

Enforce System Settings

- [System Settings \(Enforce\)](#)
- [Auto-Update](#)
- [Managing Categories](#)

System Settings (Enforce)

The System Settings area in the OPSCOM Enforce application provides centralized control over the handheld's hardware integrations and local behaviors. Its primary purpose is to allow administrators and officers to configure mobile printers, adjust License Plate Recognition (LPR) camera inputs, and customize ticket formatting directly on the device. This article is intended for OPSCOM administrators and field enforcement personnel configuring their handheld units.

Setup and Configuration

While the handheld device offers extensive local customization, several foundational settings must be established in the core administrative portal first.

Admin Side: Administrators must manage the core organization details, unique device identifiers, and the Next Offence Number through the OPSCOM web portal.

LPR Authorization To successfully use the LPR features on a handheld unit, an administrator must first toggle the LPR functionality on within the System Settings of the main Admin Portal.

User Side (Enforcement Staff):

1. Tap the main application menu icon.

2. Tap **System Settings** to open the configuration interface on the mobile device.

Using this Feature

The system settings are divided into four main categories. Enforcement personnel can interact with these menus to tailor the application's performance.

Local Device Settings

This section displays read-only device information pulled directly from the admin portal, including the organization name, country of operation, and the device's unique identifier.

General System Settings

Base settings and information about the device and system.

- **Organization:** "Name of organization connected to the handheld device".
- **Device Unique Identifier:** A string of letters and numbers unique to the device being used.
- **Device Name:** Named identifier for your device.
- **Notice Header:** The automatic header for tickets/notices.
- **Notice Footer:** The automatic footer for tickets/notices.
- **Date Format:** Tap to edit the format in which dates are displayed.
(Sample date: 07/21/2026 09:18:51)

Printer Settings

Tap any item in this list to modify how the device communicates with mobile printers and formats physical tickets.

- **Bluetooth print driver:** Tap to select the specific printer driver (e.g., Zebra).
- **Saved Bluetooth Printer:** Tap to select the physical paired printer hardware.
- **Paper Width:** Tap to set the width of text on the ticket. (must match the paper roll loaded in your printer).
- **Lines Before Ticket:** Tap to adjust the blank buffer space below the printed company logo.
- **Lines per Ticket:** Tap to set total label height for the printed citation. (blank lines added at the bottom if content is too short).

Ticket Layout

Tap any item in this list to modify how the device formats physical tickets.

- **Include Client Name and Notice:** Tap to enable the ticket to be printed with the organization name and ticket header at the top.
- **Include Dotted Header Line:** Tap to enable the ticket to be printed with a separator line below the header.
- **Show Hyphen in Ticket Number:** Tap to enable the ticket to be printed with a hyphen between the device ID and ticket number.

Ticket Content

Tap any item in this list to modify what is included in the printed ticket.

- **Include Warning Value:** Tap to show the dollar amount on printed warning tickets.
- **Include Discount Line:** Tap to show early payment discount amount and deadline on the printed ticket.
- **Include \$0.00 Towing Charge:** Tap to show towing row on the printout even when the charge is \$0.00.
- **Include QR Code:** Tap to print a QR code linking to the ticket payment page on the tickets.
- **QR Code Size:** Tap to select the magnification factor for the printed QR code. (default: 3).

Violations and Chalking

Tap any item in this list to modify the configuration of violations & chalking usage with the handheld device.

- **Violation Retention:** Tap to select the hours to retain violations for reprint after sync.
- **Chalk Units:** Tap to select the units of measurement you will be using for chalking.
- **Chalk to Violation:** Tap to select the the time until a chalked vehicle is considered in violation. (default is 20 minutes).
- **Use Default State/Province:** Tap to pre-select the most common province/state from the last 3 months.
- **Auto-Chalk:** Tap to enable automatic chalking of all plates on every manual search.
- **Multi-chalk Support:** Tap to allow multiple chawks per vehicle during manual chalking.

- **Evidence Photo:** Tap to enable the system to offer to save a photo after issuing a violation.
- **Permit Misuse Window:** Tap to enable alerts when the same permit is seen on a different plate within this window. (0=off).
- **Require Signature:** Tap to require the officers to capture a signature before submitting a violation.
- **Chalk Reset:** Tap to select the distance of your chalking reset. (default is 1000 meters = 3250 feet).

LPR Camera Settings

Tap any items in this list to select the configuration of LPR cameras attached to the device and modify scan behavior.

- **Current:** Shows the current camera(s) connected to the system with the option to edit it or delete it.
- **Scan Network:** Tap to find cameras automatically through the network in the area.
- **Enter Manually:** Tap to type in the IP address and port to connect to the camera.
- **Min. OCR Confidence:** Tap to select the confidence. Plates below selected percentage are ignored.
- **Auto Chalk Vehicles:** Tap to enable automatic chalking of vehicles during LPR scan.
- **Trigger on Inactive Vehicles:** Tap to enable the LPR cameras to trigger an alarm on vehicles marked as inactive.

