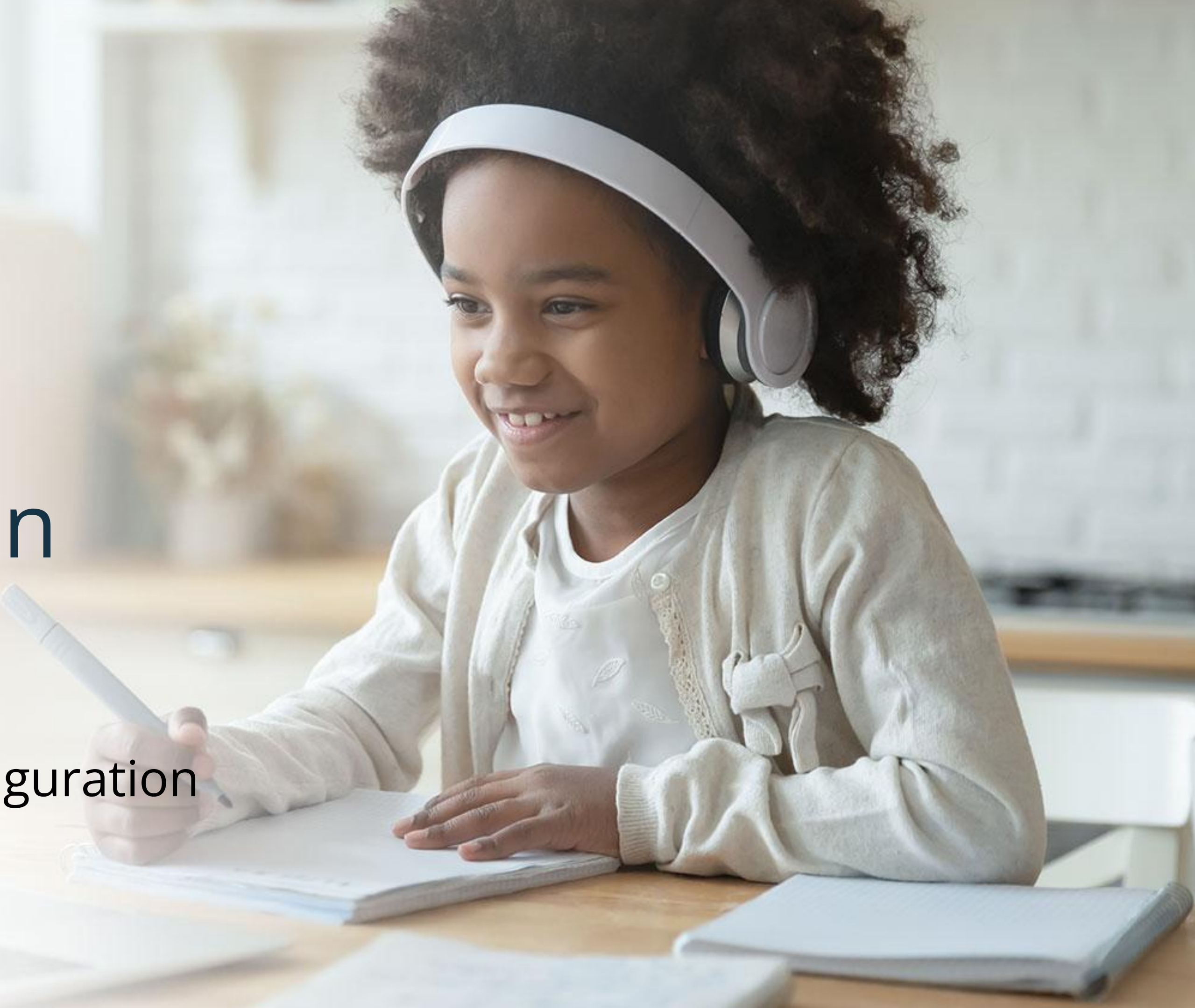
IDENTITY AUTOMATION



# Authentication

RapidIdentity IdP &
Federated Partner Configuration

# Agenda

01 Why now?

02 Productivity vs Security

03 RI Authentication Overview

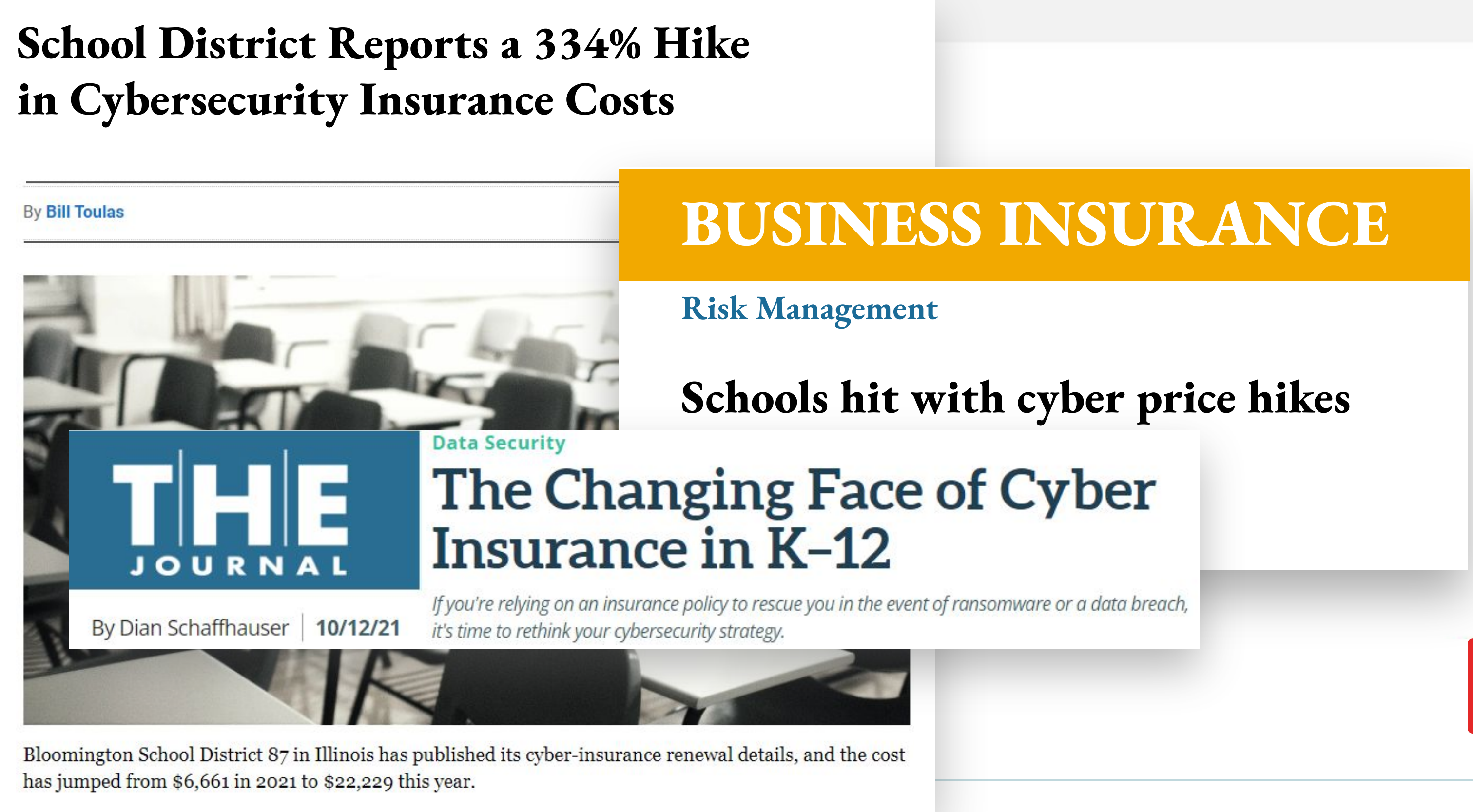
04 Single Sign-on & Federation

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

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

THE JOURNAL

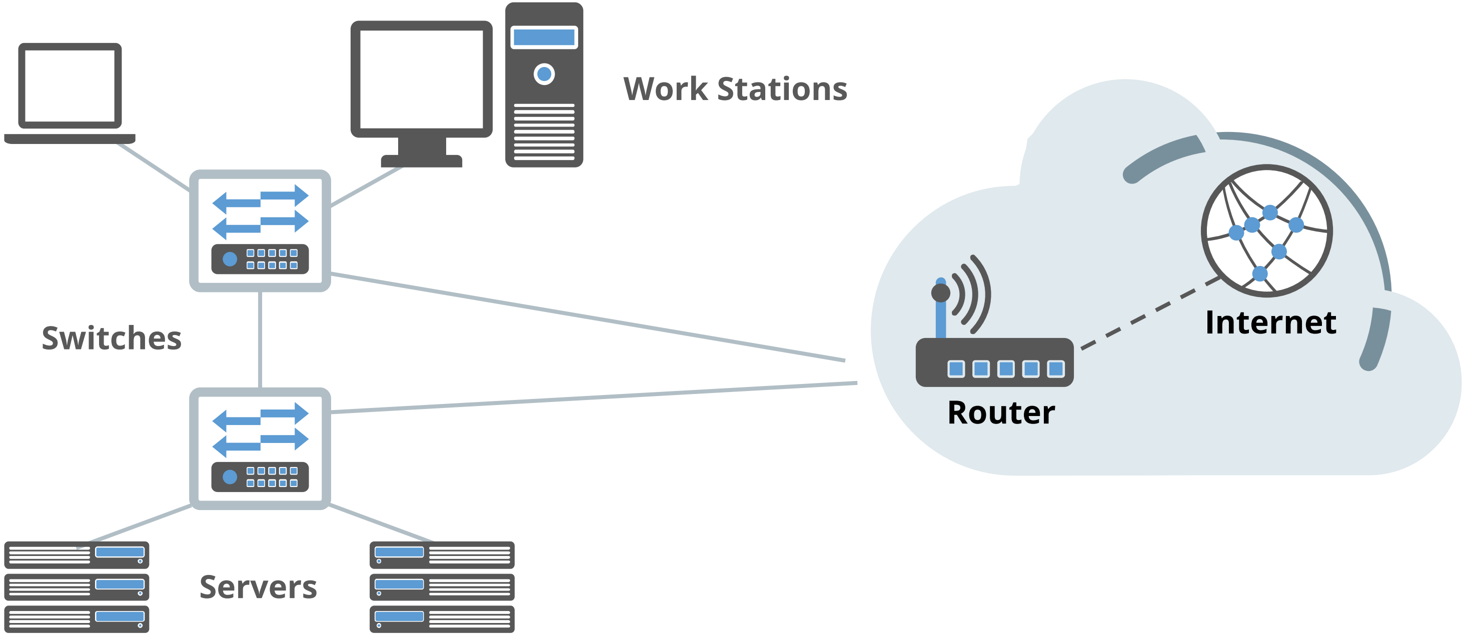
Data Security

## 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.*

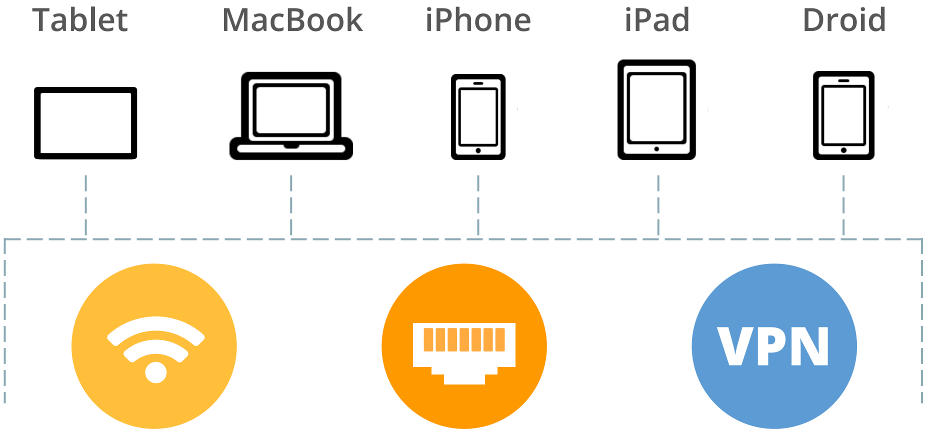
By Dian Schaffhauser | 10/12/21

# Traditional Perimeter



# Remote Learning: The Need for Phishing-Resistant Authentication

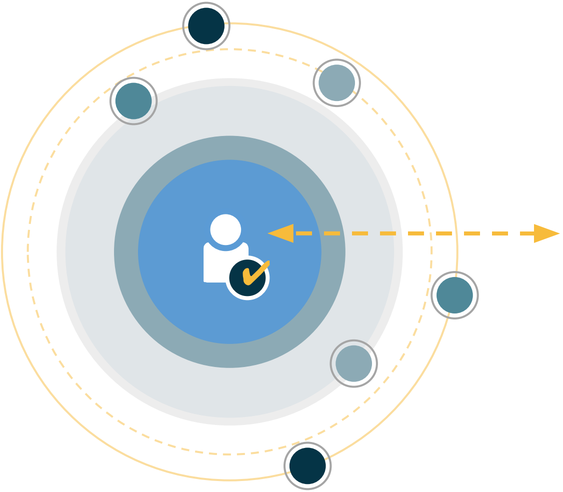
ANY DEVICE
