SERVICENOW PROJECT SUBMISSION

Tailored Application Access for Enhanced User Experience

Submitted by

Neellaparla Venkata Sravan Kumar Reddy au723921244036

Gangireddy Bharath Kumar Reddy au723921244021

Gajjala Harsha Kesava Reddy au723921244020

Mandli Manjunath Reddy au723921244030

Arjun College of Technology, Coimbatore

Anna University Chennai – 600 025

Tailored Application Access for Enhanced User Experience

Project Overview:

GlobalTech Solutions aims to enhance its operational efficiency by implementing a **Tailored Access Control System** within its ServiceNow instance. The system is designed to provide employees with role-specific access to applications and modules, minimizing confusion, ensuring data security, and improving user experience. By restricting access to only relevant features based on roles, this system streamlines workflows, reduces errors, and fosters a more organized operational environment.

Objectives:

1. **Role-Specific Access:** Assign precise access rights to employees based on their roles, ensuring they can only view and interact with relevant applications and modules.
2. **Enhanced Security:** Prevent unauthorized access to sensitive data and modules by implementing robust access controls.
3. **Improved Operational Efficiency:** Eliminate redundant options and clutter by presenting employees with a simplified and relevant interface.
4. **Scalability:** Design a flexible system that accommodates the addition of new roles, applications, and modules as organizational needs evolve.

Key Features:

1. **Role-Based Access Control (RBAC):**
    - Define roles such as Admin, Manager, Employee, and Visitor.
    - Assign permissions to specific applications and modules for each role.
2. **Dynamic User Interfaces:**
    - Tailored dashboards displaying only the relevant information and modules for each role.
3. **Secure Authentication:**
    - Multi-factor authentication (MFA) for sensitive roles to ensure secure access.

Key Features:

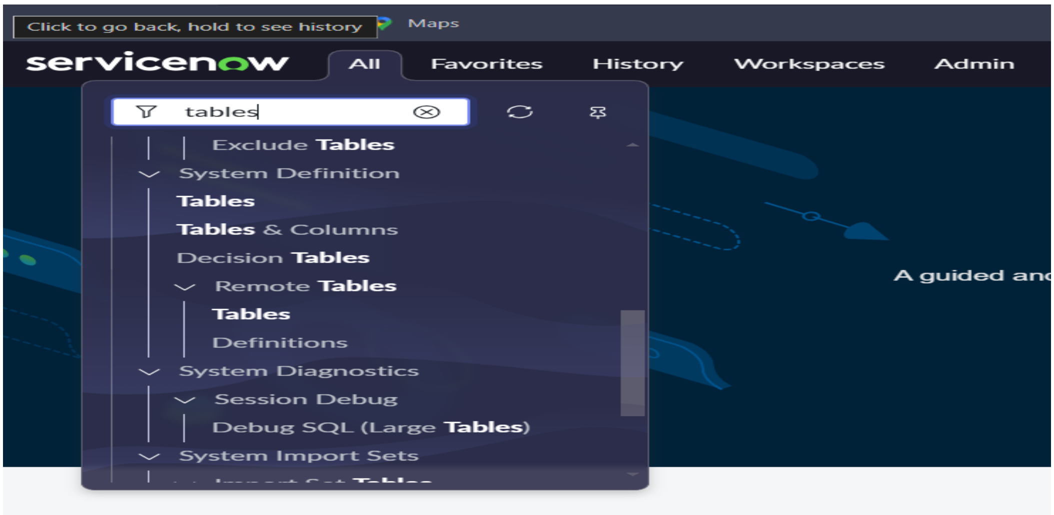
1. **Role-Based Access Control (RBAC):**
    - Define roles such as Admin, Manager, Employee, and Visitor.
    - Assign permissions to specific applications and modules for each role.
2. **Dynamic User Interfaces:**
    - Tailored dashboards displaying only the relevant information and modules for each role.
3. **Secure Authentication:**
    - Multi-factor authentication (MFA) for sensitive roles to ensure secure access.

<u>Detailed Steps to Solution:</u>

Implementation:

Step 1:

1. Open service now developer Instance
2. Click on All
3. Search for Tables.
4. Under System Definition select Tables.



5. Then click on New.
6. Fill the Details as:
7. Label : Service Request
8. Name : Auto-Populated
9. Add module to menu : Select Create New

Leave everything as Default.

