Scope

The Ticket Assignment Optimization System aims to develop a comprehensive solution on the ServiceNow platform to streamline how support tickets are routed, assigned and managed. The system will allow incoming tickets to be automatically categorized, prioritized, and assigned to appropriate agents or teams based on skill, workload and SLA criteria. It will also feature real-time monitoring of queues, dashboards for agent workload, and customizable rules to meet the needs of different support organsations. Leveraging ServiceNow's capabilities, the system ensures a secure, scalable, and user-friendly experience.

The project focuses on improving ticket assignment efficiency, reducing hand-offs and mis-routing, and increasing support responsiveness. While the system will provide routing automation, workload balancing, and monitoring tools, it will **not** include features such as full chat-bot triage, external CRM integration beyond basic ticket channels, or automated resolution of tickets.

The primary scope is to empower the support organisation with a streamlined assignment engine, better visibility over ticket flows, and improved operational efficiency.

In-Scope Activities

Ticket Categorisation & Routing Logic: Configure categories, sub-categories, tags and business rules so tickets are routed automatically based on defined criteria.

Skill-Based Assignment Engine: Develop agent profiles with skills, certifications and availability; match tickets to agents or teams accordingly.

Workload Balancing Mechanism: Implement logic to monitor agent loads and distribute tickets to avoid overload or under-utilization.

SLA & Priority Handling: Enable assignment and escalation workflows that respect ticket priority, impact, and SLA thresholds.

Real-Time Monitoring & Dashboards: Build dashboards and reporting views showing unassigned tickets, assignment time, agent workloads, SLA risks and ticket aging.

User Interface Design: Create an intuitive, accessible UI for support agents and managers to review assignments, queues, dashboards and alerts, with minimal training.

PERFORMANCE & TESTING

Procedure or Implementation steps

Phase 1 : create user

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

Phase 2 : Creation of group

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

Phase 3 : Creation of Table

Step 1: Creation of ticket Table

1. Open service now.
2.Click on All >> search for tables
3.Select tables under system definition
4.Click on new
5.Fill the following details to create a new table
6. Click on submit

Step 2: Creation of Columns(Fields)

1. Near Columns Double click near insert a new row.
2. Give the details as

   Column label : Number

   Type : String

3. Double click on insert a new row again
4. Give the details as:

   Column label : Date

   Type : Date

5. Double click on insert a new row again
6. Give the details as:

   Column label : Amount

   Type : Integer

7. Double click on insert a new row again
8. Give the details as:

   Column label : Expense Details

   Type : String

   Max length : 800

Phase 4 : **Assign roles and users to certificate group**

1.Open service now.
2.Click on All >> search for tables
3.Select tables under system definition
4.Select the certificates group
5.Under group members
6.Click on edit
7.Select Katherine Pierce and save
8.Click on roles
9.Select Certification_role and save

Phase 6 :**Assign roles & users to platform group**

1.Open service now.
2.Click on All >> search for tables
3.Select tables under system definition
4.Select the platform group
5.Under group members
6.Click on edit
7.Select Manne Niranjan and save
8.Click on roles
9.Select Platform_role and save

Phase 7 : Assign role to table

1.Open service now.
2.Click on All >> search for tables
3.Select operations related table
4.Click on the Application Access
5.Click on u_operations_related read operation
6.Click on the profile on top right side
7.Click on elevate role
8.Click on security admin and click on update
9.Under Requires role
10.Double click on insert a new row
11.Give platform role
And add certificate role
12.Click on update
13.Click on u_operations_related write operation
14.Under Requires role
15.Double click on insert a new row
16.Give platform role
And add certificate role

Phase 8 : **Create ACL**

1.Open service now.
2.Click on All >> search for ACL
3.Select Access Control(ACL) under system security
4.Click on new
5.Fill the following details to create a new ACL
6.Scroll down under requires role
7.Double click on insert a new row
8.Give admin role
9.Click on submit
10Similarly create 4 acl for the following fields

