

Phase 9 Report

Reporting, Dashboards & Security Review

Project: College Placement & Internship Management System

Batch: 4

Program: TCS Last Mile SmartBridge

Prepared by: Lowrence Devu

1. Introduction

Phase 9 focuses on enabling insightful reporting, dashboards for stakeholders, and reviewing security to ensure role-based access control and data integrity. Reports and dashboards allow Placement Officers, Recruiters, and Students to monitor applications and job postings efficiently.

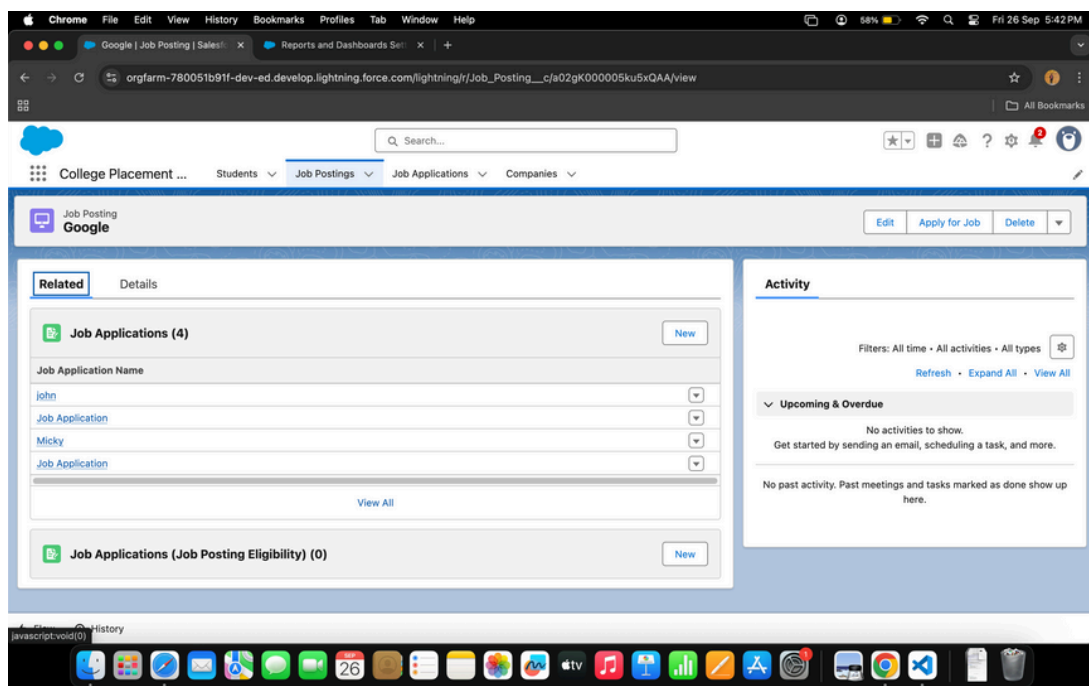
2. Objectives

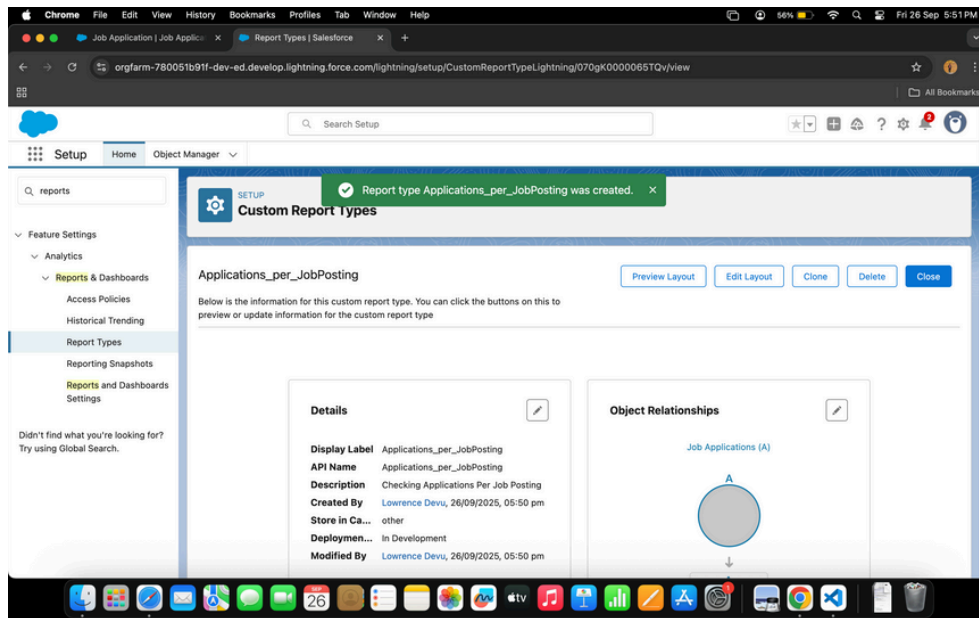
- Create meaningful **Reports** for Students, Job Applications, and Companies.
