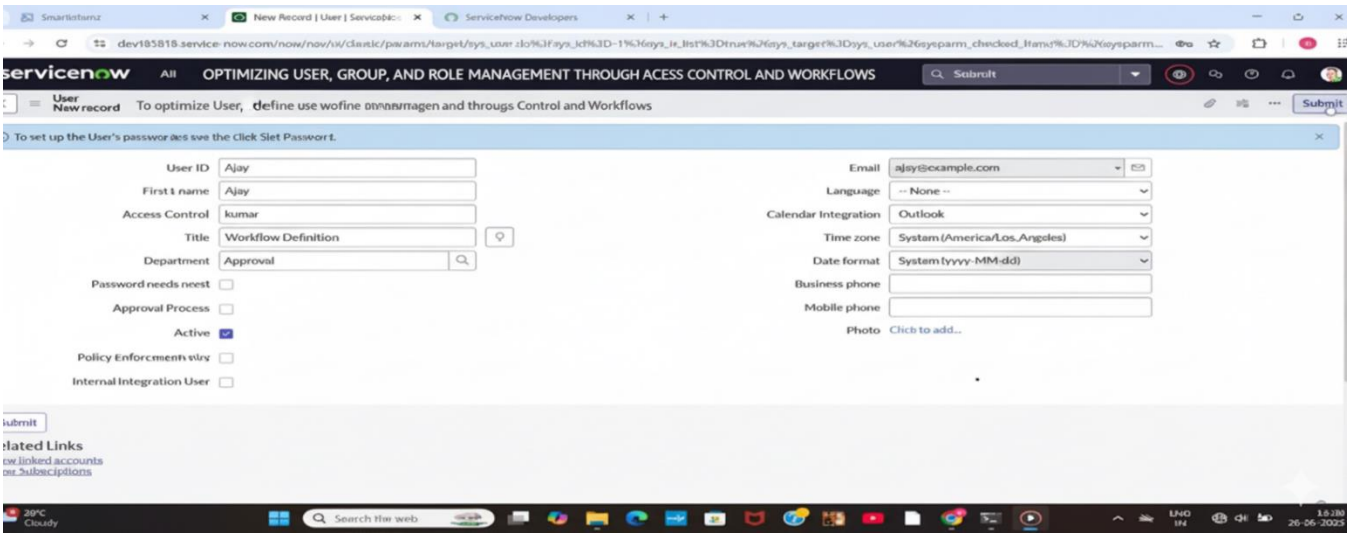
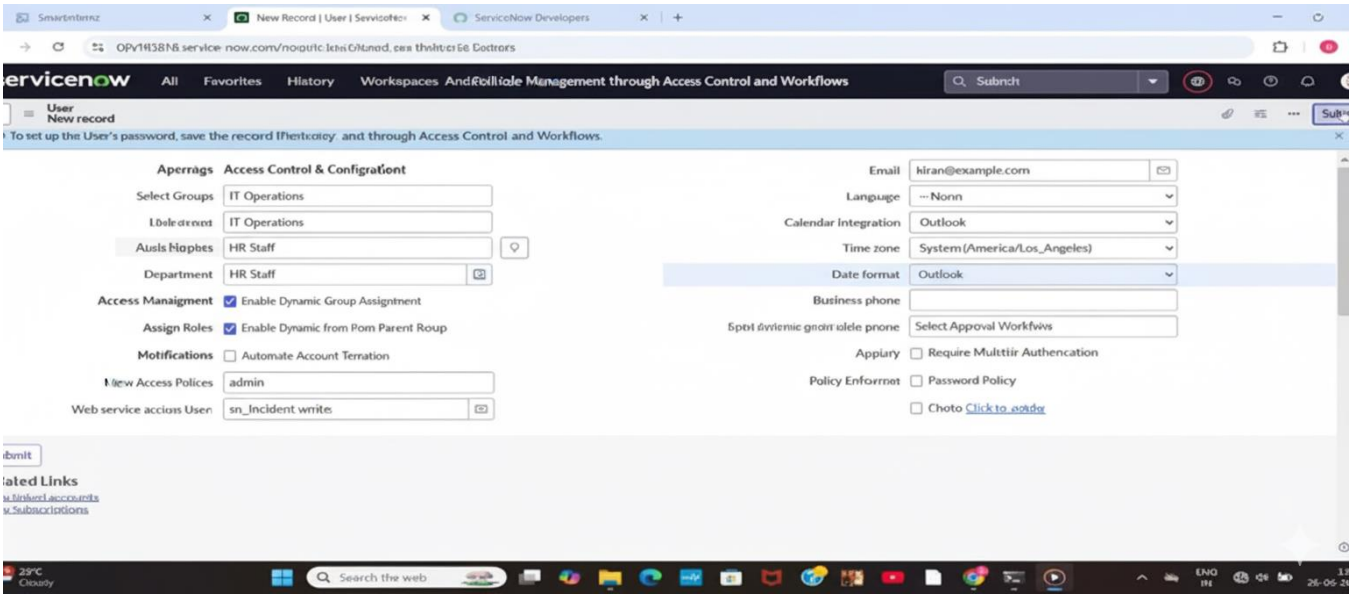
Performance and Testing

