IDENTITY AUTOMATION

Writing LDAP Filters

Tips and Tricks

Agenda

01 LDAP Overview

02 Using LDAP in RapidIdentity

03 Create an Admin Delegation

04 Write an LDAP Filter

LDAP Overview

- LDAP = Lightweight Directory Access Protocol
- A standard application protocol for accessing and managing a directory service
- LDAP Filter is a way to query the data stored in the directory; think of it like a SQL query for a database
- Online resources to help write LDAP filters:
    - Free references:
      https://ldap.com/ldap-filters/
      https://ldapwiki.com/
    - Udemy
    - …many more free resources or paid courses
    - IA Support available to answer specific questions

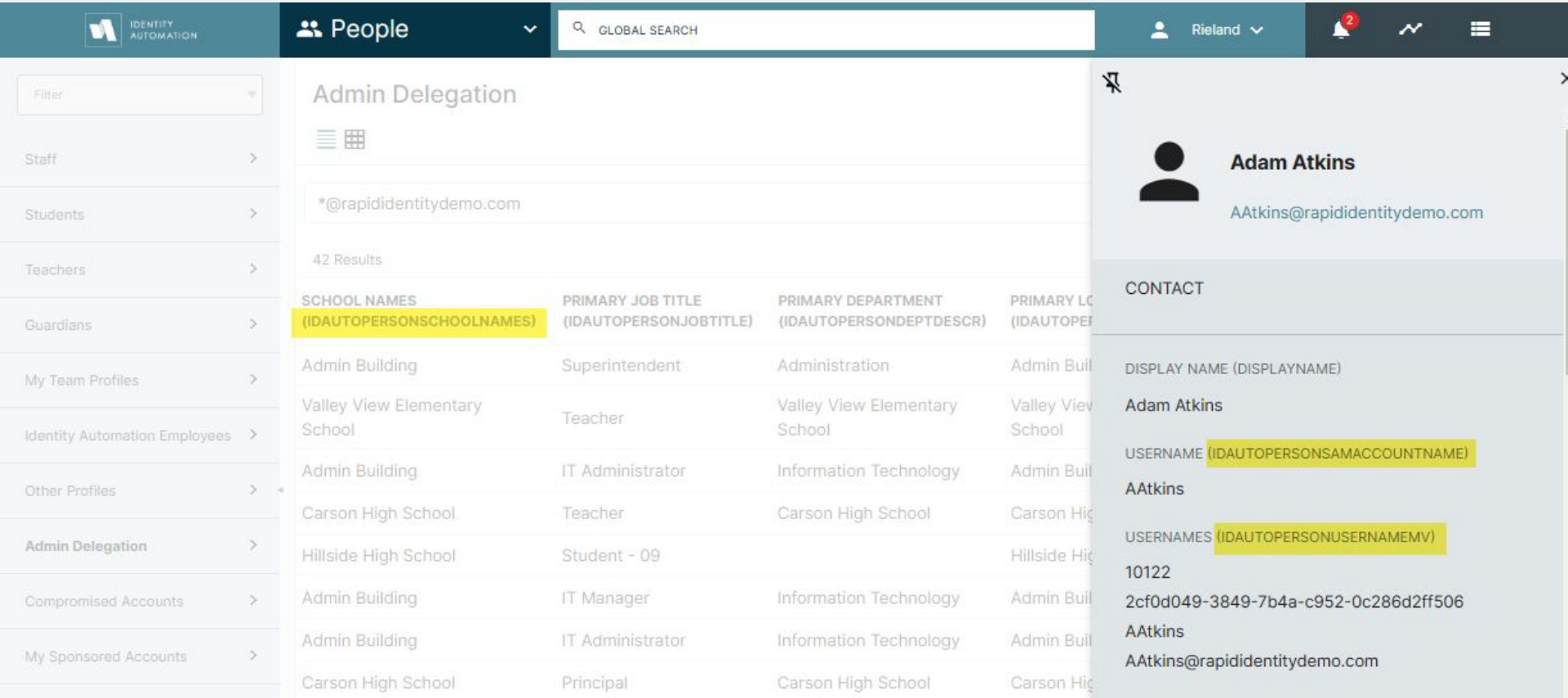
Using LDAP in RapidIdentity

- LDAP filters can be used anywhere you see Attribute Based Access Control:
  - Global module access on main drop-down menu: Applications, People, Roles, Reports, etc.
  - Access control on individual applications
  - People Delegations: Delegation Source or Delegation Target
  - Roles dynamic filters to manage membership

