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

Updated on 03/23/2026

Sign up

SailPoint Identity Security Professional Certification Training

3 days (21 hours)

Overview

The SailPoint Identity Security Professional certification validates your ability to design, configure, and operate an IGA platform to automate the identity lifecycle, strengthen compliance, and reduce access risks. It is based on real-world use cases: onboarding/offboarding, access requests, recertifications, and role control.

This training aims to make you proficient in SailPoint fundamentals: identity modeling, access governance, workflows, and integrations. You will learn to translate business requirements (separation of duties, policies, audits) into robust and maintainable configurations.

The approach is resolutely hands-on, featuring guided workshops, demonstrations, and diagnostic exercises. Course deliverables include an exam preparation checklist, configuration scenarios, and best practices for securing and standardizing your deployments.

Objectives

- Identify the key components of the SailPoint architecture and their roles.
- Configure core objects: identities, sources, attributes, and correlations.
- Set up access requests, approvals, and workflows.
- Manage roles, policies, and compliance controls (SoD, recertifications).
- Analyze incidents, logs, and errors to ensure reliable operations.

Target Audience

- IAM/IGA engineers and security consultants
- SailPoint administrators and operations teams
- Security architects / access governance managers

Prerequisites

- Solid understanding of IAM: provisioning, authentication, authorizations
- Understanding of directories (AD/LDAP) and identities
- Basic knowledge of RBAC, SoD, and auditing
- Log analysis and application troubleshooting

Technical prerequisites

- PC with at least 8 GB of RAM (16 GB recommended)
- Windows 10/11, macOS, or Linux with a modern browser
- Access to a SailPoint training environment and administrative privileges
- Text editor and terminal (PowerShell, Bash, or equivalent)

SailPoint Identity Security Professional Credential Certification Training Program

[Day 1 - Morning]

IAM Fundamentals and SailPoint Identity Security Overview

- IAM/IGA review: identity, accounts, roles, permissions, separation of duties
- SailPoint Overview: IdentityNow, IdentityIQ, use cases, and scope of the certification
- Key concepts: sources, aggregation, correlation, entitlements, access profiles
- Governance model: policies, approvals, audit, traceability
- Hands-on workshop: Mapping a target IT environment (sources, populations, applications) and defining expected IGA objects.

[Day 1 - Afternoon]

Identity modeling and lifecycle (Joiner/Mover/Leaver)

- Identity model: attributes, identifiers, correlation rules, and data quality
- Lifecycle: HR events, provisioning/deprovisioning, exception management
- Role-based access vs. profile-based access: selection criteria and operational impacts
- Design best practices: naming, normalization, testing strategy, and rollback
- Hands-on workshop: Defining a complete JML scenario and associated controls (creation, mobility, departure).

[Day 2 - Morning]

Onboarding sources and access governance

- Source types: HR, AD, applications, files; connector selection and prerequisites
- Aggregation: planning, delta management, error handling, and reconciliation
- Authorization modeling: entitlements, groups, permissions, hierarchies
- Building governance objects: Access Profiles, Roles, eligibility rules
- Hands-on workshop: Design an access model (entitlements? access profiles? roles) for a typical application.

[Day 2 - Afternoon]

Access requests, approval workflows, and policies

- Access Request: catalog, eligibility criteria, justification, and traceability
- Workflows: approvals (manager, owner, security), escalations, delegations
- Policies: SoD, high-risk access, preventive vs. detective controls
- User experience: notifications, SLAs, best practices for configuration
- Hands-on workshop: Defining an approval workflow and a SoD policy for a “finance” scenario.

[Day 3 - Morning]

Access Reviews and Compliance

- Types of reviews: manager, owner, application, entitlements; scope and frequency
- Campaigns: targeting, sampling, risk-based prioritization, delegation
- Decisions: approve/revoke, comments, evidence, and exception handling
- Remediation: triggering provisioning, campaign tracking and closure
- Hands-on workshop: Build a review campaign and define the expected remediation rules.

[Day 3 - Afternoon]

Reporting, exam preparation, and role-playing

- Key metrics: source coverage, identity quality, approval times, revocation rates
- Audit & evidence: typical requirements (SOX/ISO), exporting and traceability of decisions
- Review of certification concepts: terminology, common pitfalls, typical scenarios
- Exam strategy: time management, reading questions, eliminating distractors
- Hands-on workshop: Mock exam (scenario-based questions) and guided review with a revision action plan.

Target companies

This training is designed for both individuals and businesses, large and small,

wishing to train their teams in new advanced IT technology or to acquire specific professional knowledge or modern methods.

Placement at the start of the training

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency in various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

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

Organization

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

Assessment

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been properly acquired.

Certification

A certificate will be issued to each trainee who has completed the entire training program.

Training organization registered under number 11 75 54743 75. This registration does not constitute state accreditation.
© Ambient IT 2015-2026. All rights reserved. Paris, France - Switzerland - Belgium - Luxembourg