Phase 9:**Create a Flow to Assign operations ticket to group**

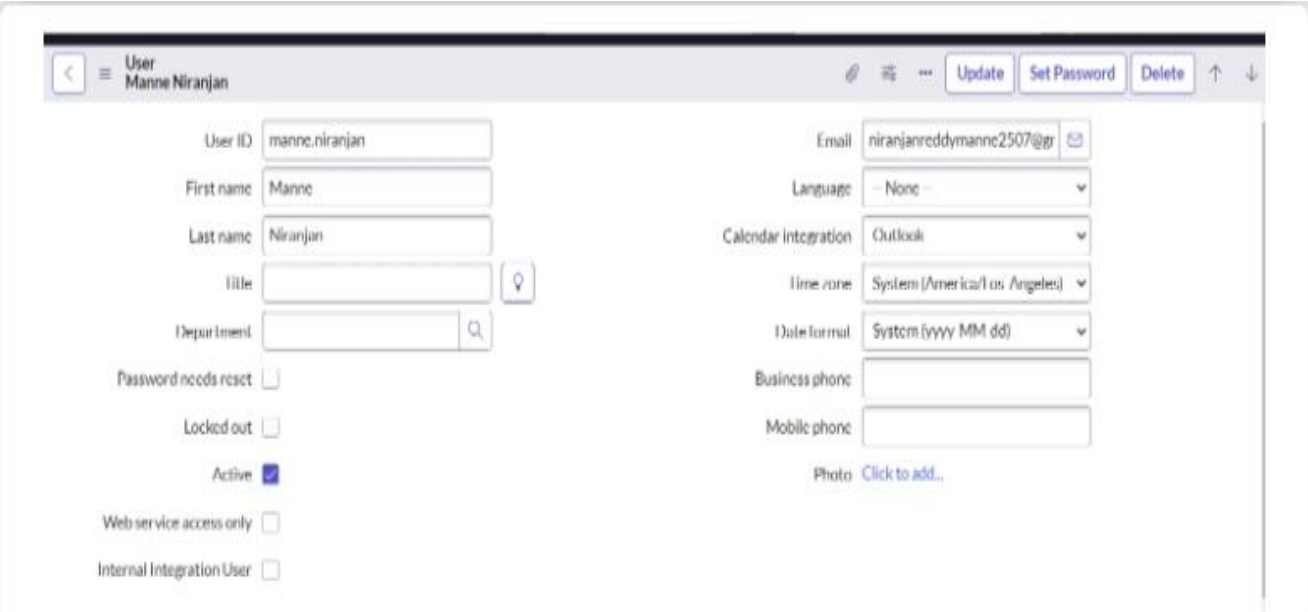
1.Open service now.
2.Click on All >> search for Flow Designer
3.Click on Flow Designer under Process Automation.
4.After opening Flow Designer Click on new and select Flow.
5.Under Flow properties Give Flow Name as " Regarding Certificate Application should be Global.
6.Select Run user as " System user " from that choice.
7.Click on Submit.

Create a Flow to Assign operations ticket to Platform group

1.Open service now.
2.Click on All >> search for Flow Designer
3.Click on Flow Designer under Process Automation.
4.After opening Flow Designer Click on new and select Flow.
5.Under Flow properties Give Flow Name as " Regarding Platform ".
6.Application should be Global.
7.Select Run user as " System user " from that choice.
8.Click on Submit.
Click on Activate.

Screenshots:

Phase 1 : Creation of New users



Phase 2 :

1. Creation of group

2 . Create a table

Column label	Type	Reference	Max length	Default value	Display
Created by	String	(empty)	40		false
Created	Date/Time	(empty)	40		false
Sys ID	Sys ID (GUID)	(empty)	32		false
Updates	Integer	(empty)	40		false
Updated by	String	(empty)	40		false
Updated	Date/Time	(empty)	40		false
Assigned to group	Reference	Group	40		false
Assigned to user	Reference	User	32		false
Comment	String	(empty)	40		false
Issue	String	(empty)	40		false
Name	String	(empty)	40		false
Priority	String	(empty)	40		false
Service request No	String	(empty)	40	javascript:getNextObjNumberPadded();	false
Ticket raised Date	Date/Time	(empty)	40		false
Insert a new row...					

3 .. Assign role to table

Access Control
u_operations_related

Update Delete

Definition

Access Control Rules allow access to the specified resource if all three of these checks evaluate to true:
1. The user has one of the roles specified in the **Role** list, or the list is empty.
2. Conditions in the **Condition** field evaluate to true, or conditions are empty.
3. The script in the **Script** field (advanced) evaluates to true, or sets the variable "answer" to true, or is empty.

The three checks are evaluated independently in the order displayed above.

