

Setup Installation and Maintenance

- [Manual Update or Installation](#)
- [Testing Your WIFI Connection](#)
- [Uninstalling the Application](#)
- [Reinstalling the OPSCOM App](#)
- [Retrieve Local Tablet Backups](#)
- [Connecting as USB Hard Drive](#)
- [Google Account](#)
- [Using the OPSCOM App in DEMO Mode](#)

Manual Update or Installation

The Manual Update or Installation process allows users to install or update the legacy Android enforcement application directly from the Google Play Store. Its primary purpose is to ensure field officers have the latest software version on their handheld devices for optimal performance and access to new features. This article is intended for OPSCOM administrators and field enforcement personnel.

Setup & Configuration

To use the software, the officer's user profile must have the proper permissions granted in the core OPSCOM system before they attempt to log into the mobile application.

Admin Side: Administrators must ensure that field users have the "Wireless handheld" permission enabled.

1. Hover over **System Config** and click **Manage Roles**.
2. Click **Permissions** beside the specific Administrator Role you wish to edit (e.g., Patrol Officer).
3. Click the **Violations** tab.
4. Enable the **Display as Ticket Writer** checkbox.

User Side (Enforcement Staff): Ensure the Android handheld device is connected to a stable Wi-Fi or cellular network before attempting to download or update the application.

Using this Feature

Field personnel can manually check for and install updates using the native Android app store.

Installing or Updating the Application

1. Tap the **Google Play Store** app on the device's Apps screen.
2. Tap the search bar and enter **OperationsCommander** or **OPSCOM**.
3. Tap the **OperationsCommander** app icon to open the installation page.
4. Tap the **Install** button to perform a fresh installation, or tap the **Update** button to perform an in-place update of the existing software.
5. Tap **Accept** when the settings window pops up requesting access to integrated device features. *(Note: On newer tablets, these permission requests may appear during the initial startup of the application instead).*
6. Tap the **Open** button directly within the Play Store, or return to the device's home screen and tap the newly created shortcut to launch the application.

Install vs. Update Tapping the **Install** button performs a fresh installation where a new shortcut and a fresh local database are created. Tapping the **Update** button performs an in-place update, meaning a new database is not created and your existing local data will not be disrupted.

Best Practices & Considerations

- **Always synchronize before updating: It is highly recommended to perform a full manual data sync before proceeding with any**

kind of update. While an update typically will not disrupt existing data, syncing first guarantees that no offline tickets or chalk records are lost during the software transition.

- **Grant all requested permissions: It is critical to grant access to all requested permissions during installation or initial startup.** The OPSCOM application requires these integrations (such as camera, location, and storage) to function correctly in the field.

Testing Your WIFI Connection

The Testing Your WIFI Connection process guides users in diagnosing wireless network stability on Android handheld devices using a third-party application. Its primary purpose is to help identify signal drops and channel congestion that may disrupt real-time communication with the server. This article is intended for OPSCOM administrators and field enforcement staff.

Setup and Configuration

To accurately test your network connection, you must install a specific third-party diagnostic application on your Android handheld device.

Admin Side:

1. Open the Google Play Store on your Android handheld device.
2. Search for and download **WifiAnalyzer (open-source)** by VREM Software Group. This is a free utility application.

Using this Feature

Administrators and staff can use this application to take a precise measurement of their Wi-Fi strength and identify the source channel to aid in troubleshooting.

Monitoring Wi-Fi Strength

1. Open the **WifiAnalyzer** application on your device.

2. **Tap** the hamburger icon (three parallel lines) located at the top left of the screen to open the main menu.
3. **Tap Access Points** to view a graphic representation of your available networks and their current signal strengths.
4. **Tap** the hamburger icon again and select **Channel Graph** to view a visual representation of channel congestion and overlapping network signals.

Visual Cues & Status Indicators

- **Signal Strength Graph:** The signal strength is visually represented as a column of color rising from the bottom of the graph, typically ranging from -100 dBm to -20 dBm.
 - **Reading dBm Values:** Signal strength is measured in negative numbers. The smaller the negative number, the higher (stronger) the signal. Keep in mind that a value closer to zero (e.g., -20 dBm) indicates a much better signal than a lower number (e.g., -100 dBm).
-

Best Practices & Considerations

- **Monitor signal fluctuations throughout the day.** It is highly recommended to check the app periodically, especially when drops in signal occur. Observing how much the signal goes up and down can help pinpoint exactly when connectivity drops.
- **Check channel congestion.** Pay close attention to how many devices or networks are broadcasting on the exact same channel. Too many devices trying to access the same channel simultaneously will create interference and have a severe adverse effect on your connectivity.

strength.