Create an Admin Delegation

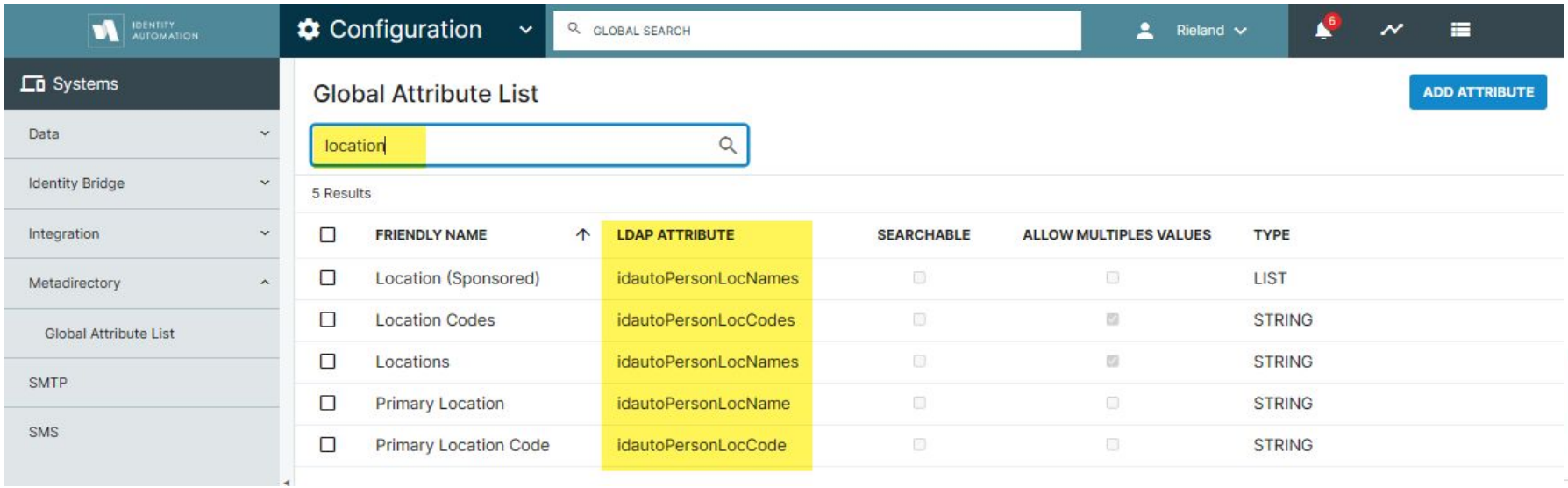
- An admin delegation can be useful for many reasons:
  - Functions like a database query to view and manage all accounts (active and disabled)
  - Display all attributes for a user account, not just a select few
    - Easy to see the attribute name + the contents in one place
  - Enable all Actions used for your business processes (change password, reset challenge questions, MFA actions, etc.)
  - Allow editing of some attributes (with caution)
  - Display Metadirectory attribute names - helpful for writing LDAP filters

