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

Updated 06/17/2025

Sign up

Authentik training

4 days (28 hours)

Presentation

Our Authentik training course will enable you to discover and master this open-source identity and access management solution. You'll learn how to centralize authentication, strengthen connection security, and precisely control access authorizations to your applications and services.

You'll start with the key concepts: user management, roles, access policies, and the principles of modern authentication. You will then be guided through the installation and configuration of Authentik, whether for a test or production environment.

You'll learn how to create personalized access portals, activate multi-factor authentication, and build customized authentication paths using dynamic flows. Each step will give you a concrete and progressive mastery of the platform.

You'll also be able to connect your internal applications, secure their access via reverse proxy, and integrate granular security rules based on users or contexts.

As with all our training courses, this one will be presented with the latest version of Authentik.

Objectives

- Understand the fundamentals of identity and access management in a centralized environment
- Install, configure and administer Authentik in a secure production environment
- Create and organize users, groups and roles to structure access rights
- Design personalized authentication paths using dynamic flows

- Implement multi-factor authentication (MFA) and define granular security policies
- Integrate internal applications via standardized connectors and secure access with the reverse proxy
- Automate account and access management with REST API and integration mechanisms
- Apply best practices for IdP operation, supervision and governance
  modern open-source

Target audience

- Fullstack developer
- Back-end developer
- System administrators

Prerequisites

- Have a basic understanding of how a Linux system works
- Network and security skills
- Know how to use Docker or have some experience with containers

Authentik Training Program

Introduction to identity and Authentik

- Differences between authentication, authorization and identity
- Protocols: OIDC, SAML, LDAP
- How an Identity Provider (IdP) works
- Comparison with Keycloak, Okta, Entra ID

Installing and configuring Authentik

- System requirements (Docker, PostgreSQL, NGINX/Traefik...)
- DNS configuration, SSL certificates, etc.
- Installation via Docker Compose
- Installation via Helm Chart (Kubernetes)
- Initial setup via web interface
- Environment variables
- Secrets, persistent volumes, backups
- Securing the admin interface

User creation and management

- Administration interface

- Custom attributes
- Manual or automatic import

Groups and permissions

- Creating groups
- Assigning roles and policies
- Rule inheritance and prioritization

External directory integration

- LDAP / Active Directory synchronization
- External OAuth connection (Google, GitHub, Azure AD)

Security and strong authentication

- MFA activation: TOTP, WebAuthn, SMS, EmailMFA application by group or policy
- User device management
- Creating customized flows
- Available steps: password, consent, CAPTCHA, etc.
- Conditional branches and logical expressions

Application integration

- Add an OIDC Provider (e.g. GitLab, Grafana, Nextcloud...)
- Scopes and claims configuration
- Redirections and security
- SAML Provider creation
- SP / IdP metadata
- SSO with compatible business or SaaS tools
- Outpost mode (reverse proxy with authentication)
- Outpost deployment on an existing web service
- Upstream access control via policies

Automation, APIs and DevOps

- Authentication via API token
- Frequent calls: users, flows, providers
- Automation with Python, curl or Postman scripts
- Deployment with Terraform (via unofficial or generic provider)
- Saving/restoring configurations
- CI/CD for flows or providers
- Integration with Prometheus / Grafana
- Log centralization via Loki, Graylog or ELK
- Authentication monitoring and alerting

User portal

- Customizing the login portal
- Add logo, text, instructions
- Using custom CSS themes

Introduction to hybrid identity

- Configuration of email templates (registration, MFA, reset...)
- Dynamic variables in messages
- Translations (i18n)

Setting up a complete SSO

- Deploying Authentik + Nextcloud + GitLab + Gitea
- Centralized user management and MFA

Integration with Azure AD as Identity Provider

- Authentik as a Relying Party
- AD group synchronization

Secure Kubernetes deployment

- Authentik in a private cluster
- Secure access to internal dashboards (Grafana, ArgoCD...)

Global security

- Separation of admin vs. user access
- MFA mandatory for admin
- Secret rotation

Large-scale access management

- Automatic provisioning
- Access expiry
- Critical action logging

Backup, updates and recovery

- Backup/restore strategies

- Secure update (rolling update, HA)
- Internal documentation for future integration

Companies concerned

This 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.