IBM Security

IBM

IBM Resilient SOAR Platform
Add-On for Splunk User Guide
V1.1

Date: August 2020

Resilient SOAR Platform
Add-On for Splunk User Guide

Version	Publication	Notes
1.1	August 2020	Added support for Python 3.
1.0	April 2018	Updated Splunk version number.
1.0	January 2018	Initial publication.

Table of Contents

Overview

The Resilient Add-On supports Splunk and Splunk ES. The Add-On provides the capability of escalating a Splunk alert or Splunk ES notable event to a Resilient incident.

The Resilient Add-On features include:

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

Installation

Requirements

The following lists the system requirements:

- Splunk version 8.0 or later for Python 3 support.
- Splunk ES 6.1.0 or later (only if working with Notable Events) for Python 3 support.
- Splunk CIM Framework. **Note:** The Add-On depends on Splunk CIM. Please install CIM before installing the Add-On.
- Resilient platform version 35 or later.
- Ability to connect directly from Splunk to your Resilient platform with HTTPS on port 443.
- A dedicated Resilient Administrator or equivalent account on the Resilient 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.

  NOTE: Connecting to Resilient with API keys is not supported. You must use an account username and password.

  NOTE: Should you later change the dedicated Resilient account to another user, the new user 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 Resilient Add-On and for all other users that need to add the Add-On as an Alert Action or an Adaptive Response action for a correlation search.

Installation and Setup

For Splunk Cloud and Splunk ES Cloud users, contact Splunk Support to create a ticket for installing the Resilient Add-On.

If you have installed Splunk or Splunk on-premises, you can download and install the add-on from Splunkbase. Alternatively, you can request an installer from IBM Resilient.

After installing the add-on and restarting Splunk, navigate back to the App Manager screen. Click **Set up** in the Resilient row. Fill out the required attributes for your Resilient platform and click **Save**. When you save, the Set Up program performs the following:

- Retrieves the incident definition from the Resilient platform, so that all fields, including custom fields, are catalogued.

  NOTE: If a Resilient administrator adds custom fields after you run Set Up, you need to run Set Up again to capture the fields.

- 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

Hostname for Resilient server: Hostname or IP for your Resilient platform. Do not include the https:// prefix.

Connect Securely: Do not check if using self-signed certificates on your Resilient platform.

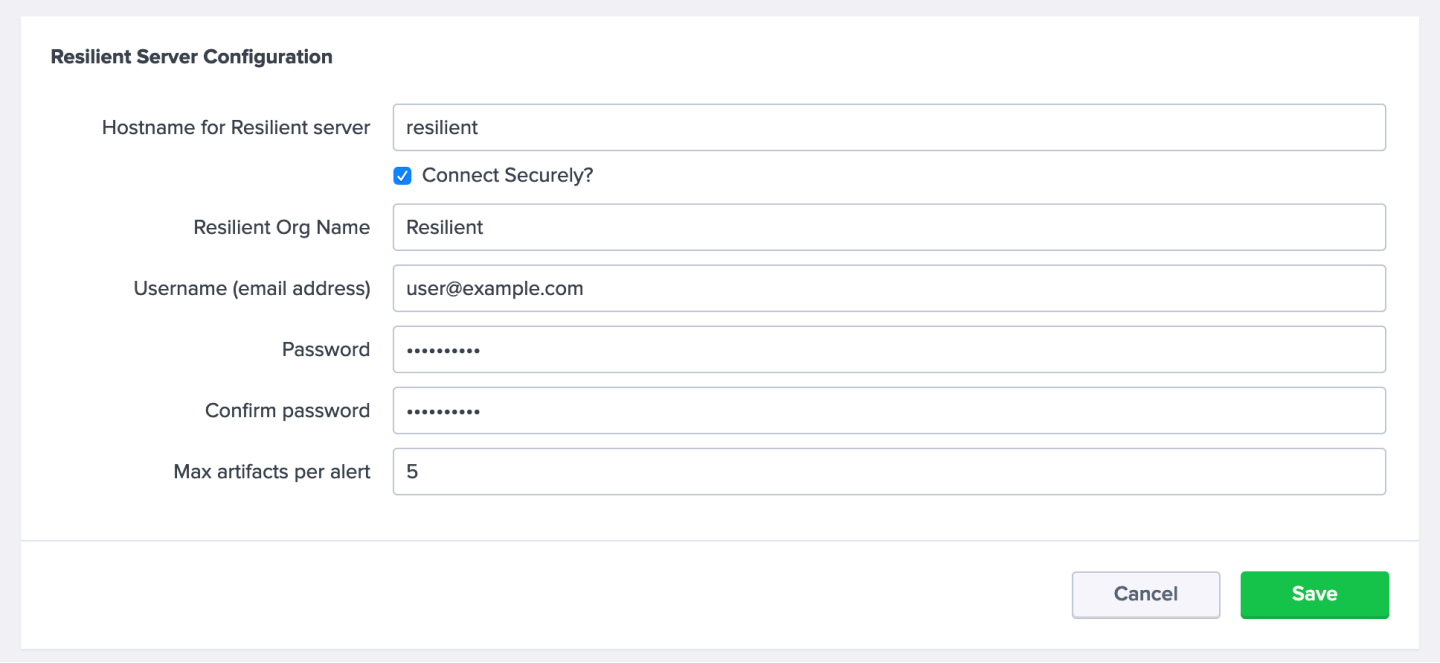
Resilient Org Name: The name of the Resilient organization.