10. Under Columns : click on insert a new row.
    Column label : Name >> Type : String
    Column label : Issue >> Type : String

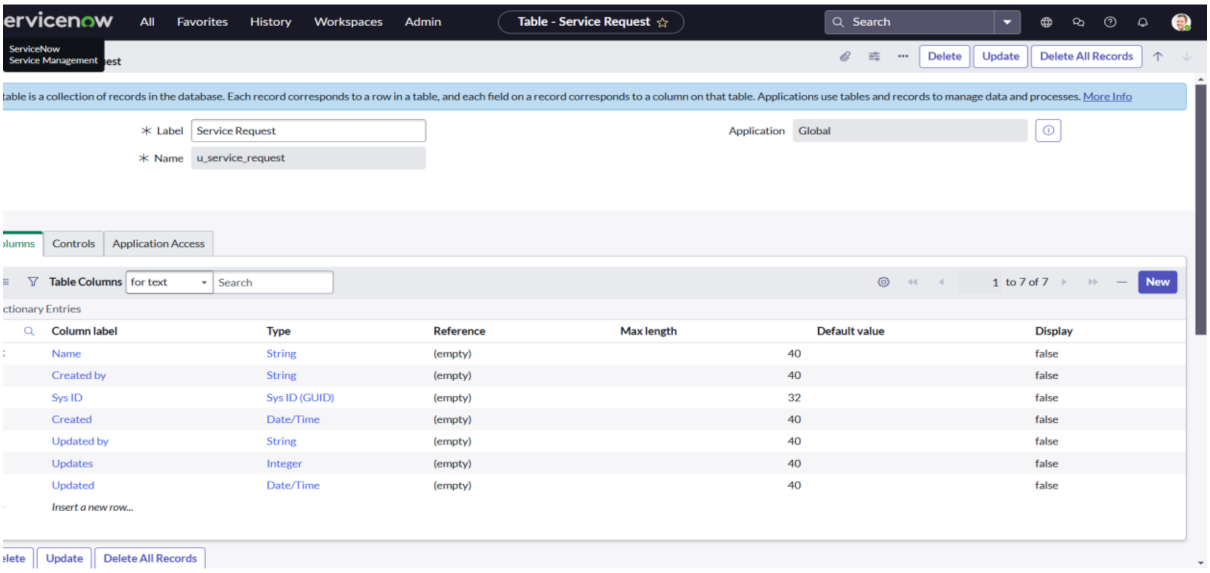


table is a collection of records in the database. Each record corresponds to a row in a table, and each field on a record corresponds to a column on that table. Applications use tables and records to manage data and processes. More Info

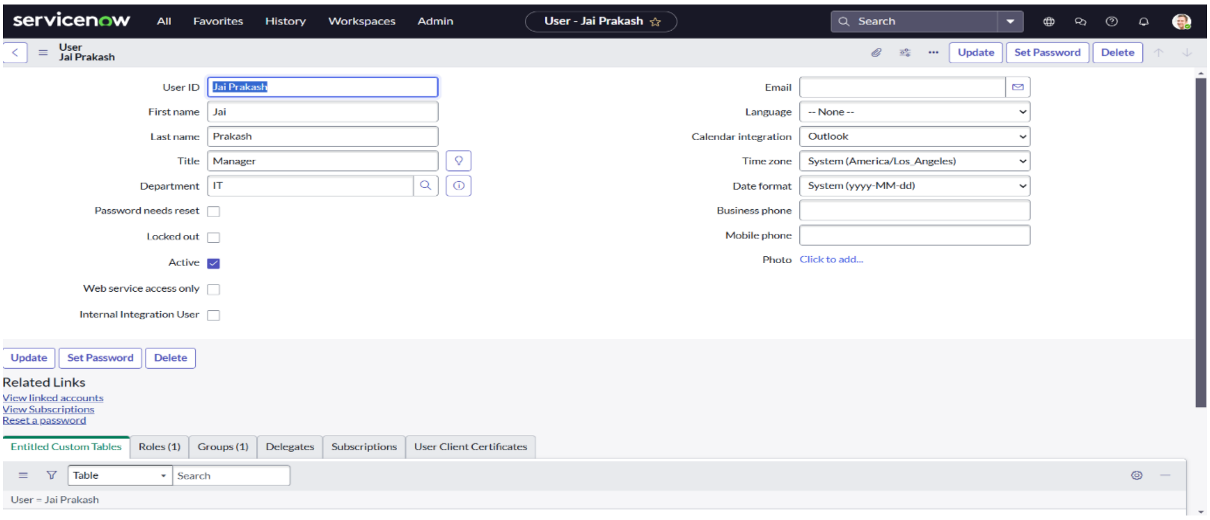
✱ Label	Service Request
✱ Name	u_service_request
Application	Global

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

11.Click On Submit.

