🔒 Sécurisation de l'Application - Système d'Administration

📋 Vue d'Ensemble

L'application est maintenant sécurisée avec un système d'administration complet. Seul l'administrateur peut approuver les nouveaux utilisateurs.

🔐 Compte Administrateur

Identifiants de Connexion

```
Email    : admin@reelgen.ai
Password : Admin123!@#
```

⚠️ **IMPORTANT** : Changez ce mot de passe après votre première connexion !

🎯 Fonctionnalités de Sécurité

1. Système de Rôles

```
enum UserRole {
  ADMIN  // Administrateur - accès complet
  USER   // Utilisateur standard - accès après approbation
}
```

2. Approbation Obligatoire

Tous les nouveaux comptes sont désactivés par défaut

```
Inscription → Compte créé (isApproved = false) → Attente approbation admin → Accès autorisé
```

3. Contrôles d'Accès

À l'Inscription

- ✅ Compte créé avec `isApproved = false`
- ✅ Message affiché : "Veuillez attendre l'approbation de l'administrateur"

À la Connexion

- ✅ Vérification de `isApproved`
- ❌ Refus si non approuvé : "Votre compte n'a pas encore été approuvé"
- ✅ Connexion réussie si approuvé

Au Dashboard

- ✅ Seuls les utilisateurs approuvés accèdent au dashboard
- ✅ L'onglet Admin est visible uniquement pour les administrateurs

🛠️ Panneau d’Administration

Accès

1. Connectez-vous avec le compte admin
2. Cliquez sur l’onglet **Admin** (icône bouclier 🛡️)

Fonctionnalités

📊 Statistiques

- **Total Utilisateurs** : Nombre total d’utilisateurs
- **En Attente** : Utilisateurs non approuvés
- **Approuvés** : Utilisateurs avec accès

✅ Gestion des Demandes Pendantes

Pour chaque utilisateur en attente :
- **Informations** : Nom, email, date d’inscription
- **Actions** :
- ✅ **Approuver** : Donne l’accès à l’application
- 🗑️ **Supprimer** : Rejette définitivement la demande

👥 Gestion des Utilisateurs Approuvés

Pour chaque utilisateur approuvé :
- **Informations** : Nom, email, nombre de vidéos générées
- **Badge** : Role (Admin/User), Statut (Approuvé)
- **Actions** :
- ❌ **Révoquer** : Retire l’accès (peut être réapprouvé plus tard)
- 🗑️ **Supprimer** : Supprime définitivement l’utilisateur et ses données

🔄 Workflow d’Approbation

Scénario 1 : Nouvel Utilisateur

```
1. Utilisateur s'inscrit
   ↓
2. Compte créé avec isApproved = false
   ↓
3. Message affiché : "Attente approbation administrateur"
   ↓
4. Admin reçoit notification dans le panneau Admin
   ↓
5. Admin approuve ou rejette
   ↓
6. Si approuvé : Utilisateur peut se connecter
   Si rejeté : Compte supprimé
```

Scénario 2 : Révocation d'Accès

```
1. Admin clique sur "Révoquer"
   ↓
2. isApproved = false
   ↓
3. Utilisateur déconnecté automatiquement
   ↓
4. Prochaine connexion : "Compte non approuvé"
   ↓
5. Admin peut réapprouver plus tard
```

🗄️ Modifications de la Base de Données

Nouveau Schéma User

```prisma
model User {
  id            String    @id @default(cuid())
  email         String    @unique
  password      String?
  firstName     String?
  lastName      String?
  name          String?

  // ✨ Nouveaux champs de sécurité
  role          UserRole  @default(USER)
  isApproved    Boolean   @default(false)
  approvedAt    DateTime?
  approvedBy    String?   // ID de l'admin qui a approuvé

  createdAt     DateTime  @default(now())
  updatedAt     DateTime  @updatedAt
}

enum UserRole {
  ADMIN
  USER
}
```

🔌 API d'Administration

Endpoints Créés

GET `/api/admin/users`

- **Auth** : Admin uniquement
- **Retour** : Liste de tous les utilisateurs
- **Données** : email, nom, rôle, statut, nombre de vidéos

POST `/api/admin/users/[userId]/approve`

- **Auth** : Admin uniquement
- **Body** : `{ "approve": true/false }`
- **Action** : Approuve ou révoque un utilisateur

DELETE `/api/admin/users/[userId]/delete`

- **Auth** : Admin uniquement

- **Action** : Supprime définitivement un utilisateur
- **Sécurité** : Un admin ne peut pas se supprimer lui-même

🎨 Interface Utilisateur

Onglet Admin (Nouveau)

Visible uniquement pour les administrateurs

Mobile

```
┌──────┬───────┬────────┬───────┬─────────┐
│Create│History│Settings│Profile│ 🛡️Admin│
└──────┴───────┴────────┴───────┴─────────┘
```

Desktop

```
┌──────┐
│ 🏠   │ Create
│ 📜   │ History
│ ⚙️   │ Settings
│ 👤   │ Profile
│ 🛡️   │ Admin ← Nouveau
└──────┘
```

