Gestion des droits d’accès – Application Salesforce LTP

1. Introduction

Ce document définit les **droits d’accès** par profil utilisateur à chaque objet Salesforce standard ou personnalisé utilisé dans l’application Lightning développée pour *Le Temps des Papillons* (LTP). Il précise également les règles d’accès aux enregistrements selon la zone géographique pour les agents de support.

---

2. Distinction entre profils, rôles et permission sets

Élément	Description	Exemple
Profil	Définit les permissions sur les objets, champs, enregistrements, onglets, applications.	Le profil *Support Agent* a l’accès en lecture seule aux objets `Account` et `Opportunity`.
Rôle	Définit la visibilité hiérarchique sur les enregistrements (OwnerId + règles de partage).	Le rôle *Support Europe* permet à un agent de voir les `Livraison__c` de la zone "Europe".
Permission Set *(optionnel)*	Étend dynamiquement les permissions d’un utilisateur sans changer de profil.	Un commercial senior peut recevoir temporairement l’accès à `Reports` via un Permission Set.

---

3. Profils utilisateurs Salesforce

Nom du profil	Description
Commercial	Membres de l’équipe de vente
Support Agent	Agents de support (France, Europe, International) – visibilité restreinte par rôle

Administrateur Système	Accès complet, maintenance et configuration

> 💡 Tous les agents support utilisent le même profil unique, car la distinction d'accès aux livraisons se fait par règles de partage + rôle hiérarchique.

---

4. Droits d'accès aux objets Salesforce

Objet Salesforce	Commercial	Support Agent	Admin	Justification
Lead	CRUD	R	Full	Seul le commercial gère les leads
Account	CRUD	R	Full	Lecture uniquement pour le support
Contact	CRUD	R	Full	Lecture d'informations clients
AccountContactRelation	CRU	R	Full	N:N entre comptes et contacts
Opportunity	CRUD	R	Full	Seul le créateur modifie
OpportunityLineItem	CRU	R	Full	Lecture des articles commandés
Product2	R	R	Full	Consultation du catalogue produit
Pricebook2	R	R	Full	Lecture des prix
Livraison__c	CRU	R U (zone assignée)	Full	Modif restreinte par zone via Sharing Rules
Transporter_Config__c	R	R	Full	Lecture technique uniquement

Légende :

- C = Create

- R = Read
- U = Update
- D = Delete
- RU(zone) = Accès conditionnel via Zone__c et Role (sharing rule)
- Full = tous les droits (CRUD)
- — = Aucun accès

---

5. Règles de visibilité des enregistrements (data access)

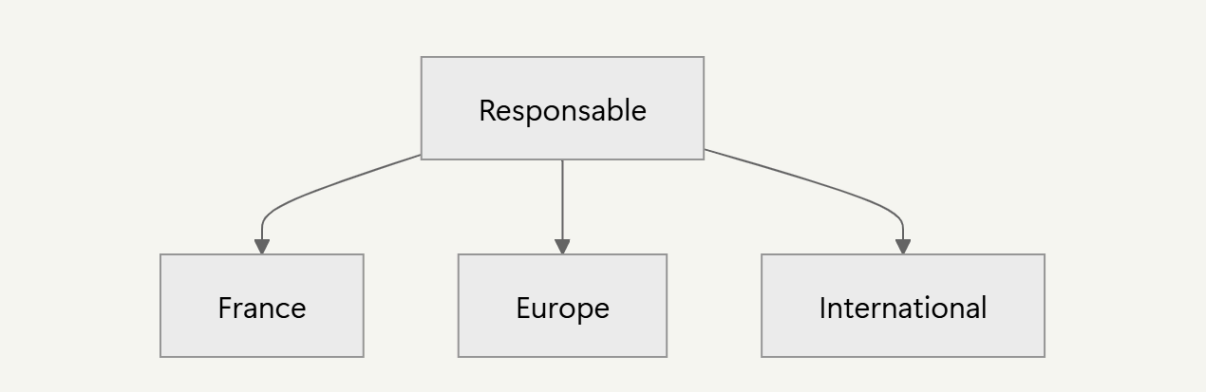
5.1 Organisation-Wide Defaults (OWD)

Objet	Accès par défaut interne (OWD)	Justification principale
Lead	Public Read/Write	Affectation et suivi Partagé entre commerciaux
Account/Contact	Public Read Only	Support + ventes
Opportunity	Public Read Only	Seul le créateur modifie
Livraison__c	Private	Restriction par zone
Transporter_Config__c	Public Read Only	Lecture uniquement

5.2 Règles de partage (Sharing Rules)

Objet	Cible	Critère de partage
Livraison__c	France	Zone__c = 'France'
Livraison__c	Europe	Zone__c = 'Europe'
Livraison__c	International	Zone__c = 'International'

5.3 Hiérarchie de rôles



Ce schéma permet d’assurer la remontée de visibilité dans la hiérarchie : un responsable peut consulter les enregistrements de ses subordonnés.

