

ACCESS CONTROL FOR PROJECT TABLE

ANBU R (team leader)

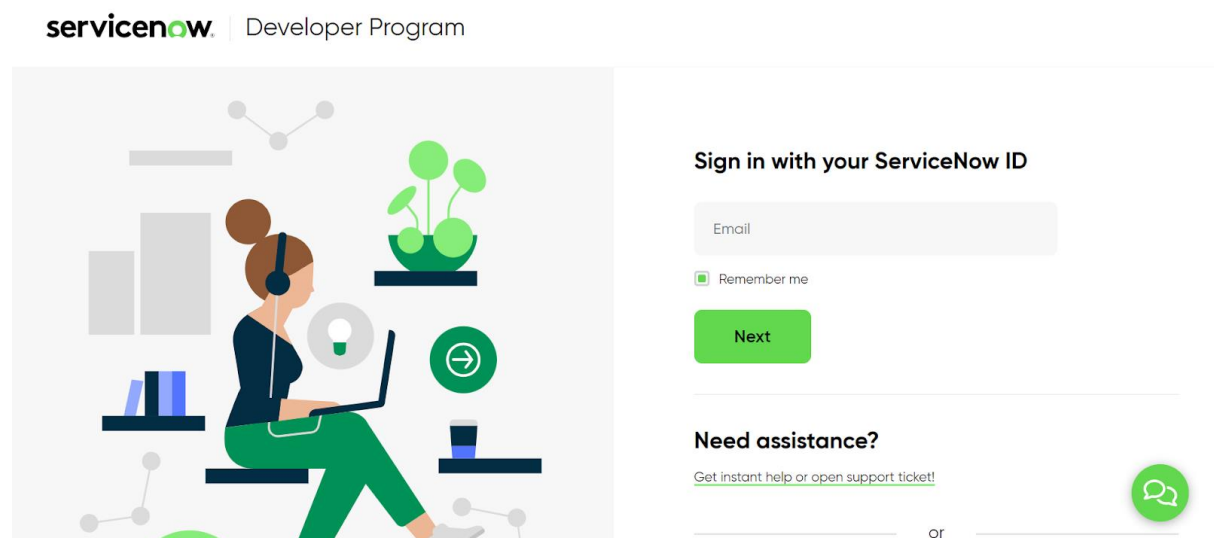
JAYASRI S

KISHORE S

SIVAKUMAR N

IMPLEMENTATION

Step 1: Sign in to ServiceNow.



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

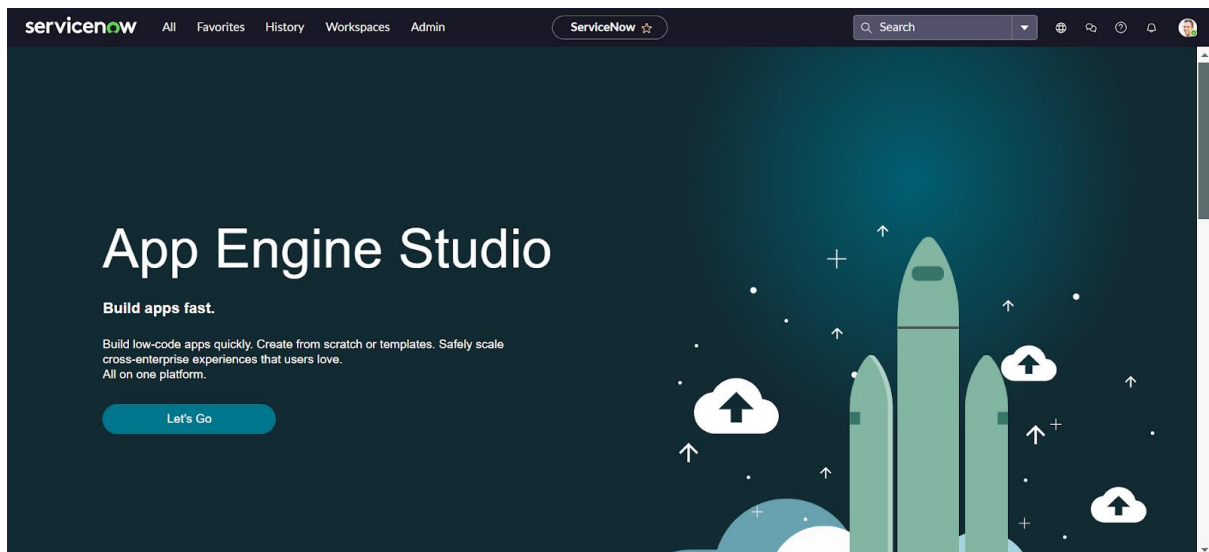
Step 3 : Once logged in, navigate to the "Personal Developer Instance" section.
Click on "Request Instance" to create a new ServiceNow instance.

