



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



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



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

People Settings

INVALID CHALLENGE SET MESSAGE *

Your Challenge Questions are not up to date. Please contact the Help Desk at x1122 or help@district.org.

ENABLE CHALLENGE QUESTIONS

ENABLE FORGOTTEN PASSWORD RETRIEVAL

ENABLE FORGOTTEN PASSWORD CAPTCHA

ENABLE FORGOTTEN USERNAME RETRIEVAL

ENABLE FORGOTTEN USERNAME CAPTCHA

ENABLE CLAIM ACCOUNT CAPTCHA

ENABLE WILDCARD (*) SEARCHES

ACCESS CONTROL *

Role-based

INCLUDED ROLES *

Portal Administrator

Hillside High School Teachers

⊕ Add Another Included Role

Cancel Save

Settings

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

IDENTIFY AUTOMATION

Filter

Staff

Students

Teachers

Guardians

My Team Profiles

Delegations

People Settings

Profile Templates

Sponsorship Attributes

Sponsorship Settings

Sponsorship Templates

Settings

People Settings

INVALID CHALLENGE SET MESSAGE *

Your Challenge Questions are not up to date. Please contact the Help Desk at x1122 or help@district.org.

ENABLE CHALLENGE QUESTIONS

ENABLE FORGOTTEN PASSWORD RETRIEVAL

ENABLE FORGOTTEN PASSWORD CAPTCHA

ENABLE FORGOTTEN USERNAME RETRIEVAL

ENABLE FORGOTTEN USERNAME CAPTCHA

ENABLE CLAIM ACCOUNT CAPTCHA

ENABLE WILDCARD (*) SEARCHES

ACCESS CONTROL *

Role-based

INCLUDED ROLES *

Portal Administrator

Hillside High School Teachers

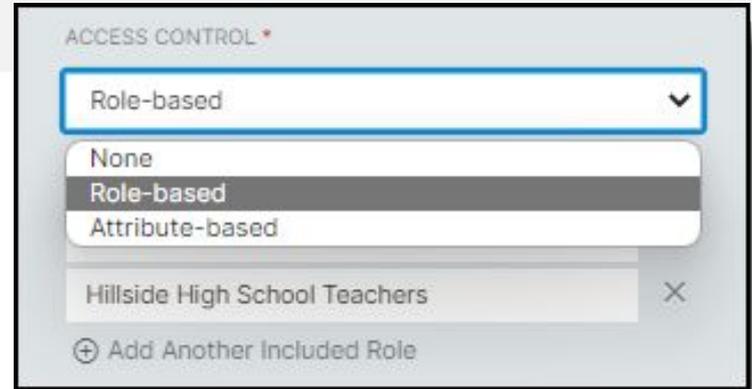
⊕ Add Another Included Role

Cancel

Save

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

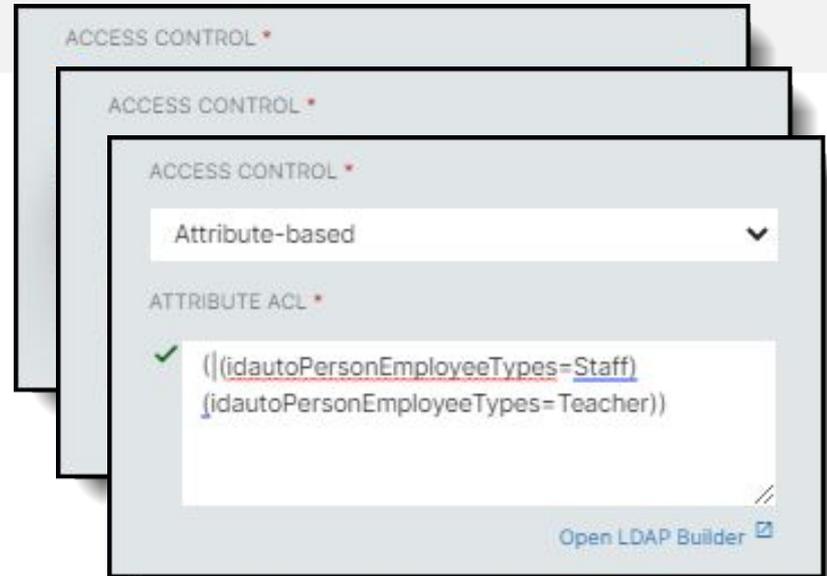
- **Access Control:** Who can see People on the drop-down menu
 - **None** - Everyone with access to login to RapidIdentity can see People.
 - Doesn't automatically grant access to view all delegations.
 - Each delegation has its own granular access control.
- **Role-based** - If Role-based is selected, 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**

The screenshot displays the 'ACCESS CONTROL' settings. The 'ACCESS CONTROL' dropdown is set to 'Role-based'. Below it, the 'INCLUDED ROLES' section shows a list of selected roles: 'Portal Administrator' and 'All Staff'. Each role has a close button (X) to its right. At the bottom of the list, there is a button with a plus sign and the text '+ 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



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

The screenshot shows the 'Challenge Policy Manager' configuration page in a web application. The interface is divided into a left sidebar and a main content area. The sidebar contains a 'Policies' menu with options for Authentication, Challenge, Claim, Forgot Username, Mobile Devices, Password, and User Agreement. The main content area is titled 'Challenge Policy Manager' and features a 'Default Challenge Policy' dropdown menu with three options: 'Default Challenge Policy', 'Staff Challenge Policy', and 'No Challenge Policy for Students'. Below this is a 'General' tab with various settings: ID (e1688806-c78-4ef6-971b-1f3456366498), Name* (Staff Challenge Policy), Description, Enabled (checked), Default Policy (unchecked), and No Challenge Policy (unchecked). The 'Affected Users' section includes 'Access Control' (Role-based), 'Included Roles*' (All Employees), and checkboxes for 'Allow Users to Skip Setup' and 'Allow Users to Create Questions'. At the bottom right, there are 'Cancel' and 'Save' buttons, along with the 'Okta Identity' logo and a 'Help' link.



