Streamlining Ticket Assignment for Efficient Support Operations

Introduction

Modern support teams require secure and automated ticket routing to ensure that new tickets reach the appropriate experts without manual triage or visibility risks.This project implements a governed assignment model on a custom Operations Related table in ServiceNow, enforcing role-based Access Control List (ACL) rules and utilising Flow Designer to automatically assign records based on the *Issue* field.The configuration includes user, group, and role setup; table and field creation; ACL rule design; and two automated flows that route certificate-related and platform-related issues to their respective groups.

Included screenshots illustrate ACL configuration and both flows from end to end for quick verification and evaluation.

Project Overview

The proposed solution streamlines ticket handling by combining least-privilege ACL security with low-code automation that deterministically sets the *Assigned To* group for Operations-related records.All configurations are built using native ServiceNow administration and workflow capabilities, ensuring long-term maintainability, scalability, and auditability.

Problem Statement

Manual ticket assignment caused delays and inconsistent access to Operations records across different teams, leading to slower response times and unnecessary rework.

Additionally, there was no standardised automation for routing certificate or platform issues, and permissions were not properly restricted based on user roles.

Objectives

- Enforce least-privilege data access on the Operations Related table using role-based ACL rules.
- Automate ticket assignment so that Issue values automatically route records to

either the Certificates or Platform group without manual intervention.

- Provide evidence through screenshots and test records to validate both access control and ticket routing functionality.

Tools and Technologies Used

- ServiceNow Modules: Users, Groups, Roles, Tables, Access Control (ACL), Flow Designer / Workflow Studio
- Flow Designer Components: Record Triggers and Update Record Actions to set the Assigned To group dynamically

Tasks and Activities

1. **Create Users:** Navigate to All → User Administration → Users → New. Populate essential fields, submit, and set passwords if required.
2. **Create Groups:** Go to All → User Administration → Groups → New. Add members and attach appropriate roles for certificate and platform responsibilities.
3. **Create Roles:** Navigate to All → User Administration → Roles → New. Define distinct roles for Platform and Certificate operations.
4. **Create the Custom Table:** Go to System Definition → Tables → New. Set the label as "Operations Related" and add required fields, including the Issue choice list.
5. **Configure ACL Rules:** Navigate to System Security → Access Control (ACL) → New.
   - Set Type = Record
   - Define operations such as Read and Write for the table
   - Add the appropriate roles for each operation or field Repeat this configuration as necessary for all access operations.
6. **Implement Flow 1 (Certificates):** Create a flow in Flow Designer with a Record Trigger on the Operations Related table.
   - Condition: Issue = Regarding Certificates
   - Action: Update Record → Set Assigned To Group = Certificates
     Save and activate the flow.
7. **Implement Flow 2 (Platform)**: Create a second flow with a Record Trigger on the same table.
   - Condition: Issue in {Unable to login to platform, 404 Error, Regarding User expired}
   - Action: Update Record → Set Assigned To Group = Platform
     Save and activate the flow.
8. **Validation:** Impersonate users from each group to verify ACL enforcement. Create sample records to confirm that tickets are automatically assigned to the correct group based on the Issue value.

Workflow Summary

- **Flow1 –** “RegardingCertificates”
  Trigger: Record created or updated with Issue = Regarding Certificates
  → Action: Update Assigned To Group = Certificates
- **Flow 2** – “Regarding Platform”
  Trigger: Record created or updated with Issue in {Unable to login to platform, 404 Error, Regarding User expired}
  → Action: Update Assigned To Group = Platform

Results and Outcomes

The new system ensures that tickets are automatically routed to the correct team, eliminating manual hand-offs and improving response time for both certificate and platform incidents.

Role-based ACLs now prevent unauthorized access while maintaining usability for authorized users, supporting simplified audits and enhanced data security.

Conclusion

By combining ACL governance with automated flows, this project delivers secure and predictable ticket routing aligned with native ServiceNow best practices.The solution is scalable, allowing new Issue values or groups to be added easily in the future. The documented setup, supported by screenshots, ensures traceability from configuration to execution and enables repeatable, maintainable deployment.