O-INSIGHTS™

O-Insights™ Command Center–1.0 User Guide

Table of Contents

About Command Center

The O-Insights Command Center for XProtect is designed to streamline incident management within security operations. It provides an intuitive interface that simplifies the automation of complex post-incident procedures. By integrating with XProtect, the Command Center ensures that users can manage incidents swiftly and efficiently, enhancing overall response effectiveness and operational continuity. This solution is ideal for environments where quick decision-making and incident resolution are critical.

Prerequisites

Ports to be opened: **9026, 9027, 9028, 9011**

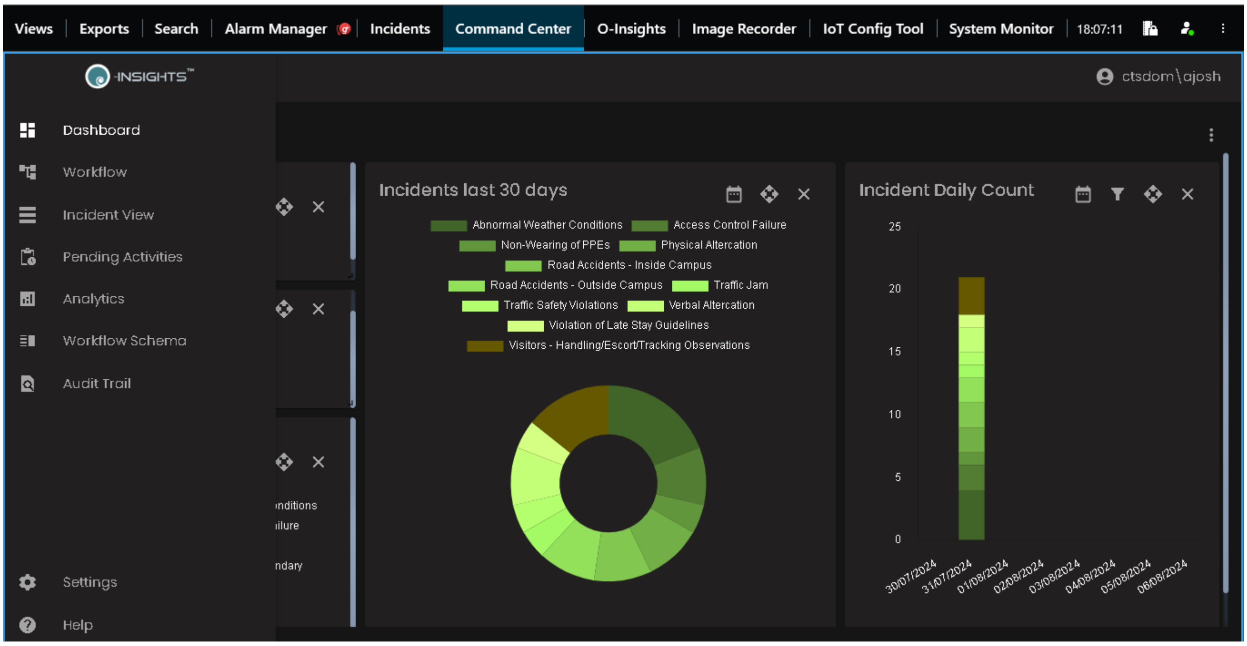
Port Number	Service	Source	Destination
9011	O-Insights Query engine service	O-Insights Command Center Service, XProtect Smart Clients running O-Insights Command Center	Server running O-Insights Query Engine
9026,9027,9028	O-Insights Command Center	XProtect Smart Clients running O-Insights Command Center	Server running Command Center

Configuration

Note: During the installation of the O-Insights Command Center service, use the system's DNS (Domain Name System) as the Query Engine address.

Dashboard

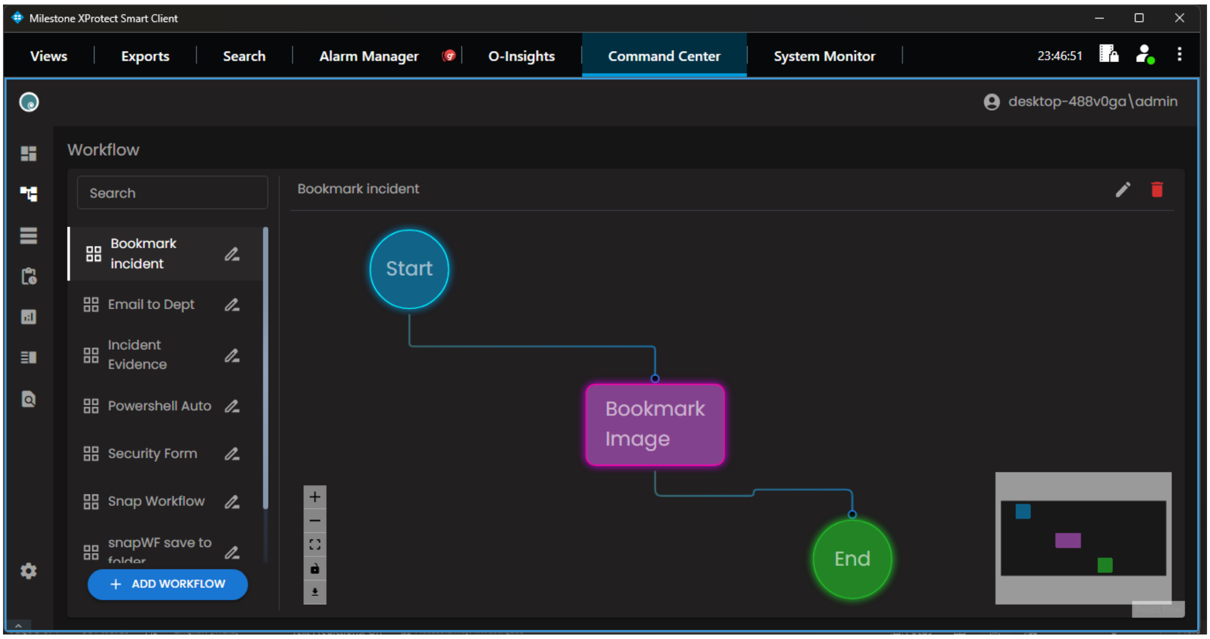
The Dashboard offers a customizable space tailored to provide users with rapid insights. It features an array of widgets that can display data through Bar charts, Donut charts, and Value cards, ensuring a personalized experience. This setup allows users to quickly access and interpret the data that matters most to them, enhancing decision-making processes and operational efficiency.



Dashboard

Workflows

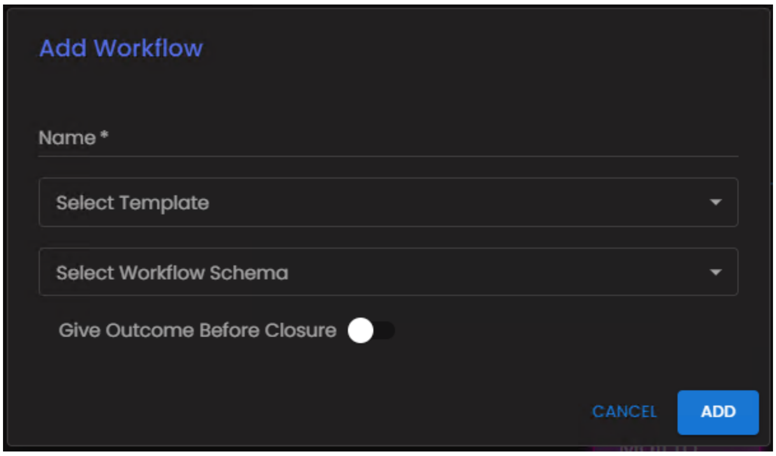
The Command Center enables users to create, update, delete, and view workflows, enhancing process management. As illustrated below, **each workflow is required to include a start and an end node**, which ensures that every process is properly initiated and completed.



Command Center

Adding a Workflow

To create a new workflow:



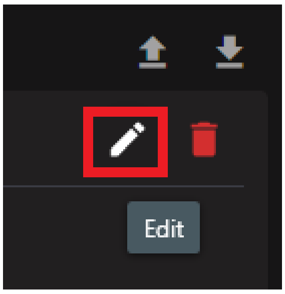
- Click on + *ADD WORKFLOW*. This will open a new pop-up as depicted in the image.
- In the *Name* field, enter the name for the workflow.

- Click on *Select Template* and choose the desired template. The default template is *basic.*
- From *Select Workflow Schema*, you can select any pre-existing schema or proceed without selecting one.
    - Go to the *Workflow Schema* from the sidebar to create a new schema.
- If you wish to add Reasons and Outcomes to a workflow for a particular incident, enable *Give Outcome Before Closure*. If not, you can proceed without it.
    - When you enable *Give Outcome Before Closure*, you need to add Reasons and Outcomes before an Incident Case is completed. This is detailed below.
- Once done, click the *Add* button and the workflow will be created and show up in the workflows list, which is searchable.

Configuring the Workflow

After adding a workflow to the workflows list, you can modify and further develop it by following these steps:

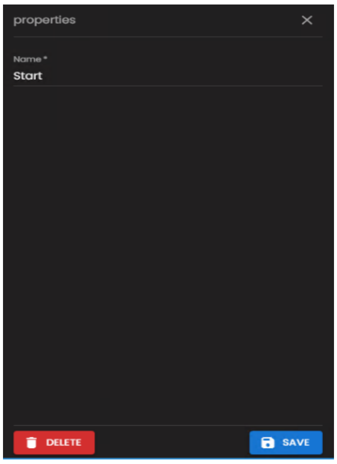
- Navigate to the workflows list and locate the workflow you wish to modify.



- Click on the *Edit* button associated with the workflow to open the workflow editing interface.

Understanding and Configuring Workflow Nodes

A node is a fundamental building block of a workflow, acting as a distinct point that can execute specific functions or decisions within the workflow sequence. It enables users to construct and customize workflows by linking various nodes together to define a clear path of operations or data processing.

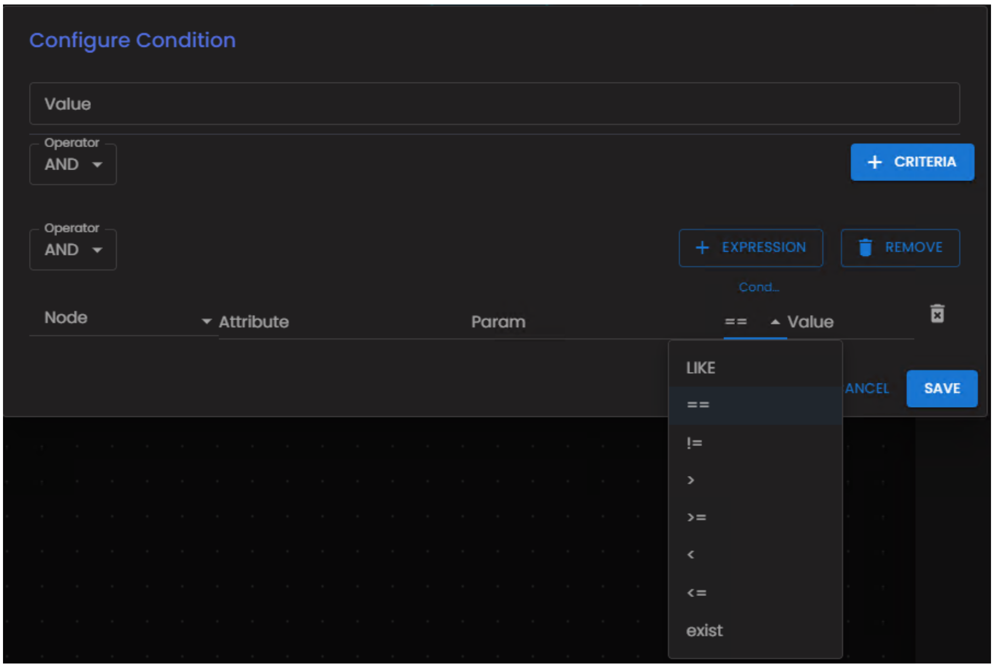


Name *
Start

- **Start Node:** Represents the beginning of the workflow. Click on it to open its *Properties* on the right, as shown above. You can edit the name in the *Name** field and click *Save*. **All workflows should begin with the Start Node.**

- **End Node:** Marks the end of the workflow. It can be edited similar to the Start Node. **All workflows should end with the End Node.**
- **Error Node:** Indicates an error has occurred within the workflow. This node can also be edited like the Start Node.
- **Task Node:** A dynamic node that triggers various actions. It can be configured for manual tasks like form filling or set for automatic processes. Task Node functionalities include:
    - Close Alarm
    - Create Bookmark
    - Create Evidence Lock
    - Email
    - Form
    - Get Snapshot
    - PowerShell
    - REST Call
    - Trigger Event
    - Video Export

- **Approval Node:** Allows specific roles and users to accept or decline workflow tasks, providing control over critical points in the workflow. When the workflow reaches this point, users can review pending tasks and choose to either accept or decline them, providing a reason for their decision.

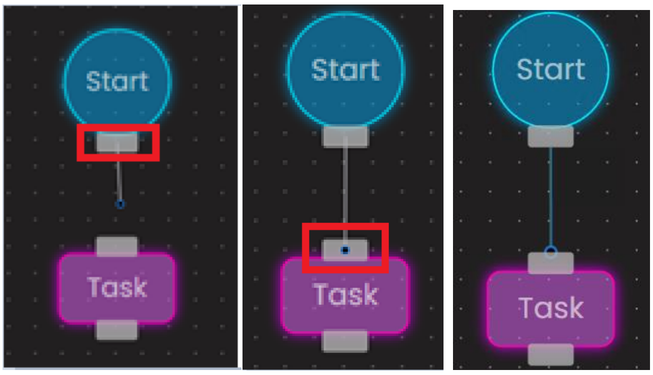


- **Condition Node:** Enables the creation of conditions that direct the workflow's path. Conditions are structured as follows:
  - *Value* and *Criteria*: Define what triggers the condition.
  - *Expressions*: Composed of a left-hand side (LHS) which includes a node, attribute, and parameter; an operator (like, ==, !=, >, >=, <, <=, exists); and a right-hand side (RHS) which defines the condition to be met.
- **Wait Node:** Ensures that all incoming routes are completed before proceeding, ensuring all conditions are met.

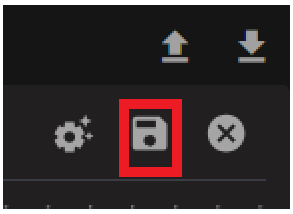
Building Workflow with Nodes

- To add new nodes, select the node type from the *Blocks* section and drag it onto the workflow canvas.
- To delete a node, select the node on the canvas and press the *Delete* button or the trash icon next to it.

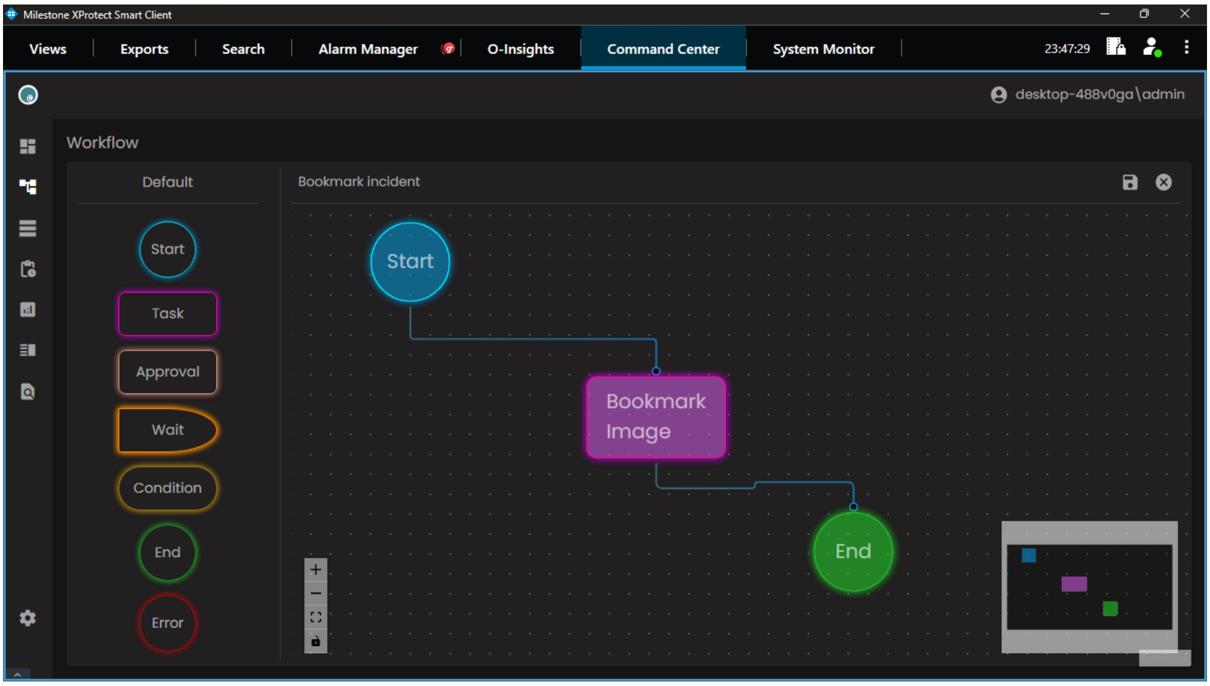
- To edit a node, click on it and modify the parameters or settings in the properties panel that appears on the right.



- To connect nodes, click on the output connector of one node and drag a line to the input connector of another node. Once done, the connected line will turn blue, indicating that the two nodes are now linked together.
    - In the above example, we have the *Start Node* being linked to the *Task Node*. For this workflow to be complete, the *Task Node* should be similarly linked to the *End Node* for a complete workflow.
- Rearrange nodes by clicking and dragging them to new positions on the canvas to better organize the workflow visually.
- Once all modifications are complete, review the workflow to ensure all nodes are properly configured and connected.



- Click on the Save button to apply the changes. If you wish to discard changes, select the Cancel button instead.

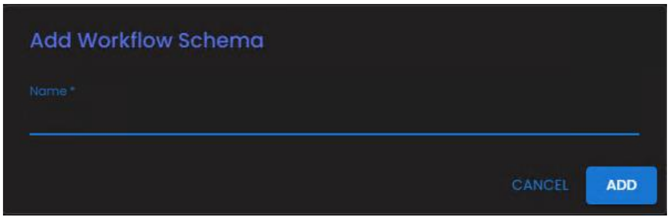


An instance of a created Workflow for Bookmarking Image

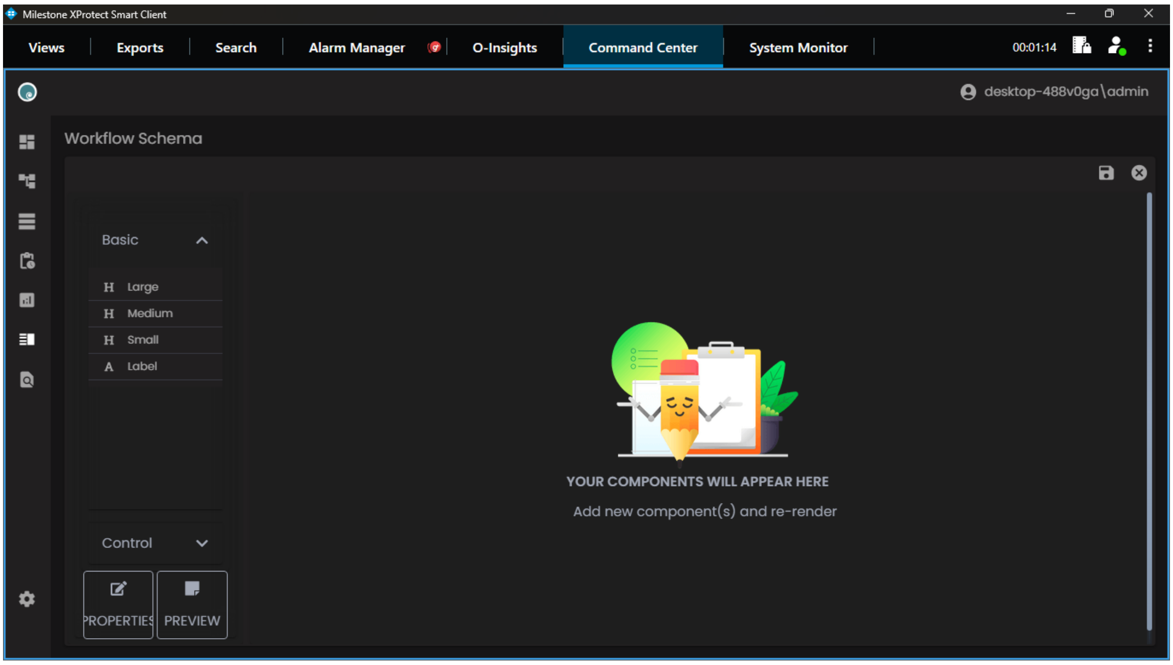
Building Forms with Workflow Schema

The **Workflow Schema** feature in the Form Viewer allows users to design dynamic inputs that are essential for capturing information during incident management processes. Here's how you can create and configure a workflow schema:

- **Initiate Schema Creation**: Click on the *ADD SCHEMA* button, prominently displayed in the interface. This action will prompt you to name your schema.



