Phase 9: Reporting, Dashboards & Security Review

Goal: Track student applications and mentorship outcomes using reports and dashboards. Ensure secure access through sharing settings, field-level security, and login restrictions. Maintain accountability with audit trails and session controls.

1. Reports

- Used to analyse student, mentor, and application data.
- In the project:
- Student Applications Report – shows how many applications each student has submitted and their statuses (In Progress, Submitted, Accepted, Rejected).
- Mentorship Sessions Report – tracks the number of mentorship sessions conducted by each mentor to evaluate engagement.

2. Report Types

- Define the combinations of objects available for reporting.
- In the project:
- A Custom Report Type (Student + Application + Mentor) was created.
- Enabled advanced analysis like "Applications guided by each Mentor" or "Student progress linked to mentorship."
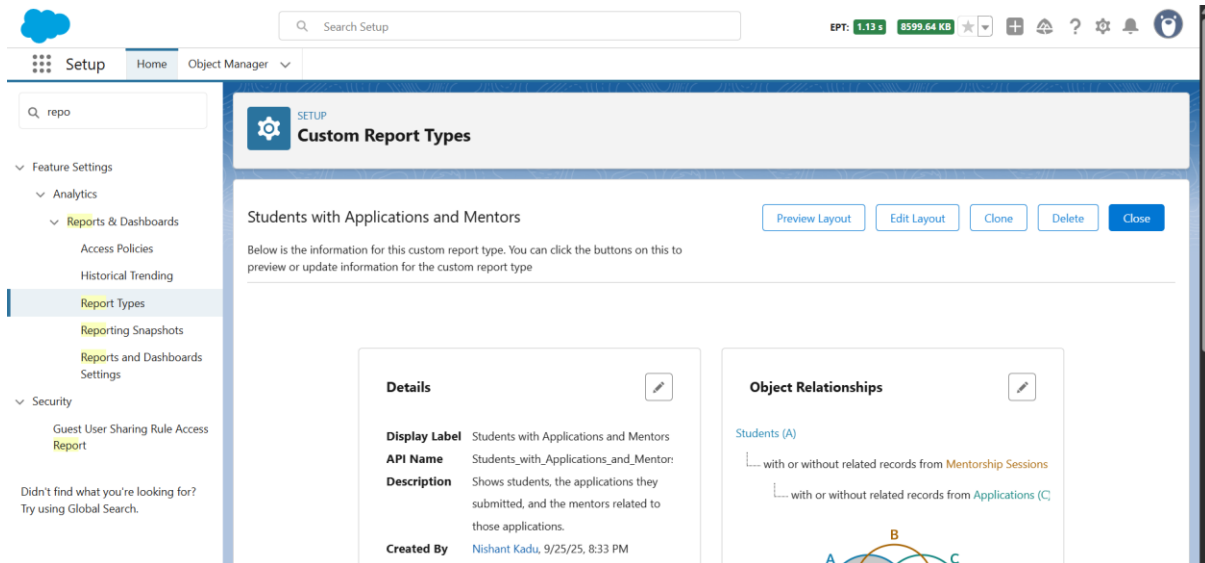

