Centers for Medicare & Medicaid Services
CMS eXpedited Life Cycle (XLC)

Identity Management (IDM)

User Guide

Version 1.01

06/01/2021

Document Number: IDM User Guide Version 1.01

Contract Number: HHSM-500-2017-00015I TO HHSM-500-T0001

Note: Working copy versions delivered to the client for review will be published as a major version. The client has agreed to review these documents as follows: as-is, ongoing, “work-in-progress” drafts and working copy versions.

Table of Contents

List of Figures

List of Tables

1. Introduction

The Centers for Medicare & Medicaid Services (CMS) is a federal agency that ensures health care coverage for more than 100 million Americans. CMS administers Medicare and Medicaid and provides funds and guidance for all of the 50 states in the nation, for their Medicaid programs, and Children’s Health Insurance Program (CHIP). CMS works together with the CMS community and organizations in delivering improved and better coordinated care.

1.1 Identity Management (IDM) System Overview

CMS created the IDM System to provide Business Partners with a means to request and obtain a single User ID which they can use to access one or more CMS applications. The IDM System uses a cloud-based distributed architecture that supports the needs of both legacy and new applications while providing an improved user experience on desktop and laptop computers as well as tablet and smartphone mobile devices.

1.2 User Guide Purpose

This user guide provides step-by-step instructions for performing the most common tasks using the IDM System. The tasks a user can perform varies depending on their role and includes, but is not limited to, creating an account, logging in to the IDM System, requesting a role, identity proofing, managing role requests, performing account management functions, and generating reports.

1.3 Application (Tier 1) Help Desk Support

Application Help Desk contact information is located on the CMS Tier 1 Help Desk Support website.

Note: When the IDM System experiences a planned or unplanned outage, application login services continue to function normally, however new user registration, role request and account management services will not be available. If an outage exists, the system will display a message that informs users about the outage and where they can obtain additional information.

2. Prepare to Access the IDM System

Users who access the IDM System using a desktop or laptop computer may need to perform software updates or configure web browser settings and privacy settings. Users who access the IDM user interface (UI) with a mobile computing device such as a smartphone or tablet generally have less control over updates and privacy settings. The procedures discussed in this section may not apply to mobile device users.

2.1 Verify the Web Browser is Supported

The IDM UI was tested for compatibility with current versions of the following modern web browsers:

- Microsoft Edge (Legacy) [1]
- Microsoft Internet Explorer (IE 11)
- Google Chrome
- Mozilla Firefox
- Safari

All of the web browsers listed above are configured by default to receive regular security updates and patches. Even in cases where the user's organization manages operating system and application software updates, users who access the IDM System UI with one of these web browsers should not encounter compatibility issues.

2.2 Verify and Adjust the Screen Resolution if Necessary

The IDM System UI is best viewed on a display resolution of 1366 x 768. Many modern desktop, laptop, and mobile computing devices have default display settings that exceed the IDM System minimum. If adjustments are necessary, use the display settings adjustment procedure that is appropriate for your device.

2.3 Review Account Creation Instructions

All users should receive account creation instructions from their organization or their CMS contact prior to creating an account on the IDM System. Not every CMS application requires the same information, so it is important for the user to review any instructions that were provided by their organization or CMS contact before starting the account creation process.

[1] Microsoft Edge (Legacy) is the default web browser on Windows 10 PCs, and many users still have this as their default web browser. The New Microsoft Edge browser was released on January 15, 2020 and it was installed automatically for some users as part of Windows 10 updates.

3. Overview of the IDM System

The following terms are introduced in this section:

- **Role** - A name, usually a function or title, given to a collection of access privileges or permissions within an application. A role defines what the user is allowed to do by virtue of having been assigned or granted that role. Each application defines the access privileges and permissions assigned to each role. For example, "Submitter" could identify a role that has permission to upload documents to an application.
- **Role Attribute** - A characteristic of a role that represents a functional limitation or additional information that modifies the scope of that role's access privileges. For example, a submitter with the role attribute of Maryland might only be permitted to upload documents to a specific folder relevant to the State of Maryland.

The IDM System provides the means for users to be approved for access to many other CMS systems and applications. IDM governs access to CMS systems by managing identity proofing, the creation of User IDs and passwords, and setting up multi-factor authentication (MFA). It also enables users to manage roles within CMS applications. IDM generally supports three types of users along with their most common features or functions:

Application End Users:

- Create an account, sign in to IDM, request a role, modify or remove a role, perform identity proofing, sign in to an application, manage their profile, and perform self-service functions such as recover a forgotten User ID, reset a forgotten password, reset an expired password, and unlock account.

Application Approvers:

- In addition to End User functions, they approve or reject role requests. Some application approvers may also be granted the capability to reset passwords and unlock accounts for users under their management.

Application (Tier 1) Help Desk Users:

- In addition to End User functions, they search and view accounts and user account details, reset passwords, unlock accounts, suspend a user's account, and update a user's email address. Some Application (Tier 1) Help Desk users may also be granted the capability to approve and reject requests for application approver roles; and to update a user's Level of Assurance (LOA).

IDM (Tier 2) Help Desk Users:

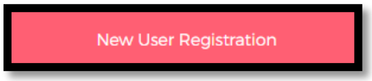
- In addition to the functions performed by all other types of users, they can also create user audit reports, role audit reports, and unsuspend a user's account.

4. How to Create a New User Account

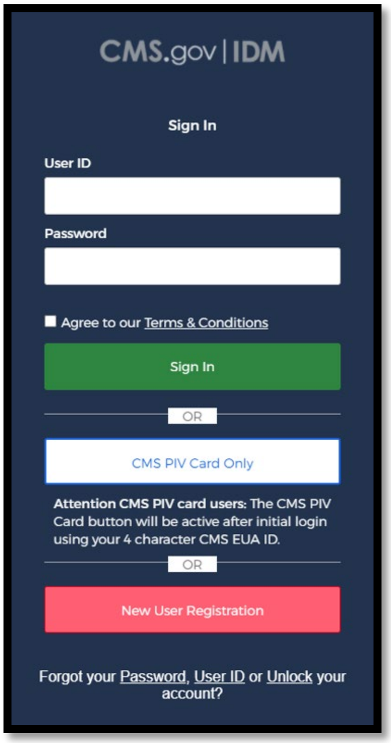
The following terms are introduced in this section:

- **Security Question and Answer (SQA) -** The security question is a question to which the user provides a unique answer. They both become part of the user's account and are used to authenticate the user when they access IDM's self-service functions.
- **User Account -** A user account generally refers to the User ID and all profile information that is associated to it. The user account does not refer to roles within the account.

Users create a new user account using the ***New User Registration*** button located on the Sign In window.



1) Navigate to https://home.idm.cms.gov/. The Sign In window appears.


CMS.gov | IDM
Sign In
User ID
Password
□ Agree to our Terms & Conditions
Sign In
OR
CMS PIV Card Only
OR
New User Registration
Forgot your Password, User ID or Unlock your account?

Attention CMS PIV card users: The CMS PIV Card button will be active after initial login using your 4 character CMS EUA ID.

Figure 1: IDM System Sign In Window

2) Click the ***New User Registration*** button. The User Registration window appears.
3) Enter the **First Name** and **Last Name**. Middle Name and Suffix are optional.
4) Enter the **Date of Birth**.
5) Enter the **E-mail Address** and the **Confirm E-mail Address**. The Email Address and the Confirm E-mail Address must match. Please ensure that the email address is valid because the IDM System uses email to communicate with users for many reasons including sign-in, security, and self-service.
6) Click the ***View Terms & Conditions*** button. Read the IDM System terms and conditions then click the ***Close Terms & Conditions*** button.

7) Click the checkbox to acknowledge agreement with the terms and conditions, then click the ***Next*** button. The User Contact Information window appears.

8) If the home address is outside the 50 U.S. states or the U.S. territories, select the ***Foreign Address*** radio button.

9) Enter the **Home Address**, **City**, **State**, **Zip Code** and **Phone Number**.

10) Click the ***Next*** button. The User Account Credentials window appears.

11) Enter the desired **User ID**, **Password** and **Confirm Password**. The Password and Confirm Password must match. [2]

12) Select a **Security Question** from the list.

13) Type the security question answer into the ***Answer*** dialog box.

14) Click the ***Submit*** button to submit the account registration request. The system will display a message that indicates the account was successfully created.

15) Click the ***Return*** button. The screen refreshes and the IDM System Sign In window appears.

Note: CMS policy requires that the combination of each user's first name, last name, and email address be unique in the IDM System. If an error occurs for this combination it may mean that the combination of information entered is already in use. Users should try entering the information again or call their Application Help Desk for assistance.

[2] Passwords must conform the guidance provided in **Appendix A: Password Policy**.

5. How to Sign In

The following terms are introduced in this section:

- **Multi-factor Authentication (MFA) -** MFA is an additional layer of security that functions as a “second” password. It is transmitted as a numeric code to the user’s email or phone and is good for one sign-in only. Some roles in IDM require MFA while others may not. See **Section 10 How to Manage MFA and Recovery Devices** for more information about MFA.

Note: CMS Enterprise User Administration (EUA) account holders may use their Personal Identity Verification (PIV) card. See the procedure in **Section 5.2 How to Sign In with a PIV Card (CMS EUA Users Only)** to sign in to the IDM System.

Note: New users who are required to log in with MFA will be required to set up an MFA device the first time they sign in to the IDM System. All users are encouraged to add additional MFA devices using the procedures described in **Section 10 How to Manage MFA and Recovery Devices**.

Note: The **Session Expiring** window appears if a user is logged in to IDM but has been inactive for 28 minutes. If the user clicks the ***Continue Session*** button, their session will be extended for another 30 minutes. If the user clicks the ***Logout*** button, they will be immediately logged out. If the user does nothing, they will automatically be logged out of the IDM System after 30 minutes of inactivity.

5.1 How to Sign In (All Users)

Use the following procedure to sign in.

1) Navigate to https://home.idm.cms.gov The Sign In window appears as illustrated by **Figure 1: IDM System Sign In Window**.
2) Enter the User ID and Password.
3) Read the Terms & Conditions, click the checkbox to acknowledge agreement, and then click the ***Sign In*** button. The Verification Code Request window appears. [3]

[3] The ***Set Up Multifactor Authentication*** window appears for users who are required to use MFA but have not yet configured it. It allows users to activate one or more MFA devices.

4) Click the ***Send me the Code*** button. The screen refreshes and the Code Request window appears. [4]

5) Enter the Verification Code. [5]

6) (Optional) Click the checkbox to select the option "*Do not challenge me on this device for the next 30 minutes*". If the checkbox is selected, users will bypass the MFA verification if they sign out and sign back into the system again within 30 minutes of their initial sign-in.

7) Click the ***Verify*** button. The IDM Self Service Dashboard appears. Go to **Section 5.3 The IDM Self Service Dashboard at a Glance** for a brief description of the IDM Self Service Dashboard.

Note: Users whose accounts where migrated from the legacy Enterprise Identity Management (EIDM) System or whose accounts where uploaded with a new application should update the answer to their security question using the procedures in **Section 11.6 How to Change the User Security Question and Answer**.

Note: It is recommended that all users add additional MFA and/or Recovery devices using the procedures in **Section 10 How to Manage MFA and Recovery Devices**.

5.2 How to Sign In with a PIV Card (CMS EUA Users Only)

The following terms are introduced in this section:

- **Personal Identity Verification (PIV) -** A PIV credential is a US Federal government credential that is used to access Federal government controlled facilities and information systems as assigned.

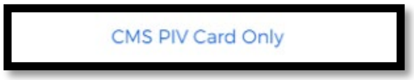
Before using the PIV button on the IDM Sign In page, EUA users must first sign in one time with their four character EUA ID and their password using the procedure in **Section 5.1 How to Sign In (All Users)**.

After a successful sign-in with an EUA ID and password, the ***CMS PIV Card Only*** button will be available to enable subsequent sign-ins using the procedure below:

[4] Users who have multiple MFA devices registered to their profile can choose which one they wish to use. The method used to deliver the verification code may vary based on the user's chosen MFA device.

[5] Users who have multiple MFA devices should follow the directions for the MFA device they have chosen to use. If the MFA device uses push notifications, a verification code is not required.

1) Click the checkbox to acknowledge agreement with the terms and conditions.

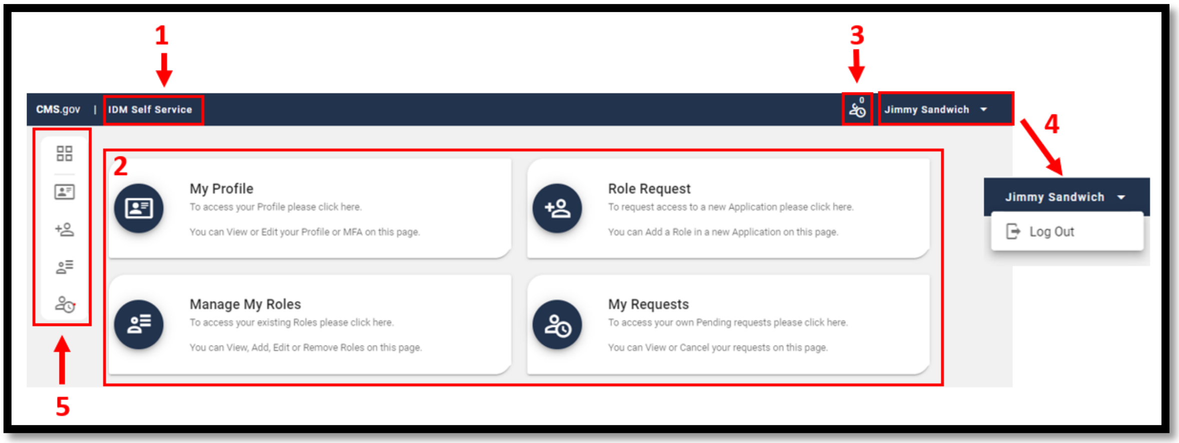


CMS PIV Card Only

2) Click the ***CMS PIV Card Only*** button.
3) Follow the prompts. The IDM Self Service Dashboard appears after the user is authenticated.

5.3 The IDM Self Service Dashboard at a Glance

The IDM Self Service Dashboard provides access to functions that allow users to manage their user profile, request new applications, and manage roles for applications to which they have been granted access.



My Profile
To access your Profile please click here.
You can View or Edit your Profile or MFA on this page.

Role Request
To request access to a new Application please click here.
You can Add a Role in a new Application on this page.

Manage My Roles
To access your existing Roles please click here.
You can View, Add, Edit or Remove Roles on this page.

My Requests
To access your own Pending requests please click here.
You can View or Cancel your requests on this page.

Figure 2: Self Service Dashboard Layout

Table 1: Self Service Dashboard Layout

Reference	Name	Description
1	IDM Self Service Home Button	This button returns the user to the IDM Self Service Dashboard.
2	IDM Self-Service Function Buttons	These buttons provide user access to the functions that are accessed through the IDM Self Service Dashboard.
3	My Requests Counter	This counter displays the number of pending requests that the user has submitted. It also provides 1-click access to a list of those requests.
4	Dropdown Menu	This menu displays user’s identity and provides access to the Log Out function when clicked.
5	Self Service Taskbar	This taskbar appears whenever a user accesses one of the Self Service functions. It enables the user to move between the various Self Service functions.

6. How to Request a Role

The following terms are introduced in this section:

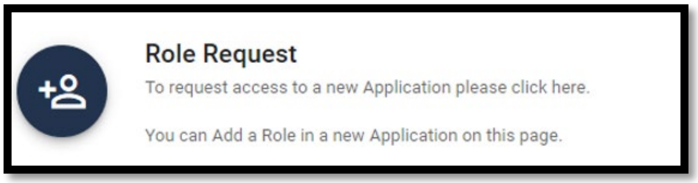
- **Remote Identity Proofing (RIDP)** - Describes the process that is used to confirm a person's identity. Most users will be required to complete RIDP as part of the process of being approved for a role. RIDP is also called Identity Verification. Users may have three opportunities to verify their identity. Verification occurs in the following order:
    - **Online Proofing** - An identity verification procedure that uses Experian's computer-based Identity Verification service.
    - **Phone Proofing** - An identity proofing procedure that uses Experian's telephone-based Identity Verification service. Phone proofing is only available if the user is unable to verify their identity using online proofing.
    - **Manual Proofing** - An identity proofing procedure that is performed by an Application (Tier 1) Help Desk in accordance with their policies. Manual proofing is not offered by every application and is only available if the user is unable to first verify their identity through online proofing and phone proofing.

Note: Users with foreign addresses will not be eligible for online proofing or phone proofing.

6.1 How to Request a Role for a New Application

Note: The Transformed Medicaid Statistical Information System (T-MSIS) application will be used in this section as an example of the typical procedure for requesting roles and for adding role attributes. The procedure for other applications may vary slightly.

Users request a role for a new application using the ***Role Request*** button that is located on the Self Service Dashboard.

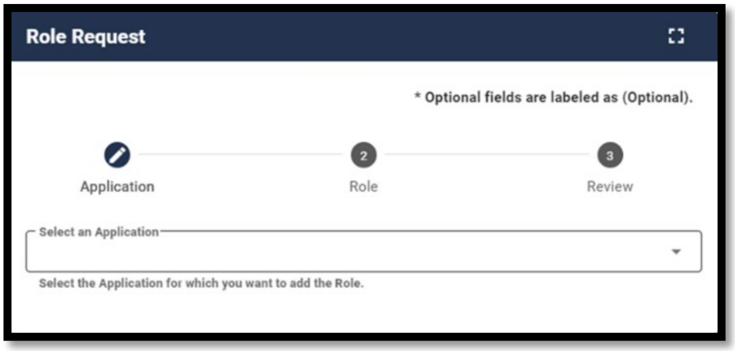


Role Request

To request access to a new Application please click here.

You can Add a Role in a new Application on this page.

1) Click the ***Role Request*** button.
   The Role Request window appears.



Role Request

* Optional fields are labeled as (Optional).

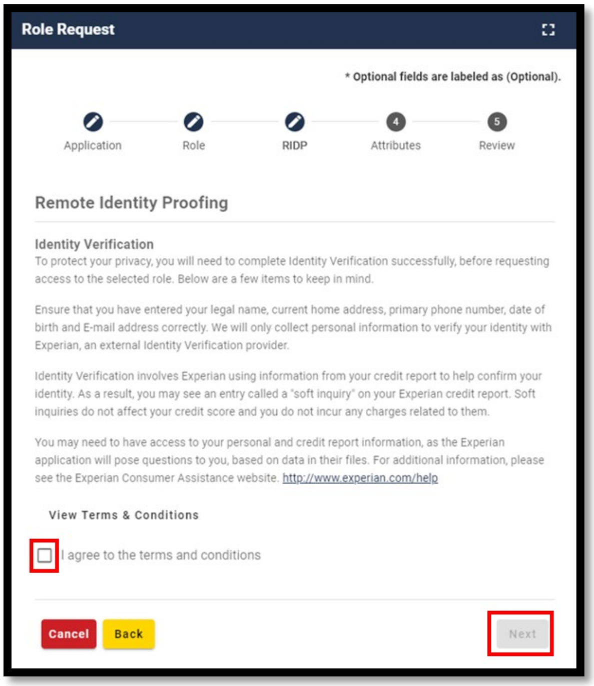
Select an Application

Select the Application for which you want to add the Role.

Figure 3: The Role Request Window

2) Select an application. The Select a Role menu appears after an application is selected. [6]

3) Select a role. The RIDP terms and conditions appear after a role is selected.



Role Request

* Optional fields are labeled as (Optional).

Remote Identity Proofing

Identity Verification

To protect your privacy, you will need to complete Identity Verification successfully, before requesting access to the selected role. Below are a few items to keep in mind.

Ensure that you have entered your legal name, current home address, primary phone number, date of birth and E-mail address correctly. We will only collect personal information to verify your identity with Experian, an external Identity Verification provider.

Identity Verification involves Experian using information from your credit report to help confirm your identity. As a result, you may see an entry called a "soft inquiry" on your Experian credit report. Soft inquiries do not affect your credit score and you do not incur any charges related to them.

You may need to have access to your personal and credit report information, as the Experian application will pose questions to you, based on data in their files. For additional information, please see the Experian Consumer Assistance website. http://www.experian.com/help

View Terms & Conditions

□ I agree to the terms and conditions

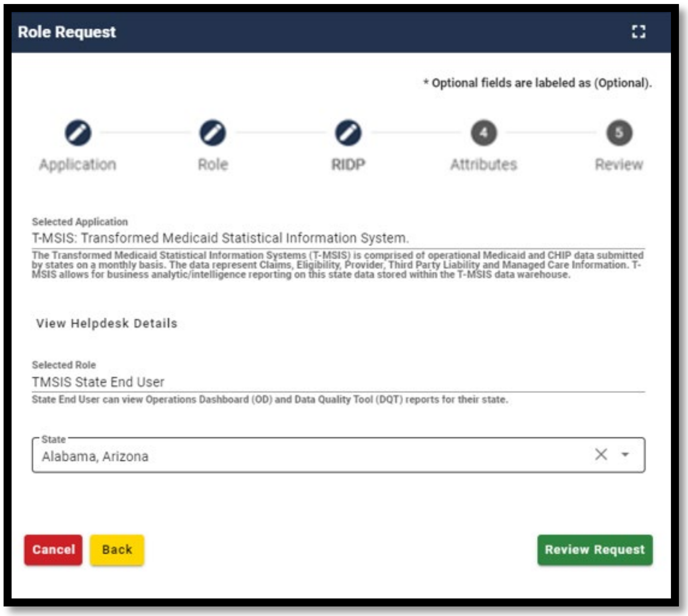
Figure 4: Role Request - RIDP Terms and Conditions

4) Review the RIDP terms and conditions, check the "*I agree to the terms and conditions*" selection box, then click the ***Next*** button. The Identity Verification form appears.

[6] The Select an Application menu will not display an application for which a user already has a role. To add a role to an existing application use the ***Manage My Roles*** button.

5) Complete the Identity Verification form and click the ***Next*** button. The RIDP proofing questions appear.

6) Answer the proofing questions and click the ***Verify*** button. The Attribute menu appears.[7]



Selected Application
T-MSIS: Transformed Medicaid Statistical Information System.
The Transformed Medicaid Statistical Information Systems (T-MSIS) is comprised of operational Medicaid and CHIP data submitted by states on a monthly basis. The data represent Claims, Eligibility, Provider, Third Party Liability and Managed Care Information. T-MSIS allows for business analytic/intelligence reporting on this state data stored within the T-MSIS data warehouse.

Selected Role
TMSIS State End User
State End User can view Operations Dashboard (OD) and Data Quality Tool (DQT) reports for their state.

State
Alabama, Arizona

Figure 5: Role Request - Attribute Selection

7) Select the required attributes.

8) Review the role request information and click the ***Review Request*** button. The Reason for Request dialog box appears.

9) Enter a justification and click the ***Submit Role Request*** button. The Role Request window displays a Request ID and a message which states that the request was successfully submitted to an approver for action. [8]

10) The ***My Requests*** indicator on the Self Service Dashboard increments to display the user's current number of pending requests.

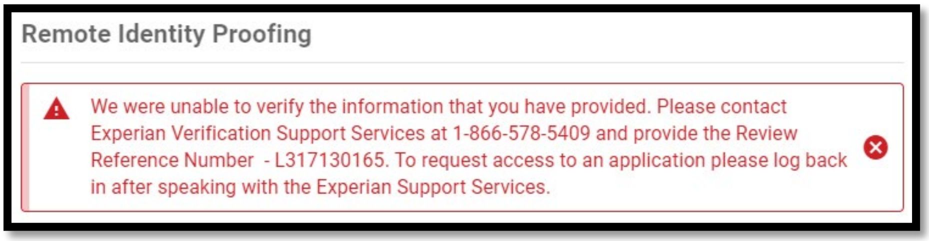
11) Click the ***Back to Home*** button. The user returns to the Self Service Dashboard.

[7] The phone number must be registered to the user who is currently navigating the RIDP workflow.

[8] An email is sent to the user's email address on record which indicates that the request was submitted successfully. Follow up emails will be sent when the request is approved, rejected, or it expires because no action was taken by an approver.

