



Secure Access

In this two-day course, participants will learn how FortiOS, FortiAP, FortiSwitch, and FortiAuthenticator enable secure connectivity, no matter where users are located and how they are connecting. The course covers the deployment and troubleshooting of advanced authentication scenarios, together with best practices for securely connecting wireless and wired users.

Product Versions

FortiOS 6.0

Formats

- Instructor-led classroom
- Instructor-led online
- Self-paced online

Agenda

1. RADIUS and LDAP
2. Certificate-Based Authentication
3. Single Sign-On
4. IPsec Dial-Up
5. FortiSwitch Management with FortiLink
6. 802.1x Port Authentication
7. Securing the Layer 2

8. Secure Wireless Access
9. Guest Access
10. Security Assertion Markup Language (SAML)

Objectives

After completing this course, participants should be able to:

- Configure advanced user authentication and authorization scenarios using RADIUS and LDAP
- Troubleshoot user authentication and authorization problems
- Implement two-factor authentication using digital certificates
- Implement and troubleshoot single sign-on solutions integrating multiple single sign-on methods
- Configure and troubleshoot IPsec dial-up and SSL VPN access
- Manage FortiSwitch devices using FortiLink
- Configure layer 2 authentication for wired and wireless users using 802.1x
- Secure the layer 2 network
- Secure the wireless network
- Provide secure access to guest users
- Implement single sign-on among multiple providers using FortiAuthenticator and SAML

Who Should Attend

This course is intended for networking and security professionals involved in the management, configuration, administration, and monitoring of FortiGate devices used to secure the access to their organizations' networks.

Prerequisites

- Knowledge of network authentication protocols
- Knowledge of layer 2 switching
- Understanding of wireless networks
- Understanding of the topics covered in the following courses:
 - NSE 4 FortiGate Security
 - NSE 4 FortiGate Infrastructure

An understanding of the topics covered in the following courses is also recommended:

- NSE 6 FortiAuthenticator
- NSE 6 Wireless LAN

System Requirements

If participants take the online format of this class, they must use a computer that has the following:

- A high-speed Internet connection
- An up-to-date web browser
- A PDF viewer
- Speakers or headphones
- One of the following:
 - HTML5 support
 - An up-to-date Java Runtime Environment (JRE) with Java plugin enabled in your web browser

Participants should use a wired Ethernet connection, *not* a Wi-Fi connection. Firewalls, including Windows Firewall or FortiClient, must allow connections to the online labs.

Certification

This course is intended to help participants prepare for the NSE 7 Secure Access certification exam.