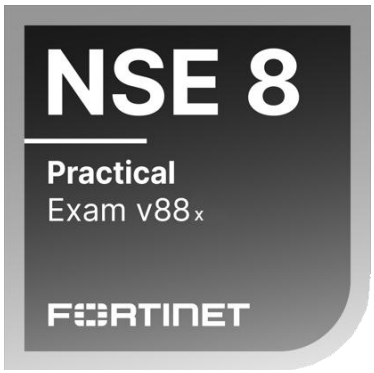



# NSE8v4 Certification

Pre-release Information

FORTINET
Training Institute

**Fortinet Product Documentation**

https://docs.fortinet.com

**Fortinet Knowledge Base**

https://kb.fortinet.com

**Fortinet Forums**

https://forum.fortinet.com

**Fortinet Product Support**

https://support.fortinet.com

**FortiGuard Labs**

https://www.fortiguard.com

**Fortinet Training Program Information**

https://www.fortinet.com/nse-training

**Fortinet Training Institute - Library**

https://training.fortinet.com

**Fortinet Training Institute Helpdesk (training questions, comments, feedback)**

https://helpdesk.training.fortinet.com/support/home

NSE 8 v4 Certification Pre-release Information for FortiGate 7.6.x and higher

Version 1.0

Last Updated: 6 October 2025

# Table of Contents

# About This Document

This document provides all the information related to the transition period between the 3rd and 4th generations of NSE 8 exams, serving as guidance for test-takers preparing for the NSE 8 exams.

**Disclaimer:** This document is subject to change without notice. Review the latest version of this document on the Fortinet public website:

https://training.fortinet.com/local/staticpage/view.php?page=fcx_cybersecurity


# Network Security Expert (NSE 8)

## Fortinet NSE 8 Certification

Welcome to the NSE 8 Certification pre-release preparation handbook. This document provides all the necessary information for test takers to prepare for the upcoming release of the NSE 8 certification exams.

The NSE 8 certification recognizes that the successful candidate has demonstrated comprehensive and in-depth ability to design, configure, and troubleshoot network security using Fortinet products in complex networks.

NSE 8 is the top-level certification in the Fortinet certification program, designed to reflect best practices for using Fortinet solutions in network security and cybersecurity.

**Important!** Fortinet Certified Expert, or FCX, was introduced on October 1st, 2023. The certification was previously known as Fortinet NSE 8. As of October 15th, 2025, Fortinet is reverting to NSE 1 through 8 for exam levels. Hence, exam names will continue to use 'NSE 8'.

## Audience

The intended audience for this document is as follows:

1. Network security and cybersecurity professionals preparing for or interested in attempting the NSE 8 certification.
2. Partners, distributors, authorized training centers (ATCs), and the members of the public seeking more information about the upcoming changes to the NSE 8 program.
3. Network security and cybersecurity professionals who are currently certified.

# Current Practical Exam Timelines

The current Network Security Expert 8 Practical Exam (NSE8_870) will be replaced with new practical exams. The following table lists important dates related to the delivery of the current NSE8_870 exam.

| | |
|---|---|
| Last day to start scheduling | February 15th, 2026 |
| Last day to take the exam | March 15th, 2026 |

Starting February 15th, only scheduling requests for the new exams will be accepted. The following table lists important dates related to the new NSE8_880 exams.

| | |
|---|---|
| First day to start scheduling for NSE8_880 exams | **February 16th, 2026** |
| First day to take the new NSE8_880 exams | April 15th, 2026 |

After March 15th, if a candidate needs to retake the NSE 8 practical exam, they must meet the requirements of the updated NSE 8 certification program.