6.1.1 What to do When Users Can't Verify Their Identity with Online Proofing

If the RIDP Online Proofing process is unsuccessful, then the system will display an error message as illustrated by **Figure 6: RIDP Online Proofing Error Message.**

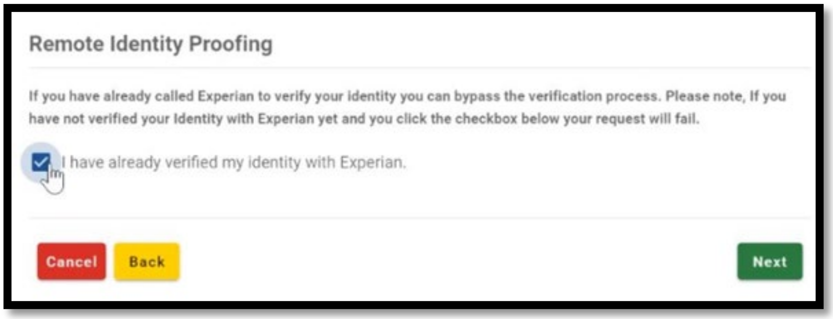


Remote Identity Proofing

We were unable to verify the information that you have provided. Please contact Experian Verification Support Services at 1-866-578-5409 and provide the Review Reference Number - L317130165. To request access to an application please log back in after speaking with the Experian Support Services.

Figure 6: RIDP Online Proofing Error Message.

1) Write down the Experian support contact information and the Review Reference Number.
2) Click the ***Cancel*** button. The Cancel Role Request Process window appears.
3) Click the ***Confirm*** button.
4) Contact Experian using the contact information provided in the error message and perform Phone Proofing.
5) If Phone Proofing was successful, sign in to the IDM System and initiate the role request procedure again. When the user reselects the desired role, IDM will be aware of the success or failure of Online and Phone Proofing. The Role Request window displays a message which asks if Experian has been contacted.



Remote Identity Proofing

If you have already called Experian to verify your identity you can bypass the verification process. Please note, If you have not verified your Identity with Experian yet and you click the checkbox below your request will fail.

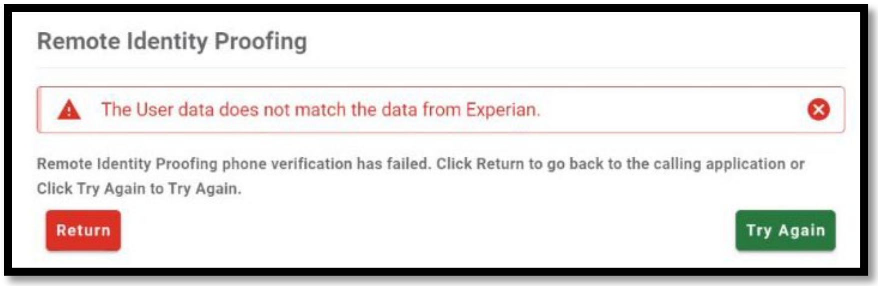
☑ I have already verified my identity with Experian.

Figure 7: Experian Phone Verification Confirmation

6) Click the "*I have already verified my identity with Experian*" checkbox if Experian has been contacted.
7) Click the ***Next*** button. The Identity Information Verification form is displayed.
8) Verify that the information in the form exactly matches the information that was used to successfully verify the user's identity by phone.
9) Click the ***Next*** button, then click the ***OK*** button. The Attribute menu appears and the user resumes the Role Request procedure.

6.1.2 What to do When Users Can't Verify Their Identity with Phone Proofing

If the Phone Proofing RIDP process is unsuccessful, then the system will display an error message as illustrated by **Figure 8: Phone Proofing RIDP Error Message**.



Remote Identity Proofing

The User data does not match the data from Experian.

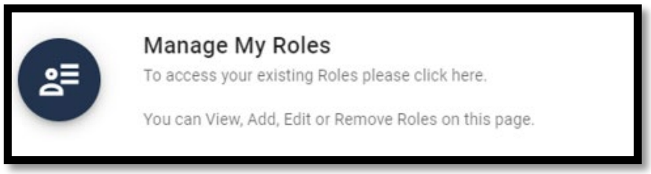
Remote Identity Proofing phone verification has failed. Click Return to go back to the calling application or Click Try Again to Try Again.

Figure 8: Phone Proofing RIDP Error Message

1) Click the ***Try Again*** button. The Identity Information Verification form is displayed.
2) Verify that the identity information which was proofed on the phone matches the data in the form, then click the ***Next*** button.
3) If the error message is displayed again, click the ***Return*** button, then cancel the Role Request procedure.
4) Contact the Application Help Desk and inquire about the Manual Proofing process. Application Help Desk contact information is located on the CMS Tier 1 Help Desk Support website.

6.2 How to Request a Role in an Existing Application

Users request a role in an existing application using the ***Manage My Roles*** button that is located on the Self Service Dashboard.

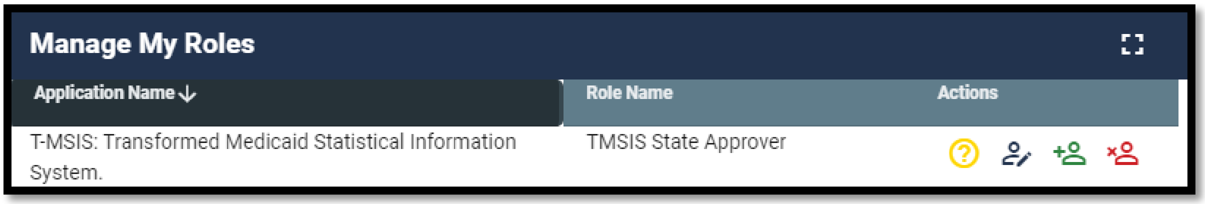


Manage My Roles

To access your existing Roles please click here.

You can View, Add, Edit or Remove Roles on this page.

1) Click the ***Manage My Roles*** button.
   The Manage My Roles window appears and displays the user's existing roles.

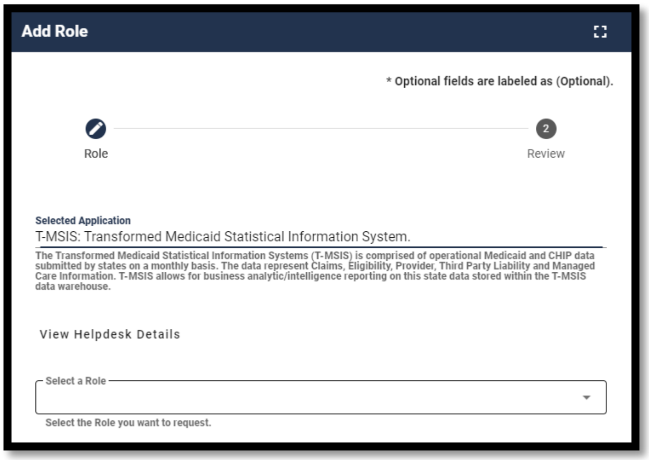


Manage My Roles

Application Name ↓	Role Name	Actions
T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State Approver	? ✎ + ×

Figure 9: Manage My Roles Window - User's Existing Roles

2) Click the ***Add Role*** button. The Add Role window appears. The Selected Application is automatically populated, and the user will not be able to change it. [9]



Add Role

* Optional fields are labeled as (Optional).

Selected Application
T-MSIS: Transformed Medicaid Statistical Information System.
The Transformed Medicaid Statistical Information Systems (T-MSIS) is comprised of operational Medicaid and CHIP data submitted by states on a monthly basis. The data represent Claims, Eligibility, Provider, Third Party Liability and Managed Care Information. T-MSIS allows for business analytic/intelligence reporting on this state data stored within the T-MSIS data warehouse.

Select a Role
Select the Role you want to request.

Figure 10: Add Role Window

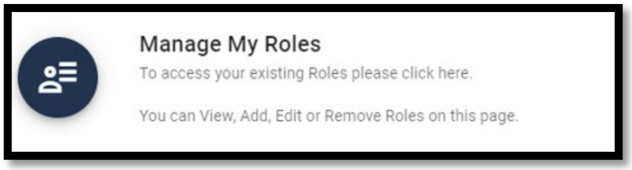
3) Select a Role. The Attribute menu appears.
4) Select the required attributes.
5) Review the role request information and click the ***Review Request*** button. The Reason for Request dialog box appears.
6) Enter a justification and click the ***Submit Role Request*** button. The Role Request window displays Request ID information and a message which states that the request was successfully submitted to an approver for action. [10]
7) The ***My Requests*** indicator on the Self Service Dashboard increments to display the user's current number of pending requests.

6.3 How to Add Attributes to an Existing Role

Users add attributes to an existing role using the ***Manage My Roles*** button that is located on the Self Service Dashboard.

[9] The IDM System evaluates the user's current role and determines if that user is eligible to add additional roles for the same application. The system will display a message if they are not eligible.

[10] An email is sent to the user's email address on record which indicates that the request was submitted successfully. Follow up emails will be sent when the request is approved, rejected, or it expires because no action was taken by an approver.



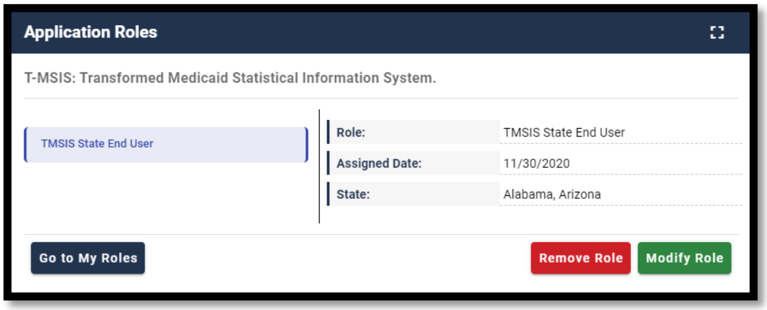
Manage My Roles

To access your existing Roles please click here.

You can View, Add, Edit or Remove Roles on this page.

1) Click the ***Manage My Roles*** button.
   The Manage My Roles window appears and displays the user's existing roles as illustrated by **Figure 9: Manage My Roles Window - User's Existing Roles.**

2) Click the ***View Details*** button. The Application Roles window appears and displays the role details for the selected role.



Application Roles

T-MSIS: Transformed Medicaid Statistical Information System.

Role:	TMSIS State End User
Assigned Date:	11/30/2020
State:	Alabama, Arizona

Figure 11: Application Roles Window - Role Details View

3) Click the ***Modify Role*** button. The Edit Role Details window appears. This window contains fields that are similar to those used during the initial role request, but it only permits the user to modify role attributes.

4) Add one or more role attributes.

5) Enter a justification statement and click the ***Submit Changes*** button. The Edit Role Details window displays Request ID information and a message that informs the user that the request was successfully submitted.[11]

6) Click the ***Go to My Roles*** button. The Manage My Roles window appears and the My Requests indicator on the Self Service Dashboard increments to display the user's current number of pending requests.

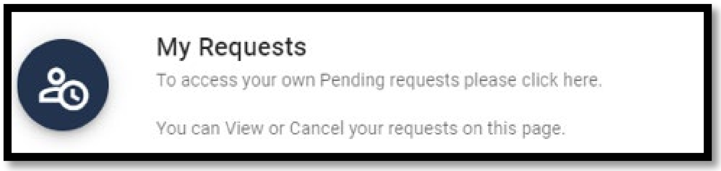
[11] Role modification requests may be auto-approved or approved after review by an approver.

7. How to View and Cancel Role Requests

Users view and cancel role requests that are pending approval action using the ***My Requests*** button located on the Self Service Dashboard. Users can also view their role requests by clicking the ***My Requests*** indicator located at the top right corner of the Self Service Dashboard.

Note: The Transformed Medicaid Statistical Information System (T-MSIS) application will be used in this section as an example of the typical procedure for viewing and cancelling role requests. The procedure for other applications may vary slightly.

7.1 How to View Role Requests



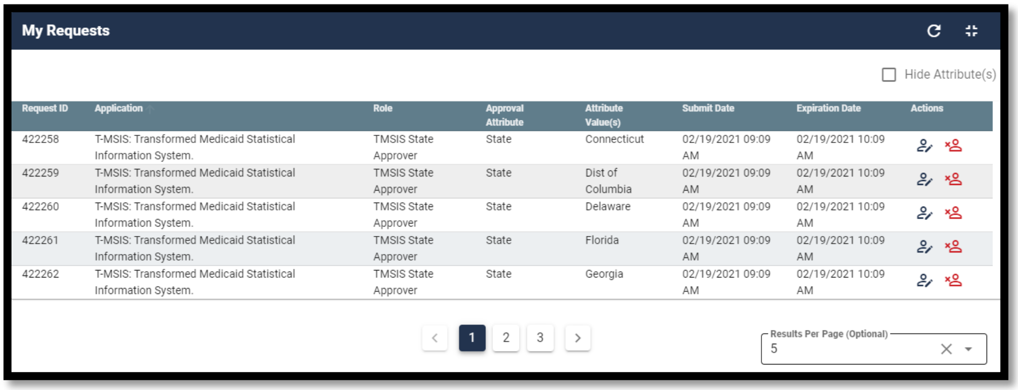
My Requests

To access your own Pending requests please click here.

You can View or Cancel your requests on this page.

1) Click the ***My Requests*** button.

The My Requests window appears and displays the user's pending role requests.[12] [13]



My Requests

☐ Hide Attribute(s)

Request ID	Application	Role	Approval Attribute	Attribute Value(s)	Submit Date	Expiration Date	Actions
422258	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State Approver	State	Connecticut	02/19/2021 09:09 AM	02/19/2021 10:09 AM	
422259	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State Approver	State	Dist of Columbia	02/19/2021 09:09 AM	02/19/2021 10:09 AM	
422260	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State Approver	State	Delaware	02/19/2021 09:09 AM	02/19/2021 10:09 AM	
422261	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State Approver	State	Florida	02/19/2021 09:09 AM	02/19/2021 10:09 AM	
422262	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State Approver	State	Georgia	02/19/2021 09:09 AM	02/19/2021 10:09 AM	

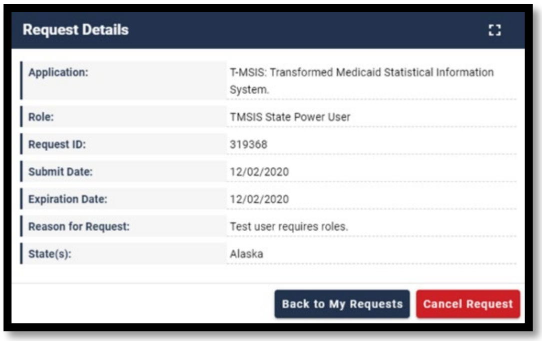
Results Per Page (Optional): 5

Figure 12: My Requests - Role Requests Pending Approval

2) Click the ***View Details*** button. The Request Details window appears and displays details of the desired pending request.

[12] The user can also view their role requests by clicking the My Requests indicator located at the top right corner of the Self Service Dashboard.

[13] (Optional) The user may click the column headings of the list to change the sorting order of the displayed information.



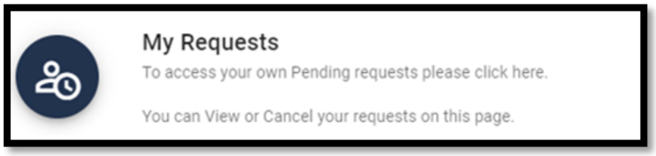
Request Details

Application:	T-MSIS: Transformed Medicaid Statistical Information System.
Role:	TMSIS State Power User
Request ID:	319368
Submit Date:	12/02/2020
Expiration Date:	12/02/2020
Reason for Request:	Test user requires roles.
State(s):	Alaska

Figure 13: Request Details Window

3) Click the ***Back to My Requests*** button. The user is returned to the My Requests window.

7.2 How to Cancel a Role Request

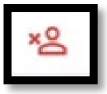


My Requests

To access your own Pending requests please click here.

You can View or Cancel your requests on this page.

1) Click the ***My Requests*** button located on the Self Service Dashboard. The My Requests window appears and displays the user's current pending requests as illustrated by **Figure 12: My Requests - Role Requests Pending Approval**.



2) Click the ***Cancel Request*** button for the role request that will be cancelled. The Cancel Role Requests decision window appears.

3) Click the ***Cancel Role Request*** button. The My Requests window appears and displays a message that informs the user that the pending request was successfully cancelled. [14]

4) The ***My Requests*** indicator on the Self Service Dashboard decreases by one for each pending request that is cancelled.

[14] An email is sent to the user's email address of record which indicates that the request was accepted.

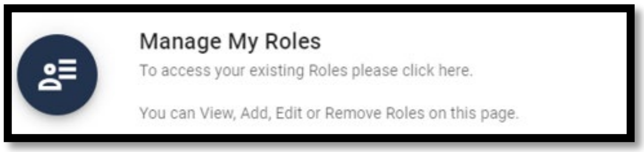
8. How to Remove Roles and Role Attributes

Users remove roles and role attributes using the ***Manage My Roles*** button that is located on the Self Service Dashboard.

Note: The Transformed Medicaid Statistical Information System (T-MSIS) application will be used in this section as an example of the typical procedure for removing roles and role attributes. The procedure for other applications may vary slightly.

Note: The IDM System will display a warning message if the role removal or attribute removal operation could affect the last approver of an organization that still has users associated with that role or attribute. Such users could be left in an "orphaned" state without an approver of record for future role requests.

8.1 How to Remove a Role

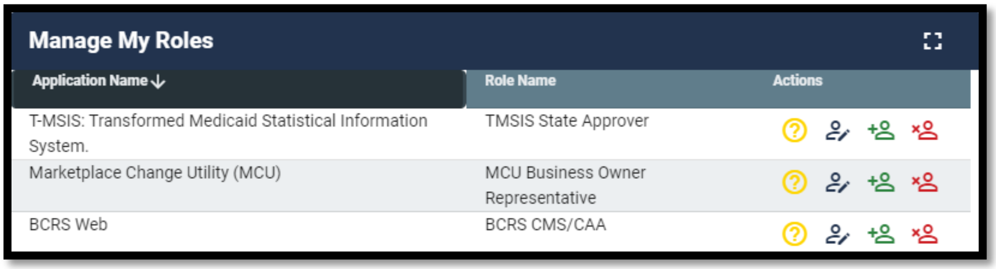


Manage My Roles

To access your existing Roles please click here.

You can View, Add, Edit or Remove Roles on this page.

1) Click the ***Manage My Roles*** button.
   The Manage My Roles window appears and displays the user's existing roles.



Manage My Roles

Application Name ↓	Role Name	Actions
T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State Approver	? ✎ + ×
Marketplace Change Utility (MCU)	MCU Business Owner Representative	? ✎ + ×
BCRS Web	BCRS CMS/CAA	? ✎ + ×

Figure 14: Manage My Roles Window

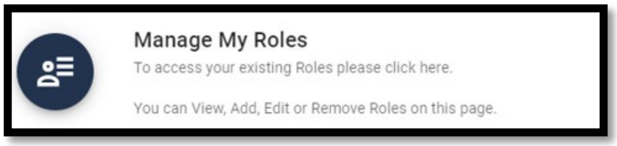
2) Click the **Remove Role** button. The Remove Role decision window appears.
3) Click the ***Remove Role*** button. The Manage My Roles window displays Request ID information and a message that informs the user that the request was successfully submitted.[15]

[15] An email is sent to the user's email address of record which indicates that the request was accepted.

4) Click the ***Go to My Roles*** button. The Manage My Roles window appears and displays the user's current roles.

8.2 How to Remove Attributes From a Role

Users remove role attributes using the ***Manage My Roles*** button that is located on the Self Service Dashboard.



Manage My Roles

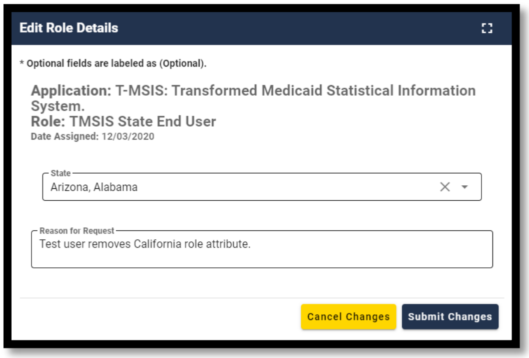
To access your existing Roles please click here.

You can View, Add, Edit or Remove Roles on this page.

1) Click the ***Manage My Roles*** button.
The Manage My Roles window appears and displays the user's existing roles as illustrated by **Figure 14: Manage My Roles Window.**

2) Click the ***View Details*** button. The Application Roles window appears and displays the role details for the selected role.

3) Click the ***Modify Role*** button. The Edit Role Details window appears. [16]



Edit Role Details

* Optional fields are labeled as (Optional).

Application: T-MSIS: Transformed Medicaid Statistical Information System.
Role: TMSIS State End User
Date Assigned: 12/03/2020

State: Arizona, Alabama

Reason for Request: Test user removes California role attribute.

Figure 15: Edit Role Details Window

4) Remove the desired role attributes.

5) Type a justification statement and click the ***Submit Changes*** button. The Edit Role Details window displays Request ID information and a message that informs the user that the request was successfully submitted. [17]

6) Click the ***Go to My Roles*** button. The Manage My Roles window appears and displays the user's current roles.

[16] The Edit Role Details window contains fields that are similar to those used during the initial role request, but it only permits the user to modify role attributes.

[17] An email is sent to the user's email address of record which indicates that the request was accepted.

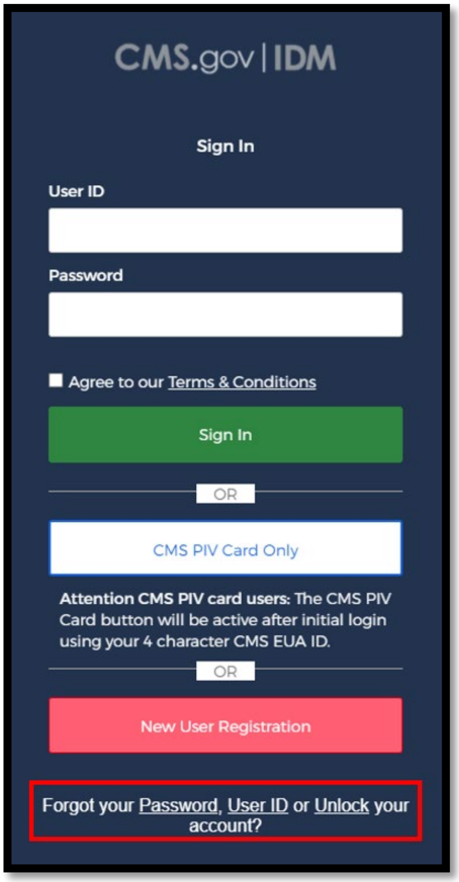
9. IDM User Account Self-Service Features

The following terms are introduced in this section:

- **Recovery -** A process that allows a user to reset their own password or unlock their own account without the assistance of a helpdesk.
- **Recovery Device -** An email, short message service (SMS), or interactive voice response (IVR) MFA device that is used to authenticate a user during the recovery process.

The Change an Expired Password feature as well as the Self-Service features which are available as links at the bottom of the IDM Sign In window can be performed without the assistance of Help Desk personnel. The Self-Service features available as links include:

- Reset a forgotten password.
- Recover a forgotten User ID.
- Unlock an account after being locked out for too many failed login attempts.



Attention CMS PIV card users: The CMS PIV Card button will be active after initial login using your 4 character CMS EUA ID.

Forgot your Password, User ID or Unlock your account?

Figure 16: IDM Sign In Window with Self-Service Links

Note: Email is automatically set up as the default recovery device for all users that are required to log in with MFA. The procedures described in this section use the Email recovery device when describing the procedures to use the Self-Service account functions. Users are encouraged to add additional factors using the procedures described in **Section 10 How to Manage MFA and Recovery Devices**.