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

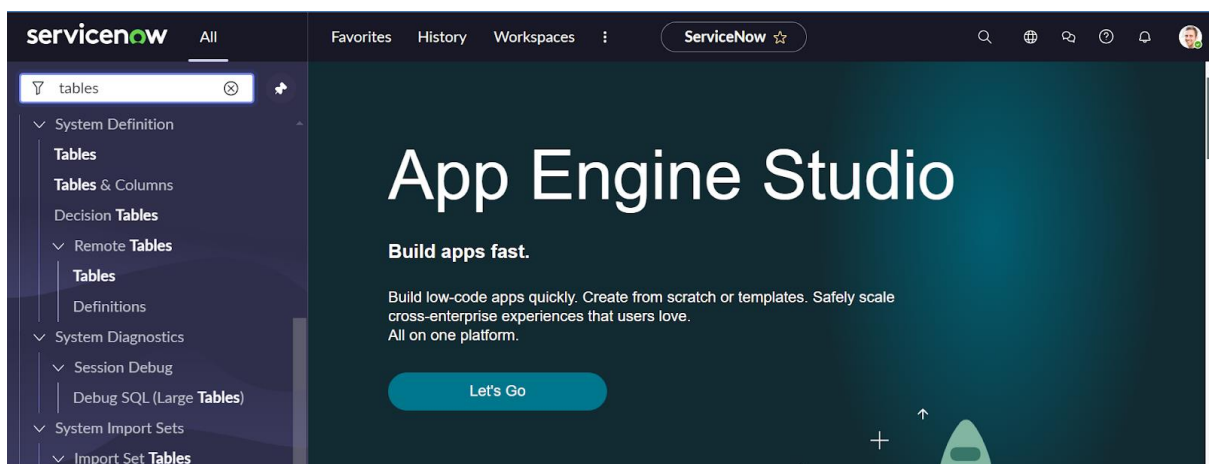
Step 5 : You'll receive an email with the instance details once it's ready.

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

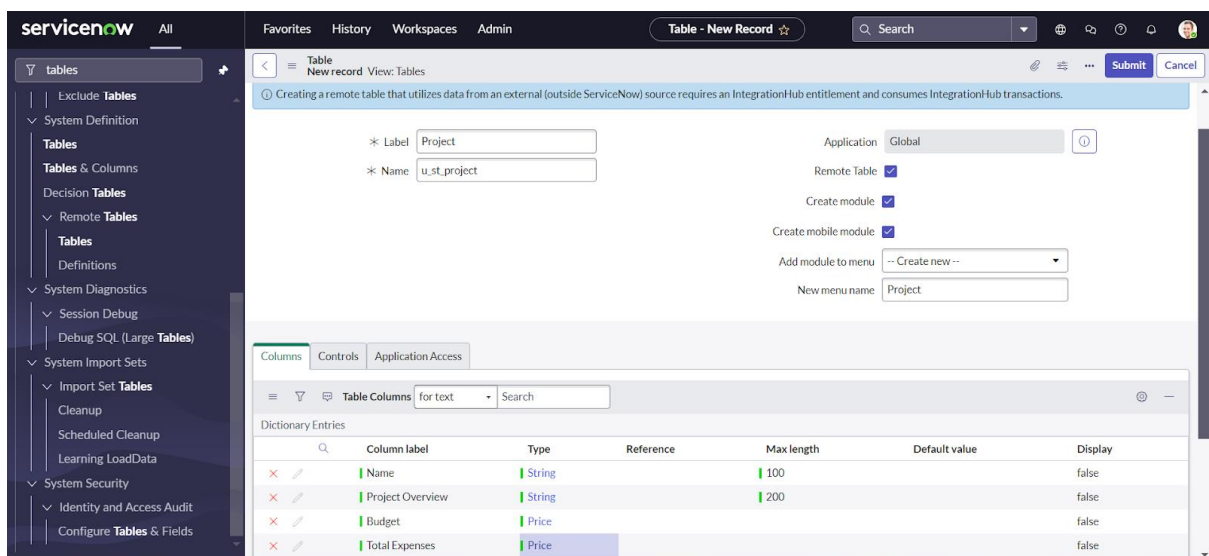
Now you will navigate to the ServiceNow.



