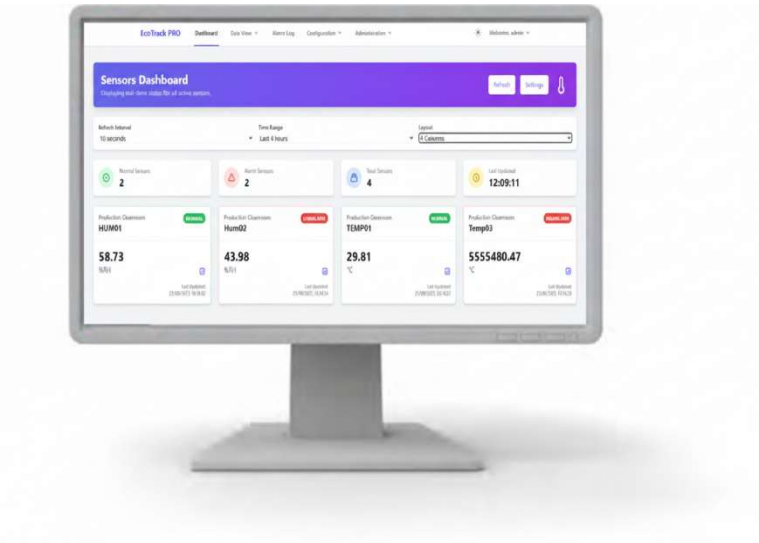
User Guide

ECOTrack Pro+

Version 1.0



"WHERE PRECISION MEETS RELIABILITY"

4D Solutions

ECOTrack PRO+ Monitoring System
User Manual

Document Version: 1.0

Document Number: EMS-UM-001

Issue Date: September 26, 2025

Classification: Controlled Document - For Pharmaceutical Use

System Version: Enterprise Edition

Software Version: 1.0

Platform: Docker Containerized Application with Windows Service

Prepared by: 4D Solutions

Reviewed by: Quality Assurance Department

Approved by: Regulatory Affairs Director

Document Control:

- This document has been prepared in compliance with 21 CFR Part 11, ISO 14644-1, and pharmaceutical GMP requirements
- All system users must be trained on this manual before system access
- This document is subject to change control procedures per SOP-QA-007
- Current version available in Document Management System

2. Table of Contents

12. Appendices
    1. Appendix A: System Specifications
    2. Appendix B: Configuration Templates
    3. Appendix C: Training Checklists
    4. Appendix D: Change Control Forms

3. Introduction

3.1 Purpose and Scope

The Environmental Monitoring System (EMS) is a comprehensive, enterprise-grade solution designed to provide real-time monitoring, data logging, and alarming for critical environmental parameters in pharmaceutical, biotechnology, and medical device manufacturing environments. This system ensures compliance with Good Manufacturing Practices (GMP) and regulatory requirements by providing validated, secure, and reliable environmental monitoring capabilities.

Primary Functions:

- Real-time monitoring of temperature, humidity, particulate matter, and other critical environmental parameters
- Continuous data logging with timestamp and validation
- Configurable alarm thresholds and notification systems
- Comprehensive audit trail for all system activities
- Electronic signature capabilities for data integrity
- Automated backup and data retention management
- Statistical analysis and reporting capabilities

This manual provides detailed instructions for system administrators, operators, and quality assurance personnel responsible for the operation, maintenance, and validation of the Environmental Monitoring System.

3.2 System Compliance and Regulatory Standards

The Environmental Monitoring System has been designed and validated to meet the following regulatory requirements and standards:

21 CFR Part 11 - Electronic Records; Electronic Signatures:

- Secure, computer-resident, and computer-generated records with equivalent probative value to paper records
- Electronic signatures with verification controls
- Audit trails for system activities
- Access controls and security measures

ISO 14644-1 - Classification of Air Cleanliness by Particle Concentration:

- Particle monitoring capabilities for cleanroom environments
- Data collection and reporting in accordance with ISO standards
- Calibration and validation requirements for monitoring equipment

Pharmaceutical Industry Standards:

- FDA Current Good Manufacturing Practice (cGMP)
- EU GMP Annex 1 - Manufacture of Sterile Medicinal Products
- PIC/S Guide to Good Manufacturing Practice
- ICH Q9 Quality Risk Management

System Validation Requirements:

- Installation Qualification (IQ)
- Operational Qualification (OQ)
- Performance Qualification (PQ)
- Risk-based approach to validation activities

3.3 Document Organization

This user manual is organized to provide comprehensive guidance for all aspects of Environmental Monitoring System operation. Each section addresses specific operational areas with detailed procedures, safety information, and compliance requirements. Users should familiarize themselves with all relevant sections before operating the system.

The manual includes step-by-step procedures with numbered instructions, tables for configuration parameters, and image placeholders for visual aids that support understanding and proper system operation in a pharmaceutical environment.

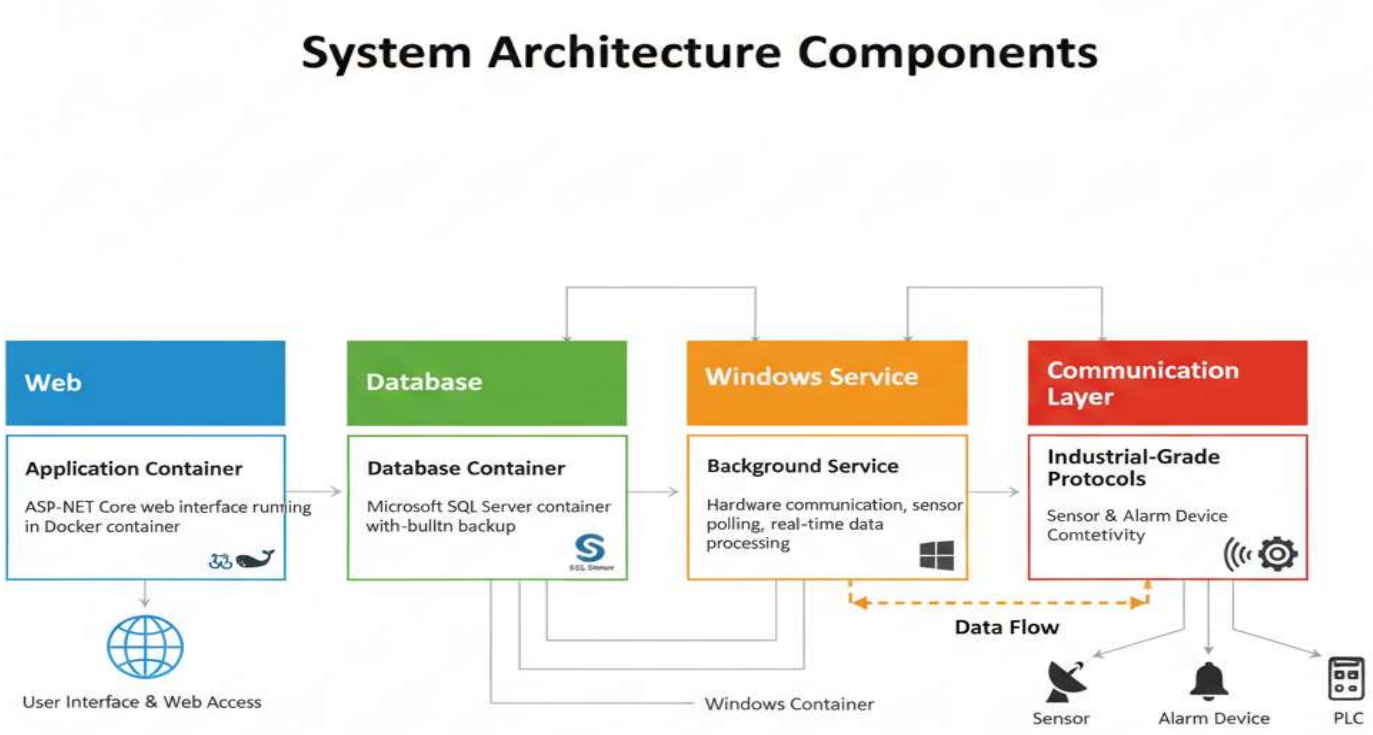
4. System Overview

4.1 System Architecture

The Environmental Monitoring System utilizes a hybrid architecture combining the robustness of Docker containerization with the hardware access capabilities of Windows Services. This architecture ensures both reliable operation and direct hardware connectivity required for industrial monitoring applications.

Core Architecture Components:

1. **Web Application Container**: ASP.NET Core web interface running in Docker container, providing user interface and web-based access to system functions
2. **Database Container**: Microsoft SQL Server container managing all application data with built-in backup capabilities
3. **Windows Service**: Background service responsible for hardware communication, sensor polling, and real-time data processing
4. **Communication Layer**: Industrial-grade communication protocols for sensor and alarm device connectivity



Data Flow Architecture:

The system employs a resilient data processing pipeline:
- Sensors send data to the Windows Service via industrial communication protocols
- The Service processes, validates, and stores data in the database
- The Web Application provides real-time visualization and reporting
- Alarm systems are triggered based on configurable thresholds

4.2 Core Components

Environmental Monitoring Service (EMS):

- Runs as a Windows Service ensuring continuous operation
- Communicates with industrial sensors and data acquisition modules
- Processes sensor data with configurable scaling and offset calculations
- Manages alarm logic with configurable delay and escalation features

Web Application Interface:

- Real-time dashboard with sensor status visualization
- Historical data analysis and trending capabilities
- Comprehensive reporting with PDF export functionality
- User management and role-based access control
- Licensing validation and management

Database System:

- Microsoft SQL Server database with comprehensive data retention
- Audit trail tracking all system activities
- Electronic signature integration for data integrity
- Automated backup and recovery capabilities