3. Dashboards

- Visual displays of multiple reports for quick insights.
- In the project:
- Student Progress Dashboard – shows % of applications Accepted, Rejected, or In Progress.
- Mentor Performance Dashboard – displays sessions conducted, feedback scores, and outcomes per mentor.
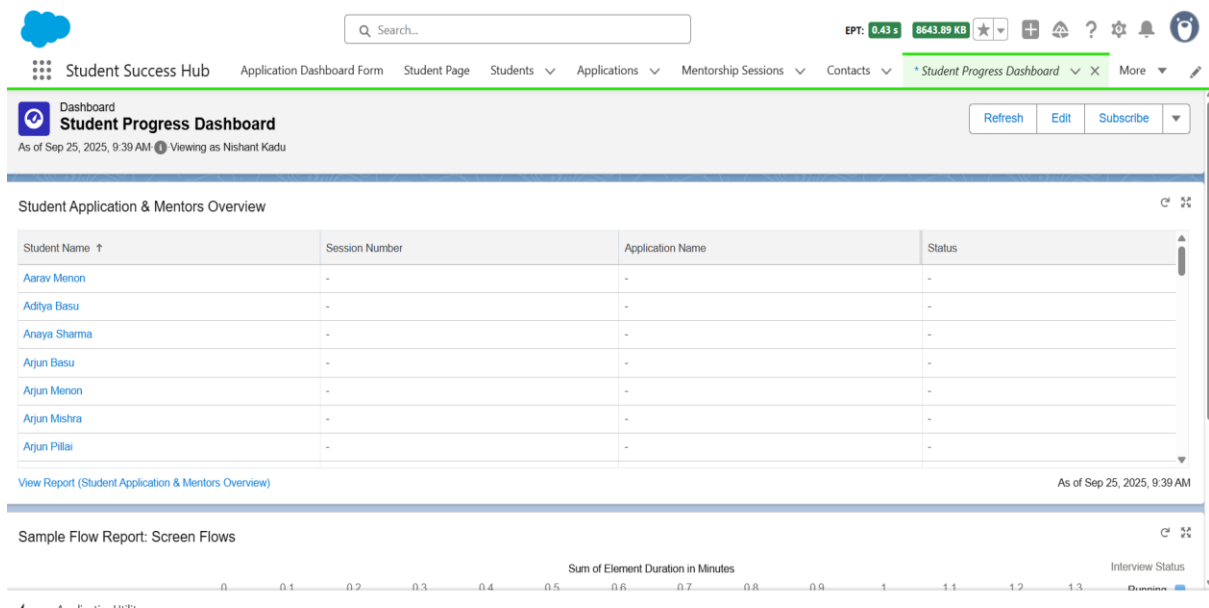
4. Dynamic Dashboards

- Dashboards that display data according to the logged-in user.
- In the project:
- Each Mentor sees only their own assigned students and mentorship data.
- Admins can see all student and mentor data.
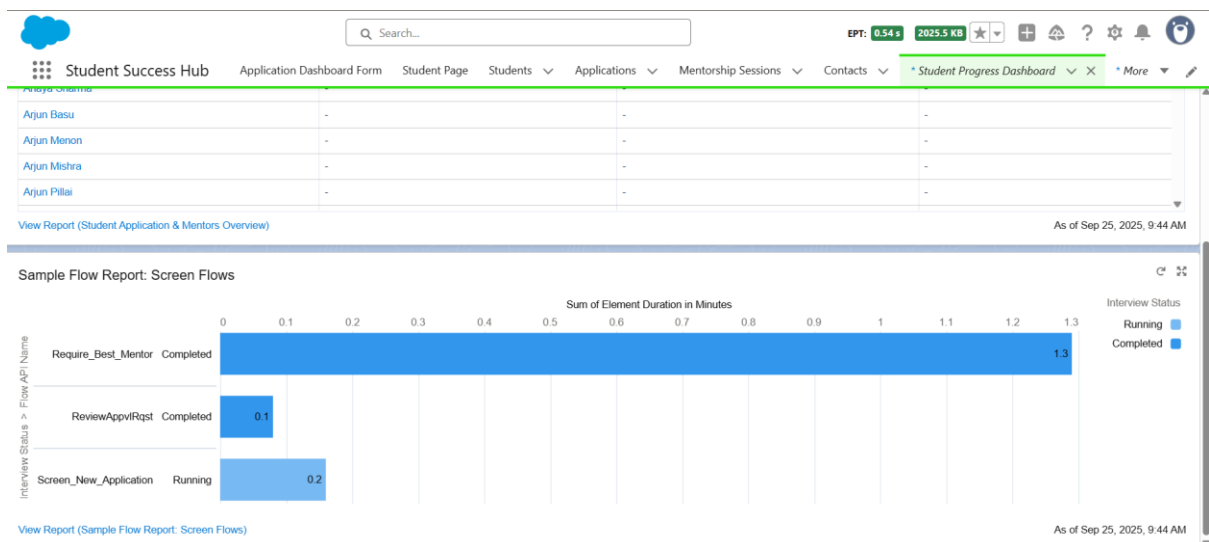
5. Sharing Settings

- Control record-level access across users.
- In the project:
- Applications → set to *Private* (only the student, mentor, and admin can view).