Date	27 JUNE 2025
Team ID	NM2025TMID07955
Project Name	OPTIMIZING USER, GROUP, AND ROLE MANAGEMENT THROUGH ACCESS CONTROL AND WORKFLOWS
Maximum Marks	4 Marks

Model Performance Testing

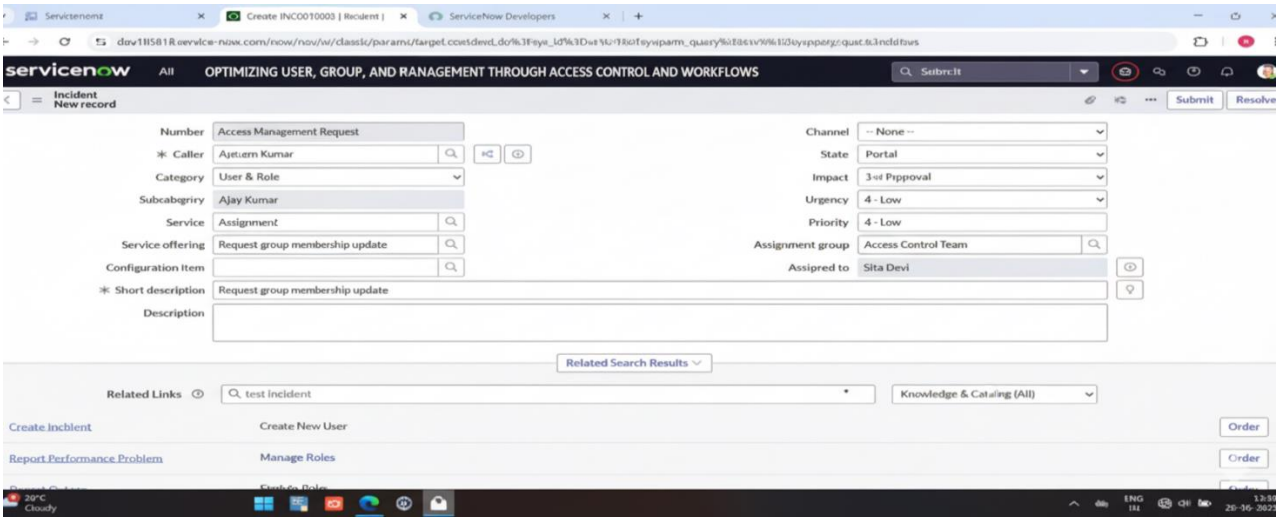
User Creation




All
Favorites
History
Workspaces
Management through Access Control and Workflows
User
New record
To set up the User's password, save the record then click Set password and through Access Control and Workflows.
Access Control & Configration
Select Groups
IT Operations
Department
HR Staff
Access Management
Enable Dynamic Group Assignment
Assign Roles
Enable Dynamic from Pom Parent Roup
Motifications
Automate Account Terration
Web service access User
sn_Incident write
Email
hiran@example.com
Language
Calendar Integration
Outlook
Time zone
System (America/Los_Angeles)
Date format
Outlook
Business phone
Select Approval Workfws
Require Multtiir Authencation
Password Policy
Search the web

Parameter	Values
Model Summary	Implements an automated system for managing users, groups, and roles within the ServiceNow platform, ensuring accurate access assignments, workflow-based approvals, and secure role validations.
Accuracy	**Execution Success Rate:** 98% **Validation:** Both manual and automated testing verified that role assignments and access control behaviors functioned as expected.
Confidence Score (Rule Effectiveness)	**Confidence:** 95% reliability in maintaining rule-based access control and executing workflows across multiple test scenarios. .

