Phase 9 — Reporting, Dashboards & Security Review

1. Reporting Setup

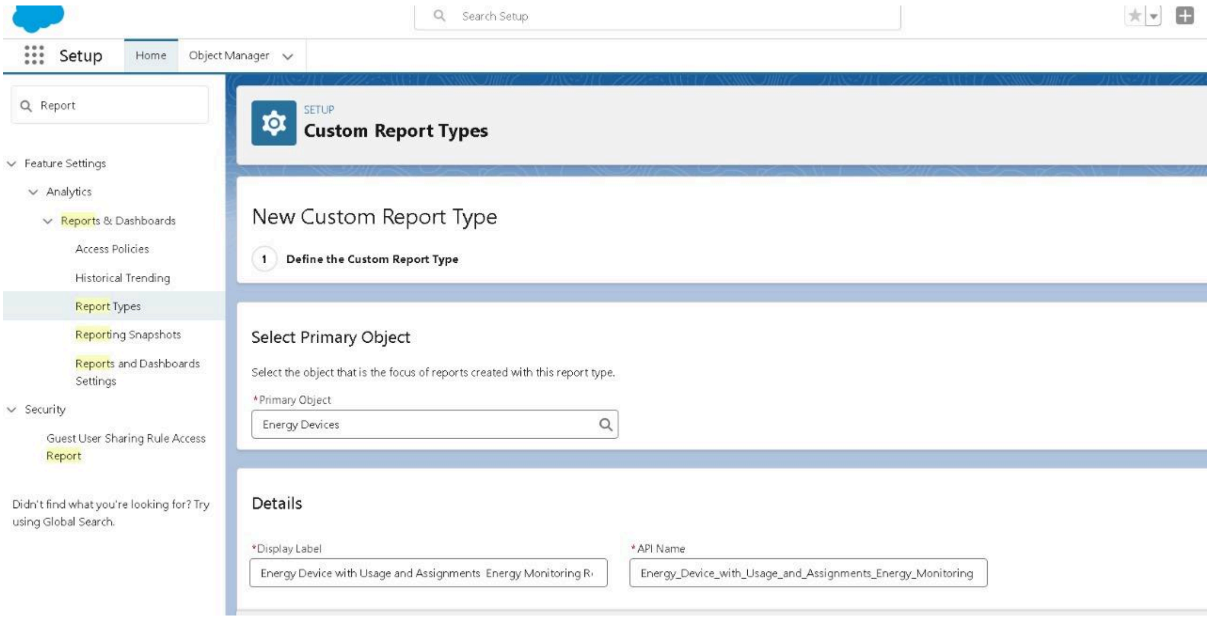
Objective: Deliver actionable insights into energy consumption and personnel activity using Salesforce's reporting capabilities.

Steps:

1. **Identify key reporting needs**
    - Energy usage trends by device.
    - Personnel activity (e.g., number of assignments completed).
    - Device assignment history and utilization.
    - Exception reports for high or abnormal usage.
2. **Create Custom Report Types**
    - Combine objects such as **Energy Device**, **Energy Usage Record**, **Personnel**, and **Device Assignment**.
    - Ensure all required relationships are available for reporting.
3. **Build reports in multiple formats:**
    - **Tabular Reports** — simple lists, e.g., recent energy usage entries.
    - **Summary Reports** — grouped totals, e.g., usage grouped by device.
    - **Matrix Reports** — cross-tab views, e.g., energy usage by device and time period.

- ◦ **Joined Reports** — related datasets, e.g., device information alongside assignment history.

4. **Validate reports** by sharing with stakeholders and refining filters, groupings, and field selections.



