Incidents Configuration

Managing Incident Categories and Sub-Categories

> **Incident Categories** and **Sub-Categories** in OPS-COM are used to define and classify incidents reported within the system. This feature allows administrators to organize incident types, control their visibility in reports, and manage associated checklists, ensuring precise documentation and effective analysis of various occurrences.

Using this Feature

The **Edit Categories and Sub Categories** page allows you to add, edit, and manage both main incident categories and their more specific sub-categories.

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

Adding Categories

1. On the **Edit Categories and Sub Categories** page, click **Add New Category** located at the bottom of the page.
2. Fill out the details for your new **Category Name**.
3. Enter the **GIS number** (optional, used by clients with geographic location codes).
4. Select whether it's an **"In House"** category (for internal use).
5. Select if you'd like this category to be **Included in Reports**.
6. Click **Save Incident Category**.

Editing Categories

1. On the **Edit Categories and Sub Categories** main page, locate the desired category from the listed items.
2. Click the **pencil icon** next to it to edit.
3. Make your changes and click **Save Incident Category** to apply your changes.

Managing Sub-Categories

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

1. To check a category for its sub-categories, click the **Sub** button next to the Category name.
2. The list of Sub-Categories for that item will display. You can add a new sub-category at the bottom of the list.
3. Enter the **Name** of the sub-category and enable the desired functions:
    - If a **Checklist** is required for incidents under this sub-category, click **Required**.
    - If it's to be **Included in Reports**, click **Include**.
    - If you wish to archive it, enable the **Archive** checkbox.
    - If you want to change the name of an existing one, click in the text box and change it.

Once you have finished, click **Save Sub-Categories**.

Best Practices & Considerations

- **Logical Hierarchy**: Create a clear and logical hierarchy between categories and sub-categories to ensure accurate incident classification (e.g., Category: "Theft," Sub-Categories: "Vehicle Theft," "Personal Belongings Theft").
- **Report Inclusion**: Carefully consider which categories and sub-categories should be **Included in Reports** based on your organization's analytical and compliance needs.
- **In-House vs. Reportable**: Distinguish between "In House" categories (for internal tracking) and those intended for broader reporting or external sharing.
- **Checklists for Consistency**: Utilizing the "Required Checklist" option for sub-categories can ensure that all necessary information is collected consistently for specific types of incidents, improving data quality.
- **Regular Review**: Periodically review your incident categories and sub-categories to ensure they remain relevant to your incident reporting needs and operational changes.

Managing Incident Flags

> **Incident Flags** in OPS-COM allow administrators to create custom tags or labels that can be attached to incident reports. This feature is vital for quickly categorizing, highlighting, or drawing attention to specific characteristics of an incident, improving reporting, search capabilities, and internal communication.

Using this Feature

The **Edit Flags** page allows you to add and edit incident flags, as well as control their visibility in reports.

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

Adding Flags

1. At the bottom of the list, click on the empty text box provided for adding a new flag.
2. Fill in the **name** (e.g., "High Priority," "Follow-Up Required," "Safety Concern").
3. Toggle the **Include In Reports** checkbox if you do not want this flag to show up in reports. By default, this checkbox is **on**.
4. Click **Add**. The new Flag entry will now appear in the list and is ready to be used when creating or editing incident reports.

Deleting Flags

1. Click the **Delete** button next to the flag and **Confirm**.

Best Practices & Considerations

- **Clear and Concise Names**: Use short, descriptive names for your flags that clearly convey their purpose (e.g., "Critical," "Resolved," "Requires Manager Review").
- **Report Inclusion**: Carefully consider whether each flag should be **Included In Reports**. Flags used purely for internal workflow might not need to appear in aggregated reports.
- **Standardization**: Develop a standardized list of flags to ensure consistency across all incident reporting. This makes it easier to filter, search, and analyze incident data.
- **Workflow Integration**: Think about how flags can integrate with your incident management workflow. For instance, a "Follow-Up Required" flag could trigger a review process.

Managing Ethnic Types

> **Ethnic Types** in OPS-COM allows administrators to define and manage a picklist of ethnic classifications for use within incident reporting. This feature supports detailed demographic data collection for incidents, enabling organizations to analyze trends, ensure fair and equitable practices, and comply with reporting standards.

Using this Feature

The **Manage Ethnic Types** page provides a straightforward interface to add, edit, and delete various ethnic types.

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

Adding

1. Click **Add Ethnic Type**.
2. Fill in the **name**.
3. Click **Save Changes**.

Editing

1. Click the **Edit** button next to the Ethnic Type you want to change.
2. Make your edits and click **Save Changes**.

Deleting

> In order to delete an Ethnic Type, it must not be in by any records in the system. You will not see a delete button unless there are no records associated to this type.

1. Click the **Delete** button next to the type and **Confirm**.

Best Practices & Considerations

- **Standardization**: Use consistent and recognized terminology for ethnic types to ensure data accuracy and facilitate meaningful analysis.

- **Data Integrity**: Always verify that an ethnic type is not actively linked to any records before attempting to delete it. This prevents data inconsistencies.
- **Reporting and Analysis**: Accurate ethnic type data can be crucial for generating demographic reports related to incidents, helping organizations identify patterns and inform initiatives related to diversity, equity, and inclusion.
- **Sensitivity and Purpose**: When collecting and managing demographic data such as ethnic types, ensure that the purpose is clearly defined, aligns with organizational policies, and adheres to privacy regulations. This information should be handled with sensitivity and used responsibly.
- **Compliance**: If your organization has specific reporting requirements related to demographics (e.g., for government or grant purposes), ensure your configured ethnic types support those needs.