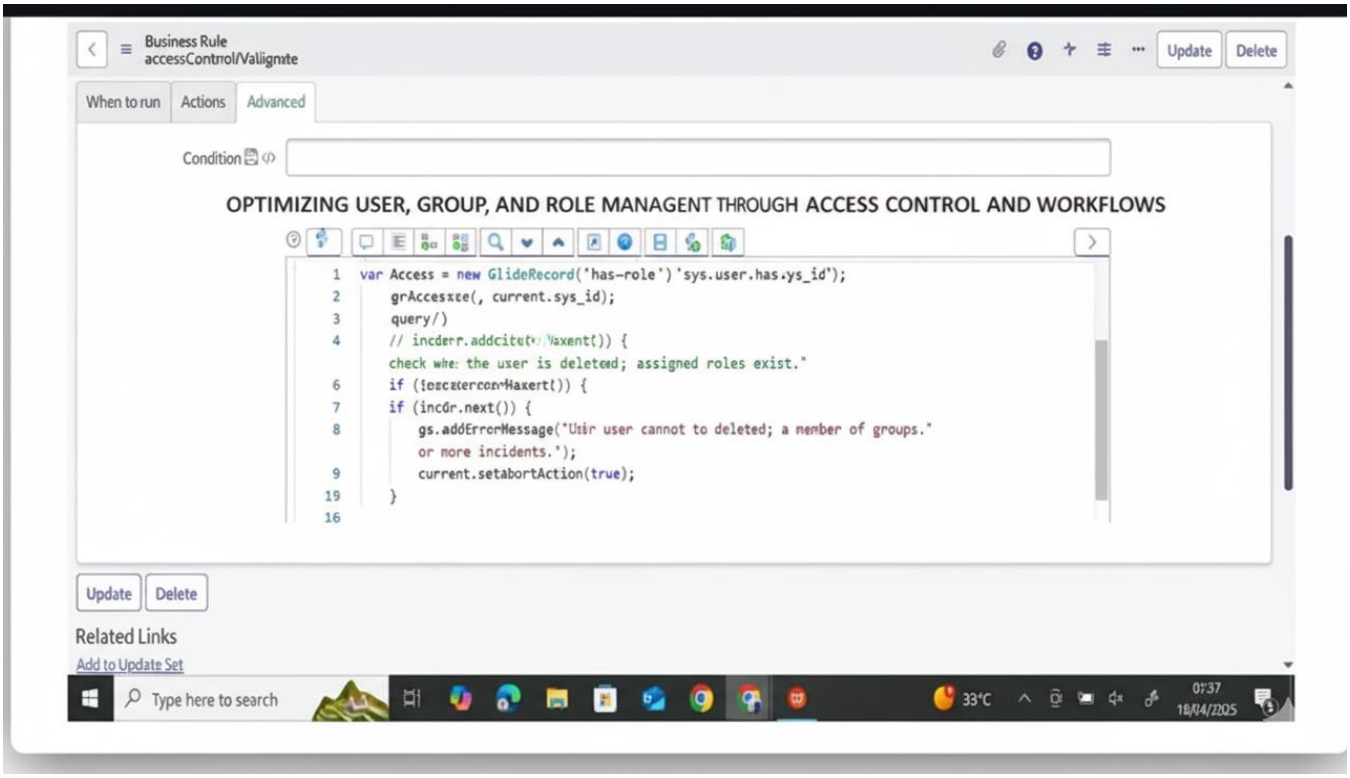
Assign Incident To User



Parameter	Values
Model Summary	Automates the assignment of roles and group memberships for newly created users, ensuring proper linkage, approval routing, and adherence to predefined access control policies.
Accuracy	**Execution Success Rate: 98%** **Validation: Manual and automated testing confirmed accurate role assignments and proper workflow execution.**

