Table of Contents

Introduction Overview

Resolver Incident Management is a cloud-based system that helps you quickly and easily record, track, report, and manage incident data. Incident Management is an out-of-the-box solution, but your system may be customized according to your organization's specifications. For more information about custom solutions, contact Resolver Support .

System Requirements

Incident Management runs on the latest versions the following Internet browsers:

- The latest version of Google Chrome; or
- Microsoft Edge (recommended) or Internet Explorer 11.

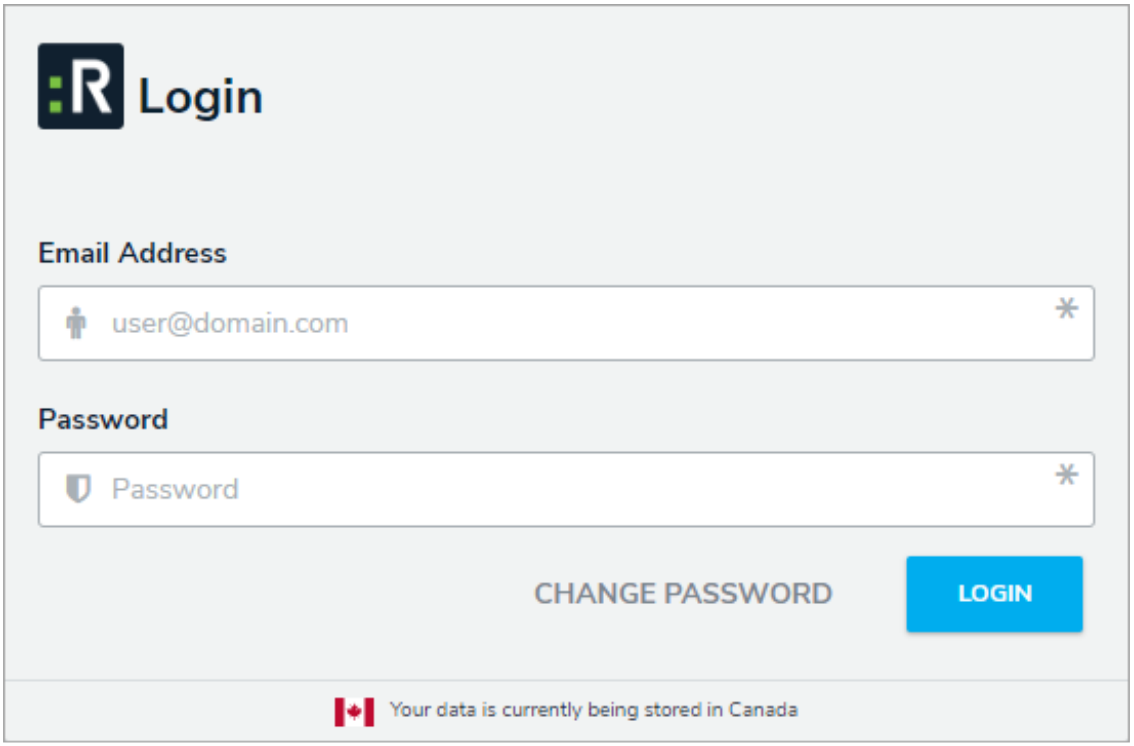
Visit the links below to download Chrome, Edge, or Internet Explorer 11 and to ensure your computer meets the minimum system requirements.

- Download and install Chrome – Google Chrome Help
- Download Microsoft Edge – Microsoft Download Center
- Download Internet Explorer 11 – Microsoft Download Center

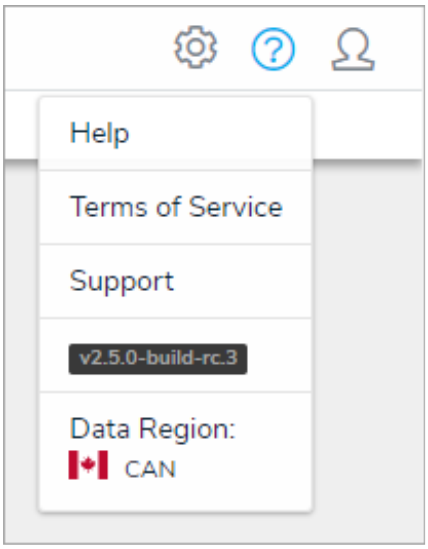
Data Region

You can review the geographical region where your organization's data is being stored from the Incident Management login screen or by clicking the icon in the top bar.

Your organization's data region is selected upon implementation. Contact Resolver Support should you require additional information.



Data region information on the login screen.



Data region information in the top bar.

Who Should Use This Guide

This guide is for users of Incident Management and covers the basic tasks the out-of-the-box user groups typically perform. Note, however, that your account may not have access to some or all the features or settings discussed in this guide.

Important Notes About This Guide

This guide is designed to help users create and manage incidents in Incident Management. These instructions are broken down based on the out-of-the-box user groups . Depending on the settings applied to your profile, **you may not be able to edit some or all the settings and features referenced in this guide**.

Additionally, the screenshots used and the applications, activities, object types, and other elements referred to are not specific to your organization, so your version of the user interface may differ.

Notes, Tips & Warnings

Throughout this guide, you'll see the following symbols:

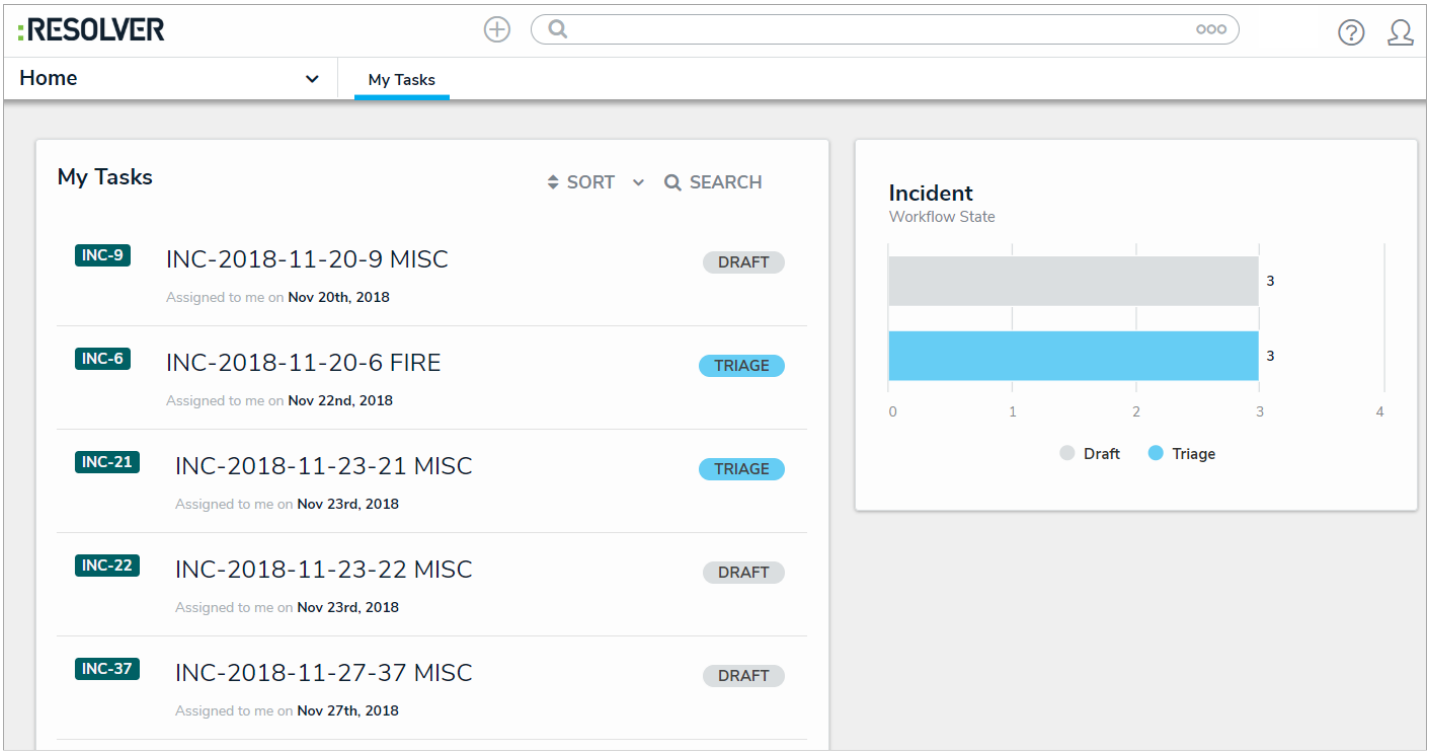
	Indicates a **NOTE**.
	Indicates a **TIP**.
	Indicates a **WARNING**.

User Interface

By default, the Incident Management homepage displays the My Tasks tab, which shows existing incidents that require your attention. The column chart to the right of your tasks shows the incidents' workflow states, such as **Triage, Under Investigation**, or **Review.**

> If you have other Resolver apps, you may see tasks from those apps in the **My Tasks** page.

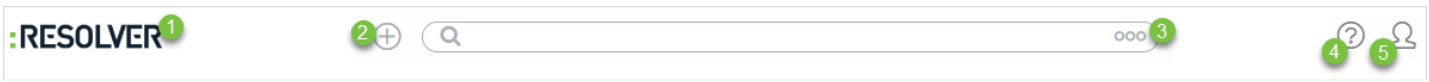
At the top of each page is the **top bar** and **nav bar.**



The My Tasks page.

Top Bar

The following components are in the **top bar** on every page:



The top bar, which is displayed on every page.

1. **Resolver or custom company logo:** Clicking the logo will return you to the **My Tasks** page.
2. **Quick Create:** Clicking the icon will open the **Quick Create** feature, which allows you to create objects outside of the Incident Management applications.
3. **Search:** Enter keywords to search for incidents and other objects. Clicking the  icon allows you to search by object type, such as Business Unit, Incident Type, or Issue.

4. **Help:** Clicking the icon will take you to the Resolver Knowledge Base, Terms of Service, or the Resolver Support site. Clicking this icon will also display your current version of the platform and your organization's data region .

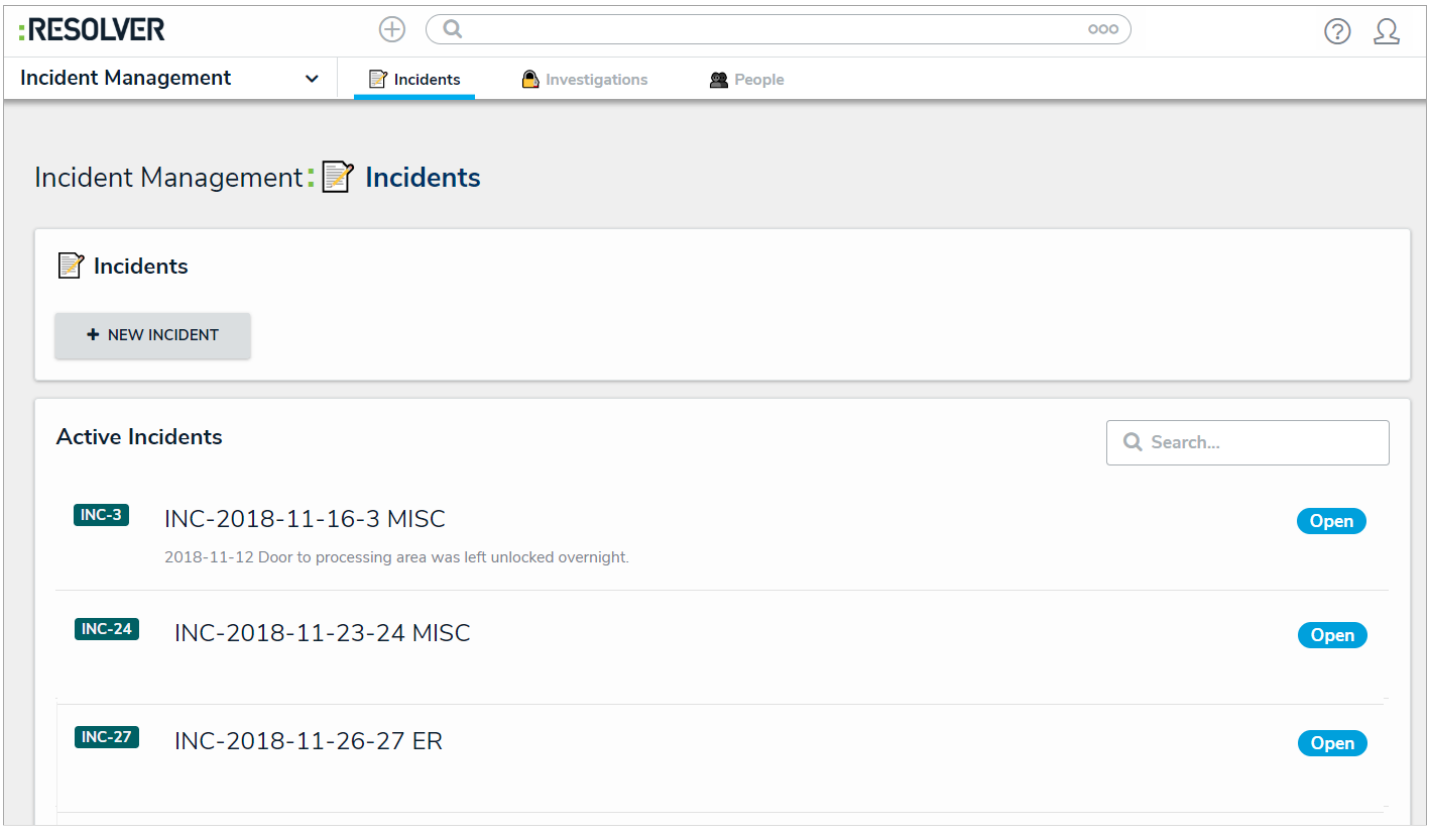
5. **User:** Clicking the icon displays the name of the currently logged in user, as well as provides links to the **My Tasks** page and the **Logout** function.

Nav Bar

The **nav bar** contains a dropdown menu that displays links to the home page and all the applications your role has permission to view (if any). When working in the **Home** area of your organization (after logging in, clicking the **Home** link in the dropdown, or clicking the company logo in the top left of any page), the **My Tasks** tab and any starred reports tabs appear in the nav bar.

The nav bar. The options in the dropdown menu change when working in the Admin settings.

Clicking the name of the application in the nav bar menu will display the application and its activities, which are displayed as clickable tabs. The tab for the first activity in the application is selected by default. To view more tabs (if any), click the icon.

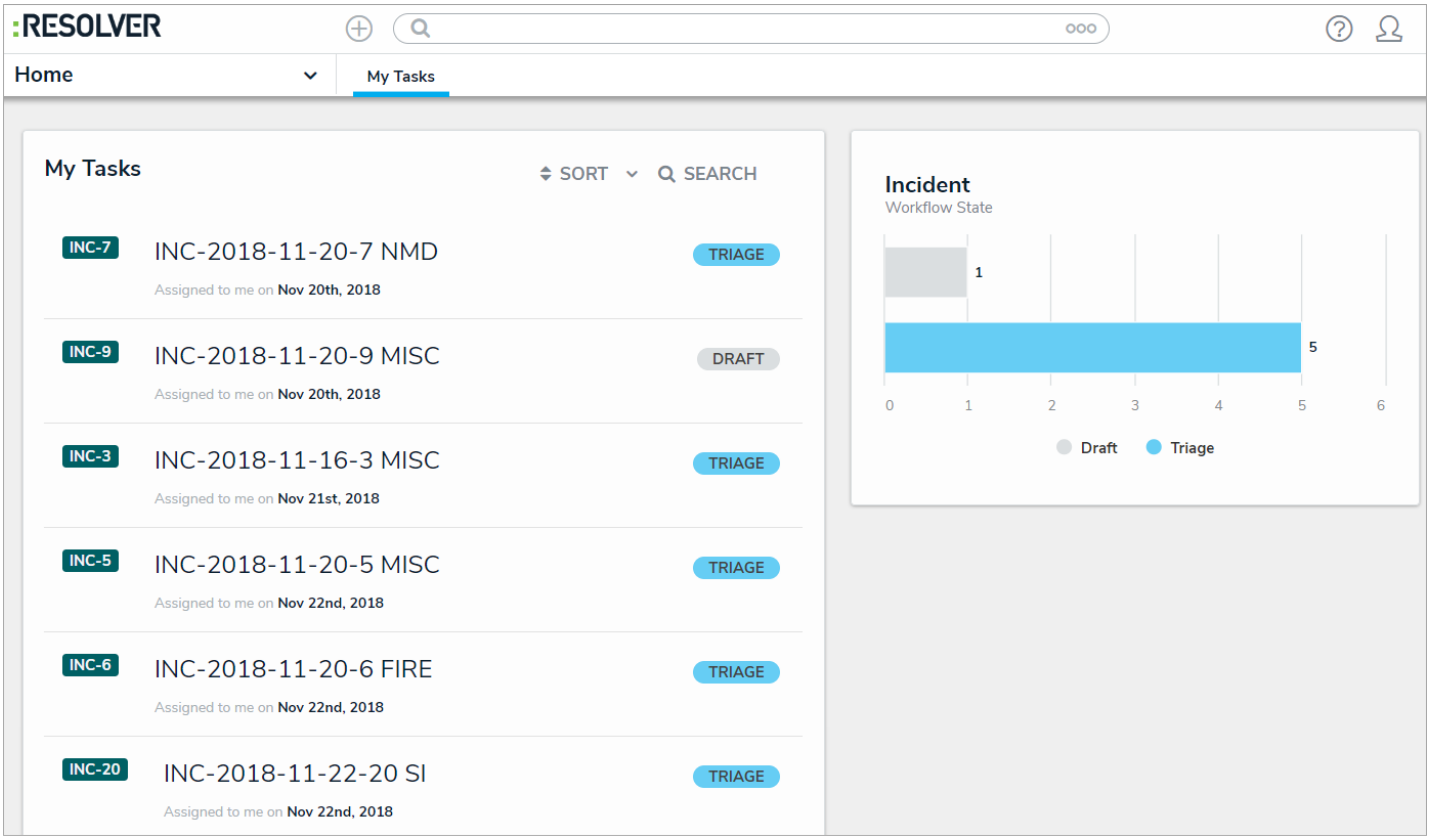


The nav bar displaying the activities in a selected application. Applications are selected from the dropdown menu to the left and activities are opened by clicking the tabs.

Clicking an activity tab displays the landing page for the activity and not the last object or report you may have been working with.

My Tasks

My Tasks is a tab in the nav bar that displays a list of existing incidents and other objects that have been assigned to the user who is currently logged in. By default, the **My Tasks** tab is displayed as the landing page whenever you're working in the **Home** area of your organization (upon login, after clicking the company logo in the top-left of the page, or selecting **Home** from the nav bar dropdown menu), although reports may also be designated as your landing page by an administrator. Any starred reports, including those that may have been flagged as the landing page, will always appear beside the **My Tasks** tab in the nav bar.



*The **My Tasks** page.*

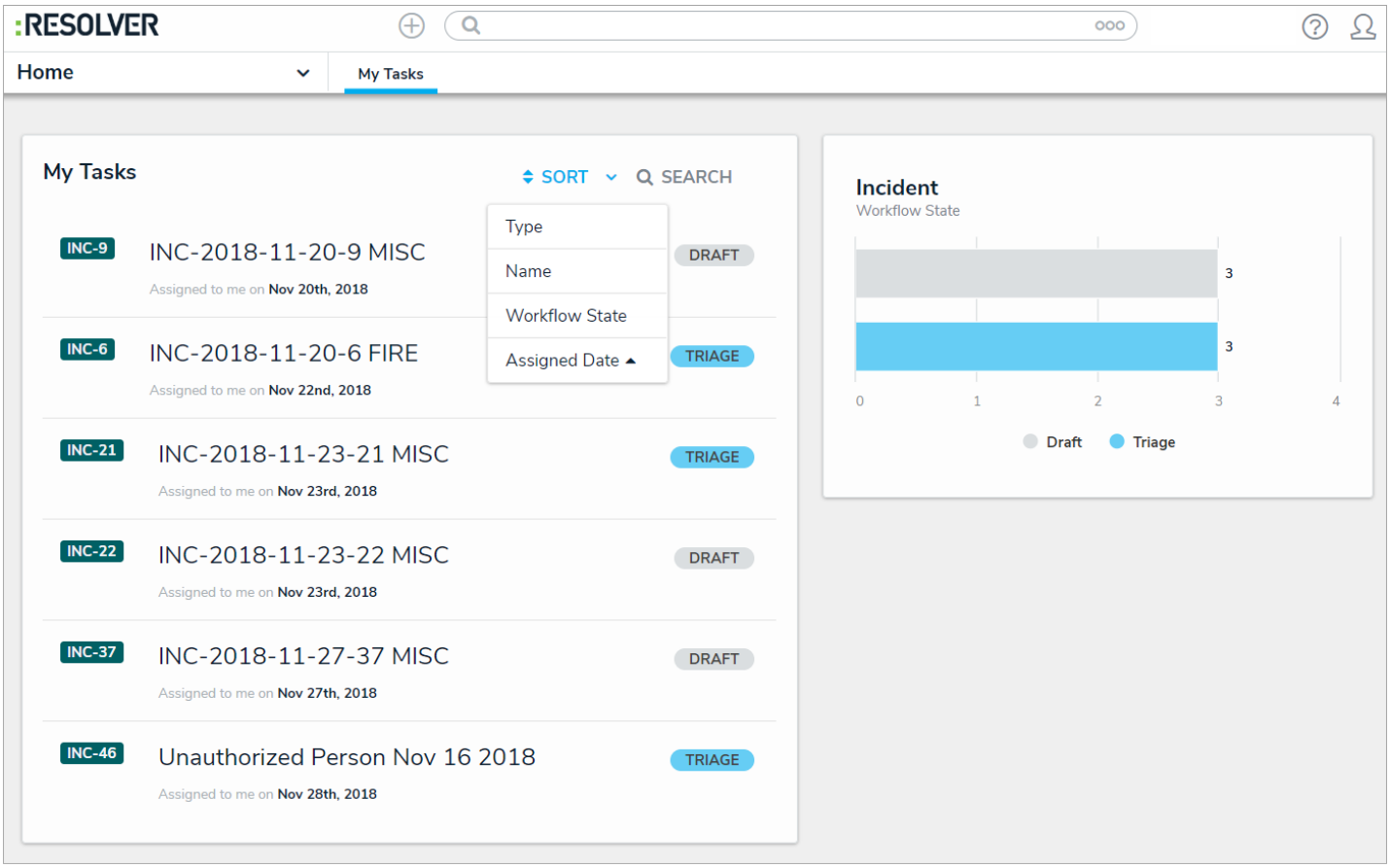
The charts to the right of the **My Tasks** section on this page outline the number of objects assigned to you and their states, such as **Triage**, **Under Investigation**, or **Review**. You can access this page at any time by clicking the Resolver logo (or your company logo, if configured) in the top-left corner of any page or by clicking **My Tasks** in the nav bar while working in an application or activity.

Objects can be viewed by clicking on them, but they won't appear in your tasks unless that has been enabled for your role. Users can still access objects, depending on their user permissions, through **Search**, activities, reports, and applications.

To arrange how objects appear on the page, click **Sort**, then select one of the following options:

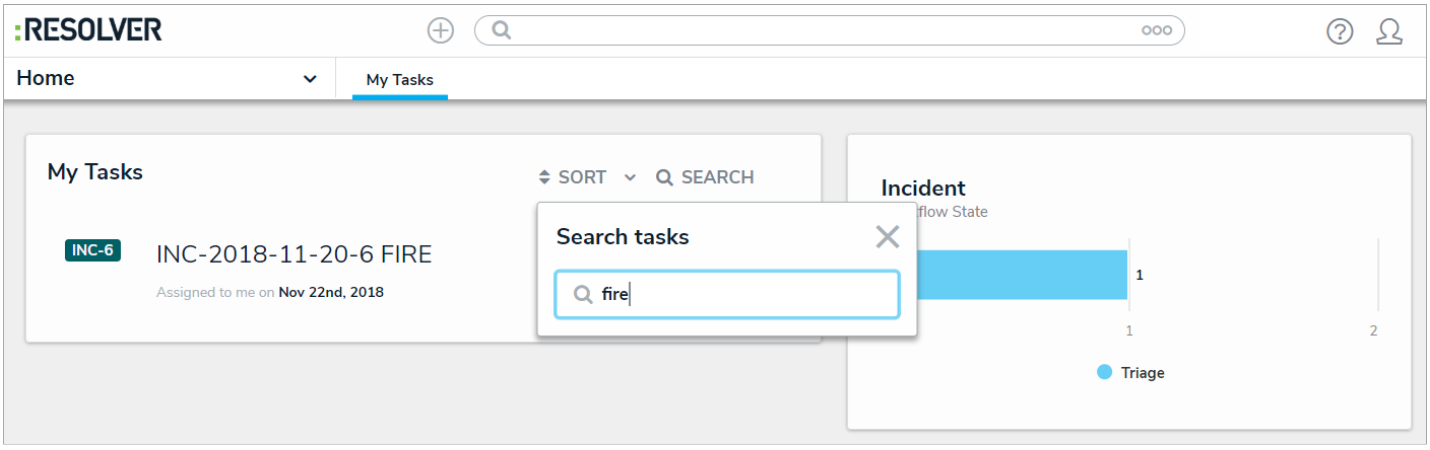
- **Type:** Sorts the assigned objects by object type.
- **Name:** Sorts the assigned objects by name.
- **Workflow State:** Sorts the assigned objects by their current workflow states.
- **Assigned Date:** Sorts the assigned objects by the date they were assigned to you.

By default, clicking an option will sort the objects in ascending order (alphabetically or by newest date first). Clicking the option again will sort the objects in descending order.



The Sort option on the My Tasks page.

You can narrow down which objects are displayed by entering keywords from one or more object names. To once again view all objects, click **Search** then click the **X** to remove the keywords.



Clicking Search then entering keywords from an object's name will narrow down which objects are displayed.

Logging In

If you're the primary administrator for your organization's Incident Management account, Resolver will provide you with the URL and login credentials required to sign in, otherwise you'll receive an email with instructions on creating your password once another administrator creates a user account for you.

If you're using single sign-on authentication to log into Incident Management, see the Single Sign-On (SSO) section for more details.

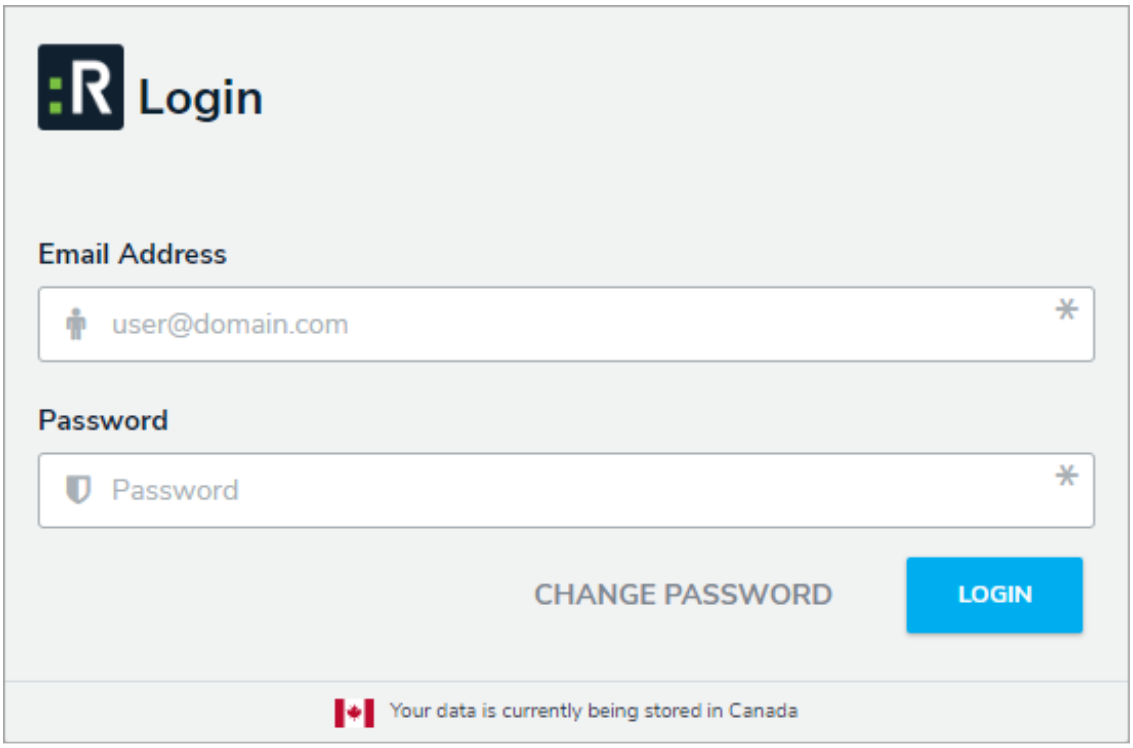
> The login screen indicates which country your data is currently being stored in. See the Data Region article for more information.

To log into Incident Management:

1. Open the email sent to you from Resolver.
2. Click the **Create Password** link from within the email.
3. Enter your password in the **New Password** field. See the Password Requirements section for more information on the password conditions that must be met.
4. Click  **Show Password** to confirm the password entered is correct.
5. Click **Set Password**.
6. Review the **Terms of Service**, then click **Accept Terms**.

> All new users must accept the **Terms of Service** before continuing.

7. From the screen confirming that your password was successfully created, click the **Log In** link.
8. Enter the email address that received the original email in the **Email Address** field.



The Login screen.

9. Enter your password in the **Password** field.
10. Click **Login** to be taken to the Incident Management homepage.

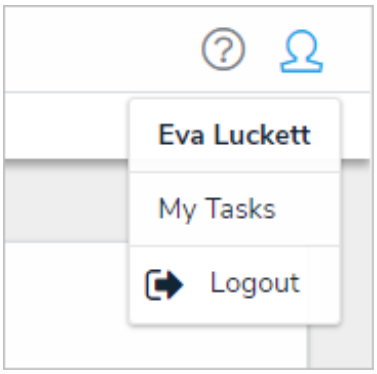
> If your version of Incident Management includes multiple organizations, you'll need to select the organization you'll be working in before the Incident Management homepage is displayed.

Logging Out

After ten minutes of inactivity, you'll be prompted to refresh your session. If, after five minutes, you haven't refreshed the session, you'll be logged out automatically (note that alternate settings may have been configured by your administrator). After being automatically logged out, you can return to the same spot in the app if you log in again without closing the browser/session.

To log out of Incident Management:

1. Click the  icon in the top-right corner of the nav bar.
2. Click **Logout.**



The logout option in the nav bar.

Multi-tenancy (Multiple Organizations)

If Incident Management has been set up to provide you with access to more than one organization, after logging in, you can click on an organization to access it. If you're already working in an organization but wish to access a different one, you must first log out then select an organization after logging in .

Single Sign-On (SSO)

If your organization requires single sign-on authentication (SSO), review theResolver Core SAML Configurations for SSO document for instructions on implementation.

If SSO is enabled, entering your email address on the Incident Management login page will redirect you to your identity provider, where you'll need to enter the login credentials configured for your SSO account. If you're logging into Incident Management for the first time, you will need to accept the Terms of Service before you can successfully log in.

Logging out of Incident Management will end your SSO session. Additionally, after ten minutes of inactivity, you'll be prompted to refresh your session. If, after five minutes, you haven't refreshed the session, you'll be logged out automatically. After being automatically logged out, you can return to the same spot in the app if you log in again without closing the browser/session.

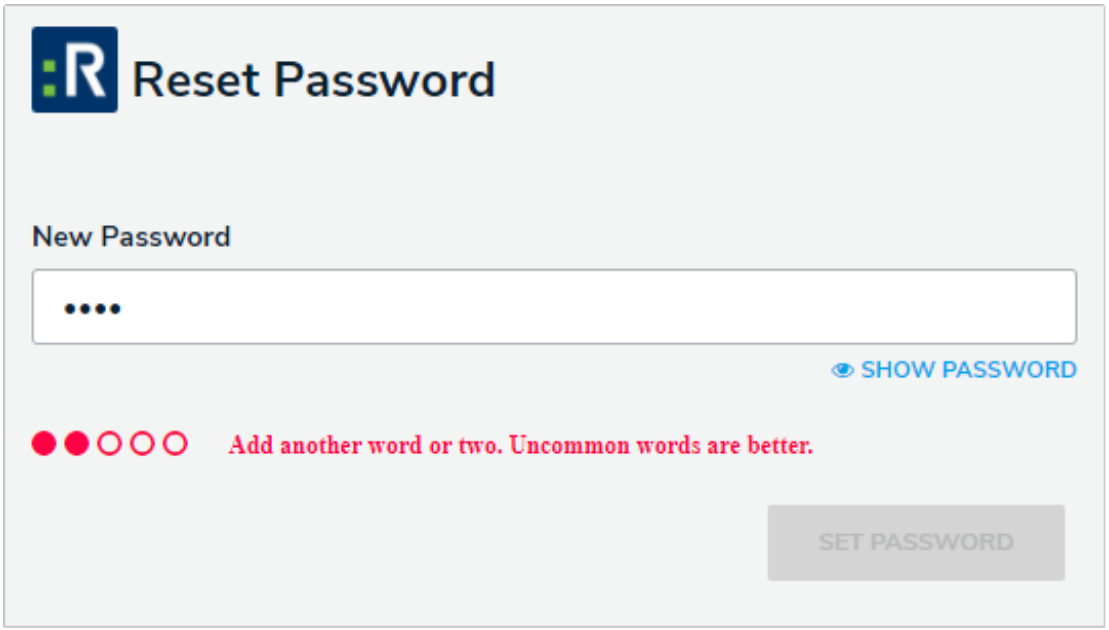
> If SSO is enabled, new users will not be required to create a password, nor will they receive an email with a link to Incident Management. As such, administrators should provide new users with the URL to access their organization.

Password Requirements

Your Incident Management password must contain at least 9 characters, which must include letters. Spaces are permitted.

When creating or resetting your password, you'll see a color-coded password strength indicator. Each color represents the following:

- **Red:** Your password does not meet any or most of the minimum requirements.
- **Yellow:** Your password does not meet some of the minimum requirements.
- **Green:** Your password meets the minimum requirements.
- **Blue:** Your password surpasses the minimum requirements.



The Reset Password screen. In this case, the password entered in the New Password field does not meet the minimum requirements.

Your password expires every 90 days. At the end of the 90-day period, you'll be prompted to change your password, following the requirements outlined above, after successful login. If you forget your password, you can send a reset link to your email account by clicking **Change Password** at the login screen.

> You cannot reuse your current password when resetting it after expiry or resetting it via email.

Search Overview

With the search tool, you can search the Incident Management app by keyword(s), object type(s), or both. When you search for individual object types, you're given additional options to refine the search results by name, description, unique ID, state, and other optional filters.

Numeric Searches

- Entering a number's full numeric term will return the exact result. For example, searching for "000000123" will return "000000123".
- If a number is separated by spaces, hyphens, parentheses, or other non-numeric or non-alphabetical characters, searching for a separated portion of that number will return applicable search results. For example, searching for "234" or "8910" will return "1 (234) 567-8910". Likewise, searching for "123" will return "123 456 789".
- Searching for a portion of a number that is **not** separated by non-numeric or non-alphabetical characters will not return any search results. For example, searching for "000000" will not return any search results, but searching for "000000123" will return "000000123".
- If a phrase contains a mix of numbers and words that are separated by spaces, hyphens, parentheses, or any other non-numeric or non-alphabetical characters, searching for a portion of that phrase will return applicable search results. For example, searching for "123" will return "Number 123."

Text Searches

- Text search terms must be in their complete forms to return results. For example, searching for “accident” will return “accident”, but searching for “Acc” will not return any results.
- If a word or phrase is separated by spaces, hyphens, parentheses, or other non-alphabetical or numeric characters, searching for a separated portion of that phrase will return applicable search results. For example, searching for “John” will return “John Doe.” Likewise, searching for “double” will return “double-check”.
- If a phrase contains a mix of words and numbers that are separated by spaces, hyphens parentheses, or any other non-alphabetical or non-numeric characters, searching for a portion of that phrase will return applicable search results. For example, searching for “Doe” will return “John Doe (555) 555-5555.”
- Searching for a root word will return that root word and its related forms. For example, searching for “accident” will return “accidental,” “accidentally,” “accidents,” etc.
- Search terms are not case-sensitive.
- Stop words (words that are considered unimportant by the search tool) are automatically removed from the search terms. Examples of stop words include:
    - “a”
    - "an"
    - "and"
    - "are"
    - "as"
    - "at"
    - "be"
    - "but"
    - "by"
    - "for"
    - "if"
    - ”in"
    - "into"
    - "is"
    - "it"
    - "no"
    - "not"
    - "of"
    - "on"
    - "or"
    - "such"
    - "that"
    - "the"
    - "their"
    - "then"

    - "there"
    - "these"
    - "they"
    - "this"
    - "to"
    - "was"
    - "will"
    - "with"

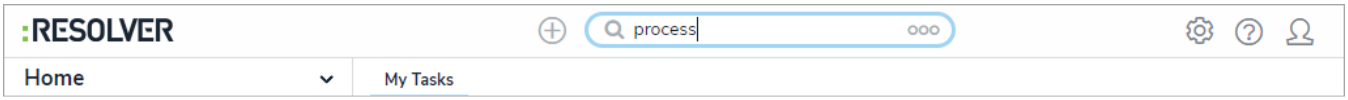
- Searching for words in possessive form will return both the possessive and non-possessive form of the word. For example, searching for “John’s” will return both “John’s” and “John.”
- If searching for words with special characters or accents, you must include the special character or accent in the search. For example, searching for “Joël” will return results, while searching for “Joel” will return no results.

Search Incident Management

The following explains how to search for objects in Incident Management. An object refers to any record created in your Incident Management app, including incidents. An object type is the category of data collected. For example, *Incident* is the object type, whereas *INC-2018-31 Unauthorized Entry* is the object.

