STORMSHIELD

GUIDE

STORMSHIELD LOG SUPERVISOR

PLAYBOOKS GUIDE

Version 2

Document last updated: July 4, 2024

Reference: sls-en_playbooks_gde

Table of contents

Change log

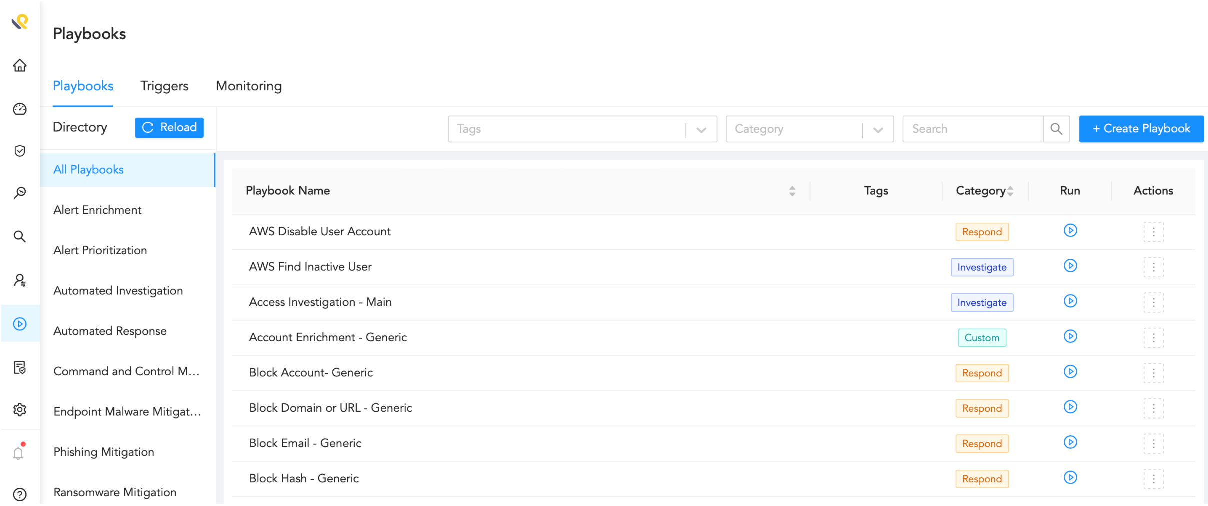
Date	Description
July 4, 2024	New document

Getting started

Welcome to the SLS version 2 Playbooks Guide.

Playbooks let you automate and coordinate workflows based on the incidents generated in SLS. Using playbooks, you can automate incident investigation and response with flow diagrams comprising of multiple blocks, with each block performing a specific task.

You can trigger playbooks based on the **incidents** generated in SLS. You can then automate the process of adding **cases** for further investigation using the triggered playbooks.



You can run the pre-configured playbooks if they suit your use cases. Click a playbook to view its process, and edit, test and export it.

You can also generate SLA reports by enabling SLA support. For more details, see Enabling SLA Support.

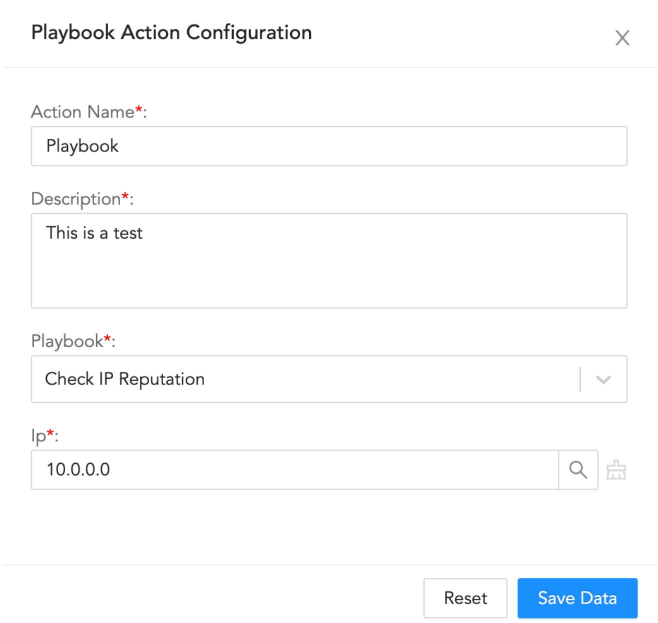
In this document, Stormshield Log Supervisor is referred to in its short form SLS. Images used in this document are from the partner vendor's (Logpoint) software program. In your SLS, the graphics may vary but user experience is exactly the same.

Action Types

Playbooks start with a **Trigger** action and end with an **End** action. In between, you can create any of the following actions:

Action Name	Description	When to Use/How to Use
Playbook	Triggers a different playbook from within the current or parent playbook.	For longer processes that playbooks automate, it can be helpful to break up the processes into parts. This will help you reuse different playbooks in different scenarios.
Annotation	Adds comments to a playbook action.	Let your colleagues know important information about the Action and Playbook.
API	Triggers an API call from within the playbook.	Connects the playbook to products and services from other vendors.
Script	Triggers a script from within the playbook. Currently, SLS only supports Python scripts.	Lets you write python scripts to customize playbook functionality.
Case Item	Adds an individual item or event to a case, the investigation's sequence of steps.	Let's you and your colleagues track and understand what happened through the course of an automated incident investigation.
Status	Sets the status of an incident.	Apply status to incidents based on severity.
Email	Sends an email from within the playbook.	Send incident based email to desired recipients from within the playbooks.
LDAP	Triggers an LDAP request.	Authenticates users/actions from within Playbooks by communicating with a central user database.

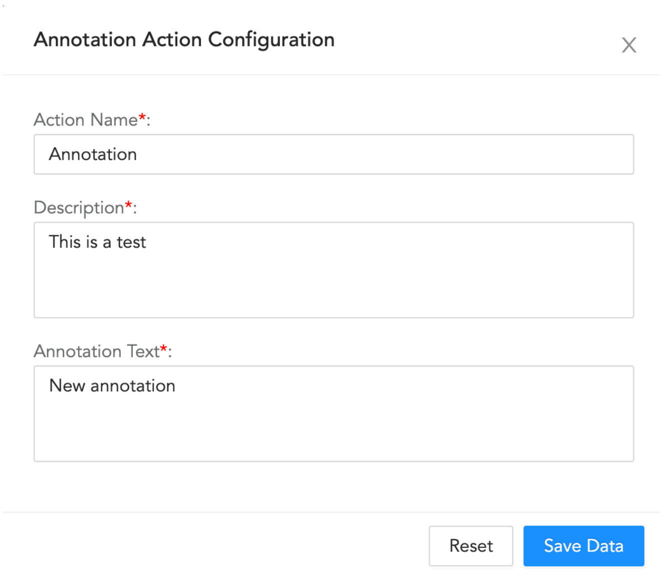
Configuring Playbook Action



To configure a playbook action:

1. Enter an **Action Name** and its **Description**.
2. Select a **Playbook**.
3. Enter the information for the playbook.
4. Click **Save Data**.

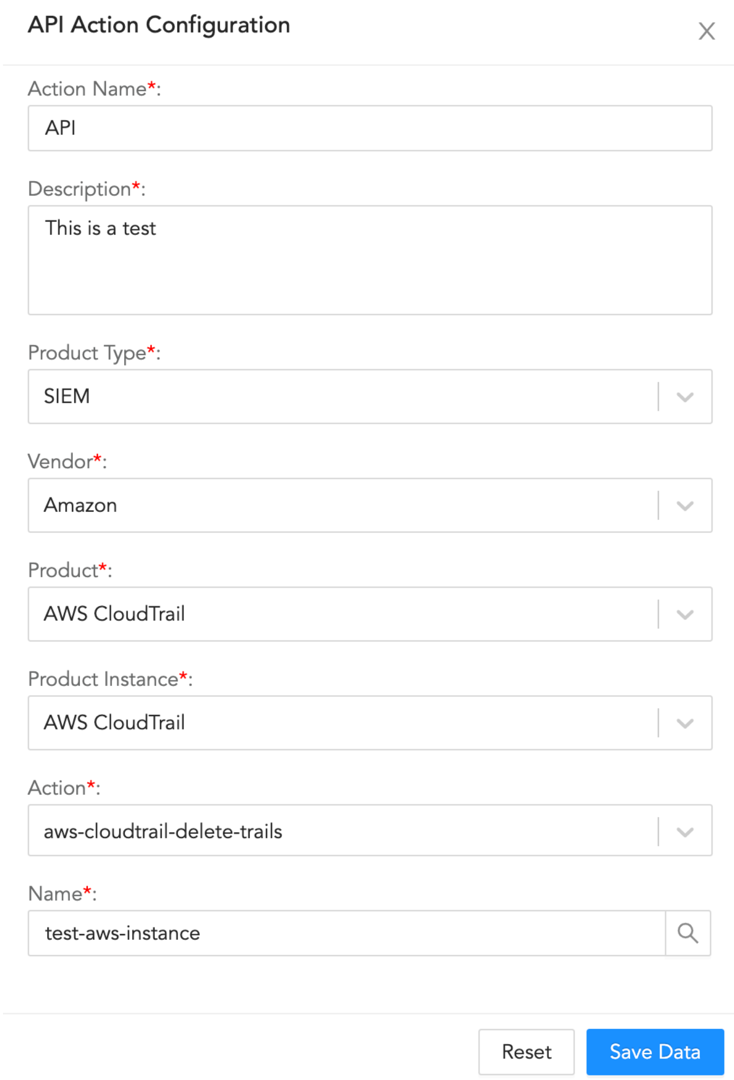
Configuring Annotation Action



To configure an annotation action:

1. Enter an **Action Name** and its **Description**.
2. Enter an **Annotation Text**.
3. Click **Save Data**.

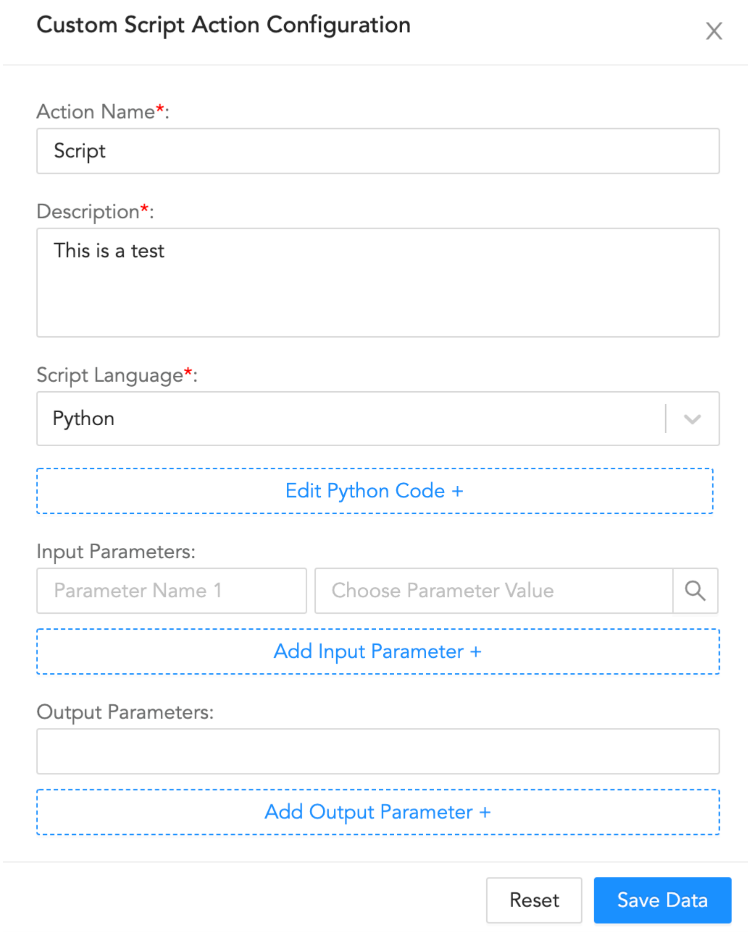
Configuring API Action



To configure an API action:

1. Enter an **Action Name** and its **Description**.
2. Select a **Product Type**, a **Vendor**, a **Product**, a **Product Instance**, and an **Action**.
3. Enter the information for the selected configuration.
4. Click **Save Data**.

