Incidents Configuration

- Managing Incident Categories and Sub-Categories
- Managing Incident Flags
- Managing Ethnic Types
- Managing Incident Relations
- Extended User Profile Options
- Missing Property Types

Managing Incident Categories and Sub-Categories

> The Incident Categories and Sub Categories feature allows administrators to accurately define and classify all incidents reported within the system. Its primary purpose is to organize incident types, control their visibility in reports, and enforce required checklists to ensure precise documentation. This article is intended for OperationsCommander (OPSCOM) administrators responsible for managing incident configurations and reporting.

Setup and Configuration

This feature is a core administrative tool used to establish the drop-down options available to enforcement officers when logging an incident.

Admin Side: Administrators must have the appropriate system role permissions enabled to access the incident configuration menus and manage category lists.

Using this Feature

Administrators can use the following instructions to navigate the management interface to seamlessly add, edit, or manage both main incident categories and their specific sub-categories.

Accessing the Management Interface

1. Hover over **System Configuration**, click **Incidents**, then **Categories**.

Adding Categories

1. Click the **Add New Category** button located at the bottom of the page.
2. Enter the details for your new category into the **Category Name** field.
3. Enter a code into the **GIS number** field if your organization utilizes geographic location mapping.
4. Enable the **In House** checkbox if this category is strictly for internal tracking and administrative use.
5. Enable the **Included in Reports** checkbox if you want incidents of this type to actively appear in standard system reports.
6. Click the **Save Incident Category** button to finalize the addition.

> The GIS number field is strictly optional and is only required for clients who utilize an external geographic location code system or mapping integration.

Editing Categories

1. Locate the desired category from the active list on the main management page.
2. Click the **Pencil icon** next to the entry you wish to edit.
3. Make the necessary updates to the configuration fields.
4. Click the **Save Incident Category** button to apply your updates.

Managing Sub Categories

Sub-categories provide a finer level of detail and granularity for incidents.

1. Click the **Sub** button next to a main category name to view its associated sub-categories.

2. Enter the new name into the **Name** field at the bottom of the list to add a new sub-category, or click directly into the text box of an existing entry to change its name.
3. Enable the **Required** checkbox if a specific checklist must be completed for incidents filed under this sub-category.
4. Enable the **Include** checkbox if this sub-category should be included in generated reports.
5. Enable the **Archive** checkbox to retire a sub-category that is no longer actively in use.
6. Click the **Save Sub-Categories** button to apply all updates to the list.

Best Practices and Considerations

- **Establish a logical hierarchy: Create a clear and logical hierarchy between categories and sub-categories to ensure accurate incident classification.** For example, using "Theft" as a main category with "Vehicle Theft" and "Personal Belongings Theft" as sub-categories makes reporting incredibly intuitive.
- **Leverage checklists for consistency: Utilize the Required checklist option for sub-categories to ensure that all necessary information is collected consistently.** This directly improves data quality and officer compliance for specific types of critical incidents.
- **Manage report inclusion carefully: Carefully consider which categories and sub-categories should be included in reports based on your organization's analytical and compliance needs.**
- **Distinguish internal data: Clearly distinguish between In House categories meant for internal tracking and those intended for**

broader reporting or external sharing. Keeping sensitive internal HR or administrative incidents out of general reports maintains data security.

- **Conduct regular reviews: Periodically review your incident categories and sub-categories to ensure they remain relevant.** As your operational needs or reporting requirements change, your categories should be updated or archived to match.

Managing Incident Flags

> The Managing Incident Flags feature allows administrators to create custom tags or labels that can be attached to incident reports. Its primary purpose is to quickly categorize, highlight, or draw attention to specific characteristics of an incident, thereby improving reporting capabilities, search efficiency, and internal communication. This article is intended for OperationsCommander (OPSCOM) administrators responsible for managing incident configurations and workflows.

Setup and Configuration

This feature is a core administrative tool used to establish the descriptive labels available to enforcement officers and administrative staff when documenting incidents.

Admin Side: Administrators must have the appropriate system role permissions enabled to access the incident configuration menus and manage the list of available flags.

Using this Feature

Administrators can use the following instructions to navigate the management interface to seamlessly add or delete incident flags, as well as control their visibility in reports.

