# HAYLO

## Web Admin Dashboard

### User Manual v2.0

Version: 2.0.0 | Build: 20260328

Date: April 2026

Classification: Confidential

# Table of Contents

# 1. Introduction

The Haylo Web Admin Dashboard is a centralized management console for the Haylo IoT security system. It provides administrators with full control over devices, users, firmware updates, security alerts, and system configurations.

## Key Features

- Real-time device monitoring and heartbeat tracking
- Cluster and site hierarchy management
- OTA firmware management and deployment
- Security alert monitoring with severity filtering
- User management with role-based access control (RBAC)
- Arm/disarm event logging and audit trail
- SOS emergency event tracking and response
- System health monitoring and configuration

## System Requirements

- Modern web browser (Chrome, Firefox, Edge, Safari)
- Internet connection to access the admin portal
- Admin credentials (provided by system administrator)

## Access URL

Production: https://haylo.palawan-privagate.com/

# 2. Login

To access the Haylo Admin Dashboard, navigate to the admin URL in your web browser. You will be presented with the login screen.

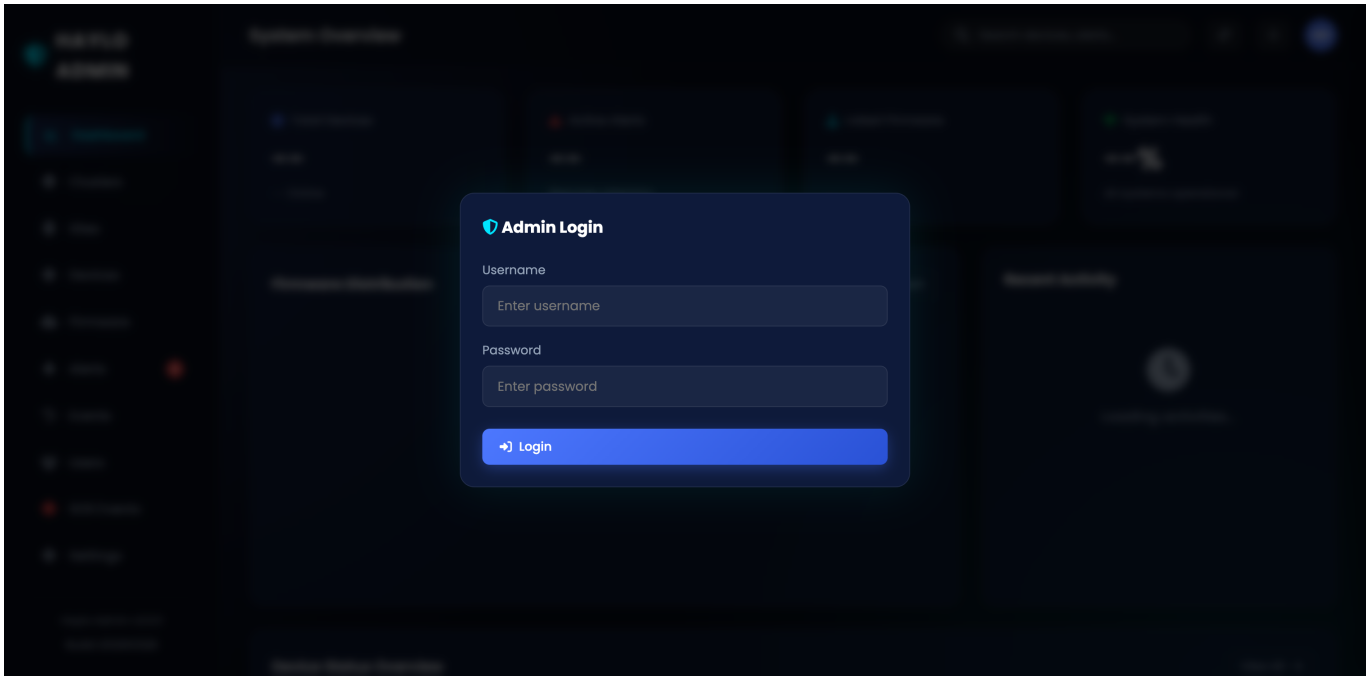


*Figure 2.1 - Login Screen*

## Login Steps

- Enter your username in the 'Username' field
- Enter your password in the 'Password' field
- Click the 'Login' button to authenticate

Upon successful authentication, you will be redirected to the Dashboard. The available menu items in the sidebar will depend on your assigned role.

# 3. Dashboard

The Dashboard provides a system overview with key metrics, firmware distribution, recent activity, and device status at a glance.

