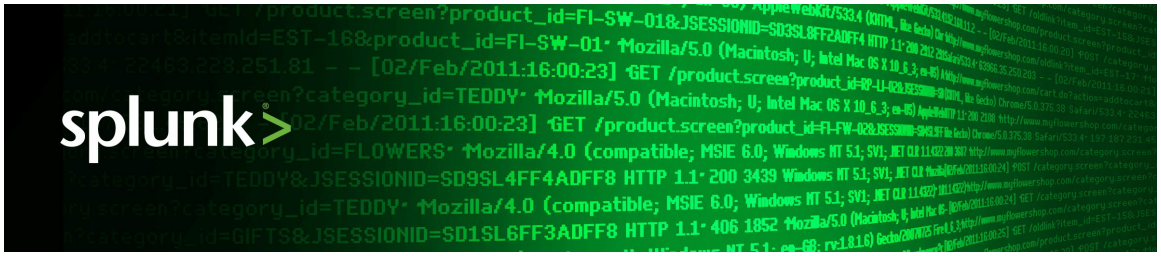

Splunk® Enterprise Search Tutorial 7.2.4

About the Search Tutorial

Generated: 11/25/2019 11:54 am

About the Search Tutorial

The Search & Reporting application (Search app) is the primary interface for using the Splunk software to run searches, save reports, and create dashboards. This Search Tutorial is for users who are new to the Splunk platform and the Search app.

Use this tutorial to learn how to use the Search app. Differences between Splunk Enterprise and Splunk Cloud are specified throughout this tutorial.

Already have access to Splunk software?

For this tutorial, use a free Trial version of the Splunk software.

Why? Because this tutorial uses a specific set of data to ensure consistency in your search results and the features that you are learning about. In the tutorial, you will upload this tutorial-specific data to the Splunk platform. You might not have permission to upload data in your production, work environment. Additionally, using a free Trial version of the software ensures that the tutorial data is not mixed in with your work data.

The Trial version of the software converts to a Free version after 30 days. If you have a Free version of the Splunk software, some of the features, such as changing Preferences in the User account menu, are not available. See About Splunk Free in the *Admin manual*.

The steps for downloading a free Trial version of Splunk Enterprise or Splunk Cloud are described in the tutorial.

What's in this tutorial?

You will learn how to use the Search app to add data to your Splunk deployment, search the data, save the searches as reports, and create dashboards. If you are new to the Search app, this tutorial is the place to start.

How to use this tutorial

Each Part in the Search Tutorial builds on the previous Part. For example, the searches that you create in Part 5 are used to create reports and charts in Part 7. It is important that you don't skip any Part.

- **Part 1: Getting started**

- **Part 2: Uploading the tutorial data**
- **Part 3: Using the Splunk Search app**
- **Part 4: Searching the tutorial data**
- **Part 5: Enriching events with lookups**
- **Part 6: Creating reports and charts**
- **Part 7: Creating dashboards**

Using the PDF version of the tutorial

You can copy and paste search strings or regular expressions directly into the Search & Reporting App from this online tutorial in your web browser.

Do not copy and paste search strings or regular expressions directly from the electronic PDF into the Search app. Pasting data from the PDF can cause errors in searches, because of hidden characters that are included in the PDF formatting.

See also sections

At the end of most of the topics in this tutorial is a section called **See also**. These sections contain links to Splunk documentation that is related to the information discussed in that topic.

Additional resources

See Additional resources at the end of this tutorial for information about:

- The Splunk community
- Links to Quick Reference information
- Links to the Splunk documentation
- How to provide feedback