

NSE 6 FortiNAC 9.1 Course

Course Duration: 24 Hrs.

Course Code: NSE6-FNAC-9.1

Course Overview

The **NSE 6 FortiNAC 9.1** course is designed for network and security professionals responsible for securing and managing network access in enterprise environments. This course provides in-depth knowledge of deploying, configuring, and managing FortiNAC 9.1 to enforce network access control policies, monitor devices, and enhance network visibility. Participants will learn how to identify, classify, and control endpoints, mitigate security risks, and integrate FortiNAC with the Fortinet Security Fabric. The course also prepares learners for the NSE 6 FortiNAC certification exam.

What You'll Learn?

By completing this course, you will be able to:

- Deploy and configure FortiNAC 9.1 in enterprise networks
- Discover, classify, and monitor network endpoints
- Implement role-based network access control policies
- Detect and mitigate rogue devices and security threats
- Integrate FortiNAC with FortiGate, FortiSwitch, and Security Fabric
- Monitor network activity and generate compliance reports
- Troubleshoot and optimize FortiNAC deployments

Target Audience

This course is ideal for:

- Network Security Engineers and Administrators
- SOC Analysts and Incident Response Teams

- IT Infrastructure and Network Operations Teams
- Professionals managing endpoint and network access security
- Professionals preparing for the NSE 6 FortiNAC certification

Pre-Requisites

Participants should have:

- Strong understanding of networking fundamentals (TCP/IP, VLANs, routing)
- Familiarity with network security concepts and NAC solutions
- Experience with Fortinet products or NSE 4-level knowledge is recommended

Course Content

Module 1: FortiNAC 9.1 Architecture and Deployment

- FortiNAC components and architecture
- Deployment options and sizing
- Initial configuration and system setup

Module 2: Network Visibility and Endpoint Discovery

- Device discovery and classification
- Endpoint inventory management
- Monitoring device behavior and traffic patterns

Module 3: Network Access Control Policies

- Role-based access control (RBAC)
- Policy enforcement and quarantine actions
- Guest and BYOD management

Module 4: Threat Detection and Mitigation

- Rogue device detection
- Threat response and automated remediation
- Integration with FortiGate and FortiSwitch

Module 5: Reporting, Dashboards, and Compliance

- Monitoring dashboards and analytics
- Custom and scheduled reports
- Compliance management and audit trails

Module 6: Troubleshooting, Maintenance, and Best Practices

- System diagnostics and troubleshooting
- Performance optimization
- Best practices for FortiNAC deployment and operations