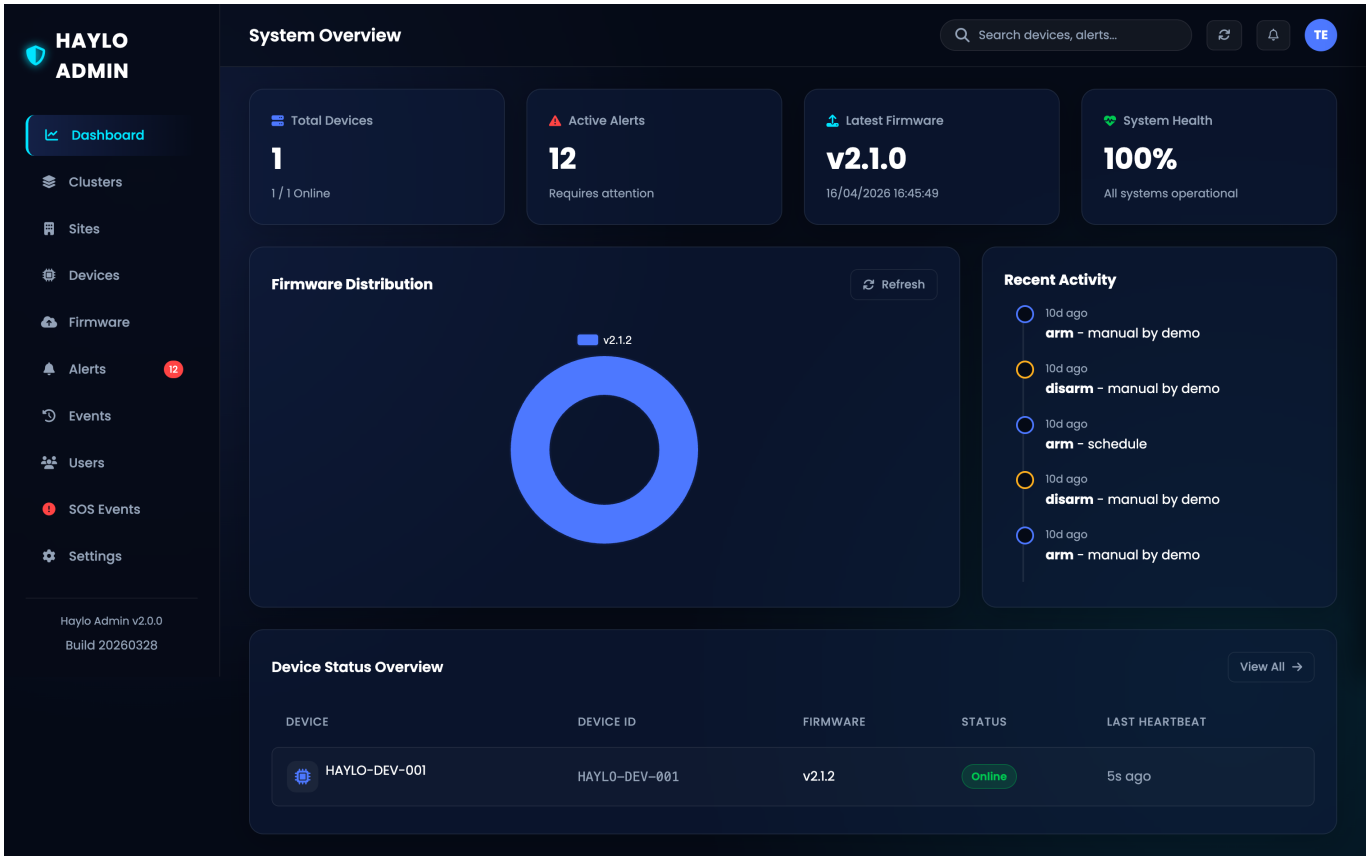


*Figure 3.1 - System Overview Dashboard*

## Dashboard Components

- Total Devices: Shows the total number of registered devices and how many are currently online
- Active Alerts: Displays the count of unacknowledged security alerts requiring attention
- Latest Firmware: Shows the most recent firmware version and its release date
- System Health: Displays overall system health percentage
- Firmware Distribution: A donut chart showing firmware version distribution across devices
- Recent Activity: Timeline of recent arm/disarm events with user and method details
- Device Status Overview: Table listing all devices with their current status and last heartbeat

# 4. Cluster Management

Clusters represent organizational groups (e.g., regions, buildings, or client organizations). Each cluster can contain multiple sites. Clusters can be synced from iMOPS or created manually.

