



IDENTITY  
AUTOMATION

# Authentication

---

RapidIdentity IdP &  
Federated Partner Configuration



# Agenda

---

- 01 Why now?
- 02 Productivity vs Security
- 03 RI Authentication Overview
- 04 Single Sign-on & Federation
- 05 Identity Provider Overview
- 06 Federated Partner Configuration
- 07 Recommended Authentication  
Methods by User Role



# Schools Are Becoming Uninsurable

## School District Reports a 334% Hike in Cybersecurity Insurance Costs

By Bill Toulas



By Dian Schaffhauser | 10/12/21

Data Security

### The Changing Face of Cyber Insurance in K-12

*If you're relying on an insurance policy to rescue you in the event of ransomware or a data breach, it's time to rethink your cybersecurity strategy.*

Bloomington School District 87 in Illinois has published its cyber-insurance renewal details, and the cost has jumped from \$6,661 in 2021 to \$22,229 this year.

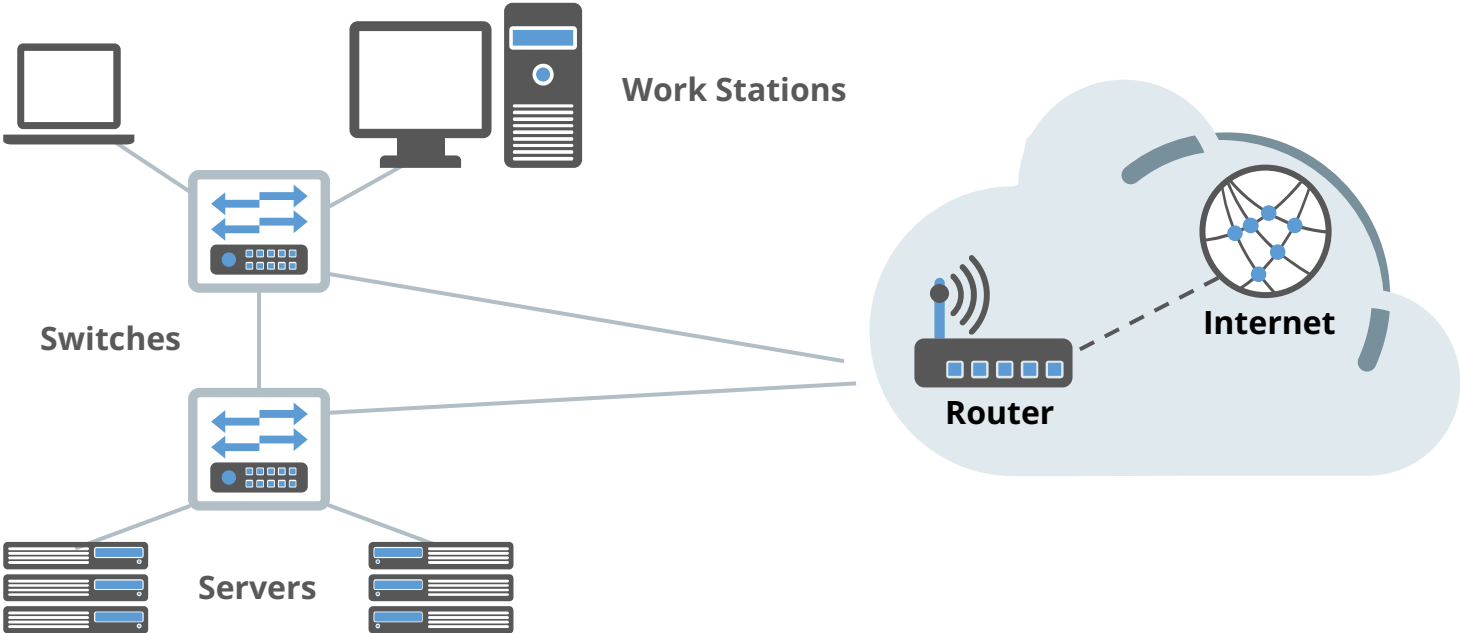
## BUSINESS INSURANCE

Risk Management

### Schools hit with cyber price hikes



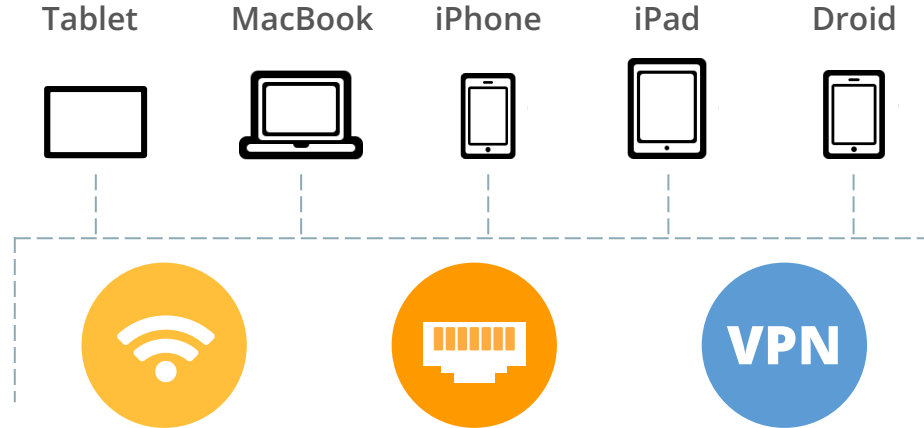
# Traditional Perimeter



# Remote Learning: The Need for Phishing-Resistant Authentication



ANY DEVICE  
ANY NETWORK



# Delicate Balance of Productivity vs Security

---

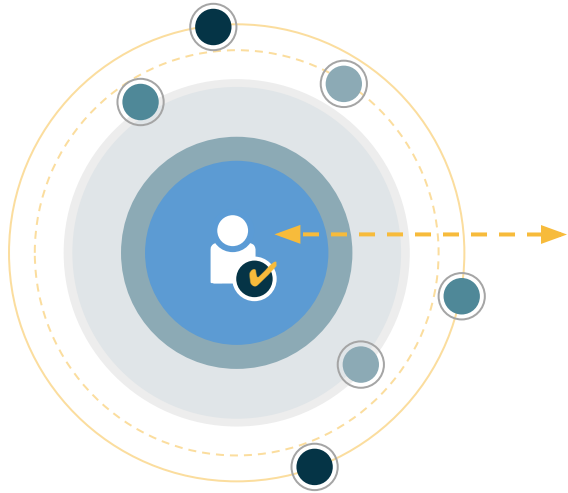


**PRODUCTIVITY** *vs* **SECURITY**



# RapidIdentity Authentication

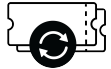
---



- Help meet your cybersecurity insurance requirements
- Secure and track access to your resources
- Strengthen your position against ransomware attacks & malicious actors
- Simplified experience for users
- Lockdown digital classrooms without interfering with learning



