IDENTITY AUTOMATION

People Module

Settings and Policies

Agenda

01 People Module Overview

02 People Settings

03 Challenge Questions

04 Password Policies

05 Authentication Policies (MFA)

06 Forgot Username

07 Claim Account

CONFIDENTIAL

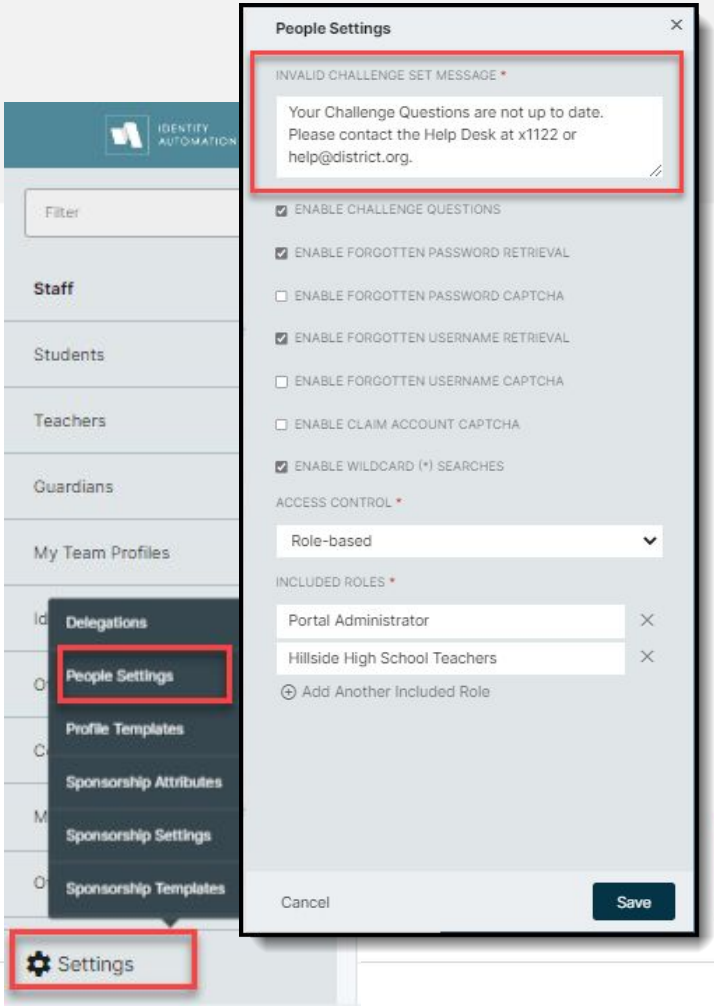
People Module Overview (Major Use Cases)

- Manage account profiles via Delegations
- Enable self-service actions on the MY delegation type
- Enable Actions, including change password and reset authentication
- Override active/disabled status

CONFIDENTIAL

People Settings

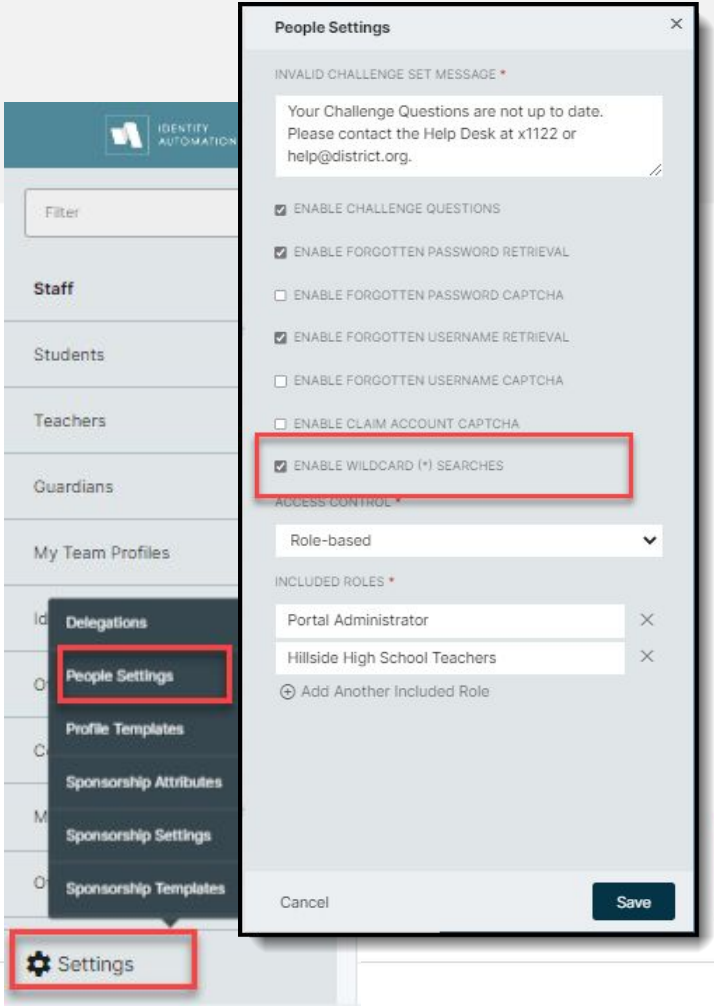
- Invalid Challenge Set Message
  - Default message ends after “help desk.”
  - Consider adding a phone number, email address, or information to sign in to your ticketing system
- Enable Wildcard (*) Searches - Example: search for *jackson* finds all user accounts where the first or last name, or school name, is Jackson.
  - Disabling this feature will require a full name search, ex. Jackson Smith or Jackson Elementary School
- Deprecated settings: Challenge Questions, Forgot Password and Username
  - Settings moved to Configuration > Policies



CONFIDENTIAL

People Settings

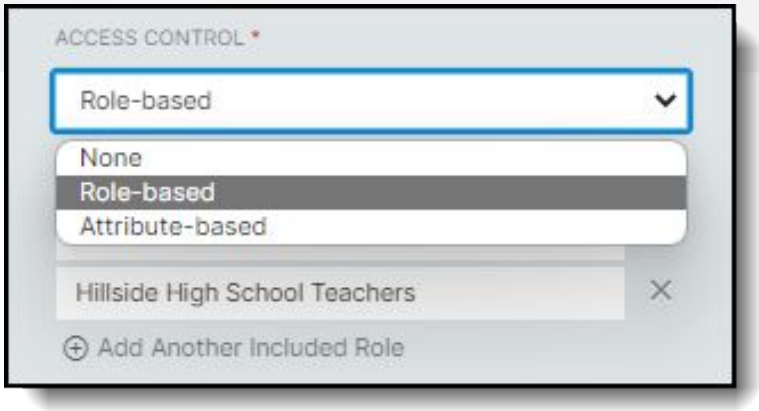
- Invalid Challenge Set Message
  - Default message ends after “help desk.”
  - Consider adding a phone number, email address, or information to sign in to your ticketing system
- Enable Wildcard (*) Searches - Example: search for *jackson* finds all user accounts where the first or last name, or school name, is Jackson.
  - Disabling this feature will require a full name search, ex. Jackson Smith or Jackson Elementary School
- Deprecated settings: Challenge Questions, Forgot Password and Username
  - Settings moved to Configuration > Policies



CONFIDENTIAL

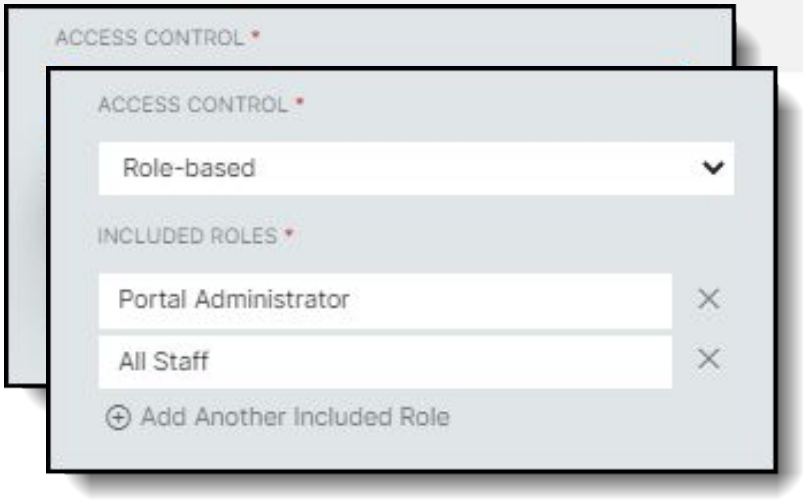
People Settings

- **Access Control**: Who can see People on the drop-down menu
  - **None** - Everyone with access to login to RapidIdentity can see People.
    - Doesn't automatically grant access to view all delegations.
    - Each delegation has its own access control via Delegation Source



