# Micro Focus Security
# ArcSight SOAR

Software Version: 3.1

## User Guide for ArcSight SOAR 3.1

Document Release Date: May 2021
Software Release Date: May 2021

## Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

## Copyright Notice

## Trademark Notices

## Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

# Support

## Contact Information

| | |
|---|---|
| **Phone** | A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information |
| **Support Web Site** | https://softwaresupport.softwaregrp.com/ |
| **ArcSight Product Documentation** | https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs |

# Contents

# User Guide for ArcSight SOAR

This guide presents concepts and guidelines to configure and use ArcSight SOAR Capability.

- Introduction to SOAR
- Setting Up SOAR
- Working With Cases
- Automating Response With Playbook
- System Status
- Data Visualization Through Dashboard and Reports

Intended Audience

This user guide is intended for individuals responsible for deploying, configuring and managing the ArcSight SOAR Capability.

Additional Documentation

The ArcSight SOAR documentation library includes the following resources:

- *Administrator's Guide to the ArcSight Platform*, which provides information about deploying, configuring, and maintaining the products that you deploy in the containerized environment.
- *Integration Guide for ArcSight SOAR*, which provides information about deploying and configuring various third party integrations for SOAR Capability.
- *Release Notes for ArcSight SOAR*, which provides information about the latest release.
- *Release Notes for ArcSight Platform*, which provides an overview of the products deployed in the containerized environment and their latest features or updates.
- *Technical Requirements for the ArcSight Platform*, which provides information about the hardware and software requirements for installing SOAR as well as the other containerized capabilities.

For the most recent version of this guide and other ArcSight SOAR documentation resources, visit the documentation site for ArcSight SOAR .

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

For specific product issues, contact Micro Focus Customer Care.

# I Introduction to SOAR

SOAR is a leading **S**ecurity **O**rchestration **A**utomation and **R**esponse platform that combines orchestration of technology and people, and automation and case management into a seamless experience.

By providing tactical automation and orchestration through a single pane of glass, it enables SecOps teams to ramp up their output despite a growing cybersecurity skills gap and an increasing volume of complex attacks and alerts.

This section of the **SOAR User Guide** provides an introduction of the ArcSight SOAR capability.

- Overview of SOAR
- Understanding SOAR Workflow

# Overview of SOAR

ArcSight SOAR delivers an automated incident response solution for repetitive security events and imparts a seamless security management experience by performing faster threat detection and remediation.

The main value proposition of SOAR lies in assisting your organization for human and machine-led analysis of the alerts, and leveraging an automated solution for threat response and remediation.

ArcSight SOAR is fully programmable and can easily integrate with the existing technology stack of your organization. This application is capable to meet security teams' unique needs, and enables multiple forms of automation, analyst augmentation, collaborative investigation and response through an intuitive interface.

## ArcSight SOAR Features

Some of the key features of ArcSight SOAR includes:

**Case Management**: ArcSight SOAR enables you to manage and collaborate data to resolve case efficiently on a single pane of glass. The case management helps streamline investigations and expedite incident resolution.

**Consolidation**: You can aggregate alerts from different sources based on configured time-span or common conditions. This helps in gathering all the correlated information for the suspected threat and further helps in finding the optimized solution for incident handling.

**Orchestration**: The automated solutions provided by SOAR can seek information from the SOC or pass the control to the security operations center (SOC) for decision making and then take the control back to automation. Depending on the case scenario, ArcSight SOAR can orchestrate the control flow from automation to human analyst.

**Enrichment**: SOAR uses enrichment feature to gather additional information about the event contexts. These additional insights act as guides to carry on the detailed threat investigation.

**Automation**: SOAR leverages both fully automatic and semi automatic solution for threat remediation and response. You can automate mundane repetitive tasks, prioritize events and streamlines security processes to deliver accelerated incident response.

**Response**: SOAR automation can execute protective actions, stored in playbooks, to prevent any threat impact to your organization. This capability offers unique solution to respond to events in a quick and effective manner.

**Reporting and Analytics**: You can generate reports to view detailed information about cases. SOAR offers a pre-defined report template for data presentation or you can create your own template to specify which data you want to include. To analyze the data further, you can view all data statistics in the form of tables and charts in Dashboard.

## Challenges Faced by Organizations:

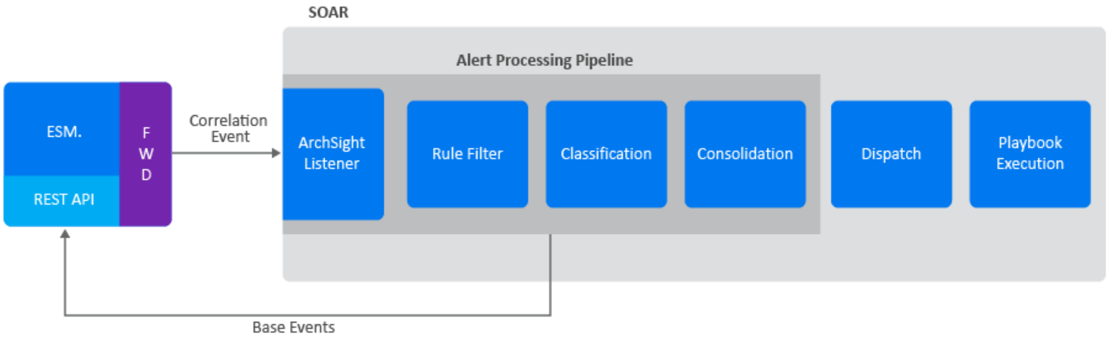
Existing cybersecurity landscape presents lots of challenges to the organizations including:

- **Attack speed**: Attacks keep getting faster every day. Modern attacks are almost entirely automated.
- **Attack volume**: An average organization gets more than 300 cyber alerts per day (IDC). Investigating and responding to an alert takes around 8 full hours.
- **Disparate tools**: SOC analysts use 15- 20 different tools throughout their daily jobs to investigate and respond to attack alerts. Tier-1 analysts are not able to investigate (and use the tools) and they are merely expensive human filters.
- **No single pane of glass**: There is no trail of investigation and response activities and there isn’t a proper answer to “who is working on which case and doing what” at any point in time on the SOC floor.
- **Lack of KPIs and metrics**: As most SOCs lack the practice of investigation and response, it is almost impossible to come up with relevant, easy-to-collect KPIs and metrics. Getting a grip on who needs more training, SLA adherence, incident backlog trends, etc. is difficult and intuitive-only.
- **Cyber Security Skill Shortage**: Currently, the cybersecurity sector is facing a severe expert shortage. Currently, there are 350,000 vacant positions in the U.S. alone and the industry shortfall is expected to rise to 3.5 million cyber expert vacancies.

# Understanding SOAR Workflow

SOAR receives alerts from different sources. These alerts are processed to form cases. The newly created case are dispatched to SOCs. Most of the cases can be resolved automatically by executing associated playbooks, however, at times human interventions are needed for decision making.

Following figure presents a general workflow of ArcSight SOAR:



1. "ESM Sending Alerts to SOAR" below
2. "Processing Alerts" on the next page
    a. Receiving Alerts Through ArcSight Listeners
    b. Defining Action Plans by Rule Names
    c. Classifying Alerts
    d. Consolidating Alerts to form cases
3. "Dispatching cases" on the next page
4. "Automating case Handling by Playbooks" on page 15

## ESM Sending Alerts to SOAR

The ArcSight ESM forwards alerts and their respective correlated events to SOAR to identify, analyze and resolve a probable attack. To send alerts to SOAR, ESM must be integrated and configured as an alert source on the SOAR platform. SOAR receives alerts with rule names that were defined at the ESM. The rule names are used for alert classifications during case creation.

When an alert is created, the ArcSght ESM stores various base events that produced that alert. For example, if a **Remote Port Scan Detected** alert is created, the ESM will store a number of events, each with a separate log entry received from systems under attack or probe. SOAR gets these base events since they contain useful information (for example time of each event, attacker username and attacker remote address) through correlated events. These information are displayed on the case page, created and bound with the respective alert. The correlated events are also helpful during defining the scope items for the alert analysis.

## Processing Alerts

After integrating with ESM, SOAR follows a set of procedures for alerts processing as follows:

**Receiving Alerts through ArcSight Listener**

After configuring ESM as an alert source, the ArcSight Listeners starts listening to the configured ports and get alert messages. These alert messages are usually brief including useful information, for example the type of alert, time of event, count of base events that produced the alert, and the severity of the alert. Context of the alert messages depends on the alert source and the rules configured.

**Defining Action Plans by Rule Names**

A rule name is configured as pre-processor rules in the ESM for tagging and forwarding the base events to SOAR. These rule decides the action plans for the alerts. Based on the directions imposed by rules an alert can be considered as a threat alert or a normal event.

**Classifying Alerts**

Depending upon the conditions directed by rules, a label is added to the alerts. The labeling helps in selecting the appropriate playbook/s for the case handling and response.

**Consolidating Alerts to form cases**

Depending upon the configuration settings, different correlated alerts are consolidated to form cases. At this point, the ArcSight SOAR decides to consolidate alerts to form a new case or the respective alert can be added to a pre-existing case.

## Dispatching cases

When a new case is created, a case severity is assigned to the case, based on the severity mapping of the alert source. After the severity assignment, the case is assigned to a user or a user group. The dispatching of the case is done by running **case Dispatch Playbook**. If the playbooks cannot find an assignee, SOAR leaves the case as unassigned. Running these playbooks may find more than one assignee, but SOAR only selects the first one.

Dispatch playbooks might also change case’s severity or add watchers or labels to the case.

# Automating case Handling by Playbooks

After a case is created and dispatched, SOAR runs a playbook/s with matching conditions as defined during alert consolidation. All matching playbooks are executed sequentially and in their rank order. Higher rank playbooks are executed earlier.

Each executed playbook can run a number of enrichment operations and queue actions in an arbitrary order. Enrichments are synchronous, that is, playbook execution waits for their completion before continuing with the next operation.

Actions are always asynchronous. There is a separate queue of actions, manageable in the **Action and Rollback Queue** tab. Completed actions are moved from the queue to the **Alerts** tab of **Status** menu.

A completed action can be either automatically or manually rolled back, if the action's capability supports rollback operation.

If playbook contains a case close element, SOAR automatically closes the case, otherwise, case remains open after all the tasks are completed.

# II Setting Up SOAR

ArcSight SOAR supports customization to suit your organizational requirements. This section of the **SOAR User Guide** presents a detailed description on configuring ArcSight SOAR capabilities.

# Setting Up SOAR to Receive Alerts

Select **SOAR** > **Configuration**.

The SOAR offers an end to end solution to provide automated response to cases. To ensure seamless security resilience, SOAR solution must be configured to receive alerts from disparate security tools and platforms.

You must create a user credential in the **Credential** tab to communicate with other components. After a credential is created, you must add the alert source in the SOAR platform. Every alert in SOAR is generated through a rule in the alert source and whenever an alert is received by SOAR, it is received with the rules that were used to process the alerts.

After the Alert source is added, you must integrate the component with SOAR in the **Integration** tab.

You can enable additional configuration parameters for enrichment or to forward events by other component on a specific port number or any other configuration in the **Parameters** tab.

Creating User Credentials

Configuring Alert Source

Integrating Other Components with SOAR

Configuring Additional Parameters

## Creating User Credentials For Integration

Select **SOAR** > **Configuration** > **Credential**.

SOAR listens to alerts, forwarded from different components to identify a threat possibility. To receive an alert, SOAR must have integration with other components. The **Credentials** tab allows you to create user credentials to interact with other components during the integration procedure.

The Credentials tab displays a list of user credentials. You can view the credential names, the last modification date and the name of the modifier.

### Searching a Credential

You can search a specific user credential, through the **Search** option. Click the ⚙▾ button next to search, allows you to view search results based on **ID, Credential Name** and **Last Modified By**.

### Creating a User Credential

Click the **+Create Credential** button to create a new user credential. In the **Credential Editor** window, specify the details for following fields:

**Type**: Select <Internal Credential, External Condition>. **InternalCredentials** are stored in SOAR's database table. **External Credentials** are stored in integrations such as Cyberark Central Credential Provider.

**Name**: Specify a name for the credential set. The name that you create here is displayed on the **Credentials** field during alert source and integration configuration. You must select this name to ensure that SOAR communicates with other components through this name identity.

**Username**: Specify a username for the credential set.

**Password**: Specify a password for the credential set.

**Private Key**: Specify a private key for the credential set, if needed.

### Editing and Deleting a User Credential

You can edit an existing user credential by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Credential Editor** window is displayed. Specify the values in editor window as per your requirement and click **Save** to modify.

You can delete an existing credential by clicking the **Delete** button under the **Actions** column.

> You cannot delete a user credentials that is used in the integration with other components.

## Configuring Alert Source

Select **SOAR** > **Configuration** > **Alert Source**.

An alert source must be configured on SOAR to ensure seamless reception of the correlated alerts.

The **Alert Source** tab allows you to create new alert source configurations, displays a list of existing alert source configuration and options to modify the existing alert source configuration.

