Manage Your Team

Publication date October 30, 2020
# Table of Contents

1. Case Manager Queues .............................................................................................................. 3  
   1.1. Create A Queue ............................................................................................................. 3  
   1.2. Edit A Queue ................................................................................................................. 3  
   1.3. Delete A Queue ............................................................................................................. 3  
2. Exabeam Phases ...................................................................................................................... 5  
   2.1. Create A Phase .............................................................................................................. 5  
   2.2. Rename A Phase ........................................................................................................... 5  
   2.3. Reorder Phases ............................................................................................................. 6  
   2.4. Delete A Phase .............................................................................................................. 6  
3. Exabeam Tasks ........................................................................................................................ 7  
   3.1. Create A Task For A Phase Or Incident Type .............................................................. 7  
   3.2. Edit A Task For A Phase Or Incident Type ................................................................. 7  
   3.3. Delete A Task For A Phase Or Incident Type .............................................................. 8  
   3.4. Create A Task For A Specific Incident ........................................................................... 8  
   3.5. Manage A Task In An Incident .................................................................................... 9
1. **Case Manager Queues**

Effectively manage a shared workload and organize your investigation with queues.

A queue is a group that individuals are assigned to. When Case Manager creates an incident, it routes the incident to a queue. Anyone assigned to the queue can work on this incident. Until someone closes the incident or transfers it to another queue, the incident remains in the queue.

By default, everyone is assigned to the out-of-the-box Unassigned Queue. Create new queues that better fit your needs. You might create queues based on SOC tiers (tier 1, tier 2, and tier 3) or a 24-7 service model.

### 1.1. Create a Queue

To assign incidents to a group of people, create a queue.

1. In the navigation bar, click the Menu, select **Settings**, then navigate to **Case Management > Queues**.
2. Select the add button.
3. Enter a name for the queue.
4. (Optional) Describe the queue.
5. Add members to the queue:
   - In the list of users, click the + icon next to the user's name. To quickly find and add a user, use the search.
   - To add all users in the system, click **ADD ALL**.
6. Click **CREATE QUEUE**.

### 1.2. Edit a Queue

Change the name, description, or member list of an existing queue.

1. In the navigation bar, click the Menu, select **Settings**, then navigate to **Case Management > Queues**.
2. Hover over a queue, then select the pencil.
3. Edit the queue name, description or member list.
4. Click **SAVE QUEUE**.

### 1.3. Delete a Queue

If you've created a queue, you can delete it. Any people and incidents assigned to the queue are reassigned to the default Unassigned queue.
1. In the navigation bar, click the Menu , select Settings, then navigate to Case Management > Queues.

2. Hover over a queue, then select the trash 🗑.

3. Select DELETE.
2. **Exabeam Phases**

Organize your investigations and ensure everyone responds consistently using phases.

A phase is a general stage of your investigating process. It contains tasks that an analyst must complete in each phase.

Phases and tasks ensure everyone across your organization responds to different security scenarios consistently. A manager builds a set of standard scenarios and creates processes for each one. When analysts investigate an incident, they follow this process, working on separate items in parallel so their efforts don’t overlap.

Exabeam provides five phases out of the box:

- Detection
- Containment
- Eradication & Mitigation
- Recovery
- Post-Incident Activity

*Rename phases* or *create your own phases* according to your needs. You can also *delete* and *reorder phases*.

**2.1. Create a Phase**

To standardize how you respond to incidents, break out your investigating process into phases and assign tasks to each one.

1. In the navigation bar, click the Menu, select **Settings**, then navigate to **Case Management** > **Incident Configuration**.
2. Select the **Tasks & Phases** tab.
3. Click **ADD PHASE**.
4. Enter a unique phase name, then click **SAVE**.
5. Click **PUBLISH**. The phase appears only in new incidents. It doesn’t appear in existing incidents, open or closed.

**2.2. Rename a Phase**

Rename any phase to change how they appear in incidents.

1. In the navigation bar, click the Menu, select **Settings**, then navigate to **Case Management** > **Incident Configuration**.
2. Select the **TASKS & PHASES** tab.
3. Hover over a phase, then select the pencil ☛.
4. Change the phase name.
5. Click SAVE.
6. Click PUBLISH. Your changes are reflected in new incidents. They don’t apply to existing incidents, open or closed.

2.3. Reorder Phases
Reorder a phase to change the order that they appear in incidents.

1. In the navigation bar, click the Menu ☰, select Settings, then navigate to Case Management > Incident Configuration.
2. Select the Tasks & Phases tab.
3. Hover over a phase, then select the up ⇑ or down ⇓ arrows to move the phase up or down.
4. Click PUBLISH. Your changes are reflected in new incidents. They don’t apply to existing incidents, open or closed.