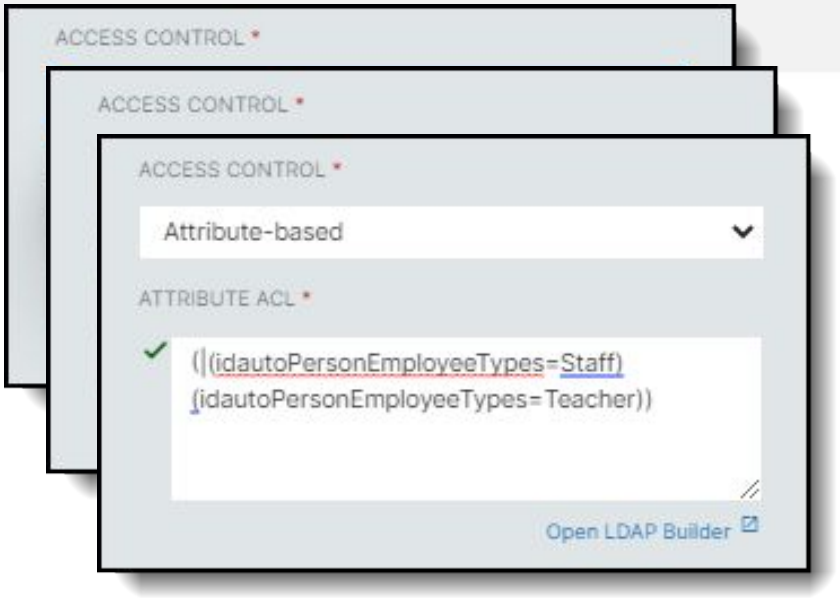
People Settings

- **Access Control**: Who can see People on the drop-down menu
  - **None** - Everyone with access to login to RapidIdentity can see People.
    - Doesn't automatically grant access to view all delegations.
    - Each delegation has its own granular access control.
- **Role-based** - If Role-based is selected, the field **Included Roles** will display. These are roles that exist in the Roles module.
  - Begin typing the role name to search
  - Multiple roles can be selected here by clicking **+Add Another Included Role**



People Settings

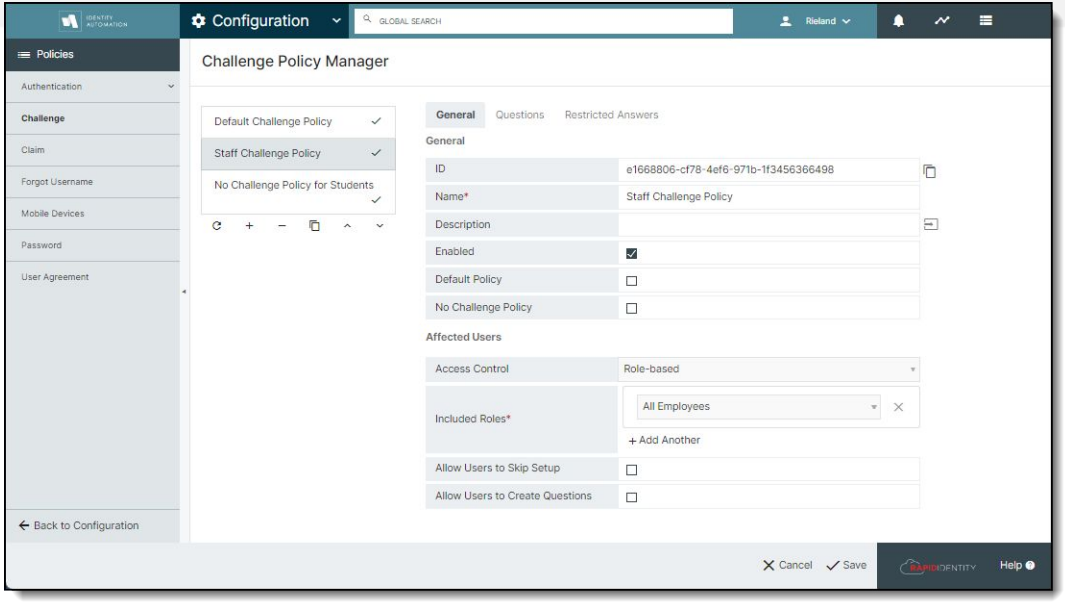
- **Access Control**: Who can see People on the drop-down menu
  - **None** - Everyone with access to login to RapidIdentity can see People.
    - Doesn't automatically grant access to view all delegations.
    - Each delegation has its own granular access control.
- **Role-based** - If Role-based is selected, the field **Included Roles** will display. These are roles that exist in the Roles Module.
  - Begin typing the role name to search
  - Multiple roles can be selected here by clicking **+Add Another Included Role**
- **Attribute-based** - If Attribute-based is selected, the **Attribute ACL** field displays.
  - Enter an LDAP filter here to grant access



CONFIDENTIAL

Configuration Policies - Challenge Questions

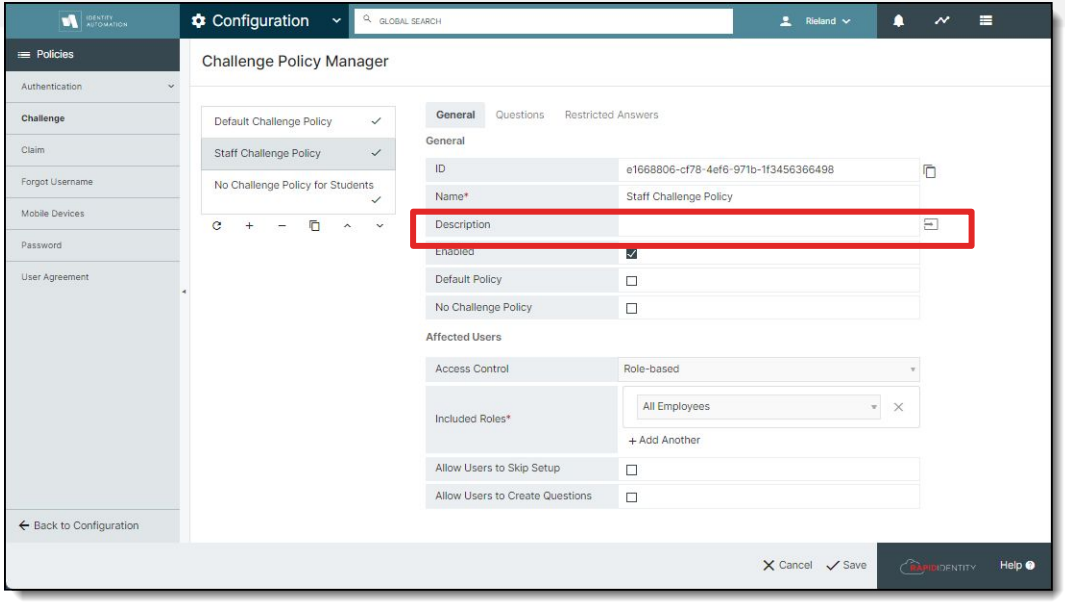
- Multiple policies for staff, students (early grades vs. later grades), sponsored accounts, or guardians
  - Policy details are defined here, then an Authentication Policy applies Challenge Questions to Forgot Password or MFA



CONFIDENTIAL

Configuration Policies - Challenge Questions

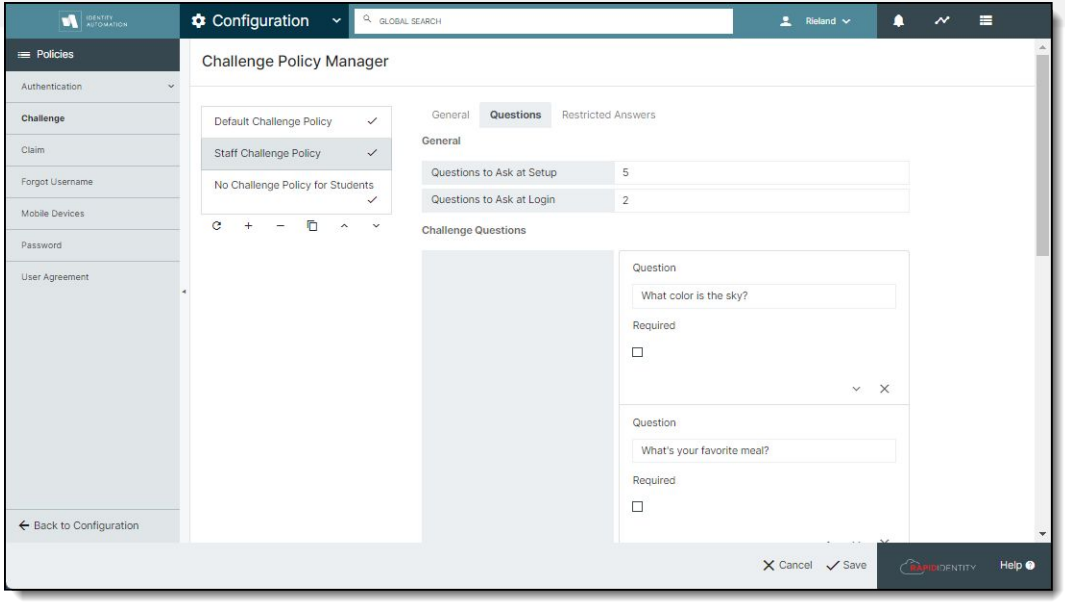
- Multiple policies for staff, students (early grades vs. later grades), sponsored accounts, or guardians
  - Challenge policy details are defined here, then an Authentication Policy applies Portal Challenge to Forgot Password or MFA
- Users see the Description during setup, so add detailed instructions
  - Number of questions to answer
  - Answers must be unique
  - Minimum length
  - Other rules defined in your policy



