

# Module 13

## Creating Scheduled Reports and Alerts

# Why Scheduled Reports?

Scheduled Reports are useful for:

- Monthly, weekly, daily executive/managerial roll up reports
- Dashboard performance
- Automatically sending reports via email

# Creating a Scheduled Report

1. Create your search
2. From the Save As menu, select Report

The screenshot shows the 'New Search' interface in Splunk. The search query is 'index=security fail\* root'. The results show 212 events from 1/9/18 7:00:00.000 PM to 1/10/18 7:05:31.000 PM. The 'Save As' menu is open, and 'Report' is selected. The interface also shows a timeline visualization and a list of events.

**New Search** Save As ▾ Close

index=security fail\* root

✓ 212 events (1/9/18 7:00:00.000 PM to 1/10/18 7:05:31.000 PM) No Event Sampling ▾ Job ▾ || ■ → ↻

Events (212) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect 1 hour per column

List ▾ / Format 20 Per Page ▾

< Prev 1 2 3 4 5 6 7 8 9 ... Next >

< Hide Fields All Fields

SELECTED FIELDS

- a host 4
- a source 4
- a sourcetype 1

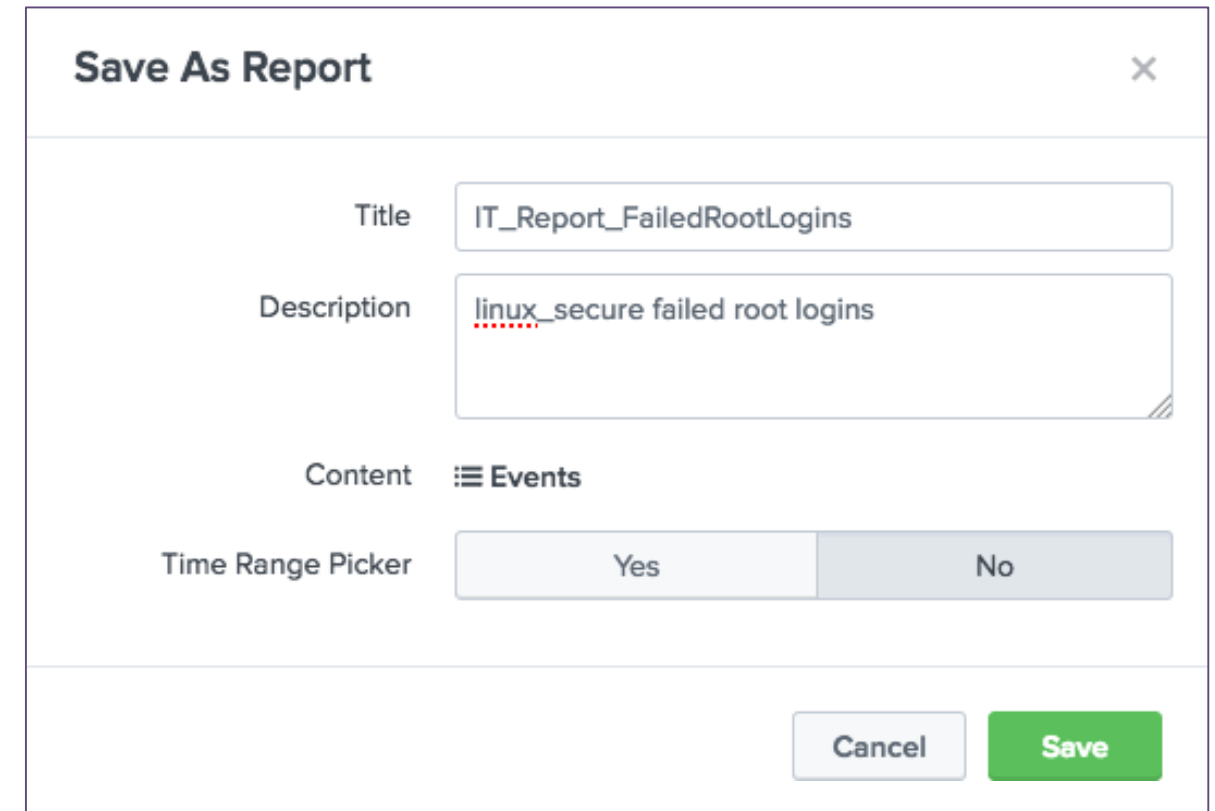
INTERESTING FIELDS

- a action 1

i	Time	Event
>	1/10/18 6:26:20.000 PM	Wed Jan 10 2018 18:26:20 www3 sshd[5509]: Failed password for root from 87.194.216.51 port 1220 ssh2 host = www3   source = /opt/log/www3/secure.log   sourcetype = linux_secure
>	1/10/18 6:15:51.000 PM	Wed Jan 10 2018 18:15:51 www1 sshd[2276]: Failed password for root from 221.207.229.6 port 2505 ssh2 host = www1   source = /opt/log/www1/secure.log   sourcetype = linux_secure

# Creating a Scheduled Report (cont.)

3. Enter Title
4. Enter Description
5. Set Time Range Picker to No
6. Click Save



The screenshot shows a 'Save As Report' dialog box with a close button (X) in the top right corner. It contains four fields: 'Title' with the text 'IT\_Report\_FailedRootLogins', 'Description' with the text 'linux\_secure failed root logins' (where 'linux\_secure' is underlined in red), 'Content' with a menu icon and the text 'Events', and 'Time Range Picker' with two buttons: 'Yes' and 'No'. The 'No' button is highlighted. At the bottom right are 'Cancel' and 'Save' buttons.