Users must meet the following conditions to use the self-service procedures to reset their forgotten password or unlock their account as described in this section of the user guide:

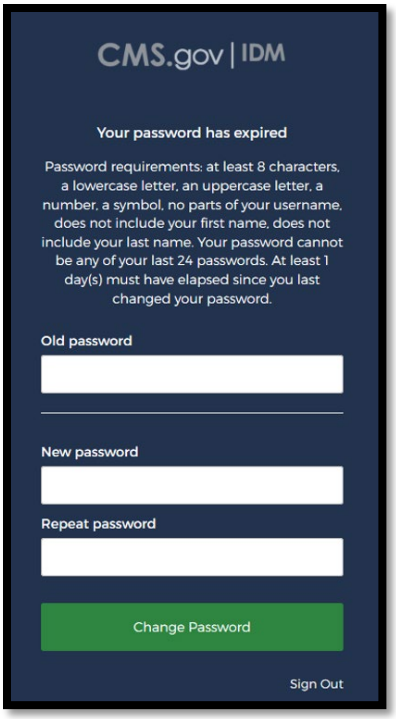
- The user must remember the security question answer that they established when they created their account.
- The user must have an Email, IVR, or SMS recovery device registered and active in their user profile. [18]

Users who do not meet these conditions will not be able to use these self-service procedures and must contact their respective Application Help Desk to obtain assistance. Application Help Desk contact information is located on the CMS Tier 1 Help Desk Support website.

9.1 How to Change an Expired Password

When a user's password expires, the IDM System Sign In window displays a message that informs the user that their password has expired, as shown in **Figure 17: IDM Self-Service Change Expired Password Window**. The user is required to create a new password using the procedure described in this section before they can sign in to the IDM System.

[18] Users are encouraged to add additional factors using the procedures described in **Section 10 How to Manage MFA and Recovery Devices**.



Your password has expired

Password requirements: at least 8 characters, a lowercase letter, an uppercase letter, a number, a symbol, no parts of your username, does not include your first name, does not include your last name. Your password cannot be any of your last 24 passwords. At least 1 day(s) must have elapsed since you last changed your password.

Figure 17: IDM Self-Service Change Expired Password Window

1) Enter the Old Password.
2) Enter the New Password and the Repeat Password.
3) Click the ***Change Password*** button.[19]

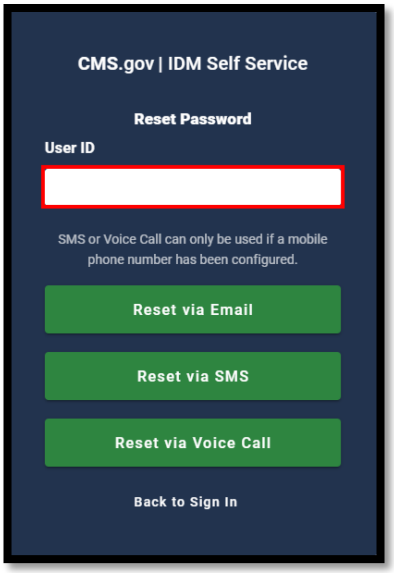
The User can now log in using the new password.

9.2 How to Reset a Forgotten Password

Users who forget their passwords can reset their own password using the ***Password*** link that is located at the bottom of the IDM Sign In window as illustrated in **Figure 16: IDM Sign In Window with Self-Service Links**.

1) Click the ***Password*** link. The Reset Password window appears.

[19] .The system sends an email to the user's address on record which indicates that the user's password was changed. It also indicates where the user can obtain assistance if they have questions.



CMS.gov | IDM Self Service

Reset Password

User ID

SMS or Voice Call can only be used if a mobile phone number has been configured.

Figure 18: IDM Self-Service Reset Password Request

2) Enter the User ID.
3) Click the ***Reset via Email*** button. The screen refreshes and the system displays a message that informs the user that an email which contains password reset instructions has been sent.
4) Click the ***Back to Sign In button***. The IDM System sends an email to the email address listed in the user's profile. The email informs the user that a password reset request has been made, and it contains a ***Reset Password*** hyperlink that the user must use to complete the password reset procedure. [20]
5) Click the ***Reset Password*** hyperlink contained within the "Forgot Password" email. The Reset Your Password window appears and prompts the user to respond to a security question.
6) Enter the security question answer, and then click the ***Reset Password*** button. The screen refreshes and the user is prompted to enter a new password.

[20] The ***Reset Password*** hyperlink expires after four hours have elapsed. The user will be required to repeat this entire procedure if the link expires.

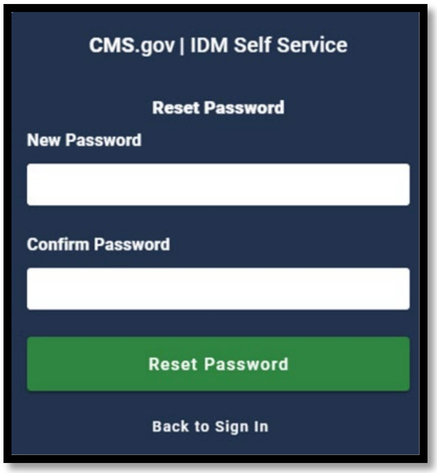


Figure 19: IDM Self-Service Reset Password Set New Password

7) Enter the New Password and the Confirm Password. The New Password and the Confirm Password must match.
8) Click the ***Reset Password*** button. The screen refreshes and displays a message which states that the password was successfully changed.
9) Click the ***Back to Sign In*** button. The user returns to the IDM Sign In window.

9.3 Recover a forgotten User ID

Users who forget their User ID can recover it using the ***User ID*** link that is located at the bottom of the IDM Sign In window as illustrated in **Figure 16: IDM Sign In Window with Self-Service Links**.

1) Click the ***User ID*** link. The Forgot User ID window appears.

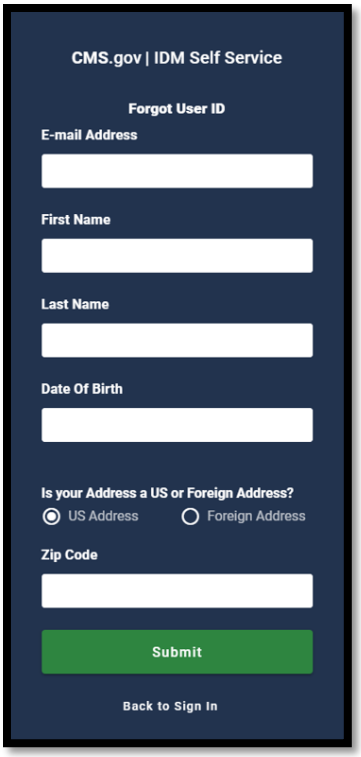

CMS.gov | IDM Self Service
Forgot User ID
E-mail Address
First Name
Last Name
Date Of Birth
Is your Address a US or Foreign Address?
● US Address ○ Foreign Address
Zip Code
Submit
Back to Sign In

Figure 20: IDM Self-Service Forgot User ID Window

1) Enter the E-mail Address, First Name, Last Name, and Date of Birth.
2) Keep the default "***US Address***" setting if the address is a US address. If the address is foreign, click the "***Foreign Address"*** radio button control.
3) Enter the Zip Code and click the ***Submit*** button. The Forgot User ID window displays a message that informs the user that an email with the requested information has been sent. [21]
4) The IDM System sends an email to the email address listed in the user's profile. This email contains the user's User ID.
5) Click the ***Back to Sign In*** button. The user returns to the IDM Sign In window.

9.4 How to Unlock a User Account

Users whose accounts are locked for exceeding the maximum number of failed sign-in attempts are automatically redirected to the self-service Unlock Account window illustrated in **Figure 21: IDM Self-Service Unlock Account Window**. Alternatively, the user may select the **Unlock** link that is located at the bottom of the IDM Sign In window as illustrated in **Figure 16: IDM Sign In Window with Self-Service Links**.

[21] A zip code is not required for foreign addresses. The Zip Code dialog box will not be displayed if the user indicates that they have a foreign address.

When a user is locked out of their account for excessive failed sign-in attempts, the IDM System also sends an email that explains why the account was locked and steps the user should take to unlock the account.

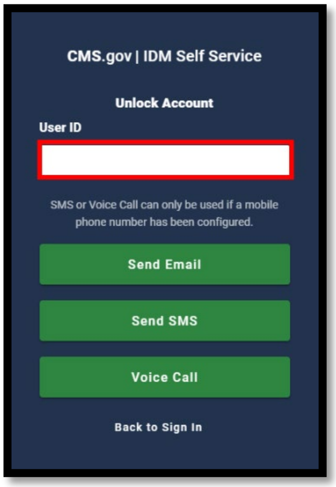

CMS.gov | IDM Self Service
Unlock Account
User ID
SMS or Voice Call can only be used if a mobile phone number has been configured.
Send Email
Send SMS
Voice Call
Back to Sign In

Figure 21: IDM Self-Service Unlock Account Window

1) Enter the User ID.
2) Click the ***Send Email*** button. The Unlock Request Sent window appears.
3) Click the ***Back to Sign In*** button.
4) The IDM System sends an Account Unlock Request email to the email address listed in the user's profile. This email informs the user of the account unlock request and it contains an Unlock Account hyperlink that the user must use to complete the Unlock Account procedure. [22]
5) Click the ***Unlock Account*** hyperlink contained within the "Account Unlock" email. The Answer Unlock Account Challenge window appears.
6) Enter the security question answer, and then click the ***Unlock Account*** button. The screen refreshes and displays a message which states that the account was successfully unlocked.
7) Click the ***Back to Sign In*** button. The IDM System Sign In window appears and the user's account is now unlocked.

[22] The ***Unlock Account*** hyperlink expires after four hours have elapsed. The user will be required to repeat this entire procedure if the link expires.

10. How to Manage MFA and Recovery Devices

The following terms are used in this section:

- **Recovery -** A process that allows a user to reset their own password or unlock their own account without the assistance of a helpdesk.
- **Recovery Device -** An email, short message service (SMS), or interactive voice response (IVR) MFA device that is used to authenticate a user during the recovery process.

A user may have multiple active MFA devices registered to their account if they desire. An email is sent to the user's email address of record anytime changes occur to an MFA device that is associated with the user's account.

Note: Adding an MFA device will not add MFA to a user's sign-in if it is not already required for their role or application.

Table 2: MFA and Recovery Device Summary lists the MFA and Recovery devices that are supported by the IDM System. [23]

Table 2: MFA and Recovery Device Summary

MFA Device	Device Function	Actions	Modifiable Setting	Edit Settings
Email	MFA & Recovery	Add, Activate, Modify, or Remove[24].	Email Address	User can activate a device that is in pending status.
Text Message (SMS)	MFA & Recovery	Add, Activate, or Remove.	Mobile Phone Number	User can activate a device that is in pending status.
Interactive Voice Response (IVR)	MFA & Recovery	Add, Activate, or Remove.	Phone Number	User can activate a device that is in pending status.

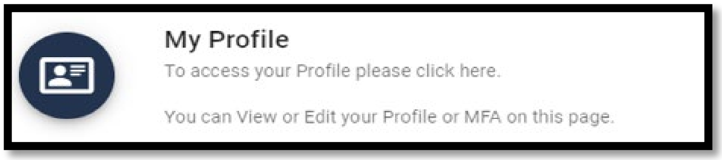
[23] Email, Text, and IVR MFA devices also function as Recovery devices that can be used to recover a forgotten password or unlock an account if the user has registered those devices to their account.

[24] Users who have email as the default MFA and Recovery device will not be given the option to remove it.

MFA Device	Device Function	Actions	Modifiable Setting	Edit Settings
Google Authenticator	MFA Only	Add or Remove.	N/A	Edit is not applicable.
Okta Verify	MFA Only	Add or Remove.	N/A	Edit is not applicable.
YubiKey	MFA Only	Add or Remove.	N/A	Edit is not applicable.

MFA and Recovery device information is part of the user's account profile. Users view, add, and remove MFA and Recovery devices using the IDM Self Service Dashboard ***My Profile*** button and the ***Manage MFA and Recovery Devices*** window.

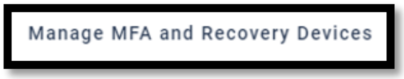
10.1 How to View MFA and Recovery Devices



To access your Profile please click here.

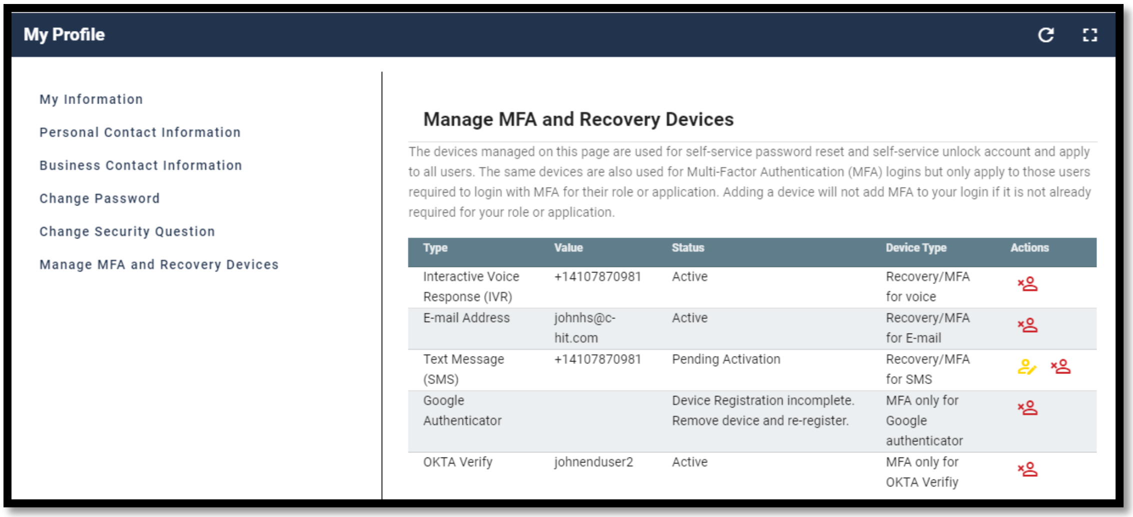
You can View or Edit your Profile or MFA on this page.

1) Click the ***My Profile*** button.
   The My Profile window appears.



2) Click the ***Manage MFA and Recovery Devices*** button.
   The Manage MFA and Recovery Devices window opens and displays a summary of the MFA devices that are registered to the user's profile. [25]

[25] Refer to **Table 2: MFA and Recovery Device Summary**.



My Profile

My Information
Personal Contact Information
Business Contact Information
Change Password
Change Security Question
Manage MFA and Recovery Devices

Manage MFA and Recovery Devices

The devices managed on this page are used for self-service password reset and self-service unlock account and apply to all users. The same devices are also used for Multi-Factor Authentication (MFA) logins but only apply to those users required to login with MFA for their role or application. Adding a device will not add MFA to your login if it is not already required for your role or application.

Type	Value	Status	Device Type	Actions
Interactive Voice Response (IVR)	+14107870981	Active	Recovery/MFA for voice	
E-mail Address	johnhs@c-hit.com	Active	Recovery/MFA for E-mail	
Text Message (SMS)	+14107870981	Pending Activation	Recovery/MFA for SMS	
Google Authenticator		Device Registration incomplete. Remove device and re-register.	MFA only for Google authenticator	
OKTA Verify	johnenduser2	Active	MFA only for OKTA Verifiy	

Figure 22: Manage MFA and Recovery Devices Window

10.2 How to Add an Email, IVR, or SMS MFA/Recovery Device

Users add an Email, IVR, or SMS MFA / Recovery device using the Manage MFA and Recovery Devices window and the following procedure.

1) Access the Manage MFA and Recovery Devices window using the procedure in **Section 10.1 How to View MFA and Recovery Devices**. The Manage MFA and Recovery Devices window opens as illustrated by **Figure 22: Manage MFA and Recovery Devices Window**.
2) Use the ***Add another device*** menu to select the E-mail Address option, Interactive Voice Response (IVR) option, or Text Message (SMS) option. The device configuration window appears.
3) Enter the E-mail address for an Email MFA/Recovery device or enter the Phone Number, then enter the Extension if applicable for an IVR MFA/Recovery device.
4) Click the ***Verify MFA*** button. The MFA confirmation window appears.
5) The IDM System sends an email to the email address that is currently associated with the user's profile places if the Email option was selected. Alternately, if the IVR or SMS option was selected, it places an automated voice call or sends a text message to the phone number that was provided when the device was configured. The email, automated voice call, or text message communicates a one-time verification code to the user.
6) Enter the one-time verification code and click the ***Confirm MFA*** button. The system displays a message which states that the MFA device was successfully added.
7) Click the ***OK*** button.

10.3 How to Activate a Pending Email, IVR, or SMS MFA/Recovery Device

An Email, IVR, or SMS MFA/Recovery device is placed in "*pending*" status when a user does not complete the add device procedure. Users activate a pending MFA/Recovery device using the following procedure.

1) Access the Manage MFA and Recovery Devices window using the procedure in **Section 10.1 How to View MFA and Recovery Devices**. The Manage MFA and Recovery Devices window opens as illustrated by **Figure 22: Manage MFA and Recovery Devices Window**.
2) Click the ***Activate Factor*** button. The Activate Factor window appears and displays a message which indicates that an MFA code has been sent.
3) The IDM System sends a one-time verification code to the MFA device that is being activated.
4) Enter the one-time verification code and click the ***Confirm MFA*** button. The system displays a message which states that the MFA device was successfully added.
5) Click the ***OK*** button.

10.4 How to Add a Google Authenticator Mobile App MFA Device

Users add a Google Authenticator mobile app MFA device using the Manage MFA and Recovery Devices window and the following procedure.

6) Access the Manage MFA and Recovery Devices window using the procedure in **Section 10.1 How to View MFA and Recovery Devices**. The Manage MFA and Recovery Devices window opens as illustrated by **Figure 22: Manage MFA and Recovery Devices Window**.
7) Use the ***Add another device*** menu to select the Google Authenticator option. The Google Authenticator registration window opens.
8) Click the ***Next*** button and follow the on-screen prompts for installing a Google Authenticator MFA device.
9) Download and install the Google Authenticator mobile app onto the mobile device. Obtain the app from the appropriate app store. [26]
10) Click the ***Register Device*** button on the IDM Google Authenticator setup window. The window displays a QR code.
11) Start the Google Authenticator app on the mobile device and click the ***Get Started*** button. The Account Setup screen appears.

[26] Users who access the IDM System with CMS issued mobile phones must download the Google Authenticator app through the CMS app store and may require the assistance / permission of their IT department. Users who access the IDM System with personally owned mobile phones must use their respective app stores.

12) Click the ***Scan a QR code*** button on the Google Authenticator app, and then scan the QR code using the Google Authenticator mobile app. The Google Authenticator app generates a one-time verification code.[27]

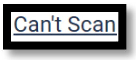
13) Enter the one-time verification code into the IDM Confirm MFA Code dialog box and click the ***Confirm MFA*** button. A message is displayed which indicates the MFA device was successfully added.

14) Click the ***OK*** button.

10.5 How to Add an Okta Verify MFA Device

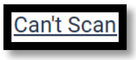
Users add an Okta Verify mobile app MFA device using the Manage MFA and Recovery Devices window and the following procedure.

1) Access the Manage MFA and Recovery Devices window using the procedure in **Section 10.1 How to View MFA and Recovery Devices**. The Manage MFA and Recovery Devices window opens as illustrated by **Figure 22: Manage MFA and Recovery Devices Window**.
2) Use the ***Add another device*** menu to select the Okta Verify option. The Okta registration window opens.
3) Click the ***Next*** button and follow the on-screen prompts for installing an Okta Verify MFA device.
4) Download and install the Okta Verify app onto the mobile device. Obtain the app from the appropriate app store. [28]
5) Click the ***Register Device*** button on the IDM Okta Verify setup window. The window displays a QR code.
6) Start the Okta Verify app on the mobile device. The Welcome to Okta Verify screen appears.
7) Click the ***Add Account*** button on the Okta Verify mobile app, then choose the **Organization** account type.
8) Scan the QR Code using the Okta Verify mobile app. [29]

[27] Users who are unable to scan the QR code may click the ***Can't Scan*** link. 

This link displays a manual Setup Key and instructions that explain how to use the key to activate the device.

[28] Users who access the IDM System with CMS issued mobile phones must download the Okta Verify app through the CMS app store and may require the assistance / permission of their IT department. Users who access the IDM System with personally owned mobile phones must use their respective app stores.

[29] Users who are unable to scan the QR code may click the ***Can't Scan*** link. 

This link displays a manual Setup Key and instructions that explain how to use the key to activate the device.

9) A message is displayed which indicates the MFA device was successfully added. Click the ***OK*** button.

10.6 How to Add a YubiKey MFA Device

The YubiKey MFA device consists of a hardware-based MFA device that plugs into a Universal Serial Bus (USB) port on the user's desktop or laptop computer.

Note: YubiKey MFA device use is restricted to users who cannot use other supported MFA devices. Each Application Team/Owner of an application that uses YubiKey MFA devices to authenticate users is responsible for purchasing, preparing, managing, and distributing the YubiKey MFA devices to their application users.

Users add a YubiKey MFA device using the Manage MFA and Recovery Devices window and the following procedure.

1) Access the Manage MFA and Recovery Devices window using the procedure in **Section 10.1 How to View MFA and Recovery Devices**. The Manage MFA and Recovery Devices window opens as illustrated by **Figure 22: Manage MFA and Recovery Devices Window**.
2) Use the ***Add another device*** menu to select the YubiKey option. The YubiKey registration window opens.
3) Click the ***YubiKey Passcode*** field.
4) Insert the YubiKey device into a USB port and press the ***button on the YubiKey***. A passcode is generated and automatically entered into the YubiKey Passcode field.
5) Click the ***Confirm YubiKey*** button. A message is displayed which indicates the MFA device was successfully added. Click the ***OK*** button.

10.7 How to Edit MFA Device Settings

Only Email MFA device settings can be modified. IVR, SMS, Google Authenticator, Okta, and YubiKey MFA device settings must be removed and then re-added if the settings need to be modified.

Note: The Email MFA device uses the same email address that stored in the user's IDM profile.

Users modify their Email MFA device settings using the My Profile - Personal Contact Information window and the following procedure.

1) Click the ***My Profile*** button as described in **Section 11.1 How to Open and Close the My Profile Function.** The My Information window appears**.**

2) Click the ***Personal Contact Information*** button.
The Personal Contact Information window appears.

3) Click the ***Edit*** button. The Personal Contact Information becomes modifiable.

4) Enter the new Email Address and click the ***Submit Changes*** button. A message is displayed which indicates the user's contact information was updated successfully.

Note: The updated Email MFA device may not appear in the Manage MFA and Recovery Devices window until the user logs out and signs in again.

10.8 How to Remove an MFA Device

Users may remove MFA devices using the Manage MFA and Recovery Devices window and the following procedure. [30]

Note: If a user removes an active YubiKey MFA device from their account, they must contact their Application Helpdesk before they attempt to re-activate it. The user's Application Helpdesk must update the YubiKey device with a new seed file and update those changes in IDM's authentication database before the user can re-activate that device.

1) Access the Manage MFA and Recovery Devices window using the procedure in **Section 10.1 How to View MFA and Recovery Devices**. The Manage MFA and Recovery Devices window opens as illustrated by **Figure 22: Manage MFA and Recovery Devices Window**.

2) Click the ***Remove Factor*** button for the MFA device that requires removal. The Remove MFA Device decision window appears.

3) Click the ***Remove MFA Device*** button.

[30] Users who are required to use email as the default MFA device will not have the option to remove the Email MFA device.

11. How Manage User Account Profile Information

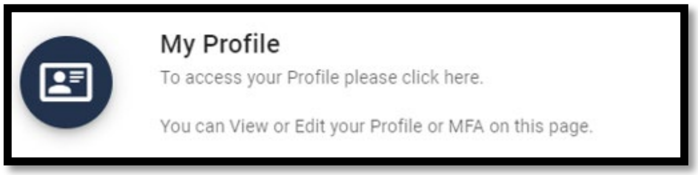
Users view and edit their user account profile information using the IDM Self Service My Profile Function. This function enables users to view and/or modify various attributes of their user profile to include:

- View a summary of their user profile.
- Modify their personal contact information.
- Modify their business contact information.
- Change their password.
- Change their security question.
- Manage their MFA and recovery devices.

An email is sent to the user’s email address of record whenever the user makes a change to their profile information.

11.1 How to Open and Close the My Profile Function

Open the My Profile Function:



My Profile

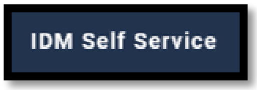
To access your Profile please click here.

