UNIVERSITY COLLEGE OF ENGINEERING – PATTUKKOTTAI

RAJAMADAM – 614701

(A CONSTITUENT COLLEGE OF ANNA UNIVERSITY, CHENNAI)

Department of

COMPUTER SCIENCE AND ENGINEERING

Accompanied with

NAAN MUDHALVAN AND SERVICENOW ADMINISTRATION

Completed the project named as

OPTIMIZING USER,GROUP,AND ROLE MANAGEMENT WITH ACCESS CONTROL AND WORKFLOWS

Optimizing User,Group,And Role Management With Access Control And Workflows

Team ID: NM2025TMI00169

Team Size: 4

Team Leader: ASWINRAM T

Team Member: SAKTHIVEL S

Team Member: SAKTHI T

Team Member: SHOBAN VR

1. Project Overview

The Educational Management System (EMS) is a streamlined solution built on the ServiceNow platform to enhance administrative efficiency within educational institutions. It manages student and teacher data, simplifies the admission process, and provides tools for tracking academic progress. By implementing EMS in ServiceNow, institutions benefit from a user-friendly, customizable, and automated environment that supports better decision-making and operational management.

2. Setting Up the ServiceNow Instance

Sign Up for a Developer Account

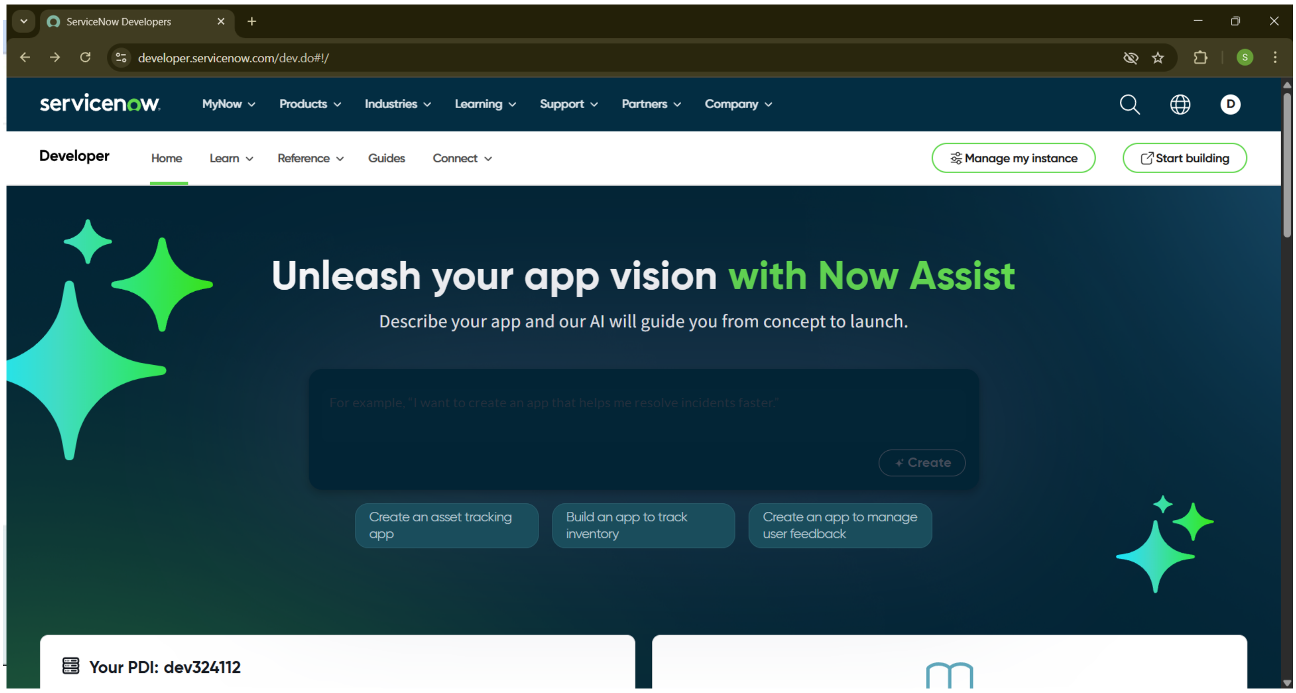
- Visit the ServiceNow Developer Portal at https://developer.servicenow.com.
- Create a new developer account by providing the required information.

Request a Personal Developer Instance

- Log in to your developer account.
- Navigate to the “Manage > Instance” section.
- Click “Request Instance” and choose the latest available release.
- You will receive an email with the instance details (URL, username, and password).

Access Your Instance

- Open the instance URL received via email.
- Log in using the provided credentials to access your personal ServiceNow instance.



