|  |  |
| --- | --- |
| MoH Keycloak | |
| User Management Console – Training Guide | |
| CGI Ministry of Health  Date: 2024-09-20 |  |

1. **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 |
| 1.6 | September 20, 2024 | Filip Florek | Update content for UMC |

1. **Referenced or Related Documents**

|  |  |
| --- | --- |
| Document Title | Description / Location |
|  |  |
|  |  |
|  |  |

**Table of Contents**

[MOH Keycloak Solution 4](#_Toc177729812)

[Document Purpose 4](#_Toc177729813)

[Background 4](#_Toc177729814)

[Keycloak Solution Components 5](#_Toc177729815)

[User Management Application Overview 7](#_Toc177729816)

[Access to User Management 7](#_Toc177729817)

[Application URLs 7](#_Toc177729818)

[Users Search Guide 8](#_Toc177729819)

[Basic User Search 8](#_Toc177729820)

[Advanced User Search 9](#_Toc177729821)

[Bulk Removal of User Permissions via Advanced Search 10](#_Toc177729822)

[User Update Guide 11](#_Toc177729823)

[Update User Details 11](#_Toc177729824)

[Add/Edit User Roles 12](#_Toc177729825)

[Add/Edit Mailbox Authorizations 13](#_Toc177729826)

[Update User Groups 14](#_Toc177729827)

[Register New User 15](#_Toc177729828)

[Error Messages Related to Manual Registration of New User 16](#_Toc177729829)

[Dashboard Page Guide 17](#_Toc177729830)

[Active User Count 17](#_Toc177729831)

[User Metrics 17](#_Toc177729832)

[Total Number of Users 18](#_Toc177729833)

[Unique User Counts 18](#_Toc177729834)

[Organizations Page Guide 19](#_Toc177729835)

[Organization Search 19](#_Toc177729836)

[Create Organization 19](#_Toc177729837)

[Appendix A: User Already Exists 21](#_Toc177729838)

# 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.

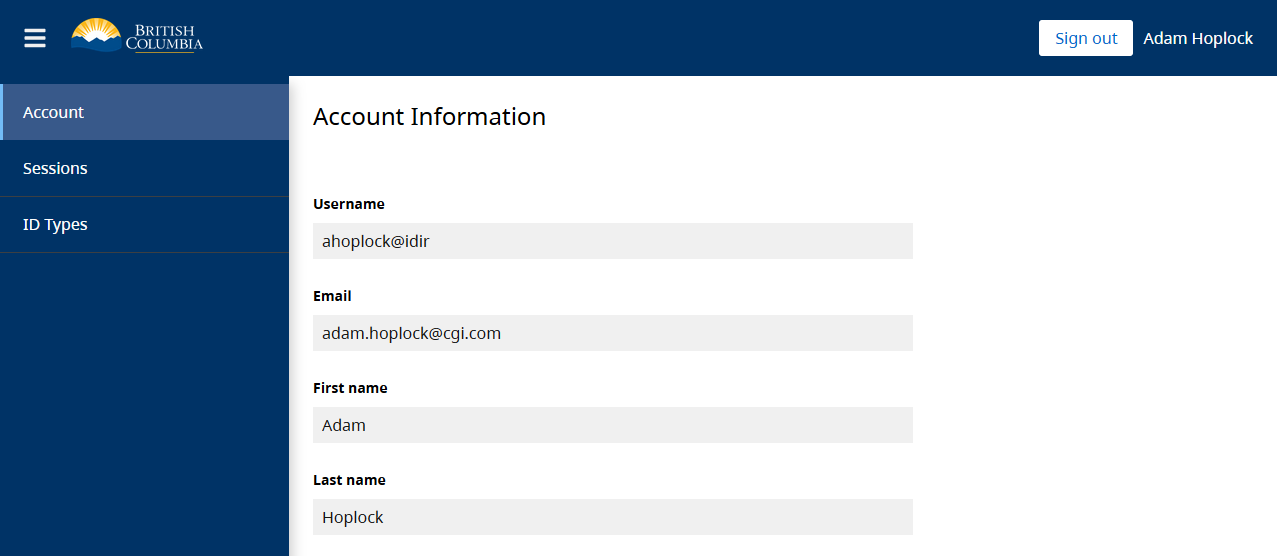
## Keycloak Solution Components

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.

