Identity Management (IdM)
Local Access Manager (LAM) User Guide

Updated 7/30/2026

Contents

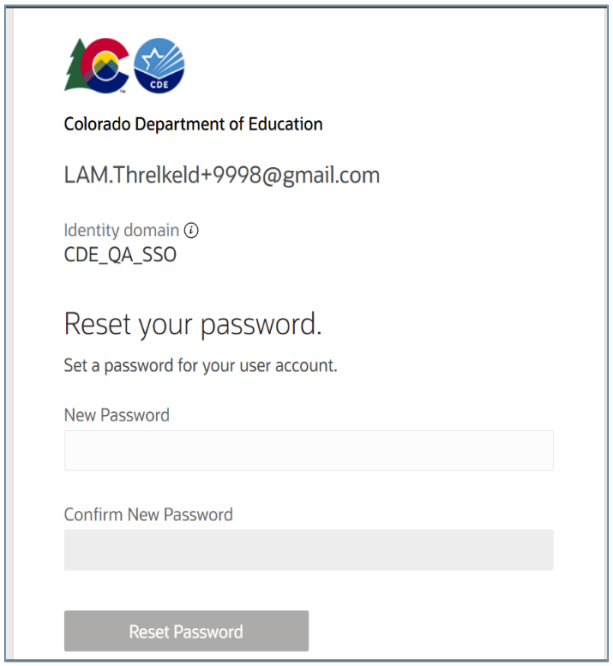
Account Activation **2**
Multifactor Authentication **3**
Access Manager Application **5**
Create a New Users 5
Searching For Users 6
Disabling User Accounts 6
Managing User Access Rights 7
Application LAM Rights Tab 8
User Organization Tab 8
Exporting User Accounts 9
Reports 10

Account Activation

Once your account is setup you will receive an email from Oracle 'no-reply@mailer.us-luke-1.identity.ics.oci.oraclegovcloud.com.' If you don't see this in your inbox, you may need to search for it and/or check the junk or spam folders. ***You will have 30 days to activate your account.***

Click the **Activate Your Account** link in the email.

A web page will open, directing you to set your password.



Password requirements:

- Must have between 12 and 40 characters
- Cannot contain the First Name of the user
- Cannot contain the Last Name of the user
- Cannot contain the user name
- Must have at least 1 lowercase character
- Must have at least 1 uppercase character
- Must have at least 1 numeric character
- Cannot repeat last 4 passwords

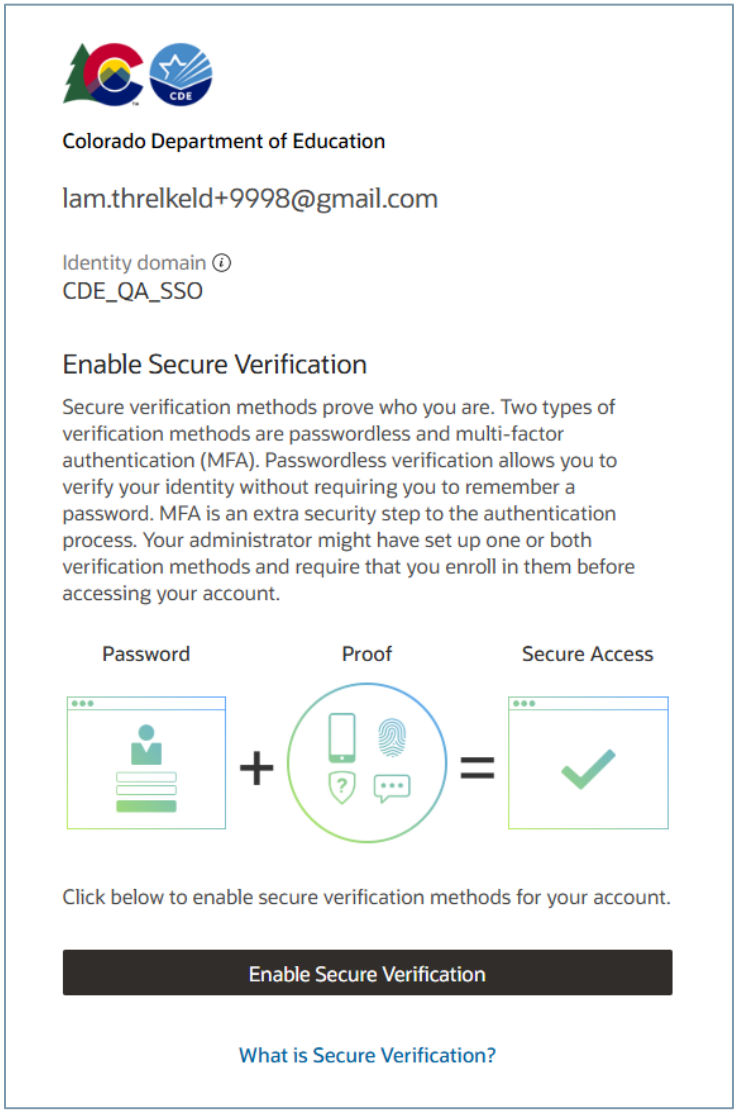
Multifactor Authentication

Once you have activated your account, you will be able to log into the **Access Manager Application** (https://lam.cde.state.co.us/ords/r/cdelam/delegated-administration/landing)