- **Capture data for support. Please provide screen captures of both the Access Points and Channel Graph screens when contacting OPSCOM support.** Having a visual record of the exact dBm reading for your Wi-Fi source and the channel congestion allows the support team to assist you much more effectively.

Uninstalling the Application

The Uninstalling the Application process outlines how to safely remove the legacy OPSCOM Parking Enforcement app and its associated data folders from an Android handheld device. Its primary purpose is to guide users through a standard removal or a full clean data purge to prepare the device for troubleshooting or a fresh installation. This article is intended for OPSCOM administrators and IT support personnel.

Setup and Configuration

Before removing the application, it is critical to ensure that all local data has been safely transferred to the core database.

Admin Side: Administrators should ensure the device has an active network connection and verify that all recent patrol data has successfully synchronized to the backend.

User Side (Enforcement Staff): Field staff must log in to the application one final time and check the **Replication Status** page to ensure all records have been pushed to the server.

Using this Feature

The uninstallation process can be completed natively on the Android device. In the event of a full clean install, residual files must also be deleted using the device's file manager or a connected PC.

Standard Application Uninstall

1. Tap **Settings** from the main Android applications menu.
2. Tap the **General** tab.
3. Tap **Applications** under the Device Manager section to view the installed apps list.
4. Tap the **OperationsCommander** application in the list.
5. Tap **Uninstall** to remove the application from the unit.

Full Clean Install with Data Purge

In some cases, [OPSCOM Support](#) may ask you to perform a full clean install. This requires removing the app (following the steps above) and manually deleting all associated local files to prevent artifacts from affecting the new installation.

Data Loss Prevention If you are uninstalling the software to reinstall it, do not uninstall the software if the **ViolationTransfer** and/or **VehicleTransfer** tables contain data (viewable under **Replication Status**). These tables must be replicated to the server first to avoid permanent data loss and integrity issues.

Delete Files with Handheld Tools

1. Tap the **App Tray** at the bottom right of the home screen display.
2. Tap the **My Files** application.
3. Locate and Tap and Hold the **OPSCOM** folder from the directory list.
4. Tap **Delete** from the pop-up options window.
5. Tap **OK** on the confirmation screen to remove the folder and all its contents.

Delete Files using a PC (USB Connection)

1. Connect the handheld device to your computer via USB.
 2. Open **Windows Explorer** and locate the device under **This PC**.
 3. Click **Tablet** (or internal storage) to view the file content of the device.
 4. Locate the folder named **OPSCOM**.
 5. Right-click the folder and click **Delete** from the drop-down menu to remove the folder and all its contents.
-

Best Practices and Considerations

- **Always verify replication status before uninstalling: Ensure the ViolationTransfer and VehicleTransfer tables are completely empty.** Uninstalling with unsynced data will result in permanent data loss for the organization.
- **Purge files for persistent issues: If the application is crashing frequently, perform the full clean install with a data purge** before reinstalling the OPSCOM Legacy app. This ensures corrupted cache files do not carry over to the fresh installation.

Reinstalling the OPSCOM App

The Reinstalling the OPSCOM App process guides users through completely removing the legacy Android application and preparing the device for a fresh installation. Its primary purpose is to help resolve persistent application issues or update the software when automated updates are unavailable. This article is intended for OPSCOM administrators and field enforcement personnel using the legacy Android application.

Setup and Configuration

Before removing the application, it is critical to ensure that the device is prepared and that no local data is left unsynchronized.

Admin Side: Administrators should ensure the device has a stable Wi-Fi or cellular connection to successfully download the new application package once the old version is removed.

User Side (Enforcement Staff): Enforcement officers must verify that all recent patrol data (such as offline violations or chalk records) has successfully synchronized to the backend database before beginning the uninstallation process.

Using this Feature

The uninstallation process is performed natively through the Android operating system's application manager.

Uninstalling the Application

1. Tap **Settings** from your device's home screen or app drawer.
2. Tap the **General** tab at the top of the settings menu.
3. Tap **Applications** under the **Device Manager** section on the left side of the screen to bring up a list of installed apps on the right.
4. Scroll through the list and tap the **OPSCOM** application.
5. Tap **Uninstall** to remove the application and its base data from the unit.

