Table of Contents

1. Problem Statement

In many organizations, managing users, groups, and roles across multiple systems is a complex and time-consuming task. Manual access management often leads to inconsistencies, security risks, and administrative overload. When employees join, move, or leave, access rights are rarely updated on time, resulting in unauthorized access or workflow interruptions. Traditional methods lack centralized control, audit trails, and automation, making compliance and governance difficult.

This project aims to solve these challenges by designing an optimized system that automates user provisioning, enforces role-based access control (RBAC), and streamlines approval workflows through a secure and centralized platform..

2. Abstract

This project focuses on the development of a smart access management system that simplifies and automates user, group, and role handling within an organization. The proposed system integrates access control principles and workflow automation to ensure secure, efficient, and compliant management of user privileges.

By implementing Role-Based Access Control (RBAC), the system ensures that every user receives permissions aligned with their role, reducing human errors and potential security breaches. Additionally, workflow automation allows for dynamic approvals, auditing, and real-time monitoring.

The outcome is an intelligent solution that minimizes administrative effort, enhances security, and optimizes operational efficiency in enterprise environments.

3. Introduction

Organizations today rely on digital systems that require precise and secure access control. Managing user permissions manually can cause inefficiency, data breaches, and compliance issues. As companies expand, maintaining accurate records of who can access what becomes increasingly difficult.

User, group, and role management forms the backbone of identity and access governance. Automating these processes through technology ensures that the right individuals have the right access to the right resources at the right time.

This project introduces a centralized, automated approach using RBAC principles and workflow automation to improve security, traceability, and operational productivity in access control management.

4. Objectives

The main objectives of this project are:

1. To design a centralized system for managing users, groups, and roles efficiently.
2. To implement Role-Based Access Control (RBAC) for consistent and secure permission assignment.
3. To integrate automated workflows for approvals and access modifications.
4. To minimize manual intervention and administrative workload.
5. To improve auditability, compliance, and transparency in access management.
6. To enhance overall security by reducing unauthorized or redundant access.

5. Methodology

The implementation of this project is carried out in several structured steps:

Step 1: Creating Users

- Navigate to: All → Users → New
- Create users such as Alice P and Bob P.
- Assign them specific roles and save.

Step 2: Creating Groups

- Navigate to: All → Groups → New
- Create groups:
  - Project Team
- Submit the groups.

Step 3: Creating Roles

- Navigate to: All → Roles → New
- Create roles:
  - Project Member
  - Team Member
- Assign each role to its corresponding group.

Step 4: Creating a Custom Table

- Go to: System Definition → Tables → New

- Label: Project table & Task Table 2
- Check:
  - Create Module
  - Create Mobile Module

Step 5: Assigning Users and Roles

- Assign Alice to the *project manager team* and give her *the following roles:*
  - *Project_Member*
  - *u_project_table*
  - *u_task_table*
- Assign Bob to the *Team Member team* and give him the *following roles:*
  - *Team_Member*
  - *Table_role*

Step 6: Assigning Table Access to the Applications

• While creating a table, an application and module are automatically created.

- Navigate to: Application Navigator → Search "Project Table" application.
- Click Edit Module → Assign Project_Member role.
- Search Task Table 2 → Click Edit Application.
- Assign Project_Member and Team_Member roles.

Step 7: Setting Access Controls (ACLs)

- Navigate to: System Security → Access Control (ACL)
- Create ACLs for the *Task Table.*
- Add the Team_Member role under *Requires Role.*
- Create four ACLs for the required fields.

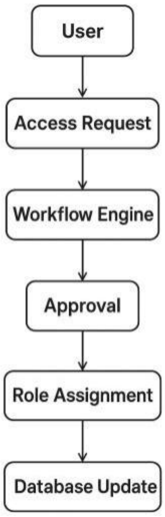
Step 8: Designing the Flow

- Navigate to: Flow Designer → New Flow
- Create a flow "Task Table"
- Trigger: When a record is created in Operations Related
- Condition: Status is: In progress AND comments is feedback AND assigned to is bob
- Action: Update record → Status completed

.

6. Architecture Diagram

Below is the workflow architecture of the automation system



Flow Explanation:

1. User submits an access request for a specific role or module.
2. The request record is stored in the Access Management table.
3. The Workflow Engine triggers automatically when a new request is created.
4. The system checks the request type and identifies the required approval path.
5. The manager or admin reviews and approves/rejects the request.
6. Once approved, the system assigns the appropriate role to the user.
7. The database is updated with the new access details.
8. A notification is sent to both the user and approver confirming the update.

7. Workflow Explanation

Manual Workflow (Before Automation):

- User requests access manually through email or form submission
- Admin reviews the request and assigns roles manually.
- Delays occur due to manual approval and communication gaps.
- High chances of errors or unauthorized access due to lack of tracking.

Automated Workflow (After Implementation):

- User submits an access request through the system.
- The Workflow Engine automatically triggers and identifies the request type.
- The approval process is routed to the respective manager or admin.

- Upon approval, the system automatically assigns roles and updates the database.
- Notifications are sent to both user and admin confirming the update.

This automation ensures faster access provisioning, reduces manual effort, and improves security and accuracy in role and access management..

