PERFORMANCE TESTING

Date	01/11/2025
Team ID	NM2025TMID02331
Project Name	Lease management

User creation :

In ServiceNow, users represent the people who can log in, access, and perform various actions based on their assigned roles. Creating users is an essential part of setting up the system and managing access control. Each user record stores details such as username, email, roles, and department, ensuring that only authorized personnel have access to specific modules and data.

User creation in ServiceNow is an important administrative task that involves adding new users to the system and defining their access privileges. Each user in ServiceNow represents an individual who can log in and perform actions based on their assigned roles and permissions. This process ensures proper access control, data security, and smooth workflow management within the platform.

To create a new user in ServiceNow, the administrator must first log in with an account that has sufficient permissions, such as one with the **user_admin** role. Once logged in, the administrator can navigate to the **User Administration** module through the Application Navigator. By typing **"Users"** in the search box and selecting **User Administration → Users**, the system displays a list of all existing users. To add a new one, the administrator clicks the **"New"** button, which opens a form where all relevant user details can be entered.

In the user creation form, the administrator fills out essential fields such as **User ID**, **First Name**, **Last Name**, **Email**, and **Password**. Additional optional fields like **Department** and **Manager** can also be specified to organize users according to the organization's hierarchy. It is also important to ensure that the **Active** checkbox is selected, allowing

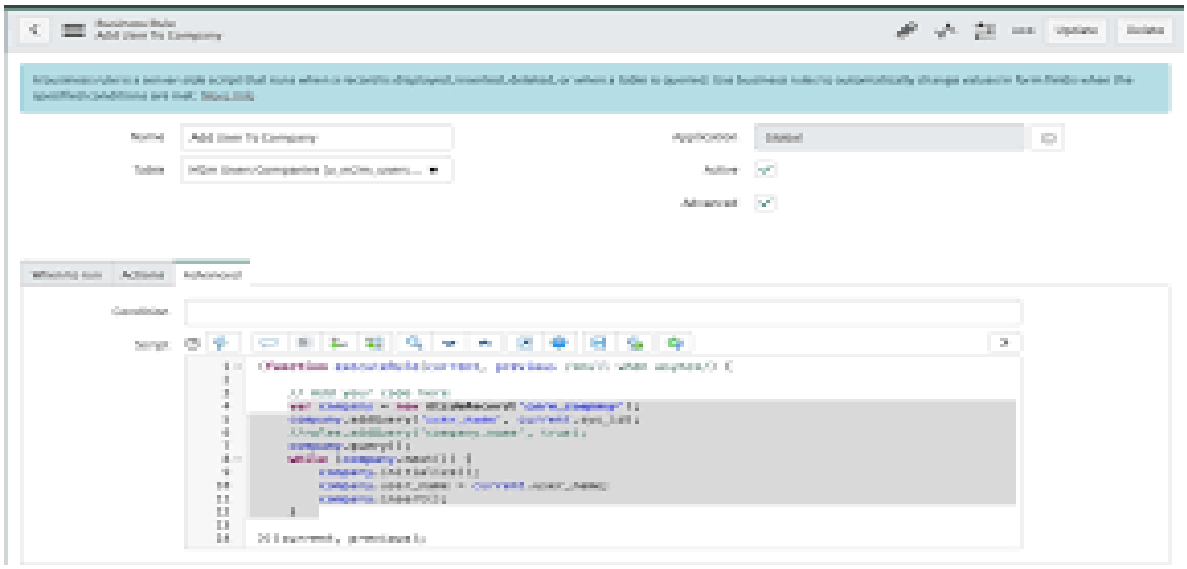
Assign Incident To User :

Assigning an incident to a user in ServiceNow is a key activity in the incident management process. It ensures that reported issues are directed to the appropriate personnel or support group for resolution. This process helps improve response time, accountability, and overall service efficiency within the organization.

In ServiceNow, incidents are created whenever a user reports an issue or disruption in a service. Once an incident is logged, it needs to be assigned to a specific user or support group responsible for resolving it. The assignment process begins by navigating to the **Incident** module. Administrators or users with the **ITIL** or **incident_manager** role can access this module through the **Application Navigator** by typing

“Incident” in the search bar and selecting **Incident → All**. This displays a list of all existing incidents recorded in the system.

Business Rule Creation :



Business Rules in ServiceNow are server-side scripts that automatically run when records are inserted, updated, deleted, or queried. They are used to automate processes, enforce data consistency, and apply custom logic without requiring manual intervention. Business rules ensure that the system behaves according to organizational policies and workflow requirements, helping streamline operations and maintain data integrity.

To create a business rule in ServiceNow, an administrator must log in with appropriate permissions such as the **admin** or **business_rule_admin** role. Once logged in, the administrator navigates to the **System Definition** application in the **Application Navigator**. By typing **"Business Rules"** in the filter navigator and selecting **System Definition → Business Rules**, the system displays a list of all existing business rules configured in the instance.

To create a new one, the administrator clicks the **"New"** button. A form opens where details about the business rule must be entered. The **Name** field specifies the rule's title, which should describe its purpose clearly. The **Table** field defines which table the rule applies to, such as *Incident*, *Problem*, *Change Request*, or a custom table like *Lease*

Record. The **When to Run** section specifies when the rule should execute—before, after, async (asynchronously), or on display. Each option determines the timing of the script execution relative to database actions.

Test Deletion :

Test deletion in ServiceNow refers to the process of removing unwanted or outdated test cases and test suites from the system, particularly those created using the **Automated Test Framework (ATF)**. Over time, as applications evolve and new functionalities are introduced, older test cases may no longer be relevant or may become redundant. Deleting such tests helps maintain a clean and organized testing environment, ensuring that only valid and up-to-date test cases are retained for future validation.

To perform test deletion in ServiceNow, an administrator or a user with the necessary permissions (such as **admin** or **atf_test_admin**) must log into the instance. Once logged in, the user navigates to the **Automated Test Framework** module through the **Application Navigator** by typing "Test" in the search field. From the displayed options, the user selects either **Test Cases** or **Test Suites**, depending on what needs to be deleted. A list of existing tests appears, showing all the configured test cases and suites in the system.

The user can then open the specific test record intended for deletion. Inside the record, the **Delete** option can be accessed from the context menu or the form's header. When the delete option is selected, ServiceNow prompts a confirmation message to ensure that the deletion is intentional, as this action permanently removes the test record and any associated test steps or related data. Once confirmed, the test is permanently deleted from the system and can no longer be executed or referenced.

For example, in a **Lease Management System**, test deletion might be necessary when a workflow or module, such as "Lease Renewal

Notification," has been redesigned or replaced. The old test case linked to the outdated functionality can be deleted to avoid confusion during future testing cycles. This ensures that only relevant test cases aligned with the current business logic remain active in the system.