Alarms

Information related to different alarms.

- [Generic Alarms](#)
- [People Alarms](#)
- [Plate and Vehicle Alarms](#)
- [The Differences Between Alerts, Plate and Vehicle Alarms and DNTT](#)

Generic Alarms

Generic Alarms in OPS-COM provide a flexible notification system for various non-specific alerts, often stemming from external system integrations or unknown user/vehicle IDs. This article details how to configure administrator permissions to view these alarms, explains how generic alarms are triggered and rolled up into dispatch logs, and guides administrators on viewing and clearing them from their dashboards.

Setup & Configuration

System Settings

There are a number of system settings you can change on the **Alarms** tab.

- **Generic Alarm Append Threshold -** 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 -** You can set the subID for consistency.
- **Allowed Alert Emails** - You enter the addresses of the systems that will be populating alerts into OPS-COM. To add recipients of alerts, use the [setting in this wiki article.](#)

To enable administrators to view and manage alarms, proper dispatch permissions must be configured for their roles.

Setting up Alarm Permissions

1. Click **System Configuration, Admin Management** and click **Manage Roles**.
2. Select the administrative role you wish to modify by clicking its **Permissions** button.
3. Within the **Editing Permissions** screen, under the **Dispatch** category, select the permissions related to alarms (e.g., **View Alarms**, **Clear Alarms**, **Add Alarm Comment**).
4. Click **Save Permissions** at the bottom of the page when you are finished.

Using this Feature

How Generic Alarms Get Pushed to the System

Generic alarms can be triggered by several mechanisms:

- **Unknown Student/Staff Number**: If a People Alarm is sent to the system with a student or staff number that does not exist in the OPS-COM database, the alert will be categorized as a generic alarm. The message will include details from the access point or any other provided information.
- **ITS-Networking Alerts Systems**: Some clients integrate their ITS (Information Technology Services) or networking alert systems with OPS-COM. In this scenario, an email alert is pushed from the external system to OPS-COM, which then parses it and issues a generic alert. Clients often utilize this for stolen device alerts, where the external system provides the incident and MAC Address.

> This specific integration with ITS-Networking Alert Systems must be set up and configured by the OPS-COM Team before it can be used. There may be setup and recurring fees associated.

Dispatch Logs and Alert Rollups

To prevent the system and administrators from being overwhelmed by a large volume of alerts, OPS-COM implements an alert rollup feature.

- **Dispatch Logs**: Once an alert is received, the system automatically creates a **dispatch report**. If a valid incident was passed to OPS-COM with the alert, the incident will be automatically linked to this dispatch log.
- **Alert Rollups**: If the same alert (e.g., for the same MAC address or incident) is triggered multiple times within a **30-minute timeframe** of the first alert, all subsequent log records for that alert will be **rolled up and added to a single dispatch log record / alert**. This keeps the alert feed concise and actionable.

Clearing/Viewing Alarms

Administrators have the ability to manage the alerts displayed on their personal dashboard.

1. To view active alarms, hover over the **bell icon** at the top-right of your screen. This will display a list of current alerts.
2. From this list, you can select a specific alert. You will then see two options:
   - **Go To Entry**: Clicking this will take you directly to the **Dispatch Log Report** and search for the specific alert, allowing for detailed review.
   - **Clear Alarm**: Clicking this will remove the alert icon from the top-right of your screen, indicating that you have acknowledged it. **Note**: Clearing an alarm only removes the alert for **your account**. Other administrators will continue to see the alert until they clear it for themselves.

> Clearing an alarm from the dashboard does **not** remove the corresponding dispatch log record. The dispatch log remains accessible for historical tracking and reporting.

Best Practices & Considerations

- **Integration with External Systems**: If integrating with ITS-Networking Alerts Systems, ensure clear communication with the OPS-COM Team during setup to define alert types, data formats (e.g., MAC Address, Incident ID), and desired actions.
- **Monitor Generic Alarms**: Regularly check the generic alarms section, as these can indicate unprofiled activity or system-level issues that require attention.
- **Consistent Alerting Protocols**: Develop internal protocols for how different types of generic alarms should be responded to by your administrative team.
- **Utilize Dispatch Logs for Analysis**: Leverage the Dispatch Log Report to analyze trends in generic alarms, identify recurring issues, or review responses over time.
- **Awareness of Rollup Feature**: Understand that the 30-minute rollup window is designed to prevent notification fatigue. If multiple similar events occur in quick succession, they will appear as a single alert on the dashboard.

People Alarms

People Alarms in OPS-COM 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 outlines how to set up alarm permissions, add people alarms to user profiles, and view/clear these alarms.

Setup & Configuration

System Settings

There are a number of system settings you can change on the **Alarms** tab.

- **People Alarm Append Threshold -** the number of minutes before an alarm will create a new dispatch log entry instead of appending to an existing one.
- **People Alarm Dispatch SubID -** You can set the subID for consistency.
- **Allowed Alert Emails** - You enter the addresses of the systems that will be populating alerts into OPS-COM. To add recipients of alerts, use the [setting in this wiki article.](#)

Before administrators can effectively use the alarm system, the necessary dispatch permissions must be assigned to their administrative roles.