- Students & Mentors → set to Public Read Only (basic details visible but edits restricted).
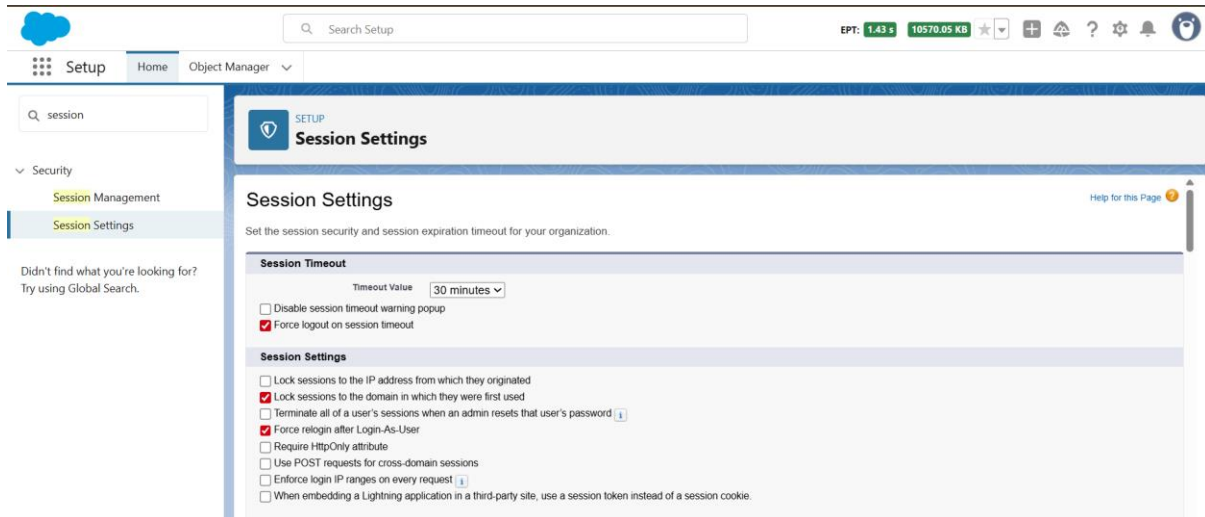

6. Field Level Security

- Restrict sensitive fields to certain profiles.
- In the project:
- Fields like Student ID Proof and personal contact details are hidden from Mentors.
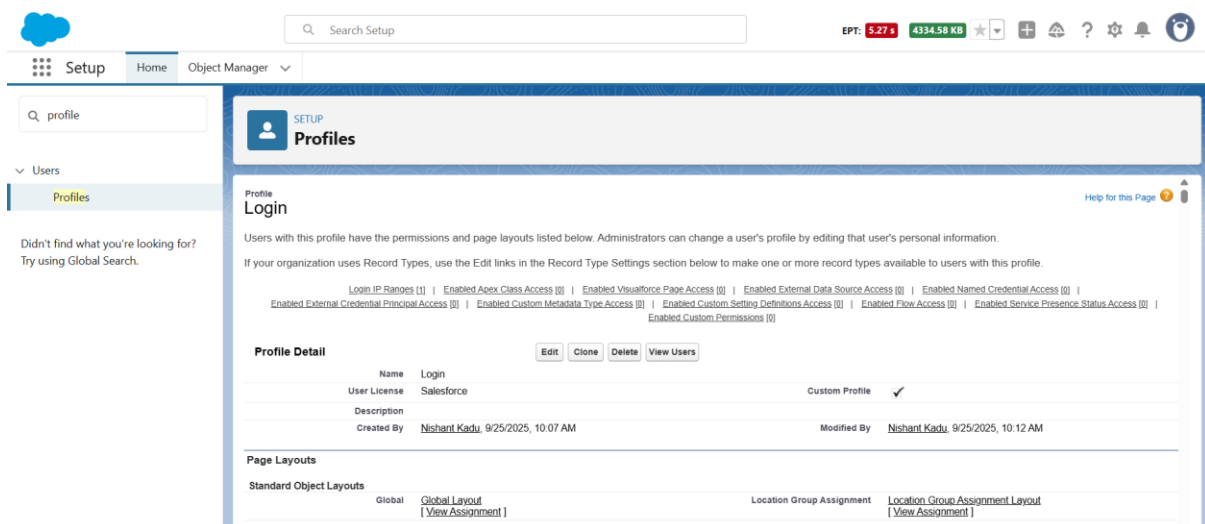- These fields are only visible to Admins.

7. Session Settings

- Manage session timeout to prevent unauthorised access.
- In the project:
- Configured session timeout to 30 minutes.

8. Login IP Ranges

- Restrict logins to specified IP addresses for enhanced security.
- In the project:
- Mentor and Admin profiles restricted to institution/office IP ranges.

9. Audit Trail

- Provides visibility into setup and configuration changes.

- In the project:
- Used to track who created, updated, or deleted records (Applications, Mentorship Sessions, etc.).
- Ensures accountability for sensitive data changes.