

MoH Keycloak User Management Console – Training Guide

CGI Ministry of Health

Date: 2024-09-23

Experience the commitment®



Table of Revisions

Version	Revised Date	Revised By	Revisions
1.0	July 28, 2020	Leon Wood	Version 1
1.2	January 6, 2023	Adam Hoplock Gary Donoghue Leah Macdonald	Updated content for UMC
1.3	November 9, 2023	Leah Macdonald, Filip Florek	Updated template, add user management
1.4	February 20, 2024	David Sharpe	Formatting
1.5	Aug 15, 2024	Helen Mak, Filip Florek, Adam Hoplock	Update content for UMC and review grammar
2.1	September 23, 2024	David Sharpe	Formatting

Table of Contents

MOH Keycloak Solution.....	4
Document Purpose	4
Background.....	4
Keycloak Solution Components	5
User Management Application Overview	7
Access to User Management	7
Application URLs	7
Users Search Guide	8
Basic User Search	8
Advanced User Search	9
User Update Guide.....	11
Update User Details	11
Add/Edit User Roles	13
Add/Edit Mailbox Authorizations.....	13
Update User Groups.....	14
Register New User.....	15
Error Messages Related to Manual Registration of New User.....	16
Dashboard Page Guide.....	17
Active User Count	17
User Metrics.....	18
Total Number of Users	18
Unique User Counts	18
Organizations Page Guide	19
Organization Search	19
Create Organization	19
Appendix A: User Already Exists	20

MOH Keycloak Solution

Document Purpose

This document serves as a user guide for individuals and teams who need to use the Keycloak User Management application to support the MoH Keycloak Authentication Service. The User Management application is utilized by several Access Teams throughout the health sector, including the ITSB Access Team, Registries Connections, Vital Stats Help Desk, and HIBC Access Management. Access may be expanded as additional applications are migrated to the Keycloak service and as new support teams require access.

Note: Permissions can be assigned to support teams in Keycloak that can restrict what applications the different support teams are able to provision access for. This can change the display of the interface for the various permission levels.

Background

Keycloak is being adopted by the Ministry of Health to assist with user authentication and authorization for Ministry applications. The MoH Keycloak Authentication Service will serve as a replacement to the current HealthNetBC Portal (LDAP based) and SiteMinder solutions being used for Java and Drupal applications and may also be used to secure other (non-Java or Drupal) Ministry applications in the future.

The MoH Keycloak Authentication Service will benefit existing web application owners and users by allowing those users to use electronic ID credentials they already have (e.g. IDIR, Health Authority IDs, BCeID, and others) to access web applications that currently require legacy LDAP IDs.

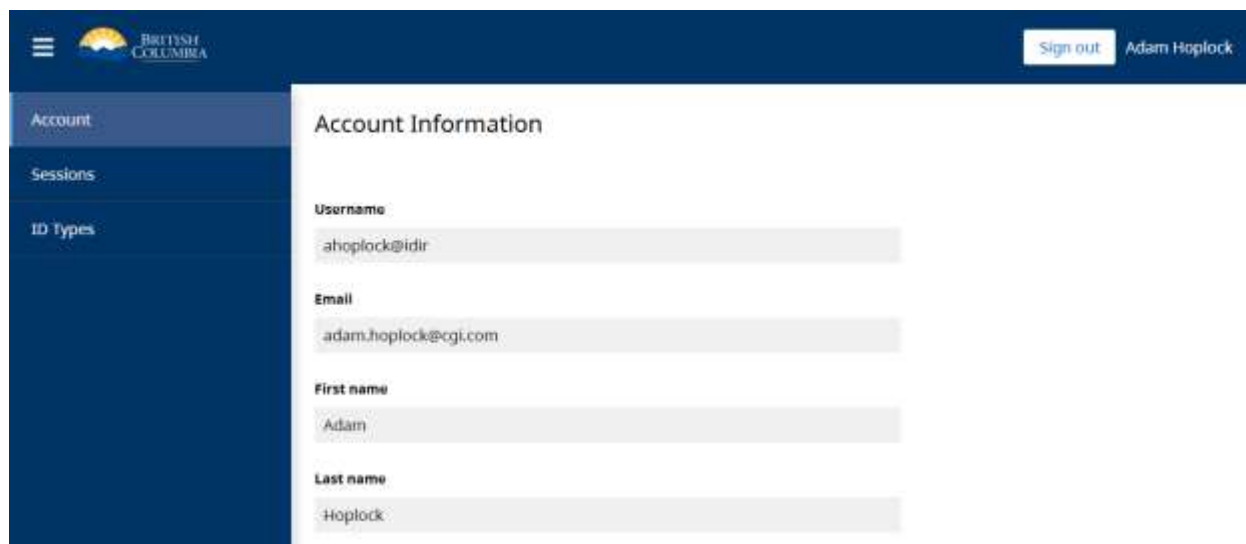
Keycloak Solution Components

The broader MoH Keycloak Authentication Service can be broken down into three different components:

