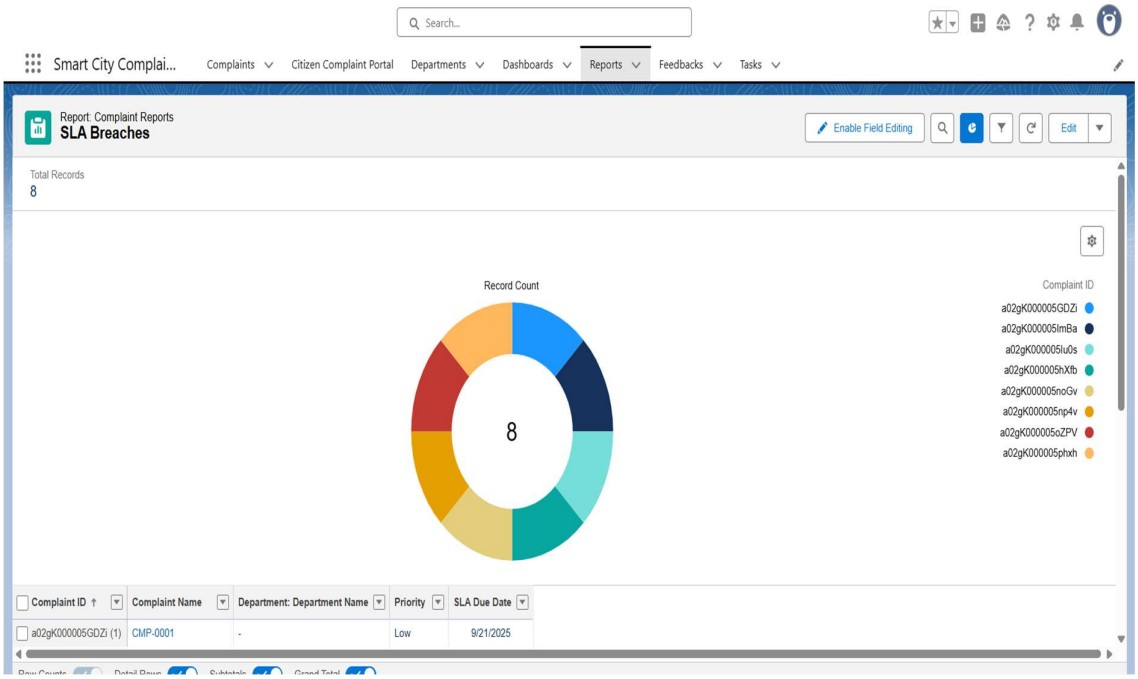
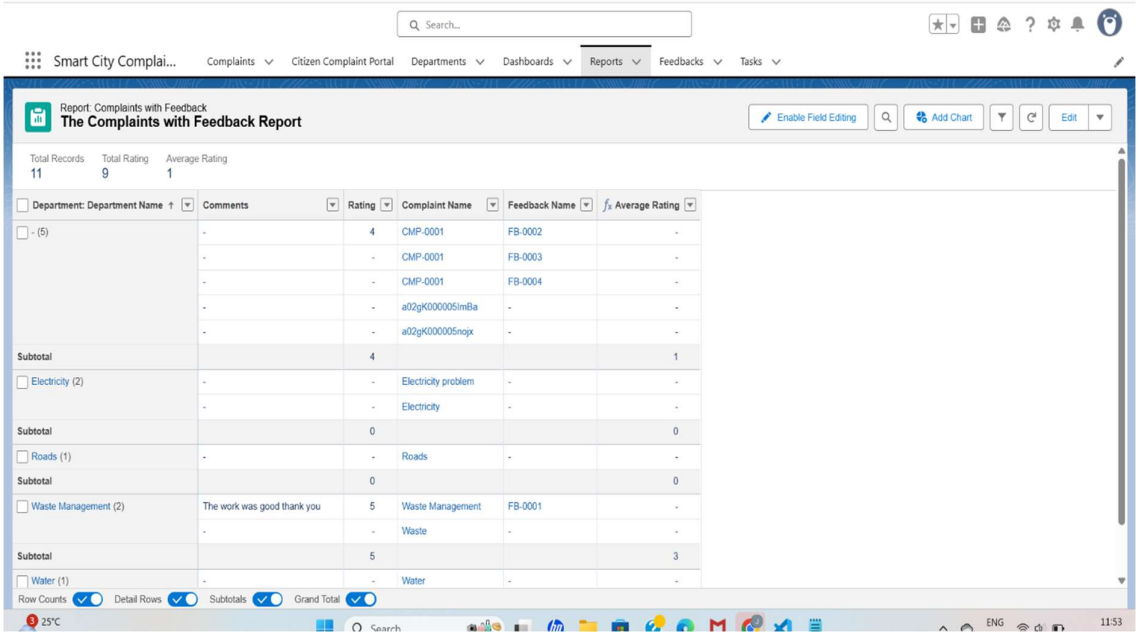
Phase 9: Reporting, Dashboards & Security Review

