

## NSE 6 FortiAuthenticator 6.1 Course

**Course Duration: 16 Hrs.**

**Course Code: NSE6-FAUTH-6.1**

### Course Overview

The **NSE 6 FortiAuthenticator 6.1** course is designed for security and network professionals responsible for identity management and authentication services in enterprise environments. This course provides in-depth knowledge of deploying, configuring, and managing FortiAuthenticator 6.1 to centralize authentication, implement Single Sign-On (SSO), and enforce secure access policies. Participants will learn to integrate FortiAuthenticator with Fortinet Security Fabric and other IT systems, while preparing for the NSE 6 FortiAuthenticator certification exam.

### What You'll Learn?

By completing this course, you will be able to:

- Deploy and configure FortiAuthenticator 6.1
- Implement centralized authentication for users and devices
- Configure Single Sign-On (SSO) and two-factor authentication (2FA)
- Integrate FortiAuthenticator with FortiGate, FortiClient, and other IT systems
- Monitor authentication events and generate compliance reports
- Troubleshoot authentication and identity management issues
- Apply best practices for identity and access management

### Target Audience

This course is ideal for:

- Network and Security Administrators
- Identity and Access Management (IAM) Professionals
- SOC Analysts and Incident Response Teams
- IT Operations Teams managing authentication and access control
- Professionals preparing for the NSE 6 FortiAuthenticator certification

## Pre-Requisites

Participants should have:

- Understanding of networking fundamentals (TCP/IP, VLANs, routing)
- Familiarity with authentication protocols (LDAP, RADIUS, SAML)
- Experience with Fortinet products or NSE 4-level knowledge is recommended

## Course Content

### Module 1: FortiAuthenticator 6.1 Architecture and Deployment

- System architecture and components
- Deployment models and sizing
- Initial setup and configuration

### Module 2: User and Device Authentication

- Authentication methods (LDAP, RADIUS, local database)
- User and device registration
- Authentication policy configuration

### Module 3: Single Sign-On (SSO) and Two-Factor Authentication

- Configuring SSO for applications and devices
- Implementing 2FA for secure access
- Integration with FortiGate, FortiClient, and third-party apps

#### **Module 4: Monitoring, Logging, and Reporting**

- Authentication event monitoring
- Dashboards and analytics
- Compliance reporting and audit trails

#### **Module 5: Integration and Security Fabric**

- Integration with Fortinet Security Fabric
- Policy enforcement across devices
- Automated response and alerting

#### **Module 6: Troubleshooting, Maintenance, and Best Practices**

- Common issues and troubleshooting steps
- Backup, restore, and upgrades
- Best practices for deployment and operations