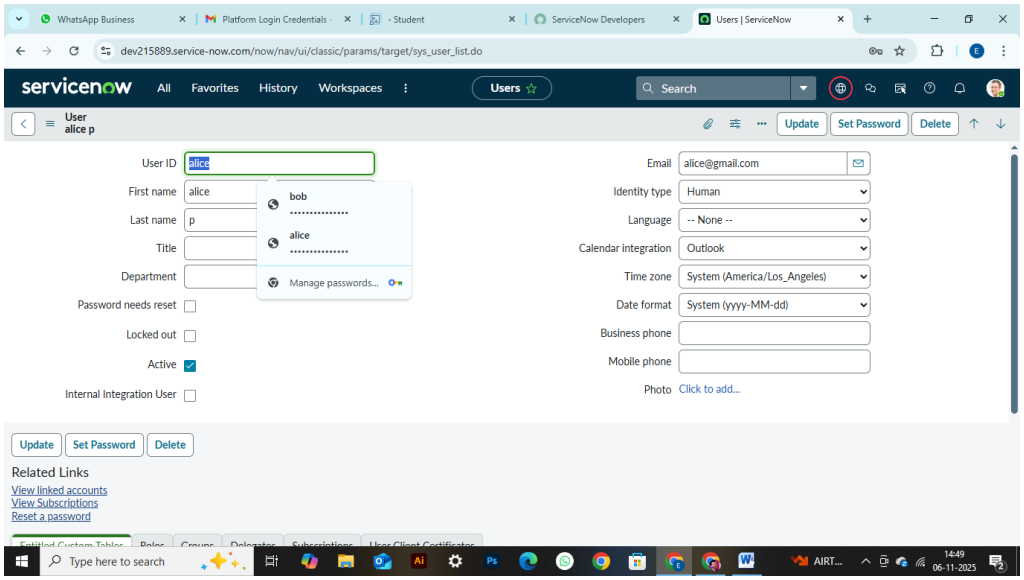
1. Users

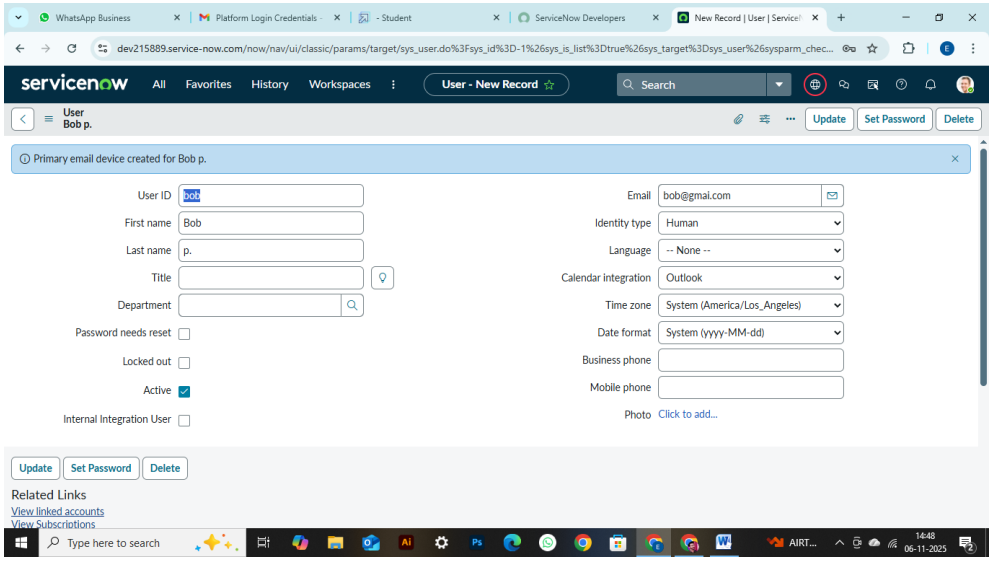
The first step in the implementation is the creation of user accounts within the ServiceNow platform. Each user profile contains critical information such as the user's name, email address, department, and user ID. This data helps in uniquely identifying each person in the system. Users can represent employees, team members, or administrators who require access to perform their duties.

