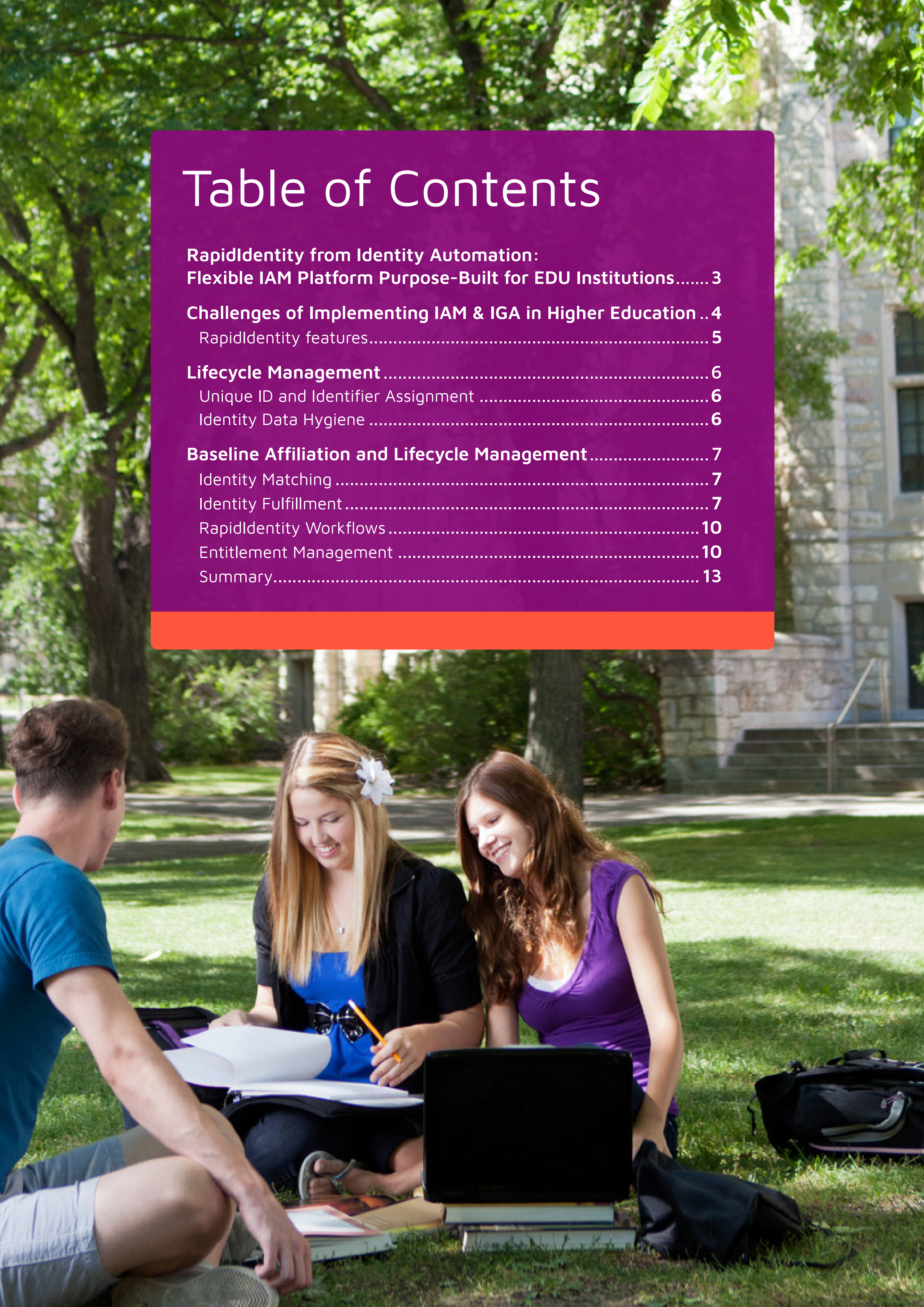
Identity Automation

RapidIdentity

Technical Overview

For Higher Education IAM and IGA

Table of Contents



RapidIdentity from Identity Automation:

Flexible IAM Platform Purpose-Built for EDU Institutions

RapidIdentity is a cloud-based IAM platform specifically designed to manage **distributed identity fabrics** across **multi-campus systems** and **complex organizational structures.** While best-of-breed approaches may offer advanced features, they are often too costly and complex for institutions to implement or maintain effectively. For a fraction of the cost, RapidIdentity delivers the **administrative flexibility** needed to empower organizations to streamline operations and scale effortlessly without locking them into overly rigid or expensive solutions.

