M2 | MVP Credentials Design

Supply Chain Data Verification Library

Prepared by: Sam Lambert (zenGate Global), Luca D’Angelo (zenGate Global), Shishir Pai (zenGate Global), Luiz Oliveira (zenGate Global) and Kyle Curry (Natures Nectar).

Last Edited: 12th June 2025

1. Executive Summary

Organic certification for honey production in Zambia faces significant challenges due to decentralized rural operations, low literacy and digital access, and costly in-person audits. Many producers operate far from infrastructure and lack the tools needed to collect and verify data consistently, **putting organic certification—and access to premium markets—at risk**.

Nature’s Nectar, a leading honey company in Zambia, has developed strong governance and field procedures that meet organic standards. However, the current mix of paper-based and siloed digital systems remains unreliable and inefficient for the demands of annual organic audits, which are expensive and logistically complex.

To address this, Nature’s Nectar is partnering with Palmyra Pro to **pilot a verifiable credentials and data verification module** designed as an **MVP** to**:**

- Ensure **only verified field supervisors** can submit organic survey data.
- Tie submissions to **verified individuals (via facial authentication) and precise farm locations (via metadata extraction)**.
- Organic certifiers gain **read-only access** to live data streams, laying the groundwork for **partial or full remote audits**.

This module will enable linking of **Credentials** to **Users** for data collection and collecting data on submission status.

By integrating **facial recognition authentication** and **photo metadata extraction** (GPS) capabilities into a Cardano-focussed **Credentials Library**, the system will **verify *who* is submitting, *where* they are, and create an immutable, credential-linked record on-chain**.

2. Problem Overview & Operational Challenges

The core challenge limiting organic certification and value capture in Zambia's honey sector is **low data fidelity and lack of verified reporting**. Field data collected during key activities — including farmer surveys, harvest records, and training documentation — is often unverifiable, **subject to tampering, manually editable, and lacks trusted provenance**. Without trusted, real-time, verifiable data, **organic certifying bodies and supply chain partners cannot ensure standards are met** — creating bottlenecks for certification, transparency, and scaling.

Current State of Nature's Nectar:

- **Digital field records** can be manually edited **without an audit trail**.

- **Paper-based records** — introduces human error, data loss, and verification challenges, especially in rural areas where literacy levels are lower.

- **Verification Process Not Transparent -** whilst some protocols exist for verifying data in real-time; this is not made transparent to other stakeholders (such as the certifiers).

- **Auditors** cannot access or validate data remotely during inspections — they **must rely on static exports** that can be cleaned or **altered before submission**, preventing true verification.

Consequences for Producers

This **lack of high-fidelity data dramatically increases the cost, time, and risk of organic certification for SMEs** like Nature's Nectar — and for the ~3,000 farmers they work with across distributed rural communities in Zambia's forests.

3. Overview of Our Solution & Operational Requirements

3.1 Credential Library Overview

The proposed **Minimum Viable Product (MVP)** will deliver a **Credentials Library** that forms the backbone of trusted data collection and verification processes. This will be applied to the **Organic Survey Workflows for Natures Nectar** (a real example of the form has been attached into the github repo).

Challenges in Credential and Authorization Systems for Non-Technical Users

In building a credential and authorization system for farmer applications and users unfamiliar with blockchain, we met key issues. Non-technical users, like farmers, would need to create and manage digital wallets for identity and verified actions. Mobile apps limit decentralized wallet use without browser support, and fail to handle cases like offline survey submissions. Our goal in this challenge is to provide a blockchain-abstracted solution that overcomes these challenges.

Proposed Solution: Biometric Security Layer with Centralized Credential Issuing

We propose a system with added biometric security and local geo location extraction for the data. The company CEO & Executive team; leverages ADA Handles to assign a main handle and sub-handles to each user for management. In library integrations, we abstract credential minting to skip wallet steps, making it simple for non-blockchain users. All data remains recorded on the blockchain for security and verification.

The Credentials Library will enable:

☑ **Credentials Issuance and Management:** assign, update and revoke credentials for users (i.e Field Staff and Agents); leveraging ADA Handles and Sub-Handles.

☑ **Location Verification:** Capture GPS coordinates and timestamps from photos (or phone location service as a back-up option) to verify physical presence at farm (or specified) locations.

☑ **Facial Recognition Verification:** Use biometric authentication to confirm that only credentialed individuals can log in, submit or **verify critical data** records. These are tied to the user credentials (and an initial upload of a baseline photo of the user).

3.2 Key Features and Solutions Delivered

Features	Problem it Solves (Nature's Nectar Use Case)
Credentials Management (via the Credentials Library)	Provides a robust system to create, assign, update, and revoke Field Supervisor (FS) credentials. Utilises **ADA handles** and **sub-handles** on **Cardano** to uniquely identify each FS and **links** them to their Palmyra Pro user accounts. This ensures that only approved supervisors can collect and submit organic survey data.
Facial Recognition Authentication	**Solves identity verification challenges** by ensuring that **only the verified Field Supervisor assigned to a credential can submit critical data events** (e.g. organic surveys). Each FS will have a **registered photo on file**, and for every critical submission, they must **complete a facial scan to confirm it is actually them submitting** – preventing impersonation or fraudulent entries.
Photo Metadata Extraction	Addresses location verification requirements by capturing **GPS coordinates and timestamps from survey photos**, proving that surveys are **conducted at the correct farm locations within**

	permissible operational areas rather than being completed elsewhere or fabricated.
Blockchain-Based Immutable Records [not part of library; done on the client side]	Solves data integrity and auditability issues by cryptographically signing and storing each survey submission on-chain via the Winter Protocol. This links the record directly to the FS credential, their verified identity, and the location data, creating tamper-proof, verifiable records for Nature's Nectar and organic certifiers, enabling trusted remote verification and audit readiness. **Note**: *This component will not be in the Credentials Library & is not in-scope for Catalyst - but demonstrates how existing tooling on Cardano such as the Winter Protocol can be used to bring the actual contents of the survey data on-chain.*

4. Stakeholder Roles and Responsibilities

Stakeholder	Role	Responsibilities
Nature's Nectar (Issuer)	Credential Issuer	Creates, assigns, updates, and revokes Field Supervisor credentials; manages operational permissions and ensures only verified supervisors can conduct organic surveys.
Field Supervisor (FS) – Credential Holder	Data Collector & Submitter	Uses issued credentials to authenticate identity via facial recognition, collect survey data on assigned farms, and submit verified records.
Palmyra Pro – Verifier Module	System Verifier & Integrator	Authenticates credentials, performs biometric verification, extracts photo metadata, enforces role-based permissions, and records submissions immutably on-chain.
Organic Certifiers / Auditors (Data Consumers)	Data Reviewer	Accesses read-only submissions linked to verified FS credentials for certification validation, compliance review, and audit processes.