---

6. Contrôle d’accès aux champs (Field-Level Security)

Certains champs sont **masqués ou limités** pour les profils support, selon leur **sensibilité métier**.

6.1 Livraison__c – Accès champ par champ

Champ	Commercial	Support Agent	Justification
`Zone__c`	RW	**Read-only**	Utilisé pour le filtrage, verrouillé
`Transporter__c`	RW	RW	Nécessaire pour logistique
`Status__c`	RW	RW	Gestion du suivi client
`Tracking_Number__c`	RW	RW	Clé d'identification de la livraison
`Delivery_Date__c`	RW	RW	Important pour prévisions client
`CSV_Imported__c`	R	R	Lecture seule (champ protégé par Apex)

6.2 Champs sensibles d'autres objets

Champ	Commercial	Support Agent	Justification
`AnnualRevenue` (Account)	Read-only	Masqué	Donnée financière sensible
`ExpectedRevenue` (Opportunity)	RW	Masqué	Donnée stratégique interne
`Jigsaw`, `NaicsCode`, `DunsNumber`	RW	Masqué	Données inutiles pour support

7. Contrôles applicatifs

Mécanisme	Technologie utilisée	Rôle
Contrôle d'intégrité (Status sans Tracking)	`Flow` déclenché sur `Livraison__c` (Before Save)	Vérification que `Status = 'Livré'` implique la présence d’un `Tracking_Number__c`
Blocage modification post-import	`Validation Rule` + champ `CSV_Imported__c` en lecture seule	Empêche modification manuelle après import Talend
Séparation logique	`Service Apex` + `Webservice REST`	Encapsulation des traitements (ex : suivi livraison, logs API)

Mécanisme	Technologie utilisée	Rôle
Sécurité et gouvernance	`with sharing`, contrôle FLS/CRUD dans Webservices	Respect de la sécurité Salesforce
Logs d'intégration	`CSV_Import_Log__c` alimenté par **Talend** ou **Webservice Apex**	Journal d'import CSV sans Trigger
Notification d'échec	`Flow` déclenché sur `CSV_Import_Log__c`	Envoie un mail ou une alerte admin en cas d'erreur critique

Exemple de Validation Rule :

```
AND(
  ISPICKVAL(Status__c, "Livré"),
  ISBLANK(Tracking_Number__c)
)
```

Message d'erreur :

"Un numéro de suivi est requis lorsque le statut est 'Livré'."

8. Extension par Permission Sets (facultatif)

Permission Set	Cible	Usage
`ReportingAccess`	Commercial senior	Accès à `Dashboard`, `Report`
`ImportControl`	Intégrateur technique	Droit temporaire d'accès aux objets `Livraison__c`, `Transporter_Config__c`
`API_Access_Extension`	Utilisateurs intégration	Utilisation REST API spécifique

> 💡 Cela permet une flexibilité sans modifier les profils de base.

---

9. Conclusion

Cette configuration :

- Respecte les bonnes pratiques Salesforce (principe du moindre privilège)
- S'appuie sur la combinaison profils + rôles + règles de partage
- Garantit une séparation logique des responsabilités
- Assure une évolutivité et une auditabilité renforcée

Annexes : Configuration Technique

10.1 Exemples de SOQL pour contrôle de visibilité

```
// Récupérer les Livraisons visibles par l'utilisateur courant (en respectant les règle
s de partage)
List<Livraison__c> livs = [SELECT Id, Status__c, Zone__c FROM Livraison__c WHE
RE Zone__c = :User.Zone__c__c];
```

10.2 Exemple de JSON Webhook entrant (transporteur → Salesforce)

```
{
  "tracking": "FR-2024-00012345",
  "status": "Delivered",
  "eta": "2024-10-12T17:30:00Z",
  "transporter": "LTP France"
}
```

10.3 Exemple de Mapping Talend (CSV → Livraison__c)

CSV Column	Salesforce Field
tracking_number	Tracking_Number__c
zone	Zone__c
status	Status__c
delivered_at	Delivery_Date__c
imported	CSV_Imported__c