Create an Admin Delegation



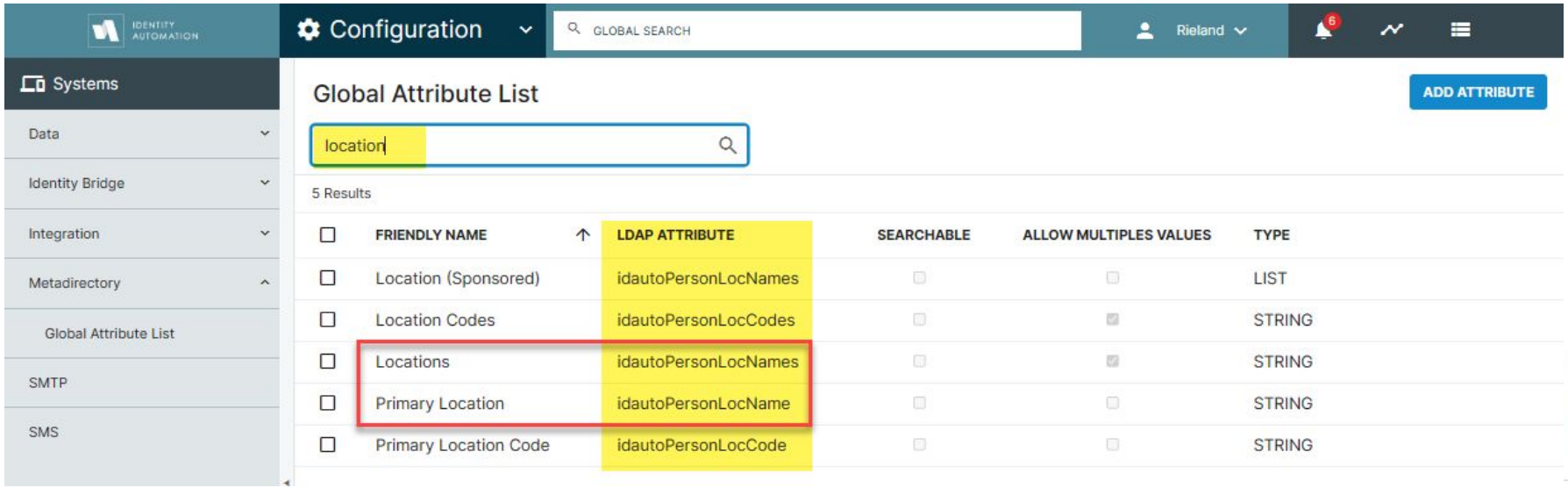
Create an Admin Delegation

- Navigate to Configuration > Systems > Metadirectory > Global Attribute List (GAL)
- Friendly Name vs. LDAP Attribute



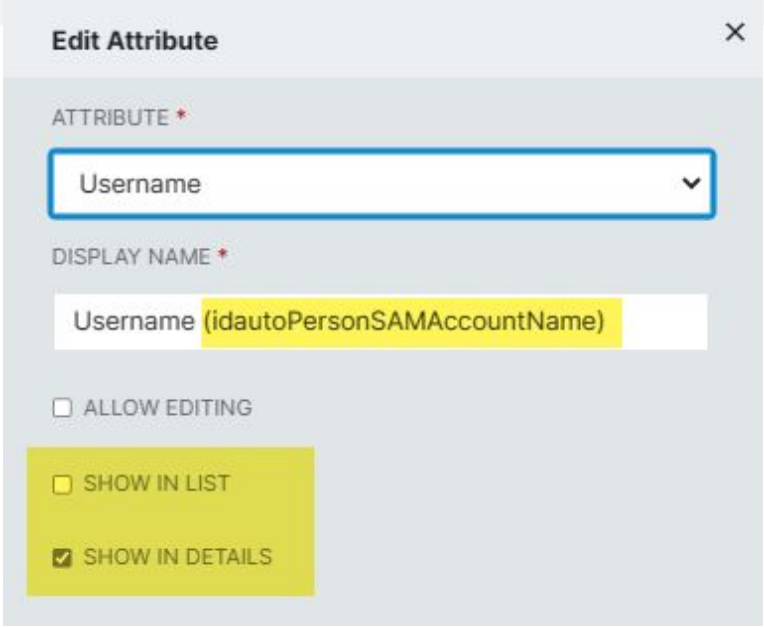
Create an Admin Delegation

- Identifies the contents of each attribute, e.g. Primary Location vs. All Locations where that employee works, or primary enrollment vs. all schools or programs that student attends