- Configure **Dashboards** for Placement Officers and Recruiters.
- Apply **Dynamic Dashboards** for role-specific visibility.
- Review **Sharing Settings, Field-Level Security, and Login Policies.**
- Audit user activity and ensure secure access to sensitive placement data.

3. Steps Performed

3.1 Reports Creation

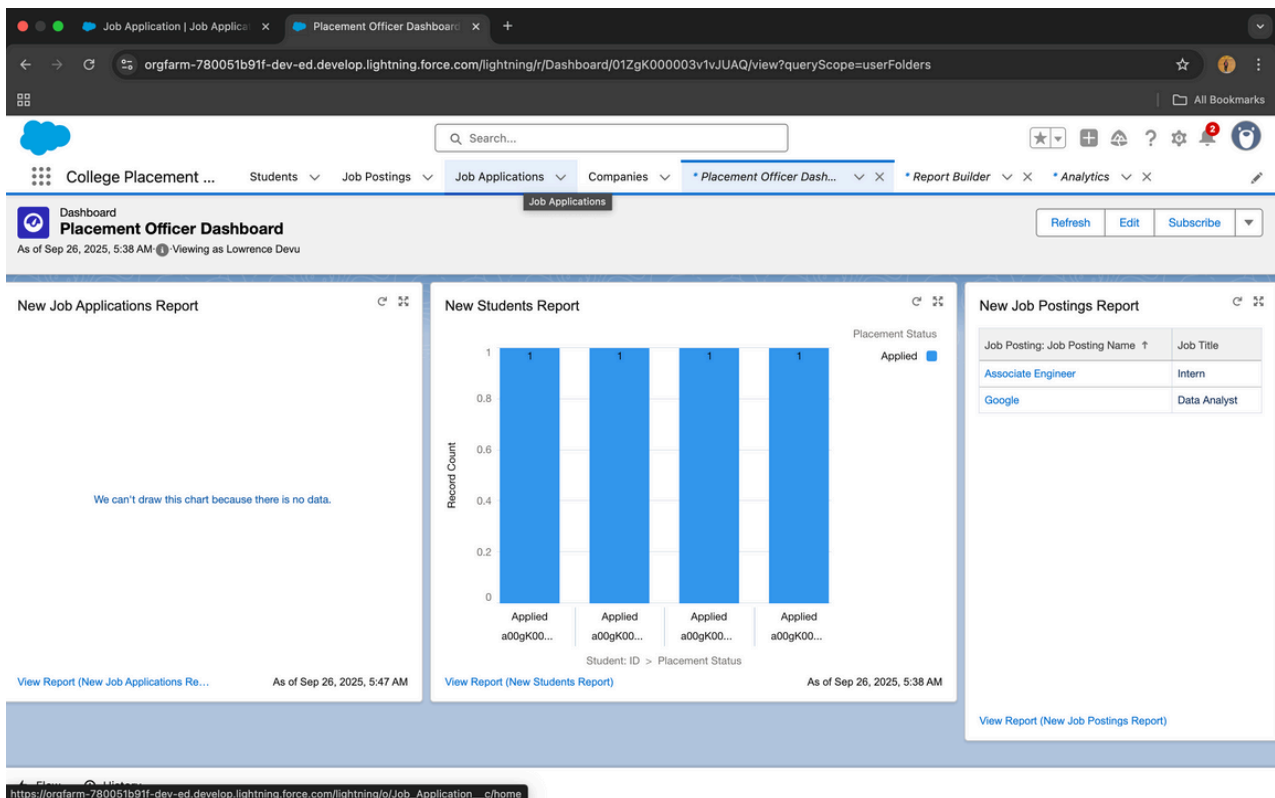
- Created **Tabular, Summary, and Matrix Reports:**
 - Applications per Job Posting
 - Students Shortlisted / Selected / Rejected
 - Companies and their Job Postings
- Used filters to show only relevant records per role.
- Saved custom report types where needed for complex relationships.