Username (email address): Username of the registered Resilient master administrator or equivalent account.

Password: Password for the Resilient account.

Max Artifacts per alert: Maximum number of artifacts you may need to map into a single Resilient incident from any given Splunk alert or Splunk ES notable event.

Note: Connecting to Resilient with API keys is not supported. You must use an account username and password.



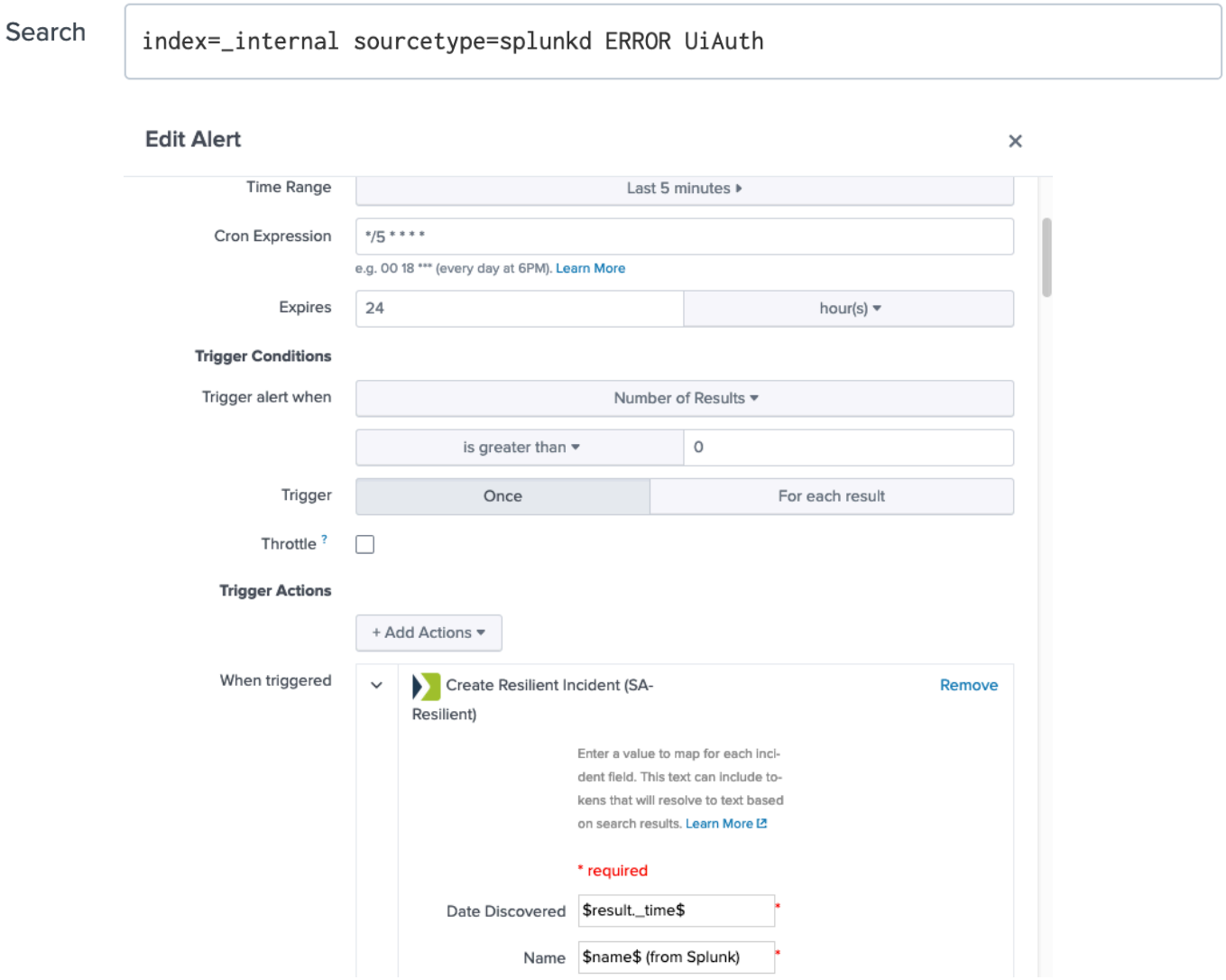
Escalating Splunk Alerts

Adding a Splunk Alert Action

To add a Resilient 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 Resilient incident. Click **Edit** and select **Edit Actions**. Click **+ Add Actions** and select **Resilient**. Update the incident 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, sa_failed_splunk_login, is included. If you enable this alert, a Resilient incident is created each time there is a failed login attempt to Splunk. If you have added custom required fields to your Resilient platform, you need to edit the mapping on the alert action screen to include them before triggering the example.



