zensar

Establishing IAM Lab: Architecture, Use Cases, and Best Practices

White paper

An RPG Company

Table of Contents

1. Purpose of the IAM Lab
2. IAM Lab Tool Stack Overview
3. High-Level IAM Lab Architecture
4. Core IAM Lab Use Cases
5. IAM Lab Best Practices
6. Common Configuration Pitfalls
7. Who This IAM Lab is for
8. Step-by-Step IAM Lab Build Guide
9. Deep-Dive: Saviynt Hands-on Walkthrough
10. HR Feed and AD Attribute Mapping
11. ServiceNow Entitlement Expansion
12. Conclusion

Executive Summary

Modern enterprises rely on HR-driven identity and access management (IAM) to automate user life cycle events, enforce least-privilege access, and meet compliance requirements. Platforms such as Saviynt, when integrated with HRMS, Active Directory (AD), Microsoft Entra ID, and ServiceNow, form a powerful identity ecosystem.

An IAM lab provides a safe, isolated environment to understand, design, and validate this ecosystem before production rollout. This white paper explains how to design an IAM lab using HRMS, Saviynt, Active Directory, Entra ID, ServiceNow, covering architecture, core use cases, and best practices.

1. Purpose of the IAM Lab

This IAM lab focuses on foundational, HR-driven identity flows using commonly deployed enterprise tools.

Primary goals:

- Understand the end-to-end identity life cycle
- Practice HR-triggered joiner-mover-leaver (JML)
- Learn Saviynt-based provisioning
- Validate AD and Entra ID account management
- Simulate ServiceNow ticket creation

2. IAM Lab Tool Stack Overview

HRMS (Identity source)

Role in lab: Authoritative source of user identities

Typical options:

- CSV/flat file feed
- Simplified HR database

Key attributes:

- Employee ID (unique key)
- First and last name
- Department
- Job title
- Manager ID
- Location
- Joining/exit date

Saviynt (IAM and IGA Platform)

Role in lab: Central identity brain

Core responsibilities:

- Ingest HRMS feed
- Create and manage identities
- Apply access policies
- Provision/deprovision accounts
- Trigger ServiceNow tickets
- Maintain audit logs

Key Saviynt modules used:

- Identity repository
- User life cycle management
- Access request
- Provisioning engine
- Basic governance (certifications)

Active Directory (AD)

Role in lab: On-prem identity store

Used for:

- Network authentication
- Group-based authorization
- Legacy application access

Saviynt provisions:

- AD user accounts
- Group membership
- Account disablement on exit

Microsoft Entra ID (Azure AD)

Role in lab: Cloud identity and access platform

Used for:

- Cloud authentication
- SaaS access
- Hybrid identity scenarios

Saviynt provisions:

- Entra ID user accounts
- Cloud group memberships
- Account disablement

ServiceNow (ITSM Integration)

Role in lab: Ticketing and visibility

Used for:

- Access request tickets
- Provisioning status tracking
- Audit and operational visibility

Saviynt creates:

- Incident or request tickets
- Automated ticket updates
- Closure on task completion

3. High-Level IAM Lab Architecture

Logical flow

- User record created/updated in HRMS
- Saviynt imports HR data
- Identity created or updated in Saviynt
- Access policies evaluated
- Accounts provisioned in:
    - Active Directory
    - Entra ID
- ServiceNow ticket generated
- Logs and reports captured in Saviynt

4. Core IAM Lab Use Cases

Joiner (new hire)

Trigger: New employee added in HRMS

Flow:

- Saviynt creates identity
- AD account created
- Entra ID account created
- Default groups assigned
- ServiceNow ticket logged

Mover (role or department change)

Trigger: HRMS attribute change

Flow:

- Saviynt detects change
- Old group memberships removed
- New groups assigned
- AD and Entra ID updated
- eNow ticket updated

Leaver (exit)

Trigger: Exit date updated in HRMS

Flow:

- Saviynt disables identity
- AD account disabled
- Entra ID account disabled
- All access revoked
- ServiceNow closure ticket

Access request via Saviynt

Flow:

- User submits access request
- Manager approval
- Optional ServiceNow ticket
- Provisioning to AD/Entra ID

Governance and audit

- Basic access review
- Manager certification
- Saviynt audit reports

5. IAM Lab Best Practices

HR-first design

- Treat HRMS as authoritative
- Avoid manual identity creation

Attribute-driven access

- Use department, role, location
- Minimize manual entitlements

Keep integrations minimal

- One HR feed
- One AD domain
- One Entra ID tenant
- One ServiceNow instance

Use test-only credentials

- No production trust
- Isolated tenants

Document end-to-end flows

6. Common Configuration Pitfalls

- Incorrect HRMS primary key mapping
- Missing correlation rule
- Overlapping AD and Entra provisioning logic
- Unclear ServiceNow ticket ownership

7. Who This IAM Lab Is for

- IAM beginners
- Saviynt administrators
- Identity engineers
- Security trainees
- Pre-sales demos

Conclusion

A well-designed HRMS, Saviynt, AD, Entra ID, or ServiceNow IAM lab provides a realistic yet safe environment to understand enterprise IAM foundations. At this level, the emphasis should remain on clear HR-driven identity flows, simple integrations, and strong visibility. This lab serves as the backbone for scaling advanced IAM, governance, and zero-trust implementations.