Data Loss Prevention Never uninstall the application while you have active, unsynced data on your device. Removing the application will permanently delete all local cache files, and any violations that have not been pushed to the main server will be lost.

Reinstalling the Application

Once the application has been successfully removed from the Android device, you must download and install a fresh copy.

1. Please refer to the [Manual Update or Installation](#) article for complete, step-by-step instructions on downloading the APK file and setting up the new application.

Best Practices and Considerations

- **Perform a full clean install for persistent issues: If a simple uninstallation does not resolve application crashes or performance issues, you may need to perform a full clean install.** This involves manually deleting residual OPSCOM folders from

the device's internal storage before reinstalling.

- **Keep the operating system updated: Ensure the Android OS is up-to-date before reinstalling the OPSCOM application.** Installing a fresh version of the app on an outdated operating system can lead to unexpected compatibility issues.

Retrieve Local Tablet Backups

The Retrieve Local Tablet Backups process allows organizations to access and extract offline violation data directly from an Android handheld device's internal storage. Its primary purpose is to recover locally stored violations in the event of a synchronization failure, accidental application uninstallation, or database error before the records are successfully uploaded to the server. This article is intended for OPS-COM administrators and IT support personnel.

Setup and Configuration

Extracting these files requires physical access to the device and a wired connection to a workstation.

Admin Side: Administrators must have a physical USB connection cable and a PC to access the device's internal file system.

User Side (Enforcement Staff): Ensure the Android tablet is powered on and actively unlocked before connecting it to the computer.

Locating a USB Cable If you do not have a dedicated USB data cable, check the tablet's charging unit. Most charging cables feature a detachable USB plug that can be removed from the wall adapter and plugged directly into your PC.

Using this Feature

Administrators must connect the device to a PC, locate the specific application data folder, and transfer the files to OPSCOM support for recovery.

Connecting the Tablet to a PC

1. Connect the tablet to your computer using a compatible USB cable.
2. Unlock the tablet screen so the PC can authorize the connection and read the internal storage.
3. Click the USB connection notification on your PC, or navigate manually through **File Explorer** to **This PC** and open the tablet's internal storage drive.

Locating and Copying Backup Files

1. Navigate through the tablet's internal storage to the following folder path:
Android\data\com.operationscommander.handheld\files\Backups.
2. Select all backup files located within this folder (or the specific files requested by support).
3. Copy the selected files.
4. Paste the files into a new, temporary folder on your local computer's desktop (e.g., "Tablet Backups").

Sharing Backups with Support

Once the files are secured on your local computer, they must be shared with the support team to complete the recovery.

1. Open a web browser and navigate to Google Drive.
2. Click **New** and select **Folder Upload**.

3. Select the temporary backup folder you created on your desktop to begin the upload.
4. Wait for the upload status window in the bottom right corner of the screen to confirm all files have successfully uploaded.
5. Share the uploaded folder with support@ops-com.com and notify the support team that the files are ready for retrieval.

You may also email the backup files directly to support if the overall file size is small enough to attach.

Best Practices and Considerations

- **Unlock the device before connecting:** Always ensure the tablet screen is unlocked before plugging it into the USB port. PCs cannot read the internal file system of a locked Android device due to native security protocols.
- **Clean up temporary files:** Delete the temporary backup folder from your local desktop once the support team confirms successful receipt. This keeps your PC free of unnecessary files and protects sensitive organizational violation data.

Connecting as USB Hard Drive

The Connecting as USB Hard Drive process allows users to physically link their Android handheld device to a desktop computer to access its internal file system. Its primary purpose is to enable the direct transfer, copying, or backup of application data and files (such as local OPSCOM folders) without relying on a network connection. This article is intended for OPS-COM administrators and IT support personnel managing the legacy Android application.

Setup and Configuration

This procedure relies on the native Android operating system and a physical connection to a desktop computer.

User Side (Enforcement Staff): The handheld device requires a physical USB data cable and must have Developer Options enabled within the Android operating system to allow debugging and mass storage access.

Using this Feature

To access the device's file system, you must first enable the correct connection mode on the handheld, then navigate the file structure on your desktop computer.