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

The screenshot displays the 'Challenge Policy Manager' interface. On the left, a sidebar lists various policy categories: Authentication, Challenge, Claim, Forgot Username, Mobile Devices, Password, and User Agreement. The 'Challenge' category is selected. The main area shows a list of policies: 'Default Challenge Policy', 'Staff Challenge Policy', and 'No Challenge Policy for Students'. The 'Staff Challenge Policy' is selected. The configuration form for this policy is shown, with tabs for 'General', 'Questions', and 'Restricted Answers'. The 'General' tab is active, showing fields for ID, Name, Description, Enabled, Default Policy, and No Challenge Policy. The 'Description' field is highlighted with a red box. Below this, the 'Affected Users' section shows 'Access Control' set to 'Role-based', 'Included Roles' set to 'All Employees', and checkboxes for 'Allow Users to Skip Setup' and 'Allow Users to Create Questions'. At the bottom right, there are 'Cancel' and 'Save' buttons, along with the 'IDENTITY' logo and a 'Help' icon.



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”

The screenshot shows the 'Challenge Policy Manager' configuration page. On the left is a 'Policies' sidebar with options like Authentication, Challenge, Claim, Forgot Username, Mobile Devices, Password, and User Agreement. The main area is titled 'Challenge Policy Manager' and has tabs for 'General', 'Questions', and 'Restricted Answers'. Under the 'Questions' tab, there are two sections: 'General' and 'Challenge Questions'. The 'General' section has two input fields: 'Questions to Ask at Setup' (value: 5) and 'Questions to Ask at Login' (value: 2). The 'Challenge Questions' section shows a list of questions, with two examples visible: 'What color is the sky?' and 'What's your favorite meal?'. Each question has a 'Required' checkbox, which is currently unchecked. At the bottom right, there are 'Cancel' and 'Save' buttons, along with a 'Help' icon.



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

The screenshot shows the 'Challenge Policy Manager' configuration page. The left sidebar lists various policy categories: Authentication, Challenge, Claim, Forgot Username, Mobile Devices, Password, and User Agreement. The main content area is titled 'Challenge Policy Manager' and has tabs for 'General', 'Questions', and 'Restricted Answers'. The 'Restricted Answers' tab is active, showing a 'General' section with the following settings: 'Restrict Words that Appear in Questions' (checked), 'Answers Must Be Unique' (checked), and 'Answers Must Be Given After' (11/04/2022). Below this is a 'Match by Text' section with a 'Full Match' checkbox (unchecked) and a list of 'Restricted Answers' containing 'ABC Elementary', 'DEF Middle School', and 'Timberwolves'. At the bottom right, there are 'Cancel', 'Save', and 'Help' buttons.



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

The screenshot displays the 'Password Policy Manager' configuration page. The left sidebar shows a 'Policies' menu with options like Authentication, Challenge, Claim, Forged Username, Mobile Devices, Password, and User Agreement. The main area is titled 'Password Policy Manager' and has tabs for 'General', 'Password Syntax', 'Restricted Passwords', and 'Password Screening'. The 'General' tab is active, showing fields for ID (default), Name (Default Password Policy), Description (HTML-formatted), Enabled (checked), and Default Policy (checked). Under the 'Password Reset' section, there are options for 'Allow Password Reset to Attribute Value' (checked), 'Attribute Value' (Birthdate), 'Allow Random Password Generation' (unchecked), and 'Default for "User Must Change Passw' (checked). The bottom right corner features 'Cancel', 'Save', and 'Help' buttons.



Configuration Policies - Passwords

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

The screenshot shows the 'Password Policy Manager' configuration page. The interface includes a sidebar with navigation options like 'Authentication', 'Challenge', 'Claim', 'Forgot Username', 'Mobile Devices', 'Password', and 'User Agreement'. The main content area is titled 'Password Policy Manager' and features a 'Default Password Policy' dropdown menu. Below this, there are tabs for 'General', 'Password Syntax', 'Restricted Passwords', and 'Password Screening'. The 'General' tab is active, displaying fields for 'ID' (default), 'Name*' (Default Password Policy), 'Description*' (HTML-formatted text), 'Enabled' (checked), and 'Default Policy' (checked). Under the 'Password Reset' section, there are fields for 'Allow Password Reset to Attribute Val' (checked), 'Attribute Value*' (Birthdate), 'Allow Random Password Generation' (unchecked), and 'Default for "User Must Change Passw' (checked). The bottom of the interface has 'Cancel' and 'Save' buttons, along with the 'ASPIRE IDENTITY' logo and a 'Help' icon.



