Phase 9: Reporting, Dashboards & Security Review

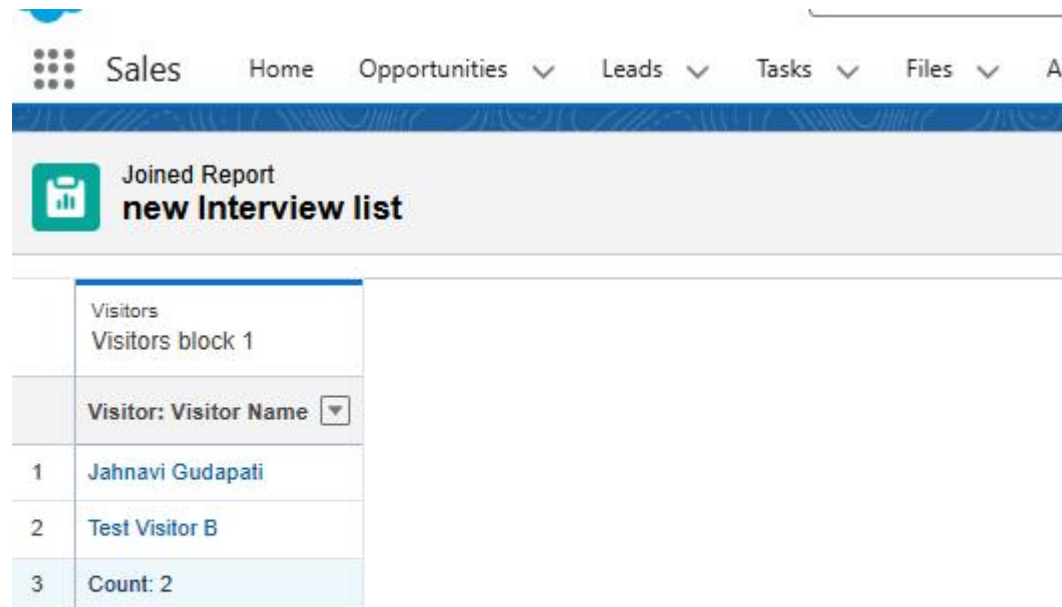**Project:Visitor CheckIn System for Offices**

1. Reports

UseCase:
Reports help analyze visitor data by displaying it in different formats. In our Visitor Management project, we used reports to track visitor check-ins and analyze visits by purpose.

Steps Done:

- Created a Tabular Report to list all Visitor__c records with Name, Email, Purpose, and Check-In Time.

- Built a Summary Report grouped by Purpose of Visit.

- Built a Matrix Report to compare Visitor Purpose vs. Host Employee.

- Created a Joined Report to compare Visitor__c with another object (like Host Employee).

2. Report Types

UseCase:
Custom Report Types allow reporting on custom objects. Since we created Visitor__c, we needed a **Custom Report Type** to generate reports on visitors.

Steps Done:

- Setup → Report Types → New.

- Primary Object: Visitor__c.