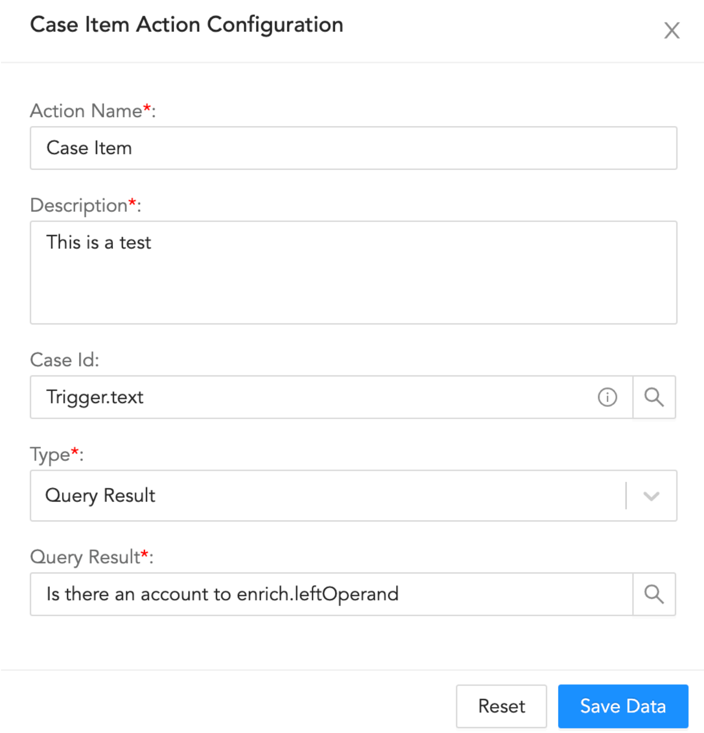
Configuring Custom Script Action



To configure a script action:

1. Enter an **Action Name** and its **Description**.
2. Select the **Script Language**.
3. Click **Edit Python Code +**, enter the required code, and click **Save**.
4. Enter or select the **Input Parameters** and their values.
5. Enter the **Output Parameters** for the block.
6. Click **Save Data**.

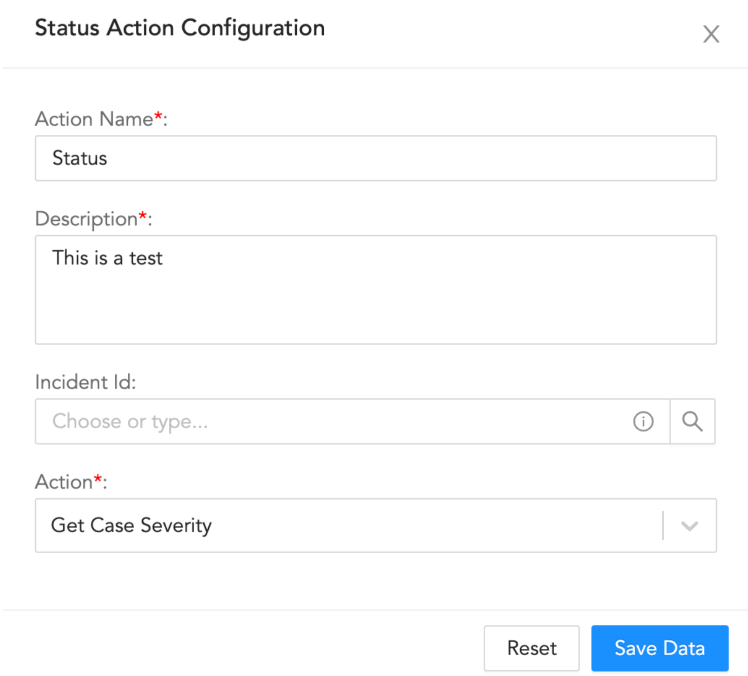
Configuring Case Item Action



To configure a case item action:

1. Enter an **Action Name** and its **Description**.
2. Enter or select a **Case Id**.
3. Select a block **Type**.
   - If you choose **Label**, enter a **Description** and a **Label**.
   - If you choose **File**, enter a **Description**, a **File Name**, and a **File Location**.
   - If you choose **Query Result**, enter a **Description**, and a **Query Result**.
4. Click **Save Data**.

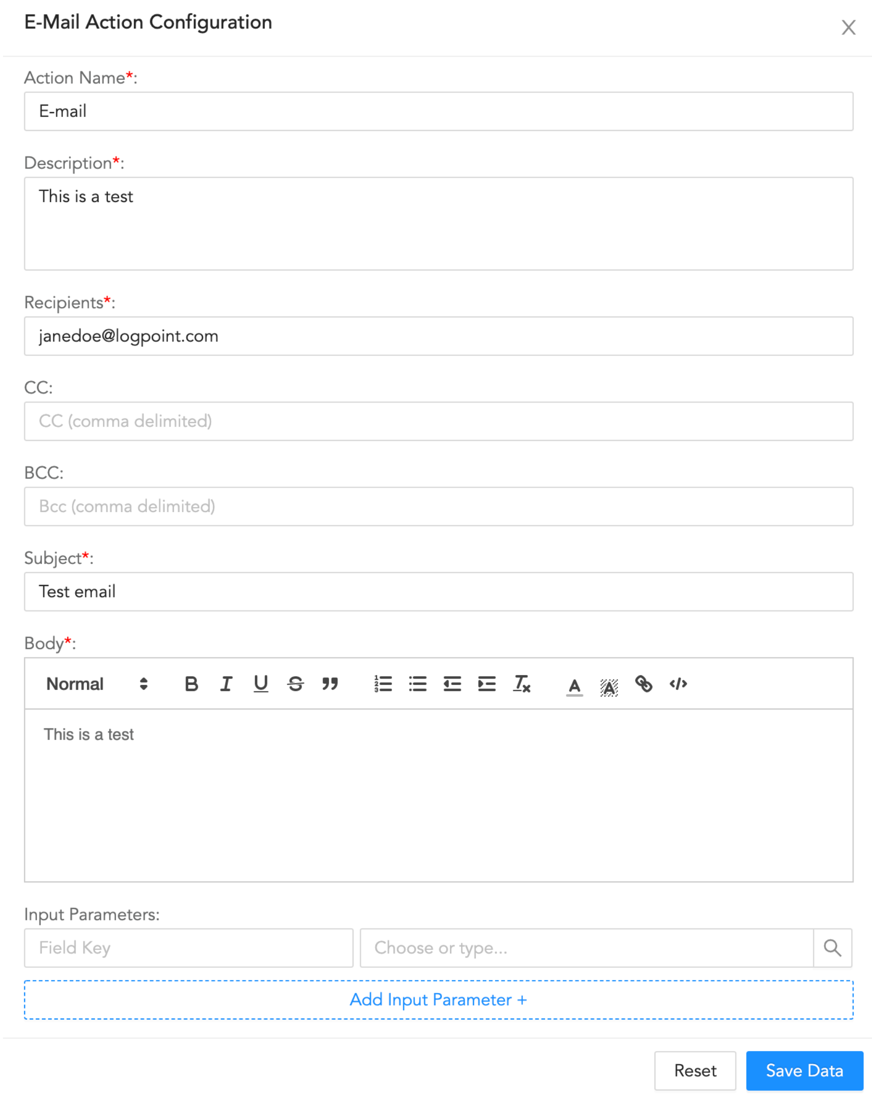
Configuring Status Action



To configure a status action:

1. Enter an **Action Name** and its **Description**.
2. Enter or select an **Incident Id**. You can leave the field blank to use a dynamically generated ID.
3. Select an **Action**.
   - If you select **Set Case Status**, select the **Status**.
   - If you select **Handling Status**, select the **Case Status**.
   - If you select **Manage Case Severity**, select the **Severity Action Type** and enter the **Decrement Severity By** value.
4. Click **Save Data**.

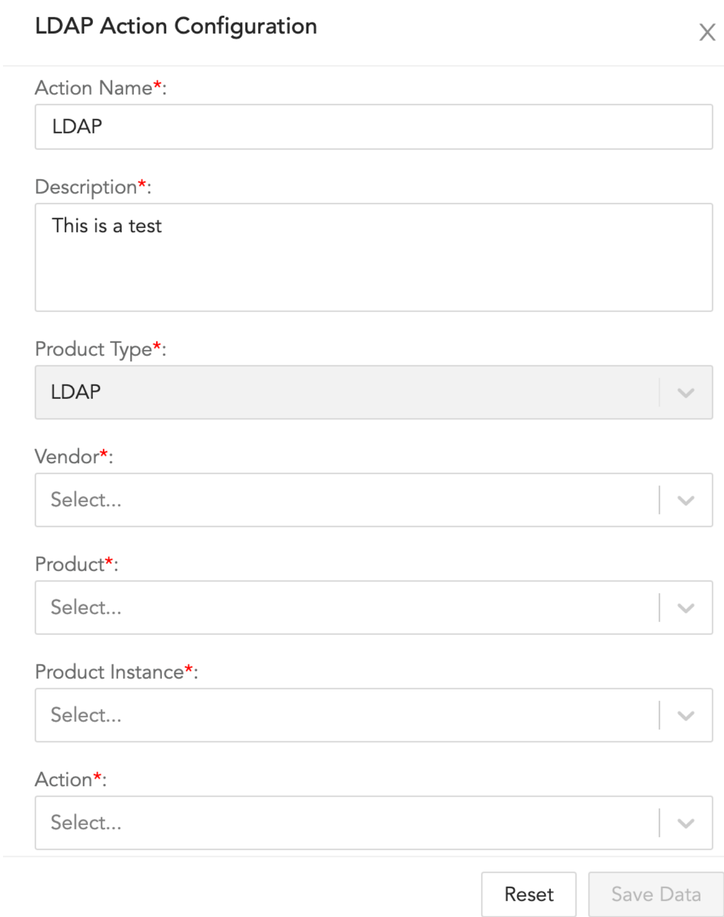
Configuring Email Action



To configure an e-mail action:

1. Enter an **Action Name** and its **Description**.
2. Enter a comma-separated list of **Recipients**, **CC** recipients, and **BCC** recipients.
3. Enter a **Subject**.
4. Enter the e-mail **Body**.
5. Enter a key-value separated list of **Input Parameters**.
6. Click **Save Data**.