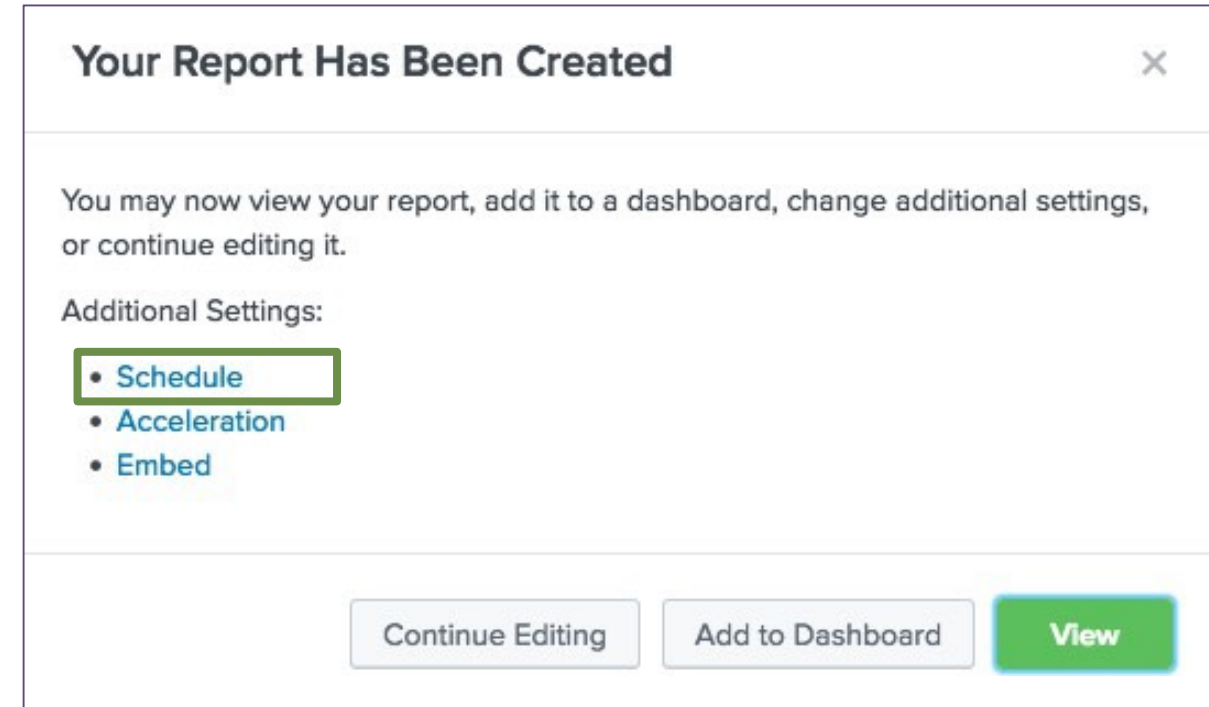
## Note



Time Range Picker cannot be used with scheduled reports.

# Creating a Scheduled Report (cont.)

- After the report is created, click Schedule
- If you inadvertently set Time Range Picker to Yes on previous screen, a warning displays and time picker is disabled



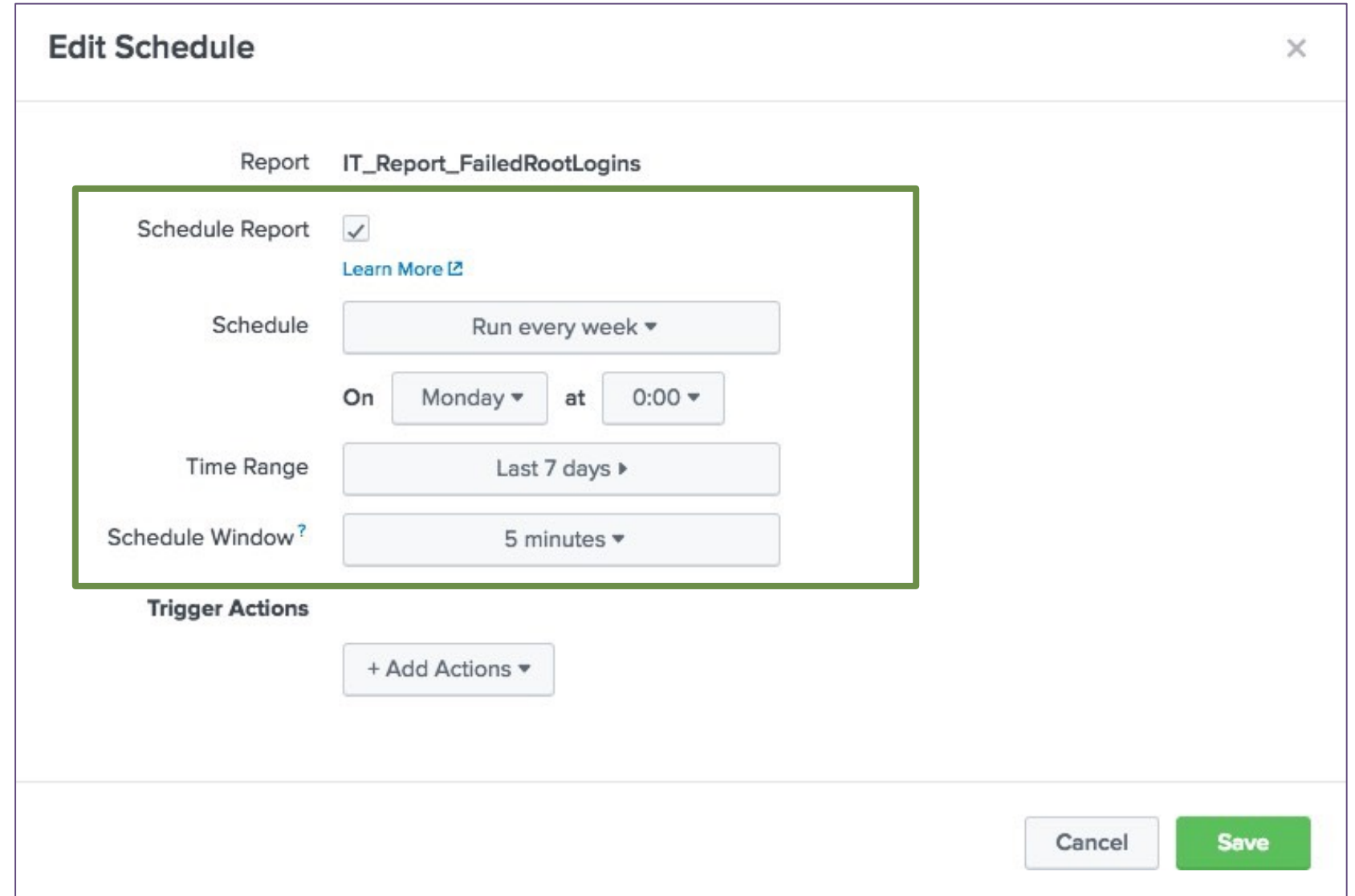
 Scheduling this report results in removal of the time picker from the report display.

## Note

Depending on the permissions granted to you by your Splunk administrator, you may be able to set permissions to share your scheduled report.

# Creating a Scheduled Report – Define Schedule

- Schedule Report – select this checkbox
- Schedule – select the frequency to run the report
  - Run every hour
  - Run every day
  - Run every week
  - Run every month
  - Run on Cron Schedule



The screenshot shows the 'Edit Schedule' dialog box for the report 'IT\_Report\_FailedRootLogins'. The dialog is titled 'Edit Schedule' and has a close button (X) in the top right corner. The report name 'IT\_Report\_FailedRootLogins' is displayed at the top. The 'Schedule Report' checkbox is checked, and a 'Learn More' link is visible below it. The 'Schedule' dropdown is set to 'Run every week'. The 'On' dropdown is set to 'Monday' and the 'at' dropdown is set to '0:00'. The 'Time Range' dropdown is set to 'Last 7 days'. The 'Schedule Window' dropdown is set to '5 minutes'. Below these settings is a 'Trigger Actions' section with a '+ Add Actions' button. At the bottom right of the dialog are 'Cancel' and 'Save' buttons.