# Authentication Methods



Kerberos



WebAuthN



OTP



Ping Me



Social Login



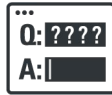
DUO Auth



Password



QR Code



Challenge



Pictograph



SMS  
Passcode



Federation





# Secure Single Sign On with Federation

---

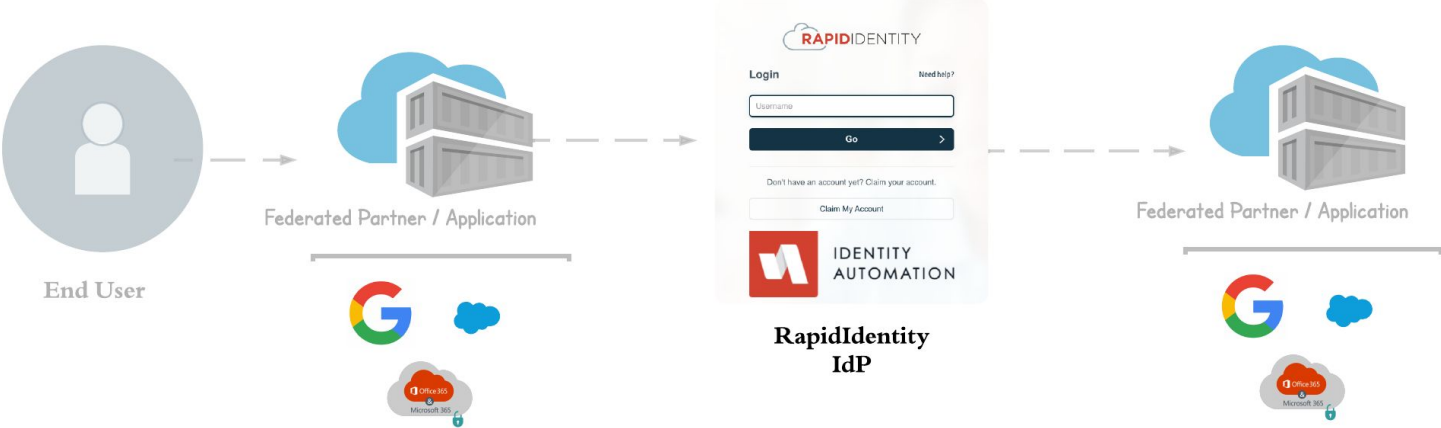


- Put all of your user's apps in one place
- Simplify the digital learning experience
- Make users' school network login the only login they need
- Don't sacrifice security while making things easier to use



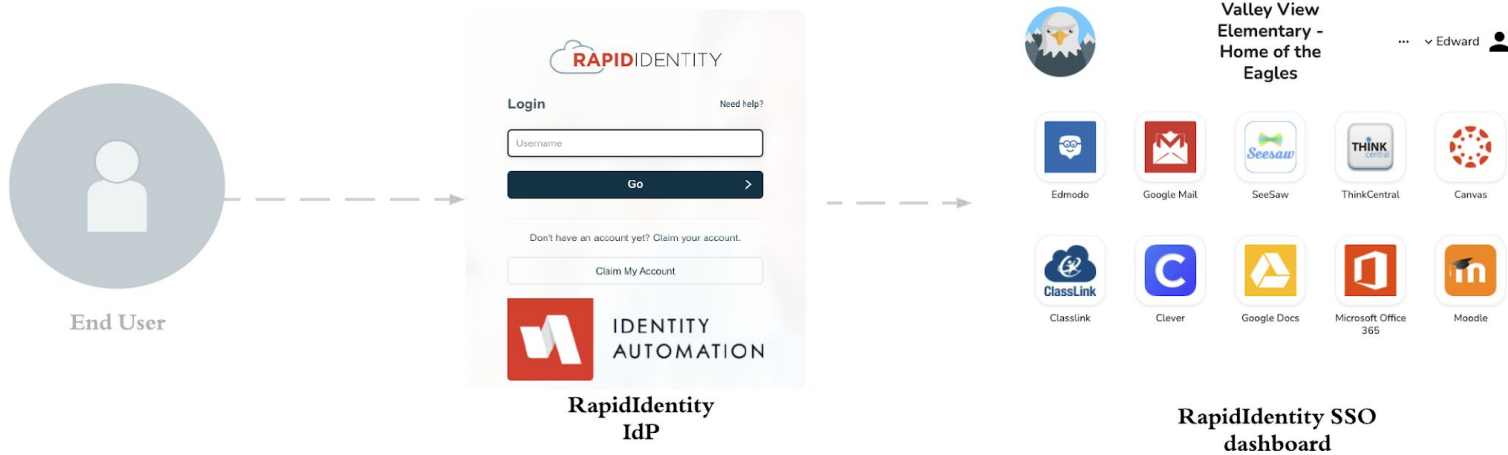
# Single Sign On with RapidIdentity - User Workflow #1

Browsing directly to Federated Applications(service provider initiated)



# Single Sign On with RapidIdentity - User Workflow #2

## Using the RapidIdentity Dashboard

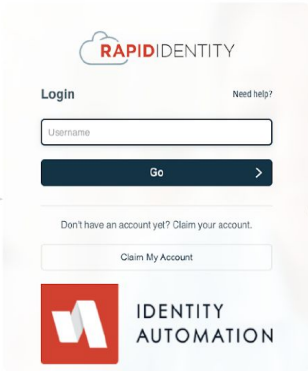


# Single Sign On with RapidIdentity - User Workflow #3(Cloud Only)

Using RapidIdentity Universal Director



End User



RapidIdentity  
IdP



Federated Partner / Application



# Using RapidIdentity as an Identity Provider - Configuration

## Useful Facts:

The Identity Provider Section of the configuration houses both the IdP, and Federated Partner Configurations

The screenshot displays a configuration menu with the following sections:

- General**: Appearance, Portal, Localization, Proxy As, Settings, Templates
- Policies**: Authentication, Challenge, Claim, Forgot Username, Mobile Devices, Password, User Agreement
- Security**: Audit Logging, Identity Providers, SafelD, Service Identities, Session Management, Grant Support Access
- Systems**: Integration, Metadirectory, SMTP, SMS
- SSO Portal**: Personas, Themes, Announcements

A red arrow originates from the 'Systems' section and points to the 'Identity Providers' sub-item within the 'Security' section, which is also enclosed in a red rounded rectangle.