You can View or Edit your Profile or MFA on this page.

1) Click the ***My Profile*** button located on the Self Service Dashboard. The My Profile window appears.

Close the My Profile Function:

1) Choose one of the following actions to close the My Profile function.



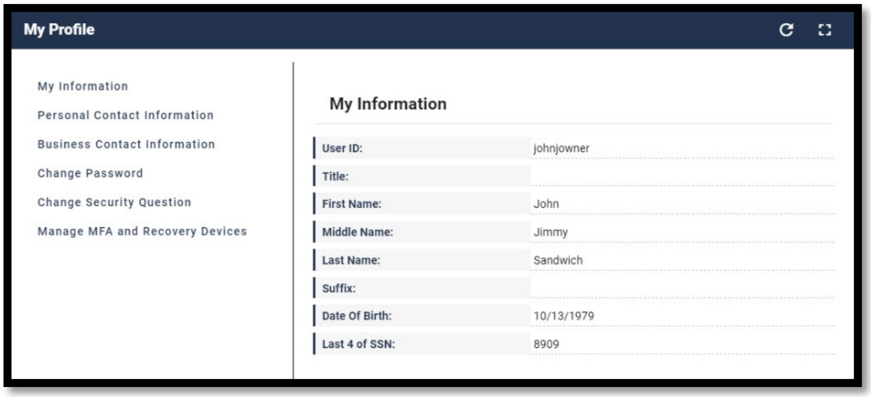
IDM Self Service

- Click the ***IDM Self Service*** button located at the top left corner of the Self Service Dashboard.
- Select another function from the Self Service taskbar.
- Select the ***Log Out*** option from the dropdown menu and log out of the system.

11.2 How to View User Profile Information

Users view a read-only summary of their user profile information using the My Profile - My Information window and the following procedure.

1) Click the ***My Profile*** button as described in **Section 11.1 How to Open and Close the My Profile Function.** The My Information window appears.


My Profile
My Information
Personal Contact Information
Business Contact Information
Change Password
Change Security Question
Manage MFA and Recovery Devices

My Information

User ID:	johnjowner
Title:	
First Name:	John
Middle Name:	Jimmy
Last Name:	Sandwich
Suffix:	
Date Of Birth:	10/13/1979
Last 4 of SSN:	8909

Figure 23: My Profile - My Information

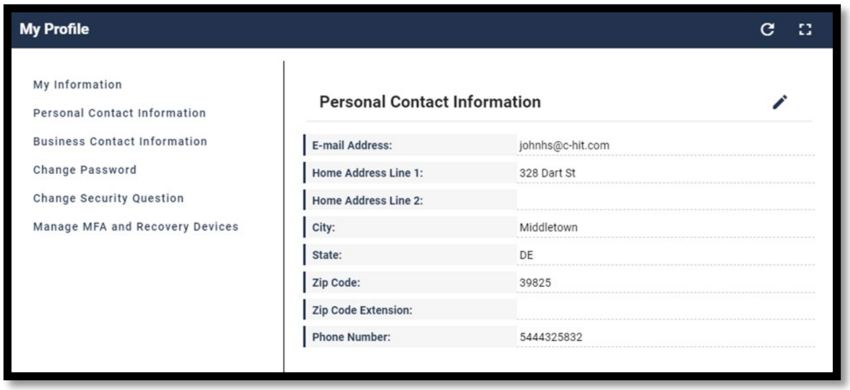
11.3 How to View and Modify Personal Contact Information

Users view and modify their personal contact information using the My Profile - Personal Contact Information window and the following procedure.

View Personal Contact Information

1) Click the ***My Profile*** button as described in **Section 11.1 How to Open and Close the My Profile Function.** The My Information window appears**.**

2) Click the ***Personal Contact Information*** button. The Personal Contact Information window appears.


My Profile
My Information
Personal Contact Information
Business Contact Information
Change Password
Change Security Question
Manage MFA and Recovery Devices

Personal Contact Information

E-mail Address:	johnhs@c-hit.com
Home Address Line 1:	328 Dart St
Home Address Line 2:	
City:	Middletown
State:	DE
Zip Code:	39825
Zip Code Extension:	
Phone Number:	5444325832

Figure 24: My Profile - Personal Contact Information

Modify Personal Contact Information

1) With the Personal Contact Information window open, click the ***Edit*** button. The Personal Contact Information becomes modifiable.

2) Make the desired changes then click the ***Submit Changes*** button. The screen refreshes and the Personal Contact Information window displays the updated information.

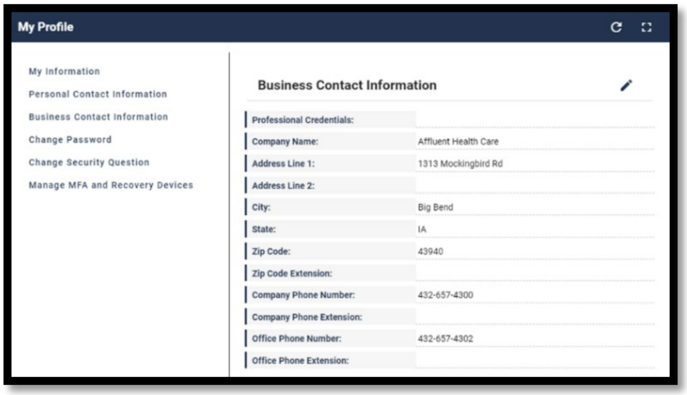
11.4 How to View and Modify Business Contact Information

Users view and modify their business contact information using the My Profile - Business Contact Information window and the following procedure.

View Business Contact Information

1) Click the ***My Profile*** button as described in **Section 11.1 How to Open and Close the My Profile Function.** The My Information window appears**.**

2) Click the ***Business Contact Information*** button.
   The Business Contact Information window appears.


My Profile
My Information
Personal Contact Information
Business Contact Information
Change Password
Change Security Question
Manage MFA and Recovery Devices

Business Contact Information

Professional Credentials:	
Company Name:	Affluent Health Care
Address Line 1:	1313 Mockingbird Rd
Address Line 2:	
City:	Big Bend
State:	IA
Zip Code:	43940
Zip Code Extension:	
Company Phone Number:	432-657-4300
Company Phone Extension:	
Office Phone Number:	432-657-4302
Office Phone Extension:	

Figure 25: My Profile - Business Contact Information

Edit the User's Business Contact Information

1) With the Business Contact Information window open, click the ***Edit*** button. The Business Contact Information becomes modifiable.
2) Make the desired changes then click the ***Submit Changes*** button. The screen refreshes and the Business Contact Information window displays the updated information.

11.5 How to Change the User Account Password

Users change their account password using the My Profile - Change Password window and the following procedure.

1) Click the ***My Profile*** button as described in **Section 11.1 How to Open and Close the My Profile Function.** The My Information window appears**.**

2) Click the Change Password button. The Change Password window appears.

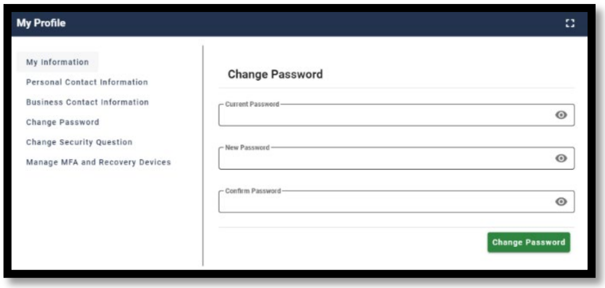


Figure 26: My Profile - Change Password Form

3) Enter the Current Password.
4) Enter the New Password and the Confirm Password.
5) Click the ***Change Password*** button.

11.6 How to Change the User Security Question and Answer

Users change their security question and answer information using the My Profile - Change Security Question window.

1) Click the ***My Profile*** button as described in **Section 11.1 How to Open and Close the My Profile Function.** The My Information window appears**.**
2) Click the ***Change Security Question*** button. The Change Security Question window appears.

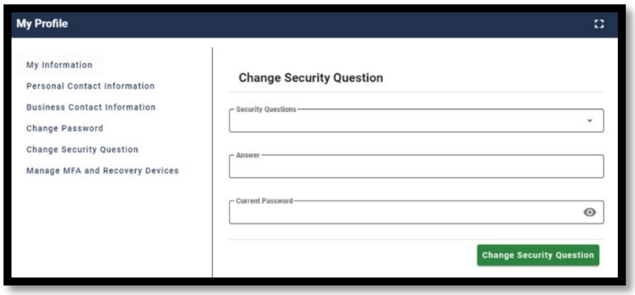


Figure 27: My Profile - Change Security Question Form

3) Select a Security Question from the list.
4) Enter the security question answer into the Answer field. [31]
5) Enter the Current Password.
6) Click the ***Change Security Question*** button.

[31] The security question answer must be at least four characters long. Additionally, it must not contain parts of the user's first name, last name, password, or security question.

12. Instructions for Approvers

The following terms are introduced in this section:

- **Role Approval** - The process used by the Business Owners, their representatives, Authorizers, Help Desks, or other Approvers to grant an application role to a user who is requesting the role.

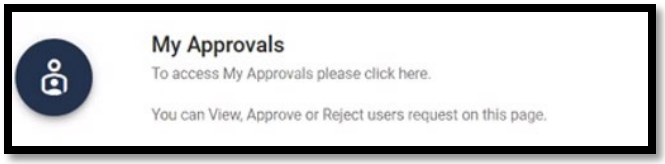
Users who possess Approver capabilities or Help Desk/Manage User capabilities for an application have the ability to approve or reject role requests from other users who have been placed under their authority. These users are granted access to the My Approvals function and may perform the following tasks:

- View a list of all requests pending approval.
- View the details of a specific request pending approval.
- Approve or reject individual requests pending approval.
- Simultaneously approve and/or reject multiple requests pending approval.
- Export a list of requests pending approval.

The system sends an email to the requesting user’s email address on record which indicates the action that was taken on the request. It also indicates where the user can obtain assistance if they have questions.

12.1 How to Open and Close the My Approvals Function

Open the My Approvals Function:



My Approvals

To access My Approvals please click here.

You can View, Approve or Reject users request on this page.

1) Click the My Approvals button located on the Self Service Dashboard. The My Approvals window opens. [32]

Close the My Approvals Function:

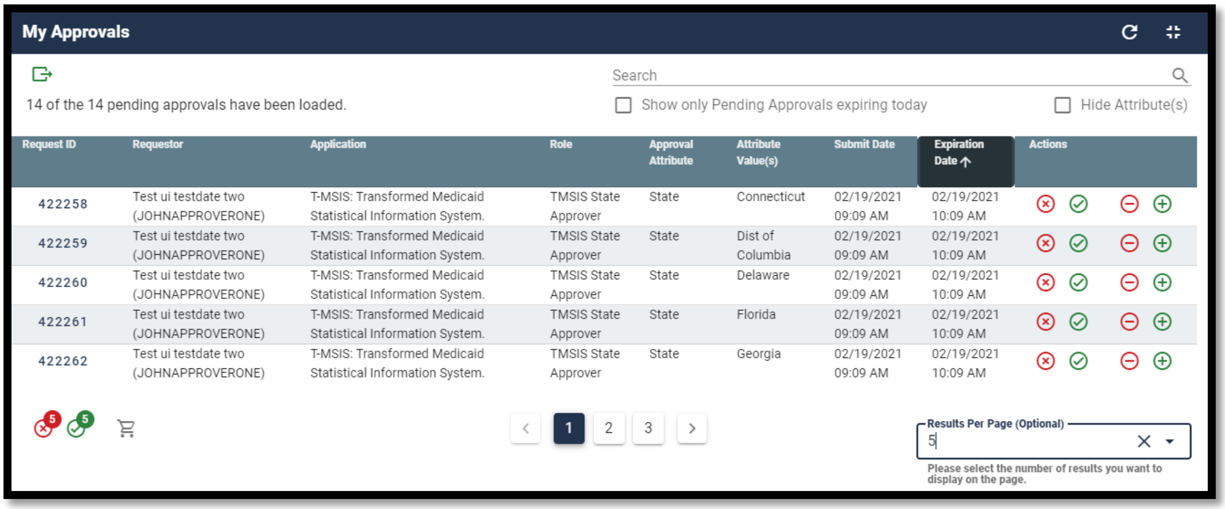
1) Choose one of the following actions to close the My Approvals function.
   - Click the ***IDM Self Service*** button located at the top left corner of the Self Service Dashboard.
   - Select another function from the Self Service taskbar.
   - Select the ***Log Out*** option from the dropdown menu and log out of the system.

[32] The user can also view their pending approvals by clicking the ***My Approvals*** indicator located at the top right corner of the Self Service Dashboard.

12.2 How to View a List of Pending Approval Requests

Users view a list of all requests that are pending approval using the My Approvals window and the following procedure.

1) Click the ***My Approvals*** button as described in **Section 12.1 How to Open and Close the My Approvals Function.** The My Approvals window appears.



My Approvals

14 of the 14 pending approvals have been loaded.

Search

□ Show only Pending Approvals expiring today

□ Hide Attribute(s)

Request ID	Requestor	Application	Role	Approval Attribute	Attribute Value(s)	Submit Date	Expiration Date ↑	Actions
422258	Test ui testdate two (JOHNAPPROVERONE)	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State Approver	State	Connecticut	02/19/2021 09:09 AM	02/19/2021 10:09 AM	⊗ ✓ ⊖ ⊕
422259	Test ui testdate two (JOHNAPPROVERONE)	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State Approver	State	Dist of Columbia	02/19/2021 09:09 AM	02/19/2021 10:09 AM	⊗ ✓ ⊖ ⊕
422260	Test ui testdate two (JOHNAPPROVERONE)	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State Approver	State	Delaware	02/19/2021 09:09 AM	02/19/2021 10:09 AM	⊗ ✓ ⊖ ⊕
422261	Test ui testdate two (JOHNAPPROVERONE)	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State Approver	State	Florida	02/19/2021 09:09 AM	02/19/2021 10:09 AM	⊗ ✓ ⊖ ⊕
422262	Test ui testdate two (JOHNAPPROVERONE)	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State Approver	State	Georgia	02/19/2021 09:09 AM	02/19/2021 10:09 AM	⊗ ✓ ⊖ ⊕

Results Per Page (Optional): 5

Please select the number of results you want to display on the page.

Figure 28: My Approvals Window

The My Approvals window displays a list that contains all requests that have been submitted by other users for the approver to review and approve or reject. An approver has 60 days to approve or reject a request. After 60 days, the request will expire.[33]

12.2.1 How to View Details for a Specific Pending Approval Request

Request ID

131316

1) While viewing records in the My Approvals window, click the ***Request ID*** for the desired record that is displayed in the My Approvals window. The Pending Approval Details window appears.
2) Click the ***Go to My Approvals*** button to close the Pending Approval Details window. The Approver returns to the My Approvals window.[34]

[33] Not every application has Group, Organization, or other Role Attribute information. These attributes are specific to each role for a given application and will not always be present in a role request.

[34] The Pending Approval Details window also provides the capability to approve or reject a single request that is pending approval. Refer **Section 12.5 How to Approve/Reject a Single Request.**

12.3 How to Approve or Reject a Single Request

Approvers approve or reject individual pending requests using the ***Approve Request Now*** and ***Reject Request Now*** buttons on the My Approvals window and the following procedure.

1) Click the ***My Approvals*** button as described in **Section 12.1 How to Open and Close the My Approvals Function.** The My Approvals window appears as illustrated by **Figure 28: My Approvals Window**.

2) Click the appropriate button to approve or reject the desired request.

   - **Approve the Request**: Click the ***Approve Request Now*** button ✓ on the My Approvals window for the individual record that will be approved. The Approve Request decision window appears.

   - **Reject the Request**: Click the ***Reject Request Now*** button ⊗ on the My Approvals window for the individual record that will be rejected. The Reject Request decision window appears.

3) Enter a brief justification.

4) Click the ***Submit*** button. The IDM System displays a message which indicates the operation completed successfully. The My Approvals indicator decrements by one.

5) Click the ***Go to My Approvals*** button. The Approver returns to the My Approvals window.

12.4 How to Approve or Reject Multiple Requests on a Single Page

Approvers approve or reject multiple pending requests that are displayed on a single page of requests using the ***Approve All on Current Page Now*** and ***Reject All on Current Page Now*** buttons on the My Approvals window and the following procedure.

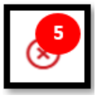
1) Click the ***My Approvals*** button as described in **Section 12.1 How to Open and Close the My Approvals Function.** The My Approvals window appears as illustrated by **Figure 28: My Approvals Window**.

2) (Optional) Use the ***Pagination*** control to change the number of requests that are displayed on a page in the My Approvals window.

Results Per Page (Optional)
5

3) Click the appropriate button to approve or reject all requests on the current page:

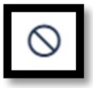
   - **Approve the Request**: Click the ***Approve All on Current Page Now*** button. ✓5 . The Pending Approvals to Process window opens and all requests on the page are listed with an action to APPROVE.

- **Reject the Request**: Click the ***Reject All on Current Page Now*** button. 

The Pending Approvals to Process window opens and all requests on the page are listed with an action to REJECT.

4) (Optional) Click the ***Request Details*** button

to view details about a specific request. Click the ***Request Details*** button again to close the details window for that request.

5) (Optional) Click the ***Remove Request*** control  to remove a specific request from the Approve or Reject list. [35]

6) Enter a brief justification. The same justification will be applied to each request.

7) Click the ***Submit*** button. All records that appear on the Pending Approvals to Process list will be processed as Approvals or Rejections.

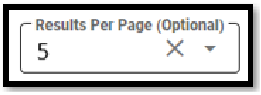
8) The IDM System displays a message that indicates the operation completed successfully and the My Approvals indicator is decremented by the number of requests that were processed.

9) Click the ***Go to My Approvals*** button. The Approver returns to My Approvals window.

12.5 How to Simultaneously Approve and Reject Multiple Requests

Approvers simultaneously approve and reject multiple requests using the ***Bulk Process as an Approval***, ***Bulk Process as a Rejection***, and ***Cart*** buttons on the My Approvals window and the following procedure.

1) Click the ***My Approvals*** button as described in **Section 12.1 How to Open and Close the My Approvals Function.** The My Approvals window appears as illustrated by **Figure 28: My Approvals Window**.

2) (Optional) Use the ***Pagination*** control 

to change the number of requests that are displayed on each page in the My Approvals window.

3) Click the appropriate button to approve or reject each individual request that is displayed on the page:

[35] The specific record will be removed from the Pending Approvals to Process list and will remain in pending status. The Approver will receive periodic email reminders about the pending requests until they are acted on, or they expire.

- **Approve the Request**: Click the ***Bulk Process as an Approval*** button. ⊕ The request is added to the Pending Approvals to Process queue with an action to APPROVE. The Cart counter increments for each record added to the queue.

- **Reject the Request**: Click the ***Bulk Process as a Rejection*** button. ⊖ The request is added to the Pending Approvals to Process queue with an action to REJECT. The Cart counter increments for each record added to the queue.

Click the ***Cart*** button. 🛒 2 The Pending Approvals to Process window appears.

4) (Optional) Click the ***Remove Request*** button ⊘ to remove a specific request from the bulk Approval/Rejection action. [36]
5) Enter a justification for the Rejections **and** a justification for the Approvals. The same rejection or approval justification will be applied to each rejected or approved request respectively.
6) Click the ***Submit*** button. All records that appear on the Pending Approvals to Process list will be processed as Approvals or Rejections.
7) The IDM System displays a message which indicates the operation completed successfully and the My Approvals indicator is decremented by the number of requests that were processed.
8) Click the ***Go to My Approvals*** button. The Approver returns to the My Approvals window.

12.6 How to Export a List of Pending Approvals

Approvers can export a list of requests that are pending approval using the ***Export*** button located on the My Approvals window and the following procedure.

1) Click the ***My Approvals*** button as described in **Section 12.1 How to Open and Close the My Approvals Function.** The My Approvals window appears as illustrated by **Figure 28: My Approvals Window**.

[36] The specific record will be removed from the Pending Approvals to Process list and will remain in pending status. The Approver will receive periodic email reminders about the pending requests until they are acted on, or they expire.

2) (Optional) Use the ***Pagination*** control to adjust the number of requests that are displayed on each page.

3) (Optional) Use the ***Search*** box to perform a search across all columns to obtain a list of records that contain a desired alphanumeric search term.

4) (Optional) Click the ***Expiring Today*** filter control to display only those requests that will expire on the current day.

5) (Optional) Click the ***Hide Attributes*** filter option to hide or view the columns of information that pertain to role attributes.

6) (Optional) Click the ***My Approvals Column Headings*** to perform an alphanumeric sort of the information in the respective columns. The sort order will alternate between normal and reverse order each time the user clicks.

7) Click the ***Export*** button. The list of pending approvals will be downloaded to the user’s computing device as a Microsoft Excel spreadsheet (.xls) file.

13. How to View IDM Application Reports

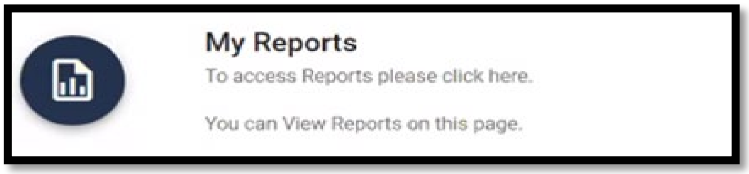
13.1 Description of the IDM Reports Function

Users who require access to the IDM Reports must submit a role request for the IDM Reports application using the procedure outlined in **Section 6.1 How to Request a Role for a New Application**.

Note: Users will receive access to a predetermined number of reports based on the specific role that they request. **Appendix B: IDM Report Categories** provides a summary of the IDM reports the system produces.

13.2 How to Access the IDM Reports

Users that possess report access privileges view the desired reports using the ***My Reports*** button which is located on the Self Service Dashboard, and the following procedure.

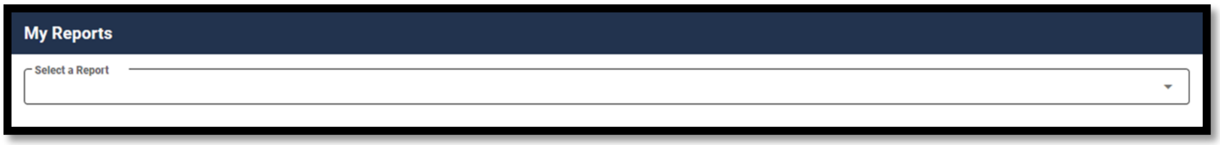


My Reports

To access Reports please click here.

You can View Reports on this page.

1) Click the ***My Reports*** button.
   The My Reports window appears.

