



Identity
Automation



Proposal for

DeKalb County School District

Quote Number: Q-28671

Generated: 2/6/2025

Valid To: 6/30/2024

Notice of Confidentiality Identity Automation. All Rights Reserved.

This document is Identity Automation Proprietary and Confidential Information and is subject to the terms and conditions. Neither this document nor its contents may be revealed or disclosed to unauthorized persons or sent outside the aforementioned institution without prior written permission.

Overview

DeKalb County School District Team,

Thank you for choosing Identity Automation.

We appreciate your investment in our solution. This proposal outlines the solution we have custom tailored to address the requirements defined by your team.

You are joining hundreds of other organizations who trust Identity Automation's RapidIdentity platform to securely provide their users access to the information technology resources they need. Whether you have chosen us to meet your needs of access, authorization, administration or audit, you have selected the most flexible and broadest identity management platform available in the marketplace.

The contact information of your dedicated team can be found in the **Contacts** section.

In order to begin this project, please review the **Closure Details** page and sign the bottom of the **Governing Terms**.

Please contact me directly with any questions you may have regarding this proposal.

Thank you again for choosing Identity Automation.

April Reid
(864) 304-2789 Work
Cell
areid@idauto.net

Pricing

Pricing estimates are provided below.

Annual Subscription Cost

Product	Quantity	Unit Price	Unit Sale Price	Total
2025 Workflow K-12 Education Qualified User - Annual Subscription RID-C-WORK12	6,500	\$11.00	\$5.83	\$37,895.00
2025 Lifecycle K-12 Education Qualified User - Annual Subscription RID-C-LIFE12	6,500	\$50.60	\$26.82	\$174,330.00
2025 RI Advanced+ Support - Annual Subscription SUP-S-ADVNCNP	1	\$15,000.00	\$15,000.00	\$15,000.00
Annual Subscription Cost TOTAL:				\$227,225.00

One-Time Cost

Product	Quantity	Unit Price	Unit Sale Price	Total
Professional Services - Services Engineer (per hour) SVC-S-SVCENG	320	\$250.00	\$200.00	\$64,000.00
One-Time Cost TOTAL:				\$64,000.00

Grand Total: \$291,225.00

Sales Tax not included. Will be added at time of invoicing, if applicable.

This proposal is for the delivery of the solution as a service.

PAYMENT TERMS

- All invoices are due within 30 days of invoice date.
- Subscription fees for software products, hosting services, and support are billed for and begin on the Effective Date of this proposal.
- All One-time fees listed as Installation, Configuration, Setup Fees, Conversion Services, or Retainer Services are billed in advance.
- Professional Services are billed based on the project progress getting to 50% stage and then to 100% completion, unless the effort is under 2 weeks (80hours), in which case they will be billed in advance.
- Milestone based professional services are billed as each milestone is achieved.
- Service Units are billed up front and expire after a year.

ANNUAL RENEWAL

Subscription Term shall automatically renew for an additional 1-year term unless either party gives the other written notice of non-renewal at least 90 days prior to the end of the relevant Subscription Term.

Initial term of this Order Form (Term): 36 Months

Product and Project Description

PROJECT INTRODUCTION

- Team Identification
- Stakeholder identification
- Roles & Responsibilities
- Scope of Work (SOW)
- Communications plan
- Project Plan with associated tasks & milestones

INFRASTRUCTURE CREATION

Identity Automation may have steps a customer must take before Identity Automation can begin our work. These will be clearly defined in the SOW.

ASSESS, DESIGN & BUILD

Collaborative and iterative process between Identity Automation and Customer Stakeholders in order to meet the requirements identified in the SOW. These tasks are detailed below.

USER ACCEPTANCE TESTING (UAT)

Customer stakeholder(s) to test each of the use cases defined in the approved design document. This signifies Identity Automation has completed its work and delivered the solution as defined in the SOW. Identity Automation will close the Project.

