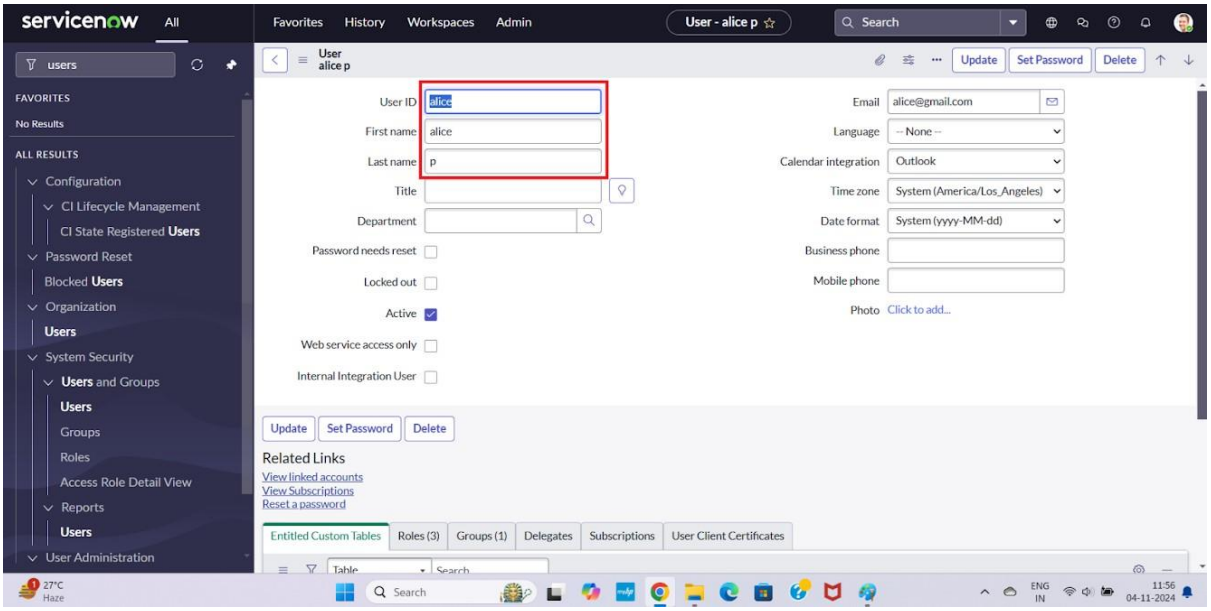
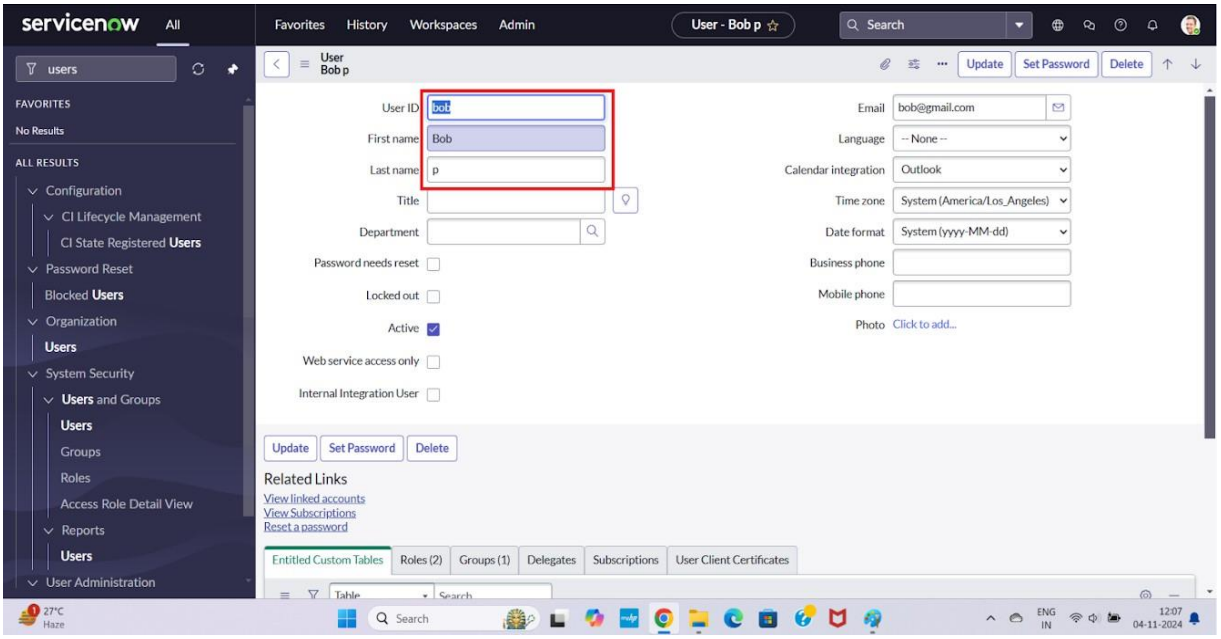
Performance and Testing

