SOLUTION GUIDE

Saviynt Integration with Multiple AD Forests via ADSI Connector

Connect Everything. Securely.

Saviynt

Infosys

Problem Statement

The customer operates across multiple forest environments (Forest 1, Forest 2, and Forest 3), each governed by unique identity lifecycle management policies, provisioning workflows, and naming conventions. The primary objective is to streamline and automate user account provisioning, updates, and de-provisioning while maintaining compliance with domain-specific requirements and reducing reliance on manual processes.

Key Challenges:

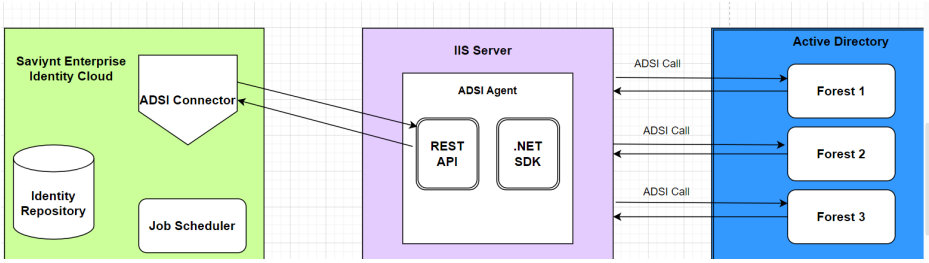
- Variability in provisioning logic across different domains
- Complex and inconsistent naming conventions, including duplication management
- Manager-to-user mapping across forest boundaries
- Handling of email notifications and one-time password (OTP) delivery
- Lifecycle management complexities for re-hires and terminations
- Restrictions due to read-only domains and the need for cross-domain group assignments

Solution Overview

Infosys has developed a solution where Saviynt EIC integrates with three Active Directory forests via ADSI to automate and manage identity lifecycle operations across domains.

Key Capabilities

- **Account Import & Provisioning:** Automatically synchronizes and creates user accounts across multiple forest environments.
- **Lifecycle Management:** Manages user updates, rehire processing, terminations, and organizational unit (OU) placements throughout the user lifecycle.
- **Account Enablement/Disabling:** Automates account status changes while updating relevant audit attributes for compliance and tracking.
- **Group Management:** Handles group assignments and removals across domains, including support for cross-forest group membership.



Business Value:

- **Seamless Access Provisioning:** Delivers streamlined and automated access provisioning across all Active Directory forests.
- **Automated User Lifecycle Management:** Handles user provisioning and deprovisioning with minimal manual effort, ensuring timely and accurate updates.
- **Right Access in the Right Forest:** Guarantees users are provisioned with appropriate access rights based on their domain-specific requirements.
- **Cross-Forest Group Assignment:** Enables assigning users to security groups across different forests, supporting hybrid and distributed environments.
- **Centralized Logging & Reporting:** Consolidates audit logs and activity reports across all forests, improving visibility and control.
- **Compliance & Audit Readiness:** Supports regulatory compliance (e.g., SOX) with unified audit trails and policy enforcement.

The architecture consists of the following key components:

IIS Server

The IIS (Internet Information Services) Server acts as an intermediary between Saviynt and Active Directory, providing a secure API gateway. It includes:

- REST API – Exposes RESTful endpoints to facilitate communication.
- .NET SDK – Provides the necessary libraries to interact with ADSI and execute directory operations.

IIS server acts as a bridge between Saviynt EIC and Active Directory. Hosts a NET SDK-based REST API that allows Saviynt to send requests securely to Active Directory. Maintains service accounts with the necessary permissions to modify user objects in AD.

Active Directory (AD) – Multi-Forest Architecture

The Active Directory (AD) infrastructure is organized into three distinct forests, each representing separate organizational domains:

- **Forest 1** – The primary corporate forest, containing multiple sub-domains: Domain 1, Domain 2, and Domain 3.
- **Forest 2** – A standalone private environment with a single domain.
- **Forest 3** – Comprises three sub domains: Domain 4, Domain 5, and Domain 6.

Each forest is managed independently, and integration with Saviynt via the ADSI Connector ensures seamless identity synchronization across all environments.

Security Considerations

- **Service Account Permissions:**

Follows a least privilege access model to limit AD service account capabilities to only what is necessary.

- **Encryption:**

All directory communications utilize **Secure LDAP (LDAPS)** to ensure data confidentiality in transit.

- **Logging & Auditing:**

Identity operations are logged within Saviynt for **auditability and compliance tracking.**

Assumptions & Dependencies

- **LDAP Accessibility:**

All AD forests must permit LDAP access from Saviynt.

- **Appropriate Permissions:**

Service accounts must be granted the required privileges for provisioning and lifecycle tasks.