POST UAT SUPPORT

The Identity Automation team will provide 30 days of post-UAT support for issues during customer deployment which fall within the SOW. This support timetable begins the day after successful UAT.

DEPLOY SOLUTION

Customer deploys solution

Scope of Work

Closure Details

Q-28671 - DeKalb County School District

This proposal is valid until 6/30/2024.

Quote Execution/Purchase Order Information

To execute on this proposal, please sign where indicated and provide a purchase order for the items outlined in your proposal. Purchase orders and proposals can be sent to orders@identityautomation.com.

Taxability Information Here

Are you a tax exempt entity? No ___ Yes ___

If marked yes, please provide your tax exempt certificate with your purchase order. An exemption certificate is required to be considered exempt from sales tax.

Onboarding Process

Identity Automation Onboarding Checklist:

- Receipt of Signed proposal from customer
- Purchase Order or signed Contract (varies by customer) from customer
- Identity Automation acceptance & approval process completed
- Licenses provided by Identity Automation
- Provisioning for Identity Automation portal accounts

Identity Automation



April Reid

Account Executive
(864) 304-2789
areid@idauto.net



Timothy Till

Sales Manager
(832) 229-4470
till@identityautomation.com



Sales Consultant



Jim Harold

Customer Success Manager
jharold@idauto.net



Greg Pearson

VP of Delivery
(281) 721-4732
gpearson@identityautomation.com

DeKalb County School District

Project Lead



Kermit Belcher

kermit_belcher@dekalbschoolsga.org

Secondary Project Contact



Executive Sponsor



Billing Contact



Governing Terms

GOVERNING AGREEMENT

This order is governed by the terms of the Software License and Subscription Agreement:
<https://www.identityautomation.com/identity-automation-saas-subscription-agreement/>.

CHANGES

All changes to this order must be in writing signed by both parties to be enforceable.

ENTIRE AGREEMENT

This Proposal, Software License and Subscription Agreement, and this order are the final, complete and exclusive agreements of the parties with respect to the subject matter hereof and supersedes all prior discussions and agreements between the parties with respect to the subject matter hereof.

DEFINED TERMS

All terms not defined in this order, have the defined meanings in the Agreement.

Signatures

By signing below, the Customer acknowledges it has read and agrees to the terms and conditions set forth in the Proposal, Software License and Subscription Agreement, and order(s) with an effective date as of the last signature date set forth below ("Effective Date").

DeKalb County School District

SIGNATURE

DATE

NAME

TITLE

BILLING CONTACT NAME

BILLING CONTACT EMAIL

Identity Automation

SIGNATURE

DATE

NAME

TITLE



RapidIdentity Support Plans

At Identity Automation, we're dedicated to providing exceptional support that empowers your organization to thrive. With every subscription or license, you gain access to reliable, expert assistance for all RapidIdentity Cloud configurations and the ability to submit feature requests to shape the future of the platform. Our support plans are crafted to meet your needs, ensuring your team stays productive and your operations uninterrupted.

Each plan includes a guaranteed 15-minute response time during standard support hours, so you're never left waiting. Emergency support is available 24X7, delivering peace of mind even during after-hours emergencies. With Identity Automation, your team is always backed by responsive, proactive support to keep you moving forward.

Feature	Advanced	Advanced +	Pro	Pro +	Enterprise
Help Center					
6 am-6 pm Central U.S. Time Email, Web, Phone Support					
24 X 7 Critical Case Support					
Service Units <i>(expire annually)</i>		10	30	50	50
Tier 2 SLAs					
Technical Account Manager					
Dedicated Slack Channel					

Managed Support Plan Details and Pricing are available exclusively for State and Large District Customers. This comprehensive plan provides a Dedicated Technical Support Lead, proactive monitoring of production-critical RapidIdentity processes, and complete management of your RapidIdentity environment.

Designed to ensure seamless performance and peace of mind, our Managed Support Plan offers unmatched support and oversight tailored to your organization's scale and needs.