5. Technical Design & Specifications

5.1 Technical Architecture

The Winter Authenticator is a **library** which is organised into **three independent**, **client-side TypeScript modules**. The objective is to attach a digital identity (handles) within a user's credential inside the system (the field supervisor) where we can reference who reviewed field surveys and other important data before it hits the blockchain, with an extra layer of security.

5.2 Required Tooling: Authentication Module

Purpose

- Perform face-to-face image matching
- Verify a live camera feed against a **reference image**, including optional liveness "challenge mode"
- Assess basic image quality (pose, blur, lighting) before any match attempt
- Enable composability to use multiple providers in multiple security levels

High-level API

- **compareByImage(...)** — one-to-one still-image comparison
- **compareByLiveVideo(...)** — video comparison with liveness prompts
- **checkImageQuality(...)** — lightweight pre-check

Key Design Points

- Able to be composable and run on multiple providers such AWS Rekognition, Azure AI Face, Google Vision, etc.
- Challenge mode issues a small, randomised set of prompts (e.g., eye-blink, head-turn) and validates completion within a caller-defined timeout in cases where providers accept it.
- A single configuration object (WinterAuthConfig) lets integrators adjust security level, model source, prompt set, provider and key setup, and timeouts without touching source code.
- Internally the module is split into detector, pre-processor, embedder, comparator, and challenge engine sub-components to keep concerns isolated.

- All images are hosted on client side (a self owned database) to reference the base image, and all new images can be stored or not based on implementation choice

5.3 Required Tooling: Image-Metadata Module

Purpose: Extract capture context (GPS, camera data, timestamp, dimensions) from still images and signal when fallback geolocation is advisable.

Capabilities

- Full EXIF/HEIC parsing
- Fast "GPS-only" shortcut for latency-sensitive paths
- Clear status codes (HAS_GPS, NO_GPS, UNSUPPORTED_FORMAT, etc.) so UI layers can react consistently

Edge Cases

- Not every image has GPS information, but mostly phones has the option to attach that information in the metadata
- Image extraction can be made not only on supervisors pictures but any picture uploaded, such bee hives, farm pictures, etc.
- We suggest in the library to ask for user location as a fallback when necessary

All type definitions and example calls are documented in the library reference;

5.4 Required Tooling: ADA Handles Module

Goal: Abstract blockchain needs to enable users to issue credentials (handles) for the company and handles for the staff members (sub handles), leveraging blockchain technology without having the user to deal with blockchain actions. Those credentials then are linked to each staff member where they represent individuals inside the traceability information on chain.

Current Limitations: Implementation is gated behind API endpoints from the ADA Handle team which are **not yet live**. Placeholder interfaces already exist; the feature can be activated via the feature flag once the endpoints are live. Our current solution is to point the Company CEO to manually create their Handles and Sub Handles directly on the ADA Handle portal; once they have this; they can link the sub-handles to their users (i.e the field staff or agent).

5.5 Privacy & Security

- Default behaviour keeps all biometric and metadata processing on the client; nothing leaves the device unless explicitly enabled by the host application.

- Codebase is open source and documentation provides a clear explanation of how every method works

5.6 Smart Contracts

Following extensive internal discussions and consultations with Nature's Nectar, we have concluded that the most effective and pragmatic approach is **not to create new smart contracts** for credential issuance or verification at this stage. Instead, we are leveraging **existing decentralized identity (DID) and credential frameworks** on **Cardano**, specifically integrating **ADA Handles** for user identification.

This decision was based on the following key factors:

- **End-User Simplicity**: The primary users of this system are field staff and farmers, many of whom are non-technical. Requiring them to manage wallets or interact with on-chain systems directly would be a significant barrier to adoption. Therefore, we prioritized **blockchain abstraction** wherever possible; enabling the CEO and Exec team to be responsible for this (as they are more technical and have a base understanding of wallet management).

- **Mobile and Browser Limitations**: Many wallet tools are not yet fully compatible with mobile-first applications or embedded browser environments. ADA Handles offer a user-friendly alternative for identity assignment that can be managed centrally and linked to credentials without requiring each user (i.e field staff) to manage a wallet themselves.

- **Security and Verification Layer Handled Off-Chain**: By embedding **biometric (facial recognition)** and **geo-verification (GPS metadata)** steps ***prior* to data submission**, we ensure a high-trust layer that validates identity and location even before reaching the blockchain. These mechanisms are tied directly to issued credentials and enable verified audit trails without smart contract complexity. These solutions were not in-scope for the initial catalyst submission - but we decided this would be the most pragmatic solution to increase **trust** and leverage **existing tooling** available through ADA Handles.