Creating users is done through the User Table (sys_user) in ServiceNow. Administrators can either manually create users or import them from an existing employee database. Each user entry is verified before being activated in the system. Properly managing user records ensures accountability and a clear structure for assigning access rights and responsibilities.

1. Create the alice user:



2. Create the bob user :

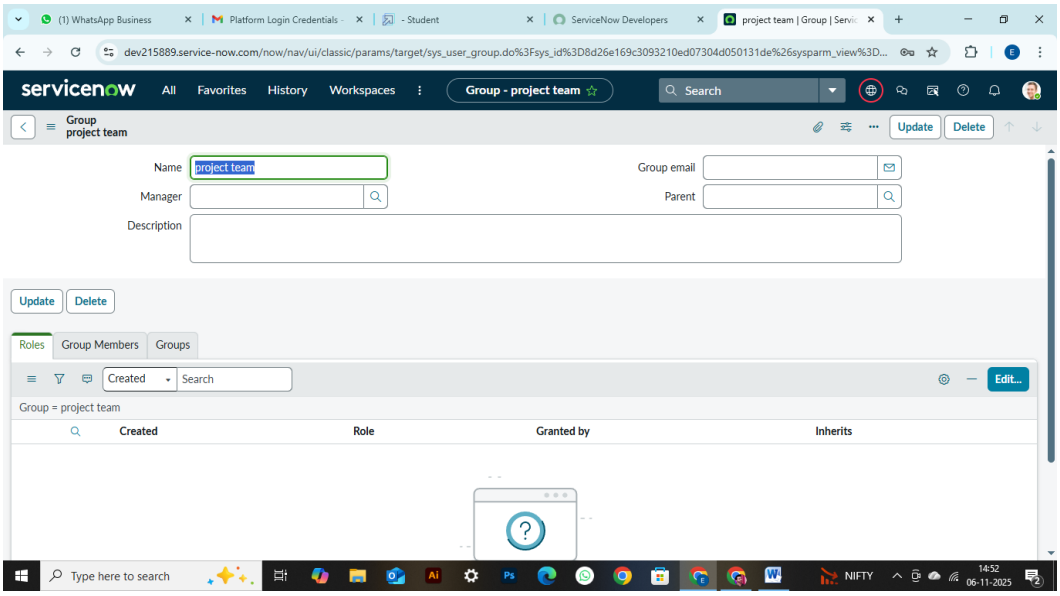


2.Groups:

Groups are essential for managing multiple users with similar job roles or project responsibilities. A **group** acts as a logical collection of users who can share access permissions, tasks, or projects. For example, all team members working on a particular project can be added to one group called “Project A Team.”

In ServiceNow, groups are stored in the **sys_user_group** table. When a group is created, it becomes easier to assign roles or tickets collectively instead of assigning them individually. Groups also play a crucial role in workflows where an entire department, such as “IT Support,” needs to receive and resolve incident tickets.