- **Name Your Schema**: Enter a descriptive name for your schema in the **Name*** field and click on the **ADD** icon to proceed.



- **Access Schema Settings**: Once added, your new schema will appear under the **Workflow Schema** section on the left side of your screen. To modify your schema, click on the **Edit** button located in the right corner of the schema listing.
- **Configure the Schema**: In the schema configuration window, you can add various fields necessary for your form. Utilize the options under *Basic* and *Control* to insert the required fields.

- **Save Your Changes:** After adding and arranging your fields as needed, click on the *Save Changes* icon located in the right corner to finalize your schema.

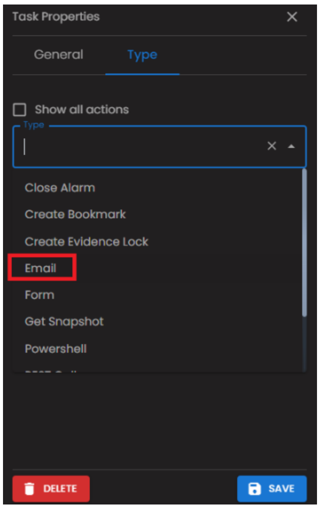
Command Center Tasks

The Command Center Task is an advanced functionality designed to integrate and automate a variety of tasks within workflows. Each task can be added by dragging a *Task Node* to the workflow and configuring the *Type* of the node.

The tasks, their function and operations are detailed below.

Email

The *Email node* within the workflow serves as a customizable communication tool that automates the process of sending tailored emails directly from the workflow.



- **Open Task Properties:**
  - Navigate to the Task Properties box within the Task block added.
  - Under the *General* tab, input the desired name and description for the Email task in the *Name** and *Description* fields.
- **Type Configuration:**
  - Switch to the **Type** tab.
  - Select *Email* from the dropdown menu.

    - In the *Type Name** field, enter a specific name for this email configuration.

- **Input Parameters**:
    - **To**: Enter the email addresses of the recipients. Multiple addresses can be separated by commas.
    - **CC**: Optionally, add email addresses for carbon copy recipients. Supports multiple addresses separated by commas.
    - **Subject**: Write the subject of the email.
    - **Body**: Compose the body of the email. The body field supports the use of special expressions to include dynamic content.

- **Outputs:**
    - **Success**: Outputs *{Result: Email Sent}* upon successfully sending the email.
    - **Failure**: Error message detailing the reason for the email sending failure.

- **Save Configuration**:
    - Click on the **SAVE** button to apply and save the email task configuration.

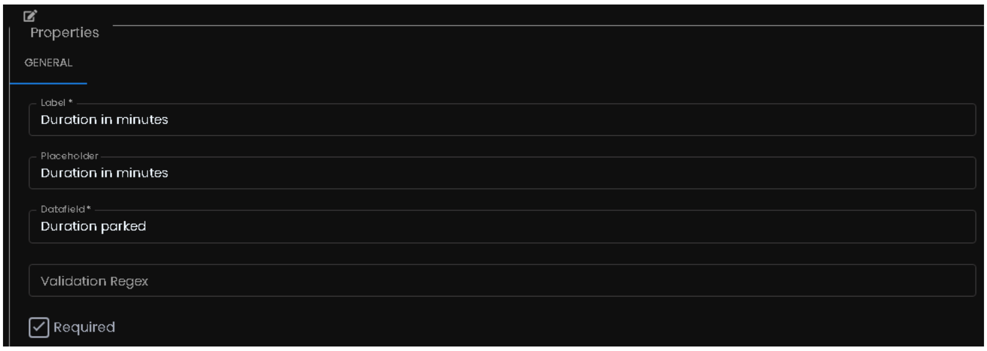
Form

The **Form Node** facilitates the creation and use of customizable forms within a workflow, allowing for detailed manual input from users.

Form Properties

- The **Label** field is the display name shown in the form.
- The **Datafield** is the ID of the form element used in the expression for the Condition block.

  For eg:



Properties

GENERAL

Label * Duration in minutes

Placeholder Duration in minutes

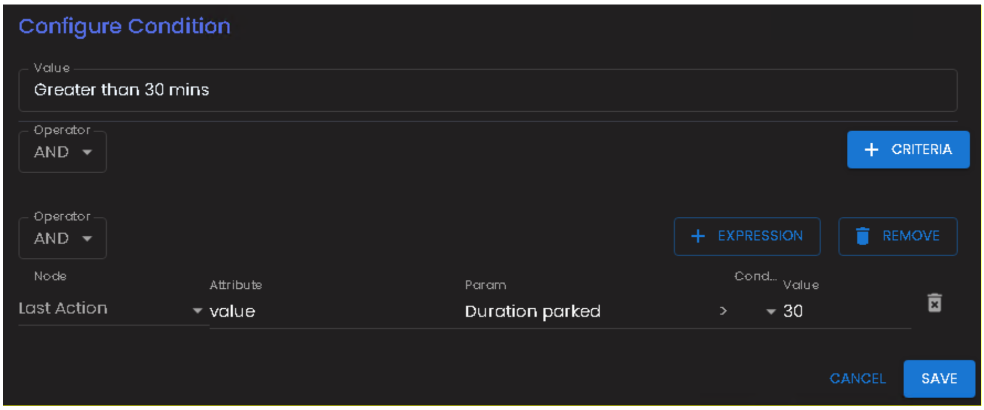
Datafield * Duration parked

Validation Regex

☑ Required

In this instance, the condition will be,

LAST_ACTION.value.Duration parked > 30



Configure Condition

Value: Greater than 30 mins

Operator: AND

Operator: AND

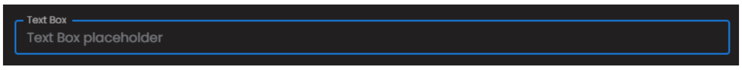
Node	Attribute	Param	Cond...	Value
Last Action	value	Duration parked	>	30

Form Options

Note: Marking a form field as Required by ticking the "Required" checkbox ensures that the field must be filled out by the user in order to successfully complete the form task.

- **User input Control for Forms**

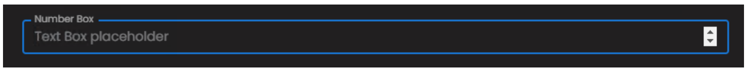
  To enhance your form with control elements, click on the *Control* button, then choose and add various fields from the options provided. This flexibility allows for tailored data collection specific to your needs



Text Box

Text Box placeholder

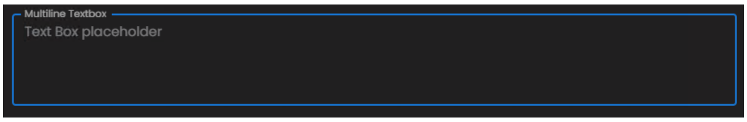
  - *Text Box*: Ideal for single-line input.



Number Box

Text Box placeholder

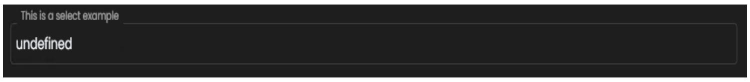
  - *Number*: Features increment and decrement buttons for numerical data.



Multiline Textbox

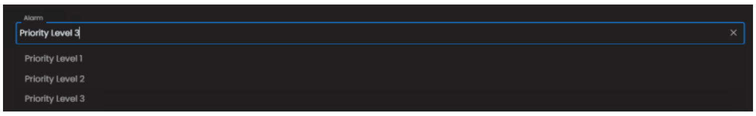
Text Box placeholder

  - *Multiline*: Suitable for longer, sentence-level input.



This is a select example

undefined



Alarm

Priority Level 3

Priority Level 1

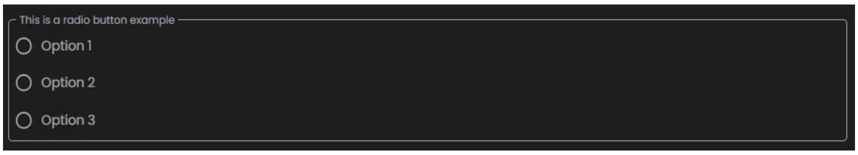
Priority Level 2

Priority Level 3

  - *Select:* The Select form element provides a dropdown menu for users to choose from predefined options within a form. Each option in the dropdown can be assigned a unique value, allowing for varied responses based on user selection. For example, in a scenario involving alarm priorities:
    - Priority Level 1 can be assigned a value of 1,
    - Priority Level 2 a value of 2,
    - Priority Level 3 a value of 3.

Here, the *Label** is added as “Alarm” and *Datafield** as “Priority Level”.

- *Display:* In the **Display box**, you can customize the text to be shown next to a form field while filling out the form. This allows you to provide clear labels or instructions, and you can also assign values to these fields as per your requirement.

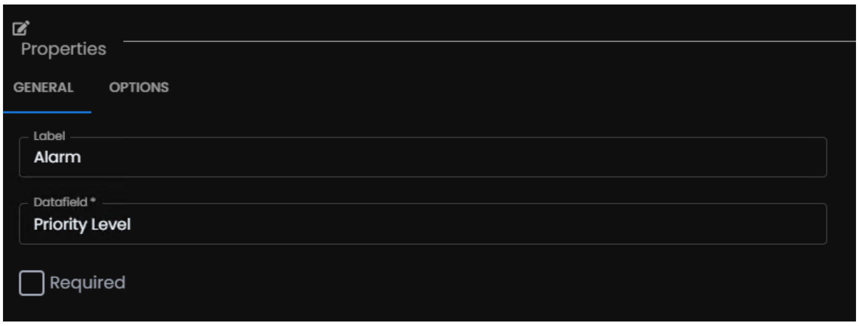


This is a radio button example

○ Option 1

○ Option 2

○ Option 3

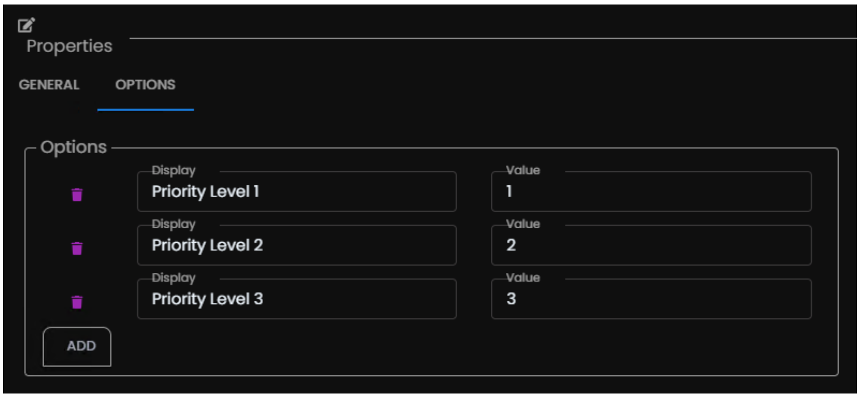


Properties

Label: Alarm

Datafield *: Priority Level

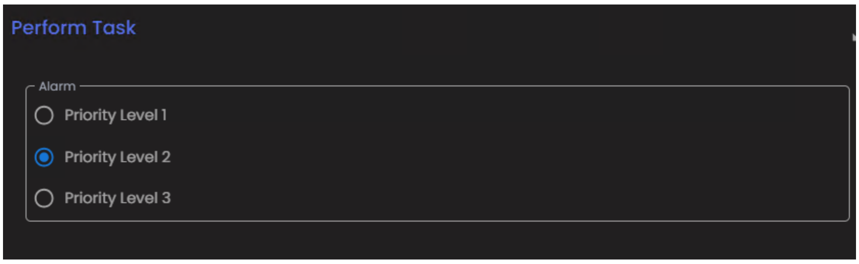
□ Required



Properties

Options

Display	Value
Priority Level 1	1
Priority Level 2	2
Priority Level 3	3



Perform Task

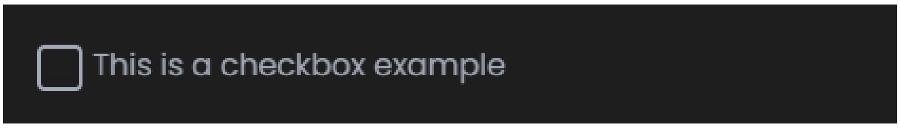
Alarm

○ Priority Level 1

● Priority Level 2

○ Priority Level 3

- *Radio:* The radio button option enables users to select one option from multiple available choices. This is similar to the *Select* option, with a different UI element.



□ This is a checkbox example

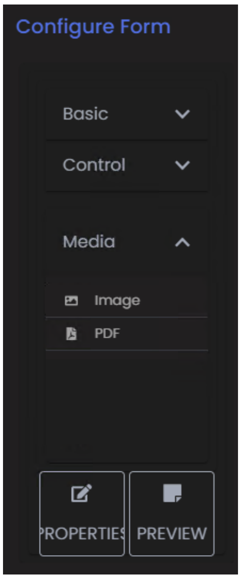
- *Checkbox:* This form element allows users to add checkboxes that can be checked off during the filling of the form. This is useful for confirming statements or choosing multiple options without restrictions.

- *Calendar:* This tool integrates a calendar into the form, allowing users to easily select the current date, which can be particularly useful for logging entry dates and times.

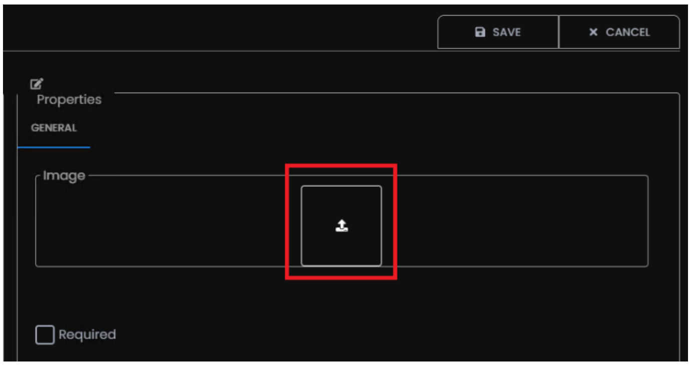
- *Date Time:* Enhances form capabilities by allowing users to add and adjust date and time entries. This is essential for forms requiring precise time stamping.

- **Media Controls**

  This feature allows for the attachment of images and PDFs directly within the form, supporting file formats such as .jpg, .jpeg, and .png for images.



  - To add an image attach form, click on the image icon to bring up an empty image box.



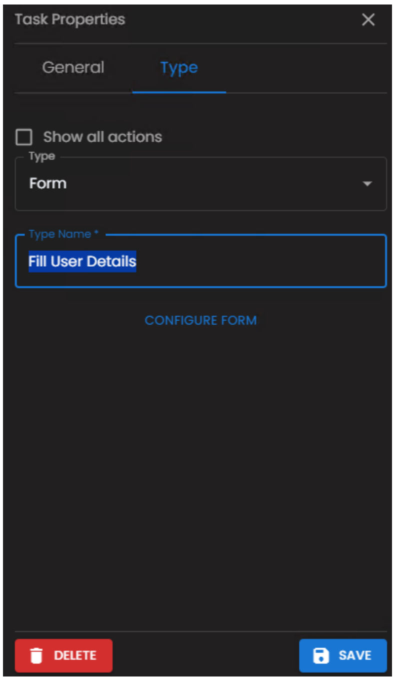
- Click the edit icon to open the Properties box, then click the red bordered icon, enter the file name, and click *Open*.
- Finally, click the *SAVE* icon followed by the blue *SAVE* button to confirm.
- Click the PDF icon and repeat these steps, in case a PDF attach form is to be added.

Example of a Form based Workflow

In this example, we will consider creating a workflow called "Fill User Details".

- **Link Nodes:**
  - Add **Start Node** and **End Node** to the workflow canvas if they are not already present.
  - Link these nodes to the Form (Task Node) to establish the workflow sequence. The Start Node initiates the workflow, leading directly to the Form, and upon completion, the workflow proceeds to the End Node, marking the workflow's conclusion.
- **Open Task Properties:**
  - Navigate to the Task Properties box within the Task block added.
  - Under the *General* tab, input the desired name (in this case "Fill User Details") and description for the Email task in the *Name** and *Description* fields.
  - This will display the name of the form as shown in the image below. You can add Description, assign Roles and Users to this form and click on the *SAVE* button

- **Type Selection:**



Task Properties

□ Show all actions

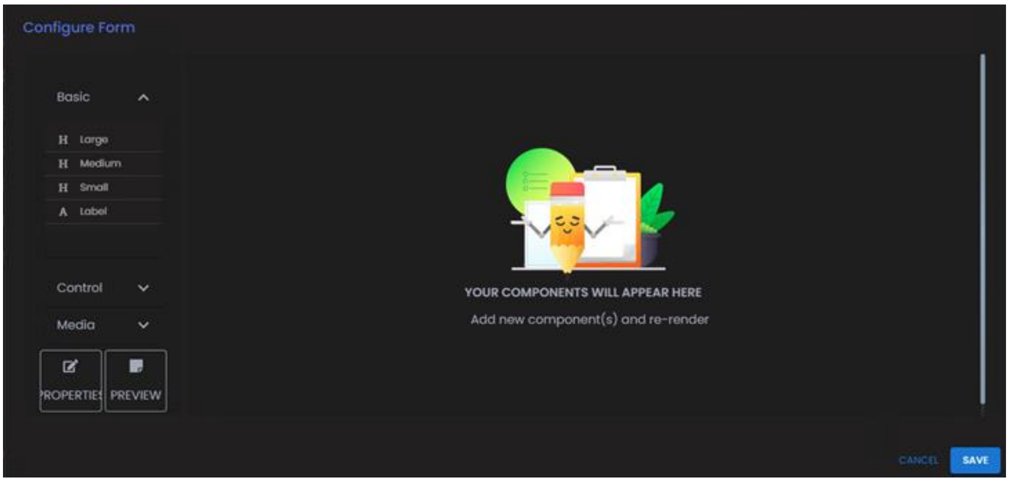
Type: Form

Type Name *: Fill User Details

  - Switch to the **Type** tab.
  - Select *Form* from the Type dropdown to specify the task type as a form.

- **Form Configuration:**
  - Click *CONFIGURE FORM* to open the form configuration window, as shown above. This allows you to add various elements to the form based on your requirements.