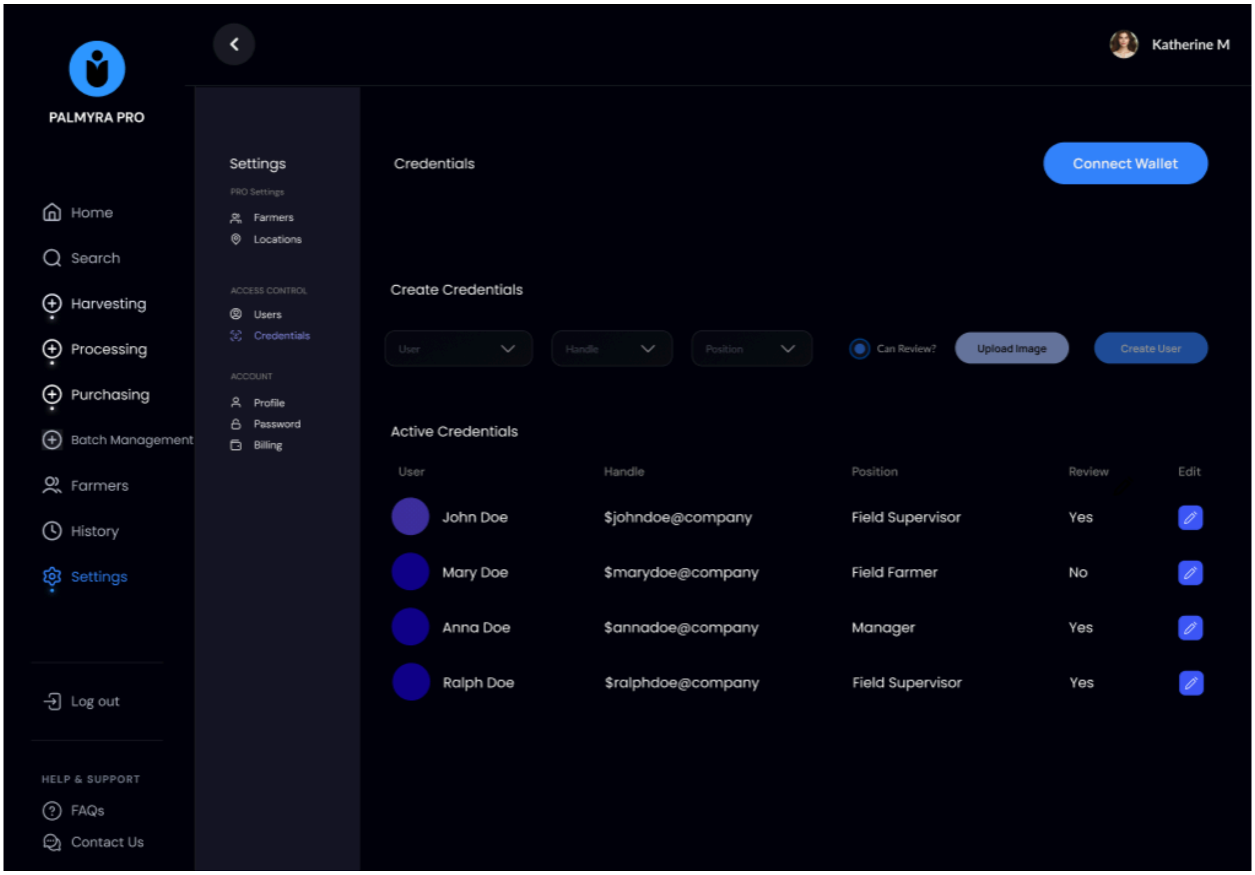
As a result, **no additional smart contract development is required for credential management** in this proposal. The verification and audit integrity are fully enforced through the layered client-side modules and the use of verifiable identity (ADA Handles).

6. Figma UI/ UX Screens

Example UI Flows

We have designed some simple flows leveraging our existing Palmyra Pro implementation with Nature's Nectar; where by the library can be leveraged both for assigning credentials to the user and the authentication tools specified above.

