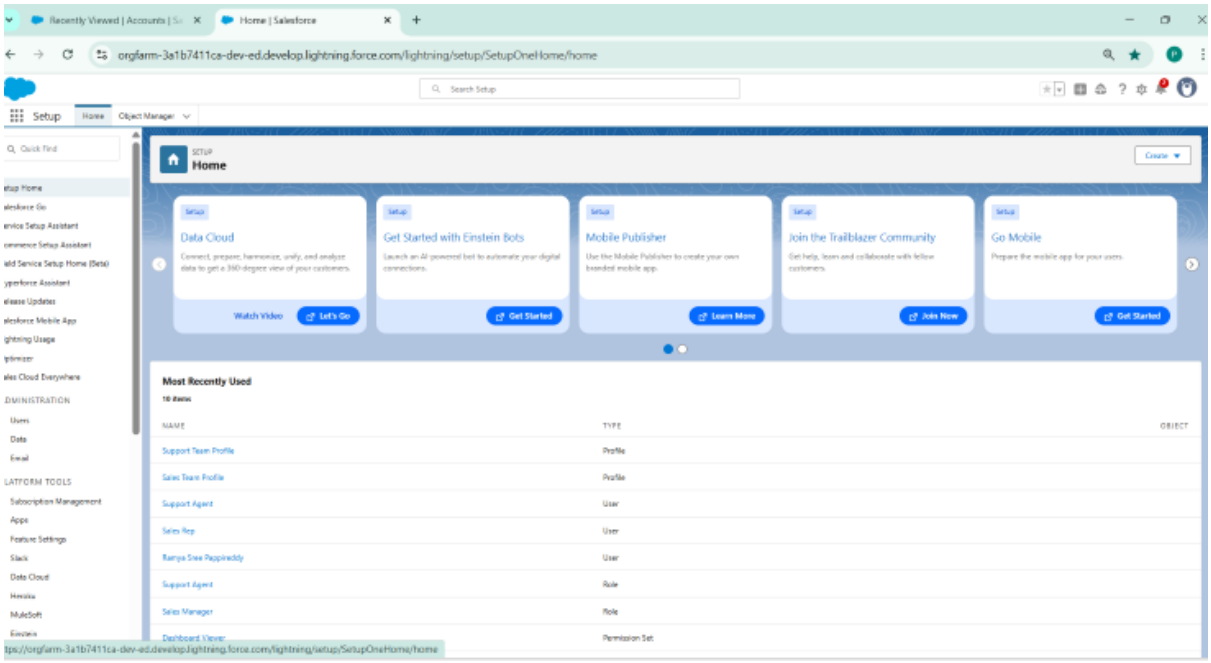
Integrated Customer Sales and Support System

Phase 2: Org Setup & Configuration

This phase establishes the foundational administrative and security settings of your Salesforce org. It's the critical step that ensures the system is properly configured to meet your business's unique requirements before you begin building the data model.

