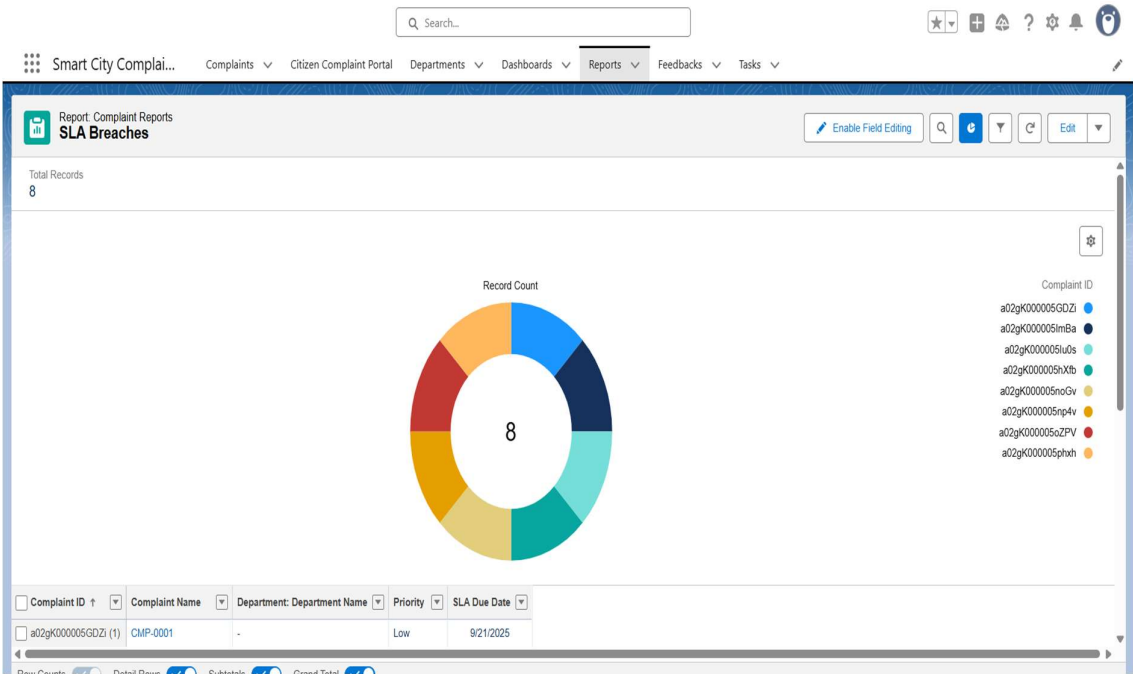


Phase 9: Reporting, Dashboards & Security Review

1. Reports

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



Smart City Complai... Complaints Citizen Complaint Portal Departments Dashboards Reports Feedbacks Tasks

Search...

Report: Complaints with Feedback
The Complaints with Feedback Report

Enable Field Editing

Add Chart

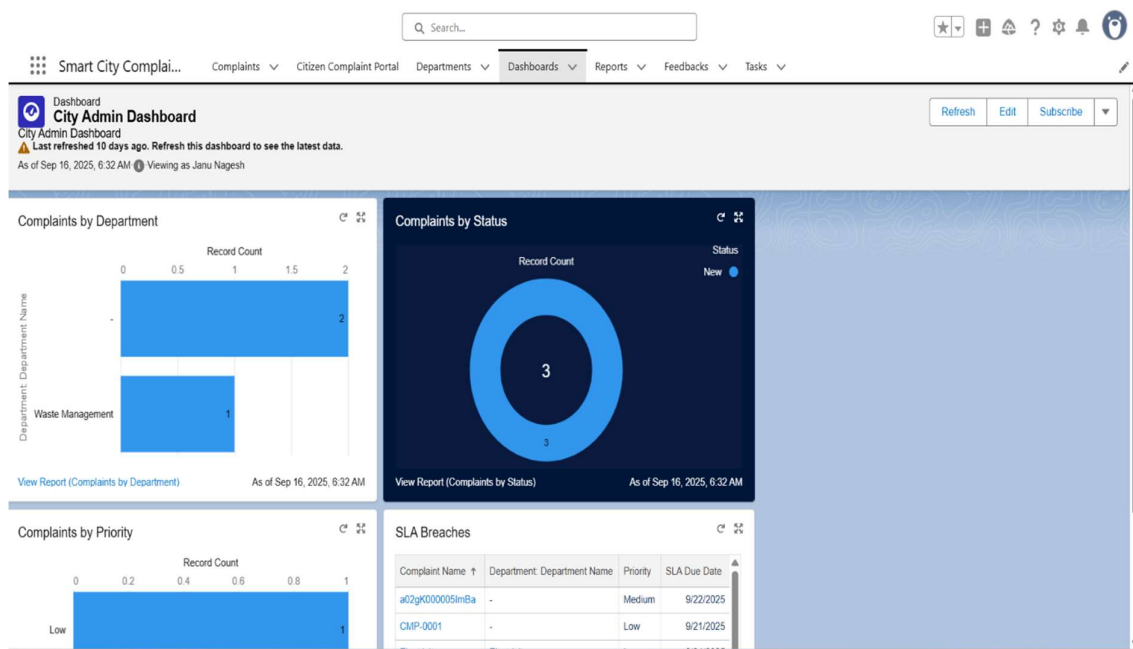
Total Records: 11, Total Rating: 9, Average Rating: 1