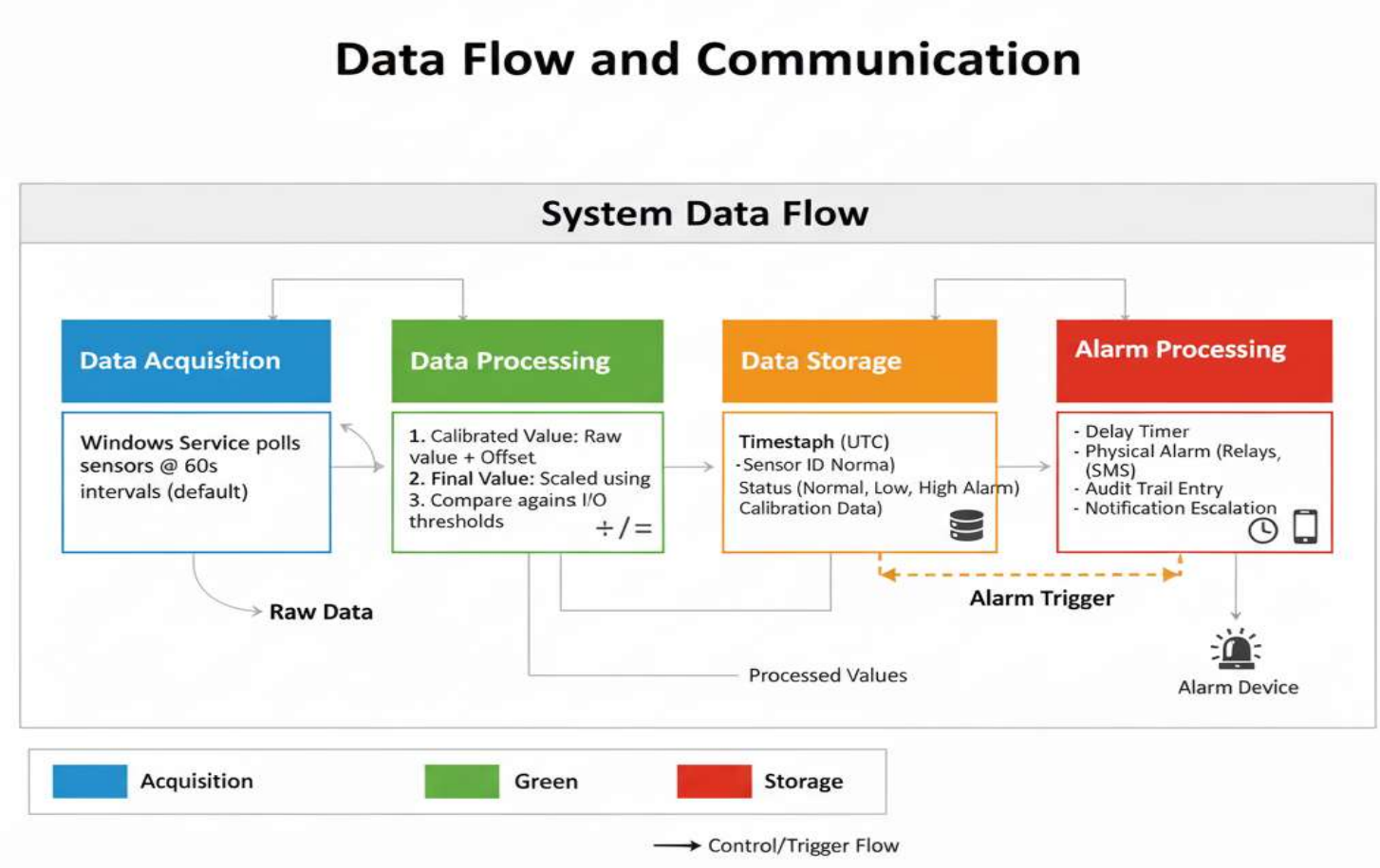
Communication Infrastructure:

- Support for ADAM-4000 series industrial I/O modules
- Modbus RTU communication protocol implementation
- Configurable serial port settings (COM5, COM4 by default)
- Resilient communication with automatic retry mechanisms

4.3 Data Flow and Communication

The system's data flow follows a structured process ensuring data integrity and reliability:

1. **Data Acquisition**: The Windows Service polls sensors at configurable intervals (default: 60 seconds)
2. **Data Processing**: Raw sensor values undergo scaling and offset calculations:
   - Raw value + Offset = Calibrated value
   - Calibrated value is scaled using input/output ranges
   - Final value is compared against alarm thresholds
3. **Data Storage**: Processed values are stored in the database with:
   - Timestamp (UTC)
   - Sensor identification
   - Status (Normal, Low Alarm, High Alarm)
   - Calibration data
4. **Alarm Processing**: Values outside threshold ranges trigger:
   - Alarm delay timer based on sensor configuration
   - Physical alarm device activation (relays, SMS)
   - Audit trail entry
   - Notification escalation based on time intervals



4.4 Hardware Integration

The system supports integration with industrial hardware components through the ADAM-4000 series protocol:

Supported Hardware Types:

- Analog Input Modules: ADAM-4015, ADAM-4017, ADAM-4018
- Relay Output Modules: ADAM-4060, ADAM-4068
- Temperature/Humidity Modules: ADAM-4013, ADAM-4014

Communication Protocol:

- RS-485 serial communication
- Modbus RTU protocol implementation
- Configurable baud rates (9600, 19200, 38400, etc.)
- Hardware addressing through slave ID configuration

Hardware Configuration Requirements:

- COM port availability (default: COM5 for ADAM modules)
- Proper grounding and electrical isolation
- Communication cable specifications as per industrial standards
- Module power supply requirements

5. Installation Instructions

5.1 System Prerequisites

Hardware Requirements:

- Windows Server 2019/2022 or Windows 10/11
- Minimum 8 GB RAM (16 GB recommended for high sensor count)
- Minimum 50 GB available disk space
- Available serial ports for ADAM module communication (COM5, COM4)
- Network connectivity for system updates and remote monitoring

Software Prerequisites:

1. Docker Desktop (version 20.10 or higher)
2. .NET 9.0 Runtime
3. Microsoft SQL Server (Express or higher) - if installing Windows Service
4. Administrative privileges for service installation
5. PowerShell 5.1 or higher

Network Requirements:

- TCP ports 8080 (Web Application) and 1433 (Database) available
- Outbound internet access for system updates (optional)
- Local network access for hardware device communication

5.2 Docker Installation Requirements

Step 1: Install Docker Desktop

1. Download Docker Desktop from the official website
2. Run the installer with administrative privileges
3. Follow the installation wizard with default settings
4. Restart the system after installation completes
5. Verify Docker is running: docker --version

Step 2: Configure Docker Resources

1. Open Docker Desktop settings
2. Allocate minimum 4GB RAM and 2 CPU cores to Docker
3. Configure secure file sharing for the project directory
4. Enable experimental features if required by system configuration

5.3 Windows Service Installation

Step 1: Database Setup

1. Ensure SQL Server is installed and running
2. Set database password in .env file:
   DB_PASSWORD=YourStrongPassword123!
3. Start the database container:
   docker-compose -f docker-compose-deploy.yml up -d db

4. Wait for the database to be ready (check with docker logs env-monitoring-db)

Step 2: Build Windows Service

1. Open PowerShell as Administrator
2. Navigate to the EnvironmentalMonitoring.Service directory
3. Build and publish the service:
   cd EnvironmentalMonitoring.Service
   .\deploy.ps1 -Configuration Release -OutputPath "..\publish" -SkipBuild:$false

Step 3: Configure Windows Service

1. Navigate to the publish directory:
   cd ..\publish
2. Edit appsettings.json to match your environment:
   - Update connection string to point to your SQL Server instance
   - Configure hardware ports (COM5, COM4, etc.)
   - Adjust other settings as needed

Step 4: Install Windows Service

1. Run the installation script:
   cd ..\EnvironmentalMonitoring.Service
   .\install-service.ps1 -BinaryPath "..\publish\EnvironmentalMonitoring.Service.exe"
2. Configure service recovery options:
   sc.exe failure EnvironmentalMonitoringService reset= 86400 actions= restart/60000/restart/60000/restart/60000

Step 5: Start Windows Service

1. Start the service:
   .\install-service.ps1 -Start

5.4 Database Configuration

Database Connection Settings:
The system uses Microsoft SQL Server for data storage. Configure the connection string in the appsettings.json file:

```
{
  "ConnectionStrings": {
    "DefaultConnection": "Server=localhost;Database=EnvMonitoring;User Id=EnvMonitorUser;Password=YourStrongPassword123!;TrustServerCertificate=True"
  }
}
```

Database Security:

1. Create a dedicated service account for the application
2. Grant minimal required permissions:
   - db_datareader
   - db_datawriter
   - db_ddladmin (for migrations only)
3. Implement strong password policies
4. Enable SQL Server authentication (Windows Authentication also supported)

5.5 Initial Setup Wizard

Step 1: Access the Web Application

1. Open a web browser and navigate to: http://<your-server-ip>:8080
2. The system will redirect to the License Management page if no valid license is installed

Step 2: Apply License Key

1. Generate license key using LicenseGenerator.Console tool
2. Copy the entire license key string
3. Paste the license key into the text area on the License Management page
4. Click "Apply New License"

Step 3: Default Login

- **URL**: http://<your-server-ip>:8080
- **Default Username**: admin
- **Default Password**: admin123

Security Warning: Change the administrator password immediately after your first login.

Step 4: Initialize System

1. Log in with default credentials
2. Navigate to System Settings to configure:
   - Global logging interval (default: 60 seconds)
   - Alarm escalation settings
   - Email notification settings
   - Backup configuration

6. System Configuration

6.1 Network Configuration

Web Application Settings:
The system exposes the web interface on port 8080 by default. For security and operational requirements:

1. **Port Configuration:**
   - Default HTTP port: 8080
   - For production environments, consider using HTTPS with port 443
   - Configure firewall to allow access to port 8080 from authorized networks only
2. **SSL/HTTPS Configuration:**
   - Generate or obtain SSL certificate from trusted CA
   - Update Docker container configuration to redirect HTTP to HTTPS
   - Configure certificate in appsettings.json:

```
{
  "Kestrel": {
    "Endpoints": {
      "Https": {
        "Url": "https://*:443",
        "Certificate": {
          "Path": "path/to/certificate.pfx",
          "Password": "certificate_password"
        }
      }
    }
  }
}
```

Container Networking:

- Web application and database run in the same Docker network
- Communication between containers is secured by Docker's internal network
- Externally accessible only through configured ports

6.2 Hardware Connection Settings

ADAM Module Communication:
The system communicates with ADAM-4000 series modules through serial communication.

