**About event types**

[**Event types**](https://docs.splunk.com/Splexicon:Eventtype) are a categorization system to help you make sense of your data. Event types let you sift through huge amounts of data, find similar patterns, and create alerts and reports.

**Note:** Using event types as a short cut for search is not recommended. If you want to shorten a portion of a search, it is much better to use a [**search macro**](https://docs.splunk.com/Splexicon:Searchmacro). Search macros are more flexible in what they can express, can include other search commands and not just base query terms, can be parameterized, and do not incur costs when events are retrieved. This can sometimes be easier to manage, because, for example, a single search macro can take the place of multiple event types.

For more information about using search macros, see [using search macros in searches](http://docs.splunk.com/Documentation/Splunk/9.3.1/Knowledge/Usesearchmacros).

**Event types and the search-time operations sequence**

When you run a search, Splunk software runs several operations to derive knowledge objects and apply them to events returned by the search. Splunk software performs these operations in a specific sequence.

**Search-time operations order**

Event types come eighth in the search-time operations order, before tags but after lookups.

**Restrictions**

Splunk software processes event types first by priority score and then by ASCII sort order. Search strings that define event types cannot reference tags, because event types are always processed and added to events before tags.

**For more information**

For more information about search-time operations, see [search-time operations sequence](http://docs.splunk.com/Documentation/Splunk/9.3.1/Knowledge/Searchtimeoperationssequence).

**How event types work**

Every [**event**](https://docs.splunk.com/Splexicon:Event) that can be returned by that search gets an association with that event type. For example, say you have this search:

sourcetype=access\_combined status=200 action=purchase

If you save that search as an event type named successful\_purchase, any event that can be returned by that search gets eventtype=successful\_purchase added to it at search time. This happens even if you are searching for something completely different.

**Note:** Using event types can consume a lot of data, because any search attempts to correlate events with any known event type. As more event types are defined, the cost in search performance goes up. You can examine the execution costs of search commands with the command.search.typer parameter. See [search job inspector](http://docs.splunk.com/Documentation/Splunk/9.3.1/Search/ViewsearchjobpropertieswiththeJobInspector).

To build a search that works with events that match that event type, include eventtype=successful\_purchase as a search term.

A single event can match multiple event types. When an event matches two or more event types, eventtype acts as a multi-value field.

**Important event type definition restrictions**

You cannot base an event type on a search that:

* Includes a [**pipe operator**](https://docs.splunk.com/Splexicon:Pipeoperator) after a simple search.
* Includes a **[subsearch](https://docs.splunk.com/Splexicon:Subsearch" \o "Splexicon:Subsearch" \t "_blank)**.
* Is defined by a simple search that uses the [savedsearch](http://docs.splunk.com/Documentation/Splunk/9.3.1/SearchReference/Savedsearch) command to reference a report name. For example, if you have a report named failed\_login\_search, you should not use this search to define the event type: | savedsearch failed\_login\_search. In this case you should instead use the search string that defines failed\_login\_search as the definition of the event type.

This last point is more of a best practice than a strict limitation. You want to avoid situations where the search string underneath failed\_login\_search is modified by another user at a future date, possibly in a way that breaks the event type. You have more control over the ongoing validity of the event type if you use actual search strings in its definition.

**Note:** If you want to use event types as a way to short cut your search, use a [**search macro**](https://docs.splunk.com/Splexicon:Searchmacro). For more information on event types vs search macros, see [About event types](http://docs.splunk.com/Documentation/Splunk/9.3.1/Knowledge/Abouteventtypes).

**Creating event types**

The simplest way to create a new event type is through Splunk Web. After you run a search that would make a good event type, click **Save As** and select *Event Type*. This opens the **Save as Event Type** dialog, where you can provide the event type name and optionally apply tags to it. For more information about saving searches as event types, see [Define and maintain event types in Splunk Web](http://docs.splunk.com/Documentation/Splunk/9.3.1/Knowledge/Defineeventtypes#Save_a_search_as_a_new_event_type).

You can also create new event types by modifying eventtypes.conf. For more information about manually configuring event types in this manner, see [Configure event types directly in eventtypes.conf](http://docs.splunk.com/Documentation/Splunk/9.3.1/Knowledge/Configureeventtypes).

**Event type tags**

Event types can have one or more tags associated with them. You can add these tags while you save a search as an event type and from the event type manager, located in **Settings > Event types**. From the list of event types in this window, select the one you want to edit.

Tag event types to organize your data into categories. There can be multiple tags per event. You can tag an event type in Splunk Web or configure it in tags.conf. For more information about event type tagging, see [Tag event types](http://docs.splunk.com/Documentation/Splunk/9.3.1/Knowledge/Tageventtypes).

**Event type tags example #1**

Use event type tags to help track abstract field values such as HTTP access logs, IP addresses, or ID numbers by giving them more descriptive names. Add tags to event types by going to **Settings > Event types**. Select the event type from the list of event types in this menu.

After you add tags to your event types, search for them in the same way you search for any tag.

Let's say that we have saved a search for page not found as the event type status=404 and then saved a search for failed authentication as the event type status=403. If you tagged both of these event types with **HTTP client error**, all events of either of those event types can be retrieved by using the search:

tag::eventtype=HTTP client error

For more information about using tags, see [Tag field value pairs in Search](http://docs.splunk.com/Documentation/Splunk/9.3.1/Knowledge/TagandaliasfieldvaluesinSplunkWeb).

**Event type tags example #2**

Event type tags are commonly used in the Common Information Model (CIM) add-on for the Splunk platform in order to normalize newly indexed data from an unfamiliar source type. We can use tags to identify different event types within a single data source.

You can apply CIM-compliant tags to your data.

1. From Splunk Web, select **Settings > Data Models**. Find the data model dataset that you want to map your data to, then identify its associated tags. For example, the cpu\_load\_percent object in the Performance data model has the following tags associated with it:

tag = performance

tag = cpu

1. Create the appropriate event types in the Events type manager in Splunk Web by going to **Settings > Event types**. You can also edit the eventtypes.conf file directly.
2. Create the appropriate tags in Splunk Web. Select **Settings > Event types**, locate the event type that you want to tag and click on its name. You can also edit the tags.conf file directly.