RapidIdentity ensures a seamless user experience, enabling institutions to manage complex identity scenarios. It offers **intelligent policy automation** that allows for fast, intuitive access to the resources users need without compromising security. Whether managing identities across disparate campuses or dealing with the intricacies of federated access, RapidIdentity ensures users get the resources they need without interrupting their productivity.

Challenges of Implementing IAM and IGA in Higher Education

Higher education institutions face distinct challenges in implementing effective IAM and IGA programs due to their complex and varied environments. Unlike corporate entities, they must manage diverse user groups, including students, faculty, staff, alumni, and external partners, each with different access needs. Decentralized IT environments, where different departments or colleges may operate independently, increase complexity and can lead to inconsistent identity management practices. Additionally, a culture of openness and academic freedom can sometimes clash with the need for strict access controls and governance.

The transient nature of student populations, with frequent enrollments, graduations, and transfers, demands robust and flexible IAM/IGA solutions that can quickly adapt to these changes while ensuring compliance with regulations such as FERPA and GDPR. Limited resources—both in terms of budget and IT staff—often hinder institutions from implementing and maintaining sophisticated IAM/IGA systems. As a result, higher education institutions need cost-effective, scalable solutions that can seamlessly integrate with existing systems and processes without disrupting the institution's primary focus on education and research.

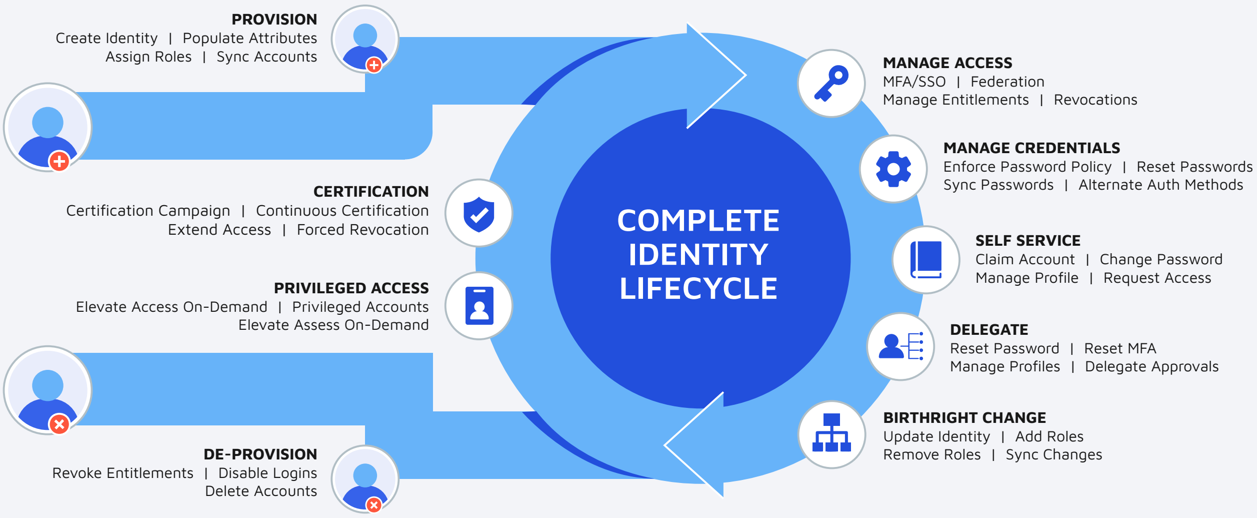
RapidIdentity bridges the gap between traditional enterprise IAM/IGA vendors and education-specific providers. **It offers enterprise-level, purpose-built features explicitly designed to address educational institutions' core IAM/IGA challenges.** Built to handle the intricacies of multi-campus systems and complex organizational structures, it allows for centralized identity management, ensuring consistent policies and seamless access management across all locations. Whether a university is managing multiple campuses or a single entity handles numerous departments, RapidIdentity can easily scale to meet these needs, providing a secure and adaptable solution for your institution's growth.

