



PIE Tech

POLLACHI INSTITUTE OF ENGINEERING AND TECHNOLOGY

(Approved by AICTE and Affiliated to Anna University)

sky is the limit

Naan Mudhalvan

ServiceNow Administrator

Access Control for Project table

NAME : Dhanush M

Register.No : 723621104012

Year : IV

Semester : 07

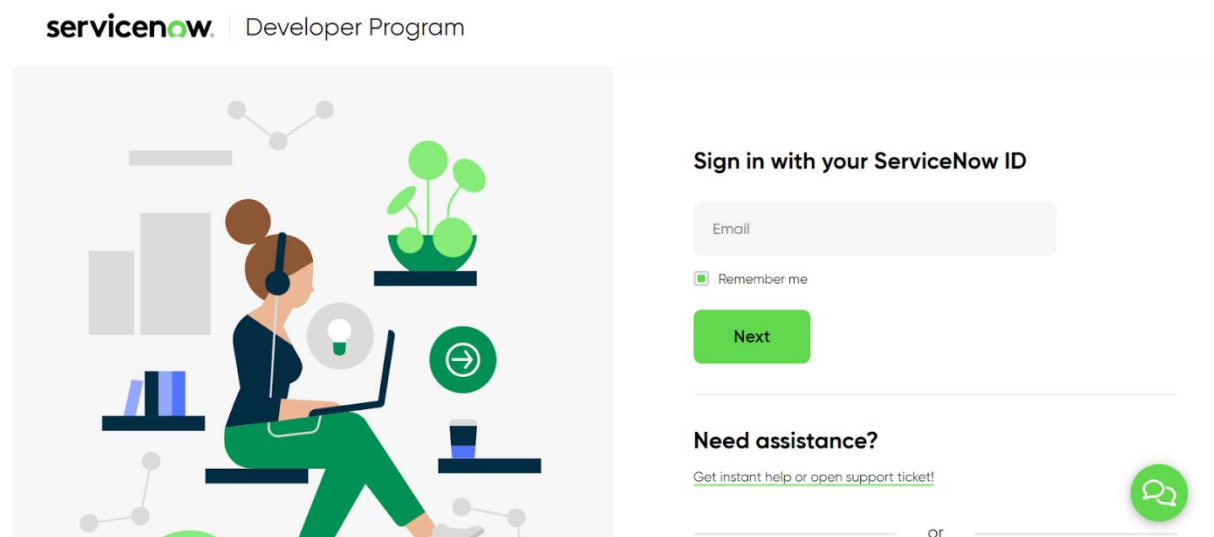
Access control for Project Table

Abstraction:

- **Access Control for the Project table in ServiceNow involves configuring security mechanisms that govern who can view, create, modify, or delete records within the Project table.**
- **By defining Access Control Rules (ACLs), administrators ensure that sensitive project data is only accessible to authorized users based on roles, permissions, or specific conditions.**
- **These access controls help enforce organizational policies, maintain data privacy, and support compliance requirements. Through appropriate ACL configurations, the system can differentiate between various user groups—such as project managers, team members, and executives—and grant them the right level of access to project-related information.**

Instructions:

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.

