AMBIENT-IT

+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated 04/23/2024

Sign up

Okta Training

3 days (21 hours)

Presentation

Our Okta training course will immerse you in the world of identity and access management, equipping you with the knowledge and skills you need to master this cutting-edge platform.

This training program exhaustively covers the essential aspects of Okta, from fundamental concepts to advanced techniques for securing cloud and on-premises resources.

You'll explore Okta's key features, such as single sign-on (SSO), identity management, application security and much more, as you familiarize yourself with the most common use cases in different industrial contexts.

With our training, you'll learn how to configure and deploy advanced security strategies to protect sensitive data, and how to effectively integrate Okta into your existing IT infrastructure.

As with all our training courses, this Okta course will present the latest version and resources of the tool.

Objectives

- Understanding Okta's position in the IAM market
- Installing and configuring Okta and Okta AD Agent
- Create, modify and delete users in Okta, and manage user groups
- Configure Single Sign-On (SSO) and integrate on-premise and cloud applications
- Configure security policies in Okta, including Multi-Factor Authentication (MFA)

Target audience

- System administrators
- IT security managers
- Application developers
- IT architects

Prerequisites

- Basic knowledge of IT and systems security is recommended
- Familiarity with authentication and identity management concepts would be an advantage
- Basic system administration and networking skills are beneficial

Okta Training Program

INTRODUCTION TO OKTA

- Understanding Okta's position in the Identity and Access Management (IAM) market
- Identify Okta's main features and benefits
- Discover the key components of the Okta platform
- Explore Okta's user interface and basic functions
- Defining Okta's fundamental terms and concepts

PREPARING AND CONFIGURING OKTA

- Installing and configuring Okta and Okta AD Agent
- Understand best practices for deploying Okta in an enterprise environment
- Configure initial security settings and organization preferences
- Establish a connection between Okta and corporate directories (Active Directory/LDAP)
- Customizing the interface and user experience

USER AND GROUP MANAGEMENT

- Create, modify and delete users in Okta
- Assign permissions and manage user roles
- Configure and manage user groups and membership rules
- Synchronize users and groups with external directories
- Using reports and audits

PROVISIONING AND SINGLE SIGN-ON (SSO)

- Understand the automatic user account provisioning process
- Configuring Single Sign-On
- Manage the identity lifecycle in Okta.

- Integrate SSO with on-premise and cloud applications
- Establish dynamic provisioning policies

APPLICATION INTEGRATION WITH OKTA

- Use Okta's integration wizard to connect applications
- Configuring Secure Web Authentication (SWA)
- Explore the Okta application catalog and the Okta Integration Network (OIN)
- Integrating custom applications with Okta
- Manage application attributes and mappings

WORKFLOW AND ACCESS MANAGEMENT

- Configure access request workflows and approvals
- Automate access granting and revocation processes
- Using access rules
- Manage pending access requests and access revisions
- Perform compliance audits and access certifications

PERSONALIZATION

- Modifying and enhancing user profiles in Okta
- Add and manage custom attributes
- Configure profile schemas and attribute mappings
- Use the universal directory to unify identity management
- Personalize user experience through Okta profiles

SECURITY POLICIES IN OKTA

- Understanding the different security policies available in Okta
- Configure authentication and password policies
- Set up session and network policies
- Configure Multi-Factor Authentication (MFA) and adaptive policies
- Test and simulate security policies

IDENTITY FEDERATION AND AUTHENTICATION PROTOCOLS

- Understand the principles and benefits of identity federation
- Become familiar with the SAML 2.0, OpenID Connect and OAuth protocols
- Configuring application federation using SAML 2.0
- Implementing OpenID Connect for modern applications
- Practical work on implementing OIDC flows and managing tokens

Companies concerned

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.