Operator View User Guide

How to use Verkada Command's new ticketing functionality.

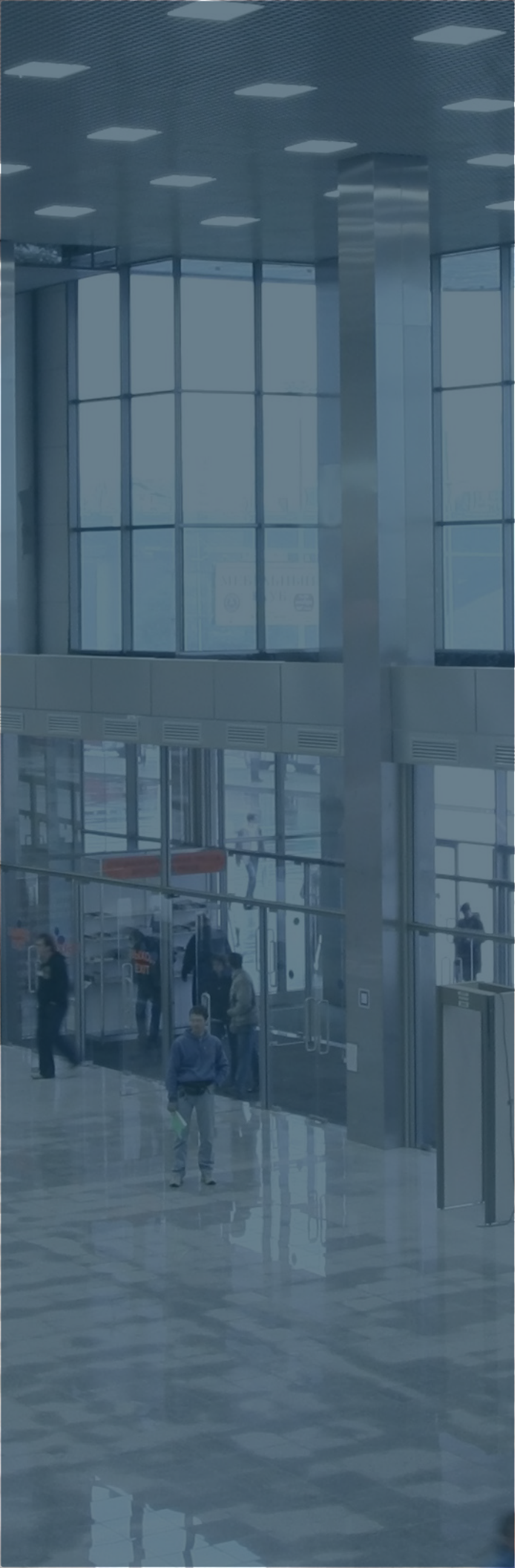


Table of contents

01 Overview

1.1 Summary

Operator view is a ticketing functionality in Command designed to transform the existing alert inbox into a centralized, ticket-based system that tracks alerts through a structured workflow. This guide outlines the essential steps and best practices for configuring alerts and managing tickets within Verkada Command. When an alert is generated, a ticket is automatically created in the operator view queue. This centralizes key system alerts and workflows to provide consistent and structured incident response. Following these guidelines will help empower security teams to work efficiently, maintain a clear audit trail, and respond to incidents with speed and precision.

1.2 Key features and capabilities

1 **Structured workflow and collaboration:**

Operator view enables security teams to investigate, share, and resolve alerts more efficiently from start to finish. Operators can claim incoming tickets to prevent duplicate work and establish a clear chain of custody. The claiming and sharing functionalities increase cross-team collaboration for incident resolution.

2 **Routing and sharing:**

Sharing events allows for collaboration with Command users as well as third parties, such as contracted security teams and law enforcement, providing them access to event footage, details, and response instructions.

3 **Guidance and resolution:**

The system provides context for an event of interest, such as related video footage, location, and event details. It uses standard operating procedures (SOPs) and resolution instructions to guide responders through predefined processes, leading to streamlined operations and improved incident response times. Once appropriate action is taken, security teams can mark incidents as closed, creating a timestamped audit trail from alert to resolution.

4 **Documentation and accountability:**

Operator view includes a dedicated activity log for responders to add notes and photos that automatically document actions taken. This provides visibility and accountability through timestamped activity logs, enabling further optimization of resolution procedures. For deeper analysis, ticket data can be exported to provide insights into operator efficiency and other security metrics.

