



Identity Lifecycle & Governance Management

AccessMatrix™ Universal Identity Manager (UIM) provides a highly flexible and systematic way to manage employee access to various company IT resources based on a predetermined entitlement policy. The best identity and access management solutions are now built around the business user. While IT still provides control and oversight, the business user needs to have a fast and simple way to implement changing access requirements without the need for numerous help desk calls or IT tickets.

Automated user provisioning, automatic role management, automated access certification, and automated password reset tools mean dramatic reductions in IT operating cost and implementation. The ability to provide self-service for business users can meet the needs of the business user faster and increase the productivity of the IT department. This means lightning fast change at the lowest maintenance costs.

AccessMatrix™ Universal Identity Manager (UIM) provides a policy-driven approach to manage default access to various companies' IT resources based on user's organizational role as well as allows users to submit ad-hoc access requests subject to management approval.

Key Features

Complete Identity Management

Enables comprehensive identity lifecycle management, featuring workflow automation, identity synchronization, and reconciliation with target applications



Automated Identity Management

Streamline identity creation, updates, and removal while eliminating manual errors



Efficient Workflows

Automate approvals and processes for seamless and efficient operations

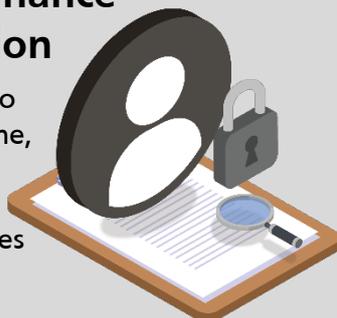


Real-Time Synchronization

Ensure accurate and up-to-date identity data across all target applications

Identity Governance & Administration

Allows organization to conduct audits anytime, ensuring compliance and securing identity management processes



Always Audit-Ready

Perform real-time audits to ensure ongoing adherence to standards



Proactive Issue Resolution

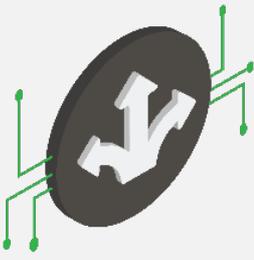
Detect and resolve inconsistencies to maintain security and compliance



Robust Governance

Strengthen organizational security with effective governance processes

Main Business Advantages



Seamless Integration and Flexibility

Leverage built-in connectors, customizable options, and Low-Code Connector Builder to integrate effortlessly and extend functionality with ease.



Ensure Compliance and Improve Governance

Separation of Duty (SoD) control and identity certification help managers and auditors oversee access rights, resolving role-resource conflicts with system admins. It ensures separation of requestor and approver roles, requiring approval for unresolved issues. Periodic reviews enforce compliance, reducing security risks from human error.



Connect to Wide Range of Target Resource

The UIM Connector Framework enables developing connectors for provisioning and reconciling on premise or cloud resources, with seamless integration of separate account and role management connectors.



Integral Component of Complete AccessMatrix™ Suite

Built on the AccessMatrix™ Suite, UIM seamlessly integrates across i-Sprint's family of IAM solutions. Customers receive the full suite, with only purchased modules enabled, allowing quick activation of additional products with minimal downtime. This ensures scalability and adaptability to evolving needs.



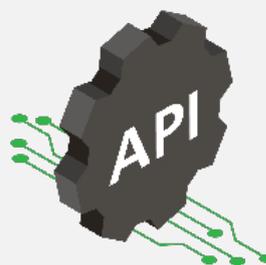
**Cost Reduction
Through Self-
Service Capability**