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

The screenshot shows the 'Password Policy Manager' configuration page. The left sidebar lists various policy categories: Authentication, Challenge, Claim, Forgot Username, Mobile Devices, Password, and User Agreement. The main content area is titled 'Password Policy Manager' and has tabs for 'General', 'Password Syntax', 'Restricted Passwords', and 'Password Screening'. The 'Password Syntax' tab is active. Under the 'General' section, there are several configuration fields: 'Password Length' with 'Minimum' (8) and 'Maximum' (255) input boxes; 'Regular Expression for Allowed Characters' (empty); 'Character Sets to Meet' (4); and 'Character Sets (4 Enabled)' with 'Uppercase Letters' having 'Minimum' (1) and 'Maximum' (0) input boxes. At the bottom right, there are 'Cancel' and 'Save' buttons, and a 'Help' icon.



Configuration Policies - Passwords

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

The screenshot displays the 'Password Policy Manager' configuration page. The interface includes a top navigation bar with 'Configuration' and a search bar. A left sidebar lists various policy categories: Authentication, Challenge, Claim, Forgot Username, Mobile Devices, Password, and User Agreement. The main content area is titled 'Password Policy Manager' and features tabs for 'General', 'Password Syntax', 'Restricted Passwords', and 'Password Screening'. The 'Restricted Passwords' tab is active, showing three sections: 'Match by Text', 'Match by Regular Expression', and 'Match by Attribute Value'. Each section contains a 'Restricted Passwords' field with a '+ Add Another' button. The 'Match by Text' section also includes 'Case Sensitive Match' and 'Full Match' checkboxes. The 'Match by Regular Expression' and 'Match by Attribute Value' sections include 'Full Match' and 'Meet AD Complexity Attribute Exclusion' checkboxes. At the bottom right, there are 'Cancel' and 'Save' buttons, along with the 'Microsoft Identity' logo and a 'Help' icon.



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

The screenshot shows the 'Password Policy Manager' configuration page. The left sidebar lists various policy categories: Authentication, Challenge, Claim, Forgot Username, Mobile Devices, Password, and User Agreement. The main content area is titled 'Password Policy Manager' and includes a search bar and tabs for 'General', 'Password Syntax', 'Restricted Passwords', and 'Password Screening'. The 'Password Screening' tab is active, showing a form with an 'Enabled' checkbox (unchecked) and a 'Screening Service*' dropdown menu set to 'Have I Been Pwned'. Below this, there is a disclaimer: 'This service is provided by Have I Been Pwned and licensed under a Creative Commons Attribution 4.0 International License.' An 'Error Message' field contains the text: 'The password you have chosen has previously appeared in a known data breach and should not be used. Please select another password.' The bottom of the interface features 'Cancel' and 'Save' buttons, along with the 'Redpoint' logo and a 'Help' link.



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



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)

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"/>



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

The screenshot displays the 'Authentication Policies' configuration page in the Identity Automation console. The left sidebar shows a navigation menu with 'Policies' expanded, listing categories like Authentication, Authentication Options, Duo, QR Code, Challenge, Claim, Forgot Username, Mobile Devices, Password, and User Agreement. The main content area shows a list of policies, with 'Email Forgot Password Policy' selected. The configuration for this policy is shown in the 'General' tab, including fields for ID, Enabled status, Name, Description, and Always Fail.

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	✓

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 (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

The screenshot displays the 'Authentication Policies' configuration page in the RapidIdentity console. The left sidebar shows a navigation menu with 'Policies' expanded to 'Authentication Policies'. The main content area shows the configuration for the 'Email Forgot Password Policy'. The 'General' tab is active, showing the following details:

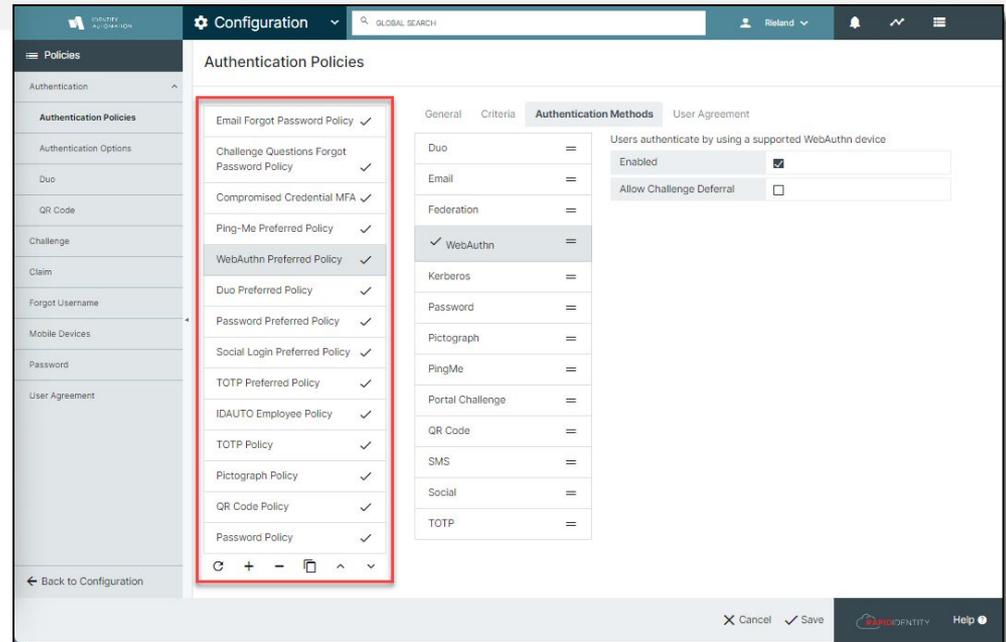
Field	Value
ID	c2548e2b-6deb-48e2-817f-9f9ec8569e21
Enabled	<input checked="" type="checkbox"/>
Is a Forgot Password Policy?	<input checked="" type="checkbox"/> Federation, Kerberos, Social, Password, and QR Code not valid
Name	Email Forgot Password Policy
Description	Forgot password policy for non students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