- **Adding Headers:**

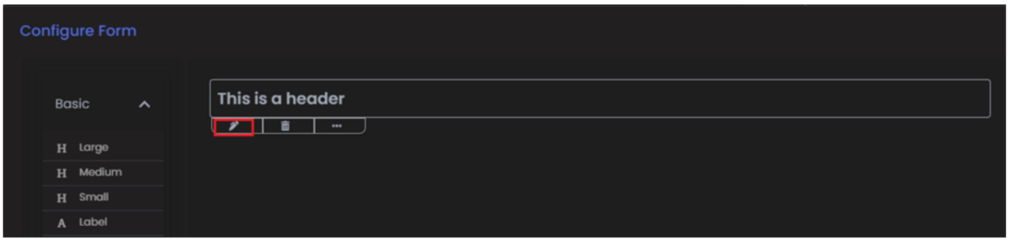


Configure Form

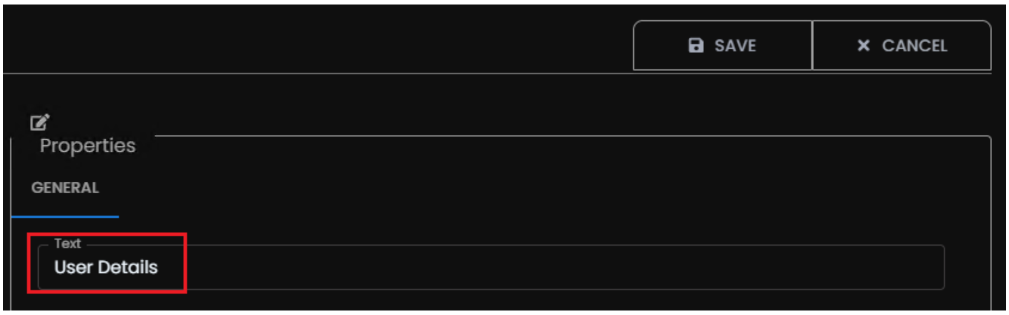
YOUR COMPONENTS WILL APPEAR HERE

Add new component(s) and re-render

- Under the *Basic* options, select a header size (Large, Medium, Small, or Label).

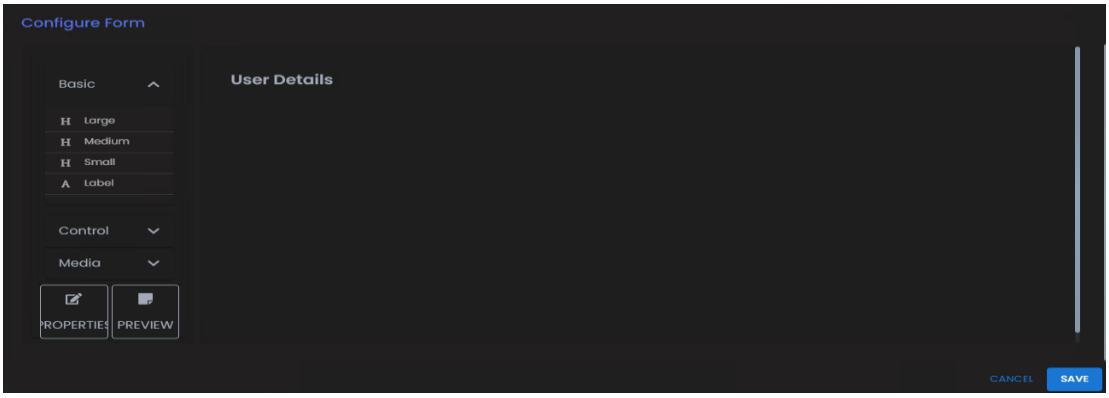


This is a header



Text: User Details

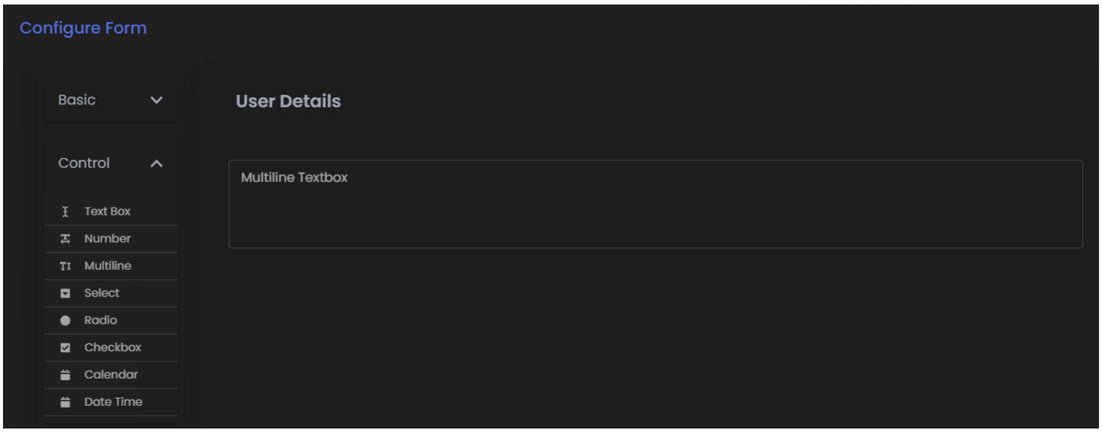
- Hover the mouse over the text field and choose the edit symbol to customize the header and field labels. In this example, "User Details" is added as the header.



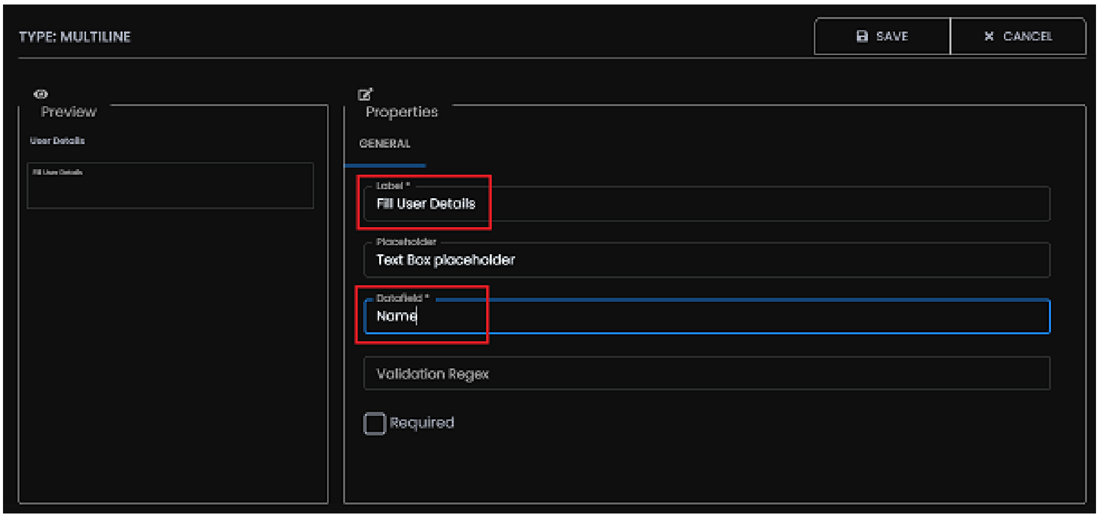
User Details

- Once done, click on the *Save* button. The header will be saved as displayed as shown above.

- **Adding Multiline Text Input Field:**



- Expand to the *Control* section within the form configuration interface and select the *Multiline* option to add a multiline textbox to the form.
- Hover over the multiline textbox and click on the edit symbol to open its settings.



TYPE: MULTILINE

User Details

Fill User Details

Label * Fill User Details

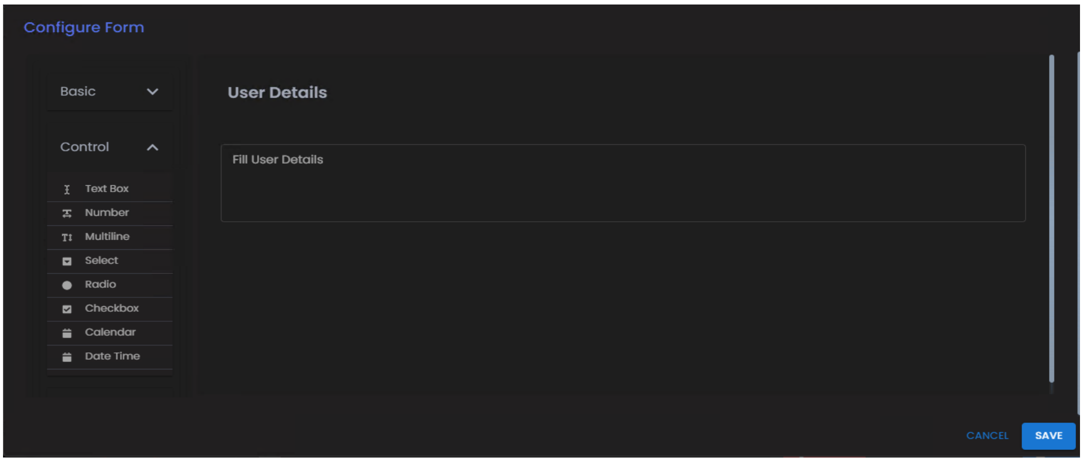
Placeholder Text Box placeholder

Datafield * Name

Validation Regex

□ Required

- In the *Label* field, type "Fill User Details" to specify what information the user should enter.
- In the *Datafield* box, enter "Name" to define the expected input for this textbox.

- 

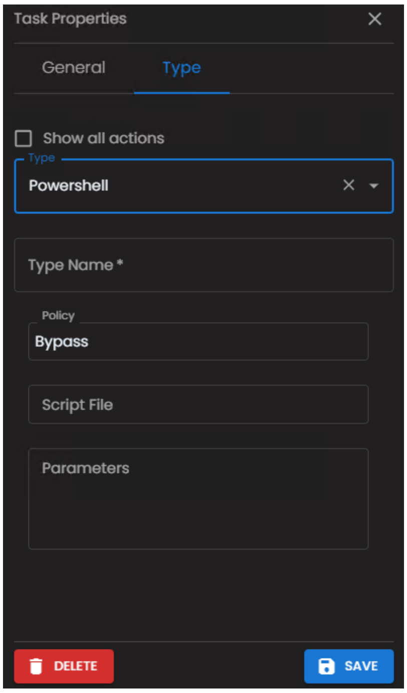
User Details

Fill User Details

- Once done, the field will be added and configured, as shown above. Click on *SAVE* button once done.

2. **Save the Textbox Configuration:**
    - Click the *Save* button to confirm and apply the settings to the multiline textbox. Ensure the settings are correctly displayed as configured.

PowerShell



Task Properties

General | Type

□ Show all actions

Type: Powershell

Type Name *

Policy: Bypass

Script File

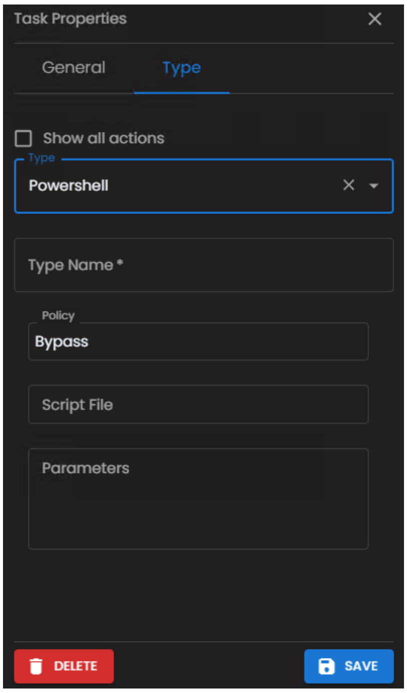
Parameters

The PowerShell task within the Command Center allows users to automate tasks using PowerShell scripts, facilitating complex operations directly from the workflow interface. This task can be configured to execute predefined scripts, handling various automation needs efficiently.

- **General Configuration:** In the Task Properties box under the General tab, enter the desired name and description for the task.
- **Type Configuration:** Navigate to the Type tab and select *'PowerShell'* from the dropdown list. Add the desired type name in the *Type Name* field.
- **Input Parameters Configuration:**
    - **Policy:** Choose the execution policy. This can be left as *Bypass*, which bypasses the policy to prevent scripts from being blocked.
    - **Script File:** Specify the path to the PowerShell script you intend to execute. The path is set under *C:\PowershellScripts\*.
        - For instance, if the script is located at *C:\PowershellScripts\pwscript.ps1*, enter *pwscript.ps1* in the task configuration.
    - **Parameters:** Input any necessary command-line or value parameters.

        - **For e.g., Command Line:** *arg1 arg2, Value param: -arg1key arg1Val*

- **Output:**
    - **Result:** The outcome of the PowerShell script execution is captured in the *Result* parameter. This can be used to determine the success or failure of the script execution.
- **Example:**

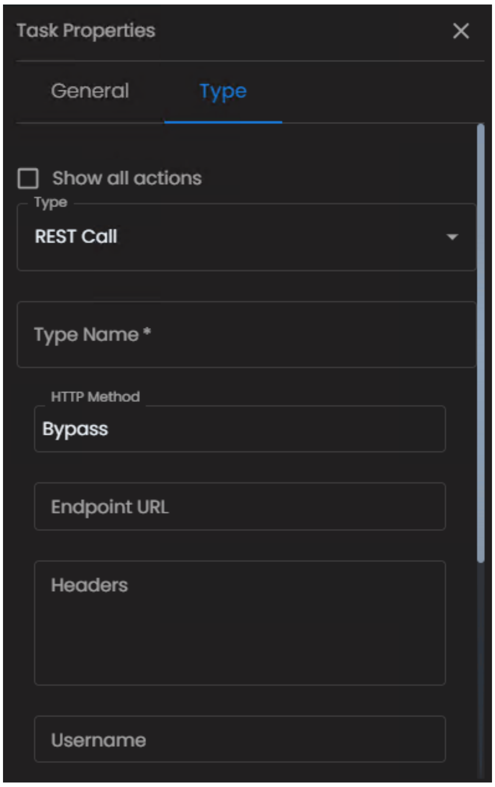


Type: Powershell

Policy: Bypass

    - For example, a PowerShell script named *wait* is configured to pause a workflow for 5 minutes. The setup for this PowerShell task is demonstrated in the above example, showing how the script and its parameters are configured within the Command Center.

REST Call



Task Properties

General | Type

□ Show all actions

Type: REST Call

Type Name *

HTTP Method: Bypass

Endpoint URL

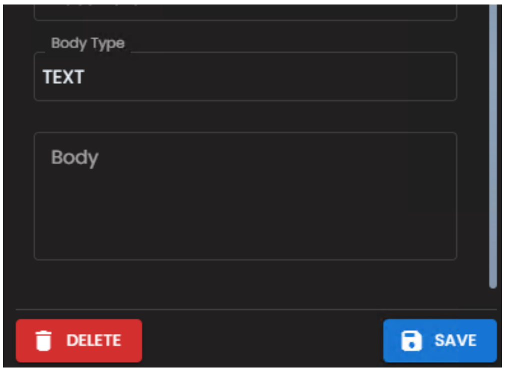
Headers

Username

The *REST Call* task in the Command Center allows users to integrate and automate interactions with external APIs directly within workflows. This functionality facilitates seamless communication between the Command Center and other systems via RESTful APIs, enhancing the automation capabilities of the platform.

- **General Configuration:** In the Task Properties box under the General tab, enter the desired name and description for the task.
- **Type Configuration:** Navigate to the Type tab and select *REST Call* from the dropdown list. Add the desired type name in the *Type Name* field. Add the necessary configurations and click *Save* to save or *Delete* to remove the task.
- **Input Parameters Configuration:**
    - **HTTP Method:** Specify the HTTP method to be used (GET, POST, PUT, DELETE), indicating the action to be performed on the resource.
    - **Endpoint URL:** Enter the URL of the API endpoint where the request will be sent.
    - **Headers:** Provide any necessary headers as a stringified JSON object, as required by the API.

- **Username and Password:** If basic authentication is needed, input the username and password.



Body Type

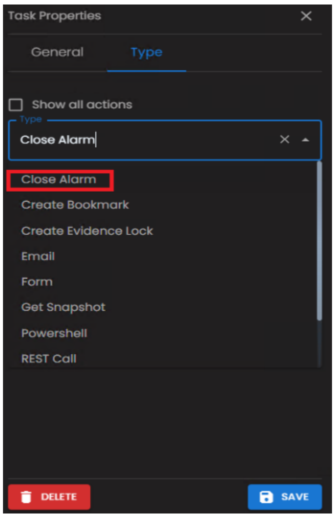
TEXT

Body

- **Body Type:** Select the format of the body data (typically *JSON* or *text*).
- **Body:** Enter the actual data to be sent to the API, formatted as a stringified JSON or text, depending on the *Body Type* specified.

- **Output:**
  - **Result:** The output from the API call will be stored in the *Value* parameter, which captures the API response data.

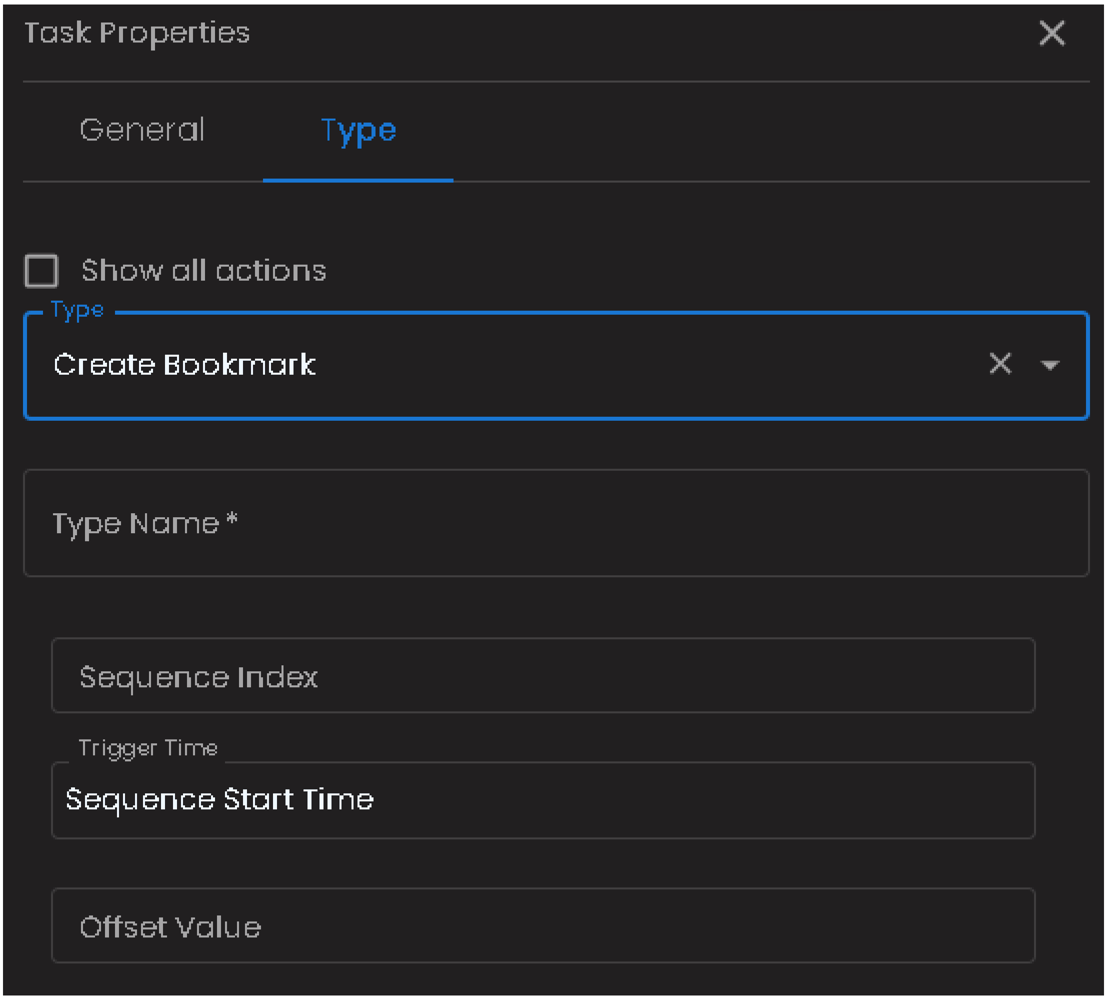
Close Alarm



The *Close Alarm* task in the Command Center allows users to automatically close alarms within the workflow. This can be used in automated processes where alarms need to be managed without manual intervention.

