

Training: Fortinet

## FortiMail Administrator



#### TRANING TERMS

2025-12-15	3 days   Warszawa / Virtual Classroom
2026-01-26	3 days   Virtual Classroom
2026-02-09	3 days   Kraków / Virtual Classroom
2026-02-16	3 days   Virtual Classroom
2026-03-02	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 analyze email security challenges that administrators face, and learn where and how to deploy, manage, and troubleshoot FortiMail to protect your network from email-borne threats. You will also explore the role of FortiMail as a specialized device, and how its features provide both high-performance and indepth security for business-critical communications.

### Objectives

After completing this course, you will be able to:

- Position FortiMail in an existing or new email infrastructure using any of the flexible deployment modes
- Understand the system architecture of FortiMail: how email flows through its modules; how it applies intelligent routing and policies to email; and how it can protect the priceless reputation of your message transfer agent (MTA)
- Use your existing LDAP server to manage and authenticate users
- Secure email transmission using best-in-class technologies, such as SMTPS, SMTP over TLS, and identity-based encryption (IBE)
- Throttle client connections to block MTA abuse
- Block spam using sophisticated techniques, such as deep header inspection, spam outbreak, heuristics, and the FortiGuard Antispam service
- Eliminate spear phishing and zero-day viruses
- Integrate FortiMail with FortiSandbox for advanced threat protection (ATP)

www.compendium.pl page 1 of 3





- Prevent accidental or intentional leaks of confidential and regulated data
- Archive email for compliance
- Deploy high availability (HA) and redundant infrastructure for maximum up-time of missioncritical email
- Diagnose common issues related to email and FortiMail

NOTE: This course covers gateway and server mode in depth. This course also covers transparent mode, however, if you require a course on the use of transparent mode in carrier environments, you should order customized training.

Who Should Attend

Security professionals involved in the management, configuration, administration, and monitoring of FortiMail in small to medium enterprise deployments should attend this course.

## **CONSPECT:**

- Email Concepts
- Basic Setup
- Access Control and Policies
- Authentication
- Session Management
- Antivirus and Antispam
- Content Inspection
- Securing Communications
- High Availability
- Server Mode
- Transparent Mode
- Maintenance
- Troubleshooting

## **REQUIREMENTS:**

You must have an understanding of the topics covered in the FCP - FortiGate Administrator course, or have equivalent experience.

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

SMTP

www.compendium.pl page 2 of 3



- o PKI
- SSL/TLS
- LDAP

# Difficulty level

# **CERTIFICATE:**

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

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

# TRAINER:

Fortinet Certified Trainer (FCT).

# ADDITIONAL INFORMATION:

### ISC<sub>2</sub>

CPE training hours: 10

∘ CPE lab hours: 10

CISSP domains: Communication and Network Security

www.compendium.pl page 3 of 3