Configuring LDAP Action



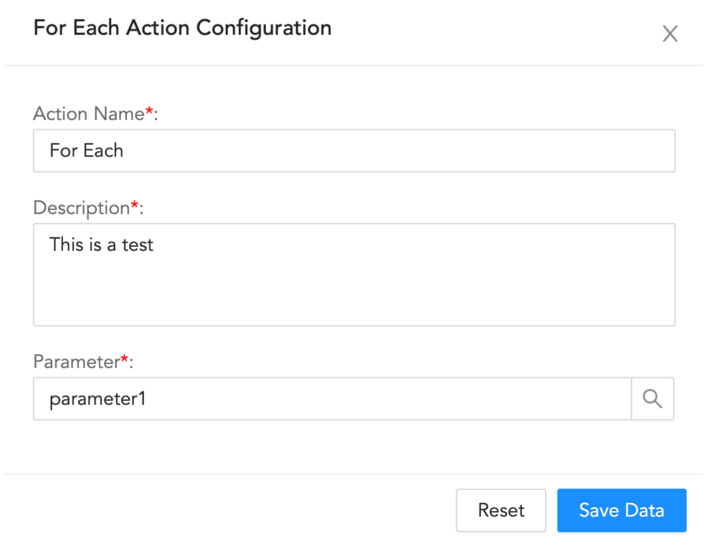
To configure an LDAP action:

1. Enter an **Action Name** and its **Description**.
2. Select a **Vendor**, a **Product**, a **Product Instance**, and an **Action**.
3. Click **Save Data**.

UML Types

UML Name	Description	When to Use/How to Use
For Each	Processes multiple queries from the same block.	When you need to loop queries through each item in an array or list.
If-Then	Processes a conditional statement.	When you need to make a specific response for a predefined event.

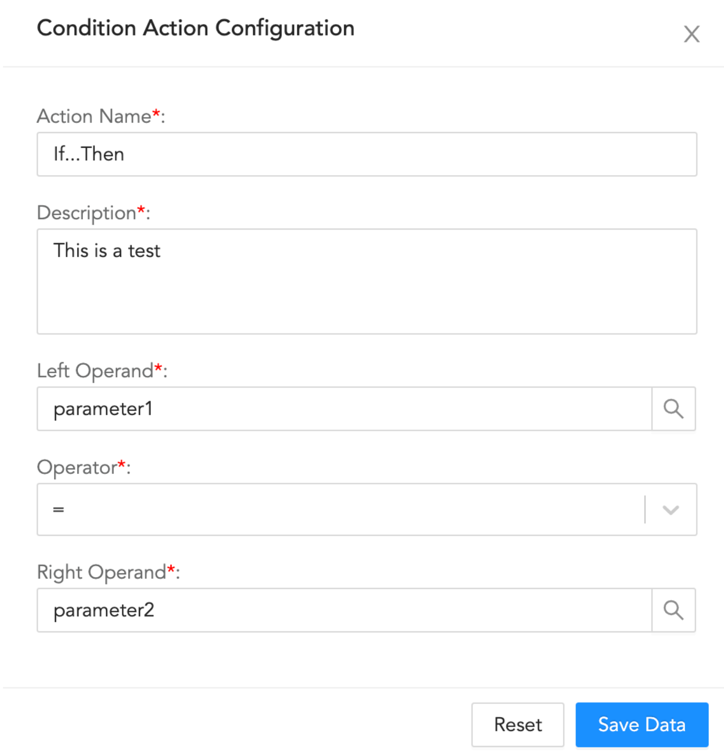
Configuring For Each Action



To configure a for-each action:

1. Enter an **Action Name** and its **Description**.
2. Enter or choose the **Parameter**.
3. Click **Save Data**.

Configuring If-Then Action



To configure an if-Then action:

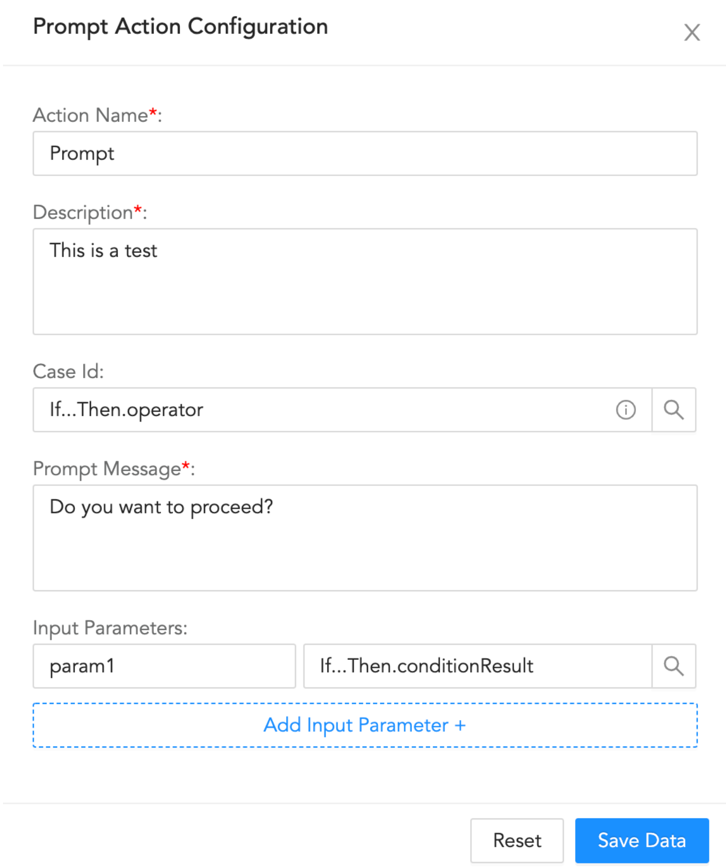
1. Enter an **Action Name** and its **Description**.
2. Enter or choose the **Left Operand**.
3. Select an **Operator**.
4. Enter or choose the **Right Operand**.
5. Click **Save Data**.

NOTE
Add another block to follow from the **Else** node when the provided condition is **False**.

Interactive Type

Interactive Name	Description	When to Use/How to Use
Prompt	Displays a message for manual action on part of user before the playbook runs.	When you want to confirm whether or not the user needs to perform certain manual actions before the rest of the automated playbook continues running.

Configuring Prompt Action



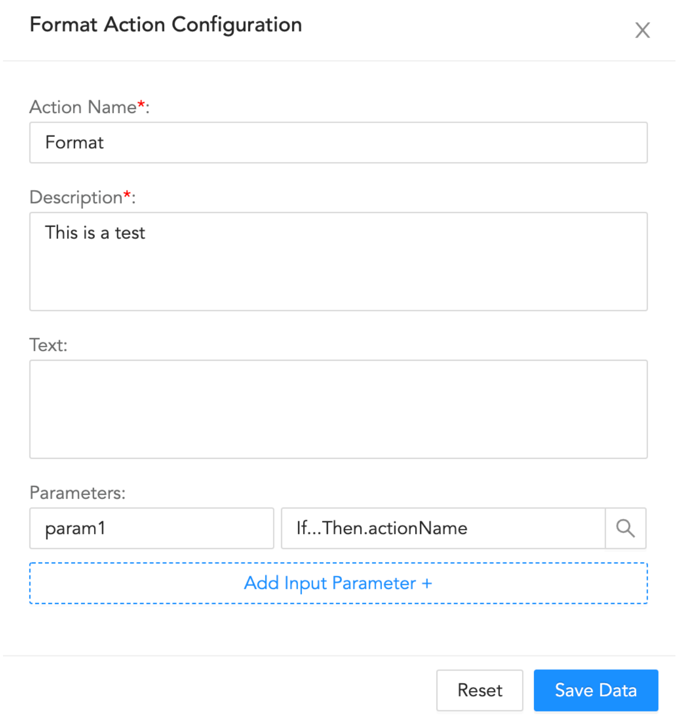
To configure a prompt action:

1. Enter an **Action Name** and its **Description**.
2. Enter or choose the **Case Id**.
3. Enter the **Prompt Message**.
4. Enter a list of key-value based **Input Parameters**.
5. Click **Save Data**.

Action Block Types

Action Block Name	Description	When to Use/How to Use
Format	Adds a block of parameters in the key-value format.	When you need to add multiple parameters and associate each with various actions.
Query	Adds a query to get specific fields.	When you need to input a query to generate output parameters based on input parameters.
Filter	Filters results using the input parameters.	When you need to filter out results based on input conditions.
Cases Query	Searches for existing cases using filters.	When you need to search and retrieve existing cases based on a specified filters.
String Utilities	Allows string manipulation on input text.	When you need to perform different string manipulations, including lowercase/uppercase conversion and encoding/decoding to different formats.

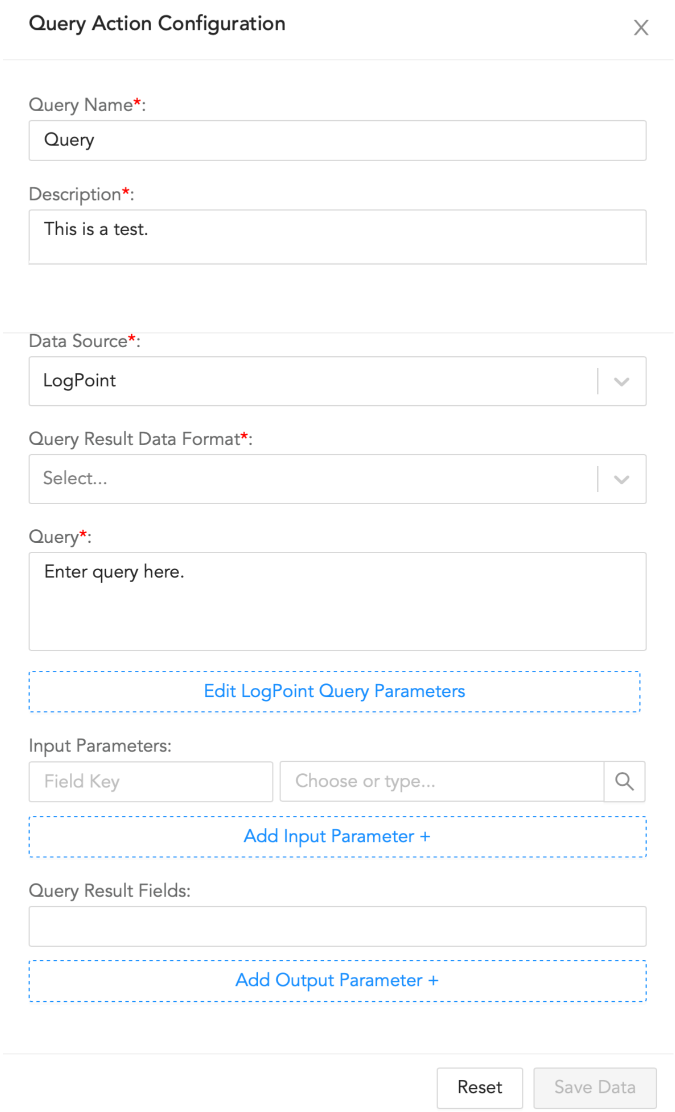
Configuring Format Action



To configure a format block:

1. Enter an **Action Name** and its **Description**.
2. Enter a **Text**.
3. Enter a list of key-value based **Parameters**.
4. Click **Save Data**.