❖ Salesforce Editions

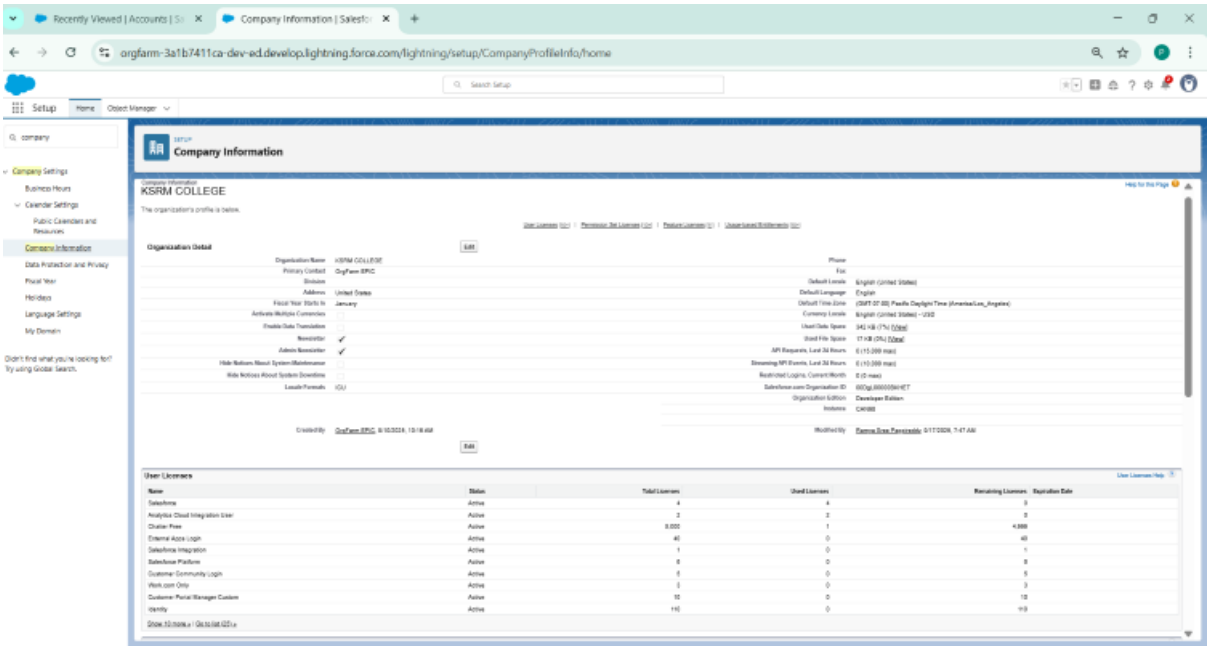
For this project, a Developer Edition Org was used. This free edition is ideal for development and learning because it includes a broad range of features, such as custom objects, flows, and the ability to write Apex code and create custom Lightning components. A key consideration for a Developer Edition is the absence of a separate sandbox environment, meaning all development and testing are performed directly within this single org.



❖ Company Profile Setup

The company's basic information was configured to ensure that all data and reporting reflect the correct business context. This was done by navigating to **Setup > Company Information**. The following details were updated:

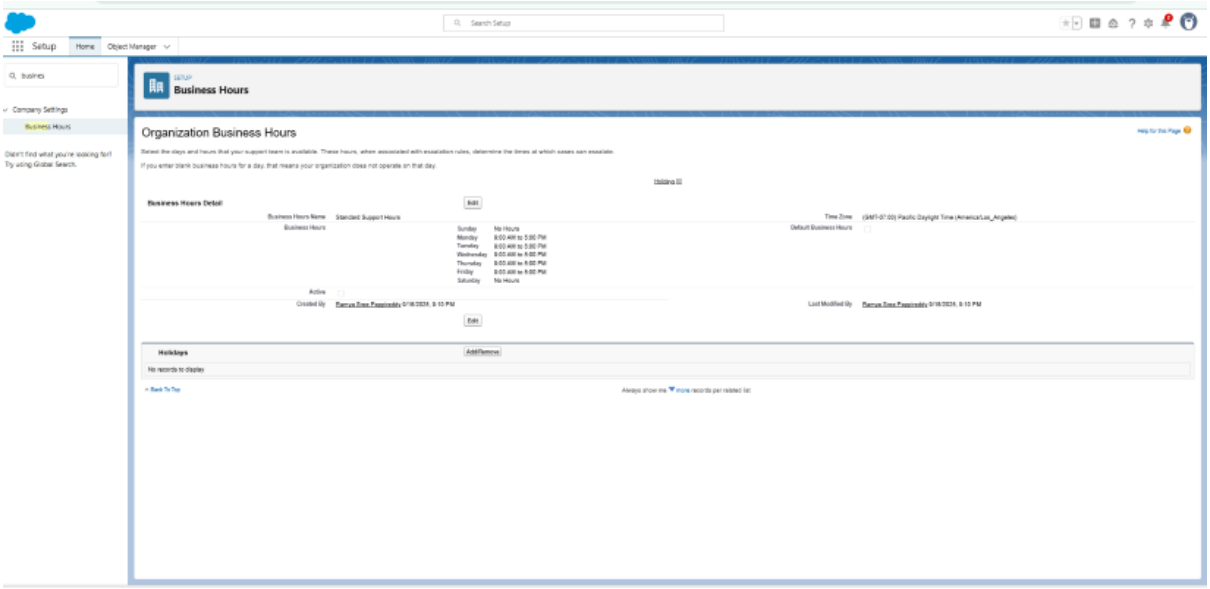
- **Timezone:** Set to the company's local timezone to ensure accurate timestamps on all records and activities.
- **Locale:** Configured to reflect the correct regional settings for date formats, currency, and other locale-specific data.