### Creating an Alert Source Configuration

Click **+ Create Alert Source Configuration** button to create a new alert source configuration. In the **Alert Source ConfigurationEditor** window, specify the details for following fields:

You might see differences in the fields of this editor for some of the alert source types (as you select it from the Type combo box list).

| Value | Description |
|---|---|
| Name | Name of the alert source |
| Type | Type of the alert source. It could be one of the alert source types listed above. |
| Address | IP address of the alert source to which SOAR connects when it wants to get data. |
| Key | A unique, auto-generated key which is used as a shared token to make sure the remote IP addresses (“Allowed IP addresses”) are correct. The value of this field must be included in the messages coming from those remote IP addresses. |
| Allowed IP addresses | Any alert coming from the IP addresses specified in this field will be processed and others will be discarded. For most alert source types, SOAR opens a TCP port (or a web service API endpoint) and waits for some alert sources to connect. This field along with the “Key” field is to improve your system’s security. The combination of these two fields prevents a potential attacker from feeding your system with fake events and causing damages. |
| Alert Severity | Severity of alert sources. Define the severities according to the priorities of tickets produced by the alert source. Use the **Add** button to create each severity. While adding the severities, you can specify the default severity by selecting the checkbox under the **Default** column. |
| Configuration Content | This area displays default configuration definitions for some type of alert sources, such as IBM Security QRadar but it is not required for many alert sources. It depends on which alert source you are trying to interact with. If there are some required data for the alert source configuration, this area shows a template and ask you to edit it if needed. |

| Value | Description |
|---|---|
| Credential | Credentials defined on the system to be used for the alert source. |
| Show alert parameters by default | Shows the default alert parameters defined for the selected device type on the system. |
| Trust Invalid SSL Certificates | Select if you want SOAR to connect anyways to an alert source ignoring warnings for untrusted SSL certificates. You may have installed alert sources with self-signed SSL certificates, which SOAR does not trust and deny connecting by default. Therefore, if you do not select this checkbox, SOAR still gets the brief alert, but cannot get more details on the alert. |

You can click **Test** to verify if the configuration is correct.

### Editing and Deleting an Alert Source Configuration

You can edit an existing alert source configuration by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Alert Source Configuration Editor** window is displayed. Specify the values in the window as per your requirement and click **Save** to modify.

You can delete an existing alert source configuration by clicking the **Delete** button under the **Actions** column.

For detailed information see the related Integration Guides.

### Configuring SOAR as an Alert Source

ArcSight SOAR creates internal alerts for some cases, such as when an action is failed permanently or an integration becomes unavailable because its firewall is not reachable. These internal alerts are generated for the event types including : action and rollback failures, auto-enrichment failures, when an integration becomes offline/online, breach of ticket resolution/first response SLAs, and custom/arbitrary alerts created by playbooks.

## Integrating SOAR With Other Components

Select **SOAR** > **Configuration** > **Integrations**.

The SOAR is integrated with other platforms and components to receive alerts. This procedure ensures streamlining the alert inflow and powers automation.

The **Integrations** tab allows you to create, manage and configure security integrations and platforms.

A list of integrations configured previously along with their action and rollback queue sizes, and their availability statuses are displayed on the **Integrations** page.

## Searching an Integration

You can search a specific integration, through the **Search** option. Click the ⚙▾ button next to search, to view search results based on **ID, Name, Type, Address, Availability, Last Modified By, Modification Date, Action Queue Size, Rollback Queue Size** and **Actions** filters.

## Creating an Integration

Click the **Create Integration** button to create an integration. In the **Integration Editor** window, specify the details for following fields:

| **Fields** | **Description** |
|---|---|
| Name | Name of the Integration. |
| Type | Type of the Integration. |
| Address | IP address of the integration. |
| Configuration | Depending on the integration type, you might select and enter various configuration commands on the black window. See the below Changing Integration Configuration section for details. |
| Credential | Credentials to be used to connect this integration. Credentials are defined in **Credentials** menu. |
| Trust Invalid SSL Certificates | Select if you want SOAR to connect to an integration ignoring warnings for untrusted SSL certificates. |
| Require Approval From | When a user is selected here, action items need to be approved by this user before executing it for integrations. |
| Notify | When a user is selected here, actions done will be notified to this user. |
| Tags | It is used to group integrations. This allows creating actions on a number of integrations having the same tag. You might want to create an action for all integrations that have a specified tag such as “block offender IP address on all firewalls that are used to manage WiFi networks”. |

You might prefer to specify some more parameters for some specific integrations. Select the **Show Additional Parameters** checkbox located at the very bottom of the **Integration Editor** to the additional configuration.

The descriptions for these additional parameters are as follows:

| Value | Description |
|---|---|
| Maintenance | Maintenance is supported by all integrations to which SOAR connects using the SSH protocol. It is essentially a generic SSH integration action script. It is best used in conjunction with Check Point Firewall integration for activating or installing a previously saved but not activated firewall policy. You can select a maintenance frequency or type your own cron job (for a scheduled maintenance) by selecting the **Custom Cron Value** option in the combobox. |
| Host Key | SSH public key of the remote integration. It is only used for integrations connected with SSH. If an SSH key is provided, then it will be validated using the specified key. This check is required to prevent man-in-the-middle attacks. |
| Batch Size | SOAR can send multiple action queue items to the integrations in a single connection. This field specifies the maximum number of action queue items that will be sent in each execution. For example, if you provided **Batch Size** as **10** and there are 25 action queue items waiting for that integration, then SOAR will send these items in 3 separate execution (10 + 10 + 5). Its default value is 1. This is a feature to avoid causing excessive system load on remote integrations when executing actions. A bigger batch size might create overhead on the integration thus failing all entries. So, you need to be careful when increasing this value. |
| Max Postpone | Maximum number of action retries. If an action cannot be executed for any reason, such as connection failures, authentication problems or another SOAR internal problem, it will automatically be retried later. There are a number of global configuration parameters to configure how and when it will retry, but, after a number of retries specified in this field, SOAR will give up and mark the action as failed. Default value is 6 (in hours). |
| Connection Limit | Maximum number of concurrent connections for the integration. Default value is 5. |
| Max Action Retry | Maximum action retry count for the integration. Default value is 5 |
| Max Rollback Retry | . Maximum rollback retry count for the integration. Default value is 5. |

## Editing and Deleting an Integration

You can edit an existing integration by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Integration Editor** window is displayed. Specify the values in editor window as per your requirement and click **Save** to modify.

You can delete an existing integration by clicking the **Delete** button under the **Actions** column.

For detailed information see the related Integration Guides.

## Testing Integration

Click **Test** to verify the integration configuration.

When you click the **Test** button, it triggers the availability check for integration and if anything fails, a detailed error message is displayed. For example, in the case of a Check Point Firewall integration, SOAR needs a credential to work with the integration. If a credential is not available, an error message is displayed.

If the administrator of the remote integration accidentally deletes the credential that SOAR uses, SOAR will no longer be able to create actions on the integration. In this case, the integration is shown as offline (and an internal alert is created) and the error message is logged into the error log.

You can click **Test** button to see the error message.

A successful test marks the integration as **online**.

## Flushing Queues

To flush the ques, select **Flush Queue** button under the **Actions** column of the integrations list. Following is the basic flow in SOAR:

1. Alert is received.

2. Matched playbooks run.

3. Action and rollback queue objects are created (waiting for execution in the queue).

4. Actions/rollbacks in the action/rollback queues are executed and saved.

When you click the **Flush Queue** button, SOAR starts executing actions/rollbacks without waiting for the execution scheduler (which consumes action/rollback queue objects).

# Configuring Additional Parameters

Select **SOAR** > **Configuration** > **Parameters**.

You might require performing some additional configuration, depending on the component or platform integration requirements.

The **Parameters** tab displays a list of parameter that can be used for the additional configuration. For more information about additional configuration for integrations, see the respective Integration Guides..

### Searching a Parameter

You can search a specific parameter, through the **Search** option. Click the ⚙▾ button next to search, to view search results based on **Parameter Name, Parameter Value, Default Value, Description, Last Modified By, Modification Date** and **Actions**.

### Editing a Parameter

You can edit an existing parameter by clicking the **Edit** button under the **Actions** column. In the **Configuration Editor** window, specify the details for the following fields:

**Parameter**: Specify the parameter name.

**Value**: Specify the parameter value.

**Description**: Specify the parameter description.

**Default Value**: Specify the default value of the parameter.

> You can not delete a parameter as it can be used in several integrations.

## Configuring Case States

Select **SOAR** > **Configuration** > **Case**.

SOAR enables you to customize case states such as statuses, severities, types and labels as per your requirement. You can configure multiple options to define case states to suit your requirement.

When you click **Cases** page, you can view the following sub tabs:

- Statuses
- Severities
- Types
- Labels

# Configuring Case Statuses

Select **SOAR** > **Configuration** > **Case > Statuses**.

You can configure the status options for a case. For example, you can define an case status as open, if the resolution procedure is ongoing for the case or closed, if it is already resolved, depending on your requirement. To bring in more clarity to the case status, you can associate colors with each case status that you create.

When you click **Statuses** page, a list of predefined case statuses is displayed.

## Searching a Case Status

You can search a specific case status, through the **Search** option. Click the ⚙▾ button next to search, to view search results based on **Name, Global, Open, Close, Color** and **Actions** of the case status.

## Creating a Case Status

Click the **+Create Status** button to create a new case status. In the **Case Status Editor** window, specify the required details in the following fields:

| Value | Description |
|---|---|
| Status Name | Name of the case status. Provide a short and explanatory name, such as, Open, Closed, InProgress. |
| Open Status | This allows to select whether the case will be in an open or closed state during the case progress. For example, it is in open state when the case is re-opened, or in closed state when the case is expired. |
| Colors | Select the color for the status from the suggested color options. |

## Editing and Deleting a Case Status

You can modify an existing case status by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Case Status Editor** window is displayed. Specify the values in editor window as per your requirement and click **Save** to modify.

You can also remove an existing case status by clicking the **Delete** button under the **Actions** column.

# Configuring Case Severities

Select **SOAR** > **Configuration** > **Case > Severities**.

SOAR enables you to create your own case severity categories to suit your requirements. You can also set ranks to these severity categories as per the case handling priority.

When you click **Severities** page, a list of case severity is displayed.

## Searching a Case Severity

You can search a specific case severity, through the **Search** option. Click the ⚙▾ button next to search, to view search results based on **Name, Response Time, Resolution Time, Color, Rank** and **Actions** filters of the case severity.

## Creating a Case Severity

Click the **+Create Severity** button to create a new case severity. In the **Severity Editor** window, specify the required details in the following fields:

| Value | Description |
|---|---|
| Name | Name of the case severity. |
| Color | Select a color from the color palette. |
| Response/Resolution Time | These fields are optional and they provide what should be the response and resolution periods for a case of a specific severity. For example, for the cases of severity **Critical**, you might require shorter times for response and resolution. |

When you select the **Show Additional Parameters** checkbox, following additional fields are displayed:

| Parameter | Description |
|---|---|
| Resolution breach alert frequency time units | It is the frequency of notifications which are sent after the resolution of the cases of this severity has passed the **Resolution Time**. |
| Response breach alert frequency time units | It is the frequency of notifications which are sent after the response time for cases of this severity has passed the **Response Time**. |
| Response Near Time | It is the time left for Response SLA time at which SOAR sends a notification. |
| Resolution Near Time | It is the time left for Resolution SLA time at which SOAR sends a notification. |

## Editing the Rank of a Case Severity

You can reassign rank to the allotted severity. Click **Edit Rank** under **Actions** column and set the rank for the severity in the **Rank** column.

## Editing and Deleting a Case Severity

You can modify an existing case severity by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Case Severity Editor** window is displayed. Specify the values in editor window as per your requirement and click **Save** to modify.

You can also remove an existing case severity by clicking the **Delete** button under the **Actions** column.

# Configuring Case Types

Select **SOAR** > **Configuration** > **Case > Types**.

The SOAR provides you an option to assign case types to specific types of cases with special backgrounds. Typically, a case type is assigned when the case goes through the playbooks. Depending on the playbook outcome, a case is categorized into a specific type. If no manual operation is needed for a case (as decided by the playbooks), it is assigned case as its type.

When you click on **Types** page, a list of case type is displayed.

## Searching a case Type

You can search a specific case type, through the **Search** option. Click the ⚙▾ button next to search, to view search results based on **Visible Name, Definition, Severities, Statuses** and **Actions** filters of case type.

## Creating a Case Type

Click the **+Create Case Type** button to create a new case severity. In the **Case Type Editor** window, specify the required details in the following fields:

| Value | Description |
|---|---|
| Name | |
| Definition | Explanation of the case type, e.g., for which cases this type can be used. |
| Visible Name | Provide a name for this case type to be shown when selecting a case type on the other pages of SOAR. |
| Severities | Select possible severities for this type. |
| Default Severity | When a case is opened by SOAR and related playbooks are executed, the default severity is assigned to the case. |
| Statuses | Select possible statuses for this type. |

| Value | Description |
|---|---|
| Default Open Status | Specify the default open status. When a case is opened by SOAR and related playbooks are executed, the default status is assigned to the case as open. |
| Default Closed Status | Specify the default closed status. When a case is closed, the default closed status is assigne dto the case. |
| Allow Case Reopen | Select this checkbox if you want to allow case of this type to be reopened after it is closed. |
| Custom Fields | Optionally, you can add your own fields to the case to be shown in the Cases page. Click the **Creat** button within the **Custom Fields** area, and type the name of field, select its type (text/date) and select whether this field will be visible, editable and shown on the Cases page when you select cases of this ticket type. After you provide the values for the fields click on the **Save** button, and your field will be added as a row within the **Custom Fields** area. You can edit or delete it using the **Edit** and **Delete** buttons, and add as many fields as you want. |

### Editing a Case Type

You can modify an existing case type by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Case Type Editor** window is displayed. Specify the values in the editor window as per your requirement and click **Save**.

