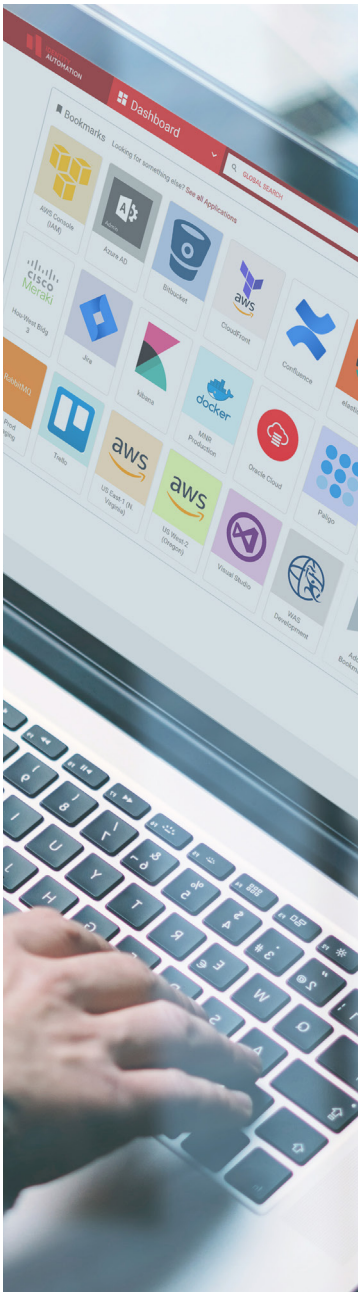
IDENTITY AUTOMATION

RAPIDIDENTITY
PLATFORM GUIDE

Contents



Modern Challenges Require Modern Solutions

There was a time when Identity and Access Management (IAM) tools could afford to be limited in purpose: preventing unauthorized access to secure resources within the organization.

Yet, the pace of technological change has disrupted every industry, every organization, and every organizational area. And IAM platforms are no exception. In addition to employees, a wide range of individuals outside of the organization now require access, including customers, partners, suppliers, and contractors.

So, the core IAM technology in many systems evolved to include identity provisioning, as well as the ability to authenticate, authorize, and audit. These expanded capabilities proved adequate for organizations as long as they had well-funded IT teams who dedicated over half of their time to low-value/high-volume tasks.

However, effectively creating and managing accounts securely, efficiently, and at scale turned out to be overwhelming due to the manual processes, scripts, and poorly integrated point solutions. Furthermore, what many systems lacked was the ability to effectively manage identities according to the reality of change.

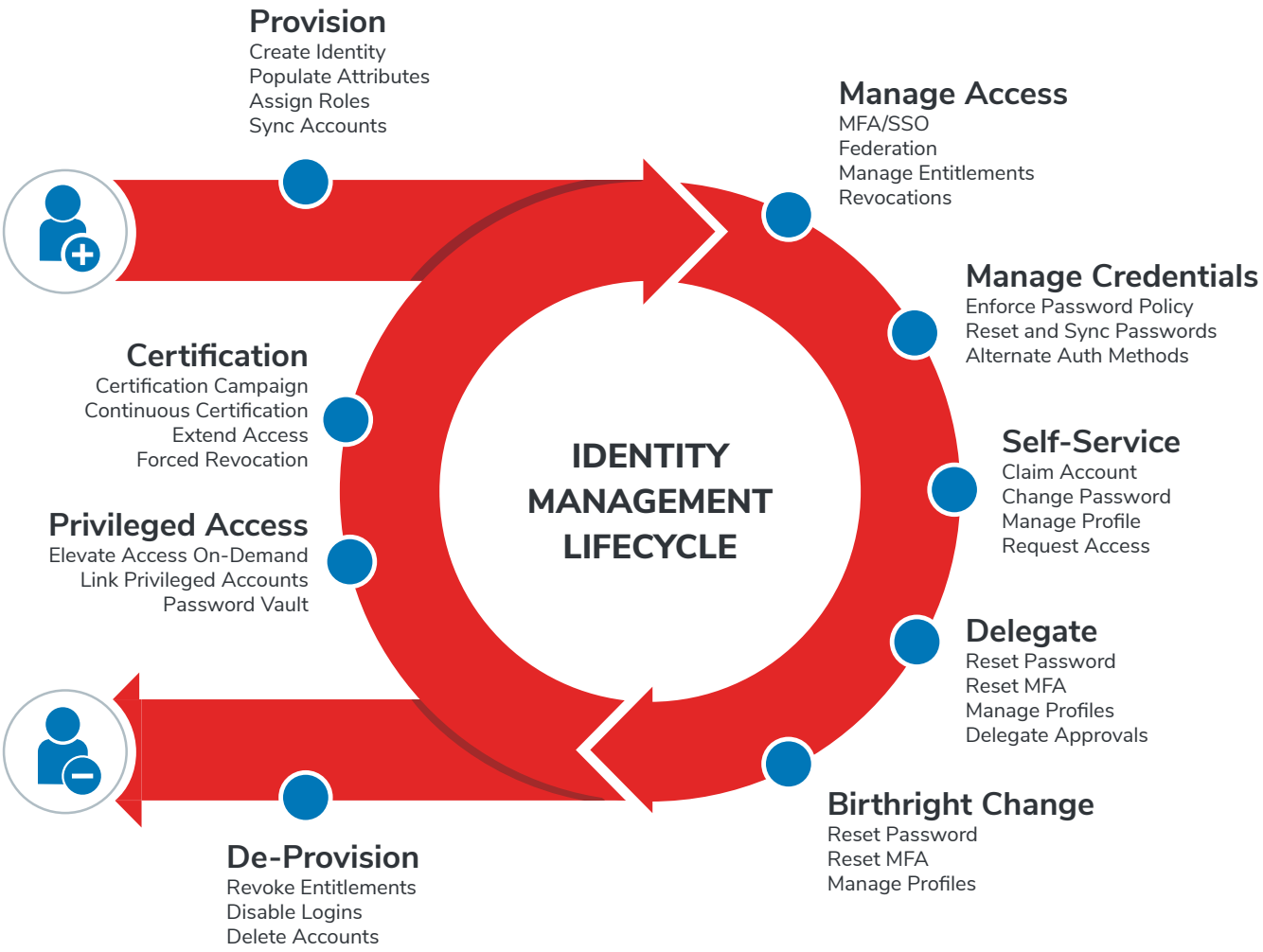
The only way to truly empower your organization— to enable a seamless experience for all users, while simultaneously limiting access risk— is identity lifecycle management. Identity lifecycle management is the ability to manage users and their accounts across systems based on well-defined and automated processes.