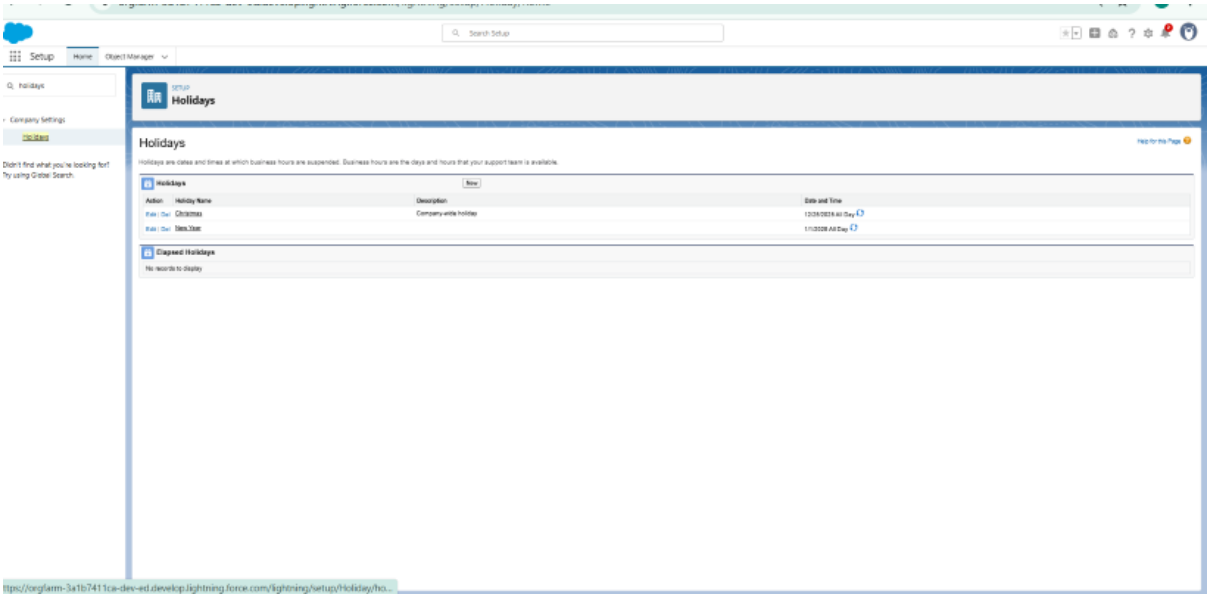
❖ Business Hours & Holidays

To accurately measure and automate time-based processes, such as case escalation rules, **Business Hours** and **Holidays** were defined. This ensures that response time metrics are only calculated during working hours and do not penalize agents for delays during non-working days.

- **Business Hours:** A set of standard working hours was defined for the support team, for example, Monday to Friday from 9 AM to 5 PM.

