

# IBM Security QRadar SOAR Add-on for Splunk User Guide V2.2.0

Date: June 2024

Licensed Materials – Property of IBM

© Copyright IBM Corp. 2010, 2022. All Rights Reserved.

US Government Users Restricted Rights: Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

## IBM Security QRadar SOAR Add-on for Splunk User Guide

| Version | Publication   | Notes   |
|---------|---------------|---|
| 2.2.0   | October 2024  | Add support for SOAR custom artifact types when mapping search results to artifacts in SOAR case.<br>Update splunklib to 2.0.2.<br>Remove request-toolbelt from the Add-on.   |
| 2.1.1   | May 2024      | Fix bug setting custom fields to null when updating existing SOAR case with the same splunk_notable_event_id.   |
| 2.1.0   | April 2024    | Update splunklib to 1.7.4.<br>Update requests-toolbelt to 1.0.0.  |
| 2.0.0   | June 2022     | Rebranded add-on to:<br>IBM Security QRadar SOAR Add-on for Splunk.<br>Folder name changed to SA_QRadar_SOAR.<br>Add SOAR case URL to Splunk ES History.<br>Update splunklib to 1.6.20.   |
| 1.3.2   | June 2022     | Bug fix related to \$ character in result tokens.   |
| 1.3.1   | May 2022      | Bug fix: Escape special characters in search result tokens.   |
| 1.3.0   | November 2021 | Support for creating multiple add-on instances via shell script.<br>Use single quotes around multiselect fields containing commas.<br>Use html format for incident description field.<br>Max Artifacts Per Alert limit set to 99 on the Set up page.<br>User Guide updates for Cloud Pak for Security and SaaS. |
| 1.2.2   | March 2021    | Setup UI patch.<br>Bug fix related to artifacts.  |
| 1.2.1   | February 2021 | Splunk Cloud compliance.  |
| 1.2.0   | December 2020 | Support for Resilient API keys.<br>Ability to update an existing incident from Splunk ES.<br>Permission for ess_analyst role to use the add-on.   |
| 1.1.0   | August 2020   | Added support for Python 3.   |
| 1.0.2   | April 2018    | Updated Splunk version number.  |
| 1.0.1   | January 2018  | Initial publication.  |

# Table of Contents

- Overview ..... 5
- Installation ..... 6
  - Requirements ..... 6
  - Installation and Setup ..... 6
  - Configuration ..... 7
- Escalating Splunk Alerts ..... 9
  - Adding a Splunk Alert Action..... 9
  - Mapping Date and Datetime Fields .....10
  - Mapping Multiselect Fields.....10
  - Mapping Multiple Artifacts of the Same Type .....11
  - Updating the Default Case Mapping.....12
- Escalating Splunk ES Notable Events ..... 13
  - Adding an Adaptive Response Action .....13
  - Ad Hoc Invocation .....15
  - Show Escalated Notable Events.....17
  - Mapping Additional Fields.....17
  - Mapping Date and Datetime Fields .....18
  - Mapping Multiselect Fields.....18
  - Mapping Multiple Artifacts of the Same Type .....20
  - Mapping event\_id for Notable Events .....21
  - Updating the Default Case Mapping.....21
- Troubleshooting ..... 23
  - Setup Screen.....23
  - Case Not Created .....23
  - Ad Hoc Invocation Failure .....24
- Support ..... 25



# Overview

The IBM Security QRadar SOAR Add-on for Splunk supports Splunk and Splunk ES. The add-on provides the capability of escalating a Splunk alert or Splunk ES notable event to a SOAR case, also called an incident.

The SOAR Add-on features include:

- **Easy Case Mapping:** Enables mapping of static values or search result tokens into custom fields in a SOAR case. You can map fields parsed from the event in the alert or notable event directly into any field. You also have custom case mapping rules for each saved alert or notable event.
- **Create Artifacts:** Maps result tokens into artifacts at the same time the case mapping is defined.
- **Custom Field Discovery:** Retrieves the case definition from SOAR so that all defined fields and field values are catalogued inside Splunk or Splunk ES. This allows you to add custom fields to SOAR, which are then available for mapping in Splunk or Splunk ES.
- **Automatic and manual escalation:** Escalates notable events from a correlation search or alerts from a saved search to SOAR cases (automatic escalation). For Splunk ES only, you can escalate notable events as an ad hoc action (manual escalation).

A Conversion Script package converts an instance of the add-on into a different instance with a user specified name. You can import the new instance into an on-premises Splunk installation and configure it to run with a different SOAR organization or platform. The package can be downloaded from the [IBM App Exchange](#).