Setting up Alarm Permissions

1. Click **System Configuration, Admin Management** and click **Manage Roles**.
2. Select the administrative role you wish to modify by clicking its **Permissions** button.
3. Within the **Editing Permissions** screen, under the **Dispatch** category, select the permissions related to alarms (e.g., **View Alarms**, **Clear Alarms**, **Add Alarm Comment**).
4. Click **Save Permissions** at the bottom of the page when you are finished.

Adding People Alarms to Users

People Alarms are configured directly within a user's profile.

1. Click **User Management, User Search**
2. Search for and select the user to whom you wish to add a People Alarm.
3. Click the **Edit** button next to their **Basic Profile Information** section.
4. This will take you to the **Edit User Profile** window.

5. Locate the option to toggle the **People Alarm**.
6. **Toggle this option On**. Once toggled, you will gain the ability to add an **Alarm Comment** in the provided field.
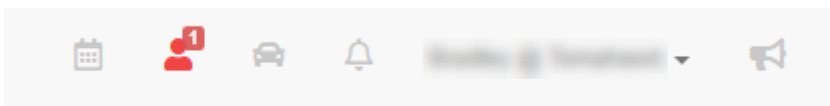
> Note: The **License Plate Alarm** and **Plate Alarm** messages will both share this same comment.

- Even if a user's profile does not have alarms explicitly toggled on or an alarm comment associated, the system will still be alerted if an API call for a specific student/staff number triggers an alarm.

Using this Feature

Viewing People Alarms

Administrators can view active alarms and dispatch logs directly from the top-right panel on the admin side of OPS-COM.

- All alarms associated with a specific user profile or license plate are consolidated into a single **Dispatch Log** entry if the alarm is triggered within 30 minutes of the first alarm related to that profile/plate. This prevents a large number of individual alarms from flooding the system. If more than 30 minutes pass, a new dispatch record will be created.
- If an API call for a person alarm is triggered with an **unknown student/staff account number**, it will be routed to the **generic alarms** section. This is typically indicated by a **bell icon** next to the people and plate alarms section. These generic alarms will also continue to be rolled up into the same dispatch log within 30 minutes of the first alarm.

Clearing Alarms

You can clear an alarm from your view if you no longer need to be notified about it.

- To clear an alarm, locate it in the alarms panel and select the clear option.

> **Important**: Clearing an alarm only removes the alert from the **administrator who cleared it**. The alarm will remain visible for other administrators until they choose to clear it for themselves.

- Even after an alarm is cleared from active view, it can still be accessed and reviewed from the **Dispatch Log Report** for historical reference.

Best Practices & Considerations

- **Clear Alarm Comments**: Use concise and actionable alarm comments (e.g., "Student requires escort," "High-risk individual"). This ensures rapid understanding and appropriate response from administrators.
- **Role-Based Notifications**: Ensure that administrators who are responsible for responding to people alarms have the correct dispatch permissions configured.
- **Timely Clearing**: Encourage administrators to clear alarms once they have been addressed. This helps keep the active alarm panel relevant and reduces notification fatigue.
- **Integration with Protocols**: Integrate the use of People Alarms with your organization's emergency or response protocols. Ensure all relevant staff know what actions to take when an alarm is triggered.
- **Regular Review of Dispatch Logs**: Periodically review the **Dispatch Log Report** to monitor alarm trends and ensure response effectiveness.

Plate and Vehicle Alarms

OPS-COM's alarm system provides critical real-time notifications for specific events, such as a flagged vehicle being scanned or a user triggering a security alert. This article guides administrators on setting up the necessary permissions to view these alarms, as well as how to attach, manage, and clear **Plate Alarms** and **Vehicle Alarms** for both profiles with and without associated user accounts.

Setup & Configuration

System Settings

There are a number of system settings you can change on the **Alarms** tab.

- **Vehicle Alarm Append Threshold -** the number of minutes before an alarm will create a new dispatch log entry instead of appending to an existing one.
- **Plate Alarm Dispatch SubID -** You can set the subID for consistency.
- **Allowed Alert Emails** - You enter the addresses of the systems that will be populating alerts into OPS-COM. To add recipients of alerts, use the [setting in this wiki article.](#)

To enable administrators to view and manage alarms, proper dispatch permissions must be configured for their roles.

Setting up Alarm Permissions

1. Click **System Configuration,** then **Admin Management,** and click **Manage Roles**.
2. Select the administrative role you wish to modify by clicking its **Permissions** button.
3. Within the **Editing Permissions** screen, under the **Dispatch** category, select the permissions related to alarms (e.g., **View Alarms**, **Clear Alarms**, **Add Alarm Comment**).
4. Click **Save Permissions** at the bottom of the page when you are finished.

