Viewing an Incident

> The View Incident screen allows OPSCOM administrators to review, edit, and manage comprehensive details of a security event. Its primary purpose is to provide a centralized hub for tracking dispatch logs, linked individuals, related vehicles, and assigned tasks associated with a specific incident. This article is intended for OPSCOM administrators and dispatch personnel responsible for incident management.

Setup and Configuration

Accessing and interacting with the View Incident screen relies heavily on the administrative roles and permissions configured within the system.

To review and modify these settings, hover over **System Configuration**, click **Admin Management**, and click **Manage Roles**.

Viewing Permissions

To simply view an incident page, an administrator must have one of the following baseline permissions:

- **View All Incidents**
- **View Incidents - Self** (Must also be the reporter, Primary Investigator, Case Manager, part of an assigned task group, or assigned directly to a task).

> If an incident is locked, administrators with the **Incident Administrator** permission can view the specific reason for the lock. Administrators with the **View/Edit Confidential Information** permission will see an additional Confidential Info section near the bottom of the page.

Editing Permissions

To access the edit options for an incident, the administrator must meet one of the following requirements:

- Possess the **Custom Permission - Open All** permission.
- Possess the **Edit Incidents** permission.
- Possess the **View Incidents - Self** permission, be the reporting admin, AND the incident must be in an Open state.

Using this Feature

Administrators can navigate to the View Incident screen from multiple areas in the system, including search results, reports, and active dispatch logs. Once on the page, the interface is divided into functional tabs and side buttons.

Managing Tabs and Details

- **Dispatch Logs:** Anyone who can view the incident can view its dispatch logs. Click the **Log** button to manually link a new dispatch entry, or navigate to the **Dispatch Logs** tab to drop a log. You must have the **Add/Drop Dispatch Logs** permission to perform these actions.
- **Linking People:** Use this tab to associate individuals with the incident. Click **show more** to view extended details about a user that are not

displayed on the primary screen.
- **Linking Other Items:** Use the respective tabs to attach vehicles, missing property, and violations to the incident record.
- **Related Incidents:** View this section to see and connect multiple occurrences that share common elements.
- **Checklists:** Certain subcategories require a checklist to be completed before the incident can be closed. If required, a warning will appear while the issue is open. Fill out the details to proceed with closing the incident. You must have the **View All Incidents** or **Incident Administrator** permission to view these checklists.
- **Use of Force Forms:** If the Use of Force setting is enabled (applicable for clients in Ontario), the government-mandated Use of Force forms will be displayed as read-only documents on this page.

Managing Tasks and Assignments

- **Case Manager Assignment:** Assign the incident to a specific manager. You must have the **Assign Incident To Case Manager** permission. The individual being assigned must have either the **Is Incident Case Manager** or **Is Incident Shift Manager** permission.
- **Primary Investigator Assignment:** Assign a lead investigator to the case. You must have the **Edit Incident Tasks**, **Is Incident Shift Manager**, or **Assign Incident To A Different Investigator** permissions (or already be the case manager). The assignee must have the **Be Assigned Tasks Directly** permission.
- **Editing Tasks and Comments:** Add or edit tasks and their associated text. You must be the primary investigator/case manager or have the **Edit Incident Tasks** / **Is Incident Shift Manager** permissions. If you

are only assigned to a task without these broader permissions, you will only see the option to reassign it.

Side Actions and Buttons

The buttons on the right side of the screen dynamically change based on your permissions and the state of the incident:

- **Close/Open Incident:** Toggles the state of the incident. Requires the **Open Incidents** permission.
- **Edit / Edit Summary / View:** Depending on your permissions (e.g., **Edit Incident Summaries**, **Incident Admin**) and the state of the incident (Locked, Open, Closed), this button allows you to modify the full incident or just the summary details.
- **Distribute** and **Email:** Allows you to share the incident report. Requires the **Incident Admin** permission.
- **Download:** Downloads a copy of the incident. Available to any admin who has permission to view the page.
- **Toggle Status:** Switches the state of the record back and forth between read and unread.
- **Delete:** Appears if the incident is eligible to be purged and the administrator possesses the **Delete Incident** permission.

Best Practices and Considerations

- **Audit Permissions Regularly: Organizations should strictly control editing and deletion permissions** to maintain the integrity of incident reports and preserve accurate historical data for legal or security audits.

- **Complete Checklists Promptly:** Ensure required checklists are filled out fully before attempting to close an incident to prevent administrative bottlenecks and ensure compliance with organizational reporting standards.

Revision #12
Created 22 July 2024 09:17:31
Updated 12 August 2026 12:29:39