

Okta Essentials

Duration: 24 Hours (3 Days)

Overview

The Okta Essentials course is designed for professionals looking to gain expertise in the Okta Identity Management solution. This course provides comprehensive Okta certification training and begins with a fundamental understanding of cloud computing before delving into what Okta is and exploring various business cases. Through hands-on lessons, learners get to set up an organization within Okta, manage users, groups, and rules, customize notifications, and navigate the Okta admin and end-client panels. As learners progress, they will explore deeper into Okta admin training, covering Security settings, Policy creation, and the Universal Directory. They will learn about User profiles, Data mapping, and integrating Okta with AD/LDAP, along with deploying Password sync and understanding Okta's Security architectures. The final module addresses the user life-cycle, Single Sign-On (SSO) strategies, multi-factor authentication (MFA), Mobile deployment, Cloud app integration, and Schema building. It concludes with a focus on Migration strategies, Change management, working with Okta APIs, and a final MCQ exam to test knowledge and understanding. This course arms learners with the skills needed to effectively manage and secure an organization's identity management with Okta.

Audience Profile

The Okta Essentials course by Koenig Solutions equips professionals with the skills to manage identity and access using Okta.

- IT Security Professionals
- System Administrators
- Network Administrators
- Identity and Access Management (IAM) Specialists
- Cloud Solutions Architects
- IT Support Staff
- DevOps Engineers
- Application Developers
- IT Managers who oversee IT security or identity management
- HR Professionals involved in onboarding and managing employee access
- Compliance Officers looking to understand identity management for auditing purposes
- Technical Consultants specializing in cloud services
- Project Managers overseeing IT projects involving secure access and identity management

Course Syllabus

Module 1 - Getting Started with OKTA

- Cloud Computing Overview
- What is OKTA? & Its Use Cases
- Lab: Getting Started with OKTA
- OKTA People
- Lab: Create and manage users in Okta
- Lab: Set administrative permissions for user accounts
- Lab: Monitor user account activities using Okta syslogs
- OKTA Admin Panel Overview

- OKTA User Dashboard Overview
- Using Browser Plugin

Module 2 - Organize Users using Groups

- Understanding Groups
- Lab: Create Groups
- Lab: Populate Group Members with Group Rules

Module 3 - Authenticate with SSO

- Select the SSO integration method for applications
- Lab: Configure Secure Web Authentication (SWA) SSO
- Lab: Configure SAML SSO

Module 4 - Manage User Lifecycle

- Identify strategies to perform provisioning operations on applications
- Lab: User Provisioning from OKTA to Application
- Lab: User provisioning from Application to OKTA

Module 5 - Manage User Profiles in Universal Directory

- Lab: Create, Transform and Map User Profile Attributes
- Lab: Manage Profile and Attribute Sourcing

Module 6 – Strengthen Security using the Okta Policy Framework

- Lab: Enforce OKTA Service-Level Security
- Lab: Set Up MFA Enrollment
- Lab: Set up security policies to satisfy the assurance requirements
- Configure self-service password recovery

Module 7 – Set Up Passwordless Authentication using Okta FastPass

- Lab: Implement Passwordless Authentication using Okta FastPass
- Manage device state

Module 8 – Explore Additional Tools

- Lab: Describe the customizable components and settings of Okta orgs
- List tools and utilities for Troubleshooting
- Work with Okta Support
- Lab: Sending Notifications
- Notification Customization

Module 9 – OKTA Migration

- OKTA Migration Approach
- Lab: Working With OKTA API