Department: Department Name	Comments	Rating	Complaint Name	Feedback Name	Average Rating
- (5)	-	4	CMP-0001	FB-0002	-
-	-	-	CMP-0001	FB-0003	-
-	-	-	CMP-0001	FB-0004	-
-	-	-	a02gK000005ImBa	-	-
-	-	-	a02gK000005nqpx	-	-
Subtotal		4			1
Electricity (2)	-	-	Electricity problem	-	-
-	-	-	Electricity	-	-
Subtotal		0			0
Roads (1)	-	-	Roads	-	-
Subtotal		0			0
Waste Management (2)	The work was good thank you	5	Waste Management	FB-0001	-
-	-	-	Waste	-	-
Subtotal		5			3
Water (1)	-	-	Water	-	-

Row Counts: Detail Rows Subtotals Grand Total

2. Dashboards

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



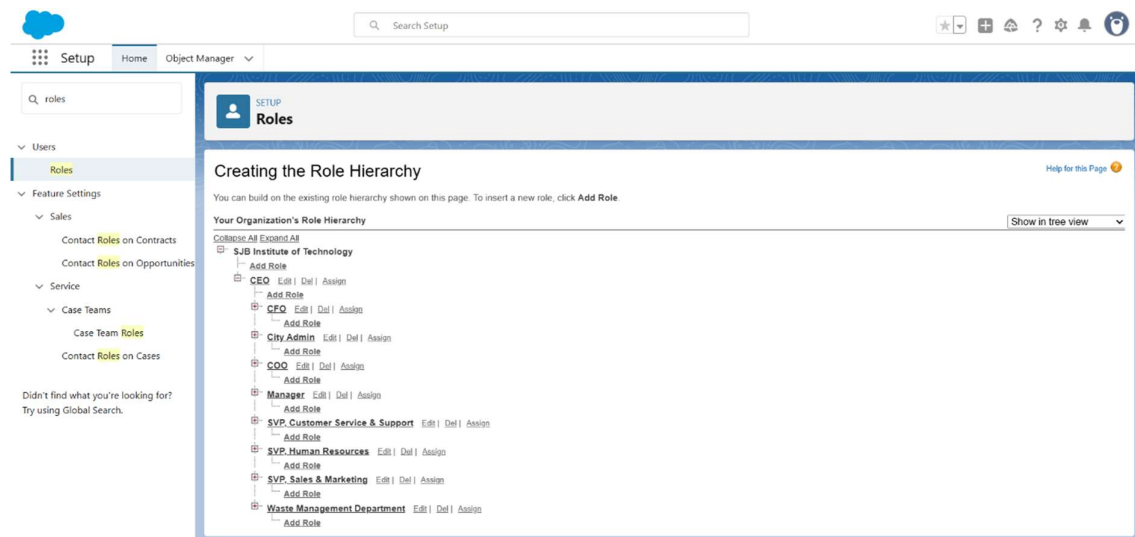
3. Sharing Settings(OWD)

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**.