Report IT\_Report\_FailedRootLogins

Schedule Report ☒ [Learn More](#)

Schedule Run every week ▼

On Monday ▼ at 0:00 ▼

Time Range Last 7 days ▶

Schedule Window? 5 minutes ▼

Trigger Actions

+ Add Actions ▼

Cancel Save

# Creating a Scheduled Report – Select Time Range

- Time Range – By default, search time range used
  - Click the Time Range button to change the time range
  - You can select a time range from Presets, Relative, or Advanced
  - Typically, the time range is relative to the Schedule

Edit Schedule

Report

IT\_Report\_FailedRootLogins

Schedule Report

☒

[Learn More](#)

Schedule

Run every week ▾

On

Monday ▾

at

0:00 ▾

Time Range

Last 7 days ▸

Schedule Window?

5 minutes ▾

Trigger Actions

+ Add Actions ▾

Select Time Range

Presets

RELATIVE

Today

Week to date

Business week to date

Month to date

Year to date

Yesterday

Previous week

Previous business week

Previous month

Previous year

OTHER

All time

Last 15 minutes

Last 60 minutes

Last 4 hours

Last 24 hours

Last 7 days

Last 30 days

> Relative

> Advanced

Back

Note

Users with admin privileges can also select a Schedule Priority of Default, Higher, or Highest.

# Creating a Scheduled Report – Schedule Window

- Schedule Window – this setting determines a time frame to run the report
  - If there are other reports scheduled to run at the same time, you can provide a window in which to run the report
  - This setting provides efficiency when scheduling several reports to run
- After you configure the report schedule, click Next

The screenshot shows the 'Edit Schedule' configuration window for a report named 'IT\_Report\_FailedRootLogins'. The 'Schedule Report' checkbox is checked, and a 'Learn More' link is visible. The 'Schedule' is set to 'Run every week'. The 'On' day is 'Monday' at '0:00'. The 'Time Range' is 'Last 7 days'. The 'Schedule Window' is highlighted with a green box and set to '5 minutes'. A dropdown menu for 'Trigger Actions' is open, showing options: 'Auto', 'No window', '5 minutes' (selected with a checkmark), '15 minutes', '30 minutes', '1 hour', '2 hours', '4 hours', and '8 hours'. At the bottom, a log shows the report was triggered at 6:15:51.000 PM on 1/10/18.

**Edit Schedule**

Report IT\_Report\_FailedRootLogins

Schedule Report ☒ [Learn More](#)

Schedule Run every week ▼

On Monday ▼ at 0:00 ▼

Time Range Last 7 days ▶

Schedule Window? 5 minutes ▼

Trigger Actions

- Auto
- No window
- ✓ 5 minutes
- 15 minutes
- 30 minutes
- 1 hour
- 2 hours
- 4 hours
- 8 hours

6:15:51.000 PM host = w  
1/10/18 Wed Jan  
6:14:03.000 PM host = m



# Creating a Scheduled Report – Add Actions

- **Log Event** – creates an indexed, searchable log event
- **Output results to lookup** – sends results of search to CSV lookup file
- **Output results to telemetry endpoint** – sends usage metrics back to Splunk (if your company has opted-in to program)
- **Run a script** – runs a previously created script
- **Send email** – sends an email with results to specified recipients
- **Webhook** – sends an HTTP POST request to specified URL

The screenshot shows the 'Edit Schedule' dialog box in Splunk. The report is named 'IT\_Report\_FailedRootLogins'. The 'Schedule Report' checkbox is checked, with a 'Learn More' link below it. The 'Schedule' dropdown is set to 'Run every week'. The 'On' dropdown is set to 'Monday' and the 'at' dropdown is set to '6:00'. The 'Time Range' dropdown is set to 'Last 7 days'. The 'Schedule Window' dropdown is set to '5 minutes'. Below these settings is a section titled 'Trigger Actions' with a '+ Add Actions' button. A list of actions is shown, including 'Log Event', 'Output results to lookup', 'Output results to telemetry endpoint', 'Run a script', and 'Send email'. The 'Log Event' action is highlighted with a green box. At the bottom right of the dialog are 'Cancel' and 'Save' buttons. The background shows a log viewer with entries from '3/12/18'.

# Creating a Scheduled Report – Send Email

1. Enter addresses in the To field, separated by commas
2. Set the priority
3. Edit or keep the default subject  
The \$name\$ variable includes the name of the report
4. If desired, include other options, such as an inline table of results
5. Define the email text type
6. Click Save

The screenshot shows the 'Send email' configuration interface. At the top, it says 'When triggered' with a dropdown arrow, followed by an envelope icon and the text 'Send email'. A 'Remove' link is in the top right corner. The configuration fields are as follows:

- To:** A text input field. To its right, a note says 'Comma separated list of email addresses.' with a link 'Show CC and BCC'.
- Priority:** A dropdown menu currently set to 'Normal'.
- Subject:** A text input field containing 'Splunk Report: \$name\$'.
- Message:** A text input field containing 'The scheduled report '\$name\$' has run.' To its right, a note says 'The email subject, recipients and message can include tokens that insert text based on the results of the search.' with a link 'Learn More'.
- Include:** A section with six checkboxes:
  - ☒ Link to Report
  - ☒ Link to Results
  - ☐ Search String
  - ☐ Inline Table (with a dropdown arrow)
  - ☐ Attach CSV
  - ☐ Attach PDF
- Type:** Two buttons: 'HTML & Plain Text' (selected) and 'Plain Text'.

# Managing Reports – Edit Permissions

## Reports

Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report. Open the report in Pivot or Search to refine the parameters or further explore the data.

1 Reports

All Yours This App's

i	Title ^	Actions	Next Scheduled Time ↕	Owner ↕	App ↕	Sharing ↕
>	IT_Report_FailedRootLogins	Open in Search Edit ▾	None	student1	class_Fund1	Private

Edit Description

Edit Permissions

Edit Schedule

Edit Acceleration

Clone

Embed

Delete

## Note

The proper permissions from your Splunk administrator are required to edit the permissions on a scheduled report.

### Edit Permissions

Report IT\_Report\_FailedRootLogins

Owner student1

App class\_Fund1

Display For 

Owner App All apps

Run As 

Owner User

[Learn More](#)

	Read	Write
Everyone	<input type="checkbox"/>	<input type="checkbox"/>
admin	<input type="checkbox"/>	<input type="checkbox"/>
can_delete	<input type="checkbox"/>	<input type="checkbox"/>
power	<input type="checkbox"/>	<input type="checkbox"/>
splunk-system-role	<input type="checkbox"/>	<input type="checkbox"/>
student	<input type="checkbox"/>	<input type="checkbox"/>
user	<input type="checkbox"/>	<input type="checkbox"/>
windows-admin	<input type="checkbox"/>	<input type="checkbox"/>

Cancel

Save

# Managing Reports – Edit Permissions (cont.)

- Run As determines which user profile is used at run time
  - Owner – all data accessible by the owner appears in the report
  - User – only data allowed to be accessed by the user role appears

**Reports**

Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report. Open the report in Pivot or Search to refine the parameters or further explore the data.