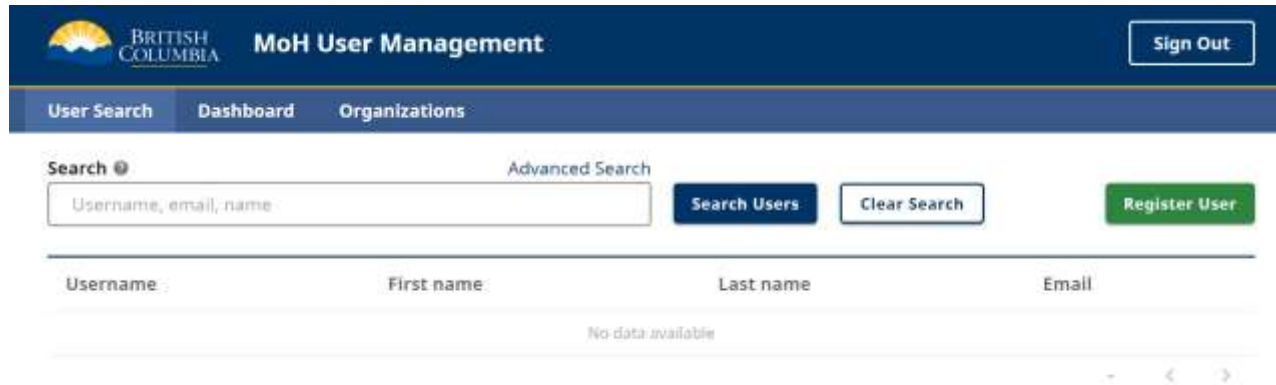
Keycloak Common Login Page. This can be configured for each application to align with what electronic IDs (e.g. IDIR, BCeID, BCSC etc.) are accepted for that specific application. The options available on the log in page may differ on an application-by-application basis or environment-by-environment basis.



Account Management Application. From this application, users can review contact info and add additional ID types to their account. This application is mainly used for diagnostic purposes and can be accessed via https://common-logon.hlth.gov.bc.ca/auth/realms/moh_applications/account/.



User Management Application. This is where the MoH Access Management Team and other support teams can manage users and their permissions and view logged audit events. This application consists of the User Management Console (UMC) frontend and the User Management Service (UMS) backend. This user guide details these pages, functions, and associated processes.



The screenshot shows the MoH User Management application interface. At the top, there is a dark blue header with the British Columbia Ministry of Health logo on the left, the text "MoH User Management" in the center, and a "Sign Out" button on the right. Below the header is a navigation bar with three tabs: "User Search" (selected), "Dashboard", and "Organizations". The main content area features a search section with a "Search" label, a text input field containing "Username, email, name", and a link to "Advanced Search". To the right of the input field are three buttons: "Search Users" (dark blue), "Clear Search" (white with blue border), and "Register User" (green). Below the search section is a table with four columns: "Username", "First name", "Last name", and "Email". The table is currently empty, displaying the message "No data available" in the center. At the bottom right of the table, there are three small navigation icons: a minus sign, a left arrow, and a right arrow.

User Management Application Overview

The User Management application is a custom purpose built Vue.js application that reads and writes information from the native Keycloak application that is installed and configured on ministry servers. The application was created to provide an enhanced user experience (over the native Keycloak application) and focuses on supporting the key tasks and processes related to user administration.

Access to User Management

Only support team members have access to the application. Individuals must have user accounts in Keycloak to be able to access the User Management application. The individuals should be assigned to the appropriate User Group for their Access Team to have the ability to access the User Management application and access the associated features. Before signing onto the User Management application, users should connect to the BC Government network via VPN if they are not signing on from the BC Government network.

If the application is down or an error has occurred, please get in touch with your organization's support team with your questions. If your organization does not have a support team supporting Keycloak applications, then please reach out to CGI VIC AMS Single Point of Contact (AMSSPOC.vic@CGI.com).

Application URLs

The URL in Test is: <https://user-management-test.hlth.gov.bc.ca/>

The Production URL is: <https://user-management.hlth.gov.bc.ca/>

There are currently three main tabs in the application:

1. User Search: Supports the creation, search, and update of Keycloak user information.
2. Dashboard: Allows executive users to view user metrics information.
3. Organizations: Supports search and creation of organizations.