CONFIDENTIAL

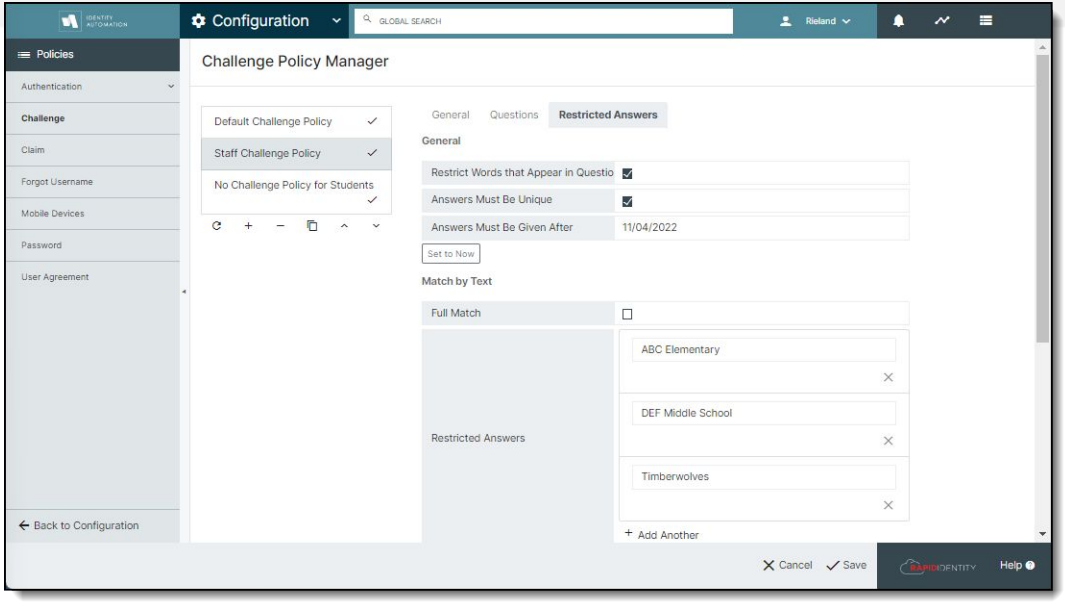
Configuration Policies - Challenge Questions

- Enter the number of questions to ask during initial setup
- Enter the number of questions to present to reset forgotten password, or use as a last-resort deviceless MFA method
- Add as many questions as selected in “Questions to Ask at Setup”
  - Need ideas? Use OWASP or other online resources
  - https://cheatsheetseries.owasp.org/
  - “Choosing and Using Security Questions Cheat Sheet”



Configuration Policies - Challenge Questions

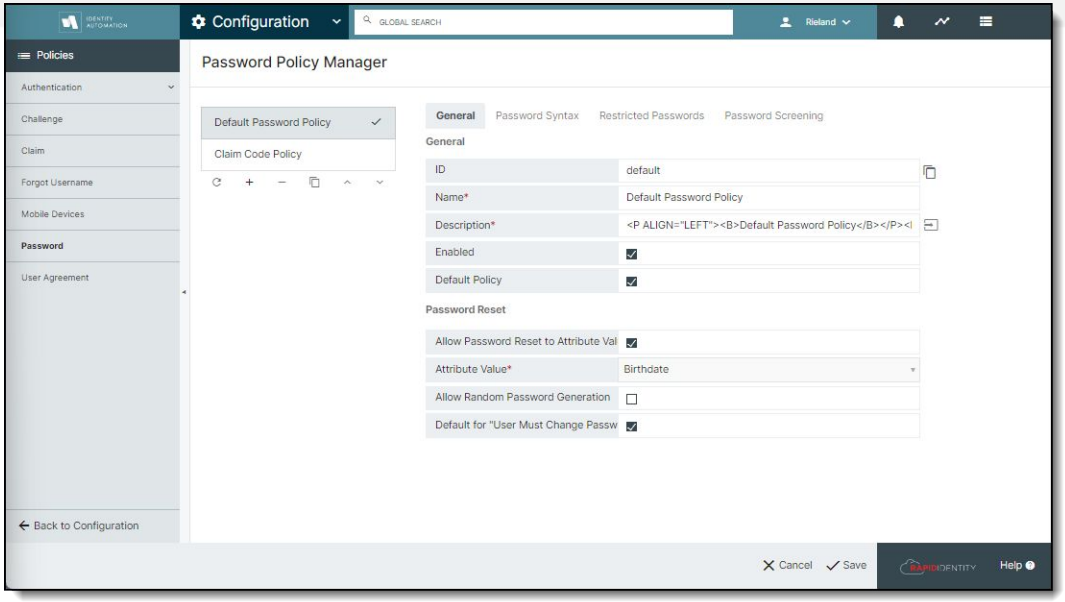
- Restricted answers:
  - Can’t use words used in the question
  - Answers to every question must be unique
  - Match By Text custom restrictions
  - Restrictions on metadirectory attributes, i.e. can’t use employee ID, first name, last name, etc. as an answer



CONFIDENTIAL

Configuration Policies - Passwords

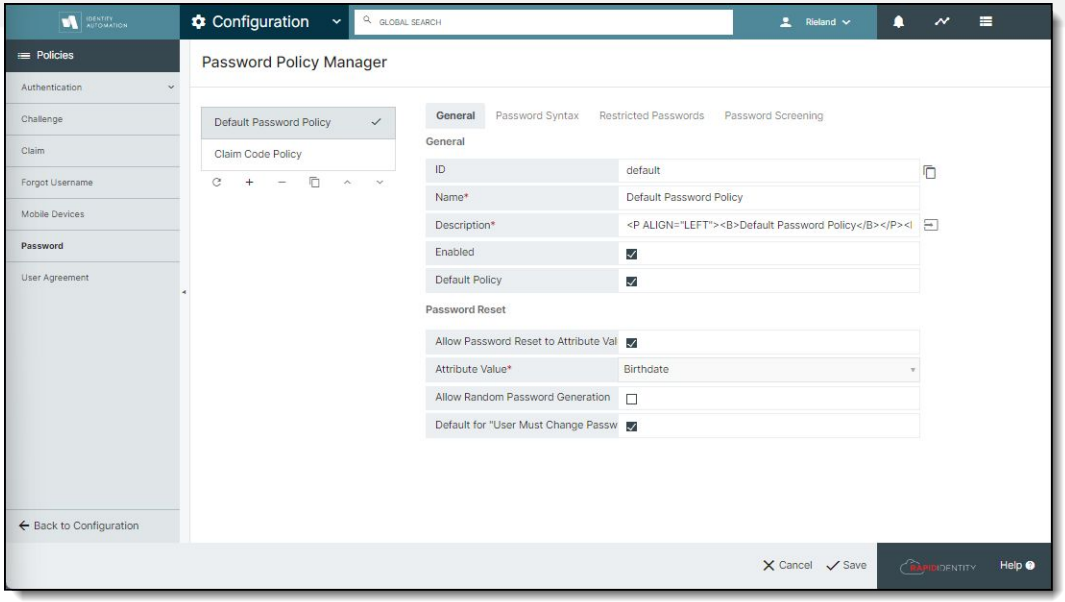
- Policy for logging in to the RapidIdentity Portal
- Depending on your configuration:
  - May sync to AD, Google, O365
  - May have a bi-directional sync if password is changed in AD (not common when RI is used to manage passwords)
- Best practice is to match your AD policy, or be more restrictive
  - If AD requires minimum of 8 characters, RI can require 10, but 6 will cause the sync from RI to AD to fail



CONFIDENTIAL

Configuration Policies - Passwords

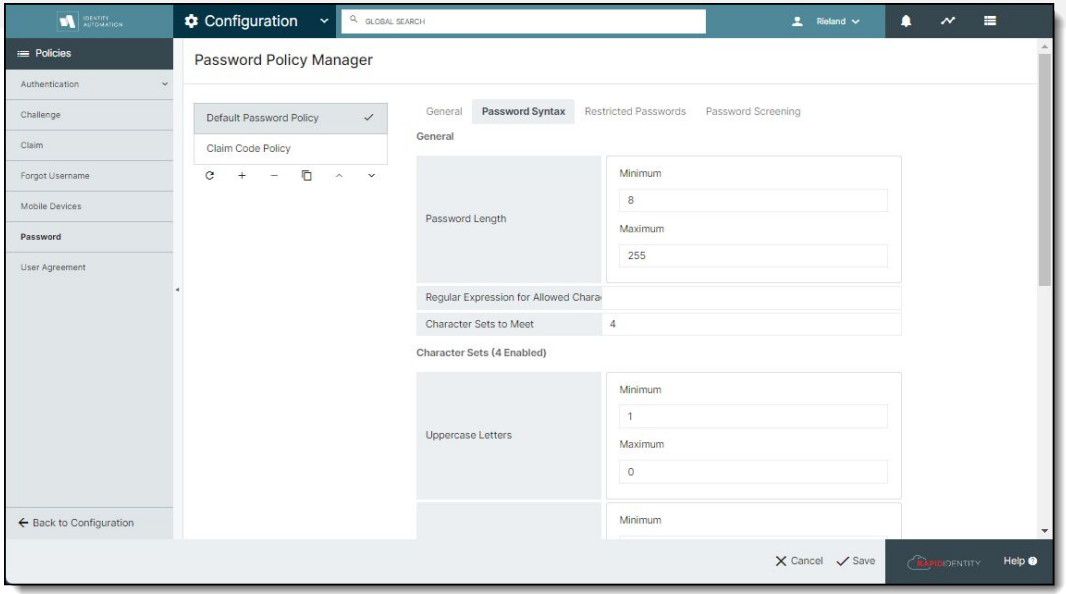
- Current password options:
  - Unique policies for different user groups - staff vs high school vs. kindergarten
  - Apply policy by roles or attributes