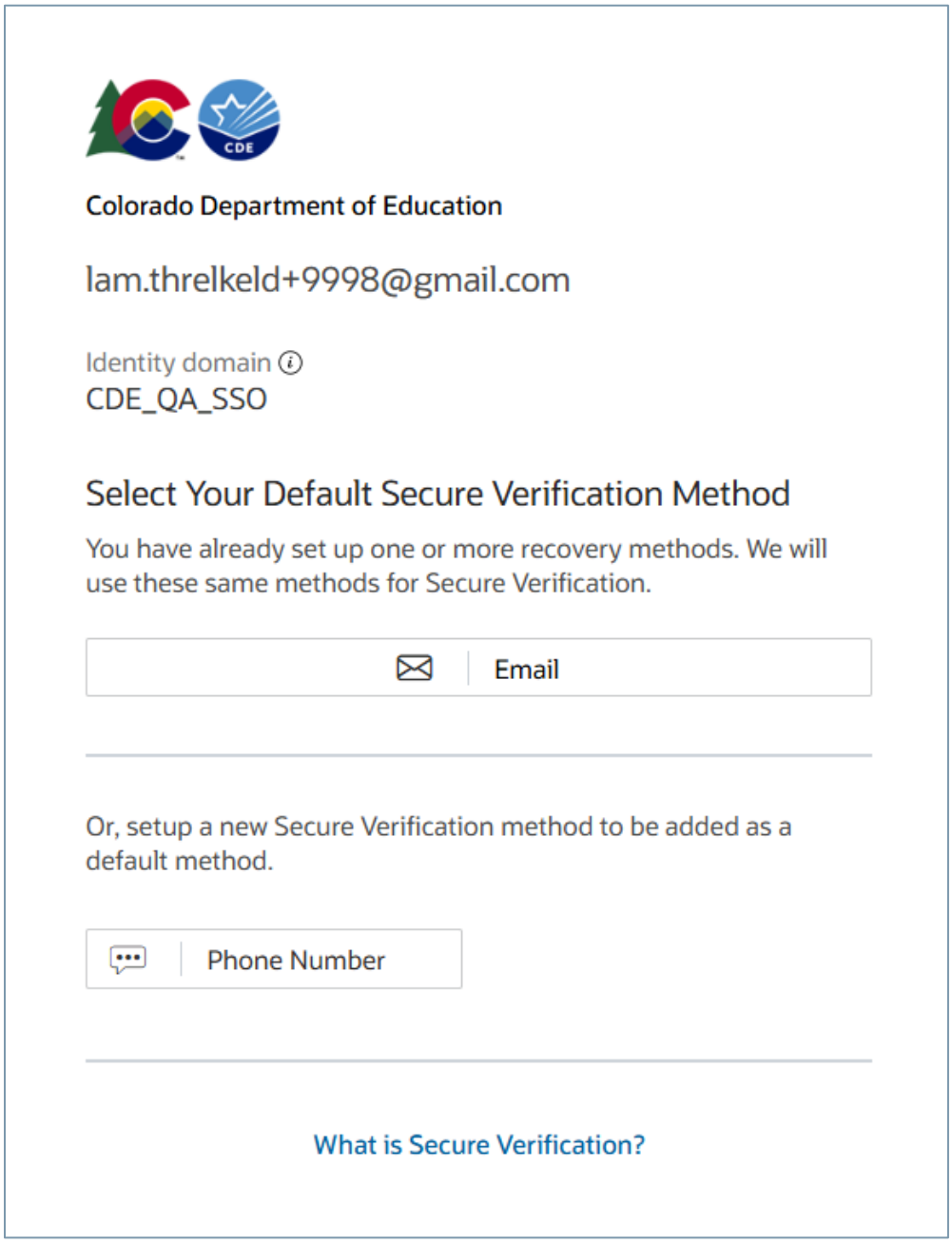
Log in with your username and password you created.

On your first login, you will be prompted to select a form of multifactor authentication.

