Phase 2: Org Setup & Configuration

Wholesaler Order Management CRM (Salesforce Project)

Author: Your Name | Date: 2025-09-18

# Objective

Set up the Salesforce Org environment with correct company settings, security model, user access, and deployment basics. This document contains step-by-step instructions and example data to configure Phase 2 of the project.

# 1. Salesforce Edition

Steps:

1. Decide on an edition. Recommended: Enterprise Edition for production.
2. Create a Developer Edition org for POC: https://developer.salesforce.com/signup
3. Create a Production or sandbox org based on licensing procurement.

Example:

* - Selected: Enterprise Edition

- Dev Org: yourcompany-dev@example.com (Developer Edition)

[Insert screenshot: screenshots/org-edition.png]

# 2. Company Profile Setup

Steps:

1. Setup → Company Information → Fill in Company Name, Address, Default Locale, Language, Default Currency.
2. Setup → Business Hours → New Business Hours: e.g., "Office Hours" Mon–Sat 09:00–18:00. Save.
3. Setup → Holidays → New Holiday: Add observed public holidays and company holidays.
4. Setup → Fiscal Year → Select Standard Fiscal Year or configure Custom Fiscal Year if required.

Example values to fill:

* - Company Name: Acme Wholesale Pvt Ltd
* - Default Locale: English (India)
* - Default Currency: INR
* - Business Hours Name: Office Hours (Mon–Sat 09:00–18:00)

[Insert screenshot: screenshots/company-profile.png]

# 3. User Setup & Licenses

Steps to create users:

1. Setup → Users → Users → New User (or clone existing user).
2. Fill required fields: First Name, Last Name, Alias, Email, Username (must be unique), Nickname, Role, Profile, User License, Locale, Time Zone.
3. When creating community users (Retailers), create the Contact inside the Retailer Account first and then click "Enable Customer User" (or Partner User) to create a Community user.
4. Assign appropriate License: Salesforce, Platform, or Customer/Partner Community licenses.
5. Assign Permission Sets after user creation if additional permissions are required.

Sample users (fill with your org data):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| User Name | Email | Role | Profile | License |
| wholesaler.ops | wholesaler.ops@acme.com | Operations Manager | Wholesaler Profile | Salesforce |
| retailer.john | john.retailer@store.com | Retailer Role | Retailer Profile | Customer Community Plus |
| sales.alice | alice.sales@acme.com | Sales Rep | Sales Team Profile | Salesforce |
| inv.manager | inventory@acme.com | Inventory Team | Inventory Manager Profile | Salesforce |

[Insert screenshot: screenshots/user-setup.png]

# 4. Security Model Configuration

## 4.1 Profiles (Base Permissions)

Steps to create/clone profiles:

1. Setup → Profiles → Click "New Profile" (or clone an existing Standard Profile).
2. Name the profile (e.g., "Wholesaler Profile") and set the appropriate User License if needed.
3. Edit Object Settings: Configure Create, Read, Edit, Delete, View All, Modify All for each object.
4. Set Tab Settings: Default On, Hidden, or Default Off for tabs.
5. Assign system permissions where necessary (e.g., "API Enabled", "View Setup and Configuration" only for admins).

Recommended Profile Permissions (example):

* **Wholesaler Profile:** Orders: CRUD, Products: CRUD, Inventory: CRUD, System Permissions: Run Reports, Export Reports
* **Retailer Profile:** Orders: Create/Edit/Read (No Delete), Products: Read Only, Minimal system permissions
* **Sales Team Profile:** Orders: Create/Edit/Read, Products: Read, View Dashboards & Reports
* **Inventory Manager Profile:** Inventory: CRUD, Products: CRUD, Orders: Read Only

[Insert screenshot: screenshots/profiles.png]

## 4.2 Roles (Hierarchy for Data Visibility)

Steps to create roles:

1. Setup → Roles → Set Up Roles → Click "Add Role".
2. Create roles according to company structure and place them in a hierarchy that reflects reporting lines.
3. Ensure roles match data visibility requirements (higher role inherits visibility of lower roles).

Example Role Hierarchy:

* CEO
* ├── Sales Manager
* │ └── Sales Rep
* └── Operations Manager
* └── Inventory Team
* └── Retailer Role (external users)

[Insert screenshot: screenshots/roles.png]

## 4.3 Permission Sets (Extra Permissions)

Steps to create Permission Sets:

1. Setup → Permission Sets → New.
2. Label: (e.g., "View Reports Set"), API Name auto-generated, License: None (recommended). Save.
3. Click "System Permissions" → Edit → Enable required permissions (e.g., Run Reports, View Dashboards). Save.
4. Assign the Permission Set: Manage Assignments → Add Assignments → Select users → Assign.