1. Reports

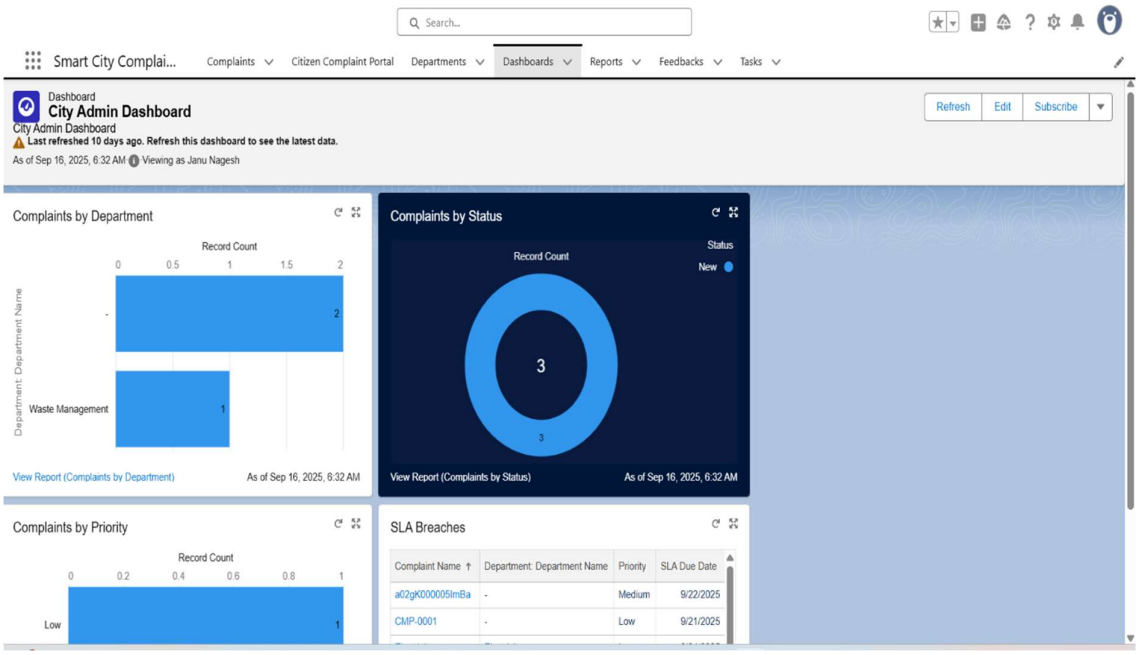
- Types: Tabular (all complaints), Summary (group by Department), Matrix (Complaint vs Priority), Joined (Complaint + Feedback).





2. Dashboards

- Dashboard: City Admin Dashboard.
- Components:
    - Bar Chart → Complaints by Department.
    - Donut → Complaints by Status.
    - Gauge → Avg Feedback Rating.
    - Table → SLA Breaches.