Accessing the Management Interface

1. Hover over **System Configuration**, click **Incidents**, then **Flags**.

Adding Flags

1. Click on the empty text box provided at the bottom of the active list.
2. Enter a descriptive name into the text field (e.g., High Priority, Follow-Up Required, or Safety Concern).
3. Disable the **Include In Reports** checkbox if you do not want this flag to appear in generated reports.
4. Click the **Add** button to append the new flag to the system.

> By default, the **Include In Reports** checkbox is automatically enabled for all new flags. Disabling this setting ensures the flag remains strictly for internal viewing and workflow management.

Deleting Flags

1. Locate the specific flag you wish to remove from the list.
2. Click the **Delete** button next to the flag.
3. Click the **Confirm** button to finalize the removal.

Best Practices and Considerations

- **Use clear and concise names: Use short, descriptive names for your flags that clearly convey their exact purpose.** Labels such as Critical, Resolved, or Requires Manager Review are instantly understandable for anyone reviewing the incident data.
- **Carefully consider report inclusion: Carefully consider whether each individual flag should be included in reports.** Flags used purely for internal workflows or temporary tracking might not need to appear in aggregated system reports.

- **Standardize your list: Develop a standardized list of flags to ensure consistency across all incident reporting.** A well-maintained and unified list makes it significantly easier to filter, search, and analyze large sets of historical incident data.
- **Integrate flags into workflows: Think about how specific flags can integrate with your broader incident management workflow.** For instance, applying a Follow-Up Required flag could become a standard operating procedure to officially trigger a management review process.

Managing Ethnic Types

> The Managing Ethnic Types feature allows administrators to define and manage a drop-down list of ethnic classifications used specifically within incident reporting. Its primary purpose is to support detailed demographic data collection, enabling organizations to analyze trends, ensure fair practices, and securely comply with standard reporting requirements. This article is intended for OperationsCommander (OPSCOM) administrators responsible for incident configuration and demographic reporting.

Setup and Configuration

This feature is a core administrative tool used to establish the drop-down options available when logging an incident in the system.

Admin Side: Administrators must have the appropriate system role permissions enabled to access the incident configuration menus and manage the list of ethnic types.

User Side: This feature is strictly a backend administrative and enforcement configuration. End-users do not interact directly with these settings on the parking portal, though patrol officers will select these types when completing specific incident reports in the field.

Using this Feature

Administrators can use the following instructions to navigate the management interface to seamlessly add, edit, or delete ethnic classifications.

Accessing the Management Interface

1. Hover over **System Configuration**, then **Incidents**, and click **Ethnicity**.

Adding Ethnic Types

1. Click the **Add Ethnic Type** button.
2. Enter the descriptive classification into the **Name** field.
3. Click the **Save Changes** button to add the new ethnic type to the list.

Editing Ethnic Types

1. Click the **Edit** button next to the specific ethnic type you wish to modify.
2. Make the necessary updates to the name field.
3. Click the **Save Changes** button to apply your updates.

Deleting Ethnic Types

1. Click the **Delete** button next to the specific ethnic type you wish to remove.
2. Click the **Confirm** button to permanently remove it from the system.

> In order to delete an ethnic type, it must not currently be in use by any records in the system. You will not see a **Delete** button unless there are absolutely no incident records associated with this specific classification.

Best Practices and Considerations

- **Standardize your terminology: Use consistent and recognized terminology for ethnic types.** This ensures data accuracy across the

board and facilitates meaningful, reliable analysis.

- **Verify data integrity before deletion: Always verify that an ethnic type is not actively linked to any records before attempting to delete it.** Attempting to force the deletion of an active classification can cause critical data inconsistencies in historical reports.
- **Leverage data for reporting and analysis: Accurate ethnic type data can be crucial for generating demographic reports related to incidents.** This data helps organizations identify patterns and effectively inform initiatives related to diversity, equity, and inclusion.
- **Handle data with sensitivity and purpose: When collecting and managing demographic data, ensure that the purpose is clearly defined and aligns with organizational policies.** This information must be handled with strict sensitivity and adhere to all relevant privacy regulations.
- **Ensure strict compliance: If your organization has specific reporting requirements related to demographics (e.g., for government or grant purposes), ensure your configured ethnic types comprehensively support those needs.**

Managing Incident Relations

> The Managing Incident Relations feature allows administrators to define specific types of connections between individuals involved in an incident, such as a Witness, Victim, Suspect, or Reporting Party. Its primary purpose is to accurately document complex incident scenarios, ensure all parties are properly identified, and facilitate comprehensive investigations. This article is intended for OperationsCommander (OPSCOM) administrators responsible for configuring incident reporting standards.