At the bottom of the configuration page, 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 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: Authentication, Authentication Policies (selected), Authentication Options, Duo, QR Code, Challenge, Claim, Forgot Username, Mobile Devices, Password, and User Agreement. The 'Authentication Policies' list contains 16 items, with 'WebAuthn Preferred Policy' highlighted in a red box. Below the list are controls for adding (+), removing (-), and reordering (up/down arrows) policies. The right-hand pane shows the configuration for the selected policy, with the 'Authentication Methods' tab active. It lists various authentication methods with reorder arrows, and 'WebAuthn' is currently selected. A 'User Agreement' section is also visible, with 'Enabled' checked and 'Allow Challenge Deferral' 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 enabled, with 'Enable Password Expiration Alert' and 'Expiration Alert Days' (set to 1) also visible. The bottom of the console shows 'Cancel' and 'Save' buttons.



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

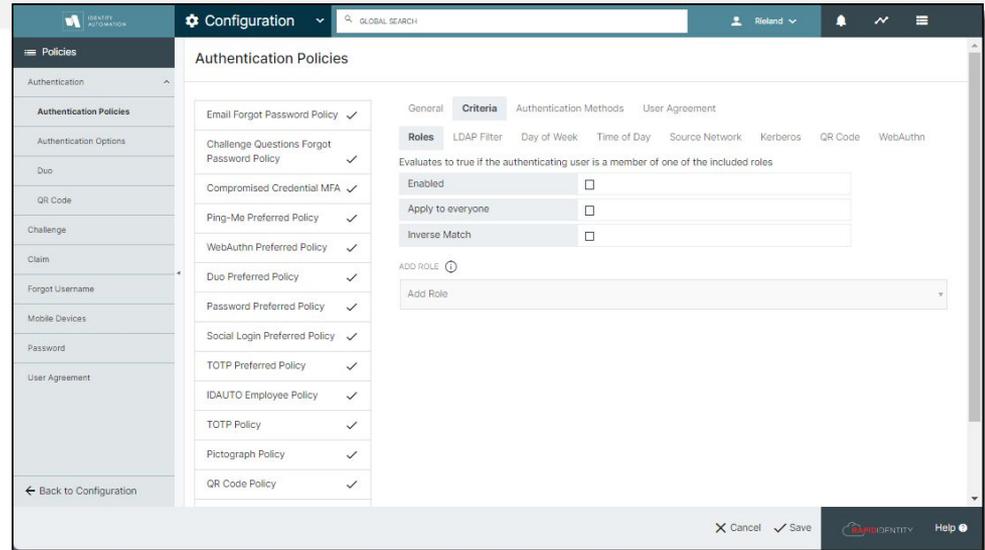
The screenshot displays the 'Authentication Policies' configuration page in the Identity Automation console. The left sidebar shows a navigation menu with 'Authentication Policies' selected. The main content area is titled 'Authentication Policies' and features a list of 14 policies, each with a checkmark 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 description: 'Evaluates to true if the authenticating user is a member of one of the included roles'. Below this, there are three checkboxes: 'Enabled' (checked), 'Apply to everyone' (unchecked), and 'Inverse Match' (unchecked). An 'ADD ROLE' button is visible, followed by a dropdown menu labeled 'Add Role'. At the bottom right, there are 'Cancel' and 'Save' buttons, along with the 'IDENTITY' logo and a 'Help' icon.