- **General Configuration**: In the Task Properties box under the General tab, enter the desired name and description for the task.
- **Type Configuration**: Navigate to the Type tab and select *Close Alarm* from the dropdown list. Add the desired type name in the Type Name field and click Save to save or Delete to remove the task.
- **Input Parameters**: There is no input parameters required for this task.
- **Output**: The task will close the alarm based on the *AlarmId* specified in the incident details from the Alarm Manager tab.

Create Bookmark



Task Properties

General | Type

□ Show all actions

Type: Create Bookmark

Type Name *

Sequence Index

Trigger Time: Sequence Start Time

Offset Value

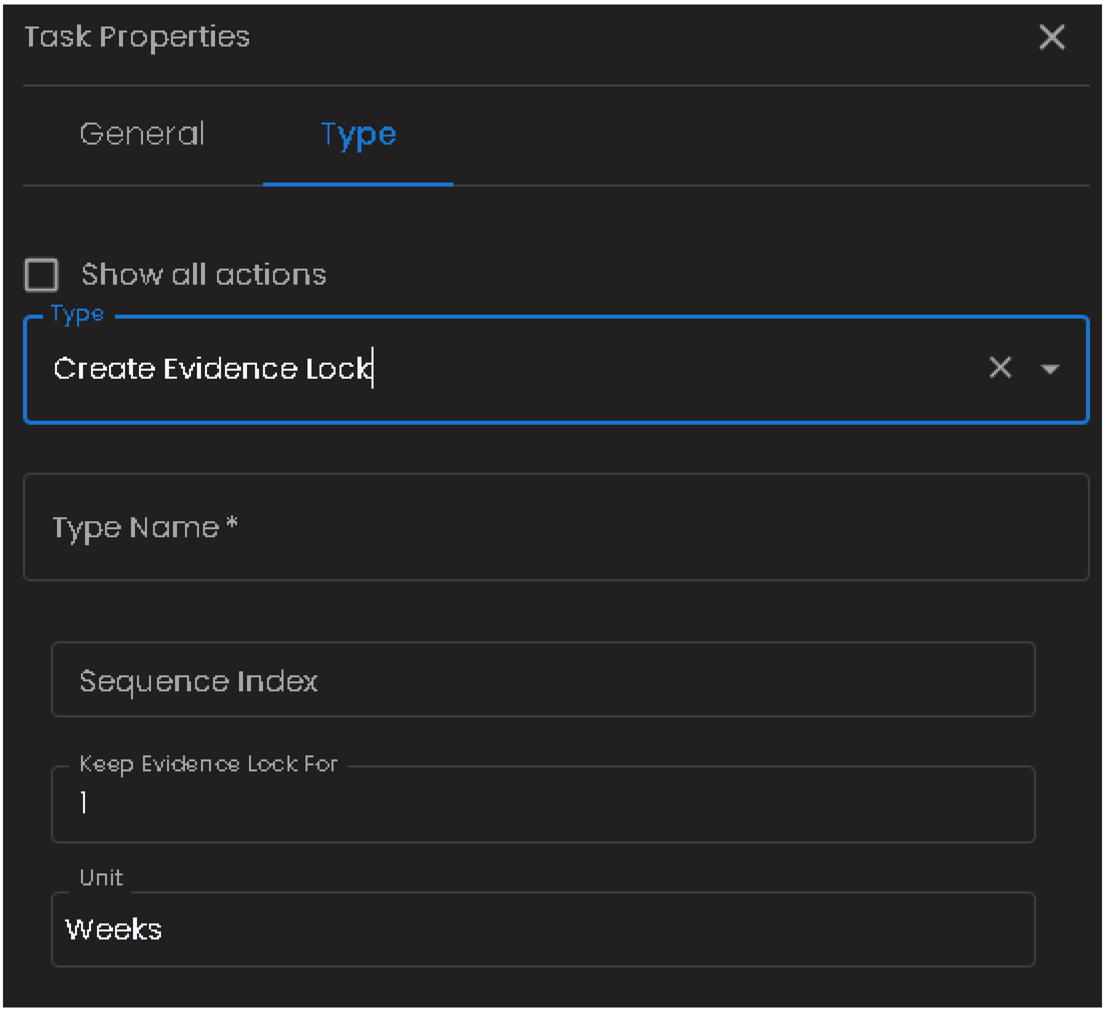
The *Create Bookmark* task in the Command Center is designed to facilitate creating Bookmarks in video feeds automatically during a workflow process. This can help in highlighting significant security events or observations without manual intervention.

- **General Configuration**: In the Task Properties box under the General tab, enter the desired name and description for the task.
- **Type Configuration**: Navigate to the Type tab and select *Create Bookmark* from the dropdown list. Add the desired type name in the Type Name field and click Save to save or Delete to remove the task.
- **Input Parameters**:
    - **Sequence Index**: Specify which camera from the sequence list should be used, with the default set to the first index.
    - **Trigger Time**: Set the specific time at which the bookmark should be created.

    - **Offset Value**: Optional parameter to adjust the Trigger Time, useful for syncing with event timings.

- **Output**:
    - Successfully executes to create a bookmark at the designated time and camera sequence in XProtect, marking important events automatically.

Create Evidence Lock



Task Properties

General Type

□ Show all actions

Type: Create Evidence Lock

Type Name *

Sequence Index

Keep Evidence Lock For: 1

Unit: Weeks

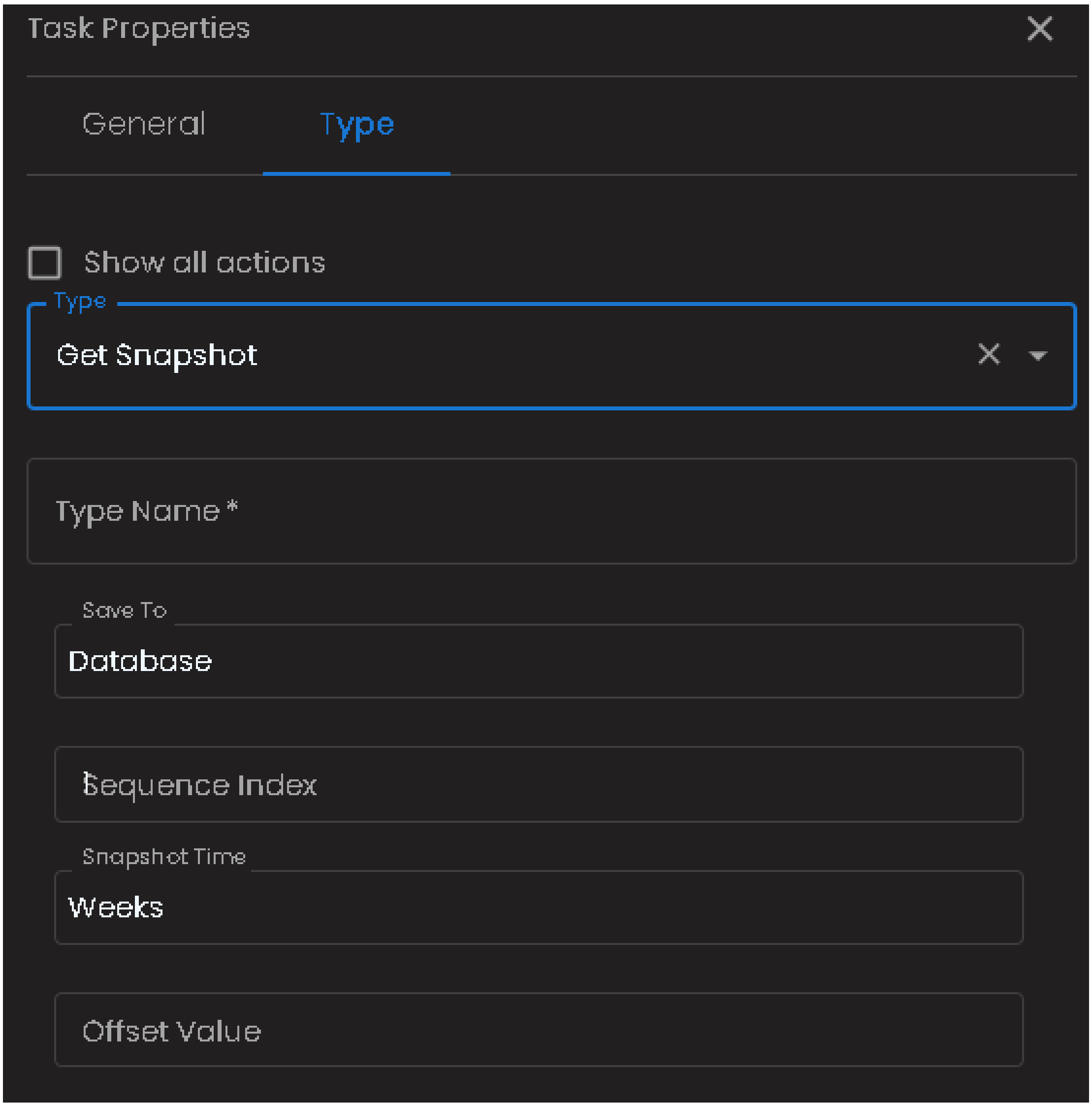
The *Create Evidence Lock* task is designed to create evidence locks automatically, ensuring that critical evidence is preserved.

- **General Configuration**: In the Task Properties box under the General tab, enter the desired name and description for the task.
- **Type Configuration**: Navigate to the Type tab and select *Create Evidence Lock* from the dropdown list. Add the desired type name in the Type Name field and click Save to save or Delete to remove the task.
- **Input Parameters:**
    - **Sequence Index**: Indicate which camera's footage is to be evidence locked, with the default being the first camera.
    - **Keep the Evidence Lock**: Specify how long the evidence lock should be in effect.

    - **Unit**: Choose the unit of time for the evidence lock expiration (*Days*, *Weeks*, *Months*, *Years*, or *Indefinite*).

- **Output**:
    - **Creates an evidence lock** on the selected camera's footage within XProtect, safeguarding critical video evidence for the specified duration.

Get Snapshot



Task Properties

□ Show all actions

Type: Get Snapshot

Type Name *

Save To: Database

Sequence Index

Snapshot Time: Weeks

Offset Value

The *Get Snapshot* task facilitates capturing a snapshot from a specified camera, automating the process of obtaining crucial visual evidence directly from the video feed in XProtect.

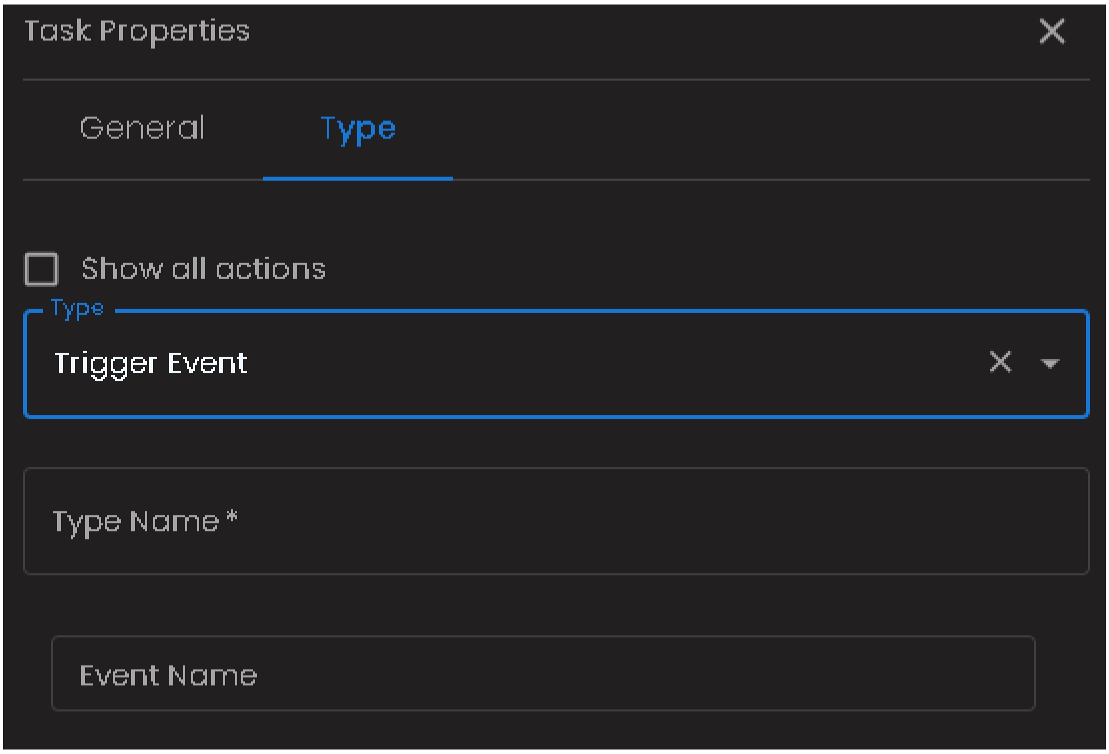
- **General Configuration**: In the Task Properties box under the General tab, enter the desired name and description for the task.
- **Type Configuration**: Navigate to the Type tab and select *Get Snapshot* from the dropdown list. Add the desired type name in the Type Name field and click Save to save or Delete to remove the task.
- **Input Parameters:**

    - **Save to**: Determine the storage location for the snapshot. You can choose to save it to a predefined folder path or directly into the database for integrated management.
        - **Folder**: If selected, specify the file path where the snapshot will be saved, typically set to *C:\IncidentManager* as per configuration in the .env file of the plugin.
        - **Database**: If selected, the snapshot will be stored exclusively within the database, ensuring centralized access.
    - **Sequence Index**: Select which camera's feed to capture the snapshot from, default being the first camera in the sequence.
    - **Snapshot Time**: The exact moment for the snapshot to be captured.
    - **Offset Value**: Optional parameter to adjust/offset the Snapshot Time, providing flexibility in timing the capture.

Output:

- The task will capture a snapshot from the designated camera at the specified time and store the image in the chosen location, either on a local server or within a database, depending on the configuration.

Trigger Event



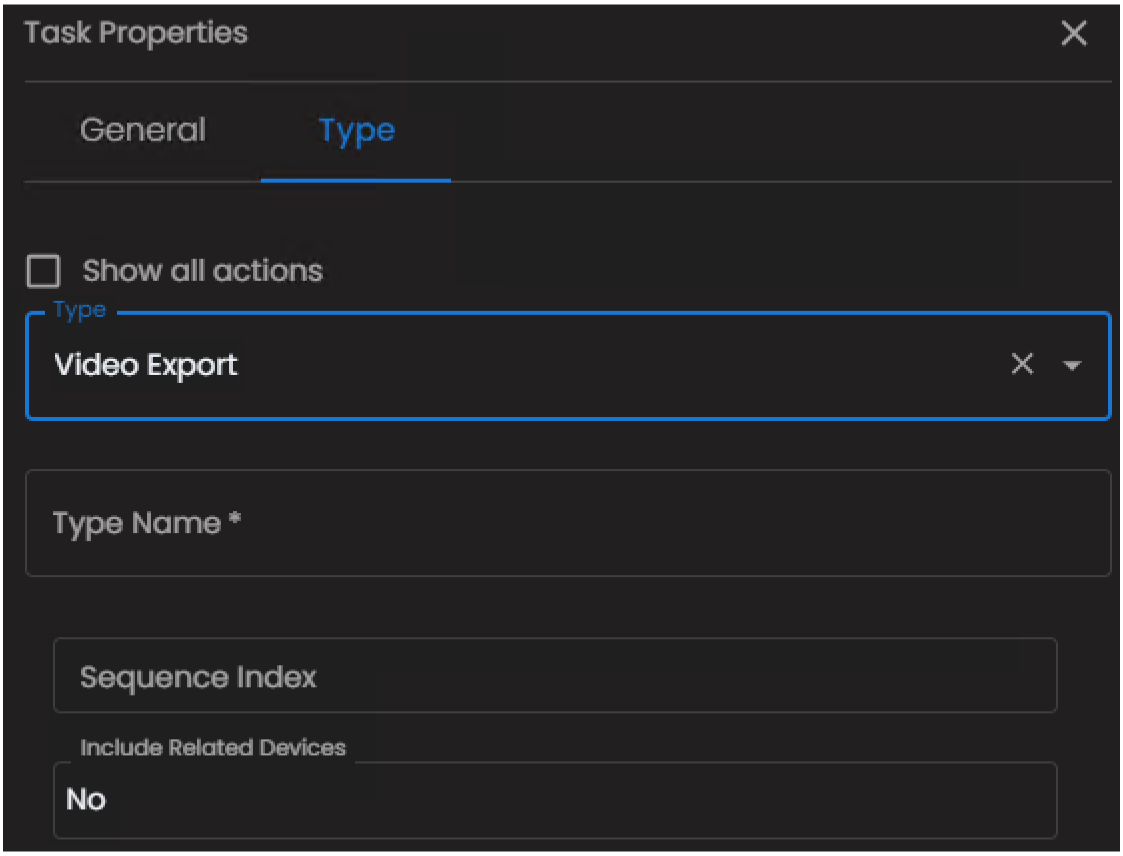
□ Show all actions

Type: Trigger Event

The *Trigger Event* task is designed to initiate specific actions or alerts within the XProtect environment, allowing for dynamic response to varying operational conditions.

- **General Configuration**: In the Task Properties box under the General tab, enter the desired name and description for the task.
- **Type Configuration**: Navigate to the Type tab and select *Trigger Event* from the dropdown list. Add the desired type name in the Type Name field and click Save to save or Delete to remove the task.
- **Input Parameters:**
  - **Event Name**: Specify the exact name of the user defined event within XProtect that this task will trigger. The name must match an event configured in XProtect to ensure proper execution.
- **Output:**
  - The task will trigger the specified event in XProtect, activating any associated alarms, recording actions, or notifications linked to that event.

Video Export



Task Properties

General | Type

□ Show all actions

Type: Video Export

Type Name *

Sequence Index

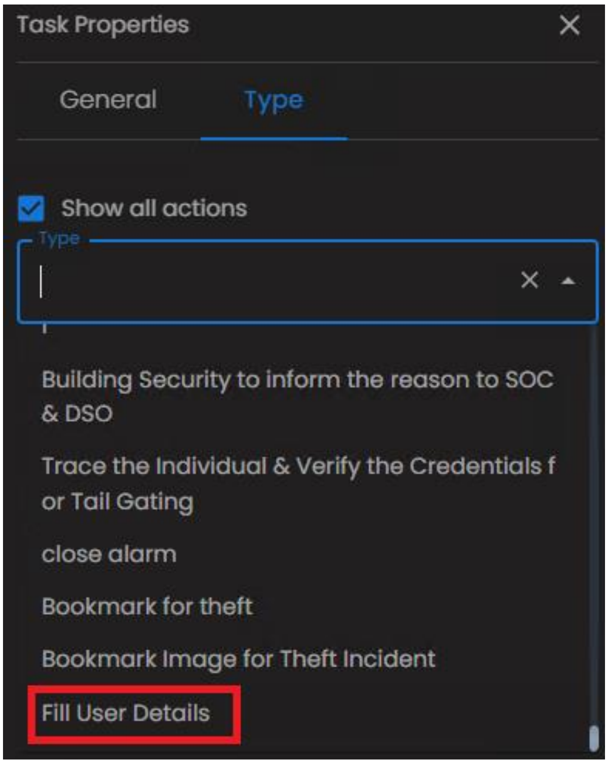
Include Related Devices: No

The *Video Export* task is essential for archiving and sharing video footage from surveillance cameras. This task allows to selectively export video sequences, helping incident investigations and compliance with data retention policies.

- **General Configuration**: In the Task Properties box under the General tab, enter the desired name and description for the task.
- **Type Configuration**: Navigate to the Type tab and select *Video Export* from the dropdown list. Add the desired type name in the Type Name field and click Save to save or Delete to remove the task.
- **Input Parameters:**
  - **Sequence Index**: Specify the index number of the camera from the sequence list whose video you wish to export. If left as default, the first camera in the sequence is selected.
  - **Include Related Devices**: Toggle this option to 'Yes' to include audio or other related data streams from devices linked to the selected camera, enhancing the export's comprehensiveness.

