OperationsCommander Vehicle and People Alarms

OperationsCommander works hard to maintain an up to date product wiki! If you have any questions or if you feel something is missing, post about it in the community.

- Generic Alarms
- People Alarms
- Plate and Vehicle Alarms
- The Differences Between Alerts, Plate, Vehicle Alarms and DNTT

Generic Alarms

> Generic Alarms provide a flexible notification system for various non-specific alerts, often originating from external system integrations or unknown user and vehicle IDs. The primary purpose of this feature is to help administrators capture and manage unprofiled activities or external system events within a single, actionable feed. This article is intended for OperationsCommander (OPSCOM) administrators responsible for monitoring dispatch alerts and configuring system integrations.

Setup and Configuration

To utilize generic alarms, administrators must configure the baseline system settings and assign the appropriate viewing permissions to administrative roles.

System Settings

1. Hover over **System Configuration** and click **System Settings**.
2. Navigate to the **Alarms** tab to configure the following settings:
   - **Generic Alarm Append Threshold**: Define the number of minutes before an alarm will create a new dispatch log entry instead of appending to an existing one.
   - **Generic Alarm Dispatch SubID**: Set a specific subID to maintain consistency across all generic alarms.
   - **Allowed Alert Emails**: Enter the email addresses of the specific external systems that are authorized to populate alerts into OPSCOM.

Setting up Alarm Permissions

Administrators must have the appropriate dispatch permissions enabled to view and interact with alarms.

1. Hover over **System Configuration**, click **Admin Management**, and click **Manage Roles**.
2. Click the **Permissions** button next to the administrative role you wish to modify.
3. Scroll to the **Dispatch** category within the Editing Permissions screen.
4. Enable the checkboxes for permissions related to alarms, such as **View Alarms**, **Clear Alarms**, and **Add Alarm Comment**.
5. Click **Save Permissions** at the bottom of the page to apply the changes.

Using this Feature

Generic alarms streamline incoming alerts by parsing external data and grouping repetitive notifications.

How Generic Alarms Get Pushed to the System

Generic alarms are typically triggered by two main mechanisms:

- **Unknown Student/Staff Number**: If a People Alarm is sent to the system featuring a student or staff number that does not exist in the OPSCOM database, the alert is automatically categorized as a generic alarm. The resulting message will include details passed from the access point.
- **ITS-Networking Alerts Systems**: Organizations can integrate their external IT or networking alert systems with OPSCOM. An email alert is pushed from the external system, which OPSCOM parses to issue a

generic alert. This is frequently used for stolen device alerts, where the external system provides the MAC Address and incident details.

> Integration with ITS-Networking Alert Systems requires specific configuration by the OPSCOM Team before it can be utilized. Please contact support to discuss setup procedures and potential recurring fees.

Dispatch Logs and Alert Rollups

To prevent notification fatigue and keep the alert feed actionable, OPSCOM manages high volumes of alerts using a rollup feature.

- **Dispatch Logs**: The system automatically generates a dispatch report the moment an alert is received. If a valid incident ID was passed to OPSCOM alongside the alert, the incident is automatically linked to this dispatch log.
- **Alert Rollups**: If the exact same alert (e.g., the same MAC address) is triggered multiple times within a 30-minute timeframe of the initial alert, all subsequent records are rolled up and added to a single dispatch log record.

Clearing and Viewing Alarms

Administrators can manage their active alerts directly from the personal dashboard.

1. Hover over the **bell icon** located at the top-right of your screen to display a list of current active alerts.
2. Click a specific alert from the list to reveal the available actions.

3. Click **Go To Entry** to navigate directly to the Dispatch Log Report and review the specific details of the alert.
4. Click **Clear Alarm** to acknowledge the alert and remove the icon from your personal dashboard view.

> Clearing an alarm from your dashboard does not delete the corresponding dispatch log record, which remains securely accessible for historical tracking. Note that clearing an alarm only removes it from *your* account; other administrators will continue to see the alert until they clear it themselves.

