SERVICENOW PROJECT SUBMISSON

ACCESS CONTROL FOR PROJECT TABLE

Submitted by

KADAPANA ROHITH KUMAR REDDY (au 723921244022)

BOGGALA CHINNA GANGADHAR REDDY (au723921244010)

Arjun College of Technology , Coimbatore

Anna University Chennai -600 025

ACCESS CONTROL FOR PROJECT TABLE

Project Overview :

The goal of this project is to implement a robust access control system for a project table that stores sensitive information related to various projects. The system will ensure that only authorized users can access, modify, or delete project data based on their roles and permissions. This will enhance data security, streamline collaboration, and ensure compliancewith organizational policies

Objective:

Assign different levels of access to the project table based on user roles to ensure that users only perform actions that are appropriate for their role.

- **Example Roles**:
    - **Admin**: Full access to create, read, update, delete, and manage user permissions.
    - **Project Manager**: Ability to create, update, delete, and assign projects, but no access to manage other users or roles.
    - **Team Member**: Limited to reading and commenting on project data.
    - **Guest**: View-only access to specific, public project data.

1. Implement Granular Permissions

- **Objective**: Fine-tune access to specific operations (e.g., create, read, update, delete) at the project table level based on user role.
- **Example**:
    - Ensure that users with the "Team Member" role can view project details but cannot update or delete project information.
    - Restrict the "Admin" role to only edit user roles and permissions, not project data unless necessary.

2. Minimize the Risk of Unauthorized Access

- **Objective**: Protect the project table from unauthorized access by enforcing strict authentication and authorization checks.
- **Example**:
    - Users should not be able to bypass authentication.
    - Implement strong password policies, multi-factor authentication (MFA), or other security mechanisms to prevent unauthorized users from accessing the system.

3. Ensure Data Integrity and Protection

- **Objective**: Ensure that users can only modify or delete project data when they are authorized to do so and that their actions are logged for accountability.
- **Example**:

- Project Managers should only be able to edit projects they are associated with or authorized to manage.
- Use validation checks to prevent unauthorized data manipulation.
- Log all access attempts, including changes to project data, for auditing purposes.

Access Levels:

1. Project Manager (PM): Full access (create, read, update, delete)
2. Team Members: Read and update access (task assignments, status updates)
3. Stakeholders: Read-only access (project overview, progress)
4. External Partners: Limited read-only access (specific project details)

Access Control Rules:

1. PM can create, update, and delete projects.
2. Team members can update task assignments and status.
3. Stakeholders can view project overview and progress.
4. External partners can view limited project details.

Key Feactures and concept used:

1. Regularly review access permissions

2. Use strong passwords and encryption

3. Limit access to sensitive data

4. Monitor audit logs

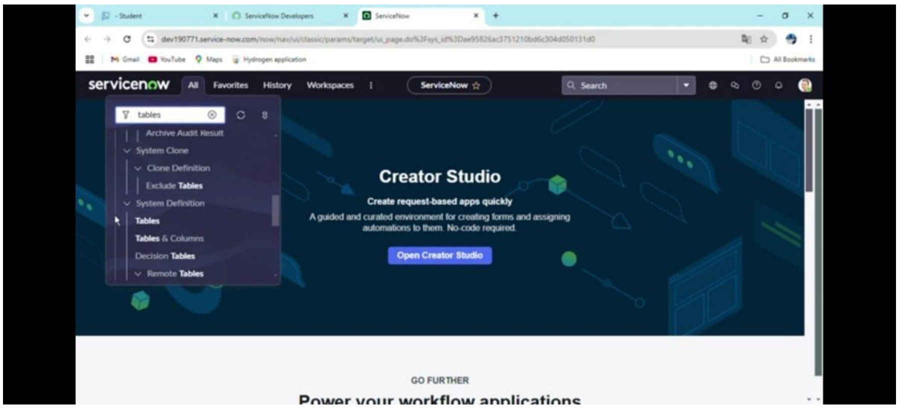
Detailed Steps To Solution Design :

Implementation :

Step 1: Sign up for a developer account on the ServiceNow Developer site

Step 2: Open Instance

Step 3: In All>>Tables



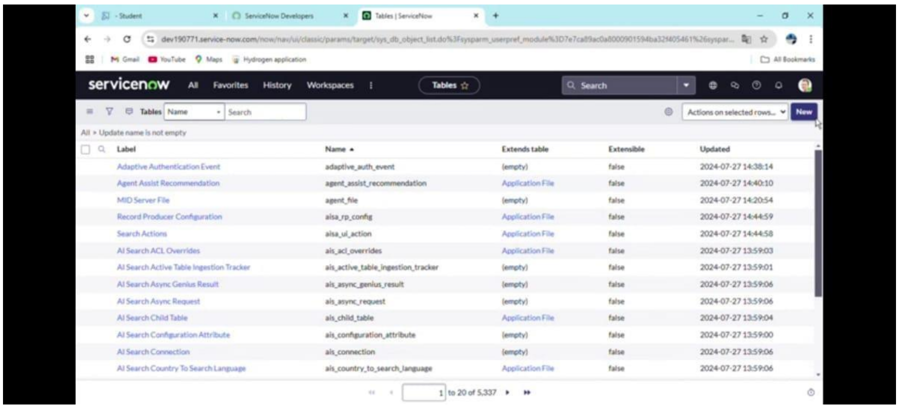
Creator Studio

Create request-based apps quickly

A guided and curated environment for creating forms and assigning automations to them. No-code required.

Power your workflow applications

Step 4: Click>>New


- Student
ServiceNow Developers
Tables | ServiceNow
dev190771.service-now.com/now/nav/ui/classic/params/target/sys_db_object_list.do%3Fsysparm_userpref_module%3D7e7ca89ac0a800090159 4ba32f405461%26syspar...
Gmail
YouTube
Maps
Hydrogen application
All Bookmarks
servicenow
All
Favorites
History
Workspaces
Tables
Search
Tables
Name
Search
Actions on selected rows...
New

All > Update name is not empty

Label	Name ▲	Extends table	Extensible	Updated
Adaptive Authentication Event	adaptive_auth_event	(empty)	false	2024-07-27 14:38:14
Agent Assist Recommendation	agent_assist_recommendation	Application File	false	2024-07-27 14:40:10
MID Server File	agent_file	(empty)	false	2024-07-27 14:20:54
Record Producer Configuration	aisa_rp_config	Application File	false	2024-07-27 14:44:59
Search Actions	aisa_ui_action	Application File	false	2024-07-27 14:44:58
AI Search ACL Overrides	ais_acl_overrides	Application File	false	2024-07-27 13:59:03
AI Search Active Table Ingestion Tracker	ais_active_table_ingestion_tracker	(empty)	false	2024-07-27 13:59:01
AI Search Async Genius Result	ais_async_genius_result	(empty)	false	2024-07-27 13:59:06
AI Search Async Request	ais_async_request	(empty)	false	2024-07-27 13:59:06
AI Search Child Table	ais_child_table	Application File	false	2024-07-27 13:59:04
AI Search Configuration Attribute	ais_configuration_attribute	(empty)	false	2024-07-27 13:59:00
AI Search Connection	ais_connection	(empty)	false	2024-07-27 13:59:06
AI Search Country To Search Language	ais_country_to_search_language	Application File	false	2024-07-27 13:59:06