Unleash your app vision with Now Assist

Describe your app and our AI will guide you from concept to launch.

For example, "I want to create an app that helps me resolve incidents faster."

Create
Create an asset tracking app
Build an app to track inventory
Create an app to manage user feedback

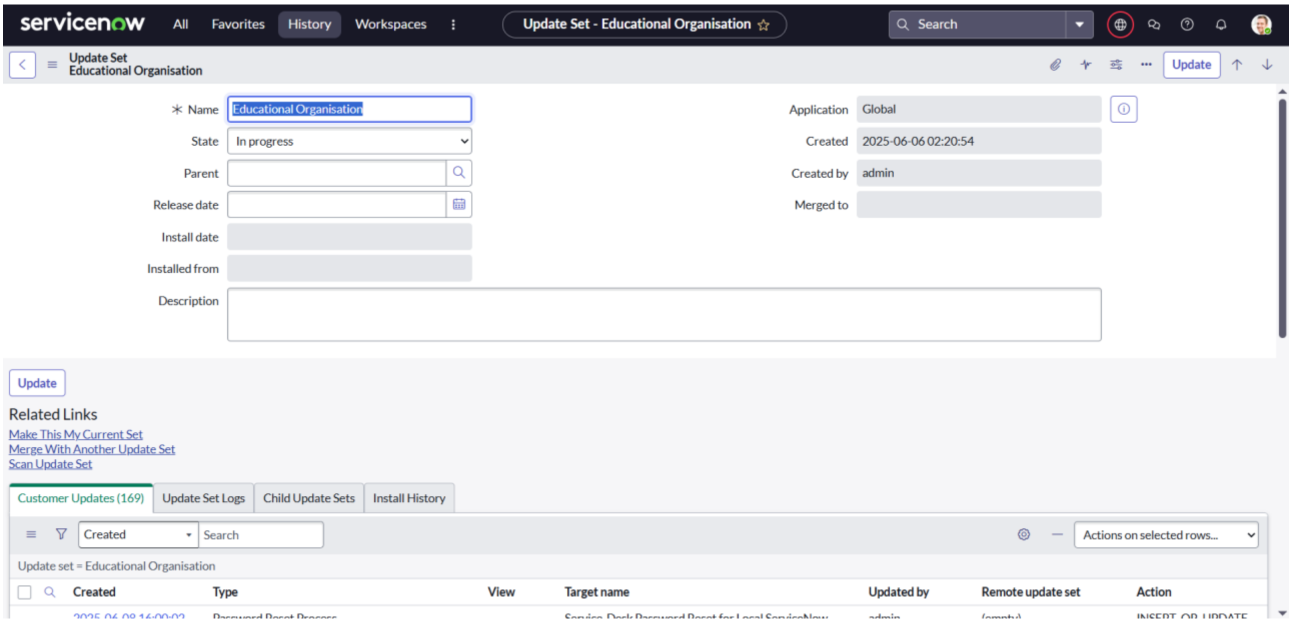
Your PDI: dev324112

3. Creating an Update Set

An Update Set tracks all configuration changes made in a ServiceNow instance, enabling migration between instances.

Steps:

- Navigate to All > Local Update Sets.
- Click New to create an update set.
- Enter the name "Educational Organisation" and submit.
- Click Make Current to activate the update set.



Update Set
Educational Organisation

* Name	Educational Organisation	Application	Global
State	In progress	Created	2025-06-06 02:20:54
Parent		Created by	admin
Release date		Merged to	
Install date			
Installed from			
Description			

Related Links
Make This My Current Set
Merge With Another Update Set
Scan Update Set