Mapping Date and Datetime Fields

If mapping values from Splunk to Date Picker or Date Time Picker fields in the Resilient platform, 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

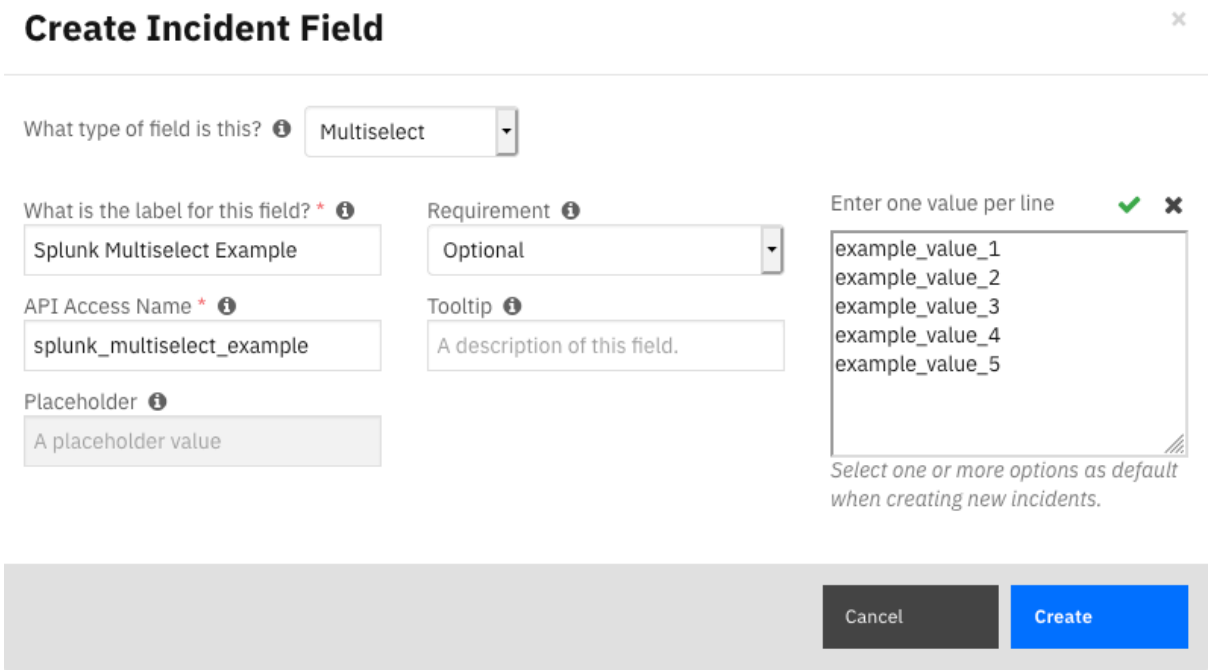
If mapping values from Splunk to Multiselect field in the Resilient platform, these values must be supplied as comma separated values (CSV) with no spaces. For example, two valid value formats to map are:

- *1,2,3*
- *$result.value1$,$result.value2$,$result.value3$*

The following introduction of spaces generates errors when creating the incident in the Resilient platform.

- *1, 2,3*
- *$result.value1$,$result.value2$, $result.value3$*

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 the Resilient platform. You need to define these accepted values manually.



Mapping Multiple Artifacts of the Same Type

Similar to adding artifacts manually through the Resilient 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 the Resilient platform. URL's need to be separated by a space and IP addresses must be comma-separated. Artifacts can also be mapped individually.

Updating the Default Incident Mapping

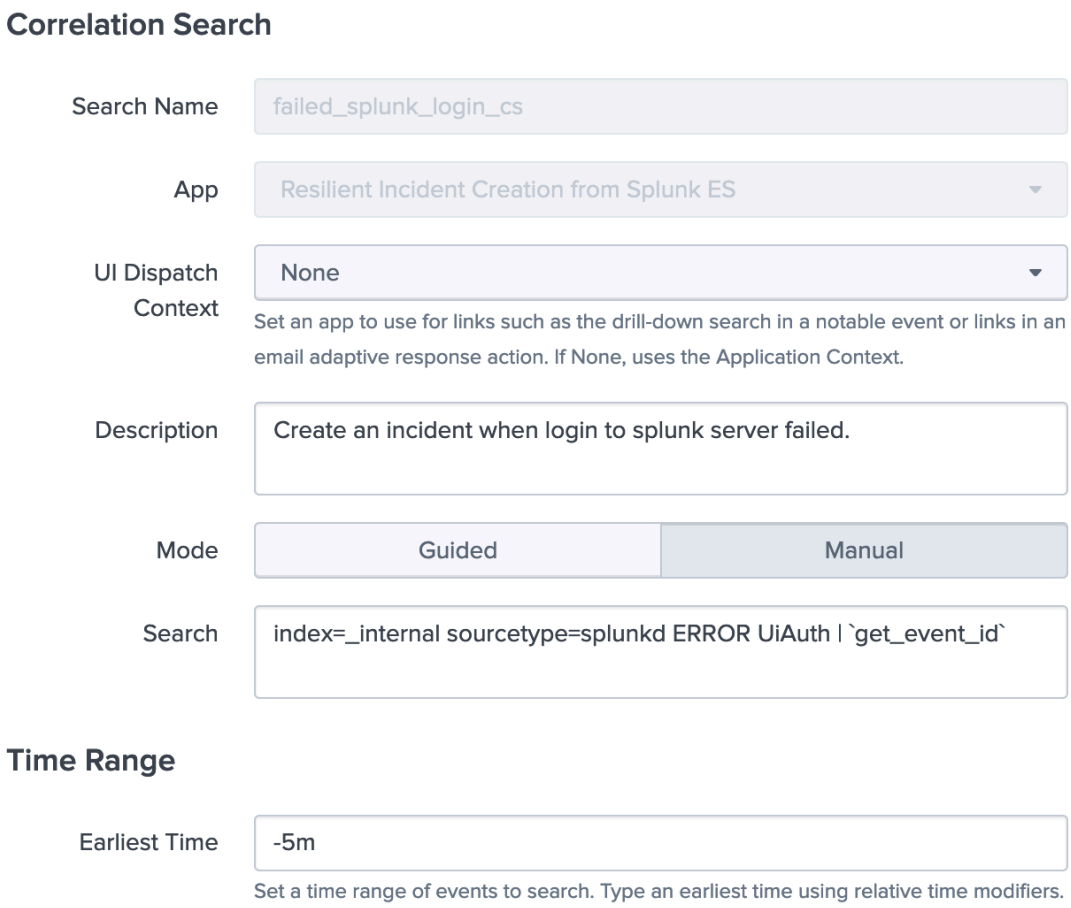
You can change the default mapping when you configure the action. If the incident mapping for most of your alerts will be very similar, you may want to override the default mapping where all the alerts start. Create an alert_actions.conf in *$SPLUNK_HOME/etc/apps/SA-resilient/local* and override the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