# Using RapidIdentity as an Identity Provider - Configuration

## Useful Facts:

For more information about RapidIdentity Metadata and IdP see the Knowledge base article: [RapidIdentity IdP Configuration](#)

Setting	Value	Action
ENTITY ID	<a href="https://demo-k12.us001-rapididentity.com/idp">https://demo-k12.us001-rapididentity.com/idp</a>	Copy
BASE URL	<a href="https://demo-k12.us001-rapididentity.com/idp">https://demo-k12.us001-rapididentity.com/idp</a>	Copy
LOGOUT URL	<a href="https://demo-k12.us001-rapididentity.com/idp/logout">https://demo-k12.us001-rapididentity.com/idp/logout</a>	Copy
LIVE METADATA URL	<a href="https://demo-k12.us001-rapididentity.com/idp/profile/Metadata/SAML">https://demo-k12.us001-rapididentity.com/idp/profile/Metadata/SAML</a>	Copy
METADATA	<a href="#">Download the registered metadata for the Identity Provider</a>	Download
PUBLIC KEY CERTIFICATE .PEM FILE	<a href="#">Download the certificate used by the Identity Provider (.pem)</a>	Download
SIGNING CERTIFICATE .DER FILE	<a href="#">Download the certificate used by the Identity Provider (.der)</a>	Download
PUBLIC KEY CERTIFICATE FINGERPRINT	24:2A:DA:C3:D5:B5:19:47:59:3D:9A:95:61:1C:FC:C9:BC:AE:3D:0D	Copy
CERTIFICATE EXPIRES	Jun 14th, 2046, 2:17 pm (in 23 years)	



# Using RapidIdentity as an Identity Provider - Configuration

The screenshot shows the configuration interface for the Identity Automation system. On the left is a navigation menu under the 'Security' header, with 'Web Template' selected. The main area is divided into sections: 'Logout Body' (empty), 'Claim Account Link Label' (set to 'Claim My Account'), 'Claim Account URL' (set to '/portal/claim/'), and 'Load Helplinks in Same Tab/Window' (checked). Below these is the 'Help Links' section, which contains a table with columns for 'Display Name' and 'URL'. One entry is visible with 'Custom Help Link' as the display name and 'www.identityautomation.com' as the URL. A '+ Add Another' button is at the bottom of the table. A red arrow points from the 'Useful Facts' callout to the 'Add Another' button.

Display Name	URL
Custom Help Link	www.identityautomation.com

## Useful Facts:

The settings for embedded claim my account, and custom help links are also configurable through the **Web Template**



# Using RapidIdentity as an Identity Provider - Configuration

## Useful Facts:

RapidIdentity can act as an Identity provider or Service provider.

**Federation Partners**

Filter by Partner Type Search Federation Partners

6 Results

<input type="checkbox"/>	NAME	↑	TYPE	DESCRIPTION
<input type="checkbox"/>	Azure Custom Control/Conditional Access		OpenID Connect	
<input type="checkbox"/>	Clever		SAML 2.0	
<input type="checkbox"/>	Global Protect		SAML 2.0	
<input type="checkbox"/>	Google Apps		SAML 2.0	Google Apps Single Sign On
<input type="checkbox"/>	Microsoft Online (Azure AD/Office365)		WS-Federation	
<input type="checkbox"/>	RapidIdentity		SAML 2.0	

ADD FEDERATION PARTNER

- SAML 2.0
- OAuth 2.0
- OpenID Connect
- WS-Federation
- CAS

← Back to Configuration





# Using RapidIdentity as an Identity Provider - Configuration

## Useful Facts:

RapidIdentity is commonly used as the primary Identity Provider for Google domains. For more information on this configuration, and step by step instructions see the knowledge base article: [SSO with Google](#)

The screenshot shows the configuration page for 'Federation Partners > Google Apps (SAML)'. On the left is a navigation sidebar with the following items: Security (selected), Audit Logging, Identity Providers, IDP Configuration, Federation Partners (highlighted), Web Template, External Auth Realms, Trusted IDPs, SafelD, Service Identities, Session Management, and Grant Support Access. At the bottom of the sidebar is a 'Back to Configuration' link. The main content area is titled 'Federation Partners > Google Apps (SAML)' and contains four expandable sections: General, SSO Settings, Attribute Mapping, and Issuer Entity IDs. Each section has a plus sign on the right side to indicate it can be expanded.



# Using RapidIdentity as an Identity Provider - Configuration

## Useful Facts:

The METADATA is sourced from the service provider, and can be edited in this window in needed.