Best Practices and Considerations

- **Monitor generic alarms regularly: Administrators should routinely check generic alarms**, as they often indicate unprofiled physical activity or system-level issues that require immediate attention.
- **Establish consistent alerting protocols: Organizations should develop internal business rules detailing how different types of generic alarms should be responded to** by the administrative team.
- **Define clear integration parameters:** When integrating with external ITS systems, ensure clear communication with the OPSCOM Team during setup to strictly define your required alert types, data formats (e.g., MAC Address, Incident ID), and desired actions.
- **Analyze dispatch logs:** Leverage the Dispatch Log Report to spot trends in generic alarms, identify recurring security issues, and audit

team responses over time.

People Alarms

> People Alarms provide a critical safety and monitoring feature by allowing administrators to flag specific user profiles with alerts. When an event associated with a flagged user occurs, the system triggers a visual alarm, notifying relevant administrators to take appropriate action. This article is intended for OperationsCommander (OPSCOM) administrators responsible for monitoring user activity, safety protocols, and system alerts.

Setup and Configuration

Before administrators can effectively use the alarm system, the necessary baseline settings must be established and dispatch permissions must be assigned to the correct administrative roles.

System Settings Configuration

1. Hover over **System Configuration** and click **System Settings**.
2. Navigate to the **Alarms** tab.
3. Configure the **People Alarm Append Threshold** to set the number of minutes before an alarm will create a new dispatch log entry instead of appending to an existing one.
4. Configure the **People Alarm Dispatch SubID** to establish consistency across your logs.
5. Enter the allowed email addresses into the **Allowed Alert Emails** field to specify which external systems can populate alerts into OPSCOM.

Setting up Alarm Permissions

1. Hover over **System Configuration**, click **Admin Management** and click **Manage Roles**.
2. Click the **Permissions** button next to the administrative role you wish to modify.
3. Navigate to the *Dispatch* category within the Editing Permissions screen.
4. Enable the **View Alarms**, **Clear Alarms**, and **Add Alarm Comment** checkboxes.
5. Click the **Save Permissions** button at the bottom of the page to apply the changes.

Adding People Alarms to Users

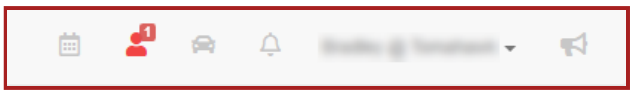
1. Hover over **User Management** and click **User Search**.
2. Search for and select the specific user you wish to flag.
3. Click the **Edit** button next to the **Basic Profile Information** section to open the Edit User Profile window.
4. Enable the **People Alarm** toggle.
5. Enter a specific, actionable note in the **Alarm Comment** field.

> The **License Plate Alarm** and **Plate Alarm** messages will both share this exact same comment. Additionally, even if a user's profile does not have alarms explicitly toggled on or an alarm comment associated, the system will still generate an alert if an API call for a specific student/staff number triggers an alarm.

Using this Feature

Administrators view and manage active alarms and dispatch logs directly from the top-right panel on the administrative dashboard.

Viewing and Managing Alarms



1. Locate the alarms panel in the top-right corner of the screen to view active notifications.
2. Check the generic alarms section, indicated by a **bell icon**, for alerts routed from an API call containing an unknown student or staff account number.
3. Locate the specific alarm in the panel and click the clear option to dismiss the notification from your active view once it has been addressed.

> Clearing an alarm only removes the alert from the specific administrator who cleared it. The alarm will remain visible for all other administrators until they choose to clear it for themselves. Cleared alarms can still be accessed and reviewed from the *Dispatch Log Report* for historical reference.

Visual Cues and Status Indicators

- **Alarm Rollups:** All alarms associated with a specific user profile or license plate are automatically consolidated into a single *Dispatch Log* entry if the alarm is triggered within 30 minutes of the very first alarm related to that profile/plate. This prevents a large number of individual, repeated alarms from flooding the system. If more than 30 minutes

pass, a completely new dispatch record is generated.

