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.

Revision #4
Created 22 May 2024 09:15:10
Updated 16 June 2025 16:13:15 by Shannon Jones