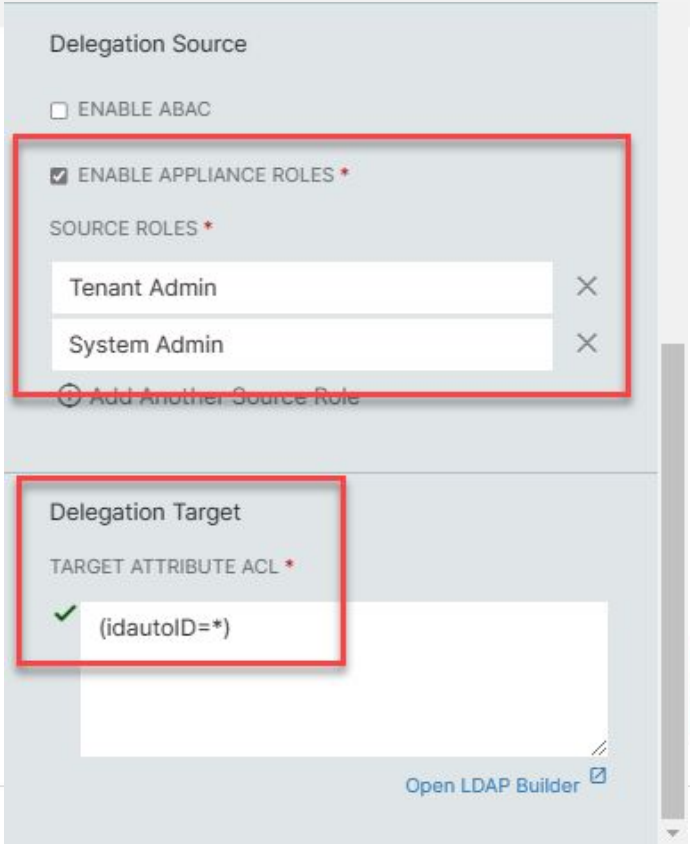
Create an Admin Delegation

- Create a delegation that includes all attributes
- Change the attribute Display Name to show the Friendly Name and LDAP Attribute from the Metadirectory
- Choose to Show In List and/or Show In Details
    - Try to keep Show In List to a minimum to reduce or eliminate the horizontal scroll bar

