Case Study Report

ClubSphere

Group-based multi-user Platform

11
Modes supported

Multi-groups
Federation /
super -federation readiness

Randomization
Randomization review
readiness support

CONTENTS

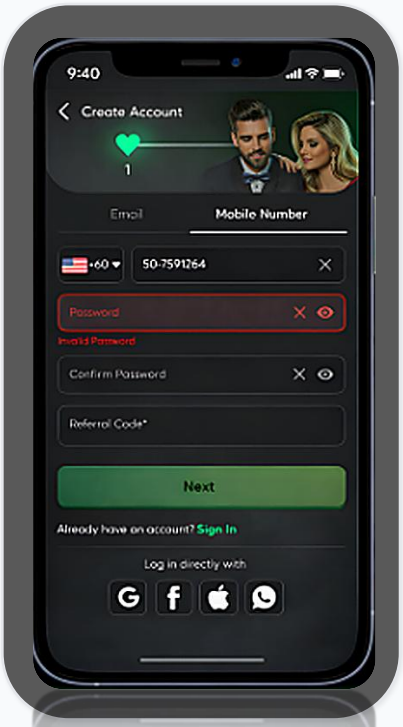
Sessions of Contents

About ClubSphere

A real-time, group-based multi-user platform implemented with Android/iOS user apps, a centralized Admin Panel, and an Ops roles Portal. Built for restricted-access groups, it supports session types and events, sessions and groups management, multi-level Ops roles hierarchy, and scheduled reports workflows. Integrity controls include verification, configurable limits, monitoring cues, and activity logs to support operational traceability.

What the platform enables

- Restricted-access groups with configurable rules and parameters
- Real-time sessions with reconnect/resume and state continuity
- Role-based administration with hierarchical permissions and periodic reporting
- Governance controls: RBAC, audit logs, and abuse detection signals



An Android/iOS multi-user platform with an Admin Panel and Ops Portal. It supports multiple gameplay modes with reconnect/resume handling and scheduled operational reports. Role-based controls manage access and visibility. Governance is supported through verification, configurable thresholds, RBAC, and activity logs.

SUMMARY

Executive Summary

What the Platform Offers

A multi-interface multi-user platform with Android/iOS user apps, an operations Admin Panel, and a Ops Portal for managing group structures and scheduled reporting cycles. It supports private groups, multiple in-app modes, and reconnect/resume for session continuity. Governance controls include verification steps, role-based access, configurable thresholds, and audit logs for traceability.

Android / iOS

User apps (mobile)

Admin Panel

Platform operations

Ops Portal.

Role hierarchy + scheduled reports

Platform surfaces (how users interact)

User App (Android / iOS)

Admin Panel (Operations)

Ops Portal (Strategic Management)

BASELINE

Client Needs & Constraints

Key operational demands

Real-time stability

Sync, reconnect/resume, consistent sessions state Real-time in-app experience updates with low-latency event handling

Restricted-access governance

Configurable operations and clear permission boundaries. RBAC separates admin vs Ops roles controls

Activity scalability

Repeatable setup templates and reporting readiness. Standardized groups configs with exportable reports

Ops roles hierarchy

Role hierarchy visibility and scheduled reports accountability. Clear role hierarchy tracking with scheduled reports traceability

Integrity readiness

RBAC, audit logs, abuse monitoring cues, randomization support. Integrity features included for governance

The platform required real-time stability with reliable sync and reconnect/resume to keep session state consistent. Restricted-access operations needed configurable controls with clear admin vs back-office permissions. role hierarchy and scheduled reports had to remain traceable, supported by governance controls such as RBAC, audit logs, monitoring cues, and documented randomization requirements.

GOALS

Objectives

01 **Real-time engage**

Implement sessions-state handling across Android and iOS, with reconnect/resume support

02 **Groups platform**

Enable restricted-access groups + unions with configurable rules, rule parameters, and permissions

03 **Ops roles operations**

Support role hierarchy tracking, scheduled reports, and export reports

04 **Governance controls**

Embed RBAC + audit logs for traceability, accountability, and controlled operations

05 **Activity scale**

Enable templates + automation-backed activity operations with reporting readiness

Focus areas

Delivery emphasis centered on in-app experience handling and operational workflows, supported by clear governance and integrity controls. Priorities also included repeatable setups and scheduled reports accountability to support consistent day-to-day execution. These focus areas reflect what was prioritized across the build, not measured percentages.

SOLUTION

Solution Summary

Implemented as a multi-interface product with three core surfaces: a User Mobile App (Android/iOS) for onboarding, private group access, account features, and core in-app flows. An Admin Panel supported platform configuration, activity/session management, and rules/settings administration. An Ops Portal enabled role-based oversight, scheduled reports, and exportable operational reports.

