I. Overview:

Account Billing and Subscription Management

- **What:** A system for administrators to manage user access to the application by assigning them to different subscription tiers. It also allows users to view their currently assigned plan and usage limits.
- **Who:** The **Application Administrator** who assigns and manages user subscription plans, and the **end-user** who views their assigned plan.
- **When:** When a new user signs up (they are automatically assigned the Free Plan), or anytime an administrator needs to manually change a user's access level.
- **Where:** This is managed within a secure `/admin/users` panel for administrators. Users can view their status on their `/account` page.
- **Why:** To control feature access and offer tailored feature sets to different user segments. It allows for a tiered access model where premium features can be granted to specific users by an administrator.
- **How:** Upon signing up via Firebase Authentication, a new user record is created in the Airtable `Users` table with a default `plan_id` of 'free'. An administrator can log in, navigate to the user management panel, find a specific user, and use a dropdown menu to change their `plan_id` to 'pro' or 'business'. The application's feature-gating middleware checks this `plan_id` from Airtable on every user request to determine their access rights.

Show me how to set up the admin panel.How does the BFF verify the Firebase token?What are the security best practices for the admin panel?

II. Business Requirements Document:

Version: 1.3 (Updates for Firebase & Airtable Integration)
Date: 2025-08-25
Status: Active

1. Introduction & Business Goals

1.1. Project Overview

This document details the requirements for implementing a user account and subscription management system into the SocialSync Pro platform. This system will be managed internally by administrators to control user access to different feature tiers.

1.2. Business Goals and Objectives

- **Control Feature Access:** Implement a tiered model to provide different levels of functionality to different users.
- **Drive User Upgrades:** Create a clear value proposition for higher-tier plans by gating advanced features, encouraging users to inquire about upgrades.
- **Support User Growth:** Offer a permanent "Free Plan" to allow users to experience the platform's core value indefinitely.
- **Maintain Clarity:** Ensure the user's current plan and its associated limits are always transparent and easy to understand.

2. Subscription Plans & Feature Gating

The platform will offer three distinct subscription tiers. All usage limits are calculated on a monthly basis and reset on the 1st of each month. **All new users are automatically placed on the "Free Plan" upon registration.**

2.1. Plan Tiers

Feature	**Free Plan**	**Pro Plan**	**Business Plan**
Assignment	Default	Admin Assigned	Admin Assigned
Brands	1	5	Unlimited
AI Post Refinements	20 / month	200 / month	Unlimited
AI Image Generations	10 / month	100 / month	500 / month
Posts per Media Plan	10	50	Unlimited
Scheduled Posts	15 / month	200 / month	Unlimited
Affiliate Vault Links	10	100	Unlimited
Direct Publishing	❌	✅	✅
Bulk Scheduling	❌	✅	✅
Export Brand Kit/Plan	❌	✅	✅

3. Functional Requirements (User Stories)

3.1. User Account & Onboarding

- **As a** new user, **I want to** create an account with my email and password **so that** I can access the platform.
- **As a** new user, **I want to** be automatically placed on the "Free Plan" upon signing up **so that** I can start using the basic features immediately.

3.2. Subscription Management (User View)

- **As a** user, **I want to** access a secure /account page **so that** I can view my current subscription status.
- **As a** user, **I want to** clearly see my current plan and my current monthly usage against my limits (e.g., "75/100 images used") **so that** I know my account status.

3.3. Subscription Management (Admin View)

- **As an** administrator, **I want to** access a secure /admin/users panel **so that** I can manage the system.
- **As an** administrator, **I want to** view a list of all users and their current subscription plans.
- **As an** administrator, **I want to** be able to manually change a specific user's subscription plan (e.g.,

from "Free Plan" to "Pro Plan") from a dropdown menu **so that** I can grant them access to premium features.

3.4. Feature Gating & Usage Limits

- **As a** user, **when I** reach a usage limit (e.g., for image generation), **I want to** be shown a clear message **so that** I understand why the feature is disabled.
- **As a** user on the Free Plan, **I want to** see "Upgrade" badges on premium features **so that** I know what functionality is available on higher-tier plans.

4. Non-Functional Requirements

- **Security:** User authentication will be handled by **Firebase Authentication**. The BFF will verify user identity via secure ID tokens on every request. Administrator access must be protected.
- **Reliability:** The system must ensure that a user's feature access is always in sync with the plan assigned to them in the Airtable database.

III. Project Plan:

Version: 1.3 (Updates for Firebase & Airtable Integration)
Date: 2025-08-25
Status: Active

1. Introduction

This document updates the project plan to incorporate the foundational "User Accounts & Access Control" feature set. This system is a prerequisite for managing user access to different feature tiers.

2. High-Level Schedule & Milestones

The original schedule is amended to include a critical preliminary phase for user management.