## Configuring Case Labels

Select **SOAR** > **Configuration** > **Case > Labels**.

You can mark a case with your own special tags, called label.

When you click on the **Labels** page, a list of case label is displayed.

### Searching a Case Label

You can search a specific case type, through the **Search** option. Click the ⚙▾ button next to search, to view search results based on **Name, Color** and **Actions** filters of the case label.

### Creating a Case Label

Click the **+Create Label** button to create a new case label. In the **Label Editor** window, specify the required details in the following fields:

| Value | Description |
|---|---|
| Label Name | Specify the name of the label. |
| Label Color | Assign a color to the new label.. |

## Editing and Deleting a Case Label

You can modify an existing case label by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, the **Label Editor** window is displayed. Specify the values in editor window as per your requirement and click **Save** to modify.

You can also remove an existing case label by clicking the **Delete** button under the **Actions** column.

# Setting Up User Access and Preferences

After integration and additional configuration are done, SOAR can receive the alerts from multiple components. These alerts have to be assigned to users. Each user is assigned a set of permissions in the user tabs.

Some of the case can be assigned to a group of users, so you can create user groups in the **User group** tab.

You can also create **Access Control list** to control the access of the users or user groups to SOAR objects including action capabilities, credentials, custom scripts, enrichment capabilities, enrichment plugins, integrations and integration types.

Configuring User

Configuring User Groups

Configuring Roles

Configuring Access Lists

## Configuring Users

Select **SOAR** > **Configuration** > **Users**.

An admin can list and edit user roles who will be interacting with ArcSight SOAR for case handling. SOAR authenticates users from Platform's single sign on provider. Initially, on authentication all the users are assigned with a **Super user** role, which can be later modified to the respective suitable role by the admin.

The **Users** page displays the list of users with options to modify an existing one.

### Searching a User

You can search a specific user, through the **Search** option. Click the ⚙▾ button next to search, to view search results based on user's **ID, User Name, Last Modified By, Modification Date, External User, Active User, User Role**and **Actions** filters.

### Editing a User

You can modify an existing user's role, phone number and avatar by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **User Editor** window is displayed. Specify the values in editor window as per your requirement and click **Save** to modify.

# Configuring User Groups

Select **SOAR** > **Configuration** > **User Groups**.

SOAR facilitates user group option for the ease of use of some operations. These operations may include assigning a case, specifying watchers for a case, or assigning operator tasks to the user groups to ensure that each of the user in the group is involved in the assigned operation.

The **User Group** page displays a list of user groups and provides you options to create more user group or edit an existing user group.

## Searching a User Group

You can search a specific user group, through the **Search** option. Click the ⚙▾ button next to search, to view search results based on list's **Name, Content Type, Size, Action Allowed, Enrichment Allowed, Last Modified By, Modification Date**and **Actions** filters.

## Creating a User Group

Click the **+ Create User Group** button to create a new user group. In the **User Group Editor** window, specify the details for following fields:

| Value | Description |
|---|---|
| Name | Name of the user group. Provide an explanatory name which gives a hint about what the user group is created for. |
| Email | Specify an email ID for the user group. |
| Users | Select the users to be included in this user group. |
| Avatar | You can select an avatar for the group by clicking on the **Choose File** button. Any image will work. It is recommended to select image files with sizes of 200 x 200 pixels. |

## Editing and Deleting a User Group

You can edit an existing user group by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **User Group Editor** window is displayed. Specify the details as per your requirement and click **Save**.

You can remove an existing list by clicking the **Delete** button under the **Actions** column.

## Configuring User Roles

Select **SOAR** > **Configuration** > **User Roles**.

The **User Role** page displays a list of user roles and options to create and edit them. The user roles define the permissions granted to a user. Depending on your role, you may or may not have access to all the tabs and features listed in this guide.

The SOAR configuration comes with some predefined user roles. These roles basically determine how would you interact with the case created on SOAR. Following are the predefined roles that comes along with an SOAR deployment:

| Default Roles | Permissions |
|---|---|
| Admin | All Playbook permissions<br>All Dashboards and Reporting permissions<br>All Status permissions<br>All Configuration permissions |
| Integration Owner | View Dashboards<br>View Logs<br>Manage Integration Configurations<br>Manage Integration Credentials |
| Analyst | All cases permission<br>All Playbooks permission<br>All Dashboards and Reporting permission except for Manage Report Templates<br>Status- View Alerts, Manage Actions and Rollback Queue, Manage Alerts and View Action and Rollback Queue permissions<br>Configurations:<br>From Alert Sources and Integrations-View Alert Sources, View Integration Configuration, and View Integration Credentials permissions<br>From Security- View Users and View User Groups permission<br>From Lists- View Exclusion Lookup Tables and View Lookup Table permissions |
| Super User roles | All permissions |

A new user is automatically assigned the role of a **Super User** on the first log in. The admin can then choose to reassign a new role to the newly authenticated user.

A user cannot be assigned more than one role.

The SOAR also allows you to create new roles to reflect your organizational requirements.

### Creating a User Role

Click the **Create User Role** button to create a new user role. In the **Role Editor** window, specify the user role attributes as follows:

| Value | Description |
|---|---|
| Role Name | Name of the user role. Consider giving an explanatory name that hints about the permission level of the user, such as., Full Administrator or Monitoring Operator. |

### Editing and Deleting a User Role

You can edit an existing user role by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Role Editor** window is displayed. Specify the values in editor window as per your requirement and click **Save** to modify.

> You can not modify a **Super User** role.

You can also remove an existing user role by clicking the **Delete** button under the **Actions** column.

## Configuring Access Control Lists

Select **SOAR** > **Configuration** > **Access Control Lists**.

The SOAR provides **Access Control Lists** (ACLs) to control the access of the users or user groups on SOAR objects. These objects include action capabilities, credentials, custom scripts, enrichment capabilities, enrichment plugins, integrations and integration types. For example, you might prefer a specific group of users to access some specific integrations. In such scenarios you can edit the access controls of the user groups in **Access Control Lists** tab.

When you click **Access Control Lists** tab, a list of SOAR objects along with users or user groups who can access those objects, and the last user and last modification date of an access control is displayed.

### Searching an Access Control List

You can search a specific access control list, through the **Search** option. The search list keeps getting updated as you type. Click the ⚙▾ button next to **Search**, to view search results based on **Object, Access, Last Modified By** filters.

## Editing and Resetting an Access Control List

You can edit an existing access control list by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Access Control List Editor** window is displayed. Specify the values in editor window as per your requirement and click **Save** to modify.

You can only edit the **Allow Access For** and **Users/Groups** fields. By default, the object list is created with the **Anyone** option. If you want to narrow down the users for an object, just edit the related object and specify the users or groups for the option you selected in the **Allow Access For** field, which can be **Only selected users/groups** or **Anyone except selected users/groups**.

After editing an **Access Control List** item, **Clear** button appears in the **Actions** column of that item. You can not remove an **Access Control List** item from the list. By clicking on the **Clear** button under the **Actions** column, you can reset value of the **Access** column.

# Setting Up SOAR for Customization

Select **SOAR** > **Configuration** > **Customization Library**.

You can customize SOAR through plugin scripts, email templates, query templates, scriptable integration codes, text and HTML templates (used for notifications and other capabilities) and other customzation. The **Customization Library** tab displays a list of customzation, and also allows you to create a new customization content or modify an existing one. When a new plugin is uploaded through configuration/integrations/upload plugin options, you can also view and manage its code on this tab.

The list of customization can be filtered to display all integrations customizations, all integration types customization and all script types customization.

## Searching a Customization

You can search a specific user customization, through the **Search** option. Click the ⚙▾ button next to **Search**, to view search results based on **ID, Name, Script Type, Integration Types, Integration, Last Modified By**, **Modification Date** and **Actions** filters.

## Creating a Customization

Click the **+Create New Customization** button to create a new customization. In the **Customization Editor** window, specify customization name, description and type and enter the respective code in the black console.

## Filtering Integration Customizations

Click **Show all integrations** filter to view the customization list based on the visible name of the integrations already defined on the environment.

## Filtering Integration Types Customizations

The **Show all integration types** filter enables you to filter the list based on integration/plugin type.

## Filtering Script Types Customizations

When you click **Show all scripts type** filter, a list of script type customizations is displayed.

## Editing, Deleting and Reseting a Customization

You can edit an existing customization configuration by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Customization Editor** window is displayed. Specify the values in editor window as per your requirement and click **Save** to modify.

You can delete an existing customization configuration by clicking the **Delete** button under the **Actions** column.

The **Reset** button resets the content of customization to out-of-the-box version.

The **Lookup** button shows the details about where this particular customization is being used.

# Referencing Documents

Select **SOAR** > **Configuration** > **Document Repository**.

The SOAR provides options to store your reference documents that might be linked to cases if needed. For example, you can add case handling guides for your SOC analysts and link these documents automatically when an case is created on SOAR.

## Searching a Document

You can search a specific document, through the **Search** option. Click the ⚙▾ button next to search, to view search results based on document's **ID, File Name, Title, Description, File Size**and **Actions** filters.

## Uploading a Document

Click the **+Upload Document** button to upload a new document in the repository. In the **Document Repository Editor** window, specify details such as document **Title**, **Description** and then select the file to be uploaded.

## Editing and Deleting a Document From The Repository

You can edit an existing document by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Document Repository Editor** window is displayed. Specify the details as per your requirement and click **Save**.

You can delete an existing document by clicking the **Delete** button under the **Actions** column.

To download a document click the **Download** button under the **Actions** column.

# Storing Lists in SOAR

Select **SOAR** > **Configuration** > **Lists**.

The SOAR enables you to store diverse set of values in lists. The lists are used as lookup tables for referencing purpose.

## Searching a List

You can search a specific list, through the **Search** option. Click the ⚙▾ button next to search, to view search results based on list's **Name, Content Type**and **Size** filters.

## Creating a List

Click the **+Create List** button to create a new list. In the **List Editor** window, specify the details of list as follows:

1. **List Name**: Specify the name of the list that you want to create. For Example, VIP user names.
2. Select the option **Add Column** to create a new list. You can select Delete Column option if you are modifying an existing list.
3. Select the type of the data for the list from the drop down menu, for example, user name.
4. Specify the name of the column and click **Add**. The column name is displayed in below pane.
5. Enter a list item in the text field below the column name and then click **Add List Item** to add the list item for the newly created column.

   > Enter the list item in JSON format.

6. (optional) Enter a list item and click **Search** for searching a list item.
7. Click ✎ button to display the console pane. Click **Expand JSON**, to view list item in a JSON formatted order on the console.
8. Under **Actions** tab, click **update** to add the list item in the list or click **discard** to remove the list item.
9. (optional) Select the **Restrict Actions** checkbox to ensure that any action can not be taken (even if the action is a part of the playbook instructions) on the list items defined in the newly created list.
10. (optional) Select the **Restrict Enrichments** checkbox to ensure that any enrichments can

not be fetched (even if the fetching enrichment is a part of the playbook instructions) for the list items defined in the newly created list.

**Example use case:**

You might create a list to store the IP addresses of your data center.When you mark the list for **Restrict Actions** checkbox, SOAR will not take any actions for the servers listed in the list even if they are involved in an Case. For example, your play book might contain a step to block all IP addresses on the Case scope, however it will not block those addresses defined in this list.

As another use case, you might define a list of VIP usernames. When you mark it for **Restrict Enrichments** checkbox, SOAR will not perform enrichments on these VIP users.

## Editing, Deleting and Downloading a List

You can edit an existing list by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **List Editor** window is displayed. Specify the details as per your requirement and click **Save**.

You can delete an existing list by clicking the **Delete** button under the **Actions** column.

You can also download a list as a text file (txt) by clicking the **Download** button.

# Setting Up Scope Items

Select **SOAR** > **Configuration** > **Scope Item Properties**.

With ArcSight SOAR 3.1, it is possible to create your own scope item property types and use them in your workflows. In order to define a new scope item property, click **Create Scope Item Property** button and specify the **Name** and **Data Type** fields. Scope item property can possibly be a:

- Number
- Text
- Json
- Percentage
- Boolean

# III Working With Cases

ArcSight SOAR help you analyze numerous alerts, coming from an array of varied alert sources. Depending on the severity and other details, these alerts are then used by SOAR to generate cases. You can map these cases on the **Cases** tab and get a comprehensive, end-to-end understanding.