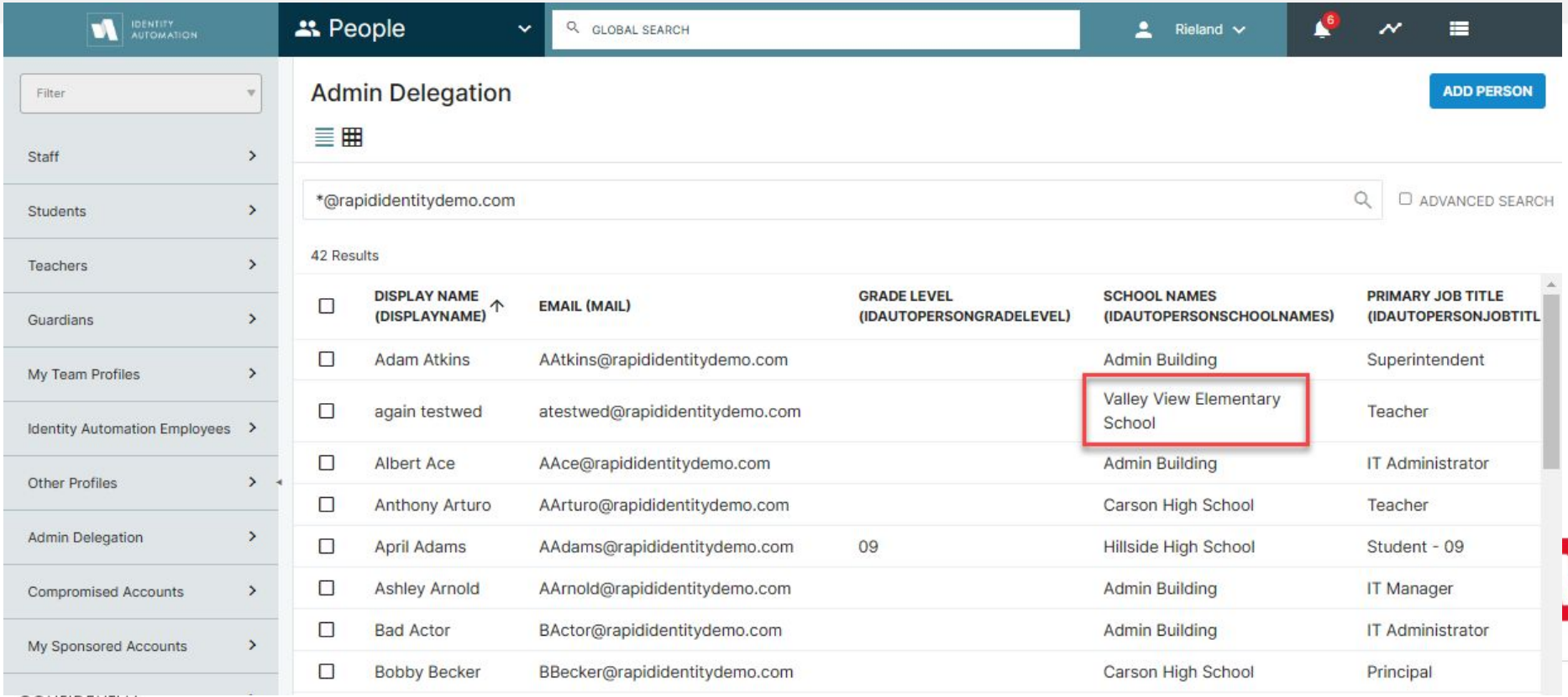


Create an Admin Delegation

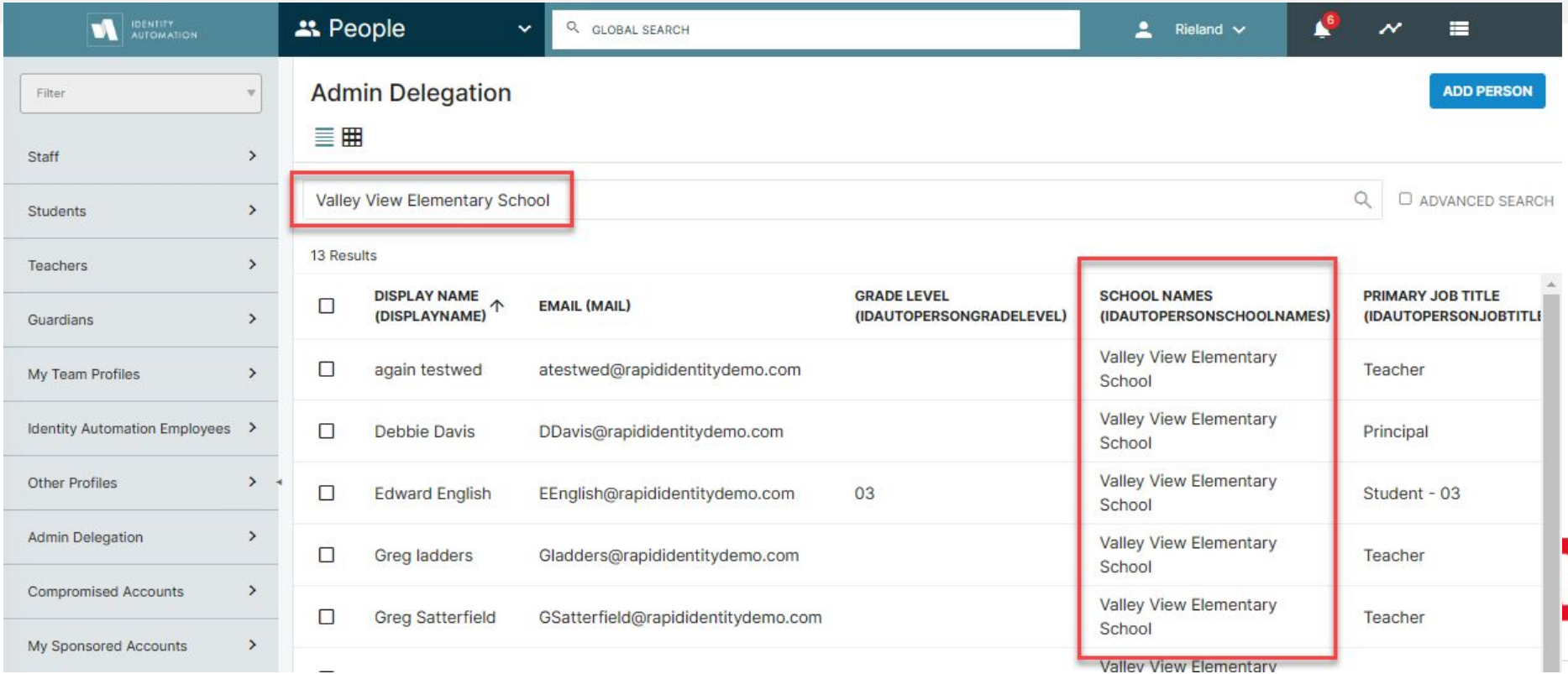
- At the bottom of the General tab, in the Delegation Source select Enable Appliance Roles, and choose Tenant Admin and System Admin
- In the Delegation Target, use the “(idautoID=*)” query to view all accounts
  - Includes sponsored accounts
  - Includes disabled accounts, because there may be times you want to see those, too
- Uncheck the box Preload All Results and do a search by default, since this could show thousands of accounts