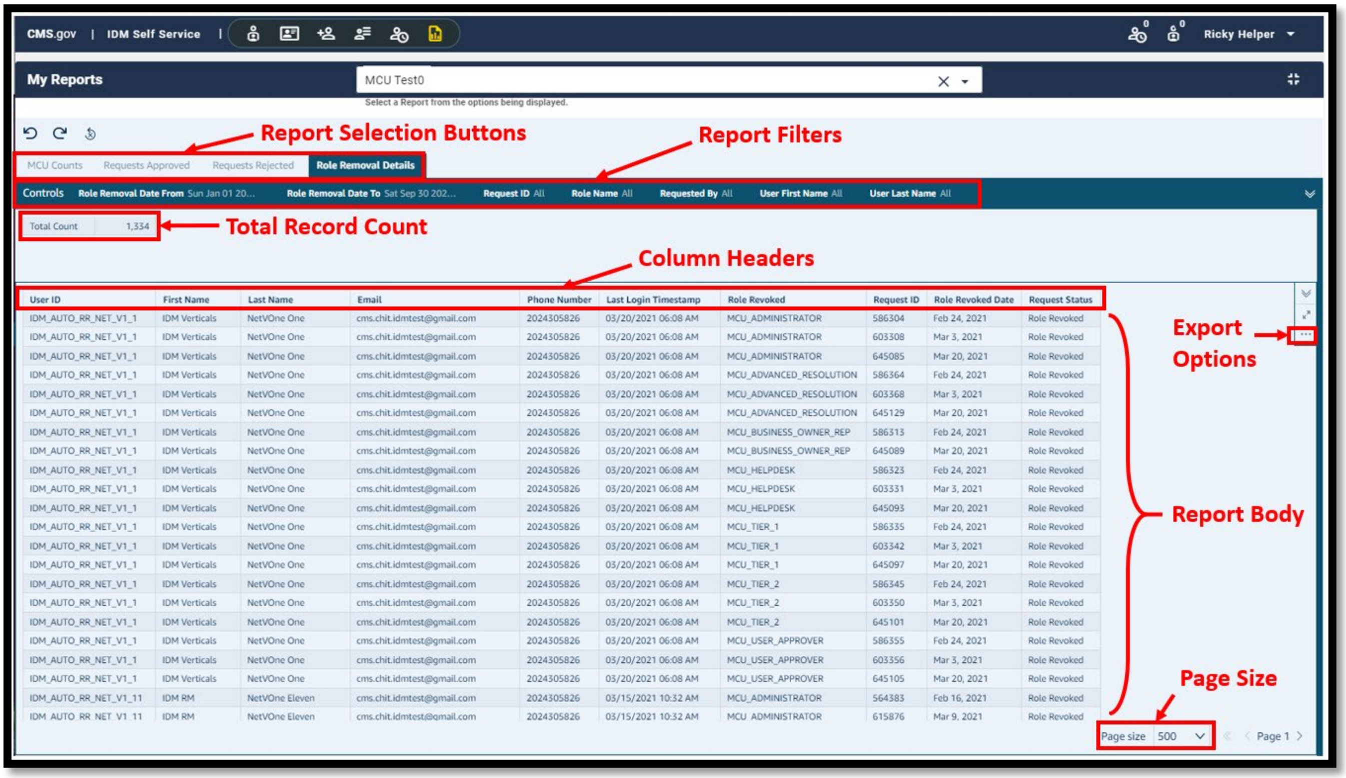


My Reports

Select a Report

Figure 29: My Reports Window

2) Select a report. The screen refreshes and the report appears.



My Reports: MCU Test0

Select a Report from the options being displayed.

MCU Counts | Requests Approved | Requests Rejected | Role Removal Details

Controls Role Removal Date From Sun Jan 01 20... Role Removal Date To Sat Sep 30 202... Request ID All Role Name All Requested By All User First Name All User Last Name All

Total Count 1,334

User ID	First Name	Last Name	Email	Phone Number	Last Login Timestamp	Role Revoked	Request ID	Role Revoked Date	Request Status
IDM_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_ADMINISTRATOR	586304	Feb 24, 2021	Role Revoked
IDM_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_ADMINISTRATOR	603308	Mar 3, 2021	Role Revoked
IDM_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_ADMINISTRATOR	645085	Mar 20, 2021	Role Revoked
IDM_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_ADVANCED_RESOLUTION	586364	Feb 24, 2021	Role Revoked
IDM_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_ADVANCED_RESOLUTION	603368	Mar 3, 2021	Role Revoked
IDM_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_ADVANCED_RESOLUTION	645129	Mar 20, 2021	Role Revoked
IDM_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_BUSINESS_OWNER_REP	586313	Feb 24, 2021	Role Revoked
IDM_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_BUSINESS_OWNER_REP	645089	Mar 20, 2021	Role Revoked
IDM_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_HELPDESK	586323	Feb 24, 2021	Role Revoked
IDM_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_HELPDESK	603331	Mar 3, 2021	Role Revoked
IDM_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_HELPDESK	645093	Mar 20, 2021	Role Revoked
IDM_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_TIER_1	586335	Feb 24, 2021	Role Revoked
IDM_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_TIER_1	603342	Mar 3, 2021	Role Revoked
IDM_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_TIER_1	645097	Mar 20, 2021	Role Revoked
IDM_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_TIER_2	586345	Feb 24, 2021	Role Revoked
IDM_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_TIER_2	603350	Mar 3, 2021	Role Revoked
IDM_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_TIER_2	645101	Mar 20, 2021	Role Revoked
IDM_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_USER_APPROVER	586355	Feb 24, 2021	Role Revoked
IDM_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_USER_APPROVER	603356	Mar 3, 2021	Role Revoked
IDM_AUTO_RR_NET_V1_1	IDM Verticals	NetVOne One	cms.chit.idmtest@gmail.com	2024305826	03/20/2021 06:08 AM	MCU_USER_APPROVER	645105	Mar 20, 2021	Role Revoked
IDM_AUTO_RR_NET_V1_11	IDM RM	NetVOne Eleven	cms.chit.idmtest@gmail.com	2024305826	03/15/2021 10:32 AM	MCU_ADMINISTRATOR	564383	Feb 16, 2021	Role Revoked
IDM_AUTO_RR_NET_V1_11	IDM RM	NetVOne Eleven	cms.chit.idmtest@gmail.com	2024305826	03/15/2021 10:32 AM	MCU_ADMINISTRATOR	615876	Mar 9, 2021	Role Revoked

Page size 500

Figure 30: My Reports Window with Sample Report (Full Screen View)

3) Click the ***Report Selection*** button that corresponds to the desired report if multiple reports are available. For example:

Role Removal Details

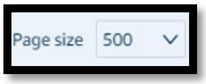
4) (Optional) Filter report columns: Click a ***Report Filter*** button to filter the report to display specific information. For example:

Role Name

5) (Optional) Sort report columns: Click a ***Column Header*** to change the sort order of the report data based on the order of the selected column. For example:

User ID

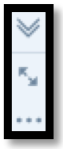
6) (Optional) Change the page size: Click the ***Page Size*** button to change the number of records displayed on the screen. For example:


Page size 500

7) (Optional) Export the report: Click the ***Export Options*** button to select the export format and export the report. For example:

13.3 How to Print a Report

To print a report, users must first export the desired report to Microsoft Excel print and print the report from that program using the following procedure.

1) Select and view the desired report using the procedure in **Section 13.2 How to Access the IDM Reports**.
2) Click any row of information in the report body. The Report Options menu appears. 
3) Click the ***Export Options*** button. The Export Options menu appears.
4) Click ***Export to Excel*** to select the export format. The Download Status window and the Save As window appear.
5) Change the file name and the save location in the Save As window if desired, then click the ***Save*** button. The Save As window closes.
6) Click the ***Done*** button.

14. Instructions for Help Desks

14.1 Description of the Help Desk/Manage Users Functions

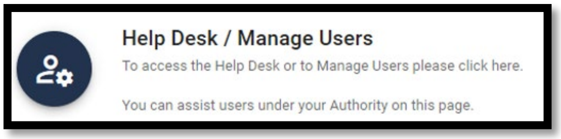
The Help Desk/Manage Users button provides access for Application (Tier 1) and IDM (Tier 2) Help Desk staff to the following functions:

- Perform an Application Search (Tier 1 only)
- Perform an Enterprise Search
- Suspend a user’s account
- Remove a user’s roles
- Cancel a user’s pending requests
- Reset a user’s password
- Unlock a user’s account
- Manage a user’s LOA
- Unsuspend a user’s account (Tier 2 only)
- Create User Audit reports and Role Request Audit reports (Tier 2 only)

14.2 How to Access the Help Desk Functions

The Help Desk Functions are accessed from the Help Desk UI. Help Desk Users access the Help Desk UI using the ***Help Desk/Manage Users*** button located on the IDM Self Service Dashboard.

Open the Help Desk UI:



Help Desk / Manage Users

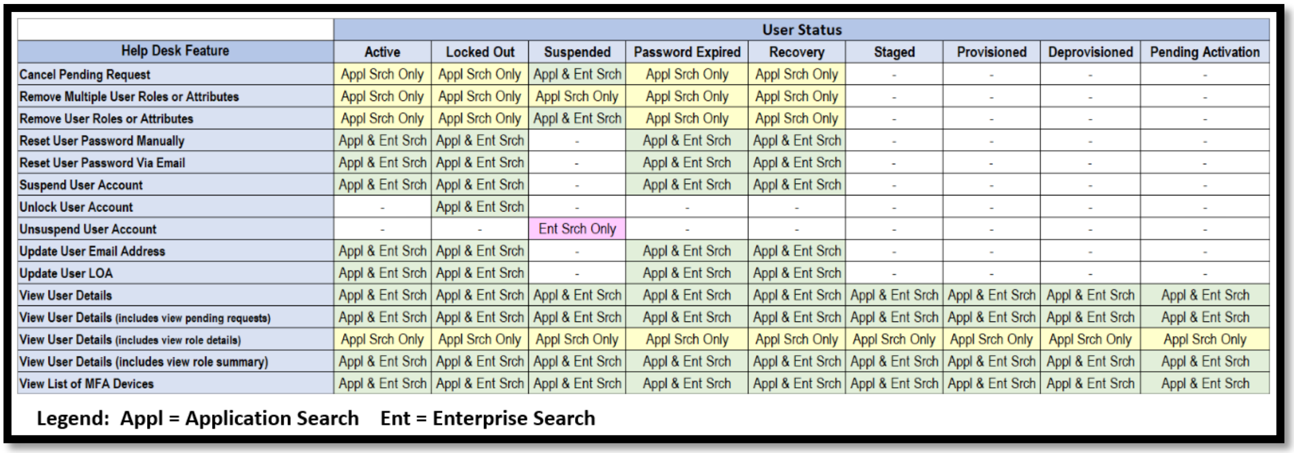
To access the Help Desk or to Manage Users please click here.

You can assist users under your Authority on this page.

1) Click the ***Help Desk/Manage Users*** button.
   located on the Self Service Dashboard. The Application Search window appears.

14.3 How to Choose the Appropriate Search

The matrix illustrated by **Figure 31: Application and Enterprise Search Capabilities Matrix** provides information to assist Help Desk Users with choosing the appropriate search for the task that needs to be performed.



	User Status								
Help Desk Feature	**Active**	**Locked Out**	**Suspended**	**Password Expired**	**Recovery**	**Staged**	**Provisioned**	**Deprovisioned**	**Pending Activation**
Cancel Pending Request	Appl Srch Only	Appl Srch Only	Appl & Ent Srch	Appl Srch Only	Appl Srch Only	-	-	-	-
Remove Multiple User Roles or Attributes	Appl Srch Only	Appl Srch Only	Appl Srch Only	Appl Srch Only	Appl Srch Only	-	-	-	-
Remove User Roles or Attributes	Appl Srch Only	Appl Srch Only	Appl & Ent Srch	Appl Srch Only	Appl Srch Only	-	-	-	-
Reset User Password Manually	Appl & Ent Srch	Appl & Ent Srch	-	Appl & Ent Srch	Appl & Ent Srch	-	-	-	-
Reset User Password Via Email	Appl & Ent Srch	Appl & Ent Srch	-	Appl & Ent Srch	Appl & Ent Srch	-	-	-	-
Suspend User Account	Appl & Ent Srch	Appl & Ent Srch	-	Appl & Ent Srch	Appl & Ent Srch	-	-	-	-
Unlock User Account	-	Appl & Ent Srch	-	-	-	-	-	-	-
Unsuspend User Account	-	-	Ent Srch Only	-	-	-	-	-	-
Update User Email Address	Appl & Ent Srch	Appl & Ent Srch	-	Appl & Ent Srch	Appl & Ent Srch	-	-	-	-
Update User LOA	Appl & Ent Srch	Appl & Ent Srch	-	Appl & Ent Srch	Appl & Ent Srch	-	-	-	-
View User Details	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch
View User Details (includes view pending requests)	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch
View User Details (includes view role details)	Appl Srch Only	Appl Srch Only	Appl Srch Only	Appl Srch Only	Appl Srch Only	Appl Srch Only	Appl Srch Only	Appl Srch Only	Appl Srch Only
View User Details (includes view role summary)	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch
View List of MFA Devices	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch	Appl & Ent Srch

Legend: Appl = Application Search Ent = Enterprise Search

Figure 31: Application and Enterprise Search Capabilities Matrix

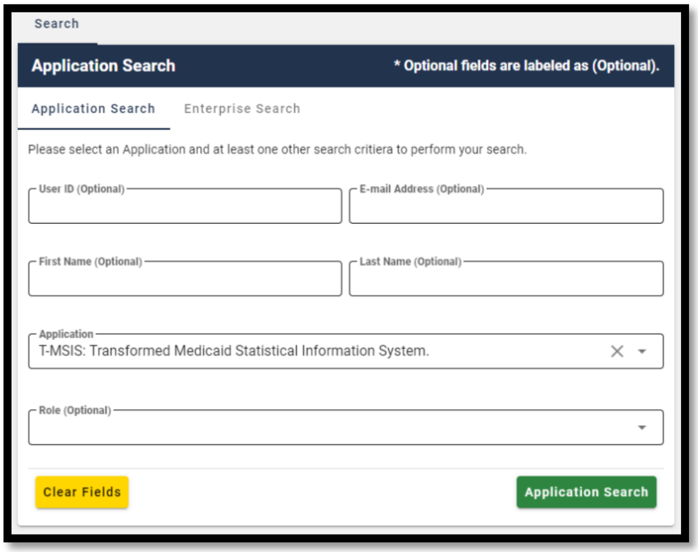
14.4 How to Perform an Application Search

The Application Search allows users with Tier 1 Help Desk capabilities to search for and assist users in their application.

The Application Search stops returning results after **50** records are returned. Users whose search results exceed this limit must use additional parameters to refine their search.

The procedure that follows provides the steps to perform an Application Search using the Help Desk UI ***Application Search*** button.

1) Click the ***Help Desk/Manage Users*** button. The Application Search form appears.



Search

Application Search * Optional fields are labeled as (Optional).

Application Search Enterprise Search

Please select an Application and at least one other search critiera to perform your search.

User ID (Optional)

E-mail Address (Optional)

First Name (Optional)

Last Name (Optional)

Application: T-MSIS: Transformed Medicaid Statistical Information System.

Role (Optional)

Clear Fields Application Search

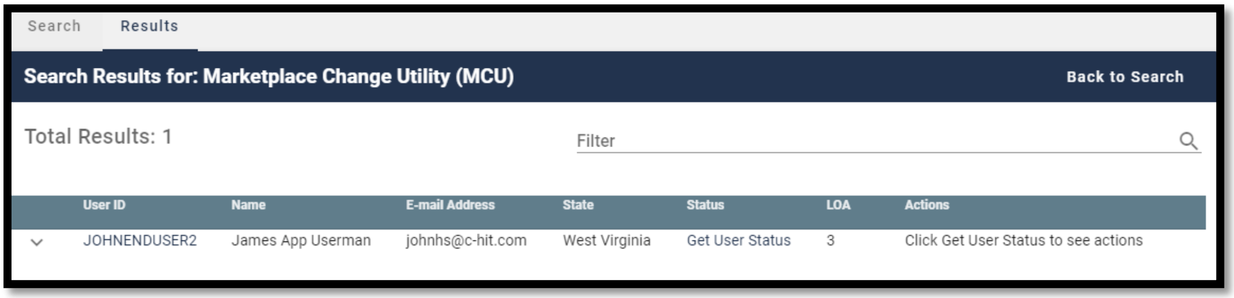
Figure 32: Help Desk Application Search Form

2) Select an application from the ***Application*** list. The Role list appears.

3) (Optional) Select a role from the ***Role*** list. Selecting a Role will limit the search to users who possess that role within the application.

4) (Optional) Enter any combination of User ID, Email Address, First Name or Last Name. Doing so will limit the number of search results to the combination of those parameters plus the application and role.

5) Click the ***Application Search*** button. The screen refreshes and the search results appear. If the search does not return results, the system displays a warning message that directs the user to refine their search parameters and submit another search.



Search Results for: Marketplace Change Utility (MCU)

Total Results: 1

	User ID	Name	E-mail Address	State	Status	LOA	Actions
⌄	JOHNENDUSER2	James App Userman	johnhs@c-hit.com	West Virginia	Get User Status	3	Click Get User Status to see actions

Figure 33: Help Desk Application Search Results

6) Perform the desired Help Desk User management functions as described in later sections of this guide.

14.5 How to Perform an Enterprise Search

The Enterprise Search allows users with Help Desk capabilities to search for users without limitation to the specific application. It is intended to allow Help Desks to assist users who either do not have a role and therefore cannot be found using Application Search, or who have called a Help Desk for an application other than their own.

All Enterprise Search form fields are considered to be optional parameters; however the Enterprise search form requires that any search contain at least a First Name and Last Name, or a User ID, or an Email Address parameter.

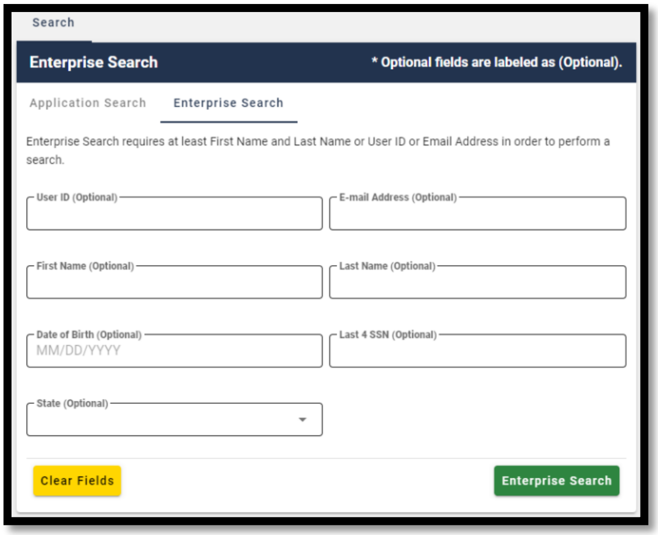
The Enterprise Search will stop returning results after **5** records are returned. Users whose search results exceed this limit will need to refine their search using additional search parameters.

The procedure that follows provides the steps to perform an Enterprise Search using the Help Desk UI ***Enterprise Search*** button.

1) Click the ***Help Desk/Manage Users*** button. The Application Search form appears for Application (Tier 1) Help Desk Users or the Enterprise Search form appears for IDM (Tier 2) Help Desk Users.

2) (Application Help Desk Users only) Click the ***Enterprise Search*** button.

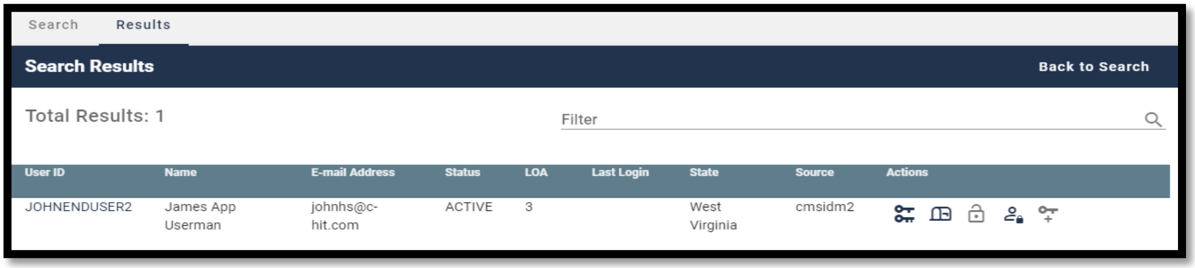
The Enterprise Search Form appears.



Enterprise Search requires at least First Name and Last Name or User ID or Email Address in order to perform a search.

Figure 34: Help Desk Enterprise Search Form

3) Enter any combination of User ID <u>or</u> Email Address <u>or</u> First Name <u>and</u> *Last Name*.
4) (Optional) Enter any combination of Date of Birth, <u>or</u> Last 4 SSN. Doing so will limit the number of search results to the combination of those parameters plus the parameters selected in Step 3.
5) (Optional) Select a State from the list. Doing so will limit the search to users whose account information matches the state plus the combination parameters selected in previous steps.
6) Click the ***Enterprise Search*** button. The screen refreshes and the search results appear.



Total Results: 1

User ID	Name	E-mail Address	Status	LOA	Last Login	State	Source	Actions
JOHNENDUSER2	James App Userman	johnhs@c-hit.com	ACTIVE	3		West Virginia	cmsidm2	

Figure 35: Help Desk Enterprise Search Results

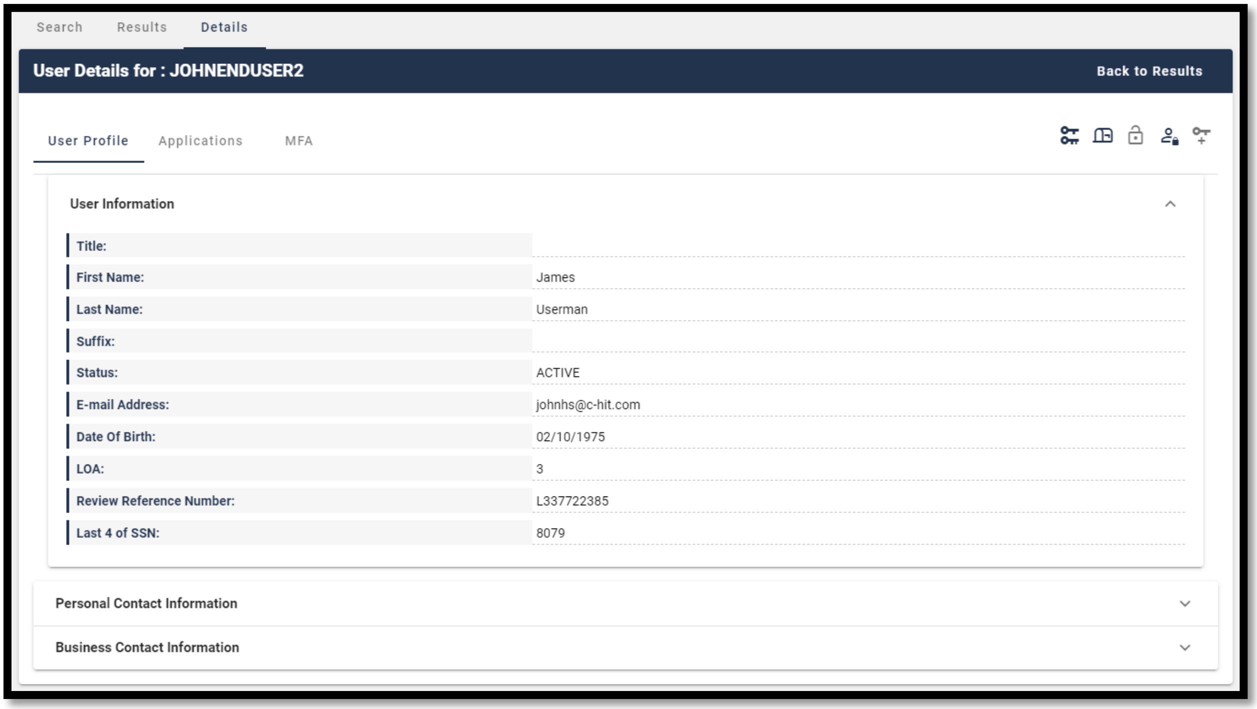
7) Perform the desired Help Desk User management functions as described in later sections of this guide.

14.6 How to View a User’s Profile

The procedure in this section provides the steps to view a user’s profile. The User Profile view provides “read-only” access.

1) Perform an Application Search according to the procedure in **Section 14.4 How to Perform an Application Search** or an Enterprise Search according to the procedure in **Section 14.5 How to Perform an Enterprise Search**. The screen refreshes and the search results appear.

2) Click the ***User ID*** JOHNENDUSER2 for the desired user. The screen refreshes, the User Details window appears and displays the User Profile information.


Search
Results
Details
User Details for : JOHNENDUSER2
Back to Results
User Profile
Applications
MFA
User Information
Personal Contact Information
Business Contact Information

Title:	
First Name:	James
Last Name:	Userman
Suffix:	
Status:	ACTIVE
E-mail Address:	johnhs@c-hit.com
Date Of Birth:	02/10/1975
LOA:	3
Review Reference Number:	L337722385
Last 4 of SSN:	8079

Figure 36: User Details User Profile Tab

3) (Optional) Click the ***Expand Detail*** button ⌄ to display or hide the details of the user’s personal contact Information and the user’s business contact information.

