Phase 9: Reporting, Dashboards & Security Review

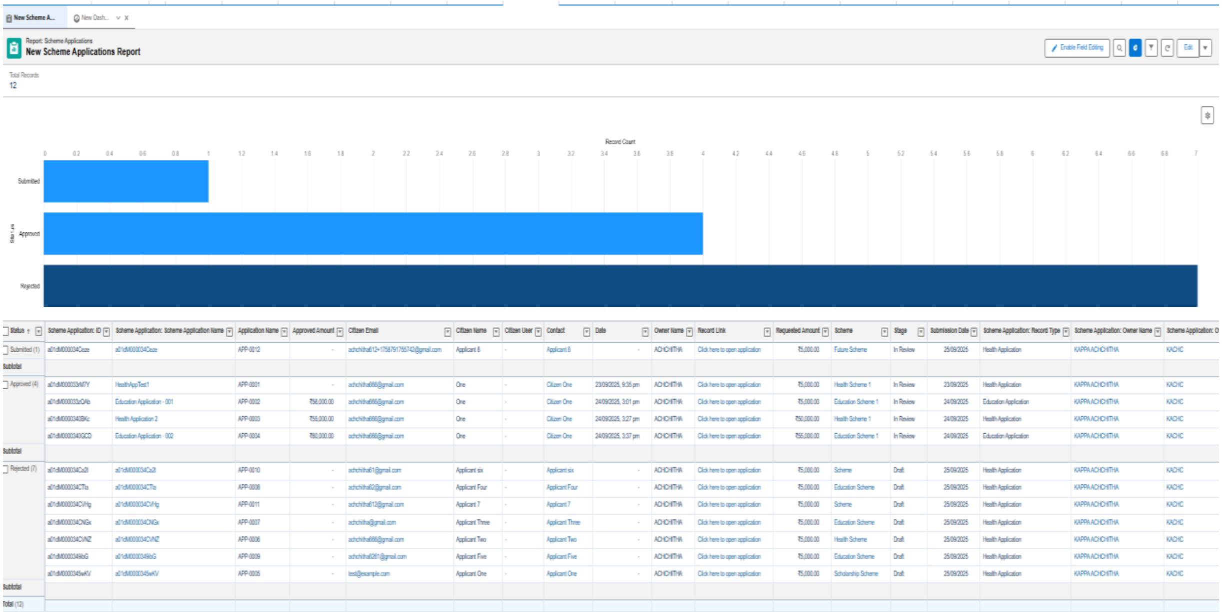
Reports

Reports allow users to analyze and display Salesforce data in a structured way. In the **Govt Schemes Management System**, reports were created to track and analyze applications submitted by citizens. Key reports include **All Scheme Applications**, **Applications by Scheme**, and **Applications by Status**.

Steps to create reports:

1. Navigate to **Reports tab → New Report**.
2. Select **Scheme Applications** as the report type.
3. Add the following columns:
   - **Scheme Name**
   - **Requested Amount**
   - **Citizen Name / Email**
   - **Submission Date**
   - **Status**
4. Group records for summary reports:
   - **Applications by Scheme** → group by **Scheme Name** to see which schemes have the most applications.
   - **Applications by Status** → group by **Status** to track pending, approved, and rejected applications.
5. Apply filters as required:
   - **Citizen Email = Current User** → for reports displayed to citizens
   - **No filter** → for officer/admin reports showing all applications
6. Save reports in the folder **GovSchemes Reports**.

These reports allow officers to monitor submissions and citizens to track their own applications.



Report Types

- **Standard report type:** Scheme Applications was sufficient for all reporting needs.
- **Custom report types:** Not required for this project since all necessary fields were available in the standard object.

Dashboards

Dashboards provide a visual summary of report data. For this project, dashboards were created to display **application distribution by scheme** and **status of applications**.

Steps to create dashboards:

1. Navigate to **Dashboards** → **New Dashboard** → **Select GovSchemes Reports folder**.
2. Add components:
   - **Bar Chart / Column Chart** → for **Applications by Scheme**
   - **Pie Chart / Donut Chart** → for **Applications by Status**

3. Set component titles:
    - **“Applications by Scheme”** → shows which schemes are most applied.
    - **“Applications by Status”** → shows the count of Pending, Approved, Rejected applications.
4. Save and run the dashboard.

