FortiAnalyzer Administrator 7.4 Course

Course Duration: 8 Hrs. **Course Code: FAZ-ADM-7.4**

Course Overview

The **FortiAnalyzer Administrator 7.4** course is designed for network and security professionals who manage centralized logging, analytics, and reporting for Fortinet security devices. This course focuses on deploying, configuring, and operating FortiAnalyzer version 7.4 to gain visibility into network traffic, security events, and compliance data. Participants will learn how to analyze logs, create reports, investigate threats, and optimize security operations across enterprise environments.

What You'll Learn?

By completing this course, you will be able to:

- Understand FortiAnalyzer architecture and deployment options
- Configure log collection from FortiGate and other Fortinet devices
- Analyze traffic and security logs effectively
- Create custom reports and dashboards
- Perform incident investigation and forensics using logs
- Manage storage, retention, and system performance
- Troubleshot logging and reporting issues

Target Audience

This course is ideal for:

- Network and Security Administrators
- SOC Analysts and Incident Responders

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

- Fortinet Solution Engineers
- Compliance and Audit Professionals
- IT Operations and Security Teams

Pre-Requisites

Participants should have:

- Basic understanding of networking and security concepts
- Familiarity with FortiGate and Fortinet security products
- Experience with log analysis is beneficial but not required

Course Content

Module 1: Introduction to FortiAnalyzer 7.4

- FortiAnalyzer role in the Fortinet Security Fabric
- Deployment models and system requirements
- User interface and navigation

Module 2: Log Collection and Device Management

- Registering and authorizing devices
- Log forwarding and real-time logging
- Log storage and retention policies

Module 3: Log Analysis and Visualization

- Traffic and security log analysis
- Dashboards and widgets
- Event correlation and filtering

Module 4: Reporting and Compliance

- Predefined and custom reports
- Scheduling and distribution of reports
- Compliance and audit reporting

Module 5: Incident Investigation and Forensics

- Log-based threat investigation
- Event timelines and analysis tools
- Integrating FortiAnalyzer with SOC workflows

Module 6: System Administration and Best Practices

- System performance and maintenance
- Backup, restore, and upgrades
- Troubleshooting and operational best practices