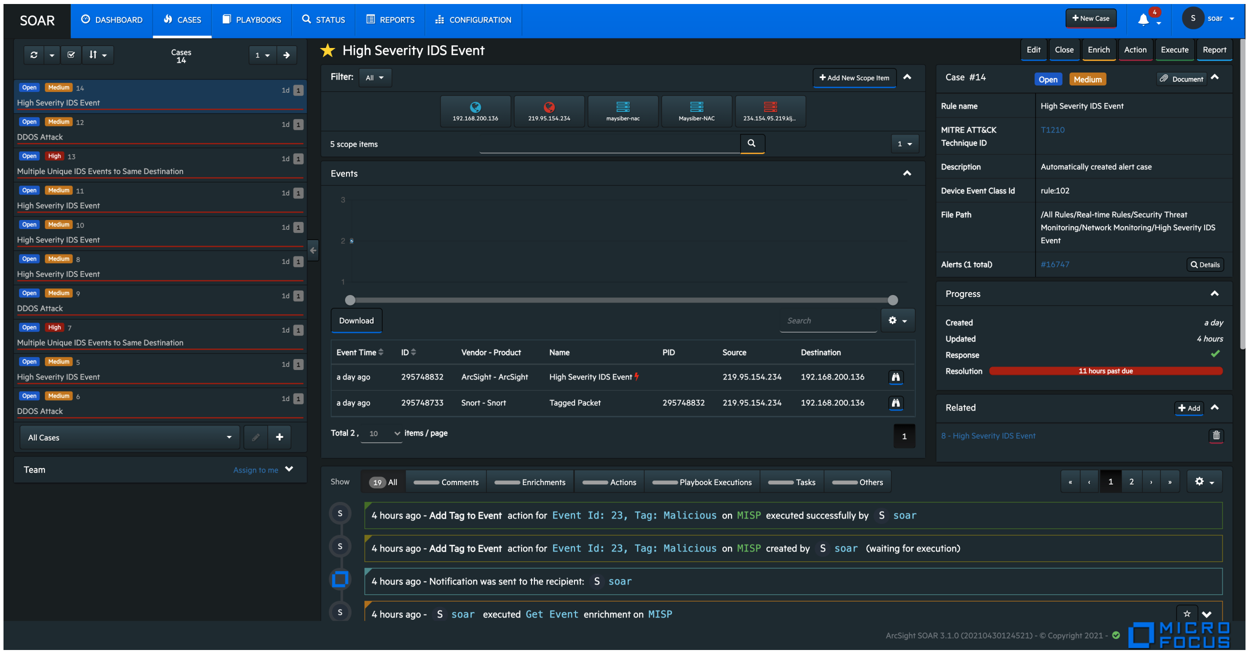
This section of the **SOAR User Guide** presents a detailed description about case handling on the SOAR application.

- Understanding Cases User Interface
- Viewing Case Details
- Creating New Case Manually
- Managing Cases

# Understanding Cases User Interface

SOAR has a very user friendly interface for tracking, viewing and managing cases in a single pane of glass. The **Case** tab of the SOAR user interface enables you to perform multiple operation on one page. You can view the list of cases, edit the case information such as its label, status and priority, add and edit assignees, add watchers , related cases, comments, and attach files, all on a single **Case** page. To perform a deeper analysis, you can also fetch enrichment for cases and perform desired actions. The Case Management service desk also facilitates the flexibility to create manual cases and generate reports for analysis.

A typical **Case** page is displayed as follows:



| | | | |
|---|---|---|---|
| Open | Medium | 14 | 1d 1 |
| High Severity IDS Event | | | |
| Open | Medium | 12 | 1d 1 |
| DDOS Attack | | | |
| Open | High | 13 | 1d 1 |
| Multiple Unique IDS Events to Same Destination | | | |
| Open | Medium | 11 | 1d 1 |
| High Severity IDS Event | | | |
| Open | Medium | 10 | 1d 1 |
| High Severity IDS Event | | | |
| Open | Medium | 8 | 1d 1 |
| High Severity IDS Event | | | |
| Open | Medium | 9 | 1d 1 |
| DDOS Attack | | | |
| Open | High | 7 | 1d 1 |
| Multiple Unique IDS Events to Same Destination | | | |
| Open | Medium | 5 | 1d 1 |
| High Severity IDS Event | | | |
| Open | Medium | 6 | 1d 1 |
| DDOS Attack | | | |

★ High Severity IDS Event

| Event Time | ID | Vendor - Product | Name | PID | Source | Destination |
|---|---|---|---|---|---|---|
| a day ago | 295748832 | ArcSight - ArcSight | High Severity IDS Event | | 219.95.154.234 | 192.168.200.136 |
| a day ago | 295748733 | Snort - Snort | Tagged Packet | 295748832 | 219.95.154.234 | 192.168.200.136 |

Total 2 , 10 items / page

Case #14 Open Medium

| | |
|---|---|
| Rule name | High Severity IDS Event |
| MITRE ATT&CK Technique ID | T1210 |
| Description | Automatically created alert case |
| Device Event Class Id | rule:102 |
| File Path | /All Rules/Real-time Rules/Security Threat Monitoring/Network Monitoring/High Severity IDS Event |
| Alerts (1 total) | #16747 |

Progress

| | |
|---|---|
| Created | a day |
| Updated | 4 hours |
| Response | ✓ |
| Resolution | 11 hours past due |

Related

8 - High Severity IDS Event

4 hours ago - Add Tag to Event action for Event Id: 23, Tag: Malicious on MISP executed successfully by S soar

4 hours ago - Add Tag to Event action for Event Id: 23, Tag: Malicious on MISP created by S soar (waiting for execution)

4 hours ago - Notification was sent to the recipient: S soar

4 hours ago - S soar executed Get Event enrichment on MISP

ArcSight SOAR 3.1.0 (20210430124521) - © Copyright 2021 -

# Viewing Case Details

Select **SOAR** > **Case**.

Viewing a case workflow is very beneficial in understanding the investigation procedure and performing end to end case management. When you select a case in the case list pane, its respective details are displayed in the panes next to it, including:

- "Case Name" below
- "Scope Item Details" below
- "Event Details" on the next page
- "Activity Details" on the next page
- "Teams" on page 45
- "Case Details " on page 45
- "Case Progress Details " on page 45

## Case Name

The name of case is displayed at the top. A star icon before the case name signifies that you are set as case watcher.

## Scope Item Details

You can view the list of the scope item defined for the case in the scope item pane of the **Case** page. Typically, scope items are artifacts or data that supports or relates to a particular case. These can be computer name, email address, file, file name, hash, host, keyword, MAC address, network address, process, rule name, unknown, username or a URL.

To view a specific set of scope items associated with a particular case, you can filter the scope item on the basis of their source from the **Filter** button at the top of the scope item pane.

When you click a scope item, the following details are displayed:

- Name, address and type of scope item.
- Source of the scope item. Typically, a scope item can be either created by you, registered from an Alert analysis, or be imported from the files or other attachments.
- Role and Other Roles of the scope item as Impact or Offender or Related.
- Hash Algorithms used for encrypting.
- Country of origin of the scope item.
- The list of number of alerts with the same scope item.

This alert list helps in narrowing down the investigation by understanding the malicious intent of the scope item in question. You can click the **Show alerts with this scope item** link to view the list of alerts with the same scope item. The **Alerts** list displays **Alert ID, Case, Creation Date, Rule Name and Actions** taken for resolving the related case. To view the actions and all the information captured for a particular case, click **Actions**.

## Event Details

You can view the events that created the case and the graph of the incoming events in the **Events** pane. Typically, an case can be created by single event or by consolidation of multiple similar events based on the SOAR configuration settings.

The **Events** pane provides detailed information about the events including:

- Event Time
- Event ID
- Vendor-Product
- Name
- PID
- Source
- Destination

You can also customize the level of details displayed in the Events pane.

To customize the Events displayed on **Events** pane:

1. Click the setting icon on the top right.
2. Select the column names that you want to view in the Event details page.
3. Click **Apply**.

After selecting the case, click the binocular icon to view the extended detail for that specific event.

## Activity Details

After you select an case, you can view the list of activities that were performed on the case in a detailed manner in the **Activity** pane. These information are displayed at the lower middle part of the **Case** page. The **Activity** pane presents following details:

- **All**: When clicked, this option displays all the list of activities performed on the case in a chronological order along with the User/User Role/Tier names.
- **Comments**: You can click on this option to view the list of comments added for this case. If you want to add some more case handling information, click on **Add Comment** button. You

can also attach a file for to further improvise the case investigation.

- **Enrichments**: This option displays the enrichments fetched and used for resolving the case.
- **Actions**: Click on this option to view all the actions performed for this case.
- **Playbook Execution**: Click this button to display the playbook name that was executed to respond the selected case.
- **Tasks**: This option displays the current task assigned from the playbook.
- **Others**: Click on this option to view other related activities.

You can also add, edit or delete comments, or attach files using the editor at the bottom of the **Activity** area.

## Teams

To view the assignee, source and watchers of the case, click the **Teams** button at the bottom left of the **Case** page.

## Case Details

You can view case number, status, severity, rule name, MITRE ID, description and label in the **Case Details** pane. This pane also presents a list of attached document related to case. To access these documents, the **Document** button. You can also click the **Details** button, to view the list of alerts that were consolidated to form this event.

> You can view the **MITRE ATT&CK Technique ID**, for cases with suspected MITRE attack. SOAR receives these events from the ESM alert source and when you click **MITRE ATT&CK Technique ID**, an associated attack detail is displayed.

## Case Progress Details

This pane shows the count of days/hours that has passed since the creation of and last update on the case. You can also track the SLA status of response and resolution here.

# Creating New Case Manually

Select **SOAR** > **Case** > **+New Case.**

Your user role must have **Create Manual Case** permission to manually create a case.

There are two primary ways for SOAR to receive alerts:

**Automatically** from the alert sources, configured during other software integrations with SOAR, such as ArcSight ESM.

**Manually** by the analyst, in the scenarios where other teams inform the operator about their Cases over calls or emails.

To create the cases manually, click **+New Case** at the top right of SOAR interface and specify the various values of different fields.The following list describes the fields:

| Parameter | Description |
|---|---|
| Type | Rule name for the type of manual Case type that you will select in the **Case Type** field. You can also use this field to create a new rule if it is not already defined in the **Rule Names**. When you start typing the rule name, this field lists you the defined rules in this combo box matching the entered characters. If the phrase you entered is not a match, just click on the **Create New Rule** in the combo box list to create one. |
| Subject | Subject for this new manual case which will be the headline of the case to be created. |
| Case Type -DEPRECATED- | Case type to be selected from this combo box which are predefined on your SOAR system. |
| Custom Fields -DEPRECATED- | You can provide values for the custom fields which are defined on your system for the selected case type. |
| Description | Description for the manual case to be created. |
| Time | Time and date of the manual case which you can select from the calendar in this field. |
| Severity | Severity of this manual case, defined on your system, which you can select from this combo box. |
| Add Scope Item | You can add a scope for this manual case by selecting the scope category and role, and entering the scope value. |
| Upload | You can attach a file (original email, a scanned document explaining the alert, etc.) to this manual case using the **Choose File** button in this field. |

When the **Save** button is clicked, SOAR creates a new case and displays it.

# Managing Cases

Case management is a collaborative process of streamlining case investigation and response activities to facilitate efficient remediation. When a case is registered, it is enriched with appropriate contextual information based on which, a suitable playbook is implemented to provide an effective response to the upcoming threat. Managing a case can include following tasks:

- " Editing Cases" below
- "Searching and Filtering Cases" on the next page
- "Sorting Cases" on page 49
- "Optimizing Threat Investigation through Scope Items" on page 50
- "Organizing Case Views Based on Layouts" on page 50
- " Adding Enrichments to Cases" on page 50" Performing Actions on Cases" on page 51
- " Performing Actions on Cases" on page 51
- "Closing Cases" on page 51
- "Executing Playbooks" on page 52
- "Analyzing Data Through Reports" on page 52
- "Relating Other Cases" on page 52

## Editing Cases

You can modify the case details to update its severity, status, label as per the different attack categories, re-assign it to new users, user groups, or tiers, add watchers and include informative descriptions.

### Editing Individual Cases

When you select an case, the corresponding details appear on the right pane of case page.

**To edit an Case**:

1. Select a case on case list to view its detail.
2. Click **Edit** and modify the following details on **Case Editor**:
   a. **Case Type**: Select the type of case.
   b. **Subject**: Specify the Subject.
   c. **Assignee**: Assign the case to selected Users or User Groups.
   d. **Watcher**: Select the watcher for the case from the displayed set of User or User Groups.

> You can assign multiple watchers to an case.

e. **Status**: Modify the case status as **Open** and **In Progress**.

f. **Severity** : Set the severity of the case as **Urgent**, **Critical**, **High**, **Medium** and **Low**.

g. **Description**: Add your comments about the case.

h. **Label**: Select the label from the list of pre-configured labels to categorize the case.

3. Click **Save**.

**Editing Multiple cases**

You can also edit multiple case at the same time, through **Multiple Edit Mode**. When you click the ☑ button on the top of the case list, the case list toggles to a view where you can select multiple case using check-boxes. You can select cases not only shown in the current case list but also the ones listed in other pages using the navigation button.

The **Multiple Edit Mode** allows you to change the severity, status, label and assignees for the selected cases in one go, through the **Update All Selected Tickets** button. You can also discard your changes by clicking on **Discard** and execute the predefined playbooks for selected cases through clicking the **Run Playbooks Again** option.

If the **Multiple Edit Mode** button is clicked once, the button’s background becomes blue and the **Multiple Edit Mode** page is displayed. If the **Multiple Edit Mode** button is clicked twice, the button’s background becomes yellow, implying that all cases in the current navigated case list page are selected. When the button is clicked for the third time, up to a 1000 cases are selected for editing and the button's background turns red. To disable the multiple edit mode, click on the button for the fourth time.

## Searching and Filtering Cases

To search a case, click the text field at the bottom of the case list. Enter the search query at the **Search** field.

To narrow down the search results, use the following set of predefined default filters below the **Search** text field:

- cases assigned to me
- cases I’m watching
- Open cases
- All cases

SOAR provides you an option to save your search queries. You can reuse the same saved search query, by selecting it from the **Saved Search Options**, below the **Default Search Options**.