1 Reports

All Yours This App's filter

i	Title ^	Actions	Next Scheduled Time ↕	Owner ↕	App ↕	Sharing ↕
>	IT_Report_FailedRootLogins	Open in Search Edit ▾	None	student1	class_Fund1	Private
<div>Edit Description</div> <div>Edit Permissions</div> <div>Edit Schedule</div> <div>Edit Acceleration</div> <div>Clone</div> <div>Embed</div> <div>Delete</div>						

**Edit Permissions** ✕

Report IT\_Report\_FailedRootLogins

Owner student1

App class\_Fund1

Display For Owner App All apps

Run As Owner User

[Learn more](#)

	Read	Write
Everyone	<input type="checkbox"/>	<input type="checkbox"/>
admin	<input type="checkbox"/>	<input type="checkbox"/>
can_delete	<input type="checkbox"/>	<input type="checkbox"/>
power	<input type="checkbox"/>	<input type="checkbox"/>
splunk-system-role	<input type="checkbox"/>	<input type="checkbox"/>
student	<input type="checkbox"/>	<input type="checkbox"/>
user	<input type="checkbox"/>	<input type="checkbox"/>
windows-admin	<input type="checkbox"/>	<input type="checkbox"/>

Cancel Save

- To access the report results from a webpage, click Edit > Embed
  - Before a report can be embedded, it must be scheduled

13

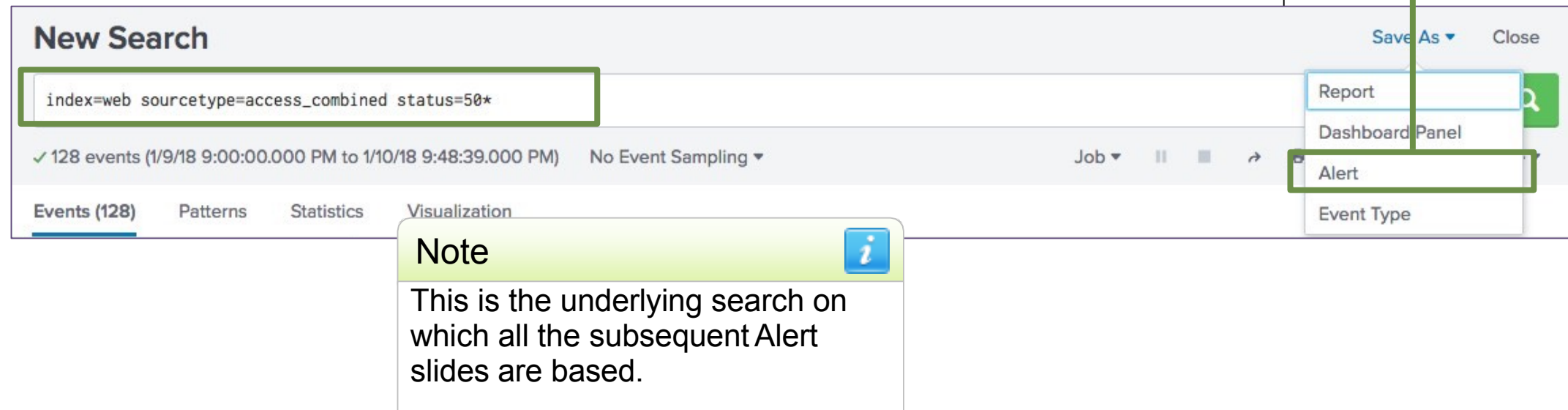
# What Are Alerts?

- Splunk alerts are based on searches that can run either:
  - On a regular scheduled interval
  - In real-time
- Alerts are triggered when the results of the search meet a specific condition that you define
- Based on your needs, alerts can:
  - Create an entry in Triggered Alerts
  - Log an event
  - Output results to a lookup file
  - Send emails
  - Use a webhook
  - Perform a custom action

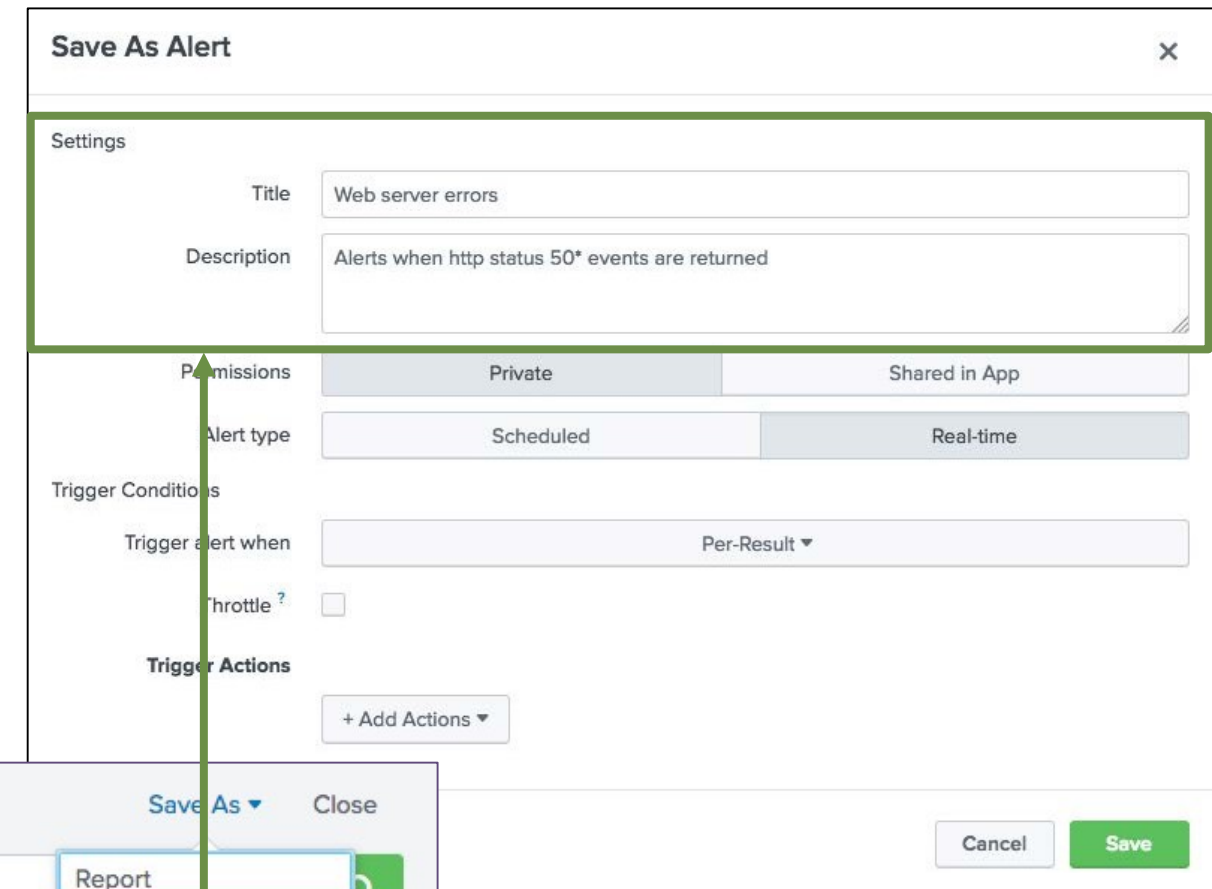


# Creating an Alert

- Run a search
  - In this example, you're searching for server errors—any HTTP request status that begins with 50 over the last 5 minutes
- Select Save As > Alert
- Give the alert a Title and Description



