

Documentation des rôles et permissions – DigitalBank

Ce document décrit la gestion des rôles, des permissions et des politiques de sécurité implémentées dans la plateforme DigitalBank via Supabase et PostgreSQL (RLS).

1. Présentation des rôles

CLIENT

Utilisateur final de la banque digitale.

- Authentification par email et mot de passe
- Authentification multi-facteurs (MFA – TOTP)
- Accès uniquement à ses propres données
- Lecture seule sur comptes et transactions

ANALYST

Profil interne chargé de l'analyse des données.

- Authentification sécurisée
- Accès en lecture à l'ensemble des comptes
- Accès en lecture à toutes les transactions
- Aucune permission d'écriture

ADMIN

Administrateur du système.

- Accès complet à toutes les tables
- Lecture et écriture sur les comptes
- Gestion des utilisateurs
- Accès aux journaux d'audit

2. Politiques RLS (Row Level Security)

Les politiques RLS assurent que chaque utilisateur n'accède qu'aux données auxquelles il est autorisé, directement au niveau de la base PostgreSQL.

3. Tableau récapitulatif des permissions

Rôle	Lecture	Écriture	Portée
CLIENT	Oui	Non	Ses propres données
ANALYST	Oui	Non	Toutes les données
ADMIN	Oui	Oui	Toutes les données