Activity - 2: Create Users

1. Open service now.
2. Click on All >> search for users
3. Select Users under system security
4. Click on new
5. Fill the following details to create a new user

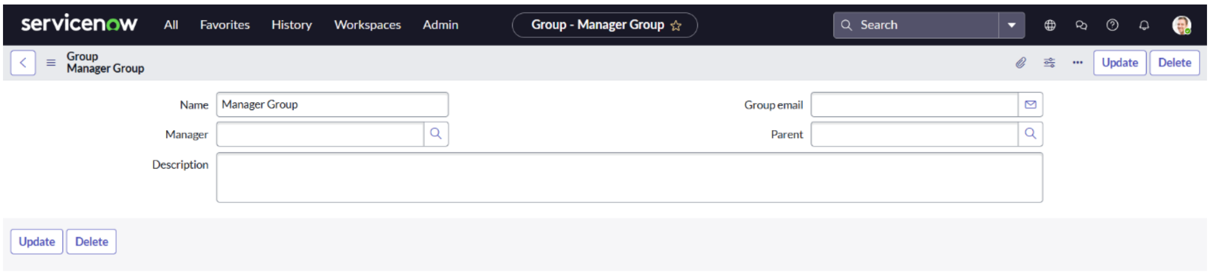


User ID	Jai Prakash	Email	
First name	Jai	Language	-- None --
Last name	Prakash	Calendar integration	Outlook
Title	Manager	Time zone	System (America/Los_Angeles)
Department	IT	Date format	System (yyyy-MM-dd)
Password needs reset	□	Business phone	
Locked out	□	Mobile phone	
Active	☑	Photo	Click to add...
Web service access only	□		
Internal Integration User	□		

6.Click on Submit.

Activity - 3: Create Groups

1. Open service now.
2. Click on All >> search for groups
3. Select groups under system security
4. Click on new
5. Fill the following details to create a new group.



Name: Manager Group

Manager:

Description:

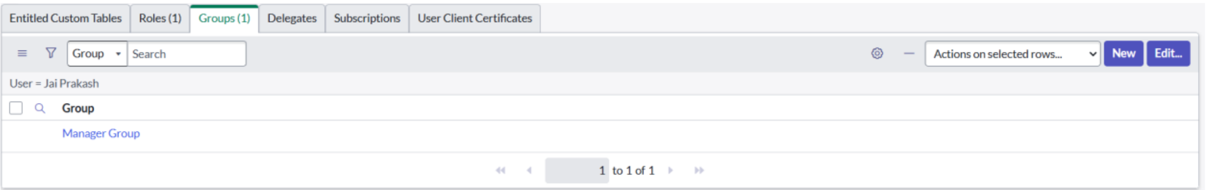
Group email:

Parent:

6.Under Group Members, click on edit.

7.Add the user(Jai Prakash) to the Manager Group and click on Save.

8.It would like below.



User = Jai Prakash

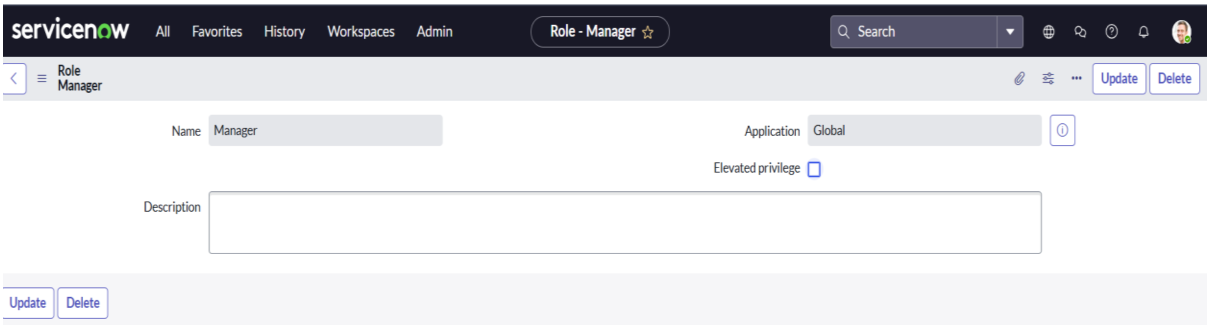
Group
Manager Group

1 to 1 of 1

9.Click On Save.

