Training: Fortinet

FortiNAC

Premier Authorized Training Center

TRANING TERMS

2026-02-23 | 3 days | Kraków / Virtual Classroom
2026-03-16 | 3 days | Virtual Classroom
2026-04-27 | 3 days | Virtual Classroom
2026-05-18 | 3 days | Virtual Classroom
2026-06-15 | 3 days | Virtual Classroom

TRAINING GOALS:

In this course, you will learn how to leverage the powerful and diverse capabilities of FortiNAC, using best practices for achieving visibility, control, and response. These fundamentals will provide you with a solid understanding of how to implement network visibility and security automation.

Objectives

After completing this course, you should be able to:

- Configure a FortiNAC system to achieve network visibility
- Leverage the control capabilities for network access and automated policy enforcement
- Integrate FortiNAC into the Fortinet Security Fabric
- Combine the visibility and control features with security device integrations to automate threat responses to security risks

Who Should Attend

Network and security administrators, managers, and other IT staff who will use FortiNAC should attend this course.

CONSPECT:

- Introduction and Initial Configuration

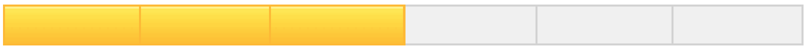
- Achieving Network Visibility
- Identification and Classification of Rogues
- Visibility, Troubleshooting, and Logging
- Logical Networks, Fortinet Security Fabric, and Firewall Tags
- State-Based Control
- Security Policies
- Guest and Contractor Management
- Security Device Integration and Automated Response
- FortiGate VPN, High Availability, and FortiNAC Control Manager Integrations

REQUIREMENTS:

It is recommended that you have an understanding of the following topics:

- Networking concepts and terms
- Networking protocols
- Infrastructure configurations

Difficulty level



CERTIFICATE:

The participants will obtain certificates signed by Fortinet (course completion).

This course prepares you also for the Fortinet *FCP - FortiNAC* exam. By passing this exam, you will be awarded the associated exam badge.

TRAINER:

Fortinet Certified Trainer (FCT)

ADDITIONAL INFORMATION:

ISC2

- CPE training hours: 11
- CPE lab hours: 6

    - CISSP domains: Communication and Network Security