Click **Enable secure verification**



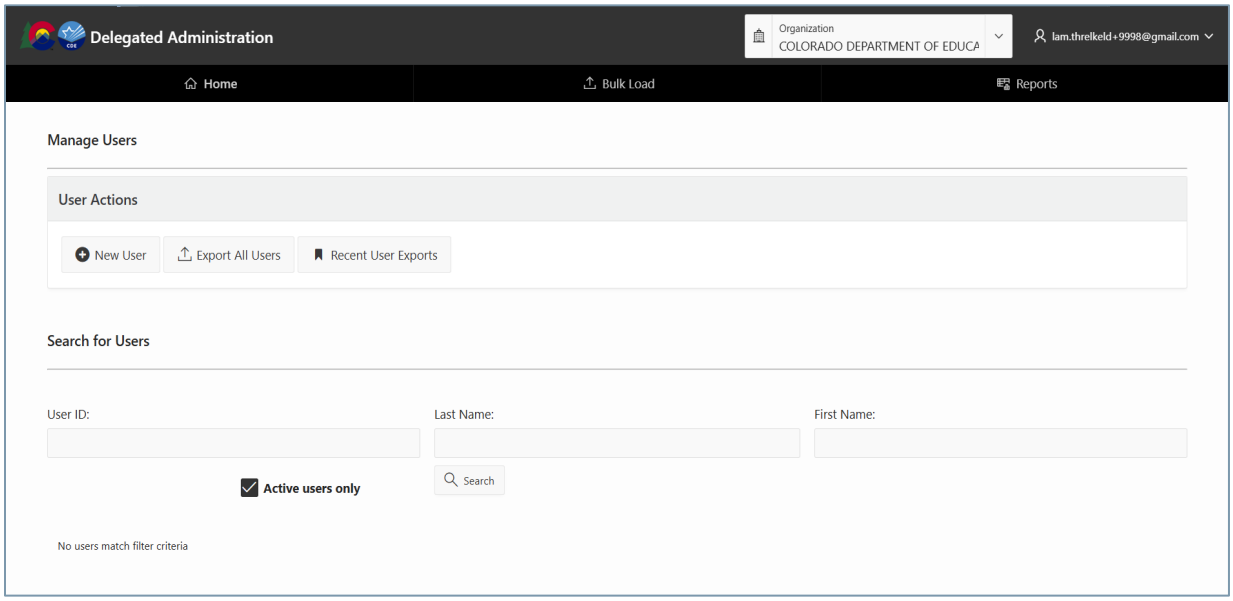
Select your default Secure Verification Method: email or text (mobile phone number required).



After your verification method selection, you will be taken to a verification screen for the method you selected. Follow directions to complete the verification and enter the code you receive.

Access Manager Application

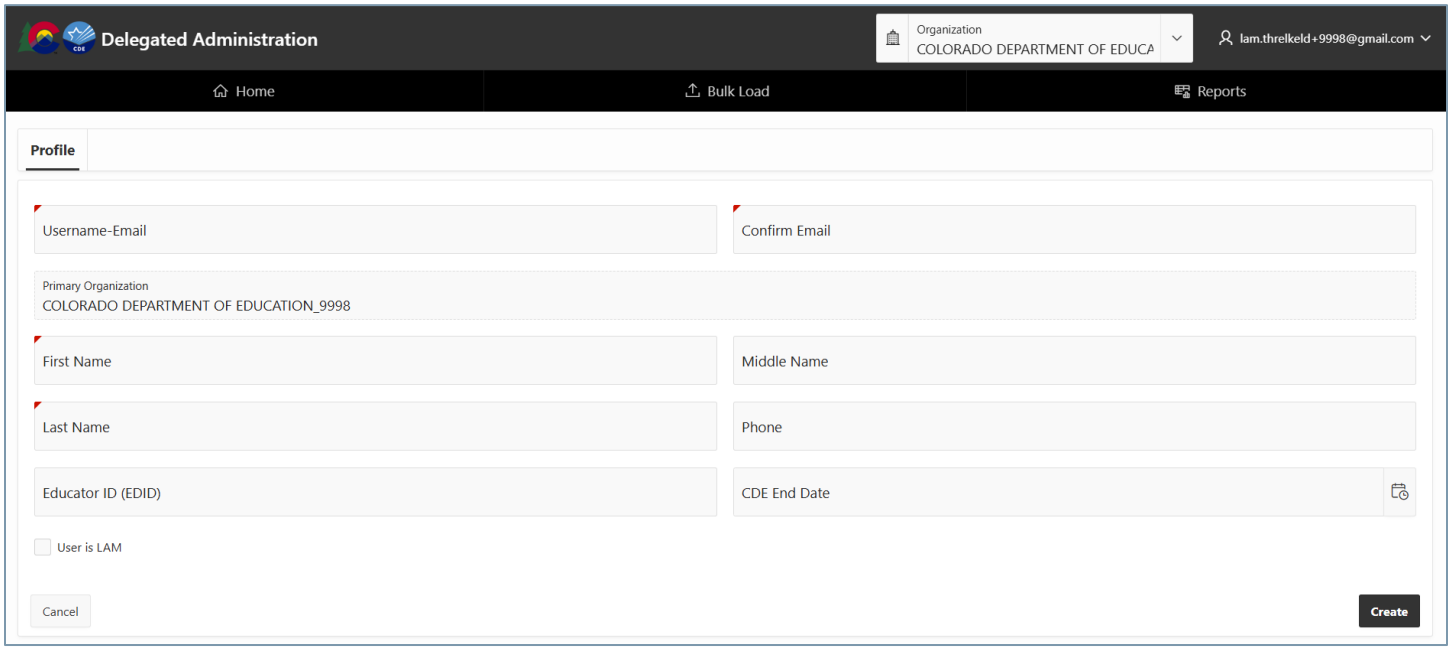
After Activating your preferred method of Secure Verification, you will be passed into the **LAM Application** (https://lam.cde.state.co.us/ords/r/cdelam/delegated-administration/landing).



The Home page will let you create, search for and manage user accounts within your organization.