RapidIdentity features include:

- Lightweight Access Certification Workflows
- High Volume Identity Change Event enablement on Large Populations
- Rapid Integrations with On-Prem and Cloud Applications & Services
- Full Cloud Delivery
- Frictionless New Account Claiming and Onboarding
- Flexibility as both an IDP and a Federation Partner with out-of-the-box support for SAML 2.0, OAuth 2.0, OpenID Connect, WS-Federation, WS-Trust, CAS, and InCommon federation protocols.
- Native MFA with Support for 3rd Party MFA Providers such as Duo, Google, & Azure

This publication explores specific features and use cases that make RapidIdentity the ideal solution for higher education.

RapidIdentity



PROVISION
Create Identity | Populate Attributes
Assign Roles | Sync Accounts
CERTIFICATION
Certification Campaign | Continuous Certification
Extend Access | Forced Revocation
PRIVILEGED ACCESS
Elevate Access On-Demand | Privileged Accounts
Elevate Assess On-Demand
DE-PROVISION
Revoke Entitlements | Disable Logins
Delete Accounts
COMPLETE IDENTITY LIFECYCLE
MANAGE ACCESS
MFA/SSO | Federation
Manage Entitlements | Revocations
MANAGE CREDENTIALS
Enforce Password Policy | Reset Passwords
Sync Passwords | Alternate Auth Methods
SELF SERVICE
Claim Account | Change Password
Manage Profile | Request Access
DELEGATE
Reset Password | Reset MFA
Manage Profiles | Delegate Approvals
BIRTHRIGHT CHANGE
Update Identity | Add Roles
Remove Roles | Sync Changes

Lifecycle Management

Lifecycle Management includes automating and streamlining the processes for provisioning, deprovisioning, account changes, and granting new access rights for all users, including employees, students, contractors, partners, and vendors. RapidIdentity's intelligent security policy automation ensures that users can access the resources they need without delays or friction. Whether managing student access to course materials or granting secure access to sensitive internal systems, RapidIdentity optimizes the user experience without inhibiting productivity. It includes **risk-based conditional access**, dynamically enforcing security protocols based on user behavior and risk levels, and support for InCommon federation.

Unique ID and Identifier Assignment

RapidIdentity ensures that all user objects across the system receive unique IDs by pulling data from authoritative sources and creating a single, comprehensive record for each user. This record includes all relevant attributes, supporting both single and multi-valued fields. The system reconciles data to maintain unique user records, even when users are associated with multiple institutions. By implementing additional layers of data validation on top of source data processes, RapidIdentity prevents the intake of inconsistent user data.

Upon creation, user records are provisioned into the client MetaDirectory, which either creates or updates the user's account (digital identity). The MetaDirectory uses a distinguishing attribute to ensure system-wide uniqueness. An Action Set focused on generating unique usernames/IDs verifies the username within RapidIdentity and resolves any collisions using an algorithm defined by the client. When users leave the system, their accounts are disabled and moved to a designated OU, allowing the Generate Username Action Set to maintain uniqueness for both active and disabled accounts when processing new users.

Identity Data Hygiene

The IAM service incorporates multiple layers of data validation, enhancing source data processes to ensure that irregular user data is not processed.

Identity Store

RapidIdentity features a Centralized Directory service for efficient management of identity and access. Recognizing the crucial role directory services play in IAM, RapidIdentity is a secure repository for identity and access information. It handles extensive identity metadata, including affiliation data. Each identity record can include a primary affiliation and an affiliation priority. Affiliation data is integrated with the corresponding identity and managed alongside other identity attributes. When an affiliation is added, removed, or modified, the system updates the primary affiliation and priorities, triggering the necessary downstream provisioning and access workflows.

