exabeam

Configure Case Manager

Exabeam Security Management Platform - Version SMP 2021.1 (CM I55)

Publication date April 26, 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

Add Case Manager and Incident Responder to Advanced Analytics Disaster Recovery

Hardware and Virtual Deployments Only

If you are upgrading from Advanced Analytics SMP 2019.1 (i48) or lower and have configured disaster recovery for Advanced Analytics, add Case Manager and Incident Responder to the existing Advanced Analytics disaster recovery.

WARNING
Configure this only with an Exabeam Customer Success Engineer.

1.1. 1. Stop the Replicator

1. Ensure that the Advanced Analytics replication is current.
2. To ensure that the passive site matches the active site, compare the files in HDFS, the local file system, and MongoDB.
3. Source the shell environment:

```
. /opt/exabeam/bin/shell-environment.bash
```

4. On the active cluster, stop the replicator:

```
sos; replicator-socks-stop; replicator-stop
```

1.2. 2. Upgrade the Passive and Active Advanced Analytics Clusters

NOTE
Both the primary and secondary clusters must be on the same release version at all times.

WARNING
If you have an existing custom UI port, please set the `web_common_external_port` variable in `/opt/exabeam_installer/group_vars/all.yml`. Otherwise, you may lose access at the custom UI port after the clusters upgrade.

```
web_common_external_port: <UI_port_number>
```

1. (Optional) Disable Exabeam Cloud Telemetry Service.
2. If you use the SkyFormation cloud connector service, stop the service.
   a. For SkyFormation v.2.1.18 and higher, run:

```
sudo systemctl stop sk4compose
```

   b. For SkyFormation v.2.1.17 and lower, run:

```
sudo systemctl stop sk4tomcat
sudo systemctl stop sk4postgres
```

> **NOTE**
> After you've finished upgrading the clusters, the SkyFormation service automatically starts. To upgrade to the latest version of SkyFormation, please refer to the *Update SkyFormation app on an Exabeam Appliance* guide at support.skyformation.com.

3. From Exabeam Community, download the `Exabeam_[product]_[build_version].sxb` file of the version you're upgrading to. Place it anywhere on the master node, except `/opt/exabeam_installer`, using Secure File Transfer Protocol (SFTP).
4. Change the permission of the file:

```
chmod +x Exabeam_[product]_[build_version].sxb
```

5. Start a new terminal session using your `exabeam` credentials (do not run as ROOT).
6. To avoid accidentally terminating your session, initiate a screen session.

```
screen -LS [yourname]_[todaysdate]
```

7. Execute the command (where `yy` is the iteration number and `zz` is the build number):

```
./Exabeam_[product]_[build_version].sxb upgrade
```

   The system auto-detects your existing version. If it can't, you are prompted to enter the existing version you are upgrading from.
8. When the upgrade finishes, decide whether to start the Analytics Engine and Log Ingestion Message Extraction engine:

```
Upgrade completed. Do you want to start exabeam-analytics now? [y/n] y
Upgrade completed. Do you want to start lime now? [y/n] y
```

1.3. 3. Add Case Manager to Advanced Analytics

1. SSH to the primary Advanced Analytics machine.
2. Start a new screen session:

```
screen –LS new_screen
/opt/exabeam_installer/init/exabeam-multinode-deployment.sh
```

3. When asked to make a selection, choose **`Add product to the cluster`**.
4. From these actions, choose option **`4`**.

```
1) Upgrade from existing version
2) Deploy cluster
3) Run precheck
4) Add product to the cluster
5) Add new nodes to the cluster
```

```
6) Nuke existing services
7) Nuke existing services and deploy
8) Balance hadoop (run if adding nodes failed the first time)
9) Roll back to previously backed up version
10) Generate inventory file on disk
11) Configure disaster recovery
12) Promote Disaster Recovery Cluster to be Primary
13) Install pre-approved CentOS package updates
14) Change network settings
15) Generate certificate signing requests
16) Exit
Choices: ['1', '2', '3', '4', '5', '6', '7', '8', '9', '10', '11', '12',
'13', '14', '15', '16']: default (1): 4
```