02 How to Get Started

2.1 Initial setup and configuration

Proper setup is crucial for ensuring teams receive the right alerts at the right time, with clear instructions for a coordinated response.

2.2 Enabling operator view

Command organization admins must activate the operations features within the alert inbox.

1. Navigate to the **alert inbox** (bell icon in the bottom left of Command).
2. Select the **gear icon** to open the alerts settings page.
3. Toggle on the **enable operations option**.

This action will instantly transform the alert inbox into the "alerts and operations" inbox, which adds a new tab called **operator view**, where all ticketed events will be managed.

2.3 Understanding roles and permissions

Users must be granted specific operator view permissions to use the ticketing portal.

Organization admins:

- Have full, unrestricted access by default.
- Can claim, manage, add notes to, release, reopen, and close any ticket, even those claimed by others.

Operator admins:

- Possess the same full permissions as organization admins for operator view.
- This role is ideal for security managers who need full control over operations without having broader system-wide admin privileges.

Operators:

- Have restricted access focused on ticket management.
- Can claim, investigate, and close tickets.
- Cannot close tickets already claimed by other users.
- Cannot access alert configuration or other admin-level settings.

Feature	Organization admins	Operator admins	Operators
Enable operations	✓	✓	x
Manage operators	✓	✓	x
Manage alerts routed to operator view	✓	✓	x
Export ticket CSV	✓	✓	x
Manage tickets owned by other user	✓	✓	x
Claim tickets / close owned-tickets	✓	✓	✓
Add comments to tickets	✓	✓	✓
Add tags to tickets	✓	✓	✓
Share claimed tickets	✓	✓	✓

Granting operator view roles

There are two options for managing permissions and roles for Verkada operations. We recommend creating a Command user group for both operator admins and individuals with operator roles, to simplify the onboarding and offboarding of users.

Option 1	Option 2
Navigate to **admin > users and permissions > users**, select a user, and under Command roles, click edit to assign the operator admin or operator role.	Navigate to **alerts and operations inbox > settings > operators**, find users or groups in the search bar and assign them with the appropriate role.

2.4 Configuring alerts for ticketing functionality

Operator admins or organization admins will be able to route new and/or existing alerts directly into the operations ticketing queue. For new alerts, users will have to select the "+ new alert" option on the alert & operations page, which will open the alert rule modal. After selecting the alert type they wish to configure, users will be able to route the alert to operations. Users can access this same alert configuration modal for existing alerts by editing the alert rule directly. Users can edit alert rules by either navigating to the "manage alerts" page, or by finding it in the left side navigation menu in the alerts and operations page. To successfully route an existing alert to operator view, following the instructions below:

1. From the **alert and operations inbox**, find an alert to be routed into the ticketing system.
2. Select **edit alert** to open its configuration menu.
3. Under the response section, click on **operations**.
4. Toggle on the **route to operations**.
5. Optional-add specific alert-level instructions to guide operators through their response.
6. This alert will now generate a ticket in the operator view queue whenever it is triggered.

Best Practices for Writing Ticket Response Instructions	Example Instructions - Loitering Procedure
When routing an alert, you can add custom ticket instructions to guide operators through their response and investigations. Clear instructions are the key to consistent and effective incident response. Users can create bullet or numbered instruction lists, add hyperlinks, and include phone numbers as part of an event response plan. Other recommendations for response SOPs are: • **Be specific and action-oriented:** Start each step with a command verb (e.g., verify, contact, dispatch, document). • **Define escalation paths:** Clearly state who to contact and what to do if a situation escalates or requires higher-level approval. • **Keep it concise:** Use simple language and bullet points so operators can read, understand, and act quickly under pressure.	1. **Acknowledge and monitor:** Observe the individual's behavior via camera. Note their actions, duration, and if they appear to be surveying the area or waiting for someone. 2. **Assess intent:** After a set time (e.g., 15 minutes) with no clear purpose, dispatch an officer to make contact. 3. **Engage and offer assistance:** The officer should approach professionally and offer assistance. This is a low-conflict way to determine their purpose. 4. **Request departure:** If the individual has no legitimate business on the property, politely inform them they need to leave. Offer to escort them off the premises. 5. **Escalate if needed:** If they become hostile or refuse to leave, escalate to law enforcement and have them escort the individual off site.

