

Splunk® Enterprise Search Tutorial 7.3.1

Specifying time ranges

Generated: 8/06/2019 11:32 am

Specifying time ranges

Restricting, or filtering, your search criteria using a time range is the easiest and most effective way to optimize your searches.

You can use time ranges to troubleshoot an issue, if you know the approximate timeframe when the issue occurred. Narrow the time range of your search to that timeframe. For example, to investigate an incident that occurred sometime in the last hour, you can use the default time range **Last 24 hours**, but a better option is **Last 60 minutes**.

Let's explore the data from the Buttercup Games online store using the different time ranges.

1. To start a new search, click **Search** in the Apps bar.
2. To search for a keyword in your events, type **buttercupgames** in the Search bar and press **Enter**.

buttercupgames

The keyword is highlighted in the events that are returned.

The screenshot shows the 'Search & Reporting' interface. At the top, there's a navigation bar with 'Search', 'Metrics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The 'Search' tab is active. Below the navigation bar, there's a 'New Search' section with a search bar containing 'buttercupgames' and a 'Last 24 hours' time range selector. A green search button is to the right. Below the search bar, it shows '1,986 events (4/16/19 9:00:00.000 AM to 4/17/19 9:29:50.000 AM)' and 'No Event Sampling'. There are tabs for 'Events (1,986)', 'Patterns', 'Statistics', and 'Visualization'. The 'Events' tab is selected. Below the tabs, there's a 'Format Timeline' dropdown, a 'Zoom Out' button, a 'Zoom to Selection' button, and a 'Deselect' button. A timeline visualization shows a series of green bars representing events. Below the timeline, there's a 'List' view button, a 'Format' button, and a '20 Per Page' dropdown. The main content area shows a table of events. The first event is highlighted with a red circle around the URL 'http://www.buttercupgames.com/oldlink?itemId=EST-14'. The second event is also highlighted with a red circle around the URL 'http://www.buttercupgames.com/oldlink?itemId=EST-15'. The third event is highlighted with a red circle around the URL 'http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01'. The table has columns for 'Time' and 'Event'. On the left side of the table, there's a sidebar with 'SELECTED FIELDS' and 'INTERESTING FIELDS'. The 'SELECTED FIELDS' section includes 'a host 3', 'a source 3', and 'a sourcetype 1'. The 'INTERESTING FIELDS' section includes 'a action 5', '# bytes 100+', 'a categoryid 8', 'a clientip 100+', '# date_hour 10', '# date_minute 59', 'a date_month 1', 'a date_second 60', and 'a date_wday 1'.

i	Time	Event
>	4/16/19 6:22:16.000 PM	91.205.189.15 - - [16/Apr/2019:18:22:16] "GET /oldlink?itemId=EST-14&JSESSIONID=SD6SL7FF7ADF53113 HTTP 1.1" 200 1665 "http://www.buttercupgames.com/oldlink?itemId=EST-14" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 159 host = www2 : source = tutorialdata.zip:/www2/access.log : sourcetype = access_combined_wcookie
>	4/16/19 6:20:56.000 PM	182.236.164.11 - - [16/Apr/2019:18:20:56] "GET /cart.do?action=addtocart&itemId=EST-15&productId=9 S-AG-089&JSESSIONID=SD6SL8FF18ADFF53101 HTTP 1.1" 200 2252 "http://www.buttercupgames.com/oldlink?itemId=EST-15" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 586 host = www1 : source = tutorialdata.zip:/www1/access.log : sourcetype = access_combined_wcookie
>	4/16/19 6:20:55.000 PM	182.236.164.11 - - [16/Apr/2019:18:20:55] "POST /oldlink?itemId=EST-18&JSESSIONID=SD6SL8FF18ADFF53 101 HTTP 1.1" 408 893 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01" "Mozilla /5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 134 host = www1 : source = tutorialdata.zip:/www1/access.log : sourcetype = access_combined_wcookie

Notice that hundreds of events are returned.

You use the time range picker, which is to the right of the Search bar, to set time boundaries on your searches. The default time range is **Last 24 hours**. You can restrict the search to one of the preset time ranges, or use a custom time range.

Time ranges and the tutorial data

When you run a search using the tutorial data, if no events are returned, it is probably because you downloaded the `tutorialdata.zip` file more than one day ago. When you download the ZIP file, timestamps are generated at that moment in time and are added to the data.

The tutorial data for the Buttercup Games store contains events for a seven day period. The dates of the events are based on the date that you downloaded the tutorial data file. For example, if you download the file today, the dates for the events begin the previous week. If today is a Wednesday, the events have a timestamp starting the previous Wednesday. The last events are from yesterday. There are no events from today. Searching for events using **Today** or any time less than the last 24 hours will return no events.

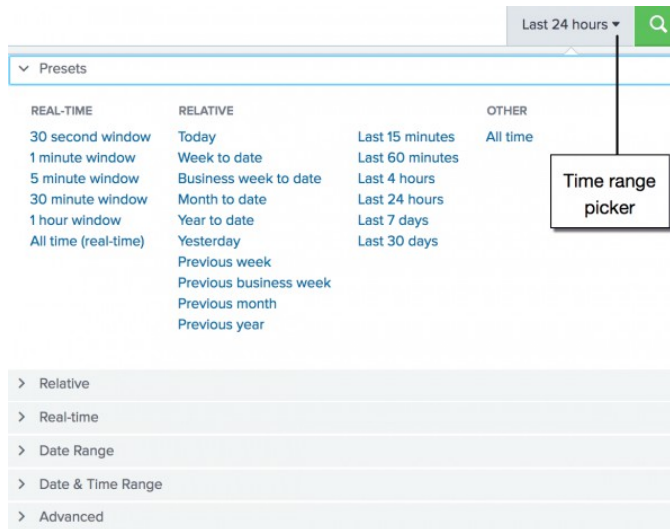
For all of your searches that use the tutorial data files, you need to adjust the search time range based on when you downloaded the tutorial data files. If you downloaded the tutorial data file 3 days ago, there are no events from the last 3 days. Try a different Relative time range, such as **Previous week** or **Last 7 days**.