1 to 20 of 5,337

Step 5: Fill The Details And Click Submit

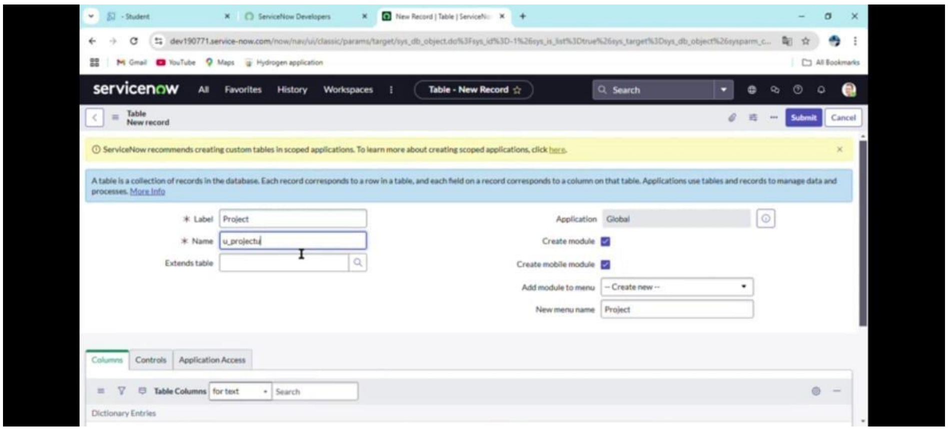


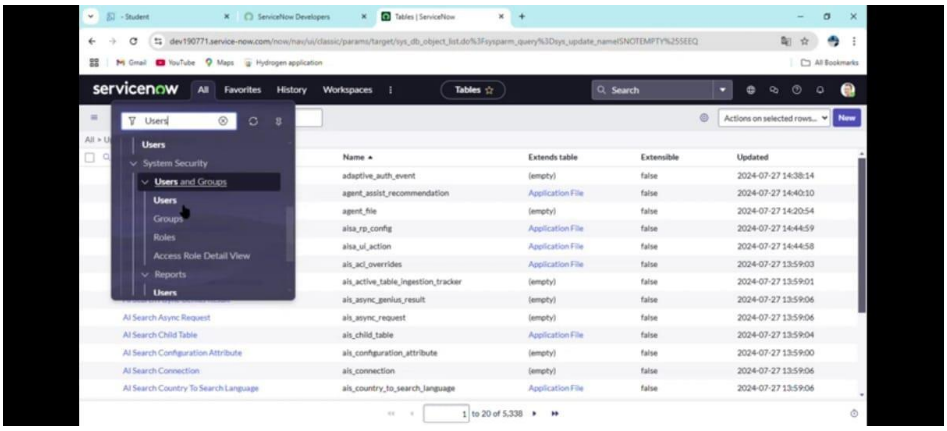
Table
New record

ⓘ ServiceNow recommends creating custom tables in scoped applications. To learn more about creating scoped applications, click here.

A table is a collection of records in the database. Each record corresponds to a row in a table, and each field on a record corresponds to a column on that table. Applications use tables and records to manage data and processes. More Info

* Label: Project
* Name: u_projectu
Extends table:
Application: Global
Create module: ☑
Create mobile module: ☑
Add module to menu: -- Create new --
New menu name: Project

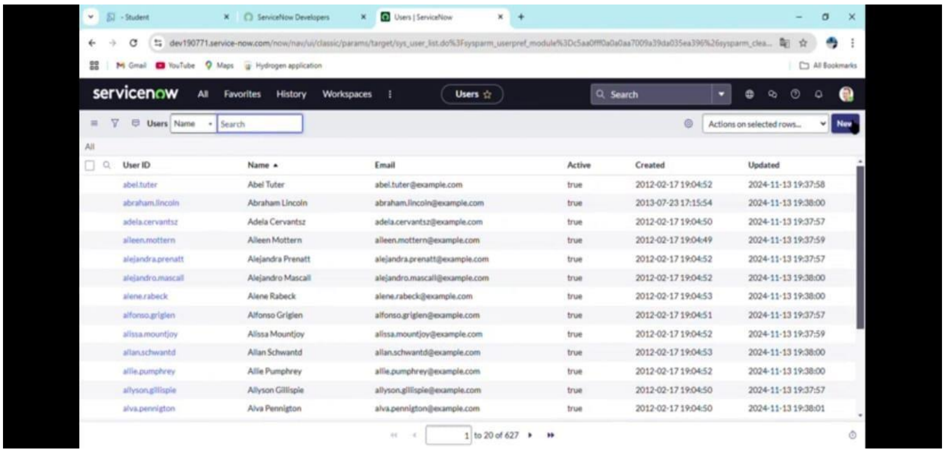
Step 6: In All>>Users


	Name ▲	Extends table	Extensible	Updated
	adaptive_auth_event	(empty)	false	2024-07-27 14:38:14
	agent_assist_recommendation	Application File	false	2024-07-27 14:40:10
	agent_file	(empty)	false	2024-07-27 14:20:54
	aisa_rp_config	Application File	false	2024-07-27 14:44:59
	aisa_ui_action	Application File	false	2024-07-27 14:44:58
	ais_acl_overrides	Application File	false	2024-07-27 13:59:03
	ais_active_table_ingestion_tracker	(empty)	false	2024-07-27 13:59:01
	ais_async_genius_result	(empty)	false	2024-07-27 13:59:06
AI Search Async Request	ais_async_request	(empty)	false	2024-07-27 13:59:06
AI Search Child Table	ais_child_table	Application File	false	2024-07-27 13:59:04
AI Search Configuration Attribute	ais_configuration_attribute	(empty)	false	2024-07-27 13:59:00
AI Search Connection	ais_connection	(empty)	false	2024-07-27 13:59:06
AI Search Country To Search Language	ais_country_to_search_language	Application File	false	2024-07-27 13:59:06

