FORTINET NSE Training Institute

Course Description

FortiAuthenticator

In this two-day class, you will learn how to use FortiAuthenticator for secure authentication and identity management. You will learn how to configure and deploy FortiAutheticator, use FortiAuthenticator for certificate management and two-factor authentication, authenticate users using LDAP and RADIUS servers, and explore SAML SSO and how FortiAuthenticator can act as both a SAML identity provider and service provider. Finally, you will examine some helpful troubleshooting techniques.

In interactive labs, you will explore how to authenticate users, with FortiAuthenticator acting as a RADIUS and LDAP server, a certificate authority (CA), and logon event collector that uses—and extends—the Fortinet Single Sign-On (FSSO) framework to transparently authenticate users. You will explore portal services, FortiTokens, and digital certificates.

Product Version

FortiAuthenticator 6.1

Formats

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

Agenda

1. Introduction and Initial Configuration
2. Administering and Authenticating Users
3. Two-Factor Authentication
4. Fortinet Single Sign-On
5. Portal Services
6. 802.1X Authentication
7. Certificate Management
8. SAML Configuration

Objectives

After completing this course, you will be able to:

- Deploy and configure FortiAuthenticator
- Configure the LDAP and RADIUS service
- Configure the self-service portal
- Configure FortiAuthenticator and FortiGate for two-factor authentication
- Provision FortiToken hardware and FortiToken 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 and 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

Who Should Attend

Anyone who is responsible for the day-to-day management of FortiAuthenticator.

Prerequisites

- Familiarity with all topics presented in *FortiGate Security* and *FortiGate Infrastructure*
- Understanding of authentication, authorization, and accounting

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

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

Certification

This course is part of the preparation for the NSE 6 certification exam.