8. Step-by-Step IAM Lab Build Guide

HR feed –> Saviynt import

Objective: Establish HRMS as the authoritative identity source.

Steps:

1. Create a mock HR feed (CSV or flat file)
2. Include mandatory attributes: -

employeeId (primary key)

firstName,

lastName

department

jobTitle

location

3. Configure the Saviynt user import job
4. Schedule import (daily or on-demand)

Outcome: Identities are created or updated automatically in Saviynt.

Saviynt user import JSON (sample)

```
{
 "employeeId": "${empId}",
 "username": "${email}",
 "firstname": "${firstName}",
 "lastname": "${lastName}",
"department": "${department}",
 "jobtitle": "${jobTitle}",
"manager": "${managerId}",
 "status": "${status}",
   "startdate": "${startDate}",
   "enddate": "${endDate}"
}
```

Correlation rules (Saviynt)

Purpose: Prevent duplicate identities.
Best practice:
Primary: employeeId
Secondary (fallback): email/username

Example logic: If employeeId matches, then correlate; else create a new identity

Active Directory connector setup

Key configurations: -

AD domain details
- Service account with suggested permissions
- OU mapping for users and groups

Provisioning scope:
- Create AD user
- Update attributes
- Add/remove group memberships
- Disable account on exit

Entra ID (Azure AD) connector setup

Key configurations:

- Tenant ID
- Client ID and secret
- Graph API permissions
-

Provisioning scope:
- Cloud user creation
- Group assignments
- Account disablement

ServiceNow integration and CreateTicketJSON

Purpose: Operational visibility and audit trail

Sample CreateTicketJSON:

```
{
  "short_description": "IAM Provisioning Request",
  "description": "User ${username} provisioned with access: ${entitlement}.",
  "caller_id": "${manager}",
  "assignment_group": "IAM Support",
  "category": "Access",
  "subcategory": "Provisioning"
}
```

Conclusion

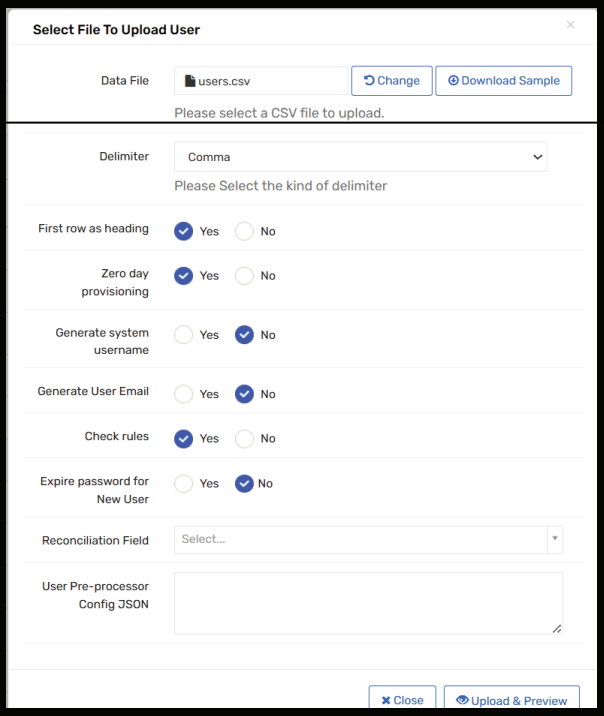
This IAM Lab transforms a foundational setup into a practical, enterprise-ready learning environment. By combining HRMS, Saviynt, AD, Entra ID, and ServiceNow, teams gain real-world experience across the identity life cycle, provisioning, and governance.

9. Deep-Dive: Saviynt Hands-on Walkthrough

Saviynt UI walkthrough – HR user import

Navigation path:

Admin → Identity Repository → Users → Actions → Upload User



Steps:

1. Click 'create new import job.'
2. Select 'source type: File/DB (as per lab).'
3. Upload HR feed or configure connection.
4. Map source attributes to Saviynt user attributes.
5. Define primary key (employeeId).
6. Enable create/update user.
7. Save and run job.