Best Practices and Considerations

- **Match printer drivers to hardware: Always ensure the Bluetooth print driver matches the exact Bluetooth Printer selected.** If these two settings do not align, the printer will fail to connect or will print unreadable code instead of a formatted ticket.
- **Leverage Auto Synchronization cautiously: Carefully consider your Auto Synchronization Frequency based on your field network reliability.** Setting the sync frequency too high in areas with poor cellular reception can drain the device battery as it repeatedly attempts to connect to the database.

Auto-Update

The Setting Device to Auto Update process allows organizations to configure their handheld devices to automatically download and install application updates. Its primary purpose is to ensure that the OPSCOM Enforce app, along with other critical device software, remains on the latest version without requiring manual intervention from field staff. This article is intended for OPSCOM administrators and IT personnel responsible for provisioning enforcement devices.

Setup and Configuration

This configuration is performed directly within the Play Store. It does not require any backend adjustments within the OPSCOM administrative portal.

Admin Side: Administrators configuring the field devices prior to deployment should ensure the device is connected to a stable network and logged into an active account to access the Play Store settings.

User Side (Enforcement Staff): Generally, field officers do not need to configure this setting if the device was pre-provisioned by administration. If manual configuration is required in the field, follow the steps outlined below.

Using this Feature

Administrators interact with the Play Store settings to dictate how the device handles application updates.

Configuring Auto Update Settings

1. Tap the **Play Store** application on the handheld device to open it.
2. Locate the **Menu** within the app. (For google play you have to press your account icon in the top right corner and scroll down).
3. Tap **Settings** from the slide-out menu.
4. Tap **Auto-update apps** to open the configuration prompt.
5. Select your preferred method of updating: Update all apps over Wi-Fi or mobile data, Update with limited amounts of mobile data, Update over Wi-Fi only or Don't auto-update apps.

Data Charges and Connectivity When selecting the option to update apps with both connections, be aware that the device will utilize whatever network is currently active. If the device is not on Wi-Fi, cellular data charges may apply based on your organization's mobile carrier plan.

Best Practices and Considerations

- **Maintain up-to-date software: Organizations should establish a business rule to keep auto-updates enabled whenever possible.** Allowing the device to update automatically ensures field officers always benefit from the latest bug fixes, security patches, and feature enhancements for the OPSCOM application.
- **Monitor cellular data usage: If your organization uses strict or limited cellular data plans, consider using the Wi-Fi only update option if available on your device's Android version.** This prevents large app updates from exhausting your monthly cellular data allowance while officers are actively patrolling.

Managing Categories

The Incident Categories feature allows organizations to classify and organize different types of incidents, such as security events, parking violations, or maintenance requests. Its primary purpose is to help administrators standardize reporting and dispatching by defining a structured hierarchy of categories and sub-categories. This article is intended for OPSCOM administrators.

Setup and Configuration

This feature is managed entirely within the core OPSCOM administrative portal.

Admin Side: Hover over **Admin Options** and click **Incidents** then **Categories**. This will open the **Edit Categories and Sub Categories** main page.

Automatic Synchronization Handheld devices will automatically inherit the updated category and sub-category lists during their regular background synchronization with the core database.

Using this Feature

Administrators can use this interface to build a custom list of incident types, create granular sub-categories, and define operational rules such as field checklist requirements.

Adding a New Category

1. Scroll to the bottom of the **Edit Categories and Sub Categories** main page.
2. Click the **Add New Category** button.
3. Enter a descriptive name in the **Category Name** text field.
4. Enable the **In-House** checkbox if this incident type is handled strictly internally.
5. Enter a **GIS** number if applicable for spatial tracking and mapping integration.
6. Enable the option to include this category in system reports, if desired.
7. Click the **Save Incident Category** button to finalize and add the new category to the system.

Editing an Existing Category

1. Locate the specific category in the listed items on the main page.
2. Click the **pencil icon** next to the category to open the edit screen.
3. Update the category name or specific configuration details as needed.
4. Click the **Save Incident Category** button to apply your changes to the database.

Managing Sub-Categories

Sub-categories allow you to break down broad incidents into highly specific, actionable events.

1. Click **Sub** next to an existing category on the main list to view its associated sub-categories.
2. Enter a new name in the provided text field to add a new sub-category.
3. Enable the **Required** checkbox under the checklist column if a formal checklist must be completed by the officer when this specific sub-

category is selected in the field.

4. Enable the **Include** checkbox if you want this specific sub-category to be visible in statistical reports.
 5. Click the **Save SubCategory** button to add the new sub-category to the parent group.
-

Best Practices and Considerations

- **Standardize your naming conventions: Organizations should establish a clear and consistent naming convention for all categories and sub-categories.** This prevents duplicate entries and ensures dispatchers and field officers can quickly select the correct option during an active, high-stress incident.
- **Utilize checklists for complex incidents: Enable the checklist requirement for sub-categories that involve multi-step procedures or critical safety protocols.** This ensures field officers follow standard operating procedures when responding to specific incident types, greatly reducing organizational liability.