ANY NETWORK



# 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

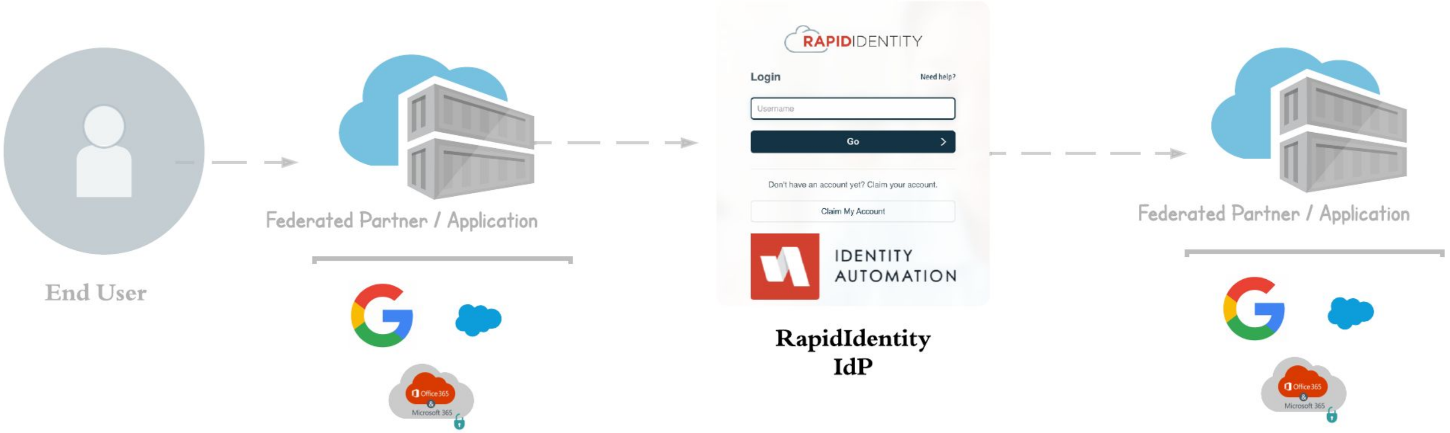
Federation

# 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 intiated)**



End User

Federated Partner / Application

RAPIDIDENTITY

Login

Need help?

Username

Go

Don't have an account yet? Claim your account.

Claim My Account

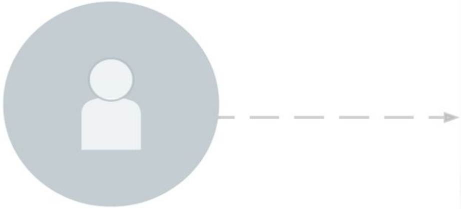
IDENTITY AUTOMATION

**RapidIdentity IdP**

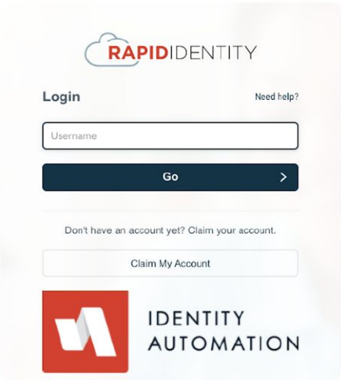
Federated Partner / Application

# Single Sign On with RapidIdentity - User Workflow #2

## Using the RapidIdentity Dashboard



End User



RAPIDIDENTITY

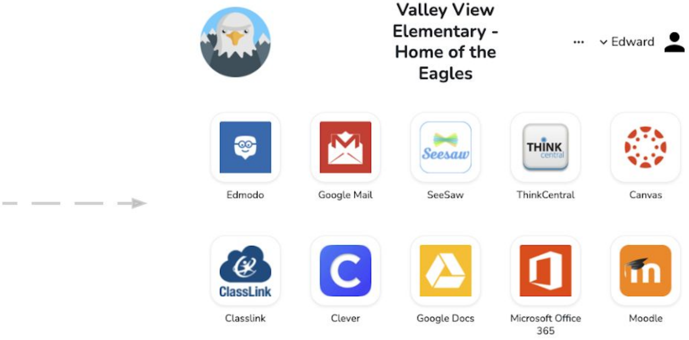
Login

Username

Don't have an account yet? Claim your account.

