

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**.

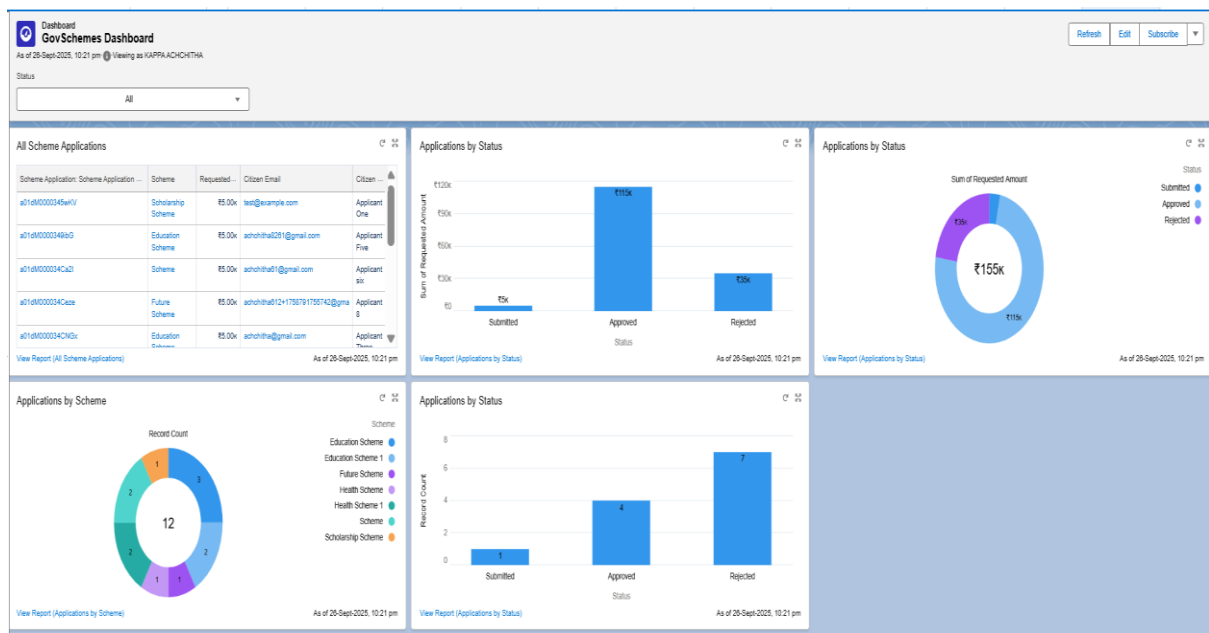
These reports allow officers to monitor submissions and citizens to track their own applications.

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	<input type="checkbox"/>

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 Help for t

Approved Amount

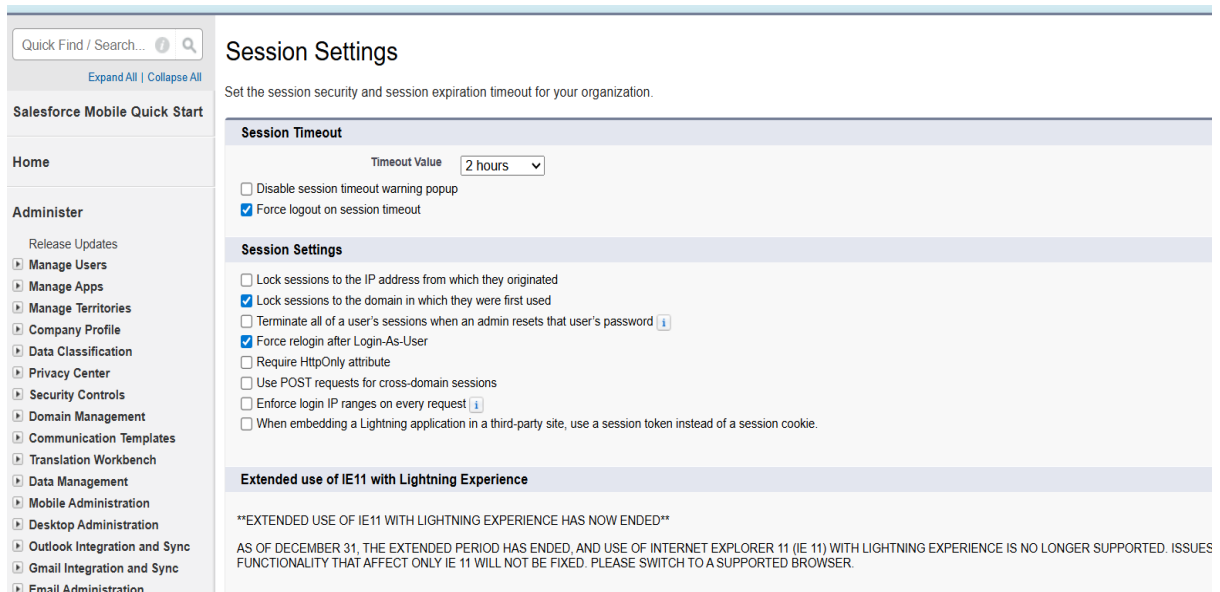
Save Cancel

Field Label	Approved Amount
Data Type	Currency(16, 2)