A screenshot of a login screen

Description automatically generated

**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.

**A screenshot of a computer screen

Description automatically generated**

# 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](mailto: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

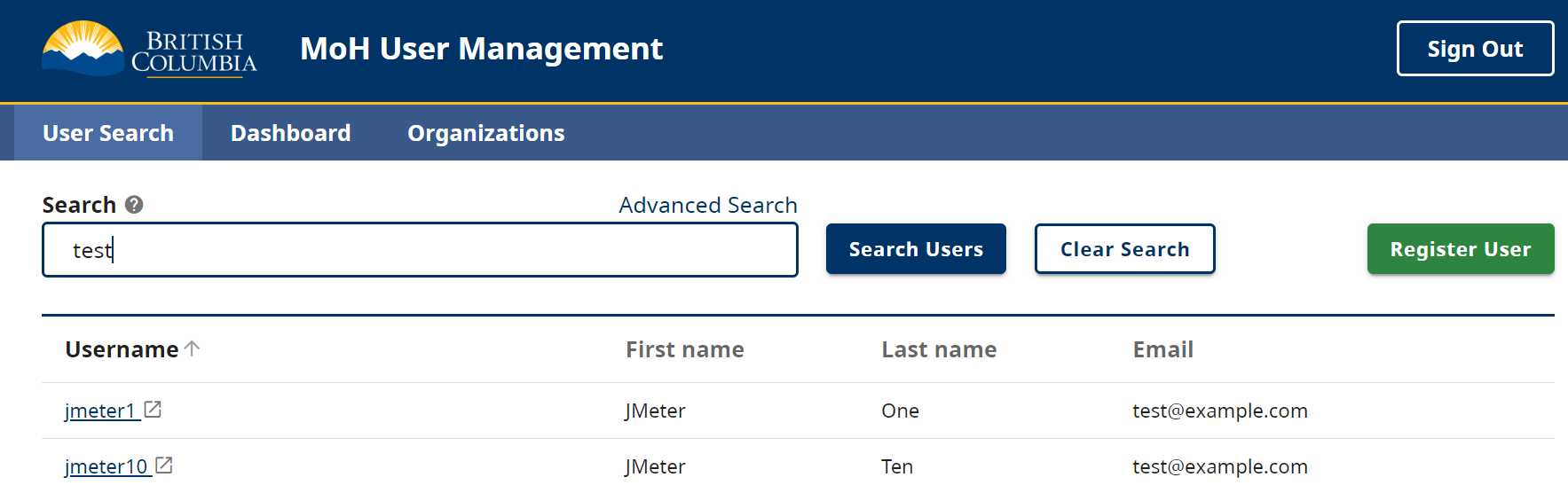
A screenshot of a computer screen

Description automatically generated

## 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:



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

A white background with black text

Description automatically generated