8. Benefits of Automation

1. Reduced Administrative Overhead: Automated workflows eliminate repetitive manual tasks.
2. Enhanced Security: Permissions are dynamically updated based on roles, reducing unauthorized access.
3. Improved Compliance: Automatic logging and reporting support audits and regulatory requirements.
4. Time Efficiency**:** Access provisioning and revocation happen instantly after approval.
5. Scalability: The system can handle large organizations with thousands of users easily.
6. Transparency: Every access change is visible and traceable.

9. Results and Outcomes

After implementing the system, the organization can expect::

- Up to 60% reduction in access management time.
- Fewer access-related errors and security incidents.
- Improved employee onboarding and offboarding experience.
- Real-time visibility into user access and activity.
- Centralized control and unified reporting for all departments.

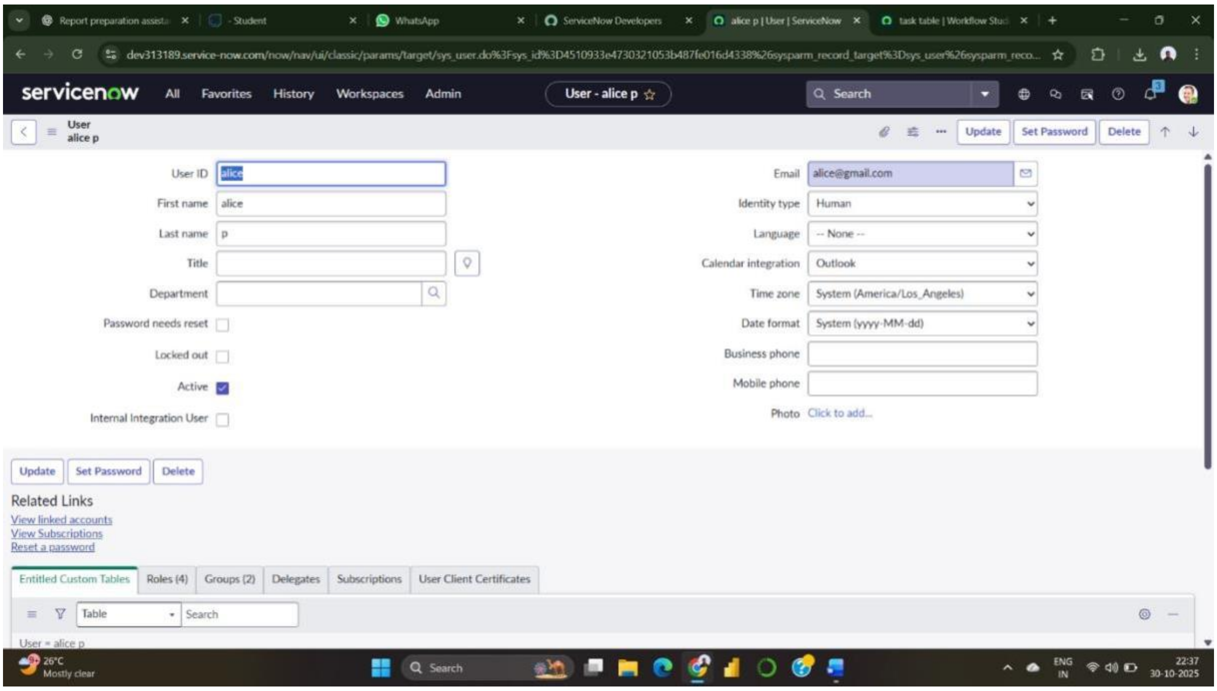
Performance testing indicates a significant improvement in efficiency compared to manual methods.

10. Future Scope

- Integrate AI to suggest appropriate access levels based on user behavior.
- Extend support for cloud services like AWS IAM, Azure AD, or Google Workspace.
- Provide mobile-based access request and approval features.
- Using immutable ledgers for enhanced transparency and tamper-proof auditing.
- Introducing dashboards with anomaly detection and usage insights.