Create an Admin Delegation



Create an Admin Delegation



Write LDAP Filters

To write an LDAP filter that finds all Valley View accounts:

(idautoPersonSchoolNames=Valley View Elementary School)

OR select the primary location attribute:

(idautoPersonLocName=Valley View Elementary School)

OR select the all locations attribute:

(idautoPersonLocNames=Valley View Elementary School)

One reason why an admin delegation is useful is to show you which attribute(s) can be used to write filters

All of these attributes can be viewed under the Details pane with the exact value stored in the attribute to copy/paste into the filter (for example, “Valley View” will not work; it must be the full name)

Write LDAP Filters

Combine attributes to limit the list further, so selecting only Staff or only Students from Valley View looks like this:

(&(idautoPersonLocName=Valley View Elementary School)(employeeType=Staff))

(&(idautoPersonLocName=Valley View Elementary School)(employeeType=Student))

Write LDAP Filters

Combine attributes to limit the list further, so selecting only staff at Valley View looks like this:
Use case: email groups or application access in RI

The ampersand means AND, so you are selecting Location AND employeeType of Staff

(&(idautoPersonLocName=Valley View Elementary School)(employeeType=Staff))

(&(idautoPersonLocName=Valley View Elementary School)(employeeType=Staff))

(&(idautoPersonLocName=Valley View Elementary School)(employeeType=Staff))

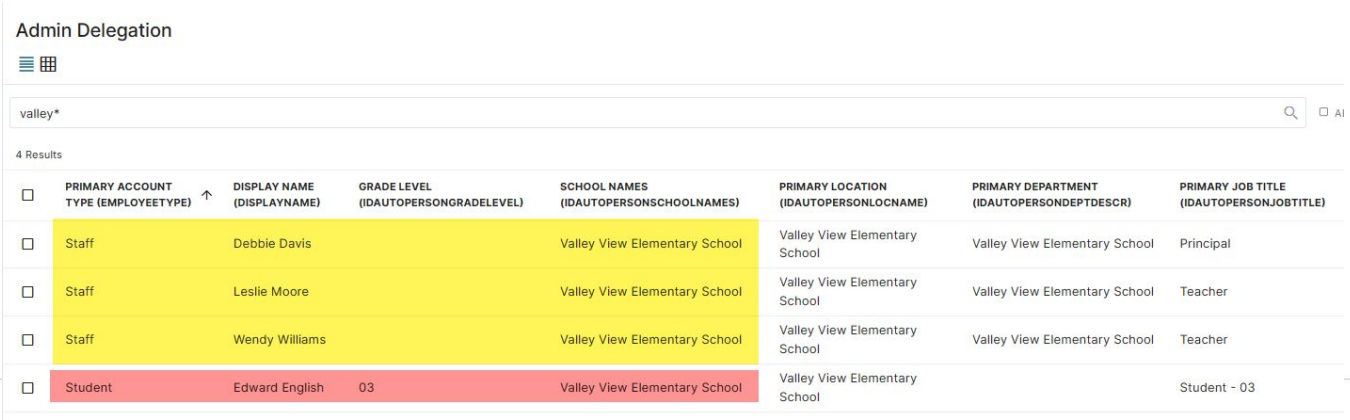
Write LDAP Filters

Combine attributes to limit the list further, so selecting only staff at Valley View looks like this:
Use case: email groups or application access in RI