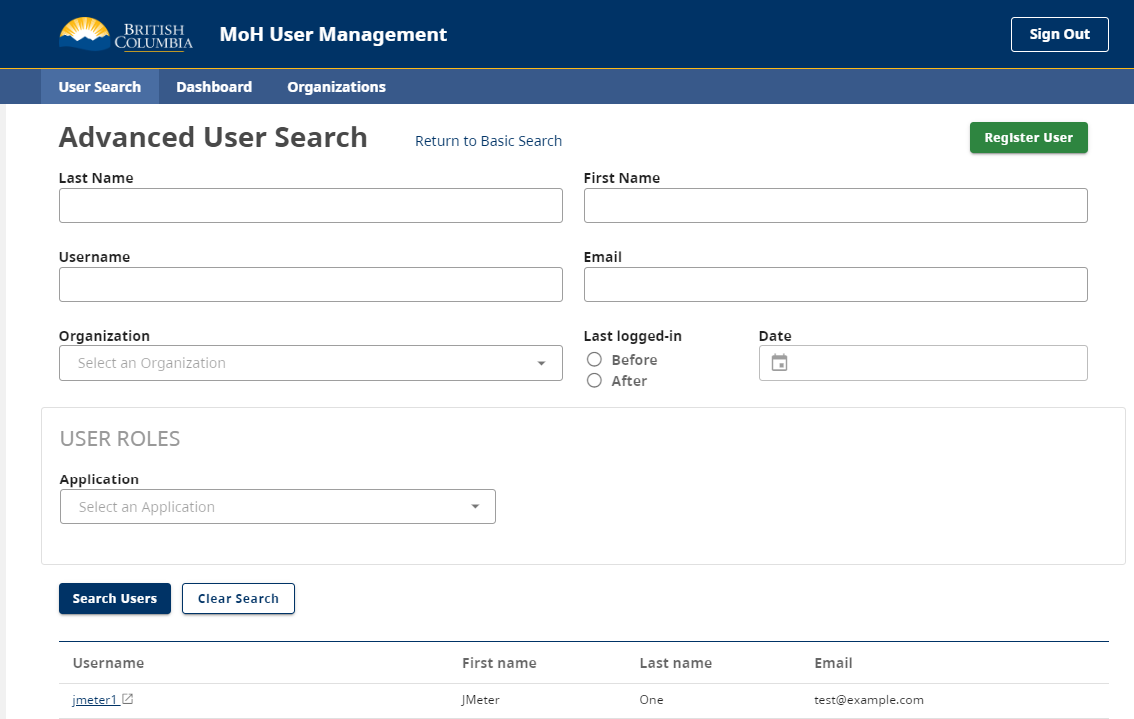
## Advanced User Search

Advanced search is an option within the User Search tab.

A screenshot of a computer screen

Description automatically generated

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.



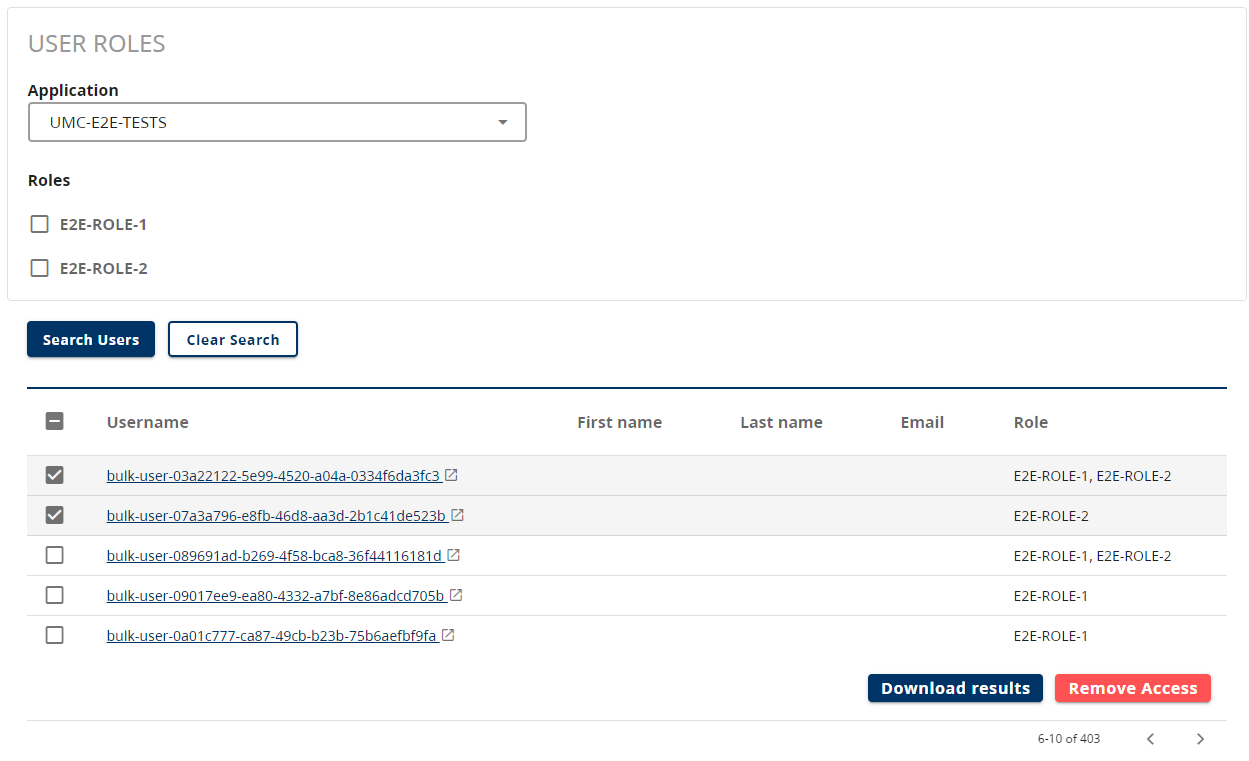
Depending on which fields are populated in the Advanced User Search, it will determine what column headers are visible in the search results. The default search results headers are Username, First name, Last name, and Email. When the Last logged-in Date field is populated, the “Last Log Date,” column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