# Installation

## Requirements

The following lists the system requirements

- Splunk version 8.0 or later.
- Splunk ES 6.1.0 or later (only if working with Notable Events).
- Splunk CIM Framework.

**Note:** The add-on depends on Splunk CIM. Install CIM before installing the add-on.

- QRadar SOAR platform version 35 or later.
- Ability to connect directly from Splunk to your QRadar SOAR platform with HTTPS on port 443.
- A dedicated SOAR Administrator or equivalent account on the SOAR platform. This can be any account that has the permission to create incidents and simulations, and view and modify administrator and customization settings. You need to know the account username and password.

**or**

A dedicated API key/secret pairing with equivalent permissions. This can be any API key that has the permission to create incidents and simulations, and view and modify administrator and customization settings. You need to know both the API key and secret.

**Note:** Should you later change the dedicated SOAR account or API key, the new credentials must also have the permission to edit incidents, in addition to the permission to create incidents and simulations and view and modify administrator and customization settings. The edit permission is necessary so that the integration can continue to modify or synchronize the incidents escalated by the original user account.

You can refer to the [Playbook Designer Guide](#) for more information about simulations.

- Splunk admin role for the user who installs and sets up QRadar SOAR Add-on for Splunk. Both the admin and ess\_analyst roles may use the add-on as an Alert Action or an Adaptive Response Action for a correlation search.

## Installation and Setup

**If upgrading SA\_QRadar\_SOAR, clear your browser cache after installing the upgrade.**

For Splunk Cloud and Splunk ES Cloud users, contact Splunk Support to create a ticket for installing the QRadar SOAR Add-on for Splunk.

If you have installed Splunk or Splunk ES on-premises, you can download and install the add-on from [Splunkbase](#). Alternatively, you can request an installer from IBM QRadar SOAR.

After installing the add-on in a standalone or a search head cluster environment and restarting Splunk, navigate back to the Apps Manager screen. Click **Set up** in the SA\_QRadar\_SOAR row. Fill out the required attributes for your SOAR and click **Submit**. When you **Submit**, the Set Up program performs the following:

- Retrieves the case definition from SOAR so that all fields, including custom fields, are catalogued.

**Note:** If a SOAR administrator adds custom fields after you run **Set up**, you need to run **Set up** again to capture the new fields.

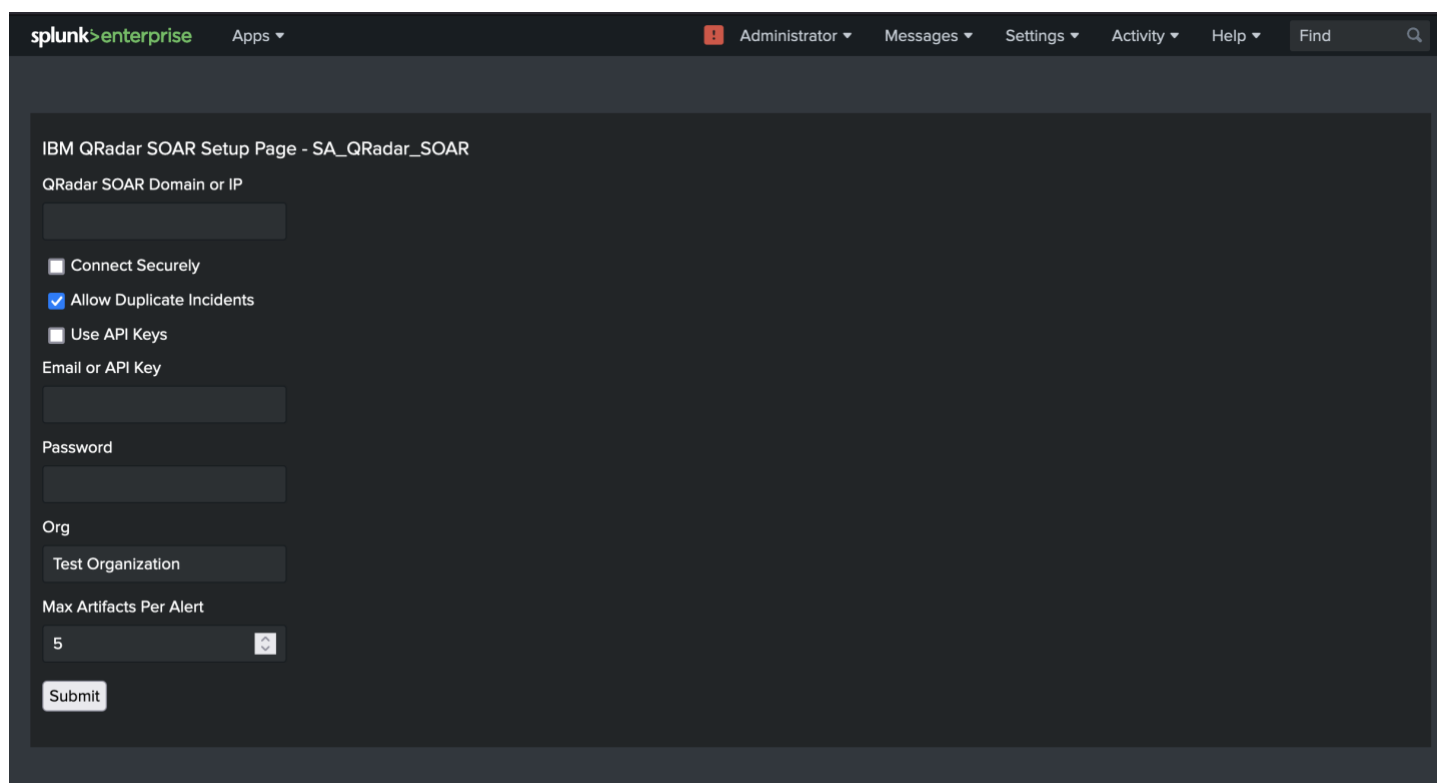
**Note:** If running in a search head cluster environment, **Set up** needs to be executed on one search head member only. **Set up** information is replicated to each of the other search head members after hitting **Submit** with successful completion.

