OPSCOM FAQs, Tips & Tricks

OperationsCommander works hard to maintain an up to date product wiki! If you have any questions or if you feel something is missing, post about it in the community.

- Quick Search Tool Functionality
- Disable Browser Auto-Fill and Auto-Complete
- Rebranding the User Portal with Custom Colors
- Why Are My Violation/Warning Notification Emails Not Going Out?
- Unsubscribe Option for Email Notifications-Opt-Out

Quick Search Tool Functionality

> The Quick Search tool is a centralized search utility that allows administrators to rapidly locate specific records across the platform directly from the main menu. Its primary purpose is to retrieve relevant data associated with users, vehicles, incidents, and financial transactions, significantly streamlining daily workflows. This article is intended for OperationsCommander (OPSCOM) administrators.

Setup and Configuration

This feature is a core administrative tool built directly into the main interface.

Admin Side: The Quick Search tool is enabled by default for all administrative accounts. No specific setup, permissions, or configuration is required to use this utility.

Using this Feature

Administrators can use the following instructions to quickly locate system records from any page within the admin portal.

1. Click the **Search** text field located in the main menu.
2. Enter a minimum of 3 characters to initiate the search query.
3. Click the desired record from the generated list of results to navigate directly to its specific details.

Searchable Data Types

The Quick Search tool scans across multiple modules to return results matching the following information:

- License plate (including the license plate of any vehicle involved in an incident)
- VIN number
- Username
- Last name
- Email address
- Student number
- Employee number
- Ticket number
- Incident number
- Payment Confirmation code

Best Practices and Considerations

- **Adhere to the character minimum: Ensure that you have entered at least three characters to initiate the search.** The system will not execute a query or generate results for entries containing fewer than three characters.
- **Leverage advanced search tools: Consider using the advanced search features within specific modules if you are unable to locate a specific record.** Navigating directly to modules such as *Permit Management* or *IncidentAdmin* provides much more granular filtering options for complex or highly specific queries.

If your search does not yield the expected results immediately, double-check your spelling and verify that you have met the three-character minimum requirement before navigating to the advanced module searches.

Disable Browser Auto-Fill and Auto-Complete

> This article provides instructions on how to disable browser auto-fill and auto-complete features on your local workstation. Its primary purpose is to prevent browsers from automatically populating administrative form fields with incorrect data, ensuring strict data integrity when managing user profiles and sensitive information. This guide is intended for OperationsCommander (OPSCOM) administrators who are experiencing data entry interference caused by their local web browsers.

Setup and Configuration

Because this configuration takes place outside of the OPSCOM environment, the setup involves modifying your local software settings.

Admin Side: Administrators must configure their local web browser settings to prevent auto-fill behaviors from overriding manual data entry within the administrative portal.

User Side: End-users may also choose to disable these settings on their personal devices for privacy reasons, though it is not strictly required for basic interaction with the public parking portal.

> Some browser plug-ins, such as third-party password managers, may also act as auto-fill utilities and cause similar data override issues. If disabling the browser's native auto-fill does not resolve your data entry issue, review your installed plug-ins and disable or configure them to explicitly exclude the OPSCOM domain.

Using this Feature

Administrators can use the following steps corresponding to their specific web browser to disable the native auto-fill features.

Google Chrome

1. Open Chrome.
2. Click the **More** icon (three vertical dots) at the top right and select **Settings**.
3. Scroll to the bottom of the page and click **Show advanced settings**.
4. Disable the **Enable Autofill to fill out web forms in a single click** checkbox located under the Passwords and forms section.

Microsoft Edge

1. Open Edge and click the **More** icon (three dots) at the top right.
2. Click **Settings** and scroll down to **Advanced Settings**.
3. Locate the **Save Form Entries** option and toggle the setting to off.

Mozilla Firefox

1. Open Firefox.
2. Type **about:config** directly into the address bar and press Enter.
3. Click the **I'll be careful, I promise** button to proceed.
4. Search for **dom.forms.requestAutocomplete** and double-click the entry to set its value to False.

Apple Safari

1. Open Safari and click **Preferences**.
2. Click **AutoFill**.

3. Deselect all checkboxes corresponding to the categories of information you do not want Safari to automatically fill.
4. Click the **Edit** button next to a specific category if you need to edit or delete existing saved information.