A screenshot of a computer

Description automatically generated

## Bulk Removal of User Permissions via Advanced Search

The Advanced Search feature allows administrators to bulk-remove user permissions. To use this feature, the administrator must search for users with specific roles in a given application. If the administrator has the necessary permissions to perform bulk removals, a **Remove Access** button will be displayed.



The administrator can either select all users from the search results or choose individual accounts. Upon clicking **Remove Access** a confirmation dialog will appear, displaying the following information:

* The name of the application (in this case UMC-E2E-TESTS)
* For each selected user, the username and the roles that will be removed.

A screenshot of a computer

Description automatically generated

After reviewing, the administrator can confirm the action, and a status message will be displayed next to each user to indicate success or failure.

A screenshot of a computer

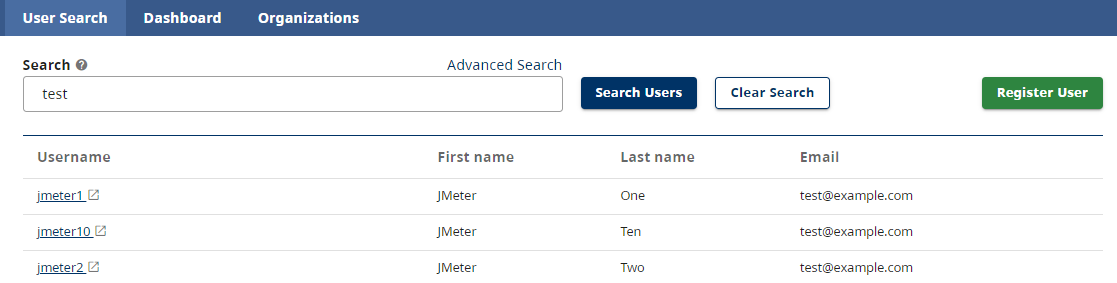
Description automatically generated

# 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 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 2: User Already Exists for more details). Users should click the ‘Update User’ button to save any changes to the User Details section.

A screenshot of a computer

Description automatically generated

### 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.

A screenshot of a computer

Description automatically generated

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.

