Splunk Enterprise System Administration

Category: AI, Data & Analytics | **Vendor:** Splunk

Duration: 16.00 hours (2 days) **13.0 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Course Overview

This course is for system administrators who are responsible for managing a 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.

Please note that classes may run across two days, consisting of 6 hour sessions. This course has 12 hours of content.

About This Course

This course is for system administrators who are responsible for managing a 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.

Please note that classes may run across two days, consisting of 6 hour sessions. This course has 12 hours of content.

Who Should Attend

- Administrators

Prerequisites & Entry Requirements

General Prerequisites:

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

- Exploring Splunk Platform Ecosystem
- Splunk User track

Detailed Course Outline

Module 1 - Deploy Splunk

- Provide an overview of Splunk
- Identify Splunk Enterprise components and deployment types
- List Splunk installation prerequisites
- Use Splunk CLI commands
- Explore security recommended practices

Module 2 - Monitor Splunk

- Use Splunk Health Report
- Enable and use the Monitoring Console
- Use Splunk Diag and Rapid Diag

Module 3 - License Splunk

- Identify the different Splunk license types
- Describe license violations
- Install a Splunk License
- Configure a Splunk License Manager
- Configure License Peers
- Configure License Pools
- Manage License warnings
- Monitor license usage using the Monitoring Console and the Splunk Chargeback app

Module 4 - Use Configuration Files

- Describe Splunk configuration directory structure

- Explore the configuration layering process
- Index time process
- Search time process
- Use Splunk tools to examine configuration settings such as btoo

Module 5 - Use Apps

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

Module 6 - Create Indexes

- Describe how Splunk indexes function
- Identify the types of index buckets
- Create and work with indexes
- Describe metrics index

Module 7 - Manage Index

- 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 8 - Manage Users

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

- Manage users in Splunk

Module 9 - Configure Basic Forwarding

- Identify forwarder configuration steps
- Configure a Universal Forwarder
- Understand the agent management

Module 10 - Configure Distributed Search

- Configure distributed search
- Define the roles of the search head and search peers
- Use Monitoring Console to monitor search activity
- Explain when and how to quarantine search peers
- Identify options and considerations for using multiple search heads
- Identify distributed search recommended practices
- Explain the use cases for Federated Search and how it is configured

Frequently Asked Questions

Q: What delivery options are available for Splunk Enterprise System Administration?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: How many CPD hours does this course provide?

The 2-day Splunk Enterprise System Administration course provides up to 13.0 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Splunk Enterprise System Administration training?

The training takes place over 2 day(s), with each day lasting approximately 16.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Splunk Enterprise System Administration?

Yes, we provide corporate training, dedicated training, and closed classes for Splunk Enterprise System Administration. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: Splunk Enterprise System Administration, Splunk Enterprise Administrator, SESA

Q: Why choose Nexus Human for Splunk Enterprise System Administration?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Splunk Enterprise System Administration training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 889 8700 (Ireland) | +44 20 8142 8961 (UK)

© 2026 Nexus Human. All rights reserved. This brochure was generated on 13/11/2026.