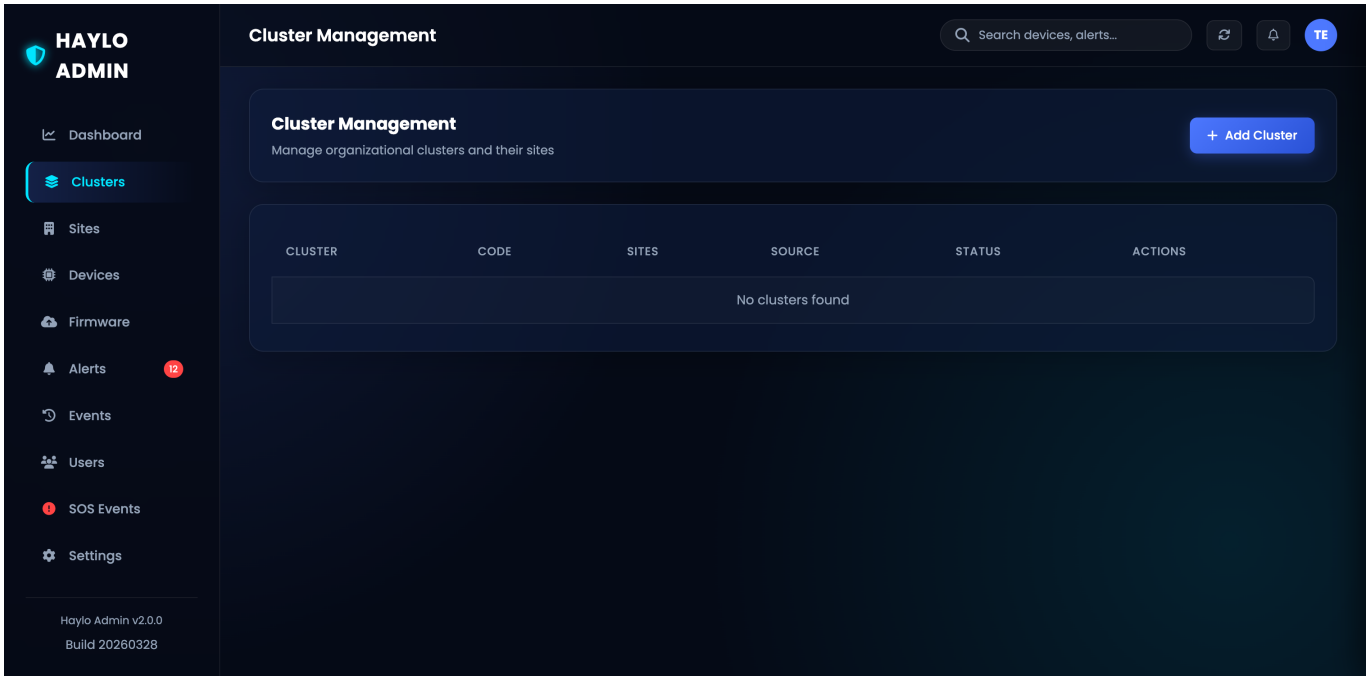


*Figure 4.1 - Cluster Management*

## Actions

- Add Cluster: Click '+ Add Cluster' to create a new cluster with name and code
- View Sites: See how many sites belong to each cluster
- Edit/Delete: Use the action buttons to modify or remove clusters

## Table Columns

- CLUSTER: Display name of the cluster
- CODE: Unique identifier code for the cluster
- SITES: Number of sites within the cluster
- SOURCE: Origin of the cluster (manual or iMOPS sync)
- STATUS: Active or inactive status
- ACTIONS: Edit and delete buttons

# 5. Site Management

Sites are physical locations within a cluster (e.g., office branches, warehouse locations). Each site can have multiple devices assigned to it.

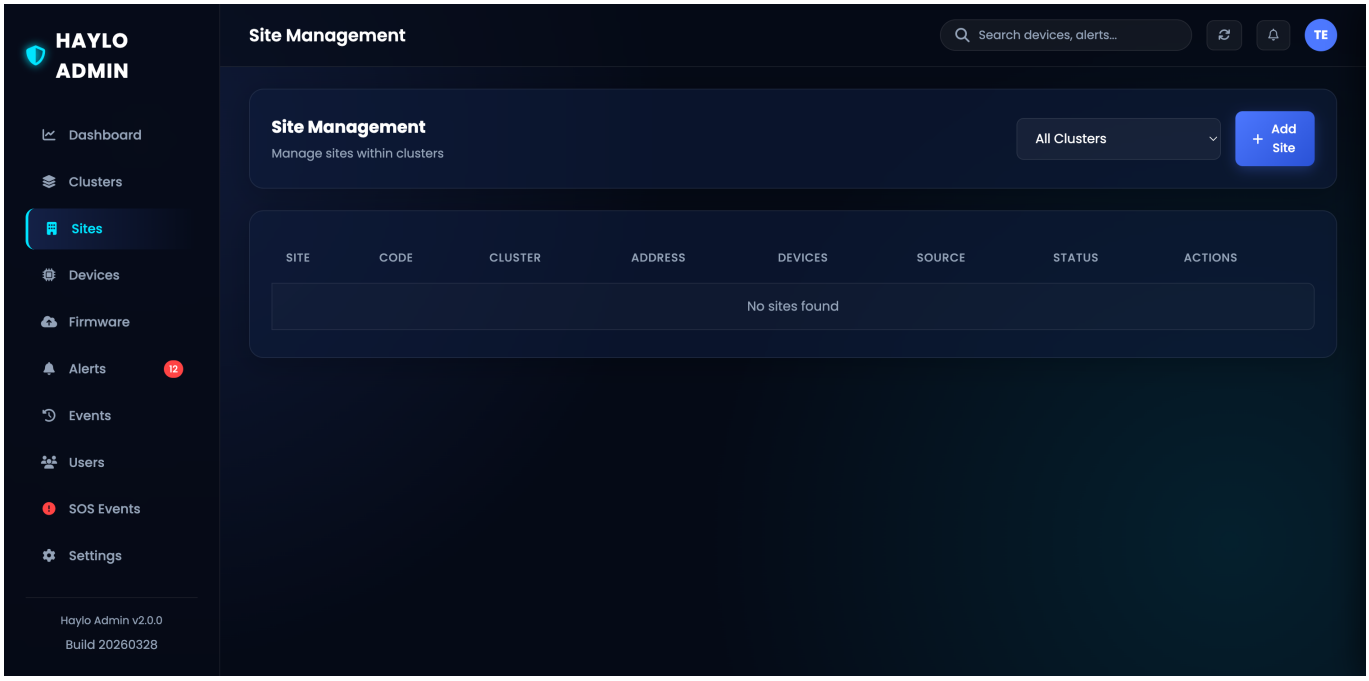


*Figure 5.1 - Site Management*

## Actions

- Add Site: Click '+ Add Site' to create a new site within a cluster
- Filter by Cluster: Use the 'All Clusters' dropdown to filter sites by cluster
- Edit/Delete: Modify site details or remove sites

## Table Columns

- SITE: Display name of the site
- CODE: Unique site identifier
- CLUSTER: Parent cluster the site belongs to
- ADDRESS: Physical address of the site
- DEVICES: Number of devices at this site
- SOURCE: Origin (manual or iMOPS sync)
- STATUS: Active/inactive status

# 6. Device Management

The Device Management page allows administrators to register, configure, and monitor IoT gateway devices. Each device represents a Haylo security controller installed at a site.