Activity - 4: Create Roles

1. Open service now.
2. Click on All >> search for roles
3. Select roles under system security
4. Click on new
5. Fill the following details to create a new role



Name: Manager

Application: Global

Elevated privilege □

Description:

6.Click on Submit.

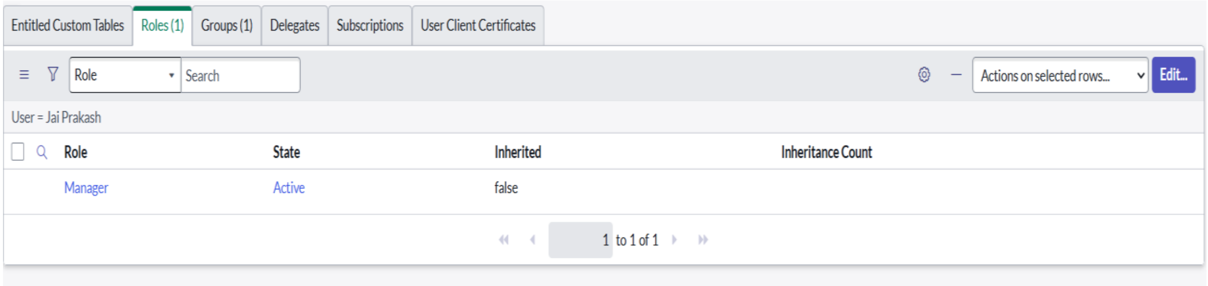
7.Click on All >> users

8.Search for “ jai prakash ”

9.Open the record, Go to the related list Click on roles

10.Click on Edit

11.Add manager to the selected list



User = Jai Prakash

□	Role	State	Inherited	Inheritance Count
	Manager	Active	false	

1 to 1 of 1

6. Click in Save.

Activity - 5: Creation of Modules

1.Click on All.

2.Search for Application Menus.

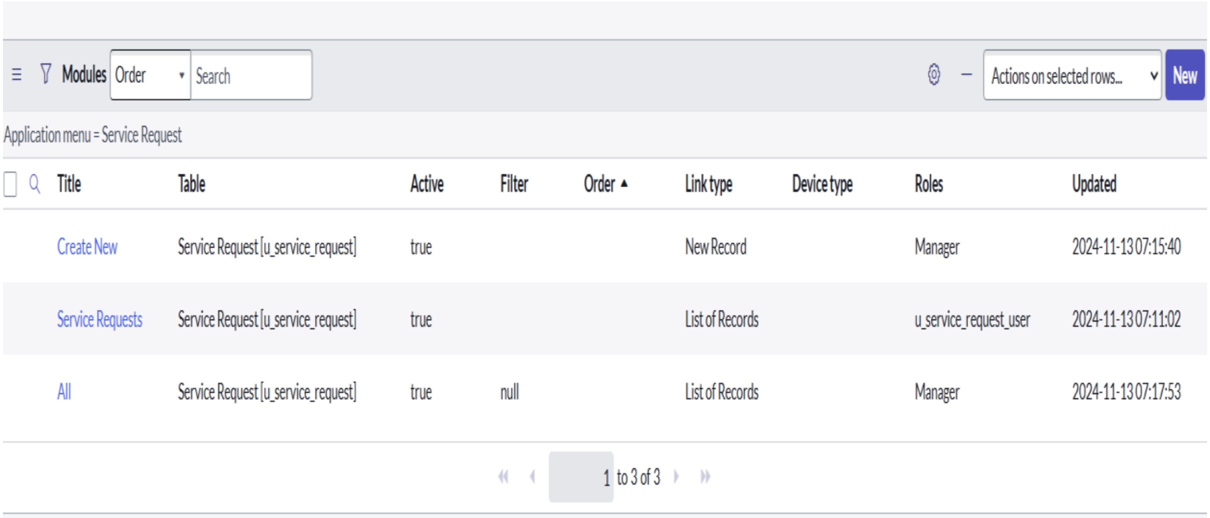
3.Open Application Menus.