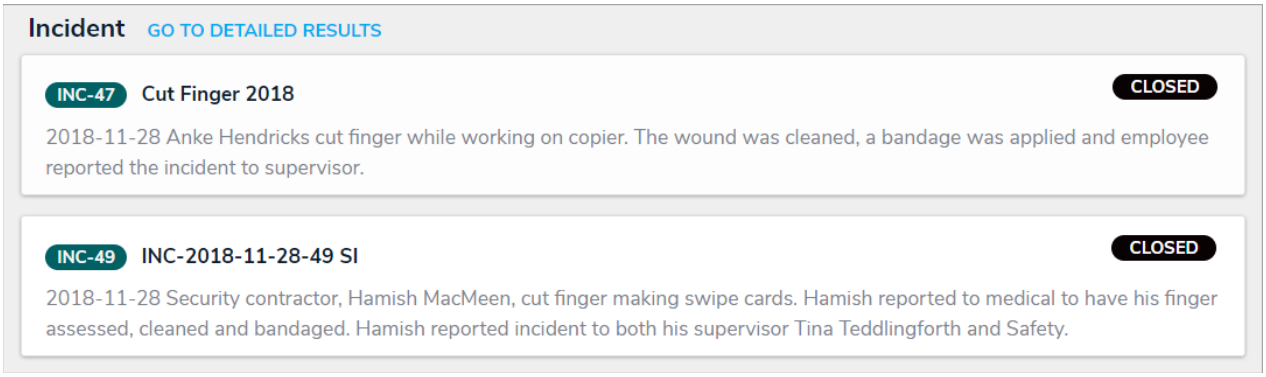
To search Incident Management by keyword:

1. Click the search text field in the nav bar, enter the name of an object, then press **Enter** on your keyboard.



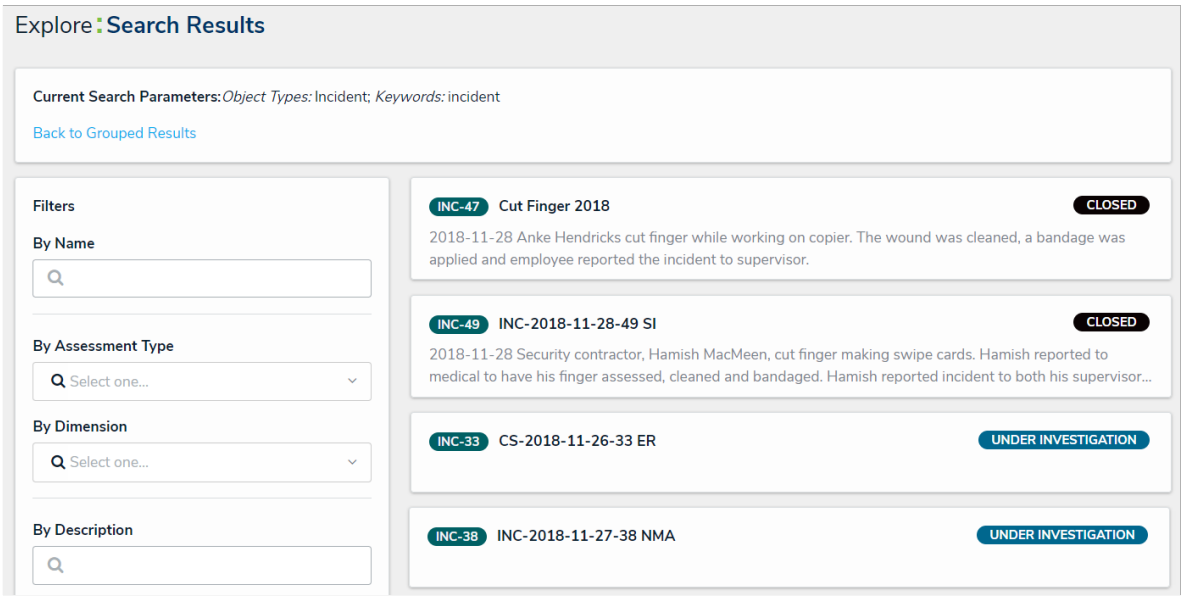
Entering keywords in the search bar.

2. Review the search results, which are organized by object name. The results also display the objects' current workflow state.
3. To view an individual object, click the area below the object's unique ID and name.
4. To apply search filters:
    a. Click **Go to Detailed Results** near the top of the search results for each object type.



Click Go to Detailed Results for filtering options.

    b. Use the filters in the **Filters** section to the left of the page to narrow down which objects are displayed. The following filters are available on this page for every object type:
        - **By Name**;
        - **By Assessment Type**;
        - **By Dimension** (note that this filter is not relevant to the Incident Management application);
        - **By Description**;
        - **By Unique ID**; and
        - **By State**.
    c. Apply additional filters as needed. These additional filters are based on any plain text, select list, and multi-select fields added to the object type:
        - If you're adding a select list or multi-select list filter, choose one or more options from the dropdown menu.
        - If you're adding a plain text filter, enter one or more keywords into the text box. All special characters, except the @ and ! symbols, will be ignored.



Clicking Go to Detailed Results to view filter options to narrow down which objects are displayed in the results.

d. Click an object to view it. The form that is used to display an object found in the search results will be based on your user group. If you are in multiple user groups, the form shown may be unexpected. Contact your Administrator for assistance.

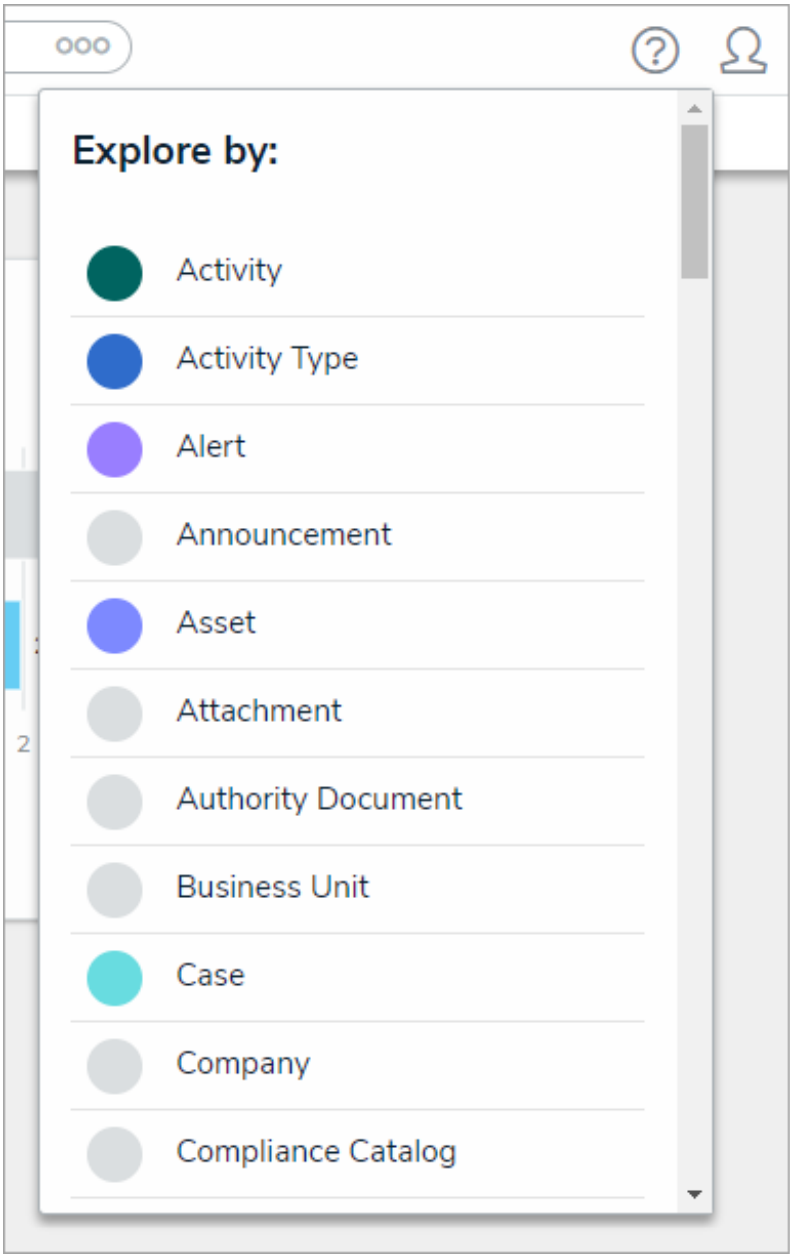
e. To return to the previous page, click **Back to Grouped Results.**

Search Incident Management by Object Type

The following explains how to search by object type in Incident Management. Object type refers to the category of data collected. Incident, Company and Location are all examples of object types. Searching by object type is an easy way to view all records of an object type. For example, you might want to view all locations to know which ones are available to be added to an incident.

To search Incident Management by object type:

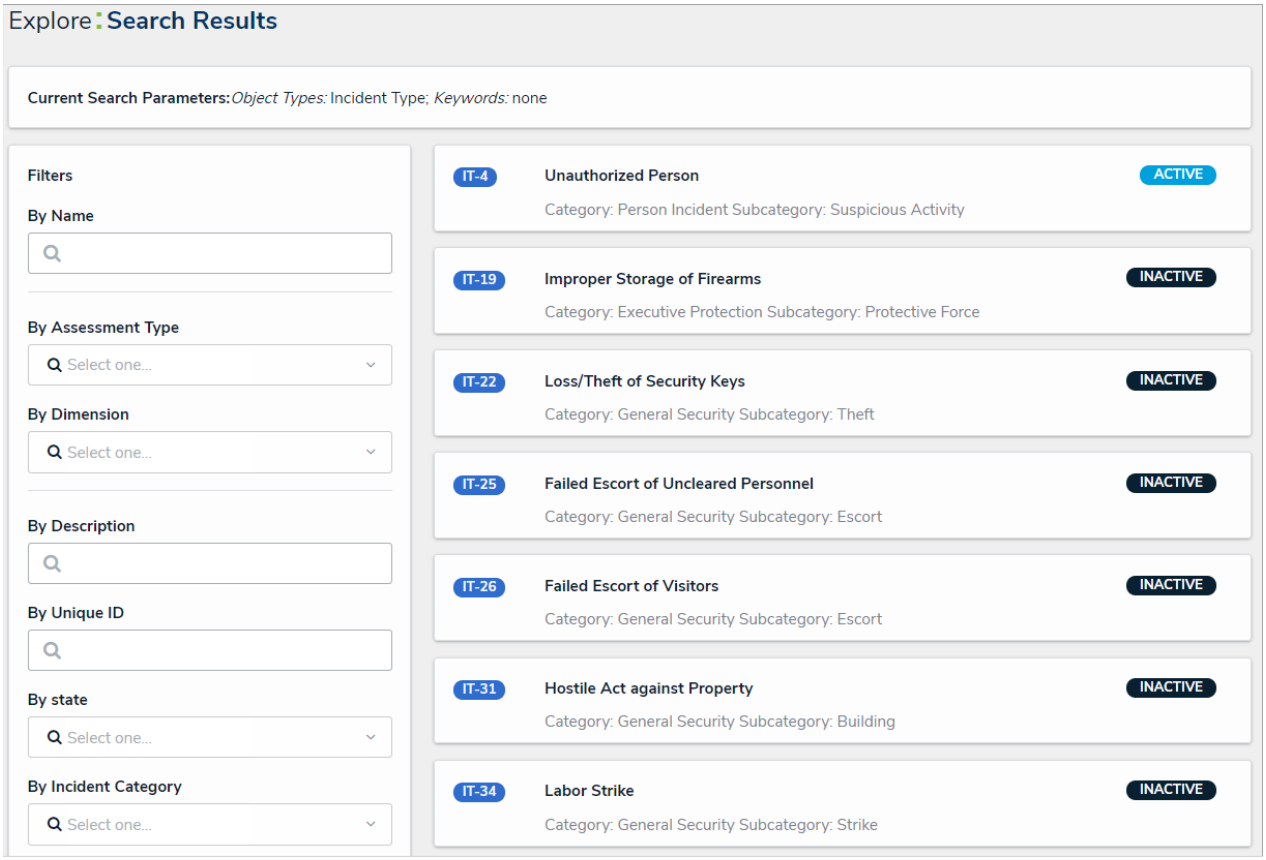
1. Click the search text field in the nav bar, then click the  icon to display the **Explore By** menu.
2. Click an object type from the list to display its objects in the search results.



The Explore By menu. Clicking an object type in this menu will display search options.

3. From the **Search Results** page, use the filters in the **Filters** section to the left of the page to narrow down which objects are displayed. The following filters are available on this page for every object type:
    - **By Name;**

- **By Assessment Type;**
- **By Dimension** (note that this filter is not relevant to the Incident Management application)**;**
- **By Description;**
- **By Unique ID; and**
- **By State.**



The Search Results page.

4. Apply additional filters as needed. These additional filters are based on any plain text, select list, and multi-select fields added to the object type:
    - If you're adding a select list or multi-select list filter, choose one or more options from the dropdown menu.
    - If you're adding a plain text filter, enter one or more keywords into the text box. All special characters, except the @ and ! symbols, will be ignored.

User Groups

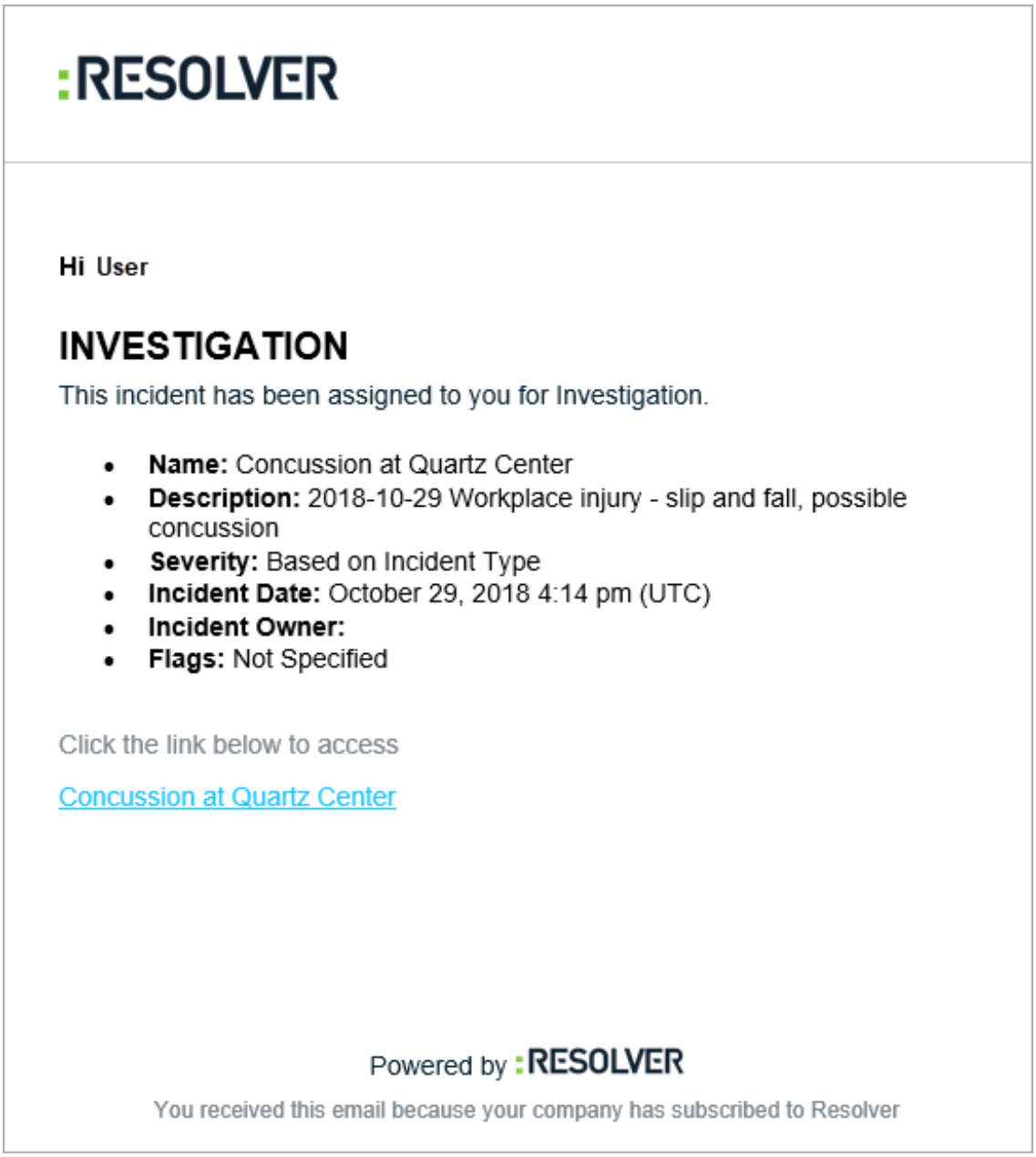
User groups determine the applications and fields users can access within the Incident Management app. The app has five default user groups:

- Portal Access : Users in this group can access the portal where they can submit incidents, review draft incidents, or amend incidents that were sent back for them from the Incident Screener. This user group also provides an area for occasional users across all applications to perform work. This includes task owners, issue owners, BOLO report broadcasts and **Announcements**.
- Incident Screener : Users in this group are responsible for managing incidents in the **Triage** state, including assigning incident owners, supervisors, or investigators.
- Incident Owner : Users in this group review incidents for accuracy and completion and can close the incident, return it to the **Triage**, or open an investigation. In some cases, incident owners can also create their own incidents. The Incident Owner of an incident has exclusive access to the entire record, including related data, and thus this is the central user group within Incident Management.
- Incident Investigator : These users examine the root cause and outcome of an incident. Investigators add interviews and evidence, and link the incident to related incidents and persons.
- Incident Supervisor : These users manage incidents in a **Closed** or **Review** state.
- Incident Management Administrator : These users monitor the application and have access to view all incident data.
- Administrator : Users in this group oversee the Incident Management app and are responsible for adding users and Library objects.

For more information on these user groups and the tasks they can perform, see the additional sections in this guide.

Emails Overview

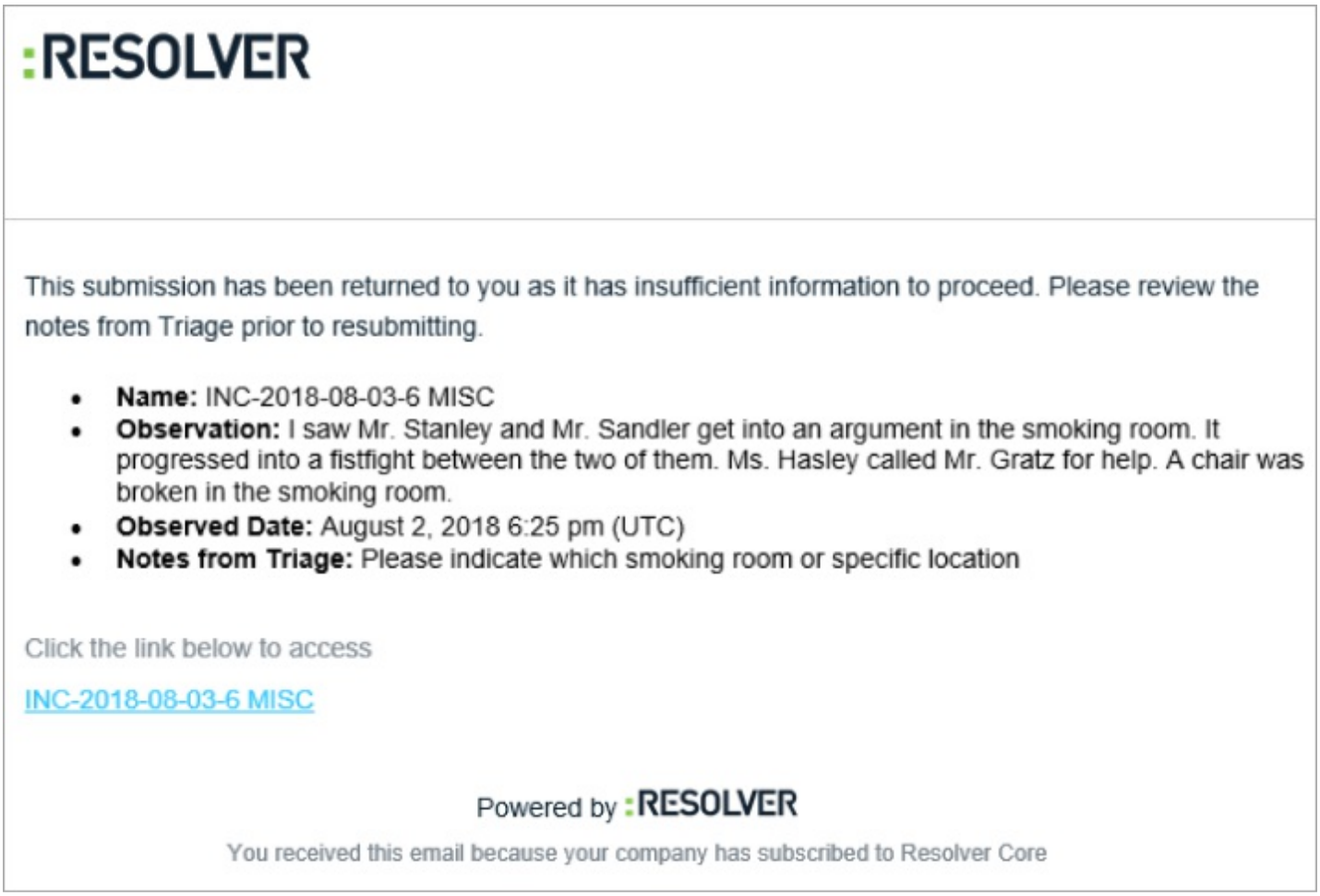
If an incident or task requires a user's attention, Incident Management will send an email with a link to the applicable form. Emails are sent to users based on their user group, so emails received may vary from user to user.



An email notification sent to an incident investigator.

Portal Access Email Notifications

Users in the Portal Access user group receive a **Submitter Return Notification** when an incident is returned to the Portal Access user by the Incident Screener.



:RESOLVER

This submission has been returned to you as it has insufficient information to proceed. Please review the notes from Triage prior to resubmitting.

- **Name:** INC-2018-08-03-6 MISC
- **Observation:** I saw Mr. Stanley and Mr. Sandler get into an argument in the smoking room. It progressed into a fistfight between the two of them. Ms. Hasley called Mr. Gratz for help. A chair was broken in the smoking room.
- **Observed Date:** August 2, 2018 6:25 pm (UTC)
- **Notes from Triage:** Please indicate which smoking room or specific location

Click the link below to access

INC-2018-08-03-6 MISC

Powered by :RESOLVER

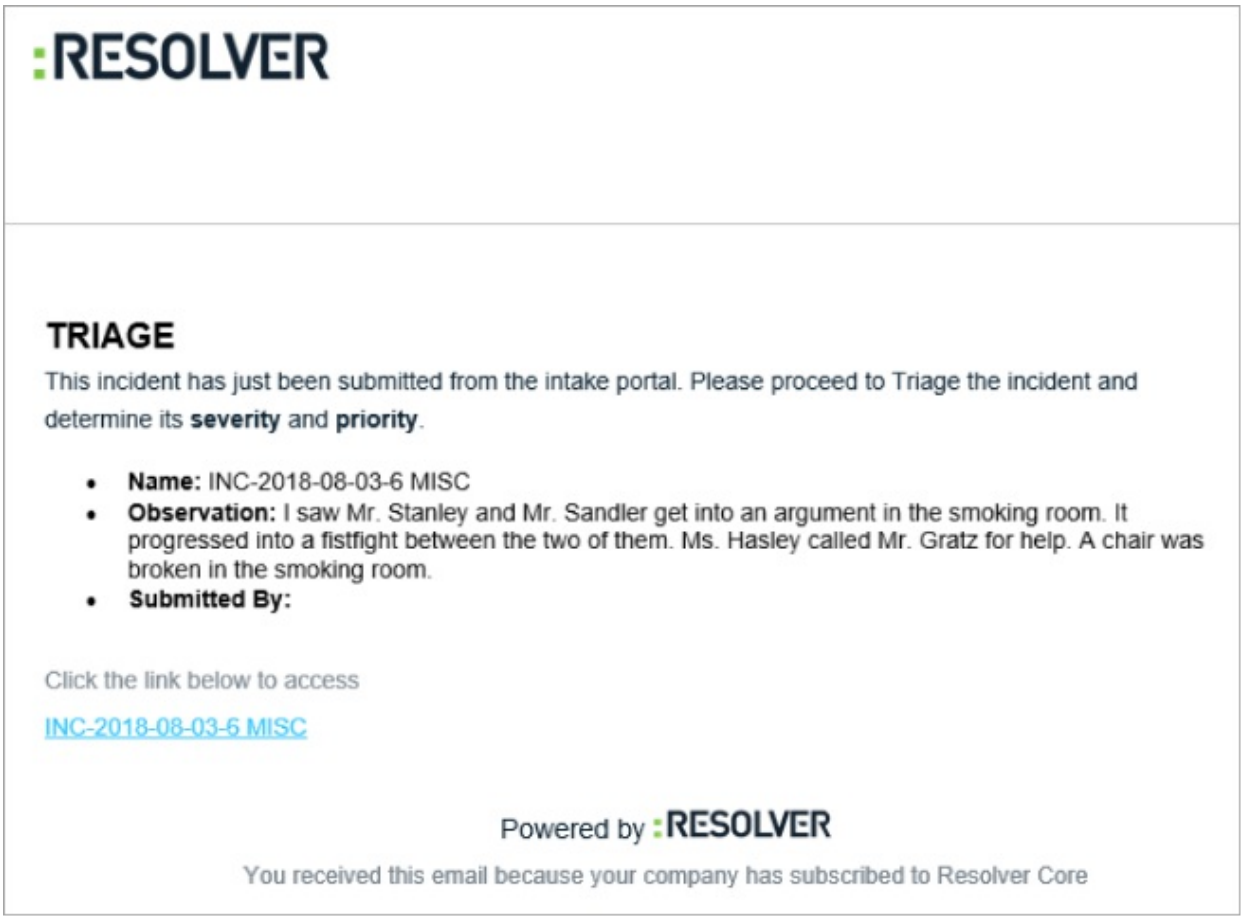
You received this email because your company has subscribed to Resolver Core

A submitter return notification email.

Incident Screener Email Notifications

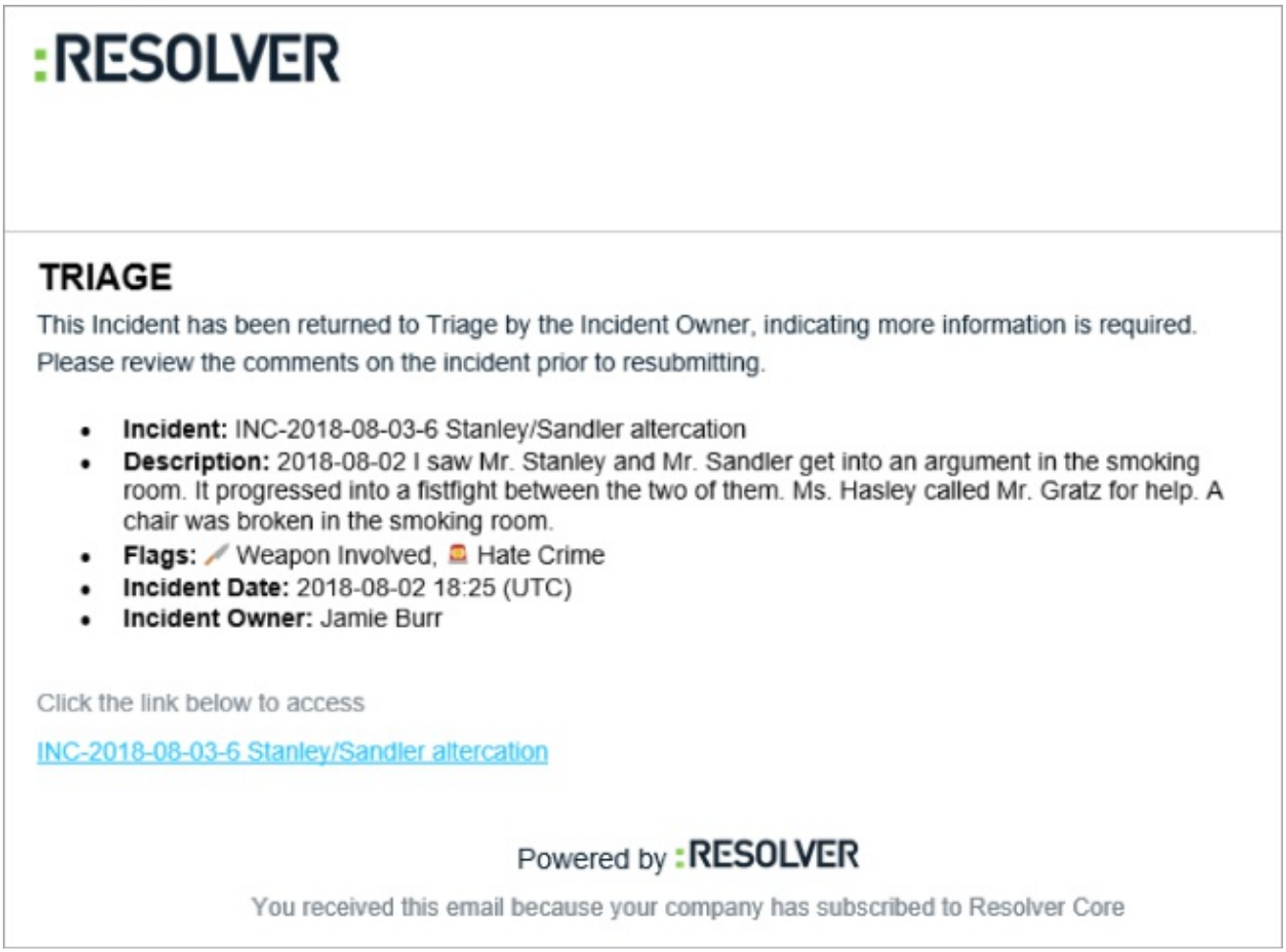
The following email notifications are sent to users in the Incident Screener user group:

- **Incident Triage Notification**: Triggered when an Incident has been created in the portal.



An incident triage notification email.

- **Triage Return Notification**: Triggered when an incident is returned to the Triage by the Incident Owner.

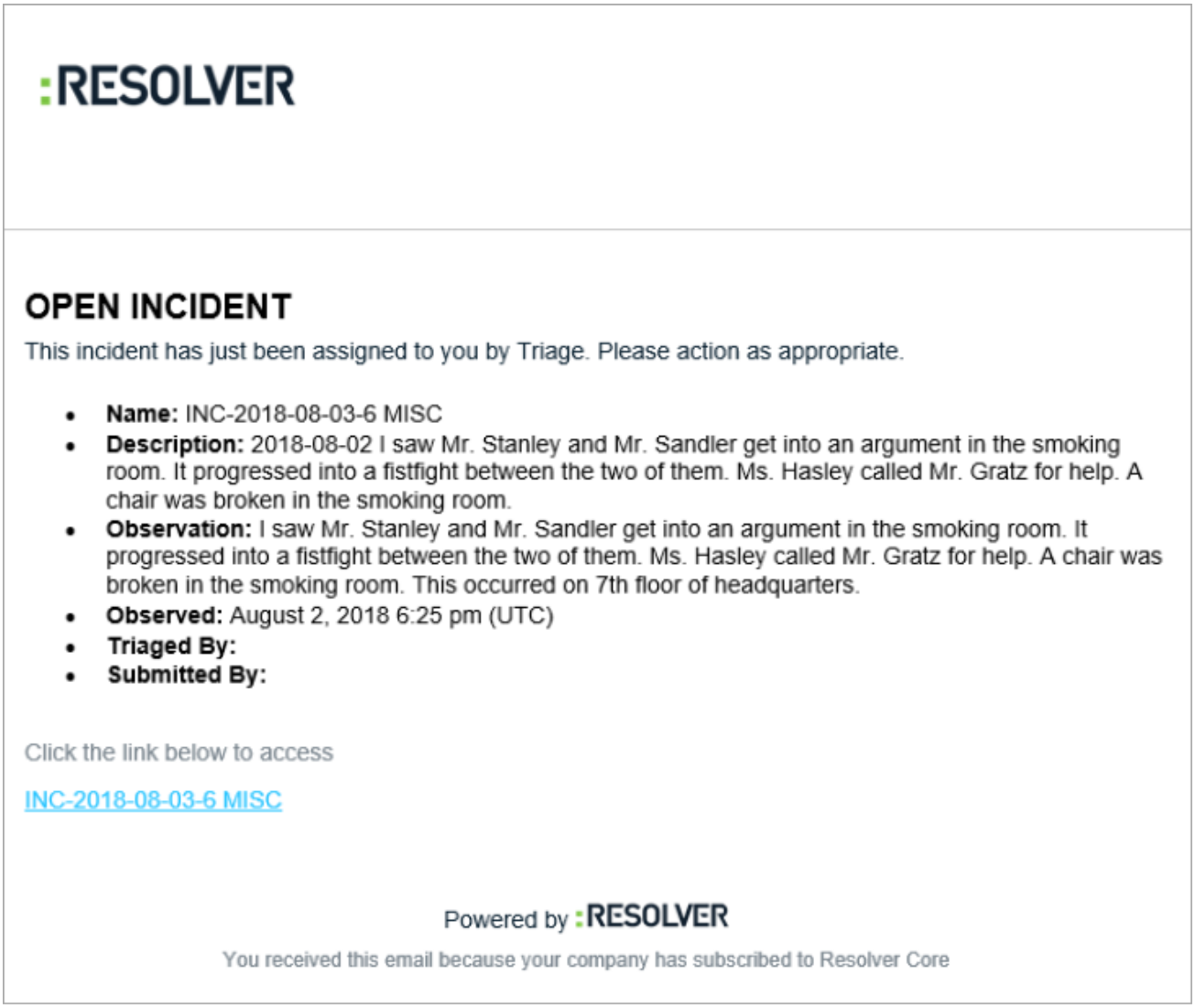


A triage return notification email.

Incident Owner Email Notifications

The following email notifications are sent to users in the Incident Owner user group:

- **Incident Open Notification**: Triggered when an incident has been completed by the Incident Screener.



:RESOLVER

OPEN INCIDENT

This incident has just been assigned to you by Triage. Please action as appropriate.

- **Name:** INC-2018-08-03-6 MISC
- **Description:** 2018-08-02 I saw Mr. Stanley and Mr. Sandler get into an argument in the smoking room. It progressed into a fistfight between the two of them. Ms. Hasley called Mr. Gratz for help. A chair was broken in the smoking room.
- **Observation:** I saw Mr. Stanley and Mr. Sandler get into an argument in the smoking room. It progressed into a fistfight between the two of them. Ms. Hasley called Mr. Gratz for help. A chair was broken in the smoking room. This occurred on 7th floor of headquarters.
- **Observed:** August 2, 2018 6:25 pm (UTC)
- **Triaged By:**
- **Submitted By:**

Click the link below to access

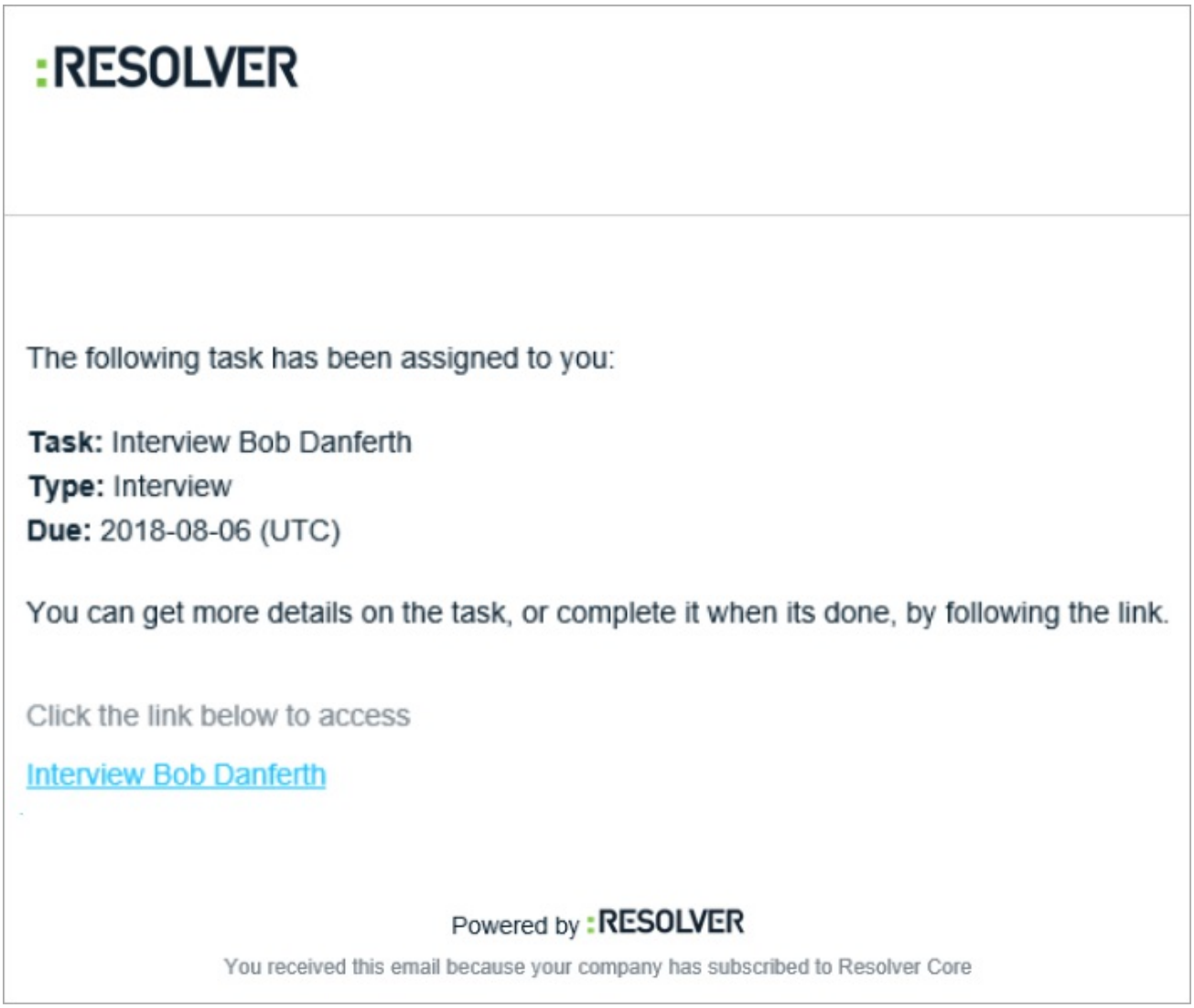
INC-2018-08-03-6 MISC

Powered by :RESOLVER

You received this email because your company has subscribed to Resolver Core

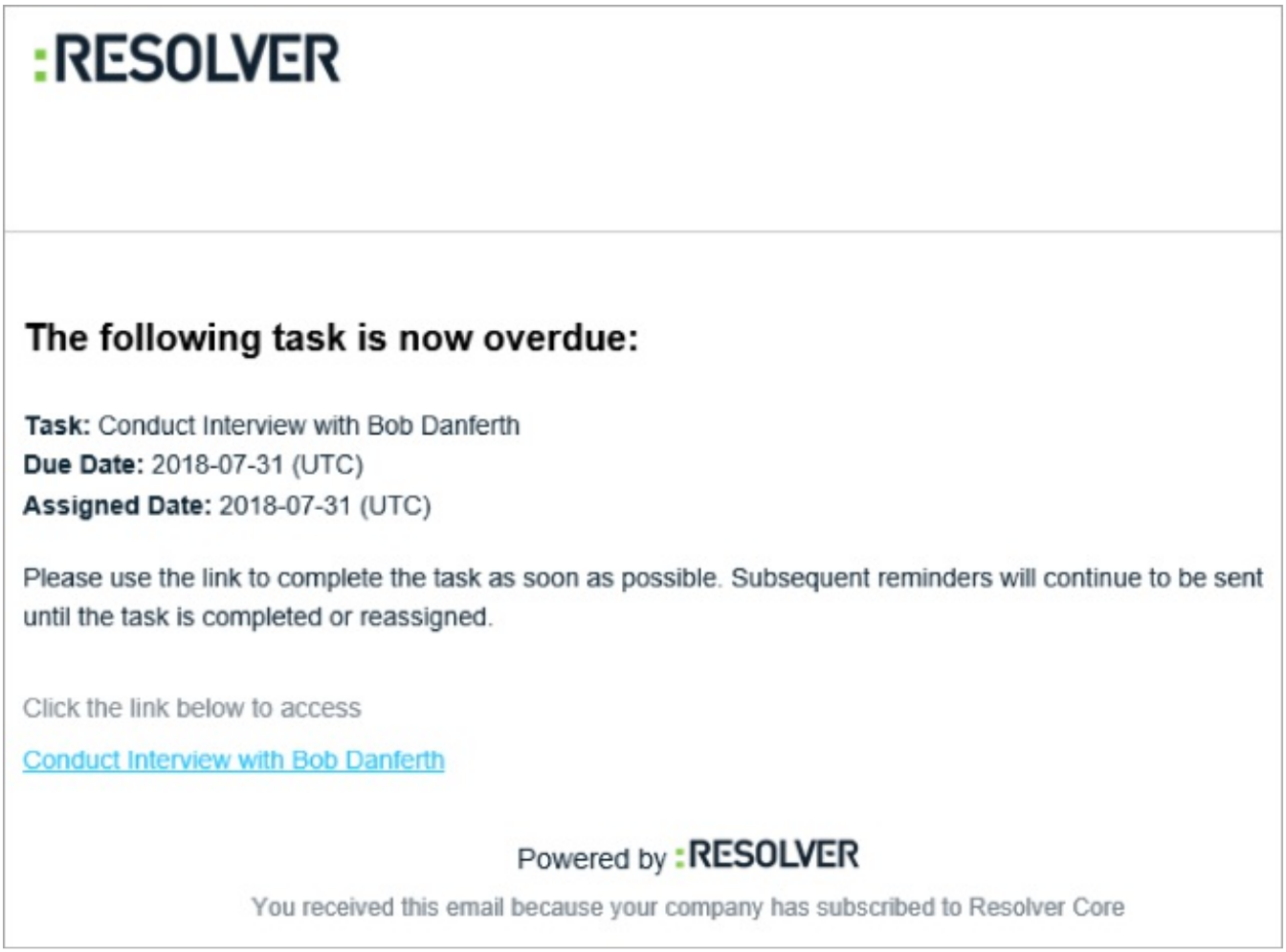
An incident open email notification.