Create a New Users

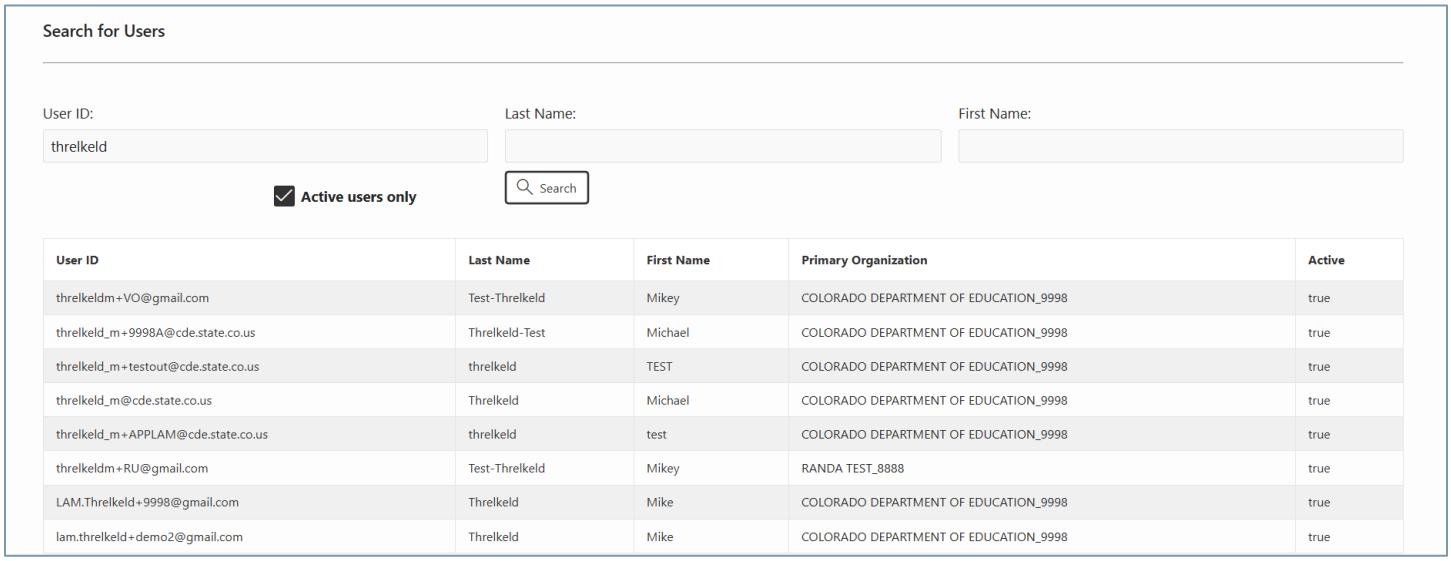
To create a new user, Click the **New User button** and enter the required fields denoted by the hashmark.



Once you click the Create button the user will be emailed by the system to activate their account. This account activation will mirror the process described above in this document.

Searching For Users

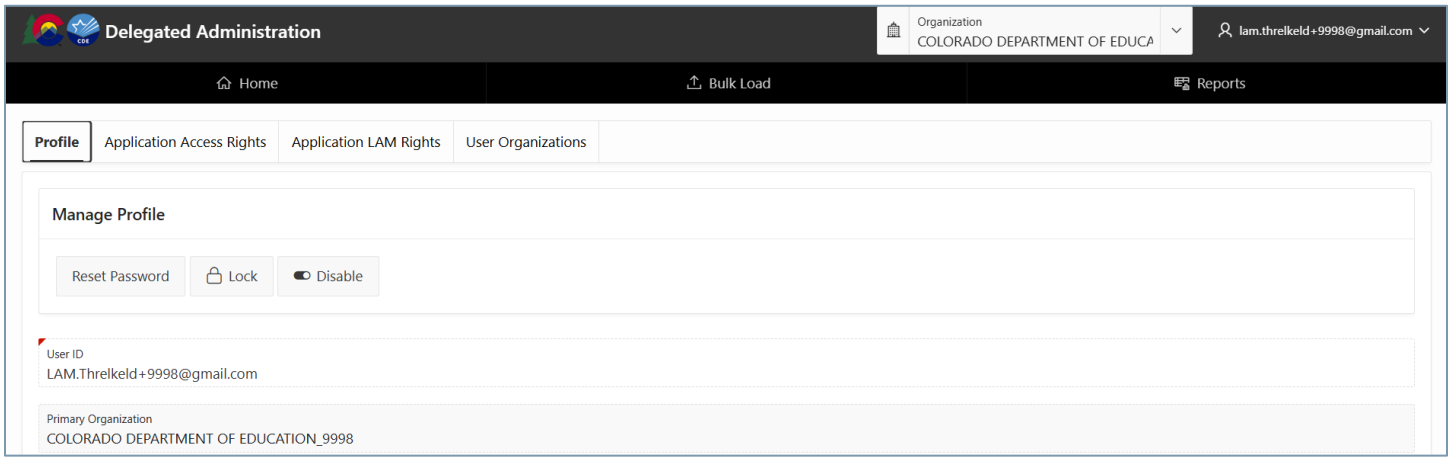
You may also search for a user from the **home page** by entering either their email address/username, first name or last name and clicking the **search button.**