Dashboards provide officers with actionable insights at a glance, helping prioritize verification and approval processes.

Dynamic Dashboards

Dynamic dashboards allow users to see data according to their access level. In this project:

- **Citizens** see dashboards filtered by **their own applications**.
- **Officers / Admins** see all applications.
- **Implementation:** Component visibility and report filters in **Experience Cloud** were configured to restrict access accordingly.

Sharing Settings

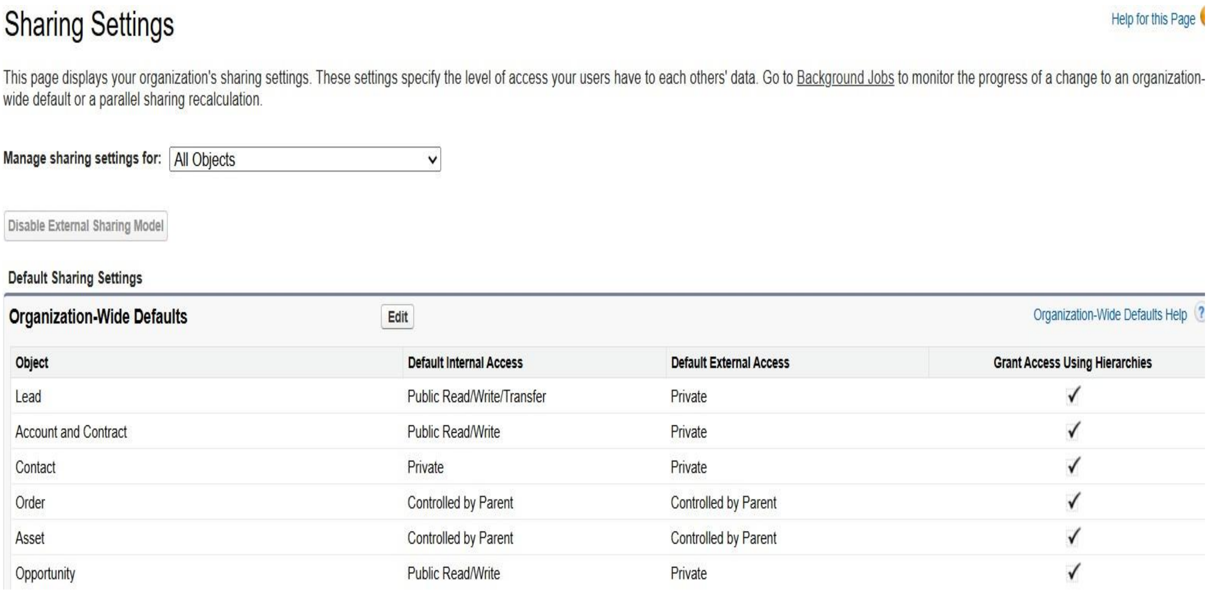
Goal: Officers can view all applications; Citizens can view only their own.

Steps:

1. Go to **Setup** → **Sharing Settings**.
2. Scroll to **Organization-Wide Defaults (OWD)**:
    - **Scheme_Application__c** = **Private** (so only owners or those with permission see records).

3. Scroll to **Roles & Role Hierarchy** → ensure officers/admins are above citizens in the hierarchy.

Citizens automatically see only their own applications because of the **OWD = Private** setting.



Sharing Settings

Help for this Page

This page displays your organization's sharing settings. These settings specify the level of access your users have to each others' data. Go to Background Jobs to monitor the progress of a change to an organization-wide default or a parallel sharing recalculation.