- **Task Assignment**: Triggered when an incident task has been created and assigned to an incident owner.



A task assignment email notification.

- **Task Overdue**: Sent to the incident owner when a task has not been completed and is past its due date. This notification will be sent every day until the task is marked complete.


:RESOLVER

The following task is now overdue:

Task: Conduct Interview with Bob Danferth
Due Date: 2018-07-31 (UTC)
Assigned Date: 2018-07-31 (UTC)

Please use the link to complete the task as soon as possible. Subsequent reminders will continue to be sent until the task is completed or reassigned.

Click the link below to access

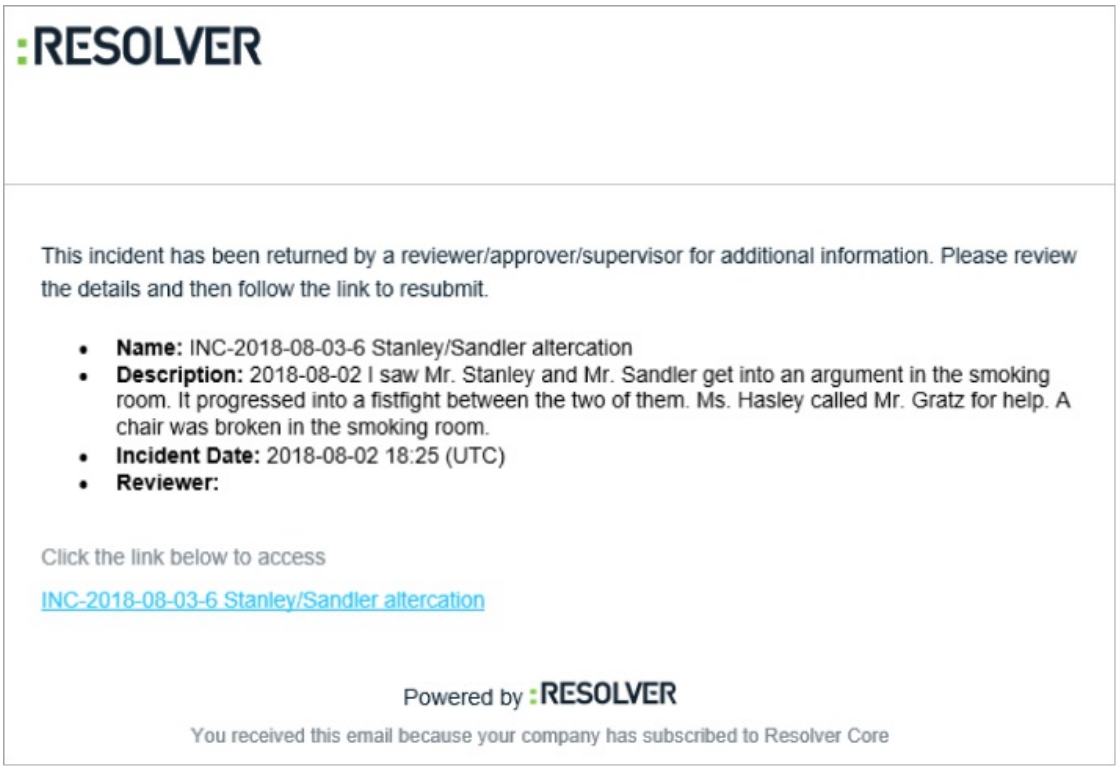
Conduct Interview with Bob Danferth

Powered by :RESOLVER

You received this email because your company has subscribed to Resolver Core

A task overdue email notification.

- **Review Returned**: Triggered when an Incident is returned by a Reviewer for more information.


:RESOLVER

This incident has been returned by a reviewer/approver/supervisor for additional information. Please review the details and then follow the link to resubmit.

- **Name:** INC-2018-08-03-6 Stanley/Sandler altercation
- **Description:** 2018-08-02 I saw Mr. Stanley and Mr. Sandler get into an argument in the smoking room. It progressed into a fistfight between the two of them. Ms. Hasley called Mr. Gratz for help. A chair was broken in the smoking room.
- **Incident Date:** 2018-08-02 18:25 (UTC)
- **Reviewer:**

Click the link below to access

INC-2018-08-03-6 Stanley/Sandler altercation

Powered by :RESOLVER

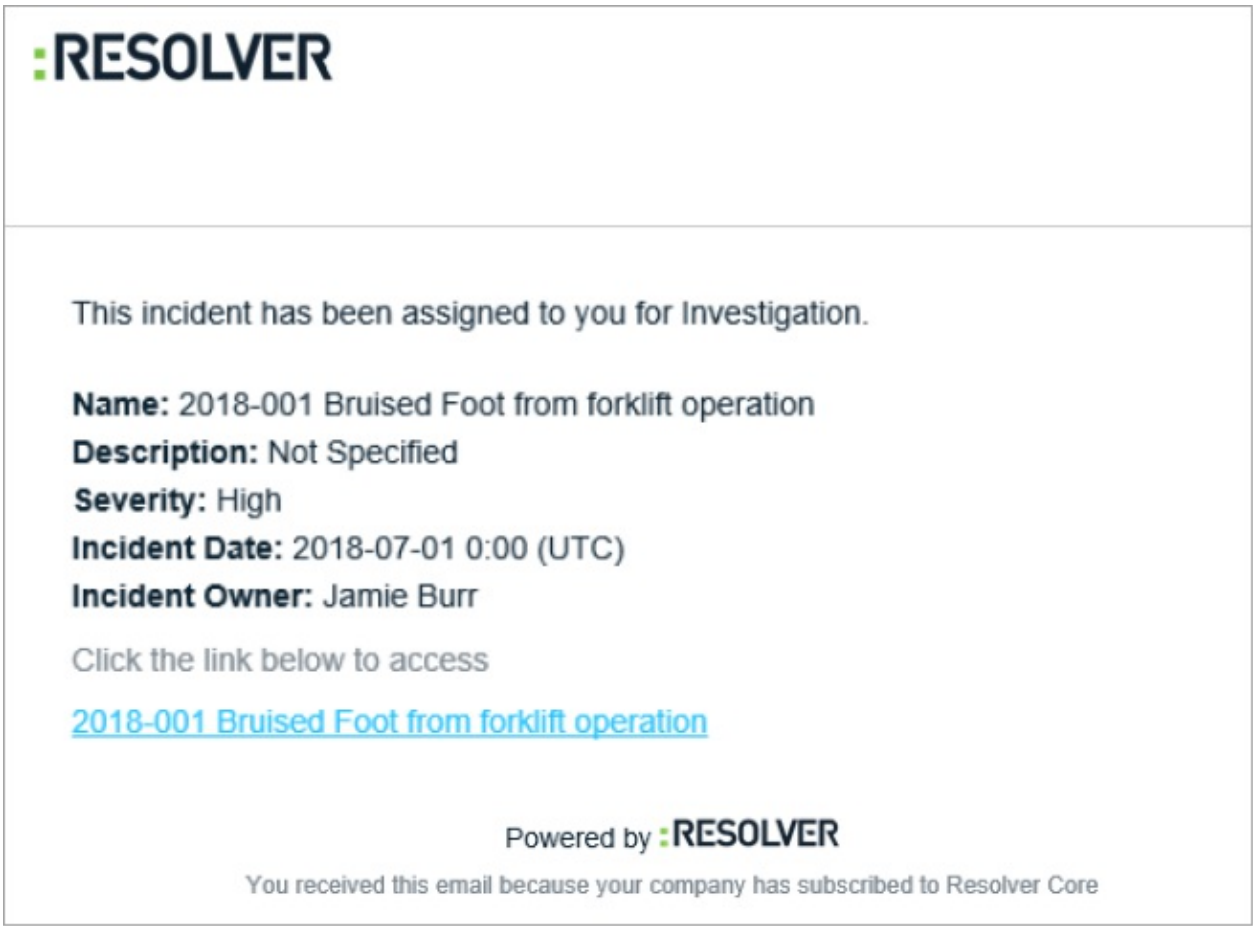
You received this email because your company has subscribed to Resolver Core

A review returned email notification.

Incident Investigator Email Notifications

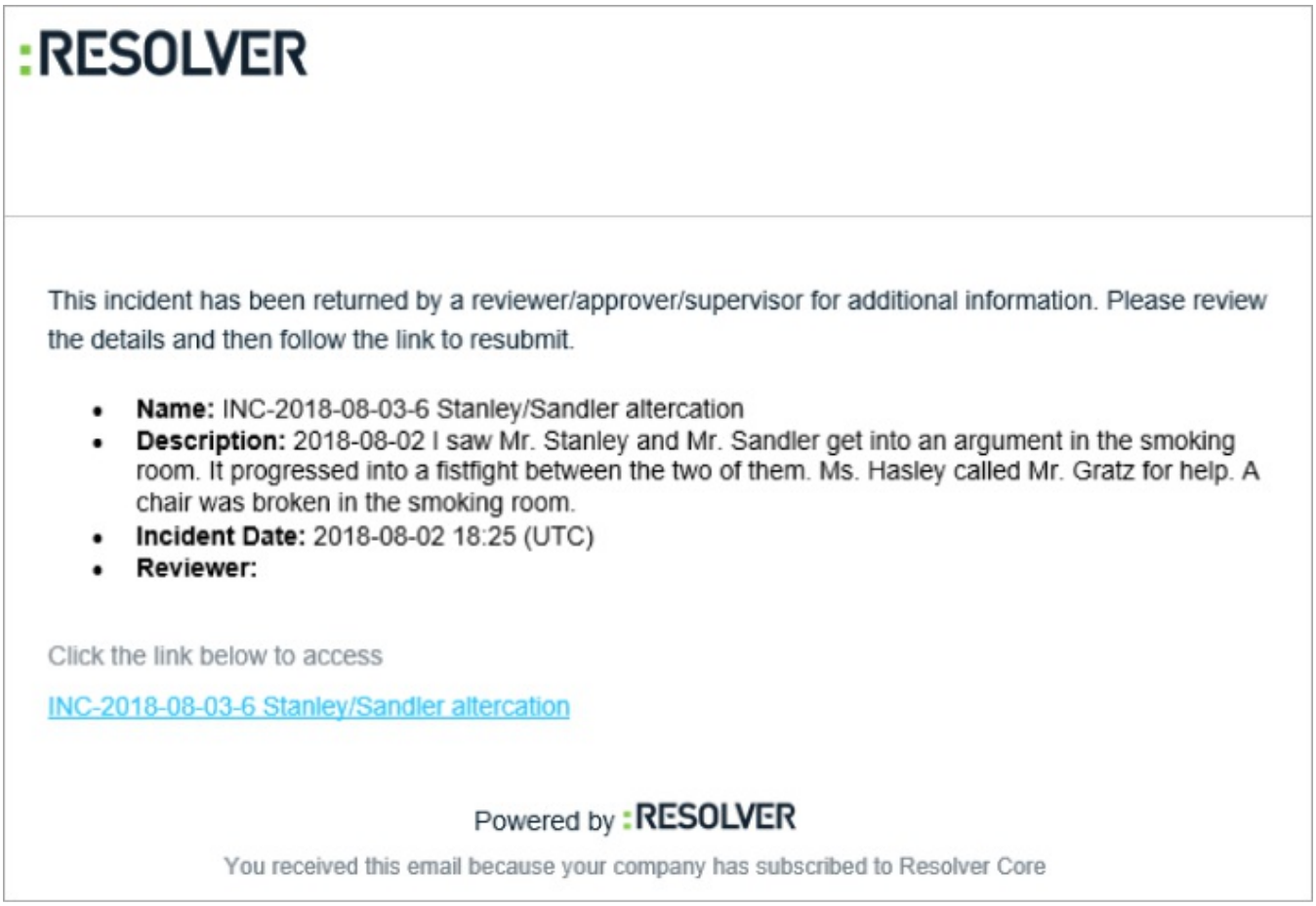
The following email notifications are sent to users in the Incident Investigator user group:

- **Investigation Notification**: Triggered when an incident has been escalated to an investigation.



An investigation notification email.

- **Review Returned**: Triggered when an Incident is returned by a Reviewer for more information.

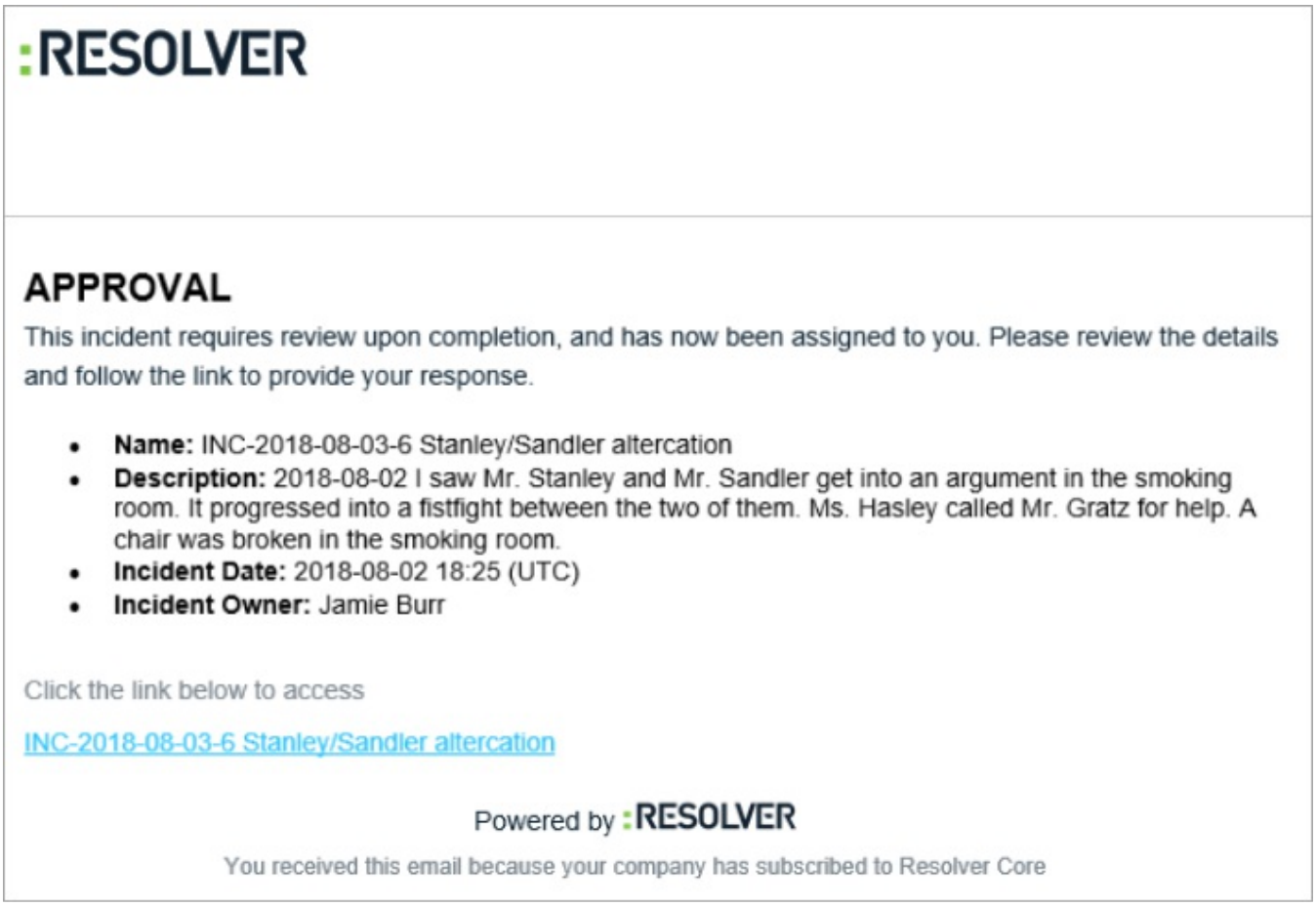


A review returned email notification.

Incident Supervisor Email Notifications

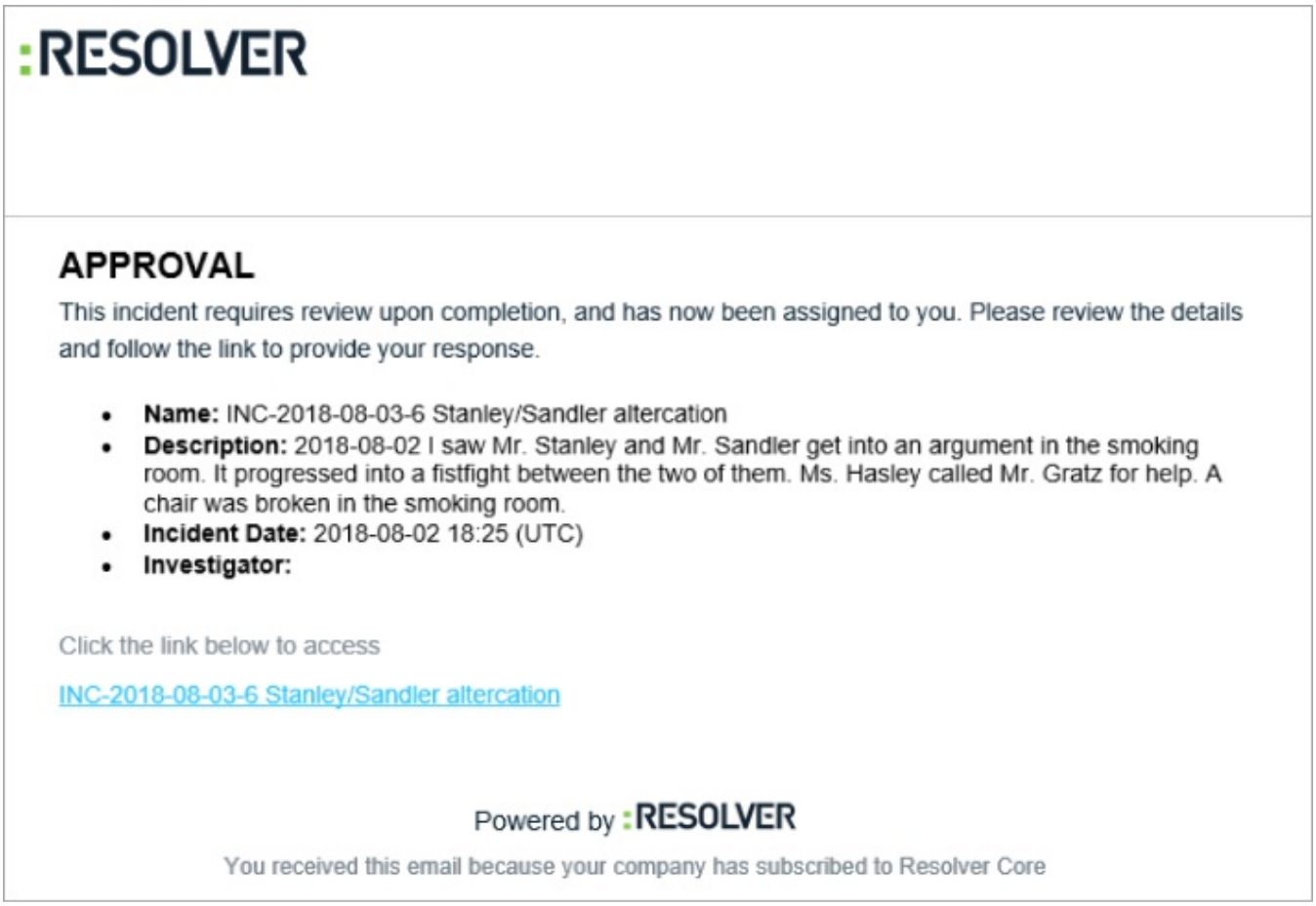
The following email notifications are sent to users in the Incident Supervisor user group:

- **Incident to Review**: Triggered when an incident is completed for review.



An incident to review email notification.

- **Investigation to Review**: Triggered when an Investigation is completed for review.

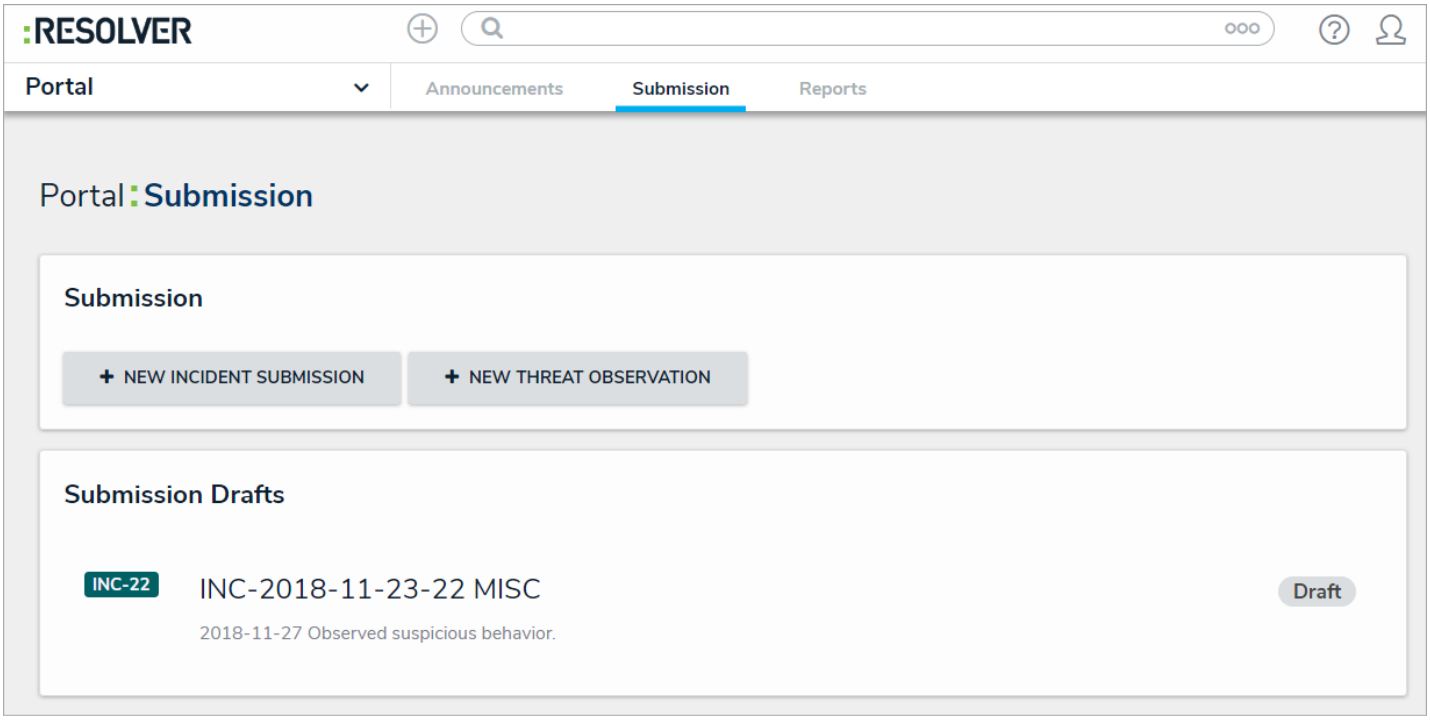


An investigation to review email notification.

Portal Access Overview

Users in the **Portal Access** user group have access to the Portal application, where they can:

- Submit incidents and edit incident submission drafts;
- View incident reports;
- View announcements;
- Respond to Assigned Tasks; and
- Respond to Assigned Issues.



The Portal application.

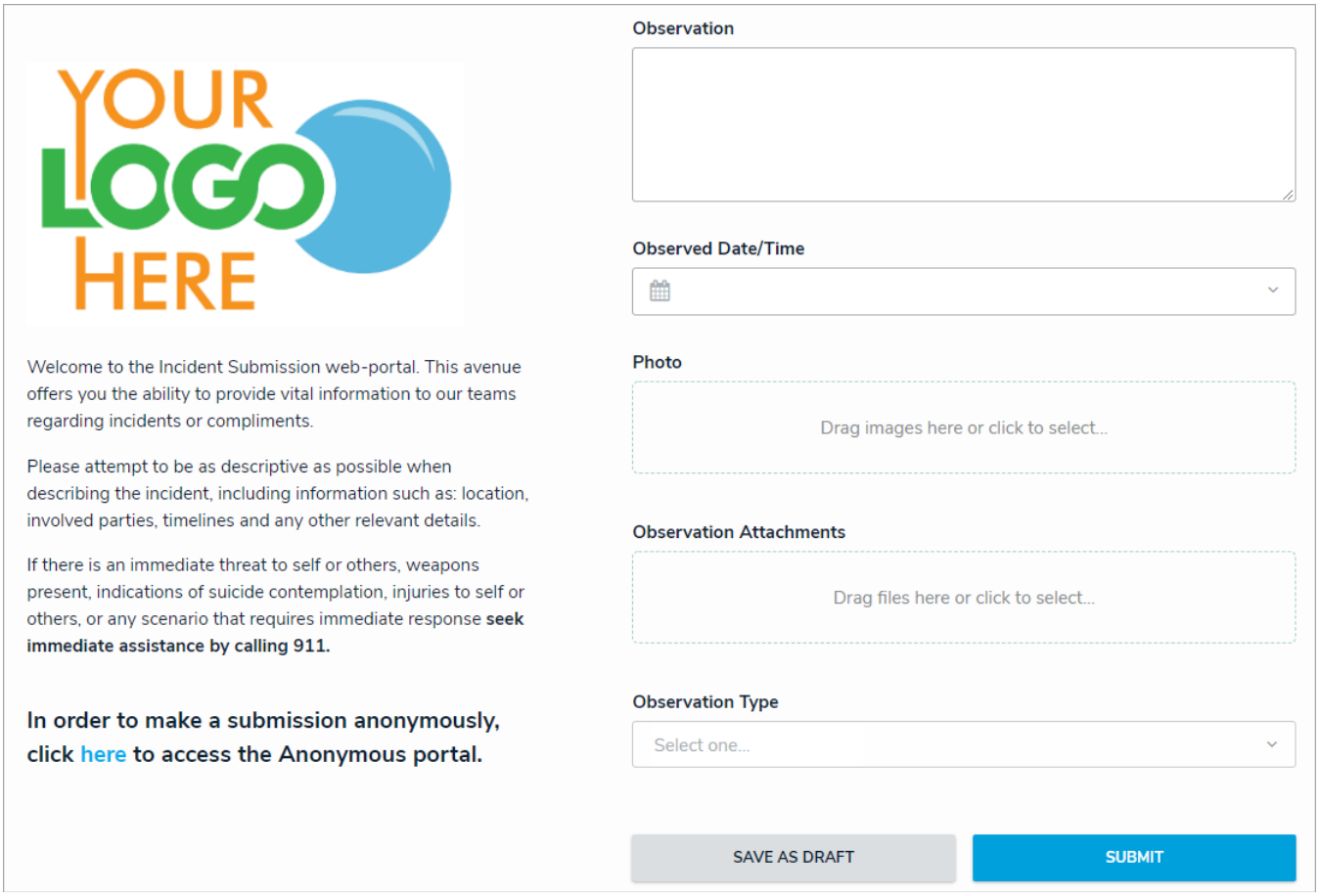
Submit an Incident

To submit an incident through the portal:

1. Log into a user account that's been added to the **Portal Access** user group.
2. Click the dropdown menu in the nav bar, then click **Portal**.

The Portal application in the nav bar.

3. Click the **Submission** tab.
4. Click **New Incident Submission**.



The Create Incident form.

5. Enter details of the incident in the **Observation** field and select a date and time from the **Observed Date/Time** field.
6. Drag images and attachments to the **Photo** and **Observation Attachments** sections to add them to your submission. You can also click in the box below **Photo** or **Observation Attachments** to browse for files on your machine.

7. Click **Submit** to submit the incident or **Save as Draft** to review or edit the incident later.

> ⚠ Navigating away from the incident form before clicking **Submit** or **Save as Draft** will delete any change made to the form.

Review Your Draft Incidents

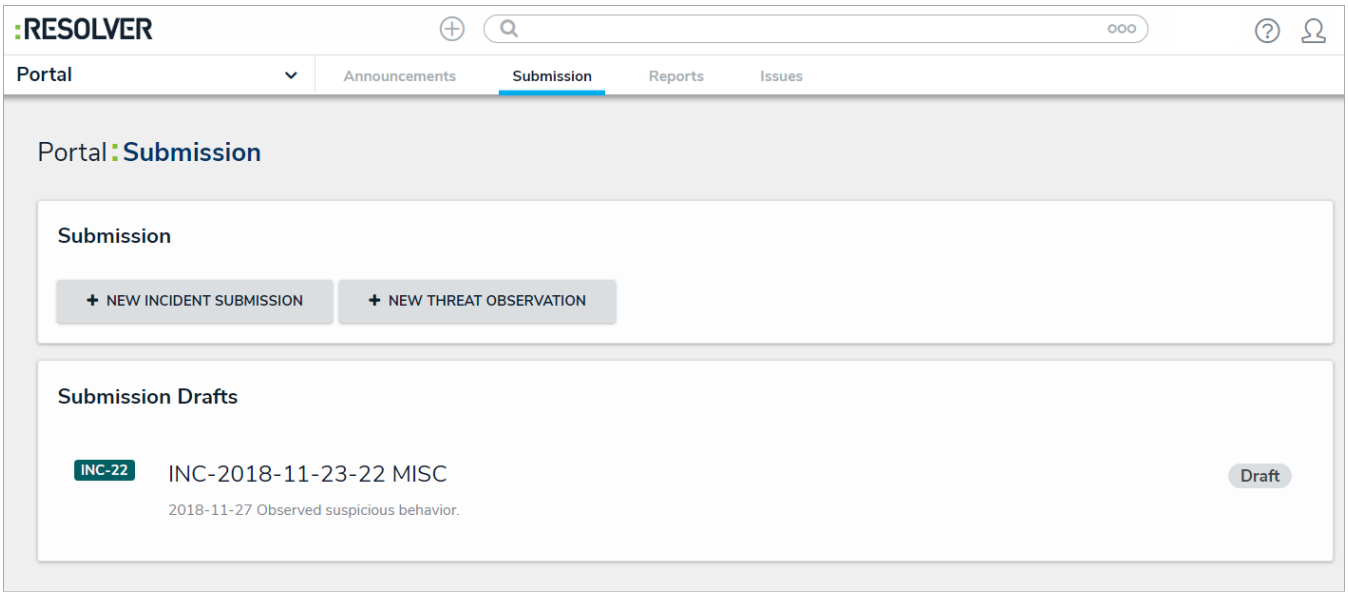
If you click the **Save as Draft** button when submitting an incident, you can view and edit your draft in the **Submission Drafts** section before submitting. Any incidents that are sent back to you for review by the Incident Screener will also appear in **Submission Drafts**. You will receive an email notification if an incident is sent back to you for review.

To review your draft incidents:

1. Log into a user account that's been added to the **Portal Access** user group.
2. Click the dropdown menu in the nav bar, then click **Portal**.

The Portal application in the nav bar.

3. Click the **Submission** tab.



The Submission Drafts section.

4. Click an incident in the **Submission Drafts** section to display the form.
5. Review the data in the form, including any comments made by the **Incident Screener**, and make your changes as needed.
6. Click **Submit** to send the form to triage or click **Save as Draft** to return the form to your drafts.

Submit an Incident Anonymously

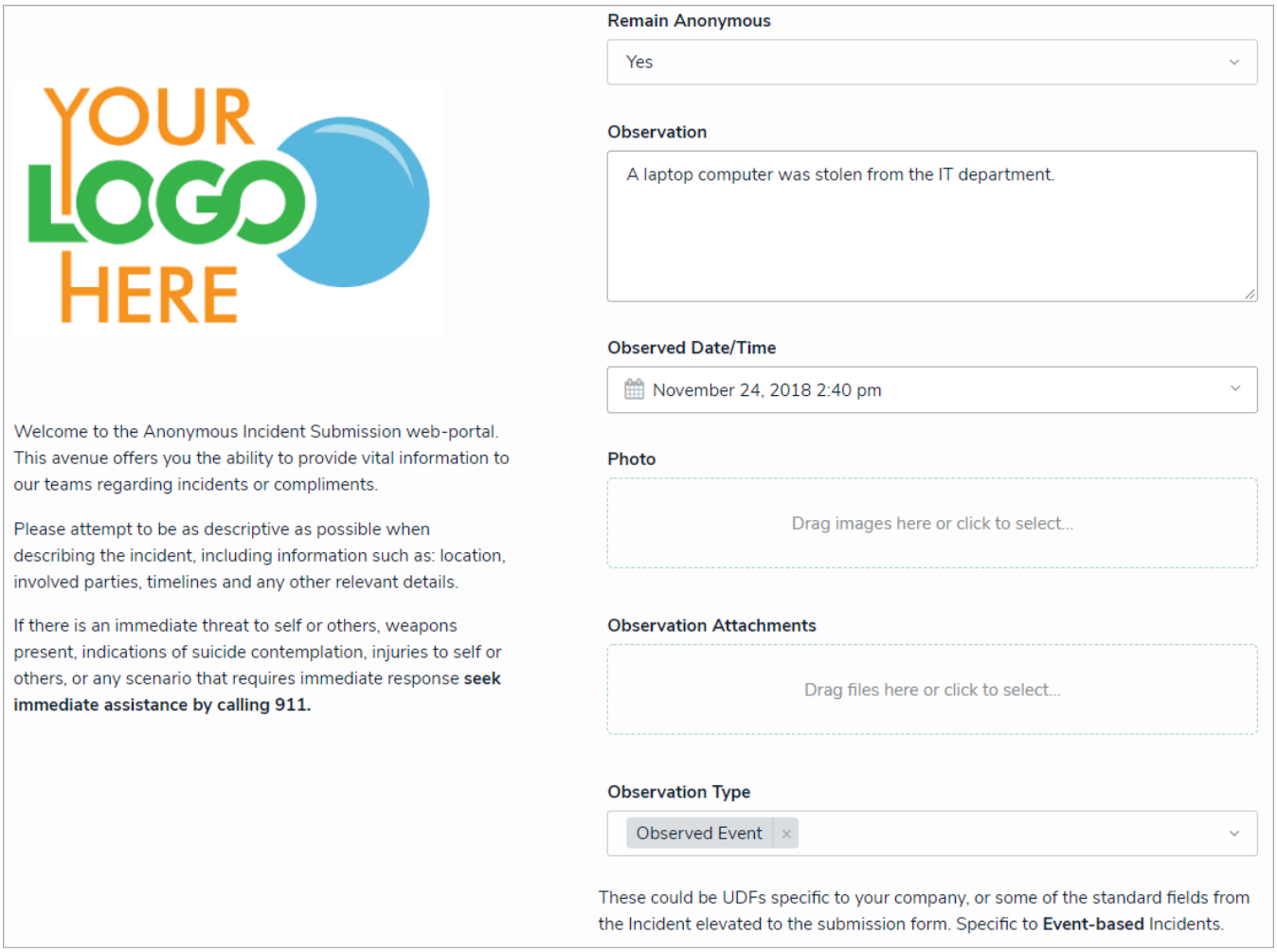
These instructions are for submitting an incident anonymously while logged into the app. If you want to submit an incident from your account, see the Submit an Incident article. If your organization has given you a direct link to the **Anonymous Portal**, you can skip to step 5.

To submit an incident anonymously:

1. Log into a user account that's been added to the **Portal Access** user group.
2. Click the dropdown menu in the nav bar, then click **Portal**.

The Portal application in the nav bar.

3. Click the **Submission** tab.
4. Click **New Incident Submission**.
5. Click the link to the Anonymous portal to display the anonymous incident form.
6. Select **Yes** in the **Remain Anonymous** dropdown menu.



A completed anonymous incident submission.

7. Enter details of the incident in the **Observation** field and select a date and time from the **Observed Date/Time** field.
8. Drag images and attachments to the **Photo** and **Observation Attachments** fields to add them to your submission. You can also click in the box below **Photo** or **Observation Attachments** to browse for files on your machine.
9. Click the **Observation Type** dropdown to select an observation type.
10. Click **Submit**.