- **Output:**
    - The task processes the export of the designated camera sequence, incorporating any related devices if specified. The resulting video file is stored at the predefined path in the .env file (*C:\IncidentManager* by default), making it accessible for review or further action.

Reusing Tasks in another Workflow



Task Properties

General | Type

☑ Show all actions

Type

Building Security to inform the reason to SOC & DSO

Trace the Individual & Verify the Credentials f or Tail Gating

close alarm

Bookmark for theft

Bookmark Image for Theft Incident

Fill User Details

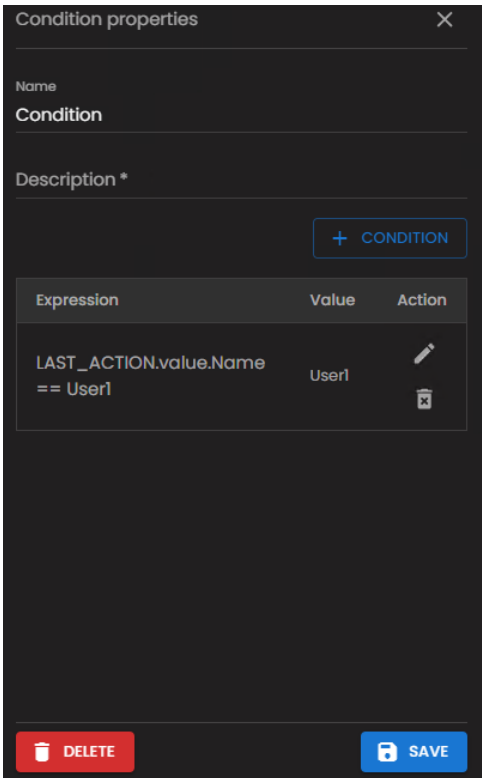
When setting up Task Nodes within a workflow, there's an option in the Task Properties to *Show all actions.* This feature is particularly useful for creating reusable tasks. For instance, if you create a form task named "Fill User Details" and enable *Show all actions* this form becomes available for reuse in other workflows.

Once enabled, the form will appear in the Type dropdown when configuring other Task Nodes, making it easy to integrate into new workflows without having to recreate the same form.

This is visually indicated in the workflow editor with a form icon highlighted with a red border, suggesting its reusable status.

Using Expressions

Expressions in workflows are built using form data to evaluate conditions that dictate the subsequent path of the workflow. These expressions are structured with three components: *Node*, *Attribute*, and *Parameters*. This structure allows for dynamic decision-making within a workflow based on user inputs or other actions.



Name
Condition

Description *

Expression	Value	Action
LAST_ACTION.value.Name == User1	User1	✎ 🗑

Expressions can be added to the workflow using the *Condition* node. Once the Condition node is added, add the name in the *Name* field, add the description in the *Description* field. Once done, add the condition by clicking on the *+Condition* button.

You may click on the edit icon to modify the condition or delete icon to delete.

Using Data to Construct Expressions in Workflows

- **Node**: Refers to the specific action in the workflow.
- **Attribute**: Pertains to the attribute of the parameter that is evaluated in the expression.
- **Parameters**: These are specific data points from forms or other inputs that are used in the expression.

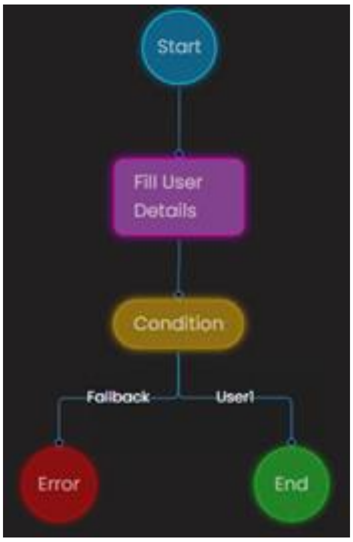
Using Last Action

The Last_Action node represents the last action executed within the workflow.

[DataField] is the form field property that can be used in the expression.

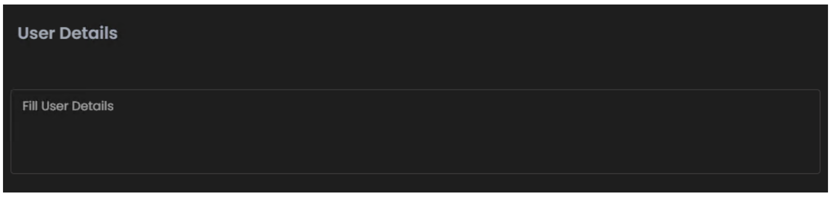
Node	Attribute	Parameters
Last Action	Value	[DataField]

- **Expression Example:** *LAST_ACTION.value.[DataField*]
    - Here, *LAST_ACTION* denotes the most recent action taken, and *value.[DataField]* specifies the value of a particular data field in that action.

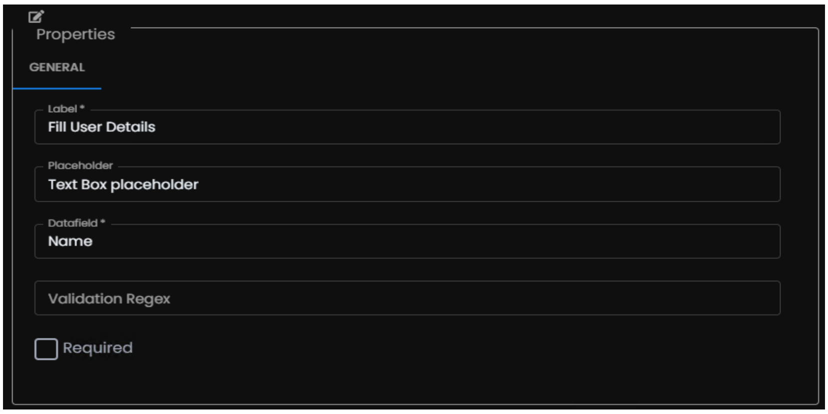


    - As per the above example, if the last form filled was "FillUserDetails" with a field named *Name*, the expression *Last_Action.value.Name* equates to the value entered in the "Name" field.

- **Example of Configuring a Condition Based on Last Action:**


User Details

Fill User Details



Properties

GENERAL

Label *
Fill User Details

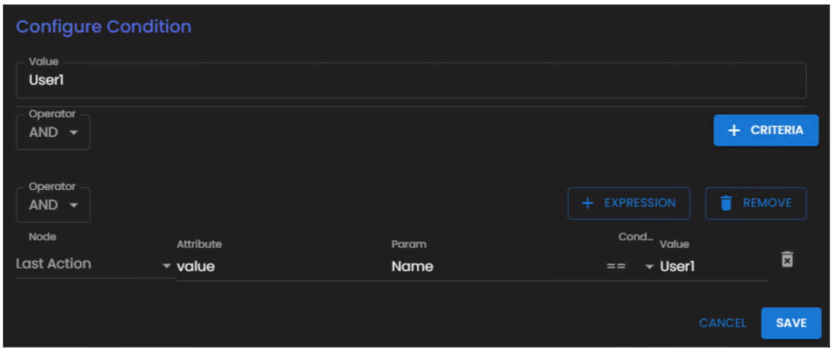
Placeholder
Text Box placeholder

Datafield *
Name

Validation Regex

□ Required

- When setting a condition, when "User1" is entered in the "Fill User Details" form, the workflow can be directed to end successfully. If any other value is entered, it redirects to an error node.
- To set this up, click on the + CONDITION button.



Configure Condition

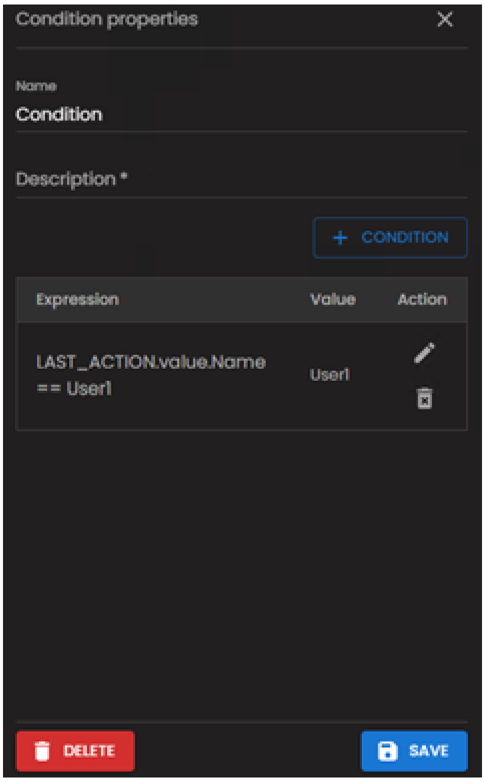
Value
User1

Operator
AND

Operator
AND

Node	Attribute	Param	Cond...	Value
Last Action	value	Name	==	User1

- Then, select *+CRITERIA*, choose *AND* as the operator, and enter *User1* in the value field.
- If multiple expressions are necessary, additional expressions can be added using the *EXPRESSION* button, then save the changes.



Name
Condition

Description *

Expression	Value	Action
LAST_ACTION.value.Name == User1	User1	

   - The configured expression will appear in the Condition properties tab, and you can save to finalize.

Using Last Action

The *ALL_ACTIONS* node allows referencing any action within the workflow.

[Action Name] specifies the particular action to reference, and *value.[DataField]* is the value within a specified data field from that action.

Node	Attribute	Parameter
All Action	[Action Name]	value.[DataField]

- **Expression Example:** *ALL_ACTIONS.[Action Name].value.[DataField*]
   - For instance, in a form named "FillUserDetails" that includes a field "Name", the expression *ALL_ACTIONS.FillUserDetails.value.Name* checks the value entered in the "Name" field.

Using Data to Construct Expressions in Workflows

Task data in workflows can be used for constructing expressions that determine the flow's progression. These expressions are structured into three key components:

- **Node**: Refers to the specific action node within the workflow. This is where the action originates or is processed.
- **Attribute**: Pertains to the specific attribute of the node that is relevant for the expression. This might include outcomes like results or status codes.
- **Parameter**: Involves the specific elements of the attribute that are to be assessed or utilized in the condition of the workflow.

Utilizing these elements, workflows can dynamically adapt based on the results of tasks, making them highly responsive and tailored to conditions and outcomes.

Using Last Action

Node	Attribute	Parameters
Last Action	result	data code

- **LAST_ACTION.result.data**: This expression is commonly used to check the output of a PowerShell script or a REST API call that was the most recent action in the workflow. To access specific data from this action, the expression *LAST_ACTION.result.data.value== is* used, where you can specify the expected value right after the double equals sign.
- **LAST_ACTION.result.code**: This expression evaluates the exit code of the most recent action, which is crucial for determining its success or failure. A typical use includes:
    - *LAST_ACTION.result.code == 0* indicates that the action executed successfully without errors.
    - *LAST_ACTION.result.code == 1* indicates that the action failed and returned an error.

Using All Actions

Node	Attribute	Parameter
All Action	[Action Name]	result.data result.code

- **ALL_ACTIONS.[Action Name].result**: This expression is particularly useful for reviewing the outcomes of actions such as PowerShell scripts or REST API calls. For example, the expression *ALL_ACTIONS.RestAPICall.result.data.value==* can be tailored to evaluate specific data points returned by a REST API call, allowing the workflow to proceed based on predefined conditions.
- **ALL_ACTIONS.[Action Name].result.code**: This expression is used to check the execution status of a designated action by its name. It provides a way to ascertain whether a specific task was successful or not:
  - *ALL_ACTIONS.SnapshotTaken.result.code == 0* signifies that the action named *SnapshotTaken* was executed successfully.
  - Conversely, *ALL_ACTIONS.SnapshotTaken.result.code == 1* indicates that the action encountered an error and thus failed.

Using Custom Data to Construct Expressions in Workflows

Expressions based on custom data within an incident can be highly effective for routing workflows or customizing notifications according to specific incident attributes.

Node	Attribute	Parameter
Custom_Data	Entity	[PropertyName]

Below are examples of how to utilize these expressions and include incident data in various workflow tasks like emails and scripts:

Expressions Using Custom Incident Data

- ***PropertyName* in Custom Data:** You can reference custom data fields within an incident. For example, if an incident has a custom property named "Location," you could use it in an expression:
  - *CUSTOM_DATA.ENTITY.Location == 'Goa':* This expression evaluates whether the Location property of the incident equals 'Goa.'

Using Incident Data in Task Parameters

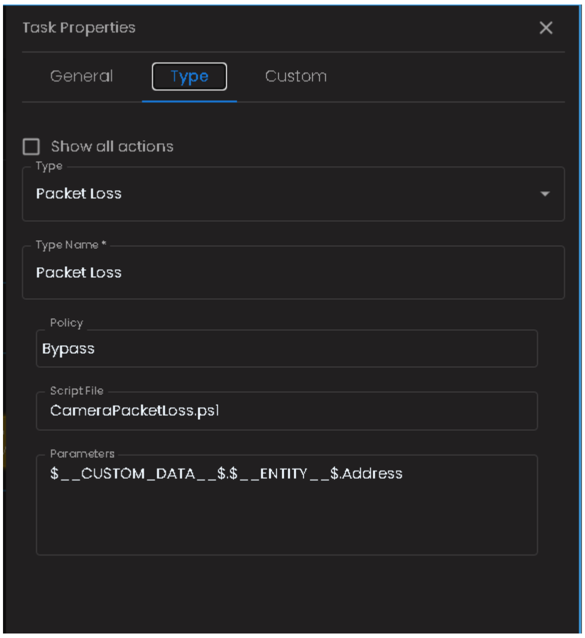
Incident data can be dynamically inserted into tasks like email notifications or PowerShell scripts, allowing for customized responses based on the specifics of the incident:

- **Incident Name**:
  - *$__ENTITY__$.name:* Retrieves the name of the incident to include in task parameters, such as the subject or body of an email.
- **Incident Description**:
  - *$__ENTITY__$.description*: Pulls the description of the incident, useful for detailed notifications or log entries.
- **Incident Creator**:
  - *$__ENTITY__$.created_by*: Identifies who created the incident, which can be crucial for tracing actions.
- **Incident Priority**:
  - *$__ENTITY__$.priority*: Extracts the priority level of the incident, where the possible values are:

- *1* - Low
- *2* - Medium
- *3* - High
- *4* - Critical

Examples

- **Using custom data for PowerShell script argument**



Task Properties

□ Show all actions

Type: Packet Loss

Type Name *: Packet Loss

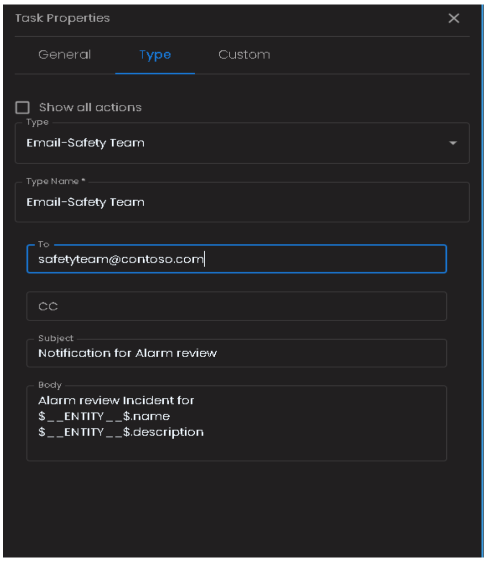
Policy: Bypass

Script File: CameraPacketLoss.ps1

Parameters: $__CUSTOM_DATA__$.$__ENTITY__$.Address

Task Properties

- **Using Incident data in Email Body:**



□ Show all actions

Type: Email-Safety Team

Type Name *: Email-Safety Team

To: safetyteam@contoso.com

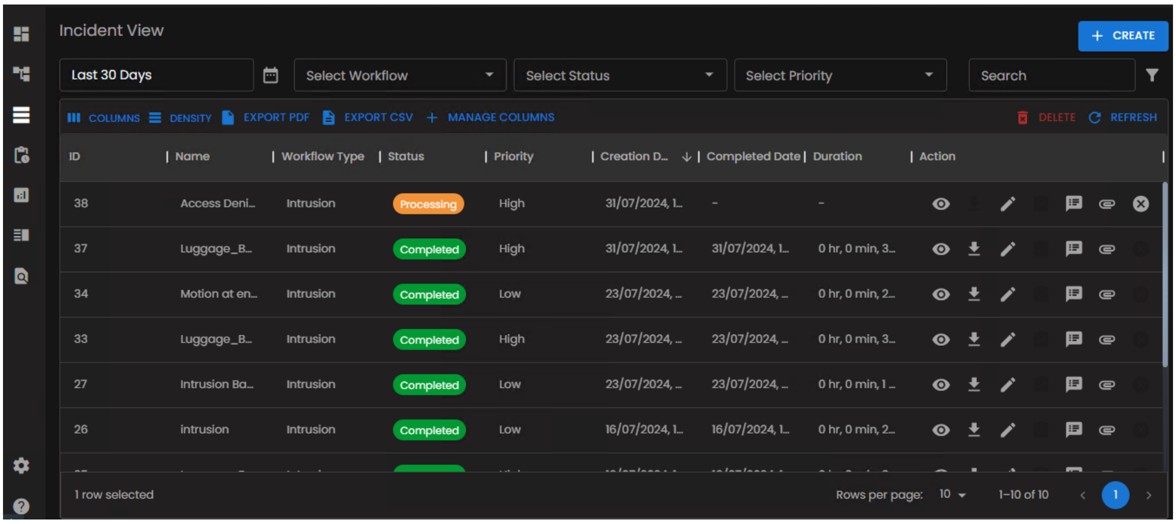
CC

Subject: Notification for Alarm review

Body:
Alarm review Incident for
$__ENTITY__$.name
$__ENTITY__$.description

Task Properties

Incident View



ID	Name	Workflow Type	Status	Priority	Creation D...	Completed Date	Duration	Action
38	Access Deni...	Intrusion	Processing	High	31/07/2024, 1...	-	-	
37	Luggage_B...	Intrusion	Completed	High	31/07/2024, 1...	31/07/2024, 1...	0 hr, 0 min, 3...	
34	Motion at en...	Intrusion	Completed	Low	23/07/2024, ...	23/07/2024, ...	0 hr, 0 min, 2...	
33	Luggage_B...	Intrusion	Completed	High	23/07/2024, ...	23/07/2024, ...	0 hr, 0 min, 3...	
27	Intrusion Ba...	Intrusion	Completed	Low	23/07/2024, ...	23/07/2024, ...	0 hr, 0 min, 1 ...	
26	intrusion	Intrusion	Completed	Low	16/07/2024, 1...	16/07/2024, 1...	0 hr, 0 min, 2...	

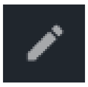
1 row selected Rows per page: 10 1–10 of 10 1

Incident View

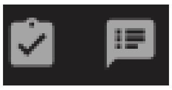
The Incident View provides a comprehensive environment for managing incidents effectively, equipped with various tools for complete incident lifecycle management.

Incident Management Capabilities

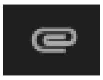
- **Create, Delete, and Update Incidents:** Users can Create, Delete and Update incidents, providing flexibility in managing incident records. These actions can be performed directly from the Incident View tab using the *Create*, *Delete*, and *Update* buttons as shown below.



- **Keeping Comprehensive Records of Incidents:**



  - **Notes**: Add detailed annotations to incidents for clarity and additional information.
  - **Reasons and Outcomes**: Define the reasoning behind decisions and the outcomes of incidents to capture decision-making contexts.



  - **Attachments**: Attach files to incidents for added context and evidence. To manage attachments, click on the Attachments icon. Ensure all relevant details are consolidated and accessible.