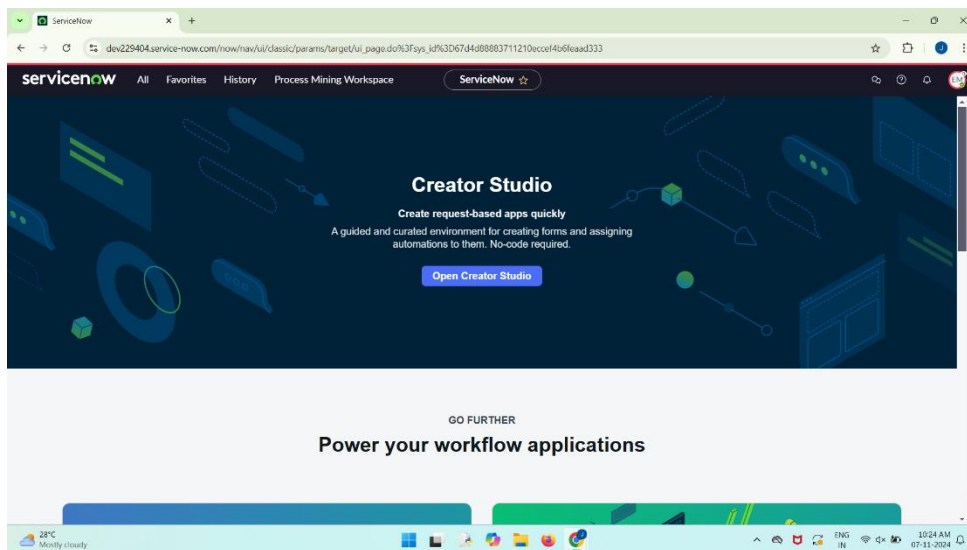
Click on "Request Instance" to create a new ServiceNow instance.

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

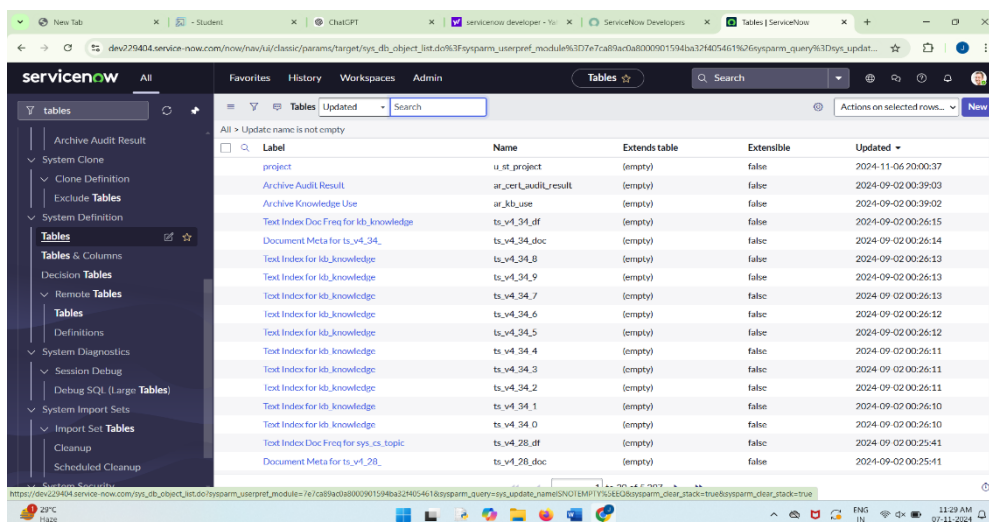
Step 5 :You'll receive an email with the instance details once it's ready.

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.

Creating a remote table that utilizes data from an external (outside ServiceNow) source requires an IntegrationHub entitlement and consumes IntegrationHub transactions.

* Label: Project
 * Name: u_st_project

Application: Global
 Remote Table: ☒
 Create module: ☒
 Add module to menu: -- Create new --
 New menu name: Project

Table Columns for text

Column label	Type	Reference	Max length	Default value	Display
Name	String		100		false
Project Overview	String		200		false
Budget	Price				false
Total Expenses	Price				false