1. Create the Groups:

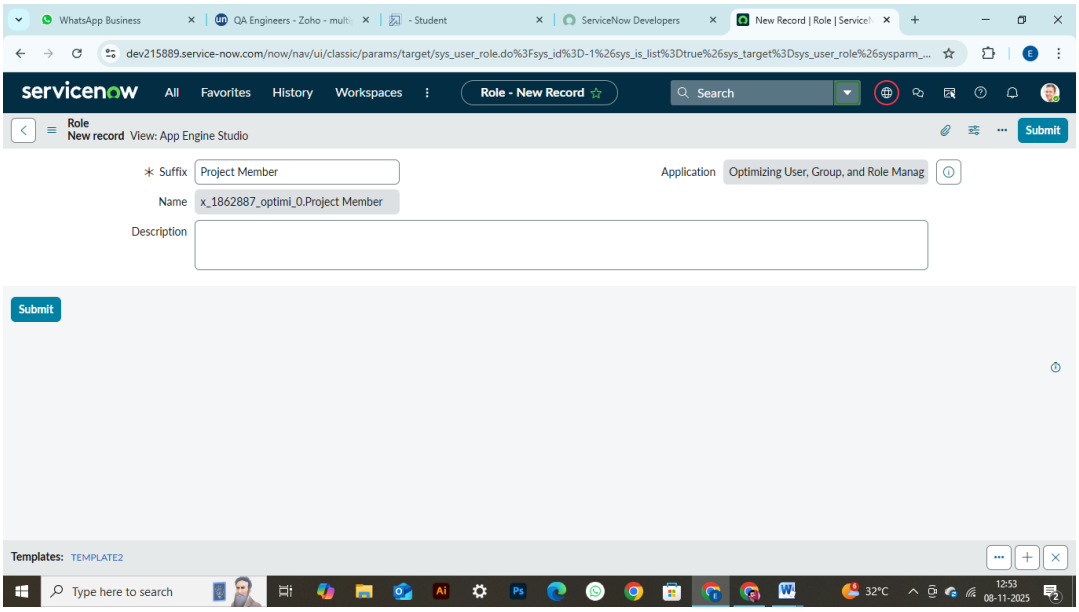


3.Roles:

Roles define the **level of access and privileges** that a user or group has within the system. Each role is associated with specific permissions that control what actions a user can perform. Examples include roles like *admin, itil (IT Service Management), hr_admin*, and *project_manager*.

By assigning the correct roles, administrators ensure that sensitive data and operations are protected. For instance, an admin can create and modify records, whereas a project member may only view or update assigned tasks. Roles are stored in the **sys_user_role** table, and multiple roles can be linked to one user depending on their function.

1. Create the Roles:

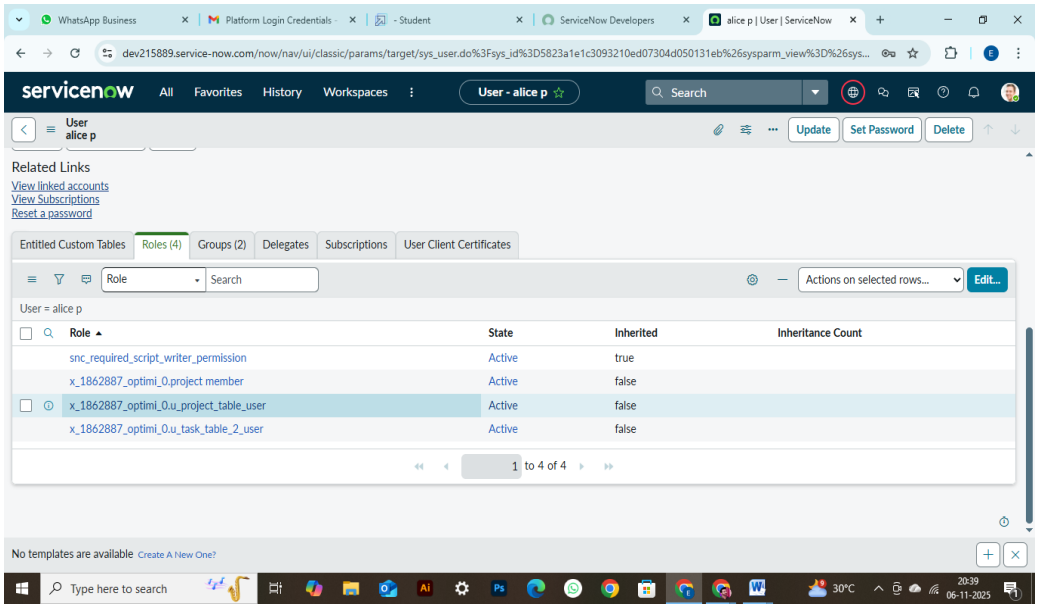


4.Assign Users to Groups:

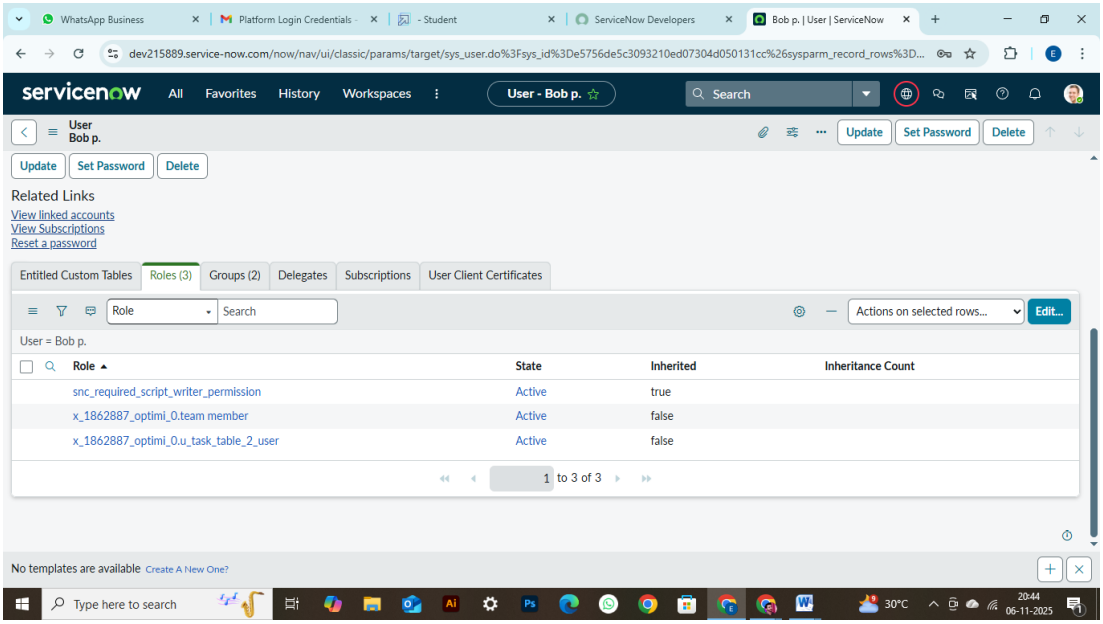
Once users and groups are created, the next step is to **assign users to their respective groups**. This helps organize members efficiently according to projects or departments. For example, *Alice* and *Bob* can be added to the *Development Team* group.

This assignment simplifies task management and approval processes. When an incident or project task is created, it can be automatically assigned to a specific group rather than an individual. The system uses this mapping to route workflows efficiently, improving team collaboration and reducing response times.

1. **Assign Roles to Alice User :**



2.Assign Roles to Bob User :