11. Appendix

1. Create User

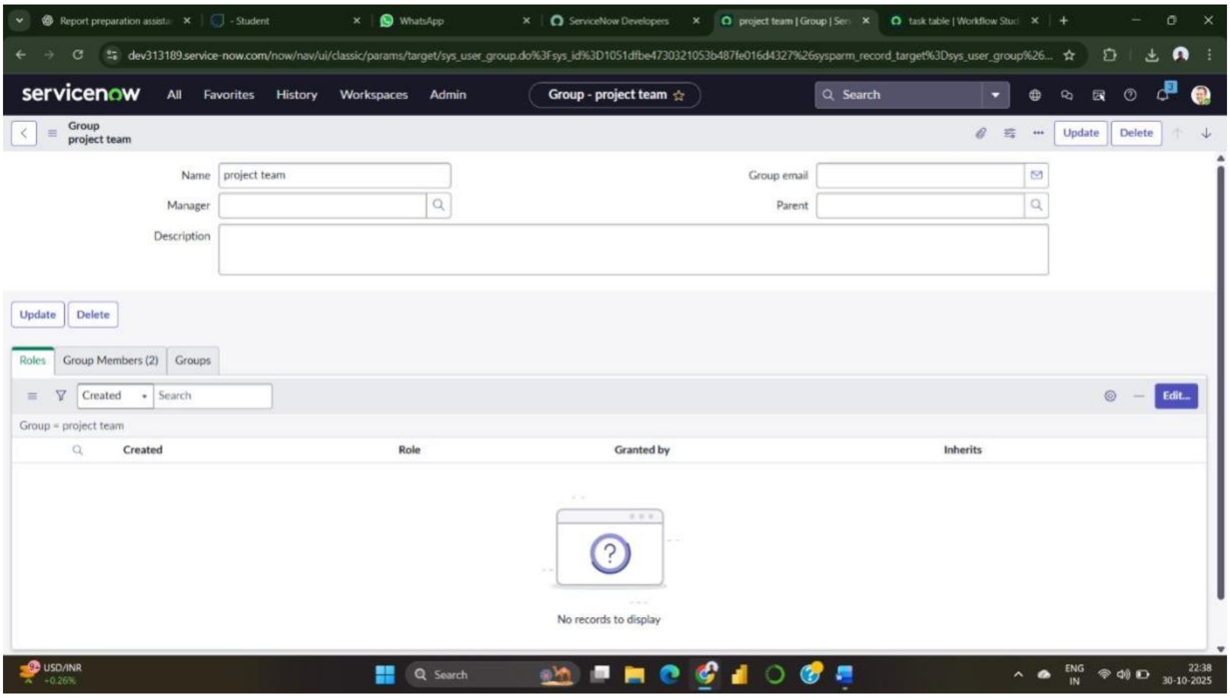


User
alice p

User ID	alice	Email	alice@gmail.com
First name	alice	Identity type	Human
Last name	p	Language	-- None --
Title		Calendar integration	Outlook
Department		Time zone	System (America/Los_Angeles)
Password needs reset	□	Date format	System (yyyy-MM-dd)
Locked out	□	Business phone	
Active	☑	Mobile phone	
Internal Integration User	□	Photo	Click to add...

User = alice p

2. Create Groups


Report preparation assista
- Student
WhatsApp
ServiceNow Developers
project team | Group | Ser
task table | Workflow Stud
dev313189.service-now.com/now/nav/ui/classic/params/target/sys_user_group.do%3Fsys_id%3D1051dfbe4730321053b487fe016d4327%26sysparm_record_target%3Dsys_user_group%26...
servicenow
All
Favorites
History
Workspaces
Admin
Group - project team
Search
Update
Delete
Roles
Group Members (2)
Groups
Created
Search
Edit...
USD/INR
+0.26%
Search
ENG
IN
22:38
30-10-2025

Group
project team

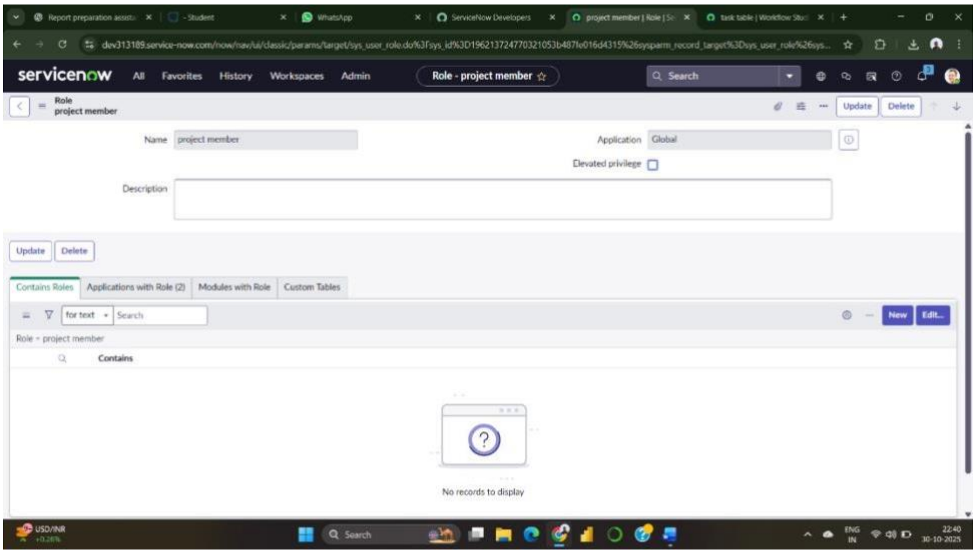
Name	project team	Group email	
Manager		Parent	
Description			

Group = project team

Created	Role	Granted by	Inherits

No records to display

3. Create Role



Name: project member

Application: Global

Elevated privilege: □

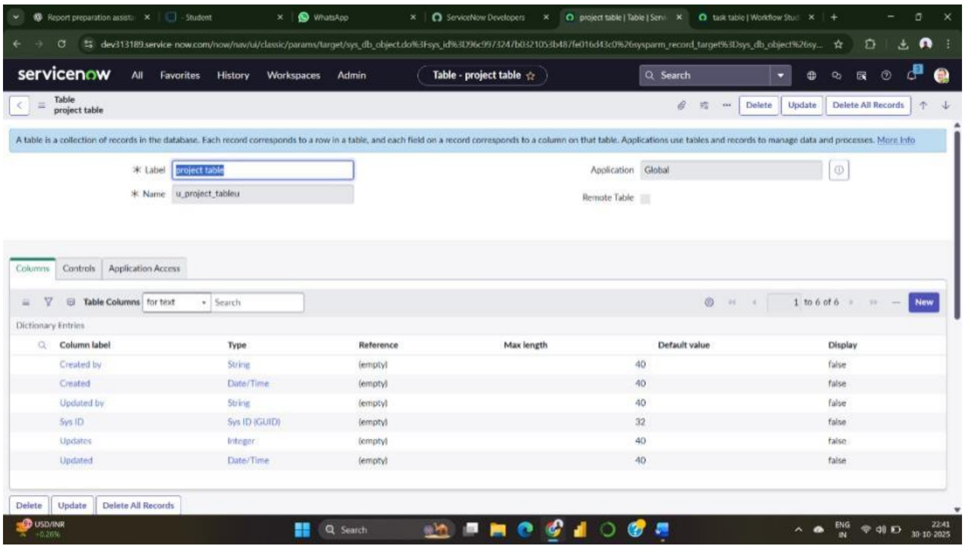
Description:

Role = project member

Contains

No records to display

4. Create a Table and Assign the operations



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 table

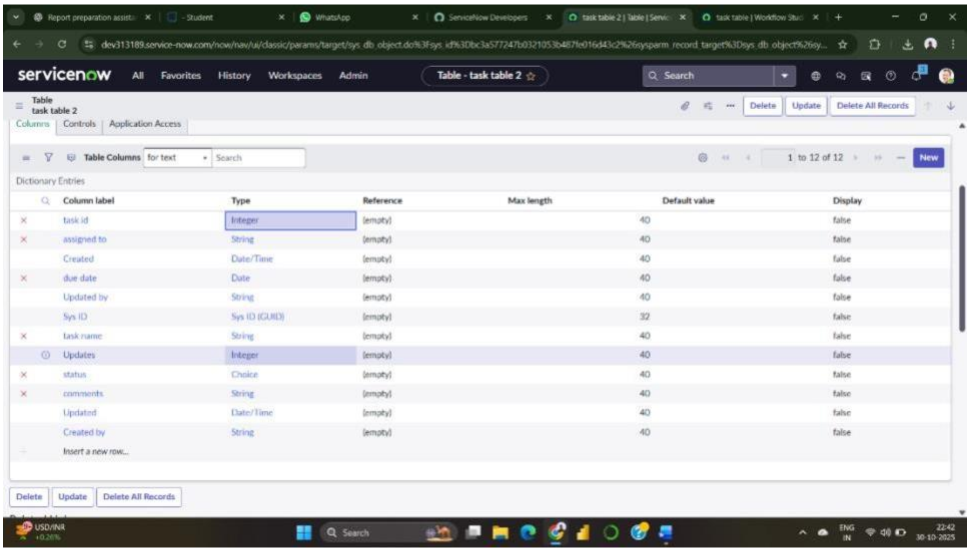
* Name: u_project_tableu

Application: Global

Remote Table: □

Dictionary Entries

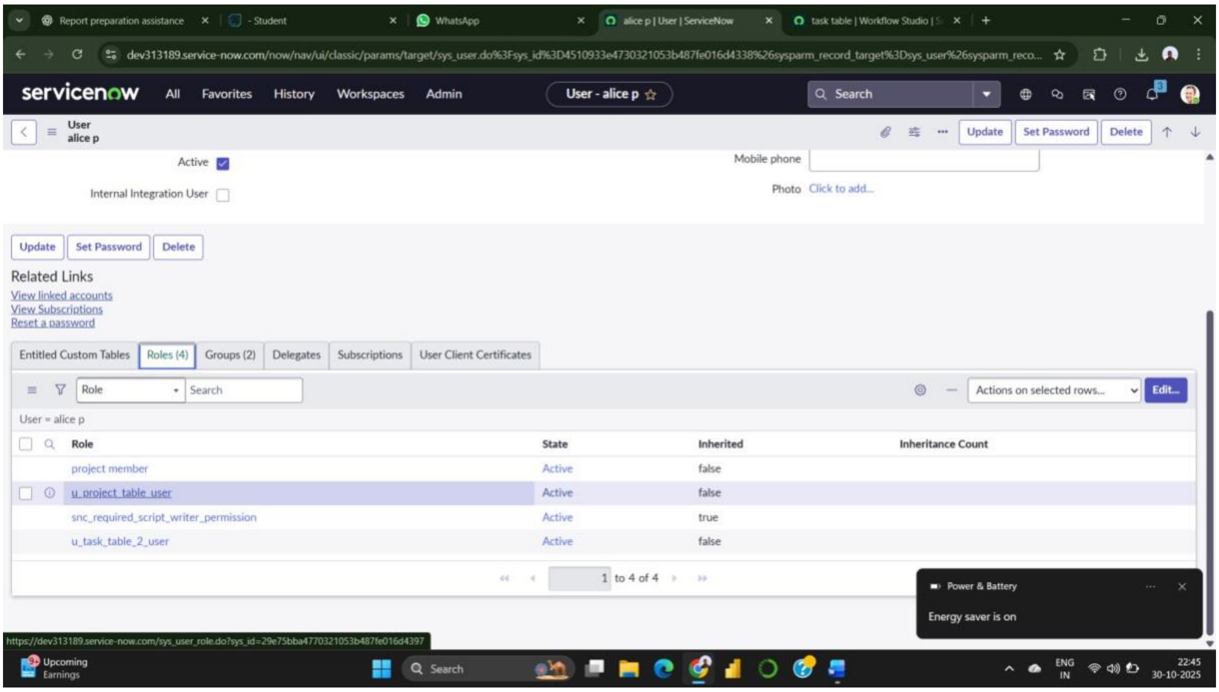
Column label	Type	Reference	Max length	Default value	Display
Created by	String	(empty)	40		false
Created	Date/Time	(empty)	40		false
Updated by	String	(empty)	40		false
Sys ID	Sys ID (GUID)	(empty)	32		false
Updates	Integer	(empty)	40		false
Updated	Date/Time	(empty)	40		false