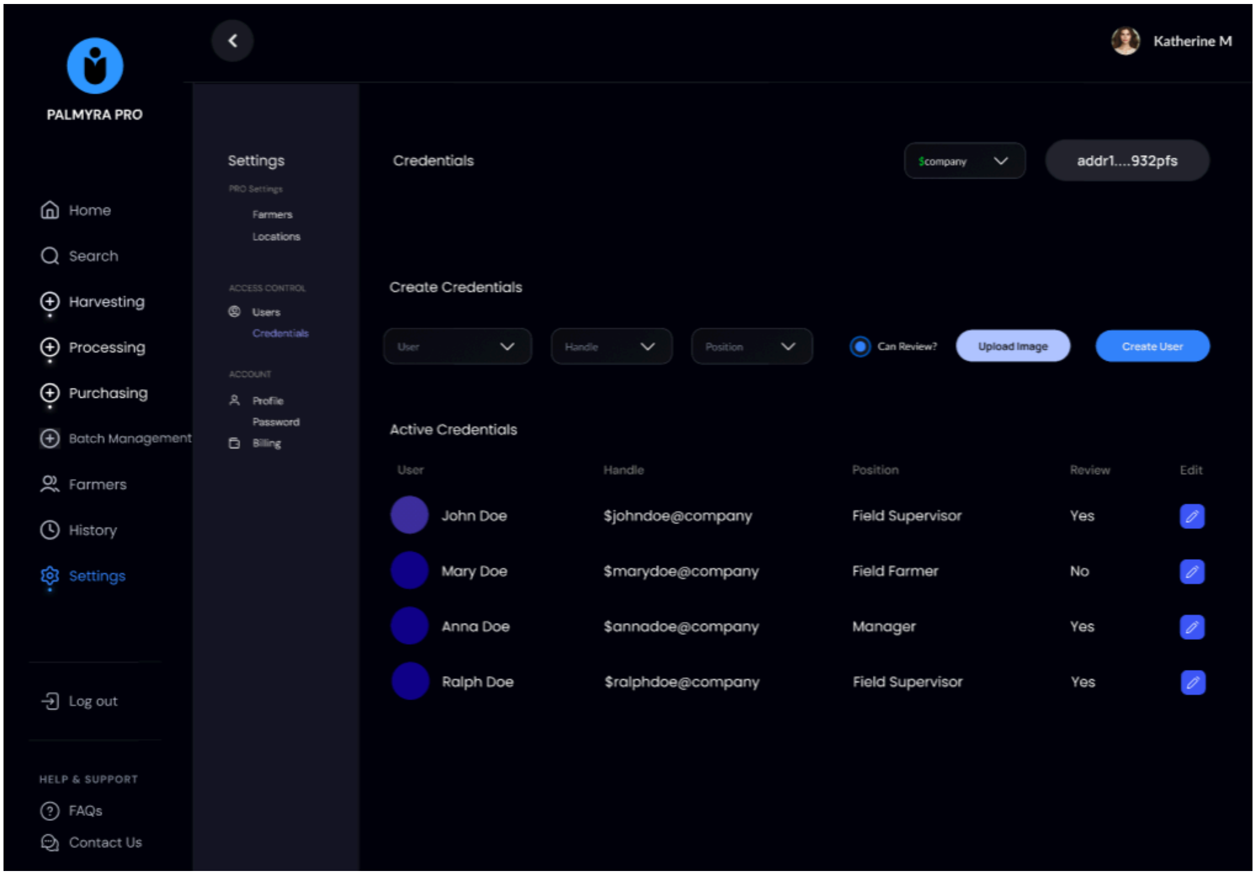
Assign Credentials Screen #1



Active Credentials

User	Handle	Position	Review	Edit
John Doe	$johndoe@company	Field Supervisor	Yes	✎
Mary Doe	$marydoe@company	Field Farmer	No	✎
Anna Doe	$annadoe@company	Manager	Yes	✎
Ralph Doe	$ralphdoe@company	Field Supervisor	Yes	✎

Assign Credentials Screen #2



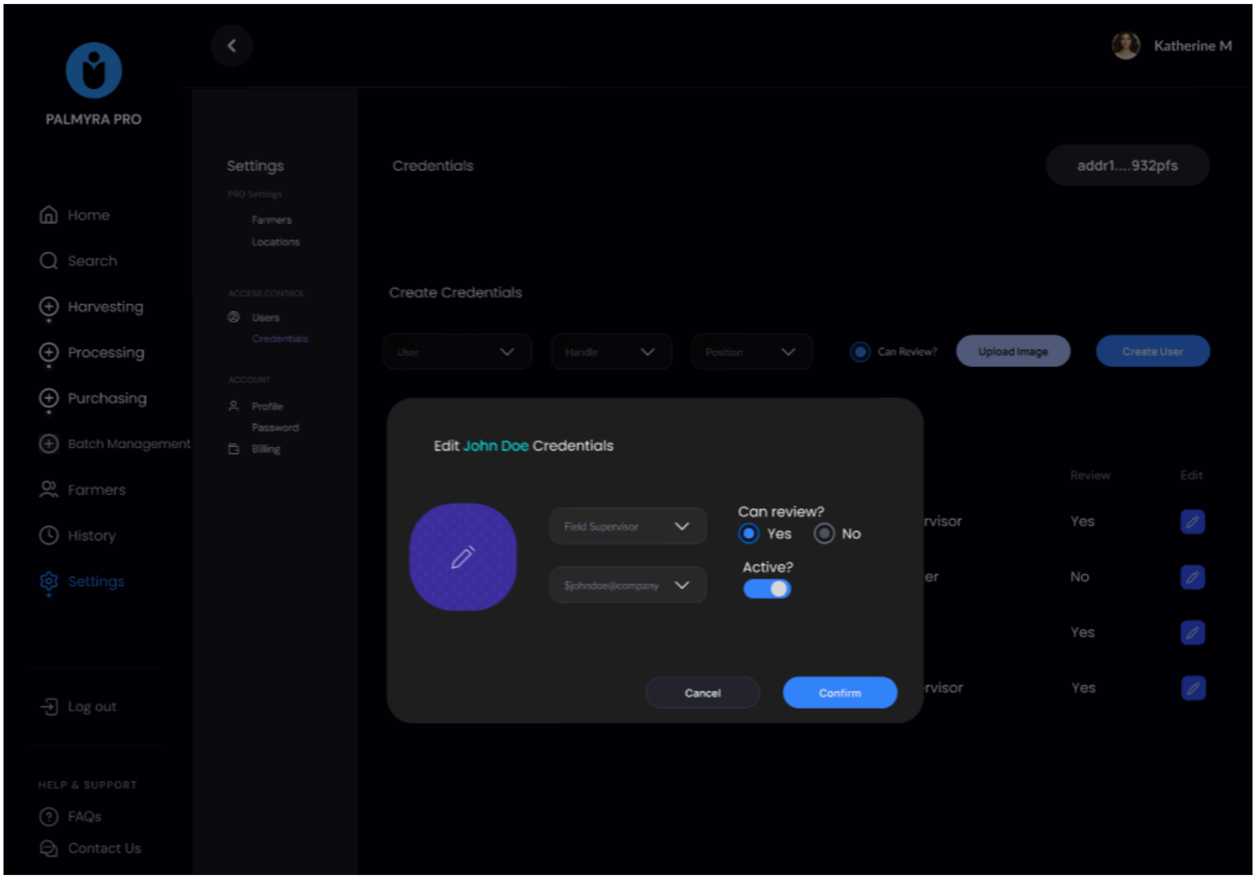
Credentials

Create Credentials

Active Credentials

User	Handle	Position	Review	Edit
John Doe	$johndoe@company	Field Supervisor	Yes	✎
Mary Doe	$marydoe@company	Field Farmer	No	✎
Anna Doe	$annadoe@company	Manager	Yes	✎
Ralph Doe	$ralphdoe@company	Field Supervisor	Yes	✎