Enabling Developer Options

If you do not already see a Development option in your settings menu, follow these steps to unhide it:

1. Tap **Settings** from the device's main menu.
2. Scroll down and tap **About phone**.
3. Scroll down to locate **Build number**.
4. Tap **Build number** seven times in rapid succession. A notification will appear confirming that the Developer setting is now unlocked.

Connecting the Device

1. Tap **Settings**, select **Applications**, tap **Development**, and enable the **USB debugging** checkbox.
2. Plug the USB cable into your desktop computer and connect the other end to your Android device. A USB icon will appear in the device's top status bar.
3. Swipe down from the top edge of the Android device screen to reveal the notification shade.
4. Tap **USB Connected** and select the option to mount the device (e.g., **Connect USB storage** or **Mount**).
5. Tap **Ok** to confirm. The Android icon will change color (typically to orange), indicating the phone is now in USB Mass Storage mode.

Accessing Files on the Desktop Computer

1. Open the file explorer on your desktop computer and navigate to the connected devices or removable storage section.
2. Click the newly mounted hard drive letter associated with the Android device.
3. Locate and click the **OPSCOM** folder (sometimes labeled **ParkAdmin**) to browse, copy, or transfer the required files.

Disable Mass Storage Mode Turn off USB hard drive mode on the handheld device immediately when you are finished copying files. Leaving this connection active can cause read/write conflicts and operational issues with the OPSCOM software.

Best Practices and Considerations

- **Use a data-capable cable: Ensure the USB cable you are using supports data transfer.** Some standard charging cables only provide power and will fail to trigger the USB connection prompt on your computer or device.
 - **Safely eject the device: Always safely eject the USB drive from your desktop computer's operating system before physically unplugging the cable.** This prevents data corruption within the OPSCOM folders during active file transfers.
-

Related Video

<https://www.youtube.com/embed/mp07dPusJNA?wmode=opaque>

Google Account

The Google Account configuration process guides users on how to add a Google profile to their Android handheld device. Its primary purpose is to grant access to the Google Play Store for downloading, updating, and troubleshooting the legacy OPSCOM Parking Enforcement app, as well as managing beta releases. This article is intended for OPSCOM administrators and field enforcement personnel configuring their devices.

Setup and Configuration

You will require a valid Gmail email account and password to access the Google Play Store on your handheld device.

Admin Side: Administrators configuring field devices prior to deployment should ensure the device is connected to a stable network and a standardized organizational Google account is available for use.

User Side: Depending on your Android version, the exact naming conventions may vary slightly, but the core steps remain the same.

1. Tap **Settings** from the main menu of your Android device.
2. Tap **Accounts** (or **Users & Accounts**).
3. Tap **Add account** from the settings list.
4. Tap **Google** from the list of available account types.
5. Enter your assigned Gmail email address and password, then follow the on-screen prompts to finalize the login.

Removing an Account If you already see Google in the accounts area and need to switch profiles, you can remove existing Google accounts from the device by tapping **Google** and selecting the remove option before adding the new account.

Using this Feature

Enforcement personnel and administrators use the active Google account to manage app updates, clear system caches, and opt into beta testing directly through the Google Play Store.

Clearing Google Play Cache

Google Play will cache application details for hours to even a day or more. Clearing the cache ensures that the most recent version of the application that is available is accessible to your device.

1. Access your device's native app settings.
2. Tap the **Google Play Store** application.
3. Tap **Storage** or **Storage & cache**.
4. Tap **Clear cache** to remove the temporary data.

Joining or Leaving the Beta Program

At times, new beta (non-production) releases may be offered that address client-reported issues or new functionality. Clients may test the beta versions to ensure issues are resolved and that normal functionality is not disrupted.

1. Navigate to the [Beta Program on Android](#) on your handheld device, or the [Beta Program on the Web](#) on a desktop browser.