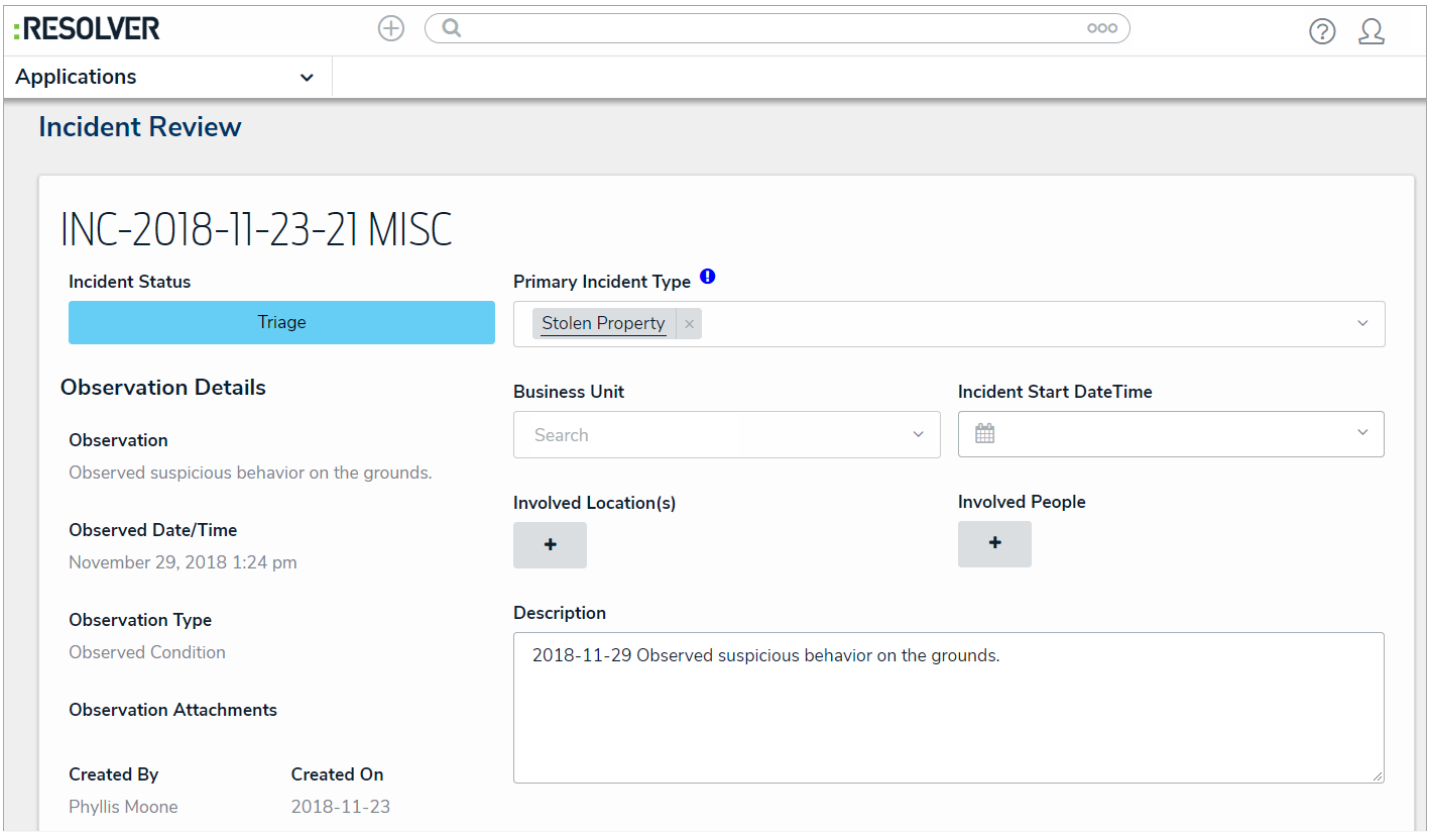
> ⚠ Navigating away from the incident form before clicking **Submit** will delete any change made to the form.

Incident Screener Overview

When an employee submits an incident through the Portal , that incident object is sent to users in the **Incident Screener** user group. Users in this group are responsible for managing incidents in the **Triage** state, including:

- Providing additional details about the incident, such as business unit, date and time, and involvements, depending on the incident type chosen;
- Assigning incident owners, supervisors, or investigators;
- Adding comments about the incident; and
- Returning the incident object back to the employee as a draft to collect additional information.

The primary objective of the Incident Screener is to ensure an accurate primary incident type is selected. Incident screeners can also read incidents in an **Open** state, read and edit incidents in the **Draft** state, or create new incident objects, depending on the primary incident type chosen.



An incident object as it's displayed to a user in the Incident Screener user group.

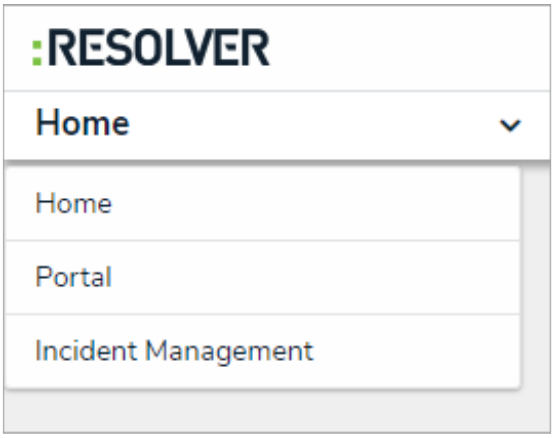
Triage an Incident

The following provides instructions for accessing incidents in the **Triage** state from the **Incident Management** application, however, **Incident Screeners** can also view and open these incidents from the homepage (My Tasks).

To triage an incident:

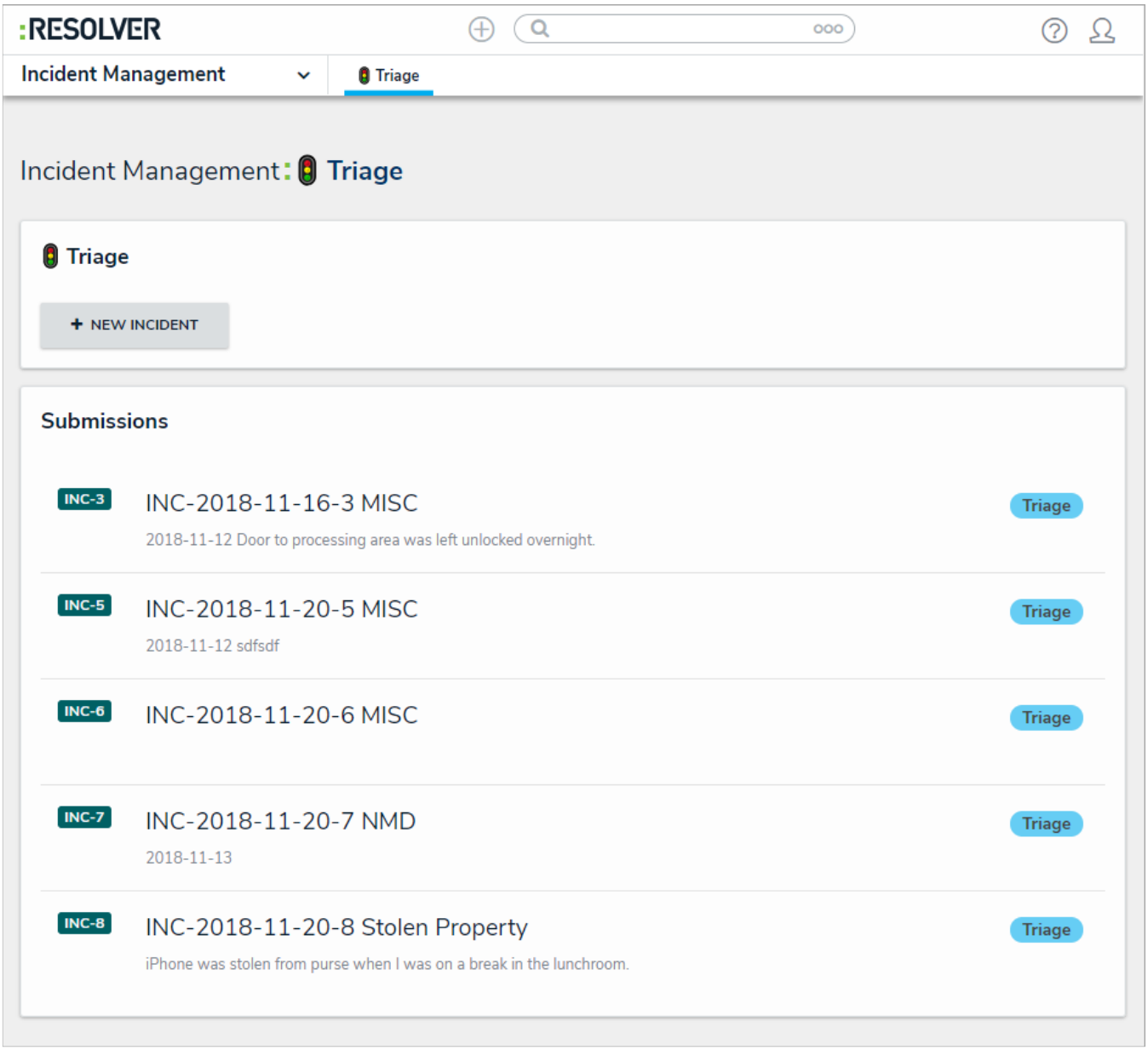
> Incident screeners receive emails when incidents are submitted through the portal. Click the link in the email to go directly to the Triage form and skip to step 4.

1. Log into a user account that's been added to the **Incident Screener** user group.
2. Click the dropdown in the nav bar **> Incident Management** to display the **Triage** activity.



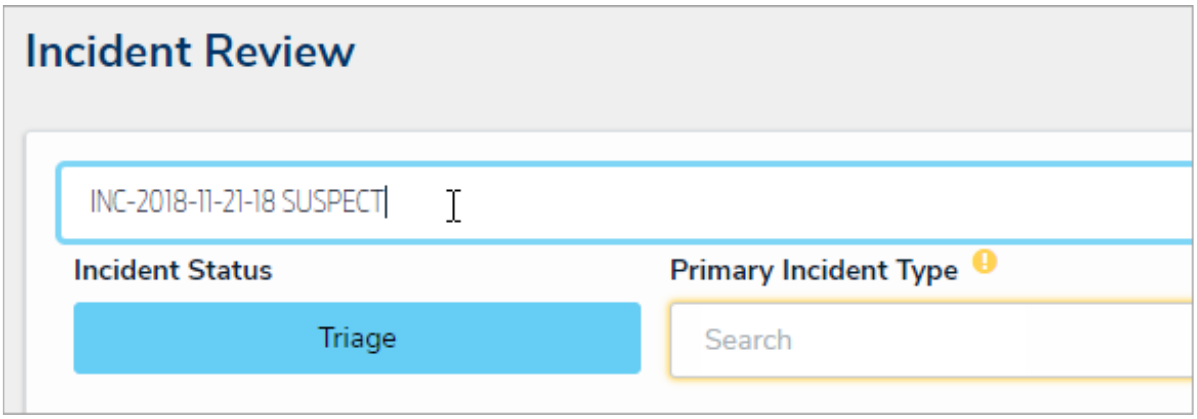
The nav bar.

3. Click an incident in the **Submissions** section to display it.



The Triage section of Incident Management.

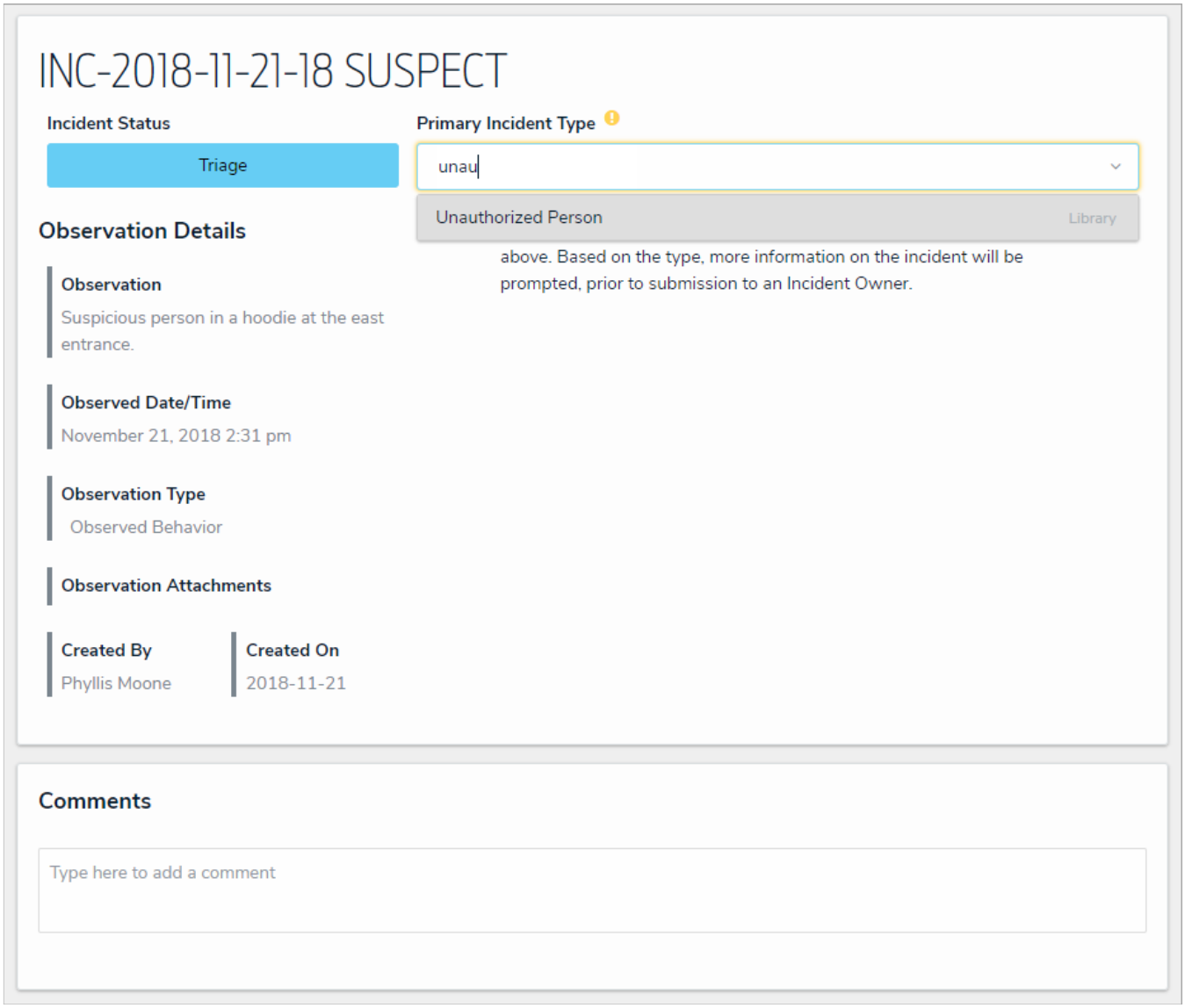
4. **Optional:** Click the title of the incident (e.g. INC-2018-11-21 MISC) to make changes to the title as needed, then click away from the title to save your changes.



Clicking the name of the incident object will allow you to make changes as needed.

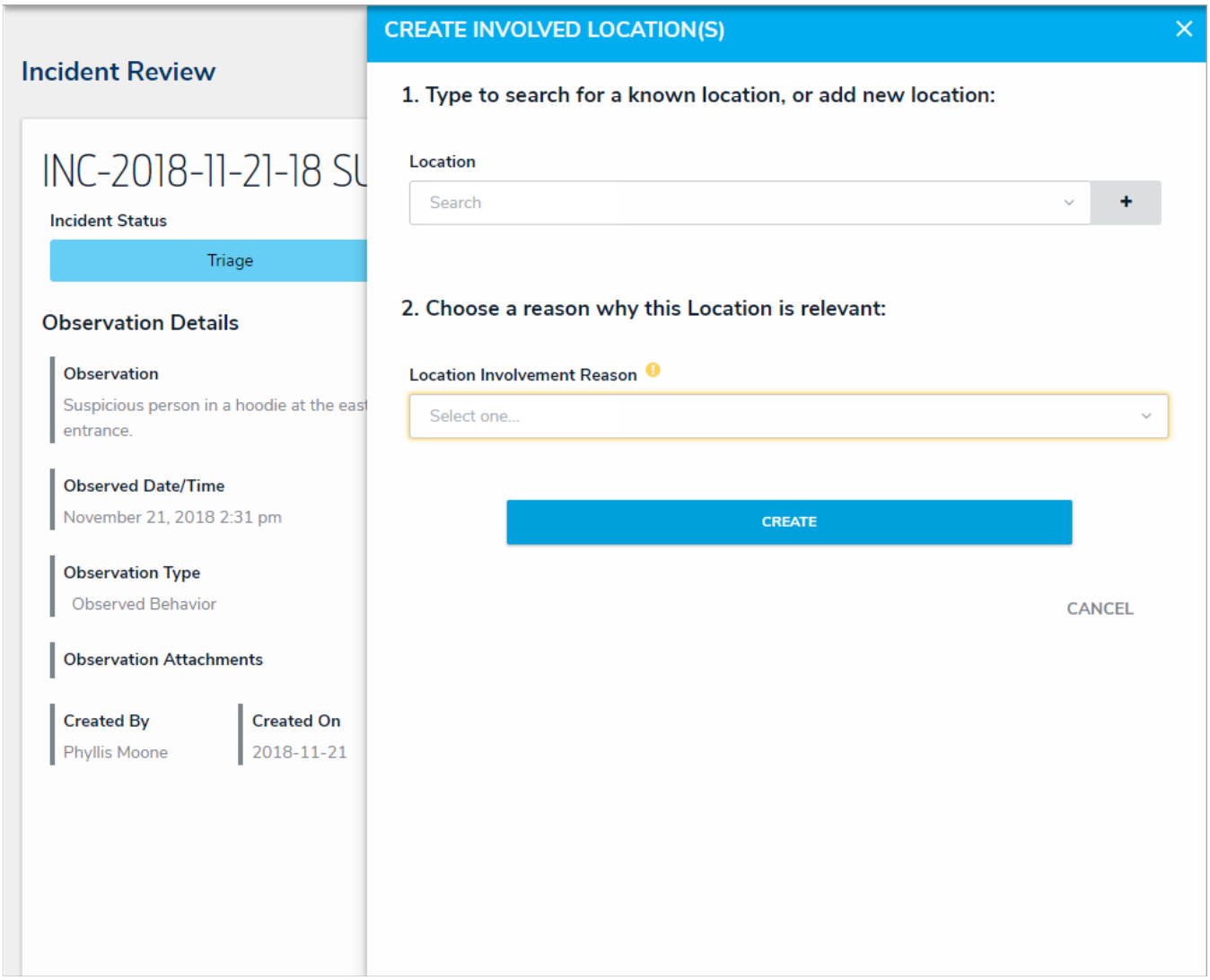
5. Click the **Primary Incident Type** field, then begin typing keywords to display a list of available options, then click to select

the appropriate incident type based on the **Observation Details** provided by the submitting employee. Your selection in this field will display additional fields on the form, which will vary depending on the incident type.



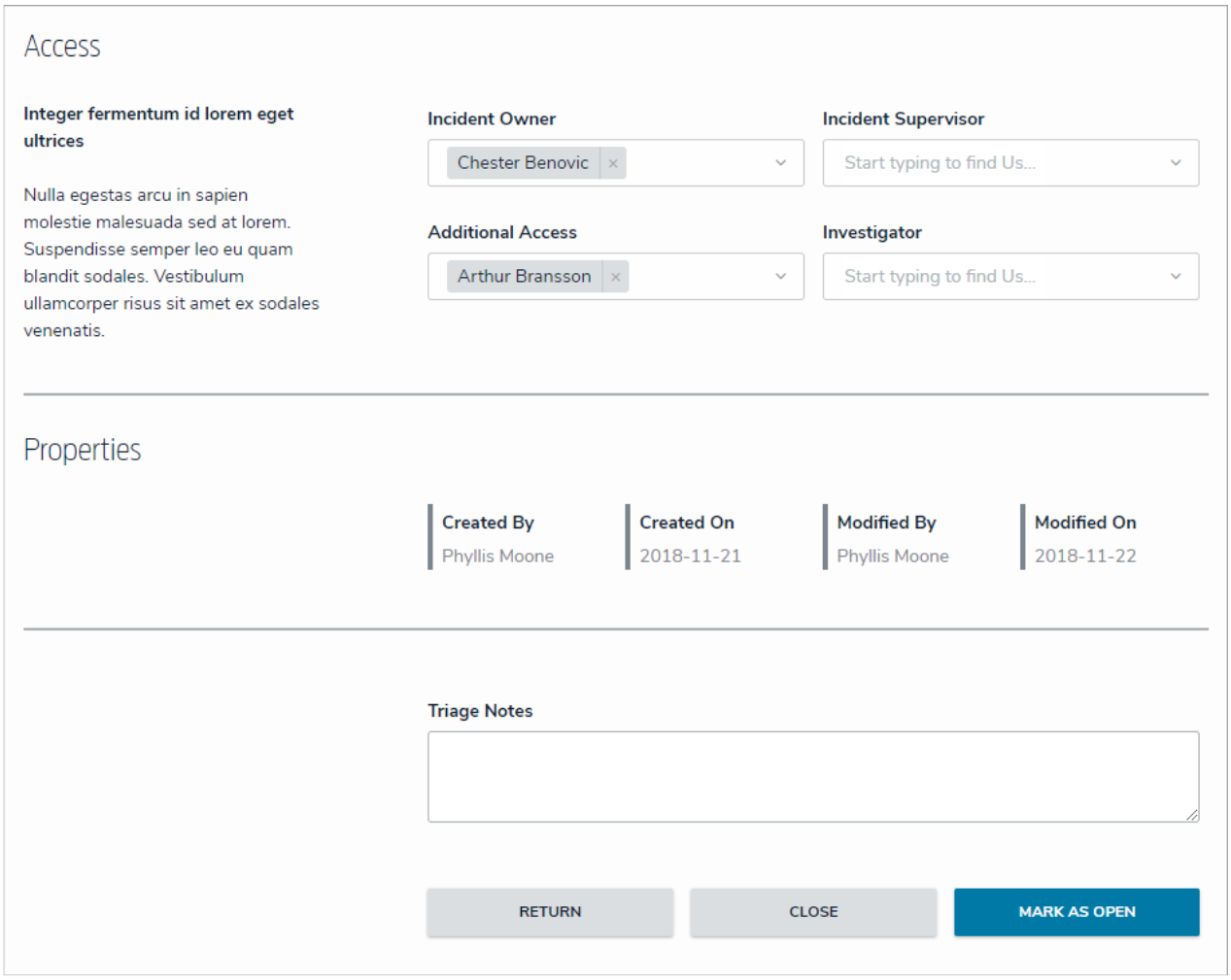
Selecting an incident type, which will determine the remainder of the fields that will need to be completed on the form.

6. If you selected an incident type that requires a business unit, region or market in step 5 above, begin typing the name of the record in the **Business Unit, Region** or **Market** field, then click to select it.
7. Select a start date and time for the incident from the **Incident Start DateTime** field.
8. To create a new involvement, click the + icon below **Involved [Location(s)**, **People**, **Organization**, **Items/Assets**, or **Vehicles]** to open the creation palette, then complete the fields as required.



The involvement palette.

9. Complete the fields in the **UDFs** section as required.
10. Define who should be able to access the incident object by selecting users or user groups in the following fields in the **Access** section:
    - **Incident Owner:** Creates and/or edits the incident objects assigned to them, as well as the appropriate rdationship objects. An email notification is sent to the user(s) once an incident is assigned to them and opened for the first time.
    - **Incident Supervisor:** Fully manages the incident objects that are in the **Archive** or **Review** state.
    - **Additional Access:** Additional users or groups who may need to access the incident.
    - **Investigator:** Documents incident investigations.
11. Enter any notes, including any additional instructions to the incident submitter, in the **Triage Notes** text box.
12. Enter comments, tagging other users if needed, in the **Comments** text box (at the bottom of the page). See the Incident Form Comments article for more information on using this feature.
13. Click one of following buttons:
    - **Return:** Returns the incident back to the submitter in the **Draft** for additional information.
    - **Close:** Closes the incident because no further action is required.
    - **Mark As Open:** Sends the incident to the user(s) in the **Incident Owner** field for further action.



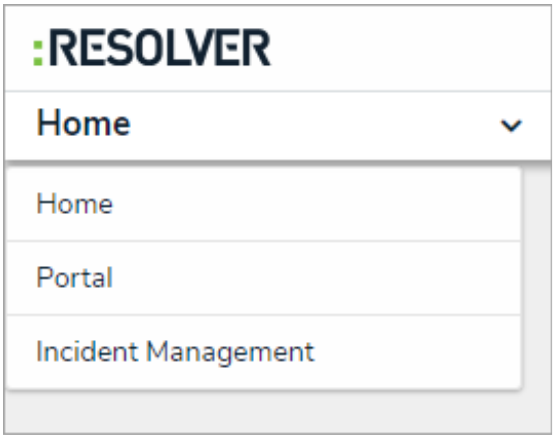
Additional fields on the incident form.

Submit an Incident from the Triage Activity

Users in the **Incident Screeners** user group can create new incident records from the **Triage** activity. The fields on this form are identical to the form accessible by portal users , except that incident screeners can select an incident type at the time of submission.

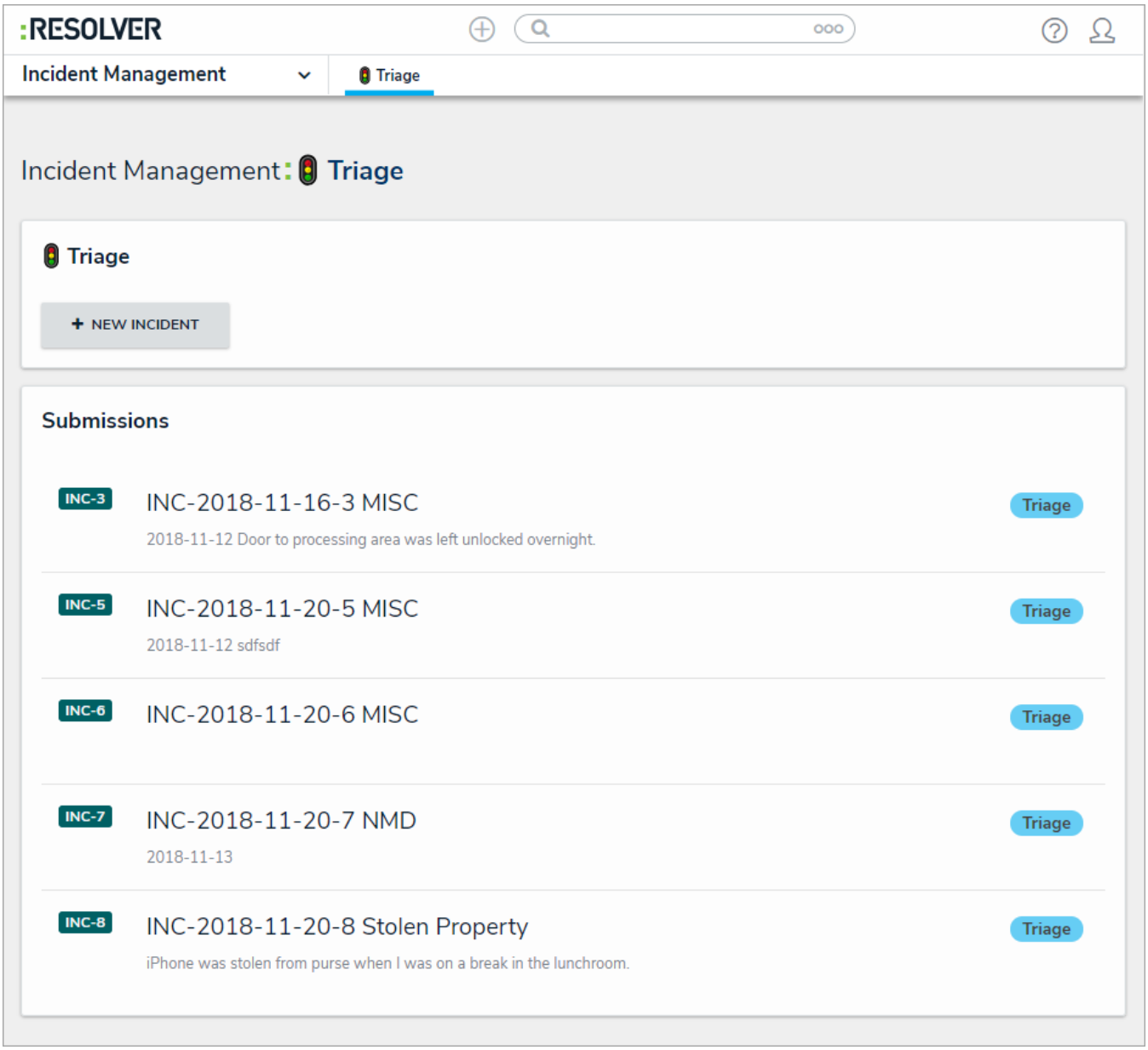
To submit an incident from the Triage activity:

1. Log into a user account that's been added to the **Incident Screener** user group.
2. Click the dropdown in the nav bar **> Incident Management** to display the **Triage** activity.



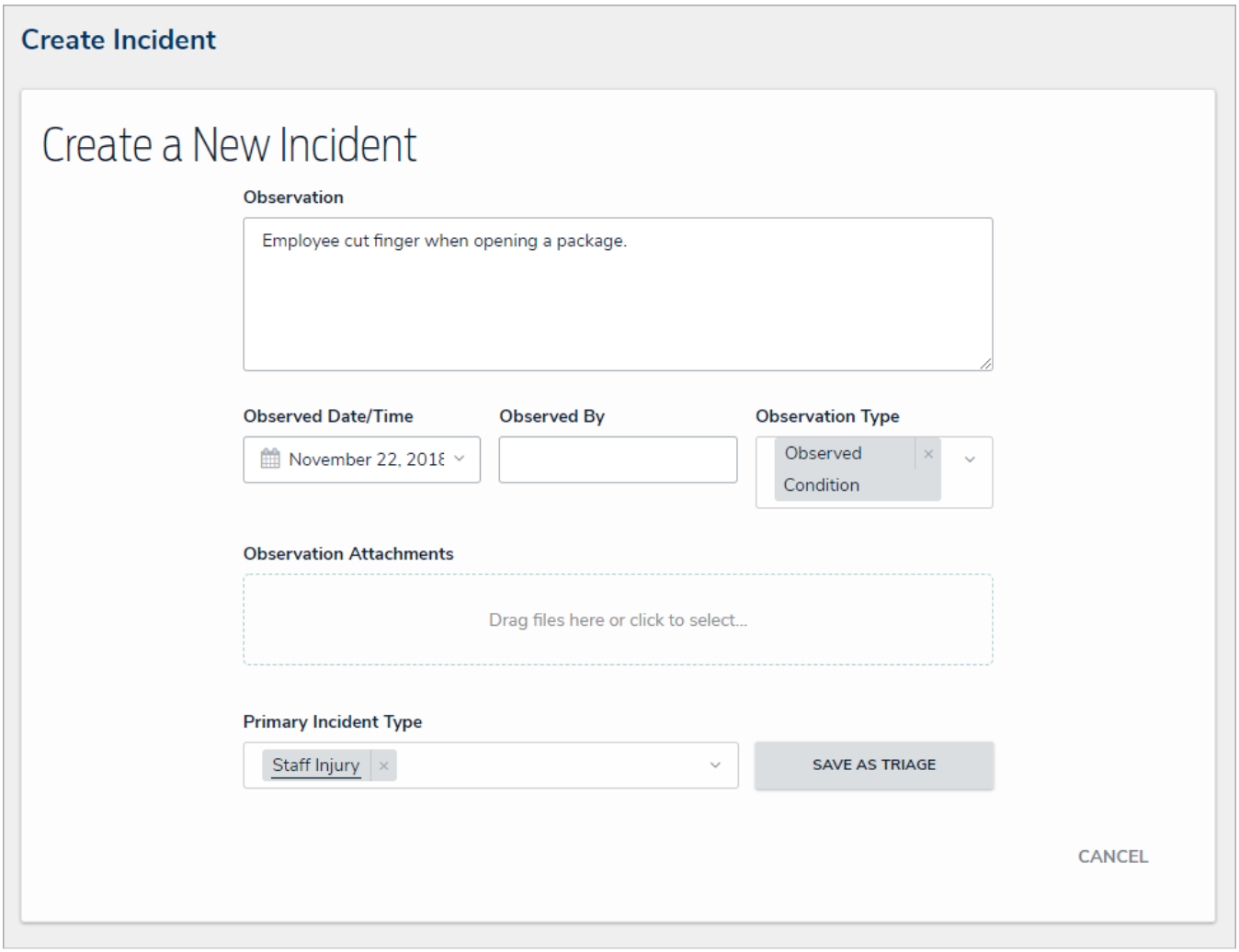
The nav bar.

3. Click **New Incident** in the **Triage** section to display the **Create a New Incident** form.



The Triage section of Incident Management.

4. Enter details of the incident, including the general notes, date and time, observation type, and attachments, as needed.
5. Select an incident type from the **Primary Incident Type** dropdown menu. Note that this field is mandatory once the incident object is saved and moved to **Triage**.



A new incident form from the Triage activity.

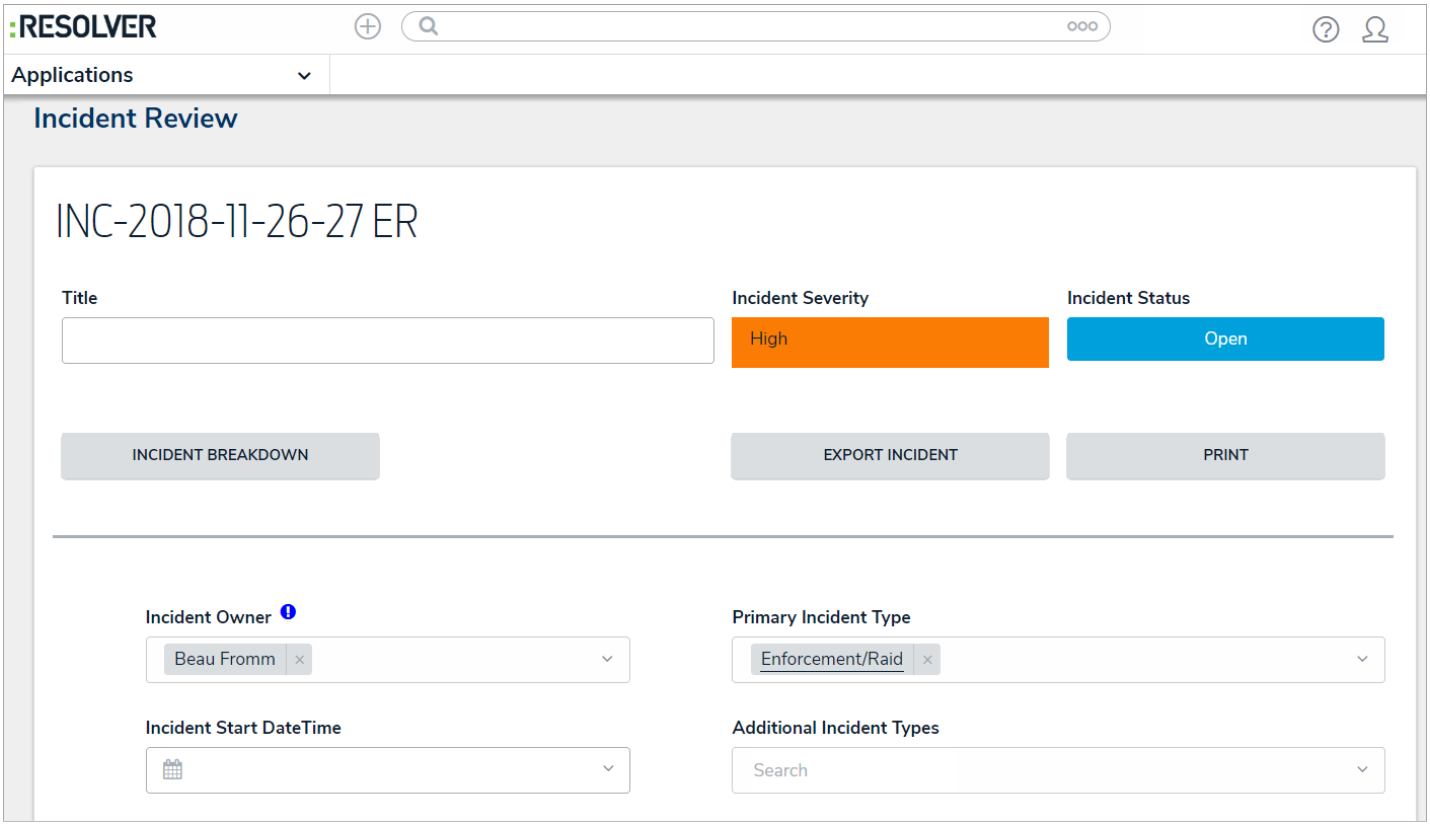
6. Click **Save As Triage** to create the new incident object and display the incident triage form .

> ⚠ Navigating away from the incident form before clicking **Save as Triage** will delete any change made to the form.

Incident Owner Overview

Once incidents are submitted through the portal, the Incident Screener assigns an incident owner. The Incident Owner reviews the record for accuracy and completion and can perform the following actions:

- Close the incident;
- Return the incident to the Triage for review;
- Create, edit, and complete incident tasks; and
- Assign an investigator and open an investigation.