2. Dashboard Creation

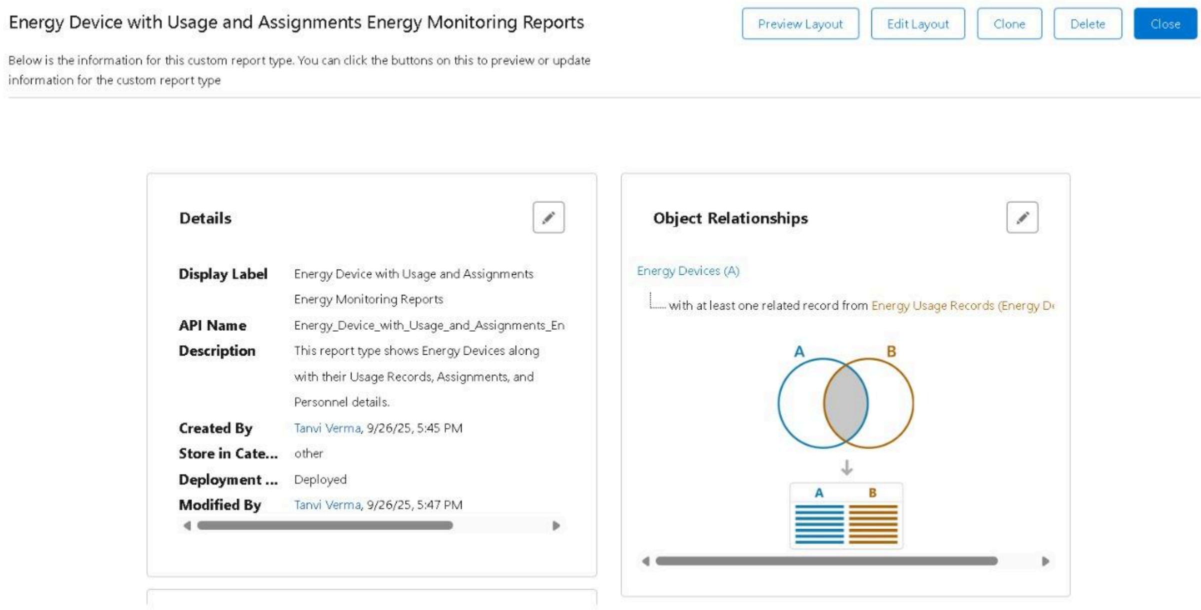
Objective: Provide executives, managers, and technicians with **real-time visual insights** into system performance.

Steps:

1. **Design dashboards** aligned with critical KPIs, such as:
   - ◦ Total energy consumed in the current month.
   - ◦ Devices with highest/lowest usage.
   - ◦ Technician assignment completion rates.
   - ◦ Active vs. inactive devices.
2. **Add dashboard components**

- Charts (bar, line, donut, funnel) to visualize usage and performance.
- Metric summaries for single-number KPIs.
- Report tables for detailed drill-downs.
- Report links for direct access to underlying reports.

3. **Enable Dynamic Dashboards**
   - Configure dashboards to run "as logged-in user" to ensure each role (Manager, Technician, Agent, Customer) sees data according to their permissions.



3. Security Review

Objective: Ensure the system protects sensitive energy and personnel data, while enabling appropriate access.

Steps:

1. **Audit Sharing Settings**
   - Define org-wide defaults for each custom object.
   - Create sharing rules for role-based access (e.g., Managers see all devices, Technicians see assigned devices).
2. **Review Field-Level Security (FLS)**
   - Ensure sensitive fields (e.g., internal notes, cost values) are visible only to authorized roles.
   - Remove edit access from fields that should remain read-only.
3. **Configure Session Security**
   - Enforce session timeouts after inactivity.
   - Require secure connections (HTTPS) for all logins.
   - Enable two-factor authentication for admin and high-privilege users.
4. **Set Login IP Ranges**
   - Restrict access to trusted office or institutional networks.
   - Configure per-profile or per-user as needed.
5. **Enable Audit Trail & Monitoring**
   - Track administrative configuration changes.
   - Monitor user activity logs to detect anomalies or unauthorized access attempts.