Escalating Splunk ES Notable Events

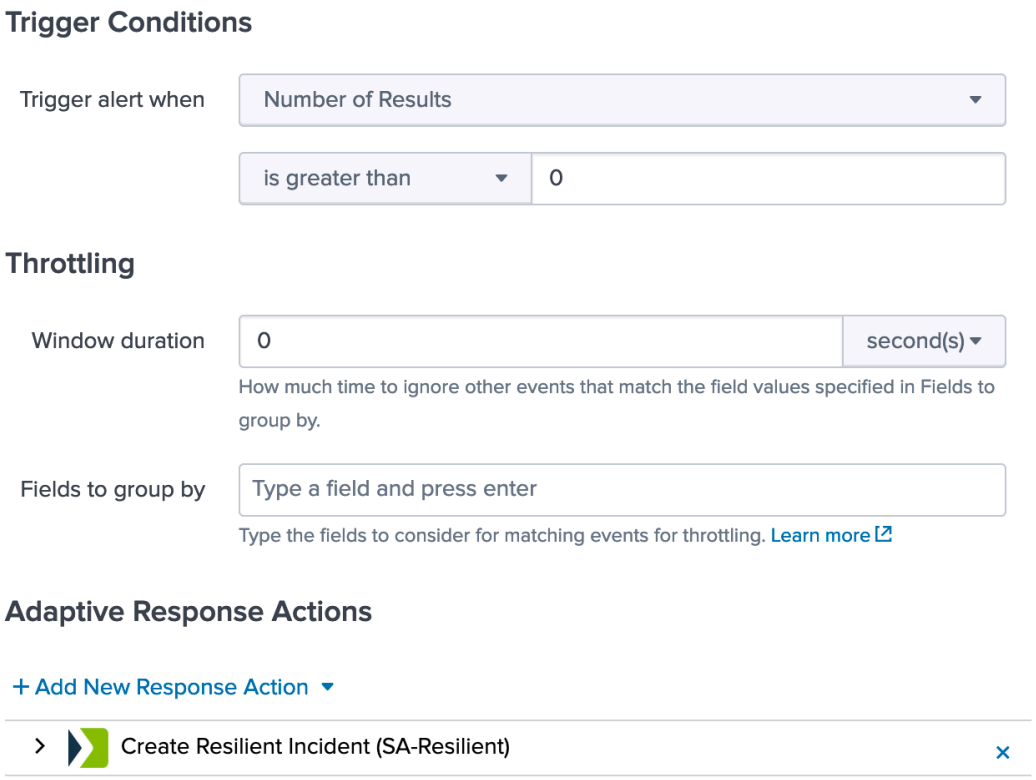
Adding an Adaptive Response Action

To add a Resilient 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 Resilient incident and scroll down to the **Adaptive Response Actions** section. Click **+ Add New Response Action** and select **Create Resilient Incident (SA-Resilient)**. Update the incident 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_cs, is included, which you can find in **Content Management**.