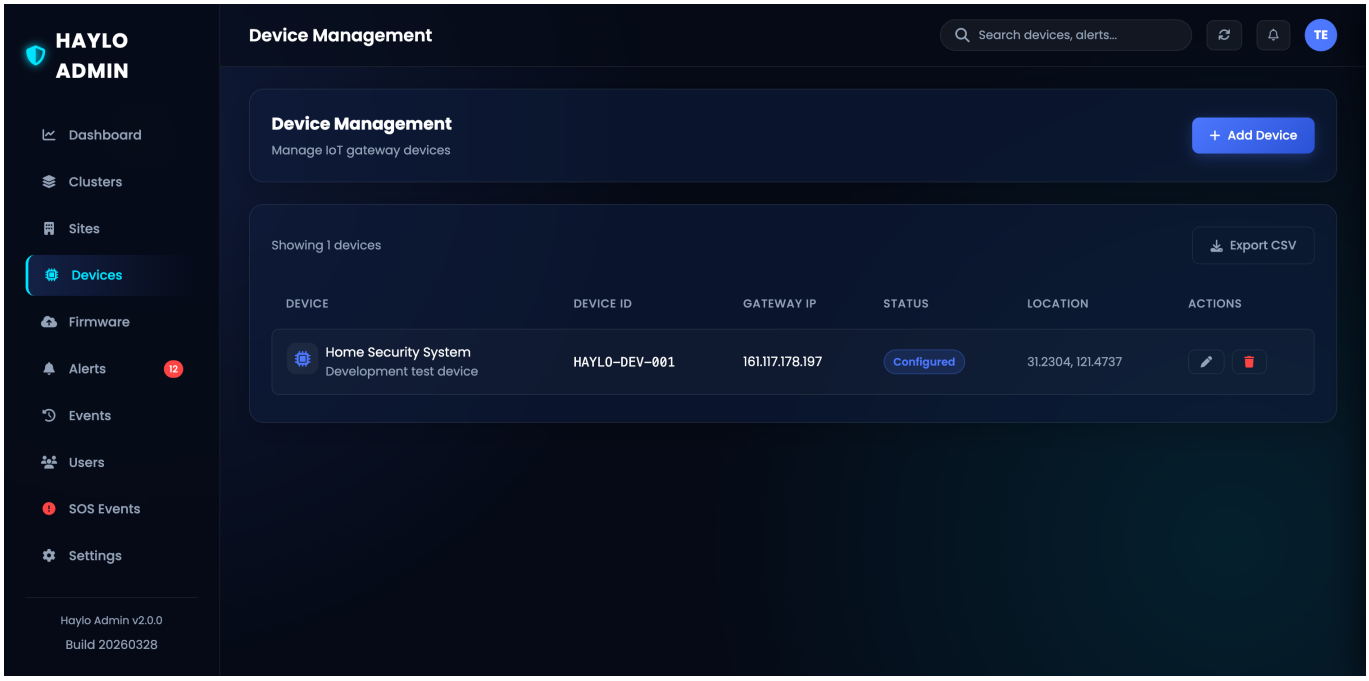


*Figure 6.1 - Device Management*

## Actions

- Add Device: Register a new IoT gateway device with its device ID and gateway IP
- Export CSV: Download device data as a CSV file for reporting
- Edit: Modify device name, description, location, or gateway IP
- Delete: Remove a device from the system

## Table Columns

- DEVICE: Device name and description
- DEVICE ID: Unique hardware identifier (e.g., HAYLO-DEV-001)
- GATEWAY IP: The IP address of the device controller
- STATUS: Configured / Online / Offline
- LOCATION: GPS coordinates (latitude, longitude)
- ACTIONS: Edit and delete buttons

# 7. Firmware Management

The Firmware Repository manages OTA (Over-The-Air) firmware updates for Haylo devices. Administrators can upload new firmware packages and track deployment status.

