Phase 9: Security, Access, and User Management

1. Profiles & Permission Sets

Purpose: Control user access to objects, fields, and features.
Steps Performed:

1. Navigate to **Setup → Profiles**.
2. Configure **Manager**, **Agent**, and **Customer** profiles:
   - Assign object-level and field-level permissions for **Policy**, **Claim**, and **Agent** objects.
   - Set access to tabs and apps based on roles.
3. Use **Permission Sets** to grant additional permissions beyond profiles as needed.

---

2. Roles & Role Hierarchy

Purpose: Ensure proper record-level access based on organizational hierarchy.
Steps Performed:

1. Navigate to **Setup → Roles**.
2. Create roles such as **Manager**, **Agent**, **Customer Service**.
3. Define hierarchy so that managers can see records owned by their subordinates.
4. Assign users to appropriate roles.

---

3. Sharing Rules

Purpose: Provide access to records beyond role hierarchy when needed.
Steps Performed:

1. Navigate to **Setup → Sharing Settings**.
2. Create **Sharing Rules** for objects like Policy and Claim.
3. Define criteria-based or owner-based sharing to grant read/write access.

---

4. Login & Authentication Settings

Purpose: Ensure secure access to Salesforce.
Steps Performed:

1. Navigate to **Setup → Session Settings** and **Login Access Policies**.
2. Enable IP restrictions or trusted IP ranges if required.
3. Optionally configure **Two-Factor Authentication** (2FA) for added security.

---

5. User Management

Purpose: Manage creation, activation, and roles of users in Salesforce.
Steps Performed:

1. Navigate to **Setup → Users**.
2. Create users for **Managers**, **Agents**, and **Customers**.
3. Assign appropriate **Profile**, **Role**, and **License**.
4. Verify login access and permissions.