5. Indicate how the node should be configured:

```
Which product(s) do you wish to add? ['ml', 'dl', 'cm']: cm
How many nodes do you wish to add? (minimum: 0): 1
What is the IP address of node 1 (localhost/127.0.0.1 not allowed)?
10.10.2.40
What are the roles of node 1? ['cm', 'uba_slave']: cm
```

6. To configure Elasticsearch, Kafka, DNS servers, and disaster recovery, it's best that you use these values:

```
How many elasticsearch instances per host? [2] 1
What's the replication factor for elasticsearch? 0 means no replication. [0]
How much memory in GB for each elasticsearch instance? [16] 16
How much memory in GB for each kafka instance? [5]
Would you like to add any DNS servers? [y/n] n
Do you want to setup disaster recovery? [y/n] n
```

7. Once the installation script successfully completes, restart the Analytics Engine.

1.4. 4. Configure Disaster Recovery on the Advanced Analytics and Case Manager Passive Clusters

1. On the secondary site, run:

```
screen -LS dr_setup
/opt/exabeam_installer/init/exabeam-multinode-deployment.sh
```

2. Select option: `Configure disaster recovery`.
3. Select the third option: `This cluster is for file replication (configuration change needed)`

```
Please select the type of cluster:
1) This cluster is source cluster (usually the primary)
2) This cluster is destination cluster (usually the dr node)
3) This cluster is for file replication (configuration change needed)
```

4. Enter the IP address of the source cluster.

```
What is the IP of the source cluster?
```

5. Select option: `SSH key`.

```
The source cluster's SSH key will replace the one for this cluster. How do
you want to pull the source cluster SSH key?
1) password
2) SSH key
```

6. Enter the private key path.

```
What is the path to the private key file?
```

   The deployment may take some time to finish.

7. The primary cluster begins to replicate automatically, but all replication items are disabled. You must manually enable the replication items.
   On the secondary site, access the custom configuration file /`opt/exabeam/config/custom/custom_replicator_disable.conf`, then enable replication items.
   For example, if you wish to only fetch compressed event files, then set the `Enabled` field for the [“`.evt.gz`”] file type to `true`:

```
{
    EndPointType = HDFS
    Include {
        Dir = "/opt/exabeam/data/input"
        FilePattern = [".evt.gz"]
    }
    Enabled = true
}
```

8. Start the replicator:

```
sos; replicator-start
```

9. Log on to the standby cluster GUI.
10. To gather context from the active cluster to synchronize the standby cluster, navigate to **LDAP Import** > **Generate Context**, then click **Generate Context**.

1.5. 5. Start the Replicator

On the active cluster, start the replicator:

```
replicator-socks-start; replicator-start
```

2. Configure a Proxy

If your environment has a proxy configured, you must configure a proxy for Case Manager and Incident Responder. Some Case Manager and Incident Responder features use your proxy to function correctly, including services, email ingest and incident email.

1. In the navigation bar, click the menu  , select **Settings**, then select **Core**.
2. Under **SERVICE INTEGRATIONS**, select **Proxy**.
3. To enable the proxy you're configuring, click the **Enable Proxy** toggle.
4. Enter information about your proxy connection:
   - **Hostname/server** – Enter the name of the host or server for the proxy server.
   - **Protocol** – Enter the protocol the proxy server uses: HTTP or SOCKS.
   - **Port** – Enter the port number for the proxy server.
   - **(Optional) Username** – If the proxy is protected by a password, enter your proxy account username.
   - **(Optional) Password** – If the proxy is protected by a password, enter your proxy account password.
   - **(Optional) Whitelist** – whitelist host names and/or domains, like wildcards (for example, 192.168.*) or IP ranges (for example, 192.168.0.0/24). The Incident Responder docker is already whitelisted by default.
5. To validate the connection to your proxy, enter a URL, then select **TEST CONNECTIVITY**. If you see an error, verify the information you entered then retest the connection.
6. Click **SAVE**.

Prerequisites for Configuring Microsoft Exchange Online with OAuth2.0 Authentication

If your Microsoft Exchange Online account uses OAuth2.0 modern authentication, ensure that you complete certain tasks before you configure email ingest and incident email.