Baseline Affiliation and Lifecycle Management

Managing identities with multiple affiliations is a common challenge in higher education. RapidIdentity Lifecycle Management simplifies and automates the processes of provisioning, deprovisioning, account updates, and assigning new access rights for all types of users, including faculty, staff, students, alumni, affiliates, applicants, contractors, partners, and vendors. The system allows affiliations to be weighted and prioritized, such as in cases where students are enrolled in joint degree programs, ensuring seamless and efficient management across various roles and access needs.

Identity Matching

RapidIdentity is capable of matching identities across multiple source systems, even in the absence of a standard unique ID. For example, it recognizes when a new employee is also an alumnus. The system identifies multiple roles for a user through multi-attribute matching and validation, checking whether a set number of attributes—like email addresses or phone numbers—match. RapidIdentity can detect slight variations in character matches within the attribute pairs using an algorithm based on Levenshtein Distance. It can then either automatically merge matching identities or flag them for manual review based on pre-established business rules.

Additionally, RapidIdentity can incorporate new identity sources into the reconciliation process. It flags potentially matching identities for manual review before creating a duplicate account, ensuring accuracy and preventing errors.

Identity Fulfillment

RapidIdentity Connect enables the bidirectional flow, transformation, and validation of data between otherwise disconnected systems. This component focuses on Enterprise Application Integration (EAI), Extract, Transform, and Load (ETL) processes, and identity management provisioning. Connect operates through user-defined Action Sets, which are processed by its logic engine via a scheduler or external triggers using the RESTful API. These Action Sets contain Actions that handle data transformations and interact with external systems through various connectors or "adapters." Common adapters include text, database, LDAP, web services (API), command-line interface, email, and directory adapters.

Connect serves as the primary data integration engine between source systems, RapidIdentity, institutions, and target applications. Its built-in API gateway facilitates connections between RapidIdentity, higher education institutions, and third parties. Utilizing advanced technology, Connect ensures that data flows with the highest level of reliability and integrity to and from the RapidIdentity Data Store and Identity Store.

Account Admin Tools

The RapidIdentity Portal features a delegated user management interface that enables the assignment of administrative activities to administrators outside of the central IT team at the application layer. Delegation can also be extended to other user groups, such as faculty, if desired. For instance, a faculty manager can be granted the authority to reset passwords or perform other administrative functions for direct reports or contractors without requiring elevated rights. This approach allows managers to lead their teams effectively without IT assistance or authorization.

The portal includes a configurable People module that displays and manages identities through delegated views. These views are tailored to the individual logged into the portal and only permit the authorized administrative actions for that view. The People Module is central to RapidIdentity's capability to enable institutions to delegate identity and access administration while providing self-service functions for end users. It allows for detailed control and visibility, enabling tasks such as resetting passwords, enabling or disabling accounts, resetting authentication methods, and modifying attribute values. Additionally, some customers configure RapidIdentity for access request and approval, integrating with ITSM ticketing and tracking systems for two-way support.

Guest/Affiliate Identity Services

The Sponsorship module offers a way to manage the lifecycle of "external" user accounts, which are accounts handled outside of authoritative systems like HR or Payroll. Examples include contractors, adjuncts, and volunteers. This module allows designated sponsors to create, expire, delete, re-attest, and transfer accounts to other sponsors. It also enables managers to perform sponsor actions for accounts associated with their direct reports.

Administrators can appoint Sponsorship Administrators, who have the authority to manage any sponsored account within the system. Customer service or help desk departments often utilize this role to assist other sponsors in managing their accounts. It's important to differentiate between the user registration system and the Sponsorship module, as they serve similar purposes but are distinct components with different functionalities.