Setup and Configuration

This feature is a core administrative tool used to establish the drop-down options available when documenting individuals involved in an active incident.

Admin Side: Administrators must have the appropriate system role permissions enabled to access the incident configuration menus and manage the list of relations.

Using this Feature

Administrators can use the following instructions to navigate the management interface to seamlessly add or edit incident relations.

Accessing the Management Interface

1. Hover over **System Configuration**, click **Incidents**, then **Relations**.

Adding Relations

1. Locate the empty text box provided at the bottom of the list.
2. Enter the desired name for the connection (e.g., Witness or Victim) into the text field.
3. Choose a unique color for this specific relationship type to visually distinguish it within the system.
4. Click the **Insert New** button to add the new relation to the list.

Editing Relations

1. Locate the specific relation you wish to modify in the list.
2. Click the **Edit** button next to the entry.
3. Make the necessary updates to the name or color.
4. Click the **Save Changes** button to apply your updates.

Best Practices and Considerations

- **Establish comprehensive definitions: Define all relevant relationship types that might occur in your incident reporting.** Providing a complete list ensures accurate and comprehensive documentation of any complex scenario your officers might encounter.
- **Use clear naming conventions: Use concise and unambiguous names for relations to avoid administrative confusion.** For instance, clearly establishing the difference between a "Victim" and a "Complainant" guarantees field officers select the correct role during documentation.
- **Enforce standardization: Encourage consistent use of defined relations by all personnel involved in incident reporting.** Consistent application drastically improves overarching data quality

and long-term reporting reliability.

- **Verify data integrity before deletion: Always ensure that a relation is not actively linked to any incident parties before attempting to delete it.** Attempting to force the removal of an active relation can cause critical data inconsistencies in historical incident reports.
- **Leverage relations for reporting value: Properly categorized relations are essential for generating accurate reports.** This structured data is highly valuable for analyzing incident demographics and auditing the distinct roles of individuals involved across your property.

Extended User Profile Options

> The Extended User Profile Options feature allows administrators to define and manage highly granular descriptive categories and values for user profiles, which are primarily used during incident reporting. Its primary purpose is to enable enforcement officers to accurately record unique physical features or personal identifiers of individuals involved in an incident, significantly enhancing the detail and accuracy of investigations. This article is intended for OperationsCommander (OPSCOM) administrators responsible for managing incident configurations and reporting standards.

Setup and Configuration

This feature is a core administrative tool used to establish the descriptive drop-down options available when documenting individuals involved in an active incident.

Admin Side: Administrators must have the appropriate system role permissions enabled to access the incident configuration menus and manage the list of extended profile values.

User Side: This feature is strictly a backend administrative and enforcement configuration. End-users do not interact directly with extended profile options on the parking portal, though patrol officers will select these descriptive values when completing specific incident reports in the field.

Using this Feature

Administrators can use the following instructions to navigate the management interface to seamlessly add or edit extended user value types.

Accessing the Management Interface

1. Hover over **System Configuration**, click **Incidents**, then **Ext. User Profile Options**.

> The management page displays a list of currently defined extended values. A Value Type acts as a broad category (e.g., Hair Type), while the Value Description details the specific characteristic (e.g., Balding, Red, or Long).

Adding Extended User Value Types

1. Scroll to the bottom of the management page.
2. Select an existing category from the **Value Type** drop-down menu (e.g., Clothing Color or Tattoo Location).
3. Enter the specific characteristic into the **Value Description** text box.
4. Click the **Insert New** button to add the new extended user value to the system.

Editing Extended User Value Types

1. Locate the specific extended value you wish to modify in the list.
2. Click the **Edit** button next to the entry.
3. Select the appropriate text box and make the desired changes to the category or name.
4. Click the **Save Changes** button to apply your updates.