- **Network Configuration:**

Firewall rules must be in place to allow communication between Saviynt and the AD environments.

Use Case Implemented

Infosys has implemented a use case where a user is provisioned by default in Domain 1 (Forest 1), receiving birthright access along with an email and UPN sourced from Domain 1. Upon termination, the account is disabled, moved to a designated deletion OU, and all group memberships are removed except for the email license. In the event of a rehire, access rules are re-evaluated, the account is reactivated, and an OTP is sent to facilitate password reset.

Group assignments can span across Forest 1, Forest 2, and forest 3. If the manager is not in domain 1(Forest 1), the value is fetched from domain 3 (Forest 1). Domain 2 (Forest 1) is read-only, while domain 3 only manages existing accounts. In Forest 2 and Forest 3, accounts follow similar lifecycle rules with domain-specific logic for manager assignment and group provisioning.

This framework outlines a unified yet domain-specific identity governance model using Saviynt Enterprise Identity Cloud (EIC). It supports user provisioning, lifecycle management, and access governance while respecting the operational rules of each Active Directory domain and forest.

Domain 1 (Forest 1)

- **Provisioning:** Default provisioning for new users.
- **OU Mapping:** Reuses existing Organizational Unit mappings.
- **Re-hire Logic:** Re-evaluates birthright rules on rehire.
- **Termination:** Disables account and removes all group memberships except email license.
- **Password Delivery:** No password sent to manager; OTP emailed directly to the user.
- **Naming Source:** Domain 1 is authoritative for email and UPN generation.
- **Manager Mapping:** Uses Domain 1 for manager mapping; if not available, maps from other domains.
- **Cross-Forest Grouping:** Supports cross-forest group assignments.

Business Value:

- **Conditional, Multi-Forest Workflows:** Facilitates complex identity workflows that span multiple forests — e.g., provisioning in Forest 1 and group assignment in Forest 2.
- **Simplified Multi-Domain Management:** Reduces administrative complexity in managing identities across multiple domains and forests.
- **Consistent Security Policy Enforcement:** Ensures uniform application of access policies, reducing the risk of gaps or violations across environments.
- **Reduced Risk of Orphaned Accounts:** Minimizes the likelihood of unused or inconsistent access rights, improving security posture and operational hygiene.

Customer Value:

- **Operational Efficiency:** Automated provisioning and lifecycle management reduce manual effort and errors.
- **Compliance & Governance:** Ensures domain-specific policies are enforced consistently.
- **Scalability:** Supports cross-domain and cross-forest group assignments, enabling future growth.
- **Security:** OTP-based password delivery enhances account security.
- **•User Experience:** Streamlined onboarding and re-hire processes improve turnaround time.
- **Auditability:** Clear rules and naming conventions support traceability and audit readiness

Domain 2 (Forest 1)

- **Access Type:** Read-only domain.
- **Provisioning & Lifecycle:** No provisioning or lifecycle actions performed via Saviynt.

Domain 3 (Forest 1)

- **Account Creation:** No new accounts created.
- **Lifecycle Management:** Limited to managing existing accounts only.

Forest 2

- **Provisioning:** New accounts created based on predefined rule sheet.
- **Termination:** Moves account to designated Termination OU and removes group memberships.
- **Re-hire Logic:** Automatically triggers access rule evaluation on rehire.
- **OTP Delivery:** One-Time Password email sent upon account creation.
- **Manager Mapping:** Sets manager field to blank if not found in domain.

Forest 3

- **Account Creation:** Initiated post Role Management reconciliation.
- **Birthright Access:** Assigns birthright groups automatically.
- **Termination:** Moves account and removes all group memberships.
- **Re-hire Logic:** Triggers access rule evaluation on rehire.
- **OTP Delivery:** One-Time Password email sent upon account creation.
- **Manager Mapping:** Maps manager across all Domain 5 sub-domains within the forest.
- **Cross-Domain Access:** Supports group assignments across domains within the forest.

Naming Conventions

To maintain consistency and prevent conflicts, naming standards will be enforced across all forests:

- **Format:** Standardized naming structure.
- **Case:** All names in lowercase.
- **Character Handling:** Diacritics removed; special characters sanitized.
- **Duplicates:** Resolved using numeric suffixes.
- **Length Restrictions:** Enforced character limits for usernames and account attributes.

Solution Benefits:

Centralized Lifecycle Management Across Forests

Benefits: Automates identity lifecycle events — c**reate, update, enable, and disable — across Forest 1, Forest 2, and Forest 3,** ensuring consistency, accuracy, and timely execution.

Example:

- New users are provisioned by default in **Forest 1.**
- Rehire and termination processes are seamlessly automated across **Forest 2** and **Forest 3.**

Domain-Specific Logic with Centralized Governance

Benefits: Enables enforcement of **domain-specific policies** while maintaining centralized visibility and control through Saviynt.