IDENTITY AUTOMATION

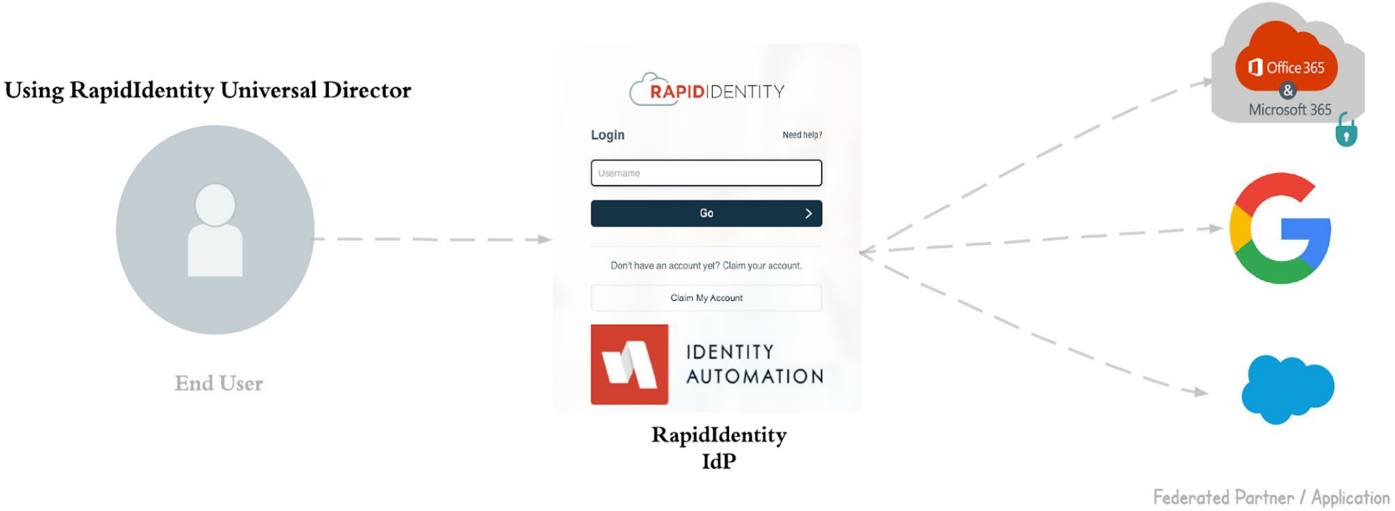
RapidIdentity IdP



Valley View Elementary - Home of the Eagles

RapidIdentity SSO dashboard

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



Using RapidIdentity Universal Director

End User

RapidIdentity IdP

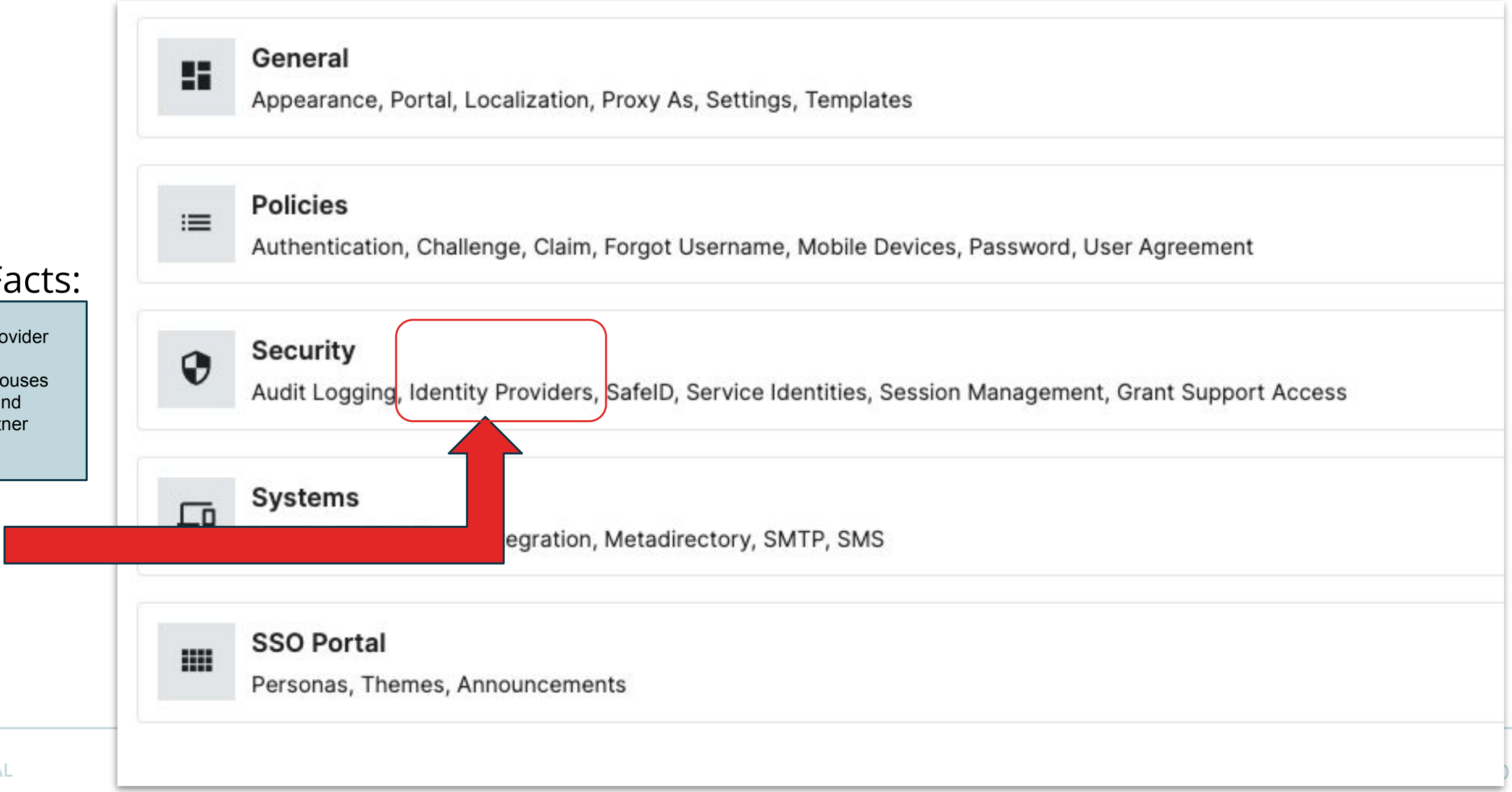
Federated Partner / Application

Don't have an account yet? Claim your account.

# Using RapidIdentity as an Identity Provider - Configuration

Useful Facts:

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



**General**

Appearance, Portal, Localization, Proxy As, Settings, Templates

**Policies**

Authentication, Challenge, Claim, Forgot Username, Mobile Devices, Password, User Agreement

**Security**

Audit Logging, Identity Providers, SafeID, Service Identities, Session Management, Grant Support Access

**Systems**

egration, Metadirectory, SMTP, SMS

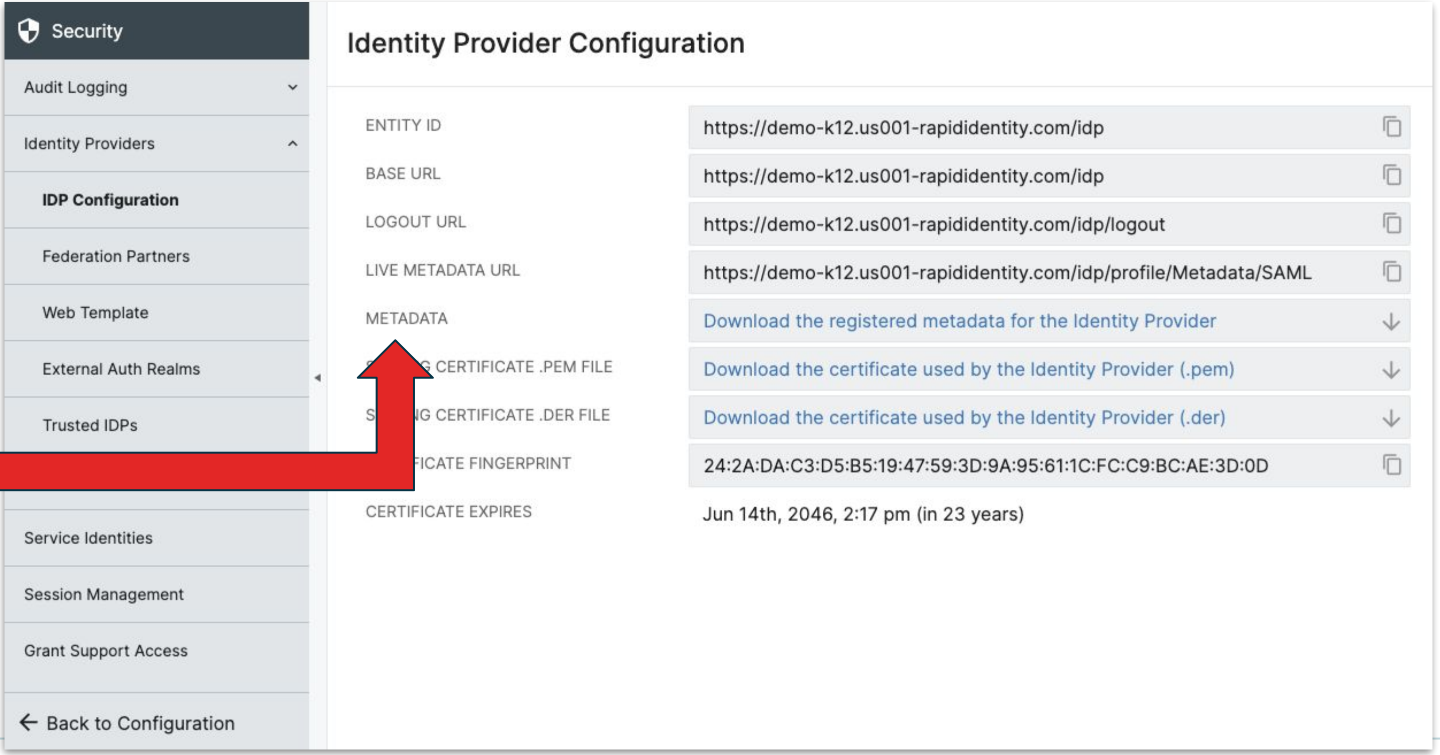
**SSO Portal**

Personas, Themes, Announcements

# Using RapidIdentity as an Identity Provider - Configuration

## Useful Facts:

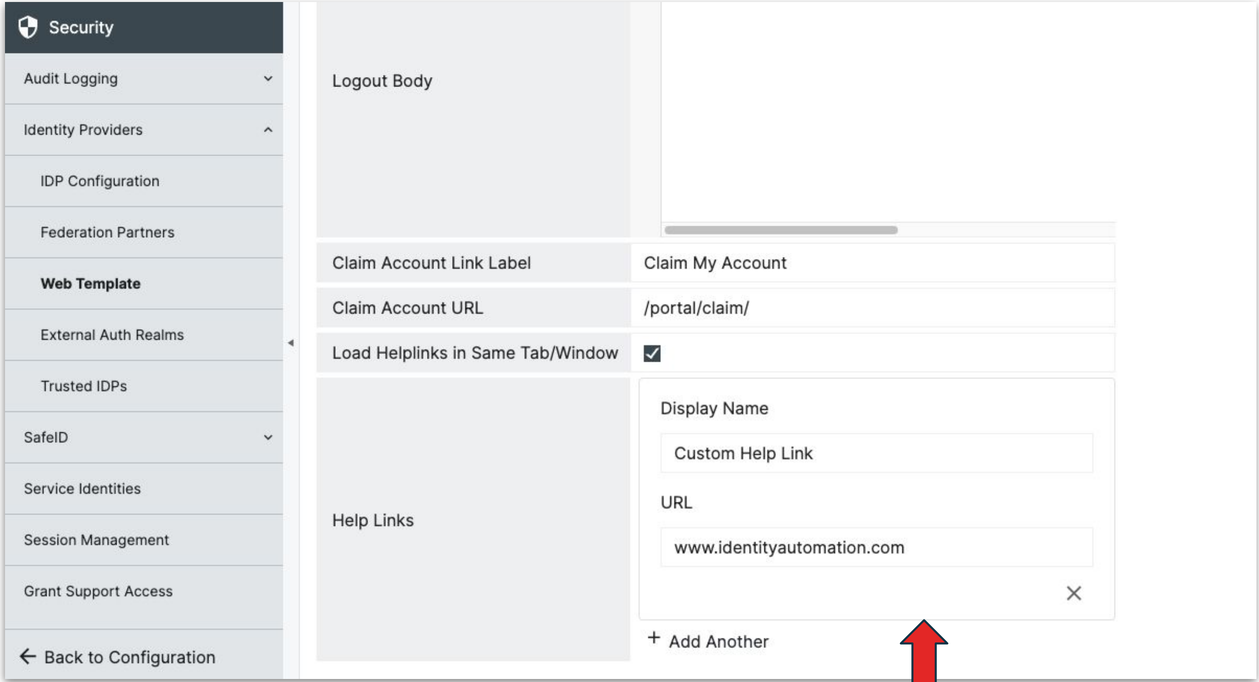
For more information about RapidIdentity Metadata and IdP see the Knowledge base article: [RapidIdentity IdP Configuration]()



