SPLUNK EDUCATION

Course Description

# Creating Field Extractions

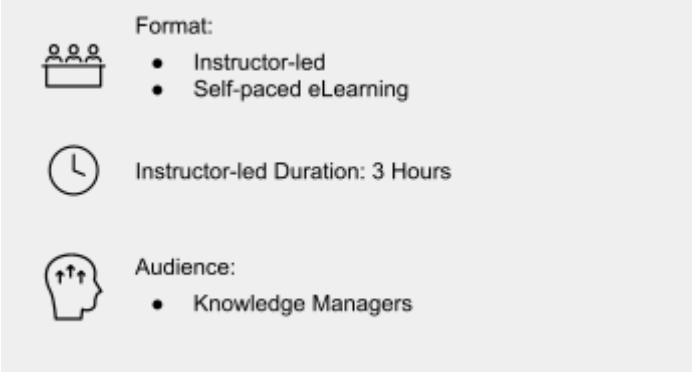
## Summary

This course is for knowledge managers who want to learn about field extraction and the Field Extractor (FX) utility.

The course will cover when certain fields are extracted and how to use the FX to create regex and delimited field extractions.

### Prerequisites

- To be successful, students must have completed these Splunk Education course(s) or have equivalent working knowledge:
  - How Splunk works
  - Knowledge objects




## Course Outline

### Module 1 – Use the Field Extractor

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

### Module 2 – Create Regex Field Extractions

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

### Module 3 – Create Delimited Field Extractions

- Identify delimited field values in event data
- Explore the delimited field extraction workflow
- Explain the use of forwarder management
- Configure forwarders to be deployment clients
- Managing forwarders using deployment apps

## About Splunk Education

With Splunk Education, you and your teams can learn to optimize Splunk through self-paced eLearning and instructor-led training, supported by hands-on labs. Explore learning paths and certifications to meet your goals. Splunk courses cover all product areas, supporting specific roles such as Splunk Platform Search Expert, Splunk Enterprise or Cloud Administrator, SOC Analyst or Administrator, DevOps or Site Reliability Engineer, and more. To learn more about our flexible learning options, full course catalog, and Splunk Certification, please visit http://www.splunk.com/education.

To contact us, email education@splunk.com.