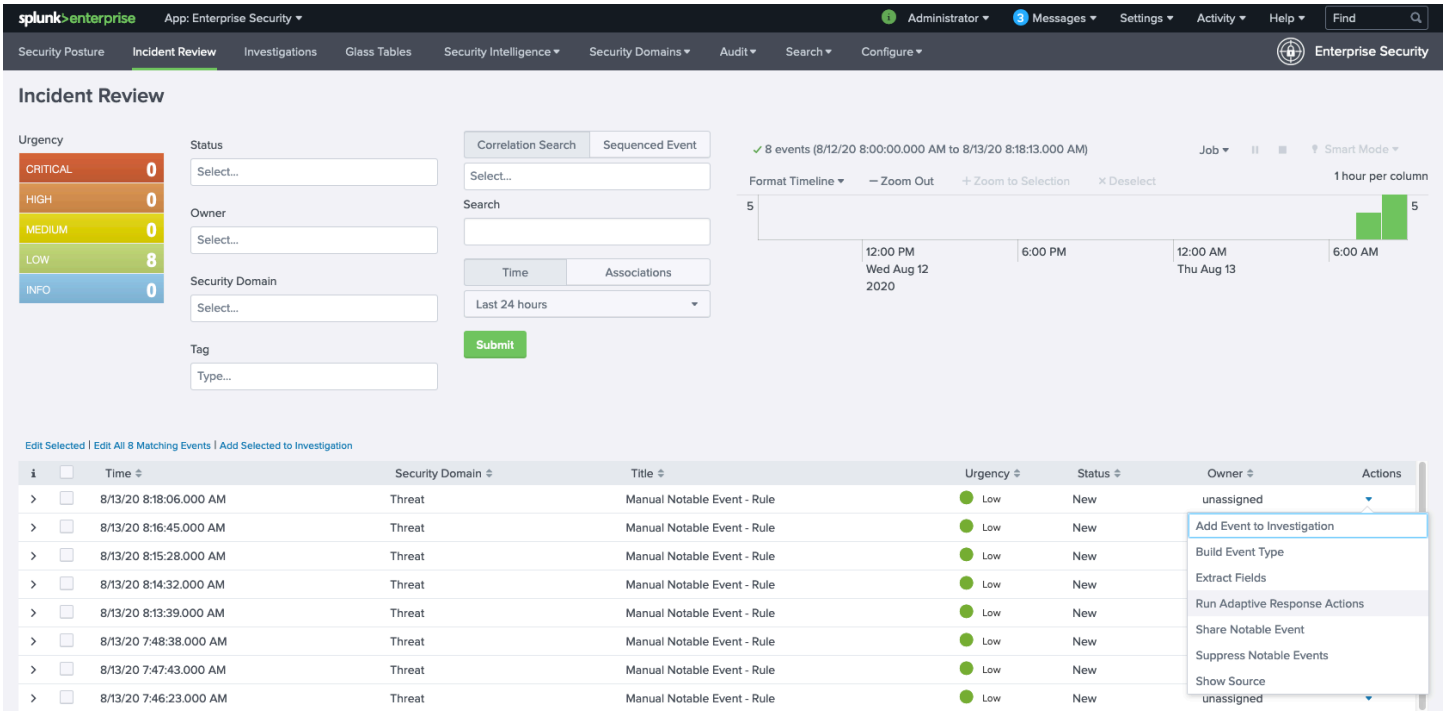


Scroll down to the Adaptive Response Actions section and view that the Resilient Add-On has been added as a response in this sample correlation search. You can change the default configuration.