CONFIDENTIAL

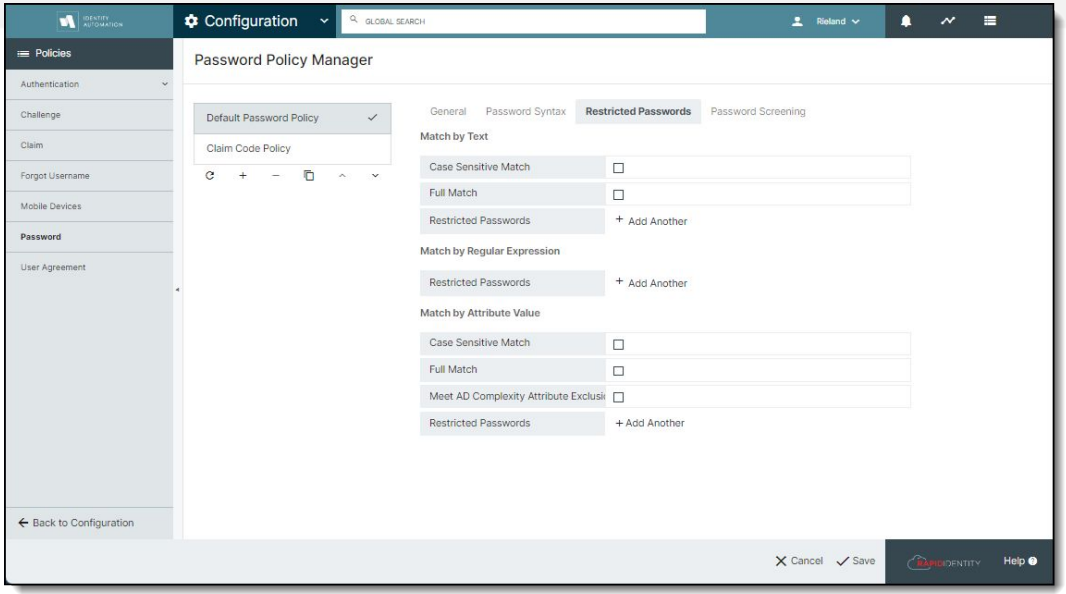
Configuration Policies - Passwords

- Current password options:
  - Min/max length
  - If downstream systems can't use some characters, like asterisk, single or double quote, use the Regular Expression for Allowed Characters
  - Complexity requirements: X out of 5 upper/lower/number/ symbol/unicode character
    - Can specify that more than one of these exist, so 2 uppercase letters



Configuration Policies - Passwords

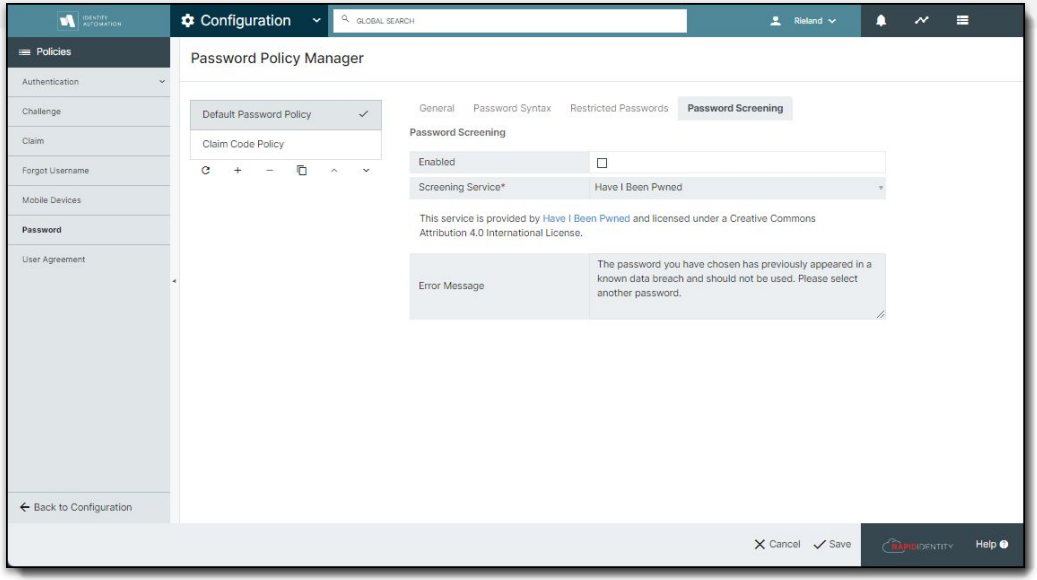
- Current password options:
  - Restricted passwords
    - Similar to restrictions in challenge answers
    - Adds regular expressions



CONFIDENTIAL

Configuration Policies - Passwords

- Feature to screen a newly-created password against the Have I Been Pwned database
  - Word of caution: Before this feature is enabled, consider creating a new help desk default password because your current password may be in this database, especially if it's been in use for many years



CONFIDENTIAL

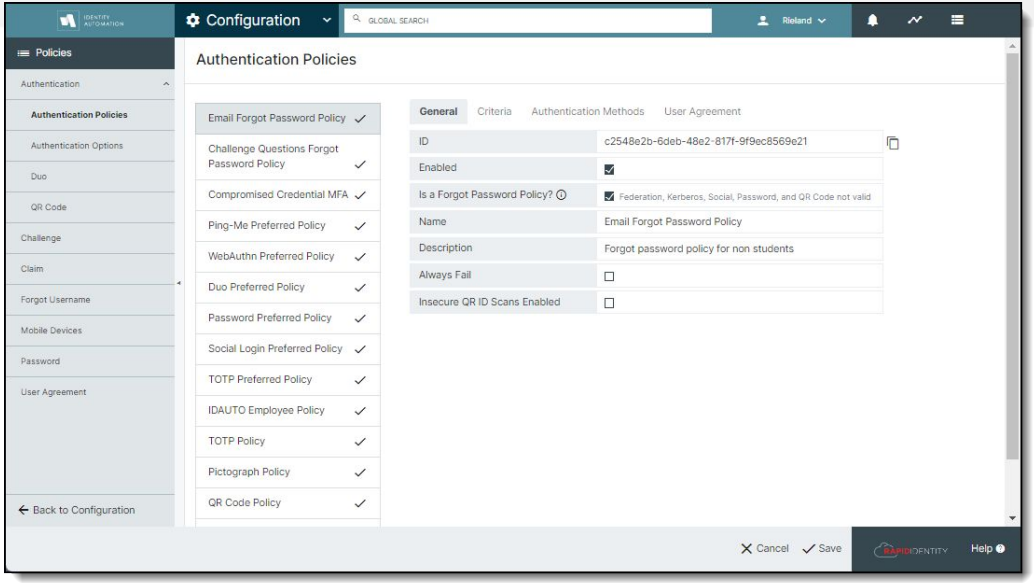
Configuration Policies - Passwords

- Q4 enhancements to password policies includes:
  - Password reuse history
  - Auto lock after x failed attempts
  - Auto unlock after x minutes
  - Password expiration notification will be enabled at the login screen
  - Verify against SafeID that username+password hasn't been compromised

CONFIDENTIAL

Configuration Policies - Authentication Policies (MFA)

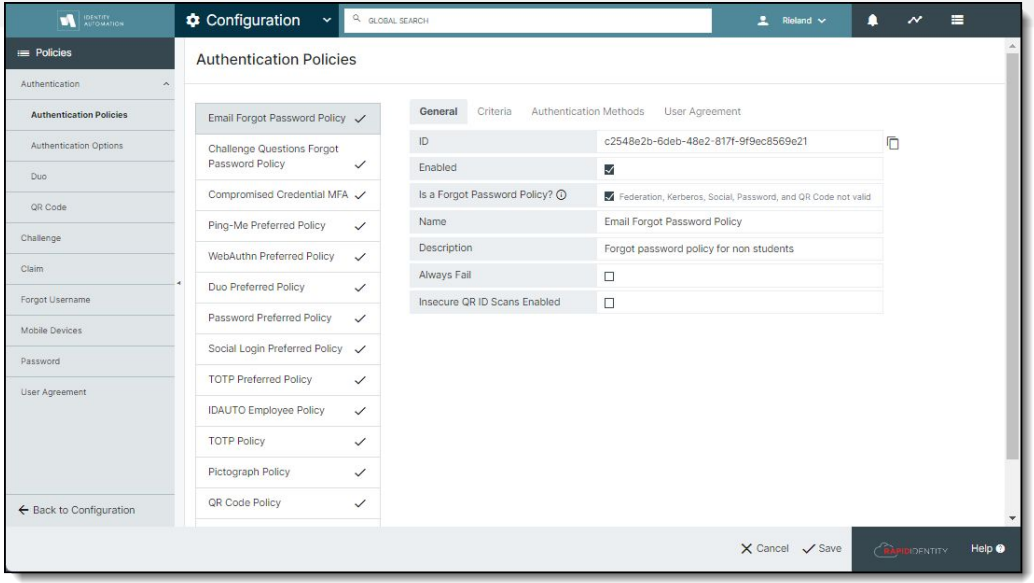
- MFA policies vs. Forgot Password policies
- Primary device-based methods
  - Duo (proprietary app)
  - PingMe (RapidIdentity mobile app)
  - WebAuthN (Windows Hello, Apple Touch ID, FIDO key, etc.)
  - SMS (text message)
  - TOTP (time-based one-time password, generated by authenticator app)



