



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

The screenshot displays the Identity Automation interface. The top navigation bar includes the Identity Automation logo, a 'People' dropdown menu, a 'GLOBAL SEARCH' input field, and a user profile for 'Rieland'. The main content area is titled 'Admin Delegation' and shows search results for '*@rapididentitydemo.com'. A table lists 42 results with columns for School Names, Primary Job Title, Primary Department, and Primary Location. A user profile card for Adam Atkins is shown on the right, displaying contact information and user identifiers.

Admin Delegation

*@rapididentitydemo.com

42 Results

SCHOOL NAMES (IDAUTOPERSONSCHOOLNAMES)	PRIMARY JOB TITLE (IDAUTOPERSONJOBTITLE)	PRIMARY DEPARTMENT (IDAUTOPERSONDEPTDESCR)	PRIMARY LOCATION (IDAUTOPERSONLOC)
Admin Building	Superintendent	Administration	Admin Building
Valley View Elementary School	Teacher	Valley View Elementary School	Valley View Elementary School
Admin Building	IT Administrator	Information Technology	Admin Building
Carson High School	Teacher	Carson High School	Carson High School
Hillside High School	Student - 09		Hillside High School
Admin Building	IT Manager	Information Technology	Admin Building
Admin Building	IT Administrator	Information Technology	Admin Building
Carson High School	Principal	Carson High School	Carson High School

CONTACT

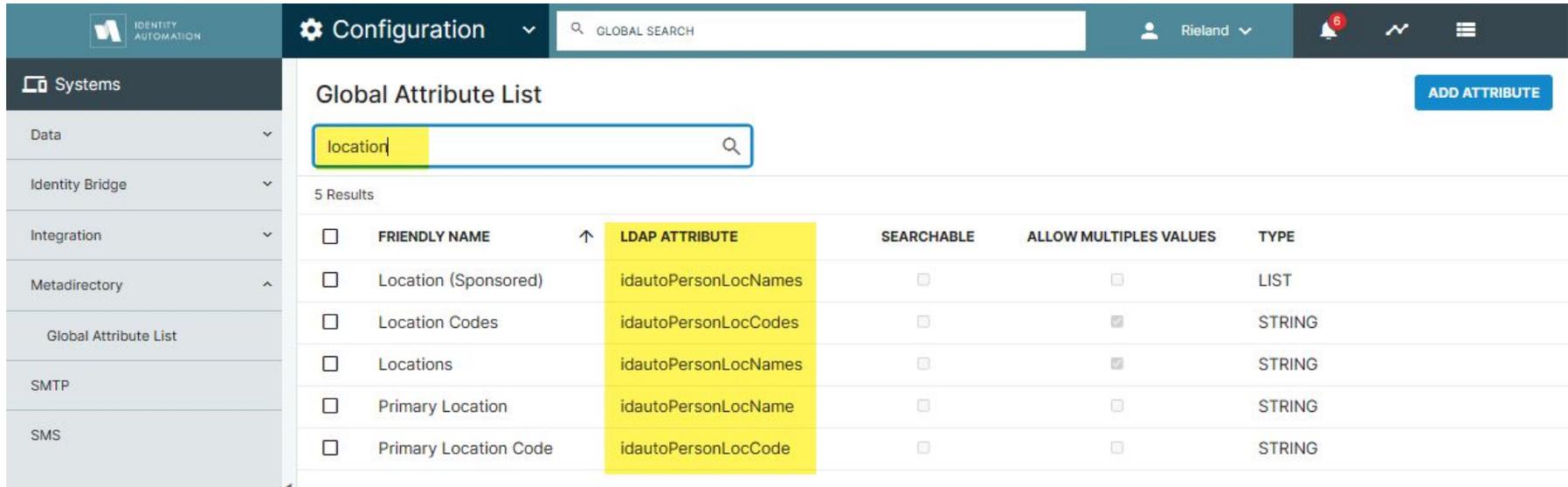
DISPLAY NAME (DISPLAYNAME)
Adam Atkins

USERNAME (IDAUTOPERSONSAMACCOUNTNAME)
AAtkins

USERNAMES (IDAUTOPERSONUSERNAMEMV)
10122
2cf0d049-3849-7b4a-c952-0c286d2ff506
AAtkins
AAtkins@rapididentitydemo.com

Create an Admin Delegation

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



The screenshot shows the Identity Automation configuration interface. The top navigation bar includes the Identity Automation logo, a 'Configuration' dropdown menu, a global search bar, and user information for 'Rieland'. The left sidebar shows a 'Systems' menu with options like Data, Identity Bridge, Integration, Metadirectory, Global Attribute List, SMTP, and SMS. The main content area is titled 'Global Attribute List' and features a search bar with the text 'location'. Below the search bar, it indicates '5 Results' and displays a table with the following columns: Friendly Name, LDAP Attribute, Searchable, Allow Multiples Values, and Type.