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

Session Settings

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



The screenshot shows the Salesforce Session Settings page. On the left is a navigation sidebar with links like 'Home', 'Administer', 'Release Updates', 'Manage Users', 'Manage Apps', 'Manage Territories', 'Company Profile', 'Data Classification', 'Privacy Center', 'Security Controls', 'Domain Management', 'Communication Templates', 'Translation Workbench', 'Data Management', 'Mobile Administration', 'Desktop Administration', 'Outlook Integration and Sync', 'Gmail Integration and Sync', and 'Email Administration'. The main content area is titled 'Session Settings' and includes a sub-header 'Set the session security and session expiration timeout for your organization.' Below this are three sections: 'Session Timeout' with a 'Timeout Value' dropdown set to '2 hours' and checkboxes for 'Disable session timeout warning popup' (unchecked) and 'Force logout on session timeout' (checked); 'Session Settings' with checkboxes for 'Lock sessions to the IP address from which they originated' (unchecked), 'Lock sessions to the domain in which they were first used' (checked), 'Terminate all of a user's sessions when an admin resets that user's password' (unchecked), 'Force relogin after Login-As-User' (checked), 'Require HttpOnly attribute' (unchecked), 'Use POST requests for cross-domain sessions' (unchecked), 'Enforce login IP ranges on every request' (unchecked), and 'When embedding a Lightning application in a third-party site, use a session token instead of a session cookie' (unchecked); and 'Extended use of IE11 with Lightning Experience' with a notice that the extended use has ended and that IE 11 is no longer supported.

Quick Find / Search... 

[Expand All](#) | [Collapse All](#)

Salesforce Mobile Quick Start

Home

Administer

- Release Updates
- Manage Users
- Manage Apps
- Manage Territories
- Company Profile
- Data Classification
- Privacy Center
- Security Controls
- Domain Management
- Communication Templates
- Translation Workbench
- Data Management
- Mobile Administration
- Desktop Administration
- Outlook Integration and Sync
- Gmail Integration and Sync
- Email Administration

Session Settings

Set the session security and session expiration timeout for your organization.

Session Timeout

Timeout Value **2 hours**


☐ Disable session timeout warning popup

☒ Force logout on session timeout

Session Settings

☐ Lock sessions to the IP address from which they originated


☒ Lock sessions to the domain in which they were first used

☐ Terminate all of a user's sessions when an admin resets that user's password 

☒ Force relogin after Login-As-User

☐ Require HttpOnly attribute

☐ Use POST requests for cross-domain sessions

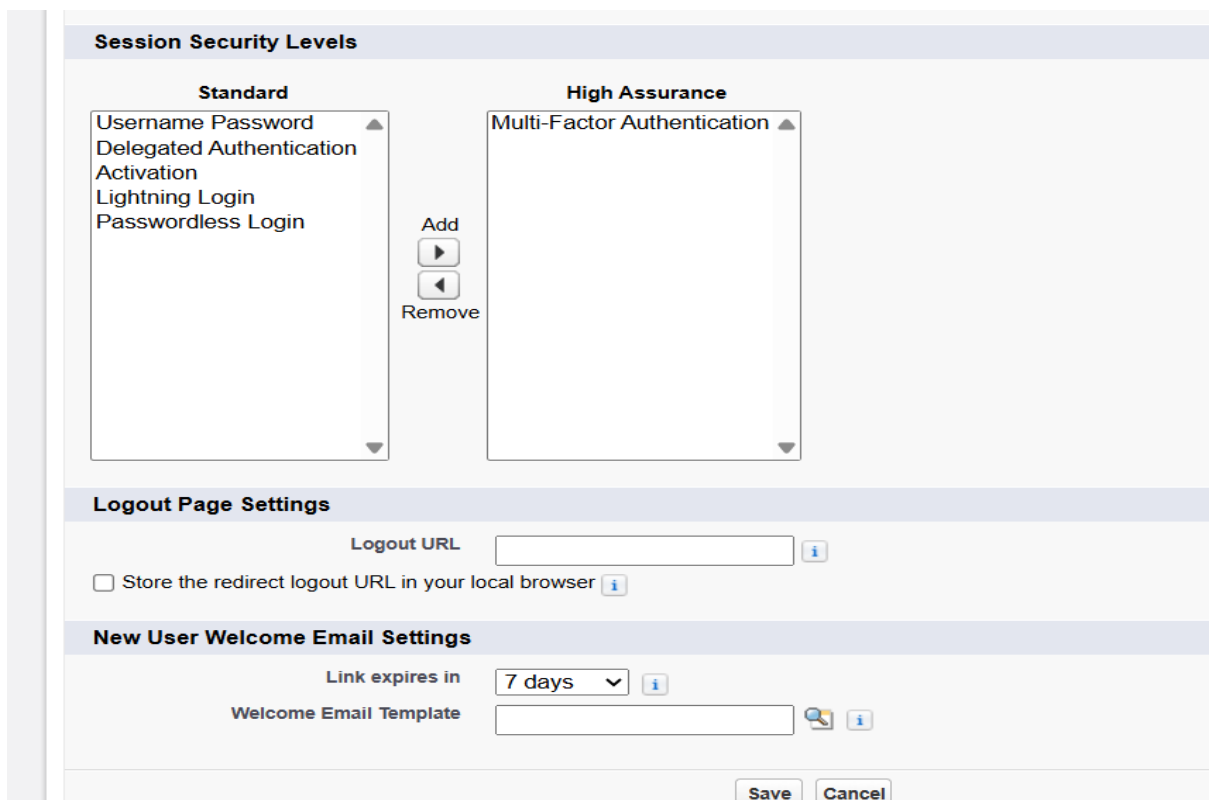
☐ Enforce login IP ranges on every request 