# New Certification Requirements

The initial assessment for the updated NSE 8 certification is composed of two practical exams:

1. Pass the NSE 8 Core exam module
2. Pass one NSE 8 Specialization exam module within one year of passing the Core exam module

The following prerequisites must be completed to be eligible for scheduling the Core module:

1. Pass the NSE 4 exam (Version 7.6 or higher)
2. Pass one NSE 5 **or** NSE 6 exam of choice
3. Pass one NSE 7 exam (Version 7.6 or higher)

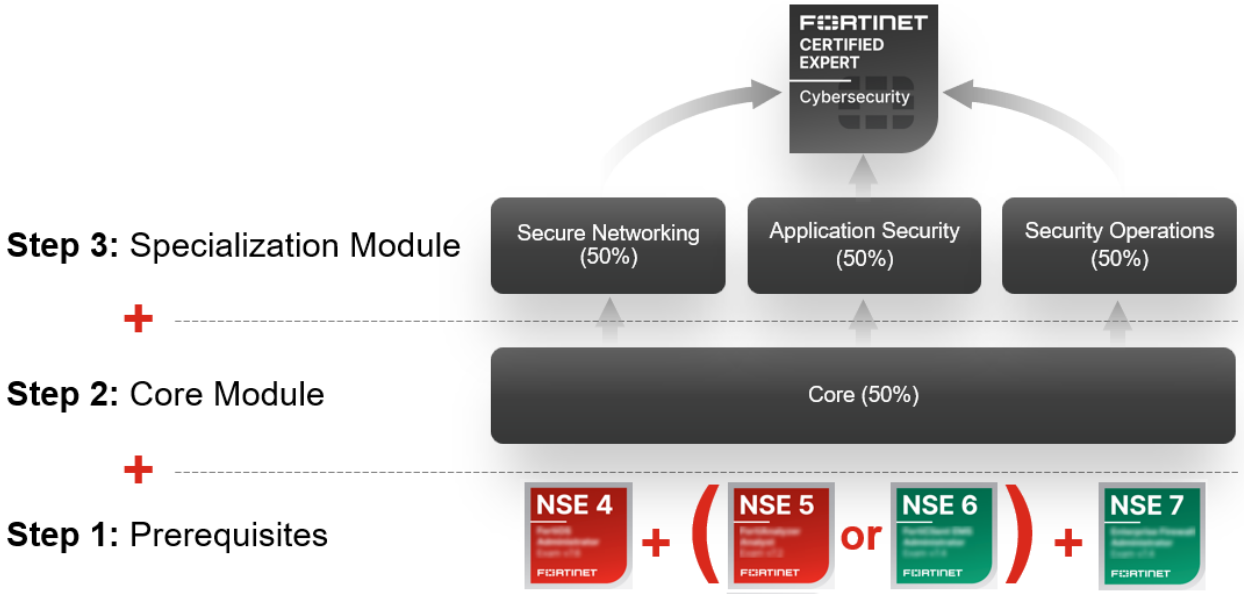
Passing only the Core module is not a certification. You must pass both practical exam modules to obtain the NSE 8 certification.

When scheduling the new version of the exams, candidates must provide the following information to ensure the best possible experience:

- Business email address (if the training account is using a generic email address)
- Country of residence
- Mobile phone number

If a candidate's records are incomplete or inconsistent, additional information may be requested to validate the candidate's identity and relationship with Fortinet.

The following image represents the complete program:




To begin, pass the NSE 4 and NSE 7 exam, and either NSE 5 or NSE 6. Exams can be taken from any of the four NSE certification tracks.

# Written Exam and Recertification

The current NSE 8 written exam (NSE8_812) will be discontinued as a prerequisite for initial certification. The last delivery date is December 31st, 2025. The NSE8_812 exam can only be used as a prerequisite for the NSE8_870 practical exam.

An updated version (NSE8_813) of the written exam will be released for current certified professionals who are required to recertify in 2026.

# Practical Exam Modules

After the candidate has passed the prerequisites, they can register to take the practical exam modules online. Every module is a four (4) hour practical assessment. During the practical exams, the candidate must build, configure, and troubleshoot a complete network topology that includes multiple Fortinet products and solutions.