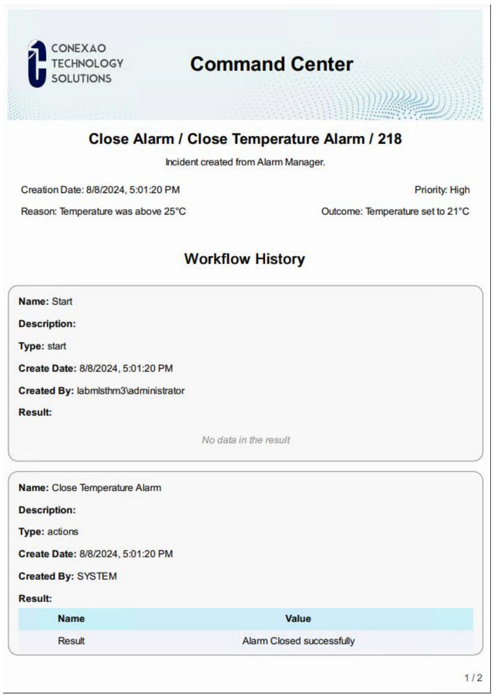
    To manage file types allowed for uploads, modify the *Allowed_Extentions* key in the configuration file located at *C:\Program Files\Milestone\MIPPlugins\O-Insights Command Center\IncidentWorkflows.dll.config* with values such as "pdf, png, jpg, jpeg". The modified key will then look like *<add key="Allowed_Extentions" value="pdf,png,jpg,jpeg" />*

- **Incident Cancellation:**

  - If an incident has to be cancelled/discontinued, click on the cancel icon.

- **Reporting and Analysis:**

  - Downloadable reports provide detailed insights for audits and deeper analysis. Reports include comprehensive data on the workflow, reasons, outcomes, and any notes or attachments associated with the incident.



CONEXAO TECHNOLOGY SOLUTIONS

Command Center

Close Alarm / Close Temperature Alarm / 218

Incident created from Alarm Manager.

Creation Date: 8/8/2024, 5:01:20 PM
Priority: High

Reason: Temperature was above 25°C
Outcome: Temperature set to 21°C

Workflow History

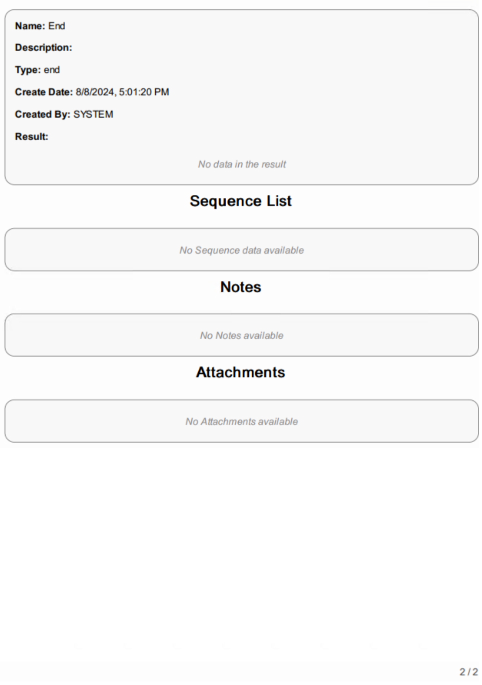
Name: Start
Description:
Type: start
Create Date: 8/8/2024, 5:01:20 PM
Created By: labmlsthm3\administrator
Result:

No data in the result

Name: Close Temperature Alarm
Description:
Type: actions
Create Date: 8/8/2024, 5:01:20 PM
Created By: SYSTEM
Result:

Name	Value
Result	Alarm Closed successfully

1 / 2



Name: End
Description:
Type: end
Create Date: 8/8/2024, 5:01:20 PM
Created By: SYSTEM
Result:

No data in the result

Sequence List

No Sequence data available

Notes

No Notes available

Attachments

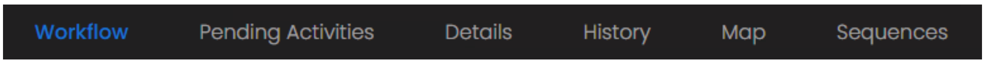
No Attachments available

2 / 2

- The report shown above is for the incident named "Close Temperature Alarm," triggered from the Alarm Manager, it provides a comprehensive overview of the incident's management and resolution. The report includes:
    - **Workflow History**: Each step of the workflow, from start to finish, is documented to show the sequence of actions taken during the incident resolution.
    - **Reason and Outcome**: The report details the rationale behind actions taken and the results of those actions, providing clear accountability and insights into the decision-making process.
    - **Sequence List, Notes, and Attachments**: While not included in this specific incident, the report has the capability to display lists of sequences, notes, and any attachments relevant to the incident, offering a complete view of all associated data.

Detailed Incident Information

- **View Details:** A critical feature that provides an in-depth look into each incident. Clicking the View Details icon (👁) reveals tabs with:

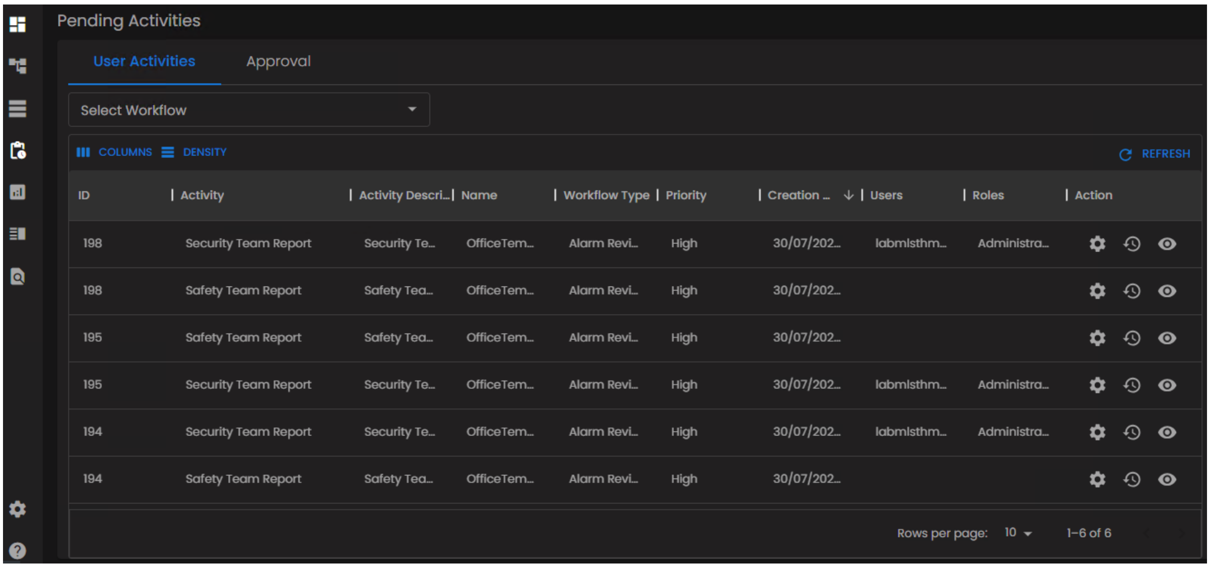


- **Workflow**: Detailed status and progression of the associated workflow.
- **Pending Activities**: Displays all pending activities within the workflow.
- **Details**: Custom tags and specifics of the devices related to the incident.
- **History**: A log of actions taken and the statuses of each workflow node.
- **Map**: Geographic location visualization based on incident coordinates.
- **Sequences**: Attached camera sequences with the ability to add multiple sequences specifying start and end times.

Customizing Incident View

- **Manage Display Columns**: Customize which columns are visible in the Incident View by using the *COLUMNS* icon.
- **Adjust Viewing Density**: Toggle between Compact, Standard, and Comfortable views using the *DENSITY* icon.
- **Column Management**: Add or remove columns via the manage columns icon.
- **Data Export**: Export incident data in PDF or CSV formats for external use or record-keeping.

Pending Activities



ID	Activity	Activity Descri…	Name	Workflow Type	Priority	Creation …	Users	Roles	Action
198	Security Team Report	Security Te…	OfficeTem…	Alarm Revi…	High	30/07/202…	labmlsthm…	Administra…	
198	Safety Team Report	Safety Tea…	OfficeTem…	Alarm Revi…	High	30/07/202…			
195	Safety Team Report	Safety Tea…	OfficeTem…	Alarm Revi…	High	30/07/202…			
195	Security Team Report	Security Te…	OfficeTem…	Alarm Revi…	High	30/07/202…	labmlsthm…	Administra…	
194	Security Team Report	Security Te…	OfficeTem…	Alarm Revi…	High	30/07/202…	labmlsthm…	Administra…	
194	Safety Team Report	Safety Tea…	OfficeTem…	Alarm Revi…	High	30/07/202…			

Rows per page: 10 1–6 of 6

Pending Activities

The **Pending Activities** section helps to streamline the handling of tasks and approvals within an organization. It effectively categorizes pending actions into two main tabs:

- **User Activities**: This tab displays all tasks awaiting user interaction, such as filling out forms. It serves as a centralized place for users to complete manual tasks efficiently.
- **Approval Tab**: Here, you can find tasks that require approval from designated roles or users, ensuring that each action receives the necessary oversight before proceeding.

Tasks Management Features

- **View and Complete Manual Tasks**: Enables users to actively engage with and complete assigned tasks, primarily focusing on manual entries such as form filling.
- **Task Details and History**: Offers in-depth information about each task, including a comprehensive log of all actions taken, which provides context and facilitates better understanding of the task lifecycle.
- **Review Incidents for Completion**: Ensures that incidents requiring specific reasons or outcomes for resolution are highlighted, allowing for proper closure and documentation of each incident.

Task Management

The **Task Management** feature enhances operational efficiency by managing user responsibilities and workflow progression. Key aspects include:

- **User Activities**: This section allows users to view and complete manual tasks, such as form filling. It streamlines the process of managing day-to-day activities, facilitating prompt and organized task completion.
- **Task Details and History**: Users can access detailed descriptions and historical data for each task. This visibility provides critical context and deeper insights into the lifecycle of tasks, aiding in analysis and decision-making.
- **Reviewing Incidents for Completion**: The module enables users to examine incidents requiring specific justifications or outcomes before they can be resolved. This ensures that all incidents are thoroughly vetted and meet all necessary criteria for closure, maintaining a high standard of process integrity and accountability.

Approval Management

Approval Management streamlines the decision-making process within incident handling, ensuring effective governance and oversight:

- **Decision Authority**: You possess the capability to either *Approve* or *Reject* incidents directly, enabling decisive action during incident management processes.
- **Reasons for Decisions**: For each approval or rejection, specific reasons can be noted, thereby enhancing transparency and accountability.
- **Reviewing Approvals**: The system allows for an easy review of approval details and historical data, facilitating a clear understanding of past decisions and their contexts.

- **Notification Configuration**: To support the approval process, email notifications can be configured to alert relevant roles and users. This is managed through modifications in the JSON configuration file located at: *C:\Program Files\O-Insights QueryEngine\Config\CommandCenterUsers.json.*

  Example configuration:

  ```
  {
    "name": "username1",
    "roles": [ "Administrators", "Operator" ],
    "email": "username1@example.com"
  }
  ```

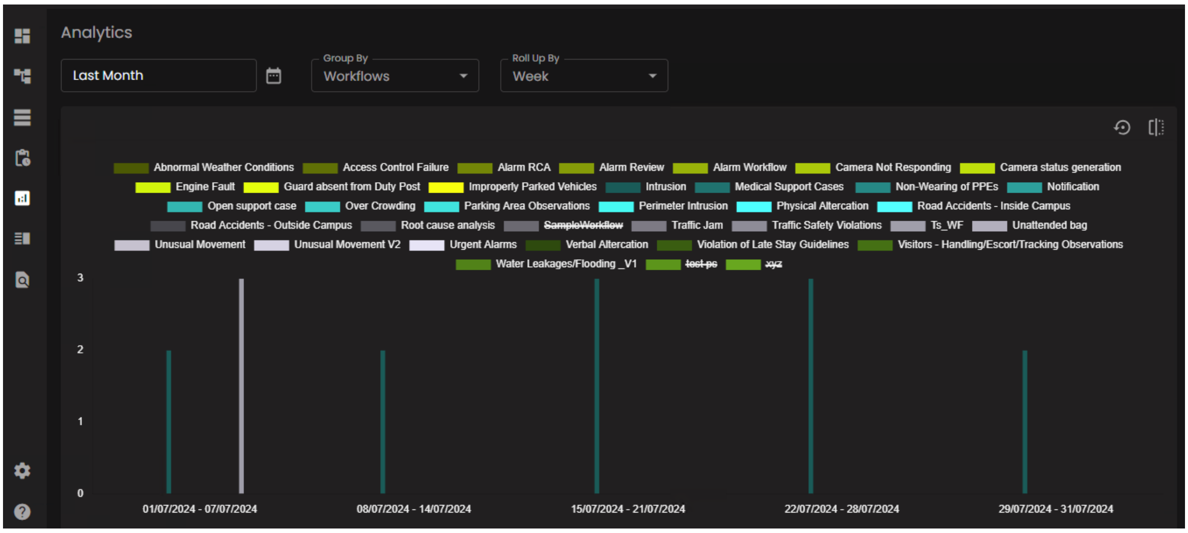
  Ensure to replace username1@example.com with the actual recipient's email address. Multiple users can be added following the structure provided.

- **.env Configuration**: Additionally, within the *.env* file at *C:\Program Files\O-Insights Command Center\Services*, set the following:

  ```
  CONFIG_SEND_NOTIFICATION_EMAIL=true
  ```

> **Note**: After updating the JSON and .env files, a system restart of the Query Engine (QE) or a cache update job is necessary to apply changes and enable notifications.

Analytics



Analytics

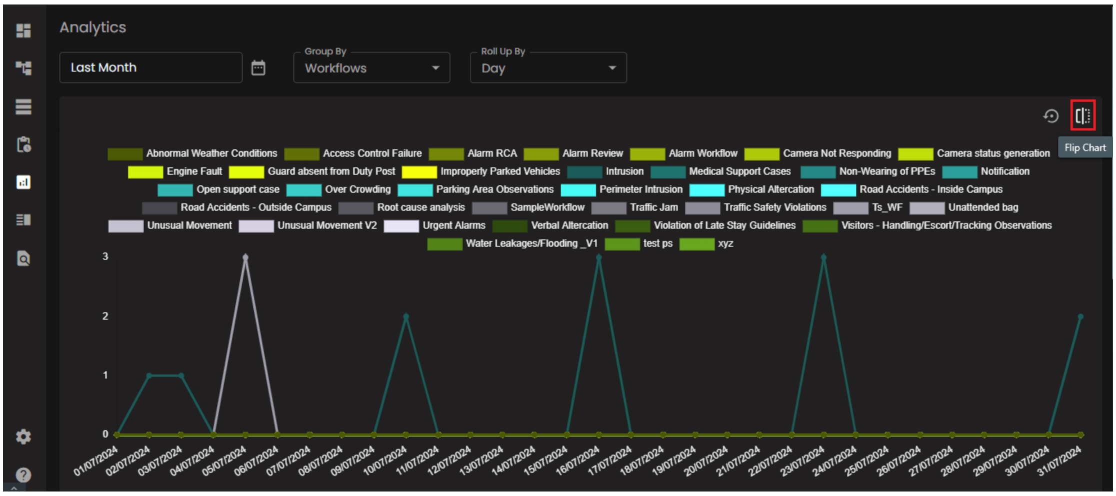
Last Month

Group By: Workflows

Roll Up By: Week

The **Analytics Module** is designed to provide robust data analysis tools, enabling users to scrutinize incident data efficiently:

- **Data Selection**: You can specify the parameters for your analysis by selecting the desired Date Range, Group By, and Roll Up options from dropdown lists available in the respective fields.



Analytics

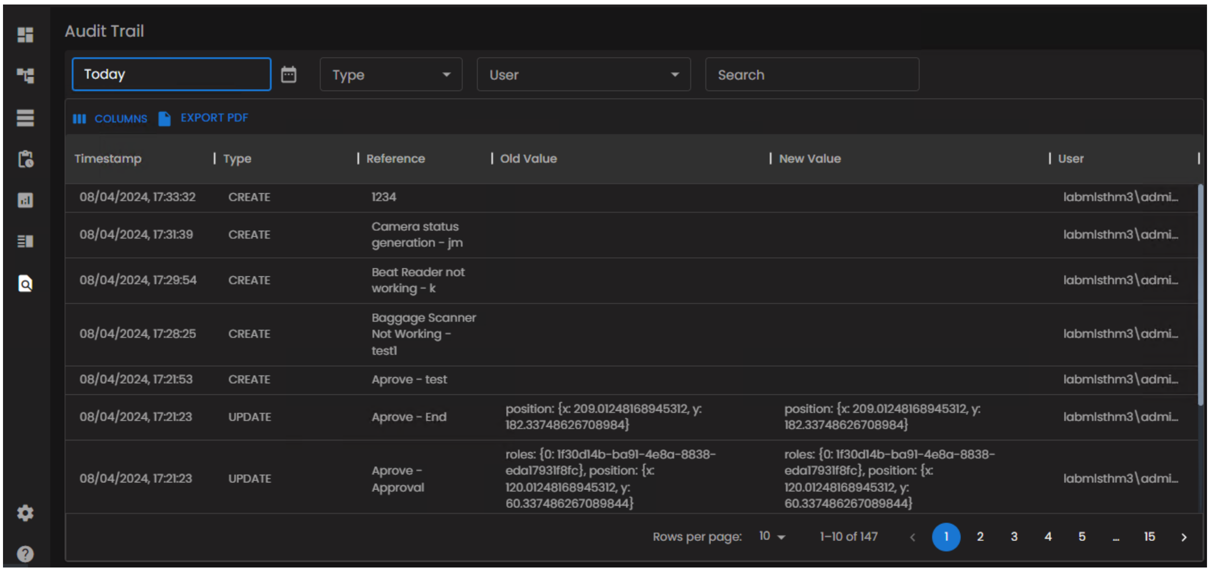
Last Month

Group By: Workflows

Roll Up By: Day

- **Visualization Tools**: Click on the Flip Chart icon to switch the data presentation between tabular views and visual line charts, enhancing the interpretability of data trends.
- **Graph Interaction**: For detailed examination of specific data points within bar graphs, right-click on the desired bars to zoom in. To return to the original graph scale, click on the Reset Zoom icon.