### Identity Provider Configuration

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

# Using RapidIdentity as an Identity Provider - Configuration



Logout Body

Claim Account Link Label: Claim My Account

Claim Account URL: /portal/claim/

Load Helplinks in Same Tab/Window: ☑

Help Links

Display Name: Custom Help Link

URL: www.identityautomation.com

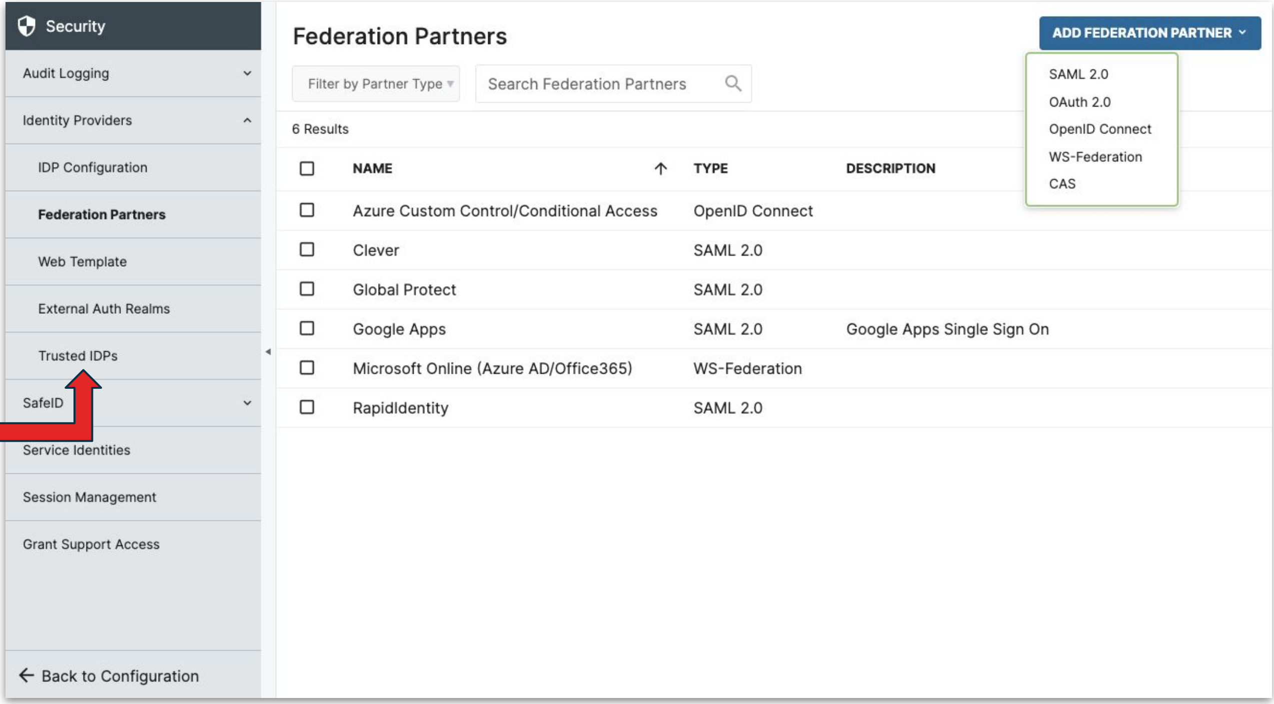
## Useful Facts:

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

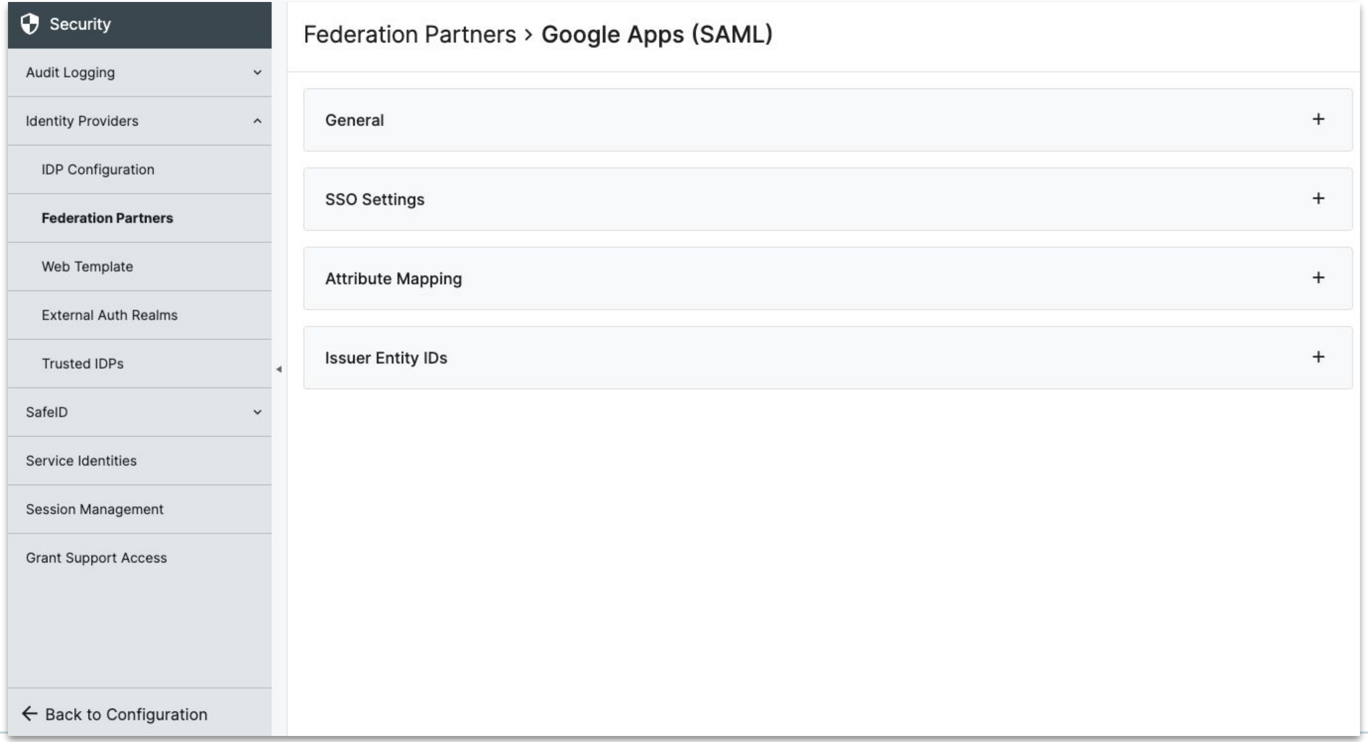
6 Results

| ☐ | 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 | |

# Using RapidIdentity as an Identity Provider - Configuration

## Useful Facts:

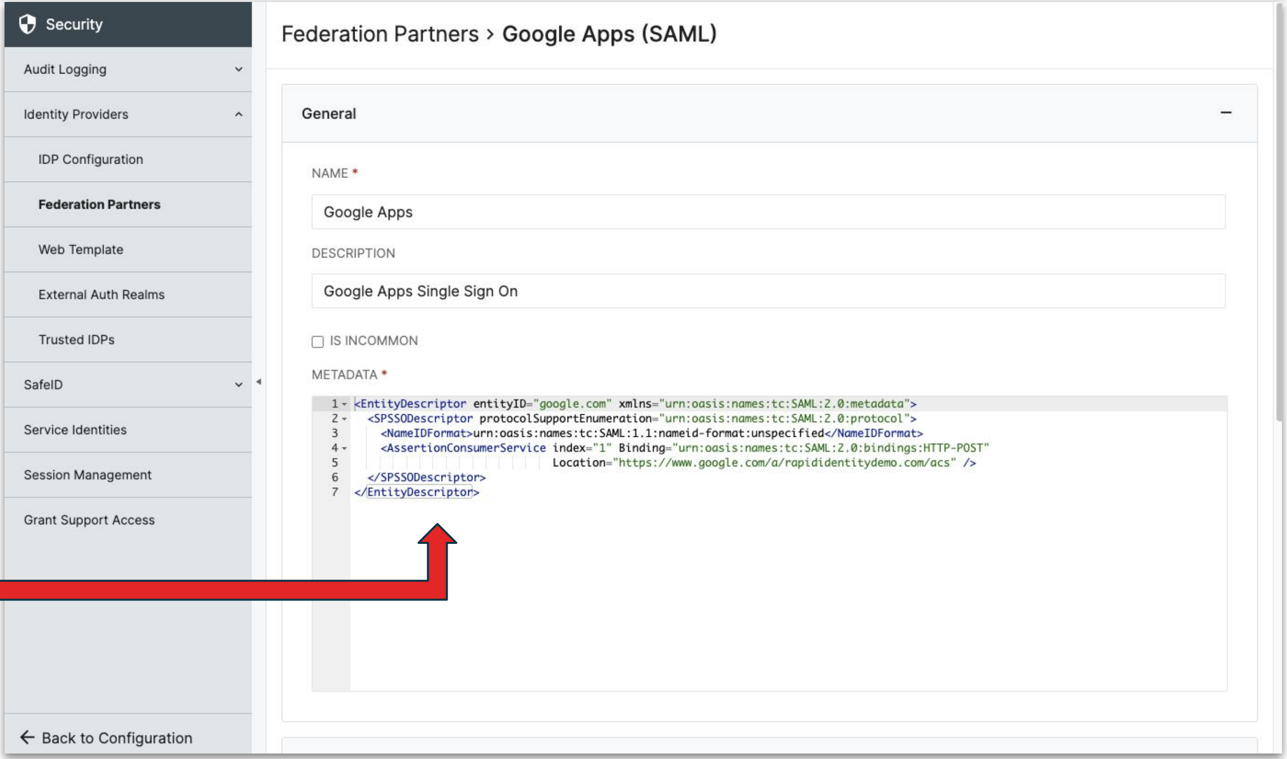
RapidIdentity is commonly used as the primary Identity Provider for Google domains. For more information on this configuration, and step by step instructions see the knowledge base article: [SSO with Google]



# 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.



Federation Partners › Google Apps (SAML)