The ampersand means AND, so you are selecting Location AND employeeType of Staff

(&(idautoPersonLocName=Valley View Elementary School)(employeeType=Staff))

The account in RI has to have both of these attributes in order to match the filter



PRIMARY ACCOUNT TYPE (EMPLOYEETYPE)	DISPLAY NAME (DISPLAYNAME)	GRADE LEVEL (IDAUTOPERSONGRADELEVEL)	SCHOOL NAMES (IDAUTOPERSONSCHOOLNAMES)	PRIMARY LOCATION (IDAUTOPERSONLOCNAME)	PRIMARY DEPARTMENT (IDAUTOPERSONDEPTDESCR)	PRIMARY JOB TITLE (IDAUTOPERSONJOBTITLE)
Staff	Debbie Davis		Valley View Elementary School	Valley View Elementary School	Valley View Elementary School	Principal
Staff	Leslie Moore		Valley View Elementary School	Valley View Elementary School	Valley View Elementary School	Teacher
Staff	Wendy Williams		Valley View Elementary School	Valley View Elementary School	Valley View Elementary School	Teacher
Student	Edward English	03	Valley View Elementary School	Valley View Elementary School		Student - 03

Write LDAP Filters

Combine attributes to limit the list further, so selecting only staff at Valley View looks like this:
Use case: email groups or application access in RI

The ampersand means AND, so you are selecting Location AND employeeType of Staff

(&(idautoPersonLocName=Valley View Elementary School)(employeeType=Staff))

(&(idautoPersonLocName=Valley View Elementary School)(employeeType=Staff))

(&(idautoPersonLocName=Valley View Elementary School)(employeeType=Staff))

Syntax notes:

- No spaces between any of the characters (with the exception of spaces in the attribute contents, i.e. Valley^View^Elementary^School
- No carriage returns inside the filter or at the end

Write LDAP Filters

Select Staff or Sponsored Accounts:
Use case: authentication or password policies

The pipe sign | means OR, so you are selecting Staff OR Sponsored accounts:

(|(employeeType=Staff)(employeeType=Sponsored))

The account in RI has to be either Staff or Sponsored

Select Staff, excluding disabled accounts:

(|(employeeType=Staff)(employeeType=Sponsored))

Write LDAP Filters

CLOUD CUSTOMERS:

Select Staff, excluding disabled accounts:

(&(employeeType=Staff)(!(idautoDisabled=TRUE)))

The exclamation point represents NOT, so this filter selects all staff that are not disabled (i.e. active staff)

** While this active status can be used in Auth Policies, module access, etc, this isn't needed in Roles for Cloud customers because there's a checkbox to exclude disabled accounts*

ON-PREM CUSTOMERS:

Use this AD Attribute to exclude disabled accounts:

(!(userAccountControl:1.2.840.113556.1.4.803:=2))

Write LDAP Filters

Some LDAP filters can be fairly complex. To create an email or security group for all active elementary students across the district, the filter looks like this:

```
(&(employeeType=Student)(!(idautoDisabled=TRUE))(|(idautoPersonGradeLevel=KG)(idautoPersonGrade
Level=01)(idautoPersonGradeLevel=02)(idautoPersonGradeLevel=03)(idautoPersonGradeLevel=04)(idaut
oPersonGradeLevel=05)))
```

Tip: Write your filters in a Role's Dynamic filter tab, then look at Members > Add or Remove Pending tabs to see the results. It provides pretty quick feedback if the filter is pulling the right results.

Thank you for joining us today!

Link to this webinar will be posted on help.rapididentity.com where you can also view upcoming events