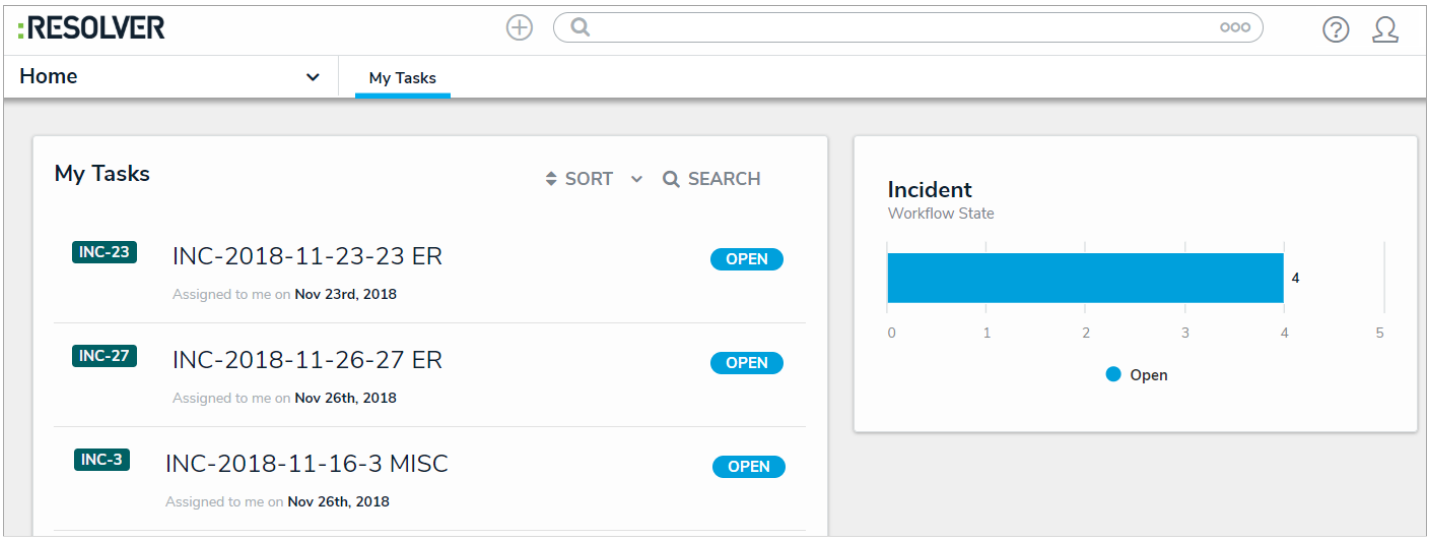


Reviewing an incident.

View & Edit Assigned Incidents

An incident owner is assigned to an incident by the Incident Screener and is responsible for assigning investigators and ensuring an incident is complete before it's closed. All incidents assigned to the Incident Owner appear on the My Tasks page.

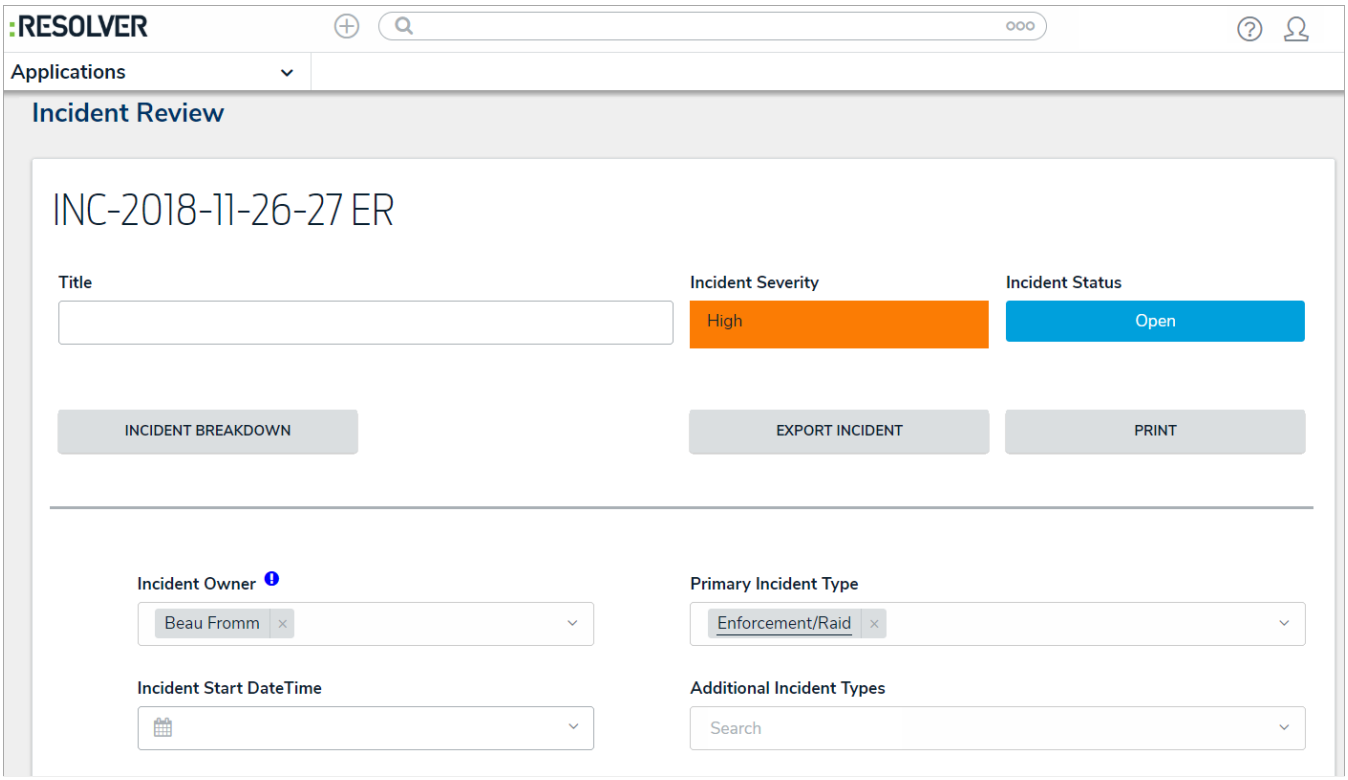
If an incident owner is named as an incident type owner on an incident type , they can create incidents of that incident type, and read all incidents of that incident type, without being directly assigned to the incident. Only an administrator can name an incident type owner.



Assigned incidents on the My Tasks page.

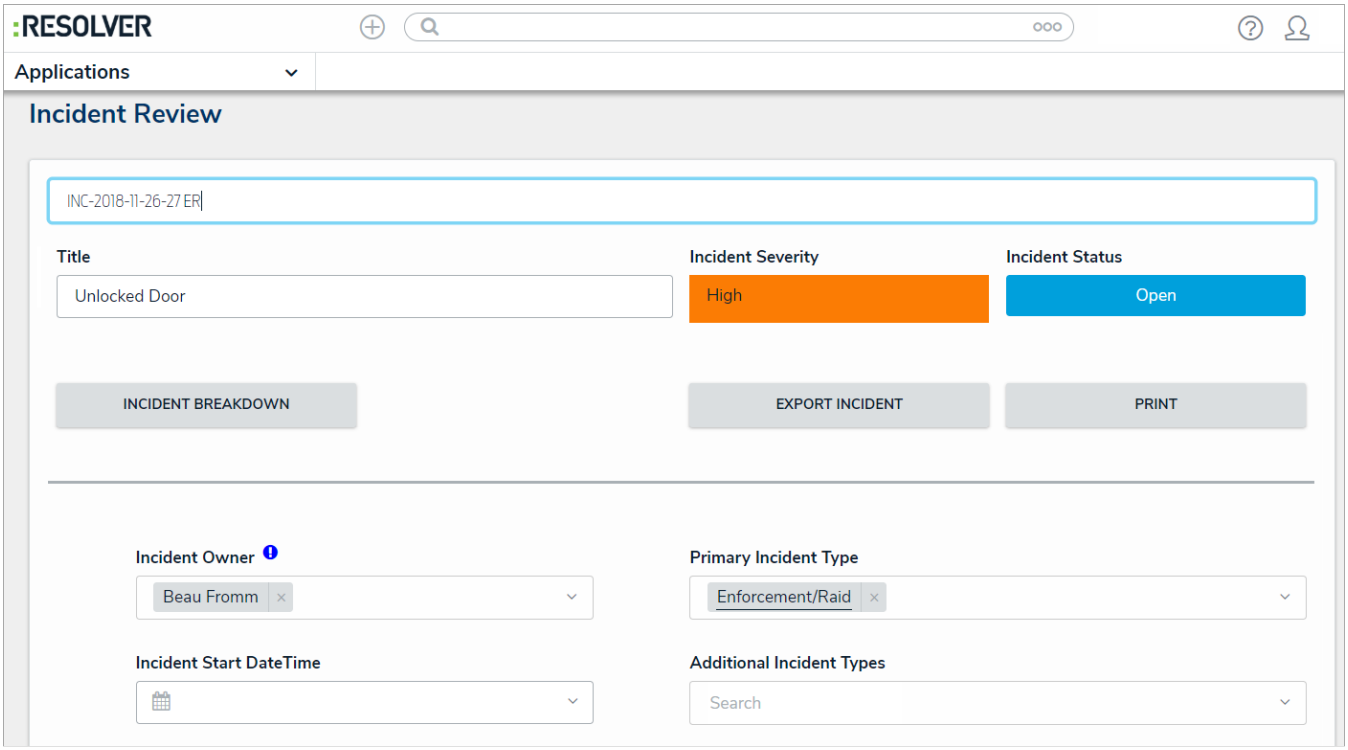
To view and edit assigned incidents:

1. Log into a user account that's been added to the **Incident Owner** user group to display the **My Tasks** page.
2. Click an incident to open the **Incident Review** form.



The Incident Review form.

3. **Optional:** Click the title of the incident (e.g. INC-2018-11-21 MISC) to make changes as needed, then click away from the title to save your changes. If your organization prefers to maintain the default title, you can also add a secondary title in the **Title** field.



Editing the default incident title in the Incident Review form.

4. Click the **Primary** and **Additional Incident Type**, and/or **Responding Person(s)** fields, begin typing keywords to display a list of available options, then click to select the appropriate option.

5. Add or change the **Severity**, **Incident Start** and **End Date/Time**, **Incident Flags**, **Reporting Source**, **Additional Responses**,

and/or **Fiscal Year** by selecting the appropriate option from the dropdown list.

6. Add a **Description** to provide additional information about the incident as needed.
7. Click the + icon below **Details**, **Loss & Recovery**, **Tasks & Action Plan**, **Record Security & Audit**, and **Linked Incidents** to open the creation palette, then complete the fields as required.
8. Add an **Investigator**.
9. Enter comments, tagging other users if needed, in the **Comments** text box (at the bottom of the page). See the Incident Form Comments article for more information on using this feature.
10. Clicking one of the following buttons will perform the following actions:
    - **Incident Breakdown**: Displays related incident details in a collapsible tree format.
    - **Export Incident**: Export incident details into Excel format for use with third-party analytics tools.
    - **Print**: View a printable incident form.
    - **Legal Hold**: Move the incident workflow stage to **Legal Hold**.
11. Click one of the following buttons to save the incident:
    - **Open Investigation:** Sends the incident to the Incident Investigator for review.
    - **Return to Triage:** Sends the incident to the Incident Screener for further action or review.
    - **Close Incident:** Closes the incident because no further action is required.

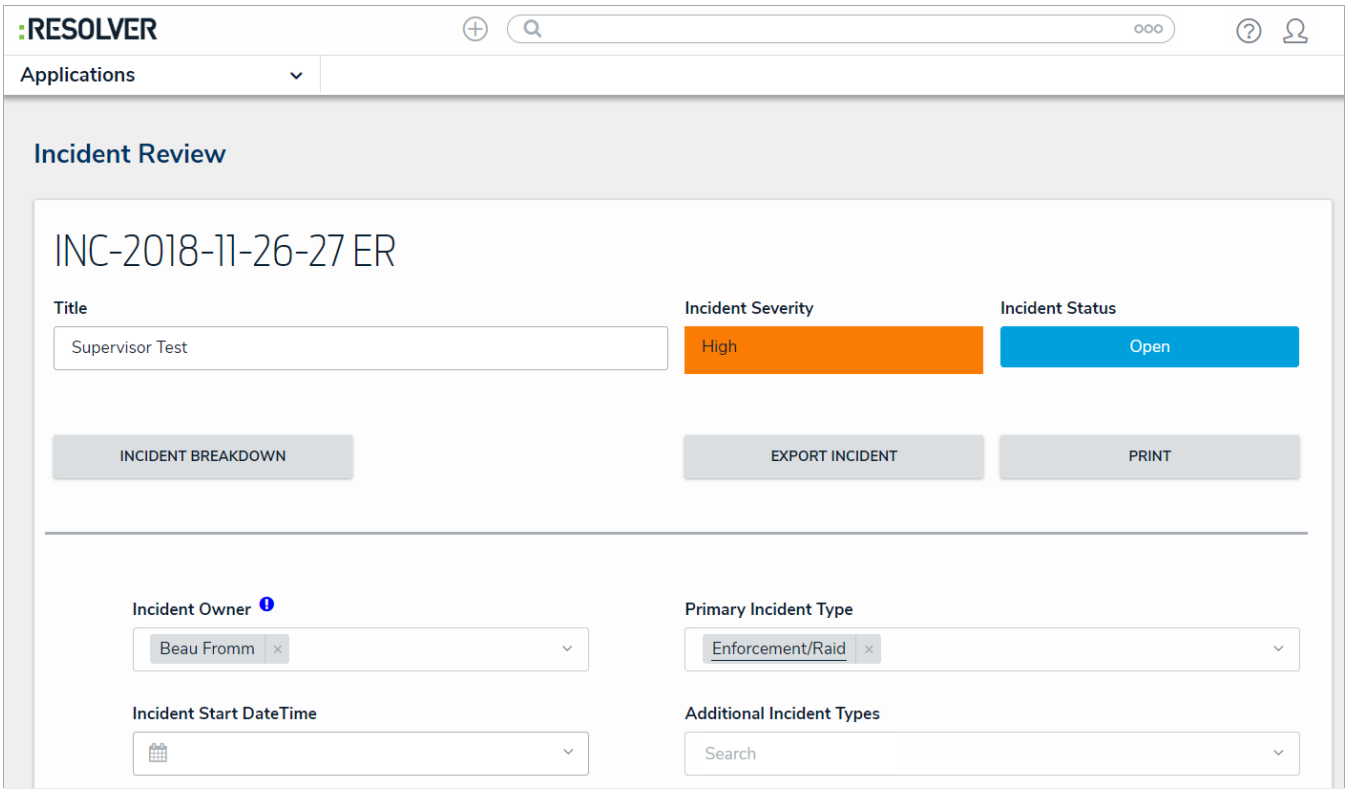
Open an Investigation

The Incident Owner can open an investigation and assign an investigator to explore an incident further and examine the outcome and root cause.

> Investigations are only available for certain incident types. If the **Open Investigation** button is not visible on the **Incident Review** form, this incident type cannot be investigated.

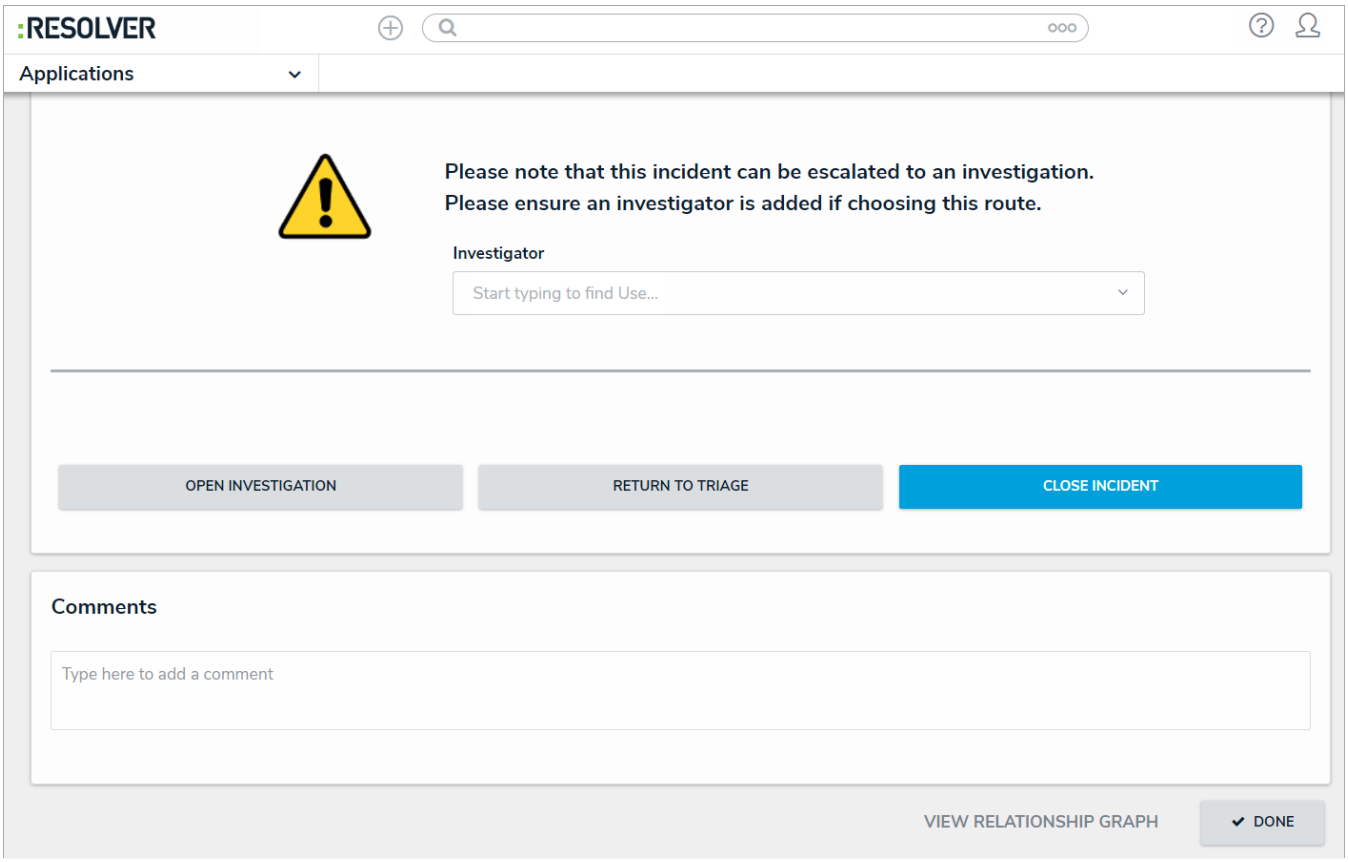
To open an investigation:

1. Log into a user account that's been added to the **Incident Owner** user group to display the My Tasks page.
2. Click an incident to open.
3. Click the **Primary Incident Type** field, begin typing keywords to display a list of available options, then click to select the appropriate option.



The Primary Incident Type on an Incident Review form.

4. Enter additional details of the incident, as required. For more information on editing an incident, see View and Edit Assigned Incidents .
5. Click the **Investigator** field, begin typing investigator usernames to display a list of available options, then click to select the appropriate person.



Selecting an investigator.

6. Click **Open Investigation**.

Once an investigation is opened, the Incident Owner will be able to view, but not edit, the incident. The incident will move to the **Under Investigation** state and an email will be sent to the assigned investigator with a link to the incident.

Reopen a Closed Incident

Incident owners and incident investigators can close incidents. Once an incident is closed:

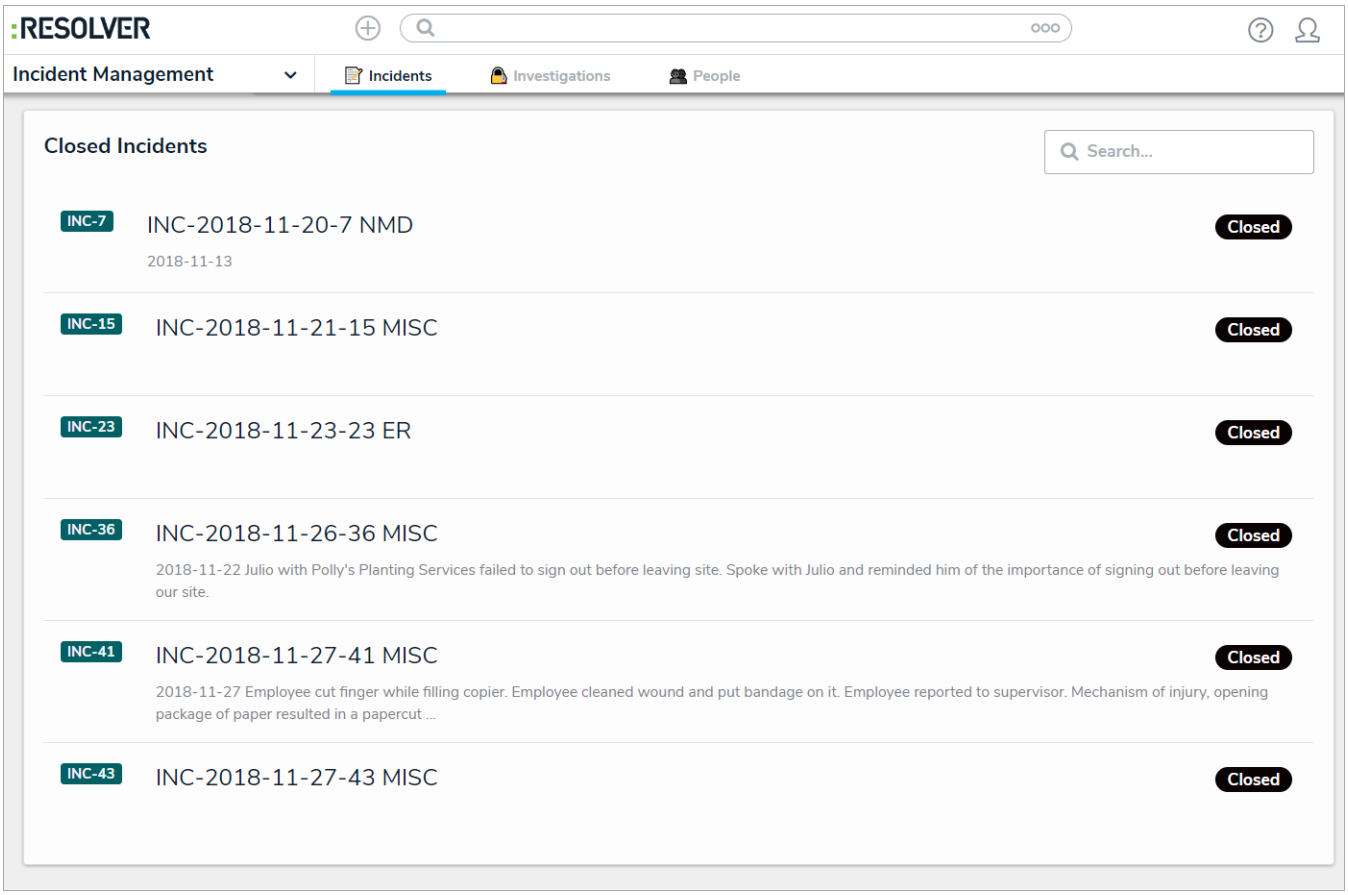
- The Incident Owner can view and reopen any incidents they own. To edit, the Incident Owner must first reopen the incident.
- The Incident Supervisor can view and reopen closed incidents if they are named as the Incident Supervisor on the incident.
- The Incident Investigator can view and reopen any incidents they have been added to.

To reopen a closed incident:

1. Log into a user account that's been added to the **Incident Owner** or **Incident Supervisor** user group.
2. Click the dropdown in the nav bar **> Incident Management** to display the **Incidents** activity.

The Incident Management application in the nav bar.

3. Click an incident in the **Closed Incidents** section to view the **Incident Review** form.



The Closed Incidents section of the Incidents application.

4. Click **Reopen** to move the incident to the **Open** state. The app will navigate to the **Incidents** activity, with the reopened incident in the **Active Incidents** section. If you are an **incident owner** or **incident investigator**, you must reopen the incident before editing. **Incident supervisors** cannot edit open incidents.
5. Click the incident in the **Active Incidents** section to display the **Incident Review** form.
6. If you are logged into a user account that's been added to the **Incident Owner** user group, you can edit the incident as needed. See View and Edit Assigned Incidents for more information about editing fields.
7. Click one of following buttons:
    - **Open Investigation:** Sends the incident to the Investigator for review.
    - **Return to Triage:** Sends the incident to the Incident Screener for further action or review.
    - **Close Incident:** Closes the incident because no further action is required.

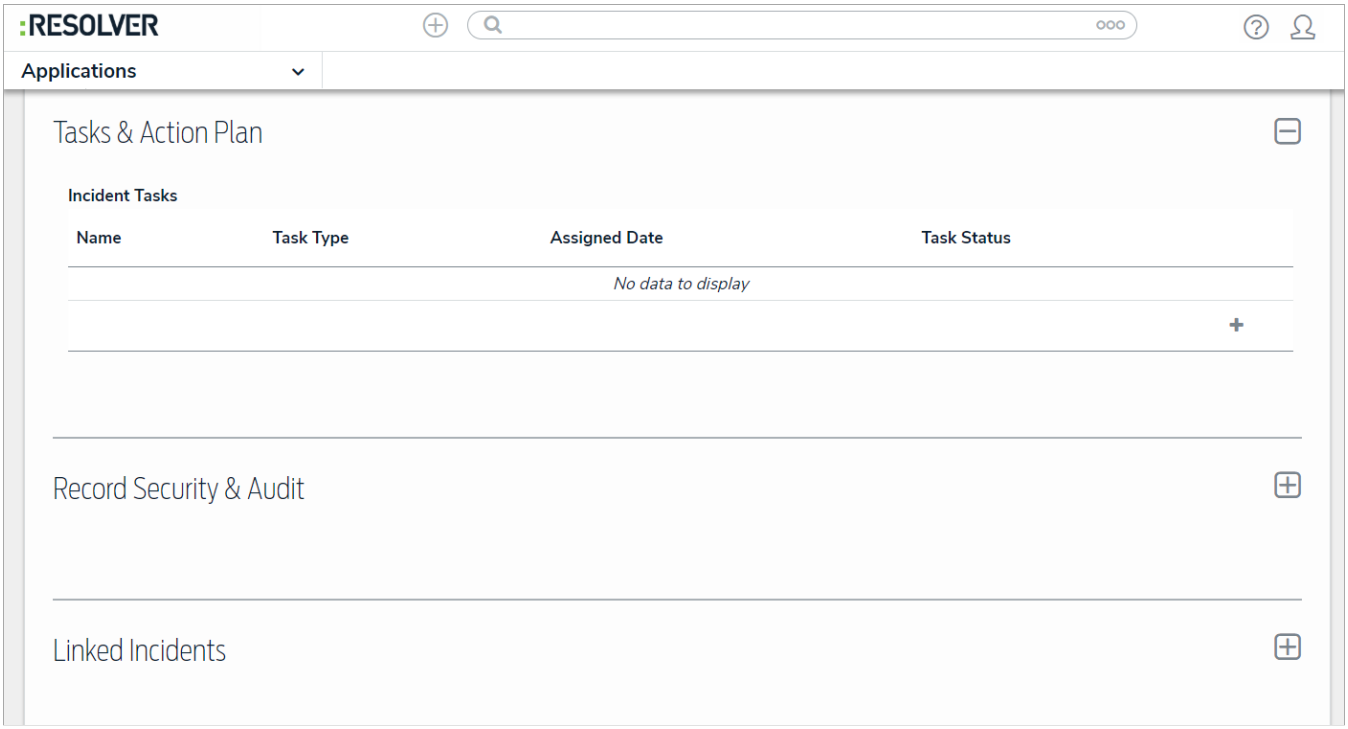
Create an Incident Task

Incident tasks are actions attached to an incident that must be completed before the incident can be closed. Incident tasks will send an email notification to the incident owner when:

- The task is created; and
- When the task is not completed by the due date. This notification will be sent the day after the due date, and will continue to send daily until the task is completed.

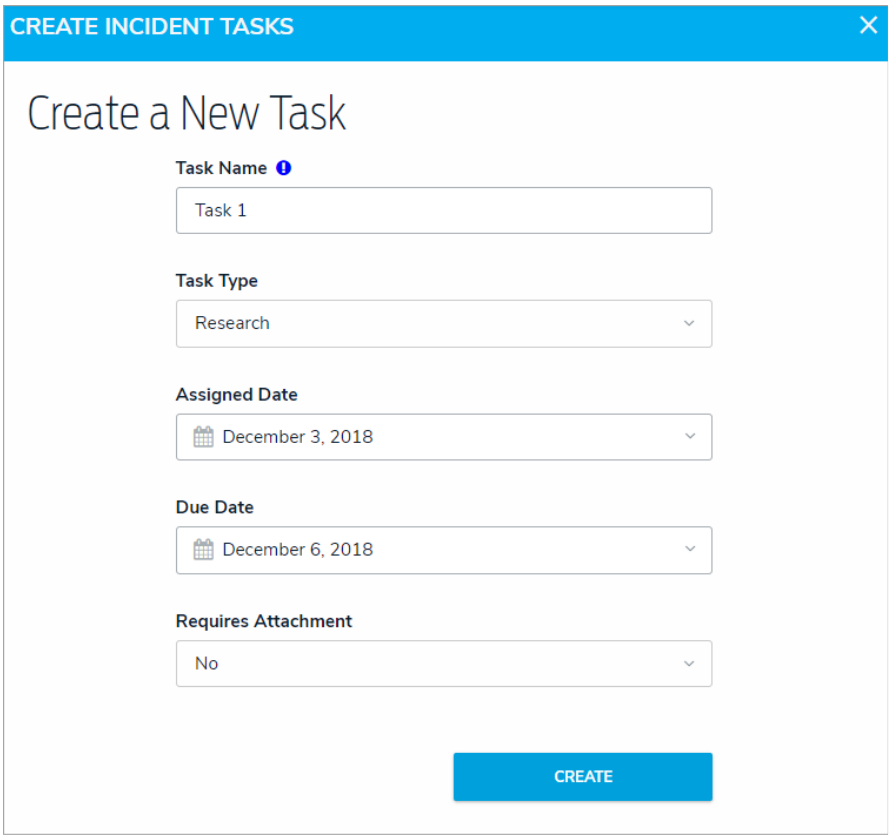
To create a task on an incident:

1. Log into a user account that's been added to the Incident Owner or Incident Investigator user group.
2. Open an incident from the My Tasks page or the **Incident Management** app.
3. Click the  icon below **Tasks & Action Plan** to display the **Incident Tasks** section.
4. Click the + icon at the bottom-right of the section to open the **Create a New Task** palette.



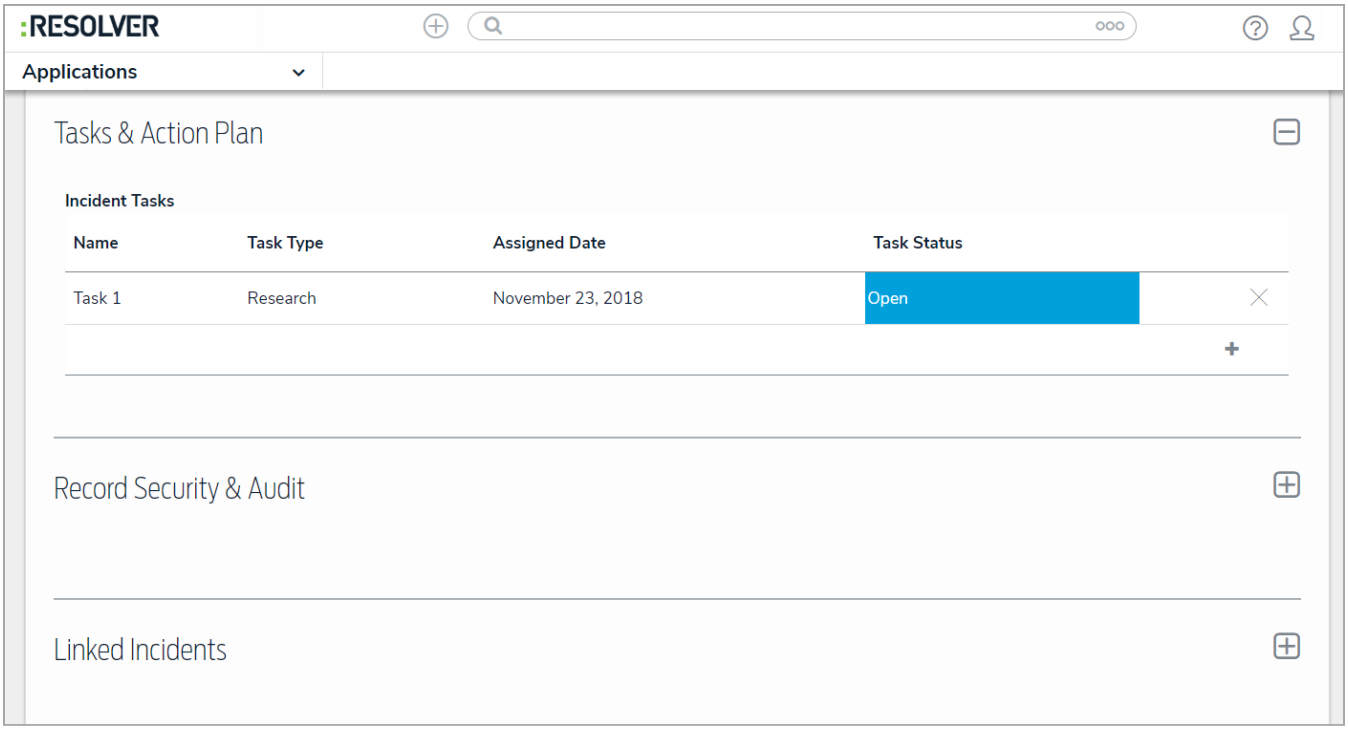
The Task & Action Plan section.

5. Add a **Task Name** and fill out the remaining fields,as needed.



Creating a task.

6. Click **Create**. The incident owner will receive an email notification for this task. If the task is for someone other than the Incident Owner, it can be assigned after it's created.



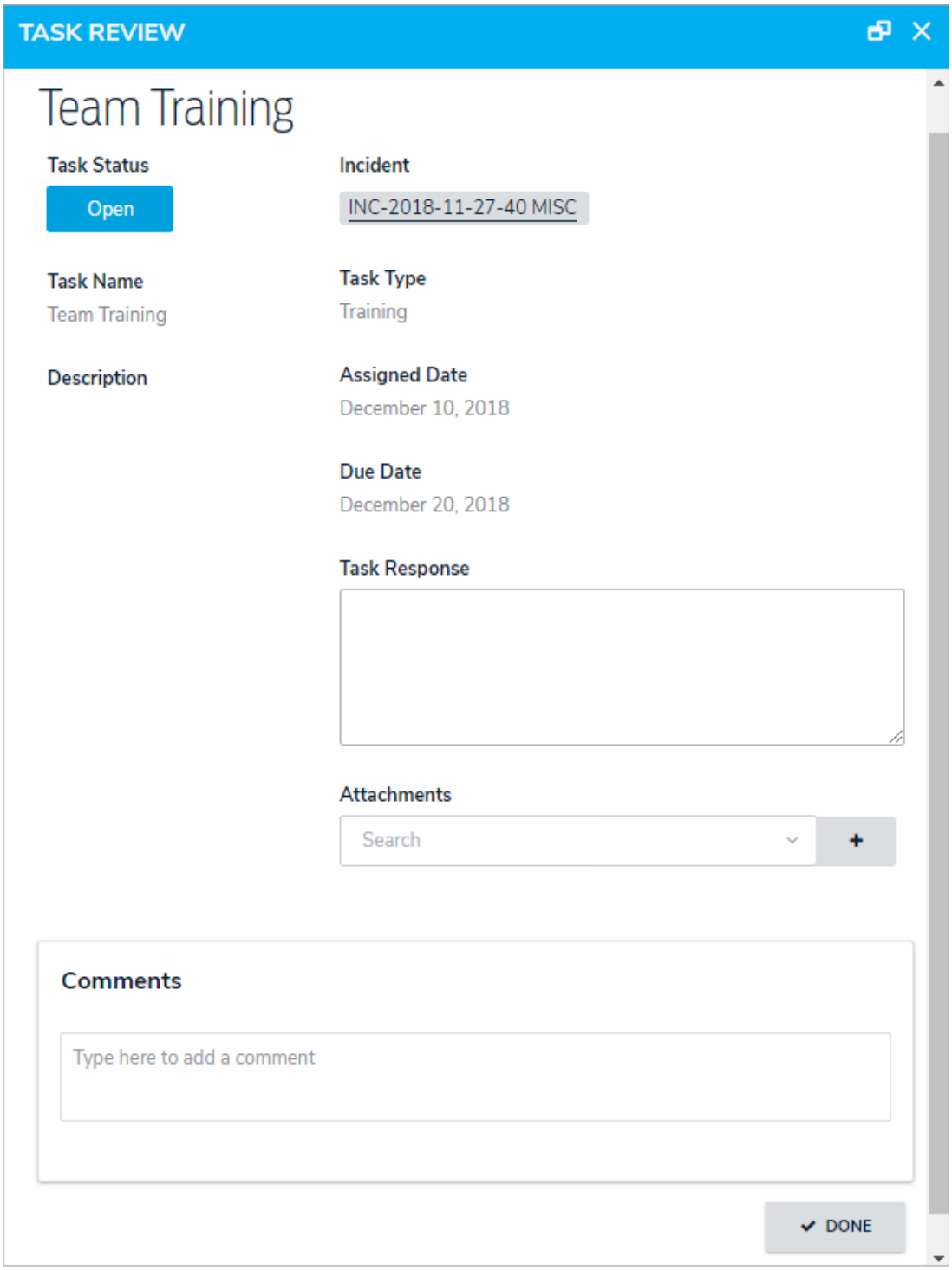
A task in the Task & Action Plan section.

7. Click the task in the **Tasks & Action Plan** section of the **Incident Review** form to open the **Task Review** palette where you can add a task response, assign a new task owner, include attachments, mark the task as complete, or add comments , if needed. See View & Manage Incident Tasks for more information.

View & Manage Incident Tasks

To view and manage your tasks:

1. Log into a user account that's been added to the **Incident Owner** user group and has been assigned a task.
2. View an assigned task via the **Task Review** form using one of the following methods:
    - Click the task on the My Tasks list;
    - Click the dropdown in the nav bar **> Incident Management** to display the **Incidents** activity. Click an incident to open the **Incident Review** form. Expand the **Tasks & Action Plan** section on the **Incident Review** form, then click the task; or
    - Click the **Tasks** activity in the **Portal.** This menu only appears if you've been assigned at least one task.
3. Add a task response, include attachments, or add comments if needed.



