

Szkolenie: Fortinet  
FortiAuthenticator

**FORTINET**Premier Authorized  
Training Center

## DOSTĘPNE TERMINY

2023-12-14 | 2 dni | Kraków / Wirtualna sala  
2023-12-18 | 2 dni | Warszawa / Virtual Classroom  
2023-12-18 | 2 dni | Warszawa / Wirtualna sala  
2024-01-23 | 2 dni | Warszawa / Wirtualna sala  
2024-01-25 | 2 dni | Virtual Classroom  
2024-02-19 | 2 dni | Kraków / Virtual Classroom  
2024-02-19 | 2 dni | Kraków / Wirtualna sala  
2024-02-19 | 2 dni | Warszawa / Virtual Classroom  
2024-02-19 | 2 dni | Warszawa / Wirtualna sala  
2024-03-11 | 2 dni | Virtual Classroom  
2024-04-22 | 2 dni | Kraków / Virtual Classroom  
2024-04-22 | 2 dni | Kraków / Wirtualna sala  
2024-04-22 | 2 dni | Warszawa / Virtual Classroom  
2024-04-22 | 2 dni | Warszawa / Wirtualna sala  
2024-06-17 | 2 dni | Kraków / Virtual Classroom  
2024-06-17 | 2 dni | Kraków / Wirtualna sala  
2024-06-17 | 2 dni | Warszawa / Virtual Classroom  
2024-06-17 | 2 dni | Warszawa / Wirtualna sala

## Cel szkolenia:

In this course, you will learn how to use FortiAuthenticator for secure authentication and identity management. You will learn how to configure and deploy FortiAuthenticator, use FortiAuthenticator for certificate management and two-factor authentication, authenticate users using LDAP and RADIUS servers, and explore SAML SSO options on FortiAuthenticator.

### Objectives

After completing this course, you will be able to:

- Deploy and configure FortiAuthenticator
- Configure the LDAP and RADIUS services
- Configure the self-service portal
- Configure FortiAuthenticator and FortiGate for two-factor authentication
- Provision FortiToken hardware / mobile software tokens
- Configure FortiAuthenticator as a logon event collector using the FSSO communication framework

- Configure portal services for guest and local user management
- Configure FortiAuthenticator for wired / wireless 802.1x authentication, MAC-based authentication, and machine-based authentication using supported EAP methods
- Troubleshoot authentication failures
- Manage digital certificates (root CA, sub-CA, user, and local services digital certificates)
- Configure FortiAuthenticator as a SCEP server for CRLs and CSRs
- Configure FortiAuthenticator as a SAML identity provider and service provider
- Monitor and troubleshoot SAML
- Configure FIDO for passwordless authentication

### Who Should Attend

Anyone who is responsible for the day-to-day management of FortiAuthenticator should attend this course.

### Plan szkolenia:

- Introduction and Initial Configuration
- Administrative Users and High Availability
- Administering and Authenticating Users
- Managing Users and Troubleshooting Authentication
- Two-Factor Authentication
- FSSO Process and Methods
- FSSO Deployment and Troubleshooting
- Portal Services
- PKI and FortiAuthenticator as a CA
- Certificate Management
- 1X Authentication
- SAML
- FIDO2 Authentication

### Wymagania:

You must have an understanding of the topics covered in the FortiGate Security and FortiGate Infrastructure, or have equivalent experience.

It is also recommended that you have an understanding of Authentication, Authorization, and Accounting.

## Poziom trudności



## Certyfikaty:

The participants will obtain certificates signed by Fortinet.

This course is also intended to help you prepare for the Fortinet - FortiAuthenticator certification exam. This exam is part of the FCP Network Security certification track. More information about Fortinet certification Program on the <https://www.fortinet.com/training-certification>

## Prowadzący:

Fortinet Certified Trainer (FCT).

## Informacje dodatkowe:

### ISC2

- CPE training hours: 8
- CPE lab hours: 5
- CISSP domains: Identity and Access Management (IAM)