Identity Automation provides a comprehensive solution for your identity lifecycle management strategy, and our mission is to make it easy for organizations to scale, embrace security, and limit risks.

Our IAM product, RapidIdentity, automates the full account lifecycle of all users, closing security gaps in identity and access controls and boosting end-user productivity. We help public service organizations secure their staff and communities by taking an identity lifecycle approach to cybersecurity.

RapidIdentity

RapidIdentity is a platform that helps organizations address their complete identity and access management needs. The RapidIdentity platform empowers organizations to manage the entire lifecycle of identities—from automatically provisioning new user accounts to providing secure authentication, managing credentials and role changes, protecting privileged access, enabling delegated management and self-service, delivering single sign-on, ensuring access certification, and more— all the way to deprovisioning access when an individual leaves the organization.



PROVISIONING IS JUST THE BEGINNING

Many IAM platforms merely provide the first step in the identity lifecycle: provisioning of identities. However, this basic approach can hinder your organization because it lacks the sophistication to handle real-world situations. Consideration must be given to the entire lifecycle as it reflects the reality of organizational needs: identities tend to change roles, need temporary access, require fringe entitlements for long-term projects, and then must be deprovisioned in an automated way. The unique lifecycle needs of contractors, vendors, partners, contingent workers, and other external users must also be considered. RapidIdentity has the ability to automate the lifecycle of all users in a single solution.

Additionally, RapidIdentity is one of the few IAM solutions that combines access management with a lifecycle approach, a product feature that reduces unnecessary complexity and expense, since there is no need to purchase and integrate multiple IAM solutions.

ACCOUNT FOR EVERY ACCESS EXCEPTION

RapidIdentity utilizes both Role-Based Access Control (RBAC, i.e. IT Systems Administrator role has automatic mid-level access to certain IT systems) and Attribute-Based Access Control (ABAC, i.e. more fine-grained access control, such as providing extended access to IT Systems Administrators at the Central office). Each one has its merits and benefits for managing access rights in specific situations.

Yet, RapidIdentity takes access management a step further by caring for exceptions.

All organizations have exception or edge use cases that arise, in which access to an application or system cannot be determined solely from the user's standard attributes. Certain access will inevitably be considered special and granted only under particular conditions, such as for limited time periods, special projects, extraordinary circumstances, or emergency situations.

These account exceptions are a natural and important part of creating value, yet they tend to be one of the most overlooked parts of access management. For example, what if an organization's IT Director needs periodic access to the finance system, such as when he or she is planning the department's annual budget? The common access-granting solution calls for creating a new Finance role for the IT Director using RBAC and ABAC static membership tools. However, this process is not the most efficient, as it requires manual monitoring and management.

RapidIdentity ensures this kind of nuance is accounted for and addressed through an approach called Just In Time (JIT) Access—granting access to applications or systems for predetermined periods of time, only when needed. A JIT approach streamlines the process for granting user access, without having to submit help tickets, convene committees, or wait days to assess the request up through the managerial chain of command. It is also a massive productivity booster that enables employees to get business tasks done faster, but without compromising security.

POWER AT ANY SCALE

Today, digital environments must support a growing number of users, devices, and applications. And, this will only increase as your organization rolls out additional digital services and new partners, contractors, vendors, and consumers need access to your systems and data.

RapidIdentity was designed for deployments of any size, with proven support for 1,000 to 10 million users. Furthermore, the power to scale with RapidIdentity does not come at the cost of speed or flexibility. The platform ensures high-availability and speed—no matter how many users— and leverages Amazon's AWS platform to enable fully automated, dynamic scaling.

DESIGNED FOR PUBLIC SERVICE AND EDUCATION

The problem is that nearly all of today's commercial IAM systems were only designed to address commercial enterprise use cases out-of-the-box. Because these IAM systems are not flexible enough to address all of a public service organization's identity challenges, expensive customization and inelegant workarounds must be implemented in an attempt to make these solutions "work". As a result, the path to addressing all of an organization's needs is filled with compromise, and in the end, many issues may simply go unaddressed. So, when a public service organization starts with an enterprise IAM system designed by a software vendor that is unfamiliar with the respective spaces, it can be a very costly approach.

The challenge is that public service organizations handle massive amounts of sensitive, personal information. Such information includes constituent, student, staff, faculty, and patient contact information, as well as financial and credit data and protected health information.