Details of the NSE 8 practical exam modules:

- Exam series: NSE8_88x
- Language: English only
- Available: Online proctored
- Cost: USD 800.00
- Number of tasks: to be determined
- Appointment time: 4 hours 30 minutes (average)
- A session consists of the following time blocks:
    - 15 minutes (average): Validation by the proctor
    - 5 minutes (max): Reading/Accepting the Terms & Conditions
    - 8 minutes (max): Lab Instruction
    - 4 hours (max): Completing the exam tasks
    - 5 minutes(max): Exam feedback
- Task scoring method: Some tasks must be 100% correct for credit, while others allow for partial credit. No deductions are made for incorrect answers.
- Type of tasks: Hands-on configuration, troubleshooting, drag and drop, and multiple choice
- Time required between unsuccessful attempts: 30 days
- Time for acknowledgment and score to be reflected in the Training Institute transcripts: 30 days
- Exam scoring: pass or fail
- The test taker will receive an Exam Summary report showing their overall result, whether they pass or fail. If the result is a ‘fail,’ performance details for each exam section will be provided. No additional information or support is provided.

The following sections detail the scope and coverage of each module.

# Core Module

The table below shows a breakdown of the domains and their associated weights.

| Domain | Weight | Products Covered |
|---|---|---|
| **1. Infrastructure** | 27% | **FortiGate**<br>**FortiManager**<br>**FortiAnalyzer**<br>**FortiAuthenticator** |
| **2. Networking** | 40% | |
| **3. Authentication** | 14% | |
| **4. Security Fabric** | 19% | |

## Core Module Topics

The topics listed below outline the potential content you may see on the exam. Your understanding and skills in these areas will be assessed through tasks involving design, configuration, and troubleshooting.

1. Infrastructure
   - 1.1. High Availability
     - 1.1.1. Aggregation (LACP)
     - 1.1.2. FGCP
     - 1.1.3. FGSP
     - 1.1.4. FortiAnalyzer HA
     - 1.1.5. FortiAuthenticator HA
     - 1.1.6. FortiManager HA
     - 1.1.7. Virtual Clustering
     - 1.1.8. VRRP
   - 1.2. SD-WAN Architecture
     - 1.2.1. Application performance
     - 1.2.2. Multi-datacenter
     - 1.2.3. Redundant connectivity
     - 1.2.4. Work from anywhere
   - 1.3. System Optimization

1.3.1. Hardening
1.3.2. Performance Tuning

1.4. System Management
1.4.1. FG-VM Bootstrapping
1.4.2. Firmware Management
1.4.3. FortiAnalyzer Integration
1.4.4. FortiGuard
1.4.5. FortiManager Policy Packages
1.4.6. Log Management
1.4.7. Multi-Tenancy
1.4.8. Virtual Domains
1.4.9. Operation modes
1.4.10. VM deployments
1.4.11. Workspace Mode

2. Networking

2.1. SASE
2.1.1. Prepping for SPA
2.1.2. SD-WAN On-ramp to SASE
2.1.3. Secure Private Access

2.2. Routing
2.2.1. Asymmetric Routing
2.2.2. BFD
2.2.3. Dynamic Routing
2.2.4. ECMP
2.2.5. Multicast
2.2.6. Policy Routing
2.2.7. Policy-Based Routing
2.2.8. SD-WAN Routing
2.2.9. Static Routing
2.2.10. VRFs

2.3. VPN

- 2.3.1. ADVPN
- 2.3.2. Dial-up
- 2.3.3. IPsec
- 2.3.4. Overlay VPN
- 2.3.5. Post-Quantum Cryptography for IPsec key exchange
- 2.3.6. SD-WAN
- 2.3.7. SSL VPN
- 2.3.8. VXLAN over Ipsec
- 2.3.9. ZTNA

