# SPLK-SESA8.2: Splunk Enterprise 8.2 System Administration

Course Code: SPLK-SESA8.2
Duration: 2 days
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

## OVERVIEW

This 2 virtual day course is designed for system administrators who are responsible for managing the Splunk Enterprise environment. The course provides the fundamental knowledge of Splunk license manager, indexers and search heads. It covers configuration, management, and monitoring core Splunk Enterprise components.

## SKILLS COVERED

- Please refer to course overview.

## WHO SHOULD ATTEND?

Everyone can attend.

## PREREQUISITES

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

- Splunk Fundamentals 1
- Splunk Fundamentals 2

OR the following single-subject courses:

- What Is Splunk?
- Intro to Splunk
- Using Fields
- Introduction to Knowledge Objects

## MODULES

### Module 1: Splunk Server Deployment

- Provide an overview of Splunk
- Identify Splunk Enterprise components
- Identify the types of Splunk deployments
- List the steps to install Splunk
- Use Splunk CLI commands

### Module 2: Splunk Server Monitoring

- Enable the Monitoring Console (MC)
- Identify Splunk license types
- Describe license violations
- Add and remove licenses
- Use Splunk Diag

### Module 3: Splunk Apps

- Describe Splunk apps and add-ons
- Install an app on a Splunk instance
- Manage app accessibility and permissions

### Module 4: Splunk Configuration Files

- Describe Splunk configuration directory structure
- Understand configuration layering process
- Use btool to examine configuration settings

### Module 5: Splunk Indexes

- Learn how Splunk indexes function
- Identify the types of index buckets
- Add and work with indexes
- Overview of metrics index

**Module 6: Splunk Index Management**

- Review Splunk Index Management basics
- Identify data retention recommendations
- Identify backup recommendations
- Move and delete index data
- Describe the use of the Fishbucket
- Restore a frozen bucket

**Module 7: Splunk User Management**

- Add Splunk users using native authentication
- Describe user roles in Splunk
- Create a custom role
- Manage users in Splunk

**Module 8: Configuring Basic Forwarding**

- Identify forwarder configuration steps
- Configure a Universal Forwarder
- Understand the Deployment Server

**Module 9: Distributed Search**

- Describe how distributed search works
- Describe the roles of the search head and search peers

**END OF PAGE**