Assign Credentials Screen #3



Edit John Doe Credentials

Field Supervisor

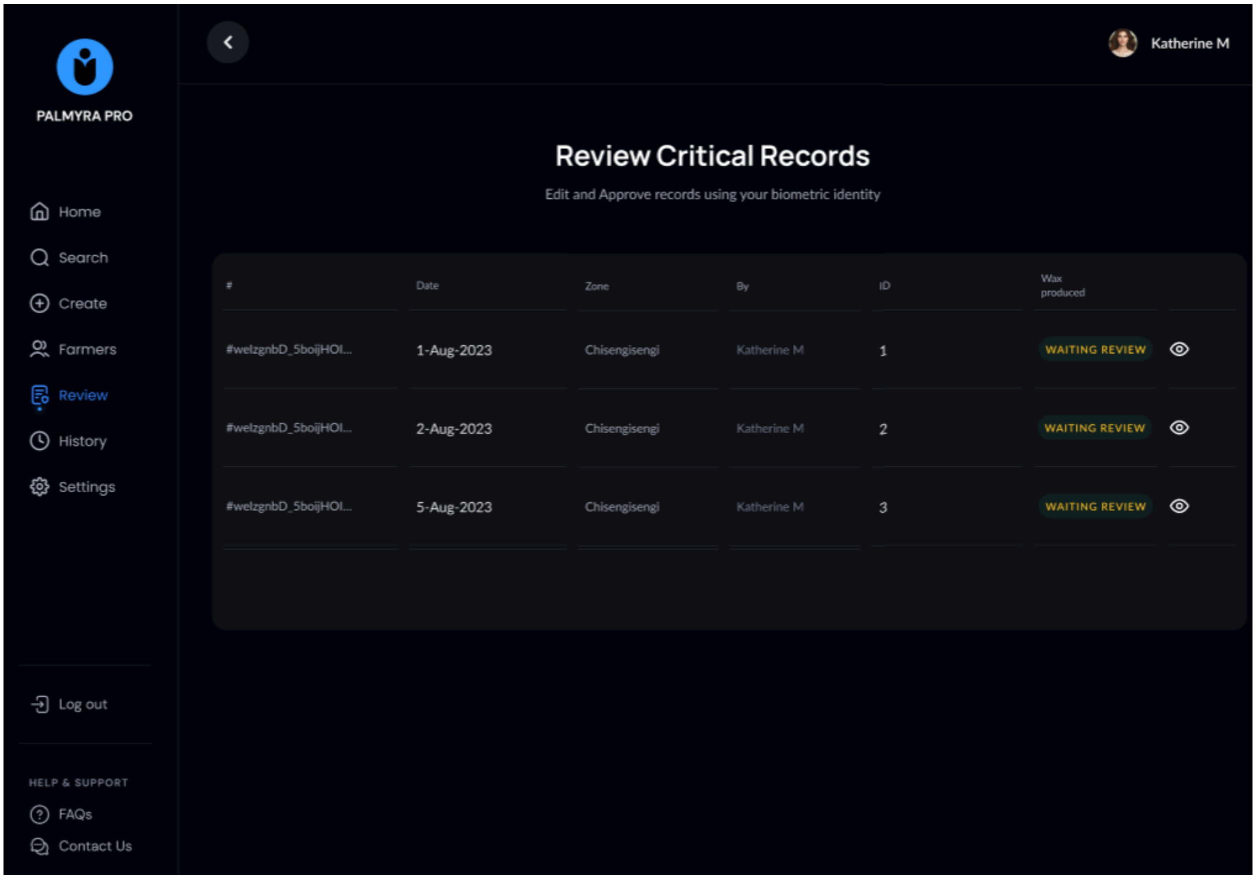
$johndoe@company

Can review?
● Yes ○ No

Active? ●

	Review
rvisor	Yes
er	No
	Yes
rvisor	Yes

Review Records Screen #1

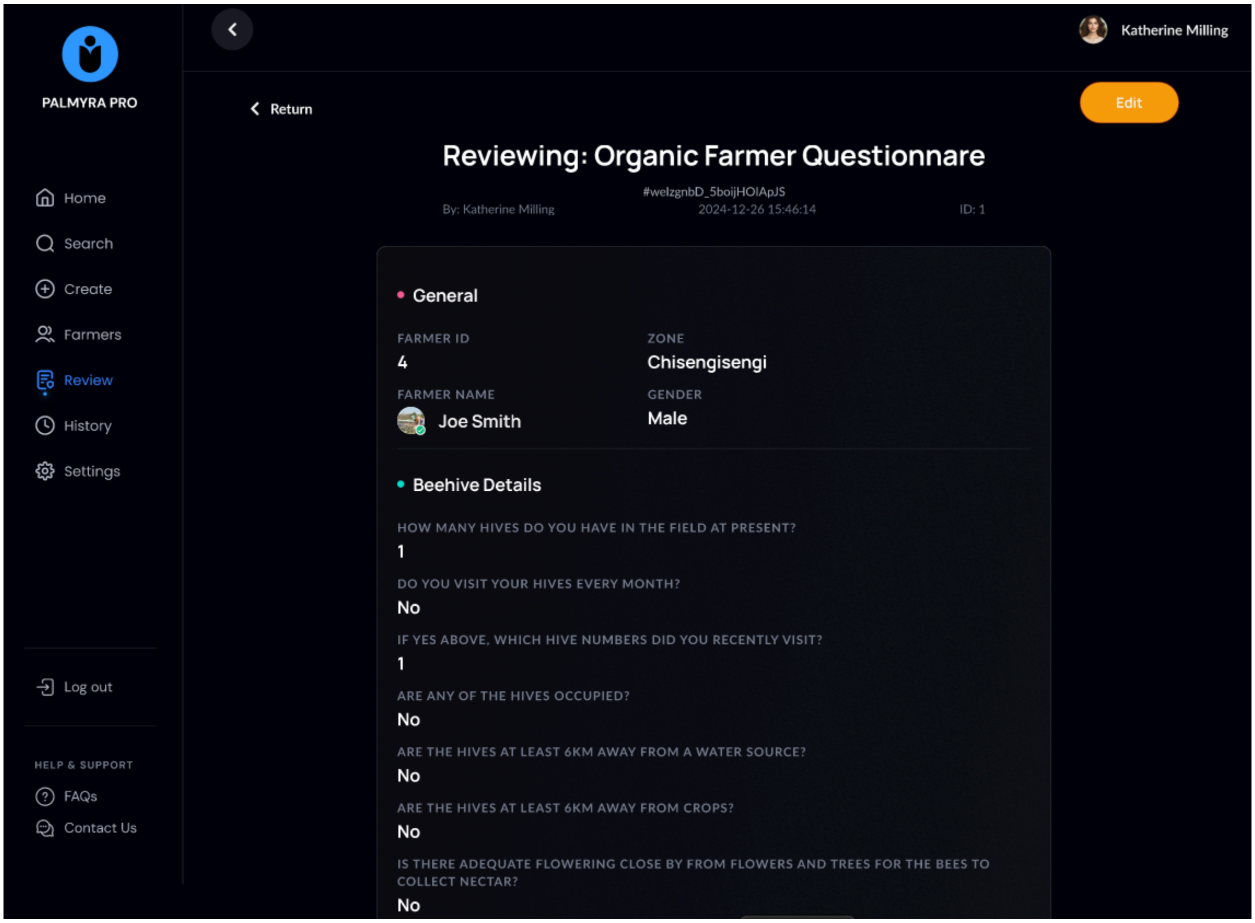


Review Critical Records

Edit and Approve records using your biometric identity

#	Date	Zone	By	ID	Wax produced	
#welzgnbD_5boijHOI...	1-Aug-2023	Chisengisengi	Katherine M	1	WAITING REVIEW	👁
#welzgnbD_5boijHOI...	2-Aug-2023	Chisengisengi	Katherine M	2	WAITING REVIEW	👁
#welzgnbD_5boijHOI...	5-Aug-2023	Chisengisengi	Katherine M	3	WAITING REVIEW	👁

Review Screen #2



Reviewing: Organic Farmer Questionnare

#welzgnbD_5boijHOIApJS

By: Katherine Milling 2024-12-26 15:46:14 ID: 1

