

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:

The screenshot shows the ServiceNow 'Users' page. The breadcrumb trail is 'Users | ServiceNow'. The page title is 'User alice p'. The form contains the following fields:

- User ID:
- First name:
- Last name:
- Title:
- Department:
- Identity type:
- Language:
- Calendar integration:
- Time zone:
- Date format:
- Business phone:
- Mobile phone:
- Photo: [Click to add...](#)

Buttons: Update, Set Password, Delete

Related Links: [View linked accounts](#), [View Subscriptions](#), [Reset a password](#)

2. Create the bob user :

The screenshot shows the ServiceNow 'User - New Record' page. The breadcrumb trail is 'User - New Record | User | ServiceNow'. The page title is 'User Bob p'. The form contains the following fields:

- User ID:
- First name:
- Last name:
- Title:
- Department:
- Identity type:
- Language:
- Calendar integration:
- Time zone:
- Date format:
- Business phone:
- Mobile phone:
- Photo: [Click to add...](#)

Buttons: Update, Set Password, Delete

Related Links: [View linked accounts](#), [View Subscriptions](#)

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:

The screenshot shows the ServiceNow interface for creating a group. The browser address bar shows the URL: `dev215889.service-now.com/now/nav/ui/classic/params/target/sys_user_group.do%3Fsys_id%3D8d26e169c3093210ed07304d050131de%26sysparm_view%3D...`. The page title is "Group - project team". The form has the following fields:

- Name:
- Group email:
- Manager:
- Parent:
- Description:

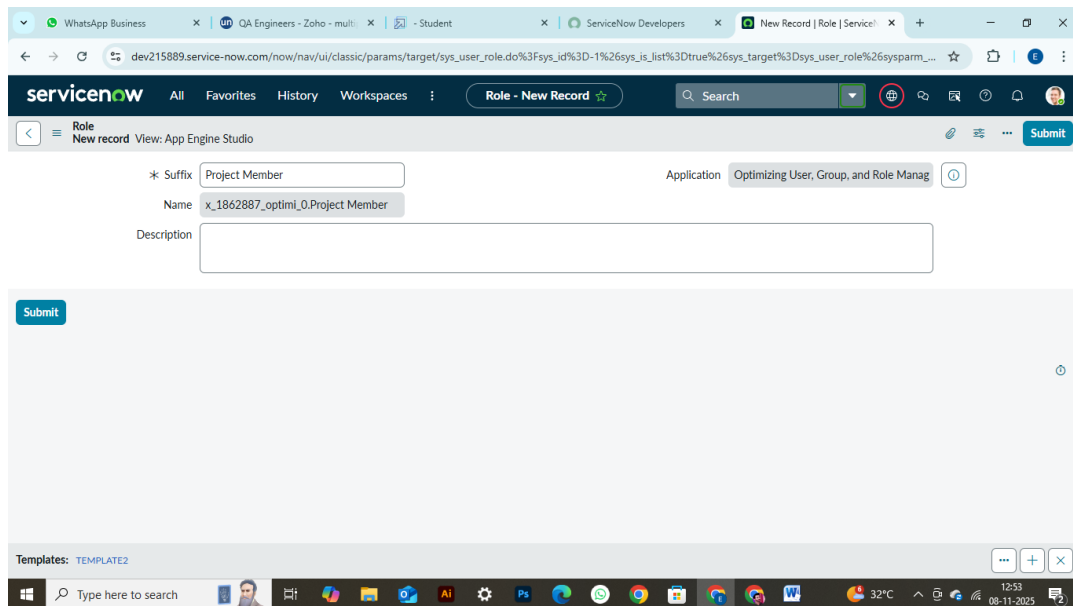
Below the form are buttons for "Update" and "Delete". There are three tabs: "Roles", "Group Members", and "Groups". The "Roles" tab is selected, showing a table with the following columns: "Created", "Role", "Granted by", and "Inherits". The table is currently empty.

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:

