AMBIENT-IT

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

Updated on 03/20/2026

Sign up

SailPoint Identity Security Administrator Certification Training

3 days (21 hours)

Overview

The SailPoint Certified Identity Security Administrator certification validates your ability to administer an IGA platform and secure the identity lifecycle. It is designed for teams that need to standardize provisioning, access reviews, and compliance.

This training provides hands-on preparation for the skills expected of a SailPoint administrator: connector configuration, identity modeling, access policies, and governance. The goal is to learn how to diagnose and correct rights discrepancies while ensuring traceability and auditability.

The approach is practice-oriented: guided workshops, configuration demos, use cases (onboarding/offboarding, recertification, exceptions), and validation exercises. You'll leave with administration checklists, troubleshooting scenarios, and a study plan aligned with the exam.

Objectives

- Configure the SailPoint environment and essential administration settings.
- Integrate identity sources and applications via connectors.
- Implement provisioning and lifecycle workflows.
- Administer access policies, roles, and segregation of duties controls.
- Leverage attestation campaigns, reports, and audit logs.

Target Audience

- IAM/IGA Administrators
- Security Engineers / Identity Security
- SailPoint consultants
- Operators and N2/N3 support teams

Prerequisites

- Solid understanding of IAM (RBAC, provisioning, SSO)
- Knowledge of Active Directory and accounts/attributes
- Basic knowledge of LDAP, groups, and application permissions
- Understanding of audit and compliance issues

Technical prerequisites

- PC with at least 8 GB of RAM (16 GB recommended)
- Windows 10/11, macOS, or Linux
- Modern browser (Chrome/Firefox/Edge) and internet access
- Text editor and terminal (PowerShell/Bash)

Course Outline for the SailPoint Certified Identity Security Administrator Certification

[Day 1 - Morning]

IAM Fundamentals and Introduction to SailPoint Identity Security Cloud

- IAM review: identities, accounts, permissions, roles, separation of duties (SoD)
- SailPoint Overview: Identity Security Cloud, IdentityNow, Key Modules
- Console navigation: tenants, menus, key objects (Identity, Source, Entitlement)
- Integration prerequisites: technical accounts, APIs, connectivity, security best practices
- Hands-on workshop: Logging into the tenant, guided exploration, and identifying key objects.

[Day 1 - Afternoon]

Sources, connectors, and aggregation: onboarding an application

- Creating a Source: connector selection, settings, authentication, and encryption
- Schema and correlation: accounts, identities, attributes, matching rules
- Entitlements: collection, hierarchies, descriptions, owners, and criticality
- Aggregation cycles: scheduling, delta vs. full, error handling, and logs
- Hands-on workshop: Onboard a demo source and run a full aggregation.

[Day 2 - Morning]

Access governance: access profiles, roles, and policies

- Modeling access: entitlements vs. access profiles vs. roles
- Building Access Profiles: bundles, attributes, owners, lifecycle, and versioning
- Business and IT roles: assignment criteria, rules, exceptions, and inheritance
- Compliance policies: SoD, sensitive access, alerts, and remediation actions
- Hands-on workshop: Create an access profile and a role, then test the assignment on identities.

[Day 2 - Afternoon]

Access Request Workflows and Approvals

- Access Requests: catalog, items, constraints, justification, and visibility
- Approval chains: managers, owners, multi-level approvals, and escalations
- Provisioning: Triggering, connector, execution tracking, and error recovery
- Notifications and traceability: events, audit, evidence, and operational reporting
- Hands-on workshop: Publish an item to the catalog, submit a request, and validate provisioning.

[Day 3 - Morning]

Lifecycle and identity: join/move/leave and continuous governance

- Identity Profiles: authority sources, attributes, correlation rules, and transformations
- Lifecycle States: triggers, transitions, dates, deactivation, and reactivation
- JML Automation: Events, Actions, Provisioning/Deprovisioning, and Controls
- Orphaned Access and Shared Account Management: Detection, Ownership, and Remediation
- Hands-on workshop: Simulate a mover/leaver and verify access and account changes.

[Day 3 - Afternoon]

Access certification, audit, and exam preparation

- Access Certifications: campaigns, scopes, reviewers, decisions, and comments
- Remediation: revocation, follow-up, exceptions, reminders, and campaign closure
- Audit & Reporting: Logs, Exports, Metrics, and Proof of Compliance
- Review of exam topics: common pitfalls, best practices for administration, and troubleshooting
- Hands-on workshop: Launching a certification campaign, handling decisions, and generating 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 industry knowledge or modern methodologies.

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 in various types of technologies, as well as their expectations and personal goals regarding 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 instruction from the instructor—supported by examples and discussion 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