**To create a new search query:**

1. Click the + button next to the search field. In the **Case Search Editor,** click **+Create**.
2. Click **Chose one of the following** and select the query criteria from the displayed list. Click the next **Chose one of the following** button and select a sub query criteria to further optimize your query.
3. To expand the search range, you can add another query criteria in the same search by clicking **+Create** button at the top of the **Case Search Editor** page.

   > You can keep including the query criteria in the same search by clicking **+Create** button.

4. Select the **Save** checkbox, then name the search query in the **Search Name** field.
5. You can clear your selections in the editor by using the **Clear Search** option.
6. Click **Close**. The newly created search will be added to the **Saved Search Options**.

You can also edit the saved search queries.

**To edit the saved search queries:**

1. Select a search query in the **Saved Search Options** and click the ✎ button next to the search field.
2. In the **Case Search Editor,** click **+Create**.
3. Click **Chose one of the following** button and select the query criteria from the displayed list. Based on the selection you made in the first **Chose one of the following** button, a set of related criteria list is displayed in the next **Chose one of the following** button. Select a sub query criteria to further optimize your query.
4. To further expand the search range, you can add another query criteria in the same search by clicking **+Create** button on the top of the **Case Search Editor** page.

   > You can keep including the query criteria in the same search by clicking **+Create** button.

5. Select the **Save** checkbox, then name the search in the **Search Name** field and click **Save and Search** to save it or **Delete** to delete the saved search.
6. You can clear your selections in the editor by using the **Clear Search** or close it by clicking **Close**.

## Sorting Cases

SOAR allows you to sort the cases by their creation date, last update, severity, respond and resolution times. You can sort the case list by using the **Sorting** button located on top of the case list.

## Optimizing Threat Investigation through Scope Items

When investigating a possible attack, it is important to understand the scope of the anomalous behavior. Scope items are artifacts related to the case.

SOAR enables you to create scope item to see the extracted artifacts of the case such as header information, email addresses, URLs, and attachments.

> The creation of a scope item depends on your role and the nature of the case.

**To create a scope item:**

1. Select a case in the case list to display a scope item pane in the middle of the case page.
2. Click **+Add New Scope Item**. In the **Scope Item Form Editor** page, enter the values for the Scope item. For some scope items, you can enter multiple values, such as IP addresses, separating each value with a newline.
3. Click **Select a category** to specify the type of the scope item.
4. Click **Select a role** to specify how the scope item is related with the case. **Impact**, **Offender** and **Related** are the options used to define the scope items relationship with the case.
5. Click **Add** to link the scope item to the respective case. The list of newly added scope items is displayed in the same page. You can also delete a scope item from the list.
6. You can also import the scope items from a CSV file. Click **Import scope from file** and in the **CSV Upload window**, click **Select the file**. Navigate and open the CSV file to import.
7. Click **Selector** and specify the type of selector used in the CSV file. Click **Save** and then **Close** the page.

Click the newly created scope item to view its extended details and properties.

## Organizing Case Views Based on Layouts

Following are the different layouts of SOAR application:

**Tier 1** is the default layout in which case Context and Scope Items take the central focus.

**Tier 2** layout is recommended for higher tier analysts who wants to handle deeper details of the cases. In this layout **Scope Items** and **Base Event** views take the central focus.

## Adding Enrichments to Cases

For investigation of some cases, you might need more detailed information. Adding context makes correlation more productive, thus enhancing the investigation capabilities. SOAR presents enrichment feature to address this issue. You can use the desired plugin for the case using the **Enrich** button located at the top right corner of the **Cases** page.

When you press the **Enrich** button, the **Launch Enrichment Plugin** dialog appears to fetch more details about the case.

Enrichment plugins are grouped according to the information they provide. So, you need to first select a group from the **Group Name** area. Then, according to your group selection, related plugins appear under the **Enrichment Plugin** area. When you select an enrichment plugin from this area, its capabilities are listed under the **Capability** area. Each capability requires different information in this editor.

## Performing Actions on Cases

You can trigger an action on an case at anytime using the **Action** button located at the top right corner of the cases page. These actions, such as sending a notification to a related person or blocking an IP address, might vary according to the case’s special condition.

When you click the **Action** button, select an integration with which the defined action will be triggered.

Each capability requires a different information in this editor. For more information, see Integration Guides for the action capabilities.

After selecting the capability, you must set the rollback interval for the this action. Click **Rollback Mode** to select the rollback period and select the respective host for it by clicking on **Host**.

When you click on the **Create Action** button, the action will fall into the **Approval Requests** field of the **Cases** page, if any integration approval is configured. The action will be performed after it is approved. If no integration approval is configured, then action will be performed automatically.

**Exclusion** list control is performed before **Approval** request.

## Closing Cases

You can close an case using the **Close** button at the top right corner of the page.

Select the status that needs to be assigned to the case after it is closed. You can also add a comment stating the reason. Click on the **Save and Close** button to close the case.

> You cannot close a case unless all the actions are approved and performed.

## Executing Playbooks

SOAR facilitate an automatic execution of Playbooks to accelerate sending response for repetitive cases. SOAR also provides decision making liberty to the analyst to re mediate the anomalous case. In scenarios where human interventions are required, you can manually execute a playbook for the selected case. Click **Execute** on the case page and select the desired playbook in **Execute Playbook and Automation Bits** window and then click **Execute** to manually implement the playbook.

## Analyzing Data Through Reports

Reporting captures the detailed analysis of the respective case including:

- Case summary
- Case timeline graphs
- Scope item recurrence analysis chart
- Detailed case timeline with actions, presented in a tabular format.

To generate a **Detailed Case Report**, click **Reports** on the case page.

## Relating Other Cases

To add other cases that you want to relate with this case, click **Add** on the **Related** pane at the bottom right of the **Case** page. Specify the related case number and relation type (which could be **DUPLICATE,RELATED** and **DEPENDSON)** in the **Add New Relation** page and click **Save** to add the related cases.

# IV Automating Response With Playbook

The SOAR facilitates automated response of the repetitive cases through playbooks. SOAR performs actions, enrichments and/or sends tasks and notifications based on the playbooks defined in the **Playbooks** menu. You can create, modify, delete, enable or disable playbooks on the **Playbook** page.

This section of the **SOAR User Guide** presents a detailed descriptions on playbooks.

- Filtering Alerts For Case Creation
- Classifying Cases on SOAR
- Consolidating Alerts to Create Cases
- Dispatching Cases
- Working With Playbook
- Handling Repetitive Tasks With Scheduled Playbooks
- Creating Custom Business Logics
- Managing Triggers
- Handling Manual Processes Through Tasks
- Managing Out Of The Box Workflows

# Filtering Alerts For Case Creation

Select **SOAR > Playbooks > Rule Name Filters**.

The SOAR receives new rule name filters automatically from different alert sources. Currently, it is not possible to create a rule name filter manually, as it is configured as pre-processor rules in the alert source to facilitate adding tags to correlated events that can be forwarded to SOAR.

So initially, when an alert is received by SOAR, it comes along with the rule name filters. No case is formed till this level. The rule name filters decide the plan of action for this alert. For example, if its possible threat, you can create a case with this alert, or receive the alert and save it and create a case with it but just ignore all base events, or you can also completely ignore the alert. The rules in this tab decide whether to register an incident with the alert or not.

The list of **Rule Names** appear in the ascending order in the **Rule Name Filters** page.

## Searching a Rule Name

You can search a specific **Rule Name**, through the **Search** option. Click the ⚙▾ button next to search, allows you to view search results based on **Rule Name ID, Rule Name, Alert Source, Ignore Mode, Pattern Matcher**, and **Actions**.

## Creating an Alert Source Rule Name

Click the **+ Create Alert Source Rule Name** button to create a new alert source rule name filter. A typical **Alert Source Rule Name Editor** screen fields are:

| Parameter | Description |
|---|---|
| Rule Name | Display name of the rule. |
| Alert Source | Type of the alert source. Select an alert source from the dropdown list of created alert sources. |
| Ignore Mode | Select from the list [**Create alerts, Ignore base events, Ignore for all alerts sources, Ignore for all alert sources of this type, Ignore for this alert source**]. |
| Pattern Matcher | Select the matching conditions. |

You can only change the **Ignore Mode** and **add / deleteScope Item Extraction** information while you are editing.

The following are the possible ignore modes:

| Parameter | Description |
|---|---|
| Create alerts | When an alert with this rule name is received an incident is created irrespective of the alert sources and alert source types. |
| Ignore base events | It does not create cases for base events. |
| Ignore for all alert sources | It does not create cases for this rule name, irrespective of alert sources defined on the system. |
| Ignore for all alert sources of this type | It does not create a case when an alert with this rule name is received, only for the alert sources of the type shown in the "**Alert Source Type**" field. It creates cases for the alert sources of other types. |
| Ignore for this alert source | It does not create a case when an alert with this rule name is received, only for the alert source shown in the **"Alert Source"** field. It creates cases for the other alert sources. |

### Scope Item Extraction Section

| Parameter | Description |
|---|---|
| Field Name | Name of the field. |
| Select Source | Select from the list **[Base Event, Correlated**]. |
| Select Category | Select from the list **[Computer Name, Email Address, File, File Name, Hash, Host, Keyword, MAC Address, Network Address, Process, Rule name, Unknown, URL, Username**]. |
| Select A Role | Select from the list [**Impact, Offender, Related**]. |
| Add | Click this button to add the scope item. |

You cannot edit an existing **Scope Item Extraction**.

You can delete an existing **Scope Item Extraction** by clicking the **Delete** button under the **Actions** column.

## Editing Rule Name Filter

You can edit the **Rule Name Filter** configurations by selecting a **Rule Name** and then clicking the **Edit** option under the **Actions** column. The **Edit** option also allows you to configure additional extraction from the base events or the correlated events. When you click the **Edit** option, **Alert Source Rule Name Editor** window is displayed. Specify the values in editor window as per your requirement and click **Save**.

> You cannot rename or delete an existing alert source rule name filter.

# Classifying Cases on SOAR

Select **SOAR > Playbooks > Classification**.

Classification tab helps you to organize or maintain your cases on the SOAR platform.

After an alert is received and a case is created with it, then it is passed for classification. On **Classification** tab, the alert is labeled depending upon the conditions. The rule names are checked depending on the rule name and a label is added to the alert. Later these classification lebels help SOAR in choosing and executing a playbook for this case.

You can view a list of classification on this page. The Classification list is processed from top to bottom and only the first match is executed. You can edit the rank of a classification rule through the **Rank** option and created items will appear as the last item in the table.

## Searching a Classification

You can search a specific **Classification** through the **Search** option. Click the ⚙▾ button next to search to view search results based on **Classification ID, Rule Conditions, Rule Actions, Last Modified by, Modification Date, Rank** and **Actions**.

## Creating a Classification Rule

You can create a classification with no condition, which will execute on all cases. You cannot create a classification without any action. After you select a condition, SOAR matches it with the alert conditions and automatically creates actions, that is defined under the **Actions** field.

Click the **Create Classification Rule** button to create a new classification. In the **Classification Editor** window, specify the details for following fields:

**Matching Mode**: Select <All condition, Any condition> to specify if the new rule allows all or any condition to be matched , similar to a logical AND /OR mode.

**Create Conditions**:

- **Type**: Select a condition type from the drop-down list. Following table presents the detailed condition types:

## Table: Condition Types

| Type | Description |
|---|---|
| Address contains | An address value which will be searched in the IP address of alert sources. You can use the “*” character as the wildcard. Assume that this value is .*.*.22, then the condition will be met when a case is created for all the alert sources having IP addresses that end with “22”. |
| Address doesn’t contain | Condition will be met when the value typed here is not a part of alert source IP addresses. |
| Address is in subnet | A subnet value, which will be searched in the subnet address of alert sources. You can use the __*__ character as the wildcard. |
| Address is not in subnet | Condition will be met when the value typed here is not a part of alert source subnet addresses. |
| Address matches regex | Condition will be met when the IP address of the alert source is matched to the regular expression specified here. |
| Address doesn’t match regex | Condition will be met when the IP address of the alert source does not match the regular expression specified here. |
| Alert is manual | Condition will be met when the alert is created manually. |
| Alert is not manual | Condition will be met when the alert is not created manually. |
| Alert parameter matches key value pair | Pair can be given as key=value. Condition will be met when the parameter (key) is equal to the value specified here for any alert parameters. |
| Alert parameter doesn’t match key value pair | Condition will be met when the parameter (key) is not equal to the value specified here for any alert parameters. |
| Alert source is | Condition will be met when the alert source of the related case is the one selected here. |
| Alert source is not | Condition will be met when the alert source of the related case is not the one selected here. |
| Alert source rule name is any of | Condition will be met when the rule name of case’s alert source is any of the selected values here. You can select multiple rule names in the **Parameters** combo box. |

| Type | Description |
|---|---|
| Alert source rule name is not any of | Condition will be met when the rule name of case’s alert source is not any of the selected values here. You can select multiple rule names in the **Parameters** combo box. |
| Alert source rule name is in list | Condition will be met when the alert source rule name of the related case is in the list selected here. |
| Alert source rule name is not in list | Condition will be met when the alert source rule name of the related case is not in the list selected here. |
| Alert source rule name matches regex | Condition will be met when the alert source rule name is matched to the regular expression specified here. |
| Alert source rule name doesn’t match regex | Condition will be met when the alert source rule name is not matched to the regular expression specified here. |
| Alert time is between (day of week) | Condition will be met when the creation time of an alert is between the dates and times selected here. |
| Alert time is not between (day of week) | Condition will be met when the creation time of an alert is not between the dates and times selected here. |
| Alert time is between (time of day) | Condition will be met when the creation time of an alert is between the times of each day selected here. |
| Alert time is not between (time of day) | Condition will be met when the creation time of an alert is not between the times of each day selected here. |
| Assignee is | Condition will be met when the assignee of the related case is the one selected here. |
| Assignee is not | Condition will be met when the assignee of the related case is not the one selected here. |
| Assignee is set | Condition will be met when the assignee of the related case is set. |
| Assignee is not set | Condition will be met when the assignee of the related case is not set. |

| Type | Description |
|---|---|
| Assignee is a member of group | Condition will be met when the assignee of the related case is a member of the group selected here. |
| Assignee is not a member of group | Condition will be met when the assignee of the related case is not a member of the group selected here. |
| Classification contains | Condition will be met when the classification typed here is in classification list. |
| Classification doesn’t contain | Condition will be met when the classification typed here is not in classification list. |
| Scope item category is | Condition will be met when the scope item category of the related case is the one selected here. |
| Scope item category is not | Condition will be met when the scope item category of the related case is not the one selected here. |
| Scope item role is | Condition will be met when the scope item role of the related case is the one selected here. |
| Scope item role is not | Condition will be met when the scope item role of the related case is the one selected here. |
| Scope item value equals | Condition will be met when the scope item value of the related case is equal to the value expressed here. |
| Scope item value doesn’t equal | Condition will be met when the scope item value of the related case is not equal to the value expressed here. |
| Scope item value is in list | Condition will be met when the scope item value of the related case is in the list selected here. |
| Scope item value is not in list | Condition will be met when the scope item value of the related case is not in the list selected here. |
| Severity is | Condition will be met when the severity of the related case is the one selected here. |
| Severity is not | Condition will be met when the severity of the related case is not the one selected here. |
| Status is | Condition will be met when the status of the related case is the one selected here. |
| Status is not: | Condition will be met when the status of the related case is not the one selected here. |

- **Parameters**: Appropriate value for the type. Select from the list or enter a value.

**Create Actions**:

- **Action**: Select an action from **Add case label** and **Change severity of Case**.
- **Parameters**: Appropriate value for the type. Select from the list or enter a value.

The newly created Classification Rule is displayed on the Classification page and is in **Disabled** state by default. You must ensure enabling the rule before using it.

## Editing and Deleting a Classification

You can edit an existing classification by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Classification Editor** window is displayed. Specify the values in editor window as per your requirement and click **Save** to modify.

You can delete an existing classification by clicking the **Delete** button under the **Actions** column.

You cannot edit an existing condition or action. You have to delete the condition or action and create a new one.

# Consolidating Alerts to Create Cases

Select **SOAR > Playbooks > Consolidation**.

Multiple alerts are generated from different alert sources, that are integrated with SOAR. These alerts are automatically consolidated to create a case as per the configuration settings. The **Consolidation** page displays a list of rules to consolidate alerts to create cases.

When an alert reaches the consolidation plugin based on the rules, all the correlated alerts are consolidated to create a case. It is after this consolidation procedure that the SOAR decides to create a new case or adding the alert into an existing one.

Consolidation rules are processed from top to bottom and only the first match is executed. Any alerts that matches the same consolidation rule is gathered in to the same case until that case status is **Close**. In that instance, a new case will be created and alerts are consolidated into this case.

## Searching a Consolidation Filter

You can search a specific **Consolidation Filter**, through the **Search** option. Click the ⚙▾ button next to search, to view search results based on **ID, Rule Conditions, Timespan, Last Modified by, Modification Date, Rank** and **Actions**.

## Creating a Consolidation Filter

Click **Create Consolidation Filter** to create a new consolidation filter. In Consolidation Filter , specify the details for following fields:

**Timespan**: Value in minutes, hours, weeks or days. Timespan provides time intervals to consolidate alerts into one case.

**Since Last Alert**: Timespan will be calculated from the last alerts creation time.

**Since First Alert**: Timespan will be calculated from the first alerts creation time.

**Until First Response**: Consolidation will stop when the case is responded by an analyst. When this checkbox is selected, SOAR will track the response status of the case and timespan and stop the consolidation at whichever comes first.

**Create Conditions**: Select a condition for alert consolidation from the following list of condition **Types** and **Parameters**:

- **Type**: Type of the consolidation. Select from the list.
  - Alert source is
  - Alert source rule name is any of
  - Alert source rule name is in list
  - Alert source rule name matches regex
  - Scope item category is
  - Scope item role is
  - Scope item value does not equal
  - Scope item value equals
  - Scope item value is in list
  - Scope item value is not in list
- **Parameters**: It varies depending on selected consolidation type.

> The newly created Consolidation Filter is displayed on the Consolidation page and is in **Disabled** state by default. You must ensure enabling the **Consolidation Filter** before using it.

## Editing and Deleting a Consolidation Filter

You can edit an existing consolidation filter by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Consolidation Filter** window is displayed. Specify the values as per your requirement and click **Save**.

You can delete an existing consolidation filter by clicking the **Delete** button under the **Actions** column.

# Dispatching Cases

Select **SOAR > Playbooks > Dispatch**.

SOAR enables you to define a set of dispatch rules to automatically assign a case to a user or user role or a tier.

After consolidation, once a case is created, you can decide to assign it to a group/ a team or a person and also add a severity to the case. If you did not assign the case to any user/group/team the SOAR automatically selects the playbook, based on rules and labels, and then executes it to resolve the issue.

The Dispatch page presents a list of dispatch rules that must be executed for the cases with specified conditions.

Dispatch rules are processed from top to bottom and only the first match is executed. You can view the rank of the rule (to see the order of dispatch actions to be applied to the cases), conditions of the dispatch rule, dispatch actions, and the user and date of last edits performed on the rule.

You can edit the rank of a dispatch rule through the **Rank** column and created items appears as the last item in the table.

If you do not want to remove the rule permanently, you can disable it using the **Disable** button in the list.

## Searching a Dispatch Rule

You can search a specific **Dispatch Rule**, through the **Search** option. Click the ⚙▾ button next to search, to view search results based on **ID, Rule Conditions, Rule Actions, Last Modified by, Modification Date, Rank** and **Actions**.

## Creating a Dispatch Rule

You can create a dispatch rule with no condition, which will execute on all cases. You cannot create a classification without any action. Once you select a condition, SOAR matches it with the alert conditions and automatically creates actions, that is defined under the **Actions** field.

Click **Create Dispatch Rule** button to create a new dispatch rule. In the **Dispatch Editor** window, specify the details for following fields:

**Matching Mode**: Select <All condition, Any condition> to specify if the new rule allows all/any the conditions to be matched , similar to a logical AND /OR mode.

**Create Conditions**: : To create conditions for the rule, click on the **Create** button within the **Conditions** box.

- **Type**

  Select the condition type from the **Type** drop-down list. Following table presents the detail condition types:

  **Table: Condition Types**

| Type | Description |
|---|---|
| Address contains | An address value which will be searched in the IP address of alert sources. You can use the "*" character as the wildcard. Assume that this value is .*.*.22, then the condition will be met when a case is created for all the alert sources having IP addresses that end with "22". |
| Address doesn't contain | Condition will be met when the value typed here is not a part of alert source IP addresses. |
| Address is in subnet | A subnet value, which will be searched in the subnet address of alert sources. You can use the __*__ character as the wildcard. |
| Address is not in subnet | Condition will be met when the value typed here is not a part of alert source subnet addresses. |
| Address matches regex | Condition will be met when the IP address of the alert source is matched to the regular expression specified here. |
| Address doesn't match regex | Condition will be met when the IP address of the alert source does not match the regular expression specified here. |
| Alert is manual | Condition will be met when the alert is created manually. |
| Alert is not manual | Condition will be met when the alert is not created manually. |
| Alert parameter matches key value pair | Pair can be given as key=value. Condition will be met when the parameter (key) is equal to the value specified here for any alert parameters. |
| Alert parameter doesn't match key value pair | Condition will be met when the parameter (key) is not equal to the value specified here for any alert parameters. |
| Alert source is | Condition will be met when the alert source of the related case is the one selected here. |

| Type | Description |
|---|---|
| Alert source is not | Condition will be met when the alert source of the related case is not the one selected here. |
| Alert source rule name is any of | Condition will be met when the rule name of case's alert source is any of the selected values here. You can select multiple rule names in the **Parameters** combo box. |
| Alert source rule name is not any of | Condition will be met when the rule name of case's alert source is not any of the selected values here. You can select multiple rule names in the **Parameters** combo box. |
| Alert source rule name is in list | Condition will be met when the alert source rule name of the related case is in the list selected here. |
| Alert source rule name is not in list | Condition will be met when the alert source rule name of the related case is not in the list selected here. |
| Alert source rule name matches regex | Condition will be met when the alert source rule name is matched to the regular expression specified here. |
| Alert source rule name doesn't match regex | Condition will be met when the alert source rule name is not matched to the regular expression specified here. |
| Alert time is between (day of week) | Condition will be met when the creation time of an alert is between the dates and times selected here. |
| Alert time is not between (day of week) | Condition will be met when the creation time of an alert is not between the dates and times selected here. |
| Alert time is between (time of day) | Condition will be met when the creation time of an alert is between the times of each day selected here. |
| Alert time is not between (time of day) | Condition will be met when the creation time of an alert is not between the times of each day selected here. |
| Assignee is | Condition will be met when the assignee of the related case is the one selected here. |
| Assignee is not | Condition will be met when the assignee of the related case is not the one selected here. |

| Type | Description |
|---|---|
| Assignee is set | Condition will be met when the assignee of the related case is set. |
| Assignee is not set | Condition will be met when the assignee of the related case is not set. |
| Assignee is a member of group | Condition will be met when the assignee of the related case is a member of the group selected here. |
| Assignee is not a member of group | Condition will be met when the assignee of the related case is not a member of the group selected here. |
| Classification contains | Condition will be met when the classification typed here is in classification list. |
| Classification doesn’t contain | Condition will be met when the classification typed here is not in classification list. |
| Scope item category is | Condition will be met when the scope item category of the related case is the one selected here. |
| Scope item category is not | Condition will be met when the scope item category of the related case is not the one selected here. |
| Scope item role is | Condition will be met when the scope item role of the related case is the one selected here. |
| Scope item role is not | Condition will be met when the scope item role of the related case is the one selected here. |
| Scope item value equals | Condition will be met when the scope item value of the related case is equal to the value expressed here. |
| Scope item value doesn’t equal | Condition will be met when the scope item value of the related case is not equal to the value expressed here. |
| Scope item value is in list | Condition will be met when the scope item value of the related case is in the list selected here. |
| Scope item value is not in list | Condition will be met when the scope item value of the related case is not in the list selected here. |
| Severity is | Condition will be met when the severity of the related case is the one selected here. |

| Type | Description |
|---|---|
| Severity is not | Condition will be met when the severity of the related case is not the one selected here. |
| Status is | Condition will be met when the status of the related case is the one selected here. |
| Status is not: | Condition will be met when the status of the related case is not the one selected here. |

- **Parameters**: Appropriate value for the selected condition type. Select from the list or enter a value.

**Create Actions**:

- **Action**: Defines case dispatch actions for the rule. Select the action from the **Action** combo box. Following are the available actions:
  - **Add a case label**: When selected, **Parameters** field toggles to a combo box listing the case labels defined in the system. You can choose a label from the list, so that when the case meeting the above conditions is created, it will be labeled as the one selected here.
  - **Assign to a user or group**: When selected, **Parameters** field toggles to a combo box listing the users/groups defined in the system. You can choose a user or group from the list, so that when the case meeting the above conditions is created, it will be assigned to the user or group selected here.
  - **Change severity of case**: When selected, **Parameters** field toggles to a combo box listing the case severities defined in the system. You can choose a severity from the list, so that when the case meeting the above conditions is created, the cases initial severity will be changed to the one selected here.

    Click the **Save** button within the **Actions** box to add your rule action. You can add as many actions as you want.

    > You cannot edit a previously created conditions or actions. You have to delete and create a new condition and action.

- **Parameters**: Appropriate value for the selected action type. Select from the list or enter a value.

> The newly created Classification Rule is displayed on the Classification page and is in **Disabled** state by default. Enable the rule before using it.

## Editing and Deleting a Dispatch Rule

You can edit an existing dispatch rule by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Dispatch Editor** window is displayed. Specify the values in editor window as per your requirement and click **Save**.

You can delete an existing dispatch role by clicking the **Delete** button under the **Actions** column.

> You cannot edit an existing condition or action. You have to delete the condition or action and create a new one.

# Working With Playbook

Select **SOAR > Playbooks > Playbooks**.

Playbooks defines the automation and orchestration part of the SOAR.

After a case is dispatched, playbook performs the response procedure. The SOAR can execute a fully automated playbook as well as a semi-automated playbook.

A completely automated playbook does not require any decision making from the agents. A semi-automatic model requires agent intervention for decision making or providing some extra information to the automation. So during a semi-automation procedure, SOAR handles the case resolution automatically till some point and then the control is passed to agents for decision making task and again after the decision is made, the control is handled by automation. If needed, SOAR automation can again assign the task to agent for some decision making or extra information requirement. So basically, SOAR performs orchestration and then finally makes a **Response**.