Using this Feature

Understanding Plate Alarms

Plate Alarms are triggered whenever a license plate with an associated alarm is scanned or read by the system. This includes:

- **Fixed Cameras**: Entrance and exit cameras.
- **Handheld Violation Entries**: By officers in the field.
- **LPR Camera Reads**: Mobile and static LPR systems.

When a Plate Alarm is triggered, a "ding" sound is typically made (for mobile LPR units), and an alert appears in the OPS-COM system. You can also configure an email address to send alarm details to. If a fixed camera triggers the alarm, the camera's name will be listed.

> Manually **Chalking Vehicles** from the handheld does **not** trigger an alert.

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:

- Issuing a **New Violation**, **Violation Warning**, or **Chalking Record** through the handheld or admin side.
- Linking the plate to an **Incident** from the admin side.

If you search for a plate on the handheld that doesn't exist in the system, you'll see a **black plus symbol** indicating the vehicle is new. On the admin side, when issuing a violation or creating an incident, you'll have an option to add a new vehicle and its information, which is where the alarm can be added.

> To add an alarm to a plate without a profile, there must be an existing incident, violation, or warning associated with the plate. If a plate only has a chalking record, you will need to 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 a direct option to view or edit vehicle details.

Steps to Add an Alarm to a Plate Without a Profile

1. **Find the Plate**:
   - Click **Violations,** then **Vehicles,** and click **Search by Plate**.
   - Enter the **Plate** you wish to add the alarm to (e.g., "JROCK").
   - Click the **Vehicle Info** icon next to the search result.
2. **Add the Alarm to the Plate**:
   - The **Vehicle Information** window will open. Click **Edit Vehicle**.
   - Toggle the **Vehicle Alarm** checkbox to **On**. You'll see a checkmark appear.
   - Once toggled, you can add an **Alarm Comment** in the provided field. This comment will be visible to officers and administrators when the alarm triggers.
   - Click **Update Vehicle** to apply the alarm correctly.

When this plate is subsequently scanned by LPR (mobile or fixed cameras), a "ding" sound will be made, alerting officers and allowing them to write a dispatch report if needed.

Adding Plate Alarms to Specific Plates (with User Profile)

If you know the user associated with the plate you wish to alarm:

1. Go to **User Management,** then **User Search**.
2. Search for and select the user's profile.
3. Click the **Vehicles** tab within their profile.
4. You'll see a list of vehicles and their associated plates. Click the **target plate** you wish to alarm. This will bring up a new window with **Vehicle Information**.
5. Follow **Steps 1-3** from "Adding the Alarm to the Plate" (above) to toggle the **Vehicle Alarm**, add a comment, and **Update Vehicle**.

Adding a Plate Alarm to All Vehicles on a User's Profile

You can apply a Vehicle Alarm to all vehicles associated with a user's profile directly from their basic profile information.

1. Go to **User Management,** then **User Search**.
2. Search for and select the user's profile.
3. Click **Edit** next to the **Basic Profile Information** section.
4. On the user's profile page, you should see two checkboxes: **Plate alarm** and **People alarm**.
5. Toggle the **Plate alarm** checkbox to **On**.
6. Add a **comment** that will be used for this alert.
7. Click **Update** to apply the alarms.

> The **People Alarms** and **License Plate Alarms** for this user will share the same message if both are toggled on the user's profile.

Best Practices & Considerations

- **Clear and Concise Alarm Comments**: Use brief, actionable comments that convey essential information quickly to officers and administrators (e.g., "DO NOT APPROACH - WARRANT," "LOST/STOLEN PERMIT," "CONTACT OWNER").
- **Permission Management**: Ensure that only authorized personnel have the ability to set and clear alarms due to their critical nature.
- **System Settings for Alarms**: Review global alarm settings under **System Settings** (e.g., `Alarm Duration`, `Email Address` for alerts, `Generic Alarm Append Threshold`) to ensure they align with your operational needs.

- **Understanding Alarm Roll-Up**: Be aware that multiple alarms for the same plate/profile will be rolled up into a single dispatch log entry within a 30-minute window to avoid flooding the system with redundant notifications.
- **Manually Triggered vs. Automated**: Understand that manual chalking does not trigger alerts, but LPR reads and violation entries do.
- **Regular Review**: Periodically review active alarms and dispatch logs to ensure timely responses and to clear alarms that are no longer relevant to keep the system efficient.

The Differences Between Alerts, Plate and Vehicle Alarms and DNTT

Alarms and DNTT states are similar in regards to be able to put a flag so to speak on a vehicle.

Do Not Ticket or Tow has a specific meaning and convention to it as it was used in police force jargon for years. The acronym is readily recognizable and therefore pretty straight forward. DNTT has the added feature of being able to set a start date and end date for the DNTT privilege to be valid. You can also specify a location in the DNTT.

If a DNTT is in place a red exclamation mark will appear on the handheld read of the plate but no audible alarm will sound.

On the other hand the alarms and alerts on vehicles are not scheduled or associated to a specific location. They are general alarms.
This will trigger an alarm whenever that plate it scanned by the handheld or seen by an LPR camera. These alarms can then be turned into dispatch logs and can be actioned by your Security team.