Best Practices and Considerations

- **Leverage granular detail for incidents: Utilize extended values to capture specific, unique identifiers for individuals involved in incidents.** Accurate documentation of physical features can be highly critical for subsequent identification and internal investigations.
- **Establish standardized terminology: Establish clear, consistent terminology for both Value Types and Value Descriptions.** Preventing overlapping descriptions ensures strict uniformity in data collection across all officers and administrators.
- **Provide adequate training for officers: Train field officers on the importance of these fields.** Ensure they know exactly how to accurately select and describe extended values when creating live incident reports on their handheld devices.
- **Avoid system redundancy: Review existing categories and values before adding new ones to prevent database duplication.**
- **Adhere to privacy considerations: Be mindful of privacy regulations and your organization's policies regarding the collection of detailed personal identifiers.** Ensure that the collection of such sensitive demographic data is fully justified, compliant with local laws, and used responsibly.

Missing Property Types

> The Missing Property Types feature allows administrators to define and categorize different kinds of missing or stolen property (e.g., Electronics, Jewelry, Documents) within incident reports. Its primary purpose is to enable detailed and structured data collection for lost or stolen items, enhancing the overall accuracy of incident documentation and supporting external investigations. This article is intended for OperationsCommander (OPSCOM) administrators responsible for managing incident configurations and reporting.

Setup and Configuration

This feature is a core administrative tool used to establish the specific categories and data points available to enforcement officers when documenting missing property.

Admin Side: Administrators must have the appropriate system role permissions enabled to access the incident configuration menus and manage missing property categories.

Using this Feature

Administrators can use the following instructions to navigate the management interface to seamlessly add, edit, or delete property types and their associated fields.

Accessing the Management Interface

1. Hover over **System Configuration**, click **Incidents**, then **Missing Property Types**.

Adding Property Types

1. Click the **Add New Type** button.
2. Enter the descriptive category in the **Name** field.
3. Click the **Add New** button to save the new missing property type to the system.

Adding Fields to Types

1. Click the **View Fields** button next to the specific property type you wish to expand.
2. Click the **Add New Field** button.
3. Enter a descriptive title in the **Field Name** field (e.g., Serial Number, Color, or Brand).
4. Select the appropriate formatting option from the **Field Type** drop-down menu (e.g., checkbox, textbox, or dropdown).
5. Enable the **Required** checkbox if this piece of information must be collected to successfully submit the incident report.
6. Click the **Add New** button to save the new field configuration.

Editing Property Types

1. Click the specific property type name you wish to modify.
2. Enter the desired changes into the name field.
3. Click the **Save Changes** button.

> To modify any of the specific descriptive fields associated with the property type, click the **View Fields** button.

Deleting Property Types

Deleting a missing property type is a two-step process if it currently has associated fields attached to it.

1. Click the **View Fields** button next to the specific property type.
2. Click the **Delete All** button.
3. Click the **Save Changes** button to delete the selected fields.
4. Click the **Delete Property Type** button to permanently remove the category from the system.

> If there are absolutely no fields currently associated with that property type, you can immediately click the **Delete Property Type** button without performing the field deletion steps.

Best Practices and Considerations

- **Implement structured data collection: Use fields within each property type to ensure structured and consistent data collection.** For example, when configuring an "Electronics" category, add specific fields for "Make," "Model," and "Serial Number" to guarantee officers capture actionable data.
- **Maintain clear and concise names: Use descriptive names for both property types and their fields.** Utilizing clear nomenclature improves usability and clarity for officers actively filling out incident

reports in the field.

- **Use required fields carefully: Carefully consider which fields are truly required.** While complete data is valuable, forcing too many required fields can create an unnecessary data entry burden for officers during high-stress situations.
- **Understand data integrity locks: Remember that a property type cannot be deleted if it has associated fields.** This structural mechanism helps prevent orphaned data and ensures the historical integrity of your incident records.
- **Leverage structured data for reporting: Well-defined missing property types and their fields significantly enhance the quality of reports.** Accurate, categorized data directly aids in comprehensive investigations and property recovery efforts.