JOINER · MOVER · LEAVER AUTOMATION

Every employee exit leaves an open door. Every new hire deserves Day One access. IDAM closes one. And opens the other.

Esii IDAM automates the complete employee identity lifecycle - from onboarding through internal movements to departure across your HR systems and your Microsoft identity environment. Whether your organisation runs on-premises Active Directory, Azure Entra ID or Microsoft 365, IDAM ensures every identity event is handled automatically, accurately and with a complete audit record. Without a single manual step from your IT team.

- Joiner - Account Provisioned
- Mover - Access Updated
- Leaver - Access Revoked

THE PROBLEM

Manual Employee Indentity management is a security liability that most organisations have quietly accepted.

01 Departed employees retain active accounts after leaving the organization.

Every employee resignation leaves behind an active account in Active Directory, Microsoft Entra ID, or Microsoft 365. Former employees continue to hold valid credentials for days or weeks after their exit date. Every active account is an unnecessary entry point into your enterprise environment, increasing security risk and exposing a clear compliance gap during audits.

02 New employees are waiting for access while IT teams manually process onboarding tickets.

HR confirms a hire in their system. A ticket is raised to IT. By the time the account is created and access permissions are assigned whether in Active Directory, Entra ID or Microsoft 365, the employee has already lost their first day of productive work.

03 Internal transfers and promotions are not reflected in Active Directory access for weeks.

An employee moves from the Finance team to Operations. Their old Finance folder access is never removed. The next internal audit flags it as a policy violation, months after the fact.

Automated Sync
HR event to Identity action

Zero Orphaned Accounts
On every leaver event

Full Audit Trail
Every action logged

WHAT ESII IDAM DOES

IDAM sits between your HR system and your Microsoft identity environment that is on-premises Active Directory, Azure Entra ID or Microsoft 365, ensures that every identity event is handled automatically, accurately and with a complete audit record.

👤 **Automated Account Provisioning**
Internal transfers and promotions recorded in your HRMS trigger automatic attribute updates across your identity environment. Previous access permissions are removed and updated permissions are applied within the same sync cycle - across Active Directory, Entra ID or Microsoft 365.

🔄 **Access Updates on Role Changes**
When a new joiner is confirmed in your HR system, IDAM provisions the account in your identity environment that is Active Directory, Azure Entra ID or Microsoft 365, assigns role-based permissions and logs every action with a timestamp and trigger source. No IT ticket is raised at any stage.

🚪 **Immediate Access Revocation on Exit**
The moment a resignation or termination is recorded in your HR system, all access is revoked - across Active Directory, Azure Entra ID and Microsoft 365. M365 licenses are removed, the identity is disabled and the exact timestamp is captured in the audit log for compliance review.

🏢 **Multi-Client Configuration**
Each business unit or location operates under its own governance rules, identity environment configuration and attribute mappings within the same IDAM platform. Client data is fully isolated and each entity maintains an independent configuration and audit trail.

HOW IT WORKS

The entire lifecycle is managed through a five-step automated process, with no manual intervention required at any stage.

1

A lifecycle event is triggered in your HRMS

A new hire confirmation, a department transfer or an exit recorded in your connected HR system triggers the IDAM process automatically. No manual submission is required from the HR team.

2

Employee data is ingested into the IDAM platform

IDAM pulls the relevant employee record via API or scheduled batch sync. The data is validated before any further processing takes place.

3

Attribute mapping and validation is applied

HR field names are aligned to the target identity environment schema - Active Directory, Azure Entra ID or Microsoft 365 - using a configurable, client-specific mapping engine. This eliminates the need for custom development with each new HR or identity environment configuration.

4

The action is executed in on-premises Active Directory

The account is created, updated or deactivated in the target identity environment - on-premises Active Directory, Azure Entra ID or Microsoft 365 - on the next scheduled sync cycle. Where applicable, Microsoft 365 licenses are assigned or removed as part of the same action. Sync frequency is configurable per business unit, with no dependency on overnight batch windows.

5

Logs and dashboards are updated in real time

Every action is written to the audit log with a full timestamp, attributed to the HR event that triggered it. The admin dashboard and compliance reports reflect the update immediately.

KEY FEATURES

Designed for enterprises managing identity lifecycle across on-premises Active Directory, Azure Entra ID and Microsoft 365.

Build for On-Premises AD, Hybrid and any Cloud Environment Identity Stack

Designed to manage identity lifecycle across on-premises Active Directory, Azure Entra ID and Microsoft 365. IDAM operates in whichever identity environment your organisation runs today - and scales as your infrastructure evolves toward hybrid or cloud.

Automated Synchronisation

HR events trigger identity actions on a configurable sync schedule that runs as frequently as the organisation requires. Identity data remains consistent and accurate across every connected environment without manual intervention.

Dynamic Attribute Mapping

A configurable mapping engine handles differences between HR field names and AD schema for each client. No custom development is needed when field structures change.

Governance-First Role Model

Two clearly defined roles Admin and User establish clean privilege boundaries across the platform. This structure prevents configuration errors, simplifies administrator onboarding and eliminates the risk of access creep accumulating over time.

Multi-Client Isolation

Each business unit, subsidiary or location is managed as a separate client with its own configuration, ensuring complete data separation and governance independence.

Audit-Ready Architecture

Every identity action is logged with a timestamp, trigger source and change record. Compliance reports are generated from the admin dashboard without requiring manual effort.

WHERE ESII IDAM MAKES THE BIGGEST DIFFERENCE

Enterprises with frequent employee movement across on-premises, hybrid or cloud Microsoft identity environments benefit most from IDAM.

ENTERPRISE ONBOARDING

Day-one access is ready before the employee arrives

The moment HR confirms a hire in the HRMS, IDAM creates the Active Directory account, assigns role-based permissions and logs the action. The new employee arrives to a fully provisioned account, without any IT ticket having been raised.

SECURITY AND COMPLIANCE

Zero orphaned accounts after any resignation or termination

An exit recorded in the HRMS triggers immediate revocation of all Active Directory access. The audit log records the exact timestamp. Compliance teams have a clean, verifiable record for every departure, available at any time.

INTERNAL TRANSFERS

Role changes are reflected in access within the hour

Promotions, department transfers and designation changes recorded in the HRMS are automatically propagated to Active Directory. Old access permissions are removed and new ones are granted, with no manual follow-up required from the IT team.

MULTI-SITE ENTERPRISES

Consistent identity mapping across every location

Multi-client configuration allows each office, subsidiary, or business unit to maintain attribute mappings while keeping all data isolated within the same IDAM platform.

SUPPORTED ENVIRONMENTS AND INTEGRATIONS

LIVE

On-Premises Active Directory | Darwinbox | SAP SuccessFactors | Any API-enabled HRMS

FUTURE SHIPPED FEATURES

Azure Entra ID | Microsoft 365 | Configurable Scheduled Sync

See IDAM working in your environment.

mapped to your HR system, your Active Directory configuration and your Microsoft identity roadmap. No data sharing required. No infrastructure changes needed for the demonstration.

Book a Demo →

esii.in
info@esii.in
A PC Solutions IP Brand
New Delhi, India