2.4. Next Generation Firewall

- 2.4.1. Fabric Integrations
- 2.4.2. Inspection Modes
- 2.4.3. IPv6
- 2.4.4. Policy Modes
- 2.4.5. Proxy rules
- 2.4.6. Security Profiles
- 2.4.7. DLP
- 2.4.8. Web Filtering
- 2.4.9. SSL Inspection
- 2.4.10. IPS
- 2.4.11. Transparent mode

2.5. Advanced Networking

- 2.5.1. Asymmetric Routing
- 2.5.2. Explicit Proxy
- 2.5.3. Inter-VDOM Routing
- 2.5.4. IPv6
- 2.5.5. Local-In policies
- 2.5.6. Local-out routing
- 2.5.7. NAT

- 2.5.8. Traffic Shaping
- 2.5.9. Transparent Mode
- 2.5.10. Transparent Proxy
- 2.5.11. VLANs
- 2.5.12. Zones

3. Authentication
   - 3.1. Authentication Solutions
     - 3.1.1. 802.1X
     - 3.1.2. ADOM-Scoped Admins
     - 3.1.3. Advanced authentication
     - 3.1.4. API Authentication
     - 3.1.5. Captive Portal
     - 3.1.6. Device/user authentication
     - 3.1.7. Fabric Single Sign-On
     - 3.1.8. Fortinet Single Sign-On
     - 3.1.9. Identity access management
     - 3.1.10. LDAP
     - 3.1.11. OAuth
     - 3.1.12. RADIUS
     - 3.1.13. RSSO
     - 3.1.14. SAML
     - 3.1.15. SNMPv3
     - 3.1.16. SSOMA
     - 3.1.17. SYSLOG SSO
     - 3.1.18. Tacacs+
   - 3.2. Certificate Management
     - 3.2.1. Certificate Authority
     - 3.2.2. Certificate-based authentication
     - 3.2.3. CMP
     - 3.2.4. OCSP

# Secure Networking Module

The table below presents a breakdown of the domains, with their associated weight.

| Domain | Weight | Products Covered * |
|---|---|---|
| **1. Secure SD-WAN** | 25% | **FortiClient EMS**<br>**FortiSwitch**<br>**FortiNAC**<br>**FortiSandbox** |
| **2. Endpoint Security** | 20% | |
| **3. Threat Mitigation** | 30% | |
| **4. Enterprise Networking** | 25% | |

* The Secure Networking specialization module expands on the Core module. Therefore, all products in the core module are also part of this Specialization module.

## Secure Networking Topics

The topics listed below outline the potential content you may see on the exam. Your understanding and skills in these areas will be assessed through tasks involving design, configuration, and troubleshooting.

1. Secure SD-WAN
    1.1. Overlay VPN and Advanced Routing
        1.1.1. 4G/5G "last option" links
        1.1.2. Advanced ADVPN
        1.1.3. Advanced IPSec troubleshooting (finding network-id mismatch,
        1.1.4. ADVPN 2.0 vs Legacy
        1.1.5. Application-based Routing
        1.1.6. Bandwidth Aggregation
        1.1.7. BGP multipath
        1.1.8. Deploy SD-Branch
        1.1.9. Dynamic BGP
        1.1.10. Dynamic QoS
        1.1.11. FEC

1.1.12. Full Mesh Overlay Networks (different than IPSec and BGP)
1.1.13. Load Balancing & Redundancy
1.1.14. MOS
1.1.15. Performance Monitoring
1.1.16. Performance SLAs & Service Rule
1.1.17. Policy Based Routing
1.1.18. Remote health signaling from Spokes to Hub
1.1.19. Remote health signaling to 3rd party device - MED or AS-Path prepend
1.1.20. Route Monitoring / Triaging (Why can Br1 get to Br3)
1.1.21. SD-WAN Interfaces
1.1.22. Self-healing with BGP
1.1.23. Single hub / dual hub
1.1.24. SLA probe DSCP marking
1.1.25. VRFs