General

NAME *

Google Apps

DESCRIPTION

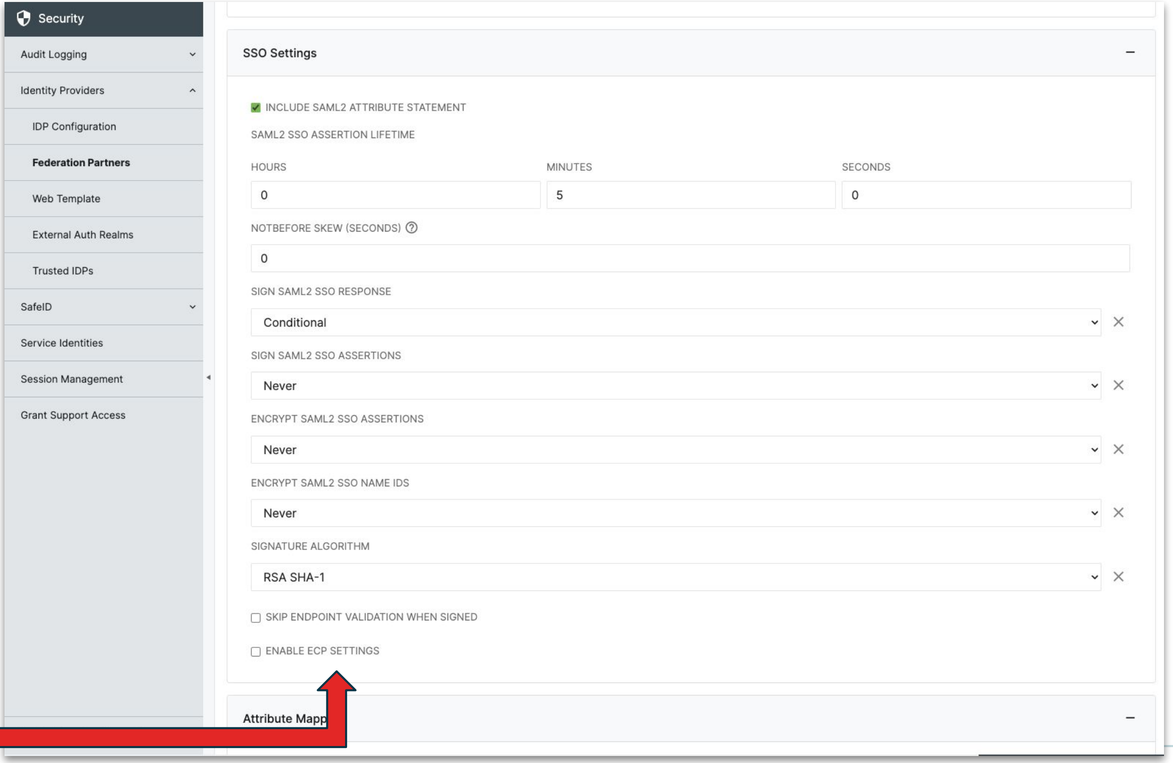
Google Apps Single Sign On

□ IS INCOMMON

METADATA *

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

# Using RapidIdentity as an Identity Provider - Configuration



SSO Settings

☑ 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

Attribute Mapp

## Useful Facts:

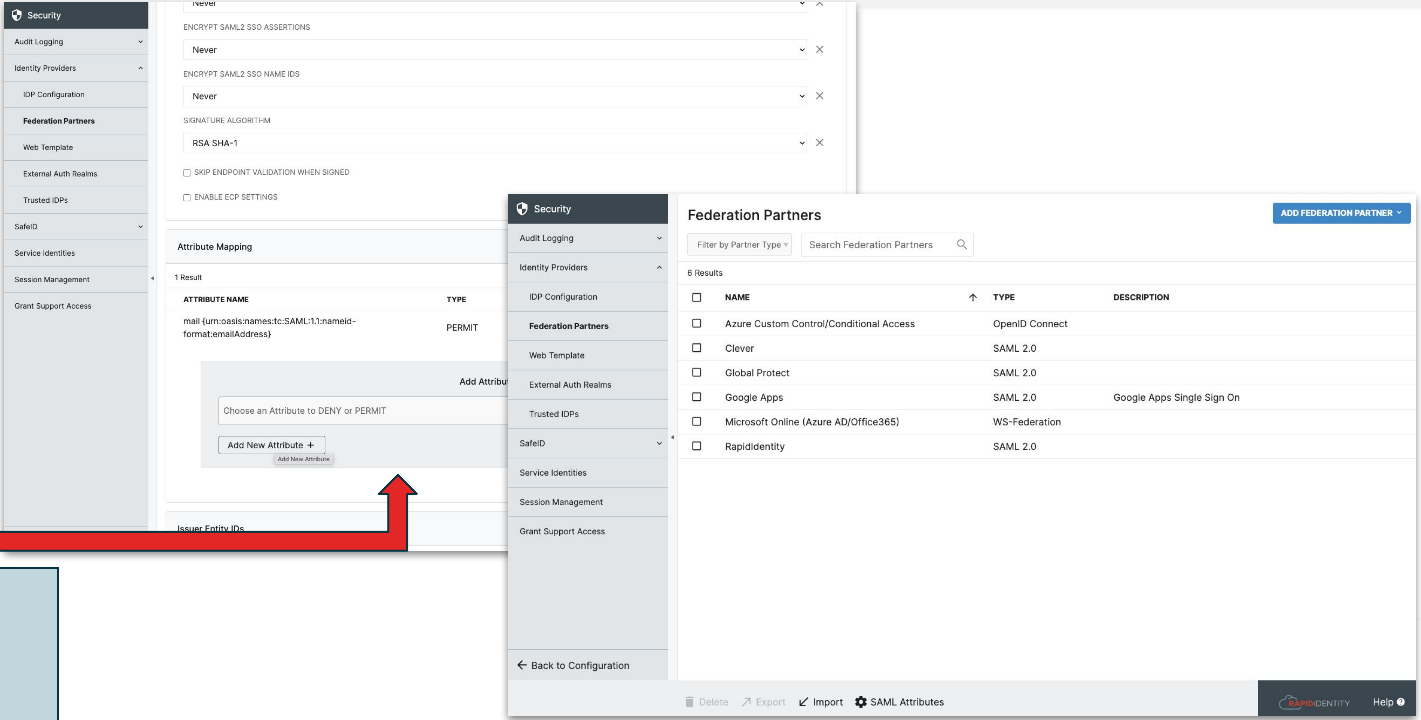
When selecting the Enable ECP Settings checkbox, the ECP Settings section will become available beneath the SSO Settings along with the configuration options. In this case, ECP settings are not to be enabled.

# 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.



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

Attribute Mapping

1 Result

| ATTRIBUTE NAME | TYPE |
|---|---|
| mail {urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress} | PERMIT |

Add Attribu

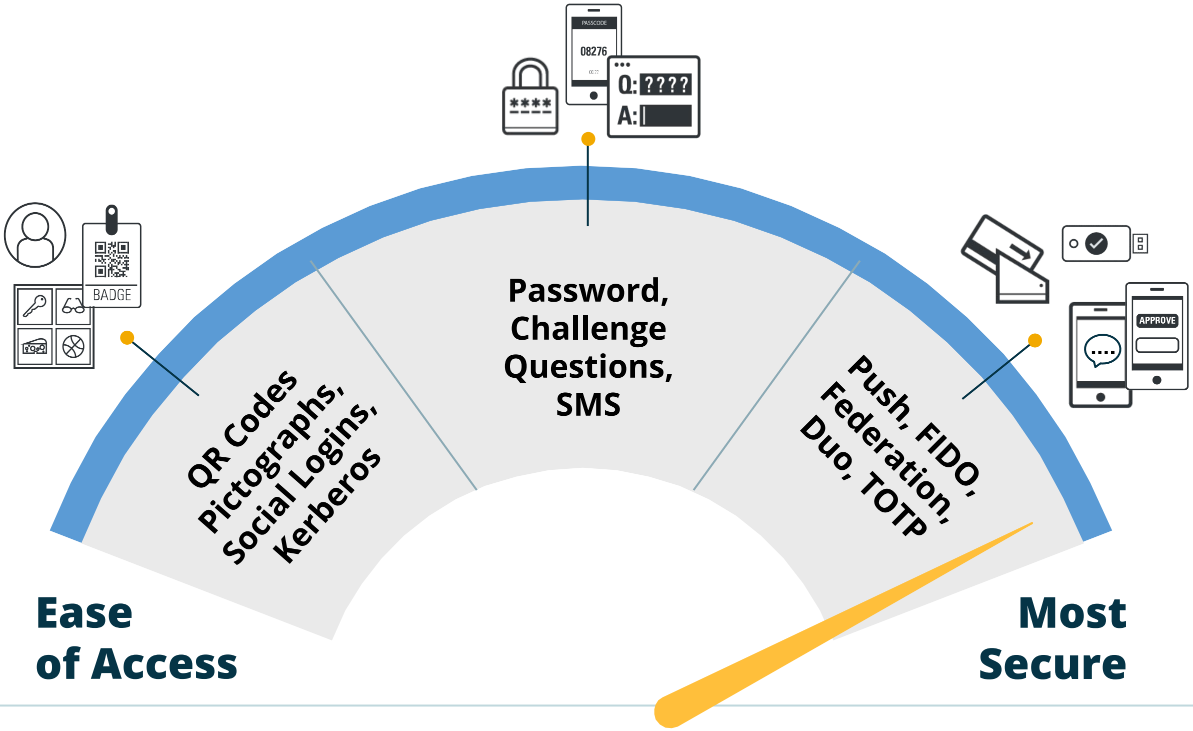
Choose an Attribute to DENY or PERMIT

Federation Partners

6 Results

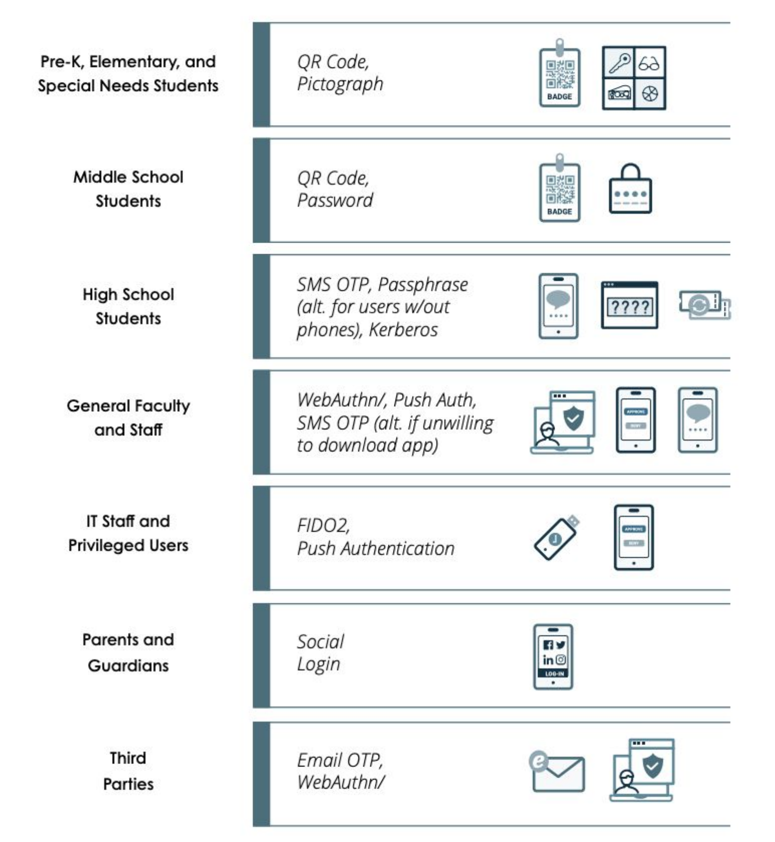
| ☐ | NAME | TYPE | DESCRIPTION |
|---|---|---|---|
| ☐ | Azure Custom Control/Conditional Access | OpenID Connect | |
| ☐ | Clever | SAML 2.0 | |
| ☐ | Global Protect | SAML 2.0 | |
| ☐ | Google Apps | SAML 2.0 | Google Apps Single Sign On |
| ☐ | Microsoft Online (Azure AD/Office365) | WS-Federation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

