FortiAuthenticator

Course Description

In this course, 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 options on FortiAuthenticator.

Product Version:
- o   FortiAuthenticator 6.4

Course Duration:
2 days

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

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

Prerequisites:
You must have an understanding of the topics covered in NSE 4 FortiGate Security and FortiGate Infrastructure or have equivalent experience. It is also recommended that you have an understanding of Authentication, Authorization, and Accounting.

Outlines:

1. Introduction and Initial Configuration
2. Administrative Users and High Availability
3. Administering and Authenticating Users
4. Managing Users and Troubleshooting Authentication
5. Two-Factor Authentication
6. FSSO Process and Methods
7. FSSO Deployment and Troubleshooting
8. Portal Services
9. PKI and FortiAuthenticator as a CA
10. Certificate Management
11. 802.1X Authentication
12. SAML
13. FIDO2 Authentication

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