- Tests the configuration to verify that the connection is successful. If the configuration saves successfully, you are up and running.

Refer to the Troubleshooting section if you encounter a problem.

## Configuration

Configure the QRadar SOAR Add-on for Splunk to access your SOAR on the Setup Page pictured below. Navigate to this page from the **Apps Manager** screen.



The screenshot shows the 'IBM QRadar SOAR Setup Page - SA\_QRadar\_SOAR' within the Splunk interface. The page has a dark theme. At the top, there's a navigation bar with 'splunk>enterprise' and 'Apps' dropdown. Below this, a header bar contains 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a search icon. The main content area is titled 'IBM QRadar SOAR Setup Page - SA\_QRadar\_SOAR'. It contains several input fields and checkboxes: 'QRadar SOAR Domain or IP' (text input), 'Connect Securely' (checkbox), 'Allow Duplicate Incidents' (checkbox, checked), 'Use API Keys' (checkbox), 'Email or API Key' (text input), 'Password' (text input), 'Org' (text input), 'Test Organization' (button), 'Max Artifacts Per Alert' (dropdown menu set to 5), and a 'Submit' button at the bottom.

Guidelines for configuring the **Set Up** Page parameters:

- **QRadar SOAR Domain or IP:** Hostname or IP for your SOAR. Do not include the https:// prefix.

**Note:** If configuring for Cloud Pak for Security, prefix the hostname with **cases-rest**.

For example: cases-rest.cp4s-domain.com

If configuring for Cloud Pak for Security SaaS, contact CP4S SaaS Support for the cases rest and stomp endpoints.

For DNS Mapping, the user should save the IP and domain name in the file **/etc/hosts** on the Splunk server.

- **Connect Securely:** Do not check if using self-signed certificates on your SOAR.
- **Allow Duplicate Incidents:** If **unchecked**, the add-on searches for an existing open case or incident in SOAR and, if found, updates that case. If there is no match, a new case is created. If this box is **checked**, a new case is created every time the action is triggered.

**Note:** Updating existing cases or incidents in SOAR requires use of Splunk ES and the `splunk_notable_event_id` custom field. See [Mapping event\\_id for Notable Events](#).

- **Use API Keys: Check** to authenticate with SOAR using an API key and secret. **Uncheck** to authenticate with SOAR using an email and password.

**Note:** If configuring for Cloud Pak for Security, API key must be used.

- **Org:** The name of the SOAR organization.

**Note:** If configuring for Cloud Pak for Security, the Org name must be in UUID format.

- **Email or API key:** Email address or API key ID you use when authenticating with SOAR.

**Note:** If configuring for Cloud Pak for Security, API key must be used.

- **Password:** Password for the SOAR account or API key secret for the SOAR API key. This is a mandatory field, and the value must be entered before clicking **Submit**.

- **Max Artifacts per alert:** Maximum number of artifacts you may need to map into a single SOAR case from any given Splunk alert or Splunk ES notable event. This field takes an integer.

**Note:** Wait a few moments after clicking **Submit** to allow the setup process to complete. Your browser displays a pop-up dialog with the results of the setup process when completed. Once you have successfully configured the add-on, the setup page displays the last successful configuration in the form, except for **Password**, which you must enter.



