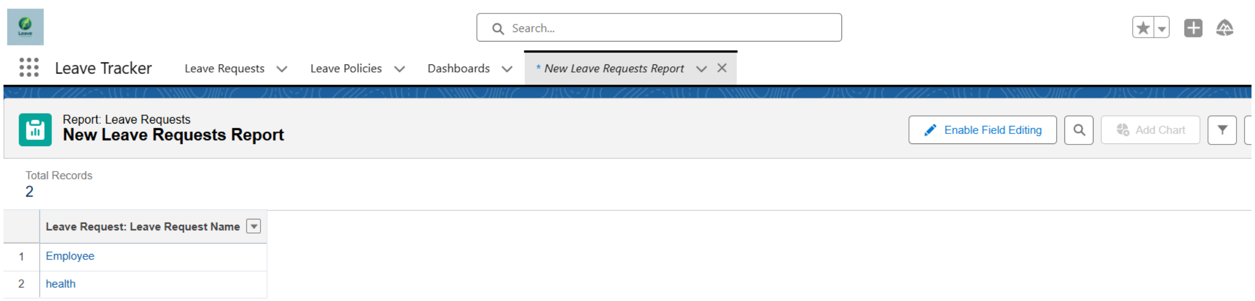
Project: Leave Tracker

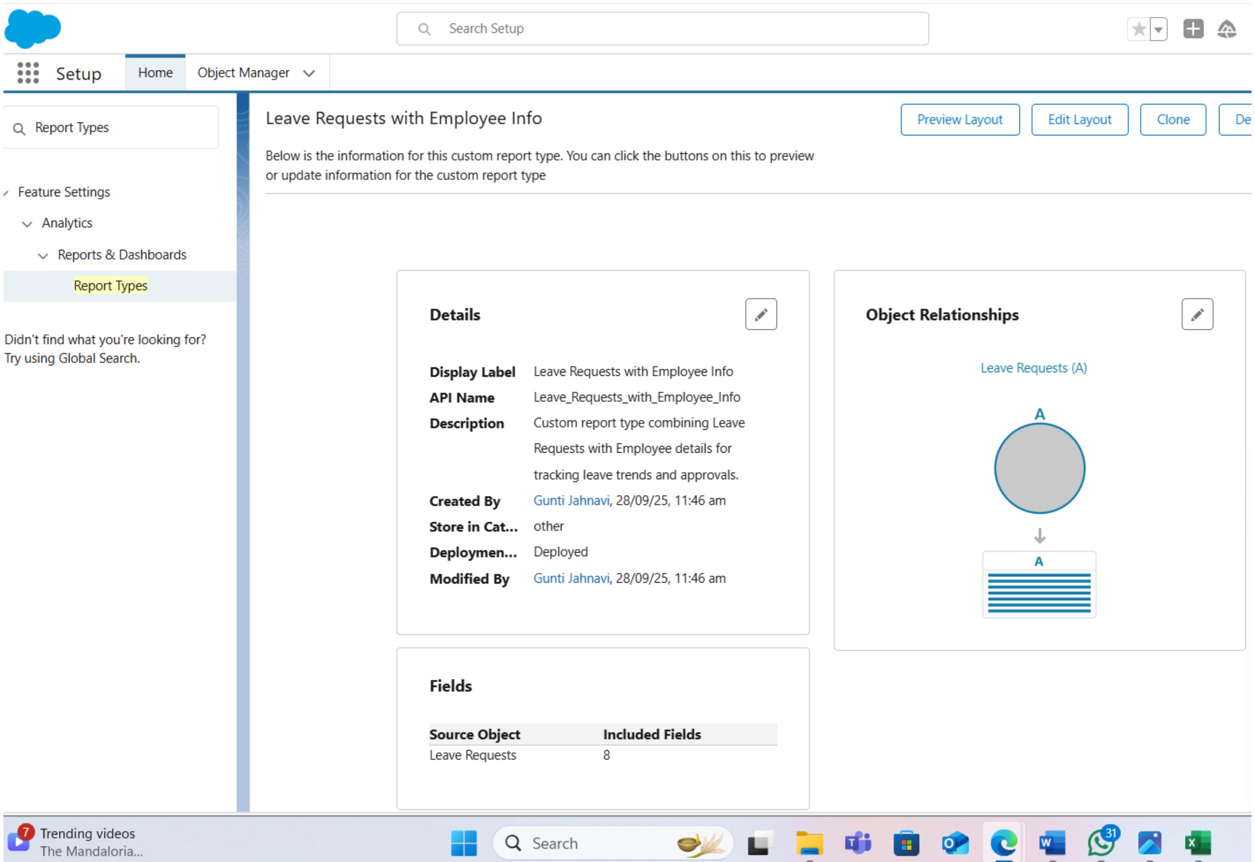
Phase 9: Reporting, Dashboards & Security Review