Any unique challenges the district faced were accommodated by the professional services team at Identity Automation. Regardless of the engineer working on your implementation, the insight and quality of support exceeded expectations.

Matt Roper, Supervisor of Network and Security Services, Cherokee County School District.

Every RapidIdentity implementation includes robust support, packed with features and resources designed to ensure your success:

Help Center

Your central hub for all things support—easily access FAQs, product guides, training videos, and log cases. Here, you can view and update cases, engage with the support customer community, submit feature requests, review product errata, and more.

Commitment to Excellence

We hold ourselves to the highest standards in SaaS delivery. Our DevOps and Security teams are top-tier experts dedicated to safeguarding your data and ensuring seamless operations. Our practices include:

- Change Management
- Alerting, Monitoring, and Logging
- Data Security
- System Patching
- Continuous Improvement

We take pride in our commitment to excellence. For detailed insight into our security and operational controls, request a copy of our latest SOC-2 report—a comprehensive third-party audited document validating our rigorous service standards.

Please review our Master Subscription Agreement Terms and Conditions for further details on our contractual commitments to security and uptime.

Tier 2 SLAs

Response times are prioritized to ensure swift and effective support once a ticket is escalated from Tier 1 to Tier 2. Our maximum response times, based on ticket priority, are as follows:

	Professional +	Enterprise
Critical	2 hours	1 hour
Major	2 BDs	8 hours
Minor	4 BDs	2 BDs

Technical Account Manager

Supporting complex Enterprise implementations demands continuity. That's why we offer a dedicated Technical Account Manager with our Enterprise plan—to ensure your team always has a knowledgeable partner who understands your unique environment and needs.

Dedicated Slack Channel

Stay connected with your Technical Account Manager through a dedicated Slack channel for Enterprise customers. While standard support cases follow our usual processes, this channel enables quick check-ins, questions, and direct communication, bringing support closer to your daily operations.

Service Units

As your organization evolves, so does your RapidIdentity environment. With our Professional and Enterprise plans, you'll have direct access to our world-class Professional Services team to keep your implementation current and optimized.

Common Use Cases for Service Units

Use Case	Description
Custom Action Sets	<p>Custom action sets can be used for a variety of automated workflows that allow you to get the most out of your digital identity platform. Common use cases include:</p> <ul style="list-style-type: none">• Filtering a subset of accounts and exporting them to a .csv file or other target, such as a customer-owned FTP server, to easily merge data for business analytics or other work.• Syncing groups to Active Directory, Google Workspace, Microsoft 365, or other systems.
Advanced Sponsorship	<p>Enhance the standard account provisioning use case with advanced sponsorship policies that allow you to customize policies to conform to your organization's unique workflows, such as originating accounts outside the student information system (SIS) or human resources management system (HRMS).</p>
One-On-One Connect Training	<p>Especially useful for developers, one-on-one training helps administrative power users use our low code environment to create custom action sets that make RapidIdentity the industry's most flexible digital identity platform.</p> <p>Advanced training for portal configuration, account maintenance, roles, and configuration policies.</p>
Review Authentication Policies	<p>Conduct a detailed review of your authentication policies with a cybersecurity expert to ensure that your policies are optimized for the experience of your users and the need to protect your organization from account takeovers.</p>



**SCOPE NAME**

The following are the proposed items to be included in the for this implementation:

SCOPE STATEMENT

Customer would like to deploy a Standard K12 Implementation of RapidIdentity Cloud to manage the full lifecycle of employee and student accounts in Active Directory and Office 365/Google Workspace (if desired), while also leveraging the Portal to allow end users to claim their account, provide self-service functionality and automatic and dynamic role management.