2.5 Integrating with New Alarms

Not only can operator view be used to manage any Verkada alert, it can also be used to route New Alarms events into the operators' queue. Org admins or operator admins can enable the integration by navigating to the alerts and operations settings, and toggling on **route alarm incidents**.

- By enabling this feature, all New Alarm raised events will generate a corresponding ticket in the operator view queue.
- Operators will be able to claim incoming alarm raised tickets, review the clip, and investigate the incident.
- Clicking on the **investigate** button will result in the user being redirected to the alarms detail page to see all associated information and details. Users will have the option to dispatch emergency services or resolve the alarm depending on the severity of the incident.

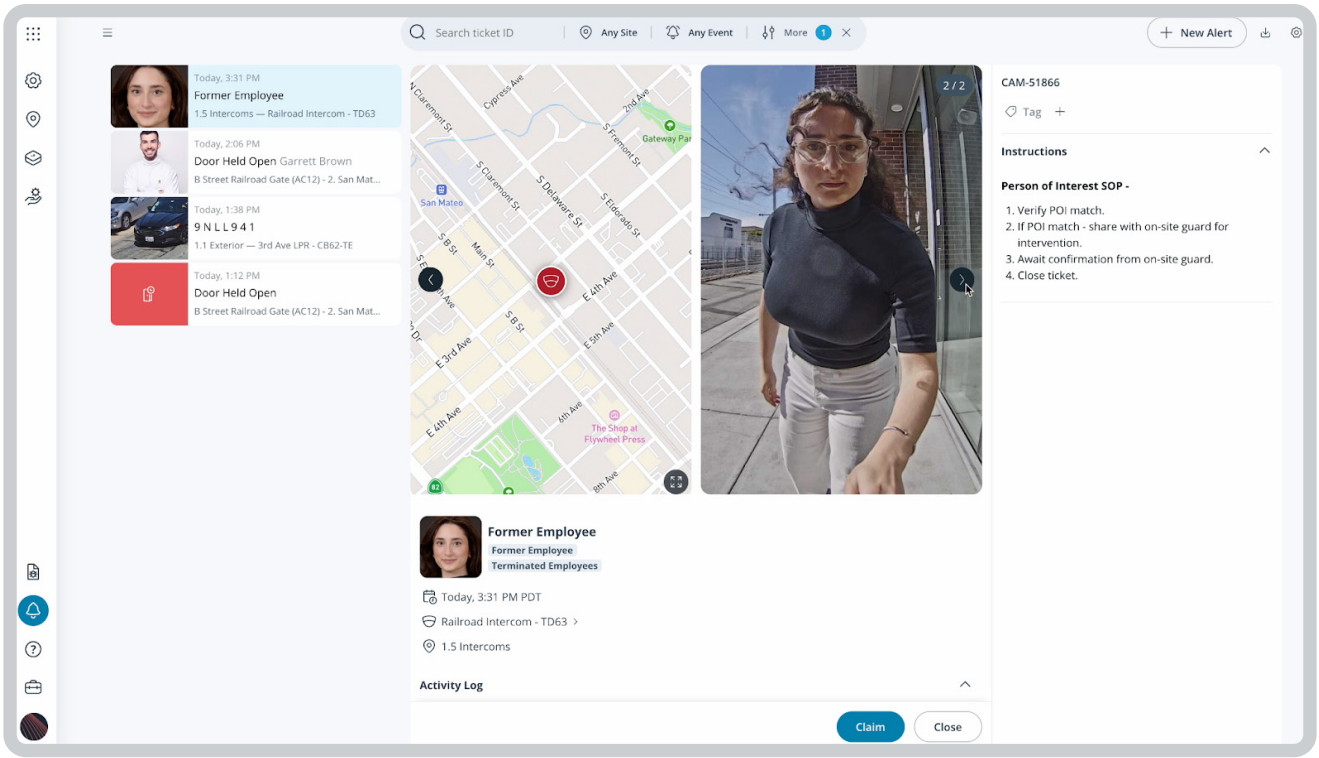
03 Managing Tickets from Start to Finish

Follow this workflow to manage tickets efficiently from creation to resolution.

3.1 Review and claim incoming tickets

When an alert is triggered, a ticket appears in the operator view queue.

