# NSE 5 Network Security Analyst—FortiManager 7.0 Course

**Course Duration: 16 Hrs.** **Course Code: NSE5-FMG-7.0**

## Course Overview

The **NSE 5 Network Security Analyst — FortiManager 7.0** course is designed for experienced network and security professionals who manage and analyze large-scale Fortinet security deployments. This course focuses on advanced centralized management using FortiManager 7.0, enabling participants to efficiently control policies, configurations, and device lifecycles across multiple FortiGate devices. The training also prepares learners for the NSE 5 Network Security Analyst certification with a specialization in FortiManager.

## What You'll Learn?

By completing this course, you will be able to:

- Deploy and manage FortiManager 7.0 in enterprise environments
- Use Administrative Domains (ADOMs) for scalable and multi-tenant management
- Design and manage advanced policy packages and objects
- Automate workflows and configuration tasks
- Perform firmware, configuration, and revision management
- Integrate FortiManager with the Fortinet Security Fabric
- Analyze and troubleshoot centralized management issues

## Target Audience

This course is ideal for:

- Network Security Analysts
- Senior Network and Security Engineers

- Fortinet Solution Architects
- SOC and NOC Professionals
- Managed Security Service Provider (MSSP) Teams

## Pre-Requisites

Participants should have:

- Strong hands-on experience with FortiGate firewalls
- Solid understanding of networking and security concepts
- Prior exposure to FortiManager or NSE 4-level knowledge is recommended

## Course Content

**Module 1: FortiManager 7.0 Architecture and Deployment**

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

**Module 2: ADOMs and Advanced Device Management**

- ADOM structure and best practices
- Device onboarding and lifecycle management
- Multi-tenant and MSSP use cases

**Module 3: Centralized Policy and Object Management**

- Policy packages and object databases
- Policy installation workflows
- Revision control and validation

**Module 4: Automation and Workflow Optimization**

- Scripts, automation, and API usage
- Workflow mode and approval processes
- Configuration templates and provisioning

**Module 5: Compliance, Integration, and Change Management**

- Configuration compliance and auditing
- Firmware management
- Integration with Fortinet Security Fabric

**Module 6: Monitoring, Troubleshooting, and Best Practices**

- Monitoring FortiManager operations
- Troubleshooting synchronization and policy issues
- Operational best practices and exam preparation