The screenshot shows the Splunk 'New Search' interface. The search bar contains the query `index=web sourcetype=access_combined status=50*`. Below the search bar, it indicates '128 events' and provides a time range. The 'Save As' dropdown menu is open, showing options: Report, Dashboard Panel, Alert, and Event Type. The 'Alert' option is highlighted with a green box. A green arrow points from the 'Alert' option to the 'Save As Alert' dialog box shown in the top right. A note box at the bottom states: 'Note: This is the underlying search on which all the subsequent Alert slides are based.'



The 'Save As Alert' dialog box is shown. It has a 'Settings' section with a 'Title' field containing 'Web server errors' and a 'Description' field containing 'Alerts when http status 50\* events are returned'. Below this are 'Permissions' (Private/Shared in App), 'Alert type' (Scheduled/Real-time), 'Trigger Conditions' (Trigger alert when: Per-Result), and 'Trigger Actions' (+ Add Actions). At the bottom are 'Cancel' and 'Save' buttons. A green box highlights the 'Title' and 'Description' fields, and a green arrow points from the 'Alert' option in the 'Save As' dropdown to this dialog.

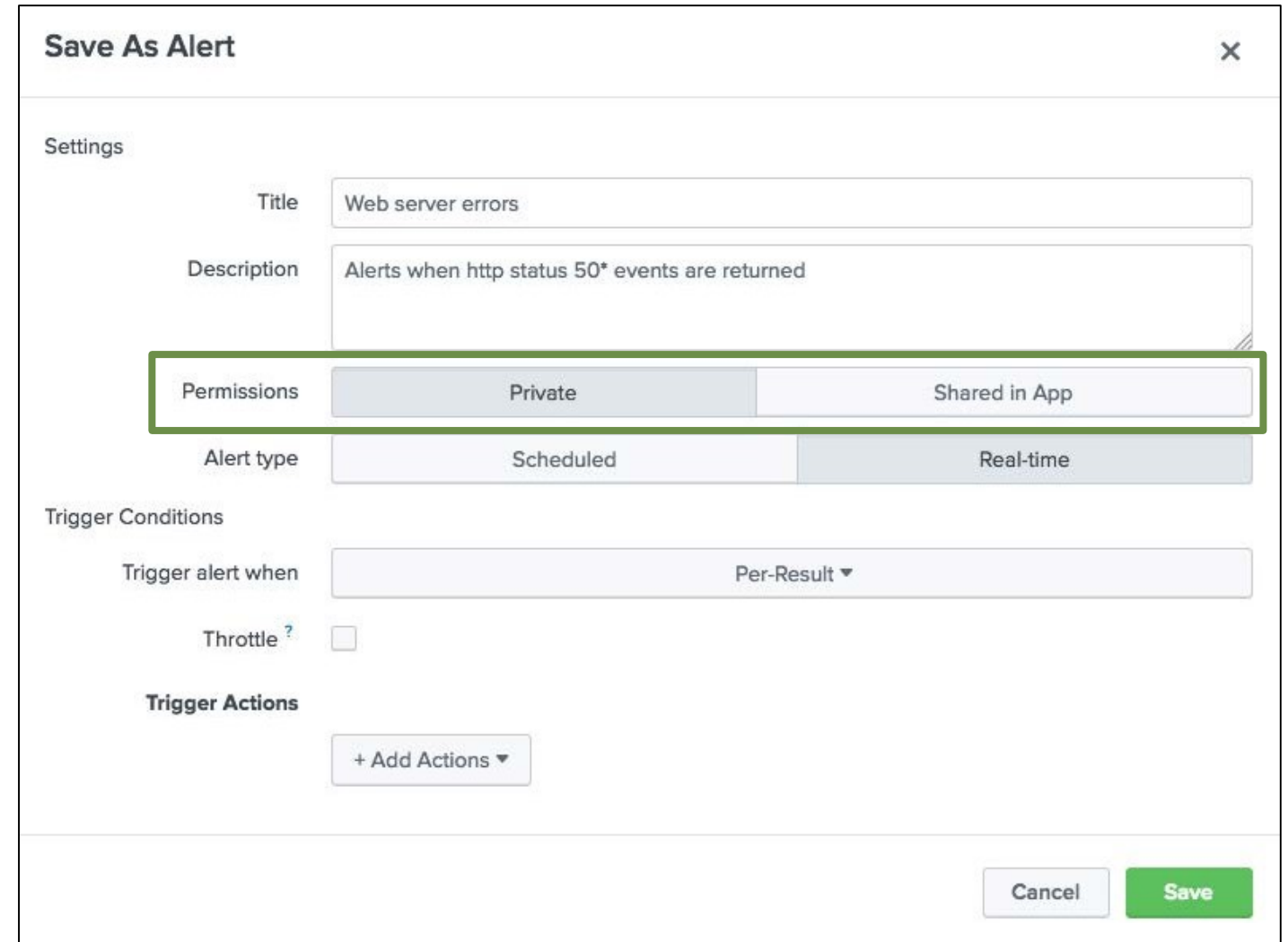
# Setting Alert Permissions

- Private – only you can access, edit, and view triggered alerts
- Shared in app
  - All users of the app can view triggered alerts
  - By default, everyone has read access and power has write access to the alert

## Note



The proper permissions from your Splunk administrator are required to set the permissions on an alert.



The image shows a 'Save As Alert' dialog box with a close button (X) in the top right corner. The dialog is divided into several sections: 'Settings', 'Trigger Conditions', and 'Trigger Actions'. In the 'Settings' section, there are fields for 'Title' (Web server errors) and 'Description' (Alerts when http status 50\* events are returned). Below these is a 'Permissions' section with two radio buttons: 'Private' (selected) and 'Shared in App'. Below the permissions is an 'Alert type' section with two radio buttons: 'Scheduled' (selected) and 'Real-time'. In the 'Trigger Conditions' section, there is a 'Trigger alert when' dropdown set to 'Per-Result', and a 'Throttle' checkbox which is unchecked. In the 'Trigger Actions' section, there is a '+ Add Actions' button. At the bottom right of the dialog are 'Cancel' and 'Save' buttons.