- **Review the event:** Click on the ticket to view the event clip, camera, location, and time.
- **Claim the ticket:** Click **claim**. This assigns the ticket to the claiming operator, preventing duplicate work and establishing a clear chain of custody in the audit log. The activity log will update with "claimed by [operator name]."



3.2 Follow the instructions

Use all available tools to understand the full context of the event.

- **Read the instructions:**

  The instructions, which act as the ticket's standard operating procedure, are displayed prominently next to the event video. Follow these steps methodically.

- **Analyze the video:**

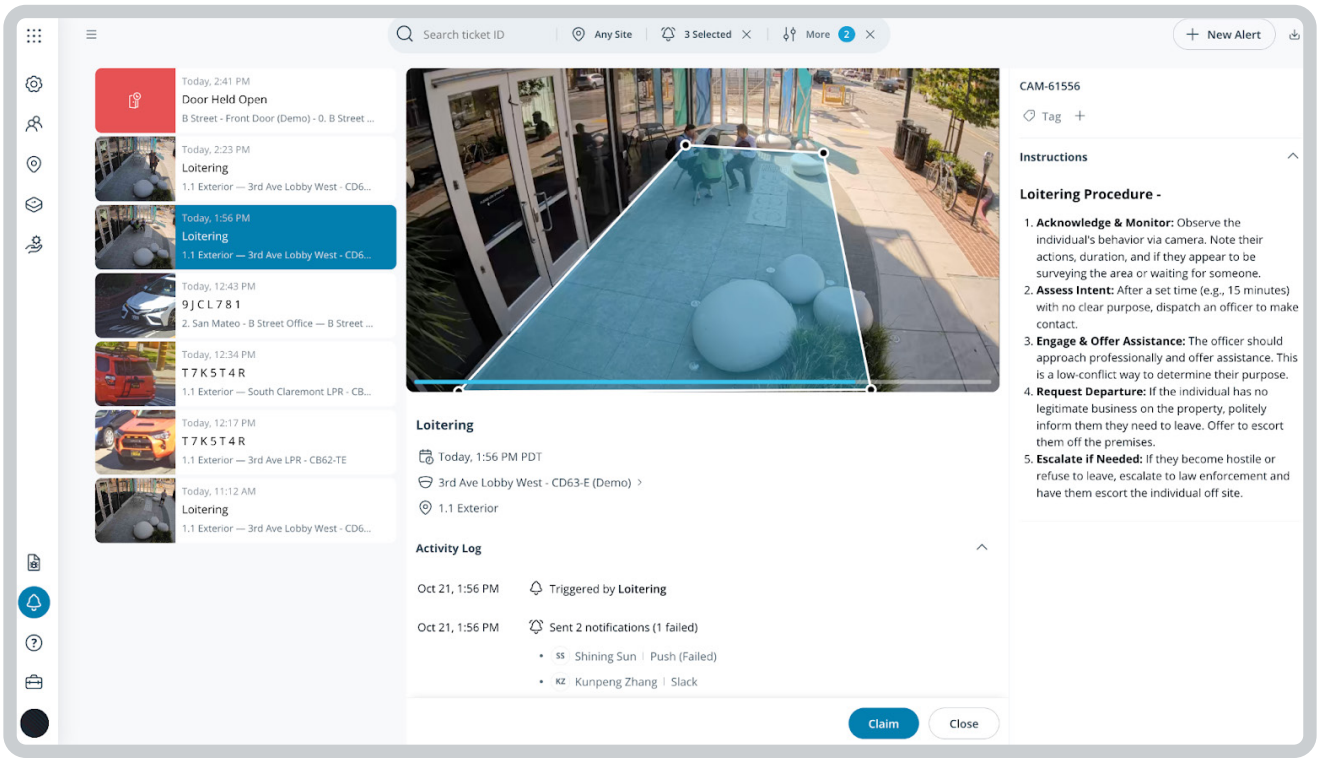
  Review the entire event clip. Click the icon in the bottom right corner to enter the full-screen history player for a more detailed view.

- **Check live feeds:**

  Toggle between the **event clip** and **live** tabs to see what is happening at the location in real-time.

- **Utilize multiple views:**

  For complex alerts (e.g., license plate recognition), switch between the camera feed, map view, and detailed images (like a license plate close-up) to gather all necessary facts.



3.3 Document every action in the activity log

The **activity log** is the official, time-stamped record of the incident. A detailed log is critical for audits, post-incident reviews, and team collaboration.