Users Search Guide

The screenshot shows the 'MoH User Management' interface. At the top, there is a 'Sign Out' button. Below it, a navigation bar contains 'User Search', 'Dashboard', and 'Organizations'. The 'User Search' tab is active. Below the navigation bar, there is a search section with a 'Search' label, a search input field containing 'Username, email, name', and an 'Advanced Search' link. To the right of the input field are 'Search Users' and 'Clear Search' buttons. Further right is a green 'Register User' button. Below the search section, there is a table header with columns: 'Username', 'First name', 'Last name', and 'Email'. Below the header, it says 'No data available'.

Basic User Search

When doing a basic search, users can search by Username, Email, or Name. Note that Username is a combination of the ID followed by the '@' character and then the ID type (e.g. "msmith@idir"), except for Health Authority ID types where the ID is instead prefixed with their Windows domain (e.g. "@phsa"). The use of wildcard characters is not required.

Once search results are returned the user can sort ascending or descending on a column by clicking the arrow icon on each of the column headers. An example of the arrow that appears to sort when hovering on the column name is shown here:

The screenshot shows the 'MoH User Management' interface with search results for 'test'. The search input field contains 'test'. Below the search section, there is a table with columns: 'Username', 'First name', 'Last name', and 'Email'. The 'Username' column header is highlighted with a red box, and a red arrow points to it. The table contains two rows of results:

Username	First name	Last name	Email
jmeter1	JMeter	One	test@example.com
jmeter10	JMeter	Ten	test@example.com

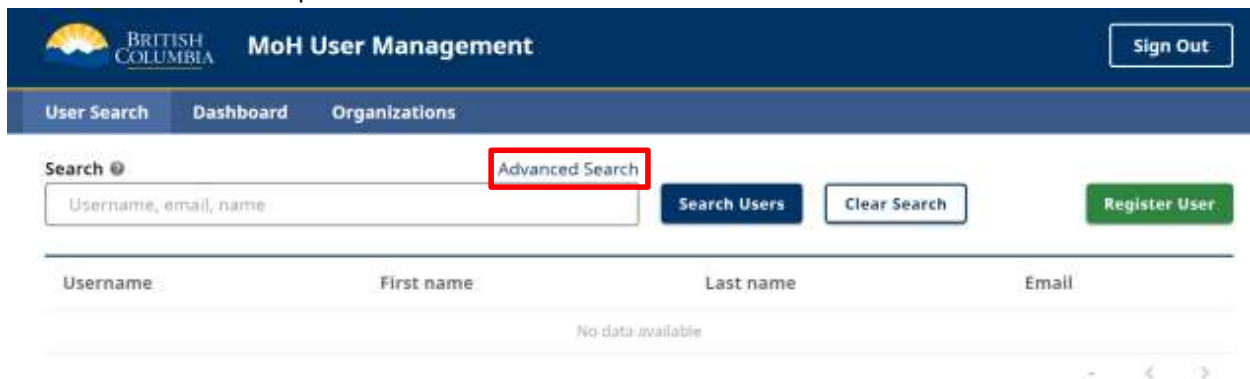
Search results can also be saved as a .csv file by clicking the 'Download results' button near the table pagination controls.

20811-test9	20811	Test9	noreply@localhost
2855-plrtest2	2855 Primary	Source	noreply@localhost

