Identity Federation and Single Sign-On (SSO) in the Cloud Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The Cloud Transformation era demands a paradigm shift in managing user access, moving beyond legacy, on-premises directory services. Organizations globally are grappling with the complexity of securing diverse, distributed cloud resources and SaaS applications while maintaining a frictionless User Experience (UX). This is where Identity Federation and Single Sign-On (SSO) emerge as non-negotiable pillars of a modern, Zero Trust Security model. Identity Federation establishes a Trust Relationship between independent systems (Identity Provider (IdP) and Service Provider (SP)), allowing for the secure and standardized exchange of identity assertions using protocols like SAML 2.0 and OpenID Connect (OIDC).

Identity Federation and Single Sign-On (SSO) in the Cloud Training Course dives into the Architecture and Implementation of these foundational Cloud IAM strategies across major platforms. We will provide Hands-on Labs and Real-World Scenarios to master the configuration, Governance, and Auditing required to secure your hybrid and Multi-Cloud environments, ensuring Compliance and mitigating the high risk of Credential Compromise and Token Theft. Master the art of Streamlined Access without sacrificing stringent security.

Programme Curriculum

Identity Federation and Single Sign-On (SSO) in the Cloud Training Course

Introduction

The Cloud Transformation era demands a paradigm shift in managing user access, moving beyond legacy, on-premises directory services. Organizations globally are grappling with the complexity of securing diverse, distributed cloud resources and SaaS applications while maintaining a frictionless User Experience (UX). This is where Identity Federation and Single Sign-On (SSO) emerge as non-negotiable pillars of a modern, Zero Trust Security model. Identity Federation establishes a Trust Relationship between independent systems (Identity

Provider (IdP) and Service Provider (SP)), allowing for the secure and standardized exchange of identity assertions using protocols like SAML 2.0 and OpenID Connect (OIDC).

Identity Federation and Single Sign-On (SSO) in the Cloud Training Course dives into the Architecture and Implementation of these foundational Cloud IAM strategies across major platforms. We will provide Hands-on Labs and Real-World Scenarios to master the configuration, Governance, and Auditing required to secure your hybrid and Multi-Cloud environments, ensuring Compliance and mitigating the high risk of Credential Compromise and Token Theft. Master the art of Streamlined Access without sacrificing stringent security.

Course Duration

5 days

Course Objectives

1. Master the Architecture of Federated Identity Management (FIM) and its crucial role in Cloud Security Posture.
2. Differentiate clearly between traditional SSO, Federation, and modern Workload Identity Federation concepts.
3. Implement and Configure core federation protocols: SAML 2.0 and OpenID Connect (OIDC).
4. Design secure and Scalable SSO solutions for both SaaS Applications and Custom Cloud Workloads.
5. Integrate on-premises Active Directory with leading Cloud IdPs like Microsoft Entra ID and Okta for seamless Hybrid Identity.
6. Secure the Identity Lifecycle by implementing Just-in-Time (JIT) Provisioning and Automated De-provisioning in federated systems.
7. Enforce strong authentication by integrating Multi-Factor Authentication (MFA) and Adaptive Authentication into SSO flows.
8. Configure Claim Transformations and Attribute Mapping for fine-grained authorization using Role-Based Access Control (RBAC).
9. Troubleshoot common federation issues, including Token Validation Errors, Certificate Management, and Metadata Exchange.
10. Apply Zero Trust Principles to identity governance, focusing on Least Privilege Access across federated domains.
11. Perform Centralized Auditing and Logging to ensure Regulatory Compliance of access events.
12. Explore advanced topics like API Security with OAuth 2.0 and Client-Side SSO for mobile applications.
13. Optimize User Experience (UX) while maintaining robust security to reduce Password Fatigue and Help Desk tickets.

Target Audience

1. Cloud Security Architects.
2. Identity & Access Management (IAM) Engineers.
3. DevOps & Platform Engineers.
4. IT Administrators/System Engineers.
5. Cybersecurity Analysts/Auditors.
6. Enterprise Architects.
7. Technical Project Managers.
8. Software Developers.

Course Modules

Module 1: Cloud IAM and The Federation Imperative

- Foundations of Cloud Identity and Access Management
- The business and security drivers for SSO and Identity Federation.
- Comparing IdP and SP roles and the Trust Anchor concept.
- Understanding the Hybrid Identity challenge
- Case Study: Enterprise-Wide Adoption

Module 2: Core Federation Protocols Deep Dive

- Detailed review of SAML 2.0 Message Flows.
- OpenID Connect and OAuth 2.0 for modern applications and APIs.
- Metadata Management and Certificate Rollover best practices.
- Security Context of ID Tokens and Access Tokens.
- Case Study: SaaS Integration Challenge.

Module 3: Implementing Single Sign-On (SSO) in Hybrid Environments

- Connecting AD/LDAP to the cloud via sync tools.
- Configuring Federation Services for SSO.
- Seamless SSO and Pass-through Authentication options.
- Advanced Conditional Access Policies based on user location, device, and risk.
- Case Study: Remote Workforce Security.

Module 4: Multi-Cloud and Cross-Domain Federation

- Federating Identities across major public clouds
- Setting up Workload Identity Federation for non-human identities
- Handling Attribute Assertions and Group Synchronization in multi-cloud.
- Implementing JIT User Provisioning using protocols like SCIM.
- Case Study: B2B Partner Access.

Module 5: Authentication and Authorization Security

- Implementing Multi-Factor Authentication and Passwordless methods in SSO.
- Designing Authorization Models based on Claims-Based Access Control.
- Token Management strategies.
- Protecting against Token Theft, Replay Attacks, and Privilege Escalation.
- Case Study: High-Value Application Protection.

Module 6: Identity Governance and Auditing

- Identity Lifecycle Management.
- Defining and maintaining Role-Based Access Control across federated domains.
- Centralized Logging and Monitoring of all authentication and authorization events.
- Conducting periodic Access Reviews and Compliance Audits
- Case Study: Compliance Failure Mitigation.

Module 7: Troubleshooting and Operational Excellence

- Using IdP and SP Logs to diagnose common SSO failures.
- Troubleshooting SAML Signature Validation and Encryption issues.

- Strategies for managing High Availability and Disaster Recovery for the IdP.
- Health Checks and Monitoring of the federation infrastructure.
- Case Study: Outage Scenarios.

Module 8: Future Trends and Advanced Federation

- Client-Side SSO and Mobile Identity Management.
- API Security using OAuth 2.0 Scopes and the Gateway pattern.
- Introduction to Decentralized Identity and Verifiable Credentials.
- The evolution of Zero Trust Network Access and its reliance on FIM.
- Case Study: The API Economy.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com