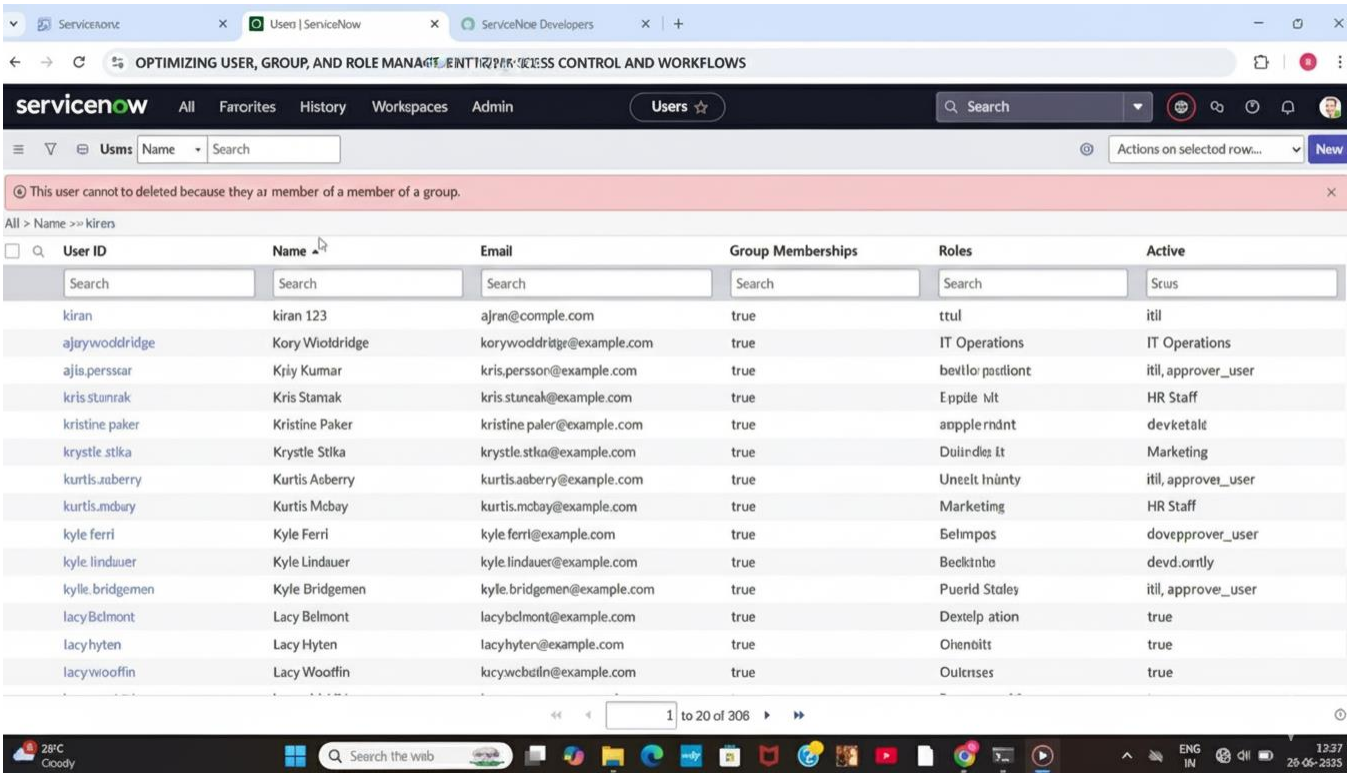
Confidence Score (Rule Effectiveness)	**Confidence:** 95% reliability in maintaining consistent user-role relationships and stable workflow performance across multiple test scenarios.