Best Practices and Considerations

- **Clear Alarm Comments: Always use concise and actionable alarm comments** (e.g., "Student requires escort," "High-risk individual"). This ensures rapid understanding and an appropriate, immediate response from other administrators.
- **Role-Based Notifications:** Ensure that only administrators who are actively responsible for responding to people alarms have the correct dispatch permissions configured to avoid unnecessary clutter for non-security staff.
- **Timely Clearing: Encourage your team to clear alarms immediately once they have been addressed.** This keeps the active alarm panel relevant and significantly reduces notification fatigue.
- **Integration with Protocols:** Integrate the use of People Alarms closely with your organization's established emergency or response protocols. Ensure all relevant staff know exactly what actions to take when a specific type of alarm is triggered.
- **Regular Review of Dispatch Logs:** Periodically review the *Dispatch Log Report* to monitor alarm trends, identify recurring issues, and ensure the overall effectiveness of your team's response.

Plate and Vehicle Alarms

> The OperationsCommander (OPSCOM) alarm system provides critical real-time notifications for specific events, such as when a flagged vehicle is scanned or a user triggers a security alert. Its primary purpose is to help administrators and field officers rapidly identify and respond to vehicles of interest. This article is intended for OPSCOM administrators and details how to configure permissions, attach, manage, and clear plate and vehicle alarms for both profiled users and unprofiled vehicles.

Setup and Configuration

To utilize plate and vehicle alarms, administrators must configure the baseline system settings and assign the appropriate dispatch permissions to administrative roles.

System Settings

1. Hover over **System Configuration** and click **System Settings**.
2. Navigate to the **Alarms** tab.
3. Configure the **Vehicle Alarm Append Threshold** to set the number of minutes before a new alarm creates a new dispatch log entry instead of appending to an existing one.
4. Configure the **Plate Alarm Dispatch SubID** to establish consistency across your dispatch logs.
5. Enter the approved email addresses into the **Allowed Alert Emails** field to specify which external systems are permitted to populate alerts into OPSCOM.

Setting up Alarm Permissions

1. Hover over **System Configuration** and click **Admin Management** then **Manage Roles**.
2. Click the **Permissions** button next to the administrative role you wish to modify.
3. Navigate to the **Dispatch** category within the Editing Permissions screen.
4. Enable the **View License Plate alarms**, **Receive License Plate alarms via email**, **View People alarms**, and **Receive People Plate alarms via email** checkboxes.
5. Click the **Save Permissions** button at the bottom of the page to apply the changes.

Using this Feature

Plate alarms are triggered automatically whenever a flagged license plate is scanned or read by the system.

Understanding Plate Alarms

Alarms will trigger from the following sources:

- **Fixed Cameras:** Entrance and exit cameras scanning a lot.
- **Handheld Violation Entries:** Manual citation entries by officers in the field.
- **LPR Camera Reads:** Both mobile and static License Plate Recognition systems.

When a Plate Alarm is triggered, an alert appears in the OPSCOM system, and an audible ding sounds for officers using mobile LPR units. If a fixed camera triggers the alarm, the specific camera's name will be listed in the alert.

> Manually chalking vehicles from the handheld unit does not trigger an alert. Only LPR reads and violation entries initiate the alarm sequence.

Attaching an Alarm to a Plate Without a Profile

Plates can exist in the system without a full user profile if they are initially entered via a new violation, a violation warning, a chalking record, or an incident report.

> If a plate only has a chalking record associated with it, you must issue a violation to it or link it to an incident to access the vehicle information fields required to add an alarm. Chalking records alone do not provide direct edit access to vehicle details.

1. Hover over **Violations** and click **Vehicles** then **Search by Plate**.
2. Enter the target plate and execute the search.
3. Click the **Vehicle Info** icon next to the search result.
4. Click the **Edit Vehicle** button.
5. Enable the **Vehicle Alarm** checkbox.
6. Enter an actionable note in the **Alarm Comment** field.
7. Click the **Update Vehicle** button to apply the alarm.

Adding Plate Alarms to Specific Profiled Plates

1. Hover over **User Management** and click **User Search**.
2. Search for and select the user's profile.
3. Click the **Vehicles** tab within their profile.
4. Click the target plate to open the vehicle information window.
5. Click the **Edit Vehicle** button.

6. Enable the **Vehicle Alarm** checkbox.
7. Enter your note in the **Alarm Comment** field.
8. Click the **Update Vehicle** button.

Adding a Plate Alarm to All Vehicles on a User Profile

You can rapidly apply a vehicle alarm to every vehicle associated with a user directly from their primary profile settings.