Update set = Educational Organisation

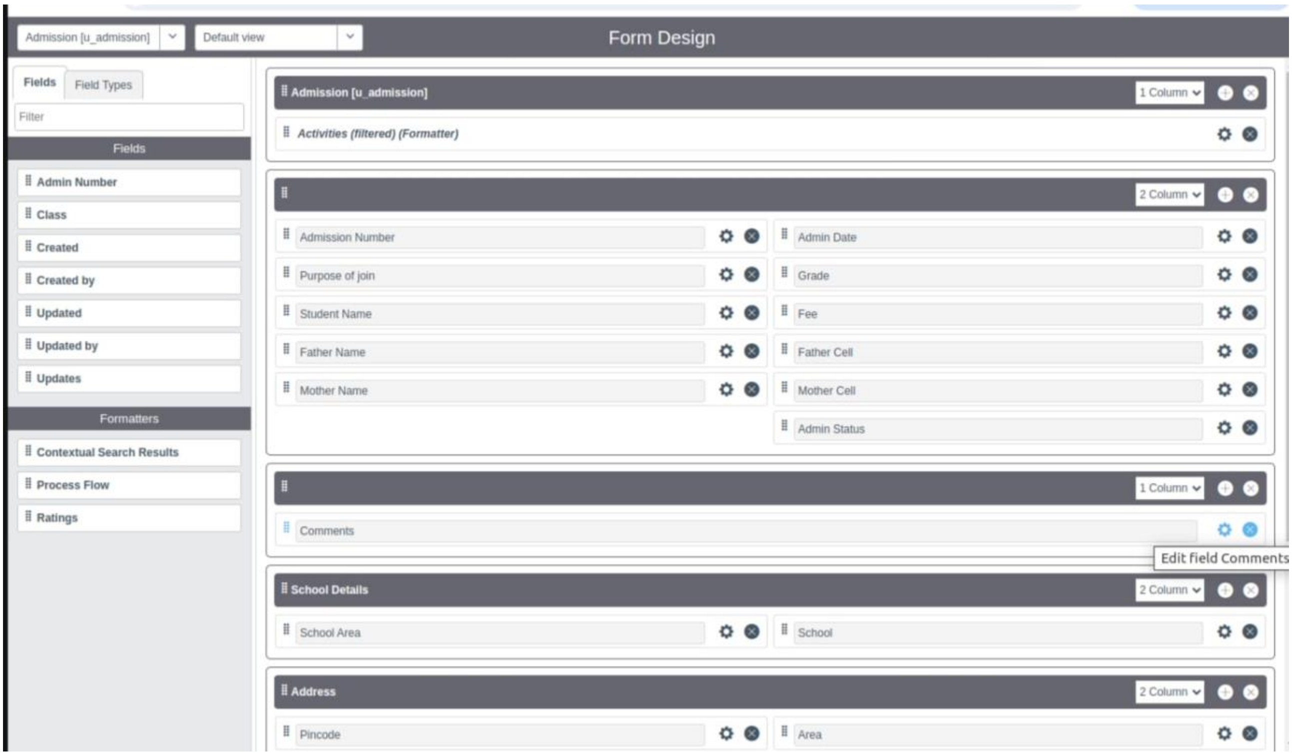
Created	Type	View	Target name	Updated by	Remote update set	Action

4. Creating the Salesforce Table

The Salesforce table manages core student information.

Steps:

- Navigate to All > Tables > New.
- Enter the label "Salesforce". The system will auto-generate the table name.
- Add required fields, including:
  - Admin Number (Set Display to True, mark Extensible, and set Dynamic Default to "Get Next Padded Number").
  - Grade (Configure as a choice field with values such as Primary, Secondary, etc.).



Admission [u_admission] | Default view | Form Design

Fields | Field Types

Filter

Fields

Admin Number
Class
Created
Created by
Updated
Updated by
Updates

Formatters

Contextual Search Results
Process Flow
Ratings

Admission [u_admission] — 1 Column

Activities (filtered) (Formatter)

2 Column

Admission Number	Admin Date
Purpose of join	Grade
Student Name	Fee
Father Name	Father Cell
Mother Name	Mother Cell
	Admin Status

1 Column

Comments

Edit Field Comments

School Details — 2 Column

School Area	School

Address — 2 Column

Pincode	Area

5. Creating the Admission Table

This table manages data related to student admissions and extends the Salesforce table.

Steps:

- Navigate to Tables > New.
- Label the table as "Admission".
- Set "Extends Table" to Salesforce.
- Add to application menu for visibility.
- Add necessary fields such as Admission Number, Grade, School, and Pincode.

OPTIMIZING USER GROUP AND ROLE MANAGEMENT WITH ACCESS CONTROL AND WORKFLOWS

INTRODUCTION: THE CRITICALITY OF USER MANAGEMENT

Effective management of user groups, roles, and their associated permissions is fundamental to an organization's security posture, operational efficiency, and regulatory compliance. As systems grow and user bases expand, manual or ad-hoc approaches to managing access become increasingly untenable, leading to security vulnerabilities, operational bottlenecks, and increased risk.

This document outlines strategies for optimizing user group and role management by leveraging robust access control mechanisms and well-defined workflows. We will explore key concepts, best practices, and the benefits of a structured approach.

UNDERSTANDING CORE CONCEPTS

User Groups

User groups are collections of users who share common attributes or job functions. Assigning permissions to groups, rather than individual users, simplifies administration. When a user joins or leaves a team, their group memberships can be updated, automatically granting or revoking the relevant access.

Roles

Roles represent a set of permissions and access rights associated with a specific job function or responsibility within an organization. Users are assigned roles, which in turn dictate their access to resources. This promotes consistency and adherence to the Principle of Least Privilege.