CONFIDENTIAL

Configuration Policies - Authentication Policies (MFA)

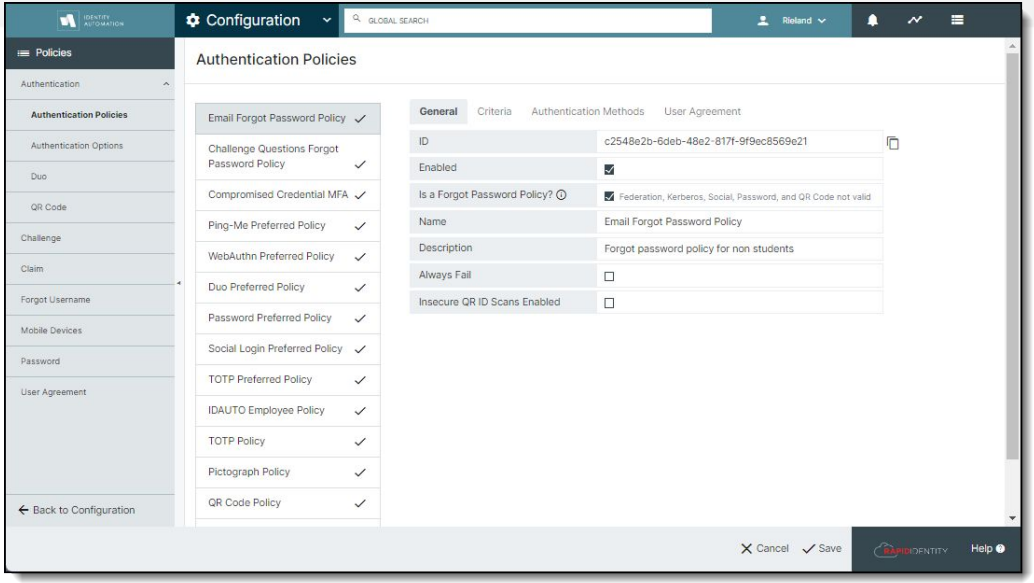
- Secondary methods not dependent on a mobile device
  - Email
  - Password
  - Pictograph
  - Portal Challenge Questions
  - QR Code
  - Social (Google, Facebook, Twitter, LinkedIn)
- Setup a primary method that uses a device, and secondary or backup method in case the user doesn't have access



CONFIDENTIAL

Configuration Policies - Authentication Policies (MFA)

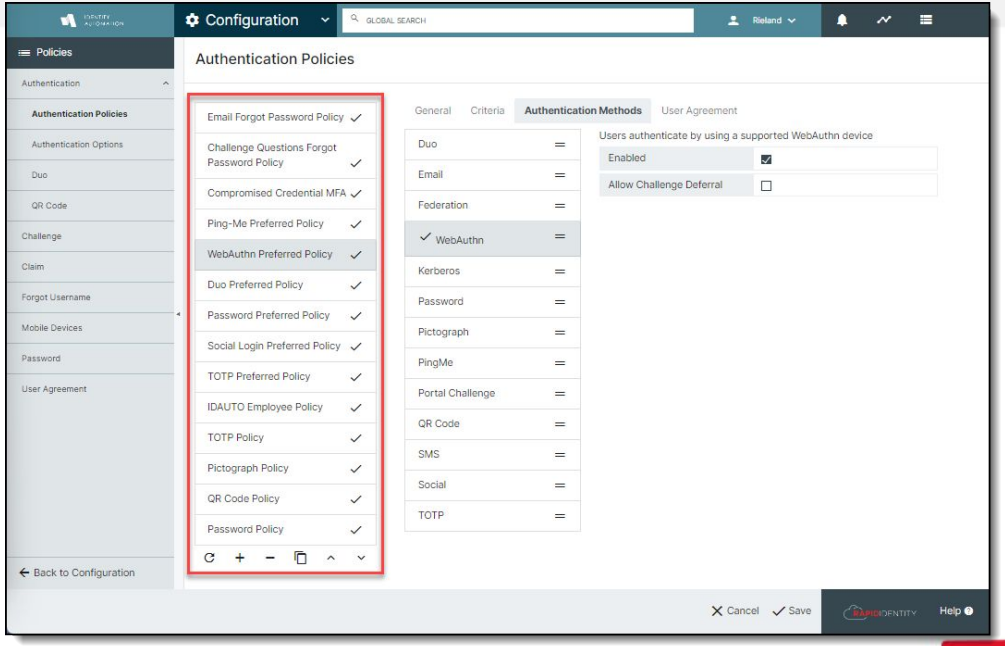
- Forgot Password policies
  - Can receive a code through email or SMS
  - Requires personal email or mobile number stored on employee's profile in advance of the request
  - Enable self-service data entry on the staff MY Delegation If this contact info is not collected and stored in your source system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



CONFIDENTIAL

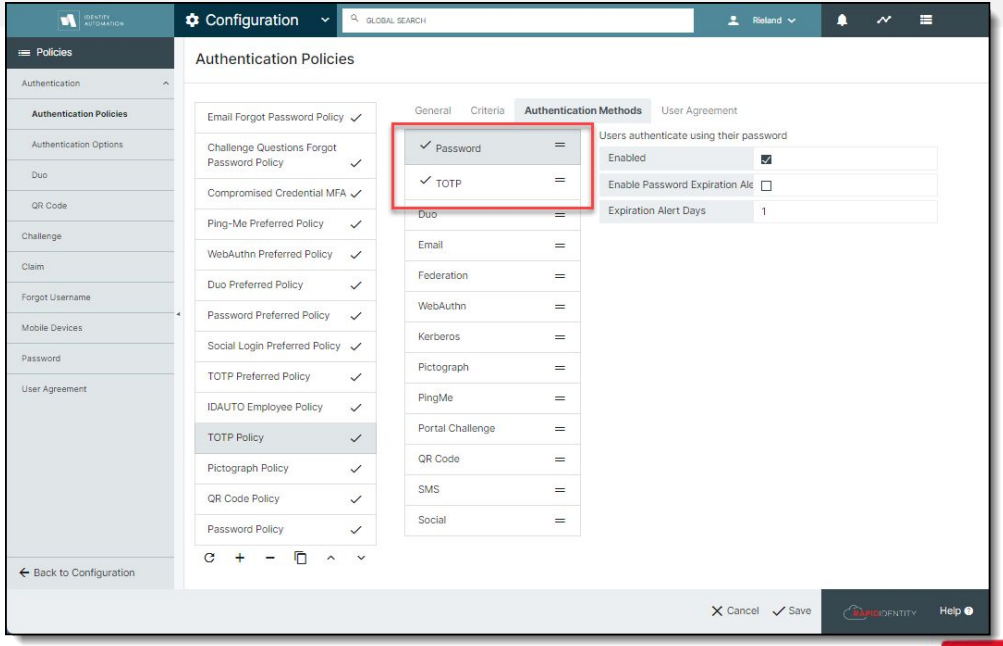
Configuration Policies - Authentication Policies (MFA)

- 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



Configuration Policies - Authentication Policies (MFA)

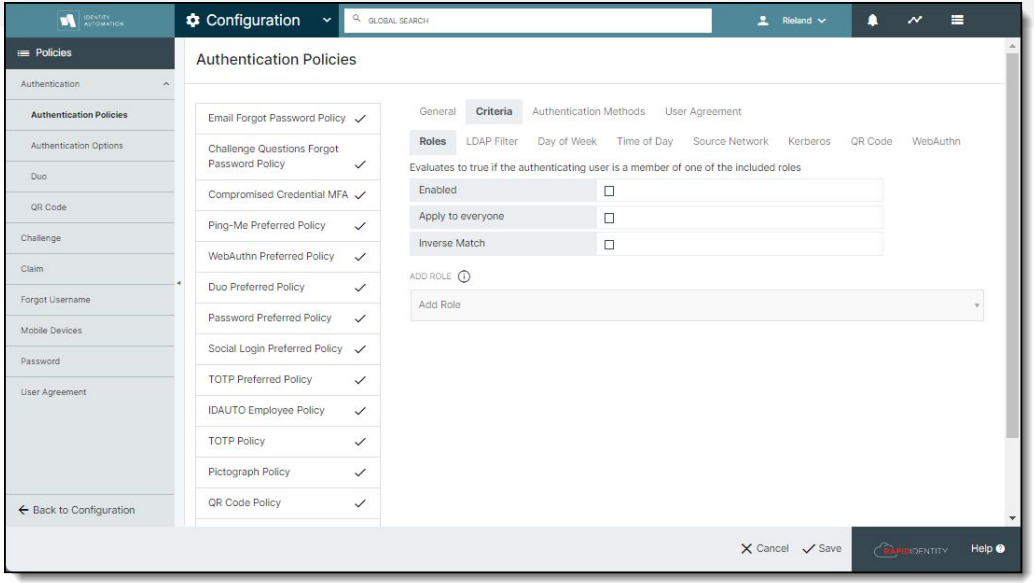
- The order of the policies matters, so if you allow Try Another Method, it will step down to the next policy that matches on that user's attributes, i.e. PingMe first, then TOTP second
- Within each policy, the order of the Authentication Methods you've enabled also matters
  - In this example, the 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