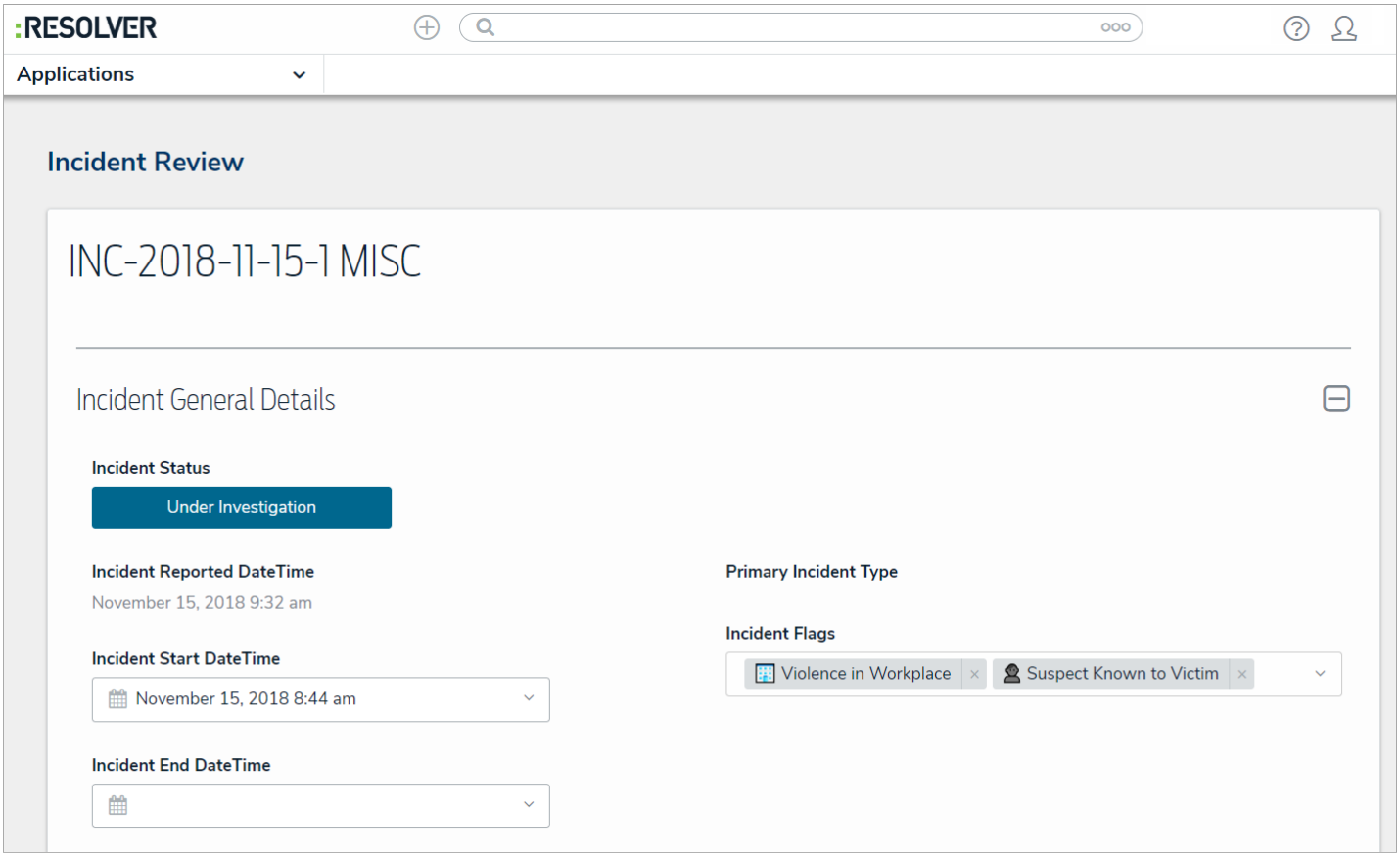
Completing a task.

4. Click **Complete** to move the task to the **Completed** state.

Incident Investigator Overview

Investigations are opened by the Incident Owner and are assigned to the Incident Investigator. Incident investigators can:

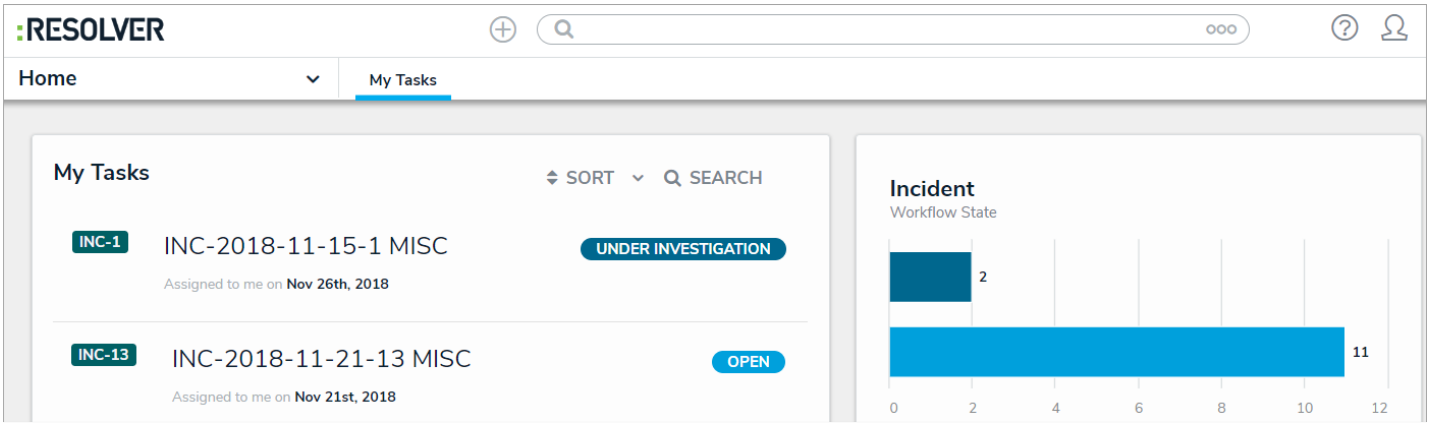
- Add interviews and evidence;
- Link incidents to related incidents and persons; and
- Determine the incident outcome and root cause.



An incident under investigation.

Investigate an Incident

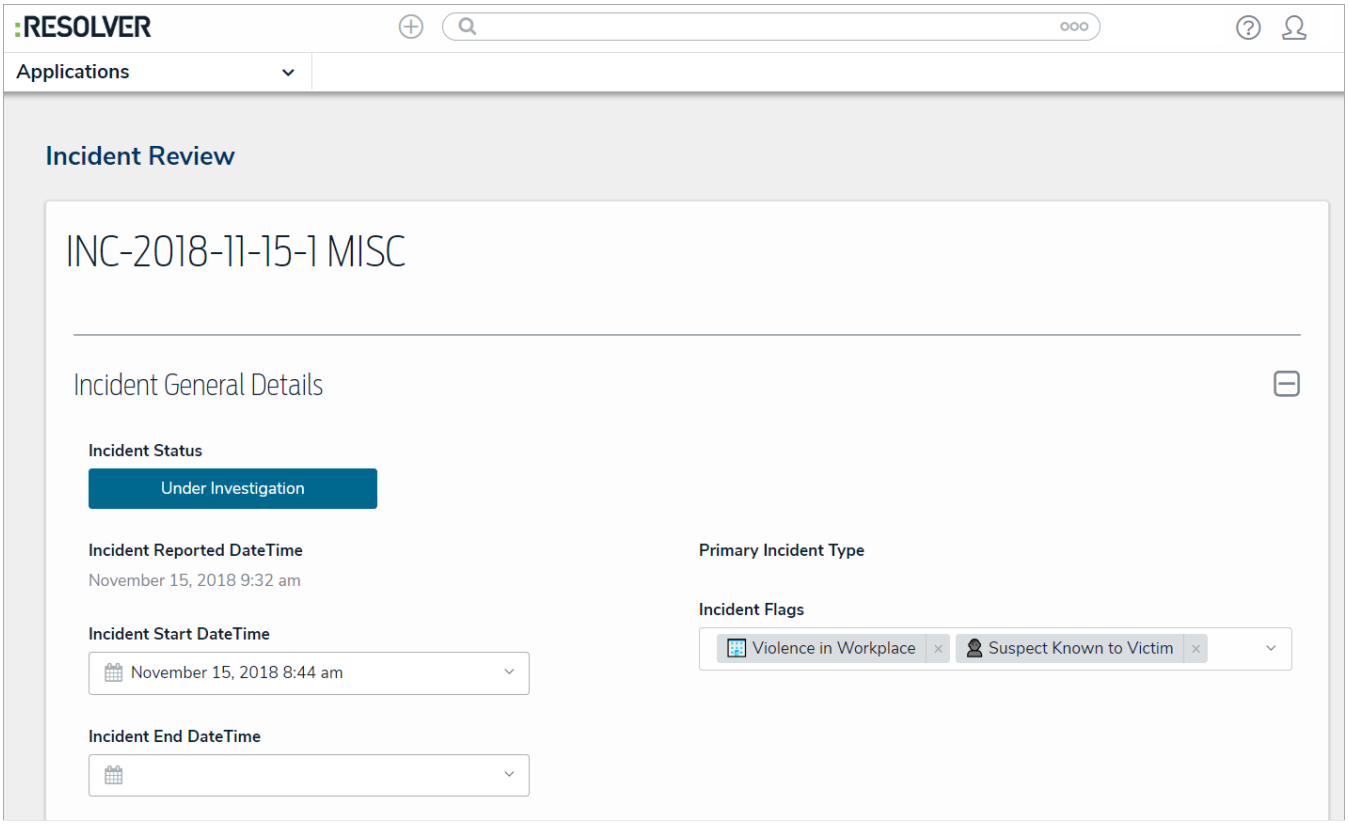
The Incident Owner is responsible for opening investigations and assigning investigators.



An incident under investigation in the My Tasks page.

To document an investigation on an incident:

1. Go to the **My Tasks** page.
2. Click an incident in the **Under Investigation** state to open the **Incident Review** form.



Viewing an incident under investigation.

3. Complete the following fields in the **Incident General Details** section as needed:
    - **Incident Start DateTime** and **Incident End DateTime**: When the incident began and when it ended.
    - **Incident Flags**: High-risk and important incident details, with a related symbol for easy reference.

- **Description**: Details of the investigation or incident.

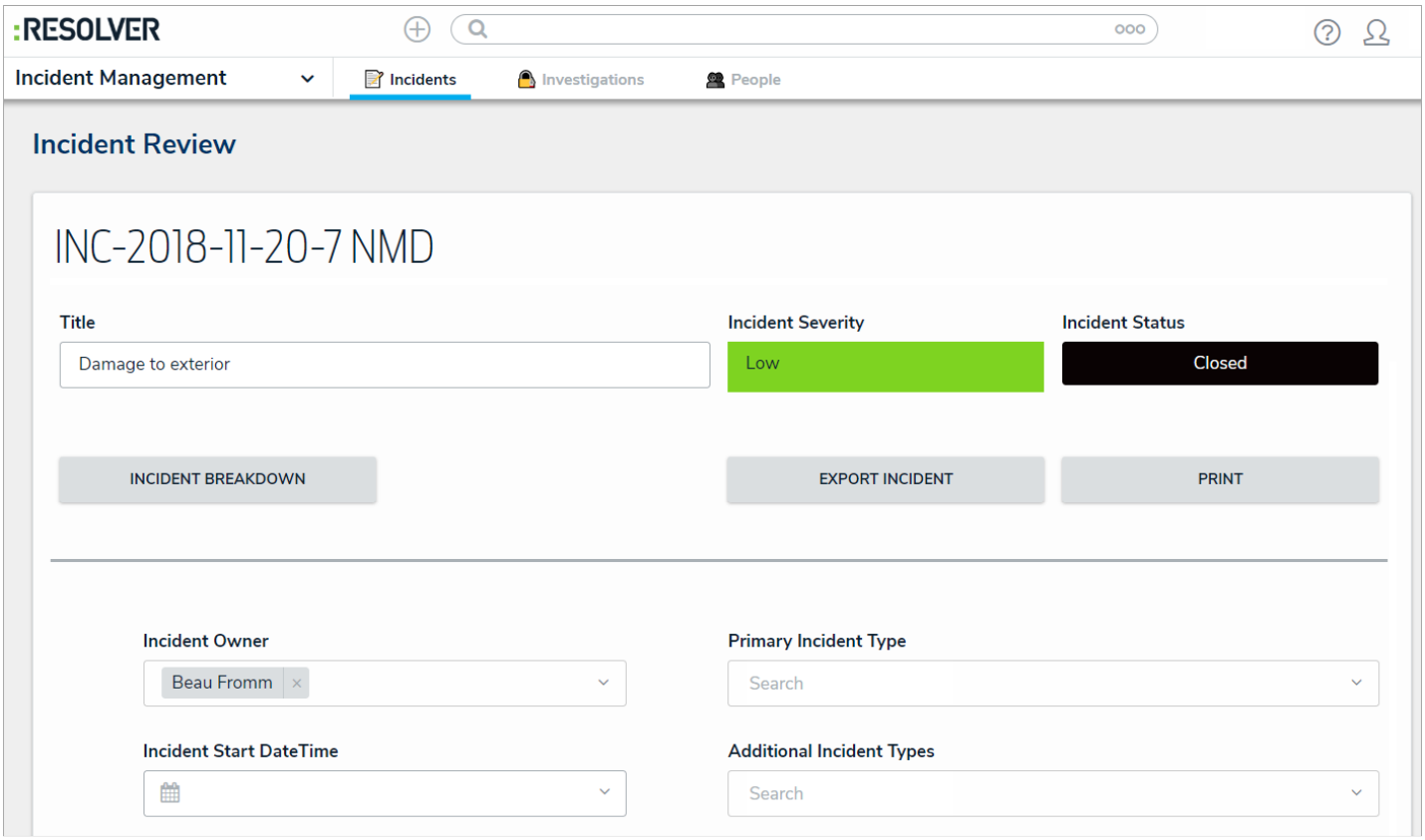
4. Complete the **Investigation Start Date** and **Investigation Close Date**, as needed.
5. Complete the fields in the remaining **Logs**, **Interviews**, **Evidence**, **Links**, **Outcomes & Root Cause**, **Attachments**, and **Incident Properties** tabs. Note that your user group may not be permitted to complete all fields.
6. Click one of following buttons:

    - **Return:** Returns the incident back to the incident owner in the **Open** state.
    - **Complete Investigation:** Closes the incident because no further action is required. The incident can be viewed and reopened by the Incident Owner and the Incident Supervisor. See View and Reopen a Closed Incident for more information.

Incident Supervisor Overview

The Incident Supervisor manages incidents in a **Closed** or **Review** state. This allows incident supervisors to monitor and resolve issues with closed incidents in their Business Unit, without the help of the Incident Management Administrator . Users in this group can:

- View investigations and reports; and
- View closed incidents.



A closed incident object as it's displayed to a user in the Incident Supervisor user group.

Assign an Incident Supervisor

Incident Supervisors can only view incidents that they open or that are assigned to them by the Incident Screener or Incident Owner .

To assign an incident supervisor to an individual incident:

1. Log into a user account that's been added to the **Incident Screener** or **Incident Owner** user group.
2. Go to the My Tasks page and click an incident to open it.
3. Click the **+** icon below **Record Security & Audit** to open the palette.
4. Click the **Incident Supervisor** field. Begin typing an incident supervisor's name to display a list of available options, then click to select the appropriate person.

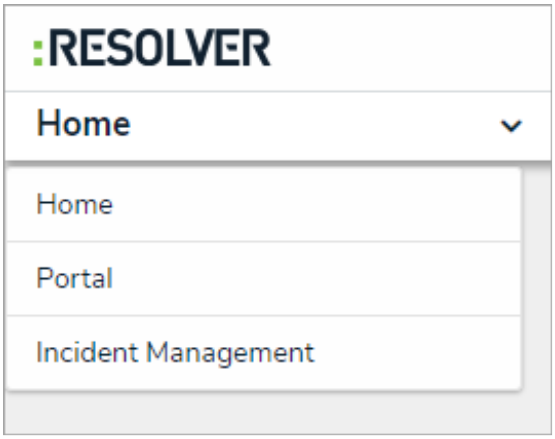
> The Incident Supervisor field may appear in different parts of the **Incident Review Form**, depending on what application you use to open the incident and your account permissions. In the **Triage** application, it will be in the **Access** section of the form. When opened from the **Incidents** application, it will be under **Record Security & Audit.**

Review an Incident

The following provides instructions for accessing incidents in the **Review** state from the **Incident Management** application, however, these incidents will also appear on the homepage (My Tasks).

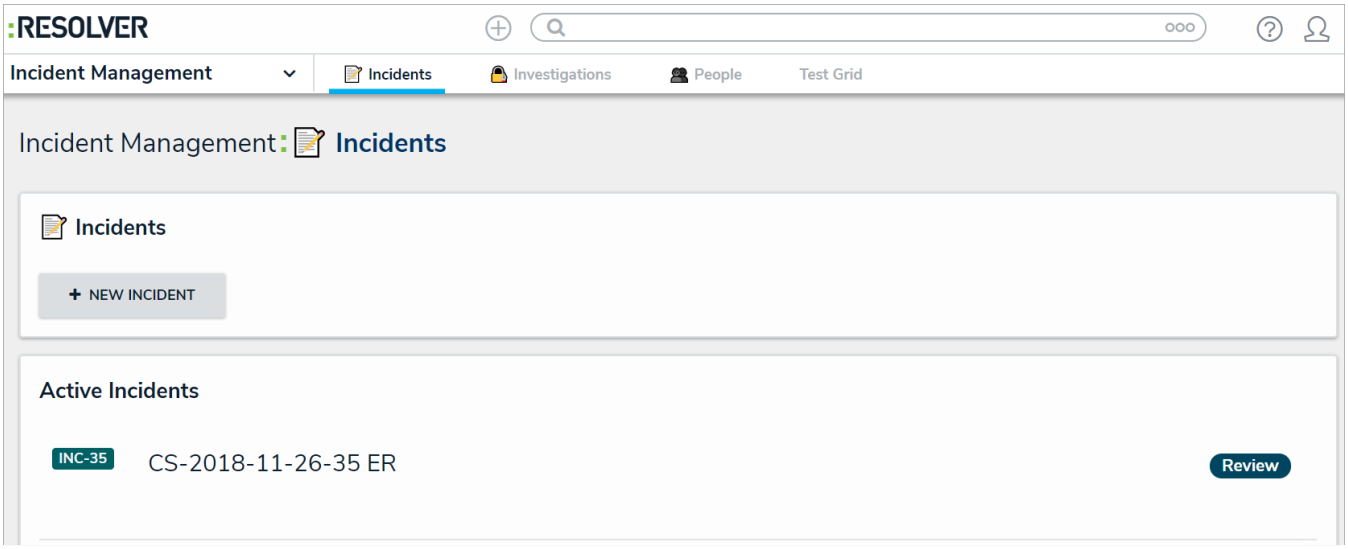
To view an incident in the Review state:

1. Log into a user account that's been added to the **Incident Supervisor** user group.
2. Click the dropdown in the nav bar **> Incident Management** to display the **Incidents** activity.



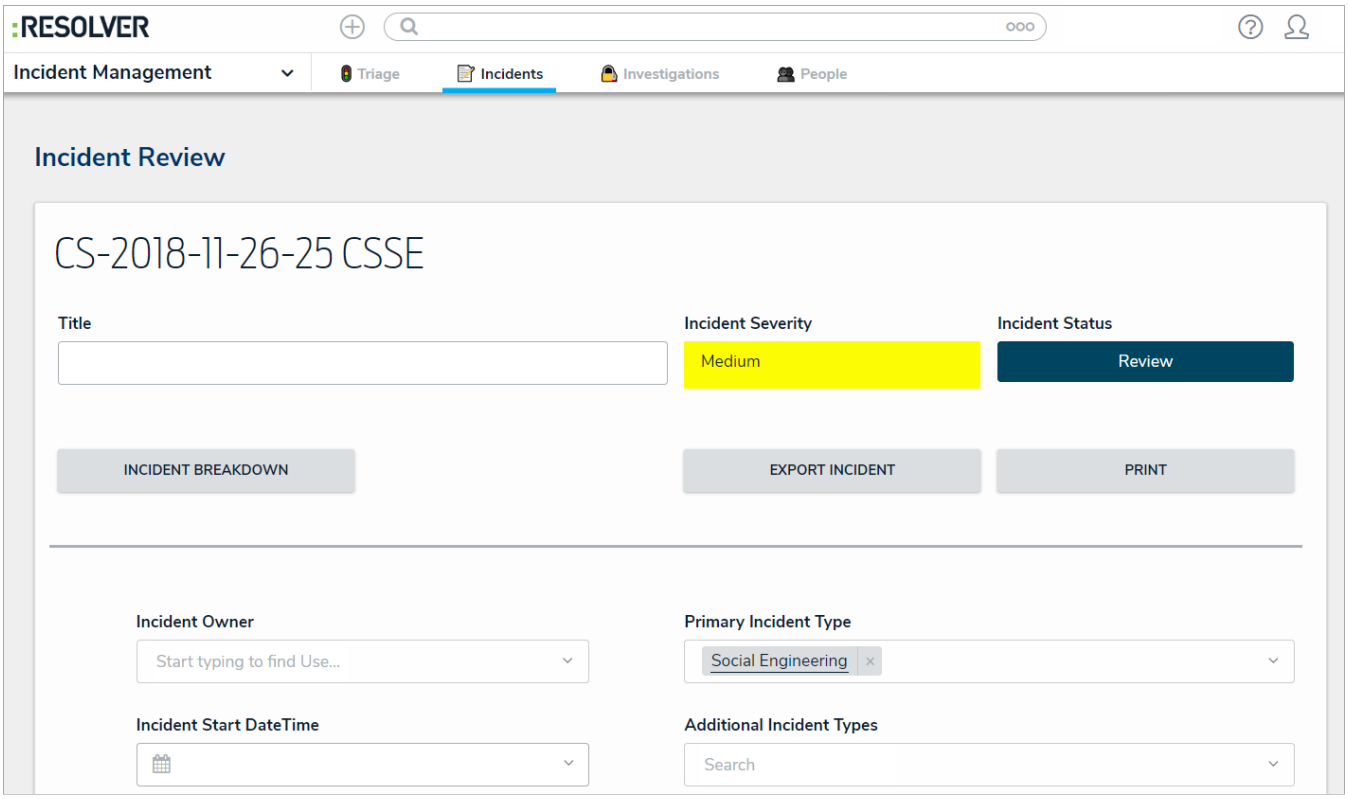
The nav bar.

3. Click an incident in the **Active Incidents** section to display it. Incidents ready for review will be in the **Review** state.



An incident in the Review state.

4. Review and edit the incident as needed. Enter comments, tagging other users if needed, in the Comments text box (at the bottom of the page).



Viewing an incident in the Review state when logged in as an Incident Supervisor.

5. Click one of the following buttons:
    - **Return:** Returns the incident back to the **Open** or **Under Investigation** state.
    - **Complete Review:** Closes the incident because no further action is required.

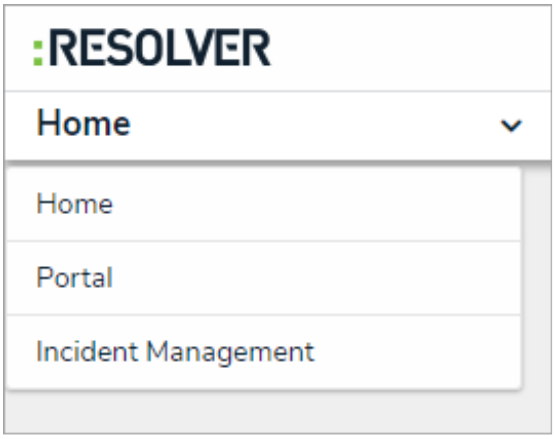
> Incidents can be moved into the **Review** state only if the objects selected in the **Business Unit** or **Incident Type** fields have the **Supervisor Review** option selected.

Reopen a Closed Incident

Incident supervisors can reopen closed incidents to edit or delete them.

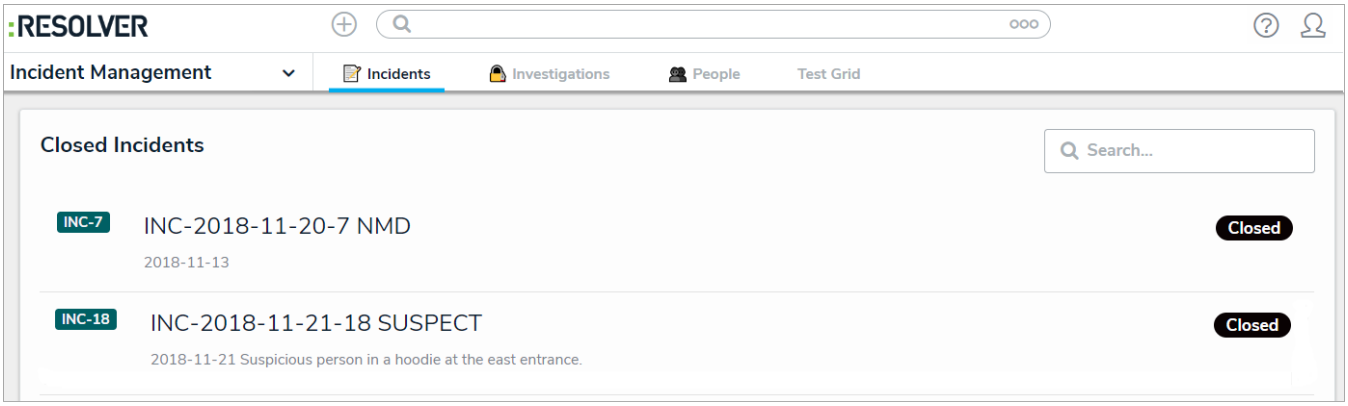
To reopen a closed incident:

1. Log into a user account that's been added to the **Incident Supervisor** user group.
2. Click the dropdown in the nav bar **> Incident Management** to display the **Incidents** activity.



The nav bar.

3. Click an incident in the **Closed Incidents** section to display it.



The Closed Incidents section.

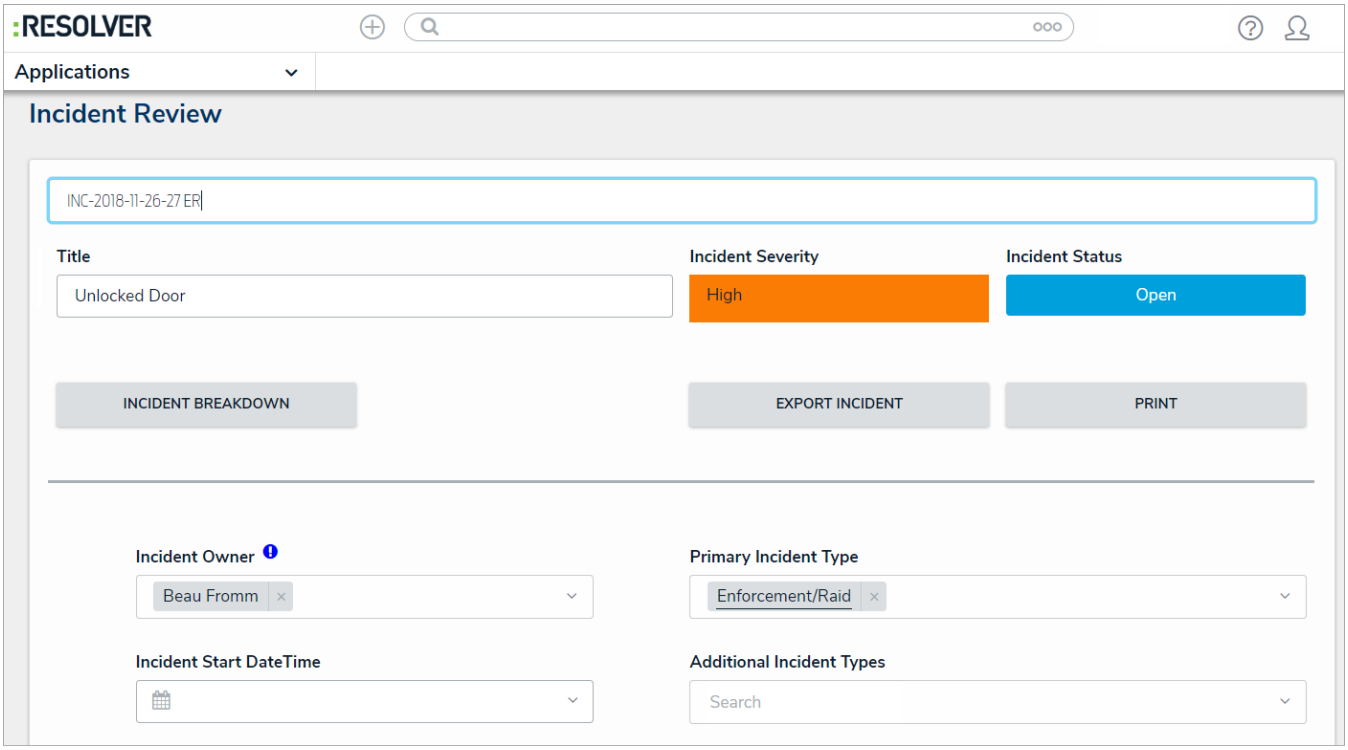
4. Review and edit the incident as required. Enter comments, tagging other users if needed, in the Comments text box (at the bottom of the page).
5. Click one of the following buttons:
    - **Done:** Saves your work and keeps the incident in the **Closed** state.
    - **Reopen:** Moves the incident to the **Open** state.

Incident Management Administrator Overview

The Incident Management Administrator oversees all incident data. This allows users in this user group to monitor the application, including viewing all accepted incidents. Users in this group have the following role permissions:

- Access to all incident and intake records and their involvements; and
- Read-only access to the Library .

> The Incident Management Administrator can view incident objects. It is not to be confused with the Administrator user group, who can add Library objects, or the Core Administrator, who can add users.



Reviewing an incident as the Incident Management Administrator.

Review Incidents

Incident Management Administrators have access to view all incidents and intake records and their involvements. These users can review individual incidents or view incident reports.

> The Incident Management Administrator can view incident objects. It is not to be confused with the Administrator user group, who can add Library objects, or the Core Administrator, who can add users.

To view individual incidents:

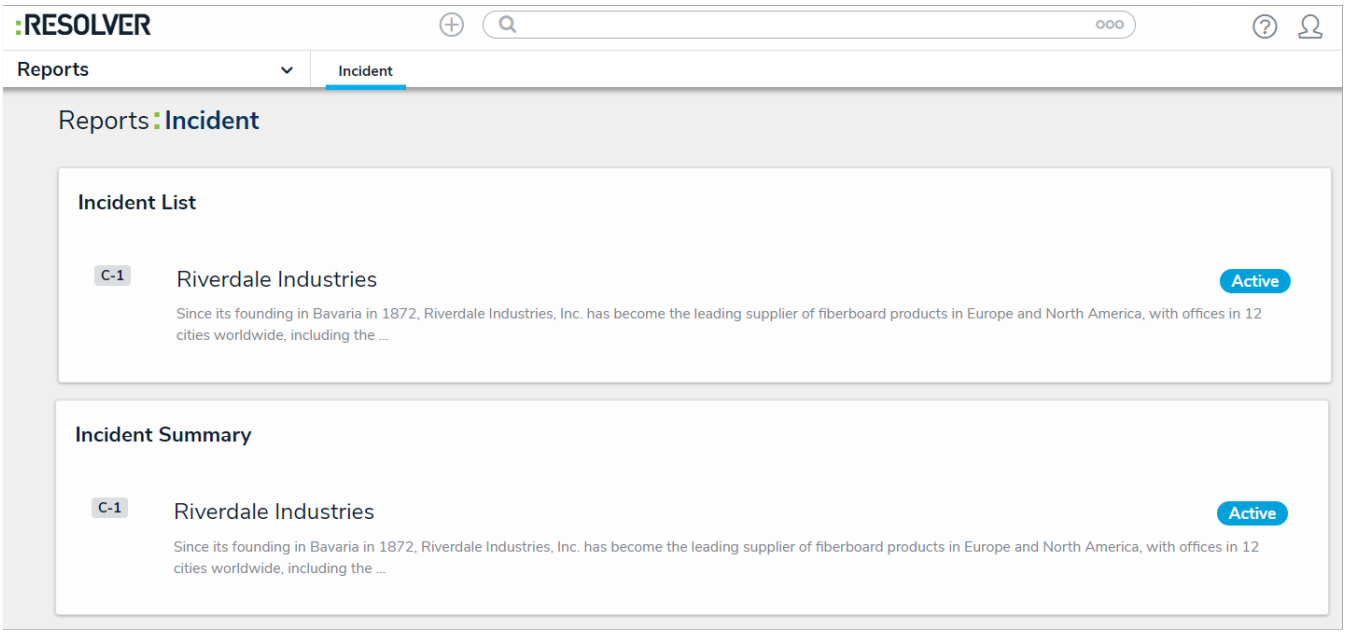
1. Log into a user account that's been added to the **Incident Management Administrator** user group.
2. Use the search function to search by incident name or by object type .

To view a report:

1. Log into a user account that's been added to the **Incident Management Administrator** user group.
2. Click the dropdown in the nav bar **> Reports** to display the **Incident** activity.

The Reports application in the nav bar.

3. Click a report to open.



Clicking on an anchor object to open a report.

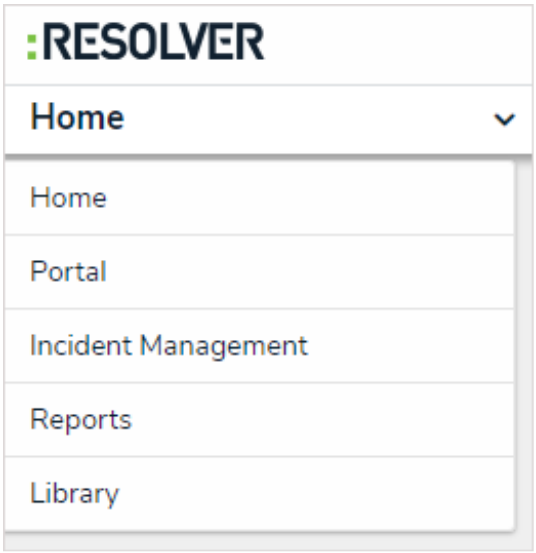
View Library Objects

Incident management administrators have read-only access to the Library application. Library objects are categories available to add to incidents, such as business units, persons, and locations. Only users in the Administrator user group can add library objects.

> The Incident Management Administrator can view incident objects. It is not to be confused with the Administrator user group, who can add Library objects, or the Core Administrator, who can add users.

To view library objects:

1. Log into a user account that's been added to the **Incident Management Administrator** user group.
2. Click the dropdown in the nav bar > **Library.**



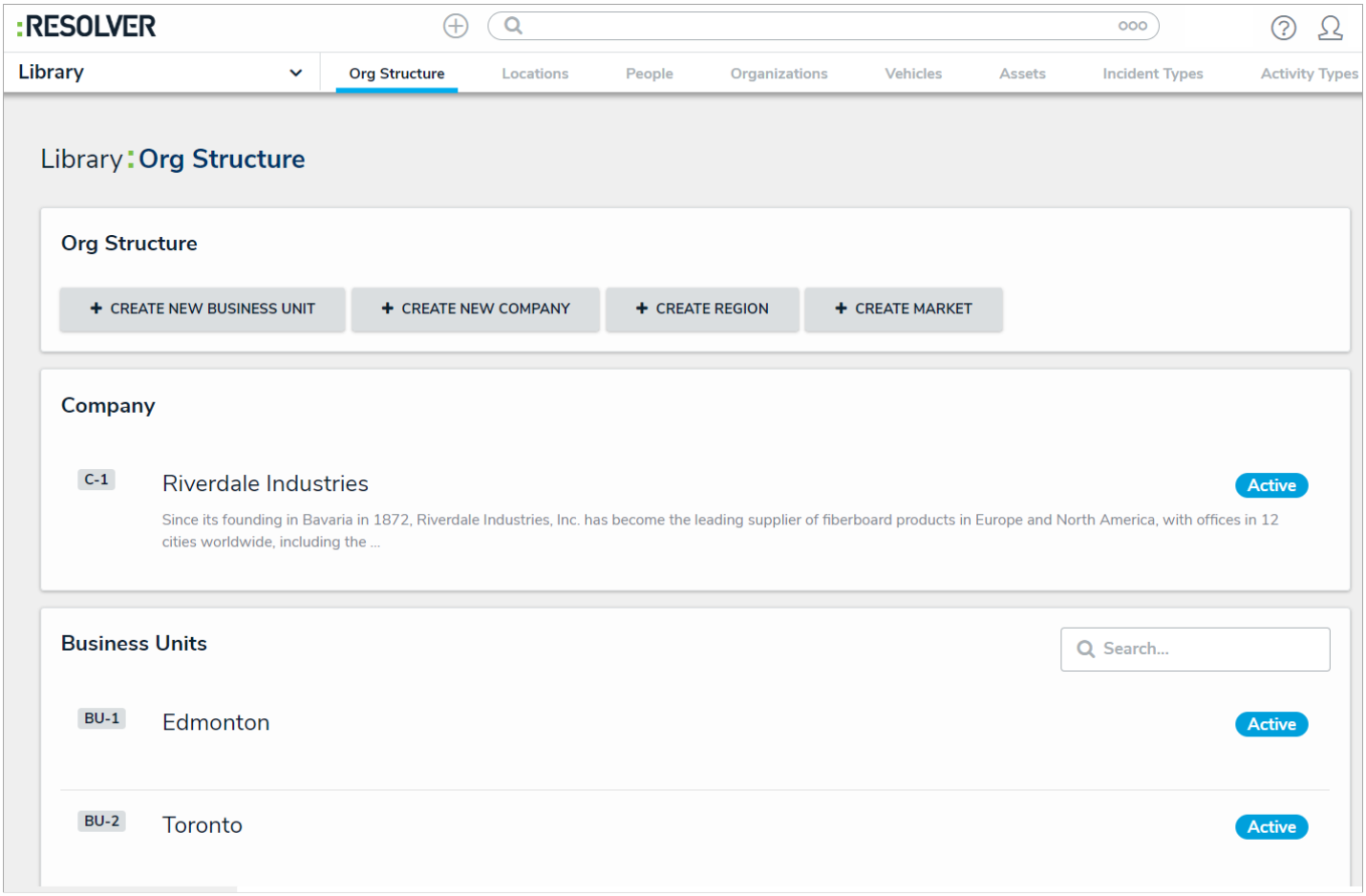
Accessing the Library application from the nav bar.

3. Click the tab that corresponds to the type of object you want to view, such as **Locations**, **Vehicles**, or **Assets**.
4. Click an object to view the object record.

Administrator Overview

Administrators are responsible for adding Library objects to Incident Management. Users in this group oversee the Library application to manage the reference data available to users, including locations, persons, and incident types.

> The Administrator user group can create library objects only. It is not to be confused with the Incident Management Administrator, who can view incident objects, or the Core Administrator, who can add users.