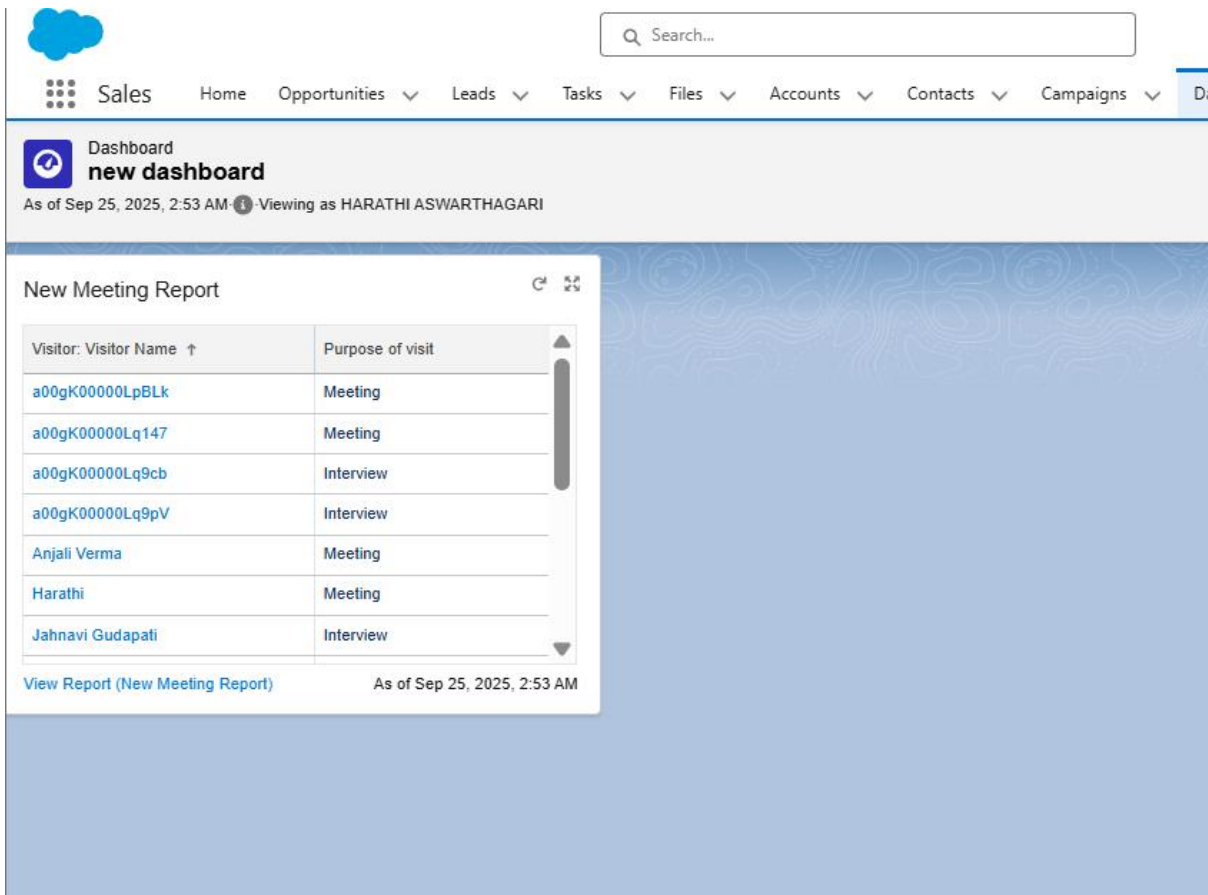- Deployed report type and used it to generate visitor reports.

3. Dashboards & Dynamic Dashboards

UseCase:
Dashboards visualize report data with charts and metrics. Dynamic Dashboards display information based on the logged-in user's access.

Steps Done:

- Created a Dashboard to show:

    o Pie chart of Visitors by Purpose.

    o Bar chart of Visitors per Host Employee.

    o Line chart of Visitors over time.

- Configured a **Dynamic Dashboard** so each Host Employee only sees their visitors.

4. Profiles

UseCase:
Profiles control object-level and field-level permissions. In our project, we created separate profiles for Receptionist (can create visitor records) and Host Employee (can only view visitors).

Steps Done:

- Created a custom profile Visitor Receptionist.

- Assigned CRUD permissions on Visitor__c.
- Restricted Host Employee profile to Read-only access.

5. Roles

UseCase:

Roles determine record visibility in role hierarchy. Receptionists should see all visitors, but employees should only see their own.

Steps Done:

- Created a Role Hierarchy with:
  - Receptionist at the top to handle visitor's information.
  - Host Employees below.
- Assigned users to roles.

6. Permission Sets

UseCase:
Permission Sets provide extra access without changing profiles. For example, giving an employee temporary ability to export reports.

Steps Done:

- Created a Visitor Reporting Permission Set.

- Granted "Run Reports" and "Export Reports" permissions.

- Assigned it to selected users.

7. Organization-Wide Defaults (OWD)

UseCase:
OWD defines the default record access. For visitors, we restricted access to **Private** so that only owners (receptionists) and higher roles can see them.

Steps Done:

- Setup → Sharing Settings → OWD.

- Visitor__c set to **Private**.

| Visit | Public Read/Write | Private | ✔ |
| Visitor | Public Read/Write | Private | ✔ |

8. Sharing Rules

UseCase:
Sharing Rules open up record visibility beyond OWD. For example, share all Visitor__c records with the Security Team.

Steps Done:

- Setup → Sharing Rules.

- Object: Visitor__c.

- Rule: Share with Security Team Public Group.

