

# Forti-Web Administrator 6.4

**Course Duration: 3 Days**

## **Who Should Attend:**

Security professionals involved in the management, configuration, administration, and monitoring of FortiWeb in small to large enterprise deployments should attend this course.

## **Prerequisites**

You must have an understanding of the topics covered in FCP - FortiGate Administrator, or have equivalent experience.

It is also recommended that you have an understanding of the following topics:

- HTTP protocol
- Basic knowledge of HTML,
- JavaScript, and
- server-side dynamic page languages, such as PHP

## **Table of Contents**

1. Introduction
2. Basic Setup
3. Compliance
4. Authentication and Access Control
5. Web Application Security
6. DoS and Defacement
7. SSL/TLS and Certificates
8. Application Delivery
9. API Protection
10. Machine Learning
11. Additional Configuration
12. Troubleshooting

## **Objectives:-**

After completing this course, you will be able to:

- Define web application firewall and describe its role in the network
- Perform basic configuration and initial deployment
- Configure FortiWeb for deployment in a load balanced network environment
- Implement FortiWeb machine learning capabilities
- Configure and customize FortiWeb signatures
- Configure FortiWeb to protect against DoS and defacement attacks
- Configure API protection and bot mitigation
- Implement SSL/TLS encryption, including inspection and offloading
- Configure user authentication and access control features
- Configure FortiWeb to ensure PCI DSS compliance of your web applications | Configure FortiWeb to perform caching and compression tasks