Download results
1-15 of 81

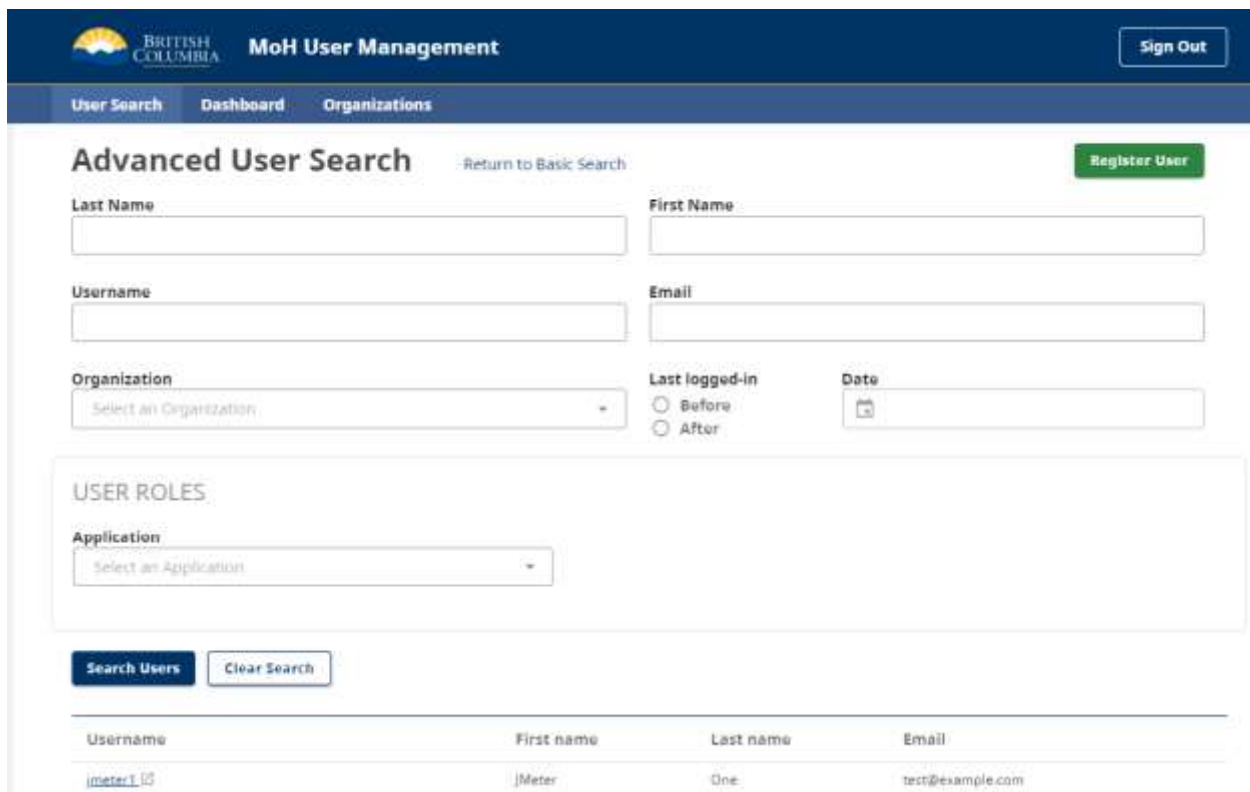
Advanced User Search

Advanced search is an option within the User Search tab.



The screenshot shows the 'MoH User Management' interface. At the top, there's a 'Sign Out' button. Below it, a navigation bar contains 'User Search', 'Dashboard', and 'Organizations'. The 'User Search' tab is active. A search bar contains the placeholder text 'Username, email, name'. To the right of the search bar, the 'Advanced Search' link is highlighted with a red box. Further right are buttons for 'Search Users', 'Clear Search', and 'Register User'. Below the search bar, a table header is visible with columns: 'Username', 'First name', 'Last name', and 'Email'. The table body shows 'No data available'.

When doing an advanced search, users can search by a variety of metrics. These include Last Name, First Name, Username, Email, Organization (this drop down select field has a searchable list to choose from), and User Roles by Application. You can also set the Last logged-in Date to Before or After a specific date for auditing purposes. Note that the date picker limits date selection to within 365 days from the current date, as Keycloak events are stored for one year by default.



The screenshot shows the 'Advanced User Search' form. At the top, there's a 'Sign Out' button. Below it, a navigation bar contains 'User Search', 'Dashboard', and 'Organizations'. The 'User Search' tab is active. The 'Advanced User Search' title is followed by a 'Return to Basic Search' link and a 'Register User' button. The form contains several input fields: 'Last Name', 'First Name', 'Username', 'Email', 'Organization' (a dropdown menu), 'Last logged-in' (radio buttons for 'Before' and 'After'), and 'Date' (a date picker). Below these fields is a section titled 'USER ROLES' with an 'Application' dropdown menu. At the bottom of the form are 'Search Users' and 'Clear Search' buttons. Below the form, a table header is visible with columns: 'Username', 'First name', 'Last name', and 'Email'. The table body shows a single row with the following data: 'jmeter1_02', 'jMeter', 'One', and 'test@example.com'.

Depending on which fields are populated in the Advanced User Search, it will determine what column headers are visible in the search results. The default search results headers are Username, First name, Last name, and Email. When the Last logged-in Date field is populated, the "Last Log Date," column header appears in the table below. When the User Roles field is populated, the "Role," column header

appears. In the User Roles section of the Advanced User Search, there is the ability to select applications from a list of available ones. Once one is selected, a checklist of the available user roles for the application appears. Some user roles have descriptions that can be viewed by hovering over the text.

Last Name

First Name

Username

Email

Organization

Select an Organization

Last logged-in

☒ Before
 ☐ After

Date

2022-12-05

×

USER ROLES

Application

FMDB

×

▼

Roles

☐ MOHUSER

The base user permission for FMDB

☐ PSDADMIN

Search Users

Clear Search

User Update Guide

This section outlines how to update user details, add/edit user roles, add/edit mailbox authorizations and update user groups.

