



Tailored Application Access for Enhanced User Experience

1. Project overview:

This project focuses on addressing the challenge of optimizing user access to applications within the ServiceNow platform. Leveraging ServiceNow's powerful service management capabilities, the goal is to configure a personalized and efficient access framework. The project aims to enhance operational efficiency, improve user satisfaction, and ensure secure and accurate access control. By doing so, it supports the organization's long-term objective of delivering seamless and user-centric IT services..

2. Objectives:

Business Goals:

- Enhance IT service management by optimizing access to applications based on user roles and responsibilities.
- Improve user satisfaction by providing a streamlined and personalized experience through ServiceNow's dynamic access capabilities.

Specific Outcomes:

- Configure ServiceNow to provide tailored access to applications based on user roles and responsibilities.
- Implement role-based access control (RBAC) to ensure only authorized users can view and interact with relevant applications.
- Develop personalized dashboards that display customized tools and data for individual users.
- Automate access management workflows to handle role updates, onboarding, and offboarding seamlessly.
- Generate detailed reports and analytics on access patterns to support data-driven decision-making..

3. Key Features and Concepts Utilized

Personalized Application Access Configuration

- Design a user-specific access framework within ServiceNow to optimize application visibility and usability.
- Enable dynamic application availability based on individual roles, responsibilities, and preferences.

Role-Based Access Control (RBAC)

• Implement RBAC to ensure that application access is secure and restricted to authorized users only.

• Define and assign precise roles and permissions to maintain compliance and control.

Automated Workflow Management

- Develop workflows to manage application access requests efficiently.
- Include automated approval systems, real-time notifications, and task tracking for streamlined operations.

Enhanced User Interface and Experience

- Customize the ServiceNow interface to offer intuitive navigation and effortless application access.
- Introduce user-friendly dashboards with personalized shortcuts and access summaries.

Data Analytics and Usage Insights

- Leverage advanced analytics to track access patterns, identify bottlenecks, and assess application utilization.
- Use these insights to make informed decisions about resource allocation and user access policies.

Integration with ITSM Processes

- Ensure seamless integration of tailored access controls with existing ITSM frameworks.
- Align access management with organizational service workflows to maintain consistency and operational efficiency.

Security and Compliance Monitoring

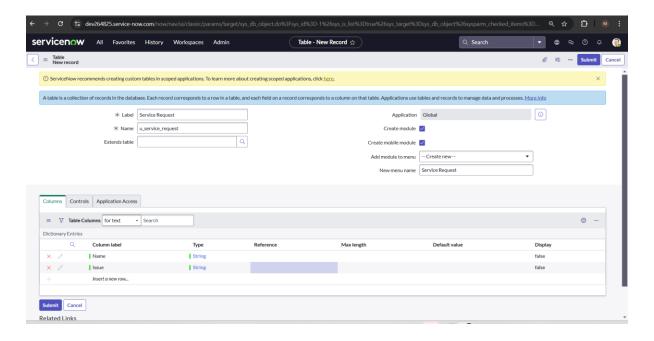
- Implement real-time security checks to ensure compliance with access policies.
- Conduct regular audits and generate reports to maintain accountability and transparency.

4. Detailed Steps to Solution Design

Implementation

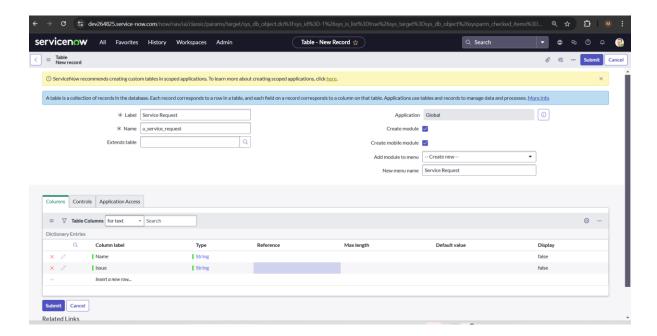
Activity-1:

- Open service now developer Instance
- Click on All
- Search for Tables.
- Under System Definition select Tables.
- Then click on New.
- Fill the Details as :Label : Service Request Name : Auto-Populated ,Add module to menu : Select Create New Leave everything as Default.
- Under Columns : click on insert a new row. Column label : Name >> Type : String Column label : Issue >> Type : String
- Click on Submit.



