

# SmartFleet – Phase 2: Org Setup & Configuration

## Introduction

In this phase, the Salesforce Org was configured to support the SmartFleet solution. The setup ensures that fleet managers, engineers, and vendors have the correct level of access, while maintaining strong security for IoT-driven vehicle data. Proper profiles, roles, and sharing settings were implemented to streamline fleet monitoring and service ticket management.

---

## Objectives

- Configure Company Information, Business Hours, and Holidays for logistics operations.
  - Create Users, Roles, and Profiles to represent Fleet Managers, Engineers, and Vendors.
  - Set up Organization-Wide Defaults (OWD) and Sharing Rules to control data visibility.
  - Provide Permission Sets for IoT integration and service operations.
  - Configure Login & Session Policies for security.
  - Set up Developer Org and Sandbox to prepare for development and testing.
- 

## Configuration Steps

### Step 1: Company Profile Setup

- **Company:** *SmartFleet Logistics Solutions*.
- **Business Hours:** 8 AM – 8 PM (Mon–Sun).
- **Holidays:** Logistics downtime and public holidays.
- **Fiscal Year:** Standard (January–December).

### Step 2: User Setup & Licenses

- **Users created:**
  - Fleet Manager (full access to reports and dashboards).
  - Service Engineers (ticket handling for vehicles).
  - Vendor/Supplier (limited spare part object access).
  - System Admin (manages configurations and deployment).
- **Licenses:** Salesforce Platform licenses for operational staff, Salesforce CRM licenses for managers.

### Step 3: Roles & Profiles

- **Roles:**
  - Director → Fleet Manager → Service Engineers.
- **Profiles:**
  - Fleet Manager Profile → Full access to Vehicle, Tickets, Reports.
  - Engineer Profile → Limited to assigned service tickets.
  - Vendor Profile → Read-only on spare parts, can update stock requests.

### Step 4: Permission Sets

- **IoT Integration Permission:** API Enabled, Modify All on Vehicle Sensor Data.
- **Spare Part Controller Permission:** Manage inventory and approve restocking.

### Step 5: OWD & Sharing Rules

- **OWD Settings:**
  - **Vehicles:** Private.
  - **Sensor Data:** Private.
  - **Service Tickets:** Private.
  - **Spare Parts:** Read-only.
- **Sharing Rules:**
  - **Fleet Managers:** Full access to all Service Tickets.
  - **Engineers:** Access restricted to tickets assigned to them.

### Step 6: Security Settings

- IP Whitelisting applied for trusted office/logistics network.
- Two-Factor Authentication enabled for admins and managers.
- Session timeout configured at 1 hour due to mobile/field access.

### Step 7: Dev Org & Sandbox Setup

- Developer Org connected with VS Code using Salesforce CLI (SFDX).
- Developer Sandbox created for LWC and Apex testing.
- GitHub repo established: SmartFleet-Salesforce.

### Step 8: Deployment Basics

- Source tracking enabled with SFDX Push/Pull.
  - Test deployment carried out with sample Vehicle and Ticket objects.
  - Deployment documented for migration to higher environments.
-

## **Results / Observations**

- Users successfully onboarded with correct access levels.
  - OWD and Sharing rules ensured privacy for sensitive fleet data.
  - Permission sets provided flexible access control for IoT and spare part management.
  - GitHub integration established for collaborative development.
- 

## **Next Steps**

- Move to Phase 3: Data Modeling & Relationships.
- Create objects such as Vehicle, Sensor Data, Service Ticket, Spare Part.
- Define relationships between Vehicle and Service Tickets to support automation.