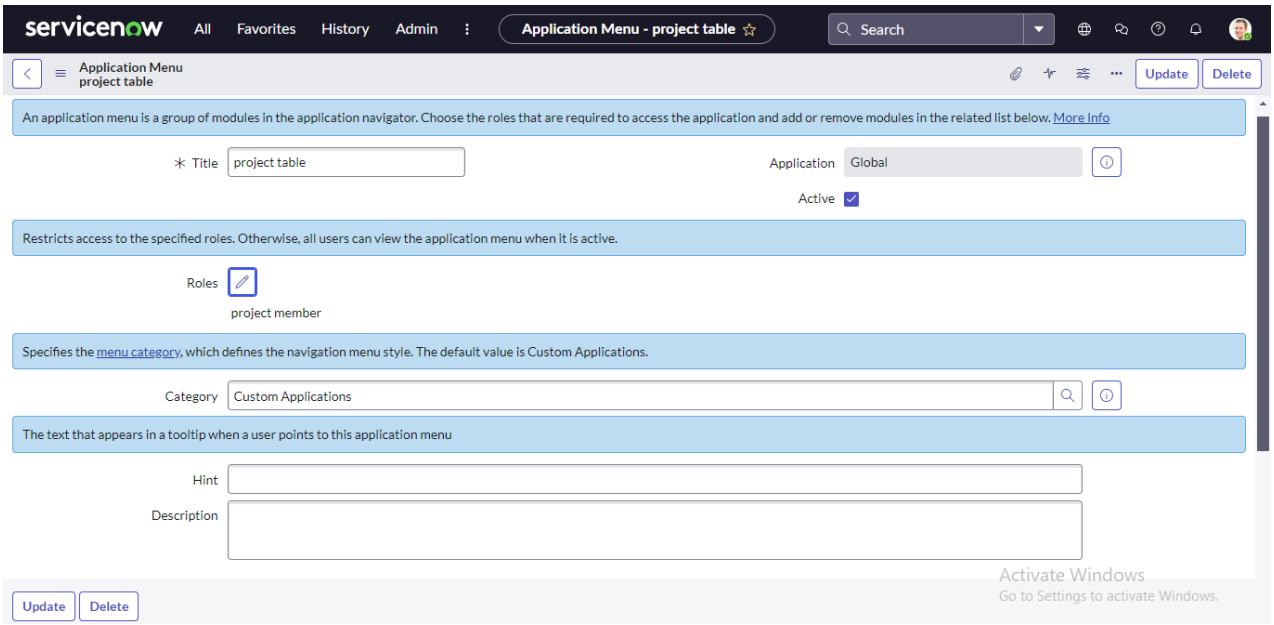


5.Application Access

The **Application Access** module defines which users, roles, or groups can access specific applications within the ServiceNow environment. By default, not every user can access all applications. Administrators configure access restrictions at the application level to safeguard sensitive modules.

This step helps prevent misuse and unauthorized entry into modules like HR, Finance, or IT Service Management. Assigning appropriate application access enhances security and ensures that users only interact with data relevant to their duties.

1.Assign table access to application:

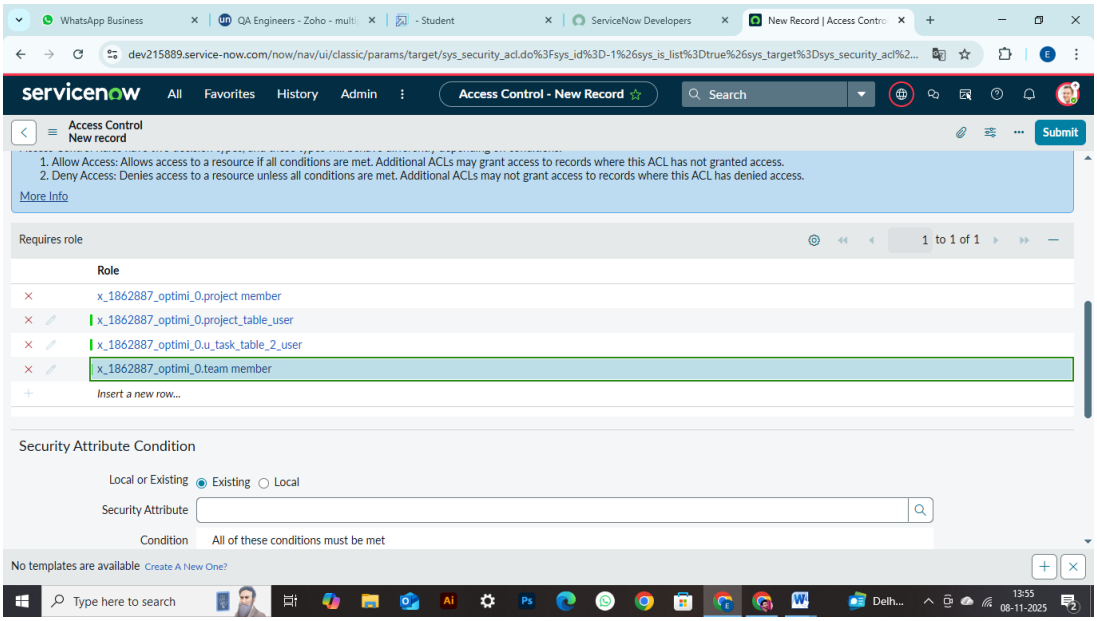


6. Assign Table Access to Application :

In this step, administrators configure **table-level access controls** to ensure proper data protection. ServiceNow applications often contain multiple tables (like `incident`, `task`, or `request`), and each table may have sensitive information.

By assigning access to specific tables, administrators ensure that users can only read, write, or update records that pertain to their work. For instance, a project member can view their own tickets but not modify another team's data. This fine-grained access management aligns with data confidentiality standards.