1. Hover over **User Management** and click **User Search**.
2. Search for and select the user's profile.
3. Click the **Edit** button next to the Basic Profile Information section.
4. Enable the **Plate alarm** checkbox.
5. Enter your alert message in the **comment** field.
6. Click the **Update** button to apply the alarms.

> The People Alarms and License Plate Alarms for this user will share the exact same message if both are enabled simultaneously on the user's profile

---

Best Practices and Considerations

- **Clear and Concise Alarm Comments: Always use brief, highly actionable comments** (e.g., DO NOT APPROACH - WARRANT, LOST/STOLEN PERMIT, CONTACT OWNER). This ensures essential information is conveyed immediately to officers and administrators without ambiguity.

- **Understanding Alarm Roll-Up:** Multiple alarms triggered for the exact same plate or profile are automatically rolled up into a single dispatch log entry within a 30-minute window. This prevents redundant notifications from flooding the system during an active event.
- **Permission Management: Ensure that only authorized and trained personnel have the ability to set and clear alarms** due to the critical nature of these alerts.
- **Regular Review:** Periodically review active alarms and dispatch logs to ensure field officers are responding timely and to manually clear alarms that are no longer operationally relevant.

The Differences Between Alerts, Plate, Vehicle Alarms and DNTT

> The OperationsCommander (OPSCOM) system provides distinct flagging features—Alerts, Plate and Vehicle Alarms, and Do Not Ticket or Tow (DNTT) statuses—to help administrators and field officers identify specific vehicles during patrols. Understanding the operational differences between these statuses ensures that vehicles are appropriately monitored or properly exempted from enforcement. This article is intended for OPSCOM administrators responsible for managing vehicle profiles and dispatch operations.

Setup and Configuration

These flagging tools are configured directly on individual vehicle profiles within the administrative portal.

Configuring DNTT

The **DNTT** feature allows administrators to schedule enforcement exemptions and restrict them to specific physical locations.

1. Navigate to the relevant **Vehicle Profile** in the administration portal.
2. Locate the **DNTT** configuration section.
3. Enter the **Start Date** and **End Date** to define the exact validity period of the exemption.
4. Specify the applicable **Location** if the exemption is site-specific.
5. Click the **Save** button to apply the status.

Configuring Alerts and Alarms

Alerts and Alarms are general security and monitoring flags that are not limited by schedule or location.

1. Navigate to the relevant **Vehicle Profile**.
2. Locate the **Alerts/Alarms** configuration section.
3. Enter the necessary details or select the appropriate alarm type from the drop-down menu.
4. Click the **Save** button to activate the flag.

> Unlike **DNTT** statuses that expire based on a schedule, standard Alerts and Alarms remain active indefinitely until they are manually removed by an administrator.

Using this Feature

Administrators and enforcement personnel interact with these features primarily through handheld scanning devices or License Plate Recognition (LPR) cameras in the field.

Visual Cues and Status Indicators

- **DNTT Status:** When a vehicle with an active **DNTT** status is scanned, a red exclamation mark icon appears on the handheld device screen. No audible alarm will sound, allowing the officer to silently bypass the vehicle.
- **Alerts and Alarms:** When a vehicle with an active Alert or Alarm is scanned by a handheld device or detected by an LPR camera, the system triggers an immediate visual notification and an audible alert to draw the officer's attention.

Available Actions

- **Dispatch Logs:** Once an Alert or Alarm is triggered in the field, it can be converted into a Dispatch Log. This allows the security team to actively track, investigate, and document the resolution of the alert.

Best Practices and Considerations

- **Define Clear Business Rules: Organizations should establish clear policies regarding who has the authority to apply a DNTT status** and the specific circumstances under which it is granted (e.g., medical exemptions, maintenance vehicles, VIP guests).
- **Maintain Accurate Records: Regularly review active Alerts and Alarms** to ensure that outdated or resolved flags are removed. This prevents notification fatigue and unnecessary alerts during standard enforcement activities.
- **Utilize Dispatch Logs: Always convert triggered Alerts into Dispatch Logs** to maintain a comprehensive and permanent audit trail of how security personnel responded to the field notification.