**Lead Management & Task Tracking System Phase 9: Reporting, Dashboards & Security Review**

## 1. Introduction

This phase focuses on creating reports, dashboards, and implementing security measures in Salesforce to monitor and protect the Lead Management & Task Tracking System. Proper reporting helps managers track performance, while security settings ensure data privacy and compliance.

Objectives:

* Generate insightful reports on leads and tasks.
* Create dashboards for real-time monitoring.
* Implement security best practices to protect data.

## 2. Reports

Salesforce provides multiple report formats: Tabular, Summary, Matrix, and Joined.

Setup Steps:

1. Go to App Launcher → Reports → New Report.
2. Choose object (Lead or Task).
3. Select report type:
   * Tabular: Simple list of records.
   * Summary: Group records by a field (e.g., Status).
   * Matrix: Group by row and column (e.g., Lead Source by Assigned Rep).
   * Joined: Combine multiple report blocks.
4. Apply filters and save the report.

Example Reports:

* Leads by Status (Summary report)
* Tasks due this week (Tabular report)
* Leads by Lead Source and Assigned Rep (Matrix report)

Deliverable: Reports for tracking leads, tasks, and team performance.

## 3. Report Types

Custom Report Types allow combining objects not supported in standard reports.

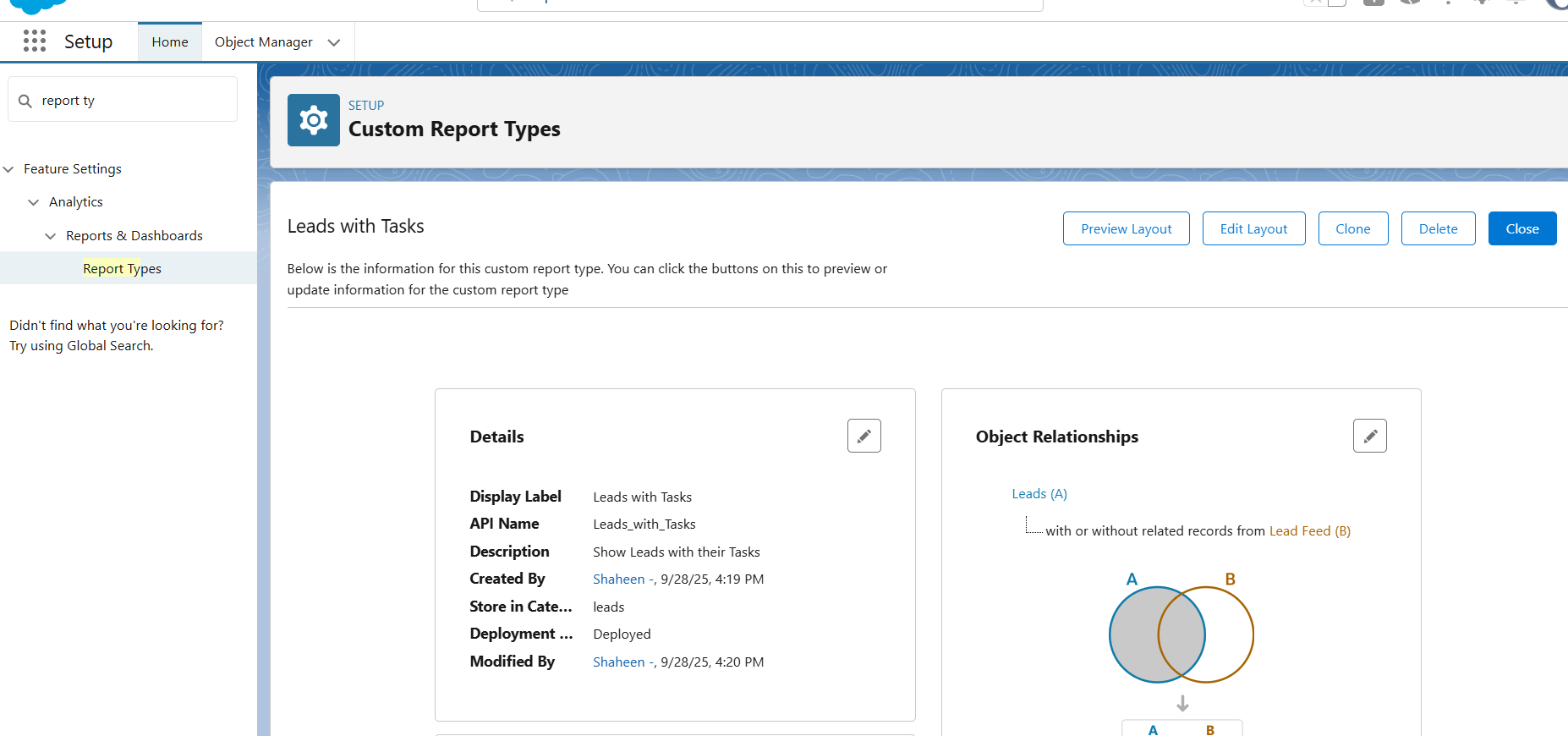
Setup Steps:

1. Go to Setup → Report Types → New Custom Report Type.
2. Primary Object: Lead
3. Related Object: Task
4. Save and deploy for reporting.