SCOPE OF WORK

1. Employee and Student Account Lifecycle Management
 - a. HRMS to RapidIdentity
 - b. SIS to RapidIdentity
 - c. RapidIdentity to Active Directory
 - d. RapidIdentity to Office 365 (if desired)
 - e. RapidIdentity to Google Workspace (if desired)
2. RapidIdentity Portal configuration
 - a. Profiles Module
 - b. Account Claiming
 - c. Roles Module (Group Management)
 - i. Dynamic role (group) management in RapidIdentity
 - ii. Group sync to:
 1. Active Directory
 2. Office 365 (if desired)
 3. Google Workspace (if desired)
 - d. Reporting Module
 - e. Login Page Branding
3. MFA for Education
 - a. One-Time Password
 - b. QR Code
 - c. Pictograph
 - d. Knowledge transfer for additional configurations
4. Solution Acceptance
 - a. Solution Overview
 - b. Customer Acceptance Testing
5. Solution Administration Knowledge Transfer
 - a. Common system administration tasks within RapidIdentity
 - b. Overview of <https://help.rapididentity.com>
 - c. Opening a Support Ticket with Identity Automation

SUCCESS CRITERIA AND ACCEPTANCE CRITERIA

- o Full lifecycle management automation for employee and student accounts in Active Directory and Office 365/Google Workspace (if desired)
 - Add
 - Update
 - Move
 - Rename



- Enable
- Disable
- Delete
- o Group management in RapidIdentity (Dynamic and Static)
- o Group synchronization:
 - RapidIdentity to Active Directory
 - RapidIdentity to Office 365 (if desired)
 - RapidIdentity to Google Workspace (if desired)
- o End user self-service capability for account claiming and password resets
- o Ability to automate dynamic role management in RapidIdentity
- o Ability to sync groups to AD, Office 365, and Google Workspace
- o Ability to configure reports

RISKS

- Business process complexity
- Appropriate requested access to source systems/data and target systems granted
- Availability of Project resources from Customer
- Initial syncs require Customer to dedicate substantial time to validate actions to be taken

ASSUMPTIONS

- This SOW allows for a single domain O365/Azure, and Google - if additional domains are required, a change order to the SOW will be required.
- The scope accounts for a single forest, single domain directory environment only.
- Any additional hardware and software purchases related to unforeseen items during the project are not included in this project scope of work.
- Customer will provide access to all devices, facilities, systems/applications, and services necessary to complete the tasks in this SOW in a timely manner. Failure to provide timely access will result in a change order and resetting of any project timelines and anticipated go-live date.
- Uniquely identifiable information must be populated within the applications in scope.
- Identity Automation does not provide consulting services on source systems or destination systems to properly create queries or views. Any triggers (database view, CSV export, SQL queries, etc.) that need to be created in the HR/SIS system will need to be done by the Customer (or their system vendor at the expense of the Customer).
- Identity Automation may request additional data be exposed as business logic requires. Customer will be expected to provide said data or the business logic will need to be changed.
- For data cleansing items, Identity Automation will provide basic analysis and reports of data from source systems (upon Customer providing the data) that needs to be cleansed. Customer will be responsible for all the actual data corrections based on the needs for this project to ensure proper automatic processing. Data will need to be cleansed before the automated synchronization can begin.
- Customer will perform acceptance testing in advance of production rollout to the user population.
- Test cases will be written and provided prior to completion. Successful completion of these test cases will constitute completion.
- Customer agrees that Identity Automation shall be able to allocate additional resources, as Identity Automation deems appropriate, so long as such allocation does not cause production costs to exceed the amount provided herein.
- If the Customer chooses not to follow best practices, that decision will be documented and will be placed on a RAID log for the project.



