

Splunk Core Certified User

Exam Description: The Splunk Core Certified User exam is the final step towards completion of the Splunk Core Certified User certification. This entry-level certification exam is a 57-minute, 65-question assessment which evaluates a candidate's knowledge and skills to search, use fields, create alerts, use lookups, and create basic statistical reports and dashboards. Candidates can expect an additional 3 minutes to review the exam agreement, for a total seat time of 60 minutes. It is recommended that candidates for this certification complete the lecture, hands-on labs, and quizzes that are part of the Splunk [Fundamentals 1](#) course in order to be prepared for the certification exam. Splunk Core Certified User is a recommended entry-level certification track for all candidates.

The following content areas are general guidelines for the content to be included on the exam:

- Introduction to Splunk's interface
- Basic searching
- Using fields in searches
- Search fundamentals
- Transforming commands
- Creating reports and dashboards
- Creating and using lookups
- Scheduled reports
- Alerts
- Using Pivot

The following content categories and objectives provide more specific guidance for the purpose of exam composition; however, other related topics may also appear on any specific delivery of the exam. In order to better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

1.0 Splunk Basics	5%
1.1 Splunk components	
1.2 Understand the uses of Splunk	
1.3 Define Splunk apps	
1.4 Customizing user settings	
1.5 Basic navigation in Splunk	

2.0 Basic Searching	22%
2.1 Run basic searches	
2.2 Set the time range of a search	
2.3 Identify the contents of search results	
2.4 Refine searches	
2.5 Use the timeline	
2.6 Work with events	
2.7 Control a search job	
2.8 Save search results	
3.0 Using Fields in Searches	20%
3.1 Understand fields	
3.2 Use fields in searches	
3.3 Use the fields sidebar	
4.0 Search Language Fundamentals	15%
4.1 Review basic search commands and general search practices	
4.2 Examine the search pipeline	
4.3 Specify indexes in searches	
4.4 Use the following commands to perform searches: tables, rename, fields, dedup, & sort	
5.0 Using Basic Transforming Commands	15%
5.1 The top command	
5.2 The rare command	
5.3 The stats command	
6.0 Creating Reports and Dashboards	12%
6.1 Save a search as a report	
6.2 Edit reports	
6.3 Create reports that display statistics (tables)	
6.4 Create reports that display visualizations (charts)	
6.5 Create a dashboard	
6.6 Add a report to a dashboard	
6.7 Edit a dashboard	

7.0 Creating and Using Lookups **6%**

- 7.1 Describe lookups
- 7.2 Examine a lookup file example
- 7.3 Create a lookup file and create a lookup definition
- 7.4 Configure an automatic lookup
- 7.5 Use the lookup in searches

8.0 Creating Scheduled Reports and Alerts **5%**

- 8.1 Describe scheduled reports
- 8.2 Configure scheduled reports
- 8.3 Describe alerts
- 8.4 Create alerts
- 8.5 View fired alerts