Example:

* Custom report type: Lead with Tasks, showing all open tasks per lead.

Deliverable: Custom report types configured for advanced reporting.



## 4. Dashboards

Dashboards provide a visual representation of reports using charts, tables, and metrics.

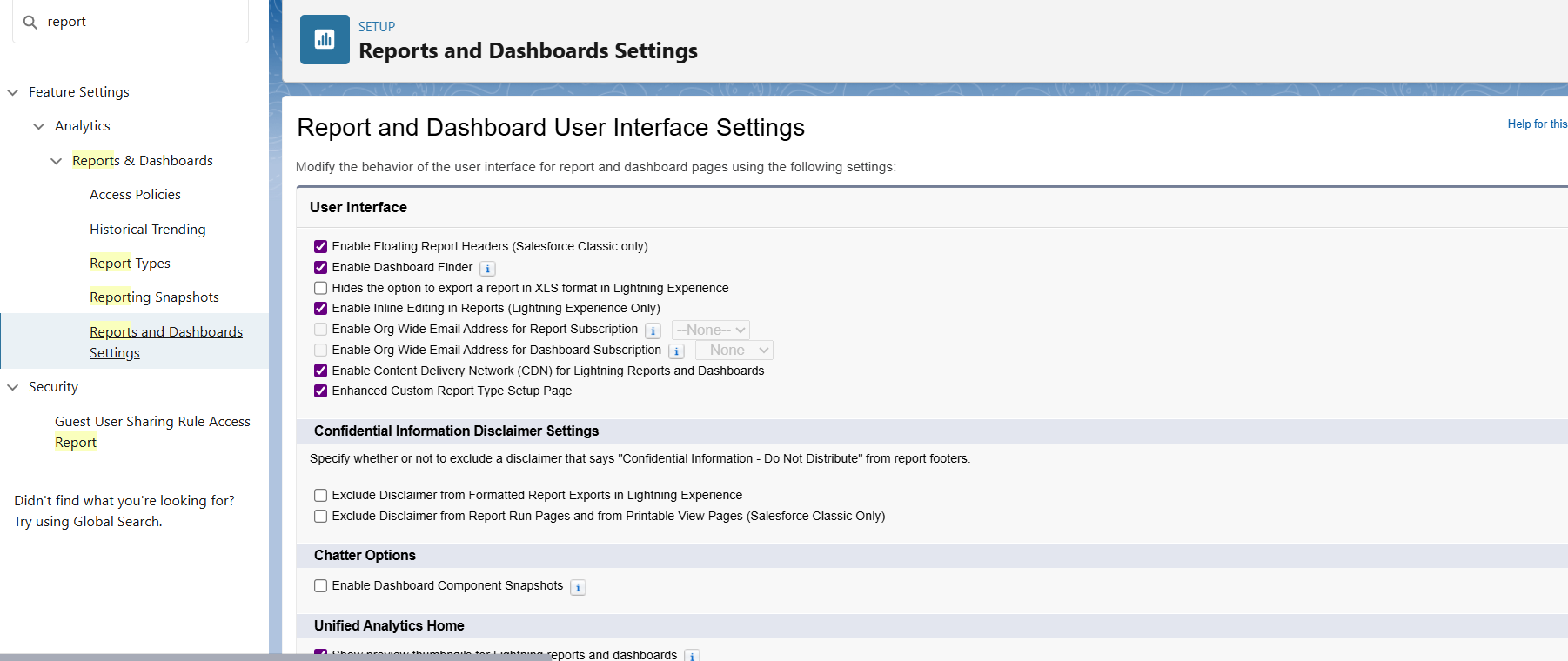
Setup Steps:

1. Go to App Launcher → Dashboards → New Dashboard.
2. Add components: charts, tables, metrics linked to reports.
3. Organize dashboard layout for reps and managers.

Example Dashboard Components:

* Leads by Status (Pie Chart)
* Tasks Due (Bar Chart)
* High-Priority Leads (Table)

Deliverable: Dashboard displaying lead and task performance metrics.



## 5. Dynamic Dashboards

* Dynamic dashboards allow users to see data based on their role or profile.

Setup Steps:

1. Create or edit a dashboard.
2. Select View Dashboard as: Logged-in User.
3. Assign visibility based on profiles or roles.

