Alarms System Settings

> The Alarms System Settings feature allows administrators to configure and manage automated system alerts. Its primary purpose is to notify administrative and field enforcement staff of critical information regarding specific users, vehicles, or general events, thereby improving operational awareness and security. This article is intended for OperationsCommander (OPSCOM) administrators responsible for backend configuration and enforcement operations.

Setup and Configuration

This feature is a core administrative tool used to define the active alerts that trigger within the system and on field enforcement devices.

Admin Side: Administrators must have the appropriate system role permissions enabled to access and configure these settings.

1. Hover over **System Configuration** and click **Alarms System Settings**.
2. Review the active alarm categories and select the specific type you wish to configure or manage.
3. Save any modifications to ensure they immediately propagate to the database and sync with active handheld devices.

Using this Feature

Administrators can use this feature to categorize and manage three distinct types of system alarms.

Available Alarm Types

- **People:** Configure alarms that are tied directly to user profiles. This is commonly used to flag banned individuals, VIPs, or users with a history of severe parking infractions or unpaid violations.
- **Plate/Vehicle:** Configure alarms that are tied directly to specific license plates or registered vehicles. This ensures that field enforcement officers are immediately alerted if they scan a scofflaw, a stolen vehicle, or a plate associated with a suspended permit.
- **Generic:** Configure general alarms for broader system use that do not strictly tie to a single user profile or specific vehicle record.

> Alarms configured in the backend sync directly to the handheld units used by enforcement staff. When an officer searches a flagged plate or user profile, the Android device will prominently display the alert on the screen so the officer can take immediate action.

Best Practices and Considerations

- **Standardize alarm descriptions: Ensure that all configured alarms include clear, concise instructions for responding staff.** Field officers need to know exactly what action to take when an alarm triggers (e.g., "Do not approach, call dispatch immediately" versus "Issue a standard warning").
- **Prevent alert fatigue: Regularly review active alarms and remove those that are no longer applicable.** Keeping hotlists and

active alarm triggers clean ensures that enforcement officers take alerts seriously when they do appear, rather than habitually dismissing them.

- **Restrict configuration access: Organizations should strictly limit which administrators have the permission to create or modify system alarms.** Tightly controlling this backend access prevents the system from becoming cluttered with unnecessary, duplicate, or poorly defined alerts.

Revision #8
Created 22 May 2024 08:11:34
Updated 13 July 2026 10:54:03