Phase	Milestone	Description	Estimated End Date
Phase 0	**User Accounts & Access**	Implement user registration, login, the admin user management panel, and feature gating logic. This is a **BLOCKER** for all subsequent phases.	Q3 2025
Phase 1	**Architecture & Foundation**	*(No change)*	Q3 2025
Phase 2	**Core Feature MVP**	*(No change)*	Q4 2025
Phase 3	**Advanced Feature Integration**	*(No change)*	Q4 2025
Phase 4	**Stabilization & Testing**	*(Scope expanded to include all account and admin features)*	Q1 2026
Phase 5	**Version 1.0 Launch**	*(No change)*	Q1 2026

3. Phase 0: User Accounts & Access - Detailed Tasks

This new phase includes the following key tasks:

1. **Technology Selection & Configuration:**
   - Configure a new **Firebase Authentication** project for the application.
   - Define the Users table schema in the existing Airtable base.

2. **Backend Development (BFF):**
   - Integrate the Firebase Admin SDK for verifying ID tokens.
   - Develop a middleware to protect all secure endpoints. This middleware will verify the Firebase ID token and then fetch the user's plan/role from Airtable.
   - Implement a "first-time login" logic: when a user's token is verified but they don't have a record in Airtable, create one for them with the default "Free" plan.
   - Implement secure, admin-only endpoints for listing users and updating a user's plan in Airtable.
3. **Frontend Development:**
   - Integrate the Firebase Client SDK for handling user registration and login flows.
   - Build the user registration and login forms.
   - Build the user-facing /account page to display the current plan and usage.
   - Build the admin-facing /admin/users panel to list all users and allow plan changes.
   - Integrate UI elements that reflect subscription status (e.g., usage counters, "Upgrade" prompts).
4. **Integration & Testing:**
   - Thoroughly test the end-to-end user registration and admin plan management flows.

4. Risk Management (Additions)

Risk ID	Description	Probability	Impact	Mitigation Strategy
R-05	**Insecure Admin Access:** The admin panel for changing user plans is not properly secured, allowing unauthorized users to elevate privileges.	Medium	High	Implement strict role-based access control (RBAC) on the BFF for all admin endpoints, based on the role field in Airtable. Ensure frontend routes for the admin panel are also protected.
R-06	**Manual Process Errors:** As the number of users grows, the manual process of changing plans becomes error-prone, leading to users being assigned the wrong plan.	Medium	Medium	Design the admin UI to be as clear as possible, with confirmation steps before a plan is changed. Implement detailed logging for all admin actions.

IV. System Architecture Document:

Version: 1.3 (Updates for Firebase & Airtable Integration)
Date: 2025-08-25
Status: Active

1. Introduction

This document updates the system architecture to incorporate **Firebase Authentication** for identity management and **Airtable** as the user profile database. This hybrid approach separates secure credential handling from application-specific user data.

2. System Overview (Updated)

The architecture now uses Firebase as a dedicated authentication service. The BFF acts as a bridge, verifying Firebase users and then retrieving their application-specific data (like their plan) from Airtable.

2.1. High-Level Architecture Diagram (Updated)

```
+-----------------+     +----------------------------+     +------------------------+
|               |     |                         |     |  External Services    |
|  Frontend      |----->|     Firebase Auth         |     | - Airtable (User &     |
|  (React, Vite)  |     |    (Handles Login)       |     |    Project Data)       |
|               |<---->|                         |<---->| - Gemini/OpenRouter (AI)|
+-----------------+     +----------------------------+     | - Cloudinary (Storage) |
       ^               |                         |     | - Facebook (Publish)   |
       | (ID Token)     |  Backend-for-Frontend (BFF)|     +------------------------+
       v               | (Verifies Token, Gets      |
+-----------------+     |  User Data from Airtable)  |
|     BFF       |----->|                         |
+-----------------+     +----------------------------+
```

3. Component Breakdown (Additions & Changes)

3.1. Firebase Authentication (New Component)

- **Service:** Google Firebase Authentication
- **Purpose:** To provide a secure, dedicated service for all user identity operations.
- **Key Responsibilities:**
  - Handling user sign-up and sign-in flows (email/password, social logins).
  - Securely storing and managing user credentials (password hashes).
  - Issuing short-lived, secure ID tokens to the frontend upon successful login.

3.2. Airtable (Updated Role)

- **Purpose:** Continues to store project data and now also stores user profile data linked to their authentication record.
- **Key Responsibilities:**
  - Storing user-specific application data like their assigned plan_id and role.
  - Linking this data to a user via their unique firebase_uid.

3.3. Backend-for-Frontend (BFF) (Updated Responsibilities)

- **Authentication Middleware:** A new middleware will protect almost every API endpoint. It will:
    1. Expect a Firebase ID Token in the Authorization header of every request.
    2. Use the Firebase Admin SDK to verify the token's validity and signature.
    3. If valid, extract the firebase_uid from the token.
    4. Use the firebase_uid to look up the user's record in the Airtable Users table.
    5. Attach the user's plan and role to the request object for use by the downstream logic.
- **Admin-Only Endpoints:** Endpoints like /api/admin/users will have an additional check in the middleware to ensure the user's role (retrieved from Airtable) is admin.

