Phase 5 – Security, Profiles & Permission Sets

1. Objective

Phase 5 focuses on securing the Visitor Management CRM system by setting up profiles, permission sets, field-level security, and providing the correct access levels to users. The goal is to ensure data protection, controlled visibility, and secure operations.

2. Understanding Salesforce Security Model

Salesforce uses several layers of security:

1. Organization-Level Security
2. Object-Level Security (Profiles, Permission Sets)
3. Field-Level Security
4. Record-Level Security (OWD, Sharing Rules)

Phase 5 will cover all these areas.

3. Profiles Setup

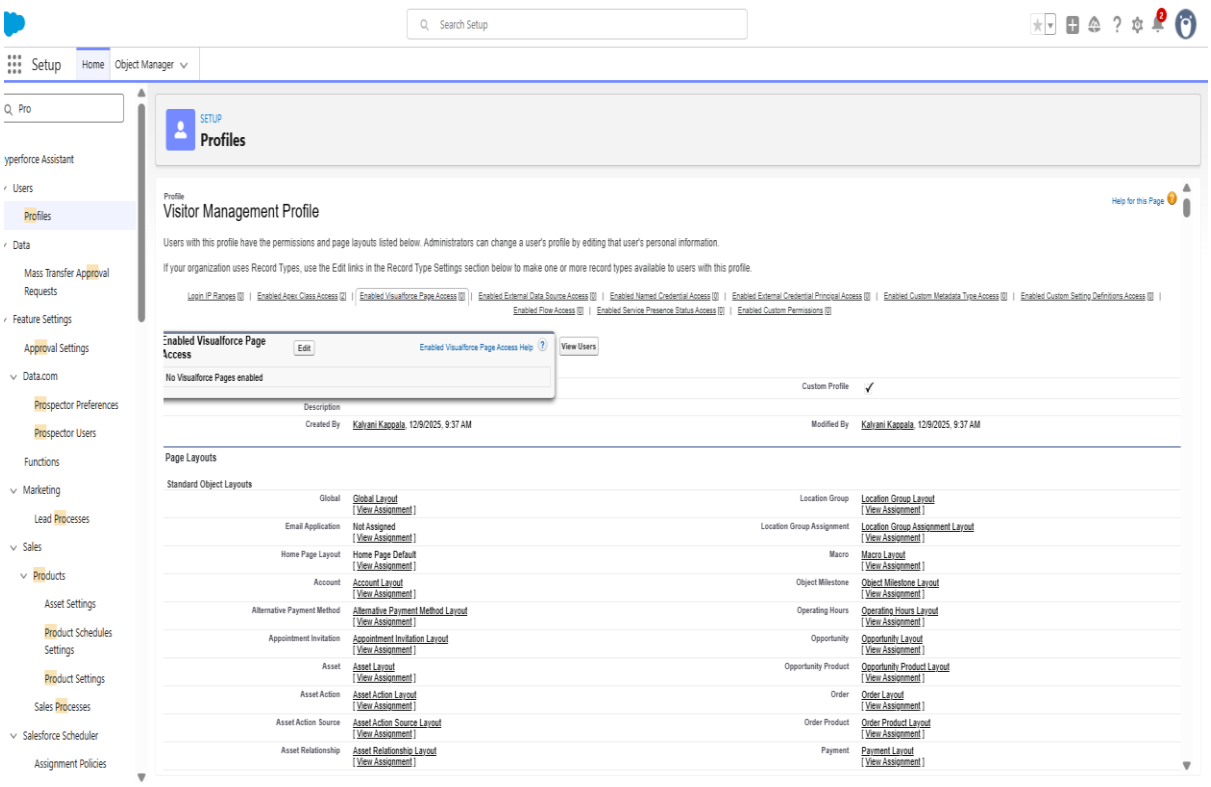
Profiles determine what users can *do* in Salesforce.

3.1 Steps to Configure Profiles

1. Go to Setup → Profiles.
2. Clone the Standard User profile to create:
    - Visitor Management Profile
3. Assign this profile to users who manage visitor entry.

