

FortiAnalyzer Administrator 7.4 Course

Course Duration: 8 Hrs.

Course Code: FAZ-ADM-7.4

Course Overview

The **FortiWeb Administrator Version 7.4** course is designed for security professionals responsible for protecting web applications using Fortinet's FortiWeb Web Application Firewall (WAF). This course focuses on deploying, configuring, and managing FortiWeb 7.4 to secure web applications against common and advanced threats such as OWASP Top 10 attacks, bots, and API abuse. Participants will gain practical knowledge to implement effective WAF policies, monitor application traffic, and ensure compliance and performance in enterprise environments.

What You'll Learn?

By completing this course, you will be able to:

- Understand FortiWeb architecture and deployment modes
- Configure web application protection policies
- Protect against OWASP Top 10 and zero-day threats
- Implement bot mitigation and API security
- Monitor, log, and analyze web traffic and attacks
- Tune policies to reduce false positives
- Troubleshoot and optimize FortiWeb deployments

Target Audience

This course is ideal for:

- Web Application Security Engineers
- Network and Security Administrators

- SOC Analysts and Incident Responders
- DevOps and Application Support Teams
- Professionals managing WAF solutions

Pre-Requisites

Participants should have:

- Basic understanding of networking and HTTP/HTTPS
- Familiarity with web application concepts
- Experience with security fundamentals is recommended

Course Content

Module 1: Introduction to FortiWeb 7.4

- FortiWeb role in application security
- Deployment modes and architecture
- FortiWeb interface and system settings

Module 2: Web Application and Server Protection

- Creating protected web applications
- Server pools and load balancing basics
- SSL/TLS configuration

Module 3: Security Policies and Threat Protection

- Signature-based and behavior-based protection
- OWASP Top 10 protections
- Zero-day threat mitigation

Module 4: Bot Mitigation and API Security

- Bot detection and management
- API security fundamentals
- Protecting REST and SOAP APIs

Module 5: Monitoring, Logging, and Tuning

- Traffic monitoring and attack logs
- Reducing false positives
- Performance optimization

Module 6: Maintenance, Troubleshooting, and Best Practices

- Backup, restore, and upgrades
- Troubleshooting common issues
- Best practices and course wrap-up