**Security**

- Audit Logging
- Identity Providers
- IDP Configuration
- Federation Partners**
- Web Template
- External Auth Realms
- Trusted IDPs
- SafelD
- Service Identities
- Session Management
- Grant Support Access

### Federation Partners > Google Apps (SAML)

**General**

NAME \*  
Google Apps

DESCRIPTION  
Google Apps Single Sign On

IS INCOMMON

METADATA \*

```
1 - <EntityDescriptor entityID="google.com" xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
2 -   <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
3 -     <NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified/>NameIDFormat
4 -     <AssertionConsumerService index="1" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
5 -       Location="https://www.google.com/a/rapididentitydemo.com/acs" />
6 -   </SPSSODescriptor>
7 - </EntityDescriptor>
```

← Back to Configuration



# Using RapidIdentity as an Identity Provider - Configuration

The screenshot displays the configuration interface for RapidIdentity. On the left is a sidebar menu with the following items: Security (selected), Audit Logging, Identity Providers, IDP Configuration, Federation Partners, Web Template, External Auth Realms, Trusted IDPs, SafeID, Service Identities, Session Management, and Grant Support Access. The main content area is titled 'SSO Settings' and contains the following configuration options:

- INCLUDE SAML2 ATTRIBUTE STATEMENT
- SAML2 SSO ASSERTION LIFETIME
  - HOURS: 0
  - MINUTES: 5
  - SECONDS: 0
- NOTBEFORE SKEW (SECONDS): 0
- SIGN SAML2 SSO RESPONSE: Conditional
- SIGN SAML2 SSO ASSERTIONS: Never
- ENCRYPT SAML2 SSO ASSERTIONS: Never
- ENCRYPT SAML2 SSO NAME IDS: Never
- SIGNATURE ALGORITHM: RSA SHA-1
- SKIP ENDPOINT VALIDATION WHEN SIGNED
- ENABLE ECP SETTINGS

At the bottom of the SSO Settings section, there is a partially visible 'Attribute Mapp' section. A red arrow points from the 'ENABLE ECP SETTINGS' checkbox to the 'Attribute Mapp' section header.

## Useful Facts:

When selecting the Enable ECP Settings checkbox, the ECP Settings section will become available beneath the SSO Settings along with the configuration options. In this case, ECP settings are not to be enabled.



# Using RapidIdentity as an Identity Provider - Configuration

## Useful Facts:

You can Add attributes to be mapped directly in the federated partner Settings

They can also be added in the Federated Partner Configuration menu.

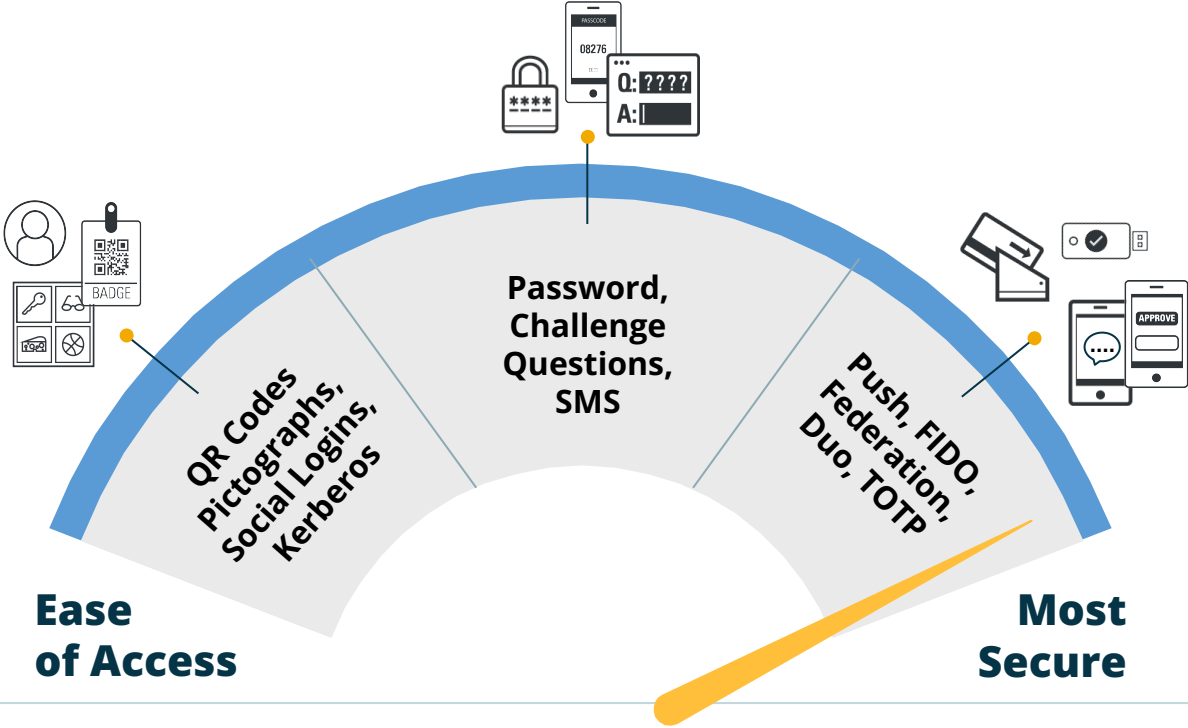
The screenshot displays the Azure AD Security Center interface. On the left is a navigation menu with options: Security, Audit Logging, Identity Providers, IDP Configuration, Federation Partners, Web Template, External Auth Realms, Trusted IDPs, SafeID, Service Identities, Session Management, and Grant Support Access. The main area is split into two panels. The top panel shows configuration for 'ENCRYPT SAML2 SSO ASSERTIONS' and 'ENCRYPT SAML2 SSO NAME IDS', both set to 'Never', and 'SIGNATURE ALGORITHM' set to 'RSA SHA-1'. There are checkboxes for 'SKIP ENDPOINT VALIDATION WHEN SIGNED' and 'ENABLE ECP SETTINGS'. The bottom panel shows 'Attribute Mapping' with one result: 'mail (urn:oasis:names:tc:SAML:1:1:nameid-format:emailAddress)' with a 'PERMIT' type. Below this is a section to 'Add Attribute' with a dropdown to 'Choose an Attribute to DENY or PERMIT' and a button 'Add New Attribute'. The right panel shows the 'Federation Partners' list with a search bar and a table of 6 results:

NAME	TYPE	DESCRIPTION
Azure Custom Control/Conditional Access	OpenID Connect	
Clever	SAML 2.0	
Global Protect	SAML 2.0	
Google Apps	SAML 2.0	Google Apps Single Sign On
Microsoft Online (Azure AD/Office365)	WS-Federation	
RapidIdentity	SAML 2.0	

At the bottom of the interface are buttons for 'Delete', 'Export', 'Import', 'SAML Attributes', and 'Help'. A red arrow points from the 'Add New Attribute' button in the Attribute Mapping panel to the 'Federation Partners' table.