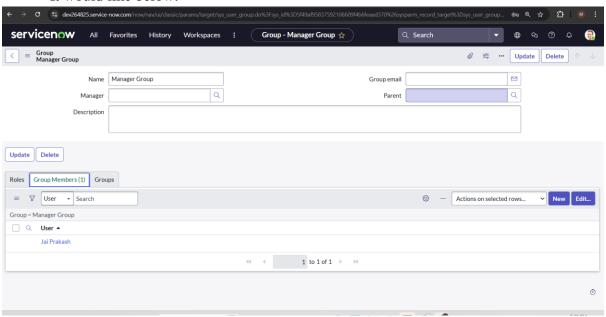
Activity - 2: Create Users

- Open service now.
- Click on All >> search for users
- Select Users under system security
- Click on new
- Fill the following details to create a new user
- Click on Submit.



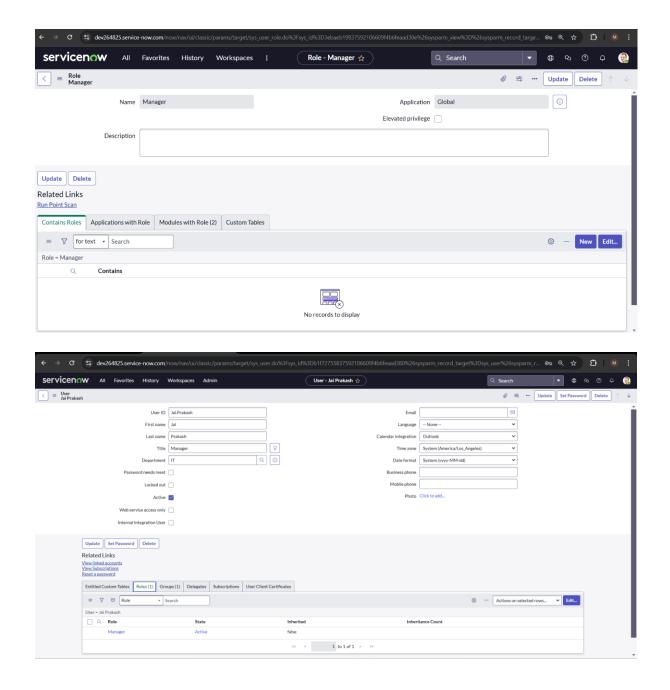
Activity - 3: Create Groups

- Open service now.
- Click on All >> search for groups
- Select groups under system security
- Click on new
- Fill the following details to create a new group.
- Under Group Members, click on edit.
- Add the user(Jai Prakash) to the Manager Group and click on Save.
- It would like below.



Activity - 4: Create Roles

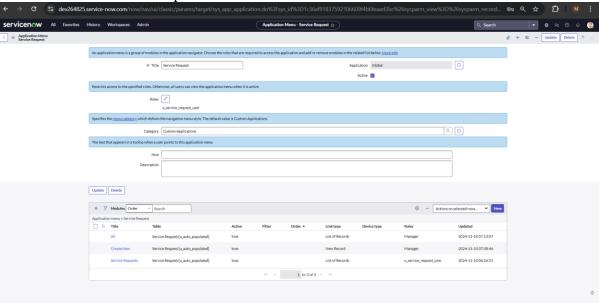
- Open service now.
- Click on All >> search for roles
- Select roles under system security
- Click on new
- Fill the following details to create a new role
- Click on Submit.
- Click on All >> users
- Search for "jai prakash"
- Open the record, Go to the related list Click on roles
- Click on Edit
- Add manager to the selected list and Click in Save.



Activity - 5: Creation of Modules

- Click on All.
- Search for Application Menus.
- Open Application Menus.
- Under Title search for Service Request and open service request.
- Under Roles, click on roles and Select the Role to which this should be viewed.
- Click on Done.
- Now under Modules. Click on New.
- Enter the details as:
- Title : Create New

- Under Visibility >> Select roles and select the role you want to assign.
- In Link Type, fill details as shown in figure.
- Click on Save.
- Now under Modules. Click on New.
- Enter the details as:
- Title : All
- Under Visibility >> Select roles and select the role you want to assign.
- In Link Type, fill details as shown in figure.
- Click on Save.
- After that the Modules would look like below.
- Hover over to the top and double click on the context menu and click on the Save



Result

- Go to Profile and click on Impersonate user.
- Select the user you have been created and click on Impersonate user.
- Go to All >> search for Service Request
- Then you can find The Application(Service Request) and Modules(Create New, All)