To integrate Exabeam with Microsoft Azure Active Directory, register an application on the Microsoft identity platform. Since you can't use the same email account for email ingest and incident email, you must create a separate application for each account. Under **Supported account types**, ensure that you select **Accounts in this organizational directory only**.

- Save the client ID for the application you created. You use this client ID later.
- Add a client secret and save it. You use this client secret later.
- Configure specific Microsoft Graph permissions for your application:
  - Mail.Read
  - Mail.Send
  - Mail.ReadWrite
- Configure the Office 365 Exchange Online **full_access_as_app** permission for your application. Follow the same steps to configure Microsoft Graph permissions, but instead of selecting **Microsoft Graft**, click the **APIs my organization uses** tab, select **Application permissions**, then select **Office 365 Exchange Online**. Select the **full_access_as_app** permission, then click **Add permissions**.
- Grant administration consent to the permissions you configured for your application.

4. Ingest Data into Case Manager

To use Case Manager, you must ingest data from an incident source and pull a specific type of data using an incident feed. After Case Manager has this data, it can create incidents for you to work on.

An **incident source** is the server from which Case Manager ingests data, like:

- Advanced Analytics. Case Manager automatically creates an incident when a user or asset crosses a risk threshold and becomes notable.
- A security product such as a SIEM or an endpoint solution.
- Microsoft Office 365 or Outlook via email ingest.

An **incident feed** is the type of data you pull (Carbon Black, FireEye, etc.). You must configure an incident server before you configure an incident feed.

You create, edit, or delete incident sources and feeds.

4.1. Add an Incident Source

Add an incident source, like ServiceNow, Splunk, or IBM QRadar, to ingest logs from those servers into Case Manager. You must add an incident source before specifying which logs to ingest.

- IP address or host name of the server
- TCP port
- Username and password

To add ServiceNow, you must complete specific prerequisites.

1. In the navigation bar, click the menu, select **Settings**, then select **Core**.
2. Under **INCIDENT INGESTION**, select **Incident Sources**.
3. Click **Add a new incident source**.
4. Enter information about the incident source:
   - **Server Type** – Select the source you wish to ingest data from.
   - **IP Address or Hostname** – Enter the IP address or host name of the server.
   - **TCP Port** – Enter the TCP port number of the server.
   - **Username** – Enter your username for the server.
   - **Password** – Enter your password for the server.
5. To validate your connection to the source, click **TEST CONNECTIVITY**. If you see an error, verify the information you entered, then retest the connection.
6. Click **SAVE**.
   To specify the type of data to query from the source, add an incident feed.

4.2. Add an Incident Feed

If you've added an incident source, specify the type of data to query from the source.

1. Ensure that you've added an incident source.
2. In the navigation bar, click the menu, select **Settings**, then select **Core**.
3. Under **INCIDENT INGESTION**, select **Incident Feeds**.
4. Click **Add a new incident feed**.
5. Fill in the fields, then click **SAVE**.
6. Click **RESTART LOG INGESTION ENGINE**.
7. Choose to restart the log engine immediately or specify a date, then click **RESTART**.

4.3. Email Ingest

Ingest suspicious emails and investigate phishing incidents using Email Ingest.

Case Manager Email Ingest creates incidents from potential phishing emails. It ingests suspicious emails from a designated phishing mailbox, parses relevant fields, creates an incident, then deletes the email from the inbox.

4.3.1. CONFIGURE EMAIL INGEST

Link Case Manager to your phishing inbox to forward suspicious emails to Case Manager and ingest suspicious emails.

- A dedicated phishing inbox that Case Manager has access to. No one should delete, move, or otherwise touch the emails in this inbox. The mailbox cannot be a shared mailbox or subfolder. You can't use the same email account you use for incident email.
- Credentials for the phishing inbox. The account and credentials must have read and write access to the entire mailbox.
- Connection to IMAP, POP3, or Exchange.

Protocol	Port
IMAP	143
IMAP + SSL	993
POP3	110
POP3 + SSL	995
Exchange	443

- If you use Microsoft Exchange Online with OAuth2.0 modern authentication, ensure that you complete specific prerequisites.