4.Under Title search for Service Request and open service request.

5.Under Roles, click on roles and Select the Role to which this should be viewed.

6.Click on Done.

7.Now Under Modules Click on New
8.Create Three Modules, By Clicking on NEW
Module 1: Create New
Module 2: Service Requests
Module 3: All
9. After that the Modules would look like below.



Application menu = Service Request

Title	Table	Active	Filter	Order ▲	Link type	Device type	Roles	Updated
Create New	Service Request [u_service_request]	true			New Record		Manager	2024-11-13 07:15:40
Service Requests	Service Request [u_service_request]	true			List of Records		u_service_request_user	2024-11-13 07:11:02
All	Service Request [u_service_request]	true	null		List of Records		Manager	2024-11-13 07:17:53

1 to 3 of 3

10.Click on Save.

Testing and Validation

1. Test User Authentication

Objective:

Ensure the authentication mechanisms function correctly, preventing unauthorized access while allowing legitimate users to log in seamlessly.

Key Activities:

- Login Validation:

    - Test login functionality with valid and invalid credentials.
    - Attempt login with incorrect passwords and usernames to confirm rejection.
- Multi-Factor Authentication (MFA):
    - Verify that MFA triggers correctly for roles requiring additional security (e.g., Admin, Manager).
    - Test various MFA methods, such as SMS, email, or authenticator apps, for functionality and reliability.
- Session Management:
    - Validate that sessions expire after a predefined period of inactivity.
    - Test forced logouts when permissions or roles are updated.

2. Validation

Objective:

Ensure the system correctly enforces role-based access control (RBAC), validates module access, and prevents unauthorized actions.

Key Activities:

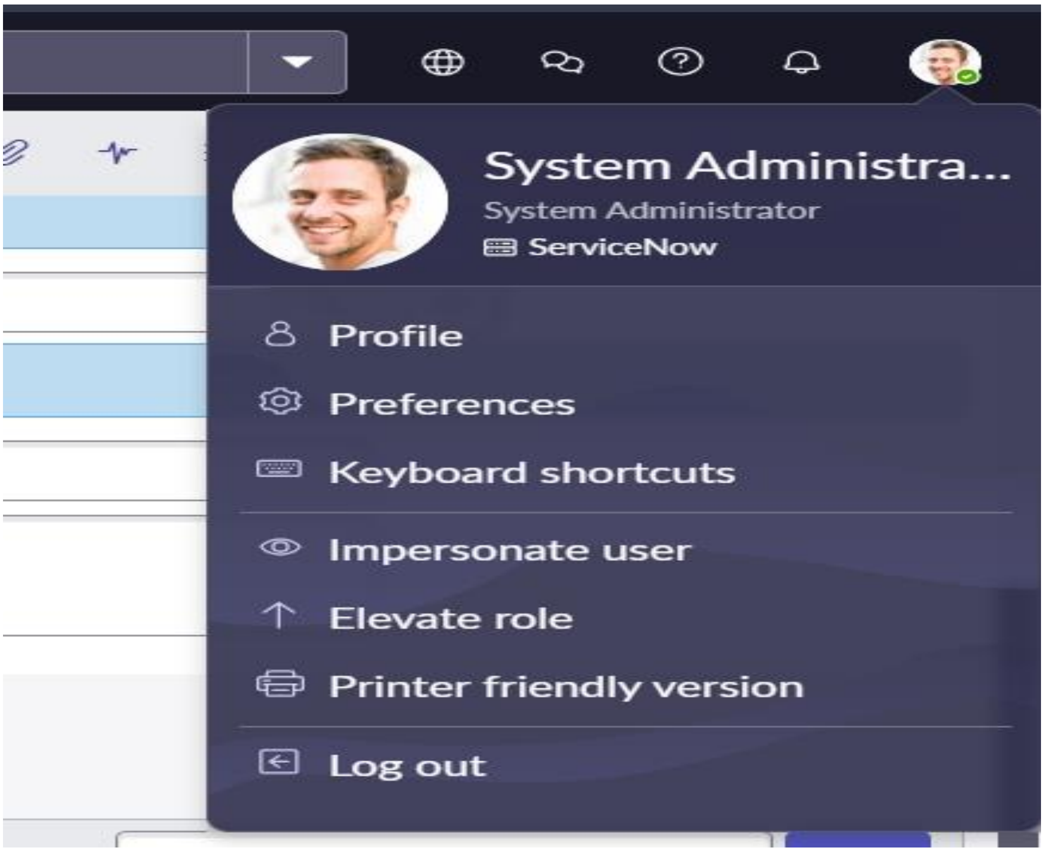
- Role-Specific Access Validation:
    - Log in with accounts from each role (Admin, Manager, Employee, Guest) and attempt actions outside the permitted scope.