2. Scroll down the page to determine your current status under the beta header.
 3. Tap **Join** to enter the program, and tap **Join** (or **Confirm**) a second time when prompted.
 4. Tap **Leave** if you wish to remove yourself from the beta program and no longer receive pre-release updates.
-

Best Practices and Considerations

- **Limit beta testing to specific devices: We recommend that only one device be used for the Beta program as these releases may be unstable.** Testing on a single, dedicated unit ensures normal operations are not disrupted for the rest of your enforcement fleet.
 - **Verify your active profile: Ensure the handheld operates under the specific Google profile intended for beta access.** If you are not sure what account you are using, review the linked accounts under settings within Android. Alternatively, simply follow the beta links above to use whatever profile you are currently logged into.
 - **Clear cache for missing apps: If you cannot see the OPSCOM app or the latest update on the Play Store, clear the Google Play cache immediately.** If issues persist, there are additional troubleshooting steps available for [Google Play Store app visibility issues](#).
-

Related Video

<https://www.youtube.com/embed/INwRDqyk7IA?wmode=opaque>

Using the OPSCOM App in DEMO Mode

The Using the OPSCOM App in DEMO Mode feature allows users to explore and test the legacy OPSCOM Parking Enforcement application without needing to officially register a handheld device. Its primary purpose is to provide a safe, pre-populated sandbox environment for training and familiarizing staff with the software's core functions. This article is intended for OPSCOM administrators and field enforcement personnel.

Setup and Configuration

No formal registration or backend configuration is required to access the demonstration environment.

Admin Side: Administrators do not need to configure specific user permissions or device profiles within the core OPSCOM portal for devices operating strictly in demo mode.

User Side (Enforcement Staff): Enforcement officers simply need to ensure the legacy Android application is successfully installed on their handheld device.

Using this Feature

Enforcement personnel can bypass the standard device registration screen to access a fully functional, pre-populated version of the application for testing purposes.

Accessing Demo Mode

1. Boot up the application after the initial installation on your Android device.
2. Tap **DEMO MODE** on the initial *Device Not Recognized* pop-up screen.
3. Review the sign-in screen. The demonstration username and password credentials will automatically populate.
4. Tap **LOGIN** to access the main index screen and begin testing.

Available Actions and Testing Scope

Once logged into DEMO mode, users can practice various core enforcement actions without affecting live database records. Recommended testing actions include:

- **Searching Vehicles:** Querying by plate or VIN.
- **Searching Permits:** Verifying active and unpaid permits.
- **Searching People:** Looking up user profiles and associated vehicles.
- **Virtual Chalking:** Practicing the digital tire chalking workflow.
- **Issuing Violations:** Generating both person and plate-based citations.

Key Information Displayed: Test Data Profiles

The demonstration environment is pre-loaded with sample data. Use the following profiles to test different search queries, permit statuses, and violation scenarios:

Username	First Name	Last Name	User Type	Plate	VIN Number	Violations	Permits
spencer	Spencer	Carr	Full Time Staff	SPENCE			

jparson s	Julie	Parsons	Compli mentar y	JULPAR ASDA3 47	1q2124 214312 4213		COM10 0 - Unpaid
jrockwo od	James	Rockwo od	F/T Student	JROCK	5SXHA NDC38 RZ5550 6		R102 - Red Student Lot W
sjamies on	Steph	Jamieso n	P/T Student	SJAM SJAM2	2T1BU4 EE5DC9 72469 1N4AL3 AP5DN 517821	TT- 10001	100 - Red Student W 102 Red Student W
johndo e	John	Doe	F/T Staff	ABC316	1FMCU 0EG1C KB6545 4		501 - Unpaid
skjones	Jones	Sarah	Daily Reserv ed	AKRJ25 9			
vcosta	Voula	Costa	Daily Reserv ed	VCOST	2GCEC 19V531 113601		L103 - Unpaid
bcamer on	Brady	Camero n	Compli mentar y	BCAM			COM10 0 - Unpaid
sbyers	Sheldo n	Byers	Daily Reserv ed	SHELBY	1G8ZN 12871Z 117051		L100 - Unpaid

pbirch	Patricia	Birch	F/T Staff	BIRCH No Plate	1N6AD 0ER5FN 709323 1GKS1 AKC7FR 518845	TT- 10003	None
mashbu ry	Micheal	Ashbur y	P/T Staff	MASH ASDA4 37 BDHE3 85	JNAMA4 3H9XG E50339	15- 170420 TT- 10010	Monthly 0005 - Red Staff Lot West 0002 - Red Staff Lot West 50 - After 4PM 500 - Green Staff Lot East - UNPAID

Best Practices and Considerations

- **Use demo mode for training: Organizations should establish a business rule requiring all new field officers to complete training exercises in DEMO MODE before issuing live tickets.**

This ensures staff are comfortable with the interface and prevents

accidental test violations from entering the live production database.