In addition to the previously described benefits, RapidIdentity meets these challenges in unique ways:

Remove Bottlenecks

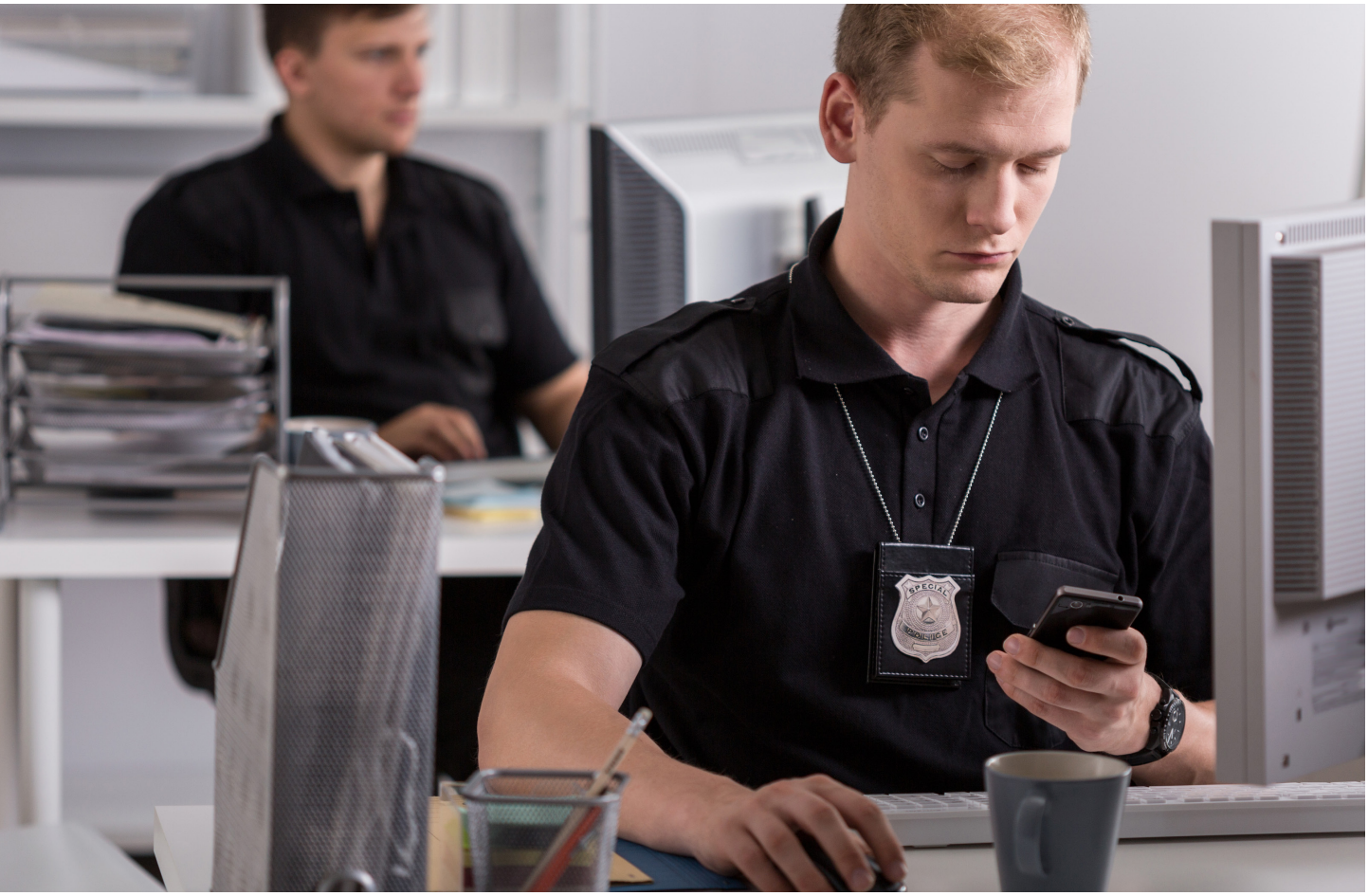
RapidIdentity provides "delegated administration," which enables users with the proper authorization to perform actions on behalf of other users. This capability empowers non-IT organizational users to perform administrative tasks in a secure and guided fashion, eliminating a bottleneck for approvers. For example, if a college library wanted to provide computer access to the public, it would be unwieldy for IT to handle the volume of temporary access requests. However, with delegated administration, library staff can easily provide temporary access for public users without engaging IT. Delegated administration has the added effect of improving the security posture of the entire organization because, although delegation pushes authorization further through the hierarchy, this does not negatively impact control as all policies are still centralized.

Streamlines Management of Multiple Affiliations

RapidIdentity overcomes the challenges of managing users with multiple accounts by intelligently detecting individual users with multiple affiliations (roles) and merging those roles into a single, unified account. This can cut the help desk burden significantly, as users only need to remember a single set of credentials for all their activities. A common example from Higher Education is a student taking continuing education classes who also works for the university as a Teacher's Assistant. The same identity is both a student and an employee. While cases like this are extremely common in Higher Ed, unfortunately, most commercial IAM solutions are not designed to handle them. In fact, these legacy solutions treat these unique identities as different

users, resulting in users having to manage multiple credentials in both Active Directory and downstream systems, and IT having to provision and manage all those credentials.

RapidIdentity solves this challenge in a unique way by recognizing multiple roles per individual user using multi-attribute matching and validation. This allows the system to discover whether or not a predetermined number of attributes attached to a particular identity, such as email address or phone number, match. From there, RapidIdentity either automatically merges matching accounts or flags them for IT to consider merging, depending on pre-established business rules. By having one account for multiple roles—it's easier on the user and far easier on help desk staff.