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



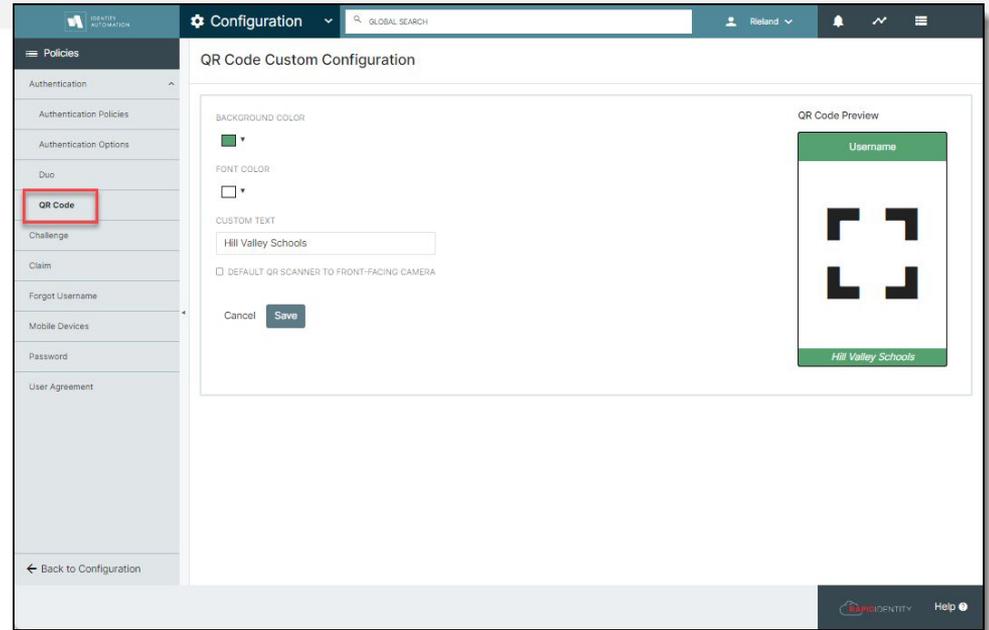
The screenshot displays the Microsoft Identity Automation Configuration console. The left sidebar shows a navigation menu with 'Policies' expanded, listing various authentication methods like Duo, QR Code, and Password. The main area is titled 'Authentication Policies' and shows a list of 14 policies, each with a checkmark indicating it is enabled. The 'Criteria' tab is selected, showing configuration options for roles, LDAP filters, and time-based conditions. The 'Roles' section includes checkboxes for 'Enabled', 'Apply to everyone', and 'Inverse Match'. An 'ADD ROLE' section is visible at the bottom of the criteria configuration area.



Configuration Policies - Authentication Policies (MFA)

MFA methods designed for students

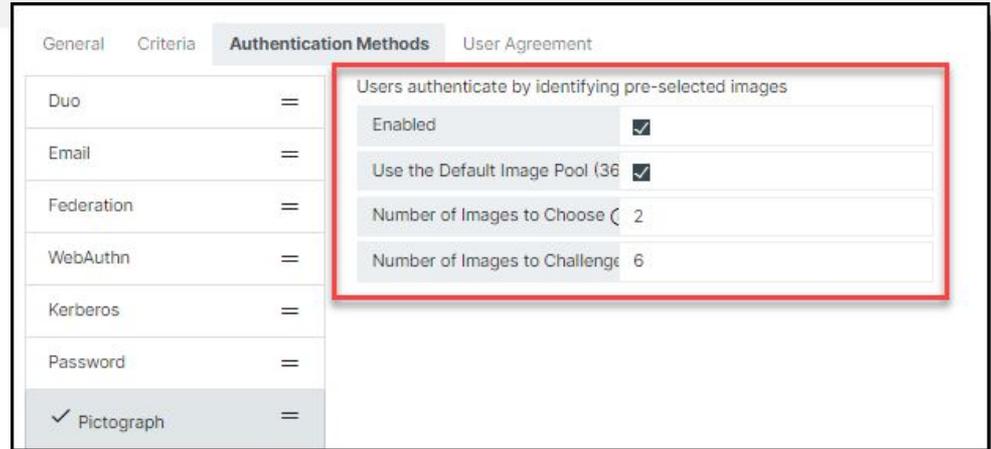
- QR Codes - secure vs. insecure does not refer to the embedded content in the code; it refers to the protection requirements
 - Secure: embedded username and password and must be stored or kept in a secure location or under a person's control at all times
 - Insecure: embedded username, and a password 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



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



General	Criteria	Authentication Methods	User Agreement
Duo	=		
Email	=		
Federation	=		
WebAuthn	=		
Kerberos	=		
Password	=		
✓ Pictograph	=		

Users authenticate by identifying pre-selected images

Enabled

Use the Default Image Pool (36)