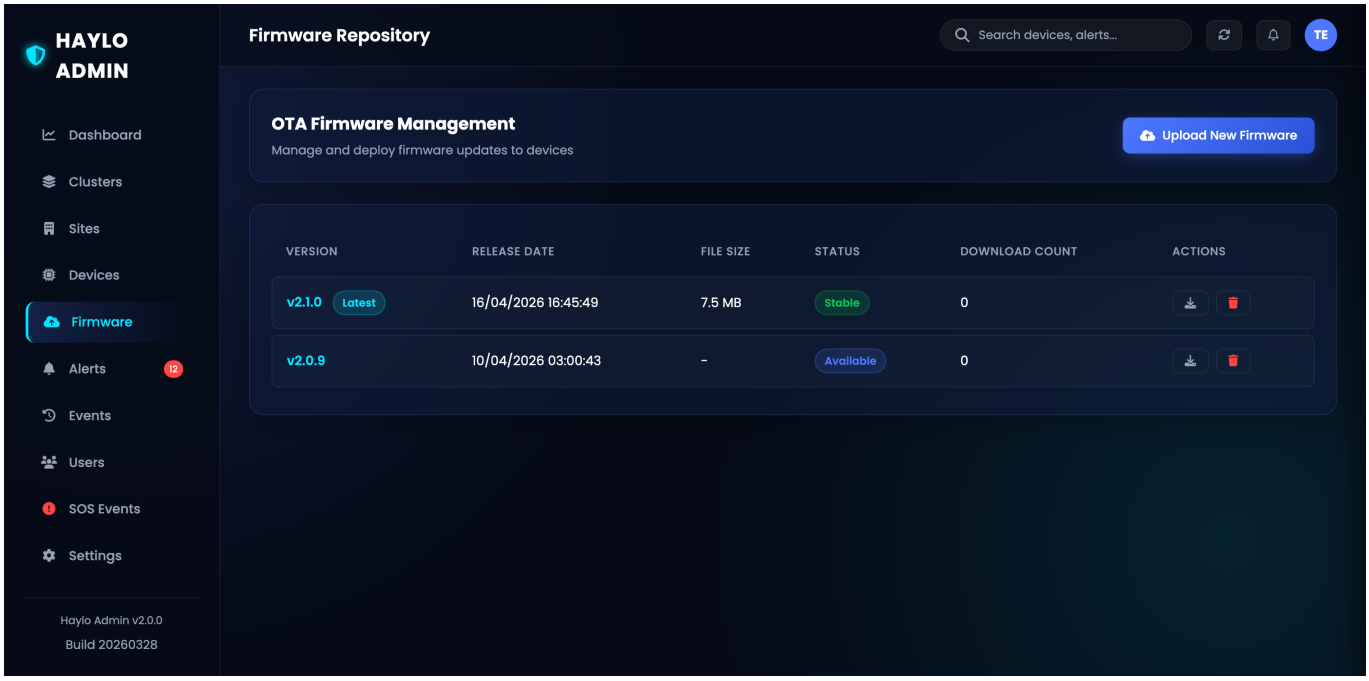


*Figure 7.1 - Firmware Repository*

## Actions

- Upload New Firmware: Upload a firmware binary with version number and release notes
- Download: Download a firmware package for manual deployment
- Delete: Remove a firmware version from the repository

## Table Columns

- VERSION: Firmware version number (e.g., v2.1.0). The latest version is tagged with 'Latest'
- RELEASE DATE: Date and time the firmware was uploaded
- FILE SIZE: Size of the firmware binary
- STATUS: Stable / Available / Deprecated
- DOWNLOAD COUNT: Number of times devices have downloaded this version

## OTA Update Process

1. Upload firmware via the admin dashboard
2. Devices check for updates via heartbeat mechanism
3. If a newer version is available, the device downloads and installs it automatically
4. The download count is incremented for tracking

# 8. Security Alerts

The Security Alerts page displays all security-related notifications from devices, including sensor triggers, device offline events, and motion detections.

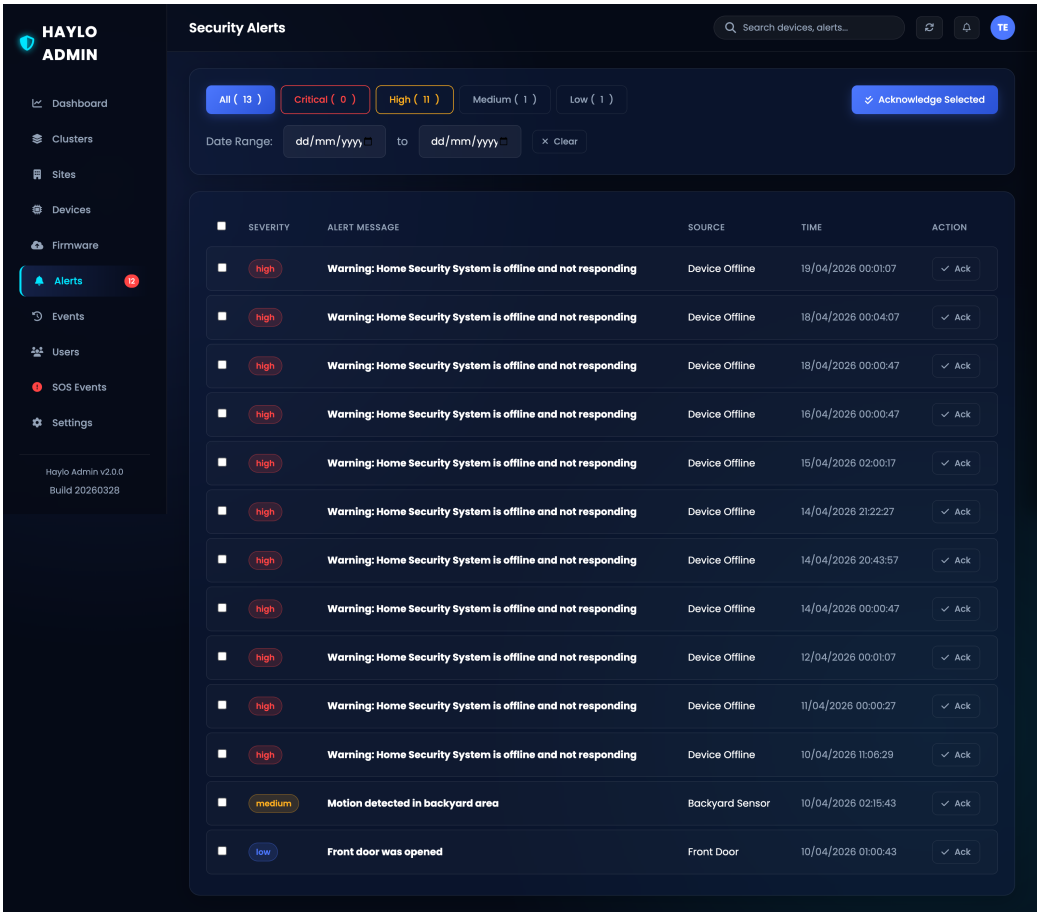


*Figure 8.1 - Security Alerts*

## Severity Filters

- All: Show all alerts regardless of severity
- Critical (red): Highest priority alerts requiring immediate attention
- High (orange): Important alerts that should be addressed promptly
- Medium (yellow): Moderate alerts for awareness
- Low (green): Informational alerts

## Actions

- Filter by severity: Click severity buttons to filter the alert list
- Date Range: Filter alerts by specific date range
- Acknowledge: Mark individual alerts as acknowledged
- Acknowledge Selected: Bulk acknowledge multiple selected alerts

# 9. Event Logs

The Event Logs page provides a complete audit trail of all arm/disarm events in the system. This is useful for security auditing and incident investigation.

