

Splunk Enterprise Data Administration (SEDA)

ID SEDA Prix sur demande Durée 18 heures

A qui s'adresse cette formation

This module is designed for administrators who are responsible for getting data into Splunk Indexers.

Cette formation prépare à la/aux certifications

Splunk Enterprise Certified Admin (SECA)

Pré-requis

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

- Fundamentals 1 (Retired)
- Fundamentals 2 (recommended) (Retired)

Or the following single-subject modules:

- What is Splunk? (Retired)
- [Intro to Splunk \(ITS\)](#)
- [Using Fields \(SUF\)](#)
- [Intro to Knowledge Objects \(IKO\)](#)
- [Creating Knowledge Objects \(CKO\)](#)
- [Creating Field Extractions \(CFE\)](#)

Students should also understand the following module:

- !Splunk Enterprise System Administration (SESA) (recommended)

Objectifs

- Understand sourcetypes
- Manage and deploy forwarders
- Configure data inputs
- File monitors
- Network inputs (TCP/UDP)
- Scripted inputs
- HTTP inputs (via the HTTP Event Collector)
- Customize the input phase parsing process
- Define transformations to modify data before indexing
- Define search time knowledge object configurations

Splunk Enterprise Data Administration (SEDA)

Centres de formation dans le monde entier



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, <https://www.flane.ch>