3.2 Permissions to Provide

- Read, Create, Edit on **Visitor Object**
- Read access to **User Object** (for Host lookup)
- Read access to dashboards and reports

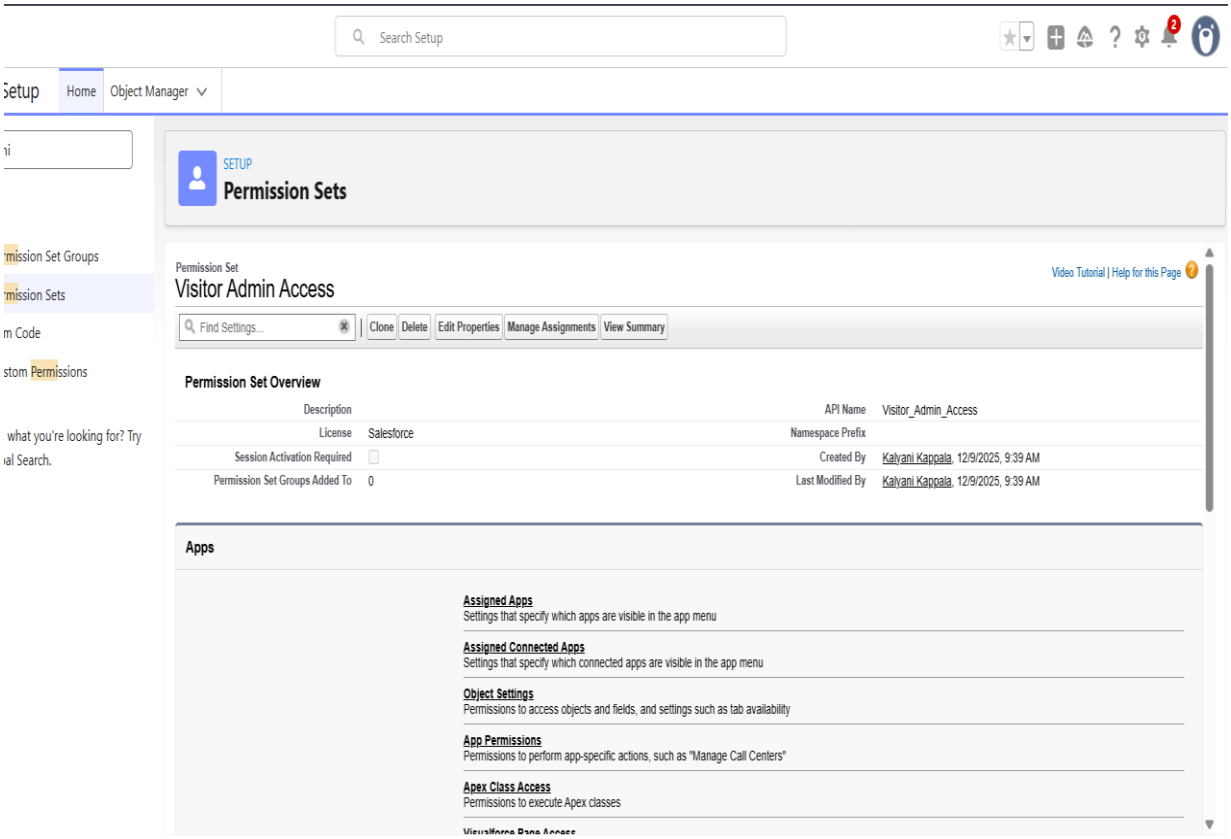


4. Permission Sets

Permission Sets are used to give extra access without changing the profile.

4.1 Create a Permission Set

1. Setup → Permission Sets → **New Permission Set**
2. Label: **Visitor Admin Access**
3. License: Salesforce
4. Save



4.2 Add Permissions

- Modify All on Visitor Object
- Manage Reports
- Manage Dashboards

4.3 Assign Permission Set

Assign to admin-level users who need advanced access.