Update User Details

Once search results are returned a user can click on a returned result to access the User Details screen.

The screenshot shows the 'User Search' interface. At the top, there are tabs for 'User Search', 'Dashboard', and 'Organizations'. Below the tabs is a search bar with the text 'test' and a 'Search Users' button. To the right of the search bar is a 'Clear Search' button and a 'Register User' button. Below the search bar is a table with the following columns: Username, First name, Last name, and Email. The table contains three rows of search results. The first row has the username 'jmeter', first name 'JMeter', last name 'One', and email 'test@example.com'. A red box highlights the 'jmeter' username, and a red arrow points to it. The second row has the username 'jmeter10', first name 'JMeter', last name 'Ten', and email 'test@example.com'. The third row has the username 'jmeter2', first name 'JMeter', last name 'Two', and email 'test@example.com'.

The following fields are available for update:

Name	Required	Comment
Username	Yes	Read-only; Combination of the ID followed by the '@' character and then the ID type (e.g. IDIR), except for Health Authority ID types where the ID is instead prefixed with their Windows domain (e.g. "@phsa").
First Name	Yes	
Last Name	Yes	
Email Address	Yes	Basic validation exists
Telephone Number	No	
Organization	No	This comes from a prepopulated list of parent organizations extracted from LDAP. CGI must be contacted to add a new organization at this time.
Notes	No	

From this screen, users with certain permissions can reset the Identity Provider Link by clicking the icon next to the specified Linked Identity Type, which should resolve "Account already exists" errors that users sometimes encounter in Keycloak (see Appendix A: User Already Exists for more details). Users should click the 'Update User' button to save any changes to the User Details section.

Update - 14734-test1

USER DETAILS

Username *

14734-test1

First Name *

14734

Last Name *

Test 1

Email Address *

noreply@localhost

Telephone Number

Organization

Notes

Update User

Linked Identity Types

MoH LDAP [14734-test1]



Reset Identity Provider Link

Add/Edit User Roles

The User Roles section is where access to applications and associated roles are managed. The Application drop down menu includes all of the applications that are available to grant a user access to. Once the application is highlighted the available Roles for that application will appear.

Edit User Role

Application *
PLR_IAT

Roles

- ☒ CONSUMER
- ☐ DSR_USER
- ☐ MOH_APPROVER
- ☐ PRIMARY_SOURCE
- ☐ REG_ADMIN
- ☐ SECONDARY_SOURCE

Effective roles represent all roles assigned to a user for this client. This may include roles provided by group membership which cannot be directly removed.

Save User Roles Cancel

Administrators can select a Role for the user and click the 'Save User Roles' button to save any changes. Administrators can also select an application and then remove any assigned roles for that user which will effectively remove that user's access to the selected application.

Effective Roles are typically associated with a group application (e.g. being part of the access team group in Keycloak) and cannot be individually removed. Removal from the associated group will remove these Effective Roles.

Add/Edit Mailbox Authorizations

The Mailbox Authorization section is present only if the user has an assigned role with specific applications (currently SFDS and HSCIS). If it's present, there's the ability to add a Mailbox Authorization, which requires the following information.

Add Mailbox Authorization

Mailbox *

A mailbox is required

Use *

At least one use is required

Permission *

get
send
get-send
get-delete
get-send-delete

Save Mailbox Authorization

Cancel

Update User Groups

Depending on the role that users have, they may be able to assign/revoke all groups or only existing groups. When hovering over the User Group, a description tooltip appears to describe the abilities for administrators within that group.

USER GROUPS

☐ CGI Developer
☐ CGI Midtier
☒ CGI QA
☐ CGI Registries
☐ EMCCD Access Team
☐ HIBC Access Management
☐ ITSB Access Team
☐ MAID Access Management
☐ PIDP Management
☐ Primary Care Access Team
☐ Registries Admin
☐ Registries Connections Team
☐ WebCAPS User Admin