Step 7 : Open “Tables” >> New.



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



The screenshot shows the ServiceNow 'Users' page. The left sidebar contains a navigation menu with 'Users' selected. The main content area displays a table of users with columns: User ID, Name, Email, Active, Created, and Updated. The table lists various users including Sandeep Gujja, admin, MishraSri, aes.creator, eddie.gauer, bmscheduler, problemmanager, germaine.bruski, rebekah.lindboe, steve.schorr, darrel.ruffins, judi.kivel, lina.hybarger, pat.hoshaw, ATF.User, and article.alp.

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
MishraSri	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
bmscheduler	Benchmark Scheduler		true	2017-02-24 12:14:31	2024-03-18 21:38:30
problemmanager	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.

The screenshot shows the ServiceNow 'Users' page after creating two new users. The table now includes 'Employee Management' and 'Product Management' at the top, followed by the existing users. The 'Email' column for the new users is empty.

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
MishraSri	Mishra Sri	Mishra6@gmail.com	true

Step 11 : Open Role >>New

The screenshot shows the ServiceNow 'Roles' page. The left sidebar has 'Roles' selected. The main content area displays a table of roles with columns: Name, Description, and Elevated privilege. The table lists various roles including action_category_creator, action_designer, activity_admin, activity_creator, actsub_admin, actsub_user, admin, agent_admin, agent_security_admin, and agent_workspace.user.

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 wif_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 'User - Product Management' configuration page in ServiceNow. The left sidebar contains a navigation menu with categories like System Logs, System Security, Users and Groups, Reports, System User Guide, and User Administration. The main content area includes fields for User ID (Product Management), First name (Product), Last name (Management), Title, and Department. There are also checkboxes for 'Password needs reset', 'Locked out', 'Active' (checked), 'Web service access only', and 'Internal Integration User'. On the right, there are fields for Email, Language, Calendar integration, Time zone, Date format, Business phone, and Mobile phone. Below these fields are buttons for 'Update', 'Set Password', and 'Delete'. A 'Related Links' section provides links for 'View linked accounts', 'View Subscriptions', and 'Reset a password'. At the bottom, there is a table titled 'Entitled Custom Tables' with a tab for 'Roles (1)'. The table has columns for Role, State, Inherited, and Inheritance Count. The data row shows 'u_project_user' with State 'Active', Inherited 'false', and Inheritance Count '1'.

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

The screenshot shows the 'User - Employee Management' configuration page in ServiceNow. The layout is similar to the previous screenshot, with fields for User ID (Employee Management), First name (Employee), Last name (Management), Title, and Department. The 'Active' checkbox is checked. The 'Related Links' section is present. The 'Entitled Custom Tables' table at the bottom shows a single row for 'Employee' with State 'Active', Inherited 'false', and Inheritance Count '1'.

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

The screenshot shows the 'Access Controls' interface in ServiceNow. The left sidebar has a navigation menu with categories like Configuration, Application Servers, Database Servers, Database Instances, Database Catalogs, System Properties, System Security, and Access Control (ACL). The main content area displays a table of access control records. The table has columns for Name, Operation, Type, Active, and Updated by. The data rows include various roles like 'u_st_project' and 'u_project' with operations like 'read', 'write', 'delete', and 'create'. On the right, there is a user profile sidebar for 'System Administrator' with options like Profile, Preferences, Keyboard shortcuts, Impersonate user, Elevate role, Printer friendly version, and Log out.

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 21:33:03
u_overview	create	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.

Access Control
u_project

* Type: record

* Operation: read

Application: Global

Active: ☒

Admin overrides: ☒

Protection policy: -- None --

* Name: project[u_project]

Description:

Condition: 3 records match condition

Conditions:

Role
Employee

Local or Existing: ☐ Existing ☒ Local

Condition: All of these conditions must be met

-- choose field --

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

Access Control - New ...

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.