1 to 20 of 5,338

Step 7: Click>>New

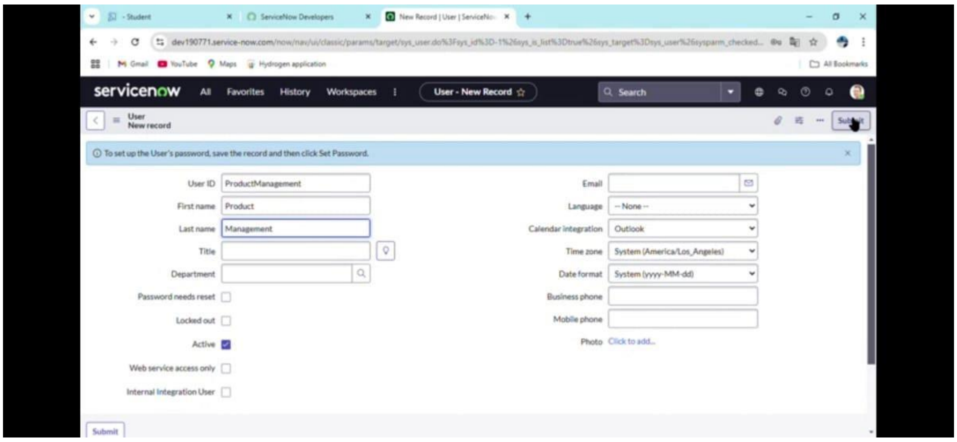
Create Two Users Product Manager and Employe Management



User ID	Name ▲	Email	Active	Created	Updated
abel.tuter	Abel Tuter	abel.tuter@example.com	true	2012-02-17 19:04:52	2024-11-13 19:37:58
abraham.lincoln	Abraham Lincoln	abraham.lincoln@example.com	true	2013-07-23 17:15:54	2024-11-13 19:38:00
adela.cervantsz	Adela Cervantsz	adela.cervantsz@example.com	true	2012-02-17 19:04:50	2024-11-13 19:37:57
aileen.mottern	Aileen Mottern	aileen.mottern@example.com	true	2012-02-17 19:04:49	2024-11-13 19:37:59
alejandra.prenatt	Alejandra Prenatt	alejandra.prenatt@example.com	true	2012-02-17 19:04:52	2024-11-13 19:37:57
alejandro.mascall	Alejandro Mascall	alejandro.mascall@example.com	true	2012-02-17 19:04:52	2024-11-13 19:38:00
alene.rabeck	Alene Rabeck	alene.rabeck@example.com	true	2012-02-17 19:04:53	2024-11-13 19:38:00
alfonso.griglen	Alfonso Griglen	alfonso.griglen@example.com	true	2012-02-17 19:04:51	2024-11-13 19:37:57
alissa.mountjoy	Alissa Mountjoy	alissa.mountjoy@example.com	true	2012-02-17 19:04:52	2024-11-13 19:37:59
allan.schwantd	Allan Schwantd	allan.schwantd@example.com	true	2012-02-17 19:04:53	2024-11-13 19:38:00
allie.pumphrey	Allie Pumphrey	allie.pumphrey@example.com	true	2012-02-17 19:04:52	2024-11-13 19:38:00
allyson.gillispie	Allyson Gillispie	allyson.gillispie@example.com	true	2012-02-17 19:04:50	2024-11-13 19:37:57
alva.pennigton	Alva Pennigton	alva.pennigton@example.com	true	2012-02-17 19:04:50	2024-11-13 19:38:01

1 to 20 of 627

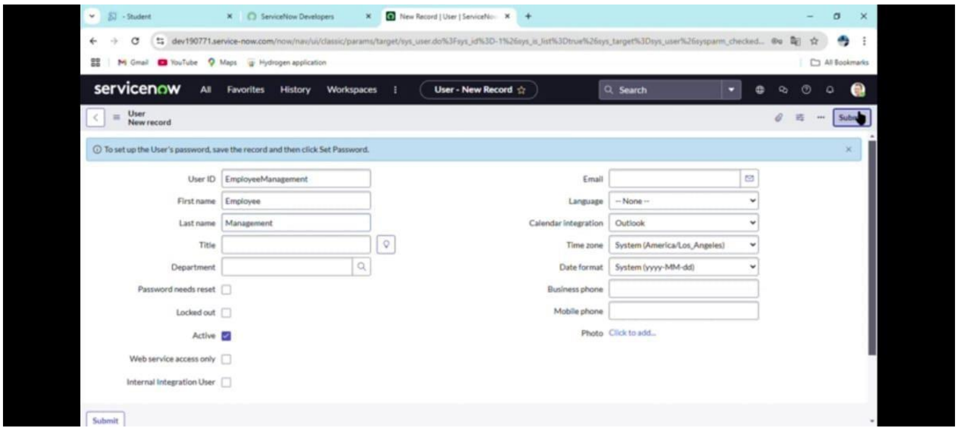
Step 8: Fill The Details And Click>>Submit



To set up the User's password, save the record and then click Set Password.

User ID: ProductManagement
First name: Product
Last name: Management
Title:
Department:
Password needs reset ☐
Locked out ☐
Active ☑
Web service access only ☐
Internal Integration User ☐

Email:
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...

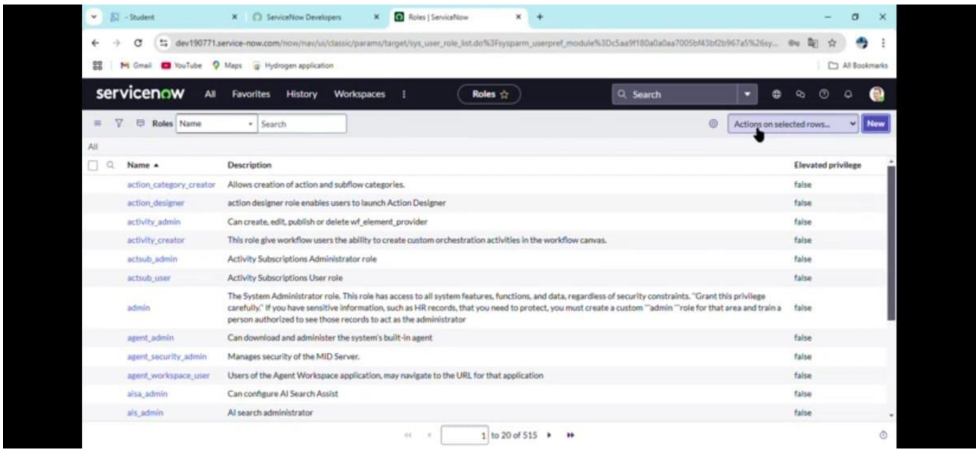


To set up the User's password, save the record and then click Set Password.

User ID: EmployeeManagement
First name: Employee
Last name: Management
Title:
Department:
Password needs reset ☐
Locked out ☐
Active ☑
Web service access only ☐
Internal Integration User ☐

Email:
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...

