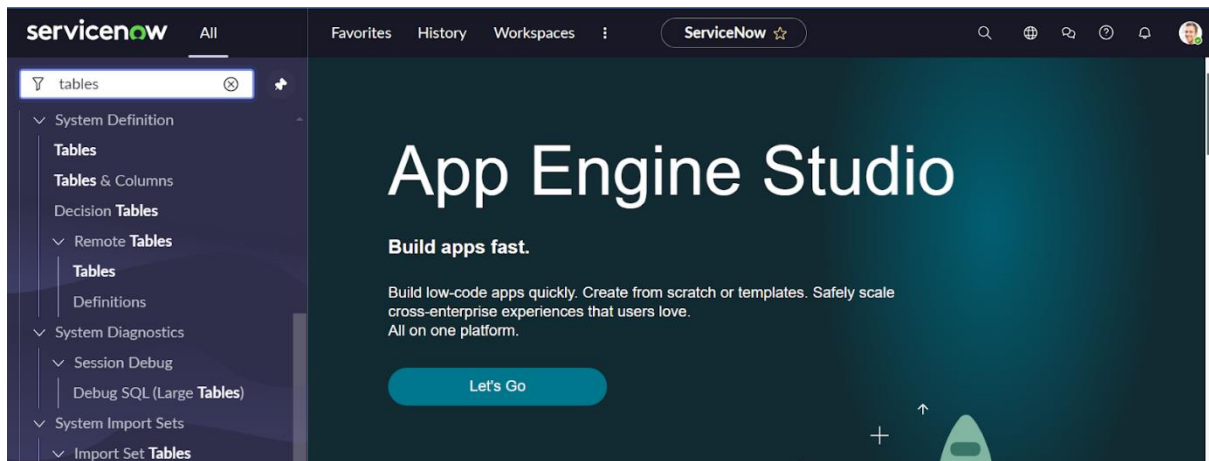
Step 4 : Fill out the required information and submit the request.

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

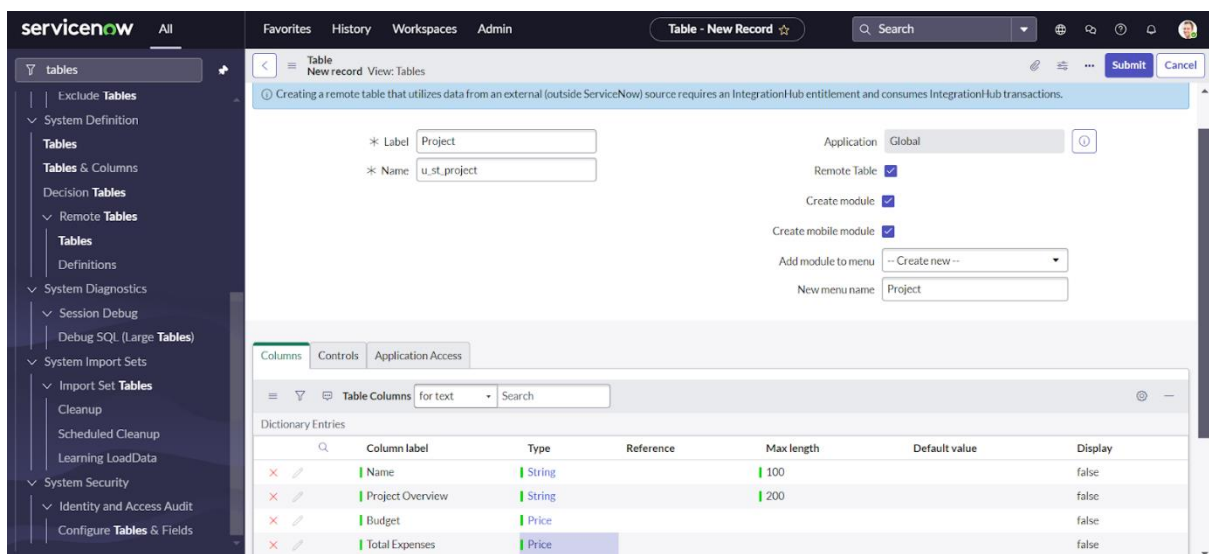
Step 6 : Log in to your ServiceNow instance using the provided credentials.
Now you will navigate to the ServiceNow.



Step 7 : Open “Tables” >> New.