# Escalating Splunk Alerts

## Adding a Splunk Alert Action

To add a SOAR escalation to an alert, go to the **Alerts** tab in the Search & Reporting app and find the alert for which you want to create a SOAR case. Click **Edit** and select **Edit Actions**. Click **+ Add Actions** and select **Create QRadar SOAR Case (SA\_QRadar\_SOAR)**. Update the fields to indicate how you want them mapped. You can use static values or tokens from the alert data. In addition to the fields parsed in your particular alert search, the [Splunk documentation](#) has a list of the default tokens available in any search.

Be sure to map a valid value for the Date Discovered field, which is always required.

A sample alert, failed\_splunk\_login\_send\_to\_qradar\_soar, is included. If you enable this alert, a SOAR case is created each time there is a failed login attempt to Splunk. If you have added custom required fields to your SOAR, you need to edit the mapping on the alert action screen to include them before triggering the example.

Search

index=\_internal sourcetype=splunkd ERROR UiAuth

### Edit Alert



Cron Expression

\* / 5 \* \* \* \*

e.g. 00 18 \* \* \* (every day at 6PM). [Learn More](#)

Expires

24

hour(s) ▼

#### Trigger Conditions

Trigger alert when

Number of Results ▼

is greater than ▼

0

Trigger

Once

For each result

Throttle ?

☐

#### Trigger Actions

+ Add Actions ▼

When triggered



Create QRadar SOAR Case  
(SA\_QRadar\_SOAR)

[Remove](#)

Enter a value to map for each incident field. This text can include tokens that will resolve to text based on search results. [Learn More](#)

\* required

Date Discovered

\$result\_time\$

Name

\$name\$ (from Splunk)

Cancel

Save

## Mapping Date and Datetime Fields

If mapping values from Splunk to Date Picker or Date Time Picker fields in SOAR, the formatting of those values in the mapping must meet certain requirements. If you are parsing the date/datetime value from the Splunk search using a token, the value is already properly formatted and there is no additional action required. However, if you are providing a static value for the mapping, dates must be formatted as `YYYY/MM/DD`. Similarly, datetime values must be provided as `YYYY/MM/DD HH:MM:SS ±xxxx`. The `±xxxx` following the time is the UTC offset value. For example, the value for Cambridge, Massachusetts, United States is `-0500`. Be sure to include a leading zero if your offset value is a single-digit number of hours.

In Python3, you may include a colon between the hour and minute values (in the Cambridge example this is `-05:00`). However, in Python2 the UTC offset must be only the directional sign and exactly four digits. This value is optional when providing a static datetime. If you do not provide a UTC offset value, the datetime object is assumed to be in Greenwich Mean Time (GMT).

## Mapping Multiselect Fields

If mapping values from Splunk to Multiselect field in SOAR, these values must be supplied as comma separated values (CSV). If Splunk result tokens (tokens delimited by leading and trailing `$`-character) are used in mapping values, no space can be specified before the comma. For example, valid value formats to map are:

- `$result.value1$, $result.value2$, $result.value3$`

The following introduction of spaces **generates errors** when creating the case in SOAR.

- `$result.value1$, $result.value2$, $result.value3$`

When mapping values without Splunk result tokens, a space can be placed between the values after comma. The following are valid formats:

- `1,2,3`
- `1,2, 3`
- `1, 2, 3`
- `$result.value1$, 1, 2, 3`

These examples assume that values 1, 2, 3 and the values returned from Splunk after evaluating `$result.value1$`, `$result.value2$`, and `$result.value3$` are valid selections for the multiselect field you desire to fill or update in SOAR. You need to define these accepted values manually.

**Note:** Use single quotes around any multiselect value that contains comma or special characters.

- `'New York, NY', 'Los Angeles, CA'`

Here is an example of a Multiselect field as defined in SOAR:

Create Incident Field

Type of field ⓘ  
Multiselect

Label for the field \* ⓘ  
Splunk Multi-select Example

API name \* ⓘ  
splunk\_multiselect\_example

Placeholder value (Optional) ⓘ  
A placeholder value

Requirement ⓘ  
Optional

Tooltip (Optional) ⓘ  
A description of this field.

Enter one value per line ✓ ✕  
Example Value 1  
Example Value 2  
Example Value 3  
Example Value 4  
Example Value 5  
*Select one or more options as default when creating new incidents.*

Cancel

Create

## Mapping Multiple Artifacts of the Same Type

Similar to adding artifacts manually through the SOAR UI, you can add multiple artifacts of the same type at once as long as the artifact type allows multiple values. This setting can be found under **Customization Settings > Artifacts** in SOAR. URLs need to be separated by a space and IP addresses must be comma-separated. Artifacts can also be mapped individually.