User ID	Last Name	First Name	Primary Organization	Active
threlkeldm+VO@gmail.com	Test-Threlkeld	Mikey	COLORADO DEPARTMENT OF EDUCATION_9998	true
threlkeld_m+9998A@cde.state.co.us	Threlkeld-Test	Michael	COLORADO DEPARTMENT OF EDUCATION_9998	true
threlkeld_m+testout@cde.state.co.us	threlkeld	TEST	COLORADO DEPARTMENT OF EDUCATION_9998	true
threlkeld_m@cde.state.co.us	Threlkeld	Michael	COLORADO DEPARTMENT OF EDUCATION_9998	true
threlkeld_m+APPLAM@cde.state.co.us	threlkeld	test	COLORADO DEPARTMENT OF EDUCATION_9998	true
threlkeldm+RU@gmail.com	Test-Threlkeld	Mikey	RANDA TEST_8888	true
LAM.Threlkeld+9998@gmail.com	Threlkeld	Mike	COLORADO DEPARTMENT OF EDUCATION_9998	true
lam.threlkeld+demo2@gmail.com	Threlkeld	Mike	COLORADO DEPARTMENT OF EDUCATION_9998	true

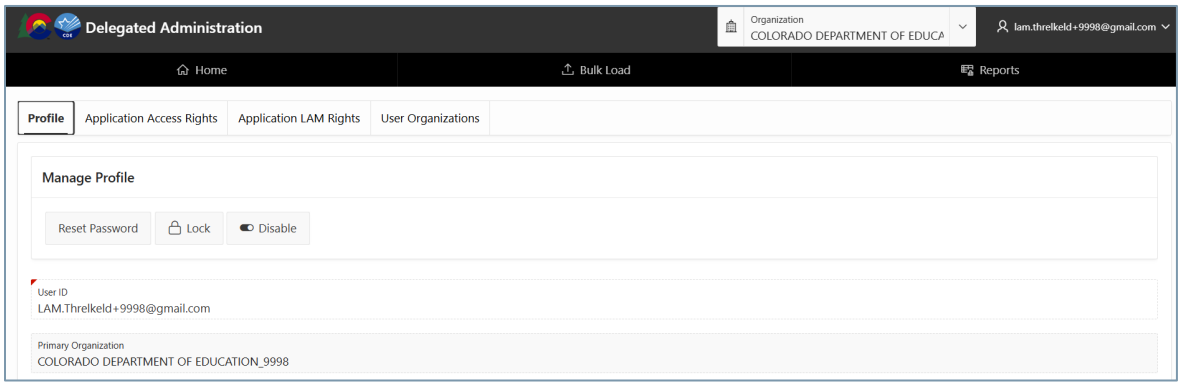
Disabling User Accounts

User accounts can be Locked/Unlocked or Disabled from the **Profile tab.**

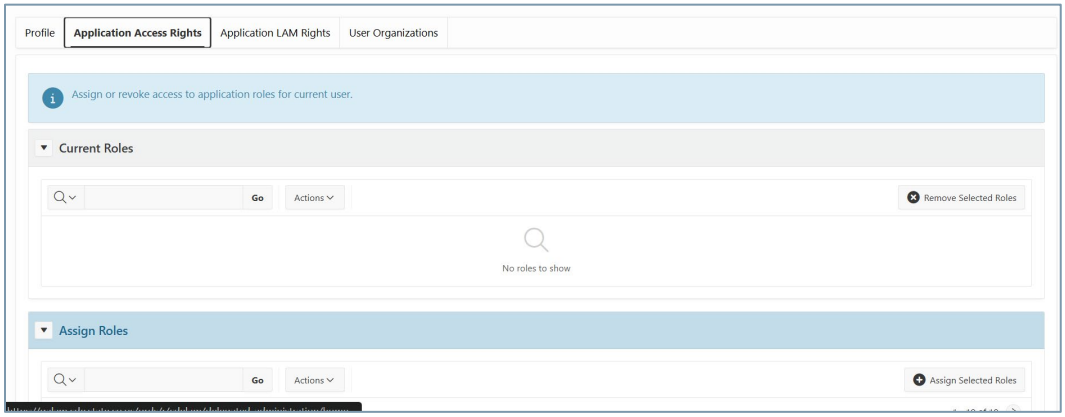


Managing User Access Rights

Once you have created or selected a user you can assign them access rights from the **Application Access Rights Tab** along the top of the page.



From this Tab, currently assigned groups will be listed in the first section, **Current Roles**, while available groups will be listed in the lower section, **Assign Role**.