Configuration Parameters:

- **Port Name**: Default is COM5 for ADAM modules
- **Baud Rate**: 9600 (configurable up to 115200)
- **Data Bits**: 8
- **Parity**: None
- **Stop Bits**: One
- **Slave Address**: Unique identifier for each module (01-99)

Hardware Configuration in appsettings.json:

```
{
  "Hardware": {
    "AdamPortSettings": {
      "PortName": "COM5",
      "BaudRate": 9600,
      "DataBits": 8,
      "Parity": "None",
      "StopBits": "One"
    },
    "GsmPortSettings": {
      "PortName": "COM4",
      "BaudRate": 9600,
      "DataBits": 8,
      "Parity": "None",
      "StopBits": "One"
    }
  }
}
```

6.3 Data Module Configuration

Adding Data Modules:

1. Navigate to Data Modules in the system interface
2. Click "Add New Data Module"
3. Complete the configuration form:

Parameter	Description	Example Value
Module Name	Descriptive name for the module	"Temperature Room A"
Module Type	Type of module (Analog/Relay)	"Analog Input"
Slave Address	Communication address (1-99)	"01"

Validation Requirements:

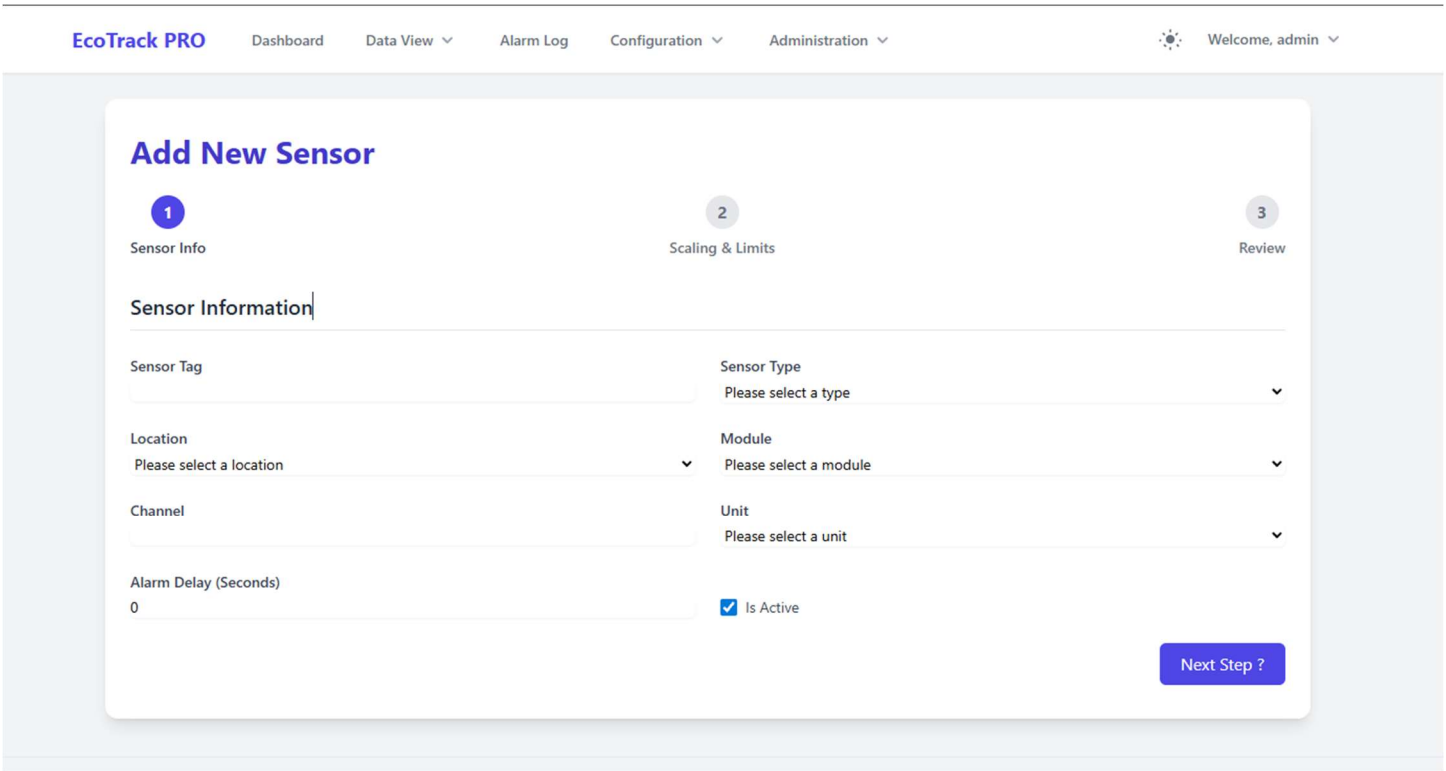
- Module Name must be unique
- Slave Address must be unique within each communication port
- Module Type must match the physical hardware capabilities

6.4 Sensor Configuration

Sensor Parameter Configuration:
Each sensor requires precise configuration for accurate data collection and scaling:

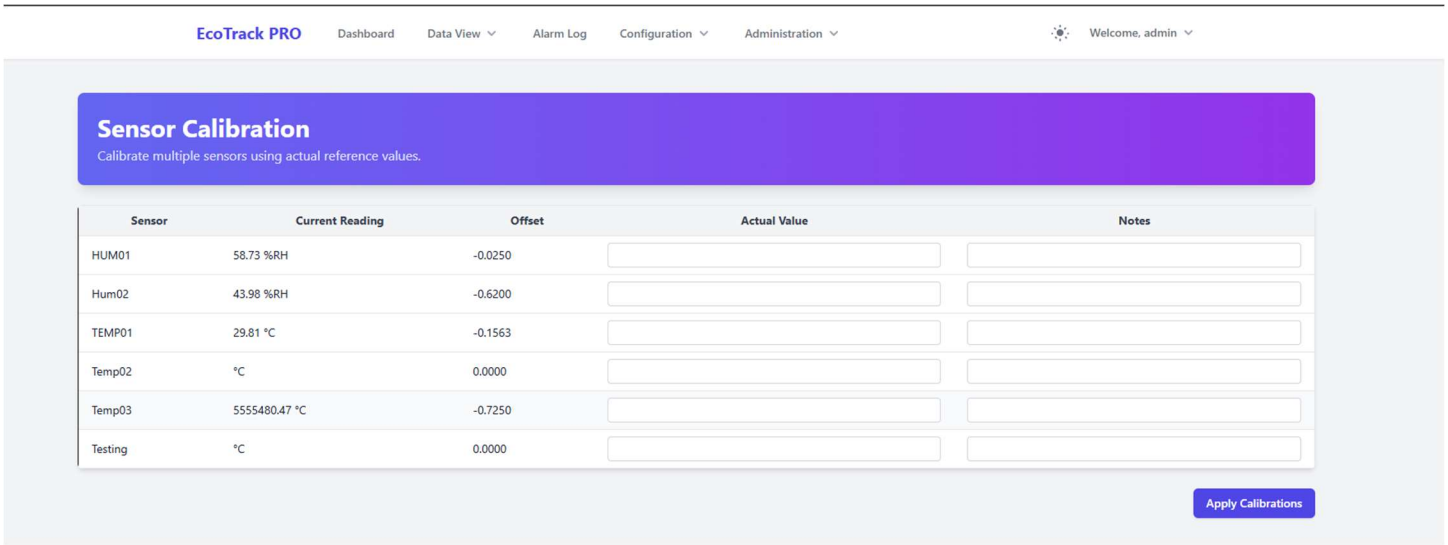
Basic Sensor Information:

1. **Data Module**: Select the associated data module
2. **Location**: Assign to a defined location
3. **Sensor Tag**: Unique identifier (e.g., "ROOMA_T1")
4. **Sensor Type**: Temperature, Humidity, Pressure, etc.
5. **Unit of Measure**: °C, %RH, PSI, etc.



Calibration Settings:

- **Input Range**: Raw signal range (e.g., 4-20mA, 0-10V)
  - Input Min: 4.0000
  - Input Max: 20.0000
- **Scale Range**: Engineering units (e.g., 0-50°C, 0-100%RH)
  - Scale Min: 0.0000
  - Scale Max: 50.0000
- **Offset Value**: Calibration offset (±999.9999)



Alarm Configuration:

- **Low Alarm Limit**: Lower threshold value
- **High Alarm Limit**: Upper threshold value
- **Alarm Delay**: Delay period in seconds before alarm triggers
- **Active Status**: Enable/disable the sensor

Hardware Address:

- For ADAM modules: Channel number (0-7 for 8-channel modules)
- Example: Channel 1 for ADAM-4017 module

6.5 Alarm Device Configuration

Supported Alarm Device Types:

1. **Relay Devices**: For physical relay activation
2. **SMS Devices**: For text message notifications

Relay Device Configuration:

1. **Device Name**: Descriptive name (e.g., "Red Light", "Horn")
2. **Device Type**: Set to "Relay"
3. **Hardware Address**: Channel number on the relay module
4. **Data Module**: Link to the appropriate relay module

SMS Device Configuration:

1. **Device Name**: Descriptive name (e.g., "Maintenance SMS", "Manager Alert")
2. **Device Type**: Set to "SMS"
3. **Hardware Address**: Phone number in international format
4. **Data Module**: Not required for SMS devices

Alarm Mapping:

1. Navigate to Alarm Mapping section
2. Link sensors to appropriate alarm devices
3. Multiple alarm devices can be mapped to a single sensor
4. Each sensor can be linked to multiple alarm devices

6.6 Calibration Settings

Calibration Process:
The system supports offset-based calibration for improved accuracy:

Calibration Parameters:

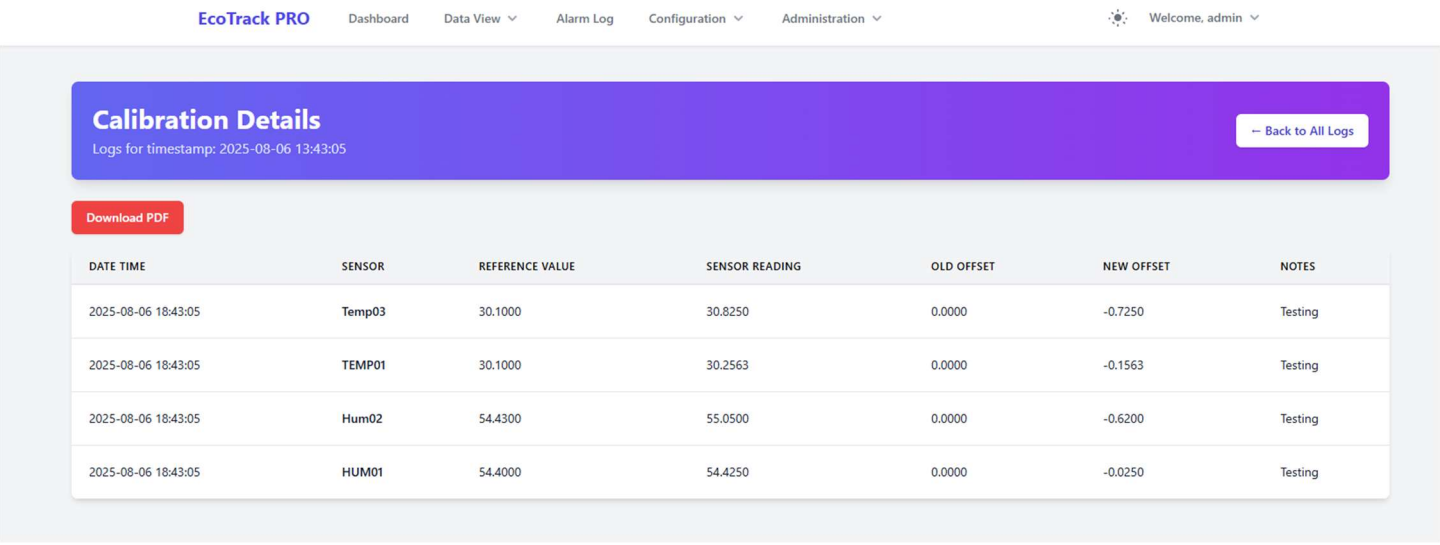
- **Reference Value**: Known accurate value from calibrated instrument
- **Uncalibrated Reading**: Raw value from the sensor
- **Old Offset**: Previous offset value
- **New Offset**: Calculated offset for accurate readings
- **Notes**: Documentation of calibration conditions