1.2. SD-WAN Orchestration

1.2.1. Central VPN
1.2.2. Jinja2 templates
1.2.3. Overlay Orchestrator
1.2.4. Variables
1.2.5. FMG Zero Touch Provisioning
1.2.6. Jinja scripting
1.2.7. Templates

2. Endpoint Security

2.1. ZTNA

2.1.1. ZTNA profiles
2.1.2. Agent-less portal on FortiGate
2.1.3. Zero Trust Tags
2.1.4. ZTNA Access proxy - HTTP/HTTPS
2.1.5. ZTNA TCP Proxy

2.2. Endpoint Protection

2.2.1. Endpoint malware protection
2.2.2. AntiExploit
2.2.3. Antiransomware
2.2.4. FortiClient
2.2.5. FortiClient EMS HA
2.2.6. FortiClient EMS Integration
2.2.7. Quarantine
2.2.8. Sandbox Integration

3. Threat Mitigation

3.1. Advanced Threat Protection

3.1.1. Custom IPS Signatures
3.1.2. DDoS (FGT)
3.1.3. Deep Traffic Inspection
3.1.4. FortiGuard
3.1.5. In-line integration
3.1.6. Sandbox Detection
3.1.7. FortiSandbox HA
3.1.8. Sniffer integration
3.1.9. Threat feed integration
3.1.10. Vulnerability Scan

3.2. Next Generation Firewall

3.2.1. CASB
3.2.2. CGNAT
3.2.3. Domain Fronting Protection
3.2.4. Fabric Integrations
3.2.5. Inspection Modes
3.2.6. IPv6
3.2.7. OT Security
3.2.8. Policy Modes
3.2.9. Proxy rules

4.3.17. VLANs

4.3.18. VRF Routing

4.3.19. VXLAN

4.3.20. VXLan over IPsec

4.3.21. VLAN inside VXLan

4.3.22. Zones

# Application Security Module

The table below presents a breakdown of the domains, with their associated weight.

| Domain | Weight | Products Covered * |
|---|---|---|
| 1. **Email Security** | 27% | **FortiADC**<br>**FortiWeb**<br>**FortiMail**<br>**FortiSandbox** |
| 2. **Application Delivery** | 44% | |
| 3. **Threat Detection** | 12% | |
| 4. **Infrastructure** | 17% | |

* The Application Security specialization module expands on the Core module. Therefore, all products in the Core module are also part of this Specialization module.

## Application Security Topics

The topics listed below outline the potential content you may see on the exam. Your understanding and skills in these areas will be assessed through tasks involving design, configuration, and troubleshooting.

1. Email Security
    1.1. Email Infrastructure
        1.1.1. Archiving
        1.1.2. DNS Security
        1.1.3. Domains
        1.1.4. Email Encryption
        1.1.5. Identity Based Encryption
        1.1.6. Monitoring
        1.1.7. Quarantining
        1.1.8. SMTP/IMAP/POP3
        1.1.9. User Authentication
        1.1.10. Webmail
    1.2. Antispam and Threat Protection

1.2.1. AntiSpam Profiles
1.2.2. Antivirus Profiles
1.2.3. Bounce Verification
1.2.4. Content Disarm and Reconstruction
1.2.5. Content Profiles
1.2.6. DLP
1.2.7. Endpoint Reputation
1.2.8. IP Policies
1.2.9. Recipient-Based Policies
1.2.10. Sandbox Integration
1.2.11. Sender-Based Policies
1.2.12. Session Profiles
1.2.13. Threat Feeds
1.2.14. URL Filter

2. Application Delivery
   2.1. Application Access
      2.1.1. Application Access Manager
      2.1.2. Single Sign-on
      2.1.3. Agentless Application Gateway
      2.1.4. Users & Authentication
   2.2. Load Balancing
      2.2.1. Global Load Balance
      2.2.2. Network Security
      2.2.3. Application Load Balancing
      2.2.4. Scripting
      2.2.5. Server Load Balance
      2.2.6. WCCP
   2.3. Web Security
      2.3.1. Advance Bot Protection
      2.3.2. API Protection

