

# **SailPoint Identity Security Architect**

## *COURSE CONTENT*

### **GET IN TOUCH**



Multisoft Systems  
B - 125, Sector - 2, Noida



(+91) 9810-306-956



[info@multosoftsystems.com](mailto:info@multosoftsystems.com)



[www.multosoftsystems.com](http://www.multosoftsystems.com)

## About Multisoft

Train yourself with the best and develop valuable in-demand skills with Multisoft Systems. A leading certification training provider, Multisoft collaborates with leading technologies to bring world-class one-on-one and certification training. Intending to empower professionals and businesses across the globe, we offer more than 1500 training courses, which are delivered by Multisoft's global subject matter experts. We offer tailored corporate training, a comprehensive learning solution with lifetime e-learning access, after-training support and globally recognized training certificates.

## About Course

SailPoint Identity Security Architect Training is an advanced learning program focused on the architectural planning and governance of enterprise identity security environments using SailPoint Identity Security Cloud (ISC). The course covers identity lifecycle architecture, source and application integrations, identity profiles, access models, provisioning, access requests, certifications, roles, APIs, security controls, compliance, and scalability considerations. Through architecture-focused scenarios and practical exercises, participants learn how to evaluate organizational requirements, select suitable identity strategies, structure secure access frameworks, and support scalable SailPoint solutions across complex enterprise environments.

## Module 1: SailPoint Identity Security & Architecture Fundamentals

- ✓ Enterprise Identity and Access Management landscape
- ✓ Identity Security and Identity Governance concepts
- ✓ SailPoint capabilities within an enterprise IAM ecosystem
- ✓ Understanding architect, engineer, and administrator responsibilities
- ✓ Identity security architecture principles
- ✓ Business, security, compliance, and technical requirements
- ✓ Functional versus non-functional requirements
- ✓ Understanding common enterprise identity challenges
- ✓ Architectural viewpoints and solution boundaries
- ✓ Identity security architecture lifecycle
- ✓ Introduction to architectural documentation and design decisions

## Module 2: Identity Security Architecture and Core Components

- ✓ Understanding the SailPoint architectural landscape
- ✓ Major functional and architectural components
- ✓ Identity, account, entitlement, access profile, and role relationships
- ✓ Sources and connected enterprise systems
- ✓ Identity governance services and processes
- ✓ Provisioning and access fulfillment architecture
- ✓ Certification and access review components
- ✓ Policy and risk control considerations
- ✓ Cloud, SaaS, on-premises, and hybrid application landscapes

- ✓ Architectural dependencies between identity services
- ✓ Mapping enterprise IAM requirements to SailPoint capabilities
- ✓ Reference architecture considerations

## Module 3: Enterprise Identity Data Model & Identity Lifecycle Architecture

- ✓ Identity data architecture fundamentals
- ✓ Identifying authoritative identity sources
- ✓ Designing identity attributes
- ✓ Attribute mapping and transformation considerations
- ✓ Identity profile architecture
- ✓ Identity creation and aggregation considerations
- ✓ Identity correlation strategy
- ✓ Account-to-identity relationships
- ✓ Handling multiple authoritative sources
- ✓ Identity lifecycle states
- ✓ Joiner, mover, and leaver architecture
- ✓ Employee, contractor, partner, and external identity considerations
- ✓ Rehire and returning-user scenarios
- ✓ Managing identity changes across connected applications
- ✓ Data quality and identity consistency
- ✓ Identity lifecycle exception handling

## Module 4: Source Integration & Connectivity Architecture

- ✓ Enterprise application integration landscape
- ✓ Source architecture and connector selection
- ✓ Authoritative and non-authoritative sources
- ✓ Connectivity patterns for enterprise applications
- ✓ SaaS application integration considerations
- ✓ Database and directory integration scenarios
- ✓ REST and API-based connectivity
- ✓ File-based integration patterns
- ✓ Integration with legacy applications
- ✓ Account and entitlement aggregation architecture
- ✓ Provisioning-capable versus read-only integrations
- ✓ Authentication and credential considerations
- ✓ Network and connectivity dependencies
- ✓ Integration error handling
- ✓ Connector performance considerations
- ✓ Integration security requirements
- ✓ Planning reusable integration patterns
- ✓ Handling disconnected and difficult-to-integrate applications