# Tailor Authentication to the Actual User



# Authentication Methods

For more information about MFA deployment best practices, and passwordless workflows. See [K-12 MFA Guide: Make Districtwide Multi-Factor Authentication Not Only a Reality— But a Success](#)

Pre-K, Elementary, and Special Needs Students

QR Code,  
Pictograph



Middle School Students

QR Code,  
Password



High School Students

SMS OTP, Passphrase  
(alt. for users w/out phones), Kerberos



General Faculty and Staff

WebAuthn/, Push Auth,  
SMS OTP (alt. if unwilling to download app)



IT Staff and Privileged Users

FIDO2,  
Push Authentication



Parents and Guardians

Social  
Login



Third Parties

Email OTP,  
WebAuthn/



# Configuration Policies - Authentication Policies

- MFA policies vs. Forgot Password policies
- Primary device-based methods
  - Duo (proprietary app)
  - PingMe (RapidIdentity mobile app)
  - WebAuthN (Windows Hello, Apple Touch ID, FIDO key, etc.)
  - SMS (text message)
  - TOTP (time-based one-time password, generated by authenticator app)

The screenshot shows the 'Configuration' page for 'Authentication Policies'. A list of policies is shown on the left, with 'Email Forgot Password Policy' selected. The configuration details for this policy are shown on the right under the 'General' tab.

Field	Value
ID	c2548e2b-6deb-48e2-817f-9f9ec8569e21
Enabled	<input checked="" type="checkbox"/>
Is a Forgot Password Policy?	<input checked="" type="checkbox"/> Federation, Kerberos, Social, Password, and QR Code not valid
Name	Email Forgot Password Policy
Description	Forgot password policy for non students
Always Fail	<input type="checkbox"/>
Insecure QR ID Scans Enabled	<input type="checkbox"/>



# Configuration Policies - Authentication Policies

- Secondary methods not dependent on a mobile device
  - Email
  - Password
  - Pictograph
  - Portal Challenge Questions
  - QR Code
  - Social (Google, Facebook, Twitter, LinkedIn)
- Setup a primary method that uses a device, and secondary or backup method in case the user doesn't have access

The screenshot displays the 'Configuration' interface for 'Authentication Policies'. The left sidebar lists various policy categories, with 'Authentication Policies' selected. The main area shows a list of policies, including 'Email Forgot Password Policy', 'Challenge Questions Forgot Password Policy', 'Compromised Credential MFA', 'Ping-Me Preferred Policy', 'WebAuthn Preferred Policy', 'Duo Preferred Policy', 'Password Preferred Policy', 'Social Login Preferred Policy', 'TOTP Preferred Policy', 'IDAUTO Employee Policy', 'TOTP Policy', 'Pictograph Policy', and 'QR Code Policy'. The 'Email Forgot Password Policy' is expanded to show its configuration details.

General	Criteria	Authentication Methods	User Agreement
ID			c2548e2b-6deb-48e2-817f-9f9ec8569e21
Enabled			<input checked="" type="checkbox"/>
Is a Forgot Password Policy?			<input checked="" type="checkbox"/> Federation, Kerberos, Social, Password, and QR Code not valid
Name			Email Forgot Password Policy
Description			Forgot password policy for non students
Always Fail			<input type="checkbox"/>
Insecure QR ID Scans Enabled			<input type="checkbox"/>

At the bottom of the configuration panel, there are 'Cancel' and 'Save' buttons, along with the 'Identity Automation' logo and a 'Help' icon.





# Configuration Policies - Authentication Policies (Forgot password)

- **Forgot Password policies**
  - Can receive a code through email or SMS
  - Requires personal email or mobile number stored on employee's profile in advance of the request
  - Enable self-service data entry on the staff MY Delegation If this contact info is not collected and stored in your source system and provisioned to RapidIdentity

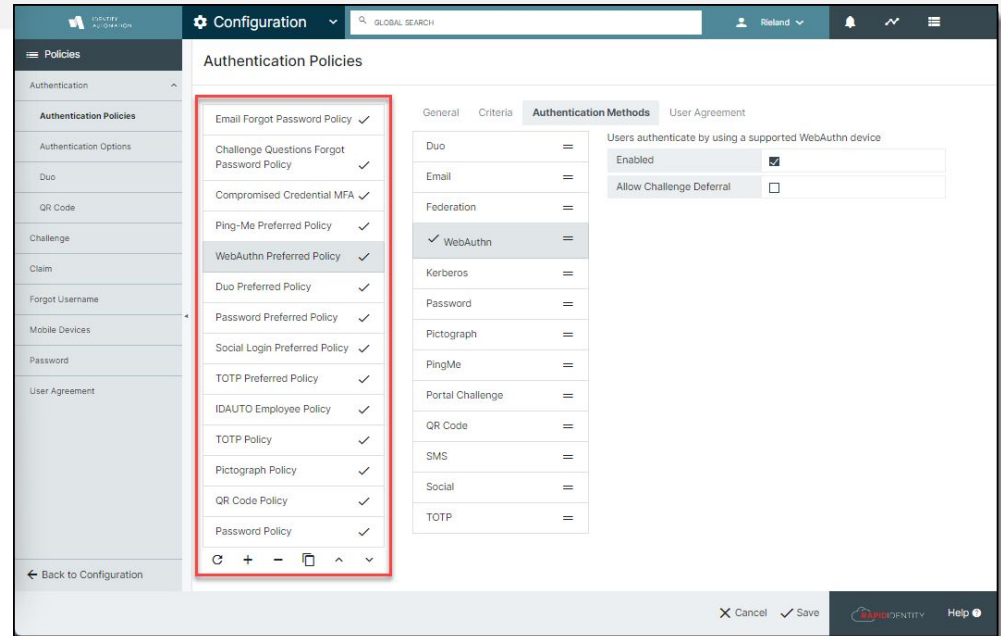
The screenshot shows the 'Authentication Policies' configuration page in the RapidIdentity console. The left sidebar lists various policy categories, with 'Authentication Policies' selected. The main area displays a list of policies, with 'Email Forgot Password Policy' highlighted. The configuration details for this policy are shown in the 'General' tab.