2.3.3. Bot Mitigation
2.3.4. DoS Protection
2.3.5. IP Protection
2.3.6. Machine Learning
2.3.7. OWASP Top 10
2.3.8. Secure connections
2.3.9. Tracking
2.3.10. WAF Adaptive Learning 2.0
2.3.11. Web Protection
2.3.12. Web Vulnerability Scanner

3. Threat Detection
   3.1. Sandbox Analysis & Detection
      3.1.1. Air-Gapped Sandboxing
      3.1.2. Malware Behavior Analysis
      3.1.3. On-Demand Scanning
      3.1.4. Risk Analysis
      3.1.5. Scan Jobs
      3.1.6. Scan Policy and Object
      3.1.7. Website Scanning
      3.1.8. Network Share Protection
      3.1.9. Operational Technology Protection
      3.1.10. Setup for dedicated internet
      3.1.11. Inline Sandbox
4. Infrastructure
   4.1. System Management
      4.1.1. FortiADC Clustering
      4.1.2. FortiWeb Clustering
      4.1.3. FortiMail Clustering
      4.1.4. FortiSandbox Clustering
      4.1.5. Virtual/Administrative Domains

- 4.1.6. Logs & Reporting

4.2. Integration & Protection

- 4.2.1. MTA/BCC Adapter integration
- 4.2.2. Operation Modes
- 4.2.3. Kubernetes Ingress Controller
- 4.2.4. Security Fabric Integration

# Security Operations Module

The table below presents a breakdown of the domains, with their associated weight.

| Domain | Weight | Products Covered * |
|---|---|---|
| **1. Automation** | 23% | **FortiSIEM**<br>**FortiSOAR**<br>**FortiEDR**<br>**FortiManager****<br>**FortiAnalyzer**** |
| **2. Analytics and Reporting** | 26% | |
| **3. Threat Handling** | 29% | |
| **4. Infrastructure** | 22% | |

* The Security Operations specialization module expands on the Core module. Therefore, all products in the Core module are also part of this Specialization module.

** This module covers FortiManager and FortiAnalyzer to the full extent of the product. Refer to the topic list for more details.

## Security Operations Topics

The topics listed below outline the potential content you may see on the exam. Your understanding and skills in these areas will be assessed through tasks involving design, configuration, and troubleshooting.

1. Automation
    1.1. Configuration Management & Scripting
        1.1.1. FMG Jinja scripting
        1.1.2. FMG Provisioning Templates
        1.1.3. Fortinet APIs
    1.2. Workflow Automation and Orchestration
        1.2.1. Automated Incident Response
        1.2.2. Automation Connectors
        1.2.3. FAZ Playbooks
        1.2.4. Fortinet Security Fabric
        1.2.5. Outbreak Alerts

1.2.6. SOAR Playbooks
1.2.7. Workflow/Workspace
1.2.8. FortiSIEM Automation Service (Cloud)

2. Analytics and Reporting
   2.1. Data Processing and Reporting
      2.1.1. CMDB
      2.1.2. Compliance Reports
      2.1.3. Custom Log Parsers
      2.1.4. Datasets
      2.1.5. FortiAnalyzer Custom Reports
      2.1.6. FortiSIEM Analytics
      2.1.7. FortiSOAR Reports
      2.1.8. Hcache
      2.1.9. Incident Reporting
      2.1.10. SIEM Parsers and Monitors
      2.1.11. SQL
      2.1.12. Dashboards
   2.2. Security Incident Analysis
      2.2.1. Case Management
      2.2.2. EDR Security Incidents
      2.2.3. Indicators of Compromise
      2.2.4. Investigation View
      2.2.5. Searches and Filters
      2.2.6. SIEM Analytics Search
3. Threat Handling
   3.1. Endpoint Detection & Response
      3.1.1. EDR Threat Hunting
      3.1.2. eXtended Detection
      3.1.3. Device Isolation and Remediation
      3.1.4. FortiEDR Connect