This phase focuses on analyzing data, visualizing key metrics, and ensuring security within the Salesforce Leave Tracker application.

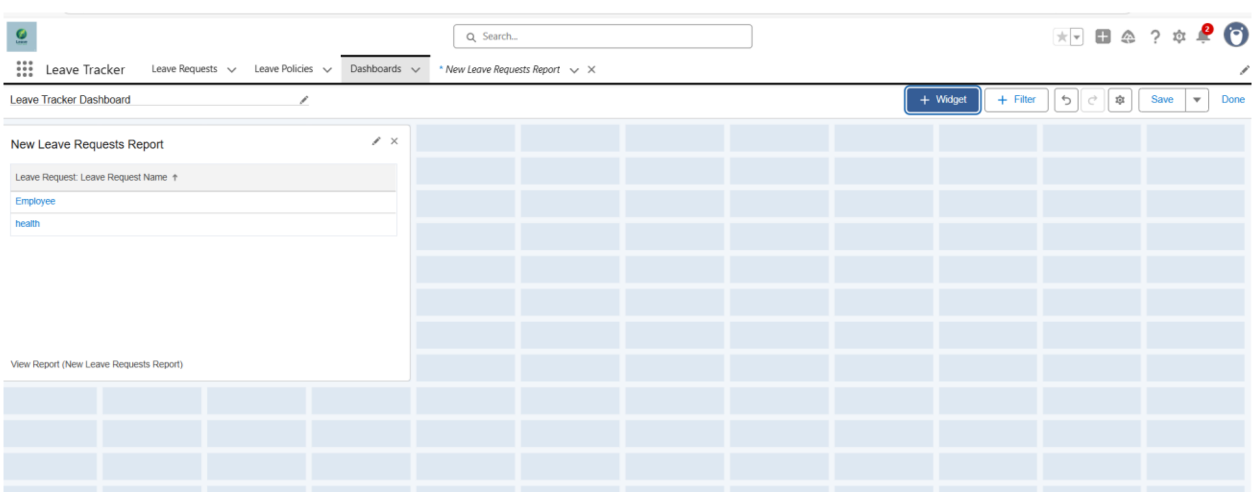
1. **Reports (Tabular, Summary, Matrix, Joined)**
    - **Purpose:** To analyze leave requests, employee data, and trends.
    - **Details:** Use different report types to get multiple views of your data:
        - Tabular: Simple lists of records.
        - Summary: Grouped data for better insights.
        - Matrix: Cross-tab analysis.
        - Joined: Combine multiple reports.



2. **Report Types**
    - **Purpose:** To define which objects and fields are available in a report.
    - **Details:** Create custom report types to analyze specific combinations of data, e.g., Employees and Leave Requests together.