Artifact 11

IP Address

7.7.7.7

description

Artifact 12

IP Address

8.8.8.8,9.9.9.9

description

## Updating the Default Case Mapping

You can change the default mapping when you configure the action. If the case mapping for most of your alerts will be very similar, you may want to override the default mapping where all the alerts start. Create an `alert_actions.conf` in `$SPLUNK_HOME/etc/apps/SA_QRadar_SOAR/local` and override the default mappings.

# Escalating Splunk ES Notable Events

## Adding an Adaptive Response Action

To add a SOAR escalation to a correlation search, go to the **Configure** tab in the Enterprise Security App, and select **Content Management**. Click the correlation search for which you want to create a SOAR case and scroll down to the **Adaptive Response Actions** section. Click **+ Add New Response Action** and select **Create QRadar SOAR Case (SA\_QRadar\_SOAR)**. Update the case fields to indicate how you want them mapped.

To create a new correlation search, go to the **Configure** tab in the Enterprise Security App and select **Content Management**. Click **Create New Content** and select **Correlation Search**. Create a new correlation. A sample correlation search `failed_splunk_login_ES_send_to_qradar_soar`, is included, which you can find in **Content Management**.

# Correlation Search

Search Name

failed\_splunk\_login\_ES\_send\_to\_qradar\_soar

App

QRadar SOAR Case Creation from Splunk

UI Dispatch Context

Select...

Set an app to use for links such as the drill-down search in a notable event or links in an email adaptive response action. If None, uses the Application Context.

Description

Create a case when login to splunk server failed.

Mode

Guided

Manual

Search

index=\_internal sourcetype=splunkd ERROR UiAuth | `get\_event\_id`

# Annotations

CIS 20

Type an attribute and press enter

Scroll down to the Adaptive Response Actions section and view that the QRadar SOAR Add-on has been added as a response in this sample correlation search. You can change the default configuration.

Trigger Conditions

Trigger alert when

Number of Results

is greater than

0

Trigger

Once

For each result

Notable response actions and risk response actions are always triggered for each result.

Throttling

Window duration

0

second(s)

How much time to ignore other events that match the field values specified in Fields to group by.

Fields to group by

Type a field and press enter

Type the fields to consider for matching events for throttling. [Learn more](#)

Adaptive Response Actions

+ Add New Response Action

>

Create QRadar SOAR Case (SA\_QRadar\_SOAR\_ext3)

X

## Ad Hoc Invocation

You can dispatch QRadar SOAR Add-on as an ad hoc invocation. To escalate a notable event, go to the Incident Review tab of Enterprise Security. Locate the notable event that you wish to escalate and select **Run Adaptive Response Actions** in the Actions column.

splunk>enterprise Apps

Administrator Messages Settings Activity Help Find

Security Posture Incident Review Investigations Security Intelligence Security Domains Cloud Security Audit Search Configure Enterprise Security

Incident Review

Search...

Show Charts

Hide Filters

Saved filters

Tag

Urgency

Status

Owner

Security Domain

Type

Search Type

Time or Associations

Select...

Add tags...

Select...

Select...

Select...

Select...

Select...

Correlation S...

Select...

Time

Last 24 ho...

Save new filters

Update

Clear all

Submit

Time Range: Last 24 hours

6 Notables

Unselect all

Edit Selected

Edit All Matching Events (6)

Add Selected to Investigation

|                          | Time                  | Security Domain | Title                 | Urgency  | Status      | Owner      |  |
|--------------------------|-----------------------|-----------------|-----------------------|----------|-------------|------------|--|
| <input type="checkbox"/> | > Today, 10:47 AM     | Endpoint        | Endpoint alert        | Medium   | In Progress | unassigned |  |
| <input type="checkbox"/> | > Today, 10:45 AM     | Threat          | New Critical Threat   | Critical | New         | unassigned |  |
| <input type="checkbox"/> | > Today, 10:43 AM     | Access          | Error                 | High     | New         | unassigned |  |
| <input type="checkbox"/> | > Today, 9:27 AM      | Access          | New Notable           | Medium   | New         | unassigned |  |
| <input type="checkbox"/> | > Yesterday, 11:10 AM | Threat          | AnnMarie Failed login | Low      | New         | unassigned |  |

Add Event to Investigation

Build Event Type

Extract Fields

Run Adaptive Response Actions

Share Notable Event

Suppress Notable Events

Search for original event


Click **+ Add New Response Action** and select **Create QRadar SOAR Case (SA\_QRadar\_SOAR)**. Update the case fields to indicate how you want them mapped.