RapidIdentity Offerings

RapidIdentity's extensive set of capabilities are grouped into the three pillars of IAM: Lifecycle, Governance, and Authentication. These three offerings are designed to meet the needs of any organization, no matter where they are on their lifecycle journey. The capability descriptions and their included features are outlined below.

LIFECYCLE

RapidIdentity Lifecycle automates and streamlines the full identity lifecycle for all users, including employees, contractors, partners, vendors, and customers, while enabling end-users to manage their own accounts and passwords according to policy. Identity lifecycle management for end users can be delivered into key production systems, including directory services, on-premise applications, and cloud applications.

With RapidIdentity Lifecycle, user account creation, location mapping, attribute updates, organizational unit moves, group memberships, and user account renames, disables and deletions can all be automated. In doing so, RapidIdentity Lifecycle closes security gaps in an organization's identity and access controls and boosts end-user productivity.

FEATURES INCLUDE:

Automated Provisioning and Deprovisioning
Fully automate identity creation at scale and ensure user accounts are managed from cradle to grave. RapidIdentity supports SAML, JIT, SCIM 2.0, and SPML provisioning standards.

Sponsorship for Non-Employee Populations
The same level of identity lifecycle management for contractors, partners, and other external users who do not exist in authoritative systems as full-time employees.

Granular Group Management
Remove the burden of manually managing group access with support for static and dynamic group assignments, inclusions and exclusions filtering, and nested group memberships.

Delegated Administration and End-User Self-Service
Put control of new account creation, role and group assignment, and access requests in the hands of business managers. Empower users to directly request additional or elevated access.

Dynamic Role Management
Automatically place users in correct groups, using role-and attribute-base provisioning policies to add and remove access rights.

Enterprise-Ready Integrations
Connect authoritative source and target systems (on-premises and cloud-based) with pre-built or custom-built connectors using Identity Automation's Software Development Kit (SDK). Integration options include: Text/Flat File (csv, xml), LDAP (AD, OpenLDAP, Open Directory, eDirectory, etc.), Database (via JDBC), Web Services (SOAP/REST), Command Line Interface (CLI).

GOVERNANCE

RapidIdentity Governance provides IT, auditors, and managers with clear insight into which employees have what access and helps ensure security through time-based certification, sponsorship, and re-attestation.

RapidIdentity Governance allows for campaign-based, as well as time-based certifications for continuous access certification. With RapidIdentity Governance, business owners gain visibility to who has access to their resources and are empowered to certify (or de-certify) that access.

FEATURES INCLUDE:

Access Management
Enforce least privilege access, while ensuring users have the access they need with robust self-service workflows. Execute time-based, role-based, annual, and ad-hoc access certification campaigns, while empowering business system owners to control them all.

Complex SOD Policy Handling
Eliminate conflicts of interest and control failures by implementing static and dynamic policies that enforce separation of duties (SOD) at a fine-grained application level.

Orphaned Account Detection
Alleviate concerns surrounding orphan and rogue accounts with reporting that automatically identifies these accounts in target systems.

API Password Management
Eliminate hard-coded credentials in application code and scripts through use of secure REST API calls.

Shared and Emergency Privileged Accounts
Enable users to request temporary access to shared and emergency privileged accounts in the event of "break-glass" situations.

Audit Logging and Reporting
Capture a complete compliance audit trail and gain security insights with comprehensive audit logging, pre-built reporting, and integration with security analytic systems, such as SIEM.

AUTHENTICATON (MFA & SSO)

RapidIdentity Authentication helps organizations boost productivity with secure, Single Sign-On (SSO) access to on-premise and cloud-based systems using industry standard federation protocols and alternative methods, as well as increase security with Multi-Factor Authentication (MFA) that confirms a user's identity before providing that access.

With RapidIdentity Authentication, organizations can replace passwords altogether and/or add an extra layer of protection for devices and Federation-based authentication, including AD, offline desktop, on-premise and cloud applications, employee and customer portals, and remote access using VPN and other technologies. RapidIdentity Authentication also supports the broadest range of authentication methods available, including the latest frictionless smartphone based technologies and risk-based authentication.

FEATURES INCLUDE:

Secure Remote Access and VPN Logins
Safeguard company data & systems being accessed via remote access solutions (VPNs, portals, VDIs, RDs, SSH, etc), and verify the identities of all remote users.

Instantly Connect to Virtual Environments
Seamlessly perform secure, fast user-switching and direct authentication to Microsoft, RDS, Citrix® XenApp, and XenDesktop, as well as to VMware® Horizon.

Multi-Factor Authentication for Windows Login
Deploy the right mix of authentication factors, while providing your users with fast, secure Windows logon.

Adaptive Multi-Factor Authentication
Require stronger, additional, and/or separate authentication methods based on conditions, such as user role, resource importance, day of week, time of day, and location, with an extra security layer for higher risk transactions, such as EPCS.

Strong Authentication for Windows Clients and Shared Workstations
Eliminate the need for users to log in again to access locally installed, virtual, or web applications once logged into their Windows desktop, thin-client, zerofootprint client, and local and remote applications, such as Citrix.

Configurable Single Sign-On
Provide users one-click access to thousands of cloud-based and on-premises applications and services with the ability to hide, remove, and organize quick-launch icons. integration options: SAML 2.0, OAuth, OpenID Connect, and Form Fill.

User-Friendly Self-Service Capabilities
Empower users to reset passwords across connected systems, manage their profiles and accounts, and make access requests.