Identity Integration Services and API

Each customer has complete access to the published APIs. They can extend their functionality using Connect actions, which are available as RESTpoints and are accessible via RESTful API calls or webhooks. Users can view detailed API information in the published Product Documentation and Developer Guides or by navigating to the API URL on the tenant at https://<portal_url>/api/rest/api-docs. Only authenticated accounts with the API Management role can access this URL. The API details are in Swagger format.

Identity Management Audit and Reporting

RapidIdentity offers robust auditing capabilities that enable the evaluation of identities and entitlements against business rules and controls. It provides comprehensive audit logging, pre-built reports, and integration with Security Information and Event Management (SIEM) systems, capturing a complete audit trail and offering valuable security insights. Every action is logged in the central audit database, whether a user logs in, accesses applications, performs self-service tasks, or delegates tasks within the portal. RapidIdentity uses these activity records to generate Dashboards, Reports, and Analytics.

The system maintains a complete history of each user’s identity lifecycle, logging role and constituency changes. RapidIdentity guarantees the uniqueness of each identity throughout all phases, from initial entry to role changes and eventual re-entry. This comprehensive historical record is preserved in the metaverse system.

RapidIdentity also flags high-risk or non-compliant access requests by classifying each entitlement with data classifications and risk levels. For example, access to HR/Payroll may be flagged as sensitive due to the nature of the data. Risk levels can be assessed at various dimensions: user attributes, application data, and user access. This information helps identify access hot spots and calculate risk scores, which are stored as attributes and used to inform authentication and authorization decisions.

System administrators can configure audit retention policies to define what is logged and for how long. The RapidIdentity Dashboard module offers a histogram and grid interface to view activity over different time periods, such as today, yesterday, the last seven days, and the previous 30 days. This ensures that every action is auditable, clarifying who did what and when.

RapidIdentity includes a comprehensive set of predefined audit reports for common user activities and allows administrators to quickly generate custom reports based on specific criteria. The Connect Auditing feature enables the sending of Syslog messages to SIEM or other data collection services. Administrators can specify the Syslog level (emergency, alert, critical, error, warning, notice, info, debug) and the message to be logged. The logAuditEvent Action records events in the audit log, returning a unique event ID upon success. As the Connect data integration engine performs user provisioning and management tasks, all related actions are audited through this feature.

Account Claim

RapidIdentity offers a fully automated and customizable account claim process. This includes a configurable URL for the Account Claim page, an automatically generated Claim Code, and notifications via SMS or email. The email notification contains a unique code along with additional user-specific information such as Student User ID, Phone Number, or Zip Code, all of which can be tailored to meet client needs.

When users claim their accounts at the beginning of their identity lifecycle, they are prompted to create a password and complete any additional authentication methods required by their assigned policy. Supported authentication methods include TOTP, FIDO, PingMe, Duo push tokens, and SMS. Users may also be asked to answer a series of configurable Challenge Response questions. The number of questions required and whether users must answer them to complete the claim process are also configurable. This ensures that all production IDs created after implementation will have the necessary Challenge Response values for users to reset their passwords through RapidIdentity's self-service feature.

The account claim process can be initiated through automated provisioning from an authoritative source or as part of the sponsorship functionality. Additionally, RapidIdentity provides a robust API for the account claim process that can be used outside the RapidIdentity Portal UI. The system supports customer-defined policies for account claiming (proofing) that can be applied to various identity types based on specific policy definitions.

Password Management

RapidIdentity offers self-service tools for users to update or change their passwords and a Forgot Password/Username utility. Changing passwords through self-service can be enabled or disabled based on user roles or attributes, allowing for customized access control. If it's inappropriate for certain users to reset their passwords, RapidIdentity supports alternative processes.

The Forgot My Password utility guides users through a predefined process to reset their passwords. RapidIdentity provides various tools and communication methods for password resets, including notifications for upcoming expiration warnings. These notifications are customizable and can be sent via text message or email.

On the RapidIdentity Login Page, users can access a password reset link with a custom workflow that may include tokens, one-time passwords sent via email or text, pictographs, WebAuthN Passkeys, or security questions. Additionally, RapidIdentity supports password screening integration, which checks passwords against known breaches to ensure they are not compromised or too weak.