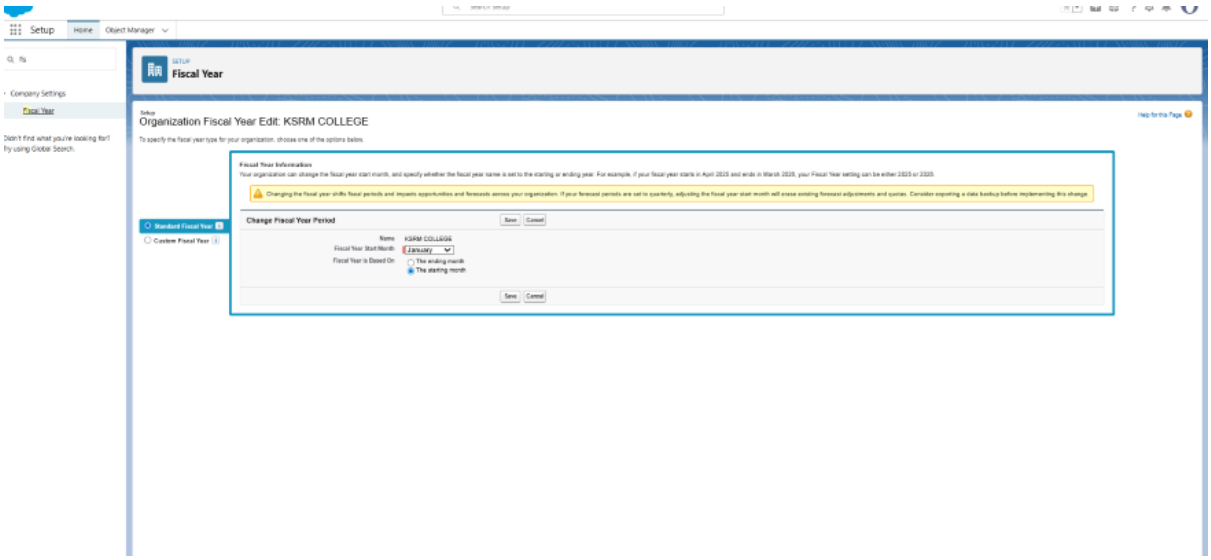


- **Holidays:** Key company holidays were added to the system, so they are automatically excluded from any time-based calculations.



❖ Fiscal Year Settings

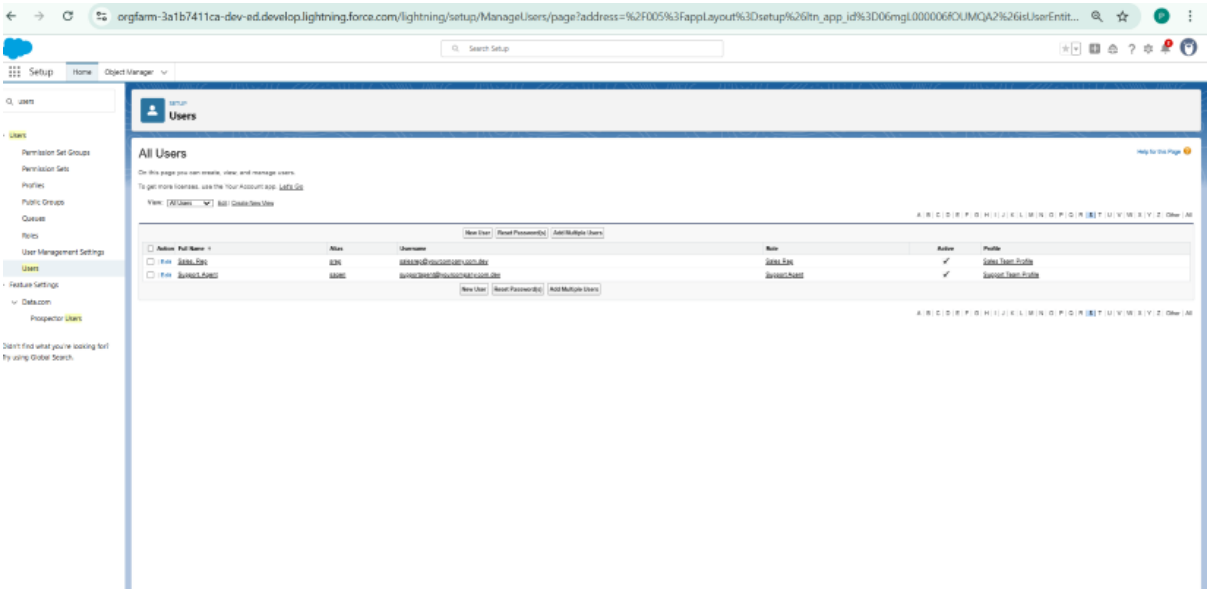
The fiscal year was configured to align with the company's financial calendar. For this project, a standard calendar year starting in January was used. This is a crucial step for sales forecasting and financial reporting, as it ensures that all reports and dashboards are grouped by the correct periods.