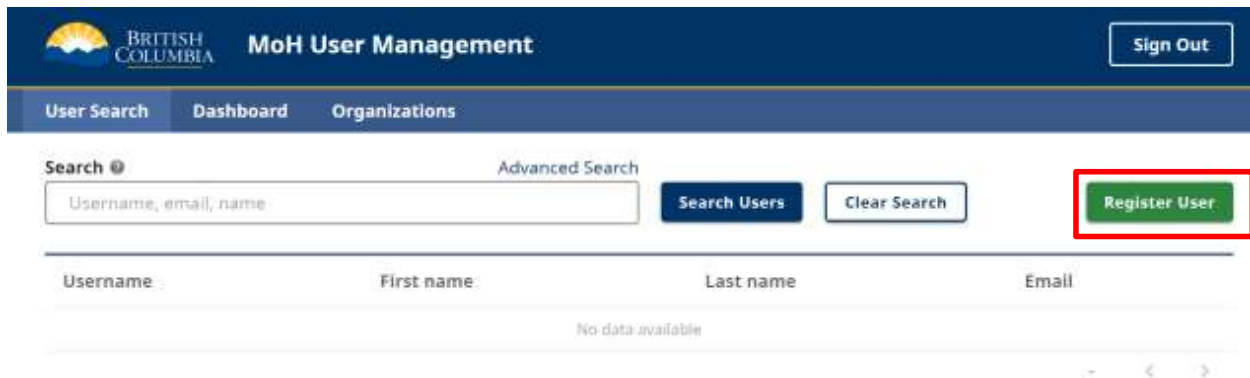
As a member of MAID Access Management group, an administrator is able to:

- Manage user groups, roles.
- Manage maid.
- View users, groups.

Save User Groups

Register New User

A new user can be registered from the Users tab by clicking the 'Register User' button.



The screenshot shows the 'MoH User Management' interface. At the top, there is a header with the British Columbia Ministry of Health logo and a 'Sign Out' button. Below the header is a navigation bar with 'User Search', 'Dashboard', and 'Organizations' tabs. The 'User Search' tab is active. In the search area, there is a search bar with the placeholder text 'Username, email, name', a 'Search Users' button, a 'Clear Search' button, and a 'Register User' button which is highlighted with a red box. Below the search area is a table with columns for 'Username', 'First name', 'Last name', and 'Email'. The table is currently empty, displaying 'No data available'.

The process for registering a user is as follows:

1. Click the 'Register User' button
2. Enter required User Details information and click 'Register User'

Note: Rules for populating the User Details are the same as what is described above in the User Updates section. A tooltip with rules surrounding how to populate the Username field is pictured.

3. Once the User has been created successfully then permissions to applications can be assigned in the User Roles section

Note: Process for assigning User Roles is same as described in section on Updating User Roles above.

USER DETAILS

Username * @

First Name *

Last Name *

Email Address *

Telephone Number

Organization

Notes

Register User

Username should include the corresponding prefix or suffix in alignment with the id type.
 IDIR: username@idir
 Business BCeID: username@bcid_business
 BC Provider: username@bcpr
 Note: The username will already contain an '@domain' that the '@bcpr' will be appended to.
 BC Services Card: username@bsc
 PHIA: username@phsa
 Note: The username will already contain an '@domain' that the '@phsa' will be appended to.
 Health Authority ID: username@phsa
 Note: The username will already contain an '@domain' that the '@phsa' will be appended to.
 This applies to all Health Authority users, for example: username@interiorhealth.ca@phsa or username@phsa.ca@phsa