4. Data Model (Airtable Users Table)

A new Users table will be created in the Airtable base.

Column Name	Data Type	Description
firebase_uid	Single line text	**Primary Key.** The unique User ID provided by Firebase Auth.
email	Email	User's email address.
plan_id	Single select	The ID of the assigned plan (e.g., free, pro, business). Default: free.
role	Single select	User's role (e.g., user, admin). Default: user.

5. Data Flow Example: New User Registration

1. **User Action:** A new user fills out the sign-up form on the frontend and submits it.
2. **Frontend to Firebase:** The Firebase Client SDK handles the request, securely creating a new user in the Firebase Authentication service.
3. **Firebase to Frontend:** Firebase returns a success response to the frontend, including a fresh **ID Token**. The frontend now stores this token and includes it in the header of all subsequent API calls to the BFF.
4. **First API Call (e.g., to fetch data):** The frontend makes a request to a secure BFF endpoint, like /api/account.
5. BFF Middleware Verification:
   a. The BFF's authentication middleware intercepts the request and extracts the ID Token.
   b. It uses the Firebase Admin SDK to verify the token. The token is valid.
   c. The middleware extracts the user's firebase_uid from the token.
   d. It queries the Airtable Users table for a record with this firebase_uid. No record is found.
6. BFF Creates User Record:
   a. Recognizing this is a first-time login, the middleware creates a new record in the Airtable Users table.
   b. It populates the record with the firebase_uid, the user's email (also from the token), and the default values for plan_id (free) and role (user).
7. **BFF Resumes Request:** The middleware, having created the user profile, proceeds to the original endpoint's logic, which now successfully finds the user's data and returns their account status to the frontend.

V. Test Plan and Strategy:

Version: 1.3 (Updates for Firebase & Airtable Integration)
Date: 2025-08-25
Status: Active

1. Introduction

This document updates the testing strategy to include comprehensive test cases for the new "User Accounts & Access Control" feature, which is built using Firebase Authentication and Airtable.

2. Scope of Testing

2.1. In-Scope (Additions)

- **User Account Lifecycle:** Registration, login, and logout via Firebase.
- **Admin Management Lifecycle:** Admin login, viewing the user list from Airtable, changing a user's plan in Airtable.
- **Role-Based Access Control (RBAC):** Verifying that non-admin users cannot access admin panels or APIs.
- **Feature Gating:** Verification that usage limits and feature access correctly correspond to the user's plan stored in Airtable.
- **First-Time Login Flow:** Ensuring a user record is correctly created in Airtable upon their first authenticated action.

2.2. Tools & Environment

- **Test Environment:** All tests will be conducted in a staging environment.
- **Authentication:** The staging environment will be connected to a dedicated **Firebase test project** to isolate test users from production users.
- **Database:** The staging environment will connect to a dedicated Airtable test base.

3. Admin-Specific Test Scenarios (E2E)

(The test scenarios remain the same as v1.2, as they test the application's behavior, which has not changed. The underlying implementation is what these documents update.)

3.1. The "Happy Path"

- **Test Case ID:** TC-ADMIN-001
- **Scenario:** New User Registration & Admin Upgrade

3.2. Security and Access Control

- **Test Case ID:** TC-ADMIN-002
- **Scenario:** Non-Admin Access Denial

3.3. Feature Gating Verification

- **Test Case ID:** TC-ADMIN-003
- **Scenario:** Usage Limit Enforcement & Downgrade

VI. User Manual

Version: 1.3 (No Change)
Welcome! This guide will walk you through the features of SocialSync Pro and help you get started on your journey to creating amazing, AI-powered social media content.

1. Getting Started with Your Free Plan

When you first sign up for SocialSync Pro, you will be automatically placed on our **Free Plan**. This gives you immediate access to the core features of the platform and allows you to start creating content right away.

2. Viewing Your Account Plan

You can check your currently assigned plan and your monthly usage at any time.

2.1. Accessing Your Account Page

1. Click on your profile icon or name in the top-right corner of the application.
2. Select **"Account"** from the dropdown menu.

2.2. What You Can See on Your Account Page

From your account page, you can:

- **View Your Current Plan:** See which plan ("Free", "Pro", or "Business") has been assigned to your account.
- **Check Your Usage:** Monitor your monthly usage of key features like AI Image Generations and Scheduled Posts against your plan's limits. Your usage resets on the first day of every month.

3. Understanding Feature Limits

Many of SocialSync Pro's features are tied to the limits of your assigned subscription plan.

- **Premium Features:** Some features, like **Bulk Scheduling** and **Direct Publishing**, are only available on our "Pro" and "Business" plans. If you are on the "Free Plan", you will see an "Upgrade" badge next to these features. If you are interested in gaining access to these features, please contact our support team.
- **Usage Limits:** Features like AI image and text generation have monthly usage limits based on your plan. If you reach your limit for the month, the feature will be temporarily disabled until your limits reset.

(The rest of the user manual, describing core features, would follow.)