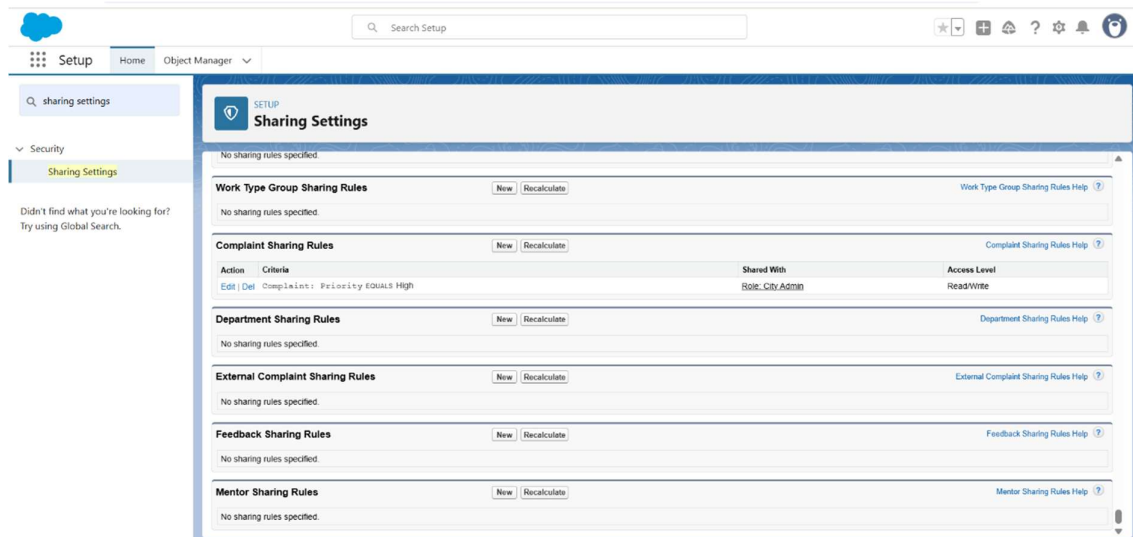
4.Roles

- 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

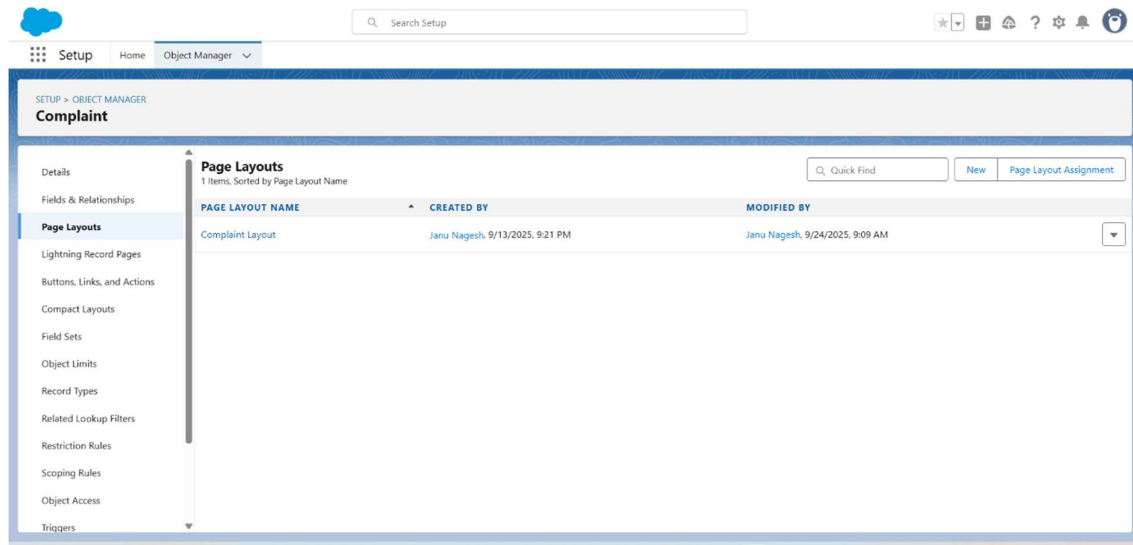
Where: Setup → Object Manager → Complaint__c → Fields & Relationships → click a field → Set Field-Level Security

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.