    - Verify that Admins have full access, Managers have module-specific access, Employees have limited access, and Guests have view-only permissions.

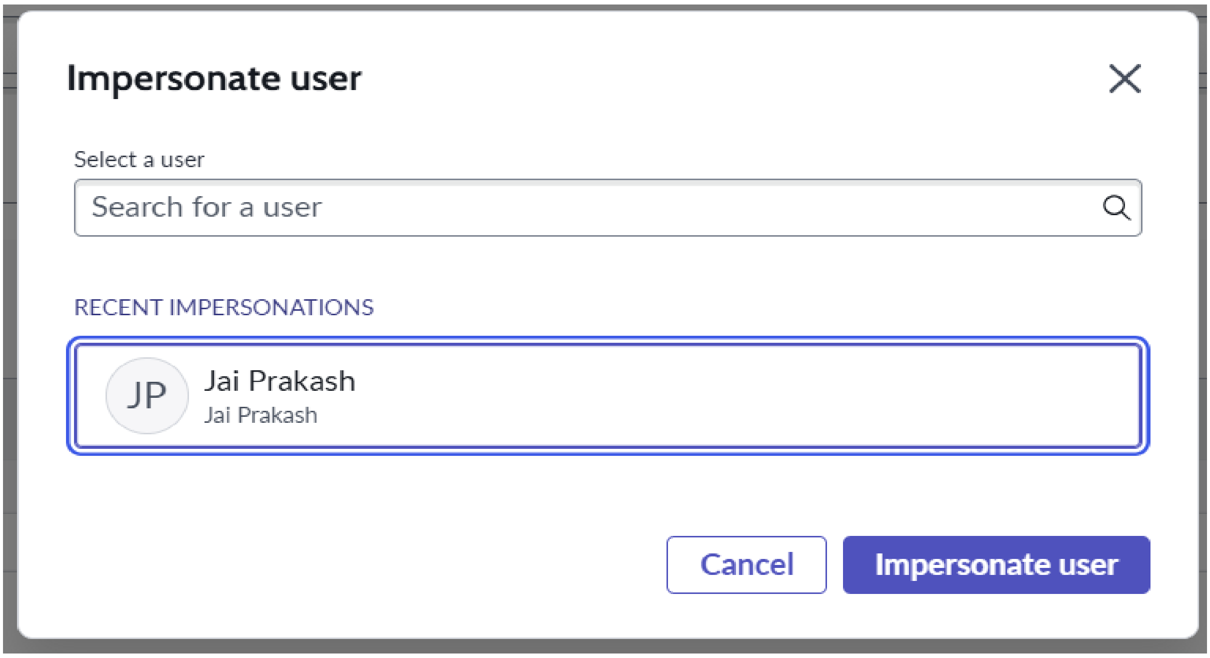
- Dynamic Dashboard Validation:
    - Check that role-specific dashboards display the correct modules, data, and actions for each role.
    - Confirm that sensitive information is hidden from roles without appropriate permissions.
- Error Handling:
    - Attempt unauthorized actions (e.g., Manager trying to change user roles) and confirm the system generates appropriate error messages.
- Data Integrity Validation:
    - Test CRUD operations (Create, Read, Update, Delete) for data by authorized roles and confirm no data corruption or leaks occur.
- Audit Trail Validation:
    - Ensure all access, changes, and unauthorized attempts are logged accurately.
    - Verify that logs capture user ID, timestamp, and details of the activity.

Result:

1. Go to Profile and click on Impersonate user.



2.Select the user you have been created and click on Impersonate user.