Example:

- **Forest 2** is read-only; no provisioning actions are performed.
- In **Forest 3**, lifecycle events are managed for existing users only; no new accounts are created (e.g., APAC scenarios).

Enhanced Security and Compliance

Benefits: Secures sensitive identity operations like **disabling accounts, removing group memberships, and updating audit attributes.**

Example:

- On termination, accounts are disabled and moved to a **pending deletion OU.**
- Audit attributes (e.g., termination date, status) are updated for compliance tracking.

Unified Audit and Reporting

Benefits: Delivers a **centralized audit trail** of all identity-related actions across forests, supporting regulatory compliance (e.g., **SOX, GDPR**, internal audits).

Example:

- Identity events such as **account creation, group assignment, and rehire processing** are fully logged.
- Rehire actions trigger reset of audit attributes and re-evaluation of access rules.

Solution Benefits:

Standardized Identity Hygiene

Benefits: Enforces consistent identity standards across forests, improving data integrity through structured rules for **OU placement, manager mapping, and attribute updates.**

Example:

- Manager values are sourced from alternate domains if not found in the user's home domain.
- OU mappings are inherited from production templates for consistency.

Cross-Domain Group Assignment

Benefits: Supports assigning users to **groups across different forests,** enabling access to shared resources regardless of domain boundaries.

Example:

- A user provisioned in **Forest 1** can be added to security groups located in Forest 2 or **Forest 3.**

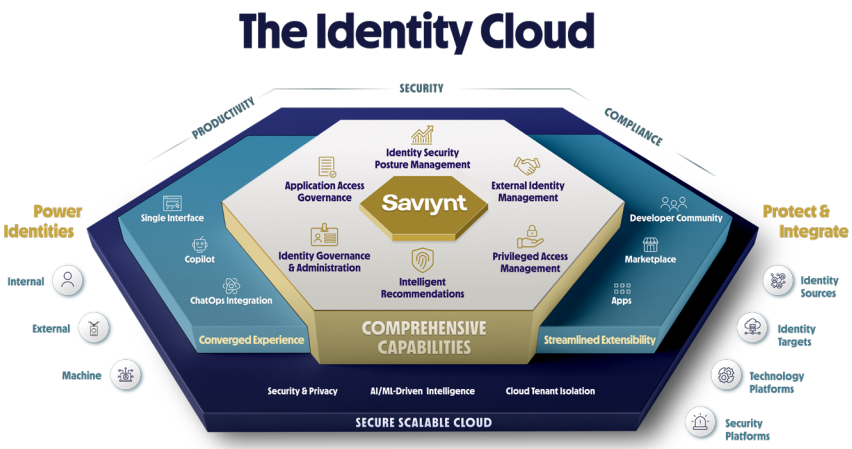
Secure Communication and Credential Handling

Benefits: Domain-specific credential handling improves security by customizing **password delivery and OTP (One-Time Password) flows.**

Example:

- In Forest 1, Azure password reset with OTP is used — **passwords are not sent to managers.**
- Forests 2 and 3 trigger OTP email delivery automatically after account creation.

The Identity Cloud combines core identity security capabilities in a single platform that enhances security while reducing costs and management headaches.



Next Steps

- View the extensive library of integrations at https://saviynt.com/integrations to see detailed information and implementation guides designed to help you get the most from the Enterprise Identity Cloud.

ABOUT PARTNER

Infosys is a global leader in next-generation digital services and consulting. Over 300,000 of our people work to amplify human potential and create the next opportunity for people, businesses and communities. We enable clients in more than 56 countries to navigate their digital transformation. With over four decades of experience in managing the systems and workings of global enterprises, we expertly steer clients, as they navigate their digital transformation powered by cloud and AI. We enable them with an AI-first core, empower the business with agile digital at scale and drive continuous improvement with always-on learning through the transfer of digital skills, expertise, and ideas from our innovation ecosystem. We are deeply committed to being a well-governed, environmentally sustainable organization where diverse talent thrives in an inclusive workplace.

Visit www.infosys.com to see how Infosys (NSE, BSE, NYSE: INFY) can help your enterprise navigate your next

ABOUT SAVIYNT

Saviynt is the leading identity governance platform built for the cloud. It helps enterprise customers accelerate modern cloud initiatives and solve the toughest security and compliance challenges in record time. The Saviynt Enterprise Identity Cloud converges IGA, granular application access, cloud security, and privileged access into the industry's only enterprise-grade SaaS solution.

Saviynt

Headquarters, 1301 E
El Segundo Bl, Suite D, El Segundo, CA
90245, United States

310. 641. 1664 | info@saviynt.com
www.saviynt.com