NOTE
For SaaS Cloud deployments, only port 443 is open. To open other ports, contact your Technical Account Manager.

1. Ensure that emails aren't encrypted and attachments are in EML format. MSG files are not yet supported.
2. In the navigation bar, click the menu, select **Settings**, then select **Core**.
3. Under **INCIDENT INGESTION**, select **Email Ingest**.
4. Enter information about your email connection:
   - **Host/Server** – A mail server or host; for example, outlook.office365.com
   - **Username** – An assigned username. For IMAP, enter the email address. For Exchange, enter [domain]\[username]
   - **Email address** – The email address where emails are sent. This can't be a shared email.
   - **Password** – The password for the username you previously entered.
   - **Protocol** – The email protocol used to connect to your mail server: **IMAP**, **POP3**, **Exchange**. Select the box if your email provider supports Secure Sockets Layer (SSL). If you select **Exchange**:
     - **Exchange version** – Select your version of Microsoft Exchange:
       - Microsoft Exchange 2007, Service Pack 1
       - Microsoft Exchange 2010
       - Microsoft Exchange 2010, Service Pack 1
       - Microsoft Exchange 2010, Service Pack 2
       - Other Exchange Version
     - **Authentication type** – Select the protocol used to authenticate to your Exchange host: **BASIC**, **NTLM**, or **OAUTH2.0**.

     If you select **OAUTH2.0**:
     - **Client ID** – Enter your Exabeam Microsoft Application (client) ID.
     - **Client secret** – Enter your Exabeam Microsoft Application client secret.
     - **Tenant ID** – Enter your Microsoft Azure AD tenant ID.
     - **National cloud** – If you have a national cloud deployment of Microsoft Azure, select your national cloud: **China**, **Germany**, or **USGovernment**. If you don't have a national cloud deployment, select **Global**.
   - **Port** – The port number your mail host or server uses.
   - **Log level** – Case Manager generates logs about your system activity that Customer Success uses to debug problems in your system. Select how detailed these log are: **low** or **verbose**. To conserve disk space, it's best to select **low**. If you have problems with your system, Customer Success may direct you to change log level to **verbose**.

- **Folder** – Which account folder you're pulling emails from. The default folder is Inbox.

5. Click **SAVE**.
6. To start ingesting emails, click **START**.
   By default, Case Manager ingests emails starting from today. To ingest emails starting from a different date, click **Select a different date**, then select a date in the calendar.

5. Configure Incident Email

Link Case Manager to an email account to send incident emails directly from an incident.

You can't use the same account you configured for email ingest.

- An email account from which users send and receive Case Manager-related messages (for example, casemanagement@mycompany.com). The mailbox cannot be a shared mailbox or a subfolder. You can't use the same email account you use for email ingest.
- Credentials for the email inbox. The account credentials must have read and write access to the entire mailbox.
- IMAP connectivity.

Protocol	Port Number
IMAP	143
IMAP + SSL	993

- If you use Microsoft Exchange Online with OAuth2.0 modern authentication, ensure that you complete specific prerequisites.

1. Ensure that emails aren't encrypted and attachments are in EML format. MSG files are not yet supported.
2. In the navigation bar, click the menu , select **Settings**, then select **Core**.
3. Under **INCIDENT INGESTION**, select **2-Way Email**.
4. Enter information about your email account, inbound connection, and outbound connection:
   - **Username** – Enter the username for the mail server. This may be an email address.
   - **Password** – Enter the password for the mail server.
   - **Email address** – Enter the email address on the mail server.
   - **Folder** – Enter the name of the folder from which emails are ingested.

   Inbound
   - **Inbound host/server** – Enter the name of the inbound mail server.
   - **Inbound protocol** – Select the mail protocol used to receive emails.
   - **Inbound port** – Enter the inbound protocol port number.

   Outbound
   - **Outbound host/server** – Enter the name of the outbound mail server.
   - **Outbound protocol** – Select the mail protocol used to send emails.
   - **Outbound port** – Enter the outbound protocol port number.
   - **Exchange protocol** – Select the box if you use Microsoft Exchange Online.