Audit Trail



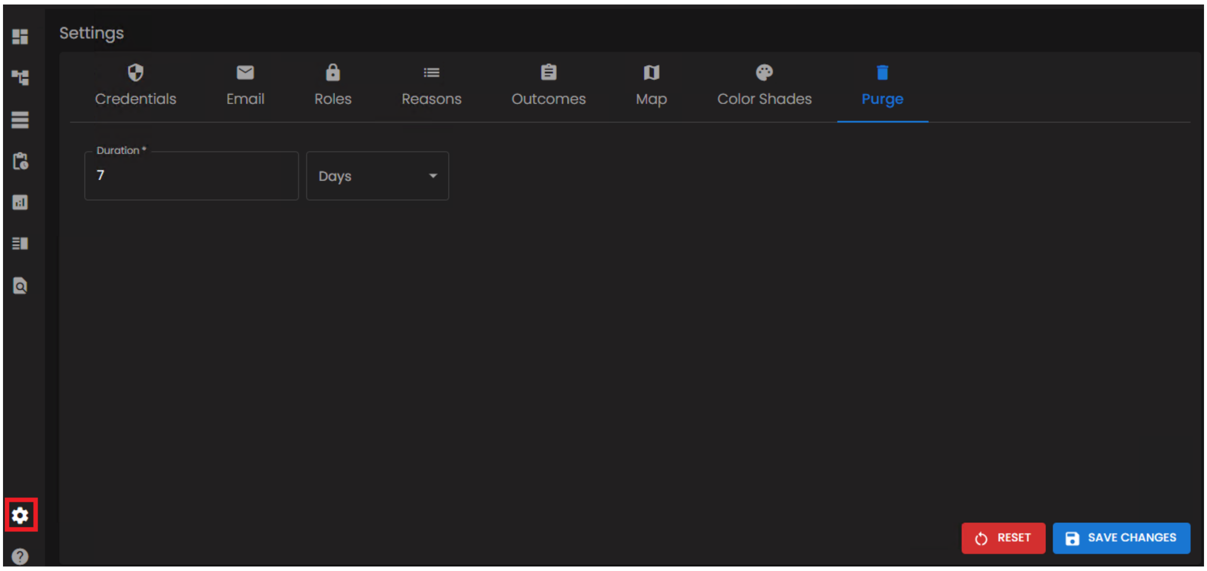
Timestamp	Type	Reference	Old Value	New Value	User
08/04/2024, 17:33:32	CREATE	1234			labmlsthm3\admi...
08/04/2024, 17:31:39	CREATE	Camera status generation - jm			labmlsthm3\admi...
08/04/2024, 17:29:54	CREATE	Beat Reader not working - k			labmlsthm3\admi...
08/04/2024, 17:28:25	CREATE	Baggage Scanner Not Working - test1			labmlsthm3\admi...
08/04/2024, 17:21:53	CREATE	Aprove - test			labmlsthm3\admi...
08/04/2024, 17:21:23	UPDATE	Aprove - End	position: {x: 209.01248168945312, y: 182.33748626708984}	position: {x: 209.01248168945312, y: 182.33748626708984}	labmlsthm3\admi...
08/04/2024, 17:21:23	UPDATE	Aprove - Approval	roles: {0: 1f30d14b-ba91-4e8a-8838-eda17931f8fc}, position: {x: 120.01248168945312, y: 60.337486267089844}	roles: {0: 1f30d14b-ba91-4e8a-8838-eda17931f8fc}, position: {x: 120.01248168945312, y: 60.337486267089844}	labmlsthm3\admi...

Audit Trail

The **Audit Trail** feature is designed to monitor and record system-level actions, focusing primarily on non-user-specific or generic activities. This includes actions such as the creation or deletion of workflows, among other system events. Here's how you can utilize the Audit Trail effectively:

- **Select Event Type**: To view specific types of audit events such as *Create, Update, Delete, Move,* and *Permanent Delete*, select the appropriate option from the dropdown list labelled *Type*.
- **User-Specific Segregation**: If you need to view actions performed by specific users, click on the *User* box to expand the dropdown menu and select the desired user.
- **Configure Display Columns**: Customize which columns are visible in the Audit Trail by clicking on the column's icon. Toggle the required options to display or hide specific columns based on your needs.
- **Export Data**: For documentation or reporting purposes, you can export the audit trail data as a PDF file. Simply click on the *EXPORT PDF* icon to download the data.

Settings



Duration * 7

Days

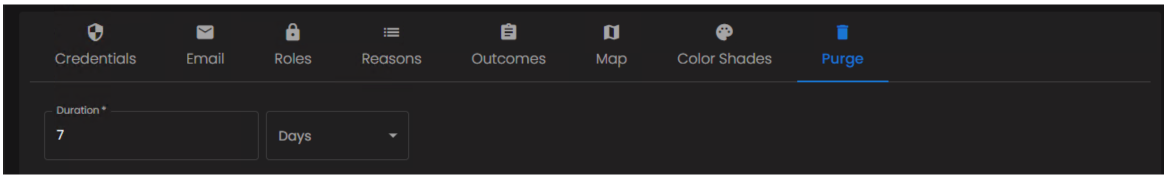
Settings

The **Settings** module lets users customize the Incident Manager to fit your requirements effectively. This module allows you to configure various settings that affect how the system operates and interacts with users.

Configuration

- **Credentials**: Securely manage server access credentials.
    - **Protocol**: Choose either *HTTP* or *HTTPS* for secure communication.
    - **Host Name**: Specify the DNS name of the server where the Query Engine is running.
    - **Port**: Default port *9011* is typically used for network communications.
- **Email Configuration:** Set up email functionalities to enable automated sending of notifications.
    - **Host Server**: Input your mail server's details.
    - **FROM**: Specify the sender's email address.
    - **Port**: Input the port number utilized by your mail server.
    - **Protocol**: Select the appropriate protocol (auto, none, SSL, TLS) for email transmission.
    - **Has Auth**: Check this if authentication is required and provide the necessary *Username* and *Password* of the mail server.

- **Roles**: Define and manage user roles to control access within the application.
  - **View**: Allows reading access to incidents.
  - **Write**: Permits creating and modifying incidents.
  - **Config**: Enables configuration of incidents, workflows, and other settings.
- **Reasons**: Set up predefined reasons that users can select during incident handling.
- **Outcomes**: Predefined outcomes for quick selection during incident resolution.
- **Map Configuration**: Integrate maps for location-based data visualization.
  - **API Key**: Enter a valid API key for either Bing or Google Maps to activate this feature.
- **Color Shades**: Customize the color scheme for charts and other visual elements within the application to enhance the user interface.
- **Purge Configuration**: Manage data retention effectively by setting automatic purge rules.



Duration * 7 Days

  - **Example**: In the above instance, the purge is configured to retain incident data for the last 7 days, with older data being automatically purged.

Report Templates

The **Report Template** module in the O-Insights Command Center offers two predefined templates—basic and standard—that help streamline the process of generating reports for workflows. These templates are located in the system at: *C:\Program Files\O-Insights Command Center\Services\externals\template*

Configurations

To customize these templates, such as editing the header to include a title, brand, or report name, and adding a logo, follow these detailed steps:

- **Convert Your Logo to Base64**: Convert your logo into a base64 string, which enables embedding the image directly into HTML.
- **Modify the HTML Template**: Open the .html file you wish to edit from the specified folder.
- **Insert the Base64 Logo**: Place the base64 string into the source attribute of an <img> tag within the HTML. Here's an example:

  ```
  <img height="85%" width="100%" src="base64_image_string_here" />
  ```

  We can convert any logo to Base64 string using online tools.
- **Add Brand/Report Name**: Utilize the following HTML tag to insert your brand or report name where appropriate:

  ```
  <h4 style="font-size: inherit">[Brand or Report Name]</h4>
  ```
- **Adjust Layout for Logo**: If you want the logo to appear on the right side of the header, wrap it in a <div> with a specified width. Adjust the width to suit your layout needs. Example:

  ```
  <div style="width: 30%; float: right;">[Logo HTML Code Here]</div>
  ```
- **Sample Header Code**: Here's how the complete header section may look, from the examples provided above:

  ```
  <div class="header">
    <div class="top-header-left-element">
      <img height="85%" width="100%"
  src="base64_image_string_here" />
    </div>
    <div style="width: 10%"></div>
  ```

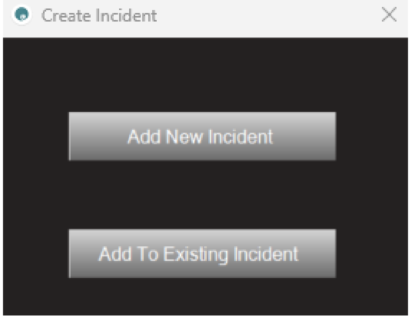
```
    <div class="top-header-middle-element">
        <h4 style="font-size: inherit">Command Center</h4>
    </div>
    <div style="width: 30%"></div>
</div>
```

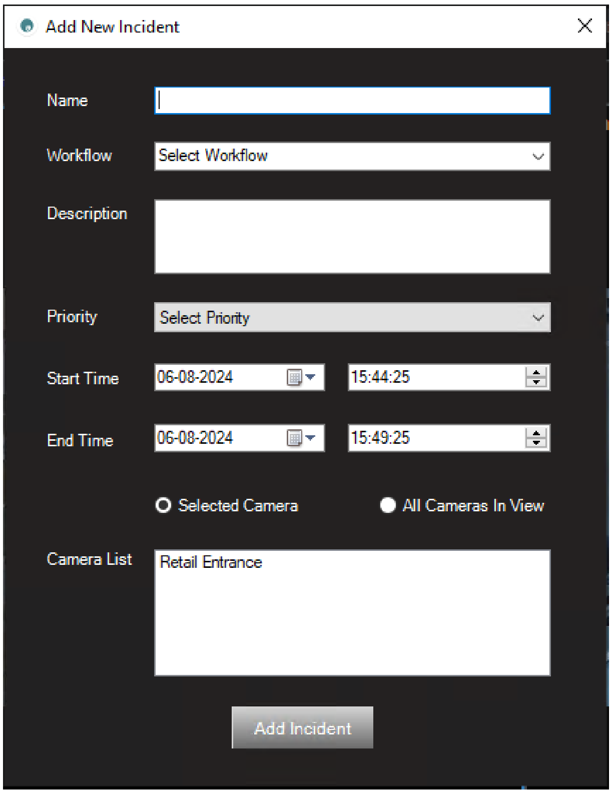
Common Plugins

Live View Plugin

The **Live View Plugin** is designed to facilitate incident creation directly from camera views and seamlessly integrate video sequences into existing incidents.

- **Create Incident**




Add New Incident

Name

Workflow: Select Workflow

Description

Priority: Select Priority

Start Time: 06-08-2024 15:44:25

End Time: 06-08-2024 15:49:25

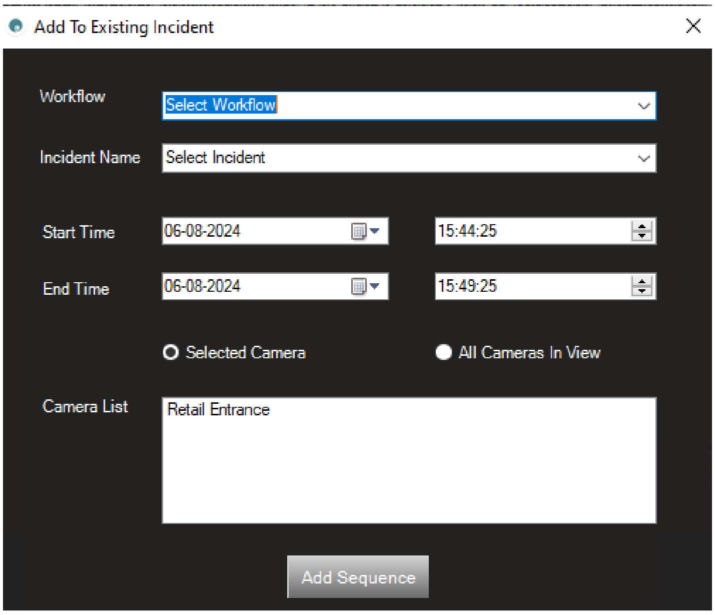
○ Selected Camera ● All Cameras In View

Camera List: Retail Entrance

- **Name**: Provide a unique name for the incident.
- **Workflow**: Select an applicable workflow from the dropdown menu to dictate the incident handling process.
- **Description**: Offer a detailed description of the incident to aid in subsequent reviews and actions.
- **Priority**: Assign a priority level (*Low*, *Medium*, *High*, *Critical*) to the incident to indicate urgency.
- **Start Time**: Set the date and exact time for when the camera sequence began before the incident occurred.
- **End Time**: Set the date and exact time for when the camera sequence ended after the incident occurred.

  - **Camera List**: Displays the name of the camera(s) involved. Selecting the option for *All cameras in view* **will include all** visible cameras as separate sequences tied to the incident.
  - **Add Incident**: Click to finalize and record the new incident.

- **Add To Existing Incident**



Workflow: Select Workflow

Incident Name: Select Incident

Start Time: 06-08-2024 15:44:25

End Time: 06-08-2024 15:49:25

○ Selected Camera ● All Cameras In View

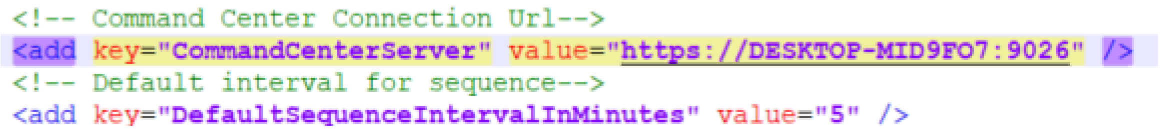
Camera List: Retail Entrance

  - **Workflow**: Choose the specific workflow under which the incident falls.
  - **Incident Name**: Select the existing incident to which the sequence will be added.
  - **Start Time & End Time**: Similar to creating a new incident, specify the time interval for the camera sequence relevant to the ongoing incident.
  - **Camera List**: Shows the camera selected for adding the sequence.
  - **Add Sequence**: Update the incident with the new sequence.

Configuration

Adjustments to the plugin settings can be managed through the file located at:

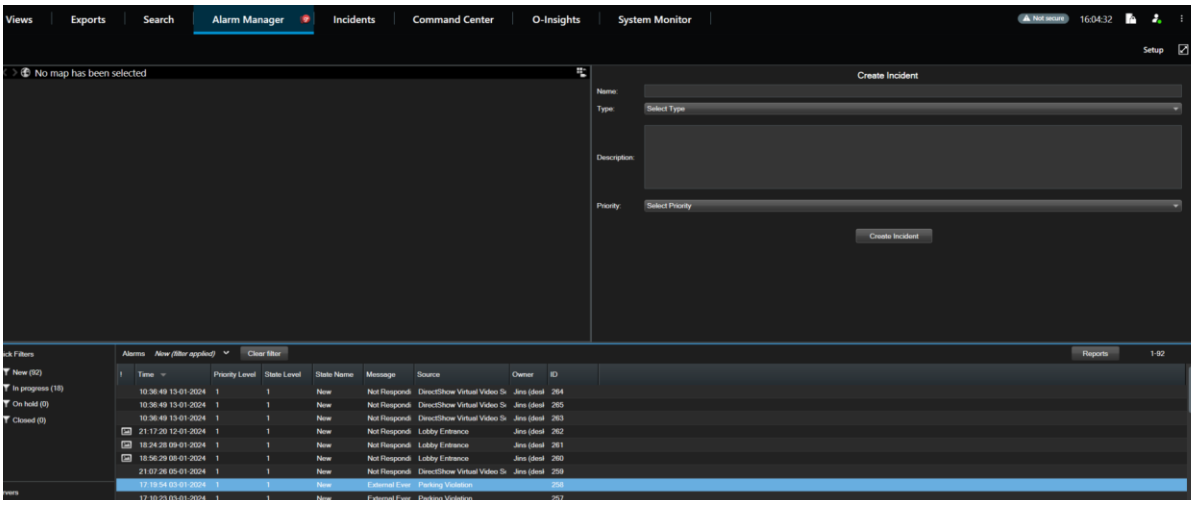
C:\Program Files\Milestone\MIPPlugins\O-Insights Command Center\OInsights Incident Creator - Live View\OInsightsLiveViewIncidentCreator.dll.config



```
<!-- Command Center Connection Url-->
<add key="CommandCenterServer" value="https://DESKTOP-MID9FO7:9026" />
<!-- Default interval for sequence-->
<add key="DefaultSequenceIntervalInMinutes" value="5" />
```

Note: The default time interval between the Start and End Time, set at 5 minutes, can be customized by altering the value for *DefaultSequenceIntervalInMinutes* within the configuration file.

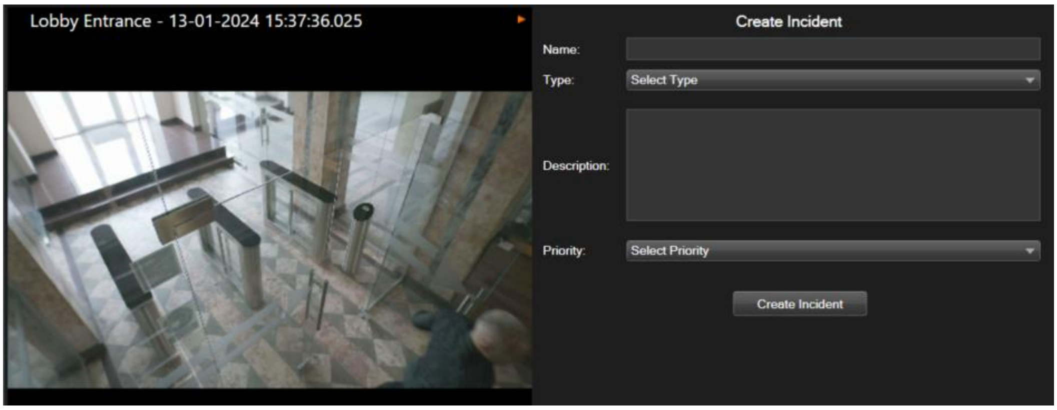
Alarm View Plugin



!	Time	Priority Level	State Level	State Name	Message	Source	Owner	ID
	10:36:49 13-01-2024	1	1	New	Not Respondi	DirectShow Virtual Video S	Jins (desl	264
	10:36:49 13-01-2024	1	1	New	Not Respondi	DirectShow Virtual Video S	Jins (desl	265
	10:36:49 13-01-2024	1	1	New	Not Respondi	DirectShow Virtual Video S	Jins (desl	263
	21:17:20 12-01-2024	1	1	New	Not Respondi	Lobby Entrance	Jins (desl	262
	18:24:28 09-01-2024	1	1	New	Not Respondi	Lobby Entrance	Jins (desl	261
	18:56:29 08-01-2024	1	1	New	Not Respondi	Lobby Entrance	Jins (desl	260
	21:07:26 05-01-2024	1	1	New	Not Respondi	DirectShow Virtual Video S	Jins (desl	259
	17:19:54 03-01-2024	1	1	New	External Ever	Parking Violation		258
	17:10:23 03-01-2024	1	1	New	External Ever	Parking Violation		257

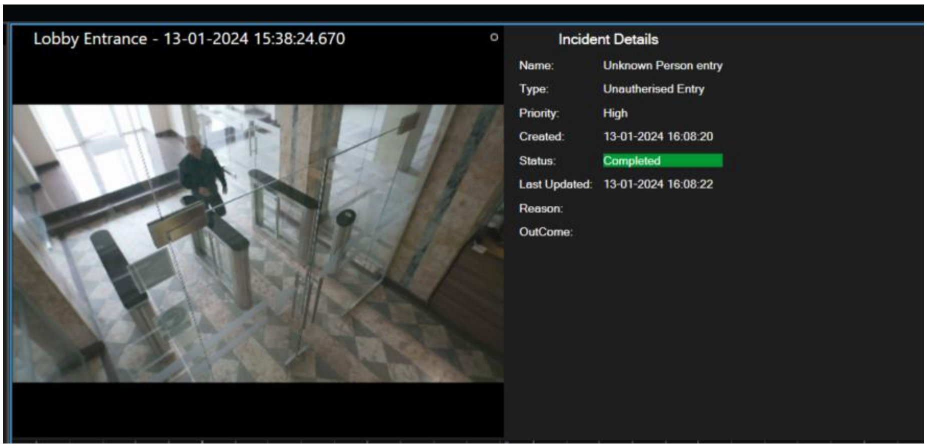
The **Alarm View** feature within the O-Insights Command Center is specifically designed to enable direct incident creation from the Alarm Manager.

- **Incident Creation from Alarm Manager**



  - **Selection**: Choose the relevant alarm from the Alarm Manager interface.
  - **Details Entry**: Input necessary details about the incident directly linked to the selected alarm.
  - **Create Incident**: Finalize and create the incident by clicking on the designated button.

- **Incident Status Monitoring**



Lobby Entrance - 13-01-2024 15:38:24.670

Incident Details

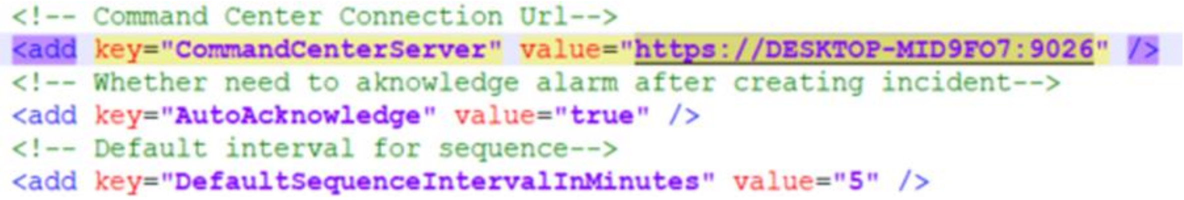
Name:	Unknown Person entry
Type:	Unauthorised Entry
Priority:	High
Created:	13-01-2024 16:08:20
Status:	Completed
Last Updated:	13-01-2024 16:08:22
Reason:	
OutCome:	

  - After creating an incident from an alarm, the system updates and displays the status of the incident, allowing users to track its progress and resolution directly from the Alarm View.