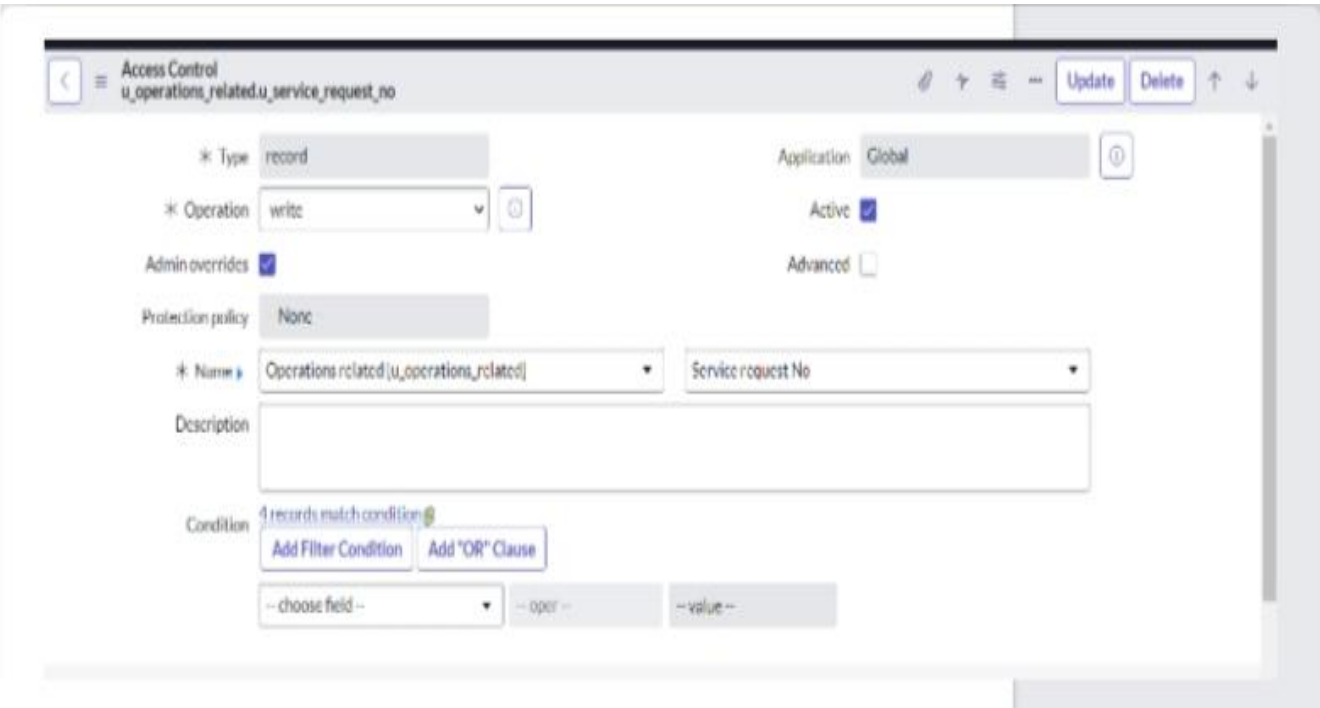
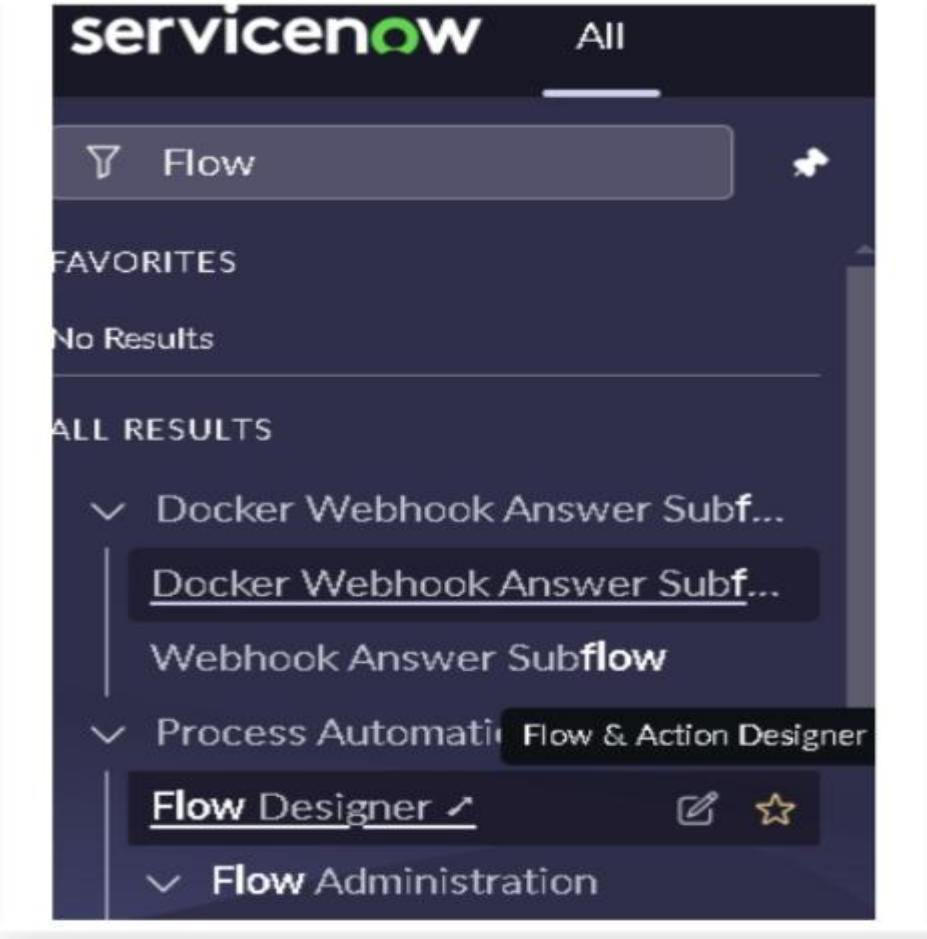
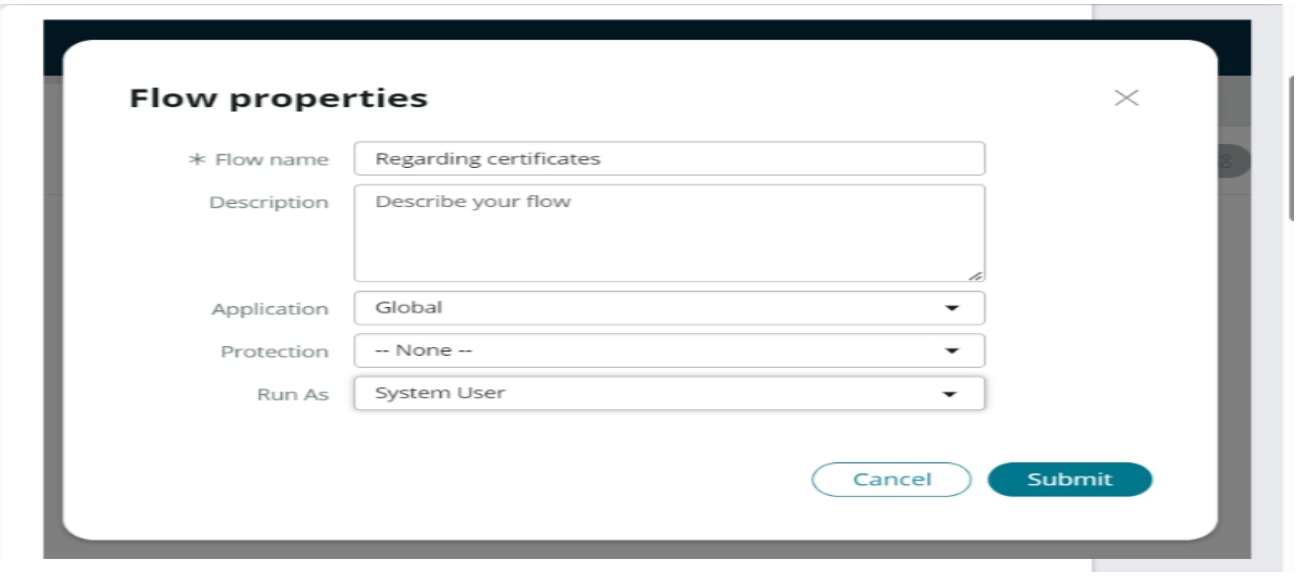
More Info

Requires role

1 to 3 of 3

Role
u_operations_related_user
Platform_role
Certification_role
Insert a new row...

4.. Create ACL


Access Control
u_operations_related.u_service_request_no
Update
Delete
Type
record
Application
Global
Operation
write
Active
Admin overrides
Advanced
Protection policy
None
Name
Operations related [u_operations_related]
Service request No
Description
Condition
1 records match condition
Add Filter Condition
Add "OR" Clause
-- choose field --
-- oper --
-- value --

Phase 3 : Create a Flow to Assign operations ticket to group