Access Control

Access control is the mechanism that enforces policies determining who (or what) can view, use, or perform actions on resources in a system. It ensures that users only have access to the information and functionalities necessary for their job roles.

Workflows

Workflows define the sequence of steps and approvals required for managing user access, including provisioning, de-provisioning, and modifications. Automated or semi-automated workflows reduce manual effort, minimize errors, and ensure timely execution of access changes.

BEST PRACTICES FOR ROLE AND GROUP MANAGEMENT

Principle of Least Privilege

This fundamental security principle dictates that any user, program, or process is granted only the bare minimum privileges necessary to perform its intended function. For user management, this means assigning roles and group memberships that grant only the required access, thereby reducing the potential attack surface.

Role-Based Access Control (RBAC)

RBAC is a widely adopted model where access permissions are tied to roles rather than individual users. Users are assigned roles, and roles are granted permissions. This simplifies management, especially in large organizations, by allowing administrators to manage permissions at the role level.

Potential Diagram: A diagram illustrating the RBAC model showing users assigned to roles, and roles having permissions for resources, would be beneficial here. It would visually represent the abstraction provided by roles.

Attribute-Based Access Control (ABAC)

ABAC offers a more granular approach where access decisions are based on a combination of attributes associated with the user, the resource, the action, and the environment. This model is highly flexible and can enforce complex policies but requires careful design and implementation.

Regular Access Reviews

Periodically reviewing user access, role assignments, and group memberships is crucial. This ensures that permissions remain appropriate as job functions change or employees move within the organization, and helps identify and revoke unnecessary access.

IMPLEMENTING ACCESS CONTROL POLICIES

Defining Granular Permissions

Permissions should be defined at a granular level, specifying precisely what actions a user can perform on which resources (e.g., read, write, delete, execute). Avoid overly broad permissions.

Centralized Policy Management

Where possible, use centralized systems or tools to define, manage, and enforce access control policies. This ensures consistency across different applications and systems.

Segregation of Duties

Critical functions should require at least two individuals to complete. This is achieved by ensuring that no single user has end-to-end control over a sensitive process. Role design should reflect this principle.

Enforcement Mechanisms

Access control policies must be effectively enforced by the underlying systems. This involves integrating with authentication services and authorization engines to validate every access request.

LEVERAGING WORKFLOWS FOR EFFICIENT MANAGEMENT

User Onboarding and Offboarding

Automated workflows can ensure that when a new employee joins, they are automatically assigned to the correct groups and roles based on their department and position. Similarly, when an employee leaves, their access is promptly and completely revoked across all systems.

Potential Diagram: A workflow flowchart detailing the steps for user onboarding, from HR notification to account creation and permission assignment, would clarify the process.

Role and Group Provisioning/Deprovisioning

Workflows can manage the creation, modification, and deletion of roles and groups themselves, including any necessary approval steps. This ensures that changes to the access structure are documented and authorized.

Access Request and Approval

Implement workflows for users to request access to specific resources or roles. These workflows should include an approval chain, ensuring that managers or system owners review and authorize requests before access is granted.

Potential Diagram: A workflow diagram illustrating the process of an access request, including submission, manager approval, IT review, and final provisioning, would be highly valuable.

Automated Re-certification Campaigns

Workflows can automate the process of periodic access reviews, prompting managers or designated personnel to certify that current access levels are still necessary and appropriate for their team members.

BENEFITS OF OPTIMIZED USER MANAGEMENT

Enhanced Security

By adhering to the Principle of Least Privilege and implementing robust access controls, the risk of unauthorized access, data breaches, and insider threats is significantly reduced.

Improved Compliance

Well-defined roles, groups, and automated workflows help organizations meet regulatory requirements (e.g., GDPR, SOX, HIPAA) by demonstrating clear control over data access and providing audit trails.

Increased Operational Efficiency

Automating manual tasks related to user provisioning, de-provisioning, and access management frees up IT resources and reduces the time it takes to grant or revoke access.

Reduced Errors and Inconsistencies

Standardized workflows and RBAC models minimize human error and ensure that access is granted consistently, regardless of who performs the administration task.

Better Auditability

Comprehensive logging and reporting capabilities, often integrated with workflow systems, provide clear audit trails for all access-related activities, simplifying compliance audits.

CONCLUSION

Optimizing user group and role management through structured access control and automated workflows is not merely a technical task but a strategic imperative. It forms the bedrock of a secure, compliant, and efficient IT environment. By implementing the principles and practices discussed, organizations can gain greater control over their digital assets, reduce operational overhead, and foster a culture of security.