

NSE 6 FortiMail 6.4 Course

Course Duration: 24 Hrs.

Course Code: NSE6-FMAIL-6.4

Course Overview

The **NSE 6 FortiMail 6.4** course is designed for security professionals responsible for protecting email infrastructure from spam, phishing, malware, and advanced email-based threats. This advanced course provides in-depth knowledge of deploying, configuring, and managing FortiMail Secure Email Gateway version 6.4. Participants will learn how to implement robust email security policies, ensure compliance, and integrate FortiMail with the Fortinet Security Fabric while preparing for the NSE 6 FortiMail certification exam.

What You'll Learn?

By completing this course, you will be able to:

- Deploy and configure FortiMail 6.4
- Implement advanced anti-spam, anti-phishing, and anti-malware protection
- Secure inbound, outbound, and internal email traffic
- Configure encryption, DLP, and compliance policies
- Integrate FortiMail with FortiGate and FortiSandbox
- Monitor email traffic, logs, and reports
- Troubleshoot and optimize FortiMail deployments

Target Audience

This course is ideal for:

- Email Security Administrators
- Network and Security Engineers

- SOC Analysts and Incident Response Teams
- Messaging and Collaboration Administrators
- Professionals preparing for the NSE 6 FortiMail certification

Pre-Requisites

Participants should have:

- Strong understanding of email protocols (SMTP, POP3, IMAP)
- Knowledge of networking and security fundamentals
- Familiarity with Fortinet products or NSE 4-level knowledge is recommended

Course Content

Module 1: FortiMail 6.4 Architecture and Deployment

- FortiMail components and architecture
- Deployment modes and system sizing
- Installation and initial configuration

Module 2: Email Protection and Threat Prevention

- Anti-spam and anti-phishing techniques
- Malware detection and outbreak prevention
- Reputation services and threat intelligence

Module 3: Encryption, DLP, and Compliance

- Email encryption and secure messaging
- Data Loss Prevention (DLP) policies
- Compliance and regulatory requirements

Module 4: Advanced Security and Integration

- FortiSandbox and FortiGuard integration
- Authentication and user protection
- Security Fabric connectivity

Module 5: Monitoring, Logging, and Reporting

- Email traffic monitoring and dashboards
- Log analysis and reporting
- Alerting and incident tracking

Module 6: Troubleshooting, Optimization, and Best Practices

- Common FortiMail issues and resolutions
- Performance tuning and high availability
- Best practices and exam preparation