**Project hospital and clinic management model**

***Phase 9: Reporting, Dashboards & Security Review***

1. ***Reports (Tabular, Summary, Matrix, Joined)***

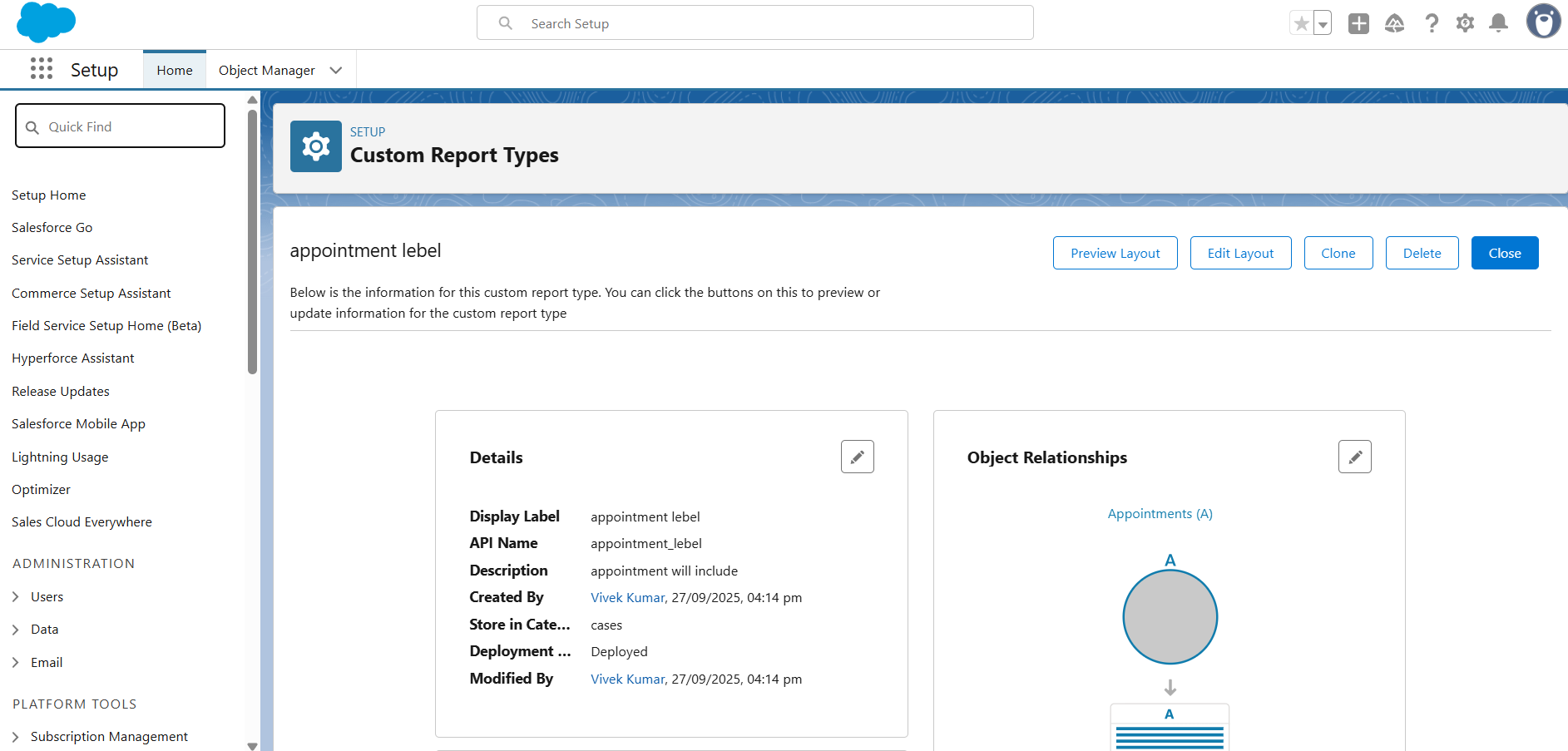
1. Navigate: App Launcher → Reports → New Report Select object or report type (e.g., Patients, Appointments, Prescriptions, Payments).
2. Choose report format:

Tabular: Simple list

Summary: Grouped rows, subtotals

Matrix: Rows & columns grouped, ideal for comparisons

1. Joined: Combine multiple reports into one
2. Apply filters.
3. Group data by fields if needed.
4. Save report with descriptive name.