Number of Images to Choose

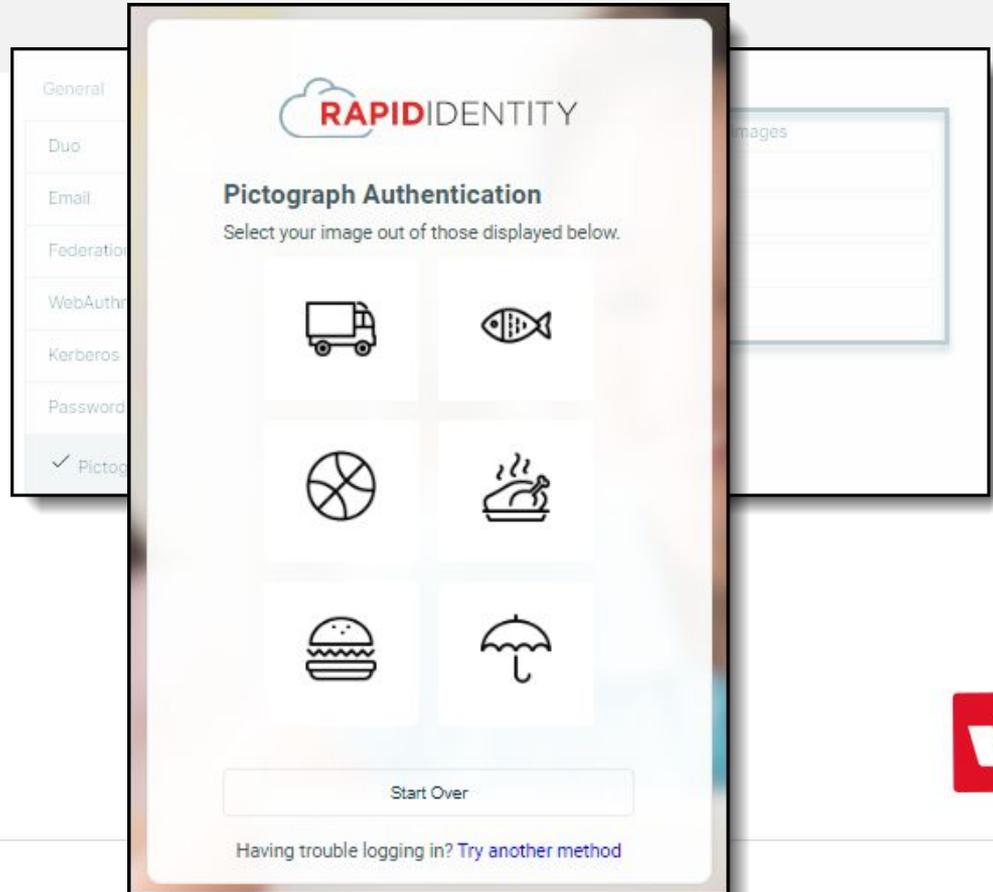
Number of Images to Challenge



Configuration Policies - Authentication Policies (MFA)

MFA methods designed for students

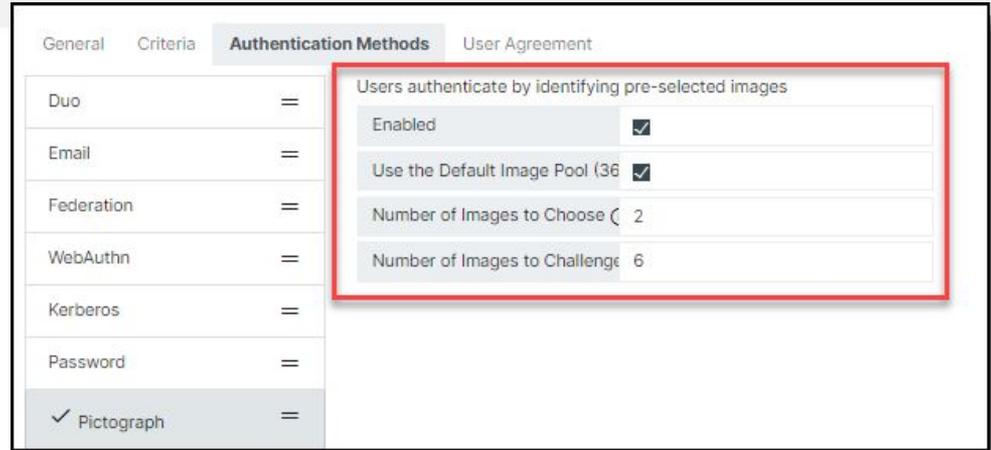
- Pictographs are a series of pictures that students can tap on a touchscreen device, or click with a mouse button
 - Helpful for young students, special education, and students acquiring the English language
- The settings here are Use the Default Image Pool, and there are 36 images to choose from
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



General	Criteria	Authentication Methods	User Agreement
Duo	=		
Email	=		
Federation	=		
WebAuthn	=		
Kerberos	=		
Password	=		
✓ Pictograph	=		

Users authenticate by identifying pre-selected images

Enabled

Use the Default Image Pool (36)

Number of Images to Choose

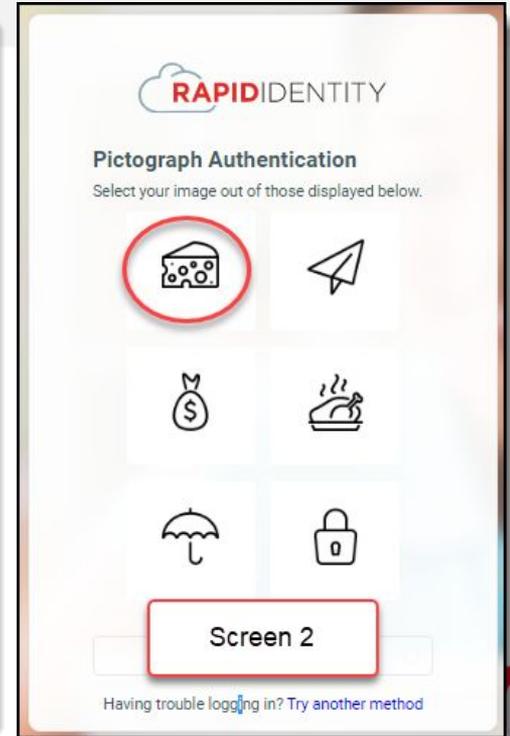
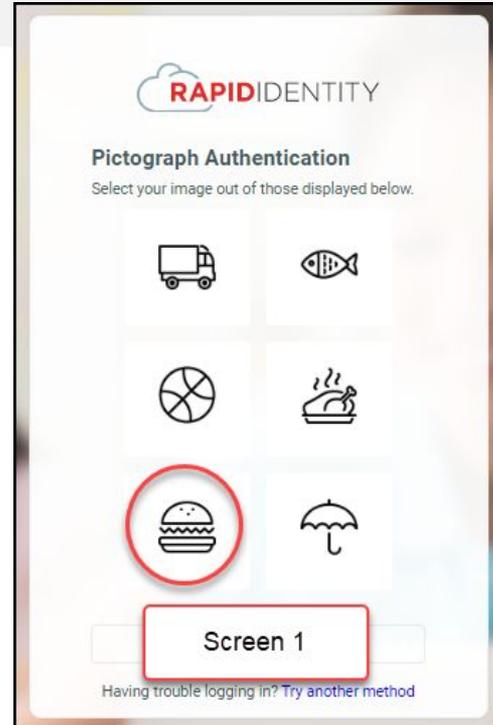
Number of Images to Challenge



