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.

Revision #8
Created 22 May 2024 09:15:10
Updated 12 August 2026 12:07:18