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



User ID	Name	Email	Active	Created	Updated
Sandeep Gujja	Sandeep Gujja	sandeepgujja999@gmail.com	true	2024-04-17 03:14:58	2024-04-17 03:14:58
admin	System Administrator	admin@example.com	true	2007-07-03 11:48:47	2024-04-17 02:44:15
Mishra Sri	Mishra Sri	Mishra6@gmail.com	true	2024-04-17 02:26:10	2024-04-17 02:31:42
aes.creator	Creator User		true	2024-03-18 22:29:50	2024-04-01 21:03:24
eddie.gauer	Eddie Gauer	eddie.gauer@example.com	true	2012-02-17 19:04:51	2024-03-18 21:38:30
bms.scheduler	Benchmark Scheduler		true	2017-02-24 12:14:31	2024-03-18 21:38:30
problem.manager	Problem Manager	problem.manager@example.com	true	2023-10-04 22:01:07	2024-03-18 21:38:30
germaine.bruski	Germaine Bruski	germaine.bruski@example.com	true	2012-02-17 19:04:50	2024-03-18 21:38:30
rebekah.lindboe	Rebekah Lindboe	rebekah.lindboe@example.com	true	2012-02-17 19:04:50	2024-03-18 21:38:30
steve.schorr	Steve Schorr	steve.schorr@example.com	true	2012-02-17 19:04:50	2024-03-18 21:38:30
darrel.ruffins	Darrel Ruffins	darrel.ruffins@example.com	true	2012-02-17 19:04:51	2024-03-18 21:38:30
judi.kivel	Judi Kivel	judi.kivel@example.com	true	2012-02-17 19:04:51	2024-03-18 21:38:30
lina.hybarger	Lina Hybarger	lina.hybarger@example.com	true	2012-02-17 19:04:51	2024-03-18 21:38:30
pat.hoshaw	Pat Hoshaw	pat.hoshaw@example.com	true	2012-02-17 19:04:51	2024-03-18 21:38:30
ATF.User	ATF User	ATF.User@example.com	true	2016-07-07 11:56:17	2024-03-18 21:38:30
article.alp	Melissa Pena		true	2019-02-08 01:52:42	2024-03-18 21:38:30

Step 9 : Open User >> New.

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

User ID	Name	Email	Active
Employee Management	Employee Management		true
Product Management	Product Management		true
Sandeep Gujja	Sandeep Gujja	sandeepgujja999@gmail.com	true
admin	System Administrator	admin@example.com	true
Mishra Sri	Mishra Sri	Mishra6@gmail.com	true

Step 11 : Open Role >>New

Name	Description	Elevated privilege
action_category.creator	Allows creation of action and subflow categories.	false
action_designer	action designer role enables users to launch Action Designer	false
activity_admin	Can create, edit, publish or delete wfl element_provider	false
activity_creator	This role give workflow users the ability to create custom orchestration activities in the workflow canvas.	false
actsub_admin	Activity Subscriptions Administrator role	false
actsub_user	Activity Subscriptions User role	false
admin	The System Administrator role. This role has access to all system features, functions, and data, regardless of security constraints. "Grant this privilege carefully." If you have sensitive information, such as HR records, that you need to protect, you must create a custom "admin" role for that area and train a person authorized to see those records to act as the administrator	false
agent_admin	Can download and administer the system's built-in agent	false
agent_security_admin	Manages security of the MID Server.	false
agent_workspace_user	Users of the Agent Workspace application. may navigate to the URI for that application	false

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.

The screenshot shows the ServiceNow User Management interface for a user named 'Product Management'. The left sidebar contains a navigation menu with categories like System Logs, System Security, Users and Groups, Reports, Identity and Access Audit, System User Guide, User Administration, and Time-Limited User Roles. The main content area is titled 'User - Product Management' and includes fields for User ID, First name, Last name, Title, Department, Password needs reset, Locked out, Active, Web service access only, and Internal integration User. There are also fields for Email, Language, Calendar integration, Time zone, Date format, Business phone, and Mobile phone. Below the form, there are buttons for 'Update', 'Set Password', and 'Delete'. A 'Related Links' section contains links for 'View linked accounts', 'View Subscriptions', and 'Reset a password'. At the bottom, there is a table titled 'Entitled Custom Tables' with columns for Role, State, Inherited, and Inheritance Count. The table shows one role, 'u_project_user', which is Active and not inherited.

Role	State	Inherited	Inheritance Count
u_project_user	Active	false	

Step 12 : Go to Employee Management User and add role : Employee role to it.

The screenshot shows the ServiceNow User Management interface for a user named 'Employee Management'. The left sidebar contains a navigation menu with categories like System Logs, System Security, Users and Groups, Reports, Identity and Access Audit, System User Guide, User Administration, and Time-Limited User Roles. The main content area is titled 'User - Employee Management' and includes fields for User ID, First name, Last name, Title, Department, Password needs reset, Locked out, Active, Web service access only, and Internal integration User. There are also fields for Email, Language, Calendar integration, Time zone, Date format, Business phone, and Mobile phone. Below the form, there are buttons for 'Update', 'Set Password', and 'Delete'. A 'Related Links' section contains links for 'View linked accounts', 'View Subscriptions', and 'Reset a password'. At the bottom, there is a table titled 'Entitled Custom Tables' with columns for Role, State, Inherited, and Inheritance Count. The table shows one role, 'Employee', which is Active and not inherited.