❖ User Setup & Licenses

Two test users were created to represent the primary stakeholders in the project. These users are essential for testing the security model from the perspective of each team.

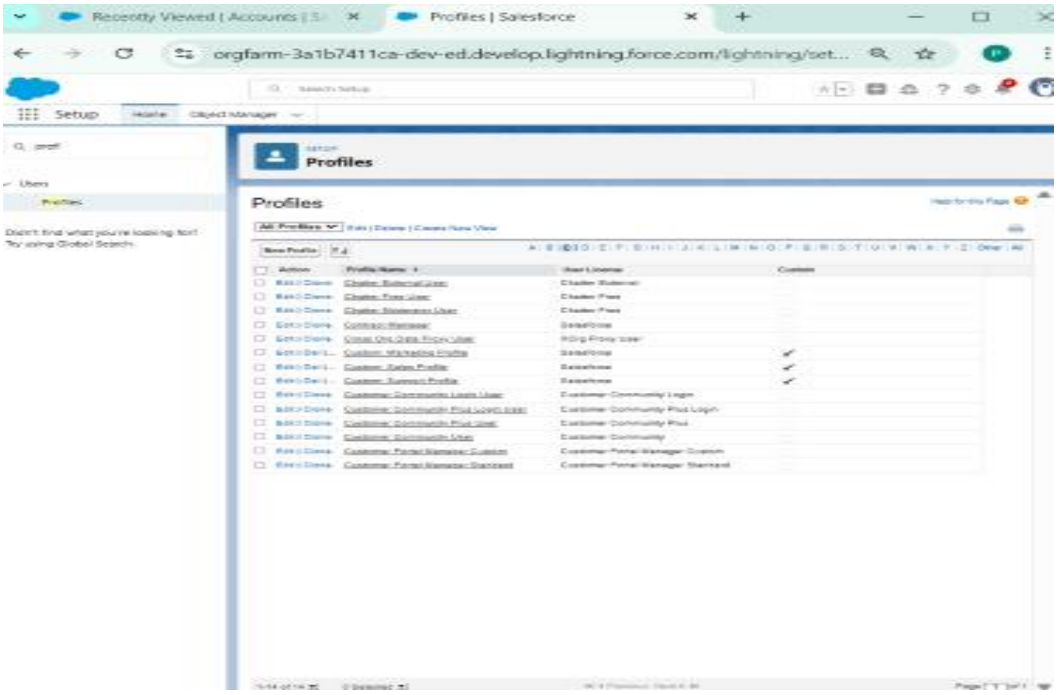
- **Sales Rep:** A user account was created to represent the sales team.
- **Support Agent:** A user account was created to represent the support team.
- Both users were assigned the **Standard Salesforce User** license, which grants them a comprehensive set of permissions necessary to work with both Sales Cloud and Service Cloud objects.