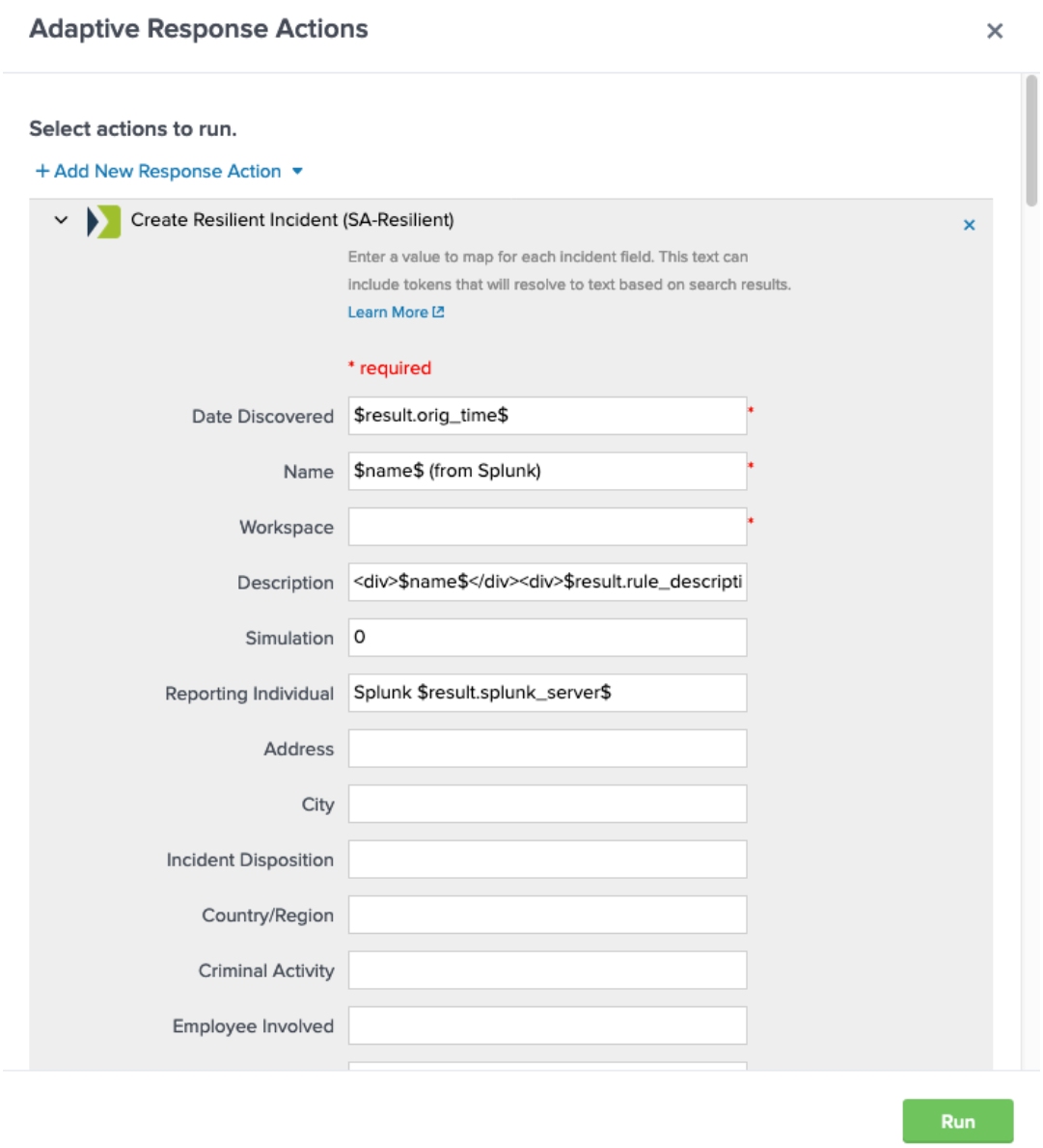


Ad Hoc Invocation

You can dispatch Resilient 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.



Click **+ Add New Response Action** and select **Create Resilient Incident (SA-Resilient).** Update the incident fields to indicate how you want them mapped.



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

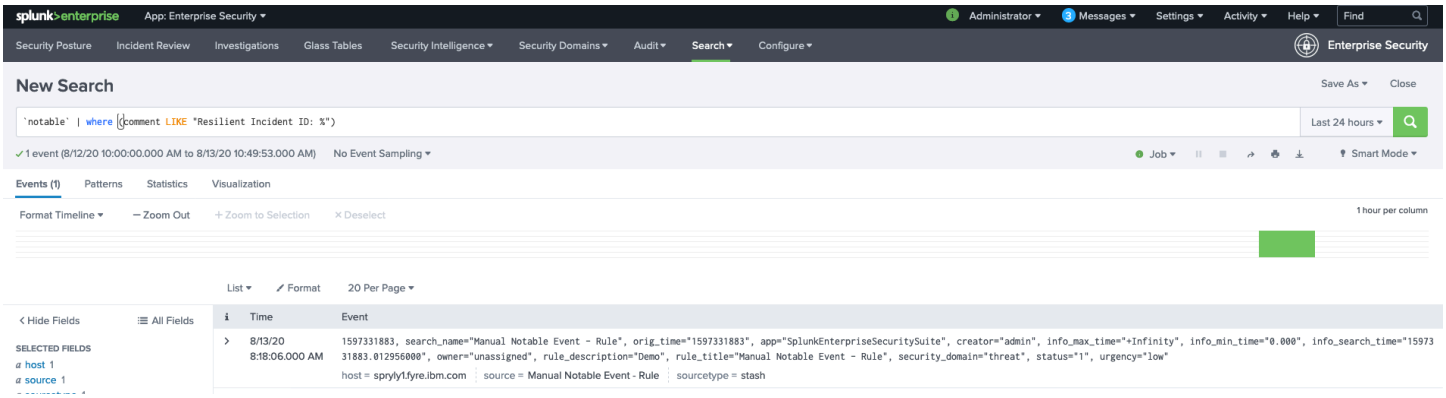
Adaptive Responses:

Response	Mode	Time	User	Status
Create Resilient Incident (SA-Resilient)	saved	2020-08-28T10:15:08-0700	nobody	✓ success
Notable	saved	2020-08-28T10:15:07-0700	nobody	✓ success

View Adaptive Response Invocations

Show Escalated Notable Events

Each time a notable event is escalated successfully, the corresponding Resilient 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 "Resilient Incident ID: %")**, in the **Search** tab of **Enterprise Security**. For example:



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 the Resilient platform, 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