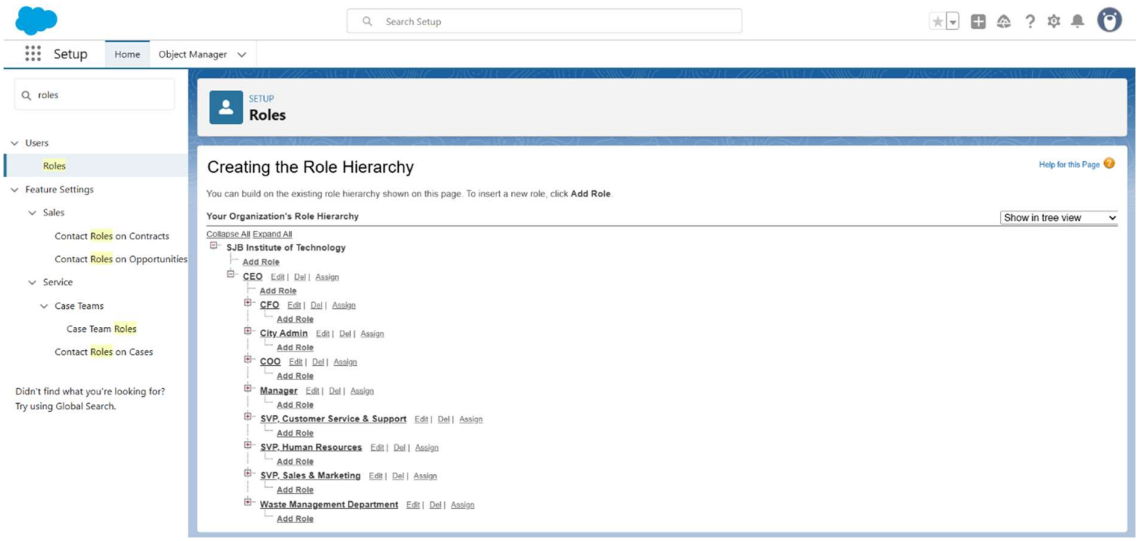
3. Sharing Settings(OWD)

Organization-Wide Defaults (OWD)

1. In Sharing Settings:
    - For Complaint__c → set **Default Internal Access** = Private (recommended)
    - For Department__c → set **Default Internal Access** = Public Read Only
2. Click **Save**.

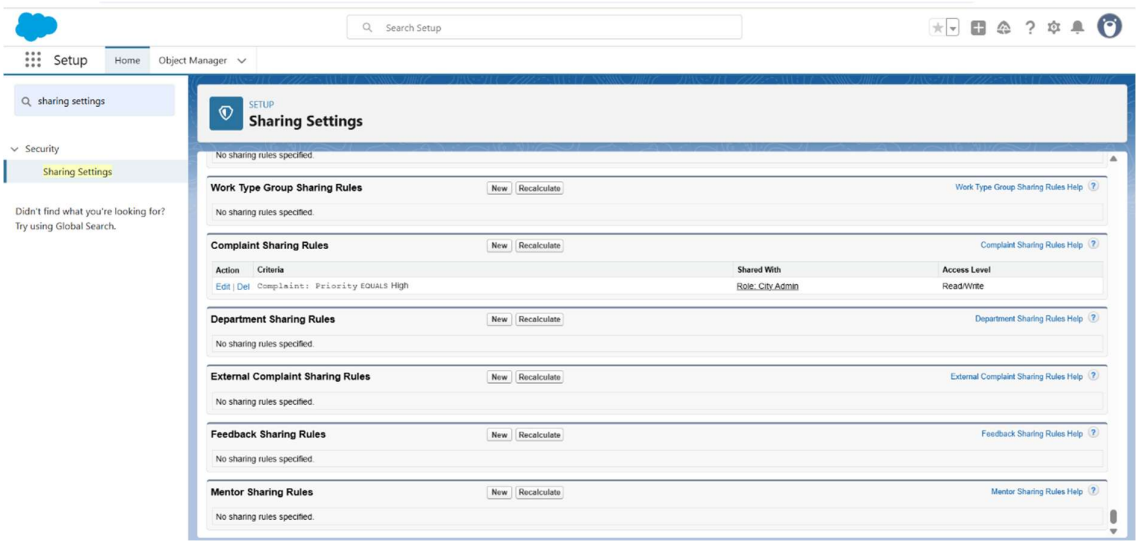
4.Roles

- Setup → Users → Roles → Set Up Roles → Add roles:
    - City Admin
    - Department Manager – Roads
    - Department Manager – Water
    - Citizen User
- Place Department Managers under City Admin as needed.