# Tailor Authentication to the Actual User



# Authentication Methods

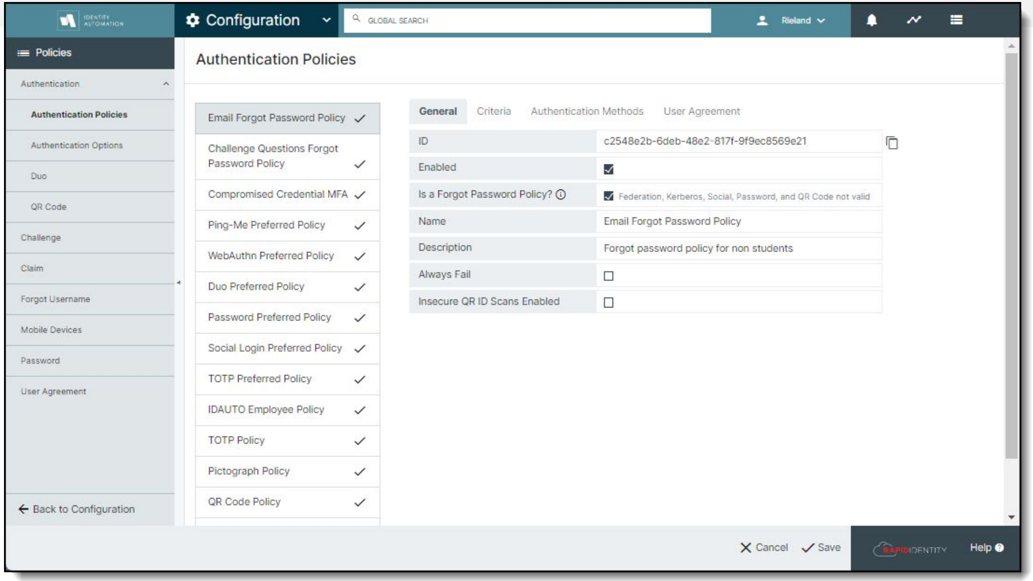
For more information about MFA deployment best practices, and passwordless workflows. See K-12 MFA Guide: Make Districtwide Multi-Factor Authentication Not Only a Reality— But a Success



| | |
|---|---|
| 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)



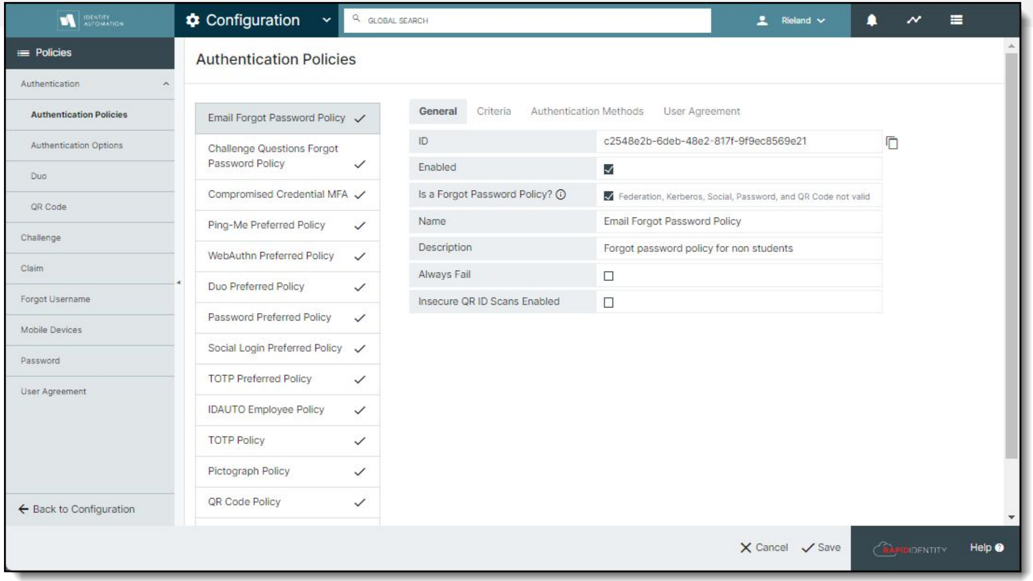
Authentication Policies

- 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 ✓

| | |
|---|---|
| ID | c2548e2b-6deb-48e2-817f-9f9ec8569e21 |
| Enabled | ☑ |
| Is a Forgot Password Policy? ⓘ | ☑ Federation, Kerberos, Social, Password, and QR Code not valid |
| Name | Email Forgot Password Policy |
| Description | Forgot password policy for non students |
| Always Fail | □ |
| Insecure QR ID Scans Enabled | □ |

# 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



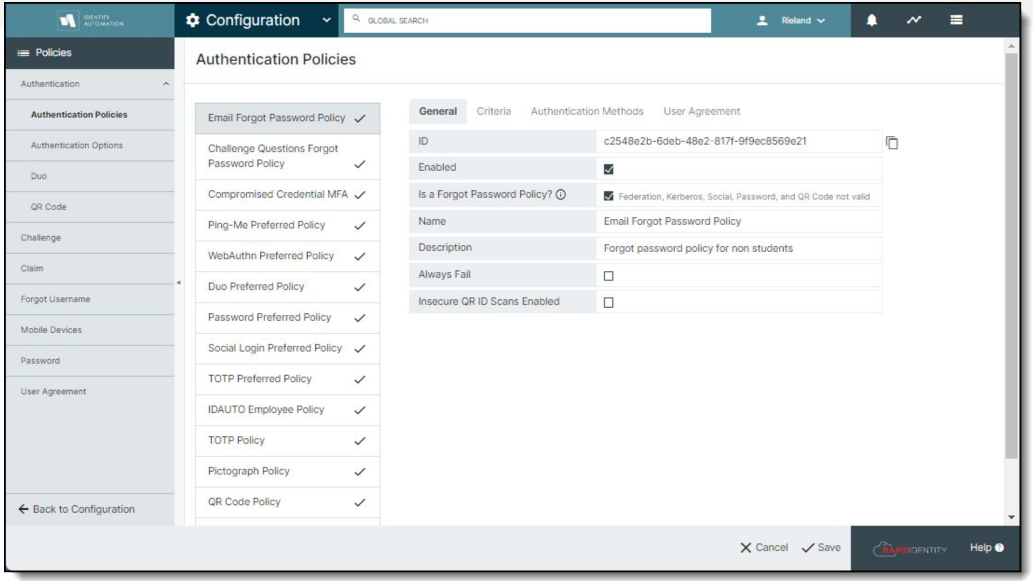
Authentication Policies

- 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 ✓

| | |
|---|---|
| ID | c2548e2b-6deb-48e2-817f-9f9ec8569e21 |
| Enabled | ☑ |
| Is a Forgot Password Policy? | ☑ Federation, Kerberos, Social, Password, and QR Code not valid |
| Name | Email Forgot Password Policy |
| Description | Forgot password policy for non students |
| Always Fail | ☐ |
| Insecure QR ID Scans Enabled | ☐ |

# 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



Authentication Policies

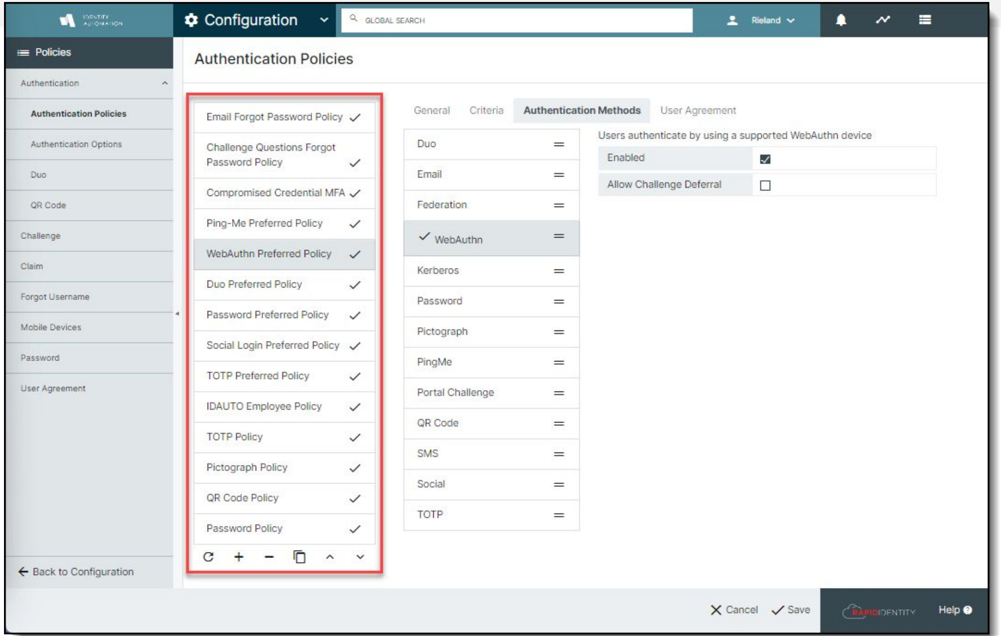
- Email Forgot Password Policy ✓
- Challenge Questions Forgot Password Policy ✓
- Compromised Credential MFA ✓
- Ping-Me Preferred Policy ✓
- WebAuthn Preferred Policy ✓
- Duo Preferred Policy ✓
- Password Preferred Policy ✓
- Social Login Preferred Policy ✓
- TOTP Preferred Policy ✓
- IDAUTO Employee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

General | Criteria | Authentication Methods | User Agreement

| | |
|---|---|
| ID | c2548e2b-6deb-48e2-817f-9f9ec8569e21 |
| Enabled | ☑ |
| Is a Forgot Password Policy? ⓘ | ☑ Federation, Kerberos, Social, Password, and QR Code not valid |
| Name | Email Forgot Password Policy |
| Description | Forgot password policy for non students |
| Always Fail | ☐ |
| Insecure QR ID Scans Enabled | ☐ |

