📘 Phase 9: Reporting, Dashboards & Security Review

🎯 Objective

The purpose of this phase is to create **meaningful business insights** through Salesforce **Reports and Dashboards** while ensuring **data security and compliance** using sharing rules, field-level security, and login restrictions.

This phase ensures that the **Customer Complaint CRM** application delivers powerful analytics while keeping customer and agent data safe.

📊 1. Reports

Description:

Reports in Salesforce help visualize and analyze CRM data such as **complaints, customers, agents, and performance**.

Types of Reports:

Type	Description	Use Case
Tabular Report	Simple table view, like Excel	List of all complaints
Summary Report	Grouped data with subtotals	Complaints grouped by Issue Type
Matrix Report	Grouped by rows and columns	Complaints by Agent and Status
Joined Report	Combines multiple report types	Compare Complaints and Customer data

Example:

Report Name: Complaints by Priority

- Object: Complaint__c
- Group by: Priority
- Show fields: Complaint Number, Issue Type, Status, Assigned Agent
- Add filter: Status != Closed

📈 **Outcome:** Quickly identify high-priority issues that are still open.

📋 2. Report Types

Description:

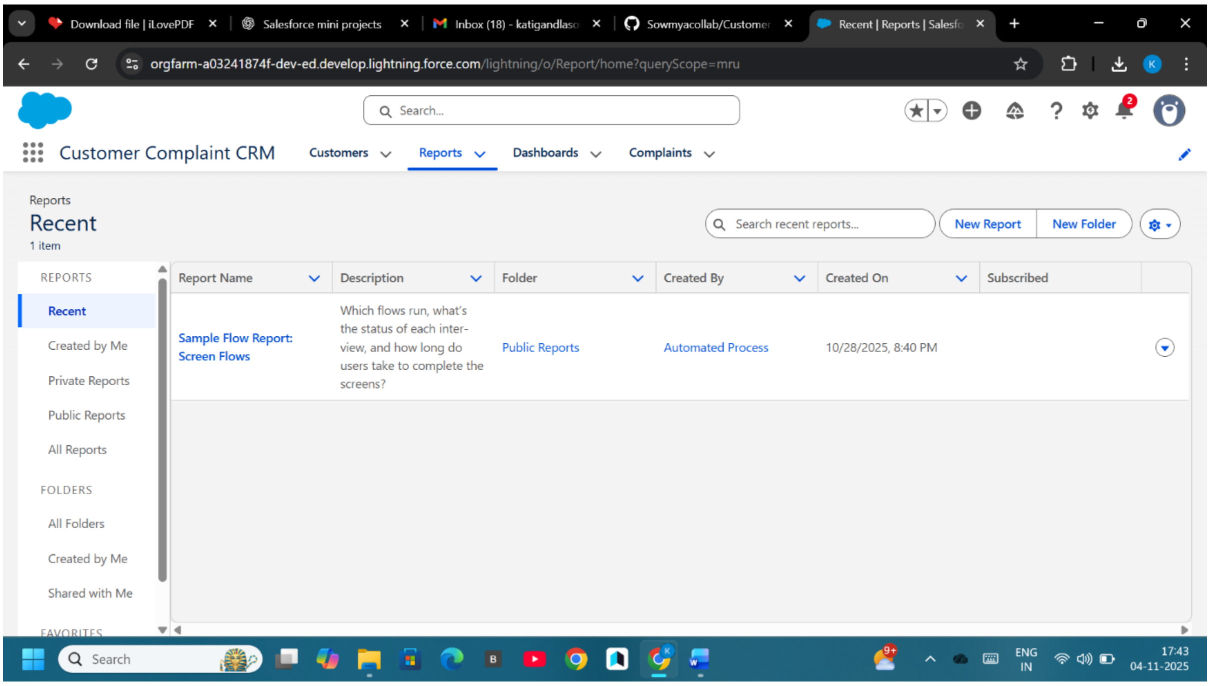
Report Types define which objects and fields are available for reporting.

Steps:

1. Setup → **Report Types** → **New Custom Report Type**
2. Primary Object: **Complaint__c**
3. Related Object: **Customer__c** (Each complaint has a customer)
4. Deploy the report type.

Use Case:

Allows reports combining both **Complaint and Customer** details (e.g., Complaints per Customer).



☑ 3. Dashboards

Description:

Dashboards visually display multiple reports in one place using charts, graphs, and tables.

Steps to Create:

1. Go to **Dashboards → New Dashboard**
2. Name: **Customer Complaint Dashboard**
3. Add components:
    - **Bar Chart:** Complaints by Status
    - **Pie Chart:** Complaints by Priority
    - **Gauge:** Agent Performance (% complaints closed)
    - **Table:** Top 5 Customers with Most Complaints
4. Save & Run.

Use Case:

Managers can monitor the CRM's overall performance in real time.

⚙ 4. Dynamic Dashboards

Description:

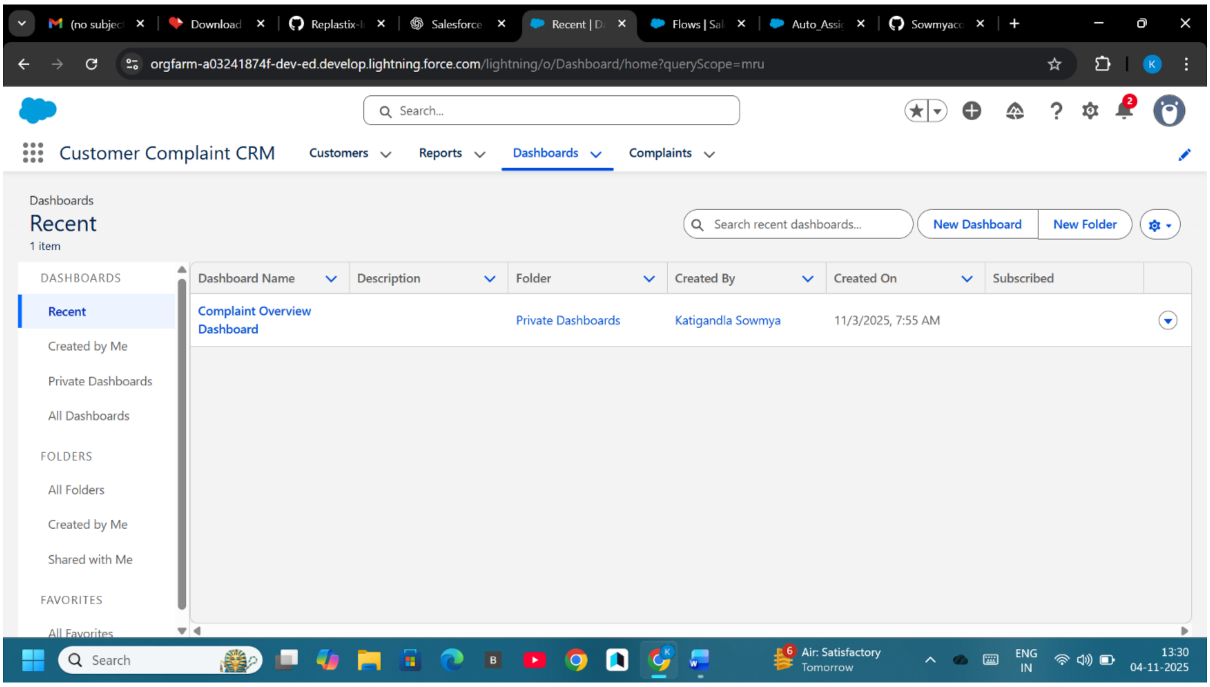
Dynamic Dashboards allow users to view data **according to their access level** — e.g., each agent only sees their own complaints.

Steps:

1. Open Dashboard → **Edit Properties**
2. Select: “View Dashboard As: Logged-in User”
3. Save & Activate

Use Case:

Ensures privacy — one agent can’t see another’s data.



🔒 5. Sharing Settings

Description:

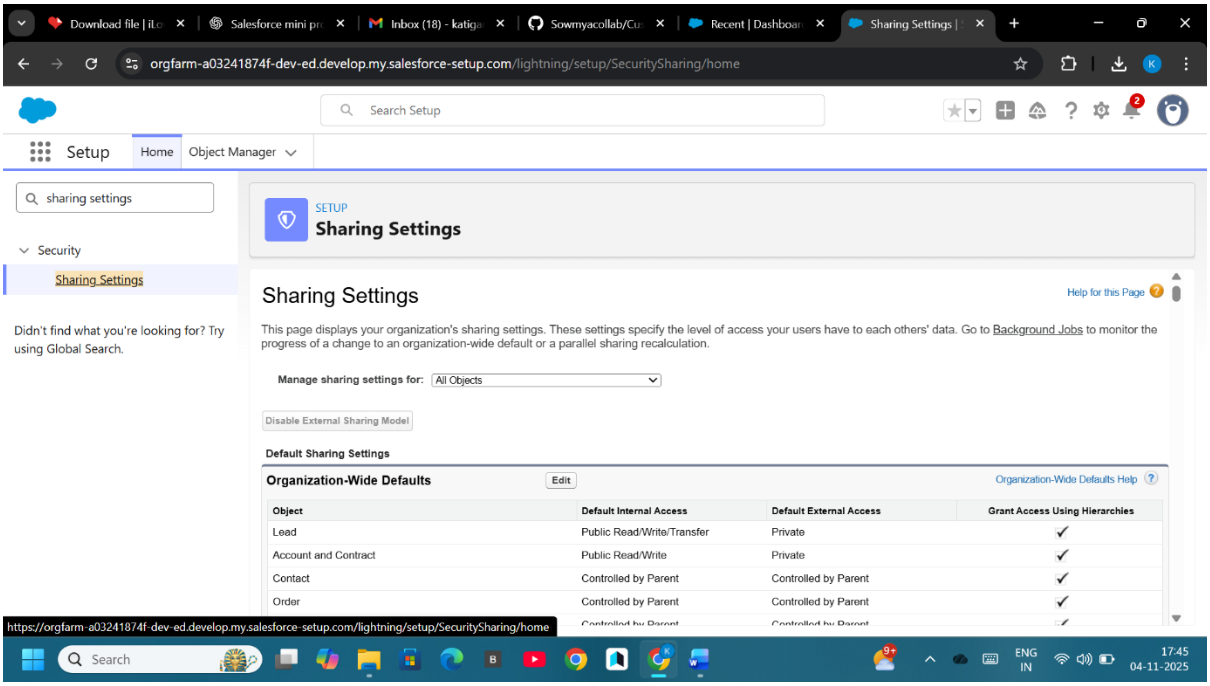
Sharing Settings define **organization-wide data visibility** and **record access** between users.

Steps:

1. Setup → **Sharing Settings**
2. Set **Organization-Wide Defaults (OWD):**
   - Complaint__c: Private
   - Customer__c: Controlled by Parent
3. Add **Sharing Rules:**
   - Share complaints with same department users.

Use Case:

Agents can view only their assigned complaints, while admins see all.



□ 6. Field-Level Security (FLS)

Description:

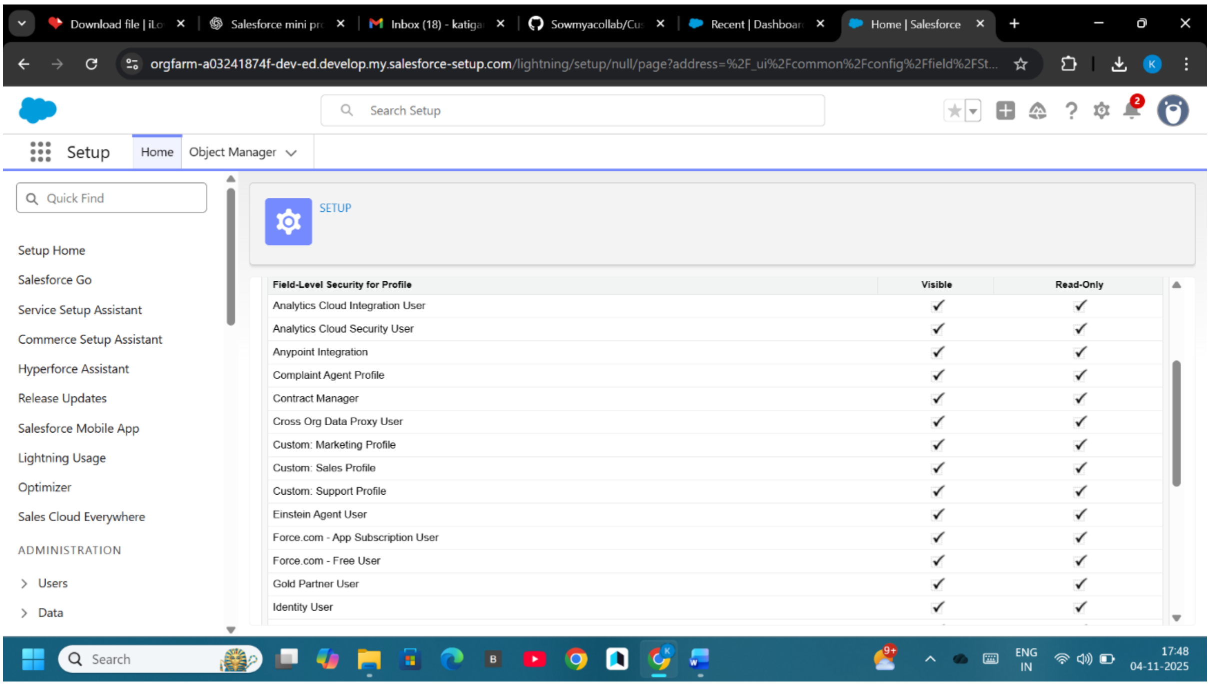
Controls which fields a user can **view or edit** in an object.

