

Saviynt IGA Level 200 Training

Training Datasheet

Authored by: Saviynt University

Learning Path Overview

The Saviynt IGA Level 200 training delivers advanced, practical expertise needed to design, implement, and manage complex identity governance solutions within the Saviynt Identity Cloud. Built for experienced IGA practitioners—including Implementation Specialists, Solution Architects, Administrators, and identity program leaders—this learning path dives deeper into the platform’s advanced capabilities and enterprise grade features.

Learners explore sophisticated functionalities such as the Advanced Access Request System, Service Account Management, REST-based Integrations, APIs, Group Management, Saviynt Intelligence, and ServiceNow Integration. Through detailed demonstrations and guided, real-time lab exercises, participants gain hands-on experience solving real-world challenges across enterprise IGA environments.

This advanced training prepares professionals to architect and operationalize end-to-end identity governance processes, automate access workflows, integrate with complex ecosystems, and optimize the security posture of modern organizations using Saviynt Identity Cloud. Equipped with deeper platform understanding and practical implementation insights, participants are enabled to confidently support and scale enterprise identity programs.

Learning Path Duration

- 26 hours of learning content
- 20% lecture, 30% demo, and 50% hands-on lab

Target Audience

- Saviynt IGA Implementation Teams
- IGA Solution Architects
- IAM Professionals
- IDM Consultants and Decision Makers in the Identity Practice

Delivery Methods

- Classroom (In-Person)
- Virtual Classroom (Live-Online)
- Onsite
- Self-Paced

Lab Environment

- Hands-on labs are included as part of this training

Prerequisites

- Saviynt IGA Level 100 or equivalent knowledge

Learning Path Objectives

This learning path enables you to achieve the following objectives:

- Explain advanced concepts of Identity Governance and Administration (IGA) and how Saviynt Identity Cloud supports complex enterprise identity solutions.
- Explain detailed concepts and solutions delivered by the Saviynt Identity Security Posture Management (ISPM), including how it unifies identity data into actionable intelligence and helps drive remediation.
- Demonstrate advanced configuration and management of the Access Request System (ARS), including workflows, bulk requests, and role-based access provisioning.
- Implement and manage Service Account lifecycle, including reconciliation, governance, and campaign management.
- Configure and manage Active Directory (AD) Group Management, including group lifecycle operations and entitlement governance.
- Integrate applications using REST Connectors, including import, provisioning, and deprovisioning use cases.
- Utilize Saviynt REST and SCIM APIs to automate access requests, approvals, and identity operations.
- Integrate Saviynt with ServiceNow for ticketing, application management, and workflow automation.
- Implement Duplicate Identity Management using import processes and detective jobs.
- Perform Role Mining and Entitlement Discovery to optimize role design and access governance.
- Explore Saviynt Intelligence features such as ISPM and Non-Human Identity (NHI).
- Implement advanced application onboarding techniques, including agentic-based onboarding and Terraform automation.
- Apply best practices and troubleshoot complex identity governance and integration scenarios.

Courses and Modules

01 | Saviynt Introduction

- About Saviynt
- Saviynt's Product Offerings
- IGA Level 200 Training

02 | ISPM Fundamentals (v2026)

- Overview
- Problem Statement
- Introduction to Saviynt ISPM
- ISPM Architecture
- ISPM for CISO
- ISPM for Compliance Leader
- ISPM for BISO
- ISPM for Identity Security Leader
- AI Trust and Safety FAQs
- Entitlement Enrichment FAQs
- Frequently Asked Questions

03 | Advanced Access Request System

- Introduction
- Workflow Management and Administration
- Bulk Request Submission
- Roles - Introduction
- Access Request for Enterprise Roles
- Access Request for Application Roles
- Access Request for Emergency Access Roles
- Account Management in Saviynt Identity Cloud
- Password Management
- Custom Form Creation Using Dynamic Attributes
- Introduction to JITA
- Best Practices and Troubleshooting

04 | REST Connector and Saviynt APIs

- REST Integration Overview and Prerequisites
- REST Connector - Import Use Cases
- REST Connector - Provisioning
- REST Connector Deprovisioning
- REST Use Case – REST-Supported Application
- Saviynt REST API Overview and Guide
- Saviynt Identity Cloud API Reference – Postman
- Saviynt API Use Case – Create Request
- Saviynt API Use Case – Request Approval
- Saviynt API Use Case - Service Account
- Saviynt API Use Case - AD Group Management
- Saviynt API Use Case – Analytics
- Saviynt SCIM APIs Overview
- Saviynt SCIM APIs Use Cases
- Best Practices and Troubleshooting

05 | Service Account Management

- Introduction
- Reconciliation of Service Accounts
- Service Account Management – Configurations
- Request for Creation of Service Account
- Request for Modification of Service Account
- Automated Ownership Transfer of Service Accounts
- Segregation of Duties for Service Accounts
- Delegation Features for Service Accounts
- Password Policy for Service Accounts
- Service Account Campaign
- Request for Removal of Service Accounts
- Best Practices and Troubleshooting

07 | Advanced Saviynt Intelligence

- Duplicate Identity Management - Overview
- Duplicate Identity Management During User Import
- Duplicate Identity Management via Detective Job
- Role Mining - Overview
- Role Lifecycle
- Create Roles Using Role Mining
- Modify Existing Roles from Workbench
- Peer Access Analytics
- Best Practices and Troubleshooting

06 | Group Management in Saviynt Identity Cloud

- Group Management Introduction
- Active Directory Group Management – Overview
- AD Group Management – Configuration Overview
- Create AD Groups
- Request Access for Newly Created AD Groups
- Update AD Groups
- Entitlement Owner Certification
- Delete AD Groups
- Entitlement Lifecycle Management
- Best Practices and Troubleshooting

08 | Saviynt Identity Cloud Integration with ServiceNow

- Introduction to ServiceNow
- Integration of Saviynt with ServiceNow
- ServiceNow as a Managed Application
- ServiceNow as a Ticketing system
- Saviynt App for ServiceNow
- Best Practices and Troubleshooting

09 | Intelligent App Onboarding Advanced

- Application Discovery
- Agentic-Based Onboarding for Disconnected Applications
- Terraform for Onboarding Automation

10 | ADD-ON Course - New Features and Improvements

- Access Request Enhancements
- Email Enhancements – Embed Approval Detail Links in Emails
- Request Enhancement – Single Select Entitlement Type
- Entra ID Connector Support For Temporary Access Pass (TAP)
- Endpoint Filter Enhancements
- Outlier Analysis And Simplified Configurations
- Intelligent Rule Recommendations

Upon Training Completion

Saviynt will provide you with a training completion certificate after completion of this training. A sample of the certificate is shown below:

