Help building searches

The Splunk Search Processing Language (SPL) includes commands and functions that you can use to build searches. All of the commands and functions are documented in the Search Reference.

Splunk Web has several built-in features to help you build and parse searches.

- Search assistant modes
- Syntax highlighting
- Auto-format search syntax
- Numbering search lines
- Shortcuts

This topic discusses using the search assistant. See Help reading searches for information about syntax highlighting, auto-formatting, line numbers, and shortcuts.

Use the search assistant to build searches

When you type a few letters or a term into the Search bar, the search assistant shows you terms and searches that match what you typed.

The Matching Terms are based on the terms that are indexed from your data. The Matching Searches are based on your recent searches.

The list continues to update as you type.

To add an item in the list to your search criteria you can click on an item, or use the arrow keys to highlight the item and press Enter.

Search assistant modes

The search assistant has three modes: Full, Compact, and None. The default mode is Compact.

Compact mode

The Compact mode displays a list of matching terms and searches when you type. When you type a pipe ( | ) character to indicate that you want to use a command, a list of the SPL commands appears. You can type a letter to jump to the section of the list that begins with that letter. For example, if you type the letter s, the list displays all of the commands that begin with the letter s.

When you type a command, a list appears showing Command History and Matching Searches. Initially, the Command History shows some command examples. As you use a command in your searches, the Command History displays your uses of the command instead of the examples.
Below the list are a brief description of the command and an example. The **Learn More** link opens the *Search Reference* in a new window and displays documentation about the command.

To access the **Learn More** link from your keyboard, use your arrow keys to highlight the command or attribute name. Press **Tab** to highlight the **Learn More** link and then press **Enter** to activate the link.

If you type something after the command, the search assistant shows any command arguments or history that match what you type.

The search assistant can also show you the data type that an argument requires. Type the argument in the Search bar. Include the equal ( = ) symbol, if that is part of the argument syntax. In the following example, the search assistant shows that a <string> value is required for the `countfield` argument.

**Full mode**

The Full mode displays a list of matching terms and searches when you type, along with a count of how many times a term appears in your indexed data. This count tells you how many search results will be returned if you search on that term. If a term or phrase is not in the list, the term is not in your indexed data.

The Full mode also provides suggestions in the How To Search section on ways that you can retrieve events and use the search commands.
When you type a command in the Search bar, the list of matching terms and searches is replaced with the **Command History** list.

To add an item in the Command History list to your search criteria click on an item, or use the arrow keys to highlight the item and press **Enter**.

The search assistant displays a brief description of the command and several examples. There are two links next to the command description: Help and More.

- The **Help** link opens the *Search Reference* in a new window and displays documentation about the command.
- The **More** link expands the information about the command that is displayed on the screen.
When you select the **More** link, several new sections appear. The **Details** section provides a detailed description of the command. The **Syntax** section shows the basic syntax for the command. The **Related** section lists commands that are related to the command that you typed. If the command has complex syntax, click the **More** link next to the syntax to expand the syntax.

<table>
<thead>
<tr>
<th>Command History</th>
<th>Command Args</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td>countfield=</td>
</tr>
</tbody>
</table>

If you type something after the command, the search assistant shows any command arguments or history that match what you type.

<table>
<thead>
<tr>
<th>Command History</th>
<th>Command Args</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td></td>
</tr>
</tbody>
</table>

The search assistant can show you the data type that an argument requires. Type the argument in the Search bar. Include the equal ( = ) symbol if that is part of the argument syntax. In the following example, the search assistant shows that a `<string>` value is required for the `countfield` argument.
None mode

You can turn off the search assistant by changing the mode to None.

Change the search assistant mode

The default search assistant mode is Compact. You can change the search assistant mode or temporarily hide the search assistant while you build your search.

When you change the search assistant mode, the change affects only your user account.

Prerequisites

- If the Search bar contains a search that you have not run, run the search before you change the search assistant mode. Otherwise, the search is lost when you change modes. Running the search adds the search to the search history, where you can access it after you change the mode.
- If you have a Splunk Free license, you cannot change the search assistant mode. The User account menu, where the Preferences options resides, is not available in Splunk Free. To learn about what is and is not included in Splunk Free, see About Splunk Free in the Admin manual.

Steps

1. On the Splunk bar, select [User_account_name] > Preferences.

2. Click SPL Editor.
3. Verify that the Advanced editor is turned on.
4. For Search assistant, click on the mode that you want to use, Full, Compact, or None.
5. Click **Apply**.

Hide and display the search assistant

By default, the search assistant opens when you type something into the Search bar. You can turn off or hide the search assistant.

**Turn off the search assistant**

To turn off the search assistant, change the search assistant mode to **None**.

**Hide the search assistant**

The options for hiding the search assistant depend on the mode that you are using.

Compact mode

You cannot hide the search assistant. You can only turn off the search assistant.

Full mode

To hide the search assistant in Full mode, you turn off the **Auto Open** feature and collapse the search assistant drop-down.

1. In the search assistant window, click **Auto Open**. This removes the check mark next to **Auto Open**.
2. Click the collapse and expand button on the right side of the Search bar to hide the search assistant.

The search assistant remains hidden until you use the expand button to show the search assistant again. See **Unhide the search assistant window** in this topic.

When you uncheck **Auto Open** and click the collapse button the search assistant is hidden, even when you start a new search or close and reopen Splunk Web. The search assistant remains hidden until you unhide it.

**Unhide the search assistant**

If the search assistant is hidden, click the expand button on the right side of the Search bar and click **Auto Open**.

If these steps do not unhide the search assistant window, then either the search assistant is turned off or there is no assistance for what you have typed into the Search bar.

To turn the Search Assistant back on, you need to change the search assistant mode to **Compact** or **Full**.
Change the default search assistant mode for all users

Individual users can change the default search assistant setting for themselves. The default search assistant mode can also be changed globally, for all users.

Prerequisites

- Only users with file system access, such as system administrators, can change the default search assistant mode for all users.
- Review the steps in How to edit a configuration file in the Admin Manual.

Never change or copy the configuration files in the default directory. The files in the default directory must remain intact and in their original location. Make the changes in the local directory.

Steps

1. Open the local user-prefs.conf.spec.in file for the Search app. For example
   \$SPLUNK_HOME/etc/apps/<app_name>/local.
2. Under the [general] stanza, change the search assistant mode by selecting one of the other mode values. Choose from full, compact, or none. For example: search_assistant=full.
3. Restart the Splunk instance.