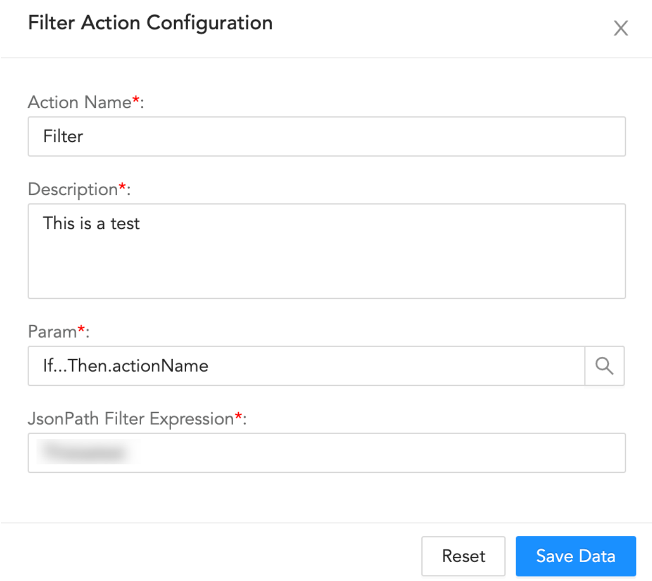
Configuring Query Action



To configure a query block:

1. Enter a **Query Name** and its **Description**.
2. Select a **Data Source** and a **Query Result Data Format**.
3. Enter a **Query** to retrieve the required logs.
4. Click **Edit SLS Query Parameters** to update the parameters.
5. Enter a **SLS Id**. The value entered here overrides the value retrieved from the SLS incident.
6. Select a **Time Range** and enter a **Limit**.
7. Select a **Time-Zone**. You can choose between a system set time zone and a custom time zone.
8. Enter a list of **Repositories**.
9. Enter a list of key-value based **Input Parameters**.
10. Enter a list of **Query Result Fields**.
11. Click **Save Data**.

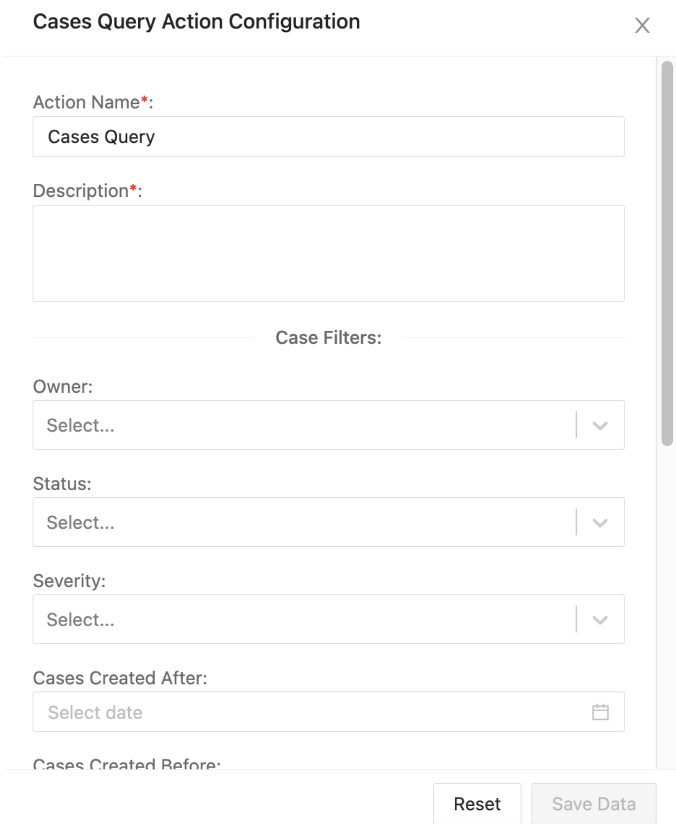
Configuring Filter Action



To configure a filter block:

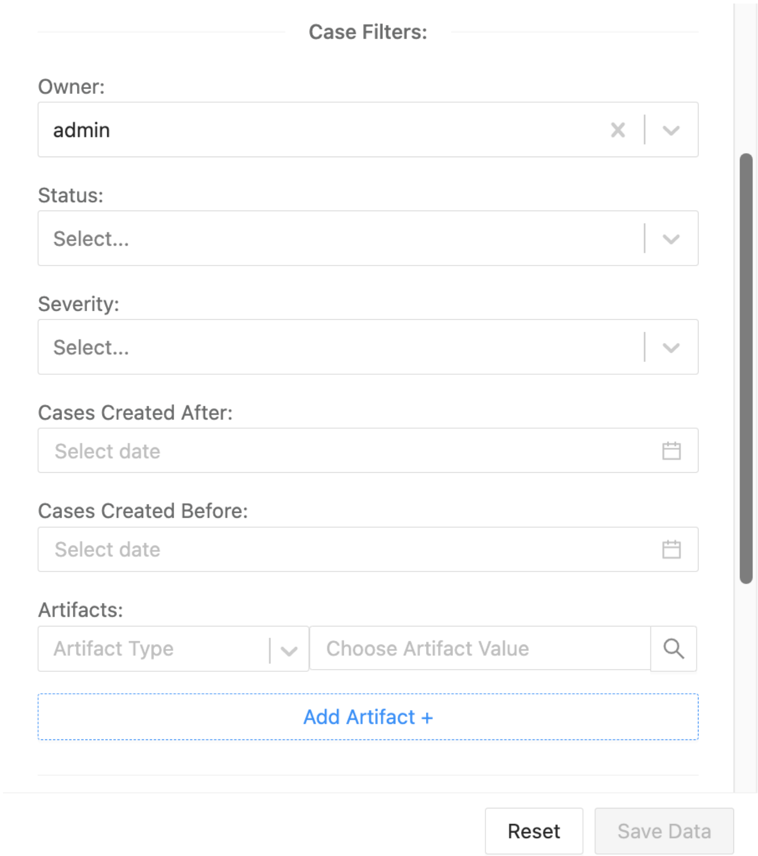
1. Enter an **Action Name** and its **Description**.
2. Enter or choose a **Param**.
3. Enter a **JSONPath Filter Expression**.
4. Click **Save Data**.

Configuring Cases Query Action

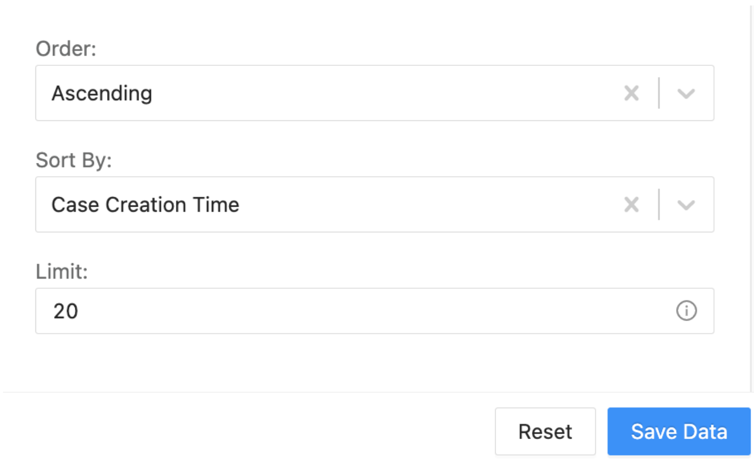


To configure cases query:

1. Enter an **Action Name** and its **Description**.
2. Choose the **Case Filters** you want to apply to retrieve cases according to:
   - **Owner**: The user who owns them.
   - **Status**: Their current status.
   - **Severity**: Their level of severity.
   - **Cases Created After**: When they were created after a specific date.
   - **Cases Created Before**: When they were created before a specific date.
   - **Artifacts**: Specific artifacts or artifact types linked to the case. You can use more than one artifact as a filter.

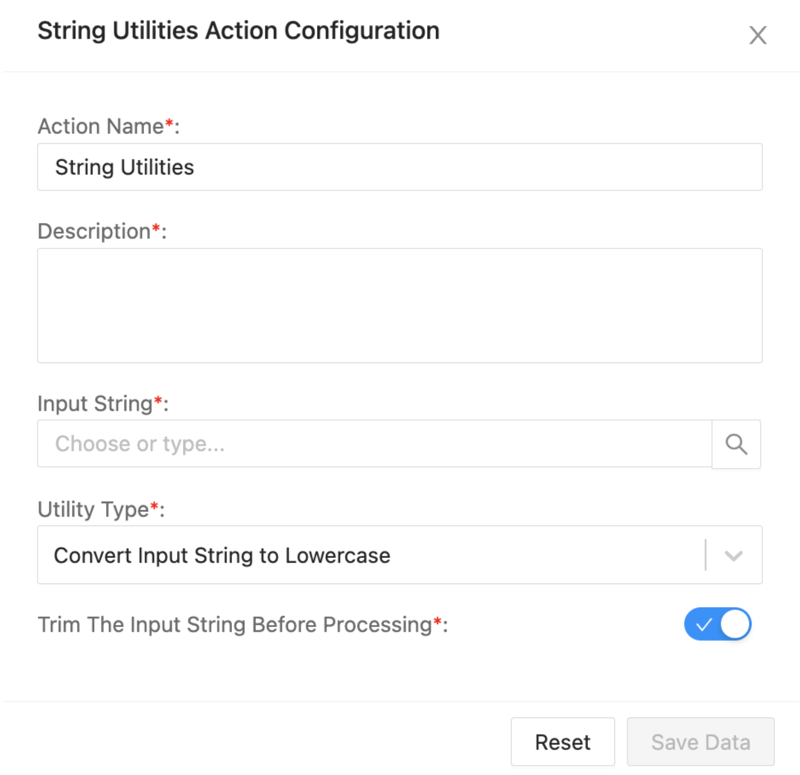


3. Select how the filtered results are displayed.
   - **Order**: Ascending or descending order.
   - **Sort By**: Group results according to **Case Creation Time**, **Severity**, or **Case Status**.
   - **Limit**: Total number of results. The maximum is 50.



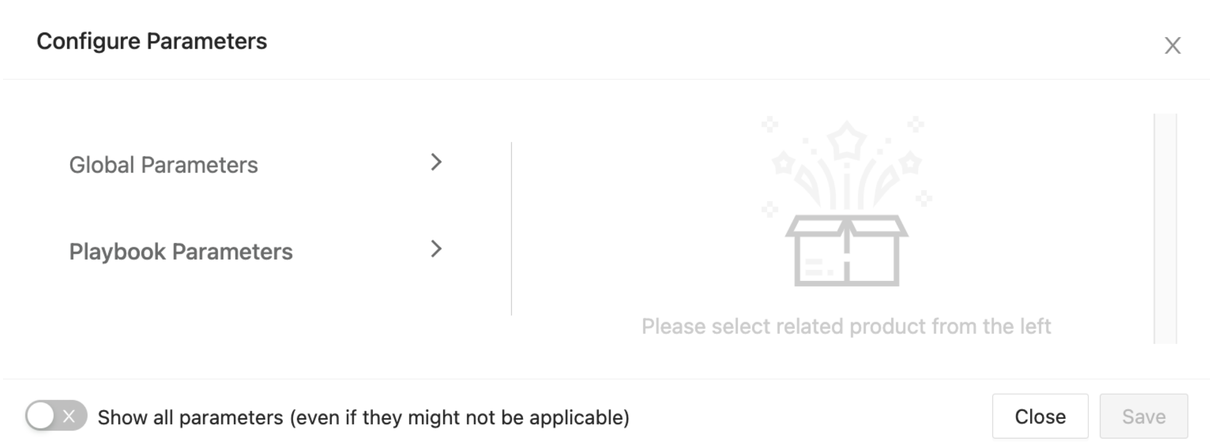
4. Click **Save Data**.

