+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 Certified Identity Security Engineer Training

3 days (21 hours)

Overview

The SailPoint Certified Identity Security Engineer certification validates your ability to design and operate an Identity Security platform to automate the identity lifecycle, strengthen compliance, and reduce risk. It is intended for teams that need to standardize provisioning, access reviews, and governance in hybrid environments.

This training prepares you to implement SailPoint's key features: identity modeling, application integrations, access policies, workflows, and audit controls. The approach focuses on real-world use cases (hires/terminations, internal mobility, privileged access, remediation).

You will alternate between guided workshops, demos, and configuration exercises. Deliverables: a reference environment, configuration templates (roles, rules, connectors), test scenarios, and an exam preparation checklist.

Objectives

- Configure the identity model and governance attributes
- Integrate applications via connectors and provisioning flows
- Define roles, policies, and task separation rules
- Set up certification and remediation campaigns
- Diagnose incidents, logs, and runtime errors

Target Audience

- IAM / Identity Security Engineers
- SailPoint administrators / RUN teams
- Security architects and access governance managers
- Integration consultants and technical project managers

Prerequisites

- Solid understanding of IAM (RBAC, provisioning, SSO)
- Understanding of LDAP/AD and application accounts
- Knowledge of REST APIs and JSON formats
- Basic security knowledge: least privilege, auditing, compliance

Technical requirements

- 16 GB of RAM recommended (8 GB minimum)
- Windows 11, macOS, or Linux with stable network access
- Modern browser (Chrome/Firefox) and code editor
- Terminal, API client (Postman or equivalent), access to a provided SailPoint tenant/lab

SailPoint Certified Identity Security Engineer Training Program

[Day 1 - Morning]

SailPoint Identity Security Cloud architecture and IGA fundamentals

- Positioning IGA: Joiner/Mover/Leaver, governance, compliance, and risk reduction
- Understanding key components: Identity Profiles, Sources, Entitlements, Access Profiles
- Modeling an Identity: Attributes, Correlation, Aggregation, and Lifecycle
- Identifying Roles and Responsibilities: Admin, Application Owner, Manager, Auditor
- Hands-on Workshop: Getting Started with the Tenant and Identifying Objects (Identities, Sources, Access).

[Day 1 - Afternoon]

Onboarding sources and modeling access

- Configuring a Source: settings, connectivity, schema, and correlation rules
- Run an aggregation and analyze the results (accounts, entitlements, anomalies)
- Building Access Profiles (entitlements, descriptions, owners, risks)
- Establishing governance: owners, reviews, separation of responsibilities
- Hands-on workshop: Onboard a source (sandbox) and create two on-demand access profiles.

[Day 2 - Morning]

Access requests and approval workflows

- Configure the Access Request: catalog, visibility, prerequisites, and eligibility rules
- Defining approval workflows: manager, owner, multiple approvals
- Manage constraints: justification, duration, temporary access, and renewal
- Monitoring Execution: Statuses, Errors, Reminders, and Traceability
- Hands-on workshop: Create a request workflow with dual approval and time-limited access.

[Day 2 - Afternoon]

Provisioning, deprovisioning, and event management

- Understanding provisioning: creating, updating, deleting, and deactivating accounts
- Configuring behaviors: attribute mapping, rules, and error handling
- Automating the Leaver process: revoking access, deactivating, and deleting accounts according to policies
- Managing exceptions: orphaned accounts, unprovisionable access, remediation
- Hands-on workshop: Simulate an employee departure and validate full deprovisioning (accounts + entitlements).

[Day 3 - Morning]

Access certifications, compliance, and auditing

- Implementing Access Reviews: campaigns, scopes, user groups, and frequencies
- Configure decisions: retain, revoke, delegate, request justification
- Optimize the reviewer experience: prioritization, recommendations, mandatory comments
- Leveraging evidence: history, traceability, and export for audit
- Hands-on workshop: Launch a certification campaign and process a batch of decisions with remediation.

[Day 3 - Afternoon]

Certification preparation: scenarios, troubleshooting, and best practices

- Review key topics: sources, access profiles, requests, provisioning, certifications
- Diagnosing common issues: correlation, aggregation, missing permissions, provisioning failures
- Applying best practices: naming, ownership, documentation, separation of duties
- Develop a deployment plan: environments, testing, production rollout, and operation
- Hands-on workshop: End-to-end case study (onboarding? request? provisioning? certification) with exam checklist.

Target Audience

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

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

Assessment upon enrollment

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.