Workflow map (end to end)

Onboard | **Join groups** | **Engage** | **Summarize** | **Govern**

The solution connects the full multi-user lifecycle ın one flow onboarding, groups entry, live engage, and structured scheduled reports. Each step is supported by operational controls and governance, so in-app experience state remains consistent and scheduled reports remain traceable. This end-to-end map shows how user actions and back-office workflows stay aligned.

WORKFLOWS

Key Workflows Delivered

User Journey

Admin Journey

Ops roles Journey

User

- Register / login
- Join restricted-access groups
- account + groups accounting
- session types + events
- Reconnect / resume

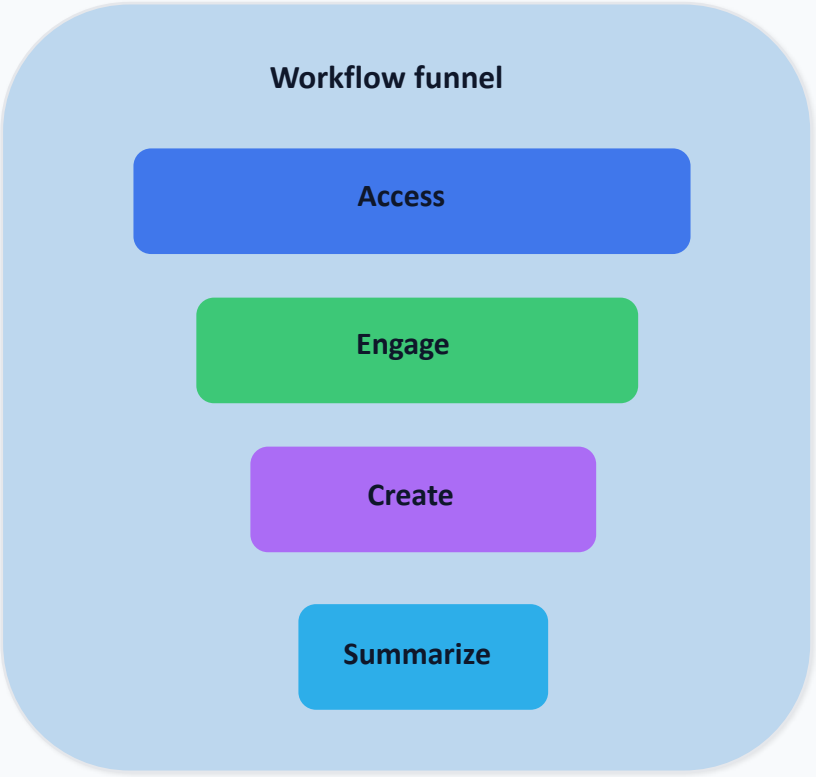
Admin / Operator

- Configure groups + rules
- Manage users + entities
- Run / supervise sessions
- activity operations
- Reporting + monitoring

Ops roles

- Role hierarchy mgmt
- Activity tracking
- scheduled reports
- allocation rules
- export reports

Workflow funnel



Designed to support the user journey from entry to live engage, while ensuring operations and governance stay clear and controlled behind the scenes.

CONTROLS

Integrity, Security & Governance

RBAC by role

Designed around admin, Ops roles, and operators to control actions.

Activity logs

Recorded events across config, operational reporting, and workflow actions.

Abuse Detection

Monitoring cues to support integrity review.

Randomization readiness

Randomization-related requirements documented for review.

Operational accountability

- Issue review supported through recorded session history
- Reviewable system events for investigations and reviews
- Permissions structured to keep sensitive actions controlled
- Governance signals visible in day-to-day operations

Controls implemented across core workflows.

DELIVERY

Implement Phases

This case study describes milestone-based delivery. The timeline below summarizes the approach in a report-ready way without asserting exact sprint dates. It highlights how core in-app experience and operational modules were built first, then expanded with governance and integrity layers. Each phase reflects incremental scope build-up and hardening through iterations.

Implementation timeline

1. **Discovery & requirements**
   In-app experience flows, role mapping, integrity checkpoints
2. **Core platform foundation**
   Auth, groups model, baseline operations
3. **In-app experience + events**
   Realtime sessions, templates, reporting readiness
4. **Ops role**
   Role hierarchy visibility, scheduled reports exports
5. **Hardening & readiness**
   Stability, controls, monitoring and release prep

Delivery principle

Treat integrity and governance as core product capabilities controls, visibility, and traceability are built into the flow throughout the build.

OUTCOMES

Outcomes & Operational Readiness

11

Modes supported

Federation

Multi-groups readiness

RBAC

Permissions + audit logs embedded

Operational outcomes

- Structured workflows support day-to-day operations
- Clear governance signals for governance visibility in operations
- Reconnect/resume handling for real-time engage
- scheduled reports exports to support operational reporting and data reconciliation

Handover & readiness

Admin and Ops roles workflows designed for daily operations (config, monitoring, scheduled reports, exports). Audit logs support accountability for accountability and issue support. Controls support scaling across multiple groups/unions while keeping permissions clear.

Stability hardening

Operationalcontrols

Reporting readiness

Export workflows