- Identity Automation will keep the Customer team updated regarding implementation progress. If functionality demos are requested, they are not to exceed the time allotted for the weekly progress checkpoint meetings.
- Customer understands that there should not be any data elements with dual, competing sources of authority.
- The Standard K12 – Basic package includes Active Directory, Office 365 and Google Workspace as targets for integration. If any of these are deemed to not be needed at the time of initial implementation, they can be removed with no change to the package cost. They cannot be swapped for any other target applications or desired functionality.
- If customer chooses to not implement one of the specified target systems (O365/Google) during initial implementation, the SOW will not change; however later addition or swapping of target systems will constitute a new project and will be scoped separately.
- Writing back to the HRMS or SIS is not included in the Standard K12 - Basic SOW.
- Use of the ADD PERSON (Sponsorship) function within RapidIdentity is limited to the out-of-the-box functions (which only provisions into RapidIdentity – no targets), and this SOW does not include any custom modification to the ADD PERSON workflow. If Customer needs additional functionality, time and cost estimates can be provided in a Change Order form to amend the SOW with customer approval.
- Account merging/splitting is not supported with this SOW (temporary/sponsored account becomes a full-time account or vice-versa). If Customer needs additional functionality, time and cost estimates can be provided in a Change Order form to amend the SOW with customer approval.
- Identity Automation will not store passwords in plain text for reference, nor will a list or export of plain text passwords be produced for reference. Passwords can be sent to other systems through appropriate APIs or methods that ensure the password is not exposed or available in plain text.
- Customers assume risk for deletion of accounts. In certain cases where there are legal requirements to delete identity data, Identity Automation will create a change order to the project and will provide an estimate of the effort required to add the functionality. Additionally, the customer will assume all risk with the deletion of the data, and will be made aware of the potential risks associated with the deletion of identity metadata.
- Projects are designed to be executed continuously to completion and production deployment (“turned on” in customer environment) once started. Any delay of the project going live or moving into production deployment will result in the Identity Automation engineer being removed from the project and placed on an alternate project. The customer will be required to coordinate with the Project Manager to reschedule the continuation of the project and rescheduling of the allocated engineer. ***NOTE: Engineer availability is limited, and requires a minimum of 30 days from time of notice in order for the engineer to finish up any active projects before being rescheduled back on to the customer project. In some cases the availability may be longer than 30 days if during peak periods such as Summer, Winter Break, or Spring Break. Any project delays may introduce risk to any originally agreed upon go-live dates, including start of school.***

Customer Resource Allocation During the Assessment Phase

- Project Manager
- System Administrators for:
 - HRMS and SIS
 - Active Directory
 - O365/Azure
 - Google Workspace



- Other identified Critical Stakeholder(s) who:
 - Have input into providing guidance around source data
 - Provide decisions around process/workflow and end-user experience
 - Provide decisions around appropriate access or authentication methods

CHANGE CONTROL

All changes to the SoW shall pass through the Change Control Board. The Change Control Board shall consist of a customer designated representative and an Identity Automation representative. Change requests, which are deemed to fall outside of scope will be reviewed; and Identity Automation shall provide time and cost estimates for customers approval prior to performing any work. Change requests within scope shall be agreed upon by both the customer and Identity Automation. The SOW shall then be amended using a Change Order form to reflect the changes prior to performing any work. All amendments to the SOW shall be signed off by both parties before the additional work is performed.

CUSTOMER ACCEPTANCE TESTING

During this phase the engineer will demonstrate each component of the solution. Should any Identity Automation deliverable not match the outlined success criteria, the Engineer will remedy and demonstrate the remedy to the Customer for validation. This will repeat until all solution deliverables and success criteria are validated.

Customer Tasks During the Test Phase

1. Provide Acceptance of solution (meets defined success criteria)
2. Customer to sign off on Acceptance once all success criteria testing scenarios are validated

Customer Resource Allocation During the Test Phase

- Project Manager
- System Administrators
- Other identified Critical Stakeholder(s)

USER USE CASES

U1 – Employee User Add

1. New employee is hired, and record is created in Source of Authority
2. New record arrives in source feed
3. New user is created in RapidIdentity with appropriate birthright entitlements
4. New user object is created and placed in Active Directory
5. New account is created in Office 365 (if desired)
6. New account is created in Google Workspace (if desired)