# 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



Authentication Policies

- 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 ✓
- Password Policy ✓

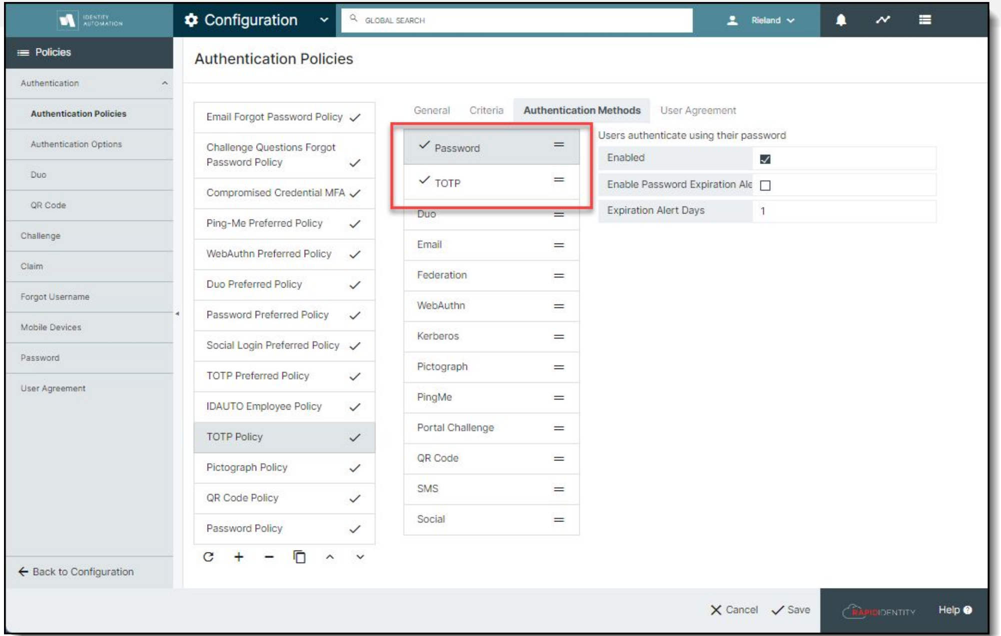
Authentication Methods: Duo, Email, Federation, ✓ WebAuthn, Kerberos, Password, Pictograph, PingMe, Portal Challenge, QR Code, SMS, Social, TOTP

Users authenticate by using a supported WebAuthn device

| | |
|---|---|
| Enabled | ☑ |
| Allow Challenge Deferral | □ |

# 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



Authentication Policies

| Policy | |
|---|---|
| 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 | ✓ |
| Password Policy | ✓ |

Authentication Methods:

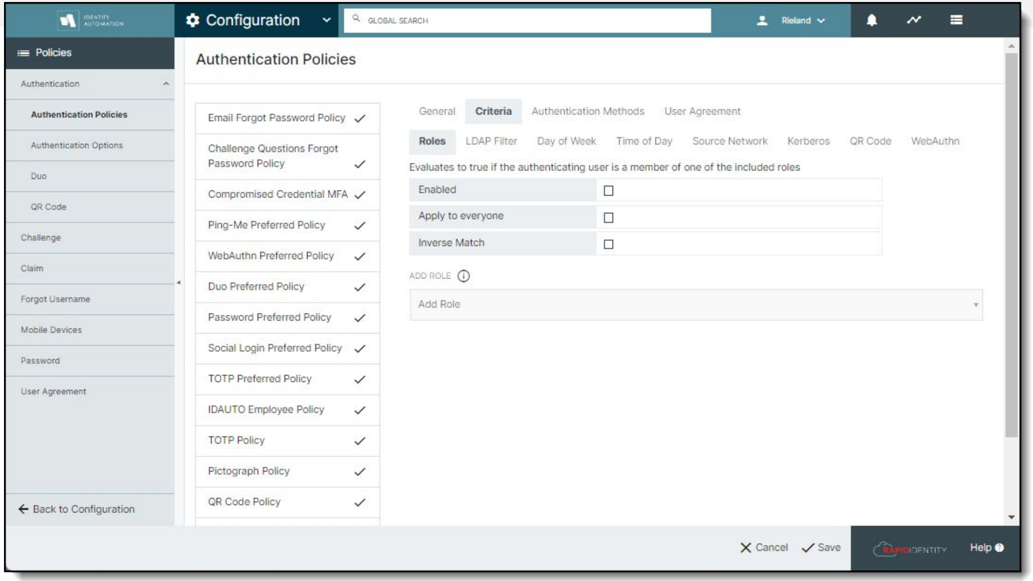
- ✓ Password
- ✓ TOTP
- Duo
- Email
- Federation
- WebAuthn
- Kerberos
- Pictograph
- PingMe
- Portal Challenge
- QR Code
- SMS
- Social

Users authenticate using their password

| | |
|---|---|
| Enabled | ☑ |
| Enable Password Expiration Ale | □ |
| Expiration Alert Days | 1 |

# 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



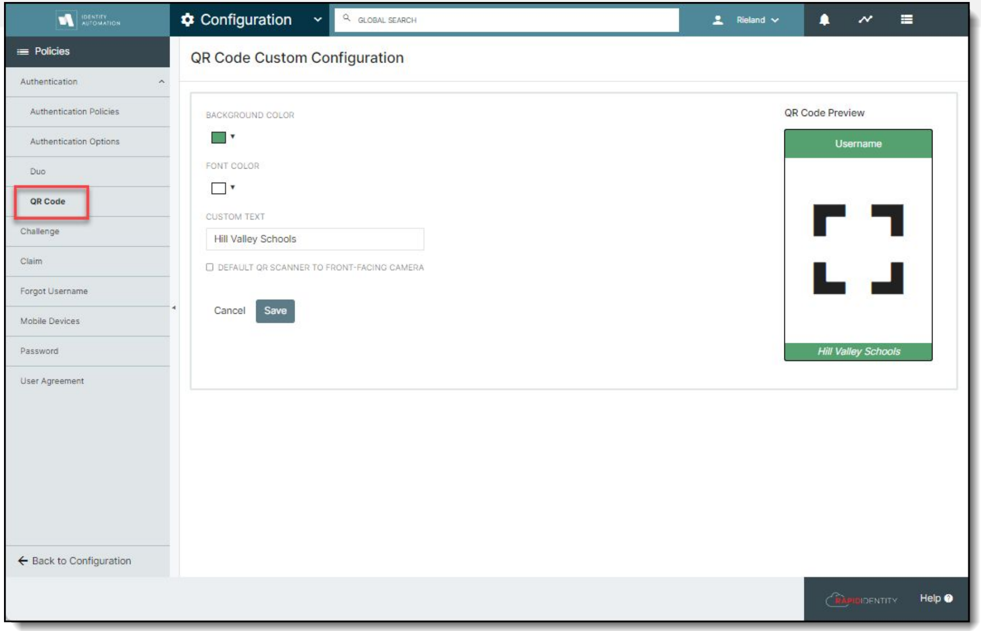
Evaluates to true if the authenticating user is a member of one of the included roles

| | |
|---|---|
| Enabled | □ |
| Apply to everyone | □ |
| Inverse Match | □ |

# 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



QR Code Custom Configuration

BACKGROUND COLOR 🟩

FONT COLOR □

CUSTOM TEXT: Hill Valley Schools

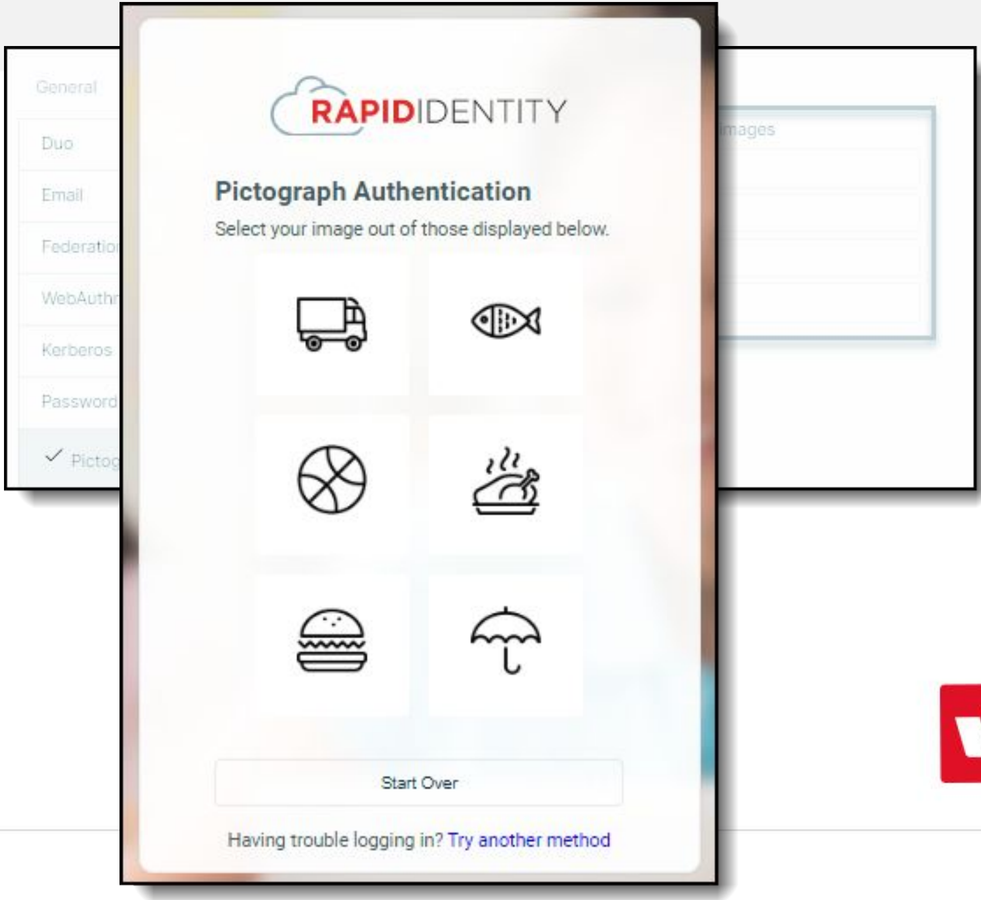
□ DEFAULT QR SCANNER TO FRONT-FACING CAMERA

Cancel Save

# 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:



Pictograph Authentication

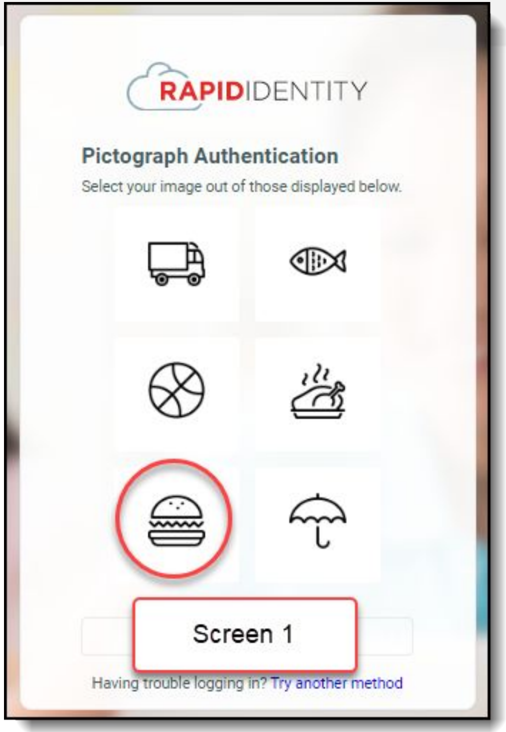
Select your image out of those displayed below.

