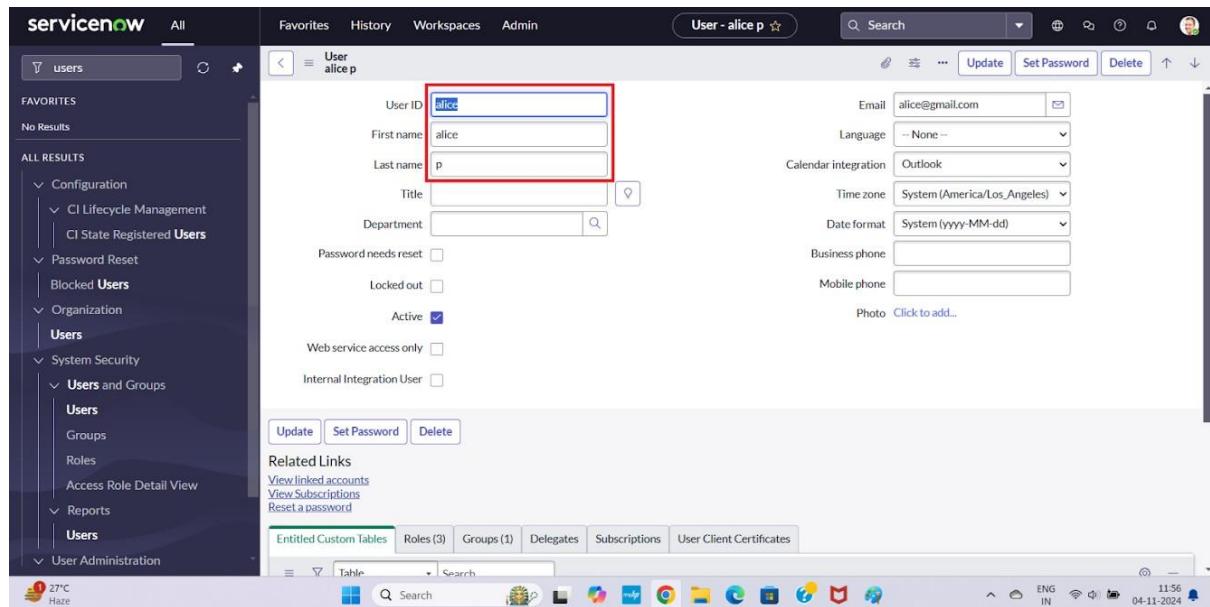


Performance and Testing

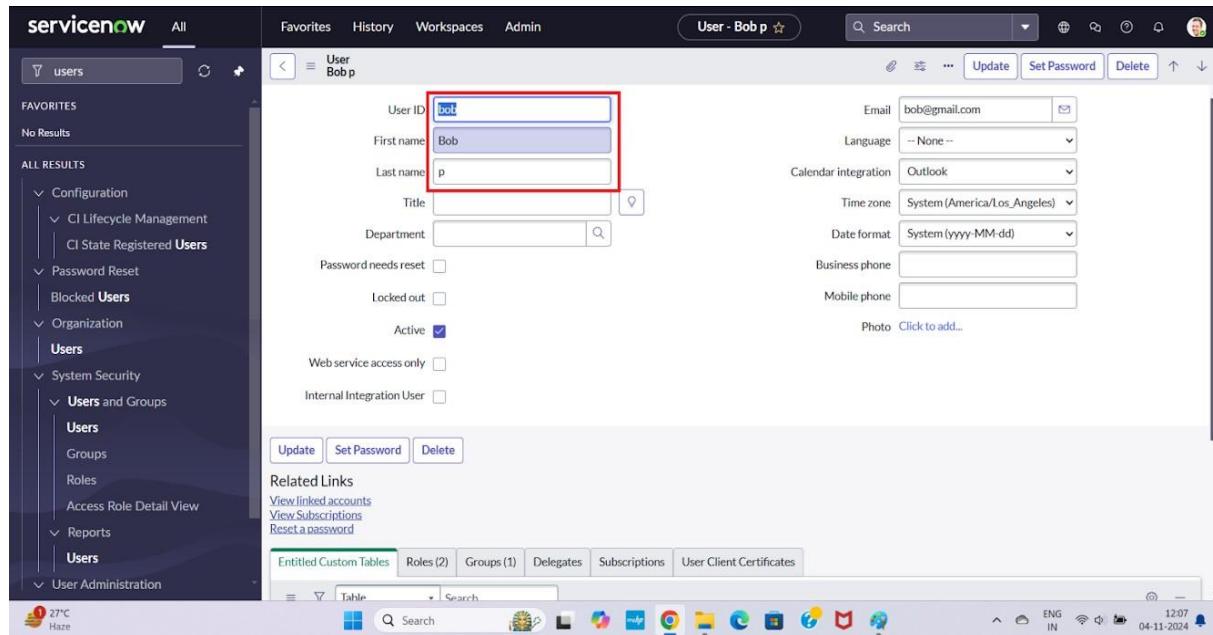
DATE	22 oct 2025
TEAM ID	NM2025TMID08298
PROJECT NAME	Optimizing User, Group, and Role Management with Access Control and Workflows
MAXIMUM MARK	4 Marks