2.4. Delete a Phase
Remove a phase from any new incidents you create.

1. In the navigation bar, click the Menu ☰, select Settings, then navigate to Case Management > Incident Configuration.
2. Select the Tasks & Phases tab.
3. You can only delete a phase that does not have tasks assigned to it. If the phase you’re deleting has any tasks assigned to it, reassign them to a new or existing phase.
4. Hover over the phase, then select the trash ☐.
5. Click DELETE.
6. Click PUBLISH. The phase doesn’t appear in new incidents. It still appears in existing incidents, open or closed.
3. Exabeam Tasks

Assign specific responsibilities and ensure everyone responds consistently using tasks.

A task is an action an analyst must complete when they investigate; for example, *confirm incident is contained*, *capture volatile data from systems as evidence*, *determine root cause*. Tasks are organized into phases of an investigation.

Phases and tasks ensure everyone across your organization responds to different security scenarios consistently. A manager builds a set of standard scenarios and creates processes for each one. When analysts investigate an incident, they follow this process, working on separate items in parallel so their efforts don't overlap.

### 3.1. Create a Task for a Phase or Incident Type

Create a task that always appears under a specific phase or incidents of a certain type.

You can create a task just for one specific incident. To automatically create a task depending on the conditions of an incident, set up a playbook.

1. In the navigation bar, click the Menu  then select **Settings**, then navigate to **Case Management > Incident Configuration**.
2. Select the **Tasks & Phases** tab.
3. Click **ADD A TASK**.
4. Fill in the fields:
   - **Name** – Enter a name for the task.
   - **Instructions** – Enter instructions, details, or other information about the task.
   - **Phase** – Select the phase that the task appears under.
   - **(Optional) Incident type** – Select the incident type that the task appears under.
   - **Due date** – If there is no due date, select **None**. If there is a due date, select how many days after the task is initiated.
   - **(Optional) Required task** – If the task is required, select this box.
5. Click **SAVE**.
6. Click **PUBLISH**.

### 3.2. Edit a Task for a Phase or Incident Type

Edit a task that appears under a phase or for all incidents of a certain type.

1. In the navigation bar, click the Menu  then select **Settings**, then navigate to **Case Management > Incident Configuration**.
2. Select the **Tasks & Phases** tab.
3. Hover over a task, then select the pencil 🆁.

4. Change the task details:
   - **Name** – Enter a name for the task.
   - **Instructions** – Enter instructions, details, or other information about the task.
   - **Phase** – Select the phase that the task appears under.
   - **(Optional) Incident type** – Select the incident type that the task appears under.
   - **Due date** – If there is no due date, select None. If there is a due date, select how many days after the task is initiated.
   - **(Optional) Required task** – If the task is required, select this box.

5. Click **SAVE**.

6. Click **PUBLISH**. Your changes are reflected in new incidents. They don't apply to existing incidents, open or closed.

### 3.3. Delete a Task for a Phase or Incident Type
Delete a task that appears under a phase or for all incidents of a certain type.

1. In the navigation bar, click the Menu 🔮, select **Settings**, then navigate to **Case Management > Incident Configuration**.
2. Select the **Tasks & Phases** tab.
3. Hover over a task, then select the trash 🗑. A warning appears.
4. Click **DELETE**.
5. Click **PUBLISH**. Your changes are reflected in new incidents. They don't apply to existing incidents, open or closed.

### 3.4. Create a Task for a Specific Incident
Create a task that only appears under a specific incident to ensure that your team doesn't miss something when they respond to it.

Under each phase, create tasks to ensure your team complete certain duties. Assign the tasks to specific people so they know exactly what they should do to work in parallel. After they complete the task, they mark it as done.

You can create a task that always appears under a phase or for all incidents of a specific type. To automatically create a task depending on the conditions of an incident, set up a playbook.

1. Navigate to **INCIDENTS**, select an incident, then select the **Tasks** tab.
2. In a phase, click **ADD TASK**
3. Fill in the fields:
• **Name** – Enter a name for the task.
• **Instructions** – Enter instructions, details, or other information about the task.
• **Assignee** – Assign the task to a person.
• **Due Date** – Select a date that this task should be closed by.

4. Click **SAVE**.

### 3.5. Manage a Task in an Incident

View, reassign, change the due date, update the status, and add notes to any task, just for that specific incident.

1. Navigate to **INCIDENTS**, select an incident, then select the **Tasks** tab.
2. Select a phase to expand it and view associated tasks, assignee(s), and due date. Hover over the task to view further details.
3. Edit the task:
   - To re-assign the task to another analyst, click the task assignee and select another analyst from the list.
   - To change the due date, click the task due date and select another date on the calendar. If a task is not closed before the due date, the due date appears in red text with a warning icon.
   - To view additional details or update the task status, select the task name. Review the due date, add notes about the conclusion, or mark the task as done.
   - To close a task, select the task name to view additional details, then click **MARK AS DONE** OR On the the **Task** tab, select the checkbox.