Dictionary Entries

Column label	Type	Reference	Max length	Default value	Display
task id	Integer	(empty)	40		false
assigned to	String	(empty)	40		false
Created	Date/Time	(empty)	40		false
due date	Date	(empty)	40		false
Updated by	String	(empty)	40		false
Sys ID	Sys ID (GUID)	(empty)	32		false
task name	String	(empty)	40		false
Updates	Integer	(empty)	40		false
status	Choice	(empty)	40		false
comments	String	(empty)	40		false
Updated	Date/Time	(empty)	40		false
Created by	String	(empty)	40		false
Insert a new row...					

5. Assign Roles


Report preparation assistance
- Student
WhatsApp
alice p | User | ServiceNow
task table | Workflow Studio | S
dev313189.service-now.com/now/nav/ui/classic/params/target/sys_user.do%3Fsys_id%3D4510933e4730321053b487fe016d4338%26sysparm_record_target%3Dsys_user%26sysparm_reco...
servicenow
All
Favorites
History
Workspaces
Admin
User - alice p
Search
Update
Set Password
Delete
Entitled Custom Tables
Roles (4)
Groups (2)
Delegates
Subscriptions
User Client Certificates
Actions on selected rows...
Edit...
Power & Battery
Energy saver is on
https://dev313189.service-now.com/sys_user_role.do?sys_id=29e75bba4770321053b487fe016d4397
Upcoming
Earnings
Search
ENG
IN
22:45
30-10-2025

User
alice p

Active ☑

Internal Integration User □

Mobile phone

Photo Click to add...

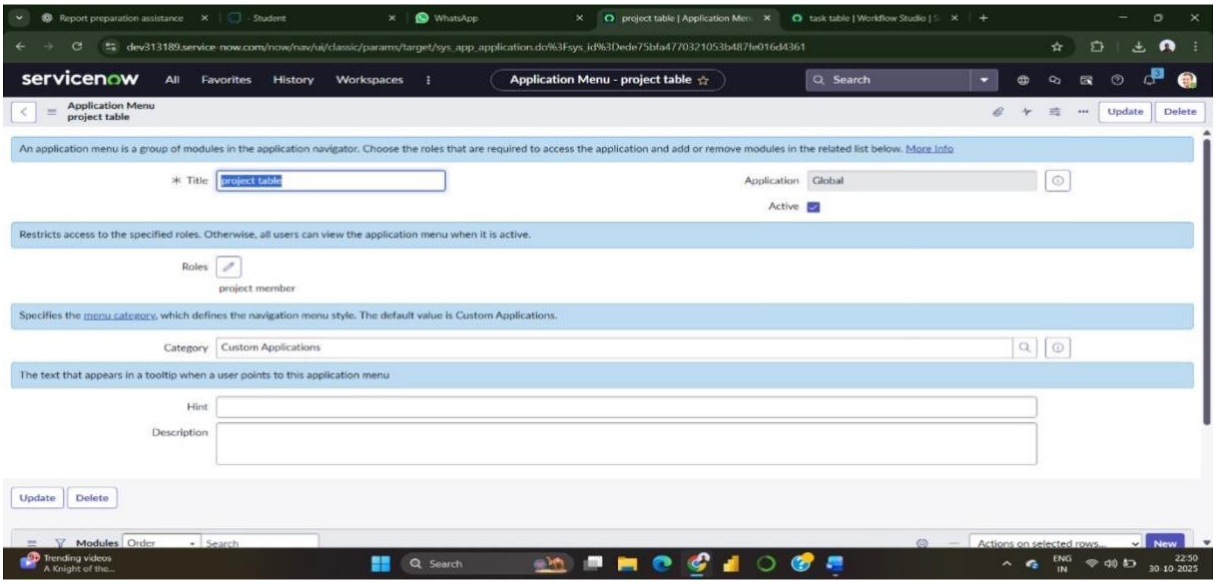
Related Links
View linked accounts
View Subscriptions
Reset a password

User = alice p

Role	State	Inherited	Inheritance Count
project member	Active	false	
u_project_table_user	Active	false	
snc_required_script_writer_permission	Active	true	
u_task_table_2_user	Active	false	

1 to 4 of 4

6. Assign Table Access to Applications


Report preparation assistance
- Student
WhatsApp
project table | Application Men
task table | Workflow Studio | S
dev313189.service-now.com/now/nav/ui/classic/params/target/sys_app_application.do%3Fsys_id%3Dede75bfa4770321053b487fe016d4361
servicenow
All
Favorites
History
Workspaces
Application Menu - project table
Search
Update
Delete
Modules
Order
Search
Actions on selected rows...
New
Trending videos
A Knight of the...
ENG
IN
22:50
30-10-2025

Application Menu
project table

An application menu is a group of modules in the application navigator. Choose the roles that are required to access the application and add or remove modules in the related list below. More Info

* Title project table

Application Global

Active ☑

Restricts access to the specified roles. Otherwise, all users can view the application menu when it is active.