Steps:

1. Setup → Object Manager → **Complaint__c** → **Fields & Relationships**
2. Click a field (e.g., "Customer Email").
3. Set **Field-Level Security** for each Profile (hide from agents if needed).

Use Case:

Hide sensitive information (like billing details) from regular support agents.



🛡 7. Session Settings

Description:

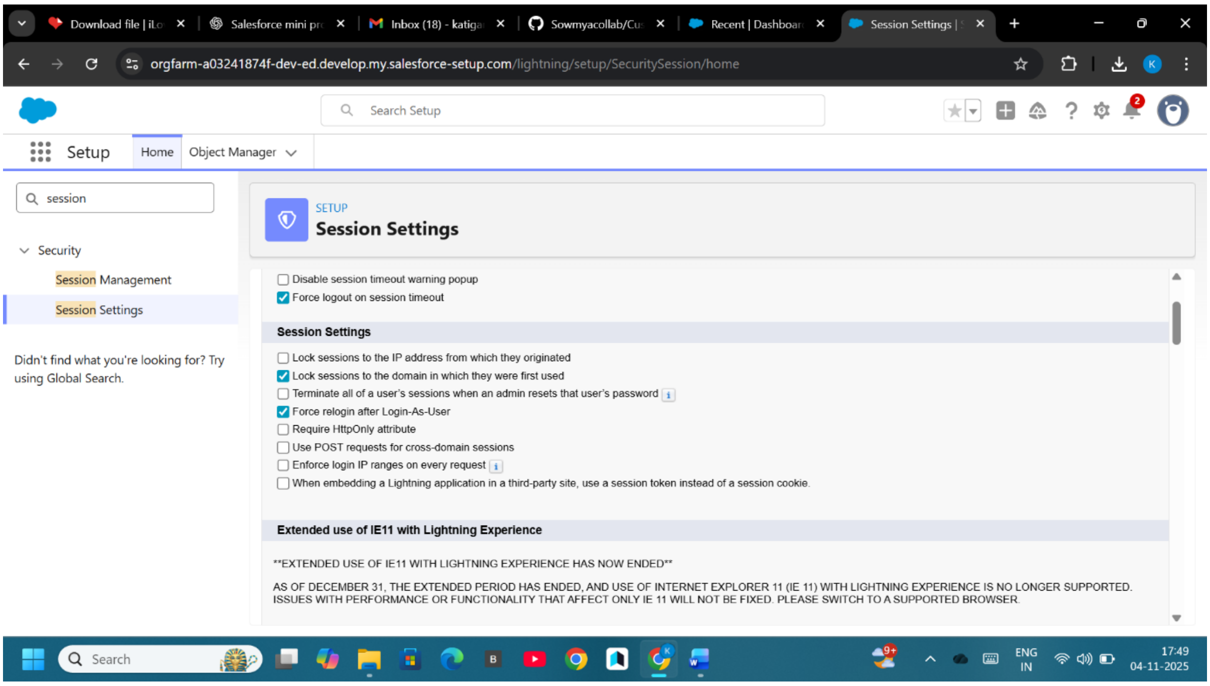
Controls session timeouts, login hours, and authentication settings to improve security.