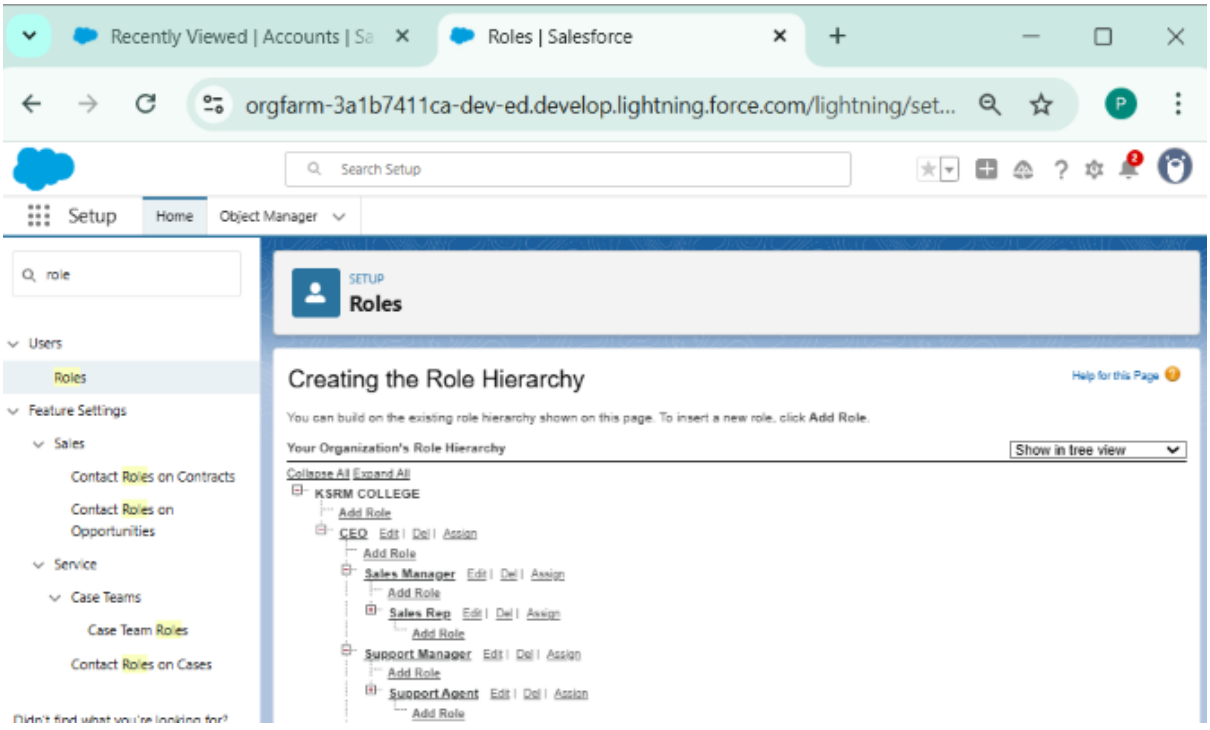
❖ Profiles, Roles, & Permission Sets

This is the core of the security model, designed to control data access and user permissions.

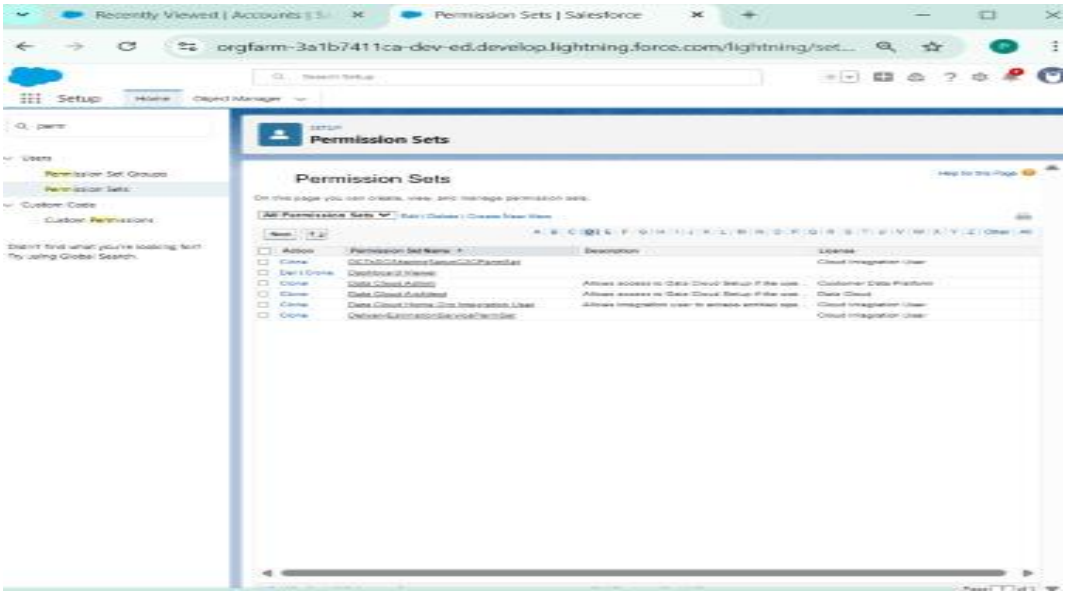
- **Profiles:** Two custom profiles were created by cloning the standard "Standard User" profile.
    - **Sales Team Profile:** Configured to grant read/write access to **Leads** and **Opportunities** while restricting access to other objects.
    - **Support Team Profile:** Configured to grant read/write access to **Cases** while restricting access to other objects.



- **Roles:** A role hierarchy was established to mirror the company's organizational structure. The hierarchy was structured as follows: **CEO → Sales Manager and Support Manager → Sales Rep and Support Agent**.



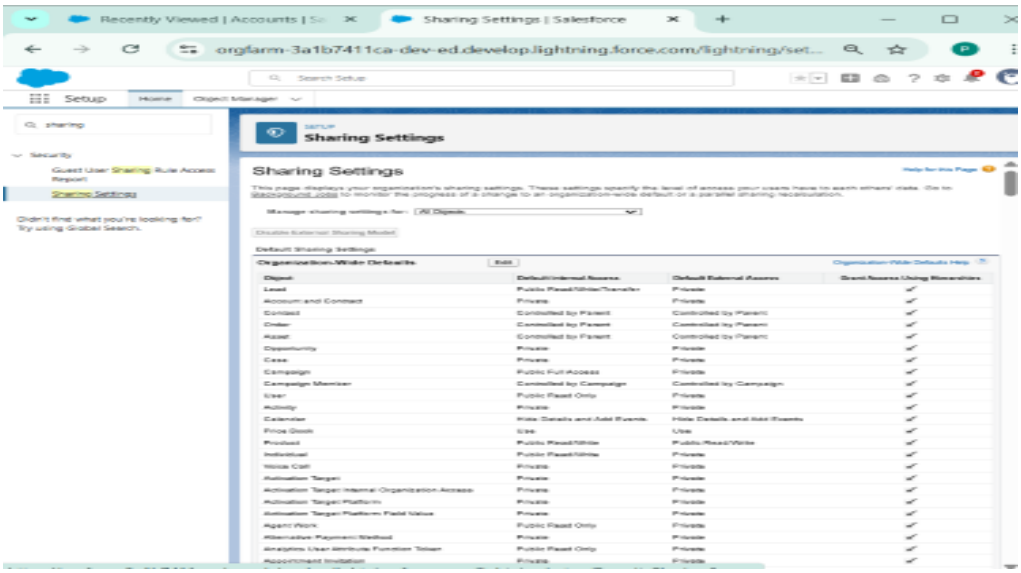
- **Permission Sets:** A Dashboard Viewer permission set was created to grant specific, additional permissions without modifying the user's base profile.



❖ OWD & Sharing Rules

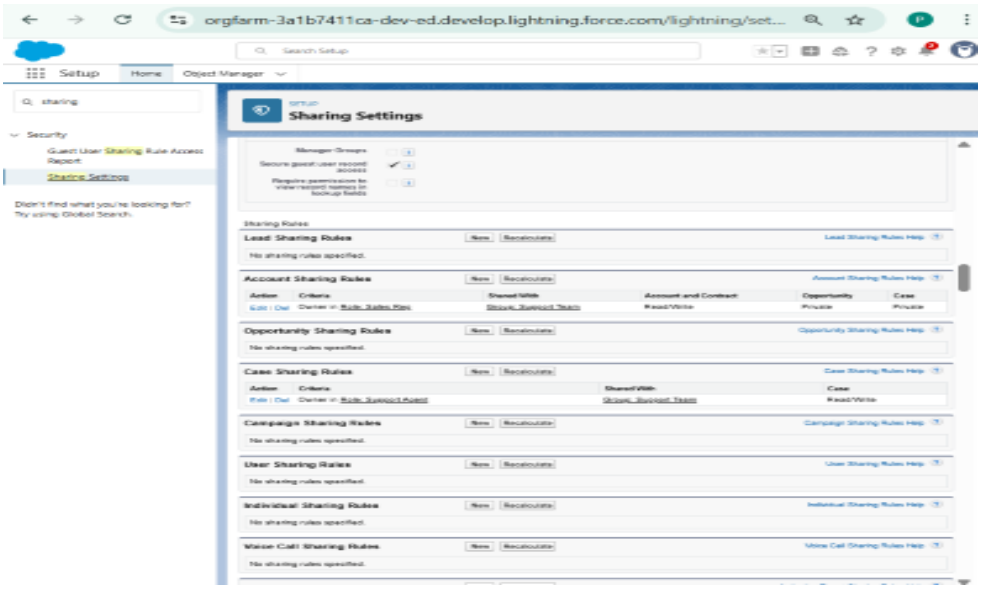
These are the primary components that determine data visibility in the org.