3.2 Dashboards Configuration

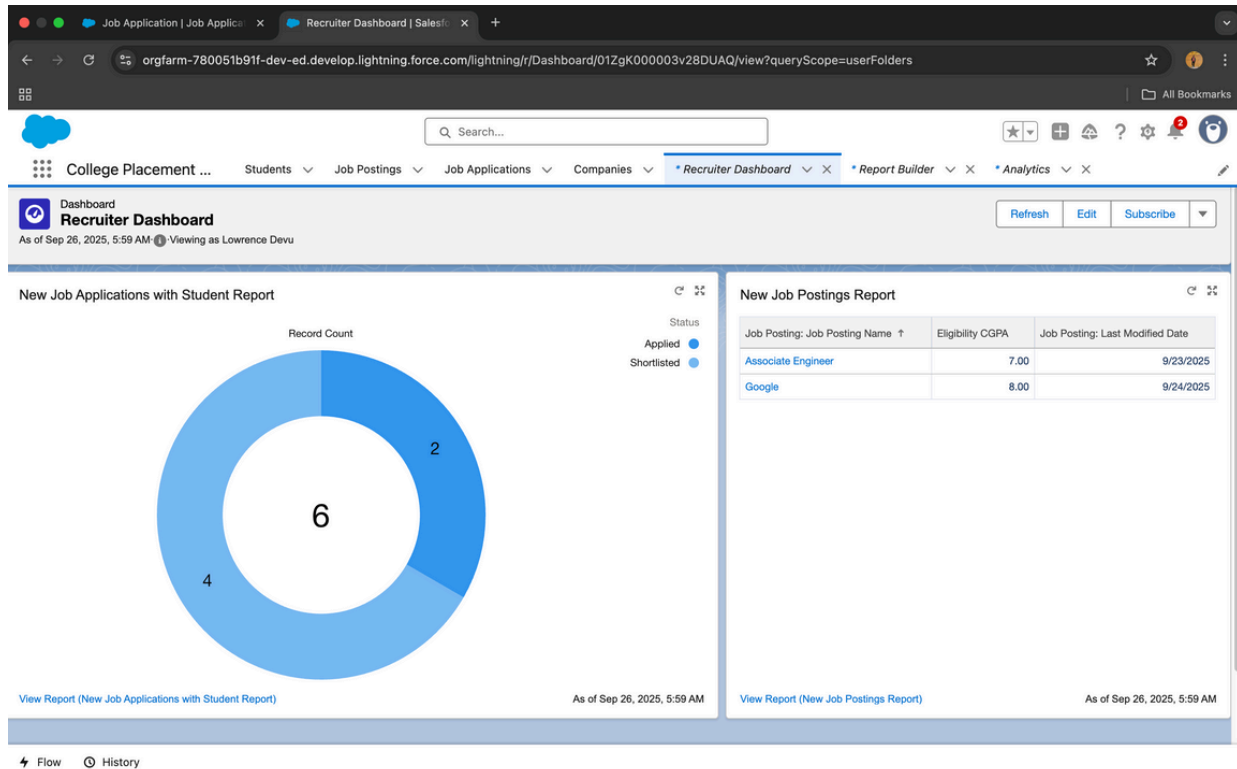
- Created Dashboards for Placement Officers:
 - Applications by Job Posting (Bar Chart)
 - Students by Placement Status (Pie Chart)
 - Upcoming Job Posting Deadlines (Table)
- Configured Dashboards for Recruiters:



- Applications assigned to recruiter (List/Table)
- Shortlisted vs Rejected students (Donut Chart)

3.3 Dynamic Dashboards

- Enabled **Run as logged-in user** to filter data dynamically.
- Placement Officers see all data, Students see only their applications.
- Validated access for multiple users.

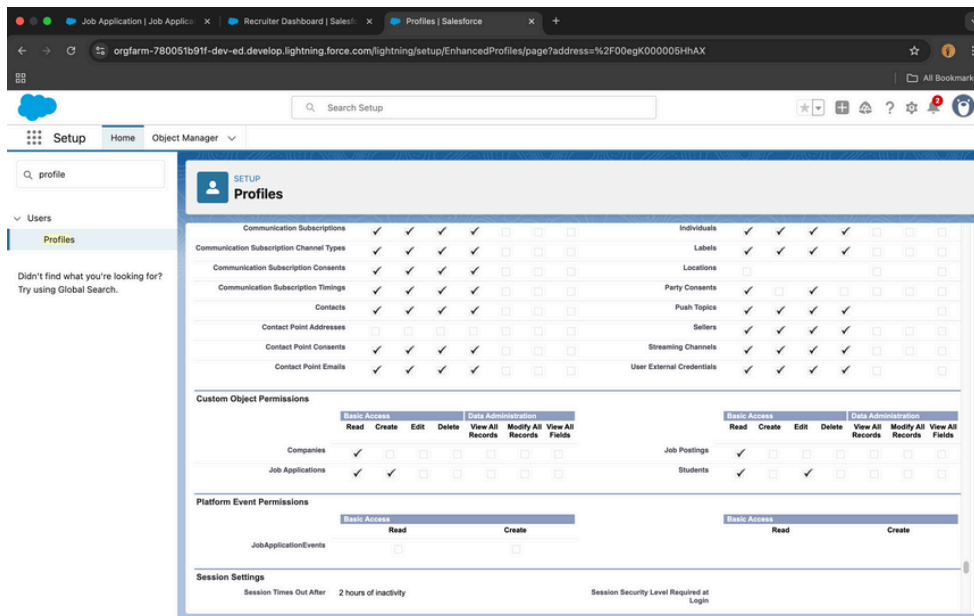


3.4 Security Review

- Reviewed **Organization-Wide Defaults (OWD)**:
 - Student: Private
 - Job Application: Controlled by Parent (Job Posting)
 - Company: Public Read Only
- Verified **Profile Permissions**:
 - Placement Officer: Full Access
 - Recruiter: Limited Access
 - Student: Only own records
- Enabled **Field-Level Security** for sensitive fields like CGPA and Remarks.
- Configured **Login IP Ranges and Session Settings** for added security.