14.7 How to View a Summary of a User’s Applications

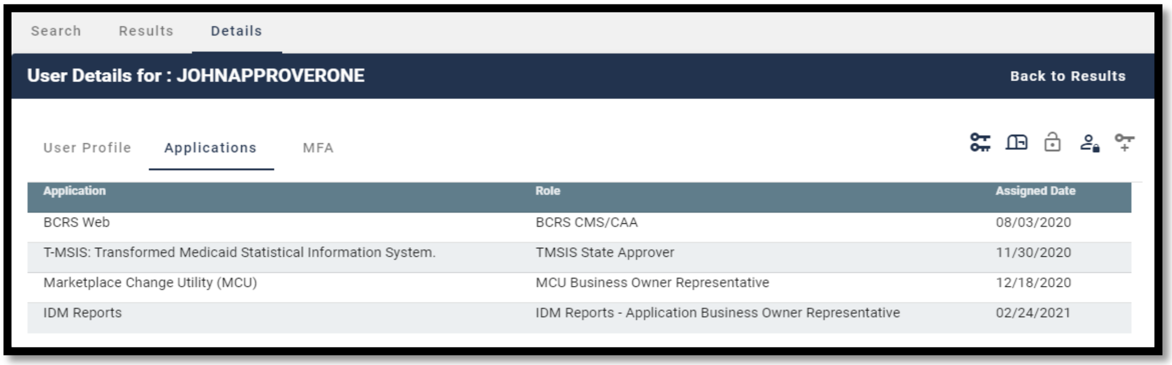
The procedure in this section provides the steps to view a user’s applications.

Note: Role Management controls and functions are only available for Application Search results, additionally, the Help Desk user must possess the capability to access those functions.

1) Perform an Application Search according to the procedure in **Section 14.4 How to Perform an Application Search** or an Enterprise Search according to the procedure in **Section 14.5 How to Perform an Enterprise Search**. The screen refreshes and the search results appear.

2) Click the ***User ID*** JOHNAPPROVERONE for the desired user. The screen refreshes, the User Details window appears and displays User Profile information.

3) Click the ***Applications*** tab. A summary of the user's Applications is displayed.

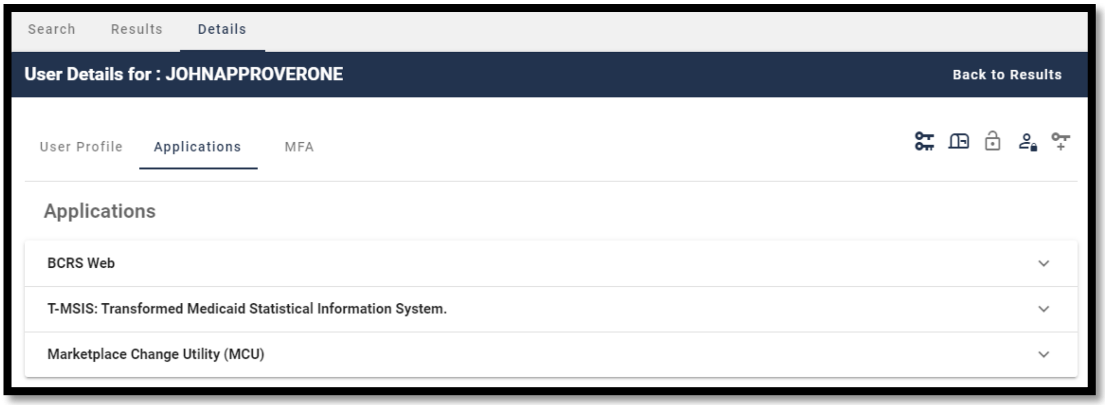


User Details for : JOHNAPPROVERONE

User Profile | Applications | MFA

Application	Role	Assigned Date
BCRS Web	BCRS CMS/CAA	08/03/2020
T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State Approver	11/30/2020
Marketplace Change Utility (MCU)	MCU Business Owner Representative	12/18/2020
IDM Reports	IDM Reports - Application Business Owner Representative	02/24/2021

Figure 37: Enterprise Search Results - Applications Tab



User Details for : JOHNAPPROVERONE

User Profile | Applications | MFA

Applications

- **BCRS Web**
- **T-MSIS: Transformed Medicaid Statistical Information System.**
- **Marketplace Change Utility (MCU)**

Figure 38: Application Search Results - Applications Tab

4) (If applicable) Click the ***Expand Detail*** button. ⌄ A summary of role information for the desired application appears. [37]

5) (If applicable) Click the ***Hide Detail*** button. ⌃ The summary of role information for that application is hidden.

14.8 How to Remove a Single Role

Help Desk Users who possess the proper privileges can use either the **Application Search Results** window or the **User Details Applications** tab and the ***Remove Now*** button to remove a single role from the account of another user.

[37] The Remove Now and Add to Remove Cart controls are displayed for the respective role if the Help Desk user has been granted access to that capability.

> Note: The IDM System will display a warning message if the role removal or attribute removal operation could affect the last approver of an organization that still has users associated with that role or attribute. Such users could be left in an “orphaned” state without an approver of record for future role requests.

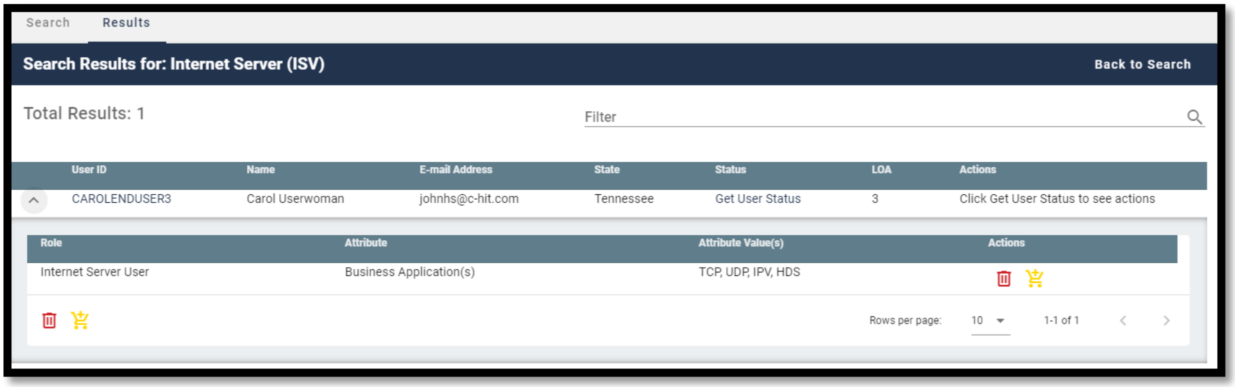
The procedure in this section provides the steps to remove a single role from an individual user’s account using the Help Desk UI ***Remove Now*** button.

1) Perform an Application Search according to the procedure in **Section 14.4 How to Perform an Application Search.**

> Note: Step 2a provides the sequence of steps that must be followed when using the **Application Search Results** window, while Step 2b provides the sequence of steps that must be followed when using the **User Details Application** tab. Both options provide access to the controls that are described in this procedure.

2a) **This option uses the Application Search Results window.**

A. Click the ***Expand Detail*** button. ⌄ A summary of the user’s role/attribute information for the desired application appears and the ***Remove Now*** and ***Add to Cart*** buttons appear.



Total Results: 1

	User ID	Name	E-mail Address	State	Status	LOA	Actions
^	CAROLENDUSER3	Carol Userwoman	johnhs@c-hit.com	Tennessee	Get User Status	3	Click Get User Status to see actions

Role	Attribute	Attribute Value(s)	Actions
Internet Server User	Business Application(s)	TCP, UDP, IPV, HDS	

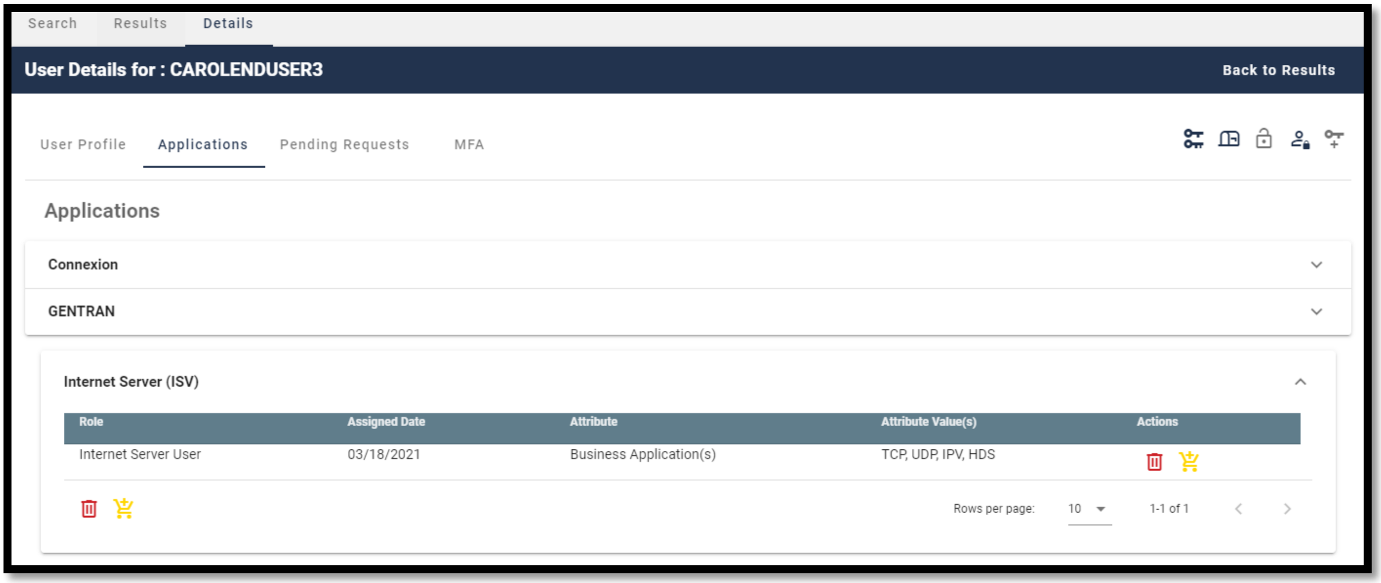
Figure 39: Application Search Results

2b) **This option uses the User Details Applications tab.**

A. Click the ***User ID*** for the desired user. The screen refreshes and the User Profile information appears.

B. Click the ***Applications*** tab. A summary of the user’s applications appears.

C. Click the ***Expand Detail*** button. A summary of the user's role/attribute information appears and the ***Remove Now*** and ***Add to Cart*** buttons appear.



Role	Assigned Date	Attribute	Attribute Value(s)	Actions
Internet Server User	03/18/2021	Business Application(s)	TCP, UDP, IPV, HDS	

Figure 40: User Details Applications Tab

3) Click the ***Remove Now*** button for the role that requires removal. The Remove Role/Attribute window appears.

4) Enter a justification and click the ***Remove Selected Roles*** button.

5) The Help Desk UI displays Request ID information and a message that informs the Help Desk User that the request was successfully submitted. [38]

14.9 How to Remove Multiple Roles

A Help Desk User who possesses the proper privileges can use either the **Application Search Results** window or the **User Details Applications** tab and the ***Remove All Now*** button to remove multiple roles from user accounts in a single operation.

[38] The system sends an email to the affected user's email address on record which indicates that a role has been removed from their account. It also indicates where the user can obtain assistance if they have questions.

Note: The IDM System will display a warning message if the role removal or attribute removal operation could affect the last approver of an organization that still has users associated with that role or attribute. Such users could be left in an “orphaned” state without an approver of record for future role requests.

The procedure in this section provides the steps to remove multiple roles in a single operation using the Help Desk UI ***Remove All Now*** button.

1) Perform an Application Search according to the procedure in **Section 14.4 How to Perform an Application Search.**

Note: Step 2a provides the sequence of steps that must be followed when using the **Search Results window**, while Step 2b provides the sequence of steps that must be followed when using the **User Details Application tab**. Both options provide access to the controls that are described in this procedure and illustrated by **Figure 41: List of User’s Roles / Attributes**.

2a) **This option uses the Search Results window**.

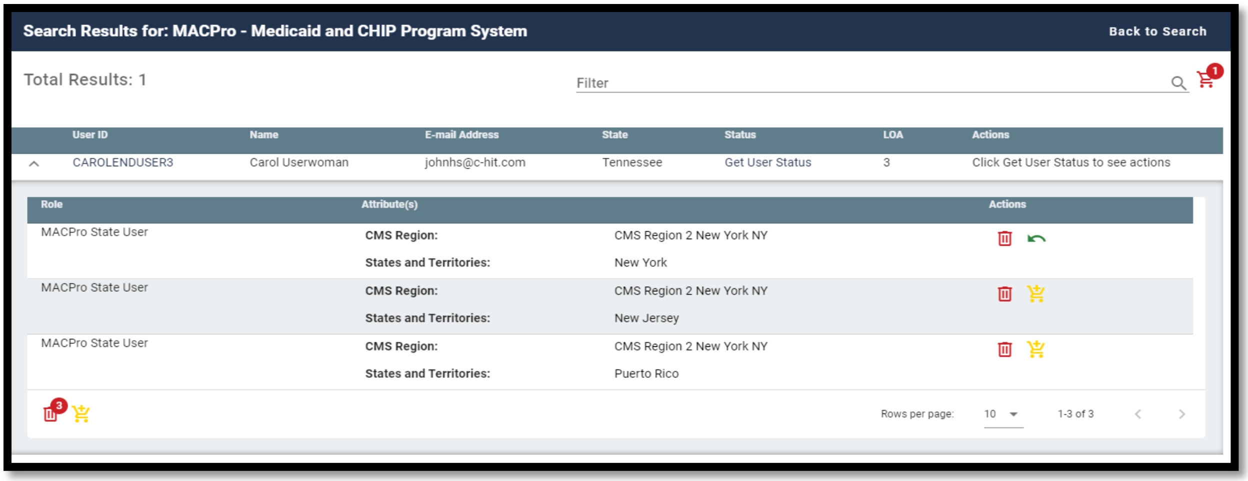
A. Click the ***Expand Detail*** button. A list of the user’s role/attribute information for the desired application appears and the ***Remove Now*** and ***Add to Cart*** buttons appear.

2b) **This option uses the User Details Applications tab**.

A. Click the ***User ID*** for the desired user. The screen refreshes and the User Profile information appears.

B. Click the ***Applications*** tab. A list of the user’s applications appears.

C. Click the ***Expand Detail*** button. A list of the user’s role/attribute information appears and the ***Remove Now*** and ***Add to Cart*** buttons appear.



Search Results for: MACPro - Medicaid and CHIP Program System

Back to Search

Total Results: 1

Filter

User ID	Name	E-mail Address	State	Status	LOA	Actions
CAROLENDUSER3	Carol Userwoman	johnhs@c-hit.com	Tennessee	Get User Status	3	Click Get User Status to see actions

Role	Attribute(s)		Actions
MACPro State User	CMS Region:	CMS Region 2 New York NY	
	States and Territories:	New York	
MACPro State User	CMS Region:	CMS Region 2 New York NY	
	States and Territories:	New Jersey	
MACPro State User	CMS Region:	CMS Region 2 New York NY	
	States and Territories:	Puerto Rico	

Rows per page: 10 1-3 of 3

Figure 41: List of User's Roles / Attributes

3) Click the ***Add to Cart*** button for the individual role that requires removal. The ***Remove From Cart*** button appears.[39]

4) (Optional) Click the ***Remove from Cart*** button for any role that should not be removed.

5) The ***Remove All Now*** button appears and increments by "1" for each role that is added to the remove queue. It will also decrease by "1" for each role that is removed from the Cart.

[39] (Optional) Click the ***Add to Cart*** button at the bottom left corner of the window to add all roles displayed on the current page to the remove queue.

6) Click the ***Remove All Now*** button. The Remove Role/Attribute window appears.[40]

7) (Optional) Review the list and click the ***Remove from Cart*** button for any role that should not be removed.

8) Enter a justification and click the ***Remove Selected Roles*** button. The Help Desk UI displays Request ID information and a message that informs the Help Desk User that the request was successfully submitted.[41]

14.10 How to Cancel Pending Requests

A Help Desk User who possesses the proper privileges can cancel pending requests for other users which they manage.

The following procedure provides the steps to cancel pending requests using the *Help Desk UI* ***Cancel Pending Role Request*** button.

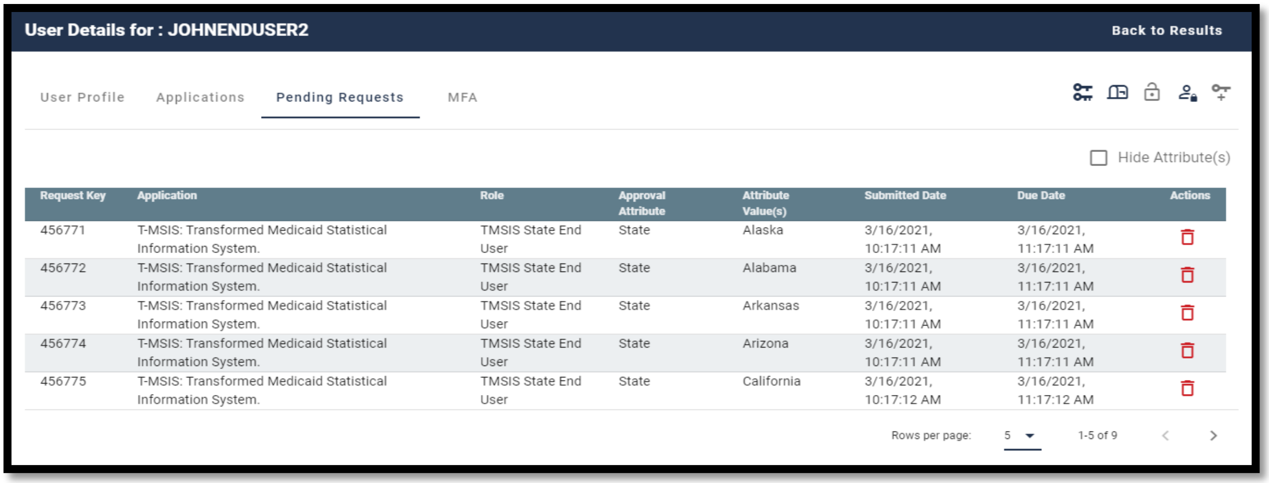
1) Perform an Application Search according to the procedure in **Section 14.4 How to Perform an Application Search.**

2) Click the ***User ID*** JOHNENDUSER2 for the desired user. The screen refreshes, the User Details window appears and displays User Profile information.

3) Click the ***Pending Requests*** tab. Pending Requests A list of the user's pending requests appears.

[40] (Optional) Click the ***Remove All Now*** button located at the bottom left of the window to remove all roles displayed on the current page.

[41] The system sends an email to the affected user's email address on record which indicates that a role has been removed from their account. It also indicates where the user can obtain assistance if they have questions.



User Details for : JOHNENDUSER2

□ Hide Attribute(s)

Request Key	Application	Role	Approval Attribute	Attribute Value(s)	Submitted Date	Due Date	Actions
456771	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State End User	State	Alaska	3/16/2021, 10:17:11 AM	3/16/2021, 11:17:11 AM	🗑
456772	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State End User	State	Alabama	3/16/2021, 10:17:11 AM	3/16/2021, 11:17:11 AM	🗑
456773	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State End User	State	Arkansas	3/16/2021, 10:17:11 AM	3/16/2021, 11:17:11 AM	🗑
456774	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State End User	State	Arizona	3/16/2021, 10:17:11 AM	3/16/2021, 11:17:11 AM	🗑
456775	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State End User	State	California	3/16/2021, 10:17:12 AM	3/16/2021, 11:17:12 AM	🗑

Rows per page: 5 ▾ 1-5 of 9 < >

Figure 42: User Details Pending Requests Tab

4) Click the ***Cancel Pending Role Request*** button 🗑 for the role request that requires removal. The Cancel Pending Role Request decision window appears.

5) Enter a justification and click the ***Cancel Pending Role Request*** button. The Help Desk UI displays Request ID information and a message that informs the Help Desk User that the request was successfully submitted. [42]

14.11 How to View a User's MFA Devices

Help Desk Users use the ***MFA*** tab to view a summary of a user's MFA devices while viewing the User Details of an Application search or an Enterprise search.

This summary consists of the following information:

- **Factor** - The type of MFA device. The IDM system supports Email, Interactive Voice Response (IVR), Short Message Service (SMS), Okta, and Google Authenticator.
- **Device** - The identifier assigned to the device. It may be a phone number, User ID, or email address.
- **Provider** - The service provider of the MFA device.
- **Status** - The device state. Active devices are ready for use. Devices that are Pending are not ready and must be activated by the user.

[42] The system sends an email to the affected user's email address on record which indicates that a role has been removed from their account. It also indicates where the user can obtain assistance if they have questions.

- **Create Date** - The date that the device was activated in the user's profile, or the date the device entered Pending Activation status.

The following procedure provides the steps to view a summary of a user's MFA devices using the Help Desk UI ***MFA*** tab.

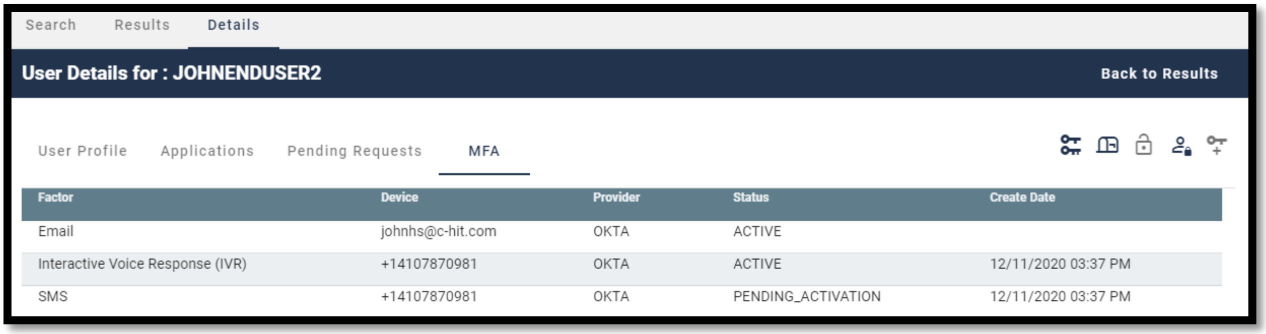
1) Perform an Application Search according to the procedure in **Section 14.4 How to Perform an Application Search** or an Enterprise Search according to the procedure in **Section 14.5 How to Perform an Enterprise Search**. The Search Results window appears.

2) Click the ***User ID*** for the desired user. The User Details window appears and displays the User Profile information.

JOHNENDUSER2

3) Click the ***MFA*** tab. The MFA device summary appears.

MFA



User Details for : JOHNENDUSER2

Factor	Device	Provider	Status	Create Date
Email	johnhs@c-hit.com	OKTA	ACTIVE	
Interactive Voice Response (IVR)	+14107870981	OKTA	ACTIVE	12/11/2020 03:37 PM
SMS	+14107870981	OKTA	PENDING_ACTIVATION	12/11/2020 03:37 PM

Figure 43: User Details MFA Device Summary

14.12 How to Update a User's Email Address

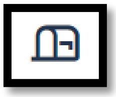
A Help Desk User who possesses the proper privileges can use the Help Desk UI ***Update Email Address*** button to update the email address of another user.

The following procedure provides the steps to update a user's email address using the Help Desk UI ***Update Email Address*** button.

Note: Subsequent to a Help Desk initiated email address change, that user's email MFA device information will not appear in the Help Desk User's MFA Device view until that user signs into the system again.

1) Perform an Application Search according to the procedure in **Section 14.4 How to Perform an Application Search** or an Enterprise Search according to the procedure in **Section 14.5 How to Perform an Enterprise Search**. The Search Results window appears.

2) (Application Search Users Only) Click the ***Get User Status*** button. The Update E-mail Address button appears under the “Actions” column.



3) Click the ***Update E-Mail Address*** button for the desired user. The Update E-Mail Address window appears.
4) Enter the new email address.
5) Enter a justification and click the ***Update E-Mail Address*** button. The system displays a message that indicates the operation completed successfully

14.13 How to Reset a User’s Password (Email Reset Method)

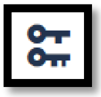
When a user is unable to reset their password using the IDM System Self Service Dashboard, that user may request the assistance of a Help Desk User to initiate a password change operation by sending a Password Reset email to the requesting user. The email is sent to the email address that is currently listed in the user’s profile and contains a hyperlink to the IDM System password reset mechanism.