Mobile Support
Give users SSO access to cloud-based apps from iOS, Android, and other mobile devices. RapidIdentity also supports SSO at the mobile application level with SAML-enabled mobile applications.

SUPPORTED MFA FACTORS

Identity Automation supports the broadest selection of authentication methods in the marketplace, so you can balance security, compliance requirements, and user experience. In addition, MFA in RapidIdentity Authentication can leverage existing security investments resulting in swift deployments with minimal end-user impact or training.

RAPIDIDENTITY PORTAL SUPPORTED AUTHENTICATION METHODS

Ping-Me (Push Notification), OTP (excluding hard tokens), FIDO, QR Code, Pictograph, Social Login, Challenge Questions

DEVICE LOGON WORKFLOWS & SUPPORTED AUTHENTICATION METHODS

Windows
RFID, Contactless Cards, Biometrics (fingerprint), PKI Smart Cards, FIDO, Ping-Me (Push Notification), OTP, Challenge Questions, Bluetooth

Mac OS
FIDO, Ping-Me (Push Notification), OTP, Challenge Questions, Bluetooth

Dell Wyse Thin Client
Ping-Me (Push Notification), OTP, Challenge Questions, USB passthrough to VDI Desktops for Contactless Cards & PKI Smart Cards

Linux
OTP, PKI Smart Cards

ADVANCED AUTHENTICATION WORKFLOWS & SUPPORTED INTEGRATIONS

Physical Device Login
Windows (10; server 2012, 2016, 2019), MacOS, Linux

Remote Authentication in Dial-In User Service (RADIUS)
Virtual Private Networks, 802.1X Wifi

Virtual Desktop Interface (VDI)
Ping-me (Push Notification), OTP, Challenge Questions, USB passthrough to VDI Desktops for Contactless Cards & PKI Smart Cards

Application Program Interface (API)
Virtual Private Networks (where applicable), Step-up Authentication for custom development/web portals

Enterprise Single Sign On (eSSO)
Windows (10; server 2012, 2016, 2019)

AUTHENTICATION METHOD DEFINITIONS

Push Authentication
Known as RapidIdentity PingMe within RapidIdentity, this method sends out-of-band push notifications to a pre-registered mobile phone or other device.

U2F FIDO Tokens
Universal 2nd Factor, or U2F, is an emerging universal standard for tokens with native support in platforms and browsers. U2F tokens are typically used for web-based access and Windows logon.

One Time Password (hard token, soft token, SMS, email, backup codes)
OTPs are unique passwords that are only valid for a single login session and defined period of time.

RFID
Radio Frequency Identification (RFID) utilizes radio waves to communicate a unique identifier between a tag embedded in an RFID card and an RFID reader to verify a user's identity and grant access.

Fingerprint Biometrics
A form of Biometric Authentication, this method automatically compares a user's fingerprint to a stored fingerprint template to validate a user's identity.

Bluetooth Authentication
This method leverages Bluetooth Low Energy (BLE) technology to enable users to effortlessly lock and unlock their computers when they approach or leave.

Smart Cards (contact / contactless)
Smart cards contain a cryptographic module that facilitates the generation and security of public key infrastructure (PKI) keys and certificates that are used for authentication.

Magnetic Stripe / 2D Barcode
Cards utilizing magnetic stripe or barcode technology are presented to and read by a magnetic stripe or optical reader.

Challenge Response Questions
Utilizes previously answered challenge questions to authenticate a user and can be configured to be used in lieu of a password or to reset "something" a user should know, like a PIN or a password.

QR Code
A QR code on a printed badge acts as a contactless card; however, instead of using a traditional card reader, a computer's internal camera is used to read the QR code badge.

Pictograph
Instead of entering username and password credentials, users select the images that comprise their password from a pool of images. This method is ideal for younger users, such as K-5 students.

Social Login
Enables end-users to conveniently register and log in to sites and user portals using their existing social network identities from Facebook, Twitter, Google+, and LinkedIn.

Use Cases

K-12 EDUCATION

There are never enough learning days in a school year, so any day lost, for a teacher or student, is a missed opportunity. A large K-12 school district with 58,000 students and 2,000+ teachers and administrators needed a guaranteed "zero day start" for both teachers and students. The school district's legacy IAM system was manually-driven and lacked fully-automated lifecycle management functionality. Despite weeks of preparation from the IT Systems team, the first days of the new school year were fraught with issues: several new teachers failed to have accounts established and lacked access to required resources, while a number of students who had dropped classes were still assigned incorrectly and had to wait an entire day to be properly placed. Furthermore, because users lacked the ability to reset their own passwords, the help desk was swamped with requests.

Today, with RapidIdentity deployed as a complete IAM platform, the accurate provisioning of user accounts is now automated and completed in hours, not weeks. Additionally, self-service adjustments to student accounts are now quickly completed by the school's end-users, counselors, and teachers themselves, without the need for constant IT support.

HIGHER EDUCATION

The constant onboarding of new students at a Texas college was an overwhelming burden. On top of simple onboarding, the college had a strategic goal of expanding to valuable cloud services and applications for students and faculty. Their legacy IAM, however, made this all but impossible to manage accounts with speed and efficiency.

Yet, after implementing RapidIdentity, IT was finally able to focus on strategic objectives. They were able to quickly introduce and manage more SaaS offerings, as well as provide a better user experience, with no incremental burden to IT's workload. Thanks to SSO and self-service password reset capabilities, the number of IT help desk calls dropped from 90,000 to 45,000 per year, representing major annual cost savings. Finally, the automated deprovisioning capability also eliminated "license creep" by deprovisioning un-used or outdated entitlements.