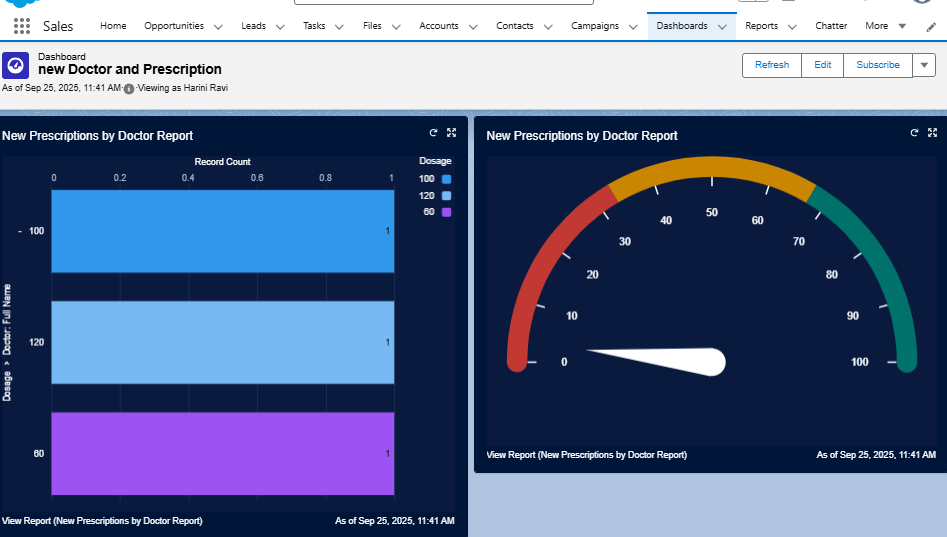
1. ***Report Types***

**Purpose :** Define which objects and relationships are available for reporting.

1. Setup → Report Types → New Custom Report Type
2. Select Primary Object (e.g., Prescription)
3. Add Related Objects
4. Define label, name, and description
5. Save.
6. ***Dashboards***

**Purpose:** Visualize reports in charts and graphs.

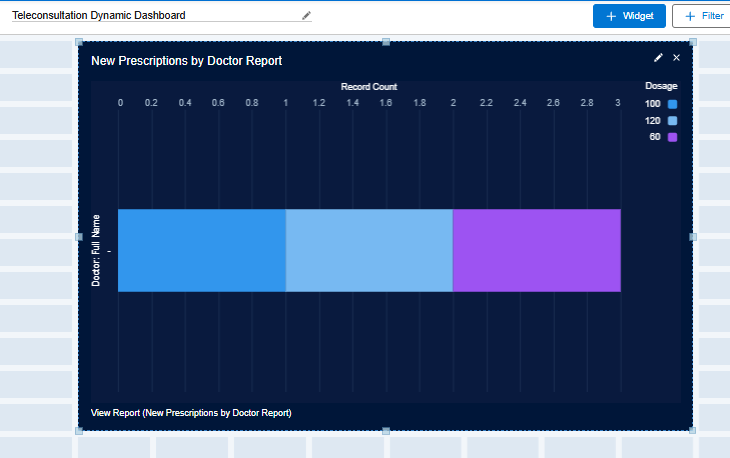
1. App Launcher → Dashboards → New Dashboard
2. Choose folder and name
3. Add components (charts, tables) based on reports
4. Select component type (Bar, Pie, Line, Metric)
5. Configure filters and data source (report)
6. Save and run dashboard



1. ***Dynamic Dashboards***

**Purpose:** Show data based on the logged-in user.

1. In the dashboard, click View Dashboard As → Run as Logged-in User
2. Save dashboard
3. Verify:
4. Doctor → sees only their prescriptions/appointments
5. Admin → sees all data
6. Support Staff → sees only records they can access.



