

FortiAnalyzer Analyst

In this course, you will learn the fundamentals of using FortiAnalyzer for centralized logging. You will also learn how to identify current and potential threats through log analysis. Finally, you will examine the management of events, incidents, reports, and task automation with playbooks. These skills will provide you with a solid foundation for becoming a SOC analyst in an environment using Fortinet products.

Product Version

FortiAnalyzer 7.4.1

Course Duration

- Lecture time (estimated): 4 hours
- Lab time (estimated): 4 hours
- Total course duration (estimated): 8 hours
 - 1 full day or 2 half days

Who Should Attend

Anyone who is responsible for Fortinet Security Fabric analytics and automating tasks to detect and respond to cyberattacks using FortiAnalyzer should attend this course.

Certification

This course is intended to help you prepare for the *FCP—FortiAnalyzer 7.4 Analyst* exam. This exam is part of the Fortinet Certified Professional - Security Operations certification track.

Prerequisites

- Familiarity with all topics presented in the *FCP - FortiGate Security* and *FCP - FortiGate Infrastructure* courses
- Knowledge of SQL SELECT syntax is helpful

Agenda

1. Introduction and Initial Access
2. Logging
3. Incidents and Events
4. Reports
5. Playbooks

Objectives

After completing this course, you will be able to:

- Understand basic FortiAnalyzer concepts and features
- Describe the purpose of collecting and storing logs
- View and search for logs in Log View and FortiView
- Understand SOC features
- Manage events and event handlers
- Configure and analyze incidents
- Perform threat hunting tasks
- Understand outbreak alerts
- Describe how reports function within ADOMs
- Customize and create charts and datasets
- Customize and run reports
- Configure external storage for reports
- Attach reports to incidents
- Troubleshoot reports
- Understand playbook concepts
- Create and monitor playbooks

Training Delivery Options and SKUs

Instructor-Led Training

Includes standard NSE training content delivered in person onsite, or live online using a virtual classroom application. Training is delivered within [public classes](#) or as a private class. Private requests are scoped, quoted, developed, and delivered by Fortinet Training (minimum quantities apply).

Use the following ILT Training SKU to purchase scheduled public classes of this course through [Fortinet Resellers](#) or [Authorized Training Partners](#):

FT-FAZ-ANS

Self-Paced Training

Includes online training videos and resources through the [Fortinet Training Institute](#) library, free of charge.

You can purchase on-demand lab access with interactive, hands-on activities using the following methods:

- Credit card, through the course on the Fortinet Training Institute
- Purchase order (PO), through [Fortinet Resellers](#) or [Authorized Training Partners](#)

After you complete the purchase, you receive lab access and the accompanying lab guide within the self-paced course.

Use the following on-demand lab training SKU to purchase lab access using a PO:

FT-FAZ-ANS-LAB

See [Purchasing Process](#) for more information about purchasing Fortinet training products.

ISC2

- CPE training hours: 4
- CPE lab hours: 4
- CISSP domains: Security Operations

Program Policies and FAQs

For questions about courses, certification, or training products, refer to [Program Policy Guidelines](#) or [Frequently Asked Questions](#).