You can specify the execution priority of playbooks by setting the **Rank** values for each playbook, the smaller the rank, the higher is the priority.

Playbooks are processed from top to bottom and when a case matches, all of the playbooks with matching conditions are executed.

While designing any playbook, you must set conditions to ensure if multiple playbooks can run on the same case or not. As the playbooks running on the same case are not aware of each other, they must be designed independently such that one playbook does not interfere with another. If possible, it is recommended that a case matches with only one playbook.

## Searching a Playbook

You can search a specific **Playbook**, through the **Search** option. Click the ⚙▾ button next to search, to view search results based on **ID, Scenario Name, Type, Last Modified by, Modification Date, Rank**, **Actions** and **Disabled**.

## Creating an Advanced Playbook

The **Advanced Playbook** allows you to write your own playbook scripts. To create an advanced playbook, click **Create Advanced Playbook** button. In the **Advanced Playbook Editor** window, specify the details for following fields:

| Value | Description |
|---|---|
| Name | Display name of the playbook. |
| Matching Mode | **All Conditions** means playbook will be executed if all the conditions are true. **Any Conditions** means playbook will be executed if any of the conditions is true. |
| Rollback Mode | Set if the action will be permanent or will be rolled back after a period of time. |
| case auto-close | From the combo box, you can select in which conditions the playbook will close the cases. |
| Script Language | Select JavaScript or Python scripting language to write your playbook scripts. |
| Conditions | Use the **Create** button to add a condition to this playbook. You can define multiple conditions. For more information, see : **Table: Condition Types**. |

In the black console area, you can write your playbook scripts in Python programming language.

You can test your playbook using the **Test** button.

Select a defined alert source from the combo box, type a value into the **Value to Block** field to test your script, and click **Test**.

Your test result is displayed on the same console.

> The option **Value to block** can be any parameter depending on your script, such as IP or email address.

## Creating Workflow Playbook

**Workflow Playbooks** run automatically and follows the visual process definition. You can specify the a name to the playbook on **Playbook Name** field.

While creating a **Workflow Playbook**, you can drag and drop elements from the right side of the page. You must enter appropriate and valid values depending on the element in the **Properties** tab. Each element must be connected to another except the last one.

When a case is created, a playbook with matching condition is executed. The match conditions of the **Workflow Playbook** are defined in the **Start** element of the playbook.

## Executing Workflow Playbooks

**Workflow Playbooks** are run automatically when:

- **A new case is created**: cases are created by the Alert Rule Name Filter configuration.
- **A new alert is received**: Alerts are added to the cases by the Consolidation rules.
- **Rules of the case is updated**: Some alert sources update an existing alert for example, QRadar Offences and these can trigger an execution.

## Workflow Playbook Elements

To create a visual process definition, you must map the executable instructions through the predefined workflow playbook elements. You can drag and drop following elements to create the workflow:

- **Automation Bit Usage**: Automation Bits are custom code created by the users to execute custom business logic. A detailed explanation for Automation Bit's can be found in Automation Bit section of this guide. While using bits, scope will be supplied from the **Start from here** element if **Scope Filter** variable is not used.
- **Actions Usage**: There are two kinds of actions in SOAR:
  - Actions coming from the SOAR itself, and these actions act on cases to change it appropriately, for example, Status, Severity.
  - The action capabilities coming from integrations. There are different capabilities depending on the target device and all of them takes some input regarding their role in the workflow.

    Action elements are named as <Integration Name> - <Capability Name>. For example, Active Directory - Lock User.

  Actions usage have several standard properties including:

| Properties | Descriptions |
|---|---|
| Title | Visible name of the element in the visual editor. |
| Continue on Error | In some cases an action on a device can return an error for example, network problems. In such cases , SOAR will stop the execution of the workflow entirely. If this option is selected, SOAR will continue execution even if the action has failed. |

| Properties | Descriptions |
|---|---|
| Rollback Mode | SOAR can undo the action after a set time if needed. In many devices there are limits to how many items can be blocked and most of these artifacts usefulness drops over time. Rollback future gives the SOAR users a way to control their actions and the health of the target device. |
| Scope Filter | The scope filter name can be changed from capability to capability but in essence filter will define which scope items from the alert will be included in the execution.<br>Some actions also have other fields and these are populated from data that resides on the target device. Such as tag's or group names. |
| Actions are synchronous | Therefore when a workflow processes an action element, it queues this action and after successful queueing of this action workflow will resume processing the next element. This means in an ideal SOAR, processing actions will not create a performance issue for the workflow execution. There however some edge cases that when SOAR is under heavy load or an unexpected error is present, actions might be queued but different elements are executed before these actions are finished. |

- **Enrichment**: Enrichments are data gathering capabilities that will assist in case response procedures and decision making.

  Enrichments have several standard properties including:

| Properties | Descriptions |
|---|---|
| Title | Visible name of the element in the visual editor. |
| Continue on Error | In some cases an enrichment on a device can return an error e.g network problems. In such cases SOAR will stop the execution of the workflow entirely. If this option is selected SOAR will continue execution even if the enrichment is failed. |
| Integration | On which integration this capability will be executed. |

| Properties | Descriptions |
|---|---|
| Scope Filter | This part’s name can be changed from capability to capability but in essence filter will define which scope items from the alert will be included in the execution. |
| Do not use cache | When a workflow processes an action element, it queues this action. After successful queueing workflow resumes processing the next element. This means in an ideal SOAR, processing actions does not create a performance issue for the workflow execution. However some when SOAR is under heavy load or an unexpected error is present, actions might be queued but different elements are executed before these actions are finished. |
| Enrichments are synchronous | When executed they will start immediately and hold the workflow execution on this state until a result is returned. It is important to note that not every enrichment works as fast as you expect and in some cases rate limits might apply affecting the execution time of the overall workflow. Some enrichments execute and then wait for the process to be completed in the target device. These are also called asynchronous for their update part but for workflow execution they are treated as synchronous as well and will stop the execution until the response is returned. |

- **Tasks**: Tasks are elements that does not have an automatic component. These elements are dependent on SOC analysts for completion. Task properties are dependant on the configuration of the task. So one or more of these properties might not appear in **Properties** tab..

  Tasks have several standard properties including:

| Properties | Descriptions |
|---|---|
| Title | Visible name of the element in the visual editor. |
| Scope Filter | The name can be changed from task to task but in essence filter will define which scope items from the alert will be included in the execution. Filters can occur more than once and they are restricted to the Scope Item Type defined for them. So a **Network Address** type filter only works on **Network Address** type scope items. |
| Timeout Span | It is when the task is due, it will be defined by this property. Task will be timed out when it is due and execution will continue. If left empty, this value will be taken from the Configuration Parameter **WorkflowTimeout** as a global value. |

- **Analyst's Decision**: This is the logic element and provides true/false options to the analyst.

  Analyst's decision have several standard properties including:

| Properties | Descriptions |
|---|---|
| Title | Visible name of the element in the visual editor. |
| Description | Description of the decision. |

| | |
|---|---|
| Timeout span | This property is defined when the task will be due. When the task is due will be defined by this property. Task will be timed out when it is due and execution will continue. If left empty, this value will be taken from the Configuration Parameter **WorkflowTimeout** as a global value. |
| Send Additional Email for Approva | When this is checked, SOAR will send an additional email for out of SOAR interaction to the selected Analyst. |
| Analyst | Recipient of the approval Email. |

- **Utilities**: There are three types of utility elements:
    - **Notification**:This element supports sending notifications to different users.

      Notifications can be sent from different channels and currently on-screen, SMS, email and windows type messages are supported. Notifications use free-form subject and a pre-defined template for the message.
    - **Decision**: Decision are standard logic element of the workflow. For a given predicate group in the property section, SOAR checks the alert scope and the workflow scope. If both of the scopes match, the automation returns a **true** value and the playbook is executed.

      The alert scope is defined at the **Start from here** element and workflow scope is the enrichment data that is specific to the workflow execution gathered till this point.
    - **User Decision**: User decisions are true/false type checkpoints and they are sent to a recipient for gathering inputs.

      The difference in the **Task Decision** and **User Decisions** can be explained as, the user decision sends the decision message to a variety of recipients. It can send the notification to a free-text e-mail address, to an SOAR user or to an the case scope.

      User decision takes a template to form the message and expects the recipient to reply with an **APPROVE** or **DENY** option. You can create more than one template to send different set of data and messages to the relevant recipients. SOAR comes with **User Decision Notification Email Template** as a built-in template in the **Customization Library**.

      You can also define scope restricted parameters that can be filled on the fly.

      > Using a scope restricted parameter in the e-mail subject shows only the first item in the parameter. Rest of the items are appended in the body of the message. The decision must appear in the body of the reply message.

## Types of Connectors in the Workflow Playbook

Every element in workflow has a pre-defined connector type. There can be one, two or three output connectors.

- **Single connector**: All actions and most other types of elements, fall into this category and after the element executes workflow continue to the next element.
- **Double connector**: Elements that contain a timeout falls into this category. First connector will lead to a successful completion of the element within the given time, these are named **then** and second connector will lead to timeout.
- **Triple connector**: User and Analyst Decision falls into this category. First two connectors will lead to true and false respectively in a successful execution and third connector will lead to timeout.

## Importing and Exporting a Workflow

You can import a pre-designed workflow by clicking the **Import Workflow** tab. In **Workflow Import Editor** window, navigate to the template file, add a suitable name for the template and then click **Save** to import a a workflow.

To export a workflow playbook, click **Export** option under the **Actions** tab.

> You can not export an advanced playbook

## Editing Rank of a Playbook

You can define the order of execution for different playbooks by assigning a rank to it. Click **Edit Rank** option under the **Actions** tab and then modify the rank of the playbook in the respective **Rank** column.

## Editing and Deleting a Playbook

To edit the previously created playbooks click **Edit** option under the **Actions** tab. In the **Workflow Playbook Editor** window, modify the visual process flow to suit you requirements.

To remove a playbook from the automation, click **Delete** option under the **Actions** tab.

# Handling Repetitive Tasks With Scheduled Playbooks

Select **SOAR > Playbooks > Scheduled Playbooks**.

You can use a **Scheduled Playbook** to close repetitive tasks or automate time based mundane tasks.

## Searching a Scheduled Playbook

You can search a **Scheduled Playbook**, through the **Search** option. Click the ⚙▾ button next to search, to view search results based on **ID, Name, Type, Description, Last Modified by, Modification Date** and **Actions**.

## Creating Scheduled Playbooks

To create a new scheduled playbook, click the **Create Scheduled Playbook** button. In the **Scheduled Playbook Editor** window, specify the details for the following fields:

| Value | Description |
|---|---|
| Name | Display name of the scheduled playbook. |
| Trigger Frequency | For Trigger Frequency, select from Every minute, Every 5 minutes, Every 10 minutes, Every 30 minutes, Every hour, Every 2 hours, Every 3 hours, Custom cron value (to define your own frequency) options. |
| Script Language | Select Python or JavaScript as programming language for your script. |

In the console area, you can type a script for the playbook using Python programming language.

After typing the script, you can test the playbook using the **Test** option. Select a defined alert source from the combo box, type a value into the **Value to Block** field, and then click **Test** . Your test results are displayed on the same console.

> The option **Value to block** can be any parameter depending on your script, such as IP or email address.

You can also refer to the API Documents at the top right of the **Scheduled Playbook Editor** window.

## Editing and Deleting a Scheduled Playbook

You can edit an existing scheduled playbook by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Scheduled Playbook Editor** window is displayed. Specify the values in editor window or edit the playbook script as per your requirement and click **Save** to modify.

You can delete an scheduled playbook by clicking the **Delete** button under the **Actions** column.

# Creating Custom Business Logics

Select **SOAR > Playbooks > Automation Bits**.

**Automation Bits** are custom code created by the users to execute custom business logic. ArcSight SOAR supports Python as programming language for to write an automation bit.

## Searching an Automation Bit

You can search a specific **Automation Bit**, through the **Search** option. Click the ⚙▾ button next to search, to view search results based on **ID, Name, Language, Last Modified by, Modification Date** and **Actions**.

## Creating an Automation Bit

Click the **+Create Automation Bit** button to create a new automation bit. In the **Automation Bit Editor** window, specify the details for following fields:

**Name**: Name of the Automation Bit.

**Description**: Description of the Automation Bit.

**Scripting Language**: Select a programming language for coding automation bit from JavaScript or Python.

**Input Parameters**: Starting parameters of the Automation Bit. These can be **Date**, **String** or **Scope Filter** and named here to be used in the Automation Bit. **Date** results in current time. **String** creates a parameter input field in workflow playbooks. **Scope Filter** creates a filter field in workflow playbooks.

Automation Bit’s are **syncronous** and will hold the workflow executions until they are done.

> This capability, if used in unexpected ways, might create longer than usual workflow execution times and delays.

You can type your **Automation Bit** script at the Black Console.

## Editing and Deleting an Automation Bit

You can edit an existing automation bit by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Automation Bit Editor** window is displayed. Specify the values in editor window as per your requirement and click **Save** to modify.

You can delete an existing automation bit by clicking the **Delete** button under the **Actions** column.

# Managing Triggers

Select **SOAR > Playbooks > Triggers**.