Section	Field/Option	Value
Settings	Title	Web server errors
	Description	Alerts when http status 50* events are returned
	Permissions	Private (selected)
	Alert type	Scheduled (selected)
Trigger Conditions	Trigger alert when	Per-Result
	Throttle	Unchecked
Trigger Actions	+ Add Actions	Button



# Choosing Real-time or Scheduled Alert Type

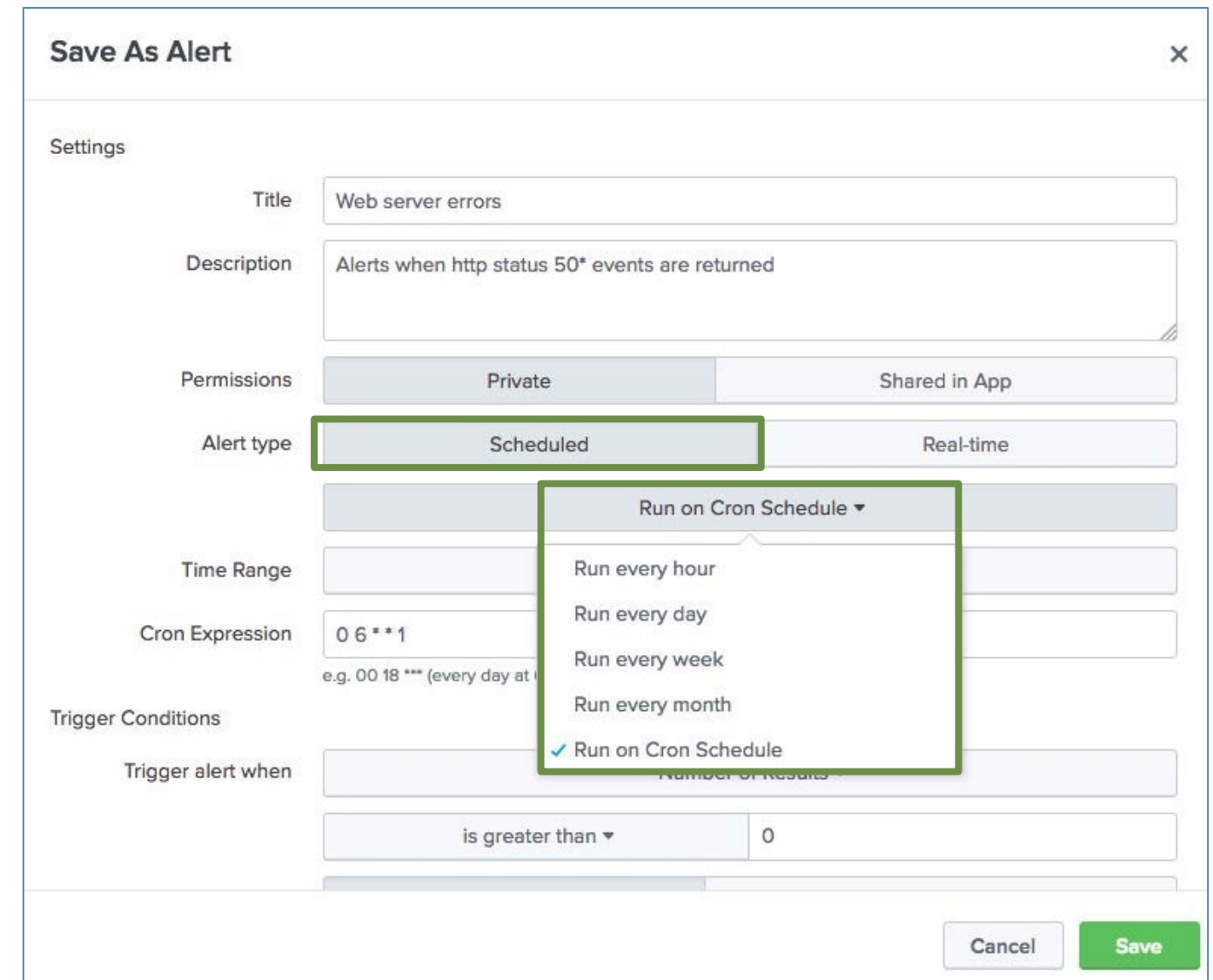
Choose an **Alert type** to determine how Splunk searches for events that match your alert

- **Scheduled** alerts
  - Search runs at a defined interval
  - Evaluates trigger condition when the search completes
- **Real-time** alerts
  - Search runs constantly in the background
  - Evaluates trigger conditions within a window of time based on the conditions you define

The screenshot shows the 'Save As Alert' dialog box in Splunk. The 'Settings' section includes fields for 'Title' (Web server errors) and 'Description' (Alerts when http status 50\* events are returned). The 'Permissions' section shows 'Private' and 'Shared in App' options. The 'Alert type' section, highlighted with a green border, shows 'Scheduled' and 'Real-time' options, with 'Scheduled' currently selected. The 'Trigger Conditions' section includes a 'Trigger alert when' dropdown set to 'Per-Result' and a 'Throttle' checkbox. The 'Trigger Actions' section has a '+ Add Actions' button. At the bottom right are 'Cancel' and 'Save' buttons.

# Setting the Alert Type – Scheduled

- From the frequency menu, choose to run the search every hour, day, week, month, or on a cron schedule
  - For the scheduled interval options, select the time the search will run
  - For cron schedule, define the cron expression



The screenshot shows the 'Save As Alert' dialog box with the following fields and options:

- Title:** Web server errors
- Description:** Alerts when http status 50\* events are returned
- Permissions:** Private (selected) / Shared in App
- Alert type:** Scheduled (selected) / Real-time
- Time Range:** (empty)
- Cron Expression:** 0 6 \* \* 1  
e.g. 00 18 \*\*\* (every day at 18:00)
- Trigger Conditions:**
  - Trigger alert when: (empty)
  - is greater than ▾ 0

The 'Alert type' dropdown menu is open, showing the following options:

- Run on Cron Schedule ▾ (selected)
- Run every hour
- Run every day
- Run every week
- Run every month
- Run on Cron Schedule (checked)

Buttons: Cancel, Save

# Setting Trigger Conditions – Scheduled

- For the cron schedule, choose a Time Range and enter a Cron Expression
- Set trigger conditions for scheduled alerts (same steps outlined for real-time alerts)
  - The alert examines the complete results set after the search is run

## Scenario

In this example, a scheduled search will run every 5 minutes.

