



FortiAnalyzer

In this 1-day class, you will learn how to use FortiAnalyzer. You will explore setup, registering supported devices and securing communications, managing logs and archives, and configuring both predefined and customized reports.

This course provides a solid understanding of how to integrate FortiAnalyzer into your network awareness infrastructure.

Product Version

FortiAnalyzer 5.2

Formats

- Instructor-led classroom

Agenda

Objectives

- 1 Introduction to FortiAnalyzer
- 2 Configuration & Administration
- 3 Device Registration
- 4 Logs & Archives
- 5 Reports

Certification

This course is part of preparation for the NSE 5 certification exam.

After completing these courses, you will be able to:

- Describe key features and concepts of FortiAnalyzer
- Deploy an appropriate architecture
- Manage ADOMs on both FortiAnalyzer and the devices that log to it
- Configure RAID
- Register supported devices
- Encrypt log transmission (SSL / IPsec)
- View & analyze current and historical logs (FortiView)
- Monitor events
- Apply disk quotas to log data from devices
- Back up, restore, and forward log data
- Use content archiving (summary and full)
- Understand the different stages of data processing, from receiving logs to compiling reports
- Understand SQL queries and datasets used by FortiAnalyzer reports
- Design datasets, charts, and custom reports
- Generate reports by schedule or on demand

Who Should Attend

Anyone who is responsible for day-to-day management of a FortiAnalyzer appliance and FortiGate security information.

Prerequisites

- Familiarity with all topics presented in FortiGate I and FortiGate II
- Knowledge of SQL 'select' syntax is helpful