**Improve Internal
Employee Job
Satisfaction and
Productivity**

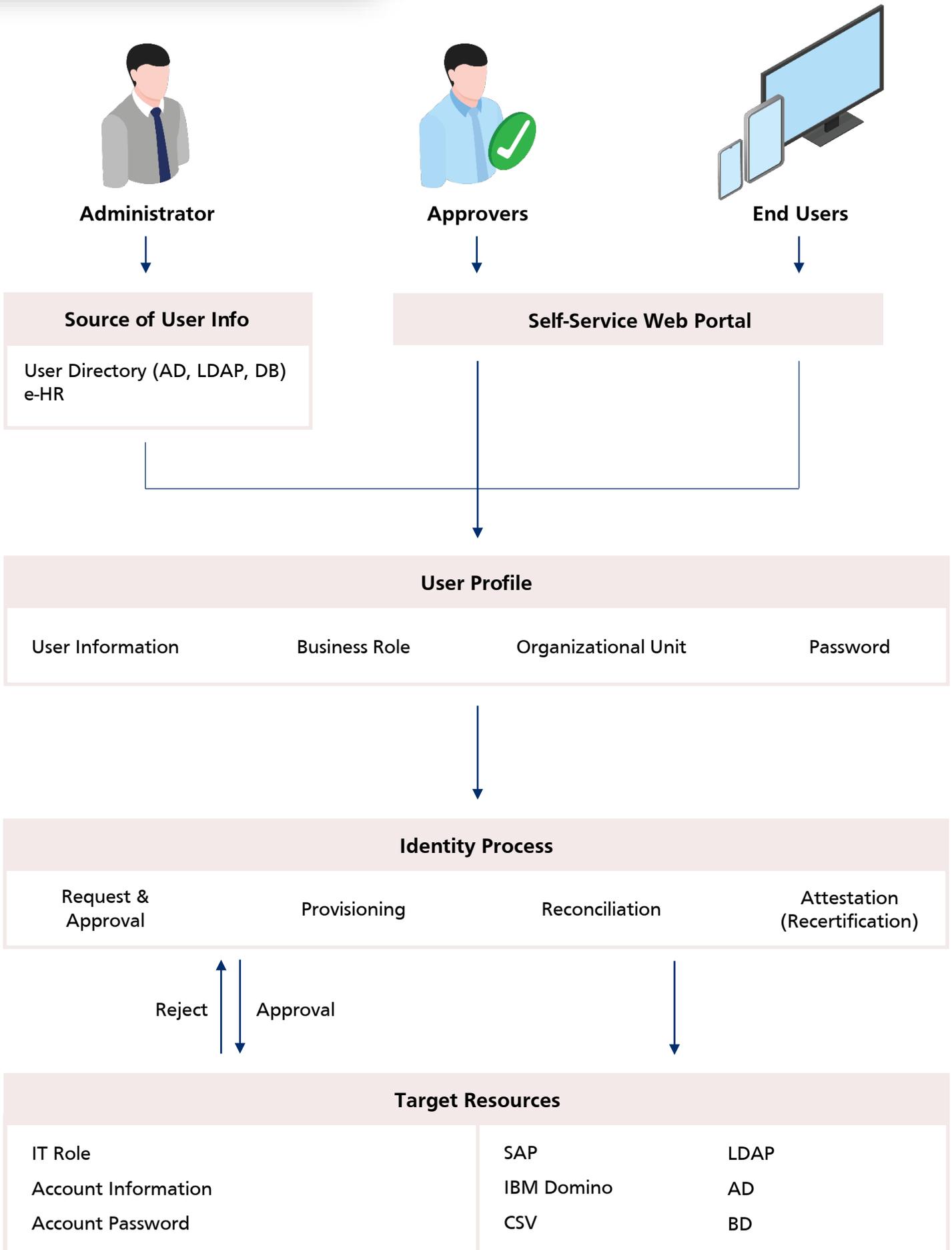


**Proven
Professional
Expertise**

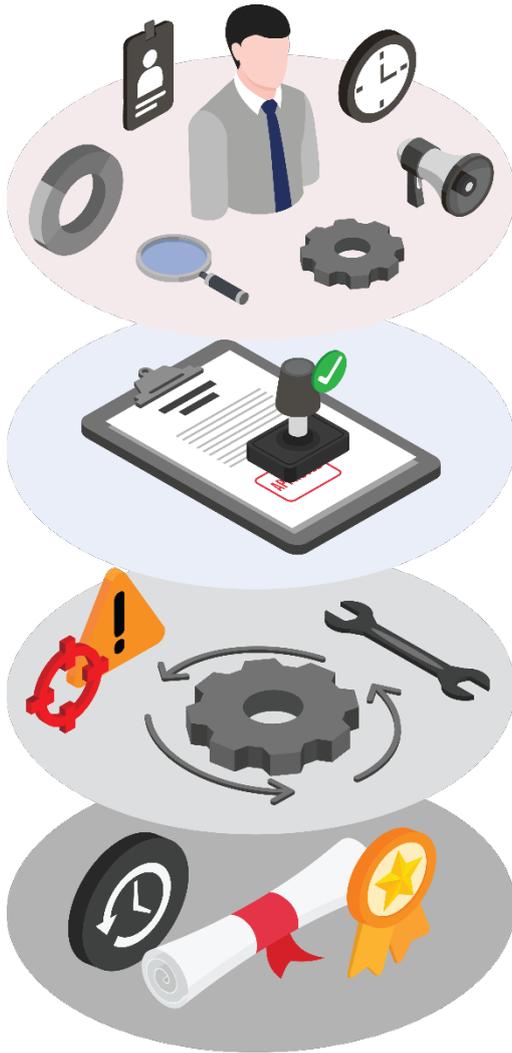


API Integration

Identity Management



Core Functionalities Processes



Provisioning (Request-based & Role-based)

Business Unit, IT, and HR departments define access rights for organizational roles, with provisioning managing updates in target applications. Access changes are triggered by role updates (e.g., hiring, reassignment, exit) or requests from administrators and employees.

Request Approval Workflow

Customizable workflow governs approvals, ensuring compliance while allowing self-service for routine requests to improve efficiency and accountability. It supports authorized delegation and reduces approval turnaround time.

Reconciliation

Proactively detects and resolves unauthorized access changes in external resources, ensuring accuracy and audit compliance. Unreconciled data are flagged for administrator actions.

Attestation (Recertification)

For broader base quality control, UIM periodically prompts users to review access requests and role-based rules. Ensuring accountability and compliance for reviewing entitlements.

System Requirements

Server OS: MS Windows Server 2022, RedHat Enterprise Linux 9.x

Application Server: Apache Tomcat and JBoss WebServer

Java Runtime: JRE 17 LTS

Database for Policy Store: MS SQL Server, Oracle RDBMS, and Oracle MySQL

Global Headquarters

Blk 750D Chai Chee Road #08-01
ESR BizPark@Chai Chee (Lobby 1)
Singapore 469004
☎ +65 6244 3900
✉ enquiry@i-sprint.com

For a complete list of our offices in
Hong Kong, Japan, Malaysia,
Thailand & United States, please visit
www.i-sprint.com/contactus



Scan for more
information

©Since 2000 i-Sprint Innovations Pte Ltd. All rights reserved.

i-Sprint, i-Sprint logo, AccessMatrix, AccessMatrix logo are registered trademarks of i-Sprint Innovations Pte Ltd. All other trademarks and registered trademarks are property of their respective owners. i-Sprint reserves the right to make changes to the specifications or other product information at any time and without prior notice.