STATE AND LOCAL GOVERNMENT

In order to stay compliant with Payment Card Industry (PCI) and Criminal Justice Information Services Security (CJIS) regulations, a city government had an existing MFA system in place for its roughly 100 police officers. However, this solution required multiple logins per device and application, adding frustration and consuming valuable time. When the city decided to roll out MFA beyond the police officers to over 500 users, they knew the existing solution was too limited to meet their needs. However, when looking at MFA vendors, the majority had the same limitations. For example, many MFA vendors could not reuse the city's existing security investment in RFID badges.

RapidIdentity provided the city with the MFA methods they needed to stay CJIS compliant, while also allowing employees flexibility, depending on their type of work. For example, some departments utilize hard

token OTPs, while single-location departments, such as administrators and finance use RFID badges to autthenticate to their Windows devices. On the other hand, mobile staff, such as police officers, use OTP soft tokens or Push Authentication to login. Ultimately, RapidIdentity MFA enabled the city to remain CJIS and PCI compliant, while also increasing efficiency and enhancing the user experience for staff.

HEALTHCARE

A medical center was experiencing decreased operational efficiency issues in the form of clinician productivity: The clinical staff was experiencing a frustrating number of retry errors when they attempted to tap in that decreased time with patients, increased cross contamination risk, as well as ongoing wrong user context issues (the user who was tapped into the machine was not necessarily the same user who was authenticated to the EMR environment). Additionally, custom scripts had to be created and maintained to clean up workstations when users logged off. In fact, their IT Systems department was spending half of their time simply maintaining the SSO.

Since implementing RapidIdentity, login times and on-screen errors have been drastically reduced because the proximity badge functionality eliminated repeated username/password input. Furthermore, patient context mismatch errors were significantly reduced, eliminating the need to manually restart programs and restoring clinician confidence in the SSO. Cross contamination risk has also been reduced in tandem with faster access to EMR. Finally, RapidIdentity increased organizational productivity, allowing clinicians to spend more time with patients and IT Systems staff to focus on other priorities.

Deployment Methods

RapidIdentity is available on-premise or in the cloud, with no sacrifices in functionality, features, or security.

ON-PREMISE

Software Appliance

CLOUD

Private Instance in Shared Infrastructure

ON-PREMISE

Packaging: Authentication, Lifecycle, Governance

CLOUD

Packaging: Authentication, Lifecycle, Governance, Rostering

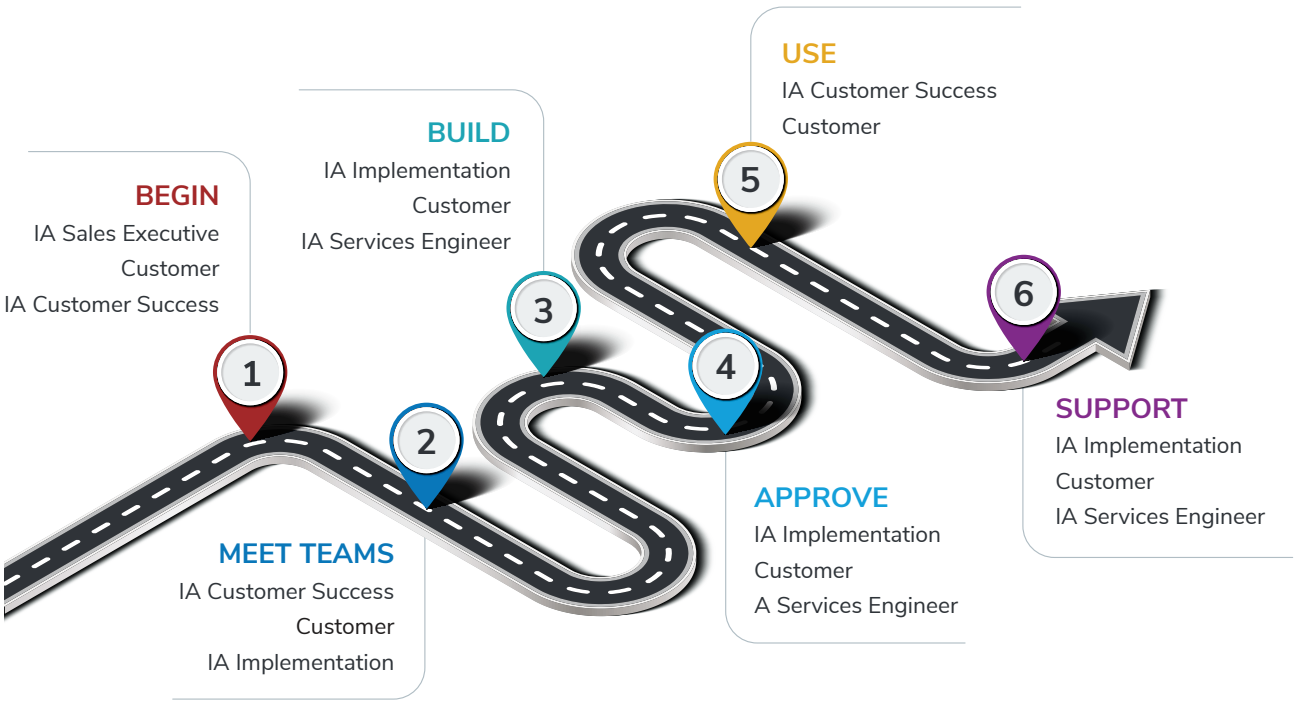
- Updates, upgrades and patches delivered seamlessly
- Leverage secure & easy to deploy Identity Bridge to connect on-premise systems
- Automated Deployments
  - Reduces time-to-value
  - Increases ROI by lowering total cost of ownership

