

SD-WAN Enterprise Administrator

Course Description

In this course, you will learn how to design, deploy, and manage advanced Fortinet Secure SD-WAN environments across branches and regions. You will also learn how to enhance and troubleshoot SD-WAN deployments, deploy complex topologies using overlay templates, and implement zero-touch provisioning for scalable deployments. These advanced topics will help you optimize SD-WAN performance and reliability in distributed enterprise networks.

Who Should Attend

Anyone responsible for designing a Fortinet SD-WAN solution or for the day-to-day management of a Fortinet SD-WAN deployment and network operations should attend this course

Prerequisites

- You must have advanced knowledge of networking, and extensive hands-on experience working with FortiGate and FortiManager.
- It is also recommended that you have an understanding of the topics covered in the following courses, or have equivalent experience:
 - SD-WAN 7.6 Core Operations Administrator
 - FortiGate 7.6 Administrator
 - FortiManager 7.6 Administrator

Agenda

1. Centralized Management
2. SD-Branch and Zero-Touch Provisioning
3. SD-WAN Overlay Design and Best Practices
4. Dual-Hub and Multiregion Topologies
5. ADVPN

Objectives

After completing this course, you will be able to:

- Describe the capabilities of the Fortinet Secure SD-WAN solution
- Configure and monitor FortiOS SD-WAN solutions with FortiManager and FortiAnalyzer
- Configure SD-WAN management on FortiManager
- Configure advanced SD-WAN features
- Use the FortiManager SD-WAN overlay orchestrator
- Use ZTP to deploy SD-WAN branch devices
- Describe the use cases for SD-WAN with dual-hub topologies
- Design a scalable SD-WAN hub-and-spoke topology

- Implement SD-WAN using ADVPN 2.0 and dynamic BGP

System Requirements

If you take the online format of this class, you 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:
 - HTML 5 support or
 - An up-to-date Java Runtime Environment (JRE) with Java plugin enabled on your web browser

You should use a wired Ethernet connection, *not* a WiFi connection. Firewalls, including Windows Firewall or FortiClient, must allow connections to the online labs.

Product Versions

- FortiOS 7.6.3
- FortiManager 7.6.3

Course Duration

- Lecture time (estimated): 6 hours
- Lab time (estimated): 7 hours
- Total course duration (estimated): 13 hours
 - 2 full days or 4 half days

Formats

- Instructor-led (classroom and online)
- Self-paced online

ISC2

- CPE training hours: 6
- CPE lab hours: 7
- CISSP domains: Security Operations

Part Number (SKU)

See Purchasing Process for more information

Certification