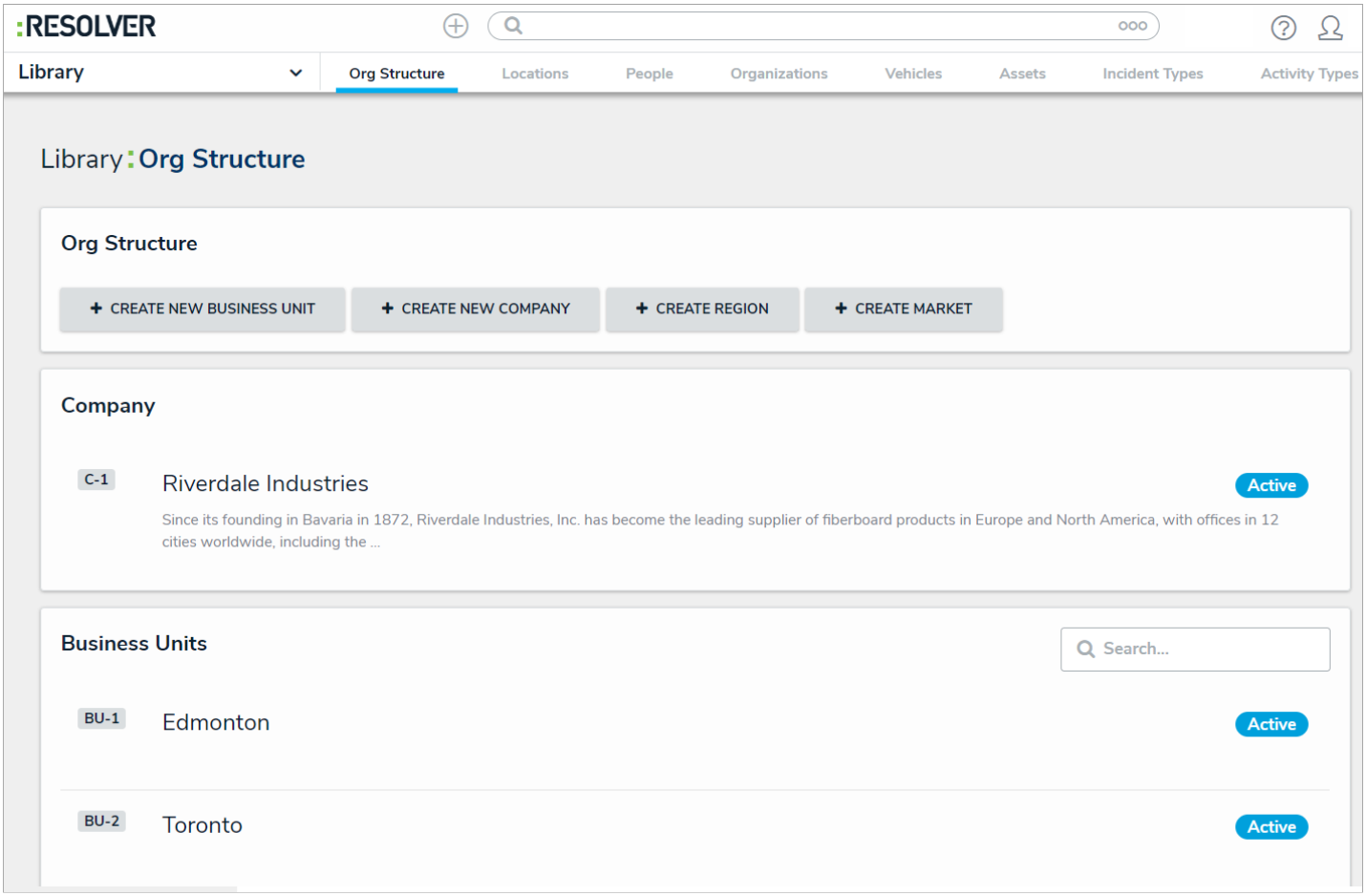
The Library application.

Library Application

If you're a member of the Administrator user group, you will see the **Library** application in your nav bar. Through this application, admins can view and create new objects, including business units, locations, people, organizations, and incident types. These objects are then available to be added to incidents, depending on the user's permissions.

> The Administrator user group can create library objects only. It is not to be confused with the Incident Management Administrator, who can view incident objects, or the Core Administrator, who can add users.

> Library items are often updated via spreadsheet import. If you edit a library item, it may revert back if another user is maintaining the item via spreadsheet import. To mass-upload objects by spreadsheet, contact Resolver Support.



The Incident Management Library application.

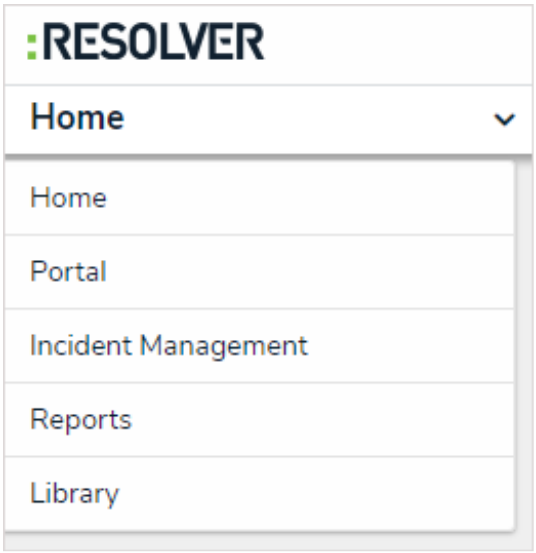
Create New Library Objects

Administrators can use the **Library** application to create new objects, including locations, people, business units, and more. These objects are then available to be added to new incidents.

> The Administrator user group can create library objects only. It is not to be confused with the Incident Management Administrator, who can view incident objects, or the Core Administrator, who can add users.

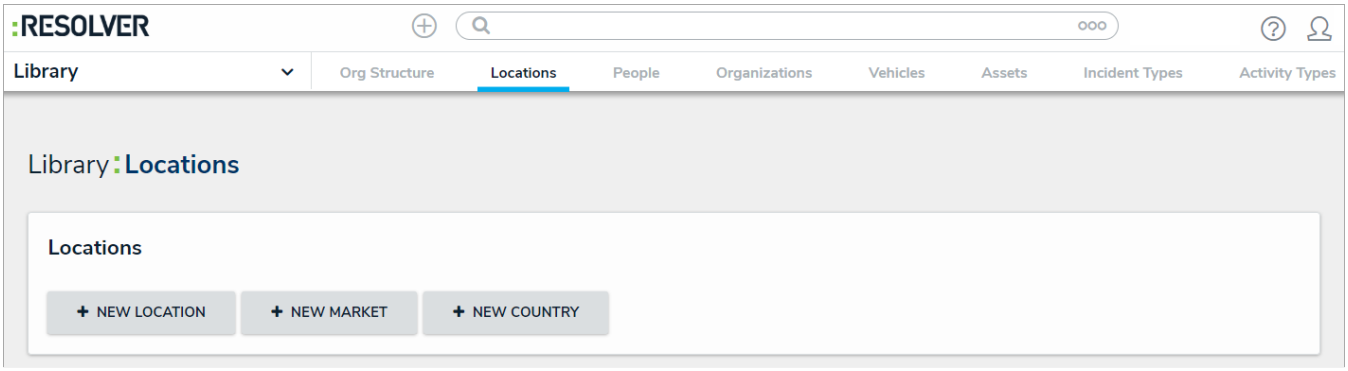
To create new Library objects:

1. Log into a user account that's been added to the **Administrator** user group.
2. Click the dropdown in the nav bar > **Library.**



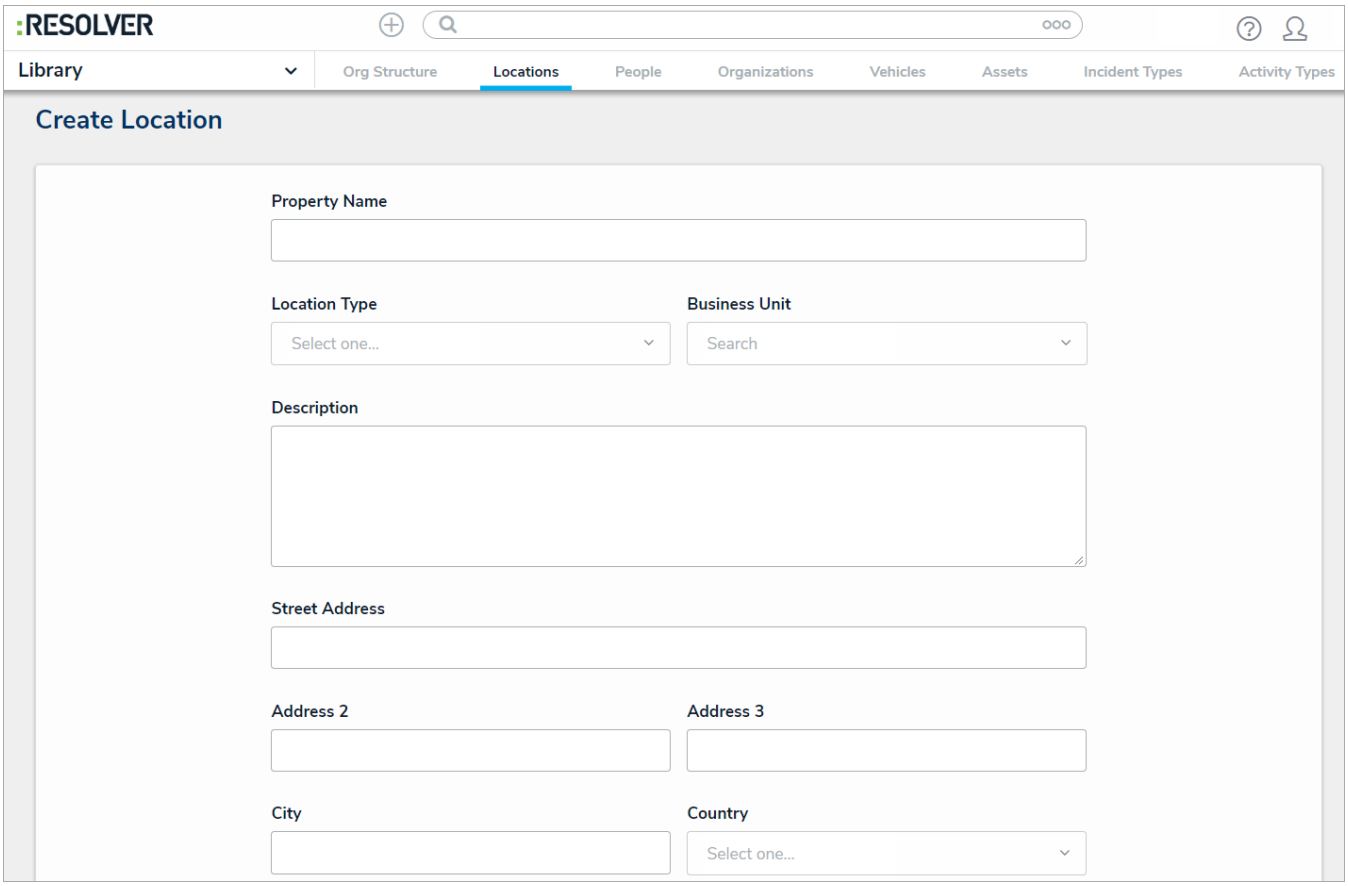
Accessing the Library application from the nav bar.

3. Click the tab that corresponds to the type of object you want to create, such as **Locations**, **Vehicles**, or **Assets**.
4. Click the applicable button at the top of the page to add an object.



Buttons for adding new Incident Management objects.

5. Complete the fields, including the object name, description, or any other fields as required. The available fields will vary depending on the object type being created.



Creating a new Incident Management object.

6. Click **Create**.

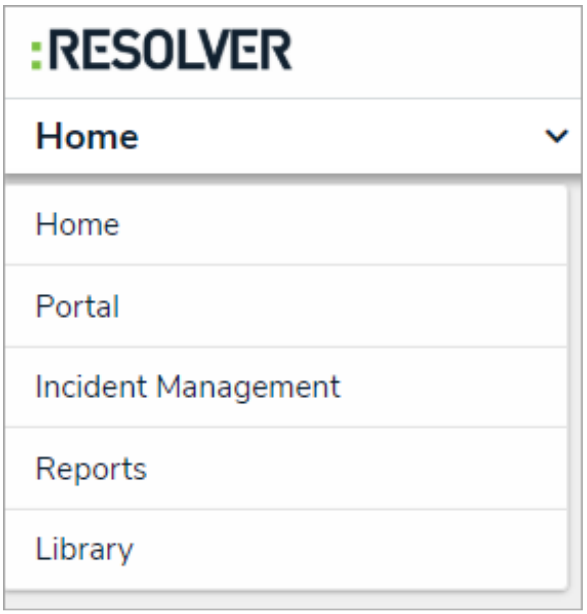
Create an Incident Type

Incident types provide further context for an incident, including severity and security restrictions, and associate it with similar incidents. The incident types available when creating an incident depend on user permissions. Only users in the **Administrator** user group can add and edit incident types.

> The Administrator user group can create library objects only. It is not to be confused with the Incident Management Administrator, who can view incident objects, or the Core Administrator, who can add users.

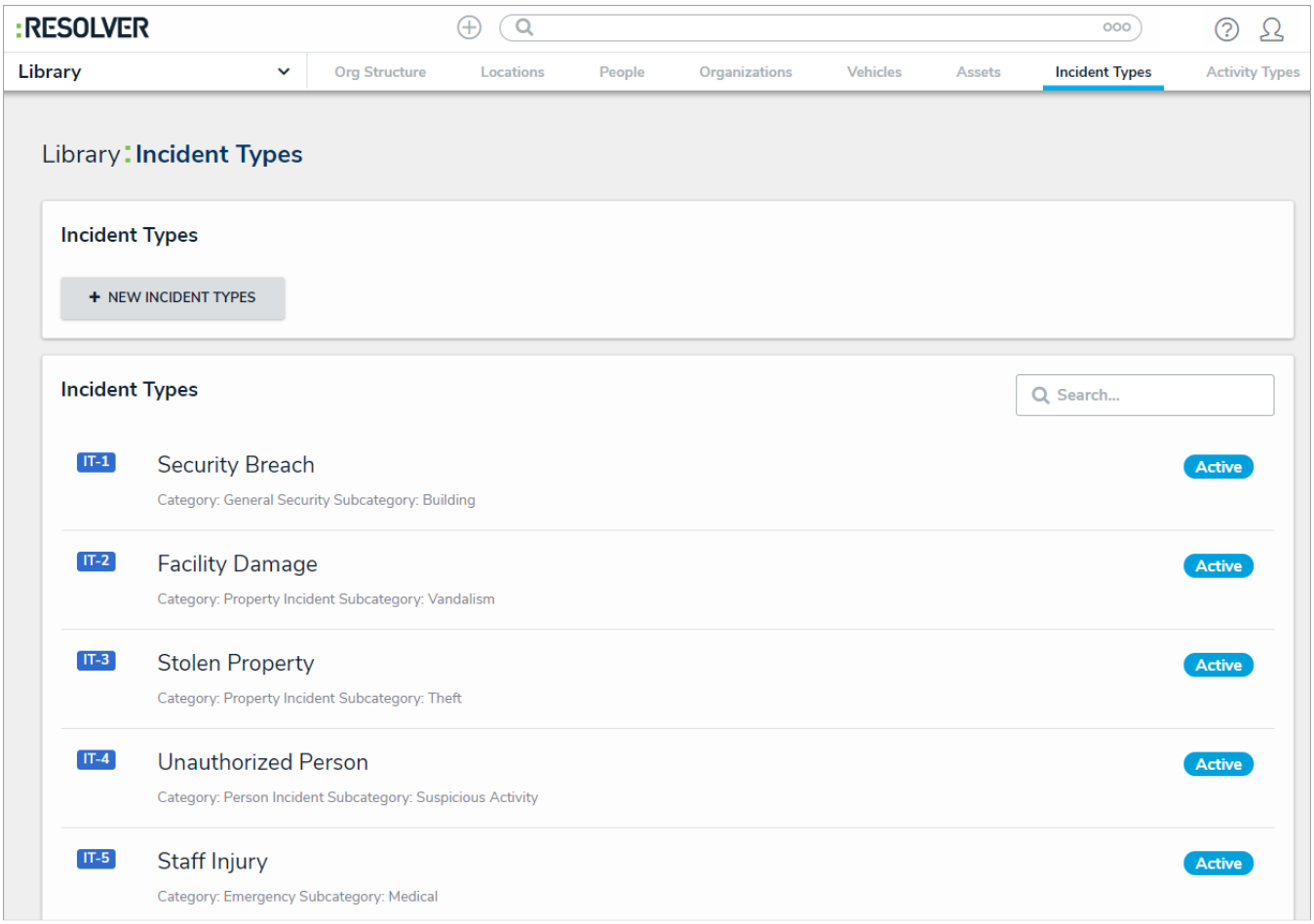
To create an incident type:

1. Log into a user account that's been added to the **Administrator** user group.
2. Click the dropdown in the nav bar > **Library.**



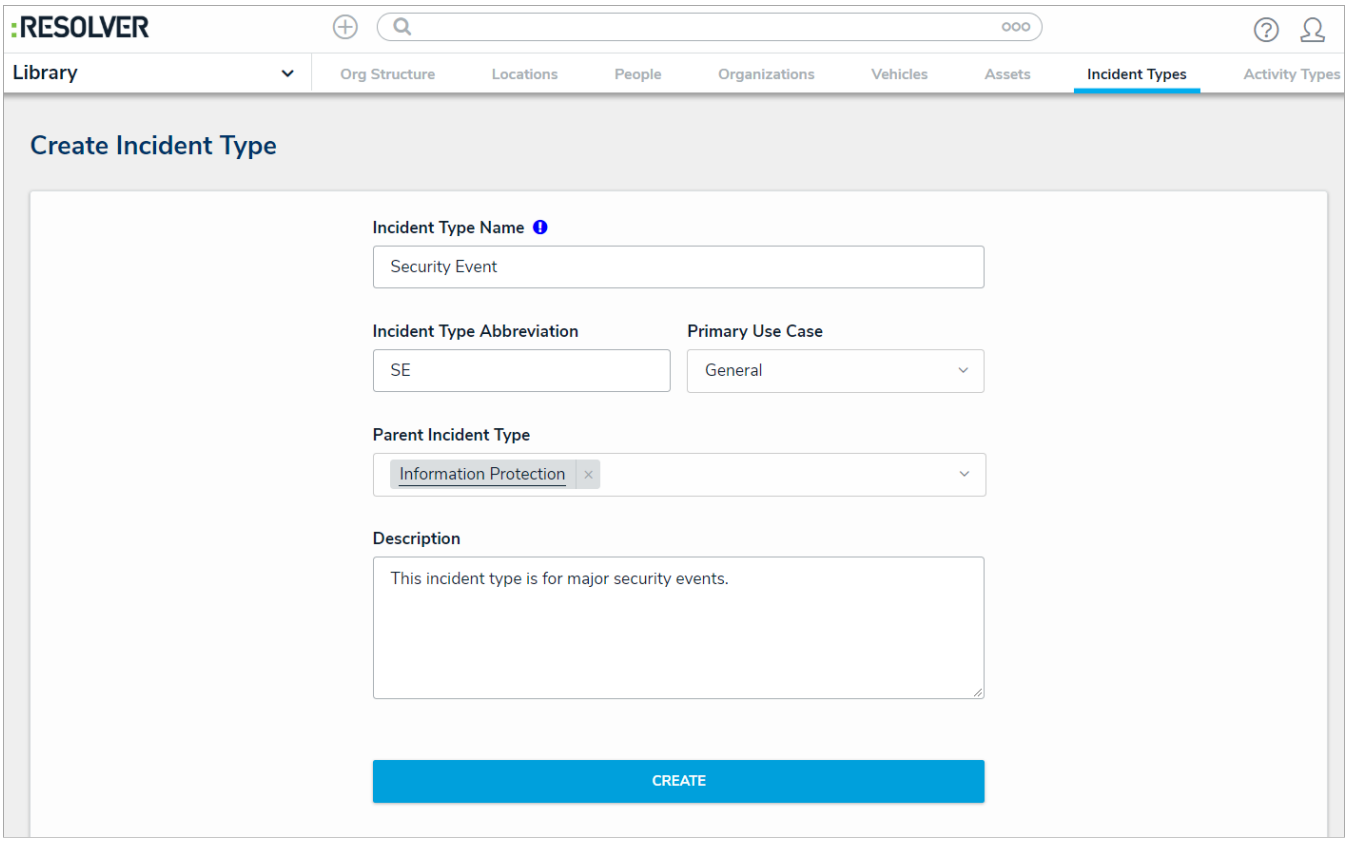
The Library application in the nav bar.

3. Click the **Incident Types** activity.



The Incident Types activity in the Library application.

4. Click **New Incident Types**.
5. Complete the **Incident Type Name**, **Incident Type Abbreviation**, and **Description** fields as required.
6. Select a **Primary Use Case** from the dropdown list, if different from the default.
7. **Optional**: Click the **Parent Incident Type** field, then begin typing keywords to display a list of available options.



A completed Create Incident Type form.

8. Click **Create**.

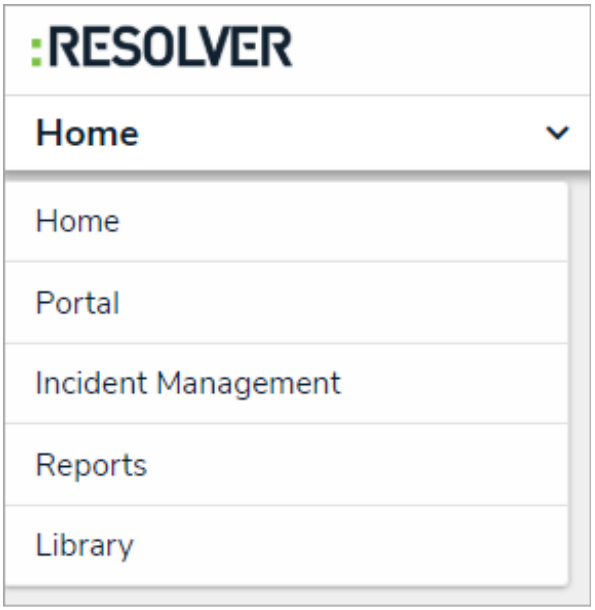
Edit an Incident Type

Clicking the incident type name on an **Incident Review** form will open the **Incident Type Review** form. Use this form to view which incidents have this object as their primary or secondary incident type, whether investigations are applicable to this incident type, and the security settings.

> The Administrator user group can create library objects only. It is not to be confused with the Incident Management Administrator, who can view incident objects, or the Core Administrator, who can add users.

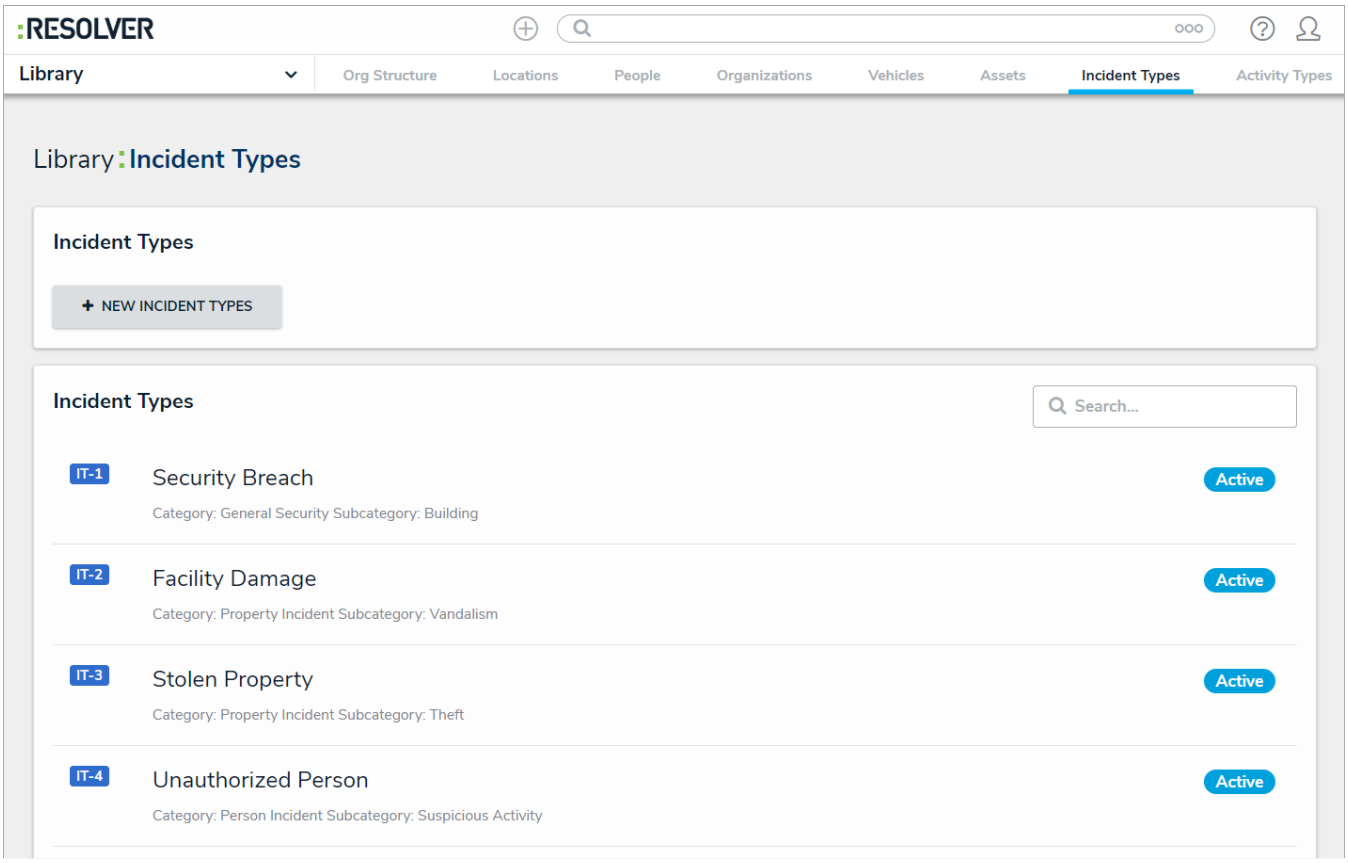
To edit an incident type:

1. Log into a user account that's been added to the **Administrator** user group.
2. Click the dropdown in the nav bar > **Library**.



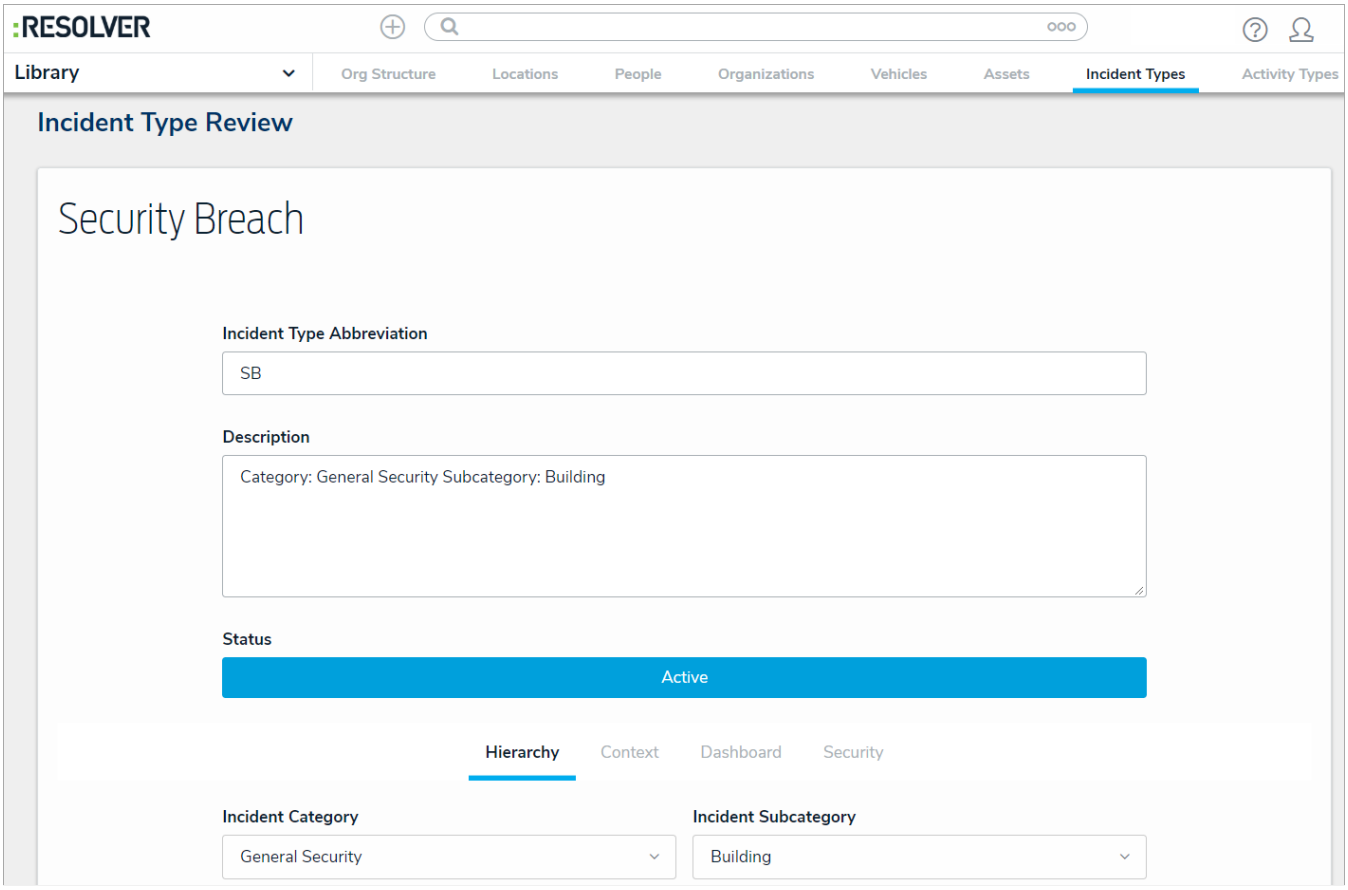
The Library application in the nav bar.

3. Click the **Incident Types** activity.



The Incident Types activity in the Library application.

4. Click an incident type to open the **Incident Type Review** form.



The Incident Type Review form.

5. Add or edit text in the **Incident Type Abbreviation** or **Description** fields as required.
6. Click the **Incident Category** or **Incident Subcategory** fields, then begin typing keywords to display a list of available options, then click to select the appropriate option. If you have used the **Parent Incident Type** field, then these fields are not required.
7. Click the **Context** tab, then select alternate options for **Primary Use Case** and other fields, as required.
8. **Optional**: Click the **Security** tab **> Incident Type Owner** field, then begin typing user names to display a list of available options.

> Incident type owners can read all incidents of that incident type, without being directly assigned to the incident. Users named as an incident type owner who are in the Incident Owner user group can also create incidents with that incident type.

9. Click the **Investigator** field, then begin typing user names to display a list of available options. This user will be able to read all incidents in this Incident Type.
10. Edit all other fields as required.
11. Click one of the following buttons:
    - **Archive**: Archives this incident type.
    - **Done**: Saves all changes.
    - **Trash can:** Deletes the incident type.

> **Do not delete an incident type that is linked to existing incidents, as this may cause irreparable harm to your app**. When you click the Trash can icon, a dialog will open that will tell you if the incident type has any existing relationships or references.

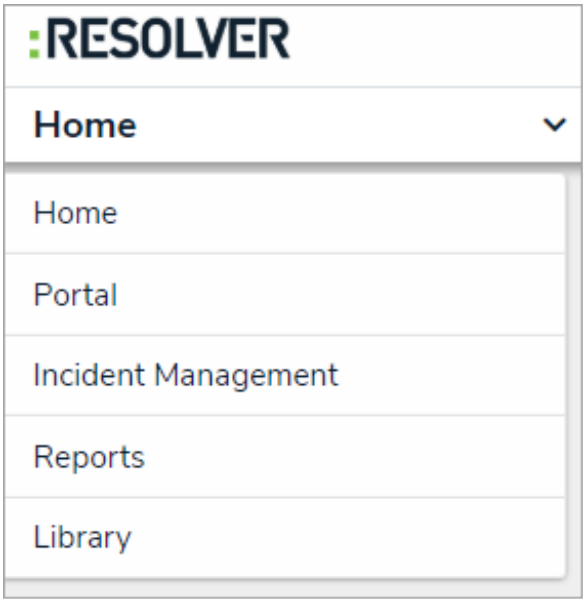
Investigation-Applicable Incident Types

An investigation can only be opened if the associated incident is given an investigation-applicable incident type . Users in the **Administrator** user group can determine if incident types are investigation-applicable.

> The Administrator user group can create library objects only. It is not to be confused with the Incident Management Administrator, who can view incident objects, or the Core Administrator, who can add users.

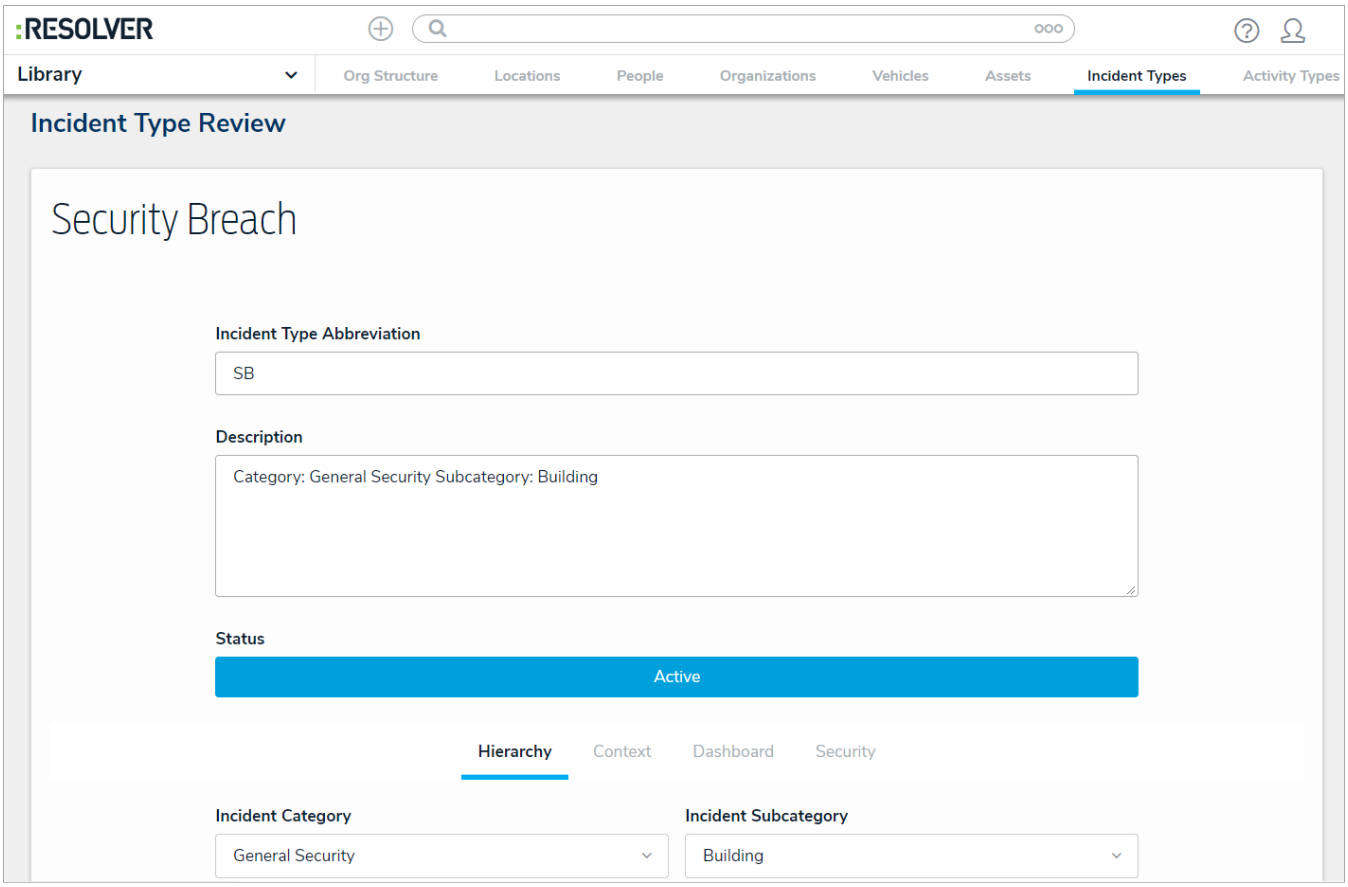
To make an incident type investigation-applicable:

1. Log into a user account that's been added to the **Administrator** user group.
2. Click the dropdown in the nav bar **> Library.**



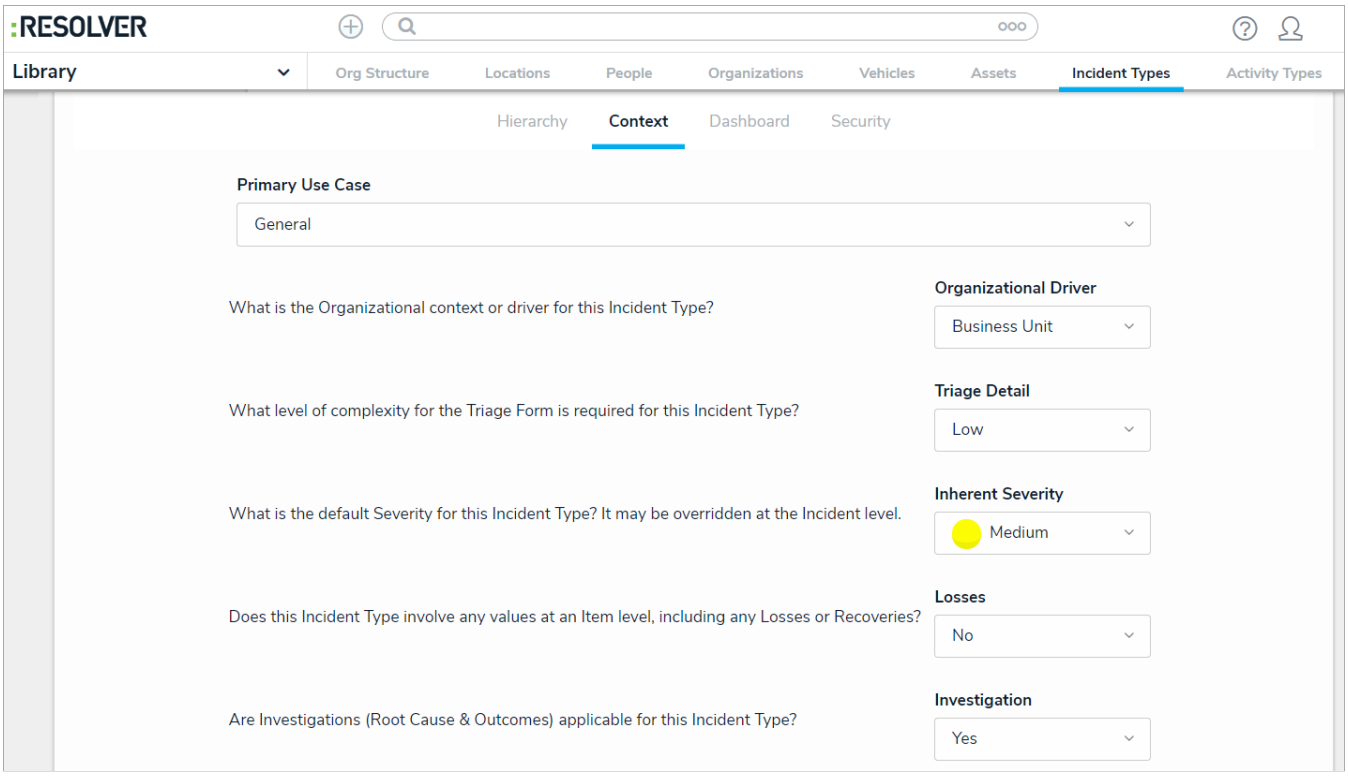
The Library application in the nav bar.