## Adaptive Response Actions

Select actions to run.

+ Add New Response Action

▼



Create QRadar SOAR Case (SA\_QRadar\_SOAR)

×

Enter a value to map for each incident field. This text can include tokens that will resolve to text based on search results. [Learn More](#)

\* required

Date Discovered

\$result.orig\_time\$\*

Name

\$name\$ (from Splunk)\*

Workspace

\*

Address

City

Incident Disposition

Run

IBM Security | October 2024

16



Click **Run** to escalate. Once completed, refresh the page to see the updated notable event. The comment contains the Case ID for the case created. The **Adaptive Responses** field, shown below, displays a success status for **Create QRadar SOAR Case**.

History:

2022 May 18 12:27:57 PM

Administrator

QRadar SOAR Case ID: 2290

[View all review activity for this Notable Event](#)

Adaptive Responses:

| Response                                 | Mode  | Time                     | User  | Status    |
|--|-------|--------------------------|-------|-----------|
| Create QRadar SOAR Case (SA_QRadar_SOAR) | adhoc | 2022-05-18T09:27:54-0700 | admin | ✓ success |
| Notable                                  | adhoc | 2022-05-18T09:27:10-0700 | admin | ✓ success |

[View Adaptive Response Invocations](#)

## Show Escalated Notable Events

Each time a notable event is escalated successfully, the corresponding SOAR Case ID is added to the comment field of the notable event. This allows Splunk ES users to easily search for all the notable events escalated successfully. To perform a search, enter the search parameter, such as `'notable' | where (comment LIKE "QRadar SOAR Case ID: %")`, in the **Search** tab of **Enterprise Security**. For example:

splunk>enterprise

Apps

Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards

Search & Reporting

New Search

Save As Create Table View Close

'notable' | where (comment LIKE "QRadar SOAR Case ID: %")

Last 24 hours

Q

✓ 3 events (5/17/22 9:00:00.000 AM to 5/18/22 9:34:29.000 AM) No Event Sampling

Job

Events (3) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

1 hour per column

List Format 20 Per Page

< Hide Fields

All Fields

SELECTED FIELDS

a source 2

a sourcetype 1

i Time Event

> 5/18/22 9:27:13.000 AM 1652891229, search\_name="Manual Notable Event - Rule", orig\_time="1652891229", app="SplunkEnterpriseSecuritySuite", creator="admin", info\_max\_time="+Infinity", info\_min\_time="0.000", info\_search\_time="1652891229.659214000", owner="unassigned", rule\_description="My new notable", rule\_title="New Notable", security\_domain="access", status="1", urgency="medium" source = Manual Notable Event - Rule : sourcetype = stash

## Mapping Additional Fields

You can customize Splunk ES notable events by adding additional fields, as described in the [Splunk documentation](#). The additional fields can be used in mapping as the following token:

```
$result.additional_field_label$
```

The **additional\_field\_label** is the label used for the additional field.

## Mapping Date and Datetime Fields

If mapping values from Splunk to Date Picker or Date Time Picker fields in SOAR, the formatting of those values in the mapping must meet certain requirements. If you are parsing the date/datetime value from the Splunk search using a token, the value is already properly formatted and there is no additional action required. However, if you are providing a static value for the mapping, dates must be formatted as `YYYY/MM/DD`. Similarly, datetime values must be provided as `YYYY/MM/DD HH:MM:SS ±xxxx`. The `±xxxx` following the time is the UTC offset value. For example, the value for Cambridge, Massachusetts, United States is `-0500`. Be sure to include a leading zero if your offset value is a single-digit number of hours.

In Python3, you may include a colon between the hour and minute values (in the Cambridge example this is `-05:00`). However, in Python2 the UTC offset must be only the directional sign and exactly four digits. This value is optional when providing a static datetime. If you do not provide a UTC offset value, the datetime object is assumed to be in Greenwich Mean Time (GMT).

## Mapping Multiselect Fields

If mapping values from Splunk to Multiselect field in SOAR, these values must be supplied as comma separated values (CSV). If Splunk result tokens (tokens delimited by leading and trailing `$`-character) are used in mapping values, no space can be specified before the comma. For example, valid value formats to map are:

- `$result.value1$, $result.value2$, $result.value3$`

The following introduction of spaces **generates errors** when creating the case in SOAR.

- `$result.value1$, $result.value2$, $result.value3$`

When mapping values without Splunk result tokens, a space can be placed between the value after comma. The following are valid formats:

- `1,2,3`
- `1, 2, 3`
- `$result.value1$, 1, 2, 3`

These examples assume that values 1, 2, 3 and the values returned from Splunk after evaluating `$result.value1$`, `$result.value2$`, and `$result.value3$` are valid selections for the multiselect field you desire to fill or update in SOAR. You need to define these accepted values manually.