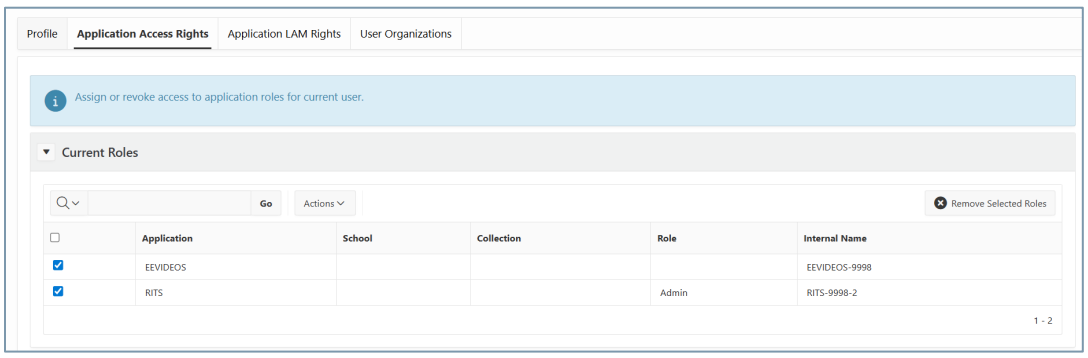


Once you have selected the group you would like the user to have simply click on the **Assign Selected Roles button** in the top right corner of the section.

Revoking access to an application can be done is much the same way as assigned access.

The list of assigned access rights will be displayed at the top of the application access rights tab.

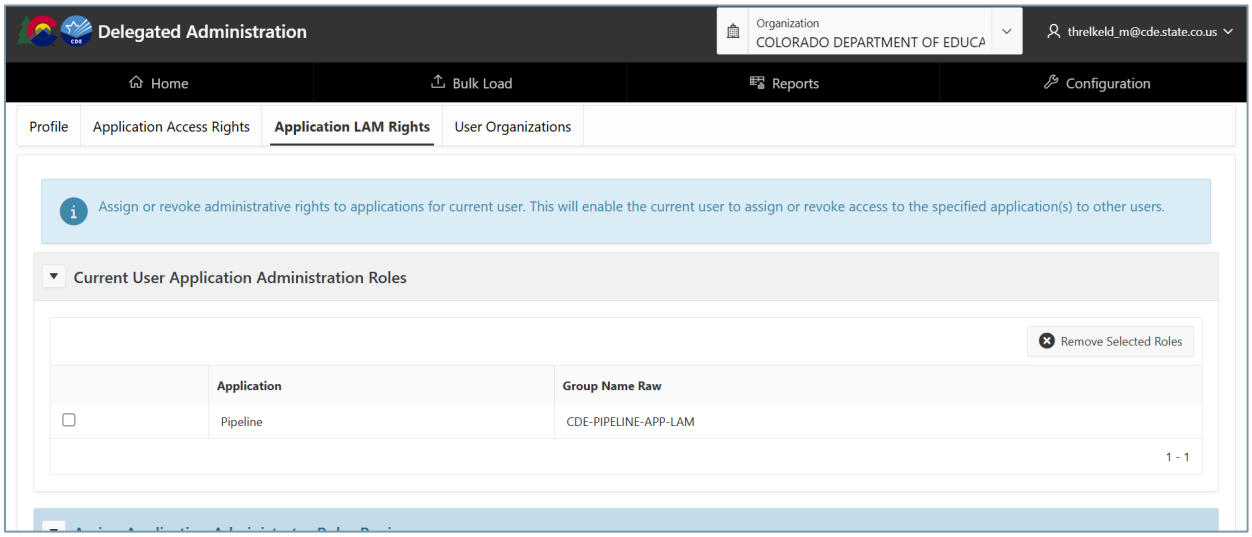
From here select the roles that the user no longer needs and then click the **Remove Selected Roles button** in the top right corner of the section.



Application LAM Rights Tab

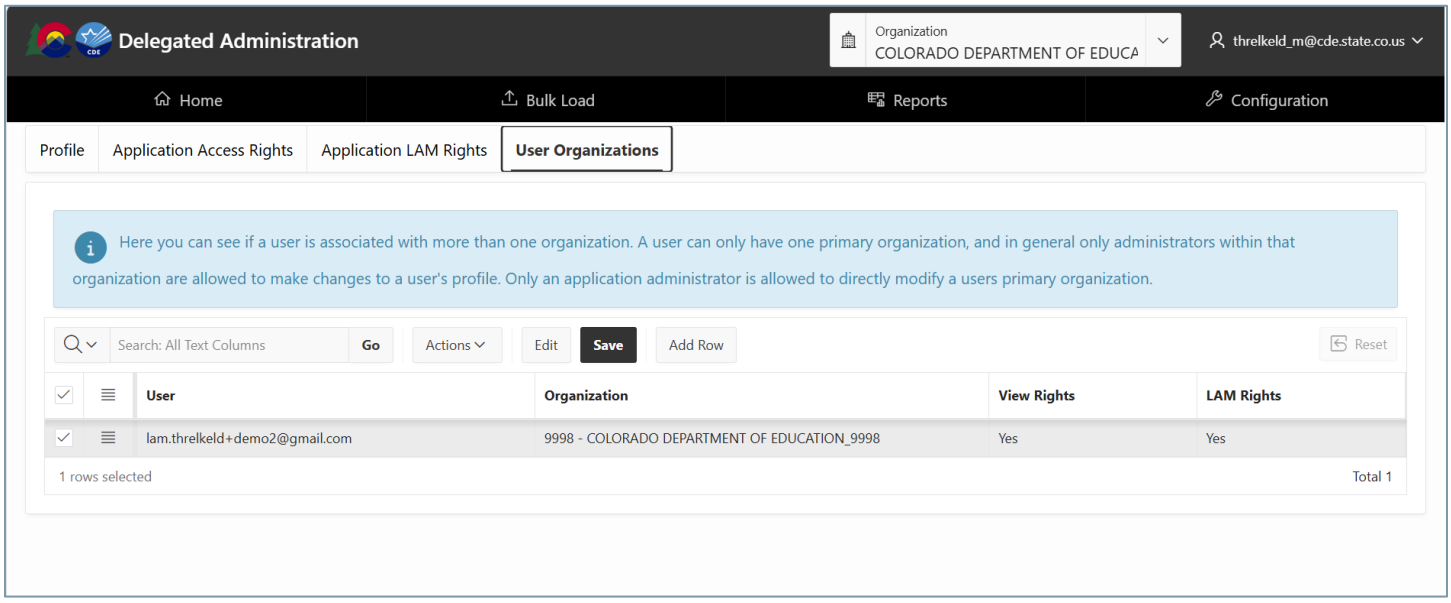
From the **Application LAM Rights tab,** a LAMs application access rights can be filtered down by application groups.