Internet Explorer

1. Click the **Tools** menu icon.
2. Click **Internet Options** and navigate to the **Content** tab.
3. Click the **Settings** button under the Auto Complete section.
4. Disable the **Forms** checkbox and the **User Names and Passwords on Forms** checkbox.

Best Practices and Considerations

- **Test after configuration: Always save your changes and refresh the system to confirm that the auto-fill issue is resolved.** Logging completely out of OPSCOM and logging back in ensures your new browser settings take effect across all portal forms.
- **Maintain security awareness: If you are using a shared workstation, be aware that disabling auto-fill is a critical step in maintaining data privacy.** Preventing your browser from saving this data safeguards against unauthorized access to saved credentials and protected user information.

Rebranding the User Portal with Custom Colors

> The custom colors feature allows administrators to modify the primary and secondary colors of the User Side interface. Its primary purpose is to align the visual appearance of the public-facing parking portal with your organization's official branding. This article is intended for OperationsCommander (OPSCOM) administrators responsible for managing system designs and user experience.

Setup and Configuration

This feature modifies the core cascading style sheets (CSS) of the user portal and requires access to the system templates.

Admin Side: Administrators must have the appropriate system role permissions enabled to access the content and design configuration menus.

Using this Feature

Administrators can use the following instructions to apply custom styling to the portal using standard color names or precise hex codes.

Editing the Portal Styles

1. Hover over **System Settings**, click **Content & Designs**, then **Templates & Design**.
2. Click the **Toggle Templates** button.
3. Click the **Edit** button under the **Styles** section.
4. Add the following code snippet to the very top of the editor, directly under the `<style>` tag:

```
:root{
--ion-color-primary: purple;
--ion-color-secondary: orange;
}
```

5. Replace `purple` and `orange` with your desired standard color names (e.g., `blue`, `green`, `red`).

Best Practices and Considerations

- **Utilize precise branding: For more precise branding control, use hexadecimal color codes instead of standard color names.** Hex codes ensure your portal matches your organization's exact marketing and brand guidelines.
- **Identify the correct hex codes: Use a browser extension such as ColorZilla or an online color picker tool to find the exact hex code for your organization's specific colors.**
- **Format the snippet correctly: In the code snippet, replace the standard color name with your six-character hex code.** Ensure you include the hashtag (#) before the code.

> When using hex codes, your CSS snippet should be formatted exactly like the example below:

```
:root{
--ion-color-primary: #6F42C1;
--ion-color-secondary: #FFA500;
}
```

Why Are My Violation/Warning Notification Emails Not Going Out?

> The automated notification system triggers emails to responsible parties when a violation or warning is issued. This troubleshooting guide helps administrators identify and resolve configuration issues preventing these automated emails from successfully sending. This article is intended for OperationsCommander (OPSCOM) administrators responsible for managing system communications and enforcement.

Setup and Configuration

Ensuring that notification emails function correctly requires verifying several core settings across both user profiles and system configurations.

Admin Side: Administrators must ensure that system tasks, email templates, and violation parameters are actively enabled and configured correctly to allow automated processing.

User Side: End-users must have a valid email address attached to their account and be designated as the primary driver of the vehicle to receive automated email notifications.

Verifying System Configurations

To ensure emails are processed successfully, verify the following configurations within your environment:

- Confirm that the user is marked as the **Primary Driver** and has a valid email address associated with their account. The system automatically

sends emails to the primary driver; users without an email address are instead flagged for the *Letter Report*.

- Hover over **System Configuration** and click **Content & Designs** then **Email Templates** to ensure that the templates for violation notices are properly configured and enabled.
- Hover over **Tools** and click **View System Task Logs** to verify that the **New Violation Notices** system task is enabled and running correctly (either on a set schedule or via manual trigger).
- Hover over **System Configuration** and click **System Settings** then **Violations** to ensure that the **Send Notices For Warnings** checkbox is enabled, assuming your organization sends warnings.
- Hover over **System Configuration** and click **System Settings** then **Violations** to verify the **Days until due** configuration. Additionally, check the **Collections** settings to ensure **Include All Unpaid Violations** is set according to your organizational requirements.