## Module 5: Identity Profiles, Correlation & Account Management Design

- ✓ Designing identity profiles
- ✓ Attribute selection and normalization
- ✓ Identity attribute transformation strategy

- ✓ Account correlation architecture
- ✓ Correlation rules and matching considerations
- ✓ Preventing duplicate identity associations
- ✓ Managing multiple accounts for a single identity
- ✓ Service and shared account considerations
- ✓ Orphan account management
- ✓ Account ownership models
- ✓ Account lifecycle architecture
- ✓ Account creation and disabling strategies
- ✓ Identity and account synchronization
- ✓ Handling incomplete or inconsistent source data
- ✓ Exception scenarios and remediation approaches

## Module 6: Access Model & Entitlement Architecture

- ✓ Enterprise access modeling principles
- ✓ Understanding accounts and entitlements
- ✓ Entitlement classification and organization
- ✓ Designing access profiles
- ✓ Access profile composition
- ✓ Role architecture fundamentals
- ✓ Business and technical role considerations
- ✓ Birthright access design
- ✓ Requestable versus automatically assigned access
- ✓ Access inheritance considerations
- ✓ Role hierarchy and access relationships
- ✓ Avoiding excessive role complexity

- ✓ Least-privilege architecture
- ✓ Access ownership and accountability
- ✓ Access model governance
- ✓ Access model lifecycle and maintenance
- ✓ Designing access structures for scalability

## Module 7: Lifecycle Management & Provisioning Architecture

- ✓ Identity lifecycle management architecture
- ✓ Joiner provisioning strategy
- ✓ Mover and organizational change scenarios
- ✓ Leaver and termination architecture
- ✓ Immediate versus scheduled deprovisioning
- ✓ Provisioning workflow considerations
- ✓ Account creation architecture
- ✓ Entitlement assignment and removal
- ✓ Automated access changes
- ✓ Birthright access provisioning
- ✓ Provisioning to heterogeneous systems
- ✓ Handling manual fulfillment requirements
- ✓ Provisioning failures and retry strategy
- ✓ Exception and escalation processes
- ✓ Lifecycle event sequencing
- ✓ Preventing orphaned access
- ✓ Designing lifecycle processes for large enterprises

- ✓ Auditing lifecycle activities

## Module 8: Access Request & Approval Architecture

- ✓ Access request architecture
- ✓ Designing the request experience
- ✓ Requestable access models
- ✓ Access catalog considerations
- ✓ Access request eligibility
- ✓ Approval workflow architecture
- ✓ Manager approval patterns
- ✓ Application and entitlement owner approvals
- ✓ Multi-level approval scenarios
- ✓ Risk-aware approval considerations
- ✓ Request validation
- ✓ Provisioning and fulfillment integration
- ✓ Manual versus automated fulfillment
- ✓ Request expiration and temporary access
- ✓ Access request cancellation and revocation
- ✓ Exception and escalation scenarios
- ✓ Tracking request status
- ✓ Auditability of request and approval decisions

## Module 9: Certification, Access Reviews & Governance Design

- ✓ Purpose of identity certifications
- ✓ Certification architecture
- ✓ Manager access reviews
- ✓ Application owner certifications
- ✓ Entitlement owner reviews
- ✓ Role-related access reviews
- ✓ Campaign design considerations
- ✓ Certification scope and frequency
- ✓ Reviewer selection strategy
- ✓ Delegation and reassignment
- ✓ Certification decision processes
- ✓ Revocation and remediation architecture
- ✓ Handling unresolved certification items
- ✓ Evidence and audit considerations
- ✓ Certification performance at enterprise scale
- ✓ Reducing reviewer fatigue
- ✓ Risk-oriented access review approaches
- ✓ Continuous governance considerations

## Module 10: Roles, Access Profiles & Policy Architecture

- ✓ Enterprise role architecture
- ✓ Business role design considerations
- ✓ IT and technical role considerations

- ✓ Role-to-access-profile relationships
- ✓ Role assignment strategy
- ✓ Role hierarchy considerations
- ✓ Role ownership and governance
- ✓ Role lifecycle management
- ✓ Role changes and impact assessment
- ✓ Role explosion and complexity management
- ✓ Policy architecture
- ✓ Access policy definition
- ✓ Preventive and detective control considerations
- ✓ Policy violation management
- ✓ Exception handling
- ✓ Designing sustainable role and policy structures

