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

Updated on 03/19/2026

Sign up

SailPoint Identity Security Expert Certification Training

3 days (21 hours)

Overview

The SailPoint Identity Security Expert Credential validates your ability to design, configure, and operate an identity security-focused IGA solution. You will learn how to address real-world use cases: join/move/leave, access requests, recertifications, and risk mitigation.

This training prepares you for the exam by covering key concepts (governance, roles, policies, connectors) and their implementation in SailPoint. The goal is to translate business and compliance requirements into measurable technical controls.

The approach is resolutely practical: guided demos, configuration workshops, analysis of common errors, and operational scenarios. You'll leave with preparation checklists, configuration templates, and a methodology for diagnosing integration and governance issues.

Objectives

- Configure the essential components of an IGA-focused SailPoint platform.
- Set up access request and approval workflows.
- Define roles, policies, and compliance rules (SoD, exceptions).
- Orchestrate the identity lifecycle (JML) and provisioning.
- Analyze logs, campaigns, and reports to reduce risk and improve auditability.

Target Audience

- IAM / IGA Engineers
- SailPoint administrators
- Security and governance consultants
- Identity architects

Prerequisites

- Solid understanding of IAM (authentication, authorization, RBAC/ABAC).
- Understanding of directories and repositories (AD, LDAP, HR).
- Basic knowledge of SQL and log analysis.
- Basic knowledge of compliance/auditing (recertification, SoD).

Technical Requirements

- PC with at least 8 GB of RAM (16 GB recommended) and a recent CPU.
- Windows 10/11, macOS, or Linux with a modern browser.
- Access to a SailPoint training environment and stable network connectivity.
- Text editor, terminal

SailPoint Identity Security Expert Credential Certification Training Program

[Day 1 - Morning]

IAM Fundamentals and the SailPoint Identity Security Scope

- IAM/IGA Review: Identity, Accounts, Permissions, Roles, Segregation of Duties
- SailPoint positioning: Identity Security Cloud, use cases, and benefits
- Key Concepts: Sources, Entitlements, Access Profiles, Roles
- Review of certification requirements: domains, question types, study strategy
- Hands-on workshop: Mapping a target IT system (sources, applications, permissions) and the associated IGA model

[Day 1 - Afternoon]

Onboarding sources and modeling access

- Onboarding a source: connectivity, attribute schemas, identity correlation
- Modeling rights: entitlements and grouping into access profiles
- Best practices for naming, descriptions, owners, and object governance
- Quality checks: duplicates, orphaned rights, missing attributes, data consistency
- Hands-on workshop: Create a demo source and build two access profiles aligned with a business need

[Day 2 - Morning]

Lifecycle management (Joiner/Mover/Leaver) and provisioning

- JML events: triggers, HR attributes, assignment rules, and exceptions
- Provisioning: requests, approvals, execution, error tracking, and follow-ups
- Account management: creation, update, deactivation, deletion, reconciliation
- Traceability: logs, reports, evidence, and audit best practices
- Hands-on workshop: Configure a JML scenario (hiring + departure) and validate expected actions

[Day 2 - Afternoon]

Workflows, policies, and governance of access requests

- Approval chains: managers, owners, conditional approvals, and escalations
- Policies: compliance controls, SoD rules, conflict detection
- Exception management: compensations, justifications, durations, and periodic reviews
- User experience: catalog, search, recommendations, and request streamlining
- Hands-on workshop: Designing a request workflow with SoD and a controlled exception

[Day 3 - Morning]

Roles, advanced access modeling, and architectural best practices

- Role mining strategies and iterative approach (MVP, hardening, adoption)
- Role design: business vs. technical, hierarchies, inheritance, and maintenance
- Role/Access Profile Alignment: Granularity, Reusability, and Governance
- Architecture: Environments, Separation of Responsibilities, Change Management
- Hands-on workshop: Defining a role model (3 roles) and linking it to existing access profiles

[Day 3 - Afternoon]

Certification readiness: access reviews, reporting, and exam preparation

- Access review campaigns: scope, sampling, delegations, decisions, and evidence
- Reporting & audit: metrics, exports, key controls, and areas of concern
- Case resolution: correlation errors, persistent rights, discrepancies between source and IGA
- Targeted review: sample questions, common pitfalls, time management, and final checklist
- Hands-on workshop: Conduct a mini access review campaign and produce the expected evidence

Target Audience

This training is intended for both individuals and companies, large or small, seeking to train their teams in new advanced IT technologies or to acquire specific business knowledge or modern methods.

Entry-level assessment

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 with 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 Training: 60% practical, 40% theoretical. Training materials will be distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the instructor, 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.