Impersonate user

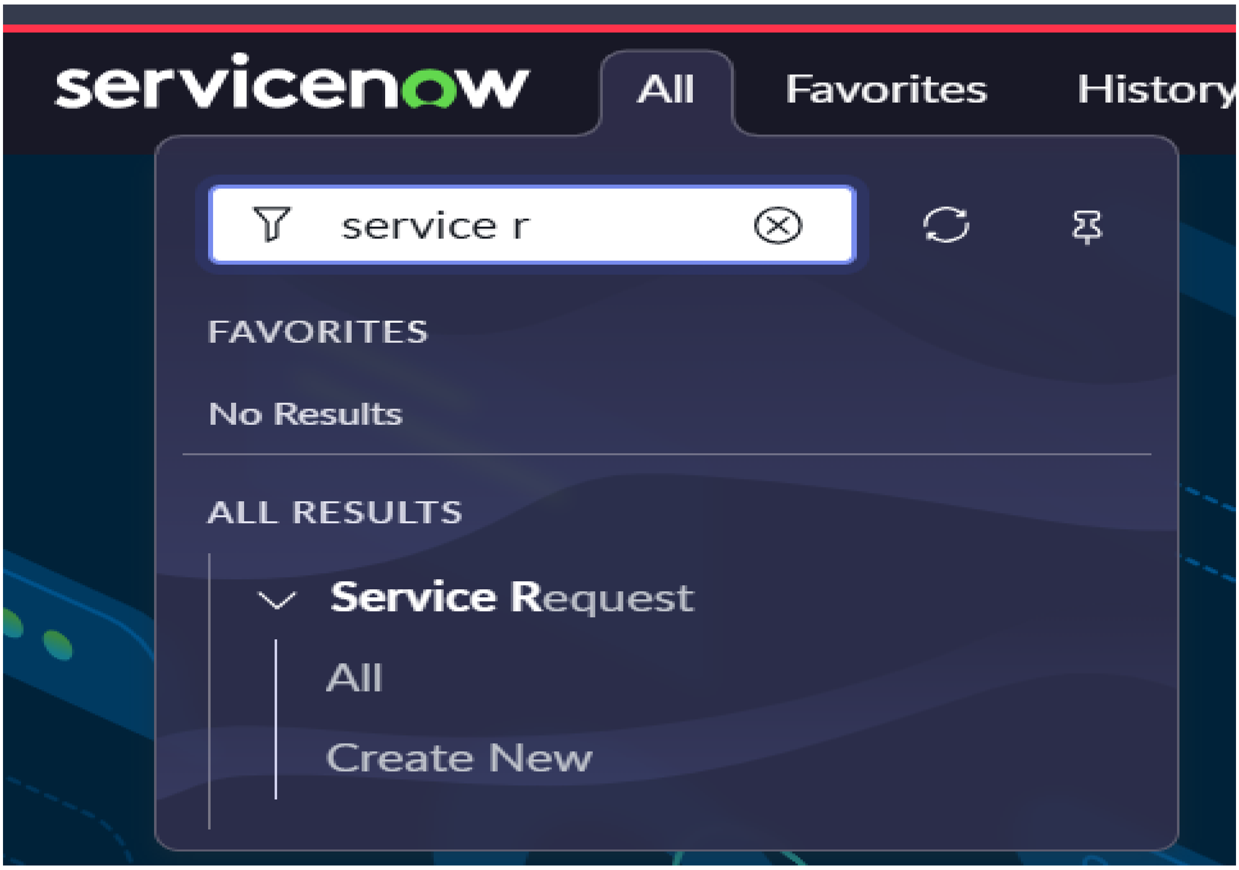
Select a user

Search for a user

RECENT IMPERSONATIONS

JP Jai Prakash
Jai Prakash

3.Go to All >> search for Service Request
4.Then you can find The Application(Service Request) and Modules(Create New, All)



Output:

The project aims to implement a tailored access control system in GlobalTech Solutions' ServiceNow instance, providing employees with role-specific applications to reduce confusion and enhance efficiency. By mapping tools to roles and simplifying the interface, employees will access only relevant features, improving navigation and productivity. Automation will handle role assignments, with regular updates ensuring accuracy. Training and support will help employees adapt, leading to streamlined workflows, increased satisfaction, and reduced administrative effort. This system will align ServiceNow's functionality with organizational needs, fostering a more efficient and user-friendly environment.