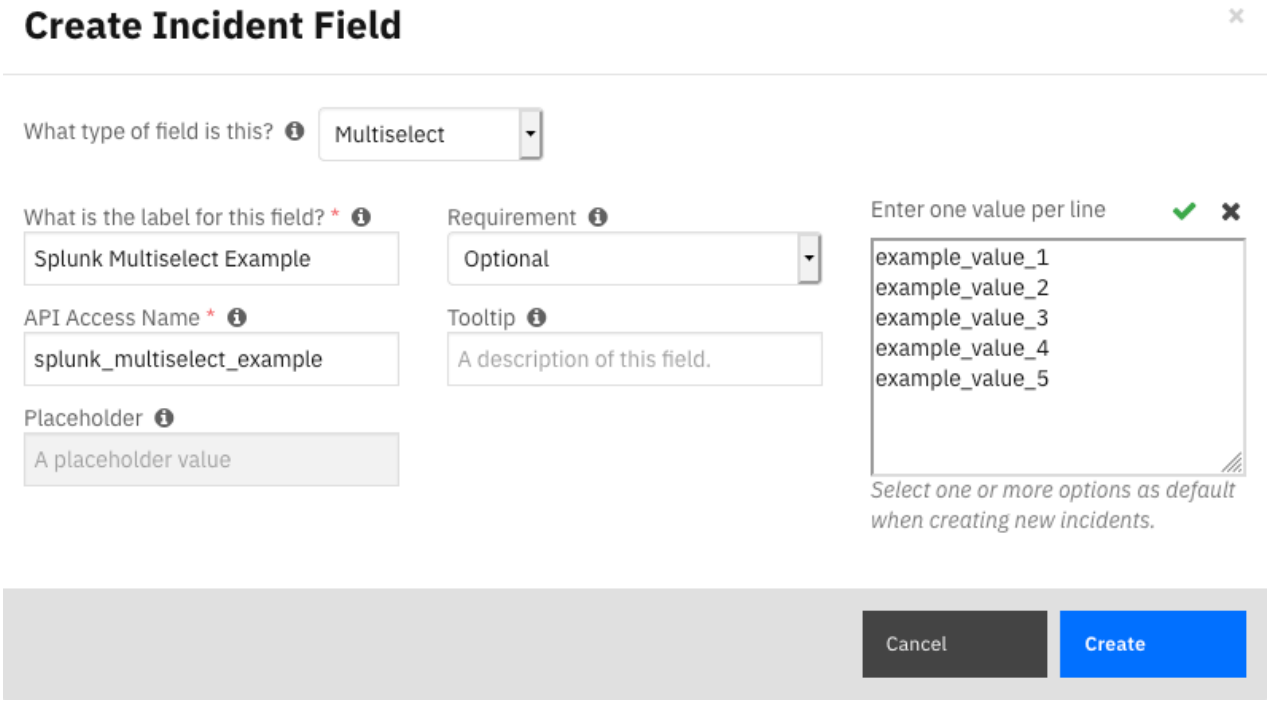
If mapping values from Splunk to Multiselect field in the Resilient platform, these values must be supplied as comma separated values (CSV) with no spaces. For example, two valid value formats to map are:

- *1,2,3*
- *$result.value1$,$result.value2$,$result.value3$*

The following introduction of spaces generates errors when creating the incident in the Resilient platform.

- *1, 2,3*
- *$result.value1$,$result.value2$, $result.value3$*

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 the Resilient platform. You need to define these accepted values manually.

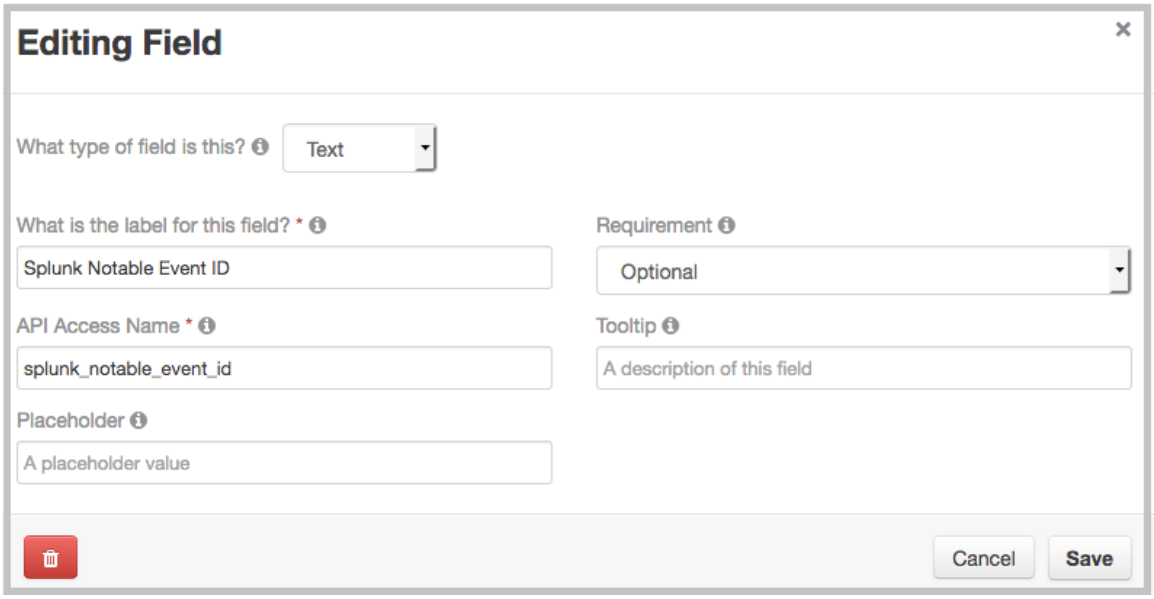


Mapping Multiple Artifacts of the Same Type

Similar to adding artifacts manually through the Resilient 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 the Resilient platform. URL's need to be separated by a space and IP addresses must be comma-separated. Artifacts can also be mapped individually.

Mapping event_id for Notable Events

In the Resilient platform, it is recommended that you create a customized field for the Resilient incident for notable event_id. In the following example, the event_id of a notable event is mapped to the customized field. Refer to the *Resilient SOAR Platform Playbook Designer Guide* for details.



