

## SPLK-CFE: Creating Field Extractions

Course Code: SPLK-CFE

Duration: 1 day

Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

### OVERVIEW

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.

### SKILLS COVERED

- Please refer to course overview.

### WHO SHOULD ATTEND?

Search Experts Knowledge Managers.

### PREREQUISITES

To be successful, students should have a solid understanding of the following:

- How Splunk works
- Knowledge Objects

### MODULES

#### Module 1: Using the Field Extractor

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

#### Module 2: Creating Regex Field Extractions

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

#### Module 3: Creating Delimited Field Extractions

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

**END OF PAGE**