<input type="checkbox"/>	FRIENDLY NAME	↑	LDAP ATTRIBUTE	SEARCHABLE	ALLOW MULTIPLES VALUES	TYPE
<input type="checkbox"/>	Location (Sponsored)		idautoPersonLocNames	<input type="checkbox"/>	<input type="checkbox"/>	LIST
<input type="checkbox"/>	Location Codes		idautoPersonLocCodes	<input type="checkbox"/>	<input checked="" type="checkbox"/>	STRING
<input type="checkbox"/>	Locations		idautoPersonLocNames	<input type="checkbox"/>	<input checked="" type="checkbox"/>	STRING
<input type="checkbox"/>	Primary Location		idautoPersonLocName	<input type="checkbox"/>	<input type="checkbox"/>	STRING
<input type="checkbox"/>	Primary Location Code		idautoPersonLocCode	<input type="checkbox"/>	<input type="checkbox"/>	STRING

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

The screenshot shows the Identity Automation Configuration interface. The top navigation bar includes the Identity Automation logo, a 'Configuration' dropdown, a 'GLOBAL SEARCH' input field, and user information for 'Rieland'. The left sidebar shows a 'Systems' menu with options like Data, Identity Bridge, Integration, Metadirectory, Global Attribute List, SMTP, and SMS. The main content area is titled 'Global Attribute List' and features a search bar with the text 'location'. Below the search bar, it indicates '5 Results' and displays a table of attributes.

<input type="checkbox"/>	FRIENDLY NAME	↑	LDAP ATTRIBUTE	SEARCHABLE	ALLOW MULTIPLES VALUES	TYPE
<input type="checkbox"/>	Location (Sponsored)		idautoPersonLocNames	<input type="checkbox"/>	<input type="checkbox"/>	LIST
<input type="checkbox"/>	Location Codes		idautoPersonLocCodes	<input type="checkbox"/>	<input checked="" type="checkbox"/>	STRING
<input type="checkbox"/>	Locations		idautoPersonLocNames	<input type="checkbox"/>	<input checked="" type="checkbox"/>	STRING
<input type="checkbox"/>	Primary Location		idautoPersonLocName	<input type="checkbox"/>	<input type="checkbox"/>	STRING
<input type="checkbox"/>	Primary Location Code		idautoPersonLocCode	<input type="checkbox"/>	<input type="checkbox"/>	STRING

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

Edit Attribute ✕

ATTRIBUTE *

Username ▾

DISPLAY NAME *

Username (idautoPersonSAMAccountName)

ALLOW EDITING

SHOW IN LIST

SHOW IN DETAILS



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

Delegation Source

ENABLE ABAC

ENABLE APPLIANCE ROLES *

SOURCE ROLES *

Tenant Admin ×

System Admin ×

+ Add Another Source Role

Delegation Target

TARGET ATTRIBUTE ACL *

✓ (idautoID=*)

Open LDAP Builder

Create an Admin Delegation

The screenshot shows the Identity Automation interface. The top navigation bar includes the Identity Automation logo, a 'People' dropdown menu, a 'GLOBAL SEARCH' input field, and a user profile for 'Rieland'. A notification bell icon shows 6 alerts. The left sidebar contains a 'Filter' dropdown and a list of categories: Staff, Students, Teachers, Guardians, My Team Profiles, Identity Automation Employees, Other Profiles, Admin Delegation, Compromised Accounts, and My Sponsored Accounts. The main content area is titled 'Admin Delegation' and features a search bar with the query '*@rapididentitydemo.com'. Below the search bar, it indicates '42 Results'. A table displays the search results with the following columns: DISPLAY NAME (DISPLAYNAME), EMAIL (MAIL), GRADE LEVEL (IDAUTOPERSONGRADELEVEL), SCHOOL NAMES (IDAUTOPERSONSCHOOLNAMES), and PRIMARY JOB TITLE (IDAUTOPERSONJOBITL). The row for 'Valley View Elementary School' is highlighted with a red box.