Step 9: Open Role >>New



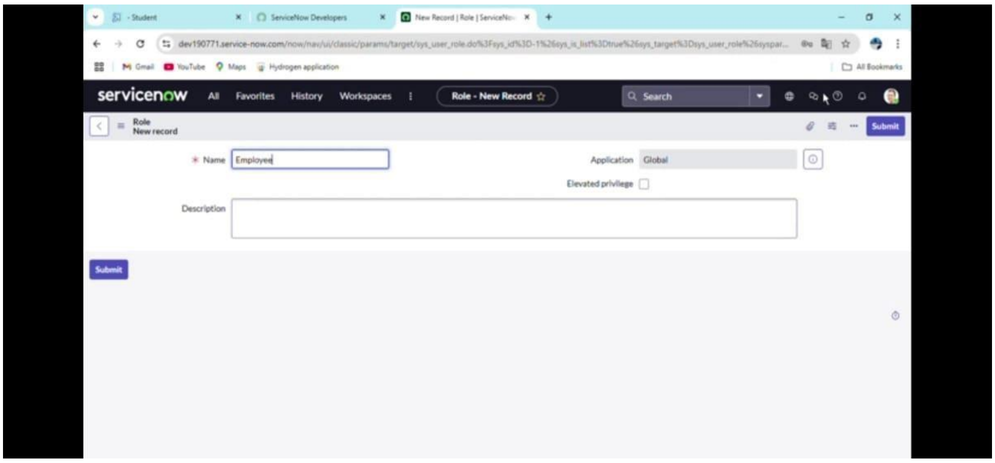
Roles

All

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 wf_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 URL for that application	false
aisa_admin	Can configure AI Search Assist	false
ais_admin	AI search administrator	false

1 to 20 of 515

Step 10: Create Employee Role

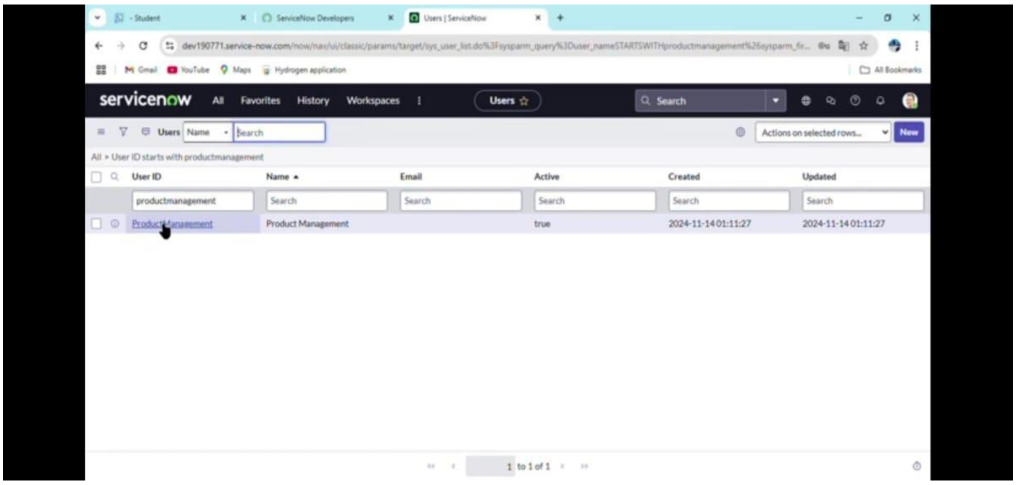


Role
New record

* Name	Employee
Application	Global
Elevated privilege	□
Description	

Step 11: In All>>Users>>Search Product Management

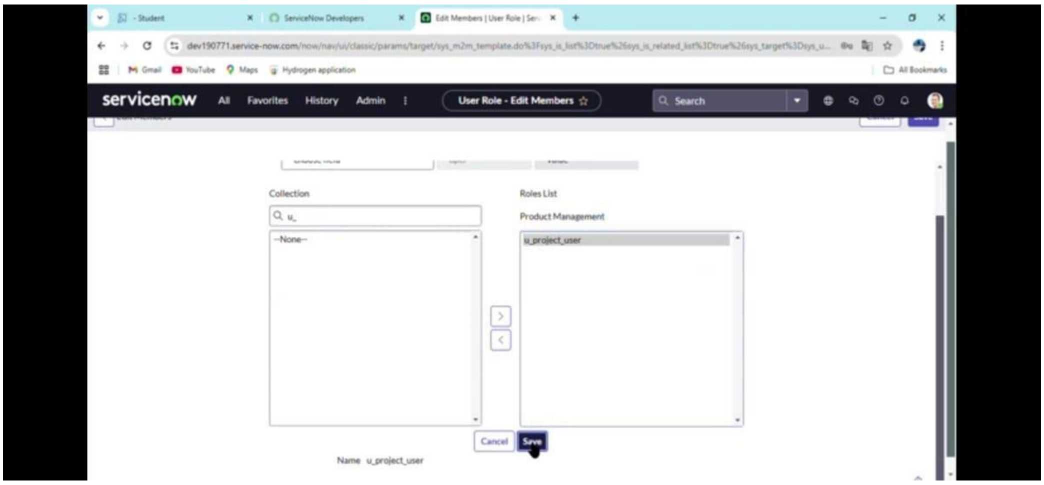
And add Role to it



All > User ID starts with productmanagement

User ID	Name ▲	Email	Active	Created	Updated
productmanagement					
ProductManagement	Product Management		true	2024-11-14 01:11:27	2024-11-14 01:11:27