CONFIDENTIAL

Configuration Policies - Authentication Policies (MFA)

- 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

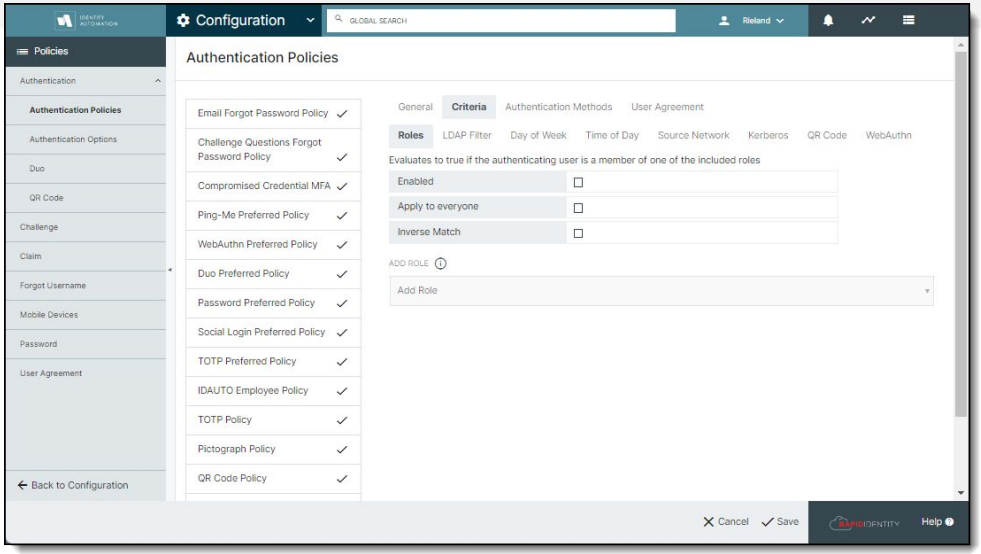


CONFIDENTIAL

Configuration Policies - Authentication Policies (MFA)

MFA 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 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 it's lost or unattended

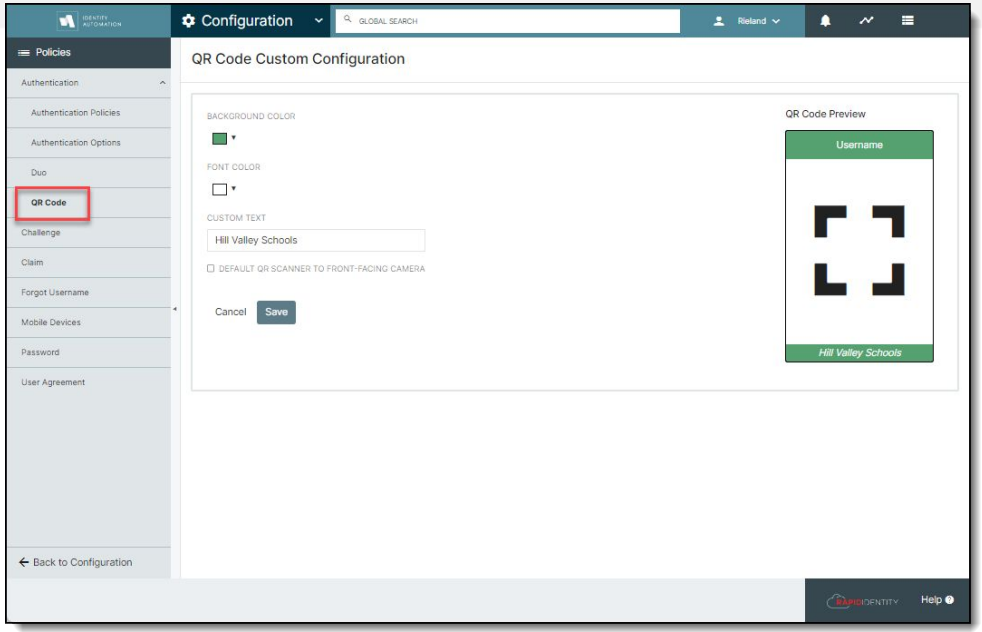


CONFIDENTIAL

Configuration Policies - Authentication Policies (MFA)

MFA 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

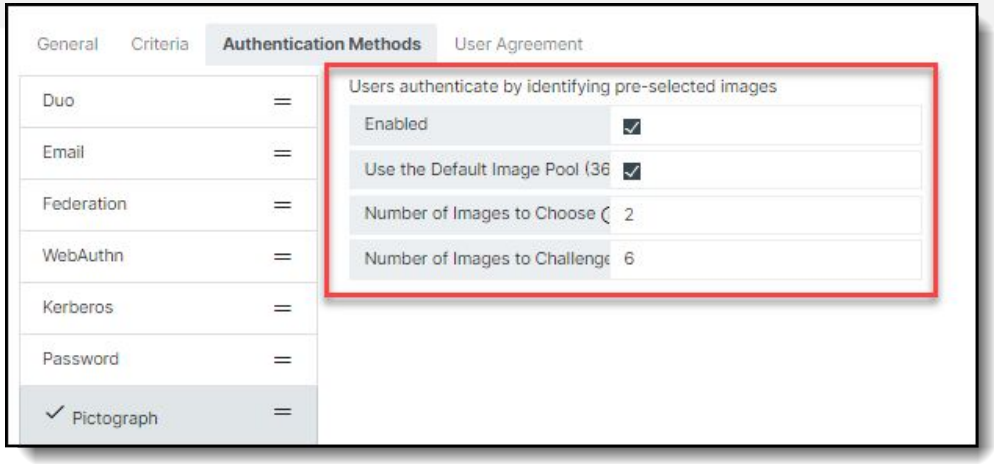


CONFIDENTIAL

Configuration Policies - Authentication Policies (MFA)

MFA 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

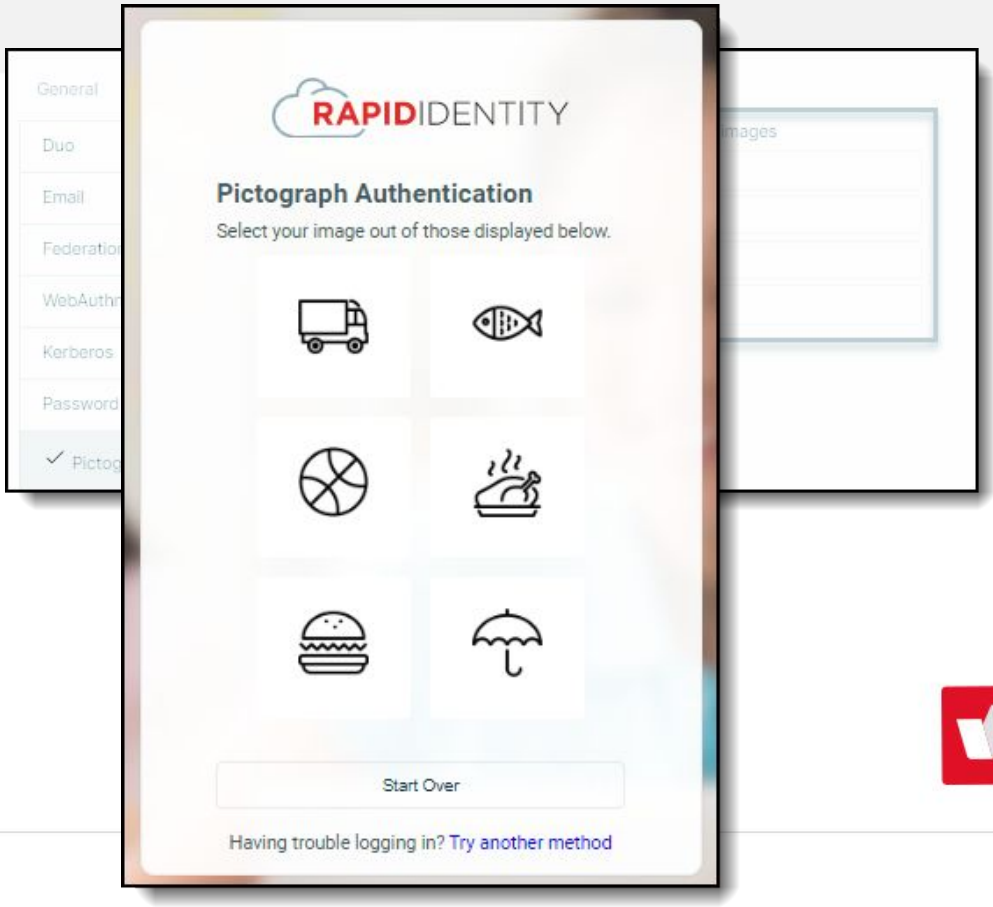


CONFIDENTIAL

Configuration Policies - Authentication Policies (MFA)