- 3.2. Incident Response & Management
  - 3.2.1. Incident Response
  - 3.2.2. War Rooms
  - 3.2.3. Simulation Mode
  - 3.2.4. Incident Handling/Response Frameworks
- 3.3. Prevention & Control
  - 3.3.1. Application Communication Control
  - 3.3.2. Application Control
  - 3.3.3. Device Control
  - 3.3.4. Execution Prevention
  - 3.3.5. Exfiltration Prevention
  - 3.3.6. Prevention Mode
  - 3.3.7. Ransomware Prevention
  - 3.3.8. Suspicious Indicators Blocking
  - 3.3.9. Vulnerability Management

4. Infrastructure
   - 4.1. Access Control & Platform Management
     - 4.1.1. Advanced Health System
     - 4.1.2. CMDB (moved)
     - 4.1.3. FortiSIEM Collectors
     - 4.1.4. Device Support Advanced Operations
     - 4.1.5. HTTP Generic Poller
     - 4.1.6. Multi-tenancy
     - 4.1.7. Role-Based Access Control
     - 4.1.8. Security Management
     - 4.1.9. Segmented Network Support
   - 4.2. High Availability
     - 4.2.1. FortiEDR High Availability
     - 4.2.2. FortiAnalyzer HA
     - 4.2.3. FortiManager HA

4.2.4. FortiSOAR High Availability

4.2.5. FortiSIEM High Availability

4.3. FortiSOAR User Interface Management

4.3.1. Application Editor

4.3.2. Content Hub

4.3.3. Modules

4.3.4. Policy Analyzer MEA

4.3.5. Queue, shift and leave management

4.3.6. Rules, Reports and dashboards

4.3.7. Solution Packs

4.3.8. Widgets

# FAQ

**Q.** What if I already scheduled my exam attempt for the NSE8_870 exam for after March 15th, 2026?

**A.** You will be informed that your appointment must be changed to a date before March 15th, 2026.

**Q.** What will happen to my valid voucher for the NSE8_870 practical exam?

**A.** Current valid vouchers cover the fee for two (2) exam modules. You can request scheduling for the Core module with your current voucher, and you will receive a new voucher for the 2nd module.

**Q.** Will passing only the Core module renew lower-level certifications?

**A.** No, the Core module is the qualification exam for the Specialty module. Lower-level certifications will be renewed, if unexpired, when the NSE 8 Certification is achieved.

**Q.** I passed the NSE8_812 exam. Can I substitute it for the NSE 4 and NSE 7 pre-requisite exam requirements?

**A.** No, because the NSE8_812 exam does not align with the changes to the new practical exams, the NSE8_812 exam can only be paired with the NSE8_870 practical exam.

**Q.** Can I take the specialization exam first and then the Core module?

**A.** No. The Core module practical exam is a qualifying exam. You must first pass the Core module exam to move on to the Specialty exam.

**Q.** If less than one year after passing the Core module my FCP expires can I still sit for the specialization module?

**A .**You can still sit for the Specialization module, but if you pass and earn the NSE 8 certification, it will only recertify lower-level certifications that are still active.

**Q.** For how long is the NSE 8 Certification valid?

**A.** For 3 years, after passing the Specialization module. After a pass grade is confirmed for both the Core and Specialization exams, the NSE 8 certification is valid for three years from the date the Specialization exam is passed.

**Q.** Is a different NSE 8 certification awarded depending on the module passed?

**A.** No. The NSE 8 Certification badge and certificate are the same, regardless of which Specialization module is passed. However, a digital badge is awarded for each practical exam module that is passed.

**Q.** Do we receive a badge after passing the Core module?

**A:** Yes, a digital exam badge is awarded for each practical exam module passed. The badge for the Core module will be awarded for a period of 1 year to indicate its validity as a prerequisite for the specialization module.