A screenshot of a computer

Description automatically generated

### 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.

A screenshot of a survey

Description automatically generated

## Register New User

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

**A screenshot of a computer screen

Description automatically generated**

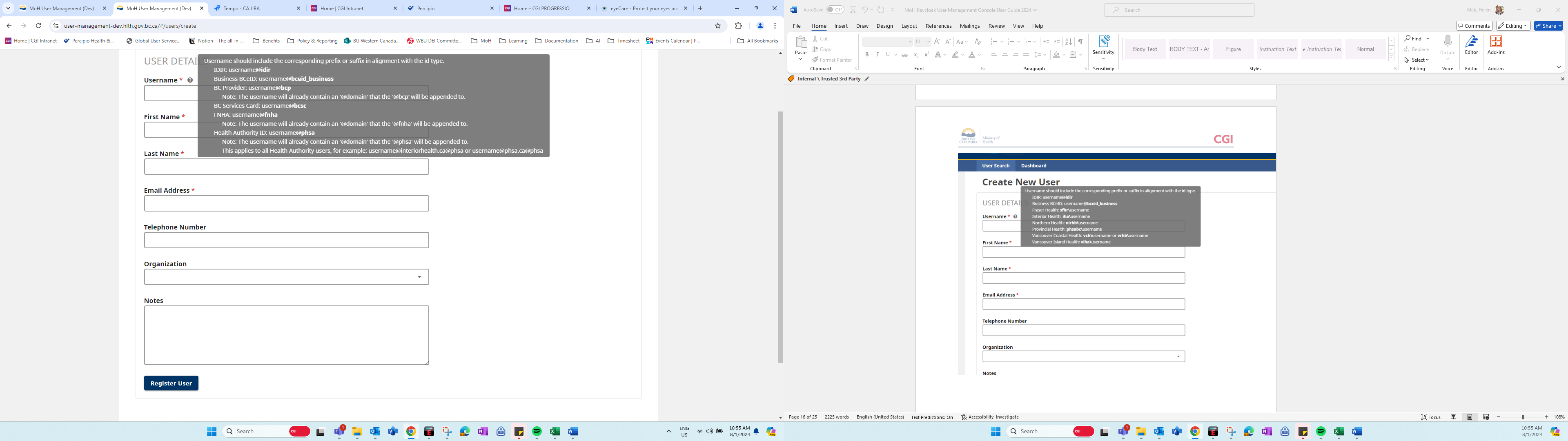
The process for registering a user is as follows:

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.

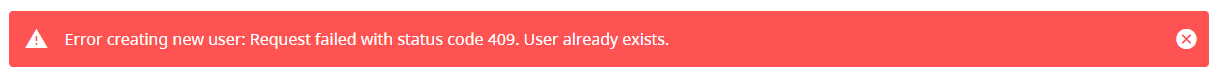
1. Once the User has been created successfully then permissions to applications can be assigned in the User Roles section