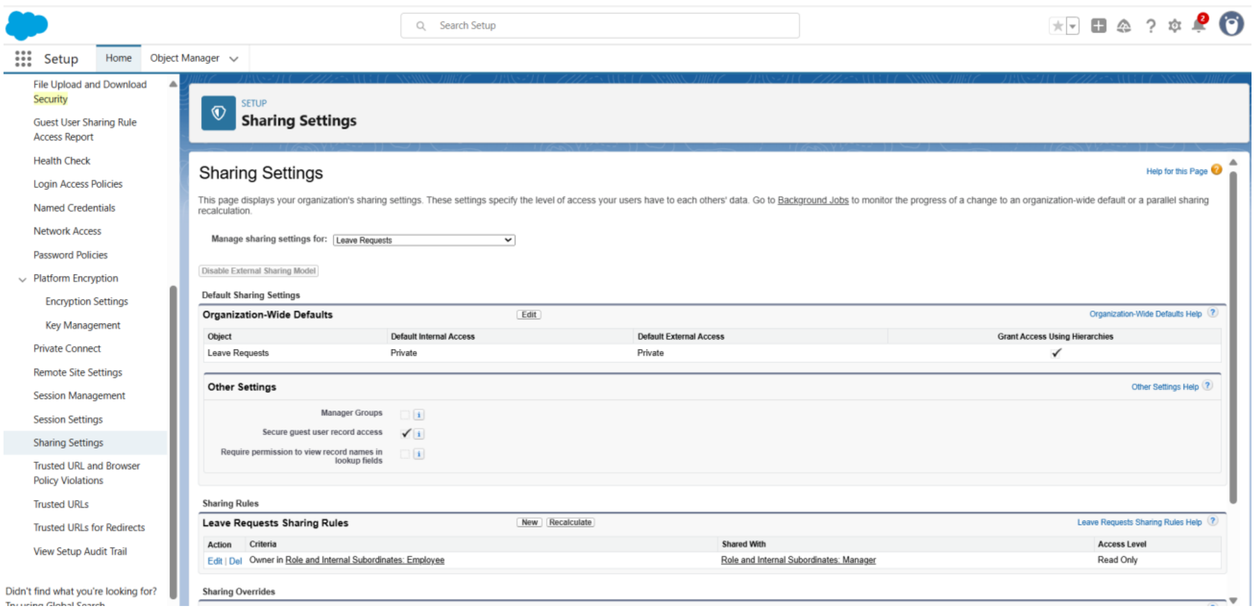
- 

3. **Dashboards**
    - **Purpose:** To visually represent report data for easier tracking.
    - **Details:** Show leave statistics, trends, and key metrics for managers or HR.