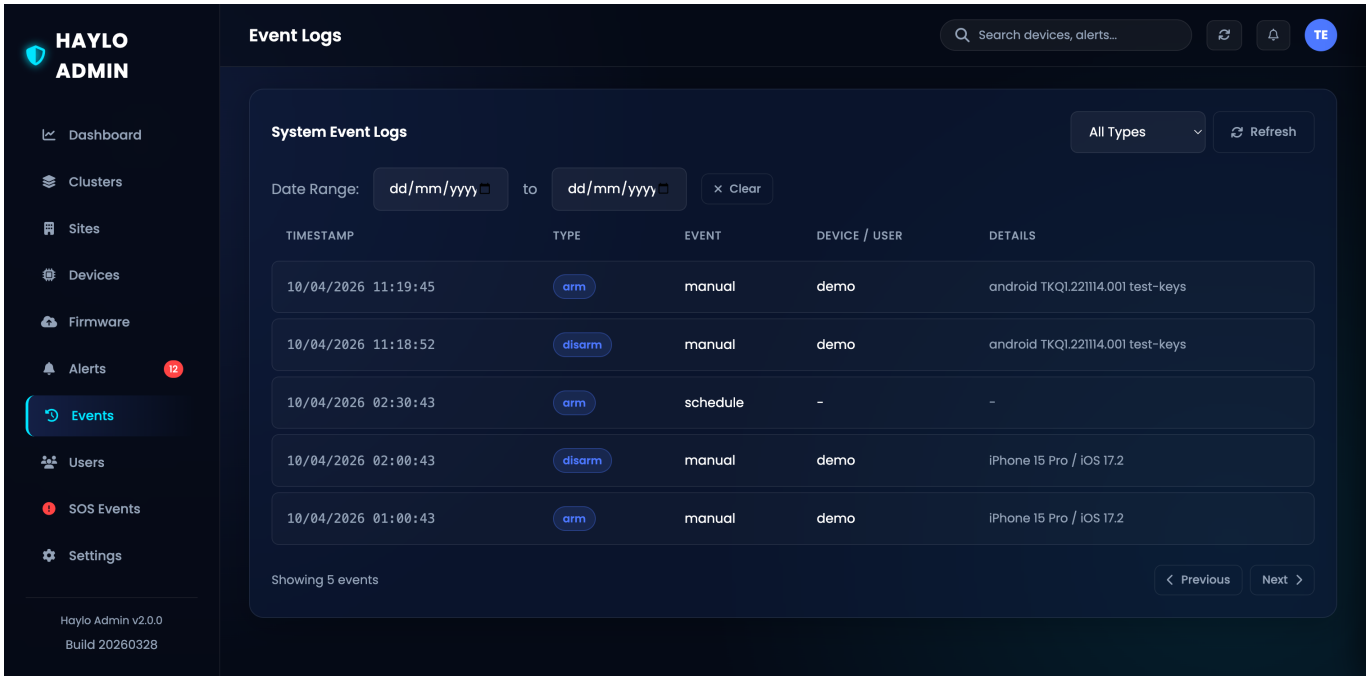


*Figure 9.1 - Event Logs*

## Table Columns

- TIMESTAMP: Date and time when the event occurred
- TYPE: Event type indicator (arm = green, disarm = red)
- EVENT: How the event was triggered (manual, schedule)
- DEVICE / USER: Which user or device initiated the event
- DETAILS: Additional context such as device type and OS version

## Filters

- All Types: Filter by event type dropdown (arm, disarm, all)
- Date Range: Filter events within a specific date range
- Refresh: Reload the latest events
- Pagination: Navigate through event pages with Previous/Next buttons

# 10. User Management

The User Management page allows Super Admins to create, edit, and manage user accounts. Each user is assigned a role that determines their access level within the system.

