strivacity

Strivacity Identity Lifecycle Management

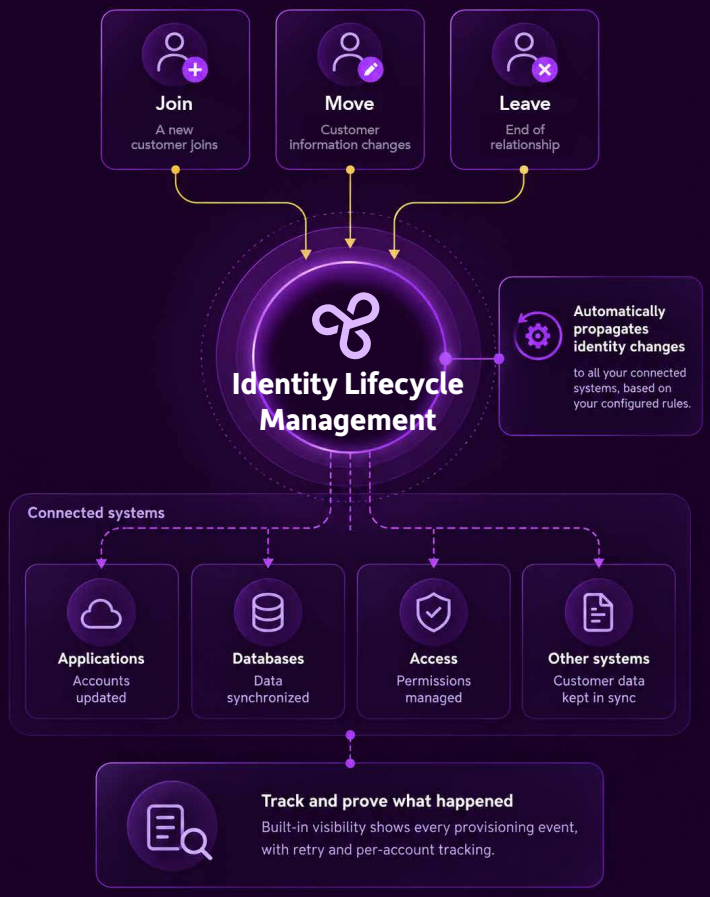
AUTOMATED IDENTITY SYNCHRONIZATION FOR CUSTOMER AND BUSINESS IDENTITIES

Keep connected systems current as customer records change

When a customer record is created, updated, or deactivated, identity changes need to propagate cleanly across all the connected systems in your environment that depend on your identity source of truth.

Without a purpose-built option, identity changes rely on a patchwork of brittle scripts and one-off integrations that can fail quietly and consume engineering time. The alternative is extending a workforce identity governance and administration (IGA) platform into customer territory, and paying enterprise prices for lifecycle management features that customer-facing identity never needed.

Strivacity Identity Lifecycle Management (LCM) propagates identity changes to your connected systems, and shows you it happened. You can configure rule-based actions, route changes, and track every provisioning event with built-in retry and per-account visibility, all on the same product that runs your customer journeys.



Benefits

Automate the full identity lifecycle

Create accounts on join, update on change, deactivate on departure, across every connected system, with built-in retry and per-account visibility.

Prove deletion across connected systems

When a relationship ends, access and data are removed across every connected system.

Keep customer data where it lives

Read identities from the database you already run. The directory connector calls out from inside your network, and all connectivity originates from your network.

Capabilities

FLEXIBLE TARGET CONFIGURATION

Configure multiple outbound targets per identity store, each with its own rules, mapping, and action logic.

CUSTOM INTEGRATION LOGIC

Actions connect to nearly any downstream system, with full extensibility for proprietary systems.

TARGETED ACTIONS

Trigger actions only on customers who meet specific conditions. Target everyone in an identity store or filter by group membership, attribute, account status, organization role, or last login

AGGREGATION FROM MULTIPLE SOURCES

Bring identity data in from external systems via API, JDBC, and LDAP.

©2026 Strivacity. All rights reserved.

Identity lifecycle orchestration in 5 steps

Detect

An identity change occurs in Strivacity or a connected upstream system.

Evaluate

Configured rules determine whether the change should trigger an action.

Queue

The system queues the appropriate provisioning, update, or deprovisioning task.

Execute

Custom action runs against the target system via API or SCIM.