1. ***Sharing Settings***

**Purpose :** Control record-level access.

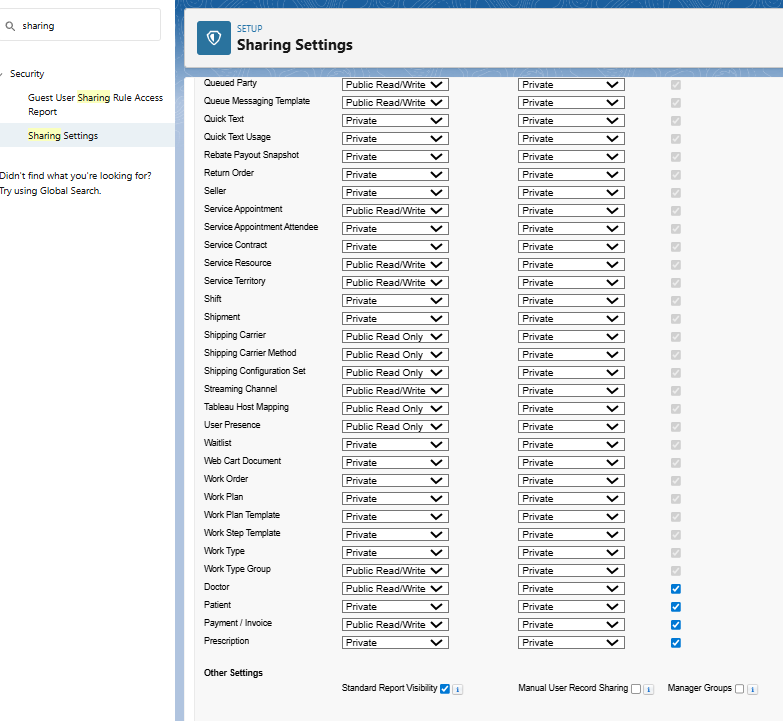
1. Setup → Sharing Settings
2. Set Org-Wide Defaults (OWD):

Patient → Private

Appointment → Controlled by Parent

Prescription → Private

1. Create Sharing Rules to give access to roles/groups:
2. Patient → Doctors → Read/Write
3. Appointment → Support Staff → Read Only



1. ***Field Level Security (FLS)***

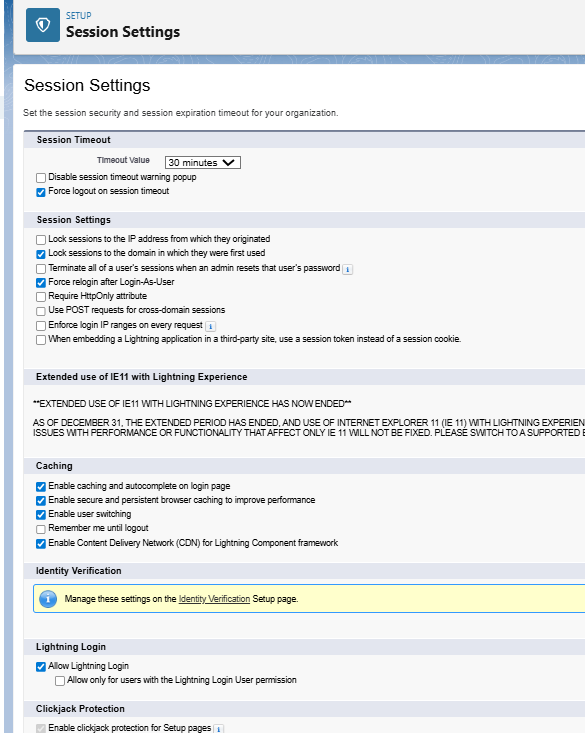
**Purpose :** Control field visibility per profile or permission set.

1. Setup → Object Manager → [Object] → Fields & Relationships → Field-Level Security
2. Select profiles to hide/edit fields
3. Use Permission Sets to grant extra access without changing profiles.
4. ***Session Settings***

**Purpose :** Control login behavior and security policies.

1. Setup → Session Settings
2. Configure:

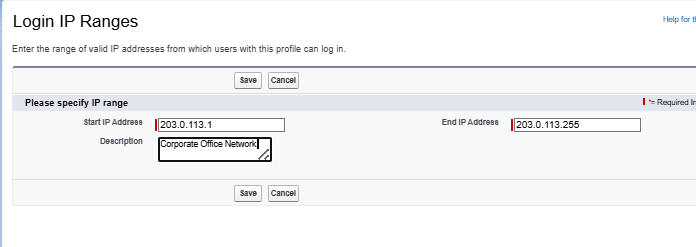
* Session timeout.
* Force logout on timeout
* Concurrent login restrictions
* High-risk session options if needed



1. ***Login IP Ranges***

**Purpose :** Restrict login access to trusted networks.

1. Setup → Profiles → [Profile] → Login IP Ranges
2. Click New → set Start IP and End IP
3. Save → only users from these IPs can log in



1. ***Audit Trail***

**Purpose :** Track administrative changes for compliance and troubleshooting.

1. Setup → View Setup Audit Trail
2. Review changes: objects, fields, profiles, permission sets
3. Download CSV to see up to 180 days of history
4. Use for compliance, troubleshooting, or documenting changes
5. I downloaded the file.
6. To see older history (up to 180 days):
7. Click Download to export a CSV file.
8. Open the CSV in Excel/Sheets to sort or filter by date, user, or action.