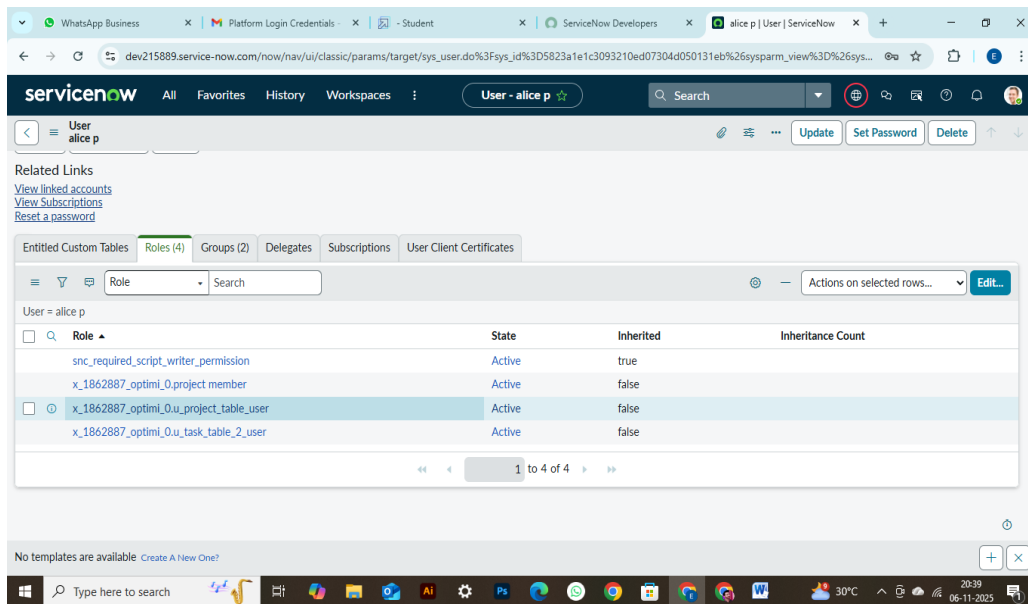


4.Assign Users to Groups:

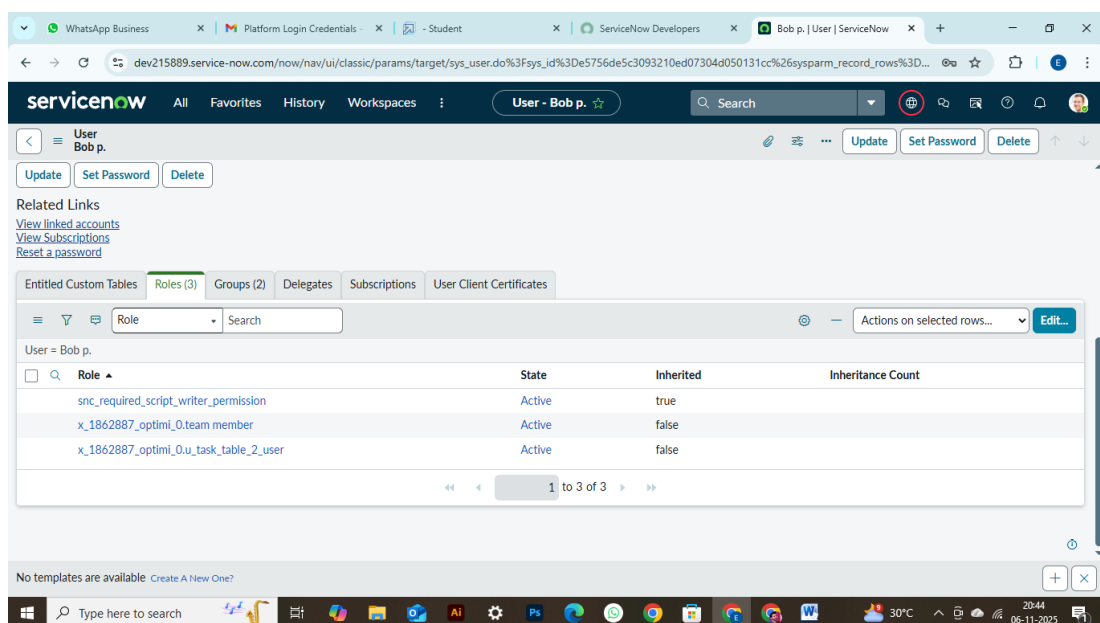
Once users and groups are created, the next step is to **assign users to their respective groups**. This helps organize members efficiently according to projects or departments. For example, *Alice* and *Bob* can be added to the *Development Team* group.

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:

The screenshot shows the ServiceNow interface for configuring an application menu. The header includes the ServiceNow logo, navigation tabs (All, Favorites, History, Admin), and a search bar. The main title is 'Application Menu - project table'. Below the title, there's a description: 'An application menu is a group of modules in the application navigator. Choose the roles that are required to access the application and add or remove modules in the related list below. [More Info](#)'. The form fields include: 'Title' (project table), 'Application' (Global), 'Active' (checked), 'Roles' (project member), 'Category' (Custom Applications), 'Hint' (empty), and 'Description' (empty). At the bottom, there are 'Update' and 'Delete' buttons. A watermark 'Activate Windows Go to Settings to activate Windows.' is visible in the bottom right corner.

servicenow All Favorites History Admin : Application Menu - project table

Search

< Application Menu project table

Update Delete

An application menu is a group of modules in the application navigator. Choose the roles that are required to access the application and add or remove modules in the related list below. [More Info](#)

* Title project table Application Global

Active ☒

Restricts access to the specified roles. Otherwise, all users can view the application menu when it is active.

Roles project member

Specifies the [menu category](#), which defines the navigation menu style. The default value is Custom Applications.