**Note:** Use single quotes around any multiselect value that contains comma or special characters.

- `'New York, NY', 'Los Angeles, CA'`

Here is an example of a Multiselect field as defined in SOAR:

## Create Incident Field

Type of field ⓘ  
Multiselect

Label for the field \* ⓘ  
Splunk Multi-select Example

API name \* ⓘ  
splunk\_multiselect\_example

Placeholder value (Optional) ⓘ  
A placeholder value

Requirement ⓘ  
Optional

Tooltip (Optional) ⓘ  
A description of this field.

Enter one value per line ✓ ✕  
Example Value 1  
Example Value 2  
Example Value 3  
Example Value 4  
Example Value 5

Select one or more options as default when creating new incidents.

Cancel

Create

## Mapping Multiple Artifacts of the Same Type

Similar to adding artifacts manually through the SOAR UI, you can add multiple artifacts of the same type at once if the artifact type allows multiple values. This setting can be found under **Customization Settings > Artifacts** in SOAR. URL's need to be separated by a space and IP addresses must be comma-separated. Artifacts can also be mapped individually.

|             |   |
|-------------|---|
| Artifact 11 | <div>IP Address ▼</div> <div>7.7.7</div> <div>description</div>           |
| Artifact 12 | <div>IP Address ▼</div> <div>8.8.8.8,9.9.9.9</div> <div>description</div> |

# Mapping event\_id for Notable Events

In SOAR, it is recommended that you create a customized field in the SOAR case for the Splunk notable event\_id. In the following example, the splunk\_notable\_event\_id of a notable event is mapped to the customized field. Refer to the *SOAR Playbook Designer Guide* for details.

**Note:** To use the update case capability and avoid creating duplicate cases, this field must have an API name of exactly splunk\_notable\_event\_id as shown below.

Edit Incident Field

Type of field ⓘ

Text

Label for the field \* ⓘ

Splunk Notable Event ID`

API name \* ⓘ

splunk\_notable\_event\_id

Placeholder value (Optional) ⓘ

A placeholder value

Requirement ⓘ

Optional

Tooltip (Optional) ⓘ

A description of this field.

Cancel

Save

# Updating the Default Case Mapping

Default mapping is provided in:

```
$SPLUNK_HOME/etc/apps/SA_QRadar_SOAR/default/alert_actions.conf
```

This default mapping includes the following tokens. The mapping also includes a hyperlink to the notable event from Splunk ES.

| Field                | Token                 |
|----------------------|-----------------------|
| Title of the notable | \$result.rule_title\$ |

| Field               | Token                       |
|---------------------|-----------------------------|
| Urgency             | \$result.urgency\$          |
| Owner               | \$result.owner\$            |
| Notable description | \$result.rule_description\$ |
| Status              | \$result.status\$           |

The following is an example of a case created in SOAR from the mapping.

The screenshot displays the IBM Security QRadar SOAR interface. At the top, the navigation bar includes 'IBM Security QRadar SOAR', 'Dashboards', 'Inbox', 'Incidents', and 'Create incident'. The user is logged in as 'Admin User' from 'Test Organization'. The main header shows '(from Splunk)' and 'Playbook progress' with 'No playbooks started'. The incident details are as follows:

- Description:** My new notable, Urgency: medium, Owner: unassigned, Status: 1. A link to the Splunk ES notable event is provided.
- Summary:** ID 2290, Phase Respond, Severity —, Date Created 05/18/2022 12:27, Date Occurred —, Date Discovered 05/18/2022 12:27, Date Determined 05/18/2022 12:27, Was personal information or personal data involved? Unknown, Incident Type —.
- People:** Created By Admin User, Owner Admin User, Members There are no members.
- Basic Details:** Name (from Splunk), Description My new notable, Urgency: medium, Owner: unassigned, Status: 1, Link to Splunk ES notable event. The ID is splunk\_notable\_event\_id: 0DE6791A-6F7D-42DC-BAF0-26D58032AE40@notable@@c71dc4f7d73d42fc61d2c7eae7a7061.

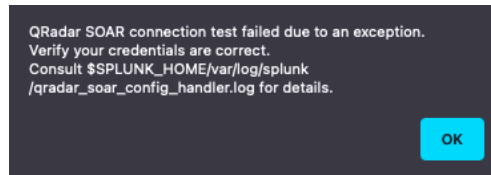
Below the description, there are tabs for Tasks, Details (selected), Breach, Notes, Members, News Feed, Attachments, Stats, Timeline, Artifacts, and Email. Under the Details tab, there are links to SentinelOne, Symantec DLP, Jira, and EXO. An 'Edit' button is visible on the right side of the incident details.