Configuring String Utilities Action



To configure string utilities:

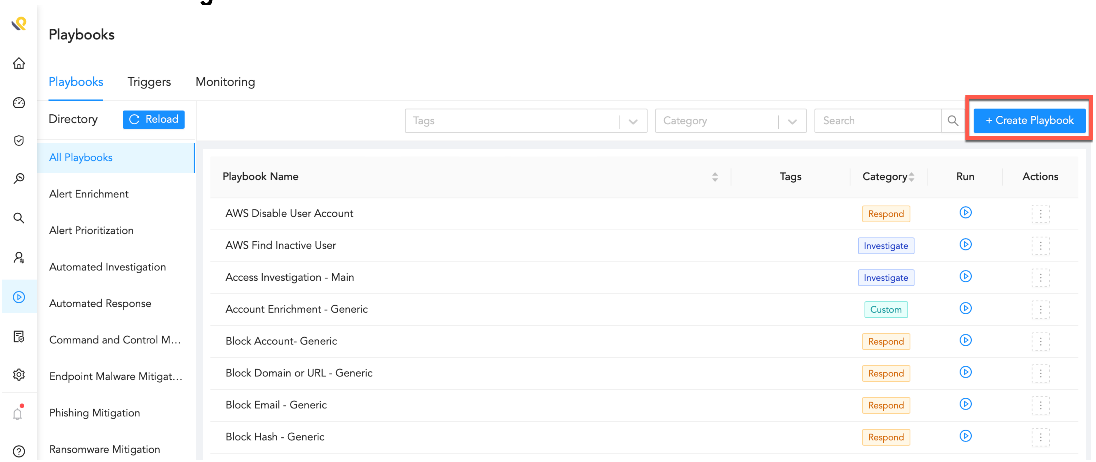
1. Enter an **Action Name** and its **Description**.
2. Enter or select an **Input String**. When you start typing, you can choose one from the auto-fill parameters list.



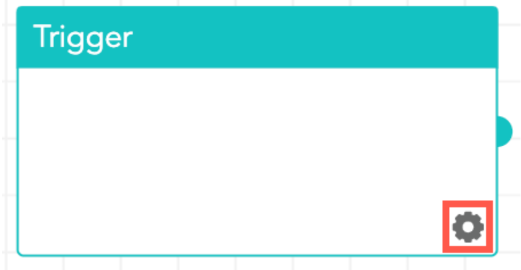
3. Select the **Utility Type** from the drop-down. The utility types are:
   - **Convert Input String to Uppercase**: It converts all input strings into uppercase. Numbers and special characters are not affected.
   - **Convert Input String to Lowercase**: It converts all input strings into lowercase. Numbers and special characters are not affected.
   - **Remove Prefix / Suffix**: It removes a substring from the prefix or suffix of the input string. You can select to remove the substring from the suffix, prefix, or both.
   - **Calculate MD5**: It calculates the MD5 sum of the input string.
   - **Encode text as Base64**: It encodes the input string into Base64 encoding.
   - **Decode text as Base64**: It decodes the input string using Base64 decoding. If the input is not Base64 encoded, the action won't work.
   - **Encode text as URL**: It encodes the input string to be used safely in a URL.
   - **Decode text as URL**: It decodes the previously URL-encoded string. If the input is not URL-encoded, it returns the input text as output.
   - **Escape text as JSON**: It escapes the input string such so it can be used inside a JSON document.
   - **Unescape text as JSON**: It removes the applied JSON escape characters from the input string.
   - **Regular Expression**: It uses the regex string to search and returns results from the input. Selecting the **Get Only First Match** returns the first string. When it's deselected it returns all matches in JSON format.
   - **Replace a Substring of the Input String**: It replaces a part of the input string with a different string.
   - **Remove Whitespaces from Prefix and Suffix**: It removes whitespaces from the start and the end of the input string.
4. Enable **Input Trimming** to remove the whitespaces from the prefix and suffix of the input string.
5. Click **Save Data**.

Adding a Playbook

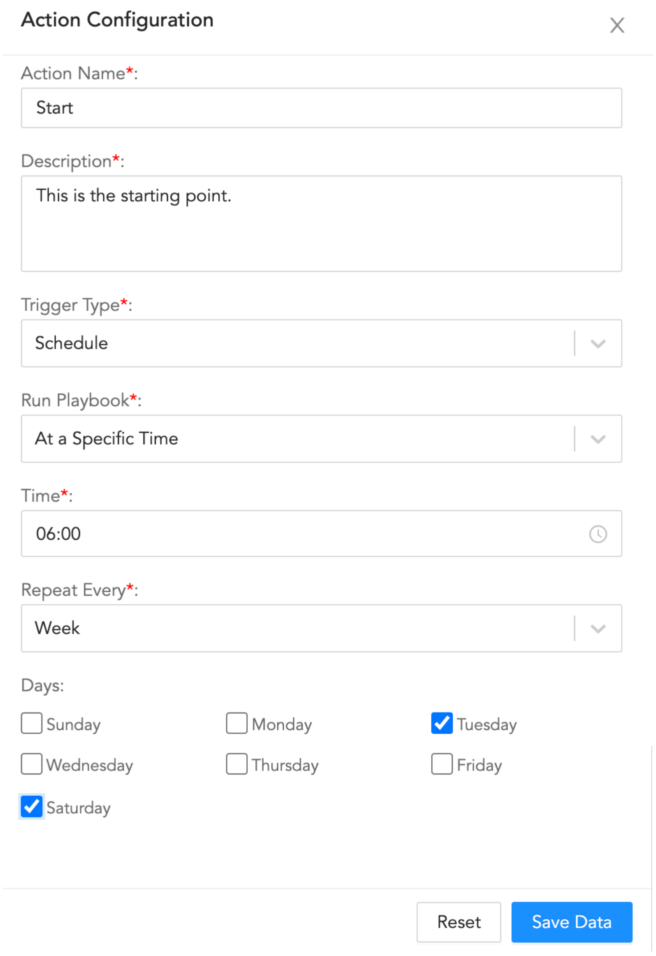
1. Click `Playbooks` in the navigation bar.
2. Click **+Create Playbook**.



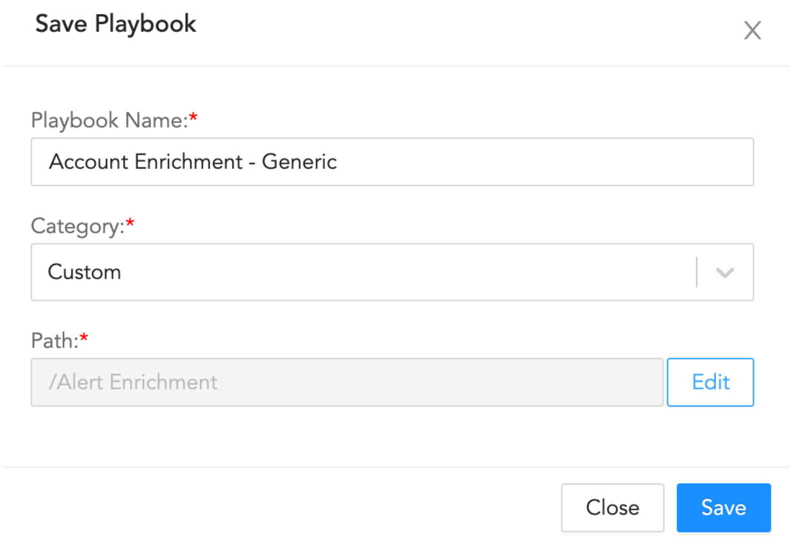
3. Click the **Configure** icon of the trigger block.



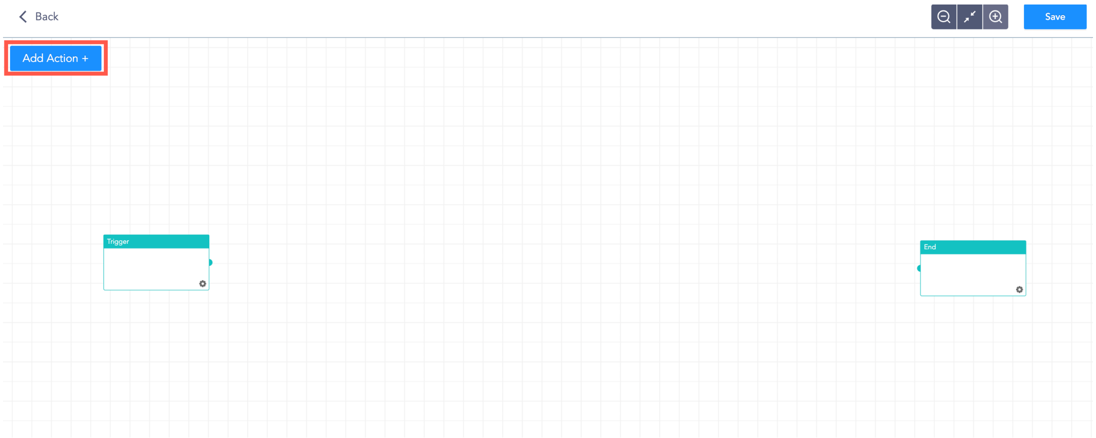
4. Enter an **Action Name** and a **Description**.
5. Select a **Trigger Type**.
   If you select **Playbook** or **SLS SIEM Incident**, enter a list of **Input Parameters**.
   If you select **Schedule**, select a **Run Playbook** time.
   - For **At a Specific Time**, select a **Time** and whether you want the playbook to repeat every **Day** or **Week**.
   - For **Every X Hours**, enter the **Hours**.
   - For **Every X Minutes**, enter the **Minutes**.



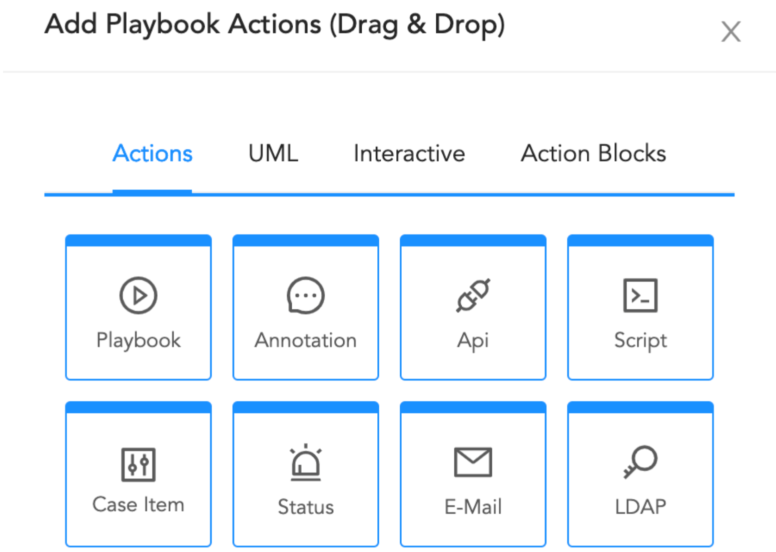
6. Click **Save Data**.
7. In **Save Playbook**, enter the **Playbook Name**, select the **Category** and the **Path**, and click **Save**.
   You can choose to save the playbook after you have finalized the playbook by clicking **Save** on the **Adding a Playbook** page.