General

FARMER ID
4

ZONE
Chisengisengi

FARMER NAME
Joe Smith

GENDER
Male

Beehive Details

HOW MANY HIVES DO YOU HAVE IN THE FIELD AT PRESENT?
1

DO YOU VISIT YOUR HIVES EVERY MONTH?
No

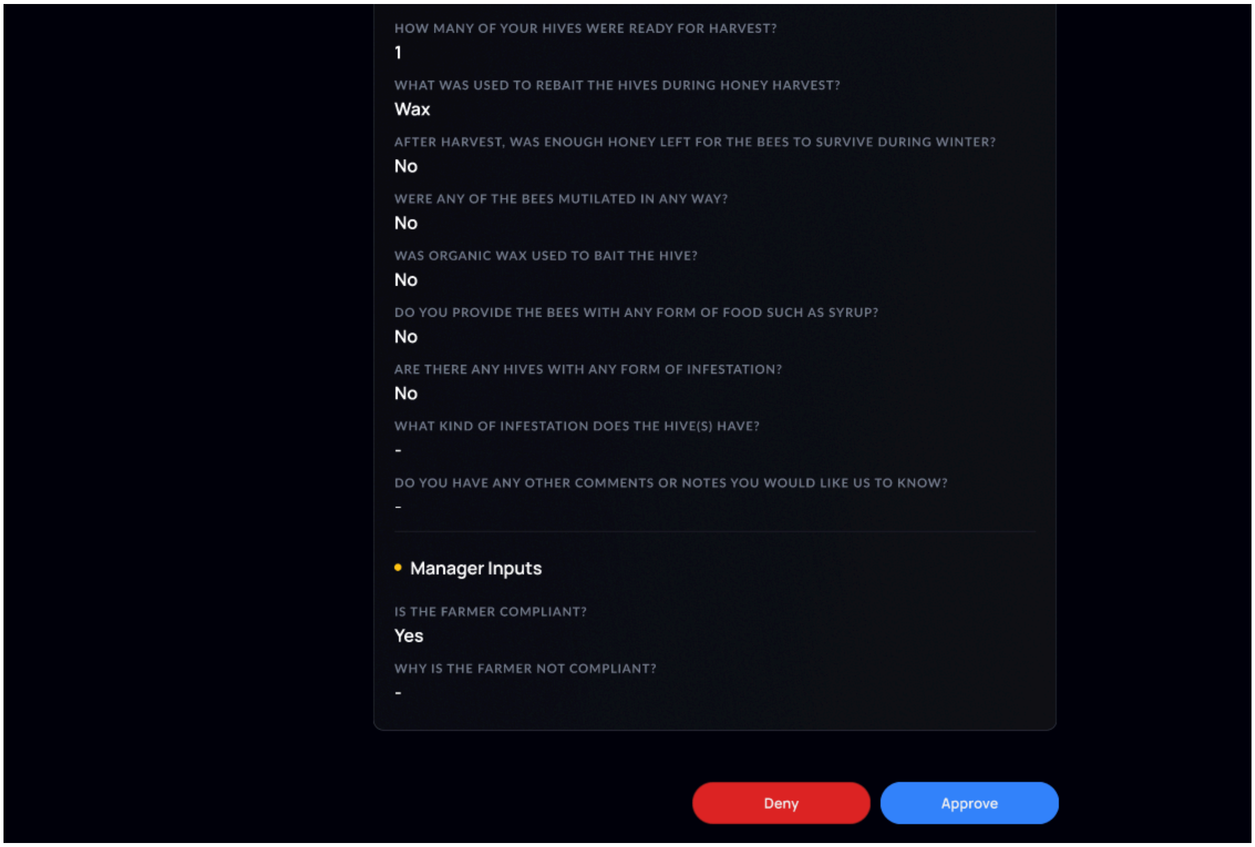
IF YES ABOVE, WHICH HIVE NUMBERS DID YOU RECENTLY VISIT?
1

ARE ANY OF THE HIVES OCCUPIED?
No

ARE THE HIVES AT LEAST 6KM AWAY FROM A WATER SOURCE?
No

ARE THE HIVES AT LEAST 6KM AWAY FROM CROPS?
No

IS THERE ADEQUATE FLOWERING CLOSE BY FROM FLOWERS AND TREES FOR THE BEES TO COLLECT NECTAR?
No



HOW MANY OF YOUR HIVES WERE READY FOR HARVEST?

1

WHAT WAS USED TO REBAIT THE HIVES DURING HONEY HARVEST?

Wax

AFTER HARVEST, WAS ENOUGH HONEY LEFT FOR THE BEES TO SURVIVE DURING WINTER?