Having trouble logging in? Try another method

# Configuration Policies - Authentication Policies - Pictograph

MFA methods designed for students

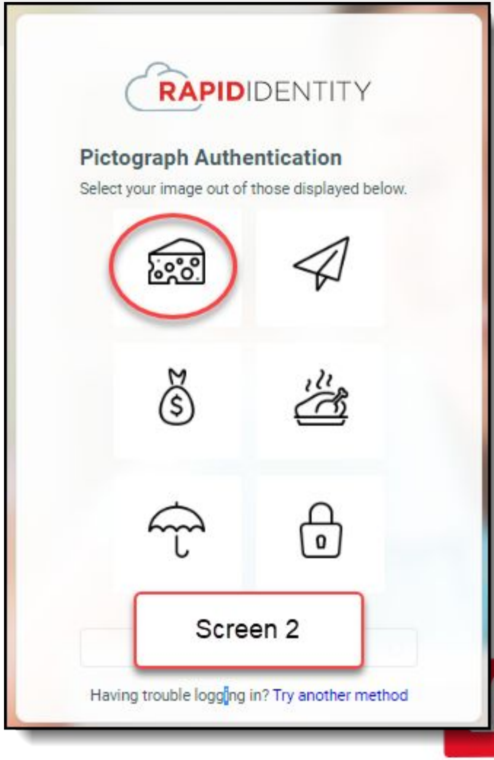
- Number of Images to Choose: This number is how many pictures a user has to tap to login (maximum 18)
  - Best practice: 2 should be the minimum (1 is too easy to 'brute force attack')
- Number of Images to Challenge: The total number of pictures that show on the screen (maximum 18)
- The first time 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



Pictograph Authentication

Select your image out of those displayed below.

Having trouble logging in? Try another method



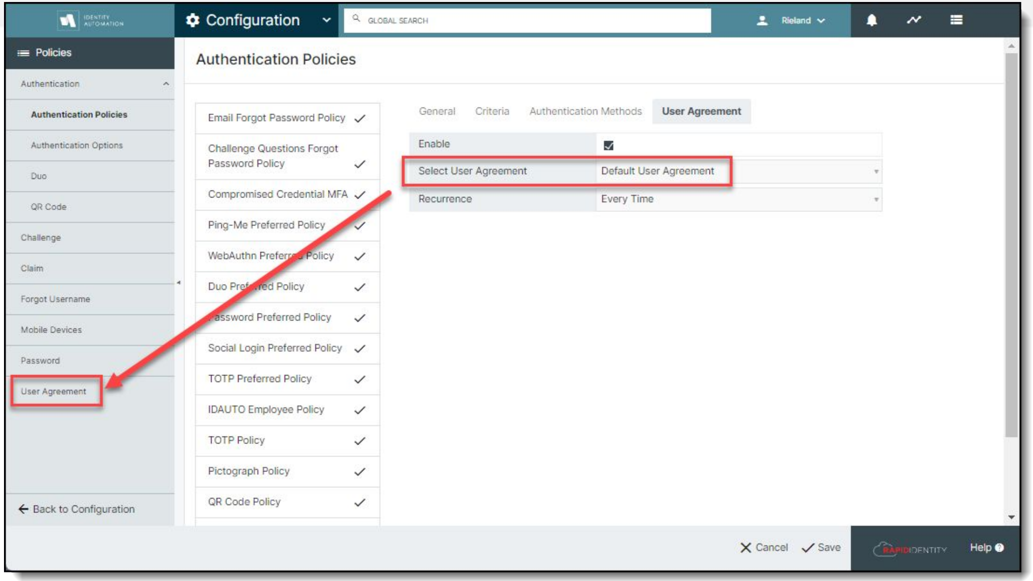
Pictograph Authentication

Select your image out of those displayed below.

Having trouble logging in? Try another method

# 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



Enable ☑

Select User Agreement: Default User Agreement

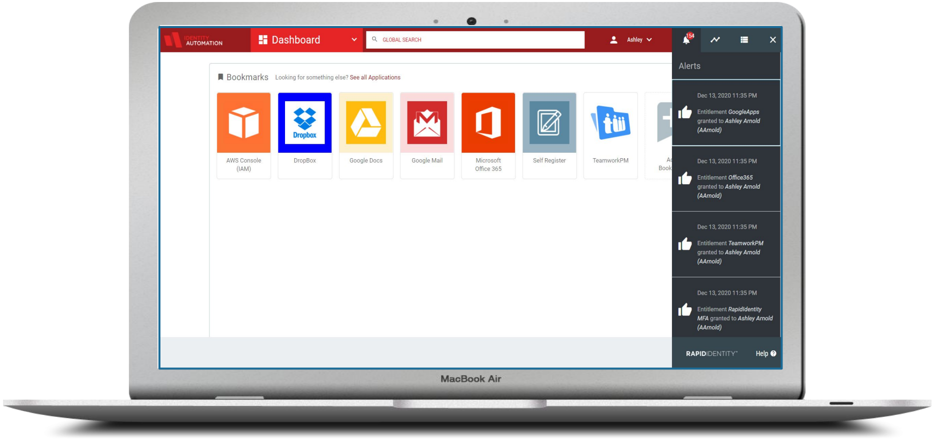
Recurrence: Every Time

# 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



Looking for something else? See all Applications

Alerts

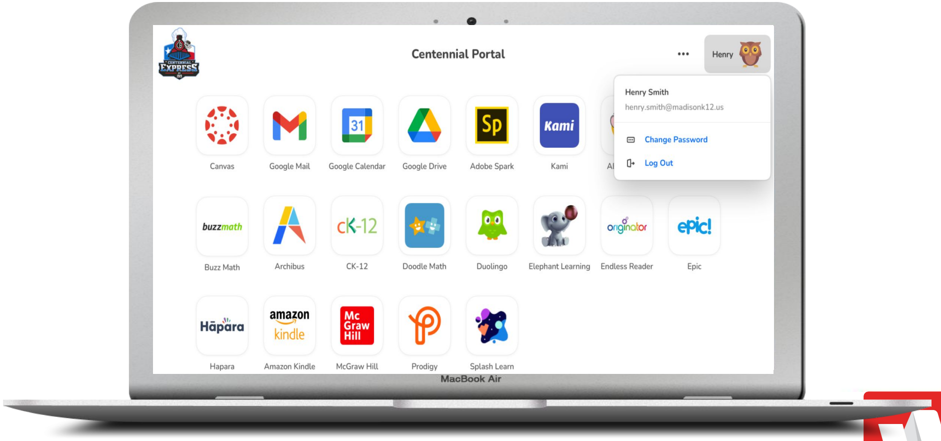
Dec 13, 2020 11:35 PM
Entitlement *GoogleApps* granted to *Ashley Arnold (AArnold)*

Dec 13, 2020 11:35 PM
Entitlement *Office365* granted to *Ashley Arnold (AArnold)*

Dec 13, 2020 11:35 PM
Entitlement *TeamworkPM* granted to *Ashley Arnold (AArnold)*

Dec 13, 2020 11:35 PM
Entitlement *RapidIdentity MFA* granted to *Ashley Arnold (AArnold)*

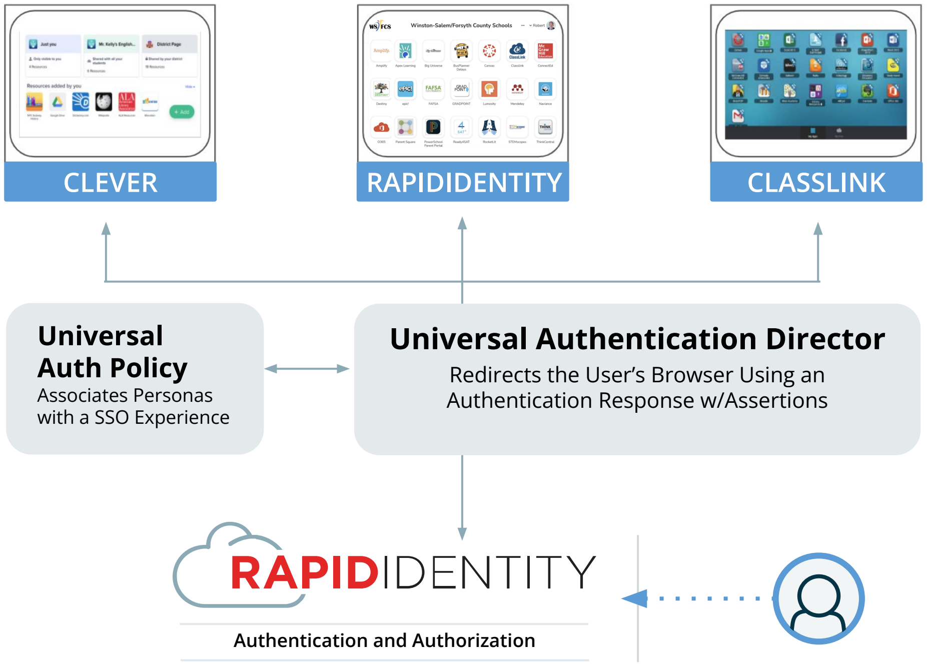
## GO! View for RI



Henry Smith
henry.smith@madisonk12.us

Change Password
Log Out

# RapidIdentity Cloud Authentication Features -Universal Authentication Director



CLEVER

RAPIDIDENTITY

CLASSLINK

**Universal Auth Policy**

Associates Personas with a SSO Experience

**Universal Authentication Director**

Redirects the User's Browser Using an Authentication Response w/Assertions

Authentication and Authorization

- 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

RapidIdentity Client for Windows
Click submit to begin logon
RapidIdentity Client for Windows
oxygen

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

IDENTITY AUTOMATION

# Q&A