**Phase 6: Security and Access Control**

**Introduction**

In this phase, we implemented **Security and Access Control** to make sure that only the right users have access to the appropriate data and functionality in our Loyalty Program project. The goal was to strike a balance between usability and data protection.

**1. Profiles**

Profiles provide baseline access to objects, tabs, fields, and permissions.  
We created and configured:

* **Support Agent Profile**
  + Can create and view Orders, Cases, and related Loyalty Members.
  + Cannot directly approve high-value redemptions.
  + Limited to operational tasks only.
* **Support Manager Profile**
  + Has extended permissions to approve Reward Redemptions above the threshold.
  + Access to dashboards and reports for monitoring team activity.
  + Can manage escalation cases.

**2. Permission Sets**

Permission Sets provide extra permissions without modifying the core profile.

* **Case\_Team\_Lead\_Access**
  + Grants additional case features like case team visibility and reassignment.
* **Experience\_Profile\_Manager**
  + Allows Experience Cloud portal features for loyalty members.
  + Manages external user access and visibility.

**3. Organization-Wide Defaults (OWD)**

To protect sensitive data, we configured OWD for custom objects:

* **Loyalty Member\_\_c → Private**  
  (Only the owner and those above in the role hierarchy can see records).
* **Reward Redemption\_\_c → Private**  
  (Only approvers/managers see high-value redemptions).
* **Loyalty Points History\_\_c → Controlled by Parent**  
  (Visibility comes from related Loyalty Member record).

This ensures sensitive loyalty data isn’t widely visible across the org.

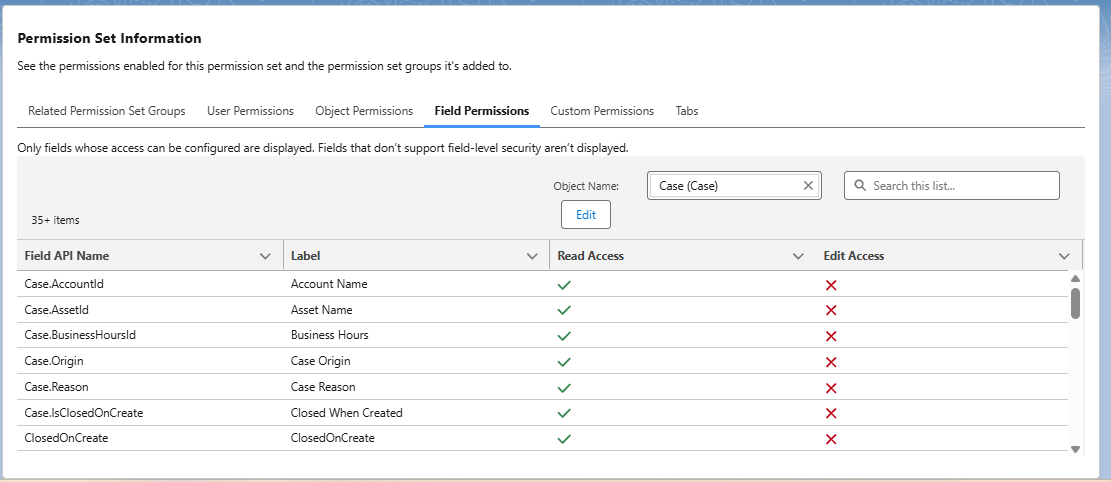
**4. Role Hierarchy**

We set up a **role hierarchy** so managers can view their agents’ records:

* **Support Manager (Top role)**
  + Sees all loyalty operations.
  + Approves escalations and high-value redemptions.
* **Support Agent (Reports to Manager)**
  + Handles customer cases and order activations.
  + Limited view of only their own customer records.

**5. Field-Level Security**

Field-level security was applied to ensure sensitive fields are only visible to appropriate users. For example:

* **CLV\_Score\_\_c (Customer Lifetime Value)** → Hidden from Support Agents, visible to Support Managers only.
* **Approver\_\_c field (Contact approval lookup)** → Editable by managers, read-only for agents.