Role	State	Inherited	Inheritance Count
Employee	Active	false	

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

Name	Operation	Type	Active	Updated by	Updated
u_st_project	read	record	true	admin	2024-05-22 23:16:31
u_st_project	write	record	true	admin	2024-05-22 23:16:31
u_st_project	delete	record	true	admin	2024-05-22 23:16:31
u_st_project	create	record	true	admin	2024-05-22 23:00:06
u_project	write	record	true	admin	2024-05-22 23:00:06
u_project	create	record	true	admin	2024-05-22 23:00:06
u_project	delete	record	true	admin	2024-05-22 23:00:06
u_project	read	record	true	admin	2024-05-21 21:33:03
u_product	write	record	true	admin	2024-05-22 23:00:06
u_product	read	record	true	admin	2024-05-22 23:00:06
u_product	delete	record	true	admin	2024-05-22 23:00:06
u_product	create	record	true	admin	2024-05-22 23:00:05
u_overview	write	record	true	admin	2024-05-21 21:33:03
u_overview	delete	record	true	admin	2024-05-21 21:33:03

Step 14 : Search & Open ACL >> New.

Name	Operation	Type	Active	Updated by	Updated
u_project	write	record	true	admin	2024-05-22 23:16:31
u_project	create	record	true	admin	2024-05-22 23:16:31
u_project	delete	record	true	admin	2024-05-22 23:16:31
u_project	read	record	true	admin	2024-05-22 23:16:31
u_product	write	record	true	admin	2024-05-22 23:00:06
u_product	read	record	true	admin	2024-05-22 23:00:06
u_product	delete	record	true	admin	2024-05-22 23:00:06
u_product	create	record	true	admin	2024-05-22 23:00:05
u_overview	write	record	true	admin	2024-05-21 21:33:03
u_overview	delete	record	true	admin	2024-05-21 21:33:03
u_overview	read	record	true	admin	2024-05-21 21:33:02
x_1346917_educat_0_admission_entries	read	record	true	admin	2024-04-03 22:02:21
x_1346917_educat_0_admission_entries	create	record	true	admin	2024-04-03 22:02:21
x_1346917_educat_0_admission_entries	create	record	true	admin	2024-04-03 22:02:21
x_1346917_educat_0_admission_entries	delete	record	true	admin	2024-04-03 22:02:21
x_1346917_educat_0_admission_entries	delete	record	true	admin	2024-04-03 22:02:21

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

* Type: record

* Operation: read

Application: Global

Active: ☒

Admin overrides: ☒

Advanced: ☐

Protection policy: -- None --

* Name: project[u_project]

Description:

Condition: 3 records match condition

Add Filter Condition Add "OR" Clause

-- choose field -- -- oper -- -- value --

Conditions

Requires role

Role
Employee

Local or Existing ☐ Existing ☒ Local

Condition: All of these conditions must be met

-- choose field -- -- value --

OR AND

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

Warning: Empty ACLs potentially allows for unauthenticated access. A Role, Security Attribute or Script must be specified to properly secure access with this ACL.

* Type: record Application: Global

* Operation: read Active: ☒

Admin overrides: ☒ Advanced: ☐

Protection policy: -- None --

* Name: project [u_project] Budget

Description:

Condition: 3 records match condition

Add Filter Condition Add "OR" Clause

-- choose field -- -- oper -- -- value --

Conditions

Requires role

Role
u_project_user

+ Insert a new row...

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

servicenow All

Favorites History Workspaces Admin

Access Control - New ...

Access Control - New record

Warning: Empty ACLs allow unauthenticated access. A Role, Security Attribute or Script must be specified to properly secure access with this ACL.

* Type: record Application: Global

* Operation: read Active: ☒

Admin overrides: ☒ Advanced: ☐

Protection policy: -- None --

* Name: project [u_project] Total Expenses

Description:

Condition: 3 records match condition

Add Filter Condition Add "OR" Clause

-- choose field -- -- oper -- -- value --

Conditions

Requires role

Role
u_project_user

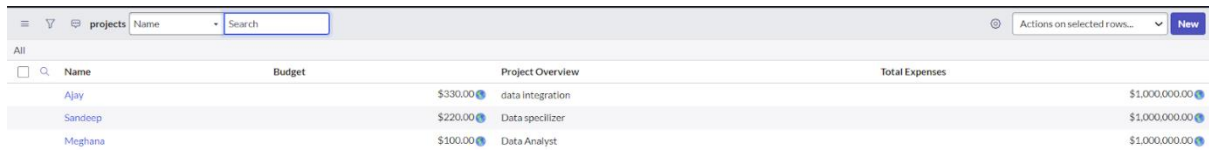
+ Insert a new row...

Local or Existing Existing Local

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 .



The screenshot shows a ServiceNow interface for a table named 'projects'. The table has columns for Name, Budget, Project Overview, and Total Expenses. There are three records listed: Ajay, Sandeep, and Meghana. Each record has a budget and a total expense of \$1,000,000.00. The Project Overview column contains details about the project, such as 'data integration' for Ajay, 'Data specilizer' for Sandeep, and 'Data Analyst' for Meghana.

Name	Budget	Project Overview	Total Expenses
Ajay	\$330.00	data integration	\$1,000,000.00
Sandeep	\$220.00	Data specilizer	\$1,000,000.00
Meghana	\$100.00	Data Analyst	\$1,000,000.00

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.