- **Organization-Wide Defaults (OWD):** The default access for all key objects (**Account**, **Opportunity**, and **Case**) was set to **Private**.



- **Sharing Rules:** To address the core problem of departmental silos, sharing rules were created to selectively "open up" access.
    - A rule was created to share all **Cases** with a "Support Team" public group.

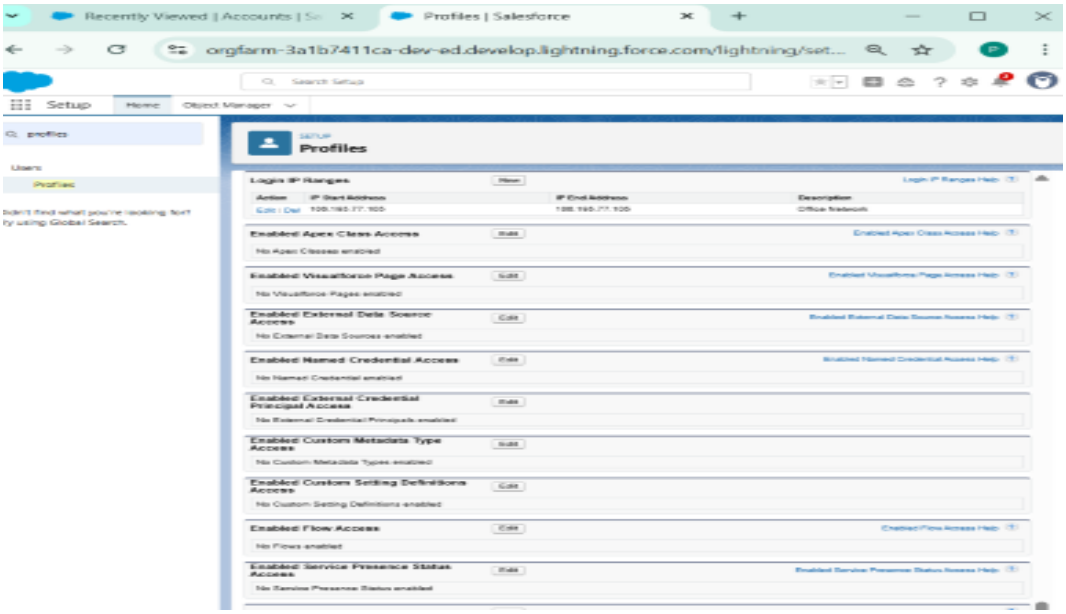
- A similar rule was implemented to share all **Accounts** and **Contacts** with the "Support Team," providing them with full customer context.



❖ Login Access Policies

To add an extra layer of security, login policies were configured. This prevents unauthorized access to the system.

- **Session Settings:** The default session security settings were reviewed to ensure they meet the project's requirements, such as enforcing HTTPS connections and preventing cross-site scripting attacks.
- **Login IP Ranges:** Login IP Ranges were configured on the custom profiles to restrict user logins to a specific, trusted IP range.



❖ Sandbox Usage & Deployment Basics

- **Sandbox Usage:** Since a separate sandbox is not available in the Developer Edition, all development for this project was conducted directly in the main org. The concept of a sandbox was understood as a critical tool for isolating development, testing, and production environments in a real-world scenario.
- **Deployment Basics:** The concept of deployment was noted, but no deployment was performed in this phase. The project is still in the development phase, and deployment will be handled in a later stage.