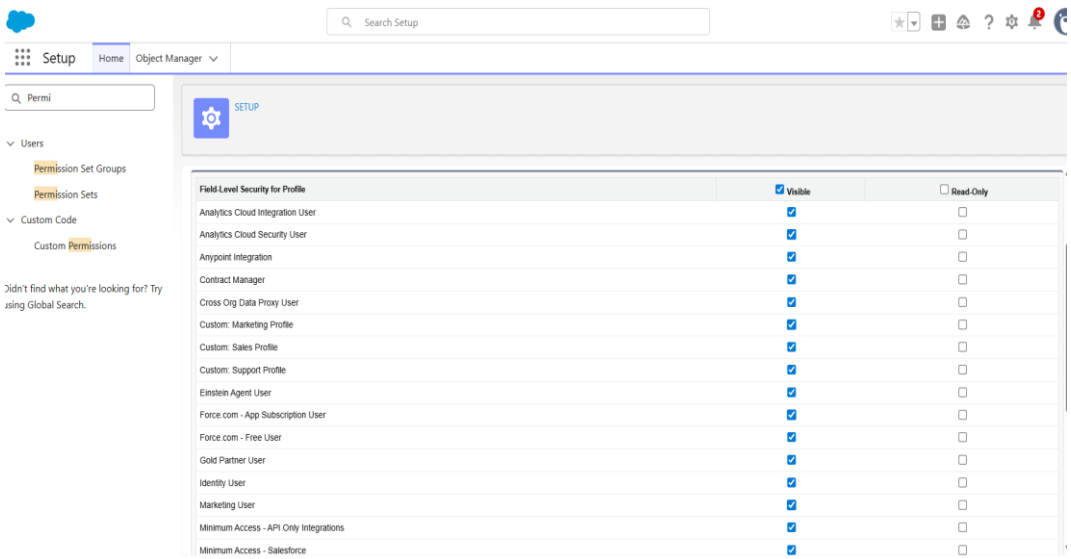
5. Field-Level Security (FLS)

FLS controls which fields are visible or editable.

5.1 Configure Field Access

1. Go to Object Manager → Visitor → Fields & Relationships
2. Select each field → Set Field-Level Security
3. Make sure:
    - ID Proof Number = Visible but not editable for standard users

- Check-In Time = Read-only for standard users
- Check-Out Time = Read-only for standard users

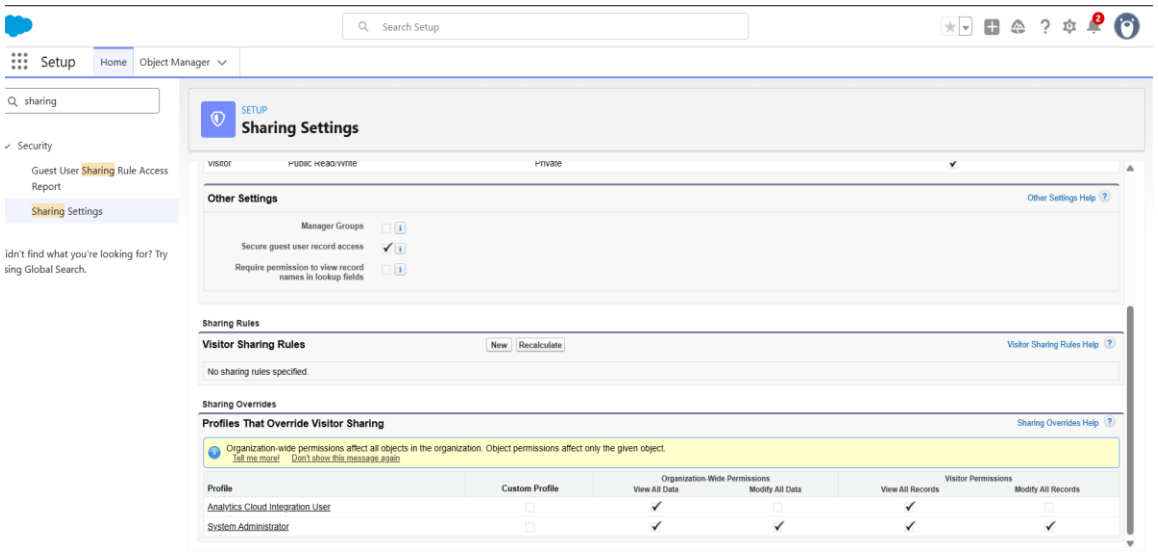


6. Organization-Wide Defaults (OWD)

Defines default record visibility.

6.1 Steps

1. Setup → Sharing Settings
2. Visitor Object → Change to:
   - Private or Public Read Only



6.2 Meaning

- Private → Only record owner and admin can see the record
- Public Read Only → Everyone can see but only owner can edit

Set according to your project requirement.