Roles
project member

Specifies the menu category, which defines the navigation menu style. The default value is Custom Applications.

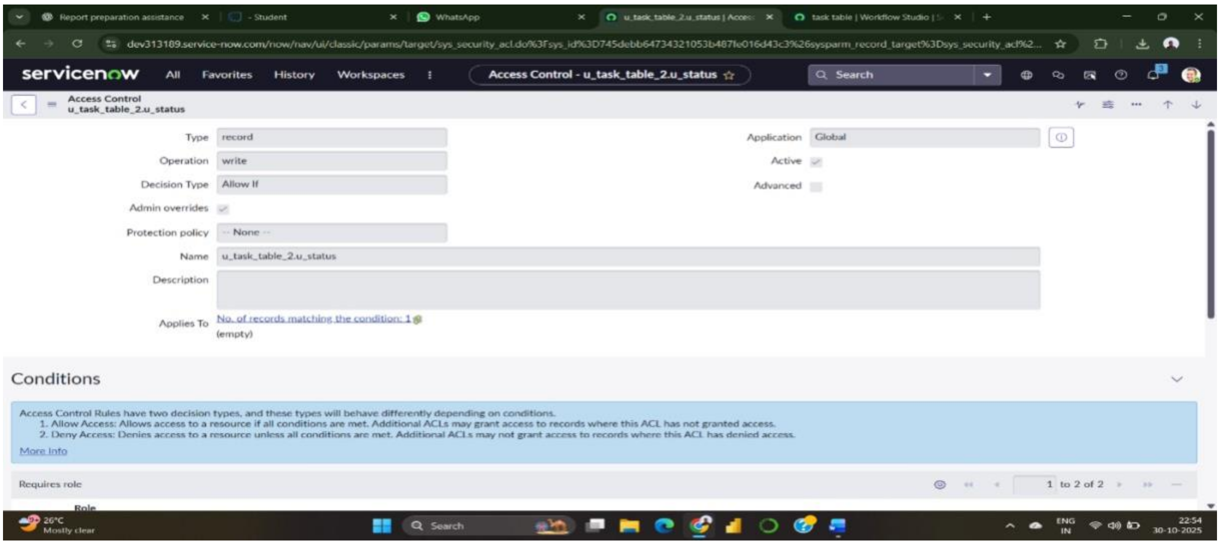
Category Custom Applications

The text that appears in a tooltip when a user points to this application menu

Hint

Description

7. Assign Access Control


Report preparation assistance
- Student
WhatsApp
u_task_table_2.u_status | Acces
task table | Workflow Studio | S
dev313189.service-now.com/now/nav/ui/classic/params/target/sys_security_acl.do%3Fsys_id%3D745debb64734321053b487fe016d43c3%26sysparm_record_target%3Dsys_security_acl%2...
servicenow
All
Favorites
History
Workspaces
Access Control - u_task_table_2.u_status
Search
26°C
Mostly clear
ENG
IN
22:54
30-10-2025

Access Control
u_task_table_2.u_status

Type record

Operation write

Decision Type Allow If

Admin overrides ☑

Protection policy -- None --

Name u_task_table_2.u_status

Description

Applies To No. of records matching the condition: 1
(empty)