Manage sharing settings for: All Objects

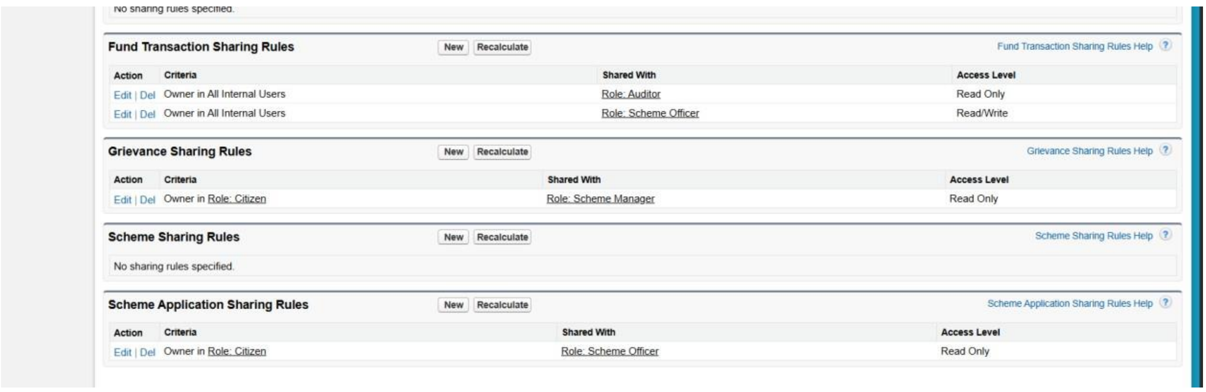
Disable External Sharing Model

Default Sharing Settings

Organization-Wide Defaults Edit — Organization-Wide Defaults Help

Object	Default Internal Access	Default External Access	Grant Access Using Hierarchies
Lead	Public Read/Write/Transfer	Private	✓
Account and Contract	Public Read/Write	Private	✓
Contact	Private	Private	✓
Order	Controlled by Parent	Controlled by Parent	✓
Asset	Controlled by Parent	Controlled by Parent	✓
Opportunity	Public Read/Write	Private	✓

Work Type Group	Public Read/Write	Private	✓
Fund Transaction	Public Read/Write	Private	✓
Grievance	Public Read/Write	Private	✓
Scheme	Public Read Only	Public Read Only	✓
Scheme Application	Private	Private	



No sharing rules specified.

Fund Transaction Sharing Rules New Recalculate — Fund Transaction Sharing Rules Help

Action	Criteria	Shared With	Access Level
Edit | Del	Owner in All Internal Users	Role: Auditor	Read Only
Edit | Del	Owner in All Internal Users	Role: Scheme Officer	Read/Write

Grievance Sharing Rules New Recalculate — Grievance Sharing Rules Help

Action	Criteria	Shared With	Access Level
Edit | Del	Owner in Role: Citizen	Role: Scheme Manager	Read Only

Scheme Sharing Rules New Recalculate — Scheme Sharing Rules Help

No sharing rules specified.

Scheme Application Sharing Rules New Recalculate — Scheme Application Sharing Rules Help

Action	Criteria	Shared With	Access Level
Edit | Del	Owner in Role: Citizen	Role: Scheme Officer	Read Only

Field Level Security (FLS)

Goal: Control visibility of sensitive fields.

Steps:

1. Go to **Setup → Object Manager → Scheme_Application__c → Fields & Relationships**.
2. Click the field (e.g., Citizen Email, Approved Amount).
3. Click **Set Field-Level Security**.
4. Set visibility:
   - Officers/Admins = **Visible**
   - Citizens = **Visible / Hidden** depending on sensitivity
5. Repeat for all fields (e.g., Scheme Name, Submission Date visible to all).