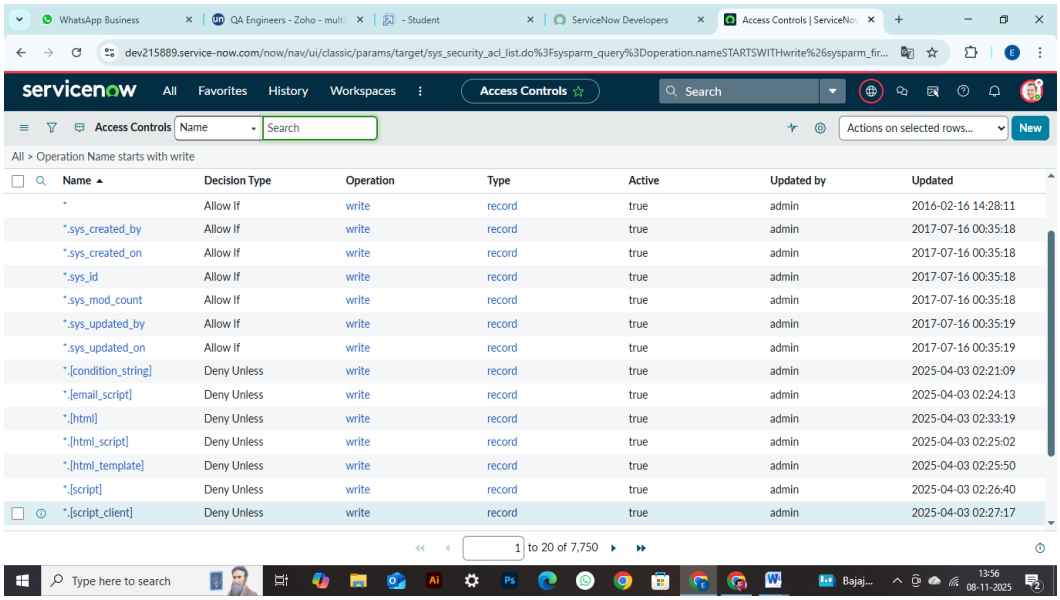
1.**Create ACL:**



7. Access Control List (ACL)

Access Control Lists (ACLs) are one of the most powerful features in ServiceNow. They provide detailed control over what data a user can view or modify at the **record or field level**. ACLs evaluate user roles, conditions, and scripts before granting access to a record.

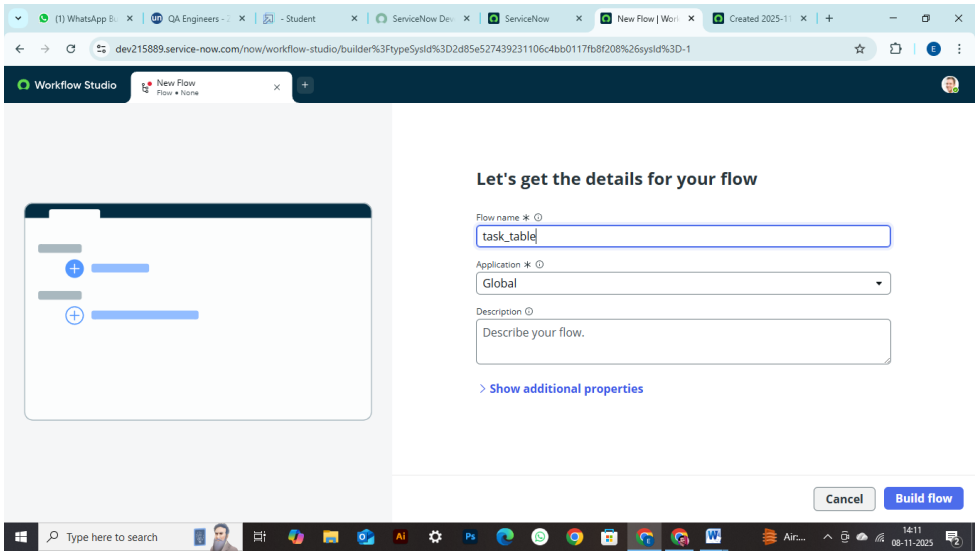
For example, an ACL rule can be set so that only users with the *manager* role can approve requests, while others can only view them. Implementing ACLs ensures system-wide data protection and adherence to organizational policies.