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



### Error Messages Related to Manual Registration of New User

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

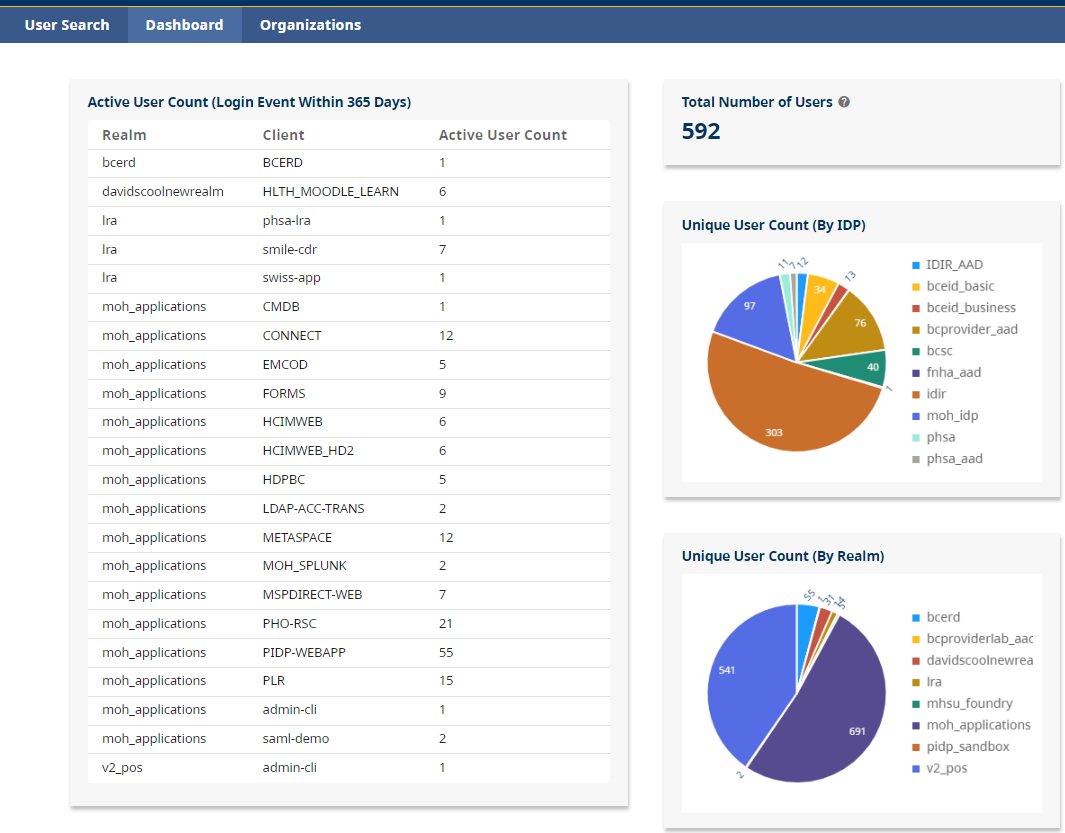


If there are connection issues between the UMC frontend and the UMS backend (e.g. UMS is down).

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](mailto:CA.AM.MoHAccessManagement@cgi.com)).



# 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.

A screenshot of a computer

Description automatically generated

## 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.

A grey box with white text

Description automatically generated

### 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. A pie chart with numbers and text

Description automatically generated

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.

A screenshot of a computer

Description automatically generated

# 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.

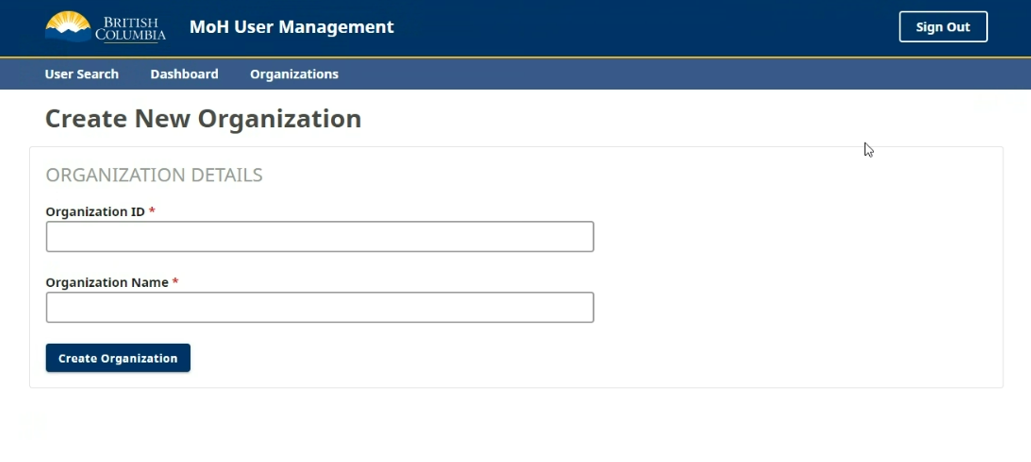
Similar to other display screens in the UMC, the results can be sorted by hovering over the ‘ID’ or ‘Name’ header and clicking the arrow icon beside the header.

A screenshot of a computer

Description automatically generated

## 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 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?"

A screenshot of a computer

Description automatically generated  
or  
  
"Account already exists"  
"User with username <username> already exists. How do you want to continue?"

A screenshot of a computer

Description automatically generated

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:

A close up of a symbol

Description automatically generated