Category Custom Applications

The text that appears in a tooltip when a user points to this application menu

Hint

Description

Update Delete

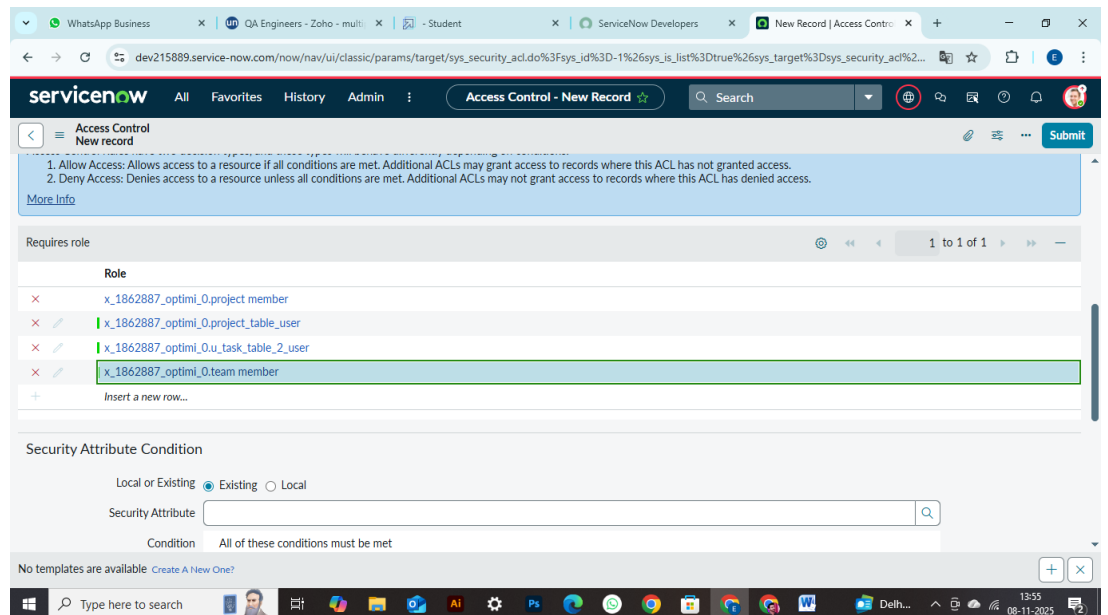
Activate Windows
Go to Settings to activate Windows.

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.

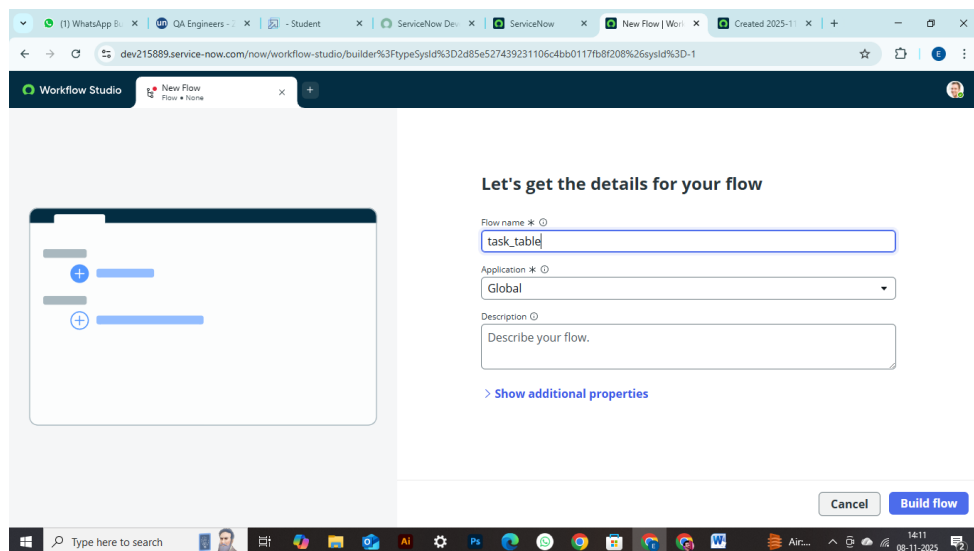
For example, an ACL rule can be set so that only users with the *manager* role can approve requests, while others can only view them. Implementing ACLs ensures system-wide data protection and adherence to organizational policies.

Name	Decision Type	Operation	Type	Active	Updated by	Updated
*	Allow If	write	record	true	admin	2016-02-16 14:28:11
*.sys_created_by	Allow If	write	record	true	admin	2017-07-16 00:35:18
*.sys_created_on	Allow If	write	record	true	admin	2017-07-16 00:35:18
*.sys_id	Allow If	write	record	true	admin	2017-07-16 00:35:18
*.sys_mod_count	Allow If	write	record	true	admin	2017-07-16 00:35:18
*.sys_updated_by	Allow If	write	record	true	admin	2017-07-16 00:35:19
*.sys_updated_on	Allow If	write	record	true	admin	2017-07-16 00:35:19
*.[condition_string]	Deny Unless	write	record	true	admin	2025-04-03 02:21:09
*.[email_script]	Deny Unless	write	record	true	admin	2025-04-03 02:24:13
*.[html]	Deny Unless	write	record	true	admin	2025-04-03 02:33:19
*.[html_script]	Deny Unless	write	record	true	admin	2025-04-03 02:25:02
*.[html_template]	Deny Unless	write	record	true	admin	2025-04-03 02:25:50
*.[script]	Deny Unless	write	record	true	admin	2025-04-03 02:26:40
*.[script_client]	Deny Unless	write	record	true	admin	2025-04-03 02:27:17

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.