8. Click **Add Action +**.



9. Drag and drop a playbook action type.

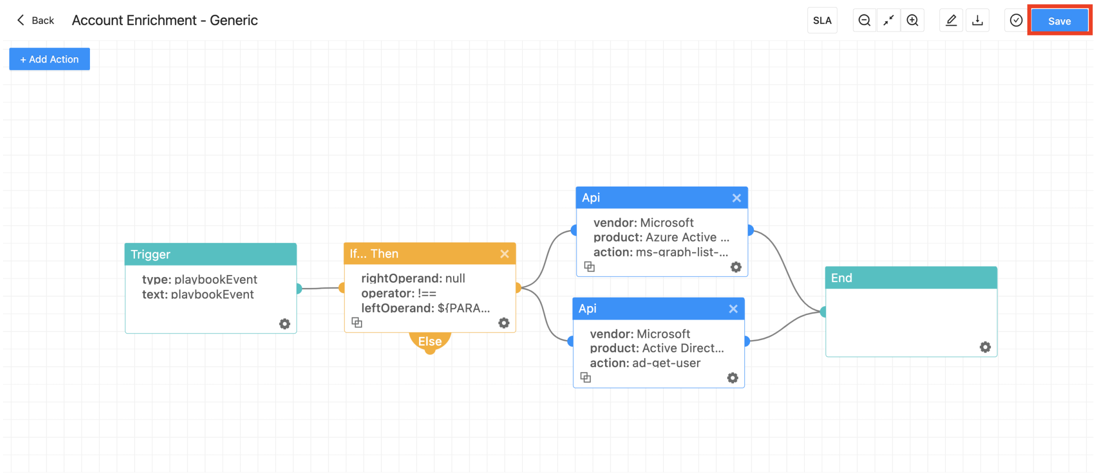


10. Click the **Configure** icon of the block and enter the details.
11. Click **Save Data**.
    Follow steps 8, 9, 10, and 11 to add multiple number of blocks.

> **IMPORTANT**
> Make sure you click **Save Data** every time you update the configurations of a block. Otherwise, the updated data may be lost.

12. Connect a node from a block to a node of another block to connect two blocks.
13. Once you finalize the playbook, connect the final block with the **End** block.

14. Click **Save**.



NOTE

You can clone an action by clicking the ( ) icon.

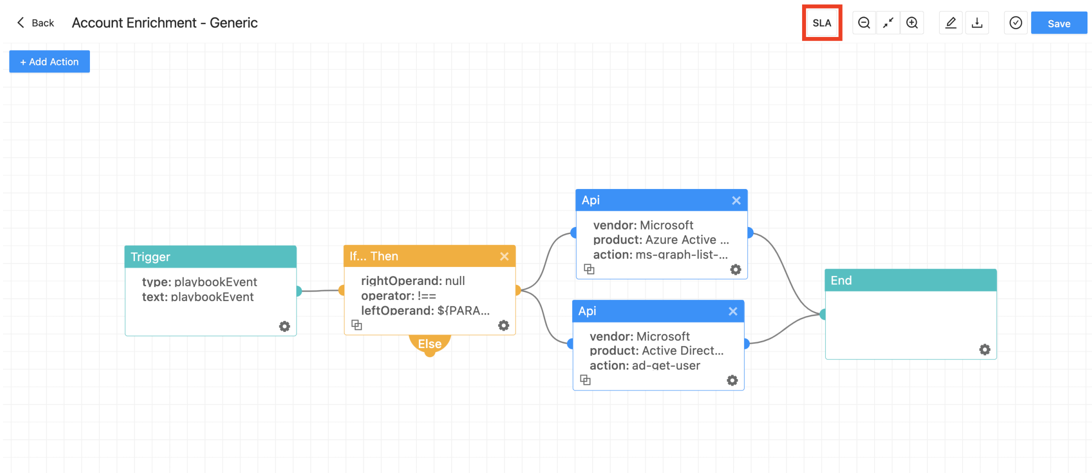
Enabling SLA Support

You can enable SLA support and generate SLA reports by editing playbook configurations. Enabling SLA support allows you to handle the cases created based on the playbook in a time period defined in the SLA configuration.

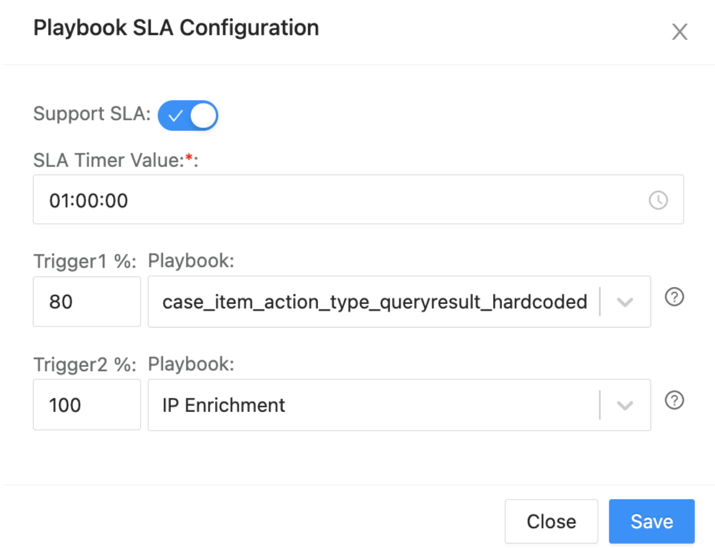
For example, if you add SLA Timer Value as 01:00:00, the case should be handled within one hour. If the first trigger % is 80%, then the selected playbook for the trigger % runs after 48 minutes. If the second trigger % is 100%, then the selected playbook for the second trigger runs after an hour.

To enable SLA support:

1. Click `Playbooks` in the navigation bar.
2. Click **Add New Playbook +**, and add and save the configuration.
   Or, select a playbook from the list in the **Playbooks** page.
3. Click **SLA**.



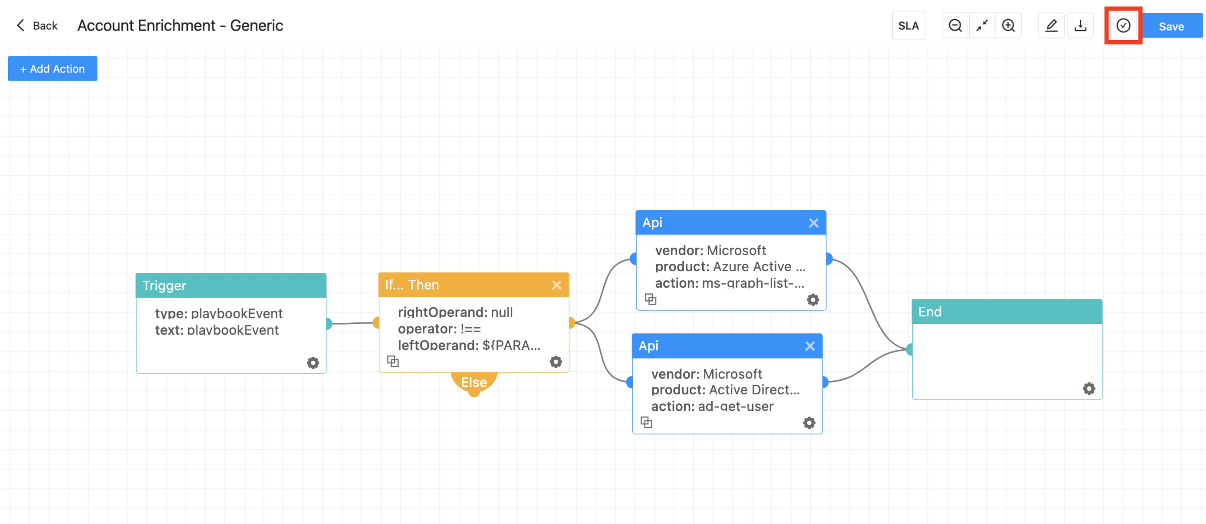
4. Enable **Support SLA**.



5. Select **SLA Timer Value**.
6. Select a **Playbook** and enter its **Trigger %**. You can add another playbook and its trigger %. When the SLA time period defined in the **SLA Timer Value** reaches the trigger %, the selected playbook runs.
7. Click **Save**.

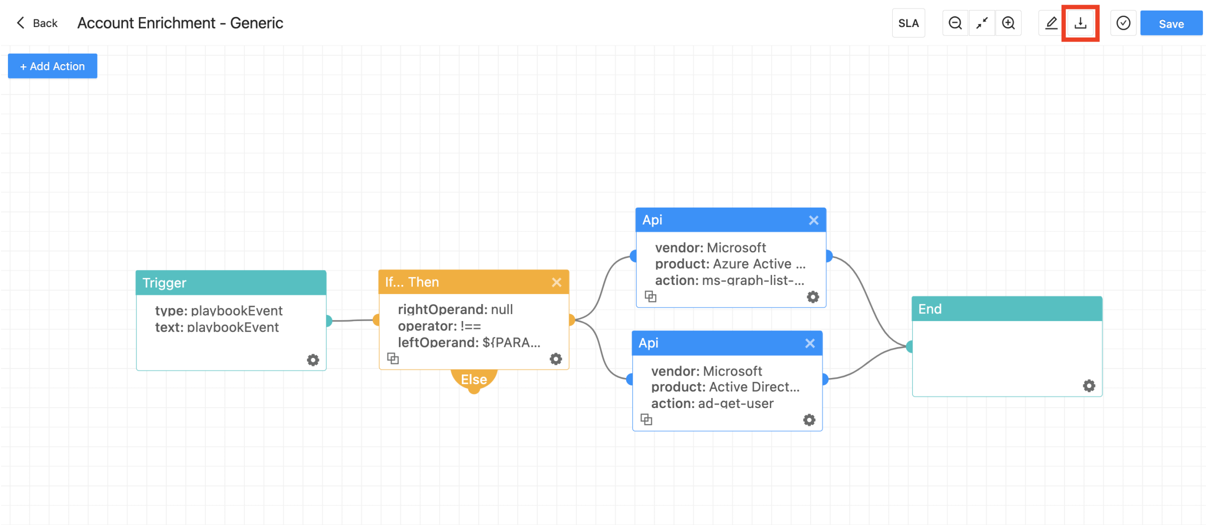
Testing a Playbook

Once you create a playbook, you can test it by clicking **Test Playbook**.



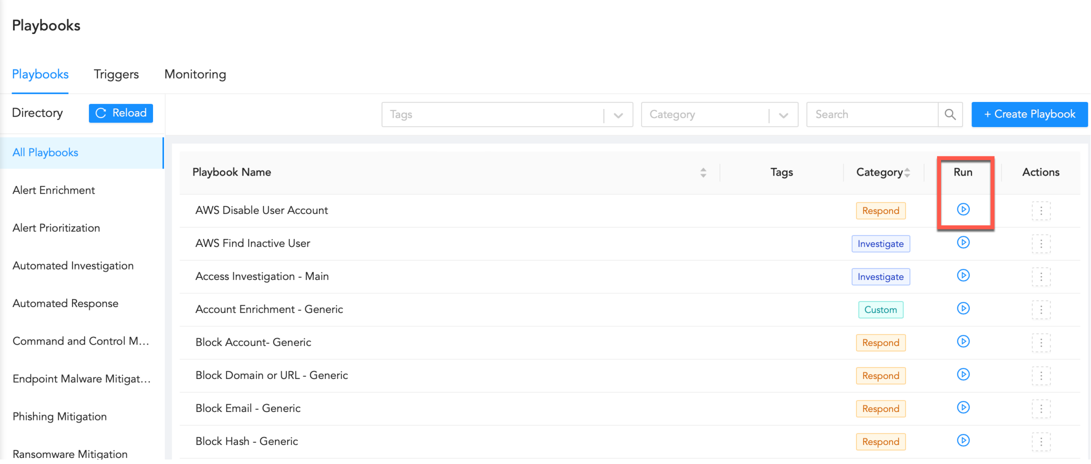
Exporting a Playbook

You can also export the playbook by clicking **Export Playbook**.


Back
Account Enrichment - Generic
SLA
Save
+ Add Action
Trigger
type: playbookEvent
text: playbookEvent
If... Then
rightOperand: null
operator: !==
leftOperand: ${PARA...
Else
Api
vendor: Microsoft
product: Azure Active ...
action: ms-graph-list-...
Api
vendor: Microsoft
product: Active Direct...
action: ad-get-user
End

Running a Playbook

1. Click `Playbooks` in the navigation bar.
2. Search for the playbook by filtering the list using the **Category** or entering the **Playbook Name**.
3. Click the **Run Playbook** icon.