☐ When embedding a Lightning application in a third-party site, use a session token instead of a session cookie.

Extended use of IE11 with Lightning Experience

****EXTENDED USE OF IE11 WITH LIGHTNING EXPERIENCE HAS NOW ENDED****

AS OF DECEMBER 31, THE EXTENDED PERIOD HAS ENDED, AND USE OF INTERNET EXPLORER 11 (IE 11) WITH LIGHTNING EXPERIENCE IS NO LONGER SUPPORTED. ISSUES FUNCTIONALITY THAT AFFECT ONLY IE 11 WILL NOT BE FIXED. PLEASE SWITCH TO A SUPPORTED BROWSER.



The screenshot shows the Salesforce Session Security Levels page. It features two columns: 'Standard' and 'High Assurance'. The 'Standard' column contains a list of authentication methods: 'Username Password', 'Delegated Authentication', 'Activation', 'Lightning Login', and 'Passwordless Login'. The 'High Assurance' column contains a list with 'Multi-Factor Authentication'. Between the columns are 'Add' and 'Remove' buttons. Below the columns is the 'Logout Page Settings' section with a 'Logout URL' field and a checkbox for 'Store the redirect logout URL in your local browser'. The 'New User Welcome Email Settings' section includes a 'Link expires in' dropdown set to '7 days' and a 'Welcome Email Template' field. At the bottom are 'Save' and 'Cancel' buttons.

Session Security Levels

Standard

Username Password
Delegated Authentication
Activation
Lightning Login
Passwordless Login

High Assurance

Multi-Factor Authentication

Add

Remove

Logout Page Settings

Logout URL

☐ Store the redirect logout URL in your local browser

New User Welcome Email Settings

Link expires in **7 days**

Welcome Email Template

Save **Cancel**

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.

Login IP Ranges

Enter the range of valid IP addresses from which users with this profile can log in.

Save

Cancel

Please specify IP range

Start IP Address

0.0.0.0

End IP Address

255.255.255.255

Description

Allow all IPs for portal users

Save

Cancel

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.

View Setup Audit Trail

The last 20 entries for your organization are listed below. You can [download](#) your organization's setup audit trail for the last six months (Excel .csv file).

View Setup Audit Trail				
Date	User	Source Namespace Prefix	Action	Section
26/09/2025, 11:32:06 pm IST	achchitha_govtschemes@rvrjc.com		Added Login Ip Range to Citizen Profile from 0.0.0.0 to 255.255.255.255	Manage Users
26/09/2025, 11:29:17 pm IST	achchitha_govtschemes@rvrjc.com		The custom field option Required for Contact on object Scheme Applications has changed from off to on	Custom Objects
26/09/2025, 11:29:17 pm IST	achchitha_govtschemes@rvrjc.com		Changed permission set 00e1a000000MWaCAAW: field-level security for Scheme Application: Contact was changed from Read/Write to No Access	Manage Users
26/09/2025, 11:29:17 pm IST	achchitha_govtschemes@rvrjc.com		Changed permission set 00e1a000000MWaGAAW: field-level security for Scheme Application: Contact was changed from Read/Write to No Access	Manage Users
26/09/2025, 11:29:17 pm IST	achchitha_govtschemes@rvrjc.com		Changed permission set 00edM000000lym7RQAR: field-level security for Scheme Application: Contact was changed from Read/Write to No Access	Manage Users
26/09/2025, 11:29:17 pm IST	achchitha_govtschemes@rvrjc.com		Changed permission set 00e1P000000RmH5QAK: field-level security for Scheme Application: Contact was changed from Read/Write to No Access	Manage Users
26/09/2025, 11:29:17 pm IST	achchitha_govtschemes@rvrjc.com		Changed permission set 00ex00000018ozk_128_09_04_12_4: field-level security for Scheme Application: Contact was changed from Read/Write to No Access	Manage Users