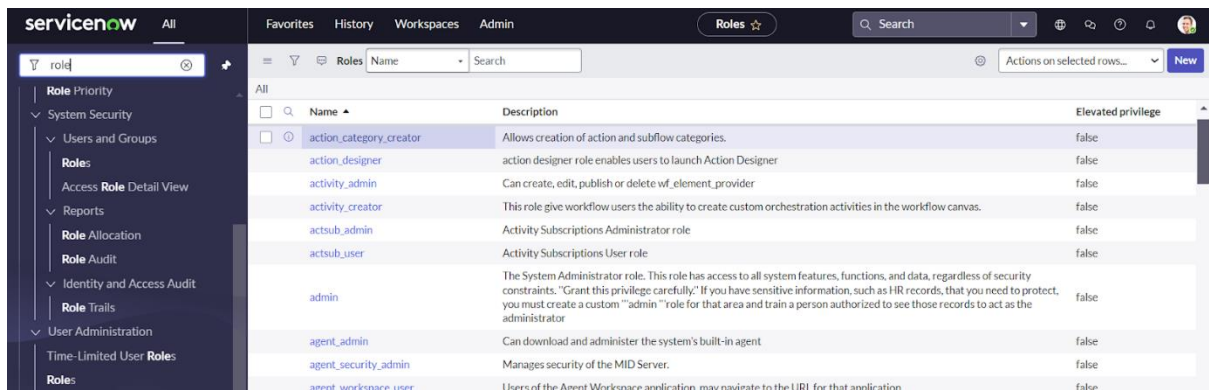
User ID	Name	Email	Active	Created	Updated
Sandeep Gujja	Sandeep Gujja	sandeepgujja999@gmail.com	true	2024-04-17 03:14:58	2024-04-17 03:14:58
admin	System Administrator	admin@example.com	true	2007-07-03 11:48:47	2024-04-17 02:44:15
MishraSri	Mishra Sri	Mishra6@gmail.com	true	2024-04-17 02:26:10	2024-04-17 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
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
Search	Search	Search	Search
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



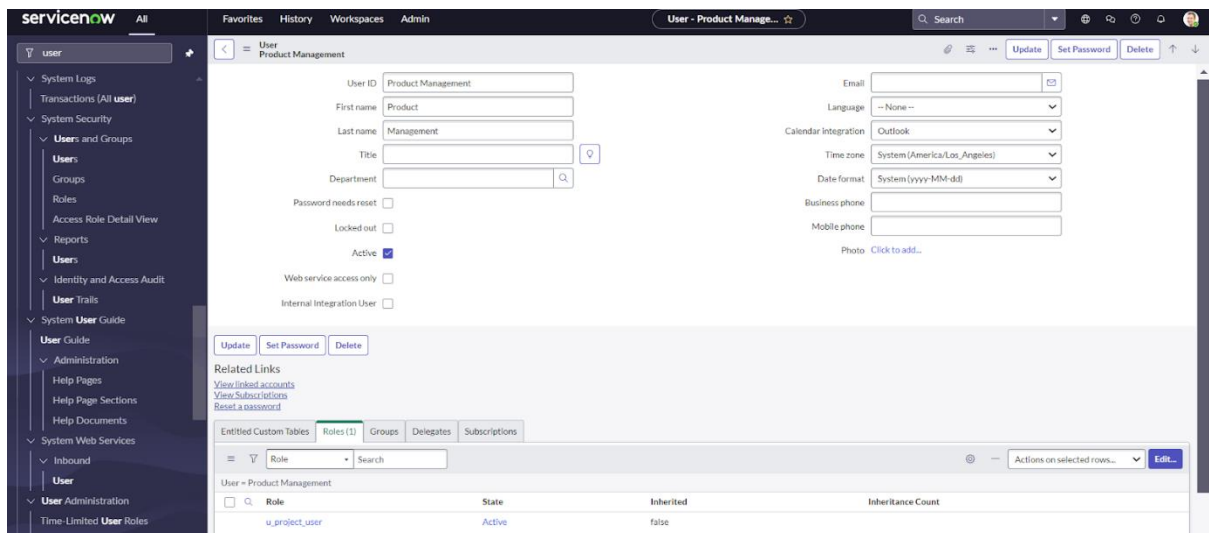
The screenshot shows the ServiceNow 'Roles' page. The left sidebar contains a navigation menu with categories like System Security, Users and Groups, Reports, Role Allocation, Role Audit, Identity and Access Audit, Role Trails, User Administration, and Time-Limited User Roles. The main content area displays a table of roles with columns for Name, Description, and Elevated privilege. The 'action_category_creator' role is selected.