MODEL PERFORMANCE TESTING

User Creation

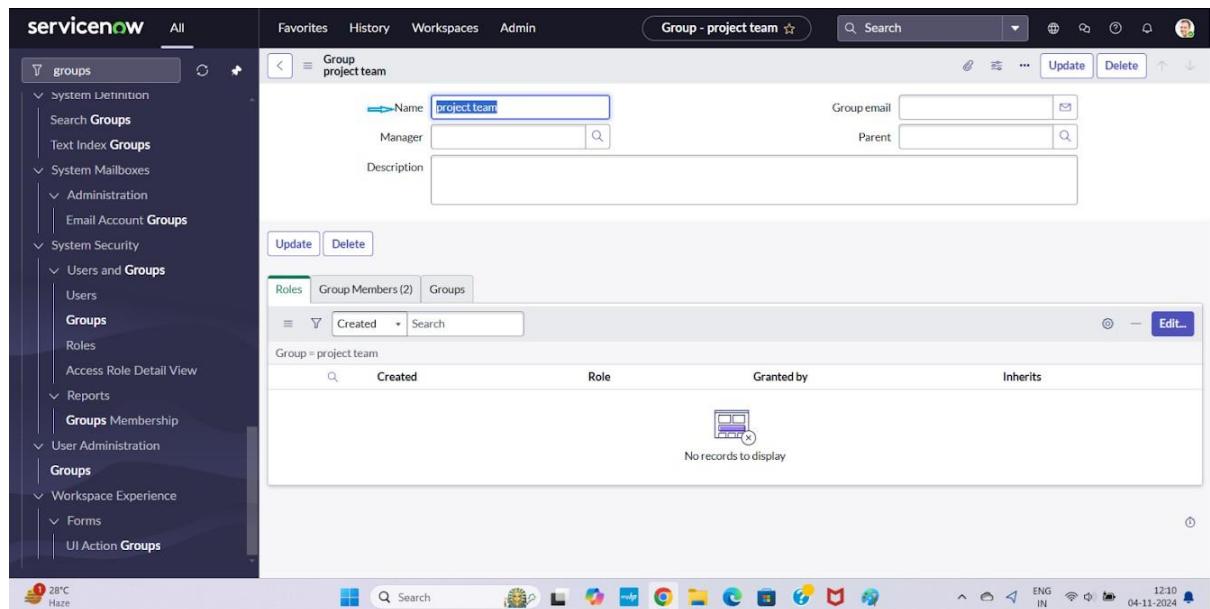


The screenshot shows the ServiceNow user creation interface. The left sidebar navigation bar includes sections like Configuration, Password Reset, Organization, and System Security. The main content area displays a user profile for 'User - alice p'. The 'User ID' field contains 'alice' and is highlighted with a red box. Other fields include 'First name: alice', 'Last name: p', 'Title: ', 'Department: ', 'Email: alice@gmail.com', 'Language: None', 'Calendar integration: Outlook', 'Time zone: System (America/Los_Angeles)', 'Date format: System (yyyy-MM-dd)', 'Business phone: ', 'Mobile phone: ', and 'Photo: Click to add...'. The 'Active' checkbox is checked. At the bottom, there are 'Update', 'Set Password', and 'Delete' buttons, along with 'Related Links' for 'View linked accounts', 'View Subscriptions', and 'Reset a password'. A navigation bar at the bottom includes 'Entitled Custom Tables', 'Roles (3)', 'Groups (1)', 'Delegates', 'Subscriptions', and 'User Client Certificates'.