1 to 1 of 1



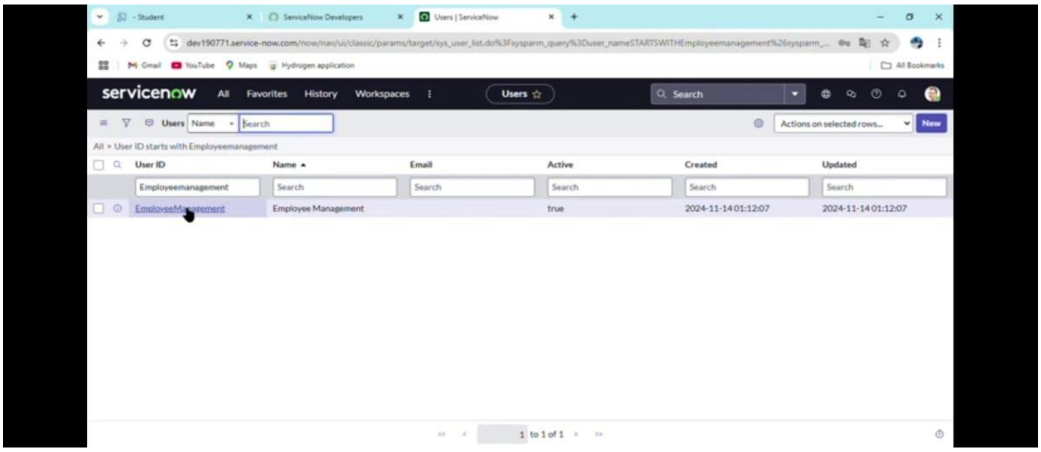
Collection: u_ — --None--

Roles List: u_project_user

Name u_project_user

Step 12: In All>>Users>>Search EmployeeManagement

And add Role to it

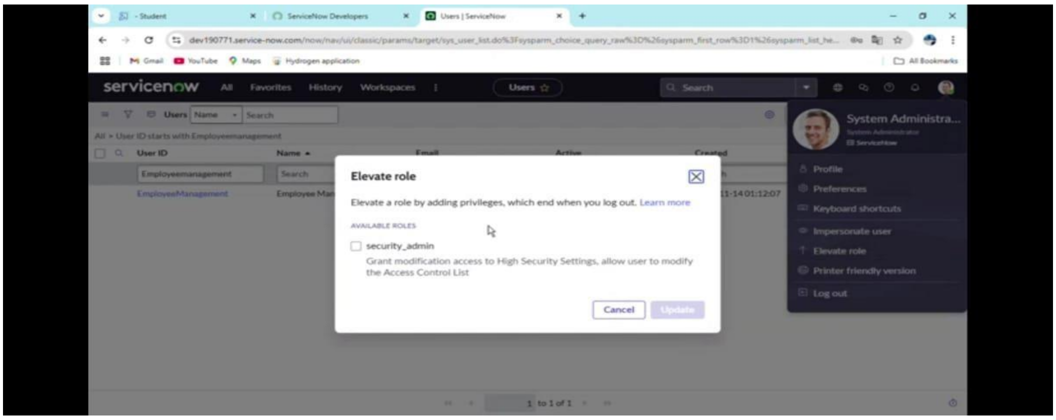


All > User ID starts with Employeemanagement

User ID	Name ▲	Email	Active	Created	Updated
Employeemanagement	Search	Search	Search	Search	Search
EmployeeManagement	Employee Management		true	2024-11-14 01:12:07	2024-11-14 01:12:07

Step 13: Click on the Profile avatar >> Elevate Role

>> Grant the high security



Elevate role

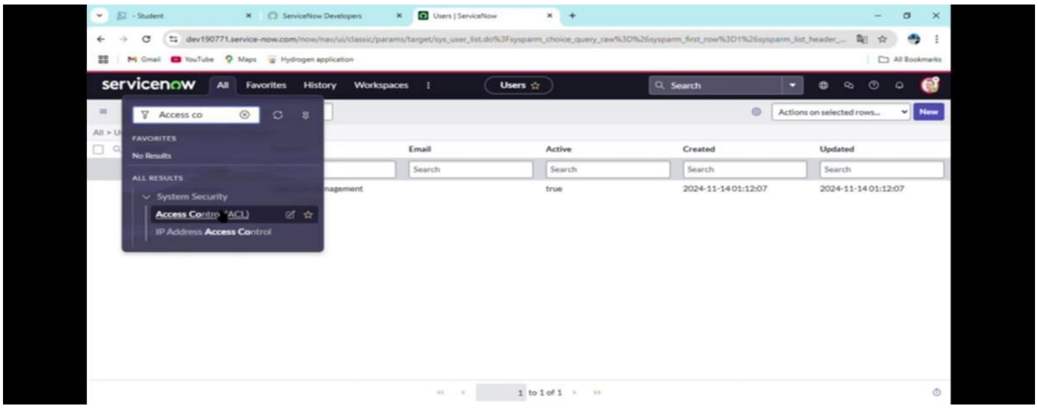
Elevate a role by adding privileges, which end when you log out. Learn more

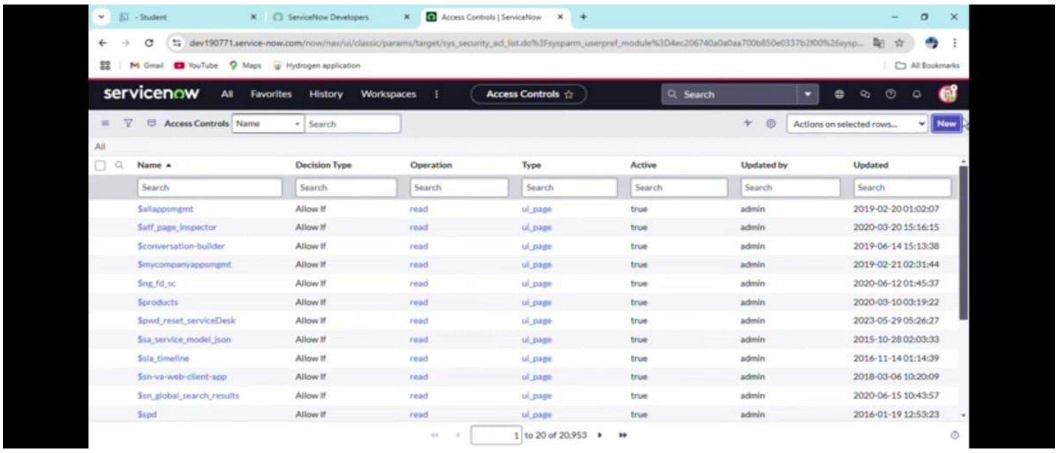
AVAILABLE ROLES

□ security_admin

Grant modification access to High Security Settings, allow user to modify the Access Control List