Error Messages Related to Manual Registration of New User

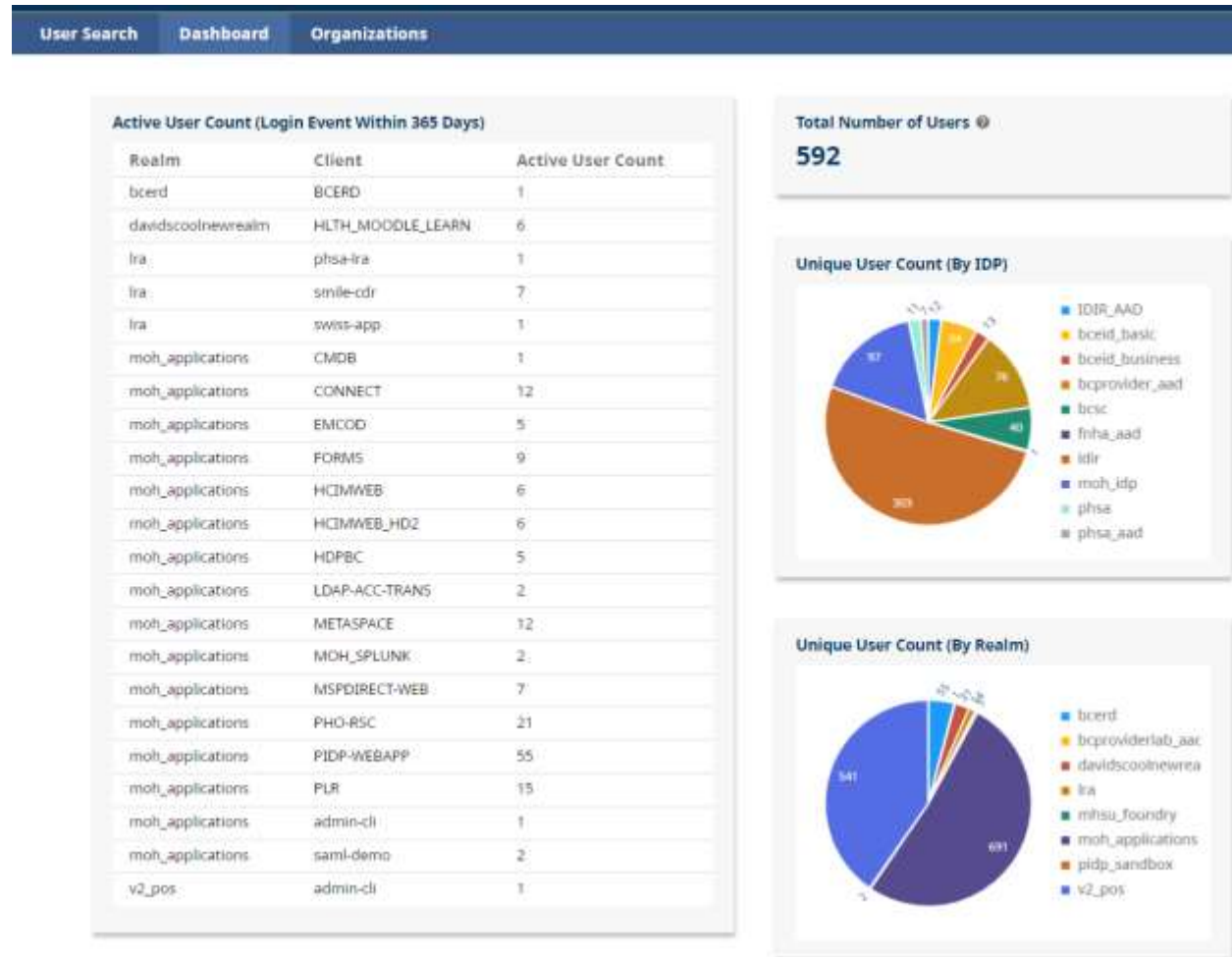
If an administrator tries to register a user with a username that already exist in Keycloak.

 Error creating new user: Request failed with status code 409. User already exists.
 

If there are connection issues between the UMC frontend and the UMS backend (e.g. UMS is down). A variation of the following errors may appear when registering a new user. This indicates communication issues between the frontend and backend of the UMC application. If the error persists, please reach out to the MoH Access Management Team (CA.AM.MoHAccessManagement@cgi.com).

 Error creating new user: Network Error
 

Dashboard Page Guide



Active User Count

The active user count reflects the number of Login Events within 365 days. The information within this table includes the Realm, Client, and Active User Count. This table has a hover feature whereby some Realms/Clients have additional available information on them if you hold your cursor over the text. An example of this is in the screenshot below.

moh_applications	MIWT_STG	28
moh_applications	The Medical Imaging Wait Times application allows the Ministry of Health (MoH) to track the wait times for various medical imaging procedure at different facilities in BC.	9
mohsu_foondry		2
idir		14
moh_applications	MAID	16

User Metrics

Total Number of Users

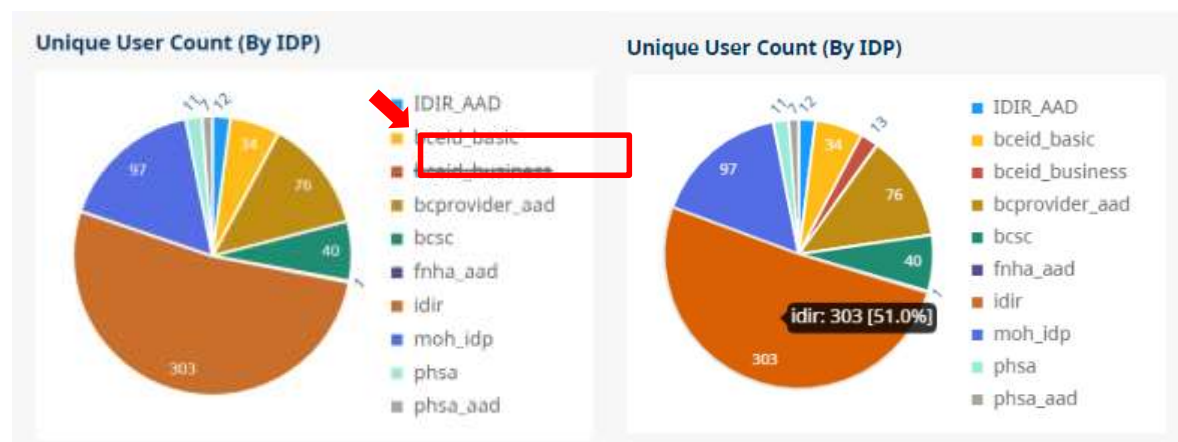
The total number of users displays the total unique User Count by IDP and MHSU Realms that do not use an IDP. The (?) icon displays a tooltip to inform the end user of where the aggregated number comes from. This metric considers duplicate users across overlapping IDPs (e.g. idir and idir_aad) which explains why it may not add up exactly to the "Total Unique User Count by IDP + MHSU Realms" that its tooltip suggests.



