splunk™>

Creating Field Extractions

This three-hour course is for knowledge managers who want to learn about field extraction and the Field Extractor (FX) utility. Topics will cover when certain fields are extracted and how to use the FX to create regex and delimited field extractions.

Course Topics

- Use the Field Extractor
- Create Regex Field Extractions
- Create Delimited Field Extractions

Prerequisite Knowledge

To be successful, students should have completed the following courses:

- Search Under the Hood
- Multivalue Fields
- Creating Knowledge Objects

Course Format

Instructor-led or eLearning

Course Objectives

Topic 1 – Use the Field Extractor

- Explore the different types of extracted fields and when they are extracted
- Define the Splunk Web Field Extractor (FX)

Topic 2 – Create Regex Field Extractions

- Identify basics of regular expressions (regex)
- Explore the regex field extraction workflow
- Edit regex for field extractions

Topic 3 – Create Delimited Field Extractions

- Identify delimited field values in event data
- Explore the delimited field extraction workflow

About Splunk Education

Splunk classes are designed for specific roles such as Splunk Administrator, Developer, User, Knowledge Manager, or Architect.

Certification Tracks

Our certification tracks provide comprehensive education for Splunk customer and partner personnel according to their areas of responsibility.

To view all Splunk Education's course offerings, or to register for a course, go to http://www.splunk.com/education

To contact us, email Education_AMER@splunk.com

Splunk, Inc.

270 Brannan St. San Francisco, CA 94107

+1 866.GET.SPLUNK (1 866.438.7758)

Contact sales