Track

Status is logged per account, surfaced in the admin console, and retried if needed.

More Capabilities

Retry and resilience

Built-in retry handling for transient failures. Queue-based processing for reliable, large-scale operation.

Manual controls

Force sync for specific customers. Trigger re-provisioning on demand. Override automated decisions when business needs require.

Visibility and status tracking

Per-account provisioning status across all targets: success, failure, pending, in-progress, with detailed logs for troubleshooting.

Native to your CIAM product

No separate product to deploy. No second admin console. No additional contract. Lifecycle management lives where your customer identity already lives.

BUSINESS VALUE

- **One product for B2B and B2C lifecycles**

  Manage both business and consumer identity lifecycles end-to-end without stitching together separate tools.

- **No separate governance product to run**

  Lifecycle runs in the product your team already operates. No second console, no second contract, no specialist headcount.

- **Less to build and maintain**

  Replace per-system scripts with targets, rules, and mappings you configure in the admin console.

- **Evidence when someone asks**

  Per–account records show what identities were provisioned or removed, and when, across connected systems.



©2026 Strivacity. All rights reserved.

Identity lifecycle management components

Strivacity Identity Lifecycle Management provides a pre-built set of components for orchestrating identity changes across your environment. Each component is configurable, extensible, and operates within the same product that runs your customer journeys.

Note: *Component availability depends on release version and deployment model. JDBC-based aggregation is available from the Philadelphia release (June 2026). Check product documentation for the most current information.*

Aggregation sources

Where identity data enters Strivacity.

- **Strivacity identity store**
- **LDAP and LDAPS directories**
- **JDBC databases:**
  - **SQL Server**
  - **Oracle**
  - **PostgreSQL**
  - **MySQL**
- **REST APIs**

Action types

Operations that can be triggered by rule evaluation.

- **Create account**
- **Update account attributes**
- **Enable / disable account**
- **Prove deletion everywhere, with no hand-coded after-delete hooks**
- **Add to group / remove from group**
- **Assign / remove organization role**
- **Create downstream mailbox (e.g., Exchange)**
- **Send notification email**
- **Execute custom scriptAPI**

Operational features

Tools for running identity lifecycle management in production.

- **Per-account status dashboard**
- **Built-in retry handling for transient failures**
- **Queue-based processing for scale**
- **Manual force-sync per user or rule**
- **Audit logs of every provisioning event**
- **Delete protection cycles guard against unintended bulk deprovisioning.**

Provisioning targets

Examples of where identity changes can be propagated. For example, a student record created in a learning system can provision a directory account, a mailbox, and application access.

- **Microsoft Entra ID**
- **Microsoft Active Directory**
- **Microsoft Exchange**
- **Salesforce**
- **Learning management systems**
- **Partner and dealer portals**
- **Billing and subscription systems**
- **Custom downstream applications via API**

Security

- **OAuth 2.1 for API authentication**
- **Directory connector initiates all connections outbound. No inbound firewall rule or VPN is required.**

Sync cadences

How and when actions are triggered.

- **Event-driven**
- **Scheduled batch sync**
- **Manual force-syncmonthly cleanup)**

Protocols and standards

Aggregation protocols (inbound)

- **REST APIs**
- **LDAP and LDAPS**
- **JDBC**

Provisioning protocols (outbound)

- **REST APIs**
- **SCIM 2.0 (outbound only via custom code)**

Filter and rule conditions

Criteria that determine whether an action is triggered.

- **User attribute match (any indexed field)**
- **Group membership**
- **Organization role assignment**
- **Account status (active, disabled, pending)**
- **Last login date**
- **Time-based filters (e.g., scheduled monthly cleanup)**
- **Custom JavaScript conditions**



To learn more about how Strivacity Identity Lifecycle Management would fit your environment, contact sales@strivacity.com.

Copyright © 2026 Strivacity. All rights reserved.

ABOUT US

Strivacity is The AI Identity Company that helps brands deliver trusted digital experiences by managing agentic, customer, and partner identities in a single product. It brings identity orchestration, account opening, sign in, consent management, and fraud prevention together to reduce friction, improve conversion, and give business and security teams clear visibility into where identity drives or blocks growth. Built on a single-instance SaaS architecture with data residency by design, Strivacity helps organizations modernize customer identity while preparing for the agentic AI era.
205 Van Buren Street | Suite 120 | Herndon, VA 20170.