Benefits:

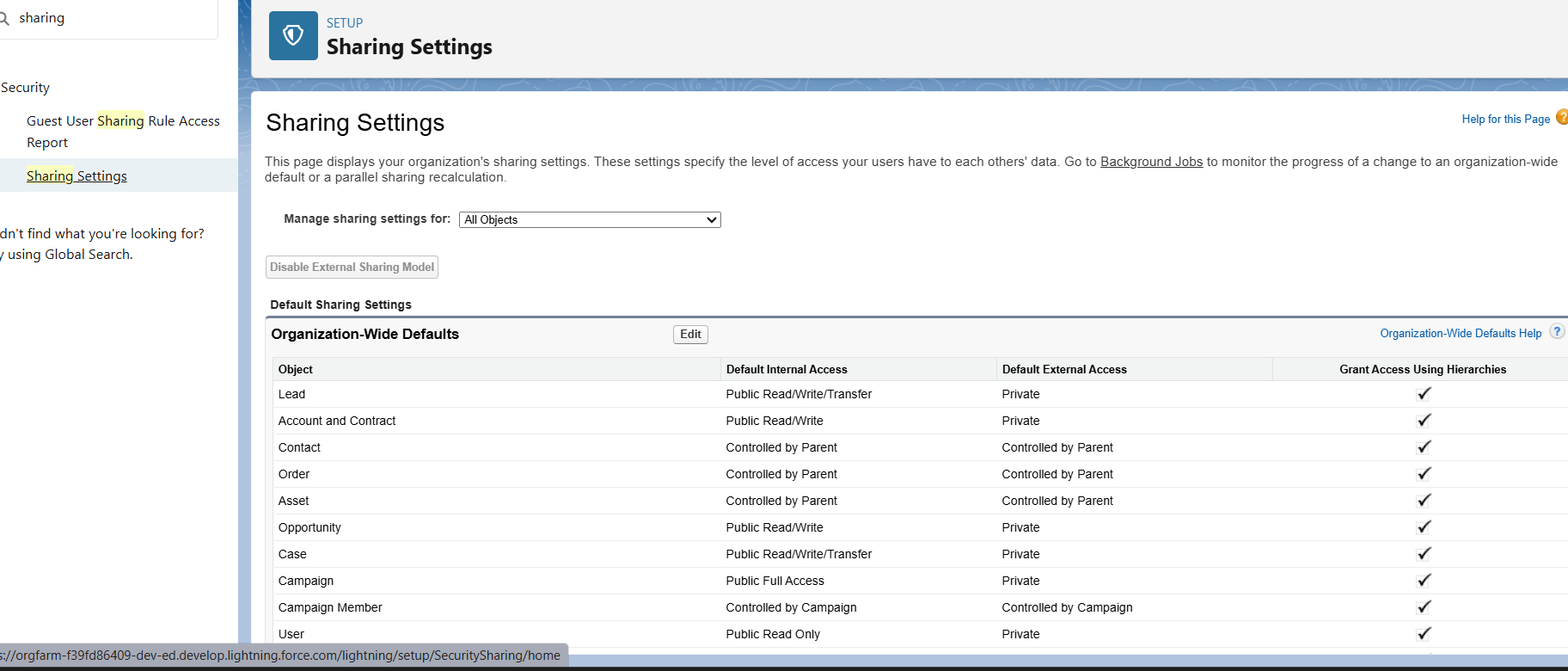
* Managers see team-wide data.
* Sales reps see only their leads and tasks.

Deliverable: Dynamic dashboards configured for roles and profiles.

## 6. Sharing Settings

Control who can view or edit records. Setup Steps:

1. Go to Setup → Sharing Settings.
2. Set Organization-Wide Defaults (OWD):
   * Lead: Private
   * Task: Controlled by Parent
3. Configure Sharing Rules for exceptions (e.g., share leads with regional managers).



## 7. Field Level Security (FLS)

Control visibility and edit permissions at the field level.

Setup Steps:

1. Go to Setup → Object Manager → Lead → Fields & Relationships → Set Field-Level Security.
2. Select profiles allowed to view/edit sensitive fields (e.g., Lead Email, Phone).

Deliverable: Field-level security enforced for sensitive lead and task fields.

## 8. Session Settings

Control user session behavior for security compliance.

Setup Steps:

1. Go to Setup → Security → Session Settings.
2. Configure settings such as:
   * Session timeout (e.g., 30 minutes)
   * Force logout after timeout
   * Enable secure session settings

Deliverable: Session settings configured to prevent unauthorized access.

## 9. Login IP Ranges

Restrict login access to trusted IP addresses.

Setup Steps:

1. Go to Setup → Profiles → Login IP Ranges.
2. Add trusted IP ranges for office networks or VPN.

Deliverable: IP restrictions applied for secure access.

## 10. Audit Trail

Track changes to configuration and user activity for compliance.

Setup Steps:

1. Go to Setup → Security → View Setup Audit Trail.
2. Review changes for the last 6 months.
3. Export for documentation or compliance reporting.

Deliverable: Audit trail enabled and monitored for configuration changes.

