FORTINET NSE Training Institute

FortiSwitch

In this course, you will learn how to deploy, provision, and manage a FortiSwitch with FortiGate using FortiLink. This course also covers the deployment and troubleshooting of Layer 2 and Layer 3 features, as well as the most common FortiSwitch stack topologies, including those that leverage multichassis link aggregation group (MCLAG) for redundancy and higher performance. You will also learn about FortiSwitch in standalone mode, its unique features, and how to manage a standalone switch directly, or from FortiSwitch Cloud.

Product Version

- FortiGate 6.4.6
- FortiSwitch 6.4.6
- FortiAnalyzer 6.4.5
- FortiManager 6.4.5
- FortiAuthenticator 6.1.1

Course Duration

- Lecture time (estimated): 11 hours
- Lab time (estimated): 6 hours
- Total course duration (estimated): 17 hours/3 days

Who Should Attend

This course is intended for networking and security professionals involved in the management, configuration, administration, and monitoring of FortiSwitch devices used to provide secure network access to endpoints.

Certification

This course is intended to help you prepare for the NSE 6 FortiSwitch certification exam.

Prerequisites

- Basic knowledge in networking
- Understanding of layer 2 switching
- Understanding of the topics covered in the following courses:
  - *NSE 4 FortiGate Security*
  - *NSE 4 FortiGate Infrastructure*

Agenda

1. Managed Switch
2. Switch Fundamentals
3. Layer 2 Design
4. Layer 2 Security
5. Advanced Features
6. Monitoring
7. Standalone Switch
8. Troubleshooting

Objectives

After completing this course, you will be able to:

- Explore the FortiSwitch portfolio and identify the supported management modes
- Describe and deploy FortiSwitch in managed switch mode (FortiLink mode)
- Understand Ethernet switching, VLANs, link aggregation (LAG), MCLAG, and Layer 2 discovery
- Identify the most common FortiSwitch topologies when deploying FortiSwitch in managed switch mode
- Understand Spanning Tree Protocol (STP), Rapid Spanning Tree protocol (RSTP), and Multiple Spanning Tree protocol (MSTP) operation and configuration, as well as other loop protection features
- Describe and configure Layer 2 security to filter unwanted traffic and perform antispoofing
- Configure Layer 2 authentication using 802.1.X, and leverage 802.1X to assign dynamic VLANs to endpoints
- Implement advanced features to increase port density, control network access, forward multicast traffic more effectively, and quarantine compromised devices
- Prioritize traffic on FortiSwitch by using QoS marking, queuing, and rate limiting features
- Simplify endpoint deployment by using Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED)
- Share FortiSwitch ports across different VDOMs using multi-tenancy
- Monitor FortiSwitch using SNMP, sFlow, and flow sampling
- Describe the most useful troubleshooting tools available on FortiSwitch

Training Delivery Options and SKUs

Instructor-Led Training

Includes standard NSE training content delivered in person onsite, or live online using a virtual classroom application. Training is delivered within public classes or as a private class. Private requests are scoped, quoted, developed, and delivered by Fortinet Training (minimum quantities apply).

Use the following ILT Training SKU to purchase scheduled public classes of this course through Fortinet Resellers or Authorized Training Partners:

FT-FSW

Self-Paced Training

Includes online training videos and resources through the NSE Training Institute library, free of charge.

See Purchasing Process for more information about purchasing Fortinet training products.

(ISC)²

- CPE training hours: 11
- CPE lab hours: 6
- CISSP domains: Communication and Network Security

Program Policies and FAQs

For questions about courses, certification, or training products, refer to Program Policy Guidelines or Frequently Asked Questions.