## Module 11: Security, Risk, Compliance & Segregation of Duties

- ✓ Identity security control architecture
- ✓ Least privilege and need-to-know principles
- ✓ Segregation of Duties (SoD) concepts
- ✓ Identifying conflicting access
- ✓ Preventive versus detective controls
- ✓ Policy violation architecture
- ✓ Risk-based access governance
- ✓ Privileged access considerations
- ✓ Sensitive entitlement governance

- ✓ Administrative access controls
- ✓ Identity security audit requirements
- ✓ Compliance evidence considerations
- ✓ Access traceability
- ✓ Regulatory and organizational policy alignment
- ✓ Exception and compensating control processes
- ✓ Governance reporting requirements
- ✓ Security considerations for identity integrations
- ✓ Architectural controls for reducing identity-related risk

## **Module 12: APIs, Extensibility, Automation & Enterprise Integrations**

- ✓ SailPoint integration and extensibility concepts
- ✓ API architecture fundamentals
- ✓ REST API integration patterns
- ✓ Authentication and authorization considerations
- ✓ API-driven identity operations
- ✓ Event-based integration concepts
- ✓ Webhook and event notification considerations
- ✓ Workflow and automation architecture
- ✓ Integration with IT service management platforms
- ✓ Integration with HR ecosystems
- ✓ Integration with directories and enterprise applications
- ✓ Integration with security platforms
- ✓ Custom transformation considerations

- ✓ External orchestration patterns
- ✓ API rate and performance considerations
- ✓ Error handling and retry mechanisms
- ✓ Logging and monitoring integrations
- ✓ Secure handling of credentials and secrets
- ✓ Establishing reusable enterprise integration patterns

## Module 13: Scalability, Performance, Deployment & Architectural Best Practices

- ✓ Designing identity solutions for enterprise scale
- ✓ Estimating identity, account, and entitlement volumes
- ✓ Aggregation performance considerations
- ✓ Provisioning workload considerations
- ✓ Certification scalability
- ✓ Integration throughput
- ✓ API consumption considerations
- ✓ Scheduling architecture
- ✓ Dependency and failure analysis
- ✓ Resilience considerations
- ✓ Monitoring strategy
- ✓ Logging and operational visibility
- ✓ Environment strategy
- ✓ Configuration promotion considerations
- ✓ Production readiness planning
- ✓ Architecture documentation standards

- ✓ Design review and governance
- ✓ Operational handover considerations
- ✓ Architectural anti-patterns
- ✓ Long-term maintainability and scalability

## Module 14: Enterprise Solution Architecture, Migration & Real-World Case Studies

### Enterprise Architecture Planning

- ✓ Gathering business and technical requirements
- ✓ Stakeholder identification
- ✓ Current-state IAM assessment
- ✓ Defining target-state identity architecture
- ✓ Gap analysis
- ✓ Functional and non-functional requirement mapping
- ✓ Integration inventory preparation
- ✓ Identity data flow mapping
- ✓ Architectural decision documentation

### Migration & Transformation Strategy

- ✓ Legacy IAM migration considerations
- ✓ Identity and account data migration
- ✓ Application onboarding strategy
- ✓ Entitlement transition planning
- ✓ Role and access model migration
- ✓ Phased versus large-scale migration approaches

- ✓ Coexistence considerations
- ✓ Migration risk assessment
- ✓ Cutover and transition planning
- ✓ Post-migration validation

## Architecture Case Studies

- ✓ Global workforce identity architecture
- ✓ Employee and contractor identity scenario
- ✓ Hybrid application integration scenario
- ✓ Joiner-mover-leaver architecture exercise
- ✓ Large-scale application onboarding scenario
- ✓ Enterprise access request architecture
- ✓ Certification and compliance scenario
- ✓ Role and access profile architecture exercise
- ✓ SoD and sensitive-access governance scenario
- ✓ API-based integration scenario
- ✓ Architecture review and optimization exercise
- ✓ Preparing an end-to-end SailPoint identity security solution blueprint