MFA methods designed for students

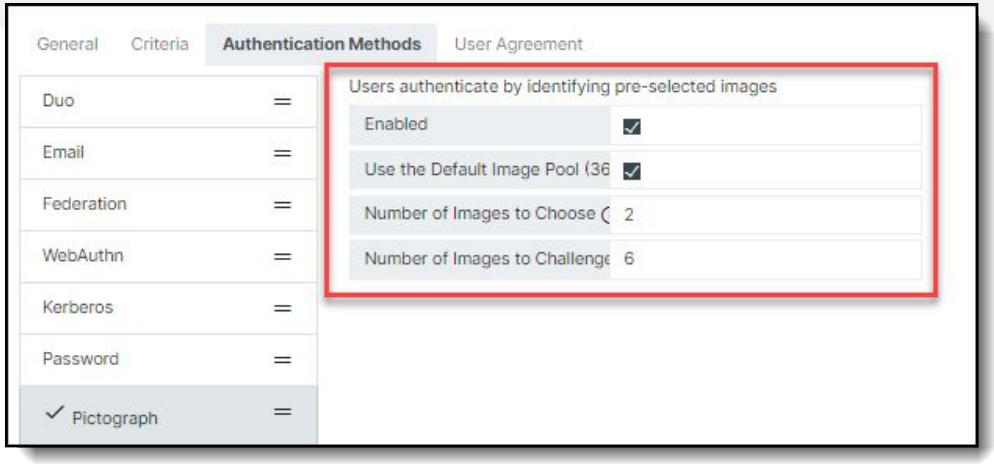
- Pictographs are a series of pictures that students can tap on a touchscreen device, or click with a mouse button
    - Helpful for young students, special education, and students acquiring the English language
- The settings here are Use the Default Image Pool, and there are 36 images to choose from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



Configuration Policies - Authentication Policies (MFA)

MFA 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
  - Uncheck the box, then click the magnifying glass to open the Pictograph image editor to select custom images

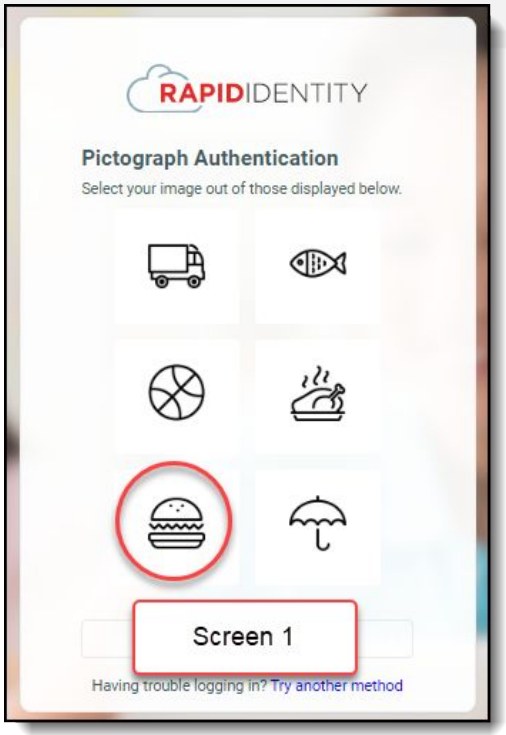


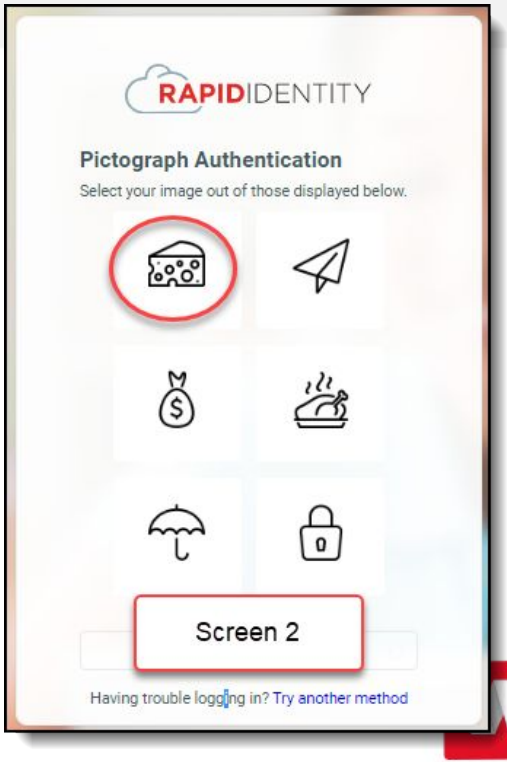
CONFIDENTIAL

Configuration Policies - Authentication Policies (MFA)

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

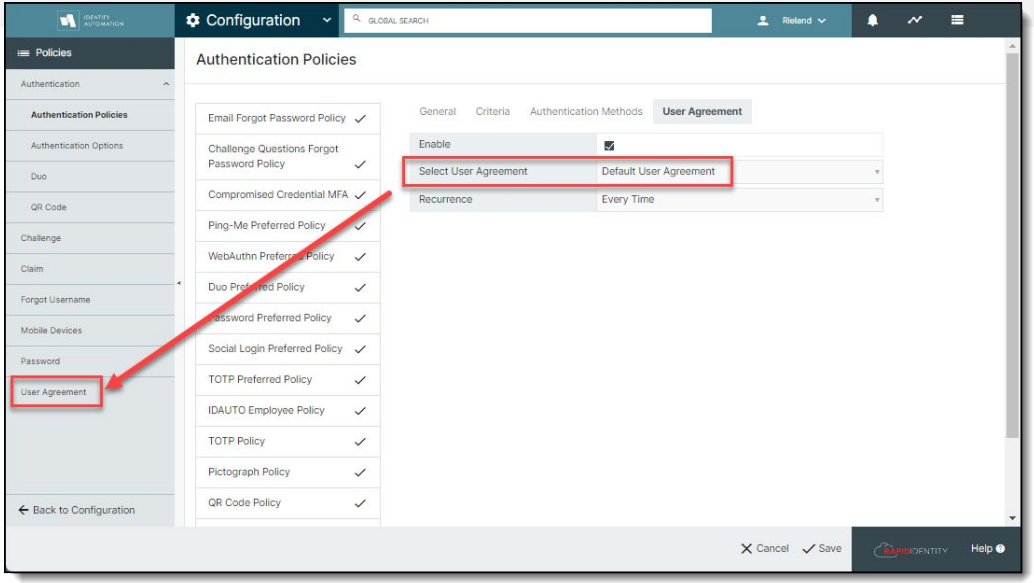




CONFIDENTIAL

Configuration Policies - Authentication Policies (MFA)

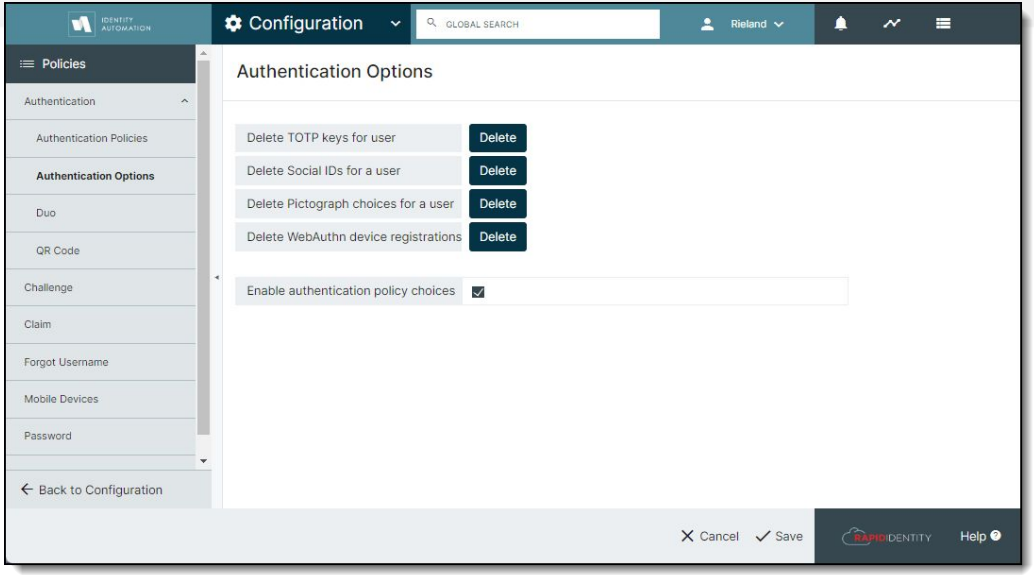
- User Agreement at login page
  - Requirement from cybersecurity insurance agencies
- Can create multiple user agreements because each auth policy can have a different agreement assigned to it
- Show one time, or at every login



