

NSE 5 FortiManager Course

Course Duration: 16 Hrs.

Course Code: NSE5-FMG

Course Overview

The **NSE 5 FortiManager** course is designed for experienced network and security professionals who manage Fortinet security devices at scale. This course focuses on advanced centralized management using FortiManager, including policy orchestration, automation, device lifecycle management, and multi-tenant administration. Participants will gain the expertise required to efficiently manage large FortiGate environments and prepare for the NSE 5 FortiManager certification exam.

What You'll Learn?

By completing this course, you will be able to:

- Deploy and manage FortiManager in enterprise environments
- Implement advanced policy and object management
- Use Administrative Domains (ADOMs) for multi-tenancy
- Automate configuration and policy workflows
- Manage firmware, revisions, and compliance
- Integrate FortiManager with the Fortinet Security Fabric
- Troubleshoot and optimize centralized management operations

Target Audience

This course is ideal for:

- Senior Network and Security Engineers
- Fortinet Solution Architects

- SOC and NOC Leads
- Managed Security Service Providers (MSSPs)
- Professionals preparing for the NSE 5 FortiManager certification

Pre-Requisites

Participants should have:

- Strong experience with FortiGate administration
- In-depth understanding of networking and firewall concepts
- Prior knowledge of FortiManager or NSE 4 level is recommended

Course Content

Module 1: FortiManager Architecture and Deployment

- FortiManager system architecture
- Deployment models and sizing
- High availability and scalability

Module 2: Advanced ADOM and Device Management

- ADOM design and best practices
- Device provisioning and lifecycle management
- Multi-tenant administration

Module 3: Centralized Policy and Object Management

- Advanced policy package design
- Object databases and normalization
- Policy installation and validation

Module 4: Automation and Workflow Management

- Scripts, automation, and APIs
- Workflow mode and approval processes
- Configuration templates

Module 5: Compliance, Revision Control, and Integration

- Policy revision history and auditing
- Firmware and configuration compliance
- Integration with Fortinet Security Fabric

Module 6: Monitoring, Troubleshooting, and Best Practices

- System monitoring and diagnostics
- Troubleshooting sync and policy issues
- Operational best practices and exam preparation