5. Sharing Rules

1. Setup → Sharing Settings → Scroll to Complaint__c Sharing Rules → New.
2. Rule Label: Share High Priority to Managers
    - Rule Type: Based on Criteria
    - Criteria: Priority__c Equals High
    - Share with: Role → choose Department Manager – Roads (or public groups)
    - Access Level: Read/Write
3. Save and run.



6. Field Level Security (FLS) & Page Layouts

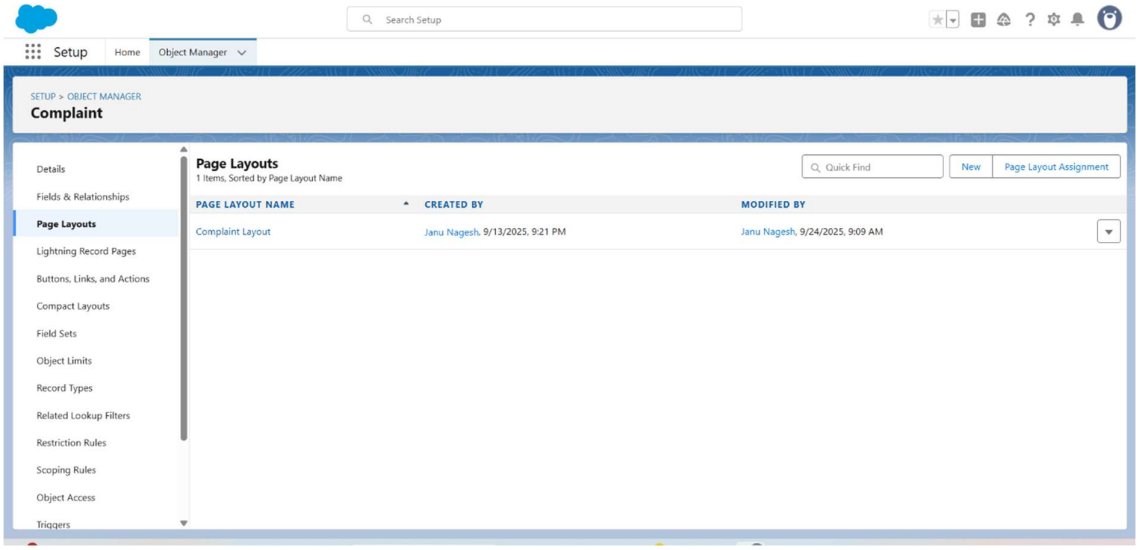
Where: Setup → Object Manager → Complaint__c → Fields & Relationships → click a field → Set Field-Level Security

Steps (example: hide SLA on Citizen profile)

1. Click SLA_Due_Date__c → Set Field-Level Security.
2. Uncheck “Visible” for Citizen Profile (if you have a Citizen profile) → Save.
3. For Admin & Manager, leave Visible checked.

Page Layout

- Object Manager → Complaint__c → Page Layouts → Edit the layout
    - Move fields into sections: Complaint Details, SLA Details, Resolution
    - Add Related Lists: Feedback, Activities
    - Save and assign layout to Profiles if needed.

