Handheld Devices and Commons

> The Handheld Devices and Commons section allows OperationsCommander (OPSCOM) administrators to manage and configure the mobile devices used for field enforcement and data collection. Its primary purpose is to centralize device registration, facilitate message broadcasting to field personnel, and manage device-specific settings to ensure accurate and seamless data synchronization.

Setup and Configuration

This feature is a core administrative tool for managing your organization's physical enforcement hardware.

Admin Side: Administrators must have the appropriate system role permissions enabled to access the device management tools. Furthermore, field devices must have the OPSCOM Android application installed and maintain an active network connection to receive configuration updates and pushed messages from the system.

Using this Feature

Administrators can use the device management interface to oversee their fleet of enforcement handhelds, push updates, and register new hardware.

Managing Devices

1. Navigate to the **Handheld Devices** section within your administrative tools.
2. Review the displayed list of currently registered enforcement devices.
3. Select a specific device from the list to view its current synchronization status and configuration details.

Available Actions and Buttons

- **Register Device:** Allows administrators to securely add a new handheld unit to the operational system.
- **Push Message:** Enables administrators to send direct communications, alerts, or system updates to active field personnel.
- **Update Settings:** Allows for the modification of device-specific configurations to ensure seamless operation and data accuracy.

> This page serves as a high-level overview of the Handheld Devices module. For detailed, step-by-step instructions on configuring specific handheld models, installing the application, or troubleshooting synchronization issues, please refer to the Handhelds Devices Settings (Handheld Commons) wiki article.

Best Practices and Considerations

- **Maintain active device lists: Administrators should routinely review the list of registered handhelds and deactivate devices that are lost, broken, or no longer in use.** Keeping a clean device list ensures system security and prevents unauthorized hardware from syncing with your live database.

- **Verify network connectivity: Remind field personnel that devices must be connected to a reliable Wi-Fi or cellular data network to receive pushed messages and settings updates.** If a device is offline, any settings updated in the admin portal will not take effect until the device reconnects and syncs.

Revision #7
Created 16 June 2025 09:52:35
Updated 17 August 2026 13:01:24