Triggers are mini playbooks that are triggered by several events. These events are created by human interaction or passage of time where SLA is concerned. Triggers evaluate the changes in the cases and if it matches to a trigger execution condition, the trigger starts automatically. Trigger executions are done from **top to bottom** and all triggers that matches the conditions will run. Only **Event Type** condition can be used in trigger **Start Condition** and the rest of the execution is done in the workflow through **Decision** elements.

As events can not be matched to two different **Event Type**, so **AND** operator is not supported.

## Searching a Trigger

You can search a specific **Trigger**, through the **Search** option. Click the ⚙▾ button next to search, allows you to view search results based on **ID, Name, Last Modified by, Modification Date**, **Rank** and **Actions**.

## Creating a Trigger

To create a trigger, click the **Create Trigger** button. In the **Trigger Playbook Editor** window, drag and drop the elements to create a workflow. To understand more on creating workflow, see **Creating Workflow Playbook.**

## Editing and Deleting a Trigger

You can edit an existing Trigger by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Trigger Playbook Editor** window is displayed. Modify the properties of the Trigger Playbook elements or add or delete the element as per your requirement and then click **Save**.

# Handling Manual Processes Through Tasks

Select **SOAR > Playbooks > Tasks**.

Tasks are a way to define manual processes for Case response. The SOAR can handle the automatic and manual elements together in a defined workflow. Analyst Task creates a task that is handled by the SOC Analysts within the SOAR Case Management.

## Searching a Task

You can search a specific **Task** through the **Search** option. Click the ⚙▾ button next to search, to view search results based on **Name, Description, Task Scopes, Task Output, Last Modified by, Modification Date** and **Actions**.

## Creating a Task

You can define the **Analyst Tasks** in this window and the resulting task can then be used in the workflow as a standard element. To create a task, click the **+Create Analyst Task** button. In the **Analyst Task Editor** window, specify the details for the following fields:

**Name**: Visible name of the element in the visual editor.

**Description**: Description of the Task to be shown to the analyst.

**Task Scope**: Task scope is enabled here and these items will be filtered and shown to the analyst and expected to be completed by him/her.

**Scope Item Categories**: Input scope item types are selected here. This area supports multiselection.

**Task Output**: Task output is enabled here.

**Scope Item Category**: Expected scope item type is selected here. Scope item’s created by the analyst will have this type. This area is single selection.

**Task Merge**: If in an Case has more than one alert or a consolidation is ongoing it is possible that the workflow will run more than once and there will be tasks recurring for the analyst to complete. **Task Merge** gathers tasks occurring from the same workflow and shows them as one task to the analyst reducing their load. **Timeout Span** will be merged as well and SOAR will update the merged tasks **Due Time** as the most current one.

Using Task Output or Analyst Decision will disable **Task Merge** capability of SOAR for that elements. **Task Scope** is limited to handle **200** scope items. A task containing more than 200 scope items will be divided into more than one task.

## Editing and Deleting a Task

You can edit an existing task by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Analyst Task Editor** window is displayed. Specify the values in editor window as per your requirement and click **Save** to modify.

You can delete an existing task by clicking the **Delete** button under the **Actions** column.

# Managing Out Of The Box Workflows

Select **SOAR > Playbooks > Playbooks**

> You must be an Administrator or a Superuser to create or import playbooks.

Out of Box Playbooks provide the templates to help you design and implement your playbook. These templates are pre-designed workflows and provide guidance to customize automated response as per your requirements.

## List of Out Of Box Playbooks for SOAR 3.1

ArcSight SOAR 3.1 provides following out of the box playbook templates:

- Access Attempts on Unidentified Protocols and Ports
- Admin Account Check
- Block Malicious IPs - CheckpointFW
- Block Malicious IPs - Palo Alto Panorama
- Check IP Reputation from Multiple Sources
- Command and Control Traffic-1
- Command and Control Traffic-2
- Command and Control Traffic-3
- Command and Control Traffic-4
- Endpoint Investigation - Windows
- Internal Scanning Device
- Multiple Authentication Failure
- Outbound Traffic to Suspicious Countries, Ports, Services
- Phishing Email
- Stolen-Lost Device
- Virus Traffic in the Network

## Prerequisites for Out of Box Playbook:

To configure and use out of box playbooks, a set of integrations/analyst tasks/lists, as listed in respective playbook guides, must be configured on your environment.

## Customizing Out of Box Playbooks

The out of box playbooks must be customized to create a playbook as per your requirement.

**To customize out of box playbooks:**

1. Click **Workflow Template** tab.
2. Click **Create Workflow** and specify a name to the workflow in **Create Workflow From Template**window.
3. After importing the playbook as a template, select it and click **Repair** to configure as per your requirements.
4. Set parameter values as specified in the respective Playbook guide, in the **Workflow Repair Wizard** window.

   > Each playbook has distinct set of parameter values for configuration. For details, see Playbook Guides.

Some of the playbooks might require additional configuration steps, for more details, see Playbook Guides.

# V System Status

To help you understand the system state, SOAR enable you to view the list of all alerts, action and rollback queues, action history, enrichment history, process queues and troubleshooting options.

This section of the **SOAR User Guide** presents a detailed description on monitoring system status.

# Understanding System Status

You can monitor the SOAR system state by viewing the action and rollback queues, alerts, actions, process queues, and logs on the **Status** page.

When you click the **Status** tab, following tabs are displayed:

- Alerts
- Action and Rollback Queues
- Action History
- Enrichment History
- Process Queues
- Troubleshooting

## Alerts

Alerts tab lets you see alerts generated by your system. To manage alerts, click on the **Alerts** tab in **Status** menu.

You can select an alert source in the **Alert Source** combo box and see the alerts only generated by the selected source. You can also narrow down the alert list by providing a time interval (Start/End Dates) and specific parameters (Alert Parameters) that are included in the alerts' context.

You can see more details on an alert by clicking on the **View Alert Details** button under the **Actions** column. You can also see the alert parameters as JSON arguments by clicking on the **View Alert Parameters as JSON**. By clicking on the **Display Case** button, you will be taken to the Case's page which has been created by SOAR for that alert.

You can use the **Process Again** button if you want SOAR to re-run the playbooks (the basic and advanced ones) on an alert. Note that **Process Again** button will not have any effect for the alerts with offender information if they have been processed previously.

## Action and Rollback Queues

SOAR has a mechanism to manage actions to be executed on the integration, called queuing. This section explains the action and rollback queues.

When SOAR receives an alert, alert is processed according to playbooks and SOAR decides the action and target integration.

SOAR adds this action process or rollback process to **Action and Rollback Queues** list which you can ignore approve or clear items. In order to filter list based on process type, Integration type, you can use buttons on the top of the list.

## Action History

Action History tab lets you display and search logs of executed actions and rollback operations. To manage action history, click on the **Action History** tab in **Status** menu.

The page allows you to filter the action list by the following criteria:

- **Stage**: Stage of the action. Available values are **Executed Actions** and **Rollback Actions**.
- **Device**: You can select a device defined on your system to see the actions only performed on that device.
- **Playbook**: You can select a playbook defined on your system to see the actions only performed as a result of that playbook.
- **Status**: Status of the action. Available values are **All**, **Successful** and **Failed**.
- **Start/End Dates**: You can refine the action list by providing start and end dates of actions using the calendar buttons at both fields.
- **Action Value (Contains)**: A value to filter the action list where the action text contains this value.

There is a **Refresh** button on top right of the **Stage** field. You can click on this button to update the filtered actions list at that moment, or choose one of the predefined intervals in the button’s dropdown list to update the list automatically at the selected interval.

There is also a **Download** button on top right of the list view. You can download your filtered action list as a CSV file to your computer using this button.

## Enrichment History

Enrichment History tab lets you display and search logs of executed enrichments. To manage enrichment history, click on the **Enrichment History** tab in **Status** menu.

The page allows you to filter the action list by the following criteria as well as date:

- **Device**: You can select a device defined on your system to see the enrichments only performed on that device.
- **Submitters**: You can filter by users or automation.
- **Status**: Status of the enrichment. Available values are **All**, **Completed**, **Failed**, **Long Running**, **Not Started**, **In Progress** and **Excluded.**

There is a **Refresh** button on top right. For each entry there’s also a **Result** column that will include a **Show** button to display the raw result of the enrichment.

## Process Queues

Process Queues tab contains the following queue sub-tabs:

- **Alert Queue**: Lists the alerts received from any alert source that are saved in the SOAR database (including base events for applicable alert sources) and waiting to be processed (create/update Cases, execute playbooks).

  You can use the **Clear** button at the very end of queue list to clear the items in the respective queue.

## Troubleshooting

**Troubleshooting Download** button under this menu lets you to download a zip archive comprised of the following files:

- actionInternals.txt
- pgLocks.csv
- pgStatActiviy.csv
- pgStats.csv
- threatDump.txt

# VI Data Visualization Through Dashboard and Reports

The SOAR Capability enables you to track statistical details using the dashboard and case details using the report features. You can use a predefined report template or create your own template to generate a report.

This section of the **SOAR User Guide** presents a detailed information on dashboard and reports feature.

- Generating SOAR Reports
- Designing Report Templates

# Generating SOAR Reports

ArcSight SOAR supports two different options for reporting. First is the Internal Reports supported as out of the box reports. Second type of reports is the External Reports. These reports are created from templates by SOAR and can be edited or created from scratch by users.

## Dashboard

For more information see Users' Guide for ArcSight Fusion.

## Out of the Box Reports

A user requires Manage Reports and View Reports permissions to access Reports. The following is the list out-of-the-box reports:

- Analyst Performance Report
- Analyst Task Summary
- Closed Cases Report
- Detailed Case Report
- Case Summary Report
- Integration History report
- Integration Summary Report
- Monthly SOC Summary
- Open Cases Report
- Scope Item Reoccurrence
- SLA Summary
- SOC Current Status Report
- SOC Summary Report
- Threat Summary Report

### Analyst Performance Report

Analyst Performance Report presents the user with KPIs about the selected analyst in the given timeframe.

### Analyst Task Summary

Analyst Task Summary Report presents list of taken action for each analyst per case.

### Closed Cases Report

This report lists the closed cases in a given timeframe.

### Detailed Case Report

This report can be called directly from the case itself or in the **Reports** pane.

### Case Summary Report

Case Summary Report presents the following data:

- Total Cases Count
- Total Analyst Count
- Total Urgent SLA Breaches
- Response SLA ratio
- Resolution SLA ratio
- Case status timeline per close types as legend
- Case severity timeline per severies as legend
- Open close case ratio in pie chart
- Top ten closure reason in bar chart
- Open and close case per analyst in seperate bar charts
- Urgent cases lists.

### Integration History Report

Integration History Report and it’s detailed counterpart presents the user with a report about all integrations or a selected integration.

### Integration Summary Report

Integrations Summary Report presents the customer with a summary information about alert sources and device integrations that exists on SOAR in the given timeframe.

### Monthly SOC Summary

Monthly SOC Summary Report presents case summary for selected month in details of severity, classification, taken action, closed or open case count and daily distribution of closed action with false positive tag for the selected month. It also gives you logged in analyst information in month and case distribution per alert source.

### Open Cases Report

This report lists the open cases in a given timeframe.

### Scope Item Reoccurence Report

Scope Item Reoccurrence Report presents top 10 reoccuring count of scope items those types are IP Address, Username, Email Address, File Name, Hostname, URL and Computer Name.

### SLA Summary Report

SLA Summary Report presents Analyst, Rule, Severity and Classification based SLA distribution in detail of response and resolution.

### SOC Current Status Report

SOC Current Status Report presents the following data:

- Open and close case count
- Analyst count
- Urgent case count
- Analyst assigned workload in bar chart per analyst in details of severities as legend
- Case chart per case severity with open-close detail as legend
- Response and resolution SLA in pie chart with miss and met ratio
- Queued activity chart and open case assignment in pie chart

### SOC Summary Report

SOC Summary Report presents following data:

- Total count of case
- Total hours saved by SOAR
- Total count of analyst
- Total count of SLA breaches and met ratio for response and resolution
- Open and closed cases by time
- Response SLA and resolution SLA miss and met count in pie chart
- Case classification
- Analyst work load per user in bar chart
- Case counts analyst distribution with users as legend.

### Threat Summary Report

This report generates a summary of threats in a given timeframe.

# External Reports

A user requires Manage Report Templates and View Report Templates permissions to access External Reports.

You can use **Configuration** -> **Report Templates** section to import new templates and change current ones in your environment. After import operation is successful new report templates are available under Reports. To create a new report with this new template you should select **Create Report Profile** -> **Report Origin** and change it to **External Reports**. **Report Type** drop down will list the available templates for creating a new report.

Every template has different variables that can be used in report profile and SOAR will show these for selection in the creation.

New report templates can be created using JasperSoft Studio v6.8.0 Community Edition which is free to use and resulting .jrxml files can be imported into SOAR.

# Designing Report Templates

Select **SOAR** > **Configuration** > **Report Templates**.

The SOAR facilitates you to design you own report template in **Jasper Reports**. You can upload it on SOAR to get the customized reports.

## Creating a Report Template

Click the **Create Report Template** button to create a new report template. In **Report Template Editor** window, specify the **Report Type Name** and navigate to the file to be uploaded.

# Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

**Feedback on User Guide for ArcSight SOAR 3.1 (SOAR 3.1)**

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Documentation-Feedback@microfocus.com.

We appreciate your feedback!