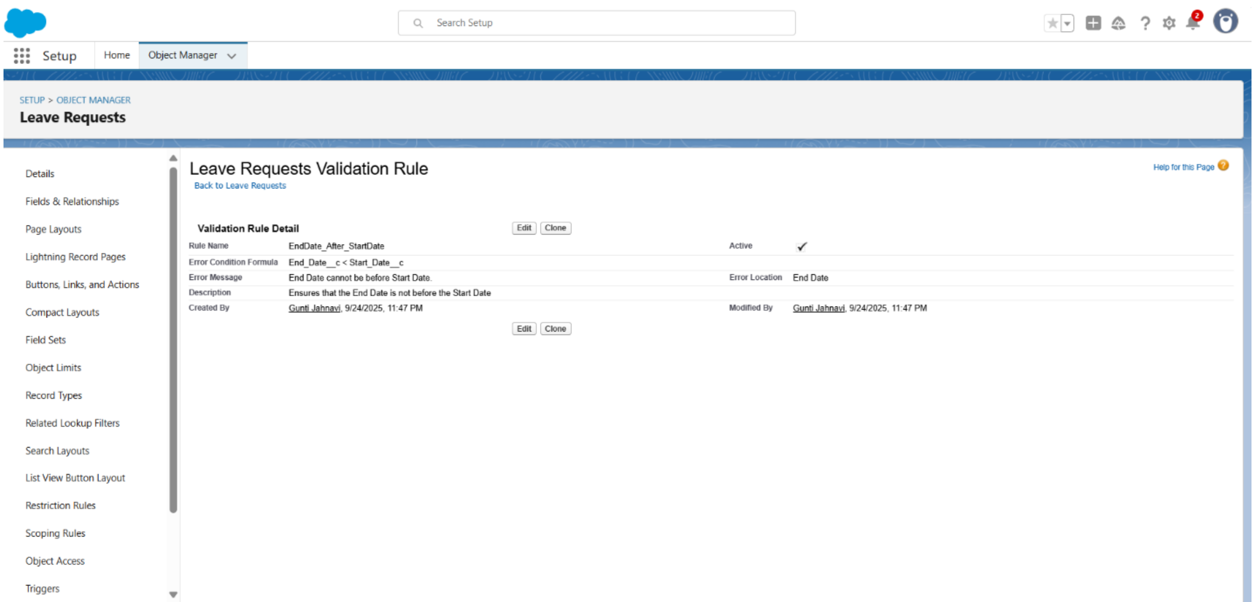


4. **Dynamic Dashboards (Optional but Recommended)**

    - **Purpose:** Allow users to see data according to their access level.
    - **Details:** Enables personalized dashboard views without creating multiple dashboards for each user.
5. **Sharing Settings**
    - **Purpose:** To control who can view or edit records.
    - **Details:** Ensure only authorized users can access or modify leave requests or employee data.



6. **Field Level Security**
    - **Purpose:** To restrict access to sensitive fields.
    - **Details:** Hide private information (e.g., salary, comments) from users who do not need access.



Login IP Ranges

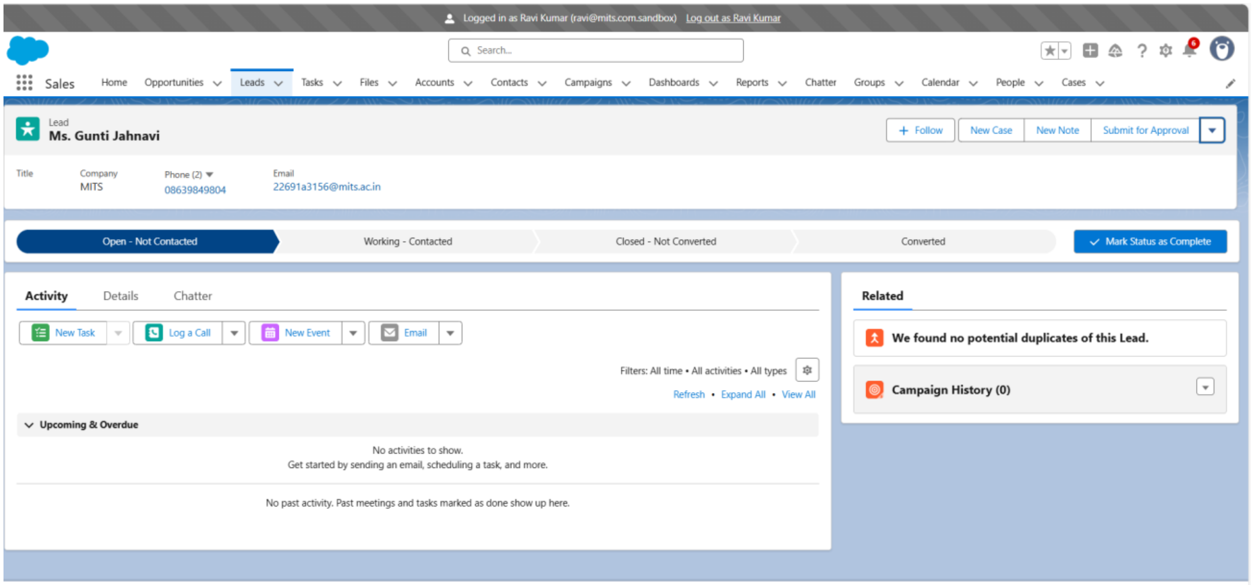
Purpose: Restrict users to log in only from trusted IP addresses.

Step 1: Go to Profiles

1. Go to **Setup → Users → Profiles**.
2. Select the **Profile** you want to restrict (e.g., HR Manager, Employee).

Step 2: Set Login IP Ranges

1. Scroll down to **Login IP Ranges**.
2. Click **New**.
3. Enter **Start IP Address** and **End IP Address**.
    - Example: Start = 192.168.1.1, End = 192.168.1.255
4. Click **Save**.

5. 

✅ **Tip:** Users outside these IPs will be blocked from logging in.

---

3. Audit Trail

Purpose: Track changes made to setup and configurations.

Step 1: Go to Setup Audit Trail

1. Go to **Setup → Security → View Setup Audit Trail**.

Step 2: Review Changes

1. You can see:
   - Who made changes
   - When the changes were made
   - What was changed (e.g., object, field, profile settings