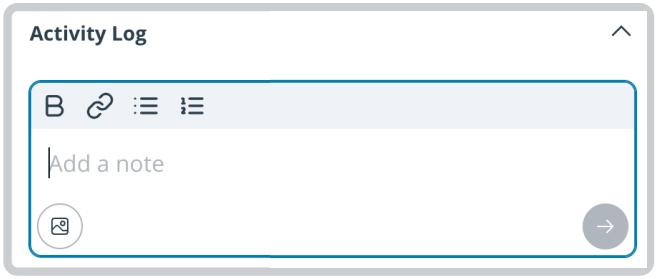
- **Add notes in real-time:**

Use the "add a note" field to document every observation, action taken, and communication made.

» **Good example:** *"Verified LPR match. Dispatched local police."*

» **Good example:** *"Contacted Michael Scott via radio. En route to investigate."*

- To leave a note in the activity log, users must have, at minimum, an operator role set of permissions (see section 2.2 on roles and permissions).



Notes enable responders and customers to track exactly what occurred during a response. All notes are automatically added to the activity log for easy auditability.

3.4 Use tags for organization and filtering

Tags categorize tickets, making it easy to search, filter, and analyze tickets.

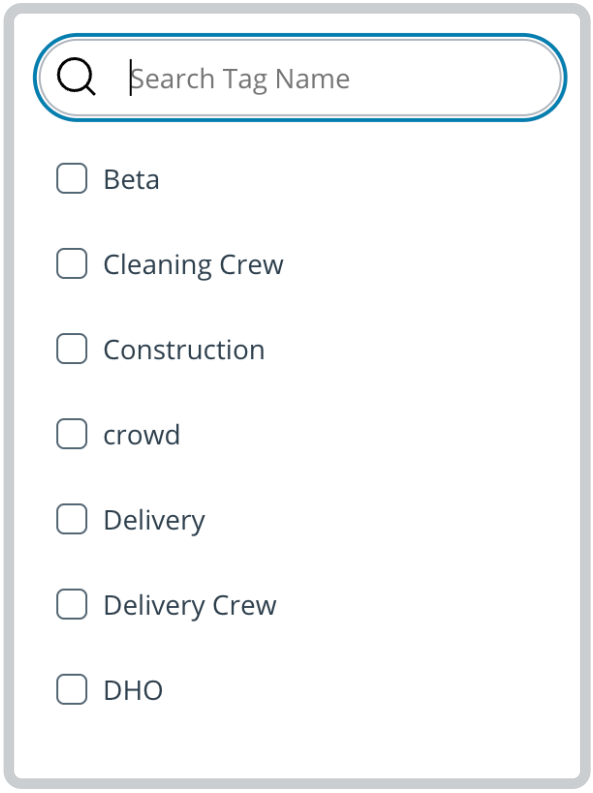
- **Apply relevant tags:**

After taking an action, add a descriptive tag. You can select an existing tag or create a new one.

» **Good example:** *Dispatch, false alarm, guard notified, maintenance required, LPR-BOLO*

- **Establish a standard:**

Create a consistent set of tags for your organization to ensure uniform data collection and reporting.



This is an example of what some helpful tags could be, but make sure to customize your organization's tags based on what is most relevant to your needs.

3.5 Collaborate and share effectively

Use the system to ensure seamless communication and handovers.

- **Communicate via notes:**

The **activity log** serves as a communication tool. Leave notes for other operators or managers to review investigations in real-time.

- **Share tickets:**

Use the **share** button to send a secure link to the ticket to internal colleagues or external partners (e.g., law enforcement, on-site guards) when necessary.

» We recommend leveraging the external contacts feature in Command, available under **admin > users and permissions > contacts**, to make it easy to share relevant tickets with non-Command users.

» Tickets can be shared via email or SMS and allow for efficient collaboration with users that may be thousands of miles away. Real-time pulling of notes as well as instant media uploads allows on-site guards to provide their centralized security team with critical "boots on the ground" information.

3.6 Resolve and close tickets

Once the incident is fully resolved and all actions are documented, close the ticket. This removes it from the active queue and signifies that no further action is required.

3.7 Maintain focus with filters

The ticket queue can become busy. Use filters to manage your view and prioritize your work.

- **Best practice:**
  Filter by **status > in progress** to see only the active tickets that currently require your attention.