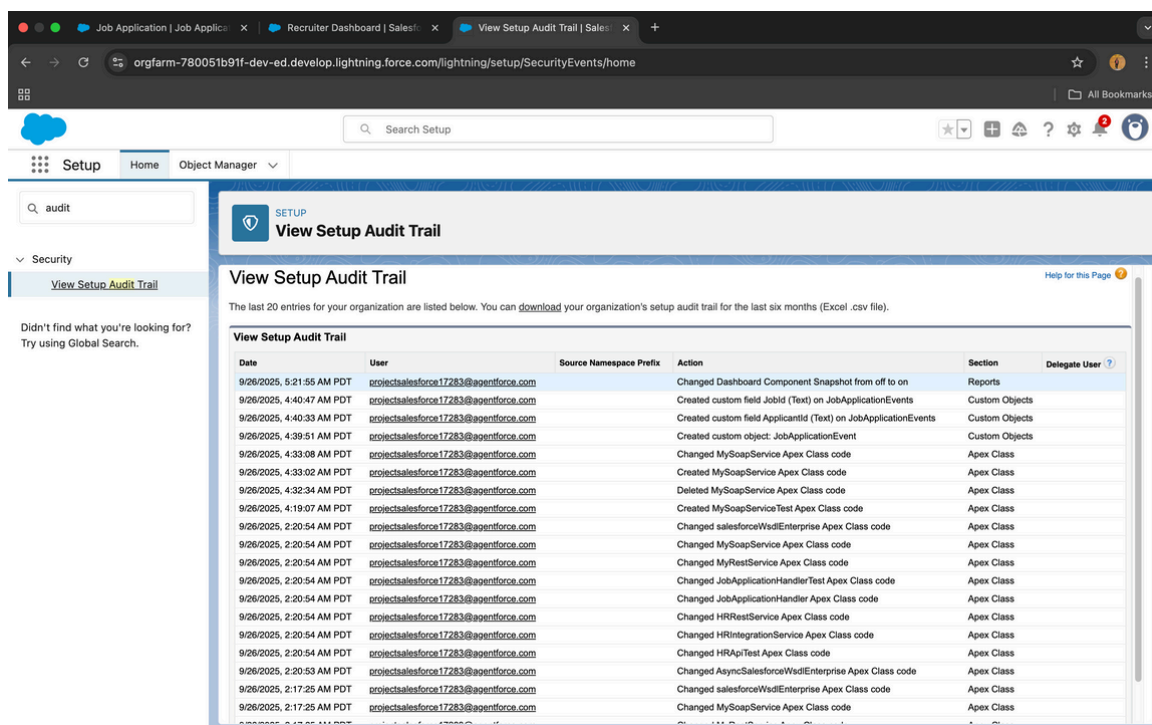
The screenshot shows the Salesforce Sharing Settings page. It lists various objects and their sharing settings. The 'Student' object is highlighted, showing its sharing settings as Private for all roles.

Object	Public Read/Write	Private	Public Read/Write
Service Resource	Public Read/Write	Private	✓
Service Territory	Public Read/Write	Private	✓
Shift	Private	Private	✓
Shipment	Private	Private	✓
Shipping Center	Public Read Only	Private	✓
Shipping Center Method	Public Read Only	Private	✓
Shipping Configuration Set	Public Read Only	Private	✓
Streaming Channel	Public Read/Write	Private	✓
Tableau Host Mapping	Public Read Only	Private	✓
User Presence	Public Read Only	Private	✓
User Provisioning Request	Private	Private	✓
Waitlist	Private	Private	✓
Web Cart Document	Private	Private	✓
Work Order	Private	Private	✓
Work Plan	Private	Private	✓
Work Plan Template	Private	Private	✓
Work Step Template	Private	Private	✓
Work Type	Private	Private	✓
Work Type Group	Public Read/Write	Private	✓
Company	Public Read Only	Private	✓
Job Application	Private	Private	✓
Job Posting	Public Read Only	Private	✓
Student	Private	Private	✓



3.5 Audit Trail & Monitoring

- Checked **Setup Audit Trail** for recent changes.
- Ensured no unauthorized changes in object configurations.
- Monitored reports for suspicious activity.



4. Expected Outcomes

- Stakeholders have access to relevant reports and dashboards.
- Role-based dynamic dashboards ensure secure, filtered visibility.
- OWD and FLS settings enforce correct access levels.
- Audit trail confirms system changes are tracked.
- Overall system is secure, auditable, and insightful.

5. Conclusion

Phase 9 ensures that the College Placement & Internship Management System is fully reportable, with dashboards for real-time monitoring. Security review guarantees proper access control and visibility for all roles, providing confidence before final deployment and presentation.