Preset time ranges

The time range picker has many preset time ranges that you can select from.

1. Click the time range picker to see a list of the time range options.
 - The **Presets** option contains **Real-time**, **Relative**, and **Other** time ranges.
 - ◆ **Real-time searches** display a live, streaming view of events. You can specify a window over which to retrieve events.
 - ◆ **Historical searches** display events from the past. You can restrict your search by specifying a relative time range or a specific date and time range.

Because the data for the Buttercup Games online store is a snapshot of historical data, you will not use the "Real-time" preset time ranges in this tutorial.



2. In the Presets option in the **Relative** list, click **Yesterday**.

The number of events returned should be larger. You changed the time range from **Last 24 hours** to **Yesterday**.

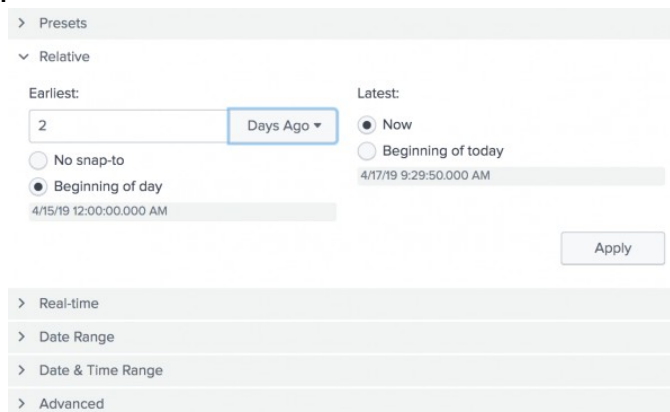
Custom time ranges

Use a custom time range when one of the preset time ranges is not precise enough for your search.

Specify relative time ranges

You can use the **Relative** option to specify a custom time range.

1. Open the time range picker.
2. To run a search over the last two days, select the **Relative** time range option.



3. For **Earliest**, type 2 in the field, and select **Days Ago** from the drop-down list.
4. For **Latest**, the default is **Now**. Select **Beginning of today**.
5. Click **Apply**.

The timestamps that appear below the radio buttons adjust based on your selections in the Relative list of time ranges.

As mentioned before, if no events are returned, select a different time range, such **4 Days Ago** or **1 Week Ago**.

Specify date and time ranges

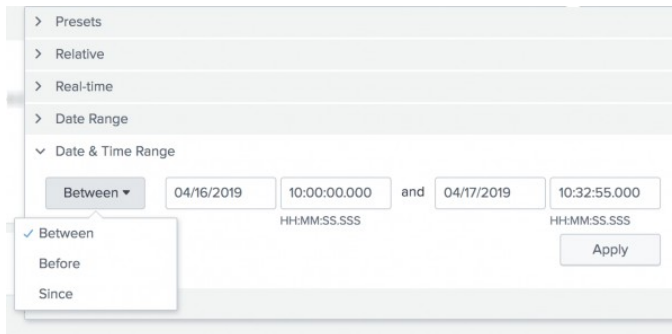
You can also use the **Date Range** and **Date & Time Range** options to specify a custom time range.

- Use **Between** to specify that events must occur between an earliest and latest date.
- Use **Before** to specify that events must occur before a date.
- Use **Since** to specify that events must occur after a date.

You use the **Date Range** option to specify dates. The following screen image shows the calendar that you can use to select a date.

The screenshot shows a user interface for selecting a date range. On the left, a sidebar contains a list of options: Presets, Relative, Real-time, Date Range (selected), Date & Time Range, and Advanced. The main area displays the 'Date Range' configuration. It includes a dropdown menu set to 'Between', two input fields for dates (04/16/2019 and 04/17/2019), and a time field set to 24:00:00. An 'Apply' button is located to the right of the time field. A calendar for April 2019 is open, showing the days of the week (Su, Mo, Tu, We, Th, Fr, Sa) and the dates. The date 16 is highlighted in blue.

You use the **Date & Time Range** option when you want to specify both a date and a time. The following screen image shows the "Between", "Before", or "Since" options.



The screenshot shows a configuration interface for a search tool. On the left, a sidebar contains a list of options: Presets, Relative, Real-time, Date Range, and Date & Time Range. The 'Date & Time Range' option is selected and expanded. The main area displays a configuration for a date and time range. It includes a dropdown menu currently set to 'Between', with a list of options (Between, Before, Since) visible below it. To the right of the dropdown are two date and time input fields. The first field contains '04/16/2019' and '10:00:00.000', with a small 'HH:MM:SS.SSS' label below it. The second field contains '04/17/2019' and '10:32:55.000', also with a 'HH:MM:SS.SSS' label below it. An 'and' connector is placed between the two fields. An 'Apply' button is located to the right of the second field.

For example, to troubleshoot an issue that took place April 16, 2019 about 10:05 AM, you can specify the earliest time of 04/16/2019 10:03:00.000 and the latest time of 04/16/2019 10:06:59.000 to show the events immediately before and after the issue took place.

Next step

This completes Part 3 of the Search Tutorial.

You have explored the Search app views and learned how important it is to specify time ranges with your searches. Continue to Part 4: Searching the tutorial data.

See also

Change the default time range in the *Search Manual*