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 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.

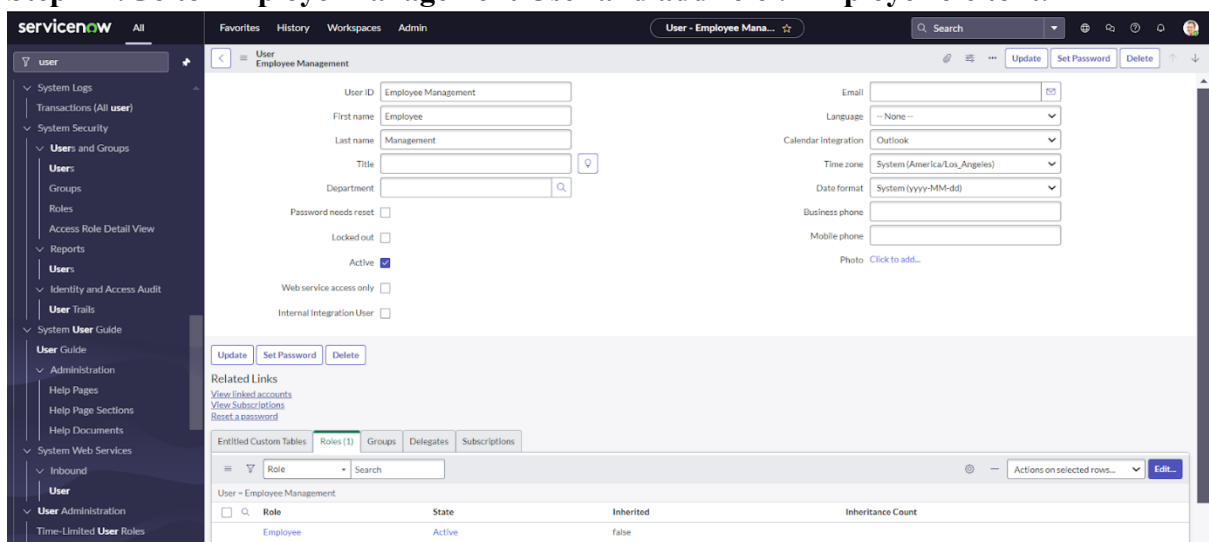
Go to Product Management User and add role : u_project_user to it.



The screenshot shows the 'User - Product Management' form in ServiceNow. The form includes fields for User ID, First name, Last name, Title, Department, Password needs reset, Locked out, Active, Web service access only, Internal Integration User, Email, Language, Calendar integration, Time zone, Date format, Business phone, and Mobile phone. Below the form is a table showing the roles assigned to the user.

Role	State	Inherited	Inheritance Count
u_project_user	Active	false	

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



The screenshot shows the 'User - Employee Management' form in ServiceNow. The form includes fields for User ID, First name, Last name, Title, Department, Password needs reset, Locked out, Active, Web service access only, Internal Integration User, Email, Language, Calendar integration, Time zone, Date format, Business phone, and Mobile phone. Below the form is a table showing the roles assigned to the user.

Role	State	Inherited	Inheritance Count
Employee	Active	false	

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

The screenshot shows the ServiceNow Access Controls interface. On the right, the user profile for 'System Administrator' is visible. The 'Elevate role' option is highlighted in the profile menu. The main table lists access control records with columns: Name, Operation, Type, Active, and Updated by. The table contains several records for 'u_st_project' and 'u_project' with operations like read, write, delete, and create.

Name	Operation	Type	Active	Updated by
u_st_project	read	record	true	admin
u_st_project	write	record	true	admin
u_st_project	delete	record	true	admin
u_st_project	create	record	true	admin
u_project	write	record	true	admin
u_project	create	record	true	admin
u_project	delete	record	true	admin
u_project	read	record	true	admin
u_product	write	record	true	admin
u_product	read	record	true	admin
u_product	delete	record	true	admin
u_product	create	record	true	admin
u_overview	write	record	true	admin
u_overview	delete	record	true	admin

Step 14 :Search & Open ACL >> New.