You can change the default mapping when you configure the action.

# Troubleshooting

## Setup Screen

When you click **Submit** on the QRadar SOAR Setup screen in Splunk, the app attempts to make a connection to your SOAR to verify that everything is configured correctly and to update the stored case definition. If this connection fails, you see an alert error that looks like this:



After a few seconds, the Splunk messages tab updates with detailed information about the cause of the failure.

Further information is logged to the following locations in Splunk:

- `$SPLUNK_HOME/var/log/splunk/qradar_soar_config_handler.log`
- `$SPLUNK_HOME/var/log/splunk/splunkd.log`
- `$SPLUNK_HOME/var/log/splunk/python.log`

Some common causes of these issues include:

- Forgot to uncheck the “Connect securely?” box for self-signed certificate.
- Port 443 is blocked.

## Case Not Created

If an alert or automatic escalation for correlation search fails to create a case, a message should be logged into the Splunk messages tab informing you of the issue. Further information is logged to the following location in Splunk:

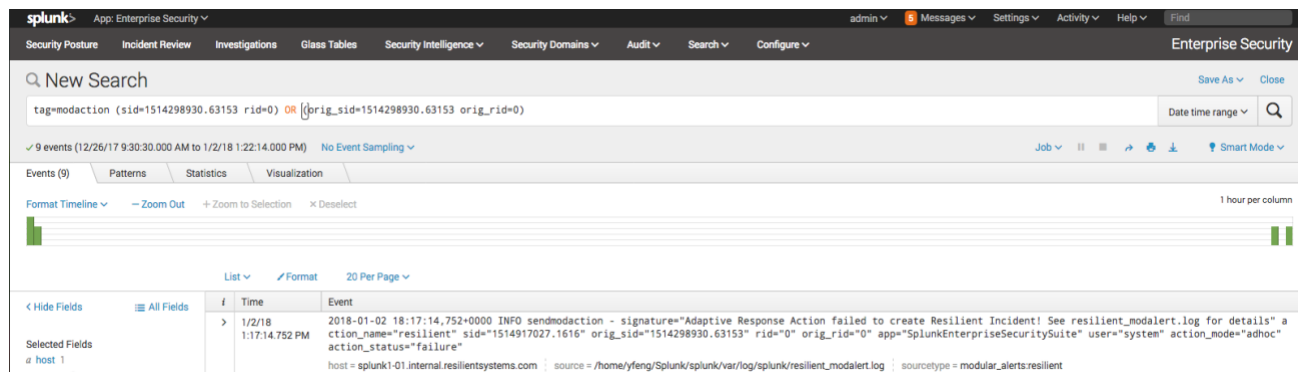
- `$SPLUNK_HOME/var/log/splunk/qradar_soar_modalert.log`

Some common causes of these issues include:

- Insufficient permissions to create a case, incident, or simulation.
- Missing mappings for required fields.
- Fields mapped with invalid values.
- Connection unavailable.

# Ad Hoc Invocation Failure

You can view the status of an ad hoc invocation when you refresh the Adaptive Response page. If it fails, click **View Adaptive Response Invocations**. In the search result, you should see a message, “See qradar\_soar\_modalert.log for details.”



You can then open `$SPLUNK_HOME/var/log/qradar_soar_modalert.log` to look for details about the failure.

If the Splunk UI dispatches an error in the UI during an adhoc invocation that reads:

*“SA\_QRadar\_SOAR could not be dispatched: ModularActionException: Invalid parameter for adhoc modular action”*

It is likely that a .conf file has been edited by a person or app other than SA\_QRadar\_SOAR. To resolve this issue, try running the setup process for SA\_QRadar\_SOAR again. If the manual action still fails to complete after re-running the setup process, you may need to manually delete all entries in `$SPLUNK_HOME/etc/apps/SA_QRadar_SOAR/local/alert_actions.conf` and run the setup process one more time to bring in the SOAR field definitions from scratch.



# Support

For additional support, go to <https://ibm.com/mysupport>.

Including relevant information will help us resolve your issue:

- version of Splunk / Splunk Cloud
- version of Enterprise Security Add-On
- version of QRadar SOAR Add-on for Splunk
- if using Splunk 8 - which Python interpreter your server is using
- steps/screenshots that will help us reproduce your issue

Including log files located in `$SPLUNK_HOME/var/log/splunk`:

- `splunkd.log`
- `python.log`
- `qradar_soar_config_handler.log`
- `qradar_soar_modalert.log`