For example, a user assigned CDE-PIPELINE-APP-LAM will only be able to view and assign PIPELINE roles.



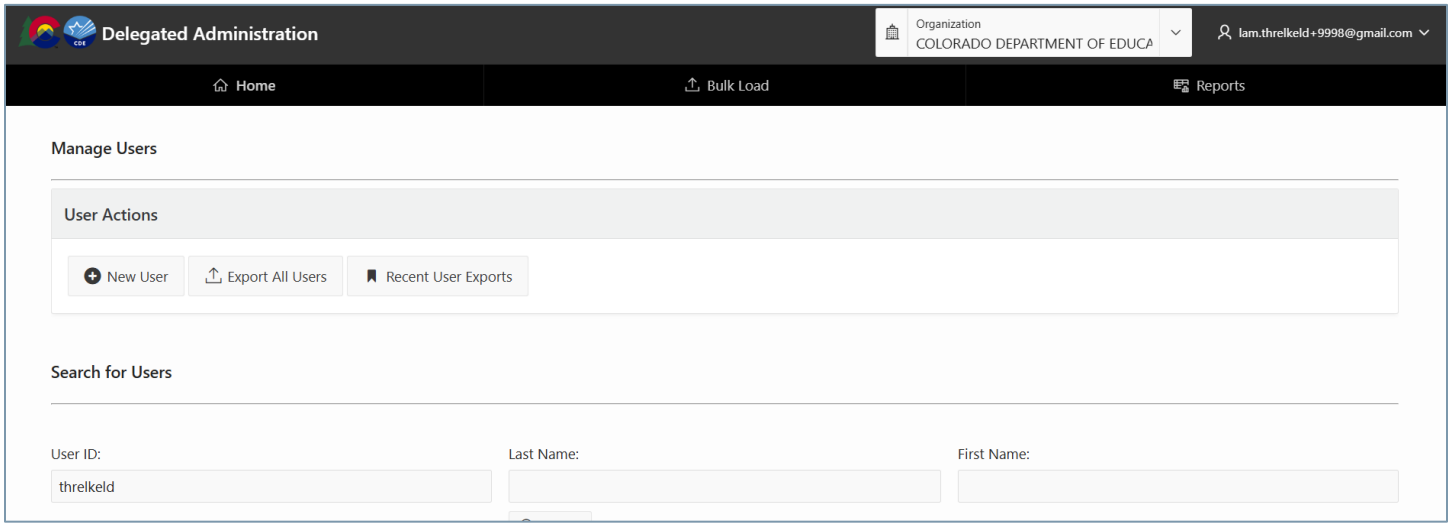
User Organization Tab

The **user organization tab** will show you each of the organizations that user has been attached to and their right within it.