Troubleshooting and Inspection

Administrators can use the following instructions to investigate further if the system configurations are correct but emails are still not sending.

1. Hover over **Violations** and click **Letter Report**.
2. Inspect the generated report to identify users who lack valid email addresses or who have unsent notices.
3. Manually review these entries to determine if they meet the criteria for automated notification.

> The system only triggers initial emails for **New Violations** (those issued on the current day). Existing or older violations may not trigger an automated notification email after the initial issuance date has passed.

Best Practices and Considerations

- **Maintain accurate user data: Regularly audit user profiles to ensure primary driver contact information is up to date.** Confirming valid email addresses prevents ongoing communication gaps.
- **Monitor your task logs: Periodically review the System Task Logs.** This confirms that automated notification processes are executing as expected without errors.
- **Maintain consistency in reporting: Use the Letter Report as a standard tool for identifying users who fall outside of the automated email criteria.** This ensures these individuals still receive necessary physical notices.

Unsubscribe Option for Email Notifications-Opt-Out

> The Email Notification Opt Out feature allows users to easily unsubscribe from non-essential email communications. Its primary purpose is to improve the overall user experience, ensure compliance with strict data privacy regulations, and significantly reduce the volume of manual unsubscribe requests. This article is intended for OperationsCommander (OPSCOM) administrators responsible for managing system communications and user settings.

Setup and Configuration

This feature requires administrators to enable a global setting and assign appropriate categories to their email templates.

Admin Side: A master setting controls whether users are able to access email preferences. This setting is deployed as off by default. Once enabled, administrators can assign pre-defined categories to the email templates on their system. The pre-defined email categories cannot be altered and include:

- **Important** (Essential)
- **Promotional Emails** (Non-essential)
- **Newsletter** (Non-essential)
- **Product Updates** (Non-essential)

User Side: When the feature is enabled, end-users can manage their email preferences through an **Email Preferences** page within their account settings. Users can access this page by navigating directly to their account

settings on the public portal or by clicking the **Unsubscribe** link located in the body or footer of any non-essential email they receive.

> System-related emails, such as payment receipts, password resets, and new account creation confirmations, are strictly exempt from the unsubscribe functionality. These essential transactional emails cannot be disabled by administrators or opted out of by end-users.

Using this Feature

Administrators and users will interact with the categorization and opt-out functionalities through the following workflows.

Assigning Email Categories

Administrators must assign a specific email category when setting up system communications. Category selection options are available on both the standard compose email page and the email template page for automated system messages.

1. Select the desired classification from the category drop-down menu when composing a new email or editing an existing template.
2. Review the system warning prompt. If a non-essential category is selected, a message will clearly display to the admin indicating that the user has the ability to opt out of receiving it.
3. Save your template or dispatch the email. Emails marked with a category flagged as essential are always sent, while emails marked with a category a user has explicitly unsubscribed from will automatically be withheld from that specific user.

Managing User Email Preferences

Users will interact with the following elements on the **Email Preferences** page to control their inbox:

- **Checkboxes:** Users can select or deselect the checkboxes next to each email category to manage their active subscriptions.
- **Popover icon (?):** Clicking this icon next to a specific checkbox will display a detailed description of that category.
- **Select/Deselect All:** Users can click this action to quickly manage all checkboxes at once.
- **Essential Categories:** Users can view a static list of essential email categories that cannot be unsubscribed from at the very bottom of the page.
- **Save Changes:** Users must click the **Save Changes** button to apply their updates. A confirmation message will immediately display to verify the action.

Best Practices and Considerations

- **Develop a clear business rule: Organizations should develop a firm business rule defining what is considered an essential versus a non-essential email.** Essential emails are critical communications that all users must receive, such as major operational announcements, emergency road closures, or advisories for lot closures due to heavy snow.
- **Use non-essential categories appropriately: Classify promotional or optional content strictly as non-essential.** Non-essential emails are those that a user can safely decide they do not

need, such as event notices for an upcoming open house or a sale at the campus store.

- **Understand the impact of disabling the feature: If the unsubscribe functionality is turned off globally after users have already unsubscribed, their personalized subscription settings will be ignored.** Users will immediately begin receiving all system emails again, which can result in spam complaints or user confusion.