Visitor Sharing Rules	New	Recalculate		Visitor Sharing Rules Help ?
Action	Criteria		Shared With	Access Level
Edit | Del	Owner in Role and Internal Subordinates: Receptionist		Role and Internal Subordinates: Visitor Manager	Read/Write

9. Field Level Security (FLS)

UseCase:
FLS restricts access to specific fields. For example, ID Proof Number should only be visible to security personnel, not hosts.

Steps Done:

- Edited Visitor Receptionist Profile → removed visibility for sensitive fields.

- Ensured Security Profile can see ID Proof Number.

10. Session Settings

UseCase:
Session settings improve login security, e.g., session timeouts or requiring re-authentication for critical actions.

Steps Done:

- Setup → Session Settings.

- Configured Timeout = 1 Hour.

- Enabled "Lock sessions to IP address".

11. Login IP Ranges

UseCase:
Restricts login access to specific IP ranges (e.g., office network only).

Steps Done:

- Setup → Profiles → Receptionist Profile.

- Set Login IP Range (Company network IP range).

12. Audit Trail

UseCase:
Audit Trail tracks configuration changes. Useful for monitoring admin changes in Visitor Management.

Steps Done:

- Setup → View Setup Audit Trail.

- Verified changes such as Profile modifications and OWD updates.

AM PDT	22691a0566732@agentforce.com	Changed Use POST requests for cross-domain sessions attribute from off to on	Settings
9/25/2025, 3:35:38 AM PDT	22691a0566732@agentforce.com	Changed clickjack protection for customer Visualforce pages with standard headers attribute from off to on	Session Settings
9/25/2025, 3:35:38 AM PDT	22691a0566732@agentforce.com	Changed Require HttpOnly attribute from off to on	Session Settings
9/25/2025, 3:35:38 AM PDT	22691a0566732@agentforce.com	Changed Terminate all of a user's sessions when an admin resets that user's password from off to on	
9/25/2025, 3:35:38 AM PDT	22691a0566732@agentforce.com	Organization setup action: killUISessionsOnPwdResetOffOn has changed.	
9/25/2025, 3:35:38 AM PDT	22691a0566732@agentforce.com	Session Security Level for Multi-Factor Authentication was set to High Assurance	Session Settings
9/25/2025, 3:35:38 AM PDT	22691a0566732@agentforce.com	Session Security Level for Passwordless Login was set to Standard	Session Settings
9/25/2025, 3:35:38 AM PDT	22691a0566732@agentforce.com	Session Security Level for Lightning Login was set to Standard	Session Settings
9/25/2025, 3:35:38 AM PDT	22691a0566732@agentforce.com	Session Security Level for Activation was set to Standard	Session Settings
9/25/2025, 3:35:38 AM PDT	22691a0566732@agentforce.com	Session Security Level for Delegated Authentication was set to Standard	Session Settings
9/25/2025, 3:35:38 AM PDT	22691a0566732@agentforce.com	Session Security Level for Username Password was set to Standard	Session Settings
9/25/2025, 3:28:50 AM PDT	22691a0566732@agentforce.com	Changed profile Employee Profile: field-level security for Visitor: ID Proof Number was changed from Read/Write to No Access	Manage Users
9/25/2025, 3:27:02 AM PDT	22691a0566732@agentforce.com	Completed Owner Rule: Visitor recalculation: Employee Access	Sharing Rules
9/25/2025, 3:27:01 AM PDT	22691a0566732@agentforce.com	Created Visitor Owner Sharing Rule Employee Access	Sharing Rules
9/25/2025, 3:27:01 AM PDT	22691a0566732@agentforce.com	Initiated Owner Rule: Visitor recalculation: Employee Access	Sharing Rules
9/25/2025, 3:22:34 AM PDT	22691a0566732@agentforce.com	Created new role Creating Updating Reporting details	Manage Users
9/25/2025, 3:21:14 AM PDT	22691a0566732@agentforce.com	Created new role Monitor Visitor Details	Manage Users
9/25/2025, 3:20:56 AM PDT	22691a0566732@agentforce.com	Deleted role Monitor Visitor Details	Manage Users
9/25/2025, 3:20:15 AM PDT	22691a0566732@agentforce.com	Created new role Monitor Visitor Details	Manage Users
9/25/2025, 3:19:27 AM PDT	22691a0566732@agentforce.com	Deleted role CFO	Manage Users

Download setup audit trail for last six months (Excel .csv file)