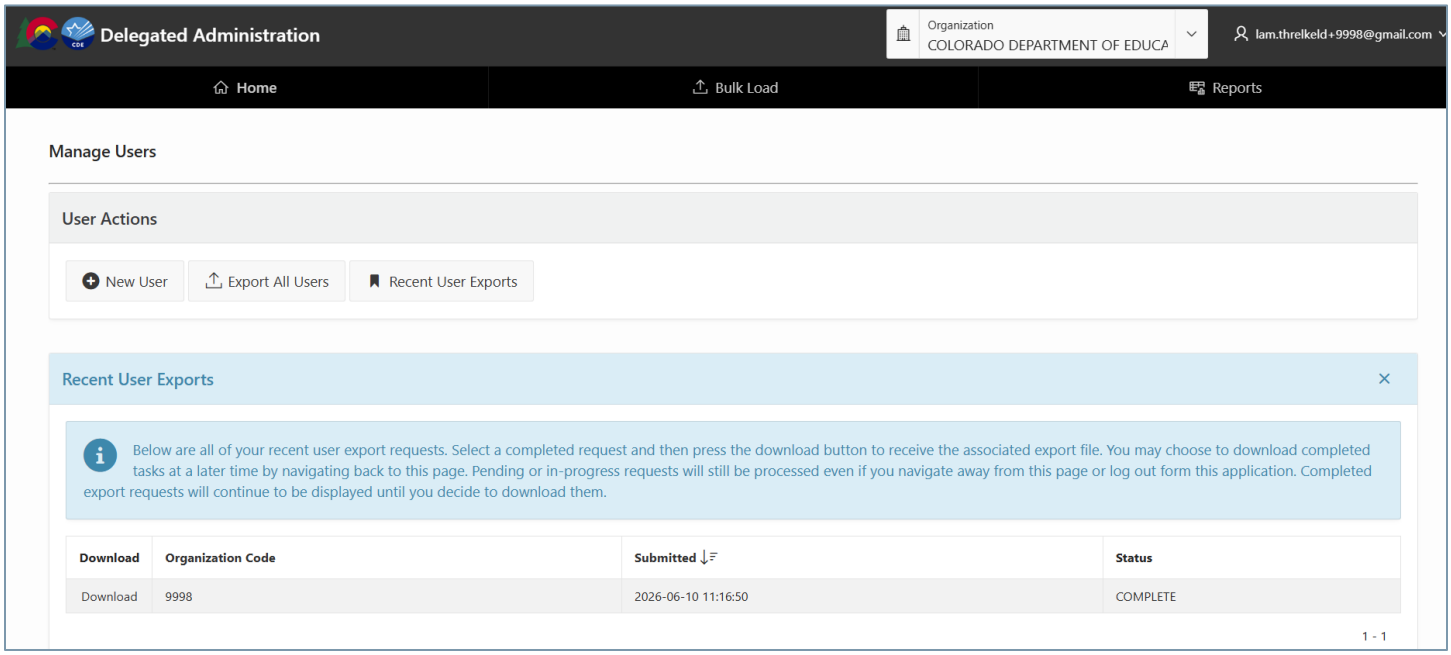


Exporting User Accounts

A full list of user accounts can be exported from the Home page.

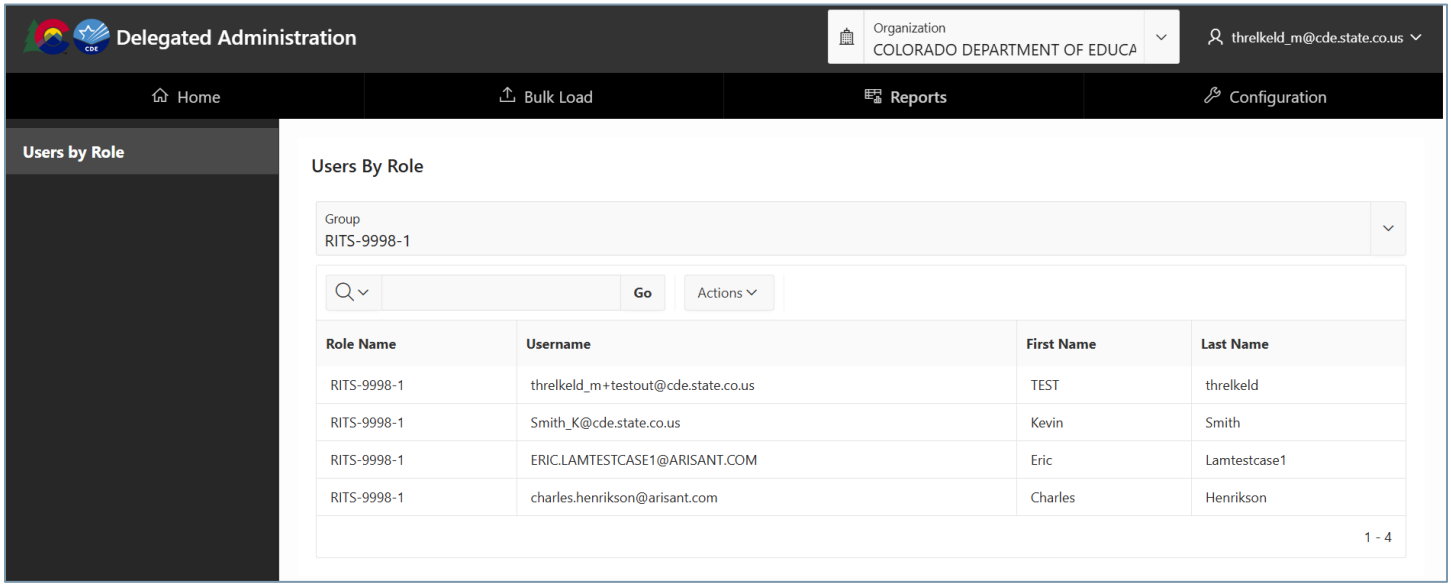


Clicking the **Export All Users button** will start the process.



You can then click the **download button** to save a copy of the user export.

Previous user exports can be viewed by clicking the **Recent User Exports button**.

Reports

The **Reports page** currently only has a query that lets you search for all the users assigned to a specific group/role. For example, the image below shows the report listing all users assigned the RITS-9998-1 role.