General	Criteria	Authentication Methods	User Agreement
ID			c2548e2b-6deb-48e2-817f-9f9ec8569e21
Enabled			<input checked="" type="checkbox"/>
Is a Forgot Password Policy?			<input checked="" type="checkbox"/> Federation, Kerberos, Social, Password, and QR Code not valid
Name			Email Forgot Password Policy
Description			Forgot password policy for non students
Always Fail			<input type="checkbox"/>
Insecure QR ID Scans Enabled			<input type="checkbox"/>



# Configuration Policies - Authentication Policies (MFA)

- The order of the policies matters, so if you allow Try Another Method, it will step down to the next policy that matches on that user's attributes, i.e. PingMe first, then QR Code second
  - Click a policy name to select it, then use the arrows at the bottom of the list to change the order (which changes the priority)
  - When implementing multi-factor authentication, a "password-only" policy should not be the final step or MFA can be bypassed on every login



The screenshot displays the Azure AD Configuration console interface. The main heading is 'Authentication Policies'. On the left, a sidebar lists various policy categories, with 'Authentication Policies' selected. The main content area shows a list of 15 authentication policies, each with a checkmark indicating it is enabled. The 'WebAuthn Preferred Policy' is highlighted with a red rectangular box. Below the list, there are navigation controls: a refresh icon, a plus sign, a minus sign, a copy icon, and up/down arrows. To the right of the list, there are tabs for 'General', 'Criteria', 'Authentication Methods', and 'User Agreement'. The 'Authentication Methods' tab is active, showing a list of authentication methods with 'WebAuthn' selected. Below this list, there is a section for 'Users authenticate by using a supported WebAuthn device' with an 'Enabled' checkbox checked and an 'Allow Challenge Deferral' checkbox unchecked. At the bottom of the console, there are 'Cancel' and 'Save' buttons, and a 'Help' icon.



# Configuration Policies - Authentication Policies (MFA)

- The order of the policies matters, so if you allow Try Another Method, it will step down to the next policy that matches on that user's attributes, i.e. PingMe first, then TOTP second
- Within each policy, the order of the Authentication Methods you've enabled also matters
  - In this example, the user will be presented with the Password field first, then the TOTP code is requested on the next screen
  - Drag and drop the Methods to change the order
  - Only the methods with a checkmark are enabled

The screenshot displays the 'Authentication Policies' configuration page in the Microsoft Identity Automation console. The left sidebar shows a list of policies, with 'TOTP Policy' selected. The main area shows the configuration for this policy, with the 'Authentication Methods' tab active. A red box highlights the 'Password' and 'TOTP' methods, both of which have checkmarks indicating they are enabled. Below the methods list, the 'User Agreement' section shows 'Users authenticate using their password' is checked and enabled, with 'Enable Password Expiration Alert' unchecked and 'Expiration Alert Days' set to 1. The bottom of the console shows 'Cancel' and 'Save' buttons, along with the 'Microsoft Identity Automation' logo and a 'Help' icon.



# Configuration Policies - Authentication Policies

- Criteria to apply policies
  - Roles (RBAC)
  - LDAP Filters (ABAC)
  - Relax or strengthen MFA on specific days or during specific hours
    - business day/week = relaxed MFA
    - after hours/weekends = strong MFA
  - Connected to Source Network = relaxed MFA
  - Kerberos/QR Code/WebAuthN = options are enabled or disabled

The screenshot displays the 'Authentication Policies' configuration page in the Identity Automation console. The left sidebar shows a navigation menu with 'Authentication Policies' selected. The main content area is titled 'Authentication Policies' and features a list of 14 policies, each with a checkmark indicating it is enabled. The 'Criteria' tab is active, showing configuration options for 'Roles', 'LDAP Filter', 'Day of Week', 'Time of Day', 'Source Network', 'Kerberos', 'QR Code', and 'WebAuthN'. The 'Roles' section is expanded, showing a list of roles and a checkbox for 'Enabled'. Below this, there are checkboxes for 'Apply to everyone' and 'Inverse Match'. At the bottom of the page, there are 'Cancel' and 'Save' buttons, and the 'Okta Identity' logo.

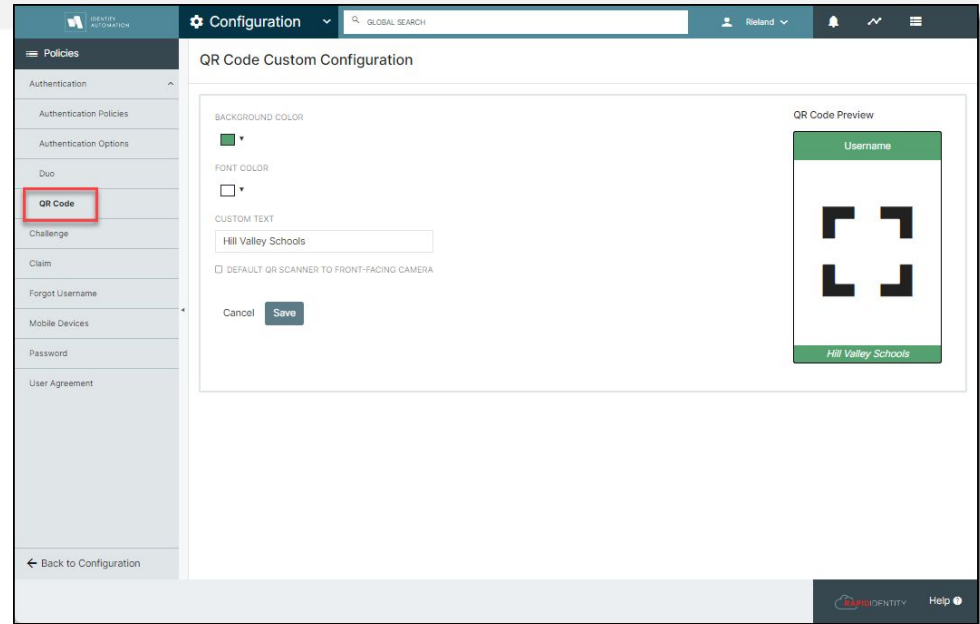
Policy Name	Status
Email Forgot Password Policy	✓
Challenge Questions Forgot Password Policy	✓
Compromised Credential MFA	✓
Ping-Me Preferred Policy	✓
WebAuthn Preferred Policy	✓
Duo Preferred Policy	✓
Password Preferred Policy	✓
Social Login Preferred Policy	✓
TOTP Preferred Policy	✓
IDAUTO Employee Policy	✓
TOTP Policy	✓
Pictograph Policy	✓
QR Code Policy	✓