Calibration Workflow:

1. Enter Calibration Module from Sensor Management
2. Select the sensor for calibration
3. Enter reference value from calibrated source
4. System calculates new offset automatically
5. Apply offset and document calibration in audit trail

Calibration Validation:

- All calibration changes are audited
- Electronic signatures required for calibration approval
- Historical calibration data maintained for trending
- Calibration certificates can be generated and exported



7. User Roles & Permissions

7.1 Role-Based Access Control

The Environmental Monitoring System implements a comprehensive role-based access control (RBAC) system to ensure appropriate access levels for different user categories. The system includes three primary roles with distinct permission sets:

Administrator Role:

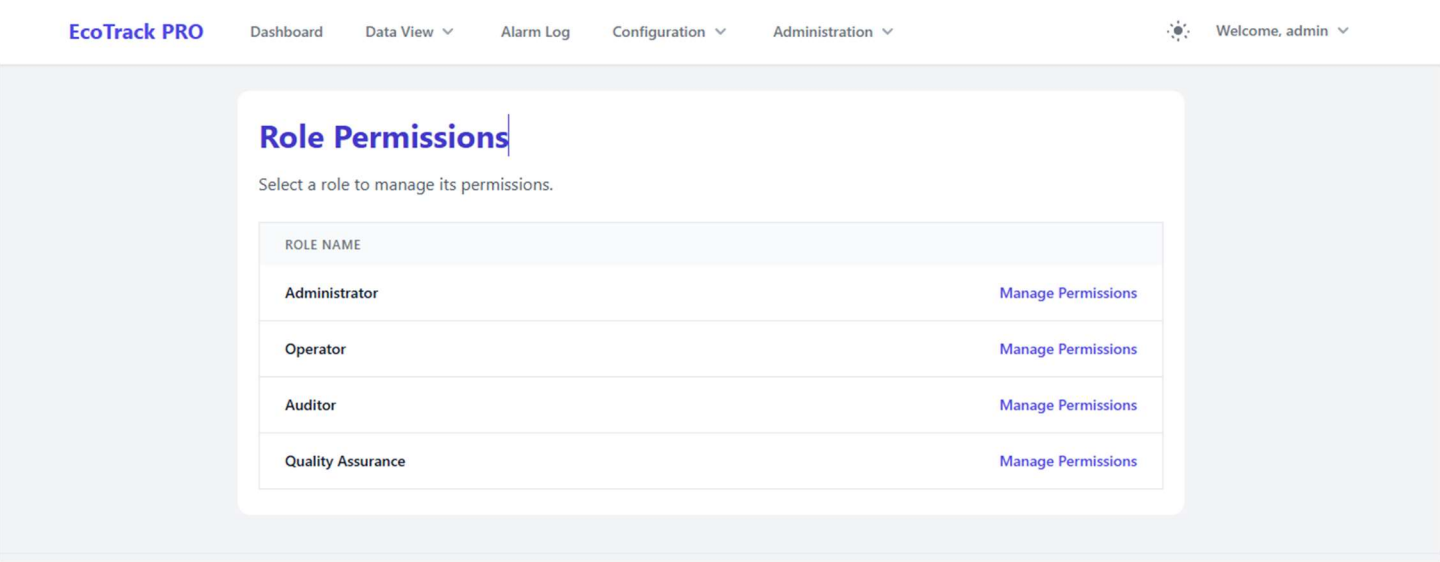
- Complete system access including configuration, user management, and system maintenance
- Ability to create, modify, and delete all system components (sensors, locations, users, etc.)
- Access to system settings and licensing management
- Full audit trail review capabilities
- Electronic signature authority for critical processes

Operator Role:

- Real-time monitoring and dashboard access
- Ability to acknowledge and resolve alarms
- Access to view and export reports
- Limited configuration access as designated by administrators
- Data verification and basic documentation functions

Auditor Role:

- Read-only access to historical data and reports
- Audit trail access for review and compliance activities
- Report generation capabilities
- No modification rights to any system data or configuration
- Electronic signature access for validation activities only



7.2 User Registration and Management

Creating New Users:

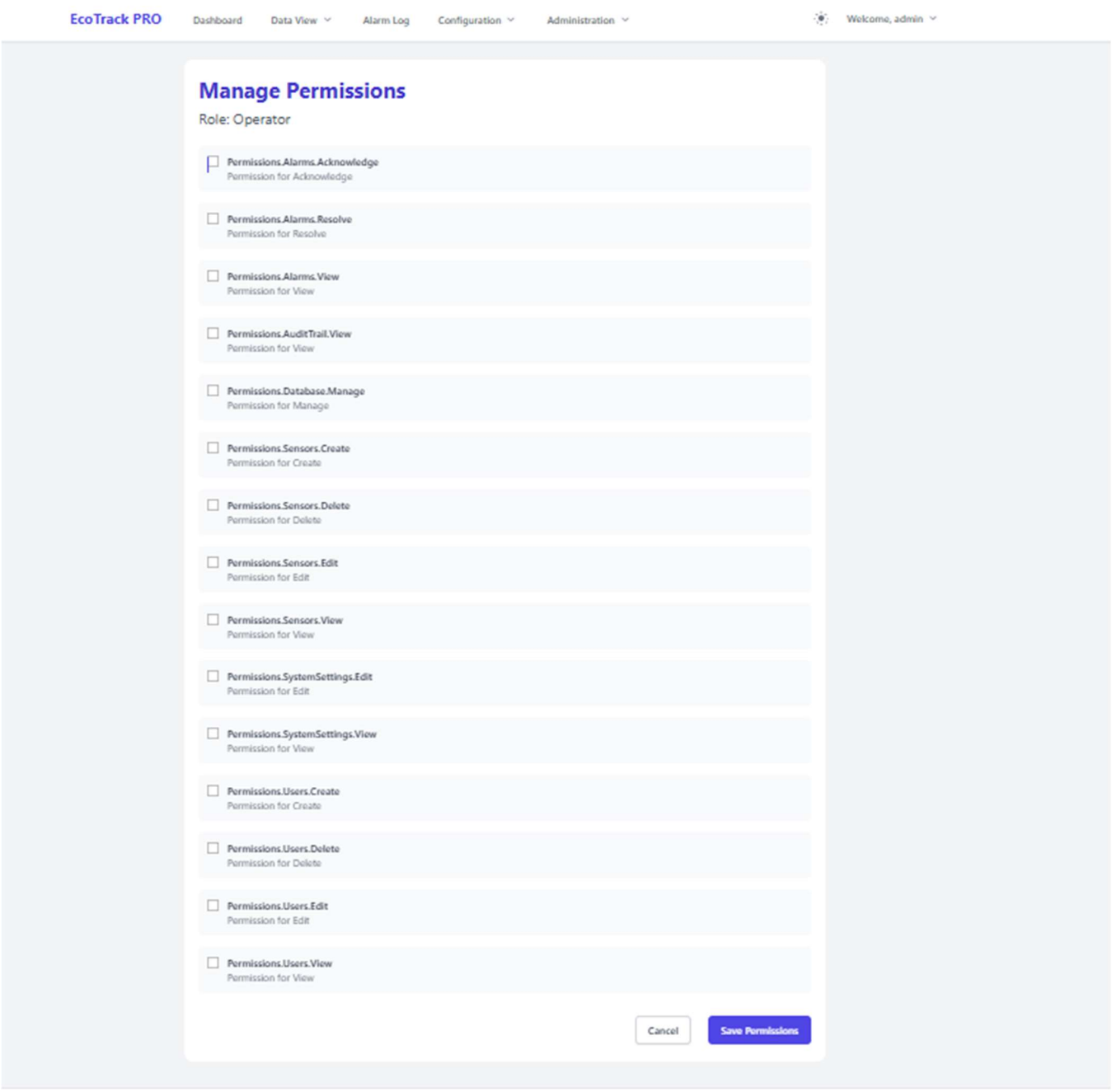
1. Log in with Administrator credentials
2. Navigate to User Management section
3. Click "Add New User"
4. Complete the user registration form:

Required User Information:

- **Username**: Unique system identifier (minimum 4 characters)
- **Full Name**: Complete name for audit trail purposes
- **Email Address**: For notification delivery
- **Initial Password**: Must meet complexity requirements
- **Active Status**: Enable/disable account access
- **Assigned Roles**: One or multiple roles based on job function

Password Requirements:

Permission	Administrator	Operator	Auditor
Dashboard Access	✓	✓	✓
View Sensors	✓	✓	✓
Create/Edit Sensors	✓	-	-
View Alarms	✓	✓	✓
Acknowledge Alarms	✓	✓	-
Resolve Alarms	✓	✓	-
View Reports	✓	✓	✓
Generate Reports	✓	✓	✓
Export Data	✓	✓	✓
User Management	✓	-	-
System Settings	✓	-	-
Audit Trail Access	✓	✓	✓
Sensor Calibration	✓	✓	-
Alarm Device Management	✓	-	-
Location Management	✓	-	-
Data Module Management	✓	-	-
License Management	✓	-	-
System Updates	✓	-	-



- Minimum 8 characters (4 characters for system default)
- No requirement for digits, symbols, or case variations (configurable)
- Password expiration policy (default: 90 days)
- History retention (last 5 passwords cannot be reused)

User Activation Process:

1. New users receive email notification with temporary access
2. Users must change their password on first login
3. System enforces immediate password change for security
4. Account remains active until deactivated by administrator

7.3 Permission Matrix

The system implements granular permissions organized by functional areas. The following table details permissions available to each role:

*Operators can perform calibration with proper authorization and electronic signature

Permission Configuration:

1. Navigate to Permissions Management
2. Select role to modify
3. Check/uncheck permissions as required
4. Save configuration - changes take effect immediately
5. All permission changes are recorded in audit trail

7.4 Audit Trail Requirements

Audit Trail Coverage:
All user activities are automatically logged in compliance with 21 CFR Part 11 requirements:

Mandatory Audit Events:

- User login and logout
- Data access and modification
- Alarm acknowledgment and resolution
- Configuration changes
- Report generation and export
- Electronic signatures
- System administration activities

Audit Trail Information:

- **User Information**: Username, full name, workstation ID
- **Event Type**: Specific action performed
- **Timestamp**: UTC timestamp with millisecond precision
- **Record Identification**: Object affected (sensor ID, etc.)
- **Before/After Values**: Data changes for traceability
- **Workstation ID**: Computer or device identifier

Audit Trail Access:

- Administrators have full access to all audit events
- Operators have access to their own activities and immediate work scope
- Auditors have read-only access to all audit events for compliance review
- Export capabilities for regulatory inspections

Electronic Signature Requirements:
For critical operations requiring additional verification:

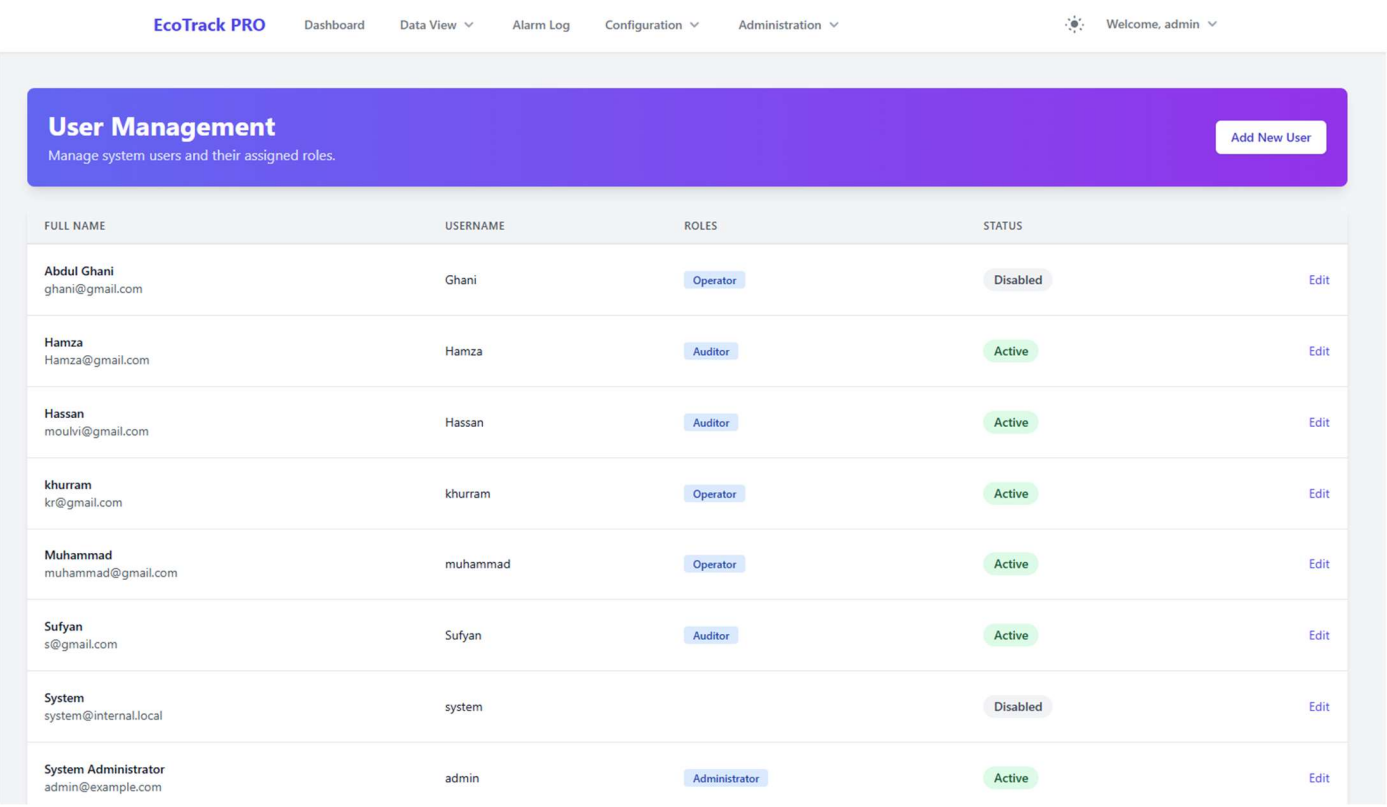
Signature Process:

1. User initiates electronic signature
2. System prompts for signature credentials
3. User enters password or uses two-factor authentication
4. System records signature with timestamp and user identity
5. Action is validated and processed

Signature Validity:

- Signatures are linked to specific user accounts
- All signature activities are recorded in audit trail
- Signature authority is role-dependent
- Signature expiration follows user session policies

[IMAGE: User Management Interface]

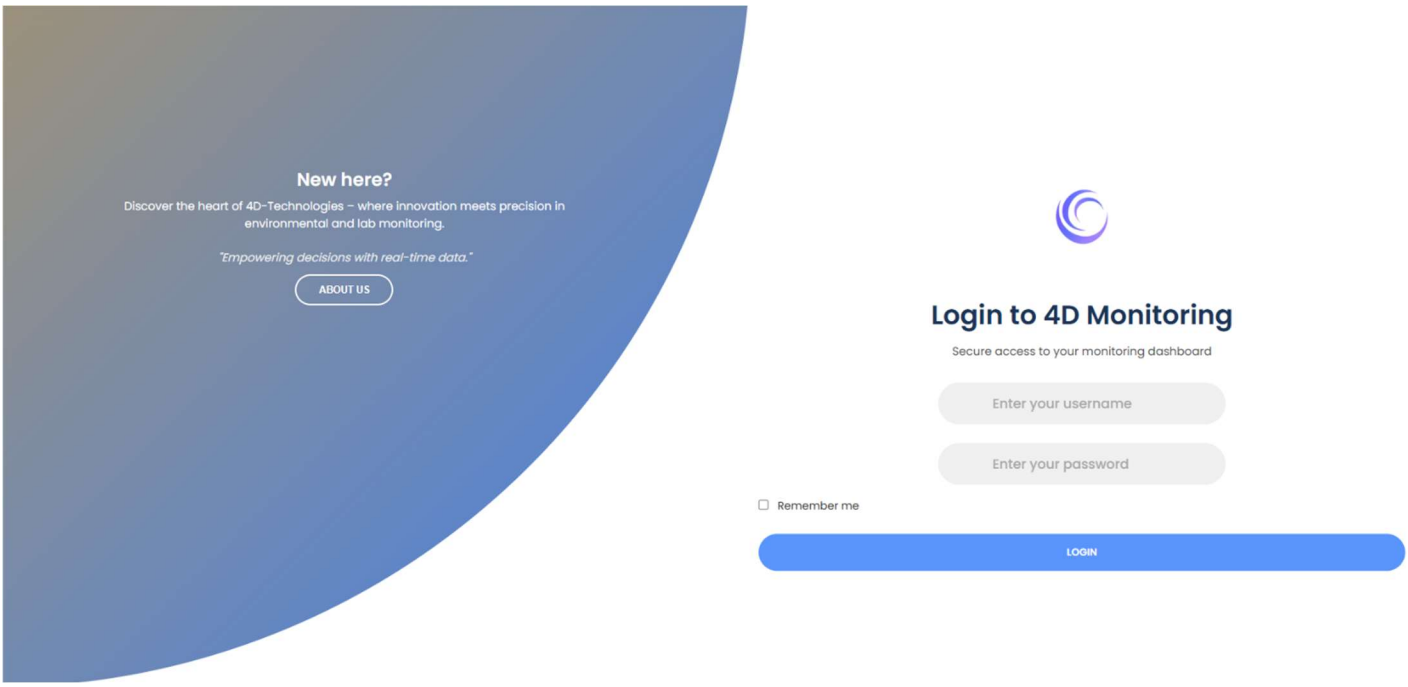


8. Operating Instructions

8.1 Login and Authentication

Standard Login Process:

1. Open a web browser and navigate to: http://<your-server-ip>:8080
2. Enter your username in the Username field
3. Enter your password in the Password field
4. Click the "Login" button
5. The system will redirect you to the dashboard if credentials are valid



Security Features:

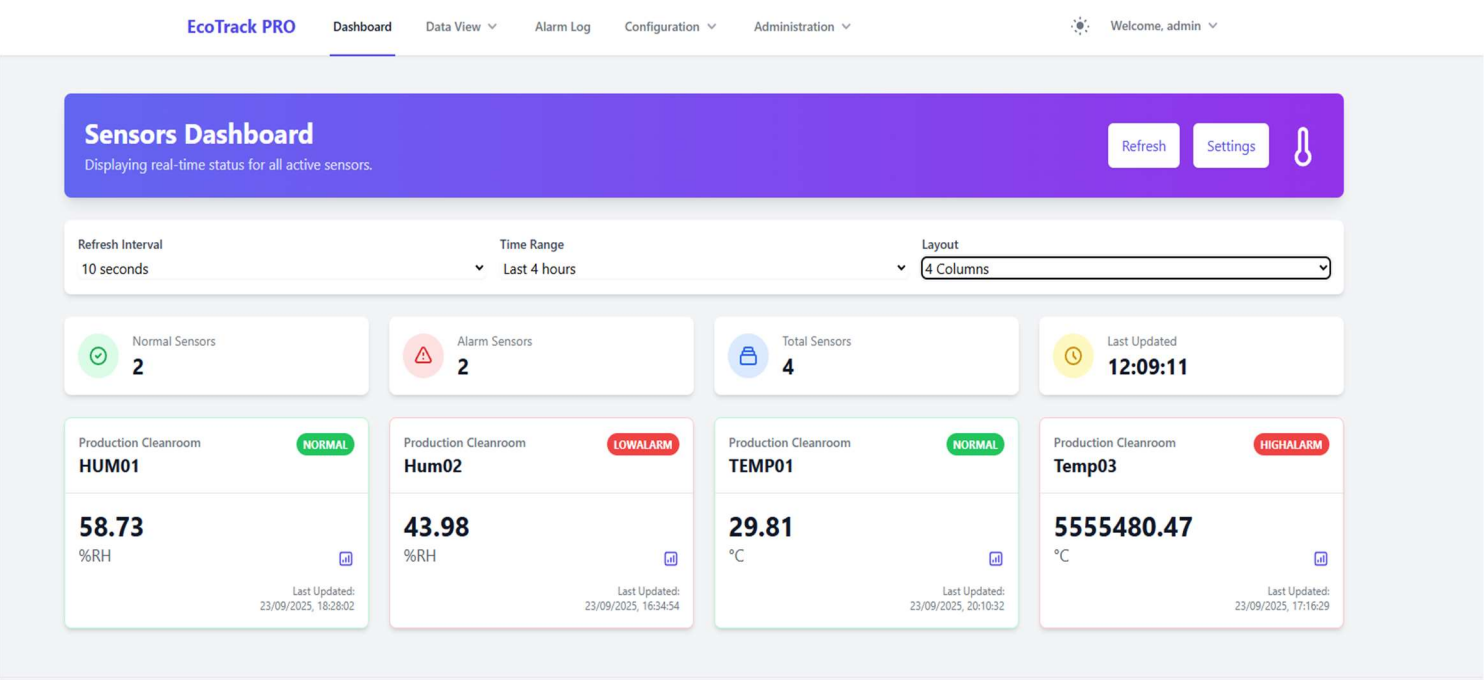
- Session timeout after 60 minutes of inactivity (default)
- Secure cookie storage with HttpOnly flag
- Sliding expiration to maintain active sessions
- Failed login attempt tracking for security monitoring