Set Field-Level Security

Approved Amount

Help for t

Save Cancel

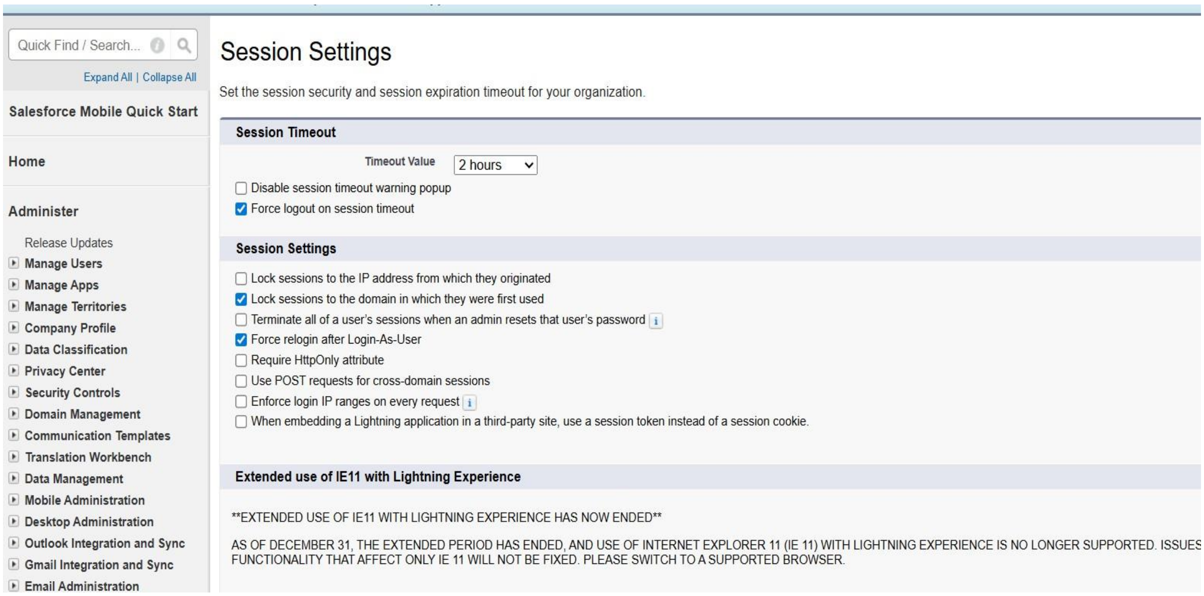
Field Label: Approved Amount

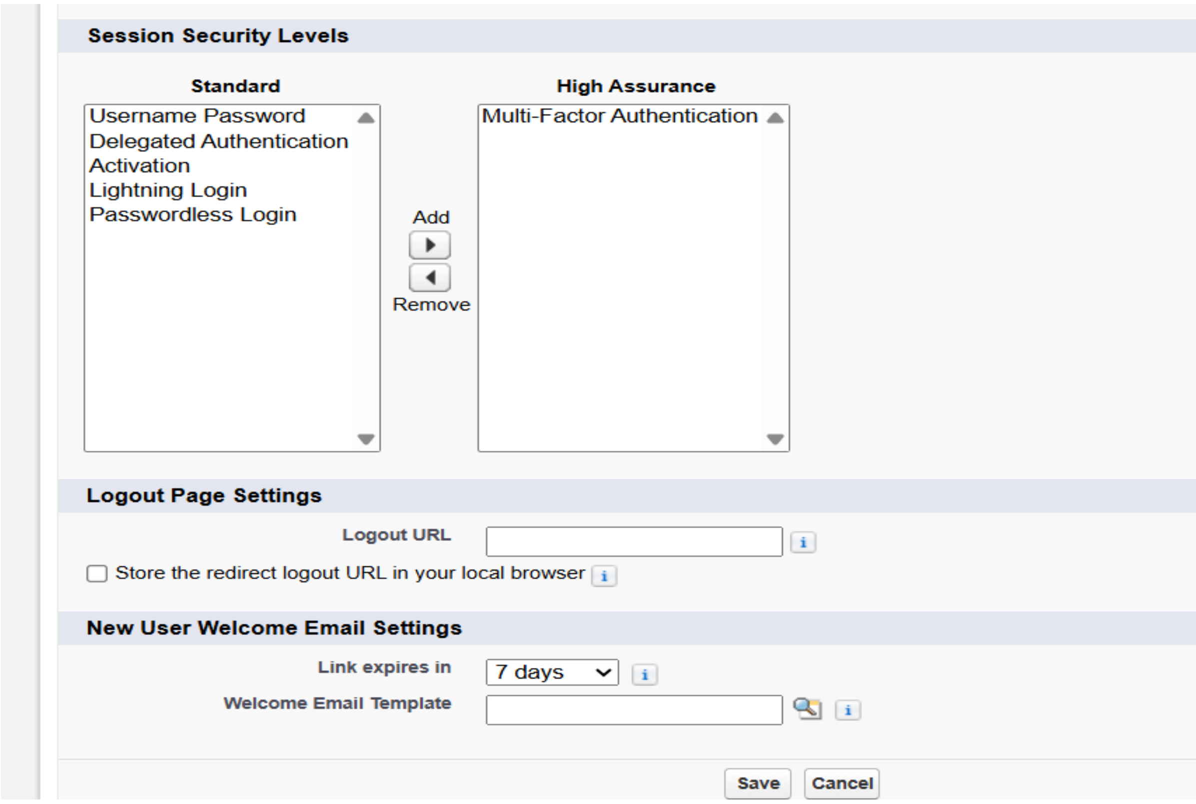
Data Type: Currency(16, 2)