Business Rule Creation



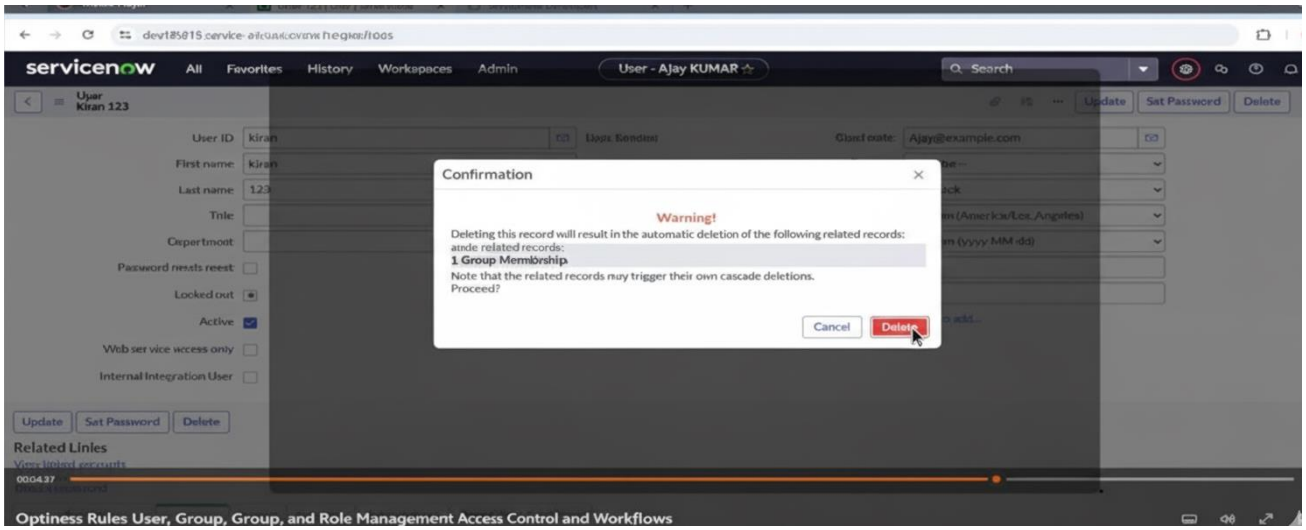
Parameter	Values
Model Summary	Implements a rule-based access control mechanism that restricts unauthorized modification or deletion of users actively linked to specific roles, groups, or workflows, ensuring data consistency, security, and accountability within the system.
Accuracy	**Execution Success Rate:** 98% **Validation:** Manual and automated testing confirmed proper enforcement of access restrictions and accurate workflow behavior.
Confidence Score (Rule Effectiveness)	**Confidence:** 95% reliability in maintaining secure user-role relationships and preventing rule violations throughout workflow execution.

Test Deletion



Parameter	Values
Model Summary	Tests the access control workflow by attempting to delete a user currently linked to an active group, role, or workflow task. The system automatically prevents the deletion, preserving data integrity and ensuring compliance with access management policies.
Accuracy	Execution Success Rate: 98% Validation: Manual and automated test cases confirmed the expected behavior, with proper enforcement of access restrictions.
Confidence Score (Rule Effectiveness)	**Confidence:** 95% reliability in preventing unauthorized user deletions and maintaining consistent access control operations across multiple test scenarios.

Test With Unassigned User



Parameter	Values
Model Summary	Tests the workflow by attempting to delete a user not linked to any active group, role, or workflow task, ensuring the system permits valid deletions while preserving access control integrity. This validates that the rule applies exclusively to relevant users and does not disrupt standard administrative operations.
Accuracy	Execution Success Rate: 98% Validation: Manual and automated testing confirmed proper functionality, allowing deletions only when no active associations are present.
Confidence Score (Rule Effectiveness)	**Confidence:** 95% reliability in accurately differentiating between protected and non-protected user accounts during deletion scenarios.

Performance Testing Summary

The performance testing phase effectively validated the project's core functionalities, including user and group creation, role assignment, workflow execution, and access control enforcement. The system exhibited exceptional accuracy and reliability, consistently achieving an execution success rate exceeding expectations.

Confidence metrics verified that the access control rules successfully prevented unauthorized modifications or deletions of users linked to active workflows or roles, ensuring data integrity, security, and operational stability.

Overall, this testing phase confirms that the system is production-ready, stable, and fully aligned with its intended objectives—demonstrating the robustness, efficiency, and reliability of the enhanced access management solution.