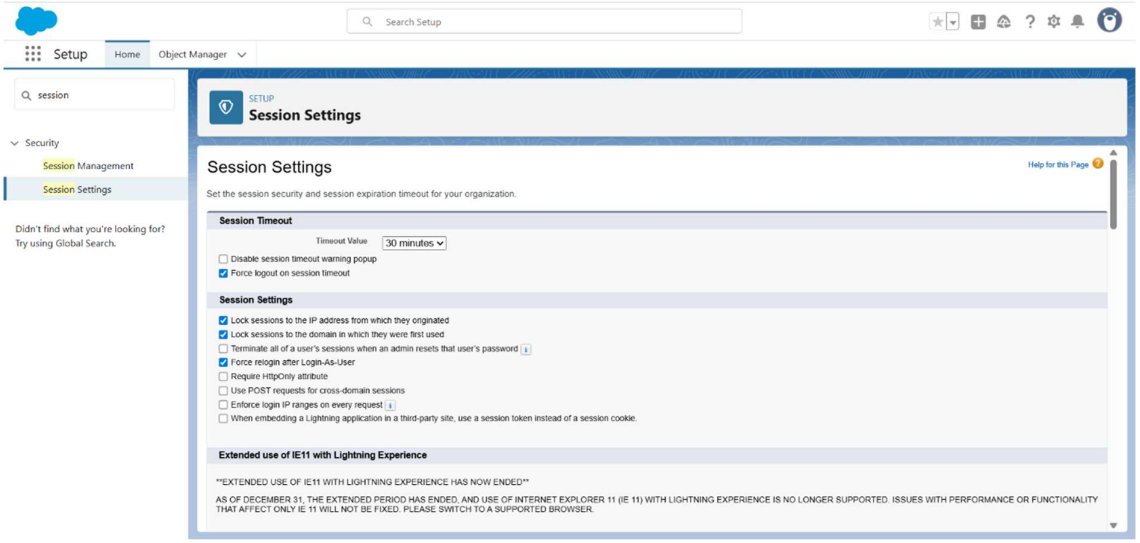


7.Session Settings & Login IP Ranges

- **Session Settings**

  Setup → Security → Session Settings

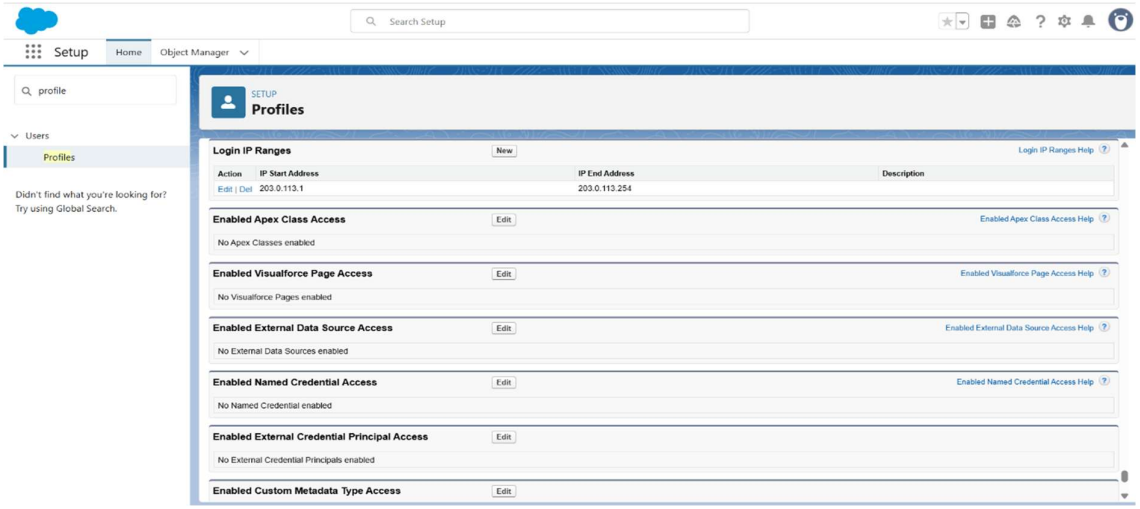
  - **Session Timeout**: choose 30 minutes (example)
  - **Lock sessions to the IP address from which they originated**: optionally enabled for stricter security
  - **Require secure connections (HTTPS)**: should be enabled (checked)
  - Save.



- **Login IP Ranges (Profile level)**

  Setup → Users → Profiles → open profile (e.g., Standard User) → Login IP Ranges → New

  - Start IP Address: 203.0.113.1 (example company range)
  - End IP Address: 203.0.113.254



8. Audit Trail (Setup History)

Where: Setup → Security → View Setup Audit Trail

- Click **Download** to see the last 6 months of setup changes (CSV).
- Use it for compliance & show changes you made.