Validation:

Navigate to 'Admin → Identity Repository → Users and verify new identities

---

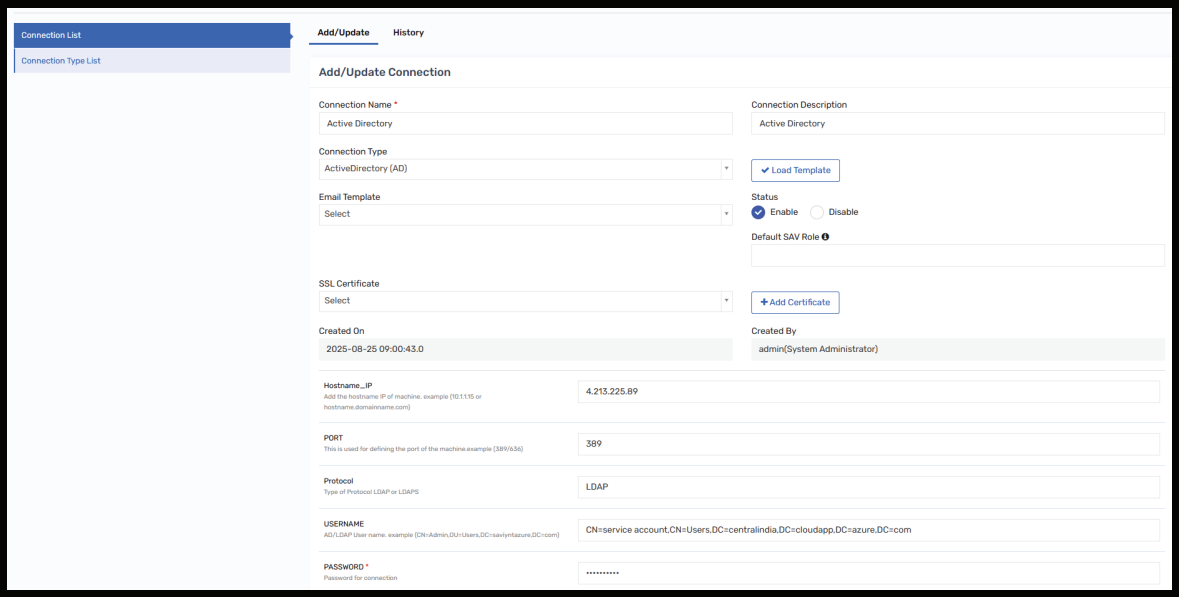
Saviynt UI walkthrough – AD Connector

Navigation path:

Admin → Connections → Create connection →AD

Steps:

1. Enter AD domain details.
2. Provide service account credentials.
3. Configure base DN and OU paths.
4. Test connection.
5. Enable provisioning JSONs tasks.



Saviynt UI walkthrough – Entra ID connector

Navigation path:

Admin→ Connections→ Create connection→ Azure AD

Steps:

1. Enter tenant ID.
2. Configure client ID and secret.
3. Assign graph API permissions.
4. Test connection.
5. Enable user and group provisioning.