No

WERE ANY OF THE BEES MUTILATED IN ANY WAY?

No

WAS ORGANIC WAX USED TO BAIT THE HIVE?

No

DO YOU PROVIDE THE BEES WITH ANY FORM OF FOOD SUCH AS SYRUP?

No

ARE THERE ANY HIVES WITH ANY FORM OF INFESTATION?

No

WHAT KIND OF INFESTATION DOES THE HIVE(S) HAVE?

-

DO YOU HAVE ANY OTHER COMMENTS OR NOTES YOU WOULD LIKE US TO KNOW?

-

Manager Inputs

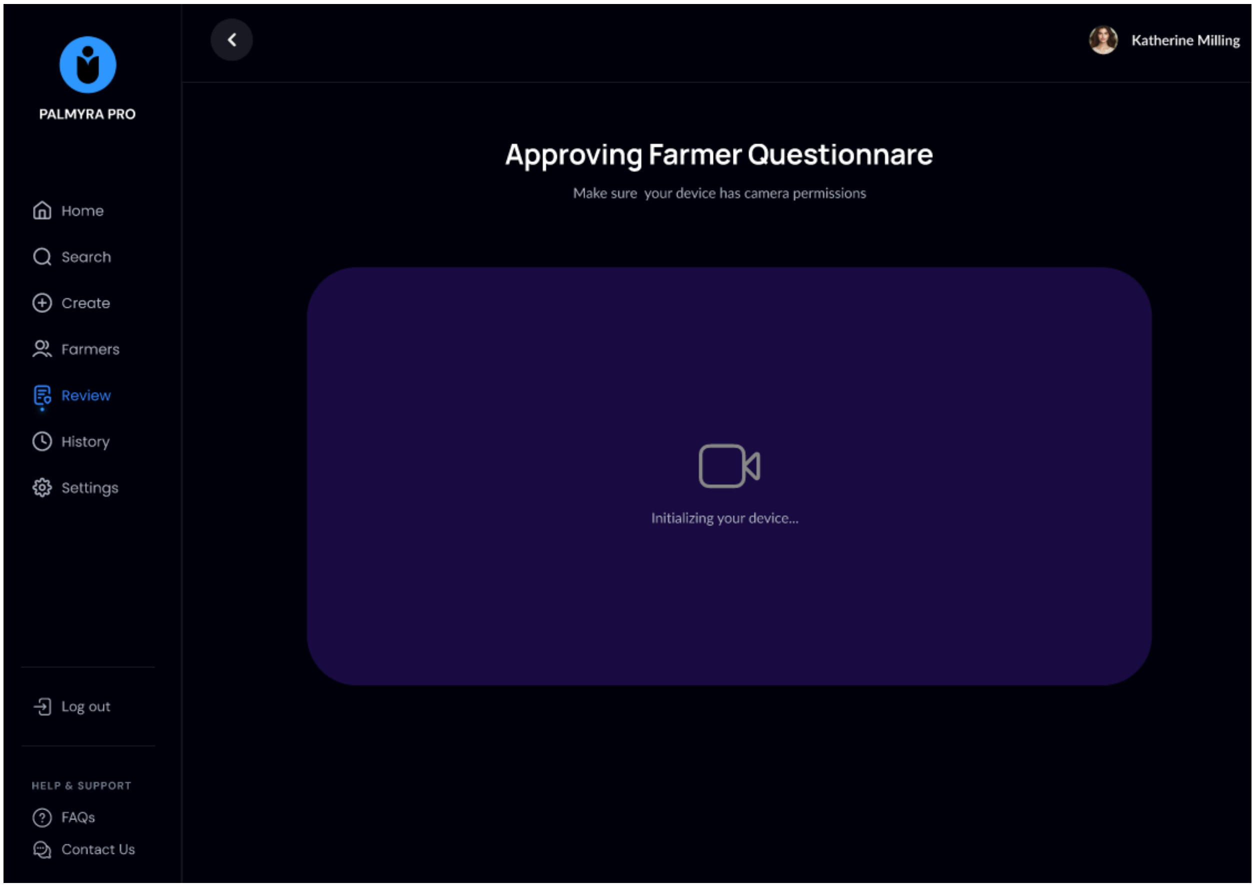
IS THE FARMER COMPLIANT?

Yes

WHY IS THE FARMER NOT COMPLIANT?

