# Track and Maintain Security Incidents

Exabeam Security Management Platform - Version SMP 2020.3 (CM I54)

Publication date February 9, 2021

**Exabeam**
1051 E. Hillsdale Blvd., 4th Floor
Foster City, CA 94404

650.209.8599

Have feedback on this guide? We'd love to hear from you!
Email us at docs@exabeam.com

Disclaimer: Please ensure you are viewing the most up-to-date version of this guide by visiting the Exabeam Documentation Portal.

## Table of Contents

# 1. Manually Create an Incident

Instead of ingesting incidents from a service as they cross a risk threshold, manually create an incident if you need one immediately.

1. In the navigation bar, click **INCIDENTS**.
2. Select **+ NEW INCIDENT**.
3. Enter information about the incident:
   - **Incident name** – Enter an incident name.
   - **Incident type** – Select an incident type.
   - **Event start time** – Indicate when the incident started.
   - **Event end time** – Indicate when the incident ended, if known.
   - **Queue** – Assign the incident to a queue. If not, the incident is assigned to the default Unassigned queue.
   - **Assignee** – Assign the incident to someone on your team. If not, it is assigned to "unassigned" by default.
   - **Priority** – Low, medium, high, or critical.
   - **Status** – Select the status of the incident: **New**, **In Progress**, **Pending**, **Resolved**, or **Closed**. Feel free to use these statuses according to your organization's workflow and needs.
   - **Restrict to** – Restrict who can access this incident. These people or groups can't see or search for this incident.
   - **Description** – Provide context about the incident.
4. Click **CREATE**.

## 2. Delete an Incident

If you created an incident by mistake or as a test, or something is wrong with your system, consider deleting an incident. When you delete an incident, you increase database storage and remove the incident from being evaluated in metrics.

1. On the **INCIDENTS** page, select the box for incident(s) you're deleting or select a specific incident.
2. Select the trash .
3. A warning appears. Select **DELETE**.

## 3. Filter Incidents

On the **INCIDENTS** page, filter the list of incidents to find those that fit a certain criteria. If you frequently use certain criteria, create your own custom filter.

In the filter panel, filter your incidents by:

- Queue
- Assignee
- Date
- Incident Type
- Status
- Priority
- Entity
- Artifact
- Keyword

There are four out-of-the-box filters.

If you frequently use certain filter inputs, create a custom filter. For example, if you frequently filter for incidents that were false positive and happened in the past 24 hours, you can save how you've configured the filter inputs so you quickly apply it when you need it.

### 3.1. Out-of-the-Box Incident Filters

There are four out-of-the-box incident filters. You can't delete them. If you don't want to use them, build off of them by duplicating them and making changes, or create your own filter from scratch.

| Out-of-the-box filter | Use this filter to view... | Filter inputs |
|---|---|---|
| All Incidents | All open incidents that have been created, no matter who it's assigned to; when it started, ended or was created; or its priority. | Status: New, in progress, resolved, pending |
| My Incidents | All open incidents you've been assigned to. | Owner: Current user<br><br>Status: New, in progress, resolved, pending |
| Unassigned Incidents | Incidents that are recently created and not assigned to a queue. | Owner: Default queue<br><br>Status: New |
| Critical incidents | All open incidents that are a critical priority, no matter who it's assigned to or when it started, ended, or was created. | Priority: Critical<br><br>Status: New, in progress, resolved, pending |

### 3.2. Duplicate an Incident Filter

If you don't want to create a custom filter from scratch, quickly create a filter using an existing filter as a starting point. You can duplicate any filter, including those that come out of the box.

1. On the **INCIDENTS** page, next to the filter name, select the down arrow. The filter menu opens.
2. Select a filter.
3. Next to the filter name, click the More ⋮ menu.
4. Select **Duplicate**. The duplicated filter is named *Copy of [Filter]*.

### 3.3. Create a Custom Incident Filter

Filter incidents to find ones that fit a certain criteria. If you frequently use certain filter inputs to match a criteria, create a custom filter.

1. On the **INCIDENTS** page, next to the filter name, select the down arrow. The filter menu opens.
2. Select **+ Create New Filter**. The existing filter inputs clear.
3. Give the new filter a unique name, then press **Enter** or **Return** on your keyboard.
4. Specify the filter inputs:
   - **Queue** – Assign the incident to queue.
   - **Assignee** – Assign the incident to a person.
   - **Date** – Specify the dates the incident started, ended, was received, or closed.
   - **Incident Type** – Select a type that best matches the security scenario.
   - **Status** – Indicate the current state of your investigation.
   - **Priority** – Indicate how urgent the incident is.
   - **Entity** – Enter the name of an entity.
   - **Artifact** – Enter the name of an artifact.
   - **Keyword** – Search for a word or phrase. You can only search incident names, fields, entity fields, and artifact names. You can't search file content.
5. Next to the filter name, click **Save**.

### 3.4. Edit a Custom Incident Filter

If you created a custom filter, edit the filter inputs to change how it's configured. You can't edit out-of-the-box filters.

1. On the **INCIDENTS** page, next to the filter name, select the down arrow. The filter menu opens.
2. Select a filter.
3. Change the filter inputs:
   - **Queue** – Assign the incident to queue.
   - **Assignee** – Assign the incident to a person.

- **Date** – Specify the dates the incident started, ended, was received, or closed.
- **Incident Type** – Select a type that best matches the security scenario.
- **Status** – Indicate the current state of your investigation.
- **Priority** – Indicate how urgent the incident is.
- **Entity** – Enter the name of an entity.
- **Artifact** – Enter the name of an artifact.
- **Keyword** – Search for a word or phrase. You can only search incident names, fields, entity fields, and artifact names. You can't search file content.

4. Next to the filter name, click **Save**.

### 3.5. Delete a Custom Incident Filter

If you created a custom filter, you can delete it. You can't delete out-of-the-box filters.

1. On the **INCIDENTS** page, next to the filter name, select the down arrow. The filter menu opens.
2. Select the filter you're deleting.
3. Next to the filter name, click the More ⁝ menu, then select **Delete**.

## 4. Search for an Incident

Jump to a specific incident based on keyword using the search bar.

On the **INCIDENTS** page, use search to jump to a specific set of incidents without using filters. You must enter at least three characters.

You search across incident names, incident fields, entity names, artifact names, incident message content. You can't search file content, the activity log, or playbook results.

1. In the navigation bar, click the search .
2. Enter a keyword. A list of matching incidents appears.
3. If you see the incident you're looking for, select it. If you don't see the incident, select **View all incidents with the keyword "[keyword]"** to view a full list in the **INCIDENTS** page.

## 5. Sort Incidents

On the **INCIDENTS** page, sort the list of incidents using the **Sort By** menu. Use this with filters and search to find the incident you need.

Sort incidents by:

- Date created
- Date updated
- Assignee
- Priority
- Status
- Type

## 6. Export a List of Incidents to CSV

To audit incidents, give details about incidents to people outside of your SOC, or archive and back up incident data to your local environment, apply a filter to export a list of incidents to CSV.

The CSV file contains one incident per row and all relevant incident fields. It does not export case notes, entities, or artifacts. You can export a maximum of 10,000 incidents. If you have no incidents, exporting is disabled.

1. Navigate to the **INCIDENTS** page.
2. To gather the incidents you will export, apply a filter. To export all incidents, apply the **ALL INCIDENTS** filter.
3. Next to the filter name, select the More ⋮ menu, then select **Export**.
4. Download the CSV file.