Unique User Counts

The unique user count pie charts are configured so that the end user can customize them. The Unique User Count (By IDP) chart describes the total amount of unique users for each Identity Provider (IDP) used by Keycloak. This metric does not account for users with multiple credentials across multiple IDPs. The Unique User Count (By Realm) depicts the total amount of unique users across each application realm configured in Keycloak.

These interactive charts allow you to strike out variables to configure the chart. By clicking on an item in the legend, it removes or adds that group to the corresponding chart.



The chart has a hover feature that enables the end user to drill down into the specific percentage results by holding the cursor over the slice of the chart. This is depicted in the following screen clipping. The charts can be easily copy and pasted to be used as artifacts.

Organizations Page Guide

Certain users have access to the Organizations tab in the User Management Console. Access to this is limited to specific teams and requires permission.

Organizations are not used by all applications. In the past, some applications that used the legacy LDAP solution. Users were stored in LDAP and grouped together into organizations. Some applications still use organizations to manage access to various applications. In this case, it uses attribute-based access.

Organization Search

Organizations can be searched by the organizations name, or by the ID number.

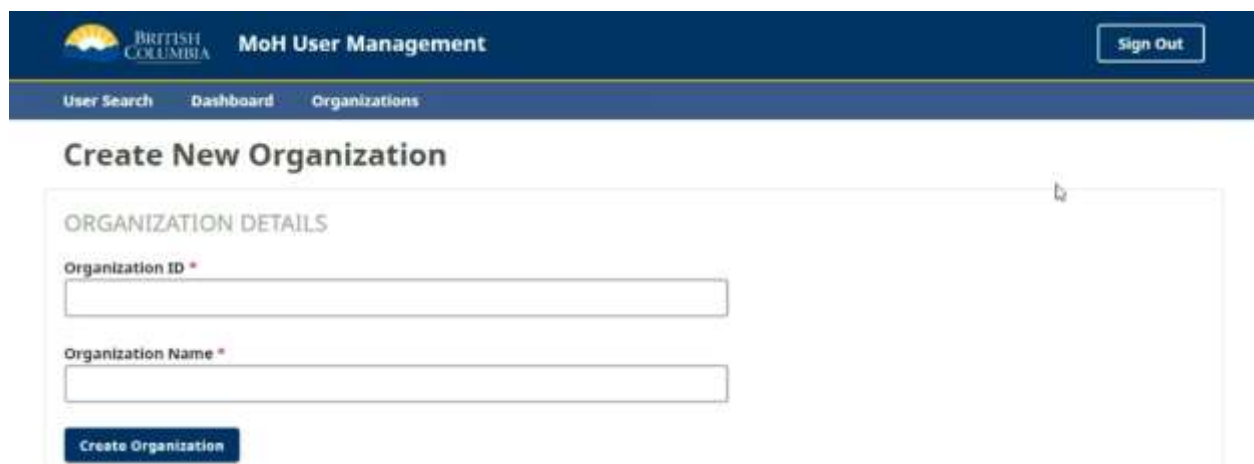
Similar to other display screens in the UMC, the results can be sorted by hovering over the 'ID' or 'Name' header and clicking the arrow icon beside the header.



ID	Name
00000010	Ministry of Health
00002855	PRS BCMOH - Registry Administrator

Create Organization

The green "Create Organization" button at the top right of the screen allows certain users with the appropriate permissions to add / edit organizations.



Organization ID *

Organization Name *

Create Organization

Organization Name and ID are required fields. The organization ID must be 8 numerical characters. Confirm the organization was created successfully by searching for it by name or ID.

Appendix A: User Already Exists

Basic BCeID, BCSC, IDIR, and Health Authority IDs have a tendency to be recreated when employees return after a leave of absence resulting in a new GUID that will not match what was previously in Keycloak the next time they log in. If this occurs, this will result in the user seeing one of the following errors:

"Account already exists"

"User with email <email> already exists. How do you want to continue?"



To resolve this through the UMC for all IDPs except Basic BCeID, log into the UMC, search for the affected user, navigate to their details and click the Reset Identity Provider Link icon next to the affected Linked Identity Type:

Linked Identity Types

- bceid_business [test_username]  [Reset Identity Provider Link](#)