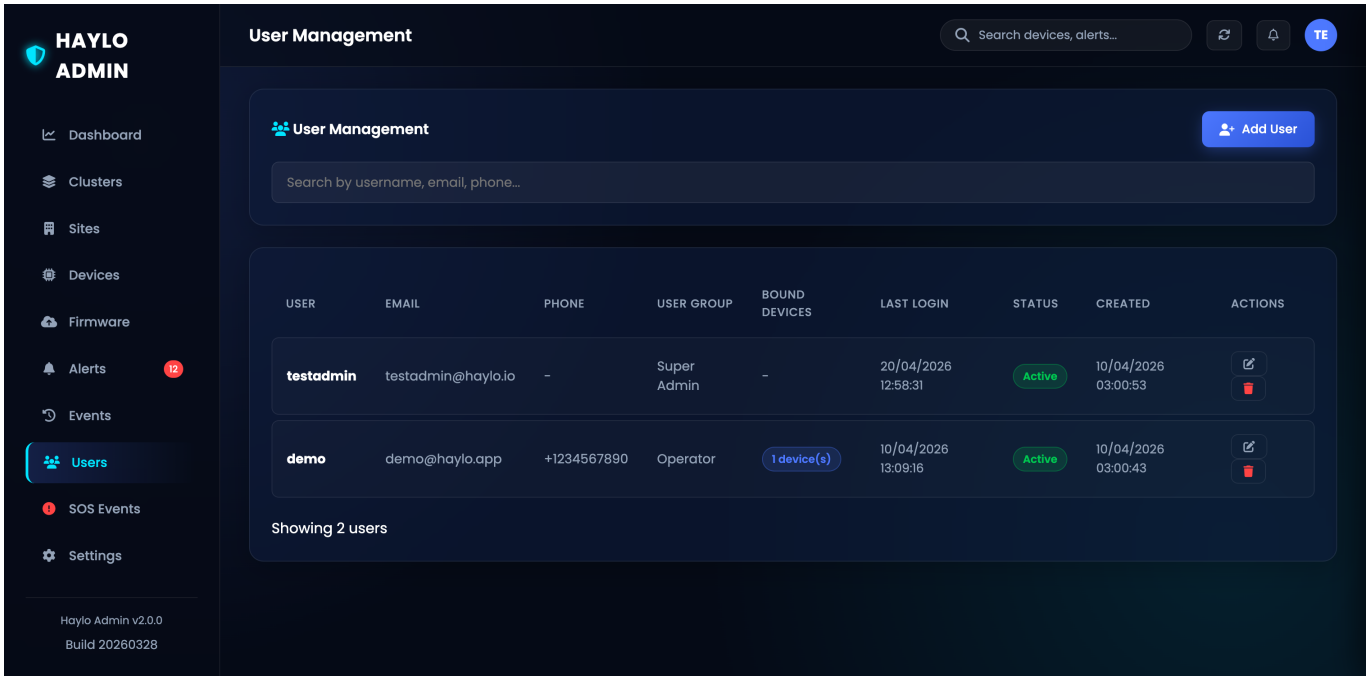


*Figure 10.1 - User Management*

## Actions

- Add User: Create a new user account with username, email, phone, role, and password
- Search: Filter users by username, email, or phone number
- Edit: Modify user details or change their role
- Delete: Remove a user account from the system

## Table Columns

- USER: Username of the account
- EMAIL: User's email address
- PHONE: Contact phone number
- USER GROUP: Assigned role (Super Admin, Cluster Admin, Operator)
- BOUND DEVICES: Number of devices assigned to this user
- LAST LOGIN: Most recent login timestamp
- STATUS: Active or inactive
- CREATED: Account creation date

# 11. SOS Emergency Events

The SOS Emergency Events page tracks emergency distress signals sent by users through the Haylo mobile app. Administrators can monitor, process, and resolve SOS events.

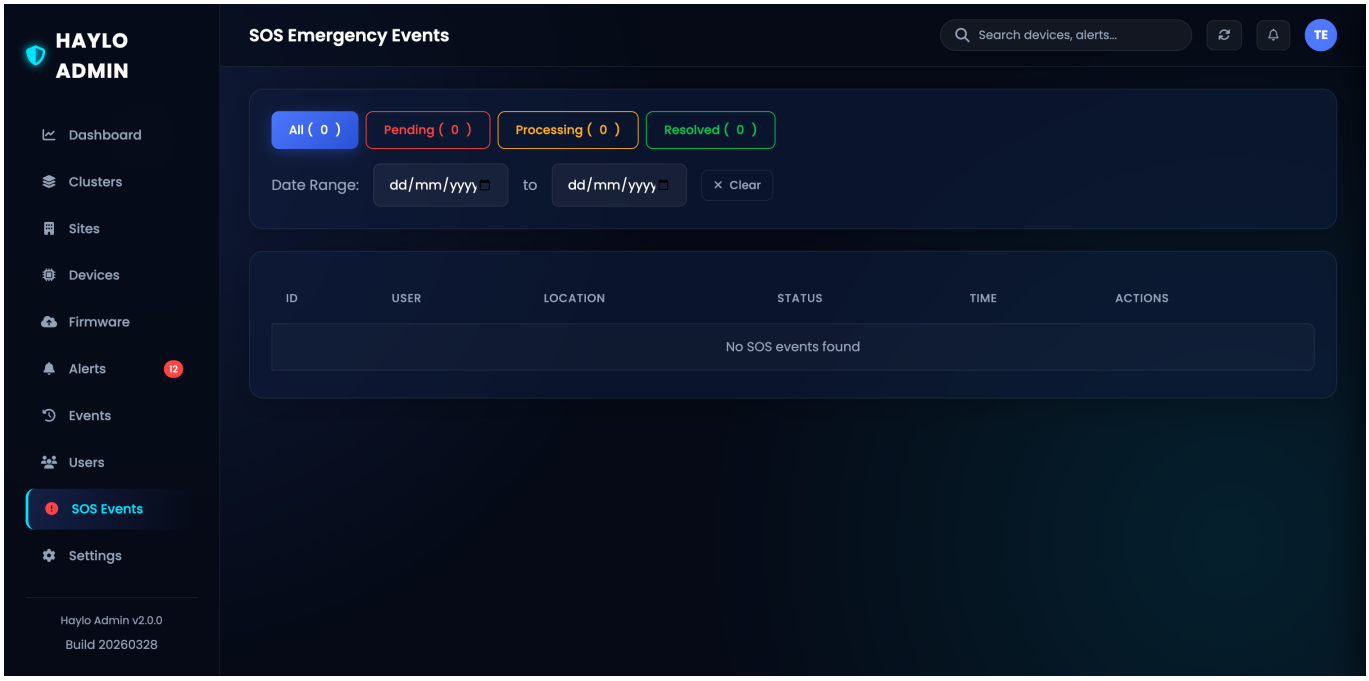


*Figure 11.1 - SOS Emergency Events*

## Status Filters

- All: Show all SOS events
- Pending (yellow): New SOS events awaiting response
- Processing (purple): SOS events currently being handled
- Resolved (green): SOS events that have been resolved

## Table Columns

- ID: Unique SOS event identifier
- USER: The user who triggered the SOS
- LOCATION: GPS coordinates of the SOS event
- STATUS: Current status of the SOS event
- TIME: When the SOS was triggered
- ACTIONS: Update status or view details

# 12. System Settings

The System Settings page provides configuration options for security behavior, notification preferences, and system status monitoring.