8.Flows:

ServiceNow's **Flow Designer** is used to automate business processes without the need for coding. A flow is a series of actions that are triggered based on certain conditions. This automation reduces manual workload and increases consistency in handling repetitive tasks.

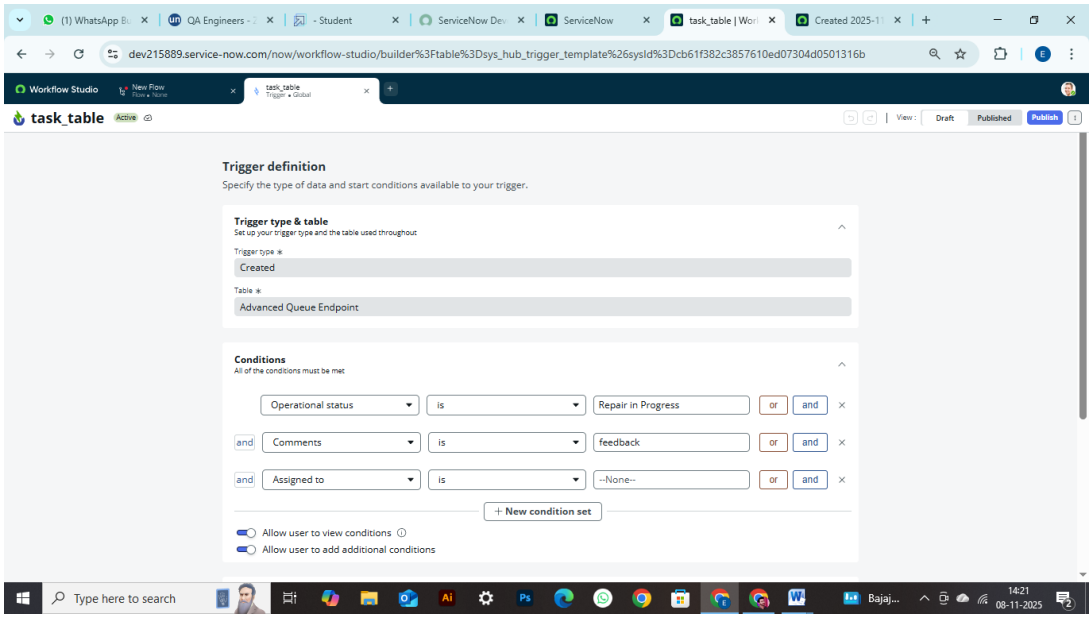
For example, when a new user joins the organization, a flow can automatically create their account, assign roles, and notify the admin. The drag-and-drop interface in Flow Designer makes it easy to design, test, and manage workflows seamlessly.



9. Create a Flow to Assign Operations Ticket to Group:

In this implementation, a specific flow is created to **automatically assign Operations tickets to a group**. When a new ticket is generated (for example, a server issue or software bug), the system triggers the flow, which checks predefined conditions and routes the ticket to the appropriate group, such as "IT Operations."

This automation ensures that no ticket is left unattended and that the correct team handles the issue immediately. It enhances productivity, reduces delays, and ensures smooth coordination across teams.


dev215889.service-now.com/now/workflow-studio/builder%3Ftable%3Dsys_hub_trigger_template%26sysId%3Dcb61f382c3857610ed07304d0501316b
Workflow Studio
task_table
Active
Draft
Published
Publish
Trigger definition
Specify the type of data and start conditions available to your trigger.
Trigger type & table
Set up your trigger type and the table used throughout
Trigger type *
Created
Table *
Advanced Queue Endpoint
Conditions
All of the conditions must be met
Operational status
is
Repair in Progress
or
and
and
Comments
is
feedback
or
and
and
Assigned to
is
--None--
or
and
+ New condition set
Allow user to view conditions
Allow user to add additional conditions
Type here to search
14:21
08-11-2025