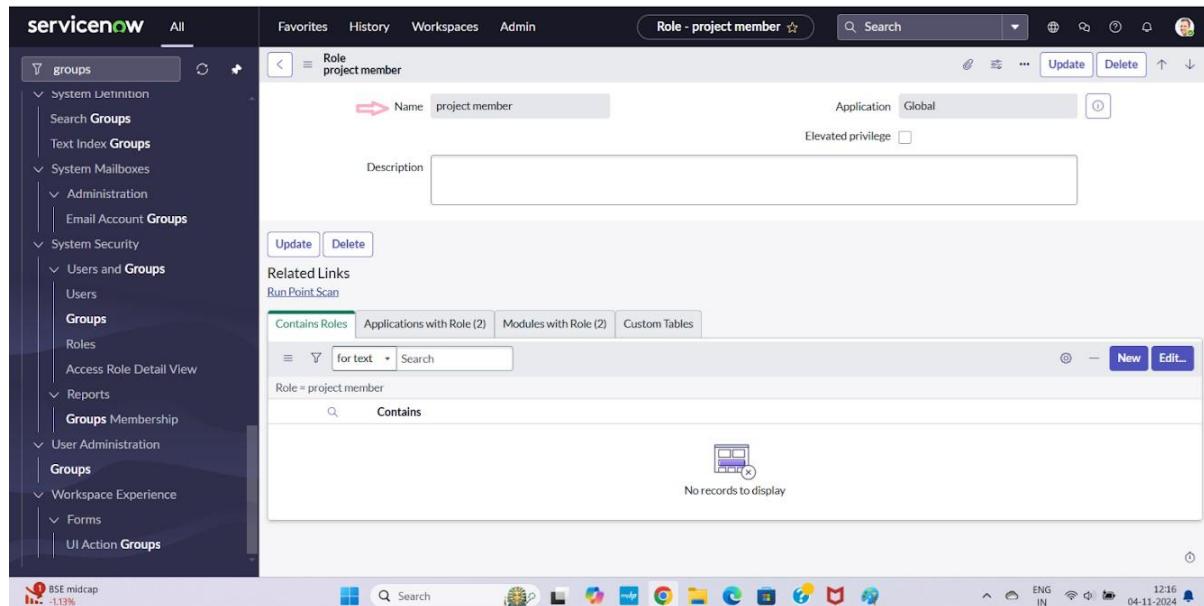
Parameter Category	Recommended Value (Optimization Best Practice)	Value (Definition/Setting)
Identity & Users	User Source of Truth	Ensure data accuracy (real-time status/department sync) and enable strong authentication (MFA).
Workflow Automation	Role Assignment Method	Scalability and Auditability. Roles assigned to Groups
Access Model	Provisioning Trigger	Automates account creation and base group assignment upon new hire.

GROUP ASSIGNING:



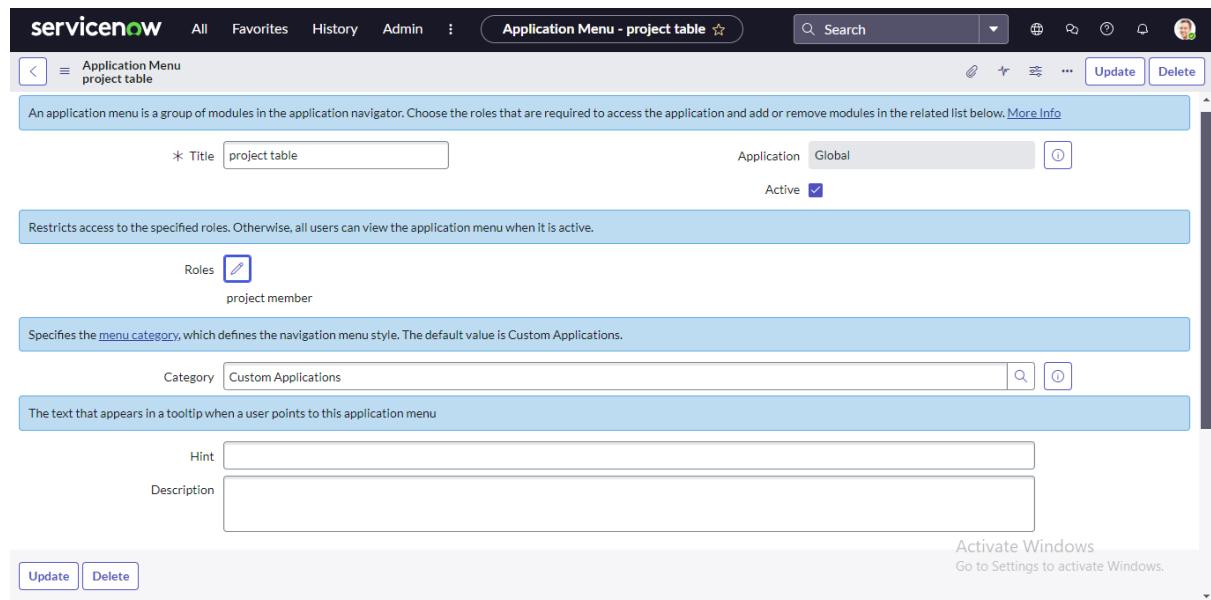
PARAMETER	VALUES
Group Name	Ensures immediate clarity on the group's purpose and ownership, aiding in searches and audits.
Group Type / Category	Defines the primary classification for easier management (e.g., <i>Security</i> , <i>Distribution</i> , <i>Team</i> , <i>Role-Granting</i>).
Group Membership Type	Establishes accountability for membership changes and participation in access recertification workflows.
Group Owner	Manual: For small, static teams. Dynamic: Based on user attributes