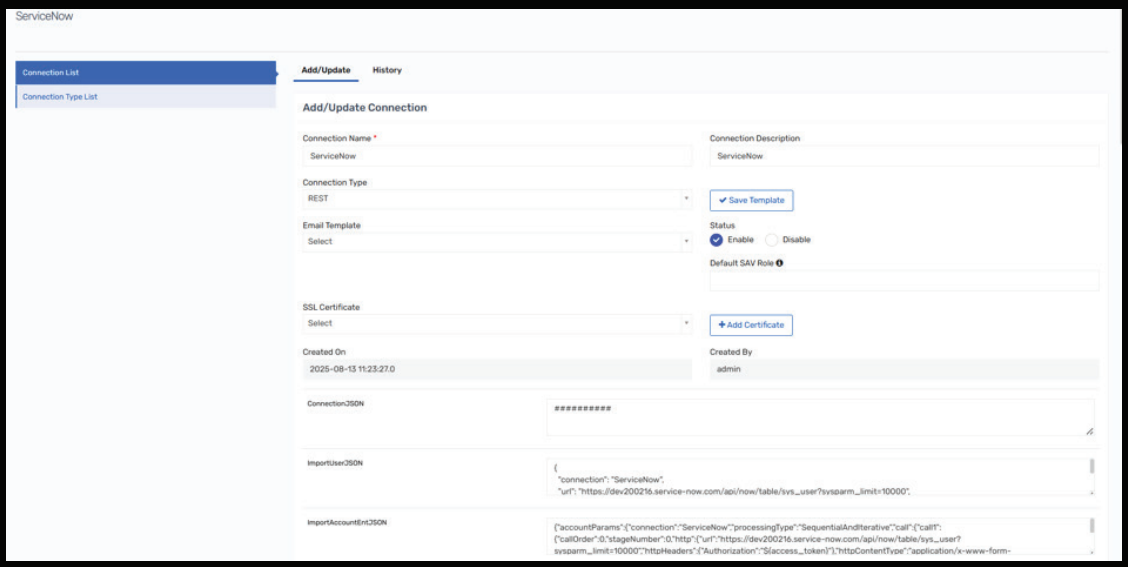
10. HR Feed and AD Attribute Mapping

HR Attribute	Saviynt Attribute	AD Attribute
employeeId	employeeId	employeeID
firstName	firstName	givenName
lastName	lastName	sn
email	email	mail
department	department	department
jobTitle	jobTitle	title
location	location	physicalDeliveryOfficeName

11. ServiceNow Entitlement Expansion

Purpose of allEntitlementsValues

Used to provide detailed entitlement information inside ServiceNow tickets.



Sample allEntitlementsValues Structure

```
[
  {
    "application": "Active Directory",
    "entitlement": "Finance_AD_Group",
    "type": "Security Group"
  },
  {
    "application": "Entra ID",
    "entitlement": "O365_E3",
    "type": "License"
  }
```

Enhanced CreateTicketJSON using allEntitlementsValues

```
{
  "short_description": "IAM Access Provisioning",
  "description": "User ${username} granted access:
${allEntitlementsValues}",
  "category": "Access",
  "subcategory": "IAM",
  "assignment_group": "IAM Operations"
}
```

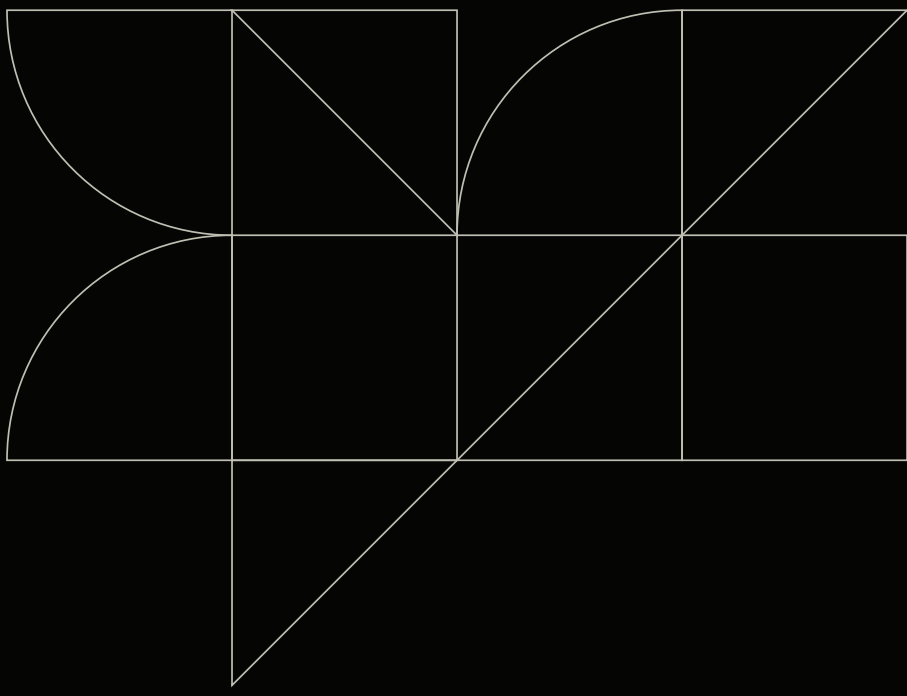
12. Conclusion

This deep-dive transforms the IAM Lab into a near-production simulation, enabling practitioners to understand not just what IAM does, but how it is configured, validated, and audited in real enterprises. With Saviynt UI walkthroughs, realistic attribute mapping, and enriched ServiceNow tickets, the lab now supports hands-on mastery and operational confidence.

Authored by

Vinit Gupta,

Solution Architect, Global Cybersecurity Practice
Cloud, Infrastructure, and Security Services (CIS)



zensar

An RPG Company

At Zensar, we're 'experience-led everything.' We are committed to conceptualizing, designing, engineering, marketing, and managing digital solutions and experiences for over 145+ leading enterprises. Using our 3Es of experience, engineering, and engagement, we harness the power of technology, creativity, and insight to deliver impact.

Part of the $4.8 billion RPG Group, we are headquartered in Pune, India. Our 10,000+ employees work across 30+ locations worldwide, including Milpitas, Seattle, Princeton, Cape Town, London, Zurich, Singapore, and Mexico City.

For more information, please contact: **info@zensar.com | www.zensar.com**