DEPLOYMENT METHOD COMPARISON

	ON-PREM	CLOUD
Features		
Multi-Factor Authentication	✔	✔
Application Single Sign-On	✔	✔
Identity Lifecycle Management	✔	✔
Password Management	✔	✔
Identity Governance	✔	✔
Privileged Access Management	✔	✔
Audit and Reporting	✔	✔
Works with On-Premise Apps	✔	✔
Works with Cloud Apps	✔	✔
Added Capabilites		
SOC-2 Certified		✔
FERPA, COPPA, SOPPA		✔
Ongoing System Maintenance		✔
Proactive Performance Management		✔
Automatic Upgrades		✔
Service Level Commitments		✔
Prerequisites		
Virtial or Physical Machines	✔	Connectivity to on-premise resources
IT Infrastructure Operations	✔	

The Customer Journey

Our commitment to our customers extends well beyond our IAM platform. We consider ourselves partners on your digital transformation journey. We work together with you, at your pace, to build the digitally connected business environment you need to compete and win. Below is a map of the customer journey.



1. THE JOURNEY BEGINS

Customer Selects Identity Automation

- Customer Success Team sends welcome email and requests an introduction meeting (within two business days of accepting and processing PC).
- Intro Meeting is scheduled per customer's availability (within five business days of project creation).
- Project Delivery team creates an implementation plan based upon products purchased and the statement of work (SOW).

2. MEET TEAMS

Implementation Introduction and Handoff to Project Delivery

- Introduction of the RapidIdentity Delivery Team and implementation process.
- Project scope validated and initial timeline for delivery is discussed based upon customer's implementation prerequisites.
- Customer's data readiness tasks are outlined and deliverable dates are set.

3. BUILD SOLUTION

Data Readiness and Solution Architecture

- Process interviews are held and the RapidIdentity Design Document is finalized for customer approval.
- RapidIdentity executes build per approved Design Document.
- Portal configurations and any customization per customer's PO & SOW.

4. APPROVE BUILD

Customer Conducts User Acceptance Testing (UAT) per Design Document

- User Acceptance Test (UAT) Plan is developed based upon Design Document.
- Customer performs UAT (pass/fail).
- UAT Pass = Customer accepts the build and identifies date(s) for internal rollout (rollout is a customer-owned task).
- Engineer walk-through of build and Portal features and functionality.

5. USE SOFTWARE

RapidIdentity Rollout Scheduled in Customer's Production Environment

- Implementation Acceptance form is signed by the customer.
- Customer's software rollout is completed.

6. ONGOING SUPPORT

Project Delivery Handoff to Support and Customer Success

- Introduction to Support and transition to Customer Success.
- Review "How do I get help" and escalation paths.
- Professional services warranty = 30 days from UAT Pass.

Appendix

ROSTERING

Integrating LMS and digital textbooks with SIS and keeping them up-to-date can be incredibly time-consuming and error-prone. RapidIdentity Rostering completely automates the process of integrating and synchronizing student roster data with target applications, giving students immediate access to class resources.

RapidIdentity Rostering is a SaaS integration service, specifically designed for curriculum departments. RapidIdentity Rostering provides timely, reliable sharing and bidirectional syncing of student roster, grades and performance data with third-party online educational resources.

FEATURES INCLUDE:

Catalog of Predefined Application Integrations
Choose your SIS, LMS, digital textbook, and other instructional applications from our catalog of predefined rostering integrations. Provide your district's related information, and let the system do the rest.

Reliable, Secure Access
Be confident each student has access to the content they need. No more wasted time or class disruptions to resolve issues.

Accurate Accounting of Licenses
Course changes are immediately updated in vendor systems, ensuring an accurate accounting of digital learning resource licenses and helping control costs.

Data Privacy Compliance
The RapidIdentity Rostering platform is a FERPA/COPPA compliant solution hosted in AWS.

Support for IMS Global OneRoster™ Standard
Identity Automation's OneRoster consumer and provider capabilities enable integration with over 300 OneRoster certified applications.

Support for Custom Delimited File Formats
Unlike other rostering solutions, RapidIdentity Rostering supports custom file formats for both provider and consumer applications, enabling districts to automate rostering with a broad range of educational application providers.

Flexible Data Derivation & Data Filtering UI
Leverage RapidIdentity's "Metaverse" to collect and stage roster data for custom outputs to consumer and provider systems through Flat Files and API's using a flexible data derivation and data filtering UI.

EPCS

RapidIdentity EPCS is a frictionless, DEA-compliant Multi-Factor Authentication (MFA) solution for securing electronic prescription of controlled substances (EPCS) workflows.

Designed with efficiency and security in mind, RapidIdentity EPCS quickly and securely verifies clinician identities when placing prescription orders, while direct EMR integration with e-prescribing workflows gives clinicians a single, streamlined workflow for all medications. Not only does this reduce the risk of prescriptions being stolen or forged, but it decreases patient wait times by sending prescriptions directly to their pharmacy of choice.

FEATURES INCLUDE:

DEA Compliant Two-Factor Authentication
Verify clinician identities using flexible MFA methods, including biometrics, and push notifications.

Direct Prescription Delivery
Securely send medication orders directly to the pharmacy, reducing the risk of prescription tampering.