Step 14: In All>> Search & Open ACL >> New

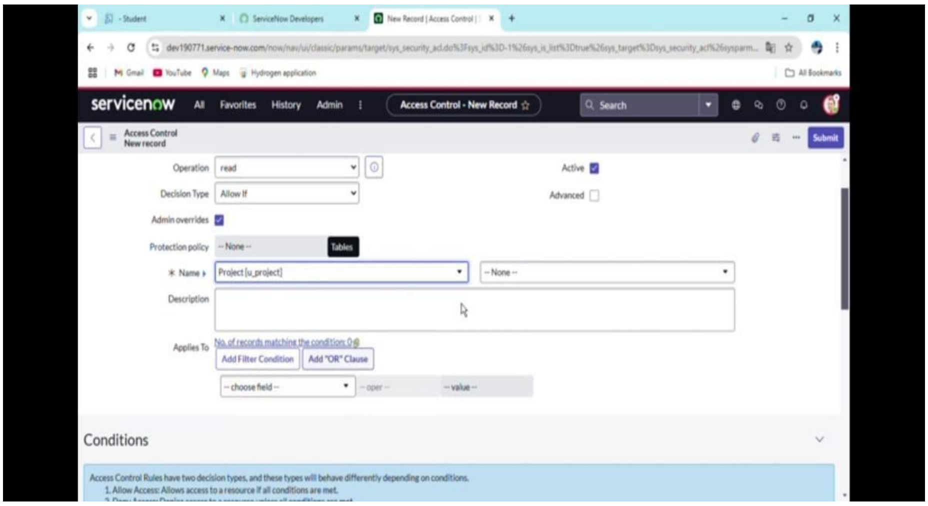




Name ▲	Decision Type	Operation	Type	Active	Updated by	Updated
$allappsmgmt	Allow If	read	ui_page	true	admin	2019-02-20 01:02:07
$atf_page_inspector	Allow If	read	ui_page	true	admin	2020-03-20 15:16:15
$conversation-builder	Allow If	read	ui_page	true	admin	2019-06-14 15:13:38
$mycompanyappsmgmt	Allow If	read	ui_page	true	admin	2019-02-21 02:31:44
$ng_fd_sc	Allow If	read	ui_page	true	admin	2020-06-12 01:45:37
$products	Allow If	read	ui_page	true	admin	2020-03-10 03:19:22
$pwd_reset_serviceDesk	Allow If	read	ui_page	true	admin	2023-05-29 05:26:27
$sa_service_model_json	Allow If	read	ui_page	true	admin	2015-10-28 02:03:33
$sla_timeline	Allow If	read	ui_page	true	admin	2016-11-14 01:14:39
$sn-va-web-client-app	Allow If	read	ui_page	true	admin	2018-03-06 10:20:09
$sn_global_search_results	Allow If	read	ui_page	true	admin	2020-06-15 10:43:57
$spd	Allow If	read	ui_page	true	admin	2016-01-19 12:53:23

1 to 20 of 20,953

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

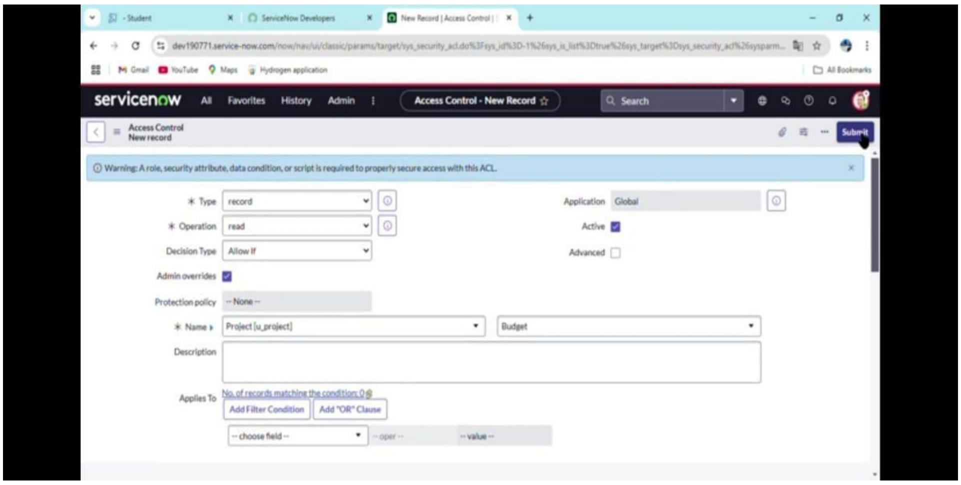


Access Control
New record

Operation: read
Decision Type: Allow If
Admin overrides: ☑
Protection policy: -- None --
Name: Project [u_project] | -- None --
Description:
Applies To: No. of records matching the condition: 0
Active: ☑
Advanced: □

Conditions

Access Control Rules have two decision types, and these types will behave differently depending on conditions.
1. Allow Access: Allows access to a resource if all conditions are met.



dev190771.service-now.com/now/nav/ui/classic/params/target/sys_security_acl.do%3Fsys_id%3D-1%26sys_is_list%3Dtrue%26sys_target%3Dsys_security_acl%26sysparm...

Access Control - New Record

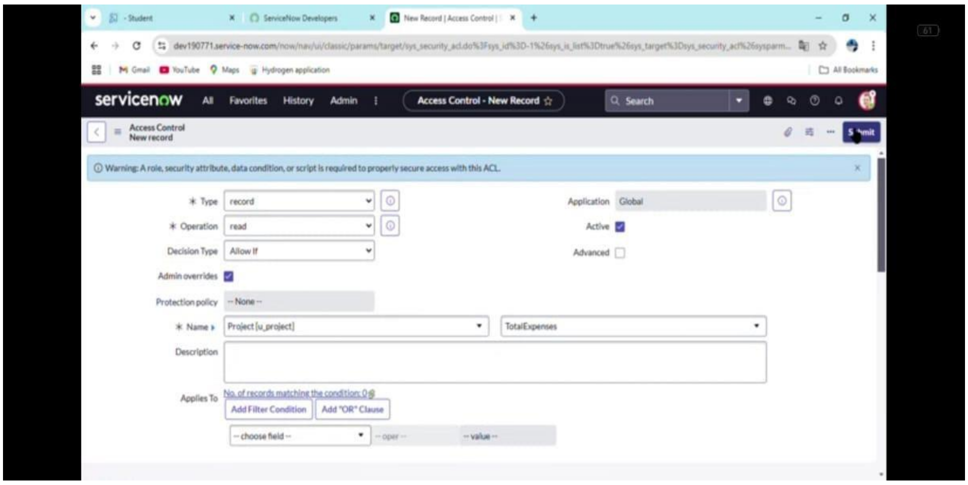
Access Control
New record

Submit

Warning: A role, security attribute, data condition, or script is required to properly secure access with this ACL.

* Type: record
* Operation: read
Decision Type: Allow If
Admin overrides: ☑
Protection policy: -- None --
* Name: Project [u_project] | Budget
Description:
Applies To: No. of records matching the condition: 0
Add Filter Condition | Add "OR" Clause
-- choose field -- | -- oper -- | -- value --

Application: Global
Active: ☑
Advanced: □



dev190771.service-now.com/now/nav/ui/classic/params/target/sys_security_acl.do%3Fsys_id%3D-1%26sys_is_list%3Dtrue%26sys_target%3Dsys_security_acl%26sysparm...