CONFIDENTIAL

Configuration Policies - Authentication Options

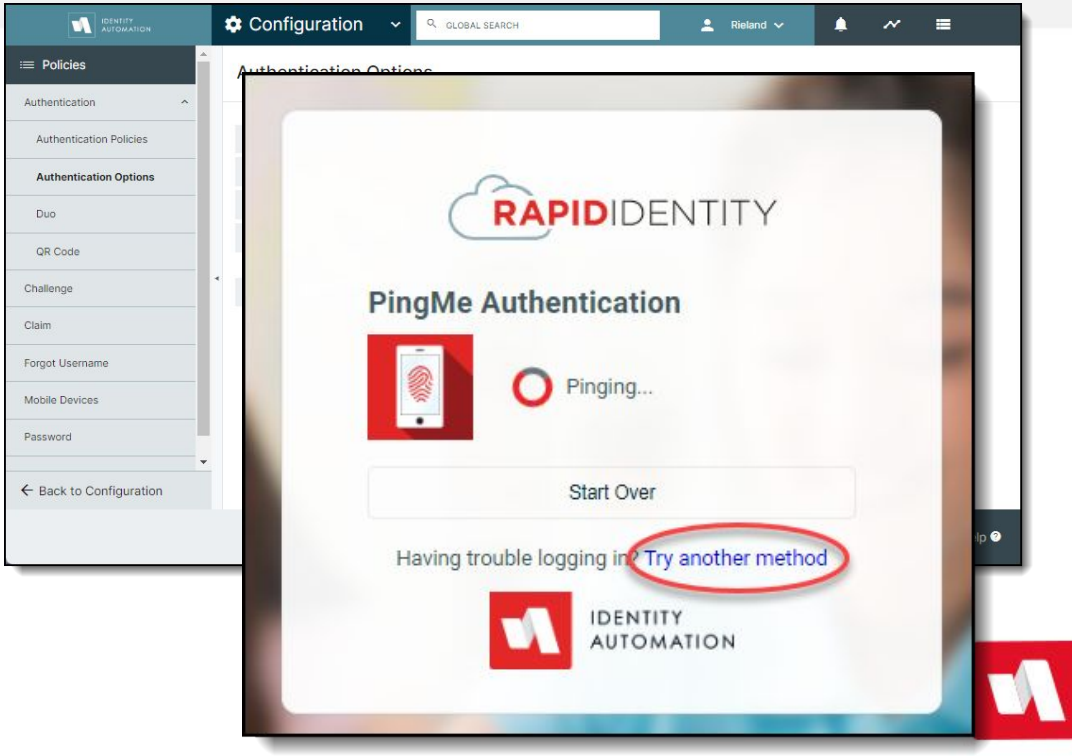
- Delete buttons - does a reset on MFA enrollments
  - Alternate method to actions on a delegation
- Enable authentication policy choices:
  - Enables the “Try Another Method” link on the portal login page



CONFIDENTIAL

Configuration Policies - Authentication Options

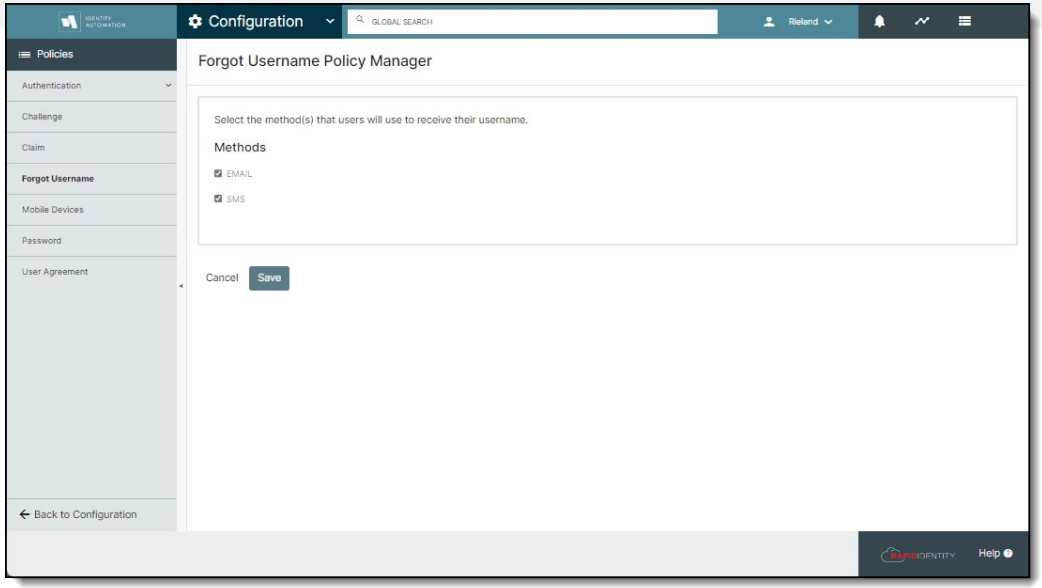
- Delete buttons - does a reset on MFA enrollments
  - Alternate method to actions on a delegation
- Enable authentication policy choices:
  - Enables the “Try Another Method” link on the portal login page
  - When this is enabled, multiple authentication policies must also exist and apply to the user’s account



CONFIDENTIAL

Configuration Policies - Forgot Username

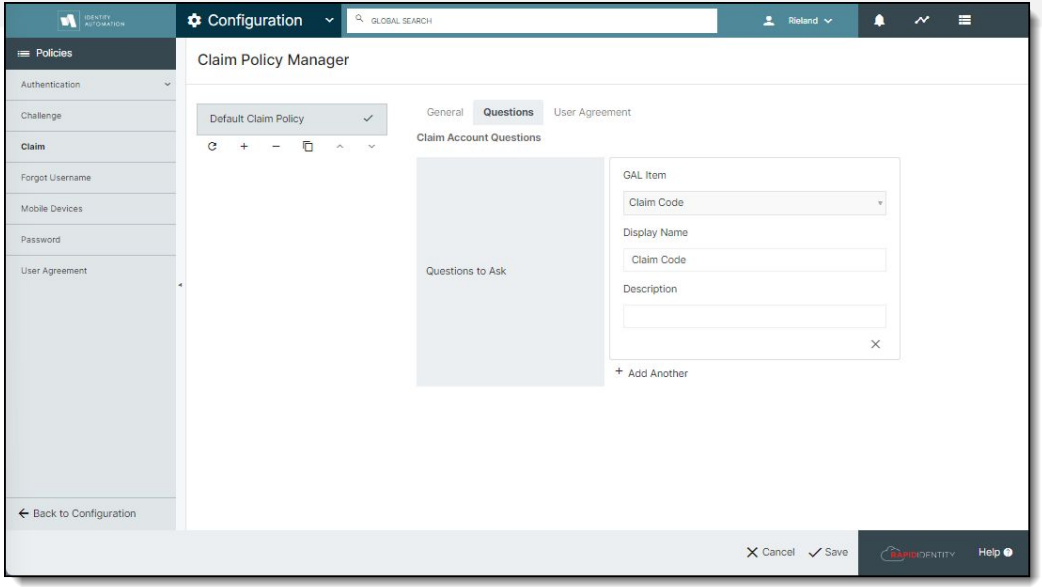
- Simple config: Enable options to receive username by Email and/or SMS
- Requires personal email or mobile number stored on employee's profile in advance of the request



CONFIDENTIAL

Configuration Policies - Claim Account

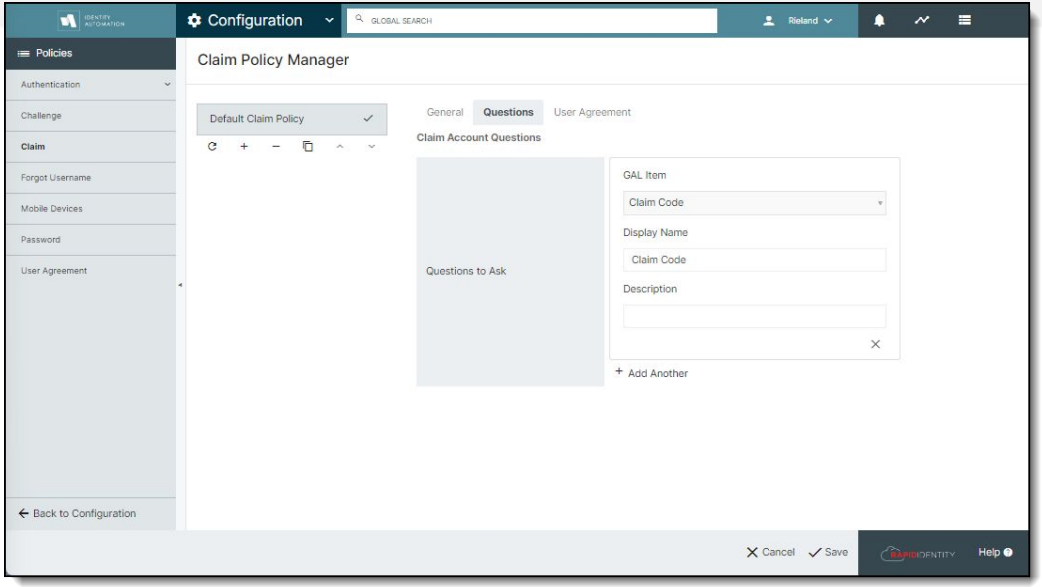
- All of the configurations for Challenge Questions, Password, MFA, and profile update requirements (personal email, mobile number) combine into a claim account policy for new employees
- Employee is contacted with instructions to login to the district's portal (via personal email, usually) and enter a claim code generated for them when their account is created



CONFIDENTIAL

Configuration Policies - Claim Account

- Claim process can:
  - Display the username generated for them by account provisioning
  - Prompt user to set a new password
  - Answer challenge questions
  - Enroll in every MFA method that applies to their account
  - Enter mobile number and personal email if attributes are marked as required on their profile



CONFIDENTIAL

Configuration Policies - Final suggestion

Use the Sponsorship function to create one or more test accounts with a unique employee type, like mfatest.

Use this unique employee type to apply each of the policies to this account.

Use the test account to login to your portal in an incognito browser to test the effects of each of these policies.

Keep testing until everything looks and works according to your plan!

CONFIDENTIAL

Thank you for joining us today!