The screenshot shows the ServiceNow Access Controls interface. The 'New' button is visible in the top right corner of the table. The table lists access control records with columns: Name, Operation, Type, Active, Updated by, and Updated. The table contains several records for 'u_project' and 'u_product' with operations like write, create, delete, and read.

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	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.

The screenshot shows the ServiceNow Access Controls 'New' form. The form is configured with the following details:

- * Type: record
- * Operation: read
- Application: Global
- Active: ☒
- Advanced: ☐
- Admin overrides: ☒
- Protection policy: -- None --
- * Name: project [u_project]
- Description: (empty)
- Condition: 3 records match condition
- Conditions table: (empty)
- Local or Existing: ☒ Existing
- Condition: All of these conditions must be met

Role
Employee

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.

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

ScreenShots:

Pic 1:

User ID	Name	Email	Active	Created	Updated
(empty)	Product Management		true	2024-11-06 20:32:57	2024-11-06 20:32:57
(empty)	Employee Management		true	2024-11-06 20:09:43	2024-11-06 20:09:43
admin	System Administrator	admin@example.com	true	2007-07-03 11:48:47	2024-11-05 20:29:33
anscreator	Creator User		true	2024-11-05 17:53:39	2024-11-05 20:29:33
jade.erlebach	Jade Erlebach	jade.erlebach@example.com	true	2012-02-17 19:04:51	2024-11-05 17:37:32
veronica.resendes	Veronica Resendes	veronica.resendes@example.com	true	2012-02-17 19:04:51	2024-11-05 17:37:32
arya.hajarha	Arya Hajarha	arya.hajarha@example.com	true	2024-09-01 09:32:04	2024-11-05 17:37:32
certification.admin	Certification Admin	certification.admin@example.com	true	2012-02-17 19:04:51	2024-11-05 17:37:32
reginald.lunan	Reginald Lunan	reginald.lunan@example.com	true	2012-02-17 19:04:51	2024-11-05 17:37:32
virgil.chini	Virgil Chini	virgil.chini@example.com	true	2012-02-17 19:04:51	2024-11-05 17:37:32
robin.groiz	Robin Groiz	robin.groiz@example.com	true	2012-02-17 19:04:51	2024-11-05 17:37:32
sherwood.deliller	Sherwood Deliller	sherwood.deliller@example.com	true	2012-02-17 19:04:51	2024-11-05 17:37:32
denise.sammah	Denise Sammah	denise.sammah@example.com	true	2012-02-17 19:04:51	2024-11-05 17:37:32
mayme.sachs	Mayme Sachs	mayme.sachs@example.com	true	2012-02-17 19:04:51	2024-11-05 17:37:32
scorbycenteruser	Scorby Center Data Collection User		true	2024-09-01 23:44:20	2024-11-05 17:37:32
wes.fortanella	Wes Fortanella	wes.fortanella@example.com	true	2012-02-17 19:04:52	2024-11-05 17:37:32

Pic 2:

Label	Name	Extends table	Extensible	Updated
project	u st project	(empty)	false	2024-11-06 20:00:57
Archive Audit Result	ar_cert_audit_result	(empty)	false	2024-09-02 00:39:03
Archive Knowledge Use	ar_kb_use	(empty)	false	2024-09-02 00:39:02
Text Index Doc Freq for kb_knowledge	ts_v4_34_df	(empty)	false	2024-09-02 00:26:15
Document Meta for ts_v4_34	ts_v4_34_doc	(empty)	false	2024-09-02 00:26:14
Text Index for kb_knowledge	ts_v4_34_1	(empty)	false	2024-09-02 00:26:13
Text Index for kb_knowledge	ts_v4_34_2	(empty)	false	2024-09-02 00:26:13
Text Index for kb_knowledge	ts_v4_34_3	(empty)	false	2024-09-02 00:26:13
Text Index for kb_knowledge	ts_v4_34_4	(empty)	false	2024-09-02 00:26:12
Text Index for kb_knowledge	ts_v4_34_5	(empty)	false	2024-09-02 00:26:12
Text Index for kb_knowledge	ts_v4_34_6	(empty)	false	2024-09-02 00:26:11
Text Index for kb_knowledge	ts_v4_34_7	(empty)	false	2024-09-02 00:26:11
Text Index for kb_knowledge	ts_v4_34_8	(empty)	false	2024-09-02 00:26:11
Text Index for kb_knowledge	ts_v4_34_9	(empty)	false	2024-09-02 00:26:10
Text Index for kb_knowledge	ts_v4_34_10	(empty)	false	2024-09-02 00:26:10
Text Index Doc Freq for sys_cs_topic	ts_v4_28_df	(empty)	false	2024-09-02 00:25:41
Document Meta for ts_v4_28	ts_v4_28_doc	(empty)	false	2024-09-02 00:25:41

Pic 3:

Label	Name	Extends table	Extensible	Updated
project	u st project	(empty)	false	2024-09-02 00:26:12
Archive Audit Result	ar_cert_audit_result	(empty)	false	2024-09-02 00:26:11
Archive Knowledge Use	ar_kb_use	(empty)	false	2024-09-02 00:26:11
Text Index Doc Freq for kb_knowledge	ts_v4_34_df	(empty)	false	2024-09-02 00:26:11
Document Meta for ts_v4_34	ts_v4_34_doc	(empty)	false	2024-09-02 00:26:10
Text Index for kb_knowledge	ts_v4_34_1	(empty)	false	2024-09-02 00:26:10
Text Index for kb_knowledge	ts_v4_34_2	(empty)	false	2024-09-02 00:26:10
Text Index for kb_knowledge	ts_v4_34_3	(empty)	false	2024-09-02 00:26:10
Text Index for kb_knowledge	ts_v4_34_4	(empty)	false	2024-09-02 00:26:10
Text Index for kb_knowledge	ts_v4_34_5	(empty)	false	2024-09-02 00:26:10
Text Index for kb_knowledge	ts_v4_34_6	(empty)	false	2024-09-02 00:26:10
Text Index for kb_knowledge	ts_v4_34_7	(empty)	false	2024-09-02 00:26:10
Text Index for kb_knowledge	ts_v4_34_8	(empty)	false	2024-09-02 00:26:10
Text Index for kb_knowledge	ts_v4_34_9	(empty)	false	2024-09-02 00:26:10
Text Index for kb_knowledge	ts_v4_34_10	(empty)	false	2024-09-02 00:26:10
Text Index Doc Freq for sys_cs_topic	ts_v4_28_df	(empty)	false	2024-09-02 00:25:41
Document Meta for ts_v4_28	ts_v4_28_doc	(empty)	false	2024-09-02 00:25:41

Elevate role

Elevate a role by adding privileges, which end when you log out. [Learn more](#)

☒ security.admin

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

Cancel Update

Result Screenshot

name	budget	project overview	total expenses
Meghana	\$100.00	Data analyst	\$100,000,000.00
ajay	\$330.00	data integration	\$100,000,000.00
Sandeep	\$220.00	Data specilizer	\$100,000,000.00

Demo Video link;

<https://drive.google.com/file/d/1cRvBHCQ5yFIGeCLSAi209RxB0wq5wFWv/view?usp=sharing>

Conclusion:

In conclusion, effective Access Control for the Project table in ServiceNow is crucial for protecting sensitive data and ensuring that only authorized users can access project records. By setting up and managing Access Control Rules (ACLs), organizations can maintain security, promote collaboration, and comply with policies. Properly configured access controls enhance project oversight, boost productivity, and minimize security risks.