<input type="checkbox"/>	DISPLAY NAME (DISPLAYNAME) ↑	EMAIL (MAIL)	GRADE LEVEL (IDAUTOPERSONGRADELEVEL)	SCHOOL NAMES (IDAUTOPERSONSCHOOLNAMES)	PRIMARY JOB TITLE (IDAUTOPERSONJOBITL)
<input type="checkbox"/>	Adam Atkins	AAtkins@rapididentitydemo.com		Admin Building	Superintendent
<input type="checkbox"/>	again testwed	atestwed@rapididentitydemo.com		Valley View Elementary School	Teacher
<input type="checkbox"/>	Albert Ace	AAce@rapididentitydemo.com		Admin Building	IT Administrator
<input type="checkbox"/>	Anthony Arturo	AArturo@rapididentitydemo.com		Carson High School	Teacher
<input type="checkbox"/>	April Adams	AAdams@rapididentitydemo.com	09	Hillside High School	Student - 09
<input type="checkbox"/>	Ashley Arnold	AArnold@rapididentitydemo.com		Admin Building	IT Manager
<input type="checkbox"/>	Bad Actor	BActor@rapididentitydemo.com		Admin Building	IT Administrator
<input type="checkbox"/>	Bobby Becker	BBecker@rapididentitydemo.com		Carson High School	Principal

Create an Admin Delegation

The screenshot shows the Identity Automation interface. The top navigation bar includes the Identity Automation logo, a 'People' dropdown menu, a 'GLOBAL SEARCH' input field, and a user profile for 'Rieland'. A left-hand navigation menu lists various categories: Filter, Staff, Students, Teachers, Guardians, My Team Profiles, Identity Automation Employees, Other Profiles, Admin Delegation, Compromised Accounts, and My Sponsored Accounts. The main content area is titled 'Admin Delegation' and features a search bar containing 'Valley View Elementary School'. Below the search bar, a table displays 13 results. The table has columns for 'DISPLAY NAME (DISPLAYNAME)', 'EMAIL (MAIL)', 'GRADE LEVEL (IDAUTPERSONGRADELEVEL)', 'SCHOOL NAMES (IDAUTPERSONSCHOOLNAMES)', and 'PRIMARY JOB TITLE (IDAUTPERSONJOBTITLE)'. The 'SCHOOL NAMES' column is highlighted with a red box. The results include entries for 'again testwed', 'Debbie Davis', 'Edward English', 'Greg ladders', and 'Greg Satterfield', all associated with 'Valley View Elementary School'.

<input type="checkbox"/>	DISPLAY NAME (DISPLAYNAME) ↑	EMAIL (MAIL)	GRADE LEVEL (IDAUTPERSONGRADELEVEL)	SCHOOL NAMES (IDAUTPERSONSCHOOLNAMES)	PRIMARY JOB TITLE (IDAUTPERSONJOBTITLE)
<input type="checkbox"/>	again testwed	atestwed@rapididentitydemo.com		Valley View Elementary School	Teacher
<input type="checkbox"/>	Debbie Davis	DDavis@rapididentitydemo.com		Valley View Elementary School	Principal
<input type="checkbox"/>	Edward English	EEnglish@rapididentitydemo.com	03	Valley View Elementary School	Student - 03
<input type="checkbox"/>	Greg ladders	Gladders@rapididentitydemo.com		Valley View Elementary School	Teacher
<input type="checkbox"/>	Greg Satterfield	GSatterfield@rapididentitydemo.com		Valley View Elementary School	Teacher

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

Admin Delegation

valley*

4 Results

<input type="checkbox"/>	PRIMARY ACCOUNT TYPE (EMPLOYEE TYPE) ↑	DISPLAY NAME (DISPLAYNAME)	GRADE LEVEL (IDAUTOPERSONGRADELEVEL)	SCHOOL NAMES (IDAUTOPERSONSCHOOLNAMES)	PRIMARY LOCATION (IDAUTOPERSONLOCNAME)	PRIMARY DEPARTMENT (IDAUTOPERSONDEPTDESCR)	PRIMARY JOB TITLE (IDAUTOPERSONJOBTITLE)
<input type="checkbox"/>	Staff	Debbie Davis		Valley View Elementary School	Valley View Elementary School	Valley View Elementary School	Principal
<input type="checkbox"/>	Staff	Leslie Moore		Valley View Elementary School	Valley View Elementary School	Valley View Elementary School	Teacher
<input type="checkbox"/>	Staff	Wendy Williams		Valley View Elementary School	Valley View Elementary School	Valley View Elementary School	Teacher
<input type="checkbox"/>	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)(idautoPersonGradeLevel=01)(idautoPersonGradeLevel=02)(idautoPersonGradeLevel=03)(idautoPersonGradeLevel=04)(idautoPersonGradeLevel=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