EPIC EMR Integration
Streamline clinician workflows with direct EMR integration that provides a seamless non-intrusive experience.

Two-Step Logical Access Control
Set access controls that ensure proper process is in place for giving EPCS permissions to approved providers.

Audit Logging & Reporting
Establish an audit trail that demonstrates end-to-end compliance with EPCS regulations.

Supervised Credential Enrollment
Facilitate the process of enrolling credentials and aligning with MFA modalities after identity-proofing.

GLOSSARY

Access Management: Access management refers to the processes and technologies that ensure access is granted to valid users and prohibited to invalid users by identifying, tracking, and regulating users' access to systems and apps.

Access Certification: The process of periodically validating acess rights to ensure entitlements still hold true and are still required by users.

Active Directory (AD): Microsoft developed AD as a user-identity directory service for Windows domain networks. Though proprietary, AD is included in the Windows Server operating system and is thus widely deployed.

Authentication: Authentication is a process used to prove a person's identity. There are two steps in the authentication process: identification and verification.

Biometric Authentication: Biometrics are a category of authentication methods that utilize unique biological characteristics (physical attributes or behavioral characteristics) to verify a user's identity. Biometric authentication can be broken down into static and dynamic methods. In the static category, there are fingerprint, facial, iris, and retina scans, as well as hand geometry. In the dynamic group, there are methods that focus on behavioral patterns, such as voice and/or speech patterns, typing rhythm, body resonance, and the old-fashioned signature.

Credential: An identifier employed by the user to gain access to a network such as the user's password, public key infrastructure (PKI) certificate, or biometric information (fingerprint, iris scan).

Delegated Administration: This core feature gives an organization's business users the ability to perform basic IT functions, such as new account creation, role and group assignment, and access requests, all without the capabilities and permissions typically tied to a privileged IT role.

Deprovisioning: The process of removing an identity from an ID repository and terminating access privileges.

Digital Identity: The ID itself, including the description of the user and his/her/its access privileges. ("Its" because an endpoint, such as a laptop or smartphone, can have its own digital identity.)

Entitlement: The set of attributes that specify access rights and privileges. When access is granted to an application it is known as an entitlement, and for each system a user can access, there is an individual entitlement associated with it.

Federation: Federation is a specific type of Single Sign-On that enables organizations to integrate with applications without exposing critical systems or data by leveraging a trusted party to identify and authenticate constituents. The trust has been established between the systems ahead of time to verify this mutual exchange of information.

Identity as a Service (IDaaS): Cloud-based IDaaS offers identity and access managment functionality to an organization's systems that reside on-premises and/or in the cloud.

Identity Lifecycle Management (ILM): Synonymous with automated lifecycle management (ALM), ILM refers to the set of processes and technologies for maintaining and updating digital identities, including the actual creation and management of user identities, taking appropriate actions for any changes, as well as the removal of identities across all the services and applications end users access within an organization's ecosystem.

Identity Synchronization: The process of ensuring that multiple identity stores—say, the result of an acquisition—contain consistent data for a given digital ID.

Lightweight Directory Access Protocol (LDAP): LDAP is open standards-based protocol for managing and accessing a distributed directory service, such as Microsoft's AD.

Multi-factor Authentication (MFA): MFA is defined by NIST SP 800-63-3 DRAFT as a characteristic of an authentication system or an authenticator that requires more than one authentication factor for successful authentication. MFA can be performed using a single authenticator that provides more than one factor or by a combination of authenticators that provide different factors.

Password Reset: In this context, it's a feature of an ID management system that allows users to re-establish their own passwords, relieving the administrators of the job and cutting support calls. The reset application is often accessed by the user through a browser. The application asks for a secret word or a set of questions to verify the user's identity.

Privileged Access Management (PAM): A subset of access management, PAM provides additional protection for privileged accounts, or the primary accounts that are at an administrative or system level. These are typically powerful accounts that give the user complete access to the system or application, so organizations make strong efforts to protect them. While access management refers to having the rights to certain resources or systems, PAM refers to having the rights to use privileged accounts.

Provisioning: The process of creating identities, defining their access privileges and adding them to an ID repository.

Reduced Sign-On (RSO): RSO reduces the frequency with which users are prompted to provide credentials for authentication, but true SSO is not reached, as the user still has to further authenticate. This occurs when users have a single credential, but have to authenticate multiple times with it to access applications or when specific application policies require additional authentication.

Risk-Based Authentication (RBA): Risk-based authentication dynamically adjusts authentication requirements based on the user's situation at the moment authentication is attempted. For example, when users attempt to authenticate from a geographic location or IP address not previously associated with them, those users may face additional authentication requirements.

Script: A script is a program or sequence of instructions that is interpreted or carried out by another program.

Self-Service Capabilities: A set of capabilities that allow an end user to perform basic tasks without outside help, such as resetting their own passwords or discovering their username if it has been forgotten. These automated capabilities increase productivity by providing the end user with an immediate resolution instead of having to wait for a response from an administrator to provide access.

Single Sign-On (SSO): A one-time login that permits a user to seamlessly access their complete workstation. This initial authentication could be an ID/password challenge or it could be a passwordless challenge, such as using physical or biometric means of authentication. Once a user successfully confirms his or her identity, he or she will not be prompted for an additional login when accessing applications within the single sign-on environment.

IDENTITY AUTOMATION

7102 N Sam Houston Pkwy W, Ste 300
Houston, TX 77064, USA

Phone: +1 281-220-0021
Email: info@identityautomation.com
www.identityautomation.com

IDENTITY AUTOMATION