Steps:

1. Setup → **Session Settings**
2. Configure:
    - Session Timeout: 30 minutes
    - Disable "Stay Logged In"
    - Enable secure HTTPS connections

Use Case:

Prevents unauthorized access if a session is left open.



🌐 8. Login IP Ranges

Description:

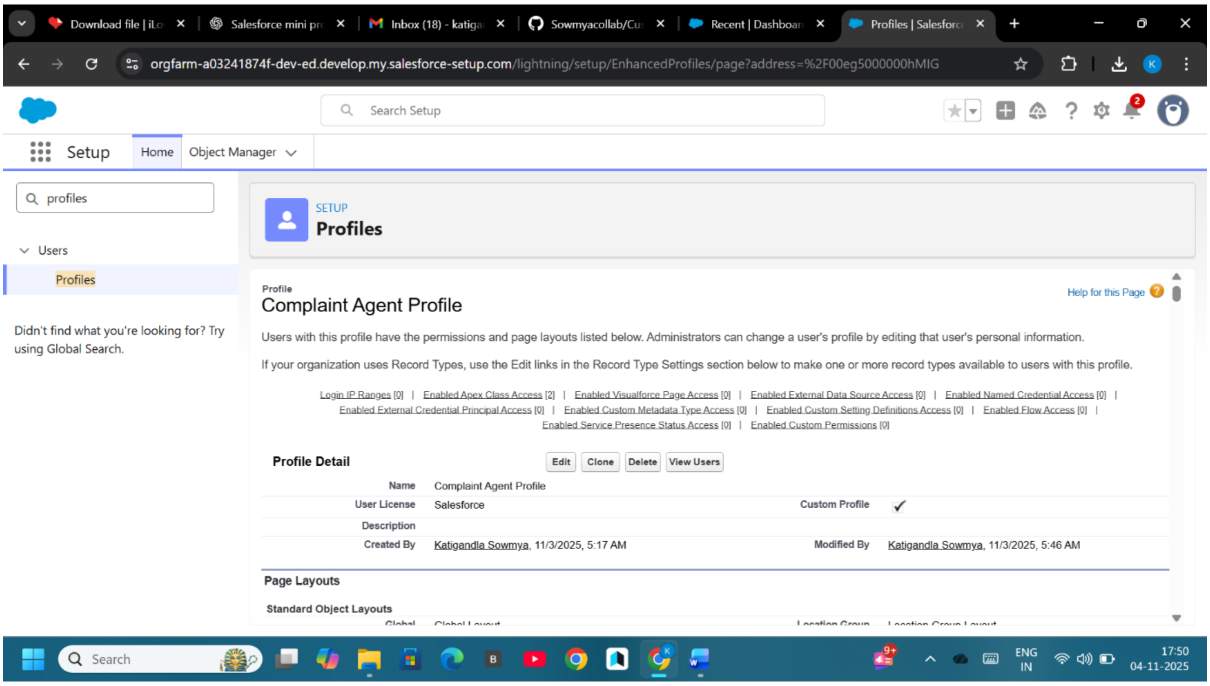
Restricts logins to specific IP ranges to prevent external access.

Steps:

1. Setup → **Profiles → Select Profile (e.g., Support Agent)**
2. Scroll to **Login IP Ranges** → **New**
3. Define allowed range (e.g., company's internal network IPs).

Use Case:

Only allow users to log in from office or company-approved networks.



9. Audit Trail

Description:

Tracks configuration changes and admin activities.

Steps:

1. Setup → **View Setup Audit Trail**
2. Review the list of changes (who changed what and when).

Use Case:

Monitor admin changes to fields, flows, security settings, etc.

🚀 Outcome

After completing **Phase 9**:

- You can generate detailed **reports and dashboards** for complaints and customers.
- Security configurations ensure that **only authorized users** can view or edit data.
- The system becomes **transparent, secure, and audit-ready**, ideal for real business CRM operations.