secorex
Powered by FIDROX

Physical Identity and Access Management (PIAM)

Enterprise Security. Automated Governance. Connected Operations.

SecoreX PIAM centralizes physical identity lifecycle, access governance, approval workflows, provisioning, and audit visibility across employees, contractors, visitors, and third parties.

Identity Lifecycle
Manage joiners, movers, leavers, badge holder data, and profile updates from a single platform.

Access Governance
Digitize requests, approvals, validations, temporary access, and policy-based controls.

System Integration
Connect with PACS, HRMS, directories, visitor systems, and enterprise applications.

Audit & Compliance
Track who requested, approved, provisioned, changed, and revoked access with full traceability.

Platform Overview

Organizations often manage physical identities and access permissions across disconnected systems, teams, and locations. This results in delays, manual effort, inconsistent controls, and audit challenges. SecoreX PIAM brings these processes onto a unified platform so enterprises can standardize identity governance and automate physical access administration.

Core capabilities

Identity Lifecycle Management

- Employee, contractor, vendor, and temporary workforce identity management
- Joiner, mover, leaver workflows
- Identity profile enrichment with configurable fields and supporting documents
- Cardholder and badge data synchronization across connected systems

Access Request and Approval Workflows

- New access requests, change requests, renewal requests, and temporary access flows
- Multi-level approvals based on role, department, site, or access type
- Policy-driven validations, escalations, and notifications

Provisioning and De-Provisioning

- Automated access provisioning to connected physical access control systems
- Access revocation during separation, transfer, expiry, or policy change
- Scheduled synchronization and bulk operations to reduce manual PACS administration

Visitor and Temporary Identity Management

- Pre-registration and host approvals for visitors and external personnel
- Temporary badge issuance, validity control, and badge return tracking
- Governed handling of consultants, auditors, service personnel, and contractors

Compliance, Audit, and Reporting

- Complete audit trail for requests, approvals, changes, and revocations
- Exception tracking and historical reporting for investigations and audits
- Operational dashboards for pending requests, expired access, and status monitoring

Integration Readiness

Physical Access Control Systems (PACS)	**HRMS and employee master systems**	**Active Directory, LDAP, SSO, and identity sources**
Visitor Management Systems	**ServiceNow and ticketing platforms** **Email, alerting, and notification services**	**Custom applications through APIs and middleware**

Business Value

- Enhances security by ensuring only authorized identities receive the right access for the right duration
- Improves compliance with governed, traceable, and auditable workflows
- Reduces turnaround time and manual effort through automation
- Provides better visibility for security, HR, facilities, and administration teams
- Scales across multi-site enterprises with complex approval and access models

Deployment fit

Ideal Use Cases

- Corporate campuses and enterprise offices
- Manufacturing plants and industrial facilities
- R&D centers and engineering environments
- Healthcare institutions and regulated facilities
- Data centers and critical infrastructure locations
- Multi-site organizations requiring centralized governance with local execution

Why Secorex PIAM

- Enterprise-focused physical identity governance platform
- Configurable workflows and approval matrix
- Integration-first architecture
- Centralized visibility across identities, badges, and access systems
- Supports automation, compliance, and operational control
- Suitable for on-premises, private cloud, and enterprise-hosted deployments

Value Proposition

SecoreX PIAM helps enterprises govern physical identities and automate access lifecycle processes across people, locations, and systems—improving security, compliance, and operational efficiency.