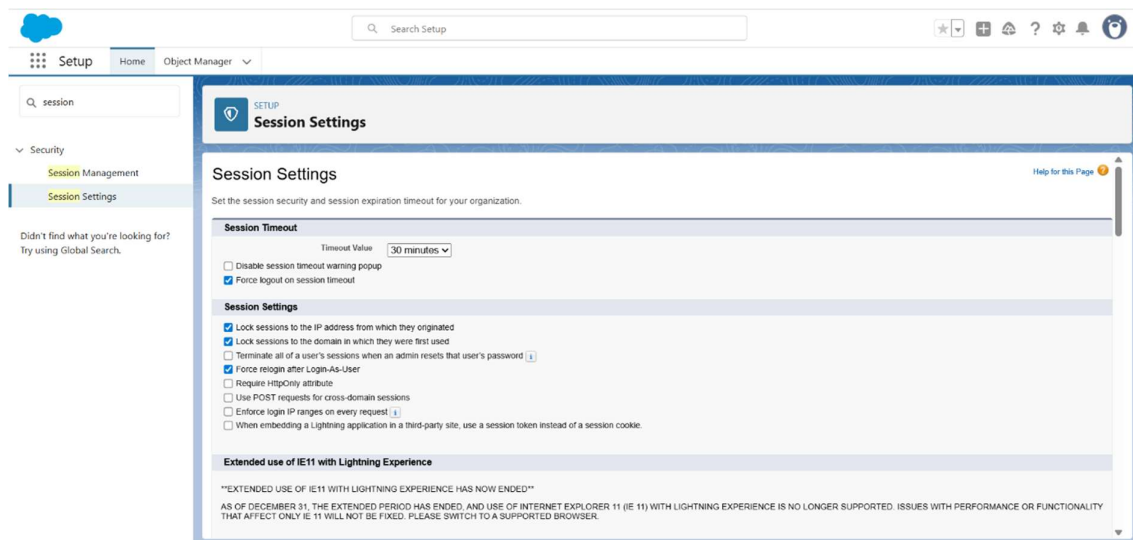


7.Session Settings & Login IP Ranges

- **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

The screenshot shows the Salesforce Setup interface. On the left, the navigation menu includes 'Setup', 'Home', and 'Object Manager'. The 'Users' section is expanded, showing 'Profiles'. The main content area is titled 'SETUP Profiles'. Under the 'Login IP Ranges' section, there is a table with columns: Action, IP Start Address, IP End Address, and Description. The table contains one row with 'Edit | Del' links, '203.0.113.1' as the start address, '203.0.113.254' as the end address, and an empty description. Below this, several other sections are listed, each with an 'Edit' link and a help icon: 'Enabled Apex Class Access', 'Enabled Visualforce Page Access', 'Enabled External Data Source Access', 'Enabled Named Credential Access', 'Enabled External Credential Principal Access', and 'Enabled Custom Metadata Type Access'.

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.

The screenshot shows the Salesforce Setup interface with the 'Security' section expanded and 'View Setup Audit Trail' selected. The main content area is titled 'SETUP View Setup Audit Trail'. It displays a table of setup changes with columns for Date/Time, User, Action, and Category. The table lists various actions such as 'Changed role for user Ram Shetty from Road Department Manager to Roads Department Manager', 'Created new role Roads Department Manager', 'Changed role Waste Management Department', 'Requested an export', 'For the 01gK000002ESuX duplicate rule Duplicate Complaint by Email, changed "Active" from "false" to "true"', 'Complaint matching rule, Match Complaint by Email, activating by Janu Nagesh', 'For duplicate rule: Duplicate Complaint by Email, changed matching rules', 'Created new 01gK000002ESuX duplicate rule "Duplicate Complaint by Email". Set "Record-Level Security" to "Enforce sharing rules"', 'For matching rule Match Complaint by Email, added matching criteria where matching method is Exact, the field is Citizen_Email and match blank fields is "Match When both blank"', 'For matching rule Match Complaint by Email, matching engine set to Exact Match Engine', 'Created new Complaint matching rule Match Complaint by Email', 'Created ExternalAPIClient Apex Class code', 'Created ComplaintSOAP Apex Class code', and 'Created ComplaintResAPI Apex Class code'. At the bottom, there is a link to 'Download setup.audit.trail for last six months (Excel .csv file)'.