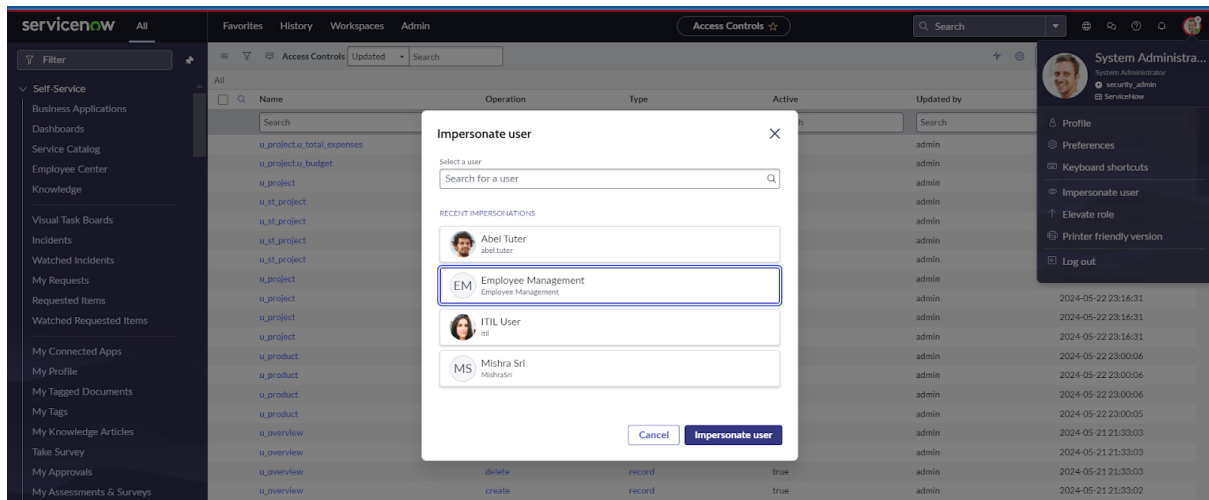
Step 19 : All >> Project >> New(We can see that the product Manager has all the CRWD access).

Step 20 : Create 3 Records with any details .

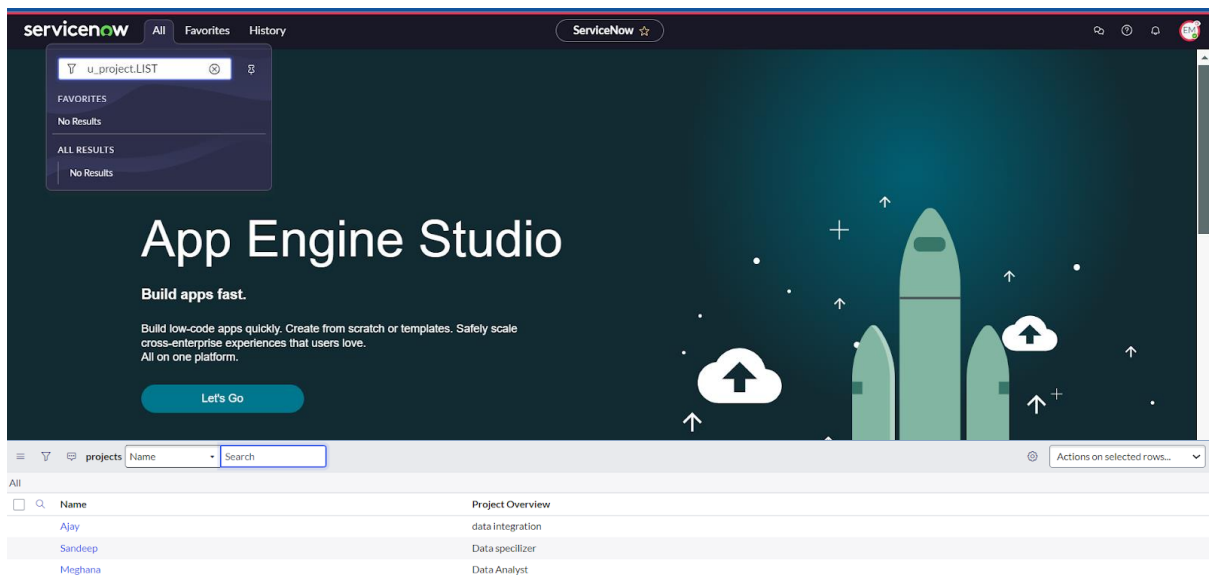
Name	Budget	Project Overview	Total Expenses
Ajay	\$330.00	data integration	\$1,000,000.00
Sandeep	\$220.00	Data specilizer	\$1,000,000.00
Meghana	\$100.00	Data Analyst	\$1,000,000.00

RESULT

Step 1 : Impersonate User >> Employee Management.



Step 2 : All >> u_project.LIST.



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