The procedure that follows provides the steps to reset a user’s password using the Help Desk UI ***Reset Password*** button and the ***Email Reset*** option.

Note: The user will not be able to complete the instructions provided by the hyperlink if they do not remember the security question answer which they established when they created their account.

1) Perform an Application Search according to the procedure in **Section 14.4 How to Perform an Application Search** or an Enterprise Search according to the procedure in **Section 14.5 How to Perform an Enterprise Search**. The Search Results window appears.

2) (Application Search Users Only) Click the ***Get User Status*** button. The ***Reset Password*** button appears under the “Actions” column.



3) Click the ***Reset Password*** button for the desired user. The Reset Password window appears.
4) Click the “***E-Mail a Password Reset link to the User***” option and enter a justification.

5) Click the ***Reset Password*** button. The system displays a message which indicates the operation completed successfully. [43] [44]

14.14 How to Reset a User’s Password (Temporary Password Method)

When a user is unable to reset their password using the IDM System Self Service Dashboard, that user may request the assistance of a Help Desk User to initiate a password change operation by providing a Temporary Password to the requesting user. This method provides a means for the Help Desk User to provide the temporary password to the user verbally over the phone, via a text message, or other form of communication.

The procedure that follows provides the steps to reset a user’s password using the Help Desk UI ***Reset Password*** button and ***Temporary Password*** option.

1) Perform an Application Search according to the procedure in **Section 14.4 How to Perform an Application Search** or an Enterprise Search according to the procedure in **Section 14.5 How to Perform an Enterprise Search**. The Search Results window appears.

2) (Application Search Users Only) Click the ***Get User Status*** button. The ***Reset Password*** button appears under the “Actions” column.

3) Click the ***Reset Password*** button for the desired user. The Reset Password window appears.

4) Click the “***Display a temporary password on-screen***” option and enter a justification.

5) Click the ***Reset Password*** button. The Reset Password window refreshes and displays a temporary password.

6) Provide the temporary password to the user. [45]

[43] The user is required to complete the Reset Password operation by clicking the Password Reset hyperlink in the email and following the on-screen prompts.

[44] The Reset Password hyperlink expires after four hours have elapsed. The user will be required to repeat this entire procedure if the link expires.

[45] Help Desk Users bear the responsibility to properly authenticate the end user before giving them the temporary password.

7) Click the ***Close*** button. The system displays a message which indicates the operation completed successfully. [46] [47]

14.15 How to Unlock a User's Account

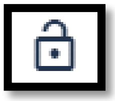
A Help Desk User who possesses the proper privileges can use the Help Desk UI ***Unlock Account*** button to unlock a user's account.

Note: The Unlock Account button will not be selectable unless the user's account is in a locked state **and** the Help Desk user possesses account unlock privileges.

The procedure that follows provides the steps to unlock a user's account using the ***Unlock Account*** button.

1) Perform an Application Search according to the procedure in **Section 14.4 How to Perform an Application Search** or an Enterprise Search according to the procedure in **Section 14.5 How to Perform an Enterprise Search**. The Search Results window appears and indicates the user's status is "LOCKED_OUT".

2) (Application Search Users Only) Click the ***Get User Status*** button. The ***Unlock Account*** button appears under the "Actions" column.

3) Click the ***Unlock Account*** button  for the desired user. The Unlock Account window appears.

4) Enter a justification and click the ***Unlock Account*** button. the system displays a message that indicates the operation completed successfully.

14.16 How to Suspend a User's Account

A Help Desk User who possesses the proper privileges can use the Help Desk UI ***Suspend Account*** button to suspend the account of another user.

Note: Once suspended, a user's account can only be unsuspended by Tier 2 Help Desk personnel.

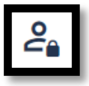
[46] The user is required to complete the Reset Password operation by signing into the IDM System with the temporary password while following any on-screen prompts that appear.

[47] The user is required to change their password when they sign into the system.

The procedure that follows provides the steps to suspend a user's account using the ***Suspend Account*** button.

1) Perform an Application Search according to the procedure in **Section 14.4 How to Perform an Application Search** or an Enterprise Search according to the procedure in **Section 14.5 How to Perform an Enterprise Search**. The Search Results window appears.

2) (Application Search Users Only) Click the ***Get User Status*** button. The ***Suspend Account*** button appears under the "Actions" column.



3) Click the ***Suspend Account*** button for the desired user. The Suspend Account window appears.
4) Click the "***I confirm that I want to Suspend the User's Account***" option.
5) Enter a justification and click the ***Suspend Account*** button. The system displays a message that indicates the user's account is suspended. [48] [49]

14.17 How to Update a User's Level of Assurance (LOA)

A Help Desk User who possesses the proper privileges can use the Help Desk UI ***Update LOA*** button to change a user's LOA.

Note: The Update LOA function is optional and configurable by application. The criteria that is used to determine the eligibility of a Help Desk User to obtain access to the Update LOA function depends on the application's established process. Help Desk Users who require the Update LOA function must follow the process that is outlined in **Appendix C: Requesting Configurable Help Desk Privileges.**

Note: A user's LOA cannot be changed if the user's account is suspended.

[48] When a suspended user attempts to sign in, the Sign In window displays a message that informs the user that they are unable to sign in.

[49] When a suspended user attempts to unlock their account, the Sign In window displays a message that informs the user that they do not have the permission to perform the requested action.

The procedure that follows provides the steps to unlock a user's account using the ***Update LOA*** button.

1) Perform an Application Search according to the procedure in **Section 14.4 How to Perform an Application Search** or an Enterprise Search according to the procedure in **Section 14.5 How to Perform an Enterprise Search**. The Search Results window appears. [50]
2) (Application Search Users Only) Click the ***Get User Status*** Button. The ***Update LOA*** button appears under the "Actions" column.

3) Click the ***Update LOA*** button for the desired user. The Update User's LOA window appears.

4) Review the user's information and manually enter the user's SSN if the SSN is required and the field is blank. [51]
5) Use the ***LOA*** menu to select the updated LOA. [52]
6) Use the ***LOA Reason*** menu to select the reason for the LOA update action.
7) Enter a justification and click the ***Update LOA*** button. the system displays a message that indicates the operation completed successfully.

14.18 How to Unsuspend a User's Account

A user whose account was suspended may have their account unsuspended by IDM (Tier 2) Help Desk personnel.

Note: Only an IDM (Tier 2) Help Desk User can unsuspend a user's account if it has been suspended. Consequently, the Unsuspend Account button will only appear on the Help Desk UI of an IDM (Tier 2) Help Desk Users.

The procedure that follows provides the steps to unsuspend a user's account using the Help Desk UI ***Unsuspend Account*** button.

[50] Help Desk Users who require but do not possess the Update LOA function must follow the process that is outlined in **Appendix C: Requesting Configurable Help Desk Privileges**.

[51] The SSN may or may not be required based on the level that the LOA is being raised to and the application(s) the user requires access to. An SSN is required when updating to LOA 3.

[52] A user's LOA can only be raised; it cannot be lowered.

1) Perform an Enterprise Search according to the procedure in **Section 14.5 How to Perform an Enterprise Search** to find a specific user. The Search Results window appears and shows the user’s Status as “***Suspended***”.

2) Click the ***Unsuspend Account*** button 🔓 for the suspended user. The Unsuspend Account window appears.

3) Enter a justification and click the ***Unsuspend Account*** button. The system displays a message that indicates the user’s account is now unsuspended.

14.19 How to Create User Audit Reports

IDM (Tier 2) Help Desk Users have the capability to create User Audit reports using the User Audit button located on the Enterprise Search form.

Note: The capability to create User Audit reports is only available to IDM (Tier 2) Help Desk Users. Consequently audit report creation buttons do not appear on the Enterprise Search form of Application (Tier 1) Help Desk Users.

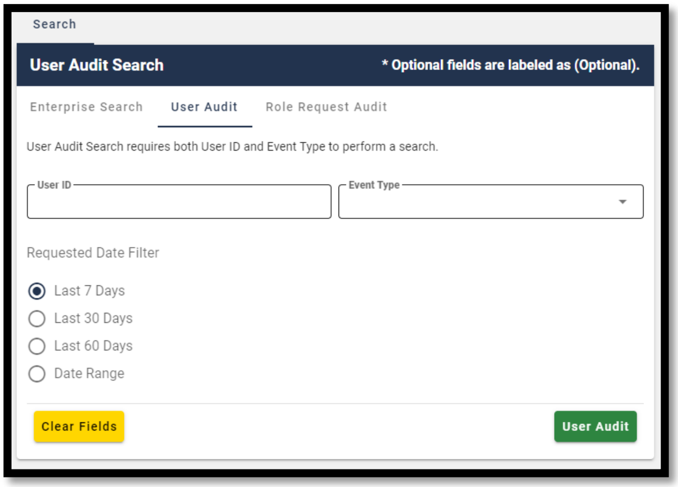
Tier 2 Help Desk Users can create User Audit reports that are created by User Profile, User Authentication, and User Access event types. **Appendix D: User Audit Report Type Summary**

summarizes the information that is contained within each User Audit report.

Help Desk users create User Audit Reports using the procedure that follows.

1) Click the ***Help Desk/Manage Users*** button as described in **Section 14.2 How to Access the Help Desk Functions.** The Enterprise Search form appears.

2) Click the ***User Audit*** button. User Audit The User Audit Search form appears.



Search

User Audit Search

* Optional fields are labeled as (Optional).

Enterprise Search | User Audit | Role Request Audit

User Audit Search requires both User ID and Event Type to perform a search.

User ID

Event Type

Requested Date Filter

● Last 7 Days

○ Last 30 Days

○ Last 60 Days

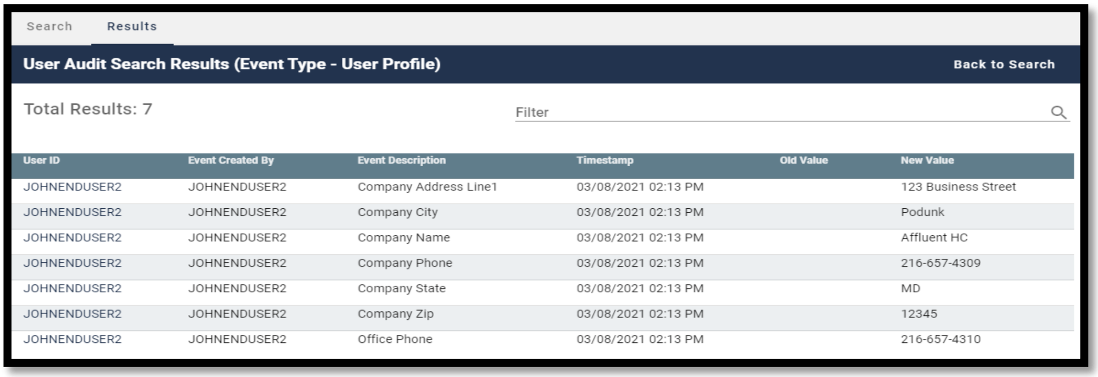
○ Date Range

Clear Fields

User Audit

Figure 44: Help Desk User Audit Search Form

3) Enter a User ID.
4) Select an Event Type from the list.
5) Select a Date Range.
6) Click the ***User Audit*** button. User Audit The screen refreshes and the report appears on the Results tab.



Search Results

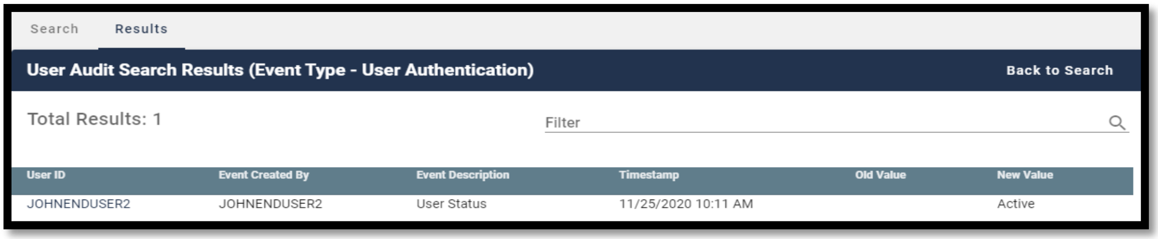
User Audit Search Results (Event Type - User Profile) Back to Search

Total Results: 7

Filter

User ID	Event Created By	Event Description	Timestamp	Old Value	New Value
JOHNENDUSER2	JOHNENDUSER2	Company Address Line1	03/08/2021 02:13 PM		123 Business Street
JOHNENDUSER2	JOHNENDUSER2	Company City	03/08/2021 02:13 PM		Podunk
JOHNENDUSER2	JOHNENDUSER2	Company Name	03/08/2021 02:13 PM		Affluent HC
JOHNENDUSER2	JOHNENDUSER2	Company Phone	03/08/2021 02:13 PM		216-657-4309
JOHNENDUSER2	JOHNENDUSER2	Company State	03/08/2021 02:13 PM		MD
JOHNENDUSER2	JOHNENDUSER2	Company Zip	03/08/2021 02:13 PM		12345
JOHNENDUSER2	JOHNENDUSER2	Office Phone	03/08/2021 02:13 PM		216-657-4310

Figure 45: User Audit Report - User Profile Events



Search Results

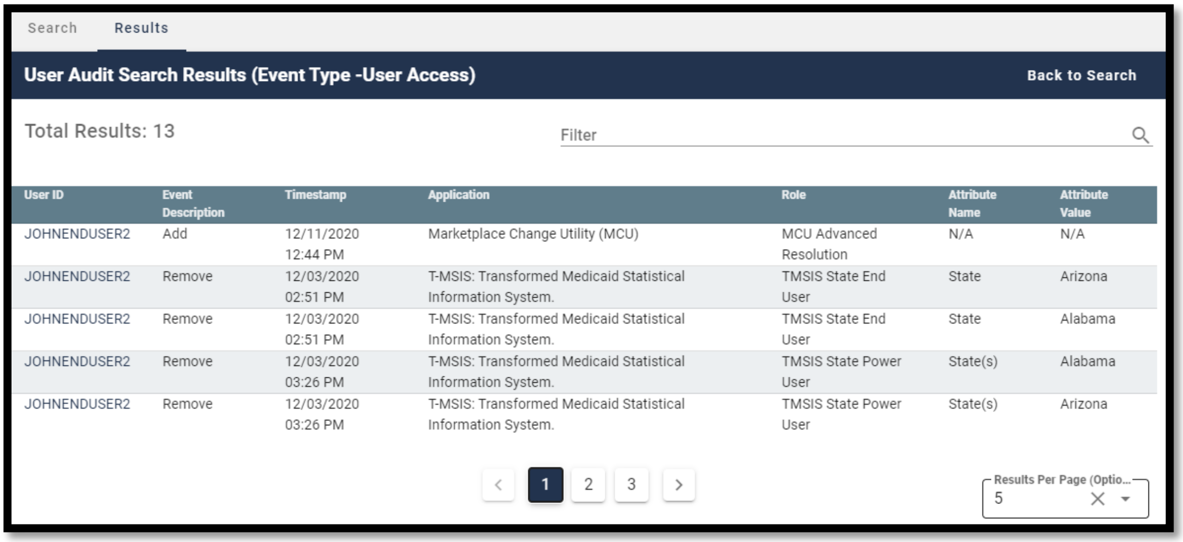
User Audit Search Results (Event Type - User Authentication) Back to Search

Total Results: 1

Filter

User ID	Event Created By	Event Description	Timestamp	Old Value	New Value
JOHNENDUSER2	JOHNENDUSER2	User Status	11/25/2020 10:11 AM		Active

Figure 46: User Audit Report - User Authentication Events



Search Results

User Audit Search Results (Event Type -User Access) Back to Search

Total Results: 13

Filter

User ID	Event Description	Timestamp	Application	Role	Attribute Name	Attribute Value
JOHNENDUSER2	Add	12/11/2020 12:44 PM	Marketplace Change Utility (MCU)	MCU Advanced Resolution	N/A	N/A
JOHNENDUSER2	Remove	12/03/2020 02:51 PM	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State End User	State	Arizona
JOHNENDUSER2	Remove	12/03/2020 02:51 PM	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State End User	State	Alabama
JOHNENDUSER2	Remove	12/03/2020 03:26 PM	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State Power User	State(s)	Alabama
JOHNENDUSER2	Remove	12/03/2020 03:26 PM	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State Power User	State(s)	Arizona

< 1 2 3 >

Results Per Page (Optio... 5

Figure 47: User Audit Report - User Access Events

7) (Optional) Click the ***User ID*** button for the desired event. The Role Audit Details window appears and displays role details for the selected event.

8) Click the ***Back to Results*** button. The search results window appears.

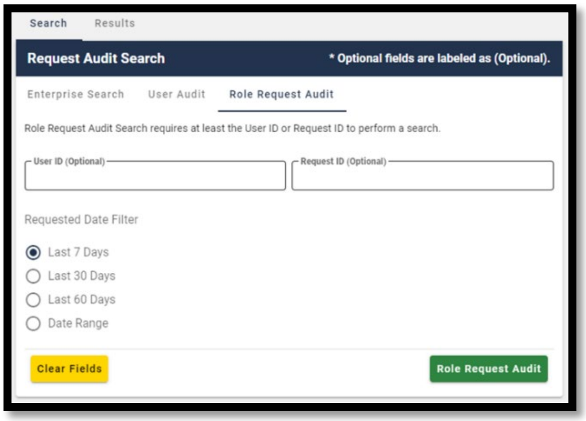
14.20 How to Create Role Request Audit Reports

Tier 2 Help Desk Users have the capability to create Role Request Audit reports using the Role Request Audit button located on the Enterprise Search form.

Note: The capability to create Role Request Audit reports is only available to IDM (Tier 2) Help Desk Users. Consequently audit report creation buttons do not appear on the Enterprise Search form of Application (Tier 1) Help Desk Users.

1) Click the ***Help Desk/Manage Users*** button as described in **Section 14.2 How to Access the Help Desk Functions.** The Enterprise Search form appears.

2) Click the ***Role Request Audit*** button. The Role Request Audit Search form appears.



Role Request Audit Search requires at least the User ID or Request ID to perform a search.

User ID (Optional)

Request ID (Optional)

Requested Date Filter

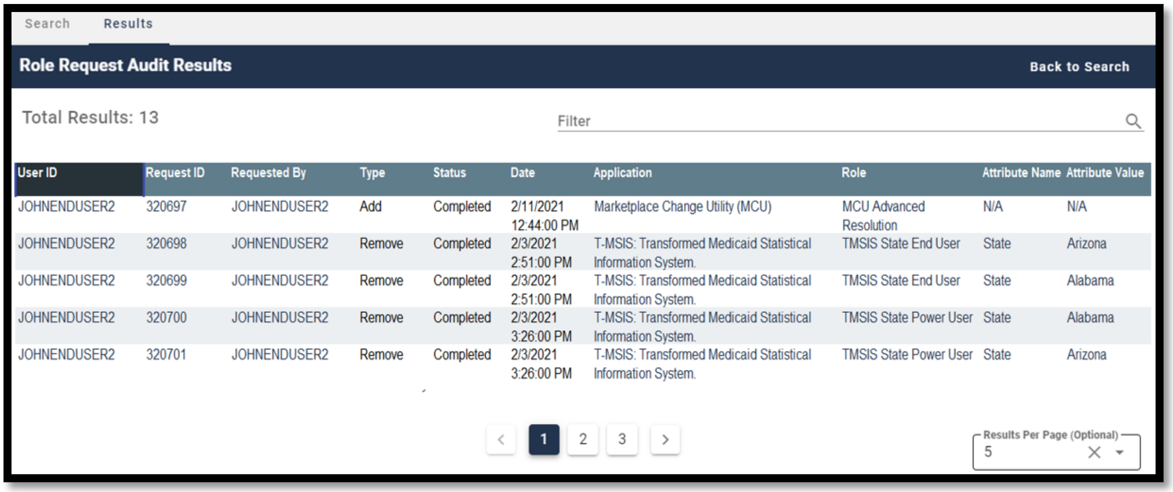
● Last 7 Days
○ Last 30 Days
○ Last 60 Days
○ Date Range

Figure 48: Help Desk Role Request Audit Search Form

3) Enter a User ID or enter a Request ID.

4) Select a Date Range.

5) Click the ***Role Request Audit*** button. The screen refreshes and the report appears on the Results tab.



Total Results: 13

User ID	Request ID	Requested By	Type	Status	Date	Application	Role	Attribute Name	Attribute Value
JOHNENDUSER2	320697	JOHNENDUSER2	Add	Completed	2/11/2021 12:44:00 PM	Marketplace Change Utility (MCU)	MCU Advanced Resolution	N/A	N/A
JOHNENDUSER2	320698	JOHNENDUSER2	Remove	Completed	2/3/2021 2:51:00 PM	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State End User	State	Arizona
JOHNENDUSER2	320699	JOHNENDUSER2	Remove	Completed	2/3/2021 2:51:00 PM	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State End User	State	Alabama
JOHNENDUSER2	320700	JOHNENDUSER2	Remove	Completed	2/3/2021 3:26:00 PM	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State Power User	State	Alabama
JOHNENDUSER2	320701	JOHNENDUSER2	Remove	Completed	2/3/2021 3:26:00 PM	T-MSIS: Transformed Medicaid Statistical Information System.	TMSIS State Power User	State	Arizona

Figure 49: Role Request Audit Report

6) (Optional) Click the ***User ID*** button JOHNENDUSER2 for the desired event. The Role Audit Details window appears and displays role details for the selected event.

7) Click the ***Back to Results*** button. Back to Results The search results window appears.

14.21 How to Manage YubiKey MFA Devices for Use with IDM

Each Application Team/Owner of an Application that uses YubiKey MFA devices to authenticate users is responsible for purchasing, preparing, managing, and distributing the YubiKey MFA devices to the application users.

The procedure in this section provides an overview of the steps that an existing IDM integrated Application Team/Owner follows to enable their Application Users to use a YubiKey MFA device to authenticate to the IDM System.[53]

1) The Application Team/Owner creates the YubiKey Seed File using the procedure outlined in **Section 14.21.1 How to Generate the YubiKey Seed File.**

[53] If the Application is not already an IDM integrated application, the Application Team/Owner also opens an IDM Jira ticket.

2) The Application Team/Owner creates an IDM Service Request (SR) and attaches the YubiKey Seed File.[54]
3) The IDM SR Team processes the IDM SR and hands it off to the IDM Okta Team.
4) The IDM Okta Team creates an IDM Jira Project Story (component=IDM-SR-Okta) then loads the Seed File. The same Seed File can be used in Okta TEST, IMPL, and PROD environments.
5) The IDM Okta Team notifies the Application Team/Owner that the YubiKey Seed File has been loaded and that the YubiKey MFA devices are ready to be used by the Application Users.
6) The Application Users add the YubiKey MFA device to their account using the procedure in **Section 10.6 How to Add a YubiKey MFA Device**. [55]

Note: Once a YubiKey MFA device has been activated on a given user's account, a different user cannot activate that same YubiKey MFA device on their account until:

- The Okta Team revokes the YubiKey MFA device from the original user's account using the procedure in **Section 14.22.1 How to Revoke a YubiKey MFA Device in Okta**.
- The Application Team/Owner creates a new Seed File for that device.
- The IDM Okta Team performs a clean load using the new Seed File.