Configuration

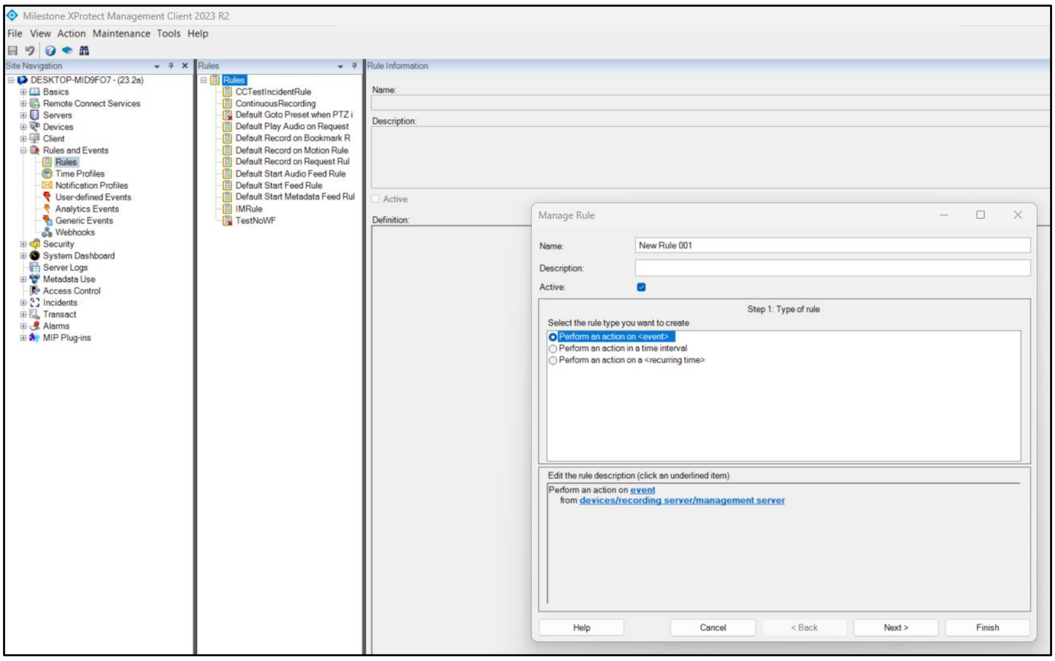
Adjustments to the plugin settings can be managed through the file located at:

C:\Program Files\Milestone\MIPPlugins\O-Insights Command Center\OInsights Incident Creator - Alarm View\OInsightsAlarmViewIncidentCreator.dll.config



```
<!-- Command Center Connection Url-->
<add key="CommandCenterServer" value="https://DESKTOP-MID9FO7:9026" />
<!-- Whether need to aknowledge alarm after creating incident-->
<add key="AutoAcknowledge" value="true" />
<!-- Default interval for sequence-->
<add key="DefaultSequenceIntervalInMinutes" value="5" />
```

Rule Plugin



Name: New Rule 001

Description:

Active: ☑

Step 1: Type of rule

Select the rule type you want to create

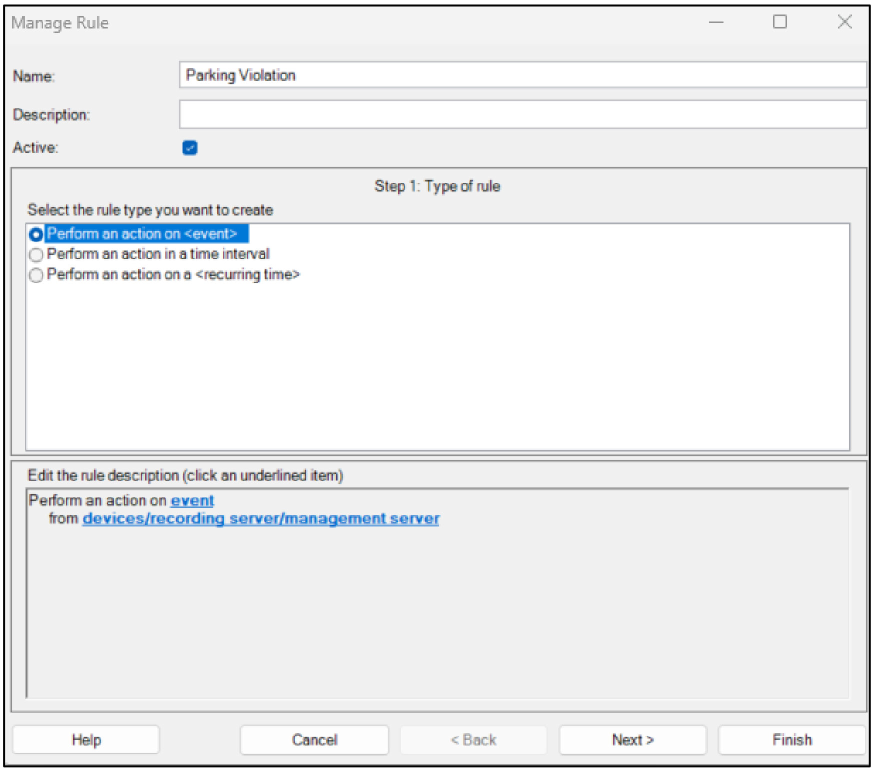
● Perform an action on <event>
○ Perform an action in a time interval
○ Perform an action on a <recurring time>

Edit the rule description (click an underlined item)

Perform an action on event
from devices/recording server/management server

The **Rule Plugin** is a component of the O-Insights Command Center designed to automate incident creation based on specific events within the XProtect environment. This functionality leverages the *Rules* of XProtect Management Client, allowing for streamlined incident management directly tied to event occurrences.

- **Integration with XProtect Rules:**



Name: Parking Violation

Description:

Active: ☑

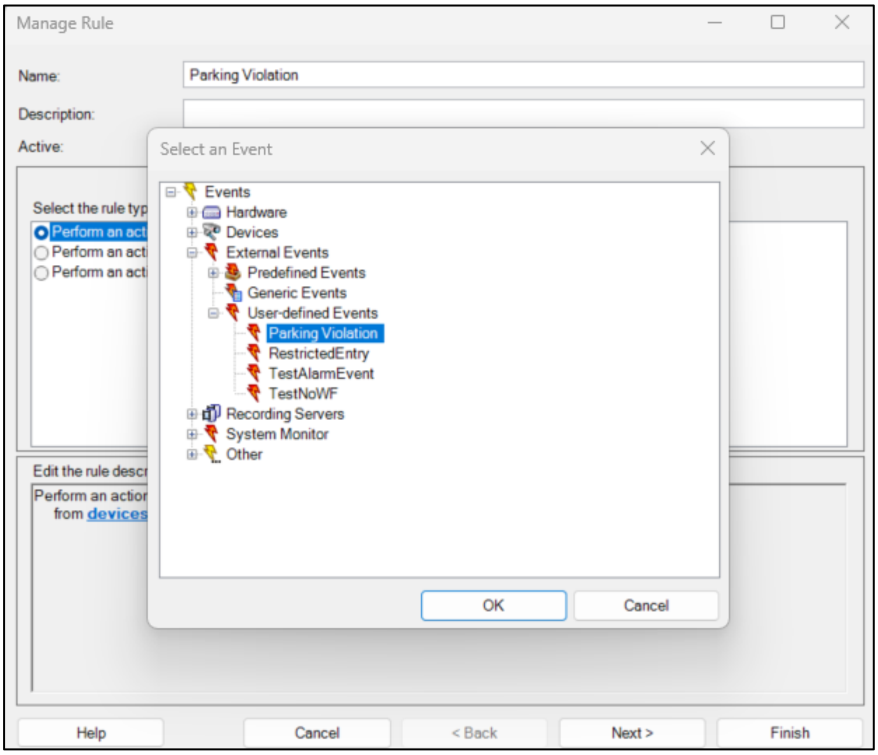
Step 1: Type of rule

Select the rule type you want to create

● Perform an action on <event>
○ Perform an action in a time interval
○ Perform an action on a <recurring time>

Edit the rule description (click an underlined item)

Perform an action on event
from devices/recording server/management server

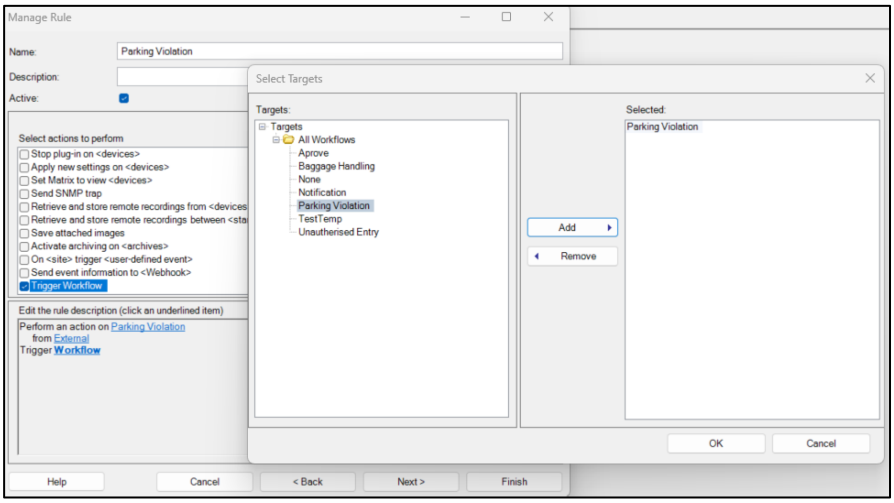

Manage Rule

Name: Parking Violation

Description:

Active:

- **Event Selection**: In the XProtect Management Client, define rules that specify which events should trigger incident creation.


Manage Rule

Name: Parking Violation

Description:

Active: ☑

Select actions to perform

- □ Stop plug-in on <devices>
- □ Apply new settings on <devices>
- □ Set Matrix to view <devices>
- □ Send SNMP trap
- □ Retrieve and store remote recordings from <devices
- □ Retrieve and store remote recordings between <sta
- □ Save attached images
- □ Activate archiving on <archives>
- □ On <site> trigger <user-defined event>
- □ Send event information to <Webhook>
- ☑ Trigger Workflow

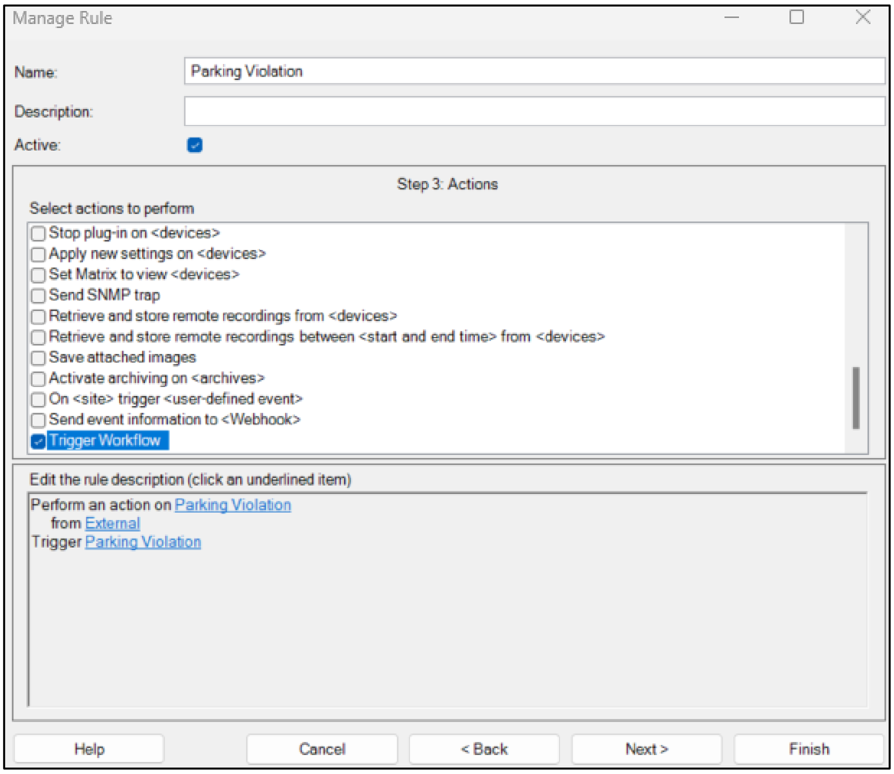
Edit the rule description (click an underlined item)

Perform an action on Parking Violation
from External
Trigger **Workflow**

Select Targets

Targets:

Selected: Parking Violation


Manage Rule

Name: Parking Violation

Description:

Active: ☑

Step 3: Actions

Select actions to perform

- ☐ Stop plug-in on <devices>
- ☐ Apply new settings on <devices>
- ☐ Set Matrix to view <devices>
- ☐ Send SNMP trap
- ☐ Retrieve and store remote recordings from <devices>
- ☐ Retrieve and store remote recordings between <start and end time> from <devices>
- ☐ Save attached images
- ☐ Activate archiving on <archives>
- ☐ On <site> trigger <user-defined event>
- ☐ Send event information to <Webhook>
- ☑ Trigger Workflow

Edit the rule description (click an underlined item)

Perform an action on Parking Violation
from External
Trigger Parking Violation

- **Workflow Association**: After selecting an event, proceed to the next section to choose a trigger workflow from the pre-defined workflows available in the Command Center.
- **Activation**: Finalize the setup by clicking *Finish* to activate the rule.

- **Restart the XProtect Event Server:** After configuring rules and associating them with workflows, a restart of the XProtect Event Server is necessary to apply changes.

Configuration

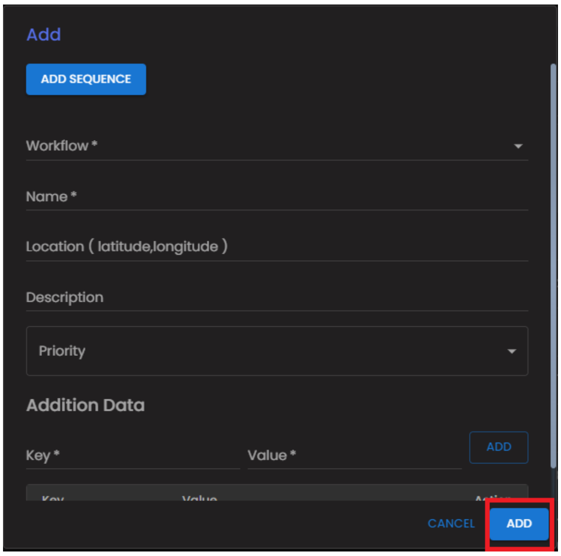
Adjust settings and configurations by accessing the file at the following location:

C:\Program Files\Milestone\MIPPlugins\O-Insights Command Center\OInsights Incident Creator – Rule\OInsightsIncidentCreator-Rule.dll.config

Note: Ensure the OInsightsIncidentCreator-Rule folder is copied to C:\Program Files\Milestone\MIPPlugins on the server where the Event server is operating.

Incident View

- **Creating a New Incident:**
  - **Access**: Navigate to the Incident View and locate the *Create* (+ CREATE) icon in the upper right corner of the interface.



  - **Incident Details**: Upon clicking *CREATE*, you must:
    - **Workflow**: Choose necessary workflow.
    - **Name**: Provide a distinctive name that clearly identifies the incident.
    - **Location:** Add the co-ordinates for the incident to indicate the location of the incident.
    - **Priority**: Set the priority level (e.g., *Low, Medium, High, Critical*) to dictate the urgency and response protocol.
    - **Additional Data:** Add *Key* and *Value* if needed.
  - **Confirmation**: Once all details are correctly filled, click on the *ADD* icon to create the incident.

FAQs for O-Insights Command Center for XProtect

How can I create an incident?

You can create an incident through multiple channels in the O-Insights Command Center for XProtect:

- **Command Center (Incident View)**
- **Via Camera Live View/Playback**
- **Using Event Rules**
- **Through XProtect Alarm Manager**
- **Using O-Insights Notification Manager**

Can I rerun an incident?

No, rerunning an incident is not supported.

Is it possible to modify an incident?

Yes, you can modify all aspects of an incident except for its workflow name. Note that features like notes and attachments may become inaccessible after the incident is completed.

Can I modify a workflow?

Modifications to the workflow are not allowed while the incident is active or running. You can make changes once the incident is completed.

Can I edit the widget name in the dashboard?

Yes, simply double-click on the widget name to edit it.

Can I customize the colors in the dashboard?

Yes, the settings menu provides options to customize graph colors and color shades.

Can I apply filters to widgets?

Yes, you can apply filters to widgets based on the configured workflow.

Can I add a camera sequence to an existing incident?

Yes, you can add sequences to incidents from the Incident view under the Sequences tab.

Can I add custom filters in the Incident view?

Yes, use the filter button located next to the search function on the Incident view page.

Why is the report view button not visible to me in the Incident view?

The report view button is only visible when the incident status is marked as Completed.

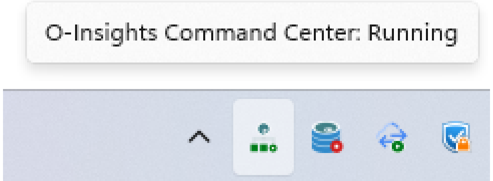
Is the Command Center available on mobile devices?

No, the Command Center is a plugin that operates exclusively within the XProtect Smart Client.

Do I need the QueryEngine for the Command Center?

Yes, the QueryEngine must be installed and running for the Command Center to function properly.

How do I know if the Command Center service is running?

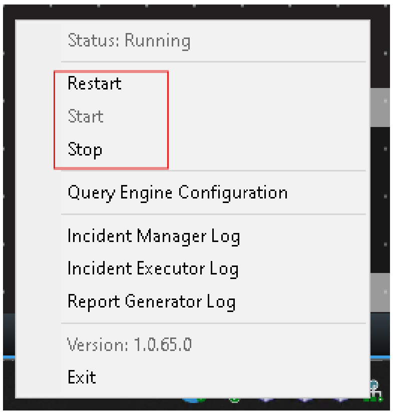


O-Insights Command Center: Running

To check if the Command Center service is running, hover over the Command Center Configuration Tool icon located in the system tray. The service status will be displayed when you do so.

How do I restart the Command Center service?

To restart the service, use the Command Center Configuration Tool by clicking its icon in the system tray and selecting "Restart" from the context menu.



What is the minimum requirement for the Command Center?

- **CPU:** Intel® Core™ i5 or higher
- **RAM:** 8GB, 16GB or more for larger systems
- **Network:** Ethernet 100 Mbit or better
- **Hard Disk:** 10 GB or more free space
- **Operating System:**
    - Microsoft® Windows® 10 Pro (64-bit) or higher

    - Microsoft® Windows® Server 2016 (64-bit) or higher
- **Milestone Version:** Milestone 2023 R1 or higher – All Editions
- **QueryEngine Version:** 5.0

How often is the Command Center updated?

The O-Insights product team regularly releases updates for all its products, including the Command Center. Updating to the latest version is recommended for optimal performance.

Can we change the export path/PowerShell script path?

Yes, modifications can be made in the .env file located at “<Install Directory>\O-Insights Command Center\Services\.env”.

Why isn't the Trigger Event task working after adding a new User-Defined Event in XProtect?

Restart the Query Engine after adding a new User-Defined Event to ensure functionality.

> **Note:** If you have any further questions or require assistance, please don't hesitate to contact our support team—we'll be happy to help!