Application Global

Active ☑

Advanced □

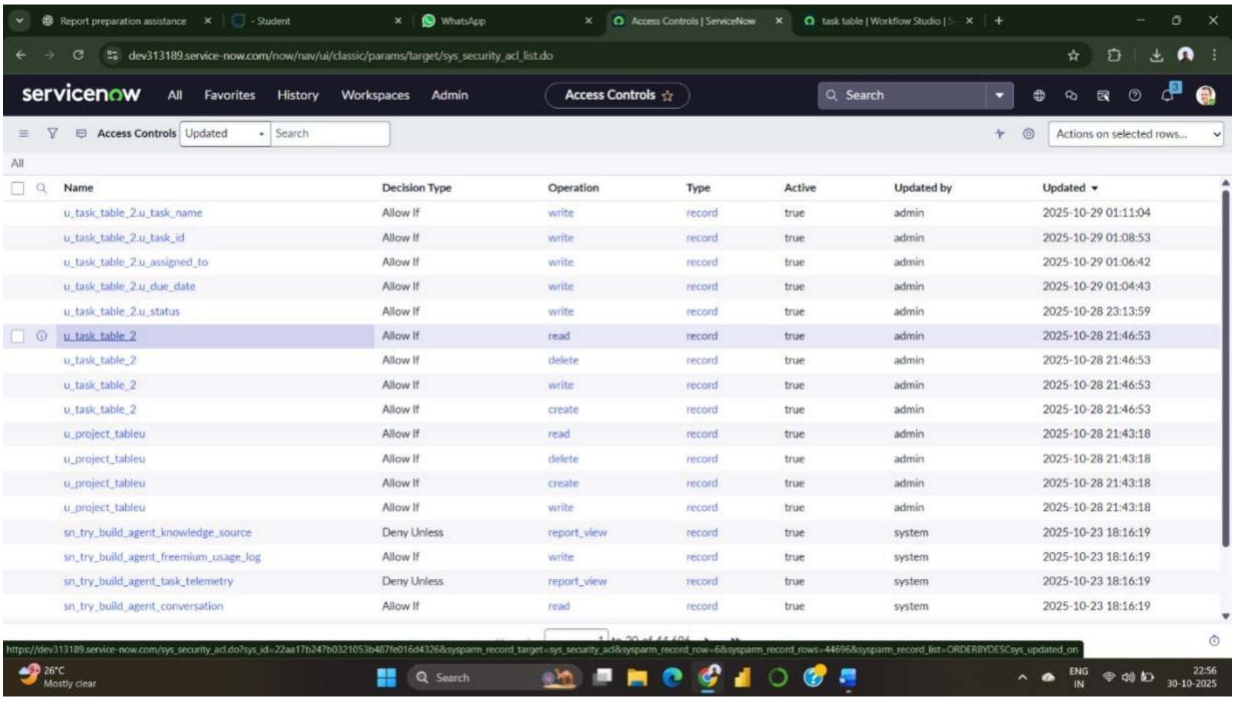
Conditions

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. Additional ACLs may grant access to records where this ACL has not granted access.
2. Deny Access: Denies access to a resource unless all conditions are met. Additional ACLs may not grant access to records where this ACL has denied access.
More Info

Requires role

1 to 2 of 2

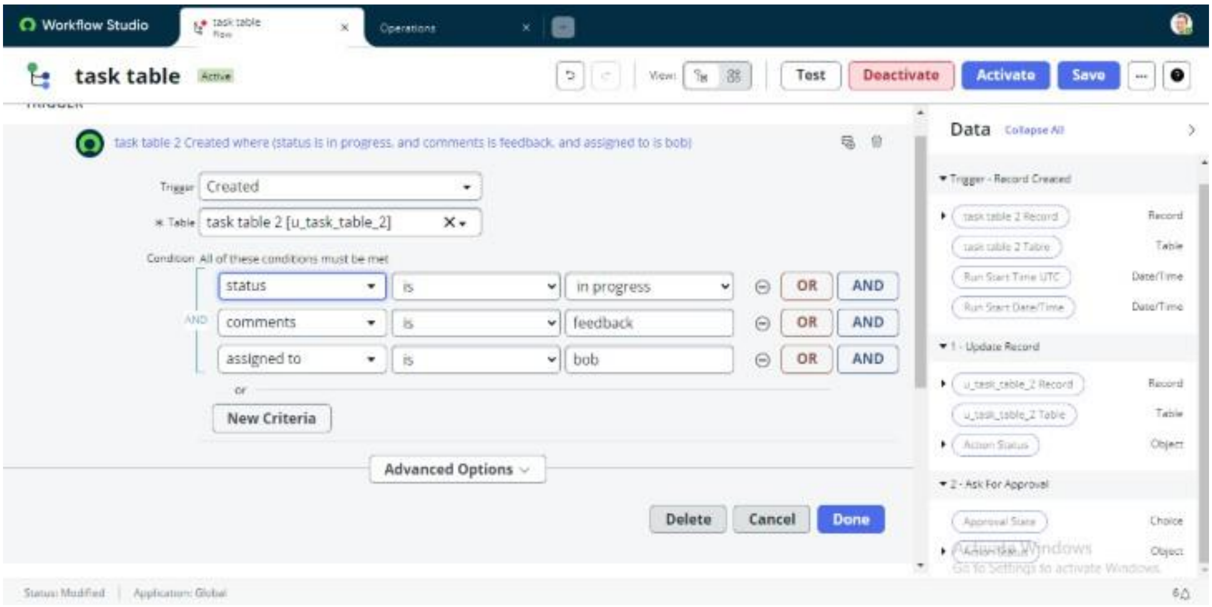
Role


Report preparation assistance
- Student
WhatsApp
Access Controls | ServiceNow
task table | Workflow Studio
dev313189.service-now.com/now/nav/ui/classic/params/target/sys_security_acl_list.do
servicenow
All
Favorites
History
Workspaces
Admin
Access Controls ☆
Search
Access Controls
Updated
Search
Actions on selected rows...
All

Name	Decision Type	Operation	Type	Active	Updated by	Updated ▾
u_task_table_2.u_task_name	Allow If	write	record	true	admin	2025-10-29 01:11:04
u_task_table_2.u_task_id	Allow If	write	record	true	admin	2025-10-29 01:08:53
u_task_table_2.u_assigned_to	Allow If	write	record	true	admin	2025-10-29 01:06:42
u_task_table_2.u_due_date	Allow If	write	record	true	admin	2025-10-29 01:04:43
u_task_table_2.u_status	Allow If	write	record	true	admin	2025-10-28 23:13:59
u_task_table_2	Allow If	read	record	true	admin	2025-10-28 21:46:53
u_task_table_2	Allow If	delete	record	true	admin	2025-10-28 21:46:53
u_task_table_2	Allow If	write	record	true	admin	2025-10-28 21:46:53
u_task_table_2	Allow If	create	record	true	admin	2025-10-28 21:46:53
u_project_tableu	Allow If	read	record	true	admin	2025-10-28 21:43:18
u_project_tableu	Allow If	delete	record	true	admin	2025-10-28 21:43:18
u_project_tableu	Allow If	create	record	true	admin	2025-10-28 21:43:18
u_project_tableu	Allow If	write	record	true	admin	2025-10-28 21:43:18
sn_try_build_agent_knowledge_source	Deny Unless	report_view	record	true	system	2025-10-23 18:16:19
sn_try_build_agent_freemium_usage_log	Allow If	write	record	true	system	2025-10-23 18:16:19
sn_try_build_agent_task_telemetry	Deny Unless	report_view	record	true	system	2025-10-23 18:16:19
sn_try_build_agent_conversation	Allow If	read	record	true	system	2025-10-23 18:16:19