Field-Level Security for Profile	☐ Visible	☐ Read-Only
Analytics Cloud Integration User	☑	☐
Analytics Cloud Security User	☑	☐
Anypoint Integration	☑	☐
Auditor	☑	☑
Authenticated Website	☐	☐
Authenticated Website	☐	☐
B2B Reordering Portal Buyer Profile	☐	☐
BI Integration User	☑	☑
Citizen Profile	☑	☐
Contract Manager	☑	☐
Cross Org Data Proxy User	☑	☐
Custom: Marketing Profile	☑	☐
Officer	☑	☐
Partner App Subscription User	☑	☐
Partner Community Login User	☐	☐
Partner Community User	☐	☐
Read Only	☑	☐
Salesforce API Only System Integrations	☑	☐
Scheme Officer Profile	☑	☐
Silver Partner User	☐	☐
Solution Manager	☑	☐
Standard Platform User	☑	☐
Standard User	☑	☑
System Administrator	☑	☐
Work.com Only User	☑	☐

Session Settings

Session settings determine session timeout and security policies. Default session settings were used for this project.



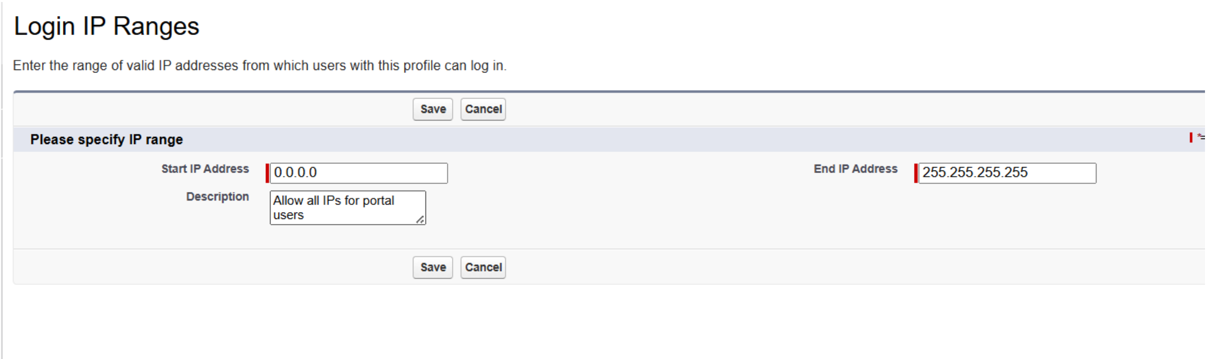


Login IP Ranges

Goal: Allow access from anywhere.

Steps:

1. Go to **Setup → Profiles → Select Profile (e.g., Citizen Portal User)**.
2. Scroll to **Login IP Ranges** → leave blank or set a wide range to allow global access.
3. Save changes.



Audit Trail

Goal: Track configuration changes for accountability.

Steps:

1. Go to **Setup → Security → View Setup Audit Trail**.
2. Salesforce automatically tracks changes for the past 6 months.
3. Export logs periodically if needed:
   - Click **Download** → CSV format

This helps monitor who changed dashboards, reports, or sharing settings.