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

Mis à jour le 17/06/2025

S'inscrire

Formation Authentik

4 jours (28 heures)

Présentation

Notre formation Authentik vous permettra de découvrir et maîtriser cette solution open-source de gestion des identités et des accès. Vous apprendrez à centraliser l'authentification, renforcer la sécurité des connexions, et contrôler précisément les autorisations d'accès à vos applications et services.

Vous débuterez par les concepts clés : gestion des utilisateurs, rôles, politiques d'accès, et principes de l'authentification moderne. Vous serez ensuite guidé dans l'installation et la configuration d'Authentik, que ce soit pour un environnement de test ou de production.

Vous apprendrez à créer des portails d'accès personnalisés, à activer l'authentification multifacteur, et à construire des parcours d'authentification adaptés grâce aux flows dynamiques. Chaque étape vous donnera une maîtrise concrète et progressive de la plateforme.

Vous saurez également connecter vos applications internes, sécuriser leur accès via proxy inverse, et intégrer des règles de sécurité granulaires en fonction des utilisateurs ou des contextes.

Comme pour toutes nos formations, celle-ci vous sera présentée avec la toute dernière version de Authentik.

Objectifs

- Comprendre les fondamentaux de la gestion des identités et des accès dans un environnement centralisé
- Installer, configurer et administrer Authentik dans un contexte de production sécurisé
- Créer et organiser les utilisateurs, groupes et rôles pour structurer les droits d'accès
- Concevoir des parcours d'authentification personnalisés à l'aide des flows dynamiques

- Mettre en place une authentification multifacteur (MFA) et définir des politiques de sécurité granulaires
- Intégrer des applications internes via des connecteurs standardisés et sécuriser l’accès avec le proxy inverse
- Automatiser la gestion des comptes et des accès grâce à l’API REST et aux mécanismes d’intégration
- Appliquer les bonnes pratiques d’exploitation, de supervision et de gouvernance autour d’un IdP open-source moderne

Public visé

- Développeur fullstack
- Développeur Back-end
- Administrateurs systèmes

Pré-requis

- Avoir les bases du fonctionnement d’un système Linux
- Avoir des notions en réseau et sécurité
- Savoir utiliser Docker ou avoir une première expérience avec des conteneurs

Programme de notre Formation Authentik

Introduction à l’identité et à Authentik

- Différences entre authentification, autorisation et identité
- Protocoles : OIDC, SAML, LDAP
- Fonctionnement d’un Identity Provider (IdP)
- Comparaison avec Keycloak, Okta, Entra ID

Installation et configuration d’Authentik

- Prérequis systèmes (Docker, PostgreSQL, NGINX/Traefik…)
- Configuration des DNS, certificats SSL, etc.
- Installation via Docker Compose
- Installation via Helm Chart (Kubernetes)
- Paramétrage initial via l’interface web
- Variables d’environnement
- Secrets, volumes persistants, sauvegardes
- Sécurisation de l’interface admin

Création et gestion des utilisateurs

- Interface d’administration

- Attributs personnalisés
- Import manuel ou automatique

Groupes et permissions

- Création de groupes
- Attribution de rôles et policies
- Héritage et priorisation des règles

Intégration d’annuaires externes

- Synchronisation LDAP / Active Directory
- Connexion OAuth externe (Google, GitHub, Azure AD)

Sécurité et authentification forte

- Activation du MFA : TOTP, WebAuthn, SMS, EmailApplication du MFA par groupe ou politique
- Gestion des appareils utilisateurs
- Création de flows personnalisés
- Étapes disponibles : mot de passe, consentement, CAPTCHA, etc.
- Branches conditionnelles et expressions logiques

Intégration avec des applications

- Ajouter un Provider OIDC (ex : GitLab, Grafana, Nextcloud…)
- Configuration des scopes et claims
- Redirections et sécurité
- Création de Provider SAML
- Métadonnées SP / IdP
- SSO avec outils métiers ou SaaS compatibles
- Mode "Outpost" (reverse proxy avec authentification)
- Déploiement Outpost sur un service web existant
- Contrôle d’accès en amont via policies

Automatisation, API et DevOps

- Authentification via token API
- Appels fréquents : utilisateurs, flows, providers
- Automatisation avec scripts Python, curl ou Postman
- Déploiement avec Terraform (via provider non-officiel ou générique)
- Sauvegarde/restauration des configurations
- CI/CD pour les flows ou providers
- Intégration avec Prometheus / Grafana
- Centralisation des logs via Loki, Graylog ou ELK
- Surveillance des authentifications et alerting

Portail utilisateur

- Personnalisation du portail de connexion
- Ajout de logo, textes, instructions
- Utilisation de thèmes CSS personnalisés

Introduction à l'identité hybride

- Configuration des modèles d’emails (inscription, MFA, réinitialisation…)
- Variables dynamiques dans les messages
- Traductions (i18n)

Mise en place d’un SSO complet

- Déploiement d’Authentik + Nextcloud + GitLab + Gitea
- Gestion centralisée des utilisateurs et MFA

Intégration avec Azure AD comme Identity Provider

- Authentik en tant que Relying Party
- Synchro des groupes AD

Déploiement Kubernetes sécurisé

- Authentik dans un cluster privé
- Accès sécurisé aux dashboards internes (Grafana, ArgoCD…)

Sécurisation globale

- Séparation des accès admin vs users
- MFA obligatoire pour l’admin
- Rotation des secrets

Gestion des accès à grande échelle

- Provisioning automatique
- Expiration d’accès
- Journalisation des actions critiques

Sauvegarde, mises à jour et reprise

- Stratégies de backup/restauration

- Mise à jour sécurisée (rolling update, HA)
- Documentation interneos d'intégration future

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.