https://dev313189.service-now.com/sys_security_acl.do?sys_id=22aa17b247b0321053b487fe016d4326&sysparm_record_target=sys_security_acl&sysparm_record_row=6&sysparm_record_rows=44696&sysparm_record_list=ORDERBYDESCsys_updated_on
26°C
Mostly clear
Search
ENG
IN
22:56
30-10-2025

8. Create Flow



task table 2 Created where (status is in progress, and comments is feedback, and assigned to is bob)

Trigger: Created

* Table: task table 2 [u_task_table_2]

Condition: All of these conditions must be met

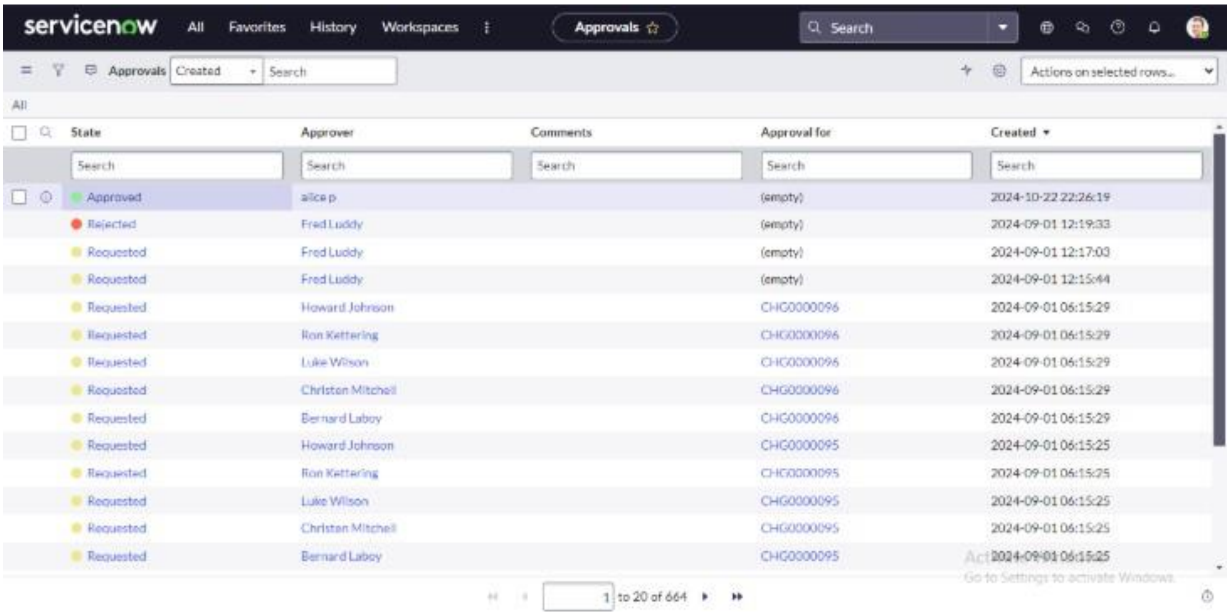
status	is	in progress	⊖	OR	AND
AND comments	is	feedback	⊖	OR	AND
assigned to	is	bob	⊖	OR	AND

or

New Criteria

Advanced Options

Delete Cancel Done



State	Approver	Comments	Approval for	Created ▾
● Approved	alice p		(empty)	2024-10-22 22:26:19
● Rejected	Fred Luddy		(empty)	2024-09-01 12:19:33
● Requested	Fred Luddy		(empty)	2024-09-01 12:17:03
● Requested	Fred Luddy		(empty)	2024-09-01 12:15:44
● Requested	Howard Johnson		CHG0000096	2024-09-01 06:15:29
● Requested	Ron Kettering		CHG0000096	2024-09-01 06:15:29
● Requested	Luke Wilson		CHG0000096	2024-09-01 06:15:29
● Requested	Christen Mitchell		CHG0000096	2024-09-01 06:15:29
● Requested	Bernard Laboy		CHG0000096	2024-09-01 06:15:29
● Requested	Howard Johnson		CHG0000095	2024-09-01 06:15:25
● Requested	Ron Kettering		CHG0000095	2024-09-01 06:15:25
● Requested	Luke Wilson		CHG0000095	2024-09-01 06:15:25
● Requested	Christen Mitchell		CHG0000095	2024-09-01 06:15:25
● Requested	Bernard Laboy		CHG0000095	2024-09-01 06:15:25

1 to 20 of 664

12. Conclusion

The project successfully demonstrates how automation and RBAC principles can optimize user, group, and role management in modern organizations. By replacing manual access control with automated workflows, the system improves security, accuracy, and productivity.

The solution not only simplifies administrative operations but also establishes a strong foundation for scalable and compliant identity management. This innovation can be extended to enterprise and cloud environments, making it a valuable contribution toward smarter, more secure organizational ecosystems.