14.21.1 How to Generate the YubiKey Seed File

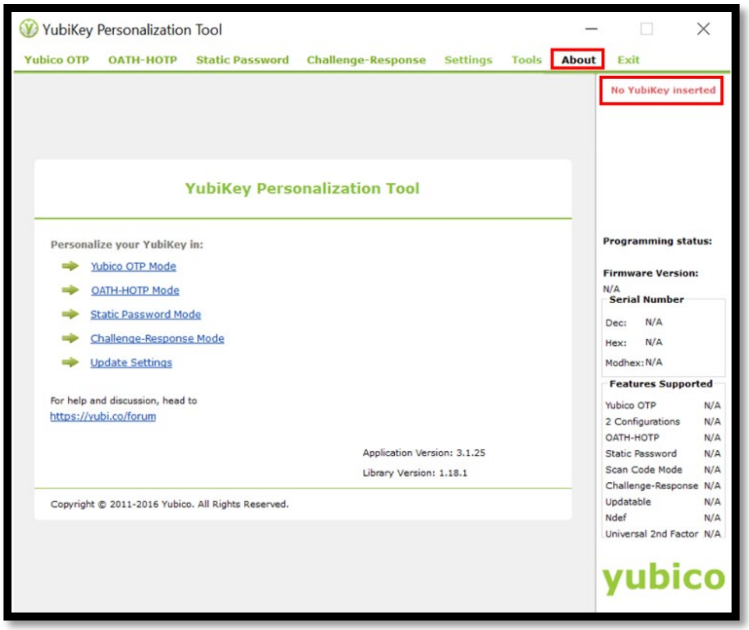
The Application Team/Owner creates the Seed File using the procedure in this section and the YubiKey Personalization Tool. This procedure applies to the creation of the initial Seed File as well as the creation of updated Seed Files. [56]

1) Start the YubiKey Personalization Tool. The YubiKey Personalization Tool UI appears.

[54] The IDM SR process is described on the IDM Confluence page: https://confluenceent.cms.gov/pages/viewpage.action?spaceKey=IDM&title=Service+Request+Process+for+IDM

[55] The Application Team/Owner must create another Seed File whenever a user removes a YubiKey MFA device from their account and later has a need to add that YubiKey MFA device back to their account.

[56] The YubiKey Personalization Tool is available for download from the Yubico website: https://www.yubico.com/support/download/yubikey-personalization-tools/



No YubiKey inserted

YubiKey Personalization Tool

Personalize your YubiKey in:

- Yubico OTP Mode
- OATH-HOTP Mode
- Static Password Mode
- Challenge-Response Mode
- Update Settings

For help and discussion, head to
https://yubi.co/forum

Application Version: 3.1.25
Library Version: 1.18.1

Copyright © 2011-2016 Yubico. All Rights Reserved.

Programming status:

Firmware Version:
N/A

Serial Number

Dec:	N/A
Hex:	N/A
Modhex:	N/A

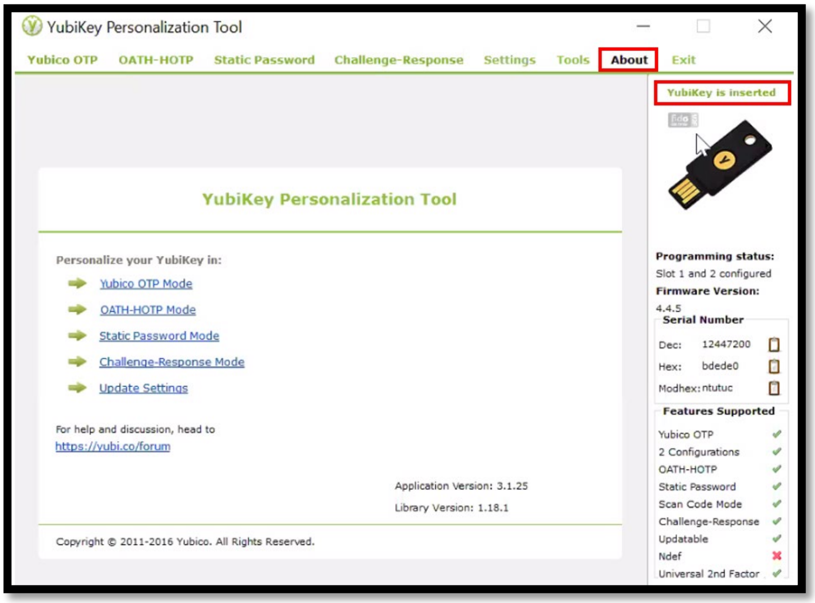
Features Supported

Yubico OTP	N/A
2 Configurations	N/A
OATH-HOTP	N/A
Static Password	N/A
Scan Code Mode	N/A
Challenge-Response	N/A
Updatable	N/A
Ndef	N/A
Universal 2nd Factor	N/A

Figure 50: YubiKey Personalization Tool Startup Window

2) Click the ***About*** tab. The device status message indicates “No YubiKey inserted”.

3) Insert the YubiKey MFA device into a USB port. The device status message changes to “YubiKey is inserted”. An image of the device, the Firmware Version, Serial Number and Features Supported information appears when the device is recognized.



YubiKey is inserted

YubiKey Personalization Tool

Personalize your YubiKey in:

- Yubico OTP Mode
- OATH-HOTP Mode
- Static Password Mode
- Challenge-Response Mode
- Update Settings

For help and discussion, head to
https://yubi.co/forum

Application Version: 3.1.25
Library Version: 1.18.1

Copyright © 2011-2016 Yubico. All Rights Reserved.

Programming status:
Slot 1 and 2 configured

Firmware Version:
4.4.5

Serial Number

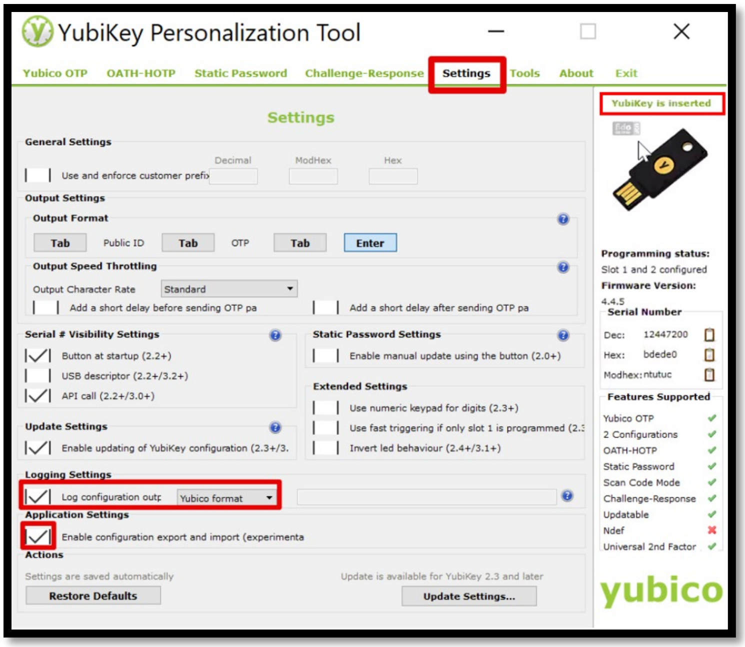
Dec:	12447200
Hex:	bdede0
Modhex:	ntutuc

Features Supported

Yubico OTP	✓
2 Configurations	✓
OATH-HOTP	✓
Static Password	✓
Scan Code Mode	✓
Challenge-Response	✓
Updatable	✓
Ndef	✗
Universal 2nd Factor	✓

Figure 51: YubiKey Personalization Tool - Device Present

4) Click the ***Settings*** tab. The Settings window appears.



General Settings

□ Use and enforce customer prefix — Decimal, ModHex, Hex

Output Settings

Output Format: Tab | Public ID | Tab | OTP | Tab | Enter

Output Speed Throttling

Output Character Rate: Standard

□ Add a short delay before sending OTP pa

□ Add a short delay after sending OTP pa

Serial # Visibility Settings

☑ Button at startup (2.2+)

□ USB descriptor (2.2+/3.2+)

☑ API call (2.2+/3.0+)

Static Password Settings

□ Enable manual update using the button (2.0+)

Extended Settings

□ Use numeric keypad for digits (2.3+)

□ Use fast triggering if only slot 1 is programmed (2.:

□ Invert led behaviour (2.4+/3.1+)

Update Settings

☑ Enable updating of YubiKey configuration (2.3+/3.

Logging Settings

☑ Log configuration outp — Yubico format

Application Settings

☑ Enable configuration export and import (experimenta

Actions

Settings are saved automatically

Update is available for YubiKey 2.3 and later

YubiKey is inserted

Programming status: Slot 1 and 2 configured

Firmware Version: 4.4.5

Serial Number

Dec: 12447200

Hex: bdede0

Modhex: ntutuc

Features Supported

Yubico OTP	✓
2 Configurations	✓
OATH-HOTP	✓
Static Password	✓
Scan Code Mode	✓
Challenge-Response	✓
Updatable	✓
Ndef	✗
Universal 2nd Factor	✓

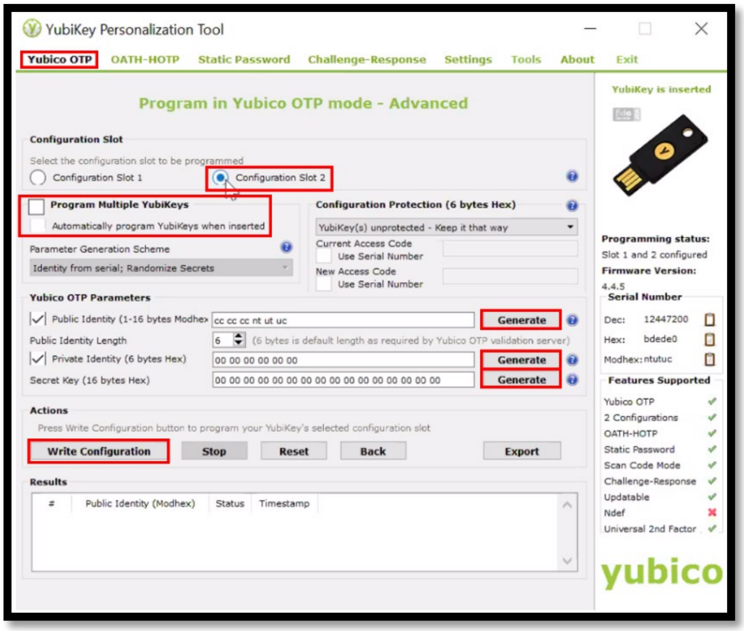
Figure 52: YubiKey Personalization Tool - Settings Tab

5) Locate the ***Logging Settings*** category then check the ***Log configuration output*** box and select ***Yubico format***.

6) Locate the ***Application Settings*** category and check the ***Enable configuration export and import*** box.

7) Click the ***Yubico OTP*** tab. The Program in Yubico OTP mode window appears.

8) Click the ***Advanced*** button. The Program in Yubico OTP mode - Advanced window appears.



Configuration Slot

Select the configuration slot to be programmed

○ Configuration Slot 1 ● Configuration Slot 2

□ Program Multiple YubiKeys

Automatically program YubiKeys when inserted

Parameter Generation Scheme: Identity from serial; Randomize Secrets

Configuration Protection (6 bytes Hex): YubiKey(s) unprotected - Keep it that way

Current Access Code □ Use Serial Number

New Access Code □ Use Serial Number

Yubico OTP Parameters

☑ Public Identity (1-16 bytes Modhex): cc cc cc nt ut uc

Public Identity Length: 6 (6 bytes is default length as required by Yubico OTP validation server)

☑ Private Identity (6 bytes Hex): 00 00 00 00 00 00

Secret Key (16 bytes Hex): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Actions

Press Write Configuration button to program your YubiKey's selected configuration slot

Results

#	Public Identity (Modhex)	Status	Timestamp

YubiKey is inserted

Programming status: Slot 1 and 2 configured

Firmware Version: 4.4.5

Serial Number

Dec: 12447200

Hex: bdede0

Modhex: ntutuc

Features Supported

Yubico OTP	✓
2 Configurations	✓
OATH-HOTP	✓
Static Password	✓
Scan Code Mode	✓
Challenge-Response	✓
Updatable	✓
Ndef	✗
Universal 2nd Factor	✓

Figure 53: YubiKey Personalization Tool - Yubico OTP Tab

9) Locate the ***Configuration Slot*** category and select a ***Configuration Slot***.

10) Locate the Yubico OTP Parameters category and click each of the three ***Generate*** buttons in the Yubico OTP Parameters section.

11) (Optional) If multiple YubiKey MFA devices need to be configured, check the ***Program Multiple YubiKeys*** box and the ***Automatically program YubiKeys when inserted*** box. Doing this will enable personnel to configure the first YubiKey, remove it, then insert the next key until all keys are configured.

12) Click the ***Write Configuration*** button. The configuration data is written to the YubiKey MFA device and a file output window appears. This file is the Seed File.

13) Save the Seed file. The seed file is saved as a comma separated value (CSV).

14) Attach the Seed File to the IDM SR. The IDM SR Team will review the SR and forward the SR and Seed File to the IDM Okta Team.

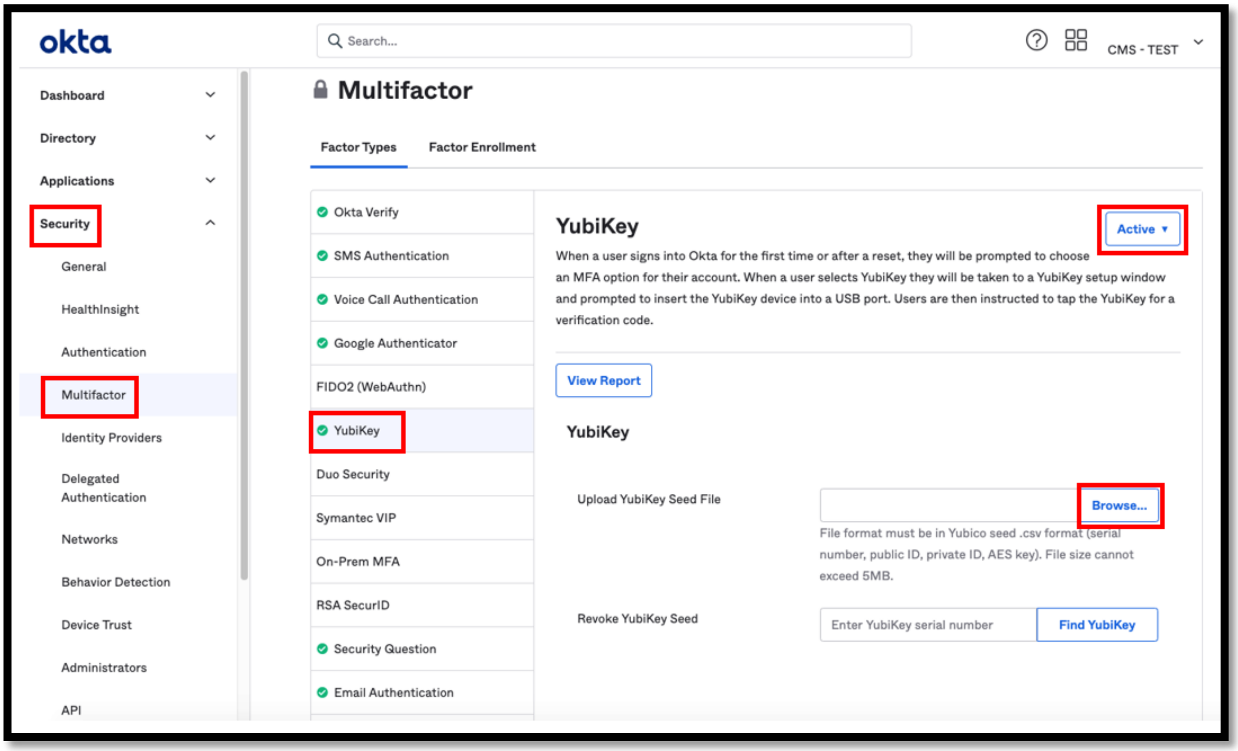
14.21.2 How to Manage YubiKey MFA Devices in Okta

The IDM Okta Team receives the YubiKey Seed File and uploads it to Okta using the procedure in this section. Use the following procedure to create the initial Seed File as well as updated Seed Files.

1) Log in to the Okta Admin Portal.

2) Click the ***Security*** menu option.

3) Click the ***Multifactor*** menu option, then select ***YubiKey***. The YubiKey administration window appears.



YubiKey

When a user signs into Okta for the first time or after a reset, they will be prompted to choose an MFA option for their account. When a user selects YubiKey they will be taken to a YubiKey setup window and prompted to insert the YubiKey device into a USB port. Users are then instructed to tap the YubiKey for a verification code.

YubiKey

Upload YubiKey Seed File

File format must be in Yubico seed .csv format (serial number, public ID, private ID, AES key). File size cannot exceed 5MB.

Revoke YubiKey Seed: Enter YubiKey serial number

Figure 54: Okta YubiKey Administration Window

4) (Optional) Select ***Active*** if the YubiKey status is in any other state. A YubiKey MFA device will have one of the following device statuses in Okta as summarized by **Table 3: YubiKey Device Status List**.

5) Click the ***Browse*** button. Navigate to the location of the YubiKey Seed file and upload it to Okta.

6) Inform the Application Team/Owner that the YubiKeys are now ready for activation by Application Users.

Table 3: YubiKey Device Status List

Device Status	Meaning
Unassigned	The Seed file has been sent to Okta and added to an Okta group, but the YubiKey has not been associated to the user's account.
Active	The YubiKey has been associated to the user's account and is functional.
Revoked	The YubiKey has been removed from the user's account.
Blocked	The YubiKey has been removed by an Okta Admin.

14.21.3 How to Revoke a YubiKey MFA Device in Okta

Once a YubiKey MFA device has been activated by a user and associated to their account, it must be revoked then deleted from Okta before it can be reactivated by the original user or reassigned to a new user. Use the following procedure to revoke a YubiKey so that it may be reactivated or reassigned.

1) Log in to the Okta Admin Portal.

2) Click the ***Security*** menu option.

3) Click the ***Multifactor*** menu option, then select ***YubiKey***. The YubiKey administration window appears as illustrated by **Figure 54: Okta YubiKey Administration Window**.

4) (Optional) Click the ***View Report*** button and obtain the serial number of they YubiKey that will be revoked.

5) Enter the YubiKey serial number into the ***Revoke YubiKey Seed*** field then click the ***Find YubiKey*** button.

6) Confirm the decision to revoke (permanently delete) the YubiKey when the ***Delete YubiKey*** modal appears. A confirmation message appears.

7) Click the ***Done*** button.

Appendix A: Password Policy

Passwords that are used to access the IDM system must conform to the following CMS guidelines:

- Passwords must be at least 8 characters in length.
- Passwords must include an uppercase letter.
- Passwords must include a lowercase letter
- Passwords must include a number (0 - 9).
- Passwords must include one of one special character.
- Passwords must not contain a space.
- Passwords must not be one of the user's last 24 passwords.
- Passwords must not contain parts of the user's First Name, Last Name, or User ID.
- 24 hours must have elapsed since the last password change.

Appendix B: IDM Report Categories

Approved users use the Amazon Web Services (AWS) QuickSight viewer to review the report categories listed in **Table 4: IDM Report Categories** which summarizes the various categories of reports. [57]

Table 4: IDM Report Categories

Category Number	Category Type	Report Name	Report Description
1	IDM Application Report	Application Summary Report	This report displays the user base for an application, and includes the cumulative count by role, of users for the application.
1	IDM Application Report	Annual Certification Summary Report	This report provides a summary of an application's annual certification counts (e.g. how many users certified, got revoked, or are due for certification).
1	IDM Application Report	Pending Certification Report	This report provides a list of an application's users and the roles that are due for certification for a specific date/period.
2	IDM User Report	User Details Report	This report provides detailed user and role-specific information of application users.
2	IDM User Report	User Role Approver Report	This report provides information about user role requests for an application, along with the corresponding details of the approvers who took an action on these requests.
2	IDM User Report	User Annual Certification Report	This report provides the annual certification details (e.g. role name, certification status, last certification date, and next due date) for application users whose certification is due within the next 60 days.
2	IDM User Report	Orphaned Organization Report	This report provides a list of orphaned organizations for the application.

[57] Users who are granted access to the My Reports function do not automatically receive access to every report category. Users are granted access to a set of pre-determined reports based on their specific role.

Category Number	Category Type	Report Name	Report Description
3	IDM Audit Report	Role Request Audit Report	This report provides the history of user role request information for an application.
3	IDM Audit Report	User Audit Report	This report provides the history of user information for an application (e.g. last login date, date of last password change, and account status).
4	IDM Aggregate Reports	IDM User Role Report	This report provides the user base by application, including a cumulative count of users by role for all applications integrated with the IDM System.
4	IDM Aggregate Reports	MAC User Role Report	This report provides user specific and role details for MAC applications.

Appendix C: Requesting Configurable Help Desk Privileges

This Appendix outlines the steps that application Business Owners and Representatives must take to request configurable Help Desk privileges in the IDM system.

1) Define the following details for each Help Desk privilege that will be requested based on information provided in **Table 5: Help Desk Privileges**.

   - Application
   - Role(s) to Update
   - Help Desk Privilege
   - Justification for the privilege

2) Submit an IDM Service Request (SR) that includes the details outlined in Step 1.[58]

Table 5: Help Desk Privileges

	Application Search			Enterprise Search		
	Application Help Desk	**Application Approver**	**IDM Help Desk**	**Application Help Desk**	**Application Approver**	**IDM Help Desk**
Remove Multiple Roles/Attributes	O	O	---	--	--	X
Export Results	X	X	--	--	--	--
View User Details	X	X	--	X	--	X
Update LOA	O	--	--	O	--	X
Lock Account	--	--	--	--	--	X
Unlock Account	--	--	--	X	--	X
Enable User	--	--	--	--	--	X
Disable User	--	--	--	--	--	X
Reset Password (Email)	--	--	--	X	--	X
Reset Password (Manual)	--	--	--	O	--	X
Manage MFA Device	--	--	--	X	--	X
Remove Roles/Attributes	--	O	--	--	--	X
Promote User	--	--	--	--	--	--

Legend: X = Default O = Optional (Configurable) -- = Not Available

[58] The IDM SR process is described on the IDM Confluence page: https://confluenceent.cms.gov/pages/viewpage.action?spaceKey=IDM&title=Service+Request+Process+for+IDM

Appendix D: User Audit Report Type Summary

Table 6: IDM Help Desk User Audit Report Type summarizes the information that is contained within each User Audit report type

Table 6: IDM Help Desk User Audit Report Type

Report Type	Event Description	Old Value	New Value
User Authentication	Last login (successful login)	Null	Last Login Date
User Profile	User account creation	Null	User ID
User Profile	Password change	Null	Null
User Profile	Password reset	Null	Null
User Profile	Account status	Locked/Unlocked	Locked/Unlocked
User Profile	User status	Active/Disabled/Deleted	Active/Disabled/Deleted
User Profile	Update LOA	Old LOA	New LOA
User Profile	Update user profile. (Includes changes made to My Information, Personal Contact Information, and Business Contact Information.)	Old profile information values.	New profile information values.
User Profile	Update security questions and answers.	Null	Null
User Access	Add	Null	New application, role, and attribute information.
User Access	Modify	Old application, role, and attribute information.	New application, role, and attribute information.
User Access	Remove	Old application, role, and attribute information.	Null
User Access	Annual certification status.	Null	Application, role, attribute information, and status (certified/revoked)

Appendix E: Acronyms

Table 7: Acronyms

Acronym	Literal Translation
BCRS	Benefits Coordination and Recovery System
C-HIT	Chags Health Information Technology
CHIP	Children’s Health Insurance Program
CMS	Centers for Medicare & Medicaid Services
CSV	Comma Separated Value
ECRS	Electronic Correspondence Referral System
EIDM	Enterprise Identity Management
EUA	Enterprise User Administration
HD	Help Desk
ID	Identity
IDM	Identity Management
IE	Internet Explorer
IMPL	Implementation Environment
IVR	Interactive Voice Response
LOA	Level of Assurance
MAC	Medicare Administrative Contractor
MFA	Multi-factor Authentication
PIV	Personal Identity Verification
PROD	Production Environment
QA	Quality Assurance
QR	Quick Response
RIDP	Remote Identity Proofing
SMS	Short Message Service
SSN	Social Security Number
SR	Service Request
TEST	Test Environment
UI	User Interface
US	United States
USB	Universal Serial Bus

Appendix F: Approvals

The undersigned acknowledge that they have reviewed this document and agree with the information presented within this document. Changes to this document will be coordinated with, and approved by, the undersigned, or their designated representatives.

Table 8: Approvals

Document Approved By	Date Approved
Carla Layne, EIDM Contracting Officer Representative, CMS	Date
Verne Webster, EIDM Government Task Leader, CMS	Date
Charles Lall, EIDM Project Manager, C-HIT	Date
Micalina Mendoza, EIDM QA Manager, C-HIT	Date