The screenshot shows the 'Save As Alert' dialog box with the following settings:

- Title:** Web server errors
- Description:** Alerts when http status 50\* events are returned
- Permissions:** Private
- Alert type:** Scheduled
- Run on Cron Schedule:** (Selected)
- Time Range:** Last 5 minutes
- Cron Expression:** 0 6 \* \* 1  
e.g. 00 18 \*\*\* (every day at 6PM). Learn More
- Trigger Conditions:**
  - Trigger alert when:** Number of Results
  - is greater than:** 2

Buttons: Cancel, Save

# Setting Trigger Conditions – Real-time

- Trigger conditions allow you to capture a larger data set, then apply more stringent criteria to results before executing the alert
- You can set alerts to trigger:
  - **Per-Result** – triggers when a result is returned
  - **Number of Results** – define how many results are returned before the alert triggers
  - **Number of Hosts** – define how many unique hosts are returned before the alert triggers
  - **Number of Sources** – define how many unique sources are returned before the alert triggers
  - **Custom** – define custom conditions using the search language

**Save As Alert** [X]

**Settings**

Title: Web server errors

Description: Alerts when http status 50\* events are returned

Permissions: Private | Shared in App

Alert type: Scheduled | **Real-time**

**Trigger Conditions**

Trigger alert when: Per-Result ▼

- ☒ **Per-Result**  
Triggers whenever search returns a result.
- Number of Results**  
Triggers based on a number of search results during a rolling-window of time.
- Number of Hosts**  
Triggers based on a number of hosts during a rolling-window of time.
- Number of Sources**  
Triggers based on a number of sources during a rolling-window of time.
- Custom**  
Triggers based on a custom condition during a rolling-window time.

Cancel Save

# Setting Trigger Conditions – Real-time (cont.)

- In this example, the trigger condition is set to Number of Results
- In this Real-time alert example, if the number of results is greater than 2 within 1 minute, the alert triggers

## Note

The Number of Results setting does **not** determine how many actions associated with the alert are triggered. Rather, it sets a threshold to determine whether the alert is triggered in the first place.

The screenshot shows the 'Save As Alert' dialog box with the following configuration:

- Title:** Web server errors
- Description:** Alerts when http status 50\* events are returned
- Permissions:** Private (selected), Shared in App
- Alert type:** Scheduled, Real-time (selected)
- Trigger Conditions:**
  - Trigger alert when: Number of Results
  - is greater than: 2
  - in: 1 minute(s)
  - Trigger: Once (selected), For each result
- Throttle:** ☐
- Trigger Actions:** (empty)
- Buttons:** Cancel, Save

# Alert Actions – Trigger Conditions: Once

- **Once** executes actions *one time* for all matching events within the scheduled time and conditions
  - Example: If your alert is scheduled to run every **5 minutes**, and 40 results are returned, the alert only triggers and executes actions one time
- Select the Throttle option to suppress the actions for results within a specified time range

The screenshot shows the 'Save As Alert' configuration window. The 'Alert type' is set to 'Scheduled'. The 'Run on Cron Schedule' dropdown is selected. The 'Time Range' is set to 'Last 5 minutes'. The 'Cron Expression' is '0 6 \* \* 1' with a hint 'e.g. 00 18 \* \* \* (every day at 6PM). Learn More'. Under 'Trigger Conditions', 'Trigger alert when' is set to 'Number of Results', which is 'is greater than' '2'. The 'Trigger' is set to 'Once', which is highlighted with a green box. Below this, the 'Throttle' checkbox is checked, and the 'Suppress triggering for' is set to '10' 'minute(s)', also highlighted with a green box. The 'Trigger Actions' section has a '+ Add Actions' button. At the bottom right are 'Cancel' and 'Save' buttons.



# Alert Actions – Trigger Conditions: For Each Result

- **For each result** – executes the alert actions once *for each result* that matches the conditions
- Select the Throttle option to suppress the actions for results that have the same field value within a specified time range
  - Certain situations can cause a flood of alerts, when really you only want one
- In this example:
  - The search runs every 5 minutes
  - 70 events are returned in a 5 minute window—50 events with status=**500**, 20 with status=**503**
  - Since *For each result* is selected, **two actions** trigger—one for each status

**Save As Alert** [X]

Alert type: **Scheduled** | Real-time

Run on Cron Schedule ▾

Time Range: Last 5 minutes ▶

Cron Expression: 0 6 \* \* 1  
e.g. 00 18 \*\*\* (every day at 6PM). [Learn More](#)

Trigger Conditions

Trigger alert when: Number of Results ▾

is greater than ▾ | 2

Trigger: Once | **For each result**

Throttle ? ☒

Suppress results containing field value: status

Suppress triggering for: 10 | minute(s) ▾

# Add Trigger Actions

- Add to Triggered Alerts – adds the alert to the Activity > Triggered alerts list
- All actions available for scheduled reports are also available for alerts:
  - Log Event
  - Output results to lookup
  - Output results to telemetry endpoint
  - Run a script
  - Send email
  - Webhook

The screenshot shows the 'Save As Alert' dialog box in Splunk. The dialog has a title bar with a close button (X). Below the title bar, there are several sections: 'Time Range' with a dropdown set to 'Last 5 minutes', 'Cron Expression' with a text input '0 6 \* \* 1' and a hint 'e.g. 00 18 \*\*\* (every day at 6PM). Learn More', and 'Trigger Conditions'. The 'Trigger Conditions' section includes a dropdown for 'Trigger alert when' and a 'Number of Results' dropdown set to '2'. Below these, there is a 'For each result' button. A modal window is open over the 'Trigger Conditions' section, listing five actions: 'Add to Triggered Alerts' (with a bell icon), 'Log Event' (with a document icon), 'Output results to lookup' (with a magnifying glass icon), 'Output results to telemetry endpoint' (with a pulse icon), and 'Run a script' (with a code icon). The 'Add to Triggered Alerts' action is highlighted with a green border. At the bottom of the modal is a '+ Add Actions' button. The main dialog has 'Cancel' and 'Save' buttons at the bottom right.



# Alert Actions – Add to Triggered Alerts

Choose an appropriate severity for the alert

Save As Alert

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

Trigger Conditions

Trigger alert when

Number of Results

is greater than

2

Trigger

Once

For each result

Throttle ?

☒

Suppress results containing field value

status

Suppress triggering for

10

minute(s)

Trigger Actions

+ Add Actions

When triggered

Add to Triggered Alerts

Remove

Severity

Medium

Info

Low

☒ Medium

High

Critical

Cancel

Save

App

CLASS: Fundamentals 1 (class\_F...

Owner

student...

Severity

All

Alert

All

<prev

next>



Showing 1-12 of 12 results

Time	Fired alerts	App	Type	Severity	Mode	Actions
<input type="checkbox"/> 2018-01-11 00:26:29 UTC	Web server errors	class_Fund1	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
<input type="checkbox"/> 2018-01-11 00:26:28 UTC	Web server errors	class_Fund1	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
<input type="checkbox"/> 2018-01-11 00:26:24 UTC	Web server errors	class_Fund1	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
<input type="checkbox"/> 2018-01-11 00:26:23 UTC	Web server errors	class_Fund1	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
<input type="checkbox"/> 2018-01-11 00:26:19 UTC	Web server errors	class_Fund1	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>

# Alert Actions – Log Event

If you have administrator privileges, you can use a log event action

- Event – Enter the information that will be written to the new log event
- Source – Source of the new log event (by default, the alert name)
- Sourcetype – Sourcetype to which the new log event will be written
- Host – Host field value of the new log event (by default, IP address of the host of the alert)
- Index – Destination index for the new log event (default value is main)

When triggered   Log Event

Event

Specify event text for the logged event.  
[Learn More](#)

Source

Value of the source field.