Access Control - New Record

Access Control
New record

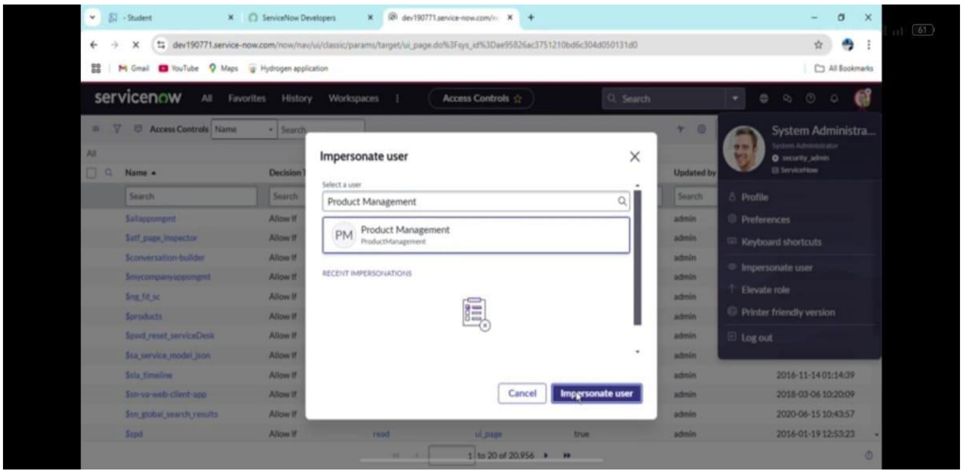
Submit

Warning: A role, security attribute, data condition, or script is required to properly secure access with this ACL.

* Type: record
* Operation: read
Decision Type: Allow If
Admin overrides: ☑
Protection policy: -- None --
* Name: Project [u_project] | TotalExpenses
Description:
Applies To: No. of records matching the condition: 0
Add Filter Condition | Add "OR" Clause
-- choose field -- | -- oper -- | -- value --

Application: Global
Active: ☑
Advanced: □

Step 16: Impersonate User >> Product Management



dev190771.service-now.com/now/nav/ui/classic/params/target/ui_page.do%3Fsys_id%3Dae95826ac3751210bd6c304d050131d0

Access Controls

Impersonate user

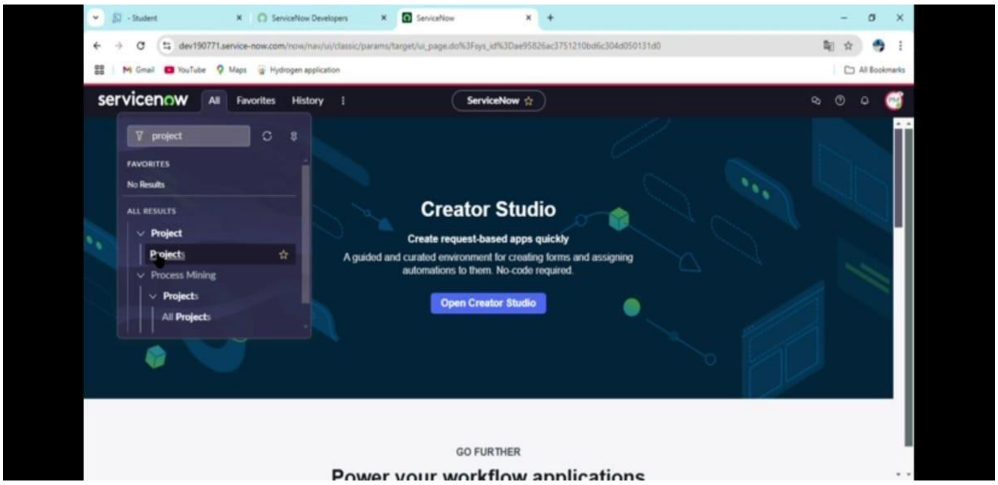
Select a user: Product Management

PM Product Management
ProductManagement

RECENT IMPERSONATIONS

Cancel | Impersonate user

Step 17: All>>Project>>New



Creator Studio

Create request-based apps quickly

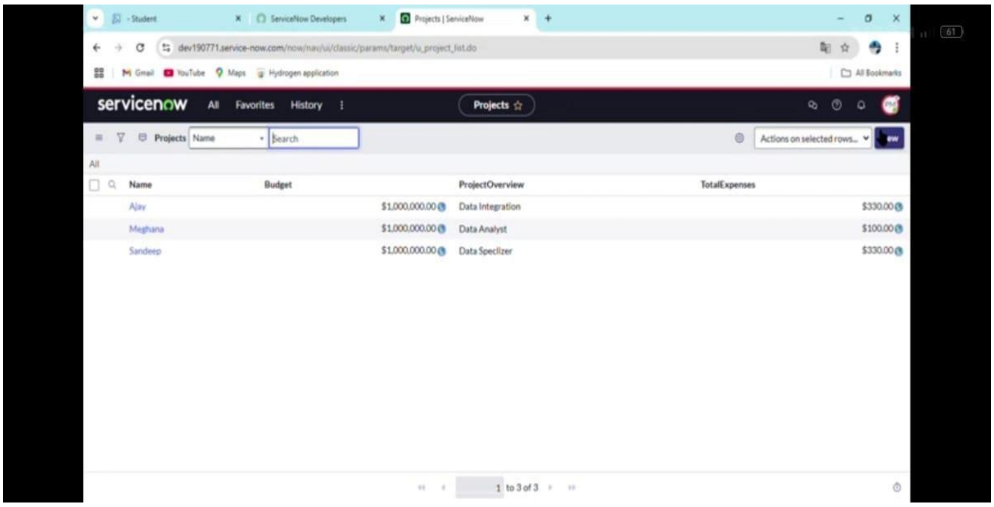
A guided and curated environment for creating forms and assigning automations to them. No-code required.

Open Creator Studio

GO FURTHER

Power your workflow applications

Step 18: Create 3 Records with any details



Name	Budget	ProjectOverview	TotalExpenses
Ajay	$1,000,000.00	Data Integration	$330.00
Meghana	$1,000,000.00	Data Analyst	$100.00
Sandeep	$1,000,000.00	Data Speclizer	$330.00

Testing and Validation:

Test User Authentication

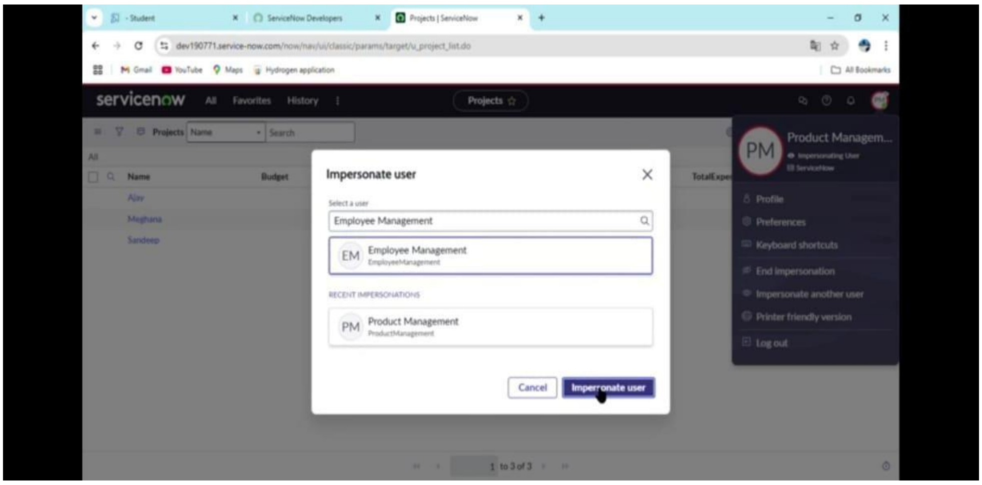
- Ensure that users can only access the project table after successful authentication (e.g., login with username and password).
- Test invalid login attempts and ensure that users cannot access the table without proper credentials.
- Verify session expiration behavior (if applicable).