RapidIdentity Workflows

Workflows streamline Identity Governance tasks by offering IT, auditors, and managers clear visibility into employee access levels and ensuring security through time-based certification, sponsorship, and re-attestation. RapidIdentity allows administrators to quickly set up automated processes for managing entitlement access triggered by system events, user requests, or other factors. Clients retain full control over resource access, including who can request and approve access.

Completed workflows can automate actions such as provisioning, deprovisioning, changing entitlement access, and updating user attributes. RapidIdentity supports complex request and approval workflows, including groups of approvers for entitlements or entitlement sets and multi-stage approval processes. Additionally, administrators can configure automated, time-based workflows to update account statuses or de-provision users, ensuring that accounts are properly maintained, recertified, or removed when no longer needed.

Entitlement Management

Complete access certification by allowing managers and resource owners to periodically review and verify user entitlements, ensuring that access remains appropriate and compliant with policies. In RapidIdentity, attestation is an ongoing process designed to help clients reduce risk.

RapidIdentity offers an interface to view and configure entitlements and workflows. Employees and Admin Users can access three distinct Request interfaces: My Entitlements, Catalog, and Workflows. Each interface provides various functions for certification and attestation, including:

- **Correlating Access**: Match employees with their system and application access, assess associated risks, and review access deemed risky or inappropriate.

- **Automating Certification**: Automate certification based on default entitlements linked to user roles and attributes and delegate exceptions to relevant business system owners.

- **Continuous Access Certification**: Conduct periodic certification campaigns swiftly, in hours rather than weeks. Review a concise list of entitlements set to expire during the campaign rather than thousands at once.

- **Ad-Hoc Certifications**: Initiate, execute, and monitor out-of-cycle certification campaigns statewide, by agency, or by application. These campaigns address new system ownership, policy changes, or evolving compliance needs with ease.

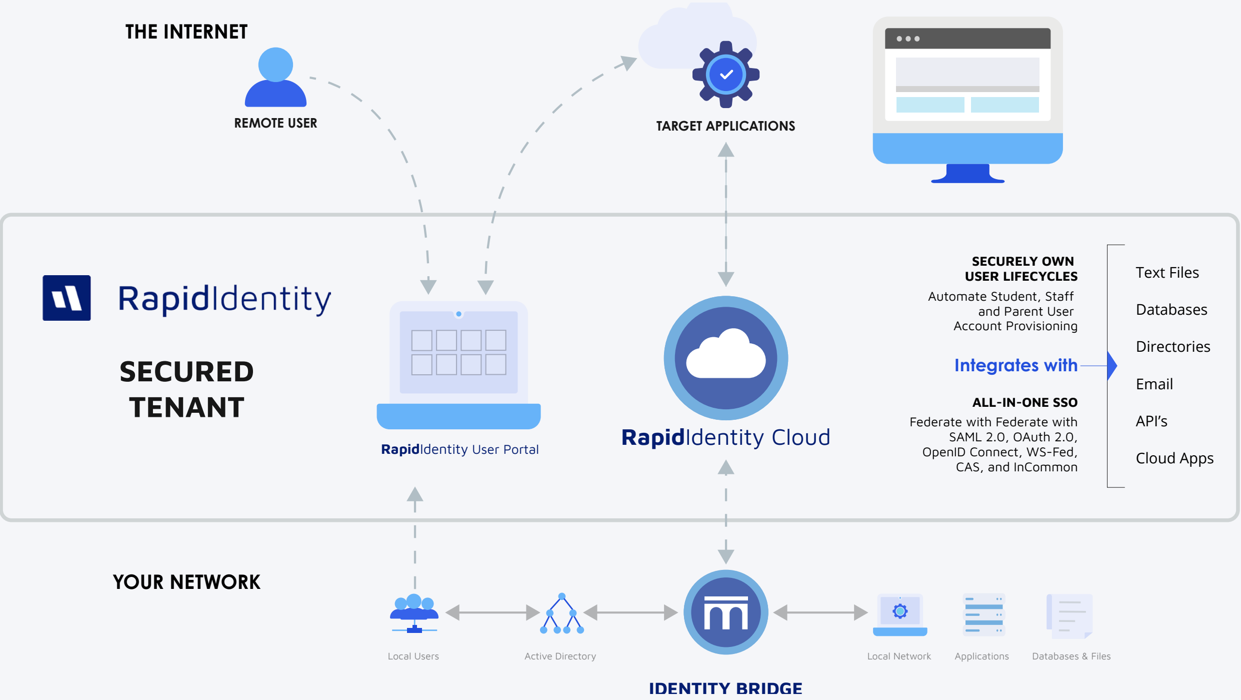
- **Time-Based Certifications**: Implement time limits on entitlements, automatically notifying system owners as expiration dates approach. Create annual certification campaigns by selecting a start date and duration, with automatic access revocation at the end of the campaign.