Sourcetype

Value of the sourcetype field.

Host

Value of the host field.

Index

Indicate a destination index for the logged event. Ensure that destination matches an existing index.

## Note

For a complete list of available tokens, go to:  
<http://docs.splunk.com/Documentation/Splunk/latest/Alert/EmailNotificationTokens>

# Alert Actions – Log Event (cont.)

When triggered

Log Event

Event

\$trigger\_date\$ \$trigger\_timeHMS\$ 50\*  
web server errors  
sourcetype=\$result.sourcetype\$

Specify event text for the logged event.  
[Learn More](#)

Source

alert:\$name\$

Value of the source field.

Sourcetype

generic\_single\_line

Value of the sourcetype field.

Host

Value of the host field.

Index

main

Indicate a destination index for the logged event. Ensure that destination matches an existing index.

## New Search

Index=main

✓ 7 events (1/11/18 11:05:00.000 AM to 1/11/18 12:05:41.000 PM) No Event Sampling

Events (7) Patterns Statistics Visualization

Format Timeline – Zoom Out + Zoom to Selection × Deselect

1 minute per c

List Format 20 Per Page

	i	Time	Event
SELECTED FIELDS			
a host 1			
a source 1			
a sourcetype 1			
INTERESTING FIELDS			
# date_hour 2			
# date_mday 1			

2018-01-11 12:00:20 50\* web server errors sourcetype=access\_combined  
host = 127.0.0.1 source = alert:Web server errors sourcetype = generic\_single\_line

2018-01-11 11:59:29 50\* web server errors sourcetype=access\_combined  
host = 127.0.0.1 source = alert:Web server errors sourcetype = generic\_single\_line

2018-01-11 11:56:39 50\* web server errors sourcetype=access\_combined  
host = 127.0.0.1 source = alert:Web server errors sourcetype = generic\_single\_line

# Alert Actions – Send Email

Customize the content of email alerts

- To - enter the email address(es) of the alert recipients
- Priority – select the priority
- Subject – edit the subject of the email (the \$name\$ token is the title of the alert)
- Message – provide the message body of the email
- Include – select the format of the alert
- Type – select the format of the text message

The screenshot shows the 'Save As Alert' dialog box with the 'Send email' action selected. The configuration fields are as follows:

- When triggered:** Send email (with a 'Remove' link)
- To:** (Empty text box) Comma separated list of email addresses. [Show CC and BCC](#)
- Priority:** Normal (dropdown menu)
- Subject:** Splunk Alert: \$name\$
- Message:** The alert condition for '\$name\$' was triggered. The email subject, recipients and message can include tokens that insert text based on the results of the search. [Learn More](#)
- Include:**
  - ☒ Link to Alert
  - ☒ Link to Results
  - ☐ Search String
  - ☐ Inline [Table](#)
  - ☐ Trigger Condition
  - ☐ Attach CSV
  - ☐ Trigger Time
  - ☐ Attach PDF
- Type:** HTML & Plain Text (selected) | Plain Text

Buttons: Cancel, Save



# Viewing Triggered Alerts

- If you elected to list in triggered alerts, you can view the results by accessing **Activity > Triggered Alerts**
- Click **View results** to see the matching events that triggered the alert
- Click **Edit search** to modify the alert definition

The screenshot shows the Splunk Enterprise interface. The top navigation bar includes 'splunk>enterprise', 'Apps', 'student1', 'Messages', 'Settings', 'Activity', and 'Help'. Below the navigation bar is a search bar with 'Find' and a magnifying glass icon. The main content area shows a table of triggered alerts. The table has columns: Time, Fired alerts, App, Type, Severity, Mode, and Actions. Three alerts are listed, all for 'Web server errors' in the 'class\_Fund1' app, triggered at 00:26:29, 00:26:28, and 00:26:24 UTC. Each alert row has links for 'View results', 'Edit search', and 'Delete'. A green box highlights the 'Triggered Alerts' link in the 'Alert' dropdown menu.

Time	Fired alerts	App	Type	Severity	Mode	Actions
2018-01-11 00:26:29 UTC	Web server errors	class_Fund1	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2018-01-11 00:26:28 UTC	Web server errors	class_Fund1	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2018-01-11 00:26:24 UTC	Web server errors	class_Fund1	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>

# Editing Alerts

1. From the search bar, click **Alerts**
2. Select the alert and click **Edit**

The screenshot shows the top navigation bar with the following items: Search, Datasets, Reports, Alerts (highlighted), Dashboards, Presentation, Lab Solutions, and Instructor. On the right of the navigation bar is the CLASS: Fundamentals 1 logo.

The main content area is titled "Alerts" and includes a description: "Alerts set a condition that triggers an action, such as sending an email that contains the results of the triggering search to a list of people. Click the name to view the alert. Open the alert in Search to refine the parameters."

Below the description, it says "1 Alerts". There are filter buttons: "All", "Yours", and "This App's". A search bar with the placeholder "filter" and a magnifying glass icon is also present.

The table below lists the alerts:

i	Title ^	Actions	Owner ↕	App ↕	Sharing ↕	Status ↕
>	Web server errors	Open in Search	student1	class_Fund1	Private	Enabled

A green arrow points from the "Alerts" tab in the navigation bar to the "Edit" button in the "Actions" column of the table. The "Edit" button is highlighted with a green box, and a dropdown menu is open below it, showing the following options: "Edit Alert", "Edit Permissions", "Disable", "Clone", and "Delete".

# Editing Alert Permissions

- Edit permissions
  - Owner – only you can access, edit, and view triggered alerts
  - App – users of the app can access, edit, and view triggered alerts

The screenshot illustrates the process of editing alert permissions. On the left, the 'Alerts' section shows a table with one alert: 'Web server errors'. The 'Edit' button in the 'Actions' column is clicked, opening a dropdown menu. The 'Edit Permissions' option is highlighted, and a green arrow points to the 'Edit Permissions' modal on the right.

**Alerts**

Alerts set a condition that triggers an action, such as sending an email that contains the results of the triggering search to a list of people. Click the name to view the alert. Open the alert in Search to refine the parameters.

1 Alerts

All Yours This App's filter

i	Title ^	Actions	Owner ↕	App ↕	Sharing ↕	Share
>	Web server errors	Open in Search Edit	student1	class_Fund1	Private	Share

**Edit Permissions**

Alert Web server errors

Owner student1

App class\_Fund1

Display For ☒ Owner ☐ App ☐ All apps

Cancel Save

# Other Resources

- Splunk App Repository  
<https://splunkbase.splunk.com/>
- Splunk Answers  
<http://answers.splunk.com/>
- Splunk Blogs  
<http://blogs.splunk.com/>
- Splunk Wiki  
<http://wiki.splunk.com/>
- Splunk Docs  
<http://docs.splunk.com/Documentation/Splunk>
- Splunk User Groups  
<http://usergroups.splunk.com/>