Password Reset:

1. Click "Forgot Password" on the login screen
2. Enter your registered email address
3. Check your email for password reset instructions
4. Follow the link and create a new password
5. Log in with your new credentials

8.2 Dashboard Navigation

Dashboard Overview:
After successful login, the dashboard provides real-time status of all monitored sensors:



Dashboard Sections:

1. **System Status Bar**: Shows overall system health and connection status
2. **Sensor Grid**: Displays all active sensors with current values and status
3. **Alarm Summary**: Highlights active alarms requiring attention
4. **Quick Actions**: Common functions accessible from the dashboard
5. **Navigation Menu**: Access to all system functions

Sensor Grid Information:

- **Sensor Tag**: Unique identifier for each sensor
- **Location**: Physical location of the sensor
- **Current Value**: Real-time reading
- **Unit of Measure**: Appropriate measurement unit
- **Status**: Color-coded status indicator
  - Green: Normal operation
  - Yellow: Warning/alarm delay period
  - Red: Active alarm condition
- **Last Updated**: Timestamp of most recent reading

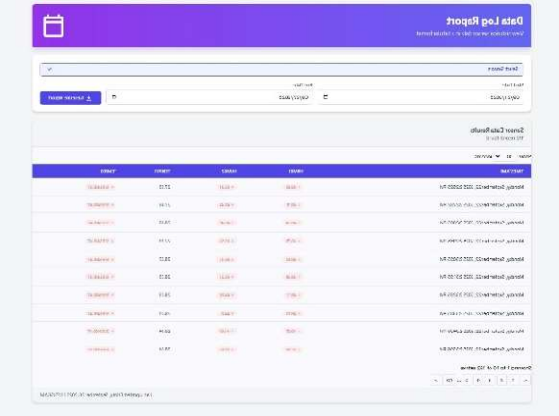
Navigation Menu:

- **Dashboard**: Return to main monitoring screen
- **Sensors**: Sensor configuration and management
- **Alarms**: Alarm log and management
- **Reports**: Generate and view reports
- **Configuration**: System settings and user management
- **Help**: Access to documentation and support

8.3 Real-time Monitoring Functions

Viewing Sensor History:

1. Click on any sensor in the dashboard grid
2. A history chart will appear showing the last 4 hours of data
3. Use chart controls to zoom, pan, or change time ranges
4. Click "View Full History" for complete historical data

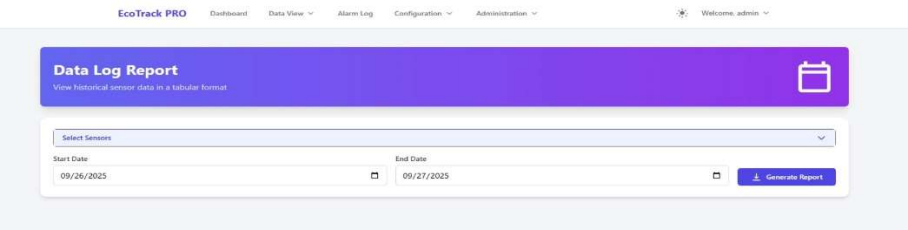


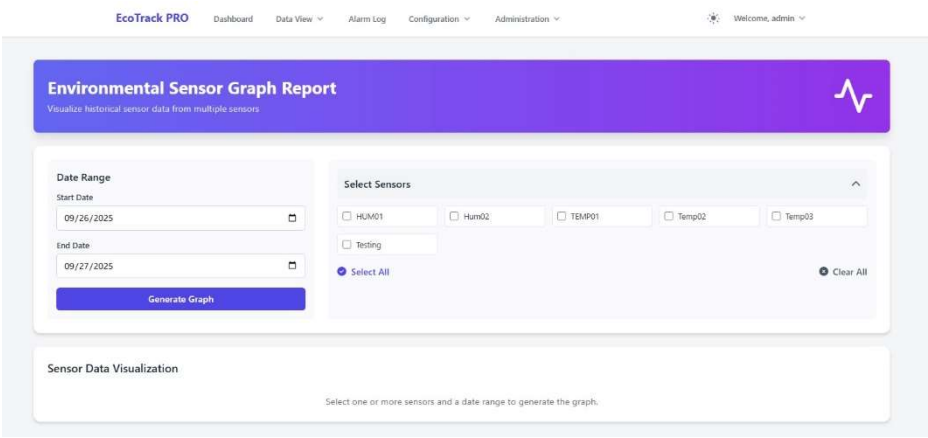
Refreshing Data:

- The dashboard auto-refreshes every 30 seconds by default
- Manually refresh by clicking the refresh icon in the top toolbar
- All data is timestamped in local time with UTC reference available

Filtering and Sorting:

- Use the filter options to display specific locations or sensor types
- Sort sensors by name, location, or status using column headers
- Export current view to Excel or PDF formats





8.4 Data Verification Procedures

Daily Verification Tasks:
For operators responsible for data verification:

Step 1: Review Alarm Log

1. Navigate to the Alarm Log section
2. Check for any unresolved alarms from the previous shift
3. Verify that all acknowledged alarms were properly addressed
4. Document any anomalies in the shift log

Step 2: Verify Critical Sensor Readings

1. Review all sensors with critical environmental parameters
2. Confirm that all readings are within acceptable ranges
3. Check for any trends that might indicate potential issues
4. Verify that all sensors are reporting current data

Step 3: Audit Trail Review

1. Access the Audit Trail section
2. Review any configuration changes from the previous period
3. Verify that all changes were authorized and properly documented
4. Report any unusual activities to the supervisor

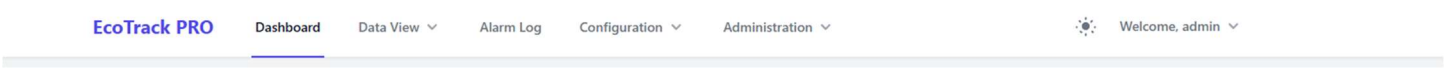
Data Integrity Checks:

- Ensure data timestamps are accurate and sequential
- Verify no gaps in data collection during operational hours
- Check that all alarmed conditions were properly logged
- Confirm that alarm acknowledgment and resolution follow procedures

Report Generation:

1. Navigate to the Reports section
2. Select the appropriate report type (Daily Summary, Trend Analysis, etc.)
3. Set the date range for the report
4. Configure report parameters as needed
5. Generate and review the report for accuracy
6. Save or export the report as required

[IMAGE: Dashboard Interface with Navigation Menu]



9. Alarm Handling & Notifications

9.1 Alarm Configuration

Alarm Thresholds:
Each sensor can have configurable alarm thresholds that trigger when environmental parameters exceed defined limits:

Low Alarm Configuration:

- Set Low Alarm Limit below normal operating range
- Alarm triggers when sensor value drops below this limit
- Recommended hysteresis of at least 0.5 units above the limit
- Example: Temperature sensor with Low Alarm Limit of 18°C for room with normal range 20-25°C

High Alarm Configuration:

- Set High Alarm Limit above normal operating range
- Alarm triggers when sensor value exceeds this limit
- Recommended hysteresis of at least 0.5 units below the limit
- Example: Humidity sensor with High Alarm Limit of 65%RH for room with normal range 45-60%RH

Alarm Delay Settings:

- Configure alarm delay in seconds (0-3600)
- Prevents spurious alarms from temporary fluctuations
- Example: Set 30-second delay for temperature sensors to avoid alarms from brief HVAC cycles

Creating Alarm Thresholds:

1. Navigate to Sensors > Edit Sensor
2. Locate Alarm Configuration section
3. Enter Low Alarm Limit (or leave blank for no low alarm)
4. Enter High Alarm Limit (or leave blank for no high alarm)
5. Set Alarm Delay in seconds
6. Save the configuration

9.2 Alarm Prioritization

Alarm States:
The system uses a three-tier alarm management system:

1. **Active Alarms**: Conditions exceeding thresholds that require immediate attention
2. **Acknowledged Alarms**: Active alarms that have been acknowledged by an operator
3. **Resolved Alarms**: Alarms where normal conditions have been restored

Alarm Severity Levels:

- **Critical**: Immediate action required (e.g., temperature excursion affecting product)

- **High**: Requires prompt attention (e.g., HVAC failure)
- **Medium**: Monitor and address within defined timeframe (e.g., backup system activation)

9.3 Notification Methods

Physical Alarm Devices:
The system supports various physical notification devices:

Relay Outputs:

- Visual indicators (warning lights, strobes)
- Audio alarms (horns, buzzers)
- Building management system integration
- Equipment shutoff controls

SMS Notifications:

- Text message alerts to designated phone numbers
- Configurable message content and escalation
- Automatic retry if first message fails

Alarm Device Configuration:

1. Navigate to Configuration > Alarm Devices
2. Add new alarm device with appropriate type
3. Configure device-specific parameters
4. Link to relevant sensors using Alarm Mapping

9.4 Alarm Acknowledgment Procedures

Active Alarm Display:

- Active alarms appear in the main dashboard
- Red status indicators highlight alarm conditions
- Alarm log shows all current alarm events
- Unacknowledged alarms remain visible until acknowledged

Acknowledging Alarms:

1. Navigate to Alarms > Alarm Log
2. Locate the active alarm requiring acknowledgment
3. Click the "Acknowledge" button next to the alarm

4. Enter acknowledgment message (optional but recommended)
5. Click "Confirm" to acknowledge the alarm

Acknowledgment Requirements:

- Only users with "Alarm Acknowledge" permission can acknowledge alarms
- Acknowledgment is logged in audit trail with username and timestamp
- Acknowledgment must be followed by resolution actions