Cartes Utilisateurs

En Attente

```
┌──────────────────────────────────────────┐
│ John Doe                    [En attente] │
│ john@example.com                         │
│ Inscrit le 26/10/2025                    │
│                                          │
│              [✅ Approuver]  [🗑️ Supprimer]│
└──────────────────────────────────────────┘
```

Approuvé

```
┌──────────────────────────────────────────┐
│ Jane Smith            [USER] [Approuvé]  │
│ jane@example.com                         │
│ 5 vidéo(s) générée(s)                    │
│                                          │
│              [❌ Révoquer]  [🗑️ Supprimer] │
└──────────────────────────────────────────┘
```

🔒 Sécurité Renforcée

1. Authentification

- ✅ Vérification de `isApproved` à chaque connexion
- ✅ Messages d'erreur clairs
- ✅ Impossibilité de contourner l'approbation

2. Autorisation

- ✅ APIs admin protégées (vérification du rôle)
- ✅ Interface admin cachée aux non-admins
- ✅ Un admin ne peut pas se supprimer lui-même

3. Traçabilité

- ✅ `approvedAt` : Date d'approbation
- ✅ `approvedBy` : ID de l'admin qui a approuvé
- ✅ Historique complet dans la base de données

📝 Modifications de Code

Fichiers Créés

```
app/api/admin/users/route.ts
app/api/admin/users/[userId]/approve/route.ts
app/api/admin/users/[userId]/delete/route.ts
app/dashboard/_components/admin-panel.tsx
```

Fichiers Modifiés

```
prisma/schema.prisma                          # Ajout role, isApproved, etc.
lib/auth.ts                                   # Vérification isApproved
app/api/signup/route.ts                       # isApproved = false par défaut
app/dashboard/_components/content-generator.tsx  # Onglet Admin
app/dashboard/_components/bottom-nav.tsx      # Navigation Admin
types/next-auth.d.ts                          # Types role, isApproved
scripts/seed.ts                               # Création compte admin
```

🧪 Tests et Validation

Tests Manuels Recommandés

1. Test Inscription

1. Créer un nouveau compte
2. Vérifier message "Attente approbation"
3. Tenter de se connecter → Devrait être refusé

2. Test Approbation

1. Se connecter en tant qu'admin
2. Aller dans l'onglet Admin
3. Approuver le nouvel utilisateur
4. Vérifier que l'utilisateur peut maintenant se connecter

3. Test Révocation

1. Révoquer un utilisateur approuvé
2. Vérifier qu'il ne peut plus se connecter

4. Test Suppression

1. Supprimer un utilisateur

2. Vérifier qu'il ne peut plus se connecter
3. Vérifier que ses données sont supprimées (cascade)

🚀 Commandes Utiles

Réinitialiser le Compte Admin

```
cd nextjs_space
yarn prisma db seed
```

Voir Tous les Utilisateurs

```
cd nextjs_space
yarn prisma studio
# Ouvre une interface web pour voir la BDD
```

Approuver Tous les Utilisateurs (Dev uniquement)

```
UPDATE users SET "isApproved" = true, "approvedAt" = NOW();
```

⚠️ Notes de Sécurité

À Faire Après Déploiement

1. **Changer le mot de passe admin**
   - Se connecter avec `Admin123!@#`
   - Aller dans Paramètres
   - Changer le mot de passe

2. **Sauvegarder les identifiants**
   - Conserver les identifiants dans un gestionnaire de mots de passe
   - Ne jamais les partager

3. **Surveiller les demandes**
   - Vérifier régulièrement l'onglet Admin
   - Approuver uniquement les utilisateurs légitimes

4. **Activer les notifications (futur)**
   - Email lors d'une nouvelle inscription
   - Alerte lors d'activités suspectes

📊 Statistiques de Sécurité

Avant

- ❌ Inscription libre
- ❌ Accès immédiat après inscription
- ❌ Pas de contrôle administrateur

Après

- ✅ Inscription avec approbation requise

- ✅ Accès uniquement après validation admin
- ✅ Contrôle total de l'administrateur
- ✅ Interface d'administration complète
- ✅ Traçabilité des actions

🎯 Prochaines Améliorations Possibles

1. **Notifications Email**
   - Notifier l'admin des nouvelles inscriptions
   - Notifier l'utilisateur de l'approbation

2. **Raisons de Refus**
   - Ajouter un champ pour noter pourquoi un utilisateur est refusé

3. **Logs d'Audit**
   - Enregistrer toutes les actions admin
   - Historique des approbations/révocations

4. **Limitation de Ressources**
   - Quotas par utilisateur
   - Limitation du nombre de vidéos

5. **2FA pour Admin**
   - Authentification à deux facteurs pour le compte admin

Date de mise en place : 26 octobre 2025
Statut : ✅ Fonctionnel et testé
Niveau de sécurité : 🔒🔒🔒🔒 (4/5)