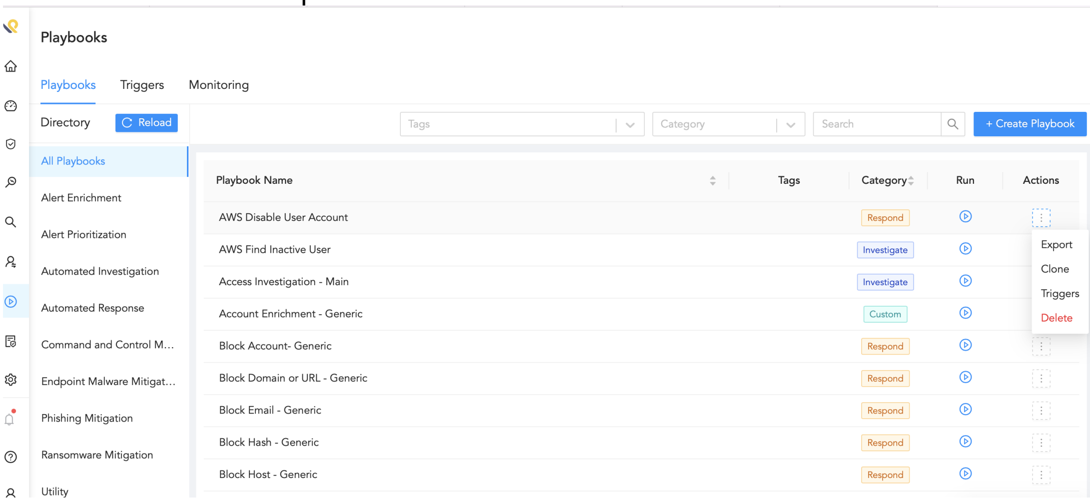


4. Enter the **Playbook Parameters**.
5. Click **Run Playbook**.

Cloning a Playbook

You can clone a playbook to modify it with minor changes and save configuration time.

1. Click `Playbooks` in the navigation bar.
2. Search the playbook by filtering the list using the **Category** or entering the **Playbook Name**.
3. Select **Clone** from the drop-down in the **Actions** column.

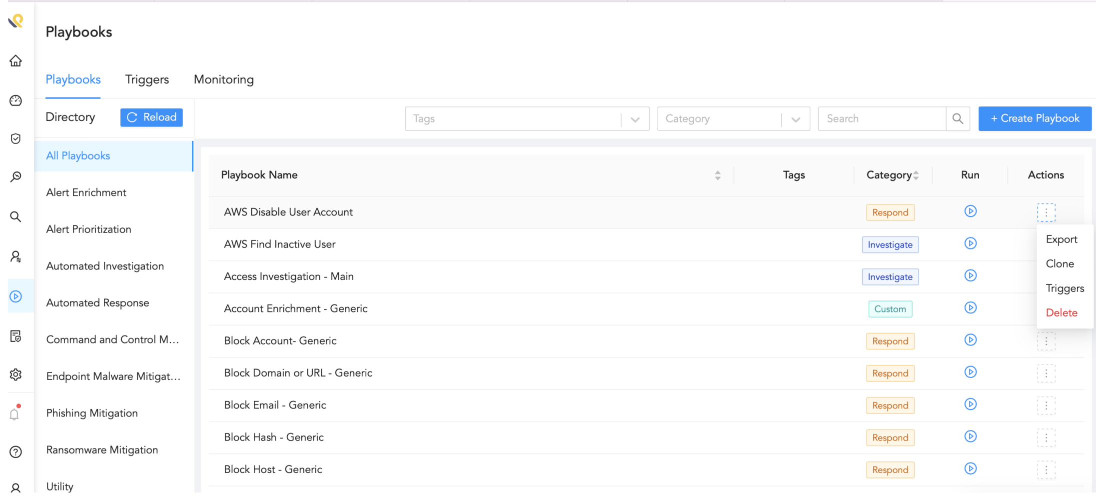


4. Enter a **Cloned Playbook Name**.
5. Click **Save**.
   A copy of the playbook appears in the **Playbooks** page.

Exporting a Playbook

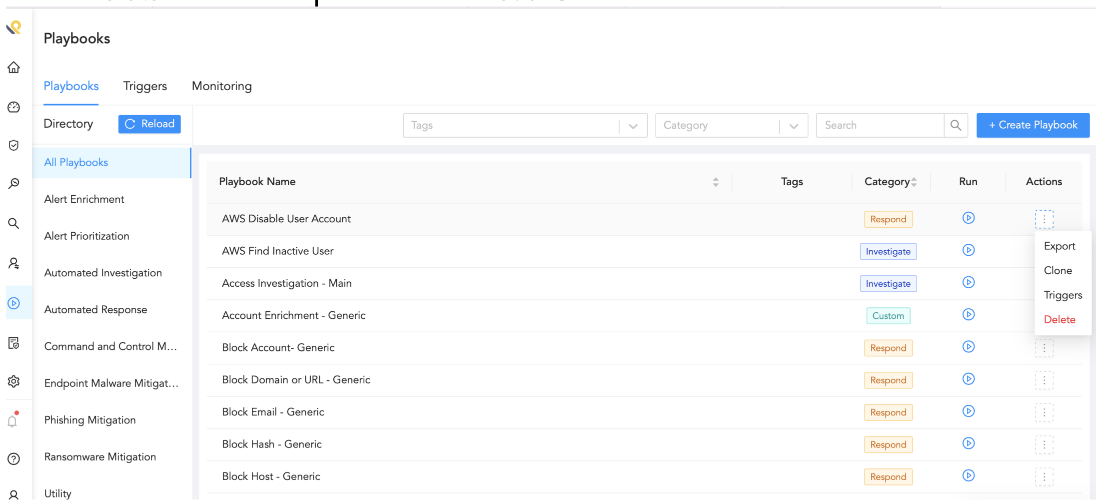
You can export a playbook from one machine and import it in other machines to save configuration time.

1. Click `Playbooks` in the navigation bar.
2. Search the playbook by filtering the list using the **Category** or entering the **Playbook Name**.
3. Select **Export** from the drop-down in the **Actions** column.



Deleting a Playbook

1. Click `Playbooks` in the navigation bar.
2. Search the playbook by filtering the list using the **Category** or entering the **Playbook Name**.
3. Select **Delete** from the drop-down in the **Actions** column.



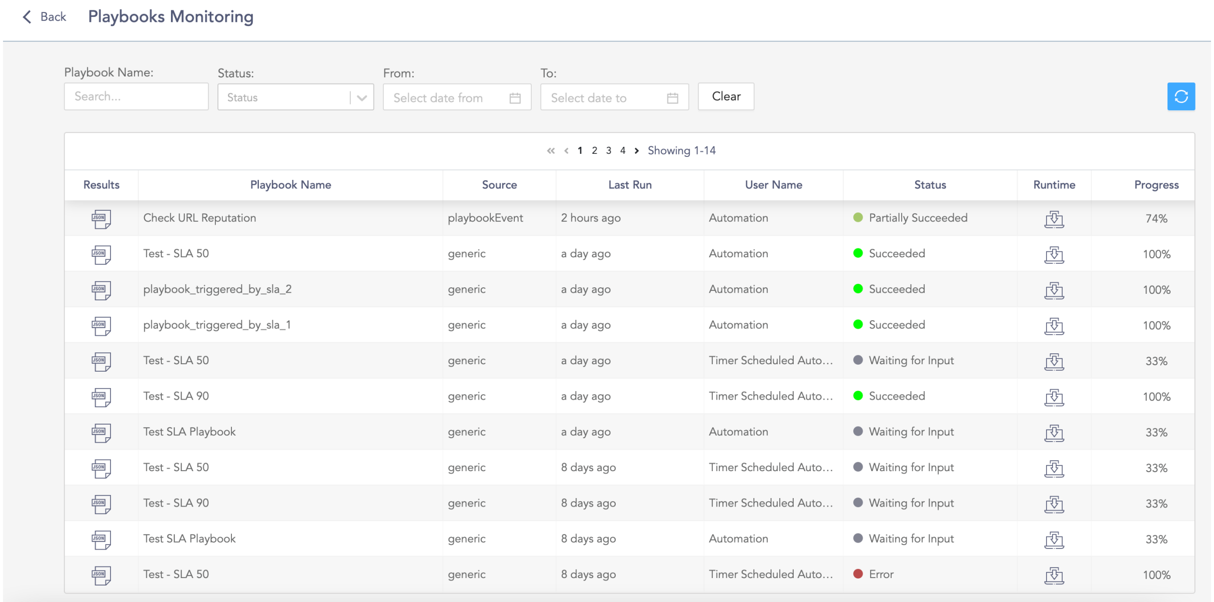
4. Click **Delete**.

Editing a Playbook

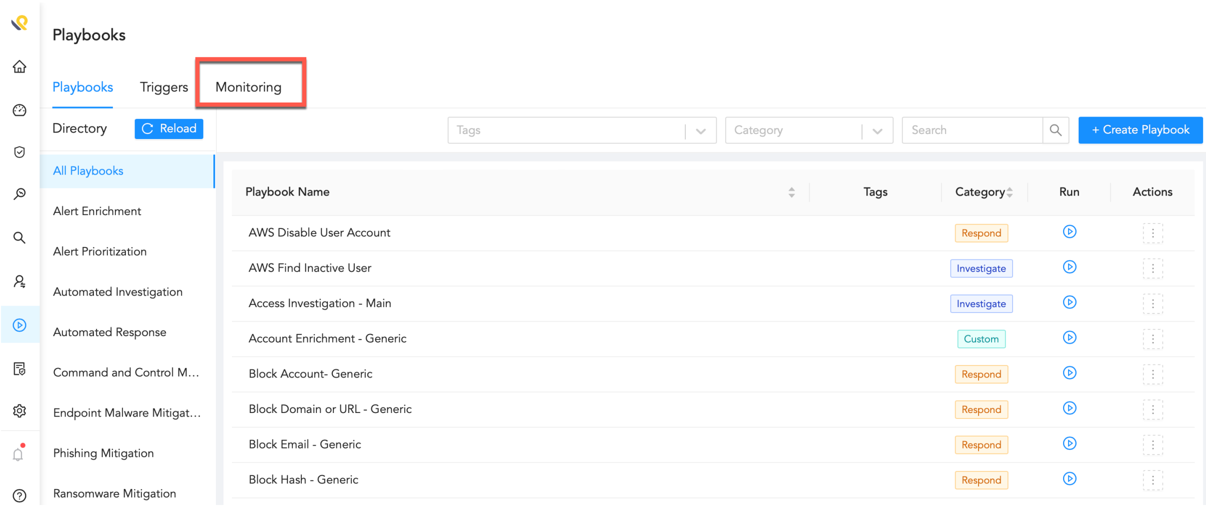
1. Click `Playbooks` in the navigation bar.
2. Search the playbook by filtering the list using the **Category** or entering the **Playbook Name**.
3. Click the playbook.
4. Make the changes.
5. Click **Save**.

Monitoring Playbooks

You can monitor the status of each playbook run and its actions from the **Playbooks Monitoring** page.



In the **Playbooks** page, click the **Monitoring** button to go to the **Playbooks Monitoring** page.