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



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

The screenshot displays the 'Authentication Policies' configuration page in the Identity Automation console. The left-hand navigation menu has 'User Agreement' highlighted with a red box. The main content area shows a list of authentication policies, each with a checkmark. The 'User Agreement' tab is selected, and the 'Select User Agreement' dropdown is highlighted with a red box. A red arrow points from this dropdown to the 'User Agreement' option in the left-hand navigation menu.

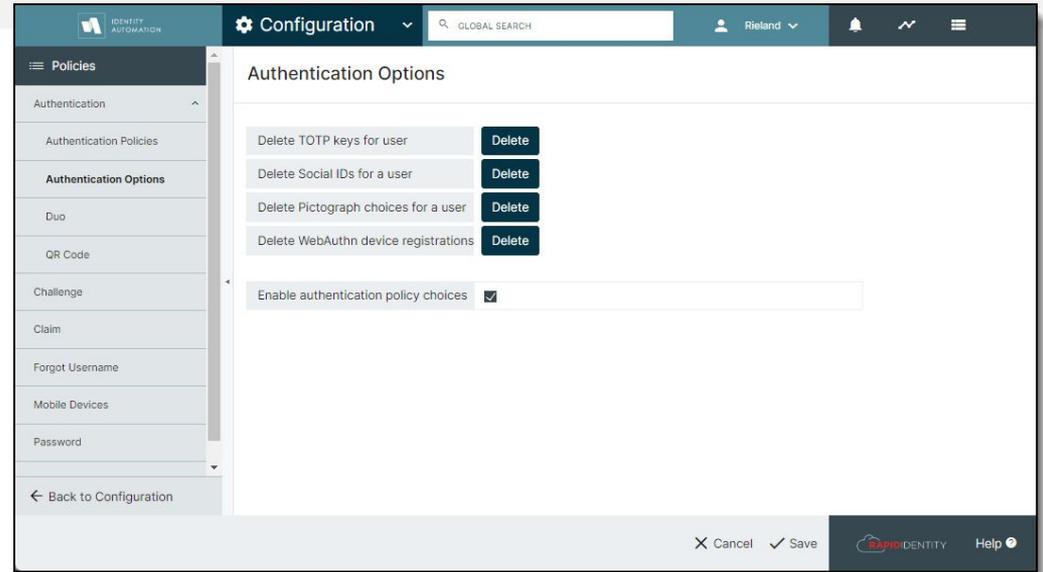
Policy Name	Status
Email Forgot Password Policy	✓
Challenge Questions Forgot Password Policy	✓
Compromised Credential MFA	✓
Ping-Me Preferred Policy	✓
WebAuthn Preferred Policy	✓
Duo Preferred Policy	✓
Password Preferred Policy	✓
Social Login Preferred Policy	✓
TOTP Preferred Policy	✓
IDAUTO Employee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

Configuration console details: 'Authentication Policies' page, 'User Agreement' tab selected. 'Select User Agreement' dropdown is highlighted with a red box. 'User Agreement' option in the left-hand navigation menu is also highlighted with a red box. A red arrow points from the dropdown to the navigation menu item.



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



The screenshot displays the 'Configuration' interface for Identity Automation. The left sidebar shows a navigation menu with 'Policies' expanded, listing 'Authentication', 'Authentication Policies', 'Authentication Options', 'Duo', 'QR Code', 'Challenge', 'Claim', 'Forgot Username', 'Mobile Devices', and 'Password'. The main content area is titled 'Authentication Options' and contains the following controls:

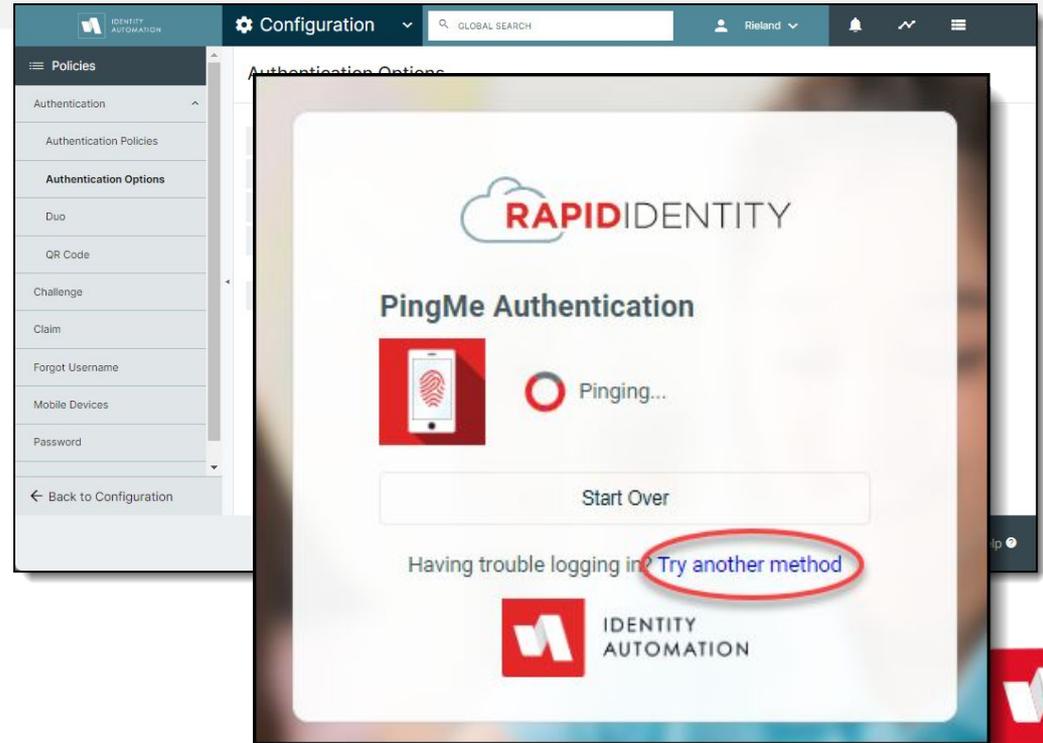
- Four 'Delete' buttons for: 'Delete TOTP keys for user', 'Delete Social IDs for a user', 'Delete Pictograph choices for a user', and 'Delete WebAuthn device registrations'.
- An 'Enable authentication policy choices' checkbox, which is currently checked.

At the bottom right, there are 'Cancel' and 'Save' buttons, along with the 'AppIDENTITY' logo and a 'Help' icon.



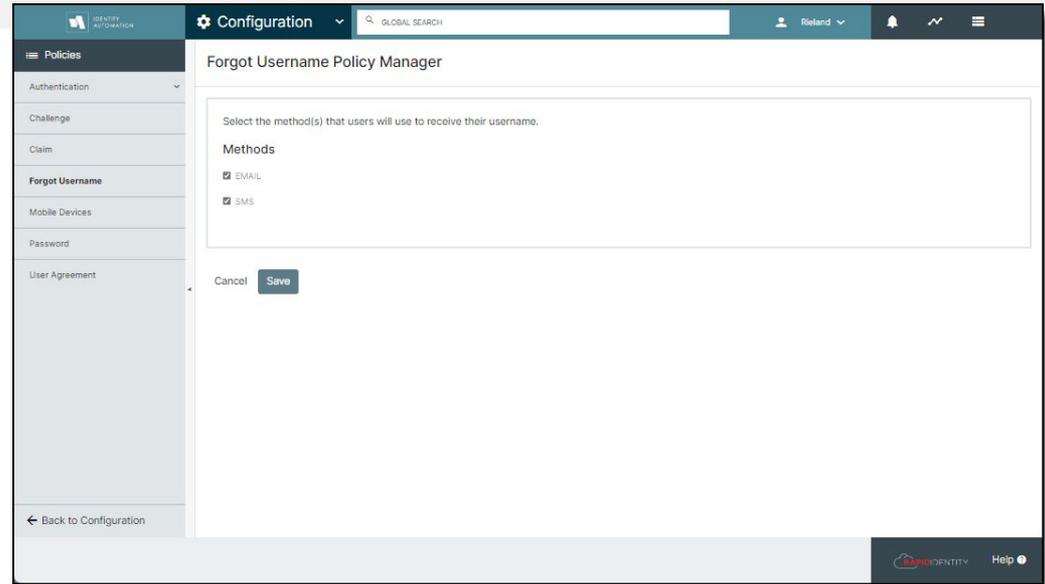
Configuration Policies - Authentication Options

- 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



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



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

The screenshot displays the 'Claim Policy Manager' interface within the Identity Automation system. The top navigation bar includes the 'Configuration' menu, a 'GLOBAL SEARCH' field, and user profile information for 'Retend'. The left sidebar shows a 'Policies' menu with options for Authentication, Challenge, Claim, Forgot Username, Mobile Devices, Password, and User Agreement. The main content area is titled 'Claim Policy Manager' and shows the 'Default Claim Policy' selected. The 'Questions' tab is active, displaying 'Claim Account Questions' and a 'Questions to Ask' section. A form on the right allows for adding questions, with fields for 'GAL Item' (set to 'Claim Code'), 'Display Name' (set to 'Claim Code'), and 'Description'. The bottom right corner features 'Cancel' and 'Save' buttons, along with the 'Identity Automation' logo and a 'Help' icon.



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

The screenshot shows the 'Claim Policy Manager' interface. The left sidebar lists various policy categories: Authentication, Challenge, Claim, Forgot Username, Mobile Devices, Password, and User Agreement. The main content area is titled 'Claim Policy Manager' and shows a 'Default Claim Policy' selected. The 'Questions' tab is active, displaying 'Claim Account Questions'. A form on the right allows for adding questions, with fields for 'GAL Item' (set to 'Claim Code'), 'Display Name' (set to 'Claim Code'), and 'Description'. The interface includes a 'Back to Configuration' button at the bottom left and 'Cancel' and 'Save' buttons at the bottom right. The top navigation bar shows 'Configuration', a search bar, and user information.



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!



alamy

Image ID: 147957
www.alamy.com

Thank you for joining us today!