5. If you selected the **Exchange Protocol** box, enter additional information about your Microsoft Exchange Online account and connection:
   - **Exchange host** – Enter the host name of your Microsoft Exchange server.
   - **SSL** – Select the box if you installed a Secure Sockets Layer (SSL) certificate on your Microsoft Exchange server.
   - **Exchange port** – Enter the port number your Microsoft Exchange host uses.
   - **Authentication type** – Select the protocol used to authenticate to your Exchange host: **BASIC**, **NTLM**, or **OAUTH2.0**.
   - **Exchange version** – Select your version of Microsoft Exchange:
     - Microsoft Exchange 2007, Service Pack 1
     - Microsoft Exchange 2010
     - Microsoft Exchange 2010, Service Pack 1
     - Microsoft Exchange 2010, Service Pack 2
     - Other Exchange Version
   - **Log level** – Case Manager generates logs about your system activity that Customer Success uses to debug problems in your system. Select how detailed these log are: **low** or **verbose**. To conserve disk space, it's best to select **low**. If you have problems with your system, Customer Success may direct you to change log level to **verbose**.
6. If you selected **OAUTH2.0** as your **Authentication type**, enter additional information about the application you registered on Microsoft:
   - **Client ID** – Enter your Exabeam Microsoft Application (client) ID.
   - **Client secret** – Enter your Exabeam Microsoft Application client secret.
   - **Tenant ID** – Enter your Microsoft Azure AD tenant ID.
   - **National cloud** – If you have a national cloud deployment of Microsoft Azure, select your national cloud: **China**, **Germany**, or **USGovernment**. If you don't have a national cloud deployment, select **Global**.
7. To validate the inbound and outbound connection to your mail server, click **TEST INBOUND** and **TEST OUTBOUND**. If you see **Failed to test Service connectivity**, verify that you entered the correct email account, inbound connection, and outbound connection information.
8. Click **SAVE**.
9. To enable the email route, click **START**.
   The email route appears in the **EMAIL FEEDS** list with a **RUNNING** status.

6. Customize Incidents

Customize incident types, fields, and layouts to better align Case Manager with your existing or other internal ticketing systems.

Depending on your organization and your industry, consider customizing incidents to tailor Case Manager to your needs. For example, a hospital SOC may create a HIPAA field to review the percentage of historical incidents in which HIPAA data was breached, or view all active incidents that contain HIPAA data.

Start by creating an incident type. Then, create custom fields for that type and organize them into a layout that works best for you.

For each incident type, create phases and tasks to standardize your team's response to that type of incident and enforce them to take certain steps.

6.1. Incident Types

Standardize information, actions, and evidence for common security incidents using incident types.

An incident type is a category that represents a security scenario. When you create an incident type, you standardize incident fields, phases, tasks, and playbooks, and ensure you have the information and tools you need to resolve an incident based on attack vector or case context.

For example: In your organization, a phishing campaign targets multiple users, and each user automatically triggers and creates an incident. Since all these incidents are of a specific type—phishing—you need a specific set of information, actions, and evidence to resolve them, like sender, recipient, or email subject. The phishing incident type makes sure those are all included in a phishing incident so you have everything you need to research and resolve it.

6.1.1. CREATE AN INCIDENT TYPE

Create an incident type to represent a common security scenario and standardize information, actions, and evidence.

1. In the navigation bar, click the menu  , select **Settings**, then select **Analytics**.
2. Under **Case Management**, select **Incident Configuration**.
3. In the **Types** tab, click **ADD TYPE**.
4. In the **CREATE INCIDENT TYPE** menu, enter a name and description for the incident type.
5. Click **SAVE**. The new incident type appears in the list of incident types with a **Custom** status. For your new incident type, create custom incident fields or design a custom layout.

6.1.2. DELETE AN INCIDENT TYPE

When you delete an incident type, you can no longer apply the type to any incidents. You won't delete an existing incident that was assigned the type or any of its data.