Validation:

When testing and validating access control for a project table, the goal is to ensure that only authorized users can access, modify, or manage the project table data according to defined roles and permissions. Proper access control testing helps protect sensitive data and ensures that users' actions are consistent with their designated permissions**.**

Result:

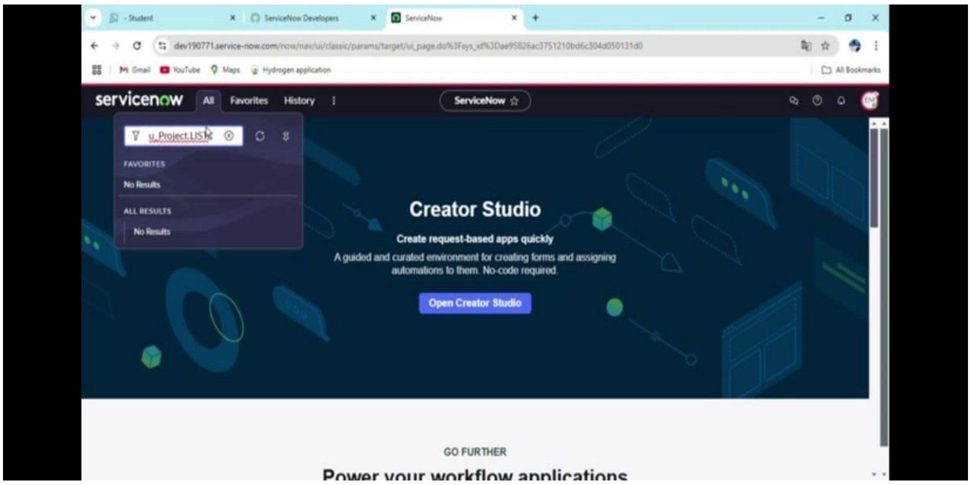
Step 1: Impersonate User >> Employee Management


dev190771.service-now.com/now/nav/ui/classic/params/target/u_project_list.do

Impersonate user

Select a user: Employee Management

Step 2: All >> u_project.LIST


dev190771.service-now.com/now/nav/ui/classic/params/target/ui_page.do%3Fsys_id%3Dae95826ac3751210bd6c304d050131d0

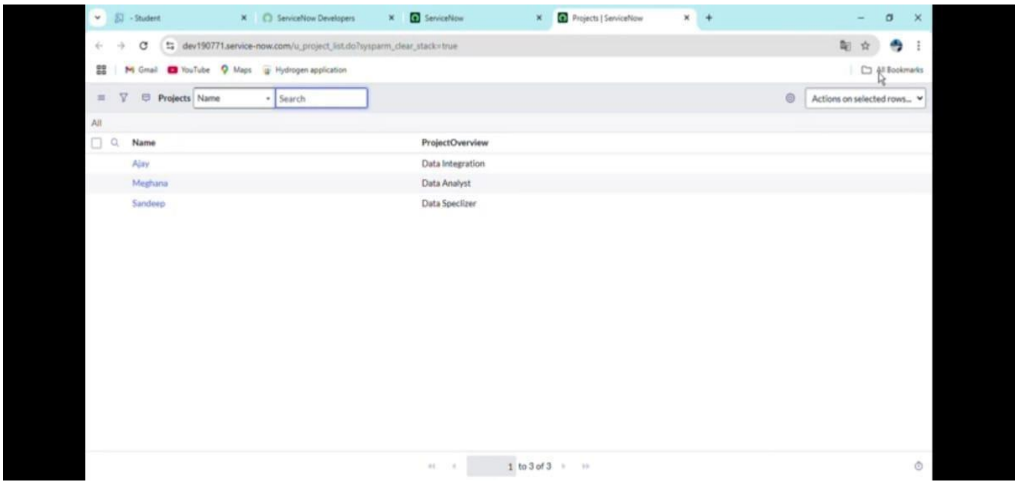
u_Project.LIST

Creator Studio

Create request-based apps quickly

A guided and curated environment for creating forms and assigning automations to them. No-code required.

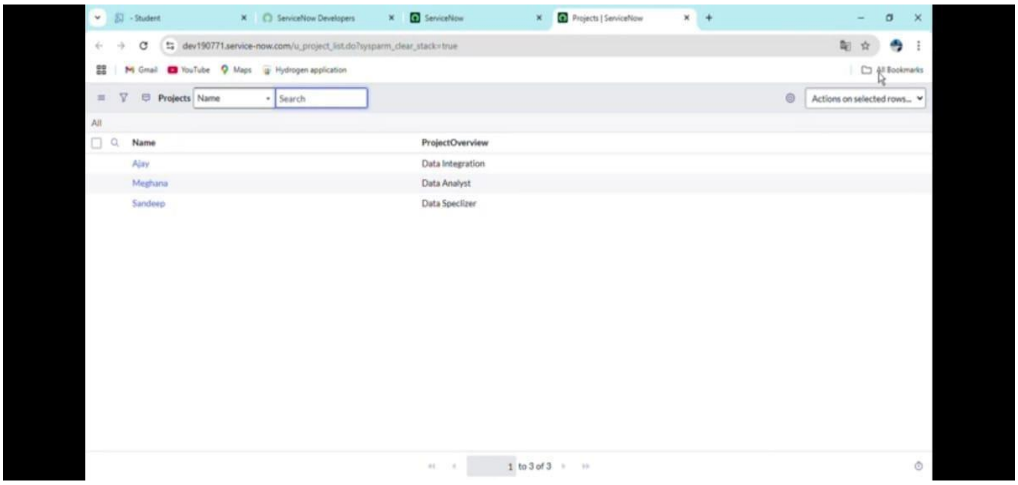
Step 3:



Name	ProjectOverview
Ajay	Data Integration
Meghana	Data Analyst
Sandeep	Data Speclizer

In the figure above, we can ensure that some fields(Budget,Total Expenses) visibility is restricted for employees on the Project table

OUTPUT:



Name	ProjectOverview
Ajay	Data Integration
Meghana	Data Analyst
Sandeep	Data Speclizer

Conclusion: Implementing access control for a project table ensures the security, integrity, and confidentiality of project data. By assigning roles and permissions, project managers Thus The Project “Access control for project Table” has been implemented successfully