9.5 Alarm Resolution Process

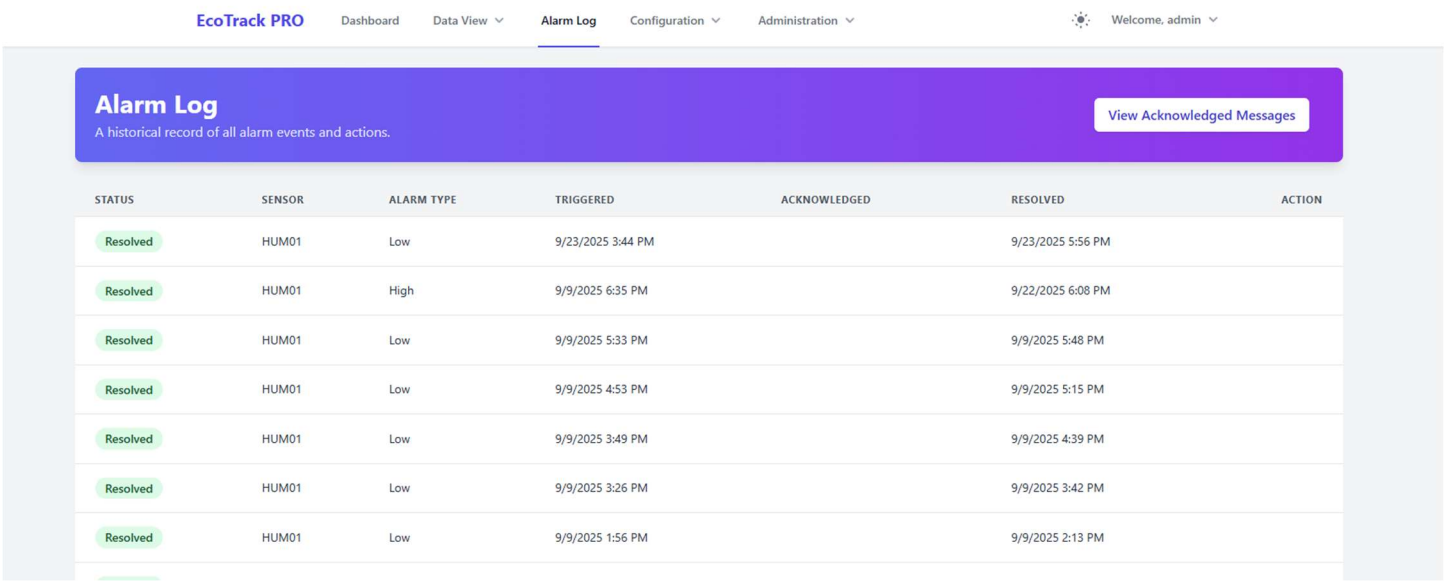
Resolution Steps:

1. Identify the root cause of the alarm condition
2. Take corrective and preventative actions to restore the parameter to normal range
3. Once the sensor reading is back within limits, the alarm will be marked as "Resolved"
4. Manually close the alarm by clicking "Resolve Alarm"
5. Enter resolution details (e.g., "HVAC filter replaced, temperature restored")
6. Require electronic signature for final resolution approval

Resolution Documentation:

- All resolution details are permanently stored in the alarm log
- Resolution requires a mandatory audit trail entry
- Link to any related change control or deviation forms

[IMAGE: Alarm Log Interface]



10. Data Logging & Reporting

10.1 Data Collection Process

Logging Interval:

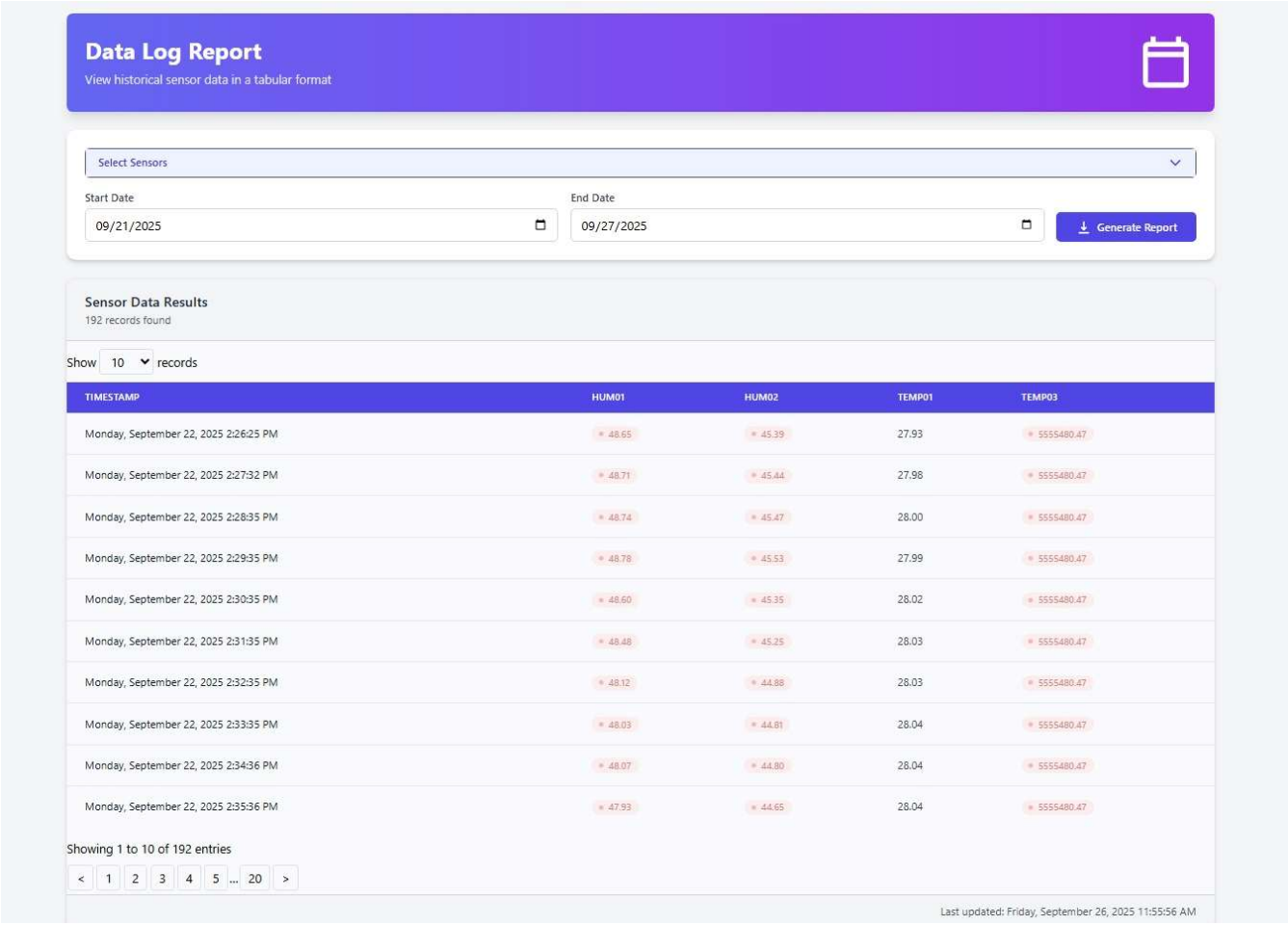
- Data points are collected and logged every 60 seconds (default)
- Logging interval is globally configurable in System Settings
- Faster logging intervals require more storage capacity

Time Stamping:

- All logged data points include a unique, unalterable timestamp
- Timestamps are recorded in UTC and converted to local time for display
- Timestamp precision: Milliseconds

Data Validation:

- Data is validated against pre-set ranges before storage
- Out-of-range data is logged with an error flag
- Checksum validation for data transmission integrity



10.2 Data Storage and Integrity

Database Structure:

- Relational database (Microsoft SQL Server) for data security
- Separated tables for: Sensor Data, Alarm Log, Audit Trail, Configuration
- Indexes optimized for rapid querying and reporting

Data Retention Policy:

- Historical data retained for a minimum of 7 years (configurable)
- Automated archiving of old data to secondary storage
- Data integrity checks run daily to ensure no loss or corruption

Integrity Checks:

- Database transaction logging enabled
- Regular database backups and validation
- Access control at the database level to prevent unauthorized modification
- Electronic signatures required for all data deletion/modification (except automated data deletion)

10.3 Report Generation

Available Report Types:

1. **Daily Summary Report**: Snapshot of average, min, max values per sensor
2. **Alarm Event Report**: Detailed log of all alarm occurrences, acknowledgments, and resolutions
3. **Out-of-Specification Report**: Lists all data points outside normal operating limits
4. **Trend Analysis Report**: Graphs and statistical summaries over a user-defined time period
5. **Audit Trail Report**: Export of all user and system activities

Report Configuration:

1. Navigate to the Reports menu
2. Select report type and date range
3. Filter by sensor, location, or parameter type
4. Generate and preview the report
5. Export the final report (PDF, Excel, or CSV format)

Report Output:

- All reports include a title page, table of contents, and pagination
- Reports include electronic signature fields for review and approval
- PDF reports are read-only to ensure data integrity

10.4 Data Export and Analysis

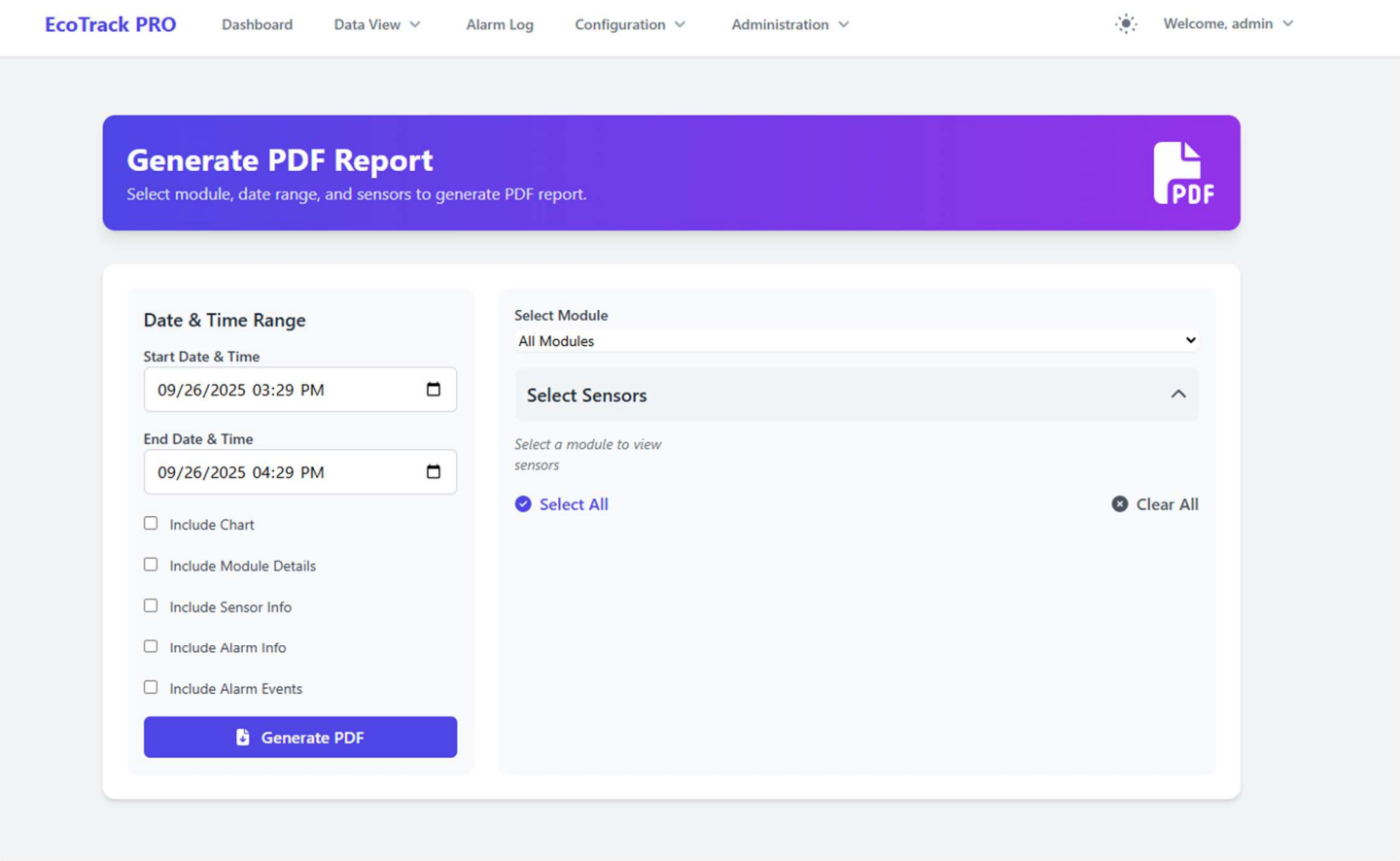
Export Formats:

- **CSV (Comma Separated Values)**: For detailed data analysis in external tools
- **PDF (Portable Document Format)**: For official, immutable records
- **Excel (XLSX)**: For tabular data analysis

Export Process:

1. Select data for export (e.g., historical data for a sensor, or a specific alarm log)
2. Choose export format and date range
3. System generates the file and prompts for download
4. Data export is recorded in the audit trail

[IMAGE: Report Generation Interface]



11. Backup & Restore

11.1 Data Backup Procedures

Automated Backup:

- Full database backup performed every 24 hours (default)
- Incremental backup performed every 4 hours
- Backup files are stored on a separate network location (configurable)
- Backup logs are generated and monitored daily

Backup Configuration:

1. Navigate to System Settings > Backup Configuration
2. Set backup frequency for full and incremental backups
3. Specify network path for backup storage (e.g., \\backup-server\ems_backups)
4. Configure retention policy (e.g., keep 30 days of full backups)

Critical Action: Verify the integrity of the automated backup process weekly by performing a test restore.

11.2 System Restore Process

Restore Prerequisites:

- Stop the Environmental Monitoring Windows Service
- Ensure the target database server is operational
- Have the latest verified backup file available
- Restore process requires Administrator credentials for the database server

Database Restore Steps (SQL Server):

1. Open SQL Server Management Studio (SSMS)
2. Right-click the database > Tasks > Restore > Database
3. Select "From device" and locate the backup file
4. Ensure "Overwrite the existing database" is selected
5. Execute the restore operation
6. Check the restore log for successful completion

11.3 Recovery Validation

Validation Steps Post-Restore:

1. Start the Environmental Monitoring Windows Service
2. Access the Web Application and log in
3. Verify a critical sensor's latest reading and historical trend
4. Check the Audit Trail for the last 24 hours of activity
5. Confirm that the system time and date are correct
6. Generate a historical report to validate data integrity

Recovery Documentation:

- Document the date and time of the restore operation
- Record the backup file used for the restore
- Note any deviations or anomalies encountered during validation
- Obtain electronic signature from IT and QA departments for recovery sign-off

12. Maintenance & Troubleshooting

12.1 Routine Maintenance Tasks

Weekly Tasks:

- Review system log files for non-critical errors
- Verify successful completion of automated backups
- Clear temporary files and cache from the application server
- Check physical condition of ADAM modules and sensor wiring

Monthly Tasks:

- Test alarm devices (horns, lights, SMS) for functionality
- Review data storage utilization and plan for capacity expansion
- Apply minor, non-critical software patches and updates
- Review user access list and deactivate inactive accounts

Annual Tasks:

- Full sensor calibration and re-validation
- Perform a full system restore drill (mock disaster recovery)

- Review and update SOPs related to EMS operation
- Renew SSL certificates and system licenses

12.2 Health Monitoring

System Health Indicators:

- **Service Status**: Environmental Monitoring Service running and consuming normal CPU/RAM
- **Database Latency**: Check query response times (should be < 500ms)
- **Communication Status**: Check for repeated communication failures in the log
- **Disk Space**: Ensure adequate disk space for the database and logs

Monitoring Tools:

- Windows Service Manager for service status
- Task Manager/Resource Monitor for resource usage
- SQL Server Monitoring tools for database health
- Built-in system status dashboard in the Web Application

12.3 Error Codes and Solutions

Common Error Codes:

Code	Description	Solution
E-COMM-001	Serial port communication timeout with module [SlaveID]	Check RS-485 wiring, power supply to module, and verify COM port settings in appsettings.json.
E-DB-101	Database connection failed.	Verify SQL Server service is running. Check connection string and database credentials.
E-LIC-200	License expired or invalid.	Contact system administrator. Apply a new valid license key in the License Management section.
E-VAL-300	Sensor reading outside input range for [SensorTag].	Verify sensor wiring and calibration input range settings. Check for hardware failure.

12.4 System Updates

Update Process:

1. Review new version release notes and compatibility matrix
2. Perform full system backup before starting the update
3. Stop the Environmental Monitoring Windows Service and Docker containers
4. Apply the update package and run migration scripts (if any)
5. Restart services and perform post-update validation
6. Document the update in the change control system

13. Glossary & Abbreviations

13.1 Glossary

- **ADAM**: Advantech Data Acquisition Module, a series of industrial I/O devices.
- **Audit Trail**: A secure, chronological record of system operations, including user logins, data changes, and alarms.
- **21 CFR Part 11**: FDA regulation concerning electronic records and electronic signatures.
- **cGMP**: Current Good Manufacturing Practice, a set of regulations for pharmaceutical manufacturing.
- **Docker**: A platform used to develop, ship, and run applications in containers.
- **Hysteresis**: A defined range around an alarm limit to prevent rapid on/off cycling of an alarm.
- **IQ/OQ/PQ**: Installation Qualification, Operational Qualification, Performance Qualification (system validation phases).
- **Modbus RTU**: A serial communication protocol used to connect industrial electronic devices.
- **Validation**: Documented evidence that the system fulfills its intended purpose and regulatory requirements.

13.2 Abbreviations

Abbreviation	Meaning
ECOTrack	Environmental Monitoring / Tracking System
GMP	Good Manufacturing Practice
cGMP	Current Good Manufacturing Practice
SOP	Standard Operating Procedure
RH	Relative Humidity
UTC	Coordinated Universal Time
RBAC	Role-Based Access Control
IQ/OQ/PQ	Installation/Operational/Performance Qualification

14. Appendices

Appendix A: System Specifications

Server Requirements:

- OS: Windows Server 2019/2022
- CPU: 4 cores minimum, 2.5 GHz or higher
- RAM: 16 GB DDR4 minimum
- Storage: 2 TB SSD for database (high I/O recommended)

Database Requirements:

- Platform: Microsoft SQL Server 2019 Standard or Enterprise
- Collation: SQL_Latin1_General_CP1_CI_AS
- Storage per Sensor/Year: Approximately 10 MB per sensor (at 60-second logging)

Communication Ports:

- COM5 (Primary ADAM Port)
- COM4 (SMS Modem Port)
- TCP Port 8080 (Web Application Access)

Appendix B: Configuration Templates

Sample Sensor Configuration Template (Temperature):

- Sensor Tag: ROOMA_T1
- Location: Room A
- Sensor Type: Temperature
- Unit: °C
- Input Min: 4.0 (mA)
- Input Max: 20.0 (mA)
- Scale Min: 0.0 (°C)
- Scale Max: 50.0 (°C)
- Low Alarm Limit: 18.0
- High Alarm Limit: 26.0
- Alarm Delay: 60 seconds

Sample User Role Template (Operator):

- Permissions: Dashboard Access, View Sensors, View Alarms, Acknowledge Alarms, Resolve Alarms, View Reports, Generate Reports, Export Data, Audit Trail Access, Sensor Calibration*
- Password Policy: Default (90-day expiration, 8 characters minimum)
- Notification Group: Operators_Email_Group

Appendix C: Training Checklists

Operator Training Checklist:

- [ ] Login and Authentication (Section 8.1)
- [ ] Dashboard Navigation and Status Check (Section 8.2)
- [ ] Real-time Monitoring and History Viewing (Section 8.3)
- [ ] Alarm Acknowledgment Procedure (Section 9.4)
- [ ] Alarm Resolution Process (Section 9.5)
- [ ] Generating Daily Summary Reports (Section 10.3)
- [ ] Emergency Contacts and Escalation Protocol (External Document Ref)
- [ ] Data Verification Procedures (Section 8.4)

Administrator Training Checklist:

- [ ] All Operator items completed
- [ ] System Installation & Service Management (Section 5)
- [ ] Sensor and Module Configuration (Section 6.3, 6.4)
- [ ] User Management and RBAC Configuration (Section 7.2, 7.3)
- [ ] Backup and Restore Procedures (Section 11)
- [ ] Audit Trail Review and Export (Section 7.4)
- [ ] System Health Monitoring (Section 12.2)
- [ ] Disaster Recovery Plan Review (Section 11.3)

Appendix D: Change Control Forms

Standard Change Request Form:

- Change Request Number: _____
- Date of Request: _____
- Requester Name: _____

- Change Description: _____
- Justification for Change: _____
- Affected System Component(s): _____
- Risk Assessment (High/Med/Low): _____
- Implementation Date: _____
- Validation Required: _____
- Test Plan Required: _____
- Change Approver: _____
- Date: _____

Emergency Change Authorization:
For emergency changes that require immediate implementation:

- Change Description: _____
- Urgency Justification: _____
- Risks of Not Implementing: _____
- Implementation Plan: _____
- Rollback Plan: _____
- Emergency Approver: _____
- Date/Time: _____

Change Verification Checklist:

- [ ] Change implemented as specified
- [ ] System functionality verified
- [ ] User access maintained
- [ ] Data integrity confirmed
- [ ] Security measures maintained
- [ ] Performance verified
- [ ] Audit trail reviewed
- [ ] Documentation updated
- [ ] User notification completed
- [ ] Post-implementation review scheduled