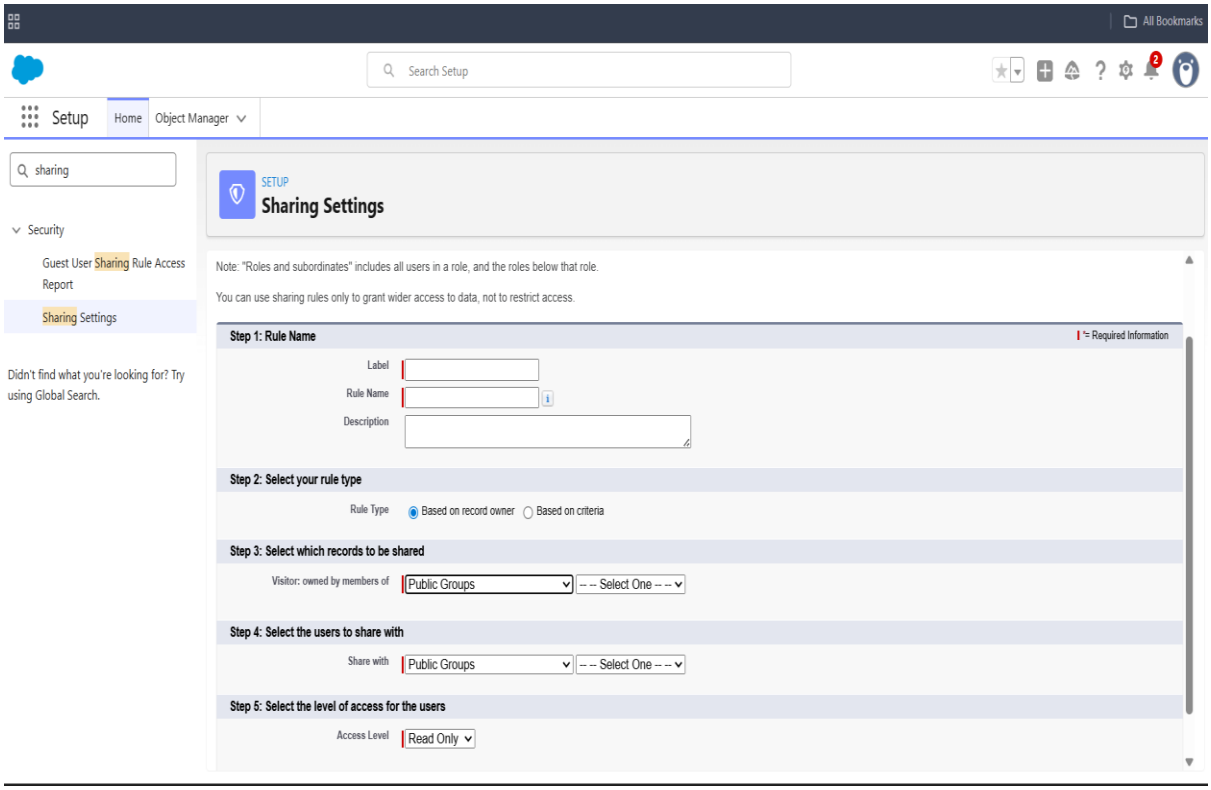
7. Sharing Rules

If OWD is Private, you must create sharing rules.

7.1 Example Sharing Rule

Goal: Allow Receptionists to view all visitor records.

1. Setup → Sharing Settings
2. Visitor Object → New Sharing Rule
3. Based on: Record Owner or Criteria
4. Share with: Public Group – Reception Team
5. Access Level: Read Only



8. Login Access Policies

Set security for login:

- Enable Two-Factor Authentication for Admin
- Restrict login times for standard users
- Restrict login IP ranges (optional)

Screenshot Placeholder: Login access settings

9. Testing Phase 5 Security

Create two test users:

User A – Reception User (Limited Access)

- Should see Visitor records
- Cannot edit restricted fields
- Cannot delete records

User B – Admin User

- Full access
- Can manage dashboards, reports, visitors

10. Summary

Phase 5 ensures your Visitor Management CRM is **secure and role-based**, with:

✓ Correct profiles
✓ Permission sets
✓ Field-level security
✓ OWD and sharing rules
✓ Controlled user access