-

Review Screen #3

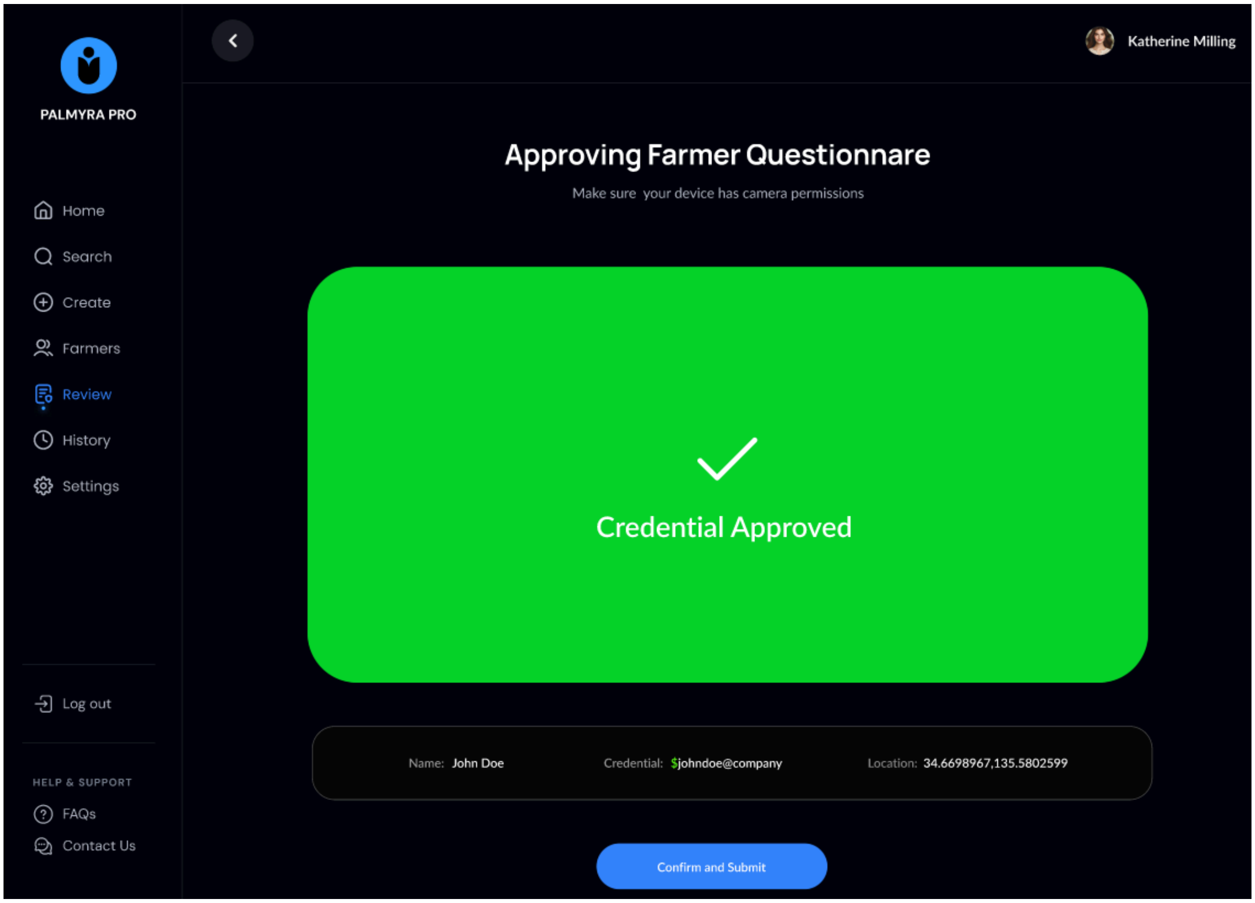


Approving Farmer Questionnare

Make sure your device has camera permissions

Initializing your device...

Review Screen #4



Approving Farmer Questionnare

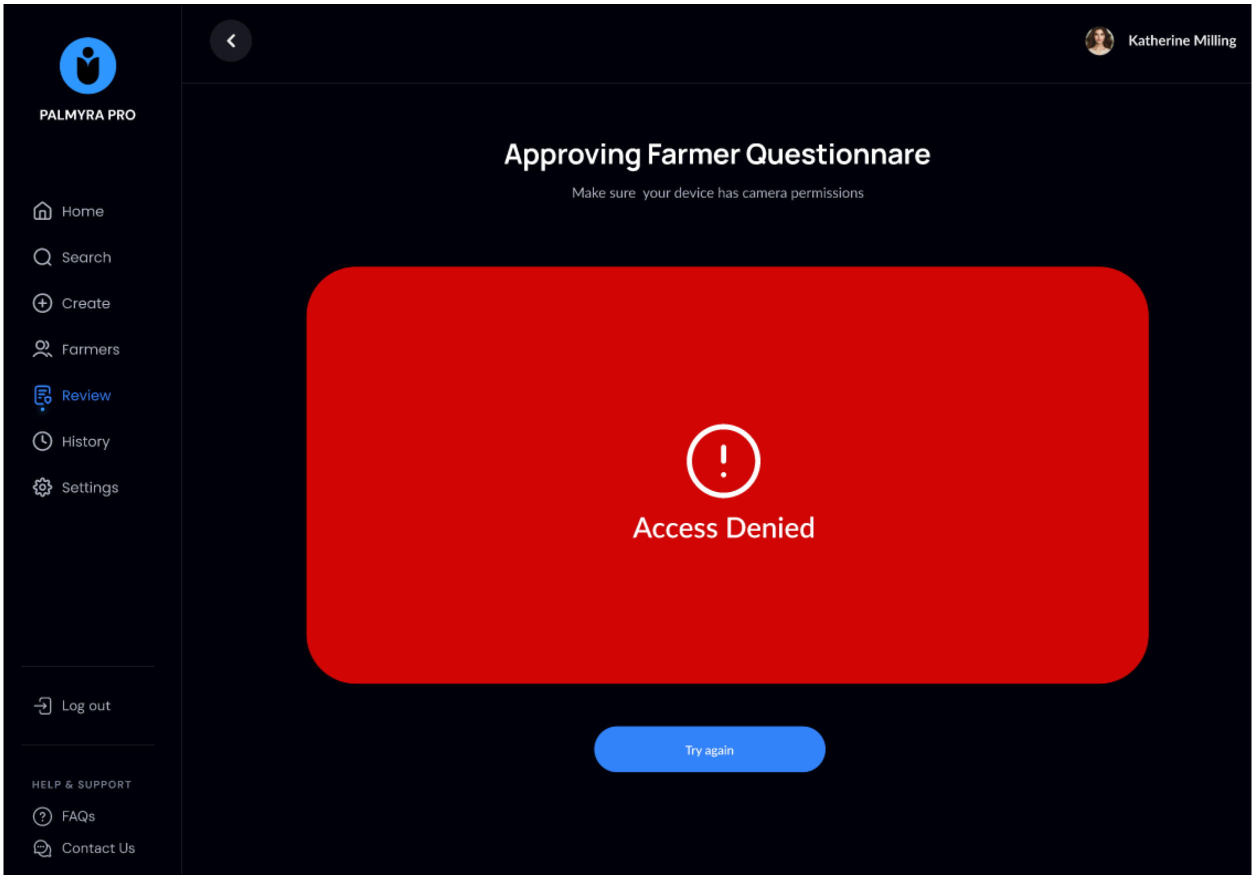
Make sure your device has camera permissions

✓

Credential Approved

Name: John Doe   Credential: $johndoe@company   Location: 34.6698967,135.5802599

Review Screen #5



Approving Farmer Questionnare

Make sure your device has camera permissions

Access Denied