Managing Incident Relations

> **Incident Relations** in OPS-COM allows administrators to define specific types of connections or relationships between individuals involved in an incident (e.g., "Witness," "Victim," "Suspect," "Reporting Party"). This feature is crucial for accurately documenting complex incident scenarios, ensuring all parties are properly identified, and facilitating comprehensive reporting and investigation.

Using this Feature

The **Relation Administration** page provides a straightforward interface to add and edit various incident relation types.

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

Adding Relations

1. Locate the empty text box provided at the bottom of the list for adding a new relation.
2. Type in the desired **relation name** (e.g., "Witness," "Victim," "Suspect," "Reporting Party").
3. Choose a unique color for this type.
4. Click **Insert New** to add the new relation to the list.

Editing Relations

1. Locate the relation you wish to modify in the list and click the **Edit** button.
2. Make your changes and click **Save Changes**.

Best Practices & Considerations

- **Comprehensive Definitions**: Define all relevant relationship types that might occur in your incident reporting to ensure accurate and complete documentation.
- **Clear Naming**: Use concise and unambiguous names for relations to avoid confusion (e.g., "Victim" vs. "Complainant" if they represent different roles in your context).
- **Standardization**: Encourage consistent use of defined relations by all personnel involved in incident reporting to improve data quality and reporting consistency.
- **Data Integrity**: Always ensure that a relation is not actively linked to any incident parties before attempting to delete it, to prevent data inconsistencies.

- **Reporting Value**: Properly categorized relations are essential for generating accurate reports on incident demographics and the roles of individuals involved.

Extended User Profile Options

> **Extended User Profile Options** in OPS-COM allow administrators to define and manage additional, highly granular descriptive categories and values for user profiles, typically used in incident reporting. This feature enables officers to record unique physical features or identifiers of individuals involved in an incident, enhancing the detail and accuracy of incident reports.

Using this Feature

The **User Extended Values Administration** page allows you to add and update a variety of descriptive values for user profiles.

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

The **User Extended Values Administration** page displays a list of currently defined extended values. Notice the various **types** you can choose from in the dropdown menus to categorize your extended values. A **Value Type** acts as a category (e.g., "Hair Type"), while the **Value Description** details the specific characteristic (e.g., "Balding," "Red," "Long").

Adding Extended User Value Types

1. Scroll to the bottom of the page and select a Value Type **from the dropdown menu** (e.g., "Hair Type," "Clothing Color," "Tattoo Location").
2. Type the **Value Description** in the textbox provided (e.g., "Curly," "Blue," "Left Arm"). Value descriptions can include a range of physical features/identifiers of a user, such as the location of a tattoo, the color of clothing, or the style of hair.
3. Click **Insert New** to add and save the new extended user value.

Editing Extended User Value Types

1. Locate the extended value you wish to edit in the list and click **Edit.**
2. Adjust the **Category** (Value Type) and/or the **Name** (Value Description) by selecting the appropriate textbox and making the desired changes (e.g., changing "Bald" to "Balding").
3. Click **Save Changes** to save and continue.

Best Practices & Considerations

- **Granular Detail for Incidents**: Leverage extended values to capture specific, unique identifiers for individuals involved in incidents, which can be critical for identification and investigation.
- **Standardized Terminology**: Establish clear, consistent terminology for both **Value Types** and **Value Descriptions** to ensure uniformity in data collection across all officers and administrators.
- **Training for Officers**: Train officers on the importance of these fields and how to accurately select and describe extended values when creating incident reports.
- **Avoid Redundancy**: Review existing categories and values before adding new ones to prevent duplication.
- **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 data is justified and used responsibly.

Missing Property Types

> **Missing Property Types** allows administrators to define and categorize different kinds of missing or stolen property (e.g., Electronics, Jewelry, Documents) within incident reports. This feature enables detailed and structured data collection for lost or stolen items, enhancing the accuracy of incident documentation and supporting investigations.

Using this Feature

The **Edit Missing Property Types and Fields** page allows you to define both the broad categories of missing property and the specific details (fields) you want to collect for each category.

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

Adding Property Types

1. Click the **Add New Type** button.
2. Type the **Name** for the new missing property type and click **Add New.**

Adding Fields to Types

1. Click **View Fields** next to the Property Type you want to add a field to.
2. Click **Add New Field**.
3. Type in the **Field Name** (e.g., "Serial Number," "Color," "Brand").
4. Select the **Field Type** from the dropdown menu (e.g., **checkbox**, **textbox**, **dropdown**, etc.).
5. Select whether or not it is a **required field** by clicking the **Required** checkbox.
6. Click **Add New** to save the new field.

Editing Property Types

1. Click the name of the property type you wish to change.
2. Change the name and click Save Changes.
3. Click the **View Fields** button if you want to edit any fields associated to this.

Deleting Property Types

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

1. **If there are NO fields found associated with that property**: You can immediately click **Delete Property Type**.
2. **If there ARE fields found associated with that property**:
    - Click View Fields and then click **Delete All**.
    - Click **Save Changes** to delete the selected fields.
    - Follow step one to **Delete Property Type**.

Best Practices & Considerations

- **Structured Data Collection**: Use fields within each property type to ensure structured and consistent data collection for stolen or missing items (e.g., for "Electronics," you might add fields for "Make," "Model," "Serial Number").
- **Clear and Concise Names**: Use descriptive names for both property types and their fields to improve usability and clarity for officers filling out incident reports.
- **Required Fields**: Carefully consider which fields are truly **Required** to avoid unnecessary data entry burden while ensuring critical information is captured.
- **Data Integrity**: Remember that a property type cannot be deleted if it has associated fields. This mechanism helps prevent orphaned data and ensures the integrity of your incident records.
- **Reporting Value**: Well-defined missing property types and their fields can significantly enhance the quality of reports, aiding in investigations and property recovery efforts.