- **Forced Expiration**: Automatically revoke entitlements at a specific date or time for a more controlled approach than traditional certification processes.

- **Temporary Access Extensions**: Extend entitlement deadlines by up to a week for individuals or groups to assist resource supervisors.

- **One-Time Access with Forced Revocation**: Grant one-time, time-limited elevated privileges with approval workflows that can be fully or partially automated.

RapidIdentity
Architectural Diagram



Integration Capability

RapidIdentity has extensibility in connector capability through building upon generic adapters (such as web services) and a full SDK for ground-up, custom adapter development. In most cases, starting with one of the base adapters and providing specific functionality meets the needs of most integration requirements. Integrations with specific systems, such as multiple on-premise Active Directory domains, Azure AD, Microsoft 365 (formerly Office 365), and G Suite, can be handled through Connect using various adapters such as the Active Directory adapter, LDAP, Web Services (via Graph API from Microsoft), and a G Suite adapter (that extends to allow full Google API capability to invoke any API call provided by Google). RapidIdentity does not depend on provisioning utilities for Microsoft EntraID (such as Azure AD Connect) or GADS/GAPS for G Suite. Both systems are provisioned natively using secure API calls provided by the respective platform.

RapidIdentity connectors commonly used in higher education:

- Active Directory
- AWS
- Command Line Interface (CLI)
- Database
- Force.com
- Google Workspace
- LDAP
- Office 365/EntraID
- Portal
- QuickSchools
- ServiceNow
- SharePoint
- Text
- Web Services
- Workday

Some of these connectors are more generic in nature and can serve as a foundation for a more comprehensive connector with specific capabilities. These connectors are commonly used for Ellucian and other sources of Authority. For example, the Web Services adapter can support both RESTful and SOAP-based web services calls and includes the following defined actions in raw format:

- HTTP Record Fields
- httpDELETE
- httpGET
- httpHEAD
- httpOPTIONS
- httpPATCH
- httpPOST
- httpPUT

Connect serves as the primary data integration engine between source systems, RapidIdentity, institutions, and target applications. The built-in API gateway facilitates connections between RapidIdentity, higher education institutions, and third parties. Connect implements cutting-edge technology that enables data to flow with the highest level of reliability and integrity to and from the Identity Hub.

Summary

RapidIdentity from Identity Automation offers a comprehensive, cloud-based IAM platform tailored to the unique needs of educational institutions. It simplifies identity management across complex, multi-campus environments while delivering the flexibility and scalability necessary to meet the evolving challenges in higher education. RapidIdentity's robust features—ranging from intelligent policy automation and seamless user experiences to advanced identity lifecycle management and extensive integration capabilities—empower institutions to enhance security and operational efficiency without the high costs or complexity of traditional enterprise solutions. RapidIdentity ensures institutions can focus on their core mission of education and research by addressing the specific identity and access management requirements of higher education.

Identity
Automation

FOR MORE INFORMATION CONTACT
sales@identityautomation.com
877.221.8401
www.identityautomation.com