Detailed Permission Set examples:

|  |  |  |
| --- | --- | --- |
| Permission Set | Key Permissions | Suggested Assignees |
| View Reports Set | Run Reports, View Dashboards | Retailers (selected), Sales Team |
| Export Data Set | Export Reports, (optional) Manage Public Reports | Trusted Wholesaler users, Analysts |
| API Access Set | API Enabled, (optional) Modify All Data if integration needs it | Inventory Integration User, System Admins |

[Insert screenshot: screenshots/permission-sets.png]

## 4.4 Org-Wide Defaults (OWD)

Steps to configure OWD:

1. Setup → Sharing Settings → Edit the Organization-Wide Defaults.
2. Set Orders: Private (recommended).
3. Set Products: Public Read Only (so retailers can browse product catalog).
4. Set Inventory: Private (only inventory team and managers view).
5. Save and plan sharing rules for broader access where necessary.

OWD Example:

* - Orders → Private
* - Products → Public Read Only
* - Inventory → Private

[Insert screenshot: screenshots/owd.png]

## 4.5 Sharing Rules

Steps to create Sharing Rules:

1. Setup → Sharing Settings → Scroll to the relevant object (Orders) → New Sharing Rule.
2. Choose rule type: Based on record owner or criteria-based.
3. If owner-based: Select "Share records owned by members of" → pick role/group → Grant Read/Read-Write.
4. If criteria-based: Define criteria (e.g., Order.Status equals "Dispatched") and share with role/group.
5. Save and run recalculation if necessary.

Sample Sharing Rules:

|  |  |  |
| --- | --- | --- |
| Rule Name | Rule Type & Criteria | Access Granted |
| Sales Managers - Team Orders | Owner-based: Owned by Sales Rep role | Read/Write to Sales Manager role |
| Wholesalers - All Retailer Orders | Owner-based: Owned by Retailer Role | Read to Wholesaler users |
| Delayed Orders Alert | Criteria-based: Order.Status = "Delayed" | Read to Ops Manager & Support Group |

[Insert screenshot: screenshots/sharing-rules.png]

## 4.6 Login Access Policies

Steps and recommended settings:

1. Setup → Session Settings → Set Session Timeout (e.g., 30 minutes).
2. Setup → Network Access → Add Trusted IP Ranges (Office Range example: 203.0.113.0/24).
3. Setup → Profiles → Select Profile → Login IP Ranges to lock profile-only IPs (for highly restricted users).
4. Setup → Identity → Multi-Factor Authentication for User Interface Logins → Enforce MFA for all users (or via permission sets).
5. Enable Login Forensics and Review Login History periodically.

Sample settings:

* - Session Timeout: 30 minutes
* - Trusted IP Range (Office): 203.0.113.0 - 203.0.113.255
* - MFA: Enforced for all internal and external users

[Insert screenshot: screenshots/login-policies.png]

# 5. Sandbox & Deployment Basics

Steps and recommendations:

1. Setup → Sandboxes → Create New Sandbox. Choose type: Developer, Partial, or Full (UAT).
2. Developer Sandbox → Use for development and unit testing (no production data).
3. Partial Copy → Use for integration tests with sample data.
4. Full Sandbox → Full copy for User Acceptance Testing (pre-production).
5. Deployment: Use Change Sets for simple metadata deployments (Setup → Outbound Change Sets).
6. For modern CI/CD use Git + SFDX + VS Code and an automated pipeline (Jenkins/CircleCI/GitHub Actions).
7. Backup: Regular data exports and backup strategy (weekly/monthly).

[Insert screenshot: screenshots/sandbox.png]

# Deliverables for Phase 2

* Completed Company Profile configuration (Business Hours, Holidays, Fiscal Year).
* Users created and assigned with correct Licenses and Profiles.
* Role hierarchy implemented matching company structure.
* Profiles and Permission Sets created and assigned.
* OWD and Sharing Rules configured.
* Login Access & Security policies enforced (IP, Session Timeout, MFA).
* Sandbox strategy documented and initial sandboxes created.
* Deployment plan (Change Sets / SFDX) documented.

# Appendix A: Sample Permission Matrix

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| User | Profile | Role | View Reports PS | Export Data PS | API Access PS |
| wholesaler.ops@acme.com | Wholesaler Profile | Operations Manager | Yes | Yes | No |
| john.retailer@store.com | Retailer Profile | Retailer Role | Yes | No | No |
| alice.sales@acme.com | Sales Team Profile | Sales Rep | Yes | No | No |
| inventory@acme.com | Inventory Manager Profile | Inventory Team | No | No | Yes |