Updating the Default Incident Mapping

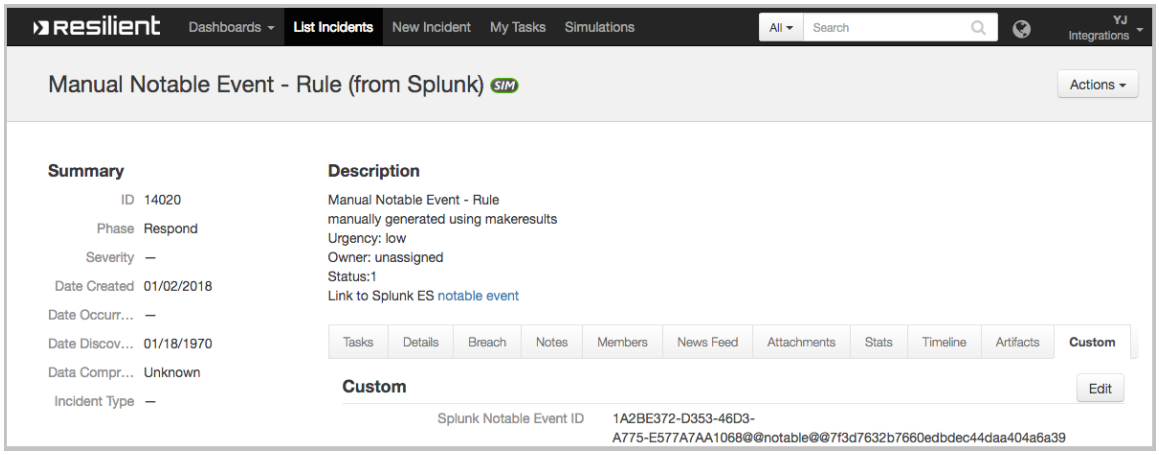
Default mapping is provided in:

```
$SPLUNK_HOME/etc/apps/SA-Resilient/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	$result.rule_title$
Urgency	$result.urgency$
Owner	$result.owner$
Notable description	$result.rule_description$
Status	$result.status$

The following is an example of an incident created in the Resilient platform from the mapping.

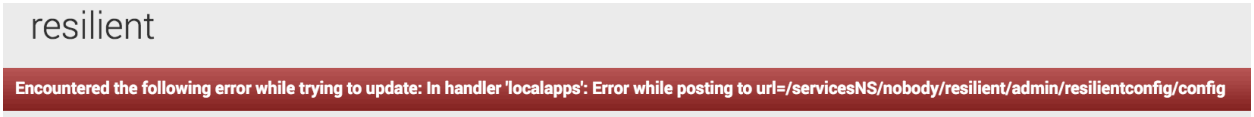


You can change the default mapping when you configure the action.

Troubleshooting

Setup Screen

When you click **Save** on the Resilient Setup screen in Splunk, the app attempts to make a connection to your Resilient platform to verify that everything is configured correctly and to update the stored incident definition. If this connection fails, you see an 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/resilient_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.

Incident Not Created

If an alert or automatic escalation for correlation search fails to create an incident, 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:

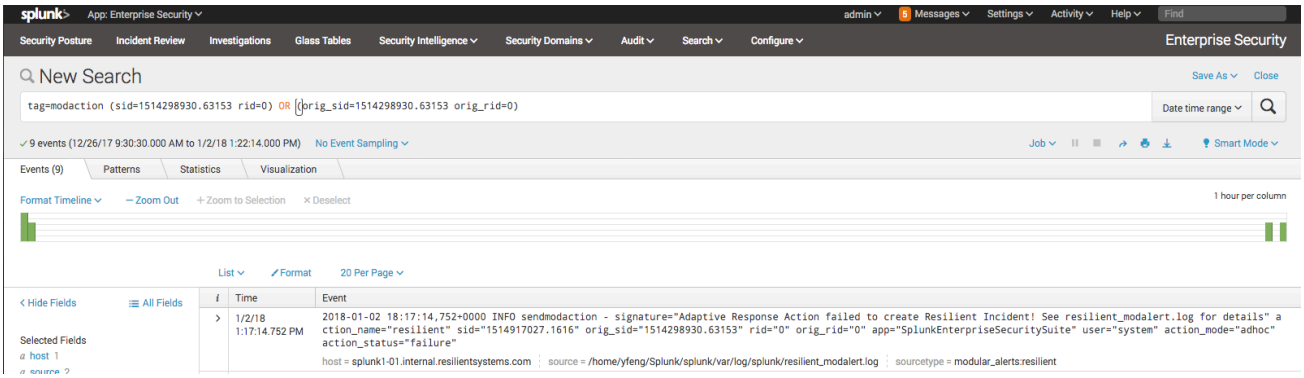
- $SPLUNK_HOME/var/log/splunk/resilient_modalert.log

Some common causes of these issues include:

- Insufficient permissions to create an 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 resilient_modalert.log for details.”



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

Support

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

Including relevant information will help us resolve your issue:

- version of Splunk server
- version of Enterprise Security Add-On
- version of Resilient Add-On
- 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
- resilient_config_handler.log
- resilient_modalert.log