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

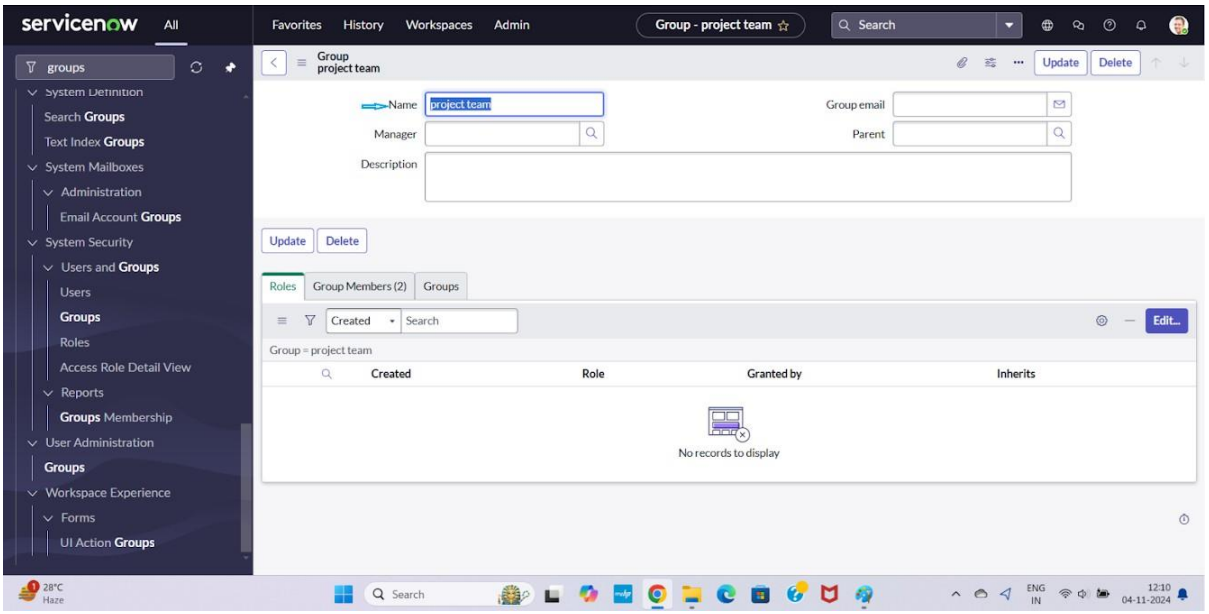
User Creation





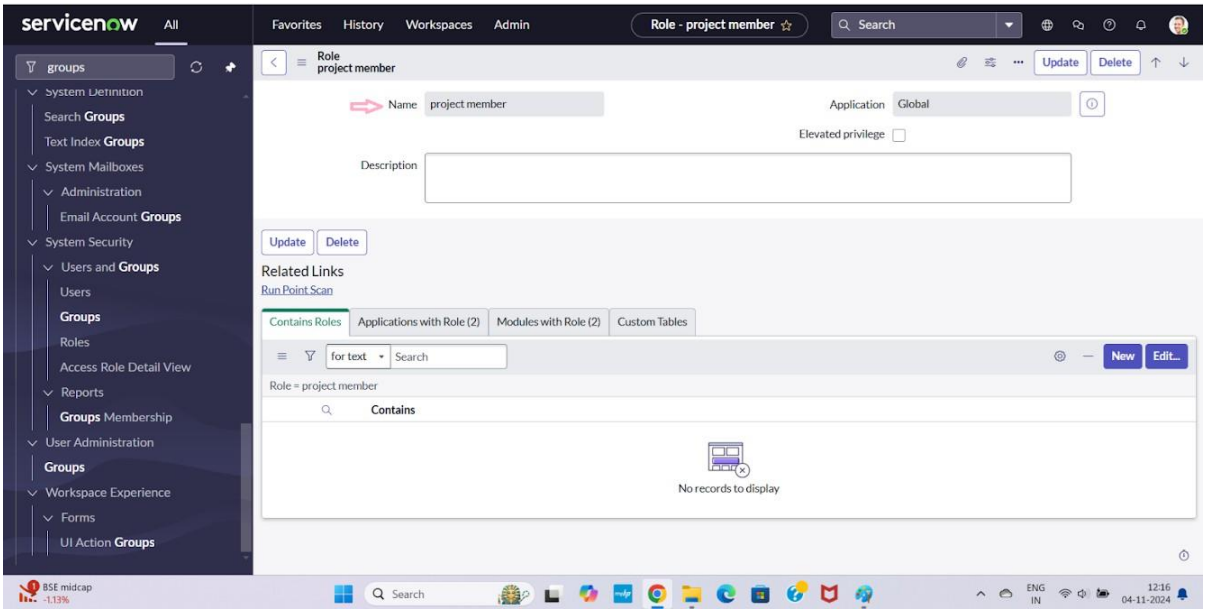
Parameter Category	Recommended Value (Optimization Best Practice)	Value (Definition/Setting)
Identity & Users	User Source of Truth	Ensure **data accuracy** (real-time status/department sync) and enable strong authentication (MFA).
Workflow Automation	Role Assignment Method	**Scalability and Auditability.**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

GROUP ASSIGNING:



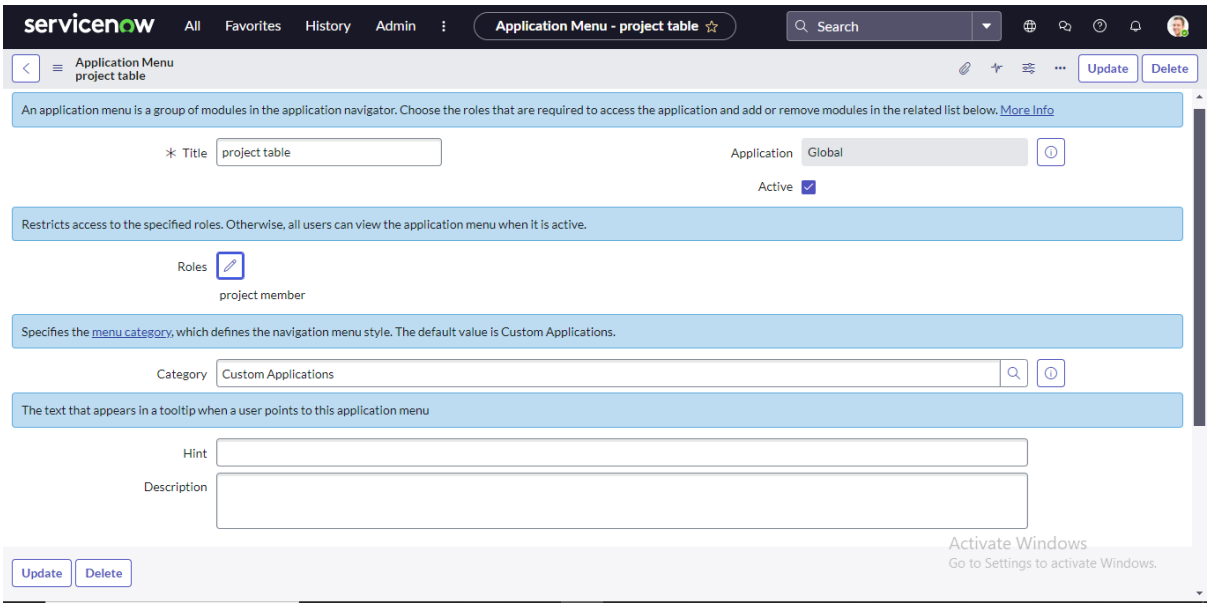
PARAMETER	VALUES
Group Name	Ensures immediate clarity on the group's purpose and ownership, aiding in searches and audits.
Group Type / Category	Defines the primary classification for easier management (e.g., *Security*, *Distribution*, *Team*, *Role-Granting*).
Group Membership Type	Establishes accountability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

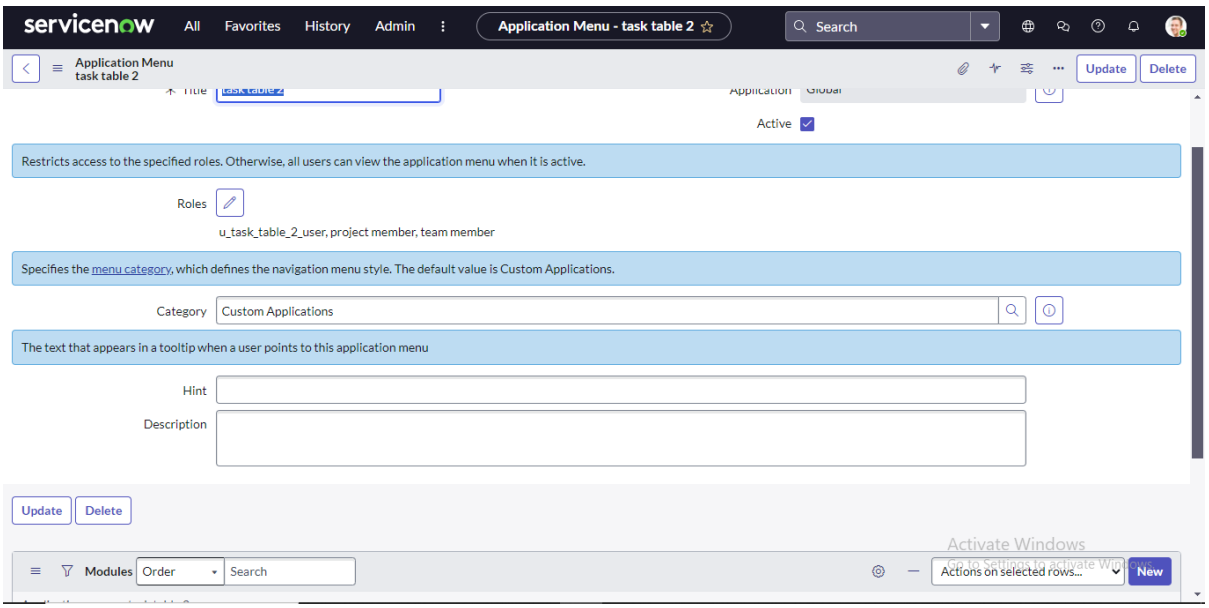
ASSIGNING ROLES:



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:





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.