You can filter the results based on the **Playbook Name**, **Status** of the runs, and date-range. You can also refresh the list by clicking the **Refresh** icon.

The table in displays the following fields for each run of the playbooks:

1. **Results** of the run in the JSON format.
2. **Playbook Name**
3. **Source**
4. **Last Run** time.
5. **User Name** of the user who triggered the playbook.
6. **Status** of the run.

7. **Runtime** takes you to the playbook's **Runtime Mode** where you can see the status of all the actions.
8. **Progress** of the run in percentage.
9. Number of **Total Actions** in the playbook.
10. Number of **Completed** actions.
11. **Start** time
12. **End** time
13. **Duration** of the run.

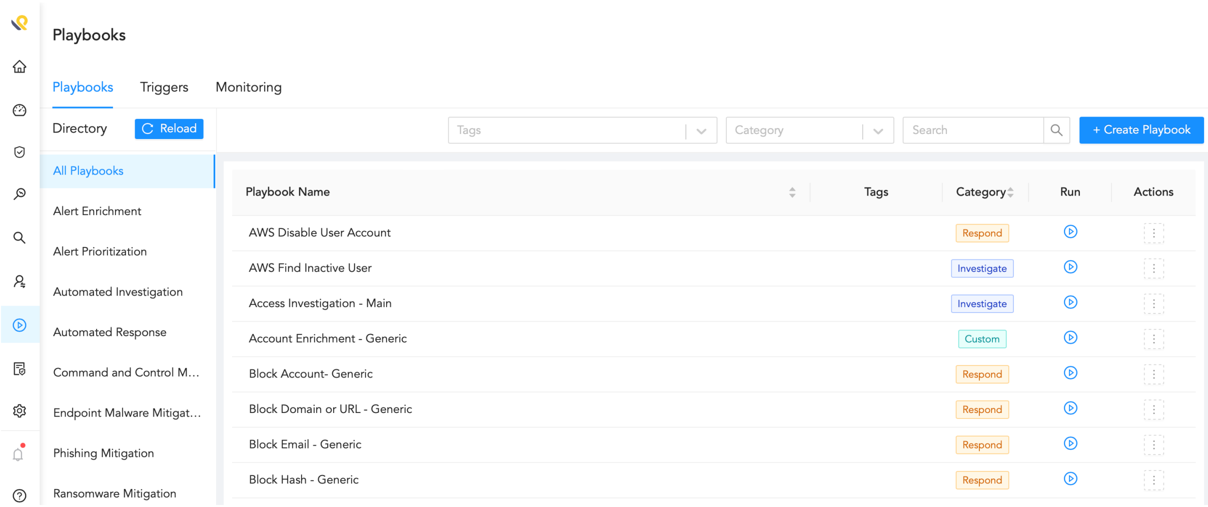
Playbook Triggers

Playbook triggers are the components that run playbooks based on the conditions defined in them. When a case is created from an incident, the system verifies a matching trigger condition. If a match is found, a trigger is started which automates the process of activating the playbook associated with it.

You can manage the triggers from the **Triggers** page.

Go to Navigation Bar and click **Playbooks**.

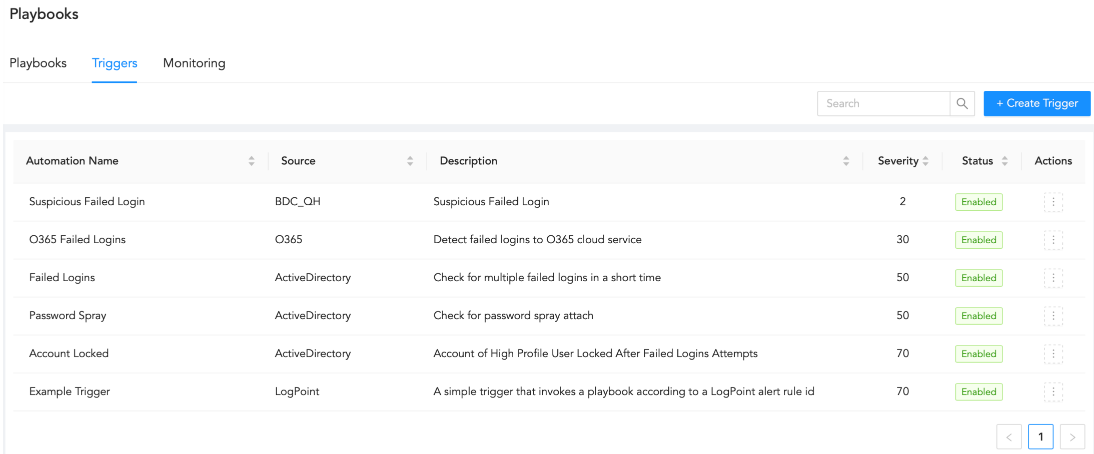
Click **Triggers**.



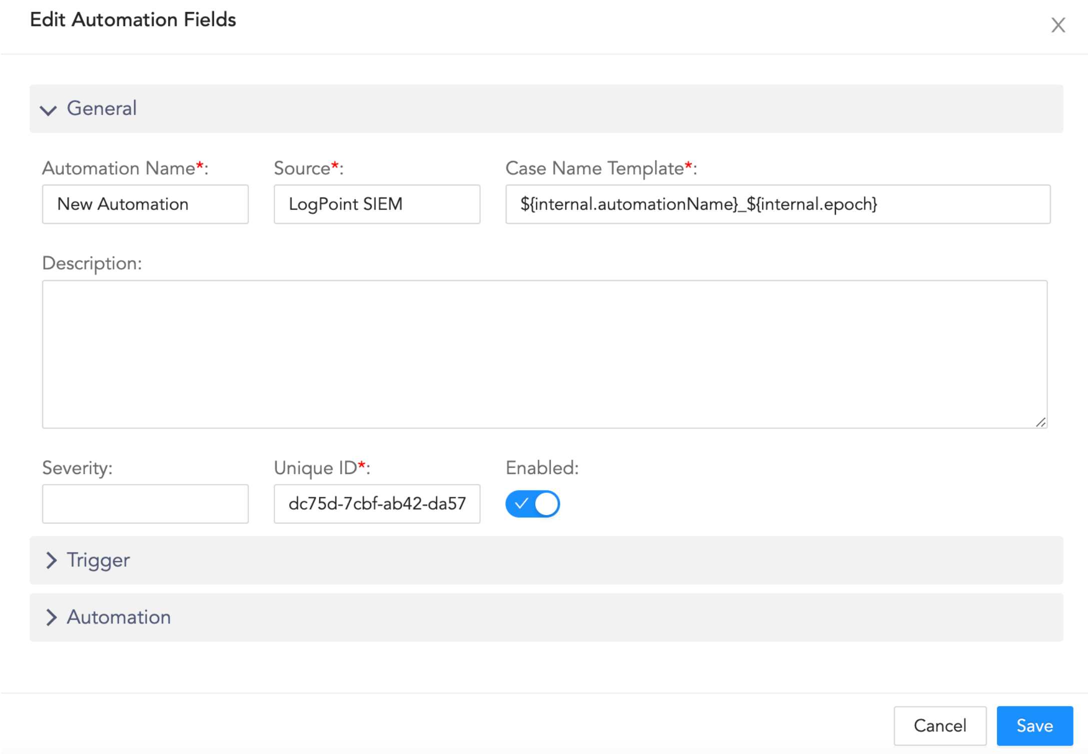
Adding a New Trigger

You can customize a playbook trigger to automate the process of activating the playbook associated with it when the trigger condition is met by adding a new automation.

1. Go to `Playbooks >> Triggers`.
2. Click **+Create Trigger**.

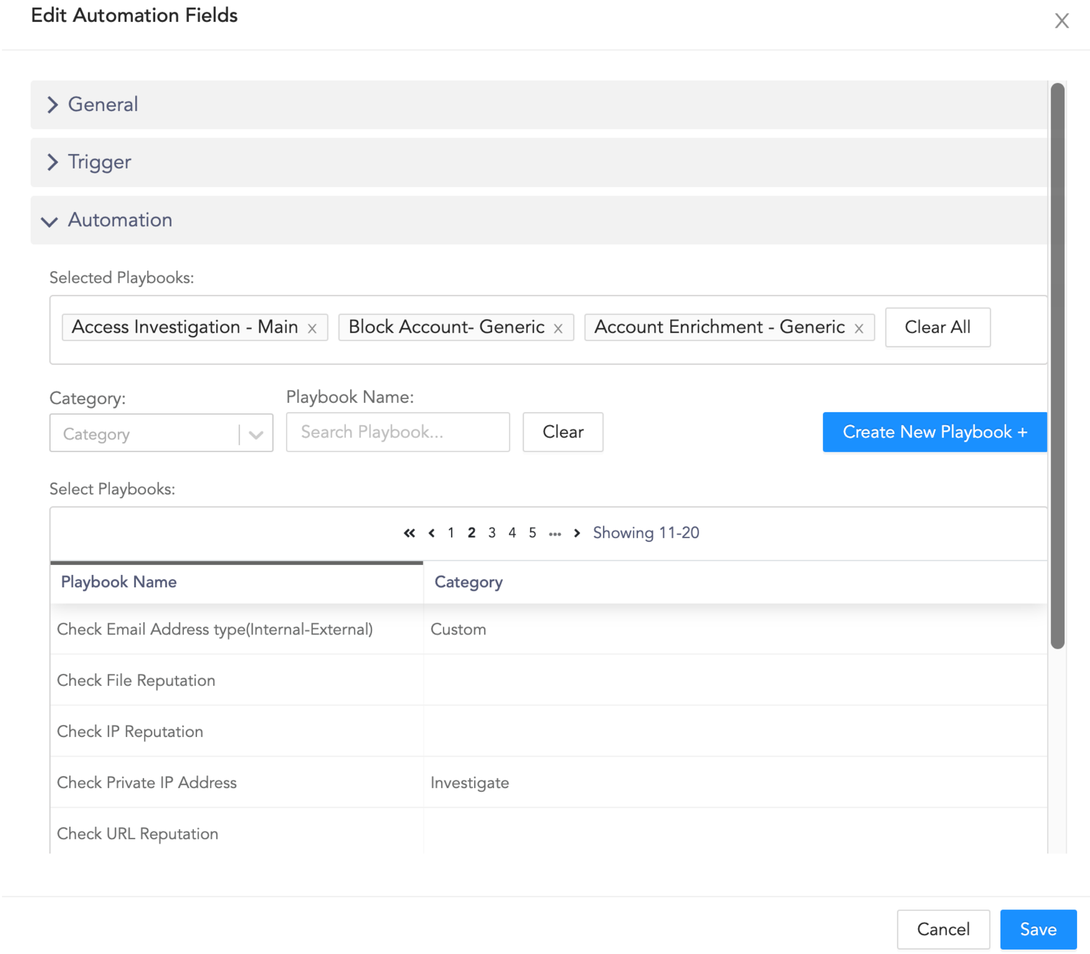


3. In the **General** section,



   1. Enter an **Automation Name**, a **Source**, and a **Case Name Template**.
   2. Enter a **Description**, a **Severity** level, and a **Unique ID** for the automation.
   3. Click **Enabled** to enable the automation.
4. In the **Trigger** section, enter an SQL query in **Trigger**. Every incident that matches the query triggers the playbooks.

5. In the **Automation** section, select the **Playbooks** that must be triggered based on the trigger. You can also configure a new playbook by clicking **Create New Playbook +**.



6. Click **Save**.

Further reading

Additional information and answers to questions you may have about SLS are available in the **Stormshield knowledge base** (authentication required).

documentation@stormshield.eu