U2 – Student User Add

1. New student is enrolled, and record is created in Source of Authority
2. New record arrives in source feed
3. New user is created in RapidIdentity with appropriate birthright entitlements
4. New user object is created and placed in Active Directory
5. New account is created in Office 365 (if desired)
6. New account is created in Google Workspace (if desired)

U3 – User Update



1. User information changes in Source of Authority
2. New information on record arrives in source feed, a comparison is done between attributes, any difference in designated attributes will prompt an update to the account.
3. User object is updated in RapidIdentity
4. User object is updated in Active Directory
5. User is updated in Office 365 (if desired)
6. User is updated in Google Workspace (if desired)

U4 – User Disable

1. Existing active user leaves organization and is designated as inactive in Source of Authority
2. New information on record arrives in source feed
3. User object is disabled in RapidIdentity
4. User object is disabled in Active Directory
 - a. *This may include OU movement*
5. User is disabled in Office 365 (if desired)
6. User is disabled in Google Workspace (if desired)

U5 – User Enable

1. Existing inactive user returns to organization and is designated as active in Sources of Authority
2. New information on record arrives in source feed
3. User object is enabled in RapidIdentity
4. User object is enabled and placed in Active Directory
 - a. *This may include OU movement*
5. User is enabled in Office 365 (if desired)
6. User is enabled in Google Workspace (if desired)

U6 – Password Reset

1. User resets password via the Portal
2. User is updated in RapidIdentity with new password
3. Password is replicated to any application synchronizing passwords with RapidIdentity that are not setup for Federation. Some systems do not allow users to sync passwords if they are Federated.

U7 – Group Management

1. Dynamic and static management of group memberships through the Roles Module in RapidIdentity
2. Creation of groups
3. Setting up dynamic inclusion/exclusion filters (rules) for managing membership
4. Adding exceptions through static inclusion (or denying inclusion through static exclusion)
5. Synchronizing of new group object to:
 - a. Active Directory (as a security group)
 - b. Office 365 (as a Microsoft 365 group as supported through the MS Graph API)
 - c. Google Workspace (as a group/distribution list)
6. Detection of membership changes and synchronization to:
 - a. Active Directory
 - b. Office 365
 - c. Google Workspace

BEST PRACTICES

The following options for the deployment represent Identity Automation best practices and are included as part of your deployment. If these options do not meet your needs, the project manager and customer success manager can discuss and scope a change order to suit your requirements.

ACCOUNT RENAMING

Usernames are a key element of an identity management system. They affect how end users login to provided services and authenticate to applications. Industry standards suggest that account renames occur only when absolutely necessary. In most cases, renaming an account requires human interaction to notify the end user that their username is changing based on an event. For the Standard K12 – Basic SOW, the account renaming option is as follows:

Rename Option

- An account will be flagged for a rename event, based on a first or last name changing in the source data (HRMS/SIS)
- The Customer will have the ability to specify the number of days between the source data changing and the rename event; which will allow the System Administrator to contact the end user to notify them that their username will be changing in XX days
- The flagging of the account for a rename will invoke a notification email to designated RapidIdentity System Administrators daily.
- At the end of the designated timeframe, the account will be renamed in all denoted systems. If any renaming operations fail, a report will be sent to the RapidIdentity System Administrators in order for them to update the respective systems manually

ACCOUNT PLACEMENT

All accounts should be placed in accordance with rights for the appropriate placement.

System Account Placement or AD/Google Account Placement. Active Directory (LDAP) Organizational Units

Organizational Units (OUs) should be designed to ease the administrative overload. All OUs should have an appropriate policy (Group Policy) to them in order to take the burden of applying granular rights to accounts. If policies are not applied at the OU level, then it is suggested to make the OU Structure less complex, unless needed for visual purposes or other systems.

Account Placement should always follow a distinctive, static format where rights need to be adjusted and formatted, i.e. location, department, grade level, etc If not defined Account Placement IA can bind to the root OU and continue with the project.

The Customer will provide a mapping or document outlining the placement rules for any systems in which accounts are placed in an OU.