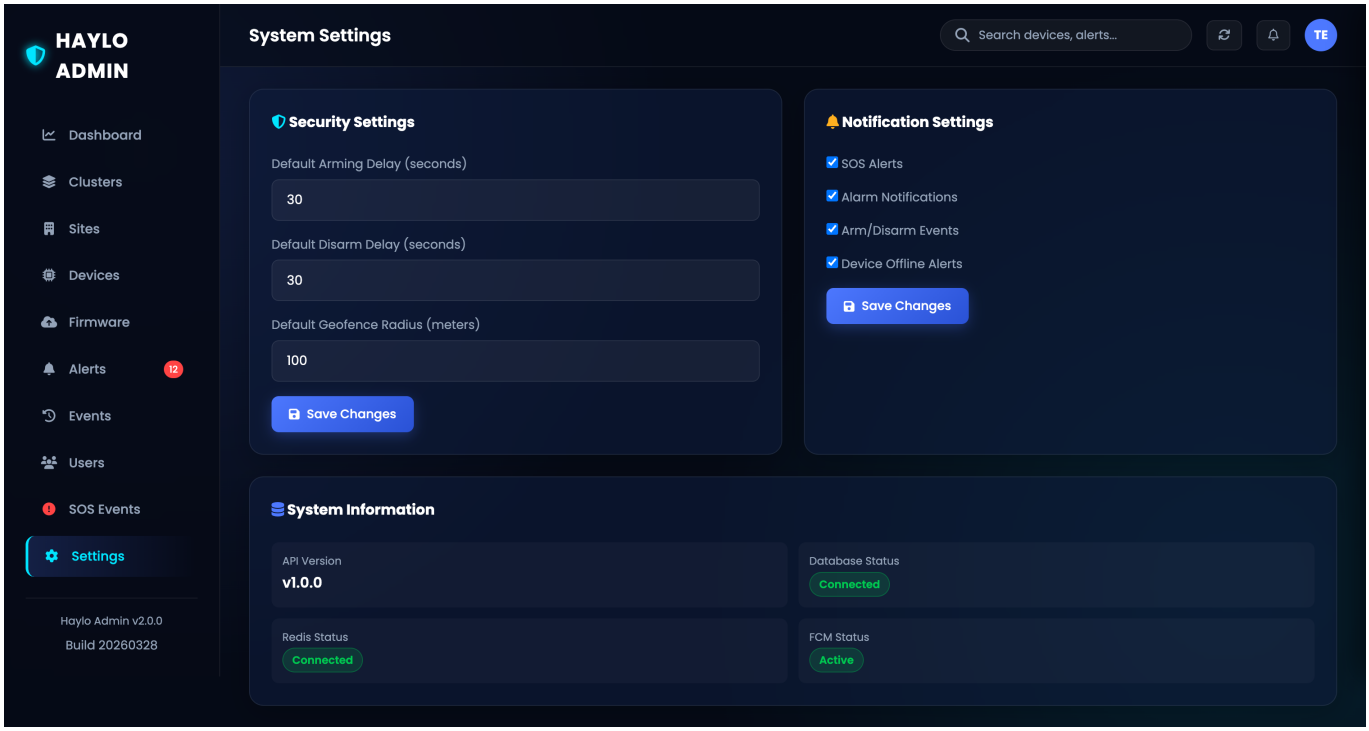


*Figure 12.1 - System Settings*

## Security Settings

- Default Arming Delay (seconds): Time delay before the system arms after activation (default: 30)
- Default Disarm Delay (seconds): Time delay before disarm takes effect (default: 30)
- Default Geofence Radius (meters): Radius for geofence-based auto arm/disarm (default: 100)

## Notification Settings

- SOS Alerts: Enable/disable push notifications for SOS events
- Alarm Notifications: Enable/disable notifications for alarm triggers
- Arm/Disarm Events: Enable/disable notifications for arm/disarm activities
- Device Offline Alerts: Enable/disable notifications when devices go offline

## System Information

- API Version: Current backend API version
- Database Status: Connection status to MariaDB
- Redis Status: Connection status to Redis cache
- FCM Status: Firebase Cloud Messaging status for push notifications

# 13. Role-Based Access Control (RBAC)

Haylo implements a three-tier RBAC system to control access to features based on user roles.

## Role Definitions

| Role | Description |
|---|---|
| Super Admin | Full system access. Can manage all clusters, sites, devices, users, and settings. |
| Cluster Admin | Manages assigned clusters and their sites/devices. Cannot manage other admins. |
| Operator | Mobile app user. Can arm/disarm bound devices and view alerts. No admin access. |

## Permission Matrix

| Feature | Super Admin | Cluster Admin | Operator |
|---|---|---|---|
| Dashboard | Yes | Yes | No |
| Cluster Management | Full | View Own | No |
| Site Management | Full | Own Clusters | No |
| Device Management | Full | Own Clusters | Bound Only |
| Firmware Management | Full | View | No |
| Security Alerts | All | Own Clusters | Bound Devices |
| Event Logs | All | Own Clusters | Own Events |
| User Management | Full | No | No |
| SOS Events | All | Own Clusters | Own Events |
| System Settings | Full | No | No |

## Data Hierarchy

Haylo organizes data in a hierarchical structure:

```
Cluster (Organization/Region)
  -> Site (Physical Location)
    -> Device (IoT Gateway Controller)
      -> Sensors / Zones
```

Users are bound to clusters (for admins) or directly to devices (for operators). This ensures data isolation between different organizational units.