1. In the navigation bar, click the menu, select **Settings**, then select **Analytics**.
2. Under **Case Management**, select **Incident Configuration**.
3. In the **TYPES** tab, hover over an incident type, select the More menu, then select **Delete**.
4. A warning appears. Click **DELETE**.

6.2. Customize the Layout of an Incident Type

If you created an incident type, organize the incident fields based on what's relevant to the type. For example, for a phishing incident type, design a layout that includes incident fields like *subject*, *sender*, and *email body*.

1. In the navigation bar, click the menu, select **Settings**, then select **Analytics**.
2. Under **Case Management**, select **Incident Configuration**.
3. To create an incident type or edit an existing type, hover over the incident type, select the More menu, then select **Edit**.
4. Design the layout:
   - To add a field to the layout, select a field, then click and drag the field from the left-side column to the editor on the right.

     To find a field, select the search then enter a search term, or select **Sort by:** to sort them.
     To create a custom field, click **+ ADD FIELD**.
   - To rearrange fields in the editor, click and drag the fields to where they should be positioned.
   - To remove a field from the layout, hover over the field, then click **REMOVE**.
5. Click **SAVE**.

6.2.1. CREATE A CUSTOM INCIDENT FIELD

If you created an incident type, create specific incident fields for that type to standardize the information you need.

1. In the navigation bar, click the menu, select **Settings**, then select **Analytics**.
2. Under **Case Management**, select **Incident Configuration**.
3. Select the **FIELDS** tab.
4. Click **ADD FIELDS**.
5. Enter information about your field. The information required varies based on field type.
   To list multiple values, select **List predefined options**. If people can enter or select multiple values from this list, select **Can enter or select multiple values**.
6. Click **SAVE**.

6.2.2. EDIT A CUSTOM INCIDENT FIELD

When you edit an incident field, the changes only apply to new incidents. If an existing incident has this field, it doesn't change.

1. In the navigation bar, click the menu , select **Settings**, then select **Analytics**.
2. Under **Case Management**, select **Incident Configuration**.
3. Select the **FIELDS** tab.
4. Hover over an incident type, click the More menu, then select **Edit**.
5. Edit the field inputs.
6. Click **SAVE**.

6.2.3. DELETE A CUSTOM INCIDENT FIELD

When you delete an incident field, the field still appears in incidents that already have it but you can't add it to a new incident layout.

1. In the navigation bar, click the menu , select **Settings**, then select **Analytics**.
2. Under **Case Management**, select **Incident Configuration**.
3. Select the **FIELDS** tab.
4. Hover over an incident field, click the More menu, then select **Delete**.

6.3. 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 phase according to your needs. You can also delete and reorder phases.

6.3.1. 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 select **Analytics**.
2. Under **Case Management**, select **Incident Configuration**.
3. Select the **Tasks & Phases** tab.
4. Click **ADD PHASE**.
5. Enter a unique phase name, then click **SAVE**.
6. Click **PUBLISH**. The phase appears only in new incidents. It doesn't appear in existing incidents, open or closed.

6.3.2. RENAME A PHASE

Rename any phase to change how they appear in incidents.

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

6.4. 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.

6.4.1. 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, select **Settings**, then select **Analytics**.
2. Under **Case Management**, select **Incident Configuration**.
3. Select the **Tasks & Phases** tab.
4. Click **ADD A TASK**.
5. Enter information about the task:
   - **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.
6. Click **SAVE**.
7. Click **PUBLISH**.

6.4.2. REORDER TASKS IN A PHASE

Reorder tasks to change the order they appear in a phase.

1. In the navigation bar, click the menu, select **Settings**, then select **Analytics**.
2. Under **Case Management**, select **Incident Configuration**.
3. Select the **Tasks & Phases** tab.
4. Hover over a task, then select the up or down arrows to move the task up or down.
5. Click **PUBLISH**. Your changes are reflected in new incidents. They don't apply to existing incidents, open or closed.

6.4.3. 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 select **Analytics**.
2. Under **Case Management**, select **Incident Configuration**.
3. Select the **Tasks & Phases** tab.
4. Hover over a task, then select the trash. A warning appears.
5. Click **DELETE**.

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