# Configuration Policies - Authentication Policies (QR)

## Authentication methods designed for students

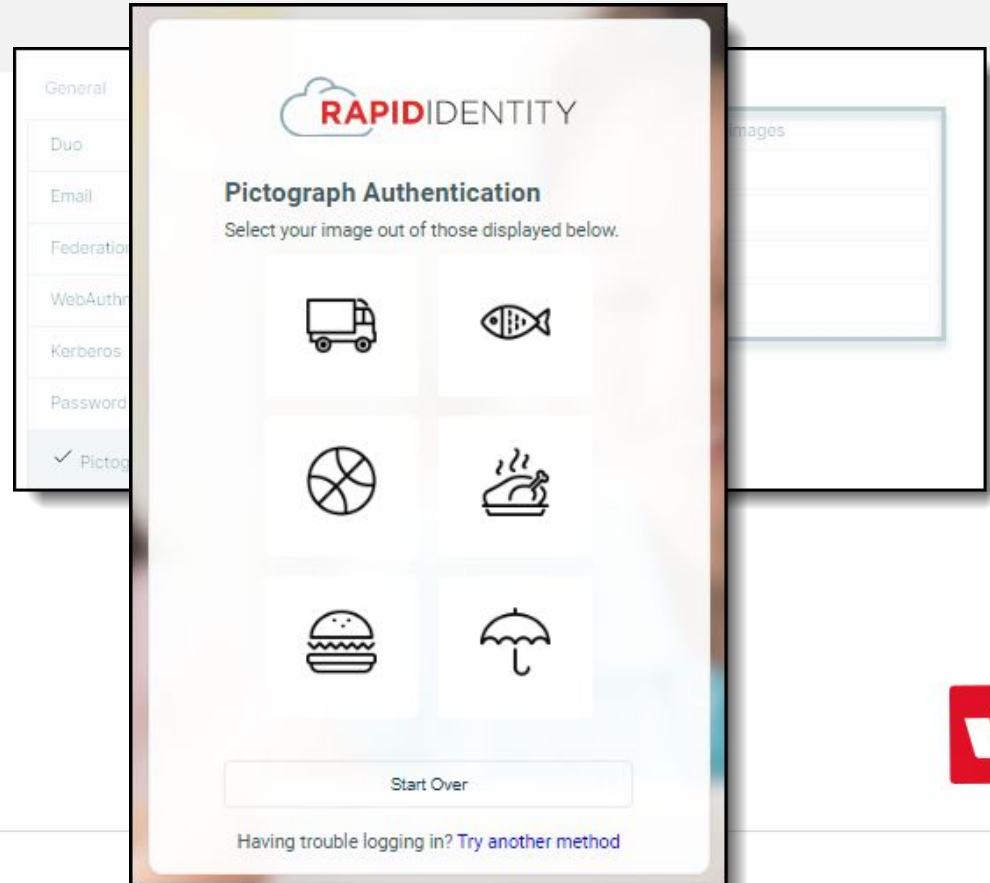
- QR Codes - secure vs. insecure does not refer to the embedded content in the code; it refers to the protection requirements
  - Secure: embedded username and password and must be stored or kept in a secure location or under a person's control at all times
  - Insecure: embedded username, and a password or pictograph is required to complete authentication so by itself, it's not easily used if found unattended
  - Color and school name can be customized under the QR Code option on the left menu



# Configuration Policies - Authentication Policies (Pictograph)

## Authentication methods designed for students

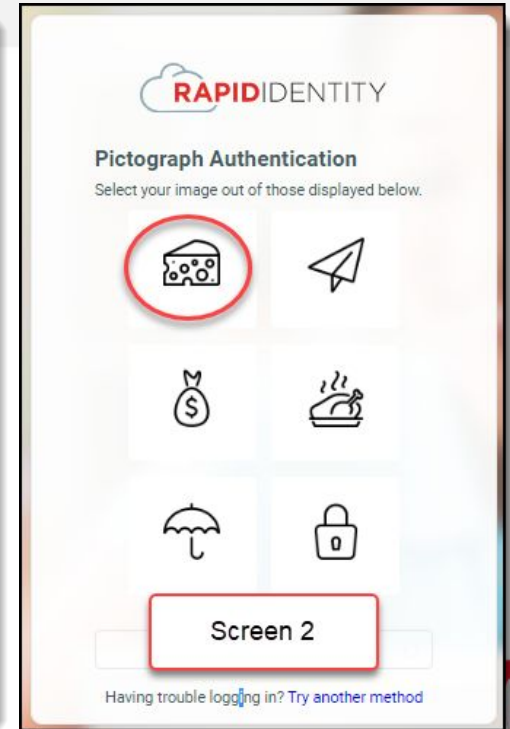
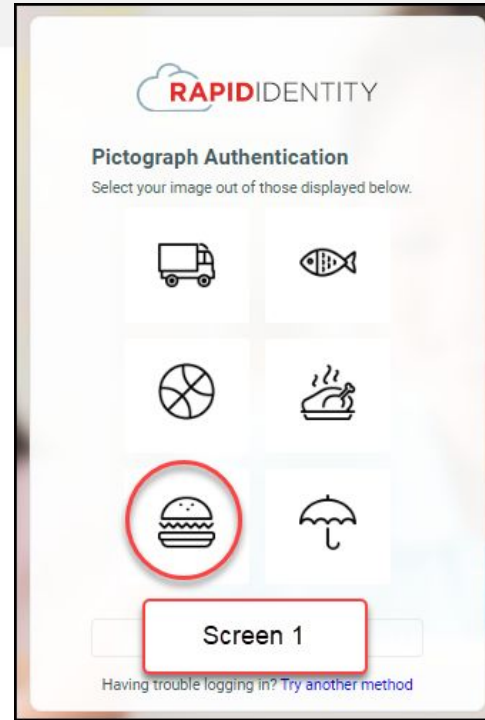
- Pictographs are a series of pictures that students can tap on a touchscreen device, or click with a mouse button
  - Helpful for young students, special education, and students acquiring the English language
- The settings here are Use the Default Image Pool, and there are 36 images to choose from
  - This is a sample of what those images look like:



# Configuration Policies - Authentication Policies - Pictograph

## MFA methods designed for students

- Number of Images to Choose: This number is how many pictures a user has to tap to login (maximum 18)
  - Best practice: 2 should be the minimum (1 is too easy to 'brute force attack')
- Number of Images to Challenge: The total number of pictures that show on the screen (maximum 18)
- The first time the user logs in to their account, they will be asked to choose their pictures, just like setting a new password
- Ex 2 and 6 = they will choose 2 images from two screens with six images on each screen



# Configuration Policies - Authentication Policies

- User Agreement at login page
  - Requirement from cybersecurity insurance agencies
- Can create multiple user agreements because each auth policy can have a different agreement assigned to it
- Show one time, or at every login

The screenshot displays the 'Authentication Policies' configuration page in the Identity Automation console. The left-hand navigation menu is expanded to show 'Authentication Policies', with 'User Agreement' selected and highlighted by a red box. A red arrow points from this menu item to the 'User Agreement' tab in the main configuration area. The 'User Agreement' tab is active, showing a table with columns for 'Select User Agreement' and 'Recurrence'. The 'Select User Agreement' column has a dropdown menu open, with 'Default User Agreement' selected and highlighted by a red box. The 'Recurrence' column shows 'Every Time'.

Select User Agreement	Recurrence
Default User Agreement	Every Time





# RapidIdentity Cloud Authentication Features

---

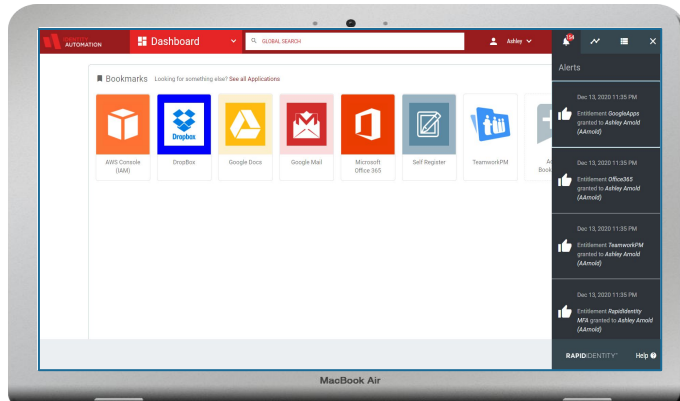


- MFA for Windows Login and Cloud Apps
- IdP for Classroom Management Tools
- Customizable Login Page
- Configurable Single Sign-On (*Bring Your Own Portal!*)
- Persona-Based Experiences
- Mobile Support
- User Friendly Self-Service Capabilities

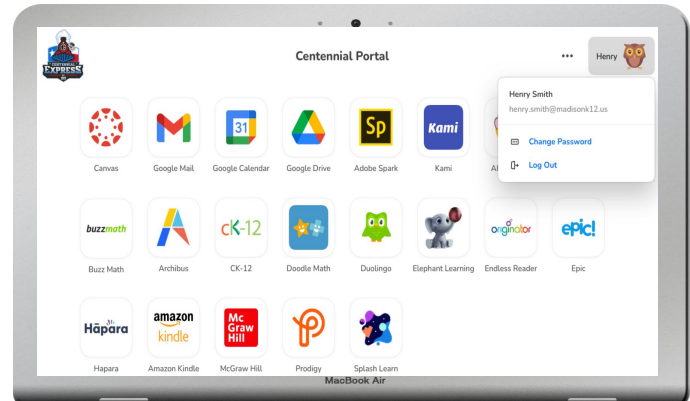


# RapidIdentity Cloud Authentication Features

## Enterprise View for RI

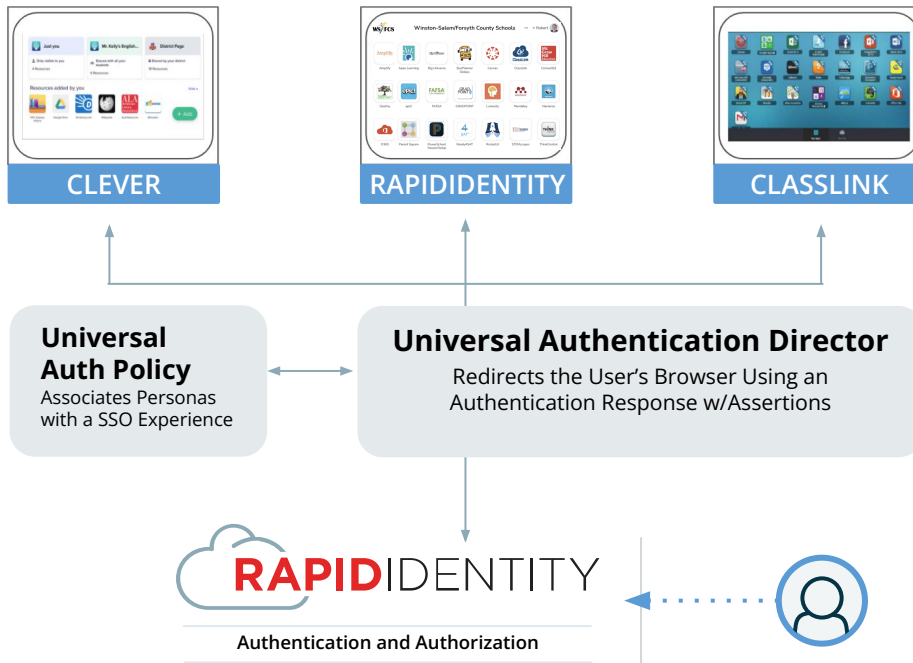


## GO! View for RI



# RapidIdentity Cloud Authentication Features

## -Universal Authentication Director



- Provides a Persona-based Portal Experience Aligned with Users Needs
- Seamlessly Redirects Users after Authentication to the Portal of Choice
- Extends Existing Persona-based SSO Experience to include Clever and ClassLink Portal



# RapidIdentity Cloud Authentication Features

## RapidIdentity Windows Authentication

---



- Native Windows Device Authentication with RapidIdentity
- Supports Domain Joined and Non-domain Joined Devices
- Provides Seamless Access into Portal





IDENTITY  
AUTOMATION

Q&A

---