3. Click the **Incident Types** activity.
4. Click an incident type name to open the **Incident Type Review** form.



The Incident Type Review form.

5. Click the **Context** tab.



The Context tab on the Incident Review form.

6. Select **Yes** under **Investigation**.

7. **Optional**: If there is an incident value threshold at which the incident should be automatically investigated, enter the amount in the **Investigation Threshold** field.

When an incident owner edits an incident with this incident type, they will have access to the **Investigator** field and **Open Investigation** button.

Core Administrator Overview

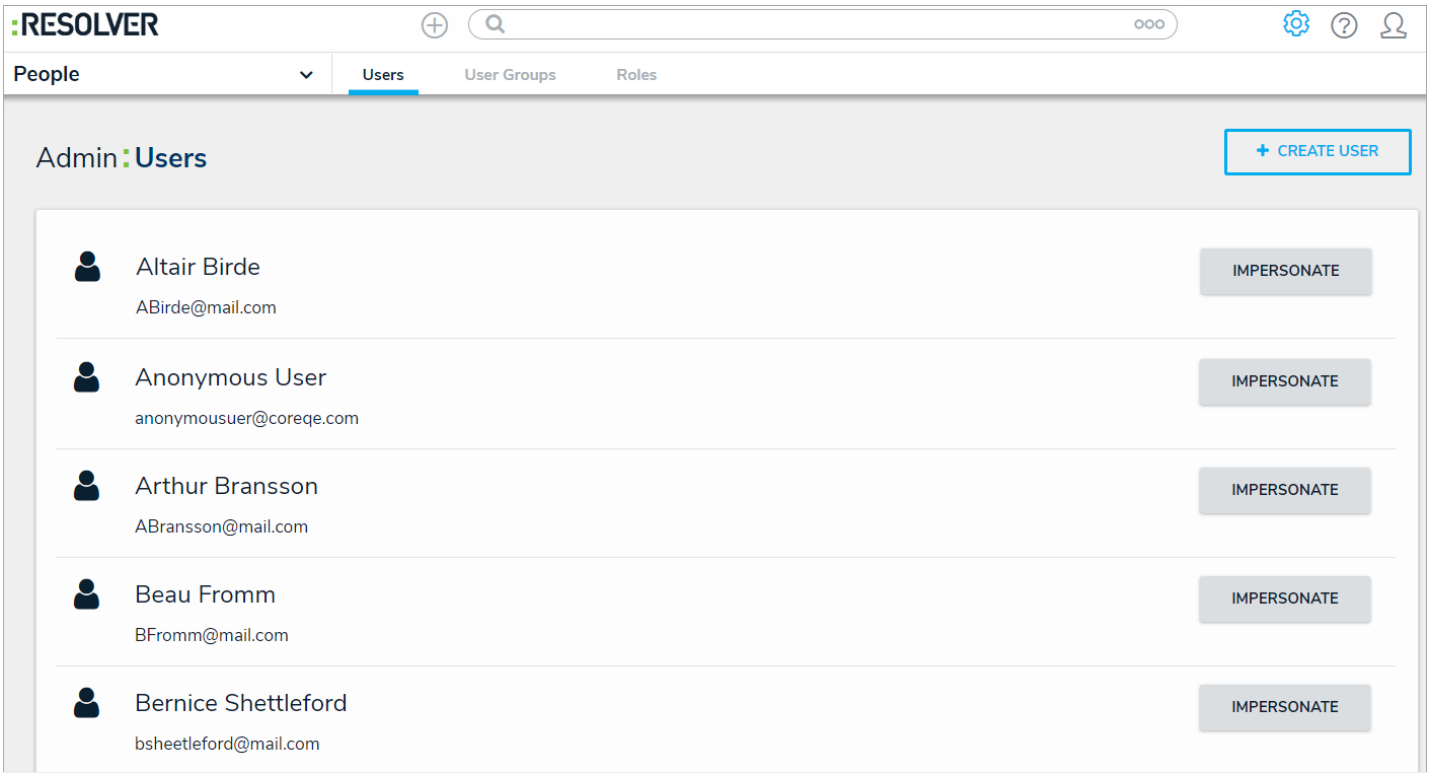
Core administrators are responsible for adding Incident Management users and assigning them to user groups They differ from users in the Administrator and Incident Management Administrator user groups in that they do not have access to Incident Management, unless they have been added to an additional role or user group.

Core administrators can access the **Admin** page by clicking the icon in the top bar on any page. If you're not a Core administrator, this icon will not be visible.

The Core Administrator can create users only. It is not to be confused with the Incident Management Administrator, who can view incident objects, or the Administrator user, who manages Library objects.

Enabling Admin or All Access account status for new users is not recommended. Admin will give usersAdministrative privileges, including the ability to cause irreparable damage to your app. **All Access** will give users the ability to see all objects and object types in your app.

As the Administrator, you may be able to edit other settings in Administration. **Deleting or changing administrative settings may cause irreparable damage to your Incident Management app.** For more information or to request additional configurations to your app's administrative settings, contact Resolver Support.



The Users activity of the Admin page.

Create a New User

Only Core Administrators can add users to Incident Management. Note that adding users is different from adding persons in the Library application. Persons are added to incidents and investigations and can include witnesses, suspects, and related parties. Persons cannot log into the application, whereas users can.

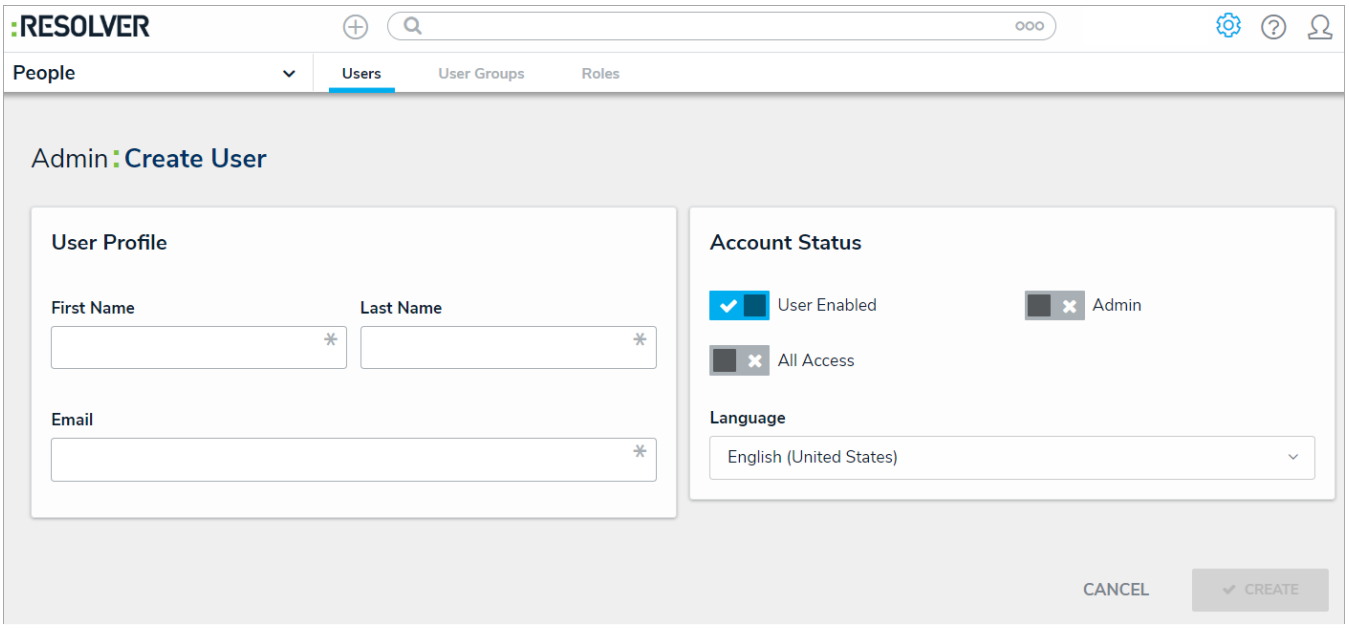
The Core Administrator can create users only. It is not to be confused with the Incident Management Administrator, who can view incident objects, or the Administrator user, who manages Library objects.

Only users with administrative rights can add users to Resolver Incident Management. Users with administrative rights enabled in their profiles can access the **Admin** page by clicking the gear icon in the top bar on any page. If you don't have administrative access enabled, this icon will not be visible.

Enabling Admin or All Access account status for new users is not recommended. Admin will give users Administrative privileges, including the ability to cause irreparable damage to your app. **All Access** will give users the ability to see all objects and object types in your app.

To create a new user:

1. Log into a user account that has access to **Administration**.
2. Click the  icon in the top bar **> Users** in the **People** section.
3. Click **Create User** to show the **Create User** page.



The Create User page.

4. Enter the user's name in the **First Name** and **Last Name** fields.
5. Enter the user's email address in the **Email** field. This is the address that will receive the email with further instructions on creating a password to sign into Core. This email address is also used to authenticate the user when he or she logs in and

therefore must be unique.

> ⚠ Because the user's email address is used to authenticate the user when he or she logs in, ensure the email address is correct before clicking **Create** as you will be unable to modify the address later.

6. **Optional:** Click the  icon next to **User Enabled** to make this user account inactive. By default, the user account is active. **Enabling Admin and All Access privileges is not recommended.**
7. Click **Create**. The new user will receive an email at the email address entered in step 5 with instructions on creating a password and signing into Incident Management.

> ⚠ If you wish to change the language settings for a user, note that translations may not be available for all available languages. Contact Resolver Supportfor assistance before selecting a new language.

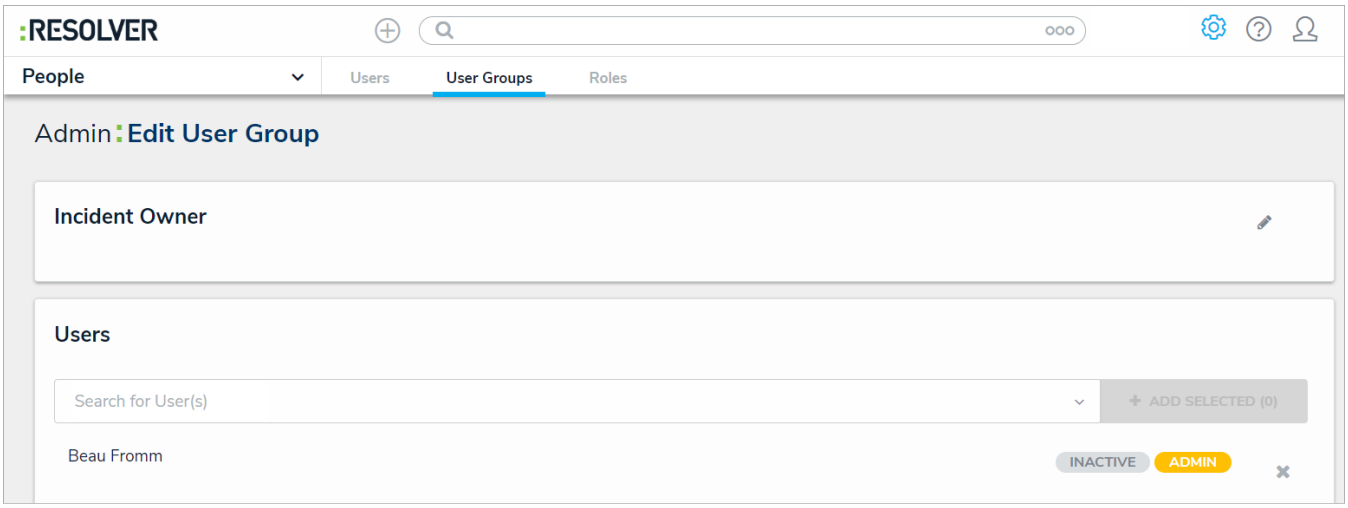
Add a User to a User Group

Incident Management relies on user groups to define user permissions and responsibilities in the app.

> The Core Administrator can create users only. It is not to be confused with the Incident Management Administrator, who can view incident objects, or the Administrator user, who manages Library objects.

To add a user to a user group:

1. Log into a user account that has access to **Administration**.
2. Click the  icon in the top bar **> User Groups** in the **People** section.
3. Click a user group.



The Edit User Group page.

4. Click the **Users** search field and start typing a username, then click the desired user.
5. Click **Add Selected**.
6. Click **Done**.

Important Notes About Deleting or Deactivating User Accounts

If a user should no longer have access to Incident Management, you have the option of disabling that user's account or deleting it. However, it's recommended that user accounts are disabled rather than deleted. If a user needs access to other Resolver apps, you can remove them from their Incident Management user group to remove their access to Incident Management only.

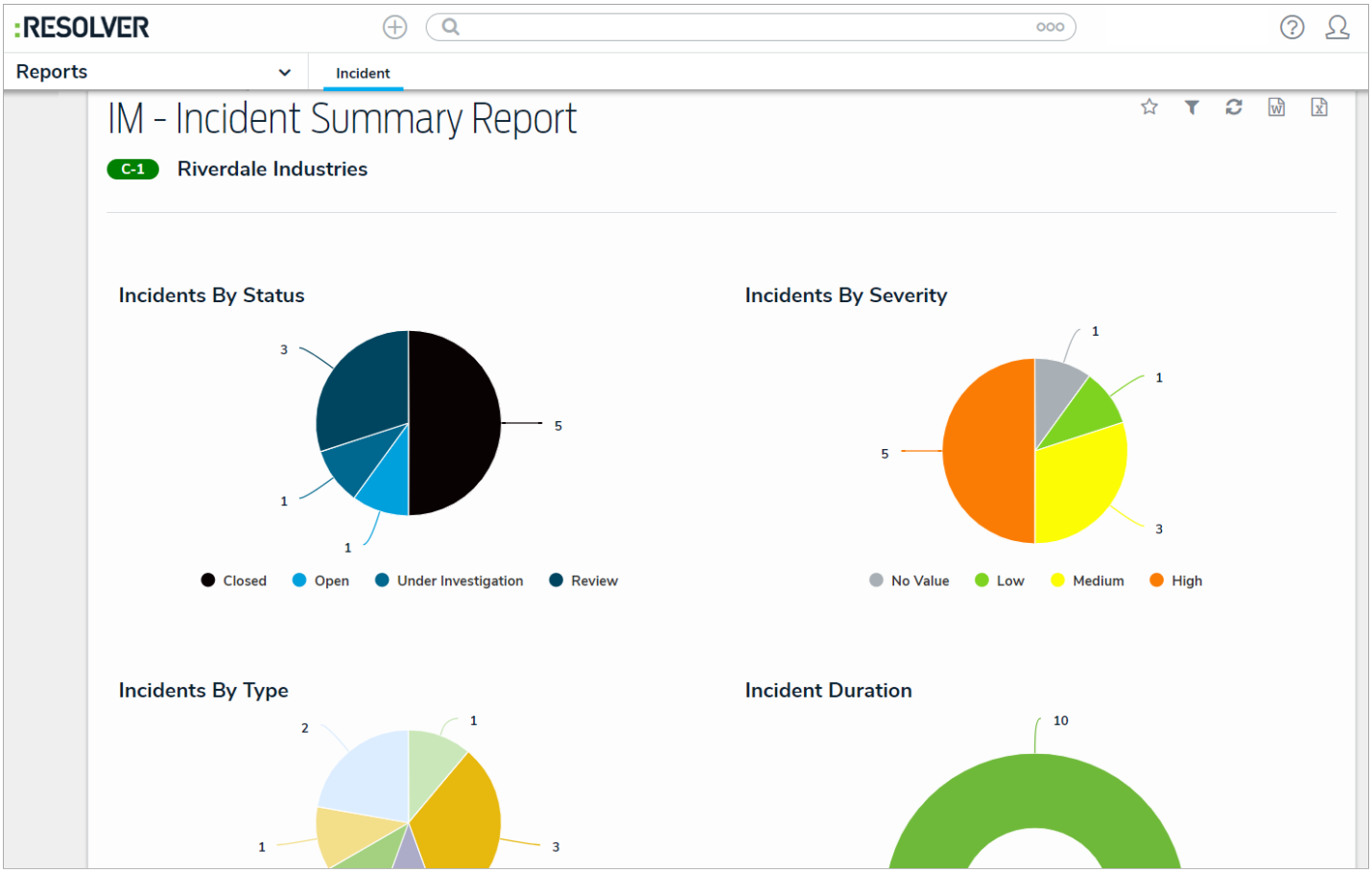
> ⚠ Deleting or disabling a user will also remove their access to any additional Resolver apps.

Deleting a user account prevents the user from logging into your organization and accessing any data and apps, but it also removes that user from any objects they were assigned to via a user group, which may affect your reporting. Disabling an account also prevents the user from logging in and accessing data and apps, but the user is not removed from any assigned objects, thus maintaining your records.

Also note that deleting an account does **not** remove the user from your Core database. If you require that one or more users are removed from the database, contact Resolver Support for assistance.

Reports Overview

Incident Management has several reports available for reviewing and analyzing your incident data. Reports can be viewed by the Incident Owner, Incident Supervisor, and Incident Management Administrator. However, depending on their user permissions, users in these user groups may be restricted from certain reports.



An Incident Management report in the Reports application.

The following reports are available in the Incident Management app.

- **Incident List:** A list of all incidents in your organization, including incident name, severity, and location.
- **Incident Summary**: Charts that display all incidents in your organization, broken down by status, severity, type and duration.
- **Incident Performance**: A visual report that displays incident age and duration.
- **Task List**: Charts and lists of all tasks in your organization, including their type and timeliness.
- **Involved Persons**: Displays all involved people across all incidents in your organization.
- **Market Report**: A list of Markets and Related Incidents (when using market-based Incident Types)
- **Brand Report**: A list of Items and Related Incidents (when using market-based Incident Types)
- **Expired Incident Report**: A list of expired Incidents that should be purged by an administrator, and are no longer visible to end users.
- **Location Overview Report** (coming in version 2.5:1): A graphical representation of Incidents by Location.
- **Region Report** (coming in version 2.5:1): A list of Regions and Related Incidents (when using region-based Incident Types).

View a Report

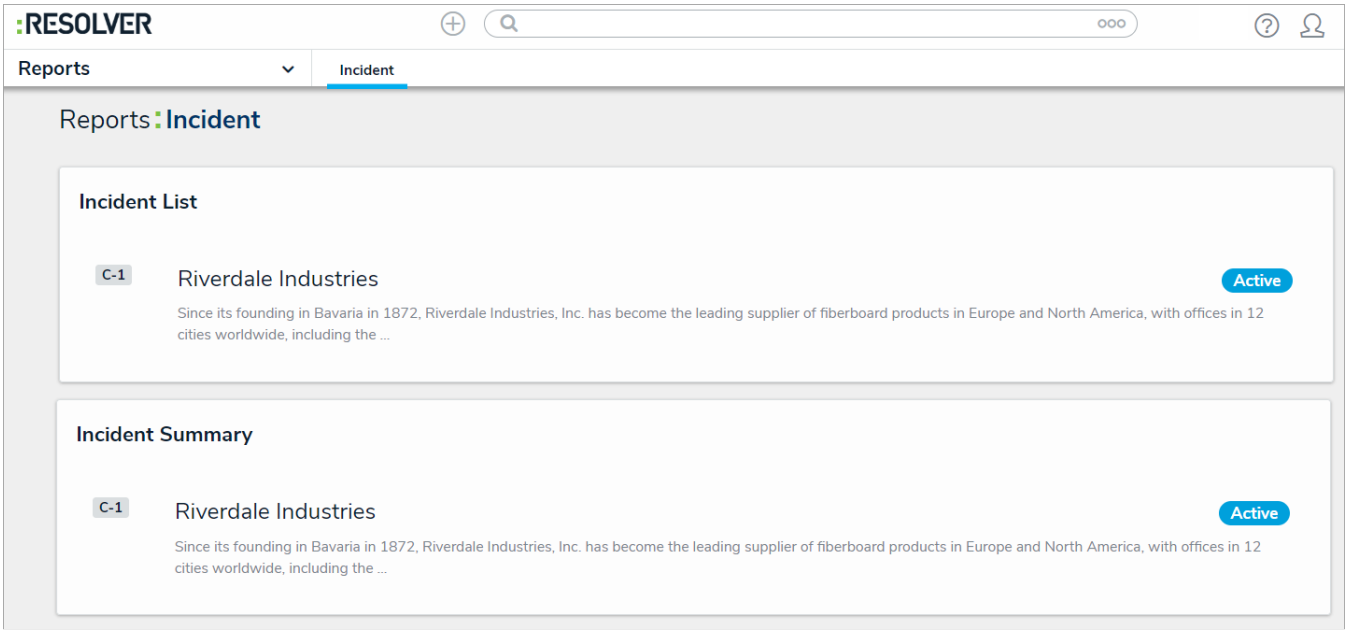
Report visibility is restricted by user group and business unit.

To view a report:

1. Log into a user account that's been added to the **Incident Owner**, **Incident Supervisor**, or **Incident Management Administrator** user group.
2. Click the dropdown in the nav bar **> Reports** to display the **Incident** activity.

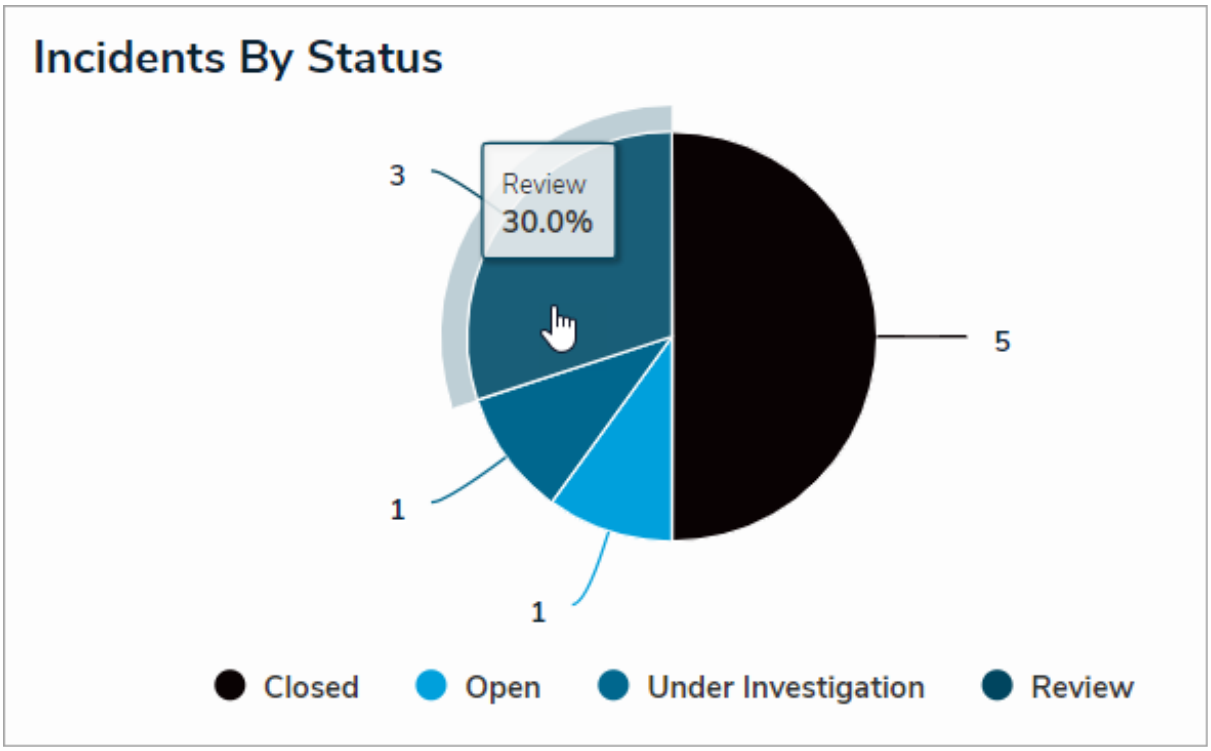
The Reports application in the nav bar.

3. Click a report to open.



Clicking on an anchor object to open a report.

4. If the report includes a bar, column, or pie chart, hover your cursor over the chart for more information about the data. Clicking on a section of a pie chart will separate it from the rest of the chart for emphasis.



Hovering your cursor over a bar, column, or bar chart will display additional information.

5. If the report includes a table:
    a. Click a cell to open the associated object in a palette.
    b. Click a column to sort the data in the table.
    c. Click **Next** or **Previous** at the bottom of the table to scroll through any additional pages.
    d. Enter search terms in the **Search Table...** field to narrow down which data is displayed.
    e. Click the icon to export the table data into a Word document or click the icon to export the table data into an Excel spreadsheet.

Closed Incidents

Search Table...

Incident Name	Incident Start DateTime	Closed Date/Time	Incident Age	Incident Owner
INC-2018-11-29-51 MISC	November 29, 2018 12:06 pm	2018-11-29 12:34	0 - 7 Days	Beau Fromm
CS-2018-11-26-35 ER	November 25, 2018 9:56 am	2018-11-27 9:46	0 - 7 Days	
CS-2018-11-26-34 MISC		2018-11-26 9:33	0 - 7 Days	
CS-2018-11-26-32 GSV		2018-11-26 8:50	0 - 7 Days	
CS-2018-11-26-26 CSMC		2018-11-26 8:00	0 - 7 Days	

Page 1 of 1 | 5 Rows

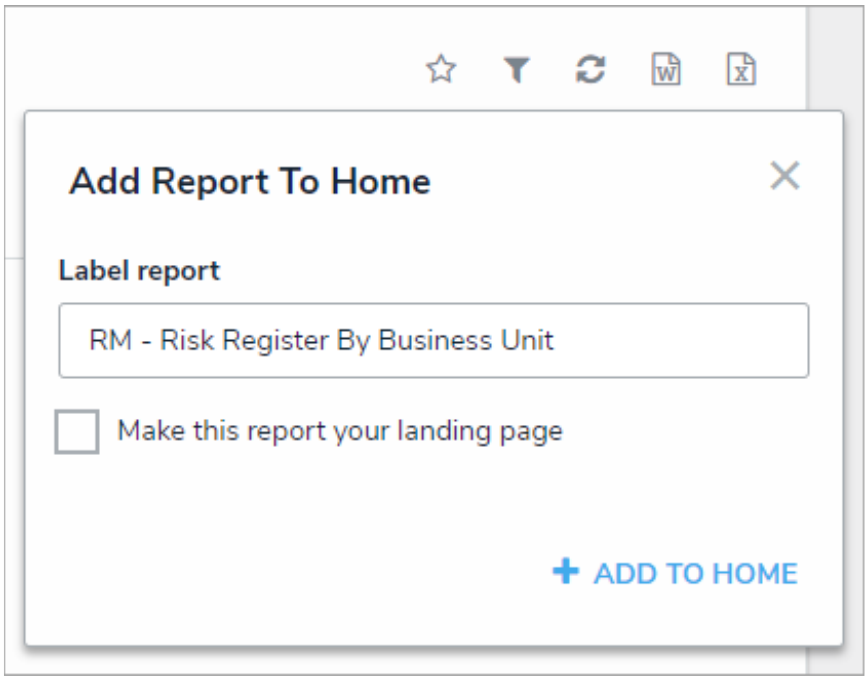
Clicking on a cell in a table will display the associated object in a palette, while clicking on a column header will sort the data in the table

Only table data can be exported into a Word document or Excel spreadsheet. If you export data from a report that also contains a chart or heat map, that data will not appear in the document or spreadsheet.

6. To star a report (create a tab for the report in the nav bar):

   a. Click the ☆ icon at the top-right corner of the report to open the **Add Report To Home** window.

   b. If needed, enter a custom name for the tab in the **Label report** field. The report's name, as saved by an administrator, appears in this field by default.



The Add Report To Home window.

   c. Select the **Make this report your landing page** checkbox if you want this report to replace the My Tasks tab or another report tab as the home page. To revert back the home page back to **My Tasks**, deselect the checkbox.

   d. Click **Add To Home** to finish.

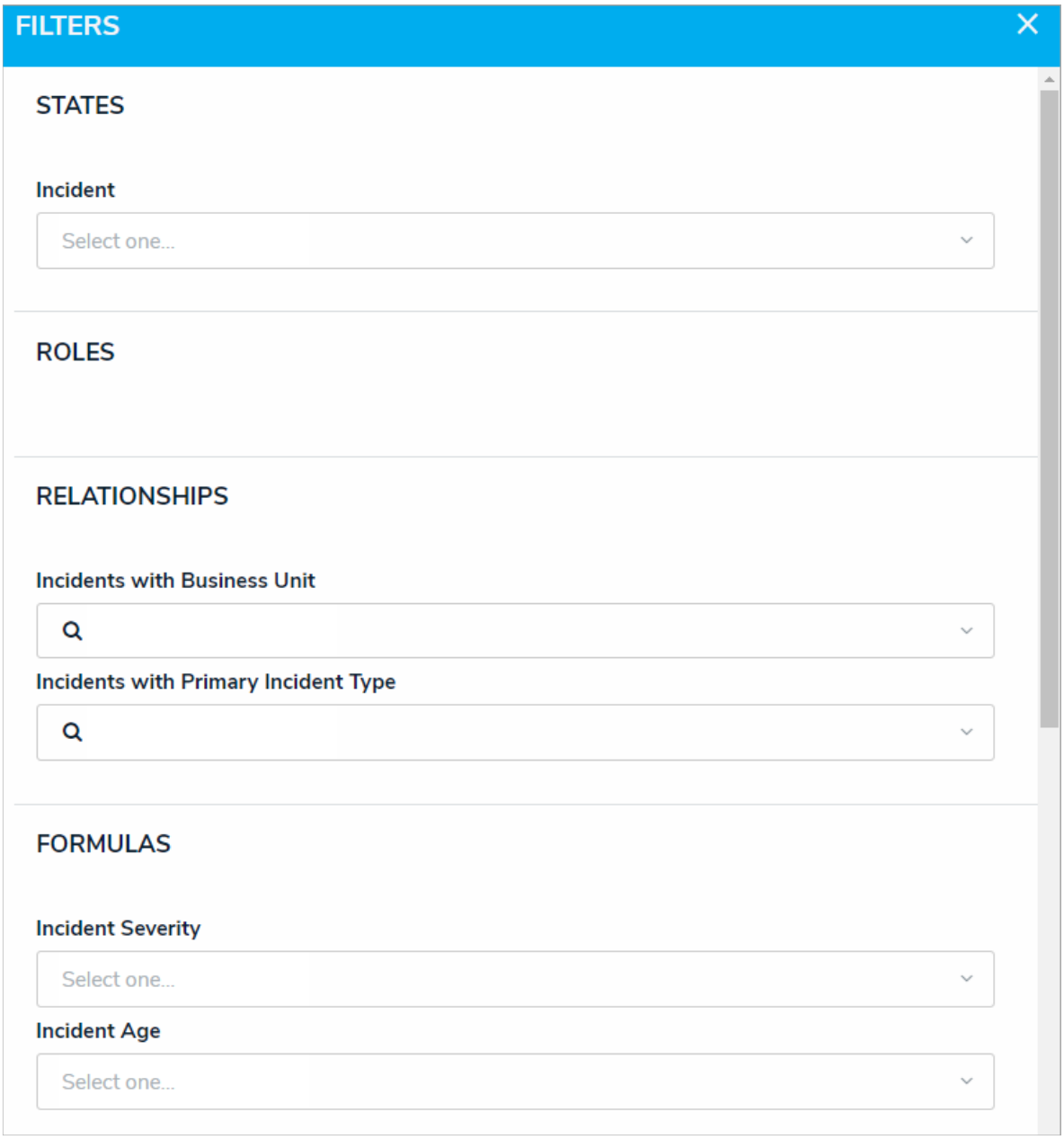
   e. To delete the tab from the nav bar, click the ★ icon, then click **Remove From Home**.

> ✓ For more information on reports added to tabs, see the Starred Reports article.

7. To apply filters to a report (if configured by an administrator):

   a. Click the ▼ icon at the top-right corner of the report to open the **Filters** palette. When a report is displayed with filters applied, the filter icon will appear with a red dot (▼!).

   b. Apply the following filters types as needed. Note that some or all of these sections may be blank if these filter types have not been added to the report by an administrator:
      - **State:** Filters report data by the objects' current workflow state(s).
      - **Role:** Filters report data by users or user groups that have been granted direct access to objects.
      - **Date & Time/Select List:** Filters report data by date and time and/or select list fields .
      - **Relationship:** Displays report data from object types, such as business units or primary incident types, that are linked to incidents.
      - **Object Type:** Displays report data from one or more selected object types.



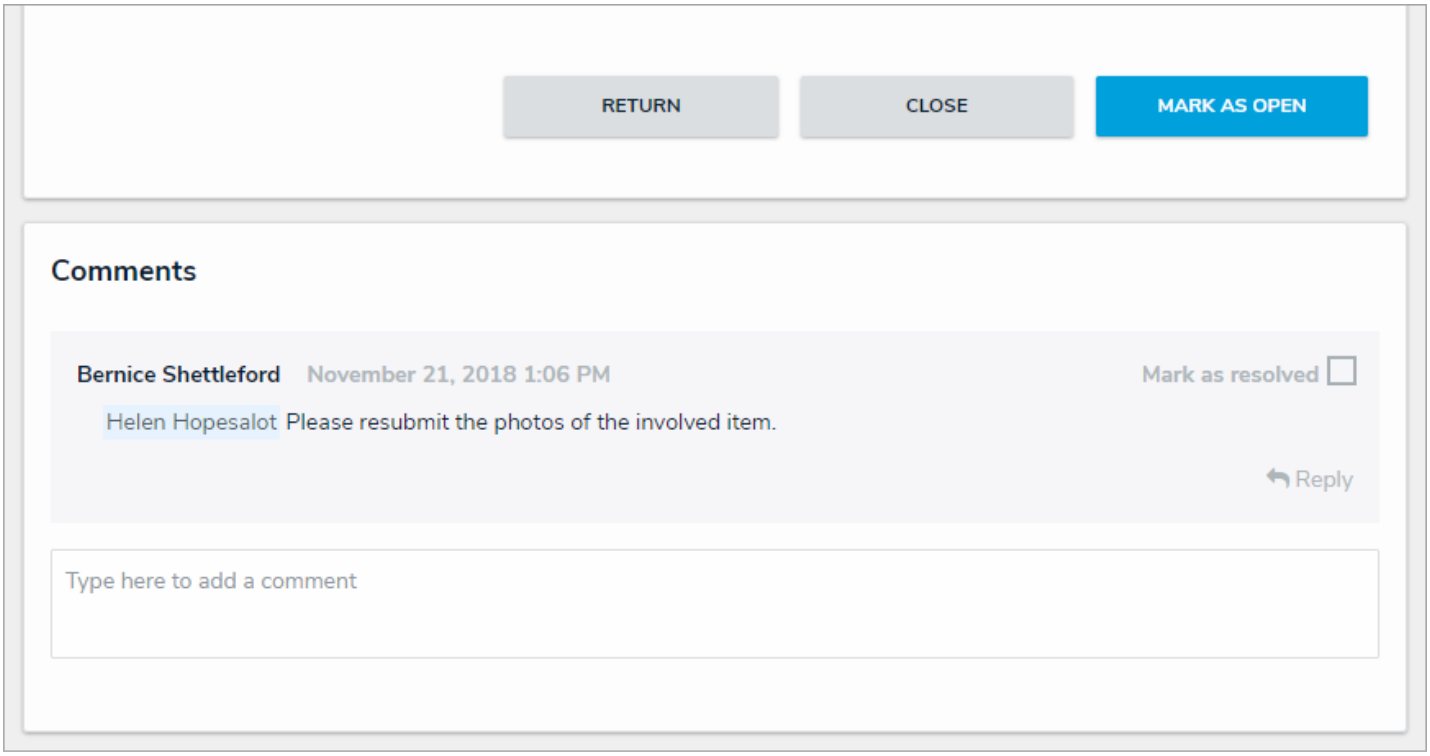
The Filters palette. If an administrator has not added filters, these sections will appear blank.

8. To refresh report data, click the icon.

Incident Form Comments Overview

Depending on their user group and account permissions, users can add and reply to comments on incident and most related objects. When enabling comments on an incident form, note that:

- Clicking **Reply** will create a new comment thread.
- You can tag other users in both comments and replies. To do so, type the @ symbol and begin typing the user's name, then click to select the user. You can tag more than one user per comment or reply.
- Tagged users will receive an email notification with a link to the incident where the comment is posted, however, if that user doesn't have permission to view the object, he or she will not be able to view the incident, or reply to the comment.
- If a user makes a comment and their account is later deleted, their comment remains intact.
- To edit your comment, click the text within the comment. Comments marked as resolved cannot be edited.



Comments on an incident form.

Glossary of Terms

TERM	*DEFINITION*
Activity	Part of an application where users can create, edit, and view data.
Application	Holds activities where users complete tasks (actions) and view information (views).
End users	The non-administrative users who work with Incident Management and its applications.
Field	A component on a form where a user can input data. Fields can include plain text, numeric, date and time formats, as well as select lists (dropdown menus), and attachments.
Incident	An event that is deemed worthy of being recorded, tracked, assessed and analyzed.
Incident Type	A category that describes an incident and can be used to group it with similar incidents.
Investigation	The action of examining an incident's cause and effect.
Library	Contains all object types and their data that can be added to incidents.
Object	A record saved to an object type (the record category). For example, Incident is the object type, while Accident, which outlines the details of an on-site incident, is the object.
Object type	The category of the data collected (e.g. Incident, Employee Record, Witnesses, Vehicles, etc.). Once a record is saved to an object type, it becomes an object.
States	The various stages of the data collection process (e.g. Create, Triage, Review, Investigate, Close) for an object type workflow.
Task	Actions attached to an incident that must be completed before the incident can be closed.
Triage	Incidents submitted to the Portal go to the Triage, where the Incident Screener

TERM	DEFINITION
Triage	vets potential incidents for their validity.
User Groups	A collection of users saved to a group (e.g. Employees or Managers). The user group they are assigned to will determine their rights within the app.
Value	Data entered or selected in a field. For example, Name is the field, but the data entered in that field, John Doe, is the value.
Workflow	Controls the flow of data as well as defines what data is displayed, where it's displayed, and to whom it's displayed through applications, activities, search results, reports, and assignments. Each object type has a workflow.