Splunk® Enterprise Alerting Manual 9.0.4

Use tokens in email notifications

Generated: 2/15/2023 3:12 am

Use tokens in email notifications

Tokens represent data that a search generates. They work as placeholders or variables for data values that populate when the search completes.

You can use tokens in the following fields of an email notification.

- To
- Cc
- Bcc
- Subject
- Message
- Footer

If you have Splunk Enterprise, you can change footer text by editing `alert_actions.conf`.

Use this token syntax to reference values from the search: `$<token>$`

For example, place the following text and token in the subject field of an email notification to reference the search ID of a search job:

```
Search results from $job.sid$
```

Tokens available for email notification

There are four categories of tokens that access data generated by searches. Token availability varies by context.

Category	Context: Alert Actions	Context: Scheduled Reports	Context: Scheduled PDF delivery
Search metadata	Yes	Yes	Yes
Search results	Yes	Yes	No
Job information	Yes	Yes	No
Server information	Yes	Yes	Yes
Dashboard information	No	No	Yes

If you have Splunk Enterprise, you can use tokens to access values for attributes listed in `savedsearches.conf` and `alert_actions.conf`. Use the attribute name with standard token syntax. For example, to access an email notification subject, use `$action.email.subject$`.

Search metadata tokens

Common tokens that access information about a search.

Token	Description
$action.email.hostname$	Email server hostname
$action.email.priority$	Search priority
$alert.expires$	Alert expiration time

Token	Description
$alert.severity$	Alert severity level
app	App context for the search
$cron_schedule$	Search cron schedule
$description$	Human-readable search description
$name$	Search name
$next_scheduled_time$	The next time the search runs
$owner$	Search owner
$results_link$	(Alert actions and scheduled reports only) Link to search results
$search$	Search string
$trigger_date$	(Alert actions only) Date when alert triggered, formatted as `Month(string) Day, Year`
$trigger_time$	(Alert actions only) Time when alert triggered, formatted as epoch time
$type$	Indicates if the search is from an alert, report, view, or the search command
$view_link$	Link to view saved search

Result tokens

You can access field values from the first result row that a search returns. Field availability for tokens depends on what fields are available in search results.

Token	Description
$result.*fieldname*$	First value for the specified field name from the first search result row. Verify that the search generates the field being accessed.

To include or exclude specific fields from the results, use the `fields` command in the base search for the alert. For more information, see fields in the *Search Reference*.

Job information tokens

Common tokens that access data specific to a search job, such as the search ID or messages generated by the search job.

Token	Description
$job.earliestTime$	Initial job start time
$job.eventSearch$	Subset of the search that appears before any transforming commands
$job.latestTime$	Latest time recorded for the search job
$job.messages$	List of error and debug messages generated by the search job
$job.resultCount$	Search job result count
$job.runDuration$	Time, in seconds, for search job completion
$job.sid$	Search ID
$job.label$	Search job name

Server tokens

Provide details about your Splunk deployment.

Token	Description
$server.build$	Build number of the Splunk deployment.
$server.serverName$	Server name hosting the Splunk deployment.
$server.version$	Version number of the Splunk deployment.

Dashboard metadata tokens

Access dashboard metadata and include it in dashboard delivery emails.

Token	Description
$dashboard.label$	Dashboard label
$dashboard.title$	Equivalent to `$dashboard.label$`
$dashboard.description$	Dashboard description
$dashboard.id$	Dashboard ID

Deprecated email notification tokens

The following tokens are deprecated.

Token	Alternative option
$results.count$	(Deprecated) Use $job.resultCount$.
$results.file$	(Deprecated) No equivalent available.
$results.url$	(Deprecated) Use $results_link$.
$search_id$	(Deprecated) Use $job.sid$.