ASSIGNING ROLES:

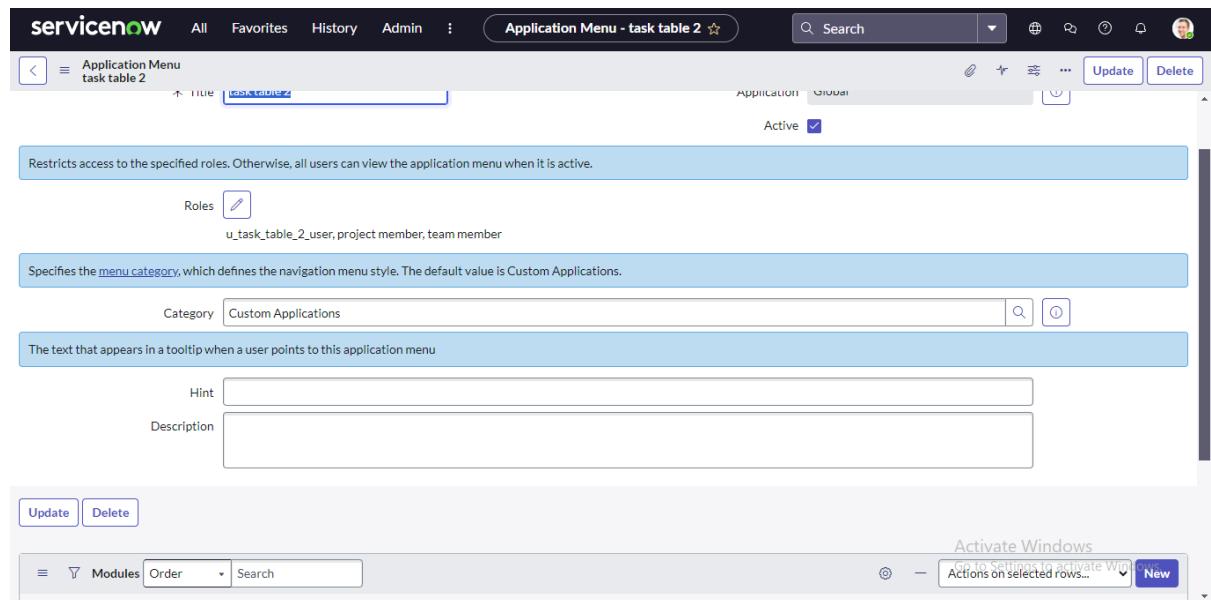


PARAMETER	VALUES
Assignment Target	Roles should be assigned to a Group which aligns with a job function. Direct user assignment should be highly restricted and documented.
Assignment Trigger	Role inheritance must be automatic upon a user joining the designated group.
Approval Chain	Enforce dual approval to ensure both the user's need and the application owner's risk tolerance are satisfied.
Enforcement of PoLP	Automatically check the requested role against the user's existing roles for Separation of Duties (SoD).

APPLICATION ACCESS:



The screenshot shows the 'Application Menu - project table' configuration page in ServiceNow. The title is 'project table'. The application is set to 'Global' and is marked as 'Active'. The 'Roles' field contains 'project member'. The 'Category' is set to 'Custom Applications'. There is a 'Hint' field and a 'Description' field, both of which are currently empty. At the bottom, there are 'Update' and 'Delete' buttons.



The screenshot shows the 'Application Menu - task table 2' configuration page in ServiceNow. The title is 'task table 2'. The application is set to 'Global' and is marked as 'Active'. The 'Roles' field contains 'u_task_table_2_user, project member, team member'. The 'Category' is set to 'Custom Applications'. There is a 'Hint' field and a 'Description' field, both of which are currently empty. At the bottom, there are 'Update' and 'Delete' buttons. Below the main form, there is a navigation bar with 'Modules', 'Order', and 'Search' buttons, along with a 'New' button and a link to 'Activate Windows'.

Optimizing Application Access relies on clearly defined parameters and standards, ensuring that access is secure, automated, and auditable across all systems. The core parameters include integrating the application via SAML/OIDC SSO with a central Identity Provider (IdP) to enforce authentication and MFA.